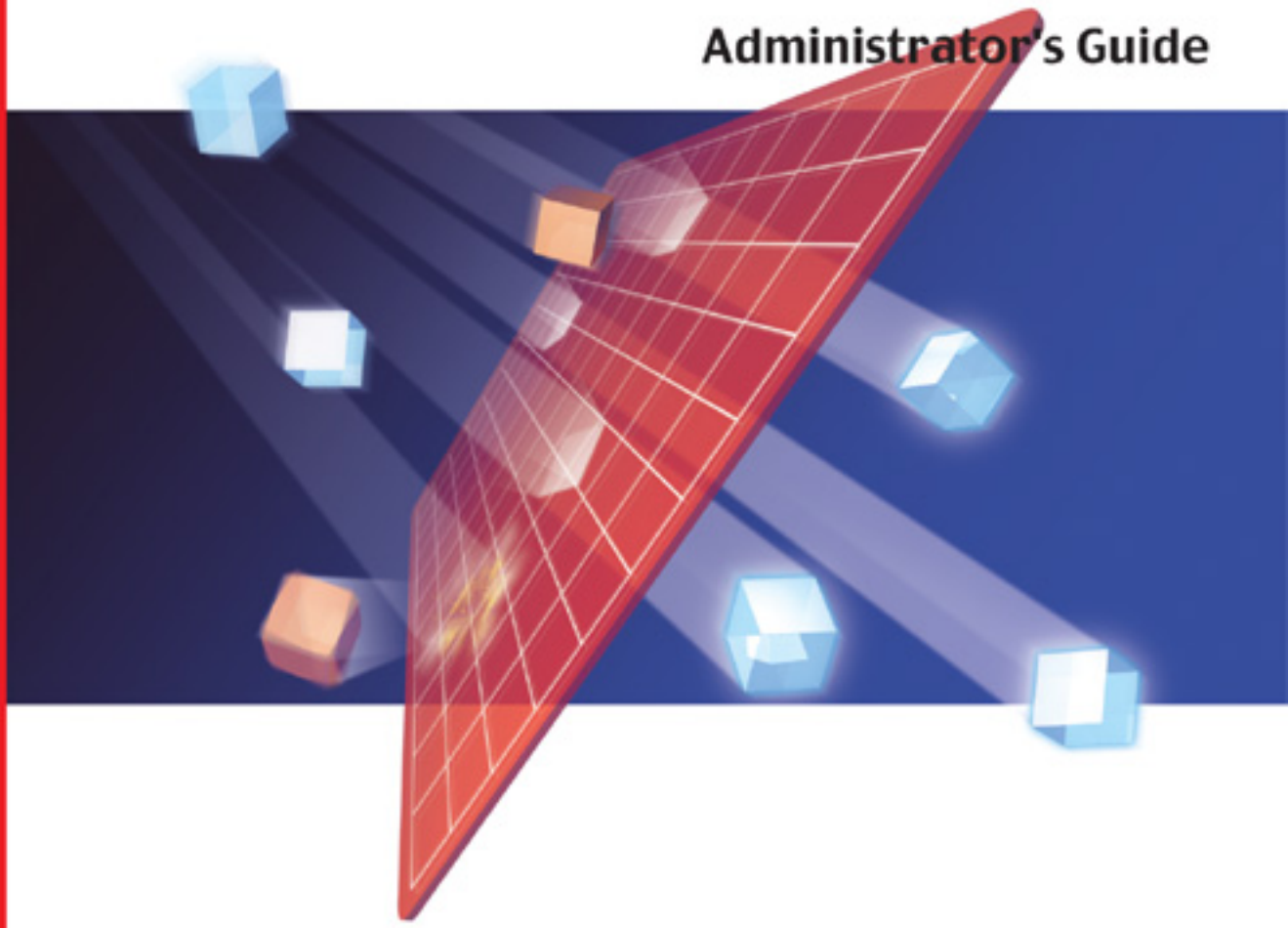
TREND MICRO™

InterScan VirusWall™ 3

Virus protection for Internet gateways

for Unix

Administrator's Guide



TREND MICRO™

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

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

NOTE: A license to the Trend Micro Software includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates and basic technical support.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

http://www.trendmicro.com/license

Document Part No. IVEM30728/20916
Release Date: September, 2002
Protected by U.S. Patent Nos. 5,623,600; 5,889,943; 5,951,698 and 6,119,165

The Administrator's Guide for Trend Micro InterScan VirusWall is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site: http://www.trendmicro.com/download/documentation/rating.asp.

Contents

Chapter 7: FTP VirusWall

Chapter 8: Web VirusWall

Chapter 9: Manual and Prescheduled Scans

Appendix A: Configuring intscan.ini with ACL Information

Index

Chapter 1

Introducing Trend Micro InterScan VirusWall

What is Trend Micro InterScan VirusWall?

Trend Micro 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 network. It is currently available for the Solaris, HP-UX, Linux and AIX platforms.

- *E-mail VirusWall* monitors all inbound and outbound email messages for viruses, including macro viruses. It also works with the *sendmail* antispam and anti-relay features under *sendmail* 8.8.8 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 corporate network through FTP file transfers. It can also exclusively protect a given server.

InterScan supports multiple network topologies and configurations. Depending on your needs, you can install InterScan between the clients and the server InterScan supports or the first application in line to receive network traffic from the Internet.

Three Editions available

InterScan VirusWall comes in three editions, all of which can be installed from the Setup package.

- **InterScan VirusWall *Standard* Edition** can be installed in any network topology, supports most firewalls, and optionally provides support for anti-spam and content filtering.
- **InterScan VirusWall *CVP* Edition** (for Solaris only) 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 Sendmail Switch Edition** (for Solaris only) is a plug-in that takes advantage of the Sendmail Switch Content Management API for mail filtering. For Sendmail Switch users, InterScan Sendmail Switch Edition simplifies deployment, reduces management cost, and provides better perfomance and security.

InterScan VirusWall Illustration

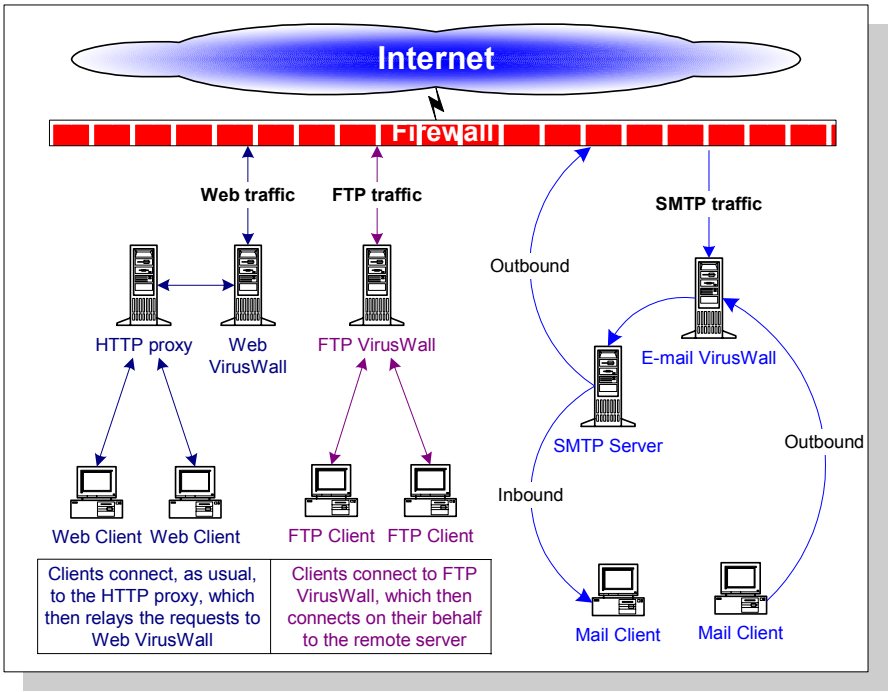


FIGURE 1-1. Web, FTP, and E-mail VirusWall are installed on a network. The arrows depict the flow of traffic in a basic network configuration using the *Standard Edition*.

InterScan Overview

All three VirusWalls provide a high degree of user configurability. Routine tasks such as virus alert notifications and virus pattern updates 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, delete, quarantine, or pass), and other program details.

Virus detection occurs using Trend Micro'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 Micro's macro virus scanning engine, MacroTrap™, to detect and remove both known and unknown macro viruses.

How Does InterScan VirusWall Work?

InterScan scans all SMTP, HTTP, and FTP traffic for viruses between the corporate network and the 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 and scans it for viruses. If the file is clean, InterScan VirusWall deletes the copy and forwards the original to its destination. If a virus is found, a notification is issued and InterScan takes the action you configure:

- **Pass** the infected file (without cleaning); the infected file is delivered with an optional notification message
- **Move** the infected file (without cleaning); the file is not delivered
- **Delete** the infected file; it is not delivered
- **Auto Clean** the infected file and send it to the original server for normal delivery

When a virus is detected, 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.

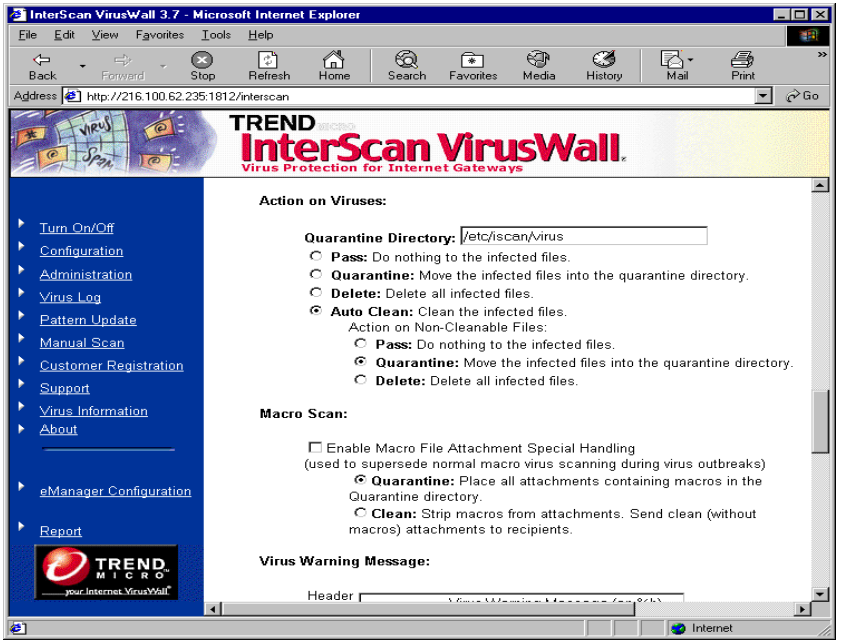


FIGURE 1-2. The Email Scan Configuration page shows the Action on Viruses, and other options.

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 email was scanned and 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 characteristic strings of virus code and compared against the tens of thousands of virus signatures that Trend Micro 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 the file 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.

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 Micro makes it easy to update the virus pattern file by supporting automatic updates. See Chapter 10, "Virus Log Files, Pattern Updates and Registration" for more information.

MacroTrap™

Macro viruses are among the most prevalent virus type. Macro viruses are not confined to any one operating system—they are application specific, so they can be spread between DOS, Windows, MACs, and even OS/2 systems. This is a fundamental change in the way viruses are spread.

With the ability to travel by email, and the increasing power of macro code, you can see that macro viruses are perhaps the biggest threat. To combat the advent of macro viruses, Trend Micro has developed MacroTrap, an intelligent technology that greatly enhances your ability to protect your corporate network.

How MacroTrap works:

The MacroTrap 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 Micro's MacroTrap checks the template for signs of unknown macro viruses by seeking out instructions that perform virus-like activity— for

example, copying parts of the template to other templates (replication), or executing harmful commands (destruction).

Compressed files

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.

Features and Enhancements

Sendmail Switch Edition

The InterScan Sendmail Switch Edition is specifically designed to work with Sendmail Switch products (version 2.1.2 or later) based on the 8.11 version open source code in a Solaris environment. The InterScan Sendmail Switch Edition takes advantage of the Content Management API for mail filtering, increasing ease of deployment, administration, and security. The InterScan Sendmail Switch Edition can also be configured to work with the open source sendmail.

eManager Plug-In Support

InterScan now supports additional plug-ins. The first plug-in available is InterScan eManager, which blocks spam and filters email content.

Check Point OPSEC CVP Certified

InterScan VirusWall UNIX passed the OPSEC CVP certification with Check Point FireWall-1. The CVP Edition works only on the Solaris platform.

MIME encoding

In addition to scanning 19 types of compressed files (up to 20 layers deep), E-mail VirusWall also decodes four types of encoding: UUencoding, Base64, quoted-printable, BinHex.

Enhanced decoding

The "block decode error" feature of InterScan has been removed and replaced by enhancing the internal decoding module.

Macro Scan

This feature gives you the option to quarantine all attachments containing macros regardless of whether they have viruses, or to strip off the macro and deliver the attachment as usual. This is an effective feature in case of a virus outbreak.

The scan engine scans for macro viruses during normal operation. However, there are situations when a new macro virus infects a company and no virus pattern file is

available to catch the macro virus. Macro Scan can stop all attachments containing macros from entering through the Internet gateway, until a new pattern file can be developed to catch the virus.

Registering Trend Micro InterScan VirusWall

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

- One year of free updates to the InterScan pattern files and scan engine
- One year of free technical support
- Important product information

You can register over the Internet, by fax, or by mail. *See* Chapter 10, "Virus Log Files, Pattern Updates, and Registration" for details.

Trial version

Trend Micro provides a free 30-day trial version of all 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 uninstall and reinstall the program. Instead, run setup again, as explained in Chapter 3 "Installing InterScan Standard Edition", Chapter 4 "Installing InterScan CVP Edition" or Chapter 5 "Installing InterScan Sendmail Switch Edition".

Serial Numbers

You product serial number can be found:

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

In addition, you may contact a Trend Micro sales representative for a serial number at the following email address:

sales@trendmicro.com

Chapter 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 a Web browser, either directly or via Trend VCS.

- *Standard* Edition—In the Standard Edition, each service is a separate daemon. Therefore, all three VirusWalls 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 —In the CVP Edition, all three services are included in one daemon. Therefore, all three services will 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. *For Solaris only.*
- Sendmail Switch Edition—In the Sendmail Switch Edition, only the SMTP daemon will be installed. The Sendmail Switch Edition should run on a machine by itself. Do not install the HTTP or FTP VirusWalls on the same machine as the Sendmail Switch Edition. *For Solaris only.*

If you install each VirusWall onto its own machine, you need to 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 requirements indicated below. Be sure to read the **Important Notes**.

Solaris Version

- Solaris 8, 2.7 or 2.6 on Sun SPARC platform
- Sun Solaris OS version 2.x with at least the end-user support configuration cluster installed
- 256MB main memory (DRAM)
- Swap space should be 2 to 3 times the main memory
- 20MB for InterScan only, 50MB if including eManager plug-in
- At least 9GB for operation (processing email messages)

HP-UX Version

- HP-UX 10.20 or later
- 128MB main memory (RAM)
- Swap space should be 2 to 3 times the main memory
- 20MB for InterScan
- At least 9GB for operation (processing email messages)

Linux Version

- IBM/AT compatible PC with Intel Pentium™ processor 133MHz or faster
- 128MB or more main memory
- Swap space should be 2 to 3 times the main memory
- 20MB for InterScan
- At least 9GB for operation (processing emails)
- OS: Linux kernel 2.2.x ONLY, glibc 2.1.x ONLY (*2)
- We have tested on these Linux distributions[1]:
    - - RedHat Linux 6.2, 7.1 and 7.2

1. C++ standard shared library (libstdc++) package needs to be installed. For more details about its installation, please refer to the manuals of your OS.

- - Suse Linux 7.2 and 7.3
- - TurboLinux Server 6.5 and 7.0

- Package name: libstdc++-compat

AIX Version

- IBM™ RS/6000™ or IBM eServer pSeries™
- IBM AIX™ version 4.3.3 or later, including AIX 5L™ version 5.1
- 256MB main memory
- Swap space should be 2 to 3 times the main memory
- 20MB for InterScan
- At least 9GB for operation (processing emails)

Important Notes

- Check Point Software's FireWall-1 version 3.0b (build 3064 or later), 4.0, 4.1 or NG are required for the InterScan *CVP Edition*
- The InterScan Sendmail Switch Edition requires Sendmail Switch 2.1.2 or later to be installed on the network. Sendmail Switch Edition has only been tested with Solaris 2.6, 2.7 and 2.8.
- The HP-UX, Linuxand AIX versions of InterScan VirusWall do not contain a CVP Edition or Sendmail Switch Edition
- *open source sendmail* users: Trend Micro recommends using InterScan Standard Edition Email VirusWall on platforms that bundle version 8.8.8 or above
- The InterScan E-mail (SMTP) VirusWall "temp" directory should be configured to 4 (InterScan VirusWall only) or 5 (including eManager) times the total number of connections (max_proc times thr_per_proc) configured. For example:

  max_proc = 25
  thr_per_proc = 5
  Average email size = 50K

  (25 X 5 X 50) X 4 = 25MB (InterScan only)

  (25 X 5 X 50) X 5 = 31.25MB (InterScan with eManager)

Note: Insufficient temporary disk space may lead to program performance problems, up to and including program failure.

Deciding Where To Install

You can install InterScan on the same machine as the original server or on a different one. In deciding where to install, the most important issue is almost always whether 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 load, CPU speed, total and available system memory, and the total amount of available swap space. Scanning one or more network 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 network bandwidth than installing InterScan on the same machine as the server it is scanning.

Setup Choices: 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 the original server uses and give the default to InterScan.

Defaults are typically: FTP: 21, SMTP: 25, HTTP: 80.

Dedicated Machine. If InterScan is installed on a 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 server or proxy server.
- 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 want to modify the MX record in the DNS configuration so that mail is routed to this machine rather than the usual SMTP server. The idea is to edit the MX record so that it directs all incoming email to the E-mail VirusWall machine.

1. Change the MX record in the DNS configuration.
2. On the **Email Scan Configuration** page, enter the host name or IP address of the original SMTP server in the **Original SMTP server location** field.

Installation Topologies

InterScan VirusWall supports installation onto most network topologies. Where 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 unique to your network.

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.

As a rule of thumb, install E-Mail VirusWall inside a firewall and on the firewall 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 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 the **-bs** flag. No port configuration is necessary.

E-mail VirusWall Example 1.

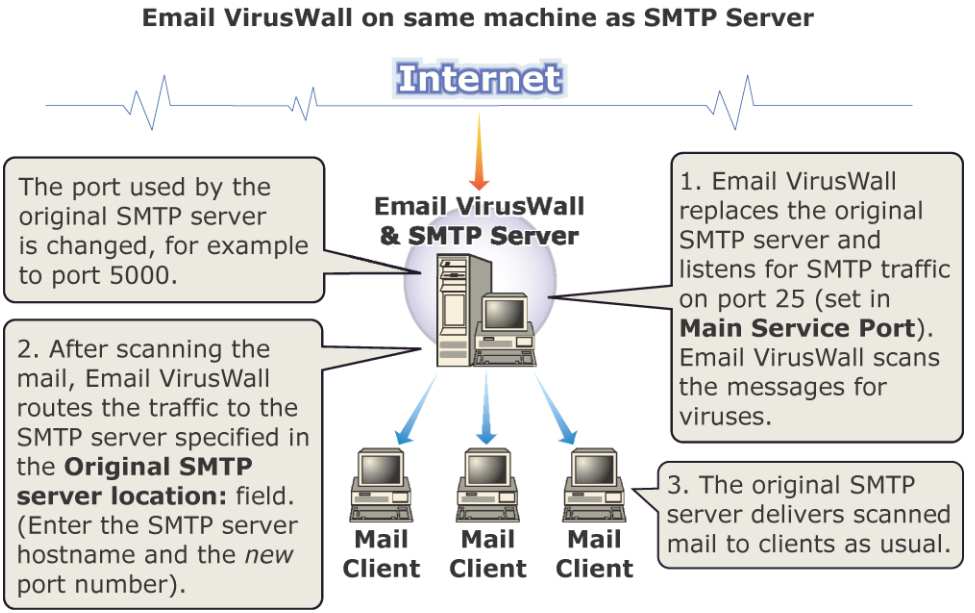


FIGURE 2-1. Notice that the SMTP server port needs to be changed.

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 **Configuration > Email Scan** page.
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.

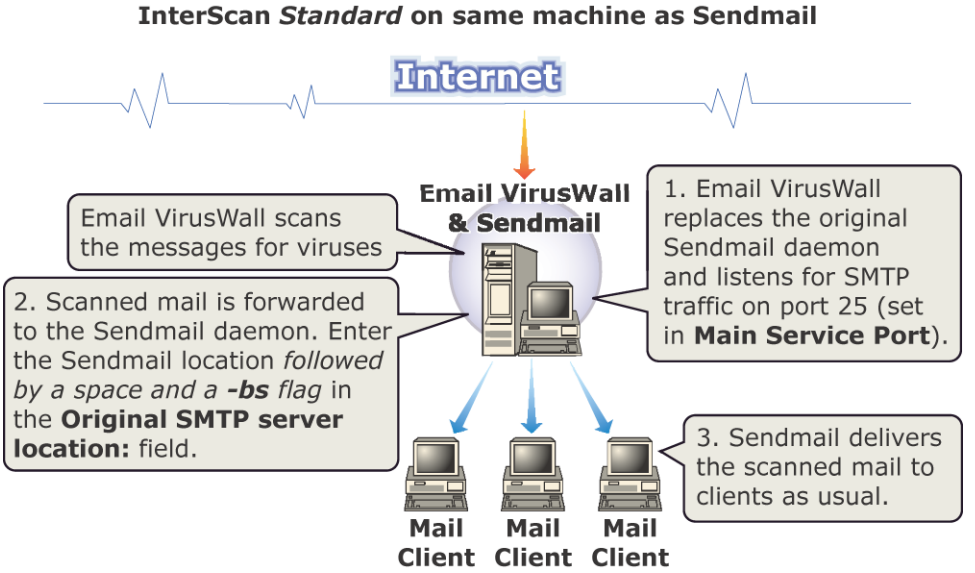


FIGURE 2-2. This topology does not take advantage of the sendmail anti-spam and anti-relay features.

E-mail VirusWall listens on port 25 for SMTP connections, scans the traffic, and forwards it to the Sendmail on the same machine. Scanned traffic is *piped* from E-mail VirusWall to Sendmail; no port needs to 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 **Configuration** > **E-mail Scan** page.
3. Enter the Sendmail path in the **Original SMTP server location:** field, for example, */usr/lib/sendmail* ***-bs***

E-mail VirusWall Example 3.

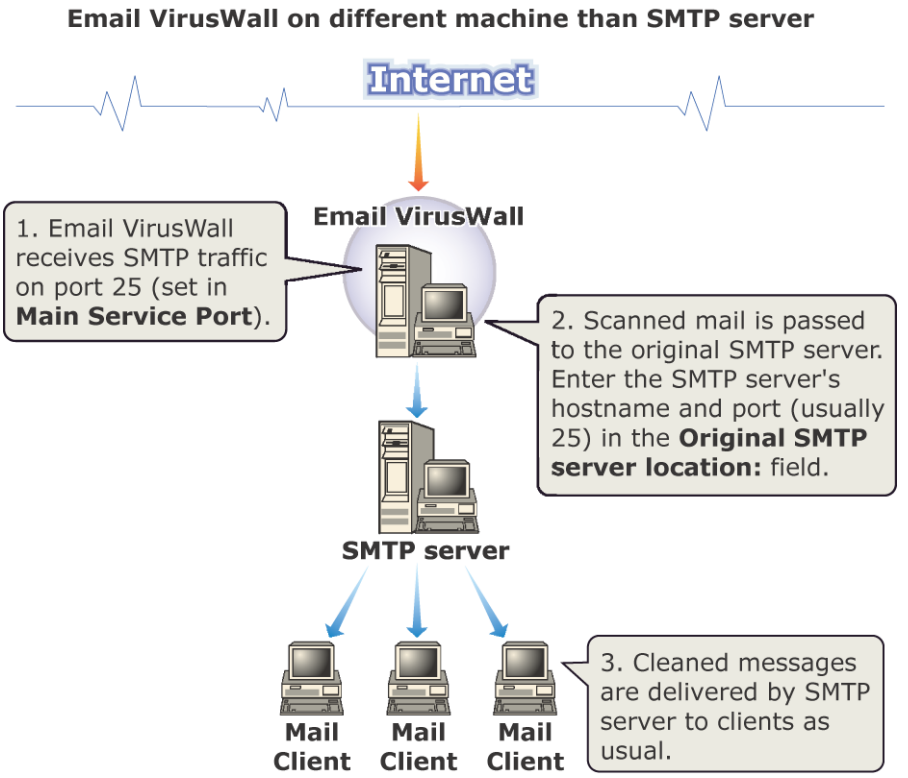


FIGURE 2-3. In this case, you may need to modify the MX record to point to the InterScan server.

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 **Configuration** > **E-mail Scan** page.
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.

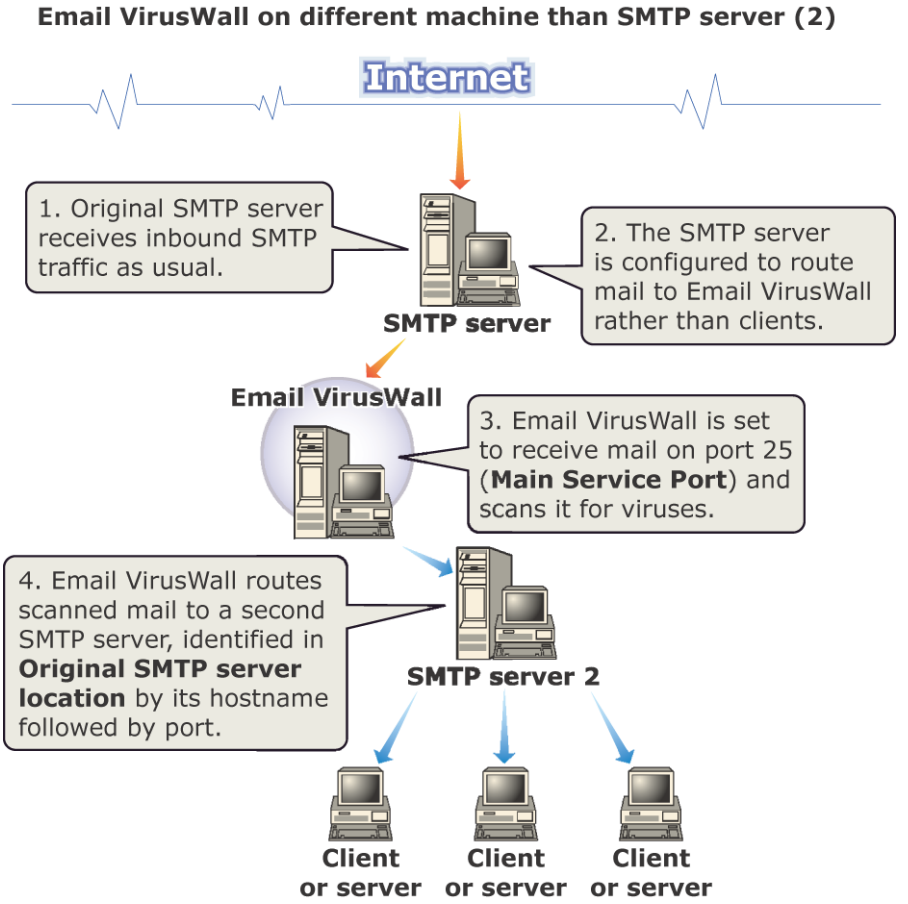


FIGURE 2-4. The SMTP server that receives the messages must be configured to forward the messages to InterScan.

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 **Configuration** > **E-mail Scan** page.
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.

