COURSE TECHNOLOGY
CENGAGE Learning™

Guide to Network Security
First Edition

Chapter Five

Network Authentication and Remote Access Using VPN

Objectives

- Define access control and identify the various ways it can be implemented
- Explain why authentication is a critical aspect of network access control
- Identify the component parts of virtual private networks (VPNs)
- List and define the essential activities that an VPN must be able to perform
- Explain the various VPN architectures in common use

Introduction

- Network security strategies authenticate machines:
  - Rather than individuals
- Stronger level of authentication
  - Network Access Control (NAC)
  - VPN access controllers
- Main types of authentication performed by network security devices
  - Client
  - User
  - Session

Access Control

- Access controls regulate admission into trusted areas of the organization
  - Logical access to information systems
  - Physical access to facilities
- Made up of policies, programs, and technologies
- Processes
  - Identification
  - Authentication
  - Authorization
  - Accountability

Access Control (cont'd.)

- Key principles of access control
  - Least privilege
    - Members allowed minimal amount of information necessary to perform required duties
  - Need to know
    - Limits user's access to specific information required for a task
  - Separation of duties
    - Tasks are divided between two or more individuals

Categories of Access Control

- Functional characteristics
  - Deterrent
  - Preventative
  - Detective
  - Corrective
  - Recovery
  - Compensating

Categories of Access Control (cont'd.)

- NIST SP800-12 classification
  - Management
  - Operational
  - Technical
- Mandatory access controls
  - Controls enforced by computer system without intervention from the data owner

	Deterrent	Preventative	Detective	Corrective	Recovery	Compensating
Management	Policies	Registration procedures	Periodic violation report reviews	Employee or account termination	Disaster recovery plan	Separation of duties, job rotation
Operational	Warning signs	Gates, fences, and guards	Sentries, CCTVs	Fire suppression systems	Disaster recovery procedures	Defense in depth
Technical	Warning banners	Login systems, Kerberos	Log monitors and IDPSs	Forensics procedures	Data backups	Key logging and keystroke monitoring

Table 5-1 Examples of controls categorized by operational level and functional characteristics

Categories of Access Control (cont'd.)

- U.S. Military classification scheme
  - Unclassified
  - Sensitive but unclassified
  - Confidential
  - Secret
  - Top Secret
- Discretionary access controls
  - Implemented at the discretion of the data owner

	Finance Shared Files	HR Shared Files	IT Shared Files	Legal Shared Files	Manufacturing Shared Files
John	r	rwx		r	
Stephanie			rwx		r
Steve					rwx
Jennifer	r	r		rwx	
Todd	rwx	r			

Access Legend:
r = Read
w = Write
x = Execute

Figure 5-1 Sample access control matrix
© *Cengage Learning 2013*

Categories of Access Control (cont'd.)

- Nondiscretionary controls
  - Determined by a central authority
  - Can be either role-based or task-based
- Other forms of access control
  - Content-dependent
  - Constrained user interfaces
  - Temporal (time-based) isolation

Identification

- Process by which a computer system recognizes a user's identity
- Accounts are stored locally or centralized
- Default accounts
  - Operating systems have a default user account
    - Root (UNIX) or administrator (Windows)
  - Default accounts should be renamed to make more difficult to access

Identification (cont'd.)

- Periodic reviews
  - Performed by network administrators
  - Ensure employee still works at the company
  - Determine if employee still requires an account

Authentication

- Act of confirming the identity or user account
- User proposes and verifies an identity with some combination of:
  - Something you know
    - Password or passphrase
  - Something you have
    - Smart card or key
  - Something you are
    - Fingerprint, iris scan, or voiceprint

Password Security Issues

- Cracking
  - Guessing, breaking, or stealing passwords to gain system access
  - Methods: dictionary and brute force attacks
- Rainbow tables
  - Contain hash outputs for many different password combinations
- Password policies
  - Guidelines to help enforce password confidentiality

Password Security Issues (cont'd.)

- Example of a password policy
  - At least eight characters
  - Contain at least one uppercase character
  - Contain at least one lowercase character
  - Contain at least one number and symbol
  - Contain no part of the user's name
  - Contain no words commonly found in a dictionary
  - Contain no repeating characters
  - Be combined with a salt when calculating hashes

Password Security Issues (cont'd.)

- Example of password policy restrictions
  - Users must change passwords at least every 90 days
  - Remember 10 or more previously used passwords
  - Lock accounts after three to five invalid login attempts
- Lax security practices to avoid
  - Using simple passwords
  - Storing passwords on paper in readily visible areas
  - Sharing passwords between systems or with others

Password Security Issues (cont'd.)

- One-time password software
  - Password generated for one-time use during a single session
  - Challenge-response passwords
  - Password list passwords
  - Token generators

Implementing Authentication

- Most operating systems equipped with authentication schemes
- Firewalls and VPN access controllers can perform user authentication
- General process to authenticate users
  - Client requests access to a resource
  - Firewall prompts for username and password
  - User submits information and is authenticated
  - Request is checked against firewall's rule base
  - Request is granted or denied

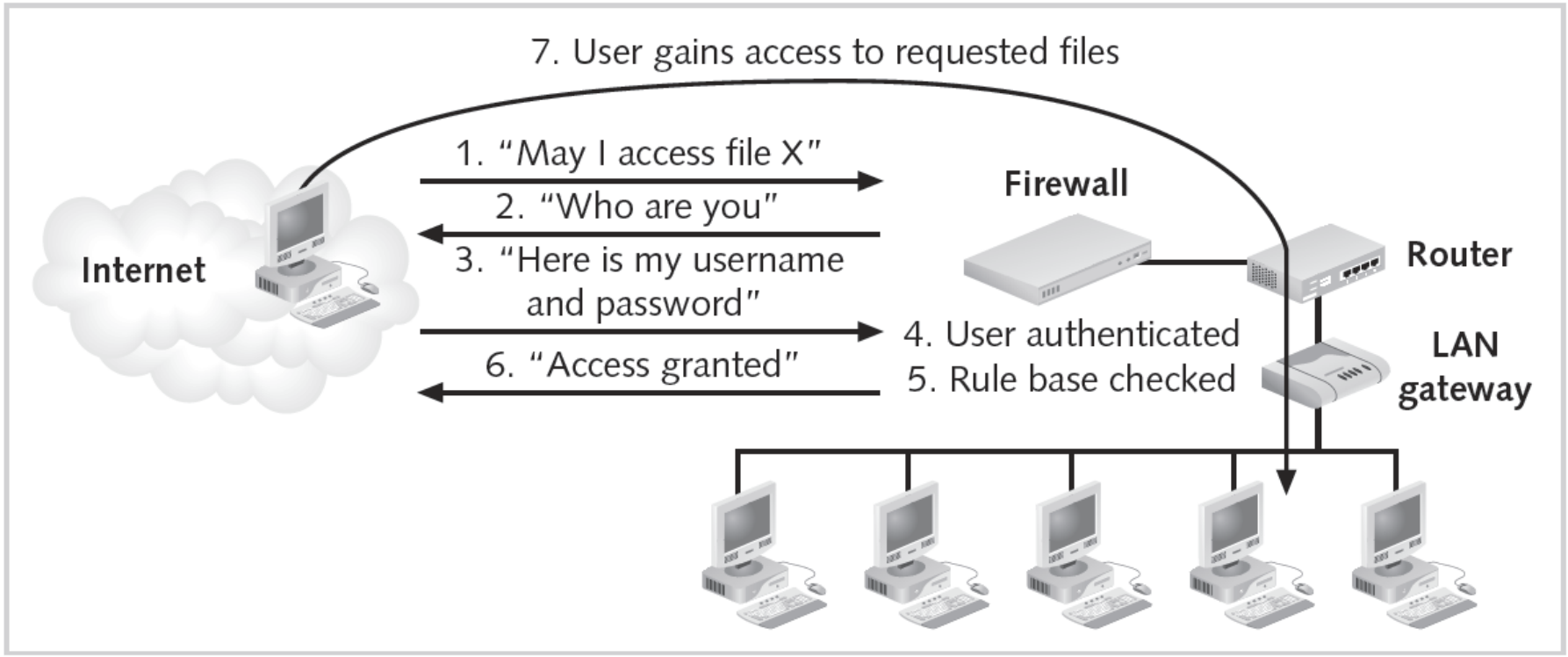

Figure 5-2 Basic user authentication

Implementing Authentication (cont'd.)

