NETWORK SECURITY

The modules in Part 4 deal with securing an enterprise computer network. In Module 8, you learn about the attacks that target networks and how to assess vulnerabilities and create physical defenses. Module 9 demonstrates how to protect a network through network security appliances and technologies. In Module 10, you will explore the concepts and tools for protecting cloud and virtual environments. Finally, in Module 11, you learn how to manage wireless network security.

PART 4

MODULE 10
CLOUD AND VIRTUALIZATION SECURITY

MODULE 11
WIRELESS NETWORK SECURITY

MODULE 8

NETWORKING THREATS, ASSESSMENTS, AND DEFENSES

After completing this module, you should be able to do the following:

1. Describe the different types of networking-based attacks
2. List the different network assessment tools
3. Explain how physical security defenses can be used

Front-Page Cybersecurity

What would you think if the CEO of Apple said, "Nobody really wants to hack us."? Or if Google posted on its website, "Attackers aren't interested in targeting us." Or the president of Amazon said, "We're not on any attacker's radar screen."

In today's cybersecurity environment, it would be surprising—probably shocking—to hear people say that attackers are not interested in them. But that's exactly what happened recently. Could it be true that attackers are not interested in a particular company? Or does the CEO of the company not understand cybersecurity?

A new startup called View manufactures and installs "smart windows" that automatically adjust to sunlight and glare. The blue-tinted windows are expensive: they cost about five times as much as traditional glass windows. However, View windows have several advantages. They reduce cooling costs by blocking heat from sunlight and they can eliminate the need for blinds or window treatments. If a criminal breaks one of the windows, police can immediately be notified. Finally, View windows allow more people to fit into a building. Because View windows reduce glare and heat from the sun, employees can be seated in areas that they could not normally use. One organization installing View windows will be able to place the same number of employees in one-third of the space.

All View windows are interconnected. They are attached to the organization's local area network (LAN), allowing them to be accessed over the Internet. In fact, each View window has its own IP address. Users can control the windows via a smartphone app.

The View CEO recently said about the company's windows, "The good news is the window's not that interesting to hack."

Most security professionals would strongly disagree with the View CEO. In fact, View windows are interesting to attackers for three reasons.

1. *Entry point into the owner's corporate network.* Internet of Things (IoT) devices, such as View windows, are the target of attackers because the devices lack security. The same week the View CEO made his bold statement, the Microsoft Threat Intelligence Center said state actors working for the Russian government were using printers, video decoders, and similar IoT devices as a beachhead or entry point to penetrate targeted computer networks. "These devices became points of ingress from which the actor established a presence on the network and continued looking for further access," Microsoft

said. In other words, IoT devices with little or no security allowed an attacker an entry point into the network. Attackers could then pivot to move through the network in search of higher-privileged accounts that would grant access to higher-value data. In the latest attack referenced by Microsoft, after gaining access to the IoT devices, the threat actors ran Tcpdump, a program often used by security personnel to assess network security by sniffing network traffic on local subnets. They also dropped a simple shell script that allowed them to stay on the network for an extended period of time. An analysis of network traffic showed the IoT devices were communicating with an external command and control (C&C) server.

2. *Attack point against other networks.* For several years, threat actors have compromised unprotected IoT devices and then gathered them into a botnet. The botnets attacked other devices or networks. Most notably, IoT-based botnets have been used to launch distributed denial of service or DDoS attacks. A company with View windows installed could find that the windows are a launching point for other attacks.
3. *Backflow into View's own network*. View requires that all its windows have remote connectivity to the company's headquarters so that View can "commission, configure, monitor, and maintain the system." The product documentation lists options for allowing remote access, ranging from "Firewall via DMZ" and "Firewall via Port Mapping" to "Firewall with VPN Access" and other options. However, an attacker who can circumvent these protections can "backflow" into the View network. Because the windows are remotely connected to View's own network, an attacker could compromise a View window belonging to another company and then sneak into the View network. In this way, View windows could allow an attacker entry into View's network.

Despite the statement from the CEO of View that "The good news is the window's not that interesting to hack," the bad news is that View windows are very interesting to hack. The worse news may be that the View CEO is evidently not taking these risks seriously.

Whereas technology devices—including smartphones, tablets, and laptop computers—usually receive all the praise for ushering the world into a new and exciting era, in reality, the invisible network that is connecting the devices should be receiving an equal share of adoration. Imagine a smartphone that cannot connect to a network to receive messages or link to websites but instead can use only what is contained on the smartphone. Most users would quickly dump an unconnected smartphone in the nearest trash bin. The connectivity through networks is what has made today's devices revolutionary.

Invisible networks can link a device to a virtually unlimited volume of information for research. They can also support relationships between people who are separated by hundreds of feet or thousands of miles. E-commerce through networks makes it possible to perform nearly any real-world task online, including retail shopping, banking, real estate transactions, airline bookings, and movie streaming. Networks have empowered today's technology devices to create our digital revolution.

However, networks have also introduced new issues surrounding privacy, trust, and reliability and are responsible for the explosive growth of cybersecurity attacks. They have opened the door for threat actors to reach across the world to invisibly and instantaneously launch attacks on any device connected to the network. Just as users can surf the web without openly identifying themselves, attackers can use this anonymity to cloak their identity and prevent authorities from finding and prosecuting them.

This module begins a study of network attacks and defenses. First, the module explores common attacks that are launched against networks today. Then it looks at tools for assessing and defending networks. Finally, it examines physical security defenses for protecting network technology devices.

ATTACKS ON NETWORKS

CERTIFICATION

1.3 Given a scenario, analyze potential indicators associated with application attacks.

1.4 Given a scenario, analyze potential indicators associated with network attacks.

3.1 Given a scenario, implement secure protocols.

Threat actors place a high priority on targeting networks in their attacks. Exploiting a single network vulnerability can expose hundreds or thousands of devices. Several types of attacks target a network or a process that relies on a network, including interception attacks, Layer 2 attacks, DNS attacks, distributed denial of service attacks, and malicious coding and scripting attacks.

Interception Attacks

Some attacks are designed to intercept network communications. Three of the most common interception attacks are man-in-the-middle, session replay, and man-in-the-browser attacks.

Man-in-the-Middle (MITM)

Suppose that Angie, a high school student, is in danger of receiving a poor grade in math. Her teacher, Mr. Ferguson, mails a letter to Angie's parents requesting a conference regarding her performance. However, Angie waits for the mail and retrieves the letter from the mailbox before her parents come home. She forges her parent's signature on the original letter declining a conference and mails it to her teacher. Angie also replaces the real letter with a counterfeit pretending to be from Mr. Ferguson that compliments Angie on her math work. The parents read the fake letter and tell Angie they are proud of her, while Mr. Ferguson is puzzled that Angie's parents are not concerned about her grades.

Angie has conducted a type of **man-in-the-middle (MITM)** attack. In an MITM, a threat actor is positioned in a communication between two parties, as shown in Figure 8-1. Neither of the legitimate parties is aware of the presence of the threat actor and communicate freely, thinking they are talking only to the authentic party. The goal of an MITM attack is to eavesdrop on the conversation or impersonate one of the parties.

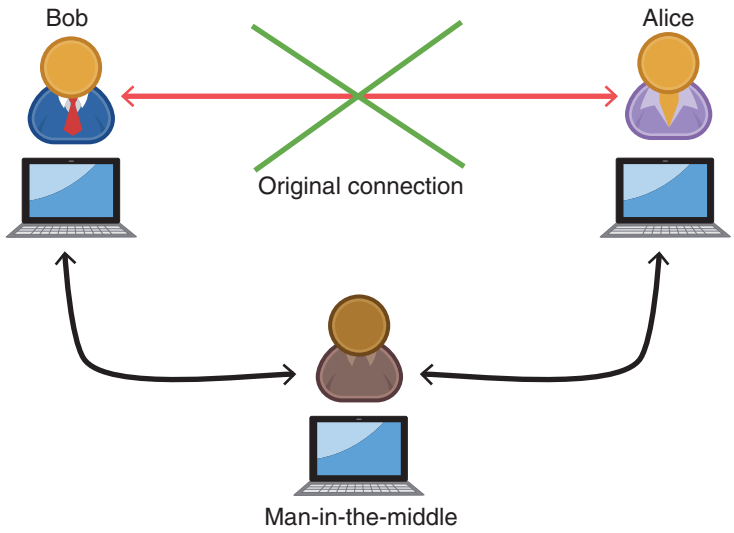


Figure 8-1 MITM attack

A typical MITM attack has two phases. The first phase is intercepting the traffic. A common form of interception is for the threat actor to pretend to be an approved web application by altering packet headers in an IP address. When users attempt to access a URL connected to the application, they are instead sent to the attacker's website.

The second phase is to decrypt the transmissions. An attacker could send a fake digital certificate associated with a compromised application to the victim's computer to trick the computer into verifying the authenticity of the application. The attacker can then access any data entered by the victim.

Session Replay

A *replay* attack is a variation of an MITM attack. Whereas an MITM attack alters and then sends the transmission immediately, a replay attack makes a copy of the legitimate transmission before sending it to the recipient. This copy is used later when the MITM "replays" the transmission.

NOTE 1

Each time a user visits a website, the web server issues a new session ID that usually remains active as long as the browser is open. In some instances, after several minutes of inactivity, the server may generate a new session ID. Closing the browser terminates the active session ID, and it should not be used again.

A specific type of replay attack is a **session replay** attack, which involves intercepting and using a *session ID* to impersonate a user. A session ID is a unique number that a web server assigns a specific user for the duration of the user's visit (session). Most servers create complex session IDs by using the date, time of the visit, and other variables such as the device IP address, email address, username, user ID, role, privilege level, access rights, language preferences, account ID, current state, last login, session timeouts, and other internal session details. Session IDs are usually least 128 bits in length and hashed using a secure hash function such as SHA-256.

Session IDs can be contained as part of a URL extension, by using hidden form fields in which the state is sent to the client as part of the response and returned to the server as part of a form's hidden data, or through cookies. A sample session ID is *fa2e76d49a0475910504cb3ab7a1f626d174d2d*.

Threat actors use several techniques for stealing an active session ID. These include network attacks (hijacks and altered communication between two users) and endpoint attacks (cross-site scripting, Trojans, and malicious JavaScript coding). Once a session ID has been successfully stolen, a threat actor can impersonate the user.

Man-in-the-Browser (MITB)

Like an MITM attack, a **man-in-the-browser (MITB)** attack intercepts communication between parties to steal or manipulate the data. Whereas an MITM attack occurs between two endpoints—such as between two laptops or a user's computer and a web server—an MITB attack occurs between a browser and the underlying computer. Specifically, an MITB attack seeks to intercept and then manipulate the communication between the web browser and the security mechanisms of the computer.

An MITB attack usually begins with a Trojan infecting the computer and installing an "extension" into the browser configuration so that opening the browser activates the extension. When a user enters the URL of a site, the extension checks whether the site is targeted for attack. After the user signs in to the site, the extension waits for a specific webpage to be displayed in which the user enters information, such as the account number and password for an online financial institution (a favorite target of MITB attacks). When the user clicks Submit, the extension captures all the data from the fields on the form and may even modify some of the entered data. The browser sends the data to the server, which performs the transaction, generates a receipt, and returns it to the browser. The malicious extension captures the receipt data and modifies it (with the data the user originally entered) so that it appears that a legitimate transaction has occurred.

Threat actors gain several advantages in an MITB attack:

- Most MITB attacks are distributed through Trojan browser extensions, which provide a valid function to the user but also install the MITB malware, making it difficult to recognize that malicious code has been installed.
- Because MITB malware selects websites to target, an infected MITB browser might remain dormant for months until triggered by the user visiting a targeted site.
- MITB software resides exclusively within the web browser, making it difficult for standard antimalware software to detect it.

Layer 2 Attacks

In 1978, the International Organization for Standardization (ISO) released a set of specifications to describe how dissimilar computers could be connected together on a network. The ISO demonstrated that what happens on a network device when sending or receiving traffic can be best understood by portraying this transfer as a series of related steps. The ISO called its work the *Open Systems Interconnection (OSI)* reference model. After a revision in 1983, the OSI reference model is still used today.

The key to the OSI reference model is *layers*. The model separates networking steps into a series of seven layers. Within each layer, different networking tasks are performed that cooperate with the tasks in the layers immediately above and below it. Each layer in the sending device corresponds to the same layer in the receiving device. The OSI model is shown in Figure 8-2.

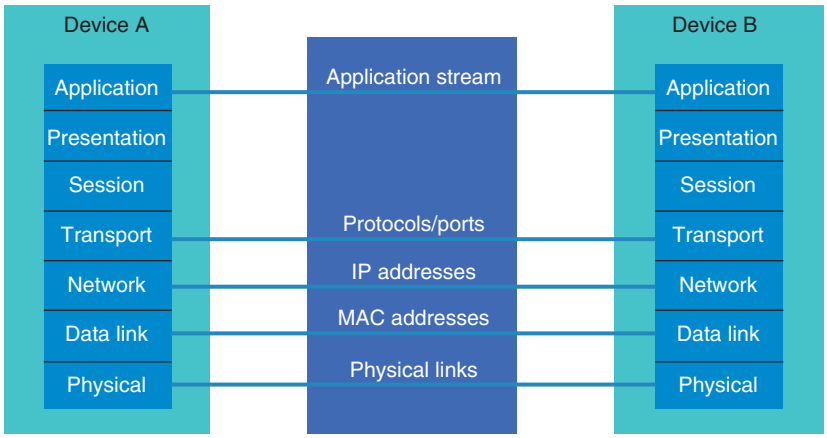


Figure 8-2 OSI model

However, the OSI model was designed so that each layer is compartmentalized: different layers work without the knowledge and approval of the other layers. This means that if one layer is compromised, the other layers are unaware of any problem, which results in the entire communication being compromised.

Layer 2 of the OSI model is particularly weak in this regard and is a frequent target of threat actors. Layer 2, the Data Link Layer, is responsible for dividing the data into packets along with error detection and correction, and performs physical addressing, data framing, and error detection and handling. A compromise at Layer 2 can affect the entire communication, as shown in Figure 8-3.

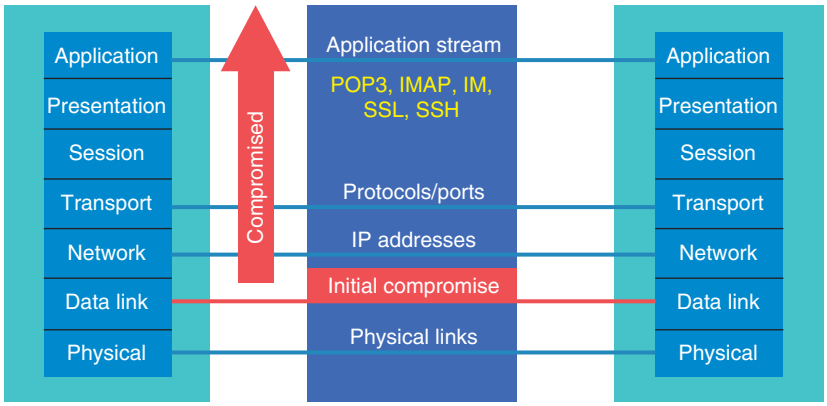


Figure 8-3 Layer 2 compromise

NOTE 2

There is not universal agreement on the usage of the terms *frame*, *packet*, *datagram*, and *segment*. The OSI uses the terms *protocol data unit (PDU)* and *service data unit (SDU)*. Usually, an Ethernet frame is used for Data Link Layer (Layer 2) functions, an IP packet or datagram is at the Network Layer (Layer 3), and a segment is at the Transport Layer (Layer 4). However, the terms are not used consistently. Although some network certification exams do require specific terminology when referring to these data units, the Security+ certification does not. To minimize confusion, the term *packet* is used in the text in a generic sense of a unit of data.

Two common Layer 2 attacks are address solution protocol poisoning and media access control attacks.

Address Resolution Protocol Poisoning

The TCP/IP protocol suite requires that logical Internet Protocol (IP) addresses be assigned to each device on a network. These addresses can be changed as necessary. However, an Ethernet LAN uses the physical media access control

(MAC) address that is permanently "burned" into a network interface card (NIC) to communicate. How can a physical MAC address be mapped to a logical and temporary IP address?

A device using TCP/IP on an Ethernet network can find the MAC address of another endpoint based on the IP address with the **Address Resolution Protocol (ARP)**. If the IP address for an endpoint is known, but the MAC address is not, the sending endpoint delivers an ARP packet to all devices on the network that in effect says, "If this is your IP address, send me your MAC address." The endpoint with that IP address sends back a packet with the MAC address so the packet can be correctly addressed. The IP address and the corresponding MAC address are stored in an ARP cache for future reference. In addition, all other endpoints that hear the ARP reply also cache that data.

Threat actors take advantage of a MAC address stored in a software ARP cache to change the data so that an IP address points to a different device. This attack is known as **ARP poisoning** and uses *spoofing*, which is deceiving by impersonating another's identity. Table 8-1 illustrates the ARP cache before and after an MITM attack using ARP poisoning. Notice that the IP address *192.146.118.4* in Victim 1's device and *192.146.118.3* in Victim 2's device now point to different MAC addresses, which would be to the threat actor's device.

Table 8-1 ARP poisoning attack

Device	IP and MAC address	ARP cache before attack	ARP cache after attack
Threat actor	192.146.118.2 00-AA-BB-CC-DD-02	192.146.118.3=>00-AA-BB-CC-DD-03 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.3=> 00-AA-BB-CC-DD-03 192.146.118.4=> 00-AA-BB-CC-DD-04
Victim 1	192.146.118.3 00-AA-BB-CC-DD-03	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.4=>00-AA-BB-CC-DD-04	192.146.118.2=> 00-AA-BB-CC-DD-02 192.146.118.4=> 00-AA-BB-CC-DD-02
Victim 2	192.146.118.4 00-AA-BB-CC-DD-04	192.146.118.2=>00-AA-BB-CC-DD-02 192.146.118.3=>00-AA-BB-CC-DD-03	192.146.118.2=> 00-AA-BB-CC-DD-02 192.146.118.3=> 00-AA-BB-CC-DD-02

NOTE 3

ARP poisoning is successful because no authentication procedures verify ARP requests and replies.

Media Access Control Attacks

Besides ARP poisoning, other attacks manipulate MAC addresses through spoofing. The target for these attacks is a network switch.

A network *switch* is a device that connects network devices and, unlike some other network devices, has a degree of "intelligence." Operating at the Layer 2 Data Link layer, a switch can learn which device is connected to each of its ports. It does so by examining the MAC address of packets it receives and observing at which of the switch's port that packet arrived. It associates the port with the MAC address of the device connected to the port, storing the information in a *MAC address table*. The switch then knows on which port to forward packets intended for that specific device.

NOTE 4

A switch not only improves network performance by limiting the number of packets distributed but also provides better security. A threat actor who installs software to capture packets on a computer attached to a switch sees only packets that are directed to that device and not those intended for any other network device.

Two common attacks involving spoofing MAC addresses on a switch are MAC cloning and MAC flooding.

MAC Cloning In a **MAC cloning attack**, threat actors discover a valid MAC address of a device connected to a switch. They spoof the MAC address on their device and send a packet onto the network. The switch changes its MAC address table to reflect the new association of the MAC address with the port to which the attackers' device is connected. All packets intended for the victim's device will now be sent to the attackers' device.

MAC Flooding A **MAC flooding attack** is another attack based on spoofing, MAC cloning, and the MAC address table of a switch. A threat actor overflows the switch with Ethernet packets that have been spoofed so that every packet contains a different source MAC address, each appearing to come from a different endpoint. This can quickly consume all the memory (called the *content addressable memory* or *CAM*) for the MAC address table.

Once the MAC address table is full and cannot store any additional MAC addresses, the switch enters a *fail-open* mode and broadcasts frames to all ports. A threat actor can then install software or a hardware device that captures and decodes packets on one client connected to the switch to view all traffic.

NOTE 5

A MAC flooding attack that consumes all the CAM on one switch will ultimately fill the CAM tables of adjacent switches.

DNS Attacks

The predecessor to today's Internet was the network ARPAnet. This network was completed in 1969 and used a 50 Kbps connection to link together single computers located at four sites (the University of California at Los Angeles, the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah). To reference the computers, each was assigned an identification number. (IP addresses were not introduced until later.) However, as computers were added to the network, it became more difficult for people to accurately recall the identification number of each computer.

The network needed a naming system that would assign computers both numeric addresses and friendlier human-readable names composed of letters, numbers, and special symbols (called a symbolic name). In the early 1970s, each computer site began to assign simple names to network devices and to manage its own *host table* that mapped names to computer numbers. However, because each site attempted to maintain its own local host table, inconsistencies developed between the sites. A standard master host table that could be downloaded to each site was then created. When TCP/IP was developed, the host table concept was expanded to a hierarchical name system for matching computer names and numbers known as the *Domain Name System (DNS)*, which is the basis for **domain name resolution** of names-to-IP addresses used today.

Because of the important role it plays, DNS is the focus of attacks. Like ARP poisoning, a DNS-based attack substitutes a DNS address so that the computer is silently redirected to a different device. A successful DNS attack has two consequences:

- *URL redirection*. The goal of DNS attacks is usually a **URL redirection**: instead of users reaching their intended site, they instead are redirected to another site. The site is often fictitious, one that looks identical to a bank or e-commerce site so that users enter their username, password, and credit card number. The threat actors at the fictitious site capture and use the confidential information.
- *Domain reputation*. Online algorithms are continually evaluating the reputation of webpages, domains, and email services. Consider email reputation: because every email message can be traced to an IP address, and IP addresses gain an IP reputation based on past incidents, an email service that has sent spam or unwanted bulk email earns a low reputation score. An email service might reject email messages with low reputation scores or deliver them more slowly than other email. Similar to an IP reputation, a **domain reputation** can identify a domain used for a distributing malware or launching attacks. A company's competitor could hire a threat actor to use a DNS attack that earns the company a low domain reputation score, thus affecting sales.

NOTE 6

On Labor Day in 1969, the first test of ARPAnet was conducted. A switch was turned on, and to almost everyone's surprise, the network worked. Researchers in Los Angeles attempted to type the word *login* on the computer hundreds of miles away at Stanford University. When a user in Los Angeles pressed the letter *L*, it appeared on the screen at Stanford. Next, the letter *O* was pressed, and it too appeared. However, when the third letter, *G*, was typed, the network crashed.

Attacks using DNS include DNS poisoning and DNS hijacking.

DNS Poisoning

Similar to ARP poisoning, **DNS poisoning** modifies a local lookup table on a device to point to a different domain. Usually, the alternative domain points to a malicious DNS server controlled by a threat actor. The DNS server redirects traffic to a website designed to steal user information or infect the device with malware.

DNS poisoning on the local device involves modifying the local host table. TCP/IP still uses host tables stored on the local device. When a user enters a symbolic name, TCP/IP first checks the local host table to find an entry; if no entry exists, it uses the external DNS system. Attackers can target a local HOSTS file to create new entries that redirect users to a fraudulent site. A sample local host table is shown in Figure 8-4.

```
127.0.0.1       localhost
161.6.18.20     www.wku.edu       # Western Kentucky University
74.125.47.99    www.google.com    # My favorite search engine
216.77.188.41   www.att.net       # Internet service provider
```

Figure 8-4 Sample HOSTS file

NOTE 7

Host tables are stored in the */etc/* directory in UNIX, Linux, and macOS, and they are located in the *Windows\System32\drivers\etc* directory in Windows.

In a DNS poisoning attack, the local HOSTS file contains an entry to a malicious DNS server. This allows the threat actor to control *all* websites that a user attempts to visit. In addition, since most users are unaware of the HOSTS file on their device, DNS poisoning infections can remain undetected for extended periods of time.

NOTE 8

Some governments use DNS poisoning to restrict their citizens from reading what they consider as unfavorable Internet content.

DNS Hijacking

Whereas DNS poisoning attempts to modify the local device HOSTS file, **DNS hijacking** is intended to infect an external DNS server with IP addresses that point to malicious sites. DNS hijacking has the advantage of redirecting *all* users accessing the server.

Instead of attempting to break into a DNS server to change its contents, attackers use a more basic approach. Because DNS servers exchange information among themselves (known as *zone transfers*), attackers attempt to exploit a protocol flaw and convince the authentic DNS server to accept fraudulent DNS entries sent from the attackers' DNS server. If the DNS server does not correctly validate DNS responses to ensure they have come from an authoritative source, it stores the fraudulent entries locally and serves them to users, spreading them to other DNS servers.

The steps in a DNS poisoning attack from attackers who have a domain name of *www.evil.net* with their own DNS server *ns.evil.net* are shown in Figure 8-5:

1. The attackers send a request to a valid DNS server asking it to resolve the name *www.evil.net*.
2. Because the valid DNS server does not know the address, it asks the responsible name server, which is the attackers' *ns.evil.net*, for the address.
3. The name server *ns.evil.net* sends the address of not only *www.evil.net* but also all of its records (a zone transfer) to the valid DNS server, which then accepts them.
4. Any requests to the valid DNS server will now respond with the fraudulent addresses entered by the attackers.

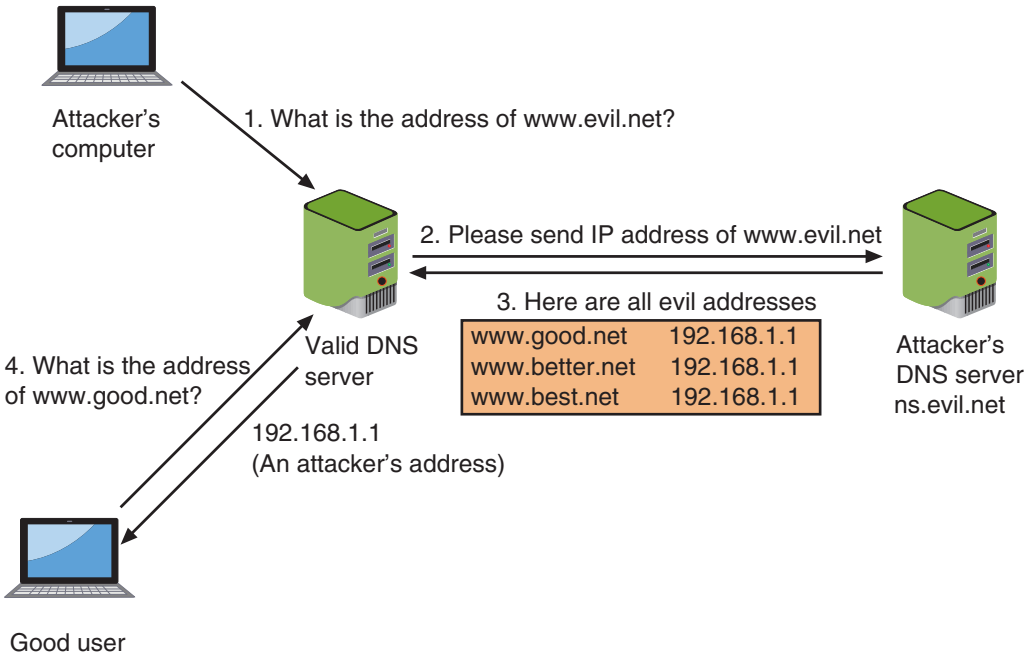


Figure 8-5 DNS server poisoning

NOTE 9

The advantage of a DNS poisoning attack is that all domains one victim uses can be controlled by a threat actor. In contrast, the advantage of a DNS hijacking attack is that although fewer domains are controlled, all users accessing the DNS server are redirected.

Distributed Denial of Service Attack

Suppose Gabe is having a conversation with Cora in a coffee shop when a "flash mob" of friends descends upon them and all talk to Gabe at the same time. He could not continue his conversation with Cora because he is overwhelmed by the number of people talking to him.

In a similar fashion, a technology-based *denial of service (DoS)* attack bombards a system with "bogus" requests, overwhelming the system so that it cannot respond to legitimate requests. DoS attacks today are **distributed denial of service (DDoS)** attacks: instead of only one source making a bogus request, a DDoS involves hundreds, thousands, or even millions of sources producing a torrent of fake requests.

The devices participating in a DDoS attack are infected and controlled by threat actors so that users are completely unaware that their endpoints are part of a DDoS attack. The sources used in DDoS attacks are listed in Table 8-2.

Table 8-2 Sources of DDoS attacks

Name	Source	Example	Target
Network	Computer	Desktop, laptop, tablet	Using Layer 3, it is designed to overwhelm web servers and networks
Application	IoT devices	Baby camera monitors, garage door openers	Focuses on cloud-based resources
Operational Technology (OT)	Endpoints that can be programmed and have an IP address	Automobiles, drones, robots	Using Layer 7, it targets infrastructures like an electrical power grid

NOTE 10

The volume of data directed at a target in a DDoS attack has continued to rise in recent years. The first massive DDoS attack occurred in 2016, when threat actors used 145,607 compromised IoT video cameras and digital video recorders (DVRs) against a French web hosting service, flooding it with 1.1 terabits per second (Tbps) of data. That record was eclipsed in 2018 with an attack of 1.7 Tbps, and again in early 2020, when a DDoS attack registered 2.3 Tbps. It is estimated that a botnet of only one million compromised IoT devices could easily send 4 Tbps in a DDoS attack, which is the equivalent of streaming 800,000 high-definition movies simultaneously.

Malicious Coding and Scripting Attacks

Several successful network attacks come from malicious software code and scripts. These attacks use PowerShell, Visual Basic for Applications, the coding language Python, and the Linux/UNIX Bash.

PowerShell

PowerShell is a task automation and configuration management framework from Microsoft. Initially, PowerShell was a Microsoft Windows component known as Windows PowerShell and was built on the Windows.NET framework (a developer platform that can be used to write apps in specific programming languages). In 2016, it was updated and released both as an open-source and a cross-platform product running on Windows, macOS, and Linux platforms.

Administrative tasks in PowerShell are performed by *cmdlets* ("command-lets"), which are specialized .NET classes that implement a specific operation. PowerShell *providers* give access to data in a data repository, such as the file system or Windows registry. Users and developers can create and add their own cmdlets to PowerShell. PowerShell also provides a hosting application program interface (API) so the PowerShell runtime can even be embedded inside other applications. On the Microsoft Windows platform, PowerShell has full access to a range of OS components and APIs. It can run locally on an endpoint or across a network accessing other endpoint devices.

The power and reach of PowerShell make it a prime target for threat actors. PowerShell allows attackers to inject code from the PowerShell environment into other processes without first storing any malicious code on the hard disk. Commands can then be executed while bypassing security protections and leave no evidence behind. PowerShell can also be configured so that its commands are not detected by antimalware running on the computer. Because most applications flag PowerShell as a "trusted" application, its actions are rarely scrutinized.

CAUTION

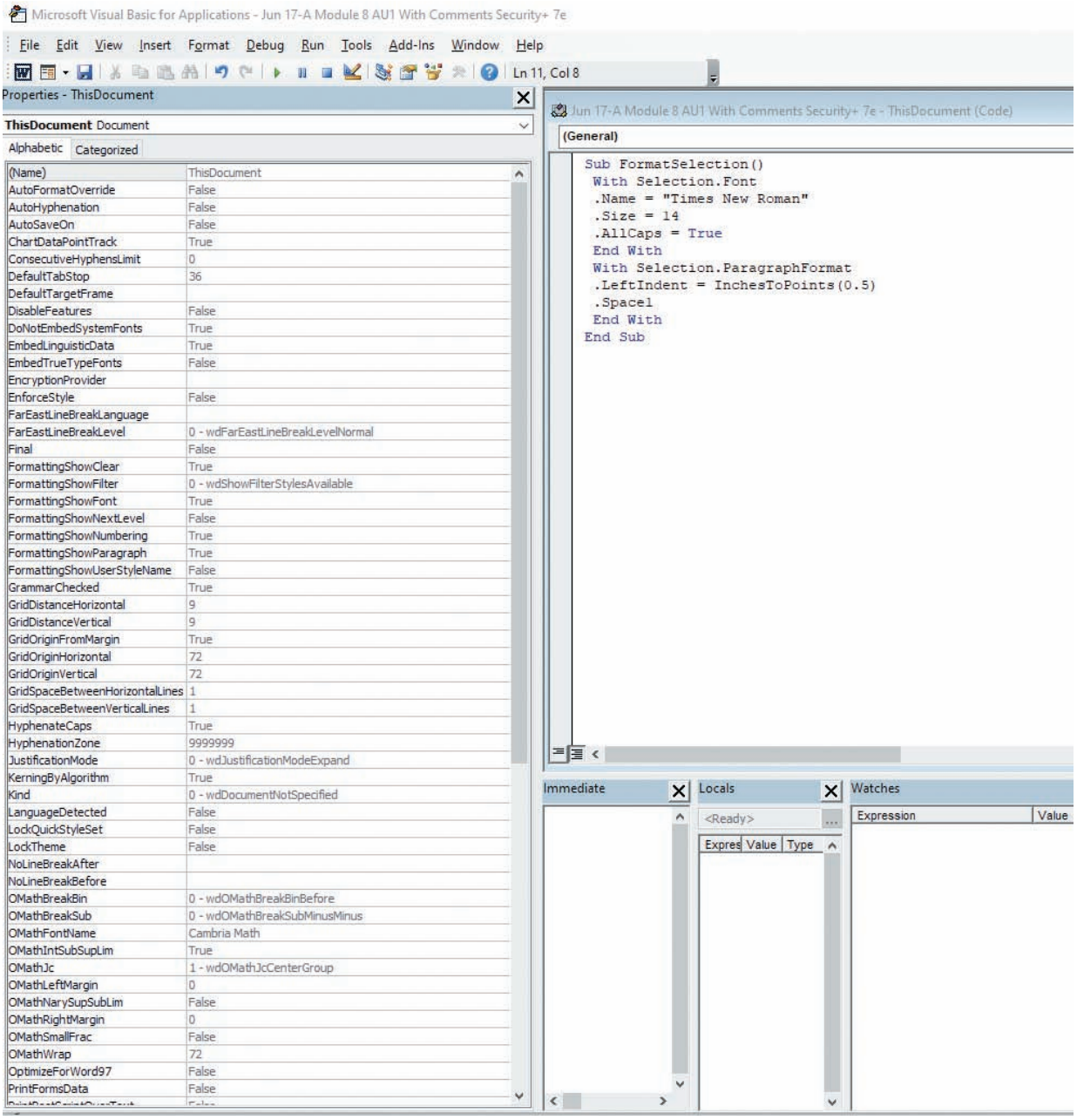
These are not vulnerabilities but rather are features of PowerShell as a result of its tight integration with the .NET Framework. PowerShell provides a powerful and easy means to access sensitive elements of an OS and is frequently used by developers and system administrators.

One recent attack illustrates how threat actors can use PowerShell. The attack started with a phishing email containing the subject line "URGENT!" and an Excel attachment with a malicious embedded script. Once the user opened the attachment and approved the script to run its active content, it decrypted and executed a PowerShell script. The script ran with the PowerShell parameters *ExecutionPolicyByPass* (allow the PowerShell script to run despite any system restrictions), *WindowStyleHidden* (run the script quietly without any notification to the user), and *NoProfile* (do not load the system's custom PowerShell environment).

Visual Basic for Applications (VBA)

Visual Basic for Applications (VBA) is an event-driven Microsoft programming language. VBA allows developers and users to automate processes that normally would take multiple steps or levels of steps. It can be used to control many tasks of the host application, including manipulating user interface features such as toolbars, menus, forms, and dialog boxes.

VBA is built into most Microsoft Office applications (Word, Excel, and PowerPoint, for example) for Windows and Apple macOS platforms. It is also included in select non-Microsoft products, such as AutoCAD, CorelDraw, and LibreOffice. VBA can even control one application from another application using Object Linking and Embedding (OLE) automation. For example, VBA can automatically create a Microsoft Word report from data in a Microsoft Excel spreadsheet. The VBA development environment is shown in Figure 8-6.



Used with permissions from Microsoft

Figure 8-6 VBA development environment

VBA is most often used to create **macros**. A macro is a series of instructions that can be grouped together as a single command. Macros are used to automate a complex task or a repeated series of tasks. Macros are generally written using VBA, are stored within the user document (such as in an Excel .xlsx worksheet or Word .docx file), and can be launched automatically when the document is opened.

Although macros date back to the late 1990s, they continue to be a key attack vector. Microsoft has reported that 98 percent of all Office-targeted threats are a result of macro-based malware, and it has warned users that Office macros, particularly in Excel, are still used to compromise Windows systems.[1] Due to the impact of macro malware, Microsoft has implemented several protections:

- *Protected View*. *Protected View* is a read-only mode for an Office file in which most editing functions are disabled and macros cannot run. When opened, files will display a Protected View warning message if they are from an Internet site, potentially unsafe location, or another user's OneDrive storage; received as an email attachment; or have active content (macros or data connections).

- *Trusted Documents*. A *trusted document* is a file that contains active content that can open without a warning. Users can access the Office Trust Center to designate files as trusted. However, files opened from an unsafe location cannot be designated as a trusted document. A system administrator can also turn off the ability to designate a trusted document.
- *Trusted Location*. Files retrieved from a *trusted location* can be designated as safe and open in standard rather than Protected View. It is recommended that if a user trusts a file that contains active content, it should be moved to a trusted location instead of changing the default Trust Center settings to allow macros.

CAUTION

Unless there is a business requirement for macros, support for their use should be disabled across the Microsoft Office suite. If macros are required, only those that have been digitally signed by a trusted publisher should be allowed to run. To prevent users or an adversary from bypassing macro security controls, all support for trusted documents and trusted locations should be disabled. Organizations can disable Trust Center settings and apply macro security controls using Group Policy settings.

Python

Python is a popular programming language that can run on several OS platforms. Python's syntax allows programmers to write code that takes fewer lines than in other programming languages such as Java and C++. Python also supports object-oriented programming. It has a large standard library in which developers can use routines created by other developers.

NOTE 11

Python was created in the late 1980s by a Dutch programmer as a side project during his Christmas vacation.

There are several best practices to follow when using Python so that the code does not contain vulnerabilities. These include using the latest version of Python, staying current on vulnerabilities within Python, being careful when formatting strings in Python, and downloading only vetted Python libraries. (A library is a collection of functions and methods that can perform actions so that the programmer does not have to write the code for it.)

Bash

Bash is the command language interpreter (called the "shell") for the Linux/UNIX OS. *Bash scripting* is using Bash to create a *script* (a script is essentially the same as a program, but it is *interpreted* and executed without the need for it to be first *compiled* into machine language). Exploits have taken advantage of vulnerabilities in Bash. For example, one vulnerability allowed attackers to remotely attach a malicious executable file to a *variable* (a value that changes) that is executed when Bash is invoked.

TWO RIGHTS & A WRONG

1. The goal of an MITM attack is to either eavesdrop on the conversation or impersonate one or both of the parties.
2. A session ID is a unique number that a web browser assigns for the duration of that user's visit.
3. In a MAC cloning attack, a threat actor will discover a valid MAC address of a device connected to a switch, spoof that MAC address on his device, and send a packet onto the network.

See Appendix B for the answer.

TOOLS FOR ASSESSMENT AND DEFENSE

CERTIFICATION

4.1 Given a scenario, use the appropriate tool to assess organizational security.

Several assessment tools determine the strength of a network. Other tools can be used to create a stronger network defense. Both types of tools can be categorized into network reconnaissance and discovery tools, Linux file manipulation tools, scripting tools, and packet capture and replay tools.

Network Reconnaissance and Discovery Tools

Some network reconnaissance and discovery tools are command-line utilities that are part of multiple OSs (sometimes with slight variations in their names or different switches or parameters), while others function under only a single OS. These tools are listed in Table 8-3.

Table 8-3 OS network reconnaissance and discovery tools

Name and OS	Description	Important switches or parameters
tracert (Windows) **traceroute** (Linux)	Shows the details about the path a packet takes from a computer or device to a destination	*-d* (Displays the route using numeric addresses and prevents tracert from resolving IP addresses to hostnames for a faster display) *-h hops* (Specifies the maximum number of hops while searching for the target)
nslookup (Windows) **dig** (Linux)	A DNS diagnostic utility; can be used in interactive mode but the non-interactive version of nslookup is easier and therefore is used more often	*host* (Look up the host using the default server) *host [server]* (Look up the host using the specified server) *-server* (Launch interactive mode using the server)
ipconfig (Windows) **ifconfig** (Linux)	Displays network configuration information such as the IP address, network mask, and gateway for all physical and virtual network adapters	*-all* (Displays detailed configuration information about all network interfaces) *-release [adapter]* (Terminates the DHCP lease on the specified adapter or on all interfaces) *-displaydns* (Displays the contents of the DNS resolver cache)
ping (Windows, Linux)	Tests the ability of the source computer to reach a specified destination computer; commonly used to verify that a computer can communicate over a network with another computer or network device	*-t* (Force the target to respond until pressing Ctrl+C) *-a* (Resolve the hostname of an IP address target) *-i TTL* (Set the Time to Live (TTL) value up to 255) *-R* (Trace the round-trip path) *-r count* (Specify number of hops between computer and the target computer)
netstat (Windows, Linux)	Provides detailed information about current network connections as well as network connections for the Transmission Control Protocol (TCP), network interfaces, and routing tables	*-a* (All active connections and the ports that the computer is listening on) *-e* (Ethernet data such as number of bytes and packets sent and received) *-g* (Multicast group membership data) *-n* (Active TCP connections with addresses and port numbers displayed numerically)
pathping (Windows)	A combination of ping and tracert that will test the connection to each hop.	*-q* (Limit number of queries) *-n* (Prevents resolving hostnames)
route (Linux)	Displays and manipulates IP routing table to create static routes to specific hosts	*-n* (Display numerical addresses) *gw gateway* (Route packets via gateway)
curl (Linux)	Transfers data to or from a server	*-o filename* (Save downloaded file with filename) *-C* – (Resume interrupted download)
hping (Linux)	Sends custom TCP/IP packets	*-i interval* (Wait *interval* seconds between sending packets)

Network reconnaissance and discovery tools from third parties are listed in Table 8-4.

Table 8-4 Third-party OS network reconnaissance and discovery tools

Name	Source	Description
theHarvester	Kali Linux	Provides information about email accounts, user names, and hostnames/subdomains from different public sources
dnsenum	Kali Linux	List DNS information of a domain
sn1per	XeroSecurity	Penetration testing tool
Cuckoo	Cuckoo	Automated malware analysis system
Nessus	Tenable	Vulnerability assessment tool
scanless	Vesche	Tool for using websites to perform port scan
nmap	Nmap	Network discovery and security auditing

Linux File Manipulation Tools

Text files are a fundamental element in the Linux OS. Because virtually all configuration files in Linux are text files, changing the configuration of a security application involves modifying the text configuration file. Thus, managing Linux security, applications, and the OS itself demands excellent text manipulation skills. Table 8-5 lists several Linux text file manipulation tools that are part of the Linux OS.

Table 8-5 Linux text file manipulation tools

Tool name	Description	Example
head	Display the first 10 lines of a file	*head etc/snort/snort.conf*
tail	Display the last 10 lines of a file	*tail etc/snort/snort.conf*
cat	Display an entire file	*cat etc/snort/snort.conf*
grep	Search for keyword	*grep apache1*
chmod	Change file permissions	*chmod 774 rules*
logger	Add content to syslog file	*logger comment*

Scripting Tools

Scripting tools are used to create scripts that facilitate tasks. PowerShell is one of the most powerful scripting tools, and Python can also be used to create scripts. Scripts can also be created when using Secure Shell (SSH), which is used to access remote computers.

NOTE 12

SSH is covered in Module 7.

Another tool that supports scripting is **OpenSSL**, a cryptography library that offers open source applications of the TLS protocol. It was first released in 1998 and is available for Linux, Windows, and macOS platforms. OpenSSL allows users to perform various SSL-related tasks, including CSR (Certificate Signing Request), private key generation, and SSL certificate installation.

Packet Capture and Replay Tools

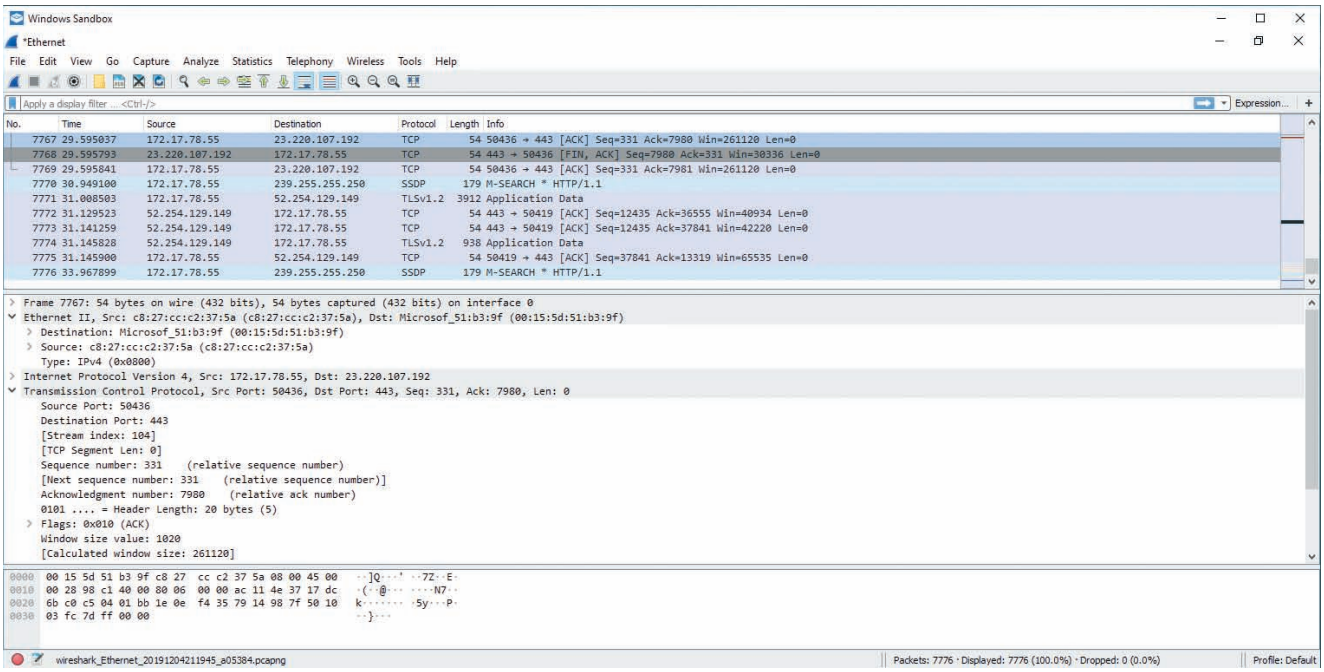
Collecting and analyzing data packets that cross a network can provide valuable information. Packet analysis typically examines the entire contents of the packet, which consists of the header information and the payload. However, because all the information needed is rarely contained in a single packet, packet analysis examines multiple packets—often hundreds and even thousands of them— to piece together the information.

