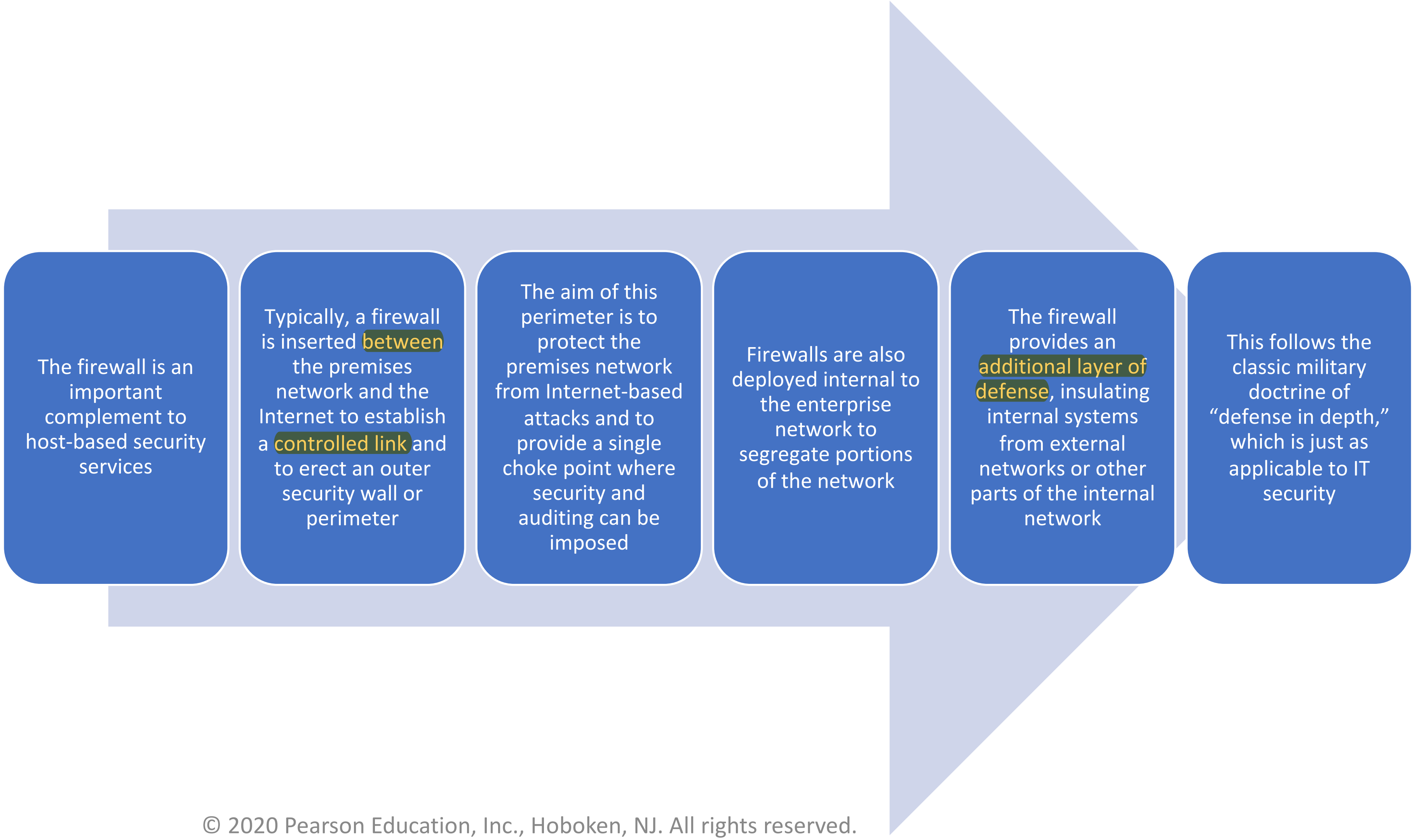
Chapter 21

Network Endpoint Security

Firewalls



The firewall is an important complement to host-based security services

Typically, a firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter

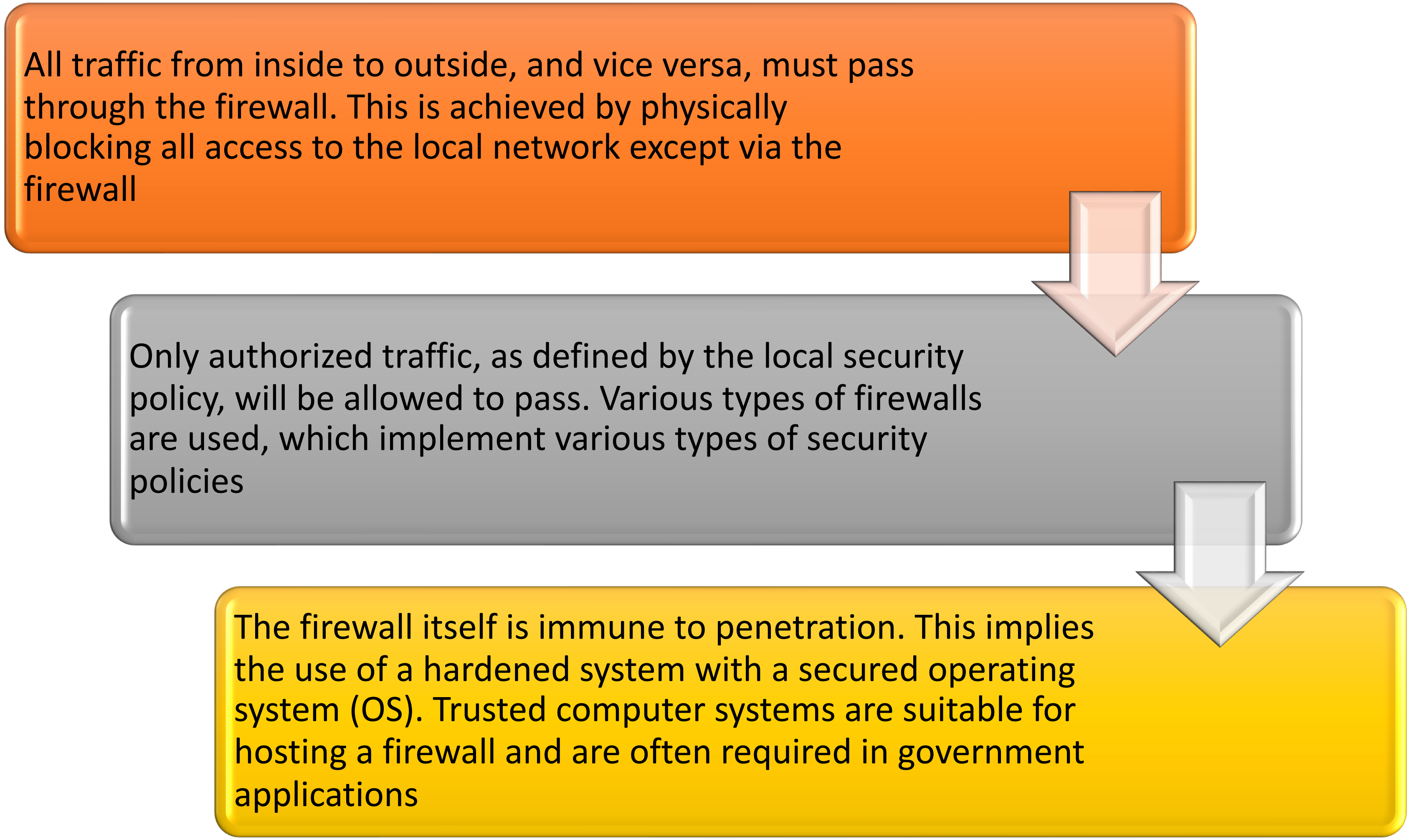
The aim of this perimeter is to protect the premises network from Internet-based attacks and to provide a single choke point where security and auditing can be imposed

Firewalls are also deployed internal to the enterprise network to segregate portions of the network

The firewall provides an additional layer of defense, insulating internal systems from external networks or other parts of the internal network

This follows the classic military doctrine of “defense in depth,” which is just as applicable to IT security

