Remote Access

- Chapter 4

Learning Objectives

- Understand implications of IEEE 802.1x and how it is used
- Understand VPN technology and its uses for securing remote access to networks
- Understand how RADIUS authentication works
- Understand how TACACS+ operates
- Understand how PPTP works and when it is used

continued…

Learning Objectives

- Understand how L2TP works and when it is used
- Understand how SSH operates and when it is used
- Understand how IPSec works and when it is used
- Understand the vulnerabilities associated with telecommuting

IEEE 802.1x

- Internet standard created to perform authentication services for remote access to a central LAN
- Uses SNMP to define levels of access control and behavior of ports providing remote access to LAN environment
- Uses EAP over LAN (EAPOL) encapsulation method

802.1x General Topology

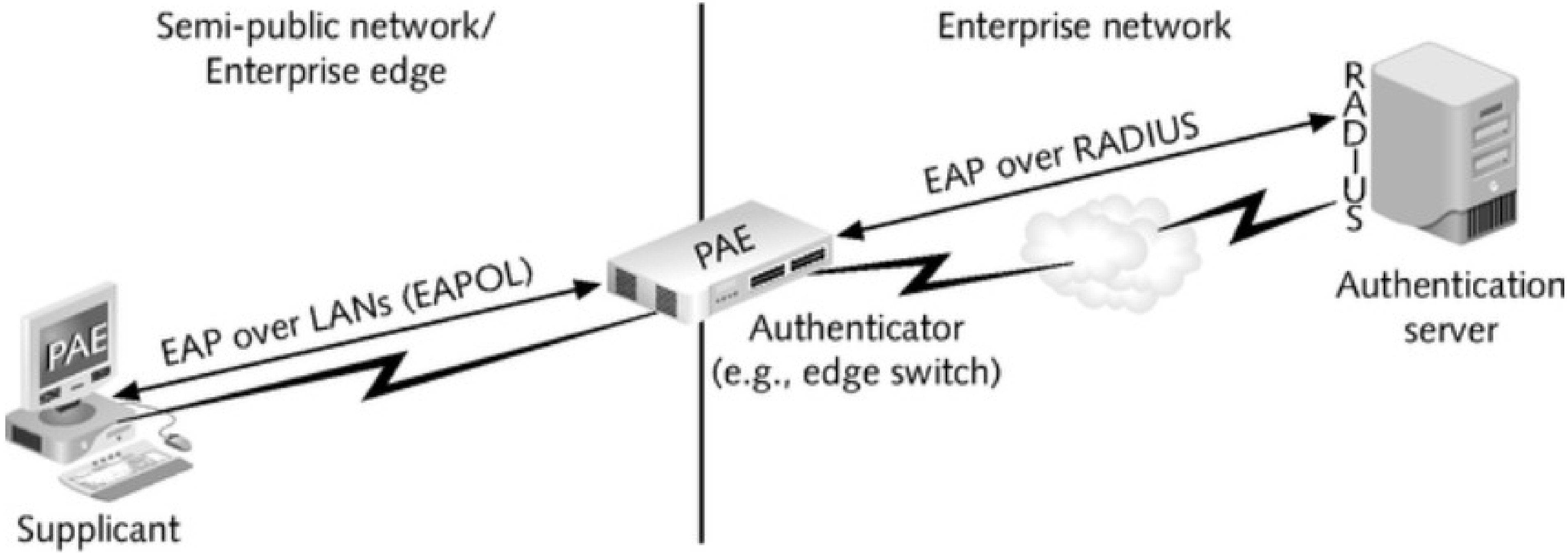

Figure 4-1 802.1x general topology

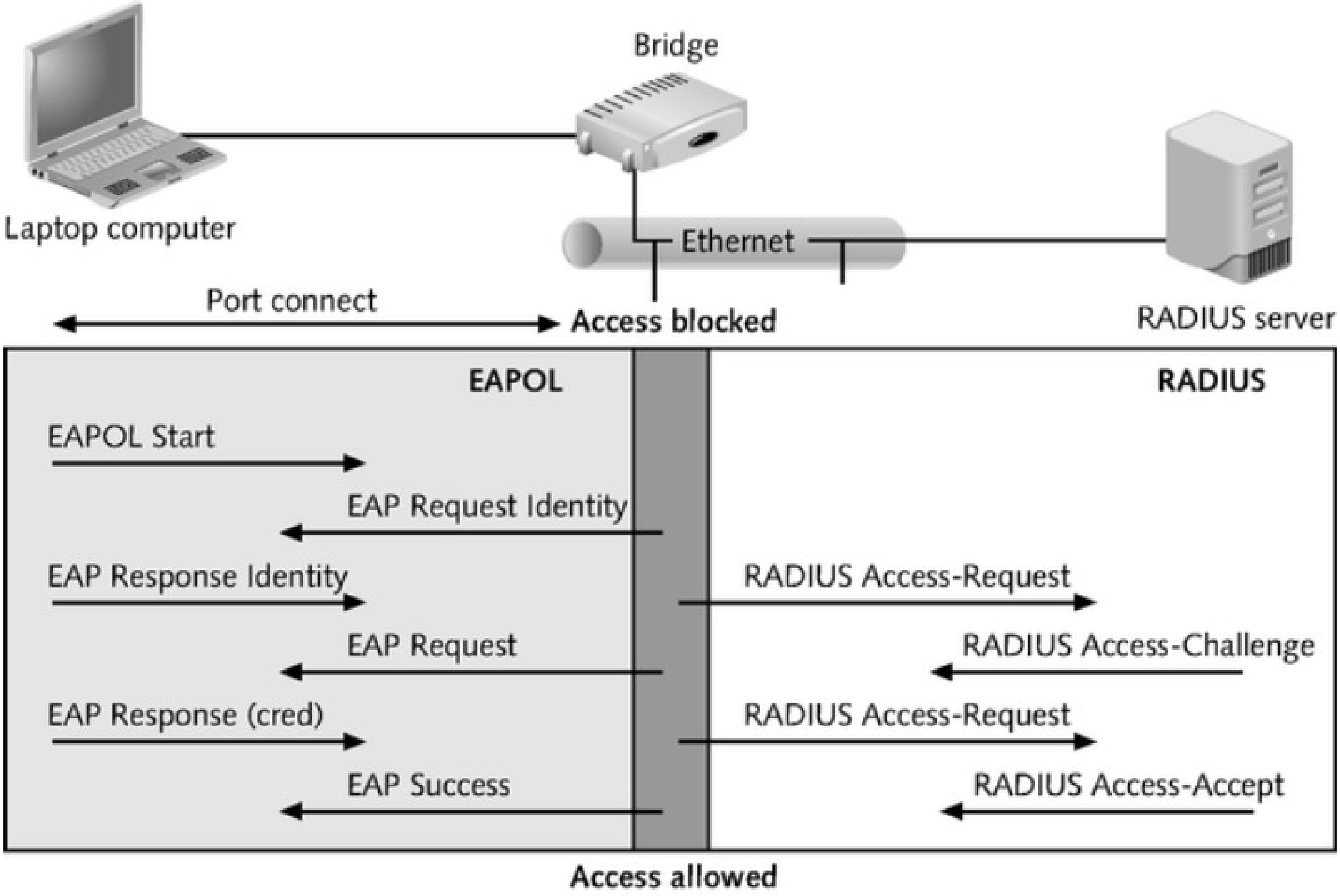