NOTE 13

Some common uses of packet analysis include troubleshooting network connectivity (determine packet loss, review TCP retransmission, and create graphs of high latency packet responses), examining Application Layer sessions (captured packets can be used to view a full HTTP session for both requests and responses, view Telnet session commands and responses, and even read email traffic), and solving DHCP issues (examine DHCP client broadcasts, view DHCP offers with addresses and options, observe client requests for an address, and see the server's acknowledgment of the request).

Packet analysis can also be used extensively for security. It can detect unusual behavior (such as a high number of DNS responses) that could indicate the presence of malware, search for unusual domains or IP address endpoints, and discover regular connections (beacons) to a threat actor's command and control (C&C) server.

Wireshark is a popular GUI packet capture and analysis tool and is shown in Figure 8-7. **Tcpdump** is a command-line packet analyzer. It displays TCP/IP packets and other packets being transmitted or received over a network. It runs on UNIX and Linux operating systems, and various forks of it are available for Windows computers. However, the output from Tcpdump can be voluminous and difficult to parse. **Tcpreplay** is a tool for editing packets and then "replaying" the packets back onto the network to observe their behavior.



Wireshark Software

Figure 8-7 Wireshark packet capture and analysis tool

NOTE 14

Several switches are available for Tcpdump. A complete list of Tcpdump switches is available at *www.tcpdump.org/manpages/tcpdump.1.html.*

TWO RIGHTS & A WRONG

1. The tools tracert (Windows) and traceroute (Linux) show the details about the path a packet takes from a computer or device to a destination.
2. Nessus is from Kali Linux.
3. The Linux text file manipulation tool logger adds content to the syslog file.

See Appendix B for the answer.

PHYSICAL SECURITY CONTROLS

CERTIFICATION

2.7 Explain the importance of physical security controls.

An obvious but often-overlooked consideration when defending a network is physical security: preventing a threat actor from physically accessing the network is as important as preventing the attacker from accessing it remotely. Physical security controls include external perimeter defenses, internal physical security controls, and computer hardware security.

External Perimeter Defenses

Some organizations use **industrial camouflage** in an attempt to make the physical presence of a building as nondescript as possible so that to a casual viewer, the building does not look like it houses anything important. When camouflage is not possible, external perimeter defenses must be used. External perimeter defenses are designed to restrict access to the areas in which equipment is located. This type of defense includes barriers, personnel, and sensors.

Barriers

Different types of passive barriers can restrict people or vehicles from entering a secure area. **Fencing** is usually a tall, permanent structure to keep out unauthorized personnel. It is usually accompanied by **signage** that explains the area is restricted and proper **lighting** so the area can be viewed after dark. However, standard chain link fencing offers limited security because it can easily be circumvented by climbing over it or cutting the links. Most modern perimeter security consists of a fence equipped with other deterrents such as those listed in Table 8-6.

Table 8-6 Fencing deterrents

Technology	Description	Comments
Anticlimb paint	A nontoxic petroleum gel-based paint that is thickly applied and does not harden, making any coated surface very difficult to climb.	Typically used on poles, downpipes, wall tops, and railings above head height (8 feet or 2.4 meters).
Anticlimb collar	Spiked collar that extends horizontally for up to 3 feet (1 meter) from the pole to prevent anyone from climbing it; serves as both a practical and visual deterrent.	Used for protecting equipment mounted on poles like cameras or in areas where climbing a pole can be an easy point of access over a security fence.
Roller barrier	Independently rotating large cups (diameter of 5 inches or 115 millimeters) affixed to the top of a fence prevents the hands of intruders from gripping the top of a fence to climb over it.	Often found around public grounds and schools where a nonaggressive barrier is important.
Rotating spikes	Installed at the top of walls, gates, or fences; the tri-wing spike collars rotate around a central spindle.	Designed for high-security areas; can be painted to blend into fencing.

Like fencing, a **barricade** is generally designed to block the passage of traffic. However, barricades are most often used for directing large crowds and are generally not designed to keep out individuals. This is because barricades are usually not as tall as fences and can easily be circumvented by climbing over them. A **bollard** is a short but sturdy

vertical post that is used as a vehicular traffic barricade to prevent a car from ramming into a secured area. A pair of bollards is pictured in Figure 8-8.

MartineDF/Shutterstock.com

Figure 8-8 Bollards

Personnel

Whereas barriers act as passive devices to restrict access, personnel are considered active security elements. Unlike passive devices, personnel can differentiate between an intruder and someone looking for a lost pet and then decide when it is necessary to take appropriate action.

Human **security guards** who patrol and monitor restricted areas are most often used as an active security defense. In settings that require a higher level of protection, two security guards may be required. This prevents one security guard who has been compromised (through bribery, threats, or other coercion) from participating in an attack, such as allowing malicious actors entrance through a locked door. Using two security guards is called **two-person integrity/control**.

NOTE 15

Most of the major heists involving the theft of large amounts of cash or precious jewels have been the result of an inside employee of a bank, airport warehouse, or other facility participating in the theft.

Some guards are responsible for monitoring activity captured by video surveillance cameras that transmit a signal to a specific and limited set of receivers called **closed circuit television (CCTV)**. Some CCTV cameras are fixed in a single position pointed at a door or a hallway, while other cameras resemble a small dome and allow guards to move the camera 360 degrees for a full panoramic view. High-end video surveillance cameras only record when they detect movement (**motion recognition**), while others can identify a suspicious object such as a backpack left in a chair and sound an alert (**object detection**). Increasingly, drones, also called unmanned aerial vehicles (UAVs), include cameras for monitoring activity.

NOTE 16

When guards actively monitor a CCTV, it is a preventive measure: any unauthorized activity seen on video surveillance results in the guard taking immediate action by going to the scene or calling for assistance. When a guard does not actively monitor a CCTV, the video is recorded and, if a security event occurs, the recording is examined later to identify the culprit.

Robot sentries that patrol and use CCTV with object detection are increasingly being used in public areas. Figure 8-9 shows a robot sentry. Armed robberies, burglaries, and hit-and-run incidents have been solved by data recorded by a robot sentry.

Sundry Photography/Shutterstock.com

Figure 8-9 Robot sentry

A **receptionist** who staffs a public reception area can also provide a level of active security. Public reception areas are an often-overlooked risk: once visitors are in the reception area, they are already inside the facility beyond external barriers. The receptionist's duty should be to observe and interact appropriately with the public so that potential malicious actors feel they are always being observed. This means receptionists should not have additional clerical duties beyond maintaining a **visitor log** or record (either paper or electronic) of those individuals granted access; otherwise, the receptionists will be distracted from their primary duty.

NOTE 17

Other precautions that should be taken in a public reception area include anchoring furnishings and wall hangings so they cannot be picked up and thrown or used as weapons. The reception room should not be used for mail deliveries, as an employee entrance, or a designated escape route. Receptionists should be able to observe visitors before they enter the reception room and electrically lock out suspicious persons. Receptionists should not be expected to physically intercept or impede a real or perceived attacker but, instead, call for help.

Sensors

With human personnel, an incident may occur during a lapse of attention by a security guard. To supplement the work of security guards, **sensors** can be placed in strategic locations to alert guards by generating an audible **alarm** of an unexpected or unusual action. Table 8-7 lists different types of sensors.

Table 8-7 Sensors

Name	Usage	Description
Motion detection	Can determine an object's change in position in relation to its surroundings.	Passive and active infrared light sensors; can be accurately placed by using sensor cards that can safely locate optical beams invisible to human eye.
Noise detection	Can detect a suspicious noise.	Microphones that turn on when the sensor is using noise-activated technology.
Temperature detection	Will detect a sudden increase or decrease in temperature or the temperature of an object in relation to its surroundings.	A thermal camera can be used to determine if a person is lurking in a dark room.
Moisture detection	Can detect water leaks, dampness, or increased moisture levels.	Often used to detect location of a leak from a water pipe.
Proximity	A sensor that detects the presence of an object ("target") when the target enters the sensor's field.	Depending on the type of proximity sensor, sound, light, infrared radiation (IR), or electromagnetic fields may be utilized by the sensor to detect a target.

Internal Physical Security Controls

External perimeter defenses are designed to keep an intruder from entering a campus, building, or other area. If unauthorized personnel defeat external perimeter defenses, they should next face internal physical access security, such as locks, secure areas, and protected cable distribution. In addition, fire suppression is considered an internal physical control.

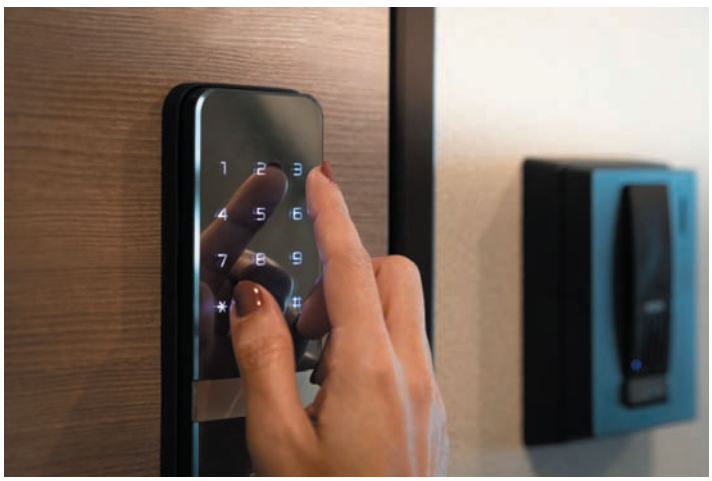
Locks

A variety of locks can restrict access. **Physical locks** that require a key or other device to open doors or cabinets are the most common types of physical locks.

NOTE 18

The categories of commercial door locks include storeroom (the outside is always locked, entry is by key only, and the inside lever is always unlocked), classroom (the outside can be locked or unlocked, and the inside lever is always unlocked), store entry double cylinder (includes a keyed cylinder in both the outside and inside knobs so that a key in either knob locks or unlocks both at the same time), and communicating double cylinder lock (includes a keyed cylinder in both outside and inside knobs, and the key unlocks its own knob independently).

However, physical locks that use keys can be compromised if the keys are lost, stolen, or duplicated. Keys distributed to multiple users to access a single locked door increases the risk of a key being compromised. A more secure option is to use an **electronic lock**, as shown in Figure 8-10. Electronic locks use buttons that must be pushed in the proper sequence to open the door. An electronic lock can also be programmed to maintain a record of when the door was opened and by which code and to allow someone's code to be valid only at specific times. Growing in popularity are *smart locks* that use a smartphone that sends a code via wireless Bluetooth to open the door, and *fingerprint locks* that have a pad that scans a user's fingerprint.



myboys.me/Shutterstock.com

Figure 8-10 Electronic lock

A problem with an electronic lock is that someone can watch a user enter the code on a physical keypad by shoulder surfing or even detect fingerprint "smudges" on keys to uncover the code. One brand of electronic lock mitigates this weakness by using a virtual screen that substitutes physical buttons with four circles. Each circle displays the numbers associated with that circle (for example, Circle A may display the digits 1, 2, and 3, while Circle B displays the digits 4, 5, and 6) and the digits are randomly assigned to different circles: Circle A now may be 4, 7, and 0 while later it is 2, 5, and 9. This prevents a shoulder surfer from pressing the same circles to unlock the door.

Secure Areas

In a combat area, a **demilitarized zone (DMZ)** separates two warring nations. In cybersecurity, a DMZ is likewise an area that separates threat actors from defenders (also called a physical **air gap**). Enterprises often have DMZs or **secure areas** in a building or office to separate the secure facilities from unknown and potentially hostile outsiders.

Before electronic security was available, vestibules with two locked doors controlled access to sensitive areas. Individuals would give their credentials to a security officer, who opened the first door to a small room (a vestibule) and asked the individuals to enter and wait while their credentials (usually a **badge** or other token that indicates they have been approved) were checked. If the credentials were approved, the second door would be unlocked; if the credentials were fraudulent, the person would be trapped in the vestibule (a *mantrap*).

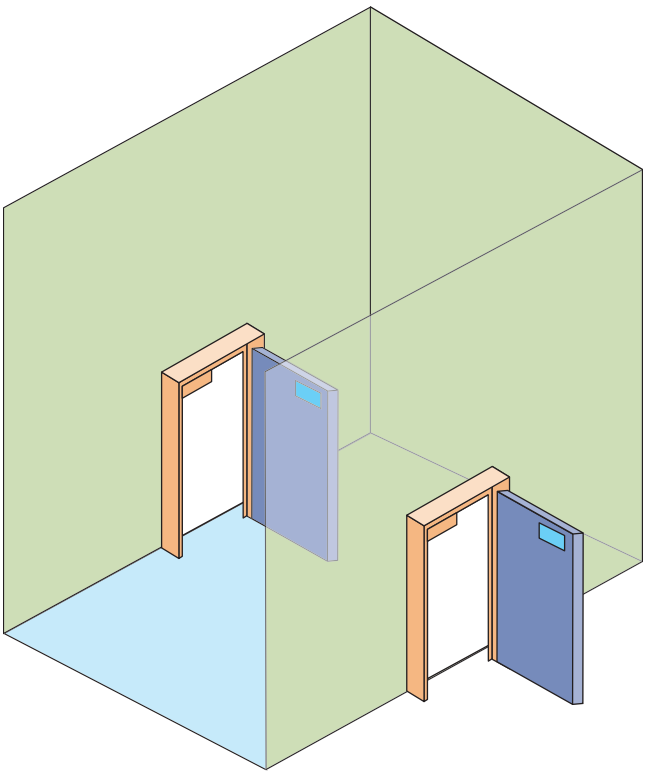
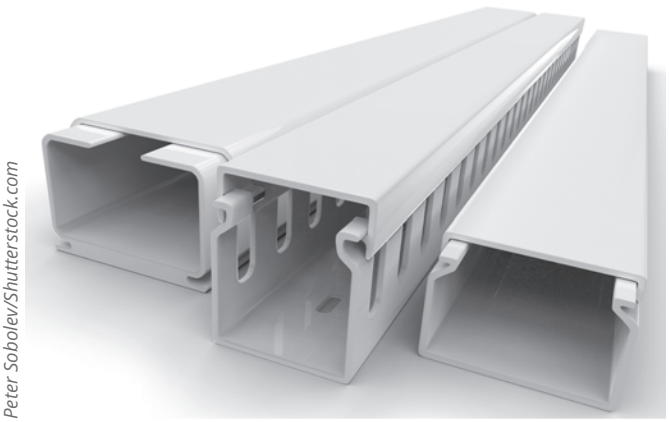


Figure 8-11 Mantrap

A modern **mantrap** is designed as an air gap to separate a nonsecure area from a secured area. A mantrap device monitors and controls two interlocking doors to a vestibule, as shown in Figure 8-11. When in operation, only one door can be open at any time. Creating a physical air gap, or the absence of any type of connection between the areas, can improve security. Mantraps are used in high-security areas where only authorized persons can enter, such as cash-handling areas and research laboratories.

Another area that must be secured is the *data center* that houses the on-prem network, server, and storage equipment. Because network equipment and servers in a data center generate large amounts of heat, a **hot aisle/cold aisle** layout can reduce the heat by managing air flow. In a data center using a hot aisle/cold aisle layout, the server racks are arranged in alternating rows, with cold air intakes facing one direction and hot air exhausts facing the other direction. The rows composed of the rack fronts are the cold aisles and face air conditioner output ducts. The rows with the backs of the racks where the heated exhausts exit are the hot aisles and generally face the air conditioner return ducts.



Peter Sobolev/Shutterstock.com

Figure 8-12 Cable conduits

Protected Cable Distribution

Cable conduits are hollow tubes that carry copper wire or fiber-optic cables, as shown in Figure 8-12. A **protected cable distribution** is a system of cable conduits used to protect classified information that is being transmitted between two secure areas. PDS is a standard created by the U.S. Department of Defense (DOD).

Two types of PDS are commonly used. In a *hardened carrier PDS*, the data cables are installed in a conduit constructed of special electrical metallic tubing or similar

material. All the connections between segments are permanently sealed with welds or special sealants. If the hardened carrier PDS is buried underground, such as running between buildings, the carrier containing the cables must be encased in concrete, and any manhole covers that give access to the PDS must be locked down. A hardened carrier PDS must be visually inspected on a regular basis.

An alternative to a hardened carrier PDS is an *alarmed carrier PDS*. In this type of PDS, the carrier system is deployed with specialized optical fibers in the conduit that can sense acoustic vibrations that occur when an intruder attempts to gain access to the cables, which triggers an alarm. The advantages of an alarmed carrier PDS are that it provides continuous monitoring, eliminates the need for periodic visual inspections, allows the carrier to be hidden above the ceiling or below the floor, and eliminates the need for welding or sealing connections.

Fire Suppression

Damage inflicted as a result of a fire is a constant threat to persons as well as property. **Fire suppression** includes the attempts to reduce the impact of a fire.

In a data center that contains electronic equipment, using water or a handheld fire extinguisher is not recommended because it can contaminate the equipment. Instead, stationary fire suppression systems are integrated into the building's infrastructure and release fire suppressant. The systems can be classified as dry chemical systems that disperse a fine, dry powder over the fire or clean agent systems that do not harm people, documents, or electrical equipment in the room. Clean agents can extinguish a fire by reducing heat, removing or isolating oxygen, or inhibiting the chemical reaction.

NOTE 19

For a fire to occur, four entities must be present at the same time: a type of *fuel* or combustible material, sufficient *oxygen* to sustain the combustion, enough *heat* to raise the material to its ignition temperature, and a chemical *reaction* that is the fire itself. The first three factors form a fire triangle; to extinguish a fire, any one of these elements must be removed.

Computer Hardware Security

Computer hardware security is the physical security that specifically involves protecting endpoint hardware, such as laptops that can easily be stolen. Most portable devices (as well as many expensive computer monitors) have a special steel bracket security slot built into the case. A **cable lock** can be inserted into the security slot of a portable device and rotated so that the cable lock is secured to the device, as illustrated in Figure 8-13. The cable can then be connected to an immovable object.

O.Bellini/Shutterstock.com

Figure 8-13 Cable lock

For storage, a laptop can be placed in a **safe** or a **vault**, which is a ruggedized steel box with a lock. Some offices have safes in employee cubicles for the users to lock up important papers when away from their desks, even for a short period of time. The sizes typically range from small (to accommodate one laptop) to large (for multiple devices). Safes and cabinets also can be prewired for electrical power as well as wired network connections. This allows the laptops stored in the locking cabinet to charge their batteries and receive software updates while not in use.

Computer systems, printers, and similar digital electronic devices emit electromagnetic fields, which can result in interference, called *electromagnetic interference (EMI)*. Electromagnetic spying, or picking up electromagnetic fields and reading the data that is producing them, is a risk.

NOTE 20

In mid-2020, researchers revealed a new technique for long-distance eavesdropping they call "lamphone." Anyone with a computer, telescope, and a $400 electrooptical sensor can listen to any sounds in a room hundreds of feet away in real time simply by observing the minuscule vibrations those sounds create on the glass surface of a light bulb inside the room. By measuring the tiny changes in light output from the bulb that those vibrations cause, the researchers show that a spy can pick up sound clearly enough to discern the contents of conversations or even recognize a piece of music.

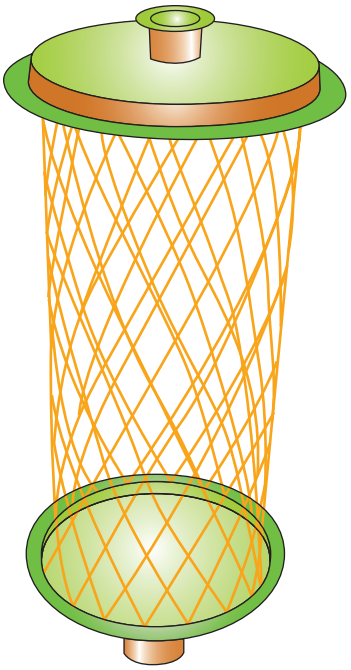


Figure 8-14 Faraday cage

One means of protecting against EMI is a **Faraday cage**, a metallic enclosure that prevents the entry or escape of an electromagnetic field. A Faraday cage, consisting of a grounded, fine-mesh copper screening, as shown in Figure 8-14, is often used for testing in electronic labs. In addition, lightweight and portable *Faraday bags* made of special materials can shield cell phones and portable computing devices such as tablets and notebook computers. Faraday bags are often used in crime scene investigations. Phones, tablets, or laptops found on scene are placed in Faraday bags, thus eliminating inbound and outbound signals and preventing the devices from being remotely wiped of evidence.

TWO RIGHTS & A WRONG

1. A barricade is a short but sturdy vertical post that is used as a vehicular traffic barricade to prevent a car from ramming into a secured area.
2. An electronic lock is a combination lock that uses buttons that must be pushed in the proper sequence to open the door.
3. A DMZ is also called a physical air gap.

See Appendix B for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in the Practice It folder in each MindTap module.

SUMMARY

- Some attacks are designed to intercept network communications. A man-in-the-middle (MITM) attack intercepts legitimate communication and forges a fictitious response to the sender or eavesdrops on the conversation. A session replay attack intercepts and uses a session ID to impersonate a user. A man-in-the-browser (MITB) attack occurs between a browser and the underlying computer. An MITB attack seeks to intercept and then manipulate the communication between the web browser and the security mechanisms of the computer.
- Layer 2 of the OSI model is particularly weak and is a frequent target of threat actors. ARP poisoning changes the ARP cache so the corresponding IP address is pointing to a different computer. In a MAC cloning attack, threat actors will discover a valid MAC address of a device connected to a switch and then spoof that MAC address on their device and send a packet onto the network. The switch will change its MAC address table to reflect this new association of that MAC address with the port to which the attackers' device is connected. In a MAC flooding attack, threat actors will overflow the switch with Ethernet packets that have been spoofed so that every packet contains a different source MAC address, each appearing to come from a different endpoint. This can quickly consume all the memory for the MAC address table and will enter a fail-open mode and function like a network hub, broadcasting frames to all ports. Threat actors could then install software or a hardware device that captures and decodes packets on one client connected to the switch to view all traffic.
- DNS poisoning modifies a local lookup table on a device to point to a different domain, which is usually a malicious DNS server controlled by a threat actor that will redirect traffic to a website designed to steal user information or infect the device with malware. DNS hijacking is intended to infect an external DNS server with IP addresses that point to malicious sites. A distributed denial of service (DDoS) attack involves a device being overwhelmed by a torrent of fake requests so that it cannot respond to legitimate requests for service.

- Several successful network attacks come from malicious software code and scripts. PowerShell is a task automation and configuration management framework from Microsoft. The power and reach of PowerShell make it a prime target for threat actors who use it to inject malware. Visual Basic for Applications (VBA) is an "event-driven" Microsoft programming language that is used to automate processes that normally would take multiple steps or levels of steps. VBA is most often used to create macros. A macro is a series of instructions that can be grouped together as a single command. Macros are still used to distribute malware. Python is a popular programming language that can run on several different OS platforms. There are several "best practices" to follow when using Python so that the code does not contain vulnerabilities. Bash is the command language interpreter (called the "shell") for the Linux/UNIX OS. Bash scripting is using Bash to create a script (a script is essentially the same as a program, but it is interpreted and executed without the need for it to be first compiled into machine language). Exploits have taken advantage of vulnerabilities in Bash.
- There are several different assessment tools for determining the strength of a network. Text files are a fundamental element when using the Linux OS. Because virtually all configuration files in Linux are text files, changing the configuration of a security application involves modifying the text configuration file. Thus, being able to manipulate text is an important skill in managing Linux security, as well as other applications and even the OS itself. There are a variety of different tools that can be used to create scripts that facilitate tasks. One tool that supports scripting is OpenSSL, a cryptography library that offers open source applications of the TLS protocol.
- Collecting and analyzing data packets that cross a network can provide a wealth of valuable information. Packet analysis can also be used extensively for security. Wireshark is a popular GUI packet capture and analysis tool. Tcpdump is a command-line packet analyzer. Tcpreplay is a tool for editing packets and then "replaying" the packets back onto the network to observe their behavior.
- An often-overlooked consideration when defending a network is physical security: preventing a threat actor from physically accessing the network is as important as preventing the attacker from accessing it remotely. External perimeter defenses are designed to restrict access to the areas in which equipment is located. Fencing is usually a tall, permanent structure to keep out unauthorized personnel. It is usually accompanied by signage that explains the area is restricted and proper lighting so the area can be viewed after dark. A barricade is generally designed to block the passage of traffic. A bollard is a short but sturdy vertical post that is used to as a vehicular traffic barricade to prevent a car from ramming into a secured area.
- While barriers act as passive devices to restrict access, personnel are considered active security elements. Human security guards who patrol and monitor restricted areas are most often used as an active security defense. Using two security guards is called two-person integrity/control. Some guards are responsible for monitoring activity captured by video surveillance cameras that transmit a signal to a specific and limited set of receivers called closed circuit television (CCTV). High-end video surveillance cameras only record when they detect movement (motion recognition) while others can identify a suspicious objective and sound an alert. Increasingly, drones/unmanned aerial vehicles (UAV) with cameras are also being used for monitoring activity. Robot sentries that patrol and use CCTV with object detection are increasingly being used in public areas. A receptionist who staffs a public reception area can also provide a level of active security. To supplement the work of security guards, sensors can be placed in strategic locations to alert guards by generating an audible alarm of an unexpected or unusual action.
- In the event that unauthorized personnel defeat external perimeter defenses, they should then face internal physical access security. A variety of types of locks can be used to restrict access. Physical locks that require a key or other device to open doors or cabinets are the most common types of physical locks. However, physical locks that use keys can be compromised if the keys are lost, stolen, or duplicated. A more secure option is to use an electronic lock. These locks use buttons that must be pushed in the proper sequence to open the door.
- A demilitarized zone (DMZ) is an area that separates threat actors from defenders (also called a physical air gap). A mantrap is designed as an air gap to separate a nonsecure area from a secured area. A mantrap device monitors and controls two interlocking doors to a vestibule. A protected cable distribution is a system of cable conduits used to protect classified information that is being transmitted between two secure areas. Damage inflicted as a result of a fire is a constant threat to persons as well as property. Fire suppression includes the attempts to reduce the impact of a fire. In a data center that contains electronic equipment, using a handheld fire extinguisher is not recommended because the chemical contents can contaminate the equipment. Instead, stationary fire suppression systems are integrated into the building's infrastructure and release fire suppressant in the room.

- A cable lock can be inserted into the security slot of a portable device and rotated so that the cable lock is secured to the device. When storing a laptop, it can be placed in a safe or a vault, which is a ruggedized steel box with a lock. Some offices have safes in employee cubicles for the users to lock up important papers when away from their desks, even for a short period of time. A Faraday cage is a metallic enclosure that prevents the entry or escape of an electromagnetic field.

Key Terms

Address Resolution Protocol (ARP)
air gap
alarm
ARP poisoning
badge
barricade
Bash
bollard
cable lock
cat
chmod
closed circuit television (CCTV)
Cuckoo
curl
demilitarized zone (DMZ)
dig
distributed denial of service (DDoS)
DNS hijacking
DNS poisoning
dnsenum
domain name resolution
domain reputation
electronic lock
Faraday cage
fencing
fire suppression
grep
head
hot aisle/cold aisle
hping
ifconfig
industrial camouflage
ipconfig
lighting
logger
MAC cloning attack
MAC flooding attack
macro
man-in-the-browser (MITB)
man-in-the-middle (MITM)
mantrap
moisture detection
motion detection
motion recognition
Nessus
netstat
nmap
noise detection
nslookup
object detection
OpenSSL
Operational Technology (OT)
pathping
physical locks
ping
PowerShell
protected cable distribution
proximity
Python
receptionist
robot sentries
route
safe
scanless
secure areas
security guards
sensors
session replay
signage
sn1per
tail
Tcpdump
Tcpreplay
temperature detection
theHarvester
traceroute
tracert
two-person integrity/control
URL redirection
vault
visitor log
Visual Basic for Applications (VBA)
Wireshark

Review Questions

1. Which attack intercepts communications between a web browser and the underlying OS?
   a. Interception
   b. Man-in-the-browser (MITB)
   c. DIG
   d. ARP poisoning

2. Calix was asked to protect a system from a potential attack on DNS. What are the locations he would need to protect?
   a. Web server buffer and host DNS server
   b. Reply referrer and domain buffer
   c. Web browser and browser add-on
   d. Host table and external DNS server

3. What is the result of an ARP poisoning attack?
   a. The ARP cache is compromised.
   b. Users cannot reach a DNS server.
   c. MAC addresses are altered.
   d. An internal DNS must be used instead of an external DNS.

4. Deacon has observed that the switch is broadcasting all packets to all devices. He suspects

it is the result of an attack that has overflowed the switch MAC address table. Which type of attack is this?
- **a.** MAC spoofing attack
- **b.** MAC cloning attack
- **c.** MAC flooding attack
- **d.** MAC overflow attack

5. Tomaso is explaining to a colleague the different types of DNS attacks. Which DNS attack would only impact a single user?
- **a.** DNS hijack attack
- **b.** DNS poisoning attack
- **c.** DNS overflow attack
- **d.** DNS resource attack

6. Proteus has been asked to secure endpoints that can be programmed and have an IP address so that they cannot be used in a DDoS attack. What is the name for this source of DDoS attack?
- **a.** Network
- **b.** Application
- **c.** IoT
- **d.** Operational Technology

7. Which of the following is NOT a reason that threat actors use PowerShell for attacks?
- **a.** It cannot be detected by antimalware running on the computer.
- **b.** It leaves behind no evidence on a hard drive.
- **c.** It can be invoked prior to system boot.
- **d.** Most applications flag it as a trusted application.

8. What is the difference between a DoS and a DDoS attack?
- **a.** DoS attacks are faster than DDoS attacks.
- **b.** DoS attacks use fewer computers than DDoS attacks.
- **c.** DoS attacks do not use DNS servers as DDoS attacks do.
- **d.** DoS attacks use more memory than DDoS attacks.

9. Which of the following is NOT true about VBA?
- **a.** It is commonly used to create macros.
- **b.** It is built into most Microsoft Office applications.
- **c.** It is included in select non-Microsoft products.
- **d.** It is being phased out and replaced by PowerShell.

10. Which of the following is NOT a Microsoft defense against macros?
- **a.** Protected View
- **b.** Trusted documents
- **c.** Trusted domain
- **d.** Trusted location

11. Theo uses the Python programming language and does not want his code to contain vulnerabilities. Which of the following best practices would Theo NOT use?
- **a.** Only use compiled and not interpreted Python code.
- **b.** Use the latest version of Python.
- **c.** Use caution when formatting strings.
- **d.** Download only vetted libraries.

12. What is Bash?
- **a.** The command-language interpreter for Linux/UNIX OSs
- **b.** The open source scripting language that contains many vulnerabilities
- **c.** A substitute for SSH
- **d.** The underlying platform on which macOS is built

13. Gregory wants to look at the details about the patch a packet takes from his Linux computer to another device. Which Linux command-line utility will he use?
- **a.** tracepacket
- **b.** trace
- **c.** tracert
- **d.** traceroute

14. Which utility sends custom TCP/IP packets?
- **a.** curl
- **b.** hping
- **c.** shape
- **d.** pingpacket

15. Which of the following is a third-party OS penetration testing tool?
- **a.** theHarvester
- **b.** scanless
- **c.** Nessus
- **d.** sn1per

16. Eros wants to change a configuration file on his Linux computer. He first wants to display the entire file contents. Which tool would he use?
- **a.** head
- **b.** show
- **c.** display
- **d.** cat

17. Which of the following is a tool for editing packets and then putting the packets back onto the network to observe their behavior?
- **a.** Tcpreplay
- **b.** Tcpdump
- **c.** Wireshark
- **d.** Packetdump

18. Estevan has recommended that the organization hire and deploy two security guards in the control room to limit the effect if one of the guards has been compromised. What is Estevan proposing?
    a. Dual observation protocol (DOP)
    b. Compromise mitigation assessment (CMA)
    c. Two-person integrity/control
    d. Multiplayer recognition

19. Which of the following sensors can detect an object that enters the sensor's field?
    a. Proximity
    b. Field detection
    c. IR verification
    d. Object recognition

20. Which of the following does NOT describe an area that separates threat actors from defenders?
    a. DMZ
    b. Air gap
    c. Secure area
    d. Containment space

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 8-1: DNS Poisoning

Time Required: 20 minutes
Objective: Given a scenario, analyze potential indicators associated with network attacks.
Description: Substituting a fraudulent IP address can be done by either attacking the Domain Name System (DNS) server or the local host table. Attackers can target a local hosts file to create new entries that will redirect users to their fraudulent site. In this project, you add a fraudulent entry to the local hosts file.

1. Go to the Western Kentucky University website at **www.wku.edu**.
2. Go the website for your school or the business where you work.
3. Find the IP address of the website of the school or business. Open a command line and enter **ping** *name_of_website* or go to **ipaddress.com/ip_lookup/** and enter the domain name to receive the correct IP address.

CAUTION If your search reveals multiple IP addresses for that website, choose another website that only has a single IP address.

4. Verify the IP address of both sites. To reach the Western Kentucky University website by IP address, use your web browser to go to **https://161.6.94.21**.

CAUTION If your browser displays warning messages when searching by IP address, click through those messages and approve using the IP address.

5. Go to the website of your school or business by entering **https:**//*IP_address*.
6. Click **Start** and then click **Windows Accessories**.
7. Right-click **Notepad**, click **More**, and then select **Run as administrator**. If you receive the message **Do you want to allow this app to make changes to the device?** click **Yes**.

8. Click **File** and then click **Open**. Click the **File Type** arrow to change from **Text Documents (*.txt)** to **All Files (*.*)**.
9. Navigate to the file **C:\Windows\System32\drivers\etc\hosts** and open it.
10. At the end of the file following all hashtags (#) in the first column, enter the IP address of **161.6.94.21**. This is the IP address of Western Kentucky University.
11. Press **Tab** and enter *www.name_of_your_school_or_business*. In this hosts table, the domain name of your school or business is now resolved to the IP address of Western Kentucky University.
12. Click **File** and then click **Save**.
13. Open your web browser and then enter the URL of your school or business. What website appears?
14. Return to the hosts file and remove this entry.
15. Click **File** and then click **Save**.
16. Close all windows.

Project 8-2: ARP Poisoning

Time Required: 25 minutes
Objective: Given a scenario, analyze potential indicators associated with network attacks.
Description: Attackers frequently modify the Address Resolution Protocol (ARP) table to redirect communications away from a valid device to an attacker's computer. In this project, you view the ARP table on your computer and modify it. You will need to have another "victim's" computer running on your network (and know the IP address), as well as a default gateway that serves as the switch to the network.

1. Open a Command Prompt window by right-clicking **Start** and selecting **Windows PowerShell (Admin)**.
2. To view your current ARP table, type **arp -a** and then press **Enter**. The Internet Address is the IP address of another device on the network while the Physical Address is the MAC address of that device.
3. To determine network addresses, type **ipconfig/all** and then press **Enter**.
4. Record the IP address of the default gateway.
5. Delete the ARP table entry of the default gateway by typing **arp -d** followed by the IP address of the gateway, such as **arp -d 192.168.1.1**, and then press **Enter**.
6. Create an automatic entry in the ARP table of the victim's computer by typing **ping** followed by that computer's IP address, such as **ping 192.168.1.100**, and then press **Enter**.
7. Verify that this new entry is now listed in the ARP table by typing **arp -a** and then press **Enter**. Record the physical address of that computer.
8. Add that entry to the ARP table by entering **arp -s** followed by the IP address and then the MAC address.
9. Delete all entries from the ARP table by typing **arp -d**.
10. Close all windows.

Project 8-3: MAC Spoofing

Time Required: 25 minutes
Objective: Given a scenario, analyze potential indicators associated with network attacks.
Description: In a MAC cloning attack, threat actors discover a valid MAC address of a device connected to a switch. They spoof the MAC address on their device and send a packet onto the network. In this activity, you will spoof a MAC address.

1. Go to the Technitium website at **technitium.com/tmac/**. (If you are no longer able to access the program through this URL, use a search engine to search for "Technitium MAC address changer.")
2. Click **Download Now**.
3. Click **Direct Download**.
4. Save the file to your computer, install the application, and then start it.
5. If necessary, click **Yes** to respond to the dialog box.
6. Scroll through the list of network connections on your computer, and then select your Internet connection.

7. Read the information on the **Information** tab.
8. Click **Random MAC Address** to display another MAC address that can be assigned to this device.
9. Click the down arrow in the box below the new random MAC address. Note the long list of different NIC vendors from which a MAC address can be chosen.
10. Click **(2C-30-33) Netgear**.
11. Look at the new MAC address under **Change MAC Address** and note the first three pairs of numbers. What does this correspond to?
12. Click **Why?** next to **Use '02' as first octet of MAC address**.
13. Read the explanation about why 02 should be used as the first octet.
14. If you want to change your MAC address, click **Change Now!** or close the application if you do not want to change the address.
15. How easy was it to spoof a MAC address? How can a threat actor use this in a MAC cloning attack?
16. Close all windows.

Case Projects

Case Project 8-1: DDoS Mitigation

How do organizations attempt to mitigate a sudden DDoS attack directed at their web servers? Use the Internet to research DDoS mitigation techniques, technologies, and third-party entities that provide mitigation services. Write a one-page paper on your research.

Case Project 8-2: DNS Services

Many organizations offer a free domain name resolution service that resolves DNS requests through a worldwide network of redundant DNS servers. The claim is that this is faster and more reliable than using the DNS servers provided by Internet service providers (ISPs). These DNS servers are supposed to improve security by maintaining a real-time blacklist of harmful websites and warning users when they attempt to access a site containing potentially threatening content. The providers also say that using their services can reduce exposure to types of DNS poisoning attacks. Research free DNS services. Identify at least three providers and create a table comparing their features. Are the claims of providing improved security valid? How do they compare with your ISP's DNS service? Write a one-page paper on your research.

Case Project 8-3: DNS-over-HTTPS (DoH)

To protect DNS, some providers are using DNS-over-HTTPS, also called DoH. As its name implies, DoH uses HTTPS instead of HTTP to send DNS queries via an encrypted HTTPS connection (Port 443) rather than sending them in cleartext (Port 53). The encrypted DoH query is sent to a special DoH-resolving server that aggregates all user's DoH queries and then translates them into regular unencrypted DNS queries for processing by DNS servers. However, DoH has become controversial. Why? What are the advantages of DoH? What are its disadvantages? How does it compare with DNS-over-TLS (DoT)? Write a one-page paper on your research.

Case Project 8-4: CCTV Technologies

Research new technologies for CCTV, including motion recognition and object detection. How accurate are the technologies? What are the advantages? What are the disadvantages? Write a one-page paper on your research.

Case Project 8-5: Robot Sentries

Research the Internet regarding robot sentries. Where are they being used? What is the purpose of a robot sentry? What are the risks? What is your projection on the future for robot sentries? Write a one-page paper on your research.

Case Project 8-6: Locks

Lock technology is changing rapidly. Use the Internet to research physical locks, electronic locks, smart locks, and fingerprint locks. Create a table of these types of locks and list their strengths, weaknesses, and costs. Which would you recommend? Why?

Case Project 8-7: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to login, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and click on **Security+ Case Projects (7th edition)**. Read the following case study.

Read again the Front-Page Cybersecurity at the beginning of this module. In addition to the three reasons listed why View windows would be interesting to attackers, can you think of two or more other reasons how attackers (either cybersecurity attackers or physical criminals) could manipulate these windows? Now pretend that you are a security consultant and View is one of your clients. What would you say to the View CEO about his public statement that "The good news is the window's not that interesting to hack." Should CEOs first talk with employees before making those statements? Or have the security employees done a poor job in educating the View CEO about cybersecurity risks? Record your answers on the Community Site discussion board.

Case Project 8-8: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist this company.

It's Your Birthday (IYB)! is a new North Ridge client that creates fun and innovative birthday experiences for clients of all ages. Recently, IYB! decided that the security at its corporate office needed to be addressed after several incidences of unauthorized personnel entering the offices. You are asked to provide information about internal physical security controls as a starting point in the discussion.

1. Create a PowerPoint presentation about internal physical security controls, including what they are, what they can protect, how they should be used, and the various types of controls. Include the advantages and disadvantages of each. Your presentation should contain at least 10 slides.
2. After the presentation, you were asked to follow up about reception areas and mantraps, especially how to configure each. Create a memo communicating which you would recommend and why.

References

1. Thompson, Mia, "How to stay safe from Office macro-based malware with email security," *Solarwinds MSP*, Feb. 10, 2020, accessed Jun. 17, 2020, www.solarwindsmsp.com/blog/how-stay-safe-office-macro-based-malware-email-security.

MODULE 9

NETWORK SECURITY APPLIANCES AND TECHNOLOGIES

After completing this module, you should be able to do the following:

1. List the different types of network security appliances and how they can be used
2. Describe network security technologies

Front-Page Cybersecurity

One constant across all of the Star Wars films is the use of weapons: lightsabers, blasters, ion cannons, and planetary turbolasers are just a few that are used by both the Rebellion and the Evil Empire. An additional weapon in the Star Wars arsenal did not appear in any film but was extremely important. The weapon kept cyber threat actors from stealing the script as it was developed. As with most Star Wars weapons, it worked.

Protecting new Star Wars scripts is a high-stakes effort. The Star Wars franchise is estimated to have grossed more than $10 billion since the first movie came out in 1977. The success of the movies shows no signs of diminishing. The latest movie, *Star Wars: The Rise of Skywalker*, has already grossed more than $1 billion since its release in December 2019. Those involved with the Star Wars films have every incentive to make sure that scripts for future releases are kept secure and are not stolen. A leaked script would spoil the impact of the storyline and affect ticket sales for the movie.

In recent years, attackers have stolen scripts or entire movies from movie studios or their affiliates. In 2017, a group of attackers stole and then leaked the entire fifth season of Netflix's *Orange Is the New Black* videos along with several other productions from Larson Studios, a Hollywood-based audio post-production company. In late 2004, attackers breached Sony security and posted online several unreleased movies, including *Annie*, *Mr. Turner*, *To Write Love on Her Arms*, and *The Interview*.

What weapons has Star Wars used to protect itself from attackers?

Consider the weapon that the writer and director, Rian Johnson, used to protect his script while he was developing *Star Wars: The Last Jedi* from theft.

He used an air gap.

One of the best means of providing security is to completely disconnect a device from any and all networks. Sometimes called an air gap, this method simply means that the device is not connected to a network or anything else. In today's world, it can be cumbersome and inconvenient to have an unconnected device, but it provides a high level of security.

That's exactly what Rian Johnson did. While writing the script, Rian never connected his MacBook Air to any network (either a LAN or the Internet) and never used it for email, online research, or anything else. In fact, his MacBook Air was

only used for one purpose: to write the script. Isolating the laptop meant that no outsiders could get to his script through a network vulnerability. While he was not using it, the MacBook Air was locked securely in a safe at the studios. Rian's air gap weapon worked as expected and the script was never stolen.

Rian did say that his producer had a constant worry. He was terrified that Rian would walk off and leave the MacBook at a coffee shop.

At one time, *information security* and *network security* were virtually synonymous. That was because the network was viewed as the "moat" around which endpoint computers could be kept safe. A secure network was seen as the key to keeping attackers away.

This approach, however, proved to be untenable. Too many entry points allow attackers to circumvent the network and introduce malware. For example, users could insert an infected USB flash drive into their computer, thus installing malware while bypassing the secure network. With computers connected to the unsecure Internet, malware could take advantage of common network protocols, such as Hypertext Transfer Protocol (HTTP), without being detected or blocked by network security appliances.

This is not to say that network security is unimportant. Having a secure network is still essential. Even today, not all applications are designed and written with security in mind, so it falls on the network to provide protection. Network-delivered services can also scale better for larger environments and can complement server and application functionality. Because an attacker who successfully penetrates a computer network can access hundreds or even thousands of endpoints, servers, and storage devices, a secure network defense remains a critical element in any enterprise's overall security plan.

This module explores network security. It investigates how to build a secure network through network security appliances and technologies.

SECURITY APPLIANCES

CERTIFICATION

2.1 Explain the importance of security concepts in an enterprise environment.

3.3 Given a scenario, implement secure network designs.

All modern networks have both standard networking devices (such as switches and routers) and specialized security appliances. Security can be achieved through the appliances that directly address security and by using the security features in standard networking devices. Using both standard networking devices and security appliances can result in a layered security approach, which can significantly improve security. To breach a network with layered security, an attacker must have the tools, knowledge, and skills to break through the various layers.

While it is worthwhile to take advantage of the security features of standard networking devices, several security appliances can be dedicated to protecting a network. These appliances include firewalls, proxy servers, deception instruments, intrusion detection and prevention systems, and network hardware security modules. In addition, these appliances must be properly configured.

NOTE 1

Security appliances are only one element in network security and should not be exclusively relied upon for protection. This can be illustrated through a successful attack on NASA's Jet Propulsion Laboratory (JPL) that resulted in 500 MB of stolen data related to a Mars mission. A 49-page report by the NASA Office of Inspector General (OIG) revealed that although the NASA JPL network had security appliances installed, the point of entry into the network by attackers was a $35 Raspberry Pi, small enough to fit in your hand, that a JPL employee connected to the JPL network without authorization.

Firewalls

Probably the most misunderstood security appliance is a firewall. Due to the nature of its name (*It's an impenetrable wall!*) and aided by inaccurate portrayals in movies and television, the general public often perceives a firewall as the ultimate security device that blocks anything and everything malicious from entering a network. Unfortunately, this is a wildly inaccurate perception. Firewalls are an important element in network security, but they fall far short of being the ultimate defense. To use them effectively, you should understand the function of firewalls and know the different types of firewalls and specialized firewall appliances.

Firewall Functions

Both national and local building codes require commercial buildings, apartments, and other similar structures to have a *firewall*. In building construction, a firewall is usually a brick, concrete, or masonry wall positioned vertically through all stories of the building. Its purpose is to contain a fire and prevent it from spreading. A computer **firewall** serves a similar purpose: it is designed to limit the spread of malware.

A firewall uses bidirectional inspection to examine both outgoing and incoming network packets. It allows approved packets to pass through but can take different actions when it detects a suspicious packet. The actions are based on specific criteria or rules; these types of firewalls are called *rule-based firewalls*. Firewall rules can contain parameters such as the following:

- *Source address*. The source address is the location of the origination of the packet (where the packet is *from*). Addresses generally can be indicated by a specific IP address or range of addresses, an IP mask, the MAC address, or host name.
- *Destination address*. This is the address the connection is attempting to reach (where the packet is going *to*). Destination addresses can be indicated in the same way as the source address.
- *Source port*. The source port is the TCP/IP port number used to send packets of data. Options for setting the source port often include a specific port number or a range of numbers.
- *Destination port*. This setting gives the port on the remote computer or device that the packets will use. Options are the same as for the source port.
- *Protocol.* The protocol defines the network protocol (such as *TCP*, *UDP*, *TCP or UDP*, *ICMP*, or *IP*) used when sending or receiving packets of data.
- *Direction*. This is the direction of traffic for the data packet (*Incoming*, *Outgoing*, or *Both*).
- *Priority*. The priority determines the order in which the rule is applied.
- *Time*. Rules can be set so they are active only during a scheduled time.
- *Context*. A rule can be created that is unique for specific circumstances (contexts). For example, different rules may be in effect depending on whether a laptop is on-site or is remote (sometimes called **geographical consideration**).
- *Action*. The action setting indicates what the firewall should do when the conditions of the rule are met. Typical firewall rule actions are listed in Table 9-1.

