

Information Security

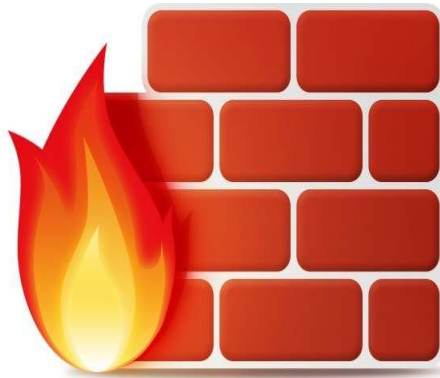
CS3002

Lecture 22
28th November 2023

Dr. Rana Asif Rehman
Email: r.asif@lhr.nu.edu.pk



Firewalls



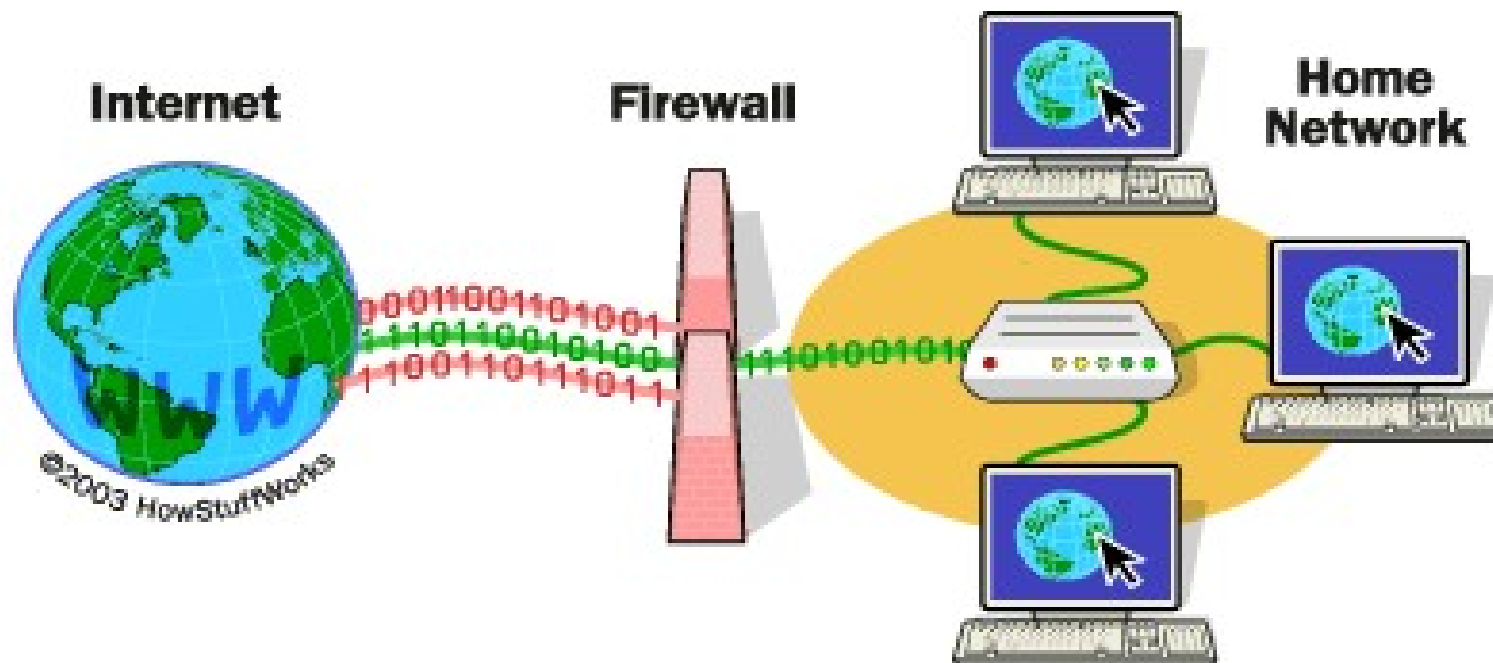
Firewalls



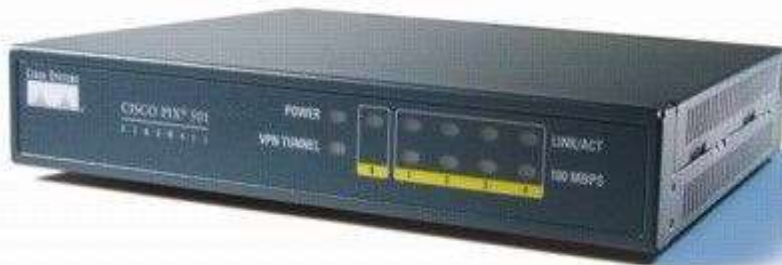
A **firewall** is a **device** or **application** that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network.

