



# Firewall Planning and Design

# Learning Objectives

- ◆ Understand the misconceptions about firewalls
- ◆ Realize that a firewall is dependent on an effective security policy
- ◆ Understand what a firewall does
- ◆ Describe the types of firewall protection
- ◆ Understand the limitations of firewalls
- ◆ Determine the best hardware and software selections for your firewall

# 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

# Misconceptions about Firewalls

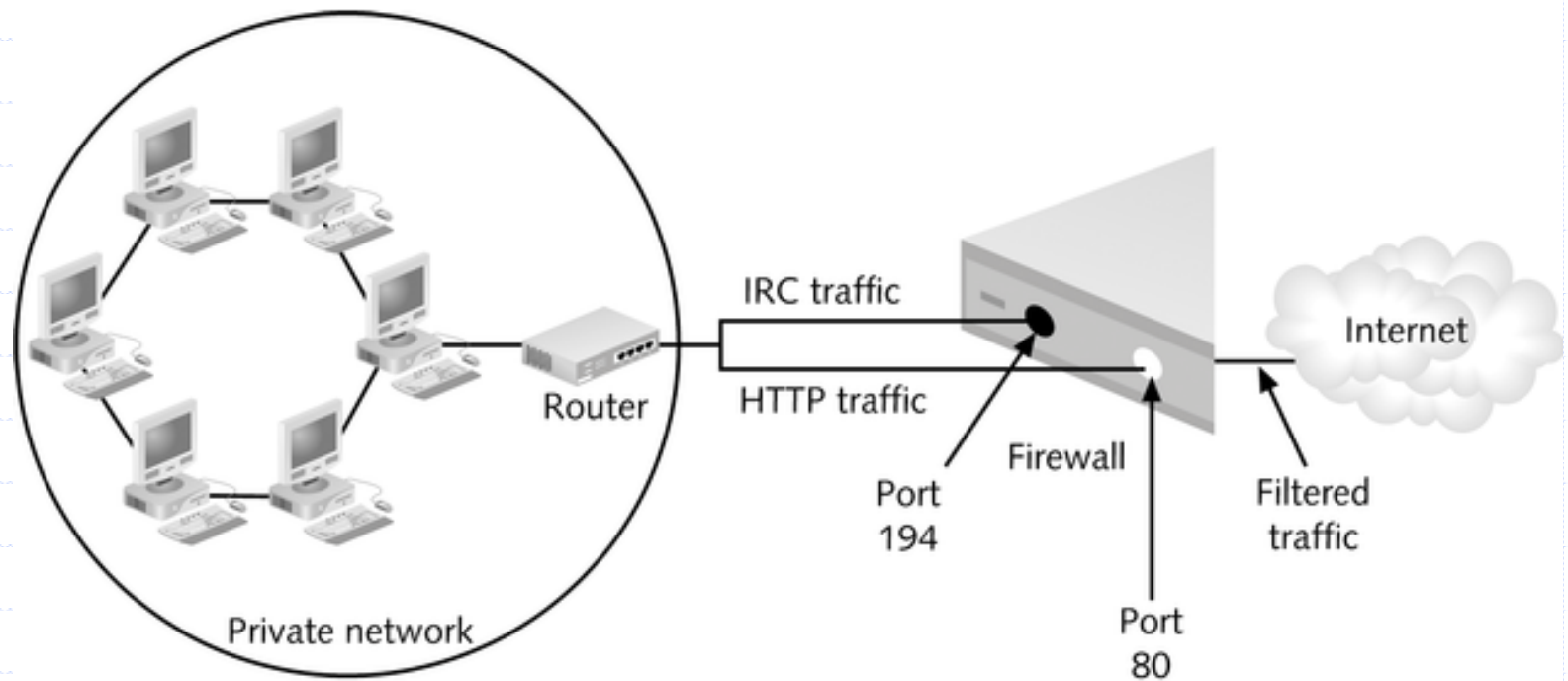
## ◆ Misconception

- Once deployed, firewalls operate on their own

## ◆ Reality

- Work best when part of Defense in Depth (DiD) security
- Need constant maintenance

# Misconceptions about Firewalls



**Figure 1-1** Firewalls filter but do not block all traffic

# What Is a Security Policy?

- ◆ Set of rules and procedures developed by management in conjunction with security professionals
  - Acceptable/unacceptable use of network
  - What resources need to be protected
  - How the company will respond to breaches of security

# Components of a Security Policy

- ◆ List of physical, logical, and network assets to be protected
- ◆ Specifications on how communications across the firewall will be audited
- ◆ Acceptable Use Policy that tells employees what constitutes acceptable use of company resources
- ◆ Description of organization's approach to security and how it affects the firewall

# What Is a Firewall?

- ◆ Hardware or software that monitors transmission of packets of digital information that attempt to pass the perimeter of a network
- ◆ Performs two basic security functions
  - Packet filtering
  - Application proxy gateways



