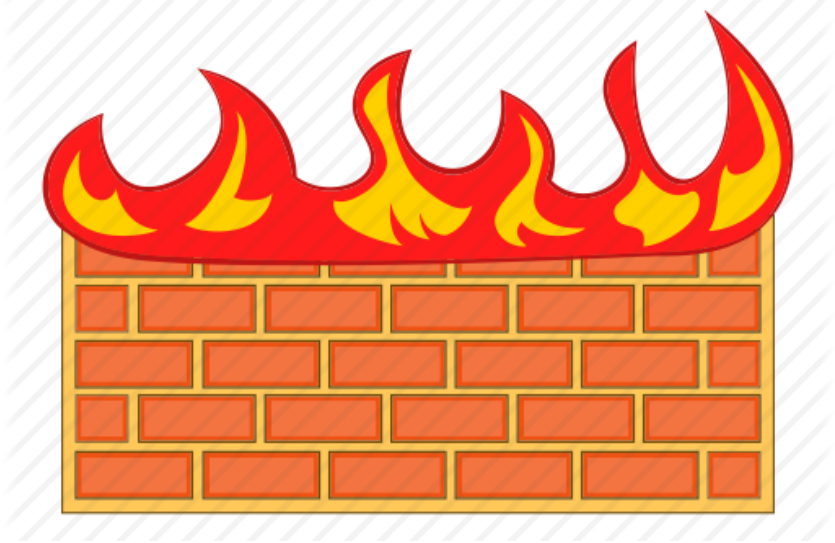
BAHRIA UNIVERSITY
Discovering Knowledge



Firewalls

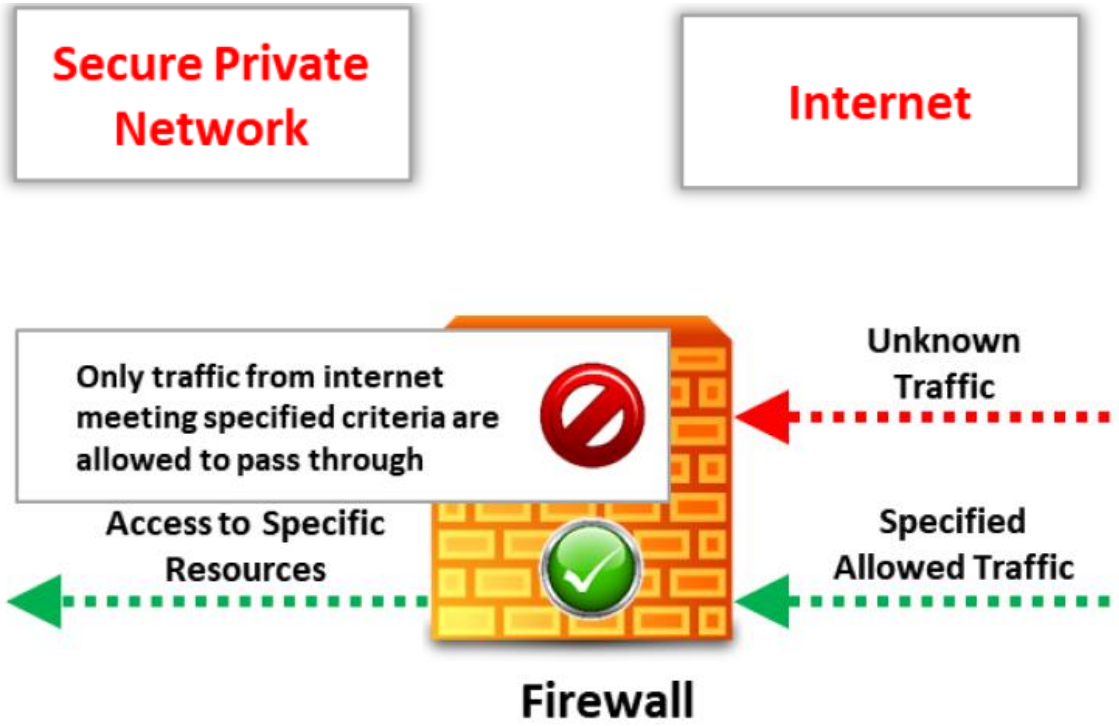
Information Security (CSC-407)