Figure 4-2 IEEE 802.1x conversation

Telnet

- Standard terminal emulation protocol within TCP/IP protocol suite defined by RFC 854
- Utilizes UDP port 23 to communicate
- Allows users to log on to remote networks and use resources as if locally connected

Controlling Telnet

- Assign enable password as initial line of defense
- Use access lists that define who has access to what resources based on specific IP addresses
- Use a firewall that can filter traffic based on ports, IP addresses, etc

Virtual Private Network

- Secures connection between user and home office using authentication mechanisms and encryption techniques
  - Encrypts data at both ends
- Uses two technologies
  - IPSec
  - PPTP

VPN Diagram

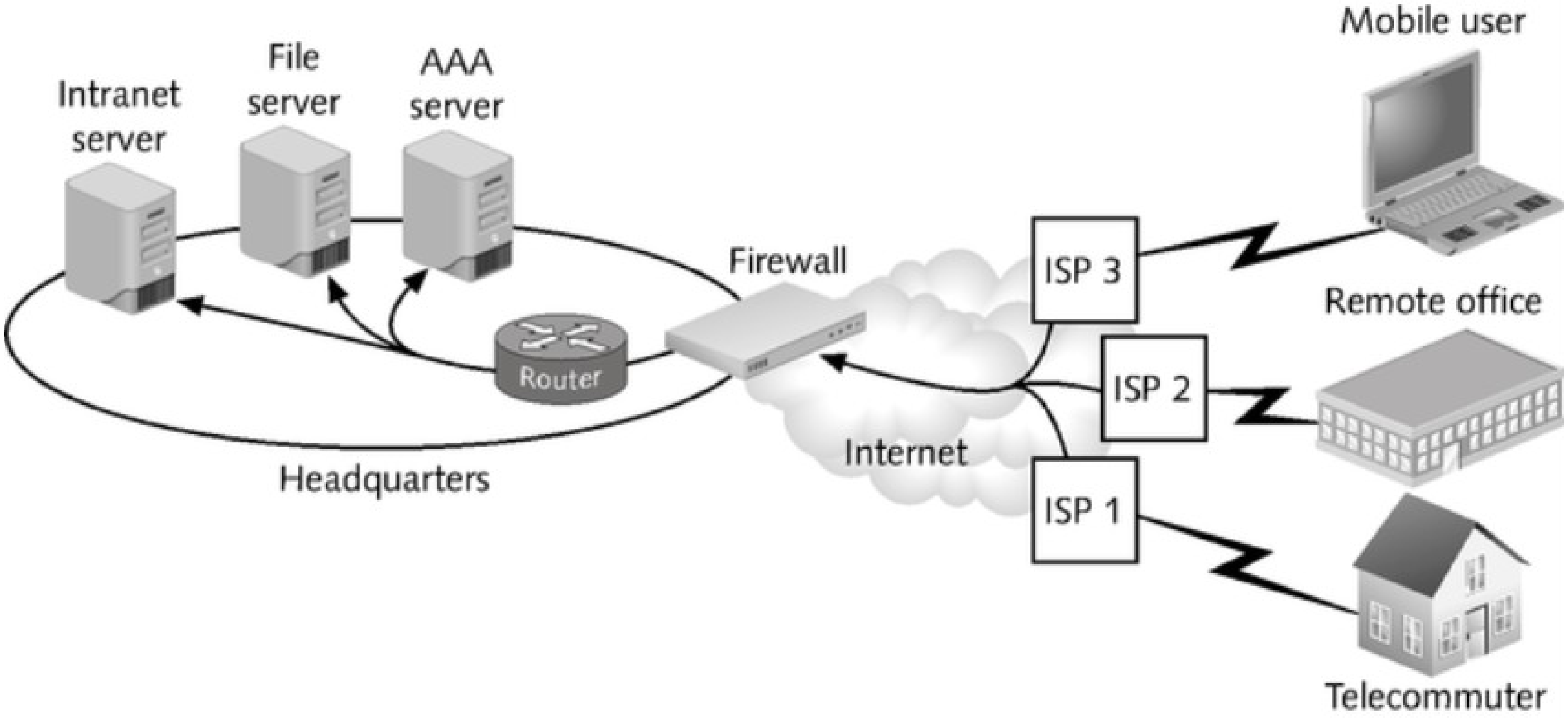

Figure 4-3 VPN diagram

FORBSEC

Tunneling

- Enables one network to send its data via another network’s connections
- Encapsulates a network protocol within packets carried by the second network