- Usually **runs** on a **dedicated device** for better performance.
- The **purpose** of a firewall is to keep "bad" things outside a protected environment.
- Firewall implements a **Security Policy (Rules)**
- **Security policy** might permit accesses only from certain places, from certain users, or for certain activities.

Firewalls



Firewalls



Cisco Firewall Device



Juniper Firewall Device

Great Firewall of China



Home Task

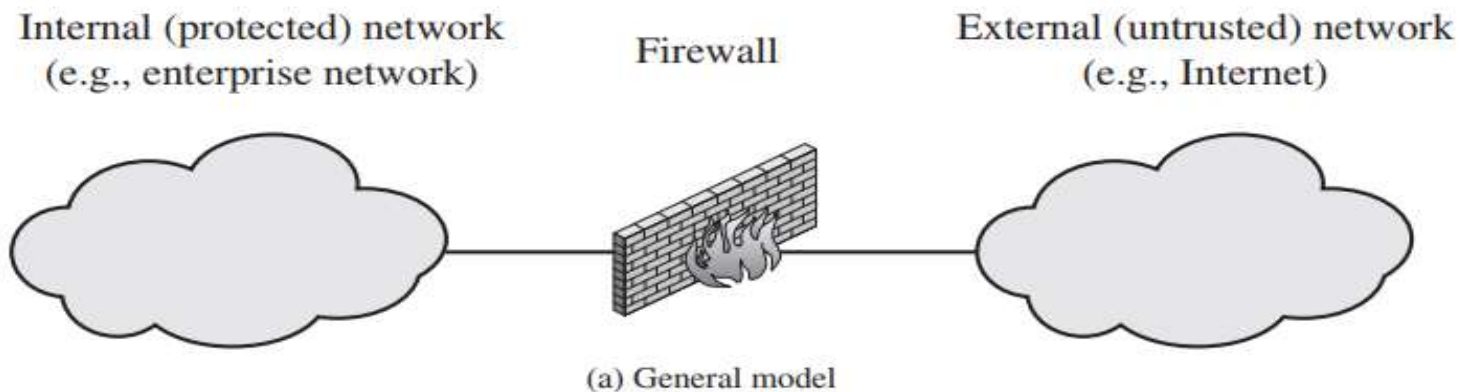
- ❑ Search and Read
How
Great
Firewall
of China
Works?



The Need for Firewalls



- Internet connectivity is essential for organizations
 - However it creates a threat
- Firewalls are effective means of protecting LANs
 - Protection at single point, rather on every computer within LAN
- Inserted between the premises network and the Internet to establish a controlled link
- Used as a perimeter defense
 - Single choke point to impose security and auditing
 - Insulates the internal systems from external networks



Firewall Characteristics



Design Goals

- All traffic from inside to outside must pass through the firewall
- Only authorized traffic as defined by the local security policy will be allowed to pass
- The firewall itself is immune to penetration

General Techniques

- Service control, e.g. filter based on IP address, port number
- Direction control, e.g. to internal LAN, to external Internet
- User control, e.g. student vs faculty
- Behaviour control, e.g. filter email with spam

Capabilities & Limitations



Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as platform for VPN end point

Limitations

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, phone, or USB drive may be infected outside the corporate network then used internally