When Network Contains Multiple SMTP Servers

It's important to understand that InterScan VirusWall is a gateway product, that can send and receive email traffic from a single SMTP server. It cannot communicate with multiple SMTP servers within your network. For example, the configuration shown in the following figure is not supported:

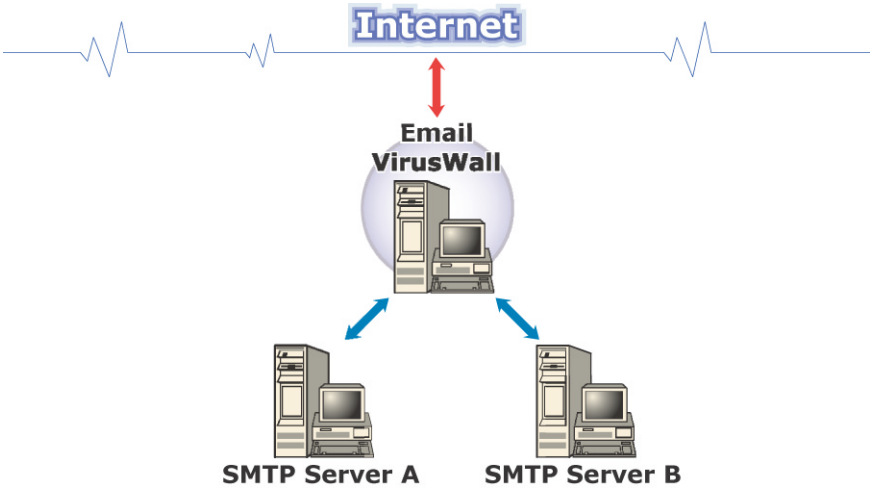


FIGURE 2-5. Sending/Receiving SMTP Traffic from Multiple Servers is Not Supported

If you have multiple SMTP servers within your network, you must install another SMTP server that:

- accepts outbound SMTP traffic from all servers and then routes it to InterScan for scanning, and
- accepts inbound SMTP traffic after InterScan has scanned it for viruses and then passes it to the SMTP servers within your network for final mail routing.

The topology of this network is shown below:

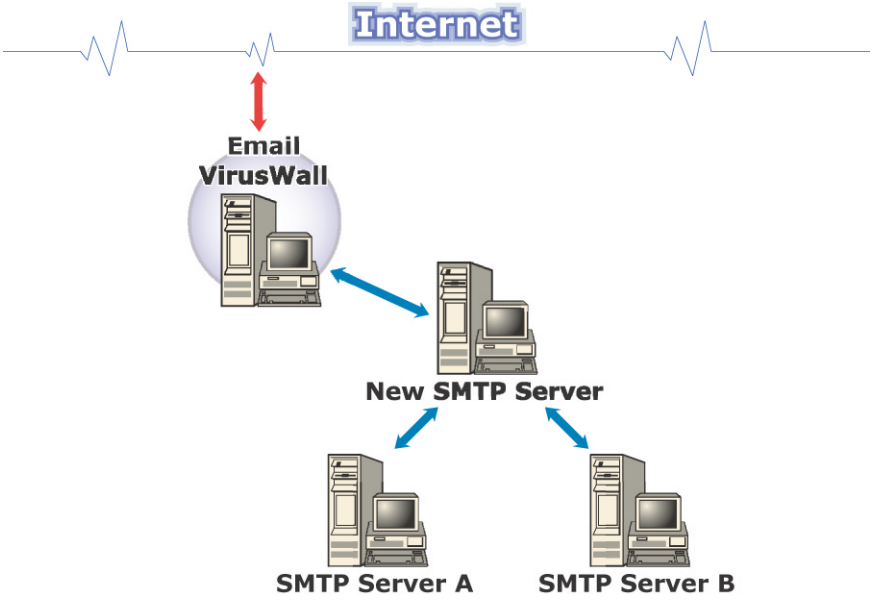


FIGURE 2-6. Adding a New SMTP Server to Process Traffic To/From Multiple Servers

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, or on a dedicated machine (in conjunction with an existing proxy). Web VirusWall can also be configured to act as its own HTTP proxy.

Web VirusWall can also be used to scan browser-based FTP file transfers—just specify Web VirusWall as the FTP proxy in the proxy server settings section of all your client browsers.

Note: If you configure Web VirusWall to act as its own 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 and security checking are not provided.

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 to the remote Web server, 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 may be 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.

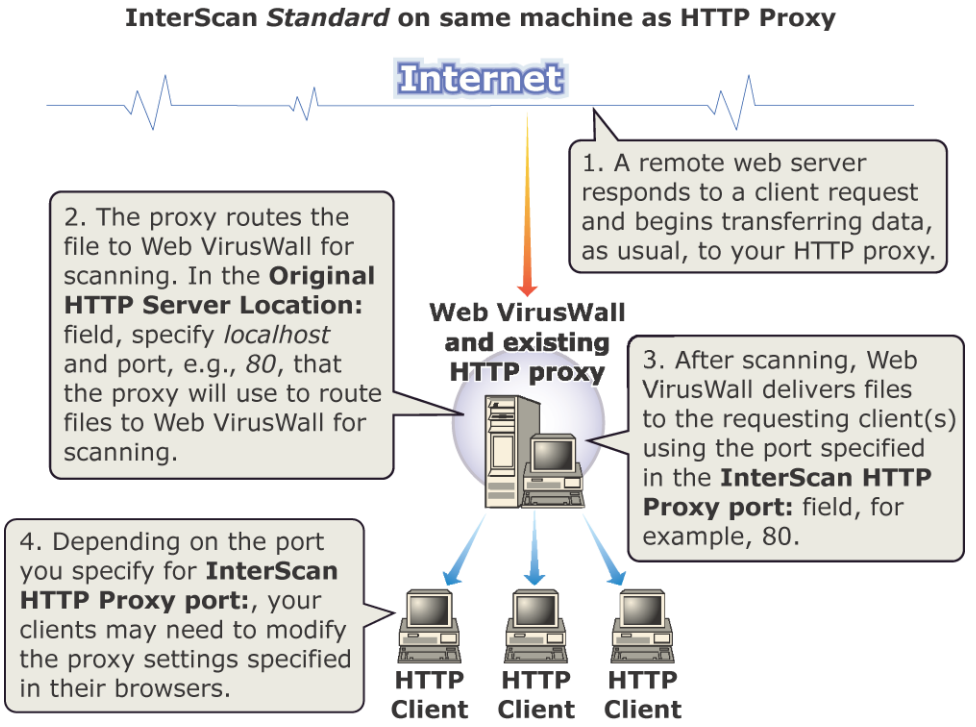


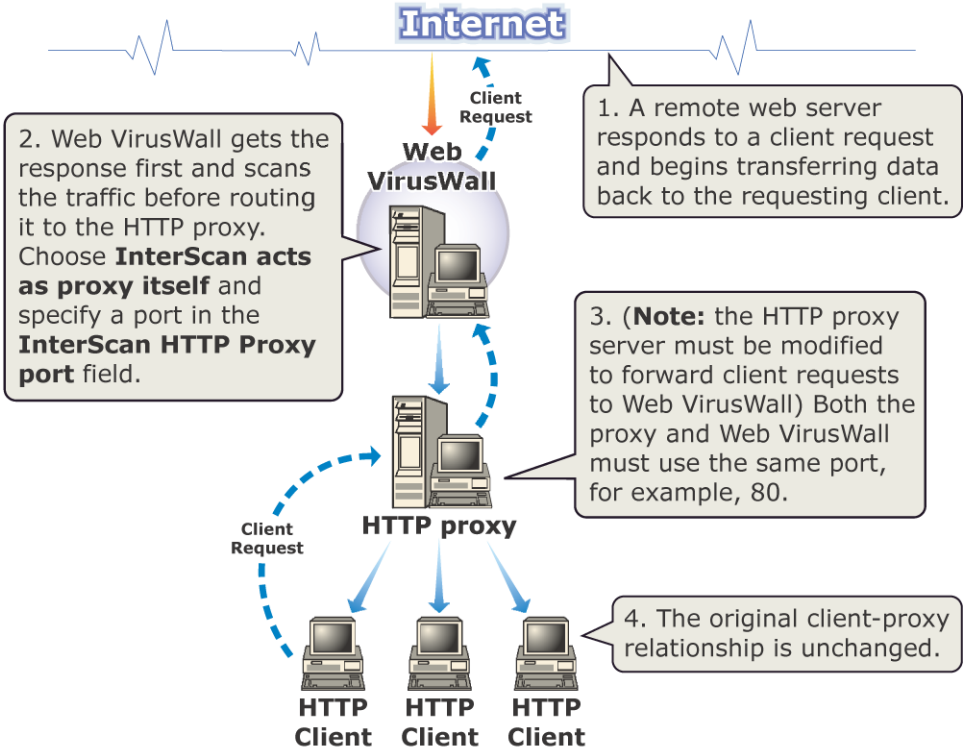
FIGURE 2-7. In this case, InterScan works with the original proxy.

Considerations:

- 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
- Use "trickle" if you encounter any proxy "timeout" issues

- Clients experience no delay between clicking a file for download and receiving the "Save as" dialog box

Web VirusWall Example 2.



Note: Installing Web VirusWall on the Internet side of the proxy can be *more* efficient because cached data is scanned only once.

FIGURE 2-8. HTTP proxy is modified to forward requests to InterScan.

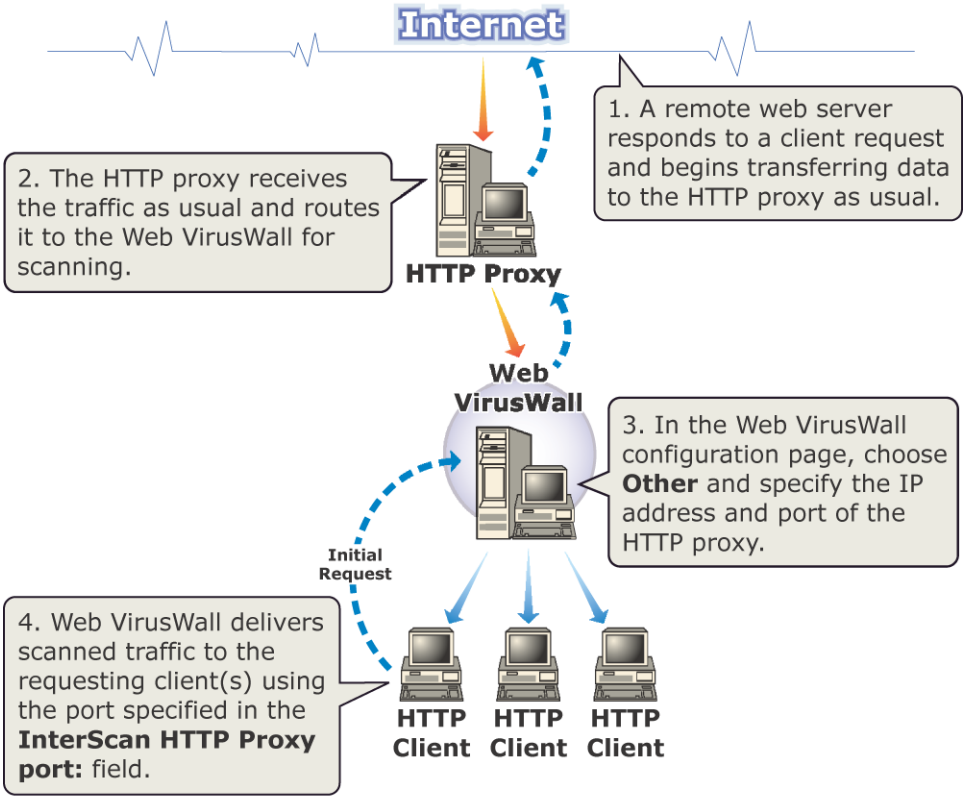
Considerations:

- 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 "timeout" 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.

InterScan *Standard*: Web VirusWall & proxy on different machines



Note: Installing Web VirusWall on the client side of the proxy can be *less* efficient because cached data will be scanned upon each request

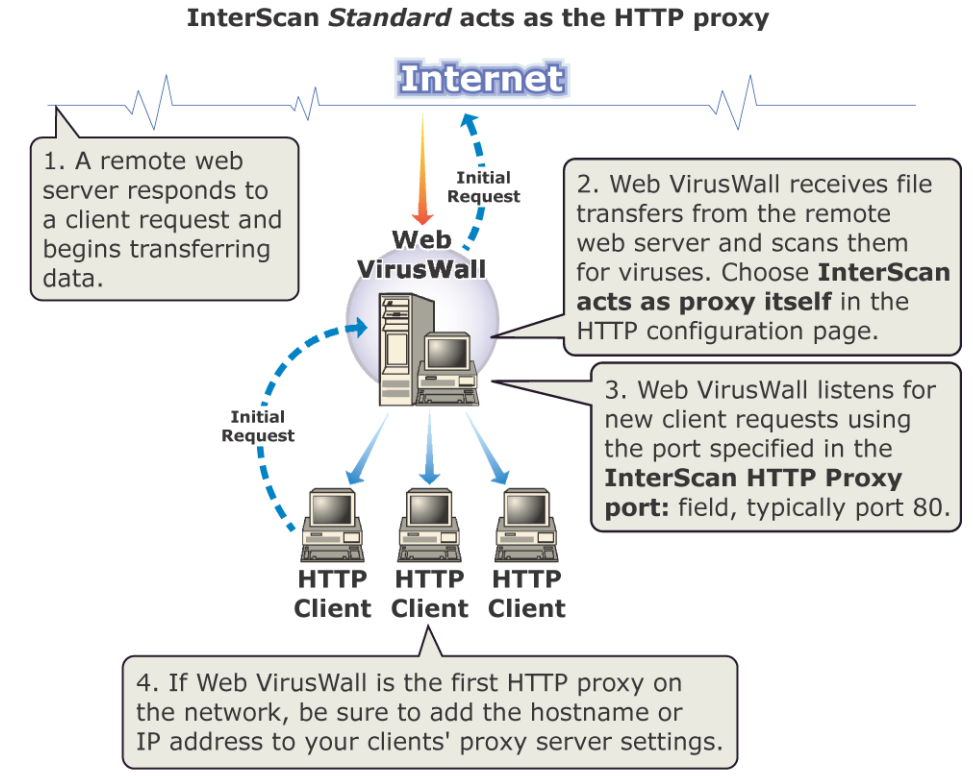
FIGURE 2-9. This topology for two machines is not as efficient as example 2.

Considerations:

- **Configuration > HTTP Scan:** Choose **Other** and specify the IP address and port of the machine where your HTTP proxy server is installed
- 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 "timeout" 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.



Note: Web VirusWall does not provide traditional proxy benefits such as caching.

FIGURE 2-10. In this case, InterScan completely replaces the original proxy.

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 "timeout" issues
- Clients may experience a lag between clicking a file for a download and receiving the "Save as" dialog box (or use trickle)
- 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`.

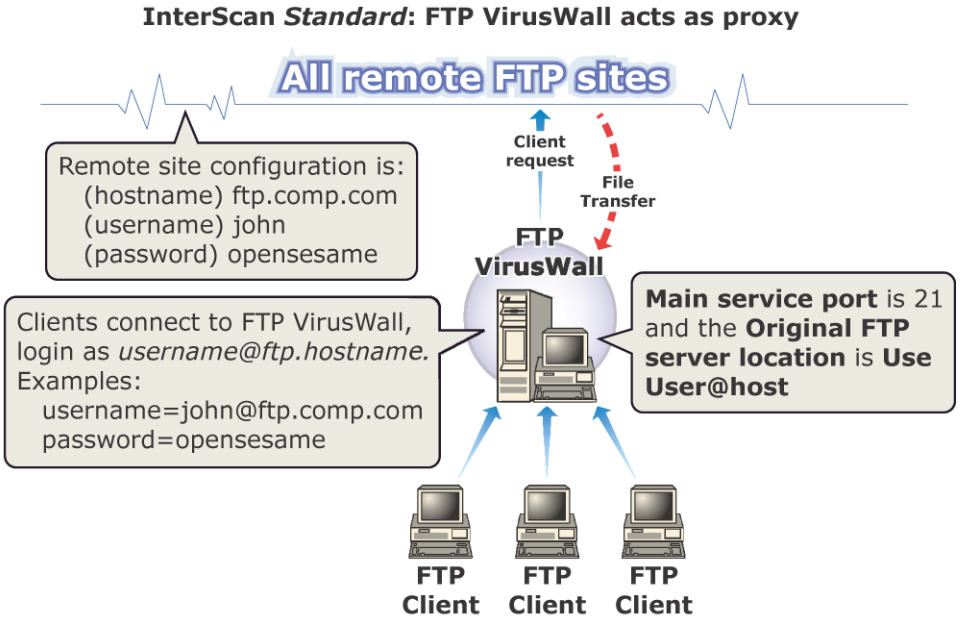
FTP VirusWall as a proxy

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 use your firewall to restrict access to port 21 to all IPs other than FTP VirusWall.)

FTP VirusWall as a sentry

If you want to scan all FTP traffic in or 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.



Note: Clients wanting to access ftp.comp.com must pass through FTP VirusWall. They log on as *username@ftp.comp.com*. FTP VirusWall connects to the remote site and mediates requests.

FIGURE 2-11. FTP VirusWall can provide basic FTP services with virus scanning.

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 to 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.

InterScan *Standard*: FTP VirusWall scans for designated FTP server

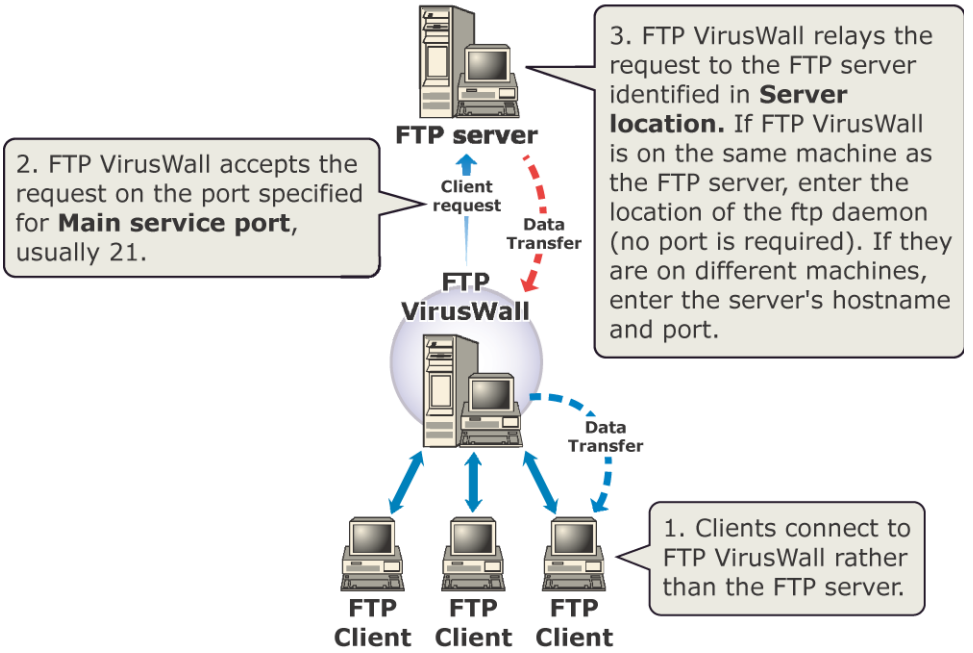


FIGURE 2-12. The original proxy provides caching and additional security.

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 they 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.

Chapter 3

Installing InterScan *Standard* Edition

InterScan VirusWall can be installed and configured to support 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.

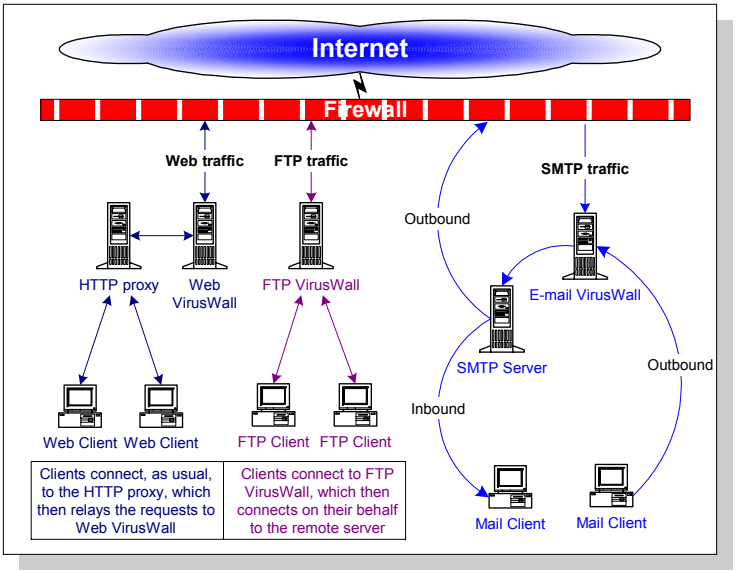


FIGURE 3-1. This illustration shows how the *Standard* edition of Web, FTP, and E-mail VirusWall might be installed on a LAN.

Chapter Overview

In this chapter you will find step by step instructions for installing InterScan *Standard* Edition. Also presented are instructions for:

- Starting and stopping the VirusWalls
- Opening the InterScan Web Console
- Using a special test virus to check your setup
- Troubleshooting installation problems
- Uninstalling Trend Micro 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.

Before Installing InterScan

Important: Before Installing InterScan, you must completely remove any existing version you may have. When you remove InterScan, the `intscan.ini` file will be temporarily saved in the following directory:

`/tmp/iscan_old.`

Note: If the tmp directory is deleted prior to reinstalling InterScan VirusWall, you will lose your previous customized values.

To remove InterScan, follow the installation instructions below. When the main menu appears, choose **Option 2**: **Remove InterScan VirusWall sub-system**. Then choose **Remove All InterScan VirusWall System**.

During the Base System installation, the script will create a new `intscan.ini` and save your old `intscan.ini` file to the following directory: `/etc/iscan/old_log_ini`.

The new `intscan.ini` file will contain default installation values. **It will not save your previous values**.

To retain your customized `intscan.ini` values, you must manually replace the default values in the new intscan.ini file with your customized values. We recommend that you print out the old `.ini` file and use it to review each value in the new `.ini` file. Use any text editor to restore the old settings and save the new `.ini` file. When finished, start the InterScan services.

Installing InterScan

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

Note: If you are installing the HP-UX or Linux versions of InterScan, the installation will differ somewhat from the description based on the Solaris platform.

---

1. If you are installing from the Trend Micro Enterprise Solutions CD, you need to mount Solutions CD #2 onto a Windows NT server, locate the directory where the files are located,

   `PROGRAMS/ISVWSOL,` for Solaris
   `PROGRAMS/ISVWHP,` for HP-UX
   `PROGRAMS/ISVNUX,` for Linux

2. Choose the English or Japanese version. FTP the program files to a UNIX server and untar them.
3. From the directory containing the InterScan installation files, type `./isinst` and press ENTER.

Note: The next step only applies to InterScan VirusWall Solaris edition.

---

4. If you are installing the InterScan VirusWall Solaris version, you are prompted to select which edition 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.
5. The **Main Menu** appears, displaying the current system configuration.
   - **Yes** means the package is not installed. This is the typical value for first time installations.
   - **No** means the package exists on the server. Before installing the current version, be sure to uninstall any previous version.
6. Choose **Option 1** to install InterScan.

   By default, InterScan will install all available systems to subdirectories of `/opt/trend`. If you want to install to a different directory, type in the path and press `ENTER`.

Note: The **Trend Virus Control System (TVCS) Agent** is not installed by default, *see* Chapter 12, "Trend Virus Control System," for more information).

---

7. Choose **Option 9, Start Installation** to start the installation.

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 computer that you will install a VirusWall on.

8. Continue to follow the screen prompts to complete the installation. 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. For information on how to buy, please refer to the following URL:

   ```
   http://www.trendmicro.com/buy
   ```

9. To install HTTP, SMTP, and FTP VirusWall, press **y** and **Enter** as prompted. To install only one VirusWall, enter **n** when prompted to install the additional VirusWall(s).

10. Once you have completed the installation, select **Exit**. InterScan will then ask if you want to start the services. If you choose **yes**, the services will start with new `interscan.ini` settings. **Please read the following section before starting the services**.

Performance Settings

When running the installation script, you have the option of changing the default InterScan VirusWall settings for the maximum and minimum number of HTTP scanning processes, and the number of pre-spawned HTTP scan processes. The installation script will assess your system and make a recommendation. You can alternatively use the default values, accept the recommendation or enter your own desired configuration.

Run Multiple Instances of InterScan

You can configure InterScan to run multiple instances on the same UNIX box using different ports.

When you start InterScan, it looks for the default `intscan.ini` file. To run multiple instances using different service ports, you will need to create a unique `.ini` file for each additional instance of InterScan.

Use the following procedure:

1. Create a separate `.ini` file with either a different name or placed in a different directory location.
2. Specify a new service port in the new `.ini` file.
3. When starting the additonal instance of InterScan, use the C option and specify the new `.ini` location:

```
/etc/iscan/sendmail -C[/direcory/filename]
```

For example: The second instance of InterScan will listen on port 26. The new `.ini` file will be called `intscan2.ini` and will be placed in the `/etc/newiscanini` directory.

At the command line, type in the following command:
`/etc/iscan/sendmail -C/etc/newiscanini/intscan2.ini`

This will start the new instance of InterScan listening on port 26.

Opening the Web 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)**. The IP address can be either the domain name or number of the InterScan machine. The port used for the Web Console is also user-configurable. For example,

```
http://domain:port/interscan
http://isvw.widget.com:1812/interscan
http://123.12.123.123:1812/interscan
```

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

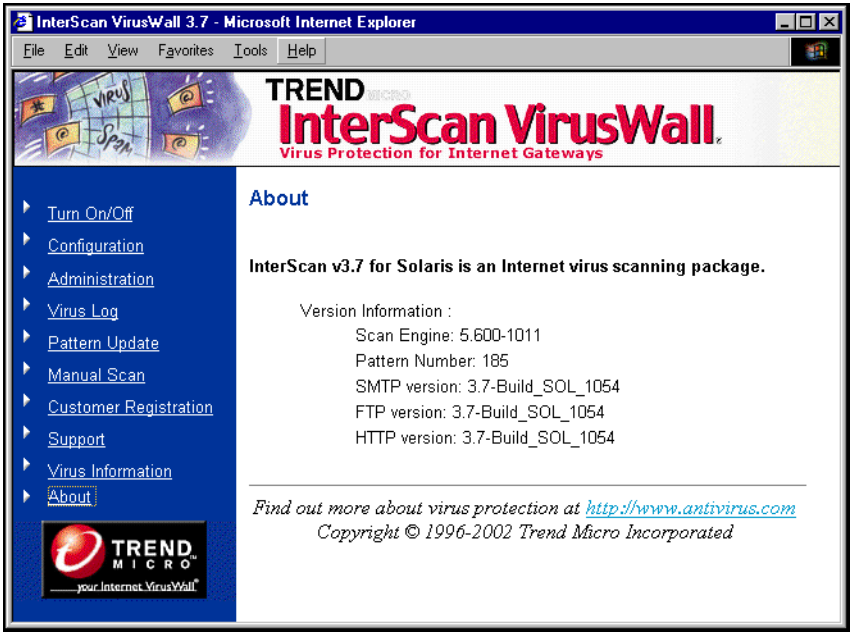


FIGURE 3-2. This InterScan console screen, displays the About topic, which shows the versions installed.

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

Note: The owner of the InterScan process is "iscan". Since stopping or starting the sendmail daemon must be performed with a "root" credential, it cannot be stopped or started from the UI when InterScan VirusWall is running in daemon mode. You will thus have

to run the `/etc/rc2.d/S88sendmail` start command after turning InterScan VirusWall on or off.

To enable/disable real-time scanning,

1. From the InterScan Web configuration menu, click **Configuration**.
2. Under the *Real-time Scan* section, click any of the buttons to toggle scanning for that service.
3. Click the **Apply** button.

Note: If you disable email virus scanning, the flow of traffic will continue without virus scanning.

