Firewalls and VPNs

Learning Objectives

Upon completion of this material, you should be able to:

- Understand firewall technology and the various approaches to firewall implementation
- Describe the technology that enables the use of Virtual Private Networks

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; a software service running on existing router or server; or a separate network containing supporting devices
- A Roadmap
  - Firewall categorization
  - Firewall configuration and management

Firewall Categorization

① Processing mode

② Development era

③ Intended deployment structure

④ Architectural implementation

Firewalls Categorization (1): Processing Modes

- Packet filtering
- Application gateways
- Circuit gateways
- MAC layer firewalls
- Hybrids

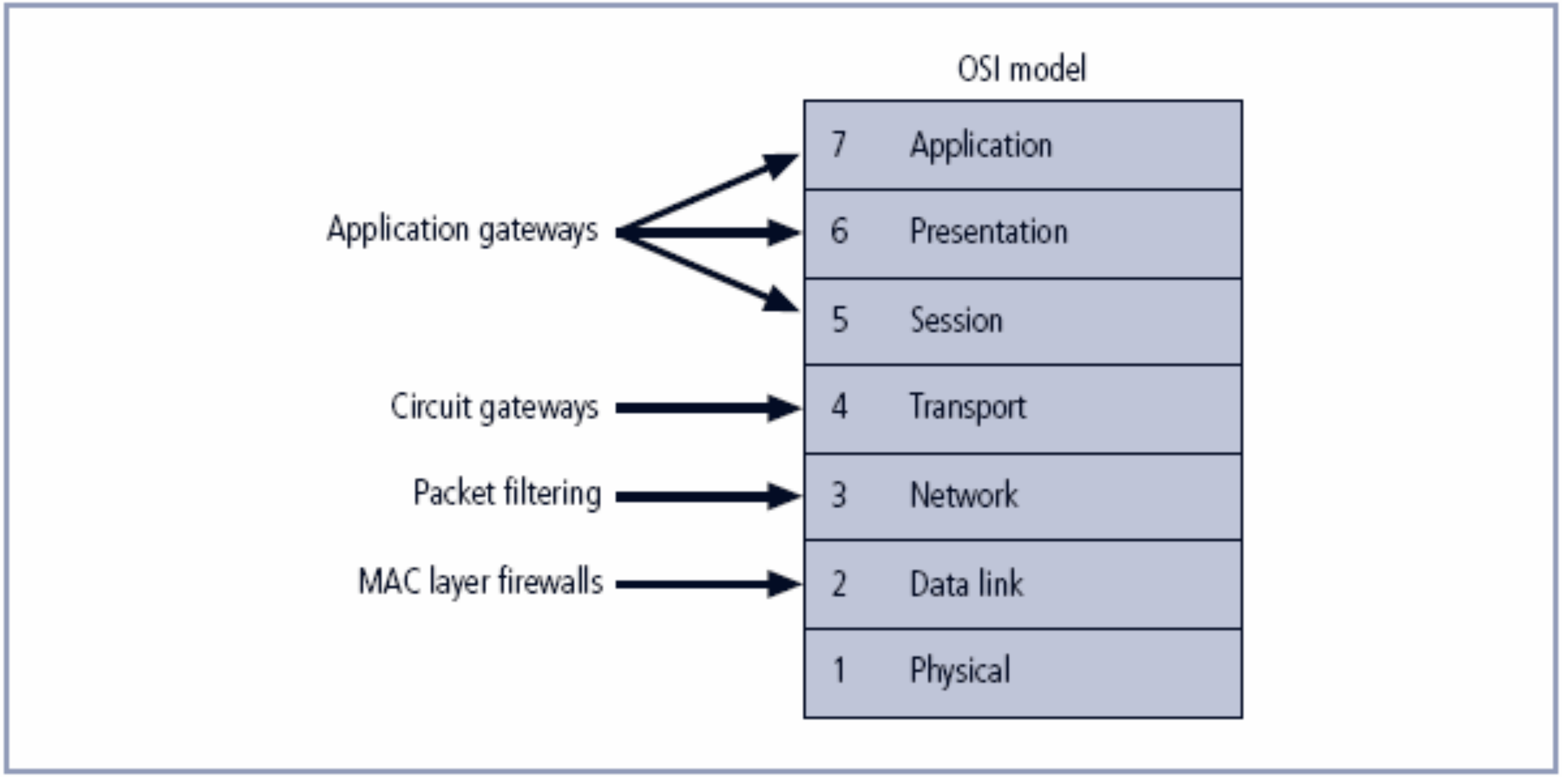


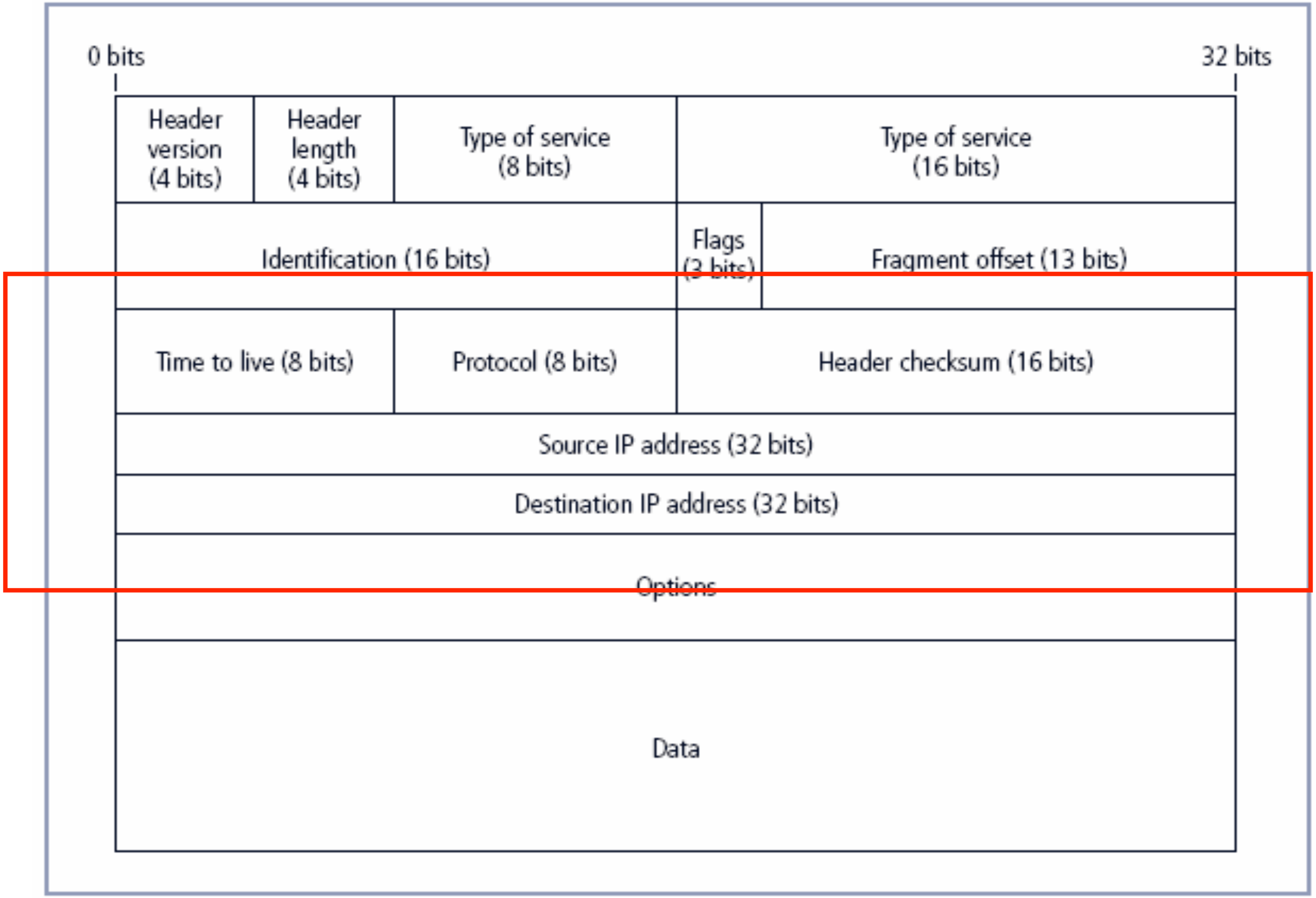
FIGURE 6-5 Firewall Types and the OSI Model

