Principles of Information Security

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:
  - Recognize the important role of access control in computerized 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 means of the authentication and authorization of users

Learning Objectives (cont'd.)

- Discuss content filtering technology
- Describe the technology that enables the use of virtual private networks

Introduction

- Technical controls are essential in enforcing policy for many IT functions that do not involve direct human control
- Technical control solutions improve an organization's ability to balance making information readily available against increasing information's levels of 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
- Nondiscretionary controls: strictly-enforced version of MACs that are managed by a central authority
- Discretionary access controls (DACs): implemented at the discretion or option of the data user

Identification

- Identification: mechanism whereby an unverified entity that seeks access to a resource proposes a label by which they are known to the system
- Supplicant: entity that seeks a resource
- 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 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
    - 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

Firewalls

- Prevent specific types of information from moving between the outside world (untrusted network) and the inside world (trusted 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

Firewalls Processing Modes (cont'd.)

- Packet filtering firewalls examine header information of data packets
- Most often based on combination of:
  - Internet Protocol (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

Firewalls Processing Modes (cont'd.)

- Three subsets of packet filtering firewalls:
  - Static filtering: requires that filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed
  - 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

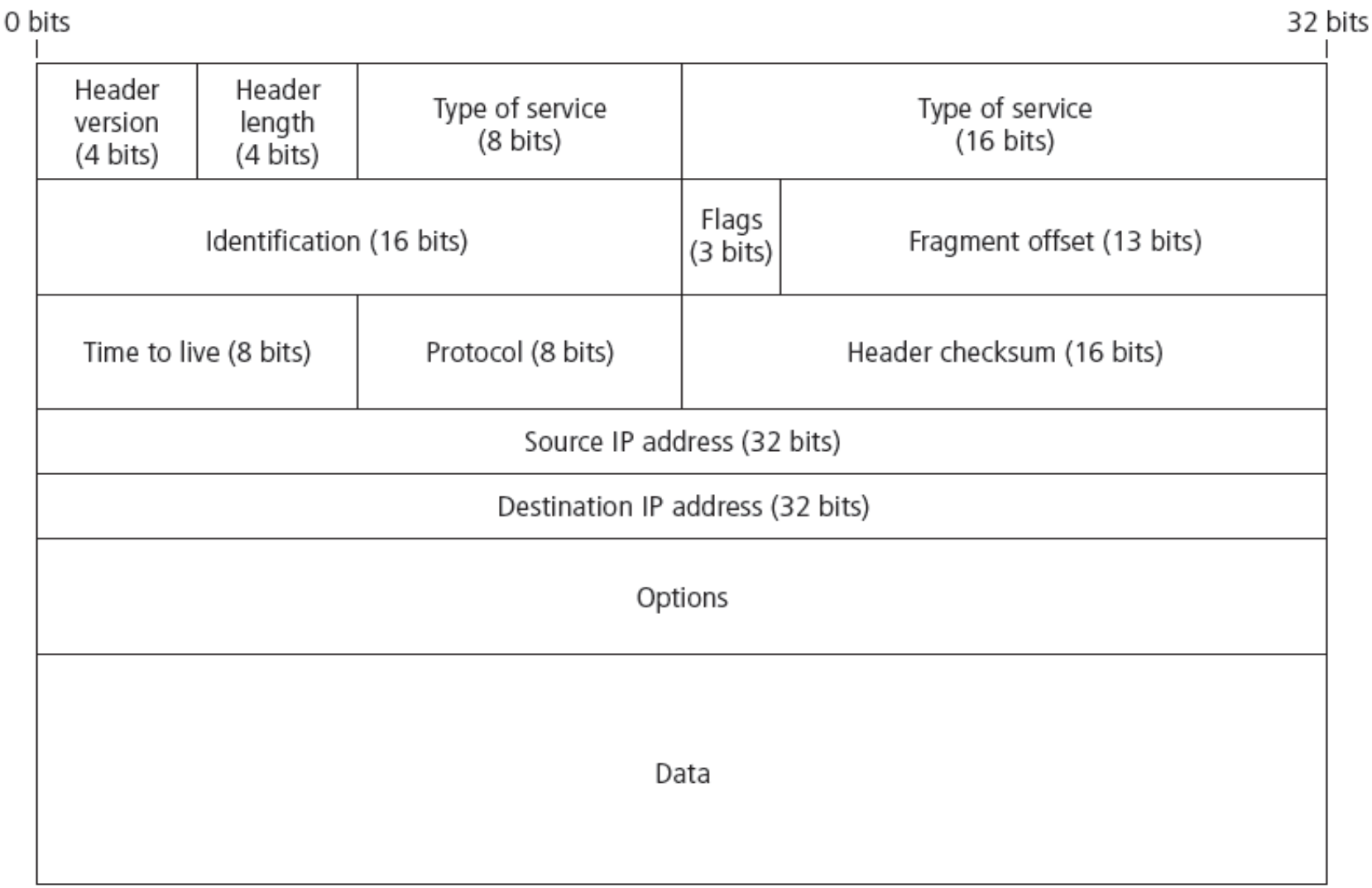

Figure 6-2 IP Packet Structure

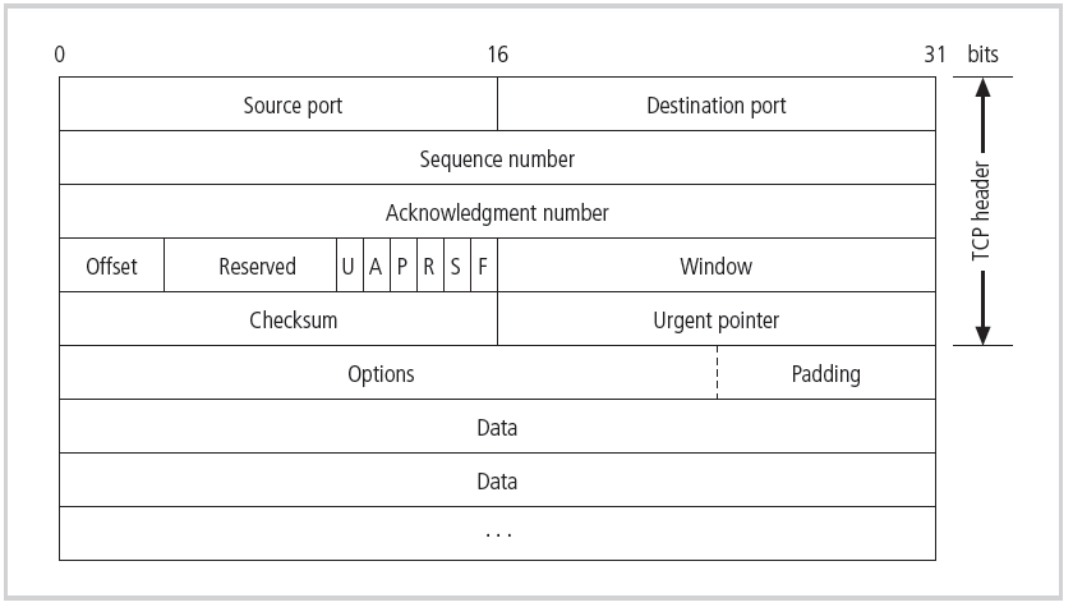

Figure 6-3 TCP Packet Structure

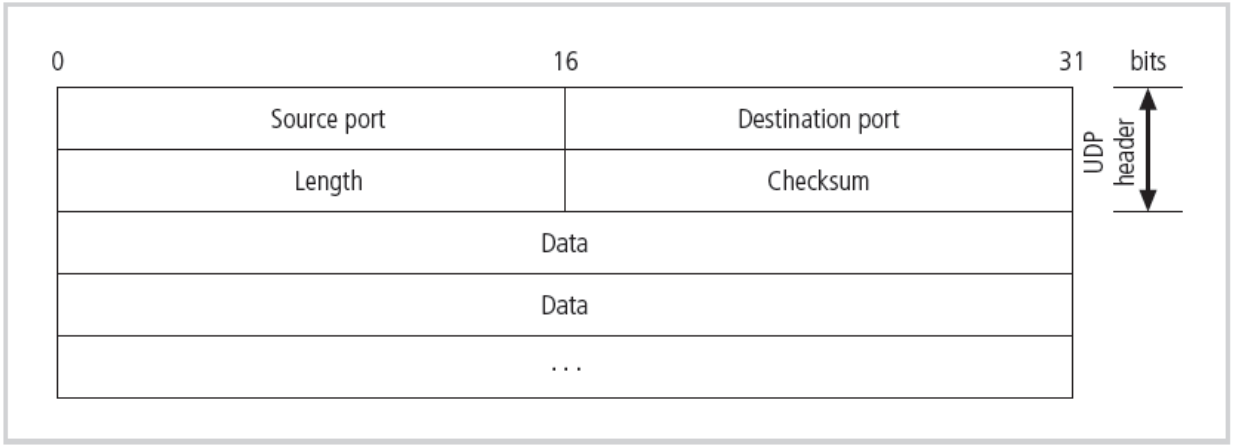

Figure 6-4 UDP Datagram Structure

Source Address	Destination Address	Service (HTTP, SMTP, FTP, Telnet)	Action (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 6-1 Sample Firewall Rule and Format

Firewalls Processing Modes (cont'd.)

- Application gateways
  - 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

Firewalls Processing Modes (cont'd.)

- Circuit gateway firewall
  - Operates at transport layer
  - Like filtering firewalls, do not usually look at data traffic flowing between two networks, but prevent direct connections between one network and another
  - Accomplished by creating tunnels connecting specific processes or systems on each side of the firewall, and allow only authorized traffic in the tunnels

Firewalls Processing Modes (cont'd.)

- MAC layer firewalls
  - Designed to operate at the media access control layer of OSI network model
  - Able to consider specific host computer's identity in its filtering decisions
  - 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

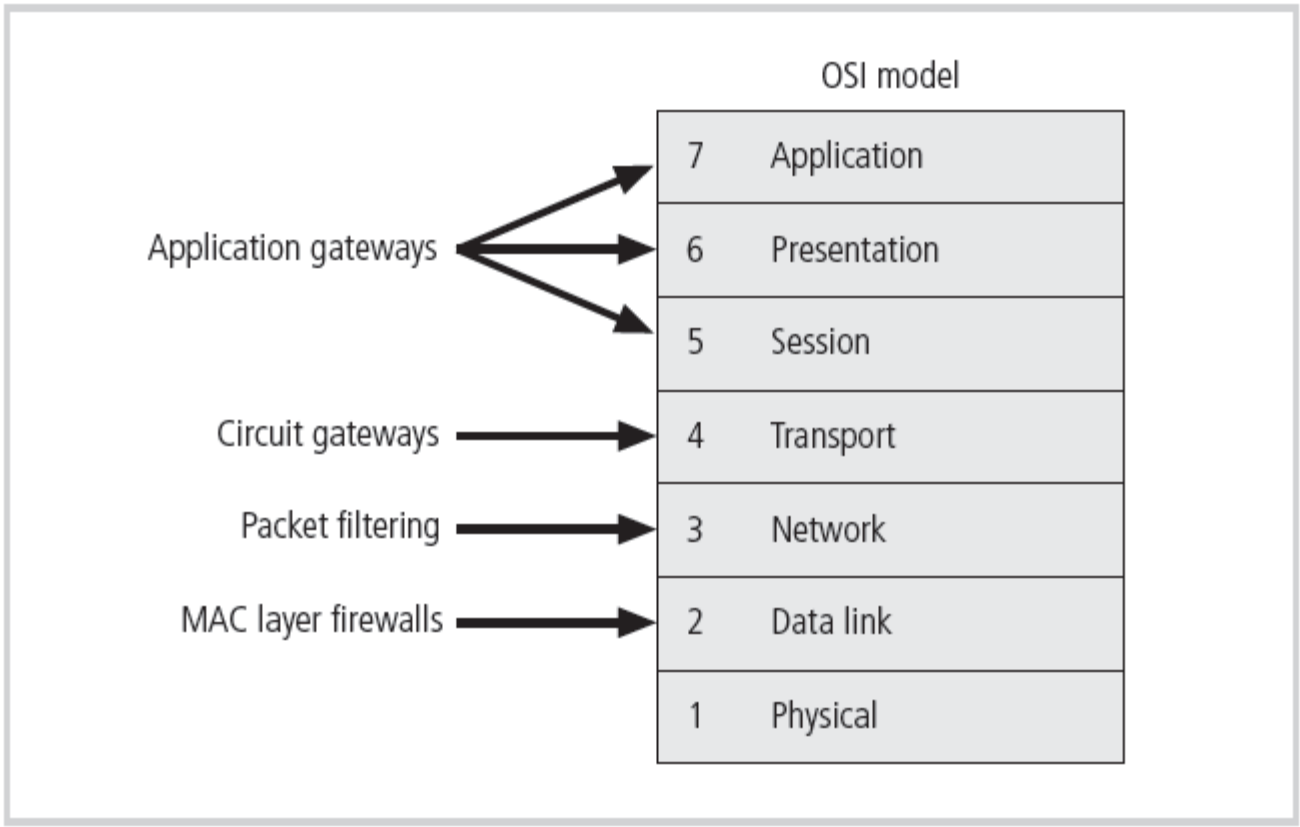

Figure 6-6 Firewall Types and the OSI Model

Firewalls Processing Modes (cont'd.)

