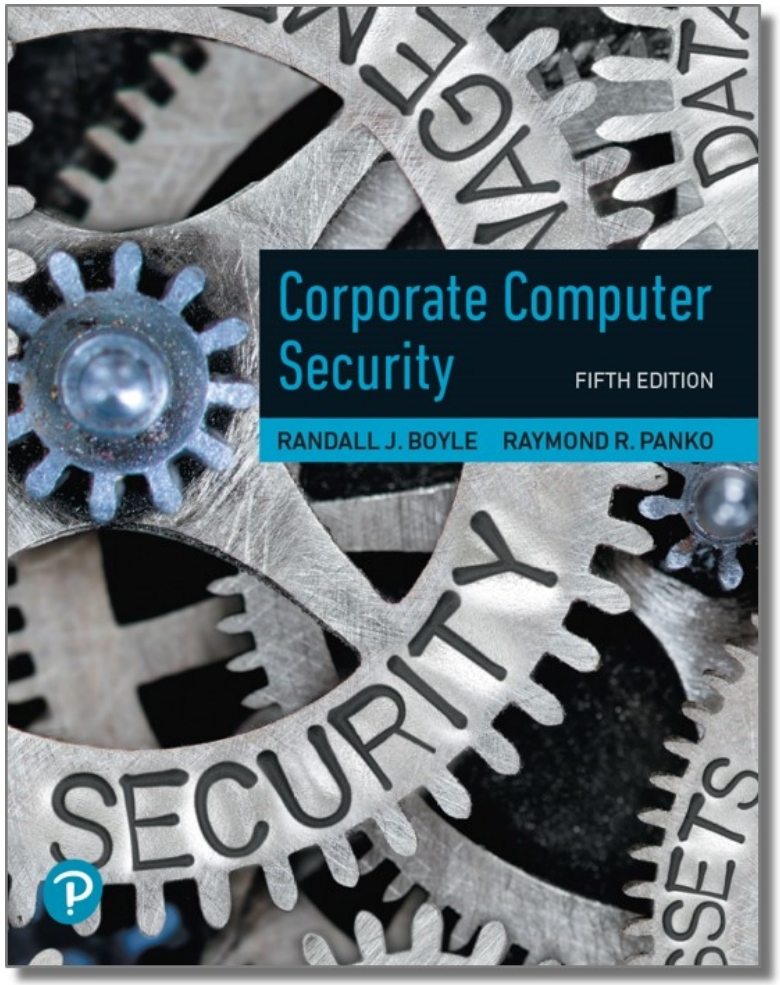
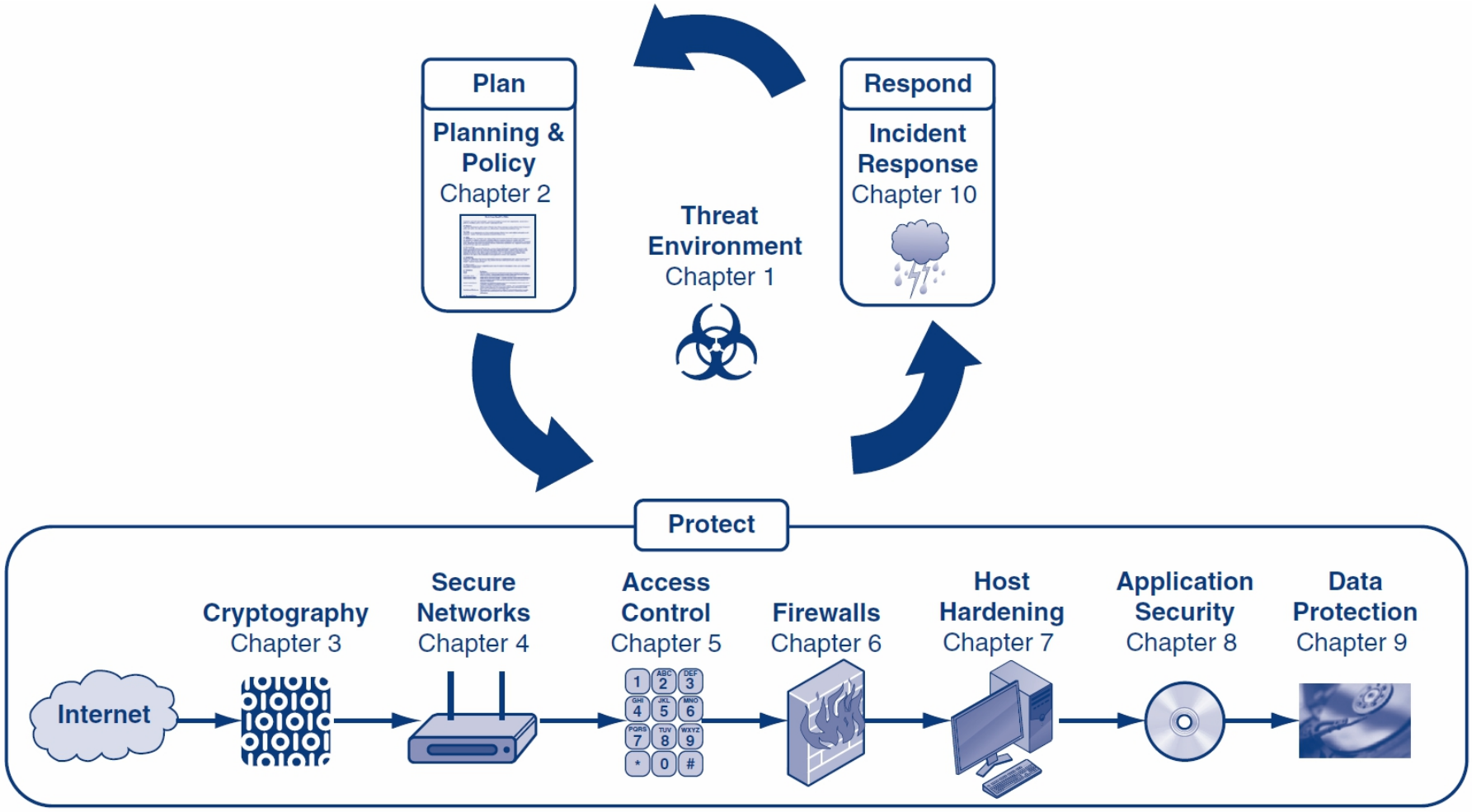


Chapter 6

Firewalls


Plan
Planning & Policy
Chapter 2
Respond
Incident Response
Chapter 10
Threat Environment
Chapter 1
Protect
Internet
Cryptography
Chapter 3
Secure Networks
Chapter 4
Access Control
Chapter 5
Firewalls
Chapter 6
Host Hardening
Chapter 7
Application Security
Chapter 8
Data Protection
Chapter 9

Learning Objectives (1 of 2)

6.1 Define firewalls in general (basic operation, architecture, and the problem of overload).

6.2 Describe how static packet filtering works.

6.3 Explain stateful packet inspection (SPI) for main border firewalls.

6.4 Describe how network address translation (NAT) works.

6.5 Explain application proxy firewalls and content filtering in SPI firewalls.

Learning Objectives (2 of 2)

6.6 Distinguish between intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).

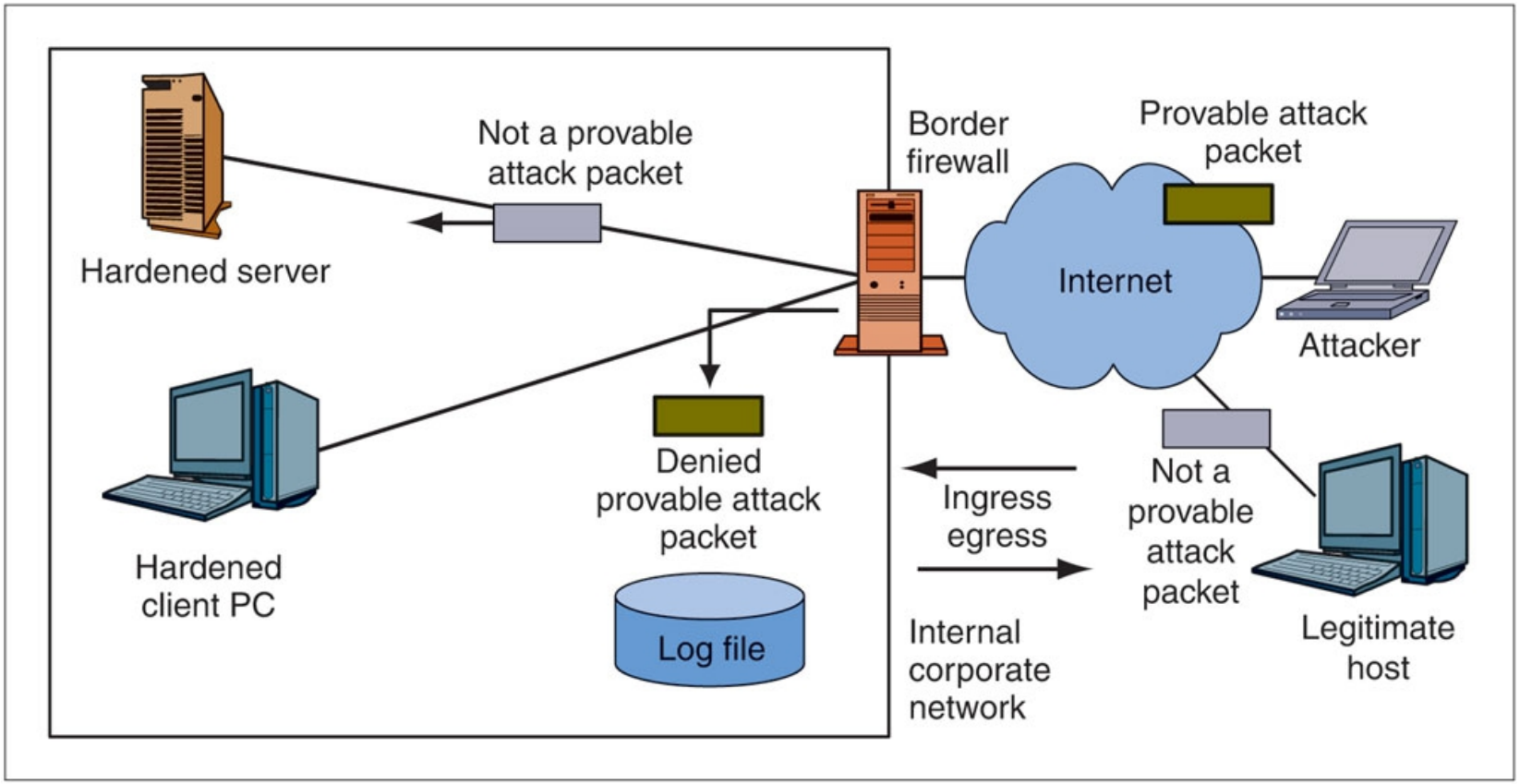
6.7 Describe antivirus filtering.