Tunneling

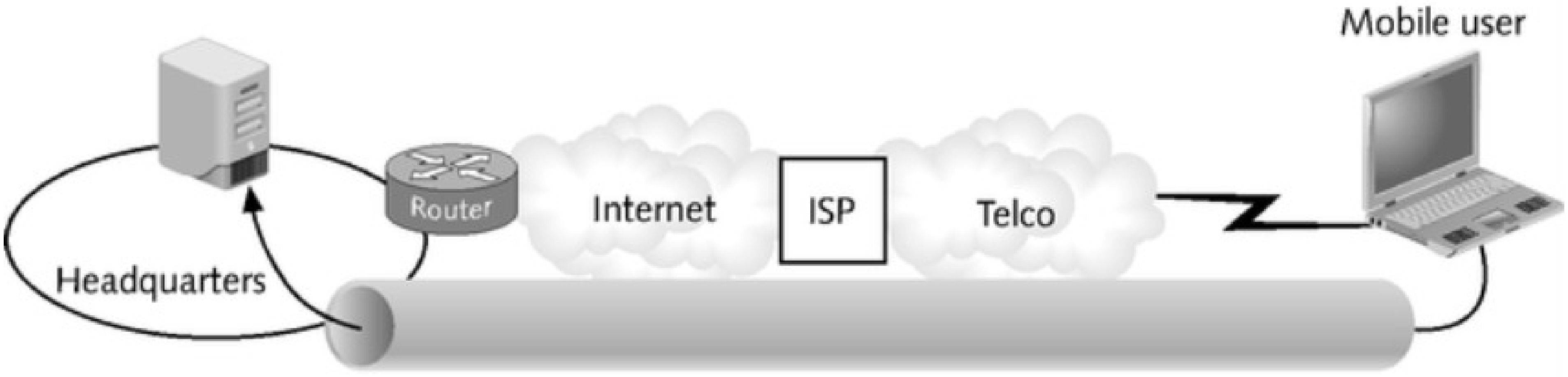

Figure 4-4 Client-side tunneling

VPN Options

- Install/configure client computer to initiate necessary security communications
- Outsource VPN to a service provider
    - Encryption does not happen until data reaches provider’s network

Service Providing Tunneling

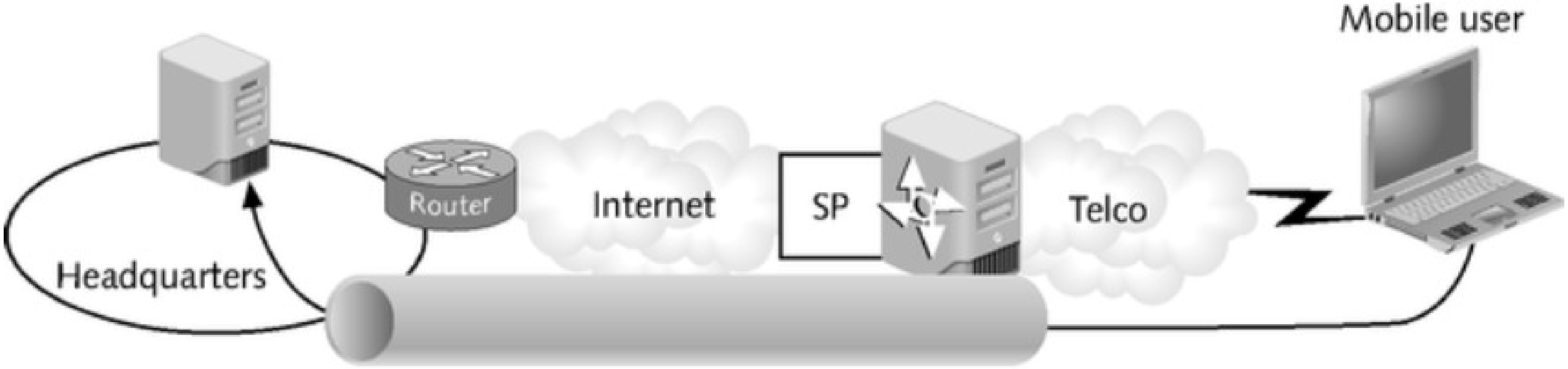

Figure 4-5 Service provider tunneling

VPN Drawbacks

- Not completely fault tolerant
- Diverse implementation choices
    - Software solutions
        - Tend to have trouble processing all the simultaneous connections on a large network
    - Hardware solutions
        - Require higher costs

Remote Authentication Dial-in User Service (RADIUS)

- Provides a client/server security system
- Uses distributed security to authenticate users on a network
- Includes two pieces
  - Authentication server
  - Client protocols
- Authenticates users through a series of communications between client and server using UDP

