Firewalls and VPNs

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

①Processing mode

②Development era

③Intended deployment structure

④Architectural implementation

Firewall Categorization (1): Processing Modes

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

Firewall Proc. Modes: Network Layers

Processing Mode	Network Layer (OSI)	Network Layer (TCP/IP)
Application gateways	7: Application	5: Application
	6: Presentation	
	5: Session	
Circuit gateways	4: Transport	4: Transport
Packet filtering	3: Network	3: Network
MAC address filtering	2: Data Link	2: Data Link
–	1: Physical	1: Physical

Source: Adapted from Fig. 6-5 in the textbook

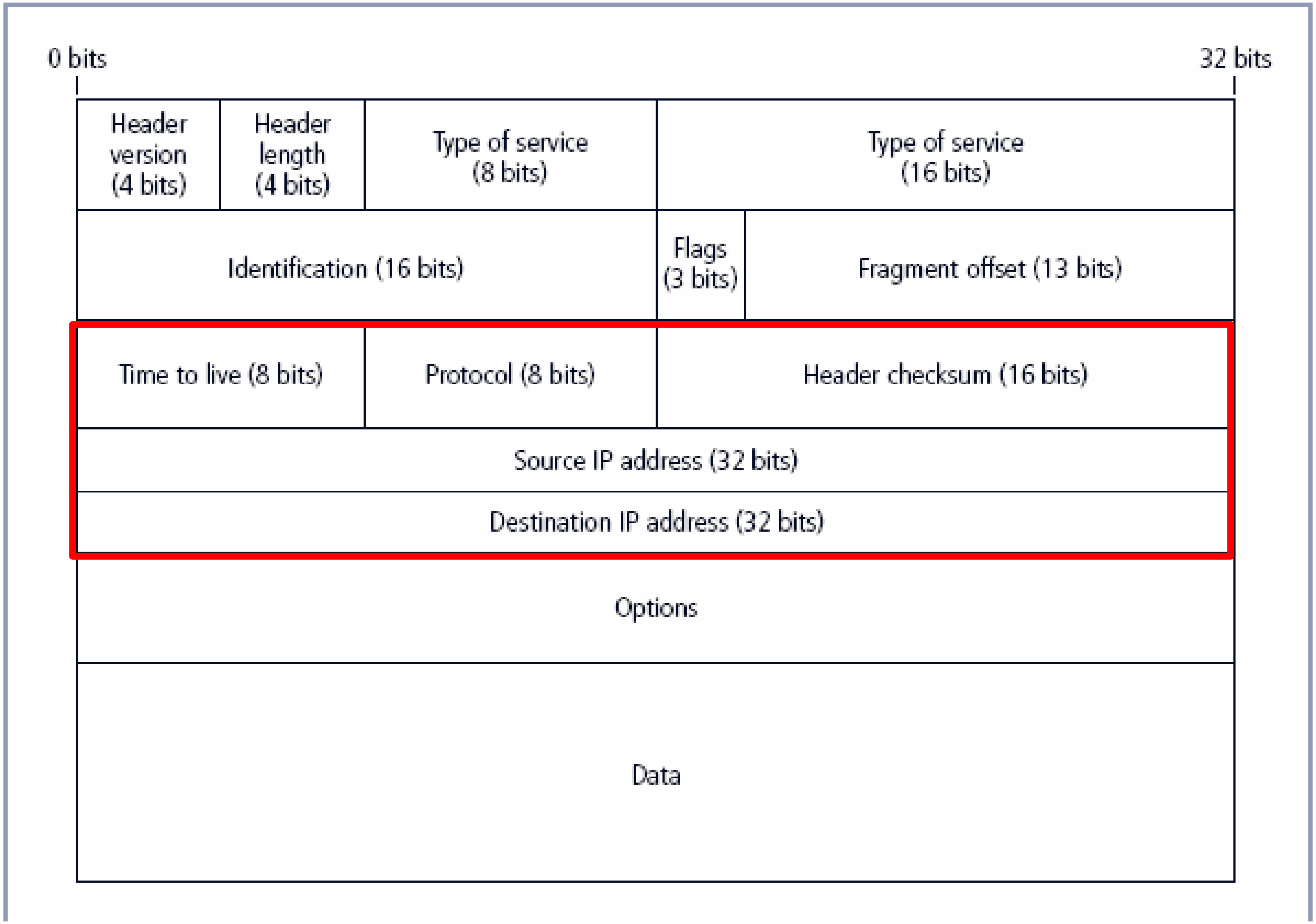
Packet Filtering (1)

- Packet filtering firewalls examine header info. for data pkts
- 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), destination port requests
- Simple firewall models enforce rules that prohibit packets with certain IP address ranges

Packet Filtering (2)

- Three subsets of packet filtering firewalls:
  - *Static filtering:* requires manual configuration of firewall rules that determine which packets are allowed, denied
  - *Dynamic filtering:* firewall can react to emergent event, update/create rules to deal with it
  - *Stateful inspection:* firewalls track each network connection between internal and external systems using a state table

IPv4 Packet Structure (Fig. 6-1)

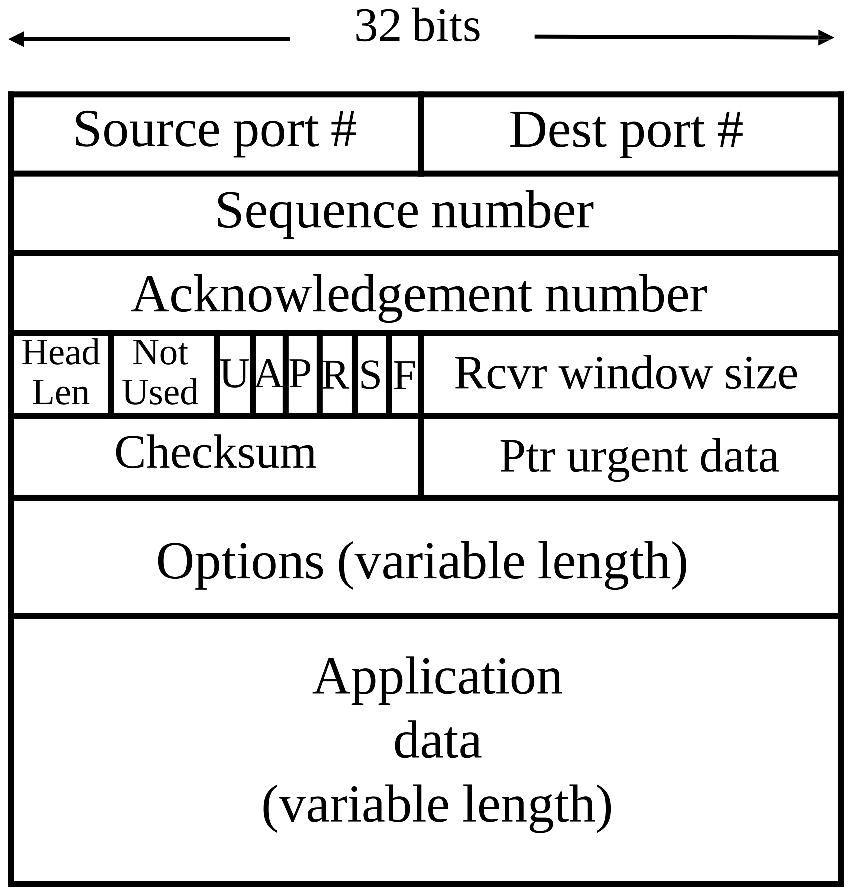


0 bits 32 bits

<table>
<tr><td>Header version (4 bits)</td><td>Header length (4 bits)</td><td>Type of service (8 bits)</td><td colspan="2">Type of service (16 bits)</td></tr>
<tr><td colspan="3">Identification (16 bits)</td><td>Flags (3 bits)</td><td>Fragment offset (13 bits)</td></tr>
<tr><td colspan="2">Time to live (8 bits)</td><td>Protocol (8 bits)</td><td colspan="2">Header checksum (16 bits)</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

