Information Security
CS3002
(Sections BDS-7A/B)
Lecture 26

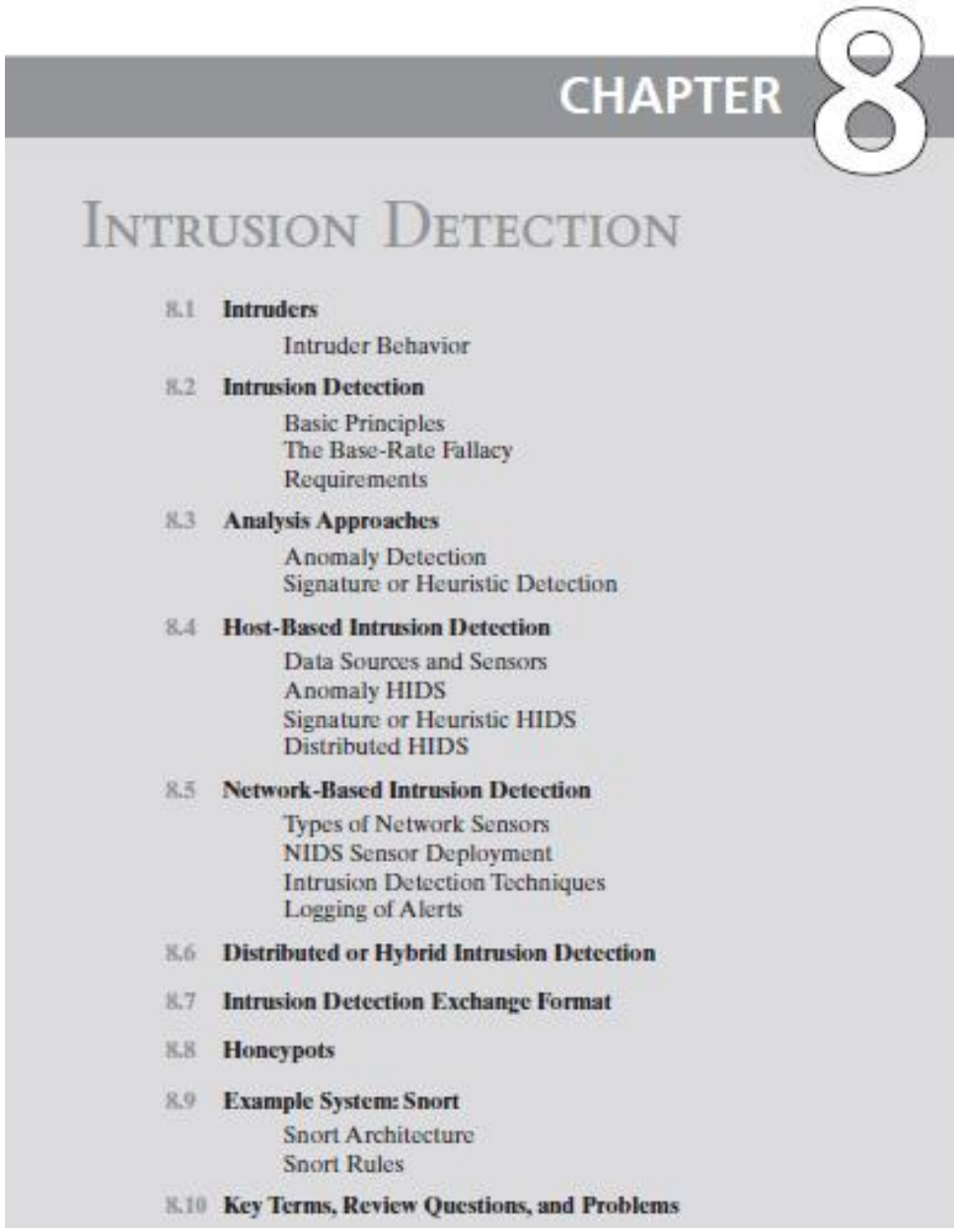
Instructor: Dr. Syed Mohammad Irteza

Assistant Professor, Department of Computer Science

20 November, 2024

Previous Lecture

- IDS
  - Maps to Chapter 8 in Computer Security: Principles and Practices (William Stallings)



CHAPTER 8

INTRUSION DETECTION

8.1 **Intruders**
- Intruder Behavior

8.2 **Intrusion Detection**
- Basic Principles
- The Base-Rate Fallacy
- Requirements

8.3 **Analysis Approaches**
- Anomaly Detection
- Signature or Heuristic Detection

8.4 **Host-Based Intrusion Detection**
- Data Sources and Sensors
- Anomaly HIDS
- Signature or Heuristic HIDS
- Distributed HIDS

