INSTITUTE OF DISTANCE AND OPEN LEARNING • UNIVERSITY OF MUMBAI •

F.Y. MCA

(TWO YEARS PATTERN)

SEMESTER - II (CBCS)

INFORMATION SECURITY

SUBJECT CODE: MCA23

Programme Co-ordinator : **Shri Mandar Bhanushe**
Head, Faculty of Science and Technology IDOL,
Univeristy of Mumbai – 400098

Course Co-ordinator : **Mr. Shyam Mohan T.**
Department - MCA, IDOL
University of Mumbai- 400098

Course Writers : **Mrs. Vidya Bharde**
Assistant Professor,
MGMCET Kamothe, Navi Mumbai

: **Mrs. Kavita Chouk**
Assistant Professor,
Satish Pradhan Dnyanasadhana college

: **Mr.Sandeep Kamble**
Assistant Professor,
Cosmopolitan's Valia College

: **Dr. Juita Tushar Raut**
Assistant Professor,
Sonopant Dandekar Shikshan Mandali's College,
Palghar

: **Dr. Ghayathri J**
Associate Professor
Kongu Arts and Science College (Autonomous),
Nanjanapuram, Kathirampatti Post,
Erode - 638107, Tamilnadu.

: **Mr. Milind Thorat**
Lecturer,
KJSIEIT, SION

: **Mrs. Asha Hulsure**
Lecturer,
S.P.M. Polytechnic Kumathe, Solapur

May 2022, Print - 1

Published by : Director,
Institute of Distance and Open Learning,
University of Mumbai,
Vidyanagari,Mumbai - 400 098.

DTP composed and Printed by:
Mumbai University Press
Vidyanagari, Santacruz (E), Mumbai- 400098

CONTENTS

Chapter No. Title Page No.

Module 1 Introduction

Module 2 Cryptography and Authentication

Module 3 Digital certificates and integrity

Module 4 Internet and web security

Module 5 Firewall and IDS

Module 6 Database and OS Security

10

FIREWALL

Unit Structure

10.0 Objectives

After this chapter, you should be able to understand the following concepts:

1. List the key characteristic of firewalls.
2. Explain the role of firewalls as part of a computer and network security strategy
3. Understand how to control the interface between private and public network
4. Understand the different kinds of firewall
5. Know about the different types of attacks of firewall
6. Classify different types of configurations
7. Know about its functionality and limitations

10.1 Introduction

The dramatic rise and progress of the Internet has opened possibilities that no one would have thought of. We can connect any computer in the world to any other computer, no matter how far the two are located from each other. This can be a nightmare for network support staff, which is left with a very difficult job of trying to protect the corporate networks from a variety of attacks.

Most corporations have large amounts of valuable and confidential data in their networks. Leaking of this critical information to competitors can be a great setback.

Internet connectivity is no longer optional for organizations. The information and services available are essential to the organization. Moreover, individual users within the organization want and need Internet access, and if this is not provided via their LAN, they will use dial-up capability from their PC to an Internet service provider (ISP). However, while Internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets.

This creates a threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. Consider a network with hundreds or even thousands of systems, running a mix of various versions of UNIX, plus Windows. When a security flaw is discovered, each potentially affected system must be upgraded to fix that flaw. The alternative, increasingly accepted, is the firewall.

A firewall can be simple a router that is used to filter the packets or a complex multi-computer, multi-router solution that performs filtering of packets along with application-level proxy services. A firewall is essentially a router or a group of routers and computers to enforce access control between two networks.

A firewall can be through of as a pair of mechanisms: allow, which permits traffic and deny, which blocks traffic. There are some firewalls which emphasize on blocking traffic, while others emphasize on permitting traffic.

Apart from the danger of the insider information leaking out, there is a great danger of the outside elements like viruses and worms entering a corporate network to create havoc.

Firewalls are the first line of defence between the internal network and untrusted networks like the Internet. A firewall is a combination of software and hardware used to maintain security of a private network by applying security policies at two or more network boundaries. Firewalls are incorporated into a wide variety of networked devices to filter traffic and lower the risk that malicious packets travelling over the public internet can impact the security of private network. First introduced conceptually in the late 1980s in a whitepaper from Digital Equipment Corporation, “firewalls” provided a then new and important function to the rapidly growing networks of the day.