TCP, UDP Segment Structures

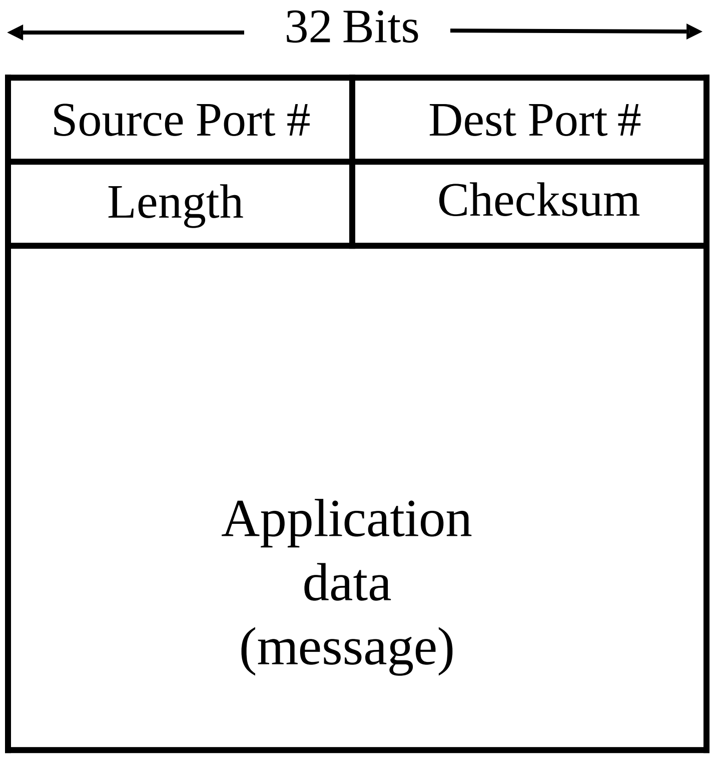
TCP Segment



32 bits

<table>
<tr><td colspan="8">Source port #</td><td>Dest port #</td></tr>
<tr><td colspan="9">Sequence number</td></tr>
<tr><td colspan="9">Acknowledgement number</td></tr>
<tr><td>Head
Len</td><td>Not
Used</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Rcvr window size</td></tr>
<tr><td colspan="8">Checksum</td><td>Ptr urgent data</td></tr>
<tr><td colspan="9">Options (variable length)</td></tr>
<tr><td colspan="9">Application
data
(variable length)</td></tr>
</table>

UDP Segment



32 Bits

<table>
<tr><td>Source Port #</td><td>Dest Port #</td></tr>
<tr><td>Length</td><td>Checksum</td></tr>
<tr><td colspan="2">Application
data
(message)</td></tr>
</table>

Source: J.F. Kurose and K.W. Ross, *Computer Networking: A Top-Down Approach*, 7th ed., Addison-Wesley, 2013.

Packet Filtering Router (Fig. 6-4)

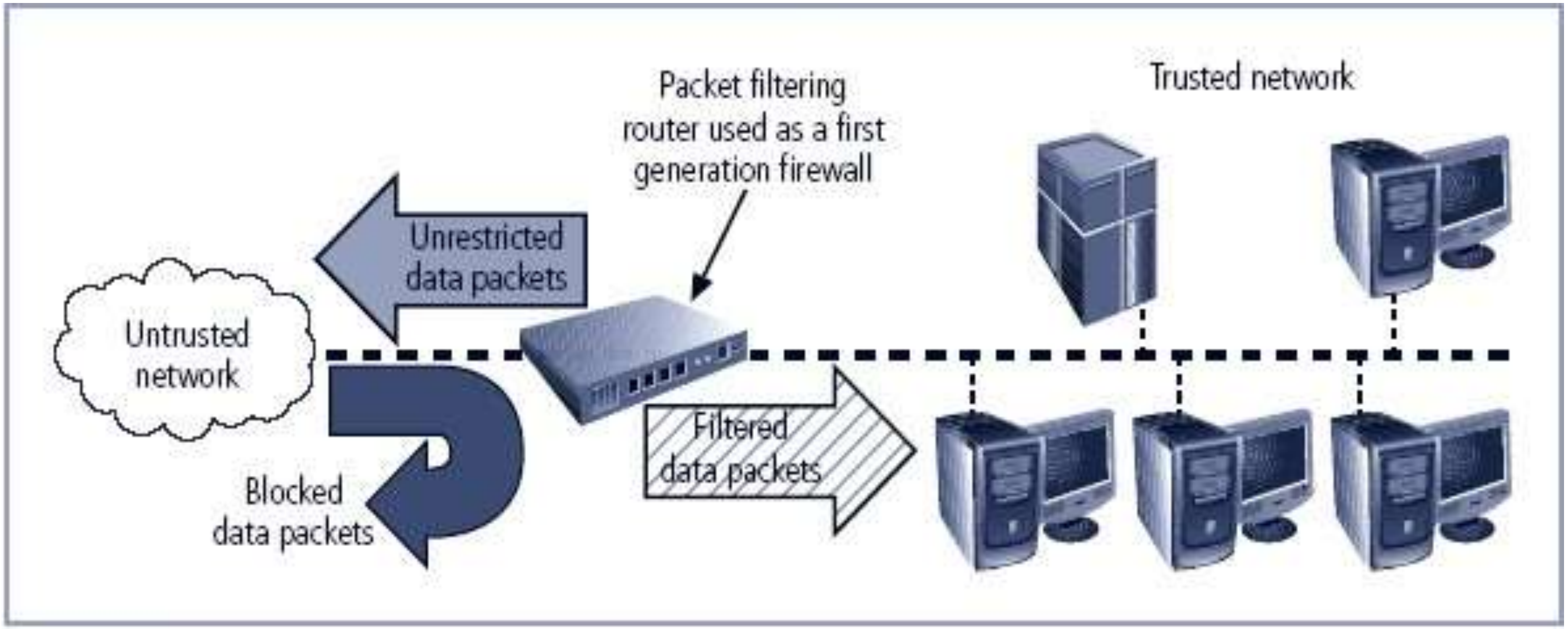


FIGURE 6-4 Packet Filtering Router

Sample Firewall Rules (Table 6-1)

