FIREWALLS & NETWORK SECURITY with Intrusion Detection and VPNs, 2nd ed.

Chapter 5
Firewall Planning and Design

Learning Objectives

- Identify common misconceptions about firewalls
- Explain why a firewall is dependent on an effective security policy
- Discuss what a firewall does
- Describe the types of firewall protection
- Identify the limitations of firewalls
- Evaluate and recommend suitable hardware and software for a firewall application

Introduction

- Networks that connect to the Internet for communications or commerce are perceived as being particularly vulnerable
- Firewalls and associated technical controls have become fundamental security tools
- No security system can ensure with absolute certainty protection of all of an organization's information all of the time
- However, firewalls are one of the most effective security tools that the network administrator has

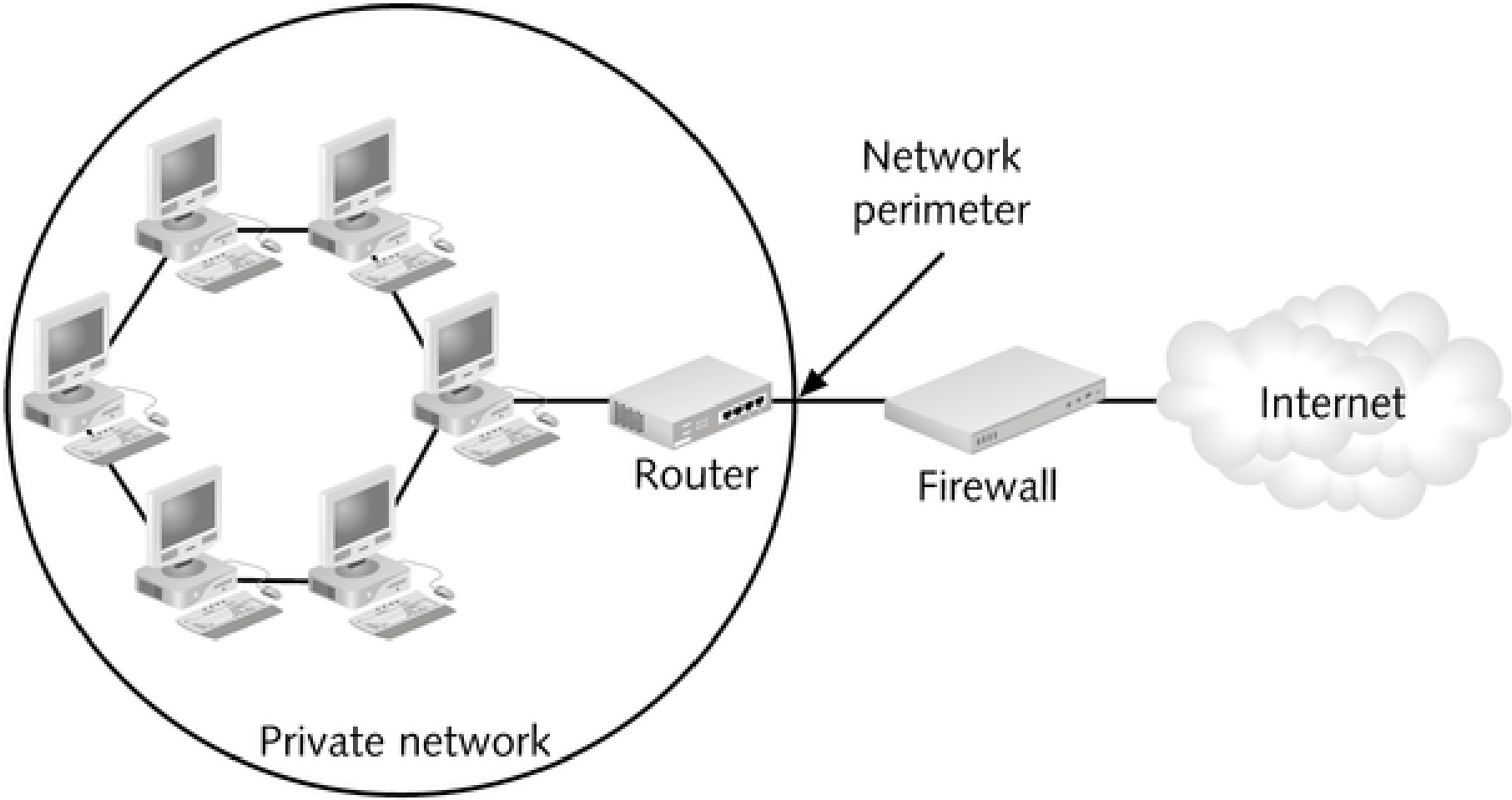
Misconceptions about Firewalls

- Misconception
  - Designed to prevent all hackers, viruses, and would-be intruders from entering
- Reality
  - Enable authorized traffic to pass through
  - Block unauthorized traffic
- Misconception
  - Once deployed, firewalls operate on their own
- Reality
  - Work best when part of defense in depth
  - Need constant maintenance

Firewalls Explained

- Firewall is anything, hardware or software, that monitors transmission of packets of digital information that attempt to pass the perimeter of a network
- Firewalls perform two basic security functions:
  - Packet filtering
  - Application proxy

Firewall at the Perimeter



Firewall Security Features

Some firewall manufacturers add features like:

- Logging unauthorized accesses into/out of a network
- Providing VPN link to another network
- Authenticating users
- Shielding hosts inside the network from hackers
- Caching data
- Filtering content considered inappropriate or dangerous

