A

Seminar report

on

“Firewall”

Submitted in partial fulfillment of the requirement for the award of degree
Of Bachelor of Technology in Computer Science

SUBMITTED TO:

www.studymafia.org

SUBMITTED BY:

www.studymafia.org

Preface

I have made this report file on the topic **Firewall**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

INTRODUCTION

The Internet has made large amount of information available to the average computer user at home, in business and education. For many people, having access to this information is no longer just an advantage; it is essential.

By connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. The intruders could gain access to your sites private information or interfere with your use of your own systems.

Users who connect their computers to the Internet must be aware of these dangers, their implications and how to protect their data and their critical systems. Therefore, security of network is the main criteria here and firewalls provide this security.

The Internet firewalls keep the flames of Internet hell out of your network or, to keep the members of your LAN pure by denying them access the all the evil Internet temptations.

What is a Firewall?

- A Firewall is simply a program or hardware device that filters the information coming through the internet connection into your private network or computer system.

What is an application firewall?

An application firewall is a special firewall that is specifically coded for the type of traffic it is inspecting. The most widely developed application firewall is the web application firewall.

A web application firewall is less concerned with source and destination addresses, and focuses on the actual data in the packet to see if the requests being sent to a web server, and the replies issued from the web server, meet its rules.

For example, a web application firewall may have a rule that says a requested URL may not be more than 256 characters long. When a packet is found that has a longer URL in the request field it can be dropped without giving it to the web server.

What is the difference between a host-based firewall and a network-based firewall?

A host-based firewall is installed on an individual computer to protect it from activity occurring on its network. The policy may affect what traffic the computer accepts from the Internet, from the local network, or even from itself.

A network-based firewall is implemented at a specified point in the network path and protects all computers on the "internal" side of the firewall from all computers on the "external" side of the firewall.

Network-based firewalls may be installed at the *perimeter*, or *edge*, of a network to protect a corporation from hosts on the Internet, or *internally* to protect one segment of the community from another, such as separating corporate and residential systems, or research systems from marketing systems. A network-based firewall cannot protect one computer from another on the same network, or any computer from itself.

Hardware firewall vs Software firewall

Hardware firewalls

Hardware firewalls are integrated into the router that sits between a computer and the Internet. They typically use packet filtering, which means they scan packet headers to determine their source, origin, destination addresses and check with the existing user defined rules to make an allow/deny decision.

Key advantages of hardware firewall.

1. Speed: Hardware firewalls are tailored for faster response times, so it can handle more traffic loads.
2. Security: A firewall with its own operating system is less prone for attacks. This in turn reduces the security risk and in addition, hardware firewalls have enhanced security controls.
3. No Interference: Since the hardware firewall is an isolated network component, it can be managed better, and does not load or slowdown other applications. The firewall can be moved, shutdown, or reconfigured with minimal interference to the network.

Software firewall

Software firewalls are installed on individual servers. They intercept each connection request and then determine whether the request is valid or not. Software firewall process all requests by using the server resources. Apart from performance limitation, the software firewall has numerous advantages.

Key advantages of software firewall.

1.While comparing with the hardware firewalls, software firewalls are easier to configure and setup.
2.Through the software firewall, we can restrict some specific application from the Internet. This makes the software firewall more flexible.
3.The software firewall give users complete control on their Internet traffic through a nice user friendly interface that requires little or no knowledge.

History of Firewalls

Firewall technology first began to emerge in the late 1980s. Internet was still a fairly new technology in terms of its global usage and connectivity. The original idea was formed in response to a number of major internet security breaches, which occurred in the late 1980s.

In 1988 an employee at the NASA Ames Research Center in California sent a memo by email to his colleagues that read, "We are currently under attack from an Internet VIRUS! It has hit Berkeley, UC San Diego, Lawrence Livermore, Stanford, and NASA Ames." This virus known as the Morris Worm was carried by e-mail and is now a common nuisance for even the most innocuous domestic user.

The Morris Worm was the first large scale attack on Internet security, of which the online community neither expected, nor were prepared for. The internet community made it a top priority to combat any future attacks from happening and began to collaborate on new ideas, systems and software to make the internet safe again.