Command line option: Solaris: E-mail, FTP and Web respectively

```
% /etc/rc2.d/S88sendmail stop
% /etc/rc2.d/S88sendmail start

% /etc/rc2.d/S99ISftp stop
% /etc/rc2.d/S99ISftp start

% /etc/rc2.d/S99ISproxy stop
% /etc/rc2.d/S99ISproxy start
```

Command line option: HP-UX: E-mail, Web, and FTP respectively

```
% /sbin/rc2.d/S540sendmail stop
% /sbin/rc2.d/S540sendmail start

% /sbin/rc2.d/S991IScanFTP stop
% /sbin/rc2.d/S991IScanFTP stop

% /sbin/rc2.d/S992IScanHTTP stop
% /sbin/rc2.d/S992IScanHTTP start
```

Command line option: Linux: E-mail, Web, and FTP respectively

```
% /etc/rc.d/rc3.d/S80sendmail stop
% /etc/rc.d/rc3.d/S80sendmail start
```

```
% /etc/rc.d/rc3.d/S99ISproxy stop
% /etc/rc.d/rc3.d/S99ISproxy start

% /etc/rc.d/rc3.d/S99ISftp stop
% /etc/rc.d/rc3.d/S99ISftp start
```

Command line option: AIX: E-mail, Web, and FTP respectively

```
% /etc/rc.iscan/rc.issmtp stop
% /etc/rc.iscan/rc.issmtp start

% /etc/rc.iscan/rc.isproxy stop
% /etc/rc.iscan/rc.isproxy start

% /etc/rc.iscan/rc.isftp stop
% /etc/rc.iscan/rc.isftp start
```

To turn on/turn off InterScan,

1. In the InterScan console, click **Turn On/Off**.
2. Click the buttons to alternatively enable or disable the InterScan services.

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".

Encrypting Browser-Console Communication

In order to prevent configuration data from being intercepted when it travels from the management console to the server, you can enable InterScan VirusWall to use a secure HTTPS protocol.

Generating a Private Key

Before you can access the InterScan VirusWall console via HTTPS, you must generate a private key. By default, InterScan VirusWall ships with a certificate (server.crt) and key (server.key):

- server.crt is in /ISADMIN/IScan.admin/conf/ssl.crt
- server.key is in /ISADMIN/IScan.admin/conf/ssl.key

You use a script called mkcert.sh in the /ISADMIN/IScan.Admin/makecert directory. Running the mkcert script creates server.crt and server.key. You can optionally

choose to encrypt the private key while running mkcert.sh, for which you will be prompted for a pass-phrase.

Disabling Prompting for Pass Phrase

If you chose to encrypt the private key when running mkcert.sh, you will be prompted for the pass-phrase every time you start the InterScan service. To disable this prompt, you can run the following commands in the directory where the private key is located:

```
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
chmod 400 server.key
```

Changing the Pass-phrase

To change the pass-phrase that protects your private key, run the following commands in the directory where it is located:

```
openssl rsa -des3 -in server.key -out server.key.new
mv server.key.new server.key
```

Accessing the Console Via HTTPS

If you want to configuration data to be encrypted as it passes from the Web-based console to the server, you must alter the URL to use the https protocol and specify port 8443 instead of port 1812. The URL to use for encrypted communication will appear similar to the following:

```
https://123.123.123.12:8443/interscan
```

By comparison, the URL used for non-encrypted communication is:

```
http://123.123.123.12:1812/interscan
```

Testing InterScan

Once InterScan VirusWall has been installed, we recommend that you test it to get familiar with the configuration and see how the program 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 Micro at:

`http://www.trendmicro.com/vinfo/testfiles/`

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

Troubleshooting a *Standard* Setup

Mail is not being delivered.

If you receive the following error when running E-mail VirusWall, "`cannot connect to original server`", check your **Original SMTP server location** settings to be sure that the IP address and port have been properly specified.

With the InterScan configuration open in a Web browser,

1. Click **Configuration > E-mail Scan.**
2. On the **Email Scan** page, check the value specified for **Original SMTP server location**.
3. Alternatively, verify that path specified for your local mail server is valid.

Can't find "moved," or 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 **Move**, infected files are written to the `/var/tmp` directory.

Uninstalling InterScan

InterScan's uninstall scripts require superuser 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 remove the service.

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

Installed Files

InterScan makes the following changes to your system:

Platform	*Directory*	*Action*	*Files/Modification*
Solaris, HP, Linux, and AIX	/opt/trend (user config.)	create dir	all files located within
Solaris, HP, Linux, and AIX	/etc/iscan	create dir	all files located within
Solaris, HP, Linux, and AIX	/etc/inetd.conf	modify file	## comment out original FTP server
Solaris	/etc/rc2.d	modify and create	Create S88sendmail, S99ISproxy, S99ISftp, S99IScanHttpd, S99ISmaild
HP-UX	/sbin/rc2.d	modify and create	add InterScan to the S540sendmail; create S991IScanFTP; S992IScanHTTP; S999IScanHttpd

Platform	*Directory*	*Action*	*Files/Modification*
Linux	/etc/rc.d/rc3.d	modify and create	Add InterScan to S80sendmail, create S99IScanHttpd, S99ISftp, S99ISproxy, S99ISmaild **Note**: Instead of "S80sendmail", the name of the start-up script will be S10sendmail on the Suse 7.2 distribution and "S11sendmail" on the Suse 7.3 distribution.
Solaris	/etc/rc2.d	create	S99IStvcs -- Trend VCS Agent
HP	/sbin/rc2.d	create	S99IStvcs -- Trend VCS Agent
Linux	/etc/rc.d/rc3.d	create	S99IScanTVCS -- Trend VCS Agent
AIX	/etc/rc.iscan	create dir	all files located within
AIX	/etc	create	rc.shutdown iscan_plugins iscanftps iscanhttpds iscanhttpproxys iscansmtps iscantvcsagts

Upgrading from the Trial Version

To upgrade a trial version to the full version:

1. Save the /etc/iscan/intscan.ini file used by your trial version. This file contains configuration settings used by your trial version software.
2. Run InterScan's install script (./isinst) to uninstall the trial version.
3. Run the install script again to install the software, and enter the serial number when prompted.
4. Replace the default intscan.ini file from your installation with your saved version and restart InterScan VirusWall.

Chapter 4

Installing InterScan *CVP* Edition

In this chapter you will find step-by-step instructions for installing InterScan VirusWall *CVP* Edition (not available for the HP-UX, Linux or AIX platforms). Also included are instructions for:

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

Installation Overview

In the *CVP* Edition, InterScan acts as a CVP server to your FireWall-1 machine and provides real-time virus scanning for SMTP, HTTP, and FTP file transfers.

InterScan receives inbound and/or outbound network traffic from the FireWall-1 server, scans it, and then routes it back to the FireWall-1 machine for delivery as usual. All three VirusWalls are installed as a single daemon. You can turn each VirusWall on or off individually.

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 are 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. If network traffic is heavy, consider using one or more dedicated servers.

Choosing the best place to install depends on your network's traffic and 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).

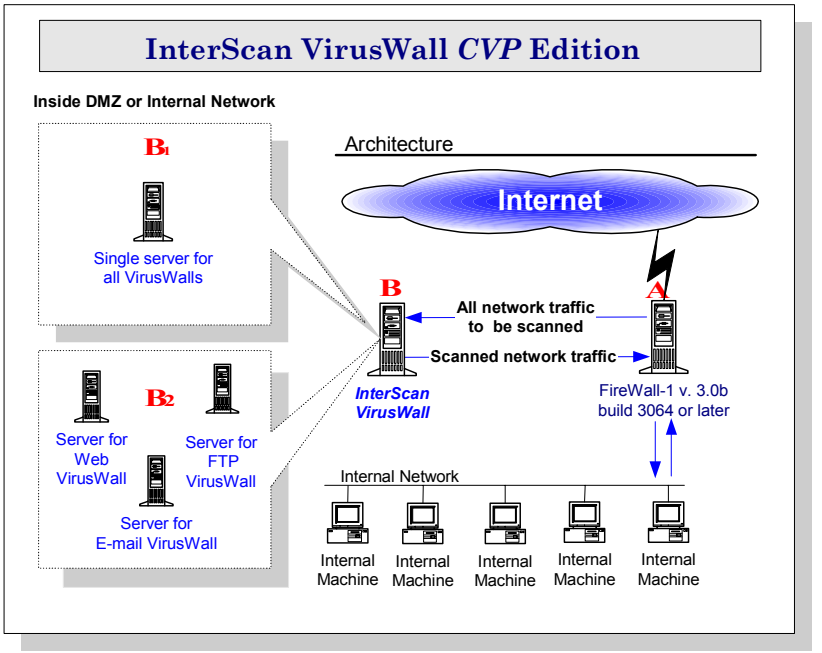


FIGURE 4-1. InterScan must receive network traffic from FireWall-1. Possible installation points for InterScan VirusWall are indicated by the letters A (the FireWall-1 machine) and B (another server).

- **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 servers 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.

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 **root**. Installation takes about ten minutes and does not require you to restart the server.

Note: The CVP library uses OPSEC SDK version 4.1 which is compatible with Sun Solaris 2.6x and 2.7.

---

1. If you are installing from the Trend Micro Enterprise Solutions CD, you need to mount Solutions CD #2 onto a Windows NT server, locate the directory where the files are located, `PROGRAMS/ISVWSOL`, choose the English or Japanese version. FTP the program files to a UNIX server and untar them.
2. From the directory containing the InterScan installation files, type `./isinst` and press `Enter`.
3. Choose **InterScan VirusWall for CVP** to install onto a FireWall-1 network and have InterScan act as a CVP server.

4. A **Setup** menu appears showing the current InterScan system configuration. **Yes** indicates that the package is not installed. **No** indicates that the package is installed.

Note: If any systems or subsystems are installed, remove them (**Option 2**) before proceeding with Setup.

Choose **Option 1** to install InterScan.

5. By default, InterScan will install all available systems to subdirectories of `/opt/trend`. If you want to install to a different directory, type in the path and press ENTER.

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

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

---

6. Choose **Start Installation** at the Setup Script menu to start the installation. Enter **y,** then press **Enter**, as prompted to continue installation.
7. 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.

   Press **Enter** without typing in 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.trendmicro.com/buy`
8. Follow the prompts to complete the Setup.

After Installing the *CVP* Edition...

After installing the InterScan program files, you need to configure InterScan and your FireWall-1 to work together. The main tasks are identified below, followed by the step-by-step instructions.

On the InterScan side...

There are three things on the InterScan side that need to be in place for scanning to work:

- The port specified as InterScan's **Main service port** must match that set for FireWall-1's FW1_cvp service; this port is typically set to 18181, and you can set InterScan's port first, then add the port used when setting your FireWall-1 rules
- If you use Check Point Software's OPSEC Authentication, enable this option in the InterScan configuration
- InterScan must be turned **ON** (when **OFF**, network traffic does not pass through InterScan and, unless re-routed, network traffic for that protocol will stop)

A. Setting the Main Service Port

1. From the FireWall-1 rule base editor, click the **Services** checkbox 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.

B. 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.

C. 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.**

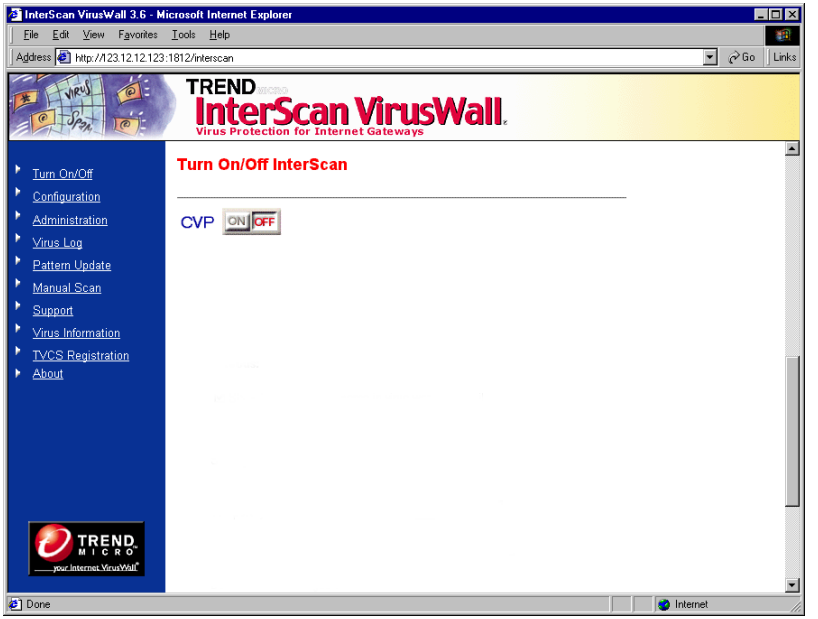


FIGURE 4-2. Be sure that each service is ON.

2. InterScan can be turned ON or OFF.
3. Click **On** to enable scanning if the current status is CVP OFF, or **Off** to disable scanning it the status is CVP ON.

On the FireWall-1 Side...

Note: Each FireWall-1 procedure is illustrated with a "screen shot" from version 4.1 that shows the Windows/Motif user interface. If you use OpenLook, some screen arrangements may look different.

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 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.

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:
   - **Network** workstation object for each computer with InterScan VirusWall installed
   - **Server** object (one for each protocol if InterScan is installed on multiple computers)
   - **Resource** (one for each protocol if InterScan is installed on multiple computers)
   - Add and install your scanning rules to the **rules base**
2. *If you are using Check Point's OPSEC Authentication*, register the InterScan computer 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 in the FireWall-1 Security Policy Editor in **Read/Write** mode (or **Cure**). See your FireWall-1 documentation for complete configuration details.

A. FireWall-1: 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 computer).

- If you installed InterScan onto the FireWall-1 computer, 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 computer.

3. In the **General** tab, enter the name of the computer where InterScan is installed in the **Name:** field. For example, Paris

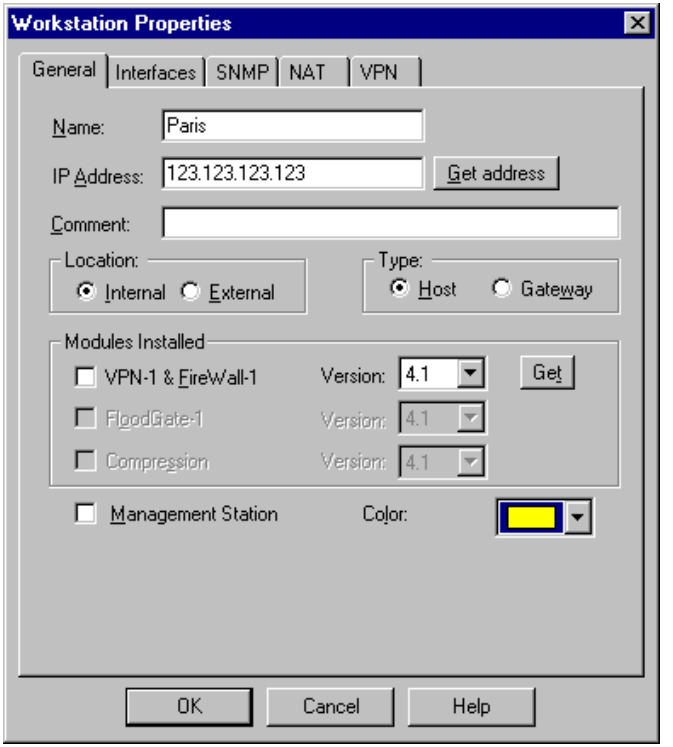


FIGURE 4-3. Create a Network Object for each of the VirusWalls.

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 setup.

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, **Email-Anti-Virus**.

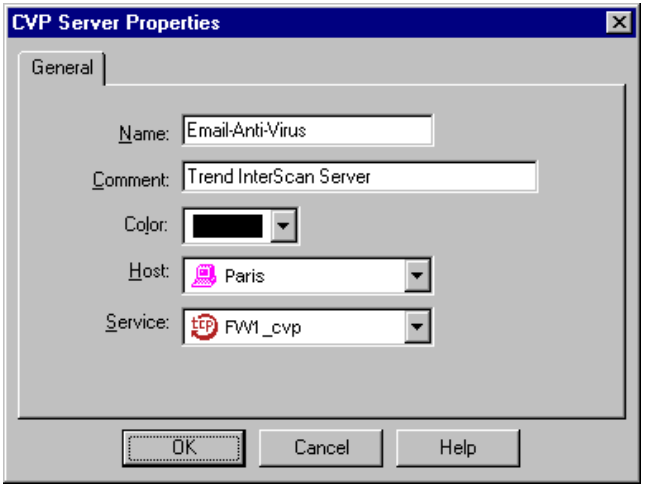


FIGURE 4-4. Define a Server Object for each of the VirusWalls.

4. Next, click the **Host** drop-down box and select from the list that appears the *Network Object* you created in task A, e.g., `Paris` in our example.
5. Accept the **Service:** type already specified, i.e., *FW1_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.
   - Choose **SMTP** for the E-mail VirusWall
   - Choose **URI** for the Web VirusWall
   - Choose **FTP** for the FTP VirusWall

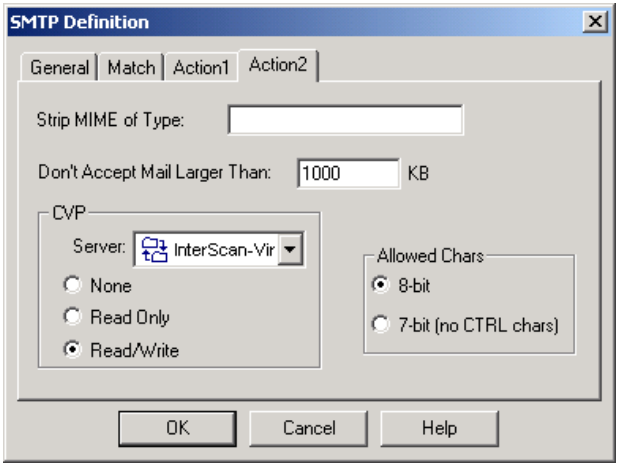


FIGURE 4-5. Define a Resource Object for each VirusWall.

3. In the **General** tab, enter a name for the Resource in the **Name:** field, for example, **Email 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 B, `Anti-virus` 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 the 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 B.

b. Click **Read/Write** to enable virus scanning and cleaning (step **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 the resources from task C, SMTP, for instance.
4. Right-click the **Action** column of the rule and choose **accept** from the menu that appears.

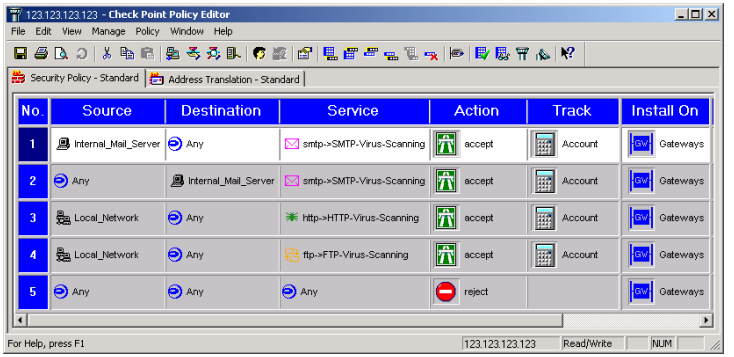


FIGURE 4-6. InterScan's scanning services are added to the CVP rule base.

5. Optionally, right-click the **Track** column of the rule and choose **Long** from the menu 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

As an option, the connection between InterScan and FireWall-1 can 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 computers. The computers identify themselves using the authentication key.
- Establish authenticated communication between the Client process (FireWall-1) and the Server process (InterScan).

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

1. On **FireWall-1**, go to the `/bin` directory and type the following at the command line prompt:

   fw putkey -opsec InterScan

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

2. Next, on **InterScan**, go to the `etc/iscan` directory and type the following at the command line prompt:

   opsec_putkey FireWall-1

   where FireWall-1 represents the host name of the computer where FireWall-1 is installed. You are prompted (twice) to enter the authentication key.

   Enter the same key as entered in Step 1. Make sure the `authkeys.C` and `rand.C` files were created in the `etc/iscan` directory.

   Note: `Putkey` must be run first on the firewall before it is run from the CVP server.

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.

4. Next, from the InterScan's configuration console, enable the **Authentication** port by clicking **Yes**.
5. Click **Apply** to save your changes and restart the daemons.

SSL Configuration for the Web Console

Overview

The InterScan VirusWall for UNIX Web Console uses HTTP 1.0 Basic authentication. The password typed from the browser is encoded by Base64 and sent to the server. However, since Base64 does not implement an encryption algorithm, there is a risk of the password being stolen by analyzing data packets using packet filtering software.

The following explains the steps to enable a SSL (Secure Socket Layer) connection between the ISVW Web console and a Web browser.

Configuration

To configure SSL (Secure Socket Layer) communication, do the following:

1. Install ssleay-0.9.0b. You can download ssleay-0.9.0b from the following URL:

   ```
   http://www2.psy.uq.edu.au/~ftp/Crypto/ssleay/
   ```

2. Create a RSA private key. Type the following command:

   ```
   % /usr/local/ssl/bin/ssleay genrsa -rand .rnd >
   key.pem
   ```

3. Create the certification. Type the following command:

   ```
   % /usr/local/ssl/bin/ssleay req -new -x509 -nodes
   -key key.pem -out dummy.pem
   ```

4. Prepare the certification for stunnel. Type the following command:

   ```
   % echo "" > dummy.txt
   ```

   ```
   % cat key.pem dummy.txt dummy.pem dummy.txt > ca.pem
   ```

   If stunnel is not installed on your system, you must intall it after downloading from the following site:

   ```
   http://www.stunnel.org/download/source.html
   ```

   Start stunnel by typing the following command:

   ```
   % stunnel -p ca.pem -d 443 -r localhost:1812
   ```

5. Open "https://ISVWhost/interscan" in your Web browser and authenticate the certificate.

Additional Information

After the configuration, you can use both the existing Web console connection via TCP port 1812 and SSL connection simultaneously.

If you need to disable an existing connection to use SSL exclusively, do the following:

1. Modify access.conf. If you have installed ISVW under the /opt/trend directory, please change the current directory as below, typing the following command:

```
# cd  /opt/trend/ISADMIN/IScan.adm/conf
```

2. Add the following 5 lines (from <Directory /> to </Directory> below) to the header of the "access.conf" file. Type the following command and lines:

```
# vi  access.conf


<Directory />
order deny, allow
allow from 127.0.0.1
deny from all
</Directory>
```

3. Send the HUP signal to the parent process of "IScanWeb" to reflect the information ("ps" is command output, and the parent process "PPID" is "1").

```
#  ps -eal | grep IScanWeb
F SUIDPIDPPID


8 S056881IScanWeb
8 S057565688IScanWeb
#  kill -HUP  5688
```

4. Access each of the following URLs, and confirm the status:
   - http://ISVWhost:1812/interscan: Confirm that the connection is refused.
   - https://ISVWhost/interscan: Confirm that HTTPS connection is available.

Opening the Web Console

After installation, InterScan will automatically stop and restart your daemons to initiate scanning. Although InterScan is configured to run on a robust set of default values, it's a good idea to open the configuration console to confirm or modify the settings to fit your 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 by default. The port is user-configurable.

   ```
   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

Note: InterScan VirusWall for CVP does not have individual controls for enabling/disabling scanning of the three different protocols. All network traffic will be stopped immediately after clicking **Turn On/Off**.

To enable/disable real-time scanning,

1. From the InterScan Web configuration menu, click **Turn On/Off**.
2. Click the button to toggle on/off CVP scanning. If you turn off the service, the screen will update and show that the service is off. The flow of traffic will continue without virus scanning.

Note: In InterScan VirusWall CVP edition, network traffic will stop immediately after clicking **Turn On/Off**. You cannot individually control scanning of each protocol.

Command line option for Solaris:

```
% /etc/rc2.d/S99IScvp stop
% /etc/rc2.d/S99IScvp start
```

To turn on/turn off InterScan,

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

Note: The InterScan VirusWall CVP version does not require you to select the network protocols that you want to disable. Network flow will stop immediately after clicking **Turn On/Off**.

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 Micro 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 Micro at:

`http://www.trendmicro.com/vinfo/testfiles/index.htm`

Once on your machine, you can use the test virus in email 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, located in the `opt/trend` directory:

```
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 installed on its host machine to send notification messages. If Sendmail is not 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 been 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 of 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.

Installed Files

In the CVP Edition, InterScan makes the following changes to your system:

Platform	*Directory*	*Action*	*Files/Modification*
Solaris	/opt/trend (user config.)	create dir	all files located within
Solaris	/etc/iscan	create dir	all files located within
Solaris	/etc/rc2.d	create	startup script creates S99IScvp, S99IScanHttpd and S99ISmailid
Solaris	/etc/rc2.d	create	startup script creates S99ISvcs *only if TVCS is installed

Upgrading from the Trial Version

To upgrade a trial version to the full version:

1. Save the /etc/iscan/intscan.ini file used by your trial version. This file contains configuration settings used by your trial version software.
2. Run InterScan's install script (./isinst) to uninstall the trial version.
3. Run the install script again to install the software, and enter the serial number when prompted.
4. Replace the default intscan.ini file from your installation with your saved version and restart InterScan VirusWall.

Chapter 5

Installing InterScan Sendmail Switch Edition

In this chapter you will find step-by-step instructions for installing InterScan VirusWall Sendmail Switch Edition (not available for the HP-UX or Linux platforms). Also included are instructions for:

- Configuring Sendmail to transfer mail to InterScan for virus scanning
- Opening the InterScan Web console
- Starting and stopping InterScan services
- Using a special test virus to check your setup
- Uninstalling Trend Micro InterScan VirusWall

Overview

The InterScan VirusWall Sendmail Switch Edition scans SMTP traffic for viruses. The Sendmail Switch Edition is for the Sendmail Switch mail server version 2.1.2 or later. By using Sendmail's Content Management API architecture, InterScan is easily configured and installed. Security is also enhanced because of the tight integration with Sendmail Switch.

Note: InterScan Sendmail Switch Edition can also be used with open source sendmail version 8.11.3. However, due to the complexity of configuring open source sendmail

to work in this environment, Trend Micro will not support any problems that may arise when setting up mail filtering in the open source environment.

InterScan receives inbound and/or outbound SMTP traffic from the Sendmail Switch program, scans it for viruses, and then routes it back to the same Sendmail Switch program for delivery as usual.

The InterScan Sendmail Switch Edition is designed to be installed on the same server as the Sendmail Switch product.

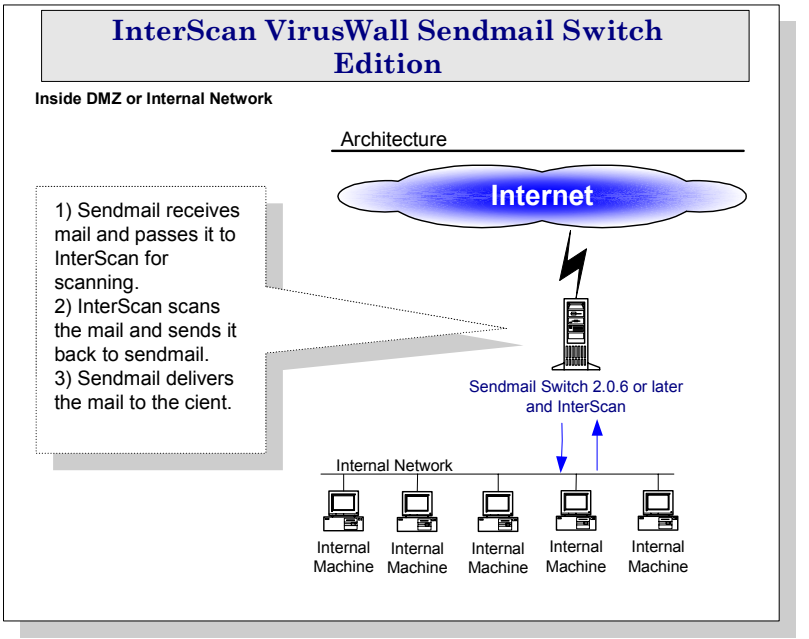


FIGURE 5-1. The InterScan Sendmail Switch Edition architecture greatly reduces the complexity of configuring SMTP virus scanning on the network. Sendmail always takes care of sending and receiving mail. There is no need to modify MX records or workstation configurations.

Installing the Sendmail Switch Edition

To install InterScan VirusWall Sendmail Switch Edition, you must be logged on to the target server as **root**. Installation takes about ten minutes and does not require you to restart the server.

