Defending with Firewalls

Session 11

LEARNING OBJECTIVES

On completion of this session you should:

- Understand why firewalls are necessary
- Discuss the design goals of firewalls
- Discuss what firewalls can and can not do
- Be familiar with different types of firewalls
- Describe the advantages and disadvantages of different types of firewalls
- Be familiar with various firewall configurations
- Discuss what level of security each configuration offers

Contents

Reading

Prescribed readings

Reading 1: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 389-391.

Reading 2: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 392-402.

Reading 3: Read the online material Introduction to Firewall by Brad Marshall.

Reading 4: Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 402-407.

11.0 Introduction

The ever increasing use of the Internet has made firewalls an absolute necessity for an organization to ensure high level of security. The software running in the internal network of an organization can never be guaranteed to be hundred percent secure and flawless. Hackers try to exploit flaws in the software running in the internal network to launch an attack. One way of reducing such risk is to have a sort of protective barrier. Firewalls, placed between the internal network and the Internet, act as the first line of defence against malicious users. If configured properly and used as a part of the overall security measures, firewalls can control access to an organization's internal network and improve security. In this study guide, we discuss the benefits and limitations of firewalls, and their various types and configurations.

11.1 What is a Firewall?

In the medieval age the use of firewall was evident in defending the castles. The main part of the castle was surrounded by tall walls and maybe one or two gates. The gates had guards and the traffic flow at the gates were restricted. The walls and gates provided certain level of protection against the invaders. The theory of protection by isolation and controlled traffic has sustained over a long period of time and is deployed in the network and security architecture of modern networks [2].

A firewall is essentially a combination of hardware and software used to implement security policies governing the network traffic between two or more networks, a trusted network and untrusted networks, using preconfigured rules or filters. It is an electronic partition between the trusted and untrusted networks, similar to the ancient firewall around the castles. A firewall serves as a primary line of defence against the external threats to organization's computer systems, networks, and critical information. It can also be used to partition organization's internal networks to reduce the risk from insider attack. Firewalls can be composed of a single router, multiple routers, a single host system or multiple hosts running firewall software, hardware appliances specifically designed to provide firewall services, or any combination thereof. They vary greatly in design, functionality, architecture and cost. For successful implementation of a firewall solution in an organization, it is important to understand what each firewall solution can or cannot do.

11.2 Firewall Design Goal

The followings are the design goals for a firewall identified by Bellovin [4,1]:

1. All traffic from inside to outside, and vice versa, must pass through the firewall. It is implemented by physically blocking all access to the local network except via the firewall.

2. Only authorized traffic, defined by local security policies, will be allowed to pass.

3. The firewall itself is immune to penetration. This underpins the use of trusted system with a secure operating system.

R. Smith [5,1] lists four general techniques that firewalls use to control access and enforce security policy:

- **Service control:** Determines the types of Internet services, inbound and outbound, that can be accessed. For example, it may filter traffic on the basis of IP address and TCP port number.

- **Direction control:** Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall.

- **User control:** Controls access to a service the user is attempting to have access. This feature is typically applied to users inside the firewall but may also be applied to incoming traffic from external users.

- **Behavior control:** Controls how particular services are used (e.g. filter e-mail to eliminate spam).

11.3 What Firewall can Do

Firewalls can offer the followings:

1. Firewalls manage access between the Internet and an organization's network. Without a firewall, security depends on individual host system, each host system on the network is exposed to attacks from outside. This means that the security of the network would depend on the "hardness" of each host's security features and the security of the whole system is then only as good as the weakest link.

2. Firewalls allow the network administrator to define a centralized "choke point" that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the protected network, and provides protection from various types of routing attacks. Firewall simplifies security management, since network security is consolidated on the firewall systems rather than being distributed to every host in the entire network.

3. Firewalls offer a convenient point where security related events can be monitored and alarms can be generated. Network administrators must audit and log all significant traffic through the firewall. If the network administrator doesn't take the time to respond to each alarm and examine logs on a regular basis, then deployment of firewall fails to achieve its purpose, since the network administrator will never know if the firewall has been successfully attacked.