6.8 Define firewall architectures.

6.9 Describe firewall management (defining policies, implementing policies, reading log files).

6.10 Describe some difficult problems associated with firewalls.

Figure 6-1: Basic Firewall Operation



6.1: Basic Firewall Operation (1 of 4)

The Problem

- If a firewall cannot filter all of the traffic passing through it, it drops packets it cannot process
- This is secure because it prevents attack packets from getting through
- But it creates a self-inflicted denial-of-service attack by dropping legitimate traffic

6.1: Basic Firewall Operation (2 of 4)

Firewall Capacity

- Firewalls must have the capacity to handle the incoming traffic volume
- Some can handle normal traffic but cannot handle traffic during heavy attacks!
- They must be able to handle incoming traffic at wire speed—the maximum speed of data coming into each port

6.1: Basic Firewall Operation (3 of 4)

Processing Power Is Increasing Rapidly

- As processing power increases, more sophisticating filtering methods should become possible
- We can even have Unified Threat Management (UTM), in which a single firewall can use many forms of filtering, including antivirus filtering and even spam filtering. (Traditional firewalls do not do these types of application-level malware filtering.)
- However, increasing traffic is soaking up much of this increasing processing power

6.1: Basic Firewall Operation (4 of 4)

Firewall Filtering Mechanisms

- There are many types
- We will focus most heavily on the most important firewall filtering method, stateful packet inspection (SPI)
- Single firewalls can use multiple filtering mechanisms, most commonly, SPI with other secondary filtering mechanisms

6.2: Static Packet Filtering (1 of 5)

Static Packet Filtering

- This was the earliest firewall filtering mechanism
- Limits
  - Examines packets one at a time, in isolation
  - Only looks at some internet and transport headers
  - Consequently, unable to stop many types of attacks

6.2: Static Packet Filtering (2 of 5)

Inspects Packets One at a Time, in Isolation

- If it receives a packet containing a SYN/ACK segment, this may be a legitimate response to an internally initiated SYN segment
  - The firewall must pass packets containing these segments, or internally initiated communications cannot exist

6.2: Static Packet Filtering (3 of 5)

Inspects Packets One at a Time, in Isolation

- However, this SYN/ACK segment could be an external attack
  - It could be sent to elicit an RST segment confirming that there is a victim at the IP address to which the SYN/ACK segment is sent
  - A static packet filtering firewall cannot stop this attack

6.2: Static Packet Filtering (4 of 5)

Static Packet Filtering Can Stop Certain Attacks Very Efficiently

- Incoming ICMP Echo packets and other scanning probe packets
- Outgoing responses to scanning probe packets
- Packets with spoofed IP addresses (e.g., incoming packets with the source IP addresses of hosts inside the firm)
- Packets that have nonsensical field settings, such as a TCP segment with both the SYN and FIN bits set

6.2: Static Packet Filtering (5 of 5)

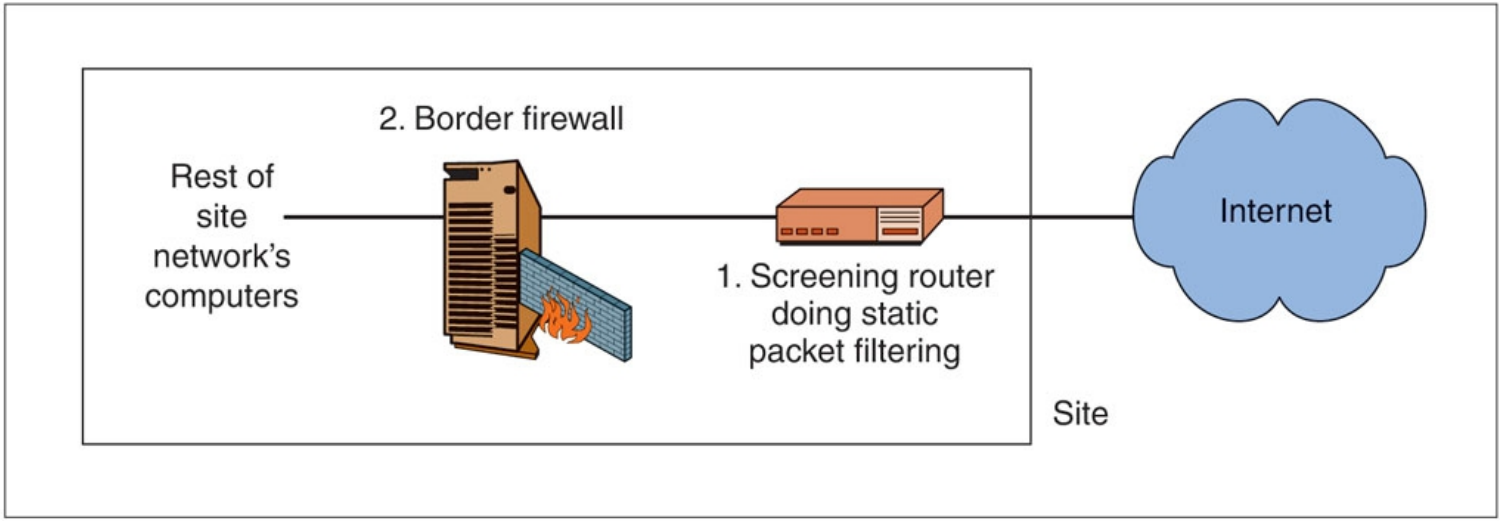
Market Status

- No longer used as the main filtering mechanism for border firewalls
- May be used as a secondary filtering mechanism on main border firewalls

Figure 6-4: Main Border Firewall and Screening Router That Uses Static Packet Filtering

Market Status

- Also may be implemented in border routers, which lie between the Internet and the firewall
  - Stops simple, high-volume attacks to reduce the load on the main border firewall



6.3: Stateful Packet Inspection (1 of 7)

Nearly all corporate border firewalls today use the stateful packet inspection (SPI) filtering method

- SPI focuses on connections
  - Persistent conversations between different programs on different computers

