Module 8

Network Security

Lesson 3

Firewalls

Specific Instructional Objectives

On completion of this lesson, the students will be able to answer:

- What a firewall is?
- What are the design goals of Firewalls
- What are the capabilities and limitations of Firewalls
- What are the possible types of Firewalls
    - Packet filters
    - Application-level gateways
    - Circuit-level gateways
- What are the possible configurations Firewalls
    - Single-homed system
    - Double-homed system
    - Screened subnet firewall system

8.3.1 Introduction

Many organizations have confidential or proprietary information, such as trade secrets, product development plans, marketing strategies, etc., which should be protected from unauthorized access and modification. One possible approach is to use suitable *encryption/decryption* technique for transfer of data between two secure sites, as we have discussed in the previous lesson. Although these techniques can be used to protect data in transit, it does not protect data from digital pests and hackers. To accomplish this it is necessary to perform user authentication and access control to protect the networks from unauthorized traffic. This is known as *firewalls*. A firewall system is an electronic *security guard* and *electronic barrier* at the same time. It protects and controls the interface between a private network and an insecure public network as shown in the simplified diagram of Fig. 8.3.1. It is responsible for partitioning a designated area such that any damage on one side cannot spread to the other side. It prevents bad things from happening, i.e. loss of information, without preventing good things from happening, that is controlled exchange of information with the outside world. It essentially enforces an access control policy between two networks. The manner in which this is implemented varies widely, but in principle, the firewall can be considered as a pair of mechanisms: one that is used to block traffic, and the other that is used to permit traffic. Some firewalls place more emphasis on blocking traffic, while others emphasize on permitting traffic. Probably the most important issue to understand of a firewall is the *access control policy* it implements. If a firewall administrator has no idea about what or whom he is protecting his network, what should be allowed and what should be prohibited, a firewall really won't help his organization. As firewall is a mechanism for enforcing policy, which affects all the persons behind it, it imposes heavy responsibility on the administrator of the firewall. In this lesson various issues related to Firewalls are discussed.

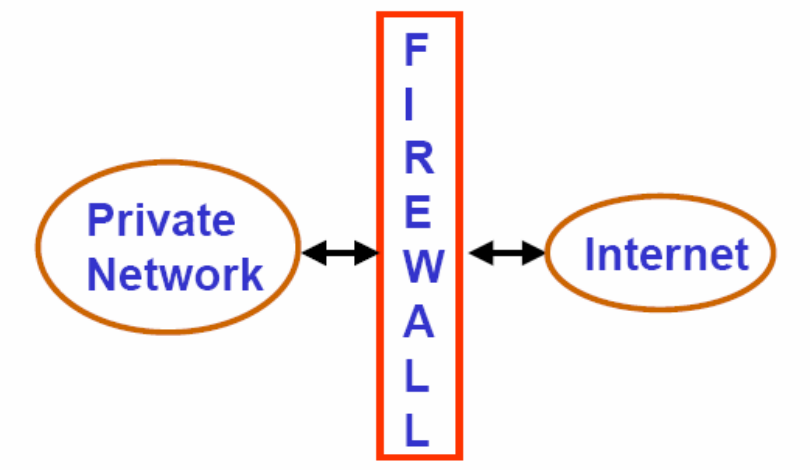

Figure 8.3.1 Schematic diagram of a firewall

8.3.2 Why a Firewall is needed?

There is no need for a firewall if each and every host of a private network is properly secured. Unfortunately, in practice the situation is different. A private network may consist of different platforms with diverse OS and applications running on them. Many of the applications were designed and developed for an ideal environment, without considering the possibility of the existence of bad guys. Moreover, most of the corporate networks are not designed for security. Therefore, it is essential to deploy a firewall to protect the vulnerable infrastructure of an enterprise.

