System Insecurity - Firewalls

Youngtae Ryu

Department of MIS, Pusan University of Foreign Studies

Abstract

The firewall is normally an intermediate system between the secure internal networks and the less secure external networks. It is intended to keep corporate systems safe from intruders, hackers, and accidental entry into the corporate system.

The primary types of firewalls are screening routers, proxy servers, and stateful inspectors. Encryption is another form of firewall protection which is being incorporated along with other firewall methods.

Before choosing a firewall architecture, a company must have the right mind set about the threat. The future will see more integration of firewall technologies and the increased use of standards in the industry. It must also determine what are the possible consequences of a breach in security and then develop a system to counter the threat.

Additionally, new firewall technologies will address the potential dangers associated with the use of Java applets and Active X-controls on the Internet.

I. Introduction

Internet connection sharpens the competitive edge of most businesses today since it gives them and their customers timely access to information. The use of the Internet spawns a new set of responsibilities and burdens for information systems(IS) departments. Internet and general purpose computing were not designed to provide any great degree of security. The recent denial-of-service attacks on Amazon.com, eBay, Yahoo, and other Web sites show the vulnerabilities of information technology(IT) architectures. IS must deliver reliable Internet services to corporate users while ensuring that systems and information stay secure from outside threats.

An enterprise using Intranet must install firewalls to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users must have access. A recent survey of key Internet hosts found that essentially 31 percent were wide open to potential attackers and 33 percent had a high risk of potential problems.

The increased accessibility to information has not come without a price.

Any time information is distributed on any type of network, there is the potential that such information will be accessed by unauthorized persons. Allowing access to authorized individuals may inadvertently allow the intelligent intruder to gain access for snooping or malicious purposes. Whether it is a computer "hacker" intentionally trying to gain access or an unintentional intrusion, the potential for lost or altered information is enormous.

So how do companies protect themselves and their information? Many companies are turning to firewalls as a means of attaining these goals. Thus, this research intends to investigate the status of firewalls and suggest some managerial issues within organization in Korea.

II. What is a firewall?

A firewall provides an important tool for protecting a corporate network from Internet intrusions. A network firewall is a hardware/software barrier between a corporate network and Internet. A firewall is also an intelligent device that controls traffic between two or more networks for security purposes. Basically, a firewall, working closely with a router program, filters all network packets to determine whether to forward them to their destination. A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks.

A fire wall usually consists of a UNIX or Windows NT computer running special firewall software. Other hardware platforms such as routers can also run firewall software. Although this software is usually associated with Internet connections, it can be used to control traffic between parts of an intranet or between networks of different corporations. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

Typically, firewalls employ one of three architectures known as screen routers, proxy servers, and stateful inspectors. By combining the strengths of more than one approach, the firewall can be more effective. Many commercial firewalls employ more than one technique to provide data protection.

II.1 Screening Routers

One of the less complex architectures is screening. This method screens requests to make sure they come from acceptable (previously identified) domain names and IP addresses. A screening router applies a set of rules to each incoming information packet and decides whether it should be forwarded (or not) to the internal system. The screening router filters packets based on information that is available in packet headers; such as protocol numbers, source and destination addresses and port numbers, and connection flags. Through this process, the router "screens" the information, allowing only approved information to pass through. The router serves an additional function of "routing" the information to the appropriate network or user.

The primary advantage of using screening routers is the low hardware costs and relative simplicity. The screening process is straight forward and the computing requirements are not excessive. Screen routers do have some important disadvantages. For example, it is difficult to set up the packet filter rules correctly. The possible combinations of sending addresses, receiving addresses, protocols, and flags make it difficult to establish rules which apply correctly in every situation and it is expensive to manage screening routers. Requirements continually change with more and more addresses required to be added to the "allowable" address lists. The screening router method also lacks user-level authentication protection. For that reason, a packet may be a "spoof" meant to look like an authorized and legal packet while in fact it has just breached the "firewall."

