Chapter 4

Securing Your Network

CompTIA Security+ objectives covered in this chapter:

1.2 Compare and contrast types of attacks.

- Wireless attacks (Replay, IV, Evil twin, Rogue AP, Jamming, WPS, Bluejacking, Bluesnarfing, RFID, NFC, Disassociation)

2.1 Install and configure network components, both hardware- and software-based, to support organizational security.

- VPN concentrator (Remote access vs. site-to-site, IPSec [Tunnel mode, Transport mode, AH, ESP], Split tunnel vs. full tunnel, TLS, Always-on VPN), NIPS/NIDS (Signature-based, Heuristic/behavioral, Anomaly, Inline vs. passive, In-band vs. out-of-band, Rules, Analytics [False positive, False negative]), Access point (SSID, MAC filtering, Signal strength, Band selection/width, Antenna types and placement, Fat vs. thin, Controller-based vs. standalone), NAC (Dissolvable vs. permanent, Host health checks, Agent vs. agentless), SSL/TLS accelerators, SSL decryptors

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- Honeypot

2.3 Given a scenario, troubleshoot common security issues.

- Misconfigured devices (Access points)

2.4 Given a scenario, analyze and interpret output from security technologies.

- HIDS/HIPS

2.6 Given a scenario, implement secure protocols.

- Use cases (Remote access)

3.2 Given a scenario, implement secure network architecture concepts.

- Zones/topologies (Wireless, Guest, Honeynets, Ad hoc), Tunneling/VPN (Site-to-site, Remote access), Security

device/technology placement (Sensors, Collectors, VPN concentrators, SSL accelerators, Taps and port mirror), SDN

4.2 Given a scenario, install and configure identity and access services.

- TACACS+, CHAP, PAP, MSCHAP, RADIUS

4.3 Given a scenario, implement identity and access management controls.

- Certificate-based authentication (IEEE 802.1x)

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

- Cryptographic protocols (WPA, WPA2, CCMP, TKIP), Authentication protocols (EAP, PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, IEEE 802.1x, RADIUS Federation), Methods (PSK vs. Enterprise vs. Open, WPS, Captive portals)

**

In this chapter, you'll learn about some of the more advanced network security concepts. Topics include intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), methods used to secure wireless networks, and virtual private network (VPN) technologies.

Exploring Advanced Security Devices

Chapter 3, "Exploring Network Technologies and Tools," discusses basic network technologies and protocols. This section explores many of the more advanced security devices used to secure networks.

Understanding IDSs and IPSs

Intrusion detection systems (IDSs) monitor a network and send alerts when they detect suspicious events on a system or network. Intrusion prevention systems (IPSs) react to attacks in progress and prevent them from reaching systems and networks.

Chapter 8, "Using Risk Management Tools," discusses protocol analyzers, or sniffers, in more depth, but as an introduction, administrators use them to capture and analyze network traffic sent between hosts. IDSs and IPSs have the same capability. They capture the traffic and analyze it to detect potential attacks or anomalies.

Both IDSs and IPSs have the ability of detecting attacks using similar

detection methods. The biggest difference is in their responses to an attack. This section presents IDSs first, and then wraps up with some information on IPSs and compares the two. However, as you go through this section, it's worth remembering that IDSs and IPSs can implement the same monitoring and detection methods.

HIDS

A host-based intrusion detection system (***HIDS***) is additional software installed on a system such as a workstation or server. It provides protection to the individual host and can detect potential attacks and protect critical operating system files. The primary goal of any IDS is to monitor traffic. For a HIDS, this traffic passes through the network interface card (NIC).

Many host-based IDSs have expanded to monitor application activity on the system. As one example, you can install a HIDS on different Internet-facing servers, such as web servers, mail servers, and database servers. In addition to monitoring the network traffic reaching the servers, the HIDS can also monitor the server applications.

It's worth stressing that a HIDS can help detect malicious software (malware) that traditional antivirus software might miss. Because of this, many organizations install a HIDS on every workstation as an extra layer of protection in addition to traditional antivirus software. Just as the HIDS on a server is used primarily to monitor network traffic, a workstation HIDS is primarily used to monitor network traffic reaching the workstation. However, a HIDS can also monitor some applications and can protect local resources such as operating system files.