6.3: States in a Connection

Connections have distinct states or stages

Different states are subject to different attacks

Stateful firewalls use different filtering rules for different states

Figure 6-5: States in a Connection

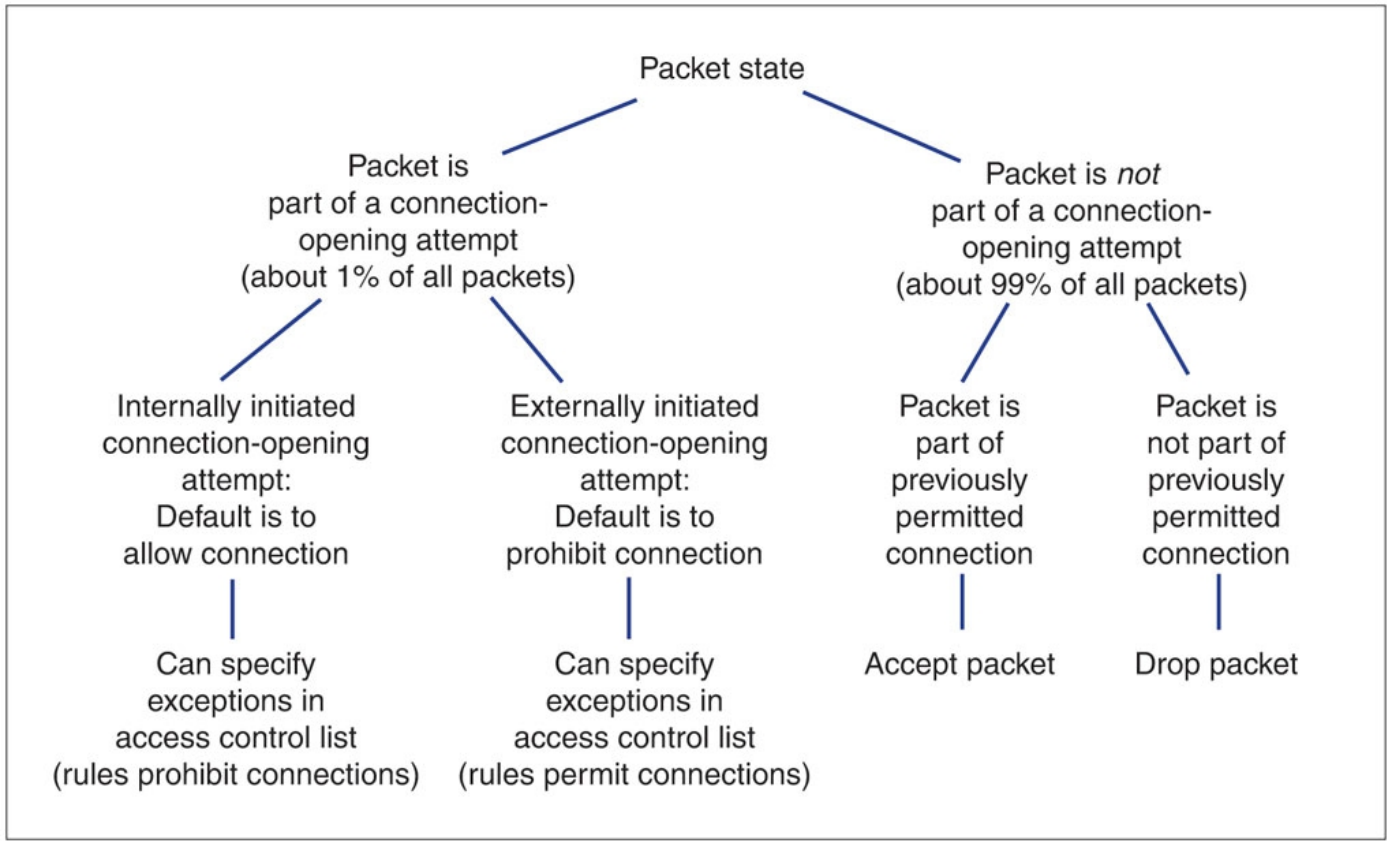
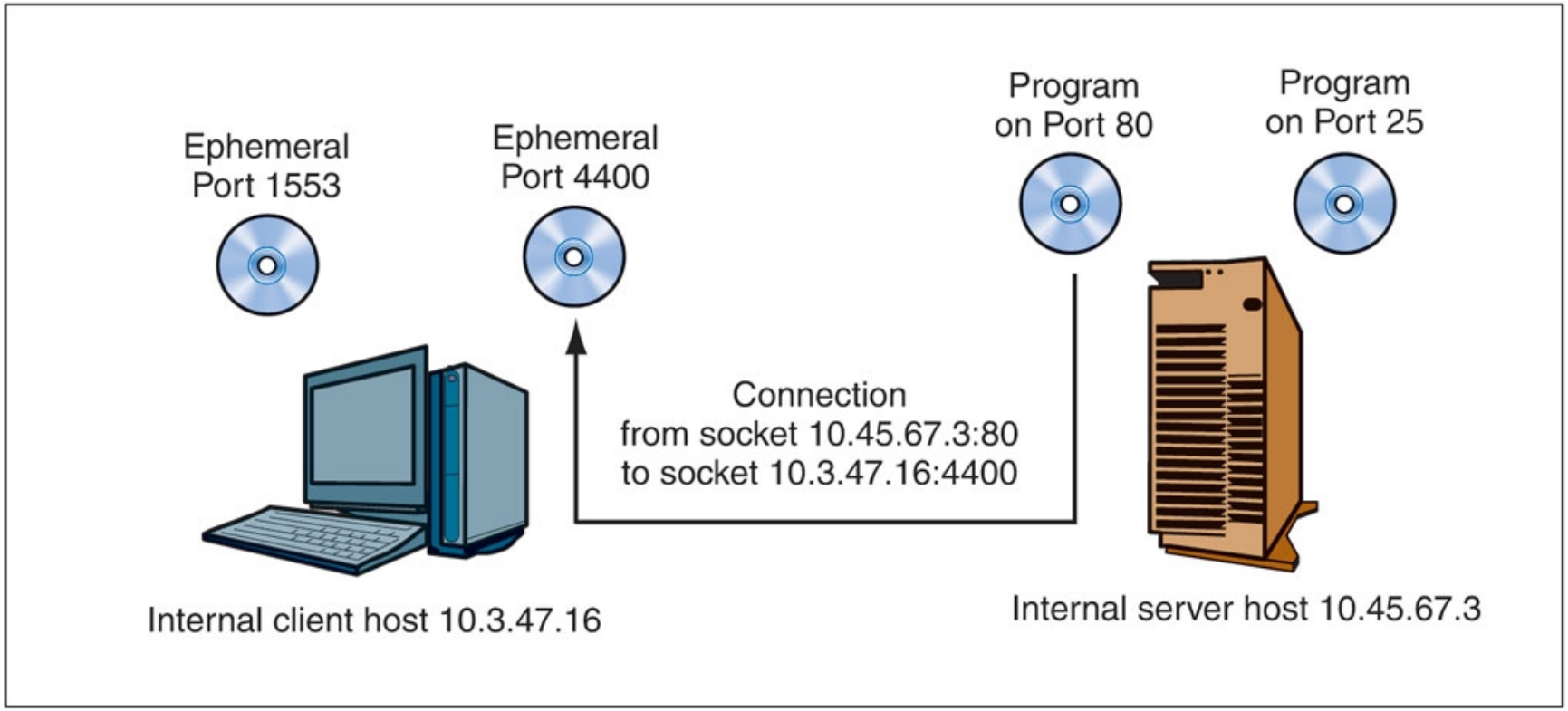
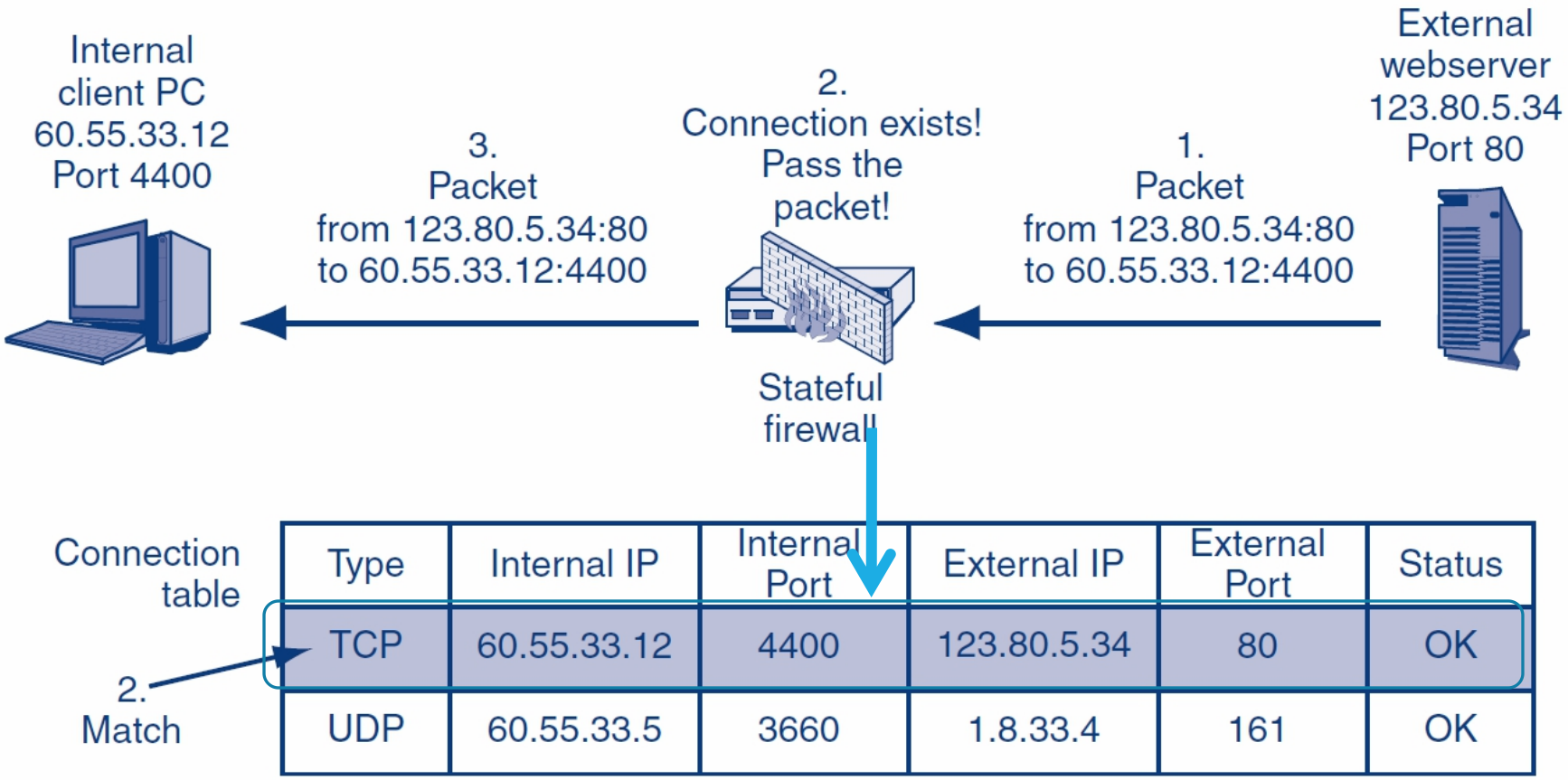


