Corporate Computer Security, 4th Edition

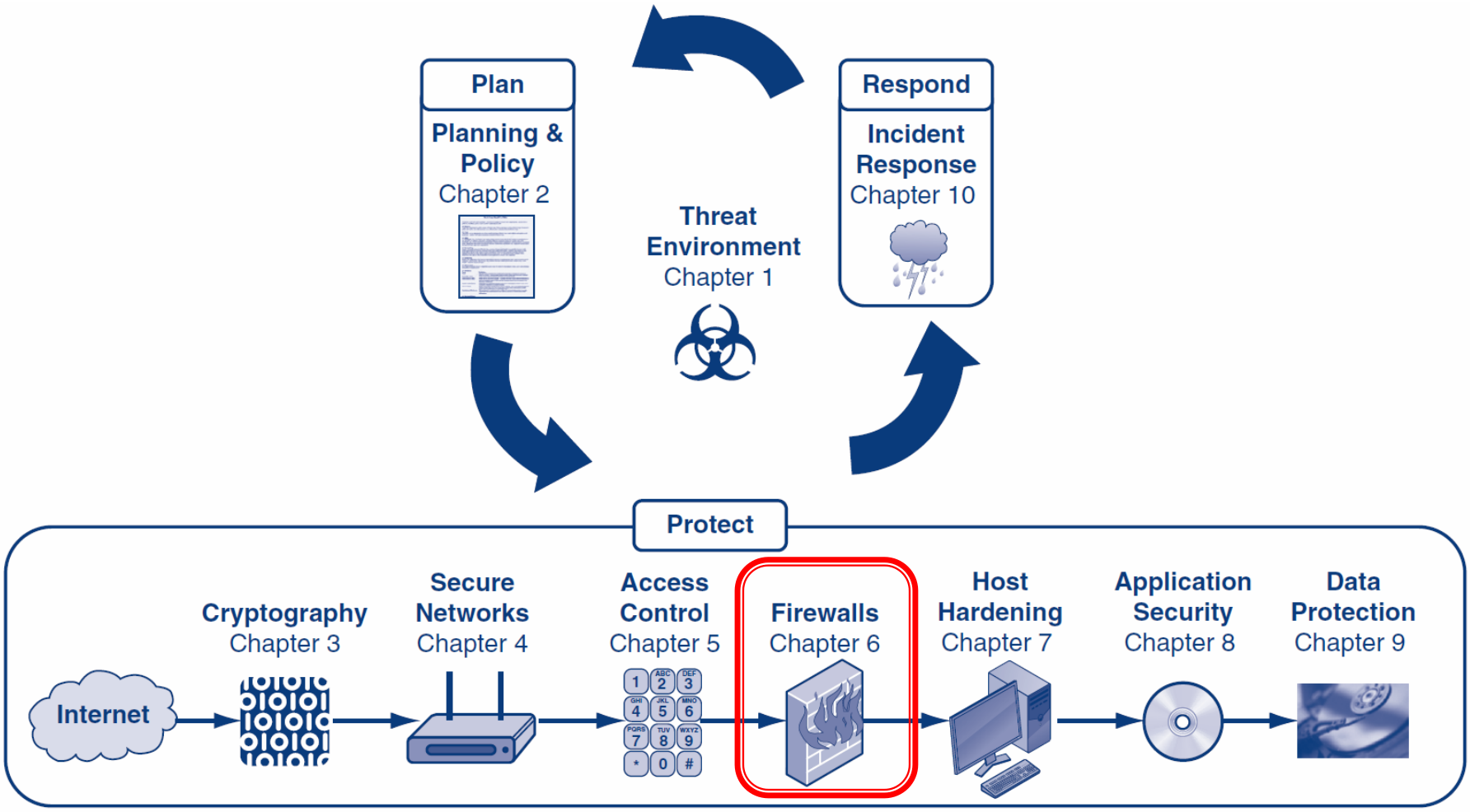
Randall J. Boyle & Raymond R. Panko

Firewalls

Chapter 6

Learning Objectives

- Define *firewalls* in general (basic operation, architecture, and the problem of overload).
- Describe how *static* packet filtering works.
- Explain *stateful* packet inspection (SPI) for main border firewalls.
- Describe how *network address translation* (NAT) works.
- Explain *application proxy* firewalls and content filtering in SPI firewalls.
- Distinguish between intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).
- Describe antivirus filtering.
- Define firewall *architectures*.
- Describe firewall *management* (defining policies, implementing policies, reading log files).
- Describe some difficult *problems* associated with firewalls.



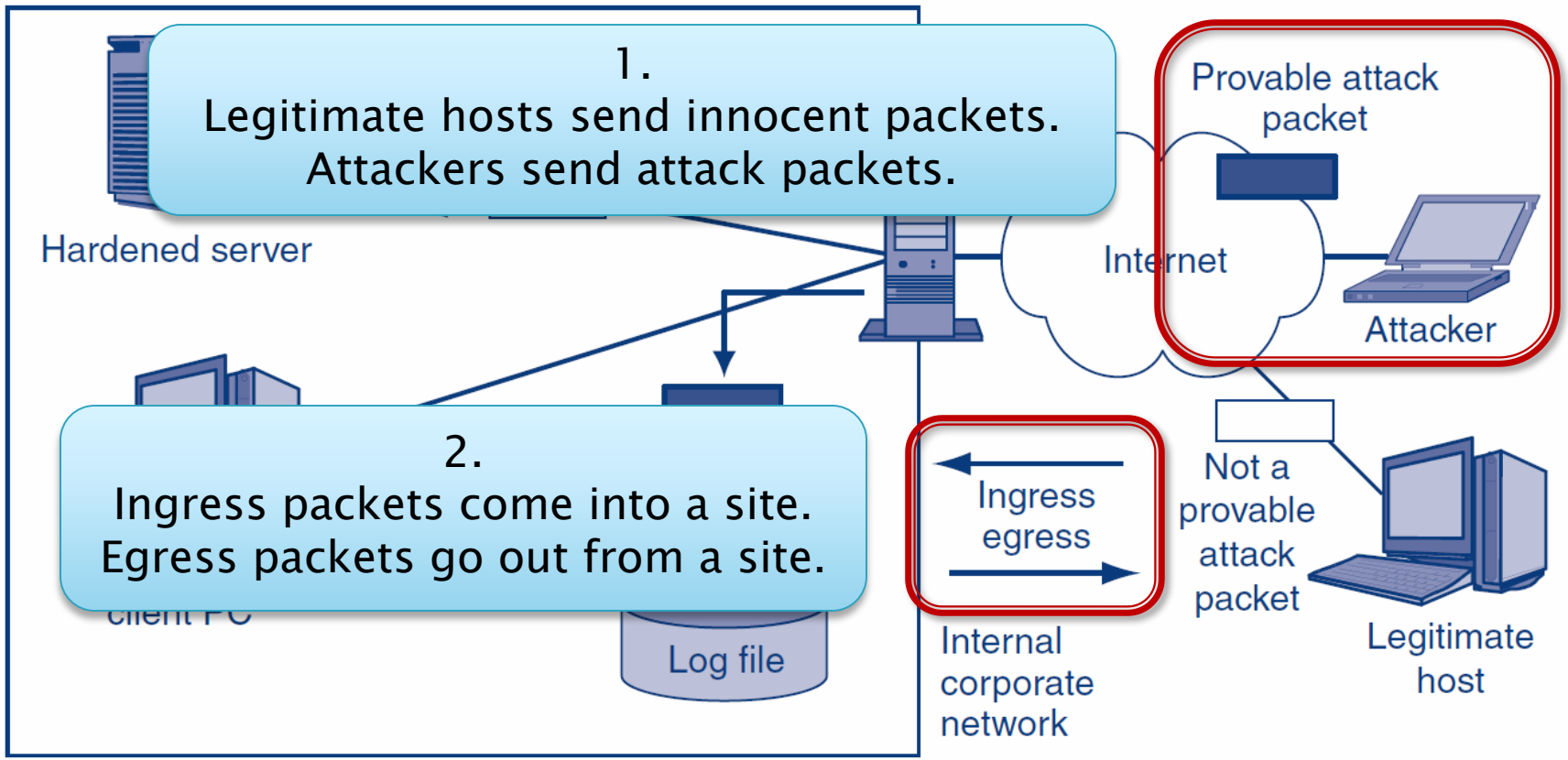
Orientation

- Chapter 5 covered many techniques for access control
- This chapter will discuss an additional tool for access control—firewalls
- Firewalls filter out traffic that consists of provable attack packets
- Firewalls are not security cure-alls, but they are critical to security protection

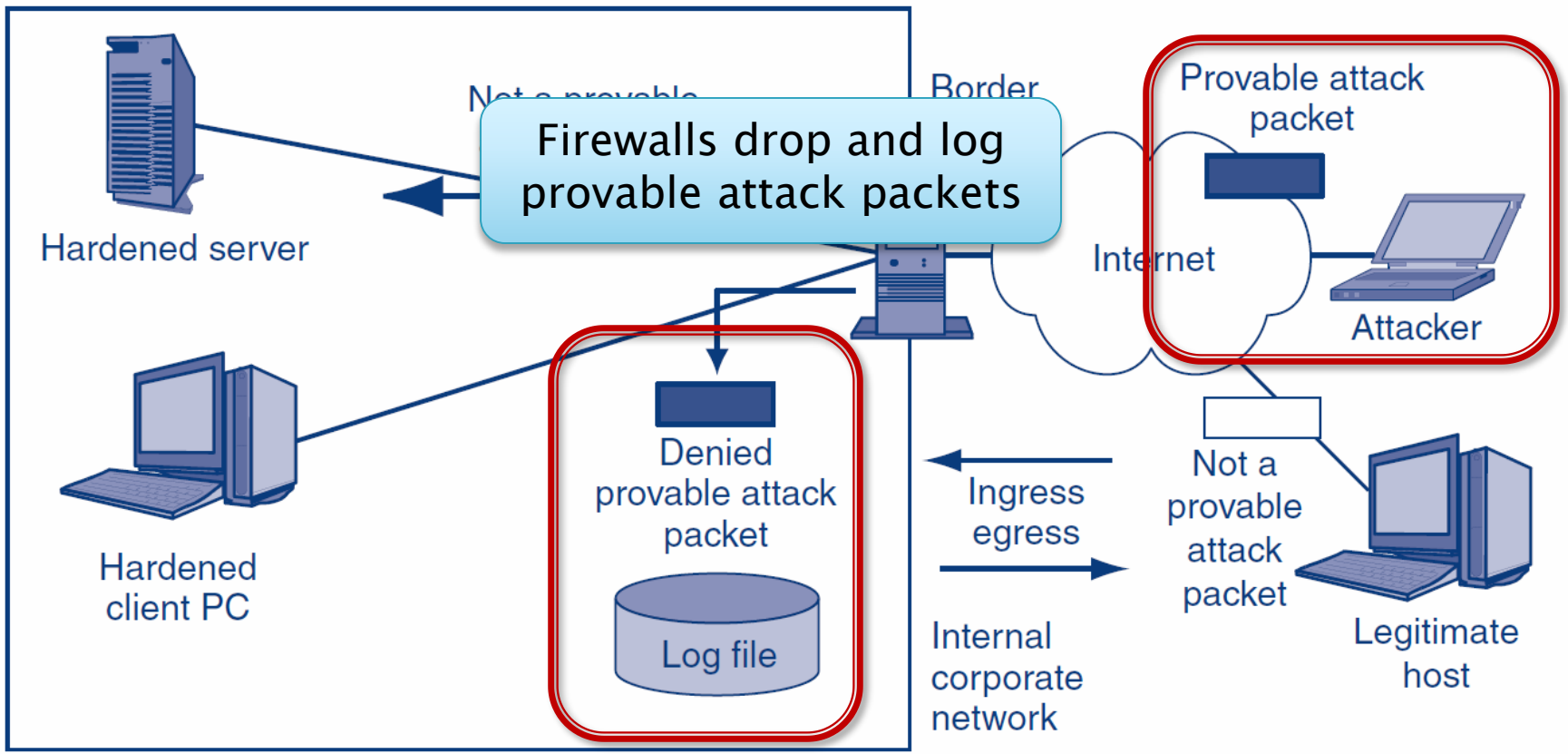
What's Next?