Packet Filtering

- 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

Packet Filtering (continued)

- 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



0 bits

32 bits

Header version (4 bits)

Header length (4 bits)

Type of service (8 bits)

Type of service (16 bits)

Identification (16 bits)

Flags (3 bits)

Fragment offset (13 bits)

Time to live (8 bits)

Protocol (8 bits)

Header checksum (16 bits)

Source IP address (32 bits)

Destination IP address (32 bits)

Options

Data

FIGURE 6-1 IP Packet Structure

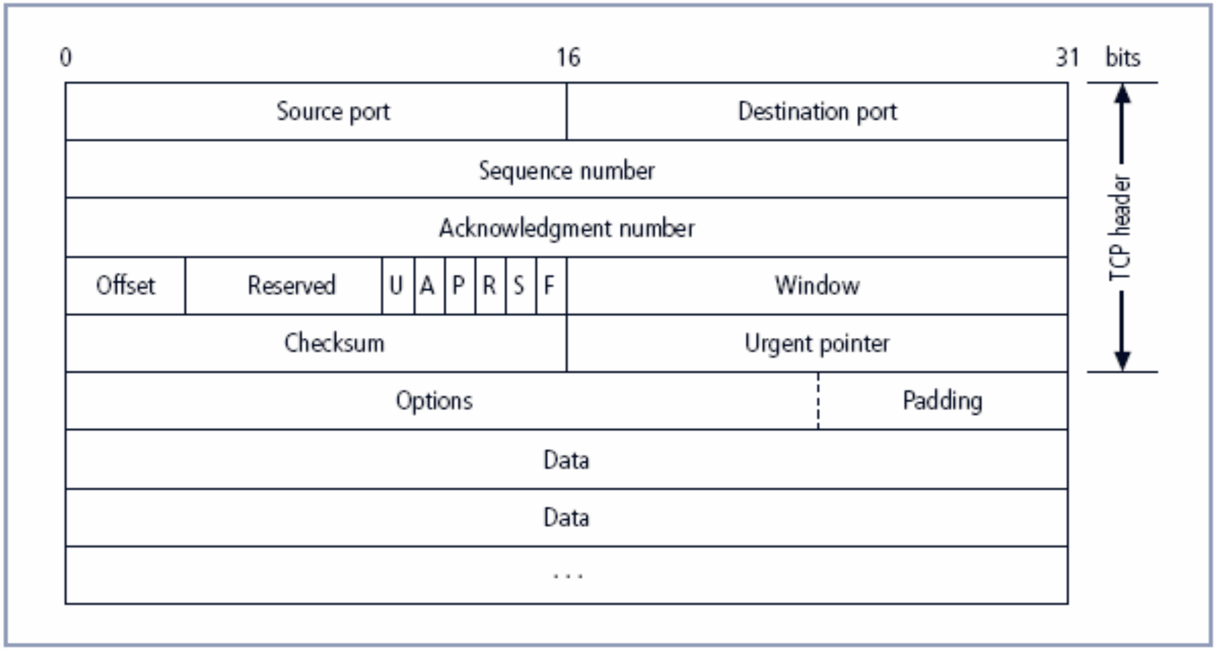


FIGURE 6-2 TCP Packet Structure

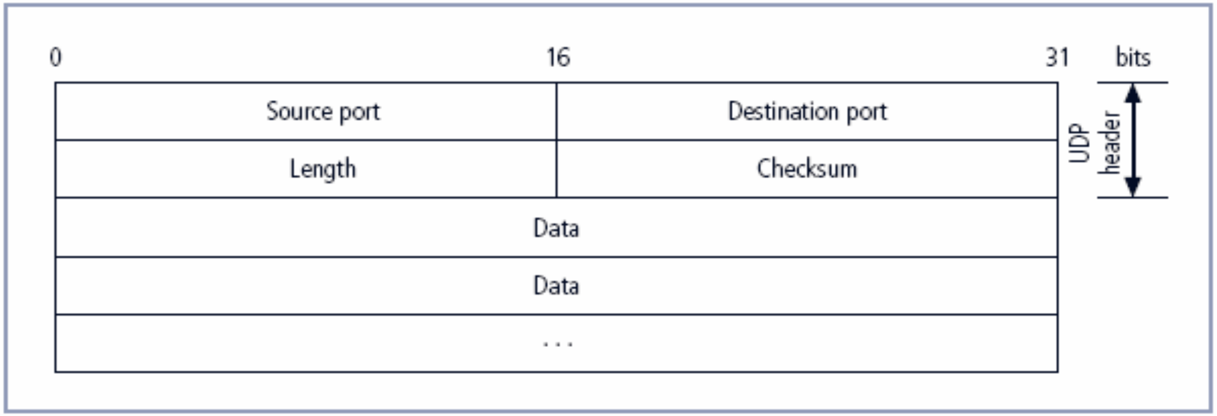


FIGURE 6-3 UDP Datagram Structure

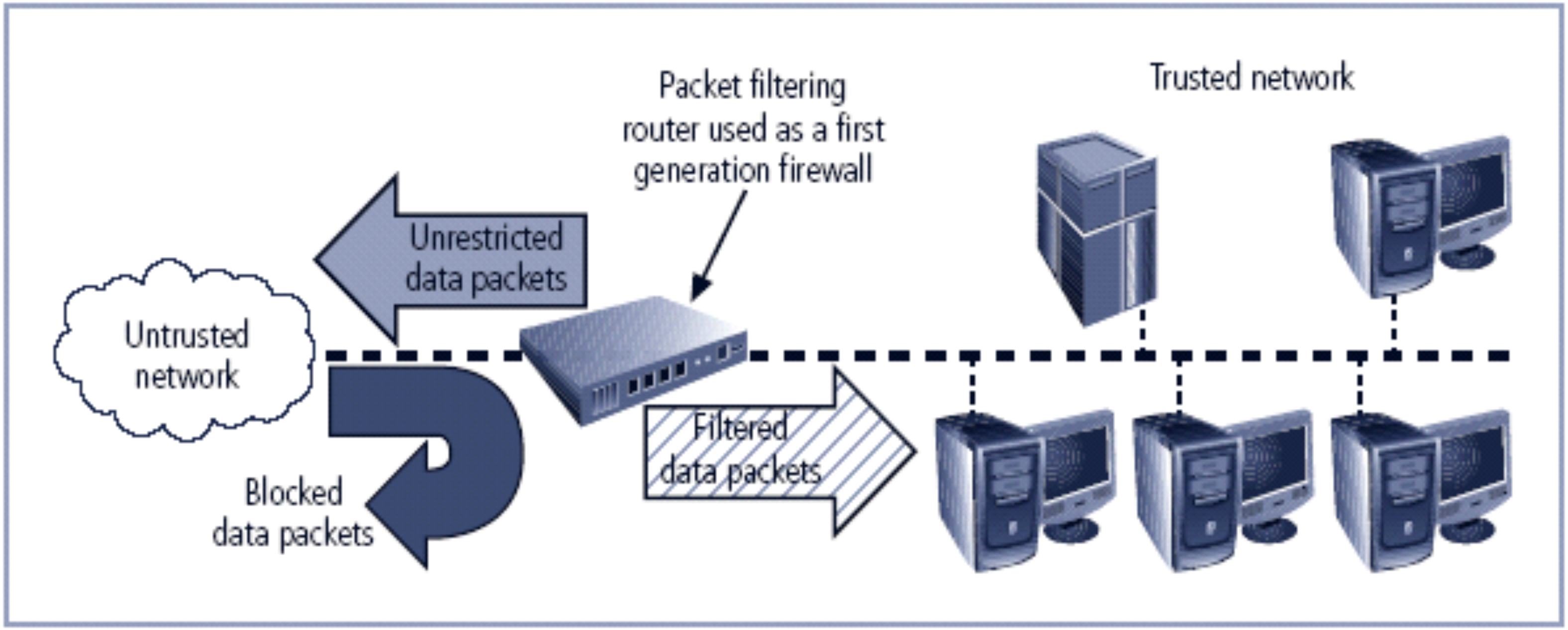

Packet filtering router used as a first generation firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

FIGURE 6-4 Packet Filtering Router

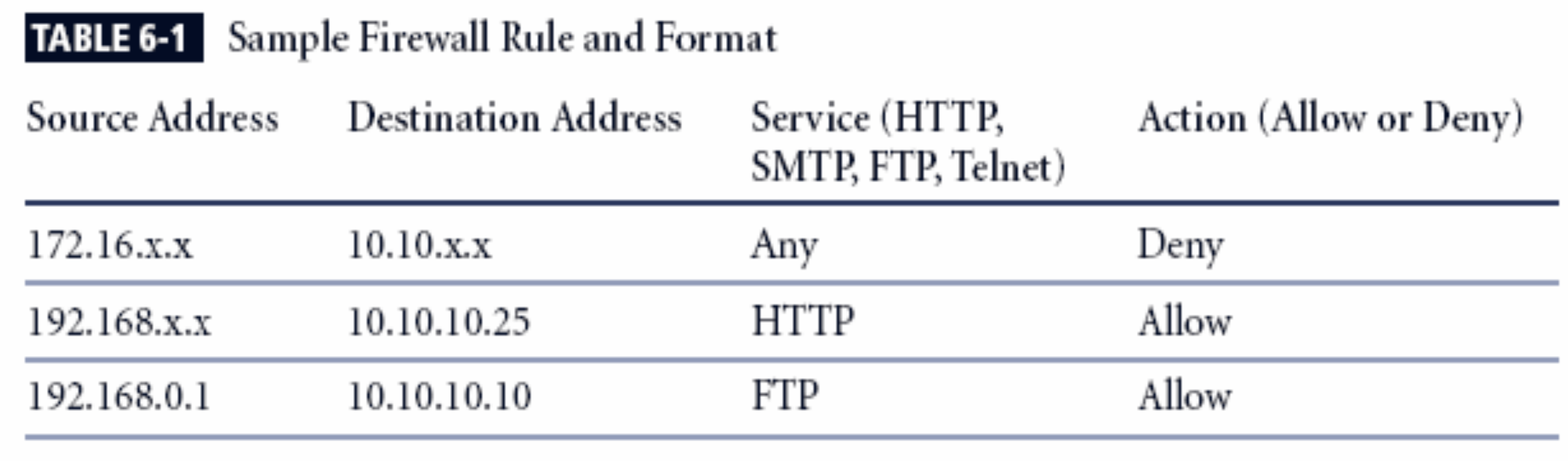


TABLE 6-1 Sample Firewall Rule and Format

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

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

Circuit Gateways

- 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

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

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 are connected to work in tandem

