Cyberoam

Unified Threat Management

White Paper

Using a Gateway Antivirus to Guard the Enterprise Protocol Spectrum

Slammer hit its first victim at 12:30 am EST. By 12:33 am, the number of slave servers in Slammer's replicant army was doubling every 8.5 seconds. By 12:45 am, huge sections of the Internet began to wink out of existence.

A virus “ infected” systems may not be actually “ affected.”

Preface

Internet is omnipresent. It has shrunk the world and has been tremendously beneficial. However, on the flip side, this shrunken virtual world is not free of threats. New blended threats have reared, rendering single security solutions inadequate. In the present scenario, Unified Threat Management (UTM) solutions guiding the network gateway have come in vogue. A standard UTM broadly comprises of Firewall, Anti-virus, Anti-spam, Intrusion Detection and Prevention (IDP), Content Filtering and Band-width Management services.

The purpose of this paper is to explore the Anti-virus facet of UTM. We will elucidate the exact role of an Anti-virus in a UTM solution. En route we will look at the various protocols that need to be tapped by the Anti-virus in case of various deployments of a UTM.

And One Night

It was little after midnight of Saturday, January 25, 2003. In a Network Operations Control Center, just down the street from MIT, Owen Maresh almost choked when Priority 1 alert popped up on his panel of screens. This Network Operations Control Center was the command room for 15,000 high-speed servers stationed around the globe commanding a God's-eye view of the activities on Internet.

This was big trouble. Fifty-five million meaningless database server requests were traversing the globe. Maresh was the first person on earth to spot the Internet worm that came to be known as Slammer.

Slammer's attack was ruthless and quick. It started with a single killer packet which was delivered through a mail. The worm hit its first victim at 12:30 am EST. The machine - a server running Microsoft SQL - instantly started spewing millions of Slammer clones, targeting computers at random.

By 12:33 am, the number of slave servers in Slammer's replicant army was doubling every 8.5 seconds. Maresh and his coworkers began calling and emailing fellow night owls at ISPs worldwide to warn them of the tsunami of traffic. It was already too late.

By 12:45 am, huge sections of the Internet began to wink out of existence. Three hundred thousand cable modems in Portugal went dark. South Korea fell right off the map: no cell phone or Internet service for 27 million people. Five of the Internet's 13 root-name servers - hardened systems, all - succumbed to the squall of packets. Lost revenue spilled over halfway into the next week. Total cost of the bailout: more than $1 billion.

This fateful day marked a paradigm shift in the history of Network Security Solutions. Firewall and desktop antivirus solutions proved hopelessly inadequate. Slammer was delivered through a mail that went undetected and it triggered a Denial of Service attack.

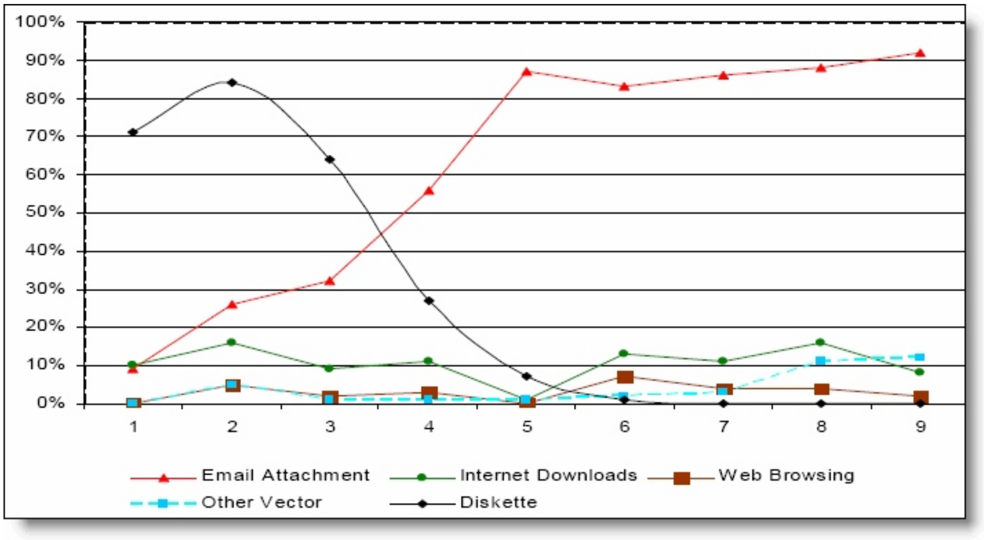
The enterprises worldwide felt an urgent need to guard their mail environment by examining the SMTP and IMAP/POP3 protocols; keep a tab on the web browsing by controlling the HTTP protocol; control the transfer of files by checking the FTP protocol and also monitor other protocols like UDP. They also felt the need to control the ports and provide a selective access to legitimate users only. Network security experts realized that though slammer had infected a single computer, its affect was felt on SQL servers, worldwide. Undoubtedly, safe mailing was the primary focus.

