COURSE TECHNOLOGY
CENGAGE Learning™

Guide to Network Security
First Edition

Chapter Four
Firewall Technologies and Administration

Objectives

- Describe what a firewall does
- Explain how a firewall restricts access to a network
- List the types of firewall protection as well as the types of firewall implementations and the ways they are used
- Describe how firewall rules are created and how they are used to control the behavior of the firewall
- Explain how intrusion detection and prevention systems are related and how they may be made to interact with one another

Introduction

- Firewall
  - Combination of hardware and software components
- Firewall security tasks
  - Restrict traffic between networks
  - Provide a checkpoint
  - Record network activity

Firewall Overview

- Firewall functions
  - Enable authorized traffic to pass through
  - Block unauthorized traffic
- Firewalls filter packets of digital information as they attempt to pass through network boundary

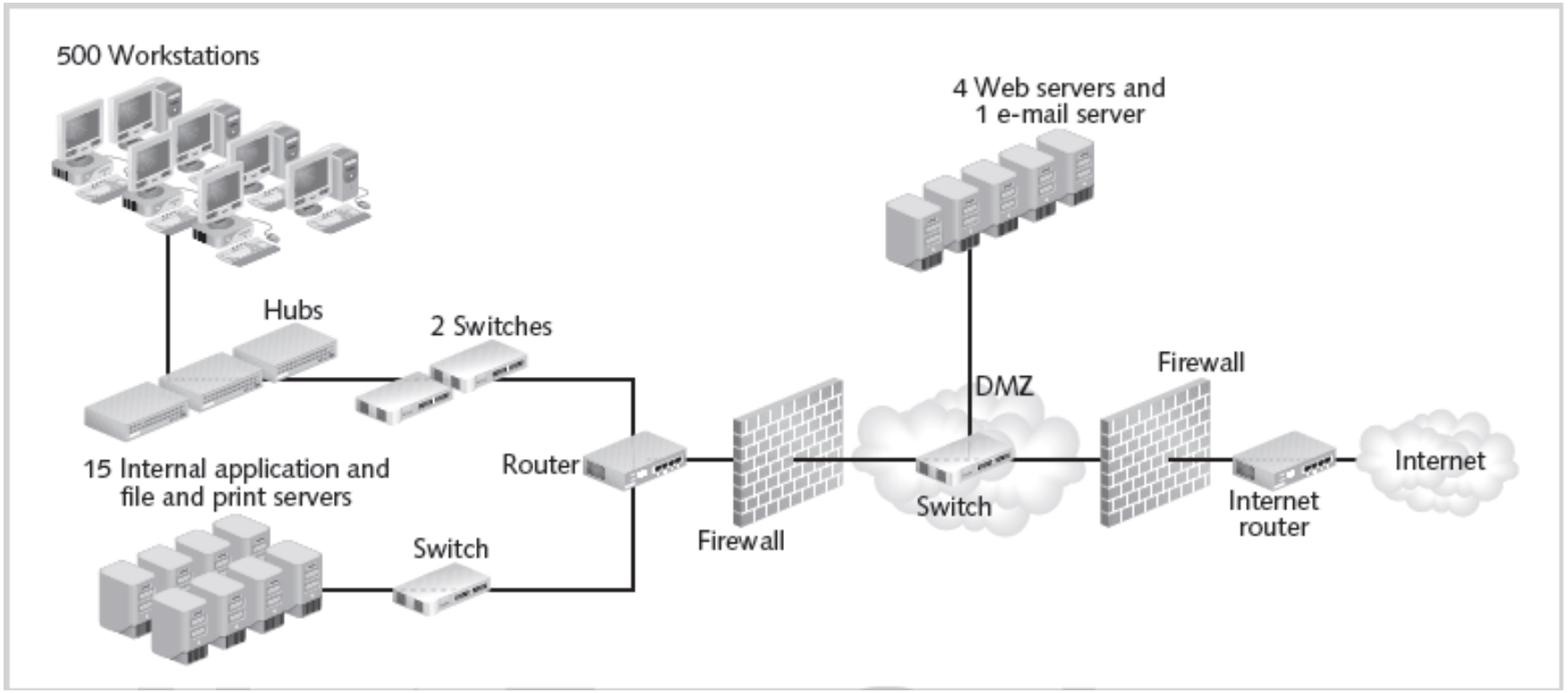

Figure 4-1 General firewall architecture

© Cengage Learning 2013

Firewall Overview (cont'd.)

- Firewall advanced features
  - Scanning for viruses
  - Repairing infected files
  - Sending alert messages
  - Providing a VPN link
  - Authenticating users
  - Shielding hosts inside the network
  - Caching data
  - Filtering content

Firewall Uses

- Major firewall applications
  - Protects a system
    - Prevent viruses and Trojan horses from entering a system
    - Alert user when attachment containing a virus is found
  - Restricts access to the network
    - Perimeter: boundary between two zones of trust
    - Common to install a firewall at the perimeter

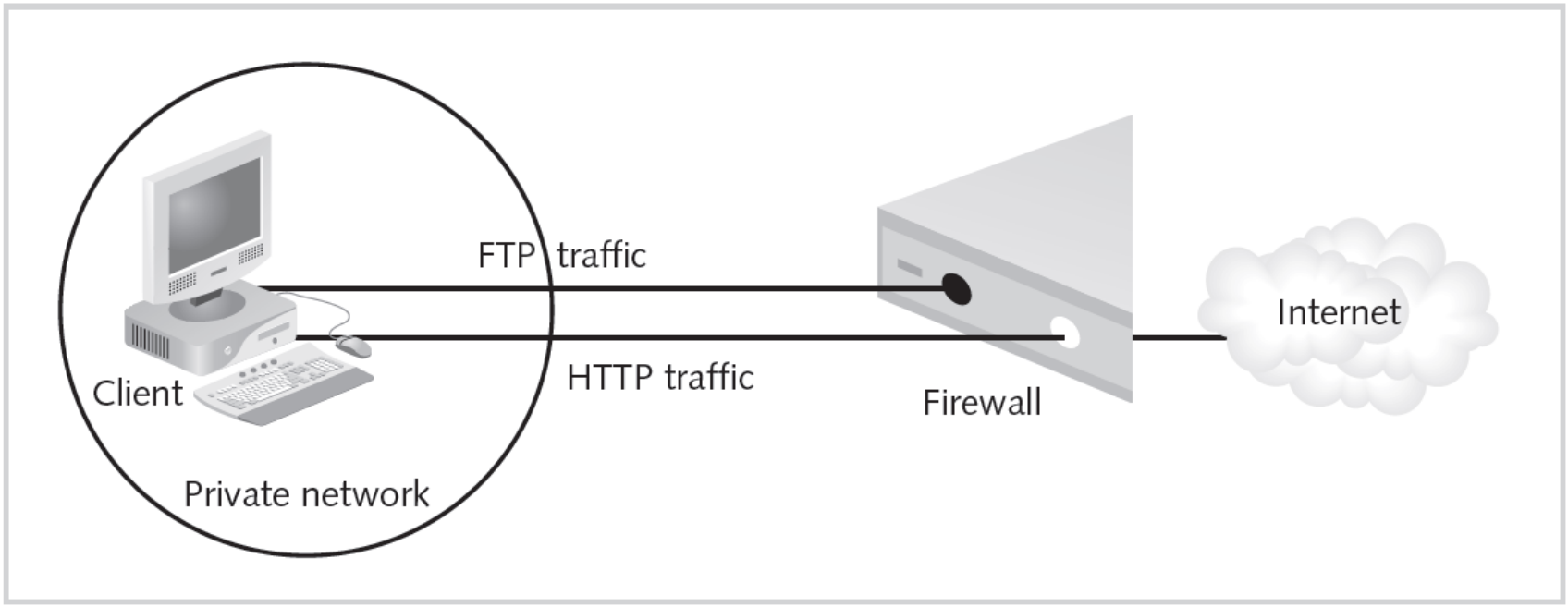

Figure 4-2 Firewall at the perimeter
© *Cengage Learning 2013*

Firewall Uses (cont'd.)

