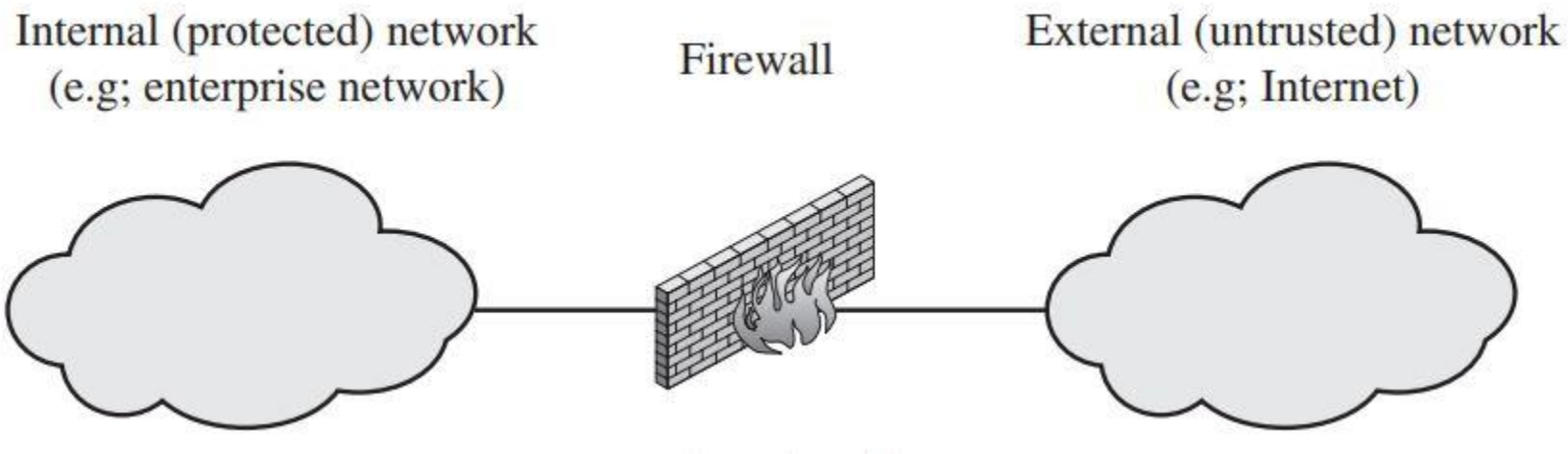
Firewall

Firewall

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- A firewall can be hardware, software.
- Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via WAN`s or the Internet

Firewall: General Model



Need for firewalls

- Internet connectivity is essential for organizations and individual users within the organization.
- Along with benefits of internet it also brings many possible threats (Internet based attacks).
- Equipping each system and server with strong security features may not be sufficient and can be cost-ineffective.
- Therefore, Firewalls provide an alternative or complementary solution to security services.

Firewall Design Principles

- Effective means of protection a local system or network of systems from network-based security threats while affording access to the outside world via Internet .

- The firewall is inserted between the premises network and the Internet.

- Aims:
  - Establish a controlled link.
  - Provide a single choke point.
  - Protect the premises network from Internet-based attacks.

Firewall Characteristics: Design Goals

- Design goals:
  - All traffic from inside to outside must pass through the firewall (physically blocking all access to the local network except via the firewall)
  - Only authorized traffic (defined by the local security policy) will be allowed to pass
  - The firewall itself is immune to penetration (use of trusted system with a secure operating system)

Firewall Characteristics: Techniques

Four general techniques:

- Service control
  - Determines the types of Internet services that can be accessed, inbound or outbound
- Direction control
  - Determines the direction in which particular service requests are allowed to flow
- User control
  - Controls access to a service according to which user is attempting to access it
- Behaviour control
  - Controls how particular services are used.

Firewall Characteristics: Firewall Access Policy

- A firewall can filter traffic based on the following access policy:
  - IP Address and Protocol Values
  - Application Protocol
  - User Identity
  - Network Activity

Access Policy: IP Address and Protocol values

- Controls access based on
  - the **source or destination addresses** and **port numbers,**
  - direction of flow being **inbound** or **outbound**,
  - **IP** headers and **TCP/UDP** headers.