- 6.1 Introduction
- 6.2 Static Packet Filtering
- 6.3 Stateful Packet Inspection (SPI)
- 6.4 Network Access Translation (NAT)
- 6.5 Application Proxy Firewalls
- 6.6 Intrusion Detection Systems (IDSs)
- 6.7 Antivirus Filtering and Unified Threat Mgt.
- 6.8 Firewall Architectures
- 6.9 Firewall Management
- 6.10 Firewall Filtering Problems

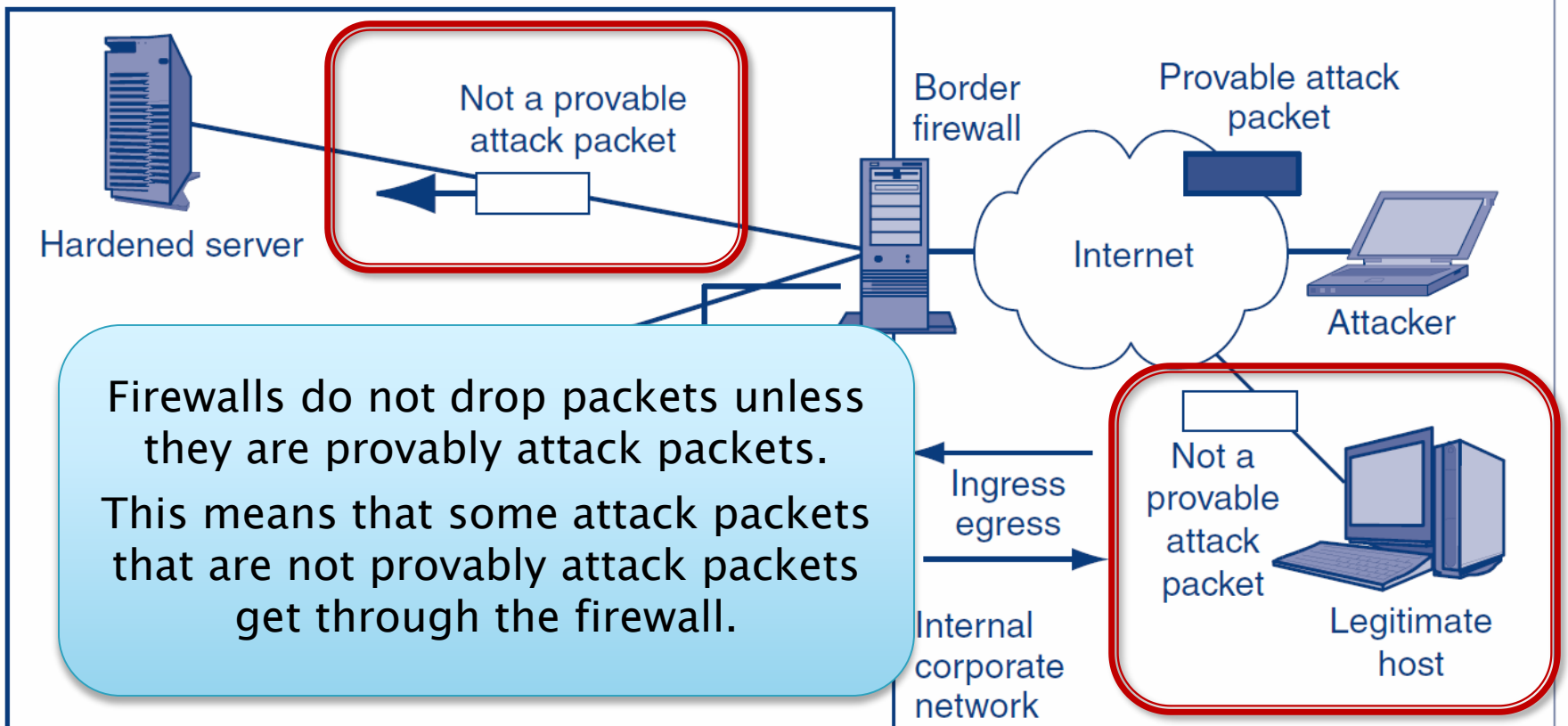
6.1: Basic Firewall Operation



6.1: Basic Firewall Operation



6.1: Basic Firewall Operation



6.1: The Danger of Traffic Overload

- **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
  - It creates a self-inflicted denial-of-service attack by dropping legitimate traffic

6.1: The Danger of Traffic Overload

- **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: The Danger of Traffic Overload

- **Processing Power Is Increasing Rapidly**
  - As processing power increases, more sophisticated 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: The Danger of Traffic Overload

- **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

What's Next?

6.1 Introduction

6.2 Static Packet Filtering

6.3 Stateful Packet Inspection (SPI)

6.4 Network Access Translation (NAT)

6.5 Application Proxy Firewalls

6.6 Intrusion Detection Systems (IDSs)

6.7 Antivirus Filtering and Unified Threat Mgt.

6.8 Firewall Architectures

6.9 Firewall Management

6.10 Firewall Filtering Problems

6.2: Static Packet Filtering

- **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

- **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

- **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

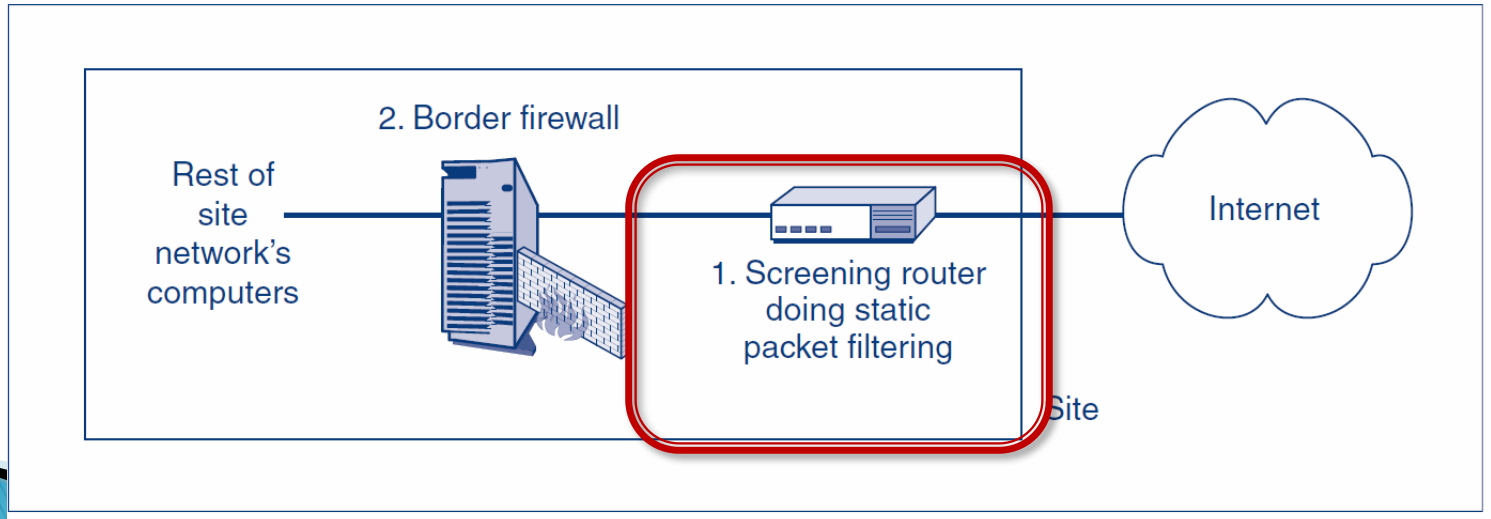
- **Static Packet Filtering Can Stop Certain Attacks Very Efficiently**
  - Incoming ICMP Echo packets and other scanning probe packets
  - Outgoing responses to scanning probe packets
  - Packets with spoofed IP addresses (e.g., incoming packets with the source IP addresses of hosts inside the firm)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

6.2: Static Packet Filtering

- **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

6.2: 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



What's Next?