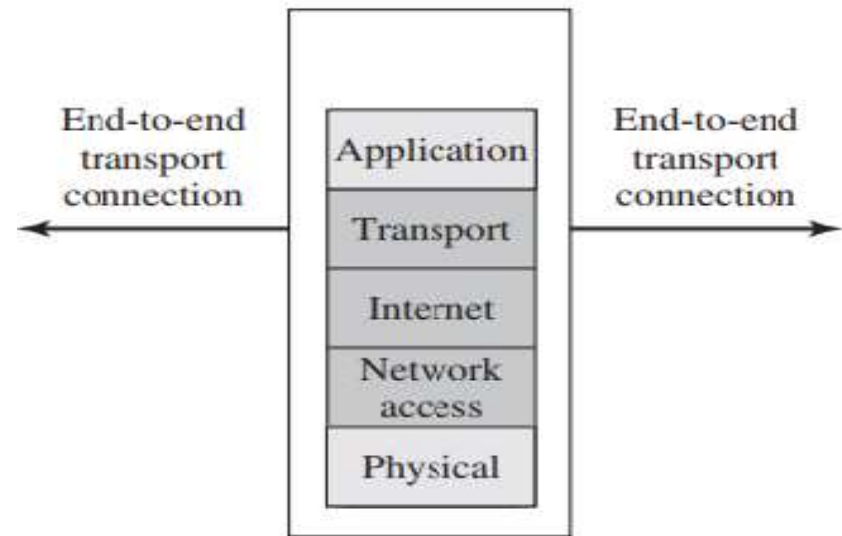
Types of Firewalls



- **Packet Filtering** accepts/rejects packets based on protocol headers
- **Stateful Packet Inspection** adds state information on what happened previously to packet filtering firewall
- **Application Proxy** relay for application traffic
- **Circuit-level Proxy** relay for transport connections
- Normally a firewall is implemented on a router
- That router may perform other (non-)security functions, e.g. VPN end-point, accounting, address and port translation (NAT)

1. Packet Filtering Firewall

- Security policy implemented by set of rules
- Rules define which packets can pass through the firewall
- Firewalls inspect each arriving packet (in all directions), compares against rule set, and takes action based on matching rule
- Default policies: action for packets for which no rule matches
- Accept (allow, forward)
- Drop (reject, discard)



(b) Packet filtering firewall

Packet Filtering Rules

Packet Information

- IP address: identifies host or network
- Port number: identifies server, e.g. web (80), email (25)
- Protocol number: identifies transport protocol, e.g. TCP or UDP
- Firewall interface: identifies immediate source/destination
- Other transport, network, data link packet header fields

Rules

- Conditions defined using packet information, direction
- Wildcards (*) support to match multiple values
- Actions typically accept or drop
- List of rules processed in order

Packet Filtering Firewalls

Advantages

- Simplicity
- Transparent to users
- Very fast

Disadvantages

- Cannot prevent attacks that employ application specific vulnerabilities or functions
- Limited logging functionality
- Do not support advanced user authentication
- Improper configuration can lead to breaches

Example

Examples

This example shows how to build a fundamental packet filter set for SMTP based traffic:

Scenario 1: Allowing inbound and outbound SMTP (sending and receiving electronic mail). Our initial packet filter rule set would be:

Rule	Direction	Src Address	Dest Address	Protocol	Dest Port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Rule A and B allow inbound SMTP connections (incoming email).

Rule C and D allow outbound SMTP connections (outgoing email).

Rule E is the default rule that applies if all else fails.

Packet Filtering Firewalls

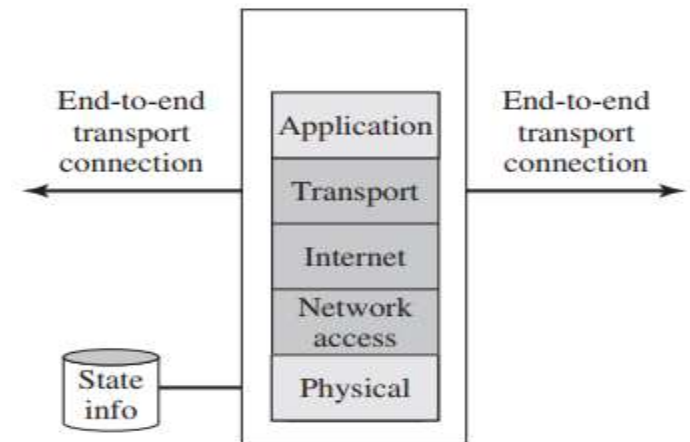
- Uses transport-layer information only
 - IP Source Address, Destination Address
 - Protocol/Next Header (TCP, UDP, ICMP, etc)
 - TCP or UDP source & destination ports
 - TCP Flags (SYN, ACK, FIN, RST, PSH, etc)
 - ICMP message type
- Examples
 - DNS uses port 53
 - No incoming port 53 packets except known trusted servers