1. If you are installing from the Trend Micro Enterprise Solutions CD, you need to mount Solutions CD #2 onto a Windows NT server, locate the directory where the files are located, `PROGRAMS/ISVWSOL`, and choose the English or Japanese version. FTP the program files to a UNIX server and untar them.
2. From the directory containing the InterScan installation files, type `./isinst` and press `Enter`.
3. If you have previously installed InterScan, the setup program will ask you to remove all packages before installing the Sendmail Switch Edition. Choose **yes** to remove all previous InterScan packages. You will be prompted to enter **Yes** for each package that needs to be removed.

Note: You **must** remove all InterScan packages to continue with the installation.

---

4. After removing all existing packages, a **Setup** menu appears showing the current InterScan system configuration. **None** indicates that the package is not installed. **Installed** indicates that the package is installed.

   Choose **Option 3** to install InterScan VirusWall Sendmail Switch Edition.

   By default, InterScan will install all available systems to subdirectories of `/opt/trend`.

5. Enter the serial number and hit `Enter`.

   Press `Enter` without typing in 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.trendmicro.com/buy`

6. The installation script will show the packages to be installed and give you an opportunity to modify the installation options. By default, the Base System, CGI

Admin, and Sendmail Switch Edition packages will be installed in English. If you wish to modify any of these options, choose one of the modification options from the menu. Then choose option 7, **Start Installation**, and press `Enter`.

7. If you want to install to a different directory, type in the path and press `Enter`.
8. Follow the prompts to complete the Setup. Once the setup is complete, return to the main menu and exit the program.

After Installing InterScan Sendmail Switch Edition...

After installing the InterScan program files, you need to install and configure Sendmail Switch for virus scanning to function properly. The following section describes how to install and configure Sendmail Switch.

Installing Sendmail Switch

The current instructions are for Sendmail Switch 2.1.2. Please consult your Sendmail Switch Installation Guide and Release Notes for the latest instructions.

Remove previous versions of Sendmail

It's a good idea to remove the previous versions of sendmail before installing Sendmail Switch. Use the `pkgrm` first to remove the older version of sendmail. After using `pkgrm`, manually remove all of the following files:

```
/etc/mail/sendmail*, /usr/lib/sendmail*,
/usr/sbin/sendmail*, /usr/local/sendmail*,
/etc/sendmail*, /etc/mail/*
```

Note: If you are currently a Sendmail Switch customer, you need to upgrade to version 2.1.2 or later, or apply the 2.1.2 patch in order to have Content Management API support.

Install Sendmail Switch

1. Locate the new sendmail package and type the following command:

```
pkgadd –d SMIswitch SMIswitch
```

In the installation process, Sendmail Switch 2.1.2 (or later) prompts you where to install the base package. For example, if you enter `/usr/local`, then Sendmail Switch creates a sub directory called *sendmail* under the specified `/usr/local` to install the base, for example, `/usr/local/sendmail`.

2. If you installed Sendmail Switch under /usr/local, then type:

   ```
   /usr/local/sendmail/smadmin-2.0.0/sbin/installer
   ```

   to install the Web-based configuration program.

   If you installed the Sendmail Switch on a machine named `emailhost.yourcompany.com`, then point your browser to `https://emailhost.yourcompany.com:2048/gui` to configure Sendmail Switch.

   When you log into the Web console's main menu for the first time, you should "create the new configuration" (`sendmail.cf`) first in order to start sendmail. We recommend that you accept all the default settings first to see if Sendmail Switch is working properly.

3. Test Sendmail Switch to make sure it is working properly before continuing with the configuration.

Configuring Sendmail Switch

1. Open the Sendmail Switch's Web configuration program and log into `https://[domain name or IP address]:8890/gui`
2. If you do not have a configuration, choose **New Configuration** and create a configuration before continuing.

3. Choose **Edit Existing Configuration**.

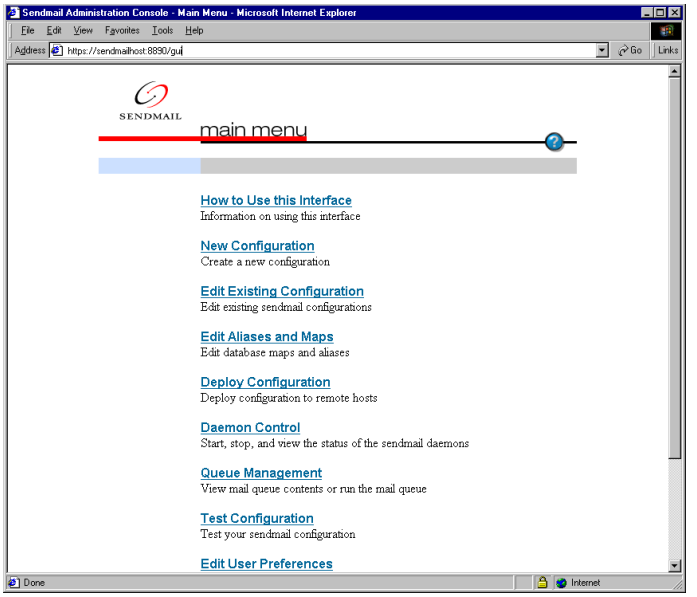


FIGURE 5-2. The Sendmail Switch main configuration page.

4. Load the configuration file. For example, `sendmail_switch.m4`.
5. Scroll down to the bottom of the page and click **Mail Filtering** on the sidebar menu.
6. Click **Add** to add the filter.

There are 2 input fields: one is **Filter Name** and the other is **Filter Equates**.

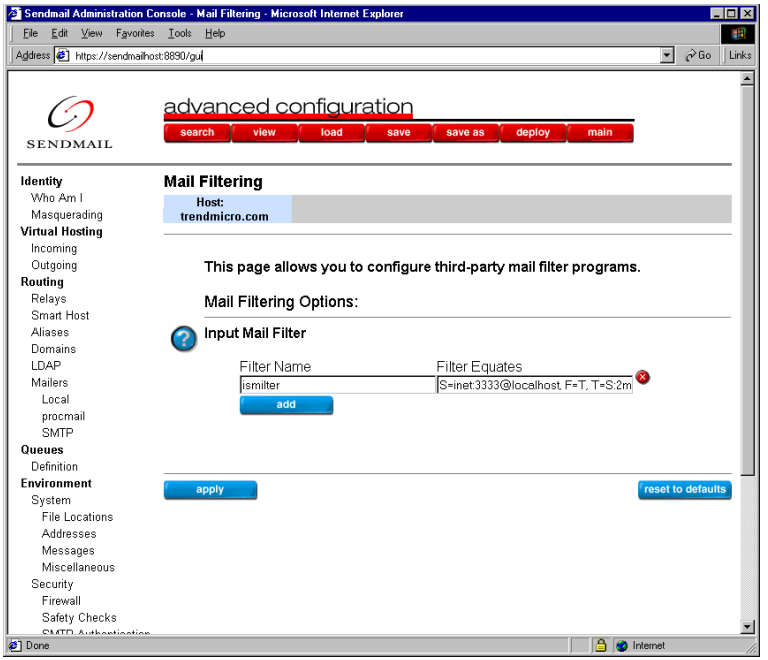


FIGURE 5-3. Mail filter options are set on this page.

7. Type `ismilter` into the **Filter Name** field and `S=inet:3333@localhost,F=T,T=S:2m;R:2m;E:5m` into the **Filter Equate** field. This is the recommended configuration for the **Filter Equates** field.
8. Click **Apply.** Once the changes are applied, you will need to "deploy" the changes to the `sendmail.cf` file for the changes to take effect.

9. Click **Deploy** on the top menu bar.

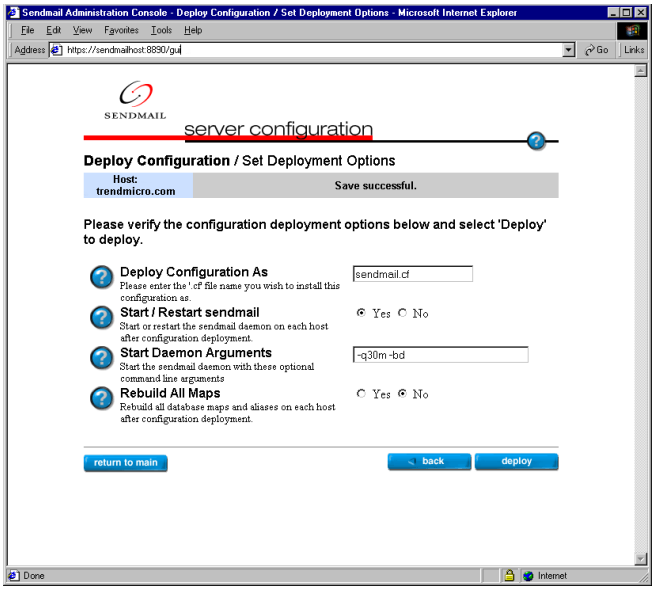


FIGURE 5-4. The picture shows the general deployment options.

10. Click the **Deploy** button on the lower right hand side of the page. Once finished, a confirmation page shows the results of the deployment.

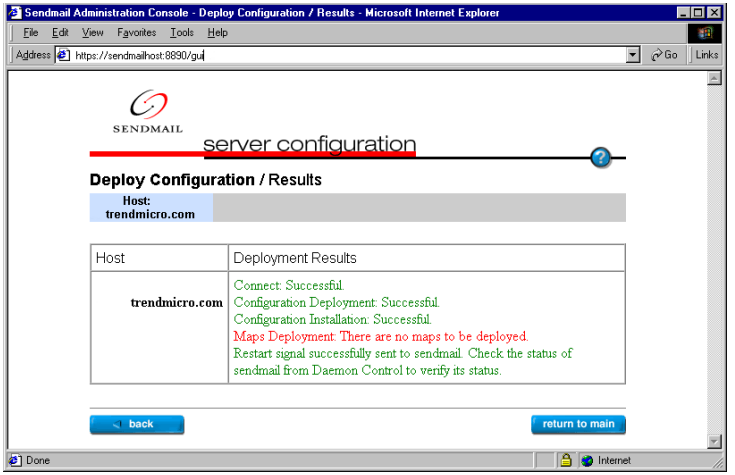


FIGURE 5-5. The deployment configuration results will be displayed after the deployment.

Filter Equates Explanations:

The Sendmail uses an IPv4 socket on port 3333 of localhost (S=inet:333). The current flags (F=) are:

R= Reject connection if filter is unavailable
T= Temporary fail connection if filter is unavailable

You can override the default timeouts used by Sendmail Switch when talking to the filters using the T= equate. There are three fields inside of the T= equate:

S = Timeout for sending information from the MTA to a filter
R= Timeout for reading reply from the filter
E = Overall timeout between sending end-of-message to filter and waiting for the final acknowledgment

T=S:2m;R:2s;E:5m where ‘s’ is seconds and ‘m’ is minutes. These are the recommended timeout settings.

Configuring InterScan Sendmail Switch Edition

By default, InterScan VirusWall Sendmail Switch Edition will create the following parameters in the [ismilter] section of the `intscan.ini` file:

```
svcport=inet:3333
logfile=/etc/iscan/log
```

Email scanning services will start automatically after the installation with the default configuration.

Note: If you change the default values in the `sendmail.cf` file, you will need to modify the values in the `intscan.ini` file and restart the InterScan service.

Opening the Web Console

After installation, InterScan will automatically stop and restart your daemons to initiate scanning. Although InterScan is configured to run on a robust set of default values, it's a good idea to open the configuration console to confirm or modify the settings to fit your 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 by default. The port is user-configurable.

   ```
   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, the InterScan service is enabled upon installation. The Sendmail Switch Edition is controlled, however, according to the following options:

- Enable/disable real-time scanning
- Turn on/turn off virus scanning

To enable/disable real-time scanning,

1. From the InterScan Web configuration menu, click **Turn On/Off**.
2. Click the button to toggle on/off email virus scanning. If you turn off the service, the screen will update and show that the service is off. The flow of traffic will stop until you either turn virus scanning back on or update the sendmail configuration without *milter*.

Command line options for Solaris:

```
% /etc/rc2.d/S87ISsml stop
% /etc/rc2.d/S87ISsml 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 5-6. The default username and password are "admin".

Testing InterScan VirusWall

Once Trend Micro InterScan 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 Micro at:

`http://www.trendmicro.com/vinfo/testfiles/index.htm`

Once on your machine, you can use the test virus in email to test SMTP scanning.

Uninstalling InterScan

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

1. To remove InterScan VirusWall, 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 uninstall.

Note: When changing from InterScan Standard to InterScan Sendmail Switch Edition, you'll be prompted to uninstall all previously installed InterScan packages.

Installed Files

In the Sendmail Switch Edition, InterScan makes the following changes to your system:

Platform	*Directory*	*Action*	*Files/Modification*
Solaris	/opt/trend (user config.)	create dir	all files located within
Solaris	/etc/iscan	create dir	all files located within
Solaris	/etc/rc2.d	create	startup script creates S87ISsml
Solaris	/etc/rc2.d	create	startup script creates S99ISvcs *only if TVCS is installed

Upgrading from the Trial Version

To upgrade a trial version to the full version:

1. Save the `/etc/iscan/intscan.ini` file used by your trial version. This file contains configuration settings used by your trial version software.
2. Run InterScan's install script (`./isinst`) to uninstall the trial version.
3. Run the install script again to install the software, and enter the serial number when prompted.
4. Replace the default `intscan.ini` file from your installation with your saved version and restart InterScan VirusWall.

Chapter 6

E-mail VirusWall & Anti-Spam Control

E-mail VirusWall scans all inbound and outbound messages for viruses. It can be installed and configured to support a variety of network configurations, including scanning for a Sendmail program on the same or a different machine, and scanning for other SMTP servers. **Important:** How you configure the **Main Service port** option in the Email Scan page depends on the installation topology you have chosen. See Chapter 2 for illustrated examples.

Enabling or disabling Email Scan

E-mail VirusWall, like all the VirusWalls, can be **Enabled** or **Disabled** from the **Configuration** page.

1. In the menu on the left, click **Configuration**.
2. In the **Real-time Scan** section, click the box next to **Email Scan**:
   - A check means real-time scanning is enabled
   - No check means real-time scanning is *not* enabled

Configuring Email 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 email attachment types to scan, who should be notified when a virus is discovered, what action should be taken—clean, delete, move, or pass it on to the recipient along with a warning message.

E-mail VirusWall features include:

- Real-time scanning of inbound *and* outbound email traffic
- Automatic, customizable virus notifications
- Option to **Clean**, **Move**, **Delete** or **Pass** on infected files
- Message-size filtering
- File-name checking to guard against the "email security flaw"
- Ability to insert customized tag line in 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 program 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 VirusWall** depends upon the installation topology you have selected.

Email Scan Configuration

Email routing

On the Email Scan Configuration page, you define the path that email takes to get to the client after it enters through the gateway and the resources used to make the journey. The path is from the firewall, through InterScan, then to the client. The resources are the ports used, email servers and services that aid the journey. The following parameters need to be set to create the email routing path.

Main service port

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

Original SMTP server location

The Original SMTP server is the server that will deliver the message after it has been scanned for viruses. InterScan VirusWall for UNIX is not an MTA, therefore it needs to send the mail to an SMTP server after scanning. The Original SMTP server can also be thought of as the "delivery" SMTP server.

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

- Command mode is used only when the MTA is on the local server. The MTA can be sendmail or any other SMTP server program. Each time a message is delivered, an instance of sendmail (or other MTA) is opened to deliver the message. Once the message is delivered, sendmail automatically closes. This process is repeated for each message that needs to be delivered.
- Daemon mode has the SMTP server program running continuously in the background. If you decide to run the SMTP server program in daemon mode, you choose the port that it will run on. The program will automatically start when InterScan starts up.

If you choose to have a remote server deliver the messages after scanning, you will only be able to configure it in daemon mode. You must enter the remote host name or IP address of the server and its port number.

Using Sendmail

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

1. Select **Configuration > Email Scan** to load the *Email Scan Configuration* page. Specify the port on which E-mail VirusWall will listen for SMTP connections (e.g., 25) in the **Main service port** field.
2. Specify the location of your Sendmail program in the **Original SMTP server location:** field. Choose either Daemon mode or Command mode. For example, if you intend to run sendmail in command mode, you would select **Command mode** and type the following in the field provided:

   /usr/lib/sendmail -bs

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

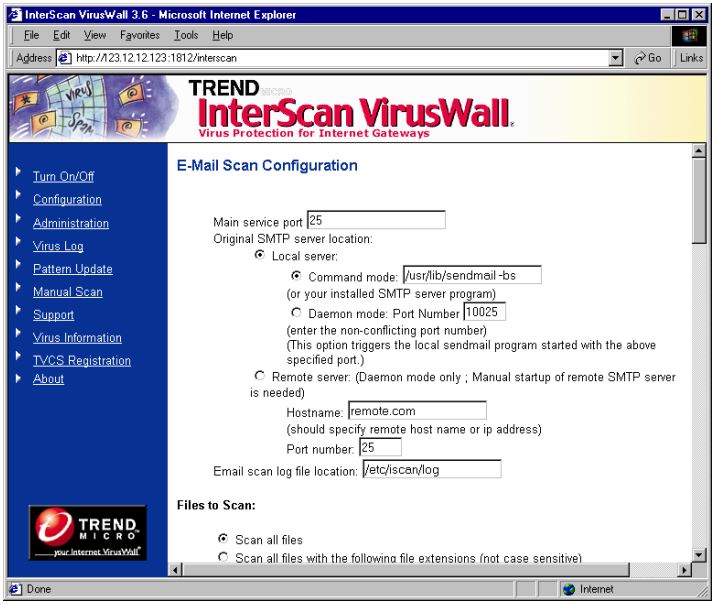


FIGURE 6-1. Your SMTP Service settings depend on where E-mail VirusWall is installed and the Edition you are running.

Note: The owner of the InterScan process is "`iscan`". Since stopping or starting the sendmail daemon must be performed with a "root" credential, it cannot be stopped or started from the UI when InterScan VirusWall is running in daemon mode. You will thus have to run the /etc/rc2.d/S88sendmail start command after modifying the email scan configuration.

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 your SMTP server to use another port, for example 5000.
3. In the **Original SMTP server location:** field, enter the location of your SMTP server followed by the new port that it will use. For example, a typical command mode setting for a local server would look similar to the following:

   ```
   localhost 5000
   ```

   Testing: Use Telnet (or a similar program) to Telnet to the InterScan IP and port and/or the SMTP server IP and port you have specified for these fields. By observing the response, you can identify and then eliminate most configuration issues.

If E-mail VirusWall 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, choose **Remote server** and specify the hostname (or IP address) and port of your SMTP server.

Using sendmail's anti-spam and anti-relay features

If you want to use *sendmail's* anti-spam and anti-relay features, you will need to use the *sandwich* configurations. The *sandwich* configurations are used specifically to enable the *sendmail* anti-spam and anti-relay features.

Email Scan Log File Location

The email scan log file location is the location of the system log for the email scan service. When you use the default location for all of the services, they will be combined into one log file. If you change the location for any of the services, that service will have a separate log file for that service. The system log file records system events, such as errors, and stopping and starting services.

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 email attachments for viruses, including individual files within a compressed volume.

Priority for Email Scanning Configuration

If your configurations on the *Email Scan Configuration* screen conflict with each other, the program will scan according to the following priority:

1. "File types to block"
2. "Files to scan"

To select which files to scan,

1. To scan all email attachments regardless of type, go to the **Configuration > Email Scan** page and click the **Scan all files** radio button. This is the most secure configuration.
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.

   The following files are shown in the file type field:

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

   You can also choose from the following file types, which potentially carry viruses:

```
.BIN .COM .DOC .DOT .DRV .EXE .SHS .SYS .XLS .XLA
.XLT .VBS .JS .HLP .HTML .HTM .CLA .CLASS .SCR
.MDB .PPT .POT .DLL .OCX .OVL .ARJ .CAB .GZ .LZH
.ZIP .RAR .Z .TAR
```

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 files 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.

To specify which files to block,

You can explicitly state the types of file attachments that you want to block.

1. Check *Block the following file types*.
2. Enable the file types that you want to block.

For more information about how file types are classified, see *File Type Classifications* starting on page 6-8. To enter *Other types*, enter the *File Type* name that you want to block.

Note: InterScan VirusWall determines the type of message attachment by its true content type. However, it cannot determine the content type when the message is BINHEX-encoded. Since BINHEX-encoded messages are classified as "Executables", you can block all BINHEX-encoded messages by enabling the "Executables" option button. Otherwise, Java applets, Executables, Office documents, etc. will not be blocked when the message is BINHEX-encoded.

Adding Explanations to the Message

If a file is blocked by InterScan VirusWall, you can choose to have some explanatory text inserted into the message body. You can either choose to add a default

explanation, append a customized message to the message text or replace the message body with a customized explanation. If choosing to use a custom explanation, type the text of the explanation in the appropriate text box.

Sending Notifications

If you want to notify the sender, recipient and/or administrator that InterScan VirusWall blocked a message, enable the appropriate *Send notification email* option button and type the content of the notification email message that will be sent.

File Type Classifications

The following table shows how true file types are classified on the InterScan VirusWall management console's user interface. In addition, you can enter a specific *File Type*.

Compressed Archives

File Type	File Type Explanation
mscomp	MSCOMP
cpio	cpioarchive
lha	LHA
ar	ararchive
tar	TAR
rar	RAR
arj	ARJ
gzip	GNUzip
zip	PKZIP
mscab	MSCabinet

Audio and Video File

File Type	File Type Explanation
av	Audio
wav	MicrosoftRIFF
midi	MIDI
mp3	MP3
voc	CreativeVoiceFormat (VOC)

Executable Files

File Type	File Type Explanation
com	COM file
exec	executable
com	DOS COM
exe	DOS EXE

File Type	File Type Explanation
lnk	Windows NT/95 shortcut
other	Compiled Term Info Entry
binhex	BINHEX
base64	MimeBase64

Java Files

File Type	File Type Explanation
java	java app
java	Java applet

Office Files

File Type	File Type Explanation
msdoc	MS Word
msppt	MS PowerPoint
msexl	MS Excel 95/97
mswri	Windows Write
mscal	Windows Calendar
msmdb	MS Access
msproj	MS Project
doc	Wordperfect
msdoc	MSWORD/DOS 4.0/5.0
hlp	HLP
afm	Adobe Font Metrics
fm	Framemaker document
ps	Postscript
rtf	Microsoft RTF
pdf	Adobe Portable Document Format (PDF)

Picture File Types

File Type	File Type Explanation
icon	Windows icon
pcx	PC Paintbrush

File Type	File Type Explanation
fli	Autodesk Animator (FLI)
bmp	Windows BMP
jpeg	JPEG
tiff	TIFF
ras	SUNRaster (RAS)
psd	Adobe Photoshop (PSD)
gif	GIF

Text File and Unknown File Types

File Type	File Type Explanation
vbs	VBScript
sbf	Script File Type
txt	ASCII text
unknown	Unknown file type
elf	ELF
emty	emtyfile (size)

Setting Virus Notifications

Upon detecting a virus, InterScan can send an automatic email 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 email 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 (**Email to administrator** or **Warning**).
2. For the administrator, enter the email address (**root**, for example) in the associated text box. For the Sender or Recipient, the address is taken from the email.

Note: Multiple email 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: Detailed Description
%a = Action taken: Delete, Move, Pass
%d = Date virus was detected
%F = File where virus was detected
%f = For email, identifies sender
%v = Virus name
%t = For email, identifies recipient
%M = When action is move, displays the destination directory and filename
%m = Detection method
%h = Host name
%r = traffic direction (either inbound or outbound)

For example,

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

which reads, "Warning! On **3-22-01**, InterScan detected the **Jerusalem** virus in the file: **Word.com.** InterScan took the following action: **delete**."

Specifying Notification Delivery Server

In order to be able to send notifications, you will need to specify the SMTP server that will deliver the notification messages.

Note: If no notification server is specified, no notifications will be sent.

---

1. Go to the **Administration** page in the InterScan Web console.
2. Under the **Notifications** section, enter the following two parameters:

- Notification server:
  Type in the name of the notification server using the domain name or IP address. The default setting, *localhost*, can be used if your SMTP server is on the same machine as InterScan.
- SMTP Server port:
  Enter the service port that the notifications server is using. The default is the standard SMTP port used on the Internet: 25. Choose another port if you have modified your SMTP server port settings.
- Mail daemon interval:
  A notification will be sent to the administrator to warn when there is a backlog in the mail queue. Enter the time interval between checking the mail queue.
- Mail queue path:
  The path used by the mail delivery daemon for the queue is shown under the Notification settings. It is not configurable.
- Mail delivery daemon log file:
  The location of the log file where the mail daemon will record status messages is shown under the Notification settings. It is not configurable.

Setting the Action on Viruses

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

- Choose **Pass** to send the infected file, along with a warning message and the original message text, to the recipient *without cleaning*.

- Choose **Quarantine** 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 email 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 **Quarantine** to deliver the message text to the recipient, but quarantine the infected file.
  - Choose **Delete** to send the message text on to the recipient and delete the infected file

.

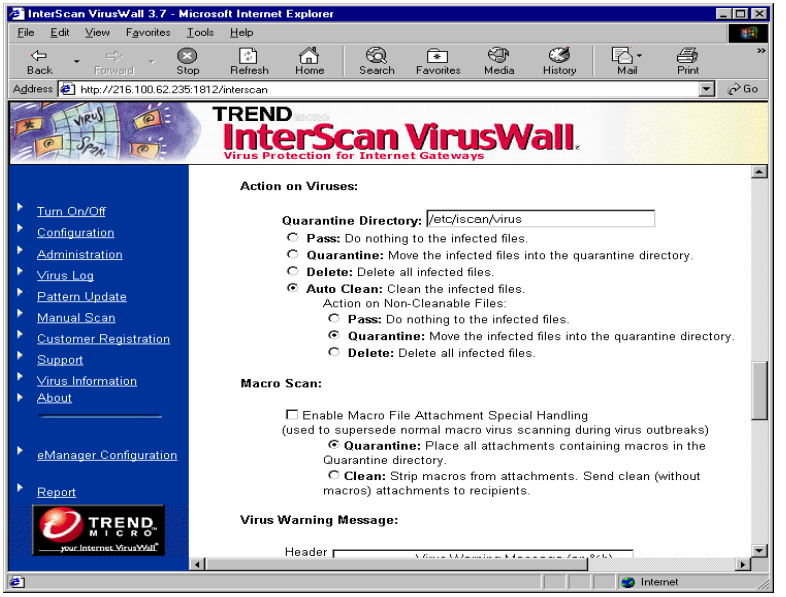


FIGURE 6-2. InterScan can take a variety of actions on infected files.

Macro Scan

The scan engine scans for macro viruses during normal operation. However, there are situations when a new macro virus infects a company and no virus pattern file is available to catch the macro virus. Macro Scan can stop all attachments containing macros from entering through the Internet gateway, until a new pattern file can be developed to catch the virus.

Macro Scan detects macros in file attachments and provides two scanning options: **Quarantine** and **Clean**. Select **Enable Macro Scan** to use this feature, then choose **Quarantine** or **Clean**.

- **Quarantine** will remove the attachment if it contains a macro and place it in the `Quarantine` directory.
- **Clean** will strip of the macro before delivering the email with the attachment.

Adding additional messages

1. Check **Additional Message** to have InterScan insert a brief note to the top of any email in which a virus is found. In the associated text field, enter your message. The additional message is sent to the recipient.
2. Check **Stamp** to have InterScan insert a brief note to the top of scanned messages letting users know that their email was scanned and found to be virus free.

   Use %F if you want InterScan to include the name of the file(s) scanned.

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

Adding Header/Tail Lines to Notification Messages

To frame your notification messages with rules above and/or below the notification text, go to the *Virus Warning Message* section of the *Email Scan Configuration* screen. You can then specify the *Header* and *Tail* lines for notification messages and the *Header* line for a Safe Stamp message.

Miscellaneous

The miscellaneous section contains a number of options that enhance the functionality of InterScan. Most of these options have been developed because of new developments in anti-virus scanning. Review the following options and decide which of these are appropriate for your security policy.

