



WHITE PAPER  
TREND MICRO™ INTERSCAN™  
MESSAGING SECURITY SUITE

JUNE 2002

TREND MICRO, INC.  
10101 N. DE ANZA BLVD.  
CUPERTINO, CA 95014  
T 800.228.5651 / 408.257.1500  
F 408.257.2003  
[WWW.TRENDMICRO.COM](http://WWW.TRENDMICRO.COM)

# Policy-based Antivirus and Content Security for the Messaging Gateway

## TABLE OF CONTENTS

3	Abstract
4	Threats to the Enterprise Messaging Environment
8	A Challenge for Information Technology Manager
9	An Effective Strategy Against Enterprise Security Threats
11	Viruses and Content Passing Through the Gateway
12	How InterScan Messaging Security Suite Works
17	InterScan Messaging Security Suite Architecture
20	Conclusion
20	About Trend Micro

June 2002  
Trend Micro, Inc.

©2002 by Trend Micro Incorporated. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of Trend Micro Incorporated. Trend Micro, the t-ball logo, AppletTrap, Control Manager, eManager, GateLock, InterScan, HouseCall, InterScan VirusWall, MacroTrap, NeaTSuite, OfficeScan, PC-cillin, PortalProtect, ScanMail, ScriptClean, ScriptTrap, ServerProtect, SmartScan, TMCM, Trend Micro Content Scanning Protocol, Trend Micro Control Manager, Trend Micro CSP, Trend Micro Damage Cleanup Server, Trend Micro Damage Cleanup Services, Trend Micro Outbreak Prevention Services, TrendLabs, Trend VCS, VirusWall, WebManager, WebProtect and WebTrap are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice.

## ABSTRACT

The increased usage and popularity of the Internet has influenced the development of the methods used to spread viruses. In the past, many computer viruses spread via floppy disks, but a new generation of email-borne viruses have emerged to threaten the corporate messaging system.

Nimda demonstrated just how vulnerable a large enterprise with high-speed networks is at the hands of a mixed-threat virus. During the Nimda outbreak, many enterprises were forced to shut down or disable all mail servers, both internal and external, to prevent users from opening infected email.

To overcome these problems, corporations need to employ a multi-layered approach to virus defense. An effective strategy should include integrated protection from the Internet gateway, groupware, file servers, and desktops. Relying on just one layer of virus defense, such as antivirus software on the desktop, is like designing a bank without a lock on the vault. However, even when antivirus software has been installed, it is not always updated and, in some instances, the software is has been disable by the users.

This white paper addresses the need to raise awareness of current threats to the corporate messaging environment and discusses a gateway antivirus strategy developed by Trend Micro —Trend Micro InterScan Messaging Security Suite.

## THREATS TO ENTERPRISE MESSAGING ENVIRONMENT

As corporations have begun to rely heavily on email for daily business operations, IT or email system administrators are often faced with the challenge of keeping the email system running 24x7. There are several threats that every administrator should be aware of:

**FACT:**

The 2001 ICSA Labs 7th Annual Virus Prevalence Survey indicated that 83% of respondents reported virus incidences caused by email attachments.

### Email-Borne Viruses

In 2000, ILoveYou caused \$2.6 billion dollars of damage worldwide, while SirCam was estimated to have done another \$2.6 billion damage worldwide. Denial-of-service (DoS) is just the beginning of problems associated with a virus outbreak. After virus pattern files become available, administrators often need to clean up infected mail storage systems, while dealing with endless calls to the help desk from panicking users.

There are several recent examples of fast spreading viruses which utilize Internet email. Most of these multiply exponentially by using the email address book of the infected computer to send copies of themselves to unsuspecting users. The amount of email generated then overwhelms the email system, thus creating a DoS attack.

**FACT:**

Based on a September 2001 study by Computer Economics, each outbreak incident results in a cost of between \$5K to \$500K per corporation.

A DoS attack is caused when someone attempts to flood an email system with enormous amounts of email resulting in the disruption of the SMTP gateways' ability to accept incoming or outgoing connections. This prevents employees from sending or receiving Internet email. As recent virus outbreaks have demonstrated, response speed is everything during a DoS attack. Mixed-threat viruses possess the ability to spread faster, requiring antivirus vendors to deliver a virus pattern file quickly to avert disaster.

Another form of DoS does not require viruses or malicious scripts to be involved. Email messages with an excessive number of attachments, attachments with excessive levels of compressions, or small compressed attachments that decompress to gigabytes of data, can absorb processing power on the SMTP gateways; resulting in the disruption of processing legitimate email.

### Malicious Email Content

Executable programs, Microsoft Office documents with macros, embedded visual basics scripts, and JavaScripts are all potential virus carriers. Malicious email usually includes these: virus-carrier executable programs (.EXE, .COM, .VXD), attachments with macros (.DOC, DO), Visual Basic Scripts (.VBS), Java, ActiveX, and/or HTML links, allowing this type of content to enter the email system.