Firewall Design Goals

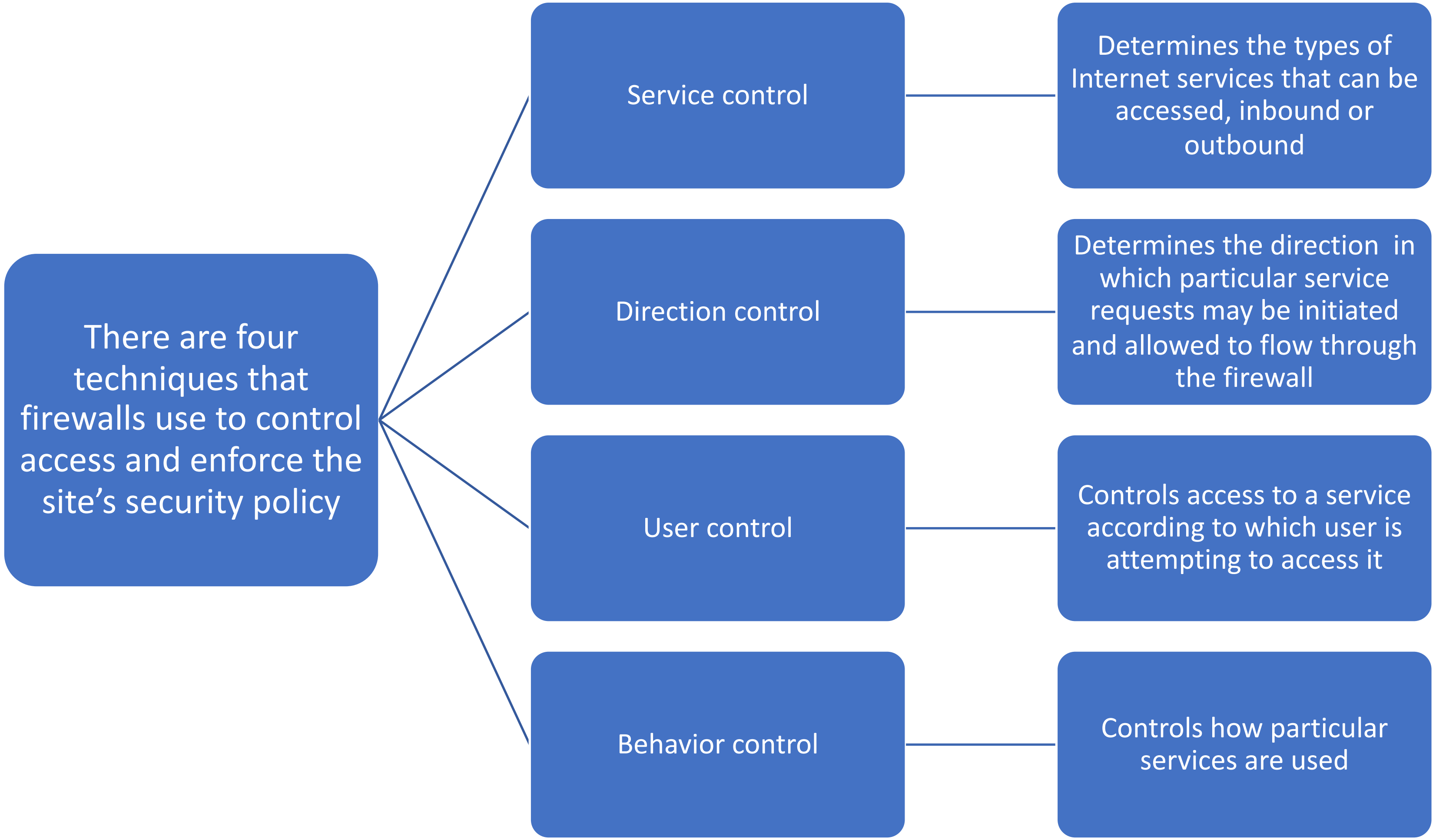


All traffic from inside to outside, and vice versa, must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall

Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies

The firewall itself is immune to penetration. This implies the use of a hardened system with a secured operating system (OS). Trusted computer systems are suitable for hosting a firewall and are often required in government applications

Firewall Techniques



There are four techniques that firewalls use to control access and enforce the site's security policy

Service control

Determines the types of Internet services that can be accessed, inbound or outbound

Direction control

Determines the direction in which particular service requests may be initiated and allowed to flow through the firewall

User control

Controls access to a service according to which user is attempting to access it

Behavior control

Controls how particular services are used

Firewall Capabilities

The following capabilities are within the scope of a firewall:

A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks

A firewall provides a location for monitoring security-related events

A firewall is a convenient platform for several Internet functions that are not security related

A firewall can serve as the platform for implementing virtual private networks

Firewall Limitations

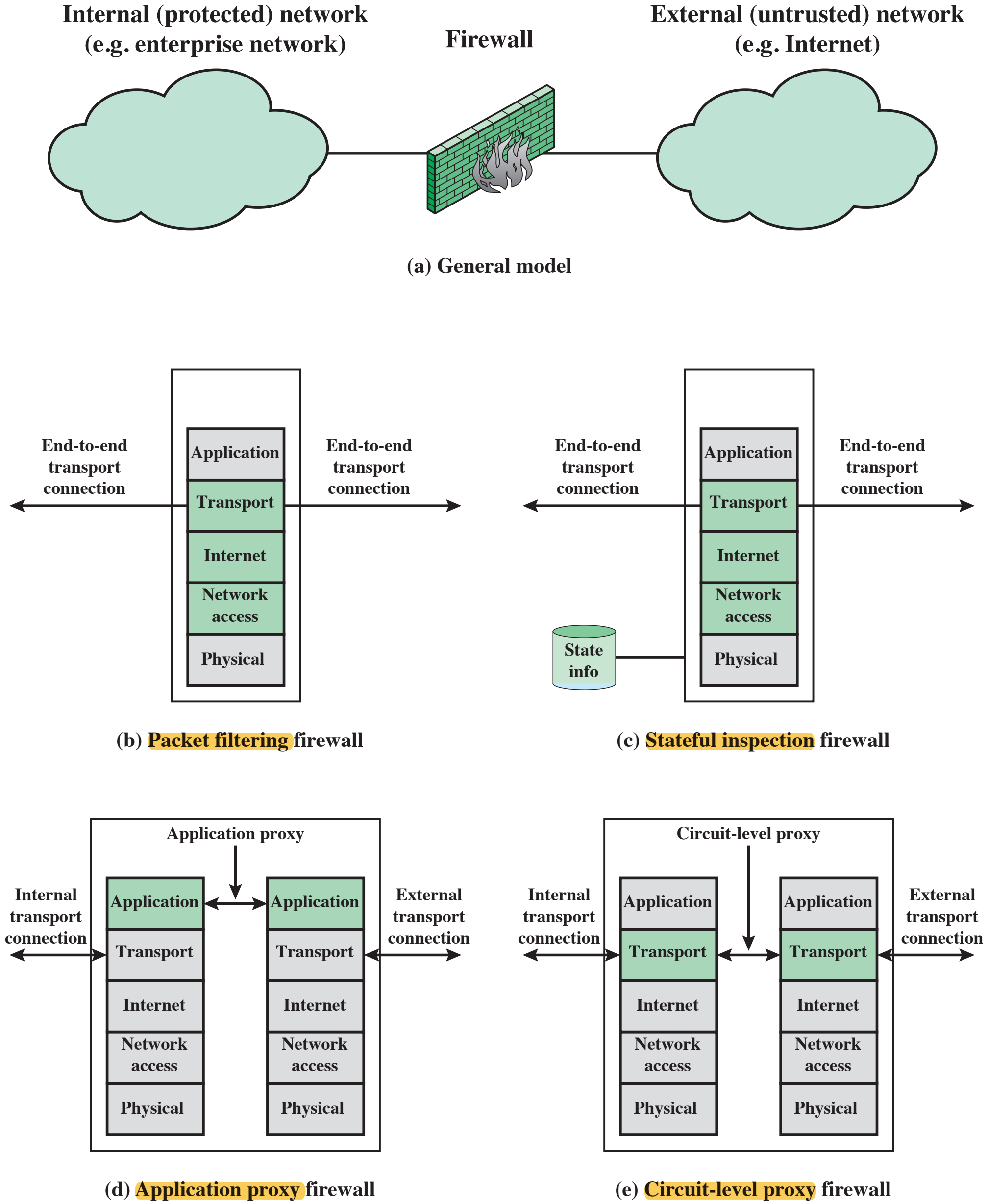
Firewalls have their limitations, including the following:

The firewall cannot protect against attacks that bypass the firewall. Internal systems may have dial-out capability to connect to an ISP. An internal LAN may support a modem pool that provides dial-in capability for traveling employees and telecommuters

The firewall may not protect fully against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker

An improperly secured wireless LAN may be accessed from outside the organization. An internal firewall that separates portions of an enterprise network cannot guard against wireless communications between local systems on different sides of the internal firewall

A laptop, smartphone, or portable storage device may be used and infected outside the corporate network, and then connected and used internally


Internal (protected) network
(e.g. enterprise network)
Firewall
External (untrusted) network
(e.g. Internet)
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
State info
Application proxy
Circuit-level proxy
Internal transport connection
External transport connection

(a) General model

(b) Packet filtering firewall

(c) Stateful inspection firewall

(d) Application proxy firewall

(e) Circuit-level proxy firewall

Figure 21.1 Types of Firewalls

Rule Set A

action	ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

Figure 21.2 Packet-Filtering Example

Packet Filtering Firewalls

- Advantages:
  - Simplicity
  - Typically transparent to users
  - Are very fast
- Weaknesses:
  - They cannot prevent attacks that employ application-specific vulnerabilities or functions
  - The logging functionality present in packet filter firewalls is limited
  - Most packet filter firewalls do not support advanced user authentication schemes
  - Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack
  - Packet filter firewalls are susceptible to security breaches caused by improper configurations

Attacks and Countermeasures

- Some of the attacks that can be made on packet filtering firewalls and the appropriate countermeasures are the following:
  - **IP address spoofing:** The intruder transmits packets from the outside with a source IP address field containing an address of an internal host
    - The countermeasure is to discard packets with an inside source address if the packet arrives on an external interface. In fact, this countermeasure is often implemented at the router external to the firewall
  - **Source routing attacks:** The source station specifies the route that a packet should take as it crosses the Internet, in the hopes that this will bypass security measures that do not analyze the source routing information
    - The countermeasure is to discard all packets that use this option
  - **Tiny fragment attacks:** The intruder uses the IP fragmentation option to create extremely small fragments and force the TCP header information into a separate packet fragment
    - A tiny fragment attack can be defeated by enforcing a rule that the first fragment of a packet must contain a predefined minimum amount of the transport header. If the first fragment is rejected, the filter can remember the packet and discard all subsequent fragments