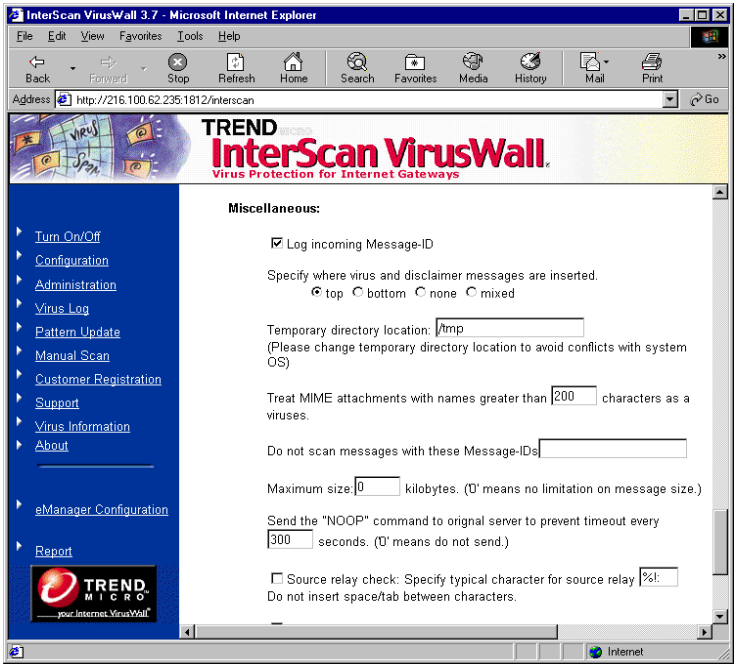


FIGURE 6-3. Miscellaneous options on the Email Scan page.

Log and skip scan Message IDs

InterScan has the ability to log the message ID and bypass scanning according to unique message IDs. This feature is used when InterScan encounters unique problem cases. If a specific email causes InterScan to crash, the MTA (Mail Transfer Agent) will recognize that InterScan is down and attempt to resend the email after a specific period of time. The problem will recur as long as the same message is being resent.

The problem email message ID can be identified in the log and entered into the **Do not scan messages with these Message-IDs** field to solve this problem. Before allowing the message to pass, make sure that it is not infected.

Prevent sendmail time-outs

Select **Send NOOP command to original server** to prevent sendmail timeouts. If sendmail times-out, InterScan will spawn another sendmail *process* to deliver email. This could impact performance. The default setting is 300 seconds.

Enable eManager plug-in

If you have installed eManager, the optional InterScan plug-in, you will need to configure InterScan to recognize and enable eManager. The following tasks must be done in the sequence shown to enable eManager.

1. Click **Configuration: Email Scan**. (Make sure the box is checked and email scan is active.)
2. Scroll down to the bottom of the page and check the box next to **Enable Plug-Ins**.
3. Go to the **Turn On/Off** page. Turn the **Mail** button **Off**, then back **On** by clicking on the image.

InterScan eManager in now enabled and active.

Specify virus and disclaimer message location

This option allows you to determine where in the email the virus warning message and/or disclaimer will appear: **top**, **bottom**, or **none**. By default, **top** is selected.

Note: If you choose **none**, no virus or disclaimer message is sent. So, if you have configured InterScan to send notification messages, choose either **top** or **bottom**.

Temporary Directory Location

By default, InterScan uses the `/tmp` to do the work of scanning for viruses. When InterScan receives a file (any type that it is configured to scan) it places a copy in a temporary directory for scanning. The directory location is configurable. Be sure to specify a directory with at least 256MB available free space.

Note: We recommend that you change the default setting of the temporary directory to avoid conflicts with the system OS or other programs that use the default temporary directory.

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).

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

2. Alternatively, enter a zero (0) to have InterScan process all messages, regardless of size.

Configuring Wildcard Characters

If you want to configure the wildcard characters used for source relay checking, enable the Source relay check option button and then type the character(s) in the text box.

Protecting Against Long Attachment Names

E-mail VirusWall solves the long attachment name problem discovered in 1998 and found to affect many email client programs. Malicious users can exploit the flaw by emailing an attachment with a very long file name to vulnerable machines. The 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 (e.g., more than 200 characters), and deletes any message containing an attachment with a very long file name—the message is not routed to the SMTP server or otherwise processed.

Because the action is delete, be sure to specify a sufficiently large number in this field (200 characters or more) or you risk losing messages that are not a security threat.

To protect against the Email 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 email attachment file name. A record of the event and a copy of the attachment are kept in the log.

Additional Email Options

The **Additional Email Options** page contains features that are related to outbound mail processing and enabling anti-relay. You can access the page by scrolling to the bottom of the **Email Scan** page and clicking on the **Additional Email Options** button.

E-mail VirusWall checks all SMTP traffic before relaying it to your SMTP server (i.e., both inbound and outbound). In addition to virus checking, additional options are available for outbound messages:

- You can block infected messages and notify the sender and/or administrator (the recipient is not notified)
- You can insert a standard tag line, or disclaimer, in 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.

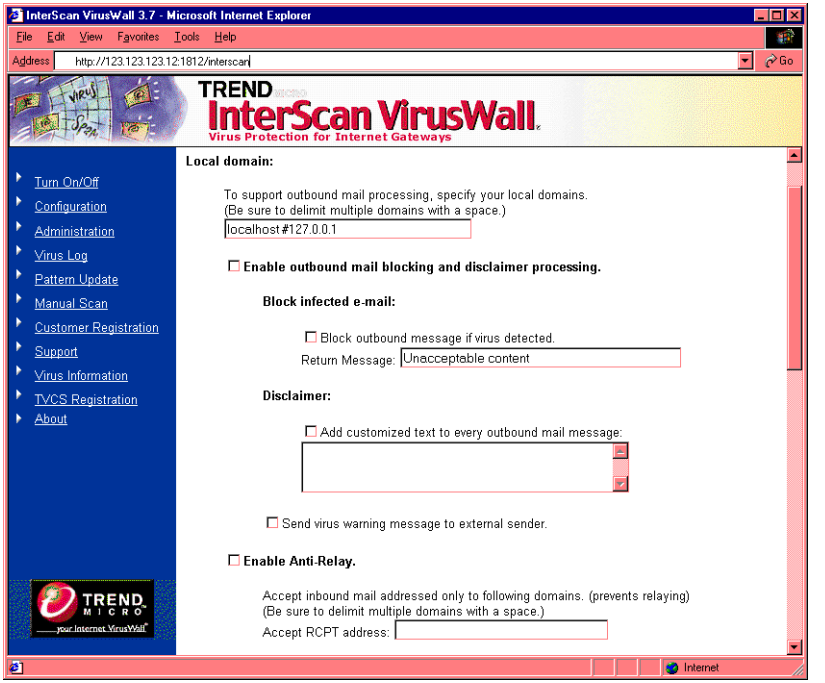


FIGURE 6-4. InterScan can stop delivery of infected outbound messages and/or insert a standard message at the top of outbound mail.

To block infected outbound messages...

1. From the **Email Scan** page, click the **Additional Email Options** button at the bottom of the screen.
2. Check **Enable outbound mail blocking and disclaimer processing**. This option must be checked for outbound email scanning and/or appending additional message text to occur.
3. Enter your local domain or sub-domain (or *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. Also, if you want to specify many sub-domains, you can indicate a file name with the format `/etc/iscan/trustedhost.list`. Separate each entry in the file with a end of line [Enter].

4. Check **Block outbound message if virus detected** to have E-mail VirusWall stop the delivery of infected email. You can also configure the *Return Message* that the sender receives. Infected messages 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 recipient of a blocked message will not receive the email and will not be notified. The Sender and Administrator are always notified, independent of the optional Notification setting.

Disclaimer

5. Choose **Add customized text to every outbound mail message** and enter the message you want appended to the top of outbound email 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."

Anti-relay

If you select anti-relay, you can prevent your server from being used to relay spam. Spam mail can be classified 2 types. One is sent directly; another one is sent indirectly by using SMTP servers on other networks. Anti-relay will prevent your server from being used to relay spam.

Anti-relay feature contains 2 steps:

1. Determine which domains are inside the network for which you want to receive messages.

2. Select **Anti-Relay** and enter the domains in the **Accept RCPT address** field.
3. Click **Apply**.

For example, the domain for Trend Micro Japan is trendmicro.co.jp. You would enter that domain in the **Accept RCPT address** field. If recipient address is `username@trendmicro.co.jp`, it is accepted and if not, it is rejected.

Forwarding Messages to Dedicated MTAs

When multiple MTAs are present in your network environment, the mail traffic relayed through InterScan can be customized so that messages originating from certain hosts are forwarded to a specific MTA. This is done using the *Forward Messages for Final Processing* function.

To forward messages from certain hosts to dedicated MTAs:

1. Check the *Enable message redirection* option.
2. For each set of originating hosts whose messages you want to forward to a dedicated MTA, click the *source host* option and:
   a. Enter the source host(s), delimiting multiple hosts with a space.
   b. Enter the recipient *MTA*'s IP addess (or name) and port that you want to use to process messages from the originating hosts that you have configured. The format <IP address>:port should be used, e.g., 123.123.123.12:25.

3. When finished entering the sets of originating host(s) and recipient MTA(s), click the **Apply** button.

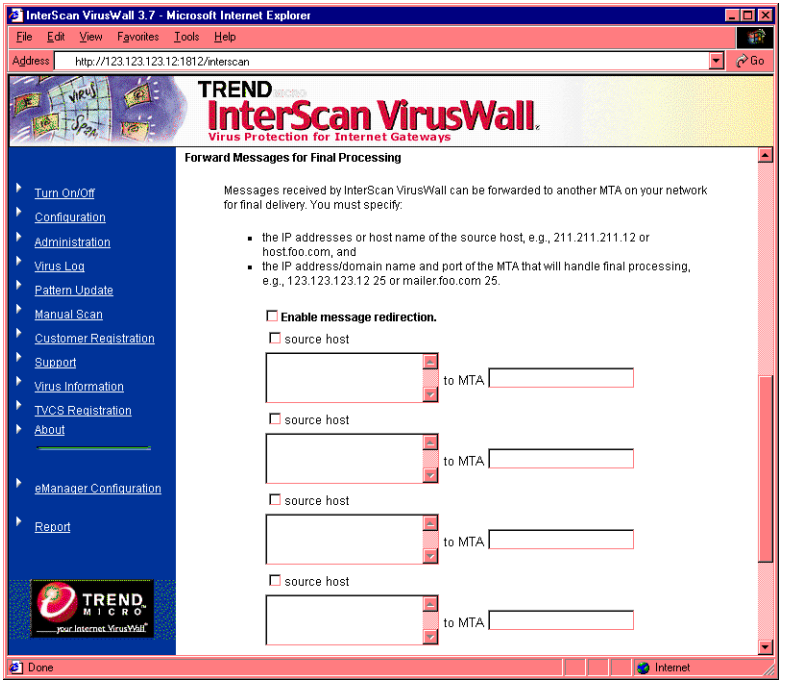


FIGURE 6-5. Multiple relay direction

You can enable or disable each "Sender-Recipient" combination according to your current network structure. When a "Sender-Recipient" combination is checked, all mail coming from the sender host will be relayed to the recipient MTA for delivery. If a sender host is not found or is unchecked, the original server (the host which InterScan VirusWall is installed upon) will be used to deliver mail.

You can specify up to 5 different "Sender-Recipient" combinations which describe 5 different traffic routes to your MTAs. A list of such combinations can be found in `/etc/iscan/direction.ini`.

Email Scan Advanced Configuration

Note: Advanced Options only pertains to InterScan *Standard* Edition. This section does not apply to the *CVP* Edition.

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.

For E-mail VirusWall, the default values are optimal for most cases.

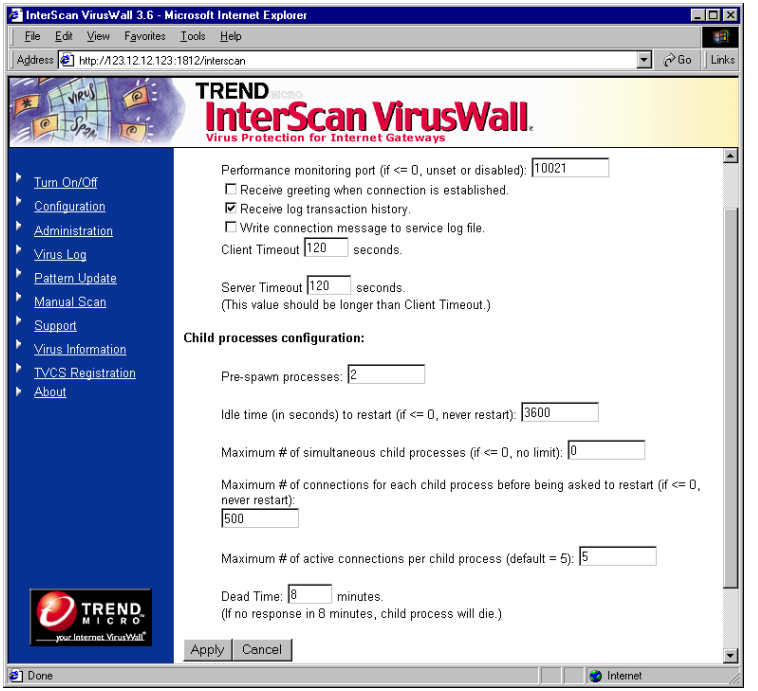


FIGURE 6-6. Child process configuration allows you to fine tune InterScan performance according to your system needs.

To edit the Advanced Options,

1. Open the InterScan console and click **Configuration > Email Scan** in the menu that appears on the left.
2. Scroll to the bottom of the Email Scan page that appears and click the **Advanced...** button.

Performance Monitoring

You can view real-time performance statistics by using performance monitoring. The default port is shown in the performance monitoring field in the GUI. The port number is configurable.

To monitor performance,

1. From the command line, go to the `etc/iscan` directory.
2. Type `perfmon [port number]` and press **Enter**.

The performance monitor will show the following:

- master process ID
- Start date
- Connections served
- Number of child processes forked

For each child process that is spawned by the master process:

- master process ID
- Start date
- Connections served
- idle time
- number of threads for example (1 / 5), which means 1 active out of 5 available threads

Receive Greeting

You can configure InterScan to send a greeting when you telnet into any port that InterScan is operating on. The greeting will display basic product information.

Logging Transactions...

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

You can specify where InterScan keeps its logs on the **Configuration** page.

Write connection message to service log file

When this option is disabled, only the IP address is logged as a connection message and InterScan VirusWall will not convert the IP address to a hostname. When the option is enabled, InterScan VirusWall will convert the IP address to a hostname.

Client/Server Timeout Settings

This feature is used to avoid having processes wait indefinitely for a reply from either server or client. Set this feature for each service.

Child Process Configuration

You can fine-tune InterScan's performance by making adjustments to settings such as 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 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 number 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 **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, this option exists to allow you to set a maximum if necessary.

Whenever the maximum number of child processes is reached, InterScan will stop spawning new threads; additional 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 redeliveries).

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 is 500, meaning that after 500 threads have been generated and extinguished, the hosting child process itself is extinguished and a new one generated (a new child is only 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 can contribute to system instability.

Dead Time

This feature will kill a slave process after a set amount of time if it does not terminate normally. Sometimes a slave process will not terminate normally due to some problem, which can cause a performance degradation. The default setting is 8 minutes.

Saving the configuration

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

Working with the *Sendmail* Anti-Spam Feature

To configure E-mail VirusWall to work with the *sendmail* anti-spam feature, you must use one of the following three topologies:

A. E-mail VirusWall and *sendmail* are installed on the same box. Only one *sendmail* daemon is running alongside E-mail VirusWall. For light network traffic only.

This configuration will have reduced server performance because InterScan delivers mail after scanning. The reduced server performance occurs when InterScan starts the *sendmail* program to deliver the mail. The performance hit is directly proportional to the time and resources required to spawn an additional daemon to deliver the mail. Not recommended for systems with heavy mail traffic.

B. E-mail VirusWall and *sendmail* are installed on the same box. Two *sendmail* daemons are spawned to enhance performance. For medium to heavy network traffic.

C. *sendmail* is running on two different Unix boxes. This is the preferred configuration for heavy mail traffic.

A. *sendmail* and E-mail VirusWall on one box—spawn one daemon

The following instructions provide the details to setup InterScan and *sendmail* on a single Unix box. Only one *sendmail* daemon runs alongside InterScan.

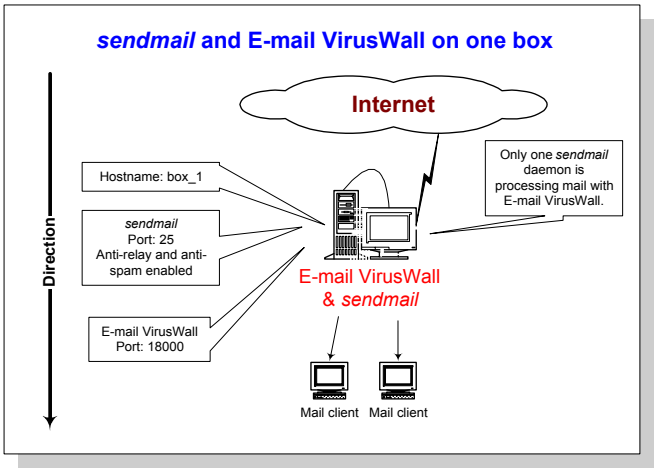


FIGURE 6-7. Illustration shows a sendmail daemon and InterScan running of the same machine.

Configure *sendmail*,

1. Make a copy of `sendmail.cf` file called `sendmail.cf.delivery`.
2. Change the A option in `Sendmail.cf` for Msmtp, Mesmtp, Msmtp8, and Mrelay from "`IPC $h`" to "`IPC localhost 18000`" where 18000 is an arbitrary free port on box_1.

Note: Port 18000 is an arbitrary port number. Please select a free port when doing the configuration below. Port 25 is the standard SMTP port. This should not be changed.

---

3. Add the k flag to the F option for Msmtp, Mesmtp, Msmtp8, and Mrelay in `sendmail.cf`.

   For example, the changes for Msmtp should look as follows:

Before:

```
Msmtp,P=[IPC],F=mDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC $h
```

After:

```
Msmtp,P=[IPC],F=kmDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC localhost 18000
```

4. Replace the local mailer with [IPC] for Mlocal in `sendmail.cf`.
5. Change the A option to "IPC localhost 18000" for Mlocal in `sendmail.cf`.
6. Add the k flag to the F option for Mlocal in `sendmail.cf`.

   For example, the changes for Msmtp should look as follows:

   Before:

```
Mlocal,P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9,
S=10/30, R=20/40,
T=DNS/RFC822/X-Unix,
A=mail.local -d $u
```

   After:

```
Mlocal,P=[IPC], F=klsDFMAw5:/|@qSmn9, S=10/30,
R=20/40,
T=DNS/RFC822/X-Unix,
A=IPC localhost 18000
```

Note: Make sure the F option of Mlocal does **not** include the 'f' flag. This flag is standard on Solaris 7 distribution of *sendmail* and needs to be removed.

Configure the delivery mail queue used by InterScan,

1. Change the mail queue to a different directory in `sendmail.cf.delivery`.

   Before:

```
O QueueDirectory=/var/spool/mqueue
```

   After:

```
O QueueDirectory=/var/spool/mqueue1
```

2. Create the directory `/var/spool/mqueue1` and make sure it has the same ownership and permission as the original in `/var/spool/mqueue`.
3. Add the k flag to the F option for Mlocal, Msmtp, Mesmtp, Msmtp8, and Mrelay in `sendmail.cf.delivery`.

Configure InterScan,

1. Make sure the Standard Edition of ISVW is installed, *not* the Sendmail Edition.
2. Edit `intscan.ini` and change the InterScan SMTP service port to 18000.
3. In `intscan.ini`, change the original SMTP server location to include "`-C /etc/mail/sendmail.cf.delivery`" where the `sendmail.cf.delivery` file is assumed to be in `/etc/mail`.

Under [smtp],

Before:

```
svcport=25
original=/usr/lib/sendmail -bs
```

After:

```
svcport=18000
original=/usr/lib/sendmail -bs -C/etc/mail/sendmail.cf.delivery
```

4. Restart InterScan SMTP by "`/etc/iscan/sendmail`".
5. Restart a new *sendmail* daemon to process the new mail queue by "`/usr/lib/sendmail -q1h -C/etc/mail/sendmail.cf.delivery`"
6. Restart *sendmail* to handle SMTP traffic on port 25 by "`/usr/lib/sendmail -bd -q1h`".

Note: Although there is a second *sendmail* daemon running, this daemon's only responsibility is to process any mail that has been queued up. If this second daemon is not running, then the user will need to manually and periodically flush the queue.

The S88sendmail rc script must be modified to correctly start the mail servers: The start script should now start 3 daemons (started in steps 12, 13, and 14).

Under start section of the script,

Before:

```
/etc/iscan/sendmail; /usr/lib/sendmail -q1h
```

After:

```
/etc/iscan/sendmail; /usr/lib/sendmail -q1h
-C/etc/mail/sendmail.cf.delivery; /usr/lib/sendmail -bd -q1h
```

B. *sendmail* and E-mail VirusWall on one box—spawn two daemons

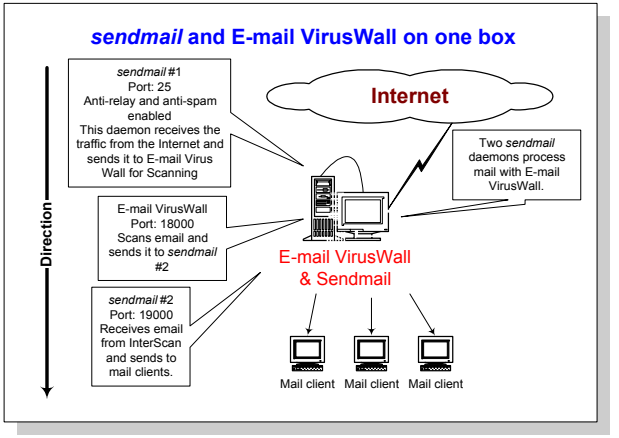


FIGURE 6-8. The illustration shows two *sendmail* daemons and InterScan on the same Unix box.

The instructions to configure the mail daemons for this configuration are as follows.

Configure *sendmail* #1,

1. Make a copy of `sendmail.cf` file called `sendmail.cf.delivery`.
2. Change the A option in `Sendmail.cf` for Msmtp, Mesmtp, Msmtp8, and Mrelay from "`IPC $h`" to "`IPC localhost 18000`" where 18000 is an arbitrary free port on box_1.

Note: Port 18000 and 19000 are arbitrary port numbers. Please replace with free ports when doing the configuration below. Port 25 is the standard SMTP port. This should not be changed.

---

3. Add the k flag to the F option for Msmtp, Mesmtp, Msmtp8, and Mrelay in `sendmail.cf`.

   For example, the changes for Msmtp should look as follows:

Before:

```
Msmtp, P=[IPC],F=mDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC $h
```

After:

```
Msmtp,P=[IPC],F=kmDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC localhost 18000
```

4. Replace the local mailer with [IPC] for Mlocal in `sendmail.cf`.
5. Change the A option to "IPC localhost 18000" for Mlocal in `sendmail.cf`.
6. Add the k flag to the F option for Mlocal in `sendmail.cf`.

   For example, the changes for Mlocal should look as follows:

Before:

```
Mlocal,P=/usr/lib/mail.local,F=lsDFMAw5:/|@qfSmn9,S=10/30,R=20/40,
T=DNS/RFC822/X-Unix,
A=mail.local -d $u
```

After:

```
Mlocal,P=[IPC],F=klsDFMAw5:/|@qSmn9,S=10/30,R=20/40,
T=DNS/RFC822/X-Unix,
A=IPC localhost 18000
```

Note: IMPORTANT: Make sure the F option of Mlocal does not include the 'f' flag. This flag is standard on Solaris 7 distribution of *sendmail* and needs to be removed.

Configure *sendmail* #2,

1. Change the port to listen on 19000 in `sendmail.cf.delivery`.

   Before:

```
#O DaemonPortOptions=Port=esmtp
```

   After:

```
O DaemonPortOptions=Port=19000
```

2. Change the mail queue to a different directory in `sendmail.cf`.delivery.

Before:

```
O QueueDirectory=/var/spool/mqueue
```

After:

```
O QueueDirectory=/var/spool/mqueue1
```

3. Create the directory `/var/spool/mqueue1` and make sure it has the same ownership and permission as the original in `/var/spool/mqueue`.
4. Add the k flag to the F option for Mlocal, Msmtp, Mesmtp, Msmtp8, and Mrelay in `sendmail.cf.delivery`.

Configure InterScan,

1. Make sure the standard version of ISVW is installed.
2. Edit `intscan.ini` and change the InterScan SMTP service port to 18000.
3. In `intscan.ini`, change the original SMTP server location to "localhost 19000".

   Under [smtp],

   Before:

```
svcport=25
original=/usr/lib/sendmail -bs
```

   After:

```
svcport=18000
original=localhost 19000
```

4. Restart InterScan SMTP by "`/etc/iscan/sendmail`".
5. Restart a *sendmail* daemon to handle SMTP traffic on port 25 by "`/usr/lib/sendmail –bd –q1h`".
6. Restart another *sendmail* daemon to receive SMTP traffic from InterScan by "`/usr/lib/sendmail –bd –q1h –C/etc/mail/sendmail.cf.delivery`".

   The S88sendmail rc script must be modified to correctly start the mail servers: The start script should now start 3 daemons (started in steps 4, 5, and 6).

Under start section of the script,

Before:

```
/etc/iscan/sendmail; /usr/lib/sendmail -q1h
```

After:

```
/etc/iscan/sendmail; /usr/lib/sendmail -bd -q1h; /usr/lib/sendmail
-bd -q1h -C/etc/mail/sendmail.cf.delivery
```

C. *sendmail* on one box, E-mail VirusWall on another box

The following instructions are applicable to those who are using two different Unix boxes to handle their mail traffic.

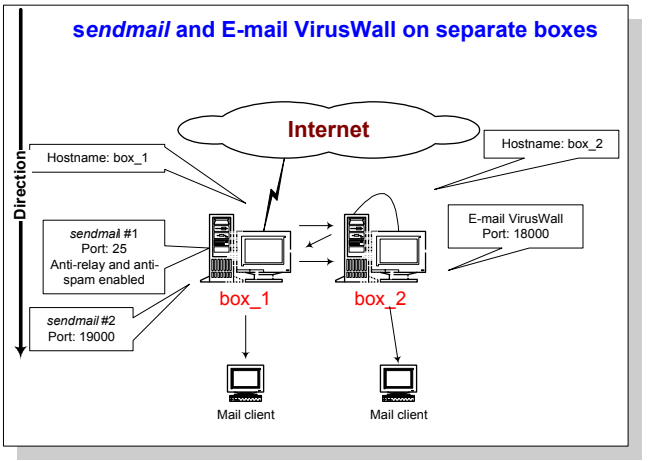


FIGURE 6-9. The illustration shows two Unix boxes configured to handle SMTP traffic.The arrows show the flow of traffic between boxes.

Configure the Mail Daemons,

On box_1...

1. Make a copy of `sendmail.cf` file `called sendmail.cf.delivery`.

2. Change the A option in `sendmail.cf` for Msmtp, Mesmtp, Msmtp8, and Mrelay from "`IPC $h`" to "`IPC box_2 18000`" where box_2 is the hostname of the box running ISVW.

Note: Port 18000 and 19000 are arbitrary port number. Please select a free port when doing the configuration below. Port 25 is the standard SMTP port. This should not be changed.

3. Add the k flag to the F option for Msmtp, Mesmtp, Msmtp8, and Mrelay in `sendmail.cf`.

   For example, the changes for Msmtp should look as follows:

Before:

```
Msmtp,P=[IPC],F=mDFMuX,S=11/31,R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC $h
```

After:

```
Msmtp,P=[IPC],F=kmDFMuX,S=11/31 R=21,E=\r\n,L=990,
T=DNS/RFC822/SMTP,
A=IPC box_2 18000
```

1. Replace the local mailer with [IPC] in `sendmail.cf`.
2. Change the A option to "IPC localhost 18000" for Mlocal in `sendmail.cf`.
3. Add the k flag to the F option for Mlocal in `sendmail.cf`.