### **Oversized and Non-Business Email**

Network and email system resources are already overburdened in every company. Transmission of non-business email with large attachments, such as pictures, games, video, music files, and spam consume valuable enterprise resources. Based on a recent study for Philip Morris, 5% of non-business related email generated 40% of data volume through their messaging system.

When an employee uses a company email account to transfer non-business related files, network bandwidth is reduced and everyone in the company suffers. Internet access is slowed to a crawl, and important business email intended for clients, partners, or vendors are caught in the queue waiting for delivery.

In addition, spam coming from the Internet also consumes network and email system resources. Spammers may attempt to flood the network with spam, but they may also attempt to leverage the SMTP server as an open relay to spam other organizations on the Internet. Relaying through the SMTP server hides the spammers identity.

### **Inappropriate Email Usage**

A corporate email network is the communications system that sustains daily business operation and, therefore, is an important company asset. Companies now find themselves in the position of being legally liable for individual employees' behaviors and misuse of email. The current trend among enterprises providing email access to employees is to define and publish an email usage policy; however, many IT managers do not have the tools to enforce such policies. This places business integrity at risk.

### **Employee Productivity**

Employee productivity is being threatened from numerous directions and one of the major threats is unsolicited electronic mail or spam. Already burdened by dozens of legitimate email messages daily, employees can find themselves inundated with everything from unsolicited advertisements for business products to chain letters and promotions for pyramid schemes.

Beyond simply being annoying, spam mail displaces normal email, wastes networking resources, and impairs productivity. Large amounts of spam consume the company's network storage, impacts an organization's resources to handle legitimate Internet email, and increases email system costs.

Furthermore, spammers pass email through corporate SMTP relays to stamp email messages with the corporations' Internet address - thereby making it appear if the company was the initiator of the message. This results in damage to corporate image and customer relations. Given the business critical nature of email services, a content security policy becomes an important issue for organizations to stop spam.

**FACT:**

Spam is an increasing irritation for Internet users and service providers, as well as for network system administrators. It is estimated that up to 30% of all email handled by major ISPs, such as AOL and Mindspring, consists of spam messages.

Another insidious threat to employee productivity is malicious software including viruses, trojans and malicious Java and ActiveX applets. Email and other Internet traffic such as FTP downloads can serve as carriers for damaging viruses and other malicious code capable of infecting entire networks and decreasing employee productivity.

New threats are emerging with potentially more far-reaching effects. Applets written in ActiveX and Java use a Web page as a host and can reach into any computer that connects to it. If ActiveX objects or Java applets exist on a Web page, they will be downloaded when a user accesses that page. Not yet in-the-wild, malicious code patterns using ActiveX and Java could cause a host of problems at the user's workstation. However, the advent of software allowing Web pages to be transferred via email already provides a powerful new transmission route for malicious applets. Theoretically, applets could access a recipient's email address book and send messages containing the attached Web pages to other recipients.

### Liability Exposure

Nearly as threatening to enterprise success as productivity losses is the liability exposure posed by employee access to email. For instance, liability for discrimination, racism, or libel could stem from statements made in employee email. In July 2000, Dow Chemical announced it had fired 50 employees and suspended 200 others without pay for sending or storing pornographic or violent email messages<sup>1</sup>. This action, hailed as "a serious crackdown," stemmed from a single complaint. There have been several lawsuits involving sexual harassment in the workplace, based on lewd comments sent by email. In many cases the organization has been held responsible for not controlling their email content so as to avoid offensive exposure to employees.

### Loss of Proprietary Information

Another potential threat is the transmission, either intentionally or inadvertently, of confidential or proprietary corporate information. Such information might range from financial or legal information on upcoming mergers or acquisitions to information on new products or marketing strategies. Inadvertent transmission of confidential materials is far more widespread than companies would admit. For instance, an employee involved in a high-level project attaches a file of needed information to an email and sends it to a supplier also involved in the project, but the file is accessible to other employees at the supplier's offices who lack proper authorization. The capability to screen outgoing email could help administrators identify and stop the loss of vital information in time. More subtle breaches in confidentiality may also be possible. Some analysts have speculated that information about high-level security projects could be gleaned from search patterns input while employees conduct research on the Web.

#### FACT:

October 1999, Edward D. Jones & Co, USA, took action against 25 employees after a member of staff complained about an email with offensive content.<sup>2</sup>

In 1999 a financial company was sued by a female employee who discovered a printout of a pornographic email on a department printer.

In 1995 Chevron Corp. paid \$2.2 million to a group of female employees to settle a suit which alleged they were sexually harassed through emails.

1. Gartner, August 2, 2000.

2. Newsbytes News Network, May 7, 1999.  
([www.newsbytes.com](http://www.newsbytes.com)).

### **Network Performance**

Large quantities of email, both legitimate email with large attachments and spam mail, can cause delays and bog down the enterprise network. Employees are increasingly using email to share large data files such as spreadsheets, graphics, reports, database updates, and sales presentations. As these attachments flow in and out of the network, bottlenecks can arise during peak work hours. Some system administrators attempt to avert this situation by imposing size parameters on email attachments. Attachments exceeding set parameters are returned to the sender who then attempts to resend the message - a source of frustration for the sender and the administrator. A more optimal strategy would involve using email management tools enabling administrators to shift email deliveries to off-peak hours, leveling the flow of messages, and easing network bottlenecks.