In other organizations, administrators only install a HIDS when there's a perceived need. For example, if an administrator is concerned that a specific server with proprietary data is at increased risk of an attack, the administrator might choose to install a HIDS on this system as an extra layer of protection.

NIDS

A network-based intrusion detection system (***NIDS***) monitors activity on the network. An administrator installs NIDS sensors or collectors on network devices such as routers and firewalls. These sensors gather information and report to a central monitoring server hosting a NIDS console.

A NIDS is not able to detect anomalies on individual systems or

workstations unless the anomaly causes a significant difference in network traffic. Additionally, a NIDS is unable to decrypt encrypted traffic. In other words, it can only monitor and assess threats on the network from traffic sent in plaintext or nonencrypted traffic.

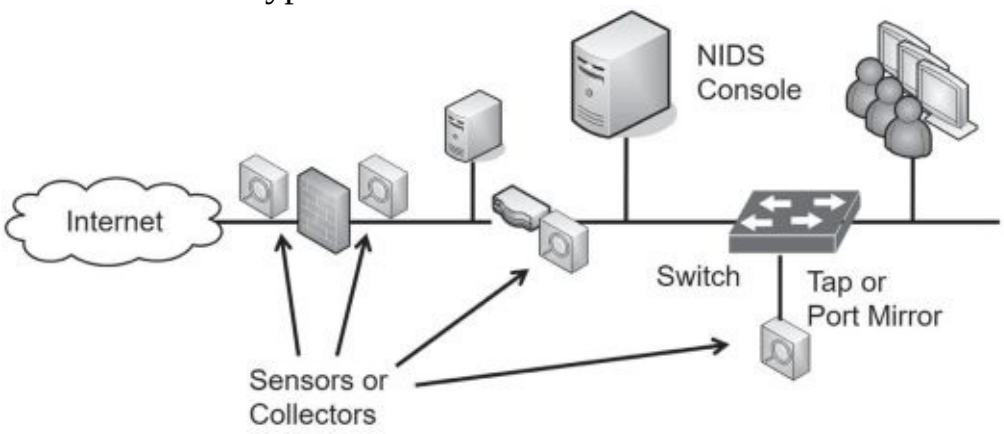


Figure 4.1 shows an example of a NIDS configuration. In the figure, sensors are located before the firewall, after the firewall, and on routers. These sensors collect and monitor network traffic on subnets within the network and report to the NIDS console. The NIDS provides overall monitoring and analysis and can detect attacks on the network.

Figure 4.1: NIDS sensors

Figure 4.1 also shows a tap or ***port mirror*** on the internal switch. Most switches support port mirroring, allowing administrators to configure the switch to send all traffic received by the switch to a single port. After configuring a port mirror, you can use it as a tap to send all switch data to a sensor or collector, and forward this to a NIDS. Similarly, it's possible to configure ***taps*** on routers to capture all traffic sent through the switch and send it to the IDS.

Sensor and Collector Placement

The decision on where you want to place the sensors depends on what you want to measure. For example, the sensor on the Internet side of the firewall will see all the traffic. However, the sensor on the internal side of the firewall will only see traffic that passes through the firewall. In other words, the firewall will filter some attacks, and the internal sensor won't see them.

If you want to see all attacks on your network, put a sensor on the Internet side. If you only want to see what gets through, put sensors internally only. If you want to see both, put sensors in both places.

Remember this

A HIDS can monitor all traffic on a single host system such as a server or a workstation. In some cases, it can detect malicious activity missed by antivirus software. A NIDS is installed on network devices, such as routers or firewalls, to monitor network traffic and detect network-based attacks. It can also use taps or port mirrors to capture traffic. A NIDS cannot monitor encrypted traffic and cannot monitor traffic on individual hosts.

Detection Methods

An IDS can only detect an attack. It cannot prevent attacks. In contrast, an IPS prevents attacks by detecting them and stopping them before they reach the target. An attack is any attempt to compromise confidentiality, integrity, or availability.

The two primary methods of detection are signature-based and heuristic- or behavioral- based (also called anomaly-based). Any type of IDS can detect attacks based on signatures, anomalies, or both. The HIDS monitors the network traffic reaching its NIC and the NIDS monitors the traffic on the network.