   For example, the changes for Mlocal should look as follows:

   Before:

   ```
   Mlocal,P=/usr/lib/mail.local, F=lsDFMAw5:/|@qfSmn9,
   S=10/30, R=20/40,
   T=DNS/RFC822/X-Unix,
   A=mail.local -d $u
   ```

   After:

```
Mlocal,P=[IPC], F=klsDFMAw5:/|@qSmn9, S=10/30,R=20/40,
T=DNS/RFC822/X-Unix,
A=IPC box_2 18000
```

Note: IMPORTANT: Make sure the F option of Mlocal does not include the 'f' flag. This flag is standard on Solaris 7 and needs to be removed.

---

4. Change the port to listen on 19000 in `sendmail.cf.delivery`.

   Before:

```
#O DaemonPortOptions=Port=esmtp
```

   After:

```
O DaemonPortOptions=Port=19000
```

5. Change the mail queue to a different directory in `sendmail.cf.delivery`.

   Before:

```
O QueueDirectory=/var/spool/mqueue
```

   After:

```
O QueueDirectory=/var/spool/mqueue1
```

6. Create the directory `/var/spool/mqueue1` and make sure it has the same ownership and permission as the original in `/var/spool/mqueue`.
7. Add the k flag to the F option for Mlocal, Msmtp, Mesmtp, Msmtp8, and Mrelay in `sendmail.cf.delivery`.

On box_2...

1. Make sure the Standard Edition of ISVW is installed.
2. Edit `intscan.ini` and change the InterScan SMTP service port to 18000.
3. In `intscan.ini`, change the original SMTP server location to box_1 port 19000 under [smtp] where box_1 is the hostname of the box running the 2 *sendmail* daemons.

   Under [smtp],

   Before:

```
svcport=25
original=/usr/lib/sendmail -bs
```

   After:

```
svcport=18000
original=box_1 19000
```

4. Restart one *sendmail* on box_1 by "`/usr/lib/sendmail -bd -q1h`".
5. Restart another *sendmail* on box_1 by "`/usr/lib/sendmail -C/etc/sendmail.cf.delivery -bd -q1h`". Replace "`/etc/sendmail.cf.delivery`" with the path where `sendmail.cf.delivery` is stored.
6. Restart ISVW on box_2.
7. Restart *sendmail* on box_2 by "`/usr/lib/sendmail -bd -q1h`".

The S88sendmail rc script must be modified to correctly start the mail servers: On box_1, two *sendmail* daemons must now be started instead of one.

Under start section of the script,

Before:

```
/usr/lib/sendmail -bd -q1h
```

After:

```
/usr/lib/sendmail -bd -q1h; /usr/lib/sendmail
-C/etc/sendmail.cf.delivery -bd -q1h
```

8. On box_2, make the following changes.

Under start section of the script,

Before:

```
/etc/iscan/sendmail; /usr/lib/sendmail -q1h
```

After:

```
/etc/iscan/sendmail; /usr/lib/sendmail -bd -q1h
```

Chapter 7

FTP VirusWall

FTP VirusWall can serve as a sentry, checking all FTP file transfers to and from a given server for viruses, or as a proxy. When installed and configured to act as a proxy, FTP VirusWall receives all FTP requests originating from within the LAN, passes them to the remote FTP server, receives the data back using the data port opened by the remote FTP server, scans for viruses, and then delivers clean files to the requesting client. See Chapter 2, "Installation Planning," for illustrated examples.

Considerations

- FTP VirusWall can serve as either the sole FTP server on the network or to 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.
- 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 **Configuration** page.

1. In the menu on the left, click **Configuration**.
2. In the **Real-time Scan** section, select the check box to enable or deselect disable **FTP Scan**:

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 daemon location) or if FTP VirusWall will independently handle FTP traffic (in this case choose **Use user@host**).

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*.

For the Standard Edition, server location and port are also 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 FTP server, whether it is installed on the same machine or a different one.

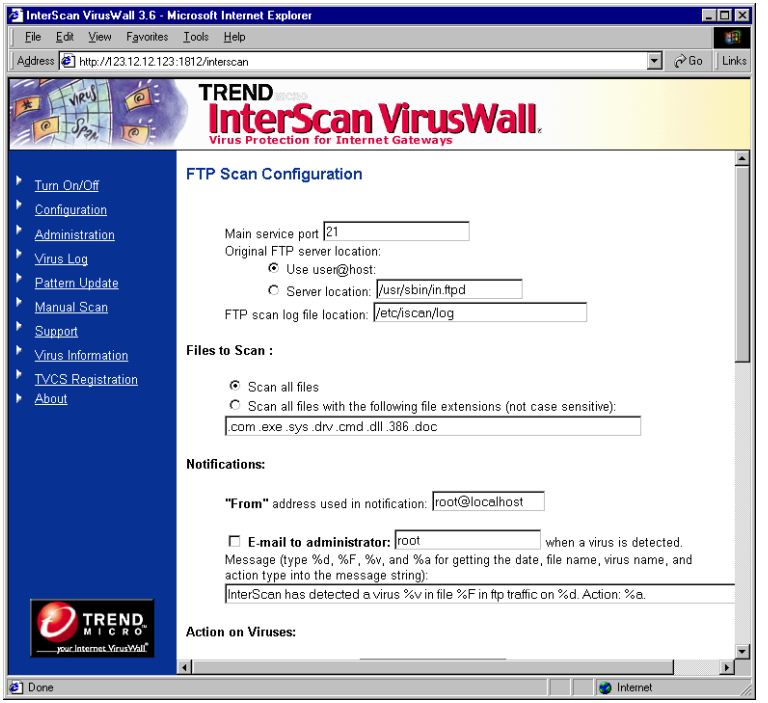


FIGURE 7-1. FTP Scan can be configured to work with an existing FTP server or as its own proxy.

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.

You also need to choose either **Use user@host** or **Server location** (for the latter, specify the FTP server's 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 open a tandem connection with the requested site. When prompted for a user name and password, clients must be sure to append the target domain to their username.

For example, to FTP *widgets.com* through FTP VirusWall, 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. Enter the location and port of the server in the Server Location field. 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
   ```

Testing: Use Telnet (or a similar program) to Telnet to the InterScan IP and port you have specified for these fields. By observing the response, you can identify and then eliminate most configuration issues.

FTP Log File Location

The FTP scan log file location is the location of the system log for the FTP scan service. When you use the default location for all of the services, they will be combined into one log file. If you change the location for any of the services, that service will have a separate log file. The system log file records system events, such as errors, stopping, and starting services.

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.

Priority for FTP Scan Configuration

If your configurations on the *FTP Scan Configuration* screen conflict with each other, the program will scan according to the following priority:

1. "File types to block"
2. "Files to scan"

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

   You can also choose from the following file types, which potentially carry viruses:

   ```
   BIN COM DOC DOT DRV EXE SHS SYS XLS XLA XLT VBS JS
   HLP HTML HTM CLA CLASS SCR MDB PPT POT DLL OCX OVL
   ARJ CAB GZ LZH ZIP RAR Z TAR
   ```

   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 files are only scanned if the file type is specified. Compressed files are opened and all files scanned. Infected Zip files cannot be cleaned and should be deleted or quarantined.

   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.

To specify which files to block,

You can explicitly state the types of files that you want to block.

1. Check *The following file types will be blocked.*
2. Enable the file types that you want to block.

For more information about how file types are classified, see *File Type Classifications* starting on page 6-8. To enter *Other types*, enter the *File Type* name that you want to block.

Sending Messages to Recipients

If a file is blocked by InterScan VirusWall, you can send a notification message to the intended recipient. You can either choose to send the default message, append a customized message to the default, or replace the default message with the customized message. If choosing to use a custom message, type the text of the message in the appropriate text box.

Sending Notification to Administrator

If you want to notify the administrator that InterScan VirusWall blocked a file, enable the *Send notification email to administrator* option button and type the content of the notification.

Setting Virus Notifications

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

"From:" field

You can specify any email 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 receive mail if users attempt to reply to the notification message.

To notify the administrator,

1. Click the **Email to administrator** checkbox.
2. Enter the email address (**root**, for example) in the associated text box.

Note: Multiple email 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: Detailed description
   %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 **3-22-01**, InterScan detected the **Jerusalem** virus in the file: **Word.com.** InterScan took the following action: **delete**."

Specifying Notification Delivery Server

In order to be able to send notifications, you will need to specify the SMTP server that will deliver the notification messages.

Note: If no notification server is specified, no notifications will be sent.

---

1. Go to the **Administration** page in the InterScan Web console.
2. Under the **Notifications** section, enter the following two parameters:

- Notification server:
  Type in the name of the notification server using the domain name or IP address. The default setting, *localhost*, can be used if your SMTP server is on the same machine as InterScan.
- SMTP Server port:
  Enter the service port that the notifications server is using. The default is the standard SMTP port used on the Internet: 25. Choose another port if you have modified your SMTP server port settings.

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 the infected file, along with a warning message to the client *without cleaning*.
- Choose **Quarantine** 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 at 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 **Quarantine** to move the infected file to the `Quarantine` directory (see **Quarantine**, above).
  - Choose **Delete** to reject the infected at the server.

Macro Scan

Macro Scan detects macros in file downloads and provides two scanning options: **Quarantine** and **Clean**. Select **Enable Macro Scan** to use this feature, then choose **Quarantine** or **Clean**.

- **Quarantine** will remove the file if it contains a macro and place it in the `Quarantine` directory.
- **Clean** will strip of the macro before delivering the file with the attachment.

Miscellaneous

Temporary directory location

By default, InterScan uses the `/tmp` to do the work of scanning for viruses. When InterScan receives a file (any type that it is configured to scan), it places a copy in a temporary directory for scanning. The directory location is configurable. Be sure to specify a directory with at least 256MB available free space.

Authorize FTP server to use commands

This feature allows FTP users to use specific commands during a FTP session, for example, "ls" and "cd". Once you have logged into the FTP server, you can get a list of available server commands by typing `help` from the command line. Not all the commands listed will be available, only the ones specified in the **Authorize FTP Servers to use the following commands** field.

FTP Scan Advanced Options

Note: Advanced Options only pertains to InterScan *Standard* Edition. This section does not apply to the *CVP* Edition.

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.

For FTP VirusWall, the default values are optimal for most cases.

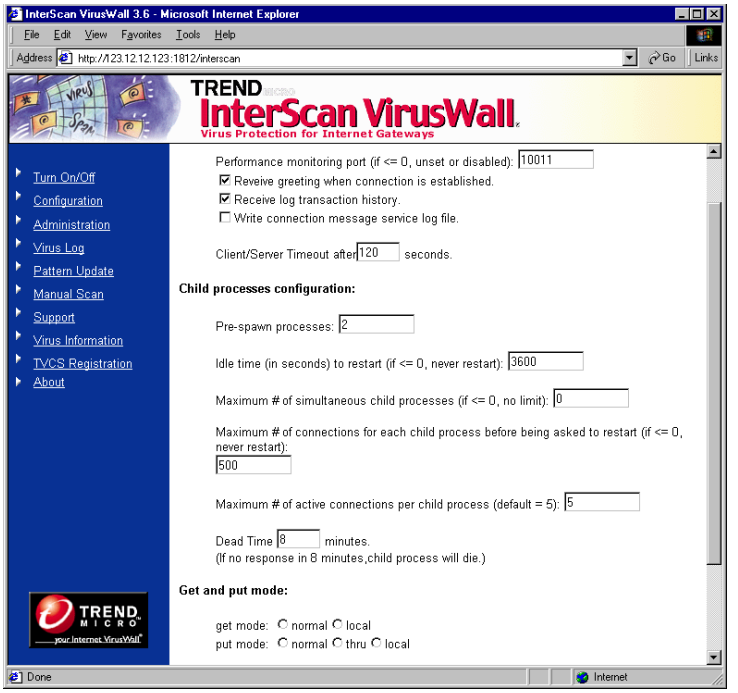


FIGURE 7-2. Advanced Options allow you to optimize performance.

To edit the Advanced Options,

1. Open the InterScan console and click **Configuration > FTP Scan**.
2. Scroll to the bottom of the FTP Scan Configuration page that appears and click the **Advanced Configuration** button.

Performance Monitoring

You can view real-time performance statistics by using performance monitoring. The default port is shown in the performance monitoring field in the GUI. The port number is configurable.

To monitor performance,

1. From the command line, go to the `etc/iscan` directory.
2. Type `perfmon [port number]` and press **Enter**.

The performance monitor will show the following:

- Master process ID
- Start date
- Connections served
- Number of child processes forked

For each child process that is spawned by the master process:

- Master process ID
- Start date
- Connections served
- Idle time
- Number of threads for example (1 / 5), which means 1 active out of 5 available threads

Receive Greeting

You can configure InterScan to send a greeting when you telnet into any port that InterScan is operating on. The greeting will display basic product information.

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**.

You can specify where InterScan keeps its logs on the **Configuration** page.

Write connection message to service log file

When this option is disabled, only the IP address is logged as a connection message and InterScan VirusWall will not convert the IP address to a hostname. When the option is enabled, InterScan VirusWall will convert the IP address to a hostname.

Client/Server Timeout Settings

This feature is used to avoid having processes wait indefinitely for a reply from either server or client. Set this feature for each service.

Child Process Configurations

You can fine-tune InterScan's performance by making adjustments to settings such as 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 existing traffic load. Depending on your system resources and traffic load levels, you may want to increase the Preprocess 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 spawning new processes 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, this option allows you to set a maximum if necessary.

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 is 500, meaning that after 500 threads have been generated and extinguished, the hosting child process itself is extinguished and a new one generated (a new child is only 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 can contribute to system instability.

Dead Time

This feature will kill a slave process after a set amount of time if it does not terminate normally. Sometimes a slave process will not terminate normally due to some problem, causing a performance degradation. The default setting is 8 minutes.

Get and Put Mode:

You can configure how InterScan behaves when sending (*put*) and receiving (*get*) files via FTP. How you set Get and Put depends entirely upon whether FTP VirusWall is 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*.

Note: When Get mode is set to Local and user@host is used as the original FTP server location (self_proxy=yes), InterScan VirusWall's FTP daemon will automatically reset the internal value back to Normal. Therefore, the files being transferred will be scanned as Normal.

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.

Note: When Put mode is set to Local and user@host is used as the original FTP server location (self_proxy=yes), InterScan VirusWall's FTP daemon will automatically reset the value internally back to Thru.

Saving the configuration

- To save the new configuration, click **Apply**.
- To "undo" your unsaved changed click **Cancel**.

Chapter 8

Web VirusWall

Web VirusWall can scan 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). It can also be installed and configured to act as the sole HTTP proxy on the network. See Chapter 2, "Installation Planning," for illustrated examples.

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**, **Quarantine**, 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 **Configuration** page.

1. In the menu on the left, click **Configuration**.
2. In the **Real-time Scan** section, select the checkbox to enable or deselect to disable **HTTP Scan**:

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.

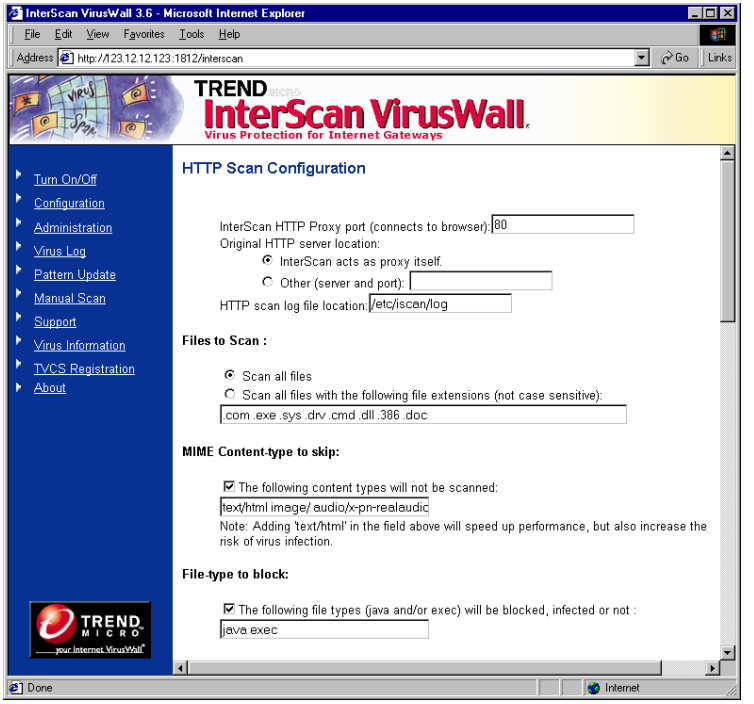


FIGURE 8-1. Configure Web VirusWall to work with an existing HTTP proxy server or as the only HTTP proxy on the network.

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.

Note: To have Web VirusWall handle FTP scanning, have your clients configure their Web browsers to use Web VirusWall as their FTP proxy.

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, explained below.

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.

Other (Server and port)

Choose this option if there is an existing HTTP proxy 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.

Testing: Use Telnet (or a similar program) to Telnet to the InterScan IP and port you have specified. By observing the response, you can solve most configuration issues.

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. Because the proxy is on a different machine, you need to specify a port.

HTTP Log File Location

The HTTP scan log file location is the location of the system log for the HTTP scan service. When you use the default location for all of the services, they will be combined into one log file. If you change the location for any of the services, that service will have a separate log file. The system log file records system events, such as errors, stopping, and starting services.

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, or can be modified in the CVP option of the left browser pane.

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 .drv .cmd .dll .386 .doc

You can also choose from the following file types, which potentially carry viruses:

```
.BIN .COM .DOC .DOT .DRV .EXE .SHS .SYS .XLS .XLA .XLT
.VBS .JS .HLP .HTML .HTM .CLA .CLASS .SCR .MDB .PPT
.POT .DLL .OCX .OVL .ARJ .CAB .GZ .LZH .ZIP .RAR .Z
.TAR
```

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 files are only scanned if the file type is specified. Compressed files are opened and all files scanned. Infected Zip files cannot be cleaned.

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 types. 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 specify which files to block,

You can explicitly state the types of files that you want to block.

1. Check *Block the following file types*.
2. Enable the file types that you want to block.

For more information about how file types are classified, see *File Type Classifications* starting on page 6-8. To enter *Other types*, enter the *File Type* name that you want to block.

Sending Messages to Recipients

If a file is blocked by InterScan VirusWall, you can send a notification message to the intended recipient. You can either choose to send the default message, append a customized message to the default, or replace the default message with the customized message. If choosing to use a custom message, type the text of the message in the appropriate text box.

Sending Notification to Administrator

If you want to notify the administrator that InterScan VirusWall blocked a file, enable the *Send notification email to administrator* option button and type the content of the notification.

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** will be 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 (java and/or exec) will be blocked, infected or not** 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.

Priority for HTTP Scanning Configuration

If your configurations on the *HTTP Scan Configuration* screen conflict with each other, the program will scan according to the following priority:

1. "MIME Content type to skip"
2. "File types to block"
3. "Files to scan"

Setting Virus Notifications

Upon detecting a virus in a user's FTP transfer, InterScan can automatically send a customized email 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).

"From:" field

You can have any email 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 **Email to administrator** checkbox.
2. Enter the email address (**root**, for example) in the associated text box. Multiple email 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: Detailed information
   %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**."

Specifying Notification Delivery Server

In order to be able to send notifications, you will need to specify the SMTP server that will deliver the notification messages.

Note: If no notification server is specified, no notifications will be sent.

---

1. Go to the **Administration** page in the InterScan Web console.
2. Under the **Notifications** section, enter the following two parameters:

- Notification server:
  Type in the name of the notification server using the domain name or IP address. The default setting, *localhost*, can be used if your SMTP server is on the same machine as InterScan.

- SMTP Server port:
  Enter the service port that the notifications server is using. The default is the standard SMTP port used on the Internet: 25. Choose another port if you have modified your SMTP server port settings.

Setting the Action on Viruses

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

- Choose **Quarantine** 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 **Quarantine** to move the infected file to the `/etc/iscan/virus` directory.
  - Choose **Delete** to reject the infected at the server.

Macro Scan

Macro Scan detects macros in file downloads and provides two scanning options: **Quarantine** and **Clean**. Select **Enable Macro Scan** to use this feature, then choose **Quarantine** or **Clean**.

- **Quarantine** will remove the file if it contains a macro and place it in the `Quarantine` directory.
- **Clean** will strip off the macro before delivering the file with the attachment.

Miscellaneous

Web VirusWall provides several "miscellaneous" options, including

- Trickle, which solves a proxy "timeout" issue that can occur under one setup topology
- Virus warning option
- FTP download option
- Temp directory location, which allows you to specify any directory for Web VirusWall logs.

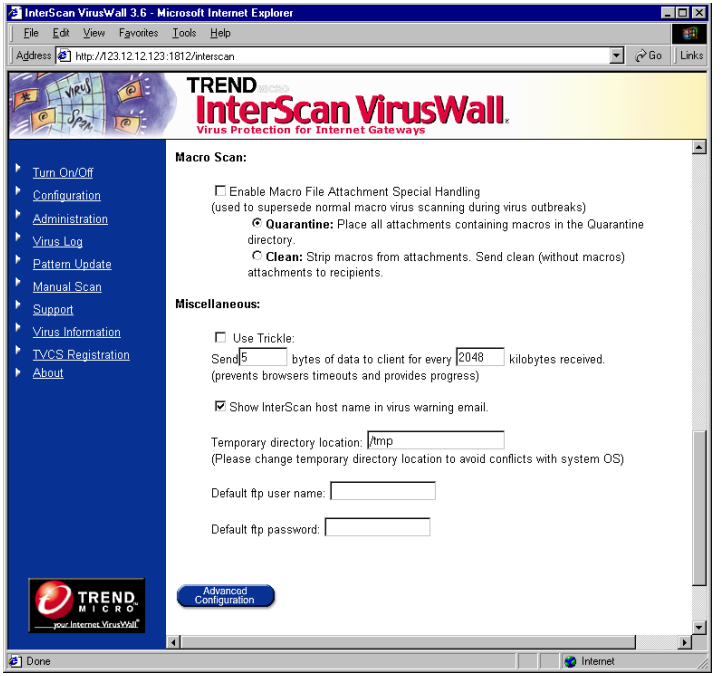


FIGURE 8-2. Web VirusWall configuration screen, continued.

"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 "timeout" 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** below for more information.

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

To have Web VirusWall "trickle" data,

1. Open the **HTTP Scan Configuration** page.
2. Specify the number of bytes you want "trickled" to 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 of the file that it receives.Once the entire file has been downloaded to the Web VirusWall machine and scanned, it is rapidly transferred to the requesting browser. 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 *without scanning*, it is theoretically possibility that virus code will be among the portion of file that has been "trickled" to the client. Users should delete these files.
- Data trickled to the client's hard drive will appear as a small, unusable file. Users should understand that Web VirusWall has not corrupted these files; rather, they have been deleted in accordance to the policy set by the administrator.
- Optimal trickle ratios (bytes:kilobytes) are likely to be from 512-2048 bytes to 128-1024 kilobytes, depending on the speed of your Web VirusWall-to-Internet connection.
- 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 on viruses set; clients are not notified.
- The predicted download time that clients receive when downloading a file will be vastly overestimated—the client *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.

Virus Warning Option

"Trend Micro" or "InterScan" does not appear anywhere that users and users' recipients can see via either email subject or email body. However, if you want InterScan to appear in the warning message, you can select this field. Warning messages will then contain the host name, which is InterScan.

Temporary directory location

By default, InterScan uses the `/tmp` to do the work of scanning for viruses. When InterScan receives a file (any type that it is configured to scan) it places a copy in a temporary directory for scanning. The directory location is configurable. Be sure to specify a directory with at least 256MB available free space.

Default FTP user name and password

InterScan can access anonymous FTP sites without any special configuration. However, InterScan cannot access the FTP site that verify domain names. Defining user name and password allows InterScan to access FTP servers that check the domain name of the user.

Skipping Scanning Based on HTTP Response Code

InterScan can be configured to skip scanning HTTP data streams based on the first digit of the HTTP response code returned by a Web server. This is helpful because InterScan cannot successfully scan Web pages that use ISHTTP or HTTP redirection time delay. Under the *Miscellaneous* section of the **HTTP Scan Configuration** screen, enter the first digits of the three-digit HTTP response code that you want to skip, separated by a space.

In addition, InterScan can be configured to skip scanning HTTP traffic if the content-length is zero by enabling the appropriate option button under the *Miscellaneous* section.

HTTP Scan Advanced Configuration

Note: Advanced Options only pertains to InterScan *Standard* Edition. This section does not apply to the *CVP* Edition.

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.

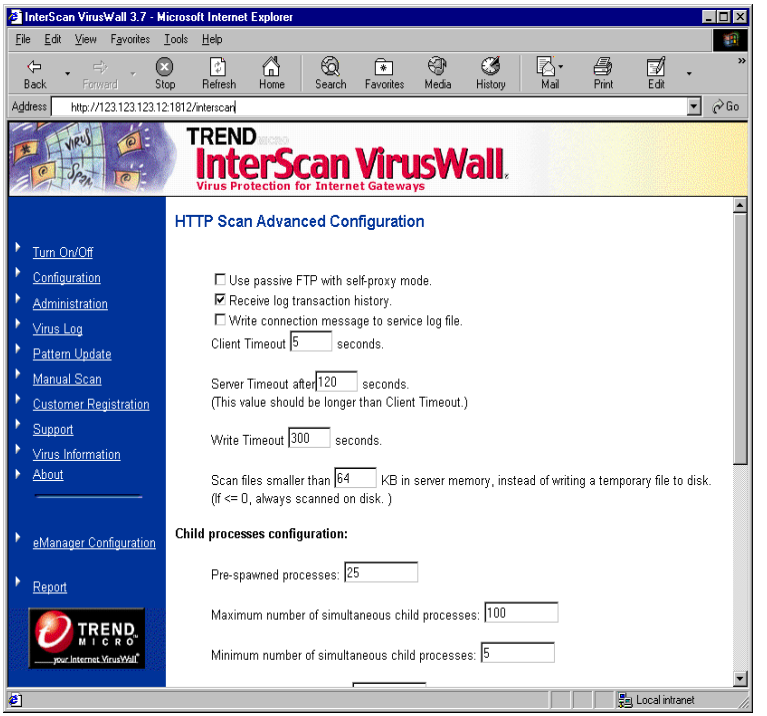


FIGURE 8-3. You can fine-tune Web VirusWall's performance with the options available in Advanced Configuration.

To edit the Advanced Options,

1. Open the InterScan console and click **Configuration > HTTP Scan**.
2. Scroll to the bottom of the HTTP Scan Configuration page that appears and click the **Advanced Configuration** button.

Performance Monitoring

You can view real-time performance statistics by using performance monitoring. The default port is shown in the performance monitoring field in the GUI. The port number is configurable.

To monitor performance,

1. From the command line, go to the `etc/iscan` directory.
2. Type `perfmonhttp` and press **Enter**.

The performance monitor shows the following information about the parent process:

- Master process ID
- Maximum and minimum number of child process in the format maximum/minimum, e.g., 100/5
- Number of present child processes

For each child process that is spawned by the master process:

- Child process ID ("PID")
- Process status ("status")
- Whether process is about to die (signified by "to_die" equal to 1)
- Number of connections ("conns")
- Period of time the connection lasted ("time")
- Origin of the connection ("address")
- Number of connections/second ("conns/sec")

FTP through HTTP

Selecting **Ftp through http** will allow clients to download from a FTP site using their Web browsers.

Writing connection message to log

By default, InterScan logs only errors and the starting/stopping of the services. To have InterScan log each connection message, select **Write connection message to service log file**.

You can specify where InterScan keeps its logs on the **Configuration** page.

Client/Server Timeout

This feature is used to avoid having processes wait indefinitely for a reply from either server or client. Set this feature for each service.

Scanning Files in Memory

InterScan VirusWall can either create a temporary file on the server's hard disk before scanning it for viruses and malicious content, or you can specify that the file be scanned while in the server's memory.

Configure the maximum size of files (in KB) to be scanned in memory, based on your server's available resources. If your server has lots of available memory, scanning small files in this manner will result in better performance compared to creating the temporary file. Leaving this setting blank, or entering 0 or a non-negative number will configure InterScan VirusWall to always create a temporary file before scanning.

Child Process Configuration

You can fine-tune InterScan's performance by making adjustments to settings such as 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.

InterScan VirusWall reserves memory space, or processes, to perform antivirus scanning. The administrator has full control over how the program manages these processes.

Pre-spawned processes...

Configure the number of pre-spawned processes that you want InterScan VirusWall to reserve in memory when the program is started. You can think of each process as

being able to scan a single file, thus configuring 25 pre-spawned processes means that the program has reserved memory space to scan 25 files simultaneously.

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

Number of simultaneous child processes...

Child processes are all of the processes that are reserved in the server's memory to perform antivirus scanning. They are created on an as-needed basis to scan files arriving through HTTP traffic. Configure the maximum number of child processes that can be created, and the minimum number that will be kept running.

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, this option exists to allow you to set a maximum if necessary. Configure the maximum number of child processes that can be created, and the minimum number that will be kept running.

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

Child Process Maintenance

You can configure the number of connections after which the child process will be restarted and the memory released. In addition, you can configure the number of processes that will be created each time new child processes are needed.

When processes are no longer needed for scanning, they will be closed after the lag time that you have configured expires.

Chapter 9

Manual and Prescheduled Scans

In addition to the real-time scanning of files as they travel via email, FTP, and HTTP, InterScan VirusWall allows you to perform manual, or "demand scans" of individual drives or directories. Any drive or 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 explain how to use InterScan VirusWall for manual and scheduled 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 fair amount of swap 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.

Manual Scans

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 **Prescheduled Scan**, described later in the chapter.

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

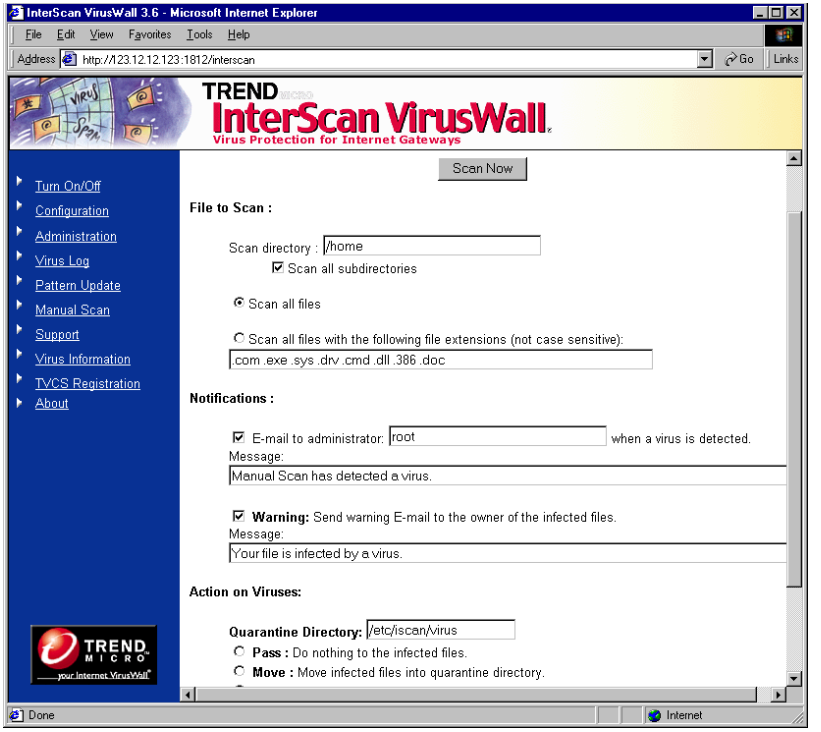


FIGURE 9-1. Manual Scans allows you to check all or selected directories on the server hard drive (and any mounted drive) for viruses.

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 top 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
   ```

   Only files included in the `/home/michelle` directory will be scanned.

