Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2d

To CVP or not to CVP
Kurt Koenigsknecht
May 2001

Introduction:

Every day it seems a new computer virus has been unleashed on the Internet community. Not only has the frequency of the viruses become more problematic but the wrath of destruction they leave has increased as well. Businesses in the United States, as well as the world, have become dependent on the reliable, unrestricted flow of electronic information. To state that information has now become the "lifeblood" of many an organization both small and large would not be an exaggeration. One would be hard pressed to find a business that would not be impacted, sometimes critically, by the loss of its data or by the disruption of its flow.

Aladdin Knowledge Systems literature states that attacks on computer systems are rising dramatically and according to International Computer Security Association (ICSA) studies, there is consistent evidence of "an approximate doubling of the risk of computer viruses to organizations each year for at least the past five years despite widespread use of [standard] anti-virus measures". Companies are using more firewalls than ever before, so why do these breaches continue to increase in number? The answer is simple: the days of traditional hacking have been replaced by a new wave of attacks – hostile programs such as vandals and viruses, as well as unmonitored transfer of confidential information by employees.

This means the use of traditional content scanning measures is no longer sufficient to protect the enterprise from today's many threats. To minimize this threat companies have turned to application vendors that provide tools that can handle multiple functions such as; filtering of HTTP protocol traffic, filtering of FTP file transfers, and filtering of SMTP mail content for viruses, providing the ability to limit and/or prevent vandals, and providing the means to scan content for undesirable text, as well as, the ability to limit the transfer of confidential material by customizing rules that can prevent this through the use of key words or restricted file names.

Today many businesses use a multi-layered approach for content scanning to protect the organization. The three most common layers are as follows:

- Internet Gateway based
- Server based

- Desktop based

Utilizing technology to render damaging content harmless at the Internet Gateway is fast becoming a strategic weapon to many who implement multi-layered content scanning. Thwarting harmful content at the perimeter, before it can enter the enterprise, has proven to be one of the most effective methods of protection.

Because the methods and number of products available for content scanning are so broad, the researcher has decided to limit the content of this paper. There are two methods for scanning content at the Internet gateway that will be discussed. The first method, depicted in Figure 1., is through the use of the Open Platform for Secure Enterprise Connectivity (OPSEC), Content Vector Protocol (CVP) based content scanning products in combination with a Firewall. The second method, depicted in Figure 2., is a standalone content scanning product that works completely independent of the firewall.

Both of these methods for scanning content at the Internet gateway will be discussed as it relates to their use with the Check Point Firewall-1 firewall. The discussion will debate the merits of using the OPSEC compliant, CVP based content scanning products verses a standalone product that is completely independent of the firewall.

CVP based content scanning:

This next section will discuss the Pros and Cons of OPSEC compliant CVP based content scanning with the Check Point Firewall-1. Figure 1. represents a typical CVP based content scanning implementation.

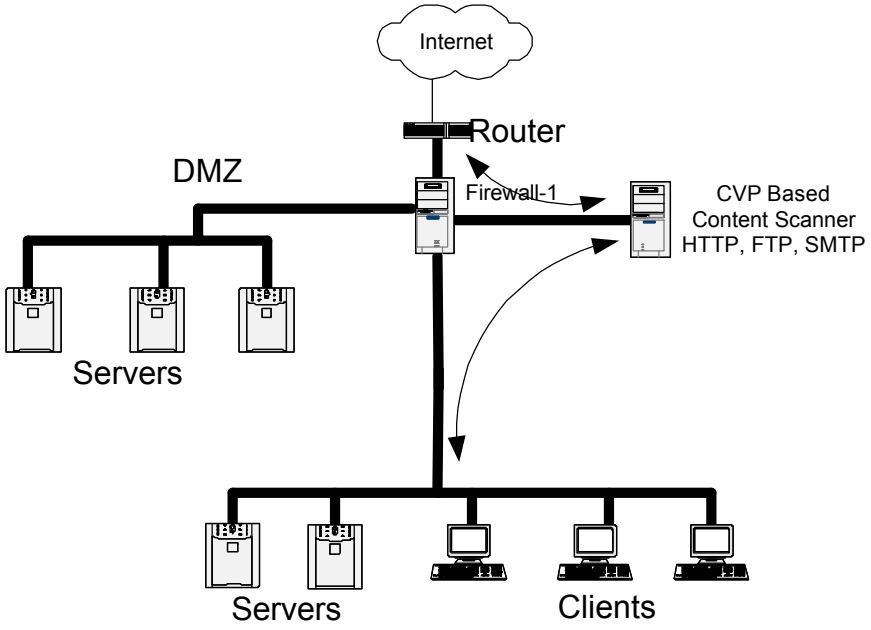

Figure 1.