# Firewalls Provide Security Features

- ◆ Log unauthorized accesses into/out of a network
- ◆ Provide a VPN link to another network
- ◆ Authenticate users
- ◆ Shield hosts inside the network from hackers
- ◆ Cache data
- ◆ Filter content that is considered inappropriate or dangerous

# Firewalls Provide Protection for Individual Users

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

# Firewalls Provide Protection for Individual Users

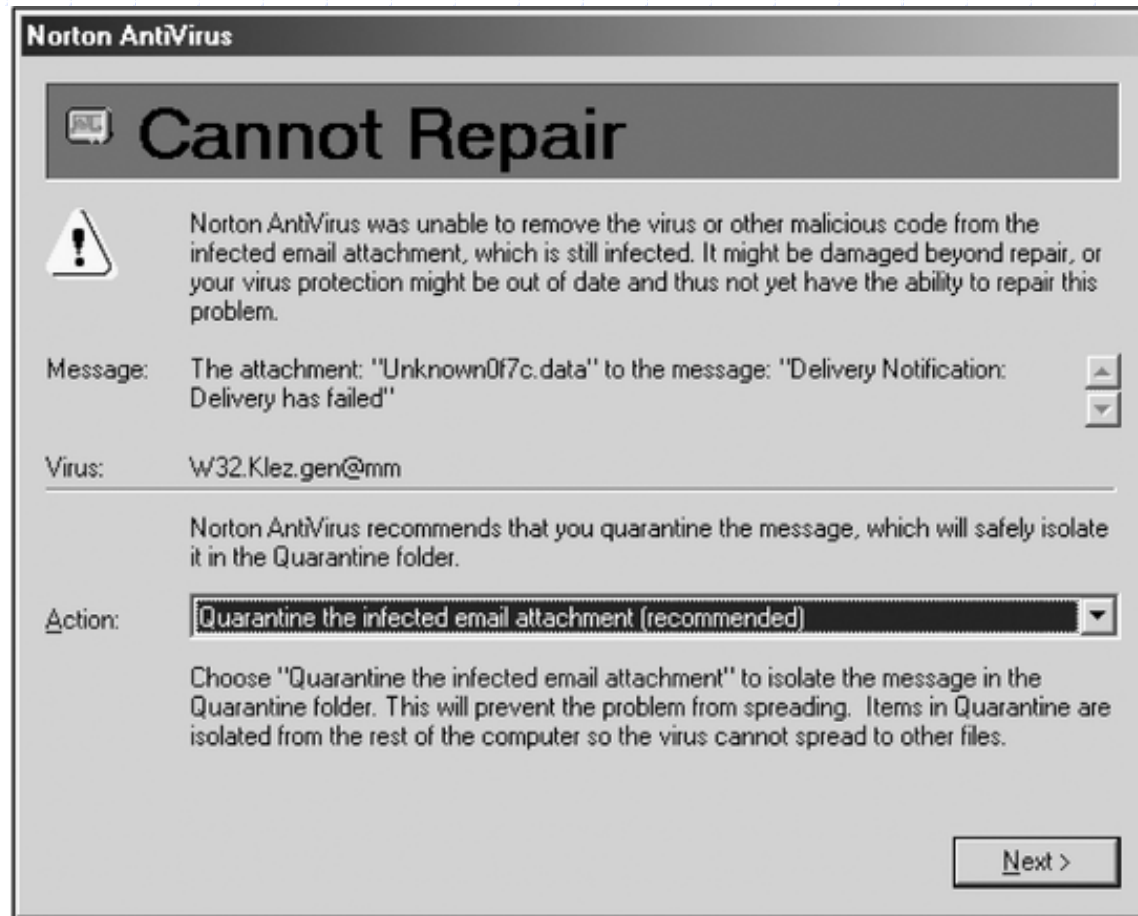
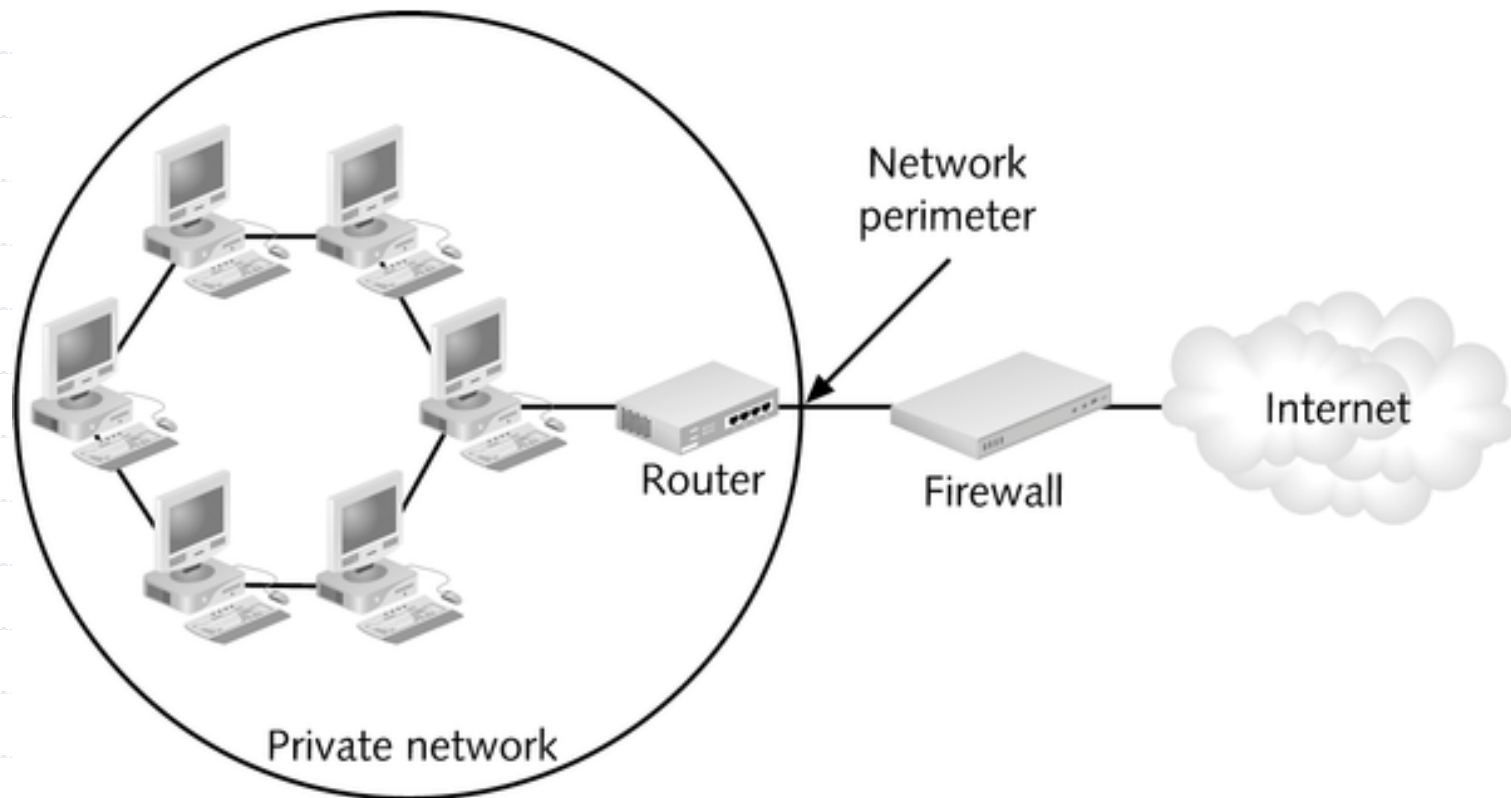