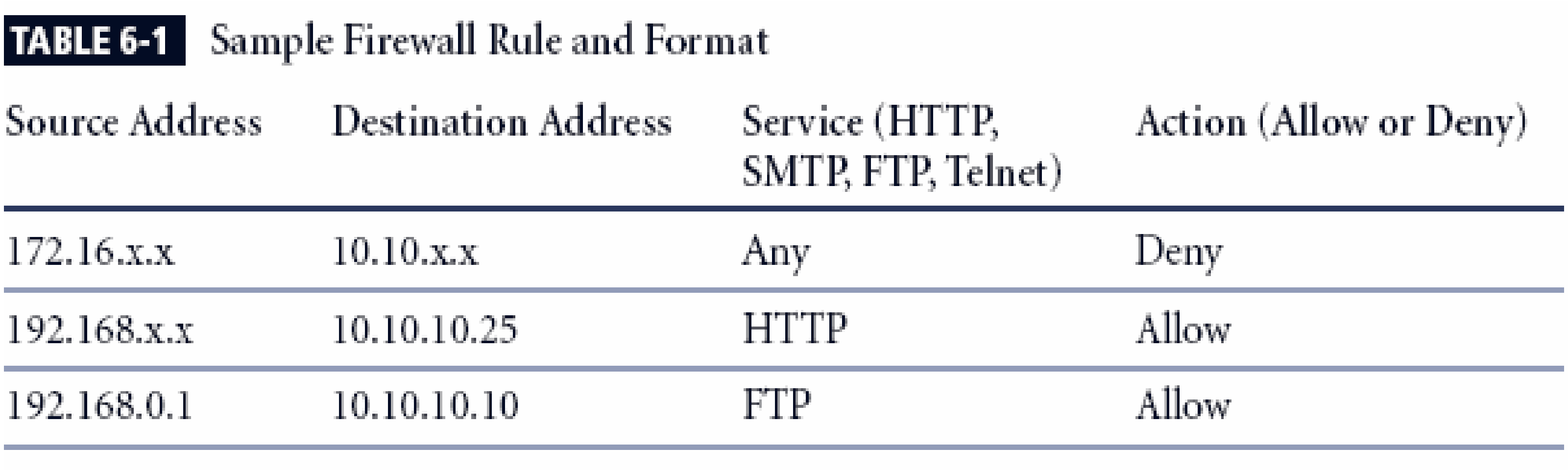


TABLE 6-1 Sample Firewall Rule and Format

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 called *proxy server*
- Proxy server is often placed in unsecured area of network (e.g., DMZ) ⇒it faces higher levels of risk from attackers
- We can place extra filtering routers behind the proxy server to protect internal systems

Circuit Gateways

- Circuit gateway firewall: transport layer
- Does not usually look at data traffic flowing between two networks; prevents direct connections between one network and another
- Mechanism: create tunnels connecting specific processes/systems on each side of firewall; only allow authorized traffic in tunnels

MAC Layer Firewalls

- Operates at data-link layer
- Considers specific host computer’s identity in filtering decision
- Only outbound traffic originating from MAC addresses of specific computers allowed
  - Mechanism: link (MAC address, Ethernet port #), administered via switches

Hybrid Firewalls

- Combine elements of multiple types of firewalls (e.g., packet filtering and proxy servers; packet filtering and circuit gateways)
- Alternately, may consist of two separate firewall devices; separate firewall systems connected to work together

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 operating system kernel

Firewall Categorization (3): Deployment Structure

- Most firewalls are appliances: stand-alone, self-contained systems
- Commercial firewall systems: consists of firewall software running on general-purpose computer
- Small office/home office (SOHO) or residential firewalls connect users' LANs or specific computers to network devices
  - Often, firewall software placed on user system

Sample Firewall Devices (Fig. 6-6)

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 connecting to Internet
- Routers can be configured to reject packets that org. forbids entering its network
- Drawbacks: limited auditing, weak authentication

Packet Filtering Router (Fig. 6-4)

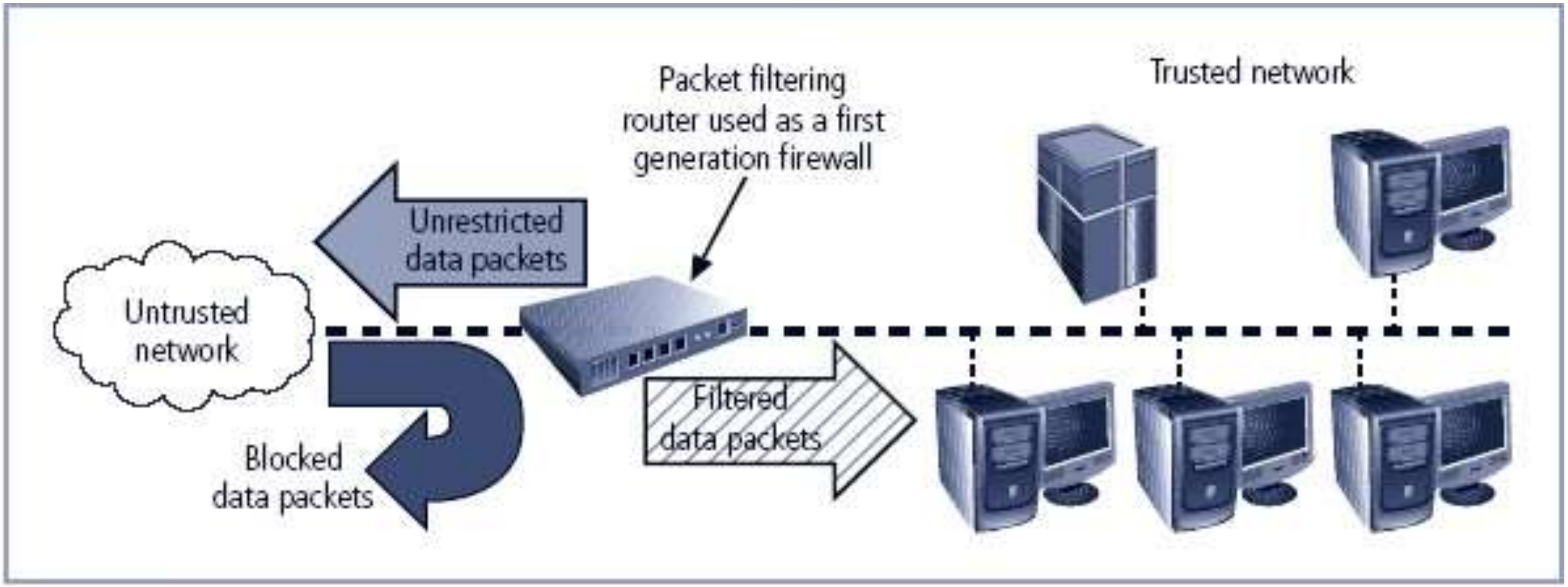


FIGURE 6-4 Packet Filtering Router

Screened Host Firewalls

- Combines packet filtering router with stand-alone firewall (e.g., application proxy server)
- Allows router to pre-screen packets to minimize load on internal proxy
- Separate host is often referred to as *bastion host*; can be rich target for external attacks, needs to be secured carefully

Screened Host Firewall (Fig. 6-11)