- Major firewall applications (cont'd.)
  - Extends the network
    - Extranet: extended network sharing part of an organization's network with a third party
    - Firewall an ideal endpoint for virtual private network
    - Most secure configuration shown in Figure 4-3

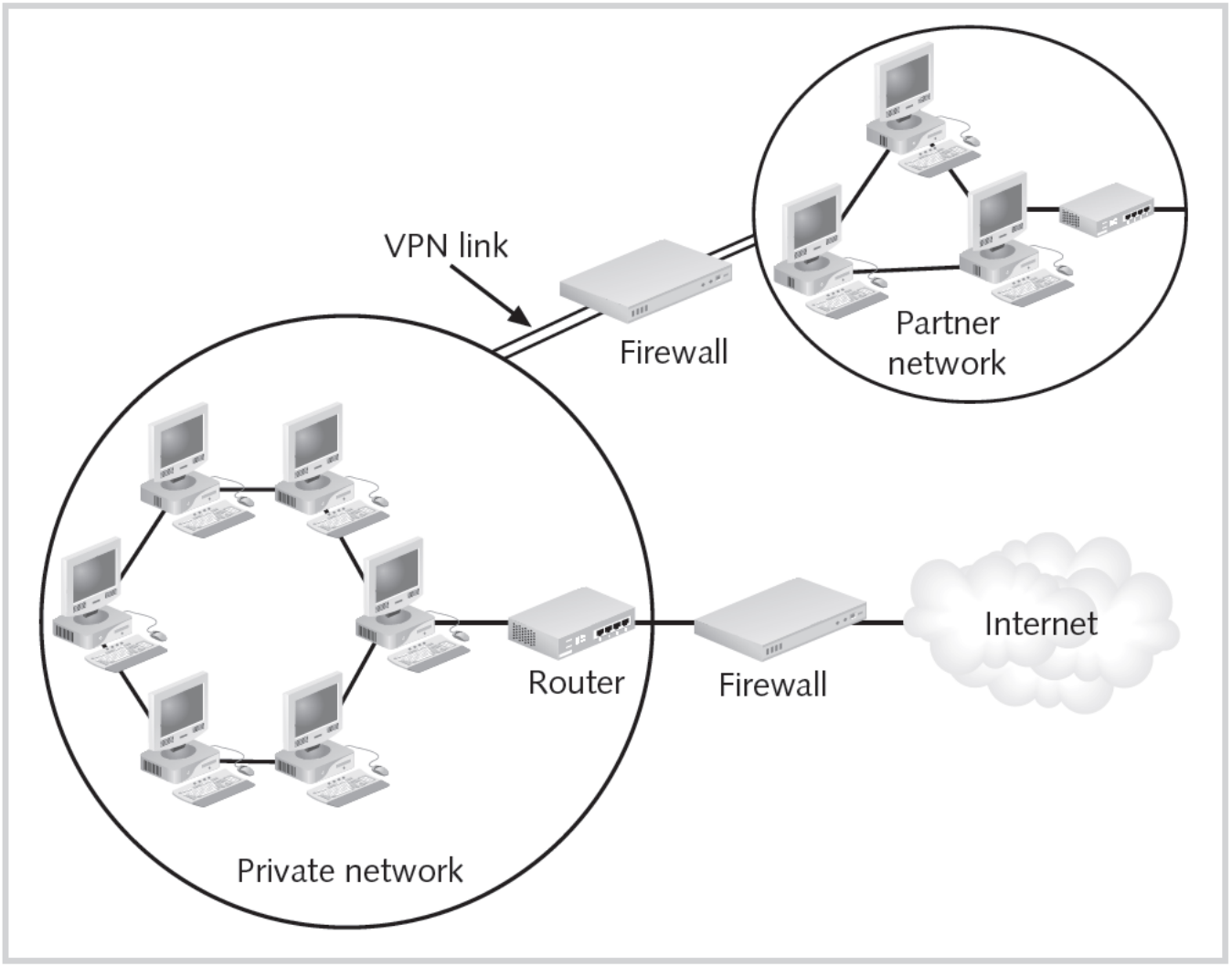

Figure 4-3 VPN perimeters
© *Cengage Learning 2013*

Firewall Uses (cont'd.)

- Major firewall applications (cont'd.)
  - Prevents malicious traffic from leaving the network
    - Users could visit malicious Web site and install malware
    - Malware can attack other organizations from inside network
  - Provides more precise control for employees using external resources