Firewall Categorization (2): Development Era

- 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

Firewalls Categorization (3): Deployment Structure

- Most firewalls are appliances: stand-alone, self-contained systems
- Commercial-grade firewall system consists of firewall application software running on general-purpose computer
- Small office/home office (SOHO) or residential-grade firewalls, aka broadband gateways or DSL/cable modem routers, connect user's local area network or a specific computer system to Internetworking device
- Residential-grade firewall software is installed directly on the user's system

FIGURE 6-6 SOHO Firewall Devices

Firewalls Categorization (4): Architectural Implementation

- Firewall devices can be configured in a number of network connection architectures
- Four common architectural implementations of firewalls:
  - Packet filtering routers
  - Screened host firewalls
  - Dual-homed firewalls
  - Screened subnet firewalls

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

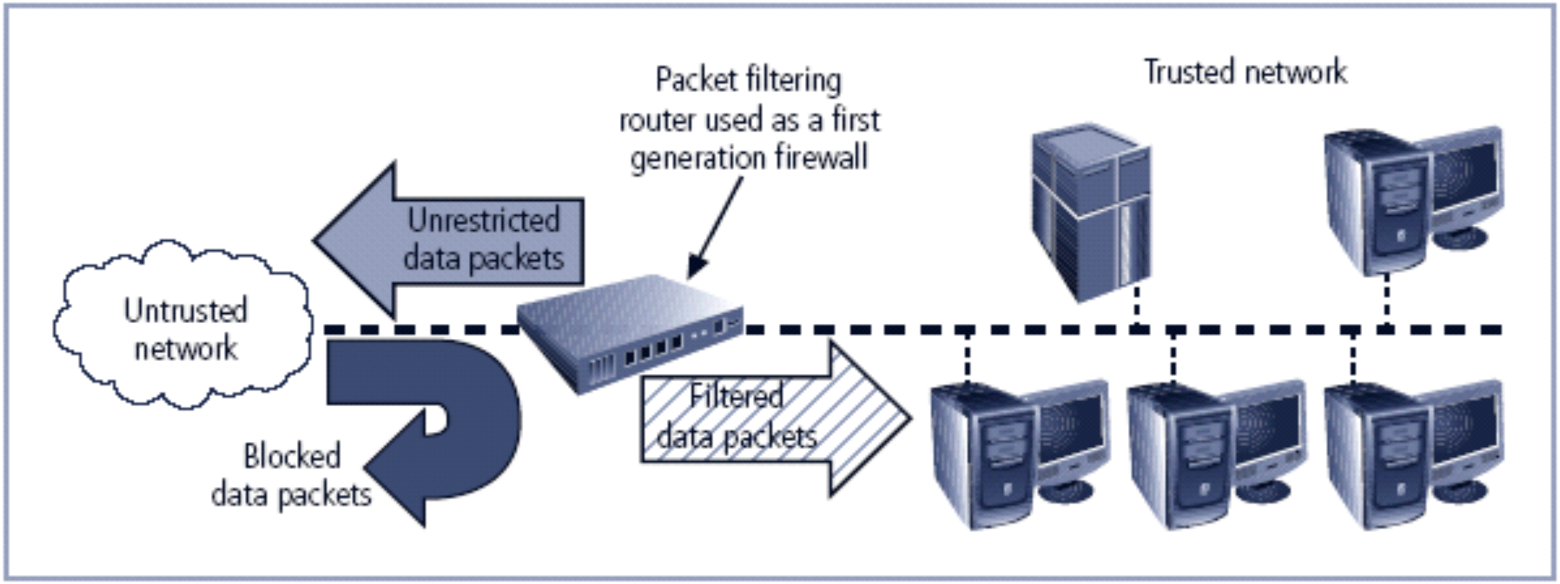


FIGURE 6-4 Packet Filtering Router

Screened Host Firewalls

- Combines packet filtering router with separate, dedicated firewall such as an application proxy server
- Allows router to pre-screen 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

