

0790326 Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 14

26th – 28th 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.



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

Host-Based Firewalls

- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- Common location is a server
- Advantages:
 - Filtering rules can be tailored to the host environment
 - Protection is provided independent of topology
 - Provides an additional layer of protection

Personal Firewall

- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- For both home or corporate use
- Typically is a software module on a personal computer
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity

Figure 9.2

Example Firewall Configuration

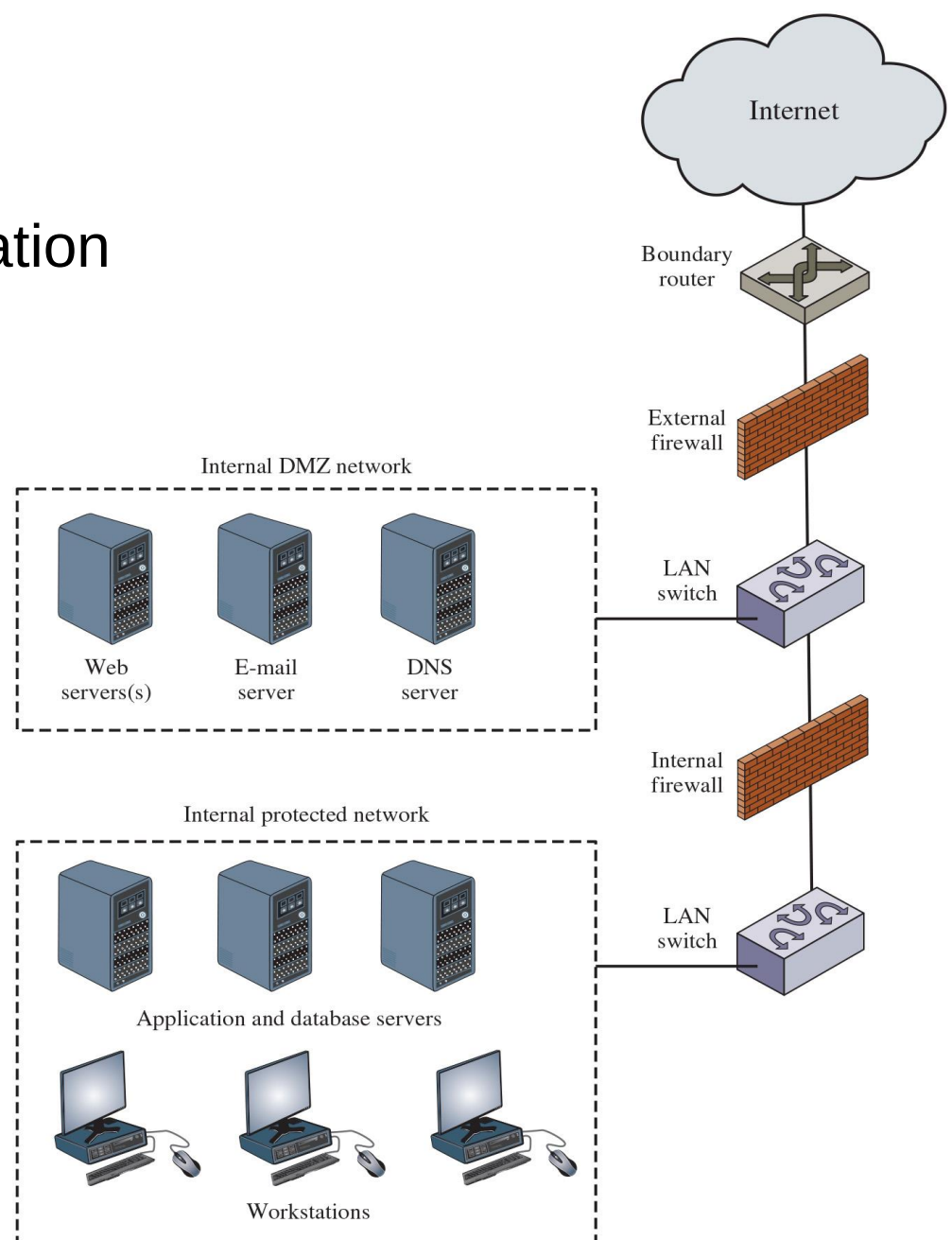
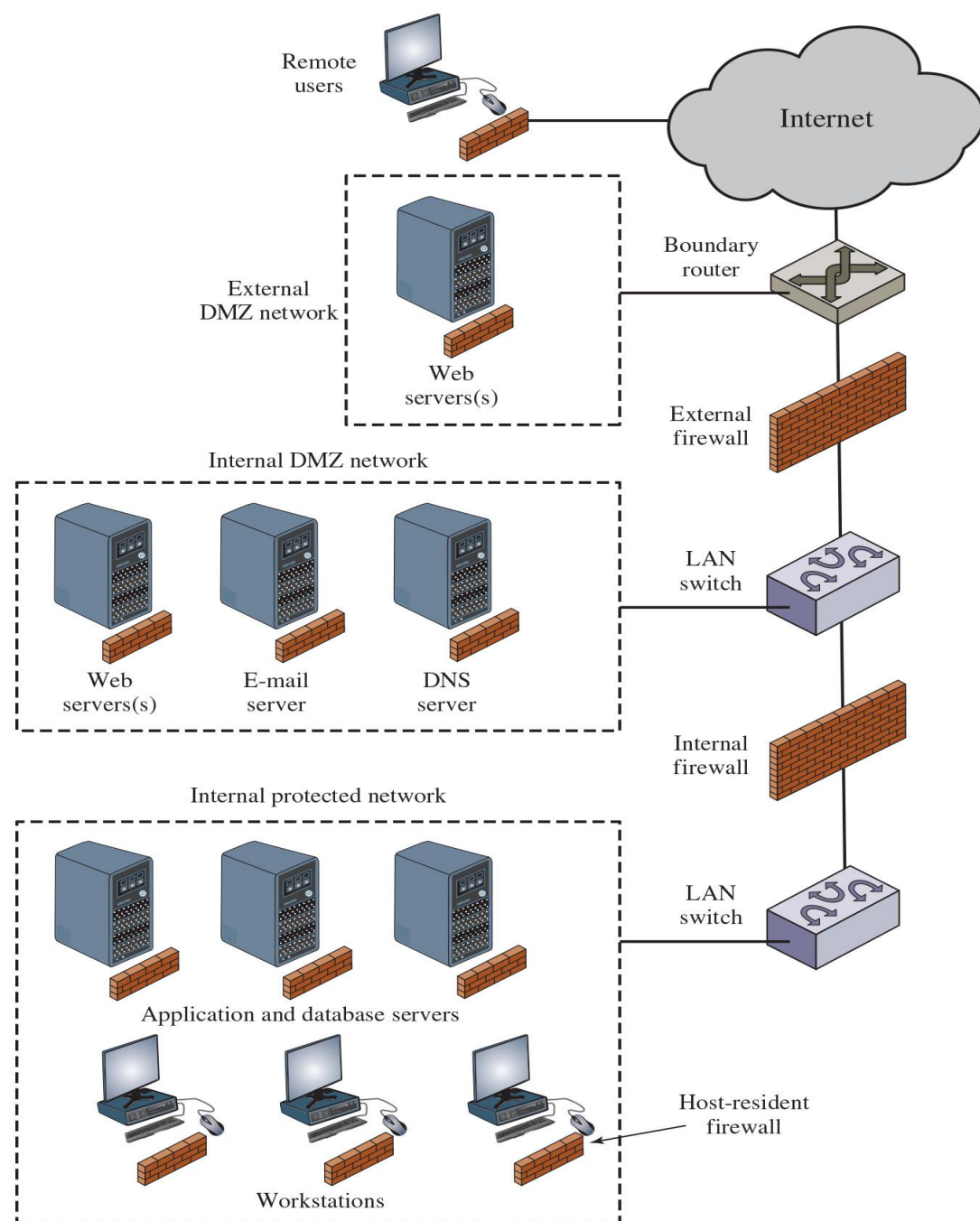