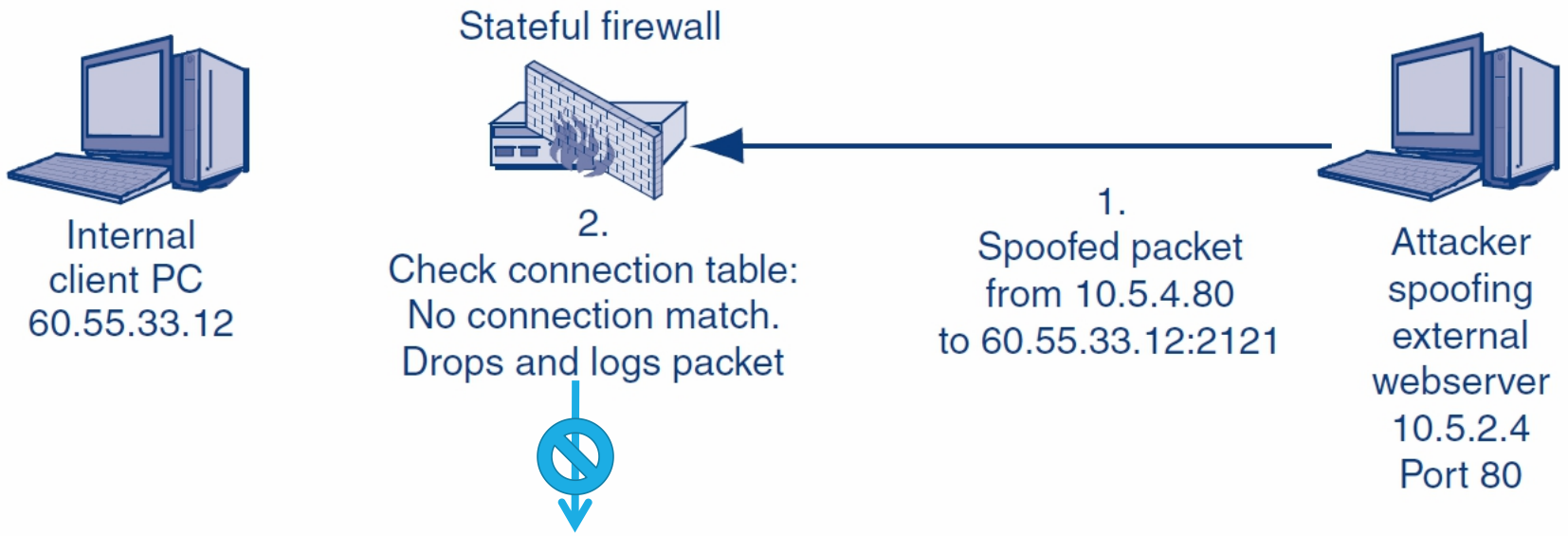
Figure 6-6: Connection and Socket



6.3: Stateful Packet Inspection for a Packet that Does Not Attempt to Open a Connection I



6.3: Stateful Packet Inspection for a Packet that Does Not Attempt to Open a Connection II



Connection table

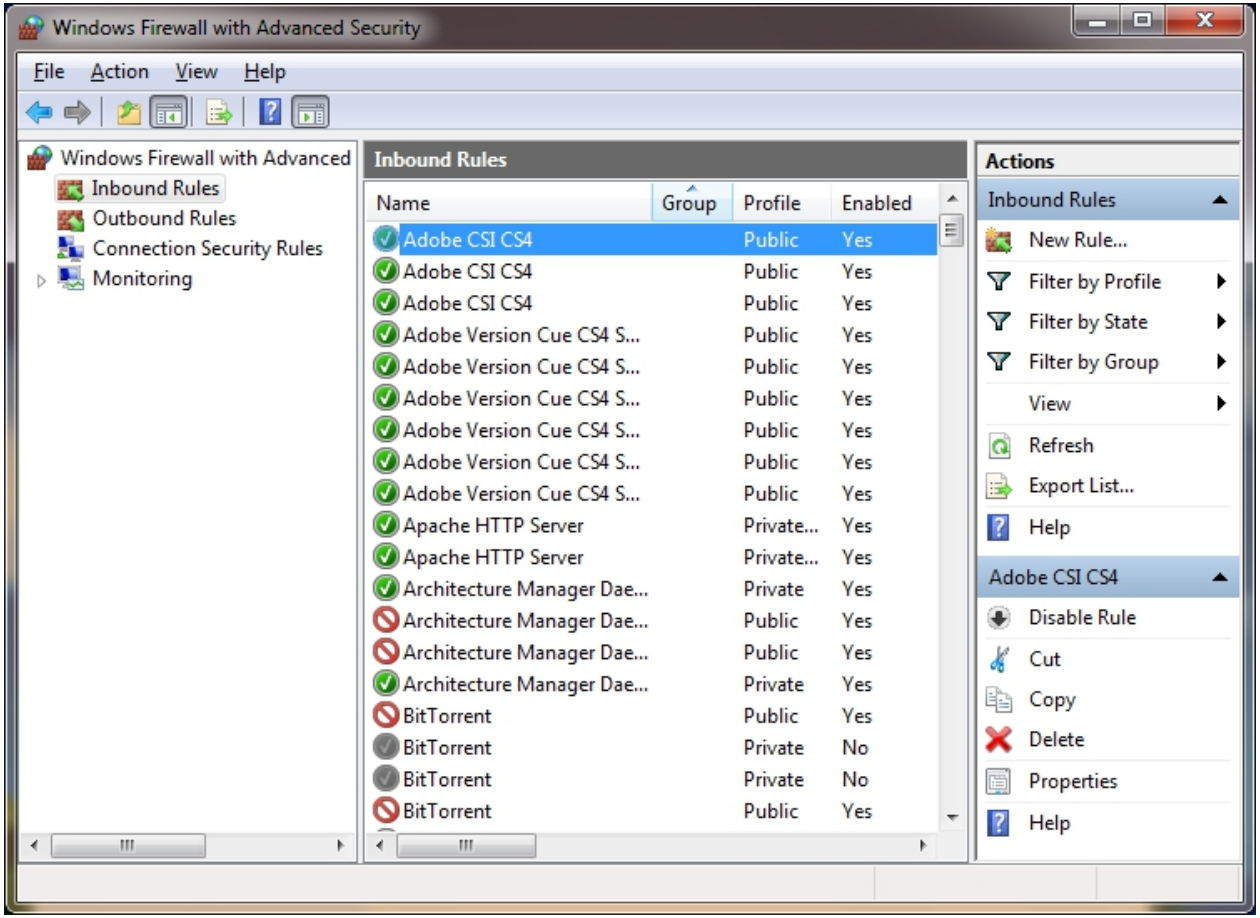
Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	4400	123.80.5.34	80	OK
UDP	60.55.33.12	3660	1.8.33.4	161	OK

6.3: Well-Known Port Numbers

Port	Primary Protocol*	Application
20	TCP	FTP Data Traffic
21	TCP	FTP Supervisory Connection
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	TCP	Domain Name System (DNS)
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP)
135–139	TCP	NETBIOS service for peer-to-peer file sharing in older versions of Windows
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	HTTP over SSL/TLS
3389	TCP	Remote Desktop Protocol (RDP)

*In many cases, both TCP and UDP can be used by an application. In such cases, the same port number is used for both. Typically, however, the use of either TCP or UDP will be predominant.