4. For the past few years, the Internet has been experiencing an address space crisis that has made registered IP addresses a less plentiful resource. This means that organizations wanting to connect to the Internet may not be able to obtain enough registered IP addresses to meet the demands. An firewall is a logical place to deploy a Network Address Translator (NAT) that can help alleviate the address space shortage and eliminate the need to renumber when an organization changes Internet service providers (ISPs).

5. A firewall is the convenient point to audit or log Internet usage. These data gives the network administrator reasons to justify the expense of Internet connection to the management, pinpoint potential bandwidth bottlenecks, and provide a method for departmental charge-backs if this fits the organization's financial model.

There are arguments that the deployment of firewalls creates a single point of failure. It should be emphasized that, because we have deployed firewalls, security of individual host system can not be neglected. Appropriate security policies must also be implemented in individual host to ensure security of the organization's network.

11.4 What Firewall can not Do

Firewall cannot and does not guarantee 100% security of the network. To achieve greater protection, a firewall should be used in conjunction with other security measures. The limitations of the firewalls are the followings:

1. Firewalls cannot protect against attacks that do not go through the firewall. For example, if unrestricted dial-out is permitted from inside the protected network, internal users can make a direct connection to an ISP. Savvy users who become irritated with the additional authentication required by firewall proxy servers may be tempted to circumvent the security system by purchasing a direct SLIP or PPP connection to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees.

2. Firewalls cannot protect against the types of threats posed by traitors or unwitting users. Firewalls do not prohibit traitors or corporate spies from copying sensitive data onto disks or PCMCIA cards and removing them from a building. Firewalls do not protect against attacks where a hacker, pretending to be a supervisor or a befuddled new employee, persuades a less sophisticated user into

revealing a password or granting them "temporary" network access. Employees must be educated about the various types of attacks and about the need to guard and periodically change their passwords.

3. Firewalls cannot protect against the transfer of virus-infected software or files. Since there are so many different viruses, operating systems, and ways of encoding and compressing binary files, a firewall cannot be expected to accurately scan each and every file for potential viruses. Concerned organizations should deploy anti-viral software at each desktop to protect against their arrival from disks or any other sources.

4. Finally, Internet firewalls cannot protect against data-driven attacks. A data-driven attack occurs when seemingly harmless data is mailed or copied to an internal host and is executed to launch an attack. For example, a data-driven attack could cause a host to modify security-related files, making it easier for an intruder to gain access to the system. As we will see, the deployment of proxy servers on a bastion host is an excellent means of prohibiting direct connections from the outside and reducing the threat of data-driven attacks.

Reading 1:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 389-391.

11.5 Types of Firewalls

There are mainly three types of firewalls categorized on the technology used to protect the internal network (see Fig. 11.1 of the textbook). These are:

- Packet-Filtering Router
- Stateful Inspection Firewall
- Application-Level Gateway
- Circuit-Level Gateway

Packet-Filtering Router

A packet-filtering firewall is usually a router based firewall that applies a set of rules to each incoming IP packet and then forwards or discards the packet. It filters packets in both directions, to and from the internal network. As the router receives a packet, it examines the header of the IP packet to gather following information:

- Source IP address,
- Destination IP address,
- Source and destination TCP or UDP port number,
- Type of the protocol (IP, TCP, UDP or ICMP),
- Message type (SYN, ACK, FIN, RST).

The packet filtering router checks the above information against a set of rules. If there is a match to one of the rules, the rule is invoked to determine whether to forward or discard the packet. For example, the rules could state that [2]:

- All packets to a destination address be blocked
- All packets to a destination address be blocked except for a certain range of IP addresses
- Allow all packets going to specific TCP ports like Web (port 80), DNS (port 53), and SMTP (port 25) be allowed, while rest of the packets be dropped
- Do not allow any packets from external network with a source IP address of the internal network (anti- spoofing protection).