The design goals include

All traffic from inside to outside a network must be pass through a firewall.

Only authorized traffic will be allowed to pass from a firewall.

The firewall itself must be strong enough, so as to render attacks on it useless.

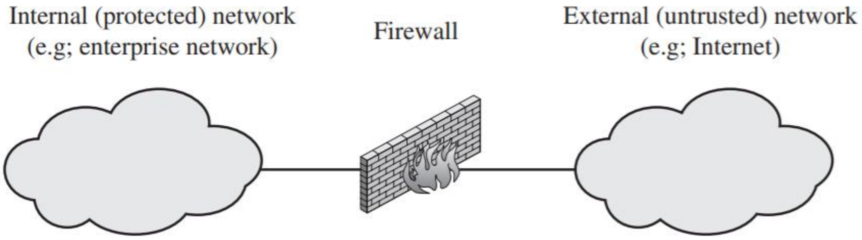
Internal (protected) network
(e.g; enterprise network)
Firewall
External (untrusted) network
(e.g; Internet)

Figure 10.1 Firewall

Firewall design principles

Internet connectivity is no longer an option for most organizations. However, while internet access provides benefits to the organization, it enables the outside world to reach and interact with local network assets. This creates the threat to the organization. While it is possible to equip each workstation and server on the premises network with strong security features, such as intrusion protection, this is not a practical approach. The alternative, increasingly accepted, is the firewall.

The firewall is inserted between the premise network and internet to establish a controlled link and to erect an outer security wall or perimeter. The aim of this perimeter is to protect the premises network from internet-based attacks and to provide a single choke point where security and audit can be imposed. The firewall can be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

10.2 Firewall Characteristics

The characteristics of firewall are

- Service Control
- Direction Control
- User Control
- Behaviour Control

- **Service Control:** Determines the types of Internet services that can be accessed by the network user. The inbound or outbound traffic may be filtered based on the basis of IP address and TCP port number. It can be implemented by proxy software or host on the server software.
- **Direction control**: Determines the direction such as inbound or outbound in which particular service requests are allowed to flow through the Firewall.
- **User control**: Controls access to a service according to the user. Each user will have a ACLs indicates their level of access. Based on ACL the user traffic may allowed or denied. This feature is typically applied to users inside the private network to control outbound traffic. It may also be applied to incoming traffic from external users, but it needs authentication technique

- **Behavior control**: It makes use of statistical data to control the traffic. Controls how particular services are used (e.g. filter e-mail to eliminate spam), or it may enable external access to only a portion of the information on a local Web server.

10.3 Types of Firewalls

There are three types of firewall namely,

1) Packet Filtering
2) Application Gateways
3) Circuit-level Gateways

1) Packet Filtering:

Firewalls filter each packet that attempt to enter or leave a private network and either accept or reject them depending on the predefined set of filter rules which is based on based on pattern-matching. Figure 5.8 shows the placement of packet filtering firewall which is between the public and private network.

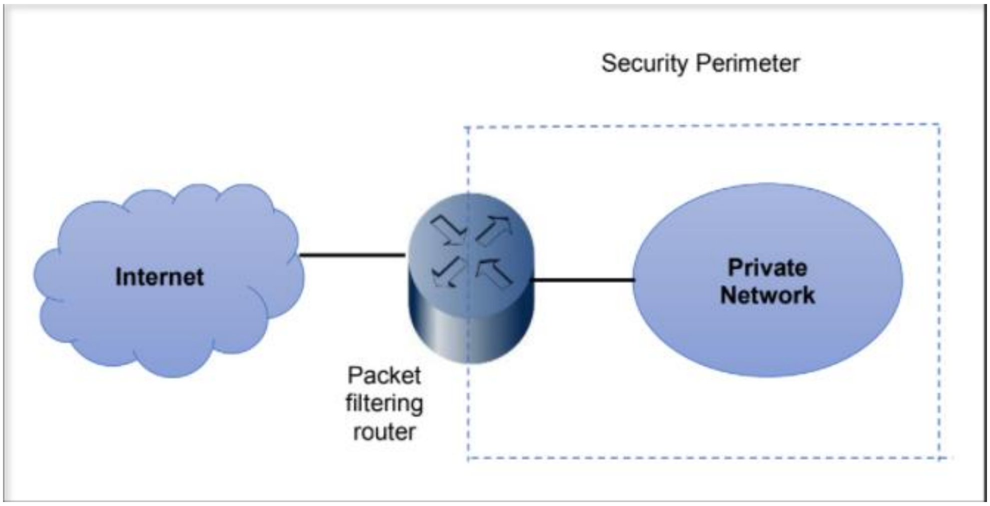

Figure 10.2 Packet Filtering Firewall

A packet filter performs the following functions.