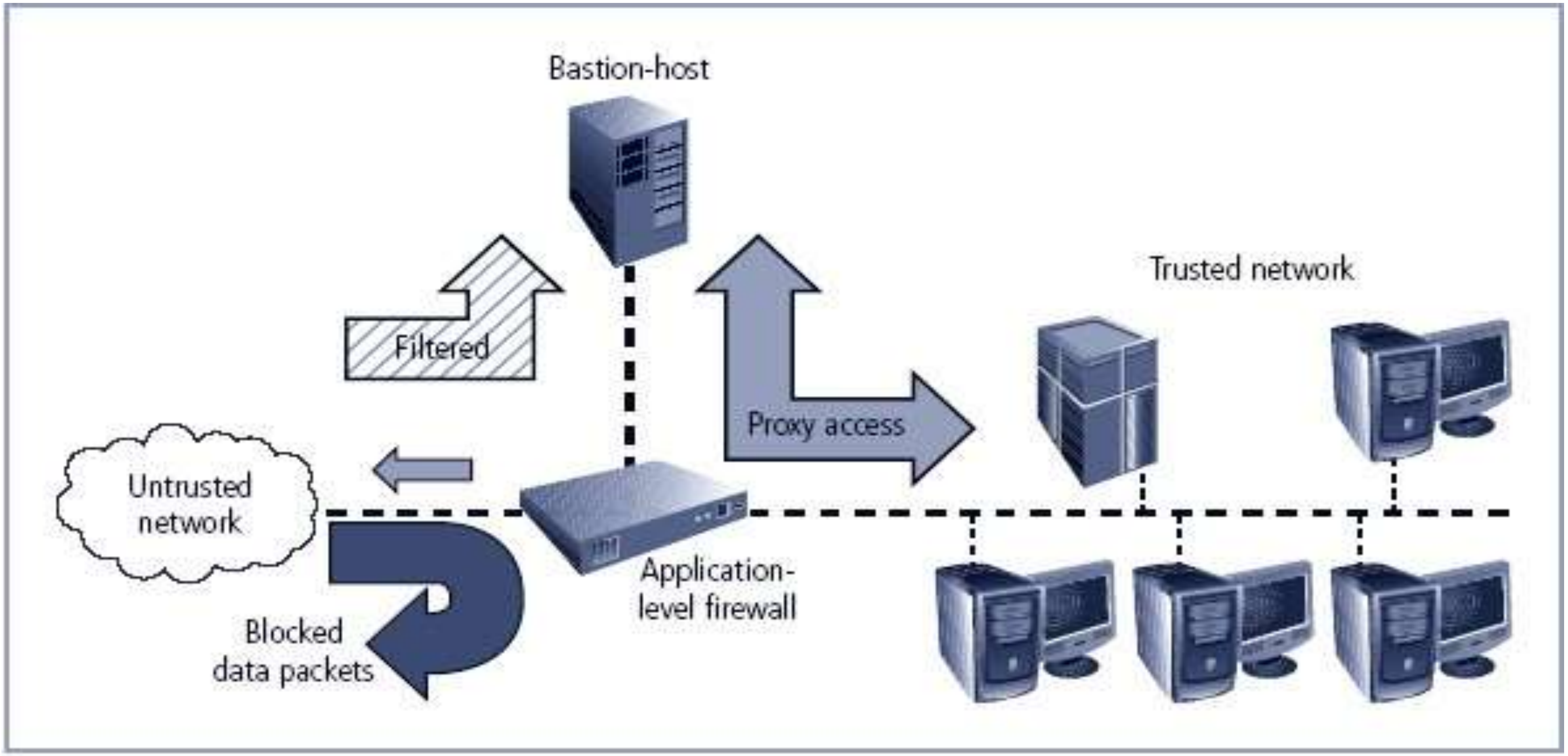


FIGURE 6-11 Screened Host Firewall

Dual-Homed Host Firewalls

- Bastion host contains two network interface cards (NICs): one connected to external network, other connected to internal network

- Architecture typically uses network address translation (NAT)
  - Another barrier to intrusion from attackers

Non-Routable IP Address Ranges

Type	IP Address Range	CIDR Mask	IP Subnet Mask	# Addresses
Class A	10.0.0.0 – 10.255.255.255	/8	255.0.0.0	2^{24} (> 16 M)
Class B	172.16.0.0 – 172.31.255.255	/12 or /16	255.240.0.0 or 255.255.0.0	2^{12} (4,096) or 2^{16} (> 65K)
Class C	192.168.0.0 – 192.168.255.255	/16 or /24	255.255.0.0 or 255.255.255.0	2^{16} (> 65K) or 2^{8} (256)

Source: Adapted from Table 6-4 in textbook, RFC 1918

Dual-Homed Firewall (Fig. 6.12)

