COURSE TECHNOLOGY
CENGAGE Learning™

Principals of Information Security, Fourth 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

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

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:
  1. Packet filtering
  2. Application gateways
  3. Circuit gateways
  4. MAC layer firewalls
  5. Hybrids

Firewalls Processing Modes (cont'd.)

Packet filtering firewalls

1. 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

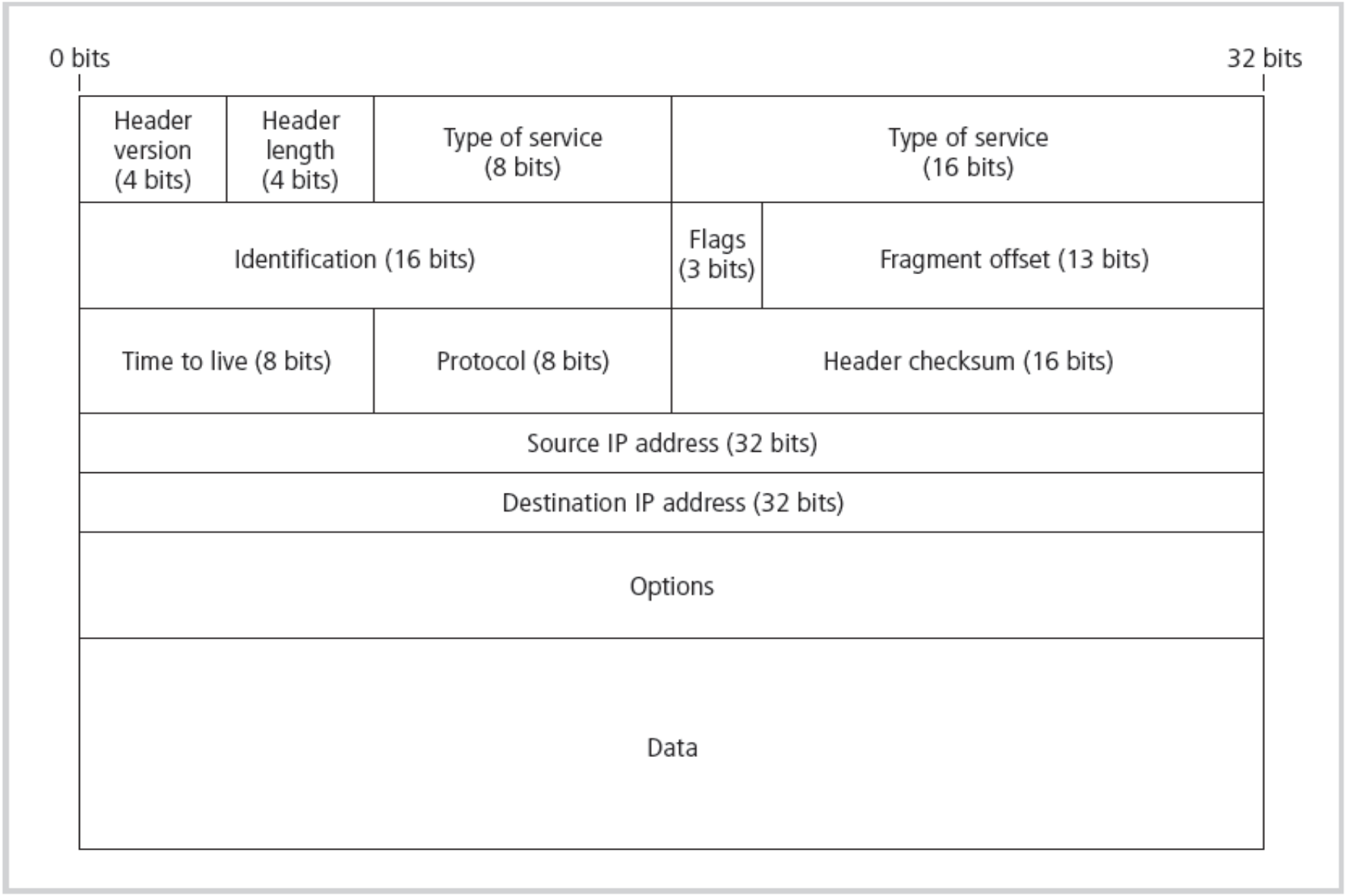

Figure 6-2 IP Packet Structure

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.)