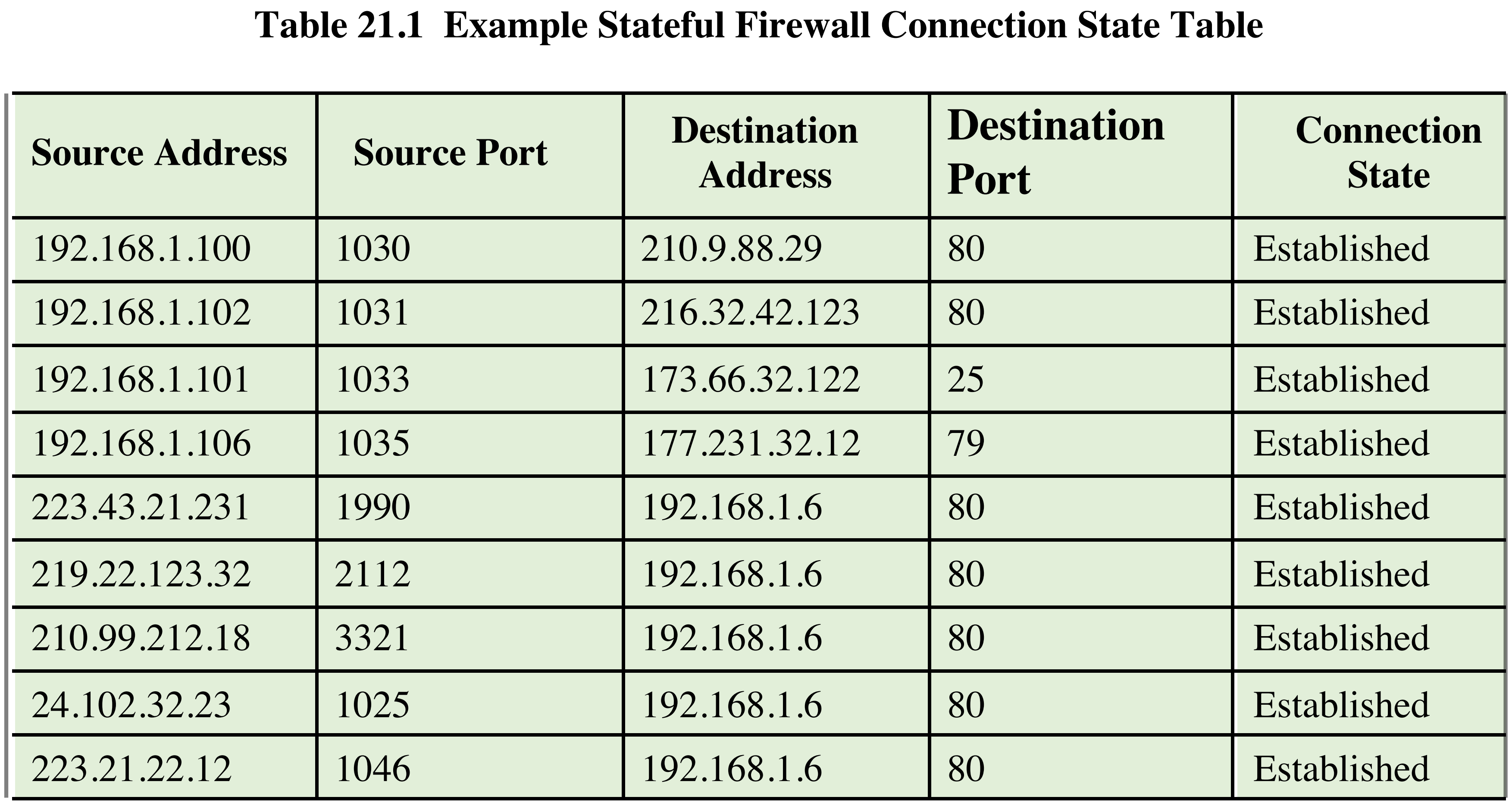


Table 21.1 Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

(Table is on page 659 in the textbook)

Application-Level Gateway

- Also called an *application proxy*
- Acts as a relay of application-level traffic
- Tend to be more secure than packet filters
  - Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications
- A prime disadvantage of this type of gateway is the additional processing overhead on each connection
  - In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions

Circuit-Level Gateway

- A fourth type of firewall is the circuit-level gateway or *circuit-level proxy*
- Can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications
- A circuit-level gateway does not permit an end-to-end TCP connection
- The security function consists of determining which connections will be allowed
- A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users

