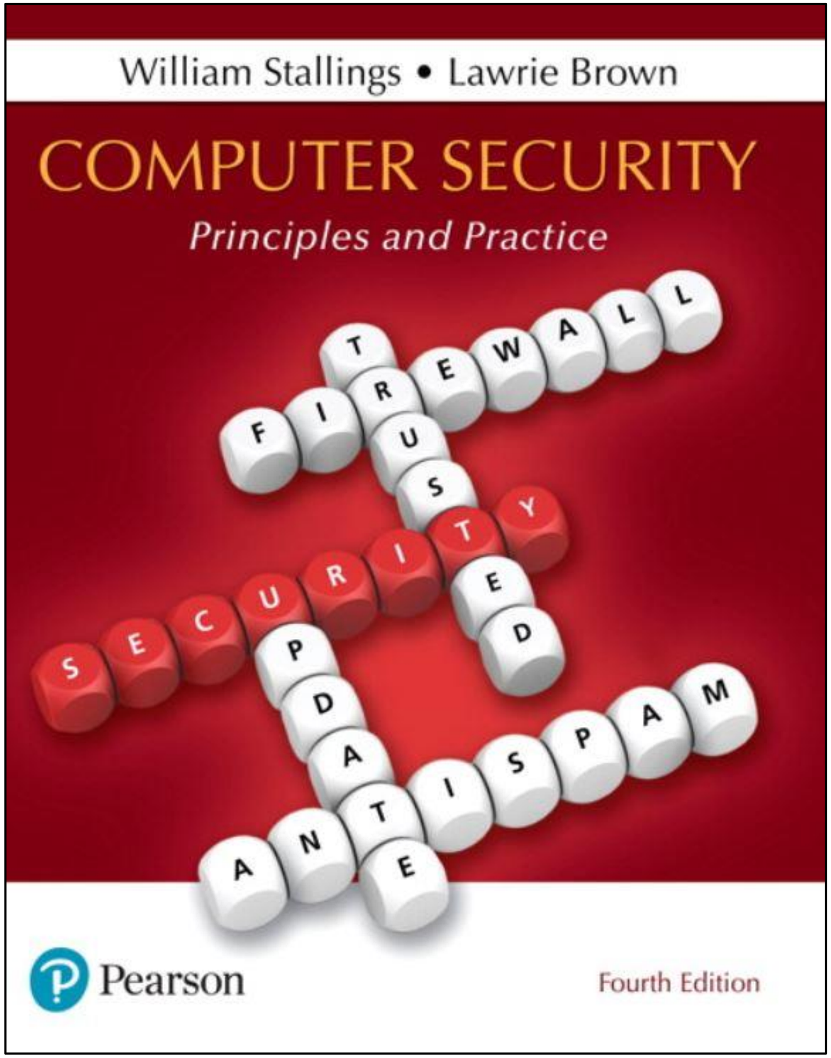
Computer Security: Principles and Practice

Fourth Edition



Chapter 9

Firewalls and Intrusion Prevention Systems

The Need For Firewalls

Choke
خانق

- 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 Force
  - Single choke point to impose security and auditing
  - Insulates the internal systems from external networks

عزل

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 تفتيش
    - 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

Pearson

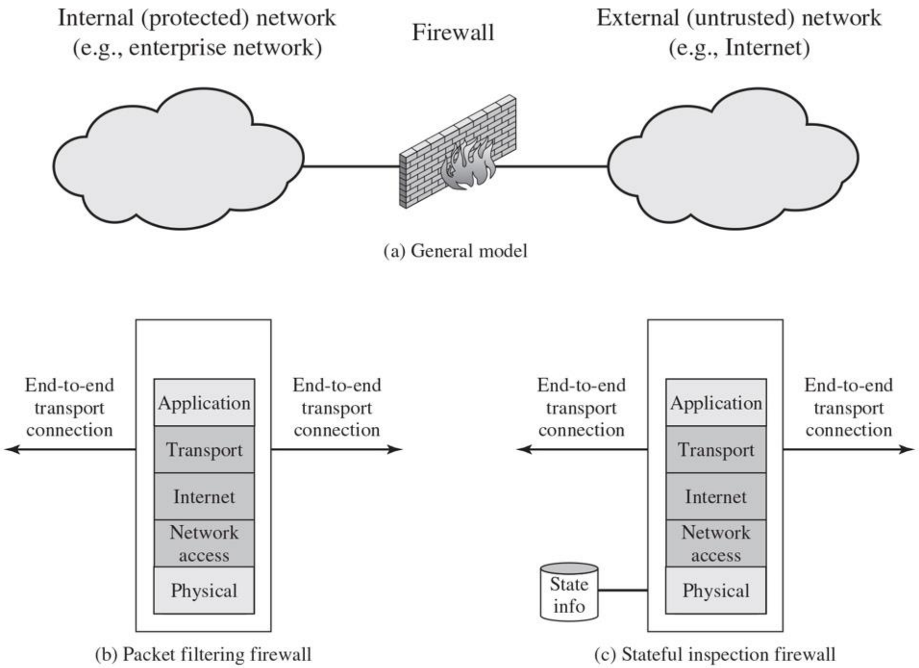
Firewall Filter Characteristics (2 of 2)

- 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 or 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 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, PDA, or portable storage device may be infected outside the corporate network then used internally

Figure 9.1 Types of Firewalls


Internal (protected) network
(e.g., enterprise network)
Firewall
External (untrusted) network
(e.g., Internet)
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info

(a) General model

(b) Packet filtering firewall

(c) Stateful inspection firewall

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 addresss	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

Pearson

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

عمل خطأ violates

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

[illegible] اعرف

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

desigend

- Advantages:
  - Filtering rules can be tailored to the host environment
  - Protection is provided independent of topology
  - Provides an additional layer of protectiona