Table 9-1 Typical firewall rule actions

Action	Description	Example	Comments
Allow	Explicitly allows traffic that matches the rule to pass	Permit incoming Address Resolution Protocol (ARP) traffic	Allow implicitly denies all other traffic unless explicitly allowed
Bypass	Allows traffic to bypass the firewall	Bypass based on IP, port, traffic direction, and protocol	Designed for media-intensive protocols or traffic from a trusted source
Deny	Explicitly blocks all traffic that matches the rule	Deny traffic from IP address	Deny generally drops the packet with no return message to the sender
Force Allow	Forcibly allows traffic that would normally be denied by other rules	Useful for determining if essential network services are able to communicate	Traffic will still be subject to inspection by other security appliances
Log Only	Traffic is logged but no other action is taken	Bypass rules do not generate log files but Log Only will	Log Only occurs if the packet is not stopped by a Deny rule or an Allow rule that excludes it

Older firewalls often listed each rule as a separate instruction that was processed in sequence so that firewall rules were essentially *IF-THEN-ELSE* constructions: *IF* these rule conditions are met, *THEN* the action occurs, *ELSE* go on to the next rule. This construction made administrators consider the rules themselves and their sequencing. For example, if Rule #13 allowed an FTP connection to a specific address, but later Rule #27 was added to deny all FTP traffic, then FTP packets meeting Rule #13 would be allowed because it occurred first. More modern firewalls allow a priority order to be created to eliminate the confusion that often surrounded conflicting rules.

A more flexible type of firewall than a rule-based firewall is a *policy-based firewall.* This type of firewall allows more generic statements instead of specific rules. For example, the policy statement *Allow management traffic from trusted networks* could translate into specific rules that allow traffic from *192.2.0.0/24* to *TCP Port 22* and *192.2.100.0/24* to *TCP Port 3389.*

In addition to filtering based on packets, firewalls can also apply **content/URL filtering**. The firewall can monitor websites accessed through HTTP to create custom filtering profiles. The filtering can be performed by assessing webpages by their content category and then creating whitelists and blacklists of specific URLs. This type of filtering is often available with consumer-oriented firewalls and advertised as a parental control feature that is easily configurable, as shown in Figure 9-1.

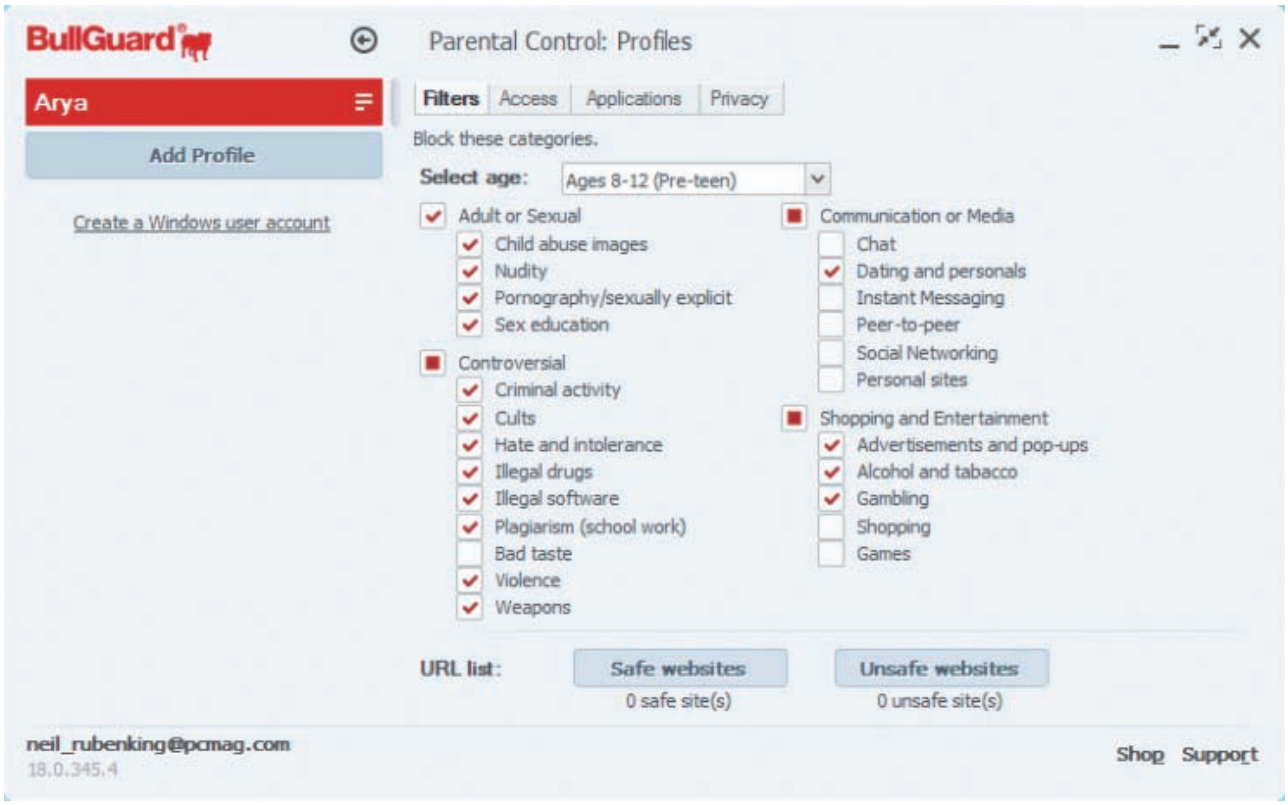


Figure 9-1 Content/URL filtering

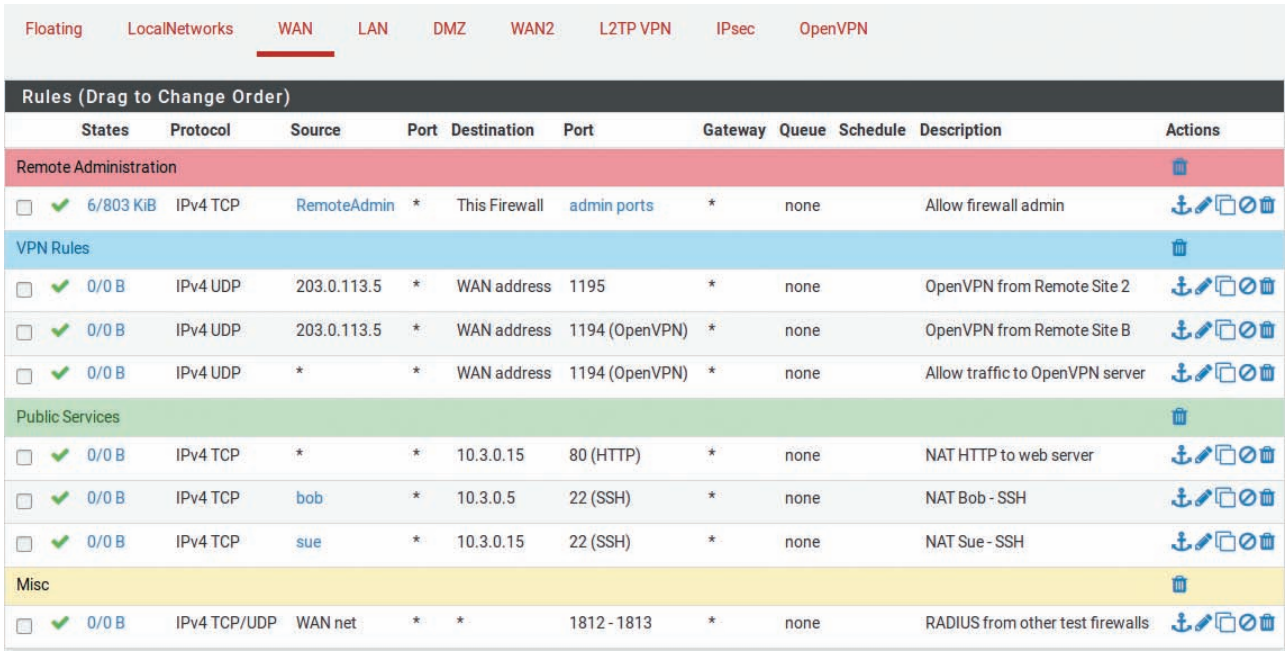
Firewall Categories

The categories of firewalls can be compared as opposites and include the following:

- *Stateful vs. stateless*. **Stateless packet filtering** looks at a packet and permits or denies it based solely on the firewall rules. **Stateful packet filtering** uses both the firewall rules and the state of the connection: that is, did the internal device request this packet? A stateful packet filtering firewall keeps a record of the state of a connection between an internal endpoint and an external device. While a stateless packet filter

firewall might allow a packet to pass through because it met all the necessary criteria (rules), a stateful packet filter would not let the packet pass if that internal endpoint did not first request the information from the external server.

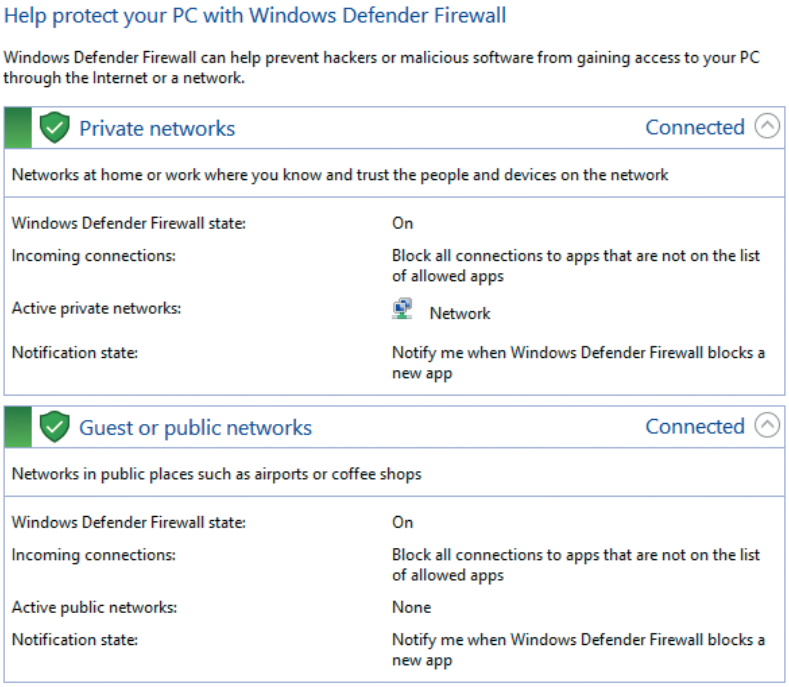
- *Open source vs. proprietary.* Some firewalls are freely available (**open source firewalls**) while other firewalls are owned by an entity that has an exclusive right to them (**proprietary firewalls**). Open source firewalls have been gaining wider acceptance as they incorporate more features and are built on a secure foundation. For example, pfSense is built on the same underlying OS as many commercial products. See Figure 9-2.



Source: pfSense

Figure 9-2 pfSense open source firewall

- *Hardware vs. software.* A **software firewall** runs as a program or service on a device, such as a computer or router. **Hardware firewalls** are specialized separate devices that inspect traffic. Because they are specialized devices, hardware firewalls tend to have more features but are more expensive and can require more effort to configure and manage. However, a disadvantage of a software firewall is that a malware infection on the device on which it is running, such as a computer, could also compromise the software firewall. Whereas a hardware firewall also has underlying software, typically that footprint is smaller (to provide less of a target for attackers) or specialized.
- *Host vs. appliance vs. virtual.* A **host-based firewall** is a software firewall that runs on and protects a single endpoint device (a host). All modern OSs include a host-based firewall. The settings for the Microsoft Windows Defender host-based firewall are shown in Figure 9-3. A closer look at the configuration settings reveals that these firewalls tend to be application-centric: users can create an opening in the firewall for each specific application. This approach is more secure than permanently opening a port in the firewall that always remains open as opposed to a port that is only opened when the application requires it and is then closed. An **appliance firewall** is typically a separate hardware device designed to protect an entire network, as shown in Figure 9-4. A **virtual firewall** is one that runs in the cloud. Virtual firewalls are designed for settings, such as public cloud environments, in which deploying an appliance firewall would be difficult or even impossible.



Used with permissions from Microsoft

Figure 9-3 Windows host-based firewall

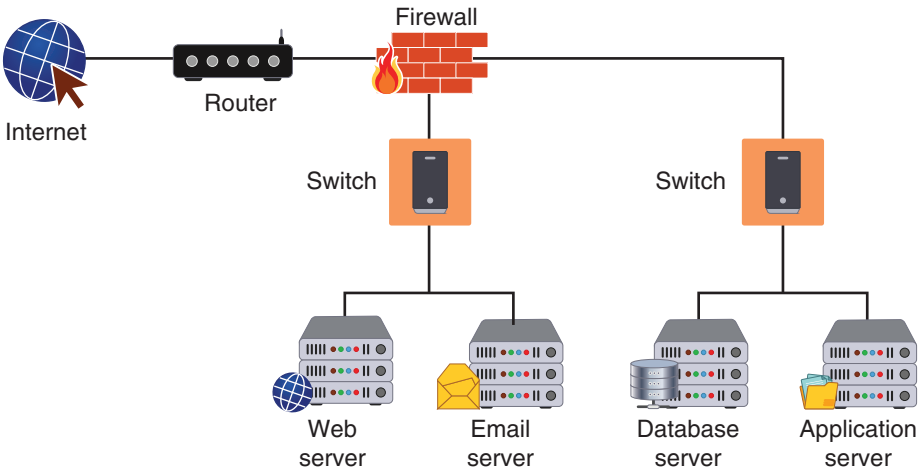


Figure 9-4 Appliance firewall

Specialized Firewall Appliances

Specialized firewall appliances include the following:

- *Web application firewall*. One specialized firewall is a **web application firewall (WAF)** that looks at the applications using HTTP. A web application firewall, which can be a separate hardware appliance or a software plug-in, can block specific websites or attacks that attempt to exploit known vulnerabilities in specific client software and can even block cross-site scripting and SQL injection attacks.
- *Network address translation gateway*. *Network address translation (NAT)* is a technique that allows private IP addresses to be used on the public Internet. It does this by replacing a private IP address with a public IP address. As a packet leaves a network, NAT removes the private IP address from the sender's packet and replaces it with an alias IP public address, and then maintains a record of the substitution. When a packet is returned, the process is reversed. A **network address translation gateway** is a cloud-based technology that performs NAT translations for cloud services. It can also provide a degree of security by masking the IP addresses of internal devices.

- *Next generation firewall*. A **next generation firewall (NGFW)** has additional functionality beyond a traditional firewall. NGFW can filter packets based on applications. NGFWs can detect applications by using *deep packet inspection* and thus can examine the payloads of packets and determine if they are carrying malware. In addition to basic firewall protections, filtering by applications, and deep packet inspection, NGFWs can also perform URL filtering and intrusion prevention services.
- *Unified threat management*. **Unified threat management (UTM)** is a device that combines several security functions. These include packet filtering, antispam, antiphishing, antispyware, encryption, intrusion protection, and web filtering.

NOTE 2

Often a device that performs services beyond that of a NGFW is called a UTM.

Proxy Servers

In general terms, a *proxy* is a person who is authorized to act as the substitute or agent on behalf of another person. For example, a family member who has been granted the power of attorney for a sick relative can make decisions and take actions on behalf of that person as a proxy.

Proxies are also devices used in computer networking. These devices act as substitutes on behalf of the primary device. A **forward proxy** is a computer or an application that intercepts user requests from the internal secure network and then processes the requests on behalf of the user. When an internal endpoint requests a service such as a file or a webpage from an external web server, it normally connects directly to the remote server. In a network using a forward proxy server, the endpoint first connects to the proxy server, which checks its memory to see if a previous request already has been fulfilled and if a copy of that file or page is residing on the proxy server in its temporary storage area (*cache*). If not, the proxy server connects to the external web server using its own IP address (instead of the internal endpoint's address) and requests the service. When the proxy server receives the requested item from the web server, the item is forwarded to the requester.

A **reverse proxy** routes requests coming from an external network to the correct internal server. To the outside user, the IP address of the reverse proxy is the final IP address for requesting services; however, only the reverse proxy can access the internal servers. Forward proxy and reverse proxy servers are illustrated in Figure 9-5.

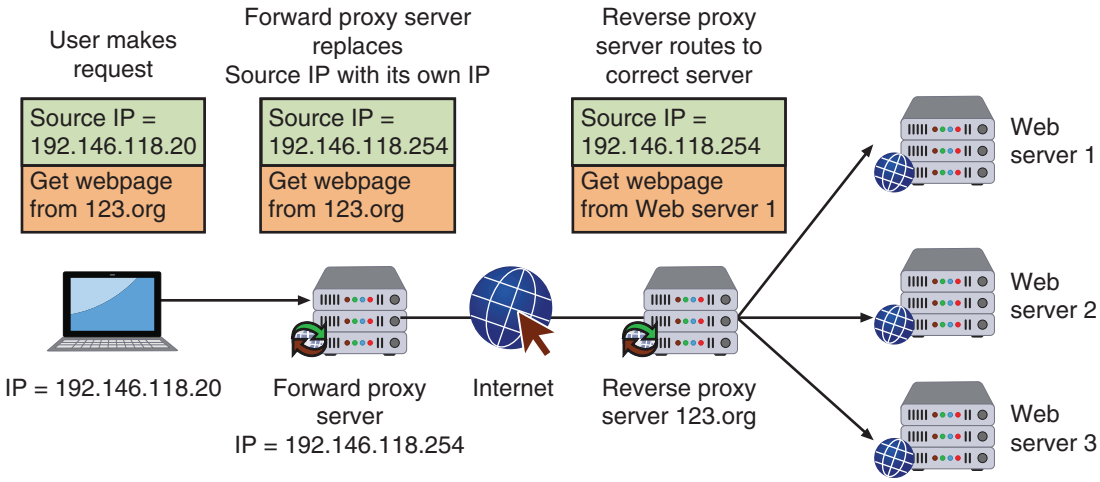


Figure 9-5 Forward and reverse proxy servers

Acting as the intermediary, a proxy server can provide a degree of protection. First, it can look for malware by intercepting it before it reaches the internal endpoint. Second, a proxy server can hide the IP address of endpoints inside the secure network so that only the proxy server's IP address is used on the open Internet.

Deception Instruments

Deception is the act of causing someone to accept as true that is false. Deception can be used as a security defense: by directing threat actors away from a valuable asset to something that has little or no value, threat actors can be tricked into thinking what they are attacking is valuable when it is not, or that their attack is successful when it is not. Creating network deception can involve creating and using honeypots and sinkholes.

NOTE 3

Niccolo Machiavelli, an Italian Renaissance diplomat and philosopher who is often called the father of modern political science, once said, "Never attempt to win by force what can be won by deception."

Honeypots

A **honeypot** is a computer located in an area with limited security that serves as "bait" to threat actors. The honeypot is intentionally configured with security vulnerabilities so that it is open to attacks. Security personnel generally have two goals when using a honeypot:

- *Deflect.* A honeypot can deflect or redirect threat actors' attention away from legitimate servers by encouraging them to spend their time and energy on the decoy server, distracting their attention from the data on the actual server.
- *Discover.* A honeypot can trick threat actors into revealing their attack techniques. Security experts can then determine if actual production systems could thwart such an attack.

Figure 9-6 shows the results from a honeypot dashboard; it lists attacker probes by time and country.

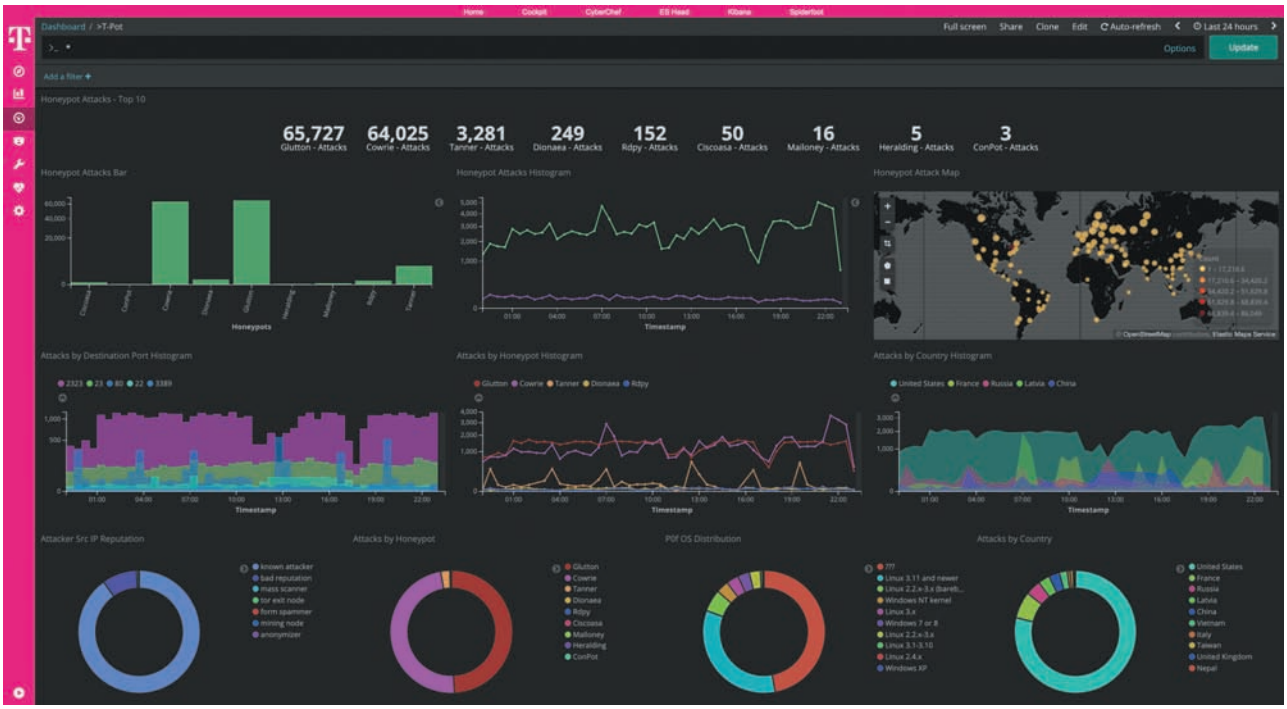


Figure 9-6 Honeypot dashboard

There are different types of honeypots. A *low-interaction honeypot* may only contain a login prompt. This type of honeypot only records login attempts and provides information on the threat actor's IP address of origin. A *high-interaction honeypot* is designed for capturing much more information from the threat actor. Usually it is configured with a default login and loaded with software, data files that appear to be authentic but are actually imitations of real data files (**honeyfiles**), and **fake telemetry.** (*Telemetry* is the collection of data such as how certain software features are used, application crashes, and general usage statics and behavior.) A high-interaction honeypot can collect valuable information from threat actors about attack techniques or the particular information they are seeking from the organization.

NOTE 4

The number of attempts against a honeypot is staggering. In one study, 10 honeypots around the world were created to simulate the Secure Shell (SSH) service. One honeypot started receiving login attempts just *52 seconds* after it went online. When all 10 of the honeypots were discovered, a login attempt was made about every *15 seconds on each one*. At the end of one month, over five million attacks had been attempted on the honeypots.[1]

Similar to a honeypot, a **honeynet** is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied; that information can then be used to increase network security. A honeynet typically contains one or more honeypots.

CAUTION Setting up a honeypot to attract threat actors can be dangerous. There must be no connection between the honeypot and the production network. A safer approach is to use a cloud service provider for setting up a honeypot.

Sinkholes

Another deception technique is to use *sinkholes*. A sinkhole is essentially a "bottomless pit" designed to steer unwanted traffic away from its intended destination to another device, deceiving the threat actor into thinking the attack is successful when the sinkhole is actually providing information about the attack. One type of sinkhole is a **DNS sinkhole**. A DNS sinkhole changes a normal DNS request to a pre-configured IP address that points to a firewall with a rule of *Deny* set for all packets so that every packet is dropped with no return information provided to the sender.

NOTE 5

DNS sinkholes are commonly used to counteract DDoS attacks. Many enterprises contract with a DDoS mitigation service to help identify DDoS traffic and send it to a sinkhole while allowing legitimate traffic to reach its destination. Law enforcement also uses sinkholes to stop a widespread ongoing attack by redirecting traffic away from the attacker's command and control (C&C) server to a sinkhole. As an added step, the sinkhole can save these packets for further examination in an to attempt to identify the threat actors.

Intrusion Detection and Prevention Systems

An *intrusion detection system (IDS)* can detect an attack as it occurs, while an *intrusion prevention system (IPS)* attempts to block the attack. An **inline** system is connected directly to the network and monitors the flow of data as it occurs. A **passive** system is connected to a port on a switch, which receives a copy of network traffic. Table 9-2 lists the differences between inline and passive systems.

Table 9-2 Inline vs. passive IDS

Function	Inline	Passive
Connection	Directly to network	Connected to port on switch
Traffic flow	Routed through the device	Receives copy of traffic
Blocking	Can block attacks	Cannot block attacks
Detection error	May disrupt service	May cause false alarm

In addition, IDS systems can be managed in different ways. *In-band* management is through the network itself by using network protocols and tools, while **out-of-band management** is using an independent and dedicated channel to reach the device.

IDS systems can use different methodologies for monitoring for attacks. In addition, IDS and IPS can be installed on networks as they can on local endpoints.

Monitoring Methodologies

Monitoring involves examining network traffic, activity, transactions, or behavior to detect security-related anomalies. The four monitoring methodologies are anomaly-based monitoring, signature-based monitoring, behavior-based monitoring, and heuristic monitoring.

Anomaly monitoring is designed for detecting statistical anomalies. First, a baseline of normal activities is compiled over time. (A *baseline* is a reference set of data against which operational data is compared.) Whenever activity deviates significantly from the baseline, an alarm is raised. An advantage of this approach is that it can detect the anomalies quickly without trying to first understand the underlying cause. However, normal behavior can change easily and even quickly, so anomaly-based monitoring is subject to false positives. In addition, anomaly-based monitoring can impose heavy processing loads on the systems where they are being used. Finally, because anomaly-based monitoring takes time to create statistical baselines, it can fail to detect events before the baseline is completed.

A second method for auditing usage is to examine network traffic, activity, transactions, or behavior and look for well-known patterns, much like antivirus scanning. This is known as **signature-based monitoring** because it compares activities against a predefined signature. Signature-based monitoring requires access to an updated database of signatures along with a means to actively compare and match current behavior against a collection of signatures. One of the weaknesses of signature-based monitoring is that the signature databases must be constantly updated, and as the number of signatures grows, the behaviors must be compared against an increasingly large number of signatures. Also, if the signature definitions are too specific, signature-based monitoring can miss variations.

Behavioral monitoring attempts to overcome the limitations of both anomaly-based monitoring and signature-based monitoring by being adaptive and proactive instead of reactive. Rather than using statistics or signatures as the standard by which comparisons are made, behavior-based monitoring uses the "normal" processes and actions as the standard. Behavior-based monitoring continuously analyzes the behavior of processes and programs on a system and alerts the user if it detects any abnormal actions, at which point the user can decide whether to allow or block the activity. One advantage of behavior-based monitoring is that it is not necessary to update signature files or compile a baseline of statistical behavior before monitoring can take place. In addition, behavior-based monitoring can more quickly stop new attacks.

The final method takes a completely different approach and does not try to compare actions against previously determined standards (like anomaly-based monitoring and signature-based monitoring) or behavior (like behavior-based monitoring). Instead, it is founded on *experience-based techniques*. Known as **heuristic monitoring**, it attempts to answer the question, *Will this do something harmful if it is allowed to execute*? Heuristic (from the Greek word for *find* or *discover*) monitoring is like heuristic antivirus detection. However, instead of creating a virtual environment in which to test a threat, IDS heuristic monitoring uses an algorithm to determine if a threat exists. Table 9-3 illustrates how heuristic monitoring could trap an application that attempts to scan ports that the other methods might not catch.

Table 9-3 Methodology comparisons to trap port scanning application

Monitoring methodology	Trap application scanning ports?	Comments
Anomaly-based monitoring	Depends	Only if this application has tried to scan previously and a baseline has been established
Signature-based monitoring	Depends	Only if a signature of scanning by this application has been previously created
Behavior-based monitoring	Depends	Only if this action by the application is different from other applications
Heuristic monitoring	Yes	IDS is triggered if any application tries to scan multiple ports

NOTE 6

A major difference between a NIDS and a NIPS is its location. A NIDS has sensors that monitor the traffic entering and leaving a firewall, and reports back to the central device for analysis. A NIPS, on the other hand, would be located inline on the firewall itself. This allows the NIPS to act more quickly to block an attack.

Network Detection and Prevention Systems IDS and IPS can be applied to networks as well as hosts (endpoints). These network-based systems include the following:

- *Network intrusion detection systems*. A **network intrusion detection system (NIDS)**, similar to a software-based host intrusion detection system (HIDS), watches for attacks on the network. As network traffic moves through the network, NIDS sensors—usually installed on network devices such as firewalls and routers—gather information and report back to a central device.
- *Network intrusion prevention system*. A **network intrusion prevention system (NIPS)** not only monitors to detect malicious activities but also attempts to stop them, much like a host intrusion detection system (HIPS).

Network Hardware Security Modules

NOTE 7

HSMs are covered in Module 6.

A *hardware security module (HSM)* is a removable external cryptographic device. For endpoints, an HSM is typically a USB device, an expansion card, or a device the connects directly to a computer through a port.

However, if many endpoints use an HSM, having a centralized device can improve processing times and increase security. A **network hardware security module** is a special trusted network computer that performs cryptographic operations such as key management, key exchange, onboard random number generation, key storage facility, and accelerated symmetric and asymmetric encryption. Due to the risks associated with a compromised network hardware security module, these are usually built on specialized hardware running a security-focused OS and have limited external access.

Configuration Management

It is essential that these security appliances be properly configured. Not only does a misconfigured device allow threat actors an opening into the network; it also provides a false sense of security that makes it difficult to realize a problem exists (*we've got our NIPS running; that will give us protection*). Basic configuration management tools include the following:

- *Secure baseline configurations*. The purpose of a *baseline* is twofold: it is the initial starting point and the minimum that can be used for comparisons. A secure **baseline configuration** for security appliances likewise has two purposes. First, it is the starting point for configuring a device. While many security appliance configurations go beyond the baseline, the baseline sets the core fundamentals of how the device should be initially configured before the specific configurations are applied. Second, the baseline configuration can be considered the bare minimum: no configuration should be less than the secure baseline configuration.

NOTE 8

Secure baseline configuration documents can be purchased to help organizations define and document what constitutes a hardened and secure system. These configurations can also ensure that the organization is meeting all statutory, regulatory, and contractual requirements.

- *Standard naming conventions*. Using the same conventions for assigning names to appliances (**standard naming conventions**) can eliminate confusion regarding the various appliances. These conventions will vary by organization, but an example is: *"Device names are limited to 15 characters by technical necessity. To ensure interoperability with other systems, only letters and numbers shall be used. Each device name shall have the following minimum structure: the first three characters are the appropriate unit identifier (mandatory); the next six numbers are the device's inventory control tag number (mandatory); the remaining six characters may be used at the discretion of the department, or not used at all (optional)."*
- *Defined Internet Protocol schema*. An **Internet Protocol schema** is a standard guide for assigning IP addresses to devices. This makes it easier to set up and troubleshoot devices and helps to eliminate overlapping or duplicate subnets and IP address device assignments, avoid unnecessary complexity, and not waste IP address space.
- *Diagrams*. Creating a visual mapping (**diagram**) of security appliances can likewise be valuable when new appliances are added or when troubleshooting is required.

TWO RIGHTS & A WRONG

1. The bypass firewall rule action is designed for media-intensive protocols or traffic from a trusted source.
2. A stateful packet filter looks at packets and permits or denies it based solely on the firewall rules.
3. A forward proxy is a computer or an application program that intercepts user requests from the internal secure network and then processes these requests on behalf of the user.

See Appendix B for the answer.

SECURITY TECHNOLOGIES

CERTIFICATION

2.1 Explain the importance of security concepts in an enterprise environment.

3.3 Given a scenario, implement secure network designs.

In addition to security appliances are general security technologies that can provide a defense. Some of these security technologies can be found in both standard networking devices (such as switches and routers) and specialized security appliances. The categories of these security technologies are access technologies, monitoring and managing technologies, and design technologies.

Access Technologies

Some security technologies are designed to grant or deny access. The access may be to the network or to specific data. These technologies include access control list, virtual private network, network access control, and data loss prevention.

Access Control List (ACL)

NOTE 9

While a separate security device can provide in-depth protection, it can also slow the flow of data as the data must be sent through the device. A router using an ACL, on the other hand, can operate at the higher speed of the router and not delay network traffic.

As its name implies, an **access control list (ACL)** contains rules that administer the availability of digital assets by granting or denying access to the assets. The two types of ACLs include *filesystem ACLs*, which filter access to files and directories on an endpoint by telling the OS who can access the device and what privileges they are allowed. *Networking ACLs* filter access to a network. Network ACLs are often found on routers.

On external routers that face the Internet, router ACLs can restrict known vulnerable protocols from entering the network. They can also be used to limit traffic entering the network from unapproved networks. ACLs can also protect against IP spoofing that imitates another computer's IP address. Because IP spoofing attacks often use known unused and untrusted addresses, an external router ACL can help block these addresses (usually by designating a range of IP addresses) and thus minimize IP spoofing attacks.

CAUTION Antispoofing ACLs on external routers require frequent monitoring because the address ranges that are denied can frequently change.

NOTE 10

Software-based VPNs are often used on mobile devices and offer the most flexibility in how network traffic is managed. However, hardware-based VPNs, typically used for site-to-site connections, are more secure, have better performance, and can offer more flexibility.

Router ACLs can also be used on internal routers that process interior network traffic. Internal router ACLs usually are less restrictive but more specific than those on external routers ACLs since the devices on the internal network are generally considered to be friendly. Internal router ACLs are often configured with explicit *allow* and *deny* statements for specific addresses and protocol services. Internal router ACLs can also limit devices on the network from performing IP spoofing by applying outbound ACLs that limit the traffic to known valid local IP addresses.

Virtual Private Network (VPN)

A **virtual private network (VPN)** is a security technology that enables authorized users to use an unsecured public network, such as the Internet, as if it were a secure private network. It does this by encrypting all data transmitted between the remote endpoint and the network, not just specific documents or files. There are two common

types of VPNs. A **remote access VPN** is a user-to-LAN connection for remote users. The second type is a **site-to-site VPN**, in which multiple sites can connect to other sites over the Internet. Some VPNs allow the user to always stay connected instead of connecting and disconnecting from it. These are called **always-on VPNs**.

The two options for using a VPN depend on which traffic needs to be protected. A **full tunnel** sends all traffic to the VPN concentrator and protects it. However, not all traffic—such as web surfing or reading personal email—may need to be protected through a VPN. In this case, a **split tunnel**, or routing only some traffic over the secure VPN while other traffic directly accesses the Internet, may be used instead. Using a split tunnel can help to preserve bandwidth and reduce the load on the VPN concentrator.

Many protocols can be used for VPNs. The most common are IPsec and SSL or the weaker TLS. The **Layer 2 Tunneling Protocol (L2TP)** is a VPN protocol that does not offer encryption or protection, so it is usually paired with IPsec (L2TP/IPsec). The current version of HTML, **HTML 5**, can be used as a "clientless" VPN on an endpoint so that no additional software must be installed. Other popular VPN protocols include OpenVPN, SoftEther, WireGuard, SSTP, and IKEv2/IPsec.

Network Access Control (NAC)

The waiting room at a doctor's office is an ideal location for the spread of germs. Waiting patients are in a confined space, feel ill, and typically have weakened immune systems. A sick patient in the waiting room could easily infect all other waiting patients. It is not uncommon for a physician to post a nurse at the door of the waiting room to screen patients. Anyone who comes to the waiting room with certain symptoms is denied access (and rescheduled to a special after-hours appointment), given a prescription by the nurse for general medication, or directed to a separate quarantine room away from other patients.

This is the logic behind **network access control (NAC)**. NAC examines the current state of an endpoint before it can connect to the network. Any device that does not meet a specified set of criteria, such as having the most current antivirus signature or the software firewall properly enabled, is denied access to the network, given restricted access to computing resources, or connected to a "quarantine" network where the security deficiencies are corrected, after which the endpoint is connected to the normal network. The goal of NAC is to prevent computers with suboptimal security from potentially infecting other computers through the network.

NOTE 11

NAC also can be used to ensure that systems not owned by the organization—such as those owned by customers, visitors, and contractors—can be granted access without compromising security.

Some NAC systems use software installed on endpoints (**agents**) to gather information (called a host agent health check). An agent may be a *permanent NAC agent* and reside on end devices until uninstalled, or it may be a *dissolvable NAC agent* that disappears after reporting information to the NAC. Instead of installing agents on each device, the NAC technology can be embedded within a Microsoft Windows Active Directory domain controller. When a device joins the domain and a user logs in, NAC uses Active Directory to scan the device to verify that it complies with the necessary criteria. This is an **agentless** NAC because no additional software is required.

An example of the NAC process is illustrated in Figure 9-7:

1. The client performs a self-assessment using a System Health Agent (SHA) to determine its current security posture.
2. The assessment, known as a Statement of Health (SoH), is sent to a server called the Health Registration Authority (HRA). This server enforces the security policies of the network. It also integrates with other external authorities such as antivirus and patch management servers to retrieve current configuration information.
3. If the client is approved by the HRA, it is issued a Health Certificate.
4. The Health Certificate is then presented to the network servers to verify that the client's security condition has been approved.
5. If the client is not approved, it is connected to a quarantine network where the deficiencies are corrected, and then the computer is allowed to connect to the network.

NOTE 12

NAC uses two methods to direct an infected endpoint away from the normal production network. Interestingly, threat actors also use each method in their attacks. The first method is ARP poisoning and the second is DNS poisoning, each of which is covered in Module 8.

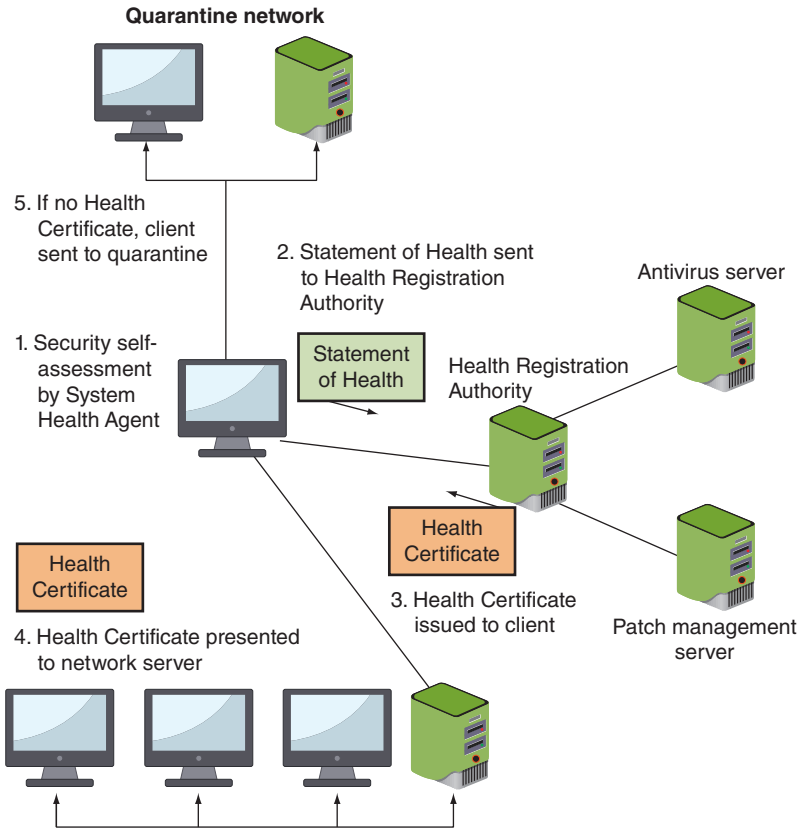


Figure 9-7 Network access control (NAC) process

Data Loss Prevention (DLP)

Keeping corporate data secure is a challenge for all organizations. While the threat of data theft from outside threat actors remains high, increasingly inside employees are careless or make mistakes when handling confidential corporate data. Employee carelessness with data has been identified in two primary areas. First, against company policy, many employees routinely send confidential data to their private email accounts so they can easily access it when needed. About one-third of employees admit to sending corporate data to their personal email accounts up to three times each month. Second, sensitive data is often sent to an approved third-party as an email attachment—but to the wrong recipient. Almost three-fourths of employees admit to sending data to the wrong recipient once per month.[2]

NOTE 13

Surprisingly, research has shown that security awareness training has not had an impact on employee mishandling of sensitive data. The percentage of employees who admit to sending misdirected emails is the highest in organizations that provide security awareness training most frequently. These same employees are almost twice as likely to send company data to their personal email accounts.

One means of securing internal corporate data is through **data loss prevention (DLP)**. DLP is considered as **rights management**, or the authority of the owner of the data to impose restrictions on its use. DLP is a system of security tools used to recognize and identify data critical to the organization and ensure it is protected. This protection involves monitoring who is using the data and how it is being accessed. Critical or confidential data can be tagged as such. A user who attempts to access the data to disclose it to an unauthorized user will be prevented from doing so.

Most DLP systems use *content inspection*. Content inspection is a security analysis of the transaction within its approved context. Content inspection looks at the security level of the data, who is requesting it, where the data is stored, when it was requested, and where it is going. DLP systems also can use *index matching*. Documents that have been identified as needing protection, such as the program source code for a new software application, are analyzed by the DLP system and complex computations are conducted based on the analysis. Thereafter, if even a small part of that document is leaked, the DLP system can recognize the snippet as being from a protected document.

DLP begins with an administrator creating DLP rules based on the data (what is to be examined) and the policy (what to check for). DLPs can be configured to look for specific data (such as Social Security and credit card numbers), lines of computer software source code, words in a sequence (to prevent a report from leaving the network), maximum file sizes, and file types. In addition, whitelists and blacklists can be created to prevent specific files from being scanned. These rules are then loaded into a DLP server.

When a policy violation is detected by the DLP agent, it is reported back to the DLP server. Different actions can then be taken. These could include blocking the data, redirecting it to an individual who can examine the request, quarantining the data until later, or alerting a supervisor of the request.

NOTE 14

One of the drawbacks of DLP is that rules must be continually created and maintained as new employees, third-party agent contractors, and customers are added and new data sets are created. Increasingly, machine learning (ML) is used by DLP to continually create and modify the criteria for protecting data.

In addition to using DLP to protect data, organizations use other techniques as well. Applying encryption can naturally protect the data but may pose barriers for the recipient to decrypt it. When the data is used only for testing purposes, such as determining if a new app functions properly, **masking** may be used. Data masking involves creating a copy of the original data but obfuscating (making unintelligible) any sensitive elements such as a user's name or Social Security number. By replacing the actual information with fictitious information, testing can still be carried out. Similar to masking, **tokenization** obfuscates sensitive data elements, such as an account number, into a random string of characters (*token*). The original sensitive data element and the corresponding token are then stored in a database called a *token vault* so that if the actual data element is needed, it can be retrieved as needed. Unlike encryption, which requires using an algorithm and a key, tokenization can hide the data while making the retrieval process more seamless. Tokenization is illustrated in Figure 9-8.

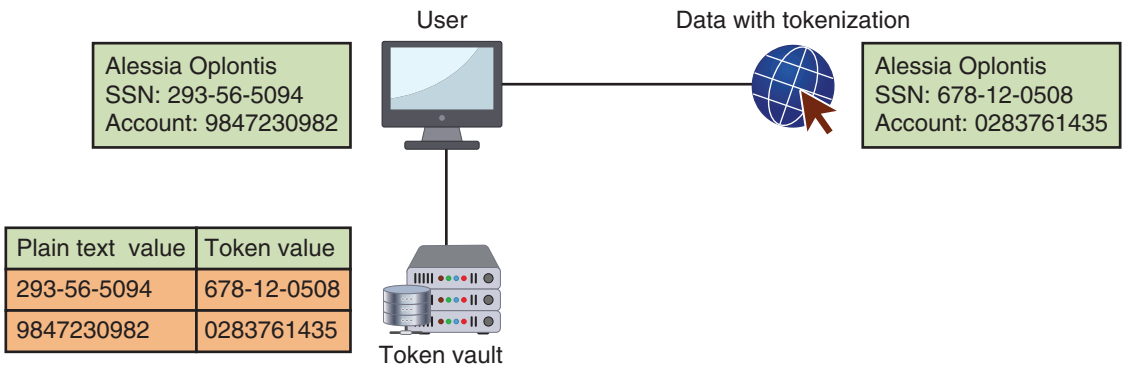


Figure 9-8 Tokenization

CAUTION

Data masking may not always provide strong protection from identifying individuals, even if the user's name or Social Security Number is obfuscated. According to a study of census data, 87 percent of the American population has a unique combination of sex, birth date, and zip code. This means that the combination of these three pieces of information is sufficient to identify a huge portion of the population.

Technologies for Monitoring and Managing

Several security technologies relate to monitoring and managing network resources. These technologies include port security, packet capture and analysis, monitoring services, file integrity monitors, and quality of service.

Port Security

Securing the ports on a network device like a switch or router is essential to securing a network. Threat actors who access a network device through an unprotected port can reconfigure the device to their advantage. This introduces a number of vulnerabilities, one of which is the compromise of **route security** or the trust of packets sent through

a router. False route information can be injected or altered by weak port security that would enable the insertion of individual false route updates or the installation of bogus routers into the routing infrastructure.

In Figure 9-9, computer Alpha, which is connected to Switch A, wants to send frames to computer Beta on Segment 2. Because Switch A does not know where Beta is located, it "floods" the network with the packet (sends it to all destinations). The packet then travels down Segment 1 to Switch B and down Segment 3 to Switch C. Switch B then adds Alpha to its lookup table that it maintains for Segment 1, and Switch C also adds it to its lookup table for Segment 3. Yet if Switch B or C has not yet learned the address for Alpha, they will both flood Segment 2 looking for Beta; that is, each switch will take the packet sent by the other switch and flood it back out again because they still do not know where Beta is located. Switch A then will receive the packet from each segment and flood it back out on the other segment. This *switching loop* causes a *broadcast storm* as the frames are broadcast, received, and rebroadcast by each switch. Broadcast storms can cripple a network in a matter of seconds to the point that no legitimate traffic can occur.

NOTE 15

Because the headers that a Layer 2 switch examines do not have a time to live (TTL) value, a packet could loop through the network indefinitely.

