TREND MICRO™

InterScan™ VirusWall™ 3

Virus protection for Internet gateways

for Windows Servers

Administrator's Guide

TREND MICRO™

Document Part No. IVEM31515/30529
Release Date: 04-30-2001

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

Contents

Chapter 3: Installing Trend Micro InterScan VirusWall

Chapter 4: Configuring Email VirusWall

Chapter 5: Configuring Web VirusWall

Chapter 6: Configuring FTP VirusWall

Chapter 7: Configuring Advanced Options

Chapter 8: Log Files

Chapter 9: Active Update

Chapter 10: Virus Encyclopedia

Chapter 11: Technical Support and Troubleshooting

Chapter 12: Intscan.ini File Settings

Appendix

Chapter 1

Introducing Trend Micro InterScan VirusWall

What is Trend Micro InterScan VirusWall?

Trend Micro InterScan VirusWall® is a suite of anti-virus programs that work at the Internet gateway to detect and clean virus-infected files before they enter the corporate network.

Email VirusWall monitors inbound and outbound email messages. *Web VirusWall* monitors all HTTP traffic, checking for viruses and malicious Java and ActiveX applets, and providing enterprise-wide Java standards. *FTP VirusWall* ensures that all file transfers made via FTP are virus-free.

Optionally available are a variety of plug-ins, called *eManager*, which give the administrator intelligent control over the allocation of network bandwidth, enterprise-wide junk mail filtering, and content filtering—a technology that monitors inbound and outbound email for sensitive or offensive content.

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

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

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

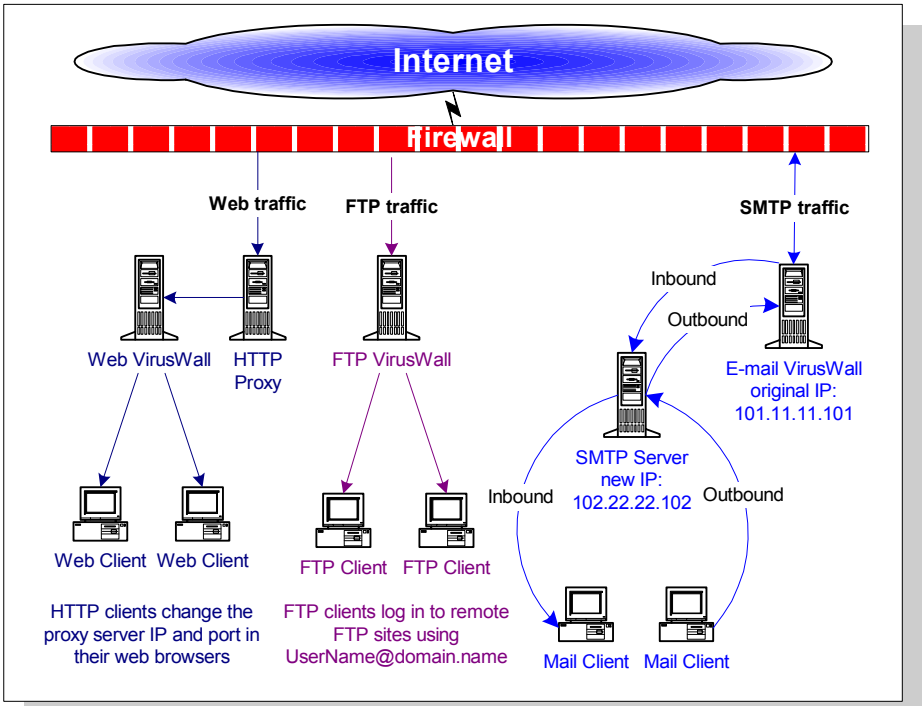


FIGURE 1-1. This topology shows Web, FTP, and Email VirusWall installed on a network. See other possible setups in Chapter 2.

Features and Capabilities

- Intercepts viruses at the Internet server or the Internet gateway—before they can enter your network and do any damage
- Protects all SMTP file transfers to and from the Internet, and HTTP—FTP downloads
- Scans inbound and outbound email messages
- Includes NT-integrated performance monitor for charting and analyzing VirusWall performance
- Provides Content Scanning with eManager
- Comes with an RFC compliant SMTP server
- Can be installed while the Internet gateway or Internet server is running—you do not have to reboot the system to install
- Complements your existing security and firewall system
- Contains the Trend Micro NCSA-certified, 32-bit, multi-threaded virus engine
- Uses the Trend Micro lightning-fast scan engine to detect and clean Macro and traditional viruses, as well as malicious Java and ActiveX code
- Active Update technology supports automatic updates of the virus pattern file and scan engine
- Allows the administrator to define a system-wide policy of Java blocking security rules
- Supports both local and remote program access via Windows GUI or web browser
- Uses HTML and text formats for viewing the log files
- Check Point OPSEC Certified
- Supports data trickle option to prevent server time-outs during HTTP and FTP file transfers

How Does InterScan VirusWall Work?

At its most basic, InterScan monitors all SMTP, HTTP, and FTP traffic between the LAN and Internet. Whenever it detects a file type that it has been configured to scan (for example, *.zip*, *.exe, .doc*), InterScan copies the file to a temporary location and opens the copy for virus checking.

If the file is clean, InterScan VirusWall deletes the copy and releases the original for delivery to the SMTP, FTP or HTTP server, which delivers the file as usual. If a virus is found, a notification is issued and InterScan takes the actions configured: **Clean**, **Delete**, **Move**, **Ignore** (or **Pass**).

When InterScan VirusWall Finds a Virus

Actions on Virus:

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

Whatever the action, a user-customized notification message can be issued to the intended recipient and any others specified. In the case of email, you can send a cleaned copy of the infected file back to the sender along with a brief message.

All virus-events and associated actions are noted in the log file.

Notifications

Notifications are as follows: Email 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 Email VirusWall, can be issued to the system administrator, the sender, and the intended recipient. If no viruses are found, Email VirusWall can insert a message into the original email stating that the email was scanned and found to be virus-free.

Of course, you can also completely mask the presence of InterScan VirusWall: no notifications are issued, and no InterScan information will appear in the header fields.

How InterScan VirusWall Finds Viruses

Pattern Matching

Using a process called "pattern matching," InterScan draws upon an extensive database of virus patterns to identify known virus signatures. Key areas of suspect files are examined for tell-tale strings of virus code and compared against the 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 it is decrypted. InterScan then scans the entire file, including the freshly decrypted code, and identifies any strings of mutation virus. InterScan then takes whatever action you have specified—clean the file, delete it, quarantine it, or ignore it.

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

MacroTrap™

Macro viruses are not confined to a particular operating system, they are application specific (i.e., the *application* acts as their operating system) and can be spread between DOS, Windows, MACs, and even OS/2 systems. This in itself is revolutionary. Now add the ability to travel by email, plus the tremendous interconnections of the World Wide Web and the increasing power of the Macro languages (Word, Excel, etc.), and you've got yourself a real threat. Trend Micro's new Macro Trap is designed to provide you with a means of protecting your network

users from ever receiving (or spreading) a Macro virus—without curtailing in any way email activities.

How it Works:

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

Compressed Files

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

Compressed files are opened and the contents examined according to the criteria specified in the Scan Files option of each VirusWall. When multiple layers of compression are encountered, InterScan recursively decompresses each, up to a limit of 20. In other words, if an archive contains *.cab* files that have been compressed using PK-ZIP, and LZEXE, PK-LITE, Microsoft Compress, etc., 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.

Performance

To maximize performance, InterScan makes some intelligent choices in regards to what files it scans, and the way it scans them. Only file types that are able to become infected and carry a virus are scanned. In addition, only key areas of these files are checked for matching virus "signatures." Files are checked against the Trend Micro proprietary database of some 15,000 known viruses. Furthermore, heuristic logic is used to analyze whether certain unknown code (unique to polymorphic viruses, for example) is virus-like in nature and warrants testing.

Obtaining a Serial Number

You product serial number can be found:

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

or obtained from a Trend Micro Sales representative at the following email address:

sales@trendmicro.com

Trial Version

Alternatively, you can install the free 30-day trial version. This 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 reinstall. Instead, open the Pattern Update page of the Trend Micro VirusWall configuration window and click **Register.** Enter the serial number you received along with your other information, and click **Register** again to send your information to Trend Micro.

Registering Trend Micro VirusWall

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

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

You can register over the Internet or by mail.

Performance Monitoring

InterScan VirusWall has built-in support for the NT Performance Monitor to provide relevant real-time information about each of its programs. Each InterScan VirusWall module will show up as an object within the Performance Monitor, and you can select which program variables you want to monitor in real-time.

Use the performance monitoring options to gather system statistics and help fine tune Email VirusWall's performance. The performance monitor uses a common interface to provide graphs, reports, and histogram representations of program data.

Starting the Performance Monitor

Performance Monitor can be accessed from the Activity Monitor (which resides, minimized, on the Windows NT taskbar) by clicking the **Perfmon** button.

Alternatively, you can start the Performance Monitor by clicking the Windows NT **Start** button, then **Administrative Tools (Common) | Performance Monitor**. Next, click **Edit | Add to Chart**.

Assuming that **Computer:** is the one where Email VirusWall is installed, click **Object**: and select InterScan. The new Email VirusWall parameters appear in the **Counter:** scroll box.

Double-click those that you want to track and modify Color:, Scale:, Width:, and Style: as desired. For a brief explanation of what any given counter measures, click the **Explain>>** button located on the right. Click **Add** to begin tracking the performance of the selected counter.

Note: Email VirusWall must be running for the performance parameters to work.

Running with eManager

eManager is an optional plug-in that expands the functionality Email VirusWall. It includes:

- Email Management
- Content Management
  - Spam filtering
  - Content filtering

Email Management

Email Management works with InterScan at the gateway to regulate the flow of traffic through the SMTP server according to the criteria you define.

You can, for example, postpone the delivery of messages to England until a time after peak SMTP usage hours in the USA, but before the start of business in London. The delivery of email messages with large attachments, too, can be postponed until off-peak hours. Sophisticated SMTP usage analysis and convenient charting are provided.

Content Management

Content Management provides a means for the SMTP administrator to evaluate and stop email on the basis of the message text itself.

Use Content Management, for example, to ensure that your SMTP server is not being used as a spam-mail router, to check whether anyone is sending out confidential information, using inappropriate language with customers, sending out resumes, or otherwise exposing the organization to abuse and liability.

When applied to inbound messages, content filtering provides the opportunity for a more sophisticated message analysis than the Anti-spam filter alone.

Anti-spam filter

Anti-spam filter helps to eliminate unwanted email before it can be processed by the SMTP server or distract your email clients.

It works by employing user-defined policies to evaluate and block messages on the basis of the information appearing in the header, i.e., the domain from which the email was sent or the contents of the **From:**, **To:**, and **Subject:** fields.

To find out more about eManager contact your Trend Micro representative or email the following address:

sales@trendmicro.com

Trend Micro System Cleaner

Trend Micro System Cleaner helps restore your Windows system after a Trojan attack. A Trojan, like a virus, attacks your system (but unlike a virus, a Trojan cannot self-replicate). When a Trojan is executed, you will likely experience unwanted system problems in operation, and sometimes loss of valuable data. These are indications that you should run the Trend Micro System Cleaner on your system.

There are two versions of Trend Micro System Cleaner. Both are free, and are described below:

- **Trend Micro System Cleaner (TSC)** works in conjunction with HouseCall, PC-cillin, and OfficeScan. Whereas these applications let you clean or delete infected files, TSC not only detects and remove Trojans, it also rids your system of dropped code and restores settings that were altered as the result of the attack.
- **Trend Micro System Cleaner Package** was developed specifically for users without Trend Micro products, and offers the same benefits as TSC. The System Cleaner Package is provided as a public service, and can be downloaded free from the Trend Micro website.

Both versions support the following:

- Terminates all malware instances in memory
- Removes malware registry entries
- Removes malware entries from system files

Additionally, the Trend Micro System Cleaner package:

- Scans for and deletes all malware copies in all local hard drives

For more information, visit:

http://www.trendmicro.com/download/tsc.asp

Chapter 2

Installation Planning

Installation Overview

The Trend Micro InterScan VirusWall anti-virus package for the gateway contains real-time scanning services that check for viruses in email (SMTP), web (HTTP), and file (FTP) transfers to and from the LAN.

Installing the VirusWalls takes about ten minutes and should be performed from the machine where the program(s) will reside. Allow another 10 or so minutes to configure InterScan to work with your existing servers. Configuration can be performed locally from a Windows NT GUI, or remotely using a web browser to access the HTML-based interface.

All three services can be installed on the same machine, or each installed onto a different machine. However, installing multiple services onto the same server is not typically recommended because scanning network traffic streams in real-time, along with the usual operations of the server, can be rather CPU and disk-intensive.

What is more typical is to run multiple iterations of Setup to install each VirusWall onto its own server (perhaps the same one that hosts the SMTP, HTTP, or FTP server). For example, run Setup once to install Email VirusWall on to the SMTP server, again to install Web VirusWall onto a HTTP proxy server, and then again to install FTP VirusWall.

System Requirements

Install InterScan on a server with at least the following:

- PC with a Pentium 200 or faster processor
- Windows 2000 or Windows NT version 4.0 build 1381 with Service Pack 3.0
- 64 MB of memory; 128 MB recommended
- 25 MB free disk space for program files; 100 to 500 MB is recommended for optimal performance on high-traffic systems
- A 800x600 monitor; 1024x768 or higher resolution is recommended
- Microsoft Internet Information Server must be installed to run the web-based configuration utility.

*Additional requirements for Web VirusWall

If you are installing Web VirusWall, add the following requirements:

- An HTTP proxy server

Planning Ahead

By default Email VirusWall takes port 25, Web VirusWall takes port 8080, and FTP VirusWall takes port 21. Depending on which services are installed and what proxy servers you have on the system, you may be prompted for the following information:

- The IP address of the current SMTP server
- The port number of the current SMTP server
- The IP address of the current HTTP proxy server
- The port number of the current HTTP proxy server
- The port number InterScan will use if it is set up as the HTTP proxy server
- The IP address of the current FTP proxy server
- The port number of the current FTP proxy server
- The port number InterScan will use if it is set up as the FTP proxy server

Microsoft Exchange

Email VirusWall will detect whether it is being installed onto the same machine as Microsoft Exchange and will prompt you to change the Exchange IMC (Internet Mail Connection) port from 25 to 6000.

Installing Web VirusWall

Web VirusWall may fail to load if there is already an HTTP server service running on the same machine. InterScan VirusWall's HTTP scanner listens on port 8080 by default. This port assignment can be changed, but bear in mind that Microsoft's Internet Information Server uses port 80, thus InterScan VirusWall HTTP scanner cannot be changed to port 80.

An HTTP proxy server on the network is required to install Web VirusWall.

Deciding Where To Install Trend Micro InterScan VirusWall

Generally speaking, it is best to install InterScan on a NT server that is inside the firewall, if any, and "in front" of the server or proxy server it will complement.

In other words, after a firewall, InterScan should be first in line to receive the network SMTP, HTTP, and/or FTP traffic. You may need to modify your firewall configuration (IP and/or port) so it routes traffic to InterScan.

The appropriate VirusWall(s) will receive inbound Internet traffic as it crosses the gateway, check for viruses, clean infected files, and then send the traffic on to the original server for delivery as usual.

Installation Topologies

InterScan can be installed on the same machine as the original server or on a different machine. To determine which option is most suitable, gauge the peak and mean loads the server handles and compare it to the overall capacity of that machine. The closer the two measures are, the more likely it is that you will want to install InterScan on a dedicated machine. You may consider, for example, bandwidth, percentage of CPU utilization, system memory, swap-file size, amount of file queueing, and similar parameters.

On the other hand, installing InterScan on a dedicated machine means that files will need to be transferred to that machine for scanning and cleaning, then back for normal delivery (Email VirusWall can, optionally, use a DNS to deliver scanned mail).

Configuration

When InterScan is installed on the same machine as the original server, chances are you will need to change the port that the original is using (InterScan will take the default). When InterScan is installed on a different machine than the original server, chances are that the port will not need to be changed, but requesting clients may need to modify the IP address they use to access the proxy (change it to the Trend Micro VirusWall's).

Installing Email VirusWall on the Same Machine as the Existing Email Server

If your SMTP server allows you to reassign port numbers, you can install InterScan on the same machine as that server. In this case, assign the original email server a new port number, for example, port 6000 or above. If you are using Microsoft Exchange, Email VirusWall Setup will detect this condition and prompt you to change the port number during installation. Whichever SMTP server you may be using, Email VirusWall must take port 25.

Installing Email VirusWall on a Dedicated Machine

If you are installing InterScan VirusWall on a dedicated machine, you may be able to keep the same relative IP address for your clients by giving Email VirusWall the original SMTP server's host name.

Other options include changing the client configurations to reflect Email VirusWall as the new (initial) SMTP server, editing the MX record to reflect the change, and swapping IP addresses between the two servers in question. The latter methods are outlined next.

Modify the MX record…

You can have the Email VirusWall machine receive SMTP traffic without modifying existing SMTP servers by modifying the MX record in the DNS configuration.

The idea is to edit the MX record so that it directs all incoming email to the Email VirusWall machine.

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

   For example, say the IP address of your original SMTP server is 111.11.11.11 and the host name of Email VirusWall is 222.22.22.22. In the InterScan SMTP Configuration page, enter 111.11.11.11 for **Forward mail to SMTP server at:**.

Swap IP addresses

If you don't want to change the MX record in the DNS, reroute incoming mail by assigning the IP address of the original server to the InterScan machine; assign a new IP address to the original server.

In the Email VirusWall configuration page, enter the original server's newly assigned IP address in the **Original server location** field.

Illustrations

The following illustrations are provided to acquaint you with possible Setup topologies. Use the one that best fits your needs, or apply the principles to a strategy of your own design.

Email VirusWall

Email VirusWall supports checking both inbound and outbound SMTP traffic for viruses and can be installed on a dedicated NT server or on the same machine as an existing SMTP server. In general, Email VirusWall should be installed inside a firewall and, for scanning inbound mail, before any existing SMTP servers. After scanning inbound traffic, Email VirusWall will then route it to the original SMTP server for delivery to the mail clients.