2. Stateful Packet Inspection

- Traditional packet filtering firewall makes decisions based on individual packets; don't consider past packets (stateless)
- Many applications establish a connection between client/server; group of packets belong to a connection
- Often easier to define rules for connections, rather than individual packets
- Need to store information about past behavior (stateful)
- Stateful Packet Inspection (SPI) is extension of traditional packet filtering firewalls
- Issues: extra overhead required for maintaining state information

Stateful Packet Inspection

- For connections accepted by packet filtering firewall, record connection information
 - src/dest IP address, src/dest port, sequence numbers, connection state (e.g. Established, Closing)
- Packets arriving that belong to existing connections can be accepted without processing by firewall rules



(c) Stateful inspection firewall

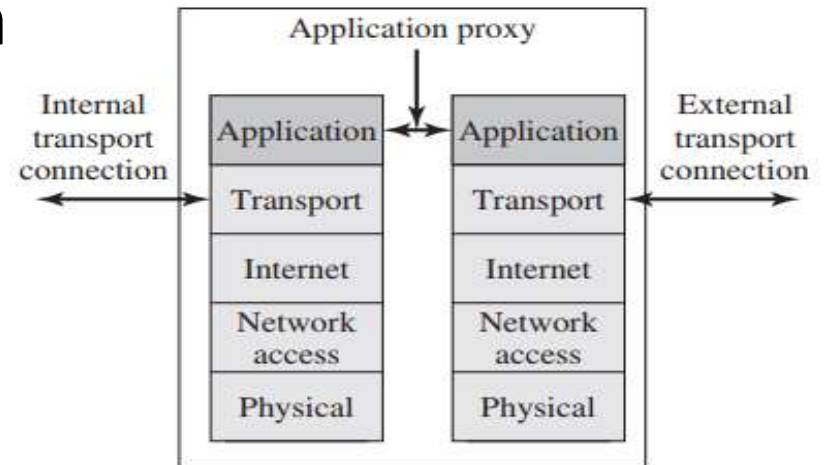
Stateful Packet Inspection

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 Proxy

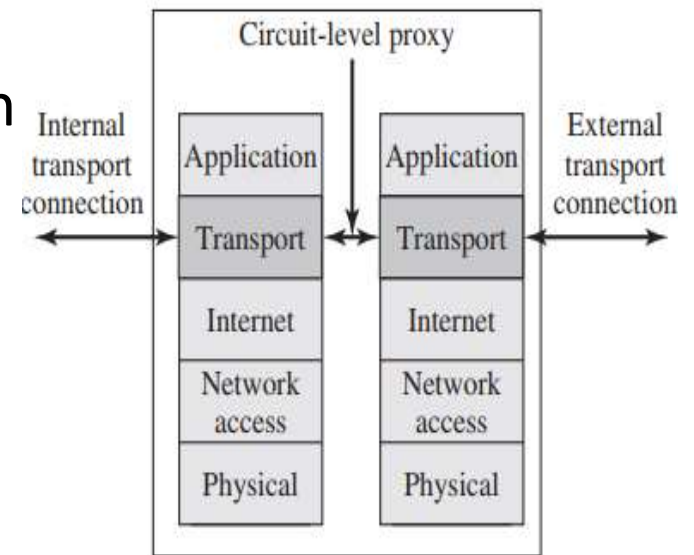
- Also called Application-level Gateway
 - Allows data into/out of a process based on that process' type
 - Can act on a single computer or at the network layer
 - e.g. allowing only HTTP traffic to a website
 - Log access – attempted access and allowed access
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection



(d) Application proxy firewall

4. Circuit-level Proxy Firewall

- Also called Circuit-level Gateway
- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
 - For incoming data
 - Proxy is server to internal network clients
 - For outgoing data
 - Proxy is client sending out data to the internet
- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed
- Typically used when inside users are trusted