Signature-Based Detection

Signature-based IDSs (also called definition-based) use a database of known vulnerabilities or known attack patterns. For example, tools are available for an attacker to launch a SYN flood attack on a server by simply entering the IP address of the system to attack. The attack tool then floods the target system with synchronize (SYN) packets, but never completes the three-way Transmission Control Protocol (TCP) handshake with the final acknowledge (ACK) packet. If the attack isn't blocked, it can consume resources on a system and ultimately cause it to crash.

However, this is a known attack with a specific pattern of successive SYN packets from one IP to another IP. The IDS can detect these patterns when the signature database includes the attack definitions. The process is very similar to what antivirus software uses to detect malware. You need to update both IDS signatures and antivirus definitions from the vendor on a regular basis to protect against current threats.

Heuristic/Behavioral Detection

Heuristic/behavioral-based detection (also called ***anomaly***-based detection) starts by identifying normal operation or normal behavior of the network. It does this by creating a performance baseline under normal operating conditions.

The IDS provides continuous monitoring by constantly comparing current network behavior against the baseline. When the IDS detects abnormal activity (outside normal boundaries as identified in the baseline), it gives an alert indicating a potential attack.

Heuristic-based detection is similar to how heuristic-based antivirus software works. Although the internal methods are different, both examine activity and detect abnormal activity that is beyond the capability of signature-based detection.

SYN Flood Attack (Sidebar)

The SYN flood attack is a common denial-of-service (DoS) attack. Chapter 3 describes the three-way handshake to establish a session. As a reminder, one system sends a SYN packet, the second system responds with a SYN/ACK packet, and the first system then completes the handshake with an ACK packet. However, in a SYN flood attack, the attacker sends multiple SYN packets but never completes the third part of the TCP handshake with the last ACK packet.

This is like a friend extending his hand to shake hands with you, you extending your hand in response, and then, at the last instant, the friend pulls his hand away. Although you or I would probably stop extending our hand back to someone doing this, the server doesn't know any better and keeps answering every SYN packet with a SYN/ACK packet.

Each uncompleted session consumes resources on the server, and if the SYN flood attack continues, it can crash the server. Some servers reserve a certain number of resources for connections, and once the attack consumes these resources, the system blocks additional connections. Instead of crashing the server, the attack prevents legitimate users from connecting to the server.

IDSs and IPSs can detect a SYN flood attack and IPSs can prevent the attack. Additionally, many firewalls include a SYN flood guard that can detect SYN flood attacks and take steps to close the open sessions. This is different than a flood guard on a switch designed to stop MAC flood attacks, as discussed in Chapter 3.

This can be effective at discovering zero-day exploits. A zero-day vulnerability is usually defined as one that is unknown to the vendor.

However, in some usage, administrators define a zero-day exploit as one where the vendor has not released a patch. In other words, the vendor might know about the vulnerability but has not written, tested, and released a patch to close the vulnerability yet.

In both cases, the vulnerability exists and systems are unprotected. If attackers discover the vulnerabilities, they try to exploit them. However, the attack has the potential to create abnormal traffic allowing an anomaly-based system to detect it.

Any time administrators make any significant changes to a system or network that cause the normal behavior to change, they should re-create the baseline. Otherwise, the IDS will constantly alert on what is now normal behavior.

Remember this

Signature-based detection identifies issues based on known attacks or vulnerabilities. Signature-based detection systems can detect known anomalies. Heuristic or behavior- based IDSs (also called anomaly-based) can detect unknown anomalies. They start with a performance baseline of normal behavior and then compare network traffic against this baseline. When traffic differs significantly from the baseline, the IDS sends an alert.

Data Sources and Trends

Any type of IDS will use various raw data sources to collect information on activity. This includes a wide variety of logs, such as firewall logs, system logs, and application logs. These logs can be analyzed to provide insight on trends. These trends can detect a pattern of attacks and provide insight into how to better protect a network.

Many IDSs have the capability to monitor logs in real time. Each time a system records a log entry, the IDS examines the log to determine if it is an item of interest or not. Other IDSs will periodically poll relevant logs and scan new entries looking for items of interest.