### **Controlling Costs**

Each of these threats compounds the effect on the enterprise's bottom line: Cost. While it is easy to see how the loss of worker productivity can end up costing tens of thousands of dollars in employees' salaries, this is only one impact. Liability exposure can result in substantial legal costs to represent the enterprise and in claim settlements. Floods of spam or a virus outbreak can impact both employee productivity and network performance. Even enterprise revenues may be at stake if lost proprietary information results in compromised market position or unsuccessful product launches. To maintain an enterprise's strategic advantage in today's competitive marketplace, these costs must be controlled.

### **Integrated Information Management**

The challenges of information and virus threat management are not irresolvable. There are applications available which provide filtering capabilities to block spam mail or monitor outgoing email. Other applications provide tools to maximize network performance. Antivirus software can scan incoming email and protect desktop computers from potential malicious code.

However, all these tools present their own challenge. Without integration, each application works against the other and the end result is they hamper network performance. The burden of maintaining and upgrading multiple separate applications adds to administrative overhead as well. Implementing numerous applications individually can also create compatibility problems. An integrated package can minimize the network impact while providing robust protection against multiple threats.

## **A CHALLENGE FOR INFORMATION TECHNOLOGY MANAGERS**

During any new virus attack, the challenge for IT managers is to minimize the impact on the network. As many antivirus vendors can testify, due to the nature and complexity of viruses, no one can guarantee to stop 100% of viruses. However, one thing an antivirus vendor can do is to provide the tools and strategy to help IT managers minimize the impact to corporate messaging server during a virus outbreak.

### **Concerns Raised by Most IT Managers during a Virus Outbreak**

#### **A need for rapid virus containment at the SMTP gateway**

A high percentage of these viruses should be stopped from entering the internal messaging system to minimize network and server downtime.

#### **Faster pattern file releases**

Before the pattern files are released and applied, the enterprise remains in danger of receiving a virus. IT managers need a solution as soon as possible to stop virus infection and return to business as usual.

#### **More accurate virus analysis data**

Time is wasted by IT staff members searching for information on new threats, because some antivirus vendors fail to provide updated, correct, or accurate information on new threats.

#### **Easy deployment**

Once an antivirus vendor provides the needed information, in large enterprise environment network-wide deployment can literally take hours. The damage to the company might already happen, especially for a mixed-threat virus or one with mass-mailing capabilities.

#### **More flexible policy management**

IT managers and xSP are often looking for a comprehensive solution providing a flexible antivirus and content security policy. Current products in the market do not provide xSP the flexibility to meet an IT administrators' needs.

## AN EFFECTIVE STRATEGY AGAINST ENTERPRISE SECURITY THREATS

3. IDC, 2001 — Antivirus Software:  
A segmentation of the market.

In 1996, Trend Micro introduced InterScan VirusWall, which now commands a 63% market share<sup>3</sup> of the world's Internet gateways antivirus protection. InterScan VirusWall scans for virus at the SMTP, HTTP, and FTP gateways in real-time.

InterScan Messaging Security Suite (InterScan MSS) is the next generation of Trend Micro's messaging gateway product, which is designed to address many IT's concerns and new threats to the corporate messaging environment. Originally, InterScan VirusWall included three protocols, SMTP, HTTP and FTP scanning. Due to the changes in market requirements, user buying behaviors, and political decision making in corporate environment, Trend Micro has made the conscious decision to separate the product into two specific areas, Messaging Security Suite and Web Security Suite. With these two strategies, Trend Micro provides the flexibility to deploy products to meet specific needs within the organization.

InterScan MSS is designed to be an integrated policy-based antivirus and content security strategy for the messaging gateway. It focuses on guarding the email gateway against viruses and malicious code. While helping to uphold business integrity, enforce email policies, and reduce spam.

InterScan MSS employs its own high-speed proxy technology to scan all relevant Internet traffic via SMTP and POP3 for viruses, content, and malicious code. By using its own proxy server, InterScan MSS is firewall independent.

The heart of an antivirus product is its virus scan engine. InterScan MSS utilizes Trend Micro's new Cheetah scan engine to deliver extraordinary scanning results. The Cheetah technology is up to 50% faster than competitive antivirus scan engines and can detect virtually all known and most unknown computer viruses. The Cheetah engine can scan 19 types of compressed files and can decode MIME, BinHex, and UUencoded files.

Trend Micro detects new macro viruses with its Trend Micro MacroTrap™ and SoftMice™ technologies that supplement traditional pattern matching techniques with sophisticated rule-based scanning. Using MacroTrap, macro commands embedded in many Microsoft Office files can be analyzed to determine whether the macro's execution would lead to a malicious behavior. If that is so, InterScan MSS can be set to eliminate the macro virus and the file will be cleaned and delivered. Virus scanning is achieved with minimal impact on network performance.

