Content Vectoring Protocol with Checkpoint and Interscan Viruswall
Jeff A. McConnell
March 4, 2002

Introduction

The global marketplace drives advancements in technology that lead to expanding markets and service areas that may not have been possible prior to the internet generation which is currently in it's infancy. As with most any situation a business or individual for that matter must be prepared to take the good as well as the bad. Conducting business with a heavy reliance on computers and Internet connectivity presents many challenges to all levels of the organization. A central focus in this environment has become ensuring continuity of the business processes that rely on the tasks of employees' workstation applications, email, e-commerce web sites and other numerous data processing technologies in use today. These processes have come under fire in increasing numbers by a vast array of threats from viruses up to international cyber crime. Several of the more costly situations that American industry has faced in the past three years has been the presence of virus' inside corporate networks with the ability to spread quickly through the network infrastructure. Wouldn't it be nice to have something that monitors all the traffic that enters and exits through a network in real time every second of the day?

Fortunately this situation can be manageable with due diligence and common sense. TruSecure analyst Roger Thompson stated it best in a January 2002 article for ComputerWorld, "The bottom line of malware prevention remains the same: Filter, patch strategically and update your antivirus software. Use common sense to protect your network's vulnerabilities." Due to the current nature of business these tasks are often a broad and overwhelming task. There are several different ways that malware, malicious code or software often classified as a virus or worm, can enter a network. Becoming a more vital defense to this daily battle is managing content of inbound and outbound Internet traffic at the perimeter beyond the traditional firewall capabilities. Checkpoint Software originally developed specifications for the Content Vector Protocol to be integrated with its firewall product to function simultaneously with separate vendors' anti-virus servers. Version 3 of Checkpoint's firewall was the first CVP introduction into the marketplace and as security needs expanded the capabilities of the specification have as well. The CVP API (Application Program Interface) was published in November 1998 as an open specification and was well accepted by security industry leaders such as Symantec and Trend Micro. I would like to discern in this document that there are many steps to defending against malicious attacks, worms or viruses but one of the more prevalent targets recently that allow harmful attacks to spread so rapidly is the internet gateway. A CVP implementation can considerably reduce the risk of malicious content entry or exit to a network through an Internet connection. This technology, although relatively new, looks to have enormous benefit potential in several different applications and environments. I will cover the primary uses for CVP today in this discussion and hopefully spark new thinking in how to defend the barriers protecting your network and business.

Policy

Due to the severity level of recent hybrid worms, companies are taking notice of how damaging these threats are and taking steps to guard against future disruptive instances. Primary focus might be to increase awareness of users in your organization to the possible dangers that exist while only performing routine activities. A typical user ordering office supplies online isn't going to be able to determine if a Java applet is sending the contents of their clipboard to an undisclosed email address. Corporate policy can specify what is acceptable and unacceptable internet/computer use by employees, however, to tip the scales in favor of content security systems, malicious programs, viruses, etc. might enter a network even when industry best practices are in use. A portion of corporate policy that may not be covered in general would be the practices of the IT professionals and how the systems are to be handled. For example, who in an organization is responsible for reviewing logs, checking all pertinent security sites and publications on a daily basis for new threats and software updates? This is an all-inclusive plan where all dangers must be considered and followed. The roles that users and administrators play in network defense is key to continuity and the simplest of threats must be addressed. Removable media like floppies or CD's, laptops with unmonitored dial up connections or home broadband connections, and internet access that may or may not be utilized according to corporate guidelines still can be harmful if a user isn't careful. IT professionals must also be sure to patch and update systems to eliminate new vulnerabilities.

Even faced with these circumstances, we must not discount the importance of protecting all internet and malware entry points that a corporation might have since a large number of corporate networks are comprised of numerous locations, LANs, WAN, internet connections and mobile users. Any unprotected internet entry point can be a stepping stone to the next segment for a virus or worm – virus software with signatures unable to detect new virus will pass along attachments as they should through a corporate network or email system quite rapidly.

Policy will be mentioned a few more times with regards to CVP implementation mainly due to the dynamic environment in corporate America. Policies will assist a great deal in establishing rules and event handling for a Firewall/CVP implementation – employees' awareness of these guidelines can also improve network and business stability.

Defending the Gate

Besides external media brought into your infrastructure, the entry point that is most often unchecked is the Internet connection. The need for a firewall when conducting business on the internet in it's current state will not be covered here – it is assumed that your company has implemented at a minimum a packet filtering device or will be obtaining one in the near future.

Since the firewall is the traffic cop that blocks information flow or lets it through with some directional assistance based on rule sets, the OPSEC Content Vectoring Protocol is an effective way to increase the capabilities and value of the firewall itself. Traffic that arrives at a firewall typically is compared to a rule set that either allows the traffic for predefined routes, rejects it, or just drops the packet entirely. This can be effective when everything is clear-cut in terms of access privileges given to your internal staff or the public outside your network. Where a large number of incidents occur is where these definitive rules of acceptable use for Internet activity expose vulnerabilities and weaknesses in defenses.

OPSEC CVP

OPSEC or Open Platform for Security gives you the ability to manage a complete network through an open structure that allows third party applications written for security purposes to fit into the infrastructure through available API's (application programming interfaces) or scripting languages. Having all components integrated into the OPSEC structure will allow management and configuration of all aspects can be done from a central policy editor. OPSEC allows different components to be installed on different machines to eliminate compatibility issues among vendors as well as provide distributed processing but requires each piece to be aware of the others. A modular approach to securing a network is preferable because you can choose what platform or software best fits your environment plus adds the flexibility of upgrading single components without affecting others.

The newest generation of CVP incorporates a CVP Manager application packaged with VPN-1 and FireWall-1. CVP Manager can be setup to link several content validation servers to scan the same file multiple times. The ability to use separate servers provides simple load sharing of traffic to multiple validation servers, allowing scalability as well as fail over inspection servers. This can also come into play when a specific CVP server vendor has features another does not. For example, you prefer to use a Symantec product for antivirus scanning and a Trend Micro product for real time HTTP or FTP traffic monitoring, you could utilize both products.

A great benefit for most of us on the defensive side of this ongoing battle is that content vectoring protocol was developed with intentions to allow a number of firewalls or packet routing devices to use a common validation server. This ability will become more meaningful as the Internet matures and the threats being faced each day continue their dramatic increase. For the 3rd year in a row the number of reported security incidents as well as reported vulnerabilities has doubled. This pace is quite alarming and most IT professionals have already begun seeing the need to focus more on security issues with their computer and network systems to the point where it has become a scrutinized budgeted cost of doing business.

CVP Client Server Relationship

The OPSEC environment employs a standard client and server relationship where the client locates the server as well as initiates the connection to the server. The CVP client makes connections to the CPV server based on rules defined in the security policy. The client can connect and send traffic in a data stream in one of the following three methods:

- Authenticated Connection using Secure Sockets Layer – does not encrypt data
- Checkpoint Proprietary Authentication – uses Checkpoint authentication algorithm
- Clear Text – authentication and data pass in clear text

**The API does not currently support encrypted connections

The CVP client collects traffic from a data stream in a buffer so that it can "look ahead" and be manipulating the traffic prior to receiving the entire stream. The client will then send a portion of the data to the CVP server for inspection along with an event handler specifying the number of bytes sent. The CVP Server will analyze the data stream according to the type and role of the server. An antivirus server will inspect entire files against a known list of viruses or a certificate validation server will check the validity of certificates in HTTP traffic. At this point the CVP server has control over what the original destination will receive and delegates this responsibility to the client to carry out one of three tasks.

- Send data from the buffer to the CVP server for inspection
- Send data from the buffer to the destination – this will occur when content inspection deems the traffic acceptable
- Send data from CVP server to destination – events causing the data to be changed could be virus or http control removal

The data stream itself however is not the only information being transmitted between client and server.

CVP Clients communicate:

- Connection information - source IP and destination port
- Data information – file type or protocol ID
- Expected Server Actions – replace or modify harmful file content

CVP Servers communicate:

- Impression of original data stream's safety (safe, unsafe, unreadable)
- Impression of validated data stream's safety (safe or unsafe)
- Actions, if any, taken to secure data (data rejected, removed, modified to cure a virus)

Content Vector Server's conclusion about data streams has a different application for each role the CVP server can fill. An antivirus server will react differently than an authentication server would.

