

Trend Micro Incorporated makes no representations or warranties with respect to the contents or use of this document or the product described herein and specifically disclaims any express or implied warranties as to the merchantability and fitness for any particular purpose. Furthermore, Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without any obligation to notify any person or entity of such changes.

InterScan VirusWall is a registered trademark of Trend Micro Incorporated. All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Copyright © 1996-1999, Trend Micro Incorporated. No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

Document Part No.

Release Date: 3-15-99

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend documents, please contact us at **support@trendmicro.com**. Your feedback is always welcome.

Table of Contents

Section I

Introduction & Installation

Chapter 1 Introducing Trend InterScan VirusWall

What is Trend InterScan VirusWall?.....	1-1
Two "flavors" available	1-2
InterScan VirusWall Illustration	1-2
InterScan Overview	1-3
How Does InterScan VirusWall Work?.....	1-3
How InterScan VirusWall Detects Viruses	1-5
What's New In Version 3?.....	1-7
Registering Trend VirusWall.....	1-8
Serial Numbers	1-8

Chapter 2 Installation Planning

Minimum System Requirements	2-2
Deciding Where To Install.....	2-3
Installation Topologies	2-5
E-Mail VirusWall	2-5
E-mail VirusWall Example 1.....	2-6
E-mail VirusWall Example 2.....	2-7
E-mail VirusWall Example 3.....	2-8
E-mail VirusWall Example 4.....	2-9
Web VirusWall	2-10
Web VirusWall Example 1.	2-11
Web VirusWall Example 2.	2-12
Web VirusWall Example 3.	2-13
Web VirusWall Example 4.	2-14

FTP VirusWall	2-15
FTP VirusWall Example 1.....	2-16
FTP VirusWall Example 2.....	2-17

Chapter 3 Installing the Standard or Plugin Edition

Chapter Overview	3-2
Installing InterScan Standard Edition	3-3
After Installing the Plugin Edition.....	3-7
Editing Sendmail.cf.is Manually	3-8
Installed Files	3-9
Opening the InterScan Console	3-10
Starting and Stopping InterScan	3-11
Starting & Stopping InterScan via Command Line ..	3-11
Changing the InterScan Password	3-12
Testing InterScan	3-12
Troubleshooting a Standard Setup	3-13
Uninstalling InterScan	3-14

Chapter 4 Installing InterScan CVP Edition

Installing the CVP Edition	4-3
Configuring InterScan.....	4-6
On the InterScan side.....	4-6
On the FireWall-1 side.....	4-7
Optional: Setting up OPSEC Authentication.....	4-14
Opening the InterScan Console	4-16
Starting and Stopping InterScan	4-16
Changing the InterScan Password	4-17
Testing InterScan	4-18
Troubleshooting a CVP Setup	4-19
Uninstalling InterScan	4-21

Section II

Configuring InterScan

Chapter 5 E-mail VirusWall & Anti-Spam Control

Configuring E-mail Scans.....	5-2
InterScan Standard Edition	5-2
InterScan Plugin Edition	5-5
InterScan CVP Edition.....	5-6
Specifying Which Files to Scan.....	5-6
Setting Virus Notifications	5-7
Setting the Action on Viruses	5-9
Miscellaneous	5-11
Displaying "InterScan" in the E-mail Header	5-11
Limiting Message Size.....	5-11
Protecting Against the "E-mail Security Flaw"	5-12
Logging Transactions... ..	5-12
Temporary Directory Location	5-12
Outbound Mail Processing.....	5-13
E-mail Scan Advanced Options	5-15
General Configuration	5-15
Child Process Configurations	5-17
E-mail VirusWall Plugin Edition.....	5-21
Configuring E-mail VirusWall Plugin Edition	5-21
Anti-Spam Control.....	5-22
Managing Access Lists	5-22

Chapter 6 FTP VirusWall

Configuring FTP Scans.....	6-3
InterScan Standard Edition	6-4
InterScan CVP Edition.....	6-5
Specifying Which Files to Scan.....	6-6
Setting Virus Notifications	6-6
Setting the Action on Viruses	6-8
FTP Scan Advanced Options	6-9

General Configuration	6-10
Child Process Configurations	6-11
Get and Put Mode:	6-14

Chapter 7 Web VirusWall

Configuring Web Scans	7-3
InterScan Standard Edition	7-4
InterScan CVP Edition.....	7-5
Specifying Which Files to Scan.....	7-6
Bypassing Specific MIME Content Types	7-6
Security Preferences	7-7
Setting Virus Notifications	7-8
Setting the Action on Viruses	7-10
Miscellaneous	7-11
HTTP VirusWall Advanced Configurations.....	7-14
General Configuration	7-16
Child Process Configuration.....	7-17

Chapter 8 Manual and Scheduled Scans

Scanning a Drive or Directory... ..	8-2
Setting Virus Notifications	8-5
Scheduled Scans	8-7

Section III

Using InterScan VirusWall

Chapter 9 Log Files, Virus Pattern Updates, and Registration

Specifying the Log Directory	9-2
Viewing or Deleting Log Files	9-3
Getting details on detected viruses	9-4
Common System Log Messages.....	9-5
The Virus Pattern File.....	9-5
Using an HTTP Proxy Server	9-8
Registering InterScan.....	9-9
Registering Over the Internet.....	9-10

Register by Fax	9-11
Registering by Mail	9-11

Chapter 10 Technical Support & the Virus Information Center

Sending Trend Your Viruses	10-2
Virus Information Center.....	10-2
Free Client Scans with HouseCall	10-4
About Computer Viruses	10-5
Types of Viruses	10-5
Virus Writers.....	10-8
How Viruses Spread	10-8
Methods of Virus Detection.....	10-9

Chapter 11 Trend Virus Control System

Installing the Trend VCS Agent	11-3
Configuring the Trend VCS Agent.....	11-5

Chapter 12 Intscan.ini File Settings

[Scan-Configuration]	12-2
[Notification]	12-3
[HTTP].....	12-3
[FTP]	12-7
[SMTP]	12-11
[Periodical-Scan]	12-15
[Manual-Scan]	12-17
[Pattern-Update].....	12-19
[View-Configuration]	12-19
[Registration]	12-22

Section I

Introduction & Installation



- **Chapter 1**
Introducing Trend InterScan VirusWall
- **Chapter 2**
Installation Planning
- **Chapter 3**
Installing InterScan *Standard* or *Plugin* Edition
- **Chapter 4**
Installing InterScan *CVP* Edition

1 Introducing Trend InterScan VirusWall

What is Trend InterScan VirusWall?

Trend InterScan VirusWall® is a suite of antivirus programs that works at the Internet gateway to detect and clean virus-infected files before they can enter your corporate LAN.

- *E-mail VirusWall* monitors all inbound and outbound E-mail messages for viruses, including macro viruses. *E-mail VirusWall* also includes an optional *Plugin* Edition that supports antispam filtering under Sendmail 8.8.6 or later.
- *Web VirusWall* monitors all HTTP traffic and checks for viruses, malicious Java & ActiveX applets. It also provides enterprise-wide Java and Authenticode standards.
- *FTP VirusWall* protects against viruses entering the LAN via FTP file transfers. Or, it can exclusively protect a given server.

In the typical scenario, you would install InterScan to sit, logically, between the clients and the server whose traffic InterScan will check. Physically, this may be the same machine as the server (or proxy) or a different one. InterScan will receive the protocol traffic, scan it in real-time, and then hand it off to the server (or proxy) for processing as usual. InterScan supports most firewalls and network topologies.

Scanning is fast, thorough, and unobtrusive to your clients.

Two "flavors" available

InterScan VirusWall 3 comes in two "flavors," either of which can be installed from the Setup package.

- **InterScan VirusWall *Standard Edition***, which can be installed in any network topology, supports most firewalls, and optionally provides support for spam filtering.
- **InterScan VirusWall *CVP Edition***, which includes support for Check Point Software's *Content Vectoring Protocol*. Install this version if you use FireWall-1 (v. 3.0b build 3064 or later) and want InterScan to act as a CVP server.

InterScan VirusWall Illustration

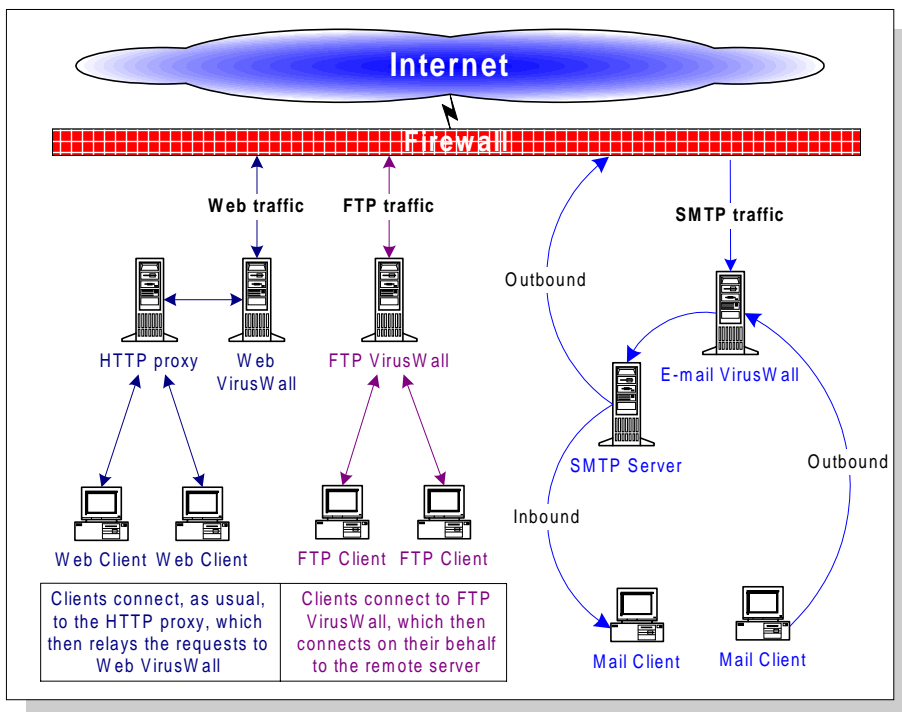


Figure 1-1. This illustration shows Web, FTP, and E-mail VirusWall installed on a LAN. Other Setups are presented in Chapter 2.

InterScan Overview

All three VirusWalls provide a high degree of user configurability. Routine tasks such as virus alert notifications, virus pattern updates, and deleting old log files can be scheduled to occur automatically—just "set and forget."

Additionally, the InterScan administrator can determine which file types are scanned for viruses, the action InterScan takes upon detecting a virus (clean the infected file, delete it, quarantine it, or ignore it), and other program details.

Virus detection occurs using Trend's 32-bit, multi-threading scan engine and a process called pattern matching. In addition to catching known signature viruses, InterScan detects and intercepts previously unknown polymorphic, or mutation, viruses.

For an additional layer of protection, the VirusWalls employ Trend's macro virus scanning engine, MacroTrap™, to detect and remove both known and unknown macro viruses.

How Does InterScan VirusWall Work?

At its most basic, InterScan monitors all SMTP, HTTP, and FTP traffic between the LAN and Internet. Whenever it detects a file type that it has been configured to scan (for example, *.zip*, *.exe*, *.doc*), InterScan copies the file to a temporary location. If the file is clean, InterScan VirusWall deletes the copy and releases the original for delivery to the SMTP, FTP or HTTP server, which delivers the file as usual. If a virus is found, a notification is issued and InterScan takes the actions configured:

- **Clean** the infected file and send it to the original server for normal delivery
- **Delete** the infected file; it is not delivered
- **Quarantine** the infected file (without cleaning); the file is not delivered

- **Pass** the infected file (without cleaning); the infected file is delivered with an optional notification message

Whatever the action, a user-customized notification message can be issued to the intended recipient and any others specified. All virus-events and associated actions are noted in the log file.

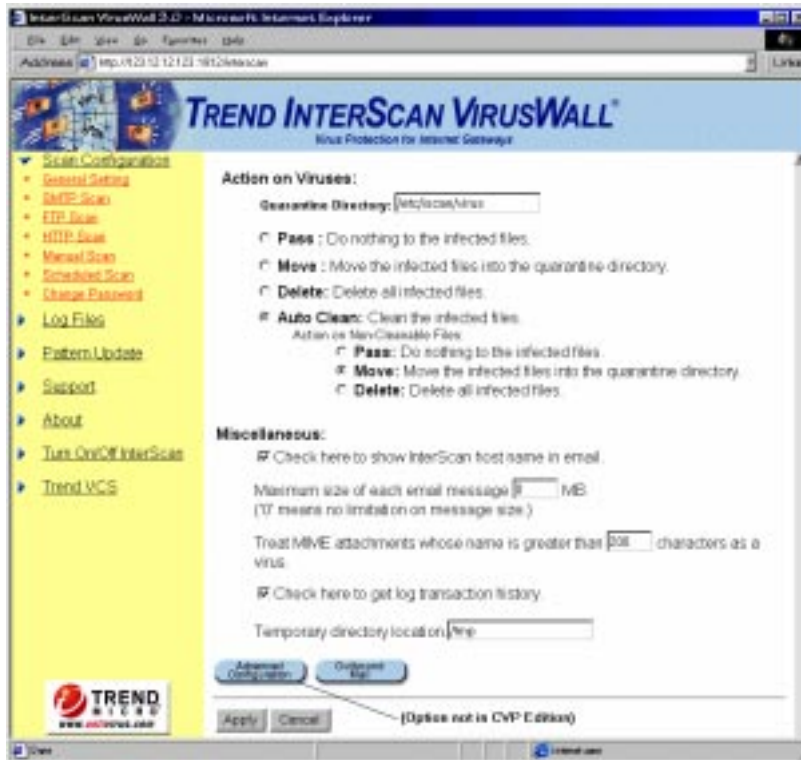


Figure 1-2. This example of the **SMTP Scan Configuration** page shows the Action on Viruses, and other options.

Notifications

Notifications are as follows: E-mail VirusWall inserts a warning message into the original message; Web VirusWall sends an HTML notification to the requesting browser, and FTP VirusWall issues an ASCII text alert to the requesting client.

Notifications are automatic and, in the case of E-mail VirusWall, can be issued to the system administrator, the sender, and the intended recipient. If no viruses are found, E-mail VirusWall can append a message stating that the e-mail was scanned and found to be virus-free.

How InterScan VirusWall Detects Viruses

Using a process called "pattern matching," InterScan draws upon an extensive database of virus patterns to identify known virus signatures. Key areas of suspect files are examined for tell-tale strings of virus code and compared against the tens of thousands of virus signatures that Trend has on record.

For polymorphic, or mutation viruses, the InterScan VirusWall scanning engine permits suspicious files to execute in a temporary environment. When the file is run, any encrypted virus code embedded within it is decrypted. InterScan then scans the entire file, including the freshly decrypted code, and identifies any strings of mutation virus, taking whatever action you have specified—clean, delete, move (quarantine), or pass.

Obviously, it is important to keep the virus pattern file up to date. By some estimates, more than a thousand new viruses are created each year—a rate of several each day. Trend makes it easy to update the virus pattern file by supporting automatic updates. See Chapter 9 for more information.

MacroTrap™

Macro viruses are among the most recent of virus types and quickly become the most prevalent. Macro viruses are unique in that they are not confined to any one operating system—they are application specific, and so can be spread between DOS, Windows, MACs, and even OS/2 systems. This is revolutionary.

Add the ability to travel by e-mail, the tremendous interconnections of the World Wide Web, and the increasing power of the Macro

languages, and you can begin to see that macro viruses are perhaps the biggest threat. To combat the advent of macro viruses, Trend's has developed MacroTrap, an intelligent technology that works in conjunction with the virus scan engine to bolster your ability to protect your LAN.

How MacroTrap Works:

The Macro Trap performs a rules-based examination of all Macro code that is saved in association with a document. Macro virus code is typically contained as a part of the invisible template (.DOT, for example, in Microsoft Word) that travels with the document. Trend's Macro Trap checks the template for signs of an unknown Macro viruses by seeking out instructions that perform virus-like activity—for example, copying parts of the template to other templates (replication), or code to execute harmful commands (destruction).

Compressed Files

InterScan recognizes over 20 types of compression and encoding formats, including PK-ZIP, LZEXE, PK-LITE, Microsoft Compress, and encoding formats such as UUencode and MIME.

Compressed files are opened and the contents examined according to the criteria specified in the Scan Files option of each VirusWall. When multiple layers of compression are encountered, InterScan recursively decompresses each, up to a limit of 20. In other words, if an archive contains *.cab* files that have been compressed using PK-ZIP, LZEXE, PK-LITE, and Microsoft Compress, InterScan will decompress each layer until no more compressed files are found (at which point the files contained within all the compression are scanned) or the limit of 20 has been reached.

What's New In Version 3?

Support for Sendmail's Antispam Filtering

To address the issue of rampant spam, InterScan contains an optional *Plugin* edition of the E-mail VirusWall that is specifically designed to support the antispam filtering capacity of Sendmail version 8.8.6 and later. You can use your own spam list, InterScan's, or combine the two.

Uniform Tagline or Disclaimer

E-mail VirusWall supports adding corporate slogans or a uniform disclaimer to all outbound mail, for example, "Visit <http://www.widgets.com> for a world of widget wonders." or "The views expressed in this e-mail are the sender's alone; there is no de facto endorsement by Widgets."

MIME Encoding

In addition to supporting 19 types of compression (up to 20 layers deep), E-mail VirusWall also decodes three compression types: UUencoding, MIME, BinHex (messages received in BinHex are recoded for delivery using UUencode).

Enhanced Logging

In addition to logging all virus events and virus pattern downloads, InterScan now provides the option to track all HTTP and FTP transactions.

Year 2000 Compliance

All components of InterScan VirusWall 3 are guaranteed to be year 2000 compliant. Please visit www.antivirus.com for details on what this guarantee entails.

Registering Trend VirusWall

Registering your copy of InterScan VirusWall is important and it entitles you to the following benefits:

- One year of free updates to the InterScan virus pattern file
- One year of free technical support
- Important product information

You can register over the Internet, by fax, or by mail. See Chapter 9 for details.

Trial Version

Trend provides a free 30-day trial version of all of our software products. This trial version is fully functional and can be installed without entering a serial number. After 30 days, however, the virus scanning services will no longer function.

Removing the 30-day Limit

If you decide to purchase InterScan, you do not need to completely reinstall the program. Instead, run setup again. Choose not to install any new packages, and enter the product serial number when prompted by the Setup script.

Serial Numbers

Your product serial number can be found:

- On the product registration card included with the software
- On the outside front cover of the Administrator's Guide

Otherwise, contact a Trend Sales representative at the following e-mail address:

sales@trendmicro.com

2 Installation Planning

Installing InterScan VirusWall takes about ten minutes and should be performed from the machine where the program(s) will reside. Allow another 10-15 minutes to configure InterScan to work with your existing servers.

You can access the InterScan console using web browser, either directly or via Trend VCS.

- *Standard* Edition—Each VirusWall can be installed onto the same machine (e.g., a dedicated server) or each can be installed onto a different machine (e.g., the server for which it will scan, or a dedicated server).
- *CVP* Edition—All three daemons must be installed onto the same machine. If you want to distribute the tasks among several CPUs, install InterScan on each machine, then control which protocols are scanned using the FireWall-1 rules base.
- *Plugin* Edition—This is a special version of E-mail VirusWall that is especially designed to complement spam filtering in Sendmail version 8.8.6 (or later). E-mail VirusWall must be installed onto the same machine as Sendmail.

Installing each VirusWall onto a dedicated machine is most common, and in this case you would run multiple iterations of Setup—once to install E-mail VirusWall, again to install Web VirusWall, and then a final time to install the FTP VirusWall.

Minimum System Requirements

Install InterScan on a system with at least the configuration indicated below. If you are installing the *CVP* or *Plugin* Edition, be sure to read the **Important Notes** below.

Solaris Version

- Solaris 2.5 or above *see note
- 128 MB RAM
- 256 MB swap space
- 15 MB disk space for program files

HP-UX Version

- HP-UX 10.10 or later *see note
- 128 MB RAM
- 256 MB swap space
- 15 MB disk space for program files

Important Notes

- E-mail VirusWall's Anti-Spam Control supports Sendmail version 8.8.6 and later
- Check Point Software's FireWall-1 version 3.0b build 3064 or later is required for the InterScan *CVP* Edition
- Systems supporting more than 1,000 e-mail accounts require at least a server-class machine.

Deciding Where To Install

You can install InterScan on the same machine as the original server or on a different one; there are no hard-and-fast rules to dictate which set up is most appropriate.

In deciding where to install, the most important issue is almost always whether or not there are sufficient resources on the target machine to adequately handle the additional load. *Before* installing InterScan, you should evaluate the peak and mean traffic loads handled by the server and compare the results to the overall capacity of that machine. The closer the two measurements are, the more likely it is that you will want to install InterScan on a dedicated machine. Additional factors to consider include network bandwidth, current CPU loads, CPU speed, total and available system memory, and the total amount of available swap space. Scanning one or more network for protocols for viruses, in real-time, can be resource intensive—do not install InterScan onto a machine that does not have the capacity to handle the additional load.

Another thing to consider, if you are planning to install InterScan on a dedicated machine, is the impact of your choice on overall network bandwidth—installing InterScan onto a dedicated machine, although less resource intensive, will consume more bandwidth than installing InterScan on the same machine as the server it is scanning for.

Setup Topology: Effects on InterScan Configuration

Same Machine. If you install InterScan on the same machine as the original server, you will most likely need to change the port used by original server and give InterScan the default (e.g., 21, 25, or 80).

- If your server does not support changing the port, you can have InterScan use a different port but be sure to modify the clients accordingly

Dedicated Machine. If InterScan is installed on different machine than the server it will scan for, you do not need to change the port of the original server. You may, however, need to modify the clients to

reflect the new IP address (or hostname) of the InterScan machine. If you would prefer not to change the clients,

- Consider swapping IP addresses (or hostnames) between the two machines so InterScan can use the original.
- Consider installing InterScan so that it is logically between the Internet and the SMTP server or HTTP proxy
- Consider modifying your MX record (for E-mail VirusWall) as explained below.

SMTP option: modify the MX record...

If E-mail VirusWall is installed on a different machine than the SMTP server, you may be able to avoid modifying all the clients by modifying the MX record in the DNS configuration instead. The idea is to edit the MX record so that it directs all incoming e-mail to the E-mail VirusWall machine.

1. Change the MX record in the DNS configuration.
2. In the InterScan configuration, enter the host name or IP address of the original SMTP server in the Original server location field.

Installation Topologies

InterScan VirusWall supports installation onto most network topologies. Where (logically) you install InterScan will directly affect how it should be configured to work on your system.

In the pages that follow, several possible installation topologies are presented. Use the one that best fits your needs, or apply the principles to an installation strategy of your own design.

E-Mail VirusWall

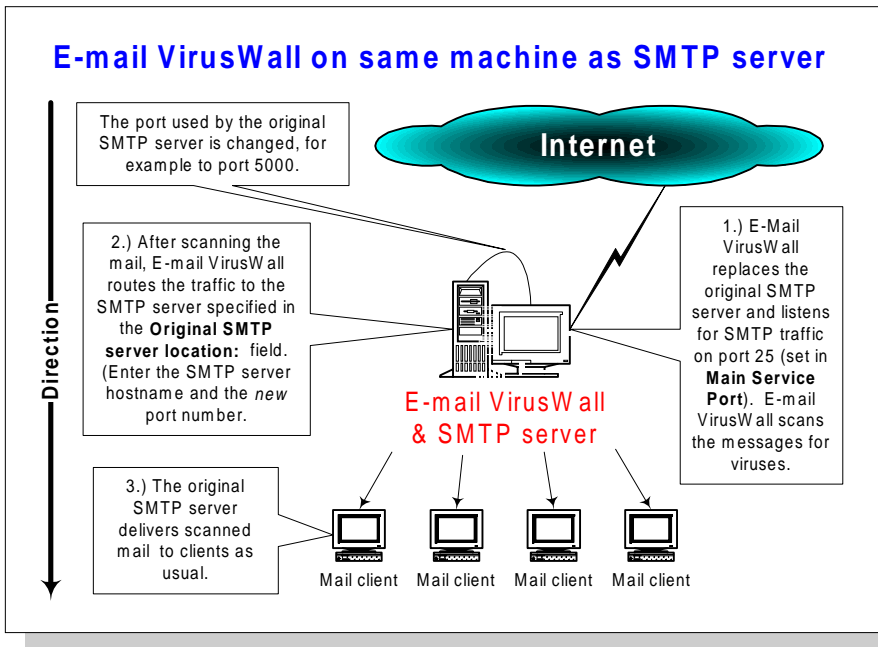
E-mail VirusWall checks both inbound and outbound SMTP traffic for viruses. It can be installed on the same machine as your existing SMTP server or on a dedicated machine.

Note: If you are installing the *Plugin* Edition of E-mail VirusWall, it must be installed on the *same machine* as your Sendmail—not on a dedicated machine or another SMTP server.

As a rule of thumb, install E-Mail VirusWall inside a firewall and, logically, on the client side of your existing SMTP server. The idea is to have E-mail VirusWall listen on port 25 for new connections, scan the SMTP traffic it receives, and then route scanned traffic to your original SMTP server for delivery as usual to the mail clients.

- If the SMTP server is on another machine, you need to specify the hostname (or IP address) and port for InterScan
- If the SMTP server is on the same machine, you will need to change the port it uses to listen for incoming SMTP connections, and specify this port and hostname for InterScan
- If the SMTP server is Sendmail and on the same machine as InterScan, you need to identify the Sendmail path and add a **-bs** flag—in this case, no port is necessary
- If you installed the *Plugin* Edition, you need to identify the Sendmail path *but no -bs should be specified*.

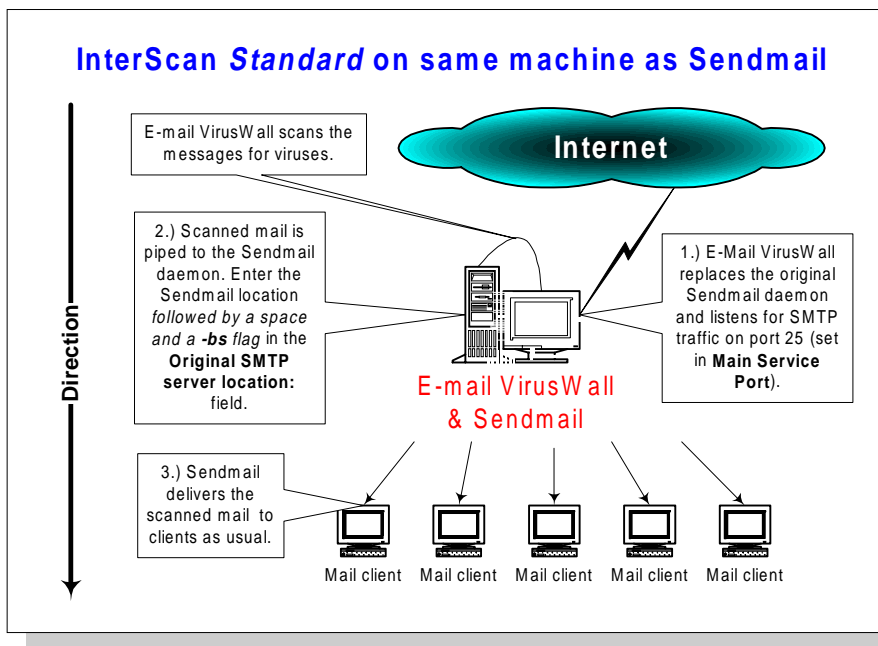
E-mail VirusWall Example 1.