- This type of filtering is used by packet filter and stateful inspection firewalls.

Access Policy: Application Protocol

- Controls access on the basis of authorized application protocol data.
- Application-level gateway that relays and monitors the exchange of information for specific application protocols.
- Example:
  - SMTP email for spam.
  - HTPP web requests to authorized sites only.

Access Policy: User Identity

- User Identity: Controls access based on the users identity.

- Typically for inside users who identify themselves as legitimate user using some form of secure authentication technology.
  - Passwords
  - Biometrics
  - Physical Identification (Smart Id cards)
  - Voice etc..

Access policy: Network Activity

- Network Activity: Controls access based on considerations of network activities such as the time or request related.
- Eg:
  - User can only access system in business hours.
  - Rate of requests for some servers is limited.
  - To detect scanning attempts by user.
  - Activity patterns such as accessing restricted websites.

Types of Firewall

- A firewall can monitor network traffic at different of levels of network –
  - Network packets at network layer, (Individual packets or part of a flow).
  - Traffic within a transport layer connection.
  - Inspecting details of application protocols.

- There are Four Common types of firewalls
  - Packet Filtering Firewall
  - Stateful Inspection Firewall
  - Application-Level Gateway
  - Circuit level Gateway

Packet Filtering Firewall

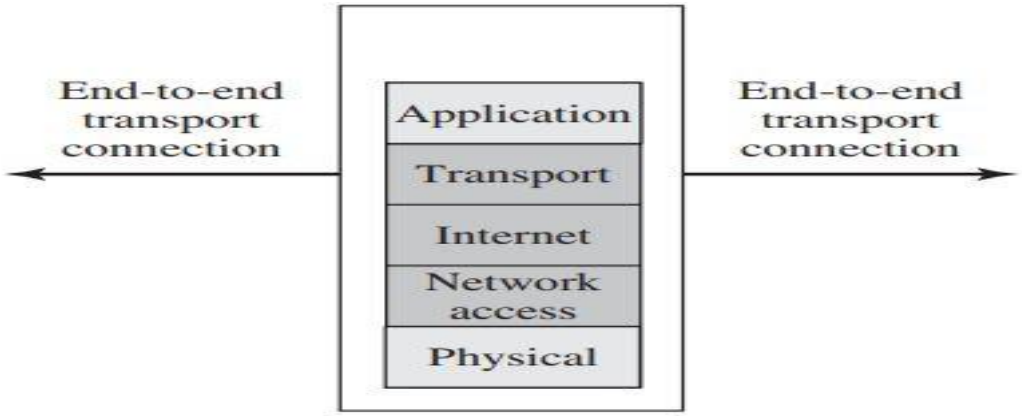
- A packet filtering firewall applies a set of rules to each incoming and outgoing IP packet and then forwards or discards the packet.
- The firewall is typically configured to filter packets going in both directions (Inbound and outbound).
- Filters traffic based on the information of network and transport layer.
  - IP header
  - TCP/UDP header

- Filtering rules are based on information contained in a network packet:
  - **Source IP address:** The IP address of the system that originated the IP packet (e.g., 192.178.1.1).
  - **Destination IP address:** The IP address of the system the IP packet is trying to reach (e.g., 192.168.1.2).
  - **Source and destination transport-level address:** The transport-level (e.g., TCP or UDP) port number.
  - **IP protocol field:** Defines the transport protocol.
  - **Interface:** For a firewall with three or more ports, which interface of the firewall the packet came from or which interface of the firewall the packet is destined for.

Packet Filtering Firewall (Contd..)

- Set up as a list of rules based on matches to fields in the IP or TCP header.
- If there is a **match** to one of the rules, that **rule is invoked** to determine whether to forward or discard the packet.
- If there is **no match** to any rule, then a **default action** is taken.
- Two default policies are possible:
  - discard: That which is not expressly permitted is prohibited.
  - forward: That which is not expressly prohibited is permitted.