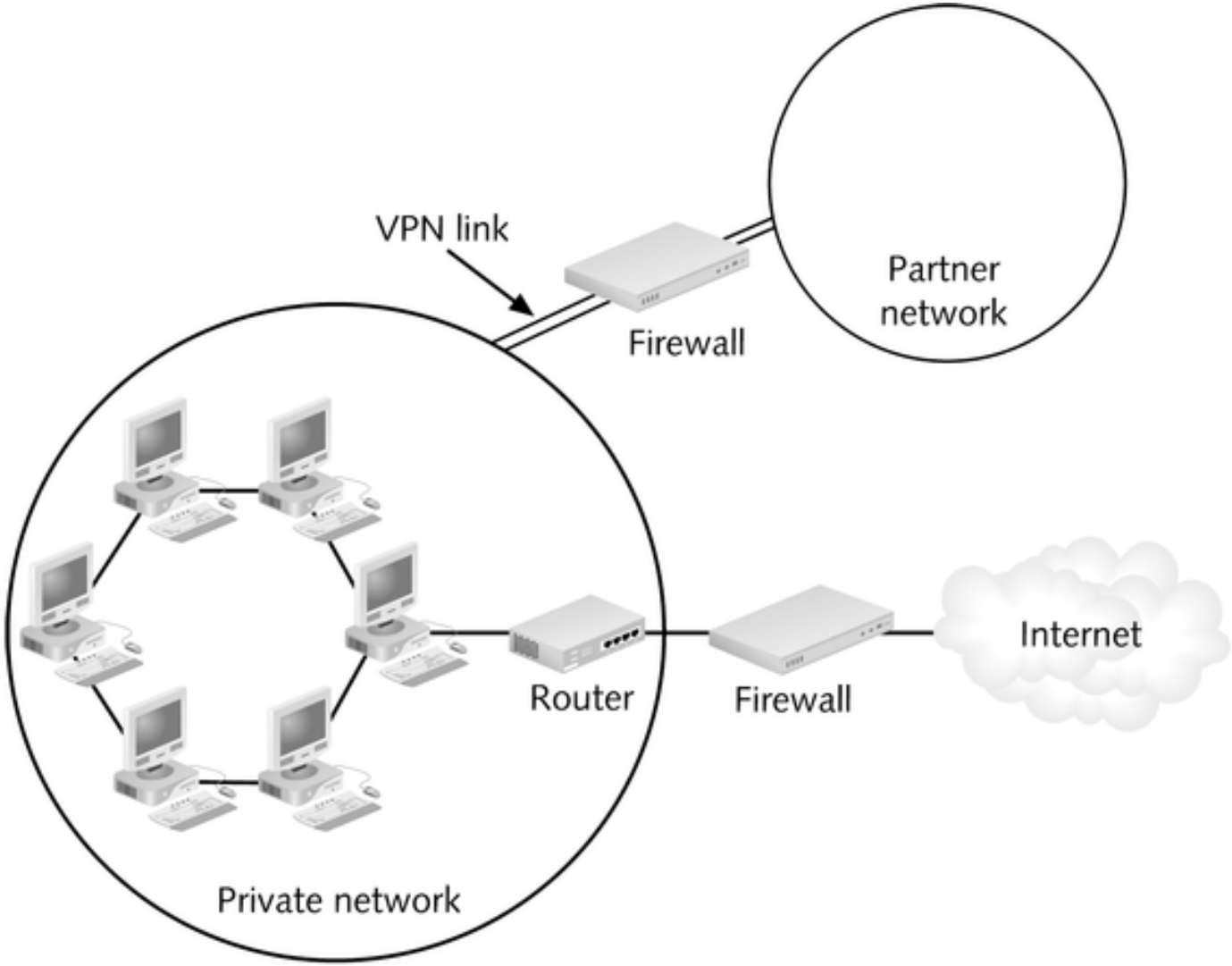
Firewall User Protection

- Keep viruses from infecting files
- Prevent Trojan horses from entering system through back doors

Firewall Network Perimeter Security

- Perimeter is a boundary between two zones of trust; common to install firewall at this boundary to inspect and control traffic that flows across it
- Extranet can extend network to third party, like business partner; if extranet operates over VPN, VPN should have its own perimeter firewall
- To be really secure, a firewall should be installed on partner's VPN host