- User authentication
  - Simplest type
  - Authorized users added to access control lists
- Client authentication
  - Similar to user authentication
  - Includes usage limits
  - Specific period of time or number of times
  - Standard or specific sign-on is used

Implementing Authentication (cont'd.)

- Network access control (NAC)
  - Before a device may communicate on the network
    - Must meet specific thresholds
  - Device has authorized user credentials needed to access network
  - Device must have appropriate security tools and up-to-date software versions
  - Device has correct system configuration
  - Device complies with security standards

Implementing Authentication (cont'd.)

- Session authentication
  - Requires authentication whenever client system attempts connection
  - A session is established
- Some advanced firewalls:
  - Offer multiple authentication methods

Method	Use When...
User Authentication	• You want to scan the content of IP packets. • The protocol in use is HTTP, HTTPS, FTP rlogin, or Telnet. • You need to authenticate for each session separately.
Client Authentication	• The user to be authenticated will use a specific IP address. • The protocol in use is not HTTP, HTTPS, FTP, rlogin, or Telnet. • You want a user to be authenticated for a specific length of time.
Session Authentication	• The individual user to be authenticated will come from a specific IP address. • The protocol in use is not HTTP, HTTPS, FTP, rlogin or Telnet. • You want a client to be authenticated for each session.

Table 5-2 Authentication methods

Implementing Authentication (cont'd.)

- Centralized authentication
  - Central server maintains all user authorizations
    - Also called authentication, authorization, and auditing (AAA) server
  - Can use several different authentication methods
    - See Figure 5-4 for Kerberos
    - See Tables 5-3 and 5-4 for TACACS+ and RADIUS