Packet Filtering Firewall (Contd..)



Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet filtering firewall rule example

Attacks on packet filtering

- **IP address spoofing:** The intruder transmits packets from the outside with a source IP address field containing an address of an internal host.

- **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.

- **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.

2.Stateful Inspection Firewalls

- A traditional packet filter makes filtering decisions on an individual packet basis and does not take into consideration any higher-layer context.

- A stateful packet inspection firewall tightens up the rules for TCP traffic by creating a directory of outbound TCP connections.

- The packet filter will now allow incoming traffic only for those packets that fit the profile of one of the entries in this directory.

Stateful Inspection Firewalls(Contd...)

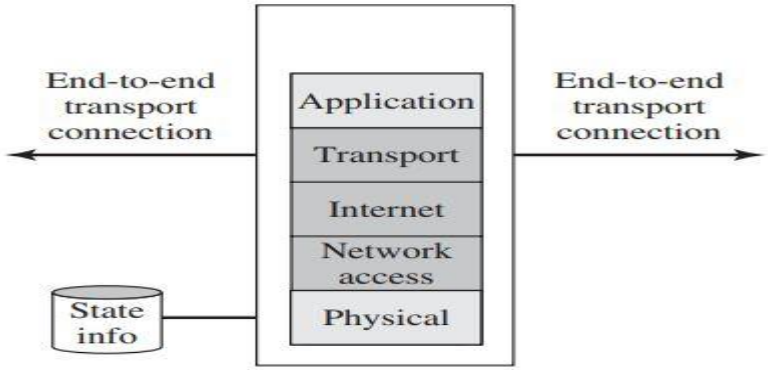


Table 9.2 **Example Stateful Firewall Connection State Table**

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

3. Application-Level Gateway

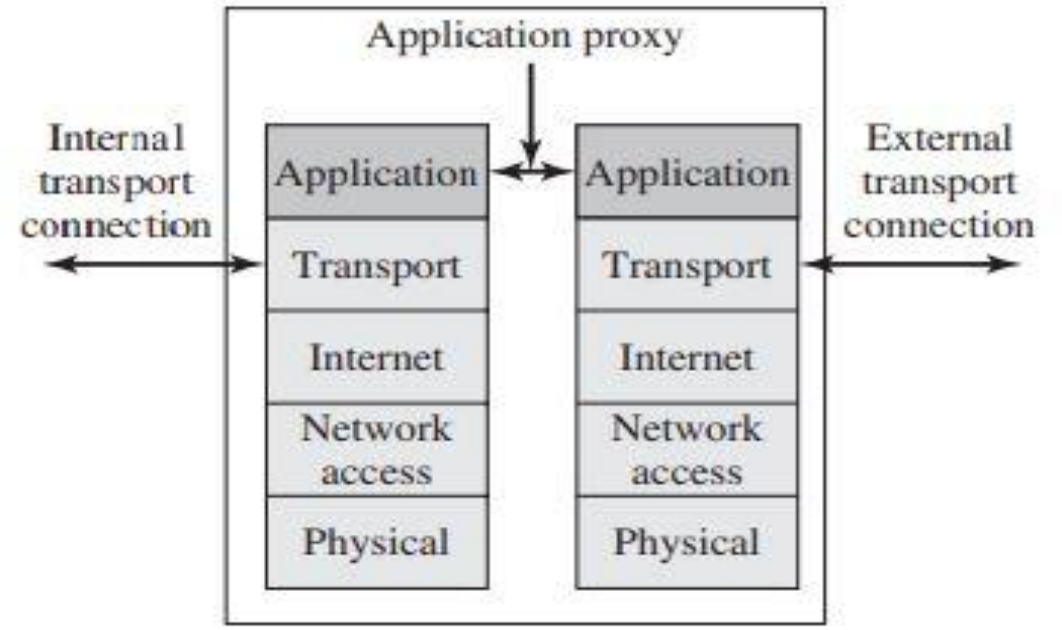
- Sometimes we need to filter a message based on the information available in the message itself (at the application layer).
- It also called an application proxy, acts as a relay of application-level traffic.
- The application gateway must implement the proxy code for each specific application for which the traffic is allowed.
- The gateway can be configured to support only specific features of an application that the network administrator considers acceptable while denying all other features.