E-mail VirusWall listens on port 25 for SMTP connections, scans the traffic, then forwards it to the SMTP server on the same machine (*localhost*) using the new port (5000). The SMTP server handles the actual delivery of the mail.

1. Install E-mail VirusWall on the SMTP server.
2. Stop the SMTP server and change its port from 25 to another, for example 5000.
3. Open the InterScan configuration console (<http://hostname:1812/interscan>) and the SMTP scan configuration page (**Scan Configuration | SMTP Scan**).
4. Assign E-mail VirusWall port 25 for the **Main Service Port**.
5. Enter *localhost port* in the **Original SMTP server location:** field. For example, *localhost 5000*.

E-mail VirusWall Example 2.

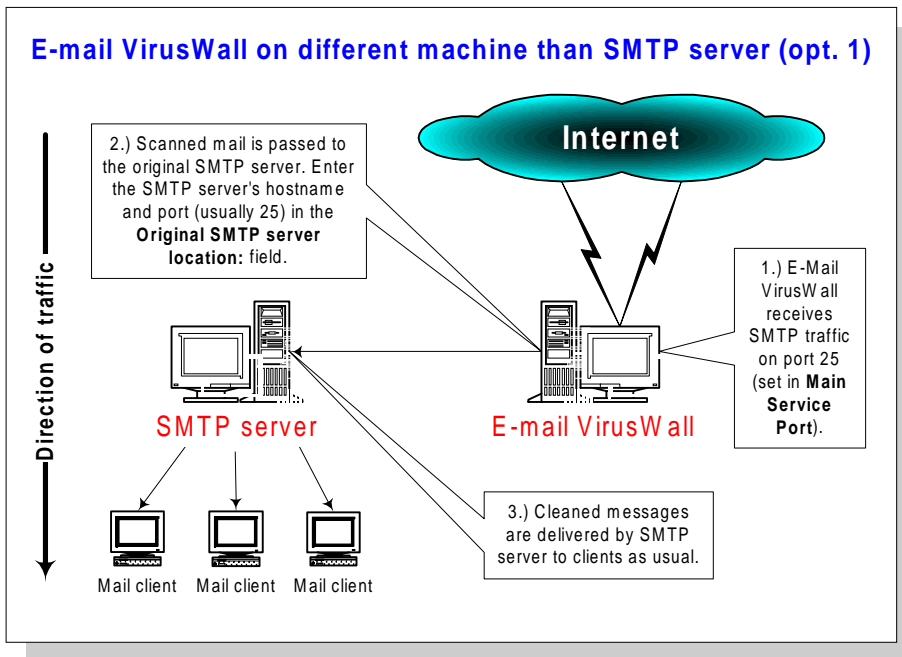


E-mail VirusWall listens on port 25 for SMTP connections, scans the traffic, and forwards it to the Sendmail daemon on the same machine. Scanned traffic is *piped* from E-mail VirusWall to the Sendmail; no port need be specified. Sendmail handles the actual message delivery.

1. Install E-mail VirusWall on the Sendmail server.
2. Open the InterScan configuration console (<http://hostname:1812/interscan>) and the SMTP scan configuration page (**Scan Configuration | SMTP Scan**).
3. Assign E-mail VirusWall port 25 for the **Main Service Port**.
4. Enter the Sendmail path in the **Original SMTP server location:** field, for example, `/usr/lib/sendmail -bs`

Note: If you are installing the *Plugin* Edition of E-mail VirusWall, (for antispamming) *do not include the -bs flag*.

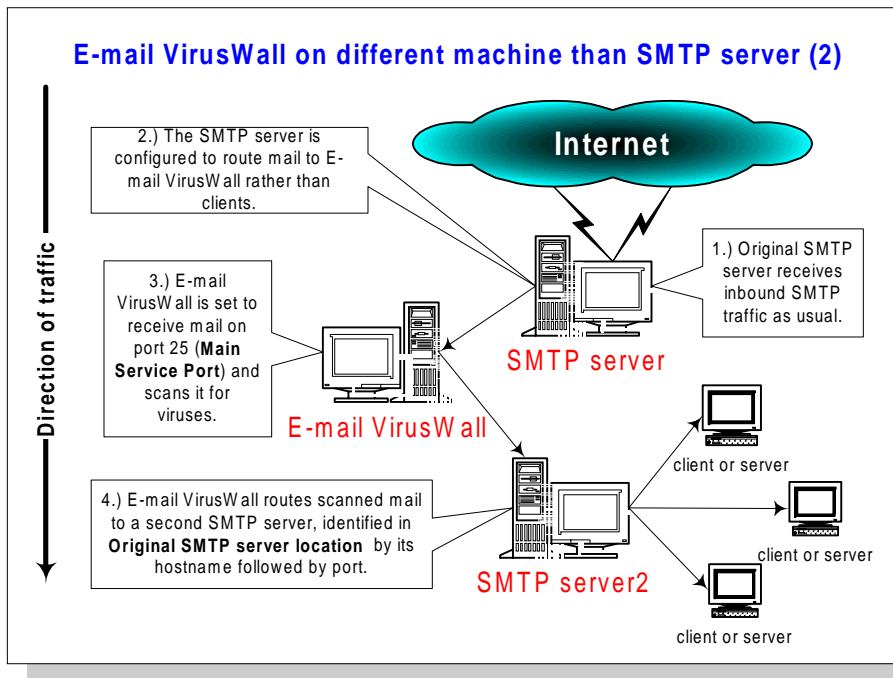
E-mail VirusWall Example 3.



E-mail VirusWall listens on port 25 for SMTP connections, scans the traffic, then forwards it to the remote SMTP server. Because the SMTP server and E-Mail VirusWall are on different machines, both can use port 25. The SMTP server handles the actual mail delivery.

1. Install E-mail VirusWall on the dedicated server.
2. Open the InterScan configuration console (<http://hostname:1812/interscan>) and the SMTP scan configuration page (**Scan Configuration | SMTP Scan**).
3. Assign E-mail VirusWall port 25 for the **Main Service Port**.
4. Enter the hostname (or IP address) *and* port of the SMTP server in the **Original SMTP server location:** field. For example, *mailserver.company.com 25*.

E-mail VirusWall Example 4.



The original SMTP server continues to receive incoming SMTP connections, but then forwards the traffic to E-mail VirusWall for scanning. Scanned traffic is relayed to a second SMTP server for delivery to clients. All three servers can use port 25.

1. Install E-mail VirusWall on the dedicated server.
2. Open the InterScan configuration console (<http://hostname:1812/interscan>) and the SMTP scan configuration page (**Scan Configuration | SMTP Scan**).
3. Assign E-mail VirusWall port 25 for the **Main Service Port**.
4. Modify your SMTP server so it routes traffic to E-mail VirusWall rather than to clients
5. Enter the hostname (or IP address) *and port* of the second SMTP server in the **Original SMTP server location:** field.

Web VirusWall

Web VirusWall checks all HTTP file transfers for viruses, malicious Java applets, and malicious ActiveX controls. It can be installed on the same machine as an existing HTTP proxy server, on a dedicated machine (in conjunction with an existing proxy) or as the sole HTTP proxy on the network.

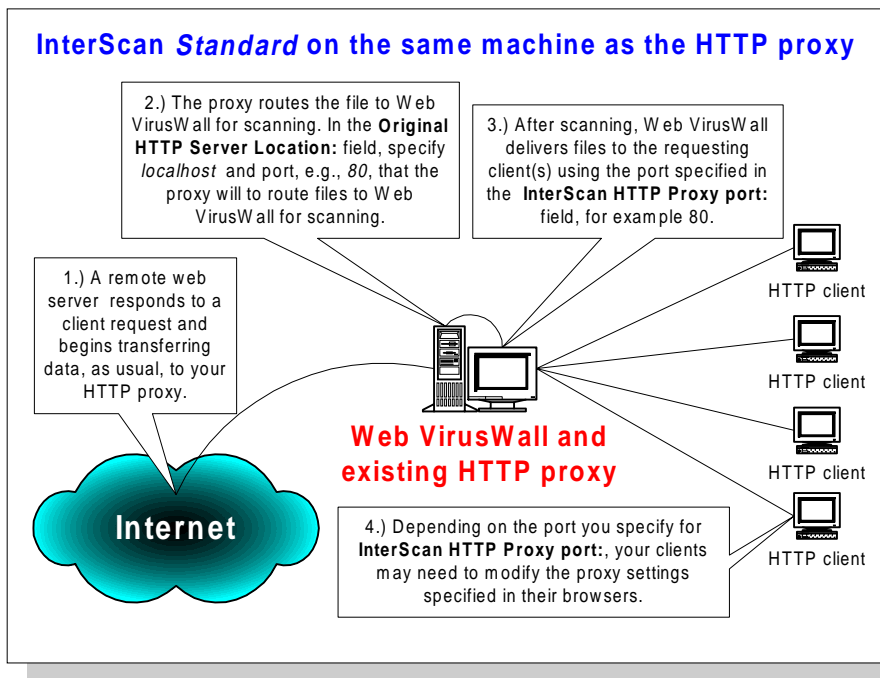
Note: If you install Web VirusWall as the sole proxy, please be aware that it does not provide any of the traditional benefits usually associated with a full proxy server, for example file caching or security checking).

In general, we recommend that you install Web VirusWall inside the firewall and (logically) between the Internet and the HTTP proxy. The idea is to have Web VirusWall listen on a port (typically 80) for requests from the HTTP proxy, relay the requests the Internet, and then scan the HTTP traffic it receives in response before passing it on to the proxy (and ultimately the requesting client).

The primary reason to choose one topology over another, however, is system resources. Both Web VirusWall and an HTTP proxy server can be CPU and I/O intensive, so you should run them both on the same machine if that machine can handle the additional load. On the other hand, installing Web VirusWall on a separate machine is only preferable if the network connection between the machines is fast, reliable, and the impact on overall bandwidth will not be an issue.

Aside from the question of system resources, other considerations are presented following each topology illustration.

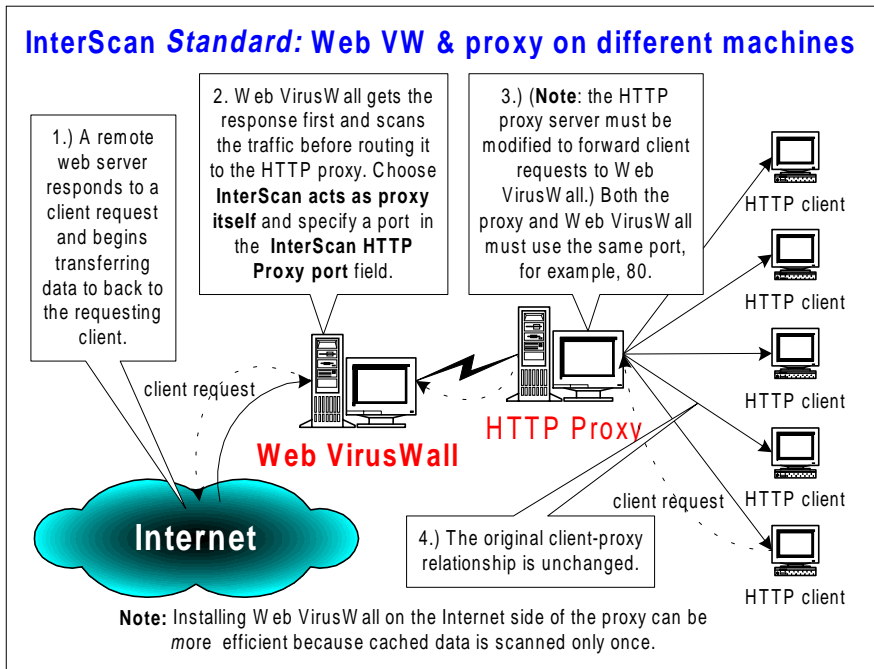
Web VirusWall Example 1.



Considerations:

- Flexible: can be configured so that Web VirusWall is logically between the Internet and the proxy (preferred) or between the clients and the proxy
- Creates no additional network traffic
- Can be CPU and disk intensive. Requires a high-end server.
- Requires that you either modify the HTTP proxy server so that it uses a port other than 80, or modify the clients so they (and Web VirusWall) use a port other than 80
- No proxy "time-out" issues
- Clients experience no lag between clicking a file for download and receiving the "Save as" dialog box

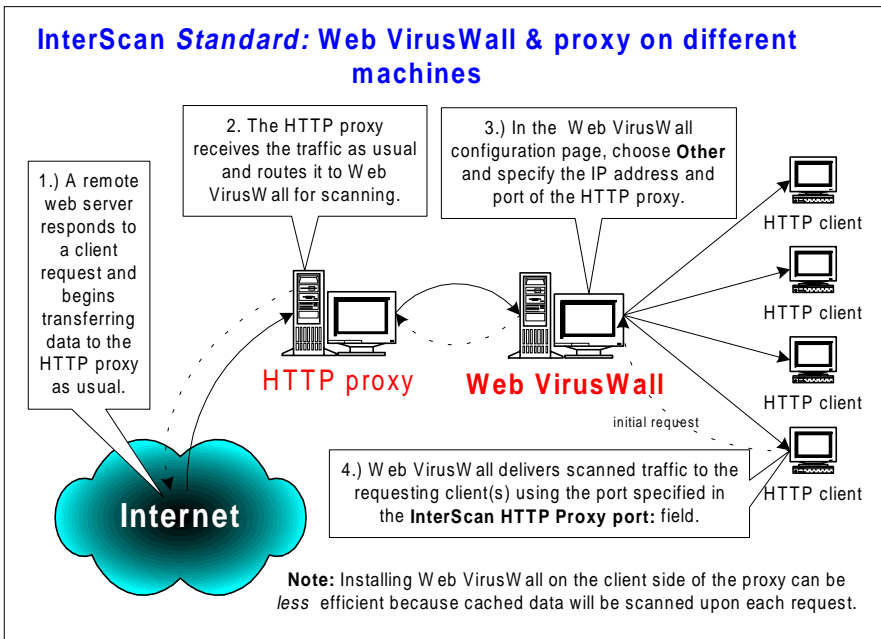
Web VirusWall Example 2.



Considerations:

- Efficient configuration, cached files are only scanned once
- No need to change the clients' proxy settings
- Clients may experience a lag between clicking a file for download and receiving the "Save as" dialog box
- Accommodates servers with tightly limited resources
- If the Internet to Web VirusWall connection is slow, the HTTP proxy server may send a "time-out" to the client browsers. In this case, set a "trickle" value in the HTTP Scan Configuration
- Must modify the proxy server so it forwards client requests to Web VirusWall

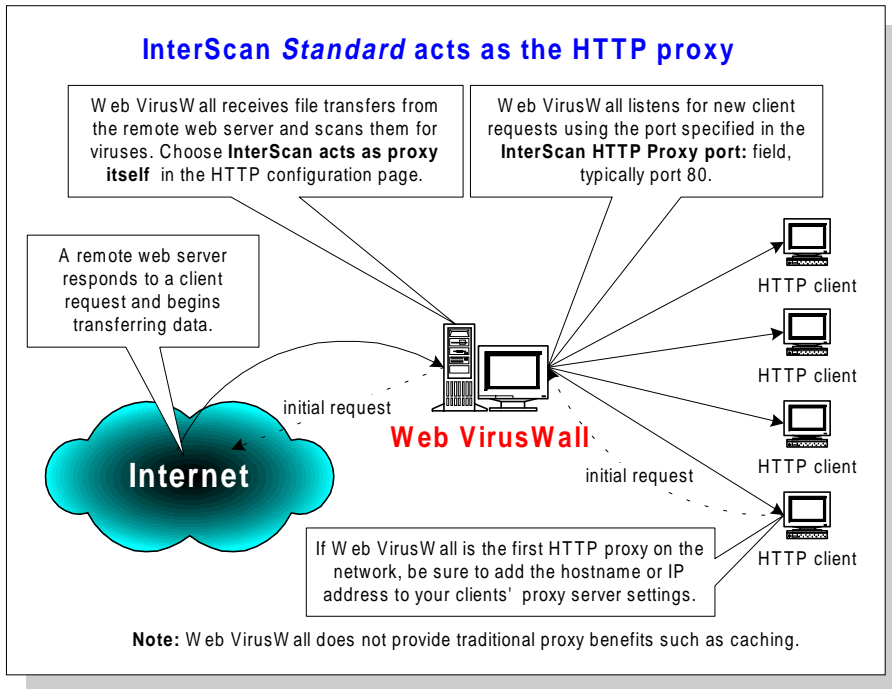
Web VirusWall Example 3.



Considerations:

- Accommodates servers with tightly limited resources
- Clients experience no lag between clicking a file for download and receiving the "Save as" dialog box
- No proxy "time-out" issues while Web VirusWall scans a file
- No need to reconfigure http proxy server
- May need to reconfigure clients to use Web VirusWall as the proxy

Web VirusWall Example 4.



Considerations:

- Requires no existing proxy server, but provides no caching or special security
- Creates no additional network traffic
- Can be CPU and disk intensive. Requires a high-end server.
- No proxy "time-out" issues
- Clients may experience a lag between clicking a file for a download and receiving the "Save as" dialog box
- Requires that you modify the clients so they point to Web VirusWall as the proxy server

FTP VirusWall

There are two ways to use FTP VirusWall: 1.) FTP VirusWall acts as a *proxy* between the requesting client and the remote site, brokering all transactions, and 2.) 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, and malicious ActiveX controls.

FTP VirusWall can be installed on the same machine as an existing FTP server, on a dedicated machine, or as the sole FTP proxy.

FireWalls

FTP VirusWall is able to work with most firewalls, usually requiring only that the firewall be modified to recognize the viruswall. A special FTP setting for use with some firewalls, called *passive mode* can be set by directly editing `intscan.ini`.

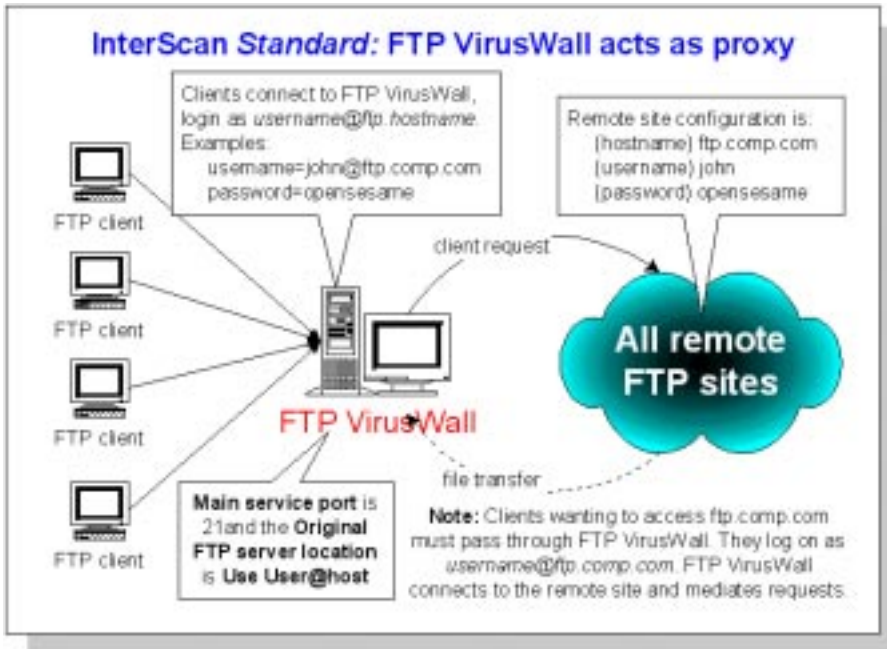
FTP VirusWall as a proxy

If you want to scan all FTP traffic in and out of the LAN, you can set up FTP VirusWall so that it "brokers" all such connections. In this case users no longer FTP directly to their target site; instead, they always FTP to FTP VirusWall, supply the logon credentials to the target site, and then let FTP VirusWall make the connection on their behalf. The remote site transfers the files to FTP VirusWall, which checks it for viruses and then delivers it to the requesting clients. (To ensure that clients no longer make the direct connection, we suggest you restrict access to port 21 to all IPs other than FTP VirusWall's.)

FTP VirusWall as a sentry

If you want to scan all FTP traffic in out of a particular FTP server (typically one that you host), you can install FTP VirusWall onto that FTP server, or on a dedicated machine between it and the requesting clients. In this case, it appears to users that they are connecting directly to the target server when in fact they are connecting to FTP VirusWall, which then relays the request to the specified server.

FTP VirusWall Example 1.



How it works

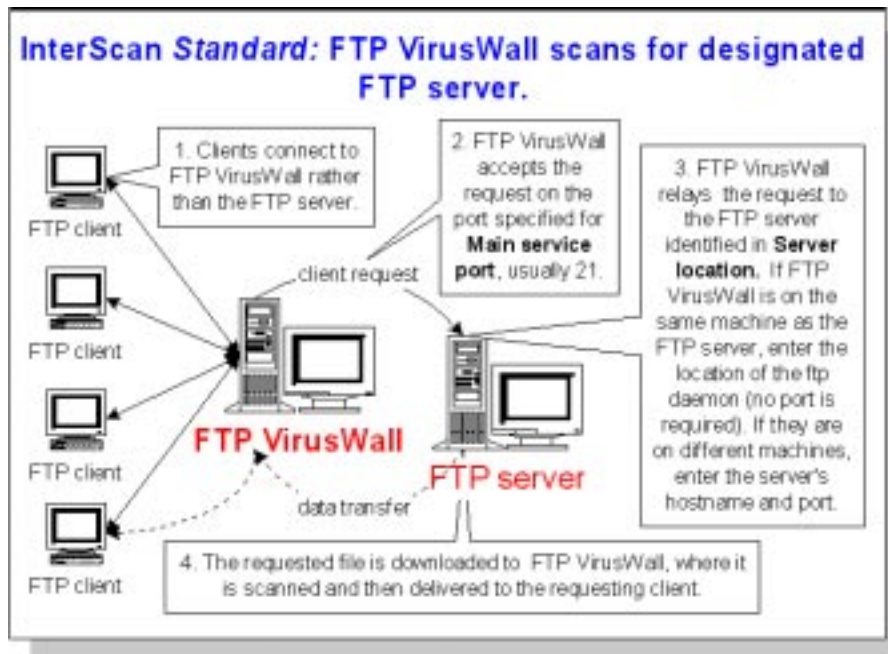
Clients no longer FTP directly to the remote FTP server, and instead always FTP to the same IP address—that of FTP VirusWall. The VirusWall prompts the client for the login credentials, and the user provides them in the following format:

`username@domainname.com`

where `domainname.com` is the address of the remote FTP server. The FTP VirusWall itself requires no independent login credentials. In comparison, without FTP VirusWall, users log on the remote FTP site directly, supplying only a username and password.

Note: FTP VirusWall is not a firewall and it will not prevent users from connecting directly to remote sites. To keep users from "going around" the VirusWall, configure your existing firewall or router.

FTP VirusWall Example 2.



How it works

Clients connect to FTP VirusWall rather than directly to the protected FTP server. If the two are installed on different machines, you may want to make FTP VirusWall transparent by swapping domain names between the machines or reassigning the IP addresses. When the log on, clients are prompted for a username and password, as usual.

You can install FTP VirusWall onto the same machine as the FTP server or on a dedicated machine. Whichever you choose, be sure to correctly identify the server in **Server Location** field.

Note that for this configuration, you must install one instance of InterScan for each FTP server it will protect. Unless you've reassigned IP addresses or swapped domains, users will still be able to FTP directly to the server unless measures are taken (outside of InterScan) to restrict the connections. Both FTP uploads and downloads will be scanned.

3 Installing the *Standard* or *Plugin* Edition

InterScan VirusWall supports any number of physical network setups, including installing each VirusWall onto the same machine as the server it will scan for, installing all three VirusWalls onto a single, dedicated machine, or installing each VirusWall onto its own dedicated machine.

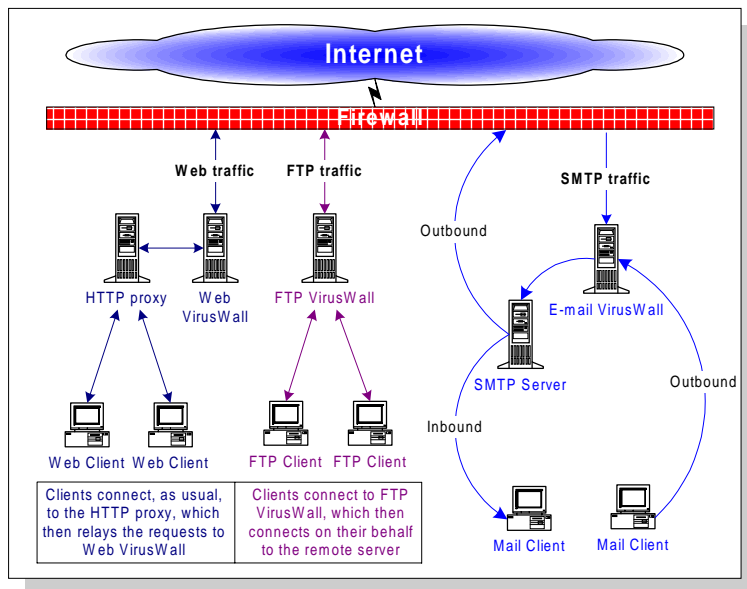


Figure 3-1. This illustration shows how the *Standard* edition of Web, FTP, and E-mail VirusWall might be installed on a LAN. See Chapter 2, Installation Planning, for detailed examples.

Chapter Overview

In this chapter you will find step by step instructions for installing both the *Standard* and *Plugin* Editions of VirusWall. Also presented are instructions for

- Setting up the *Plugin* Edition
- Opening the InterScan console
- Starting the individual services manually
- Using a special test virus to check your setup
- Troubleshooting installation problems
- Uninstalling Trend InterScan VirusWall

Depending on your network topology and the services to be installed, you may need to run multiple iterations of the Setup described below.

E-mail VirusWall

E-mail VirusWall comes in two "flavors," *Standard*, and *Plugin*. The option to install the *Plugin* appears as a choice in the *Standard* Setup.

Choose the *Standard* Edition:

- If you want to install E-mail VirusWall on a machine other than your SMTP server
- If you don't use Sendmail as your mail server
- If you do not use Sendmail for spam filtering

Choose the *Plugin* Edition:

- If you are running Sendmail version 8.8.6 or later and are already using its antispam filtering capabilities

Note: After installing the *Plugin* Edition of E-mail VirusWall, you must remove the **-bs** flag following the

`/usr/lib/sendmail` line in InterScan E-mail VirusWall's
Original SMTP server location configuration field.

Important: While installing the *Plugin* Edition, Setup will make a copy of your `sendmail.cf` file, called `sendmail.cf.org`. DO NOT DELETE this file!

Installing InterScan *Standard* Edition

The InterScan setup includes scripts requiring super-user permission—log on as **root** before installing InterScan.

1. From the directory containing the InterScan installation files, type `./isinst` and press ENTER.
2. You are prompted to select which "flavor" of InterScan you want to install, the *Standard* or *CVP* Edition.
 - Choose **InterScan VirusWall for FTP, SMTP, HTTP** to install the *Standard* Edition of InterScan
 - Choose **InterScan VirusWall for CVP** if you will be installing onto a FireWall-1 network and you want InterScan to act as a CVP server. Also, switch now to Chapter 4 of this manual for special installation instructions.
3. The **Main Menu** appears, displaying the current system configuration.
 - A status of **None** means the package is not installed. This is the typical value for first time installations.
 - A status of **Installed** means the package exists on the server. Before installing version 3, be sure to uninstall any previous version.