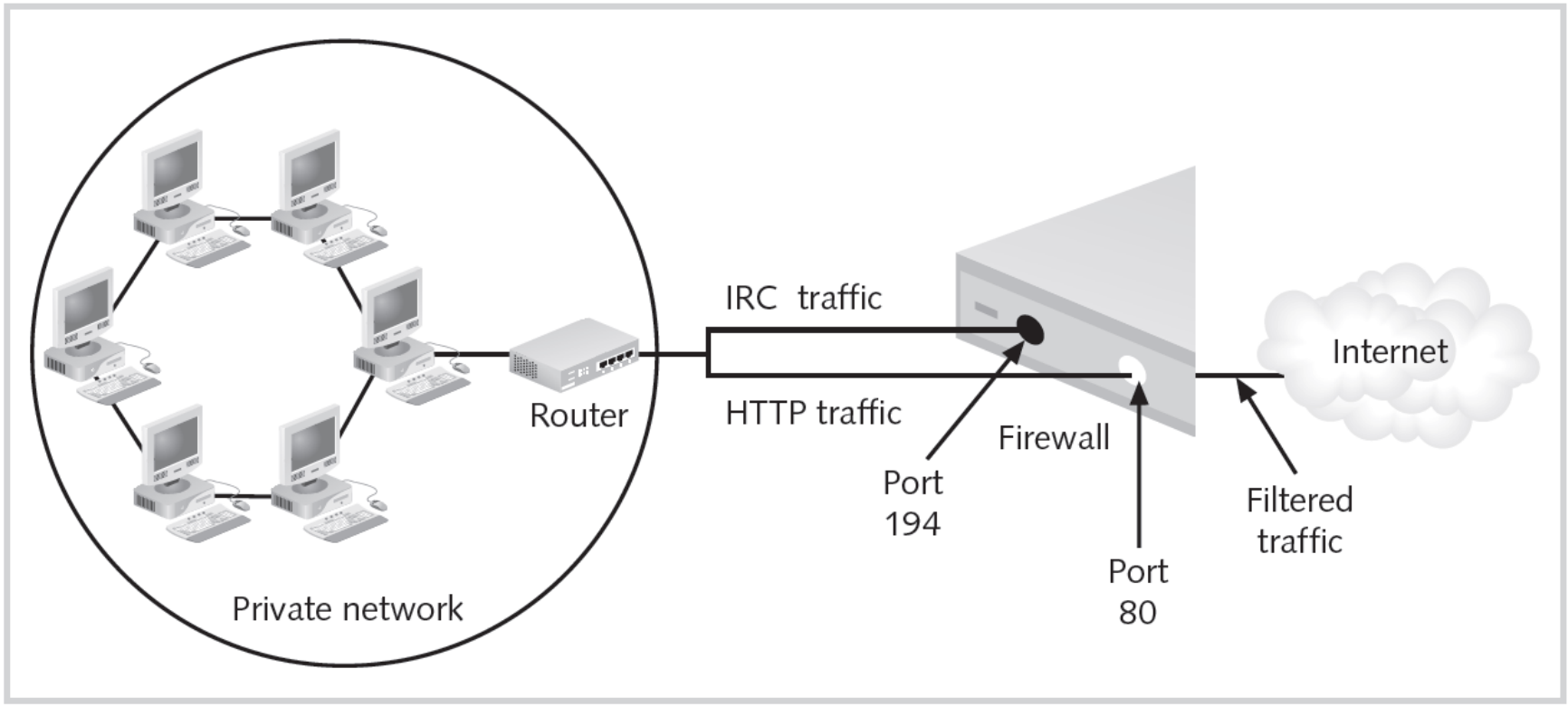

Figure 4-4 Outbound packet filtering

Firewall Uses (cont'd.)

- Major firewall applications (cont'd.)
  - Protects critical resources
    - Firewalls segment networks within an organization
    - Different types of servers separated by firewalls
  - Enables an audit trail
    - Log files record attempted intrusions
    - Review log files regularly
  - Provides authentication
    - Authentication process can be performed at the firewall
    - Protect credentials using encryption

How do Firewalls Work?

- Firewalls perform two basic security functions
  - Packet filter
  - Application proxy

Layer Number	OSI Reference Model Layer	Firewall Functions
7	Application	Application-level gateway
6	Presentation	Encryption
5	Session	SOCKS proxy server
4	Transport	Packet filtering (based on port)
3	Network	NAT and packet filtering (based on address alone)
2	Data Link	MAC address-filtering
1	Physical	N/A

Table 4-1 Network layers and firewalls
© Cengage Learning 2013

Protocols

- Internet Protocol (IP)
  - Rules control overall flow of IP traffic through a network
- Internet Control Message Protocol (ICMP)
  - Used to report transmission errors
- User Datagram Protocol (UDP)
  - Handles message addressing
- Transmission Control Protocol (TCP)
  - Provides connections for error checking
  - Enables assurance of transmission success

Ports

- Network subaddress
- Number between zero and 65,535
- Well-known ports (1023 and below)
  - Used for common services
- Ephemeral ports (1024 through 65,535)
  - Dynamically assigned as needed
  - No special meaning outside the connection using them

Packet-Filtering Firewalls

- Packet filtering: key function of any firewall
- Types of information in the frame and the packet
  - Header
  - Data
  - Trailer (footer)
- Packet-filtering firewall functions at the IP level
  - Determines whether to reject, drop, or allow a packet
  - Uses set of rules programmed into the firewall

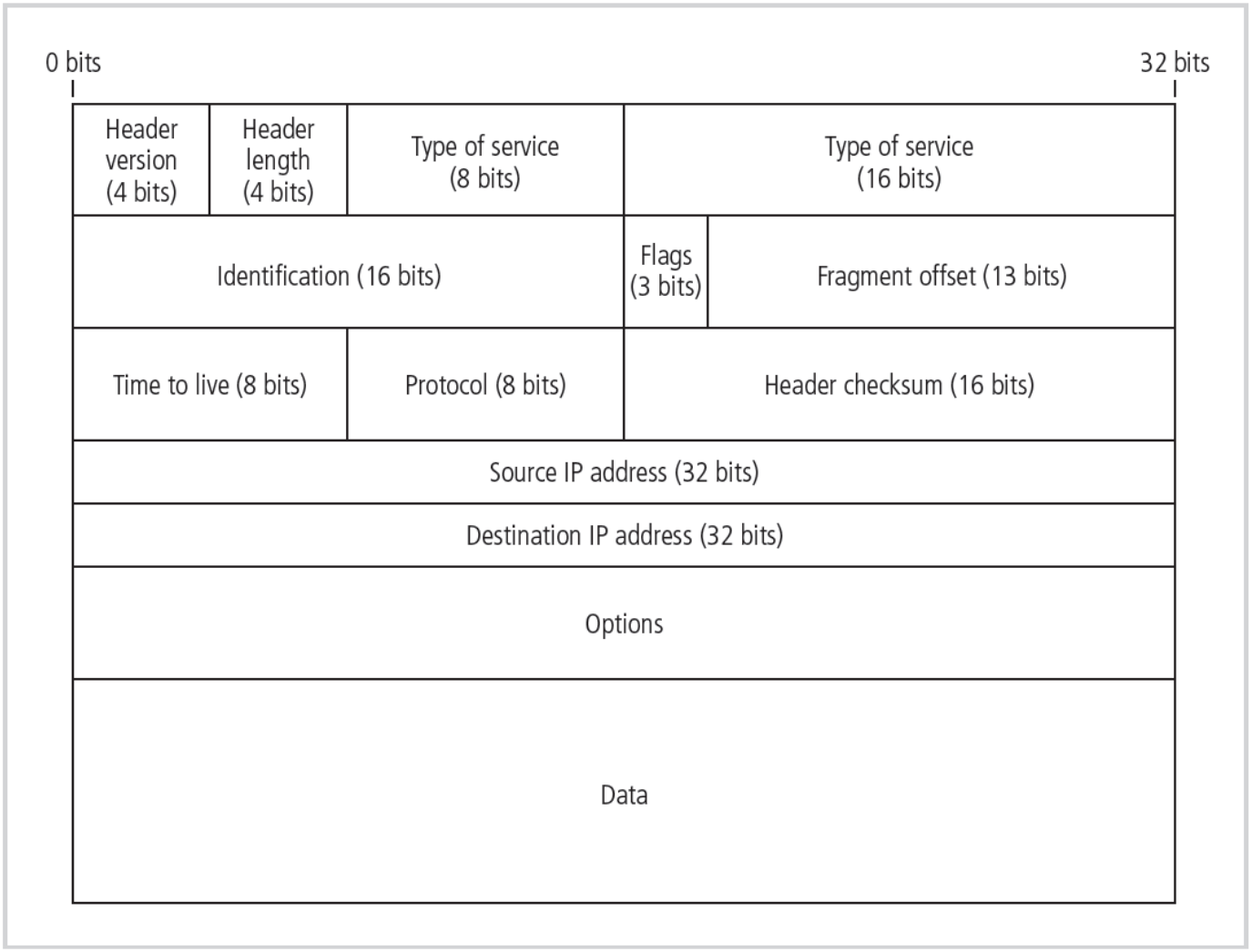

Figure 4-5 IPv4 packet structure

© Cengage Learning 2013

Packet-Filtering Firewalls (cont'd.)