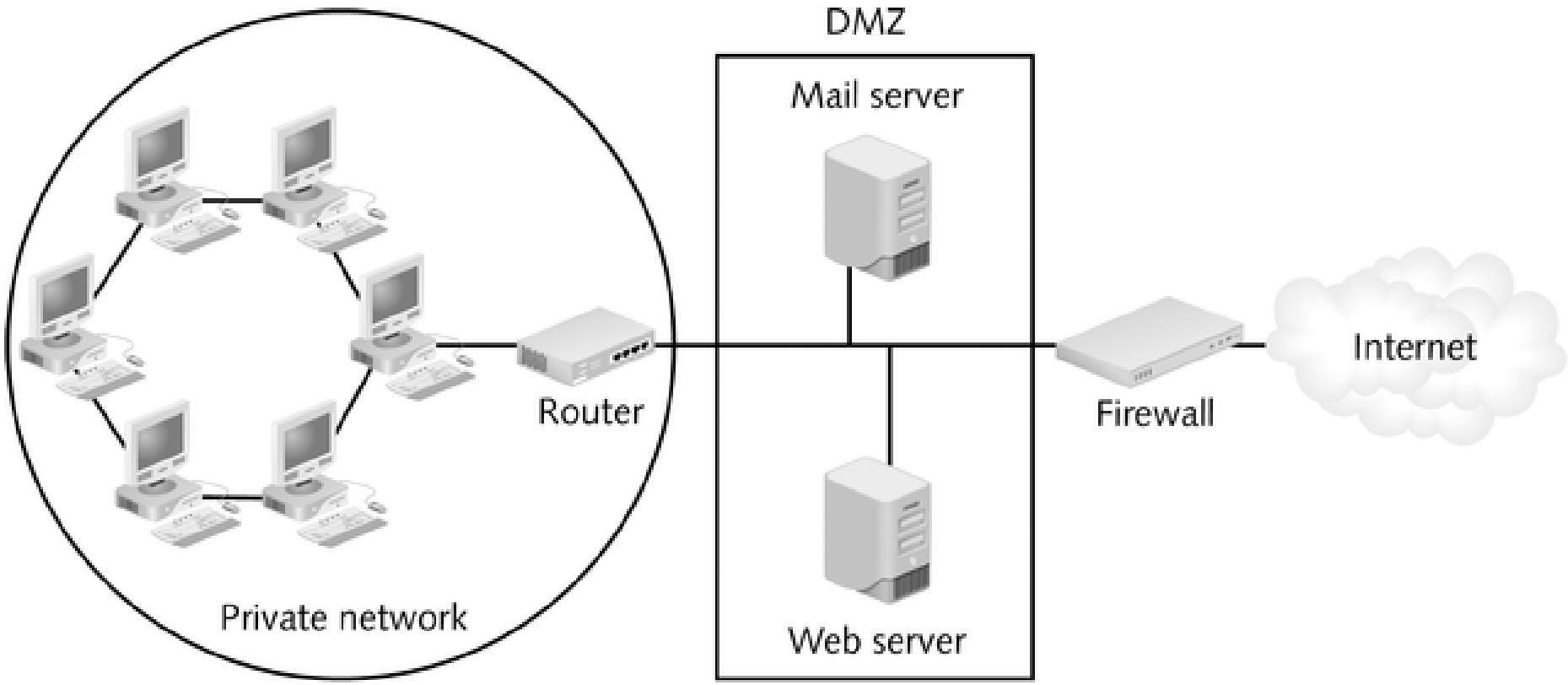
VPN Perimeter



Firewall Components

- Packet filter
- Proxy server
- Authentication system
- Software that performs Network Address Translation (NAT)
- Some firewalls:
  - Can encrypt traffic
  - Help establish VPNs
  - Come packaged in a hardware device that also functions as a router
  - Make use of a bastion host

DMZ Networks



Firewall Security Tasks

- Restrict access from outside networks using packet filtering
  - Firewall that does packet filtering protects networks from port scanning attacks
  - Port numbers come in two flavors: well-known ports (1023 and below) defined for most common services and ephemeral ports (1024 through 65535)
  - Exposed network services are one of the biggest vulnerabilities that firewalls can protect against

Firewall Security Tasks (continued)

- Restrict unauthorized access from inside network (e.g., social engineering)
  - Firewalls can help prevent some, but not all, internal threats
  - Firewall can be configured to recognize packets or to prevent access to protected files from internal as well as external hosts

Firewall Security Tasks (continued)

- Give clients limit access to external hosts by acting as proxy server
  - Firewalls can selectively permit traffic to go from inside the network to the Internet or other networks to provide more precise control of how employees inside the network use external resources
  - Application proxies can restrict internal users who want to gain unrestricted access to the Internet

Firewall Security Tasks (continued)

- Protecting critical resources against attacks (e.g., worms, viruses, Trojan horses, and DDoS attacks)
  - A worm can replicate itself, whereas a virus requires a software environment in order to run on a computer, infect it, and spread
  - Trojan horses contain malicious code that is hidden inside supposedly harmless programs
  - Distributed denial-of-service (DDoS) attacks flood a server with requests coming from many different sources controlled by an attacker

Firewall Security Tasks (continued)

- Protect against hacking, which can affect:
  - Loss of data
  - Loss of time
  - Staff resources
  - Confidentiality

Firewall Security Tasks (continued)

- Provide centralization
- Enable documentation to:
  - Identify weak points in security system so it can be strengthened
  - Identify intruders so they can be apprehended
- Provide for authentication
- Contribute to a VPN

Types of Firewall Protection

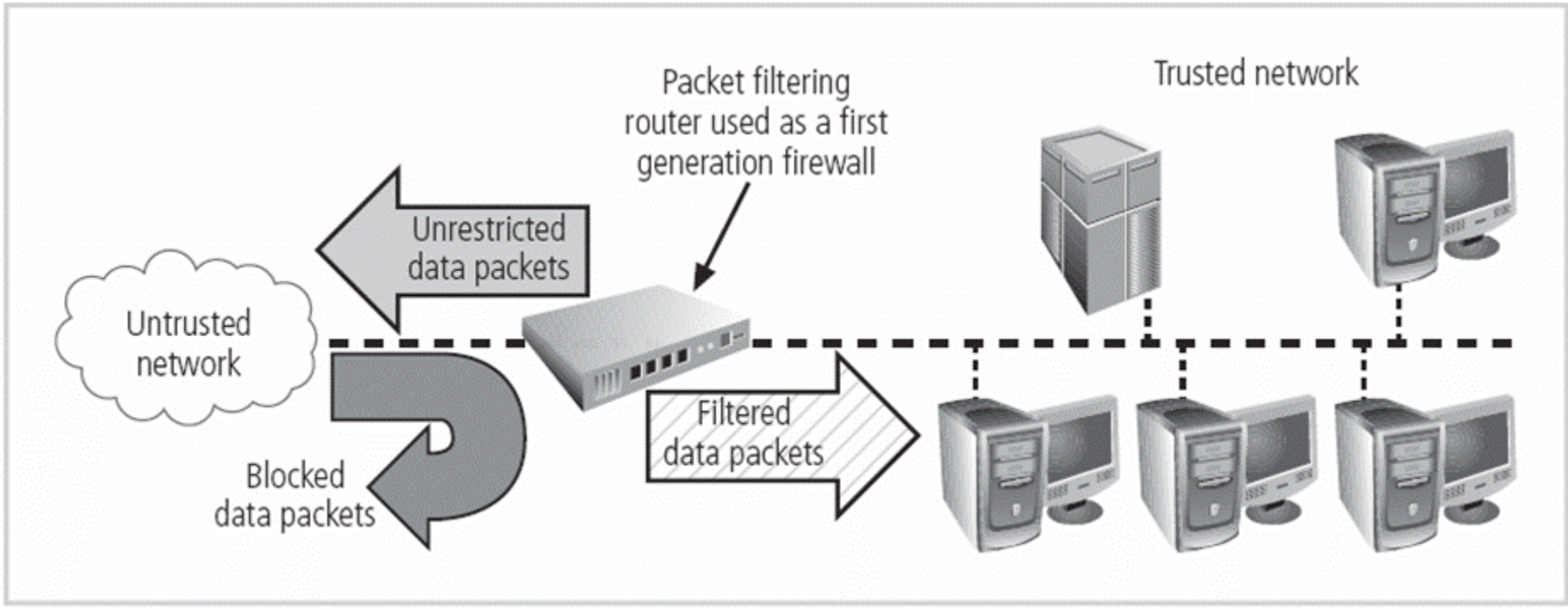
- Multilayer firewall protection

Layer Number	OSI Reference Model Layer	Firewall Functions
1	Application	Application-level gateway
2	Presentation	Encryption
3	Session	SOCKS proxy server
4	Transport	Packet filtering
5	Network	NAT
6	Physical	N/A
7	Data Link	N/A

Types of Firewall Protection (continued)