6.1 Introduction

6.2 Static Packet Filtering

6.3 Stateful Packet Inspection (SPI)

6.4 Network Access Translation (NAT)

6.5 Application Proxy Firewalls

6.6 Intrusion Detection Systems (IDSs)

6.7 Antivirus Filtering and Unified Threat Mgt.

6.8 Firewall Architectures

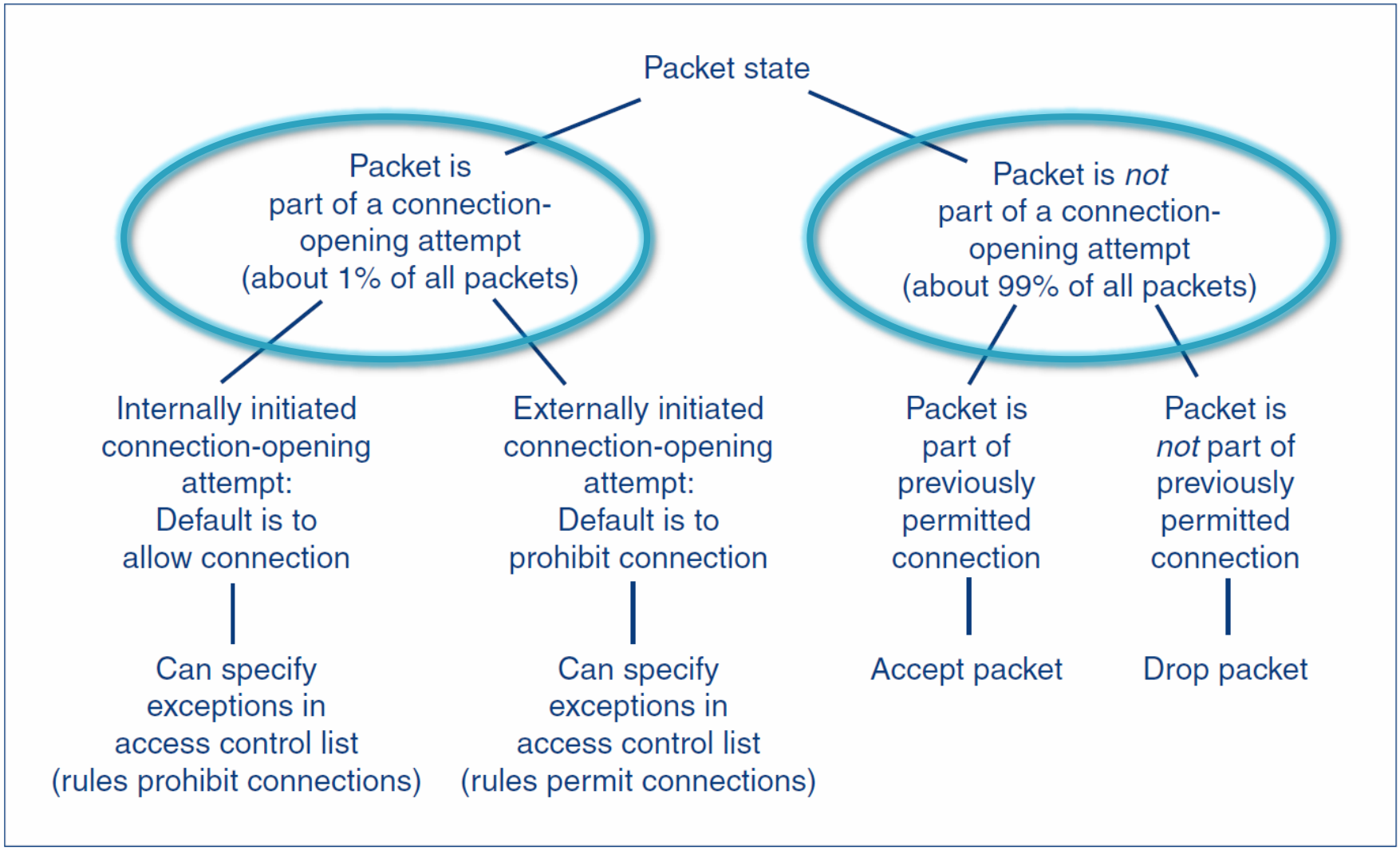
6.9 Firewall Management

6.10 Firewall Filtering Problems

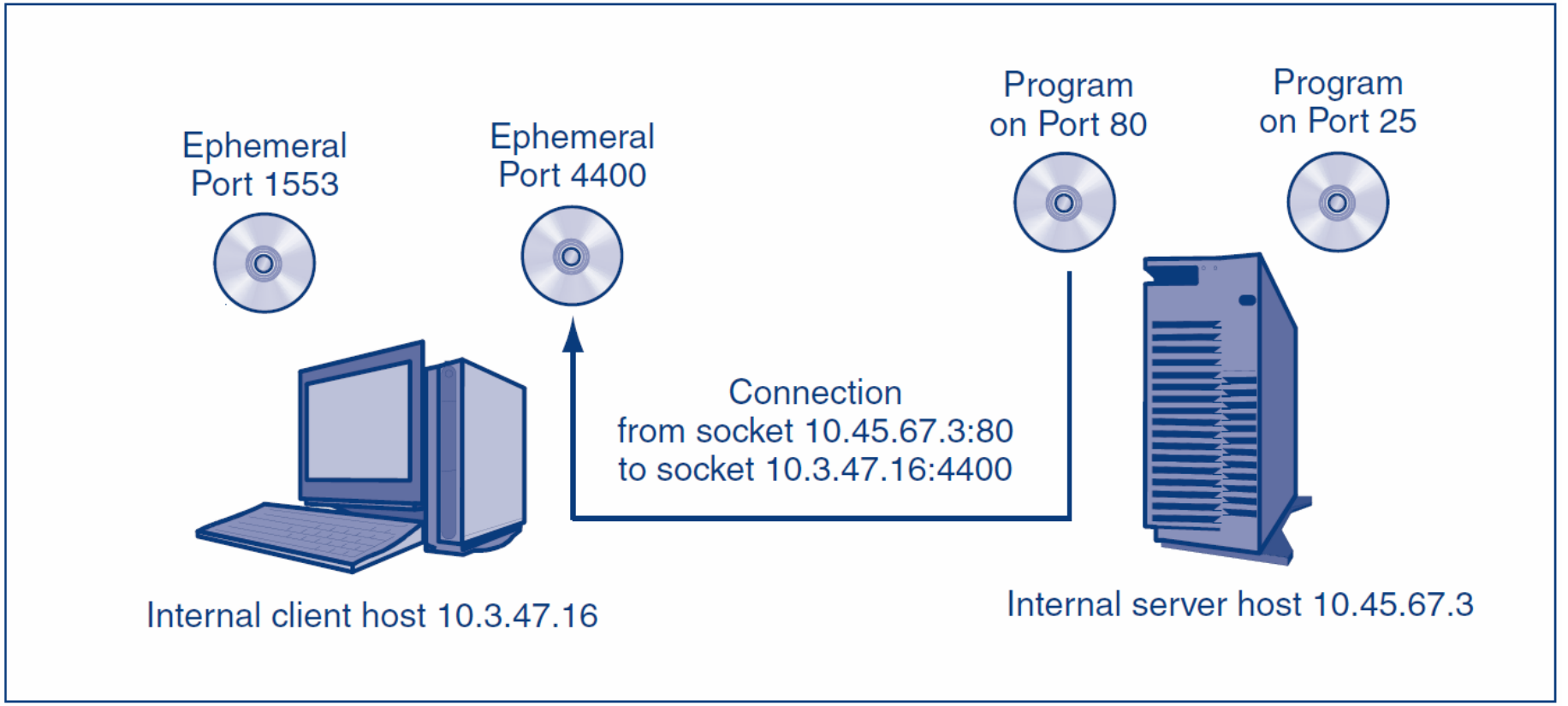
6.3: States in a Connection

- Connections have distinct states or stages
- Different states are subject to different attacks
- Stateful firewalls use different filtering rules for different states

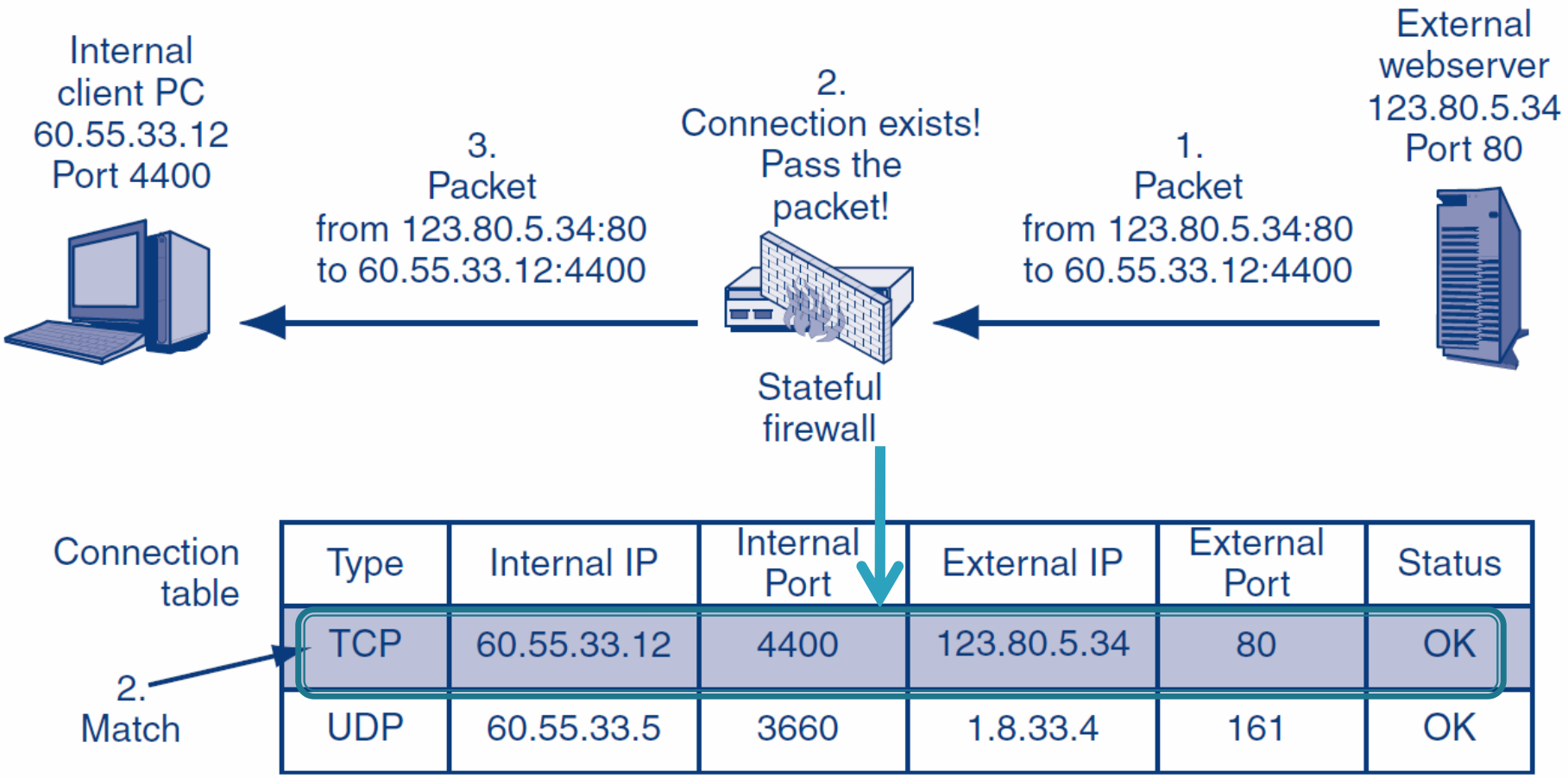
6.3: Stateful Inspection Rules with Two States