II.2 Proxy Servers

A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. The user validation may only require user identification and a password or it may be more robust depending on the security desired. An example of robustness is the use of one-time passwords and a challenge-and-response system.

The advantages of proxy servers overcome some of the disadvantages of the screening routers. For instance, the proxy server employs user-level authentication procedures which can provide some protection from spoofing which could fool the screening router. The proxy server also provides logging and accounting information. This is very useful in detecting intrusions

and intrusion attempts. It can also be used to document system use and communications workloads.

The major disadvantage of the proxy server results from the requirement to build an application-layer gateway for each application. This requirement may severely limit the deployment of new applications or at least delay them excessively. For full benefit of the proxy server, there is no alternative other than building each gateway. The Internet protocol uses packets as described in the previous section to allow access directly with the intended destination. A proxy server interrupts this direct connection by introducing a gateway between the open network and the local network. To pass through this gateway, the outside location must address the "proxy" directly and ask for access to the intended recipient.

Upon contact, the proxy asks the user for the name of the remote host to be accessed. The user will respond with the host name, valid user identification and authentication information. Only then will the proxy server contact the host and relay packets between the two communication points. The user validation may only require user identification and a password or it may be more robust depending on the security desired.

II.3 Stateful inspectors

But can a company feel safe if the packet is addressed correctly and the user authenticates appropriately? Apparently not since several firewall products now incorporate an inspection module called a stateful inspector. This module is software that inspects packets to verify the application, user, and transportation method. By looking inside the packet, the inspector can also investigate the possibility of harmful viruses hiding in audio or video packets. A special case of the stateful inspector involves Java and X-Control protection which will be discussed later. The major advantage of the stateful inspector is the ability to detect some intrusion attempts which would otherwise pass through a firewall. By looking into the packet rather than just at the header information, additional protection is afforded.

The primary disadvantage is the high maintenance activity involved with stateful inspectors. The stateful inspector also adds some delay to the transfer of data. If the purpose is to find potentially damaging information, the application must be continually updated to recognize new viruses or intrusive applets.

II.4 Encryption and firewalls

Encryption is generally not considered a part of the firewall architecture on the other hand encryption provides many of the safeguards associated with firewalls. Encryption can provide firewall protection in several ways. First, by encrypting passwords and authentication procedures, eavesdroppers are not able to copy passwords for later use in spoofing the system. Second, without the correct key, any encrypted data sent by an intruder would translate into unintelligible random characters and therefore have no meaning to the receiving system. Such corrupted data would not pass data checks on the host computer and could not be used to insert rogue viruses or programs into the host system. Third, any intruder reading corporation data being transmitted on an open network would not be able to gather any intelligence.

One use of encryption, called tunneling, is similar to the use of the proxy server firewall. At the transmitting end, the entire packet is encrypted using a company specific key. Prior to sending the packet, an unencrypted header is added which addresses the proxy server at the destination. Upon receiving the packet, the proxy server strips off the unencrypted header and deciphers the packet. If the now unencrypted header meets the protection criteria of the proxy server, the packet will be sent on to the intended host system. This method combines the advantages of encryption and the proxy

server.

One disadvantage of encryption is more political than technical. Some countries do no allow encrypted data to be transmitted or received within their borders. The United States has also placed some limits on what encryption techniques can be used outside the U.S. borders. Another disadvantage of encryption is the added cost, complexity, and data transfer delays. Adding encryption adds to the complexity of the required architecture and the network processes and then there is the added time delay as data is encrypted and later deciphered. While this disadvantage is certainly worth considering, many corporations consider it a cost of doing business in a secure manner.

III. Firewall management and architecture

Once a company has recognized that the threat exists, it must try to determine just what is the threat, how much vulnerability is acceptable, and what is needed to stop the threat. Knowing the network infrastructure is of paramount importance. The world's greatest firewall will not protect the corporate WAN from a modem in a workstation that is logged on to the corporate network and is running communications software. Nor can it protect the corporate WAN from people using their names for passwords. Threats such as these must be approached from a corporate network security viewpoint rather than relying only on firewalls.