- Packet-filtering rules
  - Simple models examine destination and source address
    - Enforce address restrictions as defined in ACLs
  - Rule specifies protocol, address or range, and desired firewall action
  - Rules are executed in order
    - Later rules can override a previous rule
  - Best practice: start with rule to drop all incoming traffic

Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet, etc.)	Action (Allow or Deny)
Any	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.x.x	10.10.10.10	FTP	Allow

Table 4-2 Sample firewall rule and format

Packet-Filtering Firewalls (cont'd.)

- Packet-filtering best practices
  - Outbound source address must be in internal network
  - Outbound destination address must not be in internal network
  - Inbound packet source address not in internal network
  - Inbound packet destination address in internal network
  - Other best practices on Pages 144-145 of the text

Packet-Filtering Firewalls (cont'd.)

- Stateless packet-filtering firewalls
  - Stateless inspection ignores state of the connection:
    - Between internal and external computers
  - Blocks or allows packets based on header information only

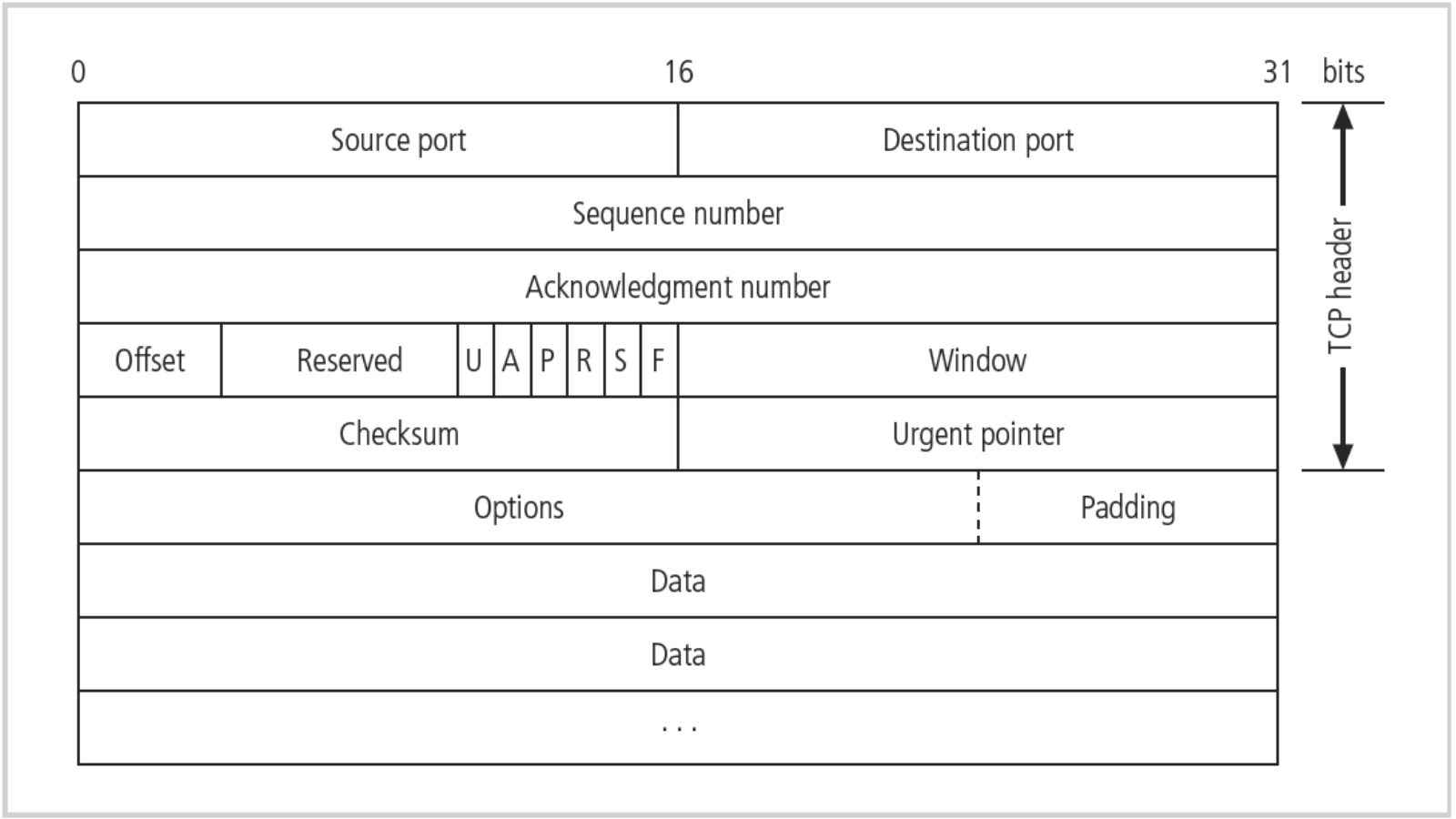

Figure 4-6 TCP packet structure
© *Cengage Learning 2013*

Packet-Filtering Firewalls (cont'd.)

- Packet-filtering router
  - Ability to restrict a specific service
    - Standard in most routers
  - Unable to detect whether packet headers have been modified
- IP spoofing
  - Falsification of the source IP address