“Infected” may not necessarily be “Affected”

Traditionally virus has always been associated with the desktop because the impact of a virus is actually seen on the desktop. However, Irrespective to the point of entry, only when a malware (viruses, worms, trojans, spyware, adware, and other malicious code) starts to affect, do we come to know that the system has been infected. So, there is a subtle difference between a malware infection and its affection. Infected simply means that the malware has penetrated the system and is now using it to spread. Melissa virus is a good case study to understand this difference.

The blitzkrieg of Slammer was matched by Melissa alone. On Friday, March 26, 1999, a mail containing a LIST.DOC unleashed a macro that mailed itself to fifty other addresses in the host's address book. The affect on the individual was minor, and it was a one-time event for those who did not repeat the mistake of re-opening the mail. However, Melissa had a devastating affect on a system that it never infected the email server. The email servers were overloaded at a dramatic pace and eventually crashed. In other words, a single infected system can affect a complete network in no time.

"Email was rated at a staggering high of 92% as the source of virus infection." -ISCA Labs Prevalence Survey 2004



Virus Encounter Vectors

The threats have now become more veiled, focused and target specific to companies or business sectors executed with sheer professionalism.

Rise of the Email

Malware have two main entry points: local media on the desktop and Internet. While desktop AV solutions cater to the local security needs, the network security is the most vulnerable point of access.

Internet has matured to become a prime source of exchange of ideas. In a META group survey 80% of respondents considered email more valuable than phone for business communication.

With the rise of email, malware have found it the most convenient carrier. According to ISCA Labs Prevalence Survey 2004, email was rated at a staggering high of 92% as the source of virus infection.

IWhile email has become a security threat, the threats posed through internet downloads and web browsing has also accounted for a combined 10%.

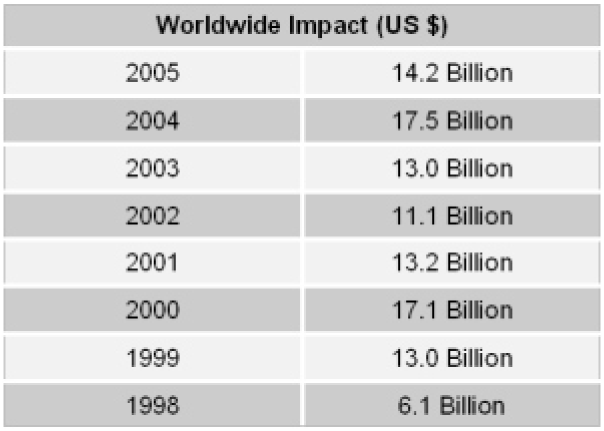
A Misleading Trend

The malware scenario has a more disturbing facet to it. As 2005 ended, the malware scene transitioned from a teenage vandals' playground to a world of opportunity for cyber-criminals. As Anti-virus solutions have started to keep up and, often, better them, virus writers have become focused. Now, malware is a tool to steal data.

According to 2005 Malware Report: The Impact of Malicious Code Attacks, published by Computer Economics, for first time since 2002, the economic impact of malware in 2005 has actually declined. But this is misleading.

The threats have now become more veiled, focused and target specific to companies or business sectors. So, unless you are the targeted, the economic impact of malware dropped.

Malware have two main entry points: local media on the desktop and Internet.



Worldwide Impact (US $)	
2005	14.2 Billion
2004	17.5 Billion
2003	13.0 Billion
2002	11.1 Billion
2001	13.2 Billion
2000	17.1 Billion
1999	13.0 Billion
1998	6.1 Billion

Financial Impact-Virus Attacks 1998-2005

Focused malware infections require a greater manual effort to eradicate, especially as the attacks are designed to leave the infected computer running. The affect is felt on the resources which are usurped by malicious code running in the background.