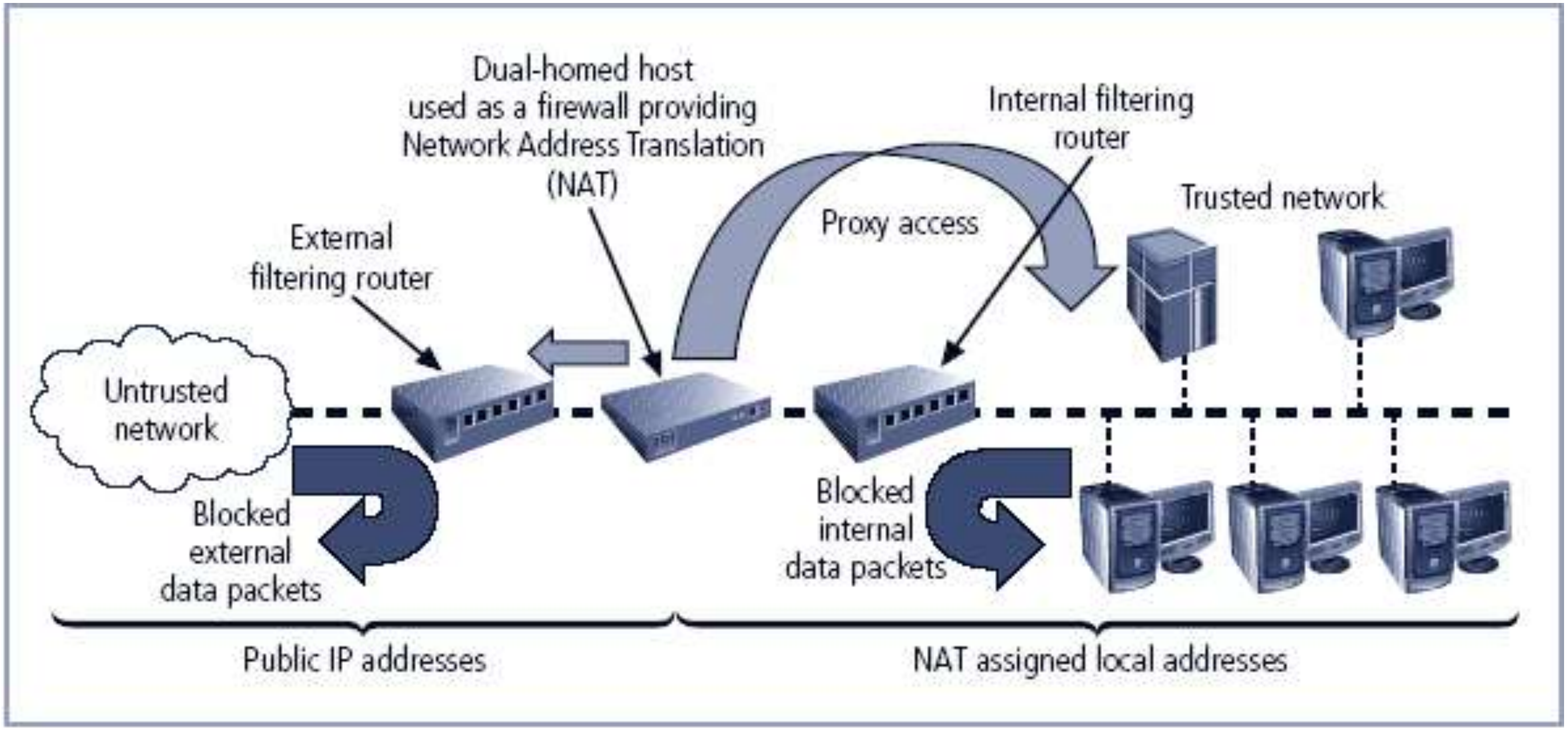

Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

FIGURE 6-12 Dual-Homed Host Firewall

Screened Subnet Firewalls (DMZ) (1)

- Dominant architecture used today
- Typically has ≥ 2 internal bastion hosts behind packet filtering router, each host protects trusted network:
  - Connections from outside (untrusted network) routed through external filtering router
  - Connections from outside (untrusted network) are routed into, out of routing firewall to separate network segment: *demilitarized zone* (DMZ)
  - Connections into trusted internal network allowed only from DMZ bastion host servers

Screened Subnet Firewalls (DMZ) (2)

- 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*

Screened Subnet Firewall (Fig. 6-13)

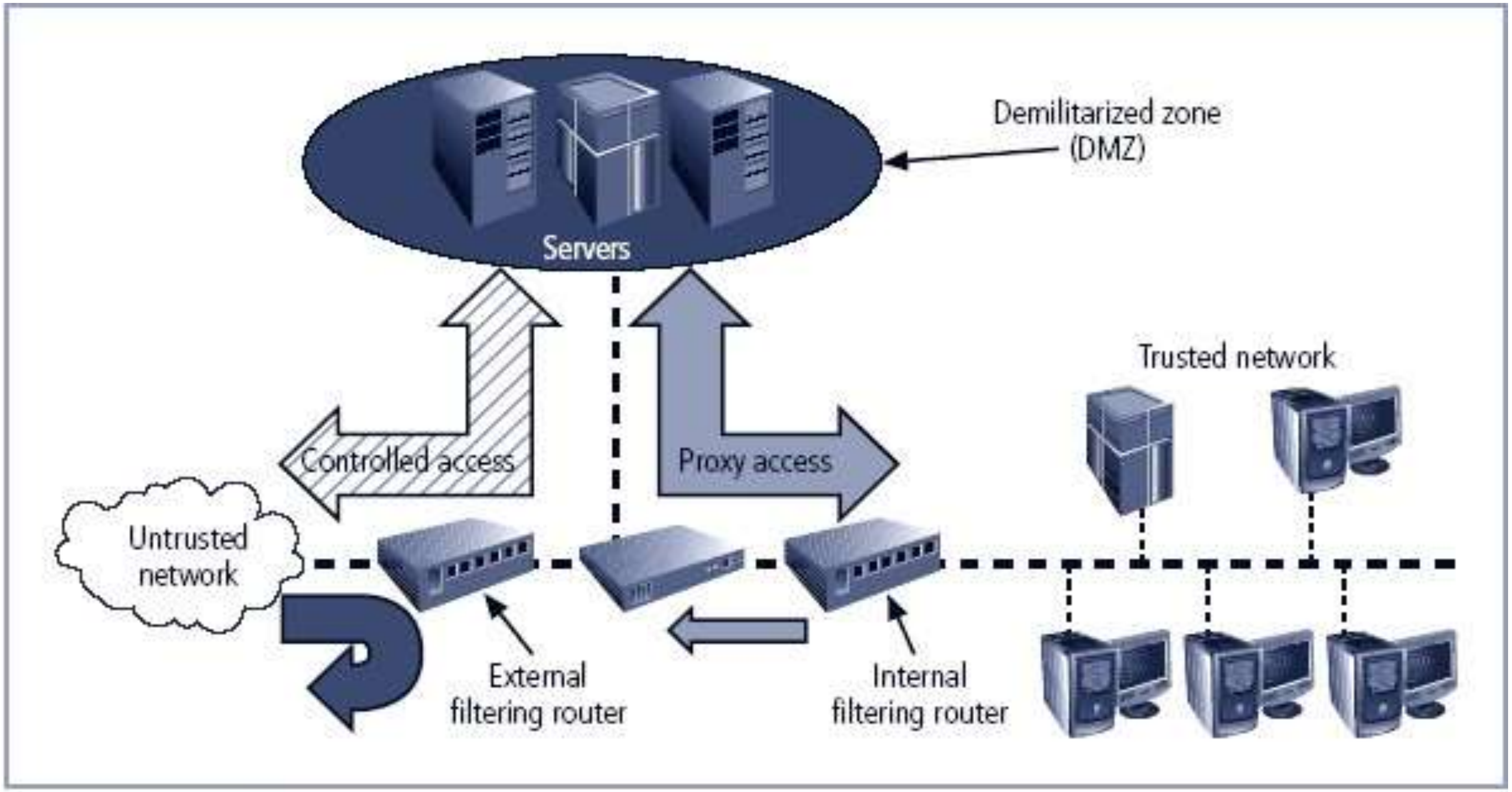


FIGURE 6-13 Screened Subnet (DMZ)

Selecting the Right Firewall

- When selecting firewall, consider a number of factors:
  - Which is the best trade-off between protection, cost for needs of organization?
  - What’s included (and what’s *not*) in base price?
  - How easy is configuration? Are staff technicians available for this purpose?
  - How well firewall adapt to org.’s growing network?
- Second most important issue: 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 (“black art”)
- When security rules conflict with business performance, security often loses!
- Linux firewall

Best Practices for Firewalls

- All traffic from trusted network is allowed out
- Use MAC address filtering for Ethernet ports, authentication for wireless LANs
- Firewall device never directly accessed from public network
- Allow Simple Mail Transport Protocol (SMTP)
- Deny Internet Control Message Protocol (ICMP)
- Telnet access to internal servers should be blocked
- If Web services offered outside firewall, block HTTP traffic 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

Example Network Config. (Fig. 6-14)