- Hybrid firewalls
  - Combine elements of other types of firewalls; i.e., 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

Firewalls Categorized by Generation

- First generation: static packet filtering firewalls
- Second generation: application-level firewalls or proxy servers
- Third generation: stateful inspection firewalls
- Fourth generation: dynamic packet filtering firewalls; allow only packets with particular source, destination, and port addresses to enter
- Fifth generation: kernel proxies; specialized form working under kernel of Windows NT

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 6-2 State Table Entries

Firewalls Categorized by Structure

- Most firewalls are appliances: stand-alone, self-contained systems
- Commercial-grade firewall system
- Small office/home office (SOHO) firewall appliances
- Residential-grade firewall software

Figure 6-7 SOHO Firewall Devices

Software vs. Hardware: the SOHO Firewall Debate

- Which firewall type should the residential user implement?
- Where would you rather defend against a hacker?
- With the software option, hacker is inside your computer
- With the hardware device, even if hacker manages to crash firewall system, computer and information are still safely behind the now disabled connection

Firewall Architectures

- Firewall devices can be configured in a number of 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, screened host firewalls, dual-homed firewalls, screened subnet firewalls

Firewall Architectures (cont'd.)

- Packet filtering routers
  - Most organizations with Internet connection have a router serving as interface to Internet
  - Many of these routers can be configured to reject packets that organization does not allow into network
  - Drawbacks include a lack of auditing and strong authentication

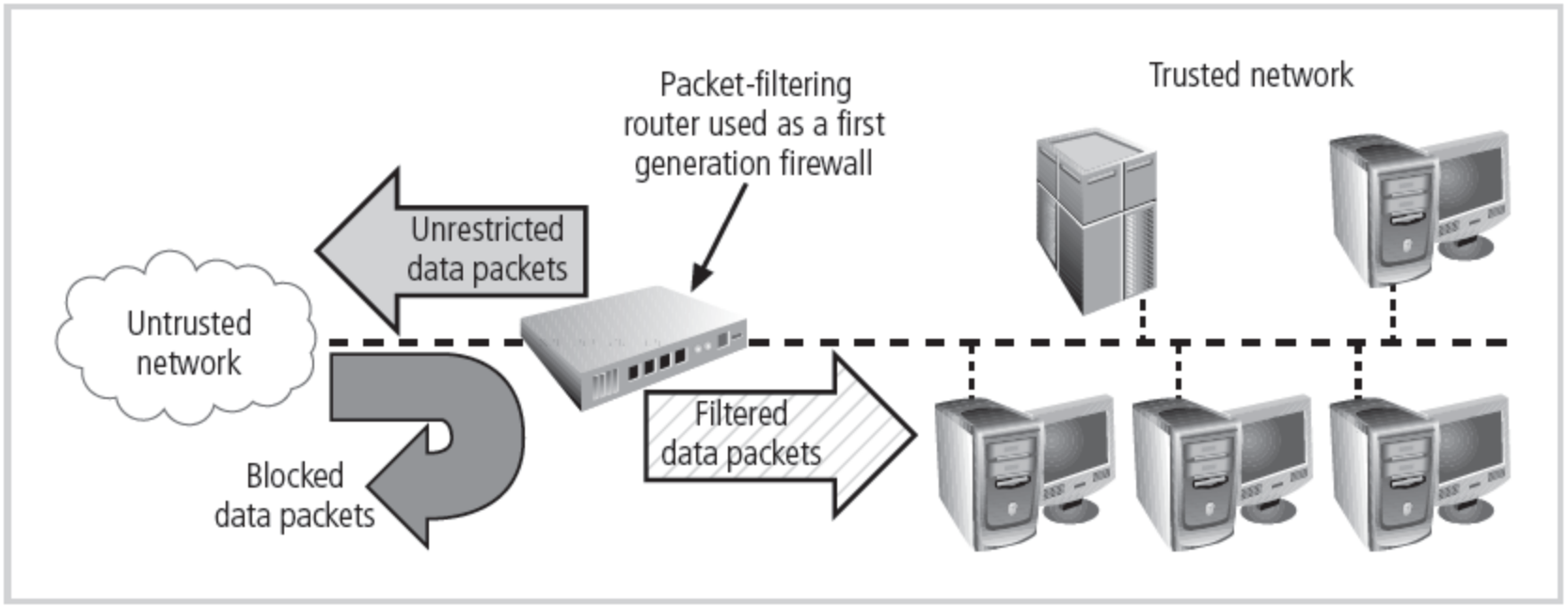

Figure 6-5 Packet-Filtering Router

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
  - Separate host is often referred to as bastion host
    - Can be rich target for external attacks and should be very thoroughly secured
    - Also known as a sacrificial host