**FACT:**

TrendLabs' ISO 9002-certified global headquarters and five regional centers back Trend Micro products with timely, high-quality service. A team of more than 250 engineers operates around the clock to monitor virus activity, develop.

### **Best Protection Against Mass Mailing Virus**

InterScan MSS is designed to determine the nature of a virus within an email based on virus characteristics. If a virus is a mass mailer, InterScan MSS can be set to delete the infected email at the gateway to ensure internal mail systems and resources are not affected. If a virus is not a mass mailer, the email will be cleaned and then delivered to its destination.

### **Unprecedented Outbreak Prevention Service Framework**

With a new capability called Outbreak Prevention Service through Trend Micro Control Manager, InterScan MSS helps stop and quarantines new viruses before updated protection is available. InterScan MSS automatically retrieves content filtering instructions from TrendLabs to block email matching the general characteristics of the new virus carriers until a solution is found.

In the event of a new outbreak, virus researchers in TrendLabs create outbreak prevention policies to block email that resemble the new email-borne virus. Control Manager periodically checks for and automatically retrieves such policies as frequent as every fifteen minutes.

Once these policies are applied at the InterScan servers, a company's email systems are protected during the virus outbreak. This will allow Trend Micro and administrator time to release, and update the pattern file, respectively.

### **Policy-based Management**

InterScan MSS's Policy Manager provides flexible management tools that offer administrators the opportunity to enforce corporate email usage policies. The Policy Manager filters threats or inappropriate message content based on the filter result, or outcome, of the pre-set filter. Policy Manager supports seven filters: Virus Filter Group, Advanced Content Filter, Message Attachment Filter, General Content Filter, Message Size Filter, Disclaimer Manager, Anti-spam Filter.

### **Proactive System Availability Monitoring**

InterScan MSS has several built-in mechanisms designed for monitoring and alerting, so administrators can be notified when attention is needed. It is capable of performing system recovery countermeasures in the unlikely event that the mail flow is interrupted or service is terminated.

### **Anti-spam/Content Filtering**

InterScan eManager provides system administrators with tools to block spam, prevent the release of unauthorized information and manage the delivery of large email. eManager offers a spam filter and a content filter module.

eManager's spam filter uses both keyword scanning and lists of known spammers to block unsolicited bulk email. Trend Micro maintains an extensive list of known sources of spam. eManager automatically retrieves updated list, then deletes, quarantines, or archives the spam message at the Internet gateway. This helps eliminate the impact of unwanted email on employee productivity.

The content filtering rules can be tailored expressly for each unique corporate culture, such as quarantining the mail without delivery, deleting the email, or archiving the message while permitting delivery. Customized notifications to the senders, recipients or others can also be provided. Diligent monitoring of this type can effectively reduce the risk of liability due to industrial espionage, insider trading or unauthorized contacts with the press. eManager also includes the ability to scan within attachment like Microsoft Word, PowerPoint, Excel, and other text format document.

## VIRUSES AND CONTENT PASSING THROUGH THE GATEWAY

**FACT:**

Trend Micro was the first antivirus company to develop and market effective technology that detects and eliminates viruses and malicious content to and from the messaging gateway. This technology is owned and patented by Trend Micro.

The Simple Mail Transfer Protocol (SMTP) gateway is a specialized Mail Transfer Agent (MTA) designed to interpret and translate the internal addressing scheme to one acceptable to the Internet. The translation of the internal addressing scheme is done at the gateway MTA and, when it is set up correctly, it is completely transparent to end users.

In addition to translating the addresses from one format to another, the message content must be transmittable through SMTP. For example, X.400 messages could include non-ASCII content that cannot be sent over SMTP. When an outgoing message containing non-ASCII content arrives at the SMTP gateway, it must be converted to a MIME attachment. Once the message is converted, it can then be sent over the Internet via SMTP.

Many non-SMTP-based messaging systems use non-ASCII character sets. In order to facilitate the transport of message content over SMTP-based MTAs on the Internet, all SMTP gateways should use a common character set when converting content.

InterScan MSS performs real-time monitoring of incoming and outgoing email attachments and message body, with the intent of eliminating viruses from the corporate network and ensuring the integrity of the internal mail servers and application servers.

InterScan MSS also is designed to act as a SMTP gateway for the purpose of scanning SMTP traffic for viruses or inappropriate content. Internet email traffic is routed through InterScan MSS. When InterScan MSS first receives an email, it determines the scanning policy to apply to the email. Once the policy is identified by the sender/recipient route, the appropriate policy is applied.

Next, a message is broken down into its components. Each data component is analyzed according to policy. After analysis, viruses are cleaned and the parts are reassembled. For instance, if you receive an email message with a Microsoft Excel spreadsheet that has a Microsoft Word file embedded in it, InterScan MSS breaks down the document until all the data is in its basic state. This recursive disassembly of a message can occur up to 20 layers deep if necessary.