2. 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.)

3. 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.)

4. 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

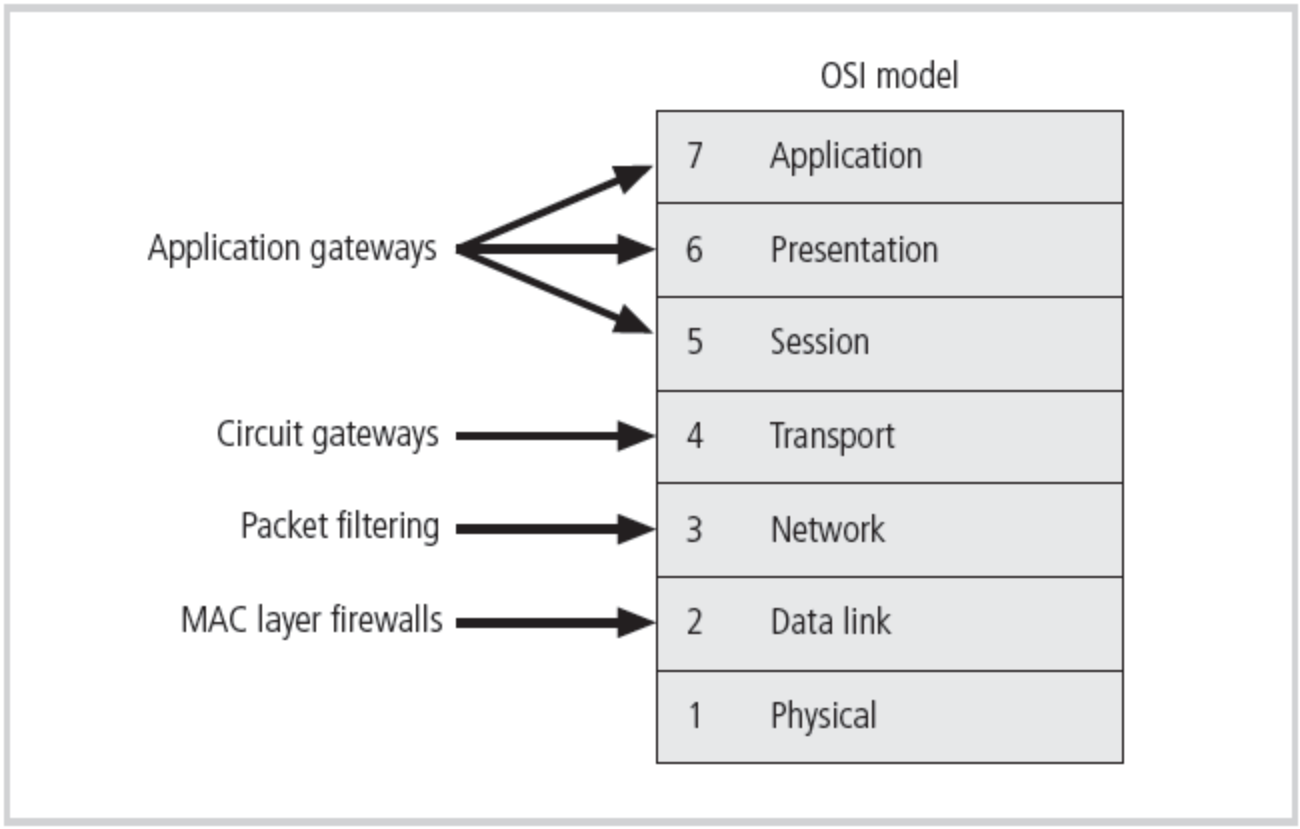

Figure 6-6 Firewall Types and the OSI Model

Firewalls Processing Modes (cont'd.)