8.3.3 Access Control Policies

Access control policies play an important role in the operation of a firewall. The policies can be broadly categorized in to the following four types:

Service Control:

- Determines the types of internet services to be accessed
- Filters traffic based on IP addresses and TCP port numbers
- Provides Proxy servers that receives and interprets service requests before it is passed on

Direction Control:
Determines the direction in which a particular service request may be initiated and allowed to flow through the firewall

User Control:

- Controls access to a service according to which user is attempting to access it
- Typically applied to the users inside the firewall perimeter
- Can be applied to the external users too by using secure authentication technique

Behavioral Control:

- Controls how a particular service is used
- For example, a firewall may filter email to eliminate spam
- Firewall may allow only a portion of the information on a local web server to an external user

8.3.4 Firewall Capabilities

Important capabilities of a firewall system are listed below:

- It defines a single choke point to keep unauthorized users out of protected network
- It prohibits potentially vulnerable services from entering or leaving the network
- It provides protection from various kinds of IP spoofing
- It provides a location for monitoring security-related events
- Audits and alarms can be implemented on the firewall systems
- A firewall is a convenient platform for several internet functions that are not security related
- A firewall can serve as the platform for IPSec using the tunnel mode capability and can be used to implement VPNs

8.3.5 Limitations of a Firewall

Main limitations of a firewall system are given below:

- A firewall cannot protect against any attacks that bypass the firewall. Many organizations buy expensive firewalls but neglect numerous other back-doors into their network
- A firewall does not protect against the internal threats from traitors. An attacker may be able to break into network by completely bypassing the firewall, if he can find a ``helpful" insider who can be fooled into giving access to a modem pool
- Firewalls can't protect against tunneling over most application protocols. For example, firewall cannot protect against the transfer of virus-infected programs or files

8.3.6 Types of Firewalls

The firewalls can be broadly categorized into the following three types:

- Packet Filters
- Application-level Gateways
- Circuit-level Gateways

Packet Filters: Packet filtering router applies a set of rules to each incoming IP packet and then forwards or discards it. Packet filter is typically set up as a list of rules based on matches of fields in the IP or TCP header. An example table of telnet filter rules is given in Fig. 8.3.2. The packet filter operates with positive filter rules. It is necessary to specify what should be permitted, and everything that is explicitly not permitted is automatically forbidden.

Computer System	Source Address	Destinat. Address	Transport Protocol	Source Port	Destinat. Port	Connection Setup	Weekdays	Time Window
A to Server-1	192.168. 5.20	192.168. 3.3	TCP	>1023	23	Yes	Mon-Fri	7AM to 6PM
Server-1 to A	192.168. 3.3	192.168. 5.20	TCP	23	>1023	No	Mon-Fri	7AM to 6PM

Figure 8.3.2 A table of packet filter rules for telnet application

Application-level Gateway: Application level gateway, also called a Proxy Server acts as a relay of application level traffic. Users contact gateways using an application and the request is successful after authentication. The application gateway is service specific such as FTP, TELNET, SMTP or HTTP.

Circuit Level Gateway: Circuit-level gateway can be a standalone or a specialized system. It does not allow end-to-end TCP connection; the gateway sets up two TCP connections. Once the TCP connections are established, the gateway relays TCP segments from one connection to the other without examining the contents. The security function determines which connections will be allowed and which are to be disallowed.

8.3.7 Bastion Host

An application level gateway is sometimes known as *Bastion Host*. It is a system identified by the firewall administrator as a very critical point in the network's security. It serves as a platform for an application-level or circuit-level gateway. It executes a very secured version of OS and configured to be very secure. It is necessary to perform additional authentication before a user is allowed to access the gateway. Each proxy server is configured to perform the following:

- Support only a subset of the application's command set
- Allow access only to specific host systems
- Maintains detailed audit information

8.3.8 Network Address Translation

NAT works by using one set of addresses for communications on the internet and a separate set of addresses for communication on the private network. IANA set aside three ranges of IP addresses given below for communication on the internal network.

- Class A addresses: 10.0.0.0 – 10.255.255.255.255
- Class B addresses: 172.16.0.0 – 172.31. 255.255
- Class C addresses: 192.168.0.0 – 192.168.255.255

As these addresses are reserved for internal network addressing, these are not routable. The Firewall performs translation of an internal address to an external IP address and vice versa to facilitate communication between the private and the public network, as shown in Fig. 8.3.3. However, the NAT affords a substantial degree of security by preventing direct communication. Moreover, NAT allows the use of same IP addresses in different private networks. This prolongs the life expectancy of IPv4 on the internet. Without NAT the supply of IP addresses would have exhausted long back.