1) Receive each packet as it arrives.
2) Pass the packet through a set of rules, based on the contents of the IP and transport header fields of the packet. If there is a match with one of the set rules, decide whether to accept or discard the packets based on that rule.
3) If there is no match with any rule, take the default action. The default can be discard all packets or accept all packets.

An advanced type of packet filter is called as **stateful packet filter or dynamic packet filter**. This packet filter allows the examination of packets based on the current state of the network. It adapts itself to the current exchange of information, unlike the normal packet filters.

Allow incoming TCP packets only if they are responses to the outgoing TCP packets that have gone through our network. Dynamic packet filter has to maintain a list of the currently open connections and outgoing packets in order to deal with this rule. So, it is called dynamic or stateful.

This type of firewall combines the speed of packet filters with the enhanced security of stored session information typified by proxies. While traffic is being forwarded through the firewall, stateful inspections of the packets create slots in session flow tables.

These tables contain source and destination IP addresses, port numbers, and TCP protocol information. Before traffic can travel back through the firewall, stateful inspections of the packets are cross-referenced to the session flow tables for an existing connection slot. If a match is found in the tables, the packets are forwarded; otherwise, the packets are dropped or rejected.

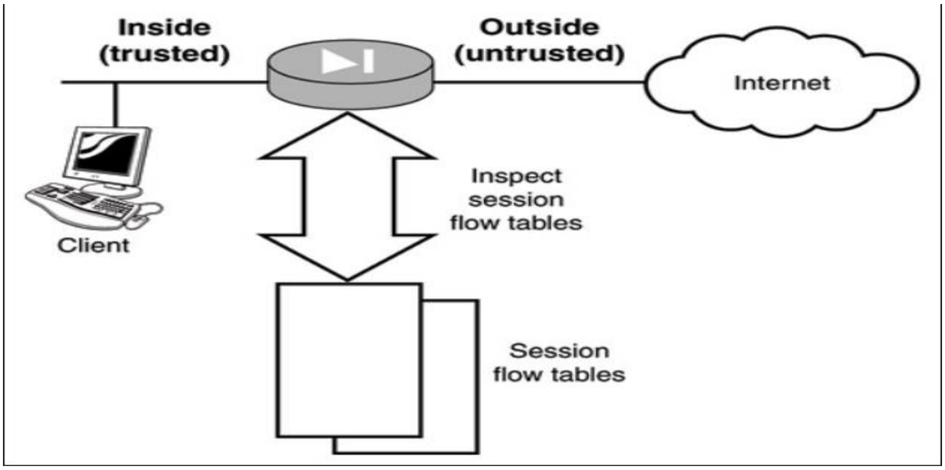

Figure 10.3 Stateful inspection

Stateless Packet Filter:

Stateless packet filtering firewalls are perhaps the oldest and most established firewall option. While they're less common today, they do still provide functionality for residential internet users or service providers who distribute low-power customer-premises equipment (CPE). They protect users against malware, non-application-specific traffic and harmful applications. If users host servers for multi-player video games, email or live-streamed videos, for example, they often must manually configure firewalls if they plan to deviate from default security policies. Manual configurations allow different ports and applications through the packet filter.

Advantages of Packet Filter Firewall:

It is simplicity

Packet filters are very fast in their operating speed.

Packet filter is transparent to the user.

Disadvantages:

Setting up the packet filter rule correctly is difficult.

Most packet filter firewalls do not support advanced user authentication schemes.

They are generally vulnerable to attacks such as layer address spoofing.

Because packet filter firewalls do not examine upper-layer data, they cannot prevent attacks that employ application-specific vulnerabilities or functions.

Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited.