5. 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

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

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

- Four common architectural implementations of firewalls:

1. packet filtering routers,
2. screened host firewalls,
3. dual-homed firewalls,
4. screened subnet firewalls

Firewall Architectures (cont'd.)

1. 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

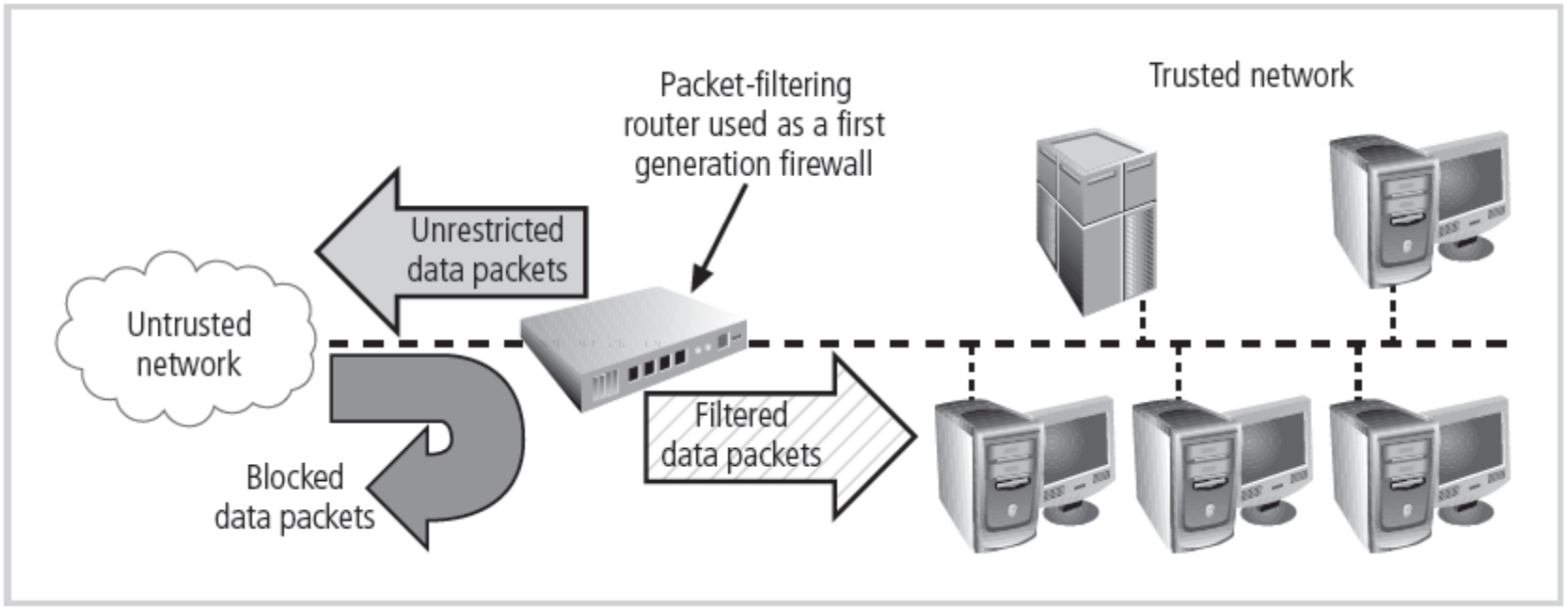

Figure 6-5 Packet-Filtering Router

Firewall Architectures (cont'd.)