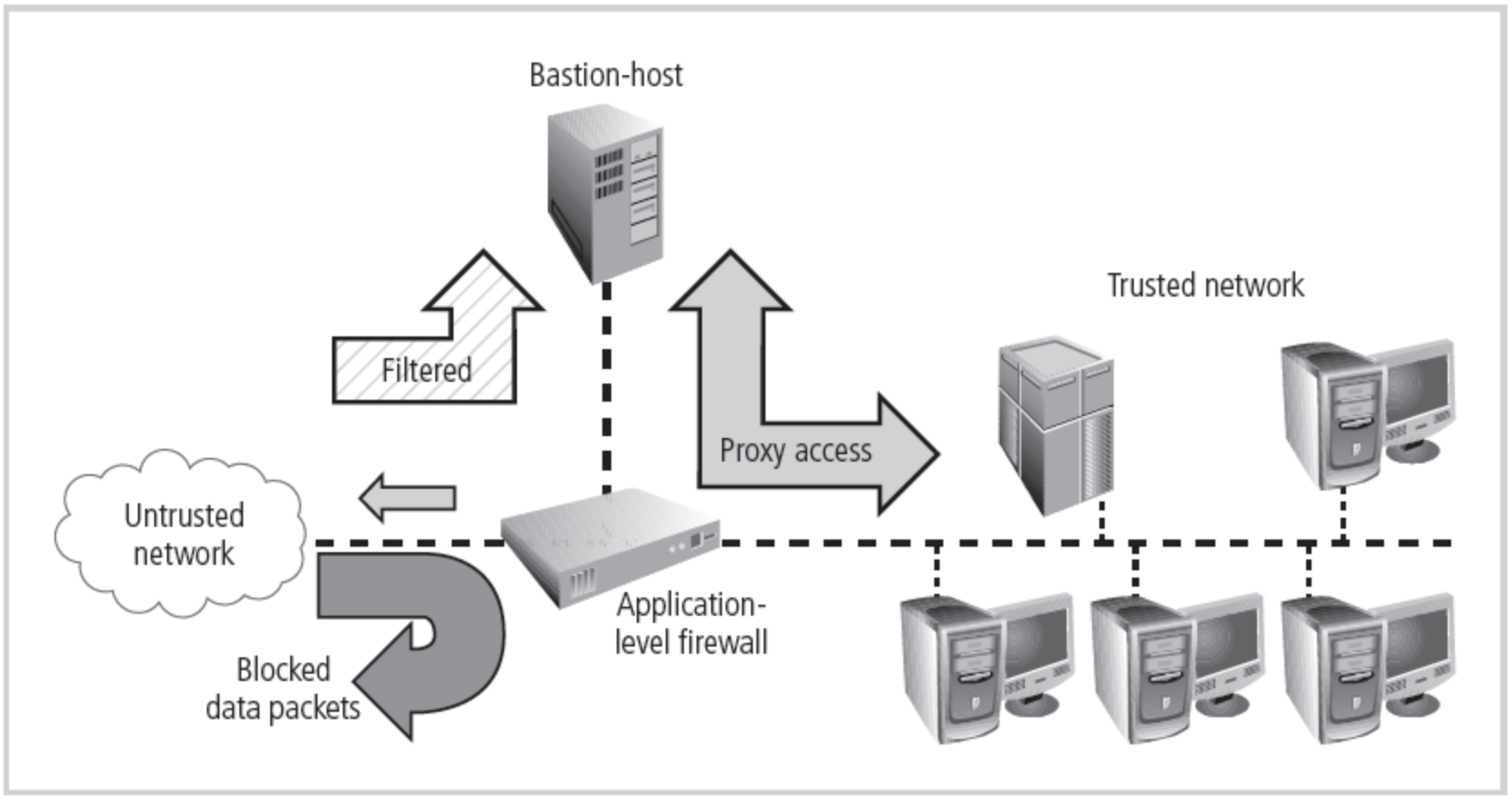

Figure 6-12 Screened Host Firewall

Firewall Architectures (cont'd.)

- Dual-homed host firewalls
  - Bastion host 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

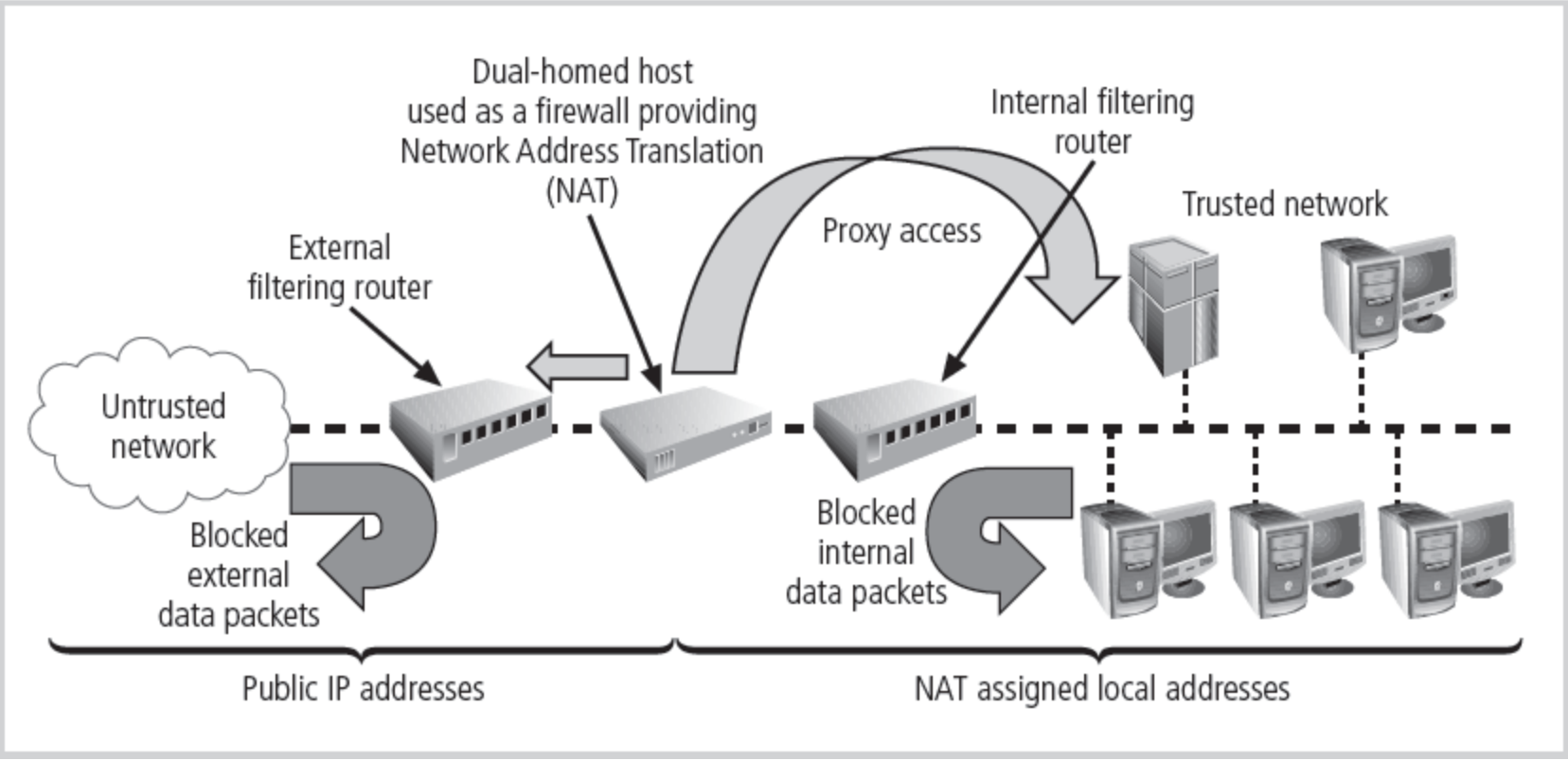

Figure 6-13 Dual-Homed Host Firewall

Firewall Architectures (cont'd.)