Reporting Based on Rules

IDSs report on events of interest based on rules configured within the IDS. All events aren’t attacks or actual issues, but instead, they provide a

report indicating an event might be an alert or an alarm. Administrators investigate to determine if it is valid. Some systems consider an alarm and an alert as the same thing. Other systems use an alarm for a potentially serious issue, and an alert as a relatively minor issue. The goal in these latter systems is to encourage administrators to give a higher precedence to alarms than alerts.

The actual reporting mechanism varies from system to system and in different organizations. For example, one IDS might write the event into a log as an alarm or alert, and then send an email to an administrator account. In a large network operations center (NOC), the IDS might send an alert to a monitor easily viewable by all personnel in the NOC. The point is that administrators configure the rules within the IDS based on the needs of the organization.

False Positives Versus False Negatives

While IDSs use advanced analytics to examine traffic, they are susceptible to both false positives and false negatives. A ***false positive*** is an alert or alarm on an event that is nonthreatening, benign, or harmless. A ***false negative*** is when an attacker is actively attacking the network, but the system does not detect it. Neither is desirable, but it's impossible to eliminate both. Most IDSs trigger an alert or alarm when an event exceeds a threshold.

Consider the classic SYN flood attack, where the attacker withholds the third part of the TCP handshake. A host will send a SYN packet and a server will respond with a SYN/ACK packet. However, instead of completing the handshake with an ACK packet, the attacking host never sends the ACK, but continues to send more SYN packets. This leaves the server with open connections that can ultimately disrupt services.

If a system receives 1 SYN packet without the accompanying ACK packet, is it an attack? Probably not. This can happen during normal operations. If a system receives over 1,000 SYN packets from a single IP address in less than 60 seconds, without the accompanying ACK packet, is it an attack? Absolutely.

Administrators configure rules within the IDS and set the threshold to a number between 1 and 1,000 to indicate an attack. If administrators set it too low, they will have too many false positives and a high workload as they spend their time chasing ghosts. If they set the threshold too high, actual attacks will get through without administrators knowing about them.

Similarly, they can configure many settings based on the analytics and capabilities of the IDS.

Most administrators want to know if their system is under attack. That's the primary purpose of the IDS. However, an IDS that constantly cries "Wolf!" will be ignored when the real wolf attacks. It's important to set the threshold high enough to reduce the number of false positives, but low enough to alert on any actual attacks.

There is no perfect number for the threshold. Administrators adjust thresholds in different networks based on the network's activity level and their personal preferences.

Remember this

A false positive incorrectly indicates an attack is occurring when an attack is not active. A high incidence of false positives increases the administrator's workload. A false negative is when an attack is occurring, but the system doesn't detect and report it. Administrators often set the IDS threshold high enough that it minimizes false positives but low enough that it does not allow false negatives.

IPS Versus IDS—Inline Versus Passive

Intrusion prevention systems (IPSs) are an extension of IDSs. Just as you can have both a HIDS and a NIDS, you can also have a HIPS and a NIPS, but a network-based IPS (***NIPS***) is more common. There are some primary distinctions of an IPS when compared with an IDS:

- An IPS can detect, react, and prevent attacks.
- In contrast, an IDS monitors and will respond after detecting an attack, but it doesn't prevent them.
- An IPS is ***inline*** with the traffic. In other words, all traffic passes through the IPS and the IPS can block malicious traffic. This is sometimes referred to as in-band.
- In contrast, an IDS is ***out-of-band***. It monitors the network traffic, but the traffic doesn't go through the IDS. This is sometimes referred to as passive.

Most IDSs will only respond by raising alerts. For example, an IDS will

log the attack and send a notification. The notification can come in many forms, including an email to a group of administrators, a text message, a pop-up window, or a notification on a central monitor. Some IDSs have additional capabilities allowing them to change the environment in addition to sending a notification.

For example, an IDS might be able to modify access control lists (ACLs) on firewalls to block offending traffic, close processes on a system that were caused by the attack, or divert the attack to a safe environment, such as a honeypot or honeynet (discussed later in this chapter). While this is sometimes referred to as an active IDS, this phrase can be misleading.

Specifically, the CompTIA Security+ objectives use the terms inline and in-band for an IPS and passive and out-of-band for an IDS.

