COURSE TECHNOLOGY
CENGAGE Learning™

# Principles of Information Security, Fifth Edition

## *Chapter 6*

## *Security Technology: Firewalls and VPNs*

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

BRUCE SCHNEIER, AMERICAN CRYPTOGRAPHER, COMPUTER SECURITY SPECIALIST, AND WRITER

# Learning Objectives

- Upon completion of this material, you should be able to:
  - Discuss the important role of access control in computer-based information systems, and identify and discuss widely used authentication factors
  - Describe firewall technology and the various approaches to firewall implementation
  - Identify the various approaches to control remote and dial-up access by authenticating and authorizing users

# Learning Objectives (cont'd)

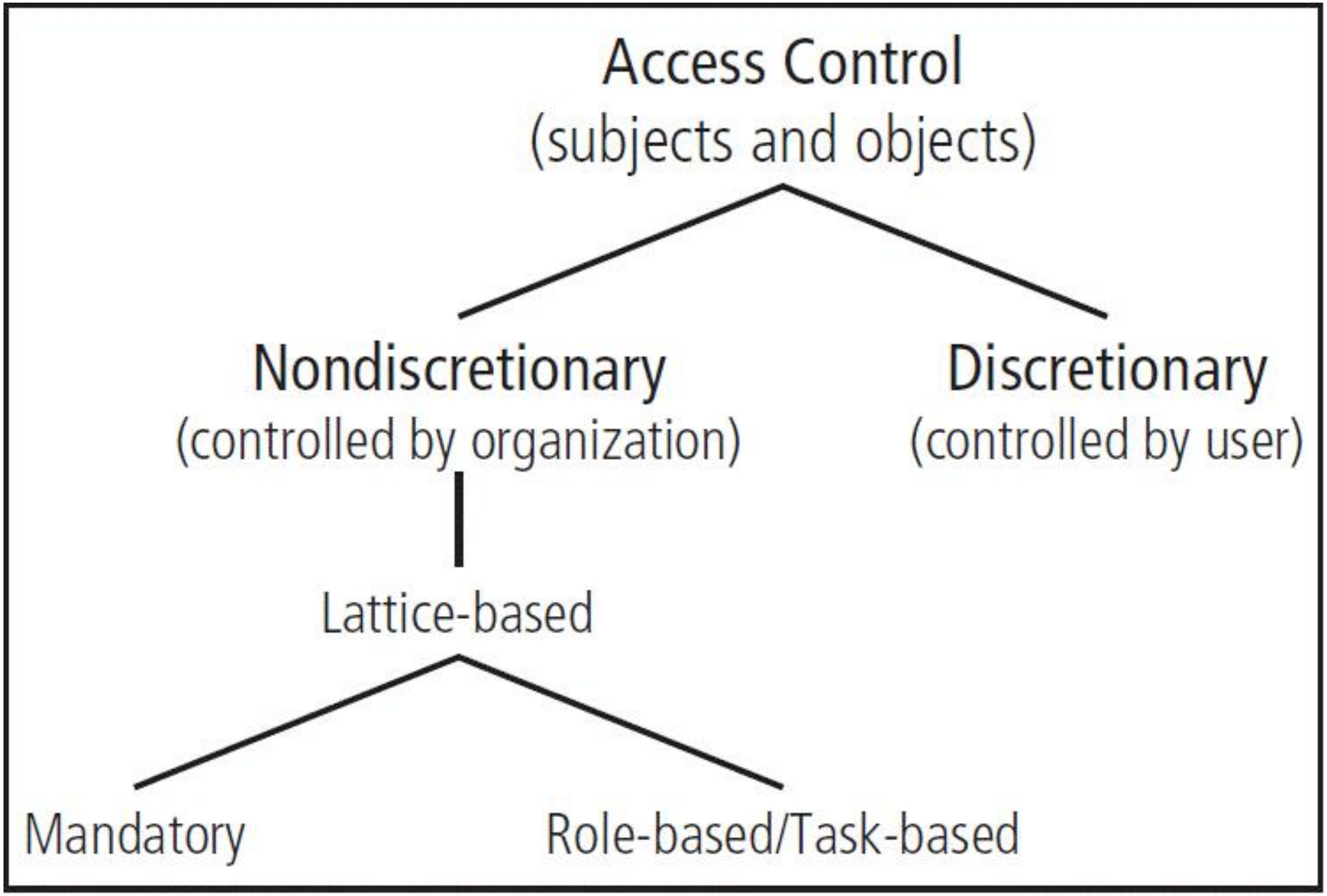
- Discuss content filtering technology
- Describe virtual private networks and discuss the technology that enables them

# Introduction

- Technical controls are essential in enforcing policy for many IT functions not under direct human control.
- When properly implemented, technical control solutions improve an organization’s ability to balance the objectives of making information readily available and preserving information’s confidentiality and integrity.

# Access Control

- Access control: method by which systems determine whether and how to admit a user into a trusted area of the organization
- Mandatory access controls (MACs): use data classification schemes
- Discretionary access controls (DACs): allow users to control and possibly provide access to information/resources at their disposal
- Nondiscretionary controls: strictly enforced version of MACs that are managed by a central authority



© Cengage Learning 2015

**Figure 6-1** Access control approaches

# Identification

- Identification: mechanism whereby unverified entities seeking access to a resource (supplicants) provide a label by which they are known to the system
- Identifiers can be composite identifiers, concatenating elements—department codes, random numbers, or special characters—to make them unique.
- Some organizations generate random numbers.

# Authentication

- Authentication: the process of validating a supplicant's purported identity
- Authentication factors
  - Something a supplicant knows
    - Password: a private word or a combination of characters that only the user should know
    - Passphrase: a series of characters, typically longer than a password, from which a virtual password is derived

# Authentication (cont’d)

- Authentication factors (cont’d)
  - Something a supplicant has
    - Dumb card: ID or ATM card with magnetic stripe
    - Smart card: contains a computer chip that can verify and validate information
    - Synchronous tokens
    - Asynchronous tokens
  - Something a supplicant is
    - Relies upon individual characteristics
    - Strong authentication

# Authorization

- Authorization: the matching of an authenticated entity to a list of information assets and corresponding access levels
- Authorization can be handled in one of three ways:
  - Authorization for each authenticated user
  - Authorization for members of a group
  - Authorization across multiple systems
- Authorization tickets

# Accountability

- Accountability (auditability): ensures that all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity
- Most often accomplished by means of system logs and database journals, and the auditing of these records
- Systems logs record specific information.
- Logs have many uses.

# Biometrics

- Approach based on the use of measurable human characteristics/traits to authenticate identity
- Only fingerprints, retina of eye, and iris of eye are considered truly unique.
- Evaluated on false reject rate, false accept rate, and crossover error rate
- Highly reliable/effective biometric systems are often considered intrusive by users.

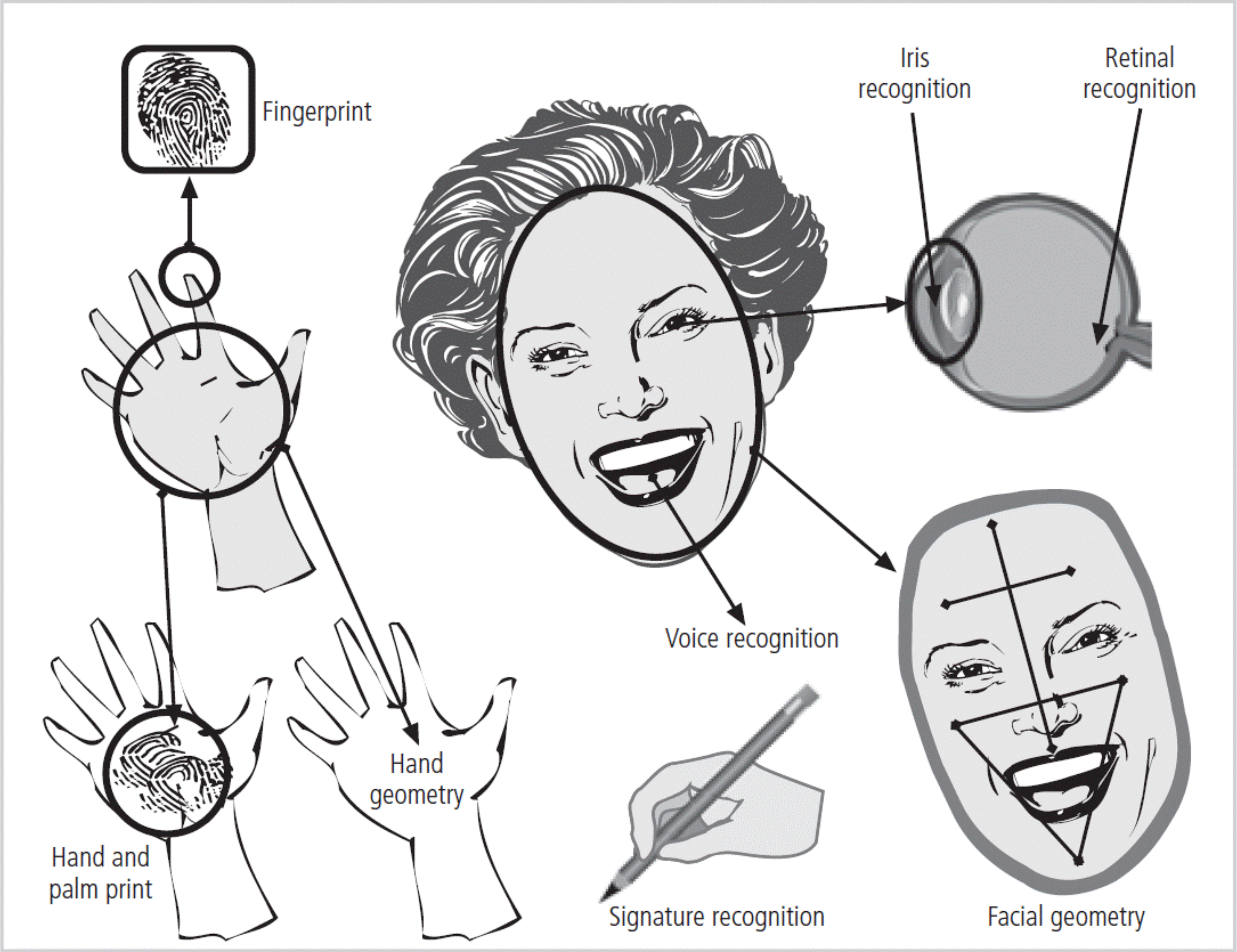
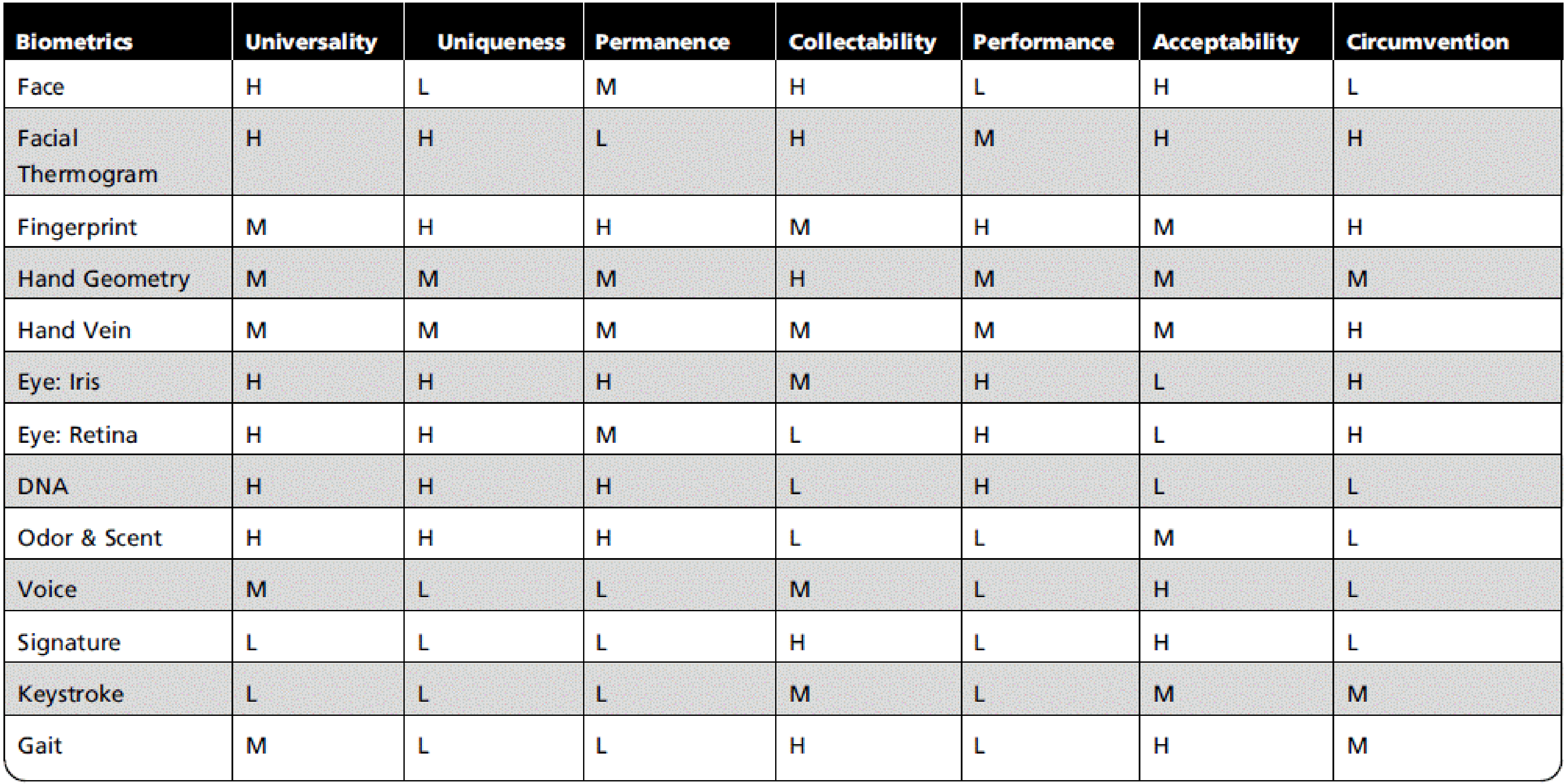