Fig. 2-1. Inbound: Use DNS to Deliver Mail

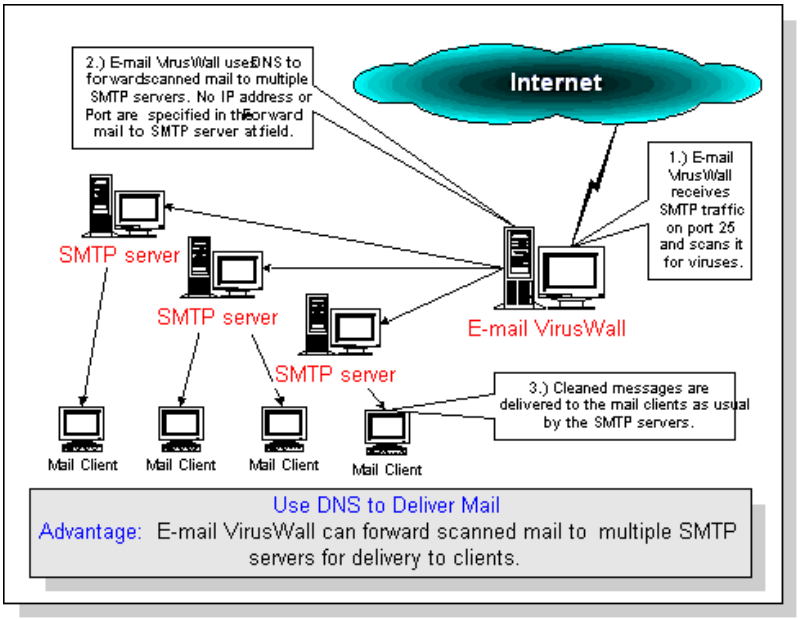


Fig. 2-2. Inbound: Different Machines, Setup 1

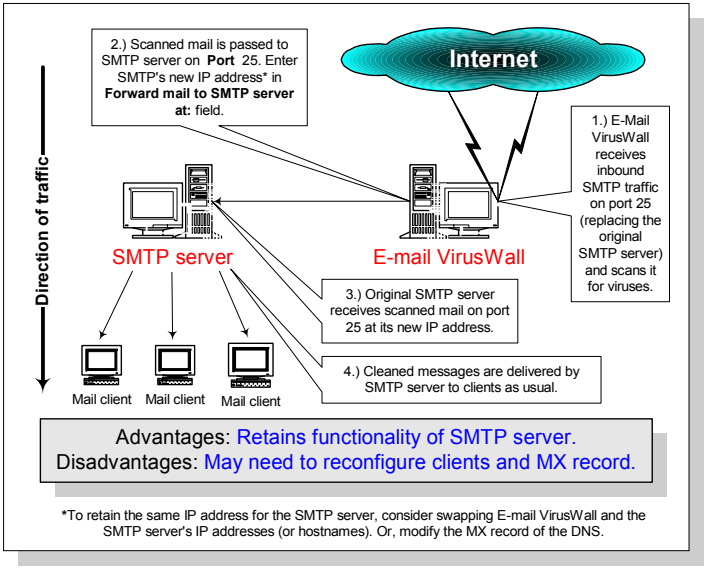


Fig. 2-3. Inbound Different Machines, Setup 2

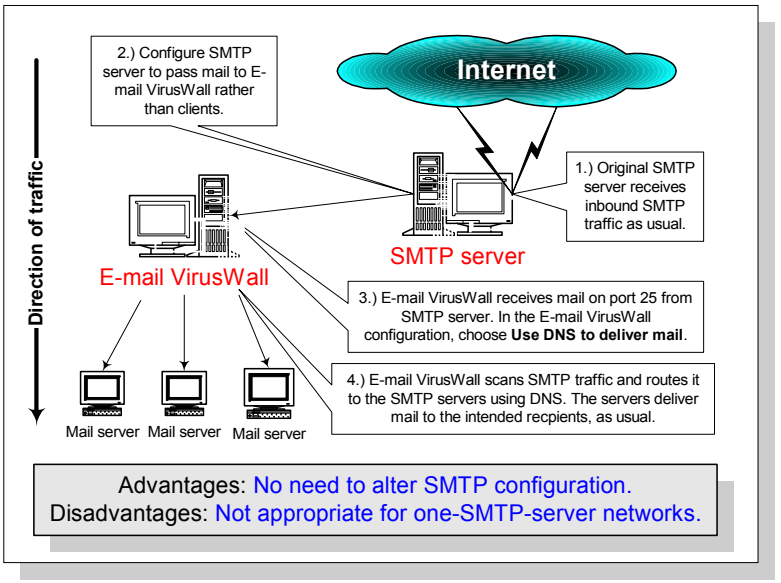


Fig. 2-4. Inbound: Same Machine

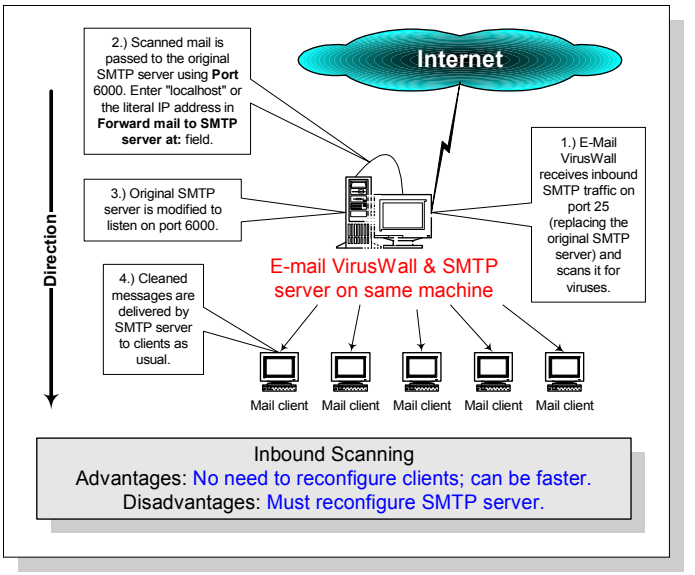


Fig. 2-5. Outbound: Use DNS to Deliver Mail

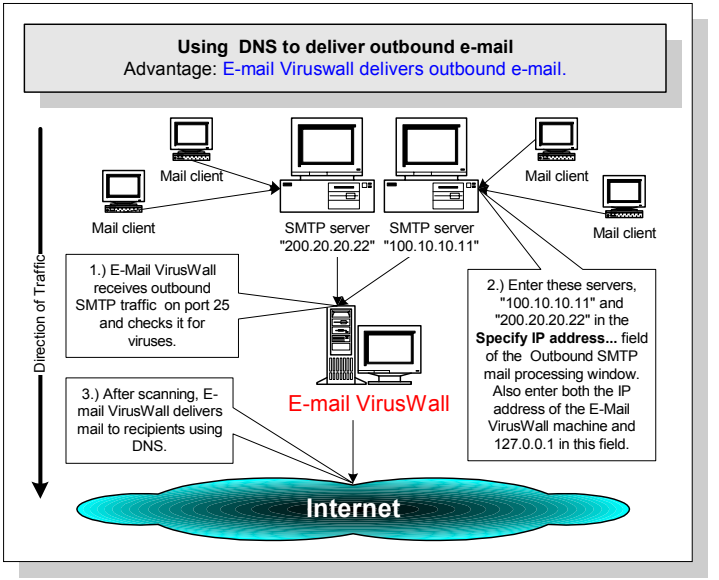


Fig. 2-6. Outbound: Different Machines

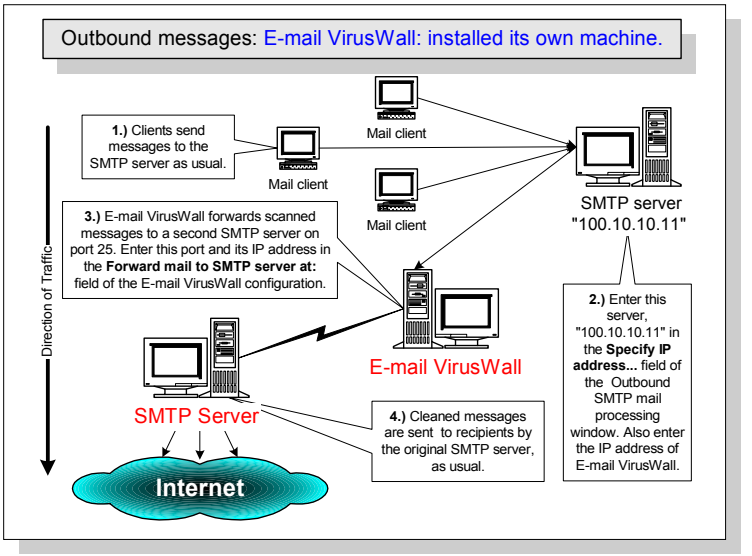
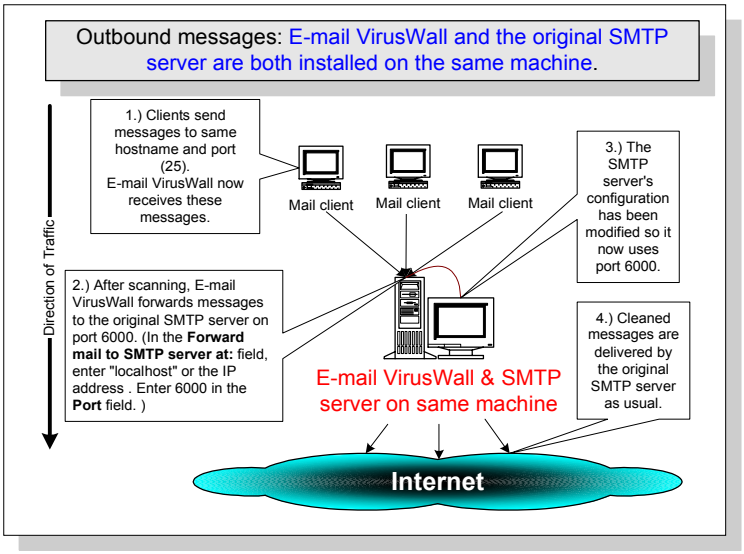


Fig. 2-7. Outbound: Same Machine



Web VirusWall

Web VirusWall can be installed on a dedicated NT server or on the same machine as an existing HTTP proxy server.

In general, install Web VirusWall inside the firewall and (logically) closest to the server accessed by clients. The client's TeleWindow download-progress monitor is not available if HTTP traffic is passed through a second proxy after Web VirusWall has scanned it.

The order in which the following illustrations appear is from most to least recommended—however, all three installations are valid and will produce HTTP traffic that is checked for viruses.

Fig. 2-8. Web VirusWall: After HTTP Proxy

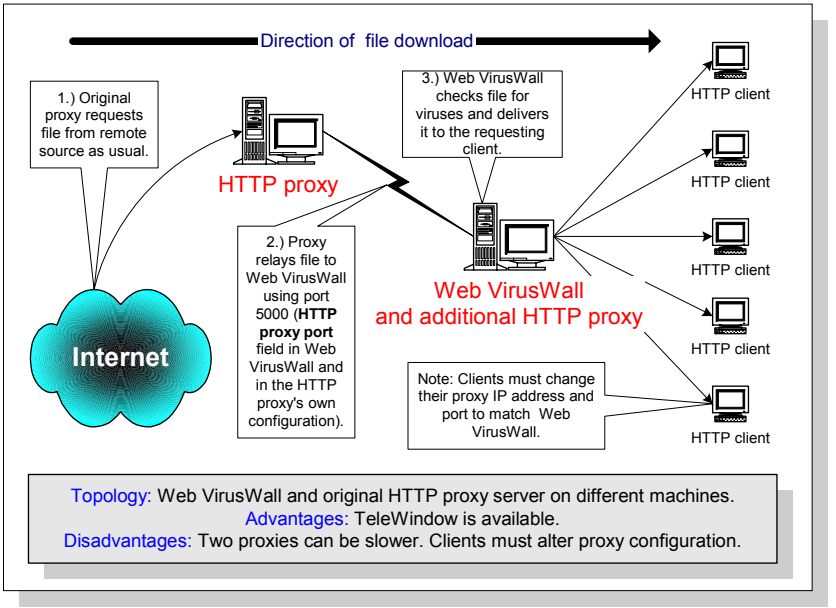


Fig. 2-9. Web VirusWall: Installed on Dedicated NT Server

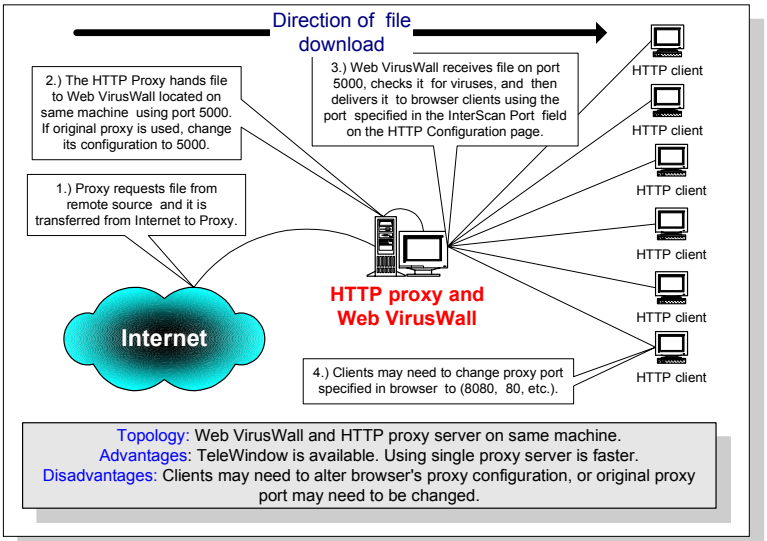
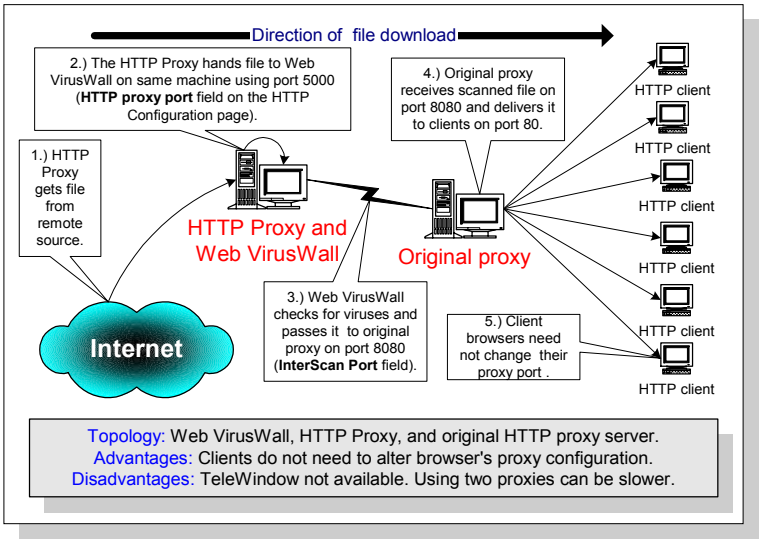


Fig. 2-10. Web VirusWall: Before HTTP Proxy



FTP VirusWall

Both illustrations assume that virus scanning is performed for the benefit of the FTP client, downloading files from a remote site onto the local LAN. Of course, you could also set it up so that virus scanning is performed on files being remotely downloaded from, or uploaded to, an FTP site that you are hosting.

Fig. 2-11. FTP VirusWall: Existing FTP Proxy Server

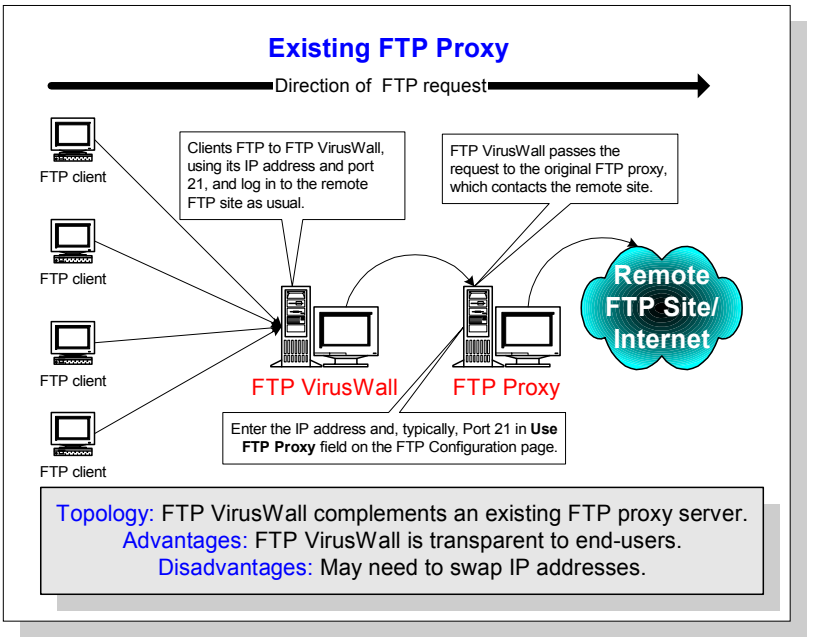
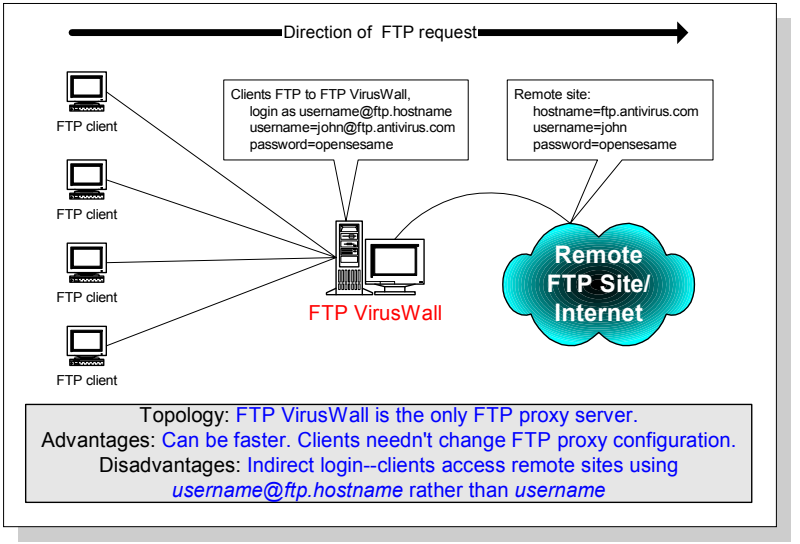


Fig. 2-12. FTP VirusWall: Stand Alone Mode



Although not illustrated, you can also install FTP VirusWall on the same server as an existing FTP proxy. The concept and procedure is much the same as for Web VirusWall: Give FTP VirusWall the default port (21) and have it forward scanned FTP traffic to the existing FTP proxy. Enter the FTP VirusWall machine's IP address and the Port FTP VirusWall will pass scanned traffic to the FTP proxy on.

You will likely need to modify the FTP proxy's port configuration.

Chapter 3

Installing Trend Micro InterScan VirusWall

Overview

In this chapter you will find step by step instructions for installing InterScan VirusWall and an explanation of the "quick configure" process that follows. Also presented are instructions for

- Accessing the configuration program
- Starting the individual services manually
- Testing your setup with a Test Virus
- 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. See Chapter 2 for installation planning.

Which Edition Should I Install?

InterScan VirusWall contains one Setup package that allows you to install either the standard edition of InterScan, or the one with Content Vectoring Protocol (CVP) support for Check Point Software's FireWall-1.

- Install the *standard edition* of InterScan if you are not running FireWall-1.
- Install *InterScan CVP edition* if you are running FireWall-1 (v.3.0b build 3064 or later) and want InterScan to act as a CVP server. If you are upgrading from a previous version of InterScan to the CVP edition, you must uninstall the existing version before installing the CVP edition.

A: Installing The *Standard* Edition

Installing the standard edition of InterScan VirusWall takes about ten minutes and should be performed from the machine where the program(s) will reside. Allow another ten or so minutes to configure InterScan to work with your existing servers. Configuration can be performed locally from a Windows NT GUI, or remotely using a web browser to access the HTML-based interface.

All three InterScan services can be installed on the same machine, or each installed onto a different machine. Installing multiple services onto the same server is not generally advisable. Scanning network traffic streams in real-time, along with the usual operations of the server, can be CPU and disk-intensive.

Typically, you run multiple iterations of Setup, thus installing each VirusWall onto its own server (this can be the same one as hosts the SMTP, HTTP, or FTP server). In this case, you would run Setup once to install Email VirusWall on to the SMTP server, relocate to the HTTP proxy server and run Setup again, then do the same for FTP VirusWall.

Deciding Where To Install

Generally speaking, it is best to install InterScan on a NT server that is inside the firewall (or in the DMZ) if any, and "in front" of the server or proxy server that InterScan will complement.

In other words, after a firewall, InterScan should be first in line to receive the network SMTP, HTTP, and/or FTP traffic. You may need to modify your firewall configuration (IP and/or port) so it routes traffic to InterScan. The appropriate VirusWall(s) will receive inbound Internet traffic as it crosses the gateway, check for viruses, clean infected files, and then send the traffic on to the original server for delivery as usual.

Step-by-Step Installation Instructions

Run Setup from the server where the program(s) will be installed. For example, after installing Email VirusWall, move to the HTTP proxy server that will host Web VirusWall and run Setup again.

1. Insert the **Trend Micro Enterprise Solution** CD into the appropriate drive. If you have Autoplay enabled, the disk will start automatically. Choose **InterScan VirusWall for NT** from the list of programs that appears, select a language, and click **Install**.
   - If Autoplay is not enabled, click the NT **Start** button, then **Run** and enter `[path]\go.exe` in the **Open** field.
   - If you are installing from a downloaded copy of the program, locate the directory containing the installation files and double-click `setup.exe`
2. After accepting the License Agreement (required to proceed) and specifying where to install InterScan, you are prompted to select the VirusWall(s) you want to install.
3. If you have purchased InterScan, enter the product serial number (serial numbers can be found on the front cover of this Administrator's Guide and on the product registration card). Use the same serial number for each VirusWall.

If You Are Installing the Trial Version

a. If you are installing the free 30-day trial version, press Enter without any a serial number. The trial version is fully functional but will "time-out" after 30 days.

b. If you decide to purchase InterScan, contact a Trend Micro sales representative at the following email address:

`sales@trendmicro.com`

for a serial number. The time-limit will be removed when you register InterScan with Trend Micro. There is no need to reinstall or reconfigure the program.

Installing Email VirusWall...

InterScan Email VirusWall typically uses port 25. If you are installing InterScan on the same machine as the SMTP server, change the SMTP port to one other than 25, for example 6000. If your SMTP server does not support other configurations, install Email VirusWall onto a different machine.

Installing onto a Microsoft Exchange Server

1. If InterScan detects that you are installing onto a Microsoft Exchange server and its IMC (Internet mail connector) is using port 25, you are prompted to change the IMC port.

   See Appendix A in the Administrator's Guide for instructions on reconfiguring Microsoft Exchange's IMC port, or see Microsoft's native documentation.
2. Choose **Change SMTP port** and click **Next** when the Exchange window appears.
3. Specify a port such as 6000 (or higher) in the **SMTP Port** field. If the port you selected is already in use, you'll be prompted to select another.

Installing Web VirusWall...

Web VirusWall requires that a HTTP proxy server be installed on the network. You can configure InterScan to run with an existing HTTP proxy server.

Note: Web VirusWall cannot start if another HTTP service is already running on the same port. Stop the conflicting service (**Control Panel | Services**) before starting Web VirusWall.

Installing FTP VirusWall...

FTP VirusWall is typically installed onto a different machine than the FTP proxy server. No preliminary configuration screens appear. If you install FTP VirusWall, however, you will be prompted to "quick configure" it, i.e., set up the VirusWall before starting the service.

Continuing with Quick Configure

After the InterScan program files have been installed, we recommend that you proceed with a "quick configure" of the new service(s) to set up InterScan to run with your existing SMTP, HTTP, and/or FTP server. Depending on your setup topology, you may also need to make configuration changes to those existing services.

If you are installing only one VirusWall, jump to the appropriate section below,

- Configuring a notification server
- Configuring Email VirusWall
- Configuring Web VirusWall
- Configuring FTP VirusWall

Quick Configuring a Notification Server

InterScan can automatically send customized alert messages to the person or persons specified in the VirusWall configuration pages. To do so, you need to identify which SMTP server it should use.

1. Enter the IP address (or host name) of the SMTP server that you will have deliver InterScan's various virus notifications.
2. Click **Next** to continue.

Quick Configuring Email VirusWall

Email VirusWall can work in conjunction with an existing SMTP server or use your DNS to handle the delivery of scanned messages.

1. Enter the IP address (name or number) of the original SMTP server in the **IP Address** field. This field should not be left blank.
2. Enter the port number for the original SMTP server in the **Port** field. The default SMTP port is 25.