6.3: Windows Firewall



6.3: Stateful Packet Inspection (2 of 7)

Access Control List Operation

- An ACL is a series of rules for allowing or disallowing connections
- The rules are executed in order, beginning with the first
- If a rule does not apply to the connection-opening attempt, the firewall goes to the next ACL rule
- If the rule does apply, the firewall follows the rule, and no further rules are executed
- If the firewall reaches the last rule in the ACL, it follows that rule

6.3: Stateful Packet Inspection (3 of 7)

Ingress ACL's Purpose

- The default behavior is to drop all attempts to open a connection from the outside
- All ACL rules except for the last give exceptions to the default behavior under specified circumstances
- The last rule applies the default behavior to all connection-opening attempts that are not allowed by earlier rules to be executed by this last rule

6.3: Stateful Packet Inspection (4 of 7)

Simple Ingress ACL with Three Rules

1. If TCP destination port = 80 or TCP destination port = 443, then Allow Connection [Permits connection to ALL internal webservers]
2. If TCP destination port = 25 AND IP destination address = 60.47.3.35, then Allow Connection [Permits connections to a SINGLE internal mail server]
3. Disallow ALL Connections [Disallows all other externally initiated connections; this is the default behavior]

6.3: Stateful Packet Inspection (5 of 7)

Low Cost

- Most packets are not part of packet-opening attempts
- These can be handled very simply and therefore inexpensively
- Connection-opening attempt packets are more expensive processes but are rare

6.3: Stateful Packet Inspection (6 of 7)

Safety

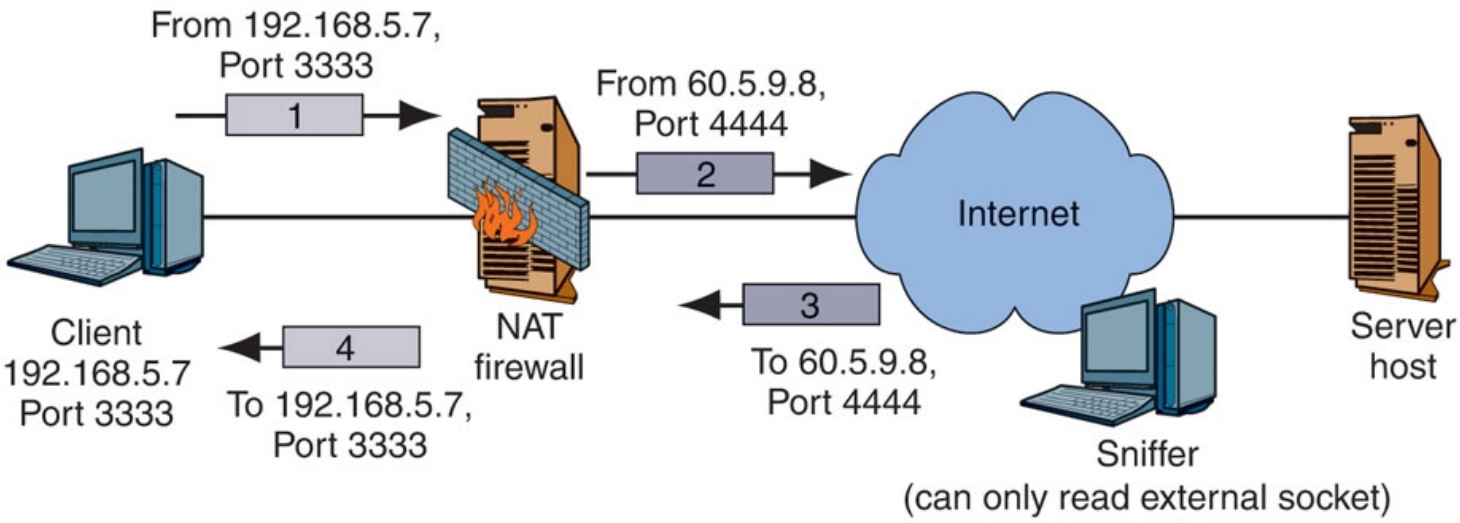
- Attacks other than application-level attacks usually fail to get through SPI firewalls
- In addition, SPI firewalls can use other forms of filtering when needed

6.3: Stateful Packet Inspection (7 of 7)

Dominance

- The combination of high safety and low cost makes SPI firewalls extremely popular
- Nearly all main border firewalls today use stateful packet inspection

Figure 6-12 Network Address Translation (NAT)



Translation table

Internal		External	
IP Addr	Port	IP Addr	Port
192.168.5.7	3333	60.5.9.8	4444
. . .	. . .	. . .	. . .

6.4: Network Address Translation

NAT/PAT

- Important to understand that NAT translates not only network IP addresses but port numbers as well
- NAT is transparent to both the internal and the external hosts
- Certain protocols have problems with NAT

6.5: Application Proxy Firewalls and Content Filtering (1 of 4)

Protections for Internal Clients against Malicious Webservers

- URL blacklists for known attack sites
- Protection against some or all scripts in webpages
- The disallowing of HTTP response messages with prohibited MIME types that indicate malware

6.5: Application Proxy Firewalls and Content Filtering (2 of 4)

Protections against Misbehaving Internal Clients

- Disallowing the HTTP POST method, which can be use to send out sensitive files

6.5: Application Proxy Firewalls and Content Filtering (3 of 4)

Protections for Internal Webservers against Malicious Clients

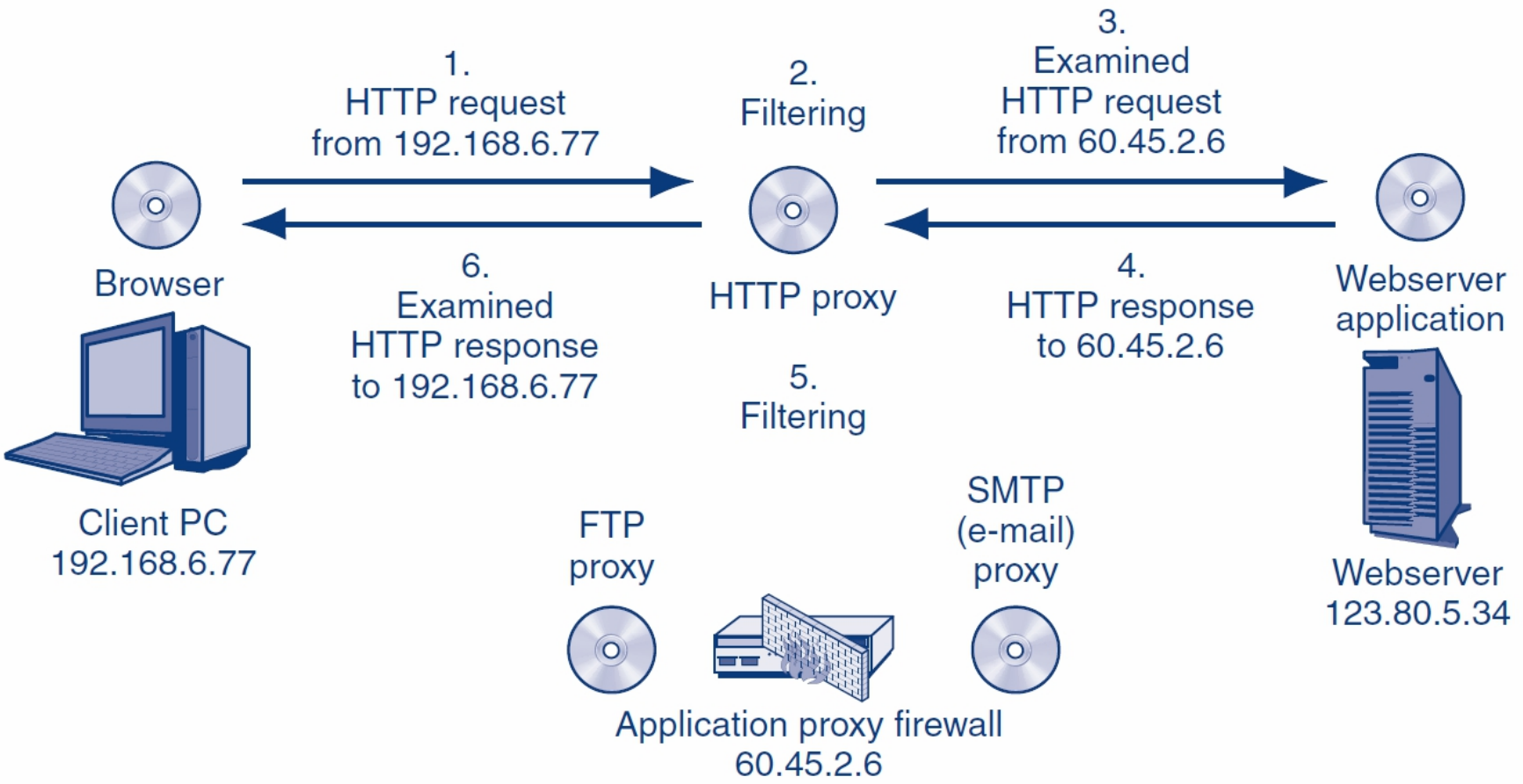
- Disallow HTTP POST methods, which could allow malware files to be placed on the server
- Indications of SQL injection attacks

6.5: Application Proxy Firewalls and Content Filtering (4 of 4)