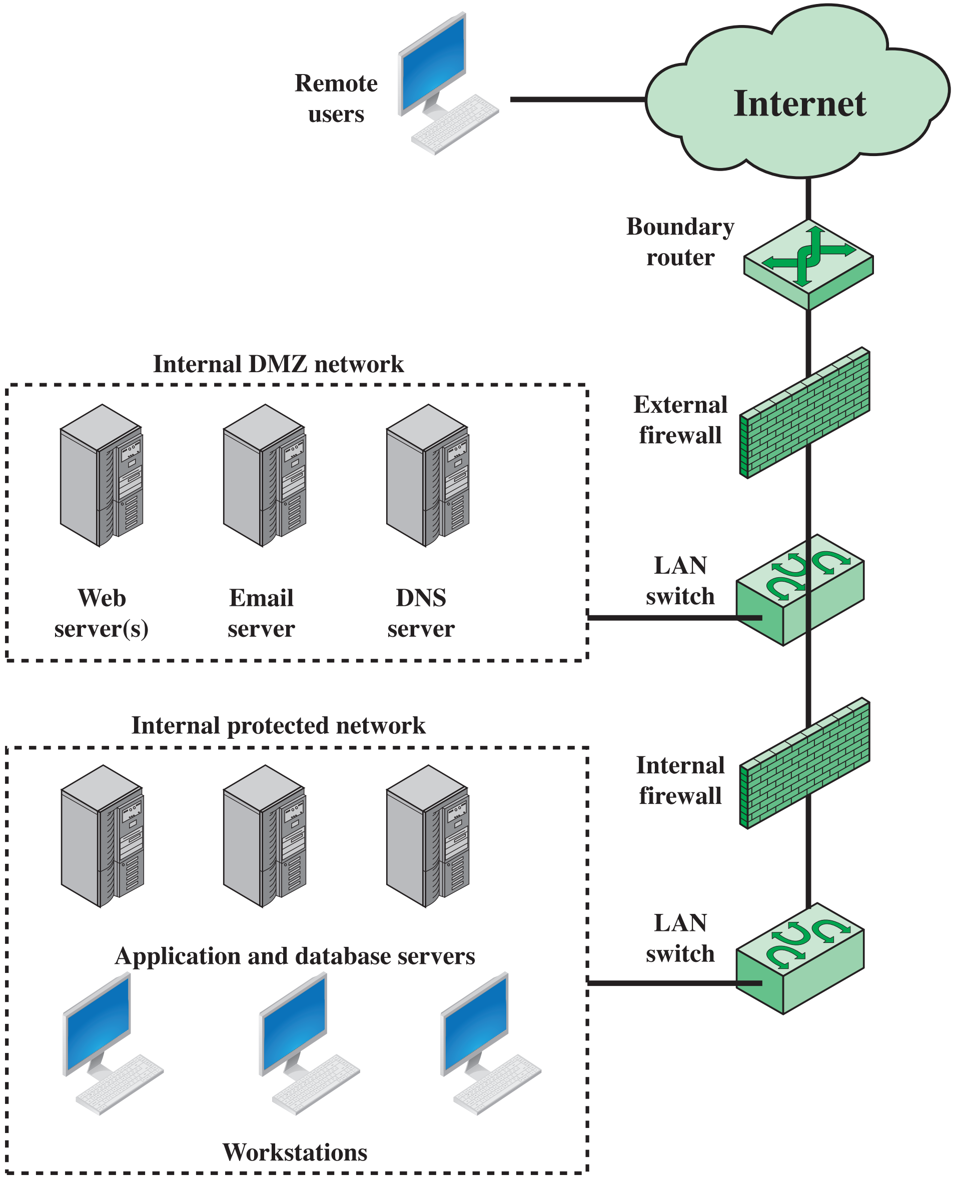


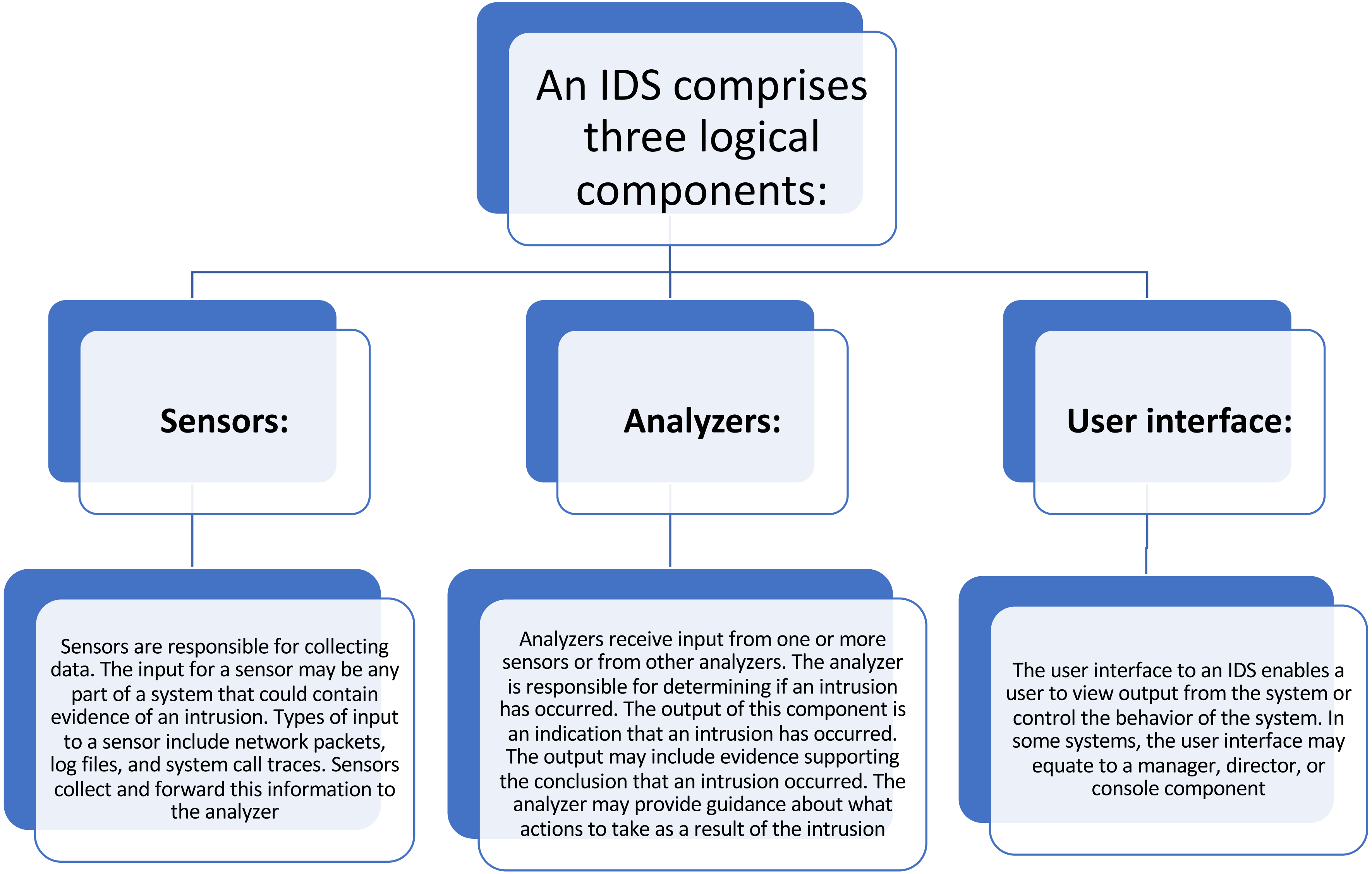
Figure 21.3 Example Firewall Configuration

Intrusion Detection Systems

- **Intrusion:**
  - Violations of security policy, usually characterized as attempts to affect the confidentiality, integrity, or availability of a computer or network. These violations can come from attackers accessing systems from the Internet or from authorized users of the systems who attempt to overstep their legitimate authorization levels or who use their legitimate access to the system to conduct unauthorized activity
- **Intrusion detection:**
  - The process of collecting information about events occurring in a computer system or network and analyzing them for signs of intrusions
- **Intrusion detection system:**
  - Hardware or software products that gather and analyze information from various areas within a computer or a network for the purpose of finding, and providing real-time or near-real-time warning of, attempts to access system resources in an unauthorized manner

Intrusion Detection Systems

- Intrusion detection systems (IDSs) can be classified as follows:
  - **Host-based IDS:**
    - Monitors the characteristics of a single host and the events occurring within that host for suspicious activity
  - **Network-based IDS:**
    - Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity



An IDS comprises three logical components:

Sensors:

Sensors are responsible for collecting data. The input for a sensor may be any part of a system that could contain evidence of an intrusion. Types of input to a sensor include network packets, log files, and system call traces. Sensors collect and forward this information to the analyzer

Analyzers:

Analyzers receive input from one or more sensors or from other analyzers. The analyzer is responsible for determining if an intrusion has occurred. The output of this component is an indication that an intrusion has occurred. The output may include evidence supporting the conclusion that an intrusion occurred. The analyzer may provide guidance about what actions to take as a result of the intrusion

User interface:

The user interface to an IDS enables a user to view output from the system or control the behavior of the system. In some systems, the user interface may equate to a manager, director, or console component

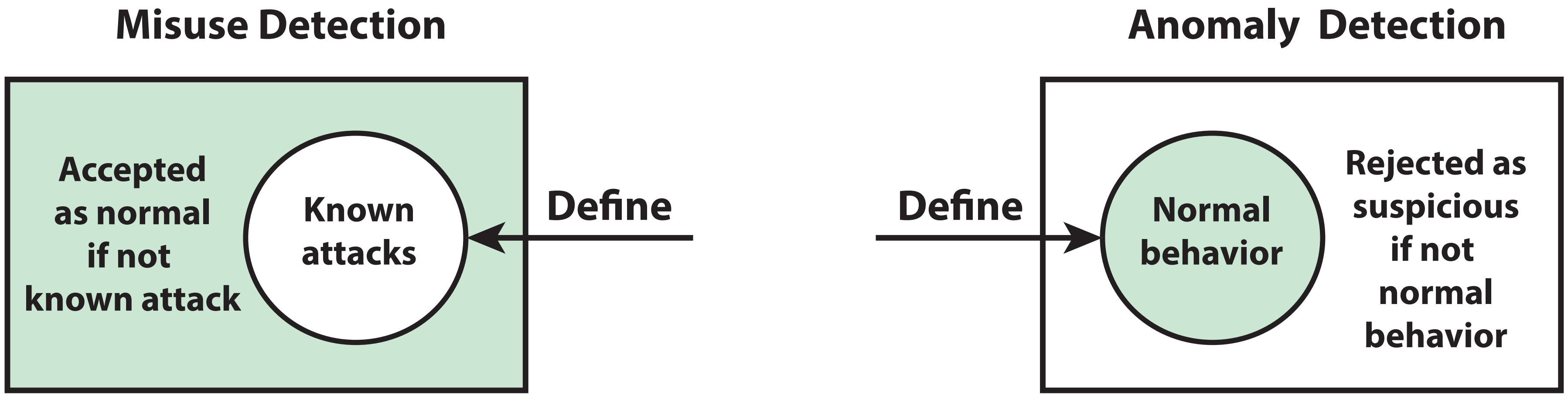

Misuse Detection
Accepted as normal if not known attack
Known attacks
Define
Define
Anomaly Detection
Normal behavior
Rejected as suspicious if not normal behavior