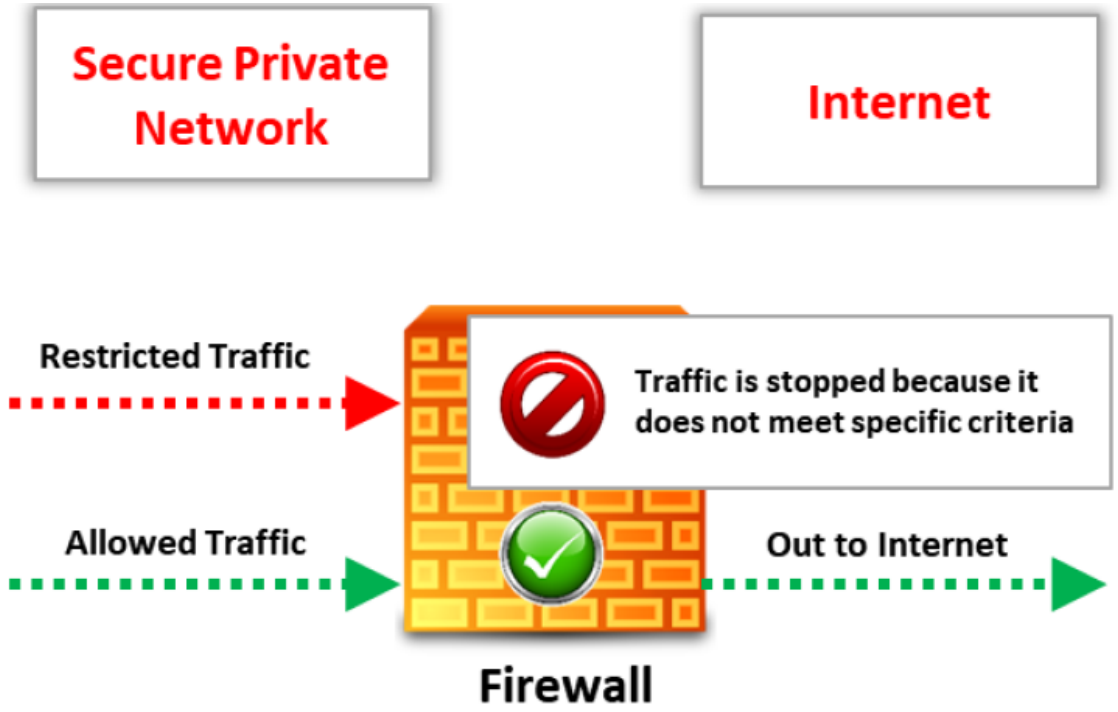
Fall 2024 (BSE-7A & 7B)

Firewall: An Overview

- **Firewall:** an information security program that prevents specific information from moving between two **different networks** or **levels of a network**.
- **Firewall** monitors and **filters** the **incoming** and **outgoing** traffic of the network. Hence controlling movement of information between **untrusted network** ***(e.g. the Internet)*** and **trusted network** **(*e.g. organization's internal network)***.
- **Firewall** is a ***software*** or ***hardware*** or a ***combination of both***.

Firewall: An Overview (Cont.)