Authenticating with a RADIUS Server

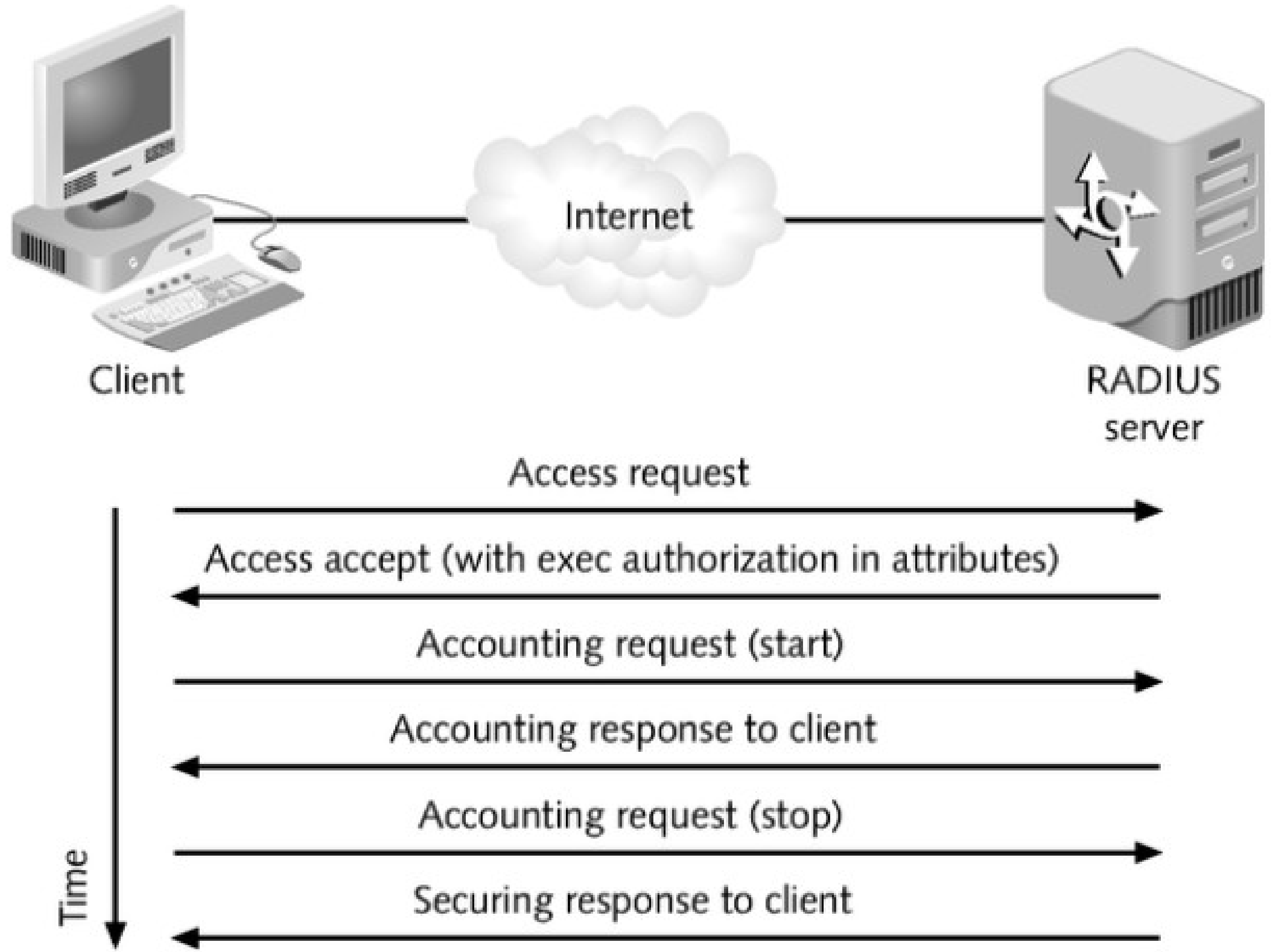
Internet
Client
RADIUS server
Access request
Access accept (with exec authorization in attributes)
Accounting request (start)
Accounting response to client
Accounting request (stop)
Securing response to client
Time

Figure 4-6 RADIUS

Benefits of Distributed Approach to Network Security

- Greater security
- Scalable architecture
- Open protocols
- Future enhancements

Terminal Access Controller Access Control System (TACACS+)

- Authentication protocol developed by Cisco
- Uses TCP – a connection-oriented transmission – instead of UDP
- Offers separate acknowledgement that request has been received regardless of speed of authentication mechanism
- Provides immediate indication of a crashed server