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

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

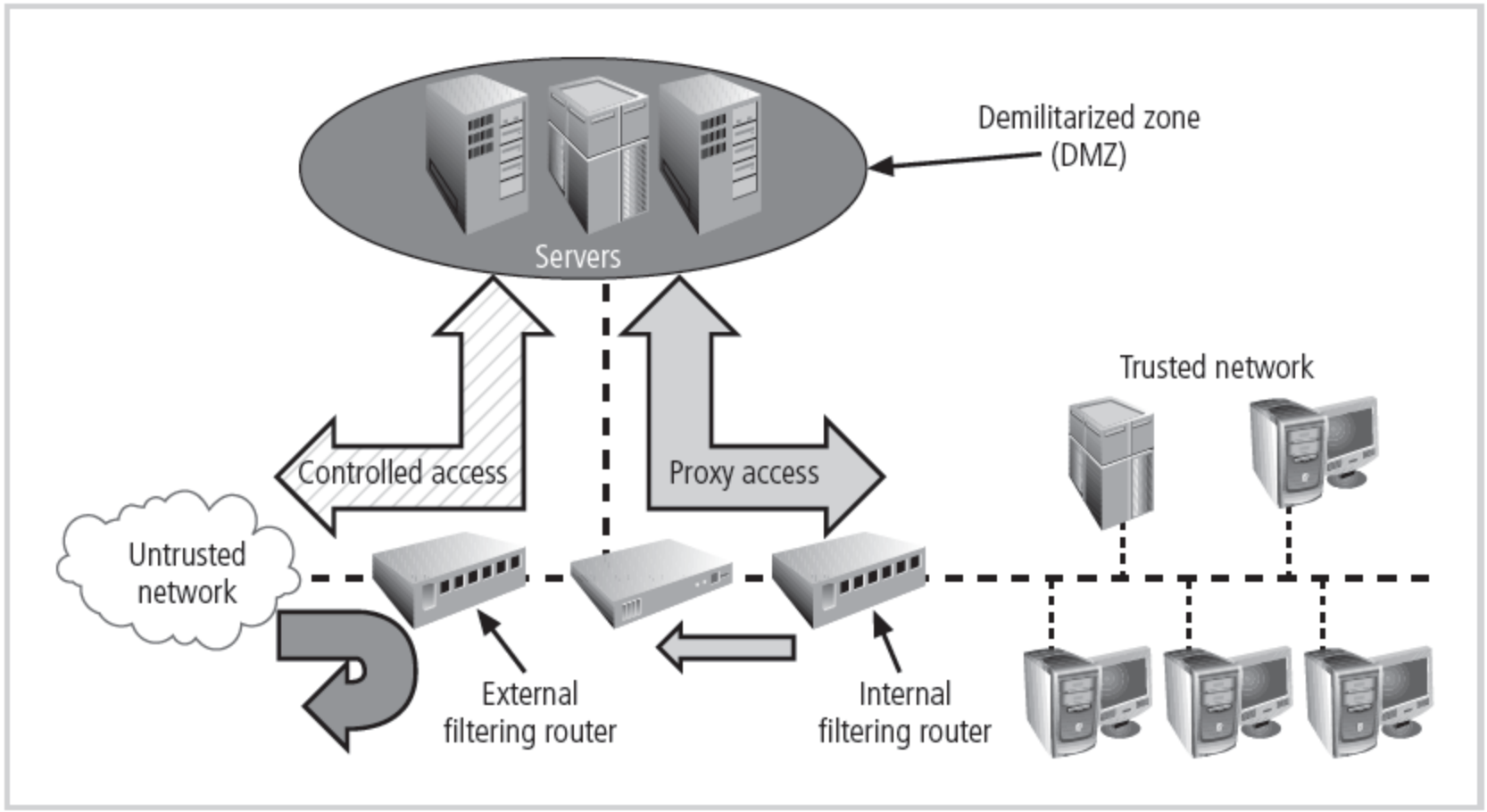

Figure 6-14 Screened Subnet (DMZ)

Selecting the Right Firewall

- When selecting firewall, consider a number of factors:
  - What firewall offers right balance between protection and cost for needs of organization?
  - Which features are included in 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

- Each firewall device must have 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 trusted network is allowed out
  - Firewall device never directly accessed from public network
  - Simple Mail Transport Protocol (SMTP) data allowed to pass through firewall
  - Internet Control Message Protocol (ICMP) data denied
  - Telnet access to internal servers should be blocked
  - When Web services offered outside firewall, HTTP traffic should be denied from reaching internal networks

Configuring and Managing Firewalls (cont'd.)

- Firewall rules
  - Operate by examining data packets and performing comparison with predetermined logical rules
  - Logic based on 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