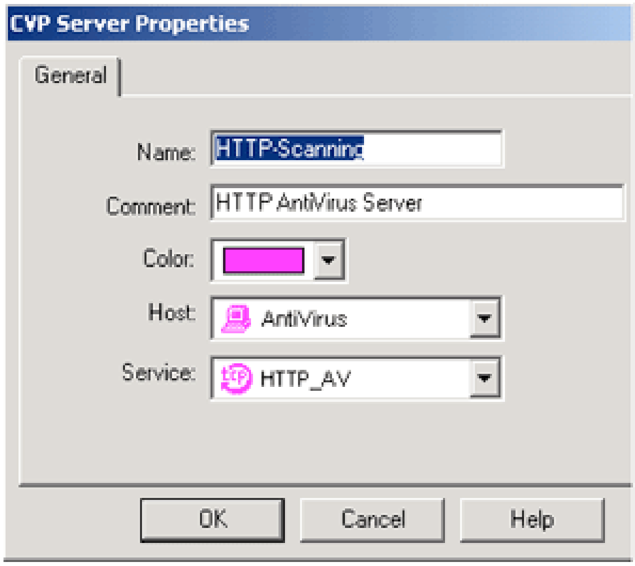
CVP Configuration

Getting CVP setup can be a complex setup depending on your organizational needs however for a single internet entry point, the evolution of the OPSEC environment as a whole has streamlined this process amongst different vendors. Without going into much detail about what and where to purchase your software, let's assume we will be using a Checkpoint Firewall-1 server with a Trend Micro Viruswall CVP server.

Client Setup

The CVP client in this case will be the Checkpoint Firewall which has this software feature built into the base product. The firewall will have a Security Policy made up of representative objects and rule sets that are applied in a top to bottom – per packet analysis.

First let's define what our CVP host will be through an object in the rule base which will simply be a descriptive name, an IP address, and any special routing instructions if necessary. If your setup will have more than one content validation server then those host objects will need to be created as well. In order to utilize the abilities of OPSEC CVP implementation we must specify what particular CVP services will be associated with each service. In the simplest case all CVP services (FTP, HTTP, SMTP) will be associated with a single CVP server but the option to define more is available to the client if you need HTTP scanning done on a different platform for example. The Checkpoint object that represents a particular CVP Server type is depicted below:


CVP Server Properties

General

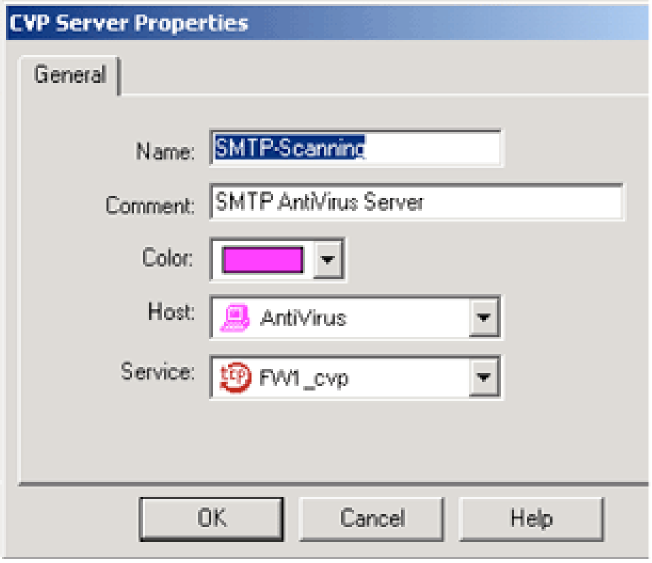
Name: HTTP-Scanning

Comment: HTTP AntiVirus Server

Color: 🟪

Host: AntiVirus

Service: HTTP_AV


CVP Server Properties

General

Name: SMTP-Scanning

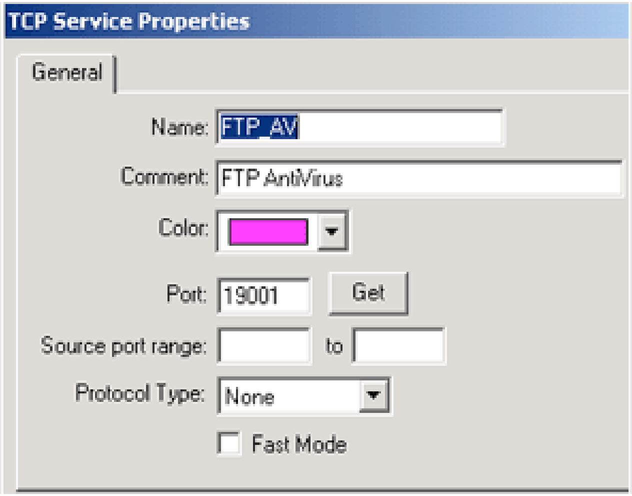
Comment: SMTP AntiVirus Server

Color: 🟪

Host: AntiVirus

Service: FW1_cvp

The properties of the CVP servers can be changed to send HTTP to a different validation host than SMTP traffic as well as define a separate service. The service parameters referenced above are predefined services in the firewall (CVP Client) that allow the client to manipulate traffic in the rule base at a more granular level. For example, the CPV and FTP antivirus services are defined as a TCP service represented by an object in the Firewall-1 GUI that has some basic definable parameters:


TCP Service Properties

General

Name: FTP_AV

Comment: FTP AntiVirus

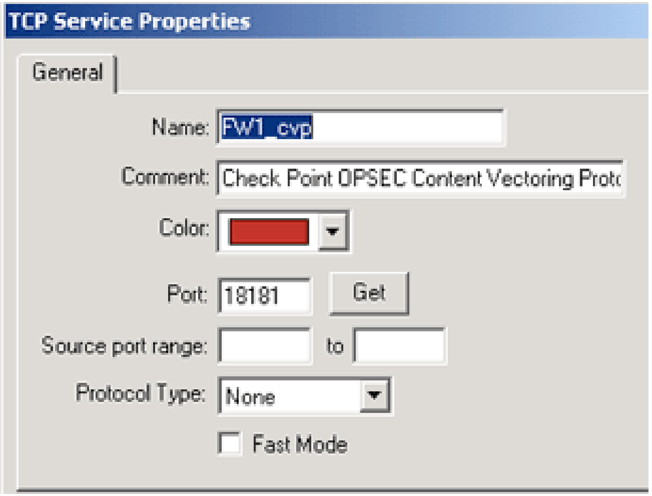
Color: 🟪

Port: 19001

Source port range: to

Protocol Type: None

☐ Fast Mode


TCP Service Properties

General

Name: FW1_cvp

Comment: Check Point OPSEC Content Vectoring Proto

Color: 🟥

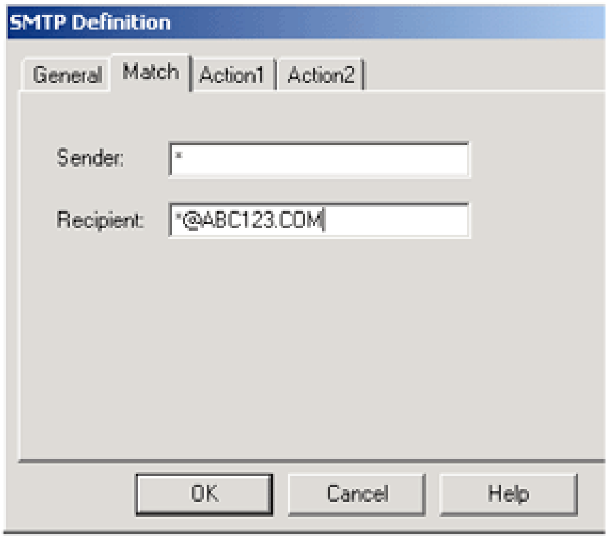
Port: 18181

Source port range: to

Protocol Type: None

☐ Fast Mode

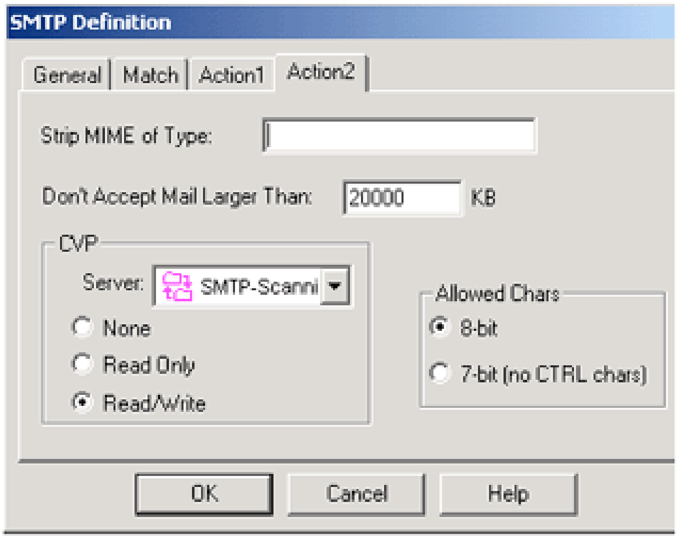
This tells us how the client will communicate with the CVP server. When the CVP client must utilize the server for data stream inspection it will pass along the necessary information so that the CVP server can take the proper course of action.