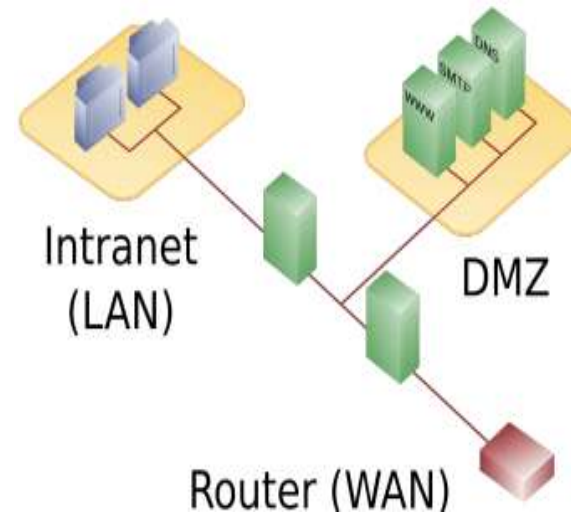
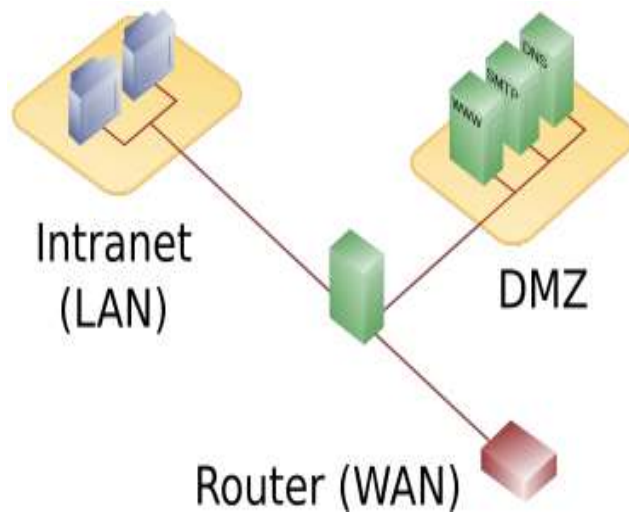