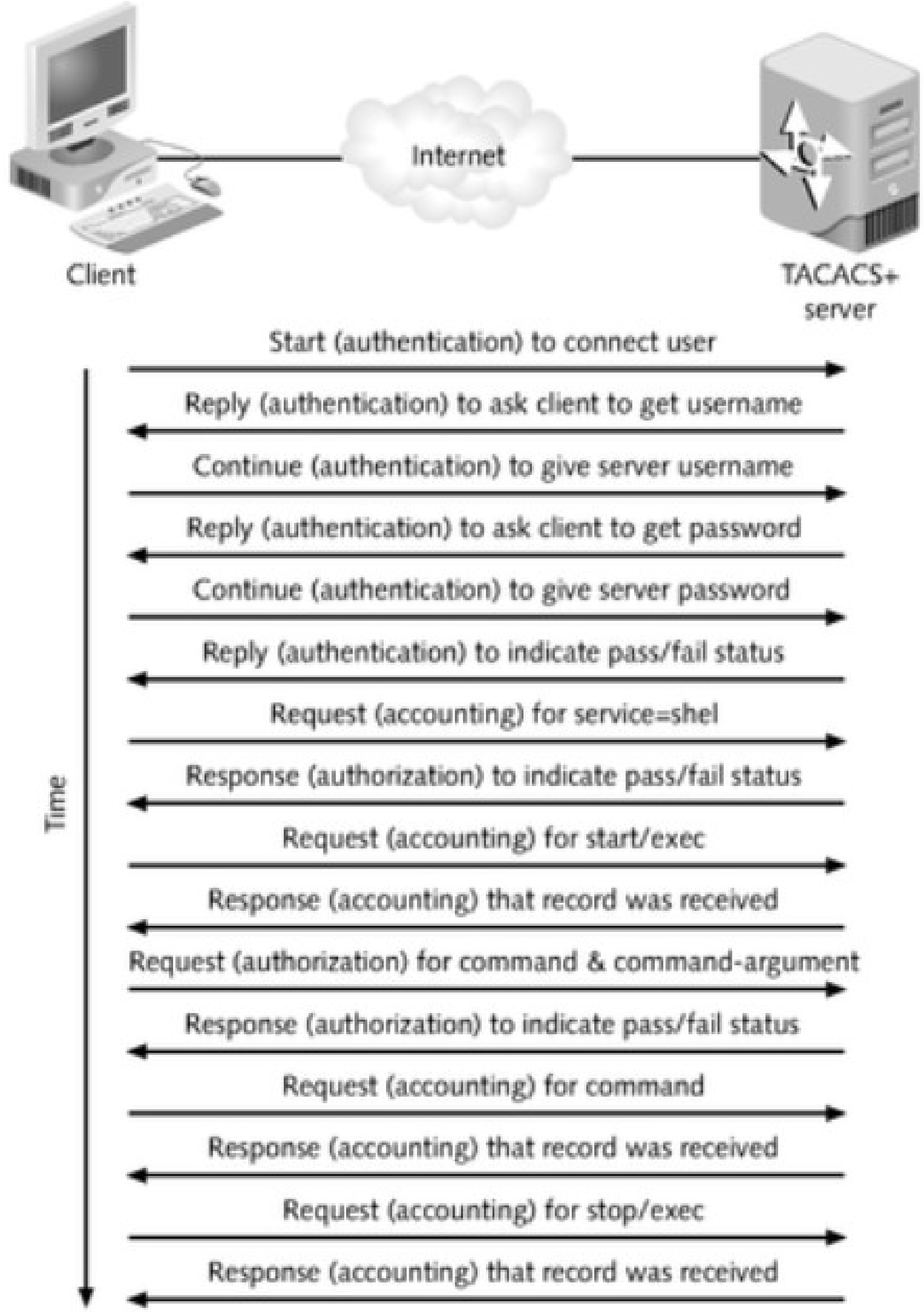
Client
Internet
TACACS+ server
Time
Start (authentication) to connect user
Reply (authentication) to ask client to get username
Continue (authentication) to give server username
Reply (authentication) to ask client to get password
Continue (authentication) to give server password
Reply (authentication) to indicate pass/fail status
Request (accounting) for service=shel
Response (authorization) to indicate pass/fail status
Request (accounting) for start/exec
Response (accounting) that record was received
Request (authorization) for command & command-argument
Response (authorization) to indicate pass/fail status
Request (accounting) for command
Response (accounting) that record was received
Request (accounting) for stop/exec
Response (accounting) that record was received

Figure 4-7 TACACS+

Advantages of TACACS+ over RADIUS

- Addresses need for scalable solution
- Separates authentication, authorization, and accounting
- Offers multiple protocol support

Point-to-Point Tunneling Protocol

- Multiprotocol that offers authentication, methods of privacy, and data compression
- Built upon PPP and TCP/IP
- Achieves tunneling by providing encapsulation (wraps packets of information within IP packets)
    - Data packets
    - Control packets
- Provides users with virtual node on corporate LAN or WAN

PPTP Tasks

- Queries status of communications servers
- Provides in-band management
- Allocates channels and places outgoing calls
- Notifies Windows NT Server of incoming calls
- Transmits and receives user data with bi-directional flow control
- Notifies Windows NT Server of disconnected calls
- Assures data integrity; coordinates packet flow

Layer Two Tunneling Protocol

- PPP defines an encapsulation mechanism for transporting multiprotocol packets across layer two point-to-point links
- L2TP extends PPP model by allowing layer two and PPP endpoints to reside on different devices interconnected by a packet-switched network

continued…

Layer Two Tunneling Protocol

- Allows separation of processing of PPP packets and termination of layer two circuit
  - Connection may terminate at a (local) circuit concentrator
- Solves splitting problems by projecting a PPP session to a location other than the point at which it is physically received

Secure Shell (SSH)

- Secure replacement for remote logon and file transfer programs (Telnet and FTP) that transmit data in unencrypted text
- Uses public key authentication to establish an encrypted and secure connection from user's machine to remote machine
- Used to:
  - Log on to another computer over a network
  - Execute command in a remote machine
  - Move files from one machine to another

Key Components of an SSH Product

- Engine
- Administration server
- Enrollment gateway
- Publishing server

IP Security Protocol

- Set of protocols developed by the IETF to support secure exchange of packets at IP layer
- Deployed widely to implement VPNs
- Works with existing and future IP standards
- Transparent to users
- Promises painless scalability
- Handles encryption at packet level using Encapsulating Security Payload (ESP)

