5.2 THE NEED FOR FIREWALLS

Information systems in corporations, government agencies, and other organizations have undergone a steady evolution. The following are notable developments:

- Centralized data processing system, with a central mainframe supporting a number of directly connected terminals
- Local area networks (LANs) interconnecting PCs and terminals to each other and the mainframe
- Premises network, consisting of a number of LANs, interconnecting PCs, servers, and perhaps a mainframe or two
- Enterprise-wide network, consisting of multiple, geographically distributed premises networks interconnected by a private wide area network (WAN)
- Internet connectivity, in which the various premises networks all hook into the Internet and may or may not also be connected by a private WAN

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 may not be sufficient and in some cases is not cost-effective.

Consider a network with hundreds or even thousands of systems, running various operating systems, such as different versions of UNIX and Windows. When a security flaw is discovered, each potentially affected system must be upgraded to fix that flaw. This requires saleable configuration management and aggressive patching to function effectively.

While difficult, this is possible and is necessary if only host-based security is used. A widely accepted alternative or at least complement to host-based security services is the firewall. The firewall is inserted between the premises network and the 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 auditing can be imposed. The firewall may be a single computer system or a set of two or more systems that cooperate to perform the firewall function.

The firewall, then, provides an additional layer of defense, insulating the internal systems from external networks. This follows the classic military doctrine of "defense in depth," which is just as applicable to IT security.

Importance of Using a Firewall :

The following points listed below are the most relevant in explaining the importance of firewalls is as follows.

Feature-1 :

Monitoring Network Traffic –

Firewall security starts with effective monitoring of network traffic based on pre-established rules and filters to keep the systems protected. Monitoring of network traffic involves the following security measures.

1. **Source or destination-based blocking of incoming network traffic –**
   This is the most common feature of most firewalls, whereby the firewalls block the incoming traffic by looking into the source of the traffic.
2. **Outgoing network traffic can be blocked based on the source or destination –**
   Many firewalls can also filter data between your internal network and the Internet. You might, for example, want to keep employees from visiting inappropriate websites.
3. **Block network traffic based on content –**
   More modern firewalls can screen network traffic for inappropriate content and block traffic depending on that. A firewall that is integrated with a virus scanner, for example, can prevent virus-infected files from entering your network. Other firewalls work in tandem with e-mail services to filter out unwanted messages.
4. **Report on network traffic and firewall activities –**
   When filtering network traffic to and from the Internet, it's also crucial to know what your firewall is doing, who tried to break into your network, and who tried to view prohibited information on the Internet. A reporting mechanism of some sort is included in almost all firewalls.

Feature-2 :

Stops Virus Attacks and spyware –

With cyber thieves creating hundreds of thousands of new threats every day, including spyware, viruses, and other attacks like email bombs, denial of service, and malicious macros, it's critical that you put protections in place to keep your systems safe. The number of entry points criminals can exploit to get access to your systems grows as your systems become more complicated and strong. Spyware and malware programs designed to penetrate your networks, manage your devices, and steal your data are one of the most common ways unwelcome persons obtain access. Firewalls are a crucial line of defense against malicious software.

Feature-3 :

Preventing Hacks –

Cyber threats are evolving at a fast pace and are widespread. Firewalls keep hackers out of your data, emails, systems, and other sensitive information. A firewall can either entirely block a hacker or push them to choose a more vulnerable target.

Feature-4 :

Promotes Privacy –

Having a firewall keeps the data safe and builds an environment of privacy that is trustworthy and a system without a firewall is accepting every connection into the network from anyone. Without a firewall, there would be no way to detect incoming threats. As a result, malicious users may be able to gain access to your devices and thereby compromising privacy. It's critical to take advantage of existing defenses to safeguard your network and the personal information stored on your computer against cybercrime.

5.3 FIREWALL CHARACTERISTICS AND ACCESS POLICY

Design goals for a firewall:

1. All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall. Various configurations are possible, as explained later in this chapter.

2. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies, as explained later in this chapter.

3.The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system. Trusted computer systems are suitable for hosting a firewall and often required in government applications.

[SMIT97] lists four general techniques that firewalls use to control access and enforce the site's security policy. Originally, firewalls focused primarily on service control, but they have since evolved to provide all four:

• **Service control**: Determines the types of Internet services that can be accessed, inbound or outbound. The firewall may filter traffic on the basis of IP address, protocol, or port number; may provide proxy software that receives and interprets each service request before passing it on; or may host the server software itself, such as a Web or mail service.

• **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 according to which user is attempting to access it. This feature is typically applied to users inside the firewall perimeter (local users). It may also be applied to incoming traffic from external users; the latter requires some form of secure authentication technology.

• **Behavior control**: Controls how particular services are used. For example, the firewall may filter e-mail to eliminate spam, or it may enable external access to only a portion of the information on a local Web server.

Before proceeding to the details of firewall types and configurations, it is best to summarize what one can expect from a firewall.

The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of a single choke point simplifies security management because security capabilities are consolidated on a single system or set of systems.

2. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system.

3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator, which maps local addresses to Internet addresses, and a network management function that audits or logs Internet usage.

Firewalls have their limitations, including the following:

1.The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters.

2.The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker.

3.An improperly secured wireless LAN may be accessed from outside the organi- zation. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on differ- ent sides of the internal firewall.

4.A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally**.**