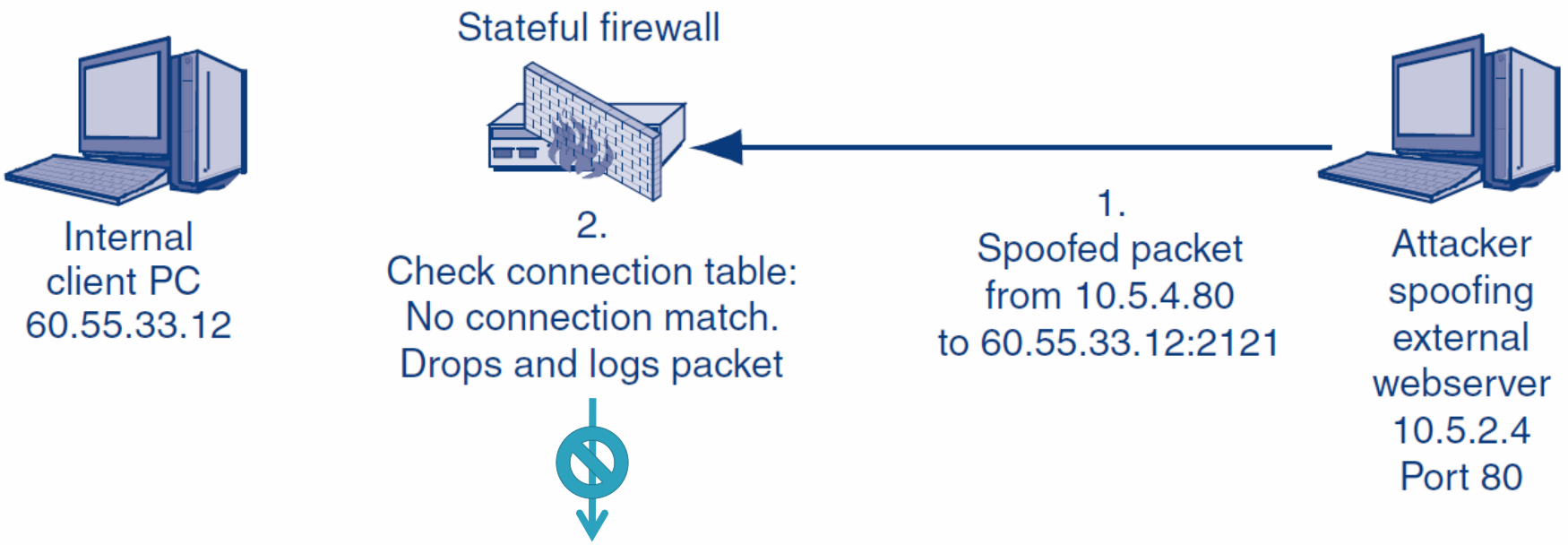
6.3: Connection and Socket



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

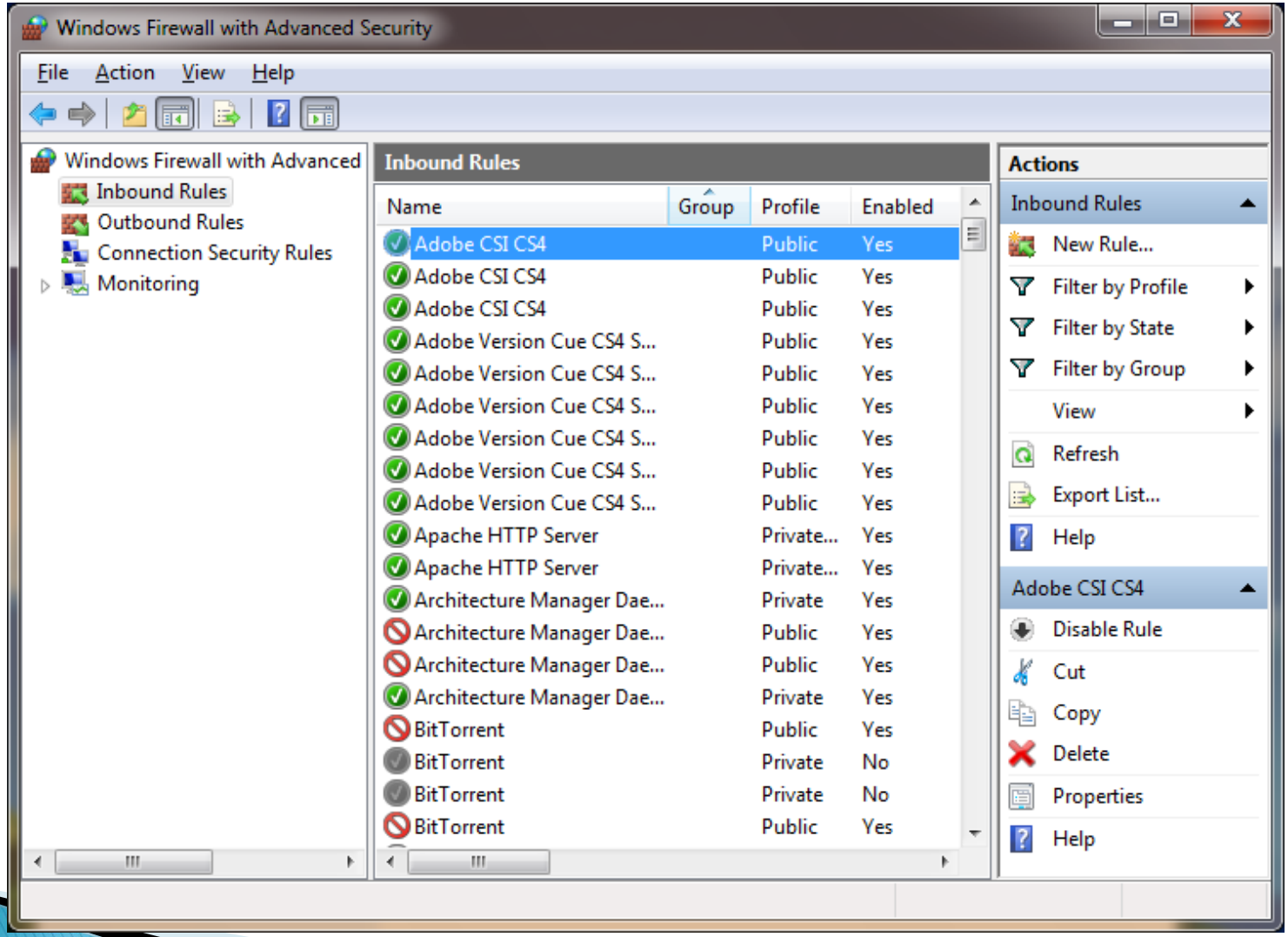
Type	Internal IP	Internal Port	External IP	External Port	Status
TCP	60.55.33.12	4400	123.80.5.34	80	OK
UDP	60.55.33.12	3660	1.8.33.4	161	OK

6.3: Well-Known Port Numbers

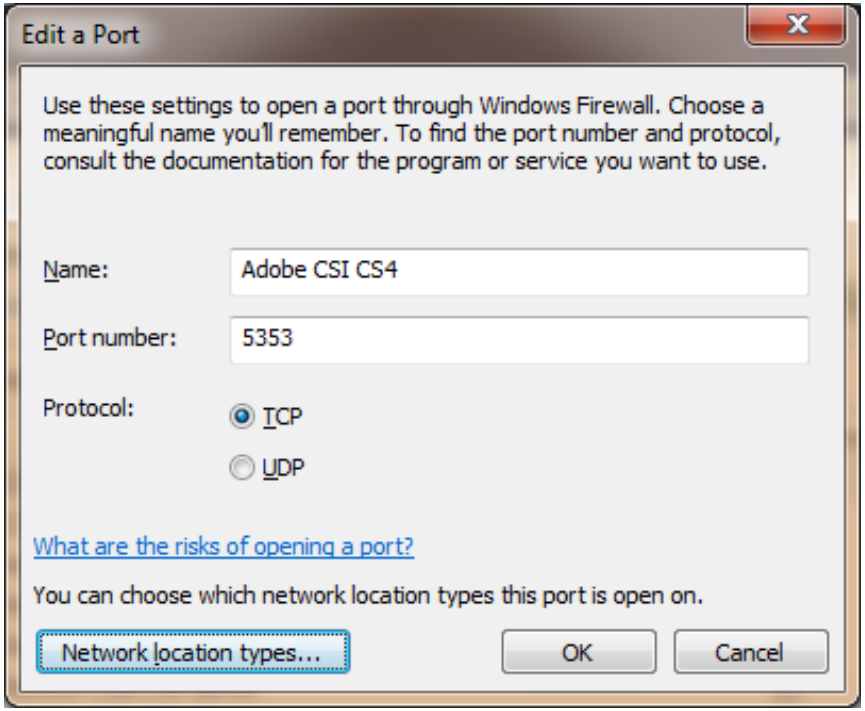
Port	Primary Protocol*	Application
20	TCP	FTP Data Traffic
21	TCP	FTP Supervisory Connection
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	TCP	Domain Name System (DNS)
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	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: Open a Port Through Windows Firewall



6.3: Ingress Access Control List (ACL) in a Stateful Packet Inspection Firewall

- **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: Ingress Access Control List (ACL) in a Stateful Packet Inspection Firewall

- **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: Ingress Access Control List (ACL) in a Stateful Packet Inspection Firewall

- **Simple *Ingress* ACL with Three Rules**
  - If TCP destination port = 80 or TCP destination port = 443, then Allow Connection
    - *[Permits connection to ALL internal webservers]*
  - If TCP destination port = 25 AND IP destination address = 60.47.3.35, then Allow Connection
    - *[Permits connections to a SINGLE internal mail server]*
  - Disallow ALL Connections
    - *[Disallows all other externally initiated connections; this is the default behavior]*

6.3: Perspective on SPI Firewalls

- **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: Perspective on SPI Firewalls

- **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: Perspective on SPI Firewalls

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

What's Next?

6.1 Introduction

6.2 Static Packet Filtering

6.3 Stateful Packet Inspection (SPI)

6.4 Network Access Translation (NAT)

6.5 Application Proxy Firewalls

6.6 Intrusion Detection Systems (IDSs)

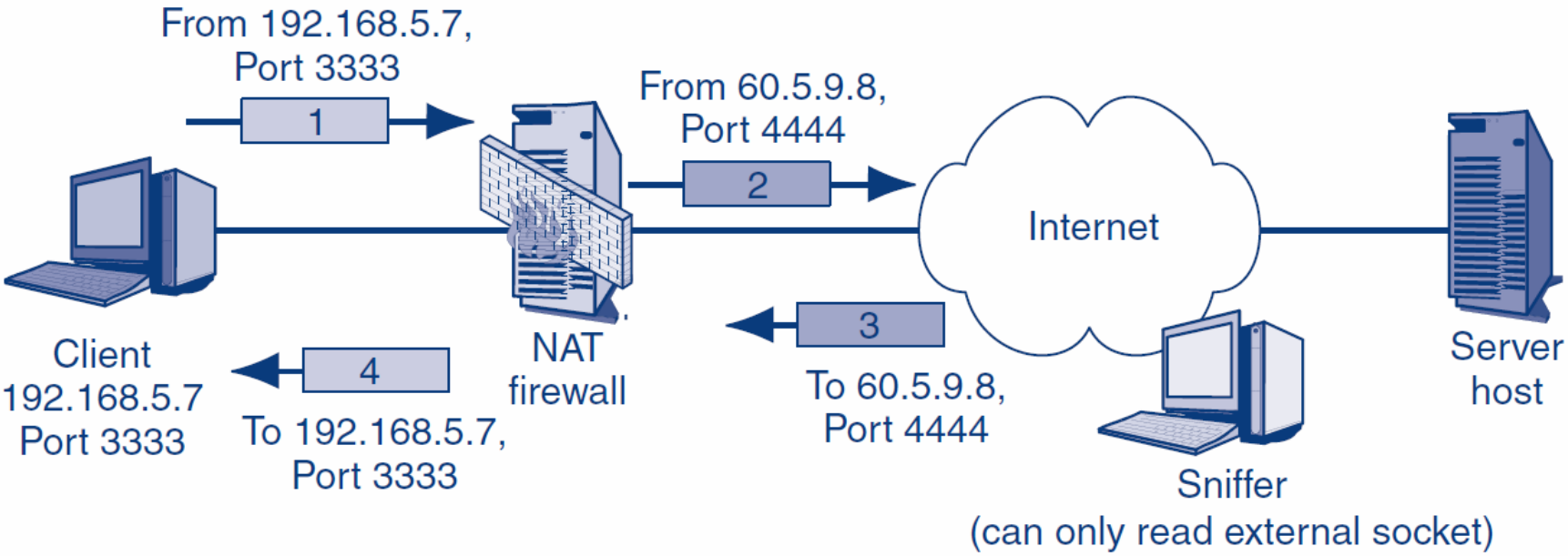
6.7 Antivirus Filtering and Unified Threat Mgt.

6.8 Firewall Architectures

6.9 Firewall Management

6.10 Firewall Filtering Problems

6.4: Network Address Translation (NAT)



Translation table

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

What's Next?