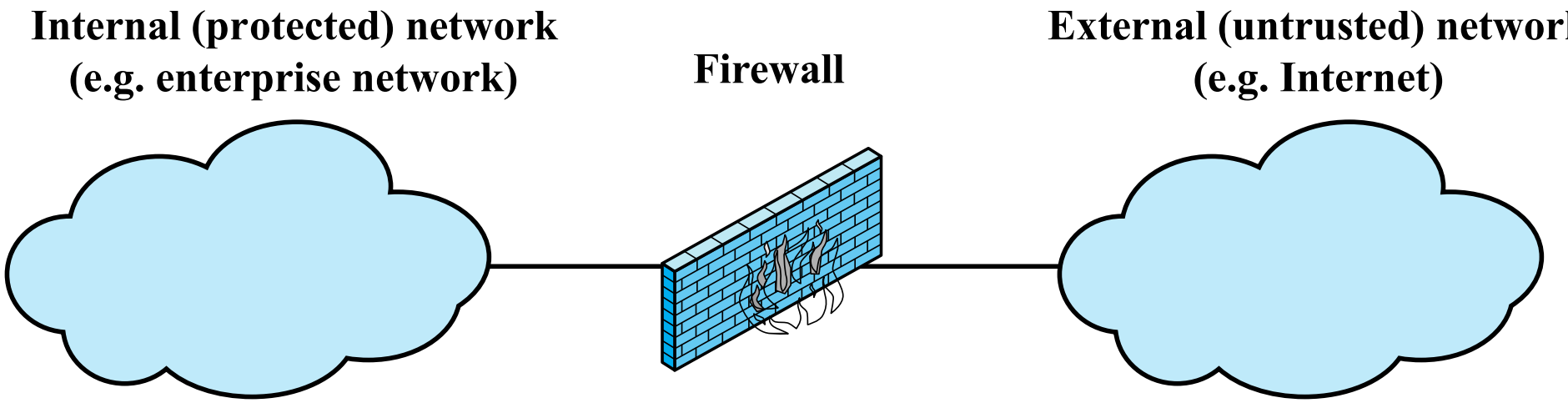


Need for Firewall

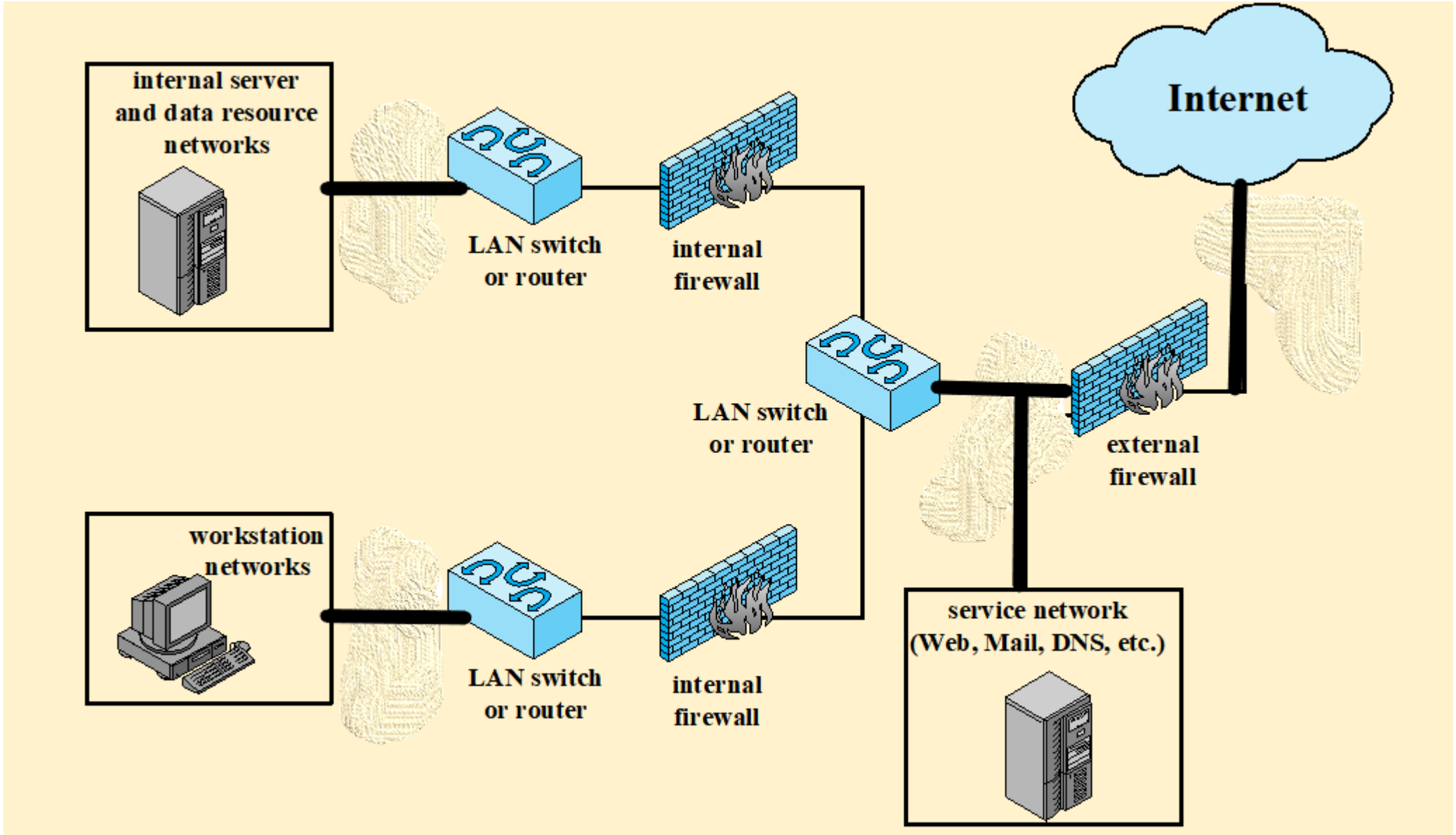
- Users within an organization need Internet access, usually provided **via LAN**.
- However, an Internet access may enable the **outside world** to reach and interact with local network assets.
- Though, it's possible to equip each ***workstation*** and ***server*** with **host-based** security services, but this is not **cost-effective**.
- A widely accepted complement to **host-based** security services is the **firewall**.

Firewall Placement

- Firewall can be a separate computer or a software service running on an existing computer ***(e.g. on a router or server)***.
- Firewall is usually placed between **premises network** and the **Internet.**



Example of Firewalls Deployment



Firewall Objective

Firewall Installation Objectives:

- To provide a **single choke point** where security and auditing can be imposed.
- To **protect premises network** from Internet-based attacks.
- To **restrict access** of hosts on private network.
- To provide an additional layer of defense ***(defense in depth)***.