Figure 21.4 Approaches to Intrusion Detection

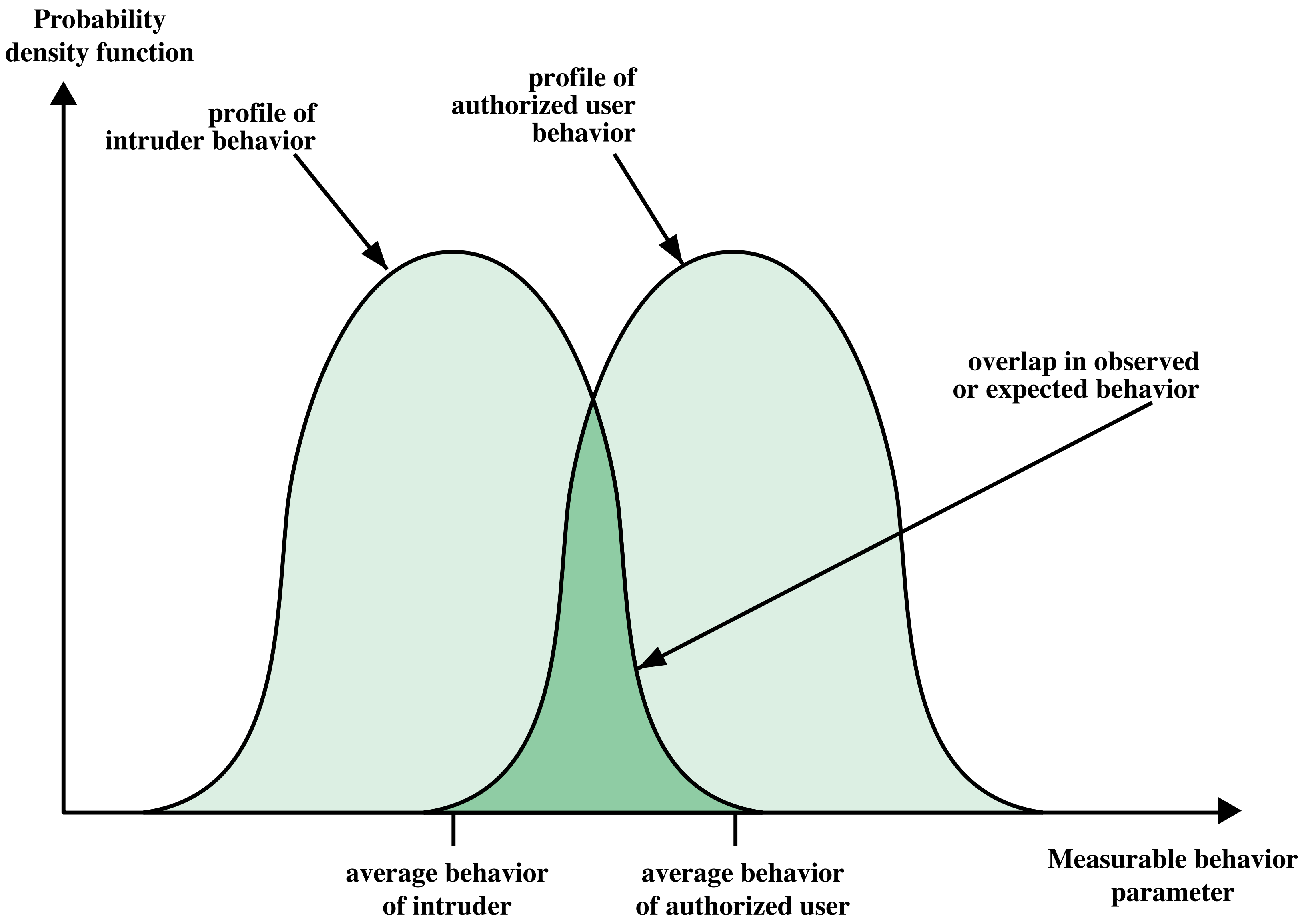
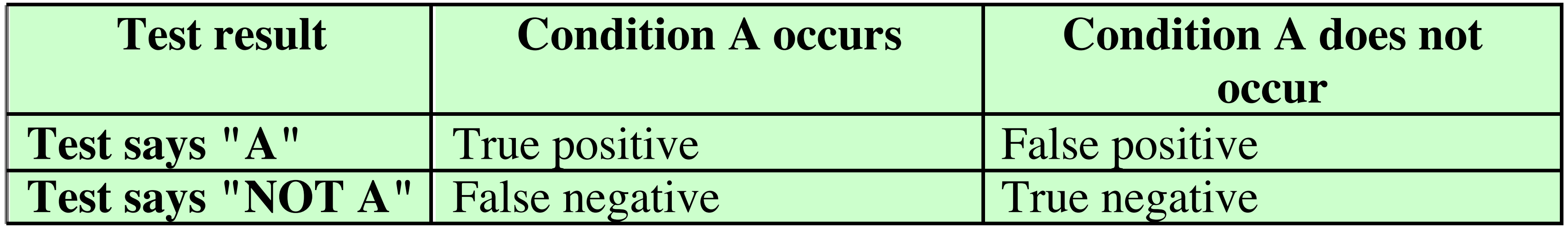

Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

Figure 21.5 Profiles of Behavior of Intruders and Authorized Users

Table 21.2 Test Outcomes



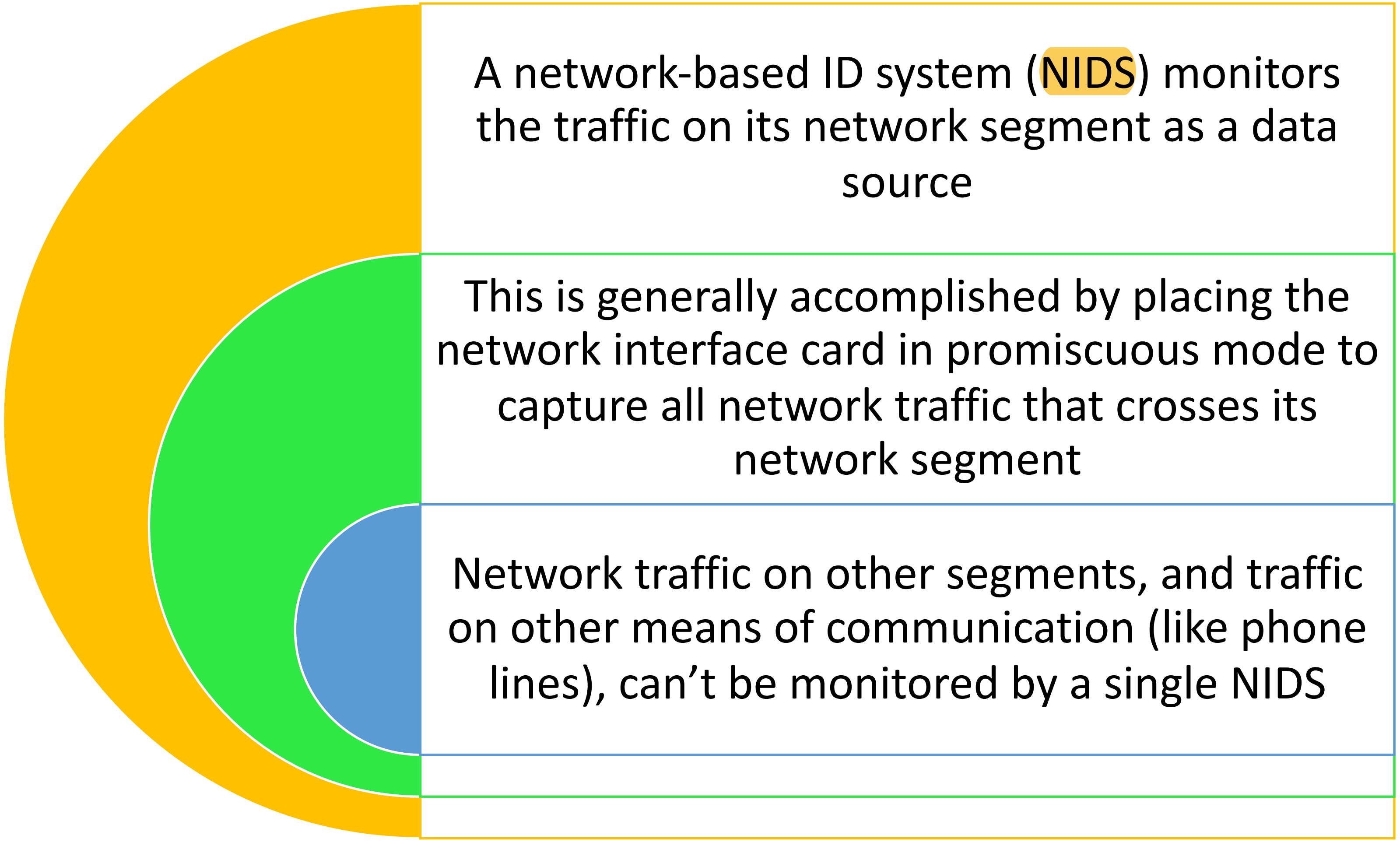
Test result	Condition A occurs	Condition A does not occur
Test says "A"	True positive	False positive
Test says "NOT A"	False negative	True negative

(Table is on page 664 in the textbook)

Host-Based IDS Techniques

- Host-based IDSs
  - Add a specialized layer of security software to vulnerable or sensitive systems
  - Monitor activity on the system in a variety of ways to detect suspicious behavior
  - In some cases, an IDS can halt an attack before any damage is done, but its primary purpose is to detect intrusions, log suspicious events, and send alerts
  - The primary benefit is that it can detect both external and internal intrusions
- Host-based IDSs use one or a combination of anomaly and misuse protection
  - For anomaly detection, two common strategies are:
    - Threshold detection
    - Profile based