6.1 Introduction

6.2 Static Packet Filtering

6.3 Stateful Packet Inspection (SPI)

6.4 Network Access Translation (NAT)

6.5 Application Proxy Firewalls

6.6 Intrusion Detection Systems (IDSs)

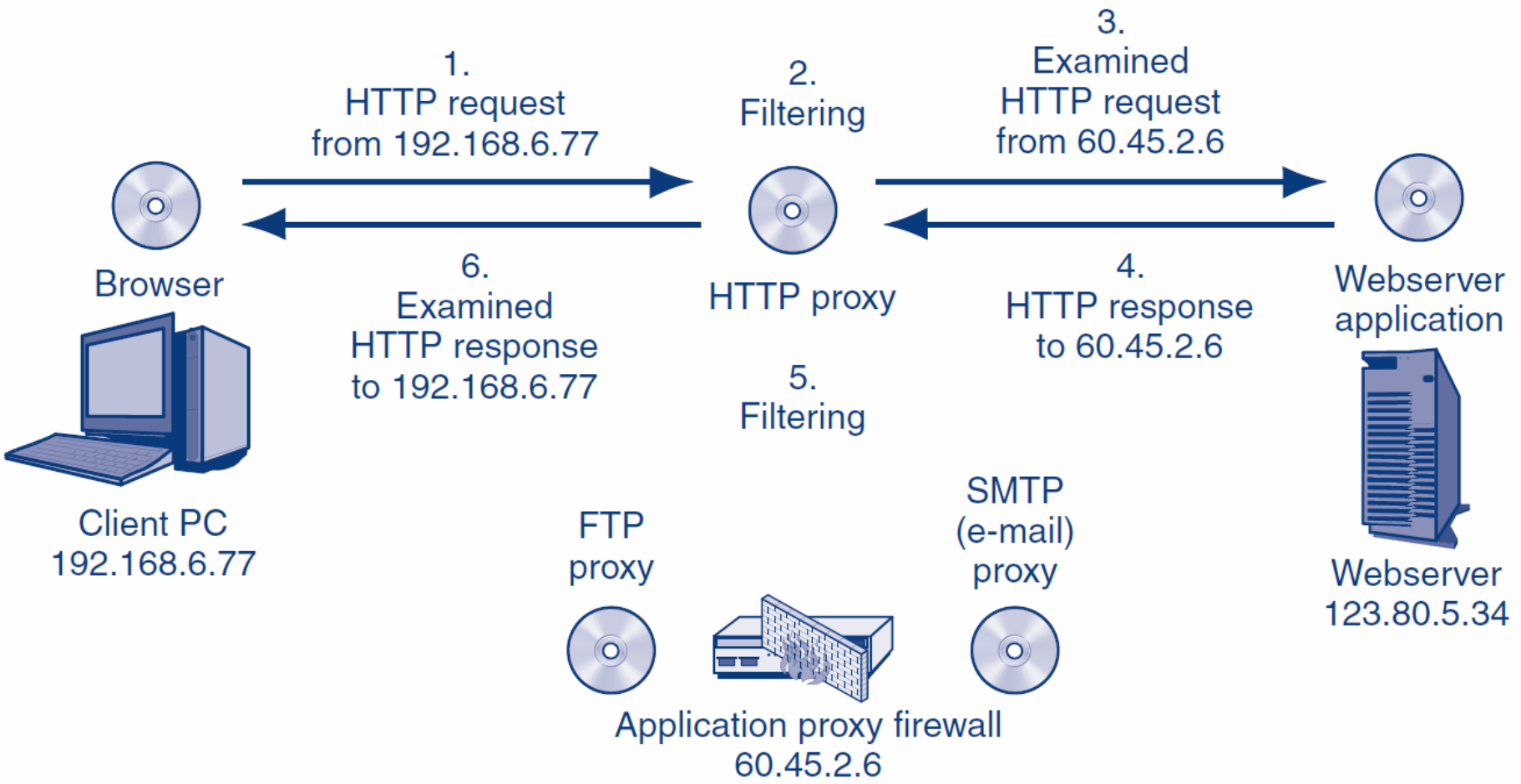
6.7 Antivirus Filtering and Unified Threat Mgt.

6.8 Firewall Architectures

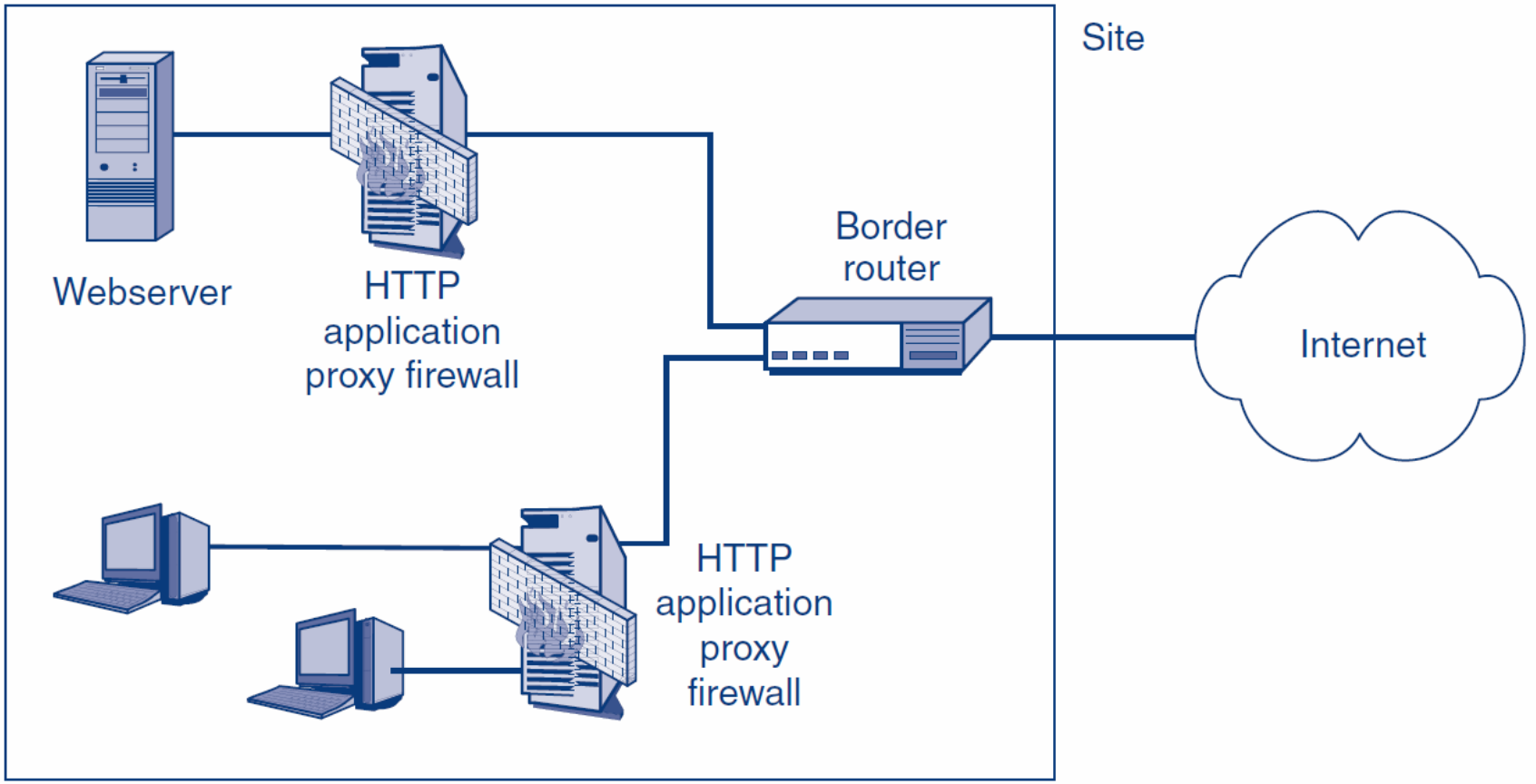
6.9 Firewall Management

6.10 Firewall Filtering Problems

6.5: Application Proxy Firewall Operation



6.5: Roles for Application Proxy Firewalls Today



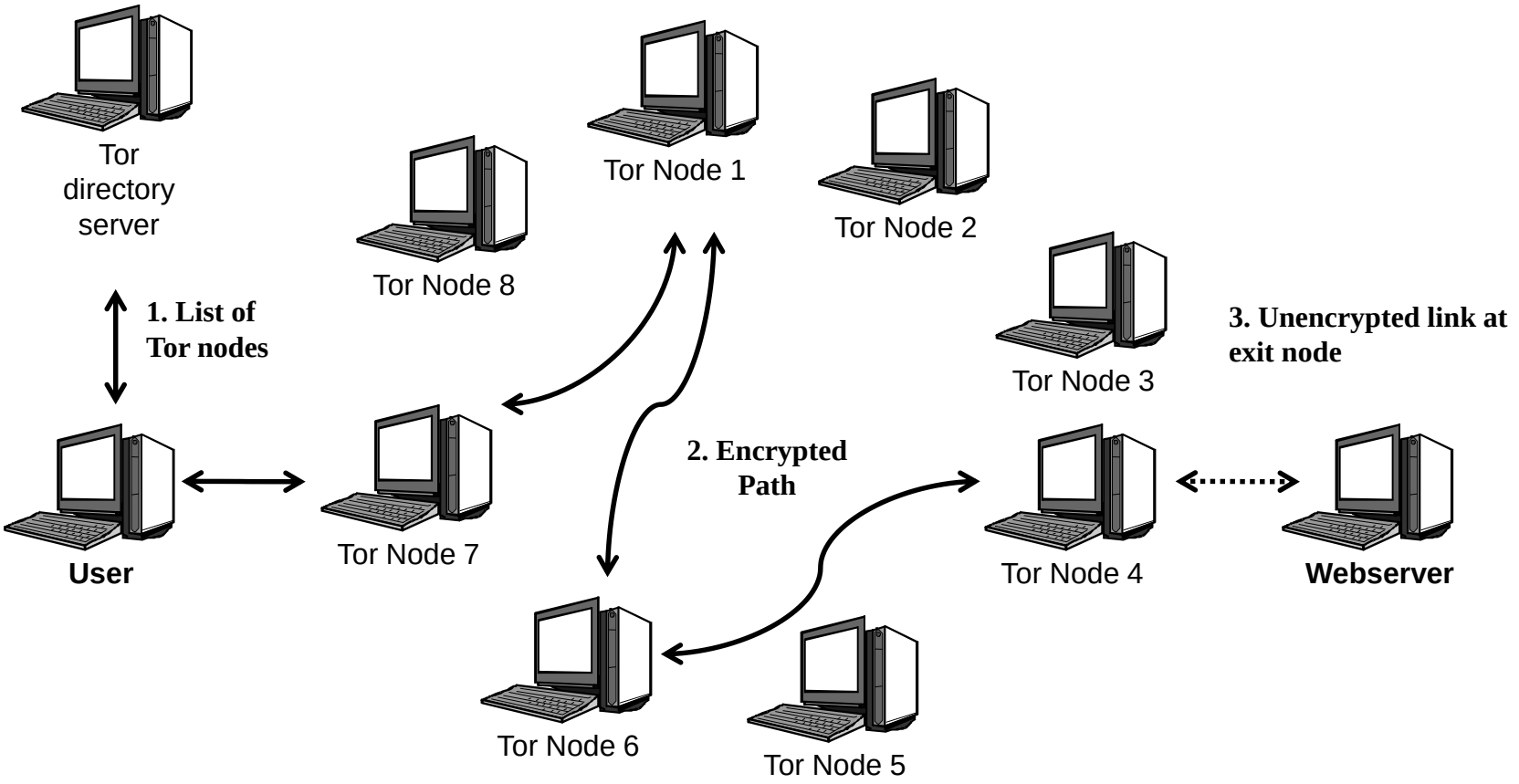
6.5: Application Content Filtering in Application Proxy Firewalls and Stateful Packet Inspection Firewalls

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	

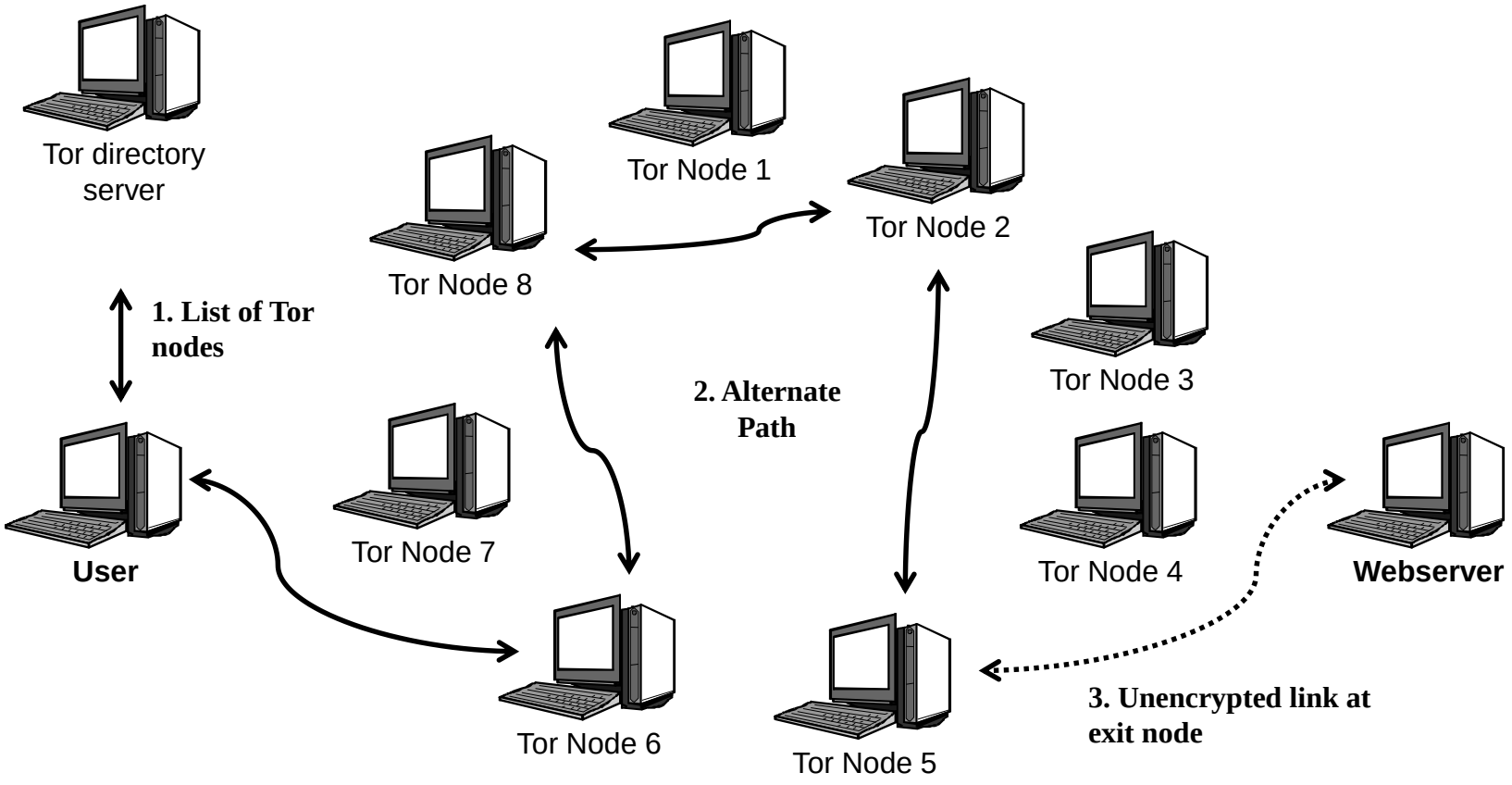
6.5: Application Content Filtering in Application Proxy Firewalls and Stateful Packet Inspection Firewalls