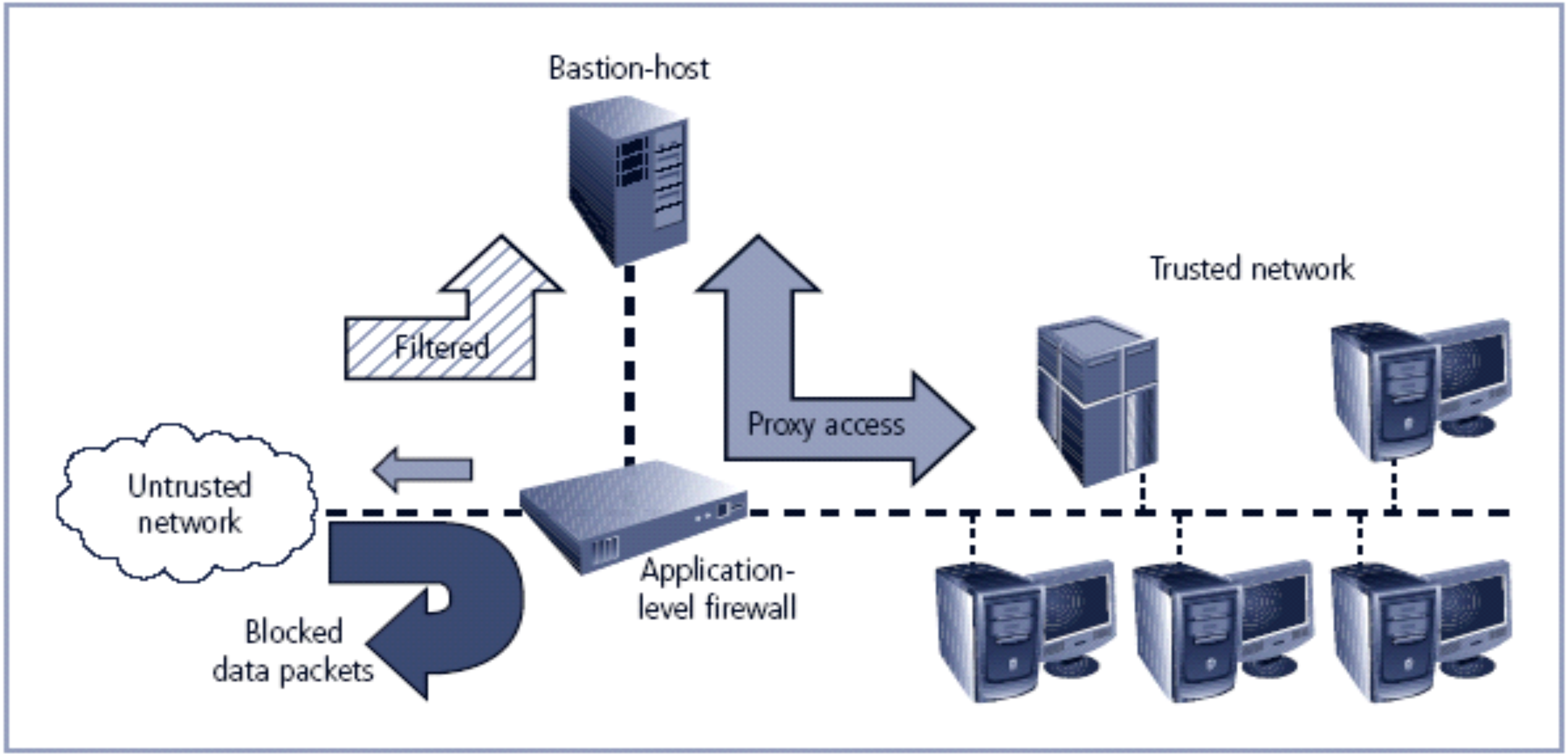


FIGURE 6-11 Screened Host Firewall

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

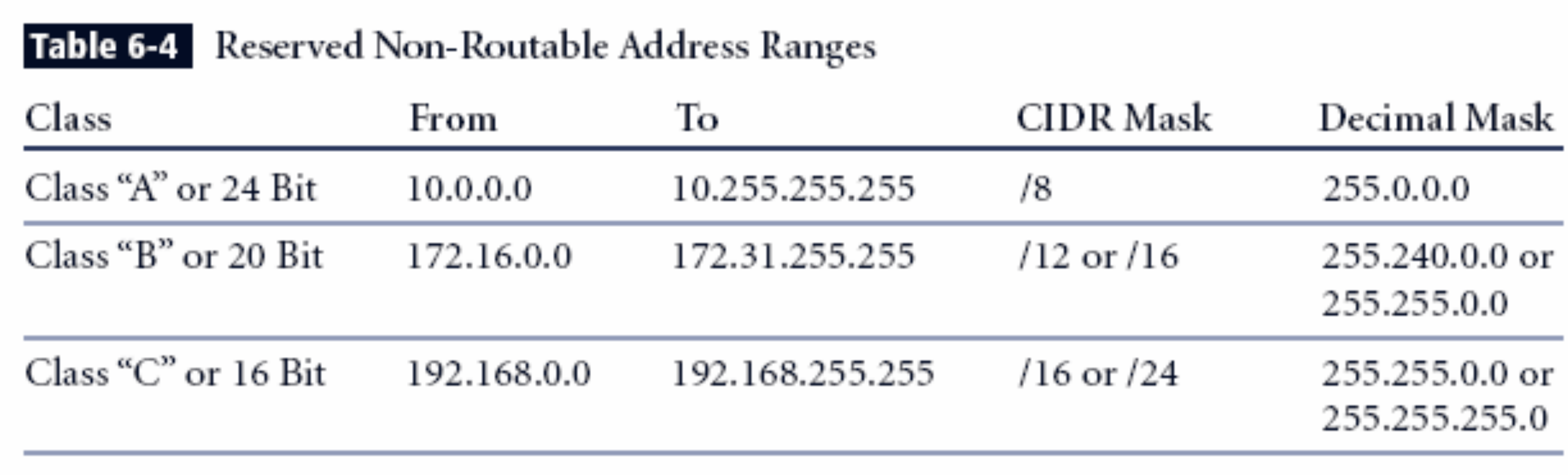


Table 6-4 Reserved Non-Routable Address Ranges

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

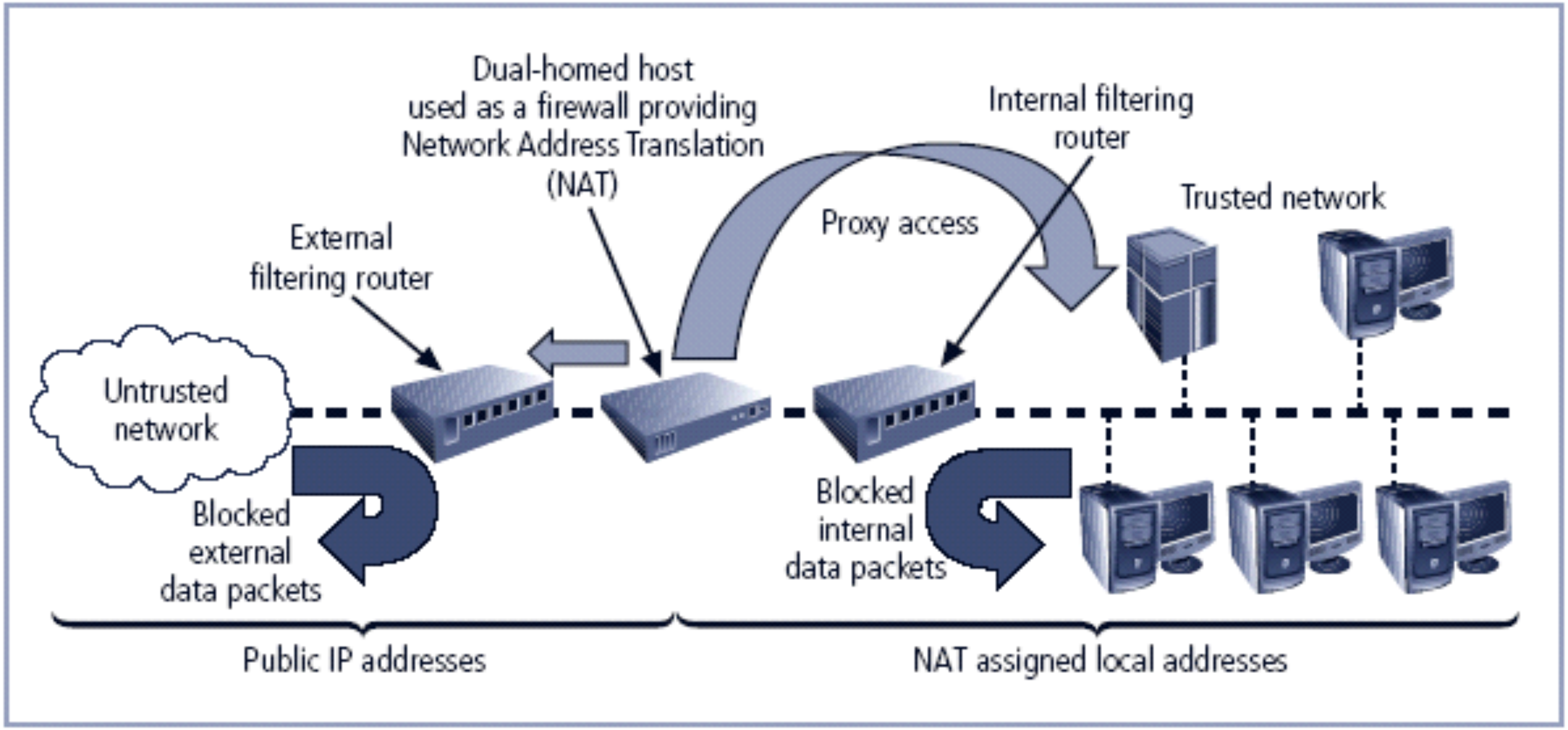

Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

FIGURE 6-12 Dual-Homed Host Firewall

Screened Subnet Firewalls (with DMZ)

- Dominant architecture used today is the screened subnet firewall