Choose **Option 1** to begin installing InterScan.

4. By default, InterScan will install all available systems to sub-directories of /opt/trend (with the exception of the **Trend Virus Control Agent**, explained later in this chapter).

InterScan VirusWall 3.0

Setup Script

```
Install InterScan Base System-----[ YES ]
Installation Path           /opt/trend/ISBASE
```

```
Install InterScan CGI Admin -----[ YES ]
Installation Path           /opt/trend/ISADMIN
```

```
Install InterScan for FTP -----[ YES ]
Installation Path           /opt/trend/ISFTP
```

```
Install InterScan for HTTP -----[ YES ]
Installation Path           /opt/trend/ISHTTP
```

```
Install InterScan for SMTP -----[ YES ]
Installation Path           /opt/trend/ISSMTP
```

```
Install TVCS Agent for InterScan -----[ NO ]
Installation Path           /opt/trend/ISTVCS
```

1. Modify option for BASE.
2. Modify option for ADMIN.
3. Modify option for FTP.
4. Modify option for HTTP.
5. Modify option for SMTP.
6. Modify option for TVCS.
7. Start installation.
8. Back to Main Menu.

Select a number [5]

To modify the Install status or path of a system,

- a. Specify the option you want to change and press **Enter**.
1=**Base** (required), 2=**CGI Admin** interface (required),
3-5 are the **VirusWalls**, and 6=**Trend VCS Agent**.

- b. Enter **y** to install the system or change the Install path, **n** to remove it from the list.
- c. Specify the new path or press **Enter** to accept the default, for example, `/opt/trend/ISBASE`.

Installing selected VirusWalls

- 5. You can select individual VirusWalls (protocols) to install.
Choose **option 7, Start Installation** in the Setup Script menu to start the installation.
 - a. Enter **y** and press **Enter** as prompted to install the BASE system and CGI Admin (interface).
The BASE and CGI Admin are required for each machine that you will install a VirusWall on.

Installing the 30-day trial version

- 6. Once the InterScan Base and Admin systems are installed you are prompted to enter a serial number.
Press **Enter** without entering a serial number to install the 30-day trial version. This version of InterScan is fully functional but will expire after 30 days, at which time it should be upgraded or removed.
- 7. To install Web and FTP VirusWall, press **y** and **Enter** as prompted.
To install only one VirusWall, for example if you will install each VirusWall to a different machine, enter **n** when prompted to install the additional VirusWall(s).

Installing E-mail VirusWall

- 8. There are two "flavors" of E-mail VirusWall, the *Standard* Edition, which replaces your existing sendmail, and the

Plugin Edition, which complements an existing Sendmail 8.8.6 or later.

Note: Only choose to install the *Plugin* Edition if you already have Sendmail 8.8.6 installed on the machine and are currently using its anti-spam capabilities.

InterScan VirusWall SMTP

- a. To install the standard version of E-mail VirusWall, choose that option and type in **y** and press **Enter** as prompted by the install script.
- b. You will be prompted for your company's domain name, for example, `trendmicro.com`. This is optional.
- c. Follow the screen prompts to complete the installation. Be sure to see **Configuring InterScan Standard**, in this chapter, after installing.

E-mail VirusWall *Plugin* Edition

- a. To install the *Plugin* Edition of E-mail VirusWall, (must be on the same machine as your Sendmail with antispam functionality), choose the **Plugin** option and type in the path of your original `sendmail.cf` file when prompted. InterScan will make a backup copy of your original `sendmail.cf` (called `/etc/iscan/sendmail.cf.org`) and create a modified version (`/etc/iscan/sendmail.cf.is`).

Note: If Setup cannot modify `sendmail.cf`, you will need to edit the file yourself. See page 3-7 for details.

- b. Follow the screen prompts to complete **Setup** and then **Exit**.

- c. See **After Installing the *Plugin* Edition** in this chapter for instructions on confirming InterScan's proposed changes to your `sendmail.cf` file.
- d. With your installation complete and `sendmail.cf` properly configured, the last thing to do is open the InterScan console and customize your E-mail VirusWall settings. See Chapter 5 for details.

After Installing the *Plugin* Edition...

To enable the Plugin Edition of E-mail VirusWall, you must do the following three things:

1. Replace your original "sendmail.cf" with the InterScan version.

Confirm InterScan's proposed changes by opening the file `/etc/iscan/sendmail.cf.is`. If the file meets your approval, copy it to: `/<original sendmail path>/sendmail.cf`. A backup of the original `sendmail.cf` file can be found in `/etc/iscan/sendmail.cf.org`

2. Edit your InterScan configuration so the **Original SMTP server location** points to the actual path of your Sendmail daemon, *and remove* the "-bs" flag (detailed on the next page).
 - a. For example, open a web browser and enter the InterScan URL:

`http://ip-address:port/InterScan`

Click **Configuration**, then **E-mail** to change the **Original SMTP server location** parameter.

3. Finally, restart your Sendmail daemon, for example:

```
% /etc/rc2.d/S88Sendmail stop
% /etc/rc2.d/S88Sendmail start
```


Editing Sendmail.cf.is Manually

If InterScan can't create `/etc/iscan/sendmail.cf.is`, for example because the mailer used cannot be recognized, you will need to modify the file yourself. There are two basic tasks involved:

1. Locate the path of your local mailer and replace it with the location of InterScan.
2. Locate the path of any remote mailers, relays, etc. that you want InterScan E-mail VirusWall to scan for and replace it with the InterScan location (`/etc/iscan/sendmail.cf.is`).

To modify your "sendmail.cf" file,

1. Use `vi` editor or another program to open `sendmail.cf`.
2. Use `vi`'s search function to locate the *Mlocal* or *Mlocalmail* line (or whatever the case may be) and make the following replacements:

Replace `"P=/bin/mail,"` or `"[IPC],"` with `"P=/etc/iscan/isfilter,"`

Replace `"A=mail -d $u"` with `"A=isfilter -f $g $u"`

where `"P=/bin/mail,"` represents the actual path of your mailer (e.g., `"/usr/lib/mail,"`) and `"A=mail -d $u"` represents your **Argument** vector list.

3. Next, use `vi`'s search function to locate the *Msmtp* or *Mether* line (or whatever the case may be) and make the following replacements:

Replace `"P=[IPC],"` (or `"P=[TCP]"`) with `"P=/etc/iscan/isfilter"`

Replace `"A=IPC $h"` (or `"A=TCP $h"`) with `"A=isfilter -f $g $u"`

Notes:

- If you have multiple remote servers that you want InterScan to check, for example an Esmtp server, repeat steps 1 & 2 above for each instance.
- If you use any mail relays that you want InterScan to check, repeat steps 1 & 2 for each instance.
- The main thing to remember here is that you want to replace the existing mailer path and configuration lines with

```
"P=/etc/iscan/isfilter," <InterScan path>
and
"A=isfilter -f $g $u"
```

Note: We recommend that you preserve the original configuration lines by commenting them out, copying them, and then editing the copied line.

Installed Files

InterScan makes the following changes to your system:

<i>Platform</i>	<i>Directory</i>	<i>Action</i>	<i>Files/Modification</i>
Solaris & HP	/opt/trend (user config.)	create dir	all files located within
Solaris & HP	/etc/iscan	create dir	all files located within
Solaris & HP	/etc/inetd.conf	modify file	## comment out original FTP server
Solaris	/etc/rc2.d	modify and create	add InterScan to S88sendmail; create S99ISproxy; S99ISftp; S99IScanHttpd
HP	/sbin/rc2.d	modify and create	add InterScan to the S540sendmail; create S991IScanFTP; S992IScanHTTP; S999IScanHttpd

Opening the InterScan Console

After installation, InterScan automatically stops and restarts your Sendmail and/or other daemons. Although InterScan is configured to run on a robust set of default values, you should at least open the InterScan console and confirm the settings.

1. Open a web browser, then enter the InterScan URL followed by the port (:1812). For example,

`http://domain:port/interscan`

The IP address can be either the domain name or number of the InterScan machine. The port is 1812.

`http://isvw.widget.com:1812/interscan`

`http://123.12.123.123:1812/interscan`

2. The InterScan configuration is password protected. By default, both the user name and password are **admin**



Figure 3-2. An example InterScan console screen, in this case, for **About**, which shows which versions are installed.

Starting and Stopping InterScan

By default, all InterScan services are enabled upon installation. Each VirusWall can also be individually controlled, however, according to the following options:

- Enable/disable real-time scanning for a given VirusWall
- Turn on/turn off the network flow of a given protocol

To enable/disable real-time scanning,

1. From InterScan, click **Configuration | General Settings**.
2. Click any of the **Real-Time Scan** settings to toggle on/off scanning for that service. The flow of traffic is not affected.

To turn on/turn off InterScan,

1. In the InterScan console, click **Configuration | Turn On/Off InterScan**.
2. Click any of the VirusWall options to stop the flow of all network traffic for the given protocol.

Starting and Stopping InterScan via Command Line

You can also stop and restart the daemons from a command line:

E-mail VirusWall

```
% /etc/rc2.d/S88Sendmail stop  
% /etc/rc2.d/S88Sendmail start
```

Web VirusWall

```
% /etc/rc2.d/S88Sendmail stop  
% /etc/rc2.d/S88Sendmail start
```

FTP VirusWall

```
% /etc/rc2.d/S88Sendmail stop  
% /etc/rc2.d/S88Sendmail start
```

Changing the InterScan Password

1. In the InterScan console, click **Configuration | Change Password**.
2. Enter your current password in the **Old Password** field, then enter and confirm the new password you want to use.
3. Click **Apply** to save your new password or **Cancel** to revert to the old one.



Figure 3-3. The default username and password are "admin".

Testing InterScan

Once Trend VirusWall has been installed, we recommend that you test it to get familiar with the configuration and see how it works.

The European Institute of Computer Antivirus Research, along with antivirus vendors, has developed a test file that can be used for checking your installation and configuration.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is a specially created file whose signature has been included in the Trend Micro virus pattern file. You can download the file from Trend at:

<http://www.antivirus.com/vinfo/testfiles/index.htm>

Once on your machine, you can use the test virus in e-mail to test SMTP scanning, and also to check FTP and HTTP file transfers.

Troubleshooting a *Standard* Setup

When troubleshooting InterScan, edit the `intscan.ini` so the verbose parameter equals on, like this: `verbose=on`. Check your InterScan logs for details.

Mail is not being delivered. Error Message

If you receive the following error when running E-mail VirusWall, "exec error, no such file or directory", check your **Original SMTP server location** settings. No **-bs** flag should appear.

With the InterScan configuration open in a web browser,

1. Click **Configuration**, then **E-mail Configuration**.
2. In the **E-Mail Scan Configuration** page, check the value specified for **Original SMTP server location**.

No flag (i.e., **-bs**) should appear at the end of the path, for example: `/usr/lib/sendmail`

Can't Find Quarantined Files

If InterScan does not have sufficient permissions to write to the designated quarantine directory, and InterScan's **Action On Virus** is set to **Quarantine**, infected files will be written to the `/var/tmp` directory.

E-mail Is Not Being Delivered

InterScan uses the original `sendmail.cf.org` file during uninstall as well as for the daily delivery of e-mail messages.

Do not delete the file `sendmail.cf.org`! `Sendmail.cf.org` is located in the `/etc/iscan` directory.

Uninstalling InterScan

InterScan's uninstall scripts require super-user privileges. You must be logged on as **root** to Uninstall InterScan.

1. To remove one or all the InterScan VirusWalls, bring up the **Main Menu** by entering `./isinst` in the directory where your InterScan files are located.
2. Choose **Option 2**, and follow the on-screen prompts to complete installation.

Note: If you are changing from one InterScan Edition to another (*CVP* to *Standard* or vice versa), you must uninstall any existing VirusWalls. The Base System and CGI Admin can remain.

Uninstalling InterScan *Plugin* Edition

Uninstall E-mail VirusWall *Plugin* Edition using the uninstall script mentioned above. Your original `sendmail.cf` file, saved as `sendmail.cf.org`, will be restored to `/etc/sendmail.cf` regardless of its original location. Be sure to copy it the appropriate directory, if necessary.

4 Installing InterScan *CVP* Edition

In this chapter you will find step by step instructions for installing InterScan VirusWall *CVP* Edition. Also included are instructions for

- Adding InterScan to your FireWall-1 rule base and setting up the optional OPSEC authentication
- Opening the InterScan console
- Starting and stopping the VirusWalls
- Using a special test virus to check your setup
- Troubleshooting installation problems
- Uninstalling Trend InterScan VirusWall

Installation Overview

In the *CVP* Edition, InterScan acts as a *CVP* server to your FireWall-1 (v. 3.0b build 3064 or later) machine and provides real-time virus scanning for SMTP, HTTP, and FTP file transfers.

It works by receiving inbound and/or outbound network traffic from the FireWall-1 server, scanning it, and then routing it back to the FireWall-1 machine for delivery as usual. All three VirusWalls are installed as a single daemon, and you can toggle on/off scanning for any of the individual VirusWalls.

When deciding where to install InterScan, consider first whether you want it inside the DMZ or inside the internal network. Next, consider your network traffic load and available resources. If you will be installing onto an existing server that is already running programs, consider available CPU, memory, and disk space. If network traffic is light, you may, for example, want to install InterScan onto the server it will scan for. If network traffic is heavy, consider using one or more dedicated servers.

Choosing the best place to install depends on your network's traffic available resources. Installing on the FireWall-1 server, for example, can be faster but is resource intensive. InterScan can also be installed on a single server (B1 in the illustration below) or each VirusWall onto a different server (B2 in the illustration below).

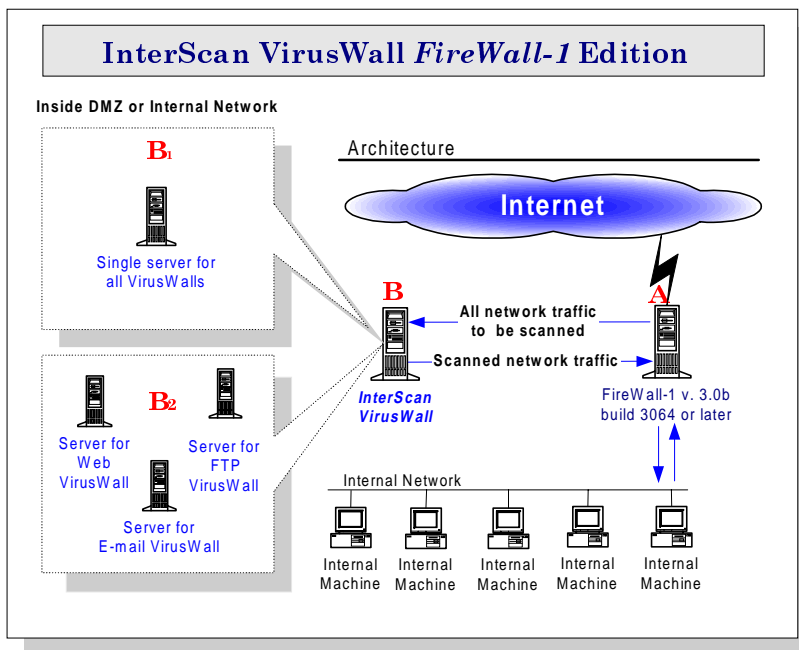


Figure 4-1. InterScan must receive network traffic from FireWall-1. Possible installation points for InterScan VirusWall are indicated by the letters A (the FireWall-1 machine) and B (another server).

- **Point A.** Installing InterScan VirusWall onto the same server as FireWall-1 is preferable for light network loads. It can be faster than transferring all traffic back and forth to the FireWall-1 machine, but expect that running InterScan in addition to FireWall-1 will place a high demand on resources.
- **Point B1.** Installing InterScan VirusWall onto a single, dedicated Solaris server (located in the DMZ or internal network) is recommended for systems with moderate to light traffic loads.
- **Point B2.** Installing InterScan VirusWall onto one or more existing server running other software is another possibility for networks with moderate network traffic loads. Of course, a lot will depend on how resource intensive the other programs are.
- **Point B2-2.** Installing InterScan VirusWall onto multiple dedicated servers (once for each protocol scanned, for example) is only suggested for heavy network traffic loads.

Note: You can use the *Trend Virus Control System* (Trend VCS) to consolidate InterScan configuration tasks among the three machines.

Installing the *CVP* Edition

To install InterScan VirusWall *CVP* Edition, you must be logged on to the target server as using the **root** account. Installation takes about five minutes and does not require that you restart the server.

1. From the directory containing the InterScan installation files, type **./isinst** and press ENTER.
2. You are prompted to select which "flavor" of InterScan you want to install, the *CVP* or *Standard* Edition.

- Choose **InterScan VirusWall for CVP** if you will be installing onto a FireWall-1 network and you want InterScan to act as a CVP server.
 - Choose **InterScan VirusWall for FTP, SMTP, and HTTP** to install the Standard Edition of InterScan. Also, switch now to Chapter 3 of this manual for special installation instructions.
3. A **Setup** menu appears showing the current InterScan system configuration. **None** indicates that the package is not installed. If any systems or sub-systems are **Installed**, remove them (**Option 2**) before proceeding with Setup.
- Choose **Option 1** to begin installing InterScan.
4. By default, InterScan will install all available systems to sub-directories of /opt/trend

```
InterScan VirusWall 3
Setup Script

Install InterScan Base System-----[ YES ]
Installation Path      /opt/trend/ISBASE

Install InterScan CGI Admin-----[ YES ]
Installation Path      /opt/trend/ISADMIN

Install InterScan CVP System-----[ YES ]
Installation Path      /opt/trend/ISCVF

Install InterScan VirusWall TVCS----[ NO ]
Installation Path      /opt/trend/ISTVCS

1. Modify option for BASE.
2. Modify option for ADMIN.
3. Modify option for CVP.
4. Modify option for TVCS. (see page 4-18)
5. Start installation.
6. Back to Main Menu.

Select a number [ 5 ]
```

To modify the Install status or path of a system,

- a. Specify the option you want to change and press Enter.
1=Base (required), 2=Administration interface (required), 3=CVP VirusWall, 4=Trend VCS Agent.
- b. Enter **y** to install the system or change the Install path, or **n** to remove it from the list.
- c. Specify the new path or press Enter to accept the default, `/opt/trend/[SYSTEM]`.

Installing selected VirusWalls

Unlike with InterScan *Standard* Edition, for the *CVP* Edition all three protocols (SMTP, HTTP, FTP) are installed as a single daemon; FireWall-1 will controls which protocol is scanned.

Note: To run each VirusWall on a dedicated machine, you need to install the **InterScan Base**, **CGI Admin**, and the VirusWall daemon onto each machine.

5. Choose **Start Installation** at the Setup Script menu to start the installation. Enter **y** as prompted to continue installation.
6. Once the **InterScan Base** and **Admin** systems are installed you are prompted to enter a serial number to continue with the installation of the VirusWall(s).

Installing the 30-day trial version

Press **Enter** without entering a serial number to install the 30-day trial version. This version of InterScan is fully functional but will expire after 30 days, at which time you should either obtain a serial number and register the product, or uninstall it and re-route your protocol traffic so InterScan is no longer a destination. To upgrade visit our web site:

<http://www.antivirus.com/buy/usc.htm>

7. Follow the on-screen prompts to complete the Setup.

After Installing InterScan...

After installing the InterScan program files, you need to configure InterScan and your FireWall-1 to work together. These steps are presented next.

Configuring InterScan

The following is a summary of the tasks required to set up both the InterScan and FireWall-1 machines. Step by step instructions follow.

On the InterScan side...

There are three things to check on the InterScan side:

1. Be sure that both InterScan's **Main service port** and FireWall-1's FW1_cvp service show the same port number. Typically, both will use port 18181.
2. If you use Check Point Software's OPSEC Authentication, enable this option in the InterScan configuration.
3. Be sure that InterScan is turned **ON** (when **Off**, network traffic does not pass thru InterScan and, unless re-routed, network traffic for that protocol will stop).



Figure 4-2. InterScan can be turned ON or OFF.

On the FireWall-1 side...

There are two main tasks for adding InterScan to FireWall-1:

1. Create the necessary objects and add the InterScan rules to the rule base.
 - a. Create a **Network** workstation object for each machine with InterScan VirusWall installed.
 - b. Create a **Server** object (one for each protocol if InterScan is installed on multiple machines).
 - c. Create a **Resource** (one for each protocol if InterScan is installed on multiple machines).
 - d. Add and install your scanning rules to the **rules base**.
2. *If you are using Check Point's OPSEC Authentication*, register the InterScan machine with FireWall-1 prior to enabling authentication in the InterScan configuration interface.

Note: InterScan does not support **Read Only** (or **Check**) mode of CVP and needs to be configured at the FireWall-1 Security Policy Editor in **Read/Write** mode (or **Cure**). See your FireWall-1 documentation for complete configuration details.

Setting The Main Service Port

1. From the FireWall-1 rule base editor, click the **Services** check box and select FW1_cvp from the list of **Services Objects** that appears. Double click FW1_cvp to see which port it is using (18181).
2. Next, from the InterScan configuration page, click **Configuration** in the left window frame and then the **CVP Configuration** button that appears on the right.

3. In the Main Service Port field, enter the port number that you have determined the FW1_cvp is using.

OPSEC Authentication Users

If you are using OPSEC Authentication,

1. Bring up the InterScan configuration page and click **Configuration**, then the **ISCVP Configuration** button.
2. Choose **ON** for the **Authentication Port** option.

Enable Virus Scanning

Upon installation, SMTP, HTTP, and FTP virus scanning are enabled and do not require subsequent configuration. To check your settings, open the web browser:

1. Bring up the InterScan configuration page and click **Turn On/Off InterScan**.
2. Click **On** to enable scanning if the current status is CVP OFF, or **Off** to disable scanning if the status is CVP ON.

Adding InterScan to the FireWall-1 Rule Base

FireWall-1 operates at the packet level, distributing the individual packets it receives on the basis of protocol type and the policies that are defined in the FireWall-1 rule base. In order for InterScan to receive these packets from FireWall-1, Server and Resource objects representing InterScan must be defined in the rule base and a policy describing their use engaged.

Each of the five FireWall-1 tasks is described below.

Note: The graphics which follow show the Windows/Motif user interface. If you use OpenLook, please be aware that the screen arrangement may look slightly different.

A.) Create a Network Object

1. In the FireWall-1 configuration page, click **Manage | Network Objects...**
2. Click **New**, then choose **Workstation** (or choose an existing Network object representing the InterScan machine).
 - If you installed the InterScan onto the FireWall-1 machine, a Network Object may already exist.
 - If you installed one instance of InterScan, create only one Network Object.
 - If you installed multiple instances of InterScan, create a different Network Object for each machine.
3. In the **General** tab, enter the name of the machine where InterScan is installed in the **Name:** field. For example,

USS_Enterprise

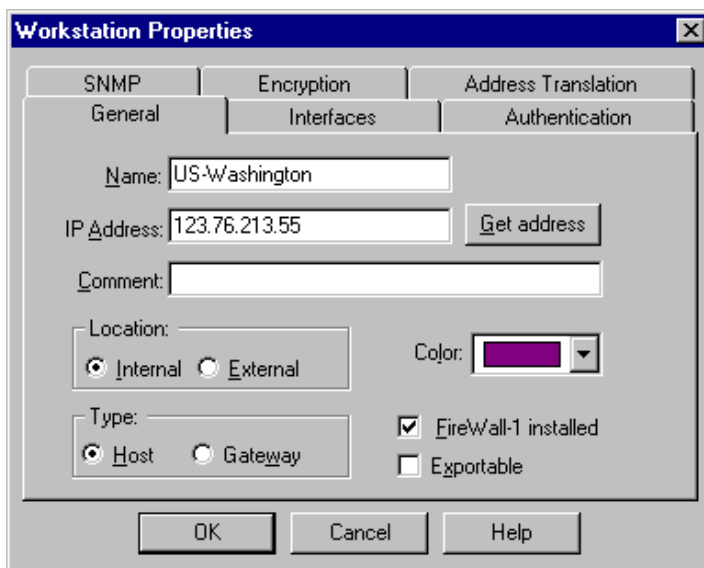


Figure 4-3. Create a **Network Object** for each of the VirusWalls.

4. In the **IP Address:** field, enter the IP address of this server or click **Get address** to have FireWall-1 resolve it automatically.
5. Fill out the rest of the page, for example, **Location** (Internal, External) and **Type** (Host, Gateway) as appropriate for your circumstances.

No particular settings are required for InterScan, and none of the other pages are directly relevant to this set up.

6. Click **Close** when you have finished.

B.) FireWall-1: Create a Server Object

1. In the FireWall-1 configuration page, click **Manage | Servers...**
2. Click **New...**, then choose **CVP** from the drop down menu.
3. Enter a name for the Server in the **Name:** field, for example, **E-mail_VirusWall_Server**.

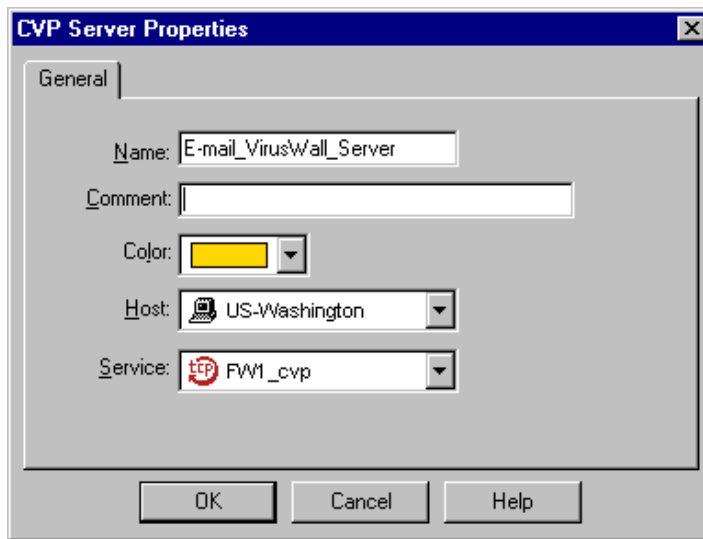


Figure 4-4. Define a **Server Object** for each of the VirusWalls.

4. Next, click the **Host** drop-down box and select from the list that appears the *Network Object* you created in task A, the **USS_Enterprise** in our example.
5. Accept the **Service:** type already specified, i.e., *FWI_cvp*.
6. Click **OK**, then **Close**. Repeat these steps for each InterScan service you will add (SMTP, HTTP, FTP).

C.) FireWall-1: Create a Resource Object

1. In the FireWall-1 configuration page, click **Manage | Resources...**
2. Click **New...**, then choose the appropriate protocol from the drop down menu that appears.
 - Choose **SMTP** for the E-mail VirusWall
 - Choose **URI** for the Web VirusWall
 - Choose **FTP** for the FTP VirusWall

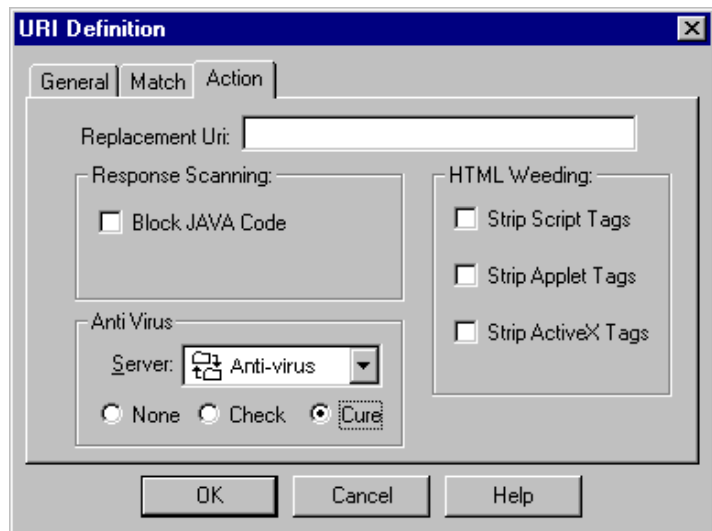


Figure 4-5. Define a **Resource Object** for each VirusWall.