**Figure 6-5** Biometric recognition characteristics



| Biometrics | Universality | Uniqueness | Permanence | Collectability | Performance | Acceptability | Circumvention |
|---|---|---|---|---|---|---|---|
| Face | H | L | M | H | L | H | L |
| Facial Thermogram | H | H | L | H | M | H | H |
| Fingerprint | M | H | H | M | H | M | H |
| Hand Geometry | M | M | M | H | M | M | M |
| Hand Vein | M | M | M | M | M | M | H |
| Eye: Iris | H | H | H | M | H | L | H |
| Eye: Retina | H | H | M | L | H | L | H |
| DNA | H | H | H | L | H | L | L |
| Odor & Scent | H | H | H | L | L | M | L |
| Voice | M | L | L | M | L | H | L |
| Signature | L | L | L | H | L | H | L |
| Keystroke | L | L | L | M | L | M | M |
| Gait | M | L | L | H | L | H | M |

**Table 6-1** Ranking of Biometric Effectiveness and Acceptance

In the table, H = High, M = Medium, and L = Low.

*From multiple sources.*[3]

# Access Control Architecture Models

- Illustrate access control implementations and can help organizations quickly make improvements through adaptation
- Trusted computing base (TCB)
  - Part of TCSEC Rainbow Series
  - Used to enforce security policy (rules of system configuration)
  - Biggest challenges include covert channels
    - Storage channels
    - Timing channels

# Access Control Architecture Models (cont’d)

- ITSEC: an international set of criteria for evaluating computer systems
  - Compares Targets of Evaluation (ToE) to detailed security function specifications
- The Common Criteria
  - Considered successor to both TCSEC and ITSEC
- Bell-LaPadula Confidentiality Model
  - Model of an automated system able to manipulate its state or status over time
- Biba Integrity Model
  - Based on “no write up, no read down” principle

# Access Control Architecture Models (cont’d)

- Clark-Wilson Integrity Model
  - No changes by unauthorized subjects
  - No unauthorized changes by authorized subjects
  - Maintenance of internal and external consistency
- Graham-Denning Access Control Model
  - Composed of set of objects, set of subjects, and set of rights
- Harrison-Ruzzo-Ullman Model
  - Defines method to allow changes to access rights and addition/removal of subjects/objects
- Brewer-Nash Model (Chinese Wall)
  - Designed to prevent conflict of interest between two parties

# Firewalls

- Prevent specific types of information from moving between an untrusted network (the Internet) and a trusted network (organization’s internal network)
- May be:
  - Separate computer system
  - Software service running on existing router or server
  - Separate network containing supporting devices

# Firewalls Processing Modes

- Five processing modes by which firewalls can be categorized:
  - Packet filtering
  - Application gateways
  - Circuit gateways
  - MAC layer firewalls
  - Hybrids

# Packet-Filtering Firewalls

- Packet-filtering firewalls examine the header information of data packets.
- Most often based on the combination of:
  - IP source and destination address
  - Direction (inbound or outbound)
  - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests
- Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through device.

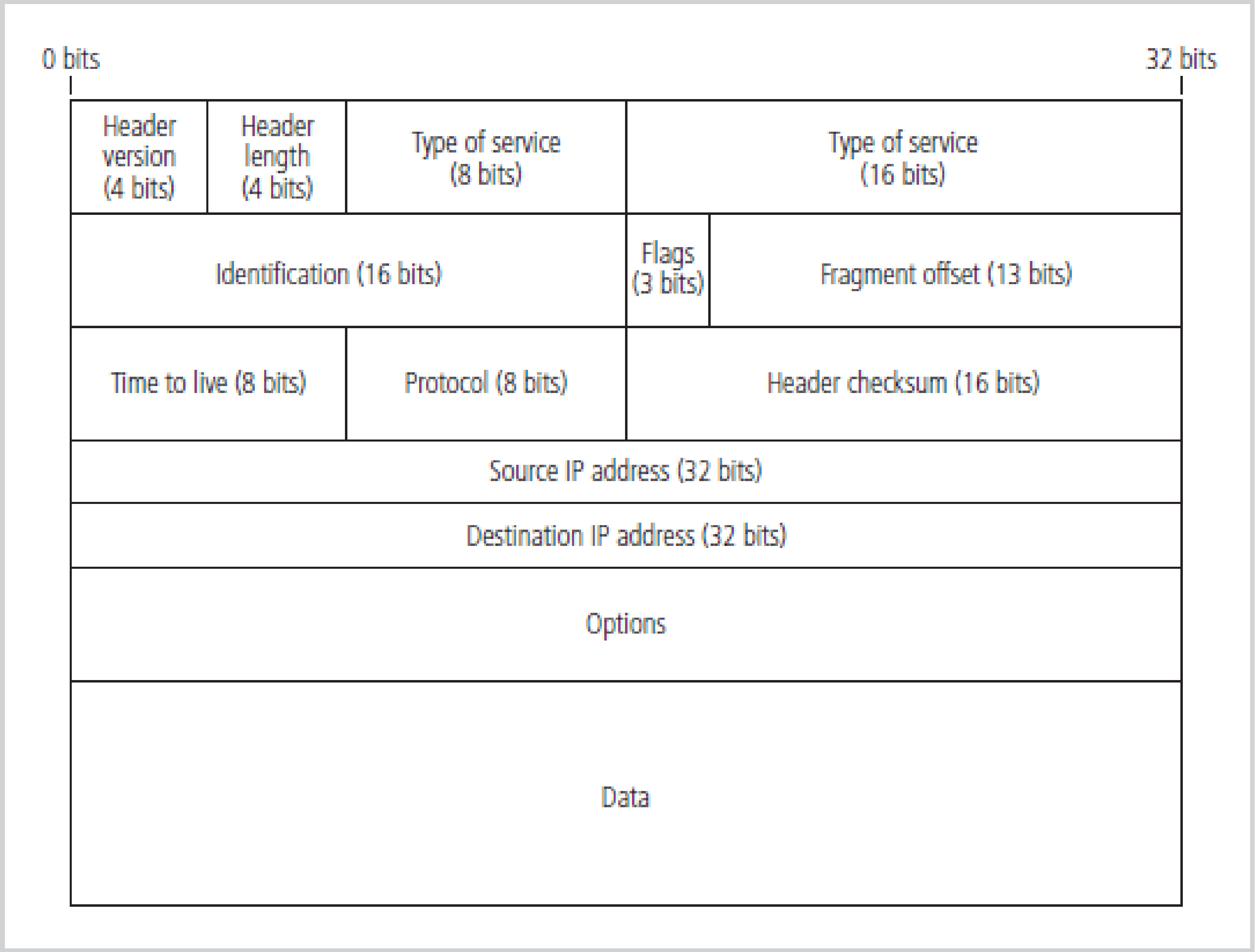
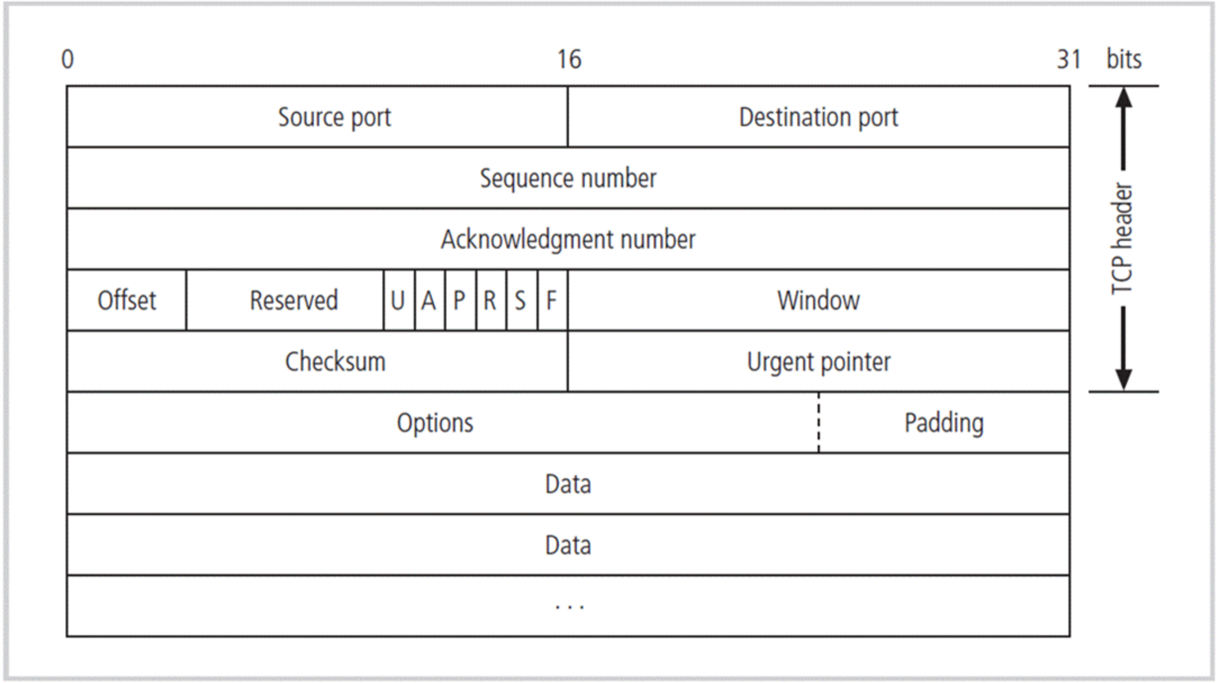
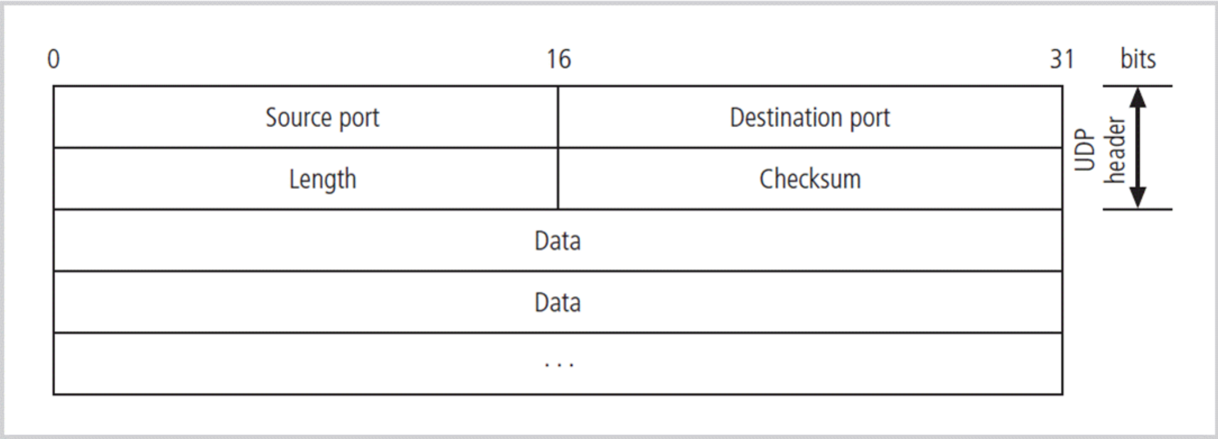