8.5 **Network-Based Intrusion Detection**
- Types of Network Sensors
- NIDS Sensor Deployment
- Intrusion Detection Techniques
- Logging of Alerts

8.6 **Distributed or Hybrid Intrusion Detection**

8.7 **Intrusion Detection Exchange Format**

8.8 **Honeypots**

8.9 **Example System: Snort**
- Snort Architecture
- Snort Rules

8.10 **Key Terms, Review Questions, and Problems**

Before Final Exam

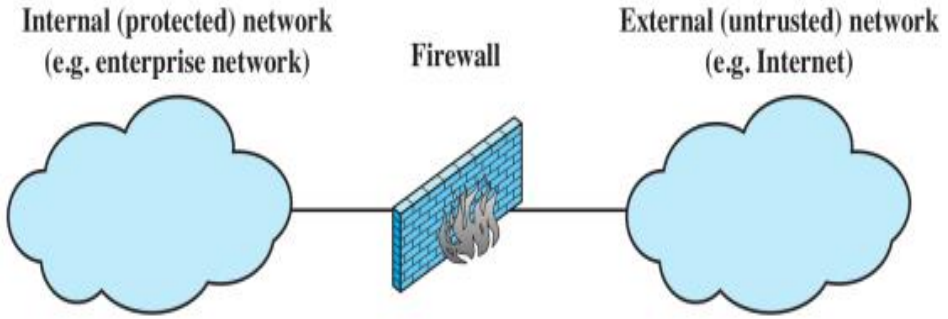
Remaining Lectures (Content)

- ***Network Security (1 lecture left)***
- Theoretical Models of Access Control (1 lecture)
- Cybercrime Laws and Ethics (1 lecture)
- Project Presentations (2 lectures at least)

Firewalls

- Firewalls
- Types of Firewalls
  - Packet-filtering
  - Stateful packet inspection
  - Application proxy
  - Circuit-level proxy
- Location of Firewall

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, and vice versa, *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
- *Behavior 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 (IPsec)*

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

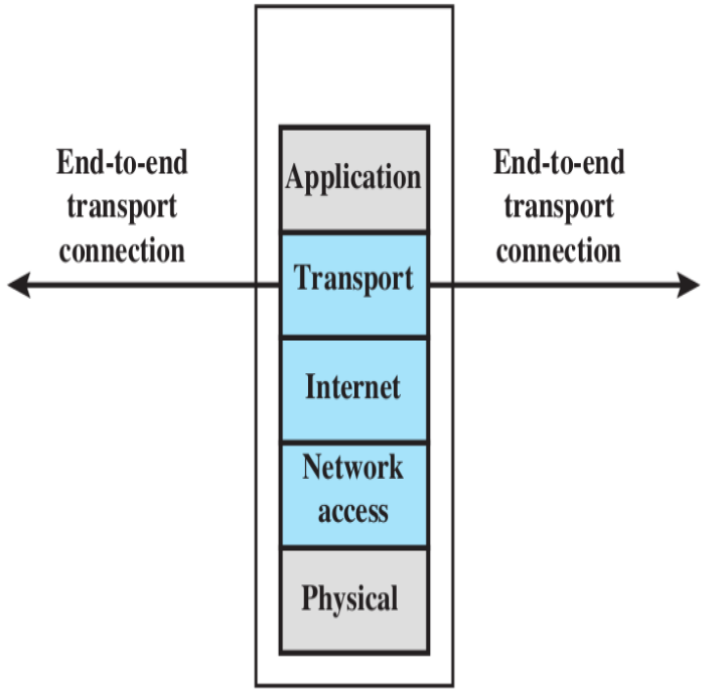
Types of Firewalls

- *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)

Packet Filtering Firewall

- Security policy implemented by *set of rules*
- Rules *define which packets can pass* through the firewall
- Firewalls *inspects 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) - *recommended*



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

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 electron 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