- 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

Screened Subnet Firewalls (with DMZ) (continued)

- 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

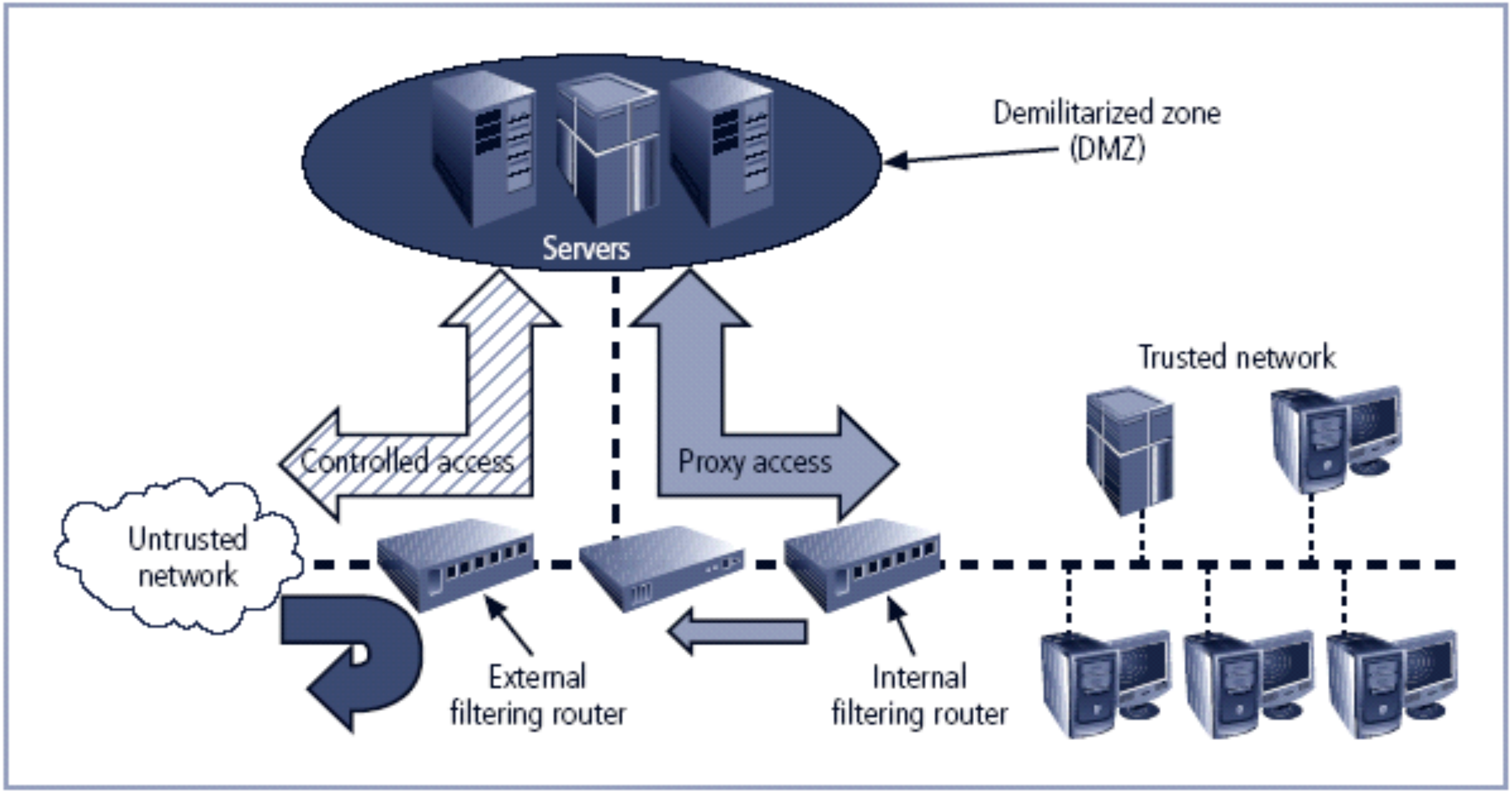


FIGURE 6-13 Screened Subnet (DMZ)

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?
  - What 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 both an art and a science
- When security rules conflict with the performance of business, security often loses