Finally, the message is classified. It means that the appropriate classification actions are applied to that message, whether it is delivery, quarantine, notification, archiving, or a number of other possible actions. InterScan MSS also gives organizations options to append legal disclaimers to email, automatically archive email messages and attach informational messages.

In addition to SMTP traffic, InterScan MSS is designed to scan POP3 messages, at the gateway, as they are retrieved by clients within the network. Even if an enterprise does not use POP3 email, it's probable that employees gain access their personal POP3 email accounts via mail clients installed on their workstations, thereby opening another virus entry point.

## HOW INTERSCAN MESSAGING SECURITY SUITE WORKS

InterScan MSS uses policies to help enforce an organization's email usage guidelines. Administrators have control over the level of antivirus and content management applied to members of an organization and different policies can be configured for different people.

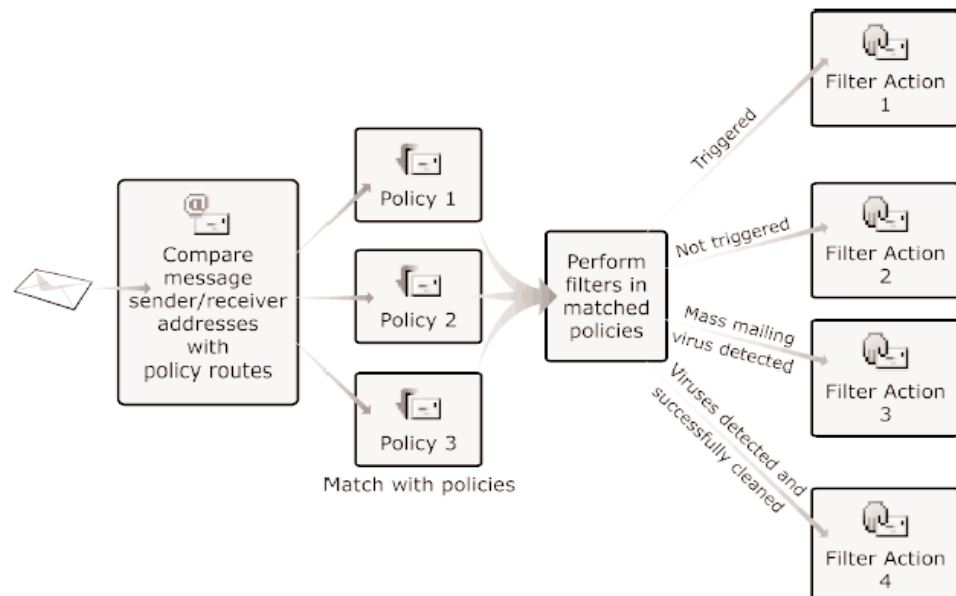


Figure 1.  
Simplified Policy Manager Process Flow

Organizations they have the tools to protect their network and business integrity by tailoring different policies for their employees. Policies simplify antivirus and content management configurations and make them easier to maintain.

**What is a Policy?**

A policy consists of:

- Which messages the policy applies to
- What message or attachment characteristics will be filtered, (e.g., viruses, keyword expressions, file types, etc.)
- What happens to messages that contain attributes that trigger the filter(s)

When a message is received by the InterScan MSS server, its sender and recipient addresses are analyzed to determine which policy will be applied. The filters configured for the chosen policy analyze the content and trigger a filter result. For each filter result, there is a corresponding filter action that dictates how the message will be processed, e.g., deliver, delete, quarantine, etc.

A policy is a set of email usage rules applied to members of the organization to enforce email usage standards. Administrators can use InterScan MSS's policies to filter and eliminate many of the security and productivity threats the messaging system faces. A policy has the following components:

- The Route : The set of sender and recipient email addresses to which the policy is applied. Address groups and wildcard expressions are normally used to simplify configuring the route.
- Filters : To check the message flow for viruses or prohibited content, InterScan MSS contains several pre-defined filters used to combat common virus and content threats. In addition, you can define your own filters using the intrinsic filters. The Antivirus Filter has several filter results, and each can perform a different filter action. Content management filters have two possible results-either the message content triggers the filter, or it does not trigger the filter.

With this new architecture, available from Trend Micro, InterScan MSS can be constructed to provide high-speed scanning, higher performance and scalable virus protection and content filter while ensuring the integrity of messages, attachments and its contents.