Remember this

An IPS can detect, react, and prevent attacks. It is placed inline with the traffic (also known as in-band). An IDS monitors and responds to an attack. It is not inline but instead collects data passively (also known as out-of-band).

As a reminder from the introduction of this section, both IDSs and IPSs have protocol analyzer capabilities. This allows them to monitor data streams looking for malicious behavior. An IPS can inspect packets within these data streams and block malicious packets before they enter the network.

In contrast, a NIDS has sensors or data collectors that monitor and report the traffic. An active NIDS can take steps to block an attack, but only after the attack has started. The inline configuration of the IPS allows an IPS to prevent attacks from reaching the internal network.

As an example, Figure 4.2 shows the location of two network-based IPSs (NIPS 1 and NIPS 2). All Internet traffic flows through NIPS 1, giving it an opportunity to inspect incoming traffic. NIPS 1 protects the internal network by detecting malicious traffic and preventing attacks from reaching the internal network.

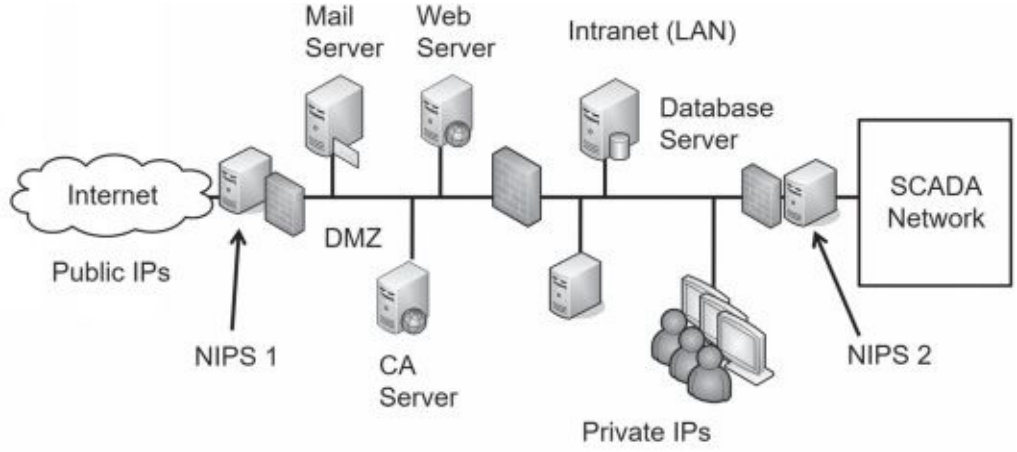


Figure 4.2: NIPS used to detect and prevent attacks

NIPS 2 is protecting an internal private network. As an example, imagine that Homer needs to manage some equipment within a supervisory control and data acquisition (SCADA) network in the nuclear power plant. The SCADA equipment is in the private network. The firewall next to NIPS 2 can have rules that allow traffic from Homer's computer into the network, but block all other traffic. NIPS 2 will then inspect all the incoming traffic and block malicious traffic.

This might seem like overkill, but many advanced persistent threats (APTs) have successfully installed remote access Trojans (RATs) onto internal systems through phishing or malware attacks. Once the ***RAT*** is installed, attackers can now attack from within. If an attacker began launching attacks on the private network from Homer's system, the firewall wouldn't block it. However, the NIPS will prevent this attack from reaching the private network.

Notice that each IPS is placed on the edge of the protected network. NIPS 1 is placed on the edge of the network between the Internet and the demilitarized zone (DMZ). NIPS 2 is on the edge of the SCADA network between it and the intranet. This placement ensures that the NIPS can inspect all traffic going into the network.

Remember this

An intrusion prevention system (IPS) is a preventive control. It is placed inline with traffic. An IPS can actively monitor data streams, detect malicious content, and stop attacks in progress. It can also be used internally to protect private networks.

SSL/TLS Accelerators

SSL/TLS accelerators refer to hardware devices focused on handling Transport Layer Security (TLS) traffic. As mentioned previously in this book, TLS is the designated replacement for Secure Sockets Layer (SSL), but many people are familiar with SSL terminology so you'll continue to see it, even if the only protocol it's using is TLS.