2) **Application Gateway Firewall**:

It is also called as proxy server. This is because it acts like a proxy and decides about the flow of application-level traffic. Application gateway work as follows:

1. An internal user contacts the application gateway using a TCP/IP application, such as HTTP or TELNET.
2. The application gateway asks the user about the remote host with which the user wants to set up a connection for actual communication. The application gateway also asks for the user id and password required to access the services of the application gateway.
3. The user provides this information to the application gateway.
4. The application gateway now access the remote host on behalf of the user and passes the packets of the user to the remote host.
5. The application gateway acts like a proxy of the actual end user and delivers packets from the user to the remote host and vice versa.

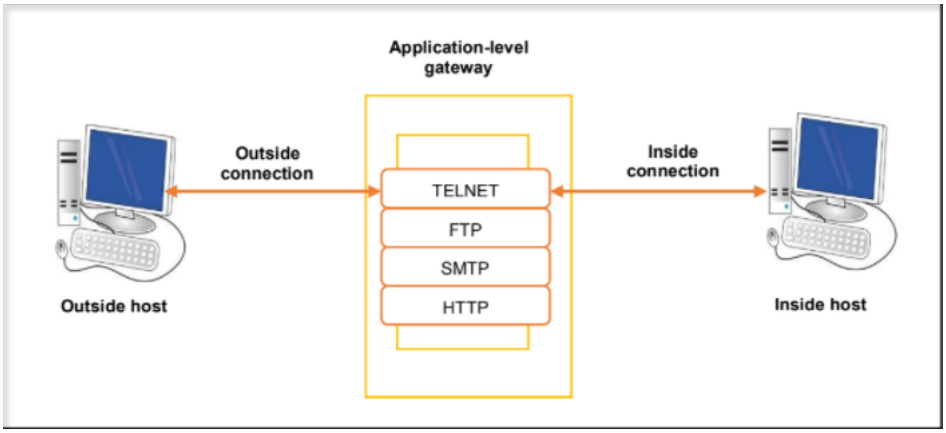

Figure 10.4 Application Gateway Firewall

Advantages:

Application gateway is more secure than packet filter because it examines every packet against a number of rules.

It is easy to log and audit all incoming traffic at the application level

Disadvantage:

Application gateway is the additional processing overhead on each connection-.

3) Circuit level Gateway:

Provides TCP and UDP connection security and works at session layer OSI model. It monitors the TCP data packet handshaking between packets to ensure the session is legitimate and fulfilment of firewall rules and policies.

Circuit level gateway can be a stand-alone system or it can be a specified function performed by an application-level gateway for certain applications. A Circuit level gateway does not permit an end-to-end TCP connection; rather, the gateway sets up two TCP connections, one between itself and a TCP user on an inner host and one between itself and a TCP user on an outer host. Once the two connections are established, 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.

A typical use of Circuit level gateways is a situation in which the system administrator trusts the internal users. The gateway can be configured to support application level or proxy service on inbound connections and circuit level functions for outbound connections.

Figure 9.5 shows the placement of circuit-level gateway firewall.