Application-Level Gateway(Contd...)

Process of an application level gateway:

- When the user client process sends a message, the application gateway runs a server(proxy) process to receive the request.
- The server opens the packet at the application level and finds out if the request is legitimate.
- The server opens the packet at the application level and finds out if the request is legitimate.
  - If it is, the server acts as a client process and sends the message to the real server.
  - If it is not, the message is dropped and an error message is sent out.

Application-Level Gateway(Contd..)



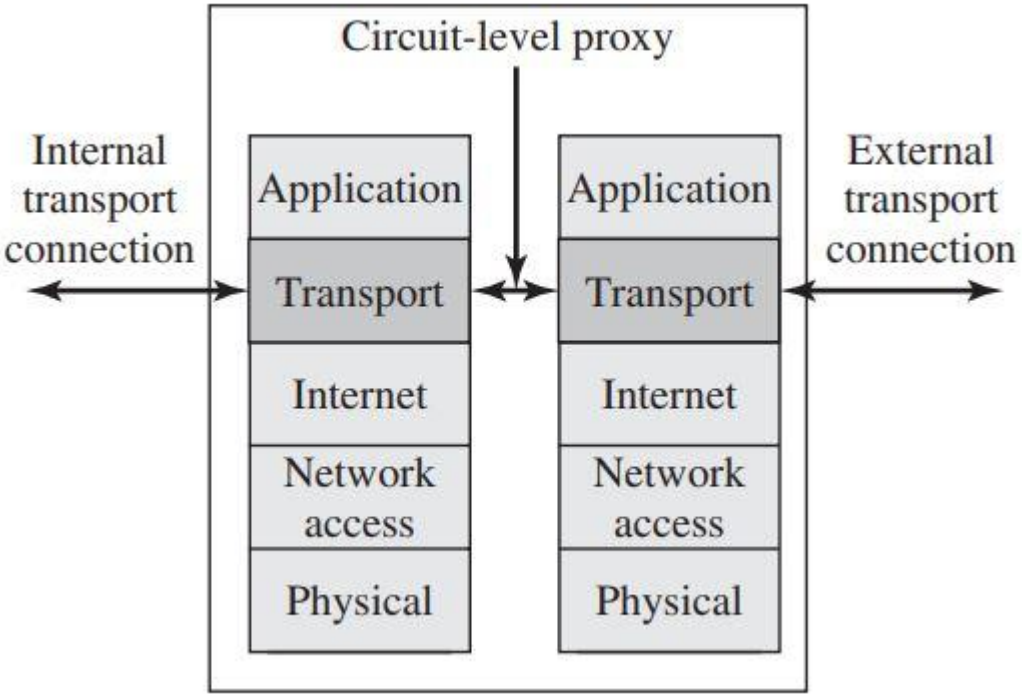
Application-Level Gateway(Contd...)

- Application-level gateways tend to be more secure than packet filters.
- It is easy to log and audit all incoming traffic at the application level.
- Disadvantage of this type of gateway is the additional processing overhead on each connection.

4. Circuit-Level Gateway

- A circuit-level gateway does not permit an end-to-end TCP connection.
- The gateway sets up two TCP connections,
  - one between itself and a TCP user on an inner host
  - one between itself and a TCP user on an outside host.
- As with an application gateway, a circuit-level gateway does not permit an end-to-end TCP connection.
- Implementations of circuit level gateway is SOCKS (Version 5 of SOCKS is specified as RFC 1928)

Circuit-Level Gateway (Contd…)