**Figure 6-7** IP packet structure



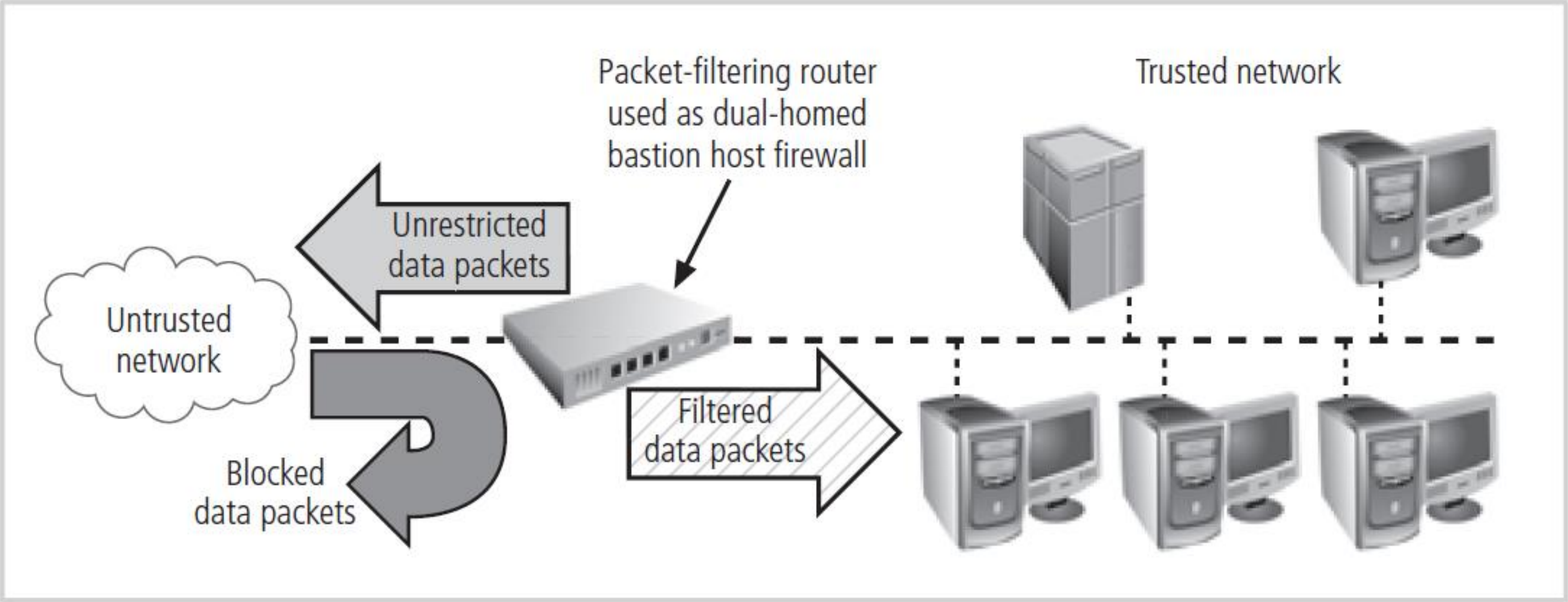
© Cengage Learning 2015

**Figure 6-8** TCP packet structure



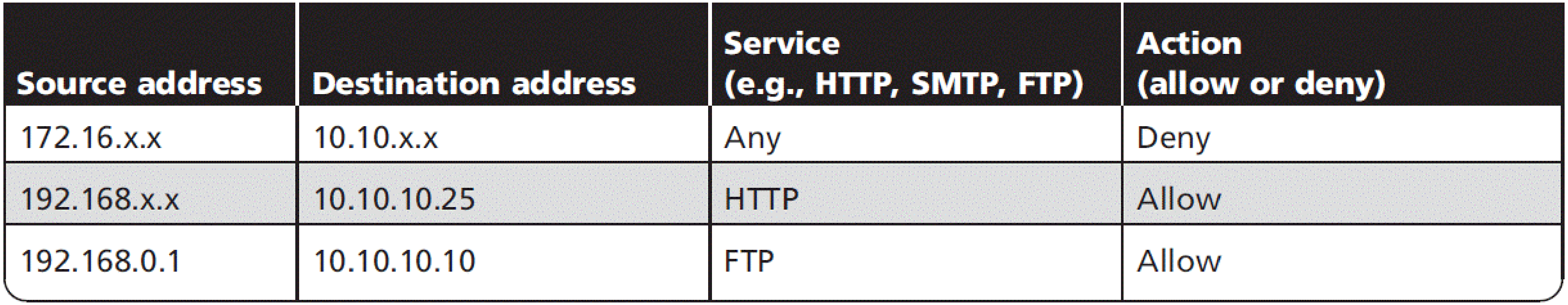
© Cengage Learning 2015

**Figure 6-9** UDP datagram structure


Packet-filtering router used as dual-homed bastion host firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

© Cengage Learning 2015

**Figure 6-10** Packet-filtering router

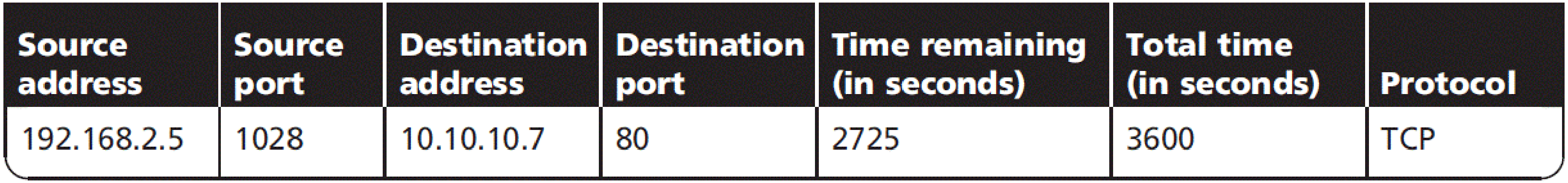


| Source address | Destination address | Service<br>(e.g., HTTP, SMTP, FTP) | Action<br>(allow or deny) |
|---|---|---|---|
| 172.16.x.x | 10.10.x.x | Any | Deny |
| 192.168.x.x | 10.10.10.25 | HTTP | Allow |
| 192.168.0.1 | 10.10.10.10 | FTP | Allow |

**Table 6-2 Sample Firewall Rule and Format**

# Packet-Filtering Firewalls (cont'd)

- Three subsets of packet-filtering firewalls:
  - Static filtering: requires that filtering rules be developed and installed within the firewall
  - Dynamic filtering: allows firewall to react to emergent event and update or create rules to deal with event
  - Stateful inspection: firewalls that keep track of each network connection between internal and external systems using a state table



| 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 6-3** **State Table Entries**

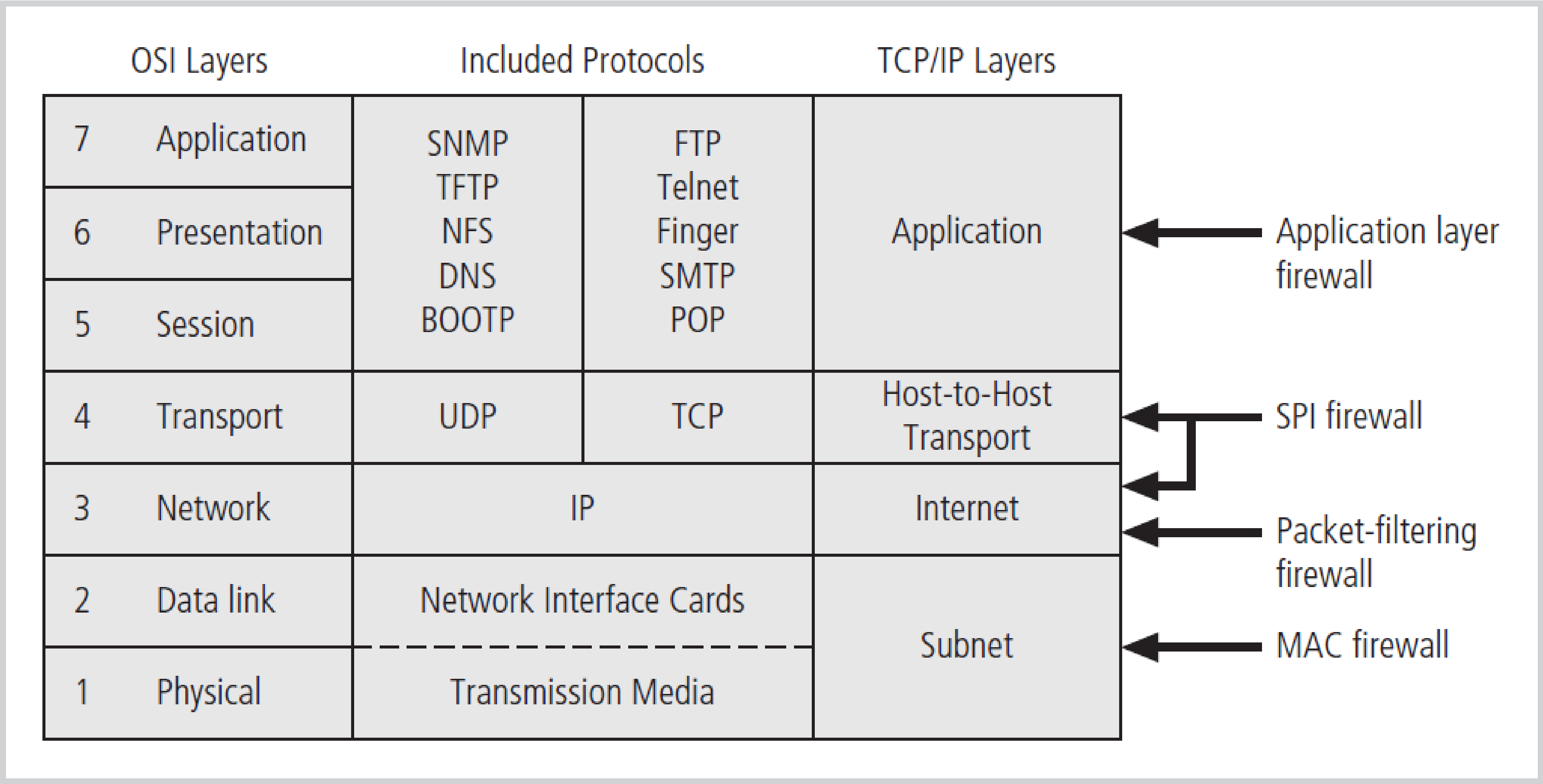
© Cengage Learning 2015

# Application Layer Firewall

- Frequently installed on a dedicated computer; also known as a proxy server
- Since proxy server is often placed in unsecured area of the network (e.g., DMZ), it is exposed to higher levels of risk from less trusted networks.
- Additional filtering routers can be implemented behind the proxy server, further protecting internal systems.