2. To scan all file in `/michelle` and in any folder below `/home/michelle`, check **Scan all subdirectories**. For example,

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

To scan all drives and directories,

You can have InterScan scan all the files on a specified drive, including mounted volumes. An overview of the tasks follows:

1. If you want to 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**.
4. Make your **Notification** selections.
5. Define the **Action on Viruses** you want InterScan to take.
6. Click the **Scan Now** button**.** InterScan will begin scanning the selected drive.

Note: No real-time report of the scanning progress is piped to the screen; however, a record of the scan results is written to 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

   You can also choose from the following file types, which potentially carry viruses:

   ```
   BIN COM DOC DOT DRV EXE SHS SYS XLS XLA XLT VBS JS
   HLP HTML HTM CLA CLASS SCR MDB PPT POT DLL OCX OVL
   ARJ CAB GZ LZH ZIP RAR Z TAR
   ```

   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 files 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 file, InterScan can automatically send a customized email to the **Administrator** and/or **Owner** of the infected file(s).

To notify the administrator, or "owner,"

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

For the file owner, the notification will be sent as a separate email to their UNIX mail account on the InterScan machine. If that machine has no Sendmail, no notification is sent, but the event will be recorded in the virus log.

2. For the administrator, enter the email address (**root**, for example) in the associated text box. Multiple email addresses are not supported.
3. In the **Message** field(s), enter the warning message you want the administrator and/or owner to receive.

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 owner *without cleaning*.
- Choose **Move** to move, *without cleaning*, the infected attachment to the `/etc/iscan/virus` directory.
- Choose **Delete** to remove the infected file from the server.
- Choose **Auto Clean** to have Web VirusWall automatically clean and process infected files. The owner is notified.

  If an infected file cannot be cleaned, for example, because the virus has corrupted it, Web VirusWall will **ignore** the infected file. The log file will contain information about the infected file. So, to remove the file, you will need to check the log to identify any infected file that could not be cleaned.

Prescheduled 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 scans should take place.

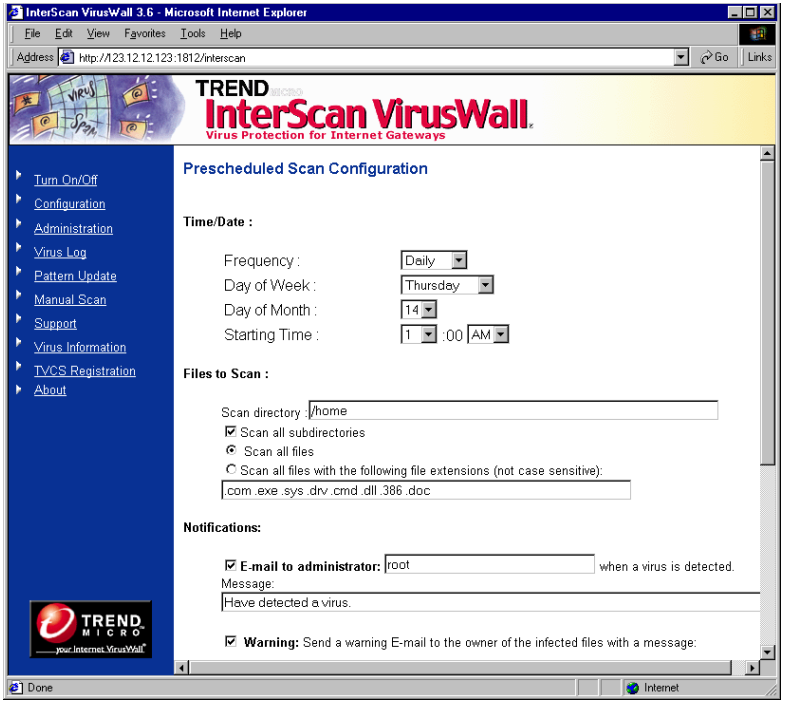


FIGURE 9-2. You can schedule InterScan to periodically scan selected drives or directories.

Only one directory can be designated for **Prescheduled Scans**; typically, this is a public directory containing a subdirectory for every user.

Scheduling Scans

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

- Check the **Prescheduled Scan** option on the **Configuration** page
- Schedule the scan frequency

- Specify a drive or directory for scanning

To enable/disable scheduled scanning,

1. Click **Configuration**.
2. Select the box in front of **Prescheduled Scan** and then click on the **Prescheduled Scan** link.
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.

Chapter 10

Virus Log Files, Pattern Updates, and Registration

InterScan VirusWall provides two types of logs: system and virus. The virus log contains only the default logging level. The system log contains three levels of logging detail: default, transactions, and verbose. All three log levels are set directly in the intscan.ini file; there is no interface support for changing the default log level.

- **Default** logging tracks error messages and notes whenever a daemon is stopped or started
- **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

---

Note: The default setting of InterScan VirusWall does not automatically remove log entries. Left unchecked, logs will grow until they consume all disk space. For information about deleting old log entries, see *To delete log files,* starting on page 10-4

By default, InterScan creates two types of log files. The system log is created every day. The virus log is updated each time there is a virus event. The log file is written to the `/etc/iscan` directory. For example, the virus log is named according to the following convention:

```
virus.log.2001.03.22
```

which can be read as *InterScan Log for March 22, 2001*.

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 256 or more megabytes.

Specifying the Log Directory

You can have InterScan write its system and virus event logs to any directory you want, provided that there is sufficient disk space.

To specify a different virus log directory,

1. Click **Virus Log > Specify Virus Log Location**.
2. Enter the location and file name that you want InterScan to use and click **Apply**. The default is,

   /etc/iscan/virus.log

To specify a different system log directory,

System logs are written for each service, SMTP, HTTP, and FTP. The directory locations are defined on the main configuration page of each service. If the same location is specified for all three services, InterScan will only create one log file. The default location for the system logs is,

/etc/iscan/virus.log

To change the default location of the system logs, E-mail VirusWall, for example,

1. Click **Configuration > Email Scan**.
2. Enter the new location and file name in the **Email scan log file location** field at the top of the page and click **Apply**.
3. Repeat this process for each service.

Note: For the **System** and **Virus** logs. InterScan adds the current date (yyyy.mm.dd) to the name.

Viewing or Deleting Log Files

InterScan keeps both Virus logs, which track all virus events, and System logs, which track system events such as error messages, the stopping and starting of the daemons, etc. New logs are written each day. The default setting of InterScan VirusWall does not automatically remove log entries. Left unchecked, logs will grow until they consume all disk space.

The procedure for viewing and deleting virus logs is given below.

Note: The system logs cannot be viewed through the Web interface. You must use an editor, such as VI, to view the system logs.

To view virus logs,

1. Open a Web browser and start the InterScan console, then click **Virus Log** in the left browser frame.
2. Click **View Virus Log**.
3. Select the service whose logs you want to view from the list.
4. Click the appropriate radio button to choose the **Date**, **User**, or **Names** you want to view.

   For example, you can view only virus logs from the **HTTP scan**, for **All dates**, **All users** (or specify a particular user name), or **All viruses** (or, choose a virus from the list).
5. Click **OK** to display the logs you have selected, or **Reset** to recall 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. Virus 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 email)
- The **action** taken

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

FIGURE 10-1. An example Virus Log from InterScan VirusWall.

To delete log files,

You can delete unwanted virus logs manually or automatically.

Delete log files manually

1. Click **Virus Log > Delete Virus Log**.
   - 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 **OK** to carry out the action or **Reset** to abort.

   The following message may appear in the log, but does not signal a problem. It indicates an occasional, transitory busy state during child process extinction. *illegal state transition*, EXIT --> OK, ignored...

Delete log files automatically

1. Click **Administration** in the Web configuration console sidebar menu.
2. Choose to delete system log files older than a certain date by entering the number of days old in the **Delete the InterScan system files that are older than [ ] days**.

   This feature will ensure that the log files, without the need for manual deletion, will be deleted after they are no longer needed.
3. Click **Apply**.

eManager Logs and Reports

If you have installed the optional eManager plug-in, you will see additional links on the side-bar menu. If you click on **eManager Configuration**, you will open the eManager configuration menu in a new window. See the eManager documentation for information on how to configure eManager.

The **Report** link has two sub-menus, **Virus Log** and **eManager Report**. The Virus Log link goes to the InterScan *Virus Log* page. The eManager Report link displays the eManager logs by date. Users can view the Virus Log and eManager Log separately.

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 telltale signatures and incorporates the information into this file. Pattern files use the following naming format:

```
lpt$vpn.###
```

where ### stands for the version (e.g., 950). If multiple files exist in the same directory, only the one with the highest number is used.

After pattern version number 999, pattern files will take the extension 101, 102, 103...199...901...999.

Trend Micro publishes a new virus pattern file every week, 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: 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.

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. The version of your current pattern file and the occasion of the last update appears.

Note: If you have not registered for a virus pattern update, you must do so before updating the virus pattern. Use the **Register for Product** page to register.

---

2. Click **Update Virus Pattern Now**. A progress bar will appear at the bottom of your browser window to indicate the update progress, and a page will then display the outcome of your update (either successful or failure).

FIGURE 10-2. Shows the current pattern information and available options for Pattern Update.

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 **Set Automatic Update Time**. The scheduling options appear.
   - Click **No automatic update** to disable scheduled updates.

- Otherwise, choose *Update hourly*, *Update daily*, *Update weekly* or *Update monthly* to select your preferred interval and select the time as appropriate.

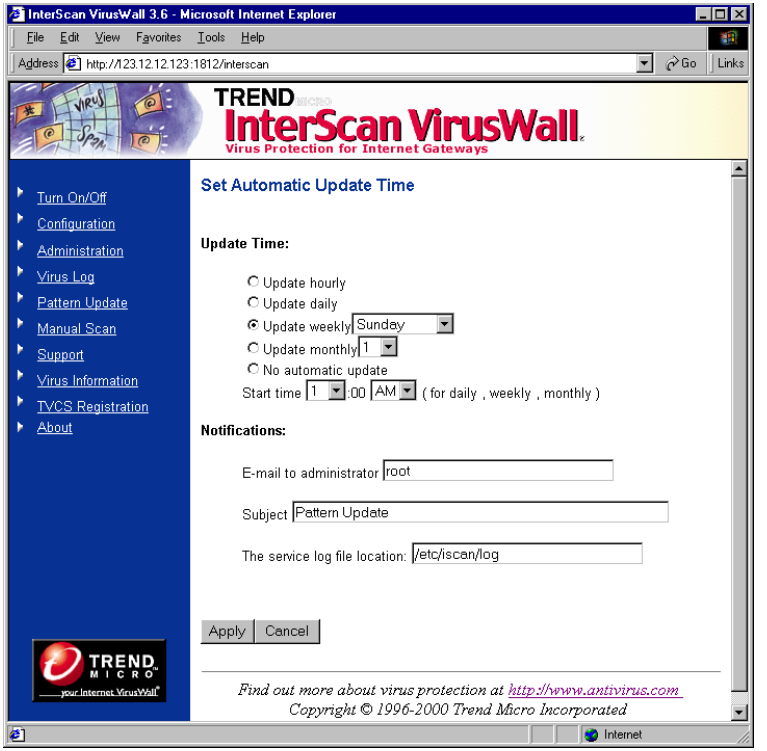


FIGURE 10-3. Trend Micro recommends that you update your virus pattern file weekly.

Using an HTTP Proxy Server

InterScan obtains new virus pattern files from `www.trendmicro.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 the proxy and supply the appropriate logon credentials.

Note: If you have 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.

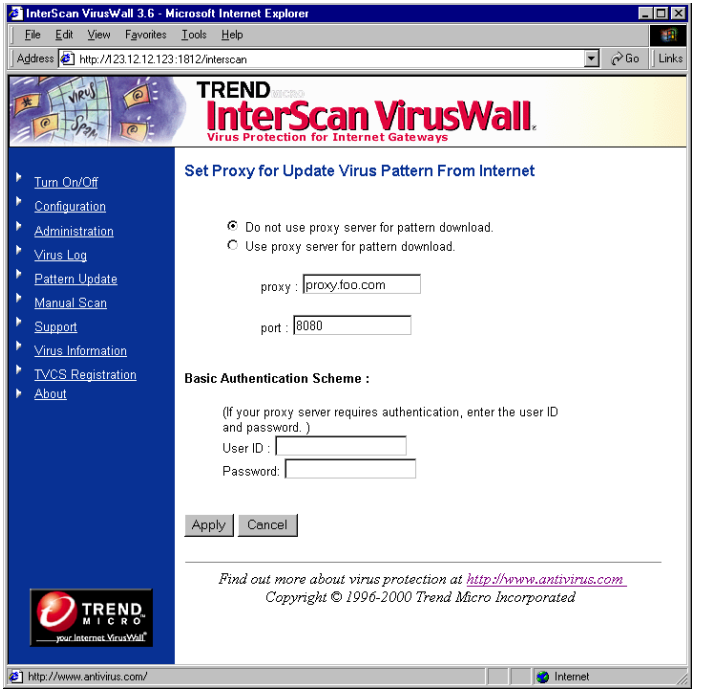


FIGURE 10-4. InterScan will use your proxy server for virus pattern updates, registration, and, if you run Trend VCS, the Trend VCS Agent.

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 **Set Proxy Server**.

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.

Retaining Old Virus Pattern Files on Your Server

The InterScan program looks in the program directory and uses the latest pattern file to scan inbound traffic. It can distinguish the latest pattern file by its file extension; e.g., lpt$vpn.864 is newer that lpt$vpn.863.

Occasionally, a new virus pattern file wrongly detects a non-infected file to be a virus infection. This problem is called a "false alarm". You can revert back to the virus pattern file that was being used prior to updating the virus pattern file by deleting the newest virus pattern file and restarting your antivirus program.

You can configure the number of virus pattern files that you want to keep on the InterScan server to prevent disk space from being unnecessarily wasted.

To specify the number of virus pattern files that you want to keep on the InterScan server:

1. On the left-hand navigation frame, click the **Administration** hyperlink.
2. In the *Administration* screen, enter the number of virus pattern files that you want to keep on the InterScan server in the appropriate text box.

Updating the Scan Engine

The scan engine for InterScan is updated on a regular basis with new features and improvements. The scan engine is updated approximately once every three months and posted for download on the Trend Micro Web site. The scan engine cannot be updated automatically.

Note: Use the **About** page in the Web Console to see which version of the scan engine is currently being used.

To update the scan engine,

1. Download the scan engine (libvsapi.so) from `www.trendmicro.com/download` and untar the file.
2. Using the Web Console, stop all the InterScan scanning services (FTP, HTTP, and/or HTTP).
3. Copy the new engine file to the `/etc/iscan` directory.
4. Restart the InterScan scanning services.

Registering InterScan

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

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

You can register InterScan in the following ways:

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

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

To register over the Internet,

1. Open the InterScan console & click **Pattern Update > Register for Product**. Alternatively, you can click the **Customer Registration** link in the left-hand frame.

2. Type in all the requested information. You need only enter one serial number for all three VirusWalls.
3. Click **Apply** to send your information to Trend Micro.

Note: You must register over the Internet in order to receive virus pattern updates from within the program.

Chapter 11

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, contact us. We also welcome your comments.

In the United States, Trend Micro representatives can be reached via phone, fax, or email. Our Web and email addresses follow:

```
http://www.trendmicro.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:      +1-800-228-5651 (sales)
Voice:          +1-408-257-1500 (main)
Fax:            +1-408-257-2003
```

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

```
Trend Micro, Inc.
10101 N. De Anza Bvld.
Cupertino, CA 95014
```

You can quickly understand and solve many problems on your own by checking *Troubleshooting* in the Index.

Version Information

In addition to updating your virus pattern file, Trend Micro also provides occasional scan engine and/or program upgrades, and other version changes. To find out exactly which version, pattern number, or scan engine build you are running, click the **About** button in the main InterScan console menu.

FIGURE 11-1. Click About to find out your InterScan version information.

Solution Bank

In addition to providing "in-person" technical support, Trend Micro customers can also search our knowledge base of thousands of technical support procedures, troubleshooting tips, and product descriptions. Access the Solution Bank at:

http://solutionbank.trendmicro.com/solutions/

New solutions are continuously being added. If you are unable to find the answer you seek, we invite you to email your question and a Technical Support engineer will contact you shortly thereafter.

Sending Trend Micro Your Viruses

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 analyze 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 information is available over the Internet at our free **Virus Information Center**. Find out about

- Viruses currently "in the wild"
- Computer virus hoaxes
- Computer virus trigger dates
- Individual viruses and their symptoms
- Product details and white papers

To open the Virus Information Center,

1. Open the InterScan console in a Web browser.

2. Click **Virus Information**. You'll be connected to Trend Micro's Web site, `www.trendmicro.com`.

FIGURE 11-2. A multitude of virus and product information is available from the Virus Information Center.

Virus Classification and Antivirus Methods

These two buttons link to general information about viruses. Click on them to learn about the types of viruses out in the wild and the methods used to detect viruses.

Client Scans with HouseCall

Of particular interest to your clients may be HouseCall, Trend Micro's free virus scanning service available to one and all. There is nothing to install; just follow the on-screen instructions to begin.

Note: Although HouseCall will detect and clean any viruses found on the user's hard drive, it does not provide real-time protection.

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.trendmicro.com/housecall`

2. Follow the instructions on the screen and HouseCall will scan your hard drive.

Chapter 12

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 works well with Trend VCS. What this means is that you can simultaneously configure multiple copies of InterScan using Trend VCS, or administer InterScan along with your other Trend Micro 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

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. 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.

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.

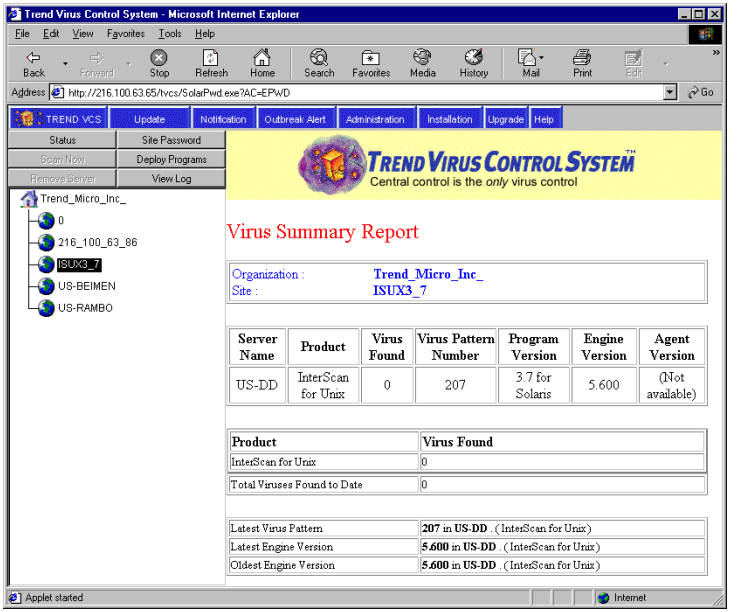


FIGURE 12-1. InterScan VirusWall for UNIX, as seen from a Trend VCS console. Most antivirus products installed on the LAN or WAN can be managed via Trend VCS, eliminating the usual limitations of product platform and physical location.

Installing the Trend VCS Agent

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 installation, or at any time later. The instructions below assume the latter.

1. From the machine where InterScan VirusWall is installed, locate the directory containing the InterScan installation files and type ./isinst.
2. In the Main Menu that appears, choose Option 1.
3. Choose Option 6, reply yes to the question "Install InterScan VirusWall for TVCS?" and press enter.

Note: Installing the Trend VCS agent requires the InterScan VirusWall Base System, the CGI Admin package, and at least one VirusWall.

---

4. 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 VCS server, as explained next.

Configuring the Trend VCS Agent

After installing the Agent, you need to configure it to work with your Trend VCS server, i.e., register it.

Note: If multiple Trend VCS servers are installed, for example on a WAN, the Agent can only be registered to one server.

What to 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 11-1 for an example.
- An administrator-level Windows NT account name and password for logging on to the Trend VCS server
- The hostname and IP address of your 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 **TVCS Registration** from the list of options in the left browser frame.

2. A page loads that displays two buttons - **Register** and **Uninstall**. Click Register to load the TVCS Server Information page or click Uninstall to remove the TVCS agent.

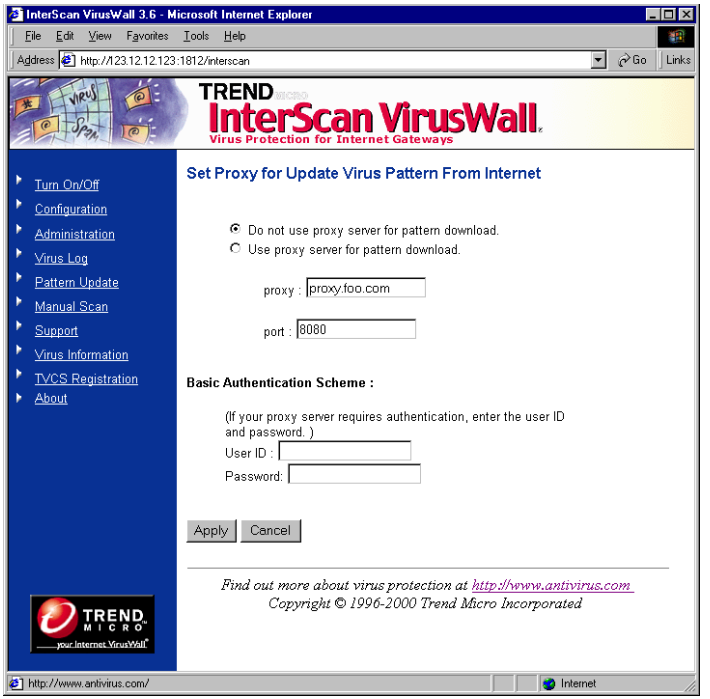


FIGURE 12-2. Proxy server settings for pattern updates.

Note: The InterScan Agent will use the proxy server (if any) configured for Pattern Updates, when communicating with the Trend VCS server.

---

3. Enter the domain name (or IP address) of the machine hosting the Trend VCS server.

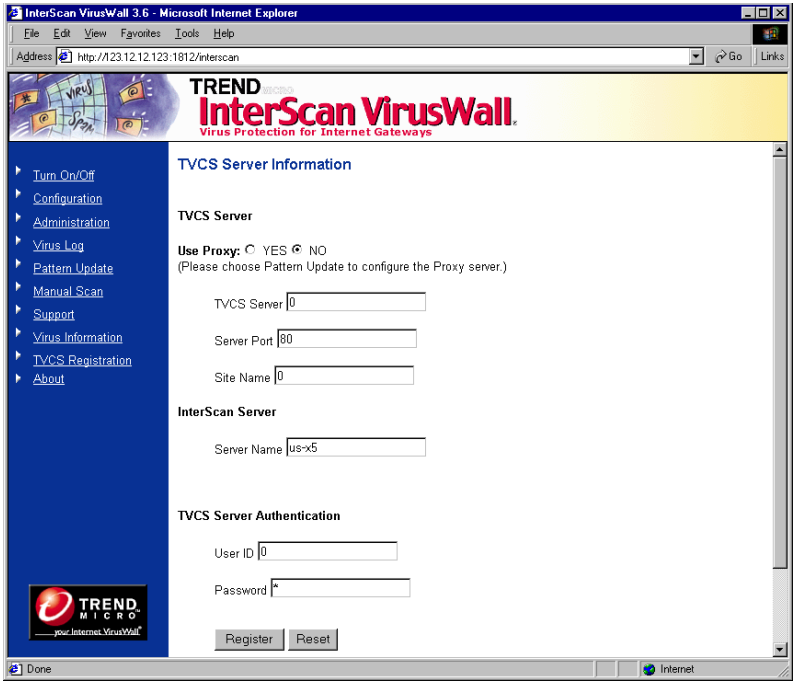


FIGURE 12-3. Trend VCS users can install an Agent for InterScan. The Agent needs to be configured to recognize the Trend VCS server, as shown here.

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 being used by the Trend VCS server.
5. Specify the Site name that you want the Agent for InterScan to appear under.
6. Enter the Trend VCS User ID and password, if 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.

7. Verify the name and IP address (not domain name) of the server running InterScan VirusWall 3 for Solaris. The Trend VCS server will use this address when contacting the Agent, for example to distribute the latest virus pattern update.

Chapter 13

Intscan.ini File Settings

This chapter contains a list 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`). Each parameter is accompanied by an explanation, its default value, a list of any other possible values, and an explanation of the other possible values.