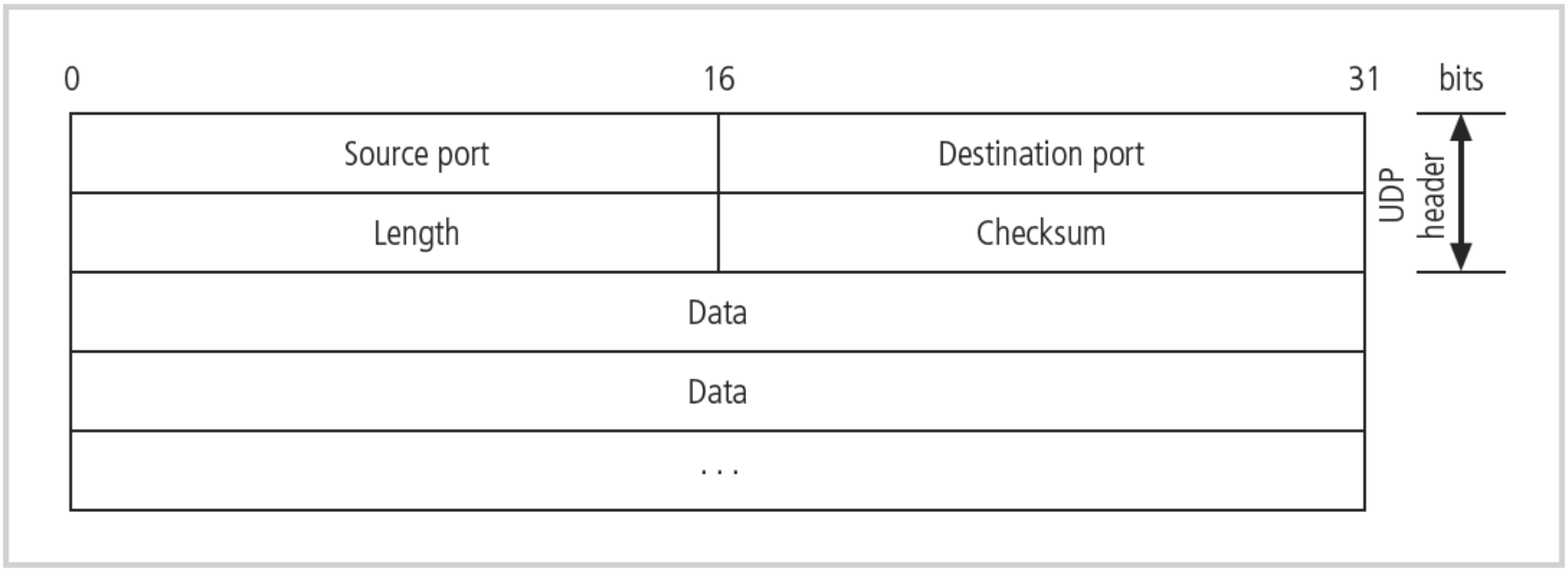

Figure 4-7 UDP packet structure
© *Cengage Learning 2013*

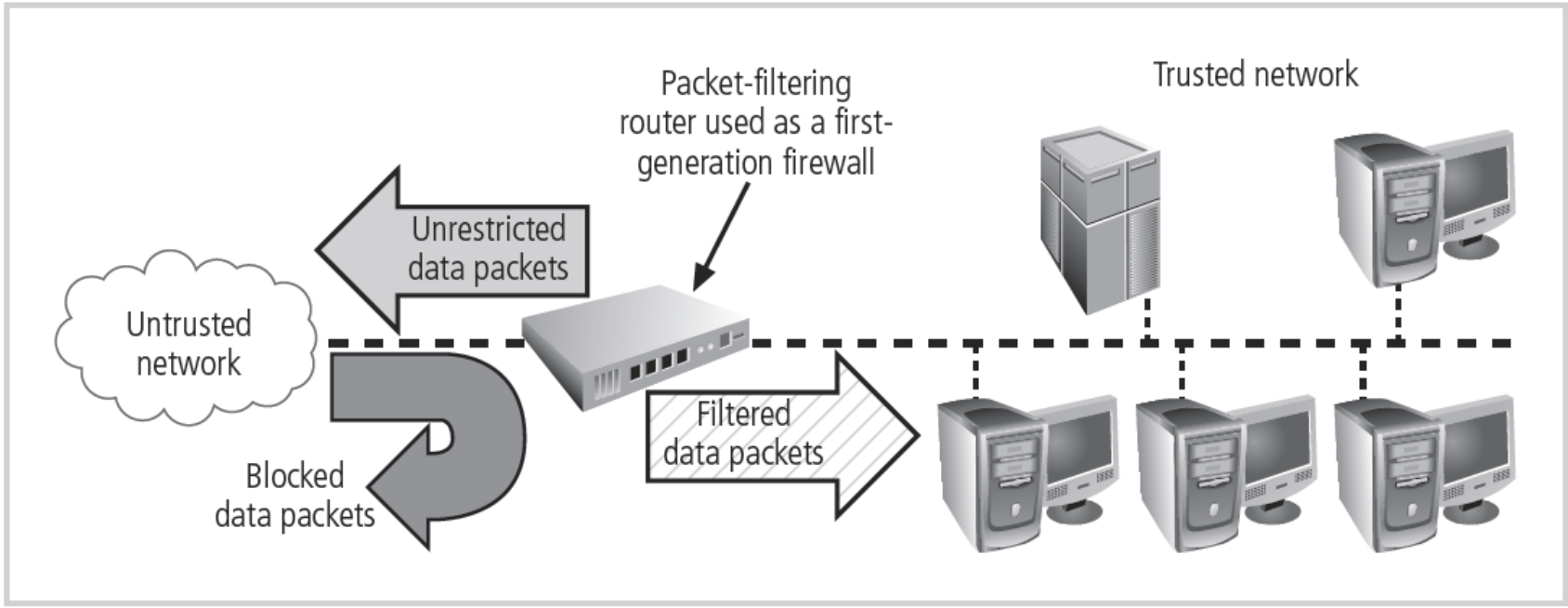

Figure 4-8 Packet-filtering router
© Cengage Learning 2013

Packet-Filtering Firewalls (cont'd.)

- Stateful packet-filtering firewalls
  - Examine data in the packet
  - Examine state of the connection between internal and external computers
- State table tracks state and context of each packet
  - Records which station sent what packet and when
- Stateful packet filtering
  - Allows incoming packets sent in response to internal requests

Packet-Filtering Firewalls (cont'd.)

- Disadvantage of stateful packet-filtering
  - Additional processing required to manage packets and verify against state table
- Dynamic stateful filtering firewalls
  - Make changes to filtering rules based on events as they happen

Source Address	Source Port	Destination Address	Destination Port	Time Remaining (in Seconds)	Total Time (in Seconds)	Protocol
192.168.2.5	1028	10.10.10.7	80	2725	3600	TCP

Table 4-3 State table entries

Application-Level Gateways

- Also called proxy server
- Works at the application layer
- Intermediary between two systems
- Control the way applications inside the network access external networks

Application-Level Gateways (cont'd.)

- Other application-level gateway tasks
  - Load balancing
  - IP address mapping
  - Filtering specific content
  - URL filtering
  - Fragmentation attack prevention