3. In the **General** tab, enter a name for the Resource in the **Name:** field, for example, **E-mail VirusWall_Resource**.

HTTP and FTP scanning

- a. Make the **Action** tab active and, in the **Server:** drop-down box, select the *Server* you created in task C, **E-mail_VirusWall_Server** in our example.
- b. Click **Read/Write**, the only valid option with InterScan, to enable virus scanning and cleaning. (The **None** option is not supported by InterScan—instead, disable virus scanning via InterScan side. InterScan does not support the **Check** option.)

SMTP scanning

- a. For the E-mail VirusWall, make the **Action2** tab active and, from the **Server:** drop-down box, select the *Server* you created in task C.
 - b. Click **Read/Write** to enable virus scanning and cleaning (see **b.** above).
4. Click **OK**, then **Close**.

D.) FireWall-1: Add Rule to the Rule Base

1. In the FireWall-1 configuration page menu, click **Edit | Add Rule | Top** to create a new rule.
2. Next, right-click the **Service** column of the rule and choose **Add With Resource....**
3. From the list of **Services** that appears, select
 - **smtp** for the E-mail VirusWall service (*task B*) and specify the E-mail VirusWall resource (*task D*)

- **http** for the Web VirusWall service (*task B*) and specify the Web VirusWall resource (*task D*)
 - **ftp** for the FTP VirusWall service (*task B*) and specify the FTP VirusWall resource (*task D*)
4. Right-click the **Action** column of the rule and choose **accept** from the menu that appears.

No	Source	Destination	Service	Action	Track
1	LocalNet	Any	ftp->AntiVirus-FTP http->AntiVirus-Web	accept	Account
2	MailServer	Any	smtp->AntiVirus-OutBoundMail	accept	Account
3	Any	MailServer	smtp->AntiVirus-InboundMail	accept	Account
4	Any	Any	Any	reject	Log

Figure 4-6. InterScan's scanning services are added to the CVP rule base.

5. Optionally, right-click the **Track** column of the rule and choose **Long** from the menu that appears to enable logging.

Installing the Rule

1. From the FireWall-1 configuration page menu, click **Policy | Install**.
2. Highlight the FireWall-1 server where you want this policy installed, and click **OK**.
3. Click **Close** to complete the operation.

Rule Base Order

FireWall-1 examines the rule base sequentially, from top to bottom, until a rule successfully matches the type of traffic being examined. We recommend that you place the InterScan CVP rules accepting

HTTP, SMTP, and FTP connections *before* any other rules which accept these services to prevent unwanted traffic from entering the network.

For example, if you define a rule allowing all HTTP connections but place this rule ahead of one specifying CVP scanning on a URI Resource, *the CVP rule will never be executed*.

Optional: Setting up OPSEC Authentication

The connection between InterScan and FireWall-1 can *optionally* be authenticated at the transport layer using Check Point's proprietary authentication algorithm. Prior to enabling the FireWall-1 authentication port in InterScan, do the following:

- Establish an authentication key for communication between the machines. The machines identify themselves using the authentication key.
- Establish authenticated communication between the OPSEC Client process (FireWall-1) and the OPSEC Server process (InterScan).

For example, say there are two machines: "**FireWall-1**" and "**InterScan**".

1. On **FireWall-1**, enter the following command:

```
fw putkey -opsec InterScan
```

where **InterScan** represents the host name of the machine where InterScan is installed. You are prompted (twice) to enter the authentication key.

2. Next, on InterScan, enter the following:

```
opsec_putkey FireWall-1
```

where **FireWall-1** represents the host name of the machine where FireWall-1 is installed. Again, you are prompted

(twice) to enter the authentication key. Enter the same key as entered in Step 1.

Note: Putkey must be run first on the firewall before it is run from the CVP server. See **Running putkey** below.

3. On **FireWall-1**, change `$FWDIR/conf/fwopsec.conf` as follows:

```
server 127.0.0.1 18181 auth_opsec
```

should be changed to

```
server InterScan 18181 auth_opsec
```

where **InterScan** represents the hostname of the CVP server.

Running putkey

4. From the CVP server, open a console and change to the `/etc/iscan` directory. Enter `opsec_putkey` followed by the host name of FireWall-1.

Alternatively, you can set the environmental variable. From the CVP server, open a console and enter

```
OPSECDIR=/etc/iscan ; export OPSECDIR
```

5. Finally, from the InterScan's configuration enable **Authentication** port by clicking **Yes**.

Opening the InterScan Console

After installation, InterScan will automatically stop and restart your Sendmail and/or other daemons to initiate scanning. Although InterScan is configured to run on a robust set of default values, its a good idea to open the configuration console to confirm or modify the settings to fit you particular needs.

1. Enter the URL of the InterScan machine. For example,

`http://IP Address:port/interscan`

The IP address can be either the domain name or number of the InterScan machine. The port is 1812.

`http://209.76.213.256:1812/interscan`
`http://av.widgets.com:1812/interscan`

2. The InterScan configuration is password protected By default, both the user name and password are **admin**

Starting and Stopping InterScan

By default, all InterScan services are enabled upon installation. Each VirusWall can also be individually controlled, however, according to the following options:

- Enable/disable real-time scanning for a given VirusWall
- Turn on/turn off the network flow of a given protocol

To enable/disable real-time scanning,

1. In the InterScan console, click **Configuration | General Settings**.
2. Click any of the **Real-Time Scan** settings to toggle on/off scanning for that service. The flow of traffic is not affected.

To turn on/turn off InterScan,

1. In the InterScan console, click **Configuration | Turn On/Off InterScan**.
2. Click any of the VirusWall options to stop the flow of all network traffic for the given protocol.

Changing the InterScan Password

1. In the InterScan console, click **Configuration | Change Password**.
2. Enter your current password in the **Old Password** field, then enter and confirm the new password you want to use.
3. Click **Apply** to save your new password or **Cancel** to revert to the old one.

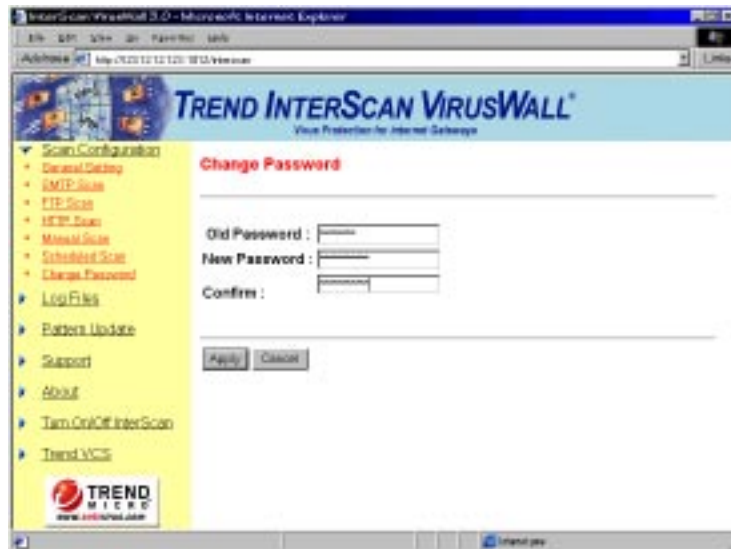


Figure 4-7. The default username and password are "admin".

Testing InterScan

Once Trend VirusWall has been installed, we recommend that you test it to get familiar with the configuration and see how it works.

The European Institute of Computer Antivirus Research, along with antivirus vendors, has developed a test file that can be used for checking your installation and configuration.

The file is not an actual virus; it will cause no harm and it will not replicate. Rather, it is a specially created file whose signature has been included in the Trend Micro virus pattern file. You can download the file from Trend at:

<http://www.antivirus.com/vinfo/testfiles/index.htm>

Once on your machine, you can use the test virus in e-mail to test SMTP scanning, and also to check FTP and HTTP file transfers.

Troubleshooting a CVP Setup

Check the version of FireWall-1

Verify that you are using the correct version of FireWall-1. InterScan is certified to correctly work with FireWall-1 versions 3.0b build 3064 and later. To check your version, open a console on the FireWall-1 machine and enter the following command:

```
$FWDIR/bin/fw ver
```

to verify the version of FireWall-1 you are using.

Turn off OPSEC authentication

Another good troubleshooting first step is to turn off OPSEC Authentication (if you are using this feature) and test again.

Use a packet sniffer

If you have access to a "packet sniffer" program, use it to check the packet headers to see if they are being properly addressed (i.e., FireWall-1 is changing the destination port number to the specified CVP service port, for example 18181). If the port is not being changed, the problem is on the FireWall-1 side. If the port is being changed, the problem may lie on the InterScan side.

Check the FireWall-1 event logs

Use the event logging available from FireWall-1 to see if SMTP, HTTP, and/or FTP traffic is being processed by FireWall-1.

Refresh your browser

If testing HTTP virus blocking, it is often necessary to refresh the browser to avoid drawing upon a cached copy of the screen/file rather than generating a new get call.

Turn on InterScan's verbose mode

Use *a* text editor to add the following parameter to the `[iscvp]` section of the `intscan.ini` file:

```
verbose=yes
```

Stop and restart InterScan after saving the change. Then check the InterScan logs to verify whether InterScan is receiving traffic from FireWall-1. If not, check your FireWall-1 rule base.

If Notification messages are not being sent/received...

InterScan automatically uses the sendmail daemon installed on its host machine to send notification messages. If no sendmail daemon is installed, or it is not running, notification messages will not be sent. You can have InterScan use a remote sendmail by specifying the IP address of that machine in the `intscan.ini` file.

If Network traffic (SMTP, HTTP, and/or FTP) has stopped...

If InterScan is "turned off" in the InterScan configuration but network traffic has not be rerouted at the firewall, all network traffic will cease. Either "turn on," scanning through the InterScan configuration or configure FireWall-1 so it no longer passes network traffic to the InterScan machine.

Network traffic may also be halted if the connection between FireWall-1 and InterScan is mismatched. Check that the **Main Service Port** used by InterScan matches the **Service Port** specified for the FW1-CVP service of FireWall-1.

Additionally, check that all the InterScan elements have been properly defined in FireWall-1 (e.g., that the IP address given for the InterScan servers is correct, that the port is correct, etc.).

Uninstalling InterScan

InterScan's uninstall scripts require super-user privileges. You must be logged on as **root** to Uninstall InterScan.

1. To remove one or all the InterScan VirusWalls, bring up the **Main Menu** by entering `./isinst` in the directory where your InterScan files are located.
2. Choose **Option 2**, and follow the on-screen prompts to complete installation.

Note: When changing from InterScan Standard to InterScan CVP Editions, you'll be prompted to uninstall any existing VirusWalls. The Base System and CGI Admin can remain.

Section II

Configuring InterScan



- **Chapter 5**
E-mail VirusWall & Anti-Spam Control
- **Chapter 6**
FTP VirusWall
- **Chapter 7**
Web VirusWall
- **Chapter 8**
Manual and Scheduled Scans

5 E-mail VirusWall & Anti-Spam Control

E-mail VirusWall scans all inbound and outbound messages for viruses. It supports a variety of network configurations, including scanning for sendmail on either the same or different machine, or scanning for a MTA server that is installed on either the same or a different machine.

How you configure the Main Service port option in the E-mail Scan page depends on the installation topology you have chosen.

Note: If you installed the *Plugin* Edition of E-mail VirusWall, see the end of this chapter for information about Anti-Spam control.

Enabling or Disabling E-mail Scan

E-mail VirusWall, like all the VirusWalls, can be **Enabled** or **Disabled** from the **General Configuration** page (figure 6-1).

1. In the menu on the left, click **Configuration**, then **General Configuration** from the drop-down options that appear.
2. In the **General Configuration** windows, click the **E-mail Scan** check box:
 - A check means real-time scanning is enabled
 - No check means real-time scanning is *not* enabled

Configuring E-mail Scans

E-Mail VirusWall offers the InterScan administrator a great deal of flexibility in configuring how the program will behave.

For example, you can choose which e-mail attachment-types to scan, who should be notified when a virus is discovered, what action should be taken—clean it, delete it, quarantine it, or pass it on to the recipient along with a warning message.

E-mail VirusWall features include:

- Real-time scanning of inbound *and* outbound e-mail traffic
- Automatic, customizable virus notifications
- Option to **Clean**, **Move**, **Delete** or **Pass** on infected files
- Message-size filtering
- File-name checking to guard against e-mail security flaw
- Ability to insert customized tag line to all outbound mail
- Customizable thread and spawning rate control

InterScan Standard Edition

E-mail VirusWall can be installed onto the same machine as your Sendmail or a different one. It also supports running with another SMTP server, installed either on the same machine or a different one. How you configure **E-mail Service** depends upon the installation topology you have selected.

Using Sendmail daemon

If E-mail Virus Wall and Sendmail are on the same machine,

1. In the **Main service port** field, specify the port on which E-mail VirusWall will listen for SMTP connections (e.g., 25).

- Specify the location of your Sendmail daemon in the **Original SMTP server location:** field. For example,

/usr/lib/sendmail -bs

Note: Only the *Standard* Edition uses the **-bs** flag (formats scanned messages for delivery to the SMTP server).

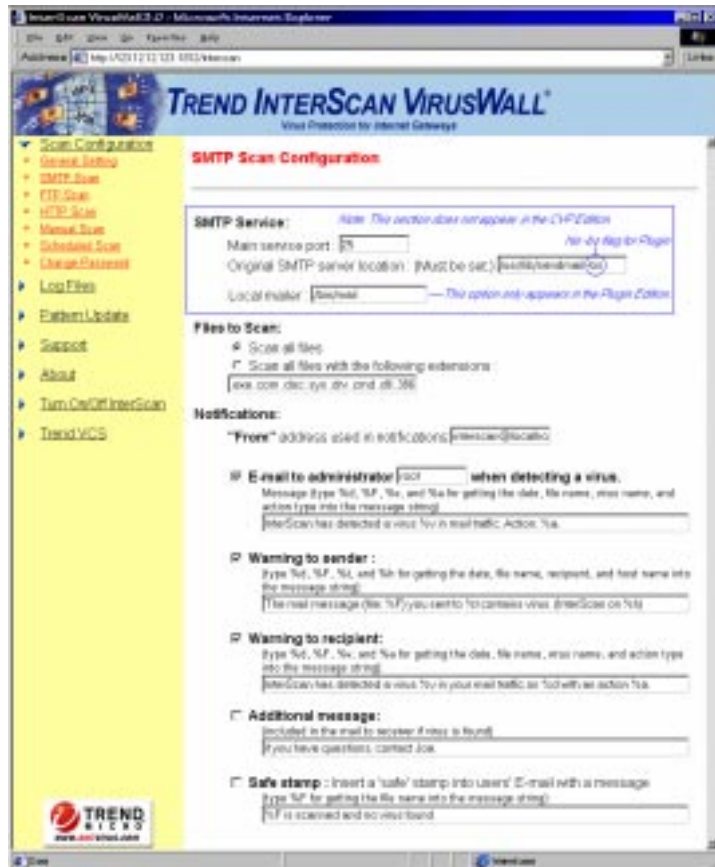


Figure 5-1. Your SMTP Service settings depend on where E-mail VirusWall is installed and the Edition you are running.

How it works: E-mail VirusWall receives SMTP traffic on port 25, scans it, and then *pipes* it to the Sendmail daemon.

If E-mail VirusWall and Sendmail are on the different machines

When E-mail VirusWall and Sendmail are installed on different machine, its configuration is the same for any SMTP server installed on a different machine. See below for details.

Using another SMTP server

If E-mail VirusWall and your original SMTP server are on the same machine,

1. In the **Main service port** field, specify port 25 (the port E-mail VirusWall will use to listen for new SMTP connections).
2. Change the port used by your SMTP server, for example to 5000.
3. In the **Original SMTP server location:** field, enter location of your SMTP server followed by the new port that it will use. For example,

```
localhost 5000  
yourcompany.com 5000  
mailserver.yourcompany.com 5000
```

How it works: E-mail VirusWall receives SMTP traffic on port 25, scans it, and then forwards it to the SMTP server as identified in the **Original SMTP server location** field.

Since both E-mail VirusWall and the SMTP server are on the same machine, and if, as is typical, E-mail VirusWall is set to use port 25, the transfer of scanned mail from E-mail VirusWall to the SMTP server cannot take place using port 25. Instead, a port such as 5000 is used for the transfer (you must configure your SMTP server to use the same port, in this example, 5000).

If E-mail Virus Wall and your original SMTP server are on different machines,

1. In the **Main service port** field, specify port 25 (the port E-mail VirusWall will use to listen for new SMTP connections).
2. In the **Original SMTP server location:** field, specify the hostname (or IP address) *and port* of your SMTP server. This port is often 25. For example,

```
mailserver 25  
mailserver.yourcompany.com 25  
123.12.12.123 25
```

How it works: E-mail VirusWall receives SMTP traffic on port 25, scans it, and then routes it to the SMTP server specified for **Original SMTP server location** using the port specified.

InterScan *Plugin* Edition

The *Plugin* Edition of E-mail VirusWall should only be installed on the same server as the Sendmail daemon it will scan for. As such, the **Original SMTP server location** will be the location of the Sendmail daemon rather than an IP address or domain name.

Note: No flag should be specified in the original SMTP server location line (contrary to the *Standard* version, which uses a **-bs** flag).

1. Specify the location of your Sendmail daemon in the **Original SMTP server location:** field. For example,

```
/usr/lib/sendmail
```
2. In the **Local mailer:** field, (see figure 5-1) verify that the location indicated is correct. During Setup, InterScan parses the value from `sendmail.cf`, where available. If the **Local**

mailer: field is blank or incorrect, you need to determine the value and the correct location. For example,

```
/bin/mail
```

InterScan CVP Edition

For the *CVP* Edition of InterScan, E-mail VirusWall receives all SMTP traffic from the firewall, scans it, and then returns it to the firewall for routing as normal. Because the firewall handles delivery of SMTP traffic to the SMTP server, no particular location or port information is required by E-mail VirusWall.

Both inbound and outbound SMTP traffic can be scanned, as determined by the policies you create in your FireWall-1 rule base.

Specifying Which Files to Scan

InterScan can check all or specified types of e-mail attachments for viruses, including individual files within a compressed volume.

To select which files to scan,

1. To scan all e-mail attachments regardless of type, click the **Scan all files** radio button. This is the most secure configuration. Compressed files are opened and all files within scanned.
2. To scan only selected file types, click the **Files with the following extensions:** radio button. Only those file types that are explicitly specified in the associated text box are scanned.

```
.com .exe .sys .doc .xls .zip .dll
```

Use this option, for example, to decrease the aggregate number of files InterScan checks, thus decreasing overall scan times. Many file types (e.g., graphics) have never been known to carry viruses.

Note: Zip and other compressed file are only scanned if the file type is specified. Compressed files are opened and all files scanned.

There is no limit to the number or types of files you can specify here. Also, note that no wildcard (*) proceeds the extension, and multiple entries are delimited by a space.

Setting Virus Notifications

Upon detecting a virus, InterScan can send an automatic e-mail notification to the **Administrator**, **Sender**, and/or **Recipient** (inbound, and unblocked outbound mail only). The notification text is fully customizable.

"From:" field

You can have any e-mail address you want appear in the "**From:**" field of the virus notification message(s) sent by E-mail VirusWall; however, only valid accounts on the local SMTP server will be delivered if users attempt to **Reply to** the notification message.

Alternatively, you could create an alias mail account with auto-reply and include that address in the "**From:**" field. Users who **Reply to** the virus notification would then receive whatever information you want them to have in regards to the virus incident.

To notify the administrator, sender, or recipient,

1. Click appropriate checkbox (**E-mail to administrator or Warning**).
2. For the administrator, enter the e-mail address (**root**, for example) in the associated text box. For the Sender or Recipient, the address is taken from the e-mail.

Note: Multiple e-mail addresses are not supported.

In the **Message** field, enter the warning message you want the administrator to receive. The following case-sensitive variables can be used in the message:

```
%a = Action taken: Delete, Move, Pass
%d = Date virus was detected
%F = File where virus was detected
%f = For e-mail, identifies sender
%v = Virus name
%t = For e-mail, identifies recipient
%M = When action is move, displays the
      destination directory and filename
%m = Detection method
%h = Host name
```

For example,

```
Warning! On %d, InterScan detected the
%v virus in the file: %F. InterScan
took the following action: %a.
```

which reads, "Warning! On **6-20-99**, InterScan detected the **Jerusalem** virus in the file: **Word.com**. InterScan took the following action: **delete**."

Note: Verbs, such as *delete* in the example above, are in simple present tense; be sure to structure the grammar of your note accordingly.

Adding additional messages

1. Check **Additional Message** to have InterScan append a brief note to the top of any e-mail in which a virus is found. In the associated text field, enter your message. The administrator, sender, and/or recipient will receive a message such as the following:

```
*****InterScan Message*****
InterScan detected a virus in your e-mail
and deleted the infected attachment. You
need to clean or delete the original
infected file from your hard drive ASAP.
*****
```

2. Check **Stamp** to have InterScan append a brief note to the top of scanned messages to let users know that their e-mail was scanned and found to be virus free. Use %F if you want InterScan to include the name of the file(s) scanned.

```
***** InterScan Message *****
InterScan checked the attached file,
Mystery.zip, and found no virus(es).
*****
```

Setting the Action on Viruses

You can specify the action InterScan takes upon finding a virus:

- Choose **Pass** to send infected file, along with a warning message and the original message text, to the intended recipient *without cleaning*.
- Choose **Move** to move, *without cleaning*, the infected attachment to the quarantine directory (by default, /etc/iscan/virus). The recipient will receive the original message text, but not the attachment.
- Choose **Delete** to remove the infected attachment from the e-mail and delete it from the server. The recipient will receive the original message text, but not the attachment.
- Choose **Auto Clean** to have E-mail VirusWall automatically clean and process infected files. The recipient will receive both the original message text and the attachment.

If an infected file cannot be cleaned, for example because the virus has corrupted it, E-mail VirusWall will then take the action specified for **Action on Non-Cleanable Files**:

- Choose **Pass** to deliver both the message text and infected file to the recipient. A separate warning message is sent.
- Choose **Move** to deliver the message text to the intended recipient, but quarantine the infected file.
- Choose **Delete** to send the message text on to the intended recipient and delete the infected file.

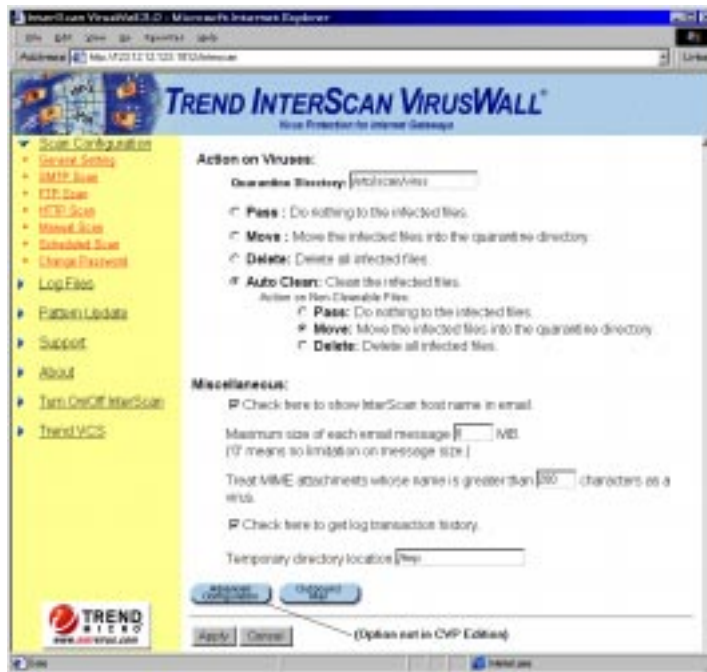


Figure 5-2. InterScan can clean infected files; a variety of miscellaneous options are also available.

Miscellaneous

In addition to scanning all inbound and/or outbound SMTP traffic for viruses, you can have InterScan reject e-mail messages larger than a specified size, and protect against the "e-mail flaw," a problem that occurs in some e-mail clients if they receive an attachment with a file name so long that it exceeds the allocated buffer.

Displaying "InterScan" in the E-mail Header

Whenever it inserts an optional Safe Stamp or virus found notification in the original e-mail, InterScan by default identifies itself. For example,

```
***** InterScan Message *****
InterScan checked the attached file,
Mystery.zip, and found no virus(es).
*****
```

If you prefer not to reveal the presence of InterScan, the top line can be replaced entirely with asterisks.

Click **Check here to show InterScan host name in email** to toggle on/off the *****InterScan Message ***** line.

Limiting Message Size

E-mail VirusWall can reject, without scanning or further processing, messages that exceed a certain size.

1. In the **Maximum size...** field, enter an integer to represent the largest allowable message (in megabytes).

E-mail messages that exceed the value specified here are rejected by InterScan. The remote SMTP server generates the non-delivery report.

2. Alternatively, enter a zero (0) to have InterScan route messages of any size.

Protecting Against the "E-mail Security Flaw"

E-mail VirusWall solves the "E-mail Security Flaw" that was discovered in 1998 and found to effect many e-mail client programs. Malicious users may exploit the flaw by e-mailing an attachment with a very long file name to vulnerable machines, potentially allowing the person to gain control of the client machine.

This e-mail security flaw is not related to InterScan, Sendmail, or any SMTP server. The InterScan solution works regardless of the clients being used. Essentially, InterScan checks for attachments with very long file names (those longer than 200 characters, for example), and take the action specified for viruses whenever a very long file name is discovered—the message is not routed on to the SMTP server.

To protect against the E-mail Flaw,

Check the **Treat MIME attachments whose name is greater than _____ characters as a virus** field and enter the maximum number of characters you want to allow for an e-mail attachment file name. A record of the event and a copy of the attachment are kept in the log.

Logging Transactions...

By default, InterScan logs only errors and the starting/stopping of the services. To have InterScan log each individual transaction, click **Check here to get log transaction history**.

Note: Specify where InterScan keeps its logs from the **General Configuration** page.

Temporary Directory Location

InterScan uses the /tmp or whatever other directory you specify to do the work of scanning for viruses.

Note: Specify a directory with at least 500 MB available free space.

Outbound Mail Processing

E-mail VirusWall checks all SMTP traffic processed by your SMTP server (i.e., both inbound and outbound).

For outbound messages, however, additional options are available:

- You can block infected messages and notify the sender and/or administrator (the intended recipient is not notified)
- You can insert a standard tag line, or disclaimer, to the top of all outbound messages

Note: For the CVP Edition of InterScan, set inbound and/or outbound traffic scanning from the FireWall-1 side by creating and adding the desired rules to the FireWall-1 rule base.