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

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

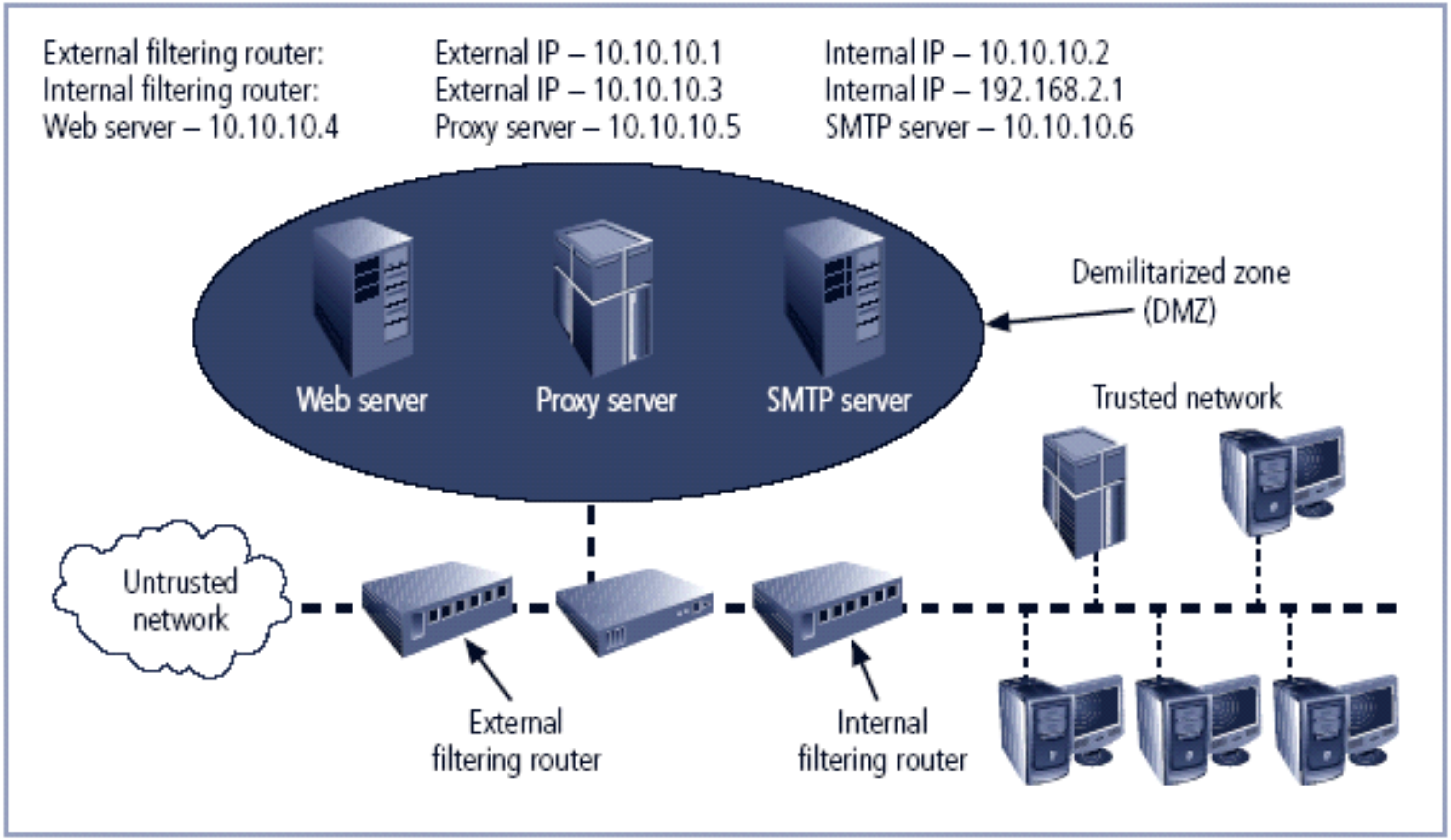

External filtering router: External IP – 10.10.10.1 Internal IP – 10.10.10.2
Internal filtering router: External IP – 10.10.10.3 Internal IP – 192.168.2.1
Web server – 10.10.10.4 Proxy server – 10.10.10.5 SMTP server – 10.10.10.6
Web server
Proxy server
SMTP server
Demilitarized zone (DMZ)
Trusted network
Untrusted network
External filtering router
Internal filtering router

FIGURE 6-14 Example Network Configuration

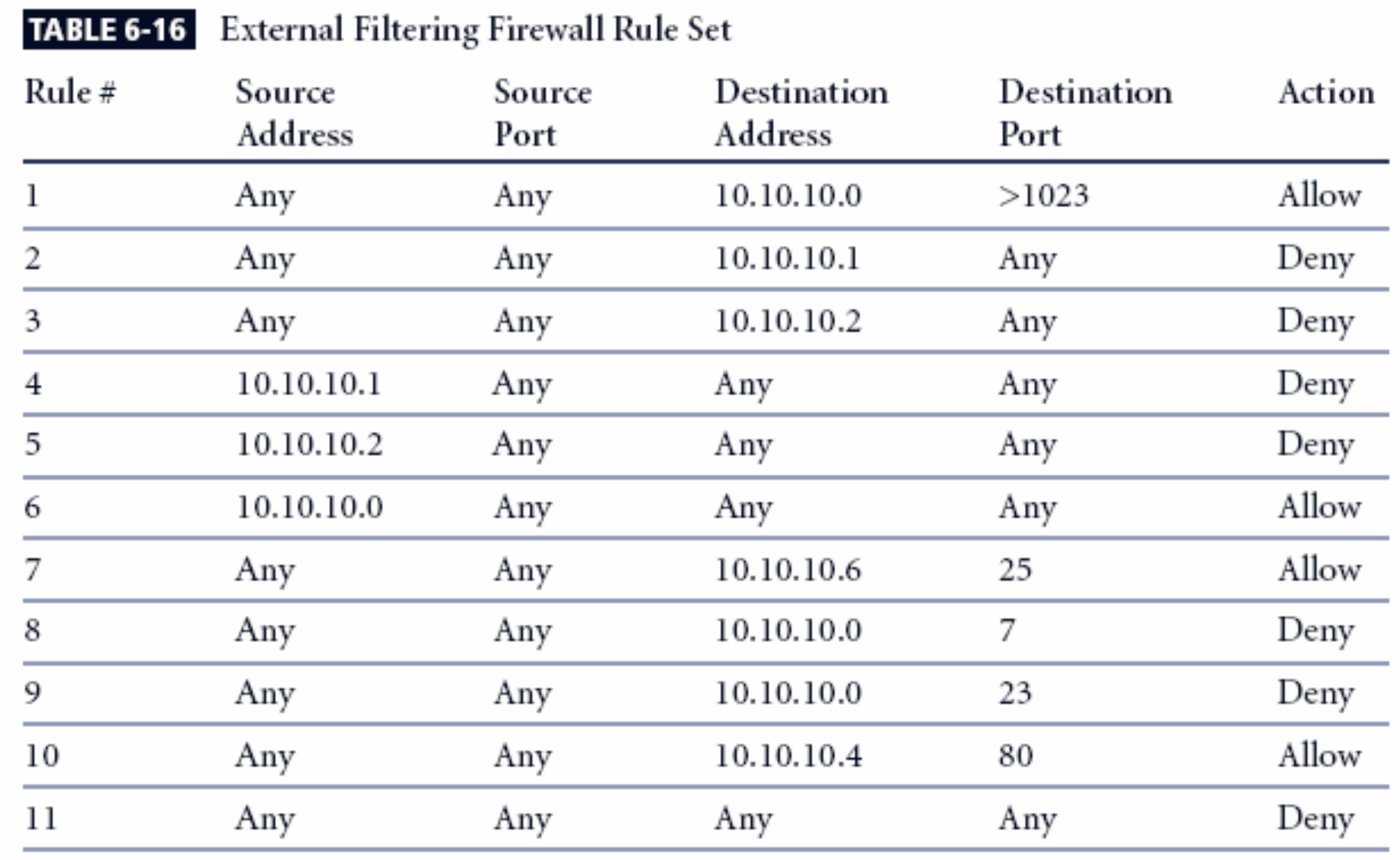


TABLE 6-16 External Filtering Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.0	>1023	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	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