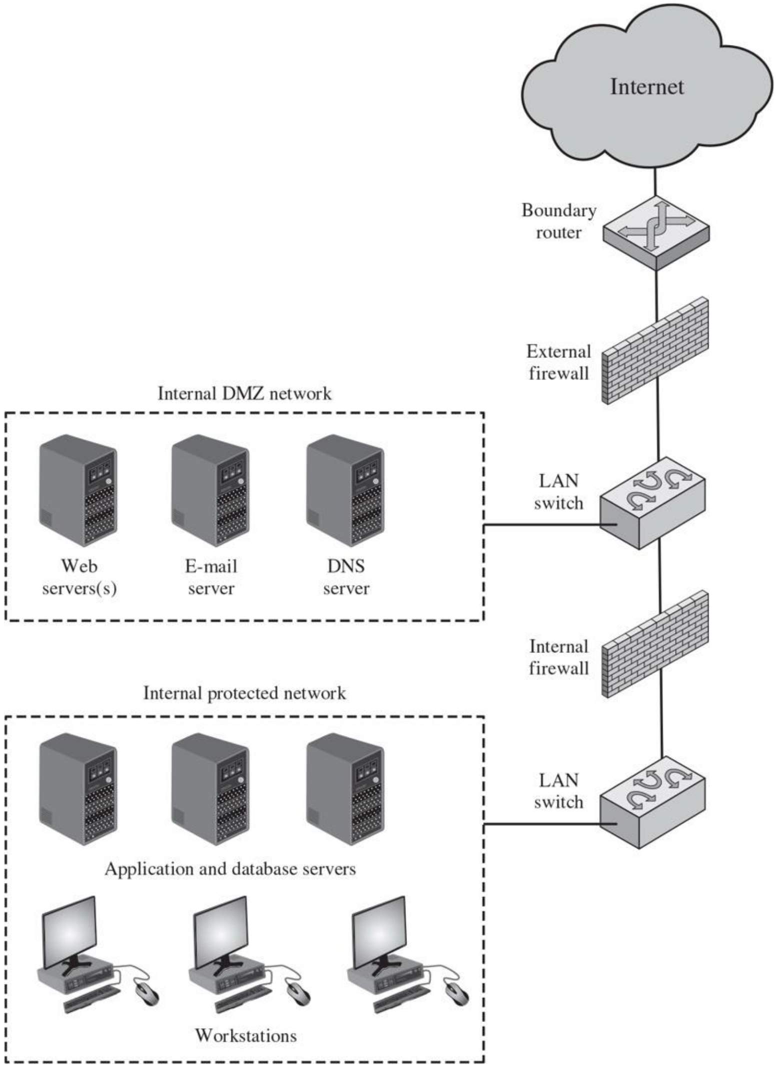
جهازك

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

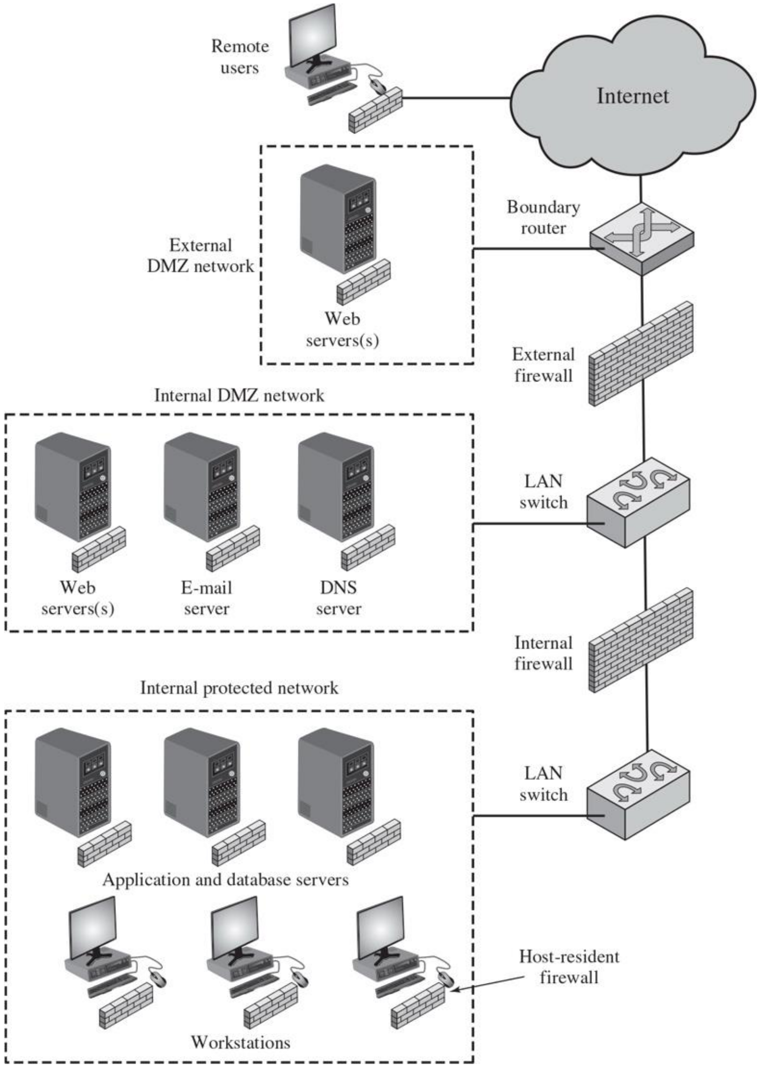
Pearson

Figure 9.2 Example Firewall Configuration



Pearson

Figure 9.4 Example Distributed Firewall Configuration



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 as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Pearson

Copyright