Assuming that the internal environment has been secured, what is the threat from the external environment? If legitimate users can access critical corporation information from outside the internal network, so can the foe. The company must determine what damage can be inflicted by intrusion. Is the potential risk acceptable? Is it more appropriate to allow some intrusion than to burden the legitimate users? What would be the effect on company operations, should data files be corrupted or rouge programs be inserted into company computers? These questions must be answered prior to developing a firewall strategy. For example, if the company wants outsiders to access a corporate database to allow them to interface more efficiently with the company, it may be wise to provide a replicated database on a standalone system for such access.

On the other hand, if highly sensitive data with competitive advantage implications is routinely sent over unsecured networks, it may be wise to install firewalls and encryption. It should by obvious that the corporation must understand the possible effects of a breach in security and attempt to eliminate or minimize the threat.

Once firewalls are in place, it is important to monitor their activity. Firewall monitoring can provide a significant amount of information about your system security. For example, it can identify the number of times a threat was detected and countered. Monitoring may also provide clues of unsuccessful detection by monitoring actual access to your internal system. Additionally, it is important to monitor firewall performance to determine the system performance degradation attributable to the firewall. Severe degradation must be address through upgrades in hardware and/or software. If security breaches are detected, a recovery process must be in-place to systematically determine the damage and provide recovery operations.

Once a firewall is operational, it is important to remain knowledgeable about firewall advances and emerging threats. Firewall technology will continue to advance providing the capability for increased protection. Changes in system architecture or data requirements may also require a change to the company's firewall strategy.

IV. Recent firewall advances and the future

The advance of Java programmed applets and Active X-controls have made protecting internal systems tied to the

Internet more difficult. One recent advance is a firewall that resides on a desktop or notebook and helps protect users against faulty and malicious Java applets and Active X-controls, Trojan horses (programs that perform an illicit activity as they run), and rogue E-mails. While this is not a firewall in the traditional sense because it does not reside as an intermediate system between the open systems and the internal system, it does provide additional security from unwanted intrusion.

Another advance is in the area of integrated firewalls. Routers that combine standards-based encryption, authentication, tunneling and firewall security into a single device optimized for Extranet should are forthcoming. The principal advantage is the guaranteed compatibility between security processes and the provision for greater security with less architectural complexity.

Future products should incorporate more industry standards. This is important because today, many encryption packages are vendor specific and unable to communicate with products from other vendors. Better agreement on industry standards should allow greater growth in the security protection arena just as it allowed greater growth in the personal computer market.

References

Anonymous (2000), Act Now to Protect Your Data, *Informationweek*, (775): pp. 101-104. Feb 28.

Elgar, Eric. (1997), "Firewalls set networking arena ablaze", *Computer Reseller News*, (734): pp. 183,198. May 5.

Farmer, Dan. (1996), Shall We Dust Moscow, http://www.fish.com/survey/introduction.htm.

Franklin, Curtis F Jr. (1997), "Enter the extranet", *CIO*, 10(15): pp. 106-112. May 15.

Frook, John Evan. (1997), "User Shares Secret Data Via Intranet", *Communicationsweek*, (651): pp. 1,72. Feb 24.

Gips, Michael A. (1997), "Wipeout", *Security Management*, 41(5): pp. 21-22. May

Girishankar, Saroja. (1997), "New Class of Routers Keeps Extranet Safe New devices will combine security and routing features", *Communicationsweek*, (672): pp. 1,73. Jul 14.

Greenfield, David. (1997), "Safe Internet Surfing", *Data Communications*, 26(1): pp. 90-92. Jan.

Henthorn, Alex. (1997), "How secure is your Internet security plan?", *As/400 Systems Management*, 25(4): pp. 34-36. Apr.

Michener, John. (1999), Systems Insecurity in the Internet Age, *IEEE* Software, 16(4): pp. 62-69, July/August.

Thompson, Amy. (1997), "Smoking out the facts on firewalls" *Security Management*, 41(1): pp. 24-30. Jan.