SMTP Definition

General | Match | Action1 | Action2

Sender: *

Recipient: *@ABC123.COM


SMTP Definition

General | Match | Action1 | Action2

Strip MIME of Type:

Don't Accept Mail Larger Than: 20000 KB

CVP

Server: SMTP-Scanni

○ None

○ Read Only

● Read/Write

Allowed Chars

● 8-bit

○ 7-bit (no CTRL chars)

Above are some properties variables that apply to the CVP client's communication with the CVP server on how to handle the data it sends for inspection. In the left hand capture, we are specifying the characteristics a data stream has to possess or match before redirection to the CVP server will take place. In this example, any Sender (*) trying to send SMTP mail to any (*) recipient @ the ABC123.COM domain will be sent to for content validation. The right hand capture adds action parameters such that only files under 20 megabytes will be allowed and that the CVP server is expected to modify (Read/Write) files. The ability to Read and Write would be necessary for the server to be able to clean viruses from email attachments. Now we know what the client is expecting the CVP server to do, the traffic must have a method for getting to the CVP server carrying those instructions.

A standard method for routing IP traffic to the proper destination is used when the CVP client needs to have data validated. Typical rule sets or access lists involve usually 4 items: a source, destination, service/protocol, and action taken if encountered.

Source	Destination	Service	Action

Internet SMTP Hosts Internal SMTP Mail Server Scanned SMTP Service Accept

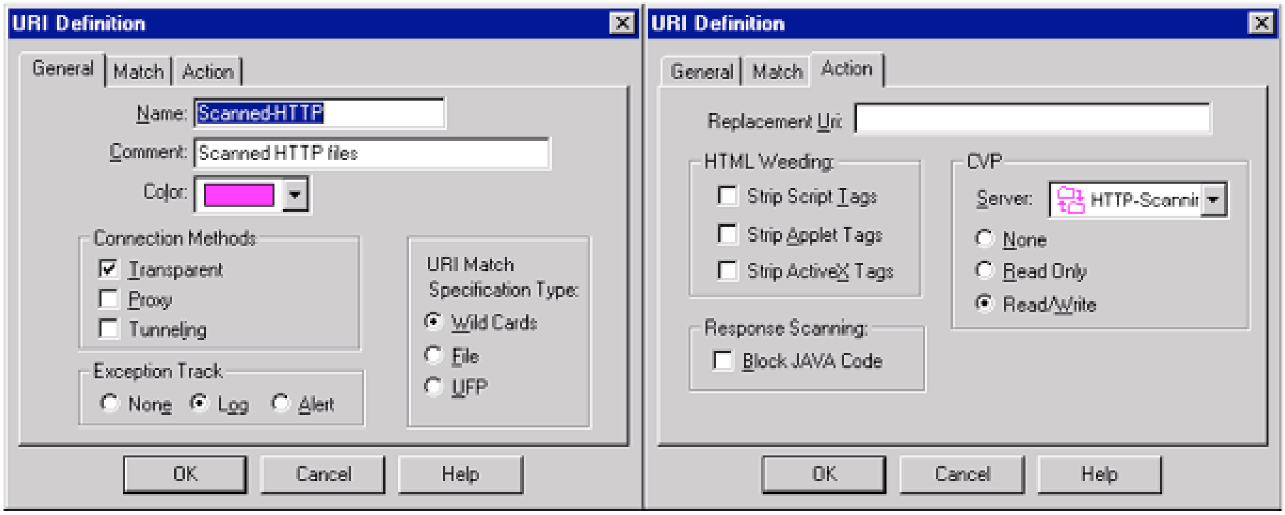
This rule simply states that any Internet SMTP relay host can send traffic to your internal email server through port 25 and it will be accepted. However, the role of the CVP client is important to note because it is acting as an integral part of the Scanned SMTP Service in this case. Any SMTP traffic destined for your internal email server is to be buffered by the CVP client and delivered to the CVP server for inspection before the final destination receives it.

Source	Destination	Service	Action

Internal SMTP Mail Server Internet SMTP Hosts Scanned SMTP Service Accept

A similar rule should applied to outgoing mail as well since you certainly don't want to risk sending viruses to clients.

Scanning web or HTTP traffic also has parameters to take into consideration – captures of the CVP Client resources for Hypertext Transfer Protocol show some parameters that the client will communicate to the CVP server. In the case of HTTP, the CVP client will ensure content validation based on what is defined in the URI or Uniform Resource Identifier.



Name: Scanned-HTTP
Comment: Scanned HTTP files
Color: 🟪

Connection Methods
☑ Transparent
□ Proxy
□ Tunneling

Exception Track
○ None ● Log ○ Alert

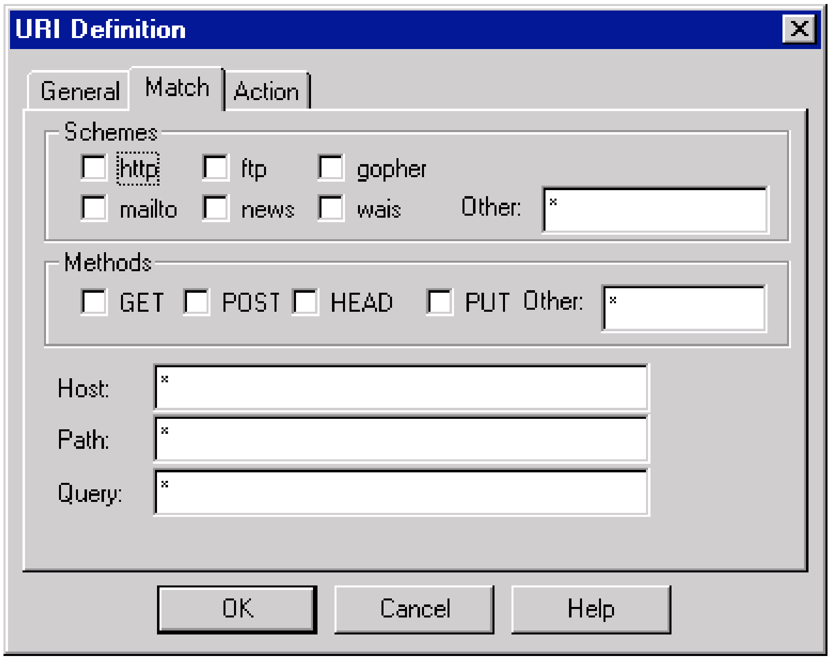
URI Match Specification Type:
● Wild Cards
○ File
○ UFP

Replacement Uri:

HTML Weeding
□ Strip Script Tags
□ Strip Applet Tags
□ Strip ActiveX Tags

Response Scanning:
□ Block JAVA Code

CVP
Server: HTTP-Scannir
○ None
○ Read Only
● Read/Write



Schemes

□ http □ ftp □ gopher

□ mailto □ news □ wais Other: *

Methods

□ GET □ POST □ HEAD □ PUT Other: *

Host: *

Path: *

Query: *

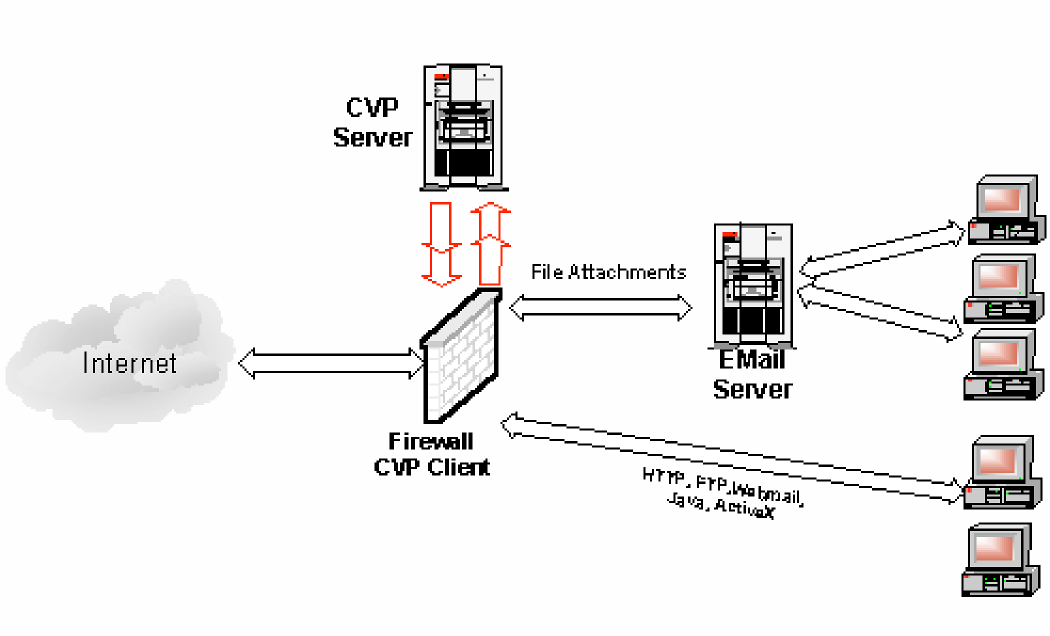
URI resources can define schemes or protocols such as HTTP, FTP, GOPHER etc., methods or commands (GET, POST), individual hosts (for example, "*.com", "*.net"), paths and queries. The settings for HTTP traffic to be inspected are for all schemes, methods, and hosts with the ability to modify (Read/Write) traffic with logging only unsafe exceptions. When scanning HTTP, a few more configurable parameters are available to security administrators like JAVA applets not being allowed even on resources that are allowed. JAVA applets, JAVA scripts and ActiveX can be removed from HTML altogether from the through the client configuration.

URL Filtering is another mainstream function for a CVP client that integrates well with Firewall-1 and the CVP specification. URL filtering gives companies the capability to monitor, manage and report traffic traveling from their internal network to the Internet. The client would send the traffic to the CVP server where it would be compared against a list of predefined URL's that are classified as either accessible or not for example. This technology and features can be found in other products however it is not present in the product being discussed from Trend Micro.

CVP Servers

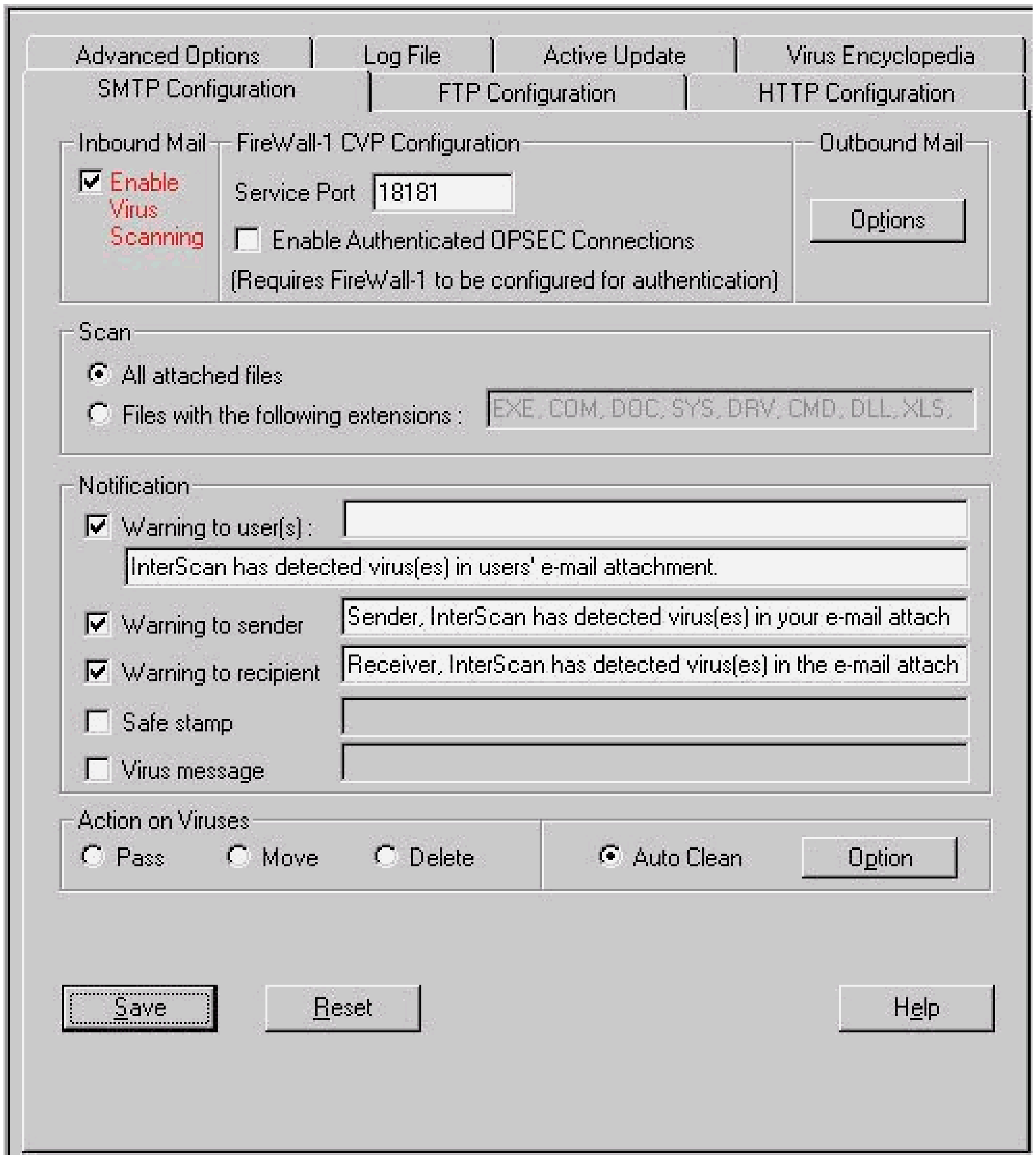
Hopefully a clear definition of what role a CVP client plays in the inspection process has been defined at this point. Since the client's responsibilities include getting the traffic over to the inspection server with the proper parameters and necessary information, determining how the CVP server will manipulate the traffic would be the next setup requirement. This discussion will be referencing Trend Micro's VirusWall server, which was one of the earlier products that integrated seamlessly with Checkpoint's Firewall-1. Viruswall is able to scan files that travel to and from the Internet in real time or pass through mode so that the process is transparent to users as to not be a disruptive feature. The product detects viruses by pattern matching key areas of suspect files to strings of virus code and compared against a database of known virus patterns. The software also has the ability to recognize over twenty types of compression formats. Files that are compressed are opened and examined for viruses – even if a compressed file contains more compressed files inside it, Viruswall will decompress the embedded files recursively up to twenty times until all files have been scanned.

A CVP server would normally be placed in a strategic section of a network so that it doesn't have any interaction with many other hosts or portions of the network you're protecting. Logically speaking it's a good idea to isolate a server whose intended purpose is to accept and process often malicious traffic. Most implementations locate the CVP server in a DMZ or Demilitarized Zone. A DMZ will usually be located between the Internet and the private network that is being protected most often by a firewall. The firewall or packet filtering device will direct specific traffic to the host in the DMZ for processing. More common implementations housed by a DMZ would be web, ftp, or mail servers that have to be publicly accessible but at the same time somewhat protected. In this case, the CVP server won't be publicly accessible but for purposes of protecting the internal network should be located in a DMZ controlled by the firewall. The firewall would need to be setup to allow traffic from the Internet or internal network to be redirected to the CVP server for inspection prior to entry or exit. We will assume this has been configured properly.



Trend Micro’s VirusWall is a CVP aware application that integrates with Firewall-1 through Checkpoint’s CVP API. Once the CVP client setup has been completed, Viruswall can be operational fairly quickly. After software installation, the necessary configuration modifications and setup parameters need to be defined so that client and server can exchange data streams for analysis.

SMTP configuration parameters are represented below – some options listed here should mirror the CVP client setup such as port number 18181 that the server will listen on will be the same that the client will communicate on.