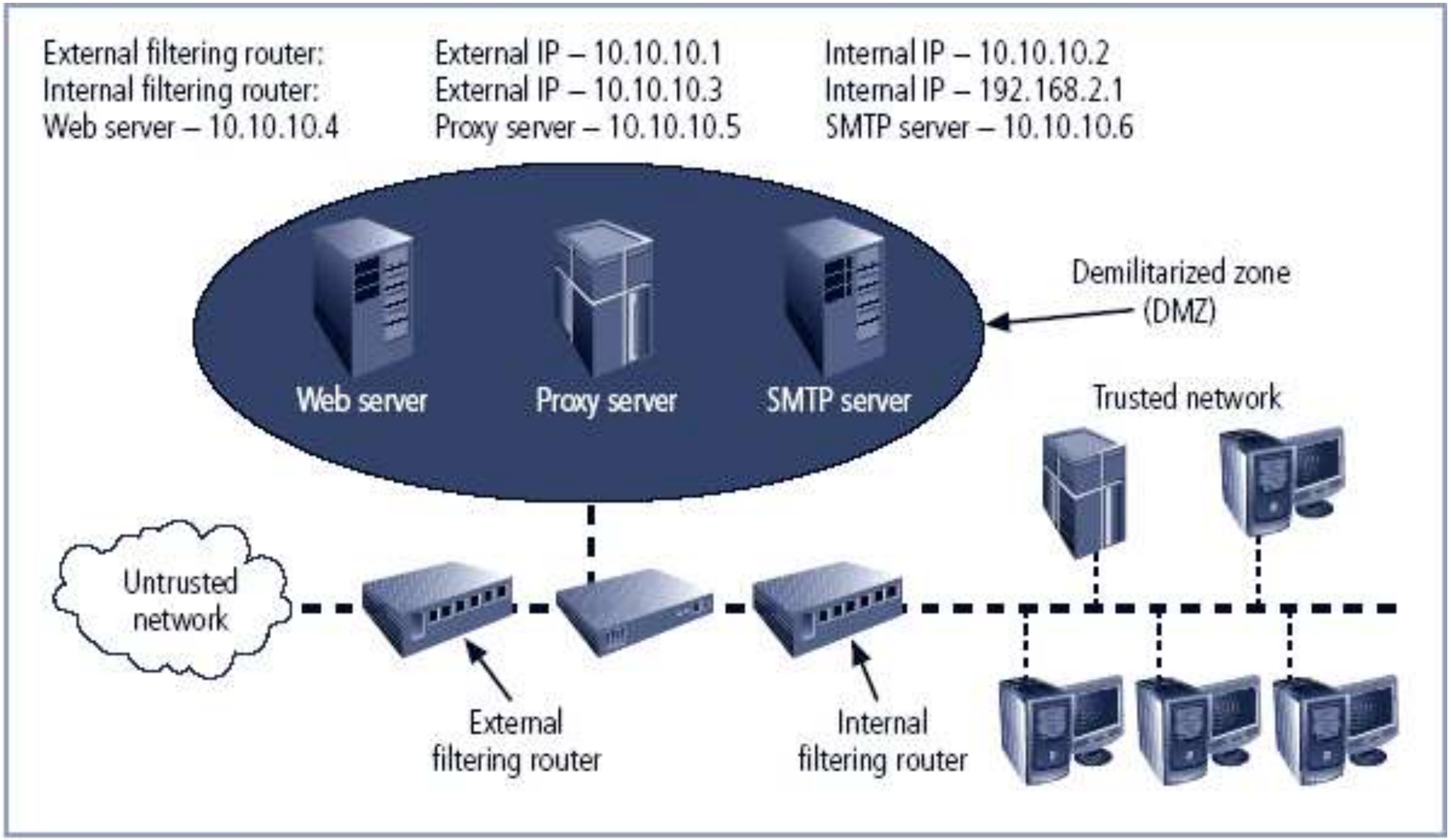


FIGURE 6-14 Example Network Configuration

Firewall Rules (1) (Table 6-16)

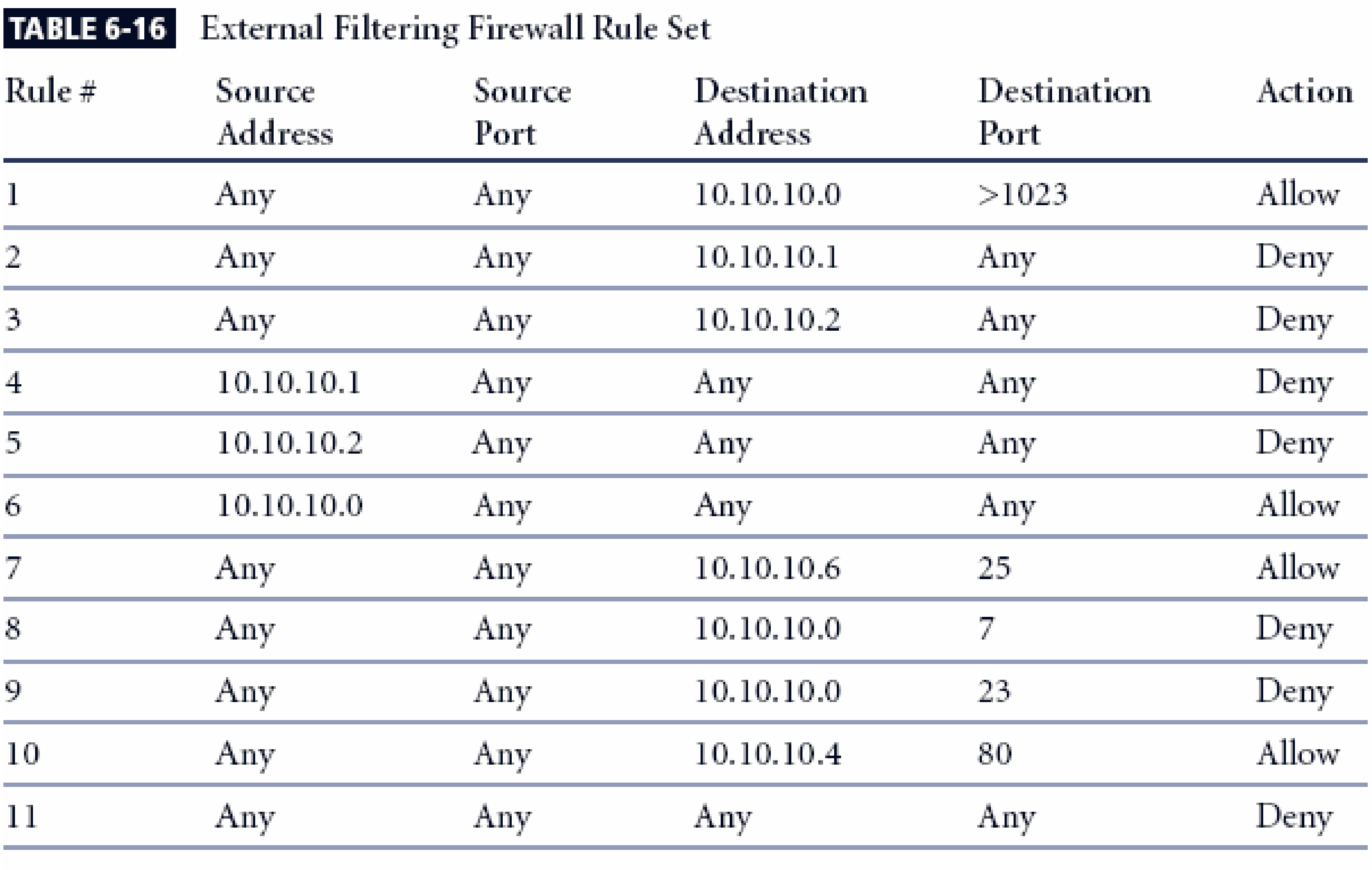


TABLE 6-16 External Filtering Firewall Rule Set

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

Firewall Rules (2) (Table 6-17)