Packet-filtering firewalls have the following advantages:

1. Typically faster than other types of firewalls. Because packet filtering is done at the lower levels of the OSI model, the time it takes to process a packet is much quicker.
2. Can be implemented transparently, typically requires no additional configuration for clients.

3. Inexpensive to build routers with packet-filtering capabilities. The routers are already in the network providing routing functionality, thus avoids additional cost of deploying a firewall.

4. Packet filtering firewalls typically scale better than the other types of firewalls since they do not have the processing overhead that other types have.

5. Packet filtering firewalls are application independent.

However, they also suffer from the following disadvantages:

1. Lack of authentication, packet filtering firewalls do not perform user authentication.

2. Defining rules and filters on a packet filtering firewall can be a complex task.

3. The accuracy of the rules or filters on packet filtering firewalls can be very difficult to test.

4. Packet filtering firewalls are prone to certain types of attacks, e.g., DoS attack.

5. Packet filtering firewalls do not work well in an environment that needs dynamic rules.

Stateful Inspection Firewalls

Unlike the traditional packet filtering router, which makes its decision based on the information in the IP packet, the stateful inspection takes into consideration higher layer context by creating a directory of outbound established TCP connections.

A stateful packet inspection firewall reviews the same packet information as the packet filter, but also records information about TCP connections. It can thus prevent attacks like session hijacking.

Application-Level Gateway

An application-level gateway, also called proxy server, acts as a relay of application level traffic. Unlike packet-filtering firewall that operates at layer 3 & 4 of OSI model, a proxy-based firewall operates at layer 7, the application layer.

This type of firewall is usually implemented on a secure host system that is running proxy servers for each application needed by the end users on the internal network. The proxy server handles connections in both directions: request from internal client to external client and vice versa. Each internal client is configured to point to the proxy server for access to a specific application like FTP, Telnet, Web. For example, Internet browsers (Netscape, IE) can be configured for proxy authentication. Application gateway operates in the following ways:

- A client on the internal network requests access to an application (e.g. web access) on the external network.
- The request is forwarded to the proxy sever (e.g., HTTP proxy server) placed in the internal network.
- The proxy determines whether the request is valid (by comparing it to the rules or filters that implements the security policies of the organization) and then sends a new request on behalf of the client to the destination. Thus a direct connection from the internal to the external network is avoided and the request appears to have originated from the application gateway/proxy.
- Any response from the external network is sent back to the application gateway/proxy, which determines its validity and then sends it on to the client.

This type of firewall can effectively hide the internal network from the external untrusted network. It is important to note that the application gateway/proxy actually builds a new request, only copying known acceptable commands before sending it to the destination. The advantages of application-level gateways are the followings:

1. More secure than packet filters.
2. Only need to scrutinize a few allowable applications.
3. It is easy to log and audit all incoming traffic at the application level.
4. Allow the network administrator to have more control over traffic passing through the firewall.
5. Application gateways/proxies offer robust user authentication.

Application-level gateways have the following limitations:

1. The prime disadvantage is the additional processing overload on each connection. It makes an impact on the performance of the network and is slower than the packet-filtering firewall.

2. Each protocol (HTTP, SMTP, etc.) requires its own gateway/proxy application. If one does not exist, then the corresponding protocol will not be allowed through the firewall.

3. Typically requires additional client configuration.

4. Since all requests are channeled through the proxy server, the proxy can be a single point of failure.

5. Implementation cost can be high. The enhanced security of application gateways/proxies may require the purchase of additional hardware, software, expertise, or support, which in turn drives up the cost of the firewall solution.

Circuit-Level Gateway

This can be a stand-alone system or a specialized function performed by an application-level gateways for certain applications. A circuit-level gateway sets up two TCP connections instead of one:- one between itself and a TCP user on internal host, and another between itself and a TCP user on the outside host. Once these two connections are made, the gateway relays TCP segments from one connection to another without examining the content. The security function consists of determining which connections will be made. Circuit level gateways work at the session layer of the OSI model.

Firewall Basing

It is common to base a firewall on a stand-alone machine running a common operating system, such as UNIX or Linux. Firewall functionality can also be implemented as a software module in a router or LAN switch.