- Packet filtering
  - Packet filtering firewalls scan network data packets looking for compliance with, or violation of, rules of firewall's database
  - Restrictions most commonly implemented in packet filtering firewalls are based on:
    - IP source and destination address
    - Direction (inbound or outbound)
    - TCP or UDP source and destination port

Packet-Filtering Router



Stateless Packet Filtering

- Firewall inspects packet headers without paying attention to state of connection between server and client computer
- Packet is blocked based on information in header
- Also called stateless inspection

Stateful Packet Filtering

- Examines data contained in packet; superior to stateless inspection
- Keeps memory of state of connection between client and server in disk cache
- Detects and drops packets that overload server
- Blocks packets sent by host not connected to server
- Also called stateful inspection

State Table Entries

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

Packet-Filtering Rules

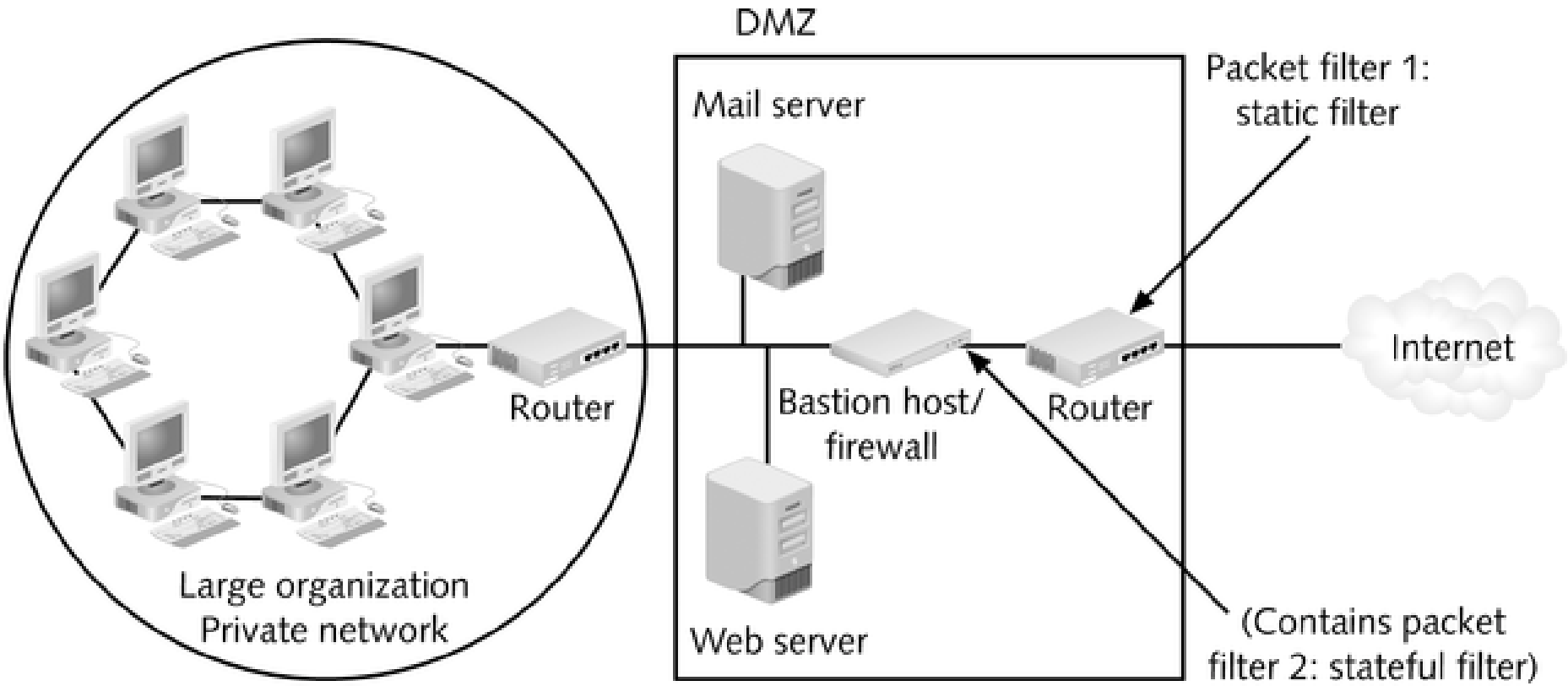
Common rules include:

- Any outbound packet:
  - Must have source address in internal network
  - Must *not* have destination address in internal network
- Any inbound packet:
  - Must *not* have source address in internal network
  - Must have destination address in internal network

Packet-Filtering Rules (continued)

- Any packet that enters/leaves your network must have source/destination address that falls within range of addresses in your network
- Include the use of:
  - Internet Control Message Protocol (ICMP)
  - User Datagram Program (UDP)
  - TCP filtering
  - IP filtering