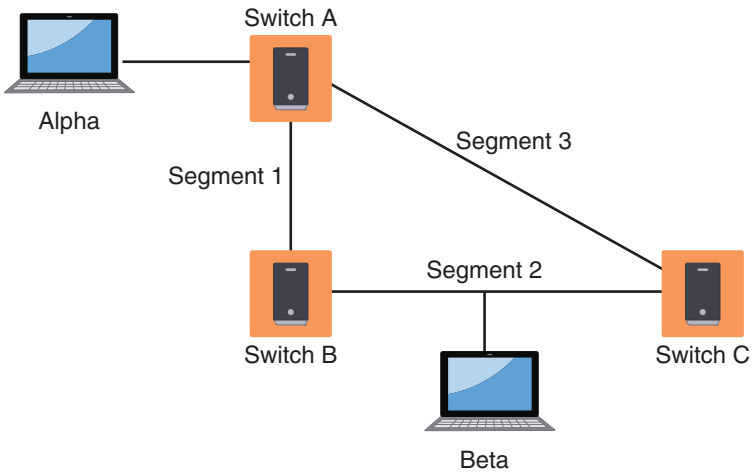


Figure 9-9 Broadcast storm

Broadcast storm prevention can be accomplished by **loop prevention**, which uses the IEEE 802.1d standard *spanning-tree protocol (STP)*. The STP uses an algorithm that creates a hierarchical "tree" layout that spans the entire network. It determines all the redundant paths that a switch has to communicate, recognizes the best path, and then blocks out all other paths. STP does this by sending out *bridge protocol data units (BPDU)* that give information about the switch port (such as MAC address and priority). This enables switches in the STP to share information with other switches. BPDUs are also periodically sent to inform other switches of port changes.

However, threat actors can try to take advantage of the STP by sending out their own malicious BPDUs to the switch to change its configuration. Because BPDUs should only be exchanged between switches, a defense is to enable **BPDU guard**, which is a feature on the switch that creates an alert when a BPDU is received from an endpoint and not a switch. In such an instance, the port on the switch is disabled and no traffic is sent or received by that port.

A BPDU guard in a switch has similar port security protections. *Dynamic Host Configuration Protocol (DHCP)* is a network management protocol that automates the process of configuring an endpoint on IP networks by dynamically assigning an IP address and other network configuration parameters to endpoints. Threat actors may attempt to connect a DHCP server to the network to offer their own IP address to DHCP clients. A switch with **DHCP snooping** drops any DHCP traffic that the switch determines is unacceptable. It also stores information about the incident for further investigation.

NOTE 16

DHCP snooping can also prevent users from connecting a consumer-grade router at their desk that also provides DHCP addresses.

Other port security steps to thwart an attack directed at network devices are summarized in Table 9-4.

Table 9-4 Thwarting attacks through port security

Type of attack	Description	Port security defense
MAC flooding	An attacker can overflow the switch's address table with fake MAC addresses, forcing it to act like a hub, sending packets to all devices.	Use a switch that can close ports with too many MAC addresses.
MAC address spoofing	If two devices have the same MAC address, a switch may send frames to each device. An attacker can change the MAC address on her device to match the target device's MAC address.	Configure the switch so that only one port can be assigned per MAC address.
ARP poisoning	The attacker sends a forged ARP packet to the source device, substituting the attacker's computer MAC address.	Use an ARP detection appliance.
Unauthorized packet capturing	Attackers connect their device to the switch's port.	Secure the switch in a locked room and close all unused ports on the switch.

Packet Capture and Analysis

Capturing packets and performing an analysis are critical for understanding the current state of the network. Analyzing packets helps to monitor network performance and reveal cybersecurity incidents.

Monitoring traffic on switches generally can be done in two ways. A separate **port TAP (test access point)** can be installed. A port TAP transmits the send and receive data streams simultaneously on separate dedicated channels so that all data arrives at the monitoring tool in real time. A port TAP is shown in Figure 9-10.

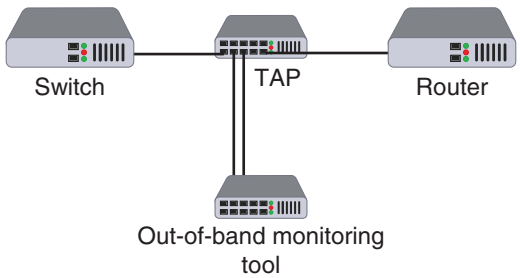


Figure 9-10 Port TAP

A managed switch on an Ethernet network supports **port mirroring**. Port mirroring is also called **port spanning** because it uses a *Switch Port Analyzer* (*SPAN*). Port mirroring allows the administrator to configure the switch to copy (mirror) traffic on some or all ports to a designated monitoring port on the switch. Port mirroring is illustrated in Figure 9-11, where the monitoring tool is connected to the mirror port and can view all network traffic moving through the switch. Port mirroring is designed for "spot checking," while a TAP is best for high-speed networks that have a large volume of traffic.

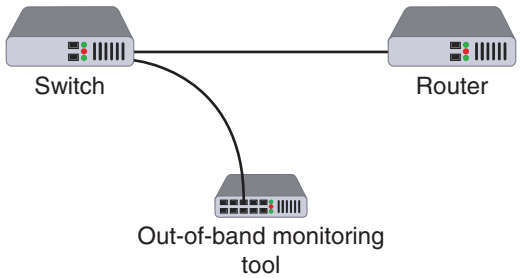


Figure 9-11 Port mirroring

NOTE 17

A TAP device is completely passive: it has no power source or IP or MAC address so that it cannot be attacked. Also, TAPs are "court approved" so that all data captured can be used as evidence in an investigation or trial.

A network TAP is one example of a device that can be placed on a network to gather information. Other devices include **network sensors** to monitor traffic (for network intrusion detection and prevention devices), **collectors** to gather traffic (for SIEM devices), and **aggregators** to combine multiple network connections into a single link.

Monitoring Services

As a supplement to the internal data gathering and analysis of security data, an external third-party **monitoring service** can also be used. These services can provide additional resources to assist an organization in its cybersecurity defenses, such as processing cybersecurity data on managed SIEM platforms and continuously updating and applying rules to detect attacks.

File Integrity Monitors

File integrity monitors are based on a technology designed to "keep an eye on" files to detect any changes within the files that may indicate a cyberattack. After establishing a baseline for "clean" files, a file integrity monitor examines files to see if they have changed, when the change occurred, how they changed, who changed them, and what can be done to restore those files if the changes are unauthorized.

File integrity monitors are used for detecting malware as well as maintaining compliance with industry-specific regulations. The Payment Card Industry Data Security Standard (PCI DSS) has no less than four requirements related to file integrity monitors. The PCI DSS Requirement 10.5.5 states that organizations in compliance will "Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert)."

NOTE 18

PCI DSS is covered in Module 2.

The problem with file integrity monitors is the high volume of "noise," or too much unhelpful information. Files may change frequently for many benign reasons with limited insight into whether a change poses a security risk. While file integrity monitors can be beneficial, they need to provide sufficient insight so that proper actions can be taken.

Quality of Service (QoS)

Modern networks have many types of traffic, all sharing the same bandwidth. However, not all network traffic is the same: a critical video conference call could be sharing the same bandwidth as someone downloading a huge movie file on the same network (in violation of company policy) so that each are competing for the same bandwidth. This often results in packet loss for the video conference call as well as delay and jitter, all of which affects the quality of the call.

Quality of Service (QoS) is a set of network technologies used to guarantee its ability to dependably serve network resources and high-priority applications to endpoints. QoS technologies provide "differentiated" handling and capacity allocation to specific network traffic. A network administrator can assign the order in which packets are handled and the amount of bandwidth given to an application or traffic flow (called traffic shaping).

The first step in QoS is that traffic must be classified or differentiated using QoS tools. Classifying traffic according to the corporate policy allows organizations to ensure the consistency and adequacy of network resources for the most important applications. While traffic can be prioritized by port or IP address, doing so has obvious limitations. (It is unlikely that a specific IP address should always have high network capacity, no matter what activity is being performed.) Instead, traffic should be viewed by the application or user, which can then result in a more meaningful classification of the data.

Almost all firewalls today recognize QoS settings. (They do so through configuring the "Type of Service" eight-bit field within an IP packet that is reserved for QoS markings.) However, some firewalls do not have this level of granularity but still provide QoS by defining "Low," "Medium," "High," and "Guaranteed" ratings to different types of traffic.

Design Technologies

Technologies that relate to the secure design of the network include network segmentation and load balancing.

Network Segmentation

Understanding network segmentation involves first knowing the principle of zero trust. Examples of network segmentation include virtual LANs and a demilitarized zone.

Zero Trust Several principles govern network segmentation. One principle is **zero trust**. Zero trust is a strategic initiative about networks that is designed to prevent successful attacks. As its name implies, zero trust attempts to eliminate the concept of trust from an organization's network architecture.

Many networks are based on a traditional security model that operates on the assumption that everything inside an organization's network should be trusted. This is now considered an outdated and broken trust model because it is assumed that a user's identity has not been compromised and that all users will act responsibly and thus can be trusted.

The zero-trust model recognizes instead that trust is a vulnerability. Once on the network, users can freely move laterally to access or exfiltrate data. Because most networks have already been compromised and threat actors are "lurking in the shadows," malicious attackers likewise can freely move through the network.

There are several steps in creating a zero-trust network architecture:

1. Identify a "protect surface" that is made up of the network's most critical and valuable data, assets, applications, and services. Because it contains only data most critical to an organization's operations, the protect surface is much smaller than the network itself.
2. Determine the entities that interact with the protect surface. This includes determining how traffic moves across the organization in relation to it. **East-west traffic** is the movement of data from one server to another server within a data center. (In contrast, *north-south traffic* describes endpoint-to-server traffic that moves between the data center and an unsecured location outside of the data center network.) Besides understanding traffic across the protect surface, this step involves knowing who the users are that access it, which applications they are using, and how they are connecting to it.
3. Put controls in place as close to the protect surface as possible. This is seen as creating a "microperimeter" around it that "moves" with the protect surface as it grows. A microperimeter is often created by deploying a NGFW to ensure only known and allowed traffic or legitimate applications have access to the protect surface.

Virtual LANs (VLANs) Zero trust requires that networks be segmented. This can be accomplished by using switches to divide the network into a hierarchy. *Core switches* reside at the top of the hierarchy and carry traffic between switches, while *workgroup switches* are connected directly to the devices on the network. It is often beneficial to group similar users together, such as all the members of the Accounting Department. However, grouping by user can be difficult because all users might not be in the same location and served by the same switch.

It is possible to segment a network by separating devices into logical groups. This is known as creating a **virtual LAN (VLAN)**. A VLAN allows scattered users to be logically grouped together even though they are physically attached to different switches. This can reduce network traffic and provide a degree of security. VLANs can be isolated so that sensitive data is transported only to members of the VLAN.

VLAN communication can take place in two ways. If multiple devices in the same VLAN are connected to the same switch, the switch itself can handle the transfer of packets to the members of the VLAN group. However, if VLAN members on one switch need to communicate with members connected to another switch, a special "tagging" protocol must be used, either a proprietary protocol or the vendor-neutral IEEE 802.1Q. These special protocols add a field to the packet that "tags" it as belonging to the VLAN.

NOTE 19

Zero trust is not designed to make a system trusted but, instead, to eliminate trust. The motto of zero trust is "Never trust; always verify."

NOTE 20

Core switches must work faster than workgroup switches because core switches must handle the traffic of several workgroup switches.

NOTE 21

Although network subnetting and VLANs are often considered to be similar, they do have differences. Subnets are subdivisions of IP address classes (Class A, B, or C) and allow a single Class A, B, or C network to be used instead of multiple networks. VLANs are devices that are connected logically rather than physically, either through the port they are connected to or by their MAC address.

NOTE 22

Another security advantage of VLANs is that they can be used to prevent direct communication between servers, which can bypass firewall or IDS inspection. Servers that are placed in separate VLANs will require that any traffic headed toward the default gateway for inter-VLAN routing be inspected.

Demilitarized Zone (DMZ) Imagine a bank that located its automated teller machine (ATM) in the middle of their vault. This would be an open invitation for disaster by inviting every outside user to enter the secure vault to access the ATM. Instead, the ATM and the vault should be separated so that the ATM is in a public area that anyone can access, while the vault is restricted to trusted individuals. In a similar fashion, locating public-facing servers such as web and email servers inside the secure network is also unwise. An attacker must only break out of the security of the server to access the secure network.

NOTE 23

DMZs were first introduced in Module 8 concerning physical security controls.

To allow untrusted outside users access to resources such as web servers, most networks employ a *demilitarized zone (DMZ)*. The DMZ functions as a separate network that rests outside the secure network perimeter: untrusted outside users can access the DMZ but cannot enter the secure network.

Consider Figure 9-4 (shown earlier), which illustrates a DMZ containing a web server and an email server that are accessed by outside users. In this configuration, a single firewall with three network interfaces is used: the link to the Internet is on the first network interface, the DMZ is formed from the second network interface, and the secure internal LAN is based on the third network interface. However, this makes the firewall device a single point of failure for the network. It also must take care of all the traffic to the DMZ and internal network. A more secure approach is to have two firewalls, as seen in Figure 9-12. In this configuration, an attacker would have to breach two separate firewalls to reach the secure internal LAN.

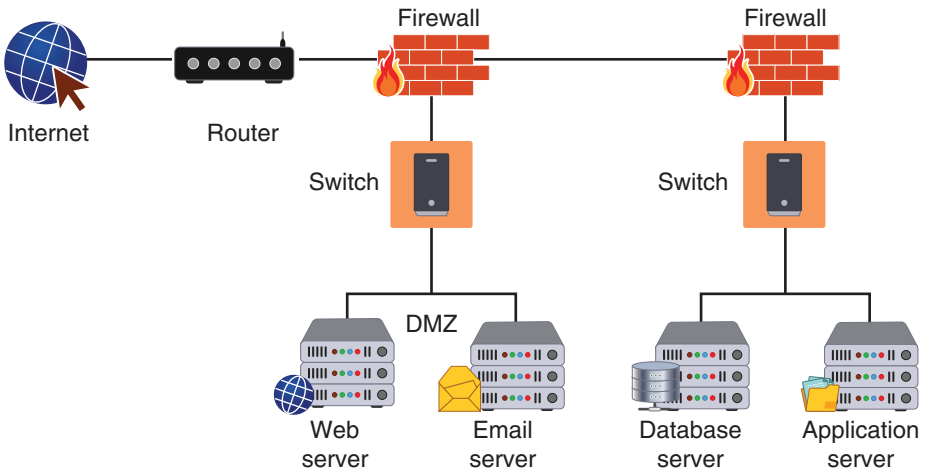


Figure 9-12 DMZ with two firewalls

CAUTION

Some consumer routers advertise support to configure a DMZ. However, this is not a DMZ. Rather, the feature allows only one local device to be exposed to the Internet for Internet gaming or videoconferencing by forwarding all the ports at the same time to that one device.

How should a DMZ be configured so that trusted administrators can still access the hardware and software in a DMZ? If a pathway is enabled for administrators to enter the zone, that same pathway, if compromised, can provide access to threat actors back to the secure network.

A common approach is to use a **jump box** (sometimes called a *jump server* or *jump host*), as shown in Figure 9-13. A jump box is a minimally configured administrator server (either physical or virtual) within the DMZ. Running only essential protocols and ports, it connects two dissimilar security zones while providing tightly restricted access between them. An administrator accesses the jump box, which is connected to the administrative interface of the devices within the DMZ.

CAUTION

To further limit the vulnerabilities of a jump box, administrators should ensure that all jump box software is regularly updated, limit the programs that can run on a jump box, implement multifactor authentication for logins, do not allow outbound access or severely restrict access from the jump box, and use ACLs to restrict access to specific authorized users.

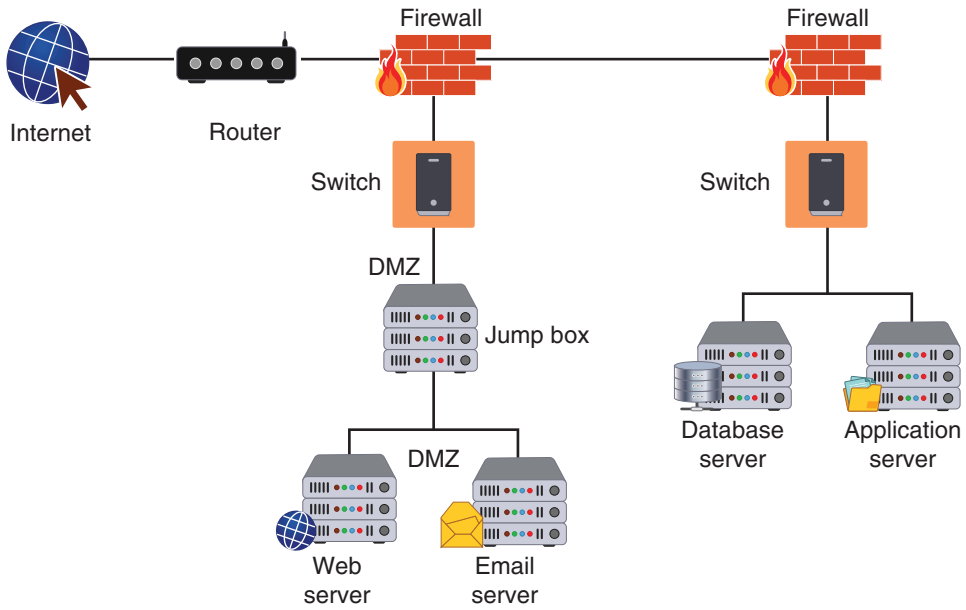


Figure 9-13 Jump box

In recent years, an additional security configuration has been used to limit risks when administering a DMZ. Instead of an administrator connecting to a jump box from any computer, only a dedicated *secure admin workstation (SAW)* can be used to connect to the jump box. Using a SAW prevents an administrator's infected computer from compromising the jump box.

Other zones can also be used for security. These are listed in Table 9-5.

Table 9-5 Other network zones

Name	Description	Security benefits
Intranet	A private network that belongs to an organization that can only be accessed by approved internal users	Closed to the outside public, thus data is less vulnerable to external threat actors
Extranet	A private network that can also be accessed by authorized external customers, vendors, and partners	Can provide enhanced security for outside users compared to a publicly accessible website
Guest network	A separate open network that anyone can access without prior authorization	Permits access to general network resources like web surfing without using the secure network

Load Balancing

Load balancing is a technology that can help to evenly distribute work across a network. Requests that are received can be allocated across multiple devices such as servers. To the user, this distribution is transparent and appears as if a single server is providing the resources. Load-balancing technology reduces the probability of overloading a single server and ensures that each networked server benefits from having optimized bandwidth. Load balancing can be performed either through software running on a computer or as a dedicated hardware device known as a *load balancer*.

Different **scheduling** protocols are used in load balancers. In a *round-robin* scheduling protocol, the rotation applies to all devices equally. A scheduling protocol that distributes the load based on which devices can handle the load more efficiently is known as *affinity* scheduling. Affinity scheduling may be based on which load balancers have the least number of connections at a given point in time.

When multiple load balancers are used together to achieve *high efficiency (H/A)*, they can be placed in different configurations. In an **active-passive** configuration, the primary load balancer distributes the network traffic to the most suitable server, while the secondary load balancer operates in a "listening mode." This second load balancer constantly monitors the performance of the primary load balancer and will step in and take over the load-balancing duties should the primary load balancer start to experience difficulties or fail. The active-passive configuration allows

NOTE 24

Load balancers in an active-active configuration can also remember previous requests from users and retain this information. If the user returns and requests the same information, the user is directed to the load balancer that previously served the request, and the information can be immediately provided.

for uninterrupted service and can also handle planned or unplanned service outages. In an **active-active** configuration, all load balancers are always active. Network traffic is combined, and the load balancers then work together as a team.

The servers behind load balancers are often given a **virtual IP (VIP)** address. As its name suggests, this is not an actual IP address. Instead, it is an IP address and a specific port number that can be used to reference physical servers. A VIP with the address and port *172.32.250.1:80* can be configured to accept one type of traffic, while the VIP *172.32.250.1:443* can accept another type of traffic. Multiple VIPs can be created using the same IP address as long as a different port number is used.

Load balancing can also support session **persistence**, a process in which a load balancer creates a link between an endpoint and a specific network server for the duration of a session. This can help improve the user experience and optimize network resource usage.

Using a load balancer has security advantages. Because load balancers generally are located between routers and servers, they can detect and stop attacks directed at a server or application. A load balancer can also detect and prevent protocol attacks that could cripple a single server. Some load balancers can hide HTTP error pages or remove server identification headers from HTTP responses, denying attackers additional information about the internal network.

TWO RIGHTS & A WRONG

1. There are two types of ACLs: filesystem ACLs filter access to files and directories on an endpoint, and networking ACLs filter access to a network. Network ACLs are often found on routers.
2. The Layer 2 Tunneling Protocol (L2TP) is a VPN protocol that does not offer any encryption or protection, so it is usually paired with IPsec.
3. Tokenization is used for creating test data.

See Appendix B for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in the Practice It folder in each MindTap module.

SUMMARY

- Today, networks have both standard networking devices and specialized security appliances. Security can be achieved by using security appliances that directly address security and by using the security features found in standard networking devices. Using both standard networking devices and security appliances can result in a layered security approach, which can significantly improve security.
- A computer firewall is designed to limit the spread of malware. A firewall uses bidirectional inspection to examine outgoing and incoming network packets, allowing approved packets to pass through but taking different actions when it detects a suspicious packet. The actions are based on specific criteria or rules. Older firewalls often processed each rule as a separate instruction in sequence, while modern firewalls allow a priority order. In addition to filtering based on packets, firewalls can also apply content/URL filtering.
- Stateless packet filtering on a firewall looks at a packet and permits or denies it based solely on the firewall rules. Stateful packet filtering uses both the firewall rules and the state of the connection. Open source firewalls are freely available; other firewalls are owned by an entity that has an exclusive right to them and are called proprietary firewalls. A software firewall runs as a program or service on a device, such as a computer or router. Hardware firewalls are specialized separate devices that inspect traffic. A host-based firewall is a

software firewall that runs on and protects a single endpoint device (a host). An appliance firewall is typically a separate hardware device designed to protect an entire network. A virtual firewall is one that runs in the cloud.

- There are several specialized firewall appliances. A web application firewall (WAF) looks at applications using HTTP. A network address translation gateway is a cloud-based technology that performs NAT translations for cloud services. A next generation firewall (NGFW) has additional functionality beyond a traditional firewall. Unified threat management (UTM) is a device that combines several security functions. These include packet filtering, antispam, antiphishing, antispyware, encryption, intrusion protection, and web filtering.
- A forward proxy is a computer or an application program that intercepts user requests from the internal secure network and then processes these requests on behalf of the user. A reverse proxy routes requests coming from an external network to the correct internal server. Acting as the intermediary, a proxy server can provide a degree of protection.
- A honeypot is a computer located in an area with limited security that serves as "bait" to threat actors. The honeypot is intentionally configured with security vulnerabilities so that it is open to attacks. A high-interaction honeypot is usually configured with a default login and loaded with software, data files that appear to be authentic but are actually imitations of real data files called honeyfiles, and fake telemetry data. A honeynet is a network set up with intentional vulnerabilities. A sinkhole is essentially a "bottomless pit" designed to steer unwanted traffic away from its intended destination to another device. One type of sinkhole is a DNS sinkhole.
- An intrusion detection system (IDS) can detect an attack as it occurs, while an intrusion prevention system (IPS) attempts to block the attack. An inline system is connected directly to the network and monitors the flow of data as it occurs. A passive system is connected to a port on a switch, which receives a copy of network traffic. Monitoring involves examining network traffic, activity, transactions, or behavior to detect security-related anomalies. The four monitoring methodologies are anomaly-based monitoring, signature-based monitoring, behavior-based monitoring, and heuristic monitoring. A network intrusion detection system (NIDS), similar to a software-based host intrusion detection system (HIDS), watches for attacks on the network. A network intrusion prevention system (NIPS) not only monitors to detect malicious activities but also attempts to stop them.
- A network hardware security module is a special trusted network computer that performs cryptographic operations such as key management, key exchange, onboard random number generation, key storage facility, and accelerated symmetric and asymmetric encryption. These security appliances must be properly configured. Not only does a misconfigured device allow threat actors an opening into the network, it also provides a false sense of security that makes it difficult to realize the problem.
- An access control list (ACL) contains rules that administer the availability of digital assets by granting or denying access to the assets. On external routers that face the Internet, router ACLs can restrict known vulnerable protocols from entering the network. Router ACLs can also be used on internal routers that process interior network traffic. These router ACLs usually are less restrictive but more specific than those on external routers ACLs since the devices on the internal network are generally considered to be friendly. A virtual private network (VPN) is a security technology that enables authorized users to use an unsecured public network, such as the Internet, as if it were a secure private network. It does this by encrypting all data that is transmitted between the remote endpoint and the network.
- Network access control (NAC) examines the current state of an endpoint before it can connect to the network. Any device that does not meet a specified set of criteria, such as having the most current antivirus signature or the software firewall properly enabled, is denied access to the network, given restricted access to computing resources, or connected to a "quarantine" network where the security deficiencies are corrected. Some NAC systems use software installed on endpoints (agents), while other systems are agentless and do not require additional software to be installed.
- Data loss prevention (DLP) is a system of security tools used to recognize and identify data critical to the organization and ensure that it is protected. This protection involves monitoring who is using the data and how it is being accessed. Data that is considered critical to the organization or is confidential can be tagged as such. A user who attempts to access the data to disclose it to an unauthorized user will be prevented from doing so. In addition to using DLP to protect data, masking may be used. Data masking involves creating a copy of the original data but obfuscates (makes unintelligible) any sensitive elements such as a user's name or Social Security number. By replacing the actual information with fictitious information, the testing can still be carried out. Similar to masking, tokenization obfuscates sensitive data elements, such as an account number, into a random

string of characters (token). The original sensitive data element and the corresponding token are then stored in a database called a token vault so that if the actual data element is needed, it can be retired as needed.

- Broadcast storm prevention can be accomplished by loop prevention, which uses the IEEE 802.1d standard spanning-tree protocol (STP). The STP uses an algorithm that creates a hierarchical "tree" layout that "spans" the entire network. It determines all the redundant paths that a switch has to communicate, recognizes the best path, and then blocks all other paths. STP sends out bridge protocol data units (BPDUs) that give information about the switch port to enable switches in the STP to share information with other switches. A threat actor can try to take advantage of the STP by sending out their own malicious BPDUs to the switch to change its configuration. Such an attack can be thwarted by a BPDU guard, which is a feature on the switch that creates an alert when a BPDU is received from an endpoint and not a switch.
- Monitoring traffic on switches generally can be done in two ways. A separate port TAP (test access point) can be installed. A TAP transmits the send and receive data streams simultaneously on separate dedicated channels so that all data arrives at the monitoring tool in real time. A managed switch on an Ethernet network supports port mirroring, also called port spanning. Port mirroring allows the administrator to configure the switch to copy (mirror) traffic that occurs on some or all ports to a designated monitoring port on the switch. As a supplement to the internal data gathering and analysis of security data, an external third-party monitoring service can also be used. File integrity monitors are based on a technology designed to "keep an eye on" files to detect any changes within the files that may indicate a cyberattack. After establishing a baseline for "clean" files, a file integrity monitor examines files to see if they have changed, when the change occurred, how they changed, who changed them, and what can be done to restore those files if the changes are unauthorized. Quality of Service (QoS) is a set of network technologies used to guarantee a network's ability to dependably serve resources and high-priority applications to endpoints. Almost all firewalls today recognize QoS settings. Load balancing is a technology that can help to evenly distribute work across a network.

Key Terms

access control list (ACL)
active-active
active-passive
agentless
agents
aggregators
always-on VPN
anomaly monitoring
appliance firewall
baseline configuration
behavioral monitoring
BPDU guard
broadcast storm prevention
collectors
content/URL filtering
data loss prevention (DLP)
DHCP snooping
diagram
DNS sinkhole
east-west traffic
extranet
fake telemetry
file integrity monitors
firewall
forward proxy
full tunnel
geographical consideration
hardware firewall
heuristic monitoring
honeyfiles
honeynet
honeypot
host-based firewall
HTML 5
inline
Internet Protocol schema
intranet
jump box
Layer 2 Tunneling Protocol (L2TP)
load balancing
loop prevention
masking
monitoring service
network access control (NAC)
network address translation gateway
network hardware security module
network intrusion detection system (NIDS)
network intrusion prevention system (NIPS)
network sensors
next generation firewall (NGFW)
open source firewall
out-of-band management
passive
persistence
port mirroring (port spanning)
port TAP (test access point)
proprietary firewall
Quality of Service (QoS)
remote access VPN
reverse proxy
rights management
route security
scheduling
signature-based monitoring
site-to-site VPN
software firewall
split tunneling
standard naming conventions
stateful packet filtering
stateless packet filtering
tokenization
unified threat management (UTM)
virtual firewall
virtual IP (VIP)
virtual LAN (VLAN)
virtual private network (VPN)
web application firewall
zero trust

Review Questions

1. Which of the following is NOT a firewall rule parameter?
   a. Visibility
   b. Time
   c. Context
   d. Action

2. Which firewall rule action implicitly denies all other traffic unless explicitly allowed?
   a. Force Allow
   b. Force Deny
   c. Bypass
   d. Allow

3. Leah is researching information on firewalls. She needs a firewall that allows for more generic statements instead of creating specific rules. What type of firewall should Leah consider purchasing that supports her need?
   a. Content/URL filtering firewall
   b. Policy-based firewall
   c. Hardware firewall
   d. Proprietary firewall

4. Emilie is reviewing a log file of a new firewall. She notes that the log indicates packets are being dropped for incoming packets for which the internal endpoint did not initially create the request. What kind of firewall is this?
   a. Stateful packet filtering
   b. Connection-aware firewall
   c. Proxy firewall
   d. Packet filtering firewall

5. What is a virtual firewall?
   a. A firewall that runs in the cloud
   b. A firewall that runs in an endpoint virtual machine
   c. A firewall that blocks only incoming traffic
   d. A firewall appliance that runs on a LAN

6. Which of these appliances provides the broadest protection by combining several security functions?
   a. NAT
   b. WAF
   c. UTM
   d. NGFW

7. Which of the following contains honeyfiles and fake telemetry?
   a. High-interaction honeypot
   b. Attacker-interaction honeypot
   c. Honeypotnet
   d. Honeyserver

8. Maja has been asked to investigate DDoS mitigations. Which of the following should Maja consider?
   a. DDoS Prevention System (DPS)
   b. DNS sinkhole
   c. MAC pit
   d. IP denier

9. Which type of monitoring methodology looks for statistical deviations from a baseline?
   a. Behavioral monitoring
   b. Signature-based monitoring
   c. Anomaly monitoring
   d. Heuristic monitoring

10. Which statement regarding a demilitarized zone (DMZ) is NOT true?
    a. It can be configured to have one or two firewalls.
    b. It typically includes an email or web server.
    c. It provides an extra degree of security.
    d. It contains servers that are used only by internal network users.

11. Which of the following functions does a network hardware security module NOT perform?
    a. Fingerprint authentication
    b. Key management
    c. Key exchange
    d. Random number generator

12. Which of these is NOT used in scheduling a load balancer?
    a. The IP address of the destination packet
    b. Data within the application message itself
    c. Round-robin
    d. Affinity

13. In which of the following configurations are all the load balancers always active?
    a. Active-active
    b. Active-passive
    c. Passive-active-passive
    d. Active-load-passive-load

14. Which device intercepts internal user requests and then processes those requests on behalf of the users?
    a. Forward proxy server
    b. Reverse proxy server
    c. Host detection server
    d. Intrusion prevention device

15. Sofie needs to configure the VPN to preserve bandwidth. Which configuration would she choose?
    a. Narrow tunnel
    b. Split tunnel
    c. Full tunnel
    d. Wide tunnel

16. Which of the following is not a basic configuration management tool?
    a. Baseline configuration
    b. Standard naming convention
    c. Diagrams
    d. MAC address schema

17. Which of the following is NOT correct about L2TP?
    a. It is used as a VPN protocol.
    b. It must be used on HTML 5 compliant devices.
    c. It does not offer encryption.
    d. It is paired with IPsec.

18. Which of the following is NOT a NAC option when it detects a vulnerable endpoint?
    a. Deny access to the network.
    b. Give restricted access to the network.
    c. Update Active Directory to indicate the device is vulnerable.
    d. Connect to a quarantine network.

19. Hanna has received a request for a data set of actual data for testing a new app that is being developed. She does not want the sensitive elements of the data to be exposed. What technology should she use?
    a. Masking
    b. Tokenization
    c. Data Object Obfuscation (DOO)
    d. PII Hiding

20. How does BPDU guard provide protection?
    a. It detects when a BPDU is received from an endpoint.
    b. It sends BPDU updates to all routers.
    c. BPDUs are encrypted so that attackers cannot see their contents.
    d. All firewalls are configured to let BPDUs pass to the external network.

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 9-1: Using GlassWire Firewall

Time Required: 25 minutes
Objective: Given a scenario, implement secure network designs.
Description: GlassWire is a firewall and Security and Information Event Management (SIEM) product. In this activity, you will download and install GlassWire.

1. Use your web browser to go to **www.glasswire.com**. (If you are no longer able to access the site through the URL, use a search engine to search for "GlassWire.")
2. Click **Features** and scroll through the page to read about the different features and configuration options in this product.
3. Click **FREE DOWNLOAD** and then click **DOWNLOAD GLASSWIRE** to download the file.
4. Navigate to the location of the downloaded file **GlassWireSetup.exe** and launch this program to install GlassWire by accepting the default settings.
5. Click **Finish** to run GlassWire.
6. Note that the information scrolls horizontally to the left regarding events that are occurring. Open a web browser and surf the Internet for several minutes.
7. Return to GlassWire.
8. Slide the scroller at the bottom of the screen to consolidate the views.
9. Click **Apps**. What information is given in the left pane? How can this be useful?
10. Click **Traffic** to view an analysis of the different traffic types.

11. Open a web browser, and then arrange the GlassWire window and the browser window side by side on your computer screen.
12. Use your web browser to surf the web, and watch the GlassWire screen as well. What can you learn from this?
13. Close the browser window and maximize GlassWire.
14. Click the **Firewall** button. What apps or services have recently gone through your firewall?
15. Click the **Usage** button to see a summary of the local Apps utilized, the Hosts accessed, and the Traffic Type.
16. Click **Alerts**. Scroll through any alerts that have been issued. What can you tell about them?
17. How valuable is this information from GlassWire?
18. Close all windows.

Project 9-2: Configuring Microsoft Windows Defender Firewall—Apps

Time Required: 20 minutes
Objective: Given a scenario, implement secure network designs.
Description: In this project, you explore configuration settings on Windows Firewall for allowing an app to penetrate the firewall.

NOTE 25

Windows Firewall uses three different profiles: domain (when the computer is connected to a Windows domain), private (when connected to a private network, such as a work or home network), and public (used when connected to a public network, such as a public Wi-Fi). A computer may use multiple profiles so that a business laptop computer may use the domain profile at work, the private profile when connected to the home network, and the public profile when connected to a public Wi-Fi network. Windows asks whether a network is public or private when you first connect to it.

1. Click **Start** and then **Settings**.
2. Click **Update & Security**.
3. Click **Windows Security**.
4. Click **Firewall & network protection**.
5. Click **Allow an app through firewall**. Depending upon your network configuration, click the type of network that says **(active)**.
6. The Microsoft Windows Defender host-based firewall is application-centric: users can create an opening in the firewall for each specific application. This is more secure than permanently opening a port in the firewall that will always remain open as opposed to a port that is only opened when the application requires it and is then closed. However, there is an issue with these types of firewalls in that installed apps routinely give themselves permissions through the firewall without making that clear to the user. Scroll down through the apps that have access through the firewall. Does this lengthy list surprise you? What are the security risks?
7. Click **Microsoft Lync**.
8. Click **Details**.
9. Click **Network Types** and read through the options. Why would an app be approved for one type but not the other?
10. Click **Cancel**.
11. Click **What are the risks of unblocking an app?** What type of information is provided? How helpful is this information? How could it be improved?
12. Close the browser window.
13. Click **Cancel**.
14. Now add an app that can penetrate the firewall. Click **Allow another app**.
15. See the apps that have been installed on this computer by clicking **Browse**.
16. Scroll down and select an app and click **Open**.
17. Click **Network Types**. For this app, which network type would you select? Why?
18. Click **Cancel**.
19. Click **Cancel** on the **Add an app** window.
20. Click **Cancel** on the **Allow apps to communicate through Windows Defender Firewall**.
21. Close all windows.

Project 9-3: Configuring Microsoft Windows Defender Firewall—Ports

Time Required: 20 minutes
Objective: Given a scenario, implement secure network designs.
Description: In this project, you explore configuration settings on Windows Firewall for opening a port on the firewall.

1. Click **Start** and then **Settings**.
2. Click **Update & Security**.
3. Click **Windows Security**.
4. Click **Firewall & network protection**.
5. Click **Advanced settings**.
6. In the **Windows Defender Firewall with Advanced Security** window, click **Inbound Rules** in the left pane. Expand the screen so you can see all of the columns.
7. Why do some apps have **Any** for **Protocol**, **Local Port**, and **Remote Port** while other apps are more restrictive for these parameters?
8. Click **Outbound Rules** and view the same parameters.
9. Create a specific rule to open a firewall port. Click **Outbound Rules** in the left pane.
10. In the right pane, notice the different ways in which a firewall filter can be created. What is the advantage of **Filter by Profile**?
11. Click **New Rule**.
12. Note that there are four types of rules that can be created. Click **Custom** and then **Next**.
13. A custom rule can apply to all programs, a specific program, or a Windows service. Click **Customize** next to **Services**.
14. Click **Apply to this service** and scroll through the list of available services.
15. Click **Cancel**.
16. Be sure that **All programs** is selected, and click **Next**.
17. Specific ports and protocols can be selected for this rule. Under **Protocol type**, select **TCP**. Note the **Protocol number** is automatically selected.
18. In **Local port**, select **Specific Ports**.
19. Enter **80**.
20. In **Remote port**, select **All ports**, if necessary.
21. Click **Next**.
22. Under **Which local IP addresses does this rule apply to?** click **These IP addresses**.
23. Click **Add**.
24. Click **This IP address range**.
25. In **From**, enter **192.168.0.0**.
26. In **To**, enter **192.168.0.255** and click **OK**.
27. Click **Next**.
28. Read through the three options for actions. Be sure that **Block the connection** is selected. Click **Next**.
29. Read through the three options for when this rule applies. Click **Next**.
30. A name can be given to this rule. However, click the back button and review each of the settings that were created for this rule. What type of rule have you just created? What will it block? Why?
31. Click **Cancel** and close all windows.

Case Projects

Case Project 9-1: Data Loss Prevention Comparison

Research at least four different data loss prevention (DLP) products from four different vendors. Create a table that compares at least six different functions and options. Based on your research, which would you choose? What features make this product the optimum? Why? Write a short paragraph that summarizes your research.

Case Project 9-2: Cloud-Based Honeypots

Research cloud-based honeypots. What are their advantages? What are their disadvantages? When should they not be used? How could one be set up? Create a one-page paper of your research.

Case Project 9-3: Hardening a Jump Box

How should a jump box be configured? Create a list of configurations that you would use to set up a jump box that had the fewest risks.

Case Project 9-4: Researching Network Access Control

Use the Internet to research the network access control products from Microsoft and Cisco. How are they different? How are they similar? What are some of the options for each product? Which would you choose, and why? Write a one-page paper on your research.

Case Project 9-5: UTM Comparison

Create a table of four UTM devices available today. Include the vendor name, pricing, a list of features, the type of protections it provides, etc. Based on your research, assign a value of 1–5 (from lowest to highest ranking) that you would give that UTM. Include a short explanation of why you gave it that ranking.

Case Project 9-6: Zero Trust

Use the Internet to research zero trust. What is it? What are its advantages? What are its disadvantages? What technologies does it require? Is it a long-term security solution? Is it widely accepted? What do you think about it? Write a one-page paper on your research.

Case Project 9-7: Network Firewall Comparison

Use the Internet to identify three network firewalls and create a chart that compares their features. Note if they are rule based or policy based, perform stateless or stateful packet filtering, what additional features they include (IDS, content filtering, etc.), their costs, etc. Which would you recommend? Why?

Case Project 9-8: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to log in, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and click on **Security+ Case Projects (7th edition)**. Read the following case study.

Some schools and libraries use Internet content filters to prohibit users from accessing undesirable websites. These filters are designed to protect individuals, but some claim it is a violation of their freedom. What are your opinions about Internet content filters? Do they provide protection for users or are they a hindrance? Who should be responsible for determining which sites are appropriate and which are inappropriate? And what punishments should be enacted against individuals who circumvent these filters? Visit the Community Site discussion board and post how you feel about Internet content filters.

Case Project 9-9: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

Believe It's Magic (BIM) is a regional hair salon with retail outlets in major cities. Because the company was the victim of several recent attacks, BIM wants to completely change its network infrastructure. Currently, the company has a small IT staff, so they have contracted with North Ridge to make recommendations and install the new equipment. First,

however, they have asked North Ridge to give a presentation to their executive staff about the current state of network security defenses.

1. Create a PowerPoint presentation for the executive staff about network security appliances. Include firewalls, proxy servers, IDS and IPS, and network hardware security modules. Your presentation should contain at least 10 slides.
2. One of the BIM's executives has heard about honeypots and has decided BIM should install it to, in his words, "punish those attackers." North Ridge has advised BIM that the purpose of a honeypot is not retaliation, but the executive has been difficult to persuade. However, he saw your presentation and was impressed with your knowledge. North Ridge has asked you to create a memo about deception instruments and why it could be risky and unnecessary for BIM to install those devices. Create a memo that outlines the advantages and disadvantages of deception instruments, and give your recommendation.

References

1. Boddy, Matt, "Exposed: Cyberattacks on cloud honeypots," *Sophos*, Apr. 9, 2019, accessed Jun. 5, 2019, *www.sophos.com/en-us/press-office/press-releases/2019/04/cybercriminals-attack-cloud-server-honeypot-within-52-seconds.aspx*.
2. "The state of data loss prevention 2020: What you need to know," *Tessian*, May 28, 2020, accessed Jun. 26, 2020, *www.tessian.com/blog/the-state-of-data-loss-prevention-2020-what-you-need-to-know/*.

MODULE 10

CLOUD AND VIRTUALIZATION SECURITY

After completing this module, you should be able to do the following:

1. Define the cloud and explain how it is used and managed
2. Explain virtualization
3. Describe cloud and virtualization security controls
4. List different secure network protocols

Front-Page Cybersecurity

"Our data center is underwater." Any system administrator who received this message would immediately go into panic mode, thinking that a flash flood or burst water pipe had ruined the enterprise's networking equipment and servers. Yet an underwater data center is exactly what Microsoft created in support of cloud computing—and all for good reason.

In 2018, Microsoft announced that it had intentionally sunk its first waterproof and self-sustaining data center. The data center, which now rests more than 100 feet (30.4 meters) beneath the ocean's surface near the Orkney Islands in Scotland, is about the size of a shipping container but shaped like a tube. It is loaded with 12 racks that contain 864 servers and is anchored to the seabed by a large triangular weight. Called Project Natick, the data center is the culmination of four years of research.

Why would anybody sink a data center to the bottom of the ocean? There are several reasons:

Time. The amount of time to build a data center on land usually takes about two years. However, a submersible data center can be fitted and sunk in only 90 days.

Temperature. One of the biggest costs of running a land-based data center is cooling: hundreds of servers generate large amounts of heat. Data centers or rooms that house this equipment typically have special cooling requirements: not only do they need additional cooling; they also need more precise cooling. This requires expensive heating, ventilation, and air conditioning (HVAC) systems. However, the floor of the ocean is naturally cool, so no additional cooling equipment is needed.

Protection. A data center on the bottom of the ocean is protected from any number of natural and man-made disasters: fires, floods, hurricanes, and wars, just to name a few. The risk of theft is decreased as well.

Energy. The naturally occurring ocean waves have been used to harvest renewable "tidal energy." The Orkney Islands are home to the European Marine Energy Center (EMEC), which uses tidal energy and wind energy to generate enough power for the 10,000 inhabitants of the islands, also powers Project Natick.

Location. More than half of the world's population lives within about 120 miles of a coastline. By putting data centers in bodies of water near coastal cities, data has a shorter distance to travel to reach users, leading to fast and smooth web surfing, video streaming, and game playing.

Project Natick may be the start of the next generation of cloud data centers. Microsoft, which has more than 160 cloud data centers around the world for its Azure cloud computing platform, could much more quickly and easily add submarine centers as needed. For now, Microsoft says that data from its first underwater data center continues to be evaluated to determine if this is the wave (pun intended) of the future.

Consider how we give input to a device. The original terminals to computer systems had integrated keyboards so that the terminal and monitor were a single unit. Moving the keyboard to make it easier to type required moving the entire terminal, often resulting in the keyboard being in the right place but not the monitor. Over time, keyboards were separated as detached units connected by a cable. Today keyboards are usually wireless devices that can be freely moved with no restrictions.

Another means by which we give input to a device today is through speech. Instead of typing, we simply speak the command. It is both faster and easier than typing on a keyboard.

Comparing these two input technologies—keyboards and speech—helps to illustrate how some changes to technology are *evolutionary* while others are *revolutionary*. The changes to keyboards from being integrated into a terminal to a wireless device show a technological evolution. But going from typing a command on a keyboard to speaking it is a revolution because it is an entirely radical and completely different way to input data.

Many technology changes are gradual and evolutionary. However, fewer changes are considered as monumental and revolutionary. In computer networking, the move to virtualization, in which hardware is created as software, is often considered as an evolutionary technology that first began in the 1960s. The move to cloud computing is considered revolutionary because it is a completely different way of providing and paying for computing and network resources.

In this module, you will explore cloud computing and virtualization. You will examine these technologies, how they function, and how they can be secured. Because cloud computing relies on secure network connections, you will also look at secure network protocols.

CLOUD SECURITY

CERTIFICATION

2.2 Summarize virtualization and cloud computing concepts.

3.6 Given a scenario, apply cybersecurity solutions to the cloud.

Understanding cloud security involves an overall introduction to cloud computing. It also means taking specific steps to secure the cloud computing environment.

Introduction to Cloud Computing

Understanding cloud computing involves knowing what cloud computing is; identifying the types of clouds, cloud locations, architectures, and cloud models; and knowing how cloud computing is managed.

What Is Cloud Computing?

Forty years ago, as computing technology became widespread, enterprises employed an on-premises model, in which they purchased all the hardware and software necessary to run their organizations. As more resources were needed, more purchases were made, and more personnel were hired to manage the technology.

Because this resulted in spiraling costs, some enterprises turned to *hosted services*. In a hosted services environment, servers, storage, and the supporting networking infrastructure were shared by multiple enterprises over a

remote network connection that had been contracted for a specific period. As more resources were needed (such as additional storage space or computing power), the enterprise contacted the hosted service and negotiated a fee as well as signed a contract for those new services.

