Comparison of Firewall, Intrusion Prevention and Antivirus Technologies

(How each protects the network)

Dr. Gaurav Kumar Jain
Regional College For Education, Research and Technology
Email: gaurav.rinkujain.jain@gmail.com
Mr. Pradeep Sharma
Regional College For Education, Research and Technology
Mukul Verma
Regional College For Education, Research and Technology

Abstract— **Widely connected enterprise networks and the Internet have enabled viruses, worms and blended threats to make use of computer networks for propagation, significantly increasing the speed of infection and damage. The Internet, with its ease of sharing and downloading of files, has also increased the risk of infection to the average user. A user may infect a computer by an action as simple as clicking on a downloaded file or an email attachment. Investment on several layers of protection is required for most enterprises for effective protection of computer networks.**

Index Terms— **enterprise network, viruses, worms, blended threats.**

1.0 Introduction

Network attacks are increasing both in sheer number as well as complexity. In recent news, we have seen how viruses, worms and other attacks can cause major business disruptions and cost companies worldwide billions of dollars. For instance, the Blaster worm infected over 1.2 million computers worldwide, and the SoBig.F virus infected over 100,000 computers[1].

Viruses and worms are all examples of what are generally known as malicious programs or malware for short. A virus is just a program that tells the computer to do something that the user does not want it to do. It requires a host program to live and infects other files so that it can "live" longer. A virus can perform destructive actions, such as displaying irritating messages, overwriting hard drives, or rendering the machine inoperable.

A worm is a program that replicates itself and spreads through network connections to infect other machines, eating up bandwidth and storage space and slowing computers down. Some worms use email to send messages to other users, while others use application vulnerabilities to replicate via the network. The distinction between viruses and worms is beginning to blur, as many viruses today also use email as their means of propagation.

"Blended threats", such as Code Red and Nimda, are sophisticated attacks that use multiple methods and techniques to propagate and inflict damage, thus spreading very rapidly and causing significant productivity disruptions. Blended threats can be part virus, part worm, and part backdoor[2].

Widely connected enterprise networks and the Internet have enabled viruses, worms and blended threats to make use of computer networks for propagation, significantly increasing the speed of infection and damage. The Internet, with its ease of sharing and downloading of files, has also increased the risk of infection to the average user. A user may infect a computer by an action as simple as clicking on a downloaded file or an email attachment.

2.0 Technologies for Network Security

In this paper, we look at network security technologies that are used to protect computer networks and mitigate the risks associated with viruses, worms and other network attacks. For effective protection of computer networks, most organizations are deploying multiple layers of security, including firewall, intrusion prevention and gateway antivirus technologies. Understanding the different kinds of protection provided by each technology is helpful in deciding what systems are required for each network.

Network security technologies can be broadly classified into four categories:

Packet level protection, such as routers' Access Control Lists (ACL) or stateless firewalls

Session level protection, such as stateful inspection firewalls

Application level protection, such as proxy firewalls and intrusion prevention systems (IPS)

File level protection, such as gateway antivirus systems

Figure 1 compares the four categories of network security technologies. Evaluation of each category by coverage of protocols/applications, level of protection, and relative performance enables organizations to choose the appropriate network security technologies to protect their networks.

	Packet Level Protection	**Session Level Protection**	**Application Level Protection**	**File Level Protection**
Examples	Packet filtering (router ACLs or stateless firewalls)	Stateful inspection firewalls	Intrusion prevention systems (IPS) and proxy firewalls	Gateway antivirus
Mechanism	Examine packet header	Examine packet header and control fields	Examine application fields	Examine files inside application traffic
Protocol and Application Coverage	N.A. packet level	Large	Medium	Small (email, web and file transfers)
Protection Provided	Client-to-server and server-to-client	Client-to-server and server-to-client	Mainly client-to-server	Mainly server-to-client
Relative Performance	High	High	Medium	Low

Figure 1. Comparison of network security technology categories

3.0 Packet Level Protection

Packet level protection, also known as packet filtering, is one of the most widely used means of controlling access to a network. The concept is simple: determine whether a packet is allowed by comparing some basic pieces of information in the packet headers. Cisco IOS Access Control List (ACL) is one of the most used packet filters. IP Chains is also a popular packet filter application, which comes bundled with many versions of Linux.