Inbound Mail
☑ Enable Virus Scanning

FireWall-1 CVP Configuration
Service Port 18181
□ Enable Authenticated OPSEC Connections
(Requires FireWall-1 to be configured for authentication)

Outbound Mail

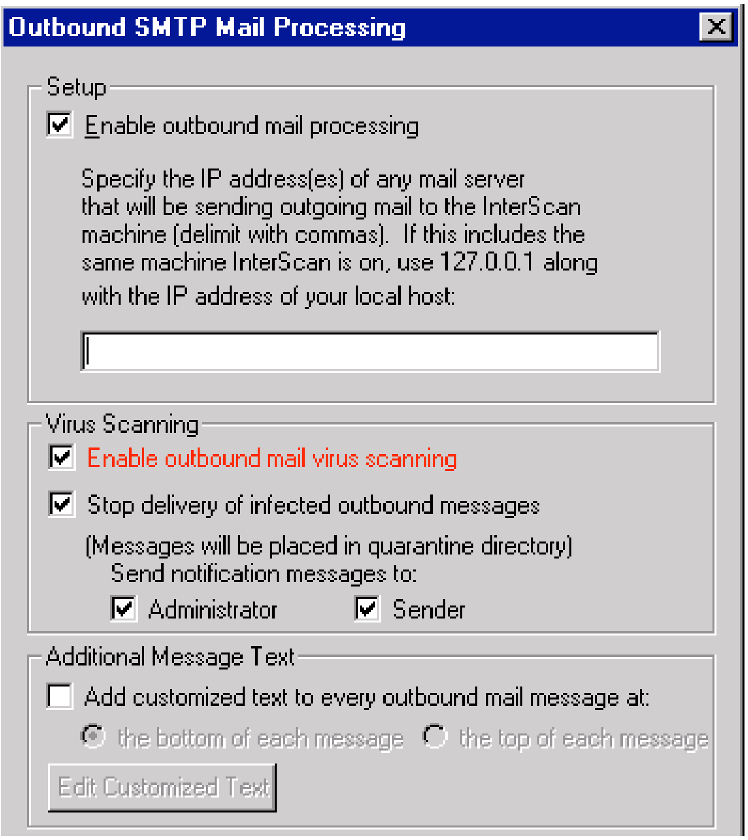
Scan
● All attached files
○ Files with the following extensions : EXE, COM, DOC, SYS, DRV, CMD, DLL, XLS,

Notification
☑ Warning to user(s) :
InterScan has detected virus(es) in users' e-mail attachment.
☑ Warning to sender Sender, InterScan has detected virus(es) in your e-mail attach
☑ Warning to recipient Receiver, InterScan has detected virus(es) in the e-mail attach
□ Safe stamp
□ Virus message

Action on Viruses
○ Pass ○ Move ○ Delete ● Auto Clean

Other options not defined by the client are essential for proper operation. The option to enable virus scanning for inbound mail must be checked plus a definition of what to scan needs to be configured. In most cases scanning all files is recommended but depending on what policies are in place for the organization, these settings can be modified to suit your needs. Outbound mail scanning might be an essential part of your defensive strategy as well – enabling this option is configurable also.

option is configurable also.


Outbound SMTP Mail Processing

Setup

☑ Enable outbound mail processing

Specify the IP address(es) of any mail server that will be sending outgoing mail to the InterScan machine (delimit with commas). If this includes the same machine InterScan is on, use 127.0.0.1 along with the IP address of your local host:

Virus Scanning

☑ Enable outbound mail virus scanning

☑ Stop delivery of infected outbound messages

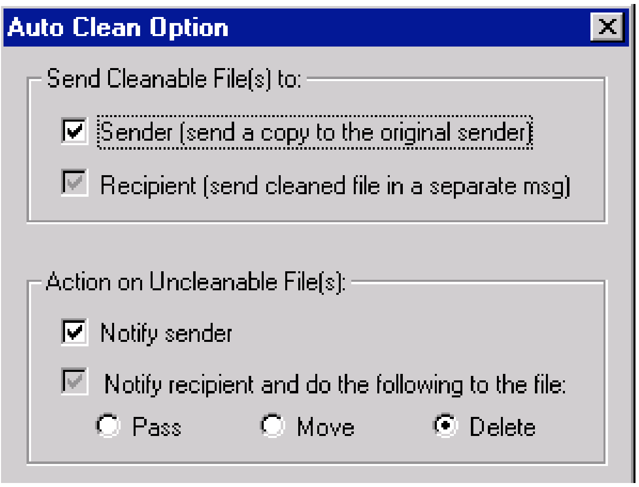
(Messages will be placed in quarantine directory)
Send notification messages to:
☑ Administrator ☑ Sender

Additional Message Text

□ Add customized text to every outbound mail message at:
● the bottom of each message ○ the top of each message

This configuration menu is accessible from the SMTP folder tab under the Outbound Mail Option button. Scanning outbound mail from an internal mail server can be setup by specifying its IP address – make sure the firewall is setup to pass SMTP (Port 25) the host and DMZ where the CVP server is located. Delivery of infected messages can be stopped and/or quarantined and a notification that can be added on each outbound message stating something along the lines that it has been scanned for viruses prior to delivery.

One of the actions we defined on the CVP client is when it sends data streams over to the CVP server it expects the CVP server to clean viruses if possible. This screen allows us to tell the server to follow the instructions of the client and clean the files if possible and to delete virus files that cannot be cleaned but to notify sender and recipient of the action that was taken.


Auto Clean Option

Send Cleanable File(s) to:

☑ Sender (send a copy to the original sender)

☑ Recipient (send cleaned file in a separate msg)

Action on Uncleanable File(s):

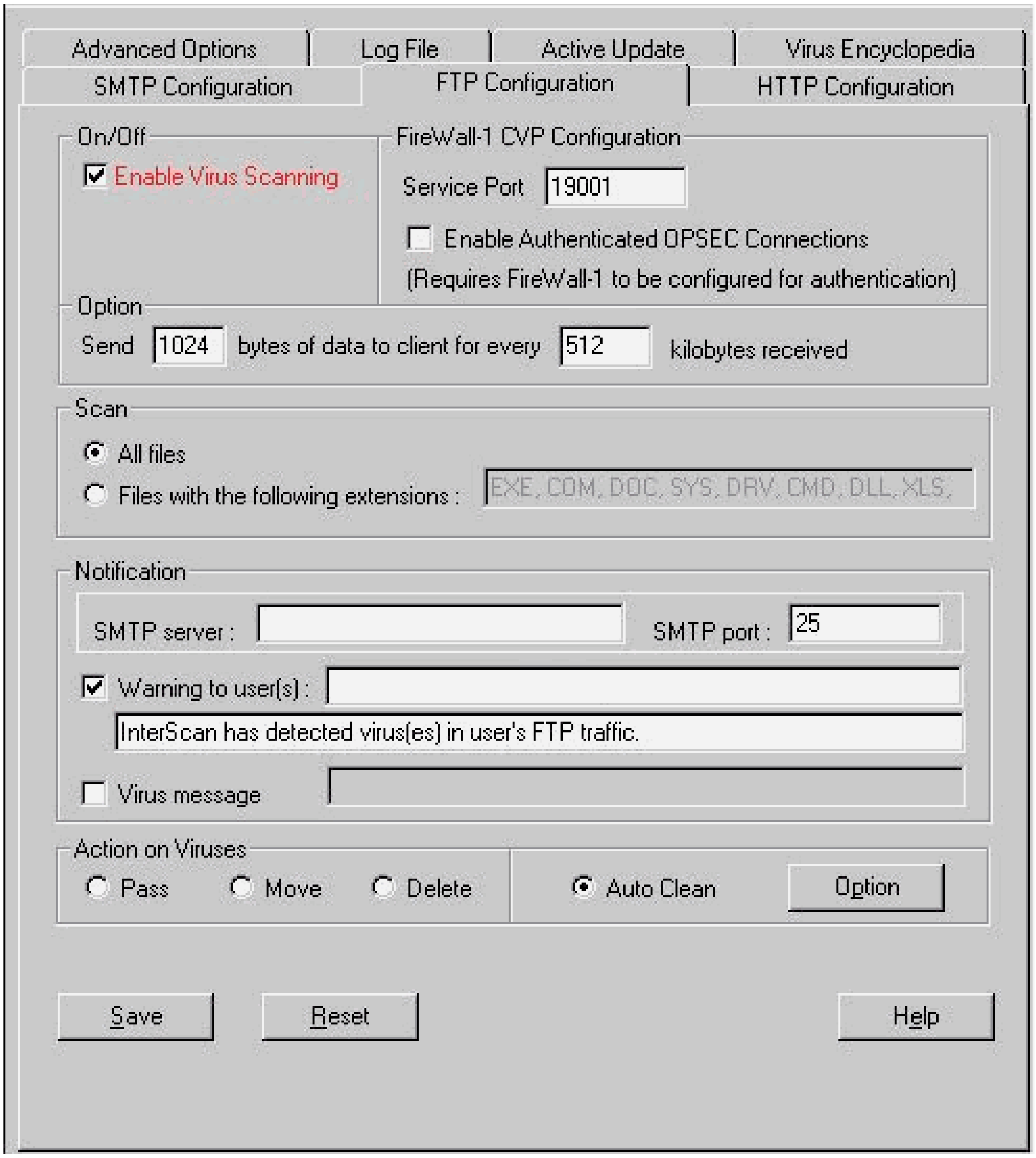
☑ Notify sender

☑ Notify recipient and do the following to the file:

○ Pass ○ Move ● Delete

Even though you may have antivirus software on every link in the delivery chain within your network, an administrator can ensure that no new viruses are getting in despite how often the individual workstations are being updated. Updating all workstations and servers as often as necessary can become too challenging.