Quick Configuring Web VirusWall

1. In the **Proxy Address** field, enter the IP address (name or number) of the HTTP proxy.

2. In the **Proxy Port** field, enter the *new* port number of the HTTP proxy server. The default is 5000.
3. In the **Iscan Port** field, enter the port where Web VirusWall will listen for incoming HTTP connections. The default is 8080. Another typical entry is port 80.

Quick Configuring FTP VirusWall

You can run FTP VirusWall in by itself, in **Stand-alone mode**, or in conjunction with an existing FTP proxy server.

Choose Stand-alone Mode

Choose **Stand-alone mode** if there is no existing FTP proxy server, i.e., FTP VirusWall will operate independently.

You will need to instruct your FTP clients to now use InterScan FTP VirusWall as the new FTP proxy server.

Choose Use FTP

Choose **Use FTP proxy** if an FTP proxy server that you want InterScan to work with already exists on the network. FTP VirusWall can operate transparently with your existing proxy.

Note: If you choose **Use FTP proxy**, you will need to instruct your FTP clients to change their FTP proxy IP address and port.

---

1. In the **Use FTP proxy** field, enter the IP address (name or number) of the original FTP proxy server.
2. In the **Port** field, enter the port number of the orginal FTP proxy server. The default is 21.

B: Installing The *CVP Edition* Of InterScan VirusWall

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

It can be installed on the same machine as FireWall-1 or on another machine. This machine might be a dedicated to InterScan for use by all three VirusWalls, it may be several existing machines that are already running other programs, or it may be several machines, each dedicated to a particular VirusWall.

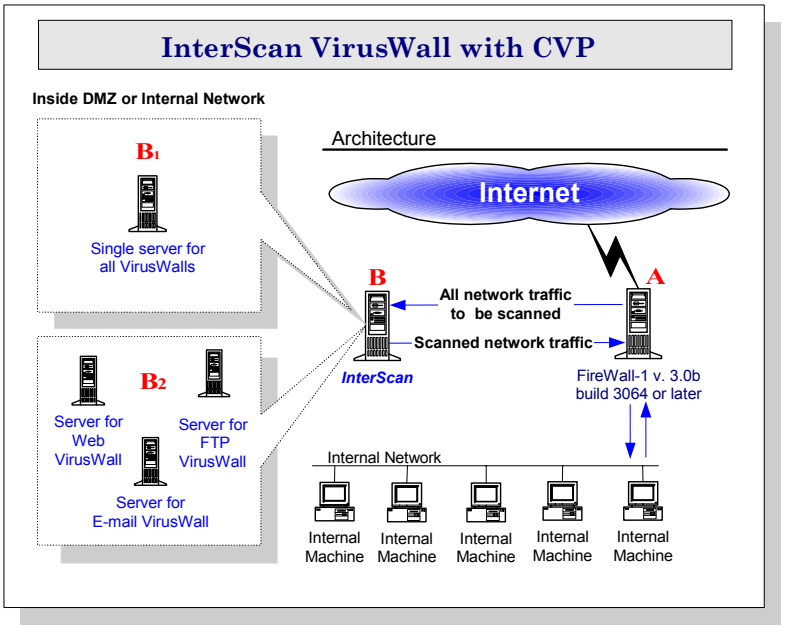


FIGURE 3-1. Possible installation points for InterScan VirusWall are indicated by the letters A and B. InterScan must receive network traffic from FireWall-1. Scanned traffic is returned to the FireWall-1 machine. All VirusWalls can be installed on the same server (B1) or each onto a different server (B2). Installing InterScan onto the FireWall-1 machine (A) can be faster but, is more resource intensive.

Deciding Where To Install

InterScan acts as a plug-in to FireWall-1; it receives all traffic from this machine, not directly from clients or the Internet.

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

- **Point A**. Installing InterScan onto the same server as FireWall-1. This setup is preferable for light network loads. Although it can be faster than transferring all traffic back and forth to the FireWall-1 machine, expect that running InterScan in addition to FireWall-1 will place a high demand on resources.
- **Point B1**. Install all three InterScan VirusWalls onto a single, dedicated NT server (located in the DMZ or internal network). Due to the potential for high resource demand, this configuration is **recommended** only for networks having moderate to light traffic loads.
- **Point B2**. Install each VirusWall onto an existing server that is already running other programs. Of course, a lot will depend on how resource intensive the other programs are. Installing InterScan Email VirusWall on to the SMTP server, for example, may overburden the server is traffic is heavy.
- **Point B2-2**. Install each VirusWall on to a dedicated server. Suggested for heavy network traffic loads. This configuration can be the most efficient for networks with heavy network loads. **Note:** Use Trend Micro's *Virus Control Center* to consolidate InterScan configuration tasks among the three machines.

Step-by-Step Instructions: Installing The CVP Edition of Trend Micro InterScan VirusWall

FireWall-1 operates at the packet level, distributing the individual packets it receives on the basis of protocol type and the policies that are defined in the FireWall-1 rule base. In order for InterScan to receive these packets from FireWall-1, **Network**, **Server**, **Service**, and **Resource** objects representing the InterScan machine and VirusWall services must be defined and added to the rule base.

While running InterScan's Setup program, you will be prompted to specify which service port you will use for each of the VirusWalls to communicate with these objects. The defaults are, 18181 for the Email VirusWall, 19001 for the FTP VirusWall, and 19000 for the Web VirusWall.

Run Setup from the server where the program(s) will be installed. For example, after installing Email VirusWall on an SMTP server, move to the HTTP proxy server that will host Web VirusWall and run Setup again.

1. Insert the **Trend Micro Enterprise Solution** CD into the appropriate drive.
   - If you have AutoPlay enabled, the disk will start automatically. Choose **InterScan VirusWall for NT** from the list of programs that appears, choose a language and click **Install**
   - If AutoPlay is not enable, click the NT **Start** button, then **Run** and enter `[path]\go.exe` in the **Open** field
   - If you are installing from a downloaded copy of the program, locate the directory containing the Setup files and double-click `setup.exe`
2. After accepting the License Agreement (required to proceed) and specifying where to install InterScan, you are prompted to select the VirusWall(s) you want to install.

3. When prompted at the Select InterScan NT Edition screen, **Choose Check Point Software's FireWall-1 edition**, and click **Next**.

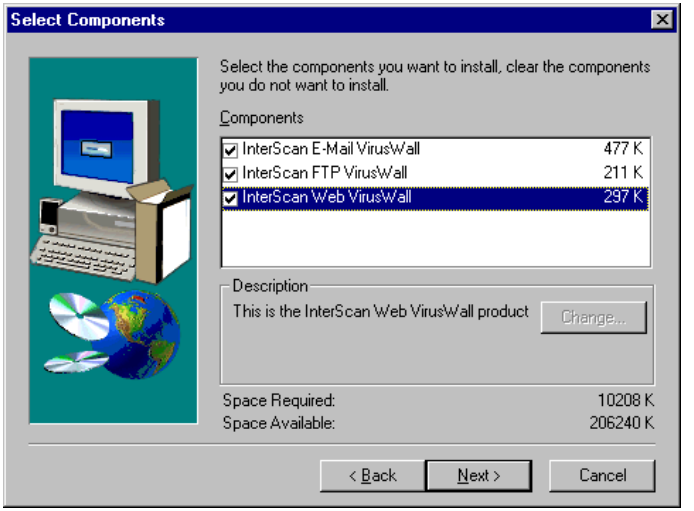


FIGURE 3-2. Select the VirusWalls you want to install.

4. Enter the product serial number (serial numbers can be found on the front cover of this Administrator's Guide and on the product registration card).
5. Next, you are prompted to enter the IP address of the machine you are installing on. Enter the actual IP address rather than localhost or 127.0.0.1.
6. Finally, click **OK** to the notification that each service has been installed.

Quick-Configuring the Email VirusWall

If you have installed the Email VirusWall, enter the **CVP Service Port** number that you want InterScan to use for communication with the FireWall-1 machine. The default is 18181.

Quick Configuring Web VirusWall

If you have installed the Web VirusWall, you are prompted to enter the **CVP Service Port** number that you want InterScan to use for communication with the FireWall-1 machine. The default is 19000.

You are also prompted to enter the IP address of the SMTP server that you want to use for sending notification messages. InterScan will use this SMTP server to route its automatic email notifications to the administrator, or others, whenever a virus is detected.

Quick Configuring FTP VirusWall

If you have installed the FTP VirusWall, you are prompted to specify the **CVP Service Port** that the FTP server will use to communicate with the FireWall-1 machine. The default is 19001.

Starting the InterScan Configuration Utility

The InterScan configuration utility can be accessed locally using the Windows-based interface or remotely, using a web browser.

- From the server where Trend Micro VirusWall is installed, access either interface by clicking the Windows NT **Start** button, then the **InterScan** folder.
- From a remote location, access the browser-based interface by opening a web browser and entering the URL of the machine where Trend Micro VirusWall is installed, for example:

  `http://123.12.12.123/InterScan/cgi-bin/interscan.dll?`

Setting up InterScan for a CVP Environment

The following is a summary of the tasks required to set up both InterScan and the FireWall-1 machine:

On the InterScan side...

1. Inbound virus scanning is enabled by default upon installation. If you want to scan outbound SMTP traffic,
   a. **Enable outbound mail processing** must be checked,
   b. the IP address of any SMTP servers sending outbound email to InterScan for scanning must be identified

c. **Enable Virus Scanning** must be checked in the Outbound SMTP Mail Processing configuration page.

2. InterScan's FireWall-1 CVP configuration **Service Ports** are usually set during installation and do not need require modification.

On the FireWall-1 side...

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

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

InterScan: Enable Virus Scanning

Upon installation, SMTP, HTTP, and FTP virus scanning are enabled and do not require subsequent configuration. Outbound scanning, set in the Email VirusWall configuration page, is *not* enabled and must be set for outbound scanning to occur.

Check your inbound settings as follows:

1. Start the InterScan VirusWall configuration, then make the **SMTP Scan Configuration** page active.
2. For **Inbound Mail**, put a check in the **Enable Virus Scanning Services** check box.
3. If necessary, repeat steps one and two for both the **HTTP Configuration** and **FTP Configuration** pages.

Outbound Mail Scanning

To enable outbound scanning,

1. Start the InterScan VirusWall configuration, then make active the **SMTP Scan Configuration** page. Put a check in the **Enable outbound mail processing** check box.
2. Next, click the **Option** button and, in the **Specify the IP address...** field, enter the IP address of any SMTP servers that will be sending InterScan outbound mail for scanning.

   Be sure to enter 127.0.0.1 *and* the literal IP address of the InterScan machine if both it and the SMTP server are running on the same machine.

InterScan: Set the InterScan Service Port

The **CVP Service Port** used by InterScan is typically set during installation. The defaults are *18181* for SMTP traffic, *19001* for FTP traffic, and *19000* for HTTP traffic. However, any free port can be used.

To change the **CVP Service Port** used by InterScan,

1. Open the InterScan configuration in a web browser and click **SMTP Configuration** in the left window frame.

2. In the **Service Port** field, enter the port number that you will later use when creating the Email VirusWall **Service Object** in FireWall-1, or accept the default.

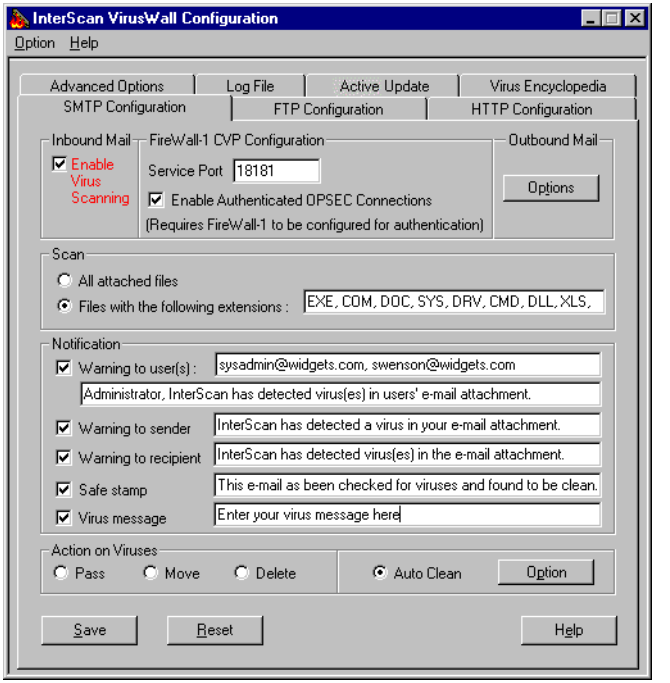


Figure 3-3. The SMTP Configuration page, where you can set the Service Port used by InterScan and FireWall-1.

3. Repeat these steps for both the **HTTP Configuration** and **FTP Configuration** pages.

After installing InterScan onto the machine(s) where it will reside, re-locate to the FireWall-1 machine and start the configuration interface. Each of the five FireWall-1 tasks is described below.

A.) Create a Network Object

1. In the FireWall-1 configuration page, click **Manage | Network Objects...**
2. Click **New**, then choose **Workstation** (or choose an existing Network object representing the InterScan machine).

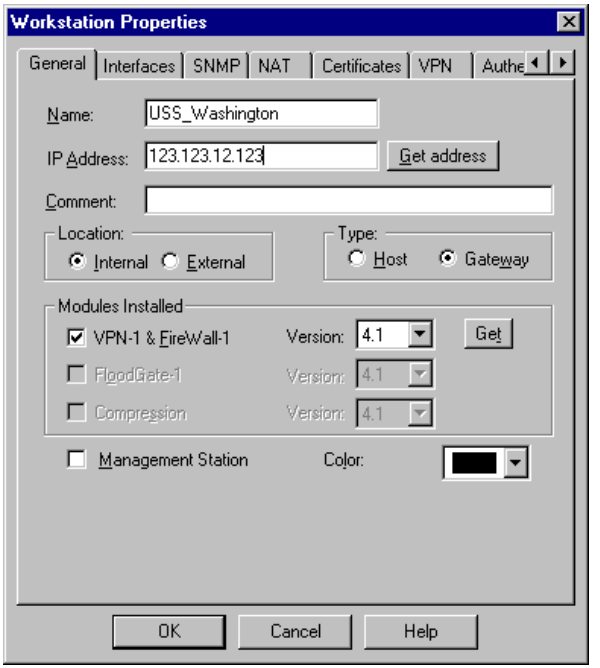


FIGURE 3-4. Create a Network Object for each of the VirusWalls.

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

   `USS_Washington`

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, **Type** (must be Gateway) and **Location** (Internal, External) as appropriate for your circumstances.

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

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

Note: If you have all three InterScan services (SMTP, FTP, and HTTP) installed on the same machine, only one Network object is required. If the scanning services are installed on separate machines, create a network object to represent each service.

B.) Create a Service Object

1. In the FireWall-1 configuration page, click **Manage | Services...**
2. Click **New**, then choose **TCP** from the drop-down menu that appears.

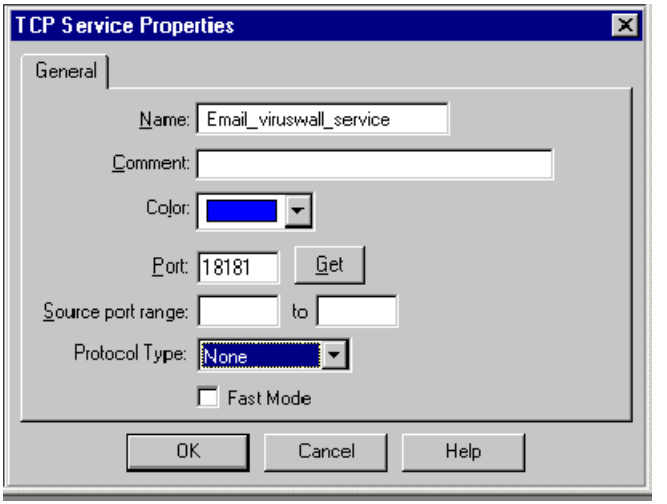


FIGURE 3-5. Define a Service Object for each of the VirusWalls.

3. In the **General** tab, enter a name for the service you are creating. For example,

   `Email_viruswall_service`

4. Specify the port used by the InterScan scanning service. The InterScan defaults are **18181** for the Email VirusWall, **19001** for the FTP VirusWall, and **19000** for the Web (HTTP) VirusWall.

5. Click **OK**, then **Close**. Repeat these steps for each InterScan scanning service you will add (once for the SMTP, HTTP, and FTP services).

C.) 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_VirusWall_Server.**

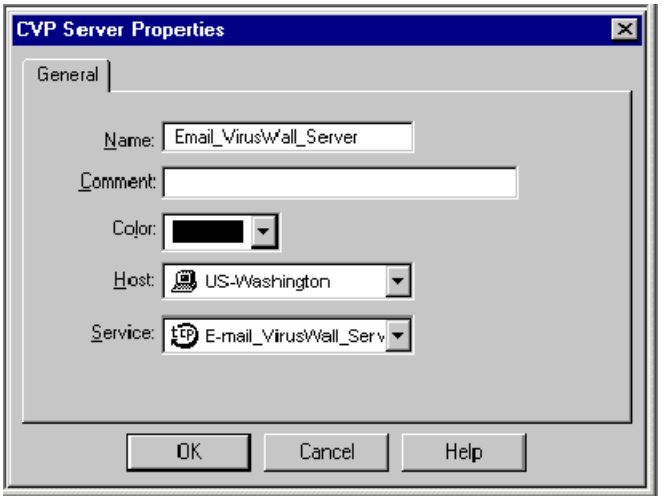


FIGURE 3-6. Define a Server Object for each of the VirusWalls.

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

D.) FireWall-1: Create a Resource Object

1. In the FireWall-1 configuration page, click **Manage | Resources...**

2. Click **New...**, then choose the appropriate protocol from the drop down menu that appears.
   - Choose **SMTP** for the Email VirusWall
   - Choose **URI** for the Web VirusWall
   - Choose **FTP** for the FTP VirusWall

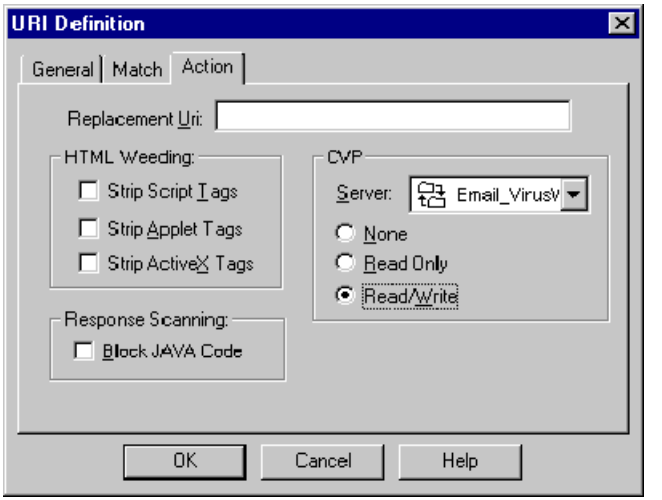


FIGURE 3-7. Define a Resource Object for each VirusWall.

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 C, **`Email_VirusWall_Server`** in our example.

b. Click **Read/Write**, the only valid option with InterScan, to enable virus scanning and cleaning. (The **None** option is not supported by InterScan—instead, disable virus scanning via InterScan side. InterScan does not support the **Check** option.)

SMTP scanning

a. For the Email VirusWall, make the **Action2** tab active and, from the **Server:** drop-down box, select the *Server* you created in task C.

b. Click **Read/Write** to enable virus scanning and cleaning (see **b.** above).

4. Click **OK**, then **Close**.

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

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

No.	Source	Destination	Service	Action	Track
1	LocalNet	Any	http->http_viruswall_resource ftp->ftp_viruswall_resource	accept	Long
2	MailServer	Any	smtp->smtp_viruswall_resource	accept	Long
3	Any	MailServer	smtp->smtp_viruswall_resource	accept	Long
4	Any	Any	Any	reject	Long

FIGURE 3-8. 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 appears to enable logging.

Installing the Rule

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

Rule Base Order

FireWall-1 examines the rule base sequentially, from top to bottom, until a rule successfully matches the type of traffic being examined. We recommend that you place the InterScan CVP rules accepting HTTP, SMTP, and FTP connections *before* any other rules which accept these services to prevent unwanted traffic from entering the network.

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

Setting up Check Point's Authentication for InterScan

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

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

On the FireWall-1 side

1. Go to the FireWall-1 "bin" directory to run "`fw putkey -opsec` [IP address of InterScan]"

You are prompted to enter a secret key. Type a sequence of at least 4 characters.

2. Edit the `$FWDIR/conf/fwopsec` file to show that the connection from InterScan is authenticated. for example,

```
server 127.0.0.1 18181
auth_opsec
```

3. should be changed to

```
server <IP_address/hostname of InterScan> 18181
auth_opsec
```

On the InterScan side:

1. The opsec_putkey.exe program needs to be run with the following command line options:

```
opsec_putkey [IP address of FireWall-1]
```

2. You will be prompted to enter the secret key which was configured on the FireWall-1 side.
3. Once `opsec_putkey` is successful, one or more *.c files will be created (i.e., authkeys.C and rand.C). These files must be copied into the same directory as the InterScan program files: `\InterScan\ISSMTPD` for Email VirusWall, `\InterScan\ISHTTPD` for Web VirusWall and `InterScan\ISFTPD` for FTP VirusWall.

Enable Authenticated OPSEC connections in the InterScan configuration program and restart.

Starting the Configuration Utility

The configuration options discussed in the following chapters can be accessed locally using the Windows-based interface or remotely, using a web browser.