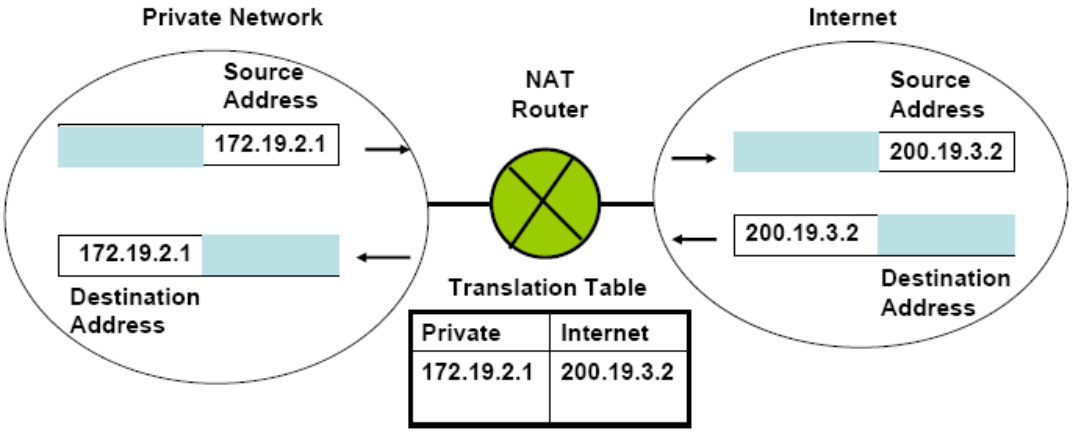

Figure 8.3.3 Function of a Network Address Translator

8.3.9 Firewall Configurations

Firewalls are typically configured in one of the four following ways:

- Screened host Firewall system (Single-homed Bastion host)
- Screened host Firewall system (dual-homed Bastion host)
- Screened subnet Firewall system (Single-homed Bastion host)
- Screened subnet Firewall system (Dual-homed Bastion host)

Screened host Firewall system: In case of single-homed Bastion host, the packets come in and go out over the same network interface as shown in Fig. 8.3.4. So the application

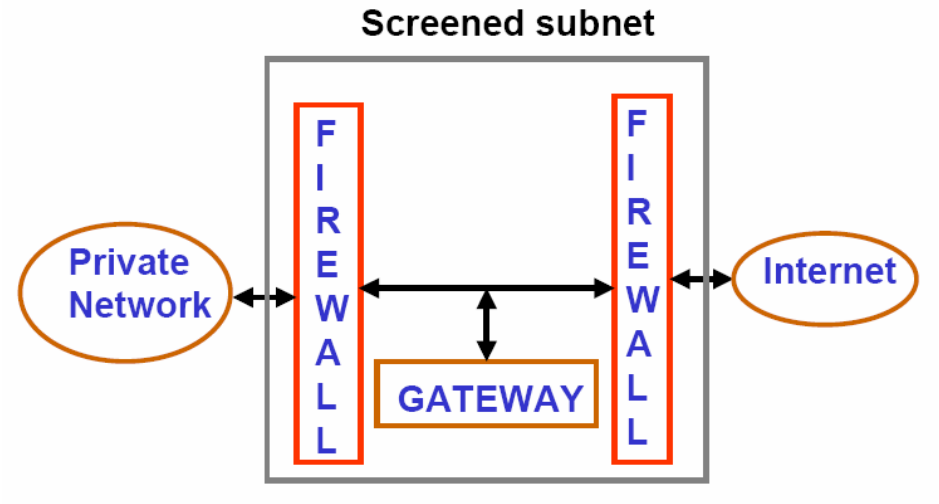

Figure 8.3.4 Screen subnet single-homed Bastion host

gateway cannot guarantee that all packets are analyzed and checked. For internet traffic, only IP packets destined for the bastion host are allowed. For intranet traffic, only IP packets from the bastion host are allowed. Bastion host performs authentication and proxy functions. This configuration affords flexibility in providing direct internet access. If the packet filtering router is completely compromised, traffic could flow directly through the router between the internet and other hosts in the private network. In case of dual-homed Bastion host, the application gateway has two separate network interfaces as shown in Fig. 8.3.5. As a consequence, it has complete control over the packets.