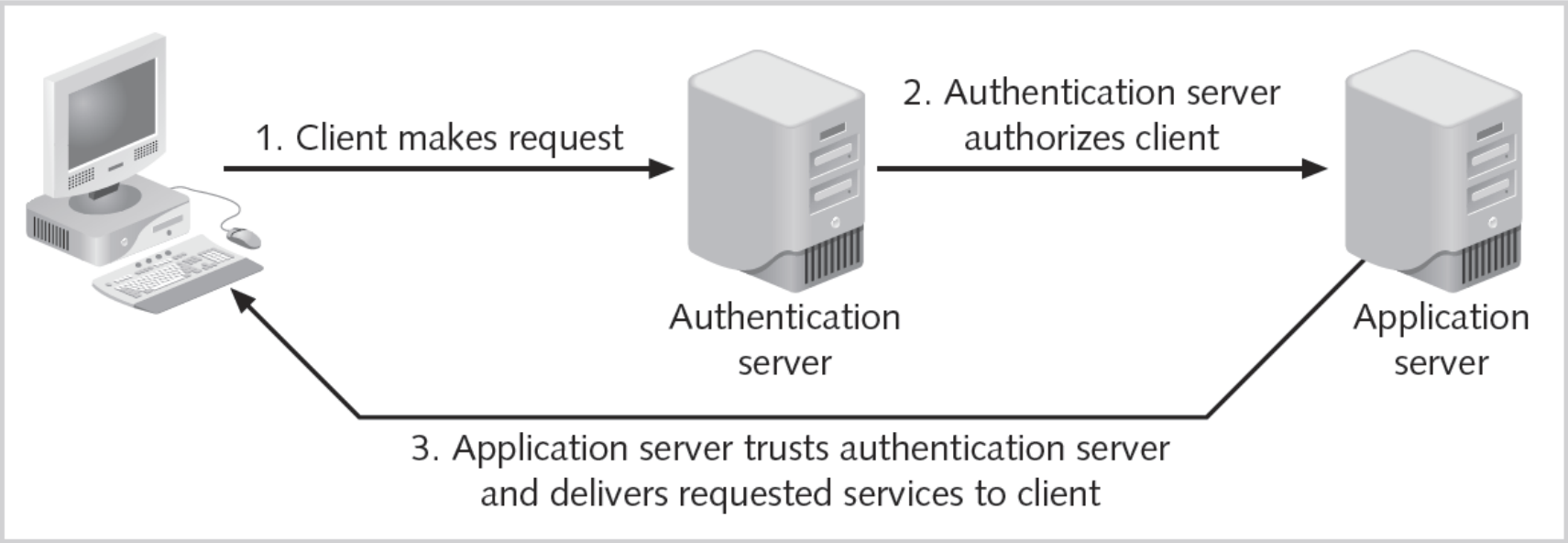

Figure 5-3 Centralized authentication
© *Cengage Learning 2013*

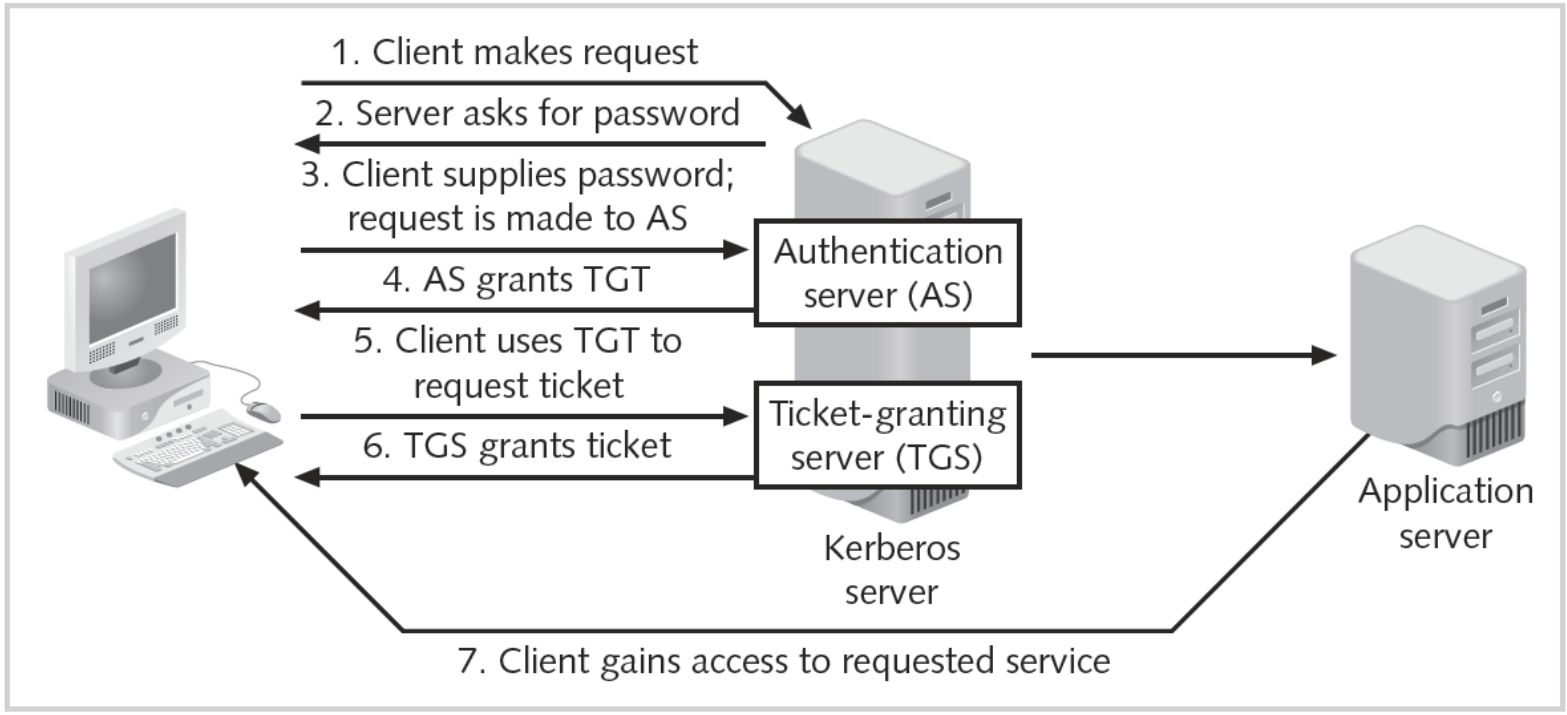

Figure 5-4 Kerberos authentication

TACACS+	RADIUS
Uses TCP	Uses UDP
Full packet encryption between client and server	Encrypts only passwords—other information is unencrypted
Independent authentication, authorization, and auditing	Combines authentication and authorization
Passwords in the database may be encrypted	Passwords in the database are in cleartext

Table 5-3 Characteristics of TACACS+ and RADIUS

Direction	Protocol	Source Port	Destination Port	Remarks
Inbound	TCP	All ports > 1023	49	Enables external client to connect to internal TACACS+ server
Outbound	TCP	49	All ports > 1023	Allows internal TACACS+ server to respond to external client
Inbound	UDP	All ports > 1023	1812	Allows external client to connect to internal RAIDIUS server
Outbound	UDP	1812	All ports > 1023	Allows internal RAIDIUS server to respond to external client
Inbound	UDP	All ports > 1023	1813	Enables auditing when external client connects to RADIUS server
Outbound	UDP	1813	All ports > 1023	Enables auditing when internal RADIUS server responds to a client

Table 5-4 Filtering rules for TACACS+ and RADIUS

Virtual Private Networks

- Connects remote workers
- Older technology
  - Dial-up connectivity
  - Leased lines
  - Remote Authentication Service
- Virtual private networks (VPNs)
  - Provide secure point-to-point communication over the public Internet
  - Data is encapsulated and encrypted

Extranets and Intranets

- Extranet
  - Extension of organization's network using the Internet
- Intranet
  - Logical network restricted to employees within the organization

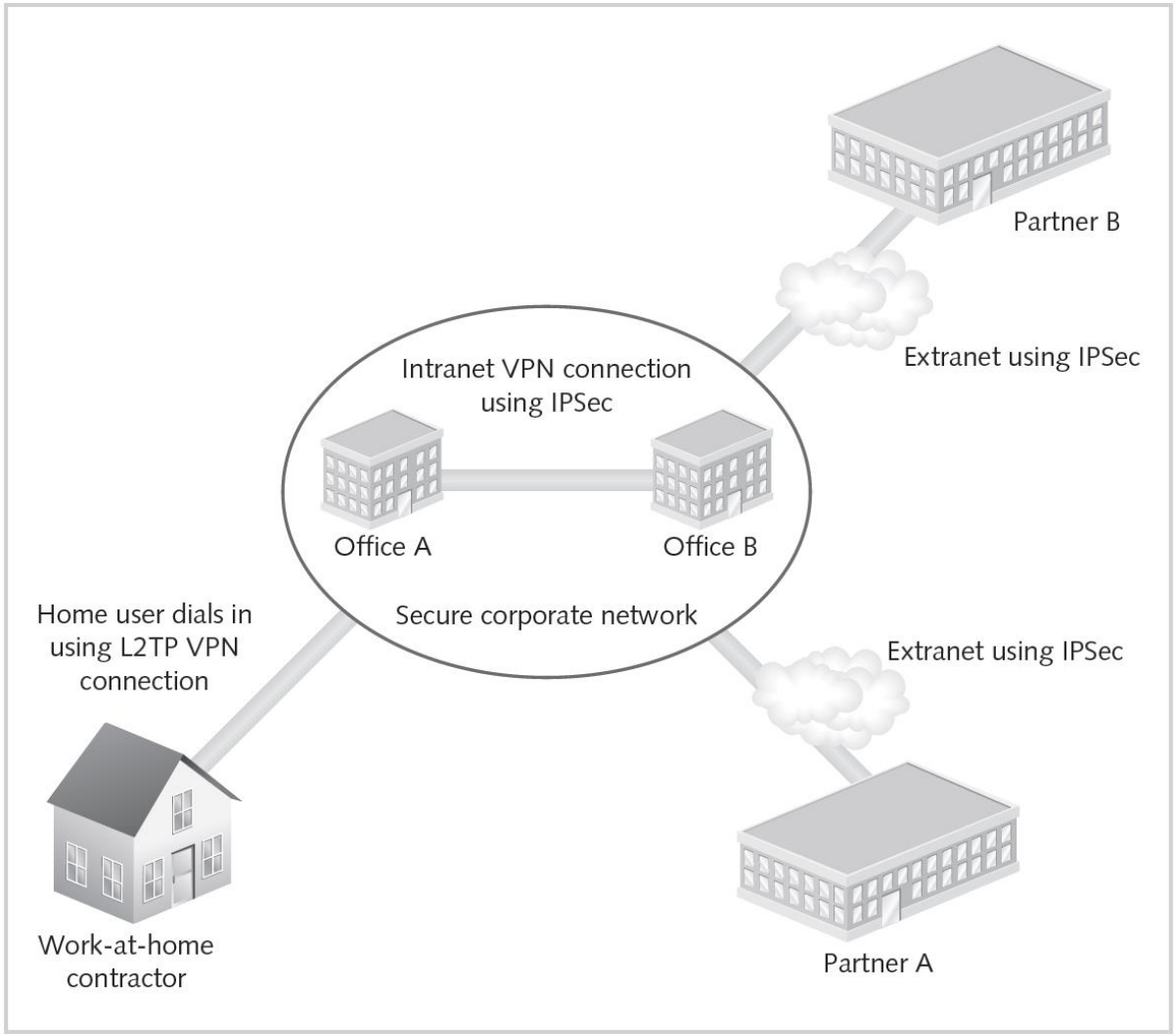

Figure 5-5 VPN for intranets and extranets
© Cengage Learning 2013

VPN Components and Operations

- Many telecommunications companies provide VPN services
- VPN components
  - Hardware devices
  - Software that performs security-related activities
- Endpoints or terminators
  - Hardware devices at each end
  - Perform encryption, authentication, and encapsulation

VPN Components and Operations (cont'd.)