Today an entirely new approach for computing has gained widespread use. This approach is known as **cloud computing**. Although various definitions of cloud computing have been proposed, the definition from the National Institute of Standards and Technology (NIST) may be the most comprehensive: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1] In some ways, cloud computing is similar to a corporate data center but at a different scale because it supports multiple tenants online while providing rapid and even automatic scalability and elasticity. Entities that offer cloud computing are called **cloud service providers**.

Cloud computing takes a much more flexible approach to computing resources. All cloud resources are available online so that users from virtually anywhere around the world can access them. Access is achieved simply through opening a web browser without needing to install additional software. Cloud computing allows an almost endless array of servers, software, and network appliances to be quickly and easily configured as needed. It is also a pay-per-use computing model in which customers pay only for the online computing resources they need. As computing needs increase or decrease, cloud computing resources can be quickly scaled up or scaled back. Cloud computing is illustrated in Figure 10-1. Table 10-1 lists the advantages of cloud computing.

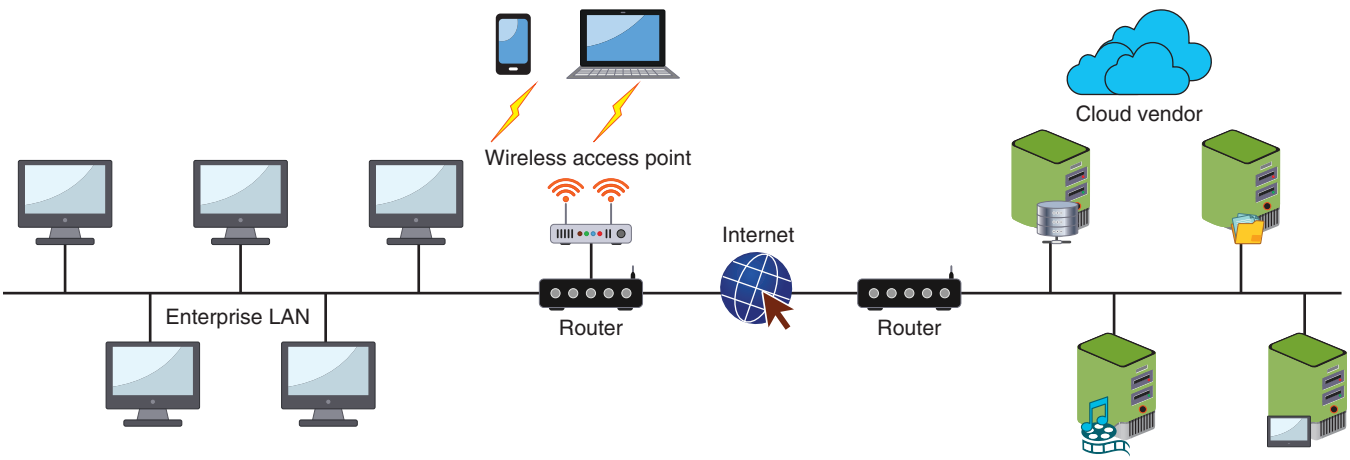


Figure 10-1 Cloud computing

Table 10-1 Cloud computing advantages

Characteristic	Explanation
On-demand self-service	The consumer can make changes, such as increasing or decreasing computing resources, without requiring human interaction from the service provider.
Universal client support	Virtually any networked device (desktop, laptop, smartphone, or tablet, for example) can access the cloud computing resources.
Invisible resource pooling	Physical and virtual computing resources are pooled together to serve multiple, simultaneous consumers that are dynamically assigned or reassigned based on the consumers' needs; the customer has little or no control or knowledge of the physical location of the resources.
Immediate elasticity	Computing resources can be increased or decreased quickly to meet demands.
Metered services	Fees are based on the computing resources used.

One of the attractive features of cloud computing is cost savings. The savings available through cloud computing are due to the following factors:

- *Elasticity and scalability.* Cloud computing gives organizations the ability to expand and reduce resources according to specific service requirements. Users can create an ongoing infrastructure or provision any number of resources only for a specific task. For example, an e-commerce site may provision multiple servers to accommodate a large number of orders during the holiday season and then drop those resources after the holidays, when they are no longer needed.
- *Pay-per-use.* Organizations pay for cloud services when they are used, either for the short term (for computing power for one day or several months) or for a longer duration (for using cloud-based storage).
- *On demand.* Because cloud services are only activated when needed, they are not permanent parts of an IT infrastructure. This means that hardware and software do not need to be purchased and installed, and IT staffing needs are also reduced.
- *Resiliency.* The resiliency of cloud services can completely isolate the failure of a server and storage resources from cloud users. If an issue occurs, the cloud provider will migrate the hardware and software to a different resource in the cloud without the user's knowledge. This relieves the organization from needing to have excess capacity sitting idle that can only to be used in an emergency.

NOTE 1

Cloud computing involves shifting the bulk of the costs from *capital expenditures* (CapEx)—or purchasing and installing servers, storage, networking, and related infrastructure to *operating expenses* (OpEx) in which the costs are only for the usage of these of resources. In some ways, this is similar to the savings from using a ride-hailing service such as Uber or Lyft to pay for transportation only when needed instead of purchasing, maintaining, and insuring a car.

Types of Clouds

There are different types of clouds. A **public cloud** is one in which the services and infrastructure are offered to all users with access provided remotely through the Internet. Unlike a public cloud that is open to anyone, a **community cloud** is open only to specific organizations that have common concerns. For example, because of the strict data requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a community cloud open only to hospitals may be used. A **private cloud** is created and maintained on a private network. Although this type offers the highest level of security and control (because the company must purchase and maintain all the software and hardware), it also reduces cost savings. A **hybrid cloud** is a combination of public and private clouds.

Locations

The introduction of cloud computing has redefined the location of computing resources. Computing now takes place in several locations. These are listed in Table 10-2 and illustrated in Figure 10-2.

Table 10-2 Computing locations

Location	Description	Example
On-premises	Computing resources located on the campus of the organization	Desktop computer, local area network, data center
Off-premises	A computing resource hosted and supported by a third party	Remote backup facility
Fog	A decentralized computing infrastructure in which data, compute capabilities, storage, and applications are located between the data source and the cloud	Automated guided vehicles on an industrial shop floor
Edge	Computing that is performed at or very near to the source of data instead of relying on the cloud or on-prem for processing	IoT device
Cloud	A remote facility for computing	Artificial intelligence processing engine

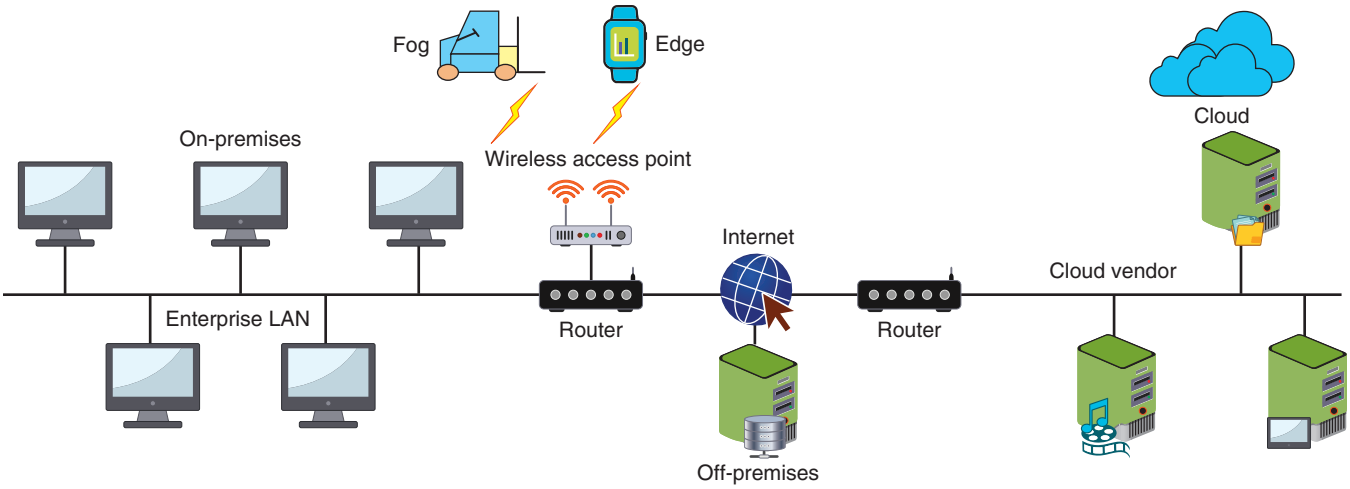


Figure 10-2 Computing locations

Cloud Architecture

Many elements make up a cloud architecture. A sampling of these elements include the following:

- *Thin client*. A **thin client** is a computer that runs from resources stored on a central cloud server instead of a localized hard drive. Thin clients connect remotely to the cloud computing environment where applications and data are stored and processing takes place.
- *Transit gateway*. A **transit gateway** is an Amazon Web Services (AWS) technology that allows organizations to connect all existing virtual private clouds (VPCs), physical data centers, remote offices, and remote gateways into a single managed source. The transit gateway gives full control over all resources—including network routing and security, VPCs, shared services, and other resources that may even span multiple AWS accounts. Transit gateways can consolidate edge connectivity and route it through a single cloud entry point.

NOTE 2

A transit gateway is considered a "hub-and-spoke" network topology that enables the user to monitor all activity.

- *Serverless infrastructure*. Although the term "serverless" is used occasionally, it is actually a misnomer. While using servers (somewhere) to perform a critical function, a **serverless infrastructure** is one in which the capacity planning, installation, setup, and management are all invisible to the user because they are handled by the cloud provider. Because the server resources of the cloud are inconspicuous to the user, this type of infrastructure is called "serverless."

NOTE 3

Serverless essentially means that provisioning, deploying, and managing a physical server disappears from a list of concerns.

Cloud Models

There are several service models in cloud computing. These are software as a service, platform as a service, infrastructure as a service, and anything as a service.

Software as a Service (SaaS) A typical enterprise must manage many sets of software licenses for the software applications it uses. These applications typically include human resources, finance, and customer relationship

management (CRM), along with OSs, productivity software, utilities, and many others. Significant costs are associated with purchasing desktop or service licenses, installing and upgrading the software, distributing patches, and managing them.

What if, as an alternative, enterprises paid a low monthly or annual fee per user for an external service to host the software on their own hardware? What if the service was made available through a web browser to users? Not only would the enterprise be relieved of the burden of purchasing and maintaining the software, but because it could be accessed via a browser, all authorized users could access the software from any number of endpoints without needing to install specialized software.

This is the definition of **Software as a Service (SaaS)**. SaaS is a cloud computing hosted software environment. SaaS eliminates software purchases, installation, maintenance, upgrades, and patches; instead, the cloud computing provider centrally manages the software on a per-user basis. SaaS usually includes provisions for a fixed amount of bandwidth and storage.

NOTE 4

SaaS offers commercial and well-known software to users, without any technical intervention from the IT staff. The software is offered as a complete *service* to users.

Platform as a Service (PaaS) **Platform as a Service (PaaS)** provides a software *platform* on which the enterprise or users can build their own applications and then host them on the PaaS provider's infrastructure. The software platform can be used as a development framework to build and debug the app and then deploy it.

NOTE 5

PaaS can also provide "middleware" services such as database and component services for use by the applications.

Unlike SaaS, in which everything is transparent to the enterprise, PaaS provides a moderate degree of control for the enterprise over the cloud computing environment. However, the enterprise does not always need to monitor usage and manually add resources; rather, the cloud provider can guarantee elasticity and scalability.

CAUTION Not all applications developed for a traditional enterprise network may seamlessly migrate to PaaS. Often the most success is from new applications developed specifically on and for the cloud.

Infrastructure as a Service (IaaS) **Infrastructure as a Service (IaaS)** provides unlimited "raw" computing, storage, and network resources that the enterprise can use to build its own virtual infrastructure in the cloud. The number of CPU processors and their speed, the amount of memory, the volume of storage, and the desired virtual networking resources such as routers and switches can be arranged to create the necessary virtual infrastructure. Enterprises can then load their own OSs (or "rent" them from the cloud provider) and software, web services, and database applications. Scaling and elasticity are not always automatically provided as with PaaS but, instead, are the enterprises' responsibility to monitor and request additional services.

How much of an enterprise's network architecture should be migrated to the cloud—and how much should remain on-prem? A traditional three-tier on-prem architecture is illustrated in Figure 10-3. (Note that for simplicity, no security appliances are illustrated.) This multitiered design helps control connections, provide scaling, and increase security. An enterprise could migrate Tier 1—Web servers and Tier 2—Application servers to a cloud computing provider but keep Tier 3—Database servers on-prem for security. However, it could just as easily migrate all three tiers to the cloud computing provider. Such a decision is based on several different factors.

Another question with IaaS involves using Layer 2 (switching) or Layer 3 (routing) when connecting to the virtual cloud network. Whereas Layer 2 is the simpler mode, in which the Ethernet MAC address and Virtual LAN (VLAN) information is used for forwarding, the disadvantage of Layer 2 networks is scalability. Using Layer 2 addressing and

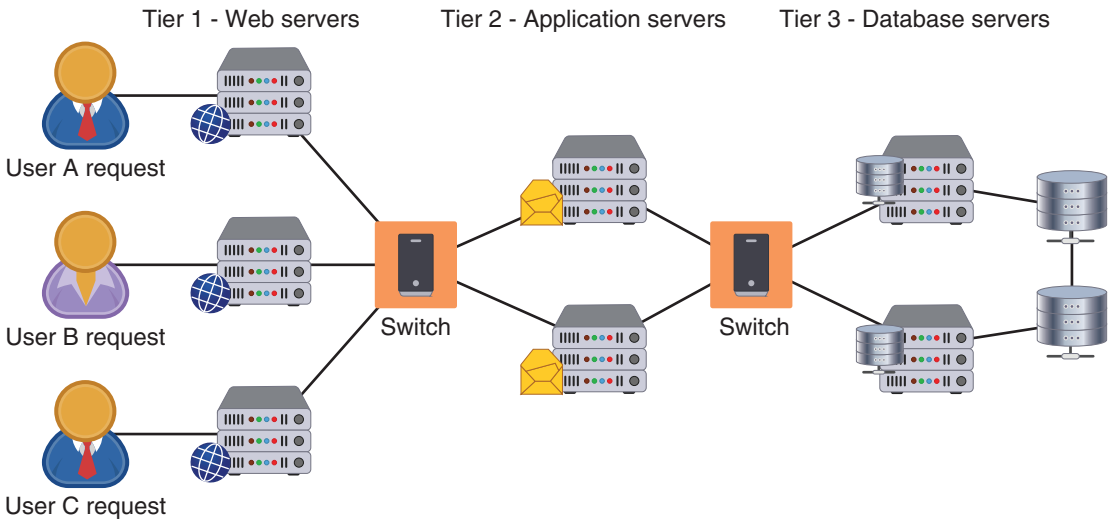


Figure 10-3 Three-tier architecture

connectivity can result in a "flat" topology, which is unrealistic with a large number of endpoints. Instead, using routing and subnets to provide segmentation for the appropriate functions provides greater flexibility but at a cost of forwarding performance and network complexity.

Anything as a Service (XaaS) **Anything as a Service (XaaS)** describes a broad category of subscription services related to cloud computing. XaaS is any IT function or digital component that can be transformed into a service for enterprise or user consumption. Today a vast number of products, tools, and technologies are delivered as a service over the Internet. For example, *Security as a Service (SECaaS)* provides security services—such as intrusion detection and SIEM—all delivered from the cloud to the enterprise. This relieves the enterprise from purchasing and managing security hardware and software.

NOTE 6

Examples of IT-based services include Communication as a Service (CaaS), Desktop as a Service (DaaS), and Healthcare as a Service (HaaS). One example of a non-IT service is ridesharing like Uber and Lyft and is called Transportation as a Service (TaaS).

A comparison of the IT responsibilities in the different cloud computing models is shown in Table 10-3.

Table 10-3 Cloud computing comparisons

Model	IT responsibilities	Explanation
SaaS	Low	The organization contracts with the cloud computing provider for access to software, relieving the IT staff of any responsibilities.
PaaS	Medium	The IT staff has moderate duties of creating the platform, but once completed, the duties diminish.
IaaS	High	Designing, building, and monitoring the virtual environment rely on IT staff.
XaaS	Varies	The role of IT depends on the service.

Management

After implementing a cloud computing solution, an organization must provide ongoing management. Managing cloud resources can be more challenging than managing on-prem resources. Typically, a cloud computing infrastructure, consisting of a virtual network and related servers, encompasses many cloud elements. It is not uncommon for a large organization to contract with several cloud computing providers. Properly managing multiple services from multiple providers can be cumbersome.

Cloud management can be conducted by the local organization performing the work itself or by contracting with a third-party management service provider.

Local Management One of the questions when locally managing cloud computing is how best to perform **services integration**, or the combined management function of multiple services into a single entity. Services integration attempts to achieve a "boundary-less" approach, which involves integrating all users across the enterprise who are using cloud computing. Services integration includes integrating SaaS and PaaS, on-prem applications, third-party gateways, and social media services. The goal is being able to monitor a seamless flow of data and transactions across systems.

When locally managing cloud computing, an enterprise should have written **resource policies** in place. These policies must clearly outline who is responsible for cloud computing, what are their duties and responsibilities, how cloud computing can be used (and not used), and the processes for acquiring these resources.

NOTE 7

Because a cloud environment can be set up by virtually all employees using their own credit card, these unauthorized or shadow IT cloud environments are a serious threat. One survey revealed that 93 percent of respondents said they continue to deal with shadow IT cloud computing, 82 percent have experienced security events as a result, and 71 percent said that employees are violating formal policies regarding cloud use by using cloud computing without authorization.[2]

Service Providers Instead of relying on local effort to manage a cloud environment, many organizations turn to external third-party service providers. A **managed service provider (MSP)** delivers services—such as network, application, infrastructure, and security—through ongoing and regular support as well as active administration of those resources. In short, an MSP assumes the role of a traditional on-prem IT organization.

An MSP can manage on the customers' premises, in the MSP's own data center (*hosting*), in a third-party data center, or in a cloud computing environment. "Pure-play" MSPs focus on a single vendor or technology, which is usually their own core offerings, while other MSPs include services from other types of providers.

A specialized type of MSP is a **managed security service provider (MSSP)**. An MSSP can assist with or even fully assume the cybersecurity defenses by providing an organization with a negotiated amount of cybersecurity monitoring and management on the organization's premises. These services typically include installing and monitoring antivirus and spam blocking, intrusion detection systems, firewalls, and virtual private networks (VPNs). An MSSP can also handle system changes, modifications, and upgrades.

Securing Cloud Computing

Cloud computing has several potential security issues. These are listed in Table 10-4.

Table 10-4 Cloud security issues

Security issue	Description
Unauthorized access to data	Improper cloud security configurations can result in data being left exposed.
Lack of visibility	Organizations have limited or no visibility into the security mechanisms of the cloud provider and thus cannot verify the effectiveness of security controls.
Insecure application program interfaces (APIs)	While APIs help cloud customers customize their PaaS by providing data recognition, access, and effective encryption, a vulnerable API can be exploited by threat actors.
Compliance regulations	Maintaining compliance requires that an organization know where its data is, who can access it, and how it is protected, but this can be difficult in an opaque cloud system, which lacks transparency.
System vulnerabilities	A cloud infrastructure is prone to system vulnerabilities due to complex networks and multiple third-party platforms.

The cloud provider should guarantee that the means are in place by which authorized users are given access while threat actors are denied. Also, the customer's data must be isolated from the data of other customers, and the highest level of application availability and security must be maintained. Finally, all transmissions to and from the cloud must be adequately protected. Securing cloud computing involves using cloud security controls, managing application security, and applying security to virtual devices.

Cloud Security Controls

A *security control* exists to reduce or mitigate the risk to assets. A control can be a policy, procedure, technique, method, solution, plan, action, or device designed to help accomplish that goal. Some controls are inherent to the cloud computing platforms and offered by the cloud computing providers to their customers (**cloud native controls**), while other security controls are available from external sources (**third-party solutions**).

Securing cloud computing involves using controls such as conducting audits, using regions and zones, implementing secrets management, and enforcing mitigations on the three function areas of cloud computing: storage, network, and compute.

Conduct Audits A **cloud security audit** is an independent examination of cloud service controls. Once completed, the auditor renders an objective assessment of the security. A cloud auditor can evaluate the services from a cloud provider in terms of security controls, privacy impact, availability, and performance. An auditor can also review the *integration* of the elements used in the overall infrastructure, such as VPCs, physical data centers, remote offices, and remote gateways.

Audits are typically performed to verify the conformance to established standards so that the organization can be authenticated as being in compliance. Auditing is particularly important for federal agencies because they are required to include a contractual clause enabling third parties to assess security controls of cloud providers. The organization itself can also benefit from the independent audit by being made aware of any deficiencies that must be addressed.

Use Regions and Zones Highly available systems are reliable because they can continue operating even when critical components fail. These systems are also resilient, meaning that they can simply handle failure without service disruption or data loss and seamlessly recover from such a failure. In a cloud computing environment, reliability and resiliency are achieved through duplicating processes across one or more geographical areas. This is called **high availability across zones**.

The cloud provider Amazon Web Services (AWS) maintains multiple geographic *Regions*—including Regions in North America, South America, Europe, China, Asia Pacific, South Africa, and the Middle East. An *Availability Zone (AZ)* is one or more data centers within an AWS Region, each with redundant power, networking, and connectivity. By spreading their cloud infrastructure across several AZs, AWS clients can create systems that are more highly available, fault tolerant, and scalable than would be possible from using a single data center. If an application is partitioned across multiple AZs, then organizations are better isolated and protected from problems such as power outages, lightning strikes, tornadoes, and earthquakes.

NOTE 8

All AZs in an AWS Region are interconnected with high-bandwidth, low-latency networking, over fully redundant, dedicated fiber connections. All AZs are physically separated from each other by a "meaningful distance" from any other AZ, although all are within 60 miles (100 km) of each other.

Implement Secrets Management Traditional application design is often called *monolithic* because the entire program is developed as a single entity. While monolithic code writing and deploying was originally done for convenience because it all occurred at a single location in the organization's office, these applications soon became larger and more complex as more features were added and requirements were expanded. This made managing the applications difficult for the following reasons:

- As the applications became larger, deployment times likewise became longer.
- Due to the complexity, any modifications often affected other parts of the code so that the application became unstable, unsecure, or failed to function as designed.
- The codebase became too large for any single developer or development team to fully understand.

The solution to monolithic application design is to divide it into smaller entities. These were not divided by *technical* processes but rather designed to make each entity a specialized part of the code. This is known as **microservices architecture** and is illustrated in Figure 10-4. A microservices architecture has smaller and more specialized elements—each of which manages its own database, generates its own logs, and handles user authentication by using **microservices APIs** and specialized APIs called RESTful APIs.

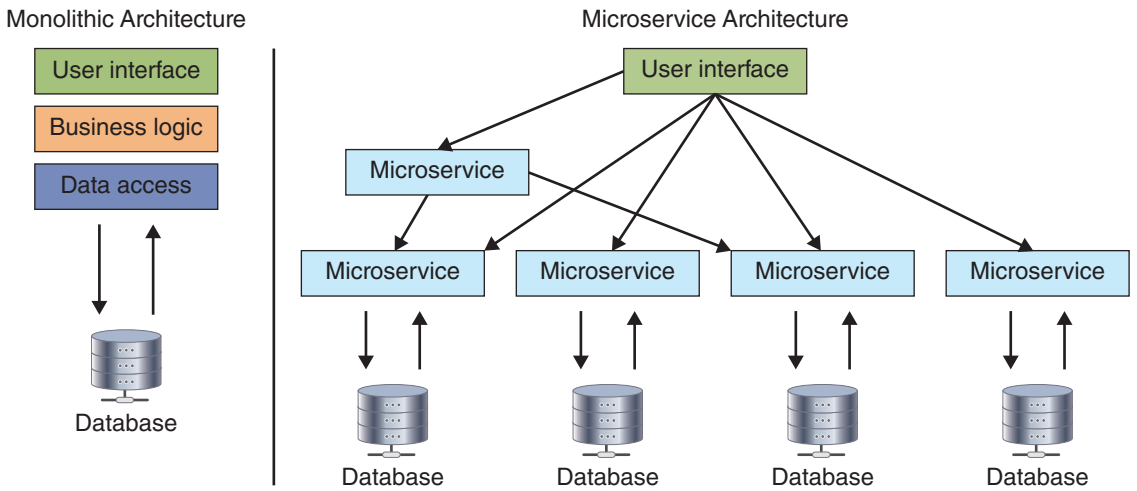


Figure 10-4 Monolithic versus microservices architecture

NOTE 9

When the British Broadcasting Corporation (BBC) moved its monolithic on-demand video platform to a cloud computing environment using a microservices architecture, the final product comprised 30 separate microservices.

The microservices need to communicate among themselves. However, cloud-based microservices must have keys to access the other microservices—such as API keys, passwords, certificates, encryption keys, and tokens. How should these "secrets" be passed or accessed securely? Embedding the keys as part of the software code (*hard coding*) is not a secure option.

The answer is to use **secrets management**. Secrets management enables strong security and improved management of a microservices-based architecture. It allows the entire cloud infrastructure to remain flexible and scalable without sacrificing security. A secrets manager provides a central repository and single source to manage, access, and audit secrets across a cloud infrastructure. Typical features of a secrets management system are listed in Table 10-5.

Table 10-5 Secrets management features

Feature	Description
Limited and automated replication	While secret data and secret names are "project-global" resources, the secret data is stored in regions, which the user can specify or the cloud provider can designate.
Secret-specific versioning	A secret can be pinned to a specific version of the code (like "v3.2").
Audit logging	Every interaction generates an audit entry in a log file that can be used to find abnormal access patterns that may indicate possible security breaches.
Default encryption	Data is encrypted in transit and at rest with AES-256-bit encryption keys.
Extensibility	One system is able to extend and integrate into other existing secrets management systems.

Cloud computing providers typically offer their own proprietary secrets management systems. Several third-party systems are also available.

Enforce Functional Area Mitigations Cloud computing has three functional areas: storage, network, and compute. Each of these has its own set of security mitigations and is listed in Table 10-6.

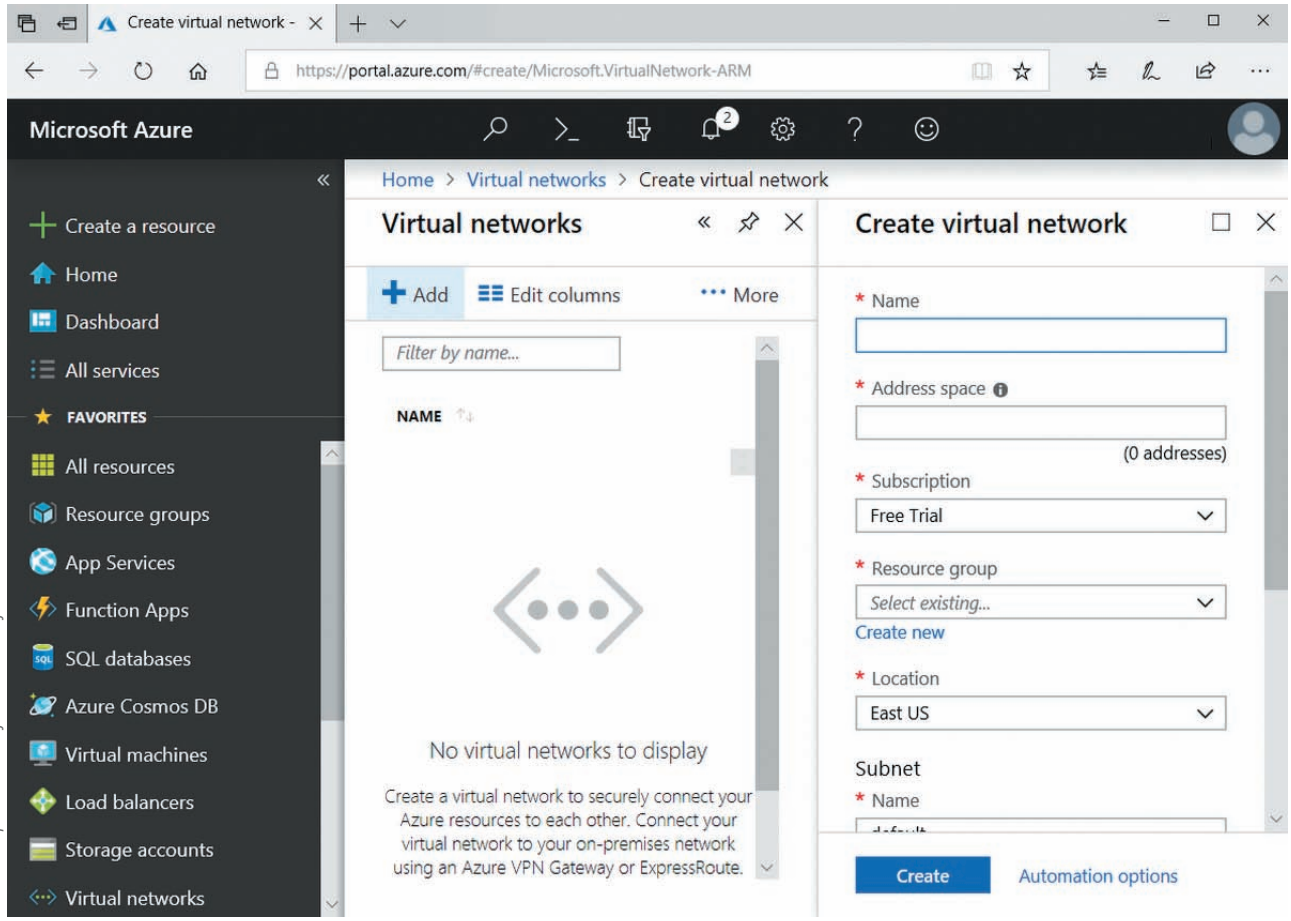
Table 10-6 Functional area controls

Functional area	Control	Description
Storage	Permissions	Enforce what actions can be taken on stored data (such as edit, delete, and copy).
Storage	Encryption	Encrypt data at rest in the cloud.
Storage	Replication for high availability	Store multiple copies of critical data across regions and zones to protect against loss.
Network	Virtual networks	Create a **virtual network** that connects services and resources such as virtual machines and database applications with each other via a secure, encrypted, and private network, as seen in Figure 10-5.
Network	Public and private subnets	Configure a VPC with a **public subnet** for public-facing web server applications and a different **private subnet** for backend servers that are not publicly accessible.
Network	Segmentation	Create network segments to enforce rules for which services are permitted between accessible zones so that only designated endpoints belonging to other approved zones can reach them.
Network	API inspection and integration	Use automated **API inspection and integration** services for authentication, authorization, encryption, availability, and policy compliance of APIs.
Compute	Security groups	Use **security groups** to segment computing resources into logical groupings that form network perimeters.
Compute	Dynamic resource allocation	**Dynamic resource allocation** is deprovisioning computing resources when they are no longer needed.
Compute	Instance awareness	Implement **instance awareness** or the ability for security appliances to differentiate between instances of cloud apps.
Compute	VPC endpoint	When creating a VPC endpoint, attach an endpoint policy that controls access to the service.

Application Security

While securing the functional areas of the cloud (storage, networking, and compute) is universally considered as important, an area often overlooked is **application security** or protecting applications. There are several common misperceptions, ranging from application security being entirely the cloud computing provider's responsibility to the native "out of the box" security of the applications providing adequate security. However, misconfigurations of the application setup and insecure APIs or interfaces can provide vulnerabilities for threat actors to exploit.

One of an organization's security protections for cloud computing application security is to use a **cloud access security broker (CASB)**. A CASB is a set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure. Acting as the gatekeeper, a CASB ensures that the security policies of the enterprise extend to its data in the cloud. For example, if the enterprise has a policy for encrypting data, a CASB can enforce that control and ensure that data is encrypted when it is copied from the cloud to a local device. Another security protection is to use cloud-based data loss prevention (DLP) to extend the enterprise's policies to data stored in the cloud.



Used with permissions from Microsoft

Figure 10-5 Virtual network

Security Virtual Device Solutions

Just as security appliances are needed in a physical network, so too are security virtual devices in a cloud computing environment. Next generation secure web gateways and virtual firewalls are considered important. However, determining which security appliances to implement in a cloud computing infrastructure is more challenging due to a lack of a cloud conceptual model.

Next Generation Secure Web Gateway (SWG) A **next generation secure web gateway (SWG)** combines several features into a single product. It examines both incoming and outgoing traffic and performs basic URL and monitoring in web applications. A next generation SWG also analyzes received traffic (even traffic encrypted by SSL), performs DLP, and provides alerts to a monitoring device such as a security information and event management (SIEM) appliance. An SWG can be placed on endpoints, at the edge, or in the cloud.

Cloud Firewall A cloud firewall is virtual software that functions in a similar manner to a physical security appliance by examining traffic into and out of the cloud. Sometimes called a *public cloud firewall, next gen firewall,* or *virtual firewall*, these devices are deployed in the public cloud. However, they have several advantages over a physical appliance such as the ability to scale quickly as the need arises.

CAUTION When deploying a cloud firewall, the costs should be considered. Like cloud providers, third-party cloud firewall providers charge an hourly rate for the service. This is especially the case if the network has been "microsegmented" with each segment requiring its own cloud firewall.

Lack of Cloud Conceptual Model Determining the correct security virtual device for the cloud can be challenging. A primary reason for this challenge is that physical networks neatly map to the **Open Source Interconnection (OSI) seven-layer model** that illustrates network functionality, as seen in Figure 10-6. When managing an on-prem infrastructure, it is relatively straightforward for a network administrator to understand what is being done at each layer, who is responsible for physical connectivity, who manages Layer 3 routing and control, and who has access to the upper layers. When "Layer 3" is used to describe IP-based routing or when "Layer 7" is used to describe functions interacting at a software level, these terms are universally and uniformly applied. Security professionals can then more easily identify the security appliances needed and understand how they interact with the other layers and appliances.

Layer	Application/Example
Application (7) Serves as the window for users and application processes to access the network services.	**End user layer** Program that opens what was sent or creates what is to be sent
	Resource sharing • Remote file access • Remote printer access • Directory services • Network management
Presentation (6) Formats the data to be presented in the Application layer. It can be viewed as the "translator" for the network.	**Syntax layer** Encrypt and decrypt (if needed)
	Character code translation • Data conversion • Data compression • Data encryption • Character set translation
Session (5) Allows session establishment between processes running on different stations.	**Synch and send to ports** (logical ports)
	Session establishment, maintenance, and termination • Session support • Perform security, name recognition, logging, etc.
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to host, flow control
	Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing
Network (3) Controls the operations of the subnet, deciding which physical path the data takes	**Packets** ("letter," contains IP address)
	Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes," contains MAC address) (NIC card—Switch—NIC card) (End to end)
	Establishes and terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgement • Frame delimiting Frame error checking • Media access control
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc.
	Data encoding • Physical medium attachment • Transmission technique • Baseband or broadband • Physical medium transmission bits and volts

Figure 10-6 OSI seven-layer model

However, with cloud computing, the OSI model no longer is as useful—if it is useful at all. First, the cloud provider manages cabling, Internet connections, power, cooling, disks, redundancy, and physical security instead of the customer. Second, everything the cloud customer "sees" is abstract and virtual, and essentially exists only as code. Third, there is a higher level of interaction: an organization may create multiple cloud computing accounts with multiple cloud providers in order to separate environments from each other, each with different VPCs for different applications, multiple subnets for different functions, and a variety of storage, network, and compute configurations. The lack of a conceptual model like the OSI model makes selecting and managing security virtual devices more challenging.

Different cloud-based conceptual models are starting to be proposed. One model is shown in Table 10-7. However, no single model has been widely adapted, and it appears that there is no model that will become the standard in the near future.

Table 10-7 Proposed cloud-based conceptual model

Layer and name	Description	Party responsible
5—Application Experience	End-user facing interface	Customer
4—Native Service	Create, store, process	Customer
3—Software-Defined Datacenter	Create infrastructure	SaaS—Cloud computing provider PaaS and IaaS—Customer
2—Virtualization Software	Software that virtualizes the hardware	Cloud computing provider
1—Physical Infrastructure	Buildings, power, cables, hardware, utilities	Cloud computing provider

TWO RIGHTS & A WRONG

1. A community cloud is a cloud that is open only to specific organizations that have common concerns.
2. The fog computing location is performed at or very near the source of the data instead of relying on the cloud or on-prem for processing.
3. A serverless infrastructure is one in which the capacity planning, installation, setup, and management are all invisible to the user because they are handled by the cloud provider.

See Appendix B for the answer.

VIRTUALIZATION SECURITY

CERTIFICATION

2.2 Summarize virtualization and cloud computing concepts.

Like cloud security, virtualization security also involves first an understanding of the topic along with specific examples. It includes specific steps to be taken to secure a virtualized environment.

Defining Virtualization

Understanding virtualization includes knowing what it is and how it can be used along with its advantages.

What Is Virtualization?

Virtualization is a means of managing and presenting computer resources by function without regard to their physical layout or location. One type of virtualization in which an entire operating system environment is simulated is known as *host virtualization*. Instead of using a physical computer, a *virtual machine (VM)*, which is a simulated software-based emulation of a computer, is created instead. The *host system* (the operating system installed on the computer's hardware) runs a VM monitor program that supports one or more *guest systems* (a foreign virtual operating system) that run applications. For example, a computer that boots to Windows 10 (host) could support a VM of Linux (guest) as well as another Windows 10 (guest) system.

Virtualization is used to consolidate multiple physical servers into VMs that can run on a single physical computer. Because a typical server utilizes only about 10–15 percent of its capacity, multiple VMs can run on a single physical server.

NOTE 10

Virtualization is not new. It was first developed by IBM in the 1960s for running multiple software "contexts" on its mainframe computers. It has gained popularity over the last 20 years as on-prem data centers used it for migrating away from physical servers to more economical VMs.

In addition, virtualization is used extensively in cloud computing environments. It gives the flexibility necessary for rapid deployments. In fact, the adoption and popularity of cloud computing can be directly attributed to the widespread use of on-prem server virtualization.

The VM monitor program is called a *hypervisor*, which manages the VM operating systems. Hypervisors use a small "layer" of computer code in software or firmware to allocate resources in real time as needed, such as input/output functions and memory allocations. There are two types of hypervisors:

- *Type I. Type I hypervisors* run directly on the computer's hardware instead of the underlying operating system. Type I hypervisors are sometimes called "native" or "bare metal" hypervisors.
- *Type II.* Instead of running directly on the computer hardware, *Type II hypervisors* run on the host operating system, much like a regular application. Type I and Type II hypervisors are illustrated in Figure 10-7.

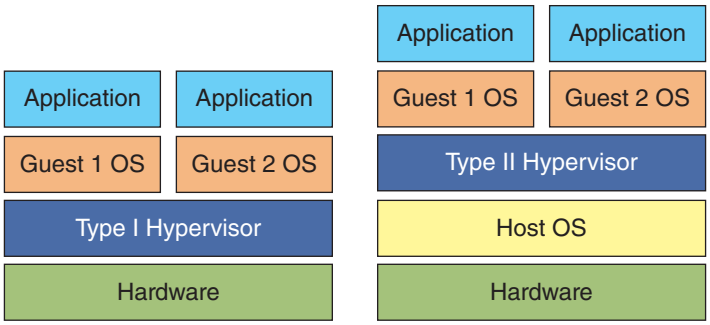


Figure 10-7 Type I and Type II hypervisors

An even more reduced instance of virtualization is a **container**. With both Type I and Type II hypervisors, the entire guest operating system must be started and fully functioning before an application can be launched. A container, on the other hand, holds only the necessary OS components (such as binary files and libraries) that are needed for that specific application to run. And in some instances, containers can even share binary files and libraries. This not only reduces the necessary hard drive storage space and random access memory (RAM) needed but also allows for containers to start more quickly because the entire operating system does not have to be started. Containers can be easily moved from one computer to another. A container is illustrated in Figure 10-8.

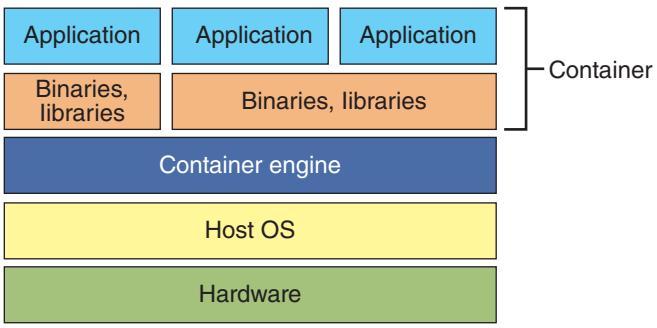


Figure 10-8 Container

NOTE 11

Another application of VMs is known as *Virtual Desktop Infrastructure (VDI)*. VDI is the process of running a user desktop inside a VM that resides on a server. This enables personalized desktops for each user to be available on any computer or device that can access the server so that their personalized desktop and files can be accessed as if they were sitting at their own computer. VDI allows centralized management as opposed to the need for technical support personnel to access a system remotely or even visit a user's desk to troubleshoot, saving substantial time and money.

Advantages of Virtualization

Virtualization has several advantages. First, new virtual server machines can be quickly made available (*host availability*), and resources such as the amount of RAM or hard drive space can easily be expanded or contracted as needed (*host elasticity*). Also, virtualization can reduce costs. Instead of purchasing one physical server to run one network operating system and its applications, a single physical server can run multiple VMs and host multiple operating systems. This results in a significant cost savings in that fewer physical computers must be purchased and maintained. In addition, the cost of electricity to run these servers as well as keep data center server rooms cool is also reduced.

Another advantage of server virtualization is that it can be beneficial in providing uninterrupted server access to users. Data centers must schedule planned "downtime" for servers to perform maintenance on the hardware or software. However, it is often difficult to find a time when users will not be inconvenienced by the downtime. This can be addressed by virtualization that supports *live migration*; this technology enables a VM to be moved to a different physical computer with no impact to the users. The VM stores its current state onto a shared storage device immediately before the migration occurs. The VM is then reinstalled on another physical computer and accesses its storage with no noticeable interruption to users. Live migration also can be used for *load balancing*; if the demand for a service or application increases, network managers can quickly move this high-demand VM to another physical server with more RAM or CPU resources.

CAUTION

Sometimes overlooked when migrating multiple physical servers to VMs is the need for increased bandwidth to the physical server that houses the VMs. Prior to the migration, each physical server had its own network connection; now, however, a single physical server must handle all the traffic for multiple VMs. Servers housing multiple VMs may need a 10 Gbps Ethernet card to handle the increase in traffic.

Infrastructure as Code

Instances of virtualization is sometimes referred to as *infrastructure as code*. Two examples are software-defined networks and software-defined visibility.

Software-Defined Network (SDN)

Virtualization has been an essential technology in changing the face of computing over the last decade. Racks of individual physical servers running a single application have been replaced by only a few hardware devices running multiple VMs, simulated software-based emulations of computers. VMs have made cloud computing possible; as computing needs increase or decrease, cloud computing resources on VMs can be quickly scaled up or back. Networks can also be configured into logical groups to create a *virtual LAN* (VLAN). A VLAN allows scattered users to be logically grouped together even though they are physically attached to different switches. The computing landscape today would simply not be possible without virtualization.

Yet VMs and virtual LANs run into a bottleneck: the physical network. Dating back more than 40 years, networks comprised of physical hardware like bridges, switches, and routers have collided with the world of VMs and VLANs.

Consider this problem. A network manager needs to make sure the VLAN used by a VM is assigned to the same port on a switch as the physical server that is running the VM. But if the VM needs to be migrated, the manager must reconfigure the VLAN every time that a virtual server is moved. In a large enterprise, whenever a new VM is installed, it can take hours for managers to perform the necessary reconfiguration. In addition, these managers must configure each vendor's equipment separately, tweaking performance and security configurations for each session and application. This process is difficult to do with conventional network switches because the *control logic* for each switch is bundled together with the *switching logic*.

What is needed is for the flexibility of the virtual world to be applied to the network. This would allow the network manager to add, drop, and change network resources quickly and dynamically on the fly.

The solution is a **software-defined network (SDN)**. An SDN virtualizes parts of the physical network so that it can be more quickly and easily reconfigured. This is accomplished by separating the *control plane* from the *data plane*, as illustrated in Figure 10-9. The control plane consists of one or more SDN servers and performs the complex functions such as routing and security checks. It also defines the data flows through the data plane.

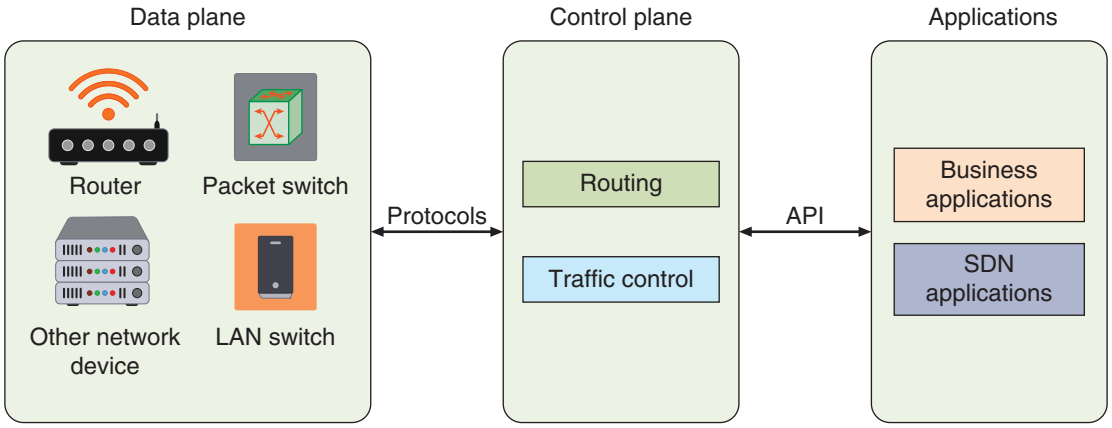


Figure 10-9 Software-defined network

NOTE 12

In an SDN, the control plane is essentially an application running on a computer that can manage the physical plane.

If traffic needs to flow through the network, it first receives permission from the SDN controller, which verifies that the communication is permitted by the network policy of the enterprise. Once approved, the SDN controller computes a route for the flow to take and adds an entry for that flow in each of the switches along the path. Because all the complex networking functions are handled by the SDN controller, the switches simply manage "flow tables" whose entries are created by the controller. The communication between the SDN controller and the SDN switches uses a standardized protocol and API.

NOTE 13

The architecture of SDN is very flexible, using different types of switches from different vendors at different protocol layers. SDN controllers and switches can be implemented for Ethernet switches (Layer 2), Internet routers (Layer 3), Transport (Layer 4) switching, or Application layer switching and routing.

With the decoupling of the control and data planes, SDN enables applications to deal with one "abstracted" network device without any care for the details of how the device operates. This is because the network applications see only a single API to the controller. This makes it possible to quickly create and deploy new applications to orchestrate network traffic flow to meet specific enterprise requirements for performance or security.