Using Multiple Packet Filters in a DMZ



PAT and NAT

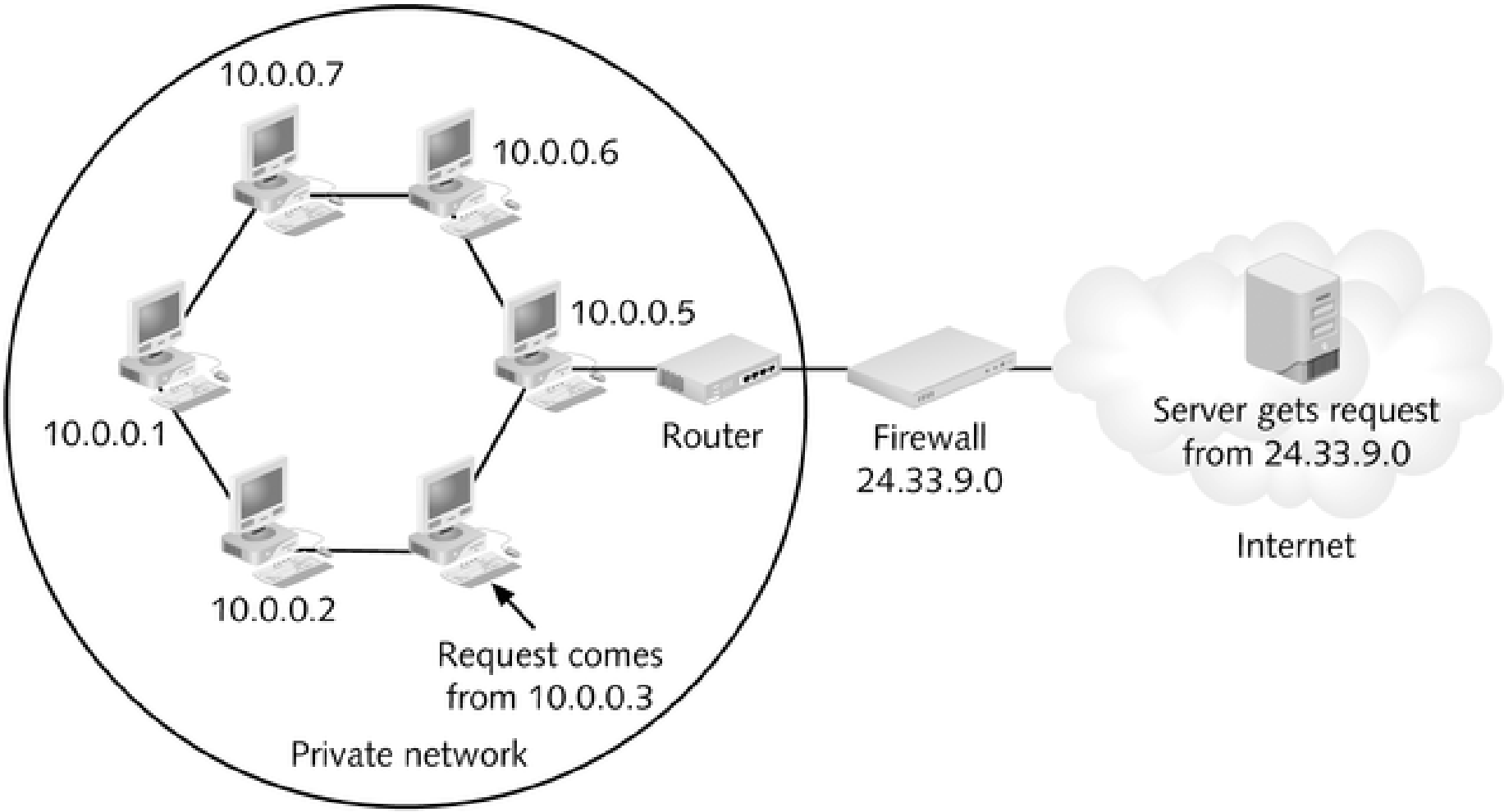
- Function as network-level proxy; convert IP addresses of internal hosts to IP address assigned by firewall
  - PAT uses one external address for all internal systems, assigning random and high-order port numbers to each internal computer
  - NAT uses pool of valid external IP addresses, assigning one of these actual addresses to each internal computer requesting an outside connection

PAT and NAT (continued)

- Hide TCP/IP information of hosts in the network being protected, preventing hackers from getting address of actual host

Class	From	To	CIDR Mask	Decimal Mask
Class "A" or 24 Bit	10.0.0.0	10.255.255.255	/8	255.0.0.0
Class "B" or 20 Bit	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	192.168.0.0	192.168.255.255	/16 or /24	255.255.0.0 or 255.255.255.0

PAT and NAT (continued)



Application Layer Gateways

- Can control how applications inside the network access the outside world by setting up proxy services
- Act as substitute for the client; shield individual users from directly connecting with the Internet
- Provide a valuable security benefit:
  - Understand contents of requested data
  - Can be configured to allow or deny specific content
- Also called a proxy server

Application-Level Security Techniques

- Load balancing
- IP address mapping
- Content filtering
- URL filtering

Firewall Categorization Methods

- Firewalls can be categorized by:
  - Processing mode
  - Development era
  - Intended structure

Firewall Categories: Processing Mode

- The processing modes are:
  - Packet filtering
  - Application gateways
  - Circuit gateways
  - MAC layer firewalls
  - Hybrids

Packet Filtering

- As described earlier, packet-filtering firewalls examine header information of data packets
- Three subsets of packet-filtering firewalls:
  - Static filtering: requires that filtering rules governing how firewall decides which packets are allowed and which are denied are developed and installed
  - Dynamic filtering: allows firewall to react to an emergent event and update or create rules to deal with event
  - Stateful inspection: keeps track of each network connection between internal and external systems using a state table

Application Gateways

- Frequently installed on a dedicated computer
- Also known as application-level firewall, proxy server, or application firewall