Network-Based Intrusion Detection System

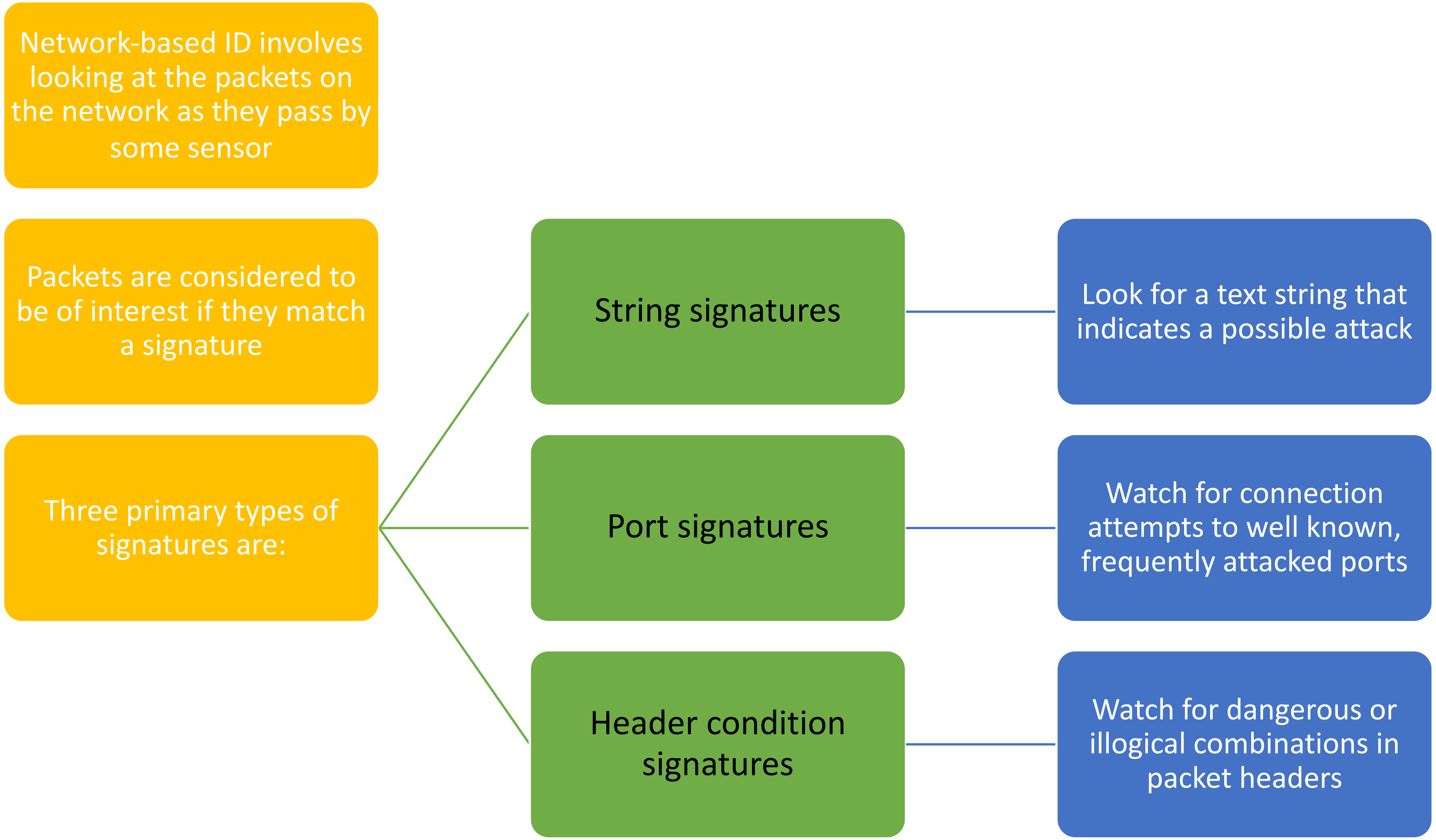


A network-based ID system (NIDS) monitors the traffic on its network segment as a data source

This is generally accomplished by placing the network interface card in promiscuous mode to capture all network traffic that crosses its network segment

Network traffic on other segments, and traffic on other means of communication (like phone lines), can’t be monitored by a single NIDS

NIDS



Network-based ID involves looking at the packets on the network as they pass by some sensor

Packets are considered to be of interest if they match a signature

Three primary types of signatures are:

- String signatures – Look for a text string that indicates a possible attack
- Port signatures – Watch for connection attempts to well known, frequently attacked ports
- Header condition signatures – Watch for dangerous or illogical combinations in packet headers

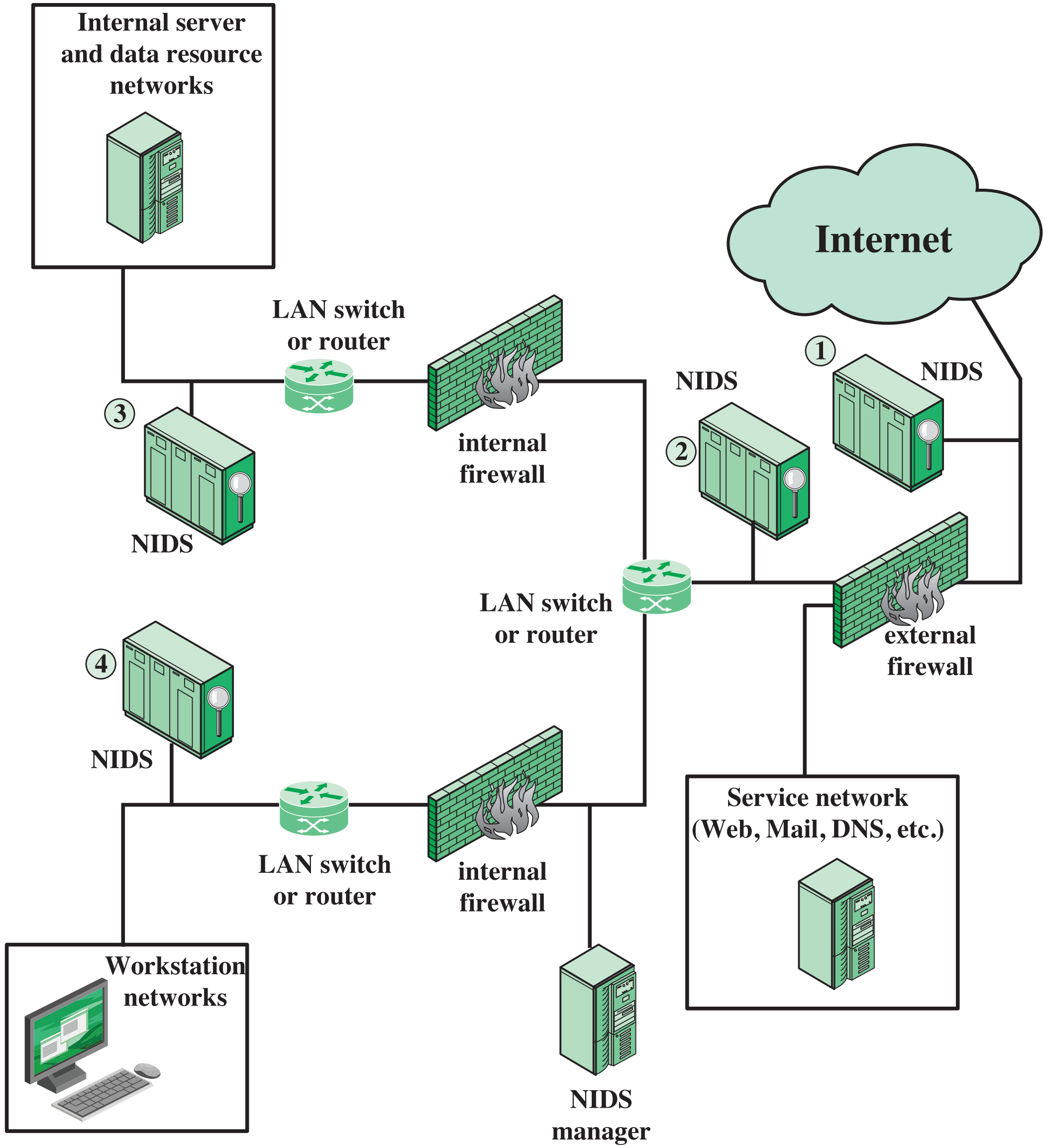


Figure 21.6 Example of NIDS Sensor Deployment

Malicious Software

- Commonly called *malware, is p*erhaps the most significant security threat to organizations
- NIST SP 800-83 (*Guide to Malware Incident Prevention and Handling for Desktops and Laptops*) defines malware as
    - “a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications, or operating system”
- Hence, malware can pose a threat to application programs, to utility programs, such as editors and compilers, and to kernel-level programs
- Malware can also be used on compromised or malicious Web sites and servers, or in especially crafted spam emails or other messages, which aim to trick users into revealing sensitive personal information

Types of Malware

- **Virus**
  - A computer program that can copy itself and infect a computer without permission or knowledge of the user
  - A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk
  - It can replicate itself and can attach to another program
  - The program to which the virus attaches itself is known as *host*
- **Worm**
  - A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself
  - The main differences between viruses and worms is that the worms can self-replicate and propagate without human interaction and that the worm does not integrate into existing code
  - Worms target systems and applications that have known vulnerabilities

Types of Malware

- **Trojan Horse**
  - A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program
  - The purpose of a Trojan horse is to make a malicious program appear like a legitimate program
  - Trojan horse can monitor users’ action, steal users’ data, and can open a backdoor for the attackers