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

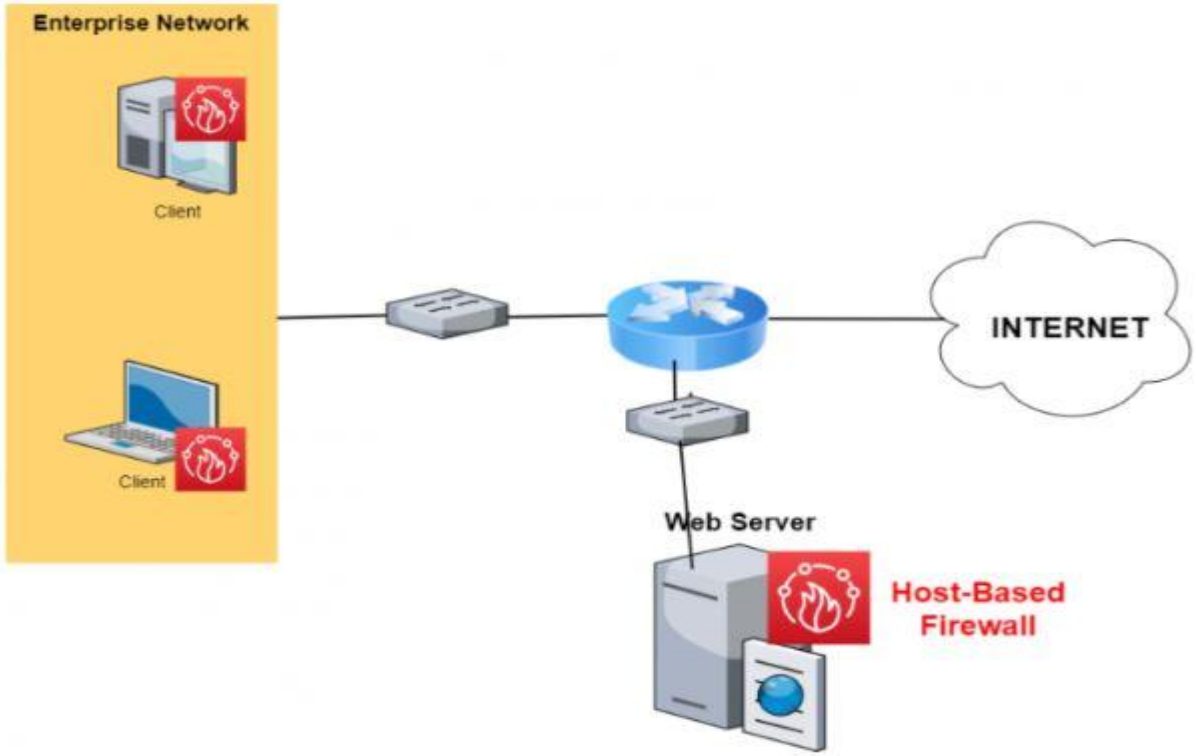
- A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security.
- Typically, the bastion host serves as a platform for an application-level or circuit-level gateway i.e. The proxy servers.
- Characteristics of Bastion Host:
  - Contains secured version of OS.
  - Only Services essential for proxy services Eg: FTP,HTTP,SMTP DNS etc.
  - Each proxy is configured to support subset of applications.
  - Each proxy is independent of other proxies.
  - Maintains audit information by logging all traffic.
  - Each proxy is configured to allow access only to specific host systems.

Host-Based Firewalls

- A host-based firewall is a software module used to secure an individual host.
- Such modules are available in many operating systems or can be provided as an add-on package.
- Like conventional stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets.

Host-Based Firewalls

- A common location for such firewalls is a server or a client machine. Also called as Server-Based or Workstation-based firewall.