**Deploying into the Messaging Environment**

InterScan MSS also acts as an antivirus and content security SMTP gateway, which can be deployed into an existing SMTP messaging environment, on the DMZ zone, in front of the

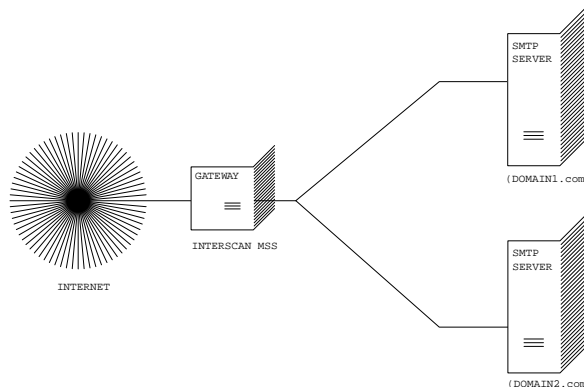


Figure 2.  
No Firewall

firewall, or behind the firewall. It provides full access control, which allows the administrator to restrict unauthorized connection and relays. InterScan MSS 's domain-based routing capability provides flexible message delivery via multiple smart hosts, or specific DNS servers.

Included here are several diagrams showing how flexible InterScan Messaging Security architecture is and the different ways how an organization can configure or install InterScan Messaging Security Suite on their gateway.

### No Firewall

Figure 2 shows one way of deploying InterScan MSS when the network without a firewall.

### Before the Firewall

Figure 3 shows the installation topology when you install InterScan MSS before the firewall:

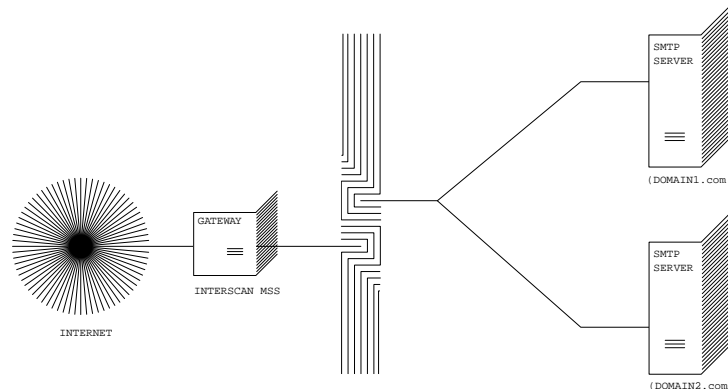


Figure 3.  
Before the Firewall

### Incoming Traffic

- InterScan MSS should be the first server to receive incoming email. Configure the MX records on the DNS servers that currently reference the SMTP gateway or firewall to reference the address of the InterScan MSS server(s).
- Configure the Relay Control settings to only allow relay for local domains.

### Outgoing Traffic

- If there is no firewall, configure SMTP gateways to route all outgoing email to InterScan MSS .
- If there is a firewall, configure the firewall (proxy-based) to route all outbound messages to InterScan MSS , so:
  - Outgoing SMTP email can only go to the InterScan MSS server(s).
  - Incoming SMTP email can only come from the InterScan MSS server(s).

- Configure InterScan MSS to allow internal SMTP gateways to relay, via InterScan MSS, to any domain.

### Behind the Firewall

Figure 4 shows how InterScan MSS can be used behind a firewall:

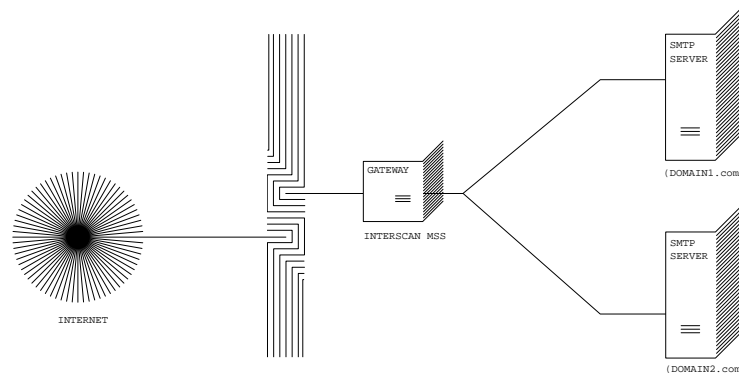


Figure 4.  
Behind a Firewall

### Incoming Traffic

- Configure the "proxy-based" firewall, so:
- Outgoing SMTP email can only go to the InterScan MSS server(s).
- Incoming SMTP email can only come from the InterScan MSS server(s).
- Configure the "packet-based" firewall. Change the MX records on the DNS server that currently reference the SMTP gateway to reference the address of the server hosting InterScan MSS .
- Configure InterScan MSS to route email destined to the local domain(s) to the SMTP gateway or the internal mail server (Exchange IMS).
- Configure relay restriction to only relay for local domain(s).