Multi-Layer Filtering

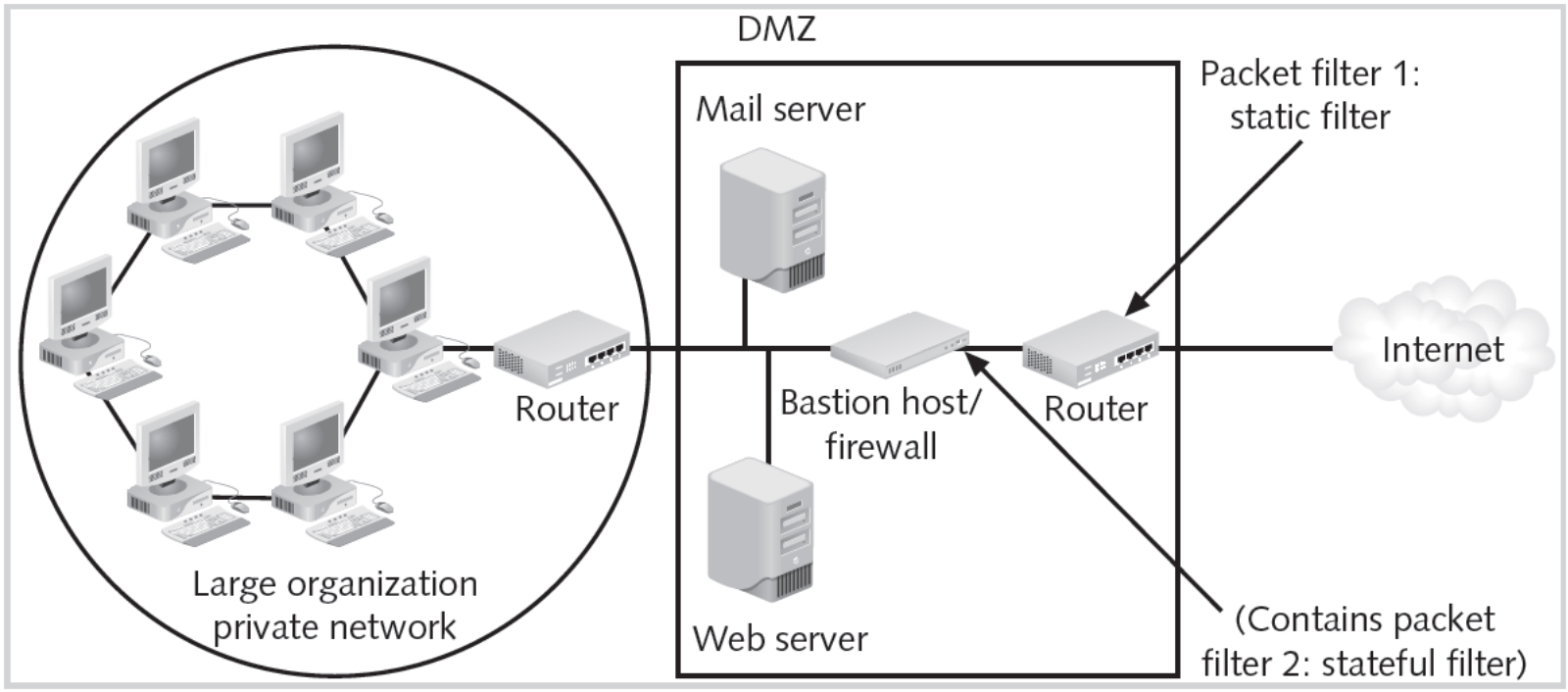

Figure 4-9 Multiple packet filters

Multi-Layer Filtering (cont'd.)

- Deep packet inspection
  - Combines stateful packet filtering with ability to analyze protocols for inconsistencies
- Disadvantage of multi-layer filtering
  - Longer processing time

Circuit-Level Gateways

- Operate at the transport layer
- Do not usually examine traffic
- Create tunnels connecting specific processes or systems

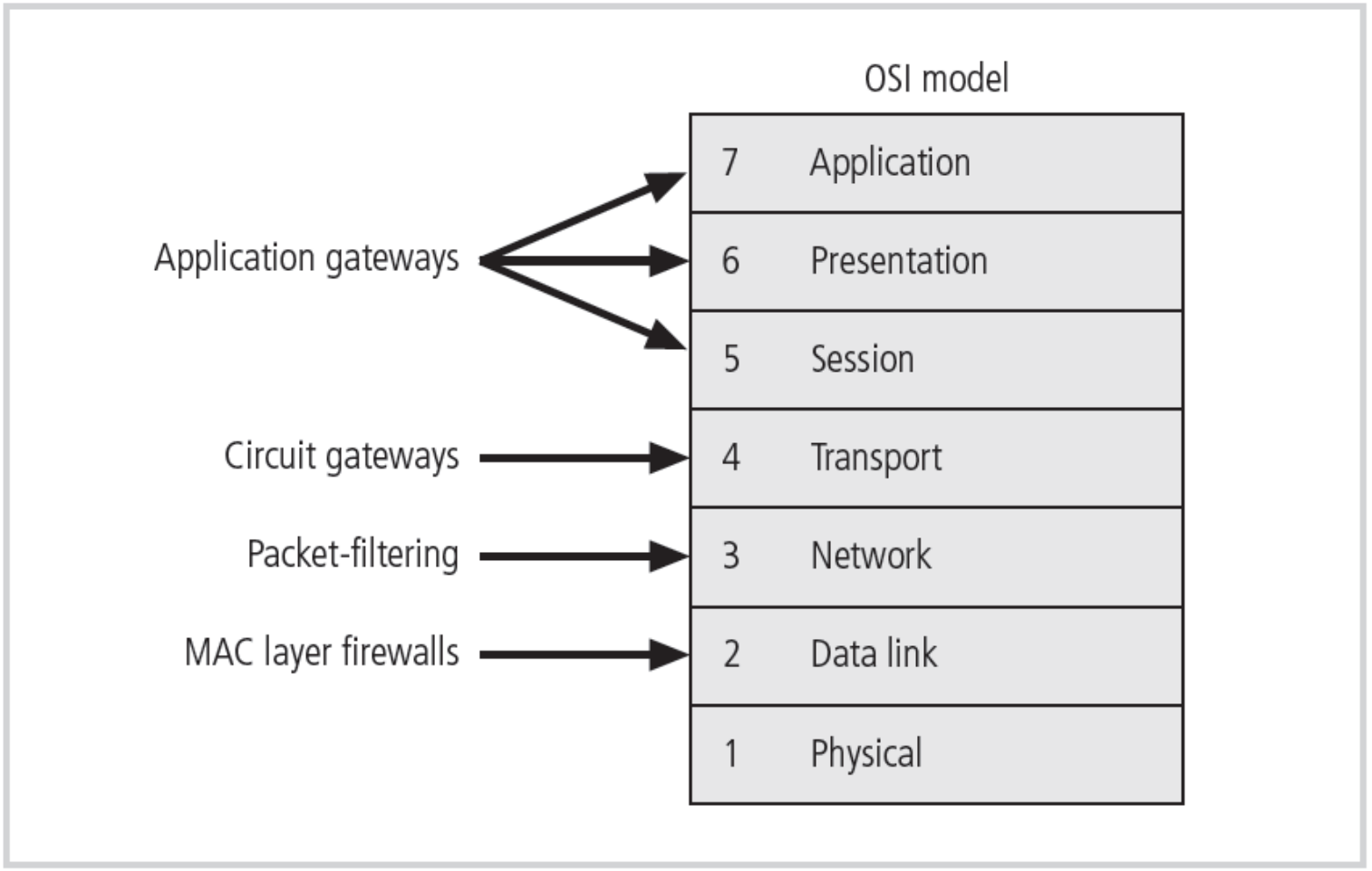

Figure 4-10 Firewalls in the OSI model
© *Cengage Learning 2013*

Firewall Form Factors

- Form factor categorization
  - Grade: residential or commercial
  - Hardware-based, software-based, appliance-based
- Commercial-grade firewalls
  - Most are dedicated appliances
  - Some are general computer systems with custom software
- Residential-grade firewalls
  - Software on user's computer
  - Simplified dedicated appliance

Firewall Appliances

- Stand-alone, self-contained
- Combine hardware and software
- Firewall rules stored in NVM
  - Configurable
  - Available each time device is restarted
- Examples of firewall appliances
  - Cisco Systems Adaptive Security Appliance
  - Fortinet Fortigate
  - McAfee Firewall Enterprise

Firewall Appliances (cont'd.)

- Firewall systems
  - Application software configured for the firewall application
    - Installed on general computer or specialized hardware
- Examples of commercial-grade firewall packages
  - Check Point Software Technologies Firewall Software Blade
  - Barracuda Networks NG Firewall

Firewall Appliances (cont'd.)

- Virtual firewalls
  - Same features as traditional firewall
  - Located on a virtual server
  - Implemented as a virtual security appliance
- Examples of virtual firewalls
  - Juniper Networks vGW Series
  - Altor v4.0
  - McAfee Firewall Enterprise, Virtual Appliance

Firewall Appliances (cont'd.)