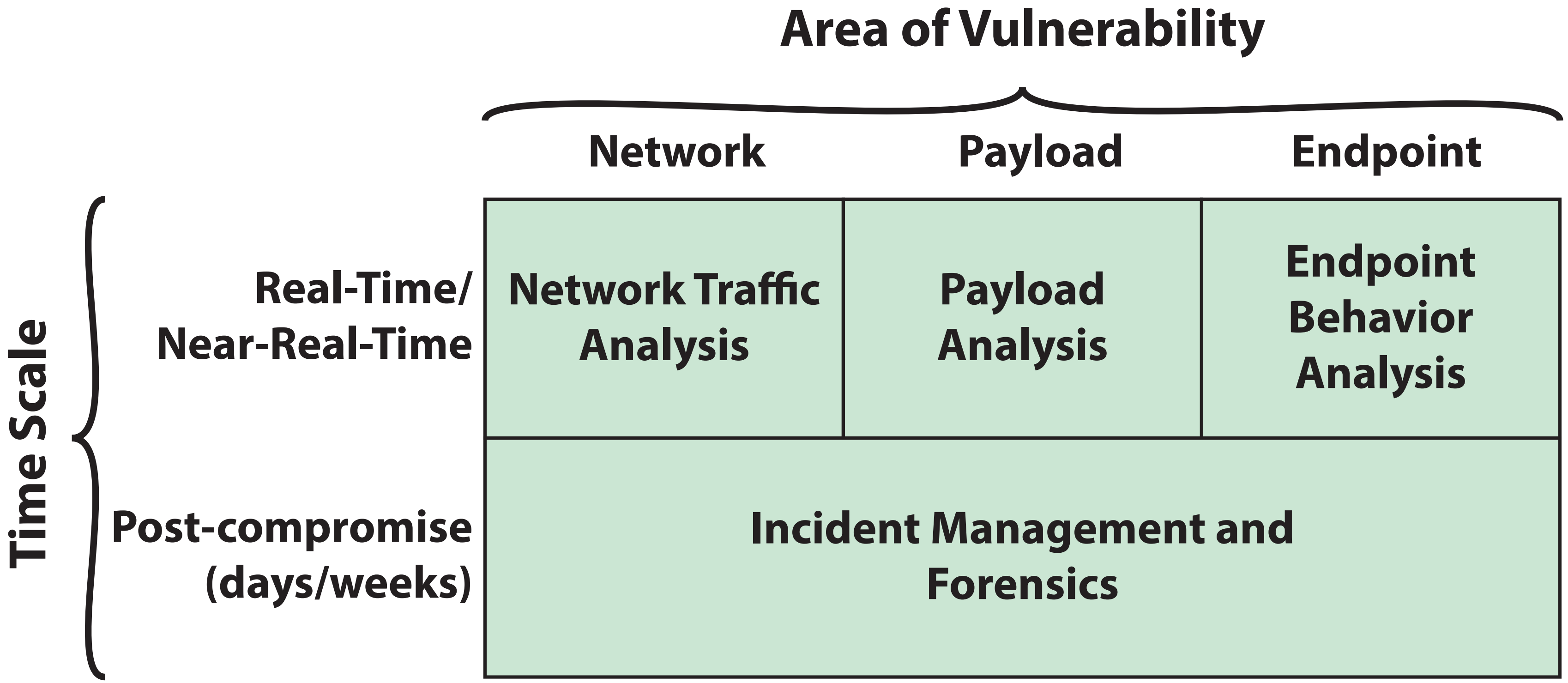
- **Spyware**
  - Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge

Types of Malware

- **Rootkit**
  - A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker's activities on the host and permit the attacker to maintain root-level access to the host through covert means
- **Backdoor**
  - An undocumented way of gaining access to a computer system
  - Typically, a backdoor is a program that has the ability to bypass a system's security control, allowing an attacker to access the system stealthily
  - Backdoors are usually installed by the attackers or by a malware program

Types of Malware

- **Mobile Code**
  - Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics
- **Bot**
  - Also known as a zombie
  - Program that is installed on a system to launch attacks on other machines
  - A collection of bots that act in concert is referred to as a *botnet*



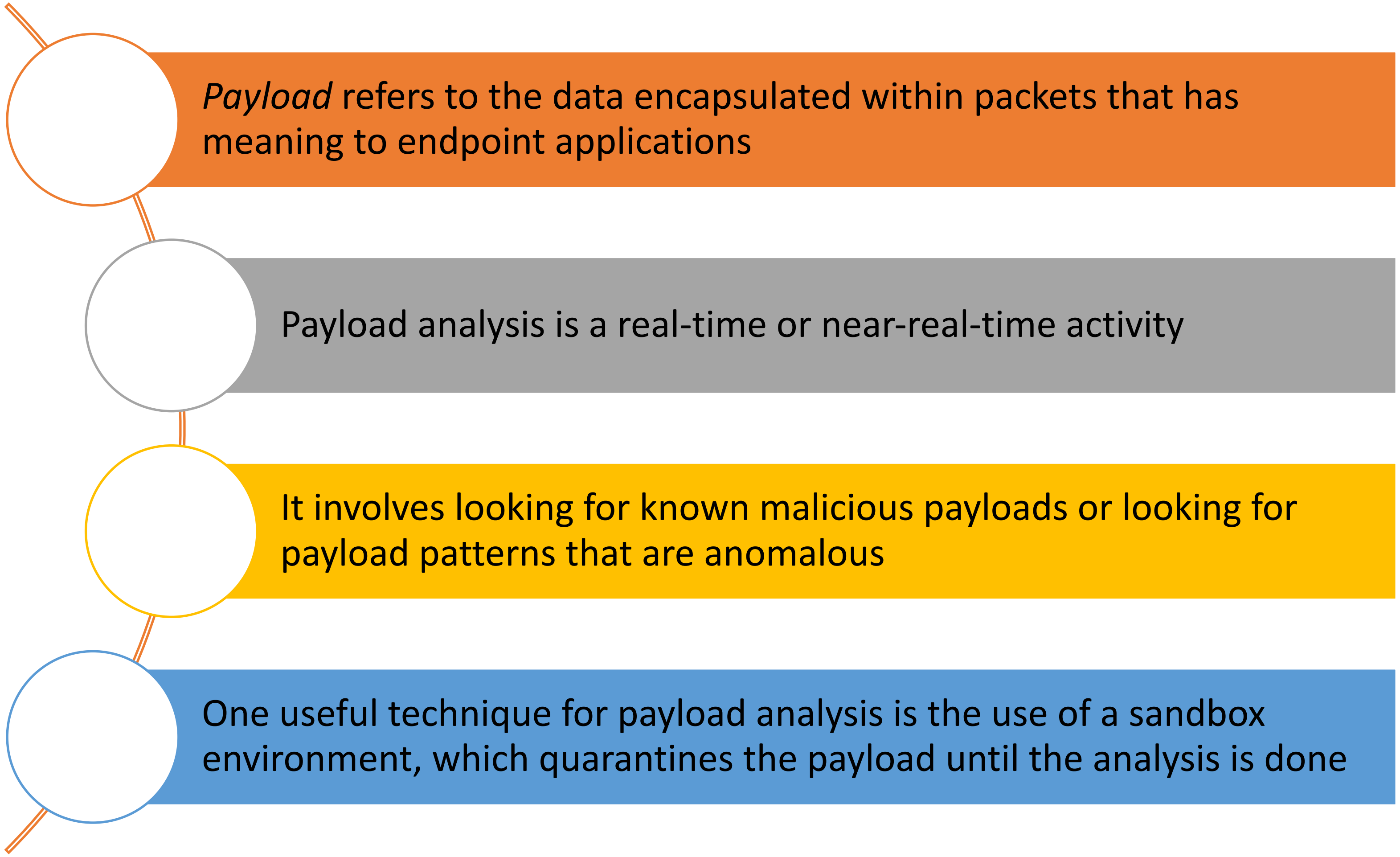
		Area of Vulnerability		
		Network	Payload	Endpoint
Time Scale	Real-Time/ Near-Real-Time	Network Traffic Analysis	Payload Analysis	Endpoint Behavior Analysis
	Post-compromise (days/weeks)	Incident Management and Forensics		

Figure 21.7 Five Elements of Malware Defense

Network Traffic Analysis

- Involves monitoring traffic flows to detect potentially malicious activity
  - Such monitors are often placed at the boundary of the enterprise network to the outside world
  - Monitors can also be placed on internal network devices or near server endpoints
- Traffic analysis can involve misuse detection (signature detection) or anomaly detection
  - As an example of misuse detection, a dramatic surge in traffic at any point likely indicates that a DDoS attack is underway
  - For anomaly detection, network security software needs to collect and maintain profiles of typical network traffic patterns, and then monitor current traffic for significant deviation from normal behavior

Payload Analysis



Payload refers to the data encapsulated within packets that has meaning to endpoint applications

Payload analysis is a real-time or near-real-time activity

It involves looking for known malicious payloads or looking for payload patterns that are anomalous

One useful technique for payload analysis is the use of a sandbox environment, which quarantines the payload until the analysis is done

Endpoint Behavior Analysis

- Involves a wide variety of tools and approaches implemented at the endpoint
- Antivirus software uses signature and anomaly detection techniques to identify malware and prevent it from executing on the host system
- Application whitelisting, which restricts application execution to only known good applications is also employed
- At the system software level, application containers can isolate applications and files in virtual containers to prevent damage

Incident Management

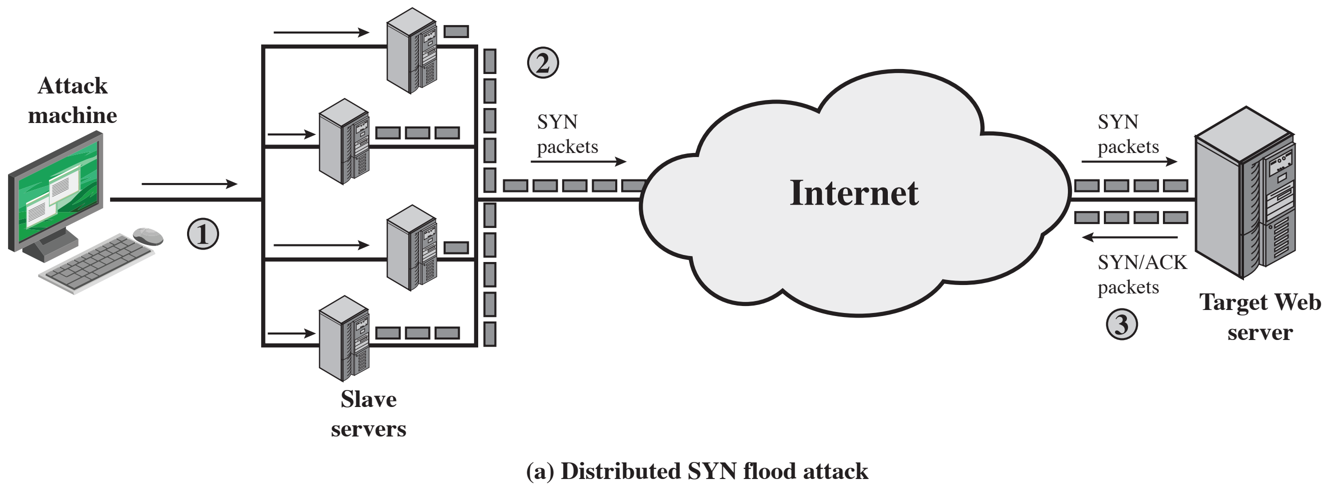
- Information security incident management consists of processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents
- Key elements of incident management include:
    - Data collection
    - Data aggregation
    - Data normalization
    - Correlation
    - Alerting
    - Reporting/Compliance