- VPN tunnel
  - Virtual communications path
  - Uses TCP/IP
- See Figures 5-6, 5-7, and 5-8 for example VPN configurations

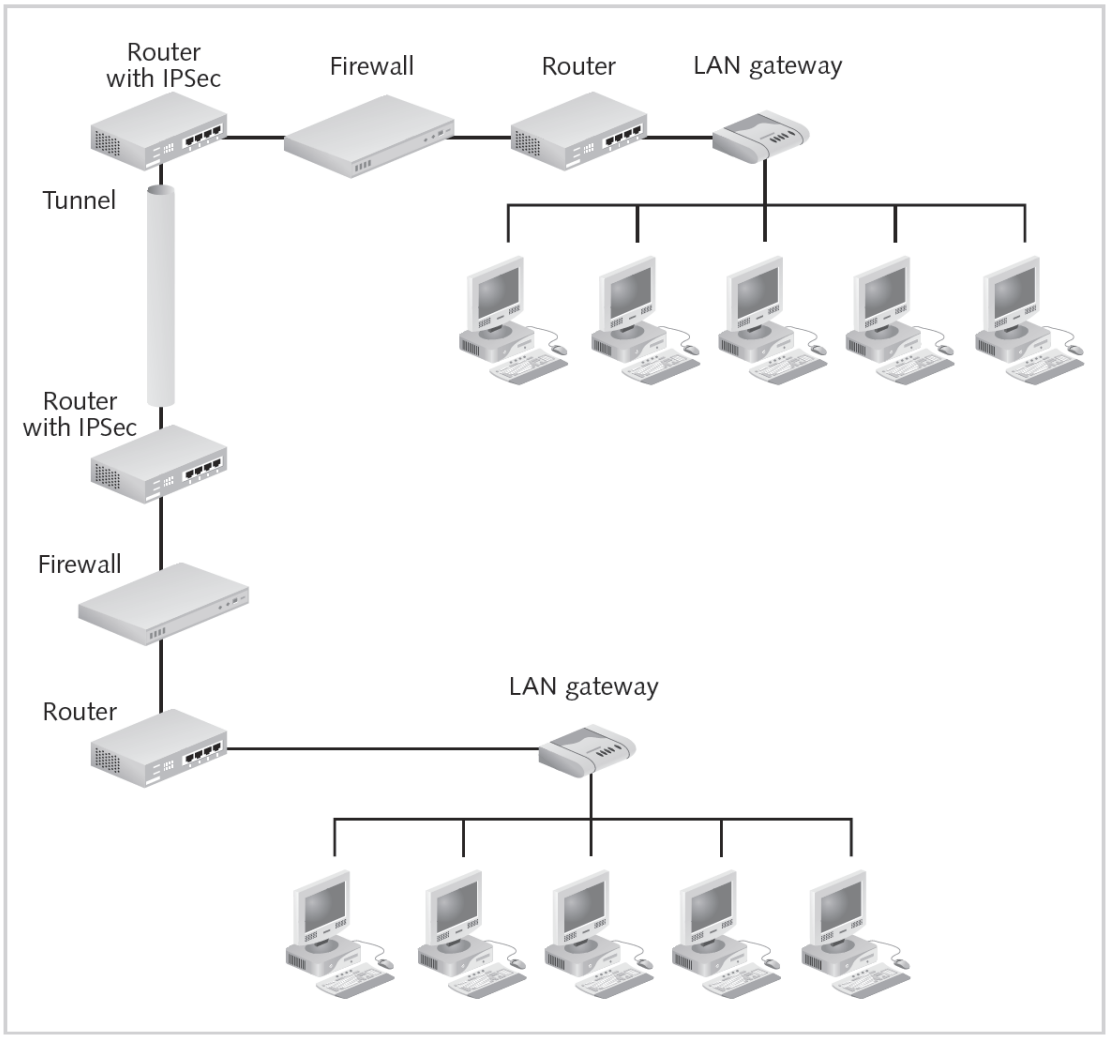

Figure 5-6 Simplified model VPN

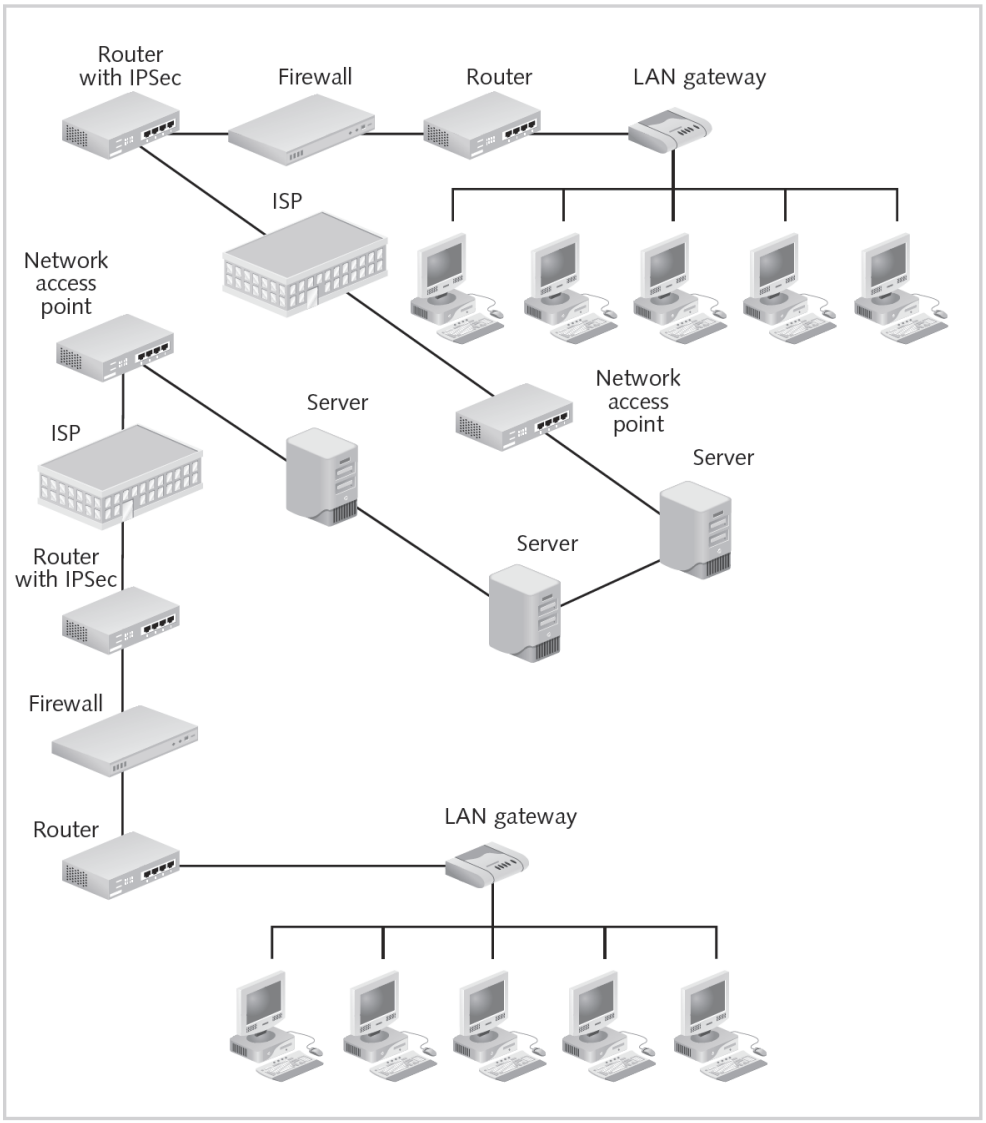

Figure 5-7 Model VPN

© Cengage Learning 2013

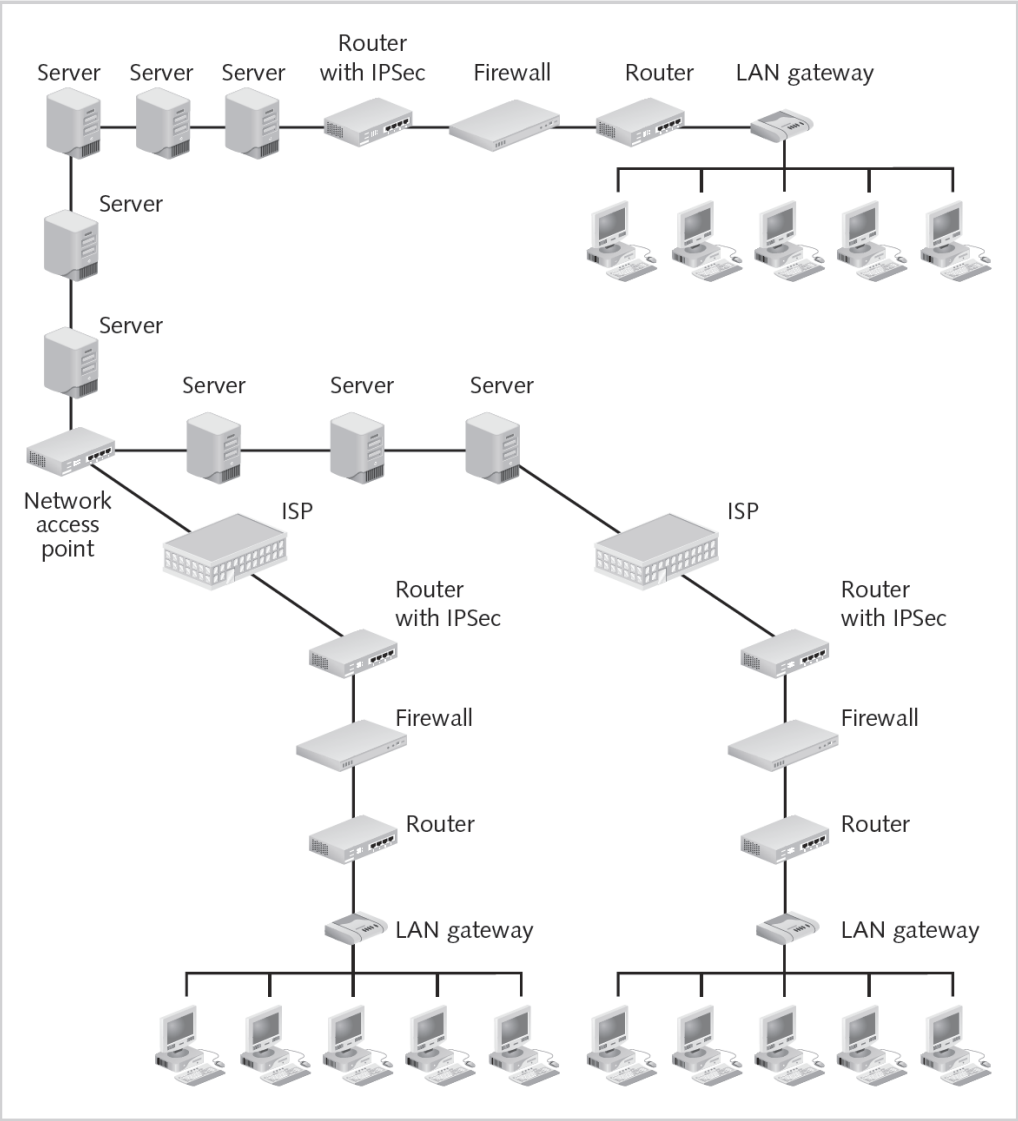

Figure 5-8 Common VPN

© Cengage Learning 2013

Essential Activities of VPNs

- IP encapsulation
  - Enclosing a packet within another packet