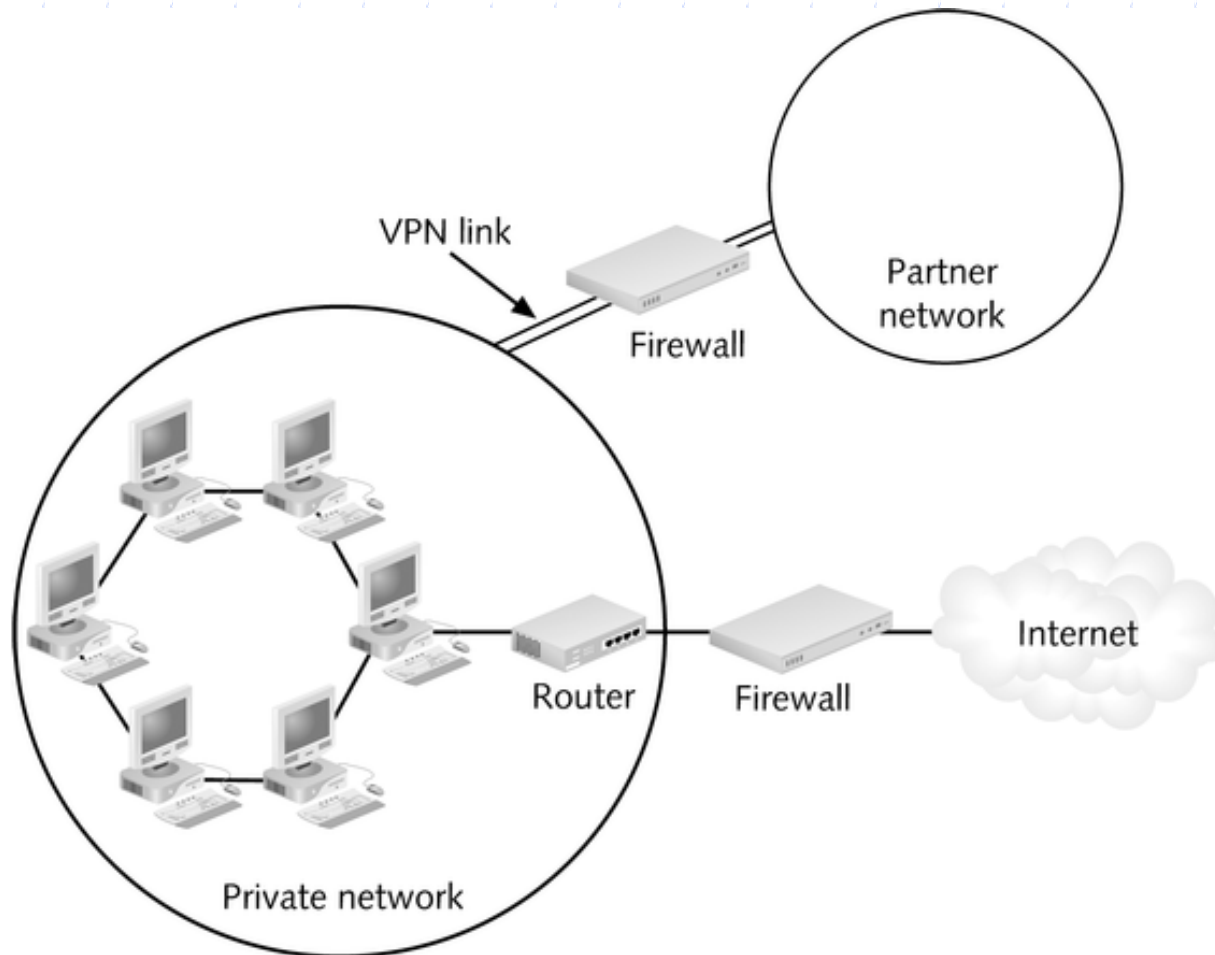
Figure 1-2 Some firewalls contain virus detection software