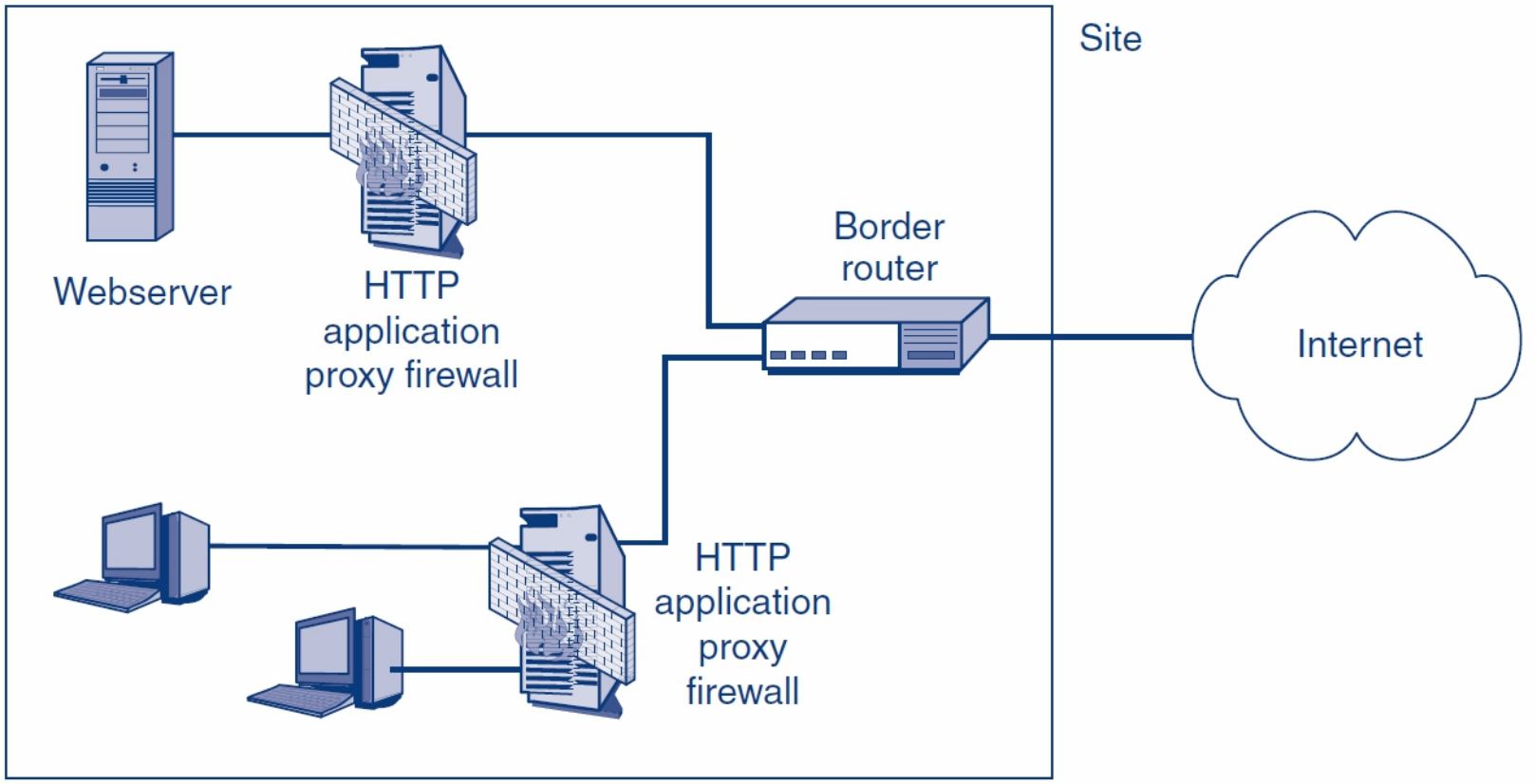
Automatic Protections

- The hiding of internal host IP addresses from sniffers
- Header destruction
  - The data link, internet, and transport headers are discarded—along with any attacks they may have contained
- Protocol fidelity
  - If the client or server does not follow the protocol of the indicated port number, communication with the firewall automatically breaks down

6.5: Application Proxy Firewall Operation



6.5: Roles for Application Proxy Firewalls Today



6.5: Application Content Filtering in Application Proxy Firewalls and Stateful Packet Inspection Firewalls

Topic	Application Proxy Firewalls	Stateful Packet Inspection Firewalls	Remarks
Can examine application layer content	Always	As an Extra Feature	
Capabilities for application layer content filtering	Somewhat More	Somewhat Less	

6.5: Application Content Filtering in Application Proxy Firewalls and Stateful Packet Inspection Firewalls

Topic	Application Proxy Firewalls	Stateful Packet Inspection Firewalls	Remarks
Uses Relay Operation with two connections per client/server pair?	Yes	No	Maintaining two connections is highly processing-intensive. Cannot support many client/server pairs. Consequently, application proxy firewalls cannot be used as main border firewalls.
Speed	Slow	Fast	

6.6: Intrusion Detection Systems and Intrusion Prevention Systems (1 of 4)

Perspective

- Growing processing power made stateful packet inspection possible
- Now, growing processing power is making a new firewall filtering method attractive

6.6: Intrusion Detection Systems and Intrusion Prevention Systems (2 of 4)

Intrusion Detection Systems (IDSs)

- Firewalls drop provable attack packets only
- Intrusion detection systems (IDSs) look for suspicious traffic
  - Cannot drop because the packet is merely suspicious
- Sends an alarm message if the attack appears to be serious

6.6: Intrusion Detection Systems and Intrusion Prevention Systems (2 of 4)

Intrusion Detection Systems (IDSs)

- Problem: Too many false positives (false alarms)
  - Alarms are ignored or the system is discontinued
  - Can reduce false positives by tuning the IDSs
    - Eliminate inapplicable rules, such as a Unix rule in an all-Windows company
    - Reduce the number of rules allowed to generate alarms
    - Most alarms will still be false alarms

6.6: Intrusion Detection Systems and Intrusion Prevention Systems (2 of 4)

Intrusion Detection Systems (IDSs)

- Problem: Heavy processing requirements because of sophisticated filtering
  - Deep packet inspection
    - Looks at application content and transport and internet headers
  - Packet stream analysis
    - Looks at patterns across a series of packets
    - Often, patterns cannot be seen unless many packets are examined

6.6: Intrusion Detection Systems and Intrusion Prevention Systems (3 of 4)

Intrusion Prevention Systems (IPSs)

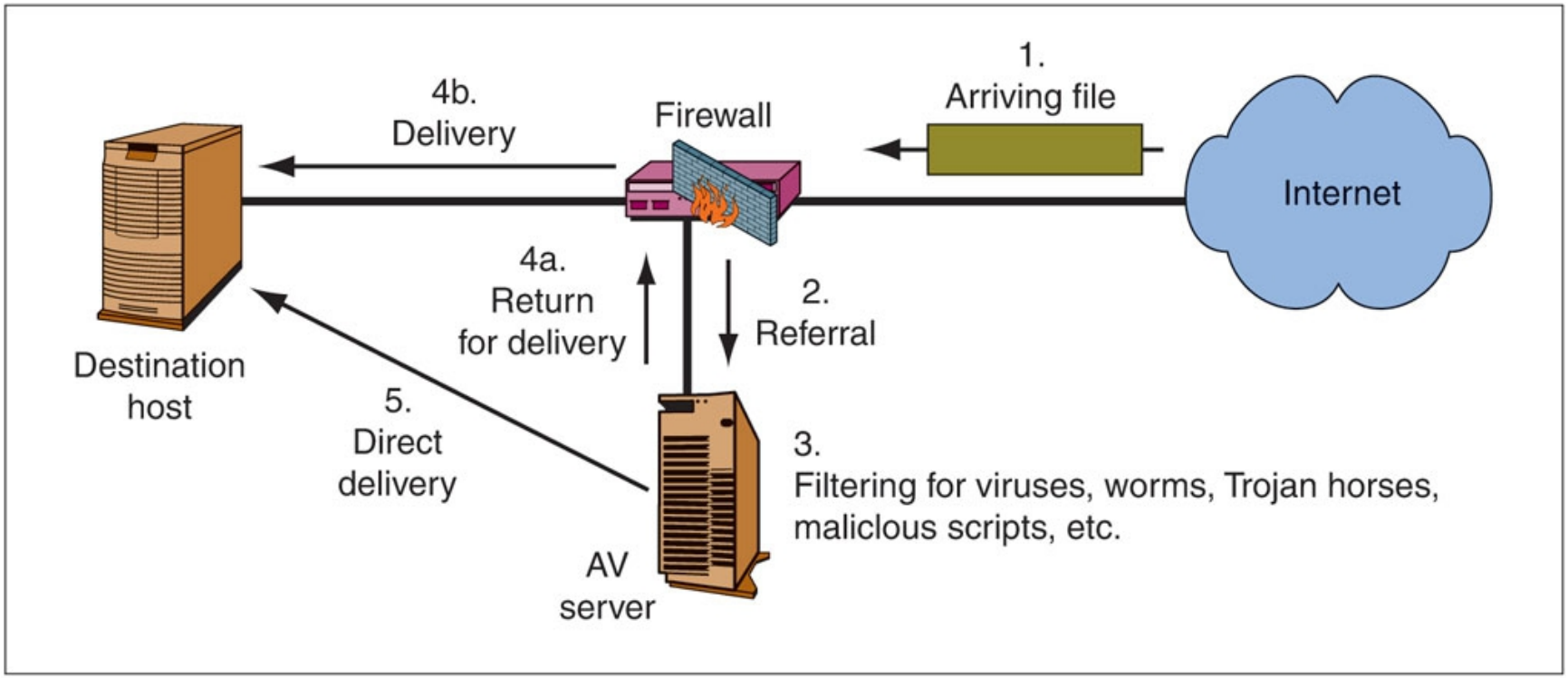
- Use IDS filtering mechanisms
- Application-specific integrated circuits (ASICs) provide the needed processing power
- Attack confidence identification spectrum
  - Somewhat likely,
  - Very likely,
  - Provable
- Allowed to stop traffic at the high end of the attack confidence spectrum
- Firm decides which attacks to stop

6.6: Intrusion Detection Systems and Intrusion Prevention Systems (4 of 4)