IPSec Security Payload

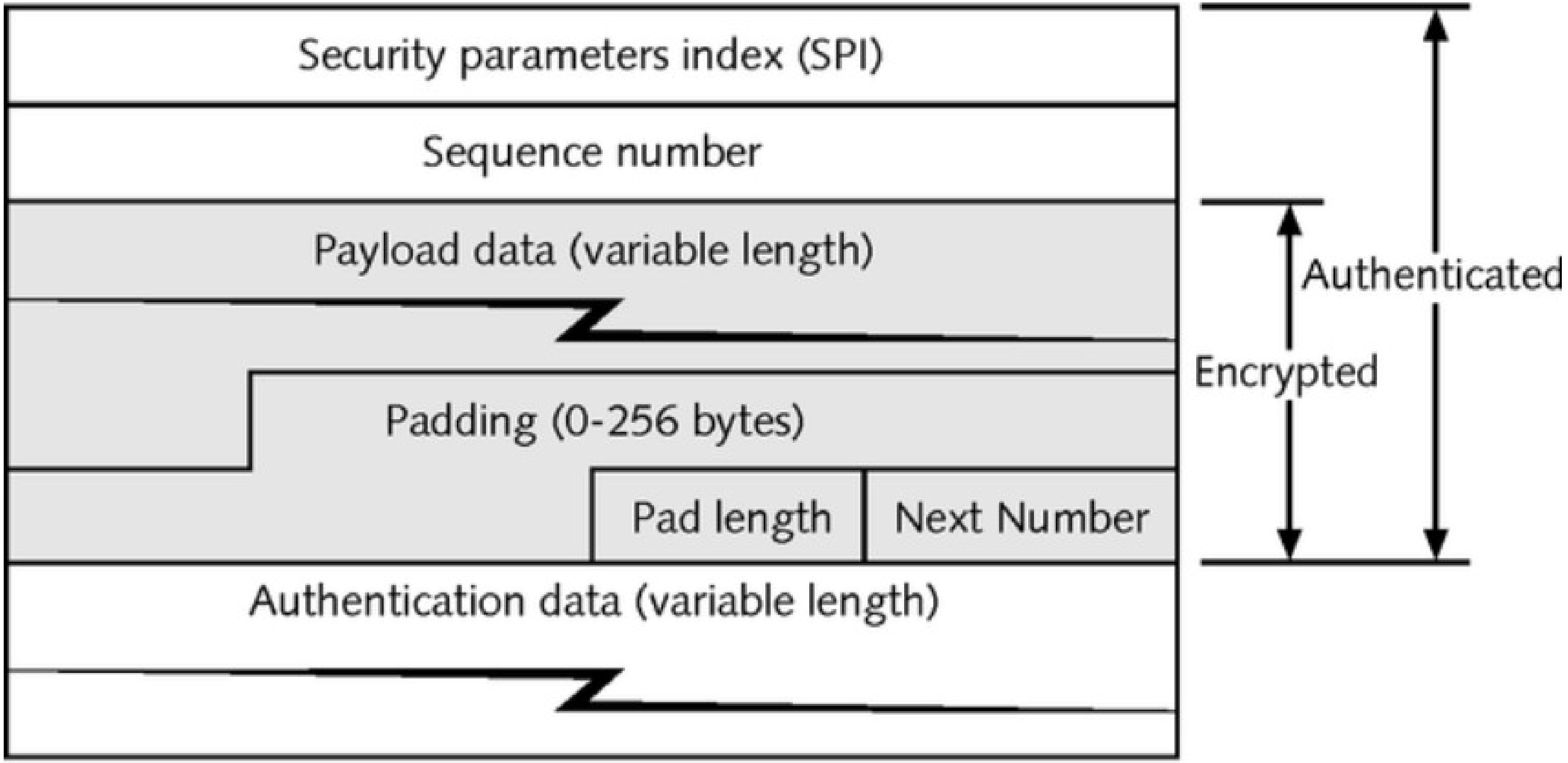
Security parameters index (SPI)
Sequence number
Payload data (variable length)
Padding (0-256 bytes)
Pad length
Next Number
Authentication data (variable length)
Authenticated
Encrypted

Figure 4-8 IPSec security payload

ESP and Encryption Models

- Supports many encryption protocols
- Encryption support is designed for use by symmetric encryption algorithms
- Provides secure VPN tunneling