TLS provides encryption for many different protocols, including Hypertext Transfer Protocol Secure (HTTPS). HTTPS uses a certificate and asymmetric encryption, both described in more depth in Chapter 10, "Understanding Cryptography and PKI." The process of establishing the HTTPS session, negotiating the best security supported by both the client and the server, sharing encryption keys, and encrypting session data all take a lot of time and resources. By off-loading this to another hardware device, it frees up the primary computer's resources, such as CPU power and RAM.

When using an SSL accelerator, it's best to place it as close as possible to related devices. For example, if you're using an SSL accelerator to off-load HTTPS sessions for a web server, place the SSL accelerator close to the web server.

SSL Decryptors

Some organizations use ***SSL decryptors*** to combat many threats. For example, attackers are often using encryption to prevent inspection methods from detecting malware coming into a network.

As an example, imagine Homer innocently goes to a malicious web site. The web site establishes a secure HTTPS connection, and then downloads malware to Homer's computer. Because the site is using HTTPS, the malware is encrypted while in transit. Even if an organization had the best content inspection methods and malware detection software, it wouldn't detect the

malware while it's encrypted.

An SSL decryptor solves this problem. You would place it in the DMZ, and redirect all traffic to and from the Internet through it. Unencrypted data goes through the device without any modification. However, any attempts to establish an encrypted session prompt the SSL decryptor to create a separate SSL (or TLS) session.

When Homer innocently goes to a malicious web site, the traffic goes though the SSL decryptor. The SSL decryptor establishes an HTTPS session between it and Homer's computer. It also establishes an HTTPS session between it and the web site. All data-in-transit is encrypted. However, the SSL decryptor can view the unencrypted data and inspect it.

SSL decryptors are often used with a NIPS. The NIPS is inline but malicious traffic can get through if it's encrypted. The SSL decryptor allows the NIPS to inspect unencrypted traffic and prevent attacks.

SDN

A software defined network (***SDN***) uses virtualization technologies to route traffic instead of using hardware routers and switches. More specifically, an SDN separates the data planes and control planes within a network. Another way of thinking of this is that an SDN separates the logic used to forward or block traffic (the data plane) and the logic used to identify the path to take (the control plane).

Hardware routers use rules within an ACL to identify whether a router will forward or block traffic on the data plane. This is always proprietary because it's implemented on specific hardware routers. However, an SDN implements the data plane with software and virtualization technologies, allowing an organization to move away from proprietary hardware.

Routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) help routers determine the best path to route traffic on the control plane. Routers use these protocols to share information with each other, creating a map of the known network. An SDN can still use these routing protocols, but without the hardware routers.

Chapter 2, "Understanding Identity and Access Management," discusses the attribute- based access control (***ABAC***), which is commonly used in SDNs. Instead of rules within ACLs, ABAC models allow administrators to create data plane policies to route traffic. A huge benefit of these policies is that they typically use plain language statements instead of complex rules

within an ACL.

Honeypots

A ***honeypot*** is a sweet-looking server—at least it's intended to look sweet to the attacker, similar to how honey looks sweet to a bear. It's a server that is left open or appears to have been sloppily locked down, allowing an attacker relatively easy access. The intent is for the server to look like an easy target so that the attacker spends his time in the honeypot instead of in a live network. In short, the honeypot diverts the attacker away from the live network.

As an example, a honeypot could be a web server designed to look like a live web server. It would have bogus data such as files and folders containing fabricated credit card transaction data. If an organization suspects it has a problem with a malicious insider, it can create an internal honeypot with bogus information on proprietary projects.

Honeypots typically have minimal protection that an attacker can easily bypass. If administrators don't use any security, the honeypot might look suspicious to experienced attackers and they might simply avoid it.

Security personnel often use honeypots as a tool to gather intelligence on the attacker. Attackers are constantly modifying their methods to take advantage of different types of attacks. Some sophisticated attackers discover vulnerabilities before a patch is released (also known as a zero-day exploit, or zero-day vulnerability). In some cases, security professionals observe attackers launching zero-day vulnerability attacks against a honeypot.