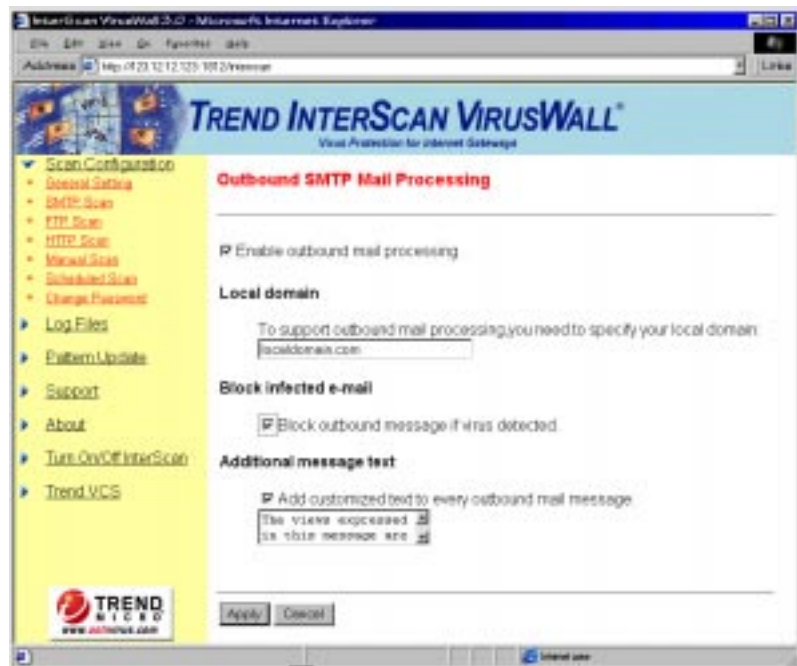


Figure 5-3. InterScan can stop delivery of infected outbound messages and/or insert a standard message at the top of outbound mail.

To block infected outbound messages...

1. From the **E-mail Scan Configuration** page (open the InterScan configuration and click **Configuration | E-mail Configuration**), click the **Outbound Mail** button.
2. Check **Enable outbound mail processing**. This option must be checked for outbound E-mail scanning and/or appending additional message text to occur.
3. Enter your local domain or sub-domain (not *IP address*). For example, enter *widgets.com* in the **Local domain** field.

Specifying Sub-domains

If you have multiple LANs or use multiple SMTP servers, you can specify a single sub-domain (for example *accounts.widgets.com*) in the **Local domain** field. In this case, infected messages sent between sub-domains will be blocked.

4. Check **Block outbound message if virus detect** to have E-mail VirusWall stop the delivery of infected e-mails. Infected message are bounced back to the sender; a copy of the infected attachment is placed in the quarantine directory (*/etc/iscan/virus* by default).

Note: The intended recipient of a *blocked* message will not receive the e-mail and will not be notified. The Sender and Administrator are always notified, independent of the optional Notification setting.

Additional message text

5. Choose **Add customized text to every outbound mail message** and enter the message you want appended to the top of outbound e-mail messages. There is no limit to the length of the message you add here. An example "tag line" and disclaimer are shown below:

"Satisfaction guaranteed at Widgets!"
<or>
"Opinions expressed in this message are
the author's alone."

E-mail Scan Advanced Options

Note: Advance Options only pertains to InterScan *Standard* Edition.
This section does not apply to the *CVP* and *Plugin* Editions.

To optimize performance, InterScan *Standard* Edition provides several "Advanced" parameters that you can configure to control how many threads InterScan spawns upon start up, how many child processes each thread may spawn, how often the threads are regenerated, and how many simultaneous threads can be supported.

To edit the Advance Options,

1. Open the InterScan console and click **Configuration | E-mail Confutation** in the left hand menu that appears.
2. Scroll to the bottom of the E-mail Scan Conversation page that appears and click the **Advanced...** button.

General Configuration

The General Configuration options allow you to set up performance monitoring, have E-mail VirusWall issue a "greeting" whenever a connection is received, and/or keep a running log of all transactions. Each of these options are explained below.

Monitoring performance...

InterScan supports the use of real-time client monitoring programs for the display of InterScan's performance data. **Perfmon**, one such program, is included with InterScan.

To use **Perfmon** or a similar program, you must enter the port number that the daemon will listen on, for example 10021, 10025, 10080.

Any free port can be used, but be sure to use a different port for each service (e-mail, FTP, or HTTP) you intend to monitor.

The monitoring program receives data, in real time, from the daemon using a port that is bound by the daemon. Tracked values include:

- Total active threads
- Individual PID's (process identification numbers)
- Total connections
- Total idle time
- Total processes created

Note: To disable port monitoring, set this value to zero.

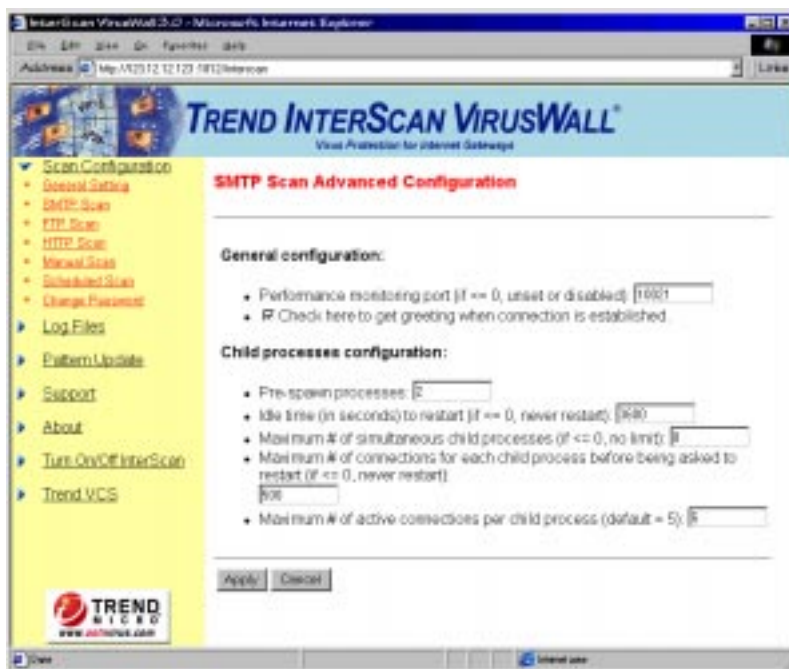


Figure 5-4. You can fine-tune InterScan's performance using the Advanced options (these options are not available in the CVP Edition).

Receiving InterScan greetings...

InterScan can send a "greeting" upon receiving new client connections. This greeting, shown below, is not user configurable:

```
220 - InterScan 3.0: Ready
```

Use Telnet or a similar program to observe how the feature works, for example by Telneting to the InterScan machine using port 25.

Child Process Configurations

You can fine-tune InterScan's performance by making adjustments to such settings and the number of processes spawned upon startup and the refresh rate of idle processes. In addition, you can limit the total number of child processes InterScan will use at any one time, and the total number of child processes spawned for a given thread.

Note: Improperly adjusting the Advanced settings can result in system instability. We recommend that you use the defaults unless there is a specific performance-based reason to alter them.

Pre-spawning processes...

By default when the InterScan E-mail VirusWall service is started it will create two child processes to handle the estimated existing traffic load. Depending on your system resources and traffic load levels, you may want to increase the Pre-process Generation number.

Note: There is no maximum allowed value. However, entering too large of a number can result in wasted system resources.

Regenerating idle processes...

InterScan will automatically generate child processes as needed to accommodate traffic spikes. As the spikes taper off, excess child

processes are left idle. You can specify, in seconds, how quickly these idle processes are extinguished in the **Idle time to restart** field.

Choosing the right idle time is important. On the one hand, the accumulation of a lot of idle child processes means system resources are being wasted. On the other hand, existing, idle processes can respond more rapidly to sudden increases in the work load than if a host of new processes must be spawned to accommodate the additional load.

Note: Specifying a value of zero (0) means that idle child processes are never extinguished.

- A typical number **Idle time to restart** value is 3600 seconds, i.e., one hour.
- An **Idle time to restart** value of zero means the number of available processes will always equal your highest usage spikes, no matter how brief or infrequent they may be.
- An **Idle time to restart** value of just a few seconds means InterScan will have to create new processes just about every time there is a change in the work load.

In specifying an **Idle time to restart** value, choose a number that represents a balance between the need to create new processes and the unwanted accumulation of idle processes.

Limiting child processes...

Before creating a new child process, InterScan checks first to see if there are any existing processes that can be used. If there are none, InterScan will create a new one.

Although there is typically no need to limit the number of child processes InterScan can create.(the limits inherent to the operating system are used) you can impose a limit on InterScan if you must define a maximum.

Whenever the maximum number of child processes is reached, InterScan will stop spawning new threads; the excess mail messages are rejected (the originating client will typically make multiple attempts to send the message before bouncing it back to the sender as undeliverable; in most cases, E-mail VirusWall will be free to accept one of these subsequent re-deliveries).

Extinguishing old connections...

As a matter of "good housekeeping," InterScan extinguishes child processes after a set number of threads have been generated and destroyed, thus ensuring that idle resources do not inadvertently remain active.

A typical number to enter in this field might be 500, meaning that after 500 threads have been generated and extinguished, the hosting child process itself is extinguished and a new one generated to replace it if necessary (a new child will only be spawned if needed). Setting this number too low can result in needlessly brief cycles.

Note: Enter a zero (0) in this field to disable the maximum number of connections option. The default value is 500.

Limiting active connections...

You can limit the number of active connections that InterScan will spawn from a given child process before creating a new child. A typical maximum is five. Entering too high a number and contribute to system instability.

Rule of thumb

You can derive the optimal number used for **Maximum # of active connections...** from the `OPEN_MAX` parameter of the file `/usr/include/limits.h`

Subtract 15 from the `OPEN_MAX` number and divide by ten to obtain a reliable maximum number of active connections per child process (*whole numbers only*).

$(OPEN_MAX - 15) / 10$

For example, if OPEN_MAX equals 45, subtract 15 and divide by 10. You would then enter the number 3 for the maximum number of active connections per child process.

Saving the Configuration

- To save the new configuration, click **Apply**.
- To "undo" your unsaved changes click **Restore**.

E-mail VirusWall *Plugin* Edition

Trend Micro provides a special version of E-mail VirusWall that is designed to work in conjunction with the anti-spam features of Sendmail 8.8.6 or later. This version, called E-mail VirusWall *Plugin* Edition, is an option available only at the time of the initial installation, when you are given the choice of installing either the *Standard* Edition of E-mail VirusWall, or the *Plugin* Edition.

It's important to note that E-mail VirusWall itself does not perform any antispam filtering. It does, however, provide a basic antispam list that can be used by itself, merged with an existing list of spammers, or disregarded

Configuring E-mail VirusWall *Plugin* Edition

As previously noted, the *Plugin* edition must be installed on the same machine as Sendmail 8.8.6 or later; it is not available with the *CVP* Edition. Only two things are necessary on the InterScan side for the *Plugin* Edition of E-mail VirusWall to work with your existing Sendmail:

1. E-mail VirusWall must be properly installed, and
2. The location of your Sendmail is properly identified.

Note: Do not install or use E-mail VirusWall's Anti-Spam Control unless you already have the Sendmail spam filter set up and running on your system. We recommend that you test your spam filter *before* installing E-mail VirusWall to verify that is functioning properly, then again after setting up the VirusWall.

A quick review of the proper **SMTP Scan Configuration** settings follows. In addition, see Chapter 3, *Installing the Standard or Plugin Edition*, pages 3-6 to 3-9 for information on modifying your `sendmail.cf` file.

SMTP Service Settings

Here's a quick review of the proper **SMTP Service** settings on the **SMTP Scan Configuration** page for the *Plugin* Edition:

Original SMTP server location: `/usr/lib/sendmail`

where `/usr/lib/` represents the location of your Sendmail version 8.8.6 or later daemon. No **-bs** flag or port are specified after the sendmail location.

Anti-Spam Control

Trend Micro provides a list of hundreds of "fresh" spammers for use with Sendmail's anti-spam filtering. You can use this list exclusively, merge it with an existing list, or disregard it entirely. Use **Anti-Spam Control** to merge the lists.

Note: Trend's list of spammers follows the standard Sendmail convention: it's a TAB delimited ASCII text file that contains two fields: Address and Rule.

Managing Access Lists

You can use **Anti-Spam Control** as a convenient, browser-based way to manage your existing **access** list (a list of e-mail addresses and associated action such as OK, RELAY, REJECT, DISCARD, or ### any text) and to review, add, edit, and delete your antispam rules.

You can also use it to merge an existing access list with Trends. In this case, there are three main steps.

1. Identify the location of your existing antispam list and merge it with Trend's.
2. Use makemap to create a database file of the merged texts.

3. Back up your current antispam database and then copy the database you just created to the appropriate directory.

To merge access lists,

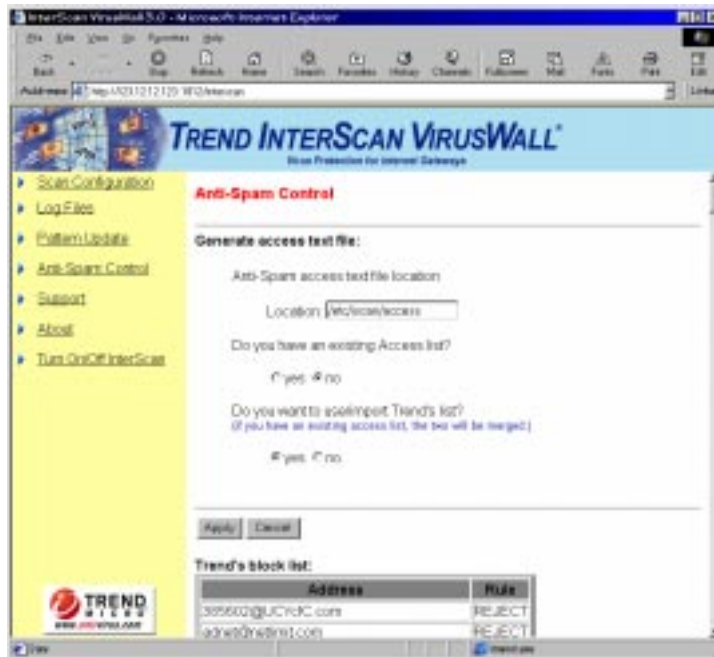
The first time you open **Anti-Spam Control** you have the option of using Trend's access (antispam) list, using an existing one, or merging the two to create a third list. Before deciding, you can preview Trend's block list as it appears at the bottom of the screen.

Note: If no "Block List" appears at the bottom of the screen and instead you see a message stating that the lists are already merged, click **Apply** (or **Generate**) to open the merged list for editing, as explained in the next section of this manual.

Proceed with following steps if you want to merge your existing access list with Trend's, or if you want to use **Anti-Spam Control** to edit your existing access list.

1. Open the InterScan console and click **Anti-Spam Control**. If you have not yet merged access lists, a screen appears with the option to **Generate access text file**.
2. Specify the location and file name of your existing access list, if any. For example, `/etc/mail/access`
3. In the **Do you have an existing Access list?** field, choose **Yes** if you have an existing access list that you want to continue to use, otherwise, choose **No**.

4. In the **Do you want to use/import Trend's list?** field, choose **Yes** to use Trend's access list, or **No** to use only your own list.



Possible combinations of steps 2 and then 3—choose:

- **Yes** and then **No** to *edit* your existing access list
 - **No** and then **Yes** to *edit* Trend's access list
 - **Yes** and then **Yes** to *merge* the two lists into third
 - **No** and then **No** to *use no list* (InterScan reports an error)
5. Click **Apply** to begin the merge. The merged file will be called `access`, and appear in `/etc/iscan/` directory

To create a database file or edit rules,

After merging Trend's access list with an existing one, (or after editing either access text file) you need to generate a database file of the data that can be read by Sendmail.

1. Once the access lists have been merged you can open use **Anti-Spam Control** as a convenient way to edit and/or maintain the list.
2. In the **Anti-Spam access text file location** field, confirm the location and file name of your existing access list, if any. For example, /etc/mail/access
3. In the **Do you have an existing Access list?** field, choose **Yes** and then click **Apply**. A list of antispam rules appears (in the example shown below, the list has been greatly abbreviated).



Figure 5-5. You can use **Anti-Spam Control** to maintain either a merged or existing access list of known spammers.

4. Enter the location of Sendmail's database creation program, `makemap`, in the **Location:** field.
5. Click any rule to mark it for editing (only one rule can be modified at a time), then click the **Add**, **Edit** or **Remove** button as the case may be. the editing options are consistent with Sendmail's:

OK Accept mail regardless of other rules in ruleset

Relay Accept mail to/from the indicated domain

Reject Reject sender/recipient with a general purpose message

Discard Discard message `$#discard` mailer (sender only)

text Where **###** is RFC821 error and text is message to return

6. After modify the rules, click **Make** to generate a Sendmail -ready database of spammers and associated rules.

InterScan will use the `makemap` specified in step 4 and generate a database file called `access.db` in the `/etc/iscan/Spamdb` directory.

To have Sendmail use the new database,

After merging the access files, editing the resulting list and generating a database file for Sendmail to use, the last step is to backup your existing antispam database and copy it to a location where Sendmail can use it. This is done from the command line.

1. Locate your original database file of antispam rules, for example, `etc/mail/access.db` and make a backup copy.
2. Copy the newly created `access.db` from its location in `etc/iscan/Spamdb/access.db` to the sendmail directory.

Sendmail will automatically "pick up" the new file. You don't need to stop and restart the daemon, etc.

6 FTP VirusWall

FTP VirusWall is usually installed so that it will scan FTP file transfers that are being downloaded to the local LAN (as opposed to scanning such transfers for remote users who are accessing a FTP site that you are hosting). Both configurations, however, are possible.

Considerations:

- FTP VirusWall can serve as either the sole FTP server on the network or it can complement an existing one.
- If complementing an existing FTP server, FTP VirusWall can be installed on the same machine or on a different one.
- Installing FTP VirusWall onto a different server (i.e., not on the existing FTP server) is typical and means the VirusWall can be transparent to the end-user (see below).
- If you install FTP VirusWall on a machine other than your original FTP server, it is often advisable to swap IP addresses or hostnames so that FTP VirusWall can have the same IP address that the original FTP server had—your clients won't need to change anything.

Enabling or Disabling FTP Scan

FTP VirusWall, like all the VirusWalls, can be **Enabled** or **Disabled** from the **General Configuration** page.

1. In the menu on the left, click **Configuration**, then **General Configuration** from the menu that appears.
2. In the **General Configuration** windows, click the **FTP Scan** check box:
 - A check in front of **FTP Scan** indicates that real-time scanning is enabled and traffic scanned
 - No check in front of **FTP Scan** indicates that real-time scanning is not enabled and traffic is not being scanned



Figure 6-1. You can enable or disable FTP scanning from the General Settings screen—the flow of traffic is not interrupted. You can also **Turn ON/OFF** the flow of FTP traffic using that menu option, seen in the menu.

Configuring FTP Scans

After installing FTP VirusWall you need to configure it to work on your system. In particular, you need to specify whether InterScan will scan FTP traffic for an existing FTP server (in this case enter the *in.ftpd* location) or if FTP VirusWall will independently handle FTP traffic (in this case choose **Use user@host**).



Figure 6-2. Configure FTP VirusWall to work with an existing FTP proxy server or as the sole FTP proxy on the network.

InterScan *Standard* Edition

The FTP server location and Port you specify in the **FTP Service** fields depends on which edition of FTP VirusWall you are running: *Standard*, or *CVP*. Both are discussed below.

FTP Service

The values entered for FTP service are determined by your set up configuration, in particular whether FTP VirusWall will serve as its own proxy, or, if installed in conjunction with an existing proxy, whether it is installed on the same machine or a different one.

Original FTP server location

In the **Main service port** field, enter the port FTP VirusWall will use to listen for new client connections. Typically, this is port 21. If FTP VirusWall and the proxy are on the same machine, change the proxy's port and give FTP VirusWall port 21. You also need to choose either **Use user@host** or **Server location** (specify location and port)

Use user@host

Choose **Use user@host** if there is no existing FTP server on the network and you want FTP VirusWall to serve as the system's FTP server. Clients will *always* FTP to InterScan, which will then broker the connection to the requested site. When prompted for a user name and password, clients simply add the target domain to their username.

For example, to FTP *widgets.com*, user John would open an FTP session to FTP VirusWall. When prompted, John enters his *Widgets* user name, modified by the *widgets.com* domain, and password.

- Without FTP VirusWall:

```
username: john
password: opensesame
```

- With FTP VirusWall:

```
username: john@widgets.com
password: opensesame
```

Server location

Choose **Server location** if there is an existing FTP server on the system, then enter location *and port* of the server. FTP VirusWall will scan all FTP traffic to and from the machine identified in this field.

If FTP server and FTP VirusWall are on the same machine...

1. In **Main service port**, enter the port used to connect to the FTP server, typically 21.
2. In **Server location**, enter the local path of your FTP daemon. For example,

```
/usr/sbin/in.ftpd
```

If FTP server and FTP VirusWall are on different machines...

1. In **Main service port**, enter the port used to connect to the FTP server, typically 21.
2. In **Server location**, enter the domain name (or IP address) *and path* of the FTP server. For example,

```
ftp-server.yourcompany.com 21  
123.12.13.123 21
```

InterScan CVP Edition

For the *CVP* Edition of InterScan, FTP VirusWall receives all FTP traffic from the firewall, scans it, and then returns it to the firewall for routing as normal. Because the firewall handles delivery of FTP traffic to the FTP server, no location or port information is required.

Both inbound and outbound FTP traffic can be scanned, as determined by the policies you create in your FireWall-1 rule base.

Specifying Which Files to Scan

InterScan can check all or specified file types for viruses, including the individual files contained in a compressed file.

To select which files to scan,

1. To scan all file types, regardless of extension, click the **Scan all files** radio button. This is the most secure configuration. Compressed files are opened and all files within scanned
2. To scan only selected file types, click the **Files with the following extensions:** radio button. Only those file types that are explicitly specified in the associated text box are scanned.

`.com .exe .sys .doc .xls .zip .dll`

Use this option, for example, to decrease the aggregate number of files InterScan checks, thus decreasing overall scan times. Many files types (e.g., graphics) have never been known to carry viruses.

Note: Zip and other compressed file are only scanned if the file type is specified. Compressed files are opened and all files scanned.

There is no limit to the number or types of files you can specify here. Also, note that no wildcard (*) proceeds the extension, and multiple entries are delimited by a space.

Setting Virus Notifications

Upon detecting a virus in a user's FTP transfer, InterScan can automatically send a customized e-mail to the **Administrator**.

"From:" field

You can have any e-mail address you want appear in the **"From:"** field of the virus notification message(s) sent by FTP VirusWall; however, only valid accounts on the local SMTP server will be delivered if users attempt to **Reply to** the notification message.

To notify the administrator,

1. Click the **E-mail to administrator** checkbox.
2. Enter the e-mail address (**root**, for example) in the associated text box.

Note: Multiple e-mail addresses are not supported.

3. In the **Message** field, enter the warning message you want the administrator to receive. The following case-sensitive variables can be used in the message:

```
%a = Action taken: Delete, Move, Pass
%d = Date virus was detected
%F = File where virus was detected
%f = Identifies FTP site
%v = Virus name
%t = Identifies requesting domain
%M = When action is move, displays the
      destination directory and filename
%m = Detection method
%h = Host name
```

For example,

```
Warning! On %d, InterScan detected the
%v virus in the file: %F. InterScan
took the following action: %a.
```

which reads, "Warning! On **6-20-99**, InterScan detected the **Jerusalem** virus in the file: **Word.com**. InterScan took the following action: **delete**."

Setting the Action on Viruses

You can specify one of four actions for InterScan to take upon finding an infected file:

- Choose **Pass** to send infected file, along with a warning message to the client *without cleaning*.
- Choose **Move** to move, *without cleaning*, the infected file to the quarantine directory (by default, `/etc/iscan/virus`). The requesting client will not receive the file.
- Choose **Delete** to reject the infected file from the server. The requesting client will not receive the file.
- Choose **Auto Clean** to have FTP VirusWall automatically clean and process infected files. The requesting client will receive the cleaned file.

If an infected file cannot be cleaned, for example because the virus has corrupted it, FTP VirusWall will then take the action specified for **Action on Non-Cleanable Files**:

- Choose **Pass** to ignore the virus and deliver the file to the requesting client.
- Choose **Move** to infected file to the Quarantine directory.
- Choose **Delete** to reject the infected at the server.

Temporary directory location

InterScan uses the `/tmp` or whatever other directory you specify to do the work of scanning for viruses.

Note: Specify a directory with at least 500 MB available free space.

FTP Scan Advanced Options

Note: Advance Options only pertains to InterScan *Standard* Edition. This section does not apply to the *CVP* and *Plugin* Editions.

To optimize performance, InterScan *Standard* Edition provides several "Advanced" parameters that you can set to control how many threads InterScan spawns upon start up, how many child processes each thread may spawn, how often the threads are regenerated, and how many simultaneous threads can be supported.



Figure 6-3. Advanced Options allow you to optimize performance.

To edit the Advance Options,

1. Open the InterScan console and click **Configuration | FTP Configuration** in the left hand menu that appears.
2. Scroll to the bottom of the FTP Scan Conversation page that appears and click the **Advanced...** button.

General Configuration

The General Configuration options allow you to set up performance monitoring, have FTP VirusWall issue a "greeting" whenever a connection is received, and/or keep a running log of all transactions. Each of these options are explained below.

Monitoring performance...

InterScan supports the use of real-time client monitoring programs for the display of InterScan's performance data. **Perfmon**, one such program, is included with InterScan.

To use **Perfmon** or a similar program, you must enter the port number that the daemon will listen on, for example 10021, 10025, 10080. Any free port can be used, but be sure to use a different port for each service (e-mail, FTP, or HTTP) you intend to monitor.

The monitoring program receives data, in real time, from the daemon using a port that is bound by the daemon. Tracked data values include:

- Total active threads
- Individual PID's (process identification numbers)
- Total connections
- Total idle time
- Total processes created

Note: To disable port monitoring, set this value to zero.

Receiving InterScan greetings...

InterScan can send a "greeting" upon receiving new client connections. This greeting, shown below, is not user configurable:

```
220 - InterScan 3.0: Ready
```

Use Telnet or a similar program to observe how the feature works, for example by Telneting to the InterScan machine using port 21.

Child Process Configurations

You can fine-tune InterScan's performance by making adjustments to such settings and the number of processes spawned upon startup and the refresh rate of idle processes. In addition, you can limit the total number of child processes InterScan will use at any one time, and the total number of child processes spawned for a given thread.

Note: Improperly adjusting the Advanced settings can result in system instability. We recommend that you use the defaults unless there is a specific performance-based reason to alter them.

Pre-spawning processes...

By default when FTP VirusWall is started it will create two child processes to handle the estimated existing traffic load. Depending on your system resources and traffic load levels, you may want to increase the Pre-process Generation number.

Note: There is no maximum allowed value. However, entering too large of a number can result in wasted system resources.

Regenerating idle processes...

InterScan will automatically generate child processes as needed to accommodate traffic spikes. As the spikes taper off, excess child

processes are left idle. You can specify, in seconds, how quickly these idle processes are extinguished in the **Idle time to restart** field.

Choosing the right idle time is important. On the one hand, the accumulation of a lot of idle child processes means system resources are being wasted. On the other hand, existing, idle processes can respond more rapidly to sudden increases in the work load than if a host of new processes must be spawned to accommodate the additional load.

Note: Specifying a value of zero (0) means that idle child processes are never extinguished.