NOTE 14

From a security perspective, SDNs can provide stronger protection. SDN technology can simplify extending VLANs beyond just the perimeter of a building, which can help secure data. Also, an SDN can ensure that all network traffic is routed through a firewall. And because all network traffic flows through a single point, it can help capture data for NIDS and NIPS.

Software-Defined Visibility (SDV)

Software-defined visibility (SDV) is a framework that allows users to create programs in which critical security functions that previously required manual intervention can now be automated. As technology moves from a user interacting with a machine to a machine interacting with multiple machines, it is necessary to improve this interaction. SDV allows network administrators to automate multiple functions in a network infrastructure—including dynamic response to detected threat patterns, adjustments to traffic mode configurations for in-line security tools, and additional IT operations-management functions and capabilities.

NOTE 15

SDV relies upon a set of APIs known as *RESTful APIs*. These RESTful APIs use existing HTTP methods of GET, PUT, POST, and DELETE. RESTful APIs have become so foundational that they are sometimes called the "backbone of the Internet."

Security Concerns for Virtual Environments

Host virtualization also has several security-related advantages:

- The latest security updates can be downloaded and run in a VM to determine compatibility or the impact on other software or even hardware. This is used instead of installing the update on a production computer and then being forced to "roll back" to the previous configuration if it does not work properly.
- A *snapshot* of a state of a VM can be saved for later use. A user can make a snapshot before performing extensive modifications or alterations to the VM, and then the snapshot can be reloaded so that the VM is at the beginning state before the changes were made. Multiple snapshots can be made, all at different states, and loaded as needed.
- Testing the existing security configuration, known as *security control testing*, can be performed using a simulated network environment on a computer using multiple VMs. For example, one VM can virtually attack another VM on the same host system to determine vulnerabilities and security settings. This is possible because all the VMs can be connected through a virtual network.
- VMs can promote security segregation and isolation. Separating VMs from other machines can reduce the risk of infections transferring from one device to another.
- A VM can be used to test for potential malware. A suspicious program can be loaded into an isolated VM and executed (*sandboxing*). If the program is malware, it will impact only the VM, and it can easily be erased and a snapshot reinstalled. This is how antivirus software using heuristic detection can spot the characteristics of a virus.

NOTE 16

Threat actors have learned that when their malware is run in a sandbox, it most likely is being examined by a security professional. Many modern instances of malware will refuse to function or even self-destruct if it detects that it is being run in a sandbox.

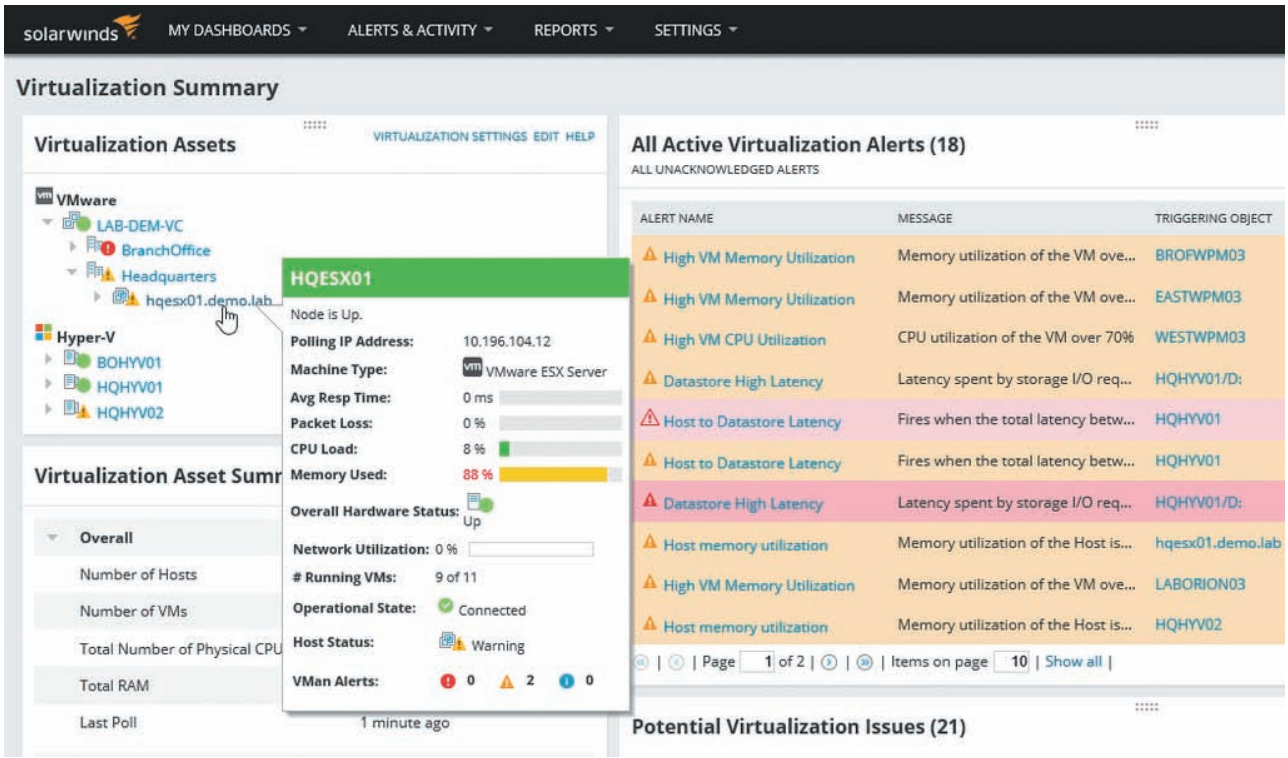
However, there are security concerns for virtualized environments:

- Not all hypervisors have the necessary security controls to keep out determined attackers. If a single hypervisor is compromised, multiple virtual servers are at risk.
- Traditional security tools—such as antivirus, firewalls, and IDS—were designed for single physical servers and do not always adapt well to multiple VMs. Instead, "virtualized" versions can be used instead, such as a *firewall virtual appliance* that is optimized for VMs.
- VMs must be protected from both outside networks and other VMs on the same physical computer. In a network without VMs, external devices such as firewalls and IDS that reside between physical servers can help prevent one physical server from infecting another physical server, but no such physical devices exist between VMs.
- VMs may be able to "escape" from the contained environment and directly interact with the host operating system. It is important to have **virtual machine escape protection** so that a VM cannot directly interact with the host operating system and potentially infect it, which could then be transmitted to all other VMs running on the host operating system.

Because VMs can easily and quickly be created and launched, this has led to *virtual machine sprawl*, or the widespread proliferation of VMs without proper oversight or management. It is often easy for a VM to be created and

then forgotten. A guest operating system that has remained dormant for a period may not contain the latest security updates, even though the underlying host operating system has been updated. When the guest is launched, it will be vulnerable until properly updated.

Combating VM sprawl is called **virtual machine sprawl avoidance**. Suggestions for limiting VM sprawl include performing regular audits to identify VMs that are no longer needed, using good naming conventions to be able to more easily identify the purpose of a VM, and periodically cleaning up VMs so that new processes can be easily added to an existing VM. Another option is to install a virtual machine manager, which can provide a dashboard of the status of the VMs. A virtual machine manager is seen in Figure 10-10.



Source: SolarWinds

Figure 10-10 Virtual machine manager

In addition to protecting VMs, **container security** or protecting containers from attacks is also important. Best practices for securing a container include the following:

- Always manage container-based processes using non-privileged user accounts.
- Use trusted images to create a container because a compromised image can more easily circumvent existing security measures.
- Use tools such as Security-Enhanced Linux (SELinux) to harden the hosts.

TWO RIGHTS & A WRONG

1. A host system runs a VM monitor program that supports one or more guest systems that run applications.
2. SDV allows network administrators to automate multiple functions in a network infrastructure.
3. Type II hypervisors run directly on the computer's hardware instead of the underlying operating system.

See Appendix B for the answer.

SECURE NETWORK PROTOCOLS

CERTIFICATION

1.3 Given a scenario, analyze potential indicators associated with application attacks.

3.1 Given a scenario, implement secure protocols.

3.3 Given a scenario, implement secure network designs.

When using remote resources like cloud providers, the importance of using secure network protocols is heightened. Yet secure network protocols are not isolated to accessing cloud resources; rather, there are several significant use cases for these protocols. Some of the common secure network protocols include the Simple Network Management Protocol, Domain Name System Security Extensions, File Transfer Protocol, secure email protocols, Lightweight Directory Access Protocol (LDAP), and Internet Protocol version 6.

Simple Network Management Protocol (SNMP)

The **Simple Network Management Protocol (SNMP)** is a popular protocol used to manage network equipment and is supported by most network equipment manufacturers. It allows network administrators to remotely monitor, manage, and configure devices on the network. SNMP functions by exchanging management information between networked devices.

NOTE 17

SNMP can be found not only on core network devices such as switches, routers, and wireless access points, but also on printers, copiers, fax machines, and even uninterruptible power supplies (UPSs).

Each SNMP-managed device must have an agent or an SNMP service that listens for commands and then executes them. These agents are protected with a password, called a *community string*, to prevent unauthorized users from taking control of a device. There are two types of community strings: a *read-only* string allows information from the agent to be viewed, and a *read-write* string allows settings on the device to be changed.

There were several security vulnerabilities with the use of community strings in the first two versions of SNMP, known as SNMPv1 and SNMPv2. Because of the security vulnerabilities of SNMPv1 and SNMPv2, significant security enhancements were made to the next (and now current) version known as **SNMPv3**. SNMPv3 supports authentication and encryption. Authentication is used to ensure that SNMPv3 information is available only to the intended recipient, while encryption ensures that any messages cannot be read by threat actors.

NOTE 18

Cloud computing virtual network equipment can also be managed by using SNMP.

Domain Name System Security Extensions (DNSSEC)

The Domain Name System (DNS), which is the basis for domain name resolution of names to IP addresses, is often the focus of attacks. These attacks using DNS include DNS poisoning and DNS hijacking.

NOTE 19

DNS, DNS poisoning, and DNS hijacking are covered in Module 8.

These DNS attacks can be thwarted by using **Domain Name System Security Extensions (DNSSEC)**. DNSSEC adds additional *resource records* (these records define the data types being used) and message header information, which can be used to verify that the requested data has not been altered in transmission. Using asymmetric cryptography, a private key that is specific to a zone is used in encrypting a hash of a set of resource records, which is then used to create the digital signature to be stored in the resource record (along with the corresponding public key).

NOTE 20

DNSSEC essentially adds two important features to the DNS protocol: data origin authentication allows a resolver to verify that the data it received actually came from the zone from which it claims to have originated, and data integrity protection proves the data has not been modified in transit since it was originally signed by the zone owner with the zone's private key.

File Transfer Protocol (FTP)

In its early days, prior to the development of the World Wide Web and Hypertext Transfer Protocol (HTTP), the Internet was primarily a medium for transferring files from one device to another. Today transferring files is still an important task. Transferring files can be performed using the **File Transfer Protocol (FTP)**, which is an unsecure TCP/IP protocol. FTP is used to connect to an FTP server, much in the same way that HTTP links to a web server.

NOTE 21

A "light" version of FTP known as *Trivial File Transfer Protocol (TFTP)* uses a small amount of memory but has limited functionality. It is often used for the automated transfer of configuration files between devices.

There are several different methods for using FTP on a local computer. These include using an FTP client application that displays files on the local endpoint as well as the remote server so files can be dragged and dropped between devices, using a web browser by prefacing a URL with the protocol ftp:// instead of the http://, or even from an OS command prompt using *get* (retrieve a file from the server), and *put* (transfer a file to the server).

FTP typically uses two ports: TCP port 21 is the FTP control port used for passing FTP commands, and TCP port 20 is the FTP data port through which data is sent and received. Using *FTP active mode,* an FTP client initiates a session to a server by opening a *command channel* connection to the server's TCP port number 21. A file transfer is requested by the client by sending a *PORT* command to the server, which then attempts to initiate a *data channel* connection back to the client on TCP port 20. In *FTP passive mode*, the client initiates the data channel connection, yet instead of using the *PORT* command, the client sends a *PASV* command on the command channel. The server responds with the TCP port number to which the client should connect to establish the data channel (typically port 1025 to 5000).

NOTE 22

Increased security can be established by restricting the port range used by the FTP service and then creating a firewall rule that allows FTP traffic only on those allowed port numbers.

Several security vulnerabilities are associated with using FTP. First, FTP does not use encryption, so any usernames, passwords, and files being transferred are in cleartext and could be accessed by using a protocol analyzer. Also, files being transferred by FTP are vulnerable to man-in-the-middle attacks.

There are two options for secure transmissions over FTP. **FTP Secure (FTPS)** uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt commands sent over the control port (port 21) in an FTP session. FTPS is a file transport layer resting on top of SSL or TLS, meaning that it uses the FTP protocol to transfer files to and from SSL- or TLS-enabled FTP servers. However, a weakness of FTPS is that although the control port commands are encrypted, the data port (port 20) may or may not be encrypted. This is because a file that has already been encrypted by the user would not need to be encrypted again by FTPS and incur the additional overhead.

The second option is to use **Secure FTP (SFTP)**. There are several differences between SFTP and FTPS. First, FTPS is a combination of two technologies (FTP and SSL or TLS), whereas SFTP is an entire protocol itself and is not pieced together with multiple parts. Second, SFTP uses only a single TCP port instead of two ports like FTPS. Finally, SFTP encrypts and compresses all data and commands (FTPS might not encrypt data).

Secure Email Protocols

Since developer Ray Tomlinson sent the first email message in 1971, email has become an essential part of everyday life. It is estimated that more than 400 billion emails are sent daily. However, only 15 percent of this total (60 billion) are legitimate; the remaining 85 percent or 340 billion daily emails are spam.[3]

Two different electronic email systems are in use today. An earlier email system uses two TCP/IP protocols to send and receive messages: the **Simple Mail Transfer Protocol (SMTP)** handles outgoing mail, while the **Post Office Protocol (POP)**, more commonly known as *POP3* for the current version, is responsible for incoming mail. POP3 is a basic protocol that allows users to retrieve messages sent to an email server by using a local program running on their computer called an *email client*. The email client connects to the POP3 server and downloads the messages onto the local computer. After the messages are downloaded, they may be erased from the POP3 server. The SMTP server listens on port 25 while POP3 listens on port 110.

CAUTION

SMTP servers can forward email sent from an email client to a remote domain, known as *SMTP relay*. However, if SMTP relay is not controlled, an attacker can use it to forward spam and disguise his identity to make himself untraceable. An uncontrolled SMTP relay is known as an *SMTP open relay*. It is important to defend against SMTP open relays. The mail relay should be turned off altogether so that all users send and receive email from the local SMTP server or limit relays to only local users.

IMAP (Internet Mail Access Protocol) is a more recent and advanced electronic email system for incoming mail. While POP3 is a "store-and-forward" service, IMAP is a "remote" email storage. With IMAP, the email remains on the email server and is not downloaded to the user's computer. Mail can be organized into folders on the mail server and read from any device: desktop computer, tablet, smartphone, etc. IMAP users can even work with email while offline. This is accomplished by downloading email onto the local device without erasing the email on the IMAP server. A user can read and reply to email offline. The next time a connection is established, the new messages are sent, and any new email is downloaded. The current version of IMAP is IMAP4.

As a means of security, a *mail gateway* monitors emails for unwanted content and prevents these messages from being delivered. Many mail gateways also have monitoring capabilities for outbound emails. For inbound emails, a mail gateway can search the content in email messages for various types of malware, spam, and phishing attacks. For outbound email, a mail gateway can detect and block the transmission of sensitive data, such as Social Security numbers or healthcare records. In addition, a mail gateway can automatically and transparently encrypt outbound email messages.

Lightweight Directory Access Protocol (LDAP)

A **directory service** is a database stored on the network itself that contains information about users and network devices. It contains information such as the user's name, telephone extension, email address, login name, and other facts. The directory service also keeps track of all the resources on the network and a user's privileges to those resources and grants or denies access based on the directory service information. Directory services make it much easier to grant privileges or permissions to network users.

The International Organization for Standardization (ISO) created a standard for directory services known as *X.500*. The purpose of the X.500 standard was to standardize how the data was stored so that any computer system could access these directories. The X.500 standard also defines a protocol for a client application to access an X.500 directory called the *Directory Access Protocol (DAP)*. However, the DAP is too large to run on a

personal computer. The **Lightweight Directory Access Protocol (LDAP)**, sometimes called X.500 Lite, is a simpler subset of DAP.

LDAP makes it possible for almost any application running on virtually any computer platform to obtain directory information. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory. Today many LDAP servers are implemented using standard relational database management systems as the engine and communicate via Extensible Markup Language (XML) documents served over the Hypertext Transport Protocol (HTTP).

CAUTION By default, LDAP traffic is transmitted in cleartext. LDAP traffic can be made secure by using Secure Sockets Layer (SSL), which is known as LDAP over SSL (LDAPS).

However, a weakness of LDAP is that it can be subject to **LDAP injection attacks**. These attacks, similar to SQL injection attacks, can occur when user input is not properly filtered. This may allow an attacker to construct LDAP statements based on user input statements. The attacker could then retrieve information from the LDAP database or modify its content. The defense against LDAP injection attacks is to examine all user input before processing.

NOTE 23

Injection attacks are covered in Module 3.

Internet Protocol Version 6 (IPv6)

The current version of the IP protocol is version 4 and is called *IPv4*. Developed in 1981, long before the Internet was universally popular, IPv4 has several weaknesses. One of the weaknesses is the number of available IP addresses: an IP address is 32 bits in length, providing about 4.3 billion possible IP address combinations, which is no longer is sufficient for the number of devices that are being connected to the Internet. Another weakness is that of security: due to its structure, IPv4 can be subject to several types of attacks.

NOTE 24

Prior to the release of IPv4 in 1981, the total number of IP addresses available was only 255.

The solution to these weaknesses is the next generation of the IP protocol called **Internet Protocol version 6 (IPv6)**. IPv6 addresses the weaknesses of IPv4 and also provides several other significant improvements. First, IPv6 increases the number of available addresses. The number of IPv6 addresses is 340,282,366,920,463,463,374,607,431,768,211,456 or 340 trillion, trillion, trillion addresses. This translates to 665 million billion IP addresses per square meter on earth.

IPv6 also has several enhanced security features. IPv6 can implement end-to-end encryption, making man-in-the-middle attacks significantly more difficult. IPv6 also supports more secure name resolution. The Secure Neighbor Discovery (SEND) protocol can send cryptographic confirmation that an endpoint is who it claims to be at the time of connection. This effectively renders Address Resolution Protocol (ARP) poisoning more difficult.

Use Cases

Different applications or "use cases" require different secure network protocols. Several of the recommended protocols for specific applications or technologies are summarized in Table 10-8.

Table 10-8 Secure network protocol recommendations

Application or technology	Recommended secure protocol
Voice and video	Secure Real-time Transport Protocol (SRTP)
Time synchronization	Network Time Protocol (NTP)
Email	Secure/Multipurpose Internet Mail Extensions (S/MIME)
Web browsing	Hypertext Transport Protocol Secure (HTTPS)
File transfer	Secure FTP (SFTP)
Directory services	Secure Sockets Layer (SSL)
Remote access	Virtual Private Network (VPN)
Domain name resolution	DNS Security Extensions (DNSSEC)
Routing and switching	IP Security (IPsec)
Network address translation	IP Security (IPsec)
Subscription services	IP Security (IPsec)

TWO RIGHTS & A WRONG

1. The current version of SNMP is SNMPv2.
2. SFTP is considered more secure than FTPS.
3. A mail gateway can automatically and transparently encrypt outbound email messages.

See Appendix B for the answer.

VM LAB You're now ready to complete the live, virtual machine labs for this module. The labs can be found in the Practice It folder in each MindTap module.

SUMMARY

- Cloud computing is a popular and flexible approach to computing resources. All cloud resources are available online from virtually anywhere, and access is achieved through a web browser without the need for installing additional software. Cloud computing allows an almost endless array of servers, software, and network appliances to be quickly and easily configured as needed, and then as computing needs increase or decrease, these resources can be quickly scaled up or scaled back. As a pay-per-use computing model, customers pay only for the online computing resources they need.
- A public cloud is one in which the services and infrastructure are offered to all users with access provided remotely through the Internet. A community cloud is a cloud that is open only to specific organizations that have common concerns. A private cloud is created and maintained on a private network. Although this type offers the highest level of security and control (because the company must purchase and maintain all the software and hardware), it also reduces cost savings. A hybrid cloud is a combination of public and private clouds.
- Computing now takes place in several different locations. On-premises is computing resources located on the campus of the organization while off-premises is a computing resource hosted and supported by a third party. Fog is a decentralized computing infrastructure in which data, compute capabilities, storage, and applications are located between the data source and the cloud. Edge is computing that is performed

at or very near to the source of data instead of relying on the cloud or on-prem for processing. Cloud is a remote facility for computing.

- There are many elements that make up a cloud architecture. A thin client is a computer that runs from resources stored on a central cloud server instead of a localized hard drive. A transit gateway is a technology that allows organizations to connect all existing virtual private clouds (VPC), physical data centers, remote offices, and remote gateways into a single managed source. A serverless infrastructure is one in which the capacity planning, installation, setup, and management are all invisible to the user because they are handled by the cloud provider.
- There are several services models in cloud computing. Software as a Service (SaaS) is a cloud computing hosted software environment. Platform as a Service (PaaS) provides a software platform on which the enterprise or users can build their own applications and then host them on the PaaS provider's infrastructure. Infrastructure as a Service (IaaS) provides unlimited "raw" computing, storage, and network resources that the enterprise can use to build its own virtual infrastructure in the cloud. Anything as a Service (XaaS) describes a broad category of subscription services related to cloud computing. XaaS is any IT function or digital component that can be transformed into a service for enterprise or user consumption. Cloud management can be conducted by the local organization performing the work itself or by contracting with a third-party management service provider.
- Cloud computing has several potential security issues. Mitigating these issues involves using security controls. Some controls are inherent to the cloud computing platforms and offered by the cloud computing providers to their customers (cloud native controls) while other security controls are available from external sources (third-party solutions). One control is a cloud security audit conducted by as an independent examination of cloud service controls. Once completed, the auditor renders an objective assessment of the security. Another control uses regions and zones. In a cloud computing environment, reliability and resiliency is achieved through duplicating processes across one or more geographical areas. This is called high availability across zones. Secrets management enables strong security and improved management of a microservices-based architecture. It allows the entire cloud infrastructure to remain flexible and scalable without sacrificing security. Cloud computing has three functional areas: storage, network, and compute. Each of these has its own set of security mitigations.
- While securing the functional areas of the cloud (storage, networking, and compute) is universally considered as important, an area often overlooked is application security or protecting applications. A cloud access security broker (CASB) is a set of software tools or services that resides between an enterprise's on-prem infrastructure and the cloud provider's infrastructure. Acting as the gatekeeper, a CASB ensures that the security policies of the enterprise extend to its data in the cloud. Just as security appliances in a physical network are important, so too are security virtual devices in a cloud computing environment. Next generation secure web gateways and virtual firewalls are considered important. However, determining which security appliances to implement in a cloud computing infrastructure is more challenging due to a lack of a cloud conceptual model.
- Virtualization is a means of managing and presenting computer resources by function without regard to their physical layout or location. One type of virtualization in which an entire operating system environment is simulated is known as host virtualization. Instead of using a physical computer, a VM, which is a simulated software-based emulation of a computer, is created instead. Virtualization is used to consolidate multiple physical servers into VMs that can run on a single physical computer. Virtualization is used extensively in cloud computing environments. The VM monitor program is called a hypervisor, which manages the VM operating systems. A reduced instance of virtualization is a container. A container holds only the necessary OS components such as binary files and libraries that are needed for that specific application to run.
- Instances of virtualization are sometimes referred to as infrastructure as code. A software-defined network (SDN) virtualizes parts of the physical network so that it can be more quickly and easily reconfigured by separating the control plane from the data plane. Software-defined visibility (SDV) is a framework that allows users to create programs in which critical security functions that previously required manual intervention can now be automated. There are security concerns for virtualized environments. One concern is that VMs may be able to "escape" from the contained environment and directly interact with the host

operating system. It is important to have virtual machine escape protection so that a VM cannot directly interact with the host operating system and potentially infect it, which could then be transmitted to all other VMs running on the host operating system. Another concern is that VMs can easily and quickly be created and launched, leading to virtual machine sprawl, or the widespread proliferation of VMs without proper oversight or management, increasing security vulnerabilities. Combating VM sprawl is called virtual machine sprawl avoidance.

- There are several secure network protocols that are used today. The Simple Network Management Protocol (SNMP) is a popular protocol used to manage network equipment and is supported by most network equipment manufacturers. It allows network administrators to remotely monitor, manage, and configure devices on the network. DNS attacks can be thwarted by using Domain Name System Security Extensions (DNSSEC), which adds resource records and message header information to verify that the requested data has not been altered in transmission. Transferring files can be performed using the File Transfer Protocol (FTP), which is an unsecure TCP/IP protocol. FTP Secure (FTPS) uses SSL or TLS to encrypt commands sent over the control port in an FTP session. Another option is to use Secure FTP (SFTP), which uses only a single TCP port instead of two ports like FTPS and encrypts and compresses all data and commands.
- There are two different electronic email systems that are in use today. An earlier email system uses two TCP/IP protocols to send and receive messages: the Simple Mail Transfer Protocol (SMTP) handles outgoing mail, while the Post Office Protocol (POP), more commonly known as POP3 for the current version) is responsible for incoming mail. IMAP (Internet Mail Access Protocol) is a more recent and advanced electronic email system for incoming mail. The Lightweight Directory Access Protocol (LDAP) is a directory service database stored on the network itself that contains information about users and network devices. A weakness of LDAP is that it can be subject to LDAP injection attacks. Internet Protocol version 6 (IPv6) addresses the weaknesses of the older version IPv4 and also provides several other significant improvements, including stronger security.

Key Terms

Anything as a Service (XaaS)
API inspection and integration
application security
cloud
cloud access security broker (CASB)
cloud computing
cloud native controls
cloud security audit
cloud service providers
community cloud
container
container security
directory service
Domain Name System Security Extensions (DNSSEC)
dynamic resource allocation
edge
File Transfer Protocol (FTP)
fog
FTP Secure (FTPS)
high availability across zones
hybrid cloud
IMAP (Internet Mail Access Protocol)
Infrastructure as a Service (IaaS)
instance awareness
Internet Protocol version 6 (IPv6)
LDAP injection attacks
Lightweight Directory Access Protocol (LDAP)
managed security service provider (MSSP)
managed service provider (MSP)
microservices APIs
microservices architecture
next generation secure web gateway (SWG)
off-premises
on-premises
Open Source Interconnection (OSI) seven-layer model
Platform as a Service (PaaS)
Post Office Protocol (POP)
private cloud
private subnet
public cloud
public subnet
resource policies
secrets management
Secure FTP (SFTP)
security groups
serverless infrastructure
services integration
Simple Mail Transfer Protocol (SMTP)
Simple Network Management Protocol (SNMP)
SNMPv3
Software as a Service (SaaS)
software-defined network (SDN)
software-defined visibility (SDV)
thin client
third-party solutions
transit gateway
virtual machine escape protection
virtual machine sprawl avoidance
virtual network
virtualization

Review Questions

1. Which of the following is NOT a characteristic of cloud computing?
   a. Metered services
   b. Immediate elasticity
   c. Universal client support
   d. Invisible resource pooling

2. Zuzana is creating a report for her supervisor about the cost savings associated with cloud computing. Which of the following would she NOT include on her report on the cost savings?
   a. Reduction in broadband costs
   b. Resiliency
   c. Scalability
   d. Pay-per-use

3. Aleksandra, the company HR manager, is completing a requisition form for the IT staff to create a type of cloud that would only be accessible to other HR managers like Aleksandra who are employed at manufacturing plants. The form asks for the type of cloud that is needed. Which type of cloud would best fit Aleksandra's need?
   a. Public cloud
   b. Group cloud
   c. Hybrid cloud
   d. Community cloud

4. Alicja is working on a project to deploy automated guided vehicles on the industrial shop floor of the manufacturing plant in which she works. What location of computing would be best for this project?
   a. Fog
   b. Edge
   c. Off-premises
   d. Remote

5. Wiktoria is frustrated that her company is using so many different cloud services that span multiple cloud provider accounts and even different cloud providers. She wants to implement a technology to give full control and visibility over all the cloud resources, including network routing and security. What product does Wiktoria need?
   a. Thin virtual visibility appliance (TVVA)
   b. SWG
   c. CASB
   d. Transit gateway

6. What does the term "serverless" mean in cloud computing?
   a. The cloud network configuration does not require any servers.
   b. Server resources of the cloud are inconspicuous to the end user.
   c. Servers are run as VMs.
   d. All appliances are virtual and do not interact with physical servers.

7. Oliwia has been given a project to manage the development of a new company app. She wants to use a cloud model to facilitate the development and deployment. Which cloud model will she choose?
   a. SaaS
   b. XaaS
   c. IaaS
   d. PaaS

8. Which cloud model requires the highest level of IT responsibilities?
   a. IaaS
   b. SaaS
   c. PaaS
   d. Hybrid cloud

9. The CEO is frustrated by the high costs associated with security at the organization and wants to look at a third party assuming part of their cybersecurity defenses. Nikola has been asked to look into acquiring requests for proposal (RFPs) from different third parties. What are these third-party organizations called?
   a. MSSPs
   b. MPSs
   c. MSecs
   d. MHerrs

10. Which of the following is NOT a cloud computing security issue?
    a. System vulnerabilities
    b. Insecure APIs
    c. Compliance regulations
    d. Bandwidth utilization

11. Which of the following is NOT correct about high availability across zones?
    a. In a cloud computing environment, reliability and resiliency are achieved through duplicating processes across one or more geographical areas.

b. An Availability Zone (AZ) is one or more data centers within a Region, each with redundant power, networking, and connectivity.
c. They are more highly available, fault tolerant, and scalable than would be possible with a single data center.
d. They require that specific security appliances be located on-prem so that the local data center can be considered as a qualified Zone.

12. Which of these is NOT created and managed by a microservices API?
a. User experience (UX)
b. Database
c. Logs
d. Authentication

13. Which of the following is true about secrets management?
a. It provides a central repository.
b. It can only be used on-prem for security but has a connection to the cloud.
c. It requires AES-512.
d. It cannot be audited for security purposes.

14. Nadia has been asked to perform dynamic resource allocation on specific cloud computing resources. What action is Nadia taking?
a. Creating security groups to segment computing resources into logical groupings that form network perimeters
b. Decreasing the network bandwidth to the cloud
c. Deprovisioning resources that are no longer necessary
d. Expanding the visibility of intrusion prevention devices

15. Which of the following is NOT a feature of a next generation SWG?
a. DLP
b. Send alerts to virtual firewalls
c. Analyze traffic encrypted by SSL
d. Can be placed on endpoints, at the edge, or in the cloud

16. Which type of hypervisor runs directly on the computer's hardware?
a. Type I
b. Type II
c. Type III
d. Type IV

17. Which of the following is NOT correct about containers?
a. Containers start more quickly.
b. Containers reduce the necessary hard drive storage space to function.
c. Containers require a full OS whenever APIs cannot be used.
d. Containers include components like binary files and libraries.

18. Which of the following virtualizes parts of a physical network?
a. SDN
b. SDV
c. SDX
d. SDA

19. Which of the following will NOT protect containers?
a. Using a hardened OS
b. Using reduced-visibility images to limit the risk of a compromise
c. Only using containers in a protected cloud environment
d. Eliminating APIs

20. Which of the following provides the highest level of security?
a. FTP
b. XFTP
c. FTPS
d. SFTP

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 10-1: Viewing SNMP Management Information Base (MIB) Elements

Time Required: 20 minutes
Objective: Given a scenario, implement secure protocols.
Description: SNMP information is stored in a management information base (MIB), which is a database for different objects. In this project, you view MIBs.

1. Use your web browser to go to **www.mibdepot.com**. (The location of content on the Internet may change without warning. If you are no longer able to access the program through this URL, use a search engine to search for "MIB Depot.")
2. In the left pane, click **Single MIB View**.
3. Scroll down and click **Linksys** in the right pane. This will display the Linksys MIBs summary information.
4. In the left pane, click **v1 & 2 MIBs** to select the SNMP Version 1 and Version 2 MIBs.
5. In the right pane, click **LINKSYS-MIB** under **MIB Name (File Name)**. This will display a list of the Linksys MIBs.
6. Click **Tree** under **Viewing Mode** in the left pane. The MIBs are now categorized by Object Identifier (OID). Each object in a MIB file has an OID associated with it, which is a series of numbers separated by dots that represent where on the MIB "tree" the object is located.
7. Click **Text** in the left pane to display textual information about the Linksys MIBs. Scroll through the Linksys MIBs and read several of the descriptions. How could this information be useful in troubleshooting?
8. Now look at the Cisco MIBs. Click **Vendors** in the left pane to return to a vendor list.
9. Scroll down and click **Cisco Systems** in the right pane. How many total Cisco MIB objects are listed? Why is there a difference?
10. In the right pane, click the link **Traps**.
11. Scroll down to **Trap 74**, which begins the list of Cisco wireless traps. Notice the descriptive names assigned to the wireless traps.
12. Close all windows.

Project 10-2: Using a Secure Email Feature

Time Required: 25 minutes
Objective: Given a scenario, implement secure protocols.
Description: Basic email lacks many privacy features. However, settings are available that allow users to encrypt and control emails. In this project, you will configure Google Gmail to send and open confidential emails.

1. Launch your Gmail email account.
2. Click **Compose** to open the **New Message** screen to create a new email message.
3. In the **To** field enter the address of someone who also has a Gmail account.
4. In the row of icons at the bottom of the **New Message** screen, click the icon that represents **Turn confidential mode on/off** (you can hover your mouse over the icons to display their functions).
5. The **Confidential mode** dialog box will open. Click **Learn more** and read about sending and opening confidential emails.
6. Return to the **Confidential mode** dialog box.
7. Under **Set Expiration**, click the down arrow and change the expiration to **Expires in 1 day**.
8. Under **Require Passcode**, click **SMS passcode**.
9. Click **Save**.
10. Note at the bottom of the **New Message** screen it tells when the email content will expire and that recipients cannot forward, copy, print, or download this email message.
11. Compose a brief message and click **Send**.
12. The **Confirm phone numbers** dialog box appears. This is required for the recipient of the email to receive a passcode through a text message. Enter the phone number of the email recipient and click **Send**.
13. The recipient of the email message will receive a text message with a passcode, which is used to open the email message that you sent.
14. The options to copy, paste, download, print, and forward the email message text will be disabled. The recipient can view the message and attachments until the expiration date or until the sender removes access.
15. How valuable is this feature? Is it easy to use? What are its limitations?
16. Close all windows.

Project 10-3: Creating a Virtual Machine from a Physical Computer

Time Required: 25 minutes
Objective: Summarize virtualization and cloud computing concepts.
Description: The VMware vCenter Converter creates a virtual machine from an existing physical computer. In this project, you download and install vCenter to create a virtual machine.

1. Use your web browser to go to **www.vmware.com**. (The location of content on the Internet may change without warning. If you are no longer able to access the program through this URL, use a search engine to search for "VMware.")
2. Click **Downloads**.
3. Click **Free Products Downloads**.
4. Click **vCenter Converter**.
5. If necessary, click **Create an account**, enter the requested information, and log into VMware.
6. If necessary, accept the terms of use and click **I agree**.
7. Click **Manually Download**.
8. When the download completes, run the installation program to install vCenter by accepting the default settings.
9. Launch vCenter to display the VMware vCenter Converter Standalone menu.
10. Click **Convert machine**.
11. Under **Select source type**, choose **This local machine**. Click **Next**.
12. Next to **Select destination type**, choose **VMware Workstation or other VMware virtual machine**.
13. Under **Select a location for the virtual machine**, click **Browse**.
14. Navigate to a location to store the new virtual machine. Click **Next** and then click **Next** again.
15. Click **Finish** to create the virtual machine from the physical machine.

NOTE 25

Note that depending upon the computer configuration, it could take up to 60 minutes to create the virtual machine.

16. When the vCenter has finished, note the location of the image, which will be one or more *.vmx and *.vmdk files in the destination folder. It will be used in the next project.
17. Close all windows.

Project 10-4: Loading the Virtual Machine

Time Required: 25 minutes
Objective: Summarize virtualization and cloud computing concepts.
Description: In this project, you download a program to load the virtual machine created in Project 10-3.

1. Use your web browser to go to **my.vmware.com**. (The location of content on the Internet may change without warning. If you are no longer able to access the program through this URL, use a search engine to search for "VMware Workstation.")
2. Click **Downloads**.
3. Click **Free Products Downloads**.
4. Click **Workstation Player**.
5. Select the Workstation Player for your computer's operating system. Click **Download**.
6. When the download completes, launch the installation program to install VMware Workstation Player.
7. Start VMware Workstation Player after the installation completes.
8. Click **Open a Virtual Machine**.
9. Navigate to the location of the virtual machine that you created in Project 10-3. Click **Open**.
10. Click **Edit virtual machine settings**. Note the different options for configuring the hardware of the virtual machine. Click through these options and, if desired, change any of the settings. Click **Close**.

NOTE 26

Note that to run this virtual machine, a previously unlicensed version of the operating system must first be installed.

11. How easy was it to create a virtual machine from a physical machine?
12. Close all windows.

Case Projects

Case Project 10-1: Trustworthy Email Protocols and Standards

In addition to S/MIME, there are several protocols and standards that protect email. These include STARTTLS, DNS-Based Authentication of Named Entities (DANE), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC). Use the Internet to research each of these. Create a summary of each along with the respective strengths and weaknesses. Which would you recommend? Why?

Case Project 10-2: Secrets Management Systems

Cloud computing providers typically offer their own proprietary secrets management systems, and there are several third-party systems available. Identify two proprietary secrets management systems from cloud providers and two third-party systems. Research each and then create a document outlining how they are used, their strengths, and their weaknesses.

Case Project 10-3: Comparing MSSPs

Identify three MSSPs and research the services that they provide. Create a document that outlines the services provided by each MSSP. Would you support contracting with an MSSP for part of an organization's security functions? Would you support using an MSSP for all security functions? Write a one-page paper arguing both the pros and cons of using MSSPs.

Case Project 10-4: Create a Cloud Conceptual Model

Use the Internet to research different cloud conceptual models and identify at least three. Then create your own model. Draw the different layers and label each along with how each layer would function.

Case Project 10-5: IPv6

Use the Internet to research the security enhancements of IPv6. Write a one-page paper on how IPv6 is more secure than IPv4.

Case Project 10-6: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to log in, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and click on **Security+ Case Projects (7th edition)**. Read the following case study.

Suppose you were working as part of a cybersecurity defense team at an organization and you were told that the company is considering hiring a managed security service provider (MSSP) to handle the cybersecurity functions. What arguments would you give to support this proposal? What reasons would you give for not supporting this proposal? Visit the Community Site discussion board and post how you would feel about MSSPs.

Case Project 10-7: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

The new CEO of Premier Landscape Services (PLS) wants to migrate all IT functions to the cloud. He argues that PLS could then downsize the IT staff as well as eliminate the need to purchase hardware and software on a regular cycle. The CEO also wants to outsource all security functions to MSSPs. The current CIO supports a migration to the cloud but only for selected services, and is opposed to using MSSPs for security. North Ridge has been brought in to help PLS.

1. Create a PowerPoint presentation for the executive staff about cloud computing. Include types of clouds, locations, architectures, models, and management. Your presentation should contain at least 10 slides.
2. The CEO of PLS was impressed with your knowledge of cloud computing and has asked for your opinion of moving all IT resources to the cloud and contracting with MSSPs for security. Create a memo that outlines the advantages and disadvantages of each side of the argument, and then give your recommendation.

References

1. Mell, Peter, and Grance, Tim, "The NIST definition of cloud computing," NIST Computer Security Division Computer Security Resource Center. Oct. 7, 2009, accessed Apr. 2, 2011, http://csrc.nist.gov/groups/SNS/cloud-computing/.
2. Donovan, Fred, "Shadow IT plagues organizations, undermining cloud security", *HIT Infrastructure*, Feb. 21, 2019, accessed Jul. 3, 2020, https://hitinfrastructure.com/news/shadow-it-plagues-organizations-undermining-cloud-security.
3. "Email & spam data," *Cisco Talos,* accessed Jul. 7, 2020, https://talosintelligence.com/reputation_center/email_rep.

MODULE 11

WIRELESS NETWORK SECURITY

After completing this module, you should be able to do the following:

1. Describe the different types of wireless network attacks
2. List the vulnerabilities of WLAN security
3. Explain the solutions for securing a wireless network

Front-Page Cybersecurity

Attacks on wireless systems are certainly not uncommon. But it may be surprising to learn that the first recorded attack on a wireless system occurred more than 100 years ago and involved the person credited as the inventor of the radio.

Guglielmo Marconi was an Italian electrical engineer and inventor who pioneered work on long-distance radio transmission. In 1895, Marconi could transmit and receive a signal for only less than one mile (1.6 kilometers or km), but through persistence and applying new techniques, he was able to increase that distance the following year to 3.7 miles (6 km). Over the next several years, the distances gradually became longer, so that by 1900, Marconi was experimenting with transmissions across the Atlantic Ocean, which he achieved the following year. However, skeptics challenged this experiment because it was not independently verified. One of Marconi's skeptics was Nevil Maskelyne, who likewise was an inventor interested in wireless systems. Maskelyne was the manager of a rival wireless company that had been involved in several disputes with Marconi over patents for wireless telegraphy systems.

In 1903, Marconi decided to put on a public demonstration of his wireless system. He wanted to show that it could indeed transmit over long distances. But he also wanted to demonstrate that his wireless system was secure. Marconi had often claimed that other signals would not interfere with his wireless transmissions. Maskelyne, on the other hand, was not convinced that Marconi's signal was secure. So Maskelyne decided to "hack" Marconi's public demonstration.

The demonstration was on June 4, 1903, at the lecture theater of the Royal Institution in London. Marconi was in Cornwall, more than 300 miles (482 km) away. The plan was for Marconi's colleague Professor Fleming to be in the theater to receive Marconi's Morse code message sent wirelessly and to be printed on an attached printer. But Maskelyne had his own ideas. He set up a wireless transmitter not far from the lecture theater. He later claimed that he did not run it at full power because he did not want to block Marconi's signal; instead, he wanted to send his own signal to show that Marconi's signal was not secure.

Toward the end of Fleming's lecture, signals started coming in—but they were not from Marconi. First a brass slide projector arc lamp in the theater, used to display Fleming's presentation, made a rhythmic ticking noise. The audience assumed that the projector was malfunctioning. But Arthur Blok, Fleming's assistant, quickly recognized it as the "tap-tap"

of a human hand keying a message in Morse code. Blok realized that someone was sending powerful wireless pulses into the theater, strong enough to interfere with the electric arc lamp. The wireless receiver came to life, and the Morse code printer started printing—but the message was from Maskelyne instead of from Marconi. One word was repeated over and over on the printer: "Rats." Then the printer spelled out an insulting limerick. Marconi's supposedly secure wireless system had been hacked.

Fleming later complained to the *London Times* of "scientific hooliganism." Fleming and Maskelyne exchanged letters, many of which were printed in the *Times*, arguing over the source of the interference. (Fleming argued that it was caused by electrical lighting in the theater.) It was also discovered that the receiver Fleming used was not tuned to the specific frequency on which Marconi was transmitting but was a receiver that could pick up signals across the frequency spectrum. Because this fact was not disclosed to the audience, the public felt that Marconi had been deceptive in his demonstration. When Maskelyne later wrote about the incident, he ended his account with a Latin legal phrase translated as, "Let him be deceived who wishes to be deceived."

Maskelyne's attack had little impact on Marconi's work or reputation. After sending the first wireless signal across the Atlantic in 1901, Marconi started a commercial transatlantic wireless service 1907. In 1909, he shared the Nobel Prize in Physics in recognition of his contributions to the development of wireless telegraphy. When Marconi died in 1937, the British Broadcasting Company (BBC) observed two minutes of radio silence in respect.

What Maskelyne's attack did do, however, was to make the scientific community question Marconi's claim that wireless signals were secure and could not be interfered with. Researchers examined how wireless signals could be monitored, jammed, or manipulated. Eventually, the research led to the development of wireless security measures that were first used in World War I and continue today.

Ubiquitous means *being everywhere*. Perhaps that is the best word to describe wireless data networks. They are *everywhere*. When was the last time you were at a coffee shop that did not have Wi-Fi? Or a library? Or a hotel? Or even a sports stadium? Not only do we expect wireless networks everywhere, but we demand it: a coffee shop that does not have Wi-Fi has more than its share of empty seats.

Statistics confirm how widespread wireless data technology has become. Almost 70 percent of the global population, about 5.7 billion users, will have wireless data connectivity by 2023 and will be using 13.1 billion devices (an increase from 8.8 billion devices in 2018). The number of public Wi-Fi hotspots will increase fourfold from 169 million in 2018 to 628 million by 2023, and the speeds at which they transmit will be even faster: Wi-Fi speeds will triple by 2023. Retail establishments will have the highest number of hotspots globally by 2023, while the fastest growth is in healthcare facilities such as hospitals, where Wi-Fi hotspots will triple.[1]

NOTE 1

The impact of those who consume the most wireless data is now inverted: in 2010, the top 1 percent of mobile users accounted for more than half of all mobile data usage; by 2019, the top 1 percent only accounted for 5 percent of wireless data usage.

Just as users are drawn to wireless data networks, so too are attackers. Wi-Fi and other wireless data networks are tempting and often too-easy targets for attackers to compromise, despite the wide range of security protections available to modern devices. However, these protections are often overlooked or misconfigured, or users are not aware of their importance.

This module explores wireless network security. You will first investigate the attacks on wireless devices that are common today. Next, you will explore vulnerabilities in wireless security. Finally, you will examine several secure wireless protections.

WIRELESS ATTACKS

CERTIFICATION

1.4 Given a scenario, analyze potential indicators associated with network attacks.

3.4 Given a scenario, install and configure wireless security settings.

3.5 Given a scenario, implement secure mobile solutions.

Several attacks can be directed against wireless data systems. These are attacks against Bluetooth systems, near field communication devices, radio frequency identification systems, and wireless local area networks.

Bluetooth Attacks

Bluetooth is the name given to a wireless technology that uses short-range radio frequency (RF) transmissions and provides rapid device pairings. Named after the tenth-century Danish King Harald "Bluetooth" Gormsson, who was responsible for unifying Scandinavia, Bluetooth was originally designed in 1994 by the cellular telephone company Ericsson to replace personal computer cables. However, Bluetooth has moved well beyond its original design.

Bluetooth is a *personal area network (PAN)* technology designed for data communication over short distances and enables users to connect wirelessly to a wide range of computing and telecommunications devices. It provides for virtually instantaneous connections with little user intervention between a Bluetooth-enabled device and receiver. Several Bluetooth-enabled products are listed in Table 11-1.