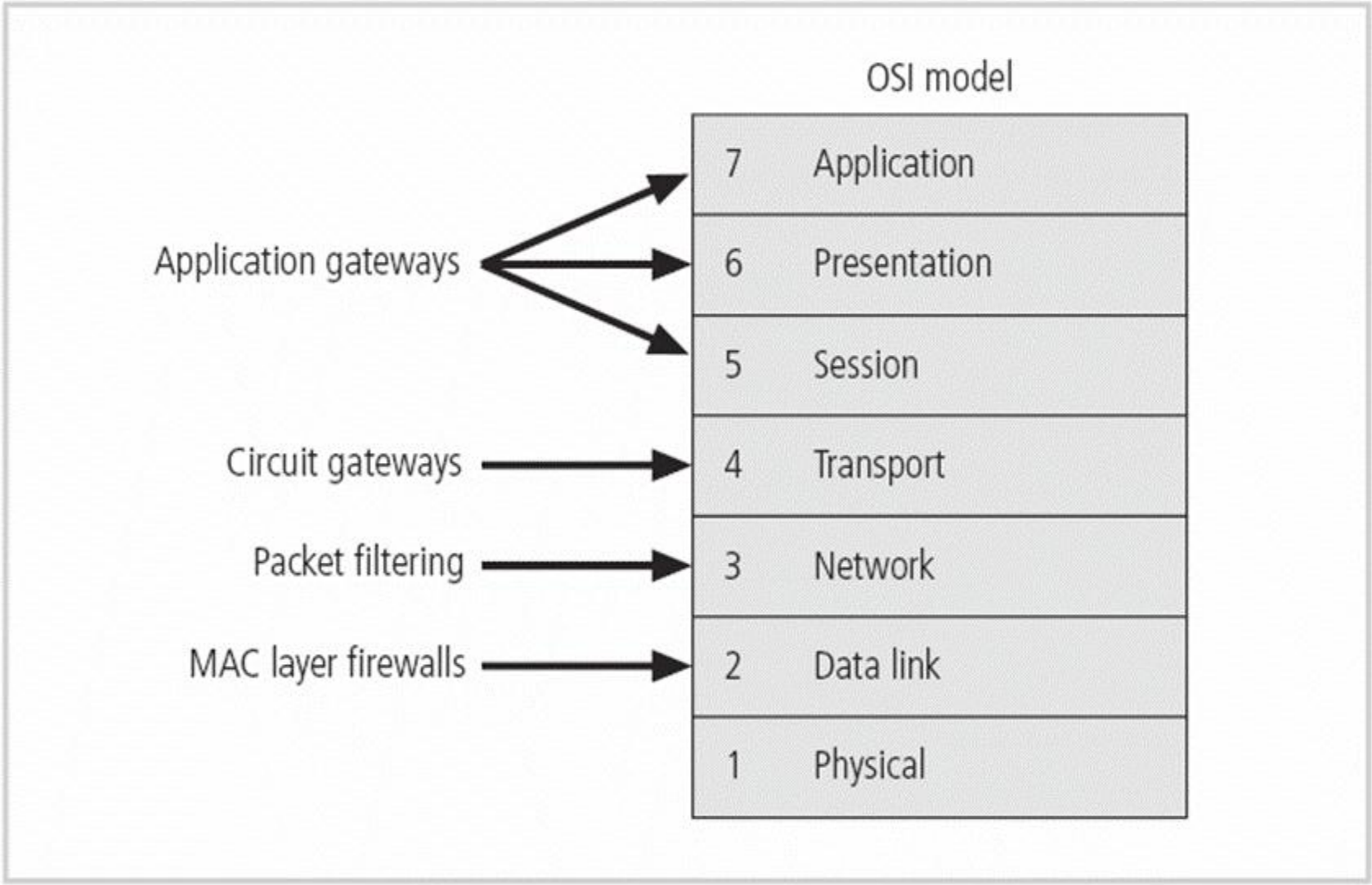
Circuit Gateways

- Operate at the transport layer
- Connections authorized based on addresses
- Like filtering firewalls, do not usually look at data traffic flowing between one network and another but do prevent direct connections between one network and another
- Accomplish this by creating tunnels connecting specific processes or systems on each side of firewall and then allowing only authorized traffic, such as a specific type of TCP connection for only authorized users, in these tunnels

MAC Layer Firewalls

- Designed to operate at the media access control layer of the OSI network model
- This gives these firewalls the ability to consider specific host computer's identity in its filtering decisions
- Using this approach, MAC addresses of specific host computers are linked to ACL entries that identify specific types of packets that can be sent to each host, and all other traffic is blocked

Firewalls in the OSI Model



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, hybrid firewall system may actually consist of two separate firewall devices; each a separate firewall system but connected so they work in tandem

Firewall Categories: Development 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
- Fifth generation: kernel proxies

Firewall Categories: Structure

- Firewall appliances are stand-alone, self-contained systems
- Commercial-grade firewall system consists of firewall application software running on a general-purpose computer
- SOHO or residential-grade firewall devices connect user's local area network or a specific computer system to the Internet device
- Residential-grade firewall software is installed directly on user's system

SOHO Firewall Devices

Software vs. Hardware: The SOHO Firewall Debate

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

Firewall Architectures

- Each of the firewall devices noted earlier can be configured in a number of architectures
- Architecture that works best for a particular organization depends on:
  - Objectives of the network
  - Organization's ability to develop and implement the architectures
  - Budget available for the function

Firewall Architectures (continued)

- Hundreds of variations exist, but four common architectural implementations of firewalls dominate:
  - Packet-filtering routers
  - Screened host firewalls
  - Dual-homed firewalls
  - Screened subnet firewalls