- A typical number **Idle time to restart** value is 3600 seconds, i.e., one hour.
- An **Idle time to restart** value of zero means the number of available processes will always equal your highest usage spikes, no matter how brief or infrequent they may be.
- An **Idle time to restart** value of just a few seconds means InterScan will have to create new processes just about every time there is a change in the work load.

In specifying an **Idle time to restart** value, choose a number that represents a balance between the need to create new processes and the unwanted accumulation of idle processes.

Limiting child processes...

Before creating a new child process, InterScan checks first to see if there are any existing processes that can be used. If there are none, InterScan will create a new one.

Although there is typically no need to limit the number of child processes InterScan can create.(the limits inherent to the operating system are used) you can impose a limit on InterScan if you must define a maximum.

InterScan stops spawning new threads whenever the maximum number of child processes is reached; excess requests are rejected.

Extinguishing old connections...

As a matter of "good housekeeping," InterScan extinguishes child processes after a set number of threads have been generated and destroyed, thus ensuring that idle resources do not inadvertently remain active.

A typical number to enter in this field might be 500, meaning that after 500 threads have been generated and extinguished, the hosting child process itself is extinguished and a new one generated to replace it if necessary (a new child will only be spawned if needed). Setting this number too low can result in needlessly brief cycles.

Note: Enter a zero (0) in this field to disable the maximum number of connections option. The default value is 500.

Limiting active connections...

You can limit the number of active connections that InterScan will spawn from a given child process before creating a new child. A typical maximum is five. Entering too high a number and contribute to system instability.

Rule of thumb

You can derive the optimal number used for **Maximum # of active connections...** from the `OPEN_MAX` parameter of the file `/usr/include/limits.h`

Subtract 15 from the `OPEN_MAX` number and divide by ten to obtain a reliable maximum number of active connections per child process (*whole numbers only*).

$$(\text{OPEN_MAX} - 15) / 10$$

For example, if OPEN_MAX equals 45, subtract 15 and divide by 10. You would then enter the number 3 for the maximum number of active connections per child process.

Get and Put Mode:

You can configure how InterScan behaves when sending (*put*) and receiving (*get*) files via FTP. It is important to know where you have FTP VirusWall installed—on the same machine as the FTP server or a different one.

Get Mode

- **Normal**—This mode is valid regardless of where FTP VirusWall is installed on the same machine the FTP server or a different one. It offers the greatest protection against viruses reaching the server, but is slower than **Local**.
- **Local**—Not valid with **Use user@host**. Specify this mode if FTP VirusWall is installed on the *same* machine as the FTP server. **Local** is the fastest mode, but if used incorrectly (i.e., it is selected but FTP VirusWall and the FTP server are on different machines), *no scanning occurs*.

Put Mode

- **Normal** —*See above*.
- **Thru**—This mode is fastest if you have FTP VirusWall installed on a *different* machine than the FTP server.
- **Local**—Not valid with **Use user@host**. **Local** mode is fastest if you have FTP VirusWall installed on the *same* machine as the FTP server.

Saving the Configuration

- To save the new configuration, click **Apply**.
- To "undo" your unsaved changes click **Restore**.

7 Web VirusWall

Web VirusWall scans HTTP and browser-based FTP file transfers for viruses, malicious Java applets, and ActiveX controls. It also provides a system-wide means of preventing clients from downloading all Java applets and/or executable files to their machines.

Web VirusWall can be installed on the same machine as an existing HTTP proxy, on a dedicated machine (in conjunction with an existing proxy) or as the sole HTTP proxy on the network. In general, we recommend that you install Web VirusWall inside the firewall and (logically) on the Internet side of the proxy. However, most any network configuration can be supported.

Of course, real-time scanning with Web VirusWall provides numerous customizable options:

- Choose whether to have Web VirusWall scan all files or selected file types
- Choose whether to log virus events or issue an automatic notification to the administrator (end-users are kept abreast of viruses and scanning progress from their web browser)
- Choose the action Web VirusWall takes whenever a virus is detected: **Clean**, **Delete**, **Move**, or **Pass**
- Fine-tune Web VirusWall's performance

Enabling or Disabling HTTP Scans

Web VirusWall, like all the VirusWalls, can be **Enabled** or **Disabled** from the **General Configuration** page.

1. In the menu on the left, click **Configuration**, then **General Configuration** from the menu that appears.
2. In the **General Configuration** windows, click the **HTTP Scan** check box:
 - A check in front of **HTTP Scan** indicates that real-time scanning is enabled and traffic scanned
 - No check in front of **HTTP Scan** indicates that real-time scanning is not enabled and traffic is not being scanned

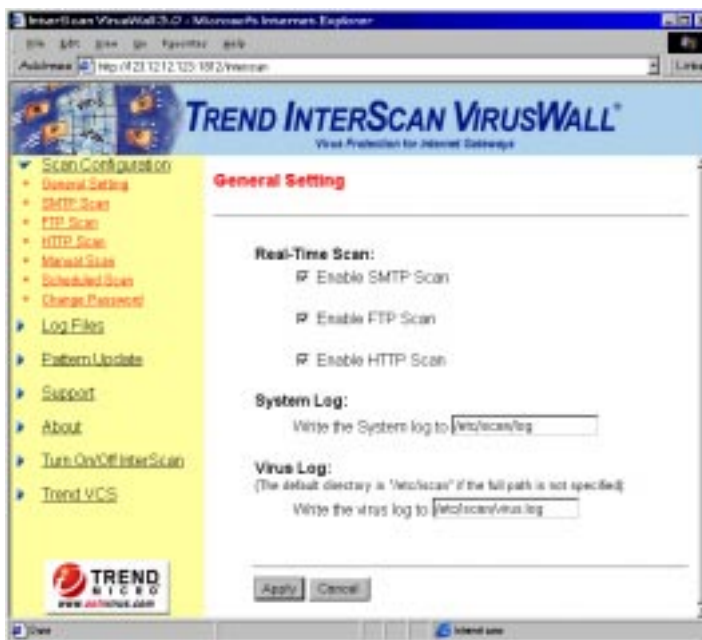


Figure 7-1. You can enable or disable HTTP scanning from the General Settings screen—the flow of traffic is not interrupted. You can also **Turn ON/OFF** the flow of HTTP traffic, also shown above.

Configuring Web Scans

After installing Web VirusWall, you need to configure it to work on your system. In particular, you need to specify the port that client browsers will use to connect to Web VirusWall (typically port 80) and then specify whether Web VirusWall has been installed to act as its own proxy server or work in conjunction with an existing proxy.

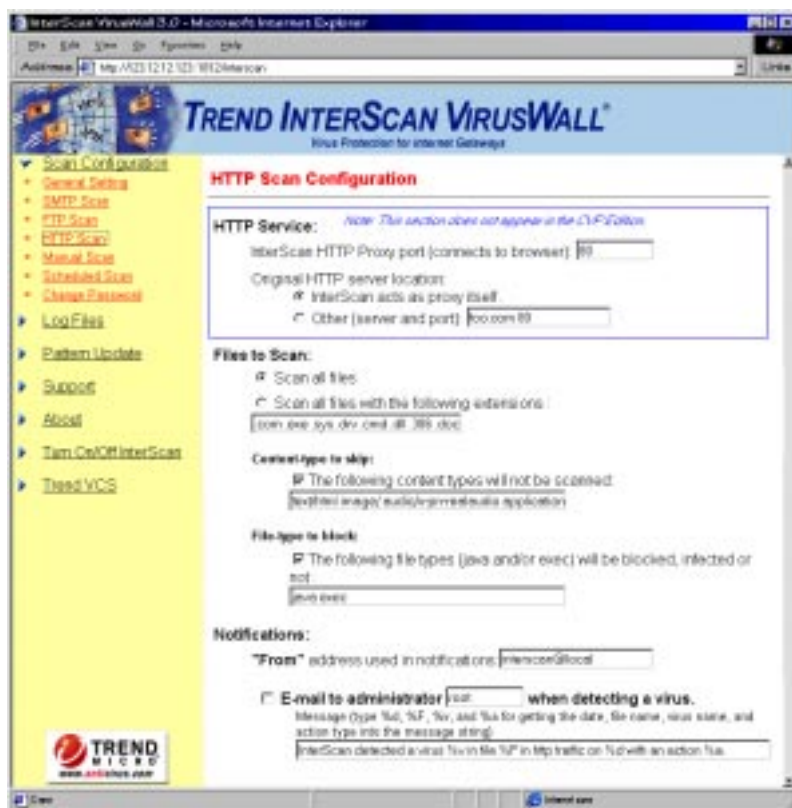


Figure 7-2. Configure Web VirusWall to work with an existing HTTP proxy server or as the sole HTTP proxy on the network.

InterScan *Standard* Edition

Depending on how your system is set up, you need to choose either **InterScan acts as a proxy itself:** or **Original HTTP server location** and specify a port (typically 80) in the **InterScan HTTP Proxy port (connects to browser):** field.

Original HTTP server location

In the **Main service port** field, enter the port Web VirusWall will use to listen for new client connections. Typically, this number is 80. If Web VirusWall and the HTTP proxy are on the same machine, you can change the proxy's port and give Web VirusWall port 80. You also need to choose either **InterScan acts as a proxy itself:** or **Other (Server and port)** and specify a location and port.

InterScan acts as proxy itself:

Choose this option if there is no HTTP proxy on the network and you want Web VirusWall to serve as the system's HTTP proxy, or if you will place Web VirusWall (logically) between the Internet and proxy.

Note: Web VirusWall supports both HTTP and FTP scans.

Other (Server and port)

Choose this option if there is an existing HTTP server on the system and enter the location *and* port of this server. Web VirusWall will scan all HTTP traffic to and from the machine identified in this field.

If the HTTP proxy server and Web VirusWall are on the same machine...

1. In **Other (server and port)**, enter the local path of your HTTP daemon. For example,

```
/usr/sbin/in.httpd
```

2. Note that there is no need to specify a port.

If the HTTP proxy server and Web VirusWall are on different machines...

1. In **Other (server and port)**, enter the domain name or IP address of the machine running the HTTP daemon (`in.httpd`). For example,

```
proxy.yourcompany.com 80  
123.12.13.123 80
```

2. Note that because the proxy is on a different machine, you need to specify a port.

InterScan CVP Edition

For the *CVP* Edition of InterScan, Web VirusWall receives all HTTP traffic from the firewall, scans it, and then returns it to the firewall for routing as usual. Because the firewall handles delivery of HTTP traffic to the HTTP proxy server (if any), no location or port information is required.

Note: A Main Service Port must be defined for use by both InterScan and FireWall-1. Typically, this port is 18181 and is set during installation. You will also need to add InterScan to your FireWall-1 (see Chapter 4 for details).

Specifying Which Files to Scan

InterScan can check all or specified file types for viruses, including the individual files contained in a compressed file.

To select which files to scan,

1. To scan all file types, regardless of extension, click the **Scan all files** radio button. This is the most secure configuration. Compressed files are opened and all files within scanned
2. To scan only selected file types, click the **Files with the following extensions:** radio button. Only those file types that are explicitly specified in the associated text box are scanned.

`.com .exe .sys .doc .xls .zip .dll`

Use this option, for example, to decrease the aggregate number of files InterScan checks, thus decreasing overall scan times. Many files types (e.g., graphics) have never been known to carry viruses.

Note: Zip and other compressed file are only scanned if the file type is specified. Compressed files are opened and all files scanned.

There is no limit to the number or types of files you can specify here. Also, note that no wildcard (*) proceeds the extension, and multiple entries are delimited by a space.

Bypassing Specific MIME Content Types

You can configure Web VirusWall to selectively bypass certain MIME content.

Why? Because, to check a file for viruses, Web VirusWall must act upon the entire file. However some file types, such as RealAudio or

other streaming contents, begin playing as soon as the first part of the file reaches the client machine and will not work properly with Web VirusWall. You can have Web VirusWall omit these file types from scanning. (To date, no viruses have ever been discovered in a streaming protocol, and the format is unlikely to ever be able to support them.)

To select which contents to skip,

1. Click **The following content types will not be scanned:** check box.
2. In the associated text field, enter the content types you want Web VirusWall to skip. Delimit multiple entries with a space.

By default, Web VirusWall is set to skip the following content types:

```
text/html image/ audio/x-pn-realaudio  
application/x-director application/pdf  
multipart
```

Note: Use open entries, such as `image/` above to include all `image` subtypes without having to individually list them.

Security Preferences

Web VirusWall supports the system-wide blocking of *Java* applets and/or executable (*exec*) files. Use this option, for example, if you want to prevent executable files from being downloaded and run on client machines.

Note: Executable files include the following types: `.exe .com .dll`

Zip or other compressed files containing blocked file types are likewise blocked.

How it works:

Web VirusWall checks each non-HTML document to see if it is a Java binary or executable file. If it is, and Java blocking has been enabled, Web VirusWall halts the transfer and instead sends the requesting client browser a notification message.

Note: Known malicious Java and ActiveX files will be detected by the virus scan engine, and the action specified in Action on Viruses taken. This is a different function than the system-wide file blocking described above.

To block certain file types,

1. Click the **The following file types...** check box. A check in the box means the option is enabled.
2. In the associated text field, enter the word `java` and/or `exec` to have Web VirusWall prevent all files of these types from being downloaded onto client machines.

Setting Virus Notifications

Upon detecting a virus in a user's FTP transfer, InterScan can automatically send a customized e-mail to the **Administrator**.

The requesting client is notified from their web browser whenever a file they are downloading is found to be infected with a virus or is blocked due to security concerns (see Security Preferences above).

Note: Clients can receive a real-time progress report whenever they download a file larger than a specified size. See **Progress Reports** for more information.

"From:" field

You can have any e-mail address you want appear in the **"From:"** field of the virus notification message(s) sent by E-mail VirusWall; however, only valid accounts on the local SMTP server will be delivered if users attempt to **Reply to** the notification message.

To notify the administrator,

1. Click the **E-mail to administrator** checkbox.
2. Enter the e-mail address (**root**, for example) in the associated text box. Multiple e-mail addresses are not supported.
3. In the **Message** field, enter the warning message you want the administrator to receive. The following case-sensitive variables can be used in the message:

```
%a = Action taken: Delete, Move, Pass
%d = Date virus was detected
%F = File where virus was detected
%v = Virus name
%M = When Action is Move, displays the
    destination directory
%m = Detection method
%h = Host name
```

For example,

```
Warning! On %d, InterScan detected the
%v virus in the file: %F. InterScan
took the following action: %a.
```

which reads, "Warning! On **6-20-99**, InterScan detected the **Jerusalem** virus in the file: **Word.com**. InterScan took the following action: **delete**."

Note: Verbs, such as *delete* in the example above, are in simple present tense; be sure to structure the grammar of your note accordingly.

Setting the Action on Viruses

You can specify one of four actions for InterScan to take upon finding an infected file:

- Choose **Pass** (and specify a wait-time in minutes) to send infected file, along with a warning message to the client *without cleaning*.

Wait time is used to delete the file from the server X minutes after *starting* to transmit it to the requesting client. Choose a time long enough that the transfer will be completed, but not so long as to risk the infected file spreading from the server.

- Choose **Move** to move, *without cleaning*, the infected attachment to the `/etc/iscan/virus` directory. The requesting client will not receive the file.
- Choose **Delete** to reject the infected file from the server. The requesting client will not receive the file.
- Choose **Auto Clean** to have Web VirusWall automatically clean and process infected files. The requesting client will receive the cleaned file.

If an infected file cannot be cleaned, for example because the virus has corrupted it, Web VirusWall will then take the action specified for **Action on Non-Cleanable Files**:

- Choose **Pass** to ignore the virus and deliver the file to the requesting client.
- Choose **Move** to infected file to the `/etc/iscan/virus` directory.
- Choose **Delete** to reject the infected at the server.

Miscellaneous

Web VirusWall provides several "miscellaneous" options, including

- Trickle, which solves a proxy "time-out" issue that can occur under one setup topology
- Transaction logging, which records all browser requests
- Temp directory location, which allows you to specify any directory for Web VirusWall logs.



Figure 7-3. Web VirusWall configuration screen, continued.

"Trickle": Keeping browser connections alive

If you have Web VirusWall installed so that it is logically between the Internet and HTTP proxy, and if the connection between Web VirusWall and the Internet is slow, clients may encounter "time-out" issues generated by the HTTP proxy server. To solve the problem, Web VirusWall provides the option to "trickle" small amounts of data to the requesting client in advance of transferring the entire scanned file. See **Important Notes** on page 7-10 for more information.

Note: Use **trickle** only if you are currently experiencing the time-out problem described above.

To have Web VirusWall trickle data,

1. Open the **HTTP Scan Configuration** page and scroll to the bottom.
2. Specify the number of bytes you want trickled to the clients. For example,

Send 1024 **bytes** of data to client for every 512 **kilobytes** received

In this example, Web VirusWall will release 1024 bytes of data to the client for each 512 KB it receives. Once the entire file has been downloaded to the Web VirusWall machine and scanned, it is rapidly transferred to the requesting browser.

Note: Disable "trickling" by entering zeros (0) in the text fields.

Important notes regarding "trickle"

- Because **trickle** works by advancing a small portion of data to the clients, it is theoretically possibility that a virus will be among the portion of file transferred to the client. **Note:** The file will not be in a usable form and poses no risk of infection.

- With **trickle** set, files that subsequently turn out to be infected or of a "blocked" type (e.g., Java or executable) will always be deleted, regardless of the Action set; clients are not notified
- When a **trickled** file is subsequently deleted, the portion advanced to the client's hard drive will remain as small, unusable file. Clients should understand that Web VirusWall has not corrupted these files; rather, they have been discarded according to the policy set by the administrator
- Using "trickle" is not supported in conjunctions with **Progress Report** (set from the **Advanced Options** page)
- The predicted download time that clients receive when downloading a file will be grossly over-estimated—the browser calculates this time according to the *trickle* it is receiving; it bears no reflection on the speed at which Web VirusWall is *receiving* the file. In fact, once the file has been scanned, transfer to the client usually only takes a few seconds.

Check here to get log transaction history...

You can have InterScan log "verbose" transaction details, including:

- Sender & Recipient
- Domain of origin
- Destination domain

You can specify where InterScan keeps the transaction log in the General Configuration page.

1. In the left window frame, click **Configuration | General Configuration**.
2. Specify the location where you want InterScan to keep the log in the **Where to write the service log file:** field.

Temporary directory location

InterScan uses the /tmp or whatever other directory you specify to do the work of scanning for viruses.

Note: Specify a directory with at least 300 MB available free space.

HTTP VirusWall Advanced Configurations

To optimize performance, InterScan provides several "Advanced" parameters that you can set to control how many threads InterScan spawns upon start up, how many child processes each thread may spawn, how often the threads are regenerated, and how many simultaneous threads can be supported.

To edit the Advance Options,

1. Open the InterScan console and click **Configuration | HTTP Configuration** in the left hand menu that appears.

2. Scroll to the bottom of the E-mail Scan Configuration page that appears and click the **Advanced...** button.

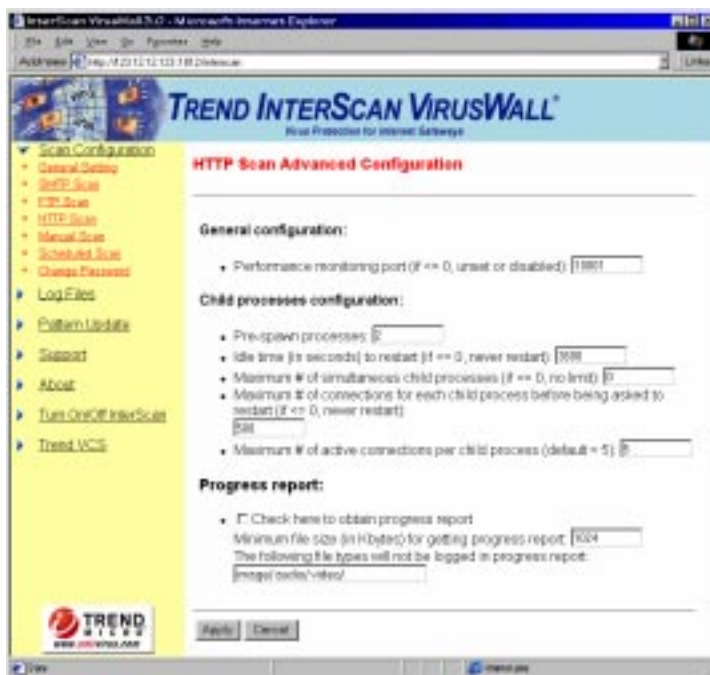


Figure 7-4. You can fine-tune Web VirusWall's performance with the options available in Advance Configuration.

General Configuration

The General Configuration options allow you to set up performance monitoring, have E-mail VirusWall issue a "greeting" whenever a connection is received, and/or keep a running log of all transactions. Each of these options are explained below.

Performance monitoring port...

InterScan supports the use of real-time client monitoring programs for the display of InterScan's performance data. **Perfmon**, one such program, is included with InterScan.

To use **Perfmon** or a similar program, you must enter the port number that the daemon will listen on, for example 10021, 10025, 10080. Any free port can be used, but be sure to use a different port for each service (e-mail, FTP, or HTTP) you intend to monitor.

The monitoring program receives data, in real time, from the daemon using a port that is bound by the daemon. Tracked data values include:

- Total active threads
- Individual PID's (process identification numbers)
- Total connections
- Total idle time
- Total processes created

Note: To disable port monitoring, set this value to zero.

Child Process Configuration

You can fine-tune InterScan's performance by making adjustments to such settings and the number of processes spawned upon startup and the refresh rate of idle processes. In addition, you can limit the total number of child processes InterScan will use at any one time, and the total number of child processes spawned for a given thread.

Note: Improperly adjusting the Advanced settings can result in system instability. We recommend that you use the defaults unless there is a specific performance-based reason to alter them.

Pre-spawn processes...

By default when the InterScan E-mail VirusWall service is started it will create two child processes to handle the estimated existing traffic load. Depending on your system resources and traffic load levels, you may want to increase the Pre-process Generation number.

Note: There is no maximum allowed value. However, entering too large of a number can result in wasted system resources.

Idle time (in seconds) to restart...

InterScan will automatically generate child processes as needed to accommodate increases in the work load. You can specify, in seconds, how quickly these child process will extinguish once the work load has decreased and the processes are left idle.

Choosing the right idle time is important. On the one hand, the accumulation of a lot of idle child processes means system resources are being wasted. On the other hand, existing, idle processes can respond more rapidly to sudden increases in the work load than if a host of new processes must be spawned to accommodate the additional load.

The number entered should be in seconds.

Note: Specifying a value of zero (0) means that idle child processes are never extinguished.

- A typical number **Idle time to restart** value is 3600 seconds, i.e., one hour.
- An **Idle time to restart** value of zero means the number of available processes will always equal your highest usage spikes, no matter how brief or infrequent they may be.
- An **Idle time to restart** value of just a few seconds means InterScan will have to create new processes just about every time there is a change in the work load.

In specifying an **Idle time to restart** value, choose a number that represents a balance between the need to create new processes and the unwanted accumulation of idle processes.

Maximum # of simultaneous child processes...

Before creating a new child process, InterScan checks first to see if there are any existing processes that can be used. If there are none, InterScan will create a new one.

Although there is typically no need to limit the number of child processes InterScan can create.(the limits inherent to the operating system are used) you can impose a limit on InterScan if you must define a maximum.

Whenever the maximum number of child processes is reached, InterScan will stop spawning new threads and instead begin queuing the addition traffic.

Note: The operating system's own limit, if any, will take precedence over the value specified in this field.

Maximum # of connections for each child process before being asked to restart...

As a matter of "good housekeeping," InterScan extinguishes child processes after a set number of threads have been generated and destroyed, thus ensuring that idle resources do not inadvertently remain active.

A typical number to enter in this field might be 500, meaning that after 500 threads have been generated and extinguished, the hosting child process itself is extinguished and a new one generated to replace it. Setting this number too low can result in needlessly brief cycles.

Note: Enter a zero (0) in this field to disable the maximum number of connections option. The default value is 500.

Maximum # of active connections per child process...

You can limit the number of active connections that InterScan will spawn from a given child process before creating a new child or queuing the additional requests. A typical maximum is five. Entering too high a number and contribute to system instability.

Rule of thumb

You can derive the optimal number used for **Maximum # of active connections...** from the `OPEN_MAX` parameter of the file `/usr/include/limits.h`

Subtract 15 from the `OPEN_MAX` number and divide by ten to obtain a reliable maximum number of active connections per child process (*whole numbers only*).

$$(\text{OPEN_MAX} - 15) / 10$$

For example, if `OPEN_MAX` equals 45, subtract 15 and divide by 10. You would then enter the number 3 for the maximum number of active connections per child process.

Progress Report

When HTTP scanning is enabled in Web VirusWall, end-users may experience delays whenever large or multi-compressed files are being checked for viruses and/or malicious Java/ActiveX content.

So that users understand the purpose of this occasional delay, Web VirusWall provides an optional **Progress Report**. As a large file is being downloaded to the requesting browser, the progress of the transaction will be displayed in the user's browser.

To accommodate variations in connection speed, InterScan allows you to set the file-size threshold for which a report is opened. With a T-1 connection, for example, the lag for files of less than 1 or 2 MB is largely unnoticeable and you may want to set the threshold to 2000KB. On the other hand, if your users rely on 28.8 modem connection, you might find 256 or 512KB to be more suitable.

To enable/disable Progress Reports,

1. Click **Check here to obtain progress report**.
2. Enter the minimum file size for which a **Progress Report** window will appear on client desktops in the **Minimum file size...** field.
3. Enter any file types that you do not want a **Progress Report** windows to open for in the **The following file types will not be logged...** field.

For example, you may not want the report window to open if the client is downloading a streaming protocols. In this case, enter the following: image/ audio/ video/

Notes:

- **Progress Report** is only available with Netscape's Navigator version 3.0 or later.

- Do not use **Progress Report** if you are also using "trickle" (described on page 11 of this chapter).
- Progress Report is only available when Web VirusWall is the first proxy in a chain of linked proxy servers.
- If specifying multiple file types in the **The following file types will not be logged...** field, delimit the entries with a space.
- Specify only the root class, for example, `image/` , to include all sub-types of the class as well.

Saving the Configuration

- To save the new configuration, click **Apply**.
- To "undo" your unsaved changes click **Restore**.

8 Manual and Scheduled Scans

In addition to the real-time scanning of files as they travel via e-mail, FTP, and HTTP, InterScan VirusWall allows you to perform manual, or "demand scans" of individual drives or directories. All drives and directory can be scanned so long as it is mounted on the server where InterScan is installed.

You can also schedule scans to take place automatically, at daily, weekly, or monthly intervals.

The following pages provide a step-by-step procedure to use InterScan VirusWall for manual, or on-demand scanning, and prescheduled scans of selected drives or directories. When you specify the root directory (/) and subdirectories, InterScan VirusWall scans the entire local file system and all NFS-mounted drives and directories. Obviously, scanning all drives under root can take require a considerable amount of disk space and take some time.

Note: Because of the transitory nature of files in (/tmp) and (/proc), files that InterScan starts to scan may already be deleted by the system by the time the scan of the file is finished. These files are noted in the logs as read or write errors.

Scanning a Drive or Directory...

In addition to having InterScan scan, in real-time, all network traffic for the SMTP, FTP, and HTTP protocols, you can run a manual scan of all local and mounted fixed disks. In fact, we encourage you to scan all files on the server right after installing InterScan.

Alternatively, you can schedule InterScan to periodically scan the drives using **Scheduled Scan**, described later in the chapter.