Firewall Design Goals

Design goals for a firewall:

- All traffic from inside to outside, and vice versa, must pass through the **firewall**.
- The **firewall** may be a ***single computer*** system or a ***set of two or more systems*** that cooperate to perform firewall function.

Firewall Access Policies

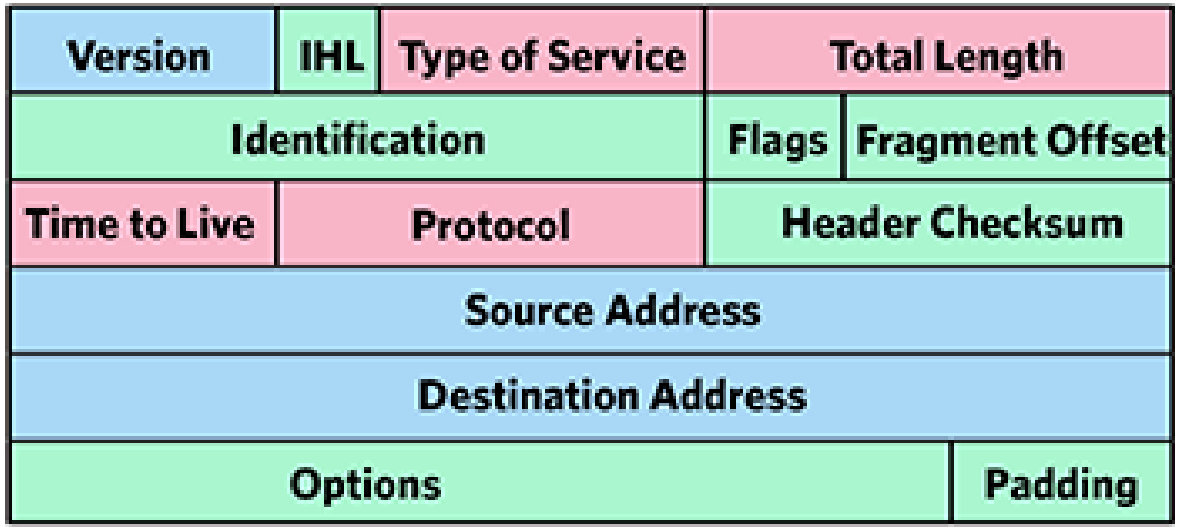
- A critical component in planning and implementation of a **firewall** is specifying a suitable **access policy**.
- **Access policy** lists the types of traffic authorized to pass.
- Only **authorized traffic**, defined by the **access policy**, will be allowed to pass.
- **Access policy** should be developed from **organization's broad specification and policy**, i.e. which traffic types the organization needs to support or to deny.

Firewall Access Policies (Cont.)

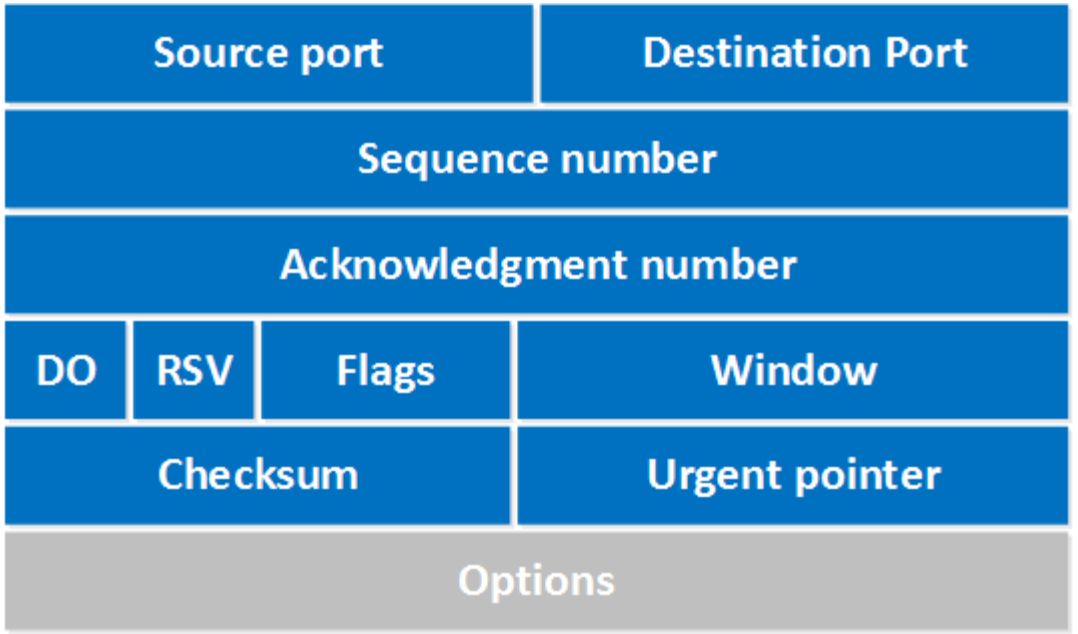
Characteristics for firewall's access policy to filter traffic:

- **IP Address and Protocol Values:** typically used to limit access to specific services.
  - Control access based on source or destination **IP addresses** and **port numbers**.
  - Control access based direction of flow, i.e. being **inbound** or **outbound**.
  - Control access based on other **network** and **transport** layer characteristics.