# Firewalls Provide Perimeter Security for Networks



**Figure 1-3** A firewall stands as a checkpoint on the perimeter of the network being protected

# Firewalls Provide Perimeter Security for Networks

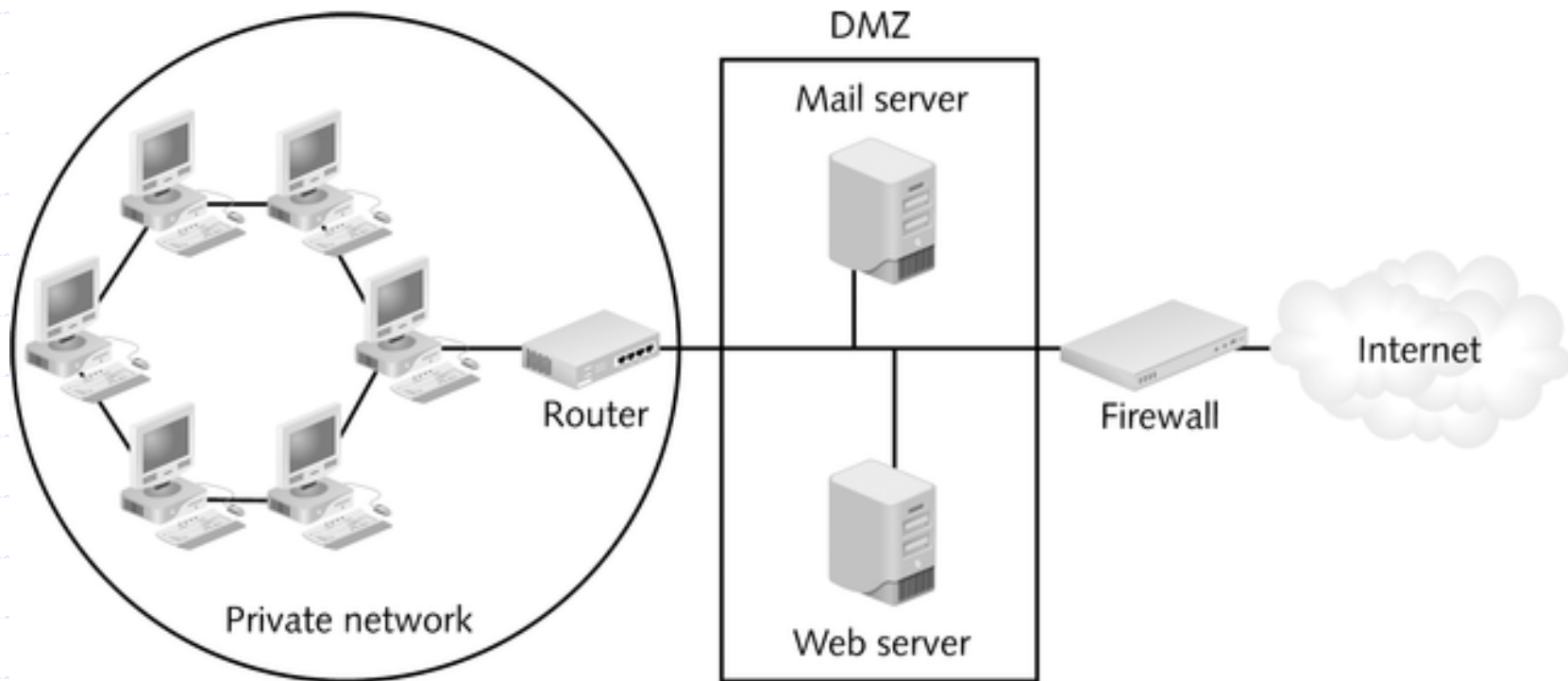


**Figure 1-4** A VPN should have its own perimeter firewall

# Firewalls Consist of Multiple 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

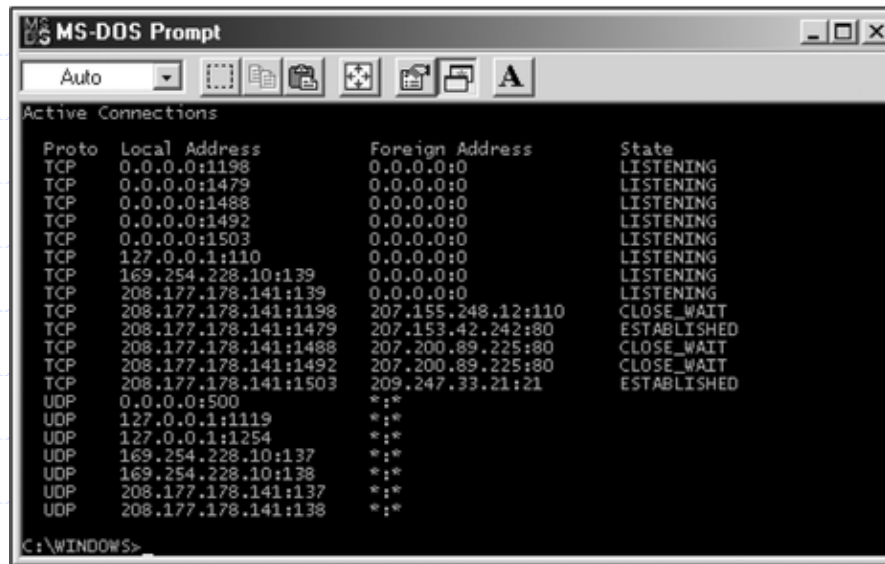
# A Network with a Bastion Host and Service Network (DMZ)



**Figure 1-5** More than one firewall can be used to create a secure network called a DMZ

# Firewalls Confront Threats and Perform Security Tasks

- ◆ Restrict access from outside network by using packet filtering



The screenshot shows a Windows command prompt window titled "MS-DOS Prompt". The window displays the output of the "netstat" command, showing active connections. The output is as follows:

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:1198	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1479	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1488	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1492	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1503	0.0.0.0:0	LISTENING
TCP	127.0.0.1:110	0.0.0.0:0	LISTENING
TCP	169.254.228.10:139	0.0.0.0:0	LISTENING
TCP	208.177.178.141:139	0.0.0.0:0	LISTENING
TCP	208.177.178.141:1198	207.155.248.12:110	CLOSE_WAIT
TCP	208.177.178.141:1479	207.153.42.242:80	ESTABLISHED
TCP	208.177.178.141:1488	207.200.89.225:80	CLOSE_WAIT
TCP	208.177.178.141:1492	207.200.89.225:80	CLOSE_WAIT
TCP	208.177.178.141:1503	209.247.33.21:21	ESTABLISHED
UDP	0.0.0.0:500	*:*	
UDP	127.0.0.1:1119	*:*	
UDP	127.0.0.1:1254	*:*	
UDP	169.254.228.10:137	*:*	
UDP	169.254.228.10:138	*:*	
UDP	208.177.178.141:137	*:*	
UDP	208.177.178.141:138	*:*	

Figure 1-6 Any computer can listen on multiple ports, each of which can be a vulnerable point

continued



# Firewalls Confront Threats and Perform Security Tasks

- ◆ Restrict unauthorized access from inside network (eg, social engineering)
- ◆ Give clients limited access to external hosts by acting as a proxy server