To open the Manual Scan Configuration Screen, start the InterScan console and click **Scan Configuration | Manual Scan** from the options menu.



Figure 8-1. Manual Scans allows you to check all or selected directories on the server hard drive (and any mounted drive) for viruses.

To scan a drive or directory,

You can use InterScan to scan individual drives or directories. Simply identify the drive or directory you want scanned, configure the scan options, and click the **Scan Now** button at the bottom of the **Manual Scan Configuration** screen. Details follow:

1. In the **Scan directory** field, type in the local drive or directory you want InterScan to scan. For example,

```
/home/michelle
```

2. Check **Scan all subdirectories** to also include all files and folders below the directory specified above, for example,

```
/home/michelle/files
```

```
/home/michelle/files/docs
```

```
/home/michelle/personal/files/letters
```

To scan all drives and directories,

You can use InterScan to scan all files on all drives, including those both local and mounted. Of course, scanning all files in all drives requires considerable swap space in the `/tmp` directory and can be time consuming.

In addition, because files in the `/tmp` and `/proc` directories are constantly being written and deleted, InterScan may not be able to properly finish scanning some files that it has started. These events are logged as read/write errors in the system log.

1. Scan all files on all drives, enter the `root (/)` in the scan directory field.
2. Click **Scan all subdirectories** if no check appears.
3. Choose either **Scan all files** or **Scan all files with the following file extensions** (details on next page).
4. Make your **Notification** selections (details on next page).

5. Define the **Action on Viruses** you want InterScan to take (details on next page).
6. Finally, click the **Scan Now** button. InterScan will begin scanning the selected drive.

Note: No progress report is piped to the screen; however, a record of the scan results are kept in the log.

To select which files to scan,

1. To scan all file types, regardless of extension, click the **Scan all files** radio button. This is the most secure configuration. Compressed files are opened and all files within scanned
2. To scan only selected file types, click the **Files with the following extensions:** radio button. Only those file types that are explicitly specified in the associated text box are scanned.

`.com .exe .sys .doc .xls .zip .dll`

Use this option, for example, to decrease the aggregate number of files InterScan checks, thus decreasing overall scan times. Many file types (e.g., graphics) have never been known to carry viruses.

Note: Zip and other compressed file are only scanned if the file type is specified. Compressed files are opened and all files scanned.

There is no limit to the number or types of files you can specify here. Also, note that no wildcard (*) proceeds the extension, and multiple entries are delimited by a space.

Setting Virus Notifications

Upon detecting a virus in a use file, InterScan can automatically send a customized e-mail to the **Administrator** and/or **Owner** of the infected file(s).

To notify the administrator, or "owner,"

1. Click the **E-mail to administrator** check box, and/or **Warning** check box, as desired.

For the file owner, the message will be sent as a separate e-mail to that person's UNIX mail account on the machine where InterScan is installed. If there is no Sendmail on that machine, no e-mail will be sent; the event will be recorded in the virus log.

2. For the administrator, enter the e-mail address (**root**, for example) in the associated text box. Multiple e-mail addresses are not supported.
3. In the **Message** field(s), enter the warning message you want the administrator and/or owner to receive. The following case-sensitive variables can be used in the message:

```
%a = Action taken: Clean, Delete, Move
%d = Date virus was detected
%F = File where virus was detected
%v = Virus name
%M = When Action is Move, displays the
    destination directory
%m = Detection method
%h = Host name
```

For example,

```
Warning! On %d, InterScan detected the
%v virus in the file: %F. InterScan
took the following action: %a.
```

which reads, "Warning! On **6-20-99**, InterScan detected the **Jerusalem** virus in the file: **Word.com**. InterScan took the following action: **delete**."

Note: Verbs (e.g., *delete*) are in simple present tense; please structure the grammar of your note accordingly.

Setting the Action InterScan Takes on Viruses

You can specify one of four actions for InterScan to take upon finding an infected file:

- Choose **Pass** to send infected file, along with a warning message to the client *without cleaning*.
- Choose **Move** to move, *without cleaning*, the infected attachment to the `/etc/iscan/virus` directory. The requesting client will not receive the file.
- Choose **Delete** to reject the infected file from the server. The requesting client will not receive the file.
- Choose **Auto Clean** to have Web VirusWall automatically clean and process infected files. The requesting client will receive the cleaned file.

If an infected file cannot be cleaned, for example because the virus has corrupted it, Web VirusWall will **Move** to the infected file to the `move` directory as specified above.

Scheduled Scans

InterScan can be scheduled to automatically scan a specified drive or directory for viruses. The procedure is the same as for **Manual Scans**, presented above, with the additional option of setting the frequency, time and date that the scan should take place.

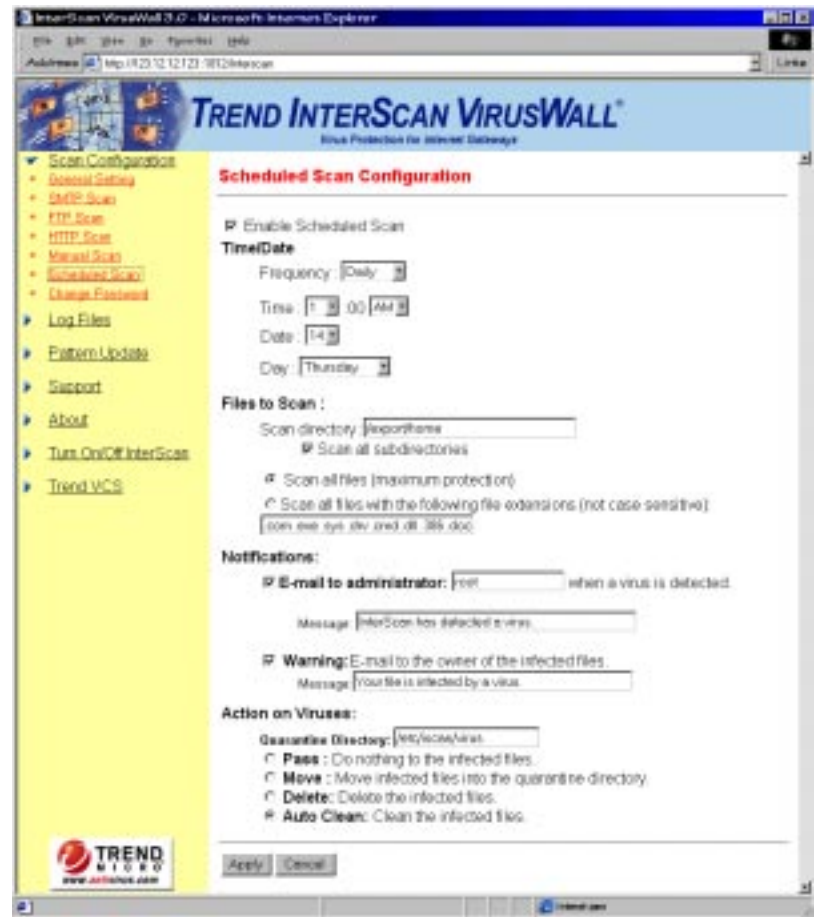


Figure 8-2. You can schedule InterScan to periodically scan selected drives or directories.

Only one directory can be designated for **Scheduled Scans**; most often, this is a shared user's directory.

To enable/disable scheduled scanning,

You need to do three things to set up scheduled scans:

- Check the **Scheduled Scan** option at the top of the **Scheduled Scan Configuration** page
- Schedule the scan frequency
- Specify a drive or directory for scanning

To toggle on/off scheduled scanning, open the InterScan console.

1. Click **Scan Configuration | Scheduled Scan**.
2. If no check appears, click **Enabled Scheduled Scan**.
3. Choose a frequency, either **Daily**, **Weekly**, or **Monthly** from the drop-down list and fill out the other frequency options as appropriate.
4. Specify the drive or directory that you want InterScan to check. All local and mounted volumes are eligible for scans.
5. Choose your file scan, notification, and action options (see **Manual Scan** for details).
6. Click **Apply** to save you settings or **Cancel** to revert to the last saved settings.

Section III

Using InterScan VirusWall



- **Chapter 9**
Virus Pattern Updates, Log Files,
& Registration
- **Chapter 10**
Technical Support & the Virus
Information Center
- **Chapter 11**
Installing & Configuring an Agent
for Trend VCS
- **Chapter 12**
Intscan.ini File Settings

9 Log Files, Virus Pattern Updates, and Registration

InterScan VirusWall can log three levels of detail: default, transactions, and verbose.

- **Default** logging tracks error messages and when a daemon stops or starts
- **Transaction** logging tracks the details of each transaction handled by the VirusWall, for example the URL of the requesting browser and the host site
- **Verbose** logging tracks all program details and should be used only temporarily, and only if problems are encountered. Verbose logging option is set directly in the intscan.ini file; there is no interface support.

By default, the VirusWalls write their logs to the directory `/etc/iscan` and create a new log each day when a virus is found. The logs are named according to the following convention:

`virus.log.1999.06.20`

which can be read as *InterScan Log for June 20, 1999*.

Note: If you use InterScan's Verbose or Transaction logging modes, be sure that you have specified a directory with plenty of disk space, for example 500 or more megabytes.

Specifying the Log Directory

You can have InterScan write its system and virus event logs to any directory you want (but be sure there's plenty of free space).

To specify a different log directory,

1. Click **Configuration | General Settings**.
2. Under the **System Log:** and **Virus Log:** headings, enter the location and file name that you want InterScan to use. The defaults are,

```
/etc/iscan/log  
/etc/iscan/virus.log
```

for the **System** and **Virus** logs respectively. InterScan adds the current date (yyyy.mm.dd) to the name specified.



Figure 9-1. You can specify the location of the System and Virus logs from the General Settings page.

Viewing or Deleting Log Files

InterScan keeps both Virus and System logs, writing a new log for each day. The procedure for viewing and deleting virus logs is given below; the same procedure can be applied to System Logs.

To view virus or system logs,

1. Open a web browser and start the InterScan console, then click **Log Files** in the left browser frame.
2. Click **View Log**. The **View Virus Log** screen appears.
3. Select service whose logs you want to view from the list.
4. Choose the **Date**, **User**, and **Names** that you want to view by clicking the appropriate radio button.

For example, you may want to view virus logs only from the **HTTP scan**, for **All dates**, **All users** (or specify a particular user name), and **All viruses** (or, choose a virus from the list).

5. Click **Apply** to display the logs you have selected, or **Cancel** to revive the last saved settings.

InterScan extracts the data from the virus log files according to your criteria and displays an HTML page with the results. Logs include the following data:

- The **name** of the scanning service that detected the virus
- The **date** and **time** the virus was discovered
- The **name** of the virus
- The **name** and **location** of the infected file
- The originating **domain**, **IP Address**, or **sender**
- The intended **recipient** (for e-mail)
- The **action** taken

Getting details on detected viruses

Virus names that appear in blue are linked to the encyclopedia on www.antivirus.com. Double-click a linked name to learn more.



Figure 9-2. An example system log from InterScan VirusWall.

To delete log files,

InterScan writes a record to the virus log each time it detects a virus and starts a new log each day. You can delete unwanted virus logs individually or *en masse*.

1. Click **Log Files | Virus Log** in the left browser frame, then the **Delete Log** button that appears.
 - To delete all log files, click **Delete all log files**
 - To delete selected log files, click **Delete selected log files** and select those logs you want deleted
2. Click **Apply** to carry out the action or **Cancel** to abort.

Common System Log Messages

- *illegal state transition*, EXIT --> OK, ignored...

This message does not signal a problem; it indicates an occasional, transitory busy state during child process extinction.

- *exec error*: No such file or directory...

This message (accompanied by a failure to deliver mail) occurs in the *Plugin* Edition of E-mail VirusWall if the **-bs** flag has not been remove from the sendmail daemon location.

The Virus Pattern File

To detect viruses, InterScan VirusWall draws upon an extensive database of virus "signatures," commonly called the virus pattern file. As new viruses are written, released onto the public and discovered, Trend Micro collects their tell-tale signatures and incorporates the information into this file. Files follow the following naming format:

`lpt$vpn.###`

where ### stands for the version (e.g., 501). If multiple files exist in the same directory, only the one with the highest number is used.

Trend publishes these new virus pattern files weekly, and we recommend that you do not wait longer than a couple of weeks between updates. Updates are available free to registered InterScan customers and can be automatically downloaded over the Internet.

Note: Only registered users are eligible for virus pattern file updates.

To manually update the virus pattern file,

1. Open a web browser and start the InterScan console, then click **Pattern Update** in the left browser frame.
2. Click **Update Now**. The version of your current pattern file and the occasion of the last update appears.
3. Click the **Update Now** button. If the pattern file available at Trend is more recent than the one on your server, the update will occur.

Note: There is no need to delete the old pattern file or take any special steps to "install" the new one. One click of the **Update Now** button takes care of everything.



Figure 9-3. You can update the virus pattern file with the click of a button or schedule InterScan to perform the operation automatically.

To enable/disable automatic virus pattern updates,

1. Open a web browser and start the InterScan console, then click **Pattern Update** in the left browser frame.
2. Click **Scheduled Update**. The scheduling options appear.
3. Click **No automatic update** to toggle on/off scheduled updating.
4. Choose **Update Weekly** or **Update Monthly** to select your preferred interval and select the time as appropriate.



Figure 9-4. Trend recommends weekly virus pattern file updates.

Using an HTTP Proxy Server

InterScan obtains new virus pattern files from www.antivirus.com. To access the site if there is an HTTP proxy server on the network that is between InterScan and the Internet, you need to identify it and supply the appropriate logon credentials.

Note: If you the Agent for Trend VCS installed, it will use this same proxy information whenever it contacts the Trend VCS server.

If there is no proxy, allow the default setting, **Do not use proxy server for pattern download**, to remain.



Figure 9-5. InterScan will use your proxy server for virus pattern updates, registration, and, if you run Trend VCS, those Agents.

To identify a proxy server,

1. Open a web browser and start the InterScan console, then click **Pattern Update** in the left browser frame.
2. Click **Proxy Server Setting**. The **Proxy Server and Authentication** screen appears.
3. Choose **Use proxy server for pattern download** if you have a proxy server between InterScan and the Internet, then
 - a. enter the domain name (or IP address) of the proxy in the **proxy:** field. For example, `proxy.company.com`
 - b. enter the port the proxy uses in the **port:** field. For example, 80, or 8080.
4. Enter a **User ID** and **Password** for InterScan to use when logging on to the proxy to perform virus pattern uploads.

Registering InterScan

Registering InterScan VirusWall is important and entitles you to the following benefits:

- One year of technical support
- One year virus pattern updates
- Valuable information about program updates and new products

You can register InterScan in a variety of ways:

- Register over the Internet
- Registration by fax
- Registration by mail

Registering Over the Internet

Registering over the Internet is fast and convenient. After registering, click **Apply** to send the data to Trend and start your eligibility for virus pattern files updates and technical support.

Note: If you have a proxy server on the network between InterScan and the Internet, you may need to configure InterScan to recognize it. See [Using a Proxy Server](#) for details.

To register over the Internet,

1. Open the InterScan console & click **Support | Registration**.
2. Type in all the requested information. You need only enter only one serial number for all three VirusWalls.
3. Click **Apply** to send your registration to Trend.

The screenshot shows the 'Product Registration' window of the InterScan VirusWall 3.0 console. On the left is a yellow sidebar with a tree view containing 'System Configuration', 'Log Files', 'Pattern Update', 'Support' (which is expanded to show 'Technical Support', 'Virus Information Center', and 'Registration'), 'About', 'Turn On/Off InterScan', and 'Trend VCS'. The main area is titled 'Product Registration' and contains a form with the following fields: Product (InterScan VirusWall 3.0), Serial No. (with a placeholder for a 12-digit number), First Name (David), Last Name (Greenman), E-Mail Address (dave_greenman@trendmicro.com), Company (Trend Micro Inc.), Office Phone (408 9045342), Office Fax (408 907 2000), Office Address (16011 N. De Anza Blvd., 9th Floor), City (Fremont), State (CA), ZIP Code (94538), and Country (USA). A red asterisk indicates that the Serial No., First Name, Last Name, and E-Mail Address fields are required. At the bottom of the form are 'Apply' and 'Cancel' buttons. The Trend Micro logo is visible in the bottom left corner of the window.

Figure 9-6. Perhaps the most immediate and convenient way to register is using the Internet.

Register by Fax

To fax your registration information, complete the registration form (click **Register** on the **Pattern Update** page) and make a print-out. Fax the print-out to the Trend office nearest you, or the following number:

Fax: (408) 257-2003

Registering by Mail

To register by mail, simply fill out and mail in the Registration Card included in the product package. Allow several weeks for your registration to be processed.

10 Technical Support & the Virus Information Center

Trend Micro, Inc. provides a full year of free technical support for InterScan VirusWall customers world-wide. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

In the United States, Trend representatives can be reached via phone, fax, or e-mail. Our web and e-mail addresses follow:

<http://www.antivirus.com>
support@trendmicro.com

For regional contact information and the specific technical support numbers for all of our regional and world-wide offices, open the InterScan console and click **Support | Technical Support**.

General US phone and fax numbers follow:

Toll free:	800-228-5651 (sales)
Voice:	408-257-1500 (main)
Fax:	408-257-2003

Our US headquarters is located in the heart of Silicon Valley:

Trend Micro, Inc.
10101 N. De Anza Blvd. 4th Floor
Cupertino, CA 95014

Sending Trend Your Viruses

You can e-mail Trend your viruses. More specifically, if you have a file you think is infected with a virus but the scan engine doesn't detect it or can't clean it, we encourage you to send the suspect file to us at the following address:

`virus_doctor@trendmicro.com`

Please include in the message text a brief description of the symptoms you're experiencing. Our team of virus engineers will "dissect" the file to identify and characterize any virus(es) it may contain, and return the cleaned file to you—usually that same day.

Virus Information Center

Comprehensive antivirus information is available over the Internet at our free antivirus center **<http://www.antivirus.com>**.

Use the **Virus Information Center** to find out about:

- Which viruses are currently "in the wild," or active
- Computer virus hoaxes
- A list of computer virus trigger dates
- How to determine if a detection is actually a false alarm
- Trend's Virus Encyclopedia, which includes a comprehensive list of virus names and symptoms for known viruses
- A basic guide to computer viruses
- Trend's virus reading room, with dozens of articles about the latest issues in computer viruses, including the threat posed by Java applets and ActiveX controls
- Product details and white papers

To access the Virus Information Center from the InterScan console,

1. Open the InterScan console in a web browser
2. Click **Support | Virus Information Center**. You'll be connected to Trend's award winning web site, www.antivirus.com.



Figure 10-1. A multitude of virus and product information is available at Trend's award winning Virus Information Center.

Free Client Scans with HouseCall



Of particular interest is HouseCall, Trend's free virus scanning service available to one and all. In 1997, Trend pioneered the concept of online scanning with a technology so hot that it remains the *only* service available to all web users. There is nothing to install; users just follow the on screen instructions to scan their hard drives.

HouseCall is also a real-life demonstration of the power of the web-based technologies that Trend is developing to make deployment and management of virus protection in corporate settings fast and easy.

It is important to note that while HouseCall will detect and clean any viruses found on the user's hard drive, it does not provide real-time protection. Use your InterScan VirusWall for that.

House Calls requires Internet Explorer 3.x or later or Netscape's Navigator 3.01 or later. Links to either browser are provided.

To use HouseCall,

1. Open a web browser and enter the following URL:
`http://www.antivirus.com`
2. Click the HouseCall icon that appears. A directory tree of your hard drive will be created, and the offer to perform a free scan presented.

About Computer Viruses

Simply put, a computer virus is a program that replicates. To do so, the virus will need to attach itself to other program files (for example, *.exe*, *.com*, *.dll*) and execute whenever the host program executes. Beyond simple replication, a virus almost always seeks to fulfill another purpose: to cause damage.

Called the damage routine, or payload, the destructive portion of a virus can range from overwriting the partition table on the main system disk to scrambling the numbers in your corporate spreadsheets to just taunting you with sounds, pictures, or effects.

It's worth bearing in mind, however, that even without a "damage routine," left unabated, viruses will continue to propagate—consuming system memory, disk space, slowing network traffic and generally degrading performance. Often buggy, virus code can also be the source of mysterious system problems that take weeks to understand. Whether it was written to be harmful or not, a virus on your system can lead to instability and should not be allowed to remain.

Some viruses, in conjunction with "logic bombs," do not make their presence known for months. Instead of causing damage right away, these viruses do nothing but replicate—until the preordained trigger day or event when they unleash their damage routines across the network.

Types of Viruses

Thousands of viruses are known to exist with more being created each day. Although most common in DOS, computer viruses also exist in Windows 95, Windows 98, OS/2, and System7 environments as well.

- Computer viruses can be roughly classified into the following categories:
- Macro Viruses

- File viruses
- Boot viruses
- Multi-partite viruses
- Mutation, or polymorphic, viruses

Macro viruses

Macro viruses are perhaps the newest type of virus. The first macro virus, written in Microsoft's Word macro language, was discovered in August, 1995. Currently, several hundred macro viruses are known to exist and include viruses written in the macro scripts of Microsoft Excel and Word, Lotus applications, and others.

Macro viruses can spread quickly and over a wide area via e-mail attachments. Since a macro virus is written in the language of an application, not an OS, it is platform independent. Macro viruses can be spread to any machine that runs the application the virus was written in. Any machine running Word, for example, whether it's a PC, Mac, or something else, is vulnerable to Word documents that contain a Macro virus.

Note: To address the special threat of Macro viruses, Trend has developed a new MacroTrap™, as discussed in Chapter 1.

File Viruses

File viruses attach themselves to executable files and are at least partially activated whenever the host file is run. File viruses are typically *TSR*, (terminate-and-stay-resident), *direct action* or *companion* programs.

TSR viruses, which are among the most common of viruses, reside in memory and attach themselves to executable programs that are run. TSR viruses then spread to other programs on the hard drive, floppies, diskettes, or network.

A ***direct action virus*** loads itself in to memory to infect other files and then unloads itself, while a ***companion virus*** acts to fool an executable file into executing from a `.com` file. For example, a companion virus might create a hidden `pgm.com` file so that when the `pgm` program is run, what happens first is that the fake `pgm.com` is executed. This file invokes its virus code before going on to start the real `pgm.exe` file.

Boot Viruses

Boot sector viruses, the most common type of virus, move or overwrite a disk's original boot sector data and replace it with the infected boot code of their own design. Floppies and hard drives are the most susceptible to being overwritten by a boot sector virus. Then, whenever the infected system (boots up), the virus loads into memory where it can gain control over basic hardware operations. Of course a boot virus can also quickly spread to any of the other drives in the system (floppy, network, etc.).

Multi-partite Viruses

Multi-partite viruses share many of the characteristics of boot sector viruses and file viruses. They can infect `.com` files, `.exe` files, and the boot sector of the computer's hard drive.

On a computer booted up with an infected diskette, the typical multi-partite virus will first make itself resident in memory, then infect the boot sector of the hard drive. From there the virus can easily infect a PC's entire environment.

Not many forms of this virus class actually exist. However they do account for a disproportionately large percentage of all infections.

Polymorphic, or Mutation Viruses

Polymorphic (mutation) viruses are unique in that they try to elude detection by changing their structure after each execution— with some polymorphic viruses, millions of permutations are possible. Of

course, this makes it harder for normal antivirus programs to detect or intercept them. It should be noted that polymorphic viruses do not, strictly speaking, constitute a new category of virus; they usually belong to one of the categories described above.

Virus Writers

In the typical scenario, it is an individual, working alone, who writes a virus program and then introduces it onto a single computer, network server, or the Internet. Why? Ego, revenge, sabotage, and basic disgruntlement have all been cited as motivations. Whatever the reason, the important thing is to make certain your company is not victimized, that your data is safe, and time is not lost tracking down and then cleaning up after a virus.

How Viruses Spread

There are many ways for a virus to enter your system:

- E-mail attachments
- World Wide Web (WWW) sites
- FTP traffic from the Internet (file downloads)
- Shared network files & network traffic in general
- Demonstration software
- Pirated software
- Computer labs
- Electronic bulletin boards (BBS)
- Diskette swapping (using other people's diskettes for carrying data and programs back and forth)

The most likely virus entry points are Internet and network connections, floppy disk drives, and modems or other serial or parallel port connections. In today's increasingly interconnected workplace (Internet, intranet, shared drives, removable drives, and

e-mail), virus outbreaks now can spread faster and wider than ever before.

Methods of Virus Detection

Three main methods exist for detecting viruses: integrity checking, (also known as checksumming) behavior monitoring, and scanning. The InterScan VirusWalls are scanning based, with E-mail VirusWall further buttressed by Trend's MacroTrap™. A short description of each of the methods follows:

Integrity checking antivirus programs begin by building an initial record of the status (size, time, date, etc.) of every application file on the hard drive. Using this data, checksumming programs then monitor the files to see if changes have been made. If the status changes, the integrity checker warns the user of a possible virus.

This methods has several disadvantages, however, the biggest being that false alarms are altogether too common. The records used by checksumming programs are often rendered obsolete by legitimate programs, which, in their normal course of operations, make changes to files that appear to the Integrity checker to be virus activity. Another weakness is that these programs can only alert the user *after* a virus has infected the system.

Behavior Monitoring programs are usually TSR and constantly monitor requests that are passed to the interrupt table. These programs are on the lookout for the type of activity a virus might engage in—requests to write to a boot sector, opening an executable program for writing, or placing itself resident in memory. The behavior these programs monitor is derived from a user-configurable set of rules.

"Rule-based" virus traps have one a strong advantage: they can prevent any kind of malicious program from damaging your system including viruses, Trojan Horses and Logic bombs. But they also have a significant disadvantage: these programs are unable to identify or clean the virus or rid your system of the threat. To identify

a virus and eliminate it from the system, only a virus scanner will work.

Scanning: Virus scanning programs rely on a virus pattern file for detecting and locating viruses. Key areas of suspect files are examined for tell-tale virus code and compared against the virus pattern file. For polymorphic viruses, the scanning engine permits suspicious files to execute in a temporary environment. To detect macro viruses in e-mail attachments, Trend provides a MacroTraptm, which employs a rules-based, line-by-line examination of all macro code that is saved in association with a document. When suspicious code is identified, it is removed and both the e-mail sender and recipient can be notified of the action.

11 Trend Virus Control System

Trend VCS is a centralized management console for coordinating, tracking, and maintaining the variety of antivirus software products often installed on a network—regardless of platform or physical location.

InterScan 3.0 is fully compatible with Trend VCS. What this means is that you can simultaneously configure multiple copies of InterScan using Trend VCS, and administer InterScan along with your other Trend antivirus products from a common Trend VCS console.

Other advantages of running InterScan with the Trend VCS include:

- Aggregate log files for enterprise-wide virus statistics
- Centralized virus pattern file updates
- Uniform configuration standards
- Simultaneous configuration changes
- Platform independence

To set up InterScan to work with Trend VCS, you need to install an "Agent" that will handle communication between InterScan and the Trend VCS. This Agent can be "pushed" from the Trend VCS server or installed from the InterScan machine. To run the installation from the InterScan machine, contact the Trend VCS administrator for the

URL and password, if any, of the Trend VCS server. You can download InterScan's Agent program (TVCSAgentSetup.exe) from the Trend VCS console by clicking **Agent Setup** in the blue button bar. Another alternative is to receive the program via e-mail. While installing, you will be prompted for the IP address of the Trend VCS server.