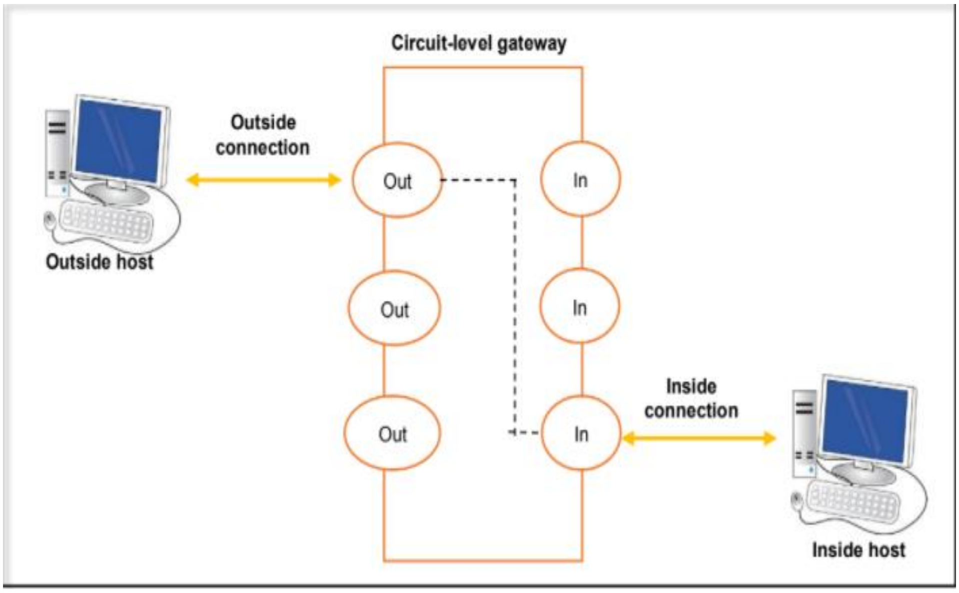

Figure 10.5 Circuit level Gateway

The SOCKS server is an example of the real-life implementation of a circuit gateway. It is client-server application. The SOCKS client runs on the internal hosts and the SOCKS server runs on the firewall.

10.4 Attacks of Packet Filter

IP address spoofing: The intruder transmits packets from the outside with a source IP address field containing an address of an internal host. The attacker hopes that the use of a spoofed address will allow penetration of systems that employ simple source address security, in which packets from specific trusted internal hosts are accepted. The countermeasure is to discard packets with an inside source address if the packet arrives on an external interface.

Source routing attacks: The source station specifies the route that a packet should take as it crosses the Internet, in the hopes that this will bypass security measures that do not analyze the source routing information. The countermeasure is to discard all packets that use this option.

Tiny fragment attacks: The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment. This attack is designed to circumvent filtering rules that depend on TCP header information. Typically, a packet filter will make a filtering decision on the first fragment of a packet.

All subsequent fragments of that packet are filtered out solely on the basis that they are part of the packet whose first fragment was rejected. The attacker hopes that the filtering router examines only the first fragment and that the remaining fragments are passed through.

A tiny fragment attack can be defeated by enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header. If the first fragment is rejected, the filter can remember the packet and discard all subsequent fragments.

10.5 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 an application-level or circuit level gateway. Common characteristics of a bastion host include the following:

- The bastion host hardware platform executes a secure version of its operating system, making it a trusted system.
- Only the services that the network administrator considers essential are installed on the bastion host. These include proxy applications such as Telnet, DNS, FTP, SMTP, and user authentication.
- The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition, each proxy service may require its own authentication before granting user access.
- Each proxy is configured to support only a subset of the standard application's command set

Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set may be applied only to a subset of systems on the protected network.

- Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. The audit log is an essential tool for discovering and terminating intruder attacks.
- Each proxy module is a very small software package specifically designed for network security. Because of its relative simplicity, it is easier to check such modules for security flaws. For example, a typical UNIX mail application may contain over 20,000 lines of code, while a mail proxy may contain fewer than 1000.
- Each proxy is independent of other proxies on the bastion host. If there is a problem with the operation of any proxy, or if a future vulnerability is discovered, it can be uninstalled without affecting the operation of the other proxy applications. Also, if the user population requires support for a new service, the network administrator can easily install the required proxy on the bastion host.
- A proxy generally performs no disk access other than to read its initial configuration file. This makes it difficult for an intruder to install Trojan horse sniffers or other dangerous files on the bastion host.
- Each proxy runs as a non privileged user in a private and secured directory on the bastion host.

10.6 Firewall Configuration

In practical implementations, a firewall is usually a combination of packet filters and application gateways. Based on this, there are three possible configurations of firewalls as shown in figure.