(e) Circuit-level proxy firewall

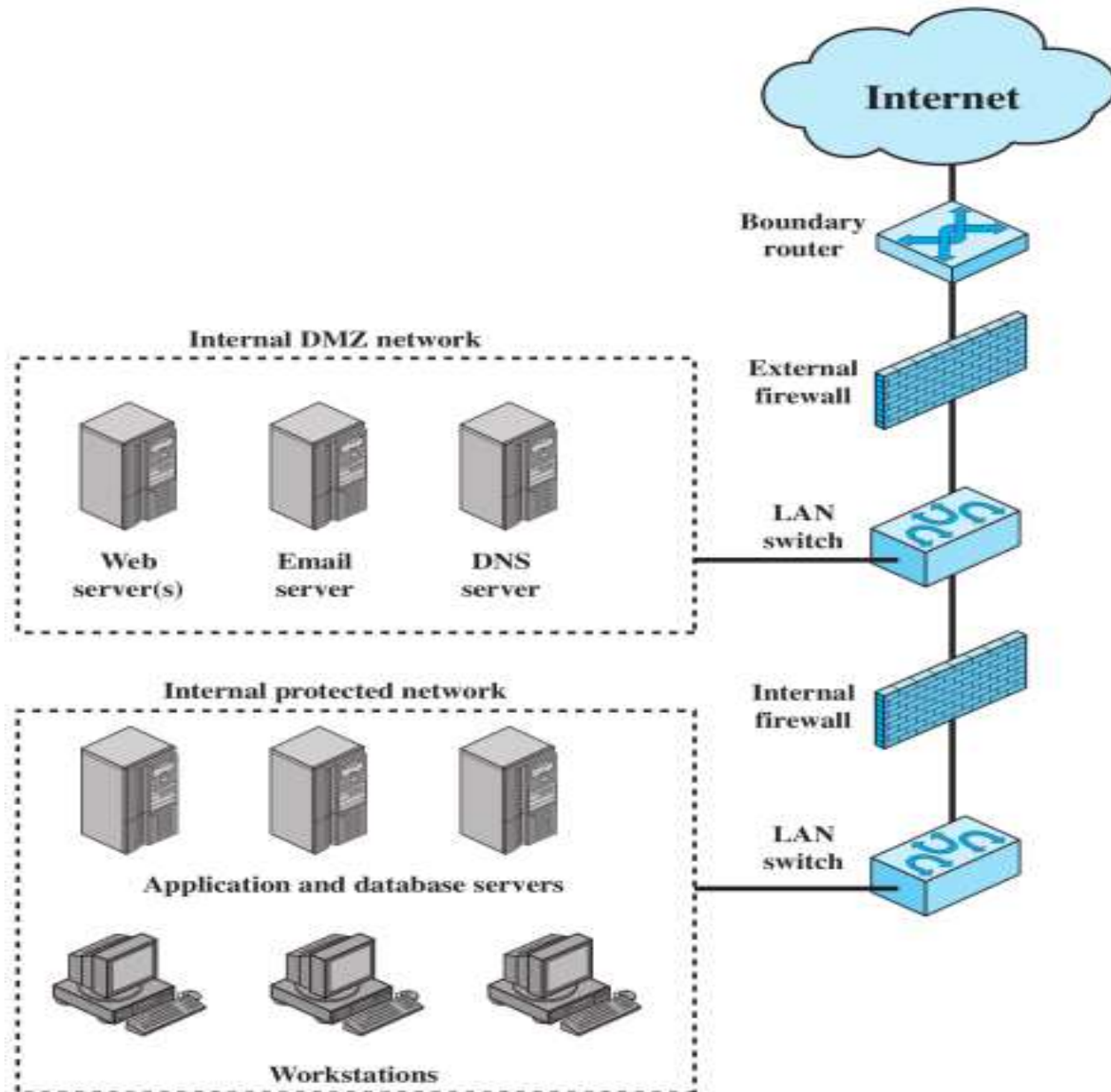
Firewall Locations

- Firewalls can be located on hosts: end-users computers and servers
- With large number of users, firewalls located on network devices that interconnect internal and external networks
- Common to separate internal network into two zones:
 1. Public-facing servers, e.g. web, email, DNS
 2. End-user computers and internal servers, e.g. databases, development web servers
- Public-facing servers put in De-Militarized Zone (DMZ)

DMZ with 1 or 2 Firewalls



Example DMZ with 2 Firewalls



Security Issues

- Complexity and human error: writing firewall rules that implement the security policy is difficult for large networks
- Bypassing security policies using tunnels
- Bypassing firewalls using other networks (WiFi, mobile) or devices (laptop, USB)

Sandboxing

- The process of isolating a program on the hard drive in order to minimize or eliminate the exposure to other apps and critical system.
- Usually programs and applications interact with multiple parts of operating system and use shared resources like storage, memory and CPU sometimes causing conflicts.
- A malware if present can utilize such vulnerabilities to cause a disaster.
- Sandboxing actually helps to reduce the impact that an individual program will have on the system.

Examples of Sandboxing

- Browser sandboxing
 - Google and Opera run in their own sandboxes
 - Other have option of selective sandboxing e.g. Mozilla
- Virtual Machines
 - It is also called manual sandboxing to purposely configure the system to sandbox and application.
 - Virtual Box
 - Vmware
- Windows Sandbox
- A temporary instance of host machine

Penetration Testing

- Penetration testing is the process of evaluating the strengths of all security controls on a computer system or network.
- Penetration tests evaluate procedural, operational as well as technological controls
- **External vs. Internal**
Penetration Testing can be performed from the viewpoint of an external attacker or a malicious employee.
- **Overt vs. Covert**
Penetration Testing can be performed with or without the knowledge of the IT department of the company being tested.

Penetration Testing

- **Reconnaissance and Information Gathering**
To discover as much information about a target (individual or organization) as possible without actually making network contact with said target
- **Network Enumeration and Scanning**
To discover existing networks owned by a target as well as live hosts and services running on those hosts
- **Vulnerability Testing and Exploitation**
To check hosts for known vulnerabilities and to see if they are exploitable, as well as to assess the potential severity of said vulnerabilities
- **Reporting**

Information Gathering

1. Find domain and sub-domain of the target
2. Find similar and parallel domain names
3. Web searches using advanced operators
4. Footprint the target using Shodan
5. Find the geographical location of company
6. List employees and their email addresses
7. Identify the key email addresses through email harvesting
8. Find key personnel of the company
9. Browse social network websites to find information about company and employees
10. Identify the types of network devices used in organization

Information Gathering

11. Search the archive.org for old information about the company
12. Examine the source code of web pages
13. Perform Whois lookup
14. Find IP addresses block allocated to organization
15. Find DNS records for domain
16. Perform reverse lookup
17. Perform DNS zone transfer
18. Draw a network diagram using traceroute analysis

Penetration Testing Types

- **Black box**
 - little or no information is provided about the specified target
- **White box**
 - where almost all the information about the target is provided
- **Gray box**
 - some information is being provided and some hidden