The first paper published on firewall technology was in 1988, when Jeff Mogul from Digital Equipment Corp. developed filter systems know as packet filter firewalls. This fairly basic system was the first generation of what would become a highly evolved and technical internet security feature. From 1980-1990 two colleagues from AT&T Bell Laboratories, Dave Presetto and Howard Trickey, developed the second generation of firewalls known as circuit level firewalls.

Publications by Gene Spafford of Purdue University, Bill Cheswick at AT&T laboratories and Marcus Ranum described a third generation firewall known as application layer firewall, also known as proxy-based firewalls. Marcus Ranum's work on the technology spearheaded the creation of the first commercial product.

The product was released by Digital Equipment Corporation's (DEC) who named it the SEAL product. DEC's first major sale was on June 13, 1991 to a chemical company based on the East-Coast of the USA.

At AT&T Bill Cheswick and Steve Bellovin were continuing their research in packet filtering and developed a working model for their own company based upon their original 1st generation architecture. In 1992, Bob Braden and Annette DeSchon at the University of Southern California were developing their own fourth generation packet filter firewall system.

The product known as "Visas" was the first system to have a visual integration interface with colours and icons, which could be easily implemented to and accessed on a computer operating system such as Microsoft's Windows or Apple's Mac/OS. In 1994 an

Israeli company called Check Point Software Technologies built this in to readily available software known as FireWall-1.

A second generation of proxy firewalls was based on Kernel Proxy technology. This design is constantly evolving but its basic features and codes are currently in widespread use in both commercial and domestic computer systems. Cisco, one of the largest internet security companies in the world released the product to the public in 1997.

Design goals for a firewall

- The first design goal for a firewall is that collectively the sum of all the network traffic from internal to external must go through the firewall physically cutting off all access to the local network except via the firewall.

- The second design goal would be only authorized traffic which is delineated by the local security policy will be allowed to proceed.

- Finally the last design goal is that the firewall itself is resistant to penetration inclusive is a solid trustworthy system with a protected operating system.

Types of firewalls

Three common types of Firewalls:

- Packet-filtering routers
- Application-level gateways
- Circuit-level gateways (Bastion host)

Packet-filtering Router

- Applies a set of rules to each incoming IP packet and then forwards or discards the packet
- Filter packets going in both directions
- The packet filter is typically set up as a list of rules based on matches to fields in the IP or TCP header
- Two default policies (discard or forward)

Advantages:

- Simplicity
- Transparency to users
- High speed

Disadvantages:

- Difficulty of setting up packet filter rules
- Lack of Authentication

Application-level Gateway

- Also called proxy server
- Acts as a relay of application-level traffic

Advantages:

- Higher security than packet filters
- Only need to scrutinize a few allowable applications
- Easy to log and audit all incoming traffic

Disadvantages:

- Additional processing overhead on each connection (gateway as splice point)

Circuit-level Gateway

- Stand-alone system or
- Specialized function performed by an Application-level Gateway
- Sets up two TCP connections
- The gateway typically relays TCP segments from one connection to the other without examining the contents
- The security function consists of determining which connections will be allowed
- Typically use is a situation in which the system administrator trusts the internal users
- An example is the SOCKS package

Bastion Host

- A system identified by the firewall administrator as a critical strong point in the network´s security
- The bastion host serves as a platform for an application-level or circuit-level gateway

Basic concepts of a firewall

To understand what a firewall is, one can simply imagine it in biological terms as the organ of a human known as skin. Skin does not actually kill foreign hostile bodies, it simply obstructs them.

In a human for example, the loss of more than 50% of skin will result in death, simply because the immune system cannot repel invaders from such a large and exposed surface area. The same can be said of firewalls which unlike IDS (Intrusion Detection Systems) can not actually detect hostile invaders but simply limits their access to your sensitive internal servers.

Properly designed and deployed, a firewall operates as a shield around your network just as skin on a human.