VirusWall software is also capable of detecting viruses not only in email but in file downloads as well. HTTP and FTP are two industry standard methods of delivering files to users or clients over the Internet.



On/Off

☑ Enable Virus Scanning

FireWall-1 CVP Configuration

Service Port 19001

□ Enable Authenticated OPSEC Connections

(Requires FireWall-1 to be configured for authentication)

Option

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

Scan

● All files

○ Files with the following extensions : EXE, COM, DOC, SYS, DRV, CMD, DLL, XLS,

Notification

SMTP server :

SMTP port : 25

☑ Warning to user(s) :

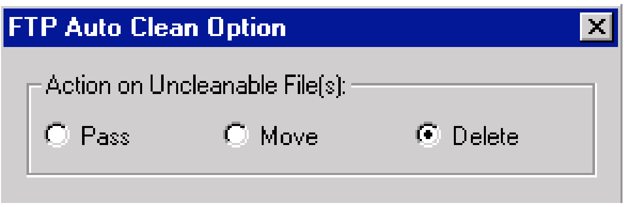
InterScan has detected virus(es) in user's FTP traffic.

□ Virus message

Action on Viruses

○ Pass ○ Move ○ Delete ● Auto Clean

FTP virus scanning configuration is a straightforward setup where we are enabling virus scanning and specifying the port 19001 that the server will listen for communication from the client on. We would want to scan all files again and input who and where a notification will be sent to if a virus is found. The Auto Clean Option again will let us specify what to do when a file beyond repair is encountered.

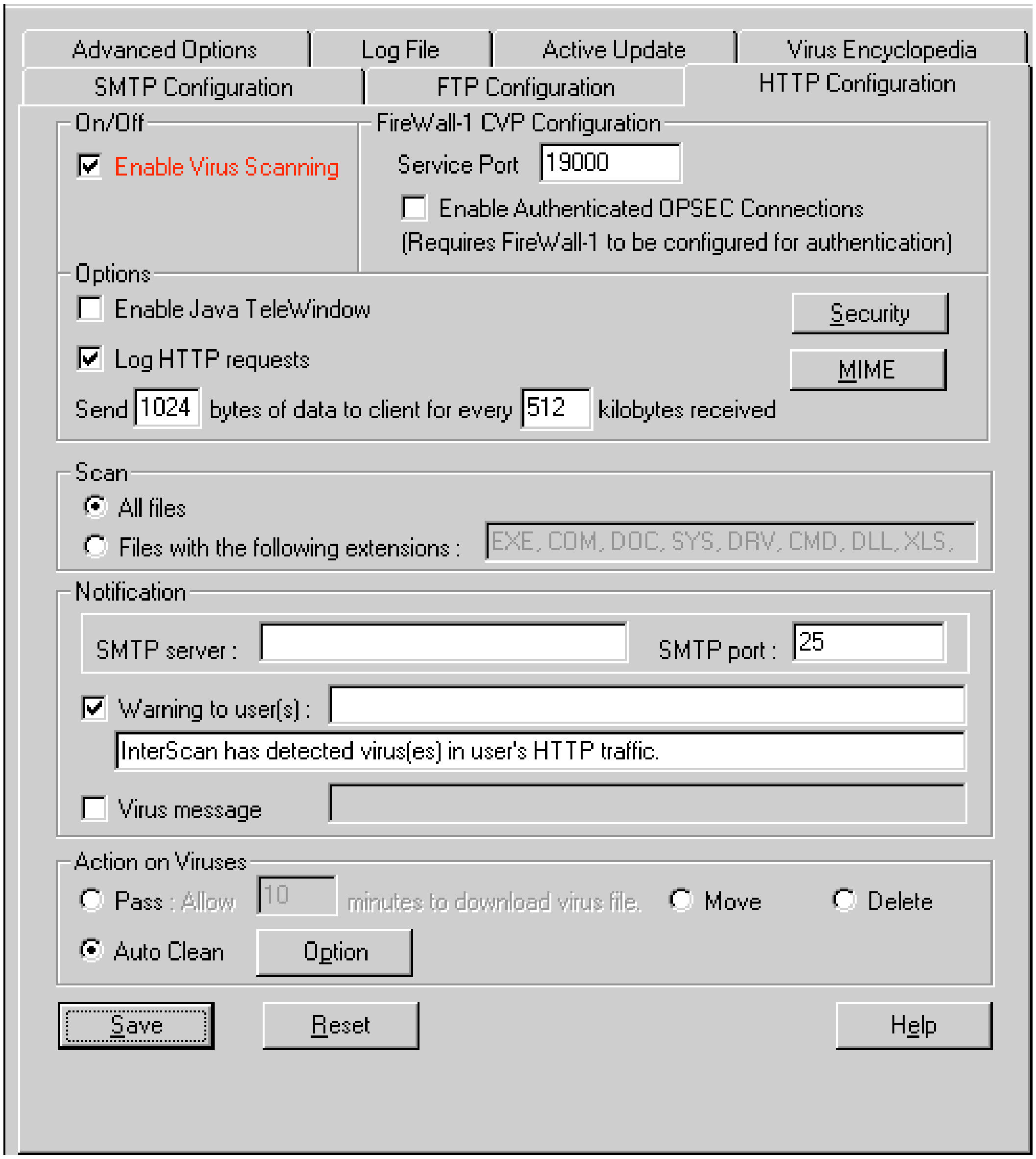


FTP Auto Clean Option

Action on Uncleanable File(s):

○ Pass ○ Move ● Delete

HTTP scanning options are almost identical except for some optional settings for data unique to HTTP. The standard Enable check box, listening port specification of 19000, scanning of all downloaded files, and event notification options are common between HTTP and FTP. Some additional options for configuring actions for Java and MIME encoding are present on this page. If expected actions are configured on the CVP client for Java or Active-X removal for example, the options should be reflected in the server setup as well.



Advanced Options | Log File | Active Update | Virus Encyclopedia
SMTP Configuration | FTP Configuration | HTTP Configuration

On/Off
☑ Enable Virus Scanning

FireWall-1 CVP Configuration
Service Port: 19000
□ Enable Authenticated OPSEC Connections
(Requires FireWall-1 to be configured for authentication)

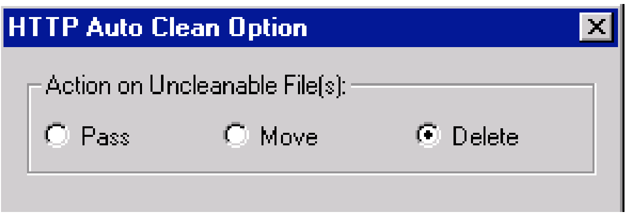
Options
□ Enable Java TeleWindow
☑ Log HTTP requests
Send 1024 bytes of data to client for every 512 kilobytes received

Scan
● All files
○ Files with the following extensions : EXE, COM, DOC, SYS, DRV, CMD, DLL, XLS,

Notification
SMTP server :
SMTP port : 25
☑ Warning to user(s) :
InterScan has detected virus(es) in user's HTTP traffic.
□ Virus message

Action on Viruses
○ Pass : Allow 10 minutes to download virus file.   ○ Move   ○ Delete
● Auto Clean

Auto Clean Options remain similar across the two protocols as well:

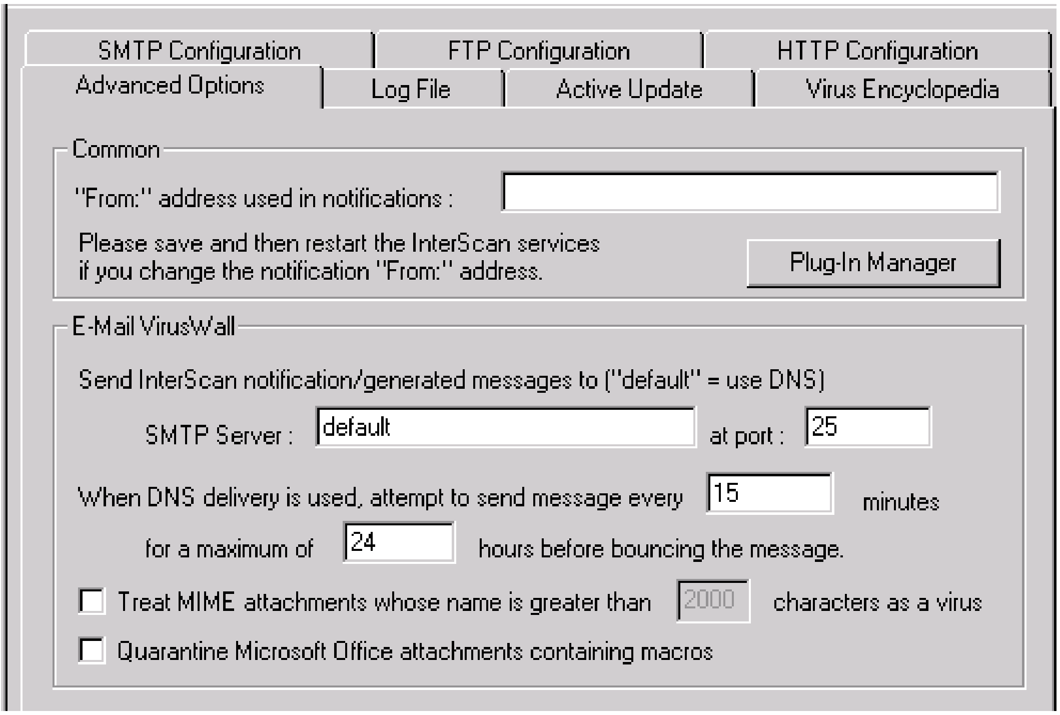


HTTP Auto Clean Option

Action on Uncleanable File(s):
○ Pass   ○ Move   ● Delete

Duplication of configuration options may seem unnecessary for FTP and HTTP but having the ability to specify settings at a more granular level is important in this scenario.

Advanced options are available on a separate folder tab where added features can be modified. Notification messages' From: or sender address is defined here and plus the method for sending these notifications. Available options your environment may require is to block Microsoft Office attachments that contain macros the defaults are usually appropriate.



Common

"From:" address used in notifications :

Please save and then restart the InterScan services
if you change the notification "From:" address.

E-Mail VirusWall

Send InterScan notification/generated messages to ("default" = use DNS)

SMTP Server : default at port : 25

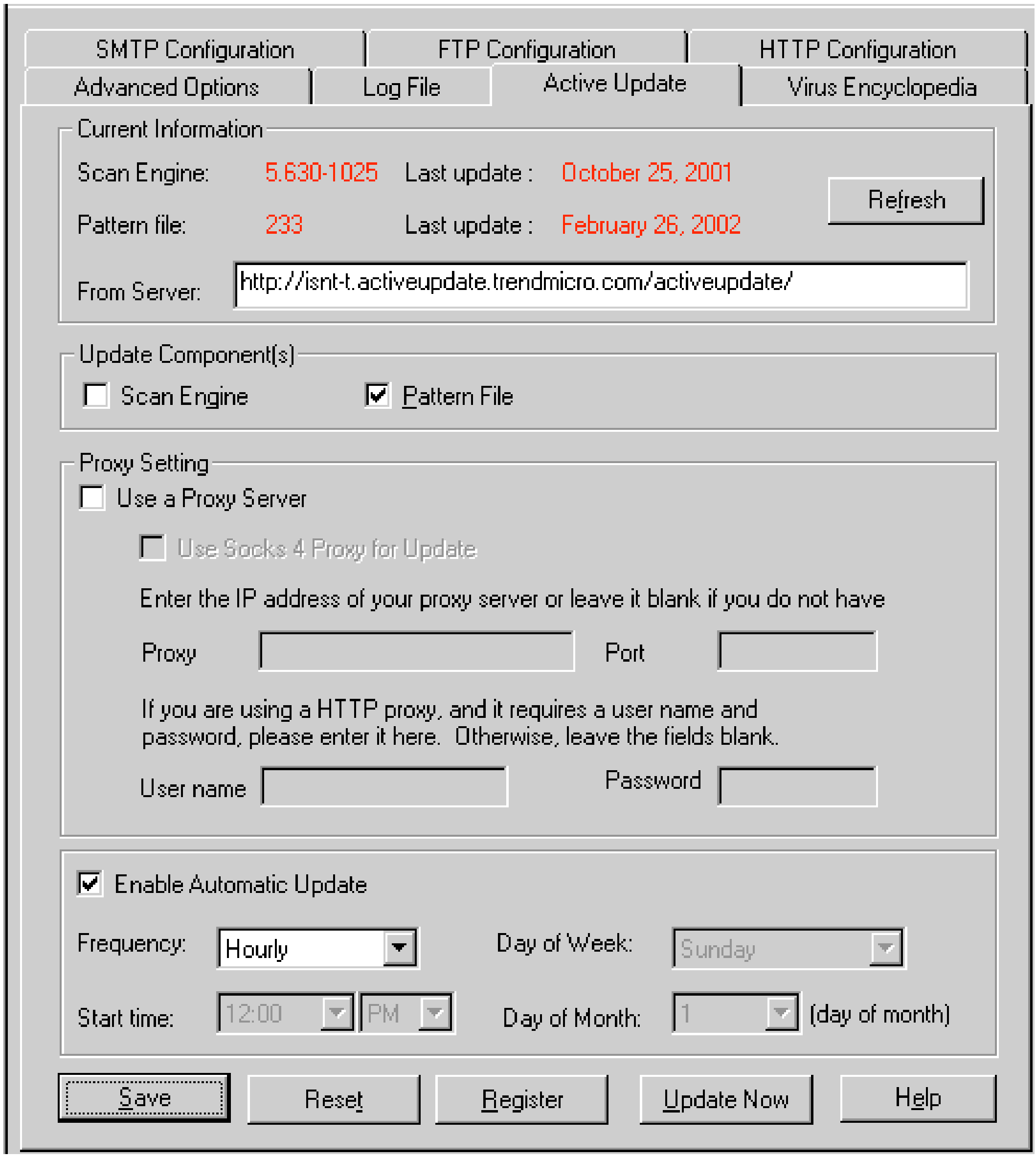
When DNS delivery is used, attempt to send message every 15 minutes

for a maximum of 24 hours before bouncing the message.

☐ Treat MIME attachments whose name is greater than 2000 characters as a virus

☐ Quarantine Microsoft Office attachments containing macros

VirusWall isn't unlike any other mainstream virus software and requires updates as frequently as possible. This process has been automated for the CVP server, which reduces administration and ensures new viruses are detectable as quickly as possible. The pattern files that define what constitutes a virus will require updates the most and it may be advisable to schedule this auto-update to occur every hour. Having the software check for an update this frequently doesn't use a noticeable amount of bandwidth unless there is an available update. The auto-update can also check to see if there is an update to the scan engine in the same instance – a scan engine software update may be required to increase the efficiency or ability to detect and repair viruses. The Active Update folder tab has the options for where to get these updates, how often to update, whether to check for pattern and engine updates, and if necessary settings for authenticating to a proxy server to gain internet access.



Current Information

Scan Engine: 5.630-1025 Last update : October 25, 2001

Pattern file: 233 Last update : February 26, 2002

From Server: http://isnt-t.activeupdate.trendmicro.com/activeupdate/

Update Component(s)

☐ Scan Engine ☑ Pattern File

Proxy Setting

☐ Use a Proxy Server

☐ Use Socks 4 Proxy for Update

Enter the IP address of your proxy server or leave it blank if you do not have

Proxy Port

If you are using a HTTP proxy, and it requires a user name and
password, please enter it here. Otherwise, leave the fields blank.