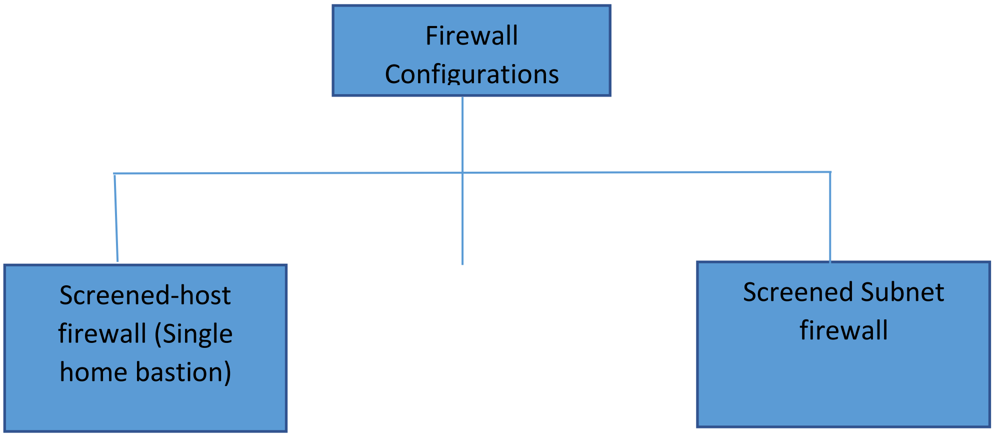

Figure 10.6 Firewall Configuration

Screened Host Firewall, Single Homed Bastion:

In the screened host firewall, a firewall set up consists of two parts: a packet-filtering router and an application gateway.

Their purposes are as follows.

The packet filter ensures that incoming traffic (i.e., form the Internet to the corporate network) is allowed only if it is designed for the application gateway, by examining the destination address field of every incoming IP packet. Similarly, it also ensures that the outgoing traffic is allowed only if it is originating from the application gateway, by examining the source address field of every outgoing IP packet.

The application gateway performs authentication and proxy functions.

The bastion host performs authentication and proxy functions. This configuration has greater security than simply a packet filtering router or an application-level gateway alone, for two reasons:

This configuration implements both packet level and application-level filtering, allowing for considerable flexibility in defining security policy.

An intruder must generally penetrate two separate systems before the security of the internal network is compromised.

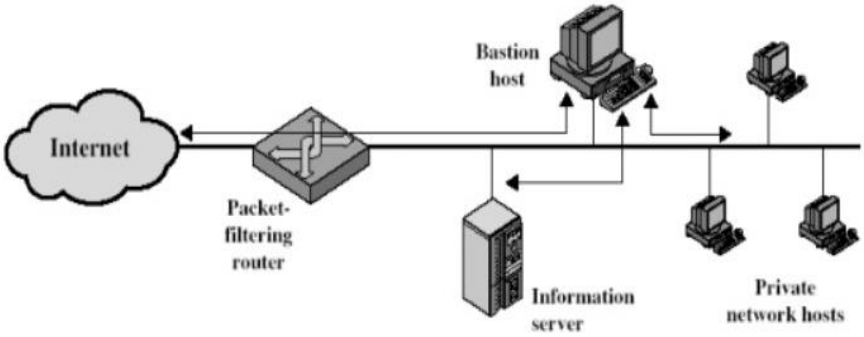

Figure 10.7 Screened-host firewall, Single homed bastion

Screened host firewall, Dual-Homed Bastion:-

To overcome the drawback of a screened host firewall, single-homed bastion configuration another type of configuration, called as screened host firewall, dual-homed bastion. In the previous configuration, if the packet filtering router is compromised, traffic could flow directly through the router between the internet and the other hosts on the private network. This configuration physically prevents such a security break. The internal hosts are protected.

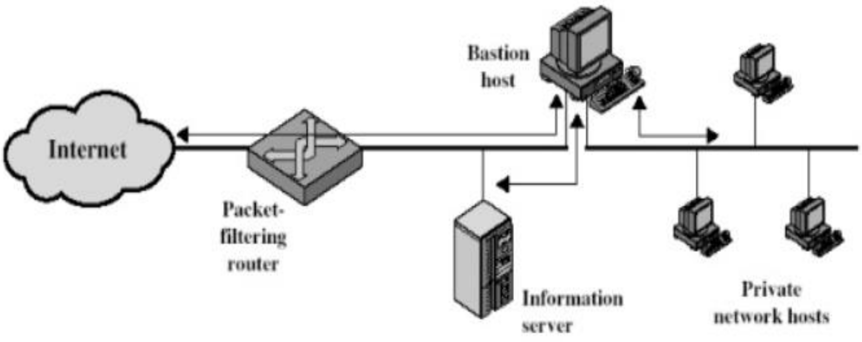

Figure 10.8 Dual-homed bastion

Screened Subnet Firewall:-

It offers the highest security among the possible firewall configurations. It is an improvement over the previous scheme of screened host firewall, dual-homed bastion. Two packet filtering routers are used, one between the bastion host and internet and one between the bastion host and the internal network.