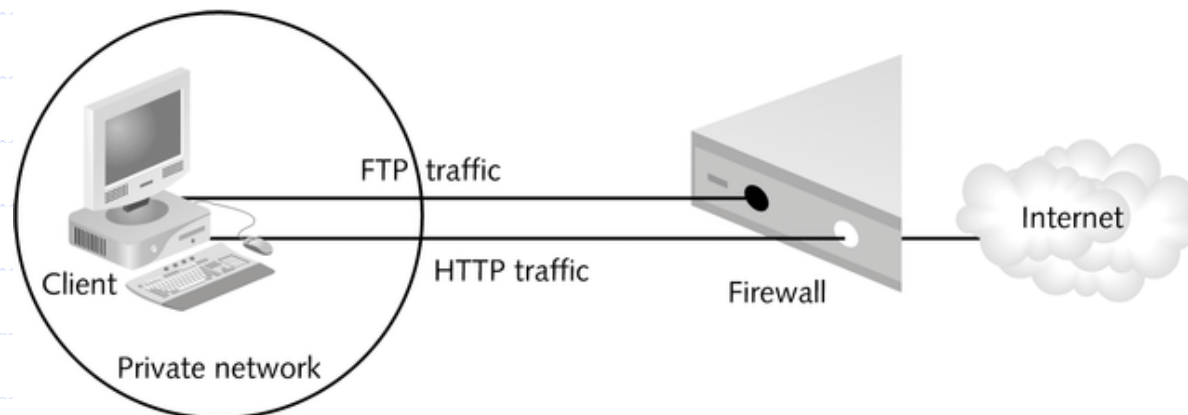


Figure 1-7 Outbound IP packet filtering

continued

# Firewalls Confront Threats and Perform Security Tasks

- ◆ Protect critical resources against attacks (eg, worms, viruses, Trojan horses, and DDoS attacks)
- ◆ Protect against hacking, which can affect:
  - Loss of data
  - Loss of time
  - Staff resources
  - Confidentiality

continued

# Firewalls Confront Threats and Perform Security Tasks

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

# Types of Firewall Protection

- ◆ Multilayer firewall protection
- ◆ Packet filtering
  - Stateful
  - Stateless
- ◆ NAT
- ◆ Application proxy gateways

# Multilayer Firewall Protection

**Table 1-1** Network layers and firewalls

Layer Number	OSI Reference Model Layer	Firewall Technology
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

# Packet Filtering

- ◆ Key function of any firewall
- ◆ Packets contain two kinds of information:
  - Header
  - Data
- ◆ Packet filters
  - Effective element in any perimeter security setup
  - Do not take up bandwidth
  - Use packet headers to decide whether to block the packet or allow it to pass

# Stateless Packet Filtering

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

# Stateful Packet Filtering

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



# Packet Filtering Rules

## ◆ Any outbound packet:

- Must have a source address in your internal network
- Must *not* have a destination address in your internal network

## ◆ Any inbound packet:

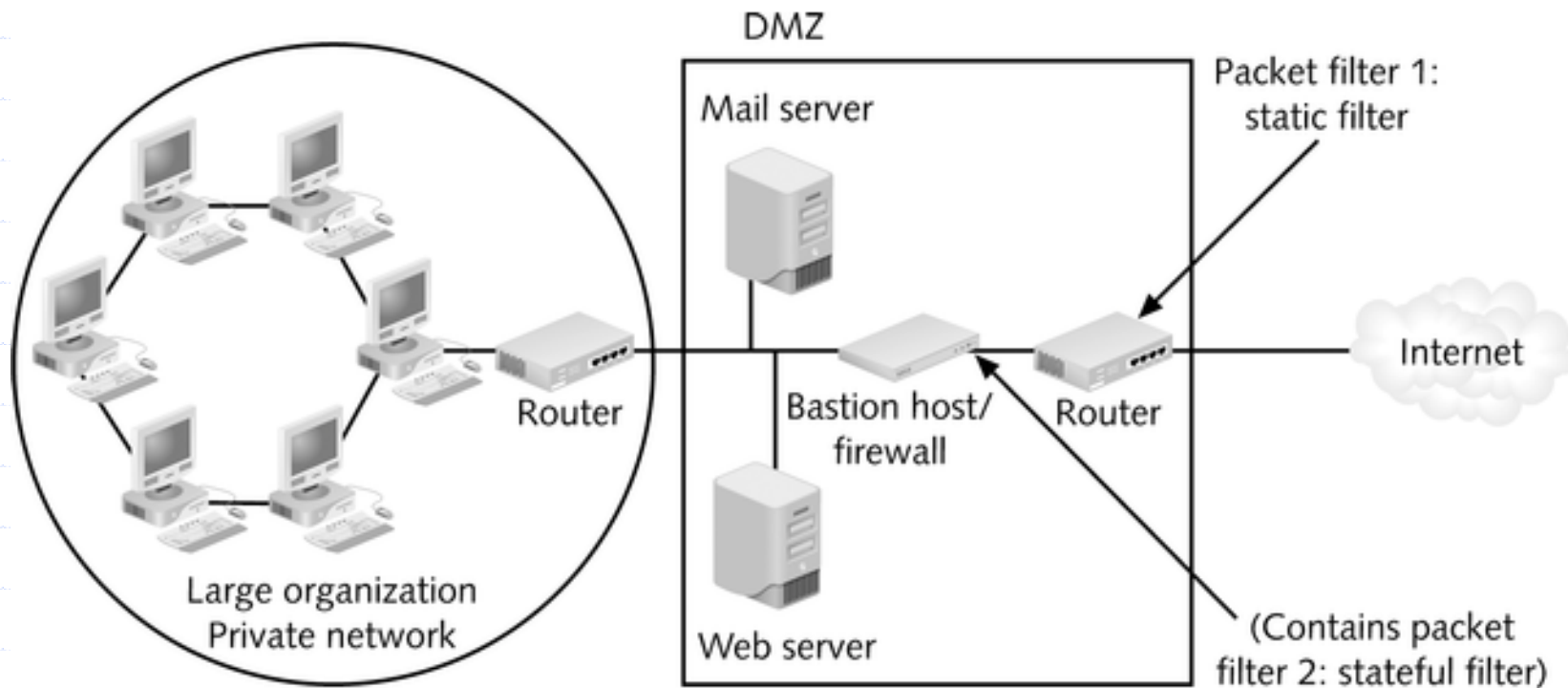
- Must *not* have a source address in your internal network
- Must have a destination address in your internal network