User name Password

☑ Enable Automatic Update

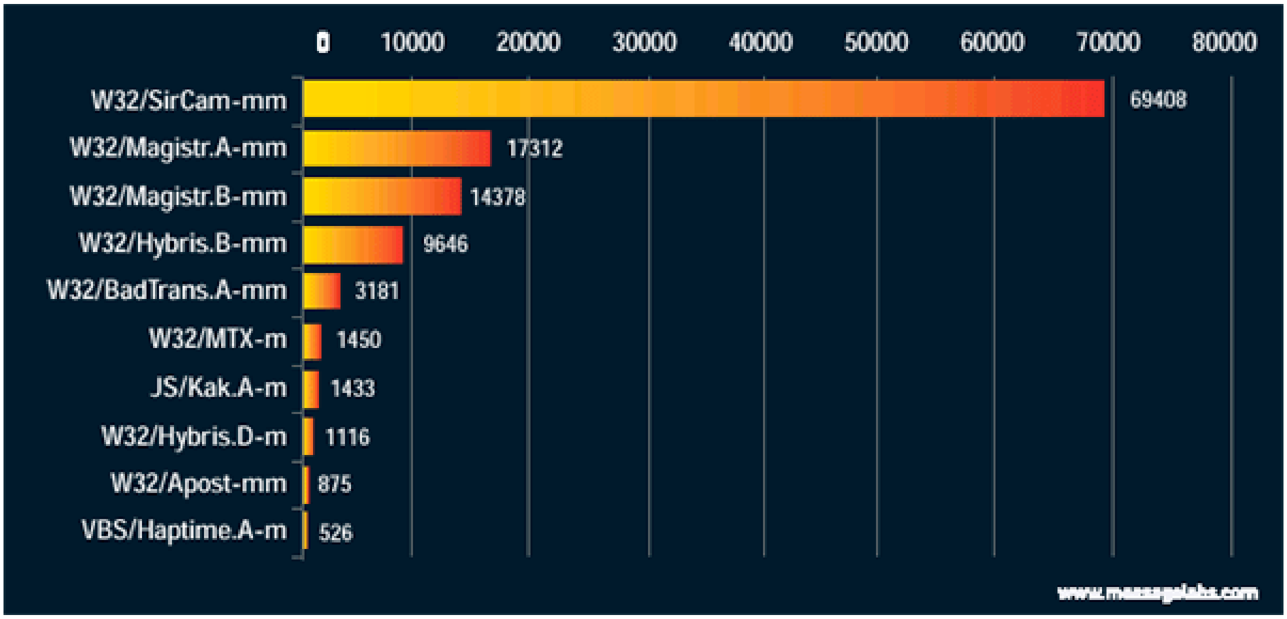
Frequency: Hourly Day of Week: Sunday

Start time: 12:00 PM Day of Month: 1 (day of month)

Having these two pieces of software setup to work together in the manner described has the ability to greatly improve the protection of your internal network as well as publicly accessible hosts such like a web or mail server. This discussion has primarily focused on threats from the public Internet or internal users, however, a content inspection server could even be used to isolate your Local Area Network from entry points such as Wide Area Network connections where organizational email or intranet resources may exchange traffic and/or data.

Continuous Threats

The numbers of viruses are increasing so quickly that perimeter antivirus solutions may soon become standard practice for companies with an Internet presence, especially when credibility and reputation are a selling point over your competitors. The chart below lists the top viruses reported by Messagelabs.com email scanning systems for the fourth quarter of 2001.



VirusEye – MessageLabs' Virus Information Service / Winter 2001 Report p.4

W32/SirCam and some variants lead the list that inevitably drew more attention to the concept of virus or malware security. This virus has the ability to infect your system and send out emails on your behalf with local files attached. Equally alarming is that the W32/SirCam virus continues to be one of the top ten viruses documented even though discovery was as early as July 2001 and another example of how important content inspection can be.

Content that the Viruswall inspection server might detect would be the JS_MENGER.GEN or Js/Messenger-Exploit, which is JavaScript malware that isn't destructive but asks a user to visit a web site containing malicious code. It also has the ability to capture a list of logon names from Microsoft's MSN Messenger program. The risk of JS_MENGER.GEN is low and doesn't seem to be very harmful but exploits similar to this are found in all types software quite frequently. Exploits such as these once identified are added to the pattern files or updates to the CVP servers' list of unacceptable software but this still leaves the potential for java script or active-X content to enter if it hasn't been labeled as malicious. The entry point is being monitored in this situation but it's only looking for what it knows to be harmful. Stopping this kind of malware before it ever gets in is the main concept and benefit in a CVP implementation.

Filtering the content of HTTP traffic is a good way to ensure that malicious software doesn't get into your network but the CVP API can take it a step further. Many implementations today are filtering what URL's are accessible by their users in order to prevent harmful malware and to deter employees from abusing Internet access. Vendors such as SurfControl, Finjan Software and WebSense have generated software that will filter web traffic based on maintained lists of harmful or undesirable URL's as well as lists administrators define based on specific needs.

Outlook for Content Inspection

Future requirements for an effective defense against threats that are present on the Internet will continue at a demanding pace as the number and frequency of exploits and vulnerabilities grow. It seems the creativity of malicious code is expanding as fast as Internet usage itself. Techniques of avoiding detection are being uncovered every day and detection tools must maintain that same pace. Several of the major software applications that specialize in URL filtering, antivirus, or HTTP content filtering may begin to merge to a single source application solution for defense against current vulnerabilities in the future possibly even including a firewall application as well for smaller businesses. Stegonography is one tool that could be used to evade current detection systems by disguising files inside other files. Software such as Stego allows a user to embed any type of file inside a harmless looking attachment by modifying the bit patterns that define the content of the host file. JPEG's and Bitmap files are often used for this type of scenario and files of this sort are typically allowed to pass through CVP servers without much scrutiny. Malicious use with this type of software has been narrow in scope but it seems this technology will have to be incorporated into future revisions of content inspection systems.

Content Vectoring Protocol implementations have the potential to fulfill many more roles in current network environments. As threats increase the ability to eliminate them will undoubtedly have to expand as well. Though a

CVP implementation only protects one of many entry points into a network, it can be a key player in a sound defense of your network and assets.

References

Vijayan, Jaikumar. "Security Challenges Take Toll"

ComputerWorld Magazine. January 7, 2002 URL:
http://www.computerworld.com/storyba/0,4125,NAV47_STO67143,00.html

CHECK POINT SOFTWARE PUBLISHES INDUSTRY LEADING CONTENT SECURITY API AS OPEN SPECIFICATION.
Checkpoint Software Technologies – Corporate Information.
November 11, 1998. URL:http://www.checkpoint.com/press/1998/cvp111198.html

Fisher, Dennis. "Malicious Activity Skyrocketing on the Net."
Eweek Magazine. January 11, 2002. URL:
http://www.eweek.com/article/0,3658,s%253D1884%2526a%253D21018,00.asp

Content Vectoring Protocol – definition
http://isp.webopedia.com/TERM/C/Content_Vectoring_Protocol.html

DMZ – Demilitarized Zone – definition
http://isp.webopedia.com/TERM/D/DMZ.html

CERT/CC Statistics 1988-2001. January 10, 2002
http://www.cert.org/stats/cert_stats.html

Check Point™ VPN-1/FireWall-1 CVP (Content Vectoring Protocol) API Specification. May 2000.
Checkpoint 2000 Distribution CD. CVP.pdf

Checkpoint Software Technologies Inc. "Checkpoint Firewall-1 OPSEC Open Specification." URL:
http://www.checkpoint.com/cvpopenspec/CVPOpenSpecification.pdf

Thurman, Mathias. "Virus Attacks Can Enter Through Many Doors."
Computerworld Magazine. January 28, 2002
http://www.computerworld.com/itresources/rcstory/0,4167,STO67720_KEY73,00.html

VirusEye – MessageLabs' Virus Information Service / Winter 2001 Report
http://www.messagelabs.com/data/downloads/q401.pdf

Trend Micro Interscan VirusWall – Administrator's Guide. V3.5, p1-6. July 2001.
http://a816.g.akamai.net/7/816/537/d49cd7252dec52/www.antivirus.com/download/documentation/internetgateway/files/isnt35ag.pdf

E. Cole. "SANS Security Essentials IV: Encryption and Exploits," Rev 1.5. Nov. 2001

SANS Security Essentials Course Materials, Day 4 Handbook, p. 4-20 – 4-25.