Telecommuting Vulnerabilities

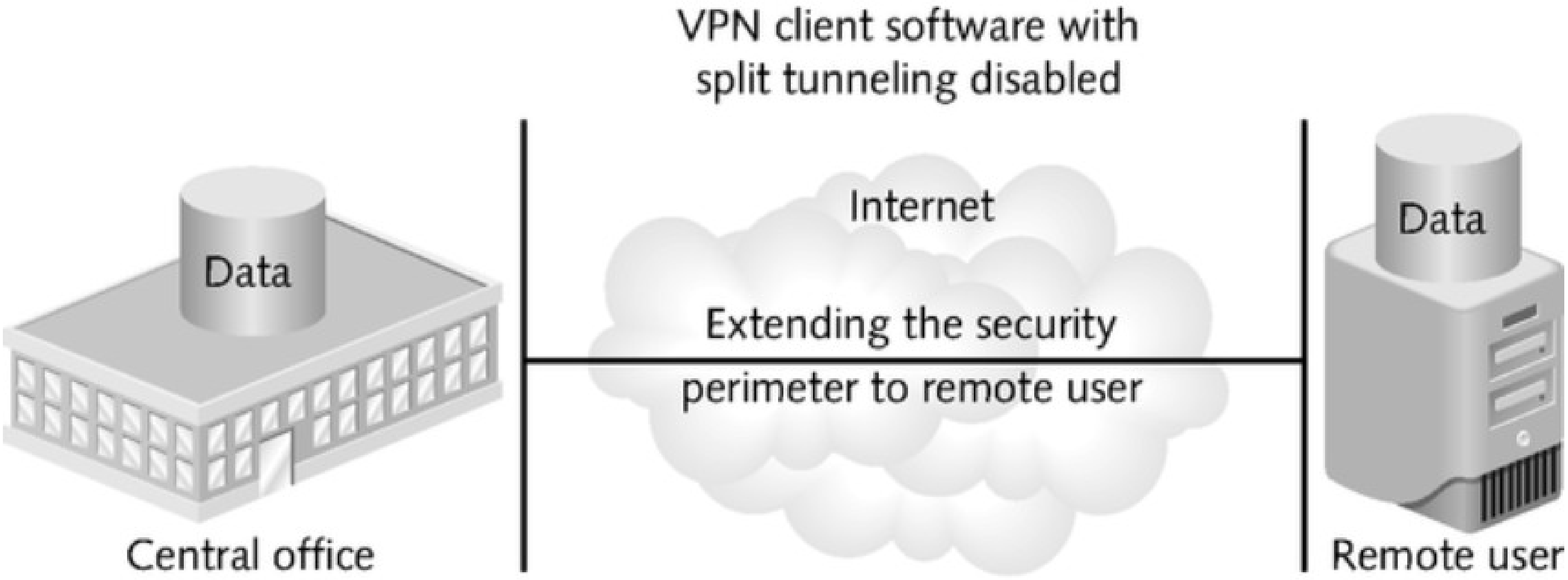

Figure 4-9 Traditional VPN

Telecommuting Vulnerabilities

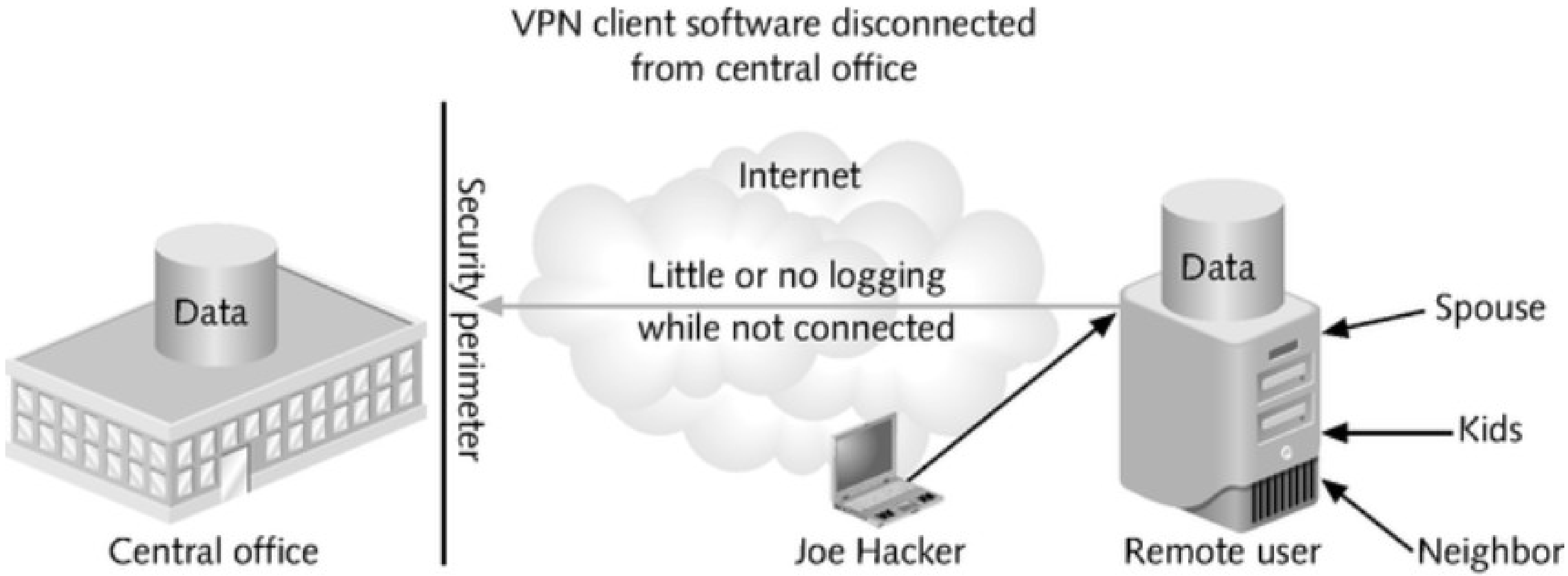
VPN client software disconnected from central office
Internet
Security perimeter
Data
Little or no logging while not connected
Data
Spouse
Kids
Neighbor
Central office
Joe Hacker
Remote user

