UNIT III

CYBER SECURITY FOR BUSINESS APPLICATIONS AND NETWORKS

Firewalls

- ✓ The firewall is an important complement to host-based security services such as intrusion detection systems. Typically, a 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 auditingare imposed.
- ✓ Firewalls are also deployed internally in an enterprise network to segregate portions of the network.
- ✓ A firewall provides an additional layer of defense, insulating internal systems from external networks or other parts of the internal network.

Firewall Characteristics

Goals for a firewall:

- All traffic from inside to outside, and vice versa , must pass through thefirewall. This is achieved by physically blocking all access to the local networkexcept via the firewall. Various configurations are possible, as explained later in this chapter.
- Only authorized traffic, as defined by the local security policy, is allowed to pass. Various types of firewalls are used, and they implement various types of security policies, as explained later in this chapter. 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.

Originally, firewalls focused primarily on service control, but they have since evolved to provide all four techniques:

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

Direction control: Determines the direction in which particular service requestsare 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 can also be applied to incoming traffic from external users, though this requires some form of secure authentication technology, such as thatprovided in IP Security (IPsec).

Behavior control: Controls how particular services are used. For example, the firewall can filter email to eliminate spam or enable external access to only a portion of the information on a local web serve.

Firewalls have limitations, including the following**:**

- Firewalls cannot stop users from accessing malicious websites, making itvulnerable to internal threats or attacks.
- Firewalls cannot protect against the transfer of virus-infected files or software.
- Firewalls cannot prevent misuse of passwords.
- Firewalls cannot protect if security rules are misconfigured.
- Firewalls cannot protect against non-technical security risks, such as socialengineering.
- Firewalls cannot stop or prevent attackers with modems from dialing in to or outof the internal network.
- Firewalls cannot secure the system which is already infected.

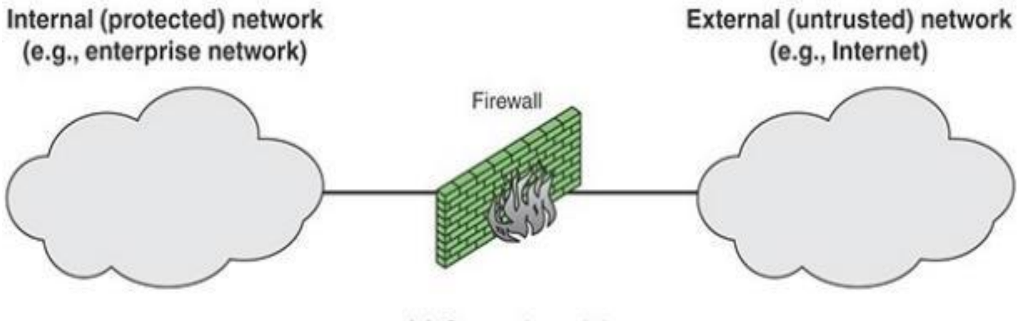
Types of Firewalls

- Three types of firewalls, such as **software firewalls, hardware firewalls, orboth**, depending on their structure. Each type of firewall has different functionality but the same purpose. However, it is best practice to have both to achieve maximum possible protection.
- A hardware firewall is a physical device that attaches between a computer network and a gateway. For example- a broadband router. A hardware firewall is sometimes referred to as an **Appliance Firewall**.
- On the other hand, a software firewall is a simple program installed on a computer that works through port numbers and other installed software. This type of firewall is also called a **Host Firewall**.

The following are types of firewall techniques that can be implemented assoftware or hardware:

- Packet-filtering Firewalls
- Circuit-level Gateways
- Application-level Gateways (Proxy Firewalls)
- Stateful Multi-layer Inspection (SMLI) Firewalls
- Next-generation Firewalls (NGFW)
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls

- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls

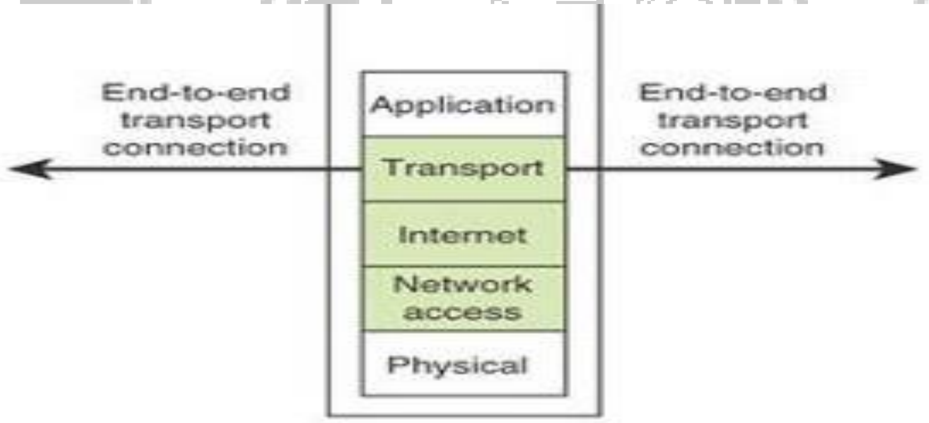

Internal (protected) network (e.g., enterprise network)
Firewall
External (untrusted) network (e.g., Internet)