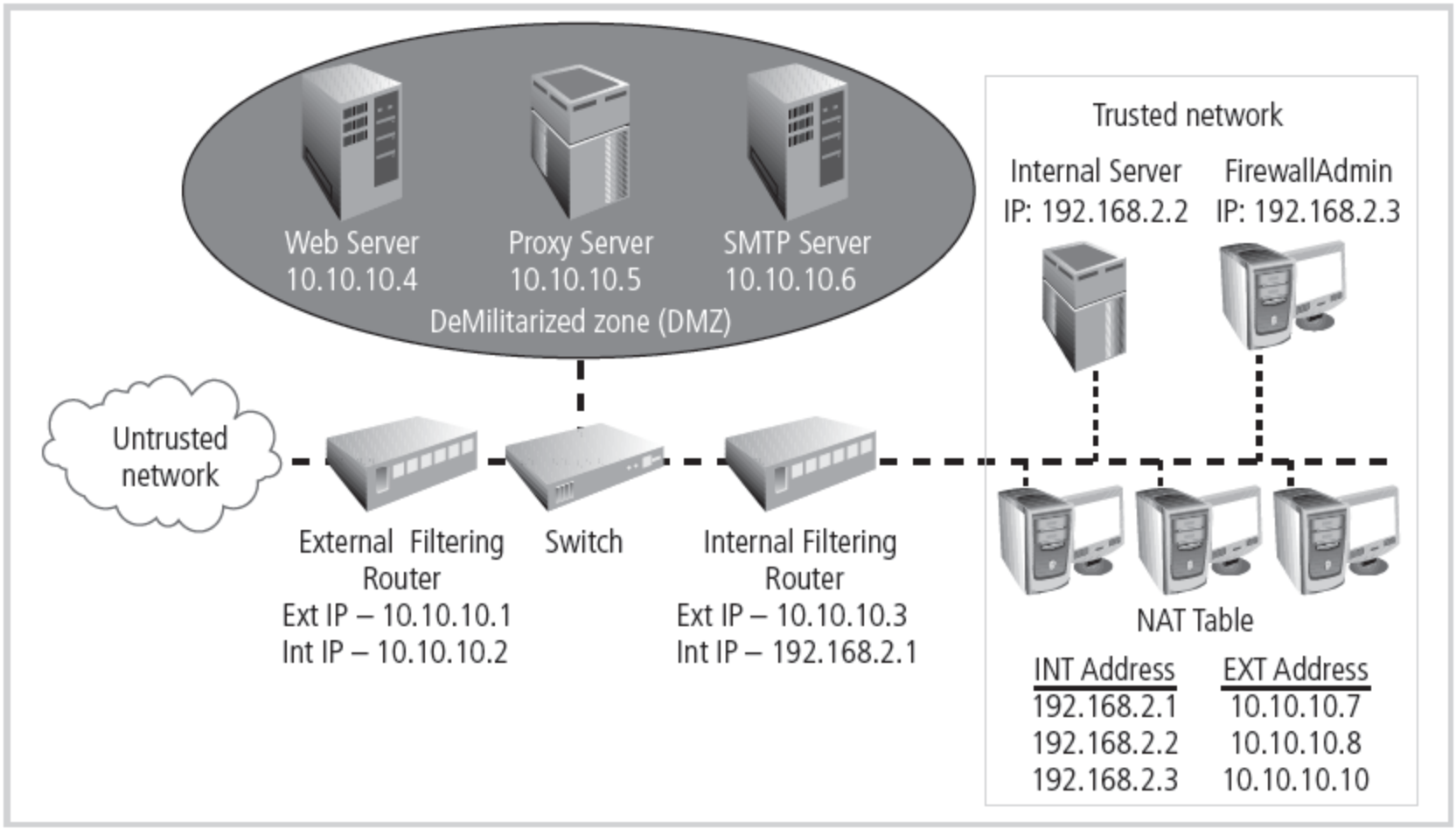

Figure 6-15 Example Network Configuration

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 Services (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

Table 6-5 Select Well-Known Port Numbers

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 network
- Essentially a set of scripts or programs restricting user access to certain networking protocols/Internet locations
- Primary focus to restrict internal access to external material
- Most common content filters restrict users from accessing non-business Web sites or deny incoming span

Protecting Remote Connections

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

Remote Access

- Unsecured, dial-up connection points represent a substantial exposure to attack
- Attacker can use device called a war dialer to locate 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 authentication process

Remote Access (cont'd.)

- RADIUS, TACACS, and Diameter
  - 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 management of user authentication system 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

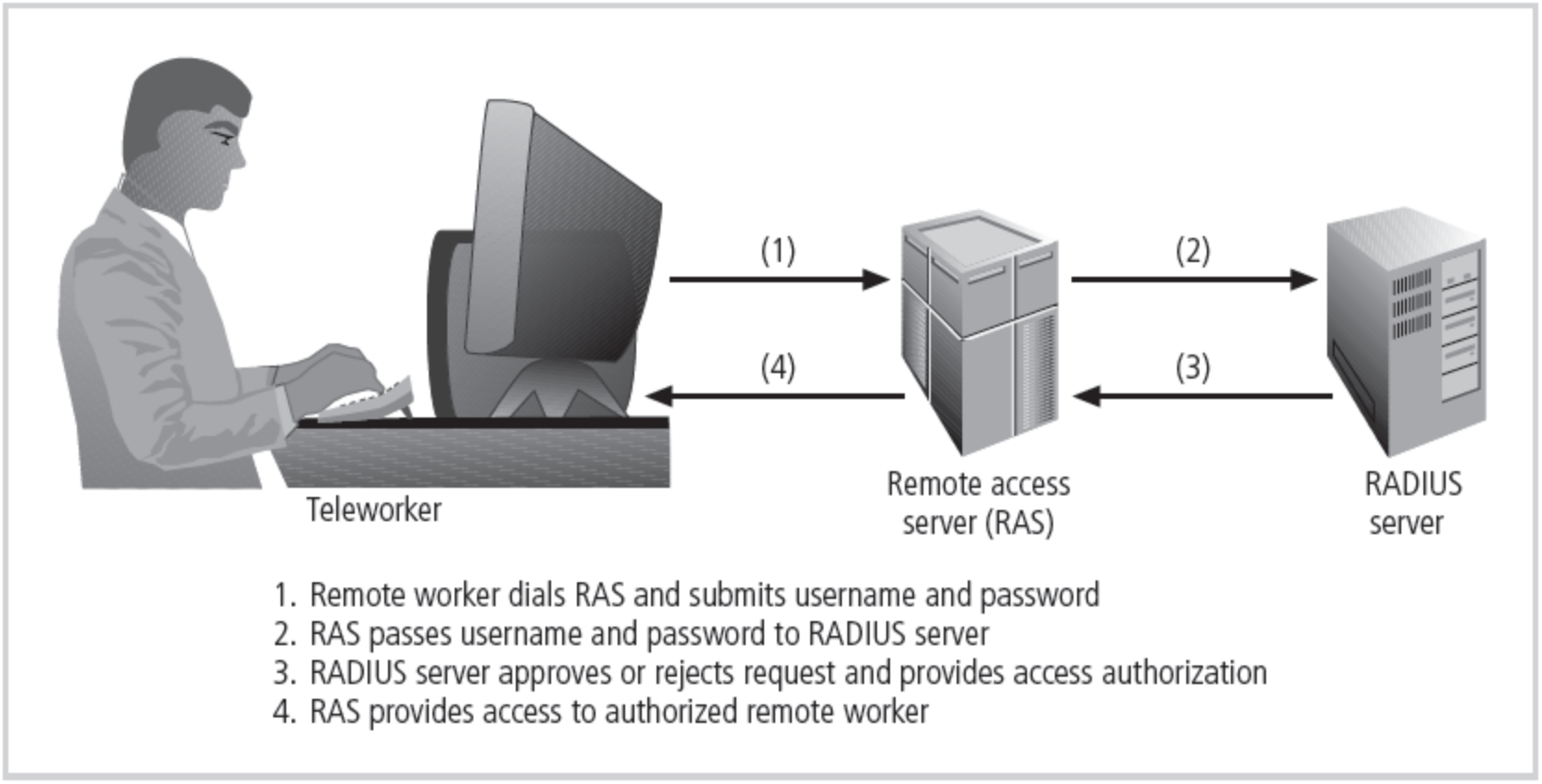

Figure 6-16 RADIUS Configuration

Remote Access (cont'd.)