This configuration creates an isolated sub-network, which may consist of simply the bastion host but may also include one or more information servers and modems for dial-in capability. Typically, both the internet and the internal network have access to hosts on the screened subnet, but traffic across the screened subnet is blocked. This configuration offers several advantages:

- There are now three levels of defense to prevent intruders.
- The outside router advertises only the existence of the screened subnet to the internet; therefore, the internal network is invisible to the internet.
- Similarly, the inside router advertises only the existence of the screened subnet to the internal network; therefore, the systems on the internal network cannot construct direct routes to the internet.

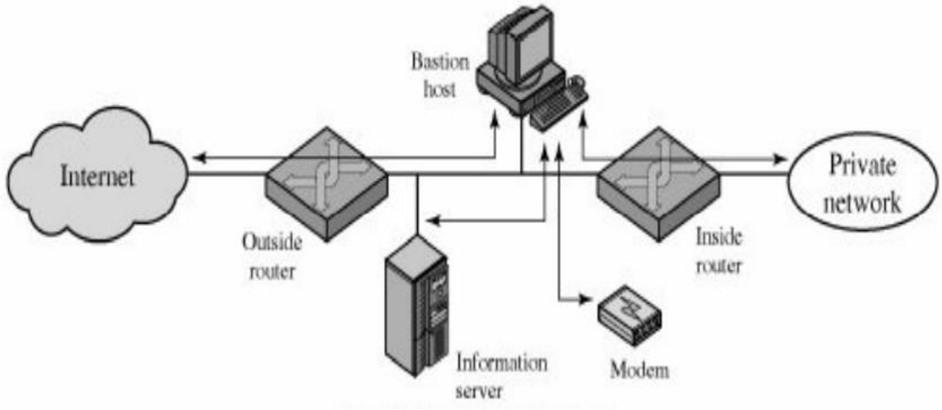

Figure 10.9 Screened subnet firewall

10.7 Limitations of Firewall

We must note that although a firewall is an extremely useful security measure for an organization, it does not solve all the practical security problems. The main limitations of a firewall can be listed as follows.

1) **Insider's intrusion:**

   As we know, a firewall system is designed to prevent outside attacks. Therefore, if an inside user attacks the internal network in some way, the firewall cannot prevent such an attack. The firewall does not protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

2) **Direct internet traffic:**

   A firewall must be configured very carefully. It is effective only if it is the only entry-exit point of an organization's network. If instead, the firewall is one of the entry-exit points, user can bypass the firewall and exchange information with the internet via the other entry-exit points. This can open up the possibilities of attacks on the internal networks through those points. Such situation can not be handled by firewall.

3) **Virus attacks:**

   A firewall cannot protect internal network from virus threats. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

10.8 Summary

This chapter provided an in-depth overview of firewalls and their roles in protecting the corporate network and also design principles of firewall. There are three main types of firewalls: packet filters, application gateways, and circuit-level gateways. Corporate networks can be attacked from outside or internal information can be leaked out. Encryption cannot prevent outside attackers from attacking a network. A firewall should be placed between a corporate network and the outside world. A firewall is a special type of router, which applies rules for allowing or stopping traffic.

10.9 Bibliography

Atul Kahate, "Cryptography and Network Security", McGraw Hill

Behrouz A Forouzan, Cryptography and Network Security

William Stallings, Cryptography and Network Security: Principles and Practice

Mark Rhodes-Ousley, The complete reference Information Security

10.10 Exercises

1. What are the limitations of a firewall?

2. List the characteristics of a good firewall implementation.

3. What is an application-level gateway?

4. What is a circuit-level gateway?

5. What is the difference between a packet filtering firewall and a stateful inspection firewall?

6. What are some weaknesses of a packet filtering firewall?

7. What information is used by a typical packet filtering firewall?

8. How is Screened host firewall, Dual-homed bastion different from screened host firewall, Single-homed bastion?

9. How is a circuit gateway different from an application gateway?

10. What is the disadvantage of a screened host firewall, Single-homed bastion?

11. Study at least one real-life firewall product. Study its features with reference to the theory introduced in this chapter.

❄❄❄❄❄❄❄