# Firewall Processing Modes (cont'd)

- MAC layer firewalls
  - Designed to operate at media access control sublayer of network's data link layer
  - Make filtering decisions based on specific host computer's identity
  - MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host; all other traffic is blocked.



| OSI Layers | | Included Protocols | | TCP/IP Layers | |
|---|---|---|---|---|---|
| 7 | Application | SNMP<br>TFTP<br>NFS<br>DNS<br>BOOTP | FTP<br>Telnet<br>Finger<br>SMTP<br>POP | Application | Application layer firewall |
| 6 | Presentation | | | | |
| 5 | Session | | | | |
| 4 | Transport | UDP | TCP | Host-to-Host Transport | SPI firewall |
| 3 | Network | IP | | Internet | Packet-filtering firewall |
| 2 | Data link | Network Interface Cards | | Subnet | MAC firewall |
| 1 | Physical | Transmission Media | | | |

**Figure 6-11** Firewall types and protocol models

# Firewall Processing Modes (cont’d)

- Hybrid firewalls
  - Combine elements of other types of firewalls, that is, elements of packet filtering and proxy services, or of packet filtering and circuit gateways
  - Alternately, may consist of two separate firewall devices; each a separate firewall system, but connected to work in tandem
  - Enables an organization to make security improvement without completely replacing existing firewalls

# Firewall Architectures

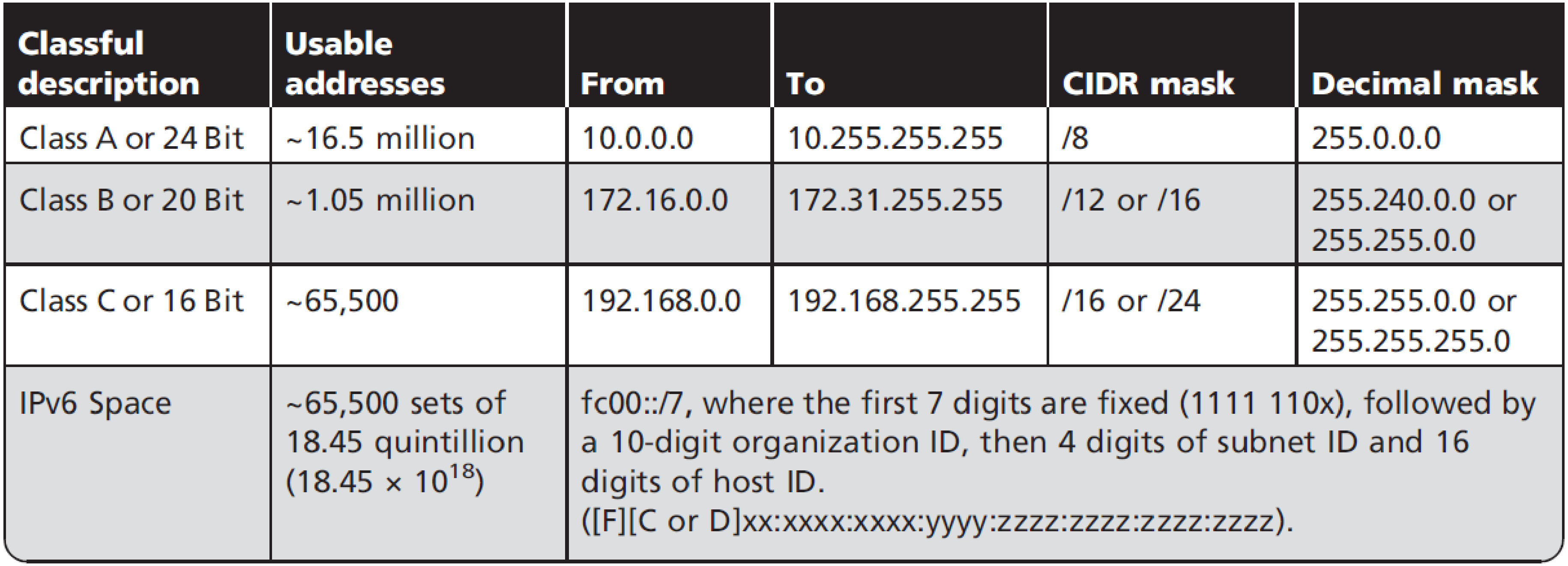
- Firewall devices can be configured in several network connection architectures.
- Best configuration depends on three factors:
  - Objectives of the network
  - Organization’s ability to develop and implement architectures
  - Budget available for function
- Four common architectural implementations of firewalls: packet-filtering routers, dual-homed firewalls (bastion hosts), screened host firewalls, screened subnet firewalls

# Firewall Architectures (cont’d)

- Packet-filtering routers
  - Most organizations with Internet connection have a router at the boundary between internal networks and external service provider.
  - Many of these routers can be configured to reject packets that the organization does not allow into its network.
  - Drawbacks include a lack of auditing and strong authentication.

# Firewall Architectures (cont'd)

- Bastion hosts
  - Commonly referred to as sacrificial host, as it stands as sole defender on the network perimeter
  - Contains two network interface cards (NICs): one connected to external network, one connected to internal network
  - Implementation of this architecture often makes use of network address translation (NAT), creating another barrier to intrusion from external attackers.



| Classful description | Usable addresses | From | To | CIDR mask | Decimal mask |
|---|---|---|---|---|---|
| Class A or 24 Bit | ~16.5 million | 10.0.0.0 | 10.255.255.255 | /8 | 255.0.0.0 |
| Class B or 20 Bit | ~1.05 million | 172.16.0.0 | 172.31.255.255 | /12 or /16 | 255.240.0.0 or 255.255.0.0 |
| Class C or 16 Bit | ~65,500 | 192.168.0.0 | 192.168.255.255 | /16 or /24 | 255.255.0.0 or 255.255.255.0 |
| IPv6 Space | ~65,500 sets of 18.45 quintillion (18.45 × $10^{18}$) | fc00::/7, where the first 7 digits are fixed (1111 110x), followed by a 10-digit organization ID, then 4 digits of subnet ID and 16 digits of host ID.<br>([F][C or D]xx:xxxx:xxxx:yyyy:zzzz:zzzz:zzzz:zzzz). | | | |

**Table 6-4 Reserved Nonroutable Address Ranges**

Note that CIDR stands for classless inter-domain routing.

*Source: Internet Engineering Task Force, RFC 1466 (http://tools.ietf.org/html/rfc1466).*

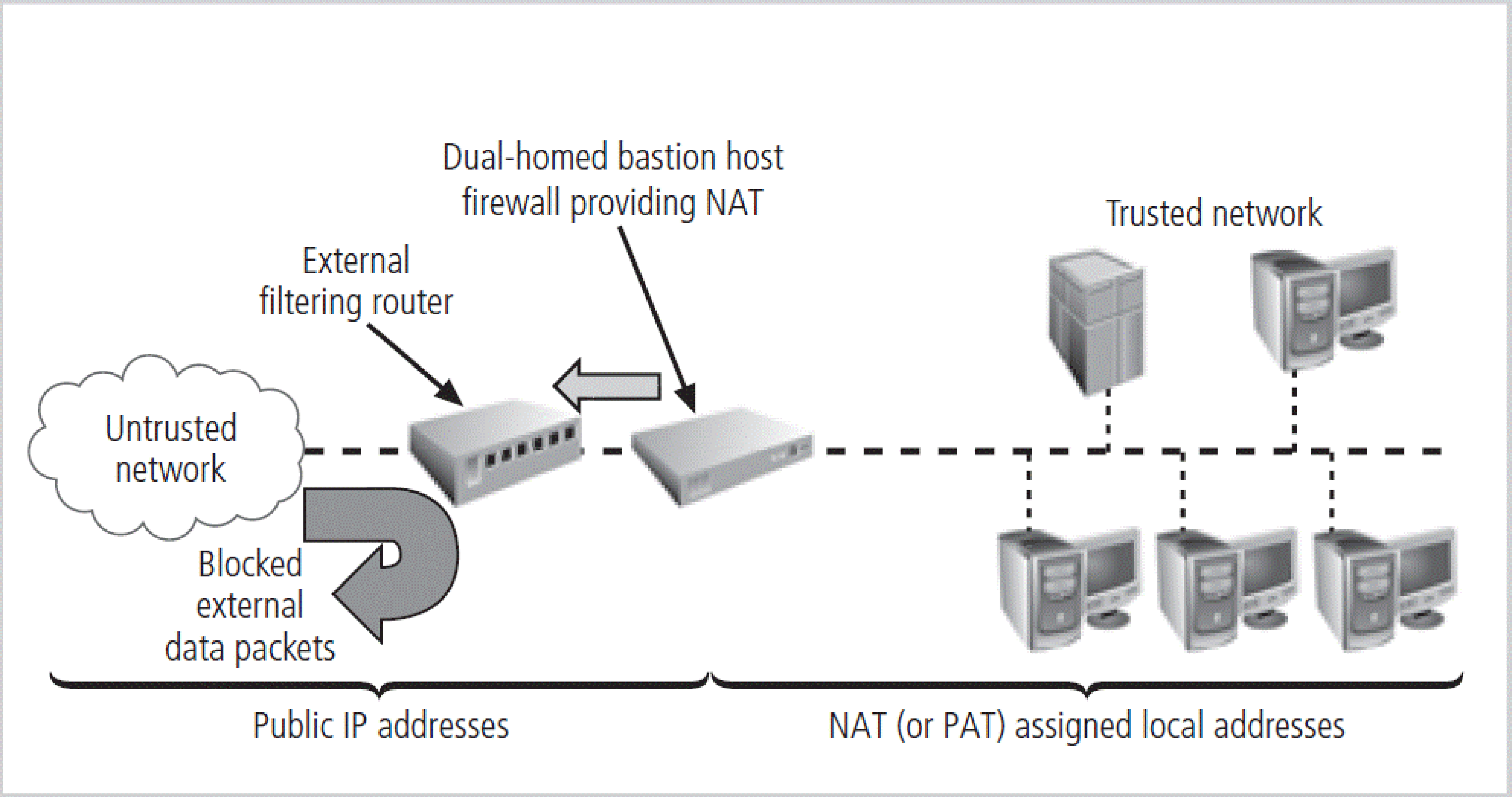


**Figure 6-16** Dual-homed bastion host firewall

# Firewall Architectures (cont'd)

- Screened host firewalls
  - Combines packet-filtering router with separate, dedicated firewall such as an application proxy server
  - Allows router to prescreen packets to minimize traffic/load on internal proxy
  - Requires external attack to compromise two separate systems before attack can access internal data