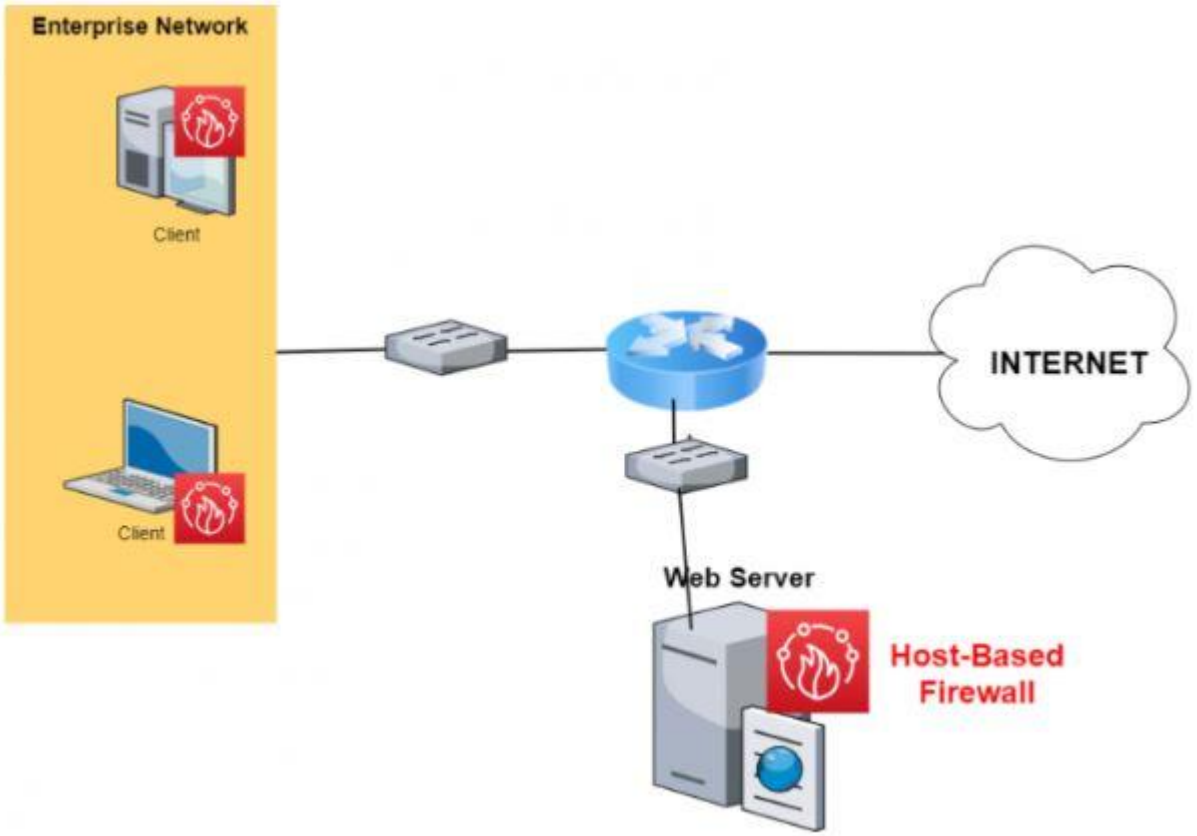
Network-Based Firewall

- It used to protect whole computer networks from attacks and also for controlling network traffic so that only allowed packets are able to reach your workstations and servers.

- Firewall filters traffic going from Internet to secured LAN and vice versa.

- At the Perimeter or border of the network like Internet handoff point to address the unauthorized access from the entry/exit point.