2. 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

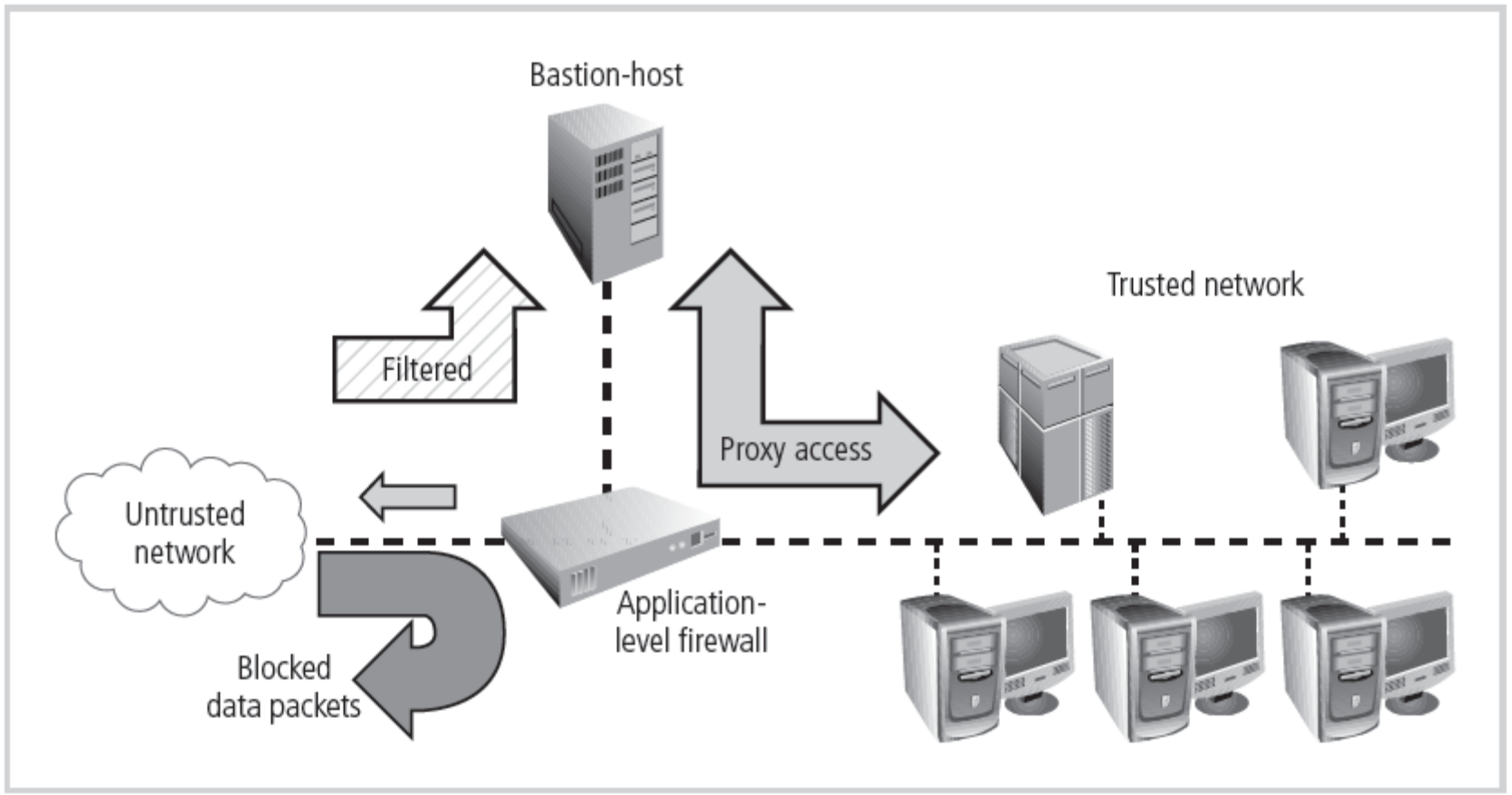

Figure 6-12 Screened Host Firewall

Firewall Architectures (cont'd.)