Possible Actions

- Drop packets
  - Risky for suspicious traffic even with high confidence
- Bandwidth limitation for certain types of traffic
  - Limit to a certain percentage of all traffic
  - Less risky than dropping packets
  - Useful when confidence is lower

Figure 6-18: Firewalls and Antivirus Servers



6.7: Antivirus Filtering and Unified Threat Management

Traditional Firewalls

- Do not do antivirus filtering

Unified Threat Management (UTM) Firewalls

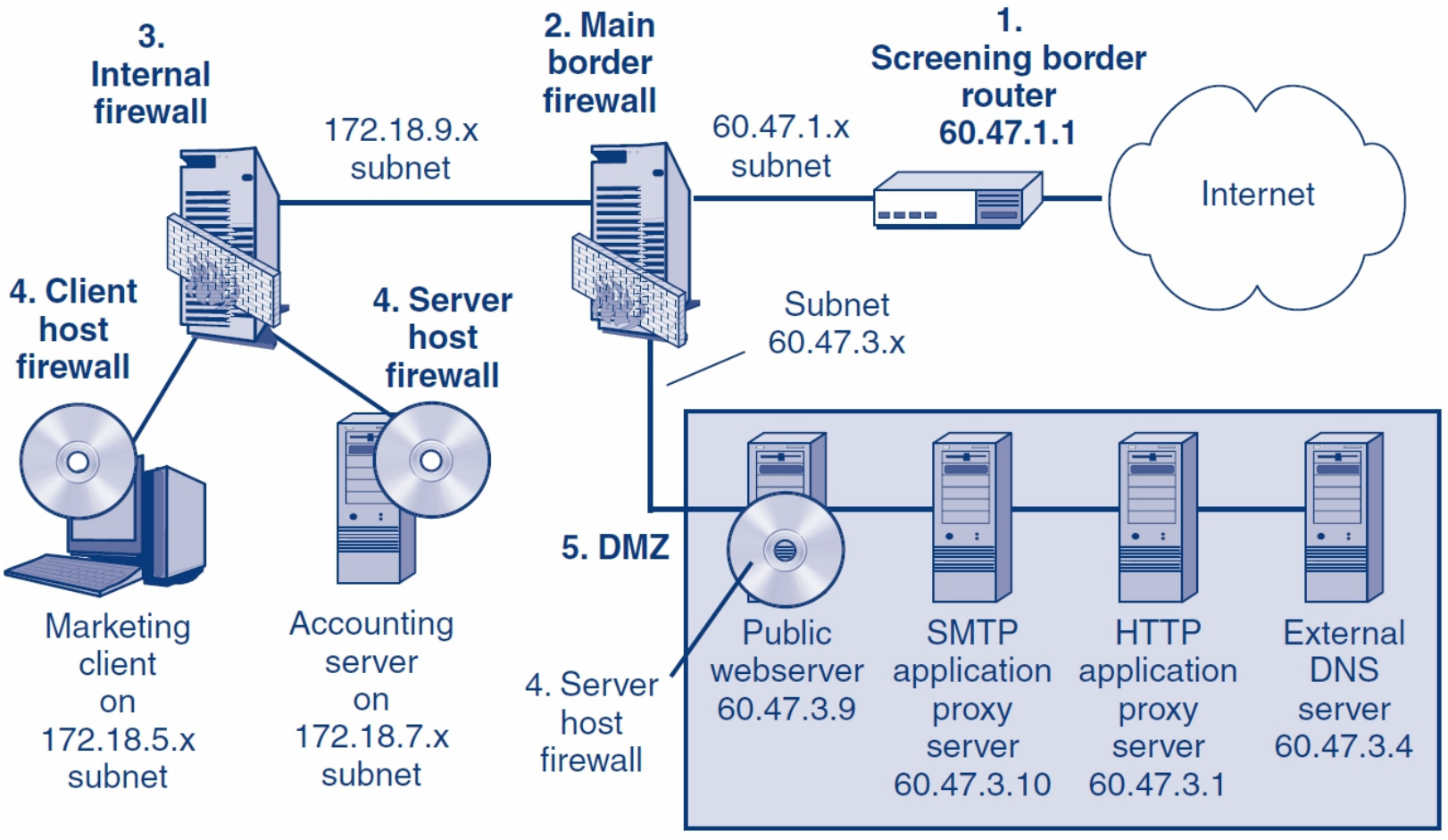
- SPI
- Antivirus filtering
- VPNs
- DoS protection
- NAT

6.8: Firewall Architectures (1 of 4)

Most firms have multiple firewalls

- Main border firewalls
- Screening border routers
- Internal firewalls
- Host firewalls

6.8: Firewall Architecture



6.8: Firewall Architectures (2 of 4)

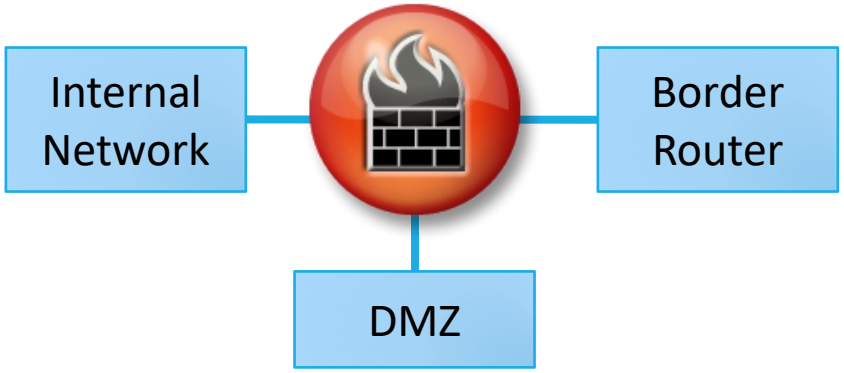
Demilitarized Zone (DMZ)

- Subnet for servers and application proxy firewalls accessible via the Internet
- Hosts in the DMZ must be especially hardened because they will be accessible to attackers on the Internet

6.8: Firewall Architectures (3 of 4)

DMZs Use Multihomed Main Firewalls

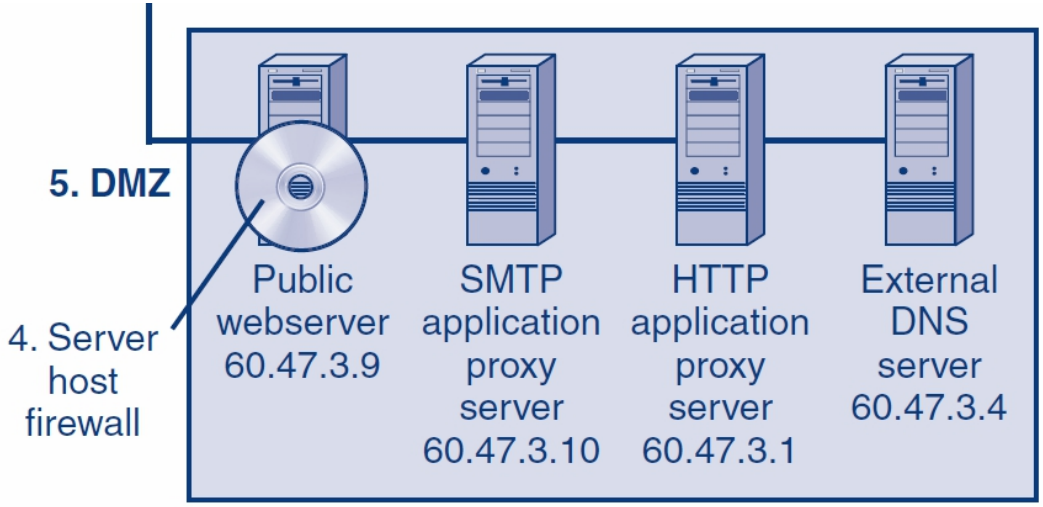
- One subnet to the border router
- One subnet to the DMZ (accessible to the outside world)
- One subnet to the internal network
  - Access from the internal subnet to the Internet is nonexistent or minimal
  - Access from the internal subnet to the DMZ is also strongly controlled



6.8: Firewall Architectures (4 of 4)

Hosts in the DMZ

- Public servers (public webservers, FTP servers, etc.)
- Application proxy firewalls to require all Internet traffic to pass through the DMZ
- External DNS server that knows only host names in the DMZ



6.9: Firewall Management (1 of 2)