    - Different IP source and destination information
- Data payload encryption
  - Transport method encrypts traffic when generated
    - Data is encrypted, not header
  - Tunnel method encrypts data in transit
    - Both header and data portions encrypted

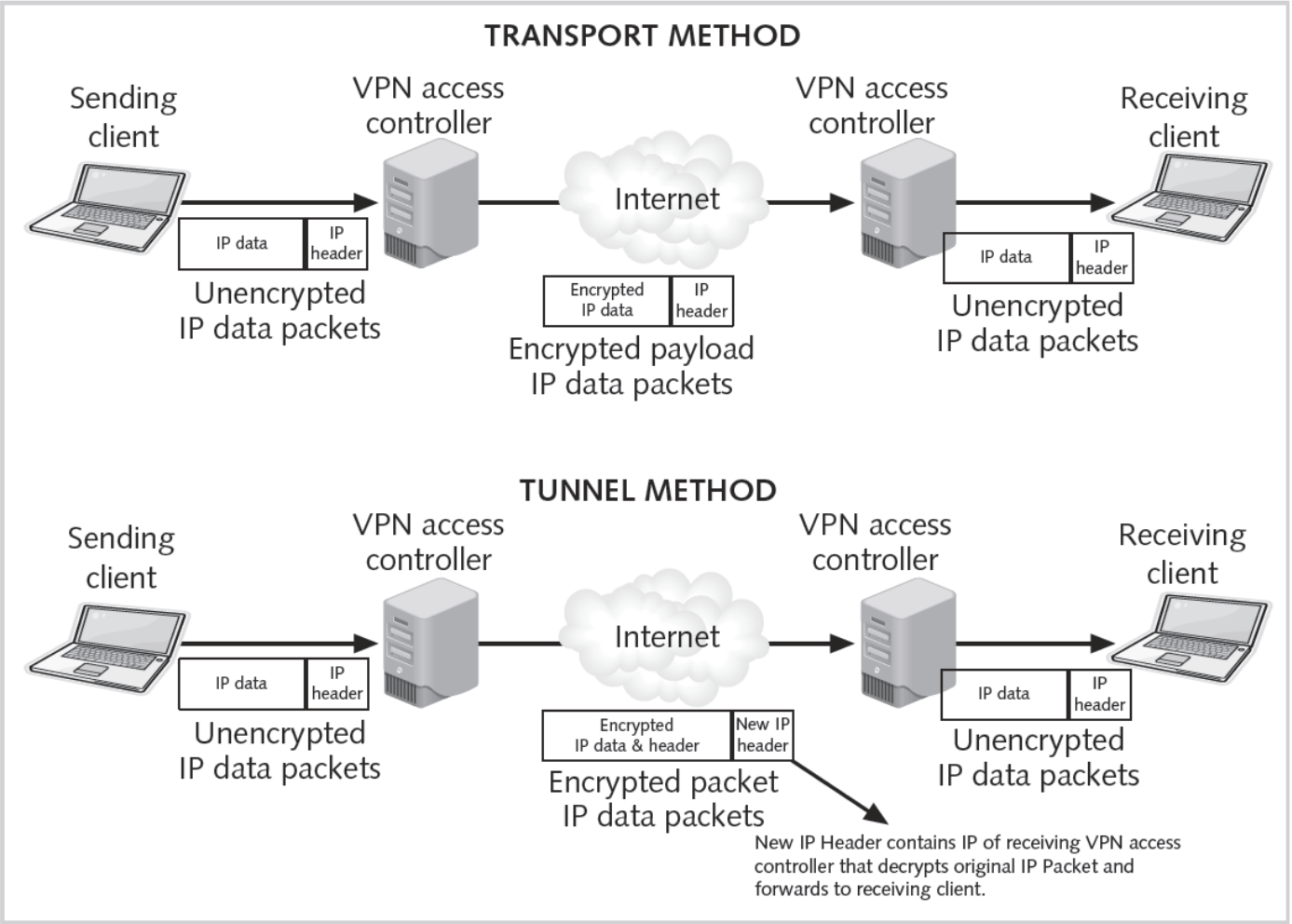

Figure 5-9 VPN IP encapsulation with transport encryption and tunnel encryption methods

© Cengage Learning 2013

Essential Activities of VPNs (cont'd.)