continued

# Packet Filtering Rules

- ◆ Any packet that enters/leaves your network must have a source/destination address that falls within the 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

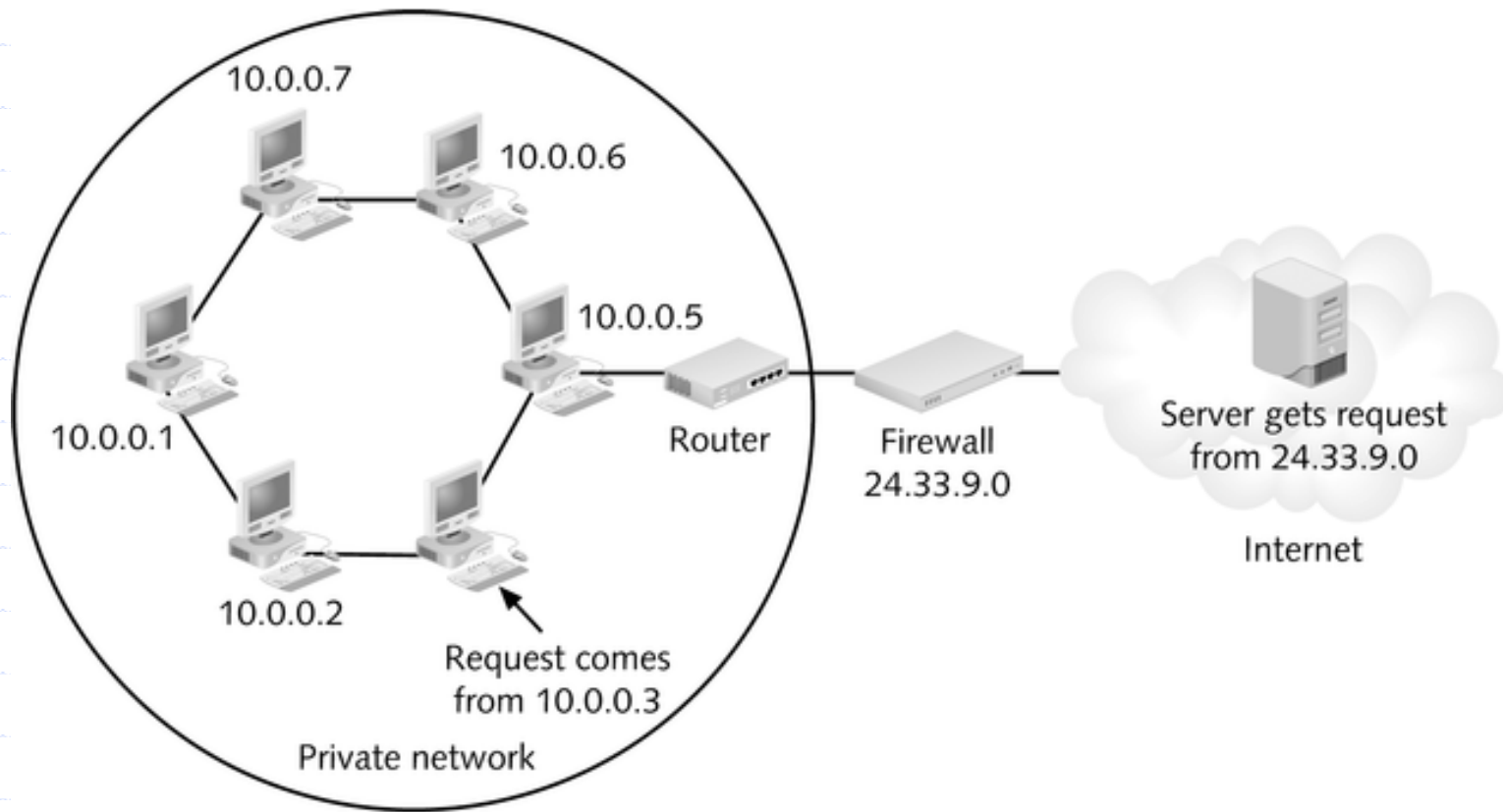


**Figure 1-8** Multiple packet filters provide extra security

# NAT

- ◆ Hides TCP/IP information of hosts in the network being protected
  - Prevents hackers from getting address of actual host
- ◆ Functions as a network-level proxy; converts IP addresses of internal hosts to IP address of the firewall

# NAT



**Figure 1-9** NAT in action

# Application Layer Gateways

- ◆ Control how applications inside the network access the outside world by setting up proxy services
- ◆ Act as a 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

# 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 (eg, ID cards, passwords, employee rules of conduct)



# Evaluating Firewall Packages

- ◆ They all do the core functions:
  - Filtering
  - Proxying
  - Logging
- ◆ Some add caching and address translation
- ◆ Price should not rule your decision

# Firewall Hardware

## ◆ Routers

- Many come equipped with packet-filtering capabilities; others come with full-fledged firewalls

## ◆ Appliances (ie, firewall products)

- Perform same basic tasks (packet filtering, application-level gateways, and logging)
- Some have low profile and sleek design

# Advantages of Firewall Hardware over Software-Only Products

## ◆ Self-contained

- Not affected by OS problems of a network host (eg, bugs or slow speed)

## ◆ Installation is generally easy if firewall software needs to be patched or updated

# Software-Only Packages

- ◆ Free firewall tools on the Internet
  - Most also run on a free operating system
- ◆ Personal/small business firewalls
  - Located between Ethernet adapter driver of machine on which they are installed and the TCP/IP stack, where they inspect traffic between the driver and the stack
  - Considered lightweight protection
- ◆ Enterprise firewall systems
  - Full-featured, full-powered packages

# Free Firewall Tools on the Internet

## ◆ Advantages

- Convenient, simple, and inexpensive

## ◆ Drawbacks

- Logging capabilities not as robust as commercial products
- Can be difficult to configure