Essentially, an infection can affect the bottom line of an enterprise in four ways:

1) Loss of revenues prior to the detection of the infection caused by depleted resources and loss of goodwill.
2) Loss of revenues due to web site and network downtime and loss of productivity while workers wait for the fix.
3) Expense of operational resources to fix the problem.
4) Liability with legal costs from confidential information like credit card/social security numbers disclosed.

To allay this situation, a gateway AV solution has to know precisely which protocols it has to guide and when. A comprehensive gateway AV should guide the mail protocol SMTP, IMAP/POP3, the Internet surfing protocol HTTP and the File Transfer Protocol (FTP). However, a blanket protection might become too unwieldy. Simultaneously a properly configured gateway AV will be able to plug the finer perforations in the security, e.g. If there is a database server sitting inside the network there is no point in scanning its traffic for HTTP protocol. Similarly, if a user's policy provides him/her surfing access and no mail access, only the HTTP traffic ought to be scanned.

A Gateway AV should guide the mail protocol SMTP, IMAP/POP3, the Internet surfing protocol HTTP and the File Transfer Protocol (FTP).

Harnessing the Email Protocols

Much of the activity needed to get the virus past your defenses and activated, is referred to as social engineering. It has been often said that humans are the weakest chink in the computer security armor. The best way to counter social engineering is to make sure that an infected mail or communication does not reach its destination end user.

Modern anti-virus system looks for virus and malware signatures a unique string of bytes that identifies a virus and zaps the virus from the file. The gateway anti-virus solution scans files that are embedded in network traffic. If an infected file is detected, it is removed from the traffic. To scan files within network traffic, gateway anti-virus must understand a broad range of file encoding protocols and file compression algorithms.

Since the application streams that are scanned for viruses must be completely reassembled by the gateway anti-virus system as the traffic crosses the network, users or servers might experience a slight delay in the scanned streams. Administrator should have a granular control of the traffic and file types that warrant scanning.

The most crucial factor in deploying a UTM based AV solution is the mail service used by an enterprise and the placement of the mail server.

Let us take various scenarios in to account.

1) **Enterprise uses proprietary mail server**
Here the enterprise has a dedicated mail server that takes care of all its mailing requirements. In this scenario all the three protocols SMTP, IMAP and POP3 can be scanned.

> “Humans are the weakest chink in the computer security armor” Social Engineering Experts

However, the UTM based AV solution should be deployed based on the network architecture and only the necessary protocols should be checked. We will look into various deployment scenarios.

2) **Enterprise uses web-based mail**
In this case the enterprise relies on web-based email solutions like Yahoo. So HTTP protocol comes into picture.

3) **File Transfer the Internet**
If the enterprise allows file transfer and downloading over Internet, it also has to guide the FTP protocol over the HTTP protocol.

Enterprise uses Proprietary Mail Server

There are four possible mail server deployments. According to the placement of the mail server in a network, the system administrator should just select the priority of the protocol scan. Let us have a look at some scenarios.

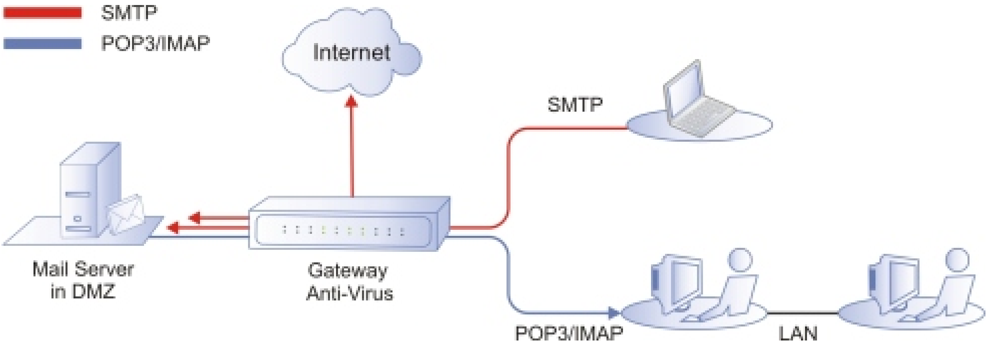
I. Mail server hosted in DMZ

The mail server is hosted in the DMZ. The antivirus solution is deployed between the Internet cloud, and the DMZ and the intranet. Here the entire mail traffic will pass

through the Gateway AV. The enterprise will have complete control over the mail server in this scenario, which means that the full mail protocol spectrum is with the enterprise to control.