Firewall Access Policies (Cont.)



IP Header



TCP Header

Firewall Access Policies (Cont.)

Characteristics for firewall's access policy to filter traffic (Cont.):

- **Application Protocol:** controls access based on **authorized application protocol's data**.
  - Used by an **application-level gateway** that monitors the exchange of information for specific **application protocols**.
  - **E.g.,** checking HTTP web requests to authorized sites only.

Firewall Access Policies (Cont.)

Characteristics for firewall's access policy to filter traffic (Cont.):

- **User Identity:** controls access based on users identity. Typically for inside users who identify themselves using some form of secure authentication technique. ***(e.g. through IP/MAC address)***
- **Network Activity:** controls access based on considerations involving activities in the network, such as:
  - The **time of request**, e.g., only in business hours.
  - The **rate of requests**, e.g., to detect scanning attempts.

Firewall Limitations

Firewalls have limitations, including the following:

- Firewall cannot protect against attacks that **bypass the firewall**. **E.g.,** an internal systems having mobile broadband access.
- Firewall may not protect fully against **internal threats**, such as an employee who cooperates with an external attacker ***(Willingly / Unwillingly)***.
- An improperly secured **WLAN** may be accessed from outside.
- An **infected laptop** or **portable storage device** attached and used internally in the corporate network.

Types of Firewalls

Types of Firewalls

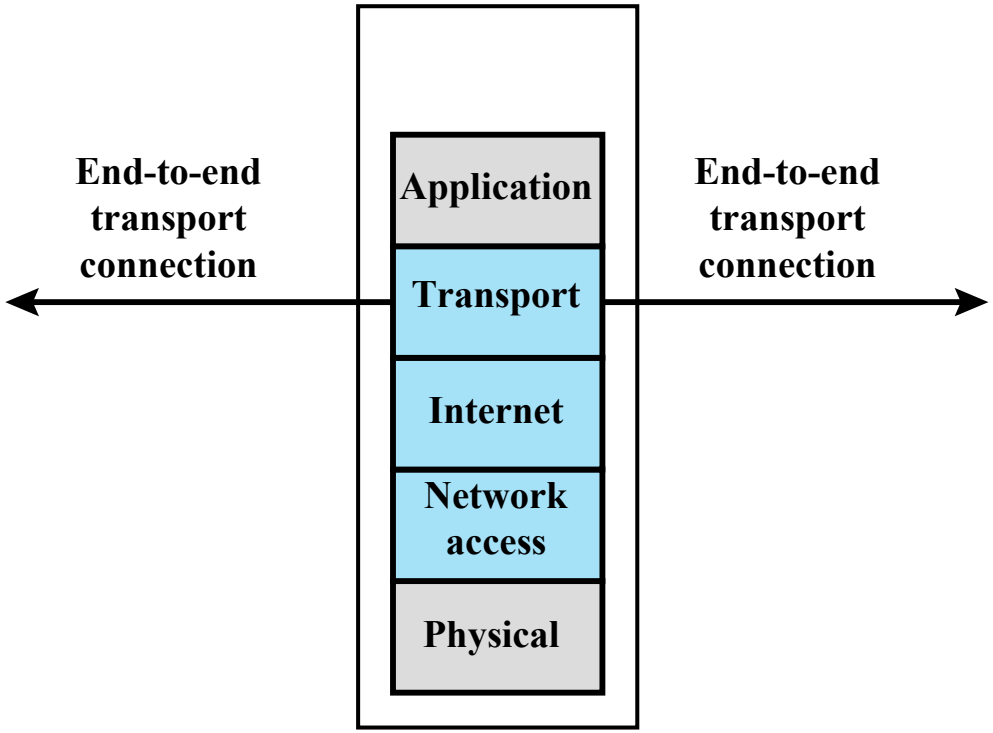
The principal types of firewalls are:

1. Packet Filtering Firewall ***(low-level network packets)***.
2. Stateful Inspection Firewalls ***(all traffic within a transport connection)***.
3. Application-Level Gateway ***(inspecting details of application protocols)***.

- Choice of which type is appropriate is determined by the desired **firewall's access policy**.