Two-way communication presents a challenge for

network security based on packet filtering. If one blocks all incoming traffic, one prevents responses to outgoing traffic from coming in, disrupting communication. Consequently, one has to open two holes, one for outgoing traffic and one for incoming traffic, without enforcing any association of the incoming traffic with existing outgoing connections in the network. Packet filtering thus can allow in crafted malicious packets that appear to be part of existing sessions, causing damage to protected resources.

Packet filtering devices do not track dynamic protocols, where a server and a client negotiate a random port for data transmission. Examples of

protocols that use dynamic ports include FTP, RPC, and H.323. To enable these applications to pass through packet filtering systems, one has to open a very large hole, significantly reducing the security protection provided by packet-filtering systems. For instance, in order to allow in standard FTP, one must let through any traffic with a destination port greater than 1,023 (1,023 – 65,500) and source port of 20, thus opening a significant security hole in the network.

4.0 Session Level Protection

Session level protection technologies control the flow of traffic between two or more networks by tracking the state of sessions and dropping packets that are not part of a session allowed by a predefined security policy. Firewalls that implement session-level protection keep state information for each network session and make allow/deny decisions based on a session state table. The most common systems for session level protection are stateful inspection firewalls.

Note that session level protection technologies are "session based," meaning that firewalls go beyond individual TCP connections to involve many such connections. Session-level firewalls support dynamic protocols by identifying port change instructions in client-server communication and comparing future session's against these negotiated ports. For instance, to track FTP sessions, the firewall inspects the control connection, used for issuing commands and negotiating dynamic ports, and then allows in various data connections for transferring files.

Because session level protection provides all the benefits of packet level protection without the limitations, it renders packet level protection unnecessary for most networks.

5.0 Application Level Protection

Application level protection technologies monitor network traffic and dynamically analyze it for signs of attacks and intrusions. Within the network security infrastructure, two common technologies for application level protection are proxy firewalls and Intrusion Prevention Systems (IPS).

Proxy firewalls are network systems that act on behalf of the client accessing a network service and shield the client and the server from direct peer-to-peer connection. The client establishes a connection with the proxy server, and the proxy server establishes a connection with the destination server. The proxy then forwards the data between the parties.

IPS are network devices that can accept or deny traffic based on IP addresses, protocol/service, and application level analysis and verification. IPS receive traffic from the network, reassemble the traffic streams and look at application primitives and commands to detect suspicious fields that warrant some predefined action. These actions vary from logging suspicious events to dropping the connection completely.

Proxy firewalls and IPS examine control and data fields within the application flow to verify that the actions are allowed by the security policy and do not represent a threat to end systems. By understanding application-level commands and primitives, they can identify content out of the norm and content that represents a known attack or exploit. Proxy firewalls and IPS perform IP de-fragmentation and TCP stream reassembly as well as eliminating ambiguity within traffic, which can be used by malicious users trying to conceal their actions.

Proxy firewalls usually support the common Internet applications, including HTTP, FTP, telnet, rlogin, email and news. Yet, a new proxy must be developed for each new application or protocol to pass through the firewall, and custom software and user procedures are required for each application.

IPS generally support a wider range of protocols and applications, including those required to protect the network against attacks from the Internet. New applications can be allowed through an IPS without requiring changes to the user workstations. In this way, IPS are more transparent to the network than proxy firewalls.

Proxy firewalls and IPS can detect certain viruses or Trojans by looking at application service fields. For instance, IPS can look at the subject field, attachment name, or attachment type within email traffic to detect characteristics of known viruses. However, application level protection does not do a detailed analysis at the file level, which is also required to detect the large number of viruses in existence.

6.0 File Level Protection

File level protection provides the ability to extract files within traffic and inspect them to detect malware, including viruses, worms or Trojans[3]. A common technology for file level protection in a network is gateway antivirus.

An antivirus system looks for virus signatures – a unique string of bytes that identifies a virus – and zaps the virus from the file. Most antivirus scanning systems catch not only the initial virus but also many of its variants, since the signature code usually remains intact.

Gateway antivirus systems scan files that are embedded in network traffic, including files in HTTP traffic (web downloads) and files in email traffic (attachments). If an infected file is detected, a gateway antivirus system removes it from the traffic, so it does not affect other users. To scan files within network traffic, gateway antivirus must understand a broad range of file encoding protocols (i.e., MIME, uucode, Base64) and file compression algorithms.

Since there are over 60,000 known viruses, gateway antivirus systems must be able to conduct thorough scans. Constant updates to the virus pattern file are required for effective protection against new virus outbreaks, since new

viruses are continuously being uncovered[4].