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	

6.5: Tor Routing



6.5: Alternate TOR Route



6.5: Application Proxy Firewall Protections

- **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
- **Protections against Misbehaving Internal Clients**
  - Disallowing the HTTP POST method, which can be use to send out sensitive files

6.5: Application Proxy Firewall Protections

- **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 Firewall Protections

- **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

What's Next?

6.1 Introduction
6.2 Static Packet Filtering
6.3 Stateful Packet Inspection (SPI)
6.4 Network Access Translation (NAT)
6.5 Application Proxy Firewalls
6.6 Intrusion Detection Systems (IDSs)
6.7 Antivirus Filtering and Unified Threat Mgt.
6.8 Firewall Architectures
6.9 Firewall Management
6.10 Firewall Filtering Problems

6.6: Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

- **Perspective**
  - Growing processing power made stateful packet inspection possible
  - Now, growing processing power is making a new firewall filtering method attractive
  - Intrusion prevention systems (IPSs)

6.6: Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

- **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 (IDSs) and Intrusion Prevention Systems (IPSs)

Firewalls versus IDSs

- Firewalls *stop provable* attack packets. If a packet is not a provable attack packet, the firewall cannot drop it. IDSs, in turn, *identify suspicious* packets that may or may not be parts of attacks.
- To give an analogy, a police officer may only arrest someone if the officer has probable cause (a relatively high standard of proof). If someone is behaving suspiciously, a police officer may only investigate them.

6.6: Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

- **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 (IDSs) and Intrusion Prevention Systems (IPSs)

- **Intrusion Detection Systems (IDSs)**
  - Problem: Heavy processing requirements because of sophisticated filtering
    - Deep packet inspection
      - looks at all fields in the packet, including the IP header, the TCP or UDP header, and the application message. Many attacks cannot be stopped if a firewall only looks at application content or only at internet and transport layer headers.

6.6: Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

- **Intrusion Detection Systems (IDSs)**
  - Packet stream analysis
    - Looks at patterns across a series of packets
    - Often, patterns cannot be seen unless many packets are examined.

For instance, a single ICMP echo message is not very diagnostic, but a stream of ICMP echo messages trying different IP addresses is a very strong sign that the company is experiencing a systematic scan.

6.6: Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

- **Intrusion Prevention Systems (IPSs)**
  - Use IDS filtering mechanisms
- IDS/IPS filtering is very processing intensive.
- The most important development leading to IPSs has been the emergence of **application specific integrated circuits (ASICs)**, which can do filtering in hardware. Hardware filtering is much faster than software filtering, allowing IPSs to be used even when traffic volume is high.

6.6: Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

- **Intrusion Prevention Systems (IPSs)**
  - Attack confidence identification spectrum
    - Somewhat likely
    - Very likely
    - Provable
  - Firm may allow firewall to stop traffic at the high end of the attack confidence spectrum
  - Firm decides which attacks to stop
  - This allows it to manage its risks

6.6: Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs)

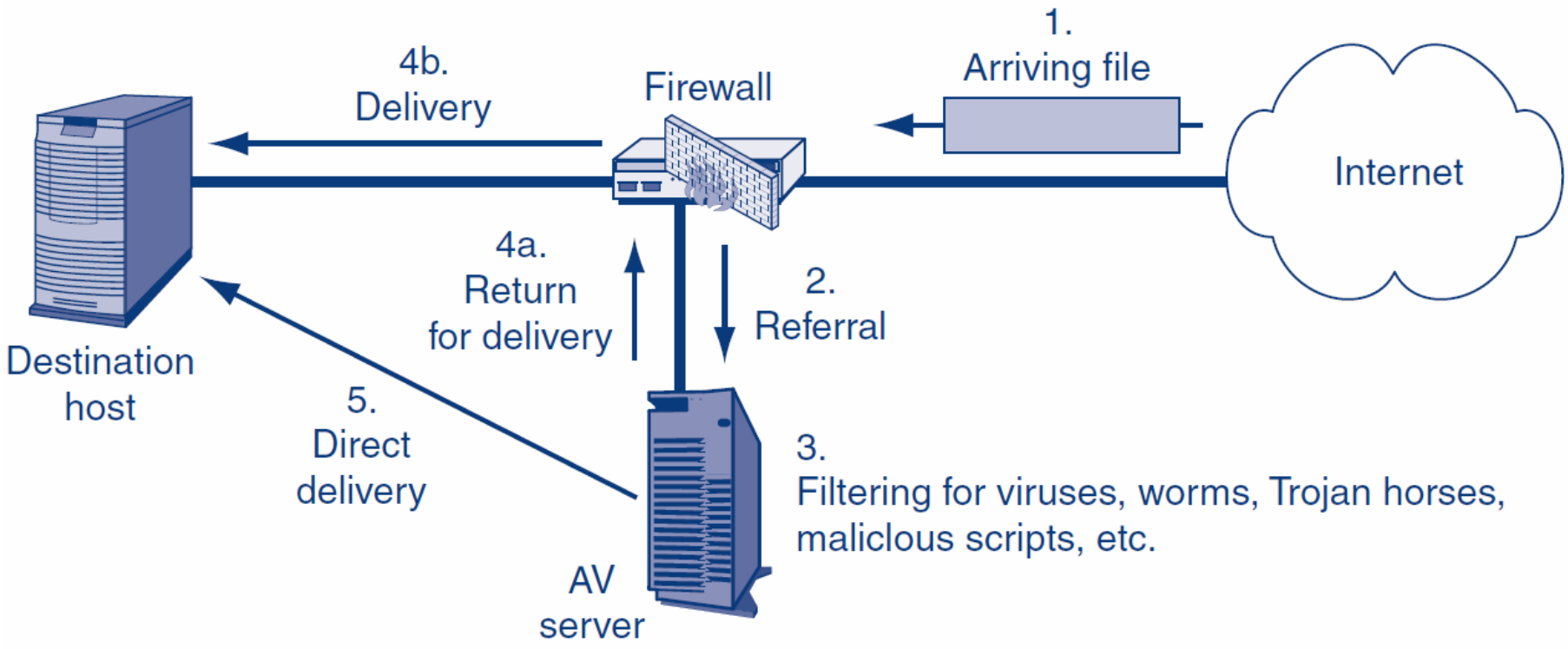
- **Possible Actions**
  - Drop packets
    - Risky for suspicious traffic even with high confidence
  - Bandwidth limitation for certain types of traffic
    - Limit to a certain percentage of all traffic
    - Less risky than dropping packets
    - Useful when confidence is lower

What's Next?

6.1 Introduction
6.2 Static Packet Filtering
6.3 Stateful Packet Inspection (SPI)
6.4 Network Access Translation (NAT)
6.5 Application Proxy Firewalls
6.6 Intrusion Detection Systems (IDSs)
6.7 Antivirus Filtering and Unified Threat Mgt.
6.8 Firewall Architectures
6.9 Firewall Management
6.10 Firewall Filtering Problems

6.7: Firewalls and Antivirus Servers

- **Traditional Firewalls Do Not Do Antivirus Filtering**
- **They Pass Files Needing Filtering to an Antivirus Server**



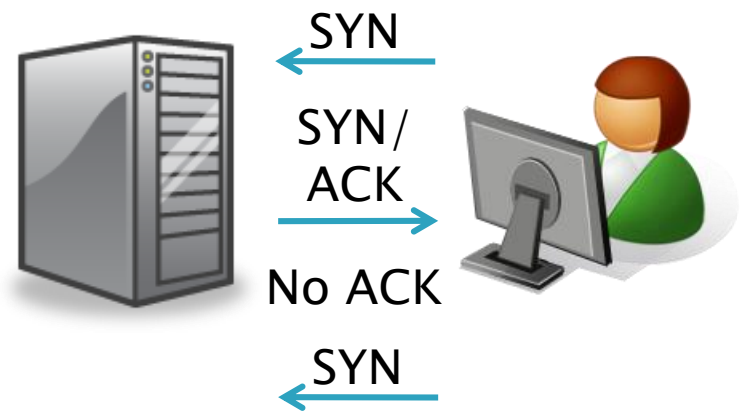
6.7: Unified Threat Management (UTM)

- **Unified Threat Management (UTM) Firewalls Go Beyond Traditional Firewall Filtering**
  - SPI
  - Antivirus Filtering
  - VPNs
  - DoS Protection
  - NAT

6.7: Stopping Denial-of-Service (DoS) Attacks

- **Perspective**
  - Done by most main border firewalls
  - DOS attacks are easy to detect but difficult to stop because their traffic looks like legitimate packets

6.7: Stopping Denial-of-Service (DoS) Attacks



- **TCP Half-Opening Attacks**
  - Attacks
    - Attacker sends a TCP SYN segment to a port
    - The application program sends back a SYN/ACK segment and sets aside resources
    - The attacker never sends back an ACK, so the victim keeps the resources reserved
    - The victim soon runs out of resources and crashes or can no longer serve legitimate traffic

6.7: Stopping Denial-of-Service (DoS) Attacks

- **TCP Half-Opening Attacks**
  - Defenses
    - Firewall intercepts the SYN from an external host
    - Firewall sends back a SYN/ACK without passing the segment on to the target host
    - Only if the firewall receives a timely ACK does it send the original SYN the destination host

6.7: Stopping Denial-of-Service (DoS) Attacks

- **Rate Limiting**
  - Set a limit on all traffic to a server—both legitimate and DoS packets
  - Keeps the entire network from being overloaded
  - Not perfect—does not protect the target server or allow legitimate traffic

6.7: Stopping Denial-of-Service (DoS) Attacks

- **DoS Protection Is a Community Problem**
  - If an organization's access line to the Internet becomes overloaded, it cannot solve the problem itself
  - Its ISP or other upstream agencies must help

What's Next?