Packet Filtering Firewall

- **Packet filtering firewall** applies a set of rules to each **incoming** and **outgoing IP packet** which then either forwards or discards the packet.
- The firewall is typically configured to filter packets going in both directions ***(i.e. from and to the internal network)***.
- **Packet filtering firewall** are usually part of a **router**.



(b) Packet filtering firewall

Packet Filtering Firewall (Cont.)

- The **packet filter** is typically set up as a "list of rules" based on matching to fields in the **TCP/IP 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:*** what is not explicitly permitted is prohibited.
  - ***Forward:*** what is not explicitly prohibited is permitted.

Packet Filtering Firewall (Cont.)

Default = Discard:

- The default discard policy is **more conservative**.
- Initially, everything is blocked and services must be added on a **case-by-case** basis.
- This policy is more visible to users, who are more likely to see the firewall as a **"hindrance"**. However, visibility to users diminishes **as rules are created**.
- However, this is the policy likely to be preferred by businesses and government organizations.

Packet Filtering Firewall (Cont.)

Default = Forward:

- The default forward policy increases ease of use for end users but provides **reduced security**.
- Security administrator must react to each new security threat as it becomes known.
- This policy may be used by generally **more open organizations**, such as **universities**.

Packet Filtering Firewall (Cont.)

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 (Cont.)

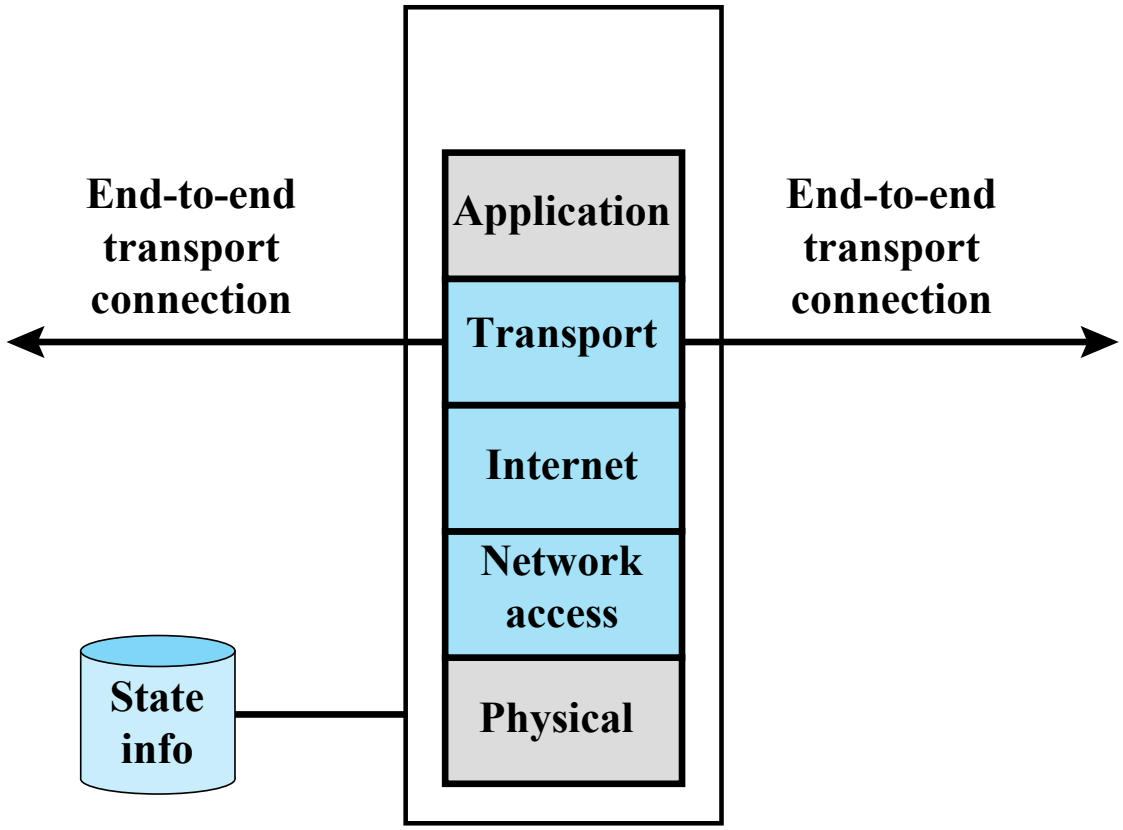
Strength: simple, transparent to users and very fast.

Weaknesses:

1. Cannot prevent attacks that employ **application-specific** vulnerabilities or functions. **E.g.** a **packet filter firewall** cannot block specific **application command(s)**, where if application is allowed then all functions within it will be permitted.
2. Vulnerable to attacks that exploits problems within the **TCP/IP protocol stack**, such as network layer **address spoofing**.
3. Susceptible to security breaches caused by improper configurations.