- From the server where Trend Micro VirusWall is installed, access either interface by clicking the Windows NT **Start** button, then the **InterScan** folder.
- From a remote location, access the browser-based interface by opening a web browser and entering the URL of the machine where Trend Micro VirusWall is installed, for example:

  `http://100.10.209.55/InterScan/cgi-bin/interscan.dll?`

Note: To configure the InterScan VirusWalls using a web browser, Microsoft's Internet Information Service (IIS) must be installed and the WWW service must be running.

Password Security

If password security has been set up for web browsers, a User Name and Password Required window will appear. Enter Administrator-level credentials to log on.

InterScan VirusWall employs the NT Server's native password and file system protection for security. For browser access, InterScan automatically sets the Microsoft Internet Information Server virtual directory. No new password restrictions are established.

See Appendix A of this Administrator's Guide for instructions on setting up password and file security.

Starting Trend Micro VirusWalls Manually

Depending on the installation options you choose, up to three services are added to the NT server: **InterScan Email VirusWall**, **InterScan Web VirusWall**, and **InterScan FTP VirusWall**.

All are automatically started following installation. If a conflicting service was detected, however, or one or more of the services were otherwise unable to start, you may need to start the services manually.

From the NT Control Panel, click the **Services** icon, to open the Services window. Locate the service you want to start and click **Start**. All services are typically set to **Automatic Startup**.

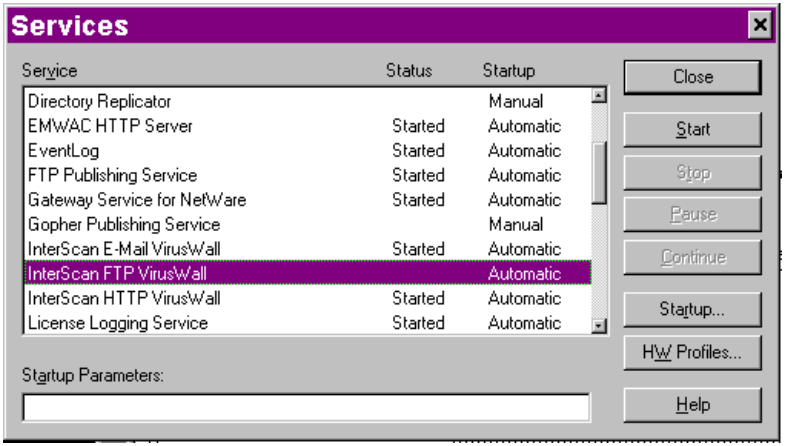


FIGURE 3-9. The Trend Micro VirusWalls can be started in the Services window.

Conflicting Services

If a conflicting service exists, for example an existing FTP server is using port 21, stop that service before starting the Trend Micro VirusWall. You will likely need to configure both that service and the VirusWall so that the VirusWall uses the default port and then passes scanned traffic to the complementary service on a different port or at a different IP address.

Testing the VirusWalls

Once Trend Micro VirusWall has been installed, you may want to test it to check the configuration and see how it works.

The European Institute of Computer Anti-virus Research, along with anti-virus vendors, has developed a test file that can be used in 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 and as such, can be detected by the virus engine.

You can download this file from Trend Micro at:

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

Note: You may need to disable HTTP scanning before downloading the file.

Once on your machine, you can include the test virus as an email attachment to test SMTP scanning, and to check FTP and HTTP file transfers.

Uninstalling Trend Micro InterScan VirusWall

The Trend Micro VirusWalls cannot be individually removed. If you have all three installed on the same server, but only want to remove one or two, consider turning off scanning for those protocols or stopping the service in NT's Services (**Control Panel | Services | InterScan**).

Otherwise, back up your `iscan.ini` file and remove all Trend Micro VirusWalls, then reinstall only those you want on the system. You may copy applicable settings from the backed up configuration to the new, or just reconfigure the VirusWall.

To remove all installed VirusWalls,

1. Click the Windows NT **Start** button, then the **InterScan VirusWall | Uninstall**.
2. InterScan will stop the following services before uninstalling:

```
InterScan Email VirusWall
InterScan FTP VirusWall
InterScan Web VirusWall
```

3. Choose **Yes** at the prompt to run Uninstall.

4. If applicable, be sure to reconfigure your original servers to use the appropriate port. For example, if you installed Email VirusWall on the same server as Microsoft Exchange, change Exchange's IMC port back to 25 if necessary.

Note: Quarantined files, which contain "live" viruses, are not deleted in Uninstall. Be sure to delete these files manually from the `\interscan\dir\virus` directory.

Chapter 4

Configuring Email VirusWall

Setting up Real-time Email Scanning

Email VirusWall will work with a single SMTP server or can complement multiple servers. It has been tested with many different SMTP email programs for NT, including SendMail from MetaInfo, NTMail, Postal Union, and Microsoft Exchange.

If possible, give Email VirusWall port 25. If a particular SMTP server cannot be reconfigured to use a port other than 25, for example, some versions of Netscape Mail Server, consider installing Email VirusWall onto a dedicated server. See also Chapter 2 for alternative Setup topologies and Chapter 7 for details on defining the Email VirusWall **Service Port**.

Generally speaking, the objective for scanning inbound SMTP traffic is to configure the network so that Email VirusWall receives SMTP traffic first. As discussed in Chapter 2, if Email VirusWall and the SMTP server are on different machines, possible ways of doing so include altering the MX record of the DNS and swapping IP addresses between Email VirusWall and the SMTP server.

If InterScan and the SMTP server are on the same machine, the IP address will be unchanged. In this case, you need only designate a new port for the SMTP server to use for receiving SMTP traffic. Email VirusWall will take port 25 and pass scanned messages to the SMTP server using its newly designated port. Alternatively, InterScan can handle the delivery of both inbound and outbound mail using the a DNS server.

Setting up Inbound Scanning...

1. Put a check in the **Enable Virus Scanning** box (Figure 4-1).

   If **Enable Virus Scanning** is not checked, Email VirusWall will continue to process SMTP traffic, to support plug-in operations, for example, but the mail is not scanned.

2. Select a method of mail delivery. You can have Email VirusWall **Forward mail to SMTP server** or **Use DNS to deliver mail** to client mailboxes itself.

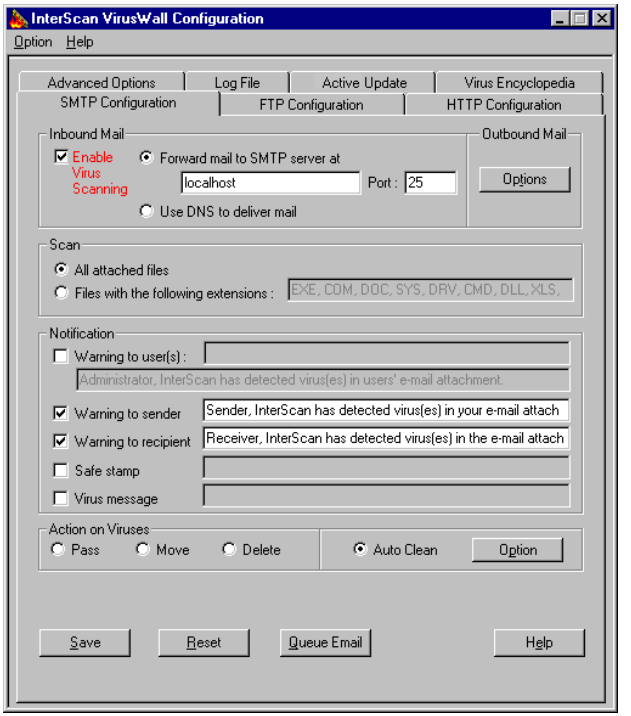


FIGURE 4-1. The Email Configuration page.

Forward mail to SMTP server at:

Use this configuration, for example, if a firewall on the network prevents Email VirusWall from delivering messages directly, if the SMTP server provides additional

functionality that you do not want to lose, or if there is only one SMTP server for the domain.

Note: The IP address and Port you specify here will depend on whether Email VirusWall is installed on the same machine as the SMTP server or a different one.

If Email VirusWall and the SMTP server are on the same machine...

Email VirusWall will receive inbound SMTP traffic on port 25, scan it for viruses, and then route it to the original SMTP server at a port other than 25, where it will be received and processed as usual.

1. Edit the original SMTP server's configuration so that it no longer receives SMTP traffic on port 25. Change it to a free port such as 6000 or above.
2. In the Email VirusWall configuration page, enter "localhost" in the **Forward mail to the SMTP server at**: field. You can also enter 127.0.0.1 or the server's actual IP address.
3. In the **Port** field, specify the original SMTP server's new port number (e.g., 6000).

If Email VirusWall and the SMTP server are on different machines...

In this case the IP address of the machine where Email VirusWall is installed must become the client's default SMTP server.

There are a number of possible ways to accomplish this, including changing the email clients to recognize Email VirusWall as the new SMTP server, editing the MX record so that Email VirusWall replaces the original SMTP server, swapping the two server's IP addresses, and swapping host names. Choose a method and take care of this before configuring Email VirusWall to pass scanned messages to the original SMTP server for delivery. Once done,

1. Enter the domain name or IP address of the original SMTP server in the **Forward mail to the SMTP server at:** field. If this IP address has changed, be sure to enter the new IP address.
2. Specify the **Port** the original SMTP server is using. Typically, this is port 25.

Use DNS to deliver mail...

Email VirusWall can deliver scanned mail itself, regardless of whether it is installed on the same machine as the original SMTP server or a different one. Choose **Use DNS to deliver mail**, for example, when there are multiple SMTP servers for the domain that you want Email VirusWall to forward inbound mail to after it has been scanned (only one IP address can be specified in the **Forward mail to SMTP server at:** field).

No IP address or port need be entered if you choose **Use DNS to deliver mail**.

Setting up Outbound Scanning...

Click the **Options** button under the Outbound Mail header to bring up the **Outbound SMTP Mail Processing** window.

1. Put a check in the **Enable outbound mail processing** box, as shown in Figure 4-2.

   If **Enable outbound mail processing** is not checked, Email VirusWall will continue to process outbound SMTP traffic, for example to support plug-in operations, but the mail will not be scanned.

   To scan outbound mail for viruses, both **Enable outbound mail processing** and **Enable outbound mail virus scanning** must be checked.

2. In the **Specify the IP address(es)**... field, enter the numerical IP address of each SMTP server that will send outbound email to InterScan for scanning.

   Delimit multiple IP addresses with a comma.

Note: If InterScan is installed on the same machine as the SMTP server sending outbound mail, enter both the actual IP address and 127.0.0.1.

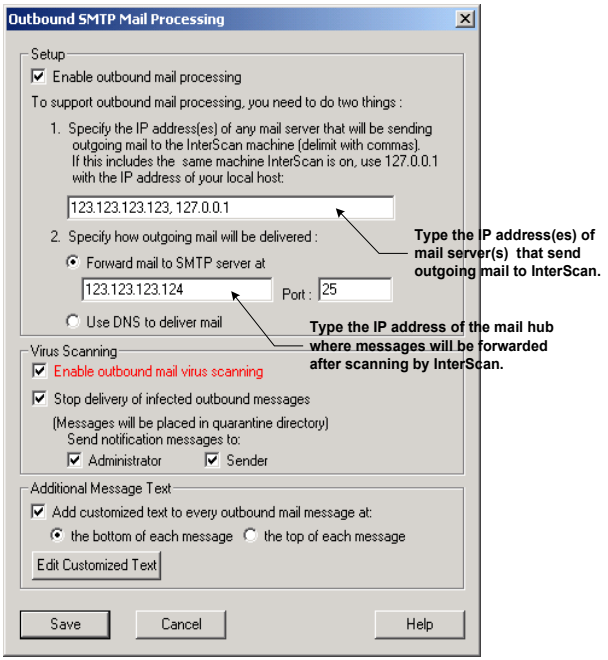


FIGURE 4-2. Email VirusWall also scans outbound mail.

Based on these IP addresses, InterScan differentiates between incoming messages, those that are to be scanned for viruses and passed to the inbound SMTP server, and outbound messages, those that are to be scanned and then routed on to the outbound SMTP server. Typically, the original SMTP server IP address is among those that are entered in this field.

3. In the **Forward mail to SMTP server at**: field, enter the IP address (name or number) of the machine that InterScan will pass scanned mail to for outbound delivery.

a. If InterScan will handle the delivery of scanned, outbound mail, choose **Use DNS to deliver mail**. No IP address(es) or port(s) need be specified in this case.

This is the typical method of handling outbound mail after scanning, regardless of whether Email VirusWall is installed on the same machine as the SMTP server or a different one.

b. If another mail gateway or mail hub will handle delivery of scanned messages on behalf of InterScan, type its IP address and port. In Figure 4-2, this mail server is represented by the IP address *123.123.123.124*.

Enabling Outbound Virus Scanning

To have Email VirusWall scan outbound mail for viruses,

1. Check **Enable outbound mail processing.**
2. Check **Enable outbound mail virus scanning**.

Stopping the Delivery of Infected Outbound Mail

InterScan can halt the delivery of outbound messages found to contain viruses. Both the message text and infected attachment(s) of "stopped" mail are moved to the quarantine directory.

If this option disabled, infected attachments are cleaned, deleted, or passed, according to the action specified on the main SMTP configuration page. A notification message (as specified under the **Notification** options on the main SMTP Configuration page) can be issued to the Sender, Administrator, or both.

For example,

Attention, Sender: InterScan detected a virus in the email attachment you sent.

Date: Thu, 10 July 2003 15:24:18 Pacific
Method: Mail
From: <bob_li@trendmicro.com>
To: <rich_romariz@generationXfiles.com>
File: Urgent.doc
Action: infected outbound message stopped in quarantine directory
Virus: Bandung.A

The subject of the notification message is "InterScan NT Alert." It will be addressed to "Mail_User@internet.com" with the return address being the one specified in the Advance Options configuration page.

Specifying Which Files to Scan

1. To scan all file types, click the **All attached files** radio button. This is the most secure configuration. All file types that are capable of carrying viruses will be scanned.
2. To scan only selected file types, click **Files with the following extensions:**.

   Only those file types that are explicitly specified here are scanned. Use this option, for example, to decrease the aggregate number of files scanned by the VirusWall, thus decreasing email scan times.

Note: Zip and other compressed file types are only scanned if specified. Compressed files are opened and all files found within scanned. If the compressed file contains other compressed file, these too decompressed and scanned, down to a maximum of 20 layers of compression.

Setting Notification Options

You can have Email VirusWall automatically notify selected individuals whenever a virus is detected in their email. If the infected attachment cannot be cleaned, separate notifications can be specified from the Action on Viruses **Option** button.

1. To alert the System Administrator or other individuals whenever an infected file is detected, select the **Warning to User(s):** checkbox.

   Enter the person's Internet email address in the text field to the right and your message text (perhaps specific to the **Action on Virus**) in the associated text field. For example,

   Note: Email VirusWall detected and cleaned a virus found in this email.

   Delimit multiple email addresses with a comma.

2. To warn the **Sender**, the **Recipient,** or both when a virus is found, put a check in the appropriate box. Enter the message you want that person to receive in the associated text field; this message is sent as a separate email.

Safe Stamp

Check **Safe Stamp** to have InterScan inform your email users that their email was scanned and was found to be virus-free. Enter a message in the associated text box. This message will be sent as an attachment to the original email when no viruses have been found. The name of the file is InterScan_disclaimer.txt.

Virus Message

Check **Virus Message** to have InterScan append a notification message to the body of the original email whenever a virus is found. Enter your message in the associated text field. For example,

For information on the virus found, visit

http://www.trendmicro.com/

Designating the Action on Infected Files

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 and the original message text, to the intended recipient *without cleaning*.
- Choose **Move** to move, *without cleaning*, the infected attachment to the `\InterScan\issmtpd\virus` directory. 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 Email VirusWall automatically clean and process infected files. The recipient will receive both the original message text and the attachment.

Setting the Auto-clean Options

Click **Option** to display the available auto-clean choices:

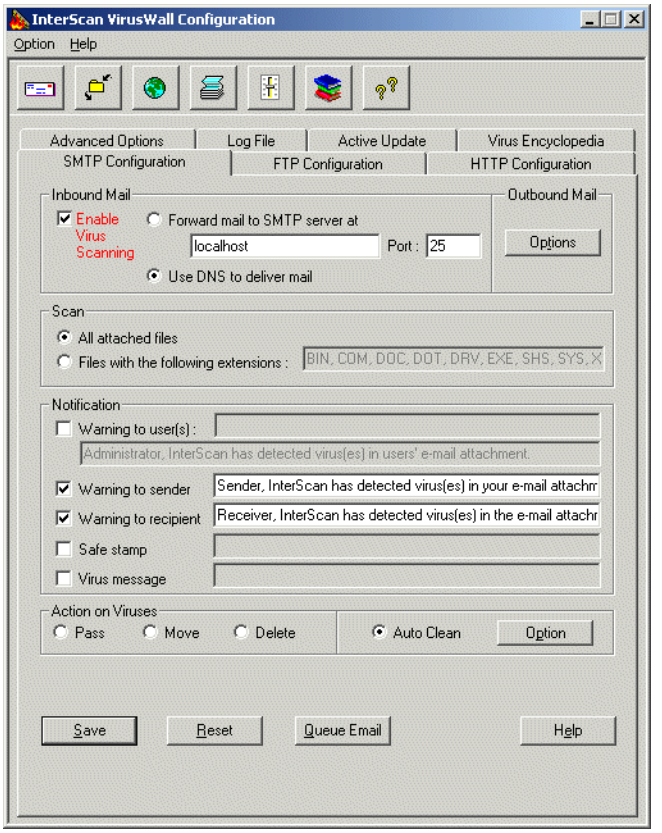


FIGURE 4-3. Infected attachments can be automatically cleaned and delivered to the intended recipient.

Specify the Destination of Cleanable Files

Put a check in the **Sender** box to have a copy of the cleaned file returned to the sender. The intended recipient always receives a copy of cleaned files.

The attachment is cleaned and UUencoded into a separate message before being delivered.

Specify the Destination of Uncleanable Files

Put a check in the **Notify Sender** box to have the Sender notified that an uncleanable file was detected in the email he or she sent.

The intended recipient is always notified; designate the action Email VirusWall should take on infected files:

- Choose **Pass** to deliver both the message text and infected file to the recipient. A separate warning message is also sent.
- Choose **Move** to deliver the message text to the intended recipient, but move the infected file to the `\interscan\issmtpd\virus` directory.
- Choose **Delete** to send the message text on to the intended recipient and delete the infected file.

Thread Pool

The thread pool limits the total number of concurrent requests per processor that InterScan will accept. Limiting the number of treads will prevent your system from being overloaded. To configure this option, add the following parameter in the "[Email-Scan]" section of the intscan.ini file:

```
[Email-Scan]

MaxScanningThreadsProc=10
```

This will limit the number of messages being scanned by InterScan at the same time to ten per processor. Additional SMTP requests will be sent a "452 Server too busy" response until the number of messages being scanned drops below the maximum.

Queue Mail

This option allows Email VirusWall to accept mail and hold it in a queue for later scanning. This feature is primarily to be used for emergency situations. If a virus outbreak has occurred, the mail can be queued (messages can continue to be transparently accepted), while a solution to the virus outbreak is put in place. Once the solution is implemented, the mail in the queue is scanned and forwarded.

To access the Queue Mail configuration menu, go to **SMTP Configuration** tab and click **Queue Mail**.

The Queue Mail menu has three options:

- Enable mail queueing
- for Inbound mails
- for Outbound mails

To activate the Queue Mail feature, check **Enable mail queueing**. Then, depending on your needs, choose inbound, outbound, or both.

Note: You must disable mail blocking in order to scan and forward mail. While mail blocking is enabled, the following pop-up warning will appear when you try to access the SMTP Configuration menu:

```
Important: Mail is currently being held in the MQUEUE directory. It
has not been sent to recipient. Disable settings in Queue Mail at
the bottom of the page to scan and send mail.
```

Saving the Configuration

- To save the new configuration, click the **Save** button.
- To revert to the previous configuration settings, click **Reset**.

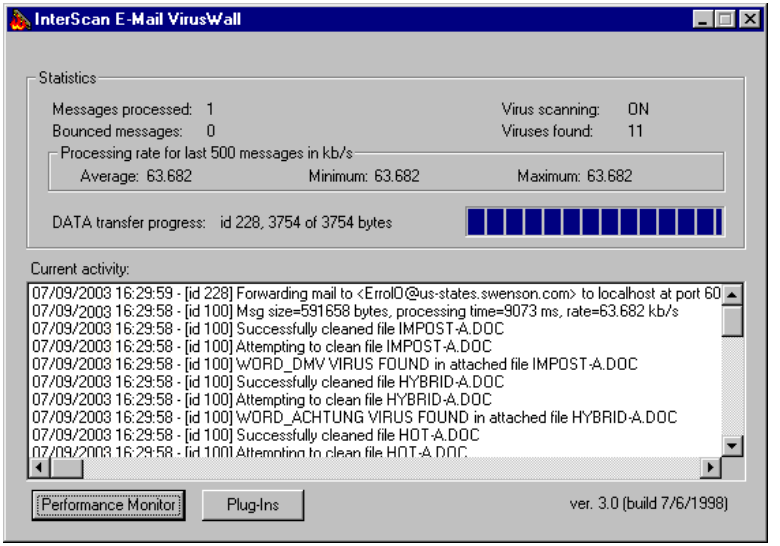
Real-time Activity Monitor

The real-time Activity Monitor appears as a minimized icon on the Windows taskbar whenever the Email VirusWall service is running. It cannot be closed, except by stopping the Email VirusWall service.

