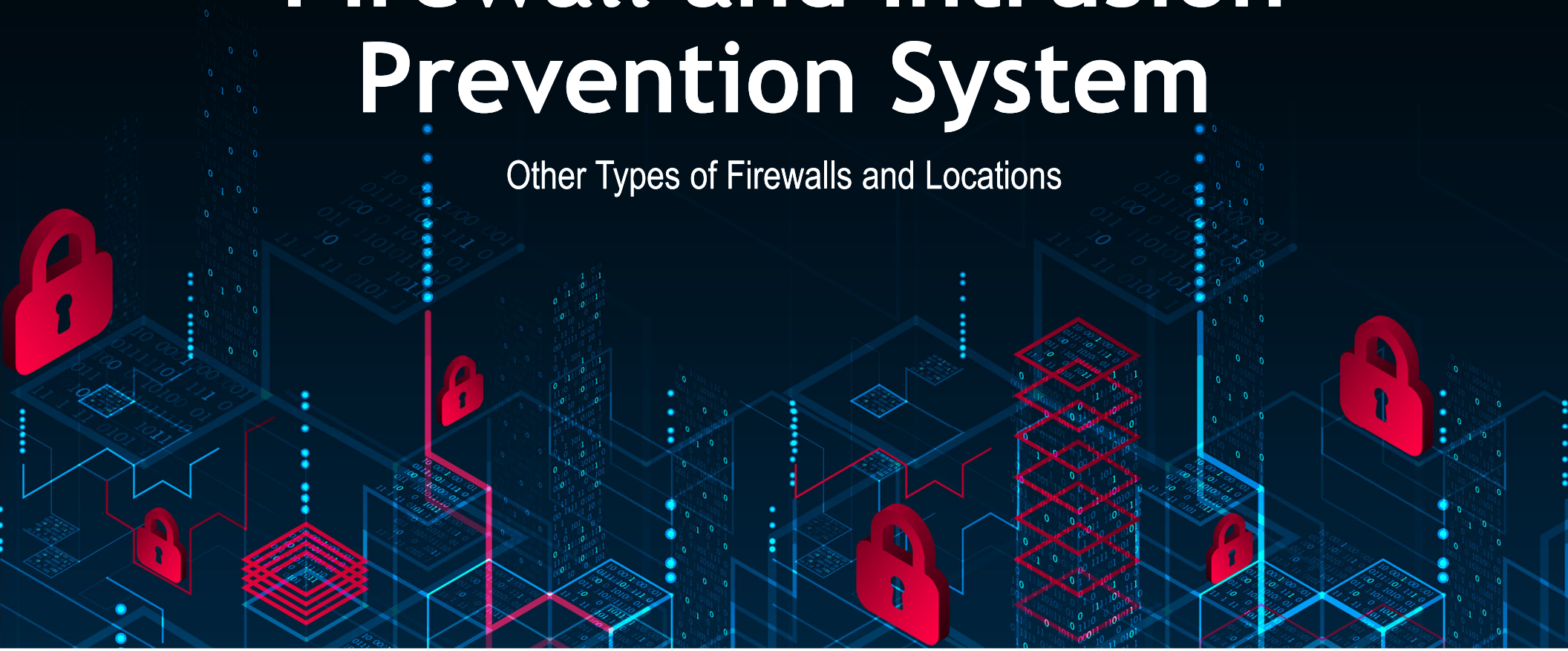
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Firewall and Intrusion Prevention System

