0790326
Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 13

19th – 21st May 2024

جامعة فيلادلفيا
Philadelphia University

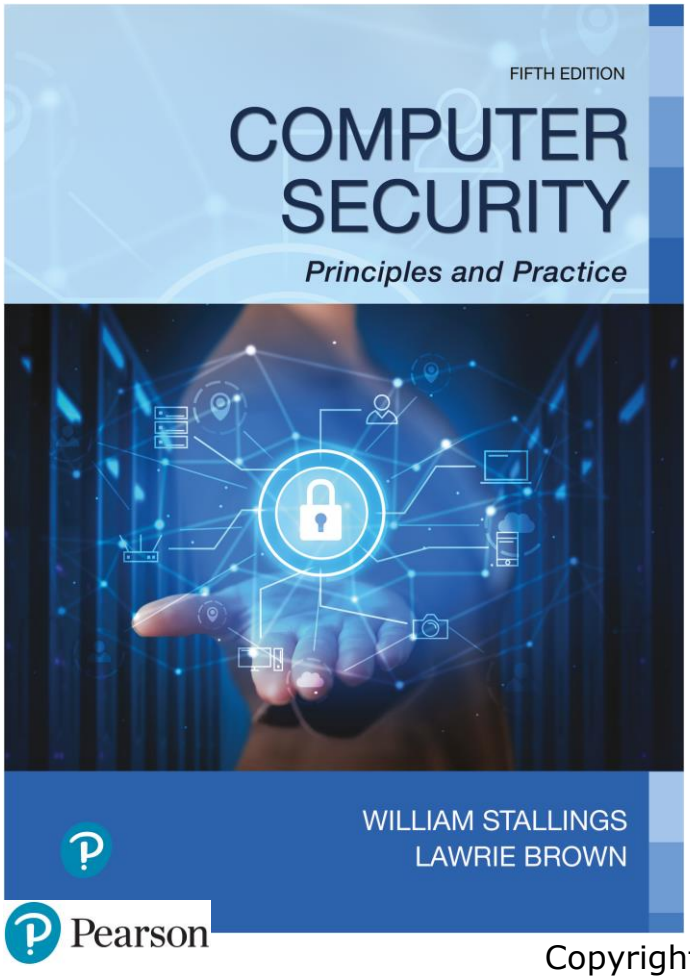
Dr. Basil Elmasri
balmasri@philadelphia.edu.jo

External Material

- Rest of the slides for this week are based on (Stallings & Brown, 2024) book, chapter 8.
  - Some extra slides have been added, their text was taken from the book.
  - Footers, dates, and slides number have been added only to help students reading the material.
- Study and exams will be based on the book chapters, not the slides.

Computer Security: Principles and Practice

Fifth Edition



Chapter 9

Firewalls and Intrusion Prevention Systems

The Need For Firewalls

- Internet connectivity is essential
  - However it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
  - Can be a single computer system or a set of two or more systems working together
- 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

Firewall Access Policy

- A critical component in the planning and implementation of a firewall is specifying a suitable access policy
  - This lists the types of traffic authorized to pass through the firewall
  - Includes address ranges, protocols, applications and content types
- This policy should be developed from the organization's information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
  - Then refined to detail the filter elements which can then be implemented within an appropriate firewall topology

Firewall Filter Characteristics (1 of 2)

- Characteristics that a firewall access policy could use to filter traffic include:
  - IP address and protocol values
    - This type of filtering is used by packet filter and stateful inspection firewalls
    - Typically used to limit access to specific services
  - Application protocol
    - This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols

Firewall Filter Characteristics (2 of 2)