6.1 Introduction

6.2 Static Packet Filtering

6.3 Stateful Packet Inspection (SPI)

6.4 Network Access Translation (NAT)

6.5 Application Proxy Firewalls

6.6 Intrusion Detection Systems (IDSs)

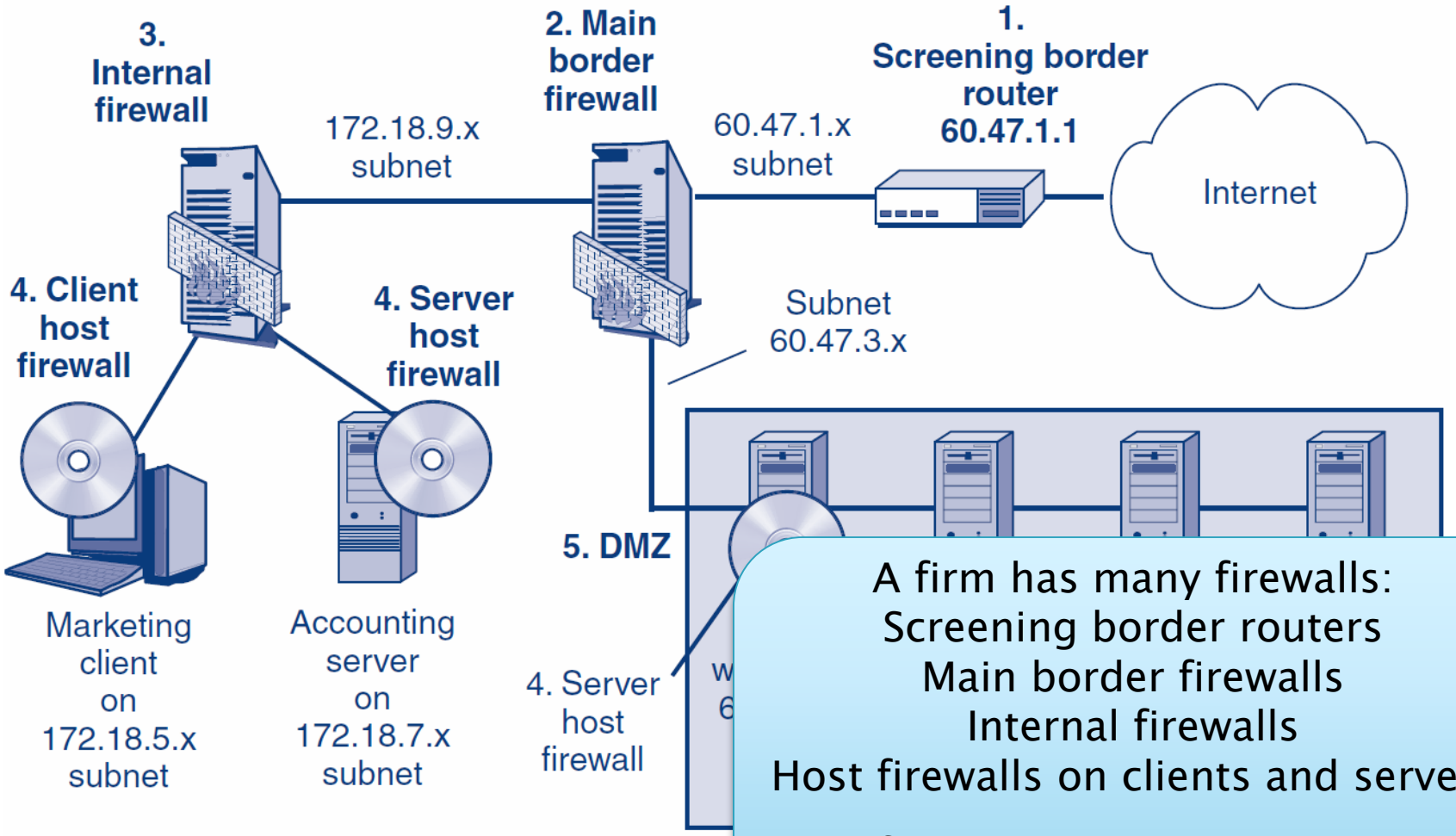
6.7 Antivirus Filtering and Unified Threat Mgt.

6.8 Firewall Architectures

6.9 Firewall Management

6.10 Firewall Filtering Problems

6.8: Firewall Architecture

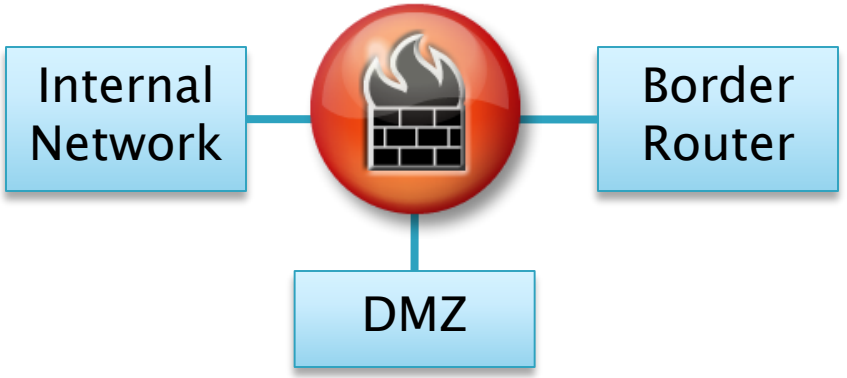


A firm has many firewalls:
Screening border routers
Main border firewalls
Internal firewalls
Host firewalls on clients and servers

The firewall architecture describes how these firewalls work together.

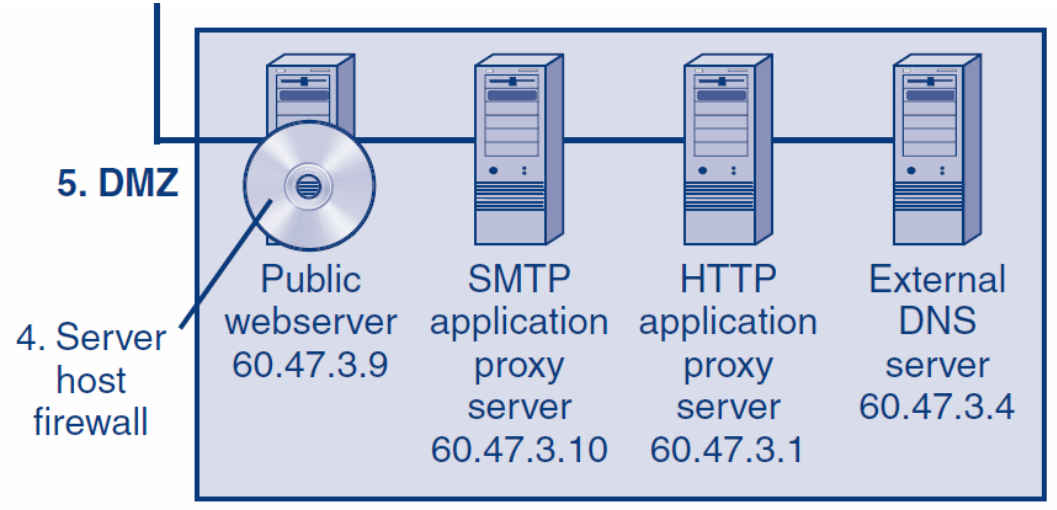
6.8: The Demilitarized Zone (DMZ)

- **DMZs Use Multi-Homed 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



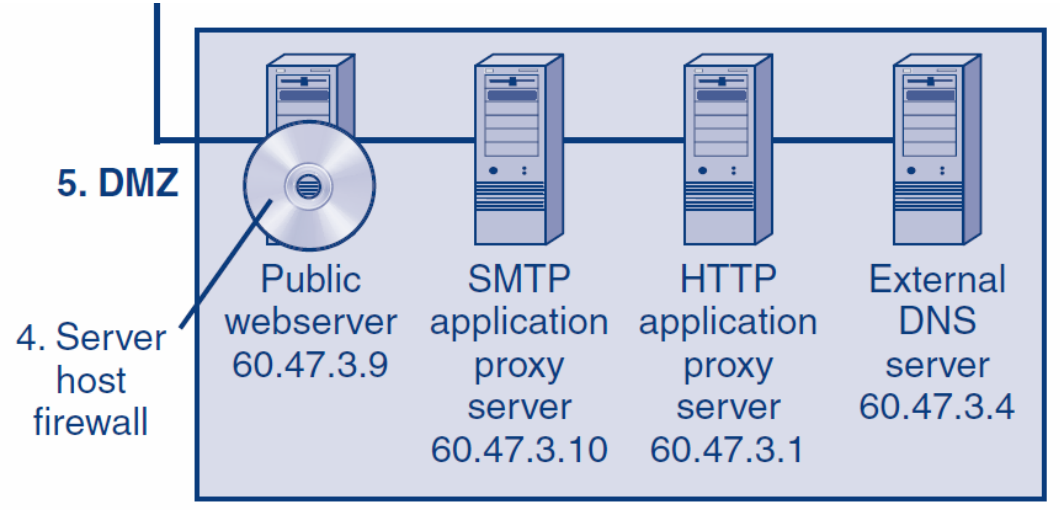
6.8: The Demilitarized Zone (DMZ)

- **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: The Demilitarized Zone (DMZ)

- **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



What's Next?

6.1 Introduction
6.2 Static Packet Filtering
6.3 Stateful Packet Inspection (SPI)
6.4 Network Access Translation (NAT)
6.5 Application Proxy Firewalls
6.6 Intrusion Detection Systems (IDSs)
6.7 Antivirus Filtering and Unified Threat Mgt.
6.8 Firewall Architectures
6.9 Firewall Management
6.10 Firewall Filtering Problems

6.9: Firewall Management

- **Firewalls Are Ineffective Without Planning and Ongoing Management**
- **Defining Firewall Policies**
  - Policies are high-level statements about what to do
  - E.g., HTTP connections from the Internet may only go to servers in the DMZ

6.9: Firewall Management

- **Defining Firewall Policies**
  - 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

Examples of Policies:

The following is a list of some possible firewall policies that a firm might use.

- The company will permit all access by internal clients to external webservers except for webservers on a blacklist of sites that deal with pornography and other problem topics.

- Only people in marketing should have access to a server containing corporate sales data.

6.9: Firewall Management

Examples of Policies:

- All individuals must authenticate themselves before they are allowed to use a server inhuman resources.

- All traffic to an engineering server must be logged.