Pros:

According to Check Point implementing an OPSEC, CVP compliant content scanning gateway provides the flexibility to implement products from a variety of competing vendors. Applications are written to plug into the OPSEC framework via a published API. Companies can easily and seamlessly integrate content scanning application into the FireWall-1 enterprise security solution. This enables all levels of the enterprise security to be defined and driven by a single, central enterprise-wide security policy. This provides for a simpler enforcement of the corporate security policy.

CVP based content scanners utilize redirects from the Check Point Firewall-1 "rule base" which determine the traffic types that will be scanned for harmful content. CVP based content scanners only receive redirected traffic types, thus all other traffic bypasses the CVP system completely avoiding delays. In addition CVP scanning allows non-infectable files, such as graphics and plain text files, to bypass scanning engine for improved performance.

CVP based content scanning applications provide the ability to filter SMTP, HTTP and FTP traffic both inbound and outbound, which prevents your organization from spreading harmful content as well, at the Internet Gateway. This scanning protects against electronic mail, macro or file viruses, in addition it can provide protection against hostile Java applets and Active-X objects. Of course, functionality may very by what the application vendor includes in their product offerings. By adhering to the OPSEC API,

vendors are free to develop unique products in the marketplace. This stimulates innovation by competing vendors as they implement the latest security developments into their products more quickly.

Note: POP mail, unlike SMTP, which is delivered to a server, is directly downloaded to the desktop and not scanned. Desktop scanners should be utilized for POP mail.

The CVP gateway can and should for improved security reside on hardware separated from the firewall system, thus providing a modular approach to implementation. This flexibility allows the enterprise to decide which platforms and products meet the business needs of the organization. An added benefit is the automatic distribution of the processing load to multiple systems. The adherence of the CVP API provides companies with the ability to change content scanning vendors with minimal impact to the Firewall software configuration.

Cons:

One big disadvantage of implementing a CVP based application is the added complexity involved in troubleshooting problems that exist with content scanning. It can sometimes be difficult to pin point the root cause of the problem when traffic flows through both the Check Point Firewall-1 "resource" as well as the content scanning application. This typically results in the customer having to manage two vendors when pursing resolution to non-trivial support incidents.

When configuring the firewall to work in CVP mode, which redirects filtered traffic, it essentially means the data will be flowing in a proxy like mode. As the "downloads" take place the content scanner has to ensure the integrity of the data before it is passed along to the client system. In some cases this can cause significant performance degradation and may even cause protocol timeouts, which terminates connections. This seems to be more prevalent in Internet Explorer than Netscape Communicator. There are two traffic conditions that are most likely to experience protocol timeouts that terminate the connection:

- Downloading large files in HTTP protocol, such as a "pdf" file
- Downloading large ZIP files

To reduce the occurrences of this, some vendors have implemented an adjustable "defeat timeout" setting. Lowering the adjustable timeout essentially allows the client to start receiving a few bites of the beginning of large files before the entire content scan has completed, thus preventing the timeout. In extreme cases, when downloads cannot be completed due to timeouts, the only workaround may be to bypass the content scanning altogether which is not an acceptable option.

CVP firewalls currently do not support HTTP 1.1, which by default is turned on in Microsoft's Internet Explorer. This tells the browser to use HTTP 1.1 when ever applicable for those sites that are making it available. As a result this typically presents itself as clients not being able to view specific Web sites, or display compete pages from others. There are two possible resolutions for this; one it to make a global modification to the objects.C which forces all HTTP traffic to be version 1.0 or by turning off the HTTP 1.1 setting in Internet Explorer at every desktop.

Problems, changes and/or deficiencies in the CVP implementation of the firewall immediately reflect on the CVP application. For example, if Check Point changes the settings in the CVP resource, via a patch or version upgrade, it may have adverse effects on the CVP application that was performing perfectly before a patch was applied. Again the client is left to manage a support incident with two vendors instead of one.

In order for an application vendor to work in CVP, vendors get a DLL from Check Point. When problems do occur, vendors may not always have full analysis abilities to debug and fix the DLL, thus they must rely on support from Check Point. Potential DLL problems complicate the troubleshooting of non-trivial CVP issues because again, the client is left to manage a support incident with two vendors instead of one.

Implementing CVP based content scanning requires extensive knowledge to configure properly; even minor issues like knowing you have to enlarge the CGI script buffer from the default settings is not common knowledge for many of those who utilize these products. It is not uncommon for a CVP vendor to provide a list of "modifications" to the Firewall-1 objects.C file to solve more than one scanning anomaly. Changes to the objects.C require extensive troubleshooting and testing, which is extremely time consuming. On top of that you have to deal with the many complaints from interrupted service, each time a newly discovered problem requires another "modification". Some of these problems are so subtle that it may take extensive data captures, that must be reviewed, to determine the root cause of the problem only to find a simple change to the objects.C was final solution.