Use the Activity Monitor to check the real-time progress of message scanning (or to check your InterScan configuration). In addition, find out:

- Total number of messages processed
- Total number of messages bounced (delivery failure)
- Current scanning status(ON/OFF)
- Total number of viruses detected
- The VirusWall message processing rate
- Current VirusWall and SMTP activity

The data is also written to a log file in the InterScan root directory.



-

Chapter 5

Configuring Web VirusWall

Setting up Real-time Scanning & Security

Web VirusWall scans HTTP and browser-based FTP file transfers for viruses. In addition, Web VirusWall provides the means for applying a single standard to all network users to block potentially harmful Java applets from being downloaded.

Setup

Web VirusWall must be used with a HTTP proxy server. When setting up Web VirusWall to work in a chain of multiple proxy servers, Web VirusWall must be the one (logically) closest to the client browsers or TeleWindow will not be available.

Setting up HTTP Scanning...

1. Put a check in the **Enable Virus Scanning** box, as shown in Figure 5-1. If **Enable Virus Scanning** is not checked, Web VirusWall will continue to process HTTP traffic but it will not be scanned.

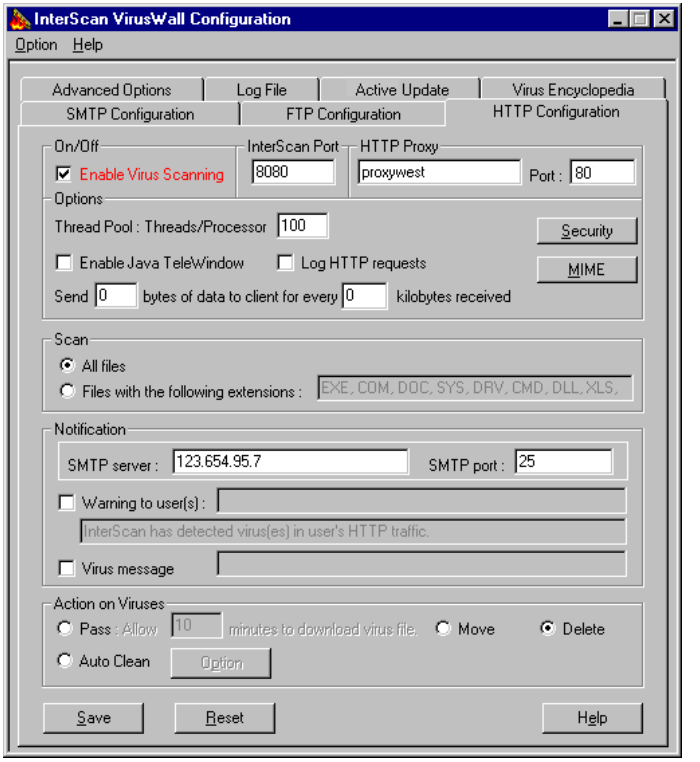


FIGURE 5-1. The Web VirusWall configuration page.

Web VirusWall and HTTP Proxy: Same Machine

If the HTTP proxy you are using is installed on the same machine as Web VirusWall,

1. In the **InterScan Port** field, enter the port where Web VirusWall will listen for incoming HTTP requests from the client browsers, for example 8080.

The Proxy field in your client browser should be configured to match the port entered here.

2. Enter "localhost" in the **HTTP proxy field.** If you are using Microsoft Proxy server, enter the actual IP address rather than "localhost".

Note: Do not use 127.0.0.1 to identify a proxy server that is on the same machine as Web VirusWall.

---

3. If you are using Microsoft Proxy server version 1.0 or later, this port is typically 80.

Note: To prevent clients from by-passing Web VirusWall, it is often advisable to reset the original proxy port to, say, 11813, or an equally improbable port.

Web VirusWall and HTTP proxy: Different Machines

If your original HTTP proxy server and Web VirusWall are installed on different machines,

1. In the **InterScan Port** field, enter the port where Web VirusWall will listen for incoming HTTP request from the client browsers, for example 8080.

   The Proxy field in your client browser should be configured to match the IP address (or hostname) and port entered here.

2. In the **HTTP proxy** field, enter the proxy IP address.
3. In the **Port** field, enter the original proxy server port. If you are using Microsoft Proxy server version 1.0 or later, for example, this port is typically 80.

Defining the Thread Pool

4. In the **Thread Pool** field, enter the number of HTTP threads you want to Web VirusWall to create upon start up.

   The thread pool is static and services all HTTP client requests. The number entered in this field will limit the total number of concurrent requests that Web VirusWall will accept; requests in excess of this number are queued. The larger the number entered here, the more memory devoted to the threads.

Each element (i.e., each .gif, Java applet, etc.) of a Web page will use its own thread. Therefore, in defining Web VirusWall's thread pool, choose a number that represents an equitable balance between available system resources and performance, i.e., one that can reduce the need for queuing.

Web VirusWall's thread pool is separate and distinct from any created by Proxy Builder.

Configuring the "Trickle" Function

InterScan VirusWall features a "trickle" function which solves a proxy or client browser "time-out" issue that can occur while scanning downloaded files.

How Does "Trickle" Work?

If the connection between InterScan VirusWall and the Internet is slow, clients may encounter "time-out" issues generated by the HTTP proxy server or their web browsers when downloading large files. To solve the problem, InterScan VirusWall provides the option to "trickle" small amounts of data to the requesting client in advance of transferring the entire scanned file.

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

Important Notes

- Because "trickle" works by advancing a small portion of data to the clients without scanning, it is theoretically possible 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 InterScan 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 InterScan VirusWall-to-Internet connection.

Note: To ensure that all files are scanned, the "trickle" value must always be less than the received data.

- With "trickle" set, clients are not notified when a file is blocked.
- The predicted download time that clients receive when downloading a file will be vastly over estimated—the client browser calculates this time according to the "trickle" it is receiving; it bears no reflection on the speed at which InterScan VirusWall is receiving the file. In fact, once the file has been scanned, transfer to the client usually only takes a few seconds.

On the Virus Scan Configuration screen, 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, InterScan 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 InterScan VirusWall machine and scanned, it is rapidly transferred to the requesting browser.

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

Security: Configuring Java Preferences

Java Security

Web VirusWall supports the system-wide blocking of Java applets to prevent them from being downloaded onto the LAN.

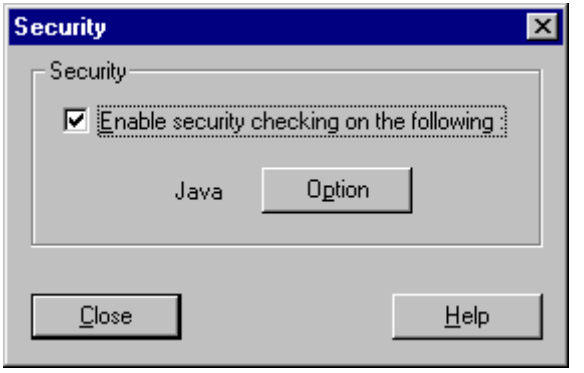


FIGURE 5-2. Enable system-wide Java security here.

How it works:

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

To Enable System-wide Java Blocking...

1. Click the **Security** button to bring up the options window (Figure 5-2), where you can enable Java applet blocking.

2. Select the checkbox labeled **Enable security checking on the following:** then click the **Java Option** button to bring up a window like the one shown in Figure 5-3.

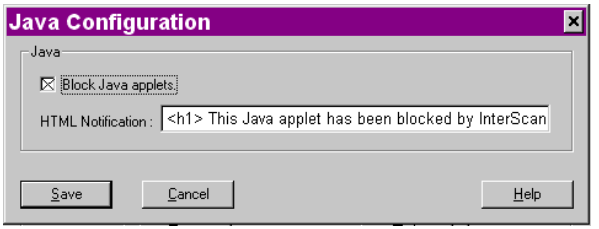


FIGURE 5-3. Use HTML formatting for the notification text.

3. Click the **Block Java applets** check box to activate Java Blocking, then enter the message text you want users to receive whenever a Java applet they try to download is blocked.

Note: Messages must be HTML formatted, for example: **<h1> your message text here </h1>**

---

4. Click **Save** to apply your configuration, or **Cancel** to lose the changes.

Setting MIME Options

Bypassing Specific MIME Content Types

The Web VirusWall administrator can configure Web VirusWall to selectively bypass certain MIME content.

This can be useful for streaming protocols such as RealAudio, for example, wherein the audio begins playing as soon as the beginning of the file arrives at the client computer. For Web VirusWall to check these files for viruses, however, the entire file must first be downloaded, a condition contrary to the methods of protocol streaming.

1. From the HTTP configuration page, click the **MIME** button to bring up the MIME configuration window (Figure 5-4).
2. Adding MIME types to this list means that these file types will not be scanned.

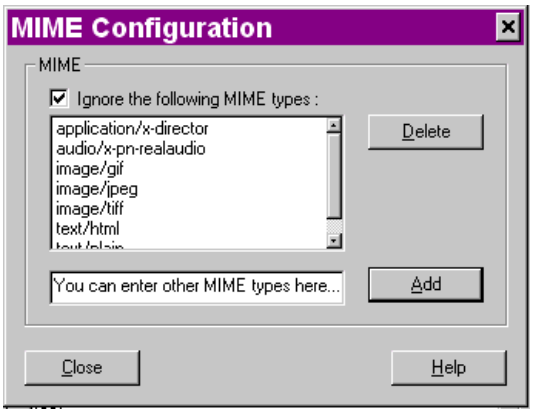


FIGURE 5-4. Add or delete scanned MIME types from this window.

3. Check the **Ignore the following MIME types** box to omit from scanning the file types that appear in the list below it.

Deleting an Existing Entry

Select the MIME file type or types that you want to remove from the list by clicking them, then click **Delete** and **OK** in the confirmation window that appears.

Since file types that do not appear on the list are scanned, removing file types from the list is equivalent to scanning those file types.

Adding a New MIME File Type

To add to the list of MIME file types not to be scanned, enter the new MIME type in the text field and click **Add**. Repeat the process for each MIME type you want to add.

Adding MIME types to this list means that these file types are not scanned for viruses and the streaming protocol is not interrupted.

Enabling the Java TeleWindow

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

So that users understand the purpose of this occasional delay, Web VirusWall provides an optional TeleWindow that automatically opens and closes with the web browser on all client machines.

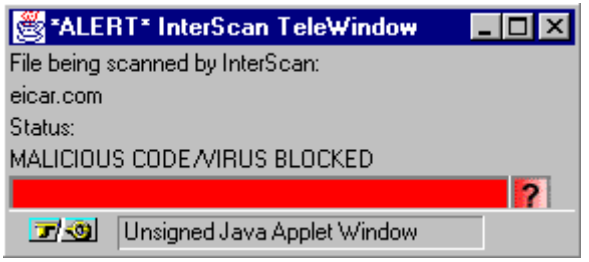


FIGURE 5-5. Web VirusWall provides a TeleWindow so end-users can stay informed about the progress of their HTTP requests.

Click **Enable Java TeleWindow** to active the TeleWindow for all users, or remove an existing check to remove the TeleWindow from all client machines.

Additional file transfer details are available by clicking the red question mark that appears in the TeleWindow to the right of the progress bar. This includes:

- The status of any current scanning operation
- The number of files scanned
- The number of viruses/malicious Java applets detected

Note: The TeleWindow is only available when Web VirusWall is the first proxy in a chain of linked proxy servers.

End users are not individually able to close their TeleWindow while a Web browser is open on their machine.

The TeleWindow will always remain open on the desktops of Internet Explorer 4.0 users (because the desktop acts as the browser).

Disabling the TeleWindow

Close the TeleWindow for all clients by removing the check from **Enable Java TeleWindow** on the HTTP Configuration page.

Logging HTTP Requests

Put a check in the **Log HTTP Requests** box to have Web VirusWall keep a running log of all URLs accessed by client browsers. Log data includes the requested URLs and the IP address of the requesting client.

HTTP Client Request Logs have the format "`iscan.log.<year>.<month>.<day>`"

For example,

iscan.log.1998.07.15

and are written to the `/InterScan` directory.

Entries are in ASCII format and can be imported to a database or spreadsheet file for analysis or archiving. You can also view the Client Request Logs using any text editor.

Specifying Which Files to Scan

1. To scan all file types, click the **All attached files** radio button. This is the most secure configuration. All file types that are capable of carrying viruses will be scanned.
2. To scan only selected file types, select **Files with the following extensions**.

   Only those file types that are explicitly specified here are scanned. Use this option, for example, to decrease the aggregate number of files scanned by Web VirusWall, thus decreasing email scan times.

Note: Zip and other compressed file types are only scanned if specified. Compressed files are opened and all files found within scanned. If the compressed file contains other compressed file, these too decompressed and scanned, down to a maximum of 20 layers of compression.

Setting Notification Options

You can have Web VirusWall automatically notify specified individuals whenever a virus is detected.

1. Identify the SMTP server that you will use for the delivery of notification messages. Enter the IP address and port. Typically, this is the same SMTP server as is specified in the SMTP Configuration page for Inbound Mail (not the Email VirusWall machine, since there is no reason to scan these messages for viruses).
2. To alert the System Administrator or other individuals whenever an infected file is detected, select the **Warning to User(s):** checkbox.

   Enter the person's Internet email address in the text field to the right and your message text (perhaps specific to the **Action on Virus**) in the associated text field. For example,

Note: Web VirusWall detected and cleaned a virus found in your HTTP file transfer.

Delimit multiple email addresses with a comma.

Virus Message

Check **Virus Message** to have Web VirusWall issue this additional notification whenever a virus is found. Enter your message in the associated text field. For example,

For information on the virus found, visit http://www.trendmicro.com/

Designating the Action on Infected Files

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

- Choose **Pass** to send the infected file to the intended recipient without cleaning. A warning message accompanies the infected file.
  In the **Time** field, enter the number of minutes that you will allow a user to download an infected file before the hyperlink to a copy of that file expires.

  *When **Pass** is selected, the **Time** field must contain a value.*
- Choose **Move** to move, *without cleaning*, the infected file to the `\InterScan\ishttpd\virus` directory. The recipient will not receive the file.
- Choose **Delete** to remove the infected attachment from the file and delete it from the server.
- Choose **Auto Clean** to have Web VirusWall automatically clean the infected file and deliver it as usual.
  The Action for files that cannot be cleaned is set by clicking the **Option** button and are the same as those listed above.

Saving the Configuration

- To save the new configuration, click the **Save** button.

- To revert to the previous configuration settings, click **Reset**.

Chapter 6

Configuring FTP VirusWall

FTP VirusWall is usually installed to so that it will scan FTP file transfers that are being downloaded to the local LAN (as opposed to scanning such transfers for remote users who are accessing a FTP site that you are hosting). Although both configurations are possible, it is the former that is discussed in this Administrator's guide.

FTP VirusWall can serve as the sole FTP proxy server on the network, or be installed to complement an existing one. It can be installed on the same machine as the existing FTP proxy or on a different one (the most typical configuration).

When installed to complement an existing FTP proxy server on a different machine, FTP VirusWall will be transparent to the end-user.

When installed on a machine other than the FTP proxy server, it is generally advisable to swap IP addresses between the FTP VirusWall machine and the original FTP proxy server (to keep the same relative IP address for your FTP clients).

See Chapter 2 for example setup topologies.

Setting up FTP Scanning...

1. Put a check in the **Enable Virus Scanning** box, as shown in Figure 6-1.

   If **Enable Virus Scanning** is not checked, FTP VirusWall will continue to process FTP traffic but it will not be scanned.

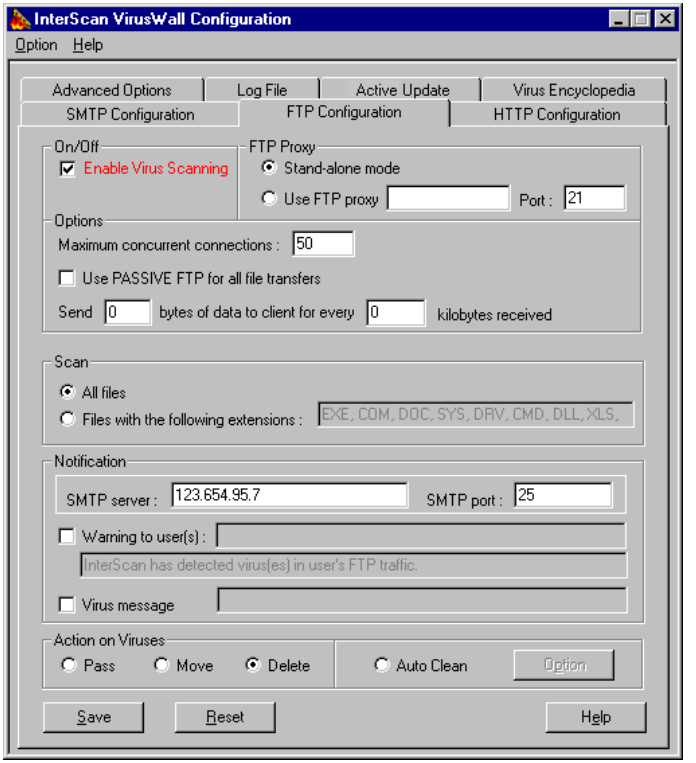


FIGURE 6-1. The FTP Configuration page.

2. Depending on how your system is set up, you need to choose either **Stand-alone Mode** or **Use FTP proxy.**

Stand Alone Mode

a. Choose **Stand-alone Mode** if there is no existing FTP proxy server on the network and you want FTP VirusWall to serve as the system's FTP proxy server.

When configured for **Stand-alone Mode**, clients always open a FTP session with FTP VirusWall (using its IP address). When prompted for a user name and password, clients will need to enter the expected user name, modified with the machine name.
For example, user John wants to FTP antivirus.com via FTP VirusWall. He opens an FTP session with the local FTP VirusWall. When prompted by InterScan, he enters the following:

```
username: john@antivirus.com

password: opensesame
```

Note: FTP VirusWall supports Proxy OPEN and User with no logon.

Use FTP Proxy

b. Choose **Use FTP proxy** if there is an existing FTP proxy server on the system that you want to continue to use. After installing FTP VirusWall, all subsequent FTP sessions will pass through it; this action will be invisible to the end user.

Enter the **IP address** (name or number) of this FTP proxy and the **Port**, usually 21.

3. Select **Use PASSIVE FTP for all file transfers** when there is a firewall on the network that does packet filtering and it is configured to deny connections bound from the Internet to the LAN (usually for ports above 1024).

In this case, **Use PASSIVE FTP for all file transfers** allows clients within the LAN to initiate Internet connections.

Maximum Concurrent Connections

4. In the **Maximum Concurrent Connections** field, enter the maximum number of simultaneous FTP connections that you want to allow InterScan to accept. Whenever this limit is reached (a very fluid condition), users trying to access the site are queued. This can improve throughput in certain circumstances, depending on the number of processors in the system.

   Choose a number that represents an equitable balance between the physical resources available on your system and the number (and frequency) of hits you anticipate.

Specifying Which Files to Scan

1. To scan all file types, click the **All attached files** radio button. This is the most secure configuration. All file types that are capable of carrying viruses will be scanned.
2. To scan only selected file types, select **Files with the following extensions**.

   Only those file types that are explicitly specified here are scanned. Use this option, for example, to decrease the aggregate number of files scanned by FTP VirusWall, thus decreasing email scan times.

Note: Zip and other compressed file types are only scanned if specified. Compressed files are opened and all files found within scanned. If the compressed file contains other compressed file, these too decompressed and scanned, down to a maximum of 20 layers of compression.

Setting Notification Options

You can have FTP VirusWall automatically notify specified individuals whenever a virus is detected.

1. Identify the SMTP server that you will use for the delivery of notification messages. Enter the IP address and port. Typically, this is the same SMTP server as is specified in the SMTP Configuration page for Inbound Mail (not the Email VirusWall machine, since there is no reason to scan these messages for viruses).

2. To alert the System Administrator or other individuals whenever an infected file is detected, select the **Warning to User(s):** check box.

   Enter the person's Internet email address in the text field to the right and your message text (perhaps specific to the **Action on Virus**) in the associated text field. For example,

   Note: FTP VirusWall detected and cleaned a virus found in your FTP file transfer.

   Delimit multiple email addresses with a comma.

Virus Message

Check **Virus Message** to have FTP VirusWall issue this additional notification whenever a virus is found. Enter your message in the associated text field. For example:

For information on the virus found, visit

http://www.trendmicro.com/vinfo/vinfo.htm

Designating the Action on Infected Files

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

- Choose **Pass** to send the infected file to the intended recipient *without cleaning*.
- Choose **Move** to move, *without cleaning*, the infected file to the `\InterScan\isftpd\virus` directory. The recipient will not receive the file.
- Choose **Delete** to remove the file from the server. The recipient will not receive the file.
- Choose **Auto Clean** to have FTP VirusWall automatically clean and process infected files.
  The Action for files that cannot be cleaned is set by clicking the **Option** button and are the same as those listed above.

Saving the Configuration

- To save the new configuration, click the **Save** button.
- To revert to the previous configuration settings, click **Reset**.

Chapter 7

Configuring Advanced Options

Advanced Options

The **Advanced Options** page contains parameters that extend the functionality of Interscan. From the Advanced Options page you can create notification addresses, open the Plug-In Manager, and extend Email VirusWall features. Many are new to InterScan version 3.x, such as the features listed below:

1. Maximum number of simultaneous SMTP client connections
2. Maximum inbound message size
3. Maximum outbound message size
4. Send InterScan notification/generated messages to
5. When DNS delivery is used, attempt to send message every X minutes
6. Disable insertion of InterScan's Received: header in processed messages
7. Treat MIME attachments whose name is greater than [X] characters as a virus
8. Quarantine Microsoft Office attachments containing macros
9. Accept inbound mail addressed only to the following domains (prevents relaying)

You will find an explanation of each in this chapter.