A firewall functions by acting on traffic based on its policy. A policy is comprised of a set of rules. A rule is an action taken on traffic that fit a certain criteria. A single rule is comprised of four basic elements:

- **Source**
  - This is where the IP traffic is coming from and is comprised of the following
  - Single IP address or multiple IP addresses
  - One or more networks in the form of a network ID and subnet mask
  - A combination of IP addresses and Network addresses
- **Destination**
  - This is where the IP traffic is going to and is comprised of the following
  - Single IP address or multiple IP addresses
  - One or more networks in the form of a network ID and subnet mask
  - A combination of IP addresses and Network addresses
- **Service**
  - This is the type of protocol that the traffic is using and is comprised of the following
  - One or more destination TCP ports
  - One or more destination UDP ports
  - A group or combination of destination TCP and UDP ports
  - Although source port can be limited to a certain range, it is generally left wide open. It is the destination port that is primarily specified.
- **Action**
  - The administrator chooses from the following options if all the above three criteria match
  - Reject the traffic
  - Drop the traffic
  - Permit the traffic
  - Encrypt the traffic on IPSEC VPN capable firewalls

The Role of Firewalls

A firewall is a term used for a ``barrier'' between a network of machines and users that operate under a common security policy and generally trust each other, and the outside world. In recent years, firewalls have become enormously popular on the Internet. In large part, this is due to the fact that most existing operating systems have essentially no security, and were designed under the assumption that machines and users would trust each other.

There are two basic reasons for using a firewall at present: to save money in concentrating your security on a small number of components, and to simplify the architecture of a system by restricting access only to machines that trust each other. Firewalls are often regarded as some as an irritation because they are often regarded as an impediment to accessing resources. This is not a fundamental flaw of firewalls, but rather is the result of failing to keep up with demands to improve the firewall.

There is a fairly large group of determined and capable individuals around the world who take pleasure in breaking into systems. Other than the sense of insecurity that it has instilled in society, the amount of actual damage that has been caused is relatively slight. It highlights the fact that essentially any system can be compromised if an adversary is determined enough. It is a tried and true method to improve security within DOD projects to have a ``black hat'' organization that attempts to break into systems rather than have them found by your real adversaries. By bringing the vulnerabilities of systems to the forefront, the Internet hackers have essentially provided this service, and an impetus to improve existing systems. It is probably a stretch to say that we should thank them, but I believe that it is better to raise these issues early rather than later when our society will be almost 100% dependent on information systems.

Advantages of firewall

- Concentration of security all modified software and logging is located on the firewall system as opposed to being distributed on many hosts;
- Protocol filtering, where the firewall filters protocols and services that are either not necessary or that cannot be adequately secured from exploitation;
- Information hiding, in which a firewall can ``hide'' names of internal systems or electronic mail addresses, thereby revealing less information to outside hosts;
- Application gateways, where the firewall requires inside or outside users to connect first to the firewall before connecting further, thereby filtering the protocol;
- Extended logging, in which a firewall can concentrate extended logging of network traffic on one system;
- Centralized and simplified network services management, in which services such as ftp, electronic mail, gopher, and other similar services are located on the firewall system(s) as opposed to being maintained on many systems.

Disadvantages of firewall

- The most obvious being that certain types of network access may be hampered or even blocked for some hosts, including telnet, ftp, X Windows, NFS, NIS, etc. However, these disadvantages are not unique to firewalls; network access could be restricted at the host level as well, depending on a site's security policy.

- A second disadvantage with a firewall system is that it concentrates security in one spot as opposed to distributing it among systems, thus a compromise of the firewall could be disastrous to other less-protected systems on the subnet. This weakness can be countered; however, with the argument that lapses and weakness in security are more likely to be found as the number of systems in a subnet increase, thereby multiplying the ways in which subnets can be exploited.

- Another disadvantage is that relatively few vendors have offered firewall systems until very recently. Most firewalls have been somewhat ``hand-built'' by site administrators, however the time and effort that could go into constructing a firewall may outweigh the cost of a vendor solution. There is also no firm definition of what constitutes a firewall; the term ``firewall'' can mean many things to many people.

Conclusion

- One of the best things about a firewall from a security standpoint is that it stops anyone on the outside from logging onto a computer in your private network.
- While this is a big deal for businesses, most home networks will probably not be threatened in this manner. Still, putting a firewall in place provides some peace of mind.

References

www.studymafia.org

www.google.com

www.wilipedia.com