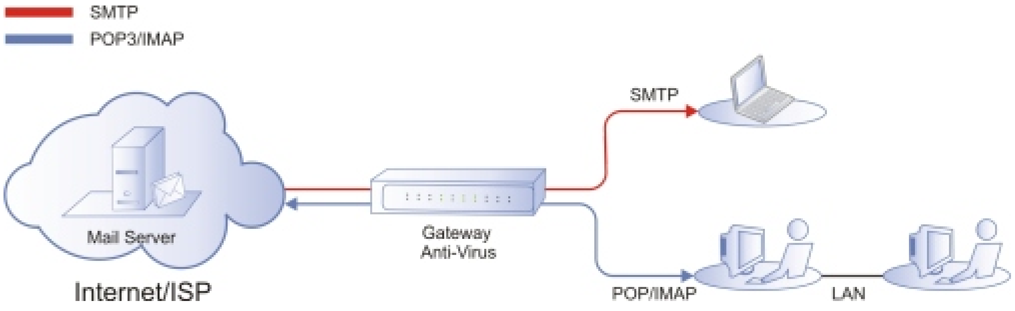
The mail server will send and receive all the mails using SMTP protocol. Once the mails reach the mail server, the intranet users will be able to retrieve their mails using IMAP/POP3 protocol.

The entire outgoing and incoming mail traffic of the mail server is SMTP based. In this scenario, it will be sufficient, if the Gateway AV scrutinizes the SMTP protocol only.



II. ISP Based External Mail Server & Individual User Access to Mailbox

In this case, the mail server is hosted with an ISP. The Gateway AV deployed between the Internet cloud/ISP and the Intranet. This scenario is subtly different from a web-based mail scenario. While web-based mail uses HTTP protocol, here SMTP and IMAP/POP3 come into play. Here the mail server is not with the enterprise, so it has to heavily rely on the security provided by the ISP. Each user has an individual access to the mail server.



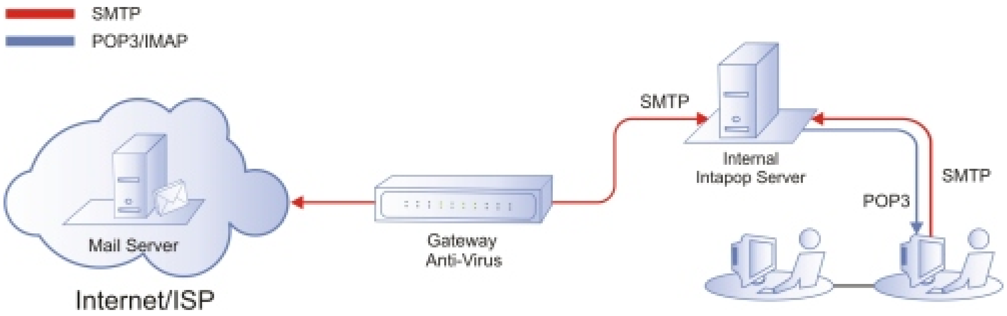
80% of respondents consider email more valuable than phone for business communication.
- META group survey

In the protocol jargon, individual user uses SMTP protocol to send mail to the mail server hosted with the ISP. To retrieve their mails, from the mail server, users will use IMAP/POP3 protocol. So the Gateway AV will have to scan both the protocols to ensure safe mailing environment.

This is a tricky scenario, as the mail server is left to the mercy of the ISP protection faculties which might prove inadequate. On the other hand, the enterprise cannot intrude into the ISP to scan its mail.

II. ISP Based External Mail Server & Internal Intrapop Server

This is a comparatively safer variant of the previous case. The mail server is hosted with an ISP. The Gateway AV deployed between the Internet cloud/ISP and the Intranet. Here the individual user does not have a direct access to the mail server. There is an intrapop server sitting within the enterprise, which forwards the outgoing mail to the mail server and fetches the mail as per the end users requirement. Here the intrapop will provide an additional rung of security. The intrapop traffic can be scanned and policies can be implemented on it.