- Encrypted authentication
  - Encryption domain: everything in the protected network behind the gateway
  - Same cryptographic system that encrypts packets:
    - Authenticates computers using the VPN

Types of VPNs

- Site-to-site VPN
  - Links two or more networks
- Client-to-site VPN
  - Makes network accessible to remote users who need dial-in access
- Two types not mutually exclusive

VPN Appliances

- Hardware device designed to terminate VPNs
  - Permits connections among large number of users
  - Does not provide file sharing and printing
- Software VPN
  - Less expensive than hardware systems
  - More scalable on fast-growing networks
- VPN combinations of hardware and software
  - Implement a VPN appliance at the central network
  - Use client software at remote end of each connection

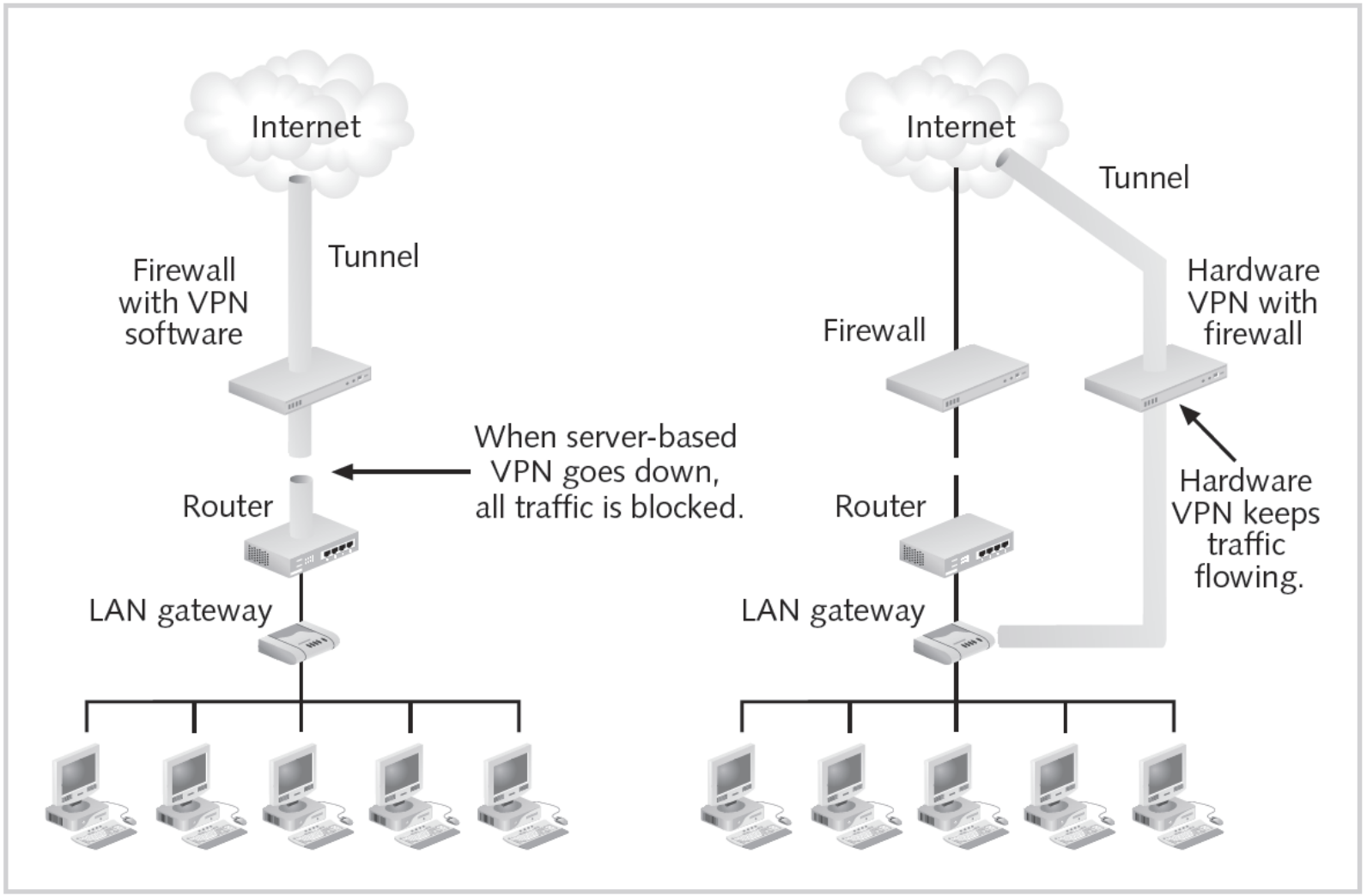

Figure 5-10 Hardware VPN

VPN Architectures

- Mesh configuration
  - Each participant in the VPN has an approved relationship with every other participant
    - Relationship called security association (SA)
- Hub-and-spoke configuration
  - Single VPN router contains records of all SAs in the VPN
  - All communication flows through central router
    - Router must have double the bandwidth of other connections