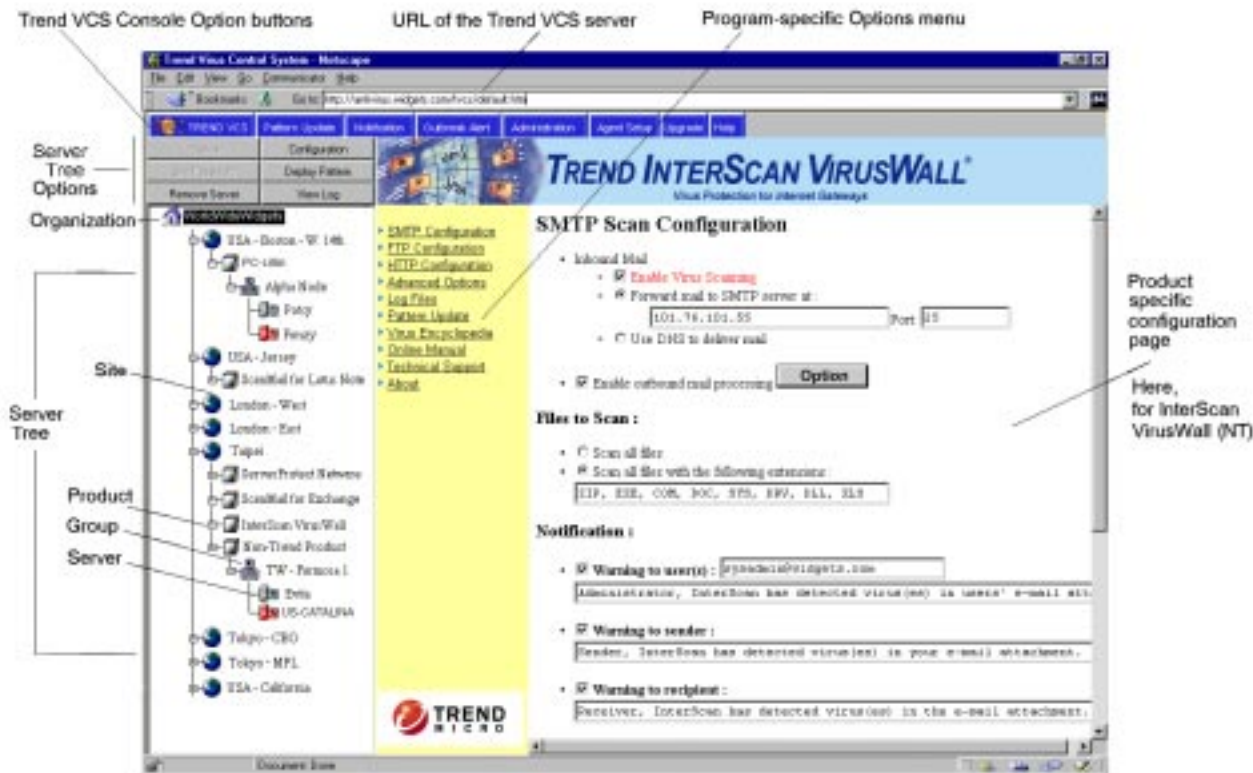


Figure 11-1. InterScan VirusWall (here, for the NT platform), as seen from a Trend VCS console. Most antivirus products installed on the LAN or WAN can be managed via Trend VCS, obviating the usual limitations of product platform and physical location.

Once the Agent has been installed, you can access InterScan (and all other Trend VCS-registered programs) in the Trend VCS console via

web browser by entering the URL and the Trend VCS password. From the Trend VCS console, InterScan can be administered in conjunction with all other antivirus products on the network.

Possible management schemes include:

- Have one administrator manage all antivirus programs, including InterScan
- Designate one administrator for all copies of InterScan installed on the LAN or WAN
- Assign InterScan to the local node administrator of the LAN where it resides

Of course, InterScan can also be administered locally, from the machine where it was installed. Installing an Agent and registering it with a Trend VCS server does not alter local operations in any way.

Installing the Trend VCS Agent

Trend VCS is a separate program that, if installed on the LAN or WAN, allows you to synchronize the configuration (and event logs) of multiple instances of InterScan and/or other programs. See Chapter 1 for more information. If you use Trend VCS on the network and want to administer InterScan VirusWall through it, please read the following section. Otherwise, jump to the section titled *Opening the InterScan Console*.

To use InterScan in conjunction with Trend VCS, you need to install a special Agent on the InterScan machine. This Agent will handle all communication between InterScan and the Trend VCS server and is installed on the InterScan machine in a two-part process:

1. Installing the Agent package.
2. Configuring the Agent to communicate with the Trend VCS server.

To install the Agent package,

You can install the Trend VCS Agent during the initial install, or at any time later. The instructions below assume the latter.

1. From the InterScan machine, locate the directory containing the InterScan installation files and type **./isinst**.
2. In the **Main Menu** that appears, choose **Option 1**.
3. Install the InterScan Agent only if you have already installed the Base System, the CGI Admin package (both are installed by default), and at least one VirusWall. The status of installed packages will read "YES". The TVCS option will read "NO".

Note: The following list shows the *Standard* and *Plugin* options; a CVP installation will appear slightly different.

```
InterScan VirusWall 3
Setup Script
Install InterScan Base System-----[ YES ]
Installation Path /opt/trend/ISBASE
Install InterScan CGI Admin -----[ YES ]
Installation Path /opt/trend/ISADMIN
Install InterScan for FTP -----[ YES ]
Installation Path /opt/trend/ISFTP
Install InterScan for HTTP -----[ YES ]
Installation Path /opt/trend/ISHTTP
Install InterScan for SMTP -----[ YES ]
Installation Path /opt/trend/ISSMTP
Install TVCS Agent for InterScan -----[ NO  ]
Installation Path    /opt/trend/ISTVCS
```

1. Modify option for BASE.
 2. Modify option for ADMIN.
 3. Modify option for FTP.
 4. Modify option for HTTP.
 5. Modify option for SMTP.
 6. Modify option for TVCS.
 7. Start installation.
 8. Back to Main Menu.
- Select a number [6]

4. Choose **Option 6**, and toggle the install option to "YES".
5. Follow the on-screen instructions to complete the setup.

After installing the Trend VCS Agent, you need to configure it to communicate with the Trend server, as explained next.

Configuring the Trend VCS Agent

After installing the Agent, you need to configure it to communicate with your Trend VCS server., or, in other words, *register* the Agent with the Trend VCS.

Note: If multiple Trend VCS servers are installed, for example on a WAN, the Agent can only be registered with one server.

Know in advance:

To register the InterScan Agent, you will need to know the following:

- Hostname or IP address of the Trend VCS server
- The port the Trend VCS server uses to communicate with Agents (typically 80)
- The Site, if one already exists, under which you want to the InterScan Agent to appear (Sites are often geographic names. If you want the InterScan Agent to appear under the same Site as other Agents from your LAN, find out from the Trend VCS administrator which Site to specify.) Otherwise, you can enter any name and the InterScan Agent will appear under it in the Trend VCS server tree. See figure 9-1 for an example.
- An administrator-level Windows NT account name and password for logging on to the Trend VCS server (an NT machine)
- The hostname and IP address of the local InterScan server

To configure the Agent to run with Trend VCS,

1. Open the InterScan console in web browser (<http://hostname:1812/interscan>) and then click **Trend VCS | Registration** from the list of options in the left browser frame.

If you use a proxy server...

2. If you have a proxy server on the network, InterScan will automatically use the **Proxy Server Settings** specified for **Pattern Updates** (explained in Chapter 9 and shown below).



Figure 11-2. The InterScan Agent will use the proxy server (if any) configured for Pattern Updates, when communicating with the Trend VCS server.

- ♦ If there is a proxy server on the network between InterScan and the Internet, choose **Yes** for **Use Proxy**.
- ♦ If there is no proxy between InterScan and the Internet, choose **No** for **Use Proxy**.

Identifying the Trend VCS server

3. Enter the domain name (or IP address) of the machine where the Trend VCS server is installed.

The screenshot shows the 'Trend VCS Registration' window within the InterScan VirusWall 3.0 interface. The window has a yellow sidebar on the left with a tree view containing items like Scan Configuration, Log Files, Pattern Update, Support, About, Turn On/Off InterScan, and Trend VCS (which is expanded to show Registration and Uninstall). The main content area is titled 'Trend VCS Registration' and contains the following fields:

- Use Proxy:** A radio button selection with 'YES' selected and 'NO' unselected. A note below says: '(Please choose Pattern Update to configure the Proxy server.)'
- Trend VCS Server:**
 - TVCS Server:** A text box containing 'CentralControl'.
 - Server Port:** A text box containing '80'.
 - Site Name:** A text box containing 'SR-HCHUD'.
- Trend VCS Server Authentication:**
 - User ID:** A text box containing 'administrator'.
 - Password:** A text box with masked characters.
- InterScan Server:**
 - Server Name:** A text box containing 'Solomon Server Server'.
 - IP Address:** A text box containing '223.12.12.123'.

At the bottom of the form are 'Apply' and 'Cancel' buttons. The Trend Micro logo is visible in the bottom left corner of the window.

Figure 11-3. Trend VCS users can install an Agent for InterScan. The Agent needs to be configured to recognize the Trend VCS server, as shown here.

4. Enter the port that the Trend VCS server uses. This port, although usually 80, could be set on the Trend VCS side to

any free port. Be sure the value you enter here matches the one your Trend VCS server is currently using.

5. Specify the Site name that you want the Agent for InterScan to appear under (see Chapter 1, figure 1-3 for an example).

Server Authentication

6. Enter the Trend VCS User ID and password that is required to access the server. By default, both values are TVCS, however the administrator will typically change them soon after setting up the Trend VCS server.

InterScan Server

7. Finally, verify the name and IP address (not domain name) of the server where you have InterScan VirusWall 3 for Solaris installed. The Trend VCS server uses this address when contacting the Agent, for example when distributing the latest virus pattern update.

12 Intscan.ini File Settings

This chapter contains a listing of the InterScan configuration options in the approximate order in which they appear in the `intscan.ini` file (found in the InterScan directory, for example `/etc/iscan/intscan.ini`). Along with a listing of the parameters, an explanation of each parameter, its default value, a listing of any other possible values, and an explanation of the possible values are provided.

Note: *Certain **intscan.ini** values should never be changed directly because they are derived from, or dependent upon, corresponding values. Changing these values, independent of their related contexts can result in invalid configurations and unexpected results.*

We recommend that you only make configurational changes to InterScan using the console -- open a web browser and enter the InterScan URL, for example:
`http://hostname:1812/interscan`. We do *not* endorse editing `intscan.ini` directly because many values are interdependent. But if you must, be sure to make a back up copy first!

Restricting access to the configuration file

To restrict access to the `intscan.ini` file to only those with root privileges, type the following lines:

```
chown root /etc/iscan/intscan.ini
chmod 600 /etc/iscan/intscan.ini
```

where `/etc/iscan` is the directory where InterScan is installed.

[Scan-Configuration]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
httpscan	toggle on/off real-time HTTP scanning	yes	yes no	yes: scanning is on no: scanning is off
ftpscan	toggle on/off real-time FTP scanning	yes	yes no	yes: scanning is on no: scanning is off
mailscan	toggle on/off real-time SMTP scanning	yes	yes no	yes: scanning is on no: scanning is off
periodicscan	toggle on/off automatic scans of the hard drive	yes	yes no	yes: scheduled scanning is on no: scheduled scanning is off
update	identifies method of pattern file update	auto	signal auto disabled	update using SIGHUP update using "update_interval" update manually
update_interval	download interval when update is set to auto	1440	integer, minutes	1440 (daily) 10080 (weekly)
virus_log	location of virus log file	/etc/iscan/ virus.log. date	any valid directory	virus.log.1999.04.15 date appended to name
pattern_path	location of virus pattern file	/etc/iscan	any valid directory	example: lpt\$vpn.502 (pattern number varies)

[Notification]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
server	SMTP host used for virus notifications	local-host	blank; hostname; IP number	blank= localhost; hostname or IP can be local or remote server
port	SMTP port number	25	integer	blank=25 or specify other

[HTTP]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
mon_port	port for InterScan performance data	10001	port number	blank, zero=disabled; any free port
idle_kill	terminate unused child processes	3600	integer	blank, zero=disabled 900=15min;3600=1hr
max_proc	maximum simultaneous child processes	0	integer	blank, zero=unlimited
proc_max_reqs	restart child processes upon reaching	500	integer	blank, zero=disabled
thr_per_proc	max. active connections per child process	5	integer	typically five or fewer, depends on resources
pre_spawn	available processes upon system start-up.	2	integer	typically two, depends on system resources
svcport	main service port	80	port number	typically 80 or 8080, depends on setup
logfile	InterScan writes it's service logfile here	etc/iscan/log.dat e	any valid directory and file-name	i.e., /etc/iscan/ virus.log.1999.04.15

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
self_proxy	Tells InterScan whether to act as its own proxy.	yes	yes no	InterScan acting as it's own proxy is fastest
original	The location of the original proxy server, when <i>self_proxy=no</i>	foo.com 80	IP address space port #	if blank, InterScan is own proxy (fastest) not valid if self-proxy=yes
skiptype	The listed MIME types are not scanned	text/html image/	MIME type	The listed MIME types are not scanned; add MIME types you do not want scanned
block_types	HTTP replies of these types are blocked, infected or not	java exec	java exec	java applications executables (.com, .exe, etc.)
move_types	HTTP replies of these types are moved to /etc (or specified movedir=), infected or not	blank	java exec	java applications executables (.com, .exe, etc.) User does not get file
warn_types	HTTP users are warned (as per notify_admin) when downloading files of these types.	blank	java exec	java applications executables (.com, .exe, etc.) File is downloaded
level	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
extensions	Scan files with the specified extensions: (<i>level</i> must be set to specific extension)		.com .exe .sys .drv .cmd .dll .386 .doc	include any or all the possible values

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
progress_report	Show progress report when downloading files?	yes	yes no	InterScan gives progress report for http and ftp downloads No progress report
no_progress_size	If <i>progress_report</i> is yes, do not show progress report for files smaller than...	1024	numeric, as high as 2000+	In kilobytes, the min. file size to show prog. rpt. The faster the network, the larger the number
no_progress_type	Do not show progress reports for the listed types	image/	any MIME file type	/image includes all <i>image</i> subtypes
action	What InterScan should do with infected files	delete	pass delete move	pass infected file to user block infected files move infected files
movedir	Specify the directory that InterScan should move infected files to	/tmp	any valid directory and file-name	directory where infected files are stored when <i>action=move</i>
passwait	How long InterScan waits for the user to retrieve a virus if action is set to <i>pass</i>	2	0 - 10	in minutes; any number is valid, but there is no need to exceed several minutes
notify_admin	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin is not notified
admin_addr	Where InterScan sends the notification	root	e-mail address	Typically, the Sys Admin's e-mail address

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
admin_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See explanation	any text variables: %F %d %v %a	"InterScan has detected a virus in the http traffic" parse file name parse date parse virus name parse action taken
passive_ftp	InterScan can use passive mode for communication with remote FTP server	no	yes no	Choose yes when self_proxy =yes and FTP URL is requested.

[FTP]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
mon_port	The port number where InterScan's FTP performance data can be obtained	10011	blank; any free port	a value of zero or less disables performance monitoring
addtl_cmd	remote authentication for ftp servers	none	auth response	firewall's authentication support
idle_kill	Number of seconds after which idle child processes are stopped and restarted	3600	numeric, seconds	a value of zero or less disables this feature (idle sons are never terminated).
max_proc	Maximum number of simultaneous child processes	0	numeric, no limit	a value of zero or less disables this feature
proc_max_reqs	InterScan will restart child processes after this number of connections is reached.	500	numeric, no limit	a value of zero or less disables this feature
thr_per_proc	Maximum number of active connections per child process	5	numeric	Usually less than 10
pre_spawn	Number of processes available on system start-up.	2	numeric	Usually less than 6
svcport	Main service port	21	numeric	This number is usually 21 for FTP
logfile	InterScan writes it's service logfile here	etc/isca n/log.dat e	any valid directory and file-name	i.e., /etc/iscan/ virus.log.1999.04.15

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
self_proxy		yes	yes no	If yes, InterScan uses dynamic mode; users must log in using user@host
original	The location of the original proxy server	/usr/sbin /in.ftpd	blank	if blank, InterScan is own proxy (fastest); path to the ftpd service
block_types	HTTP replies of these types are blocked, infected or not	java exec	java exec	java applications executables (.com, .exe, etc.)
move_types	HTTP replies of these types are moved to /etc (or specified movedir=), infected or not	blank	java exec	java applications executables (.com, .exe, etc.) User does not get file
warn_types	HTTP users are warned (as per notify_admin) when downloading files of these types.	blank	java exec	java applications executables (.com, .exe, etc.) File is downloaded
level	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
extensions	Scan files with the specified extensions: (level must be set to specific extension)		.com .exe .sys .drv .cmd .dll .386 .doc	include any or all the possible values
action	What InterScan should do with infected files	delete	pass delete move	pass infected file to user block infected files move infected files

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
movedir	InterScan <i>moves</i> infected files to this directory	/tmp	any valid directory and file-name	directory where infected files are placed when <i>action=move</i>
greeting	Indicate whether InterScan sends a greeting when connection is established	yes	yes no	The greeting is "220 - InterScan 2.0... Ready." The greeting message is not user configurable
getmode	InterScan's behavior while receiving FTP files	normal	normal local	Universal Mode Same machine, fastest. (see chapter 5)
putmode	InterScan's behavior while sending FTP files (see Chapter 5)	normal	normal thru local	Universal Mode different machine, fast same machine
notify_admin	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin is not notified
admin_addr	Where InterScan sends the notification	root	e-mail address	for example, <i>root</i> or <i>swenson@trend.com</i>
admin_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"InterScan has detected a virus in the ftp traffic" parse file name parse date parse virus name parse action taken
notify_user	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
user_msg	<p>What InterScan's virus alert message to Sys. Admin. says</p> <p>See Section II of this Admin. Guide for further parsing options</p>	See Value explanations	<p>any text variables:</p> <p>%F %d %v %a</p>	<p>"InterScan has detected a virus in the ftp traffic"</p> <p>parse file name parse date parse virus name parse action taken</p>

[SMTP]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
mon_port	The port number where InterScan's SMTP performance data can be obtained	10021	blank; any free port	a value of zero or less disables performance monitoring
idle_kill	Number of seconds after which idle child processes are stopped and restarted	3600	numeric, seconds	a value of zero or less disables this feature (idle sons are never terminated)
max_proc	Maximum number of simultaneous child processes	0	numeric, no limit	a value of zero or less disables this feature
proc_max_reqs	InterScan will restart child processes after this number of connections is reached.	500	numeric, no limit	a value of zero or less disables this feature; processes are never restarted.
thr_per_proc	Maximum number of active connections per child process	5	numeric	Usually less than 10
pre_spawn	Number of processes available on system start-up.	2	numeric	Usually less than 4
svcport	Main service port	25	numeric	This number is usually 25 for SMTP
logfile	InterScan writes it's service logfile here	etc/iscan/log.dat	any valid directory and file-name	i.e., /etc/iscan/virus.log.1999.04.15
original	Location (host port or command argument) of SMTP server	/usr/lib/send-mail -bs		This value must be defined

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
block_types	HTTP replies of these types are blocked, infected or not	java exec	java exec	java applications executables (.com, .exe, etc.)
move_types	HTTP replies of these types are moved to /etc (or specified movedir=), infected or not	blank	java exec	java applications executables (.com, .exe, etc.) User does not get file
warn_types	HTTP users are warned (as per notify_admin) when downloading files of these types.	blank	java exec	java applications executables (.com, .exe, etc.) File is downloaded
level	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
extensions	Scan files with the specified extensions: (<i>level</i> must be set to specific extension)		.com .exe .sys .drv .cmd .dll .386 .doc	include any or all the possible values
action	What InterScan should do with infected files	delete	pass delete move	pass infected file to user block infected files move infected files
movedir	InterScan <i>moves</i> infected files to this directory	/tmp	any valid directory and file-name	directory where infected files are placed when <i>action=move</i>
greeting	Indicate whether InterScan sends a greeting when connection is established	yes	yes no	The greeting is "220 - InterScan 2.0... Ready." The greeting message is not user configurable

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
addtl_message	Additional message to include to recipient if a virus is found in the e-mail	see Value explanations	any	"If you have questions, contact Sys. Admin."
notify_admin	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin is not notified
admin_addr	Where InterScan sends the notification	root	e-mail address	For example, <i>root</i> , or <i>swenson@trend.com</i>
admin_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"InterScan has detected a virus in mail traffic" parse file name parse date parse virus name parse action taken
notify_user	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
user_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"InterScan has detected a virus in your e-mail" parse file name parse date parse virus name parse action taken
notify_sender	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
sender_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"InterScan has detected a virus in your e-mail" parse file parse date parse virus name parse action taken
safe_stamp	InterScan can notify recipient that mail was scanned and no virus was found	no	yes no	include safe stamp do not include safe stamp
safe_message	Message text of the Safe Stamp	none	any text %F	Message recipients receive when no viruses are found in their e-mail. parse file name
log_trans	InterScan can keep a log of e-mail transactions	yes	yes no	keep a log do not keep a log

[Periodical-Scan]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
Frequency	frequency of automatic virus scans	Daily	daily none weekly monthly	scan selected dirs daily do not scan (disable) scan weekly scan monthly
DayOfWeek1	day to download new virus pattern file	Thursday	Monday through Sunday	only valid when <i>frequency=weekly</i>
DayOfMonth	date to download new virus pattern file	14	1 through 31	only valid when <i>frequency=monthly</i>
hour	start time of scheduled scan	1	1 through 12	
APM	day or night start time	AM	AM PM	not case sensitive (but no periods or spaces)
level	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
extensions	Scan files with the specified extensions: (<i>level</i> must be set to specific extension)		.com .exe .sys .drv .cmd .dll .386 .doc	include any or all the possible values
dir	InterScan writes it's Manual scan log file here	/export/ home	any valid directory and file-name	
recursive	Scan all sub-directories under target directory	yes	yes no	scans files in sub-dirs. only files in dir. scanned
notify_admin	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin not notified

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
admin_addr	Where InterScan sends the notification	root	e-mail address	Typically, the Sys Admin's e-mail address
admin_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"Manual Scan has detected a virus." parse file parse date parse virus name parse action taken
user_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"Your file is infected by a virus" parse file name parse date parse virus name parse action taken
notify_user	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
action	What InterScan should do with infected files	delete	pass delete move	pass infected file to user block infected files move infected files
movedir	InterScan <i>moves</i> infected files to this directory	/etc/isca n/virus	any valid directory and file-name	directory where infected files are placed when <i>action=move</i>

[Manual-Scan]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
level	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
dir	InterScan writes it's Manual scan log file here	/export/ home	any valid directory and file-name	
recursive	Scan all sub-directories under target directory	yes	yes	must scan all sub-dirs.
extensions	Scan files with the specified extensions: (<i>level</i> must be set to specific extension)		.com .exe .sys .drv .cmd .dll .386 .doc	include any or all the possible values
notify_admin	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin is not notified
admin_addr	Where InterScan sends the notification	root	e-mail address	Typically, the Sys Admin's e-mail address
admin_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"Manual Scan has detected a virus." parse file parse date parse virus name parse action taken

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
user_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"Your file is infected by a virus" parse file name parse date parse virus name parse action taken
notify_user	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
notify_sender	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
sender_msg	What InterScan's virus alert message to Sys. Admin. says See Section II of this Admin. Guide for further parsing options	See Value explanations	any text variables: %F %d %v %a	"InterScan has detected a virus in your e-mail" parse file name parse date parse virus name parse action taken
action	What InterScan should do with infected files	delete	pass delete move	pass infected file to user block infected files move infected files
movedir	InterScan <i>moves</i> infected files to this directory	/etc/isca n/virus	any valid directory and file-name	directory where infected files are placed when <i>action=move</i>

[Pattern-Update]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
Version	current virus pattern file version number	502	numeric, 502 or higher	number is derived from virus pattern file itself
Method	pattern update method	auto-matic	automatic manual	updated automatically updated on command
Frequency	frequency of automatic virus pattern file updates	Monthly	none weekly monthly	no automatic download weekly download download monthly
DayOfWeek1	day to download new virus pattern file	Sunday	Monday through Sunday	only valid when <i>frequency=weekly</i>
DayOfMonth	date to download new virus pattern file	1	1 through 31	only valid when <i>frequency=monthly</i>
hour	start time of scheduled scan	1	1 through 12	
APM	day or night start time	AM	AM PM	not case sensitive (but no periods or spaces)

[View-Configuration]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
sort	sorting criterion for generated reports	date	date user virus	order results by date order results by user order results by virus
FTP	Generate virus report for FTP virus scans	yes	yes no	include FTP scan in rept no FTP scans in report

mail	Generate virus report for SMTP virus scans	yes	yes no	include SMTP scan in rep no SMTP scans in report
HTTP	Generate virus report for HTTP virus scans	yes	yes no	include HTTP scan in rep no HTTP scans in report
periodic	Generate virus report for scheduled virus scan	yes	yes no	include sched scan in rep no sched. scans in report
manual	Generate virus report for manual virus scans	yes	yes no	include man. scans in rep no manual scans in rept
date	date of logs to include in the generated report Syear (etc.) and Eyear (etc) only valid for <i>range</i>	week	all range week OneDay Month	all virus logs logs from date to date last 7 days of logs single day lost 30 days of logs
Syear	When <i>date</i> range, Syear tells starting year	1999	year, four digits	used for viewing range of dates in virus logs
Smonth	When <i>date</i> range, Smonth tells start month	January	January through December	used for viewing range of dates in virus logs
Sday	When <i>date</i> range, Sday tells starting date	1	1 through 30	used for viewing range of dates in virus logs
Eyear	When <i>date</i> range, Eyear tells ending year	1999	year, four digits	used for viewing range of dates in virus logs
Emonth	When <i>date</i> range, Eyear tells ending month	may	January through December	used for viewing range of dates in virus logs
Eday	When <i>date</i> range, Eyear tells ending date	31	1 through 31	used for viewing range of dates in virus logs

user	Generate report regarding virus file users	All	All User-Name	include file owner and mail recipient in report
username	Generate report regarding user name when <i>User=UserName</i>	FooUser	any user-name	include user names in report
virus	Generate report regarding virus name	All	All Virus-Name	include virus names in report

[Registration]

<i>Parameter</i>	<i>Parameter explanations</i>	<i>Default Value</i>	<i>Possible Values</i>	<i>Value explanations</i>
Product	Product name	Inter-Scan Virus Wall		InterScan VirusWall
Version	Product version	2.0		2.0
Serial	Product serial number	IS65432	only one valid #	generated by InterScan, do not change!
Date	Registration date	none	date	current date or purchase date
FirstN	your first name			
LastN	your last name			
EMail	e-mail address			
HPhone	home phone number			include area code
OPhone	office phone number			include area code
Fax	fax number			include area code
RealAddr	mailing address			address, number, street
City	city			
State	state			two-letter abbreviation
ZIP	zip code			
Country	country			blank if USA
Company	name of your company			
use_proxy	do you use a proxy server?	no	yes no	a proxy server is used no proxy server is used
reg_proxy	proxy server, if any	proxy.foo.com	any proxy name or address	if <i>use_proxy</i> -yes, enter the name (or location) of the proxy server

reg_port	registration port	8080	port number	port number used by proxy server, if any
hostname	location of latest virus patter file	www.trendmicro.com		Trend's server, or companies server with newest virus pattern file