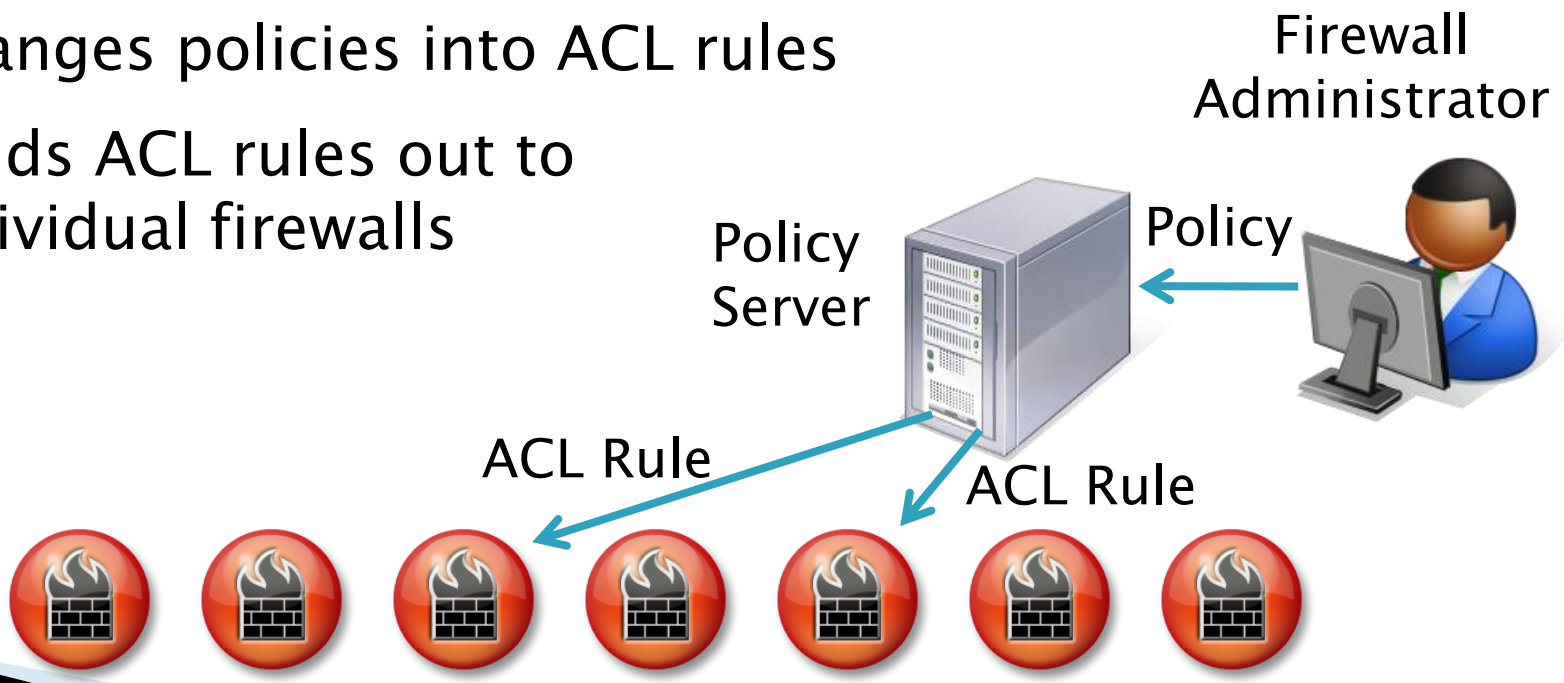
- An alert should be sent to the security administrator whenever five authentication attempts fail.

6.9: Firewall Management

- **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

6.9: Firewall Management

- **Implementation**
  - 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 Policy Database

Figure 6-24 shows a somewhat typical firewall policy database. It shows that each policy has a number of fields.

- The **policy number** field has a unique number for each policy. Policies can therefore be referred to by number.

- The **source** field and **destination** field are fairly explanatory. These can be host names, or they can be groups of IP addresses. Some groups, such as Any, are defined automatically by the system. The firewall administrator must define other groups manually.

6.9: Firewall Policy Database

- The **service** field describes the service to be filtered. Often, this will be TCP or UDP, plus the port number or name of an application. It may also be ICMP or some other type of service defined by the number in the IP header's protocol field.

- The **action** field says what firewalls should do with this service. The most obvious actions are Pass and Drop. Another possible action is Authenticate, which tells the firewall to authenticate the user. Other special-handling actions can be defined depending on the firm's specific policy.

6.9: Firewall Policy Database

- The **track** field describes what the firewall should do after taking its action. This may be nothing (“none”), logging the information in a log file, or alerting someone.

- The **firewalls** field tells the firewall management server what firewalls or routers should be sent to ACLs based upon this policy.

6.9: Firewall Management

- **Implementation**
  - Vulnerability testing after configuration
    - There *will* be problems
    - Tests, like firewall configuration, should be based on policies
    - For instance, in the case of client blacklisting, a vulnerability testing plan would have the tester try to reach several black-listed websites from each of several clients in different parts of the site or firm.

6.9: Firewall Management

- **Implementation**
  - Change authorization and management
    - First, only certain people should be allowed to request changes, and fewer people should be allowed to authorize changes. Most importantly, the change requester should always be different from the change authorizer.
    - Second, the firewall administrator should implement the change in the most restrictive way—the way that will pass the smallest number of packets. For example, instead of opening a port completely, the staff should only open it to a particular host if possible.

6.9: Firewall Management

- **Implementation**
  - Change authorization and management
    - Third, the firewall administrator should document the change carefully. Unless every change is documented very well, the firewall will become impossible to understand, and future changes may have unintended consequences. In addition, many compliance regulations require extensive documentation.
    - Fourth, the firewall should be vulnerability tested after every change to make sure that the change works and that all of the previous behaviors still work. Testing that all previous behaviors work is called regression testing. Limit the number of people who can make change requests.

6.9: Firewall Management

- **Implementation**
  - Change authorization and management
    - Fifth, the company should audit the whole process frequently to ensure compliance with these procedures. This is especially important to ensure that the firewall administrator opened the firewall as little as possible to implement the changed policy.

6.9: Firewall Management

- **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

6.9: Firewall Management

- **Implementation**
- Attackers can be black holed (have their packets dropped)
- If the attack does not look too serious, the administrator **black holes** the IP address, meaning that a rule is added to the firewall (at least temporarily) to block all traffic from that IP address.
- If the attack appears to be more serious, the administrator may log all packets from the IP address whether these packets are attack packets or not.

6.9: Ingress Firewall Log File

ID	Time	Rule	Source IP	Destination IP	Service
1	15:34:005	Echo Probe	14.17.3.139	60.3.87.6	ICMP
2	15:34:007	Echo Probe	14.17.3.139	60.3.87.7	ICMP
3	15:34:008	Forbidden Webserver Access	128.171.17.3	60.17.14.8	HTTP
4	15:34:012	External Access to Internal FTP Server	14.8.23.96	60.8.123.56	FTP
5	15:34:015	Echo Probe	14.17.3.139	60.3.87.8	ICMP
6	15:34:020	External Access to Internal FTP Server	128.171.17.34	60.19.8.20	FTP
7	15:34:021	Echo Probe	1.124.82.6	60.14.42.68	ICMP
8	15:34:023	External Access to Internal FTP Server	14.17.3.139	24.65.56.97	FTP
9	15:34:040	External Access to Internal FTP Server	14.17.3.139	60.8.123.56	FTP

6.9: Ingress Firewall Log File

ID	Time	Rule	Source IP	Destination IP	Service
10	15:34:047	Forbidden Webserver Access	128.171.17.3	60.17.14.8	HTTP
11	15:34:048	Echo Probe	14.17.3.139	60.3.87.9	ICMP
12	15:34:057	Echo Probe	1.30.7.45	60.32.29.102	ICMP
13	15:34:061	External Packet with Private IP Source Address	10.17.3.139	60.32.29.102	ICMP
14	15:34:061	External Access to Internal FTP Server	1.32.6.18	60.8.123.56	FTP
15	15:34:062	Echo Probe	14.17.3.139	60.3.87.10	ICMP
16	15:34:063	Insufficient Capacity	1.32.23.8	60.3.12.47	DNS
17	15:34:064	Echo Probe	14.17.3.139	60.3.87.11	ICMP
18	15:34:065	Forbidden Webserver Access	128.171.17.3	60.17.14.8	HTTP

6.9: Ingress Firewall Log File

This simplified log file contains six pieces of information for each packet:

- The first field is the identification number. In a real log file, there is no ID number. However, an ID number makes it easier for us to talk about entries in the log file.

- The second field gives the time the packet arrived at the firewall, in thousandths of a second.

- The third field is the rule that caused the packet to be dropped. In Figure 6-24, rules were not given names. Figure 6-25 uses names for rules, again to make reading the figure easier.

6.9: Ingress Firewall Log File

This simplified log file contains six pieces of information for each packet:

- The fourth and fifth fields give the source and destination IP addresses of the packet.

- The final field in the table is the service being requested. In this table, the services include ICMP, FTP, and HTTP.

6.9: Ingress Firewall Log File

Sorting the log File by rule

- There is no firm set of rules for reading log files. The only general advice that most firewall administrators cite is, "Look for something different from normal patterns."
- One way to look for unusual patterns is to sort the file on the various fields in the form.
- For example, in Figure 6-25, the firewall administrator might sort on the Rule column, sorting from the most frequently used rule to the least frequently used rule. Then, administrator counts the number of events for each rule.

6.9: Ingress Firewall Log File

Echo Probes

- In the figure, the most frequently used rule stops incoming ICMP echo probes, which are used in IP address scanning.
- This rule was applied eight times. If the host at the destination IP address responds by sending back an ICMP echo reply message, the attacker knows that there is a host at the ICMP echo's original destination IP address.
- Dropping incoming packets with ICMP echo messages ensures that no ICMP echo replies are sent out. Six of the eight ICMP echo requests were sent from the same source IP address, 14.17.3.139.
- The first echo message went to 60.3.87.6. Subsequent ICMP echo messages increased the host part number by 1 each time.

6.9: Ingress Firewall Log File

External Access to All Internal FTP Servers

- During the very brief period covered by the log file, the rule prohibiting external access to internal FTP servers was applied five times.
- These packets came from multiple source IP address, and they went to multiple FTP servers. If this pattern is rarely seen, and if there are multiple attacks from multiple sources to multiple destination FTP servers, this might indicate that the attacks are trying to exploit a newly discovered vulnerability in one or all FTP server programs.
- If the firm has some FTP servers that are available from the outside, say in the DMZ, they should be checked at once.
- In addition, the firm's internal FTP servers may be vulnerable from internal attackers.

6.9: Ingress Firewall Log File

Attempted Access to Internal Webservers

- There were three attempts to access a webserver to which access was forbidden.
- All were from the same source IP address. They came very quickly in time, so this was an automated attack.
- This probably is a common attack, and if there were only three attempts, this probably does not constitute a problem.
- However, the log file only covers a very brief period of time, so we cannot tell whether this is part of an ongoing attack based on attempted webserver access.

6.9: Ingress Firewall Log File

Incoming Packet with a Private IP source address

- One incoming packet was dropped because its source IP address was in an IP address range for private IP addresses—those that should only be used within companies and should never be sent over the Internet.
- This is a clumsy attack, and it is not repeated during the logging period. Consequently, it probably does not constitute a threat.

6.9: Ingress Firewall Log File

lack of Capacity

- Finally, one packet was dropped because the firewall lacked sufficient capacity to process it.
- If a firewall does not have the capacity to process a packet, it drops the packet in case it might be an attack packet.
- In this small sample of 18 packets, one packet was dropped because of a lack of capacity. If anything like this ratio holds for a longer period of time, it is imperative to upgrade the firewall's capacity immediately.

What's Next?

6.1 Introduction

6.2 Static Packet Filtering

6.3 Stateful Packet Inspection (SPI)

6.4 Network Access Translation (NAT)

6.5 Application Proxy Firewalls

6.6 Intrusion Detection Systems (IDSs)

6.7 Antivirus Filtering and Unified Threat Mgt.

6.8 Firewall Architectures

6.9 Firewall Management

6.10 Firewall Filtering Problems

6.10: The Death of the Perimeter

- **Protecting the Perimeter Is No Longer Possible**
  - There are too many ways to get through the perimeter
- **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: The Death of the Perimeter

- **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: Signature versus Anomaly Detection

- **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
  - Zero-day attacks are attacks without warning, and occur before a signature is developed
  - Signature defense cannot stop zero-day attacks

6.10: Signature versus Anomaly Detection

- **Anomaly Detection**

- One way to address threats for which no signature exists is to use anomaly detection, which looks at traffic patterns that indicate that some kind of attack is underway.

- For example, if a host that always acts like a client begins to act like an FTP server, this suggests that it is a client that has been compromised and is being used as an FTP server, perhaps as a way to store identity information that the attacker wishes to sell.

- Anomaly detection can stop new attacks that have no well-defined signatures.

6.10: Signature versus Anomaly Detection

- Accuracy
- Unfortunately, anomaly detection today is less accurate than signature-based detection.
- Traffic patterns vary for many legitimate reasons. As in IDSs, anomaly detection tends
- to generate so many false positives that many companies will not use it.
- However, given the speed with which vulnerability exploits, worms, and viruses are beginning to spread, anomaly detection is essential in firewalls today

The End