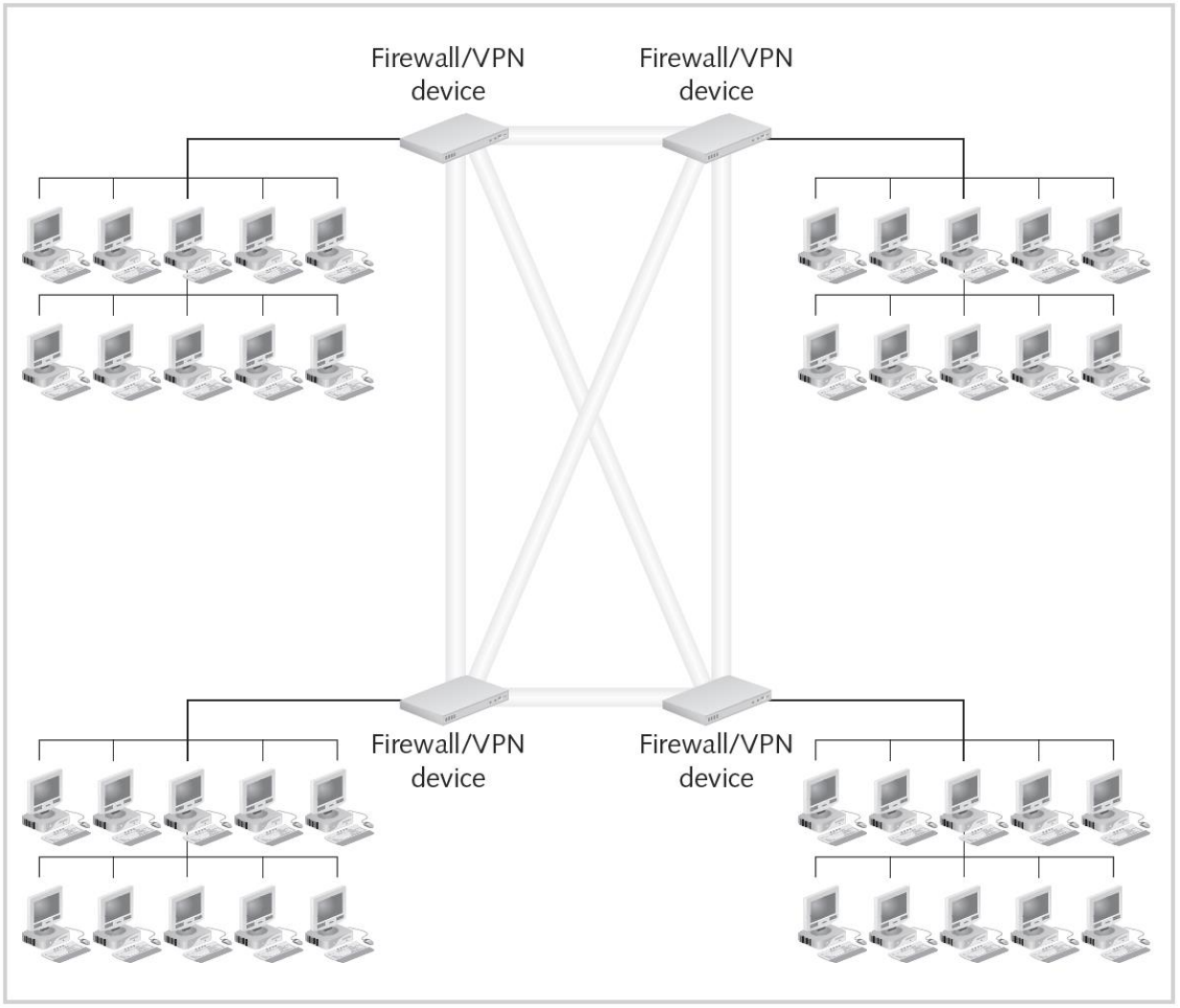

Figure 5-11 Mesh VPN

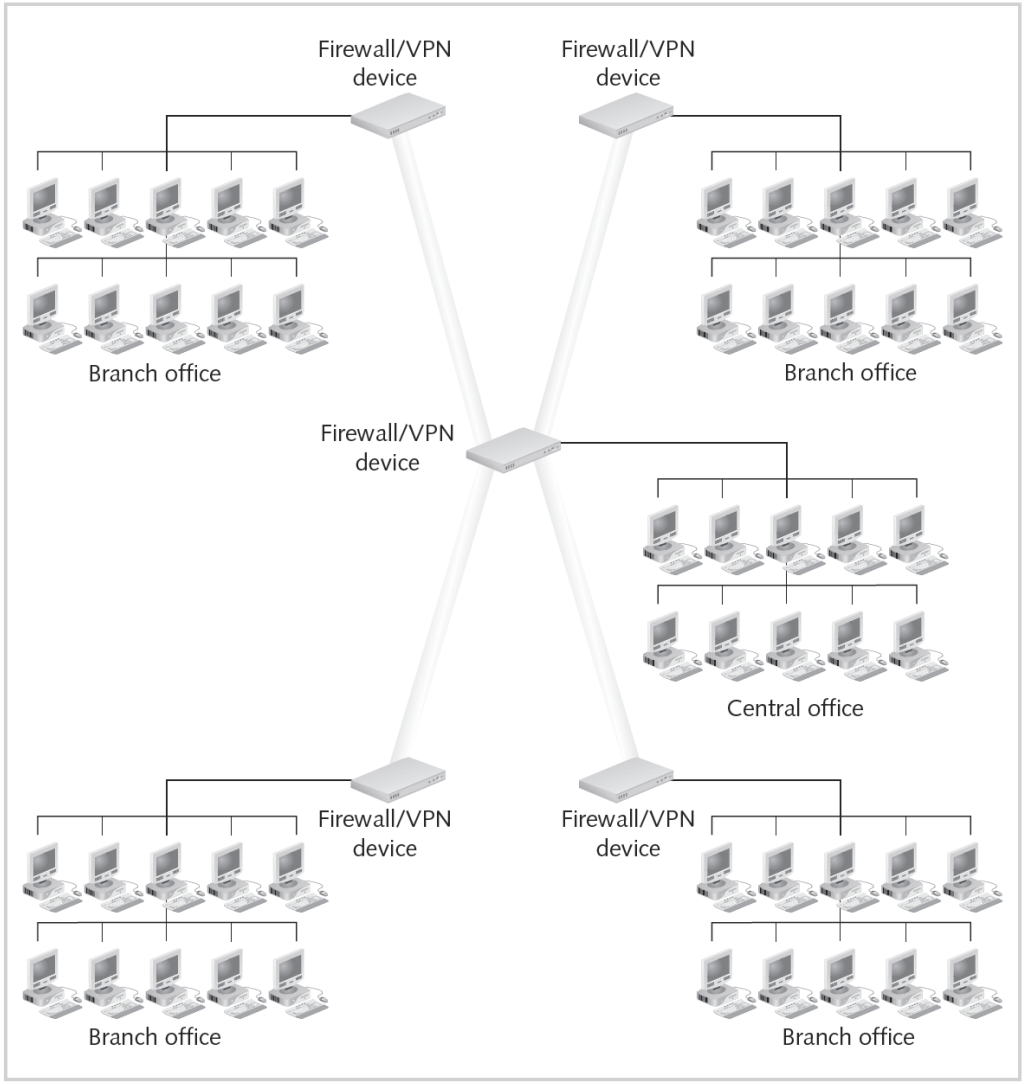

Figure 5-12 Hub-and-spoke VPN

© Cengage Learning 2013

VPN Architectures

- Hybrid configuration
  - Mixture of mesh and hub-and-spoke configurations
  - Mesh configuration should handle time-critical communications
  - Overseas branches can be part of hub-and-spoke configuration

Tunneling Protocols Used with VPNs

- Proprietary protocols used in the past
- IPSec/IKE
  - Standard for secure encrypted communication
  - Uses two security methods
    - Authenticated Headers (AH)
    - Encapsulating Security Payload (ESP)
  - Works in both transport and tunnel modes
- Point-to-point tunneling protocol (PPTP)
  - Used for connection using dial-in modem

Tunneling Protocols Used with VPNs (cont'd.)

- Layer2 tunneling protocol (L2TP)
  - Extension of PPP
  - Provides secure authenticated remote access
  - Separates process of initiating connection from process of forwarding data
- UNIX-based methods for creating VPNs
  - Point-to-point protocol over Secure Sockets Layer
  - Point-to-point protocol over Secure Shell

Protocol	Recommended Usage
IPSec/IKE	Rapidly becoming the protocol of choice for VPN connections of all sorts and should be used when the other protocols are not acceptable
PPTP	When a dial-up user has an old system that doesn't support L2TP and needs to use PPP to establish a VPN connection to your network
L2TP	When a dial-up user needs to establish a VPN connection with your network (L2TP provides stronger protection than PPTP)
PPP Over SSL	When a UNIX user needs to create a VPN connection "on the fly" by connecting to the SSL port on a server
PPP Over SSH	When a UNIX user needs to create a VPN connection "on the fly" over the UNIX secure shell (SSH) and both parties know the secret key in advance

Table 5-5 VPN protocols and their uses

VPN Best Practices

- Create a VPN policy
  - Identify who can use VPN
  - Specify proper use of the VPN
- Determine where encryption/decryption will be performed
  - In relation to packet filtering
  - See Figures 5-13 and 5-14 for external and internal options