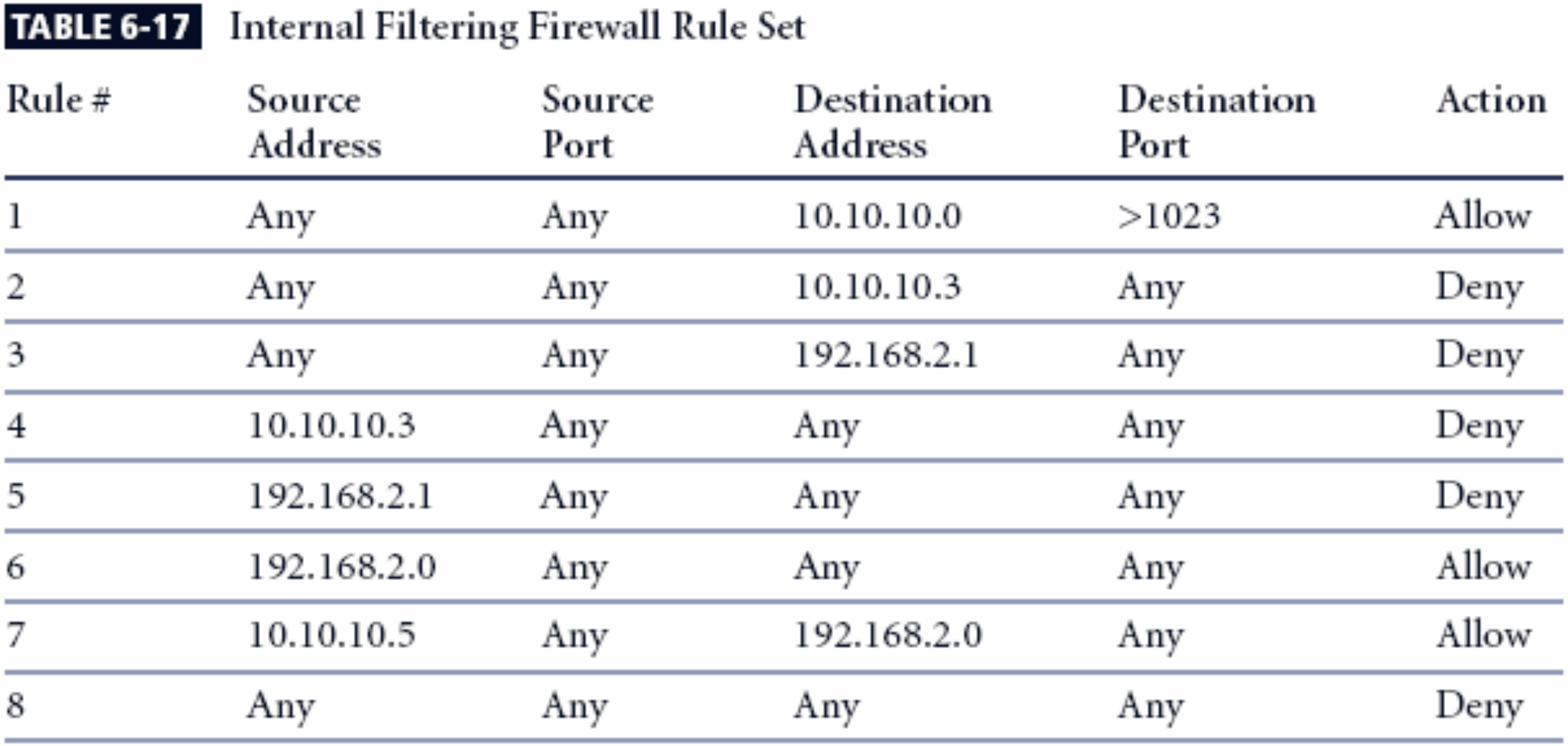


TABLE 6-17 Internal Filtering Firewall Rule Set

Rule #	Source Address	Source Port	Destination Address	Destination Port	Action
1	Any	Any	10.10.10.0	>1023	Allow
2	Any	Any	10.10.10.3	Any	Deny
3	Any	Any	192.168.2.1	Any	Deny
4	10.10.10.3	Any	Any	Any	Deny
5	192.168.2.1	Any	Any	Any	Deny
6	192.168.2.0	Any	Any	Any	Allow
7	10.10.10.5	Any	192.168.2.0	Any	Allow
8	Any	Any	Any	Any	Deny

Virtual Private Networks (VPNs) (1)

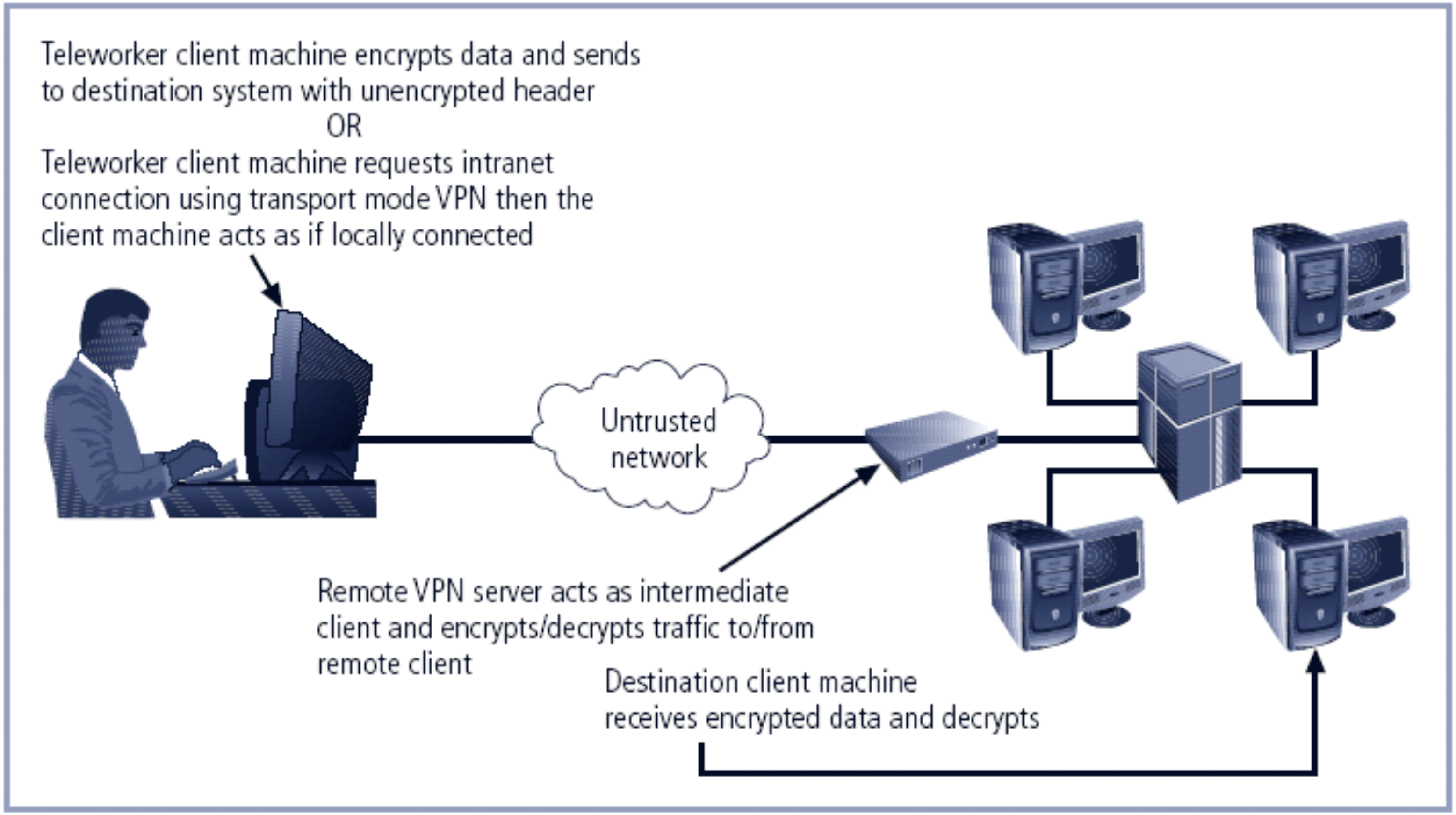
- Private and secure network connection between systems; uses data communication capability of unsecured and public network
- Securely extends organization’s internal network connections to remote locations beyond trusted network