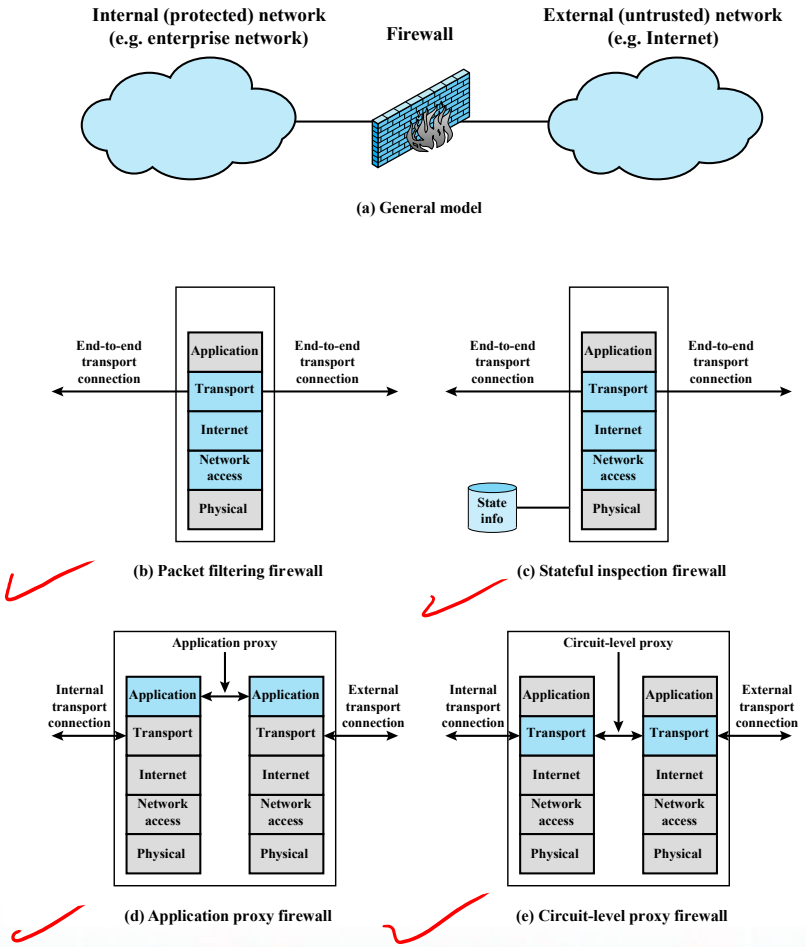
Other Types of Firewalls and Locations



Video Summary

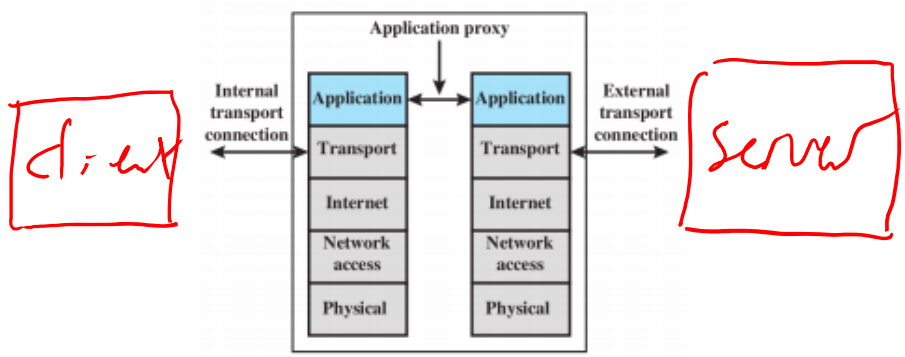
- Application-level Gateway
- Circuit-level Gateway
- Host-based Firewall
- Personal Firewall
- Firewall Location

Types of Firewall



App-level Gateway.

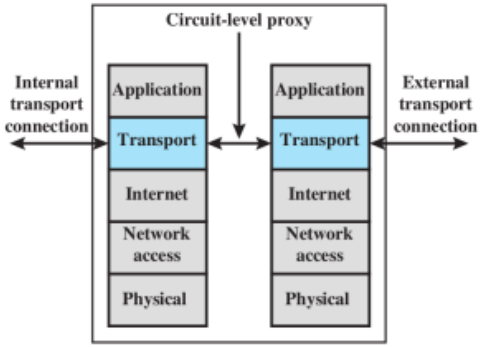
Application-Level Gateway

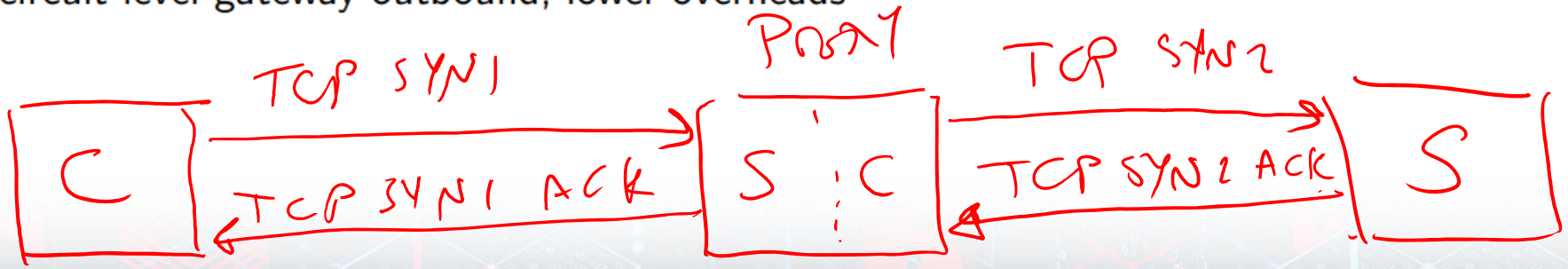


- Also called an application proxy
- Acts as a relay of application-level traffic
  - ✓ User contacts gateway using a TCP/IP application
  - ✓ User is authenticated
  - ✓ Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application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