- Usually no way to monitor firewall in real-time

## ◆ Examples

- Pretty Good Privacy (PGP)
- Netfilter

# Personal/Small Business Firewalls

## ◆ Advantages

- Some let you establish rules as needed

## ◆ Drawbacks

- Most guard only against IP threats
- Some don't do outbound connection blocking
- Some are inconvenient to configure

## ◆ Examples

- Norton Internet Security
- ZoneAlarm
- BlackICE Defender
- Symantec Personal Firewall

# Examples of Enterprise Firewall Systems

- ◆ Check Point FireWall-1
- ◆ Cisco PIX
- ◆ Microsoft Internet Security & Acceleration Server
- ◆ NAI Gauntlet

# Check Point FireWall-1

- ◆ Considered the product of choice
- ◆ Among the first to use stateful packet inspection to monitor network traffic
- ◆ Full array of security tools (authentication, virus checking, intrusion detection, packet filtering)
- ◆ Only firewall compliant with OPSEC security standard
- ◆ Good choice for large networks
- ◆ High availability feature



# Cisco PIX

- ◆ A series of secure, self-contained hardware devices that contain full-featured firewalls
- ◆ Competitive pricing
- ◆ Extensive online documentation
- ◆ Highly regarded customer support
- ◆ Reliable
- ◆ Feature-rich
  - High availability
  - Intrusion detection system
  - Protection against DoS attacks

# Microsoft Internet Security & Acceleration Server

- ◆ Authentication through integration with Active Directory
- ◆ Virus scanning (through integrated third-party products)
- ◆ Data-aware filtering capabilities
- ◆ IP packet-filtering functionality
- ◆ Supports Cache Array Routing Protocol (CARP); can be scaled to fit larger traffic requirements

# NAI Gauntlet

- ◆ One of longest-established firewall products available
- ◆ Flexible
  - Supports application proxies and packet filtering
  - Able to adjust speed of the firewall as needed
- ◆ Integrated by McAfee's anti-virus software

# Chapter Summary

- ◆ Issues involved in planning and designing firewalls
- ◆ What a firewall is *not*
- ◆ Security policies
- ◆ Rules and procedures that govern how a firewall works
- ◆ Types of firewall protection

continued

# Chapter Summary

- ◆ Limitations of firewalls
- ◆ How hardware is used to create firewalls
- ◆ Evaluations of firewall software packages