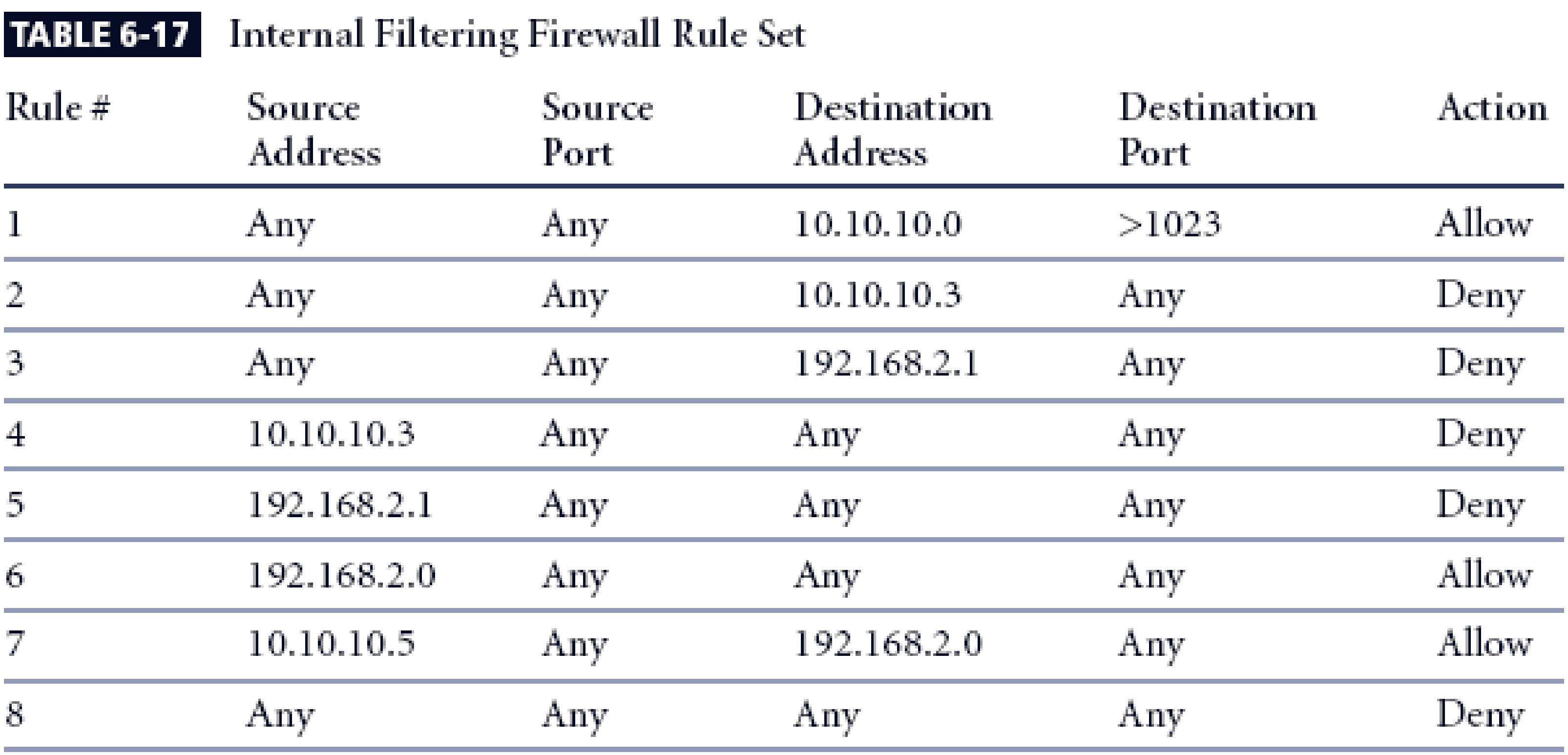


TABLE 6-17 Internal Filtering Firewall Rule Set

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, secure network connection between systems over insecure, public Internet
- Securely extends org.’s internal network connections to remote locations beyond its perimeter

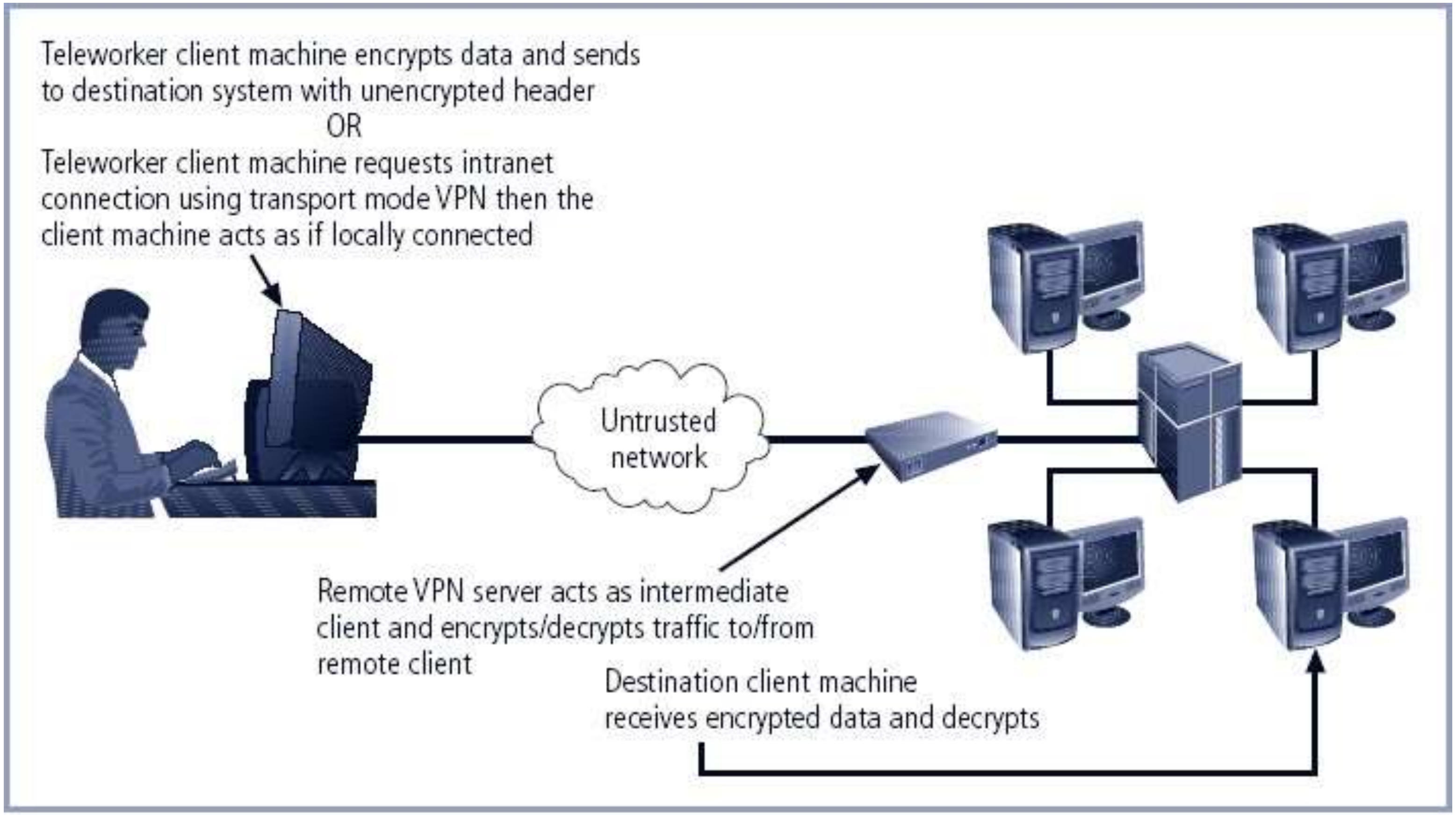
Virtual Private Networks (VPNs) (2)

- VPN must achieve three goals:
  - Encapsulate incoming, outgoing data
  - Encrypt incoming, outgoing data
  - Authenticate remote computer, user (?)