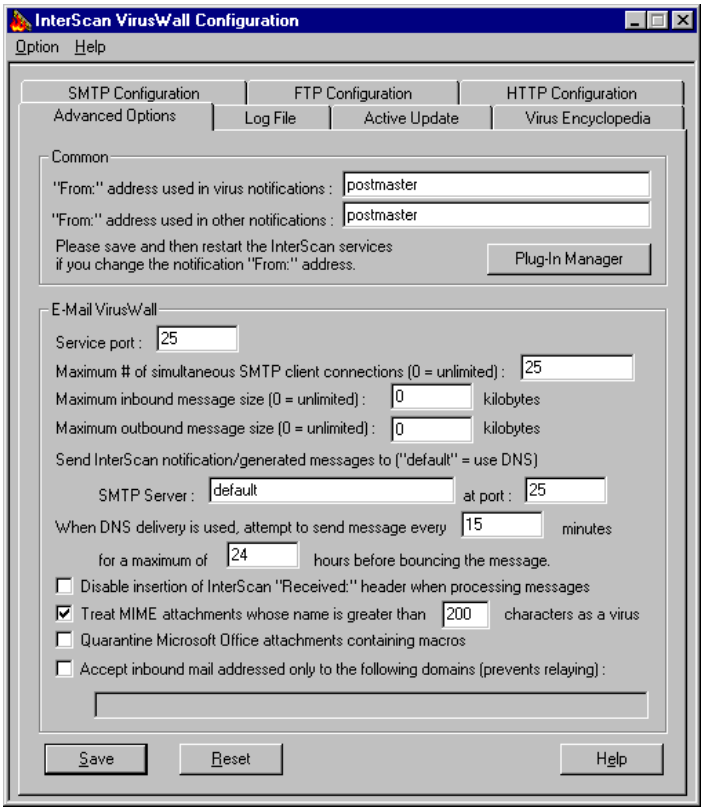


FIGURE 7-1. The Advanced Options configuration page.

Notification Messages From:

Quite often, different staff members will be responsible for network security and mail server administration. Therefore, InterScan provides two notification addresses: One for virus related events and another for non-virus related events.

From the **Advanced Options** configuration page, specify the email address that you want to appear in the **From** field of the notification message. Make sure you select the appropriate parties for both types of notification messages.

Typically this is the InterScan administrator's email address, or you may prefer to use something such as interscan@yourcompany.com

Restart Email VirusWall (**Control Panel | Services | InterScan Email VirusWall**) for the changes to take effect.

The following is a sample shown in the Message properties in Microsoft Outlook Express:

Received: from us-washington.us-states (localhost [127.0.0.1]) by us-washington.us-states with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.1960.3)id PJVA8RAF; Mon, 21 Jul 2003 11:49:35 -0700

Date: Mon, 21 Jul 2003 11:48:23 -0800
From: EmailVirusWall@yourcompany.com
To: Mail_User@internet.com
Subject: InterScan NT Alert

Sender, InterScan detected and cleaned a virus in the email you sent.

Date: Mon, 21 Jul 2003 11:48:23 -0800
Method:Mail
From: <DavidS@us-states.yourcompany.com>
To: <Iras@us-states.hiscompany.com>
File: 6-8WAZ_A.DOT
Action:cleaned Virus: WORD8_WAZZU.A

Email VirusWall

Service port

Enter the SMTP port number that Email VirusWall will use to receive messages to be processed. Typically, this port is 25.

Email VirusWall receives mail at this port, scans it for viruses, and then either **Forwards mail to the SMTP server**, or **Uses DNS to deliver mail**, as configured in the SMTP configuration page.

Maximum simultaneous SMTP client connections

You can have InterScan limit the total number of concurrent SMTP connections it will accept. The default value is 25. A zero (0) in this field means the number of connections will be unlimited.

If you are experiencing a degradation in performance, however, you may want to reduce the number of simultaneous SMTP client connections you will allow.

Maximum inbound and outbound message size

Email messages inbound or outbound from the Internet larger than the specified size, in kilobytes, will be rejected. This rejection occurs during the SMTP transaction between the remote SMTP server and InterScan. The remote SMTP server generates the non-delivery report.

Send InterScan notification/generated messages to...

Specify the SMTP server (name or IP address) and port that InterScan will use for sending Notification messages generated by Email VirusWall. (These include notifications to the sender/recipient/administrator and bounced mail messages.)

By default, InterScan will use DNS to send these automatically generated notifications. If the InterScan server does not have DNS access (no direct Internet connection, for example), a SMTP server must be specified here which can deliver Internet mail.

When DNS is used, attempt to send message every [X] minutes for [X] hours

When using a DNS to deliver notification messages and the initial delivery is unsuccessful, Email VirusWall will repeatedly attempt delivery as specified in the Advanced Options page.

Specify the length of the interval you want InterScan to wait between delivery attempts and the length of time it should continue trying. For example, set the repeat interval for 60 minutes and the try-period for 24 hours to have InterScan make a maximum of 24 attempts to deliver the message.

After 24 hours have elapsed, the message is "bounced," or delivered to the sender's mailbox with a message stating that delivery to the specified email address could not be completed.

A record of delivery attempts and results is recorded in the InterScan log file.

Disable insertion of InterScan "Received:" header in processing messages

After processing an email, InterScan "signs" the message in the header area before forwarding it to the SMTP server. This information includes the date and time when InterScan received the mail message and who it came from. In some email clients this header information is not visible.

You can completely mask InterScan by enabling the **Disable insertion...** option. In this case, no additional header information will be written by InterScan during processing.

Looking at the Message properties via Microsoft Outlook Express, for example, shows the following:

> *Received: from us-washington.us-states (localhost [127.0.0.1]) by us-washington.us-states with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.1960.3)id PJVA8RAF; Mon, 21 Jul 2003 11:49:35 -0700*
>
> *OMITTED: [Received: from 100.10.113.10 by us-washington.us-states (InterScan Email VirusWall NT); Mon, 21 Jul 2003 11:49:34 -0800]*
>
> *Date: Mon, 21 Jul 2003 11:48:23 -0800*
> *From: EmailVirusWall@yourcompany.com*

To: Mail_User@internet.com
Subject: InterScan NT Alert

Sender, InterScan detected and cleaned a virus in the email you sent.

Date: Mon, 21 Jul 2003 11:48:23 -0800
Method:Mail
From: <DavidS@us-states.yourcompany.com>
To: <Iras@us-states.hiscompany.com>
File: 6-8WAZ_A.DOT
Action:cleaned
Virus: WORD8_WAZZU.A

Treat MIME attachments whose name is greater than [X] characters as a virus

Email VirusWall provides a solution to the problem of malicious email attachments, with very long file names (typically over 200 characters), that threatens many mail clients.

You can have Email VirusWall rename suspect attachments--before they reach the SMTP server or client--and optionally quarantine the message. This solution works on behalf of all email clients and for any SMTP server.

Quarantine Microsoft Office attachments containing macros

Email VirusWall can be set to quarantine attachments containing macros. The attachments are moved to the InterScan virus directory. This provides additional security against the threat of macro viruses. When this feature is in effect, the original mail message will still be sent to the recipient. Only the attachment is quarantined.

To quarantine attachments, go to the **Advanced Options** tab of the configuration utility and select **Quarantine Microsoft Office attachments containing macros**.

Accept inbound mail addressed only to the following domains (prevents relaying)

InterScan provides a way to prevent your SMTP server from being used to relay mail. (Although once a common practice, abuse by spammers, forgers, and others has forced many administrators to seek a means of ending the practice.)

To prevent your SMTP server from relaying messages,

1. Make active the **Advanced Options** tab of the InterScan VirusWall configuration.
2. At the bottom of the screen, enable the **Accept inbound mail addressed only to the following domains**... option.
3. In the text field below, enter the domain or domains for which InterScan will accept mail.

For example, if your company name is Widgets and your domain is widgets.com, enter widgets.com in the text field. Only inbound mail addressed to users at widgets.com will be accepted.

- Delimit multiple addresses with a comma
- Entries are not case sensitive
- Wildcards are not valid

Metacharacter support

Anti-Relay now supports wildcard characters and metacharacters, such as % and #. The metacharacters must be configured in the intscan.ini file.

For the Meta char support, put the entry below in the [EMail-Scan] section.

```
RestrictInDomainMeta=!#$
```

If the customer wants todisable it, you can remove that entry or leave the string empty after the '=' sign. For example:

```
RestrictInDomainMeta=
```

Plug-In Manager

The Plug-in Manager allows the administrator to manage the allocation of distributed resources by running plug-ins on machines other than the InterScan machine.

Plug-ins include **eManager**, which allows an organization to screen inbound and outbound email for sensitive content, block spam mail at the Internet gateway, and provide bandwidth management for optimizing SMTP server usage.

Plug-in task management is on a multi-threaded DCOM (Distributed Component Object Model) architecture; plug-ins can be installed on the same server as InterScan or distributed among several machines to balance CPU load and processing.

See Chapter 1 for a description of eManager, or check the Trend Micro website at:

`http://www.trendmicro.com`

Plug in Attributes

Only one instance of the Email Manager need be installed on the LAN. Installation occurs by default with Email VirusWall, even if no plug-ins are installed.

When plug-ins are installed, double-click the **Plug-in Manager** button on the Advance Options page, then **Plug-in Attributes** to configure the tasking options.

All three tasking options described below take as their threshold the CPU utilization set in the plug-in's own configuration utility. For example, if you have set the CPU threshold to 75 percent in Email Management, and will use random distribution tasking, only machines reporting less than 75 percent CPU utilization are eligible to receive a task assigned by InterScan.

See the plug-in's native documentation for more information.

Plug-In Controlled

Plug-in Controlled is not available in the current version of InterScan VirusWall. Look for this feature in later versions of InterScan VirusWall. If Plug-in Controlled is selected, it will work in the same way as the Round Robin method.

Round Robin

By default, plug-in tasking is performed Round-robin. Using Round Robin tasking, InterScan distributes mail to be processed according to the plug-in order. For example, if there are two Content Filtering plug-ins and a mail message comes in, InterScan hands over the mail message to the first plug-in for processing. When the next mail message comes in, InterScan hands the message to the second for processing. After it has processed a message, InterScan returns to the first plug-in. Order is set in the Plug-In Manager using the **Move Up** and **Move Down** buttons.

Random Distribution

With Random Distribution tasking, InterScan will distribute mail to be processed randomly amongst the installed Content Filters. Not available in the current version.

Get Information

Get Information/Test Location verifies that a plug-in is installed properly. It also obtains information about the plug-in and displays it. We recommend that you always test newly installed plug-ins.

Add Server and Delete Server

After installing a new plug-in, it should be added to the list of servers kept by the Plug-in Manager on the Email VirusWall machine. Only those plug-in servers appearing on this list (and having a valid connection) are included in InterScan's tasking assignments.

Move Up and Move Down

Use these buttons to change the order in which plug-ins are called. This applies to Plug-In Controlled and Round Robin tasking.

Chapter 8

Log Files

The InterScan VirusWalls keep a running log of their activity. New logs are created daily and represent a valuable source of system information. You can examine all (or selected) log entries to learn what viruses were found in email, FTP and Web traffic, what files were blocked according to the preferences set for Java applets, and when the VirusWalls were stopped or started.

A log-viewing utility is provided to aid you in managing the information. The InterScan administrator can set the viewing priorities in the following ways:

- Sorted by date, user, or virus
- According to service, i.e., the Web, FTP, or email scanning.
- According to date—view log records for a single day, week, month, or a range of days.
- By all or selected users
- By all or specified viruses

Instructions for viewing and deleting virus log files are presented here.

Viewing and Deleting Log Files...

From InterScan's main Log File page (Figure 8-1), find out what logs are currently on the system, choose to delete individual logs manually, schedule automatic deletes, and view some or all of the logs. By default, the VirusWalls write their logs to the directory `c:\interscan`, where `c:\interscan` represents the directory InterScan was installed to. The InterScan logs are named as follows:

iscan.log.2003.06.24

which can be read as *InterScan Log for June 24, 2003*.

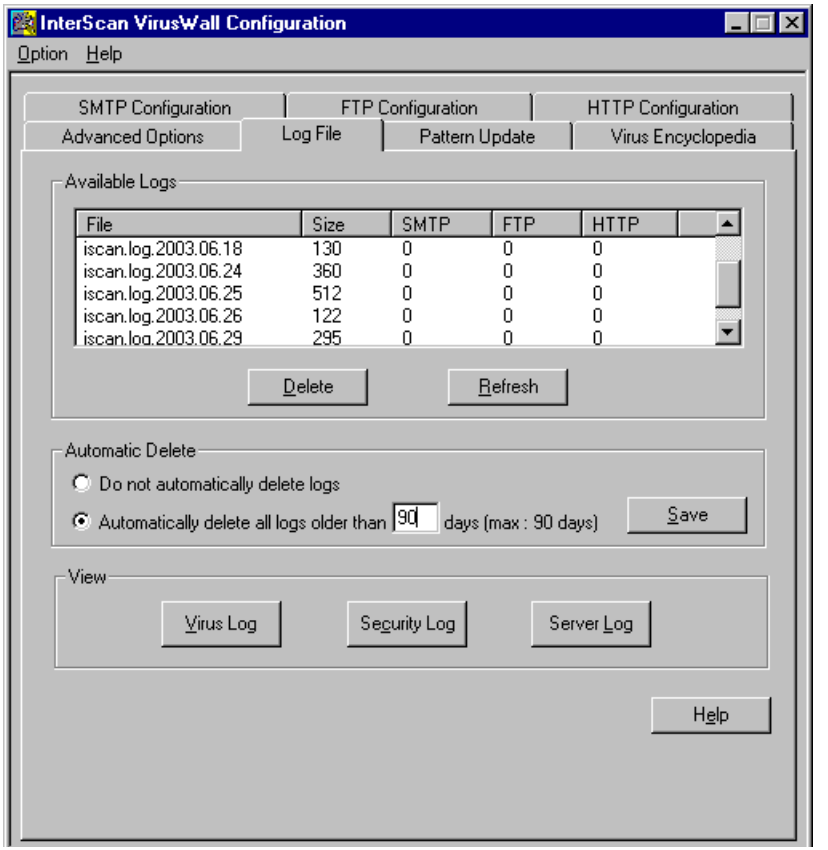


FIGURE 8-1. InterScan Log File page.

Available Logs

Available Logs is the most basic summary of InterScan's anti-virus activity, and shows the number of viruses found on a given day for each of the services. Appearing in a column under the FILE header is a cumulative list of all the InterScan log files on the system, with the file size and number of viruses found

Deleting Virus Logs

Because InterScan VirusWall creates and saves new log data every day, you may find that more logs have accumulated than you have a need for. You can delete the excess log files manually or automatically, as explained below. The current day's log cannot be deleted.

Deleting Log Files Manually

To manually delete individual log files:

1. Click the individual logs you want to remove to highlight them and then click the **Delete** button.

   a. To delete multiple, contiguous, log files hold down the SHIFT key while selecting the files to delete, then click the **Delete** button.

   b. To delete non-contiguous files, hold down the CTRL key while selecting the files, then click the **Delete** button.

   c. Delete all the files appearing on the list by clicking the delete button without any individual logs selected.

Deleting Files Automatically

You can also schedule InterScan to automatically delete log files more than a certain number of days old.

1. Click the **automatically delete all logs older than __ days** radio button to activate this feature.

2. Next, enter a value in the **days** field. The maximum is 90 days, meaning that files older than 90 days will be deleted if they are left in the default directory. The default value is 30 days.
3. Click **Save** to preserve your preferences.

Viewing Logs

You can view the Virus log, the Security log, and the Server log by clicking the relevant button. Clicking **Virus Log** brings up a page like the following (fig. 8-2).

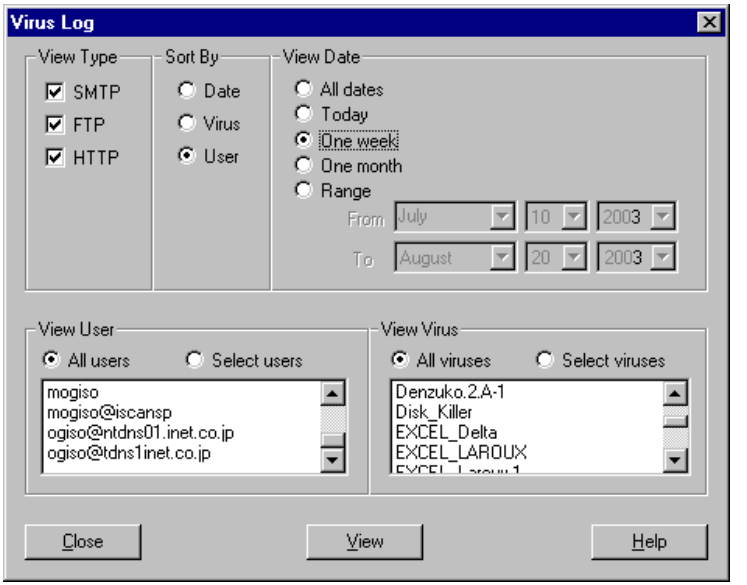


FIGURE 8-2. Selecting virus logs to view.

Viewing the Virus Logs

1. Under **View Type**, check the VirusWall for the logs you want to view, SMTP, FTP, or HTTP.

2. Under **Sort By**, choose the sorting priority, either **Date**, **Virus**, or **User**, that you want the data to appear in. For example, choosing Date as the priority to sort by results in the viewable log being built starting with the earliest dates first.
3. Next, in the **View Date** group, check the radio button for the log dates you want to view:
   a. Check the **All Dates** radio button to select for viewing the log files for all the dates.
   b. Check the **Today** radio button to select for viewing the log file generated since midnight of the current day.
   c. Check the **One Week** radio button to select for viewing the log files generated over the past seven days.
   d. Check the **One Month** radio button to select for viewing the log files generated over the past 30 days.
   e. Check the **Range** radio button to select for viewing a range of dates, and specify the start and end dates for the log files you want to view.
4. In the **View User** group, check the **All Users** radio button to see the logs for all users. Otherwise, check the **Select Users** radio button and choose from the list of individuals to see which viruses were detected in their Internet traffic.
5. In the **View Virus** group, check the **All Viruses** radio button to view the logs for all viruses. Otherwise, check the **Select Viruses** radio button and choose from the list of viruses to see, for example, the prevalence of a given virus.
6. Finally, click the **View** button. InterScan will pull data from the virus log files according to the preferences you have specified and open up a text file with the results, like so:

[FTP]

Date: 07/21/2003 11:26:36
File: lay4.zip
From: 100.10.10.11
To: john@100.10.10.22
Action: passed
Virus: Stoned.Azusa
Virus: (c)Brain
Virus: BANANA
Virus: CLOUDS_II

[FTP]
Date: 07/21/2003 11:26:41
File: v6.zip
From: 100.10.10.11
To: john@100.10.10.22
Action: passed
Virus: JERUSALEM-3-S
Virus: Stoned
Virus: BANANA
Virus: MSWORD_CONCEPT
Virus: KeyDrop-I
Virus: Alfon

[HTTP]
Date: 07/21/2003 15:26:28
File: antiexe.exe
From: http:///100.10.10.11/test/virus/ant.exe
To: 100.10.10.22
Action: moved to ant.exe.1
Virus: Trkswap

Notice that in addition to whether the file was transported via SMTP, FTP, or HTTP, the log also includes the date the virus was discovered, the name of the file it had infected, the Internet address of the originating site, the intended recipient of the file, the action that InterScan took on the infected file, and the name of the infecting virus.

Viewing the Security Logs

As you know, Web VirusWall permits the InterScan administrator to block, site-wide, certain file content types and files originating from untrusted vendors. As with all the VirusWalls, a record is kept detailing whatever actions was taken. To view the Security log,

1. Click the **Security Log** button from the main Log File page.

2. Under **View Type**, check Java Applets as shown in Figure 8-3.

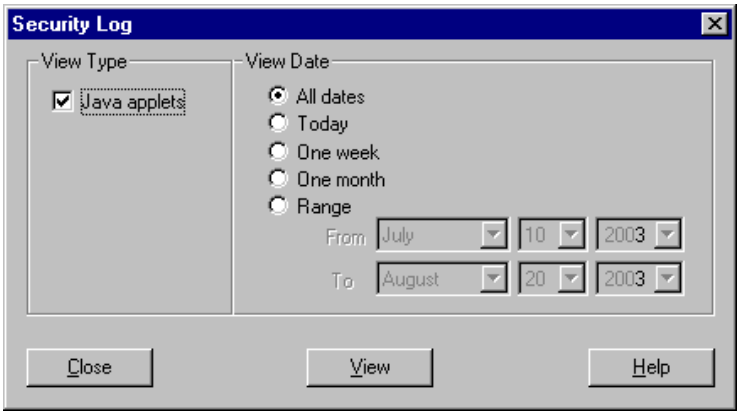


FIGURE 8-3. The Security log, where you can view which Java files have been blocked.

3. Next, in the **View Date** group, check the radio button for the log dates you want to view:

   a. Check the **All Dates** radio button to select for viewing the log for all the dates.

   b. Check the **Today** radio button to select for viewing the log generated since midnight of the current day.

   c. Check the **One Week** radio button to select for viewing the logs files generated over the past seven days.

   d. Check the **One Month** radio button to select for viewing the log files generated over the past 30 days.

   e. Check the **Range** radio button to select for viewing a range of dates and specify the start and end dates.