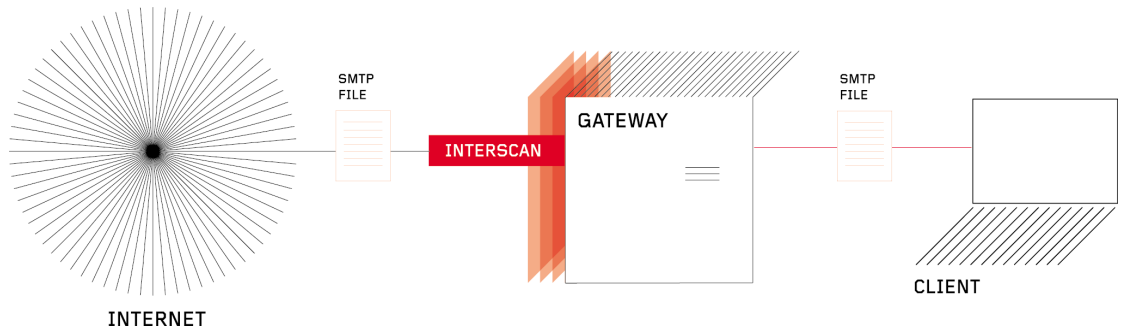
### Outgoing Traffic

- Configure all internal SMTP gateways to forward outgoing mail to the InterScan MSS server.
- If you're replacing the SMTP gateway with InterScan MSS, configure the internal mail server such as Exchange IMS to forward outgoing email to the InterScan MSS server.
- Configure InterScan MSS to route all outgoing email (those other than the local domains), to the firewall, or deliver via an external DNS server.
- Configure InterScan MSS to allow internal SMTP gateways to relay, via InterScan MSS, to any domain.

### On the Existing SMTP Gateway

Figure 5 shows how InterScan MSS can be installed on the same server that formerly hosted the SMTP gateway:

Figure 5.  
On Former SMTP Gateway



On the SMTP gateway:

- Allocate a new TCP/IP port for routing SMTP mail within the gateway. It must be a port that's not being used by any other services.
- Configure the existing SMTP gateway to bind to the newly-allocated port.
- This frees up port 25.
- Install InterScan MSS. It will bind to port 25.

Incoming Traffic

- Configure InterScan MSS to route incoming email to the SMTP gateway on localhost and the newly-allocated port.

Outgoing Traffic

- Configure the SMTP gateway to route outgoing email to InterScan MSS on local host (127.0.0.1) port 25.
- Configure InterScan MSS to route all outgoing email (those messages destined to other than the local domains), to the firewall, or deliver via an external DNS server.

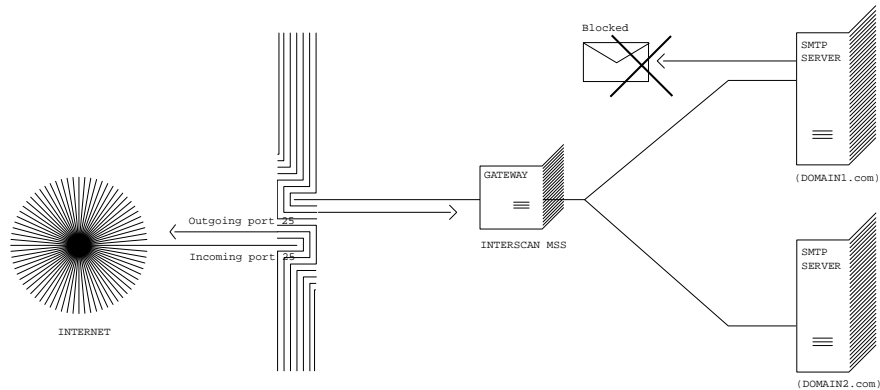
### In the DMZ

Figure 6 shows how InterScan MSS can be installed to the DMZ:

Incoming Traffic

- Configure the "proxy-based" firewall, so:
  - Outgoing SMTP email can only go to the InterScan MSS server(s).
  - Incoming SMTP email can only come from the InterScan MSS server(s)

Figure 6.  
Installation Scenario: In the DMZ



- Configure the "packet-based" firewall. Change the MX records on the DNS server that currently reference the SMTP gateway to reference the address of the server hosting InterScan MSS .
- Configure InterScan MSS to route email destined to the local domain(s) to the SMTP gateway or the internal mail server (i.e., Exchange IMS).

#### Outgoing Traffic

- Configure InterScan MSS to route all outgoing email (destined to other than the local domains), to the firewall, or deliver via an external DNS server.
- Configure all internal SMTP gateways to forward outgoing mail to the InterScan MSS server.
- Configure InterScan MSS to allow internal SMTP gateways to relay, via InterScan MSS, to any domain.

#### POP3 Scanning

The InterScan MSS POP3 scanner designed to act as a proxy, sitting between the mail clients and the POP3 servers, and scans messages as they are retrieved by clients.

In order for InterScan MSS to scan POP3 traffic, a firewall must be installed on the network and be configured to block POP3 requests from all the machines on the network, except for the InterScan MSS machine. This ensures that all POP3 traffic passes through it and secures the data flow.

Additionally, some configuration changes must be made to each mail clients retrieving messages through the InterScan MSS server. A utility called the POP3 Client Tool is provided to assist with making configurations changes on the Eudora, Microsoft Outlook/Outlook Express, Netscape Messenger, and Pegasus mail clients for non-authenticated connections. The POP3 Client Tool is packaged as an ActiveX control so that users can run it by visiting a Web page when using Microsoft Internet Explorer on a Windows platform.