Transport Mode

- IP packet data is encrypted, header info. is not
- Lets user establish secure link directly with remote host easily
- Two popular uses:
  - End-to-end transport of encrypted data
  - Remote worker connects to office network over Internet by connecting to VPN server at perimeter

Transport Mode VPN (Fig. 6-18)



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

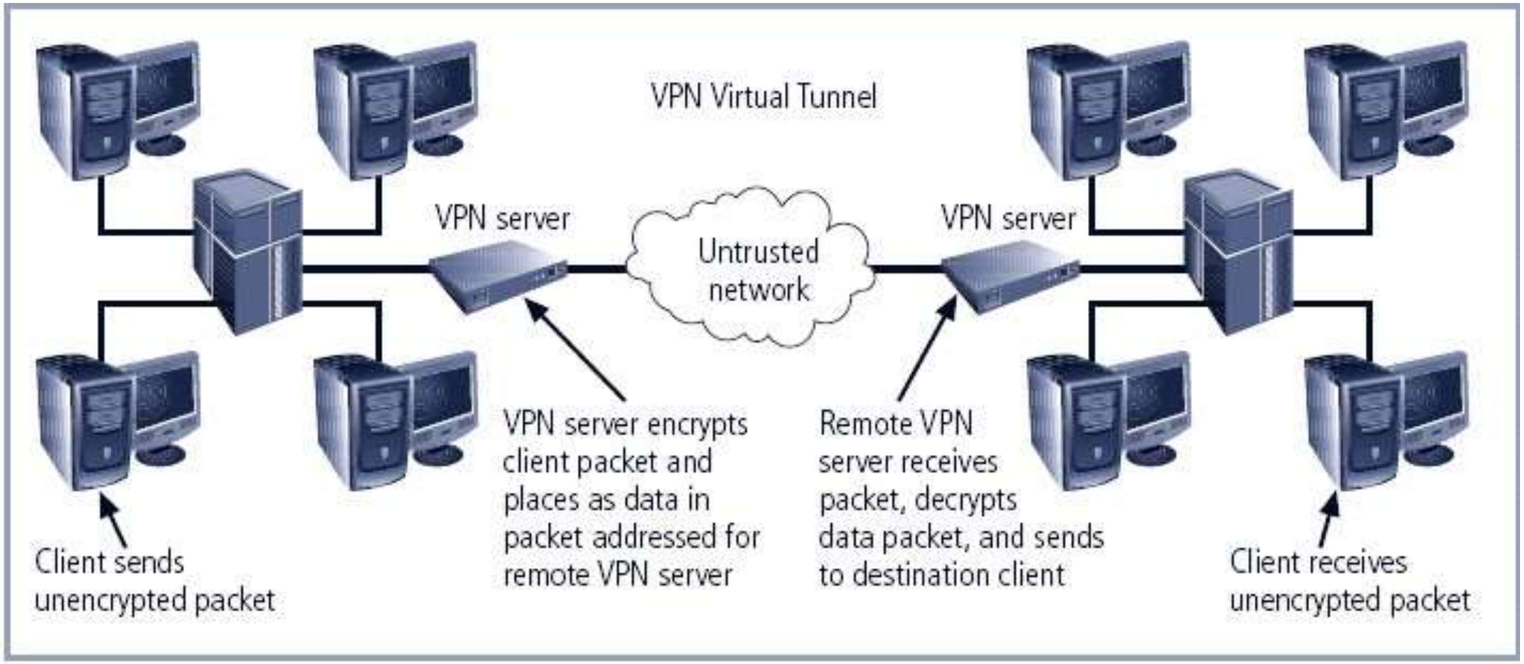
Destination client machine receives encrypted data and decrypts

FIGURE 6-18 Transport Mode VPN

Tunnel Mode

- Org. sets up two perimeter tunnel servers as *encryption points*: all net traffic encrypted in transit
- Main benefit to tunnel mode: intercepted packets reveal nothing about true destination
- Examples of tunnel mode VPNs:
  - Pulse Secure appliance
  - Microsoft Internet Application Gateway

Tunnel Mode VPN (Fig. 6-19)



VPN server encrypts client packet and places as data in packet addressed for remote VPN server

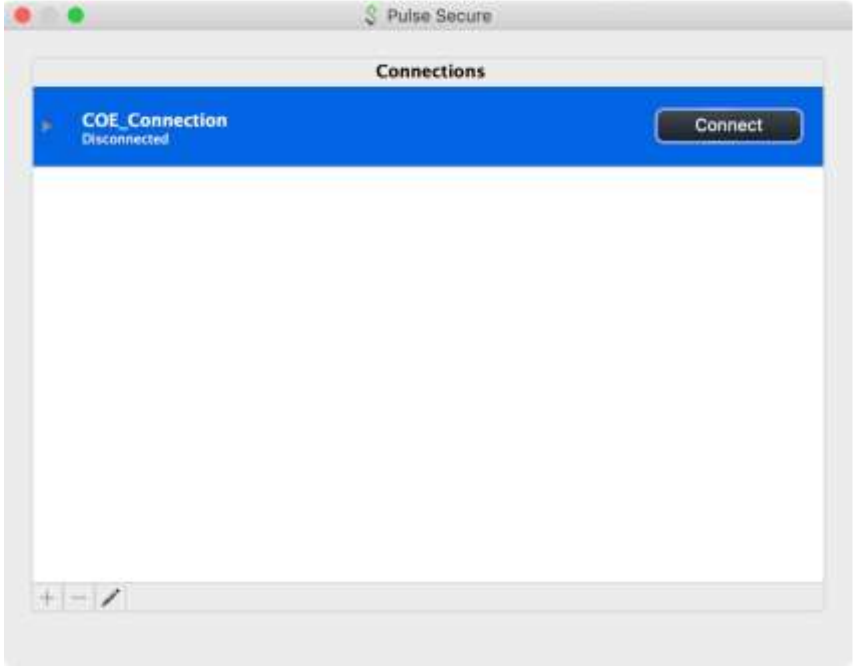
Remote VPN server receives packet, decrypts data packet, and sends to destination client

Client sends unencrypted packet

Client receives unencrypted packet

FIGURE 6-19 Tunnel Mode VPN

Example VPN: Pulse Secure



Source: Pulse Secure, LLC; https://www.pulsesecure.net/products/psa-series/ (PSA 5000)

– More VPN info: A. Marshall, Tech Radar, https://www.techradar.com/vpn/best-vpn, 16 May 2019.

Summary

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