Stateful Inspection Firewalls

- A **stateful packet inspection (SPI)** firewall keeps track of each **network connection** between internal and external systems using a **state table**.
- A **SPI** firewall tightens up the rules for TCP traffic by creating a directory of **outbound TCP connections**.



(c) Stateful inspection firewall

Stateful Inspection Firewalls

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

Stateful Inspection Firewalls (Cont.)

- In previous table, there is **an entry** for each currently established connection.
- **SPI** firewall will allow incoming traffic only for packets that match entries in directory.
- If **SPI** firewall receives an incoming packet that it cannot match in its **state table**, it will review the same packet information as a **packet filtering firewall *(i.e. refers to its ACL)*** to determine whether to allow the packet to pass or not.

Stateful Inspection Firewalls (Cont.)

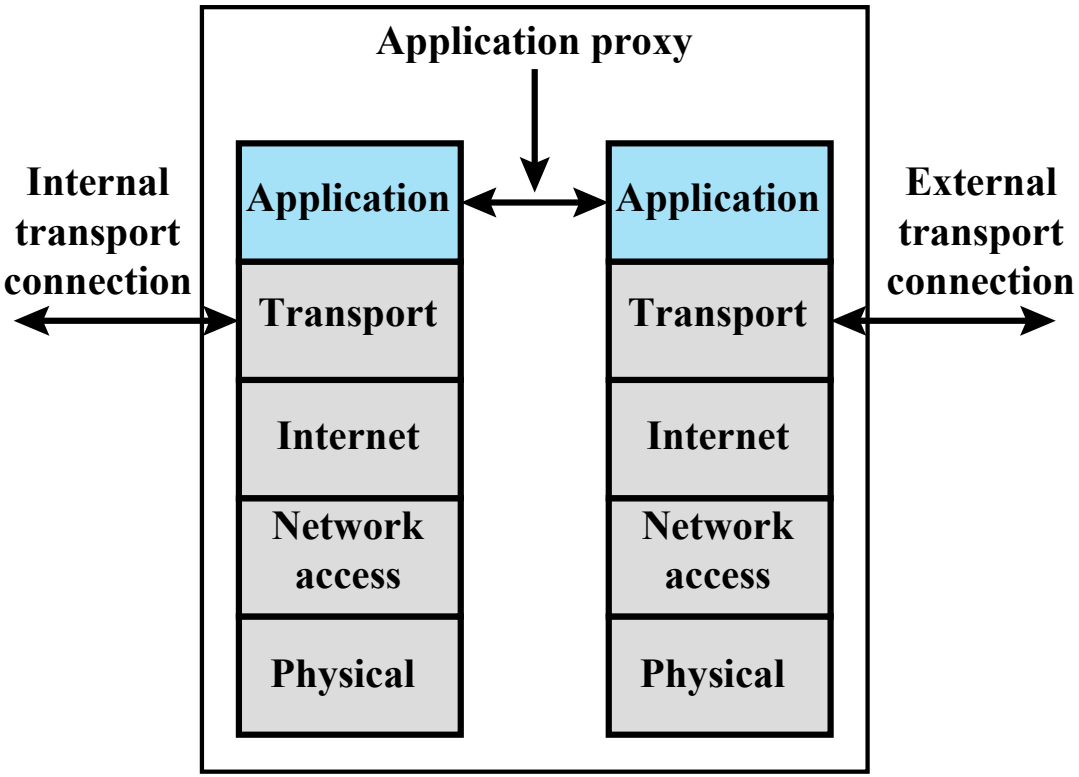
- Some **stateful firewalls** also keep track of **TCP sequence numbers** to prevent attacks that depend on the sequence number, such as **session hijacking**.

Weaknesses:

- The primary disadvantage of **SPI** firewall is the additional processing required to manage and verify packets against the **state table**.

Application-Level Gateway

- **Application-level gateway** also called **application proxy** ***OR*** **application firewall** ***OR*** **proxy server**.
- The **application-level gateway** need only scrutinize few "allowable applications" rather than dealing with **numerous possible combinations** at TCP / IP level.