(a) General model

-

Packet-filtering Firewalls

A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules. These firewalls are designed to block network traffic IP Protocols, an IP address, and a port number if a data packet does not match the established rule-set.

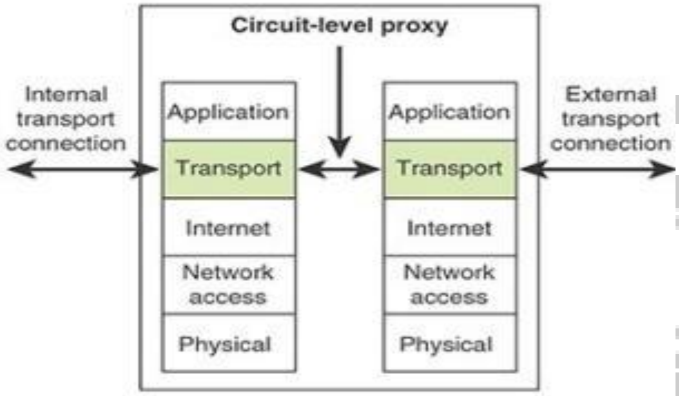

End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

(b) Packet filtering firewall

While packet-filtering firewalls can be considered a fast solution without manyresource requirements, they also have some limitations. Because these types offirewalls do not prevent web-based attacks, they are not the safest.

Circuit-level Gateways

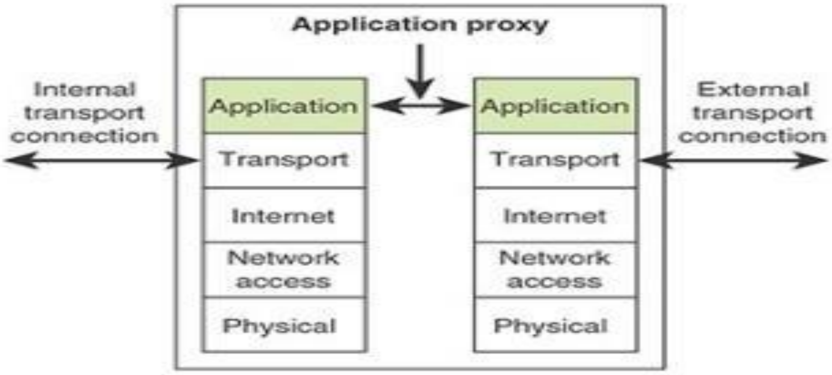
Circuit-level gateways are another simplified type of firewall that can be easilyconfigured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the session-level of the OSI model by verifying **TCP (Transmission Control Protocol)**



(e) Circuit-level proxy firewall

Application-level Gateways (Proxy Firewalls)

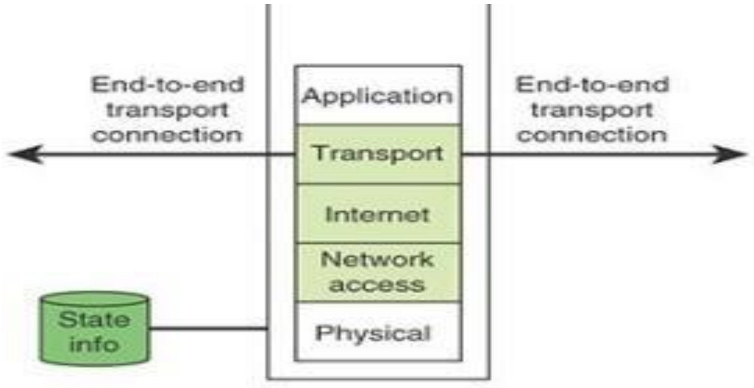
Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). Thatis why these firewalls are called **'Application-level Gateways'**.



(d) Application proxy firewall

Stateful Multi-layer Inspection (SMLI) Firewalls

- Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls superior to packet-filtering firewalls or circuit-level gateways. Additionally, these types of firewalls keep track of the status of established connections.
- In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc.