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 configuration changes to InterScan using the Web configuration—open a Web browser and enter the InterScan URL, for example:

```
http://hostname:1812/interscan.
```

Note: We do *not* recommend editing `intscan.ini` directly. But if you do, be sure to make a backup copy first!

The `intscan.ini` file also contains descriptions of the parameters.

Restricting access to the configuration file

To restrict access to the `intscan.ini` file to only those with `root` privileges, open an command prompt and 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.

Note: In the parameter name section,
(s) = Standard Edition only
(c) = CVP Edition only
(s,c) = Both editions

[Scan-Configuration]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
MailKanji	Japanese language support	jis		
LogKanji	Japanese language support	euc		
ConfKanji	Japanese language support	euc		
FtpKanji	Japanese language support	ascii		
httpscan (s)	toggle on/off real-time HTTP scanning	yes	yes no	yes: scanning is on no: scanning is off
ftpscan (s)	toggle on/off real-time FTP scanning	yes	yes no	yes: scanning is on no: scanning is off

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
mailscan (s)	toggle on/off real-time SMTP scanning	yes	yes no	yes: scanning is on no: scanning is off
periodicscan (s,c)	toggle on/off pre-scheduled scanning	no	yes no	yes: scanning is on no: scanning is off
license (s,c)	records license #			
update (s,c)	identifies method of pattern file update	signal	signal auto disabled	update using SIGHUP update periodically, as specified by update_interval never update
update_interval (s,c)	download interval when *update* is set to *auto*	1440	integer, minutes	1440 (daily) 10080 (weekly)
virus_log (s,c)	location of virus log file	/etc/iscan /virus.log	any valid directory	virus.log.2000.04.15 date appended to name
pattern_path (s,c)	location of virus pattern file	/etc/iscan /	any valid directory	example: lpt$vpn.502 (pattern number varies)
web_virinfo (s,c)	user local virus information	no	yes or no	you should enable this option
web_virinfo_url (s,c)	URL for Trend Micro's virus encyclopedia			Enabling the previous option will use this URL. You are routed to the closest regional Trend Micro Web site.

[ISCVP]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
is_cvp_conf (c)	InterScan CVP configuration file	/etc/iscan/iscvp.conf	any valid directory	iscvp.conf
svcport (c)	port used by both FireWall-1 and InterScan	18181	any number	set port for FireWall-1 and InterScan
logfile (c)	log file location	/etc/iscan/log	any valid directory	
auth_port (c)	OPSEC authentication port	no	yes no	use if using FireWall-1 OPSEC authentication
plugin (c)	states whether or not there is a plug-in	no	yes no	plug-in available plug-in not available
macroscan (c)	macro scan status	no	yes or no	status of macro scan
macro_act (c)	defines macro scan action	quarantine	quarantine or clean	you can either quarantine macros or strip off macros and deliver the attachment

[Notification]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
server (s,c)	SMTP server used to deliver virus notifications	foo	null; location; hostname	null= localhost; location=use if sendmail hostname=use if MTA
port (s,c)	SMTP port number	25	any port	null=25 or specify other

[HTTP]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
addr_to_host (s,c)		no	yes or no	enable if you want to write connection message like hostname and IP to log
plugin (s,c)	states whether or not there is a plug-in	no	yes no	plug-in available plug-in not available
log_trans (s,c)	logs client requests	yes	yes no	logging enabled logging disabled
show_is_name (s,c)	shows InterScan host name in virus warning	yes	yes, no	
cli_timeout (s,c)	time in seconds	5	any number	client times-out if no response within amount of time
srv_timeout (s,c)	time in seconds	120	any number	server times-out if no response within amount of time
proxy_acl (s,c)	IP addresses or host names separated by a comma or space	none	any IP address or host-name.Supports wilcard character * for all IP addresses within a specified range, e.g. 10.0.0.*	List of connectable host names or IP addresses. Host names IP addresses must be preceded by the number/pound symbol, i.e., "#"

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
mon_port (s)	The port number where InterScan's SMTP performance data can be obtained	10001	null; any free port	a value of zero or less disables performance monitoring
tmpdir (s,c)	temporary directory	/tmp	any dir	specify dir with 256+MB
idle_kill (s)	terminate unused child processes	3600	integer, seconds	null, zero=disabled 900=15min;3600=1hr
max_proc (s)	maximum simultaneous child processes	25	integer	null, zero=unlimited
proc_max_reqs (s)	kill child processes upon reaching	500	integer	null, zero=disabled
thr_per_proc (s)	max. active connections per child process	5	integer	typically five or fewer, depends on resources
pre_spawn (s)	available processes upon system start-up.	2	integer	typically two, depends on system resources
dead_time (s)	time in minutes	8	integer	time to force termination of slave processes
svcport (s)	main service port	80	port number	typically 80 or 8080, depends on setup
logfile (s,c)	log file location	/etc/iscan /log	any directory	location of log file
self_proxy (s)	InterScan acts as own proxy (HTTP & FTP)	yes	yes no	InterScan acting as its own proxy is fastest

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
original (s)	InterScan scans for a proxy; specify location	foo.com 80	location; hostname port	local daemon remote or local proxy
skip (s,c)	listed HTTP types not scanned	yes	yes no	do not scan listed types scan all types
oskiptype (s,c)	The listed MIME types are not scanned	image/ audio/ applica-tion/x-director video/ applica-tion/pdf multipart	MIME type	root (image/) means all subtypes not scanned
skiptype (s,c)	The listed MIME types are not scanned	image/ audio/ applica-tion/x-director video/ applica-tion/pdf multipart	MIME type	root (text/) means all sub-types not scanned
block (s,c)	content blocking	no	yes no	specified contents blocked/not blocked
oblock_types (s,c)	these HTTP replies are always blocked	java exec	java exec	java apps .com, .exe, etc.
block_types (s,c)	these HTTP replies are always blocked	none	java exec	java apps .com, .exe, etc.
warn_types (s,c)	HTTP users are warned when downloading these types	none	java exec	java apps com, .exe, etc. File is downloaded
move_types (s,c)	these HTTP replies are always moved	none	/etc	any directory; recipient does not get file

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
level (s,c)	indicates which files to scan	scanall	scanall scanext	all files are scanned; specified types scanned
extensions (s,c)	scans specified extensions (*level* must be set to scanext	.com .exe .sys .drv .cmd .dll .386 .doc		any file extension is valid;
progress_report (s,c)	users see a status report re: down-loads	no	yes no	report appears in browser; no report
no_progress_size (s,c)	min. file size for showing prog. report.	1024	In KB	faster the network, larger the number
no_progress_type (s,c)	skip progress reports for listed file types	image/ audio/ video/	any MIME file type	image/ to include all sub-types
action (s,c)	action on virus; interscan will take the specified action	clean	pass delete move clean	ignore file erase file move to specified dir remove virus
ucaction (s,c)	specified action when file is uncleanable	move	pass delete move	ignore file erase file move to specified dir
movedir (s,c)	InterScan *moves* infected files to this directory	/etc/iscan /virus	any valid directory and file-name	directory where infected files are placed when files are moved
passwait (s,c)	minutes InterScan waits for the user to retrieve infected file if action is set to *pass*	2	0 - 10	minutes
from_addr (s,c)	appear in From: field of notification	root@loc alhost	any email address	can be valid email address or label only

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
notify_admin (s,c)	notify Administrator when virus detected	no	yes no	Sys Admin is notified/ not notified
admin_addr (s,c)	Where InterScan sends the notification	root	email address	Typically, the Sys Admin's email address
admin_msg (s,c)	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 (s)	use passive mode for communication with remote FTP server	no	yes no	Choose yes when self_proxy =yes and FTP URL is requested.
proxy_behind (s,c)	is InterScan<--> proxy<-->client?	no	yes no	match your setup topology
trickle_period (s,c)	data advance to client; keep connection alive	2048	any	bytes (must be smaller than trickle_period)
trickle_amount (s,c)	amount received, at which data trickled	5	any	kilobytes
ftp_user (s,c)		none		Defining user name and password allows InterScan to access FTP servers that check the domain name of the user.
ftp_passwd (s,c)		none		
macroscan (s,c)	macro scan status	no	yes or no	status of macro scan

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
macro_act (s,c)	defines macro scan action	quarantine	quarantine or clean	you can either quarantine macros or strip off macros and deliver the attachment
addtl_virus	determines whether content is added to the HTTP blocking notification message	no	yes, no, replace	"yes" appends content to message, "replace" substitutes new text for the message
addtl_virus_message	the content that either is added to, or replaces, the HTTP scanning blocking message	If you have questions, contact administrator.	any text	text that is either appended to, or replaces, the notification message

[FTP]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
addr_to_host (s,c)		no	yes, no	
plugin (s,c)	states whether or not there is a plug-in	no	yes no	plug-in available plug-in not available
log_trans (s,c)	log client requests	yes	yes, no	
show_is_name (s,c)	shows InterScan host name in virus warning	yes	yes, no	
srv_timeout (s,c)	time in seconds	120	any number	server times-out if no response within amount of time

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
proxy_acl (s,c)	IP addresses or host names separated by a comma or space	none	any IP address or hostname.Supports wilcard character * for all IP addresses within a specified range, e.g. 10.0.0.*	List of connectable host names or IP addresses. Host names IP addresses must be preceded by the number/pound symbol, i.e., "#"
mon_port (s)	The port number where InterScan's SMTP performance data can be obtained	10011	null; any free port	a value of zero or less disables performance monitoring
tmpdir (s,c)	used to hold copies of files while being scanned	/tmp	any directory	specify dir with 256+MB
addtl_cmd (s,c)	remote authentication for ftp servers	none	auth response	firewall's authentication support
idle_kill (s)	Number of seconds after which idle child processes are killed	3600	integer, seconds	a value of zero or less disables this feature (idle child processes are never terminated).
max_proc (s)	Maximum number of simultaneous child processes	25	numeric, no limit	a value of zero or less disables this feature
proc_max_reqs (s)	InterScan will kill child processes after this number of connections is reached.	500	numeric, no limit	a value of zero or less disables this feature

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
thr_per_proc (s)	Maximum number of active connections per child process	5	numeric	Usually less than 10
pre_spawn (s)	Number of processes available on system start-up.	2	numeric	Usually less than 6
dead_time (s)	Number of minutes before killing process	8		Used to terminate processes that do not terminate normally
svcport (s)	Main service port	21	numeric	This number is usually 21 for FTP
logfile (s,c)	log file location	/etc/iscan /log		
self_proxy (s)	use InterScan as its own HTTP proxy	yes	yes no	If yes, InterScan uses dynamic mode; users must log in using ***user@host***
original (s)	The location of the original proxy server	/usr/sbin/in.ftpd	null	if null, InterScan is own proxy (fastest); path to the ftpd service
level (s,c)	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
extensions (s,c)	Scan files with the specified extensions: (*level* must be set to specific extension)	.com .exe .sys .drv .cmd .dll .386 .doc	.com .exe .sys .drv .cmd .dll .386 .doc	separate multiple entries with a comma
action (s,c)	What InterScan should do with infected files	clean	pass delete move clean	pass infected file to user block infected files move infected files

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
ucaction (s,c)	specified action when file is uncleanable	move	pass delete move	ignore file erase file move to specified dir
movedir (s,c)	InterScan *moves* infected files to this directory	/etc/iscan /virus	any valid directory	directory where infected files are placed when files are moved
greeting (s)	Indicate whether InterScan sends a greeting when connection is established	yes	yes no	The greeting is "220 - InterScan ... Ready." The greeting message is not user configurable
getmode (s)	InterScan's behavior while receiving FTP files	normal	normal local	Universal Mode Same machine, fastest. (see chapter 5)
putmode (s)	InterScan's behavior while sending FTP files (see Chapter 5)	normal	normal thru local	Universal Mode different machine, fast same machine
from_addr (s,c)	appears in From: field of notification	root@localhost		
notify_admin (s,c)	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin is not notified
admin_addr (s,c)	Where InterScan sends the notification	root	email address	for example, *root* or swen@trend.com

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
admin_msg (s,c)	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
macroscan (s,c)	macro scan status	no	yes or no	status of macro scan
macro_act (s,c)	defines macro scan action	quarantine	quarantine or clean	you can either quarantine macros or strip off macros and deliver the attachment

[SMTP]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
addr_to_host (s,c)	Used when writing connection messages to log file	no	yes, no	
plugin (s,c)	states whether or not there is a plug-in	no	yes no	plug-in available plug-in not available
plugin_dsc_dir (s,c)	the path directory containing the pointer file for plugin program	/etc/iscan_plugins		
content_alert_subject	subject line for notifications	configurable text	configurable text	this text is put in the subject line of notifications for eManager plug-in scanning notifications

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
virus_alert_subject	subject line for notifications	config-urable text	config-urable text	this text is put in the sub-ject line of notifications for virus scanning notifications
save_msgid (s,c)	save message ID from received mail	yes	yes, no	
data_intval_time (s,c)	prevent sendmail timeout by send-ing NOOP com-mand	300	integer	time in seconds
msg_size (s,c)	limits the size of email received	0	any integer	Can use letters K, M, and G. For example, 5K= 5 kilobytes and 5G=5 gigabytes 0= no limit
log_trans (s,c)	get transaction his-tory	yes	yes, no	
tmpdir (s,c)	used to hold copies of files while being scanned	/tmp	any direc-tory	
fn_len (s,c)	maximum length allowed email attachment file name	200	>=0	
show_is_name (s,c)	shows InterScan host name in virus warning	yes	yes, no	
cli_timeout (s,c)	time in seconds	120	any number	client times-out if no response within amount of time
srv_timeout (s,c)	time in seconds	120	any number	server times-out if no response within amount of time

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
proxy_acl (s,c)	IP addresses or host names separated by a comma or space	none	any IP address or hostname.Supports wilcard character * for all IP addresses within a specified range, e.g. 10.0.0.*	List of connectable host names or IP addresses. Host names IP addresses must be preceded by the number/pound symbol, i.e., "#"
out_check (s)	enable outbound mail options	no	yes, no	
local_domain (s)		localhost #127.0.0.1		
accept_rcpt (s)	local domains that will accept incoming mail	none	any domain name	separate multiple entries with a comma
out_block (s)	enable outbound infected mail blocking	no	yes, no	
anti_relay (s)	enable anti-relay	no	yes, no	
out_disclaimer (s)	add outbound disclaimer text	no	yes, no	
mon_port (s)	The port number where InterScan's SMTP performance data can be obtained	10021	null; any free port	a value of zero or less disables performance monitoring

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
idle_kill (s)	Number of seconds after which idle child processes are killed	3600	numeric, seconds	a value of zero or less disables this feature (idle child processes are never terminated)
max_proc (s)	Maximum number of simultaneous child processes	25	numeric, no limit	a value of zero or less disables this feature
proc_max_reqs (s)	InterScan will kill 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 killed.
thr_per_proc (s)	Maximum number of active connections per child process	5	numeric	Usually less than 10
pre_spawn (s)	Number of processes available on system start-up.	2	numeric	Usually less than 4
dead_time (s)	time in minutes	8	integer	time to force termination of slave processes
svcport (s)	Main service port	25	numeric	This number is usually 25 for SMTP
logfile (s,c)	location of log file	/etc/iscan /log	any directory	
original (s)	Location (host port or command argument) of SMTP server	/usr/lib/ sendmail -bs		This value must be defined
level (s,c)	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
extensions (s,c)	Scan files with the specified extensions: (*level* must be set to specific extension)	.com .exe .sys .drv .cmd .dll .386 .doc	.com .exe .sys .drv .cmd .dll .386 .doc	separate multiple entries with a comma
action (s,c)	What InterScan should do with infected files	clean	pass delete move clean	pass infected file to user block infected files move infected files
ucaction (s,c)	action on uncleanable files	move	pass delete move	pass infected file to user block infected files move infected files
movedir (s,c)	InterScan *moves* infected files to this directory	/etc /iscan /virus	any valid directory	directory where infected files are placed when *action=move*
greeting (s,c)	Indicate whether InterScan sends a greeting when connection is established	yes	yes no	The greeting is "220 - InterScan ... Ready." The greeting message is not user configurable
from_addr (s,c)	sender's address for notification email	root@localhost	any email address	
notify_admin (s,c)	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin is not notified
admin_addr (s,c)	Where InterScan sends the notification	root	email address	For example, *root*, or swenson@trend.com

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
admin_msg (s,c)	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 (s,c)	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
user_msg (s,c)	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 email" parse file name parse date parse virus name parse action taken
notify_sender (s,c)	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
sender_msg (s,c)	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 email" parse file parse date parse virus name parse action taken
addtl (s,c)	send additional message	no	yes, no, replace	

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
addtl_message (s,c)	Additional message to include to recipient if a virus is found in the email	see Value explanations	any	"If you have questions, contact administrator."
safe_stamp (s,c)	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 (s,c)	Message text of the Safe Stamp	none	any text %F	Message recipients receive when no viruses are found in their email. parse file name
rlocation (s,c)	location of virus message and disclaimer	top	top, bottom, or none	Note: if none is selected, **no** virus messages will be inserted.
skip_msgid (s,c)	do not scan messages with this ID	none	any message ID	separate multiple entries with a comma
macroscan (s,c)	macro scan status	no	yes or no	status of macro scan
macro_act (s,c)	defines macro scan action	quarantine	quarantine or clean	you can either quarantine macros or strip off macros and deliver the attachment
unaccept_err_msg (s, c)	allows configuration of the SMTP-Return Code message (550) that is sent to a mail client when content is blocked by InterScan VirusWall	Unacceptable content	any text	a general explanation why a message is rejected by InterScan VirusWall

[Periodical-Scan]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
Frequency (s,c)	frequency of automatic virus scans	Daily	daily none weekly monthly	scan selected dirs daily do not scan (disable) scan weekly scan monthly
DayOfWeek1 (s,c)	day to download new virus pattern file	Thursday	Monday through Sunday	only valid when *frequency=weekly*
DayOfMonth (s,c)	date to download new virus pattern file	14	1 through 31	only valid when *frequence=monthly*
Hour (s,c)	start time of scheduled scan	1	1 through 12	
Minute (s,c)		00		
APM (s,c)	day or night start time	AM	AM PM	not case sensitive (but no periods or spaces)
WeekPass (s,c)		0		
level (s,c)	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
extensions (s,c)	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
Dir (s,c)	InterScan writes it's Manual scan log file here	/export/home	any valid directory and filename	

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
Recursive (s,c)	Scan all sub-directories under target directory	yes	yes no	scans files in sub-dirs. only files in dir. scanned
notify_admin (s,c)	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin not notified
admin_addr (s,c)	Where InterScan sends the notification	root	email address	Typically, the Sys Admin's email address
admin_msg (s,c)	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 (s,c)	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 (s,c)	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
action (s,c)	What InterScan should do with infected files	clean	pass delete move clean	pass infected file to user block infected files move infected files clean infected file, if uncleanable, action defaults to pass

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
movedir (s,c)	InterScan *moves* infected files to this directory	/etc/iscan /virus	any valid directory	directory where infected files are placed when *action=move*
Prefix (s,c)	prepended to virus log file name	vir	not config-urable	

[Manual-Scan]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
level (s,c)	Files to scan	scanall	scanall scanext	all files are scanned only types specified below are scanned
dir (s,c)	InterScan writes it's Manual scan log file here	/export/home	any valid directory	
recursive (s,c)	Scan all sub-directo-ries under target directory	yes	yes	must scan all sub-dirs.
extensions (s,c)	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 possi-ble values
notify_admin (s,c)	InterScan can notify the Administrator when a virus is detected	yes	yes no	Sys Admin is notified Sys Admin is not notified
admin_addr (s,c)	Where InterScan sends the notifica-tion	root	email address	Typically, the Sys Admin's email address

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
admin_msg (s,c)	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 (s,c)	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 (s,c)	InterScan can notify user when a virus is detected	yes	yes no	user is notified user is not notified
action (s,c)	What InterScan should do with infected files	clean	pass delete move clean	pass infected file to user block infected files move infected files clean infected file, if uncleanable, action defaults to pass
movedir (s,c)	InterScan *moves* infected files to this directory	/etc/iscan /virus	any valid directory	directory where infected files are placed when *action=move*
Version (s,c)	current virus pattern file version number	639	numeric	number is derived from virus pattern file itself
Method (s,c)	pattern update method	automatic	automatic manual	updated automatically updated on command
Prefix (s,c)	added to front of virus log name	vir	not configurable	

[Pattern-Update]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
Version (s,c)	current virus pattern file	676	numeric	the latest file has the highest number
method (s,c)	pattern update method	automatic	automatic or manual	
admin_addr (s,c)	Where InterScan sends the notification	root	email address	Typically, the Sys Admin's email address
Subject (s,c)	subject line in messages	Pattern Update		
Frequency (s,c)	frequency of automatic virus pattern file updates	Monthly	none weekly monthly	no automatic download weekly download download monthly
DayOfWeek1 (s,c)	day to download new virus pattern file	Sunday	Monday through Sunday	only valid when *frequency=weekly*
DayOfWeek2 (s,c)	alternate day to download new virus pattern file	none	Monday through Sunday	only valid when *frequency=weekly*
DayOfMonth (s,c)	date to download new virus pattern file	1	1 through 31	only valid when *frequency=monthly*
hour (s,c)	start time of scheduled scan	1	1 through 12	
APM (s,c)	day or night start time	AM	AM PM	not case sensitive (but no periods or spaces)

[View-Configuration]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
Sort	sort type	Date	date, user, virus	
FTP	generate FTP virus scan report	yes	yes, no	
Mail	generate Mail virus scan report	yes	yes, no	
HTTP	generate HTTP virus scan report	yes	yes, no	
Periodic	generate virus report from pre-scheduled scan	yes	yes, no	
Manual	generate report from manual file server scan	yes	yes, no	
OfficeScan	for future release			do not use
Date	report range	Week	all, range, week, One-Day, Month	
SYear	start date of range	1997	any year	
SMonth	start date of range	January	any month	
SDay	start date of range	1		
EYear	end date of range	1997	any year	
EMonth	end date of range	March	any month	
EDay	end date of range	31		
User		All	all, or User-Name	
Username		FooUser		

Virus		All	all, or Virus-sName	

[Registration]

Parameter	*Parameter explanations*	*Default Value*	*Possible Values*	*Value explanations*
Upasswd (s,c)	For future release. Do not use.			
Product (s,c)	Product name	Inter-Scan Virus Wall		InterScan VirusWall
Version (s,c)	Product version	3.5		3.5
Serial (s,c)	Product serial num-ber	none	only one valid #	generated by InterScan, do not change!
Date (s,c)	Registration date	none	date	current date or purchase date
FirstN (s,c)	your first name			
LastN (s,c)	your last name			
EMail (s,c)	email address			
HPhone (s,c)	home phone number			include area code
OPhone (s,c)	office phone number			include area code
Fax (s,c)	fax number			include area code
RealAddr (s,c)	mailing address			address, number, street
City (s,c)	city			

State (s,c)	state			two-letter abbreviation
ZIP (s,c)	zip code			
Country (s,c)	country			blank if USA
Company (s,c)	name of your company			
use_proxy (s,c)	do you use a proxy server?	no	yes no	a proxy server is used no proxy server is used
reg_proxy (s,c)	proxy server, if any	proxy.foo.com	any proxy name or address	if *use_proxy-yes*, enter the name (or location) of the proxy server
reg_port (s,c)	registration port	8080	port number	port number used by proxy server, if any
Puser_id (s,c)	supports proxy authorization	none		
Ppasswd (s,c)	supports proxy authorization	none		
hostname (s,c)	location of latest virus pattern file	www.trendmicro.com		Trend Micro's server, or companies server with newest virus pattern file

Appendix A

Configuring intscan.ini with ACL Information

This appendix describes the acceptable format for entering Access Control List (ACL) information into the intscan.ini file. It applies to the following versions of InterScan VirusWall for Unix:

- InterScan VirusWall 3.5, 3.6, and 3.7 for Solaris

- InterScan VirusWall 3.5, 3.6, and 3.76 for Linux

- InterScan VirusWall 3.5, 3.6, and 3.7 for HP-UX

- InterScan Virus Wall 3.5 and 3.6 for AIX

The parameters of intscan.ini that accept ACL formatted values are:

- proxy_acl

- local_domain

Note: ACL values are always delimited by a single space.

Using Domain Names and FQDNs (Fully Qualified Domain Names)

Here is an example of the format for domain name:

ACL: hostname1 mail1 hostname.domainname.com

Using IP Addresses

The general rules for IP Addresses as ACL values are as follows:

- Numbers should be prefixed with a "#" or enclosed within "[" and "]".
- Hexadecimal values are identified with a prefix of "0x"

Here is an example:

ACL: #1.3.2.5 [1.3.2.5] #0x01030205 [0x01030205] #16974341 [16974341]

Using and Defining Network Addresses

Network addresses as ACL values must be enclosed within brackets "[and]". For example:

ACL: [192.168.0.0/16] [192.168.0.0:255.255.0.0]

Using Wildcards

Wildcards will only work for hostnames and FQDNs. Wildcards *do not* work for IP addresses (for example 10.0.*.* or 10.0.*). Here is an example of how to use wildcards properly in a FQDN:

ACL: *.domain.com *.*domain.com a*.domain.com

In the above example, "*.domain.com" matches with:

subdom1.domain.com

subdom2.domain.com

Also referring to the above example, "*.domain.com" will *not* match with:

host.mydomain.com

host.yourdomain.com

"*.*domain.com" will match with:

anyhost.1stdomain.com

anyhost.2nddomain.com

anyhost.domain.com

"a*.domain.com" will match with:

ahost.domain.com

anotherhost.domain.com

"a*.domain.com" will *not* match with:

host.domain.com

host2.domain.com

Defining Global Values

Here is an example of how to define a global value:

ACL: * [0:0]

This entry allows *any host* to connect, and it is considered valid.

Using Negation

Here is an example of using negation:

ACL: !*.trendmicro.com !#127.0.0.1 !* ![0:0]

In the example above, "!*.trendmicro.com" denies access to any host identified as belonging to "trendmicro.com".

"!#127.0.0.1" denies access to the local host or the same machine.

"!*" and "![0:0]" denies access to everyone or any host.

Reviewing Detailed Examples

Here are some detailed examples that illustrate the rules described so far in this Appendix.

Example 1

ACL: localhost #127.0.0.1 *.mydomain.com [192.168.0.0/16]

The above example will allow relay (in the case of local_domain) or will allow connections (in the case of proxy_acl) from:

a. The resolved localhost (for example, the same server)

b. The same server

c. All hosts whose FQDN is resolved to have ".mydomain.com".

d. The Class B network of "192.168.0.0"

Example 2

ACL: !#192.168.0.1 !#192.168.0.2 [192.168.0.0/16]

The above example will allow everyone into the Class B network of "192.168.0.0" except for the "192.168.0.1" and "192.168.0.2" hosts. The sequence of the entries is crucial for this ACL to function properly.

Example 3

ACL: !*.banned-domain.com [0:0]

In the above example, everyone except those from "banned-domain.com", will be allowed relays or connections.

Using the "addr_to_host" Parameter of intscan.ini

For InterScan to recognize or be able to translate hostnames and FQDNs (Fully Qualified Domain Names), the "addr_to_host" parameter of intscan.ini must be set to "yes", using the following procedure:

1. Open /etc/iscan/intscan.ini with a text editor.

Note: It is advisable to make a backup copy of intscan.ini before editing it, as a precautionary measure.

---

2. Under the [HTTP] section, edit the "addr_to_host" parameter so that it reflects the following information:

```
addr_to_host=yes
```

3. Repeat Step 2 for the "addr_to_host" parameters found in the [FTP] and [SMTP] sections.
4. Save the modified intscan.ini file.

When using the "proxy_acl" parameter, make sure "addr_to_host=yes" for the [HTTP] and [FTP] sections of intscan.ini.

When using both "proxy_acl" and "local_domain" parameters, make sure "addr_to_host=yes" for the [SMTP] section of intscan.ini.

The "addr_to_host" parameter is responsible for making InterScan VirusWall use DNS to resolve connecting IP addresses to their corresponding FQDNs or hostnames.

Index

M

N

O

P

R

S

T

U

V

W