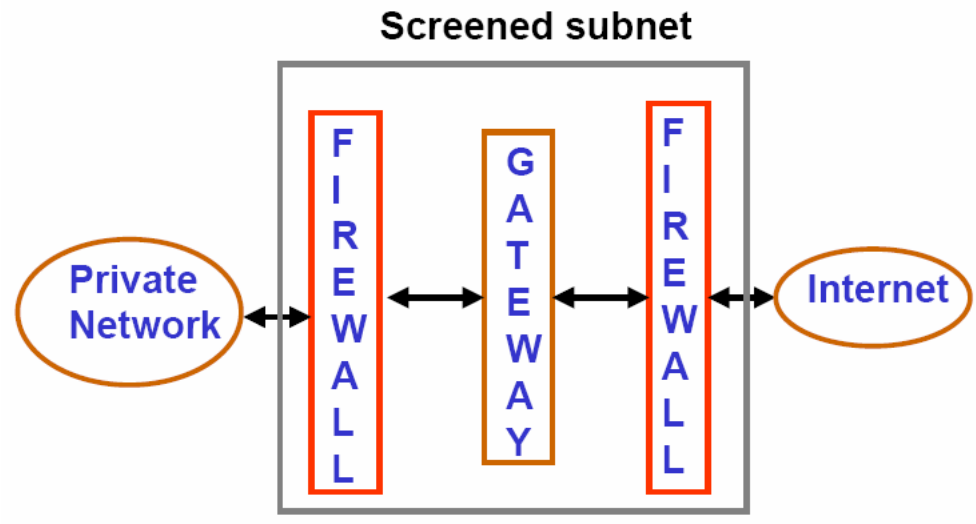

Figure 8.3.5 Screen subnet dual-homed Bastion host

8.3.10 Active Firewall Elements

The structure of an active firewall element, which is integrated in the communication interface between the insecure public network and the private network is shown in Fig. 8.3.6. To provide necessary security services, following components are required:

Integration Module: It integrates the active firewall element into the communication system with the help of device drivers. In case of packet filters, the integration is above the Network Access Layer, where as it is above the Transport layer ports in case of Application Gateway.

Analysis Module: Based on the capabilities of the firewall, the communication data is analysed in the Analysis Module. The results of the analysis is passed on to the Decision Module.

Decision Module: The Decision Module evalutes and compares the results of the analysis with the security policy definitions stored in the Ruleset and the communication data is allowed or prevented based the outcome of the comparision.

Processing module for Securityrelated Events: Based on ruleset, configuration settings and the message received from the decision module, it writes on the logbook and generates alarm message to the Security Management System.

Authentication Module: This module is responsible for the identification and authentication of the instances that are communicated through the firewall system.

Ruleset: It contains all the information necessary to make a decision for or against the transmission of communication data through the Firewall and it also defines the security-releted events to be logged.

Logbook: All security-related events that occur during operation are recorded in the loogbook based on the existing ruleset.

Security Management System: It provides an interface where the administrator enter and maintain the ruleset. It also analyses the data entered in the logbook.