Figure 9.4

Example Distributed Firewall Configuration



Firewall Topologies (1 of 2)

- **Host-resident firewall**
 - Includes personal firewall software and firewall software on servers
- **Screening router**
 - Single router between internal and external networks with stateless or full packet filtering
- **Single bastion inline**
 - Single firewall device between an internal and external router
- **Single bastion T**
 - Has a third network interface on bastion to a DMZ where externally visible servers are place

Firewall Topologies (2 of 2)

- **Double bastion inline**
 - DMZ is sandwiched between bastion firewalls
- **Double bastion T**
 - DMZ is on a separate network interface on the bastion firewall
- **Distributed firewall configuration**
 - Used by large businesses and government organizations

Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users or signature/heuristic detection to identify known malicious behavior
- Can block traffic but makes use of the types of algorithms developed for IDSs to determine when to do so

Host-Based IPS (HIPS)

- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks
 - Signature: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
 - Anomaly: IPS is looking for behavior patterns that indicate malware
- Examples of the types of malicious behavior addressed by a HIPS include:
 - Modification of system resources
 - Privilege-escalation exploits
 - Buffer-overflow exploits
 - Access to e-mail contact list
 - Directory traversal

HIPS (1 of 2)

- Capability can be tailored to the specific platform
- A set of general purpose tools may be used for a desktop or server system
- Some packages are designed to protect specific types of servers, such as Web servers and database servers
 - In this case the HIPS looks for particular application attacks

HIPS (2 of 2)

- Can use a sandbox approach
 - Sandboxes are especially suited to mobile code such as Java applets and scripting languages
 - HIPS quarantines such code in an isolated system area then runs the code and monitors its behavior
- Areas for which a HIPS typically offers desktop protection:
 - System calls
 - File system access
 - System registry settings
 - Host input/output

The Role of HIPS (1 of 2)

- Many industry observers now see the enterprise endpoint, including desktop and laptop systems, as the main target for hackers and criminals
 - Thus security vendors are focusing more on developing endpoint security products
 - Traditionally, endpoint security has been provided by a collection of distinct products, such as antivirus, antispyware, antispam, and personal firewalls

The Role of HIPS (2 of 2)

- Approach is an effort to provide an integrated, single-product suite of functions
 - Advantages of the integrated HIPS approach are that the various tools work closely together, threat prevention is more comprehensive, and management is easier
- A prudent approach is to use HIPS as one element in a defense-in-depth strategy that involves network-level devices, such as either firewalls or network-based IPS

Network-Based IPS (NIPS)

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections
- Makes use of signature/heuristic detection and anomaly detection
- May provide flow data protection
 - Requires that the application payload in a sequence of packets be reassembled
- Methods used to identify malicious packets:
 - Pattern matching
 - Stateful matching
 - Protocol anomaly
 - Traffic anomaly
 - Statistical anomaly

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>