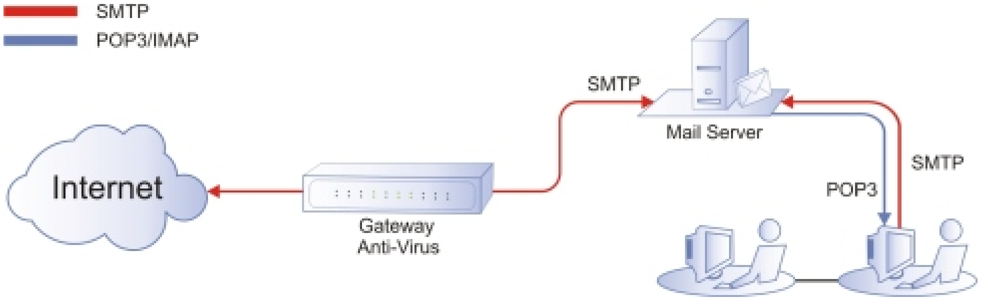


The ISP based mail server and the intrapop server will use SMTP protocol to send and receive mails. Users will internally use SMTP to send mails to the intrapop server and POP3 to retrieve their mails from the mail server through the intrapop server. So, if the SMTP protocol used by the intrapop and the mail server is put under the Gateway AV surveillance it would suffice the security needs.

III. Mail Server Hosted as a Part of the Intranet

This is a very common scenario. The mail server is placed as a part of the intranet LAN. Here the Gateway AV sits between the Internet cloud and the LAN.

Like the previous scenario, here the mail server uses SMTP to send and receive mails from the internet cloud. Individuals will use SMTP to send mails to the mail server and IMAP/POP3 to retrieve their mails. So the surveillance of the external SMTP protocol used by the mail server and the internet cloud by the Gateway AV would prove adequate enough.



Keep a tab on the HTTP to control surfing based virus.

Gateway AV Quarantine Option

If the Gateway AV fails to clean an infected email, it should be able to quarantine it. If the quarantine option is not available, it may prove to be a major hurdle. If an infected mail of vital importance is discarded by the Gateway AV solution, it might translate into a lost business opportunity.

An ideal Gateway AV should provide granular user-based policy to quarantine infected or possibly infected mails, which can be dealt with safely.

Guiding the HTTP Protocol

Guiding the email scenario is just not enough. The system administrator also has to take into account the web-based mailing services and internet surfing. This communication is carried out over the HTTP protocol. Moreover, internet downloads also utilize FTP over the HTTP protocol. These are also a major source of infections.

Most of the internet surfers are unaware of the lurking dangers. The system administrator should eliminate this weak human chink from the network security. The end users should be effectively shielded from the social engineering deployed by the malware writers.

The Gateway AV should be configured to examine the HTTP protocol data stream. FTP over HTTP should also be monitored.
Granular Control Over Gateway Anti-Virus Solution

Lack of propel configuration and control of A Gateway AV mars its Performance.

A Gateway anti-virus solution is a powerful security tool. The power has to be harnessed and configured properly. The system administrator should have complete control over the scanning policies and priorities to utilize the power of the solution.

Lack of proper configuration and control of a Gateway AV mars its performance. It can lead to a bottleneck at the gateway level or can leave loop-holes in the security. Instead, if an antivirus solution is fine tuned to inspect specific protocols based on the source and destination of the traffic and configured to give a customized response on detection, it proves very effective.

If the Gateway AV is a part of a United Threat Management (UTM) solution, it might be bale to provide the granular controls that enables the administrator to block certain files. Moreover, an UTM has its hand on the pulse of the network. A classical UTM involves Anti-spam, Firewall, IDP, Traffic Discovery, Band Width Control, and Content Filtering, apart from the anti-virus solution. So, the Gateway AV will be sensitized to multiple parameters and have fine granular controls to devise user based policies.

Summary

The threat of malware is not going to vanish or fade away. As the malware generators get more and more specific to maximize the economic outcome, the enterprise networks will never be a safe enough. The Gateway AV solution should be powerful enough to guide the complete protocol spectrum and it should have a granular control which makes it easily configurable. It should be intelligent enough to understand what is has to protect and be potent enough to protect it.

About Cyberoam

Cyberoam Unified Threat Management appliance recently announced the introduction of an advanced version of Intrusion Detection and Prevention solution. Cyberoam's Single Sign-On pinpoints the source of internal threats by the username. This ensures highest levels of security even in Wi-Fi and DHCP environments with dynamic IP allocation. Cyberoam UTM, with its multi-policy capability, allows administrators to configure different user based policies.