Table 11-1 Bluetooth Products

Category	Bluetooth pairing	Usage
Automobile	Hands-free car system with cell phone	Drivers can speak commands to browse the cell phone's contact list, make and receive hands-free phone calls, or use its navigation system.
Home entertainment	Stereo headphones with portable music player	Users can create a playlist on a portable music player and listen through a set of wireless headphones or speakers.
Photographs	Digital camera with printer	Digital photos can be sent directly to a photo printer or from pictures taken on one cell phone to another phone.
Computer accessories	Computer with keyboard and mouse	Small travel mouse can be linked to a laptop or a full-size mouse and keyboard that can be connected to a desktop computer.
Sports and fitness	Heart rate monitor with wristwatch	Exercisers can track heart rates and blood oxygen levels.
Medical and health	Blood pressure monitors with smartphones	Patient information can be sent to a smartphone, which can then send an emergency phone message if necessary.

NOTE 2

Bluetooth is also finding its way into some unlikely devices. A Victorinox Swiss Army pocketknife model has Bluetooth technology that can be used to remotely control a computer when projecting a PowerPoint presentation. Other unusual devices include Bluetooth-enabled toothbrushes, keychain breathalyzers, stethoscopes, and even trash cans that send reminders to take out the garbage.

The current version, Bluetooth 5.2, was introduced in early 2020. (All Bluetooth devices are backward compatible with previous versions.) There are two implementations of Bluetooth 5.2. Bluetooth *Classic*, also called *Bluetooth Basic Rate/Enhanced Data Rate* (*BR/EDR*), is designed for devices needing short-range continuous connectivity (such as streaming music to a Bluetooth headset), while Bluetooth *low energy (LE)* is for devices that require short bursts of data over longer distances (such as inventory control devices at a retail store). The number of *bits per second (bps)* that Bluetooth LE can transmit is between 125 Kbps and 2 Mbps, while Bluetooth Classic supports data rates from 1 Mbps to 3 Mbps. Bluetooth devices are categorized by their *class*; currently, there are three classes of Bluetooth devices. The advertised ranges for Class 1 devices are up to 328 feet (100 meters), Class 2 devices have a maximum range of 98 feet (30 meters), and Class 3 devices can send and receive up to 33 feet (10 meters).

CAUTION

A number of factors can affect the range of transmission. For Bluetooth, this includes the physical layer of the protocol, the receiver sensitivity, the device's transmit power, antenna gain, and path loss. Advertised ranges are generalizations of the range of transmission.

The primary type of Bluetooth network topology is a *piconet*. When two Bluetooth devices come within range of each other, after an initial pairing confirmation, they automatically connect whenever they meet. One device is the leader, which controls all the wireless traffic. The other device is a follower that takes commands from the leader. Follower devices that are connected to the piconet and are sending transmissions are active followers; devices that are connected but not actively participating are parked followers. Devices can also switch roles so that a follower temporarily becomes a leader but then switches back to a follower role or vice versa. An example of two piconets with multiple followers is illustrated in Figure 11-1.

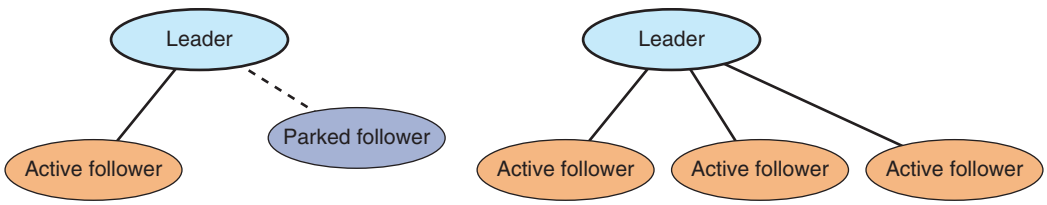


Figure 11-1 Bluetooth piconets

NOTE 3

The Bluetooth specification also allows for a device to be a member in two or more overlaying piconets that cover the same area. This group of piconets in which connections exist between different piconets is called a *scatternet*. However, scatternets are rarely used.

The *network topology* (the arrangement of the nodes of a communication network) of Bluetooth is usually **point-to-point** (one device connected one device—or, in the case of Bluetooth, one follower connected to one leader) or **point-to-multipoint** (one device connected to multiple devices), as seen in Figure 11-1. The point-to-multipoint Bluetooth topology allows, for example, a single Bluetooth-enabled smartphone to control multiple Bluetooth devices (such as a speaker and fitness tracker). Bluetooth LE also supports a *many-to-many* topology, known as a *mesh*. Mesh topologies are often used to extend the range of a Bluetooth network: instead of being limited to the range a follower can communicate with its leader, a follower can send packets to another follower closer to the leader, who can then send it on to yet another follower still closer to the leader, until the packet reaches the leader.

One of the primary features of Bluetooth is its ability for followers to connect to a leader dynamically and automatically "on the fly" as needed whenever Bluetooth devices enter and leave the coverage area. However, this also opens the door for attacks on Bluetooth. Two common Bluetooth attacks are bluejacking and bluesnarfing.

NOTE 4

Bluejacking has been used for advertising purposes by vendors.

Bluejacking

Bluejacking is an attack that sends unsolicited messages to Bluetooth-enabled devices. Usually, bluejacking involves sending text messages, though images and sounds also can be transmitted. Bluejacking is usually considered more annoying than harmful because no data is stolen; however, many Bluetooth users resent receiving unsolicited messages.

Bluesnarfing

Bluesnarfing is an attack that accesses unauthorized information from a wireless device through a Bluetooth connection. In a bluesnarfing attack, the attacker copies emails, calendars, contact lists, cell phone pictures, or videos by connecting to the Bluetooth device without the owner's knowledge or permission.

NOTE 5

Bluejacking and bluesnarfing can be mitigated by turning off Bluetooth when not needed, making the device non-discoverable, or rejecting pairing requests from an unknown device.

Near Field Communication (NFC) Attacks

Near field communication (NFC) is a set of standards used to establish communication between devices in very close proximity. Once the devices are brought within four centimeters of each other or tapped together, two-way communication is established. Devices using NFC can be active or passive. A *passive NFC* device, such as an NFC tag, contains information that other devices can read. The tag does not read or receive any information. *Active NFC* devices can read information as well as transmit data.

The NFC communication between a smartphone and an NFC tag functions as follows:

1. The smartphone (*interrogator*) sends a signal to the tag, which becomes powered by the energy in the interrogator's wireless signal.
2. The interrogator and tag each create a high-frequency magnetic field from an internal antenna. Once the fields are created, a connection can be formed between the devices (known as *magnetic induction*). This is illustrated in Figure 11-2. (In this figure, the antennas are shown outside of the interrogator and tag for clarity.)
3. The interrogator sends a message to the tag to find out what type of communication the tag uses. When the tag responds, the interrogator sends its first commands based on that type.
4. When the tag receives the instruction, it checks to determine if the instruction is valid. If it is not, the tag ignores the communication. If it is a valid request, the tag responds with the requested information. For sensitive transactions, such as credit card payments, a secure communication channel is established and all transmitted information is encrypted.

NOTE 6

The ability of an NFC tag to be powered by the interrogator's signal allows tags to be very small. It also does not require a tag to have its own battery or another power source.

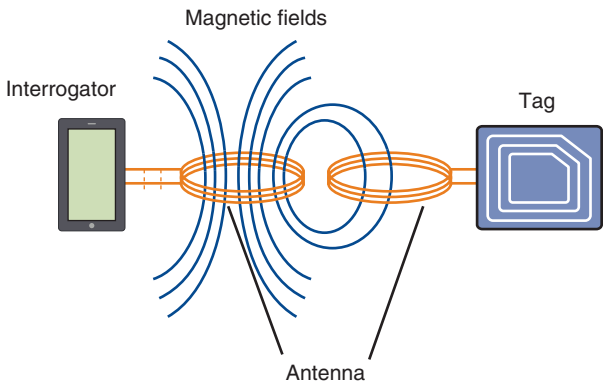


Figure 11-2 NFC magnetic induction

Examples of NFC use include the following:

- *Entertainment.* NFC devices can be used as a ticket to a stadium or concert, for purchasing food and beverages, and downloading upcoming events by tapping a smart poster.
- *Office*. An NFC-enabled device can be used to enter an office, clock in and out on a factory floor, or purchase snacks from a vending machine.
- *Retail stores*. Coupons or customer reward cards can be provided by tapping the point-of-sale (PoS) terminal.
- *Transportation.* On a bus or train, NFC can be used to quickly pass through turnstiles and receive updated schedules by tapping the device on a kiosk.

NOTE 7

There are five types of NFC tags, Type 1 through Type 5, which are used in different settings. For example, Type 2 tags are often used for event tickets and transit passes, while Type 5 is used to tag library books.

Consumer NFC devices are most often used as an alternative to cash or a credit card as a **payment method** and are called *contactless payment systems*. Users store payment card numbers in a "virtual wallet" on a watch or smartphone to pay for purchases at an NFC-enabled PoS checkout device. Figure 11-3 shows one such contactless payment system.

New Africa/Shutterstock.com

Figure 11-3 Contactless payment system

The use of NFC has risks because of the nature of this technology. The risks and defenses of using NFC are listed in Table 11-2.

Table 11-2 NFC Risks and Defenses

Vulnerability	Explanation	Defense
Eavesdropping	Unencrypted NFC communication between the device and terminal can be intercepted and viewed.	Because an attacker must be extremely close to pick up the signal, users should remain aware of their surroundings while making a payment.
Data theft	Attackers can "bump" a portable reader to a user's smartphone in a crowd to make an NFC connection and steal payment information stored on the phone.	This can be prevented by turning off NFC while in a large crowd.
Man-in-the-middle attack	An attacker can intercept the NFC communications between devices and forge a fictitious response.	Devices can be configured in pairing so one device can only send while the other can only receive.
Device theft	The theft of a smartphone could allow an attacker to use that phone for purchases.	Smartphones should be protected with passwords or strong PINs.

NOTE 8

COVID-19 generated a spike in the use of contactless payment systems. About 31 million Americans used these systems in March 2020, when the pandemic began, which was an increase of 150 percent over March 2019.[2]

Radio Frequency Identification (RFID) Attacks

Another wireless technology similar to NFC is **radio frequency identification (RFID)**. RFID is commonly used to transmit information between employee identification badges, inventory tags, book labels, and other paper-based tags that can be detected by a proximity reader. For example, an RFID tag can easily be affixed to the inside of an ID badge and can be read by an RFID reader as the user walks through the turnstile with the badge in a pocket.

Most RFID tags are passive and do not have their own power supply; instead, the electrical current induced in the antenna by the incoming signal from the transceiver provides enough power for the tag to send a response. Because it does not require a power supply, passive RFID tags can be very small, only 0.4 mm × 0.4 mm and thinner than a sheet of paper, as illustrated in Figure 11-4. The amount of data transmitted typically is limited to an ID number. Passive tags have ranges from about one-third inch to 19 feet (10 millimeters to 6 meters). Active RFID tags must have their own power source.

Nor Gal/Shutterstock.com

Figure 11-4 RFID tag

RFID tags are susceptible to attack. Table 11-3 lists several attacks that could occur in a retail store that uses RFID inventory tags.

Table 11-3 RFID Attacks in Retail Store

RFID attack type	Description of attack	Implications of RFID attack
Unauthorized tag access	A rogue RFID reader can determine the inventory on a store shelf to track the sales of specific items.	Sales information could be used by a rival product manufacturer to negotiate additional shelf space or better product placement.
Fake tags	Authentic RFID tags are replaced with fake tags that contain fictitious data about products that are not in inventory.	Fake tags undermine the integrity of the store's inventory system by showing data for items that do not exist.
Eavesdropping	Unauthorized users could listen in on communications between RFID tags and readers.	Confidential data, such as a politician's purchase of antidepressants, could be sold to a rival candidate in a "smear" campaign.

Wireless Local Area Network Attacks

A *wireless local area network (WLAN)*, commonly called **Wi-Fi**, is designed to replace or supplement a wired local area network (LAN). Devices such as tablets, laptop computers, and smartphones that are within range of a centrally located connection device can send and receive information at varying transmission speeds.

The following sections provide a brief history and the specifications of WLAN versions, identify the hardware necessary for a wireless network, and describe the types of WLAN attacks directed at both the enterprise and consumers.

NOTE 9

One of the most well-known IEEE standards is 802.3, which set specifications for Ethernet local area network technology.

WLAN Versions

For computer networking and wireless communications, the most widely known and influential organization is the *Institute of Electrical and Electronics Engineers (IEEE)*, which dates to 1884. In the early 1980s, the IEEE began work on developing computer network architecture standards. This work was called Project 802 and quickly expanded into several categories of network technology.

In 1990, the IEEE started work to develop a standard for WLANs operating at 1 and 2 Mbps. Several proposals were recommended before a draft was developed. This draft, which went through seven revisions, took seven years to complete. In 1997, the IEEE approved the final draft known as *IEEE 802.11*.

Although bandwidth of 2 Mbps was acceptable in 1990 for wireless networks, by 1997, it was no longer sufficient for network applications. The IEEE body revisited the 802.11 standard shortly after it was released to determine what changes could be made to increase the speed. In 1999, a new *IEEE 802.11b* amendment was created, which added two higher speeds (5.5 Mbps and 11 Mbps) to the original 802.11 standard. At the same time, the IEEE also issued another standard with even higher speeds, the *IEEE 802.11a* standard with a speed of 54 Mbps.

The success of the IEEE 802.11b standard prompted the IEEE to reexamine the 802.11b and 802.11a standards to determine if a third intermediate standard could be developed. This "best of both worlds" approach would preserve the stable and widely accepted features of 802.11b but increase the data transfer rates to those similar to 802.11a. The *IEEE 802.11g* standard was formally ratified in 2003 and can support devices transmitting at 54 Mbps.

NOTE 10

Opening the 1–6 GHz spectrum was ratified by the Federal Communications Commission (FCC) for Wi-Fi usage in April 2020. That same month, the Telecom Advisory Service published a report, cited by the FCC, claiming that by allowing usage of this spectrum, the total economic value would be $183 billion between 2020 and 2025, of which $23 billion would be as a result of faster Wi-Fi download speeds.[3]

In 2004, the IEEE began work on a new WLAN standard that would significantly increase the speed, range, and reliability of wireless local area networks. This standard, known as *IEEE 802.11n*, was ratified in 2009. The 802.11n standard has four significant improvements over previous standards: speed (600 Mbps), coverage area (doubles the indoor range and triples the outdoor range of coverage), increased resistance to interference, and stronger security.

Work on an updated standard to support the demand for wireless video delivery, called *IEEE 802.11ac*, was started in 2011. Building on many of the enhancements introduced in 802.11n, this standard, ratified in early 2014, has data rates greater than 7 Gbps. Another update known as *IEEE 802.11ax* is designed to operate in the unlicensed spectrum between 1 and 6 GHz.

To reduce confusion, in 2018, the Wi-Fi Alliance adopted "consumer-friendly" version numbers instead of using "IEEE 802.11" followed by one or two letters. Table 11-4 compares several WLAN standards.

Table 11-4 WLAN Standards

IEEE name	Wi-Fi Alliance version	Ratification date	Frequency used	Maximum data rate
802.11	None	1997	2.4 GHz	2 Mbps
802.11b	Wi-Fi 1	1999	2.4 GHz	11 Mbps
802.11a	Wi-Fi 2	1999	5 GHz	54 Mbps
802.11g	Wi-Fi 3	2003	2.4 GHz	54 Mbps
802.11n	Wi-Fi 4	2009	2.4 GHz & 5 GHz	600 Mbps
802.11ac	Wi-Fi 5	2014	5 GHz	7.2 Gbps
802.11ax	Wi-Fi 6	2019	2.4 GHz & 5 GHz & 1–6 GHz	9.6 Gbps

NOTE 11

Other WLAN standards that are not as widely used include IEEE 802.11ah (HaLow) designed for low-data-rate long-range sensors and controllers, IEEE 802.11af, which uses portions of unused television spectrums instead of 2.4 GHz or 5 GHz bands for transmission, and IEEE 802.11ad, created for very short range but very high speeds.

WLAN Hardware

For all of its functionality, the number of hardware elements needed to operate a WLAN is surprisingly small. Endpoints must have a *wireless client network interface card* or *wireless adapter* that performs the same functions as a wired adapter with one major exception: it has no external cable RJ-45 connection. In its place is an antenna (embedded into the adapter or the device) to send and receive signals through the airwaves.

The second hardware device needed is a wireless *access point (AP)*, which is a centrally located WLAN connection device that can send and receive information. It primarily consists of an antenna and a radio transmitter/receiver to send and receive wireless signals, special bridging software to interface wireless devices to other devices, and a wired network interface that allows it to connect by cable to a standard wired network.

An AP has two basic functions. First, it acts as the "base station" for the wireless network. All wireless devices with a wireless NIC transmit to the AP, which in turn redirects the signal—if necessary—to other wireless devices. The second function of an AP is to act as a bridge between the wireless and wired networks. The AP can be connected to the wired network by a cable, allowing all the wireless devices to access the wired network through the AP (and vice versa), as shown in Figure 11-5.

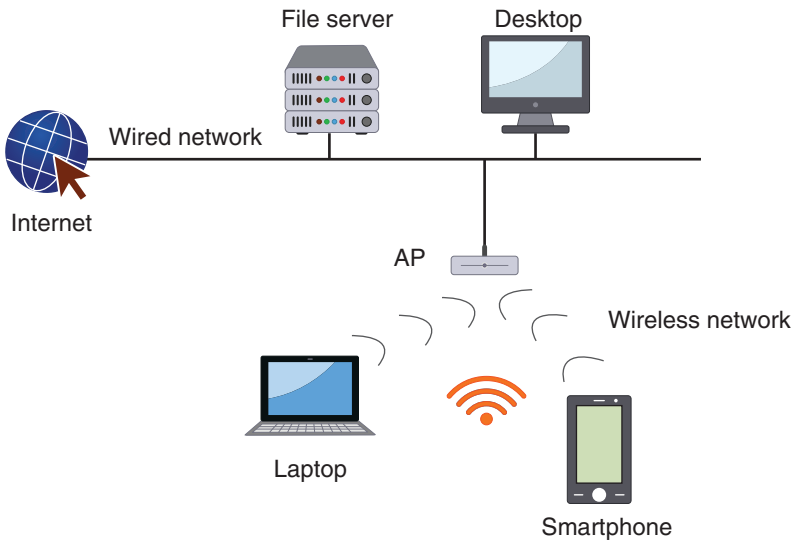


Figure 11-5 Access point (AP) in WLAN

A WLAN using an AP is operating in *infrastructure mode*. The IEEE specifications also define networks that are not using an AP. This mode is called an *Independent Basic Service Set (IBSS)* or, more commonly, **ad hoc mode**. In ad hoc mode, devices can only communicate between themselves and cannot connect to another network. The Wi-Fi Alliance has also created a similar technical specification called **Wi-Fi Direct**.

Instead of using an enterprise-grade AP, a small office or home commonly uses another device that combines multiple features into a single hardware unit. These features often include those of an AP, firewall, router, and dynamic host configuration protocol (DHCP) server, along with other features. Strictly speaking these devices are *residential WLAN gateways* as they are the entry point from the Internet into the wireless network. However, most vendors instead choose to label their products as simply *wireless routers*.

There are different types of enterprise APs. These include fat vs. thin APs, controller vs. standalone, and captive portal APs.

Fat vs. Thin APs Standard APs are *autonomous*, or independent, because they are separate from other network devices and even other autonomous APs. Autonomous

NOTE 12

Ad hoc mode is useful for quickly and easily setting up a wireless network anywhere that users need to share data between themselves but do not need a connection to the Internet or an external network. An example might be when a wireless user needs to quickly send a last-minute document to an associate across the table in a meeting room. However, this mode is rarely used.

APs have the intelligence required to manage wireless authentication, encryption, and other functions for the wireless client devices that they serve. Because everything is self-contained in these single devices, they are sometimes called *fat APs*.

Although fat APs are functional for a small office setting with a handful of APs, what happens in a large enterprise or college campus with hundreds or even thousands of APs? In this case, fat APs are not a viable option. Because each AP is autonomous, a single wireless network configuration change would require reconfiguring each AP individually, which could take an extended period and manpower to complete.

When multiple APs are widely deployed, a *thin AP* can be a better solution. These "lightweight" APs do not contain all the management and configuration functions found in fat APs. Much of the configuration is centralized in the wireless switch so that the network administrator can work directly with the switch from the wired network. This can also improve security because managing from a central location instead of visiting and configuring each fat AP reduces the risk of a security setting being overlooked.

Standalone vs. Controller APs Although thin APs can be managed from a switch, a further improvement can be made by managing from a device dedicated to configuring APs. Instead of installing *standalone APs* like fat or thin APs, **controller APs** can be managed through a dedicated *wireless LAN controller (WLC)*. The WLC is a single device that can be configured and then used to distribute the settings automatically to all controller APs. (A remote office WLAN controller is used to manage multiple WLCs at remote sites from a central location.) Controller APs with a WLC are shown in Figure 11-6.

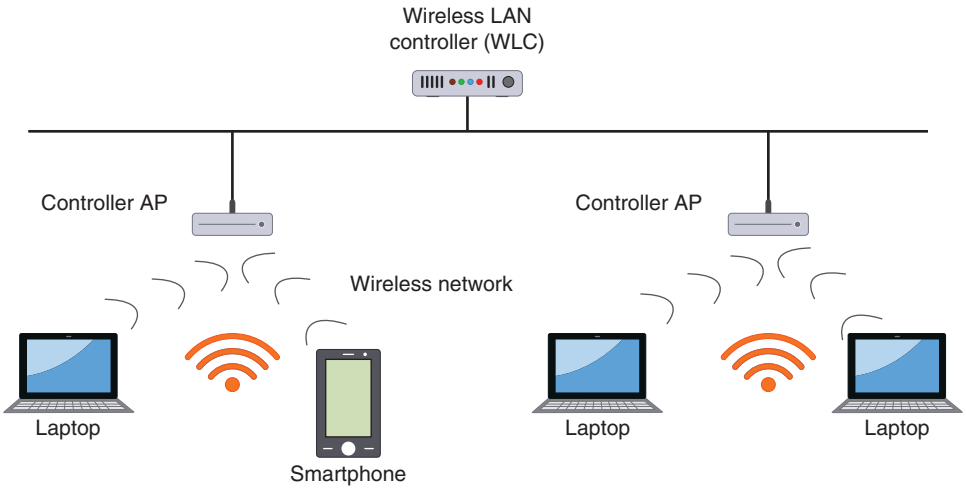


Figure 11-6 Controller APs with WLC

NOTE 13

Controller APs handle only the real-time medium access control (MAC) layer functionality within themselves; all other (non-real-time) MAC functionality is processed by the WLC. This type of division is referred to as a *split MAC architecture*.

Besides centralized management, controller APs provide other advantages over standalone APs. As wireless client devices move through a WLAN, a lengthy handoff procedure occurs during which one standalone AP transfers authentication information to another. Slow handoffs can be unacceptable on WLAN systems using time-dependent communication, such as voice or video. With controller APs, however, this handoff procedure is eliminated because all authentications are performed in the WLC. Another advantage of WLCs is the tools that many provide for monitoring the environment and providing information regarding the best locations for APs, wireless configuration settings, and power settings.

CAUTION

There are disadvantages to controller APs. WLCs still do not provide true convergence (integration) of the wired and wireless networks but only ease some of the management burdens of WLANs. In addition, these devices are proprietary, which means all the thin APs and WLCs on a network must be from the same vendor to function cohesively.

Captive Portal APs In a public area that is served by a WLAN, opening a web browser rarely gives immediate Internet access because the owner of the WLAN usually wants to advertise itself as providing this service, or wants the user to read and accept an acceptable use policy (AUP) before using the WLAN. Sometimes a general authentication, such as a password given to all current hotel guests, must be entered before users gain access to the network. This type of information, approval, or authentication can be supported through a **captive portal AP**. A captive portal AP uses a standard web browser to present information and gives the wireless user the opportunity to agree to a policy or enter valid login credentials, providing a higher degree of security.

CAUTION

When accessing a public WLAN, users should consider using a virtual private network (VPN) to encrypt all transmissions.

WLAN Enterprise Attacks

In a traditional wired network, a well-defined boundary or "hard edge" protects data and resources. There are two types of hard edges. The first is a network hard edge. A wired network typically has one point (or a limited number of points) through which data must pass from an external network to the secure internal network. This single data entry point makes it easier to defend the network because any attack must pass through the single point. Security appliances can be used to block attacks from entering the network. The combination of a single-entry point plus security appliances that can defend it make up a network's hard edge, which protects important data and resources. This is illustrated in Figure 11-7.

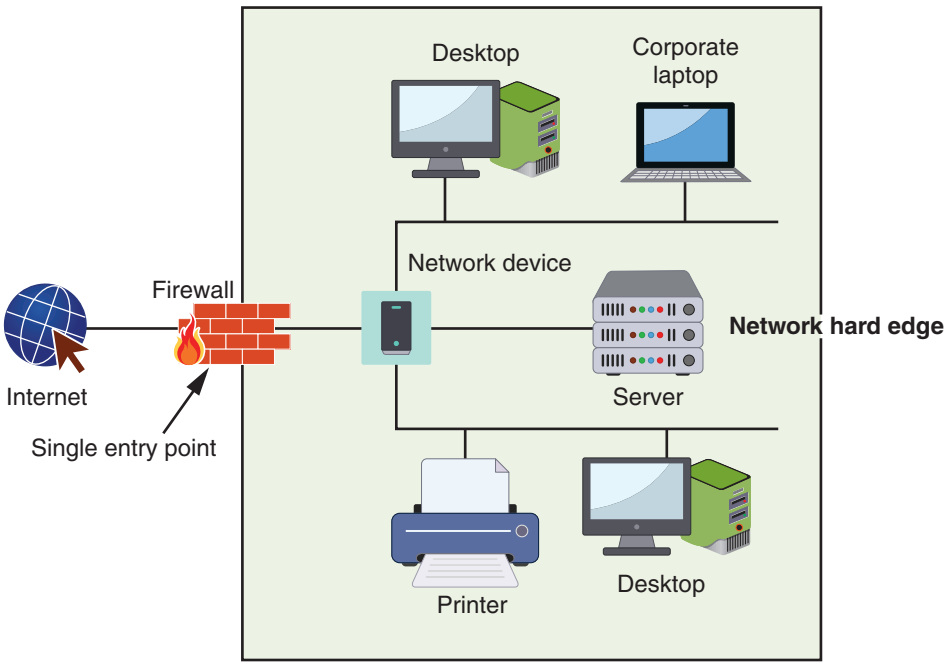


Figure 11-7 Network hard edge

The second hard edge is made up of the walls of the building that houses the enterprise. Because the walls keep out unauthorized personnel, attackers cannot access the network. In other words, the walls serve to physically separate computing resources from attackers.

The introduction of WLANs in enterprises, however, has changed hard edges to "blurred edges." Instead of a network hard edge with a single data entry point, a WLAN can contain multiple entry points. As shown in Figure 11-8, the RF signals from APs create several data entry points into the network through which attackers can inject attacks or steal data. Multiple entry points make it difficult to create a hard network edge. In addition, because RF signals extend beyond the boundaries of the building, the walls cannot be considered as a physical hard edge to keep away attackers. A threat actor in a car well outside of the building's security perimeter can still easily pick up a wireless RF signal to eavesdrop on data transmissions or inject malware behind the firewall. An AP whose security settings have not been set or have been improperly configured can allow attackers access to the network.

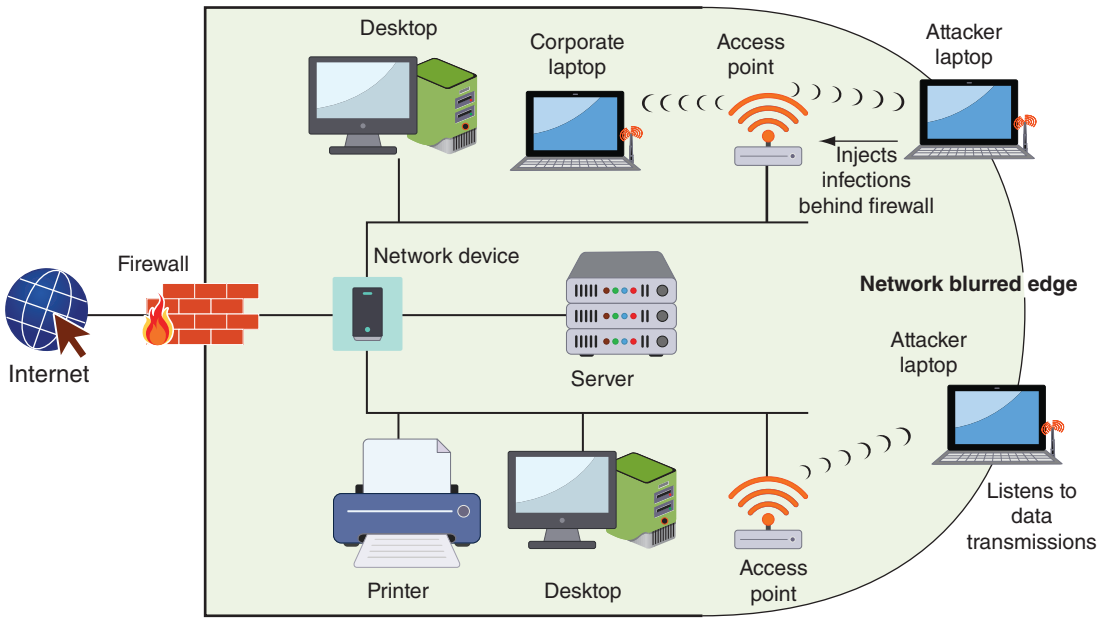


Figure 11-8 Network blurred edge

Several types of wireless attacks can be directed at the enterprise. These include rogue access points (rogue APs), evil twins, intercepting wireless data, and wireless denial of service attacks.

NOTE 14

Rogue APs do not even have to be separate network devices. The wireless Hosted Network function in Microsoft Windows makes it possible to virtualize the physical wireless network interface card (NIC) into multiple virtual wireless NICs (Virtual Wi-Fi) that can be accessed by a software-based wireless AP (SoftAP). This means any computer can easily be turned into a rogue AP. Some smartphone apps also allow these devices to function as APs.

Rogue Access Point Lejla is the manager of a recently opened retail storefront and wants to add wireless access in the employee break room. However, her employer's IT staff turns down her request for a wireless network. Lejla decides to take the matter into her own hands: she purchases an inexpensive wireless router, secretly brings it into the store, and connects it to the wired network, thus providing wireless access to her employees. Unfortunately, Lejla also has provided open access to an attacker sitting in a car in the parking lot who picks up the wireless signal. The attacker can then circumvent the security protections of the company's network.

Lejla has installed a **rogue AP** (*rogue* means someone or something that is deceitful or unreliable). A rogue AP is an unauthorized AP that allows an attacker to bypass many of the network security configurations and opens the network and its users to attacks. For example, although firewalls are typically used to restrict specific attacks from entering a network, an attacker who can access the network through a rogue AP is behind the firewall.

Evil Twin While a rogue AP is set up by an internal user, an **evil twin** is an AP that is set up by an attacker. This AP is designed to mimic an authorized AP, so a user's mobile device such as a laptop or tablet unknowingly connects to the evil twin instead. Attackers can then capture the transmissions from users to the evil twin AP.

Figure 11-9 illustrates rogue AP and evil twin attacks on an enterprise network, which further create a "blurred edge" to a corporate network.

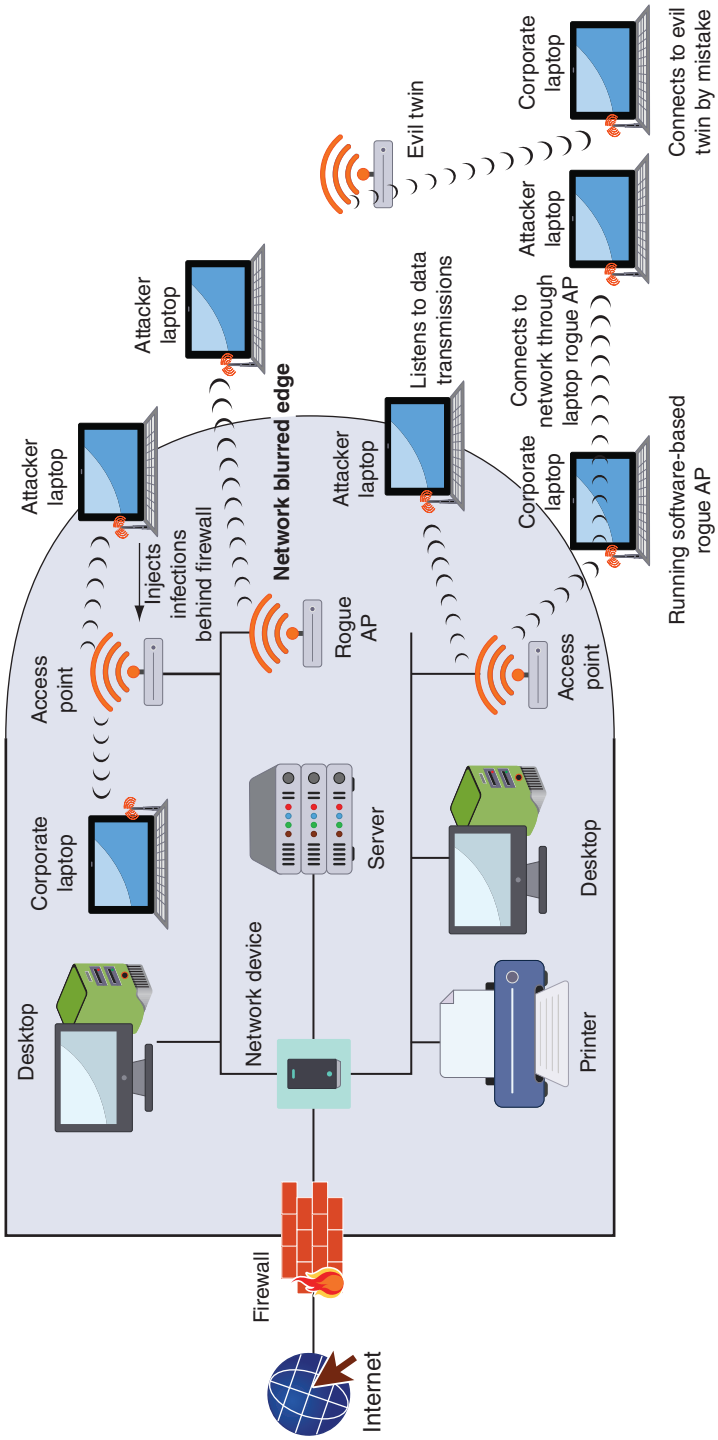


Figure 11-9 Rogue access point and evil twin attacks

Intercepting Wireless Data One of the most common wireless attacks is intercepting and reading transmitted data. An attacker can pick up the RF signal from an open or misconfigured AP and read confidential wireless transmissions. To make matters worse, if attackers manage to connect to the enterprise wired network through a rogue AP, they also could read broadcast and multicast wired network traffic that leaks from the wired network to the wireless network. Using a WLAN to read this data could yield significant information to an attacker regarding the wired enterprise network.

NOTE 15

Several types of devices transmit a radio signal that can cause incidental interference with a WLAN. These devices include microwave ovens, elevator motors, photocopying machines, and certain types of outdoor lighting systems, to name a few. These may cause errors or completely prevent transmission between a wireless device and an AP.

NOTE 16

Jamming attacks generally are rare because sophisticated and expensive equipment is necessary to flood the RF spectrum with enough interference to impact the network. In addition, because a very powerful transmitter must be used at a relatively close range to execute the attack, it is possible to identify the location of the transmitter and therefore identify the source of the attack.

NOTE 17

The amendment IEEE 802.11w was designed to protect against wireless DoS attacks. However, it only protects specific management frames instead of all management frames, requires updates to both the AP and the wireless clients, and might interfere with other security devices. For these reasons, it has not been widely implemented.

Wireless Denial of Service Attacks Because wireless devices operate using RF signals, there is the potential for signal interference. Although the wireless device itself may be the source of interference for other devices, attackers can leverage signals from other devices to disrupt valid wireless transmissions.

Attackers can use intentional RF interference to flood the RF spectrum with enough interference to prevent a device from effectively communicating with the AP. This wireless denial of service (DoS) attack prevents the transmission of data to or from network devices. In one type of wireless DoS attack, an attacker can intentionally flood the RF spectrum with extraneous RF signal "noise" that creates interference and prevents communications from occurring. This is called **jamming**.

Another wireless DoS attack takes advantage of an IEEE 802.11 design weakness. This weakness is the implicit trust of management frames transmitted across the wireless network, which includes information such as the sender's source address. Because IEEE 802.11 requires no verification of the source device's identity (and so all management frames are sent in an unencrypted format), an attacker can easily craft a fictitious frame that pretends to come from a trusted client when it is in fact from a malicious attacker. Different types of frames can be "spoofed" by an attacker to prevent a client from being able to remain connected to the WLAN. A client must be both authenticated and associated with an AP before being accepted into the wireless network and deauthenticated and disassociated when the client leaves the network. An attacker can create false deauthentication or disassociation management frames that appear to come from another client device, causing the client to disconnect from the AP (called a **disassociation attack**). Although the client device can send another authentication request to an AP, an attacker can continue to send spoofed frames to sever any reconnections.

Manipulating duration field values is another wireless DoS attack. The 802.11 standard provides an option using the Request to Send/Clear to Send (RTS/CTS) protocol. A Request to Send (RTS) frame is transmitted by a mobile device to an AP that contains a duration field indicating the length of time needed for both the transmission and the returning acknowledgment frame. The AP, as well as all stations that receive the RTS frame, are alerted that the medium will be reserved for a specific period. Each receiving station stores that information in its net allocation vector (NAV) field, and no station can transmit if the NAV contains a value other than zero. An attacker can send a frame with the duration field set to an arbitrarily high value (the maximum is 32,767), thus preventing other devices from transmitting for lengthy periods of time.

WLAN Consumer Attacks

Attacks against consumers' home WLANs are considered easy because many users fail to properly configure security on their home wireless networks. Consumers face several risks from attacks on their insecure wireless networks. Among other things, attackers can

- *Steal data*. On a computer in the home WLAN, an attacker could access any folder with file sharing enabled. This essentially provides an attacker full access to steal sensitive data from the computer.
- *Read wireless transmissions*. Usernames, passwords, credit card numbers, and other information sent over the WLAN could be captured by an attacker.
- *Inject malware*. Because attackers could access the network behind a firewall, they could inject viruses and other malware onto the computer.

- *Download harmful content*. In several instances, attackers have accessed a home computer through an unprotected WLAN, downloaded child pornography to the computer, and then turned that computer into a file server to distribute the content. When authorities have traced the files to that computer, the unsuspecting owner has been arrested and the equipment confiscated.

TWO RIGHTS & A WRONG

1. Bluetooth LE also supports a many-to-many topology, known as a mesh.
2. Most RFID tags are active and require their own power supply.
3. An AP primarily consists of an antenna and a radio transmitter/receiver to send and receive wireless signals, special bridging software to interface wireless devices to other devices, and a wired network interface that allows it to connect by cable to a standard wired network.

See Appendix B for the answer.

VULNERABILITIES OF WLAN SECURITY

CERTIFICATION

1.4 Given a scenario, analyze potential indicators associated with network attacks.

3.3 Given a scenario, implement secure network designs.

3.4 Given a scenario, install and configure wireless security settings.

The original IEEE 802.11 committee recognized that wireless transmissions could be vulnerable. Because of this, they implemented several wireless security protections in the 802.11 standard while leaving other protections to be applied at the WLAN vendor's discretion. Several of these protections, though well intended, were vulnerable and led to multiple attacks. These vulnerabilities can be divided into those based on Wired Equivalent Privacy (WEP), Wi-Fi Protected Setup (WPS), MAC address filtering, and Wi-Fi Protected Access (WPA).

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is an IEEE 802.11 security protocol designed to ensure that only authorized parties can view transmitted wireless information. WEP accomplishes this confidentiality by encrypting the transmissions. WEP relies on a shared secret key that is known only by the wireless client and the AP. The same secret key must be entered on the AP and on all devices before any transmissions can occur because the key is used to encrypt any packets to be transmitted as well as decrypt packets that are received. IEEE 802.11 WEP shared secret keys must be a minimum of 64 bits in length. Most vendors add an option to use a longer 128-bit shared secret key for higher security.

The shared secret key is combined with an **initialization vector (IV)**, which is a 24-bit value that changes each time a packet is encrypted. The IV and the key are combined and used as a seed for generating a random number necessary in the encryption process. The IV and encrypted ciphertext are both transmitted to the receiving device. Upon arrival, the receiving device first separates the IV from the encrypted text and then combines the IV with its own shared secret key to decrypt the data.

WEP has several security vulnerabilities. First, to encrypt packets, WEP can use only a 64-bit or 128-bit number, which is made up of a 24-bit IV and either a 40-bit or 104-bit default key. Even if a longer 128-bit number is used, the length of the IV remains at 24 bits. The relatively short length of the IV limits its strength, since shorter keys are easier to break than longer keys.

Second, WEP implementation violates the cardinal rule of cryptography: anything that creates a detectable pattern must be avoided at all costs. This is because patterns provide an attacker with valuable information to break the encryption. The implementation of WEP creates a detectable pattern for attackers. Because IVs are 24-bit numbers, there are only 16,777,216 possible values. An AP transmitting at 11 Mbps can send and receive 700 packets each second. If a different IV were used for each packet, then the IVs would start repeating in less than seven hours. (A "busy" AP can produce duplicates in fewer than five hours.) An attacker who captures packets for this length of time can see the duplication and use it to crack the code.

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) is an optional means of configuring security on WLANs. It is designed to help users who have little or no knowledge of security to implement security quickly and easily on their WLANs.

There are two common WPS methods. The PIN method uses a personal identification number (PIN) printed on a sticker of the wireless router or displayed through a software setup wizard. The user types the PIN into the wireless device (such as a wireless tablet, laptop computer, or smartphone), and the security configuration automatically occurs. This is the mandatory model, and all devices certified for WPS must support it. The second method is the push-button method: the user pushes a button (usually an actual button on the wireless router and a virtual one displayed through a software setup wizard on the wireless device) and the security configuration takes place. Support for this model is mandatory for wireless routers and optional for connecting devices.

However, WPS using the PIN method has significant design and implementation flaws:

- There is no lockout limit for entering PINs, so an attacker can make an unlimited number of PIN attempts.
- The last PIN character is only a checksum.
- The wireless router reports the validity of the first and second halves of the PIN separately, so essentially an attacker must break only two short PIN values (a four-character PIN and a three-character PIN).

Due to the PIN being divided into two shorter values, only 11,000 different PINs must be attempted before determining the correct value. If the attacker's computer can generate 1.3 PIN attempts per second (or 46 attempts per minute), the attacker can crack the PIN in less than four hours and become connected to the WLAN. This effectively defeats security restrictions that allow only authorized users to connect to the wireless network.

CAUTION

Some wireless vendors are implementing additional security measures for WPS, such as limiting the number and frequency of PIN guesses. However, unless it can be verified that WPS supports these higher levels of security, it is recommended that WPS be disabled through the wireless router's configuration settings.

MAC Address Filtering

One means of protecting a WLAN is to control which devices are permitted to join the network. Wireless access control is intended to limit a user's admission to the AP: only those who are authorized can connect to the AP and thus become part of the wireless LAN.

The most common type of wireless access control is **Media Access Control (MAC) address filtering**. The MAC address is a hardware address that uniquely identifies each node of a network. It is a unique 48-bit number "burned" into the network interface card adapter when it is manufactured. The IEEE 802.11 standard permits controlling which devices can connect to the WLAN but does not specify how the control is to be implemented. Since a wireless device can be identified by its MAC address, however, virtually all wireless AP vendors implement MAC address filtering as the means of access control. A wireless client device's MAC address is entered into software running on the AP, which then is used to permit or deny a device from connecting to the network. As shown in Figure 11-10, restrictions can be implemented by either whitelisting (a specific device can be allowed access into the network) or blacklisting (a device can be blocked).

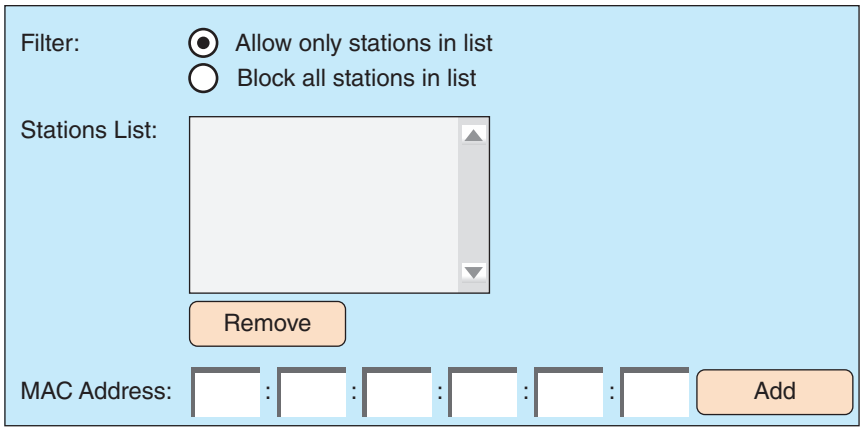


Figure 11-10 MAC address filtering

NOTE 18

MAC address filtering is usually implemented by permitting instead of preventing, because it is not possible to know the MAC addresses of all the devices that are to be excluded.

Filtering by MAC address has several vulnerabilities. First, MAC addresses are initially exchanged between wireless devices and the AP in an unencrypted format. Attackers monitoring the airwaves could easily see the MAC address of an approved device and then substitute it on their own device. Another weakness of MAC address filtering is that managing several MAC addresses can pose significant challenges. The sheer number of users often makes it difficult to manage all the MAC addresses. As new users are added to the network and old users leave, keeping track of MAC address filtering demands almost constant attention. For this reason, MAC address filtering is not always practical in a large and dynamic wireless network.

CAUTION

It is not uncommon to read of controlling access to the WLAN by hiding the *Service Set Identifier (SSID)* of the wireless network, which is the user-supplied network name of a wireless network and generally can be any alphanumeric string up to 32 characters. Although normally the SSID is broadcast so that any device can see it, the broadcast can be restricted so that only those users that know the "secret" SSID in advance would be allowed to access the network. However, the SSID can be easily discovered even when it is not contained in beacon frames because it is transmitted in other management frames sent by the AP. Hiding the SSID is not recommended as a security protection.

Wi-Fi Protected Access (WPA)

The Wi-Fi Alliance introduced *Wi-Fi Protected Access (WPA)* to fit into the existing WEP engine without requiring extensive hardware upgrades or replacements. There were two modes of WPA. *WPA Personal* was designed for individuals or small office/home office (SOHO) settings, which typically have up to 10 employees. A more robust *WPA Enterprise* was intended for larger enterprises, schools, and government agencies. WPA addresses both encryption and authentication.