Firewalls Are Ineffective Without Planning and Ongoing Management

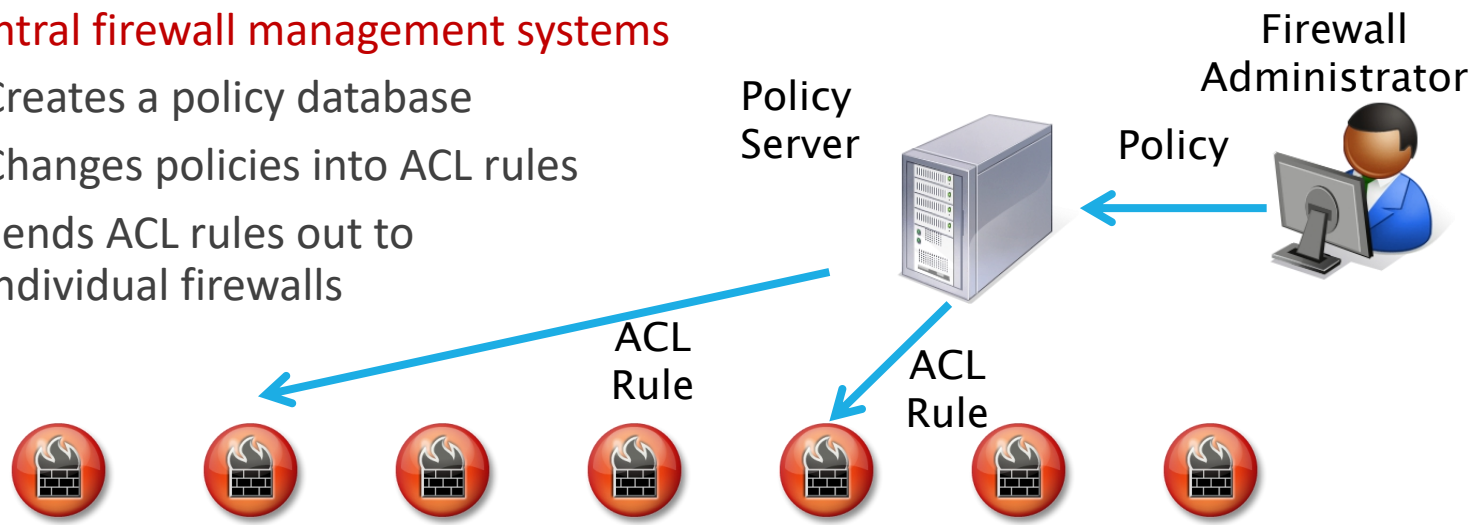
Defining Firewall Policies

- Policies are high-level statements about what to do
  - For example, HTTP connections from the Internet may only go to servers in the DMZ
- Policies are more comprehensible than actual firewall rules
- There may be multiple ways to implement a policy
  - Defining policies instead of specific rules gives implementers freedom to choose the best way to implement a policy

6.9: Firewall Management (2 of 2)

Implementation

- Firewall hardening
  - Firewall appliances are hardened at the factory
  - Vendors sell software plus a server with a pre-hardened operating system
  - Firewall software on a general-purpose computer requires the most on-site hardening
- Central firewall management systems
  - Creates a policy database
  - Changes policies into ACL rules
  - Sends ACL rules out to individual firewalls



6.9: Firewall Policy Database

Policy	Source	Destination	Service	Action	Track	Firewalls
1	Internal	DNS Servers	UDP dns	Pass	None	All
2	External	Internal	TCP http	Drop	Log	All
3	External	DMZ webserver	TCP http	Pass	None	Border
4	Internal	External	TCP http	Pass	Log	Border
5	Internal	External	ICMP	Drop	None	Border
6	Internal	Mail Server	TCP smtp	Authenticate	Log if Fail	Central
7	Marketing	Plans Server	TCP http	Authenticate	Alert if Fail	Marketing
8	Any	Plans Server	TCP http	Drop	Log	Marketing
9	Any	Any	Any	Drop	Log	All

6.9: Firewall Management (2 of 2)

Implementation

- Vulnerability testing after configuration
  - There *will* be problems
  - Tests, like firewall configuration, should be based on policies

6.9: Firewall Management (2 of 2)

Implementation

- Change authorization and management
  - Limit the number of people who can make change requests
  - Limit the number of authorizers even more
  - Require requesters and authorizers to be different people
  - Implement the rule in the most restrictive way possible—
    - To pass the least number of packets
  - Document all changes carefully
  - Do vulnerability testing after every change
    - The change should work
    - All previous behaviors should still work (regression testing)
  - Audit changes frequently
    - Focus especially on asking if each change opens the firewall in the most restrictive way possible

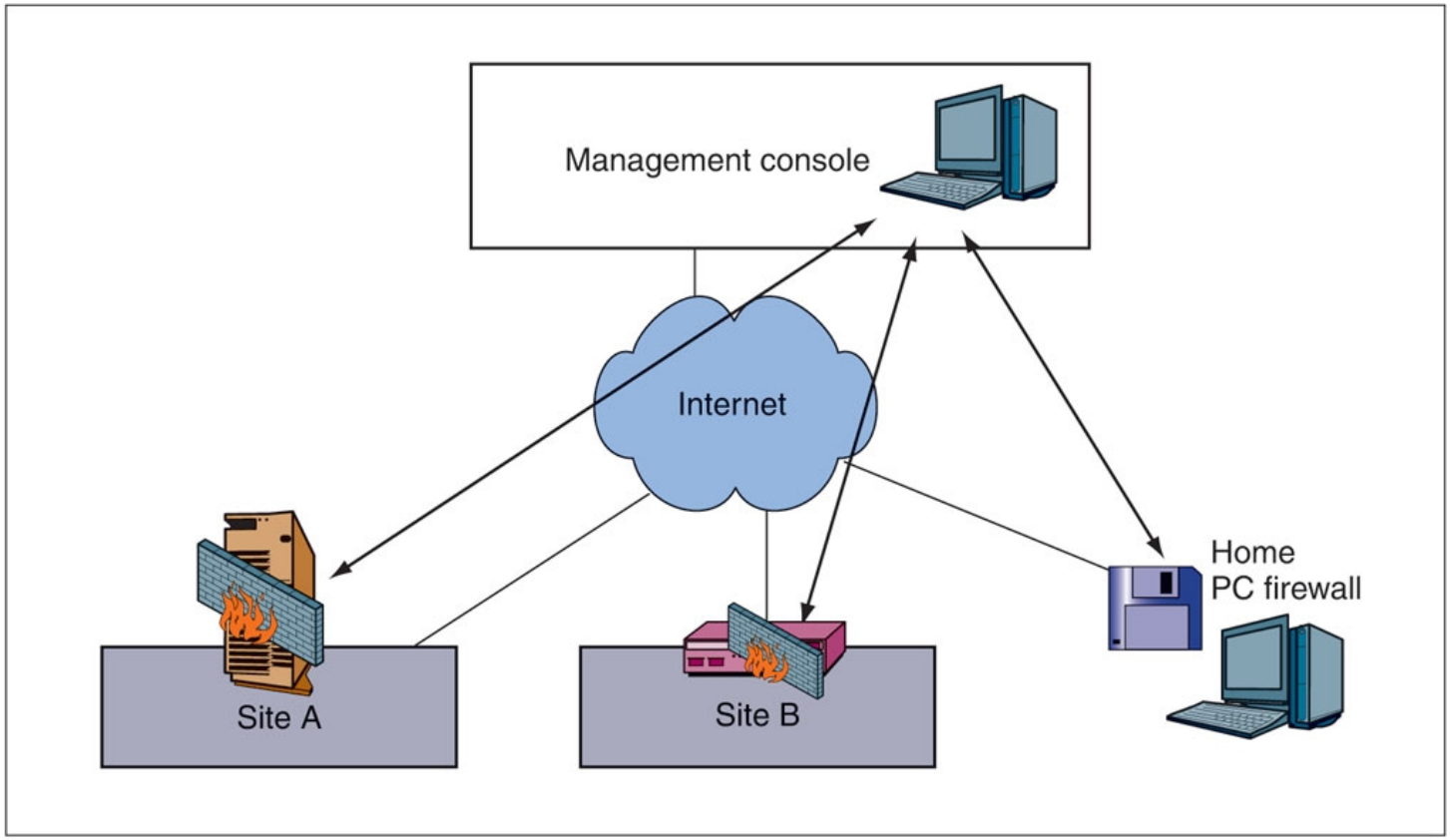
6.9: Firewall Management (2 of 2)

Implementation

- Reading the firewall logs
  - Should be done daily or more frequently
  - The most labor-intensive part of firewall management
  - Strategy is to find unusual traffic patterns
    - Top ten source IP addresses whose packets were dropped
    - Number of DNS failures today versus in an average day
  - Attackers can be black holed (have their packets dropped)

- Attackers can be black holed (have their packets dropped)

Figure 6-23: Central Firewall Management System



6.10: Firewall Filtering Problems (1 of 6)

Protecting the Perimeter Is No Longer Possible

- There are too many ways to get through the perimeter

6.10: Firewall Filtering Problems (2 of 6)

Avoiding the Border Firewall

- Internal attackers are inside the firewall already
- Compromised internal hosts are inside the firewall
- Wireless LAN drive-by hackers enter through access points that are inside the site
- Home notebooks, mobile phones, and media brought into the site
- Internal firewalls can address some of these threats

6.10: Firewall Filtering Problems (3 of 6)

Extending the Perimeter

- Remote employees must be given access
- Consultants, outsourcers, customers, suppliers, and other subsidiaries must be given access
- Essentially, all of these tend to use VPNs to make external parties “internal” to your site

6.10: Firewall Filtering Problems (4 of 6)

Most Filtering Methods Use Attack Signature Detection

- Each attack has a signature
- This attack signature is discovered
- The attack signature is added to the firewall
- Problem
  - Zero-day attacks are attacks without warning, and occur before a signature is developed
  - Signature defense cannot stop zero-day attacks

6.10: Firewall Filtering Problems (6 of 6)

Anomaly Detection

- Detects an unusual pattern indicating a possible attack
- This is difficult, so there are many false positives
- Shrinking time needed to define signatures
- Anomaly detection is necessary in today's firewalls

Thank You