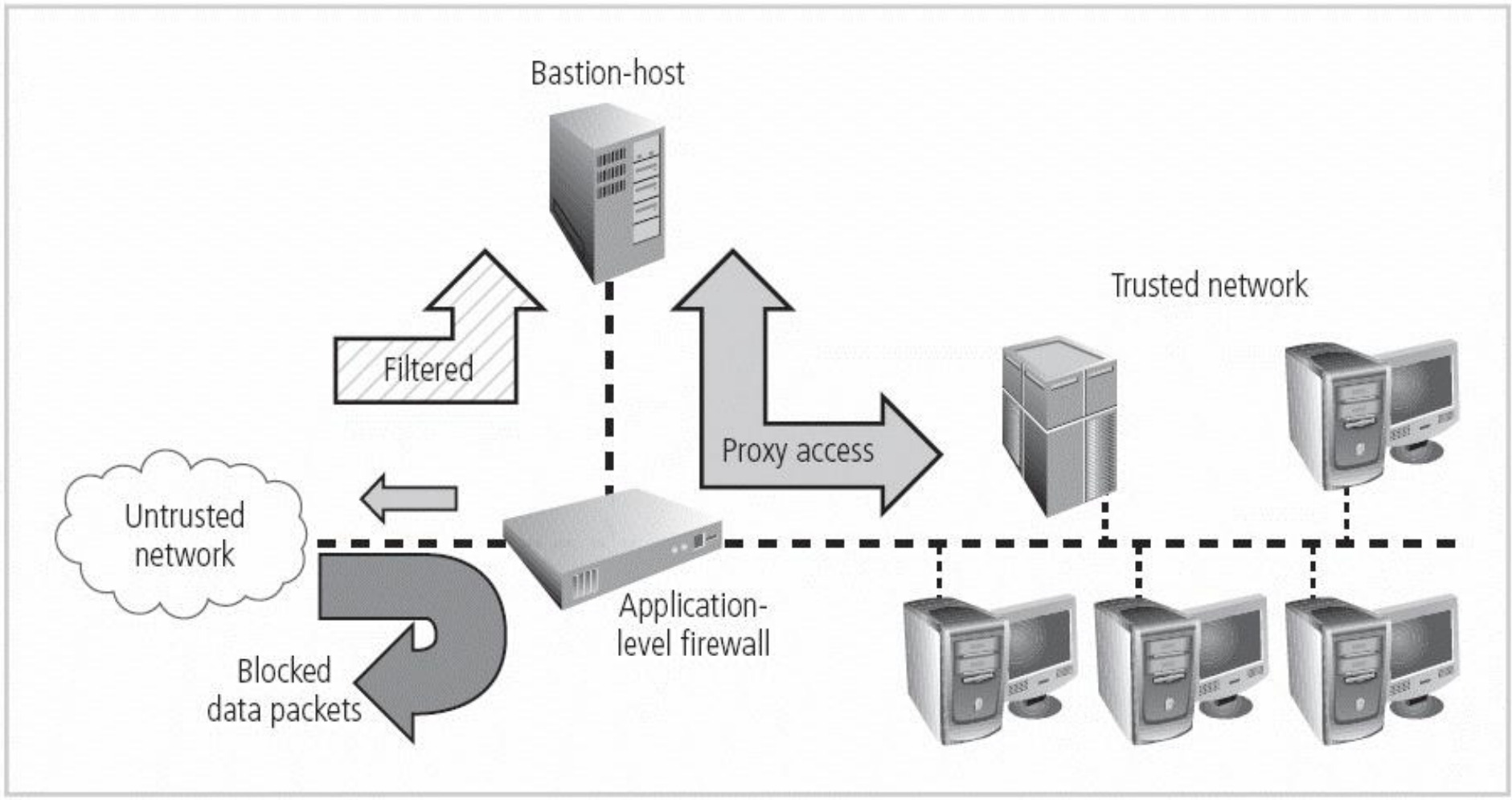
Packet-Filtering Routers

- Most organizations with an Internet connection have a router as the interface to the Internet at the perimeter
- Many of these routers can be configured to reject packets that the organization does not allow into the network
- Drawbacks to this type of system include a lack of auditing and strong authentication and the fact that complexity of the access control lists used to filter the packets can grow and degrade network performance

Screened Host Firewalls

- Combines packet-filtering router with separate, dedicated firewall; like application proxy server
- Application proxy examines application layer protocol and performs proxy services
- This separate host is often referred to as a bastion host or sacrificial host; it can be a rich target for external attacks and should be very thoroughly secured

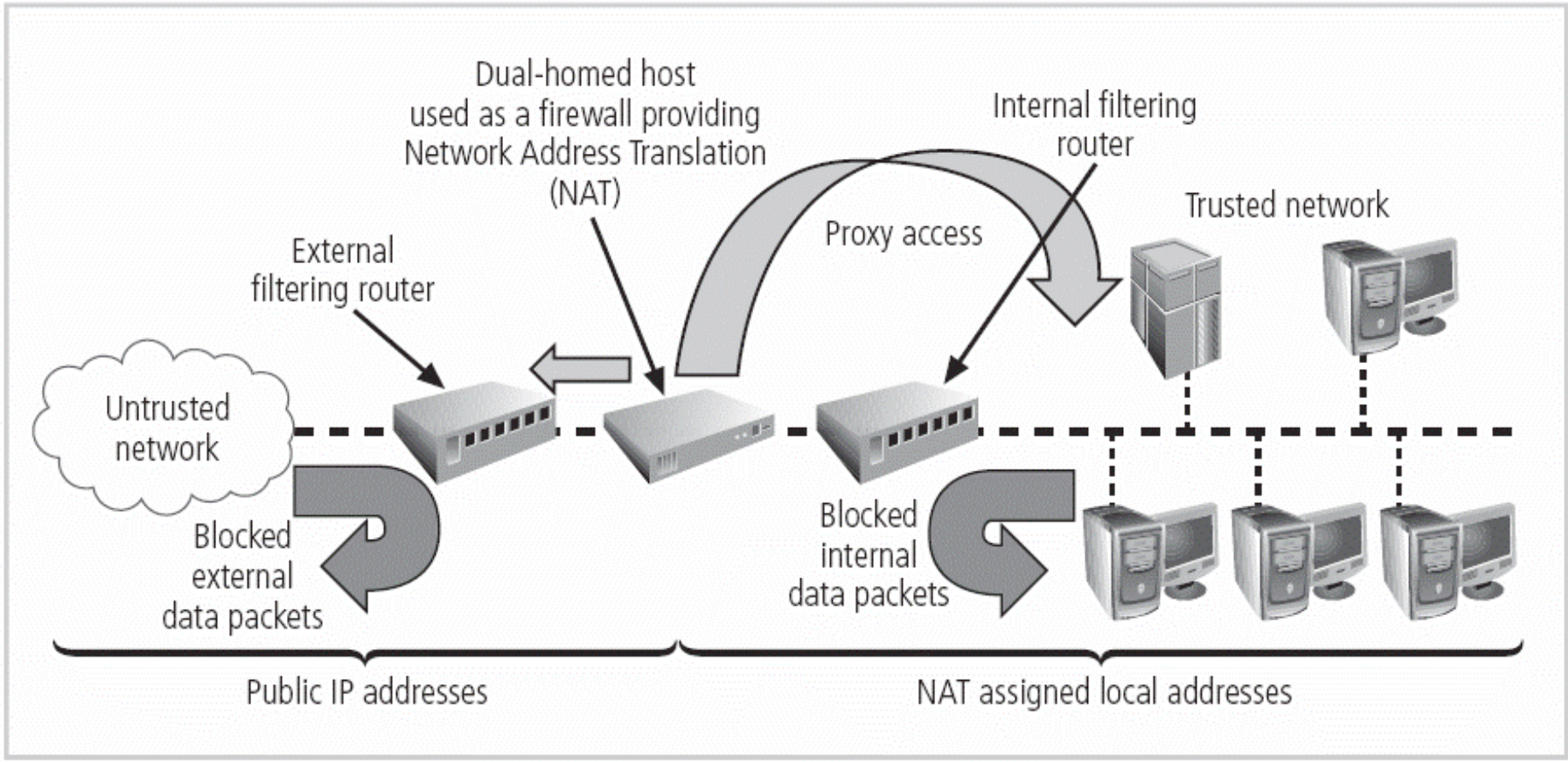
Screened Host Architecture



Dual-Homed Host Firewalls

- Bastion host contains two NICs: one connected to external network and one connected to internal network
- Implementation of this architecture often makes use of NAT by mapping assigned IP addresses to special ranges of non-routable internal IP addresses, creating yet another barrier to intrusion from external attackers