4. 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

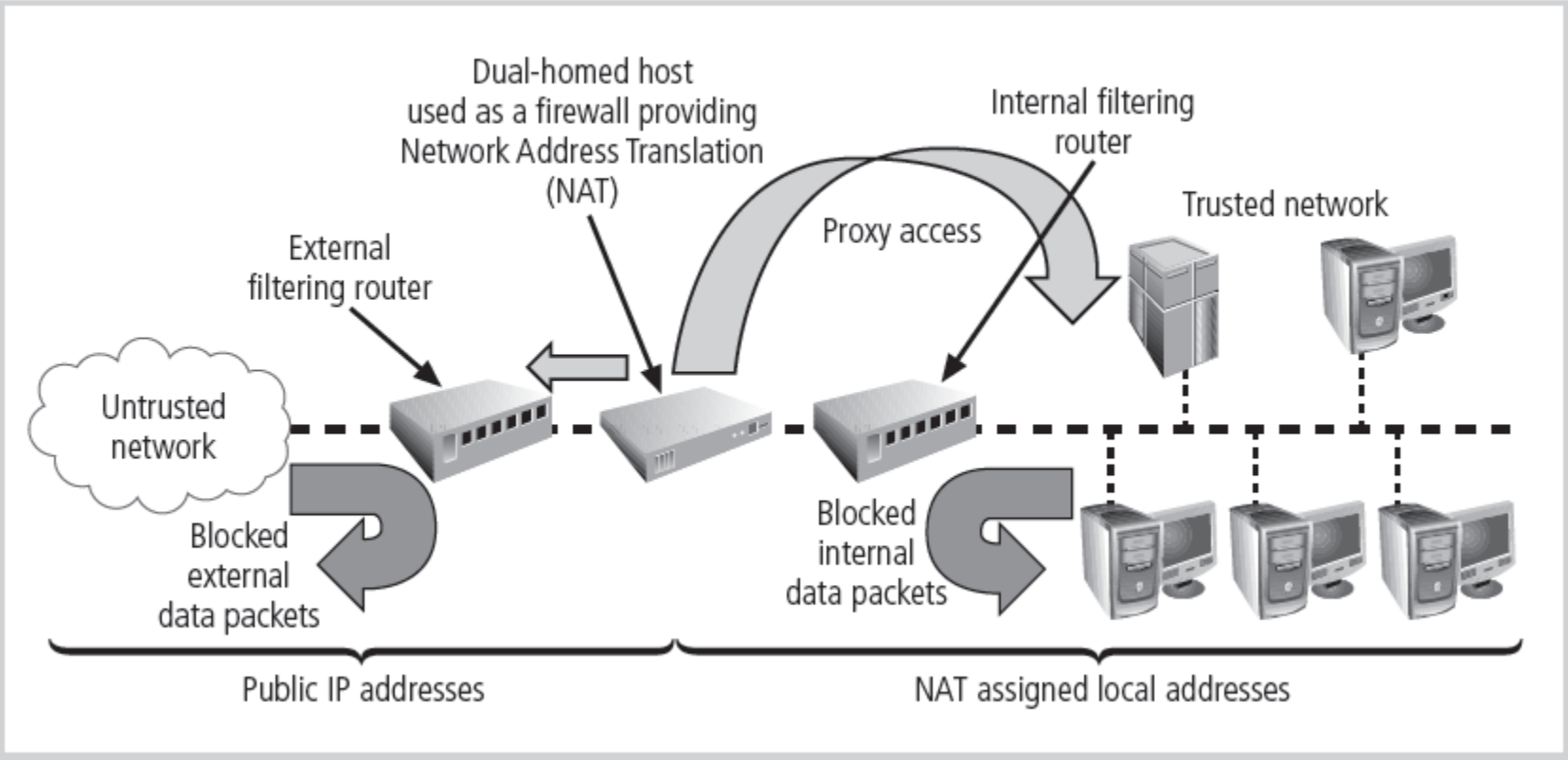

Figure 6-13 Dual-Homed Host Firewall

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