4. Click the **View** button. InterScan will pull data from the virus log files according to the preferences you have specified and open up a text file with the results, like so:

   [JAVA_APPLET]
   4.Date: 07/21/2003 16:20:55
   File: chart.class

From: http://100.10.10.11/security/chart.class
To: 100.10.10.22
Action: blocked

Viewing the Server Logs

The InterScan administrator can also view logs regarding all server activity, such as when a service was stopped or started and when virus pattern files were downloaded.

1. Under **View Type**, check the service or services (**SMTP**, **FTP**, **HTTP**) for the logs you want to view (fig. 8-4).

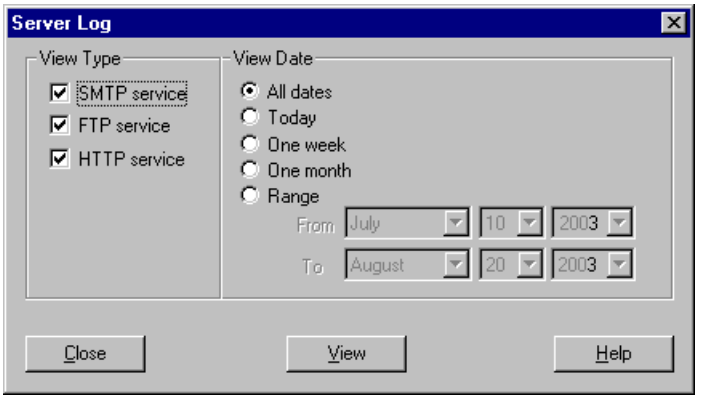


FIGURE 8-4. The Server log, where you can view a record of server activity.

2. Next, in the **View Date** group, check the radio button for the log dates you want to view:

   a. Check the **All Dates** radio button to select for viewing the log files for all the dates.

   b. Check the **Today** radio button to select for viewing the log file generated since midnight of the current day.

   c. Check the **One Week** radio button to select for viewing the log files generated over the past seven days.

d. Check the **One Month** radio button to select for viewing the log files generated over the past 30 days.

e. Check the **Range** radio button to select for viewing a range of dates, and specify the start and end dates for the log files you want to view.

3. Click the **View** button. InterScan will pull data from the virus log files according to the preferences you have specified and open up a text file with the results, like so:

07/21/2003 15:56:38 HTTP loaded pattern file: 375
07/21/2003 15:56:38 [HTTP daemon started]
07/21/2003 15:56:38 FTP loaded pattern file: 375
07/21/2003 15:56:38 [FTP daemon started]
07/21/2003 15:56:38 MACROTRAP pattern file loaded.
07/21/2003 15:56:38 MACROTRAP pattern file loaded.
07/21/2003 15:57:04 SMTP loaded pattern file: 375
07/21/2003 15:57:05 MACROTRAP pattern file loaded.
07/21/2003 15:57:06 [Mail service started]
07/21/2003 16:50:13[FTP daemon ended]

Chapter 9

Active Update

Chapter Overview

New in this version is the ability to update the pattern file and scan engine automatically from one convenient, easy-to-use Active Update configuration screen. Just select which of the components to update, the time to run the updates, and whether to update from the Internet or from another server on your network. You may choose to have one central server perform regular updates from Trend Micro's web site and then configure your other servers to obtain their updates from your central server.

New virus pattern files are available every week and you should schedule weekly pattern file updates. New scan engine updates are available periodically and you should schedule regular scan engine updates.

Updates are available free for one year to registered users and can be downloaded automatically using the InterScan's built-in "Active Update" technology. This chapter describes how to download program file updates manually from the Internet, as well as how to schedule InterScan to perform regularly scheduled updates.

To be eligible for Active Updates of the scan engine and pattern file updates, you must first register your copy of InterScan through the windows console's Registration button on the Active Update tab.

Virus Pattern File

InterScan draws upon an extensive database of virus "signatures," commonly called the virus pattern file. It is this file that InterScan uses to detect viruses in email traffic, folder replications, and archived documents.

As new viruses are written, released to the public and discovered, Trend Micro collects their telltale signatures and incorporates the information into the virus pattern file. Because new viruses are continually being discovered, we strongly suggest that you update your virus pattern files regularly. We update our virus pattern files weekly on Wednesdays.

If a particularly damaging virus is discovered 'in the wild', we will release a new pattern file as soon as we have a detection routine for that virus. Since new virus pattern files are available every week or sooner, you should schedule automatic updates at least weekly.

To obtain updated virus pattern files, you must register InterScan with Trend Micro.

Scan Engine

A virus scanning engine is the program that does the actual work of scanning files and detecting viruses.

We release new engine versions for a number of reasons:

1. Because new types of viruses have been developed that may not be detected by the old engine.
2. We have enhanced scanning performance and detection rates.
3. We have added support for virus detection to additional formats, for example, the newest Microsoft Word and Excel types.
4. We modified the scanning engine to detect and remove malicious Java and ActiveX code.

InterScan scans UUENCODE, BINHEX, and MIME encoded attachments and scans a wide variety of compression types, including: PKZIP, ZIP TO EXE, ARJ, ARJ TO EXE, LHA, LHA TO EXE, BASE64, TAR, GZIP(.GZ), LZEXE, PKLITE, DIET, MSCOMPRESS, CABINET(.CAB), UNIX LZW, COMPRESS(.Z), UNIX PACK(.Z)

Registration

There are two ways to register InterScan: (1) by filling out and mailing the Registration Card included in the InterScan package, or (2) by completing the Registration Form in the InterScan Web Console and sending it over the Internet.

Note: You must register through the windows console to receive regular pattern file updates via the Internet.

Registering through the InterScan Web Console

1. Select **Active Update**, then **Registration**. The Registration screen appears. Complete the form, filling in all required fields (all fields are required except the mailing address fields).
2. If you need to go through a proxy server to access the Internet, fill in the information in the **Proxy Setting** area before filling in the registration information.

   Type in the **Proxy server** IP address and the **Port** number. Port 80 is the most commonly used port to connect to the Internet and is displayed as the default.

   If your proxy server requires proxy authentication, enter the **User name** and **Password** you use to authenticate your Internet connection.
3. Click **Save**.
4. Click **Register** to send your online registration.

You can now download new virus pattern files from Trend Micro's web site.

Configuring Active Updates

We recommend that you update your virus pattern file every week to keep up with the latest viruses. Thousands of new viruses are written and released each year, so you should not allow the pattern file to fall months out of date. Active Update automatically updates the virus scanning engine as well when there is a new scan engine available.

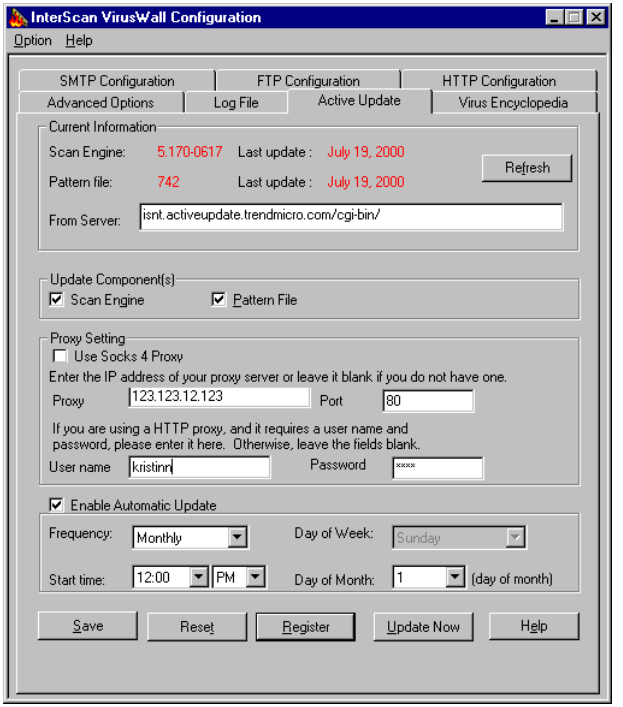


FIGURE 9-1. Active Update configuration screen

You can schedule InterScan to automatically download the latest program file updates from Trend Micro or from another server on your network. The main issue when configuring Active Update is whether you will connect directly to Trend Micro for updates or connect to a Trend Micro server that has Active Update enabled. Both configuration options are described below:

1. Select the **Active Update** tab.
2. Select the **Enable Automatic Update** checkbox.
3. In the time settings section, select the update **Frequency**. You may select Hourly, Daily, Weekly, or Monthly. If you select Weekly, select the **Day of**

Week in the next field. Likewise, if you select Monthly, select the numeric day in the **Day of Month** field.

4. Select the **Time** that you would like the updates to occur. Be sure to select the radio button for **AM** or **PM**.
5. Select which components you would like to update:
   - Pattern File
   - Scan Engine

   Normally, it is best to select both types of updates so that you will be sure to have the latest software installed.
6. Next, select the location where you would like to download the new updates from:

   a. If you do **not** have a Trend Micro server centrally managing your antivirus services, you should keep the default setting to download the latest updates directly from Trend Micro's web site.

   If you use a proxy server to access the Internet, type in the **Proxy server** IP name or number, and the **Port number**.
   If your proxy server uses the Socks 4 protocol, click the **Socks4** checkbox.
   If your proxy server requires proxy authentication, type in the **User name** and **Password** used to access it. Then click **OK**.

   b. If you have a Trend Micro server centrally managing your antivirus services and you intend to use Trend Micro to distribute Active Updates to your InterScan servers, specify the name of the server where the update package exists in the **From Server** field.

   For example,
   `http://[Domain name or IP address of your Trend Micro server]/download/activeupdate`.

Note: The Trend Micro server that you are updating from must already have downloaded a copy of the update package from Trend Micro.

---

7. Click **Save** to apply your changes.

Configuring Update Now

Update Now is used to perform an immediate update of the pattern file and scan engine. Configuration of **Update Now** is identical to configuring scheduled updates. Once the configuration is complete, click **Update Now** and InterScan will automatically update the program files to the newest versions.

Manually Updating the Pattern File

If you are not able to update directly through the Active Update connection, you may also manually copy the pattern file to your file server. InterScan will use the pattern file with the largest pattern file number. the pattern files are found in the `\InterScan` directory. For example, if you have the files `lpt$vpn.388` and `lpt$vpn.410` listed in your `\InterScan` directory, 410 is the pattern that will be used for virus scanning.

Follow these steps to manually copy the updated pattern file onto your server:

1. Open your web browser and go to the following URL:

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

2. Select **Pattern Files**.
3. Follow the online instructions to download the pattern file.
4. Stop the InterScan scanning services. Go to **Start | Settings | Control Panel | Services** and make sure that no InterScan scanning services are running.
5. Double-click the file you downloaded and unzip it.
6. Copy the pattern file to the `InterScan` directory, which by default is `c:\InterScan`.
7. Restart the InterScan scanning services.

Manually Updating the Scan Engine

If you are not able to update directly through an Internet connection, you may manually copy the scan engine to your file server or workstations. Follow these steps to manually copy the updated scan engine onto your server:

1. Open your web browser and go to the following URL:

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

2. Select **Scan Engines**.
3. Download the scan engine for your program version of InterScan.
4. Stop the InterScan Real-Time Scanning services. Go to **Start | Settings | Control Panel | Services** and make sure that no scanning services are running.
5. Double-click the file you downloaded and unzip it.
6. Copy all files listed to the `InterScan` directory, which by default is \WINNT\System32, replacing the existing files.
7. Restart the InterScan scanning services.

Chapter 10

Virus Encyclopedia

InterScan VirusWall provides an extensive online encyclopedia of computer viruses. You can use the Web browser to view the following information:

- Virus Classifications
- Anti-Virus Methods
- Detailed information about the viruses listed in the encyclopedia

Accessing the Virus Encyclopedia

Use the Virus Encyclopedia to find out more about individual viruses, including typical symptoms, the infection procedure, and the damage routine.

1. Click the Virus Encyclopedia page to bring up a window like the one shown below.

2. Scroll down the list of viruses on the left and click the one you would like to learn more about. A corresponding description appears on the right.

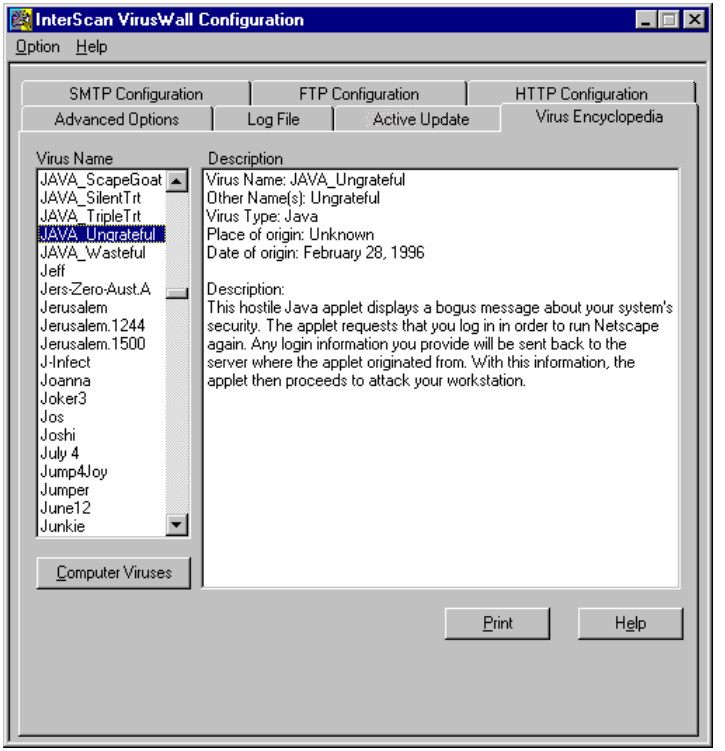


FIGURE 10-1. The Virus Encyclopedia page.

About Computer Viruses

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

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

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

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

Types of Viruses

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

Computer viruses can be roughly classified into the following categories:

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

Macro viruses

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

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

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

File Viruses

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

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

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

Boot Viruses

Boot sector viruses, the most common type of virus, move or overwrite a disk's original boot sector data and replace it with the infected boot code of their own design. Floppies and hard drives are the most susceptible to being overwritten by a

boot sector virus. Then, whenever the infected system (boots up), the virus loads into memory where it can gain control over basic hardware operations. Of course a boot virus can also quickly spread to any of the other drives in the system (floppy, network, etc.).

Multi-partite Viruses

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

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

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

Polymorphic, or Mutation Viruses

Polymorphic (mutation) viruses are unique in that they try to elude detection by changing their structure after each execution— with some polymorphic viruses, millions of permutations are possible. Of course, this makes it harder for normal anti-virus programs to detect or intercept them. It should be noted that polymorphic viruses do not, strictly speaking, constitute a new category of virus; they usually belong to one of the categories described above.

Virus Writers

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

How Viruses Spread

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

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

The most likely virus entry points are Internet and network connections, floppy disk drives, and modems or other serial or parallel port connections. In today's increasingly interconnected workplace (Internet, intranet, shared drives, removable drives, and email), virus outbreaks now can spread faster and wider than ever before.

Methods of Virus Detection

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

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

This methods has several disadvantages, however, the biggest being that false alarms are altogether too common. The records used by checksumming programs are often rendered obsolete by legitimate programs, which, in their normal course of operations, make changes to files that appear to the Integrity checker to be virus

activity. Another weakness is that these programs can only alert the user *after* a virus has infected the system.

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

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

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

Types of Anti-Virus Programs

The final target of most viruses is the local hard drive of a PC or workstation. To get there, the virus may hitch a ride on another program or remain on the server. But eventually, the intent is to damage the data and/or program files of end users. In a client-server environment, obviously, the target is corporate data.

Ideally you want to detect a virus as soon as it enters your PC, workstation, or network system. The following methods of virus safeguard are widely in use:

- **Anti-virus programs for dedicated use on workstations and PCs**. Typically, these programs are automatically invoked upon boot up but can also be run manually. They check the memory and all files on your system. Usually these programs can remove the virus, but you may need to re-boot from a clean floppy that automatically runs the anti-virus program on boot up.

- **Anti-virus programs for dedicated use on network servers.** These programs run on network servers and are typically TSRs. They scan all incoming files for viruses and alert the system administrator whenever a virus is detected.
- **Anti-virus programs for use on both workstations and servers.** These programs typically combine features found in the latter types of anti-virus programs and can be used for both workstations and servers.
- **Anti-virus programs to protect entire networks.** This type of anti-virus program, which includes the InterScan VirusWalls, runs on the network gateways or Internet servers. They intercept viruses inbound on email attachments, FTP downloads, and Web traffic *before* they enter your LAN.

Note: This type of anti-virus program is not intended to replace a firewall. Rather, it serves as a supplementary form of protection that internal firewalls alone cannot provide.

Chapter 11

Technical Support and Troubleshooting

Chapter Overview

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

We can be reached via telephone, fax, BBS, email, regular mail, and Internet at:

`http://www.trendmicro.com`

Send Trend Micro Your Viruses

You can email Trend Micro your viruses. More specifically, if you have a file you think is infected with a virus but the scan engine doesn't detect it or can't clean it, we encourage you to send the suspect file to us using the submission screen at the following URL:

http://subwiz.trendmicro.com/SubWiz/UndetectedMalware-form.asp?TMsessionid=E73B9AF63D0B4A9EBE8D9B3F510AE0D0&proc=7

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

In addition, this chapter contains several basic troubleshooting procedures that you may wish to undertake if you are experiencing a problem, as well as a complete explanation of all the InterScan VirusWall error messages.

Troubleshooting and Error Messages

Can't Get Email

If you find that you are no longer receiving email after installing Interscan VirusWall, there are a couple of things you can do before contacting Trend Micro's technical support.

The first thing to check is that the SMTP service has not been stopped, and that Email VirusWall is also running. If both check out fine, bring up the SMTP configuration page (fig. 4-1) and make a visual inspection of the IP address and port number that have been designated for the original SMTP server to be sure they are correct.

There are a couple of general rules to bear in mind regarding the InterScan SMTP configuration:

1. The original, or primary, SMTP server is often the same server that has all the mailboxes.
2. The value in PORT *should not be 25* if the InterScan Email VirusWall is installed on the same machine as the original SMTP server.

   Since InterScan uses port 25, a conflict will occur if the original SMTP server is also assigned port 25 on the same machine. Change the port to another number, such as 6000 in the InterScan configuration.
3. If the InterScan Email VirusWall is installed on a different machine than the original SMTP server, check to be sure that the value entered for original SMTP server port in the InterScan configuration *is* 25.

If all these check out, the next thing to do is have a look at how your MX record is set up, or, if you have rerouted incoming mail without modifying your MX records, what IP address is being used. See Chapter 2 of this Administrator's Guide for more information.

You can also use Telnet to help locate the source of the problem. The idea here is to use Telnet to test the validity of the IP addresses and port numbers you are using for the original SMTP server and the InterScan machine (fig. 11-1).

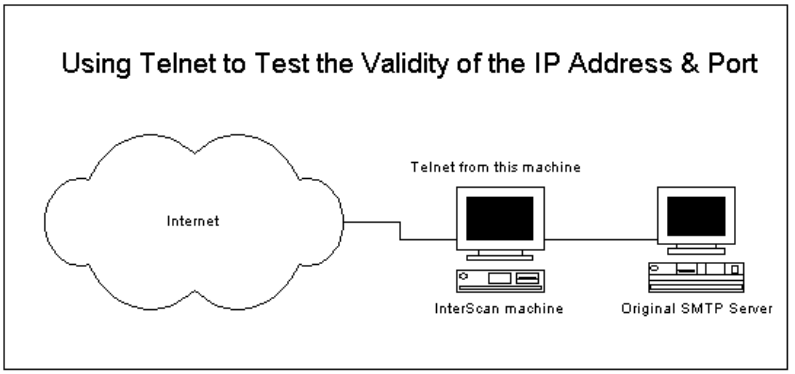


FIGURE 11-1. Using Telnet to diagnose SMTP problems.

From the machine that InterScan is installed on,

1. Bring up Telnet and click **Connect**, **Remote System**. For Host Name, enter the IP address of the original SMTP server and set the correct Port. Click **Connect**.

   If the IP address and Port are correct you will receive a message from the original SMTP server, similar to the following:

   220 name.domain InterScan VirusWall NT SMTPD ready at Tue, 04 Feb 2003 15:58

   If you don't receive such a message identifying the InterScan VirusWall, you need to either correct the IP address, correct the port, start the SMTP service, or check the connection between InterScan and the original SMTP server. You can do this by "pinging" the IP address in question, for example,

   ping 127.100.100.10

   from a DOS prompt. A `ping` failure indicates a connection error.

2. Using Telnet again, this time test the IP address and port number (25) of the machine that InterScan is installed on if it is different from the original SMTP

server. To do so, follow the procedure outlined above, this time using the IP and port for the InterScan machine.

Email Messages Come in as Attachments

If the text body of your email messages is being included as an attachment rather than text, there is a quick change you can make to the InterScan configuration to correct the problem.

1. Bring up the InterScan VirusWall configuration page and make EMAIL CONFIGURATION the active page.
2. Towards the bottom of the page, below the three warning message boxes, you'll see the following check box option:

   "__Safe Stamp"

   Remove the check mark in the box by clicking it once, then click the SAVE button in the lower left corner.

The error occurs occasionally due to the way some SMTP servers handle attachments.

Streaming Protocols Do Not Work

In order for the VirusWalls to scan a file for viruses, the files to be scanned must first be entirely downloaded. Streaming protocols, on the other hand, begin using the file contents as soon as the first part arrives at the destination. After installing Web VirusWall, if your LAN users are no longer able to play certain MIME types, chances are it is because these types have not been added to the list of MIME types Web VirusWall will ignore.