Network-Based Firewall



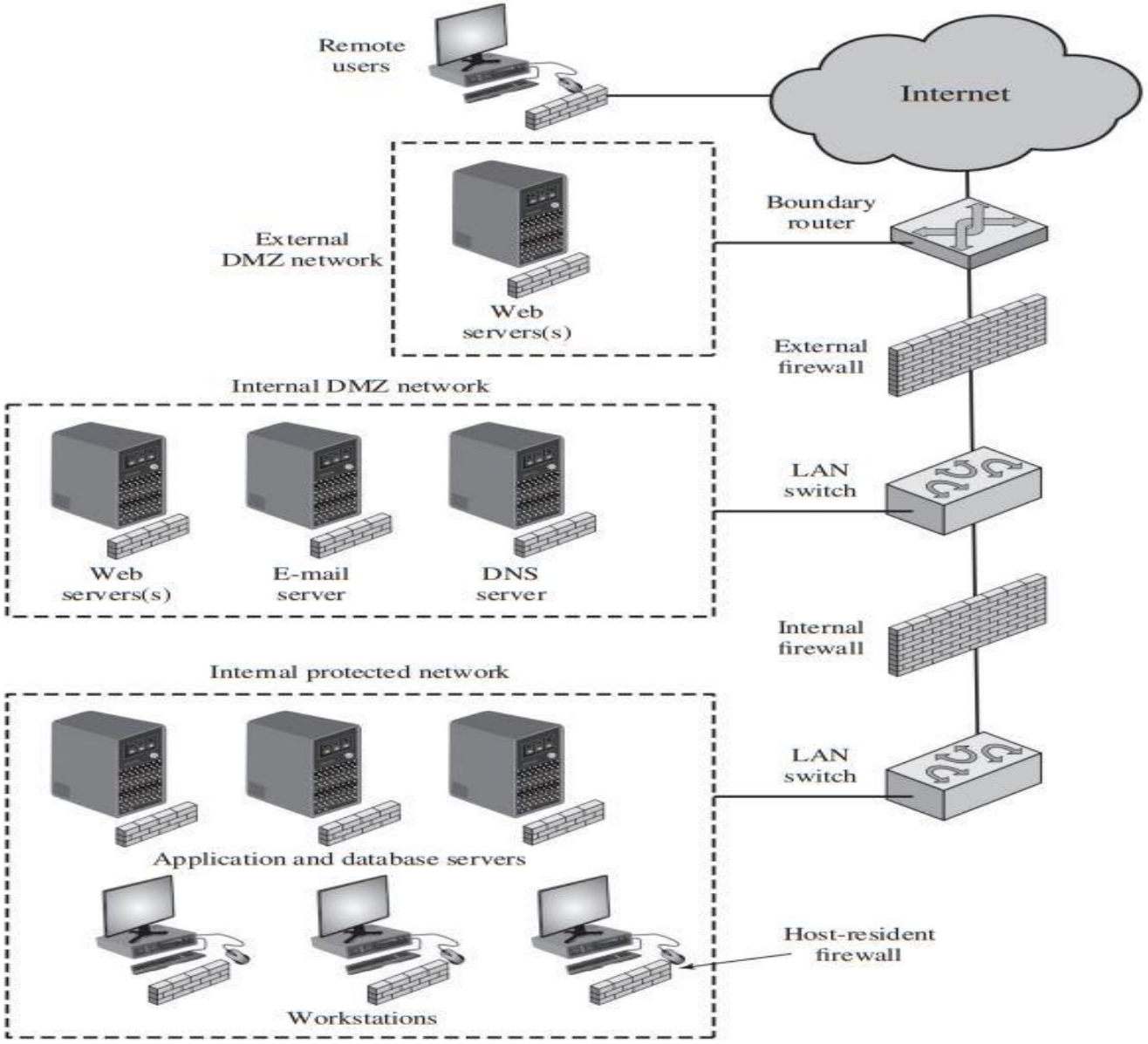
Zoning

- Zoning is one of the ways to segment the networks in sub networks.
- It is used to mitigate the risk of open network by segmenting infrastructure services into logical groupings that have the same communications security policies and security requirements.
- Demilitarized Zone (DMZ): It is a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from un-trusted traffic.
  - External DMZ
  - Internal DMZ

Internal and External Firewalls

- **Internal Firewall:** Used to protect internal protected systems.
- **External Firewall:** Used to protect DMZ networks as well as the internal protected systems.
- Multiple internal firewall can protect different systems in the internal network.
- Internal firewall are more stringent than external firewall.

Firewalls in a network



Scope of firewall

- A firewall defines a single choke point that attempts to keep unauthorized users out of the protected network.
- A firewall provides a location for monitoring security-related events.
- A firewall can serve as the platform for IPSec.
- 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
  - network management function that audits or logs Internet usage.

Limitations of Firewall

- The firewall cannot protect against attacks that bypass the firewall.
- The firewall may not protect fully against internal threats.
- An improperly secured wireless LAN may be accessed from outside the organization.
- A laptop or portable storage device may be used and infected outside the corporate network and then attached and used internally.