- Securing authentication with 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

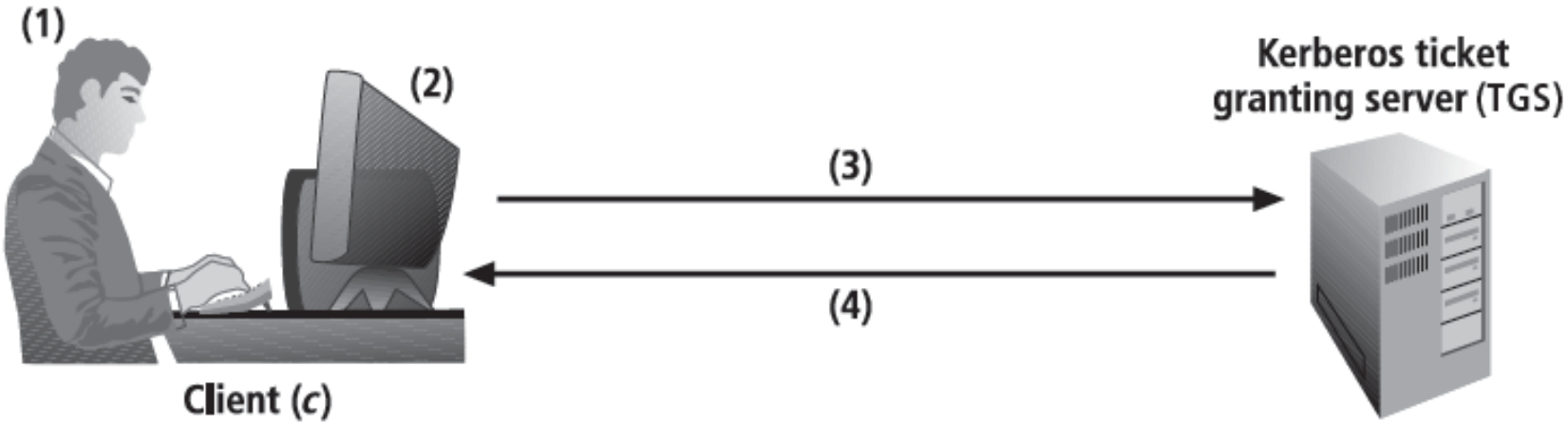

Figure 6-17 Kerberos Login

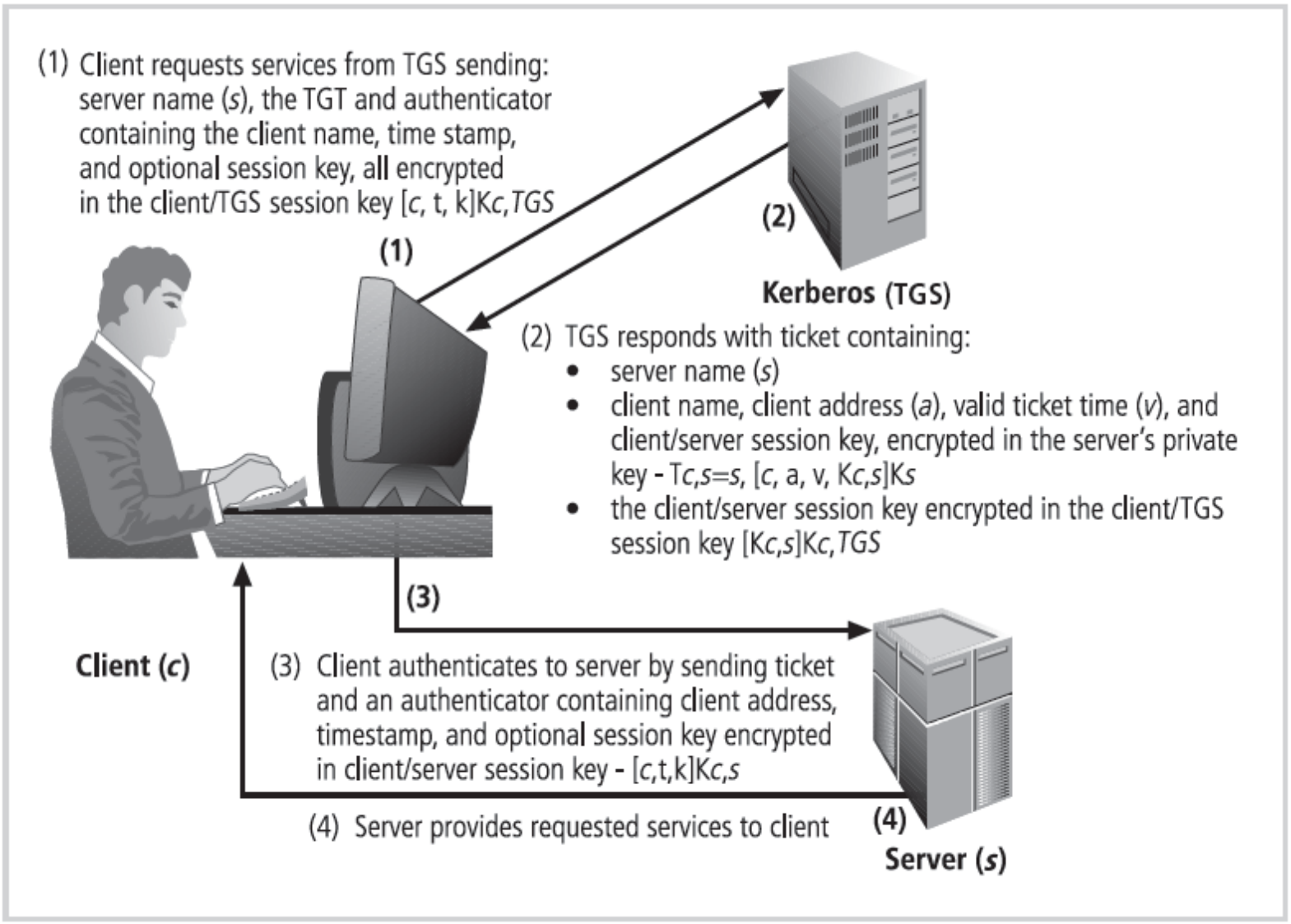

Figure 6-18 Kerberos Request for Services

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 beyond trusted network
- 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