To check this,

1. Bring up the HTTP configuration page using either the GUI or a Web browser and click the **MIME** button (or the **MIME configuration** button in the Web browser).
2. If the effected MIME type does not appear on the list, add it. InterScan will no longer scan that MIME type.

With InterScan no longer configured to scan these file types, the streaming protocols will be able to act as designed.

Error Messages

If you receive an error message from InterScan VirusWall, please refer to the alphabetical list of error messages below for further information. In many cases you will be able to resolve the error by taking the course of action suggested. For persistent errors, however, or if you are not comfortable making changes to your system, please contact Trend Micro's technical support.

Note: Some error messages are also recorded in the log file. These are so noted.

"Could not bind socket to SMTP port. SMTP server may already be running."

There are two likely reasons for this message to appear:

1. A previous installation of InterScan, using port 25, is already running.
2. Another SMTP Server application is using port 25.

   Check any other mail servers or installations of InterScan to see what port they are assigned. Since NT does not allow simultaneous use of the port, it must be freed up for exclusive use by InterScan.

   This error message is also written to the log.

"Error connecting to inbound SMTP server!"

InterScan was unable to connect to the SMTP server or host. Check the Port, Host, or both to be sure they are configured correctly.

This error message is also written to the log.

"Error reading pattern file"

The file containing InterScan's comparative virus patterns is corrupt or missing. Download the file again, or copy the file **`LPT$VPN.???`** from the original installation disk to the x:**`\interescan`** directory, where x: is the drive letter and

path that InterScan was installed to. If you correct this error by copying the original virus pattern file from the installation disks, then be sure to download the most recent version of the pattern file from Trend Micro.

This error message is also written to the log.

"Failed to clean file... "

A virus was detected, however the file could not be cleaned. The email is delivered to the intended recipient with the notification above.

Note: The virus in this file may still be "live" and capable of spreading. You will probably want to delete the file manually.

This error message is also written to the log.

"Invalid original SMTP server address"

The host name is invalid. Check the IP address listed in the InterScan configuration and change it as necessary. Use NT's Telnet to verify the listed IP address (Figure 11-1).

"Invalid outbound SMTP server address"

This error only occurs if you are using InterScan VirusWall to scan outbound mail and indicates that the IP address entered for the outbound SMTP server is invalid. Check the IP is as it appears in the InterScan SMTP page configuration and change if necessary. Use NT's Telnet to verify the listed IP address as explained on page 11-1.

"ISSMTPD failed to init"

This message indicates that the InterScan Email VirusWall did not load properly, resulting in an ISSMTPD that has not initialized properly. You may need to contact Trend Micro's technical support. (Find the contact information for the support site nearest you under the Technical Support page of the configuration window, as explained in Chapter 11.)

"Program directory could not be read from registry"

A discrepancy between where NT expects to find the InterScan product and where it is actually installed can cause this message. If you are comfortable editing the NT registry, check the following entry:

HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\ InterScan Email VirusWall\CurrentVersion

The ProgramDirectory field should match the directory where the product is actually installed. If it doesn't, you may want to back up the registry and then make the appropriate changes to the directory listed. This error occurs, for example, if InterScan was reinstalled (or moved) to a different directory, but the registry was not properly updated.

"Program working directory does not exist"

Check to see if InterScan's program directory has been renamed or moved.

"Registry data could not be read"

The NT registry is returning an error. Check the registry, or contact technical support.

"This application runs only on Windows NT"

InterScan is being installed onto the wrong platform. Check to be sure that the disks you are using contain the InterScan version written for the platform you are using and that the machine you are trying to install InterScan on is running NT version 3.51 or greater.

"Unknown recipient:—bouncing msg"

The addressee could not be found; the email message is being returned to sender. This is probably a sender addressing error.

This error message is also written to the log.

"WinSock 1.1 not installed"

InterScan was unable to locate WinSock 1.1. Be sure that NT's TCP/IP protocol, which use Winsock version 1.1 or higher, has been installed. You may need to verify that another communications program has not replaced NT's native WinSock ver 1.1

with a different version. If you find that it has, WinSock can be installed from the NT program disk(s).

"Wrong WinSock version"

If you are using a third-party TCP/IP protocol, its WinSock may be the wrong version. Be sure that NT's TCP/IP protocol, which uses Winsock version 1.1 or higher, has been installed. If you find that the wrong WinSock is on the machine, Winsock version 1.1 or higher can be installed from the NT program disk(s).

Chapter 12

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 must, be sure to make a back up copy first!

See the `intscan.ini` file itself for additional parameters and information.

[Common]

Parameter	*Default Value*	*Possible Values*	*Explanations*
NotificationFro-mAddress	postmaster	any email address	Appears in From field of Inter-Scan notifications
NotificationFro-mAddressOthers	postmaster	any email address	Appears in From field of Inter-Scan notifications

[Scan-Configuration]

Parameter	*Default Value*	*Possible Values*	*Explanations*
httpscan	yes	yes no	yes: scanning is on no: scanning is off
ftpscan	yes	yes no	yes: scanning is on no: scanning is off
mailscan	yes	yes no	yes: scanning is on no: scanning is off

[Content-Access-Configuration]

Parameter	*Default Value*	*Possible Values*	*Explanations*
HttpContentAc-cessRules	no		
AuthenticodeTrust-ComPub	0		

[HTTP-Scan]

Parameter	*Default Value*	*Possible Values*	*Explanations*
ThreadPool	100	any integer	Available processes
InterScanHTTPS-ervicePort	8080	Any unused port	Port used by InterScan to accept HTTP traffic
HOrg	localhost		
HOrgPort	5000		
HLogFile	..\iscan.log		
LogRequest	no		
Level	ScanAll		
ScanExtensions	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, LHZ, AIP, RAR, Z, TAR		
VirusMessage	No		
VirusMessageText			
SMTPServerPort	25		
EMail	No		
Addr			
Message1	InterScan has detected a virus(es) in user's HTTP traffic.		
Action	Delete		
passwait	10		
MoveDir	.\virus		

Parameter	*Default Value*	*Possible Values*	*Explanations*
IgnoreLocalIISRequests	No		
JavaBlockingStopByteCodeBinaries	No		
JavaBlockingStopByteCodeBinariesMessage	The Java applet has been blocked by InterScan NT		
Authenticodefile-Types			
AuthenticodeBlockUnsignedFiles	No		
AuthenticodeBlockUnsignedFilesMessage	The requested file has not been authenticode signed and has been blocked by InterScan NT		
AuthenticodeBlocksignedFilesExceptForTrusted	No		
AuthenticodeBlocksignedFilesExceptForTrustedMessage	The requested file is signed but not trusted and has been blocked by InterScan NT		
MIMEBypassing	Yes		

Parameter	Default Value	Possible Values	Explanations
MIMEBypassing-Types	text/html, audio/x-pn-rea-laudio, applica-tion/x-director, image/tiff, image/jpeg, image/gif		
SMTPServerAddr			
PushApplet	No		
CVPAuthentication	No		
TrickleAmount	1024		
TricklePeriod	512		

[SMTP]

Parameter	Default Value	Possible Values	Explanations
MaxScanningTh-readsProc	25		Limits the number of mes-sages being scanned per processor. Additional mes-sages are sent a "452 Server too busy" response.
MaxSMTPClient-ThreadsProc	50		Limit the number of threads created to deliver mail after scanning.

Parameter	*Default Value*	*Possible Values*	*Explanations*
BackgroundM-queueInThread-sProc	2		Fixed number of background threads per processor created to deliver inbound mail in the mqueue after scanning, When mqueu is backed up, this value can be increased.
BackgroundM-queueOutThread-sProc	2		Fixed number of background threads per processor created to deliver outbound mail in the mqueue after scanning, When mqueu is backed up, this value can be increased.
BackgroundBM-queueThreadsProc	1		Ficed number of threads to deliver InterScan generated messages in the bmqueue.
MaxClientConnec-tions	25		Maximum number of simultaneous connections accepted by InterScan.
DisableReceived-Header	No		
InterScanSMTPS-ervicePort	25		
InboundUseDNS	No		
OutboundUseDNS	Yes		
EOrg			
EOrgPort	25		

Parameter	*Default Value*	*Possible Values*	*Explanations*
NotificationsSMT-PAddr	default		
NotificationsSMTP-Port	25		
OutboundMailScan	No		
OutboundMailVi-rusScan	Yes		
OutboundMail-ClinetIP			
OutboundMailSMT-PAddr			
OutboundMailSMT-PPort	25		
HoldInfectedOut-boundMsgs	No		
DeliveryMaxHours	24		
DeliveryRetryM-inutes	15		
ELogfile	..\iscan.log		
Level	ScanAll		
ScanExtensions	EXE, COM, SYS, DRV, DLL, XLS, ZIP		
EMail	No		
Addr			

Parameter	*Default Value*	*Possible Values*	*Explanations*
Message1	Administrator, InterScan has detected virus(es) in user's email attachment.		
EWarning	Yes		
EMessage	receiver, Inter-Scan has detected virus(es) in the email attach-ment.		
EWarningSender	Yes		
EMessageSender	Sender, Inter-Scan has detected virus(es) in your email attachment.		
Stamp	No		
StampMessage	No		
VirusMessage	No		
VirusMessageText			
Action	Autoclean		
MoveDir	.\virus		
DisableForwarding	No		

Parameter	*Default Value*	*Possible Values*	*Explanations*
SenderNoVirus-Message	No		
CleanedFileDesti-nation	Recipient		
RootFolder	C:\temp		
MailFromValida-tionString	#venus_mail#		
UnCleanedFile-Destination	recipient		
UnCleanedFileRe-cipientAction	Delete		
VirusDoctorAddr			
ViceOn	No		
ViceFolder	C:\temp		
InESMTPSIZE	0		
OutESMTPSIZE	0		
CVPAuthentication	No		
MimeHeaderCheck	Yes		
MimeHeaderSize	200		
RestrictInDomain	No		
RestrictInDomain-List			
QuarantineOf-ficeMacros	No		

Parameter	Default Value	Possible Values	Explanations
VsapiFailReject-Connections	No		

[FTP]

Parameter	Default Value	Possible Values	Explanations
MaxThreads	50		
InterScanFTPSer-vicePort	21		
UseFTPProxy	No		
FOrg			
FOrgPort	21		
ForcePassiveFTP	No		
FLogFile	..\iscan.log		
Level	ScanAll		
ScanExtensions	EXE, COM, DOC, SYS, DRV, CMD, DLL, XLS, ZIP		
VirusMessage	No		
VirusMessageText			
SMTPServerPort	25		
EMail	No		
Addr			

Parameter	*Default Value*	*Possible Values*	*Explanations*
Message1	InterScan has detected virus(es) in user's FTP traffic.		
Action	Delete		
MoveDir	.\virus		
SMTPServerAddr			
CVPAuthentication	No		
TrickleAmount	1024		
TricklePeriod	512		

[Active-Update]

Parameter	*Default Value*	*Possible Values*	*Explanations*
PatternVersion	740		
EngineVersion	5.17		
Method	Automatic		
Frequency	Daily		
DayOfWeek1	Thursday		
DayOfMonth	5		
Hour	9:00		
APM	PM		

Parameter	Default Value	Possible Values	Explanations
UseSocks4Proxy	no		
HTTPProxy			
HTTPPort			
UpdateServer	isnt.activeup-date.trendmi-cro.com/active update		Location of the Active Update server.
UpdateEngine	Yes		
UpdatePattern	Yes		
UpdatePatch	No		

[View-Configuration]

Parameter	Default Value	Possible Values	Explanations
Sort	Date		
FTP	Yes		
Mail	Yes		
Periodic	No		
Manual	No		
Date	All		
SYear	1996		
SMonth	July		
SDay	10		

Parameter	*Default Value*	*Possible Values*	*Explanations*
EYear	1996		
EMonth	August		
EDay	20		
User	All		
UserName	Bob		
Virus	All		
VirusName	MSWORD-CONCEPT		
VLetter1	2		
VLetter2	9		
View	Virus		
SMPT	Yes		
HTTP	Yes		

[Log-Files]

Parameter	*Default Value*	*Possible Values*	*Explanations*
AutoDelete	Yes		
KeepLastDaysOf-Logs	30		

[Registration]

Parameter	*Default Value*	*Possible Values*	*Value explanations*
Product	InterScan Virus Wall		InterScan VirusWall
Version	3.5		3.4
Date	none	date	current date or purchase date
FirstN			
LastN			
EMail			
HPhone			include area code
OPhone			include area code
Fax			include area code
RealAddr			address, number, street
City			
State			two-letter abbreviation
ZIP			
Country			blank if USA
Company			
SMTPSerial			
FTPSerial			
HTTPSerial			

[eManagerExceptionNotifications]

Parameter	*Default Value*	*Possible Values*	*Explanations*
Notify	Yes		
Subject	Subject; inter-Scan virusWall NT emanager exception Notification		
Line1	Notification: An exception occurred in eManager		
Line2	Please restart the eManager service.		
EmanagerFailRejectConnections	No		

Appendix A

Setting up NT Security & Exchange Server

Setting up Microsoft Internet Information Server Access to the InterScan VirusWalls

During the installation of the InterScan VirusWalls, Microsoft Internet Information Server is automatically configured so that it can access the VirusWalls over the network. In the event that something happens to your settings and you need to reconfigure MS Internet Information Server without having to reinstall InterScan, you can follow the steps provided below.

1. Go to IIS and open the **Internet Service Manager**.

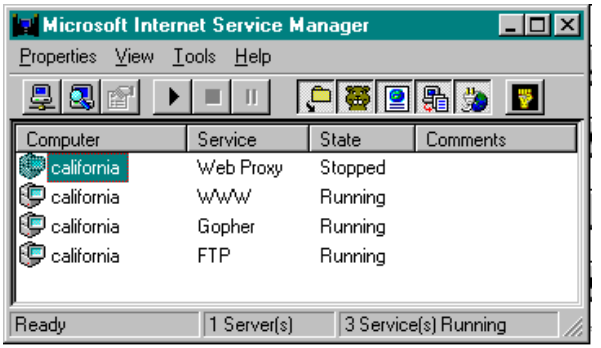


FIGURE 1-1. The Microsoft NT Internet Service Manager window.

2. Double-click on the WWW service to open the **WWW Service Properties** window.

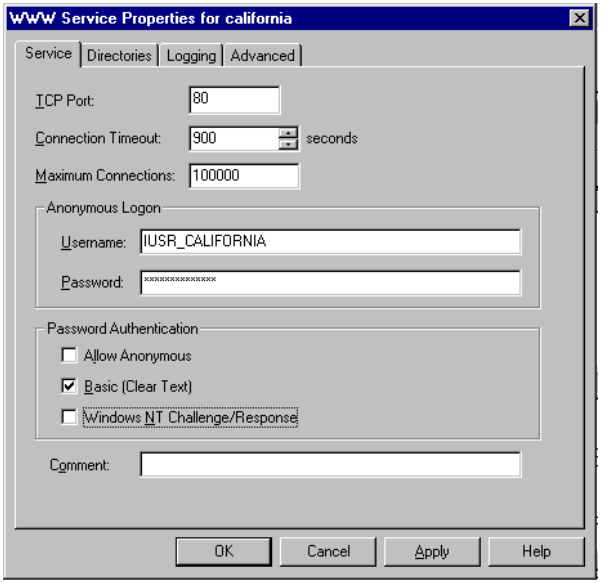


FIGURE 1-2. NT's WWW Service Properties window.

3. Go to the **Directories** page and click on **Add** to open the **Directory Properties** window.

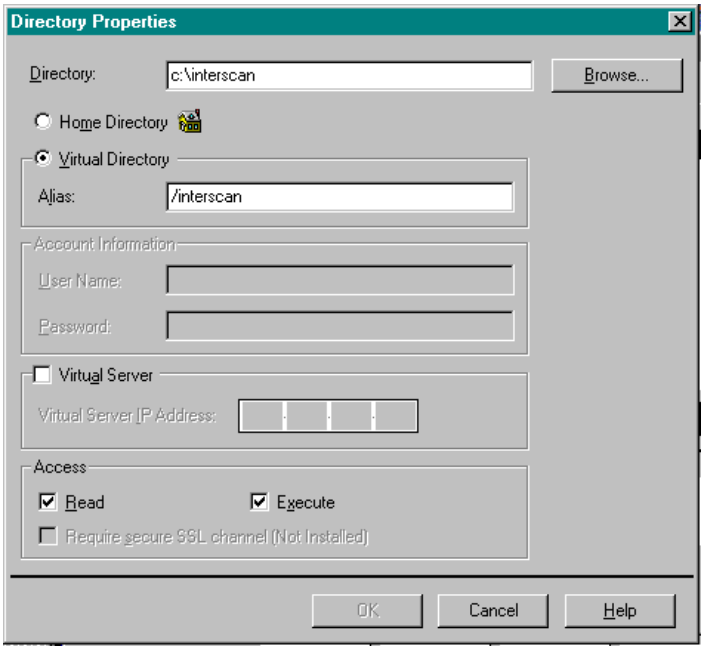


FIGURE 1-3. NT's Directory Properties window.

4. In the **Directory** field, type in the InterScan VirusWall path, typically `c:\interscan`.
5. Select the **Virtual Directory** radio button and, in the **Alias** field, type in `/InterScan`.
6. Under **Access**, select the **Execute** checkbox.
7. Click **OK** at the bottom of the page.

Setting up InterScan Security for Web Browsers

The System Administrator has the option of requiring that a Password and Username be entered in order to gain access to InterScan VirusWalls. To add this supplementary security requirement, follow the steps outlined below.

1. Go to the Microsoft Internet Service Manager and double-click on the **WWW** service listing—the **WWW Service Properties** window appears. (If the service is not running, choose **Yes** when prompted to start the service.)

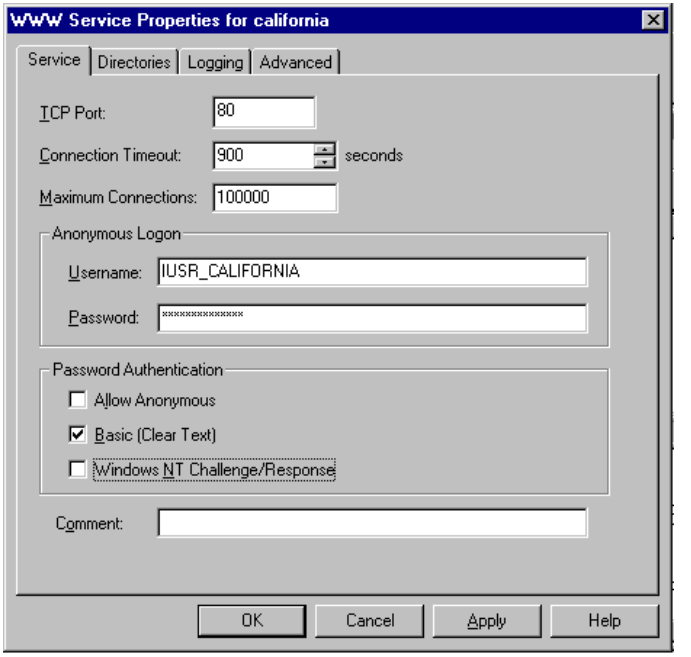


FIGURE 1-4. The Microsoft NT Server WWW service properties page, where Web browser security can be configured for InterScan.

2. Under **Password Authentication**, remove the check from **Allow Anonymous** if there is one.
3. Put a check in the box labeled **Basic (Clear Text)**.

4. Check **Windows NT Challenge/Response** if you want to enable this method.

   Note: Internet Explorer 3.0 users who are also using NT 4.0 should leave the Windows NT Challenge/Response in the Internet Server Manager unchecked, or install Service Pack 3 for NT from Microsoft.

5. Click **OK**.

Restricting File Access to a Single User

Unless the System Administrator specifically restricts access to the program subdirectory, any and all NT users (listed under the User Manager) can access the InterScan configuration. To ensure that program access is granted to only a single user, open **Explorer** and go to the directory containing InterScan.

Right-click it and go to Properties. Under the **Security** tab, select **Permissions**. Select the checkbox labeled **Replace Permissions on Subdirectories**. Next, click **Add** and choose the name of the user who will have access to the subdirectory.

Note: To access the Permissions feature, your hard drive must be in NTFS format.

Configuring Microsoft Exchange Server for Inbound and Outbound Scanning

If you are using the InterScan E-mail VirusWall to scan both inbound and outbound SMTP traffic, and if your SMTP server is Microsoft Exchange server 5.0, you need to make the following changes:

1. Configure Inbound Scanning

   To provide inbound scanning, E-mail VirusWall needs to be configured to forward all incoming mail to the Microsoft Exchange server Internet Mail Connector (IMC).

2. Configure Outbound Scanning

   To provide outbound scanning, Microsoft Exchange server IMC needs to be configured to forward outgoing mail to E-mail VirusWall (after E-mail VirusWall has been configured to scan outbound mail).

3. Configure the Exchange IMC

   Bring up the Microsoft Exchange Administrator window (NT **Start** button, then **Programs | Microsoft Exchange | Microsoft Exchange Administrator**).

   a. Under your domain name, click **Connections**, and then double- click **Internet Mail Service** for the machine Exchange server is installed on. The Internet Mail Service Properties page appears.

   b. Click the Connections tab to bring up that page and select **Inbound & Outbound**. Then click the **Forward all messages to host:** radio button and specify the IP address of the machine where InterScan is installed.

   c. Finally, click **OK** to save and apply your changes. Shut down and restart Exchange's Internet Mail Service for your changes to take effect.

Index

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z