End-to-end transport connection
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
State info

(c) Stateful inspection firewall

Next-generation Firewalls (NGFW)

- Many of the latest released firewalls are usually defined as **'next-generation firewalls'**. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include **deep-packet inspection (DPI),** surface-level packet inspection, and TCP handshake testing, etc.
- In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc.
- Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.

Network Address Translation (NAT) Firewalls

- Network address translation or NAT firewalls are primarily designed to access Internet traffic and block all unwanted connections.
- These types of firewalls usually hide the IP addresses of our devices, makingit safe from attackers.

Cloud Firewalls

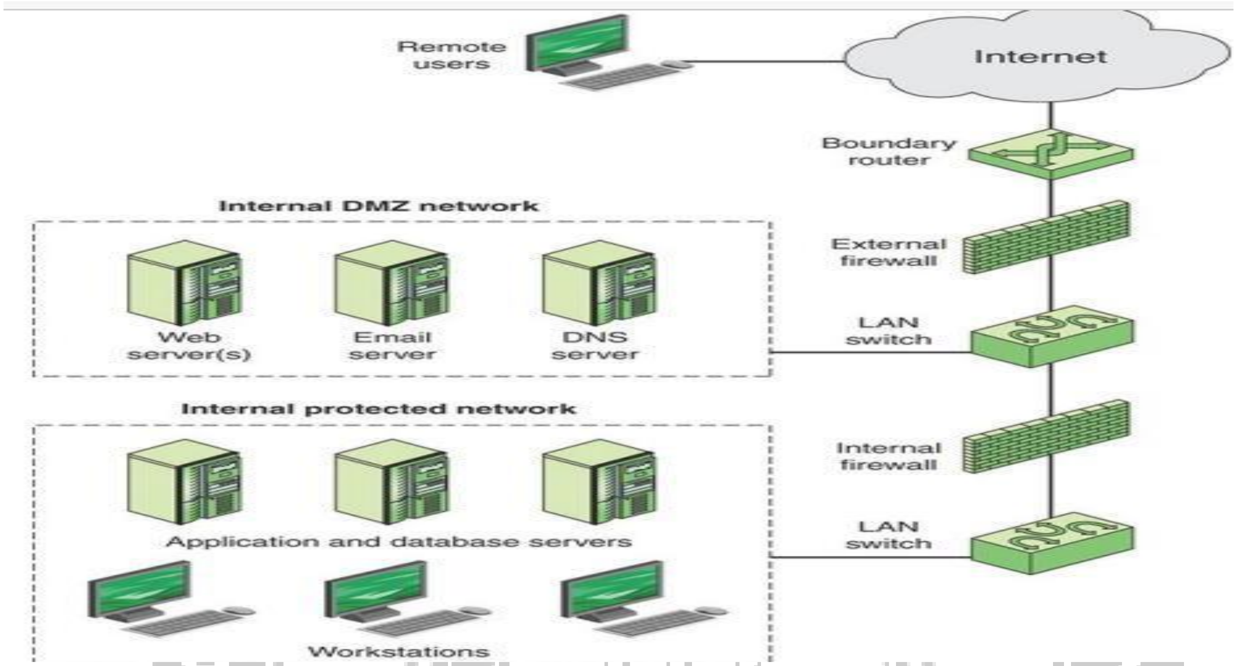
- Whenever a firewall is designed using a cloud solution, it is known as a cloud firewall or **FaaS (firewall-as-service)**. Cloud firewalls are typically maintained and run on the Internet by third-party vendors.
- This type of firewall is considered similar to a proxy firewall. The reason for this is the use of cloud firewalls as proxy servers. However, they are configured based on requirements.

Unified Threat Management (UTM) Firewalls

- UTM firewalls are a special type of device that includes features of a stateful inspection firewall with anti-virus and intrusion prevention support.
- Such firewalls are designed to provide simplicity and ease of use. These firewalls can also add

many other services, such as cloud management, etc.

.



In this type of configuration, internal firewalls serve three purposes

- ❖ An internal firewall adds more stringent filtering capability, compared to the external firewall, in order to protect enterprise servers and workstations from external attack.
- ❖ An internal firewall provides two-way protection with respect to the DMZ. First, the internal firewall protects the remainder of the network from attacks launched from DMZ systems. Such attacks might originate from worms, rootkits, bots, or other malware lodged in a DMZ system. Second, an internal firewall protects the DMZ(demilitarized zone) systems from attack from the internal protected network.
- ❖ Multiple internal firewalls are used to protect portions of the internalnetwork from each other. For example, firewalls are configured so that internal servers are protected from internal workstations and vice versa. A common practice is to place the DMZ on a different network interface onthe external firewall from that used to access the internal networks.