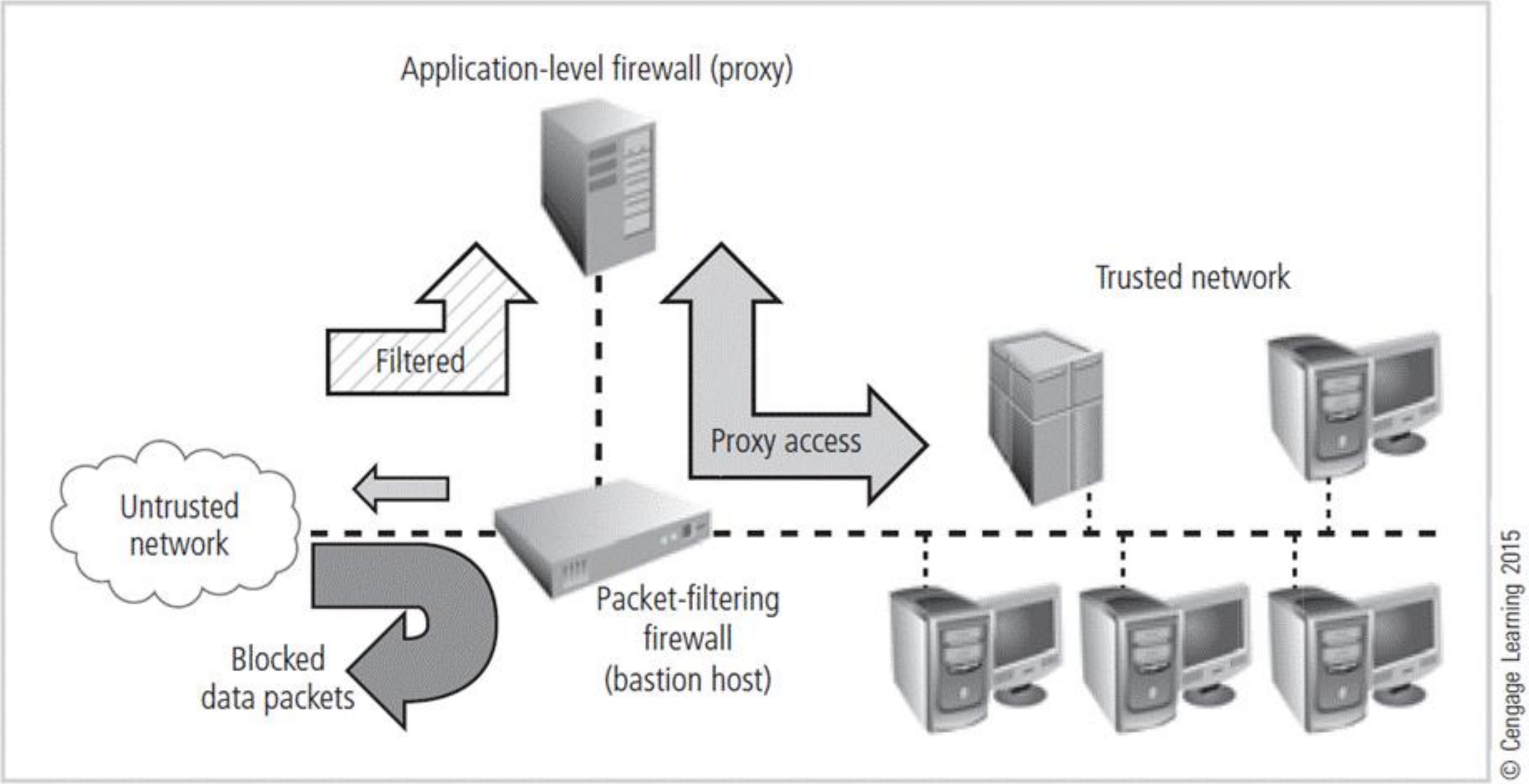


**Figure 6-17** Screened host firewall

# Firewall Architectures (cont'd)

- Screened subnet firewall (with DMZ)
  - Is the dominant architecture used today
  - Commonly consists of two or more internal bastion hosts behind packet-filtering router, with each host protecting a trusted network:
    - Connections from outside or untrusted network are routed through external filtering router.
    - Connections from outside or untrusted network are routed into and out of routing firewall to separate the network segment known as DMZ.
    - Connections into trusted internal network are allowed only from DMZ bastion host servers.

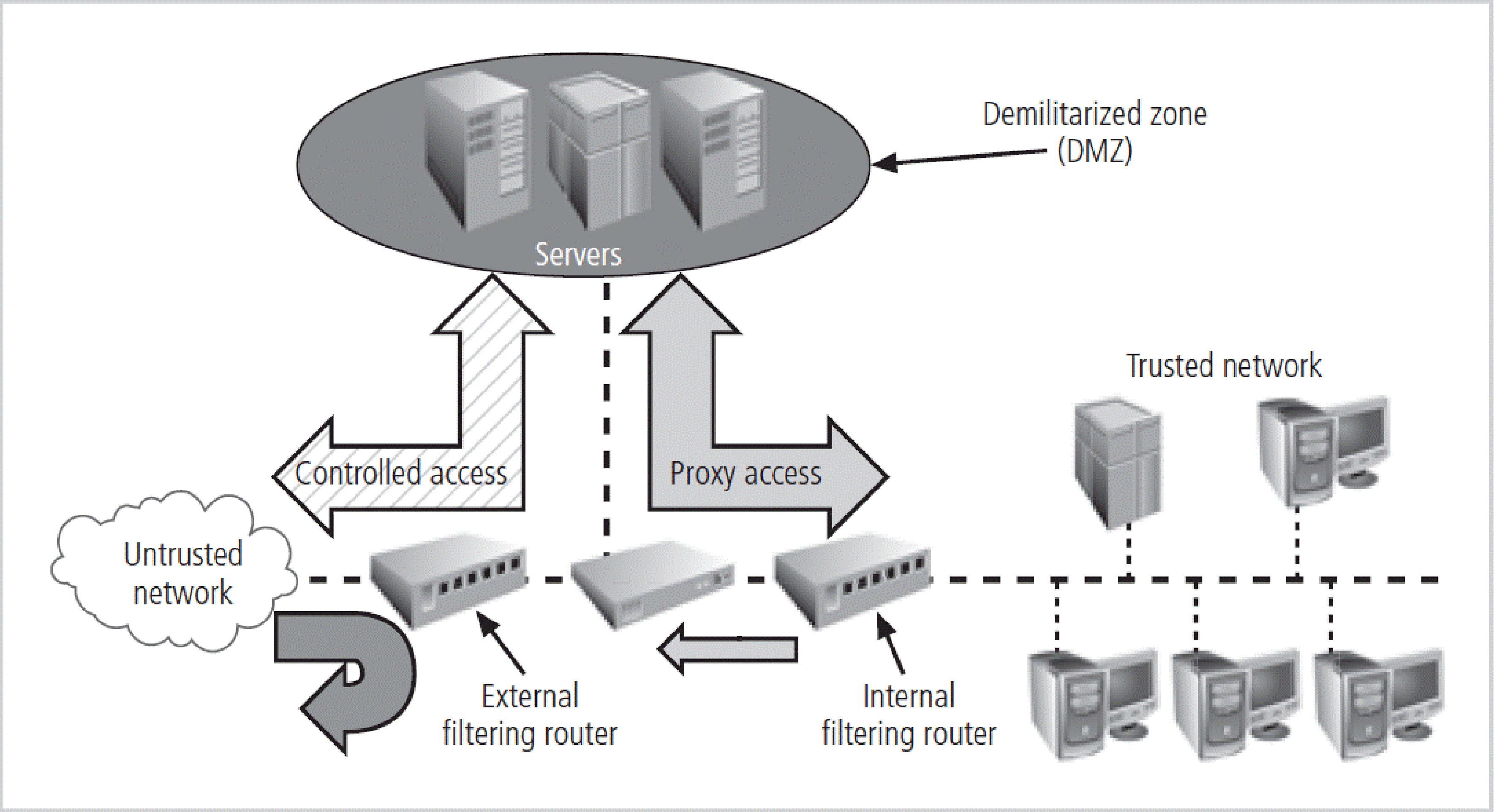
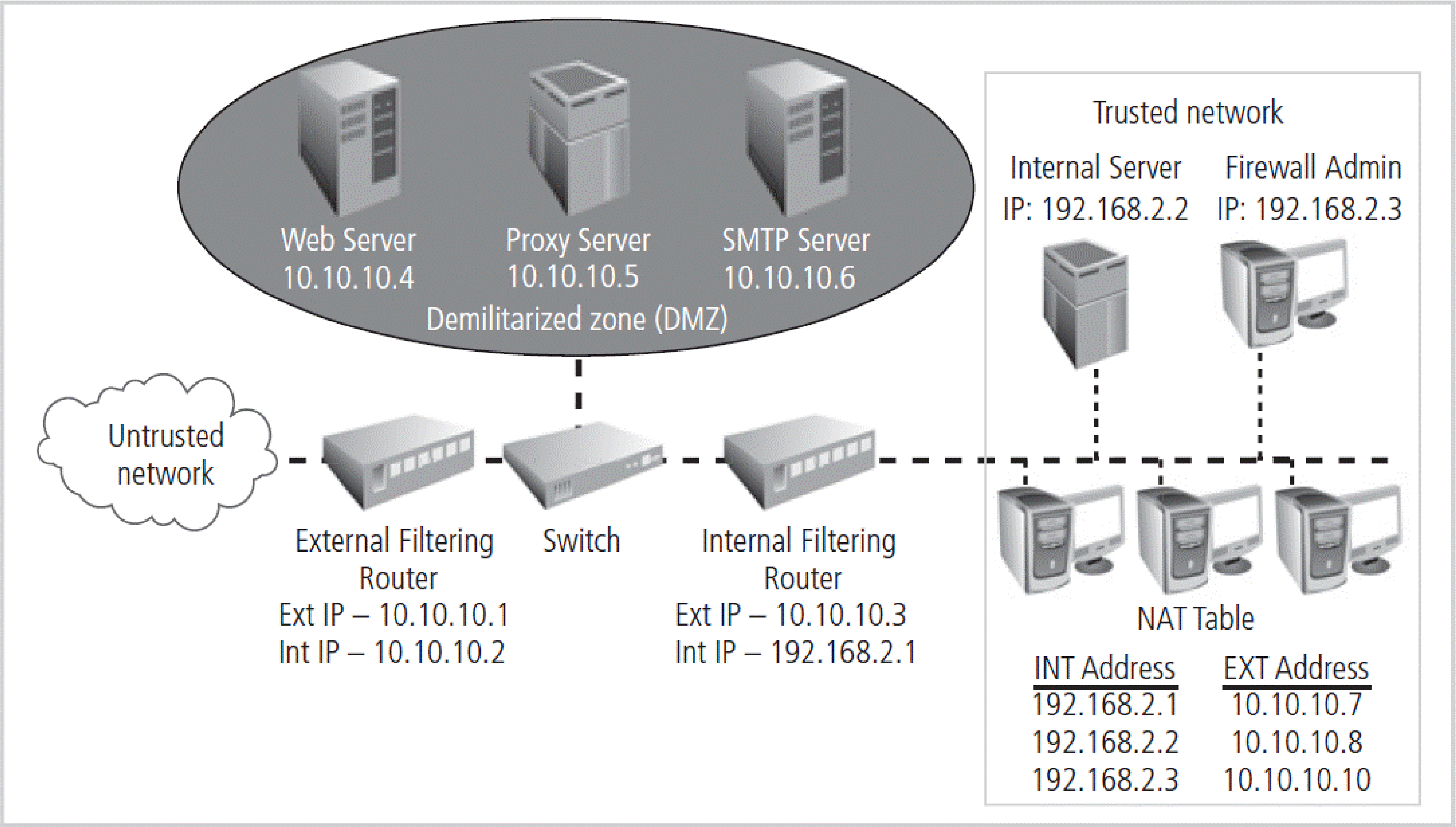


**Figure 6-18** Screened subnet (DMZ)



| INT Address | EXT Address |
|---|---|
| 192.168.2.1 | 10.10.10.7 |
| 192.168.2.2 | 10.10.10.8 |
| 192.168.2.3 | 10.10.10.10 |

**Figure 6-19** Example network configuration

# Firewall Architectures (cont’d)

- Screened subnet performs two functions:
  - Protects DMZ systems and information from outside threats
  - Protects the internal networks by limiting how external connections can gain access to internal systems
- Another facet of DMZs: extranets

# Firewall Architectures (cont'd)

- SOCKS servers
  - SOCKS is the protocol for handling TCP traffic via a proxy server.
  - A proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation
  - A SOCKS system can require support and management resources beyond those of traditional firewalls.

# Selecting the Right Firewall

- When selecting the firewall, consider a number of factors:
  - What firewall technology offers right balance between protection and cost for the needs of organization?
  - Which features are included in the base price and which are not?
  - Ease of setup and configuration? How accessible are staff technicians who can configure the firewall?
  - Can firewall adapt to organization’s growing network?
- Second most important issue is cost.