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

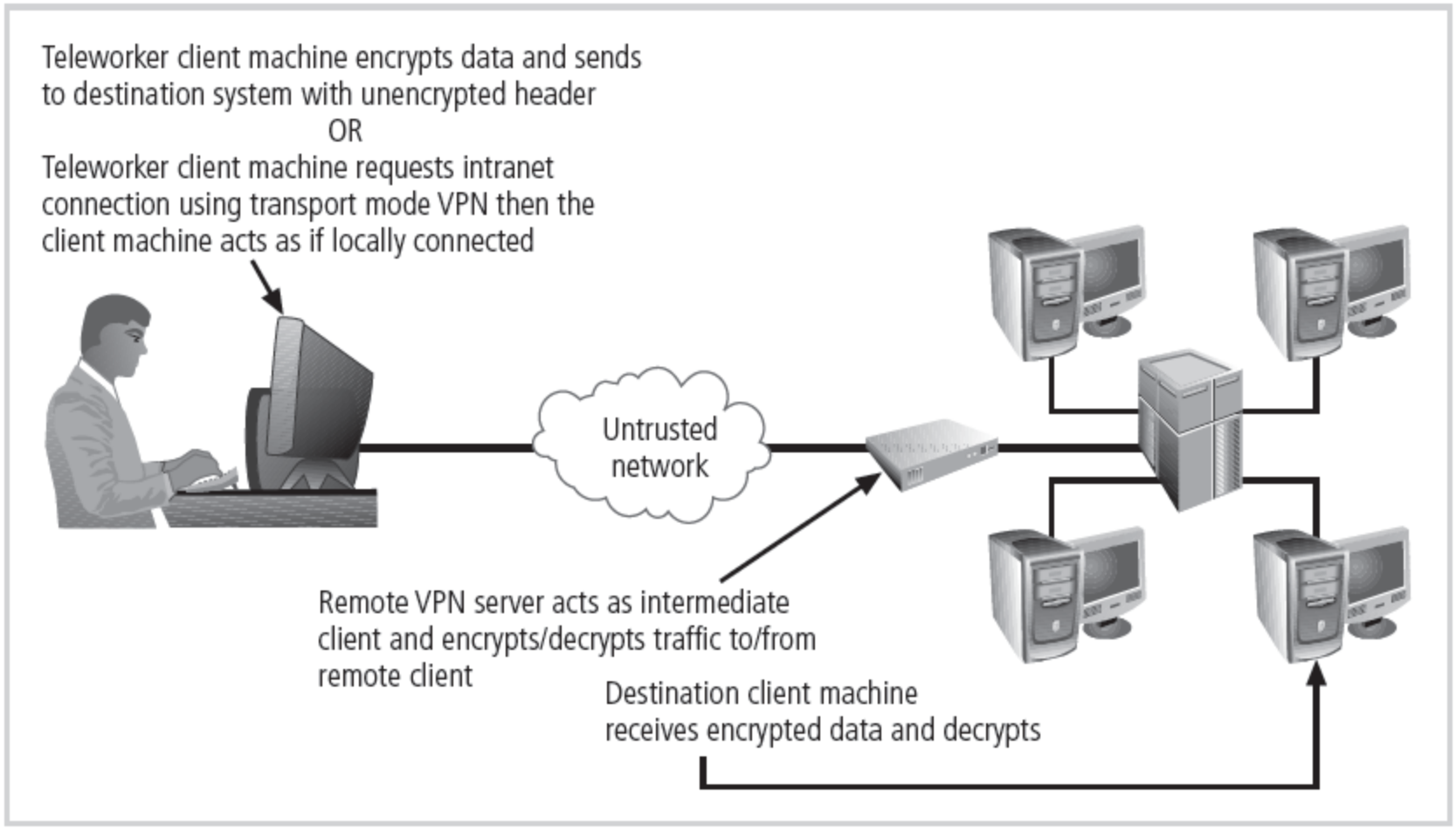

Figure 6-19 Transport Mode VPN

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

- Tunnel mode
  - Organization establishes two perimeter tunnel servers
  - These servers act as encryption points, encrypting all traffic that will traverse unsecured network
  - Primary benefit to this model is that an intercepted packet reveals nothing about true destination system
  - Example of tunnel mode VPN: Microsoft's Internet Security and Acceleration (ISA) Server

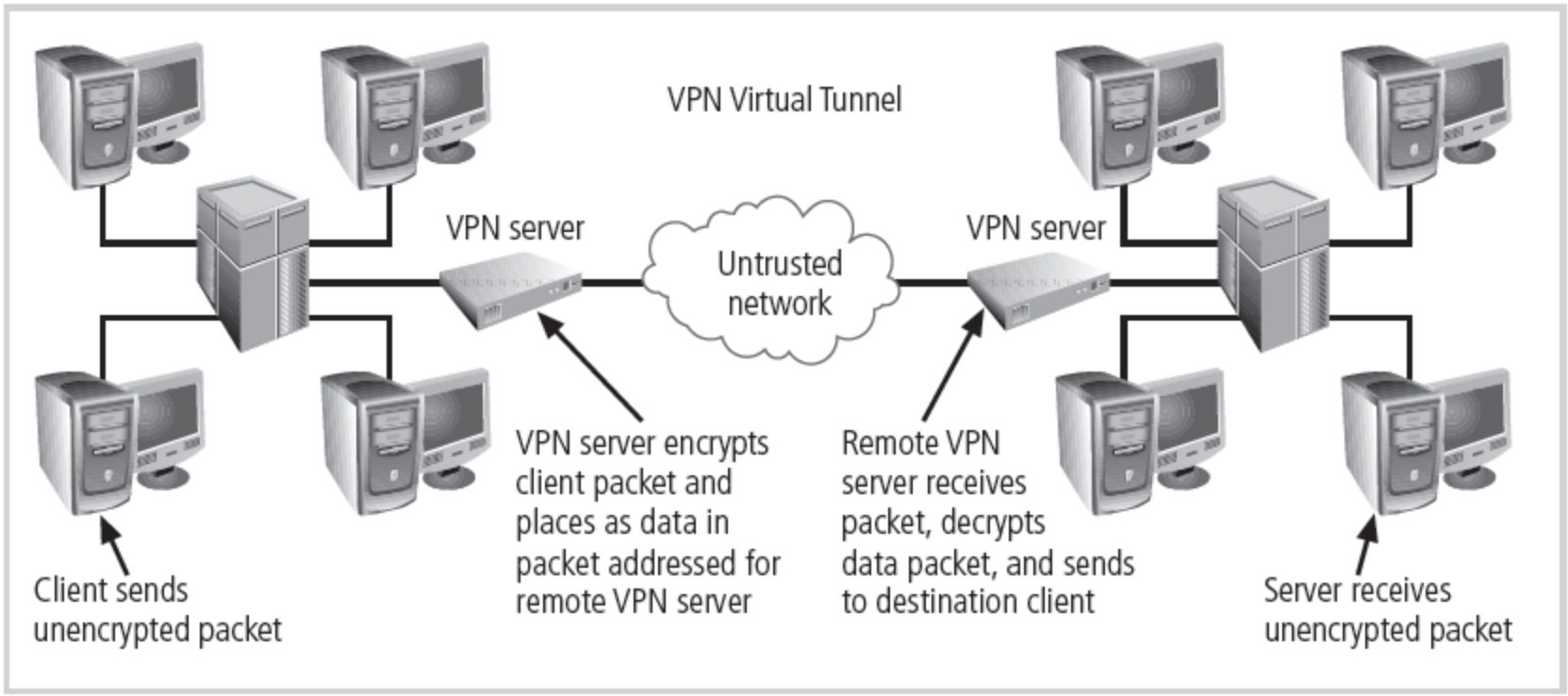

Figure 6-20 Tunnel Mode VPN

Summary

- Firewalls
  - Technology from packet filtering to dynamic stateful inspection
  - Architectures vary with the needs of the network
- Various approaches to remote and dial-up access protection
  - RADIUS and TACACS
- Content filtering technology
- Virtual private networks
  - Encryption between networks over the Internet