A wireless network in which no authentication is required, such as at a local coffee shop, is using an **open method**. However, most WLANs need to restrict who can access the network through authentication. Authentication for WPA Personal is accomplished by using a **preshared key (PSK).** In cryptography, a PSK is a value that has been previously shared using a secure communication channel between two parties. In a WLAN, a PSK is slightly different. It is a secret value that is manually entered on both the AP and each wireless device, making it essentially identical to the "shared secret" used in WEP. Because this secret key is not widely known, it can be assumed that only approved devices have the key value. Devices that have the secret key are then automatically authenticated by the AP.

CAUTION Although an improvement over WEP, WPA nevertheless has weaknesses and is not considered as a secure option.

TWO RIGHTS & A WRONG

1. An initialization vector (IV) is a 24-bit value that changes each time a packet is encrypted.
2. There are three common WPS methods.
3. Filtering by MAC address has several vulnerabilities, most notably that MAC addresses are initially exchanged between wireless devices and the AP in an unencrypted format.

See Appendix B for the answer.

WIRELESS SECURITY SOLUTIONS

CERTIFICATION

3.4 Given a scenario, install and configure wireless security settings.

Despite the vulnerabilities in some early wireless security protections, it is generally recognized that modern wireless security solutions are much more secure. Wi-Fi Protected Access 2 (WPA2) and Wi-Fi Protected Access 3 (WPA3) form the foundation of today's wireless security solutions.

Wi-Fi Protected Access 2 (WPA2)

Due to the shortcomings of WPA, a more robust wireless security standard was introduced by the IEEE known as *IEEE 802.11i*. Shortly thereafter, the Wi-Fi Alliance introduced **Wi-Fi Protected Access 2 (WPA2)**, which is based on the final IEEE 802.11i standard and is almost identical to it. As with WPA, there are two modes of WPA2, *WPA2 Personal* for individuals or small offices and *WPA2 Enterprise* for larger enterprises, schools, and government agencies. WPA2 addresses the two major security areas of WLANs—namely, encryption and authentication.

NOTE 19

CCM itself does not require that a specific block cipher be used, but the most secure cipher AES is mandated by the WPA2 standard. For this reason, CCMP for WLANs is sometimes designated as *AES-CCMP*.

AES-CCMP Encryption

The encryption protocol used for WPA2 is the **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)** and specifies the use of CCM (a general-purpose cipher mode algorithm providing data privacy) with AES. The **Cipher Block Chaining Message Authentication Code (CBC-MAC)** component of CCMP provides data integrity and authentication.

IEEE 802.1x Authentication

Authentication for the WPA2 Enterprise model (called the **enterprise method**) uses the **IEEE 802.1x** standard. This standard, originally developed for wired networks, provides a greater degree of security by implementing port-based authentication. IEEE 802.1x blocks all traffic on a port-by-port basis until the client is authenticated using credentials stored on an authentication server. This prevents an unauthenticated device from receiving any network traffic until its identity can be verified. It also strictly limits access to the device that provides the authentication to prevent attackers from reaching it. Figure 11-11 illustrates the steps in an 802.1x authentication procedure.

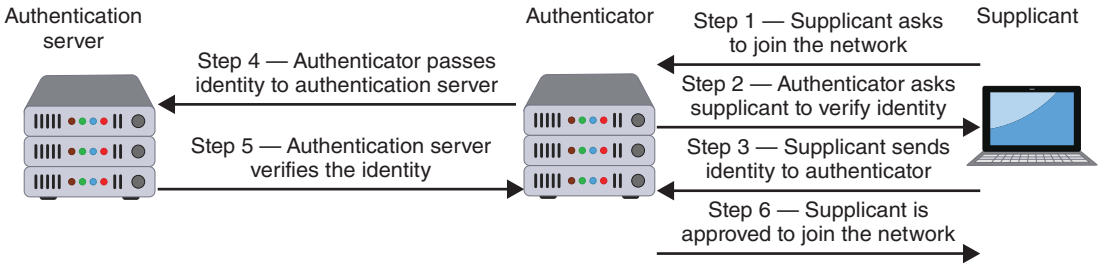


Figure 11-11 IEEE 802.1x process

1. The device (called a *supplicant*) requests permission from the *authenticator* to join the network.
2. The authenticator asks the supplicant to verify its identity.
3. The supplicant sends identity information to the authenticator.
4. The authenticator passes the identity credentials to an *authentication server*, whose only job is to verify the authentication of devices. The identity information is sent in an encrypted form.
5. The authentication server verifies or rejects the supplicant's identity and returns the information to the authenticator.
6. If approved, the supplicant can join the network and transmit data.

The communication between the supplicant, authenticator, and authentication server in an IEEE 802.1x configuration must be secure. A framework for transporting the authentication protocols is known as the **Extensible Authentication Protocol (EAP)**. Despite its name, EAP is a *framework* for transporting authentication protocols instead of the authentication protocol itself. EAP essentially defines the format of the messages and uses four types of packets: *request*, *response*, *success*, and *failure*. Request packets are issued by the authenticator and ask for a response packet from the supplicant. Any number of request-response exchanges may be used to complete the authentication. If the authentication is successful, a success packet is sent to the supplicant; if not, a failure packet is sent.

NOTE 20

Although IEEE 802.1x is commonly used on wireless networks, it can be used for wired networks as well. For example, in a public conference room, an RJ-45 network connection may be accessible to both trusted employees and untrusted public users. IEEE 802.1x permits the trusted employees to access both the secure internal corporate network and the Internet while restricting public users to Internet access only from the same network connection.

NOTE 21

An EAP packet contains a field that indicates the function of the packet (such as response or request) and an identifier field used to match requests and responses. Response and request packets also have a field that indicates the type of data being transported (such as an authentication protocol) along with the data itself.

A common EAP protocol is **Protected EAP (PEAP)**. PEAP is designed to simplify the deployment of 802.1x by using Microsoft Windows logins and passwords. PEAP is considered a more flexible EAP scheme because it creates an encrypted channel between the client and the authentication server, and the channel then protects the subsequent user authentication exchange. To create the channel, the PEAP client first authenticates the PEAP authentication server using enhanced authentication.

Several EAP protocols are supported in WPA2 Enterprise; the most common are listed in Table 11-5.

Table 11-5 Common EAP Protocols Supported by WPA2 Enterprise

EAP name	Description
EAP-TLS	This protocol uses digital certificates for authentication.
EAP-TTLS	This protocol securely tunnels client password authentication within Transport Layer Security (TLS) records.
EAP-FAST	This protocol securely tunnels any credential form for authentication (such as a password or a token) using TLS.

Wi-Fi Protected Access 3 (WPA3)

The next generation of Wi-Fi Protected Access (WPA) is known as **WPA3**. The goal of WPA3 is to deliver a suite of features to simplify security configuration for users while enhancing network security protections.

CAUTION

WPA3, as well as WPA2, is not officially a standard nor is it a protocol. WPA3 is a hardware certification program that specifies what existing standards a product must support in order to be labeled as "Wi-Fi CERTIFIED WPA3." This means that the device will be interoperable with other similar devices that have also obtained the WPA3 certified label.

The following four security improvements are part of WPA3:

- WPA3 includes **Simultaneous Authentication of Equals (SAE)**. SAE is designed to increase security at the time of the handshake when keys are being exchanged. The result is that WPA3 can give stronger security even if short or weak passwords are used.
- WPA3 supports a longer 192-bit encryption.
- When using open or public Wi-Fi networks in airports and coffee shops, WPA3 applies individualized data encryption so that every connection between a client and an AP/wireless router is encrypted with a unique key. Known as *Opportunistic Wireless Encryption (OWE)*, it can mitigate against man-in-the-middle (MITM) attacks.
- WPA3 has improved interaction capabilities with Internet of Things (IoT) devices. The older WPA2 was primarily designed to work with traditional mobile devices that had screens (such as smartphones and laptops) in which the user could enter a password and configure the wireless settings. However, most IoT devices have no screens. WPA3 contains new ways to configure security for these types of devices.

TWO RIGHTS & A WRONG

1. There are two modes of WPA2, WPA2 Professional and WPA2 Enterprise.
2. The encryption protocol used for WPA2 is the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and specifies the use of CCM (a general-purpose cipher mode algorithm providing data privacy) with AES.
3. EAP-TLS uses digital certificates for authentication.

See Appendix B for the answer.

ADDITIONAL WIRELESS SECURITY PROTECTIONS

CERTIFICATION

2.6 Explain the security implications of embedded and specialized systems.

3.4 Given a scenario, install and configure wireless security settings.

Other security steps can be taken to protect a wireless network. These include installation and configuration, specialized systems communications, and rogue AP system detection.

Installation

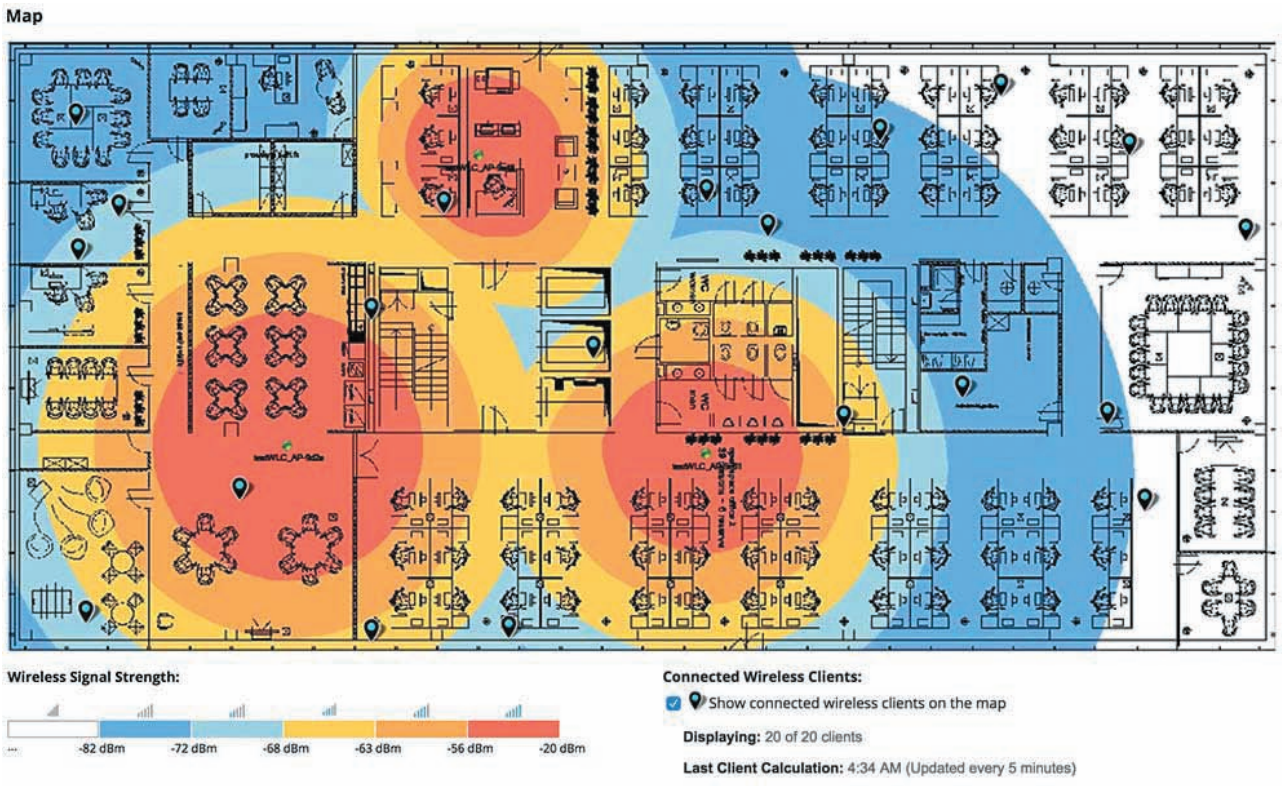
When installing a wireless LAN in a home or apartment, most users do not give much time to determining the optimum location for the wireless router so that its RF signal coverage is uniform throughout the house but extends outside it as little as possible. Instead, the devices are typically placed wherever it is convenient, such as next to the Internet connection, near a desktop computer, or even tucked away on a bookcase. If the wireless signal does not to reach into the far corners of the house or outside onto an outdoors deck, then those areas are simply recognized as being "dead space" and are avoided when using the network.

However, when installing a WLAN for an organization, areas of dead space cannot be so easily tolerated. Whereas at home a user may simply move to another room for better reception, that may not always be possible in a building with multiple offices, locked doors, and private cubicles. This means important considerations must be taken into account when installing a new WLAN for an organization: all areas of a building should have adequate wireless coverage; all employees must have a reasonable amount of bandwidth; and, for security reasons, a minimum amount of wireless signal should "bleed" outside the walls of the building.

Assuring that a WLAN can provide its intended functionality and meet its required design goals can best be achieved through a **site survey**. A site survey is an in-depth examination and analysis of a WLAN site. A site survey mainly addresses placing the AP in the optimum location, known as **wireless access point placement**.

Several tools can be used in a site survey for installation:

- *Heat maps*. A Wi-Fi **heat map** is a visual representation of the wireless signal coverage and strength. Wi-Fi heat maps are generally overlaid on top of a building or facility floor plan to help clearly indicate where problem areas are located in relation to the collected site survey data. Figure 11-12 illustrates a heat map.



Source: solarwinds.com

Figure 11-12 Wi-Fi heat map

- *Wi-Fi analyzers*. A **Wi-Fi analyzer** tool helps to visualize the essential details of the wireless network. An analyzer can provide information such as signal strength, network health, channel bandwidth, channel coverage, data rate, and interference (noise).

- *Channel overlays*. It is not uncommon for multiple APs to attempt to use the same frequency (*channel*), causing interference. Software that illustrates these **channel overlays** can help visualize conflicting overlaps. Channel overlay software is seen in Figure 11-13.

Source: Wifi Analyzer

Figure 11-13 Channel overlay software

NOTE 22

Although the placement of a wireless router in a home or apartment may not have as many options as an office, there are some principles to keep in mind that can improve Wi-Fi service. If possible, place the wireless router in a central location so the wireless signal does not have to penetrate more than two rooms and two interior walls. Also, the higher the wireless router can be placed above the heads of people, the better: one human body can block the signal about as much as one interior wall.

Configuration

Selecting the proper configuration options for the AP can also enhance security. Some of these settings are designed to limit the spread of the wireless RF signal so that a minimum amount of signal extends past the physical boundaries of the enterprise to be accessible to outsiders. AP configuration and device options include setting the signal strength and choosing the correct RF spectrum options. One device option is to select the best type of antenna and to correctly locate it.

Signal Strength Settings

A security feature on some APs is the ability to adjust the level of power at which the WLAN transmits. On devices with that feature, the power can be adjusted so that less of the signal leaves the premises and reaches outsiders. For IEEE WLANs, the maximum transmit power is 200 milliwatts (mW). APs that can adjust the power level usually permit the level to be adjusted in predefined increments—such as 1, 5, 20, 30, 40, 100, or 200 mW.

Spectrum Selection

Some APs provide the ability to adjust frequency spectrum settings. These include the following:

- *Frequency band*. An increasing number of APs support dual bands of spectrum. If one band is not being used, it should be disabled. If both bands are used, it is recommended that both have the same configuration settings.

- *Channel selection.* Some APs have an *Auto* mode in which the AP selects the optimum channel within the frequency band. On those devices in which this mode is not supported, it is important to choose a channel that is different from that of other nearby APs or sources of interference.
- *Channel width*. Channel width controls how much of the spectrum is available to transfer data. However, larger channels are more subject to interference and more likely to interfere with other devices.

Antenna Placement and Type

APs use antennas that radiate a signal in all directions. Because these devices are generally positioned to provide the broadest area of coverage, APs should be located near the middle of the coverage area. Generally, the AP can be secured to the ceiling or high on a wall. It is recommended that APs be mounted as high as possible for two reasons: to minimize obstructions for the RF signal and to prevent thieves from stealing the device. For security purposes, the AP and its antenna should be positioned so that, when possible, a minimal amount of signal reaches beyond the security perimeter of the building or campus. Another option is to use a type of antenna that focuses its signal in a concentrated direction toward authorized users instead of broadcasting it over a wide area.

Specialized Systems Communications

Several wireless technologies relate to communications for specialized and embedded systems. These include the following:

- *Zigbee*. **Zigbee** is a low-power, short-range, and low-data rate specification. It is based on the IEEE 802.15.4 standard but includes network configuration, security, and other higher-level features that are not covered by IEEE standard. Zigbee's data rate is 250 kbps and is designed for occasional data or signal transmission from a sensor or IoT device.
- *5G*. Unlike Wi-Fi transmitting over a localized geographical area, **5G** is the fifth-generation cellular wireless standard. Compared to 4G, 5G supports faster speeds, is more responsive, and can connect to more devices simultaneously.
- *Narrowband IoT*. **Narrowband Internet of Things (NB-IoT)** is a low-power wide area network (LPWAN) radio technology standard. NB-IoT is a wide-range cellular service that focuses on indoor coverage, low cost, long battery life, and high connection density.
- *Cellular IoT baseband*. One cellular-based network for IoT devices that is optimized for these transmissions uses a **baseband** radio. (Baseband refers to the original frequency range of a transmission signal before it is converted to a different frequency range.) *Cellular IoT baseband* can transmit using standard 4G transmissions or NB-IoT.
- *Subscriber identity module (SIM) card*. Some IoT devices use a **SIM card** (subscriber identity module card) for data transmissions. A SIM card is an integrated circuit that securely stores information used to identify and authenticate the IoT device on a cellular network like 5G.

NOTE 23

The Zigbee name comes from the peculiar behavior of bees. After zigging and zagging through fields when collecting nectar, bees return to the hive and perform a waggle dance to communicate the distance, direction, and type of food to other bees in the hive. Once they receive this information, the other bees fly off directly to the source of food.

Rogue AP System Detection

As the cost of consumer wireless routers has fallen, the problem of rogue APs has risen. Identifying these devices in an enterprise is known as *rogue AP system detection*. Several methods can be used to detect a rogue AP by continuously monitoring the RF airspace. This requires a special sensor called a *wireless probe*, a device that can monitor the airwaves for traffic. There are four types of wireless probes:

- *Wireless device probe*. A standard wireless device, such as a portable laptop computer, can be configured to act as a wireless probe. At regular intervals during the normal course of operation, the device can scan and record wireless signals within its range and report this information to a centralized database. The scanning is performed when the device is idle and not receiving any transmissions. Using several mobile devices as wireless device probes can provide a high degree of accuracy in identifying rogue access points.

- *Desktop probe*. Instead of using a mobile wireless device as a probe, a desktop probe uses a standard desktop PC. A universal serial bus (USB) wireless adapter is plugged into the desktop computer to monitor the RF in the area for transmissions.
- *Access point probe*. Some AP vendors have included in their APs the functionality of detecting neighboring APs, friendly as well as rogue. However, this approach is not widely used. The range for a single AP to recognize other APs is limited because APs are typically located so that their signals overlap only to provide roaming to wireless users.
- *Dedicated probe*. A dedicated probe is designed to exclusively monitor the RF for transmissions. Unlike access point probes that serve as both an AP and a probe, dedicated probes only monitor the airwaves. Dedicated probes look much like standard access points.

Once a suspicious wireless signal is detected by a wireless probe, the information is sent to a centralized database where WLAN management system software compares it to a list of approved APs. Any device not on the list is considered a rogue AP. The WLAN management system can instruct the switch to disable the port to which the rogue AP is connected, thus severing its connection to the wired network.

SUMMARY

- Bluetooth is a wireless technology that uses short-range RF transmissions. It enables users to connect wirelessly to a wide range of computing and telecommunications devices by providing for rapid "on-the-fly" connections between Bluetooth-enabled devices. The primary type of Bluetooth network topology is a piconet. Two of the common attacks on wireless Bluetooth technology are bluejacking, which is sending unsolicited messages, and bluesnarfing, or accessing unauthorized information from a wireless device through a Bluetooth connection.
- Near field communication (NFC) is a set of standards that can be used to establish communication between devices in close proximity. Once the devices are either tapped together or brought very close to each other, a two-way communication is established. NFC devices are increasingly used in contactless payment systems so that consumers can pay for a purchase by simply tapping a store's payment terminal with their smartphone. There are risks with using NFC contactless payment systems because of the nature of this technology.
- A wireless technology similar to NFC is radio frequency identification (RFID). RFID is commonly used to transmit information between paper-based tags that can be detected by a proximity reader. Because RFID tags do not require a power supply, they can be very small and thinner than a sheet of paper. RFID tags are susceptible to some types of attacks.
- A wireless local area network (WLAN), commonly called Wi-Fi, is designed to replace or supplement a wired LAN. The IEEE has developed standards for WLANs. An enterprise WLAN requires a wireless client adapter and an AP for communications, whereas a home network uses a wireless router instead of an AP. There are different types of enterprise APs. A thin AP is a lightweight AP that does not contain all the management and configuration functions found in fat APs. Much of the configuration is centralized in the wireless switch. Instead of installing standalone APs like fat or thin APs, controller APs can be managed through a dedicated wireless LAN controller (WLC). The WLC is a single device that can be configured and then used to automatically distribute the settings to all controller APs. A captive portal AP uses a standard web browser to present information and give the wireless user the opportunity to agree to a policy or enter valid login credentials, providing a higher degree of security.
- In a traditional wired network, the security of the network itself along with the walls and doors of the secured building protect the data and resources. Because an RF signal can easily extend past the protective perimeter of a building and because an AP can provide unauthorized entry points into the network, WLANs are frequently the target of attackers.

- A rogue AP is an unauthorized AP that allows an attacker to bypass network security and opens the network and its users to attacks. An evil twin is an AP that is set up by an attacker to mimic an authorized AP and capture the transmissions from users. One of the most common wireless attacks is intercepting and reading transmitted data. In addition, if attackers manage to connect to the enterprise wired network through a rogue AP, they could also read broadcast and multicast wired network traffic. Attackers likewise can use intentional RF interference to flood the RF spectrum with enough radio interference or manipulate Wi-Fi standards to prevent a device from effectively communicating with the AP, performing a wireless DoS attack that prevents the transmission of data to or from network devices. Consumer wireless networks that are not protected are subject to attackers stealing data, reading transmissions, or injecting malware behind the firewall.
- The original IEEE 802.11 committee recognized that wireless transmissions could be vulnerable and implemented several wireless security protections in the 802.11 standard while leaving other protections to be applied at the WLAN vendor's discretion. Despite their intended design, several of these protections were vulnerable to attacks. Wired Equivalent Privacy (WEP) was designed to ensure that only authorized parties can view transmitted wireless information by encrypting transmissions. WEP relies on a secret key shared between the wireless client device and the AP that is combined with an initialization vector (IV). However, WEP has several security vulnerabilities. Wi-Fi Protected Setup (WPS) is an optional means of configuring security on WLANs and is designed to help users who have little or no knowledge of security to implement security quickly and easily. However, there are significant design and implementation flaws in WPS.
- One method of controlling access to the WLAN so that only approved users can be accepted is to limit a device's access to the AP. Virtually all wireless AP vendors offer Media Access Control (MAC) address filtering. Filtering by MAC address, however, has several vulnerabilities. One weakness is that MAC addresses are initially exchanged between wireless devices and the AP in an unencrypted format. Wi-Fi Protected Access (WPA) was designed to fit into the existing WEP engine without requiring extensive hardware upgrades or replacements. WPA replaces WEP with the Temporal Key Integrity Protocol (TKIP), which uses a longer key and dynamically generates a new key for each packet that is created. WPA authentication for WPA Personal is accomplished by using preshared key (PSK) technology. A key must be created and entered in both the access point and all wireless devices ("shared") prior to ("pre") the devices communicating with the AP. Security vulnerabilities can be found in WPA.
- Wi-Fi Protected Access 2 (WPA2) is the second generation of WPA security. Encryption under WPA2 is accomplished by using AES-CCMP. The Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity and authentication. WPA2 authentication is accomplished by the IEEE 802.1x standard. Because the communication between the supplicant, authenticator, and authentication server in an IEEE 802.1x configuration must be secure, it uses a framework for transporting the authentication protocols known as the Extensible Authentication Protocol (EAP). EAP is a framework for transporting authentication protocols by defining the format of the messages. The next generation of Wi-Fi Protected Access (WPA) is known as WPA3. The goal of WPA3 is to deliver a suite of features to simplify security configuration for users while enhancing network security protections.
- Other steps can be taken to protect a wireless network. Important considerations must be taken into account when installing a new WLAN for an organization: all areas of a building should have adequate wireless coverage; all employees must have a reasonable amount of bandwidth; and, for security reasons, a minimum amount of wireless signal should "bleed" outside the walls of the building. Assuring that a WLAN can provide its intended functionality and meet its required design goals can best be achieved through a site survey. A site survey is an in-depth examination and analysis of a WLAN site. A site survey mainly addresses placing the AP in the optimum location, known as wireless access point placement.
- Selecting the proper configuration options for the AP can also enhance security. Some of these settings are designed to limit the spread of the wireless RF signal so that a minimum amount of signal extends past the physical boundaries of the enterprise to be accessible to outsiders. AP configuration and device options include setting the signal strength and choosing the correct RF spectrum options. One device option is to select the best type of antenna and to correctly locate it.

- Several wireless technologies relate to communications for specialized and embedded systems. Zigbee is a low-power, short-range, and low-data rate specification. It is best designed for occasional data or signal transmission from a sensor or IoT device. Unlike Wi-Fi transmitting over a localized geographical area, 5G is the fifth-generation cellular wireless standard. Compared to 4G, 5G supports faster speeds, is more responsive, and can connect to more devices simultaneously. Narrowband Internet of Things (NB-IoT) is a low-power wide area network (LPWAN) radio technology standard. NB-IoT is a wide range cellular service that focuses on indoor coverage, low cost, long battery life, and high connection density. One cellular-based network for IoT devices that is optimized for these transmissions uses a baseband radio. Cellular IoT baseband can transmit using standard 4G transmissions or NB-IoT. Some IoT devices use a SIM card (subscriber identity module card) for data transmissions. A SIM card is an integrated circuit that securely stores information used to identify and authenticate the IoT device on a cellular network like 5G.
- The problem of rogue APs is of increasing concern to organizations. Several methods can be used to detect a rogue AP by continuously monitoring the RF airspace. This requires a special sensor called a wireless probe, a device that can monitor the airwaves for traffic.

Key Terms

5G
ad hoc mode
baseband
bluejacking
bluesnarfing
Bluetooth
captive portal AP
channel overlays
Cipher Block Chaining Message Authentication Code (CBC-MAC)
controller AP
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
disassociation attack
EAP-FAST
EAP-TLS
EAP-TTLS
enterprise method
evil twin
Extensible Authentication Protocol (EAP)
heat map
IEEE 802.1x
initialization vector (IV)
jamming
Media Access Control (MAC) address filtering
Narrowband Internet of Things (NB-IoT)
near field communication (NFC)
open method
payment method
point-to-multipoint
point-to-point
preshared key (PSK)
Protected EAP (PEAP)
radio frequency identification (RFID)
rogue AP
Simultaneous Authentication of Equals (SAE)
site survey
subscriber identity module (SIM) card
Wi-Fi
Wi-Fi analyzer
Wi-Fi Direct
Wi-Fi Protected Access 2 (WPA2)
Wi-Fi Protected Setup (WPS)
wireless access point placement
WPA3
Zigbee

Review Questions

1. Aaliyah has been asked to do research in a new payment system for the retail stores that her company owns. Which technology is predominately used for contactless payment systems that she will investigate?
   a. Bluetooth
   b. Near field communication (NFC)
   c. Wi-Fi
   d. Radio frequency ID (RFID)
2. Nyla is investigating a security incident in which the smartphone of the CEO was compromised and confidential data was stolen. She suspects that it was an attack that used Bluetooth. Which attack would this be?
   a. Blueswiping
   b. Bluesnarfing
   c. Bluejacking
   d. Bluestealing
3. What is a difference between NFC and RFID?
   a. NFC is based on wireless technology while RFID is not.
   b. RFID is faster than NFC.
   c. RFID is designed for paper-based tags while NFC is not.
   d. NFC devices cannot pair as quickly as RFID devices.

4. Which technical specification of the Wi-Fi Alliance is the same as ad hoc mode in a Wi-Fi network?
   a. Ad hoc II
   b. Dynamic ad hoc
   c. Alliance IBSS
   d. Wi-Fi Direct

5. Fatima has just learned that employees have tried to install their own wireless router in the employee lounge. Why is installing this rogue AP a security vulnerability?
   a. It uses the weaker IEEE 80211i protocol.
   b. It allows an attacker to bypass network security configurations.
   c. It conflicts with other network firewalls and can cause them to become disabled.
   d. It requires the use of vulnerable wireless probes on all mobile devices.

6. Which of these is NOT a risk when a home wireless router is not securely configured?
   a. An attacker can steal data from any folder with file sharing enabled.
   b. Wireless endpoints must be manually approved to connect to the WLAN.
   c. Usernames, passwords, credit card numbers, and other information sent over the WLAN could be captured by an attacker.
   d. Malware can be injected into a computer connected to the WLAN.

7. Which of these Wi-Fi Protected Setup (WPS) methods is vulnerable?
   a. Push-button method
   b. Piconet method
   c. PIN method
   d. Click-to-connect method

8. Flavio visits a local coffee shop on his way to school and accesses its free Wi-Fi. When he first connects, a screen appears that requires him to agree to an acceptable use policy (AUP) before continuing. What type of AP has he encountered?
   a. Authenticated portal
   b. Captive portal
   c. Control portal
   d. Rogue portal

9. Which of the following is NOT a means by which a threat actor can perform a wireless denial of service attack?
   a. Jamming
   b. Disassociation
   c. IEEE 802.11iw separate
   d. Manipulate duration field values

10. Zariah is writing an email to an employee about a wireless attack that is designed to capture the wireless transmissions from legitimate users. Which type of attack is Zariah describing?
    a. Rogue access point
    b. Bluetooth grabber
    c. WEP-II
    d. Evil twin

11. Which of these is a vulnerability of MAC address filtering in a WLAN?
    a. Not all operating systems support MACs.
    b. APs use IP addresses instead of MACs.
    c. The user must enter the MAC.
    d. MAC addresses are initially exchanged unencrypted.

12. Which of these is a 24-bit value that changes each time a packet is encrypted and then is combined with a shared secret key?
    a. RC
    b. IV
    c. SL
    d. SSD

13. Which of these does not require authentication?
    a. Open method
    b. PSK
    c. Enterprise method
    d. Initialization method

14. Which of these is the encryption protocol for WPA2?
    a. CMAC-RSTS
    b. CPB
    c. CBD-MAC
    d. CCMP

15. Adabella was asked by her supervisor to adjust the frequency spectrum settings on a new AP. She brought up the configuration page and looked through the different options. Which of the following frequency spectrum settings would she NOT be able to adjust?
    a. Frequency band
    b. Channel selection
    c. RFID spectrum
    d. Channel width

16. Imani has been asked to purchase wireless LAN controllers (WLCs) for the office. What type of APs must she also purchase that can be managed by a WLC?
    a. Standalone AP
    b. Controller AP
    c. Fat AP
    d. Any type of AP can be managed by a WLC.

17. Which WPA3 security feature is designed to increase security at the time of the handshake?
    a. WEP
    b. MIT
    c. OWE
    d. SAE

18. Maryam is explaining the Extensible Authentication Protocol (EAP). What would be the best explanation of EAP?
    a. It is the transport protocol used in TCP/IP for authentication.
    b. It is a framework for transporting authentication protocols.
    c. It is a subset of WPA2.
    d. It is a technology used by IEEE 802.11 for encryption.

19. Minh has been asked to recommend an EAP for a system that uses both passwords and tokens with TLS. Which should she recommend?
    a. EAP-FAST
    b. EAP-TLS
    c. EAP-TTLS
    d. EAP-SSL

20. Which of these is NOT a type of wireless AP probe?
    a. Wireless device probe
    b. WNIC probe
    c. Dedicated probe
    d. AP probe

Hands-On Projects

CAUTION If you are concerned about installing any of the software in these projects on your regular computer, you can instead use the Windows Sandbox or install the software in the Windows virtual machine created in the Module 1 Hands-On Projects. Software installed within the virtual machine will not impact the host computer.

Project 11-1: Using a Wireless Monitor Tool

Time Required: 25 minutes
Objective: Given a scenario, install and configure wireless security settings.
Description: Most Wi-Fi users are surprised to see how far their wireless signal will reach, and if the network is unprotected, a long reach makes it easy for an attacker hiding several hundred feet away to break into the network. Several tools can show the different wireless signals that can be detected from Wi-Fi networks. In this project, you download and install the NirSoft WifiInfoView tool. You will need a computer with a wireless adapter, such as a laptop, to complete this project.

1. Use your web browser to go to **www.nirsoft.net/utils/wifi_information_view.html**. (If you are no longer able to access the site through the web address, use a search engine to search for "NirSoft WifiInfoView.")
2. Scroll down and click **Download WifiInfoView**.
3. Download the tool and when finished, extract the files and then launch the program.
4. Wait until WiFiInfoView displays all Wi-Fi networks that it detects.
5. Scan through the information that is displayed. Does the amount of available information from Wi-Fi networks to which you are not connected surprise you?
6. Scroll back to the first column of information.
7. Under **SSID**, is there a service set identifier for each network? Why would an SSID not appear? Does disabling the broadcast of the SSID name give any enhanced level of security? Why not?
8. Note the value under the column **MAC Address**. How could a threat actor use this information?
9. Under **RSSI**, the signal strength is displayed. (Lower numbers indicate a stronger signal.)
10. The **Frequency** column displays the frequency on which the network is transmitting, and the **Channel** column gives the corresponding channel. Click **Channel** to sort the channels. Is there any channel overlap? How could this be a problem?
11. Double-click the Wi-Fi network to which you are currently connected. A window is displayed showing the available information that is being transmitted through the Wi-Fi. This is information regarding your Wi-Fi network that anyone can see. Close this window.

12. Now select a network other than the one to which you are connected and double-click it to display information. After reading the information, close the window.
13. Scroll to the **Security** and **Cipher** columns. What security are the networks using?
14. Scroll to **WPS Support**. How many networks have WPS turned on? Is this secure?
15. What additional information do you find useful? What information would a threat actor find useful?
16. Close all windows.

Project 11-2: Viewing WLAN Security Information with Vistumbler

Time Required: 25 minutes
Objective: Given a scenario, install and configure wireless security settings.
Description: Vistumbler can be used to display the security information that is beaconed out from WLANs. Note that Vistumbler does not allow you to "crack" any WLANs but instead only displays information. In this project, you use Vistumbler to view this information. This project works best when you are in an area in which you can pick up multiple WLAN signals.

1. Use your web browser to go to **www.vistumbler.net**. (The location of content on the Internet may change without warning. If you are no longer able to access the program through this URL, use a search engine and search for "Vistumbler.")
2. Click **EXE Installer (Mirror)**.
3. Follow the prompts to download and install Vistumbler using the default settings.
4. If the program does not start after the installation is complete, launch Vistumbler.

CAUTION Some AV software may indicate that Vistumbler is a virus. It might be necessary to temporarily turn off your AV software for this project. Be sure to turn AV back on when the project is completed.

5. If necessary, expand the window to full screen.
6. Click **Scan APs**. If no networks appear, click **Interface** and then select the appropriate wireless NIC interface.
7. Note the columns **Signal** and **High Signal**. How could they be used in a site survey?
8. Click **Graph 1**.
9. Click one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes. What information is displayed on this graph?
10. Click **Graph 2**.
11. Click another one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes. What information is displayed on this graph? How is this different from the previous graph?
12. Click **No Graph** to return to the previous screen.
13. Use the horizontal scroll bar to move to the right. Note the columns **Authentication**, **Encryption**, **Manufacturer**, and **Radio Type**. How would this information be useful to an attacker?
14. Use the horizontal scroll bar to move back to the far left.
15. In the left pane, expand the information under **Authentication**. What types are listed?
16. Expand the information under these types and note the information given for the wireless LAN signals.
17. In the left pane, expand the information under **Encryption**. What types are listed? Which types are most secure? Which types are least secure?
18. Expand the information under these types and note the information given for each WLAN.
19. Record the total number of different WLANs that you can detect, along with the number of encryption types. Which type is most common?
20. One of the features of Vistumbler is its ability to use audio and text-to-speech information so that the location and strength of WLANs can be detected without the need to constantly monitor the screen. Be sure that the speakers on the laptop computer are turned on.
21. Click **Options**.
22. Click **Speak Signals**. Vistumbler will "speak" the percentage of signal strength.
23. Now carry the laptop away from the AP and note the changes. How would this be helpful to an attacker?
24. Close Vistumbler.

25. Close all windows and do not save any data. If necessary, restart your AV software.
26. How does Vistumbler compare with WiFiInfoView? Which is easier to use? Which tool gives more information?

Project 11-3: Configuring Access Points

Time Required: 25 minutes
Objective: Given a scenario, install and configure wireless security settings.
Description: The ability to properly configure an AP is an important skill for any wireless network professional as well as, to a lesser degree, for users. In this project, you use an online emulator from TRENDnet to configure an AP.

1. Use your web browser to go to **www.trendnet.com/emulators/TEW-818DRU_v1/login.htm**. (The location of content on the Internet may change without warning; if you are no longer able to access the program through this URL, use a search engine and search for "Trendnet Emulators.")
2. The emulated login screen will appear. Click **Login** without entering a username or password.
3. An emulated Setup screen is displayed, showing what a user would see when configuring an actual TRENDnet.
4. Be sure that the **BASIC** tab is selected in the left pane. Note the simulated **Network Status** information.
5. Click **Wireless** in the left pane and read the information displayed.
6. Under **Broadcast Network Name (SSID)**, click the down arrow next to **Enabled**. What other option is available? Would it be an advantage to change this setting? Why or why not?
7. Under **Frequency (Channel)**, note that the default is **Auto**. What does this mean?
8. Click the down arrow on **Auto**. When would you want to change the channel on which the wireless signal is broadcast?
9. Under **Channel BandWidth**, click the down arrow on **20 MHz**. What is the other option? Why would you choose this option? What are the advantages and disadvantages of changing the channel bandwidth?
10. Under **Security Policy** is a single configuration option, **Security Mode**. Note the default setting. Is this a good option default option? What does **WPA2-PSK** mean?
11. Click the down arrow on **WPA2-PSK**. What are the other options? What do they mean?
12. Under **WPA**, note the option **WPA Encryption**. Click the down arrow on **AES**. What are the other options available and what do they mean?
13. Under **WPA passphrase**, note the length of the default passphrase. Is that sufficient?
14. In the left pane, click **Guest Network**. A guest network allows you to have an additional open network for occasional guests that does not affect the main wireless network. How could this be an advantage?
15. Note the option under **Internet Access Only**. When would you select this option?
16. Note the option under **Wireless Client Isolation**. Why is this not enabled by default?
17. Under **Security Policy**, note that the **Security Mode** is set to **Disable** by default. Why would a guest network's security be turned off by default? (Hint: If it were turned on, what would the guests need before they could use the network?)
18. In the left pane, click **Advanced**.
19. Click **Security**.
20. Under **Access Control**, what is the **LAN Client Filter Function**? Does it provide strong security if it were enabled?
21. How easy is this user interface to navigate? Does it provide enough information for a user to set up the security settings on this system?
22. Close all windows.

Project 11-4: Using Microsoft Windows Netsh Commands

Time Required: 25 minutes
Objective: Given a scenario, install and configure wireless security settings.
Description: The Windows *netsh* commands for a wireless local area network (WLAN) provide the means to configure wireless connectivity and security settings using the command line instead of a graphical user interface (GUI). Benefits of the wireless *netsh* interface include easier wireless deployment as an alternative to Group Policy, ability to configure clients to support multiple security options, and even the ability to block undesirable networks. In this project, you will explore some of the *netsh* commands.

NOTE 24

For this project, you need a computer running Microsoft Windows that has a wireless NIC and can access a wireless LAN.

1. In Microsoft Windows, right-click the **Start** button.
2. Select **Windows PowerShell (Admin)**. The Windows command window opens in elevated privilege mode.
3. Type **netsh** and then press **Enter**. The command prompt changes to *netsh*>.
4. Type **wlan** and then press **Enter**. The command prompt changes to *netsh wlan*>.
5. Type **show drivers** and then press **Enter** to display the wireless NIC driver information. It may be necessary to scroll toward the top to see all the information.
6. Next, view the WLAN interfaces for this computer. Type **show interfaces** and then press **Enter**. Record the SSID value and the name of the profile.
7. View the global wireless settings for this computer. Type **show settings** and then press **Enter**.
8. Display all the available networks to this computer. Type **show networks** and then press **Enter**.
9. Windows creates a profile for each network that you connect to. To display those profiles, type **show profiles** and then press **Enter**. If there is a profile of a network that you no longer use, type **delete profile name**=*profile-name*.
10. Disconnect from your current WLAN by typing **disconnect** and then pressing **Enter**. Note the message you receive, and observe the status in your system tray.
11. Reconnect to your network by typing **connect name**=*profile-name* **ssid**=*ssid-name* as previously recorded and then press **Enter**.
12. Netsh allows you to block specific networks. Select another network name that you are not currently connected to. Type **show networks**, press **Enter**, and then record the SSID of the network you want to block. Type **add filter permission = block ssid**=*ssid-name* **networktype = infrastructure** and then press **Enter**.
13. Type **show networks** and then press **Enter**. Does the network that you previously blocked appear in the list?
14. Display the blocked network (but do not allow access to it). Type **set blockednetworks display=show** and then press **Enter.**
15. Type **show networks** and then press **Enter**. Does the network that you previously blocked appear in the list?
16. Click the wireless icon in your system tray. Does the network appear in this list?
17. If necessary, click the wireless icon in your system tray again. What appears next to the name of this blocked network? Click the name of the network. What does it say?
18. Now re-enable access to the blocked network by typing **delete filter permission = block ssid**=*ssid-name* **networktype = infrastructure** and then press **Enter**.
19. Type **Exit** and then press **Enter**.
20. Type **Exit** again and then press **Enter** to close the command window.

Case Projects

Case Project 11-1: Comparisons of Contactless Payment Systems

Three of the most popular contactless payment systems are Apple Pay, Google Pay, and Samsung Pay. Each has advantages and disadvantages. Using the Internet, research these three different systems. Create a table that lists each system and its features, strengths and weaknesses, ease of use, security, etc. Which of them would you recommend? In your opinion, what can be done to make these more popular? Write a one-paragraph summary to accompany your table.

Case Project 11-2: Bluetooth Range Estimator

The range at which a Bluetooth device can transmit depends on several factors. Understanding the ranges helps you be aware of whether a Bluetooth-enabled device could be the victim of a bluejacking or bluesnarfing attack. Go to **www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/range/** to explore the Bluetooth Range

Estimator tool. First, watch the video and then read the details of each of the key factors. Then use the range estimator tool, changing the different parameters (receiver sensitivity, path loss, transmit power, transmitter antenna gain, and receiver antenna gain) to determine the estimated range. What does this tell you about Bluetooth ranges? How could this tool be used? Write a one-page paper on what you have learned.

Case Project 11-3: EAP

Use the Internet to research information on the EAP protocols that are supported in WPA2 Enterprise (see Table 11-5). Write a brief description of each, and indicate the relative strength of its security. Write a one-page paper on your research.

Case Project 11-4: WPA3 Features

Use the Internet to research WPA3 features, particularly SAE and OWE. What are the primary advantages and disadvantages of each of these features? How do they enhance Wi-Fi security? Write a one-page paper on your research.

Case Project 11-5: Antennas

To many users, antennas are just one of life's great mysteries. They know from experience that any antenna is better than having no antenna and that the higher the antenna is located, the better the reception will be. Yet the antenna is arguably one of the most important parts of a wireless network. Antennas play a vital role in both sending and receiving signals, and a properly positioned and functioning antenna can make all the difference between a WLAN operating at peak efficiency or a network that nobody can use. Use the Internet to research antennas for APs. What different types of antennas are used? What are their strengths? What are their weaknesses? Which types would be used to concentrate a signal to a more confined area? Write a one-page paper on what you find.

Case Project 11-6: Your Personal Wireless Security

Is the wireless network you own as secure as it should be? Examine your wireless network or that of a friend or neighbor, and determine which security model it uses. Next, outline the steps it would take to move it to the next highest level. Estimate how much it would cost and how much time it would take to increase the level. Finally, estimate how long it would take you to replace all the data on your computer and what you might lose if the data were corrupted by an attacker. Would this be motivation to increase your current wireless security model? Write a one-page paper on your work.

Case Project 11-7: Community Site Activity

The Information Security Community Site is an online companion to this textbook. It contains a wide variety of tools, information, discussion boards, and other features to assist learners. Go to **community.cengage.com/infosec2** and click the *Join or Sign in* icon to log in, using your login name and password that you created in Module 1. Click **Forums (Discussion)** and then click **Security+ Case Projects (7th edition)**. Read the following case study.

Comcast is a nationwide ISP offering its Xfinity product to consumers. The device from Comcast that consumers use to connect to the Internet also includes a Wi-Fi wireless gateway. However, this gateway broadcasts two Wi-Fi signals: one for the consumer and a second network signal that any Xfinity Internet customer can use without the customer's permission by simply signing on. This means that any Xfinity customer can use another customer's Wi-Fi service without first receiving approval. There is not a means to disable this free service. How do you feel about Xfinity offering this service without the customer's express approval for others to access this second Wi-Fi signal? Would you want strangers accessing your Wi-Fi service without your knowledge or approval? What are the advantages? What are the risks? Visit the Community Site discussion board and post how you feel about Internet content filters.

Case Project 11-8: North Ridge Security

North Ridge Security provides security consulting and assurance services. You have recently been hired as an intern to assist them.

Pomodoro Fresco is a regional Italian pizza chain that provides free open wireless access to its customers and secure wireless access for its staff. However, Pomodoro Fresco is concerned about the security of the WLAN. They have asked North Ridge to make a presentation about wireless attacks and their options for security. North Ridge has asked you to help them in the presentation.

1. Create a PowerPoint presentation for the staff about the threats against WLANs and the weaknesses of Wi-Fi. Also, include information about the more secure WPA3. Your presentation should contain at least 10 slides.
2. After the presentation, Pomodoro Fresco is trying to decide if they should install a captive portal for their customer WLAN. Create a memo to their management outlining the advantages and disadvantages, along with your recommendation.

References

1. "Cisco annual internet report (2018–2023) white paper," *Cisco*, Mar. 9, 2020, accessed Jul. 9, 2020, www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.
2. Tepper, Taylor, "Contactless credit cards and payments: The good, the bad, and the ugly," *Wirecutter*, May 7, 2020, accessed Jul. 10, 2020, www.nytimes.com/wirecutter/money/credit-cards/contactless-payment/.
3. "Assessing the economic value of unlicensed use in the 5.9 GHz & 6 GHz bands," Telecom Advisory Service, Apr. 2020, accessed Jul. 10, 2020, http://wififorward.org/wp-content/uploads/2020/04/5.9-6.0-FINAL-for-distribution.pdf.