# Configuring and Managing Firewalls

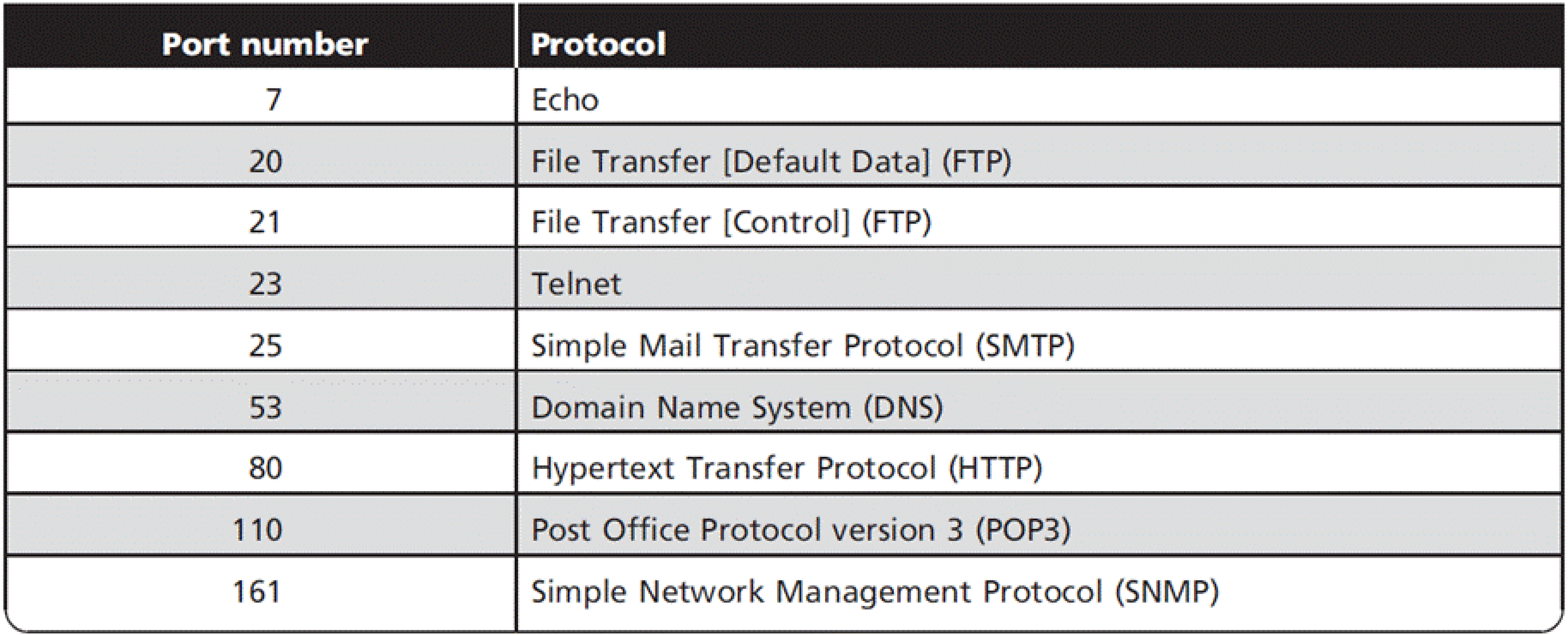
- The organization must provide for the initial configuration and ongoing management of firewall(s).
- Each firewall device must have its own set of configuration rules regulating its actions.
- Firewall policy configuration is usually complex and difficult.
- Configuring firewall policies is both an art and a science .
- When security rules conflict with the performance of business, security often loses.

# Configuring and Managing Firewalls (cont'd)

- Best practices for firewalls
  - All traffic from the trusted network is allowed out.
  - Firewall device is never directly accessed from public network.
  - Simple Mail Transport Protocol (SMTP) data are allowed to pass through firewall.
  - Internet Control Message Protocol (ICMP) data are denied
  - Telnet access to internal servers should be blocked.
  - When Web services are offered outside the firewall, HTTP traffic should be blocked from reaching internal networks.
  - All data not verifiably authentic should be denied.

# Configuring and Managing Firewalls (cont'd)

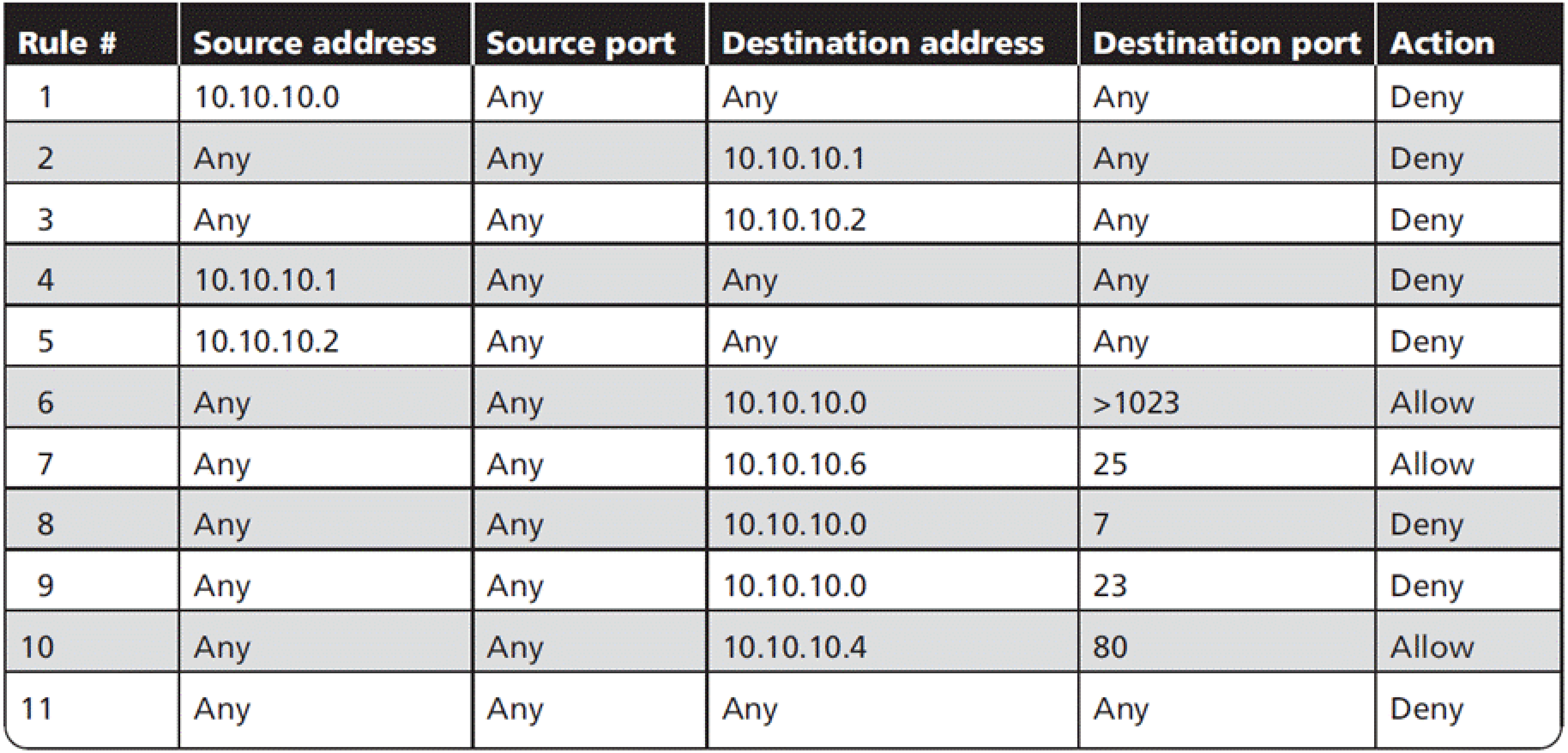
- Firewall rules
  - Firewalls operate by examining data packets and performing comparison with predetermined logical rules.
  - The logic is based on a set of guidelines most commonly referred to as firewall rules, rule base, or firewall logic.
  - Most firewalls use packet header information to determine whether specific packet should be allowed or denied.



| Port number | Protocol |
|---|---|
| 7 | Echo |
| 20 | File Transfer [Default Data] (FTP) |
| 21 | File Transfer [Control] (FTP) |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 53 | Domain Name System (DNS) |
| 80 | Hypertext Transfer Protocol (HTTP) |
| 110 | Post Office Protocol version 3 (POP3) |
| 161 | Simple Network Management Protocol (SNMP) |

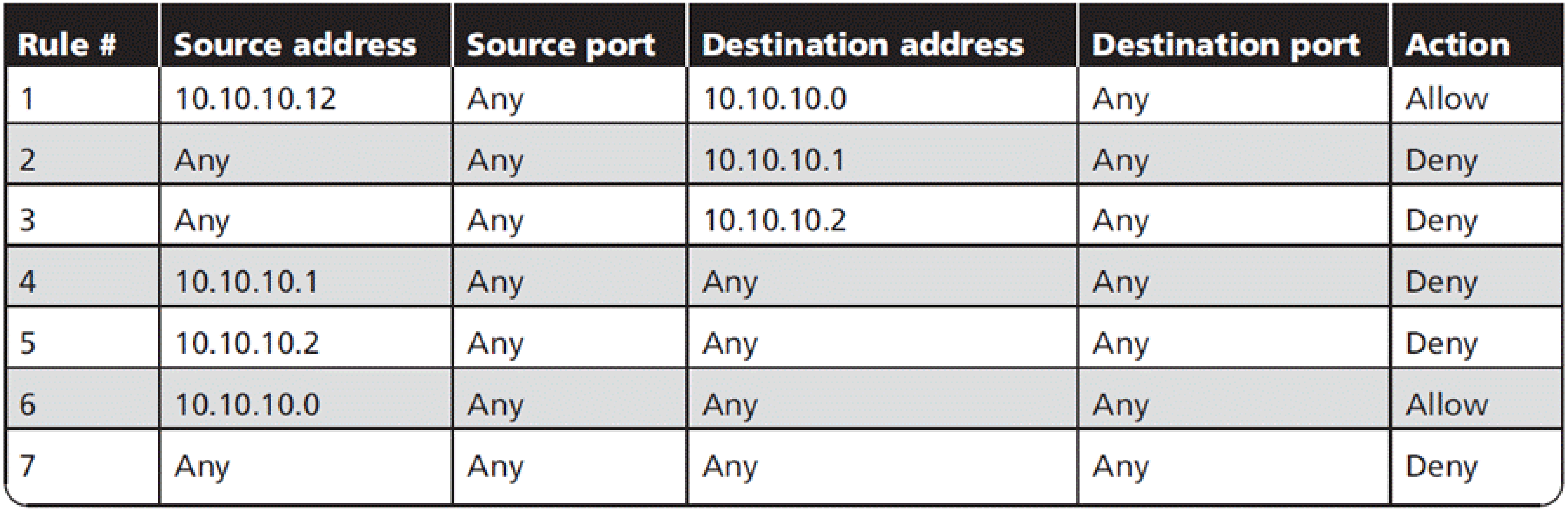
**Table 6-5 Well-Known Port Numbers**

© Cengage Learning 2015



| Rule # | Source address | Source port | Destination address | Destination port | Action |
|---|---|---|---|---|---|
| 1 | 10.10.10.0 | Any | Any | Any | Deny |
| 2 | Any | Any | 10.10.10.1 | Any | Deny |
| 3 | Any | Any | 10.10.10.2 | Any | Deny |
| 4 | 10.10.10.1 | Any | Any | Any | Deny |
| 5 | 10.10.10.2 | Any | Any | Any | Deny |
| 6 | Any | Any | 10.10.10.0 | >1023 | Allow |
| 7 | Any | Any | 10.10.10.6 | 25 | Allow |
| 8 | Any | Any | 10.10.10.0 | 7 | Deny |
| 9 | Any | Any | 10.10.10.0 | 23 | Deny |
| 10 | Any | Any | 10.10.10.4 | 80 | Allow |
| 11 | Any | Any | Any | Any | Deny |

**Table 6-16** **External Filtering Firewall Inbound Interface Rule Set**



| Rule # | Source address | Source port | Destination address | Destination port | Action |
|---|---|---|---|---|---|
| 1 | 10.10.10.12 | Any | 10.10.10.0 | Any | Allow |
| 2 | Any | Any | 10.10.10.1 | Any | Deny |
| 3 | Any | Any | 10.10.10.2 | Any | Deny |
| 4 | 10.10.10.1 | Any | Any | Any | Deny |
| 5 | 10.10.10.2 | Any | Any | Any | Deny |
| 6 | 10.10.10.0 | Any | Any | Any | Allow |
| 7 | Any | Any | Any | Any | Deny |

**Table 6-17** **External Filtering Firewall Outbound Interface Rule Set**

# Content Filters

- Software filter—not a firewall—that allows administrators to restrict content access from within a network
- Essentially a set of scripts or programs restricting user access to certain networking protocols/Internet locations
- Primary purpose to restrict internal access to external material
- Most common content filters restrict users from accessing non-business Web sites or deny incoming spam.