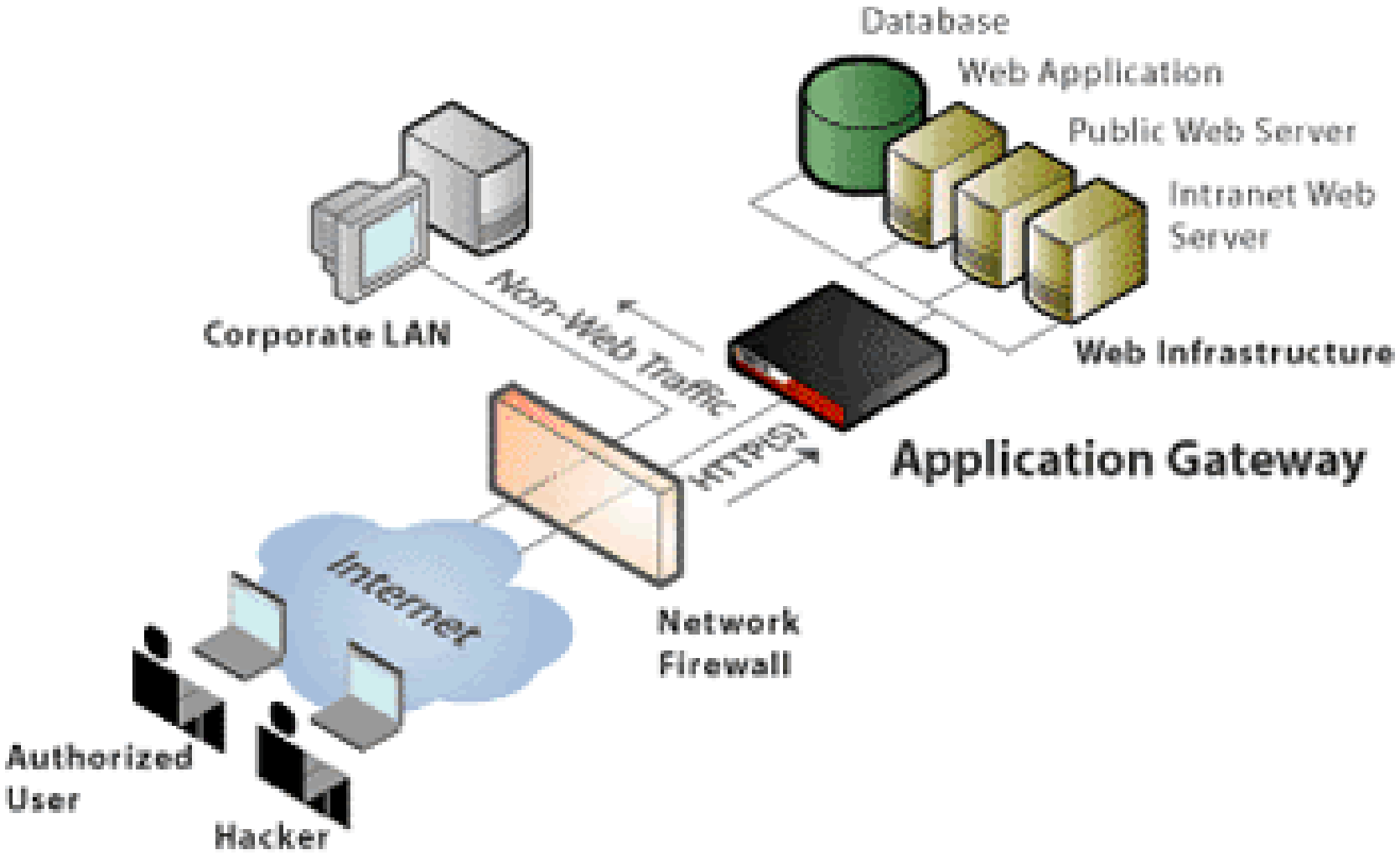


(d) Application proxy firewall

Application-Level Gateway (Cont.)

- **Application-level gateway** is usually installed on a dedicated computer.
- **Application-level gateway** can be configured to run special software that acts as a **proxy for a service request**.
- **Application-level gateway** acts as a **relay** of **application-level traffic**.

Application-Level Gateway (Cont.)



Application-Level Gateway (Cont.)

Access Mechanism:

- **User** contacts gateway using a TCP/IP application, such as Telnet or FTP.
- Gateway asks the user for name of the ***remote host*** to be accessed.
- User responds and provides valid authentication information.
- Gateway contacts the application on the ***remote host*** and **relays** TCP segments containing the application data between the two endpoints ***(i.e. user and remote host)***.

Application-Level Gateway (Cont.)

Access Mechanism (Cont.):

- If gateway does not implement the **proxy code** for a **specific application**, the service is not supported and cannot be forwarded across the **firewall**.
- Gateway can be configured to support only **specific features** of an application ***(e.g. WhatsApp messages and voice notes only)***.
- **Example;** gateway receives requests for Web pages, then accesses the Web server on behalf of the external client, and returns the requested pages to the users.

Application-Level Gateway (Cont.)

Strength:

- Tend to be more secure than packet filters.
- Easy to log and audit all incoming traffic.

Weaknesses:

- Additional processing overhead on each connection.

Thank You!