Virtual Private Networks (VPNs) (2)

- 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

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



Teleworker client machine encrypts data and sends to destination system with unencrypted header
OR
Teleworker client machine requests intranet connection using transport mode VPN then the client machine acts as if locally connected

Remote VPN server acts as intermediate client and encrypts/decrypts traffic to/from remote client

Destination client machine receives encrypted data and decrypts

FIGURE 6-18 Transport Mode VPN

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

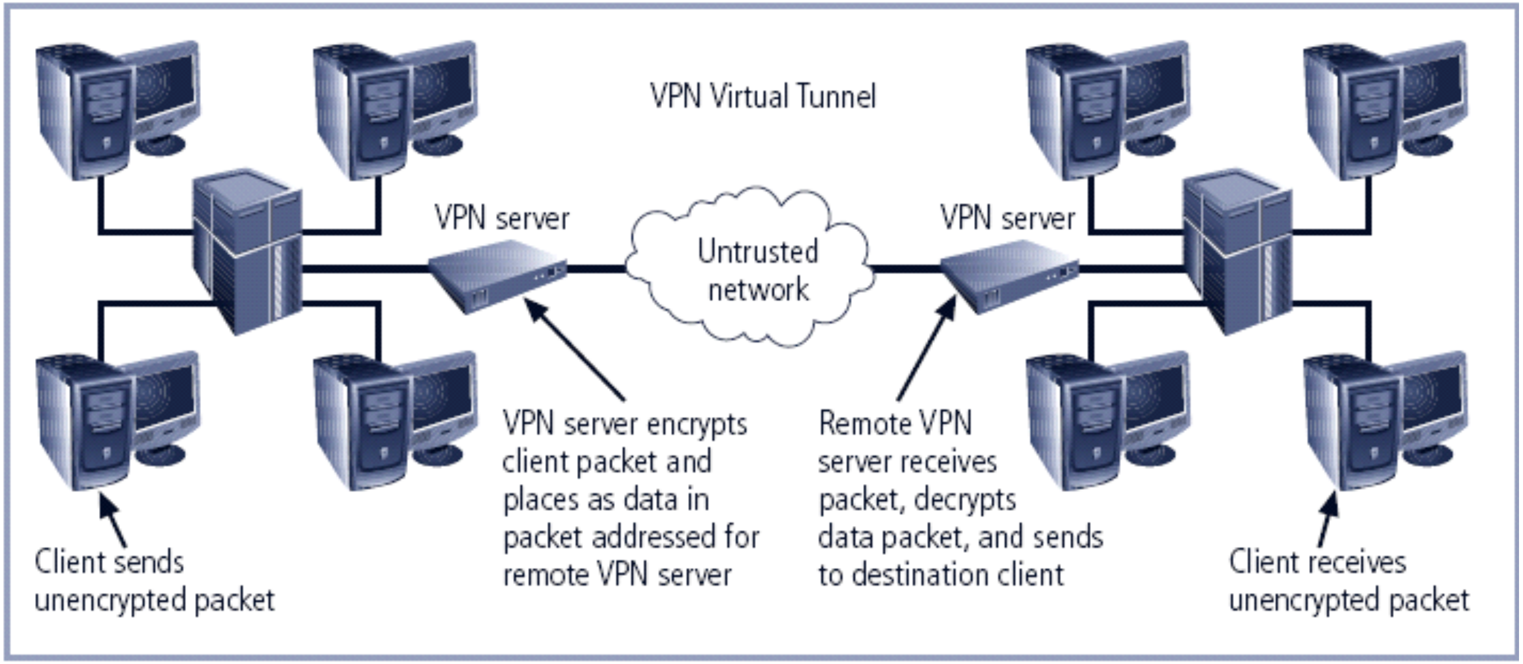
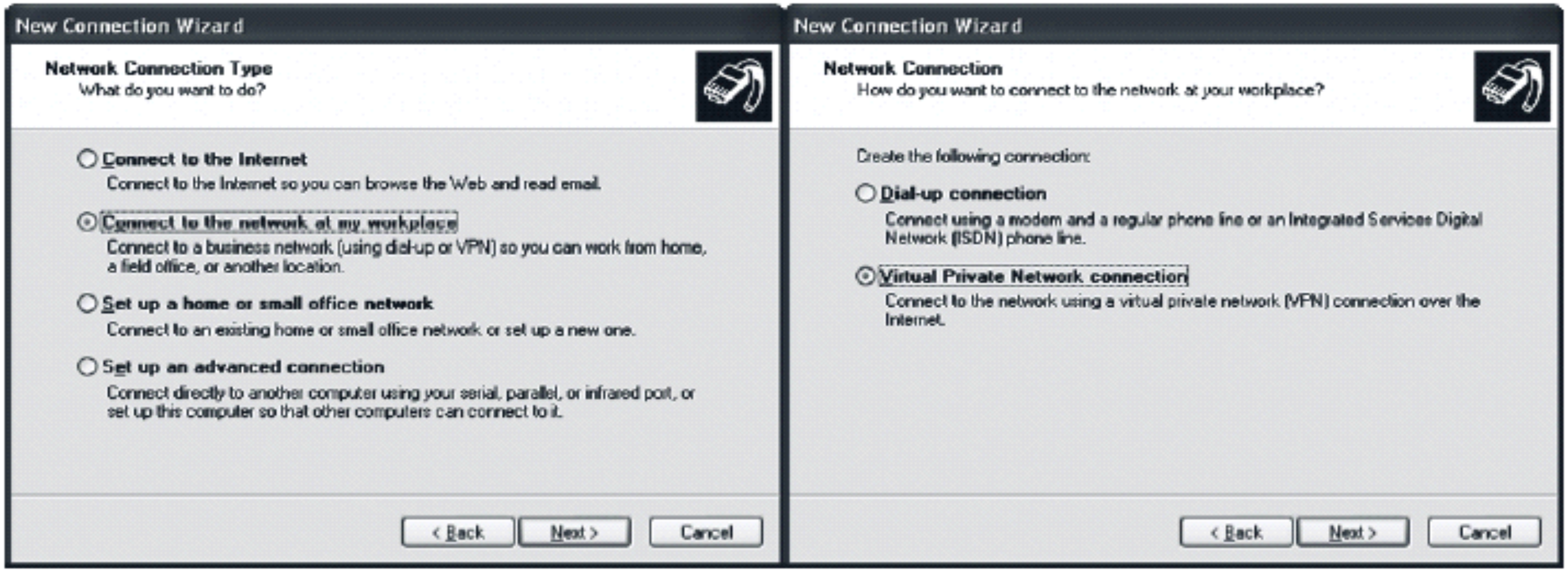

VPN Virtual Tunnel
VPN server
Untrusted network
VPN server
VPN server encrypts client packet and places as data in packet addressed for remote VPN server
Remote VPN server receives packet, decrypts data packet, and sends to destination client
Client sends unencrypted packet
Client receives unencrypted packet

FIGURE 6-19 Tunnel Mode VPN



New Connection Wizard

Network Connection Type
What do you want to do?

○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

New Connection Wizard

Network Connection
How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**
Connect to the network using a virtual private network (VPN) connection over the Internet.

FIGURE 6-20 VPN Client in Windows XP

Summary

- Firewall technology
  - Four methods for categorization
  - Firewall configuration and management
- Virtual Private Networks
  - Two modes