Figure 4-10 VPN vulnerability

Telecommuting Vulnerabilities

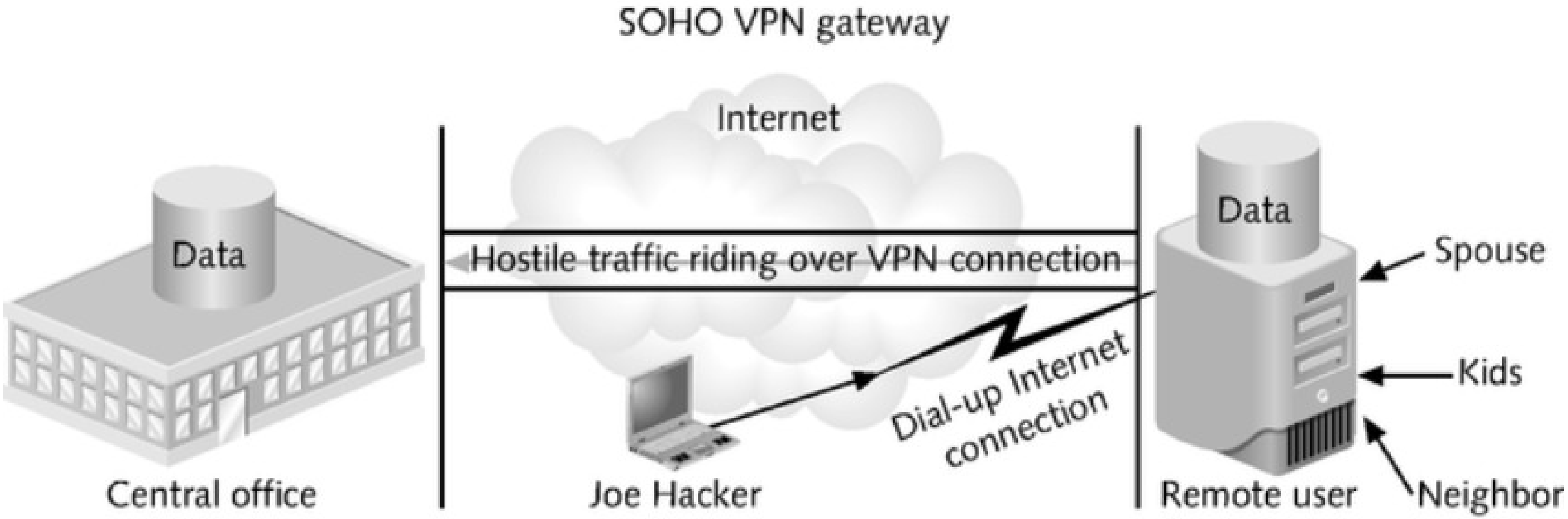

Figure 4-11 SOHO VPN

Telecommuting Vulnerabilities

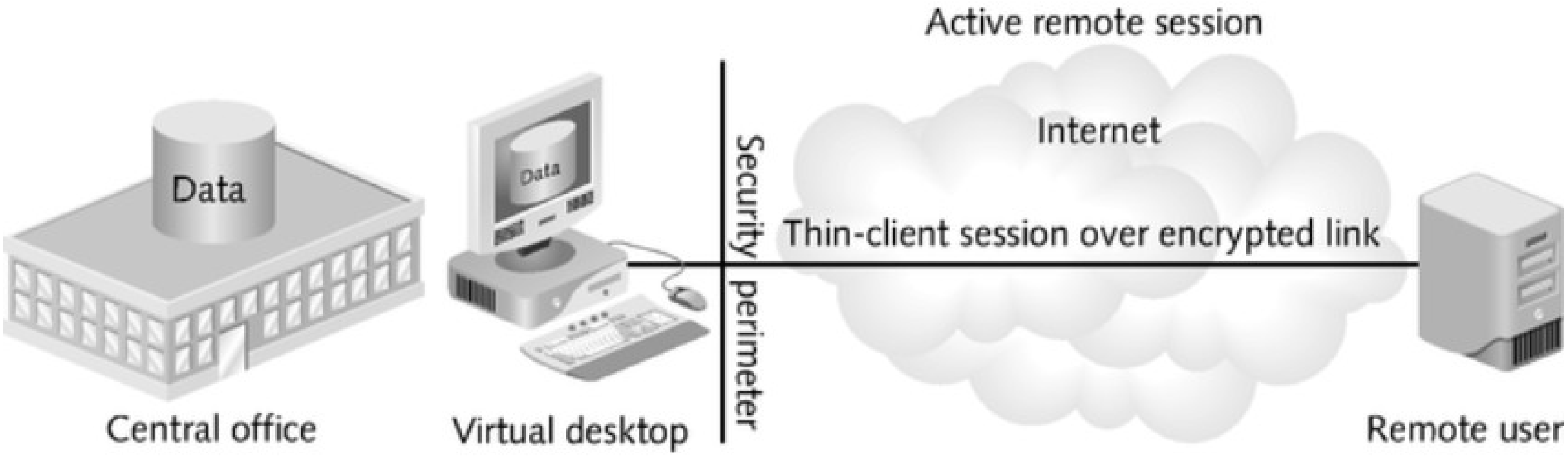

Figure 4-12 Active remote session

Telecommuting Vulnerabilities

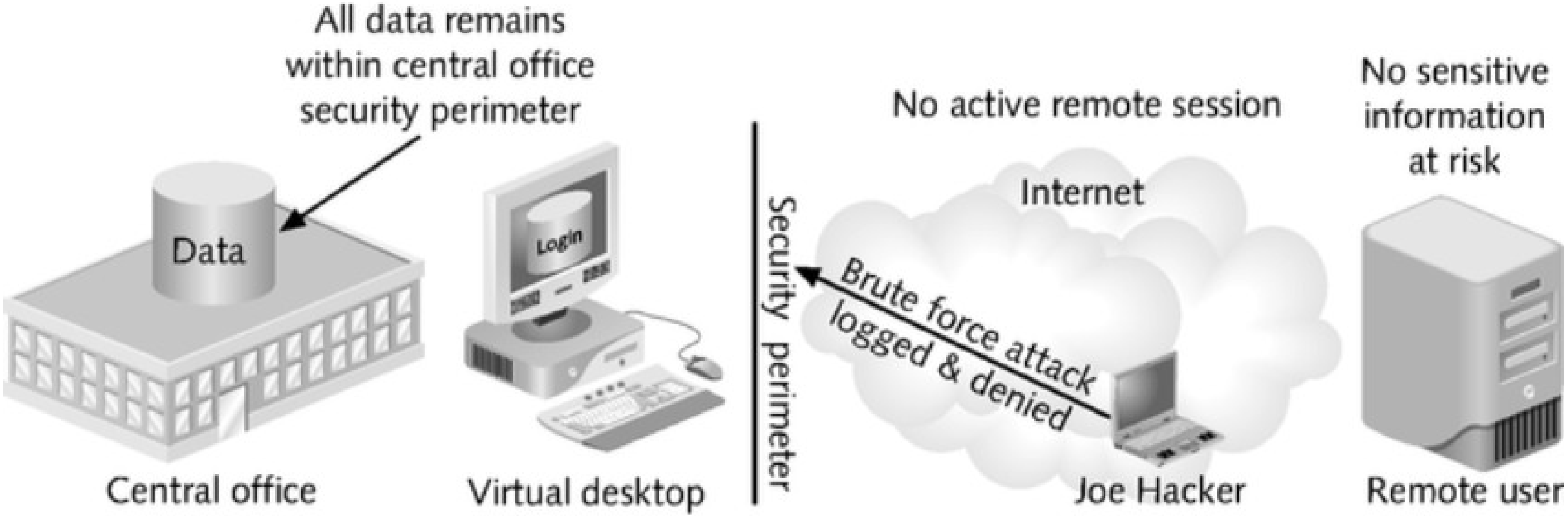
All data remains within central office security perimeter
Data
Login
Central office
Virtual desktop
Security perimeter
No active remote session
Internet
Brute force attack logged & denied
Joe Hacker
No sensitive information at risk
Remote user

Figure 4-13 No active remote session

Remote Solutions

- Microsoft Terminal Server
- Citrix Metaframe
- Virtual Network Computing

Chapter Summary

- Paramount need for remote access security
- Use of technologies to mitigate some of the risk of compromising the information security of a home network
- Importance of keeping pace with technology changes