Circuit-level 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
- 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





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 (doesn't understand http)
- 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

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

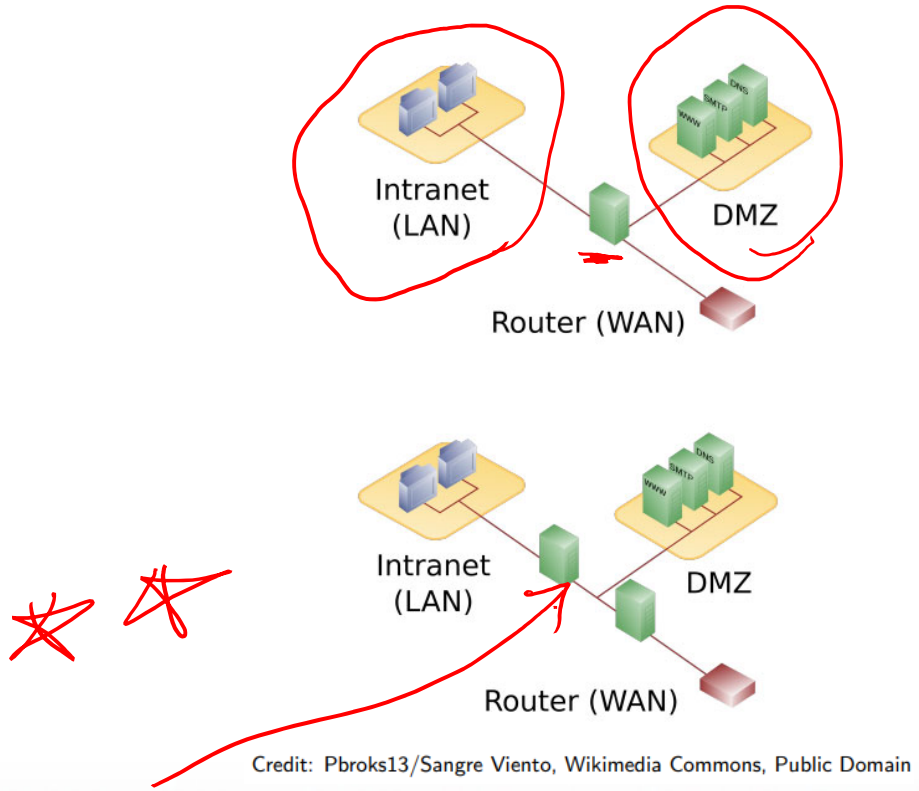
Personal Firewall

- 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

Firewall Location

- 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 one or two Firewalls



Credit: Pbroks13/Sangre Viento, Wikimedia Commons, Public Domain

DMZ with two Firewalls

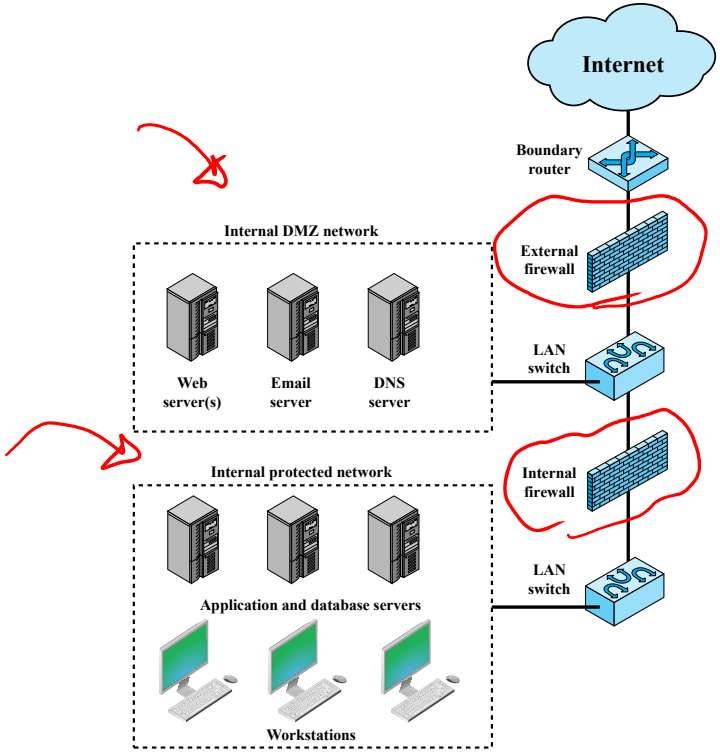


Figure 9.2 Example Firewall Configuration

Video Summary

- Application-level Gateway
- Circuit-level Gateway
- Host-based Firewall
- Personal Firewall
- Firewall Location