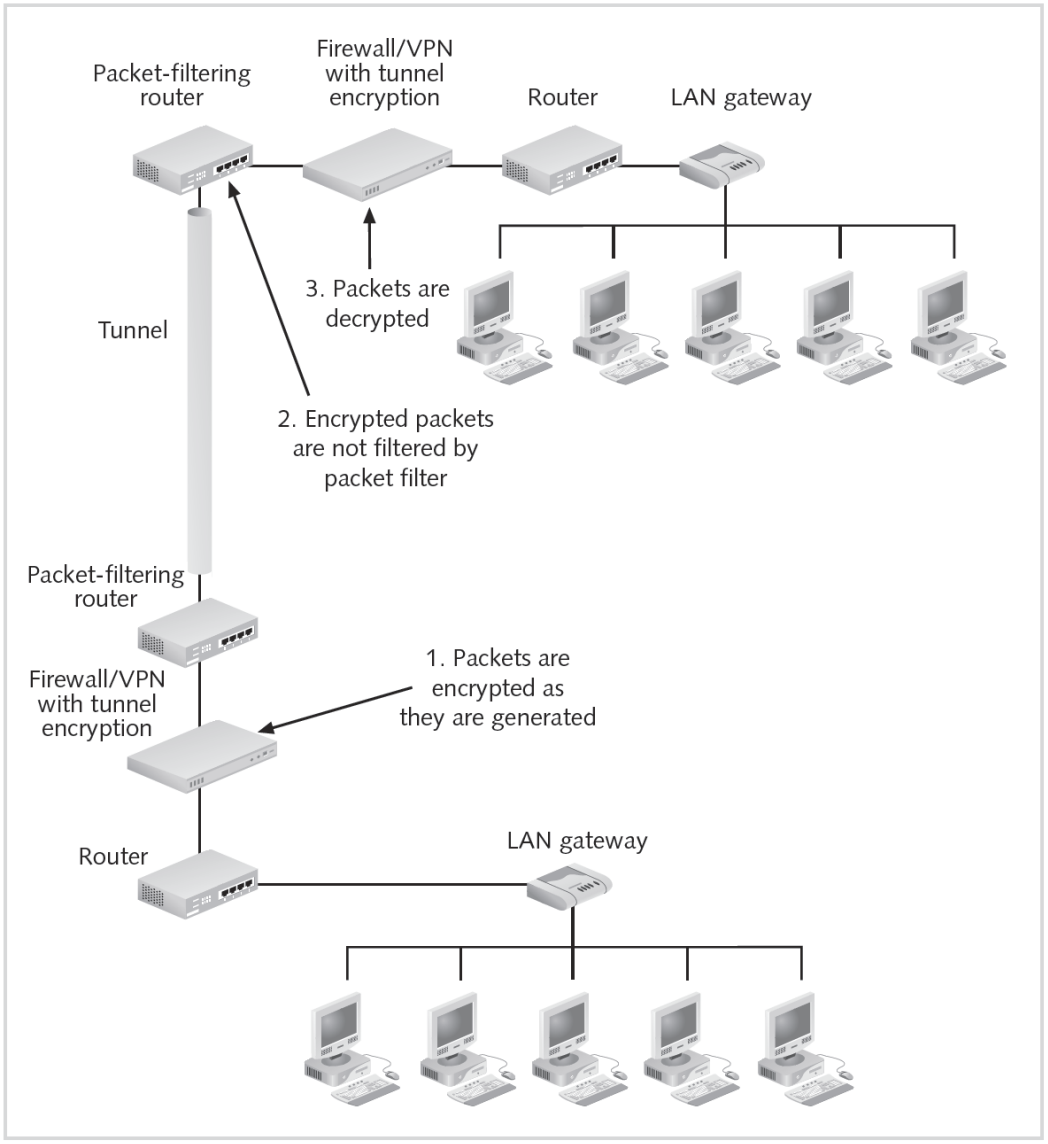

Figure 5-13 External encryption

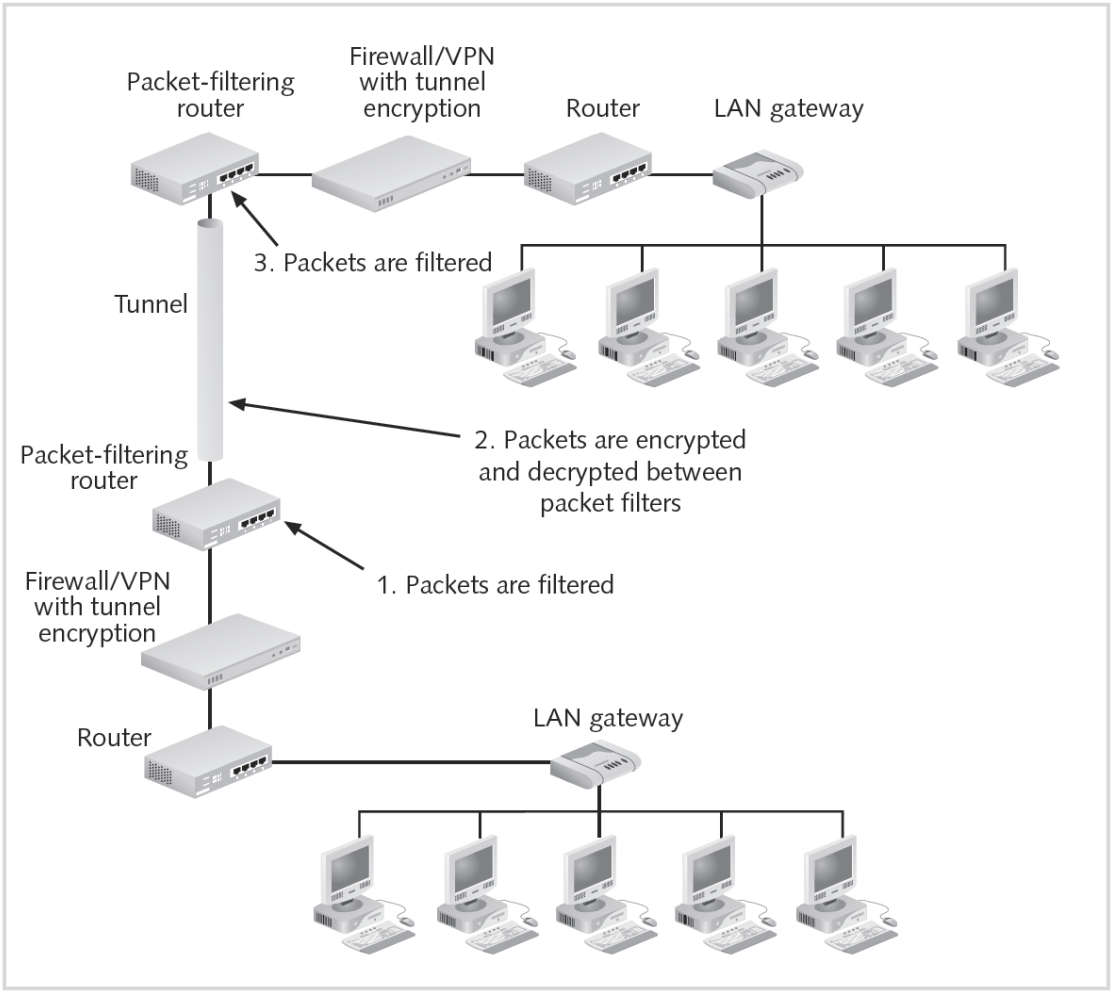

Figure 5-14 Internal encryption
© Cengage Learning 2013

Benefits and Drawbacks of VPNs

- Benefits
  - Secure networking without overhead of maintaining leased lines
  - Packet encryption/translation overhead handled on dedicated systems
    - Decreased load on production machines
- Drawbacks
  - Complex
  - Can create network vulnerabilities if improperly configured

Benefits and Drawbacks of VPNs (cont'd.)

- VPNs extend network boundaries
- Suggestions for dealing with increased risk
  - Multifactor authentication
  - Integrated virus protection
  - NAC
  - Usage limits

Summary

- Network security devices require authentication:
  - To assign different levels of authorization to different users and groups
- Network security device authentication schemes
  - User, client, and session
- Centralized authentication methods include Kerberos, TACACS+, and RADIUS
- Passwords can be static or dynamically generated
- VPNs provide secure, point-to-point communications over the Internet

Summary (cont'd.)

- VPNs can use mesh, hub-and-spoke, or hybrid configurations
- Standard protocols today include IPSec/IKE, PPTP, L2TP, PPP over SSL, and PPP over SSH