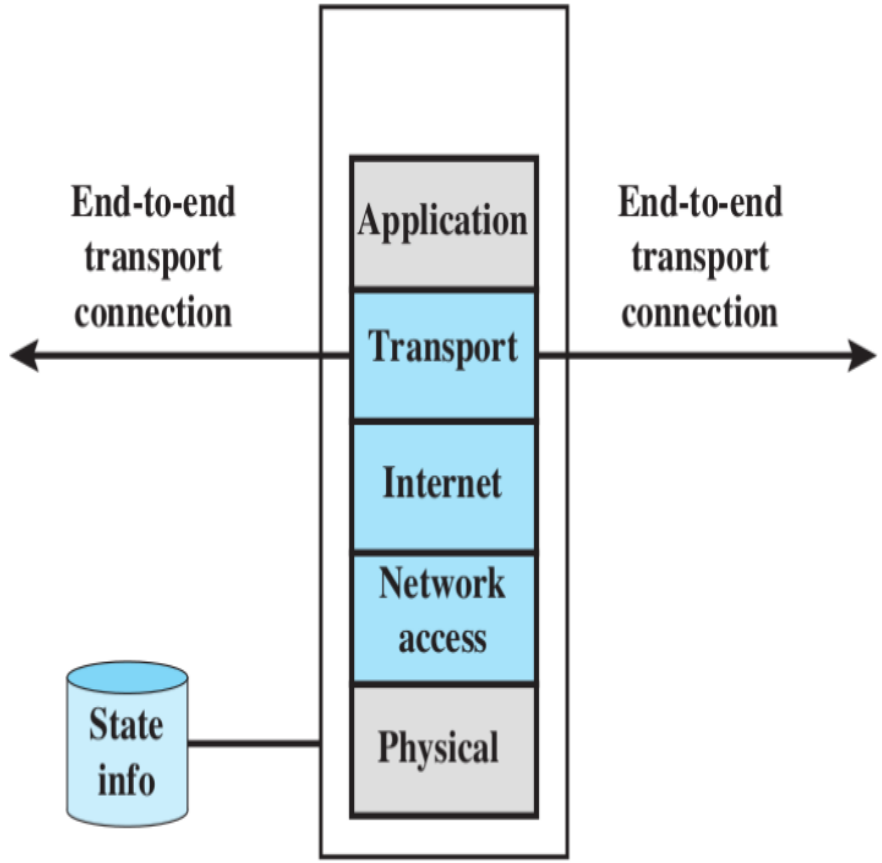
- DNS uses port 53
  - No incoming port 53 packets except known trusted servers