# Protecting Remote Connections

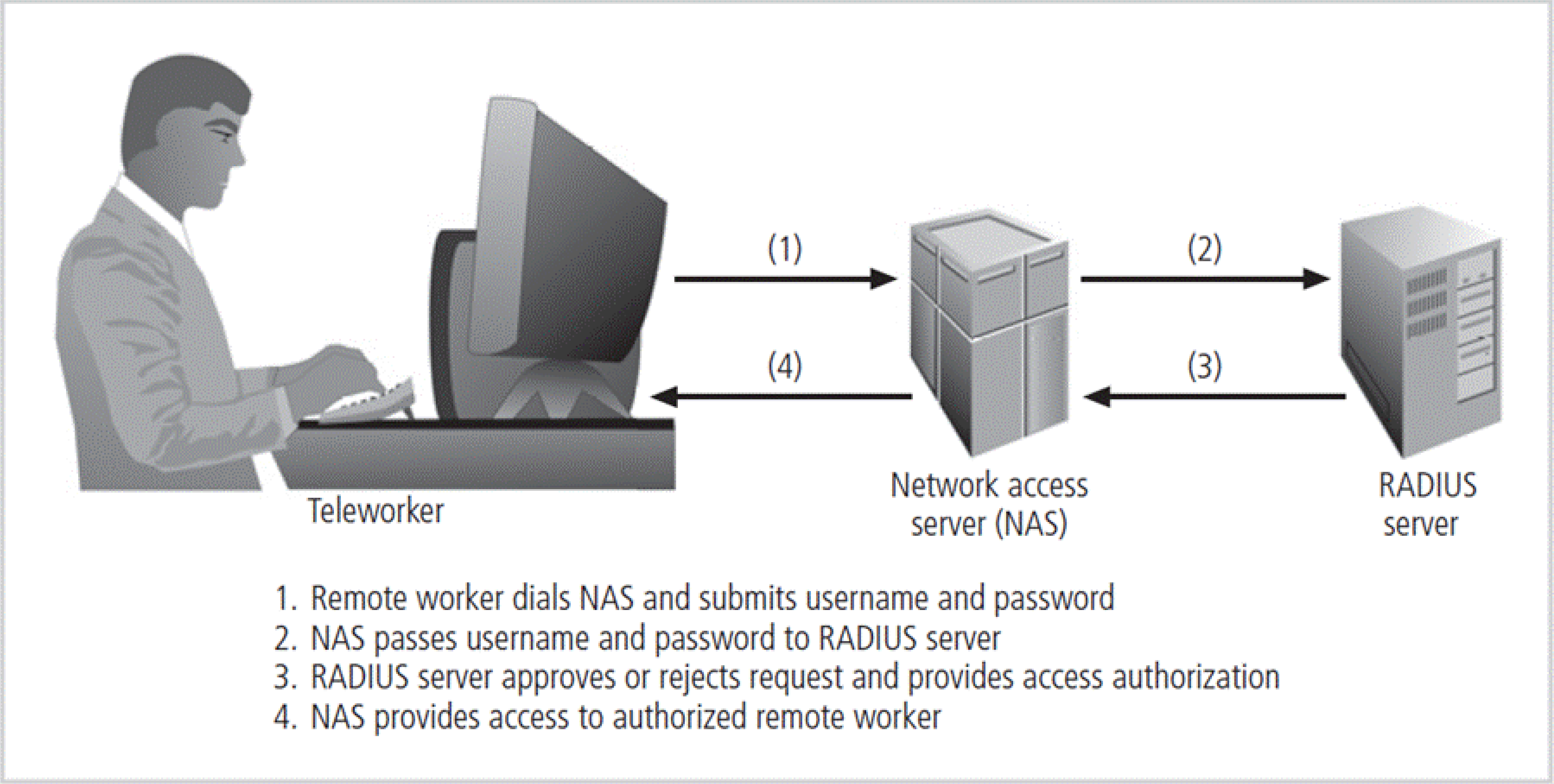
- Installing Internetwork connections requires leased lines or other data channels; these connections are usually secured under the requirements of a formal service agreement.
- When individuals seek to connect to an organization's network, a more flexible option must be provided.
- Options such as virtual private networks (VPNs) have become more popular due to the spread of Internet.

# Remote Access

- Unsecured, dial-up connection points represent a substantial exposure to attack.
- Attacker can use a device called a war dialer to locate the connection points.
- War dialer: automatic phone-dialing program that dials every number in a configured range and records number if modem picks up
- Some technologies (RADIUS systems; TACACS; CHAP password systems) have improved the authentication process.

# Remote Access (cont'd)

- RADIUS, Diameter, and TACACS
  - Systems that authenticate user credentials for those trying to access an organization's network via dial-up
  - Remote Authentication Dial-In User Service (RADIUS): centralizes responsibility for user authentication in a central RADIUS server
  - Diameter: emerging alternative derived from RADIUS
  - Terminal Access Controller Access Control System (TACACS): validates user's credentials at centralized server (like RADIUS); based on client/server configuration



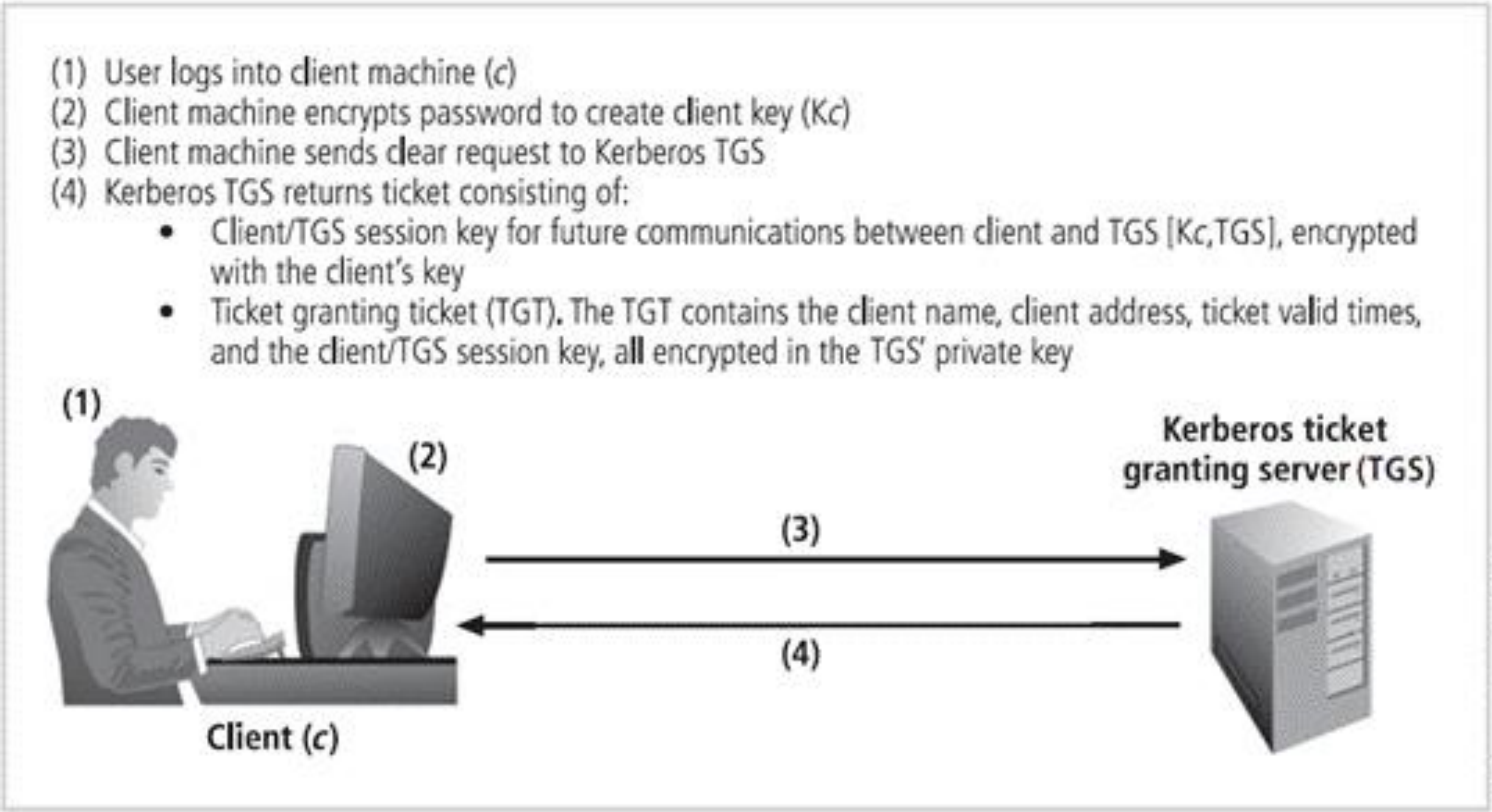
1. Remote worker dials NAS and submits username and password
2. NAS passes username and password to RADIUS server
3. RADIUS server approves or rejects request and provides access authorization
4. NAS provides access to authorized remote worker

© Cengage Learning 2015

**Figure 6-20** RADIUS configuration

# Remote Access (cont'd)

- Kerberos
  - Provides secure third-party authentication
  - Uses symmetric key encryption to validate individual user to various network resources
  - Keeps database containing private keys of clients/servers
  - Consists of three interacting services:
    - Authentication server (AS)
    - Key Distribution Center (KDC)
    - Kerberos ticket granting service (TGS)

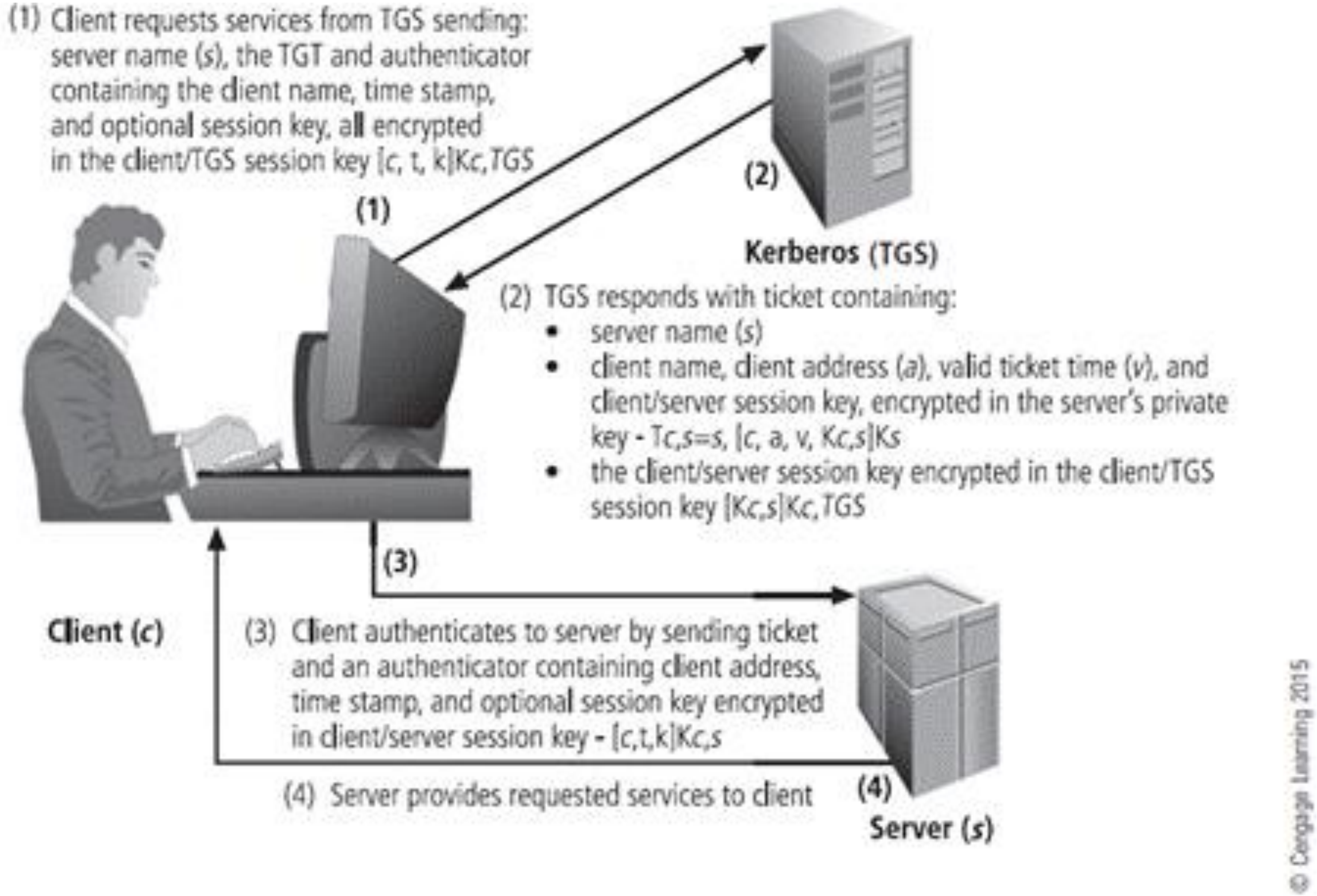


(1) User logs into client machine (*c*)
(2) Client machine encrypts password to create client key (K*c*)
(3) Client machine sends clear request to Kerberos TGS
(4) Kerberos TGS returns ticket consisting of:

- Client/TGS session key for future communications between client and TGS [K*c*,TGS], encrypted with the client's key
- Ticket granting ticket (TGT). The TGT contains the client name, client address, ticket valid times, and the client/TGS session key, all encrypted in the TGS' private key

© Cengage Learning 2015

**Figure 6-21** Kerberos login



(1) Client requests services from TGS sending: server name (*s*), the TGT and authenticator containing the client name, time stamp, and optional session key, all encrypted in the client/TGS session key [*c*, t, k]K*c*,*TGS*

(2) TGS responds with ticket containing:

- server name (*s*)
- client name, client address (*a*), valid ticket time (*v*), and client/server session key, encrypted in the server's private key - T*c*,*s*=*s*, [*c*, a, v, K*c*,*s*]K*s*
- the client/server session key encrypted in the client/TGS session key [K*c*,*s*]K*c*,*TGS*

(3) Client authenticates to server by sending ticket and an authenticator containing client address, time stamp, and optional session key encrypted in client/server session key - [*c*,t,k]K*c*,*s*

(4) Server provides requested services to client

© Cengage Learning 2015

**Figure 6-22** Kerberos request for services

# Remote Access (cont'd)

- SESAME
  - Secure European System for Applications in a Multivendor Environment (SESAME) is similar to Kerberos.
    - User is first authenticated to authentication server and receives token.
    - Token is then presented to a privilege attribute server as proof of identity to gain privilege attribute certificate.
    - Uses public key encryption; adds sophisticated access control features; more scalable encryption systems; improved manageability; auditing features; and options for delegation of responsibility for allowing access

# Virtual Private Networks (VPNs)

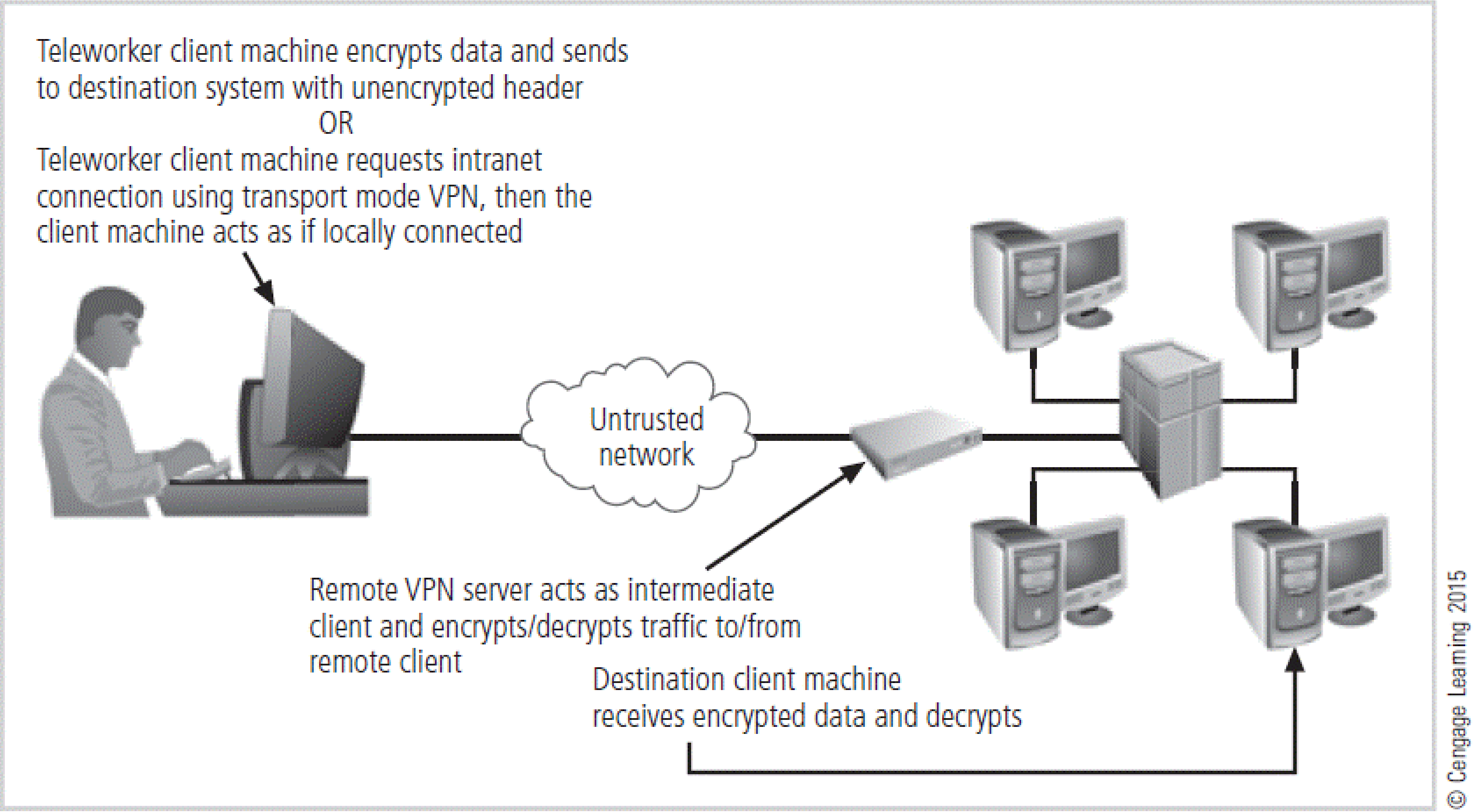
- Private and secure network connection between systems; uses data communication capability of unsecured and public network
- Securely extends organization's internal network connections to remote locations
- Three VPN technologies defined:
  - Trusted VPN
  - Secure VPN
  - Hybrid VPN (combines trusted and secure)

# Virtual Private Networks (VPNs) (cont'd)

- VPN must accomplish:
  - Encapsulation of incoming and outgoing data
  - Encryption of incoming and outgoing data
  - Authentication of remote computer and perhaps remote user as well
- In most common implementation, it allows the user to turn Internet into a private network.

# Virtual Private Networks (VPNs) (cont’d)

- Transport mode
  - Data within IP packet is encrypted, but header information is not.
  - Allows user to establish secure link directly with remote host, encrypting only data contents of packet
  - Two popular uses:
    - End-to-end transport of encrypted data
    - Remote access worker connects to office network over Internet by connecting to a VPN server on the perimeter.



Teleworker client machine encrypts data and sends to destination system with unencrypted header

OR

Teleworker client machine requests intranet connection using transport mode VPN, then the client machine acts as if locally connected

Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client

Destination client machine receives encrypted data and decrypts

© Cengage Learning 2015

**Figure 6-23** Transport mode VPN

# Virtual Private Networks (VPNs) (cont'd)

- Tunnel mode
  - Establishes two perimeter tunnel servers to encrypt all traffic that will traverse unsecured network
  - Entire client package encrypted and added as data portion of packet from one tunneling server to another
  - Primary benefit to this model is that an intercepted packet reveals nothing about the true destination system.
  - Example of tunnel mode VPN: Microsoft's Internet Security and Acceleration (ISA) Server

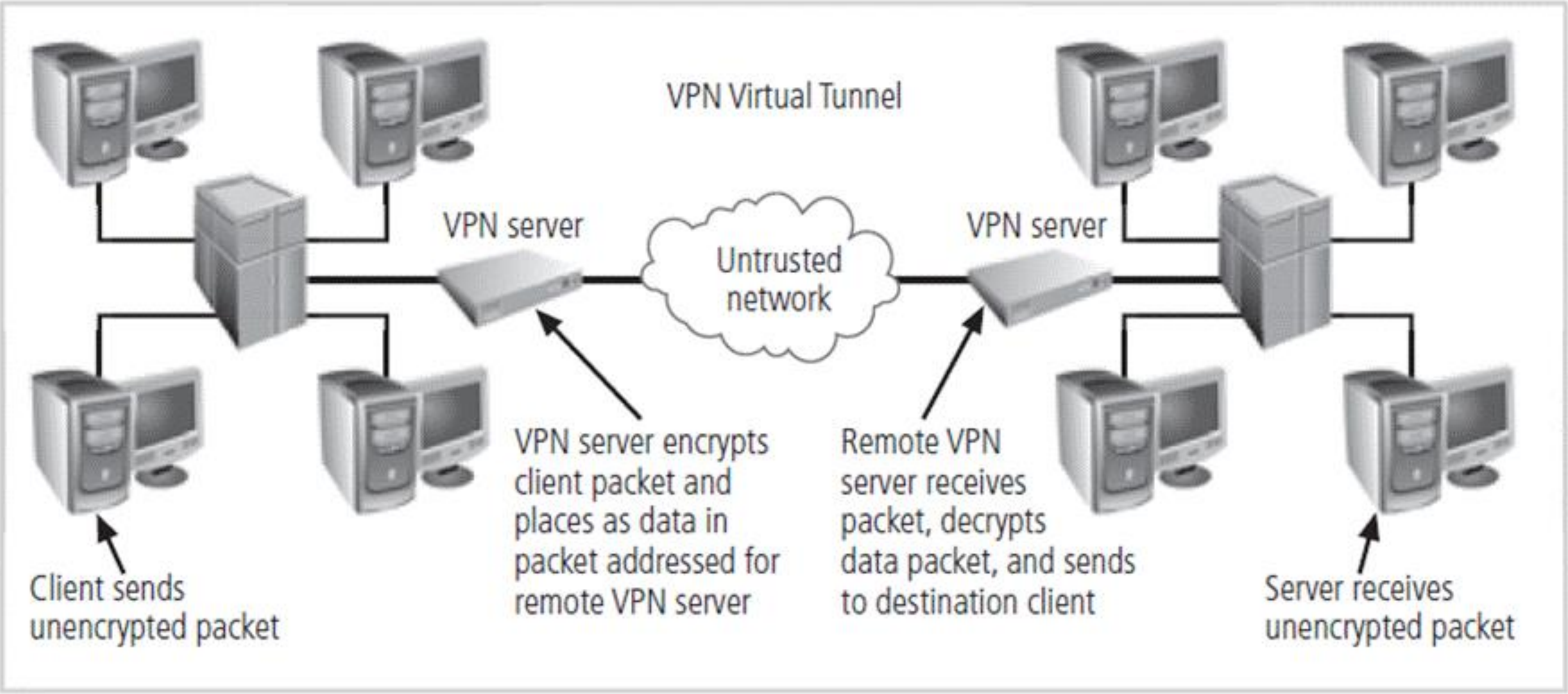

VPN Virtual Tunnel
VPN server
Untrusted network
VPN server
VPN server encrypts client packet and places as data in packet addressed for remote VPN server
Remote VPN server receives packet, decrypts data packet, and sends to destination client
Client sends unencrypted packet
Server receives unencrypted packet

**Figure 6-24** Tunnel mode VPN

# Summary

- Firewall technology
- Various approaches to remote and dial-up access protection
- Content filtering technology
- Virtual private networks