Standalone based content scanning:

This next section will discuss the Pros and Cons of Standalone content scanning protection. Figure 2. represents a typical Standalone based content scanning implementation.

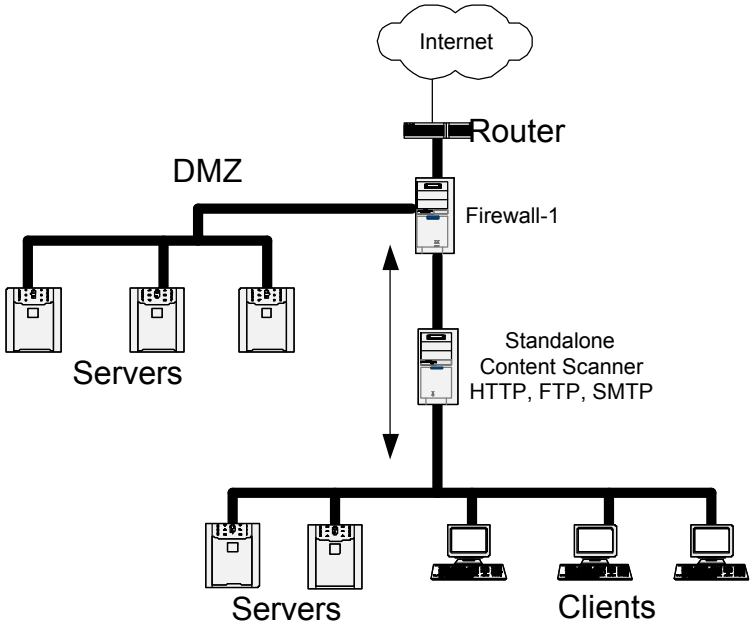

Figure 2.

Pros:

Standalone based content scanning applications provide the ability to filter SMTP, HTTP and FTP traffic both inbound and outbound, which prevents your organization from spreading harmful content as well, at the Internet Gateway. This scanning protects against electronic mail, macro or file viruses, in addition it can provide protection against hostile Java applets and Active-X objects. Of course, just like with CVP based applications, functionality may very by what the application vendor includes in their product offerings.

Utilizing a standalone content scanning application, which acts as a router rather than a proxy can provide significant performance gains. The standalone applications will pass approximately 99% of the file, for HTTP and FTP, down to the client while the scanning is being completed. Should the file be harmful it is truncated before the completed file resides on the client, thus no risk while improving performance dramatically.

A big advantage of the standalone application is that it requires no modification to the firewall since it is completely independent of the firewall application. The standalone application could be used with any firewall application.

All traffic, not just HTTP, FTP and SMTP mail, will pass through the standalone application. This positions itself well for future enhancements, should they be necessary, for scanning traffic types that may become “at risk”.

Cons:

Implementing content scanning in the standalone mode removes the ability to enforce the enterprise security policy from a single point of administration, such as through the Firewall-1 GUI. It is recommended that the same administrator who maintains the firewall also implement the content scanner to avoid any disconnect that could lead to undesired results.

Since the standalone product acts as a router, all traffic, not just HTTP, FTP and SMTP mail, must pass through the standalone system even if it's not scanned. For environments that have extremely heavy traffic this could potentially become a bottleneck.

Even though the content scanner is standalone, it does not remove completely the potential for conflicts and/or configuration issues with the Check Point Firewall-1 software. If trends continue, this is expected to continue to be minimal.

Conclusion:

Both methods of content scanning have several pros and cons yet both produce the desired results of thwarting threatening content before it reaches the enterprise. The researcher found that CVP based applications seem to require a much higher level of maintenance than standalone systems, thus making it a more complex solution overall and may be a deterrent to implementation.

The good news is that some vendors now offer both standalone and CVP based applications, thus both methods of scanning are available as the business needs dictate or should one become unacceptable to use.

References:

1. "Check Point Software Technologies And Trend Micro Team to Combat Internet Gateway Security Threats "
URL: http://www.antivirus.com/corporate/media/1998/pr100598.htm

2. "The Future of Information Security: Integrated Border Security"
URL: http://www.antivirus.com/products/isvw/white_papers.htm#Security

3. "Introduction to Content Security"
URL: http://www.eSafe.com/home/content%5Fintro.asp

4. "Open Platform for Security"
URL: http://www.checkpoint.com/opsec/architect.htm

5. "Complete Content Security for Internet Gateways and Mail Servers "
URL: ftp://ftp.ealaddin.com/pub/manuals/esgwp.pdf

6. "Malicious Software (Malware)", Track 1: Security Essentials Curriculum 1.1, Chapter 7.

© SANS Institute 2000 - 2005 Author retains full rights.