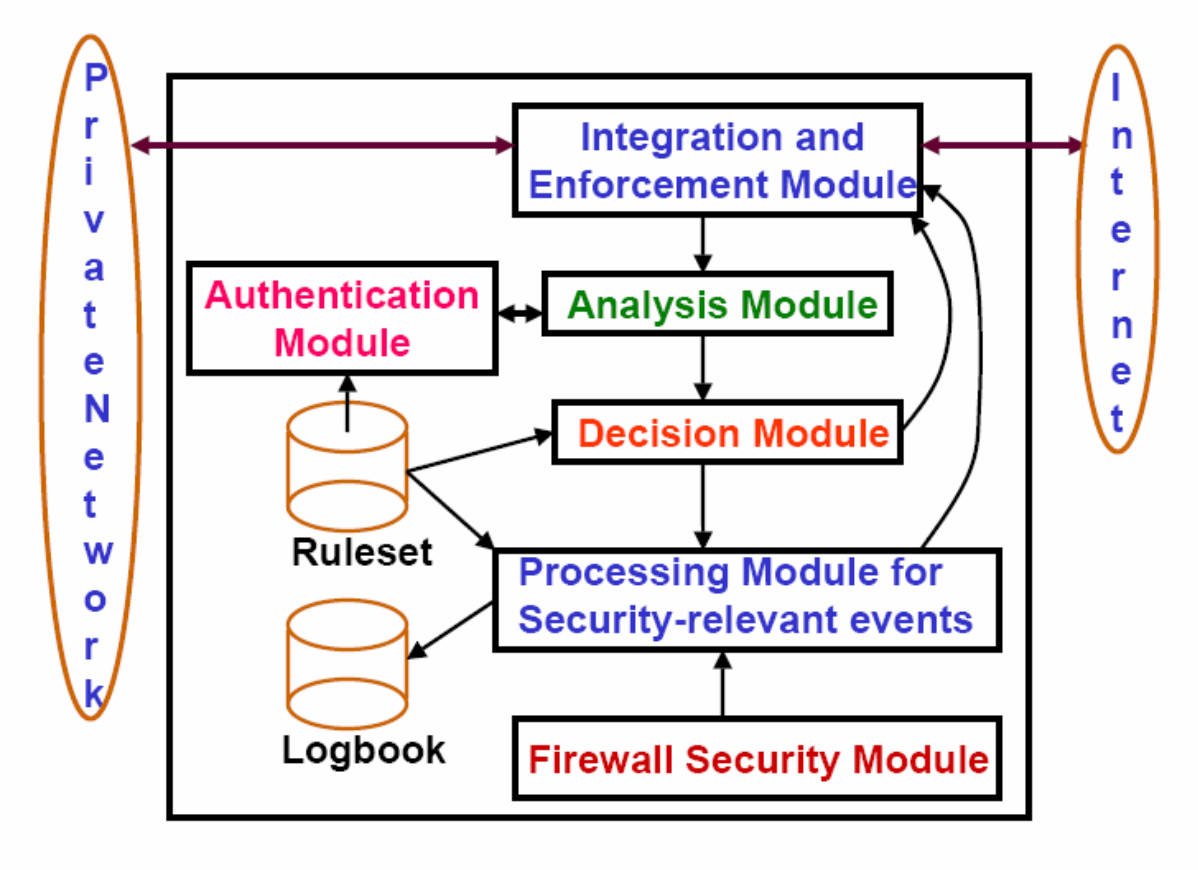

Figure 8.3.6 Components of the active firewall system

Review Questions

1.What is the purpose of a Firewall?

Ans: The purpose of the Firewall is to protect a private network from the threats of hackers coming from the Internet (a public network).

2. What are the commonly used Firewall types?

Ans: Firewalls can be of the following three types:

- Packet Filters
- Application-level Gateways
- Circuit-level Gateways.

3. Explain the operation of the packet-filter firewall.

Ans: A packet filter Firewall blocks or forwards packets based on the transport and network layer addresses and protocols. It is typically set up as a list of rules based on matches of fields in the IP or TCP header.

4. Explain the operation of the Application Gateway Firewall.

Ans: An Application Gateway blocks or forwards packets based on the information in the application layers.

5. What is NAT? How it improves network security?

Ans: Network Address Translation (NAT) allows a private network to use a set of private addresses and a set of global Internet Addresses for external communication. It uses a translation table to route messages between the two networks and provides substantial security.

References

1. **William Stallings, Cryptography and Network Security: Principles and Practices, Pearson Education, 2006**
2. **Behrouz A. Forouzan, Data Communications and Networking, 3rd Edition, Tata McGraw-Hill Publishing Company Limited, 2004**
3. **Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security: PRIVATE Communication in a PUBLIC World, Prentice-Hall of India Private Limited, 2005**
4. **Norbert Pohlmann and Tim Crothers, Firewall Architecture fot the Enterprise, FIREWALL MEDIA, 2003**