Bastion Host: a bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for application-level or circuit-level gateway. The system is most often software based and runs on a general-purpose computer that is running a secure version of the operating system.

Host-Based Firewalls: Firewall functionality is implemented as a software module used to secure an individual host, whose filtering rules can be tailored to the host environment and protection is independent of topology. These host-based firewalls when used with stand-alone firewalls provide an extra layer of protection.

Personal Firewall: controls the traffic between a personal computer or workstations on one side and the Internet or enterprise network on the other side. These firewalls are used in the home environment and/or corporate intranets. Firewall functionality is implemented as a software module in the personal computer.

When designing a firewall solution for an organization, there are a number of decisions that must be addressed by the network administrator. These are:

- overall security policy of the organization,
- type of firewall to be deployed,
- financial cost of the firewall.

Reading 2:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 392-402.

Reading 3:
Read the online material Introduction to Firewall by Brad Marshall.

11.6 Firewall Configurations

Apart from simple configuration consisting of single system, more complex firewall configurations are common in practice. The three common firewall configuration are:

Screened host firewall system (single-homed bastion host): This configuration consists of two systems: a packet filtering router and a bastion host. The configuration is such that only packets from and to the bastion host are allowed to pass through the router. The bastion host performs authentication and proxy functions. This offers more security than simple packer filtering router because, firstly, it implements both packet level and application level filtering, secondly, it makes it difficult for the intruder to penetrate two separate systems. The configuration offers flexibility in providing direct Internet access. In that outbound traffic may not be directed to the bastion host.

Screened host firewall system (dual-homed bastion host): In the above configuration, if the security of packet-filtering router is compromised, traffic may flow between the Internet and the internal hosts without passing through the bastion host. The dual-homed bastion host configuration physically prevents that from happening by forcing all traffic between the Internet and private network to flow through the bastion host.

Screened-subnet firewall system (Demilitarized Zone): This configuration offer more security than the other two configurations. This configuration has three components: two packet-filtering routers and one bastion host. One router is placed between the Internet and the bastion host, and the other between the bastion host and the internal network. This configuration creates an isolated subnet, called Demilitarized Zone (DMZ), between the two routers. Named after the buffer zone between opposing forces in a military peacekeeping scenario, the DMZ is a special separate network of servers to which external untrusted hosts have access, it really is just an area that is outside the firewall. This configuration offers several advantages [1]:

1. Three levels of defence.

2. The outside router advertises only the existence of the screened subnet to the Internet (internal network is invisible to the Internet).

3. The inside router advertises only the existence of the screened subnet to the internal network (the systems on the inside network cannot construct direct routes to the Internet).

Virtual Private Networks (VPNs): VPN consists of a set of computers that interconnect by means of a relatively unsecure network and that makes of encryption and IPSec to provide security. The Internet can be used to interconnect sites of a corporate network instead of the secure private network, and include a Firewall with IPSec at each corporate LAN site.

Distributed Firewalls: consists of a stand-alone firewall plus host-based firewalls working together under a central administrative control.

Reading 4:
Read W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011, pp. 402-407.

11.7 Conclusion

In today's Internet environment, firewalls are very much part of an organization's security infrastructure and their configuration and topology needs to be designed carefully. However, there is no single correct answer for the design and deployment of firewalls. Each organization's decision will be influenced by many different factors such as their corporate security policy, performance and reliability issues, the technical background of their staff, cost, and the perceived threat of attack.

11.8 References

[1] W. Stallings, Network Security Essentials - Application and Standard, 4th edition, Prentice Hall, 2011.

[2] K. M. Phaltankar, Practical Guide for Implementing Secure Intranets and Extranets, Artech House, 2000.

[3] J.H. Allen, The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001.

[4] S. Bellovin and W. Cheswick, "Network Firewalls, "IEEE Communication Magazine, 1994.

[5] R. Smith, Internet Cryptography, Reading, MA: Addision-Wesley, 1997.