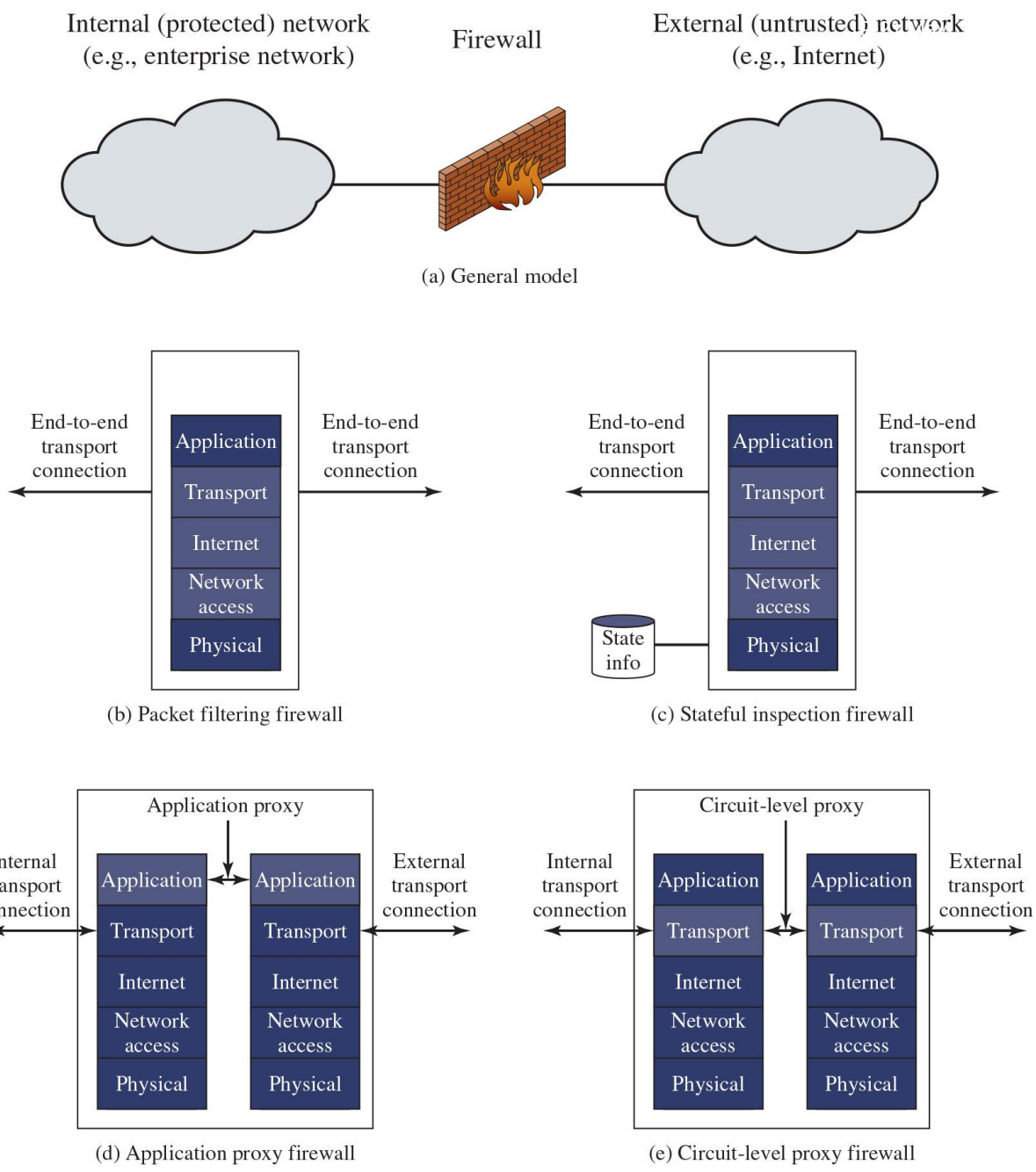
- User identity
  - Typically for inside users who identify themselves using some form of secure authentication technology
- Network activity
  - Controls access based on considerations such as the time of request, rate of requests, or other activity patterns

Firewall Capabilities And Limits

- **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 the platform for IP Sec
- **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, PDA, or portable storage device may be infected outside the corporate network and then used internally\
  - May also block necessary legitimate traffic.

Figure 9.1

Types of Firewalls



Packet Filtering Firewall

- Applies rules to each incoming and outgoing IP packet
  - Typically a list of rules based on matches in the IP or TCP header
  - Forwards or discards the packet based on rules match
- Filtering rules are based on information contained in a network packet
  - Source IP address
  - Destination IP address
  - Source and destination transport-level address
  - IP protocol field
  - Interface
- Two default policies:
  - Discard - prohibit unless expressly permitted
    - More conservative, controlled, visible to users
  - Forward - permit unless expressly prohibited
    - Easier to manage and use but less secure

Table 9.1

Packet-Filtering Examples

Rule	Direction	Src address	Dest address	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 Filter Advantages And Weaknesses

- Advantages
  - Simplicity
  - Typically transparent to users and are very fast
- Weaknesses
  - Cannot prevent attacks that employ application specific vulnerabilities or functions
  - Limited logging functionality
  - Do not support advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configuration can lead to breaches

Stateful Inspection Firewall

- Tightens rules for TCP traffic by creating a directory of outbound TCP connections
  - There is an entry for each currently established connection
  - Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory
- Reviews packet information but also records information about TCP connections
  - Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
  - Inspects data for protocols like FTP, IM and SIPS commands

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

Application-Level Gateway

- Also called an application proxy
- Acts as a relay of application-level traffic
  - User contacts gateway using a TCP/IP application
  - User is authenticated
  - Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application
  - May restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection

Circuit-Level Gateway

- **Circuit level proxy**
  - Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
  - 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**
  - May use application-level gateway inbound and circuit-level gateway outbound
  - Lower overheads

SOCKS Circuit-Level Gateway

- SOCKS v5 defined in RFC1928
  - Sometimes defined as an acronym for "socket secure"
- Designed to provide a framework for client-server applications in TCP/UDP domains to conveniently and securely use the services of a network firewall
- Client application contacts SOCKS server, authenticates, sends relay request
  - Server evaluates and either establishes or denies the connection

Components

- SOCKS server
- SOCKS client library
- SOCKS-ified client applications

Bastion Hosts

- System identified as a critical strong point in the network's security
- Serves as a platform for application-level or circuit-level gateways
- Common characteristics:
  - Runs secure O/S, only essential services
  - May require user authentication to access proxy or host
  - Each proxy can restrict features, hosts accessed
  - Each proxy is small, simple, checked for security
  - Each proxy is independent, non-privileged
  - Limited disk use, hence read-only code

References

Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice (5 ed.). Pearson. Retrieved from https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000010333/9780138091712