## INTERSCAN MESSAGING SECURITY SUITE ARCHITECTURE

### Real-time Monitor

InterScan MSS provides a real-time inbound and outbound traffic scanning against virus, malware, malicious contents, and none-business related messages and attachments. In addition, InterScan constantly monitors messages and content passing through the SMTP gateway.

### Simple Remote Deployment and Management

InterScan MSS is the one of the first gateway antivirus products on the market that could be deployed and installed on single or multiple remote SMTP gateway servers across an enterprise. This saves network administrators time and makes it unnecessary to travel those geographically isolated server locations.

InterScan MSS's offers straightforward set-up procedures to facilitate a quick and easy installation across the entire enterprise gateway environment. InterScan prompts administrators through dialogue boxes to help ensure that the appropriate modules are selected to be installed and upgraded properly. Administrators are then free to set the default policy, configuration, actions and what notification messages, if any, will be sent to network administrators, sender, or recipient.

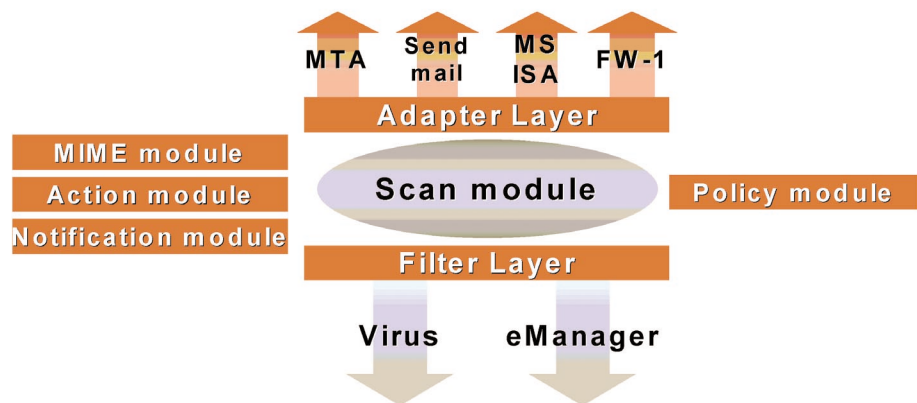


Figure 7.  
InterScan Messaging Security Suite  
Architecture

On each mail gateway installation server, InterScan MSS hosts a secured Web-based control and configuration console for that server. Hence, administrators can now quickly and easily update InterScan MSS across the entire enterprise by downloading the latest virus pattern and engine files from Trend Micro's ActiveUpdate servers.

Furthermore, InterScan MSS's Web-based management console enables network administrators to configure and manage InterScan throughout the enterprise via an Internet or intranet environment. Benefits of using a Web-based management console:

- Navigation and configuration can be completed across the Internet regardless of platforms or physical locations by using a Web browser (supports Microsoft Internet Explorer and Netscape Navigator)
- Update of new engine, virus pattern, and new patch files can be done remotely using a Web browser
- Secured data communications between local workstations and the InterScan server can be done by using SSL encryption
- Gives administrators tools to manage their antivirus products without physically being in the office or next to the messaging gateway server(s)
- Manages corporate policies, virus activities, and notification of all SMTP gateway servers regardless of where the administrator is
- Access to Trend Micro Control Manager which provides a total management of all Trend Micro products, including InterScan, thru the unique management console

#### **Handling Scan Engine, Pattern, and Scanning Policy**

InterScan MSS includes ActiveUpdate technology allowing administrators to easily update the scan engine, pattern, and scanning policies across the enterprise with the options of on-demand or at pre-scheduled update times. Pattern, engine, and scanning policies can be scheduled based on minutes, hourly, daily, week, or monthly configuration.

## CONCLUSION

Traditional desktop antivirus software alone cannot provide complete virus protection for the enterprise and it is unable to detect viruses embedded in email attachments insidemessaging servers. Desktop protection waits until users open attachments, leaving open the potential for infected files to be copied to the hard drive before scanning and cleaning is done.

Since traditional desktop antivirus applications cannot provide full protection for enterprise messaging environment and corporate network, enterprises must deploy email-specific scanning products, such as InterScan Messaging Security Suite, for more complete virus protection.

Trend Micro recommends the deployment of four tiers of virus protection. This proactive approach includes complete SMTP and POP3 scanning on the gateway, complete groupware virus protection on intranet email servers, complete file server protection on all application/file sharing servers to help ensure they are free of virus, and a desktop antivirus software solution at the user level.

Trend Micro's approach to virus control provides a complete desktop protection to aid in verifying files copied from floppy or local hard drives are scanned and cleaned. These four layers of protection help ensure the best virus protection in an organization.

## ABOUT TREND MICRO

Trend Micro provides centrally controlled server-based virus protection and content filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and service providers worldwide to stop viruses and other malicious code from a central point before they ever reach the desktop.

Trend Micro's corporate headquarters is located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters is located in Cupertino, CA. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and service providers. Evaluation copies of all of Trend Micro's products may be downloaded from its award-winning Web site, <http://www.trendmicro.com/>.