Forensics

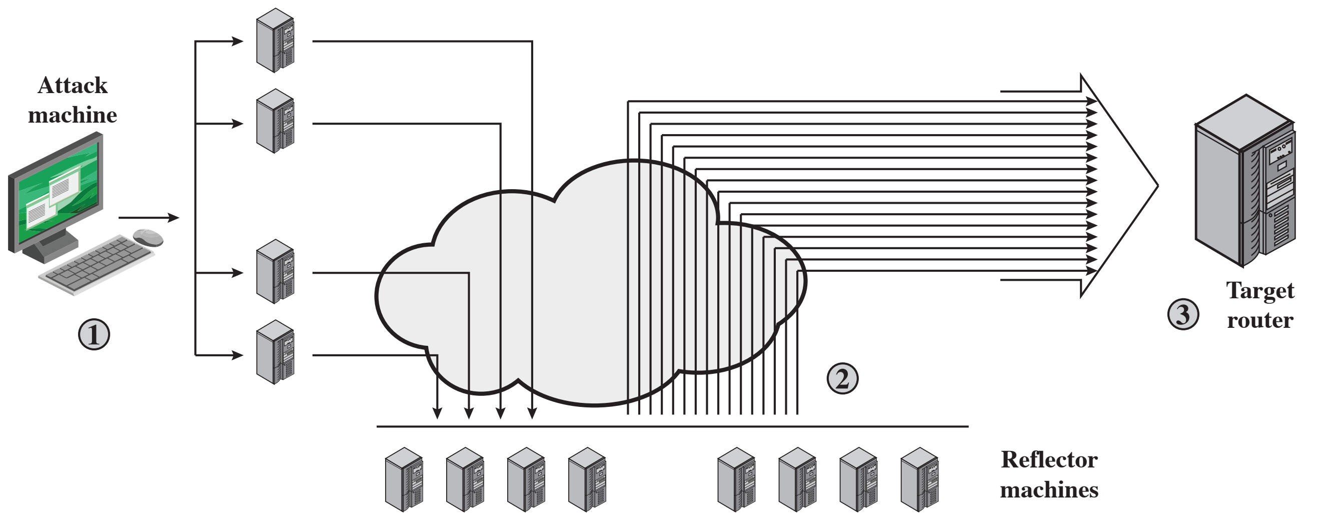
- NIST SP 800-96 (*Guide to Integrating Forensic Techniques into Incident Response*) defines computer forensics, or digital forensics, as:
  - “ The identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data”
- Computer forensics seeks to answer a number of questions including the following:
  - What happened?
  - When did the events occur?
  - In what order did the events occur?
  - What was the cause of these events?
  - Who caused these events to occur?
  - What enabled these events to take place?
  - What was affected? How much was it affected?
- Most security incidents do not require a forensic investigation but can be dealt with by the ordinary incident management process
- More serious incidents may warrant the more in-depth analysis of a forensic investigation

Denial-of-Service Attack (DoS)

- An attempt to prevent legitimate users of a service from using that service
- When this attack comes from a single host or network node, then it is simply referred to as a DoS attack
- A more serious threat is posed by a Distributed Denial-of-Service (DDoS) attack
  - DDoS attacks make computer systems inaccessible by flooding servers, networks, or even end-user systems with useless traffic so that legitimate users can no longer gain access to those resources
  - In a typical DDoS attack, a large number of compromised hosts are amassed to send useless packets

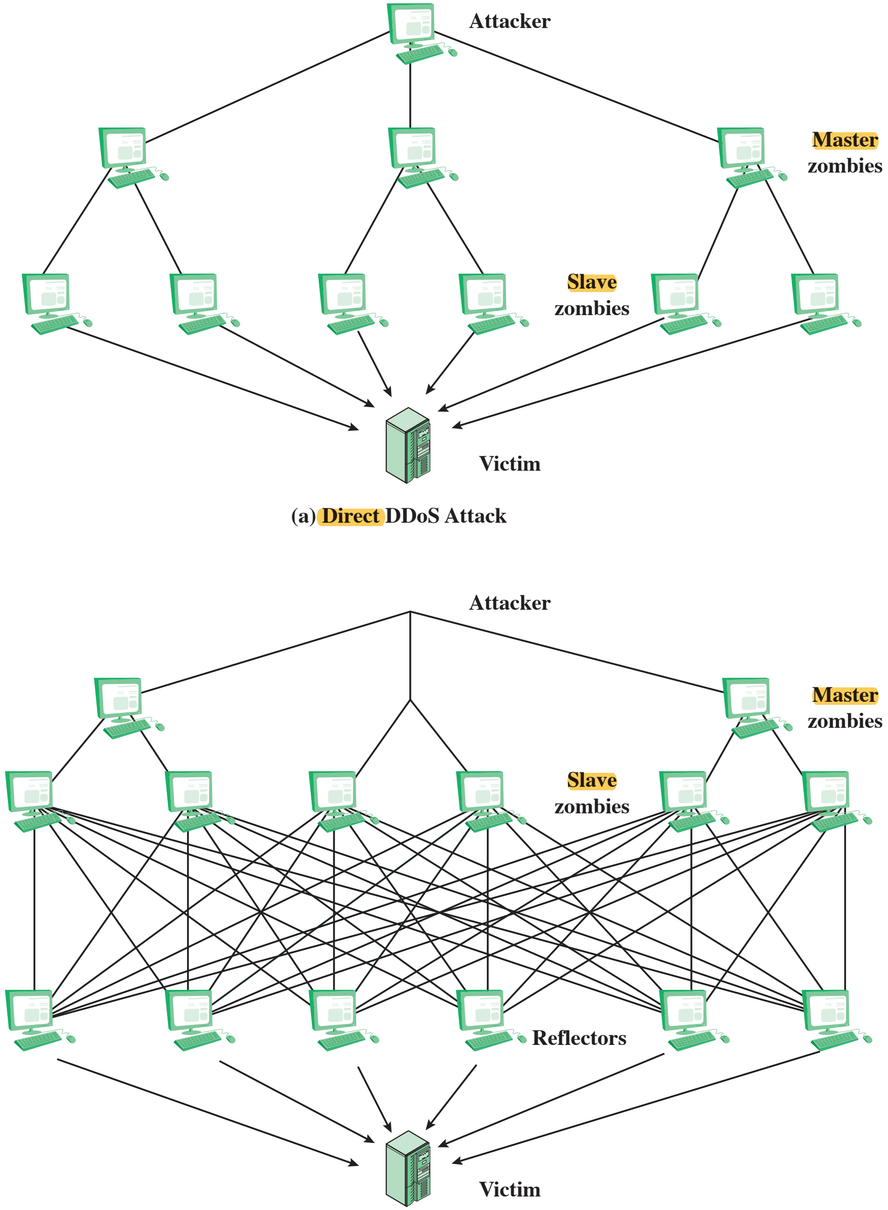


(a) Distributed SYN flood attack



(a) Distributed ICMP attack

Figure 21.8 Examples of Simple DDoS Attacks



(a) Direct DDoS Attack

(b) Reflector DDoS Attack

Figure 21.9 Types of Flooding-Based DDoS Attacks

DDoS Countermeasures

- In general, there are three lines of defense against DDoS attacks:
  - **Attack prevention and preemption (before the attack):**
    - These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients
    - Techniques include enforcing policies for resource consumption and providing backup resources available on demand
    - In addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks
  - **Attack detection and filtering (during the attack):**
    - These mechanisms attempt to detect the attack as it begins and respond immediately. This minimizes the impact of the attack on the target
    - Detection involves looking for suspicious patterns of behavior
    - Response involves filtering out packets likely to be part of the attack
  - **Attack source traceback and identification (during and after the attack):**
    - This is an attempt to identify the source of the attack as a first step in preventing future attacks. However, this method typically does not yield results fast enough, if at all, to mitigate an ongoing attack

- The challenge in coping with DDoS attacks is the sheer number of ways in which they can operate so DDoS countermeasures must evolve with the threat

Summary

- Explain the role of firewalls as part of a computer and network security strategy
- List the key characteristics of firewalls
- Understand the relative merits of various choices for firewall location and configurations
- Understand the basic principles of and requirements for intrusion detection

- Discuss the key features of intrusion detection systems
- Describe some of the main categories of malicious software
- Present an overview of the key elements of malware defense
- Discuss the nature of a distributed denial of service attack