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



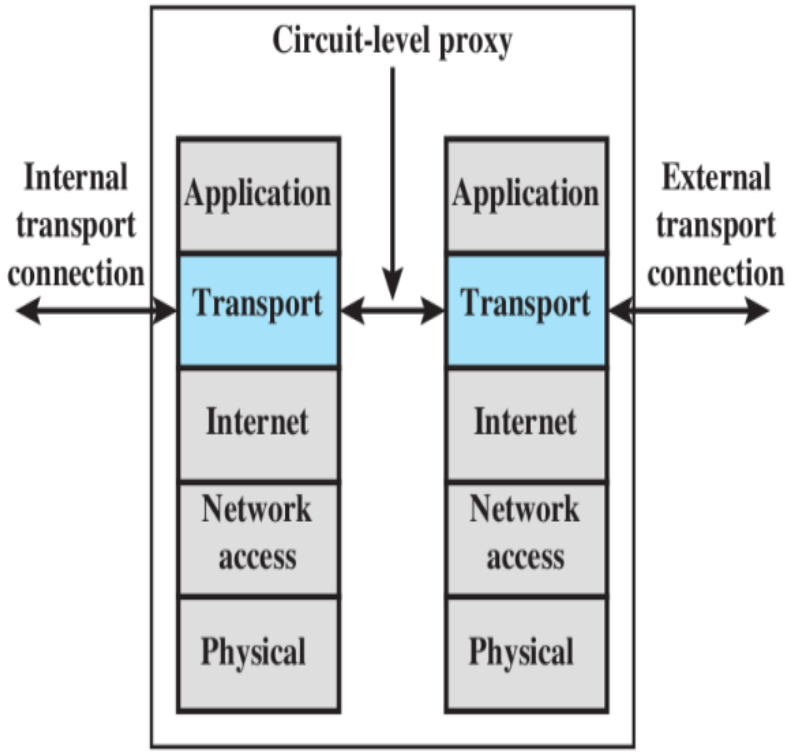
Application Proxy

- 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

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

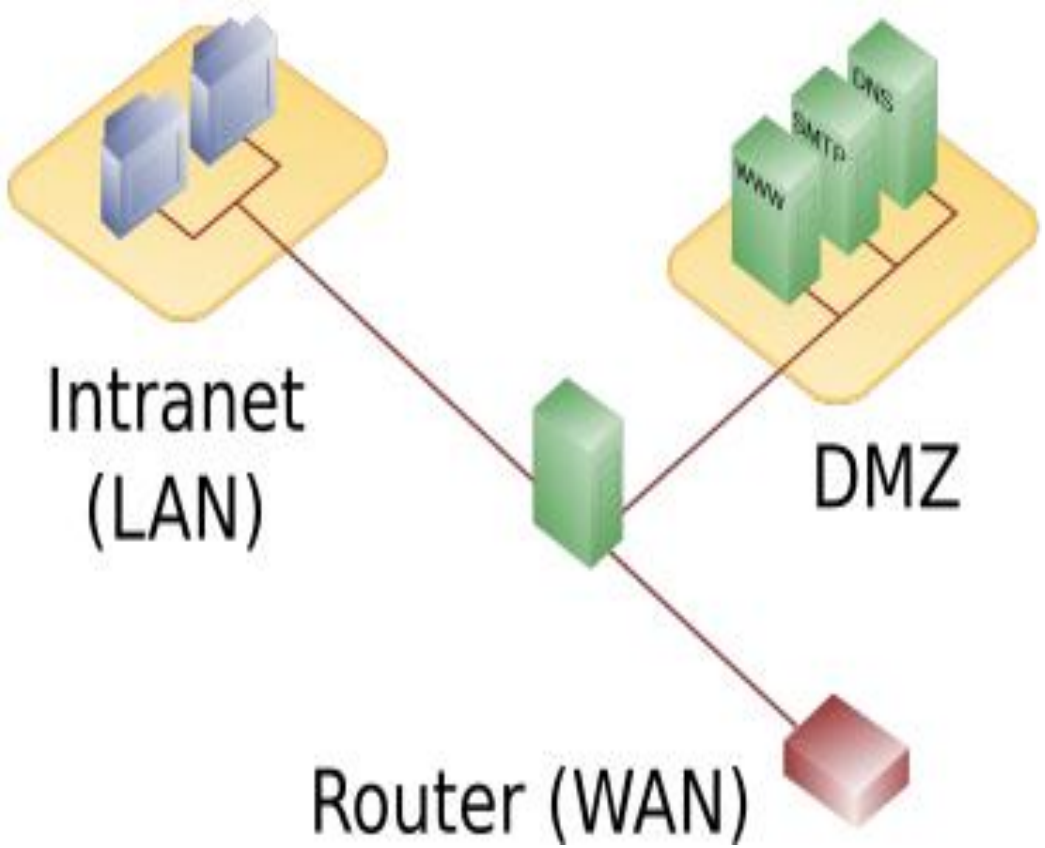


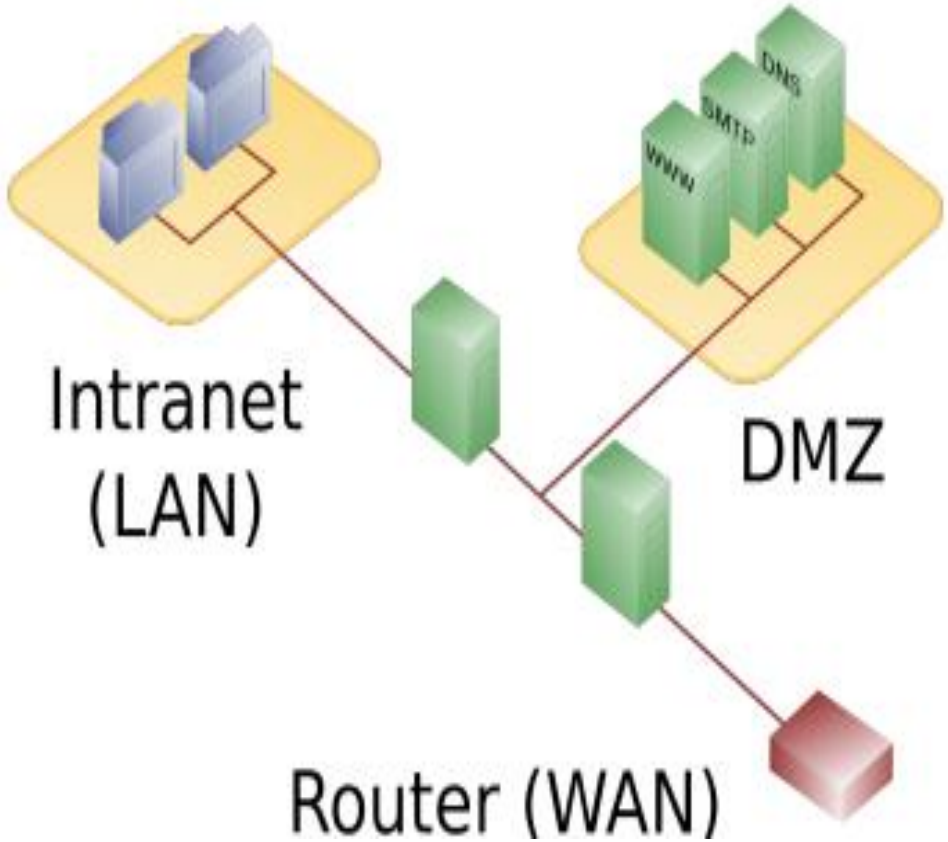
Firewall Locations

- 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

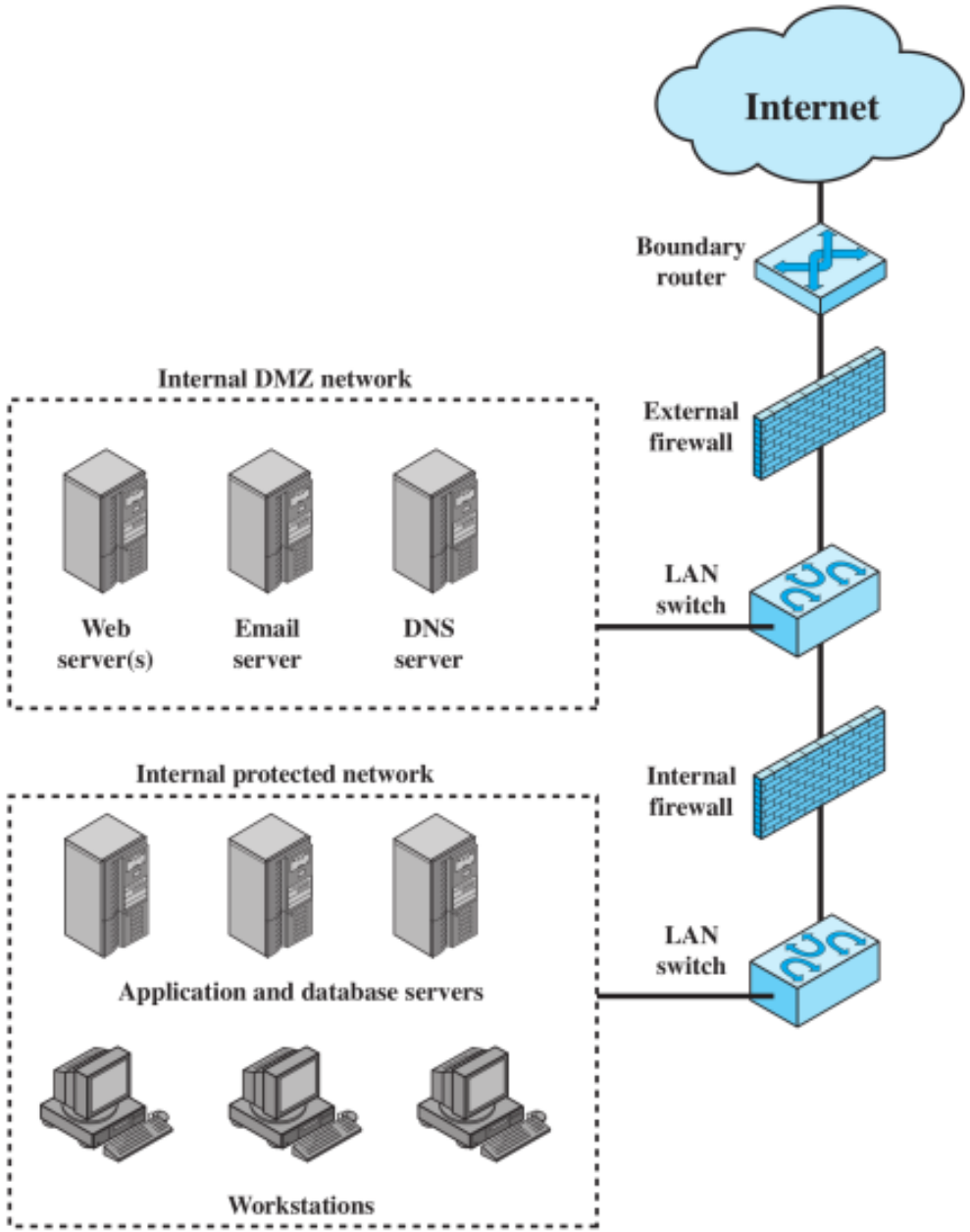
- Common to separate *internal* network into *two zones*:
  - *Public-facing servers*, e.g. web, email, DNS
  - *End-user computers and internal servers*, e.g. databases, development web servers
- Public-facing servers put in *De-Militarized Zone (DMZ)*

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 Chrome 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 an application.
- Examples: Virtual Box, VMware

- Windows Sandbox
  - A temporary instance of host machine

Acknowledgments

- Dr. Haroon Mahmood and other FAST-NU instructors