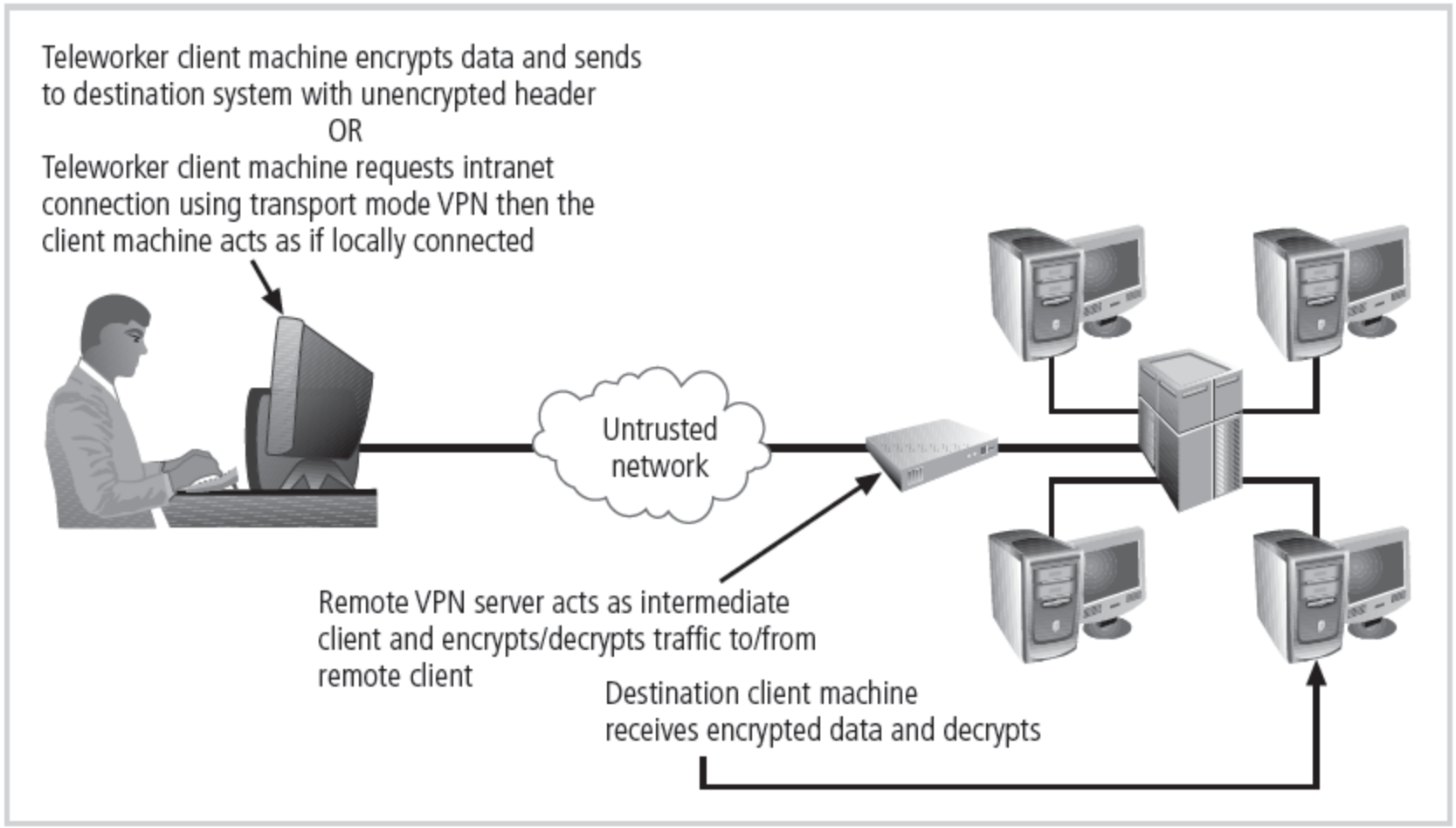

Figure 6-19 Transport Mode VPN

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

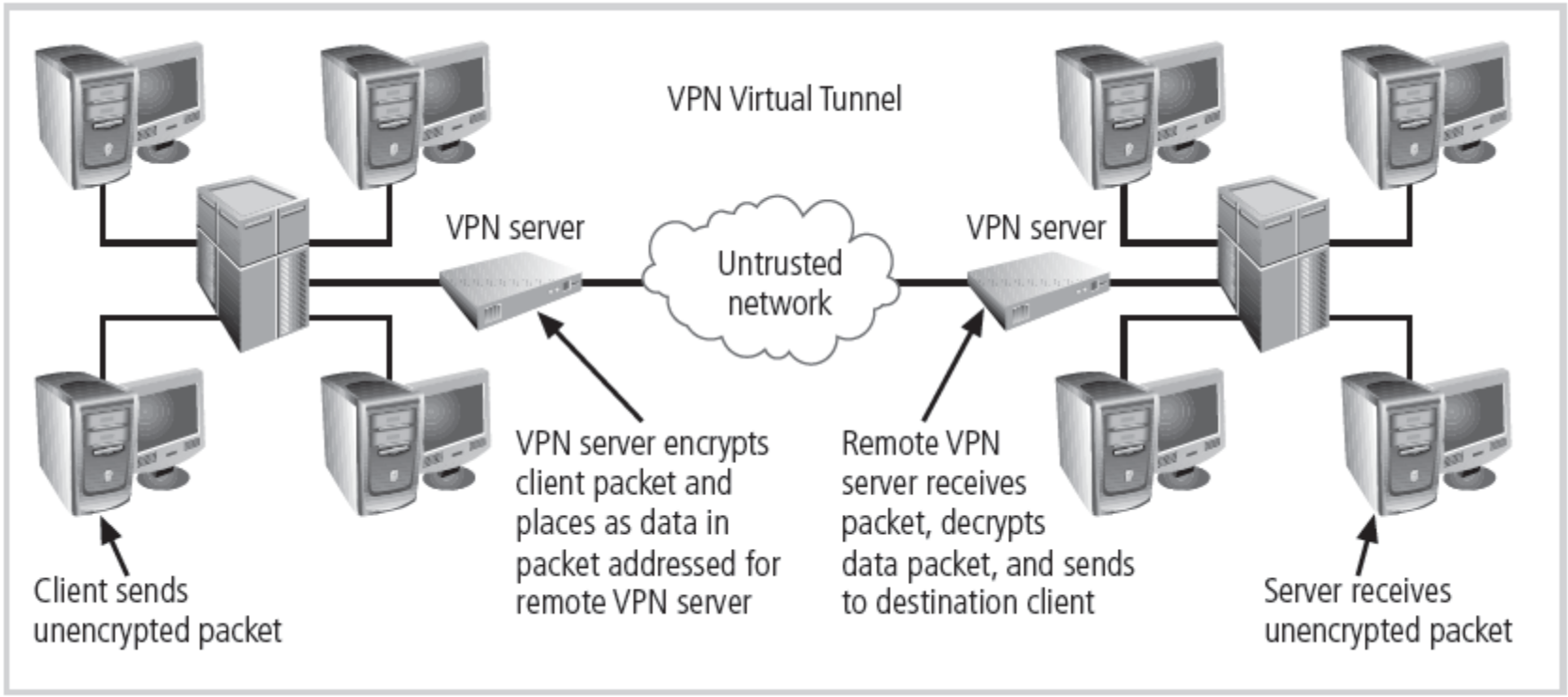

Figure 6-20 Tunnel Mode VPN

Summary

- Firewalls
  - Technology from packet filtering to dynamic stateful inspection
  - Architectures vary with the needs of the network
- Content filtering technology
- Virtual private networks
  - Encryption between networks over the Internet