Dual-Homed Host Architecture



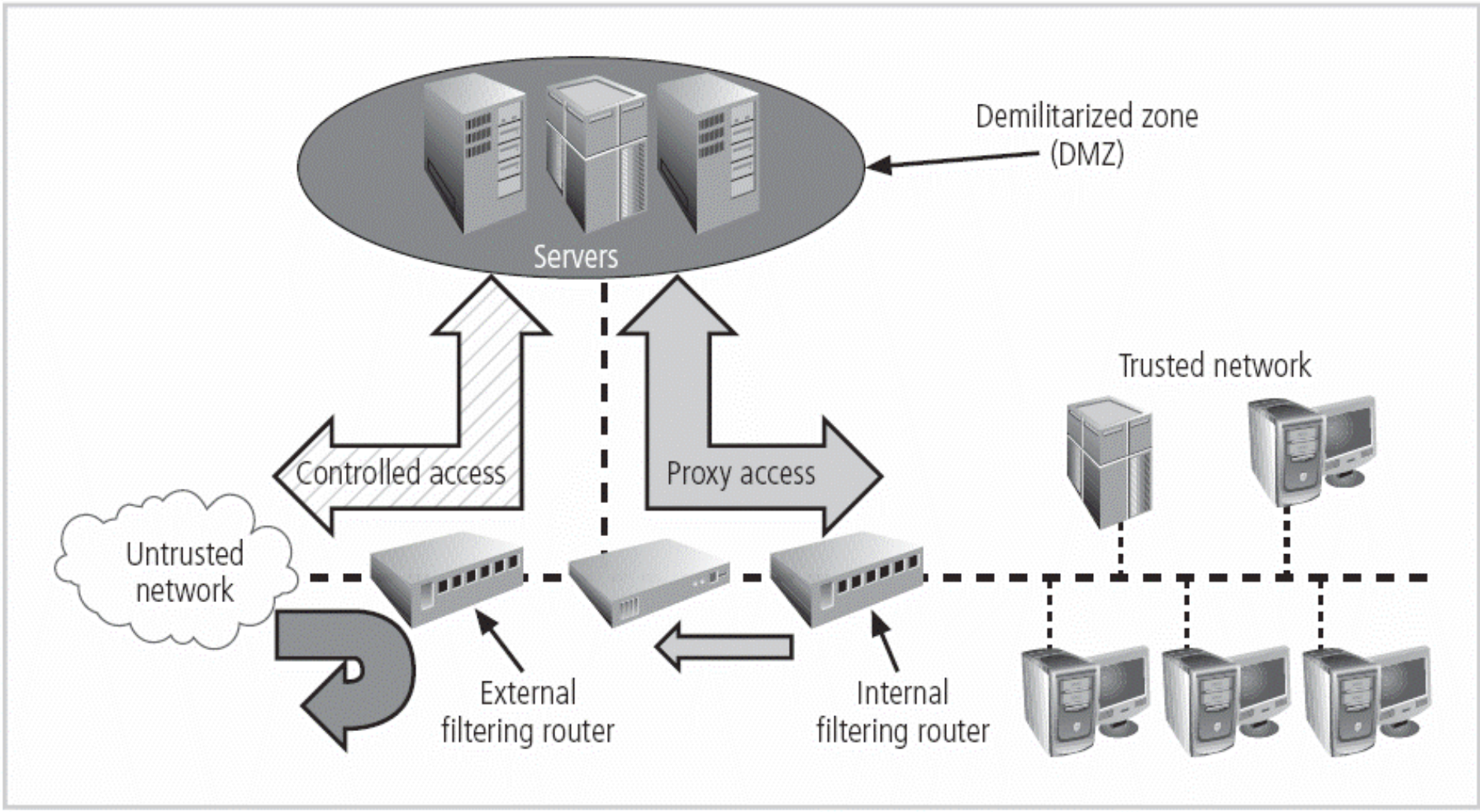
Screened Subnet Firewalls (with DMZ)

- Dominant architecture used today
- Common arrangement consists of two or more internal bastion hosts behind a packet-filtering router, with each host protecting the trusted network:
  - Connections from outside or untrusted network are routed through an external filtering router
  - Connections from outside or untrusted network are routed into—and then out of—a routing firewall to separate network segment known as the DMZ
  - Connections into trusted internal network are allowed only from the DMZ bastion host servers

Screened Subnet Firewalls (with DMZ) (continued)

- Screened subnet is an entire network segment that performs two functions:
  - Protects DMZ systems and information from outside threats by providing a network of intermediate security
  - Protects internal networks by limiting how external connections can gain access to internal systems
- DMZs can also create extranets—segments of the DMZ where additional authentication and authorization controls are put into place to provide services that are not available to the general public

Screened Subnet (with DMZ)



Limitations of Firewalls

- Should be part of an overall security plan, not the *only* form of protection for a network
- Should be used in conjunction with other forms of protection (e.g., ID cards, passwords, employee rules of conduct)

Chapter Summary

- Network security is a process that imposes controls on network resources to balance risks and rewards from network usage
- Firewall: anything that filters data packet transmission as it crosses network boundaries
  - Perform two basic security functions: packet filtering and/or application proxying
  - Can contain many components, including packet filter, proxy server, authentication system, and software
  - Some can encrypt traffic, help establish VPNs

Chapter Summary (continued)

- Packet-filtering firewall: stateless or stateful
- Stateless packet filtering ignores connection state between internal and external computer
- Stateful packet filtering examines packet data with memory of connection state between hosts
- Port Address Translation (PAT) and Network Address Translation (NAT) are addressing methods that hide internal network addresses
- Application layer gateways (proxy servers) control how internal network applications access external networks by setting up proxy services

Chapter Summary (continued)

- Firewalls can be categorized by:
  - Processing mode: packet filtering, application gateway, circuit gateway, MAC layer, hybrid
  - Generation: level of technology; later ones being more complex and more recently developed
  - Structure: residential- or commercial-grade, hardware-, software-, or appliance-based
- Four common architectural implementations of firewalls: packet-filtering routers, screened host firewalls, dual-homed firewalls, screened subnet firewalls