Global Information Assurance Certification Paper

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.

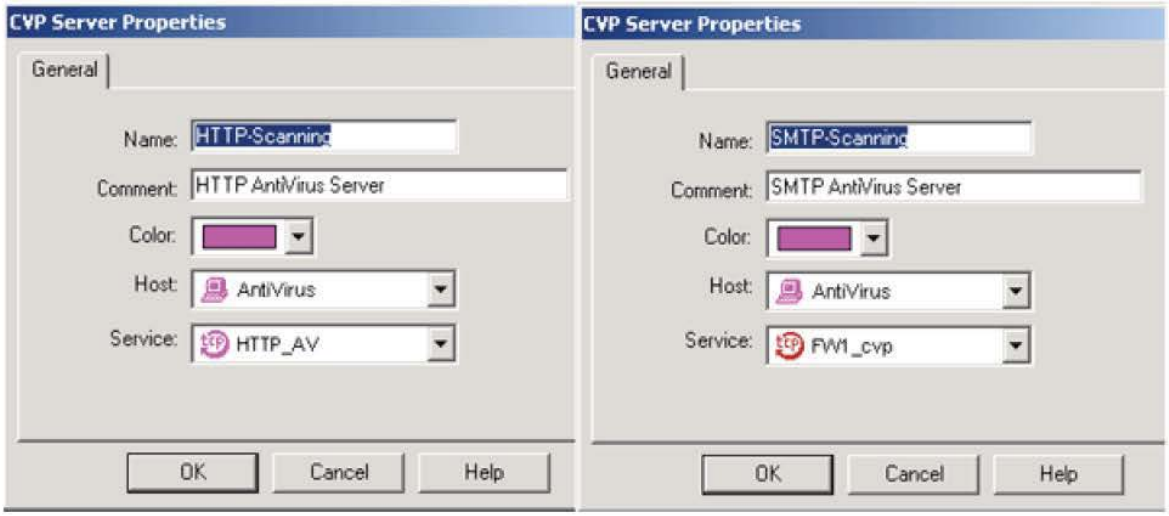
CVP Configuration

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.

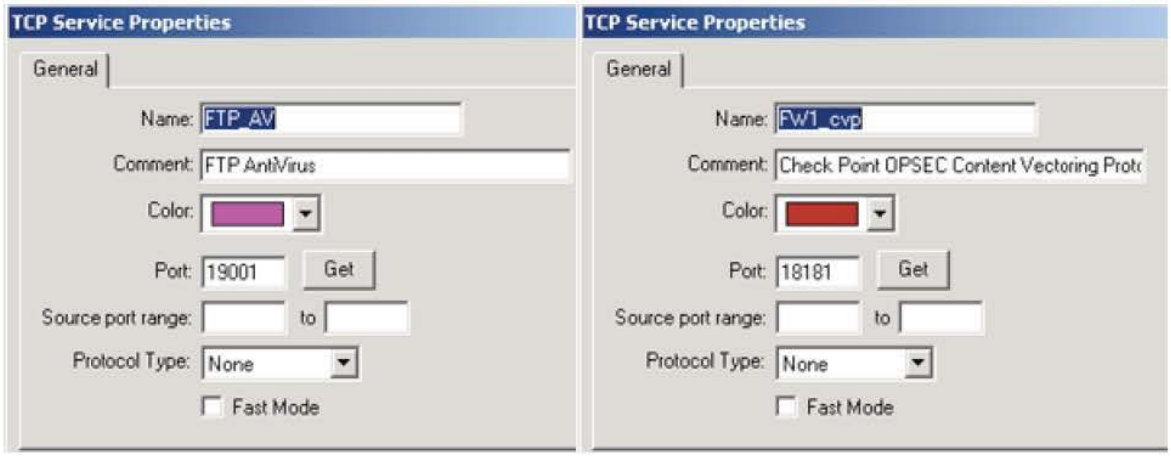
Client Setup

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.

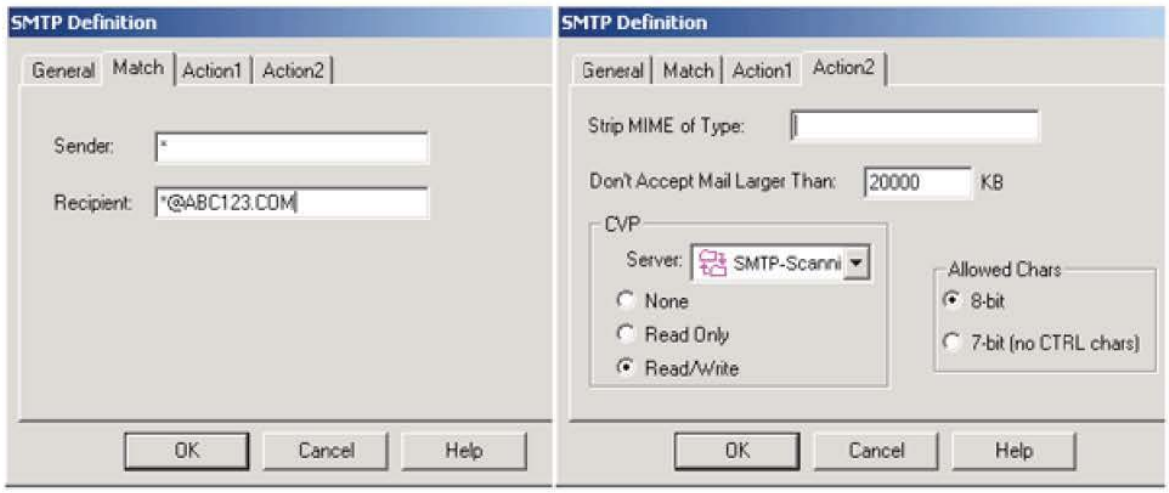
First let's define what our CVP host will be through an object in the rule base which will simply be a descriptive name, an IP address, and any special routing instructions if necessary. If your setup will have more than one content validation server then those host objects will need to be created as 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:



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:



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.



DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.