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

Antivirus typically scans files in email and web traffic, mainly inspecting communication from servers to clients. Viruses are aimed at damaging end user systems, but use various email and web servers to propagate. Consequently, it is important to detect viruses while they are being uploaded to or downloaded from servers.

7.0 Example

Network security technologies at the network level, session level, application level and file level are used by organizations to add layers of protection in the network against viruses, worms and other network attacks. Note that session level protection offers the security of packet level protection without the limitations, so it makes packet level protection unnecessary for most networks.

Figure 2 illustrates the inspection functions that take place as the packets are analyzed by stateful firewall for session level protection, Intrusion Prevention Systems (IPS) for application level protection and gateway antivirus for file level protection.
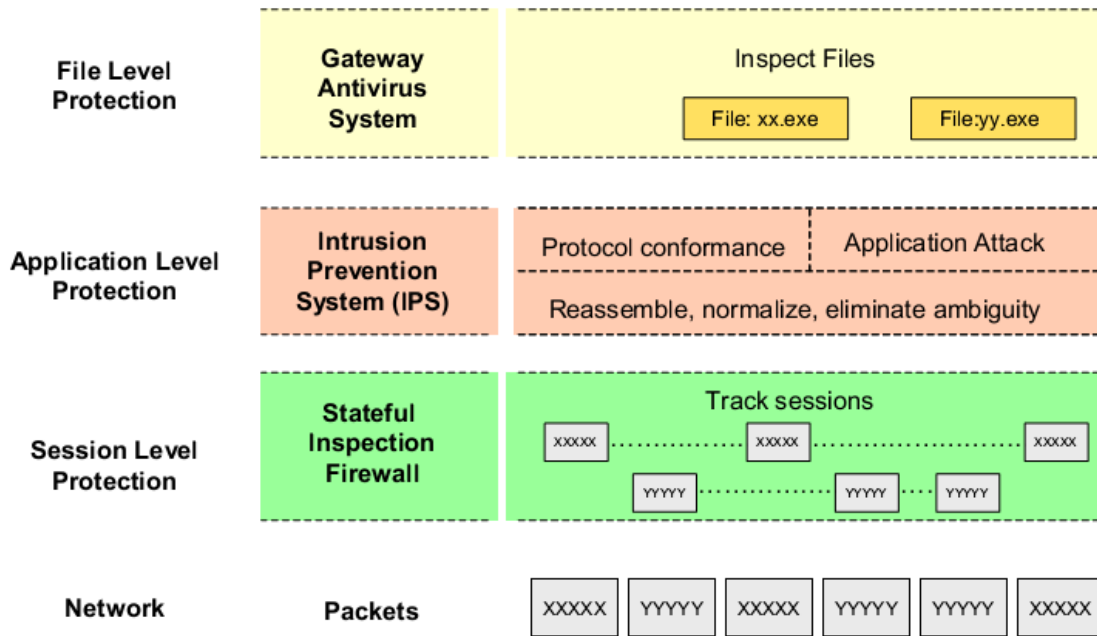
Figure 2. Network packets are inspected by session level protection, application level protection and file level protection technologies in order to defend the network from viruses, worms and other network attacks.

8.0 CONCLUSION

Organizations must deploy multiple security technologies to protect networks against viruses, worms and other sophisticated attacks. Stateful inspection firewalls offer protection at the session level, proxy firewalls and Intrusion Prevention Systems at the application level, and gateway antivirus at the file level. Investment on all these levels of protection is required for
most enterprises for effective protection of computer networks.

REFERENCES

[1.] http://www.tech-faq.com/network-attacks.html

[2.] www.ehow.com/about_6375469_blaster-worm_.html

[3.] http://blasterworm.net/

[4.] www.expresscomputeronline.com/20080728/securityspecial02.shtml

[5.] http://en.wikipedia.org/wiki/Code_Red_(computer_worm)

[6.] virus.wikia.com/wiki/Nimda

[7.] en.wikipedia.org/wiki/Backdoor_(computing)

[8.] khodenko.tripod.com/Firewalls

[9.] http://pl.safensoft.com/security.phtml?c=587

[10.] www.protocols.com/pbook/h323.htm

[11.] www.webopedia.com/TERM/P/proxy_server.html

[12.] http://en.wikipedia.org/wiki/Application_firewall