- Small office/home office firewall appliances
  - Residential-grade firewall
  - Broadband gateway or DSL/cable modem router
- Recent advancements
  - Broadband firewall combined with features of wireless access point and stackable LAN switches
  - Some systems include packet-filtering, port-filtering, and simple intrusion detection systems

Firewall Appliances (cont'd.)

- Firewall software
  - Examines communication on its installed system
- Free firewall tools on the Internet
  - Most run on free operating systems
  - Examples: Windows Firewall, Application Firewall, Netfilter and iptables, ZoneAlarm Free Firewall

Firewall Architectures

- Four common architectural implementations
  - Packet-filtering routers
  - Screened host firewalls
  - Dual-homed firewalls
  - Screened subnet firewalls
- Best firewall configuration depends on:
  - Objectives of the network
  - Organization's ability to develop and implement architecture
  - Available budget

Packet-Filtering Routers

- Simple and effective
- Drawbacks
  - Lacks auditing capability
  - Lacks strong authentication
  - Complex ACLs can degrade network performance

Screened Host Firewalls

- Packet-filtering router is combined with a separate dedicated firewall
  - Router prescreens packets and minimizes load on internal proxy

Screened Host Firewalls (cont'd.)

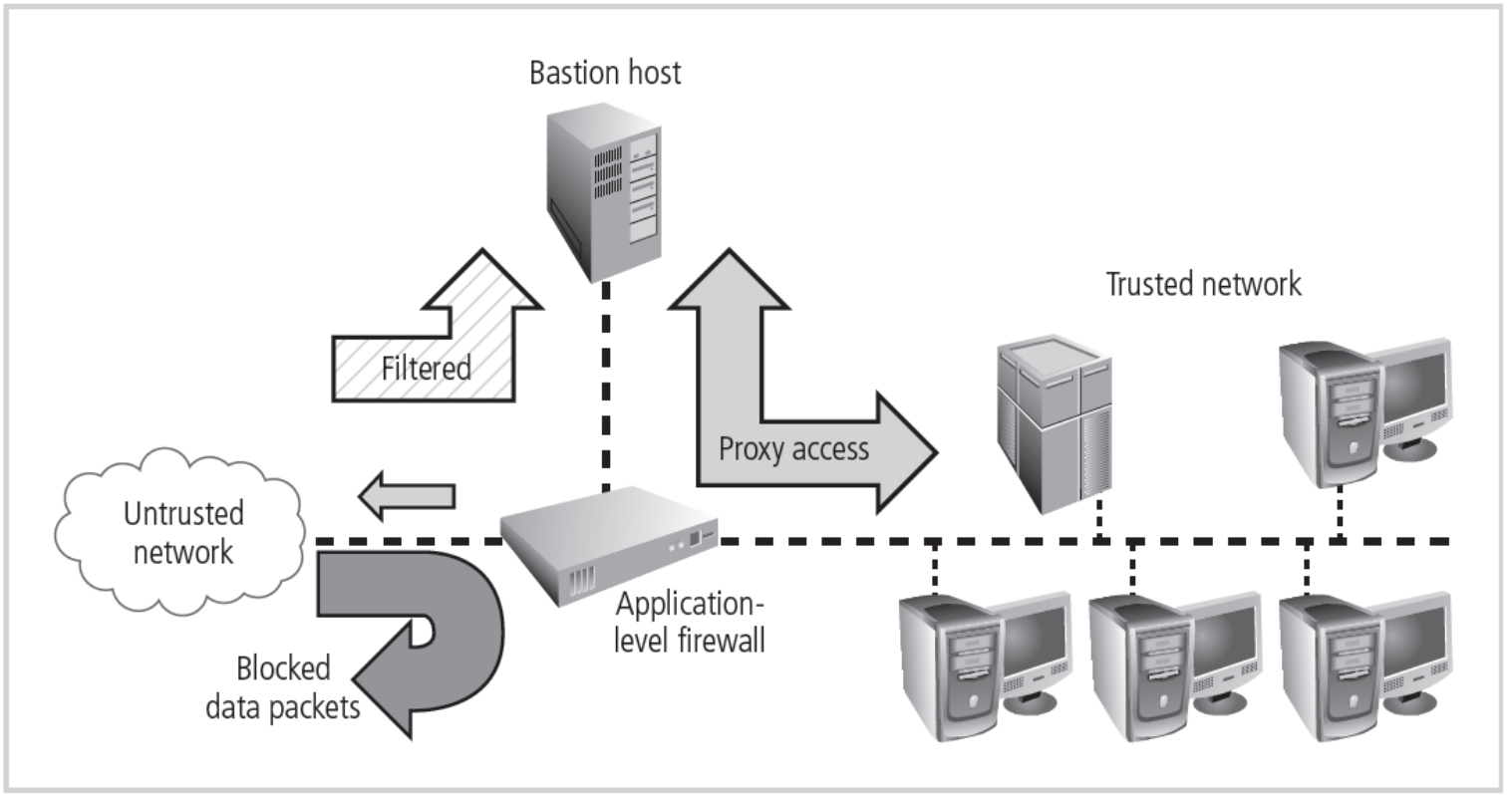

Figure 4-16 Screened host architecture

Dual-Homed Host Firewalls

- Bastion host contains two NICs
  - One NIC connected to the external network
  - One NIC connected to the internal network
- Network address translation
  - Mapping real, valid, external IP addresses to special ranges of nonroutable internal IP addresses

Dual-Homed Host Firewalls (cont'd.)

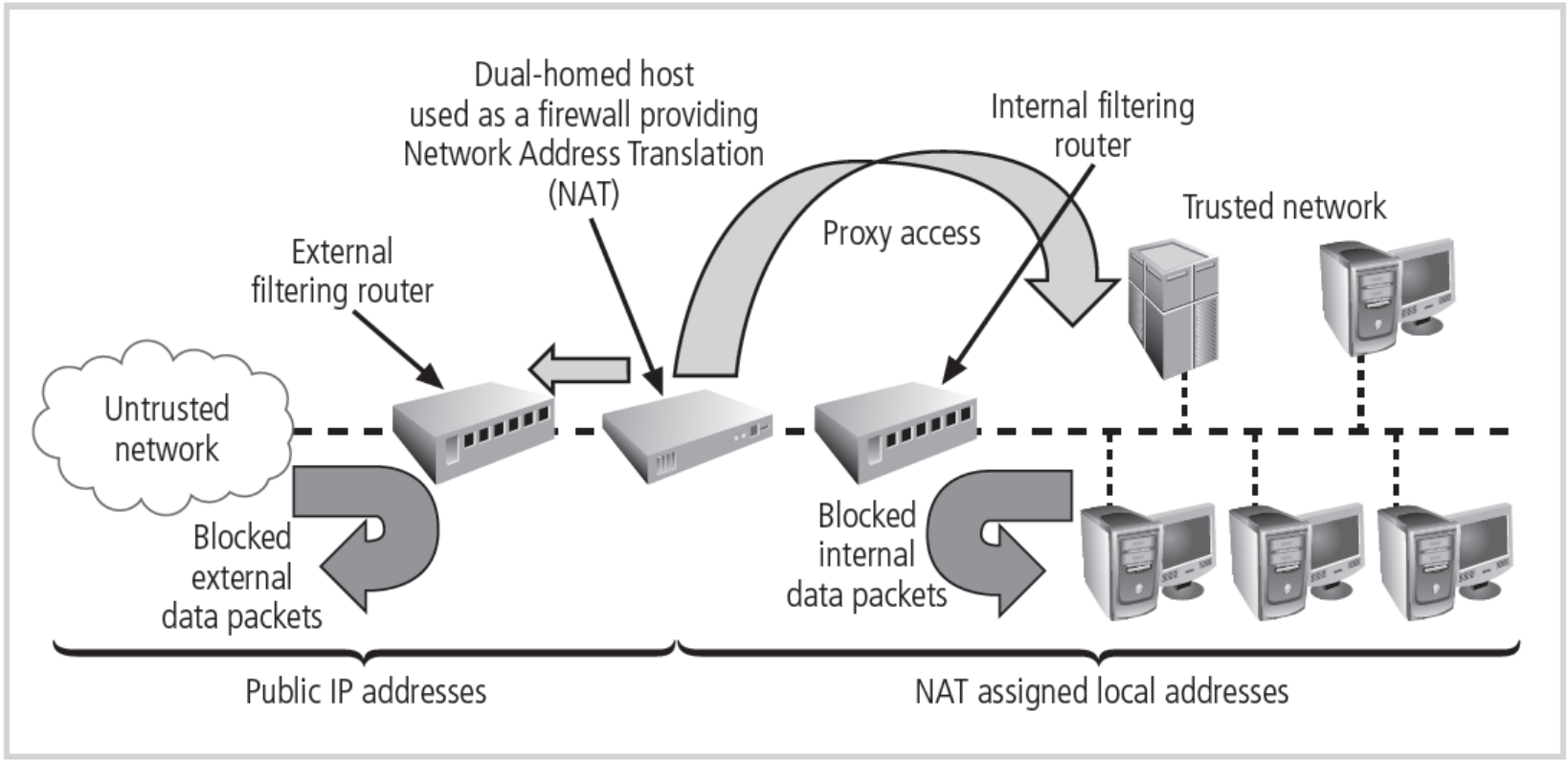

Figure 4-17 Dual-homed host
© *Cengage Learning 2013*

Screened Subnet Firewalls (with DMZ)

- Dominant architecture in use today
- DMZ
  - Dedicated port on the firewall device or connected to a screened subnet
- Extranet
  - DMZ segment with additional authentication and authorization controls

Screened Subnet Firewalls (cont'd.)

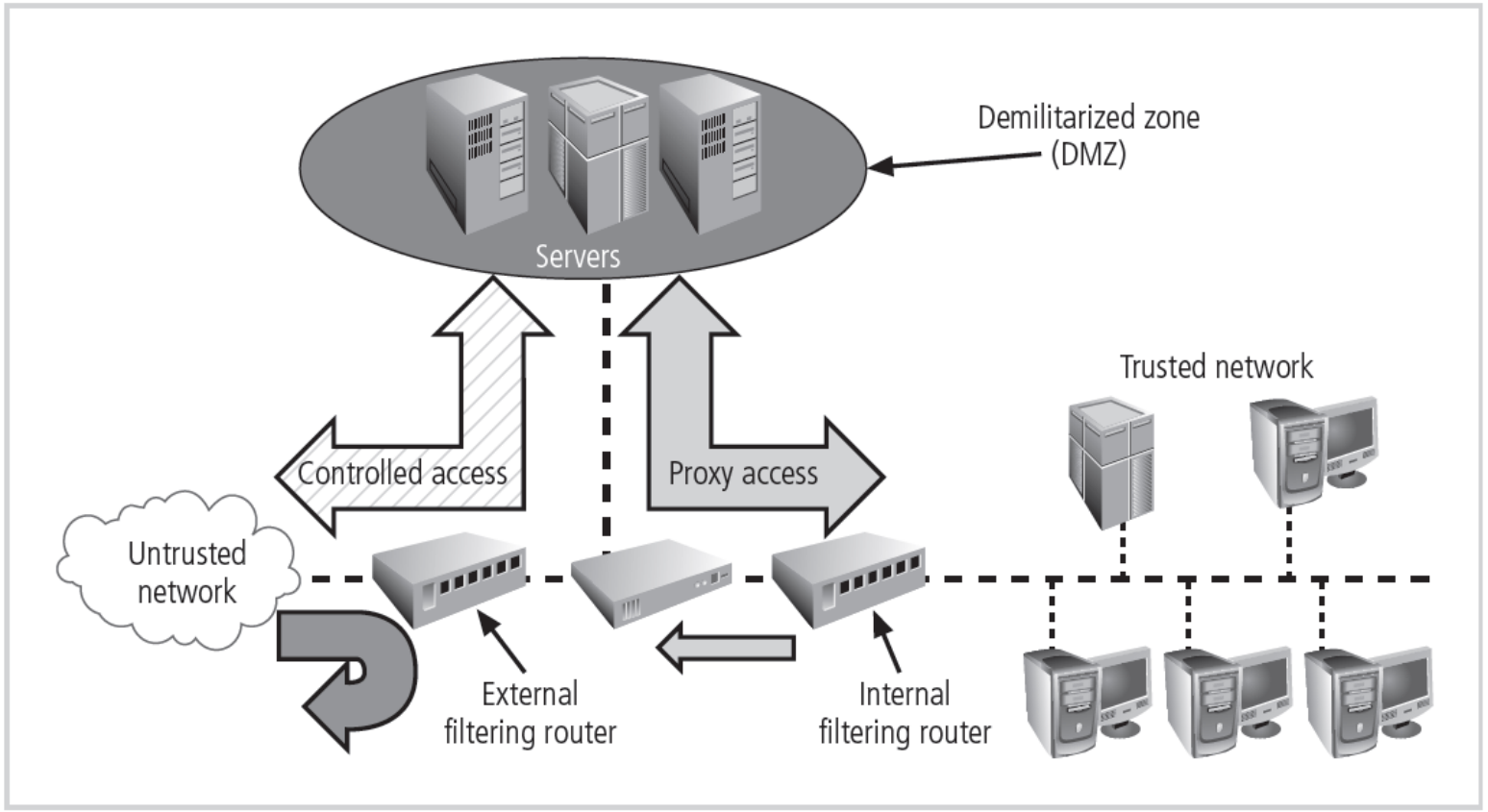

Figure 4-18 Screened subnet
© *Cengage Learning 2013*

Limitations of Firewalls

- Firewalls should be part of an overall security plan
  - Used in conjunction with other forms of protection
- Firewall infrastructure considerations
  - Packet filtering has limitations
  - Firewalls can be circumvented
  - Key concepts include defense-in-depth and principle of least privilege
  - Firewalls must be kept updated with latest patches
  - Firewall rules can be complex

Limitations of Firewalls (cont'd.)

- Firewall infrastructure considerations (cont'd.)
  - Firewall placement is crucial
  - Firewalls are not substitutes for security policy
  - Trained administrators must understand network protocols and the security policy
  - Firewalls will introduce latency

Summary

- Firewall can be hardware, software, or a combination of the two
- Firewalls filter the transmission of information packets
- Application-level gateways control the way applications inside the network access external networks
- Firewall categorization types include generation and form factor
- Firewalls can have different network connection architectures