Honeypots never hold any data that is valuable to the organization. The data may appear to be valuable to an attacker, but its disclosure is harmless. Honeypots have two primary goals:

- **Divert attackers from the live network.** If an attacker is spending time in the honeypot, he is not attacking live resources.
- **Allow observation of an attacker.** While an attacker is in the honeypot, security professionals can observe the attack and learn from the attacker's methodologies. Honeypots can also help security professionals learn about zero-day exploits, or previously unknown attacks.

Honeynets

A ***honeynet*** is a group of honeypots within a separate network or zone, but accessible from an organization's primary network. Security professionals often create honeynets using multiple virtual servers contained within a single physical server. The servers within this network are honeypots and the honeynet mimics the functionality of a live network.

As an example, you can use a single powerful server with a significant amount of RAM and processing power. This server could host multiple virtual servers, where each virtual server is running an operating system and applications. A physical server hosting six virtual servers will appear as seven systems on a subnet. An attacker looking in will not be able to easily determine if the servers are physical or virtual.

The purpose of this virtual network is to attract the attention of an attacker, just as a single honeypot tries to attract the attention of an attacker. If the attacker is in the honeynet, the live network isn't being attacked, and administrators can observe the attacker's actions.

Sun Tzu famously wrote in *The Art of War*, "All warfare is based on deception," and "Know your enemies." Cyberwarfare is occurring daily and security professionals on the front lines of network and system attacks recognize that these attacks mimic warfare in many ways. Honeypots and honeynets provide these professionals with some additional tools to use in this war.

Remember this

Honeypots and honeynets attempt to divert attackers from live networks. They give security personnel an opportunity to observe current methodologies used in attacks and gather intelligence on these attacks.

IEEE 802.1x Security

Chapter 3 discusses port security by disabling unused ports or using MAC address filtering. Another method of port security is to use ***IEEE 802.1x***, a port-based authentication protocol. It requires users or devices to authenticate when they connect to a specific wireless access point, or a specific physical port, and it can be implemented in both wireless and wired networks.

It secures the authentication process prior to a client gaining access to a

network and blocks network access if the client cannot authenticate. 802.1x can use simple usernames and passwords for authentication, or certificates for certificate-based authentication.

The 802.1x server prevents rogue devices from connecting to a network. Consider open RJ- 45 wall jacks. Although disabling them is a good port security practice, you can also configure an 802.1x server to require authentication for these ports. If clients cannot authenticate, the 802.1x server blocks or restricts access to the network.

It's possible to combine an 802.1x server with other network elements such as a virtual local area network (VLAN). For example, imagine you want to provide visitors with Internet access, but prevent them from accessing internal network resources. You can configure the 802.1x server to grant full access to authorized clients, but redirect unauthorized clients to a guest area of the network via a VLAN.

You can implement 802.1x as a Remote Authentication Dial-In User Service (RADIUS) or Diameter server, as discussed later in this chapter. This helps authenticate virtual private network (VPN) clients before they connect. You can also implement 802.1x in wireless networks to force wireless clients to authenticate before they connect.

Remember this

An 802.1x server provides port-based authentication, ensuring that only authorized clients can connect to a network. It prevents rogue devices from connecting.

Securing Wireless Networks

Wireless local area networks (WLANs) have become quite popular in recent years, in both home and business networks. A wireless network is easy to set up and can quickly connect several computers without the need to run cables, which significantly reduces costs.

The significant challenge with wireless networks is security. Wireless security has improved over the years, but wireless networks are still susceptible to vulnerabilities and many users just don't understand how to lock down a wireless network adequately.

Reviewing Wireless Basics

Before digging into wireless security, you need to understand some basic concepts related to wireless devices and networks. If you've recently passed the CompTIA Network+ exam, these topics will likely be very familiar to you, but they are still worth looking at to ensure you understand them from the perspective of the CompTIA Security+ exam.

A wireless ***access point (AP)*** connects wireless clients to a wired network. However, many APs also have routing capabilities. Vendors commonly market APs with routing capabilities as wireless routers so that's how you'll typically see them advertised. Two distinctions are:

- **All wireless routers are APs.** These are APs with an extra capability—routing.
- **Not all APs are wireless routers.** Many APs do not have any additional capabilities. They provide connectivity for wireless clients to a wired network, but do not have routing capabilities.

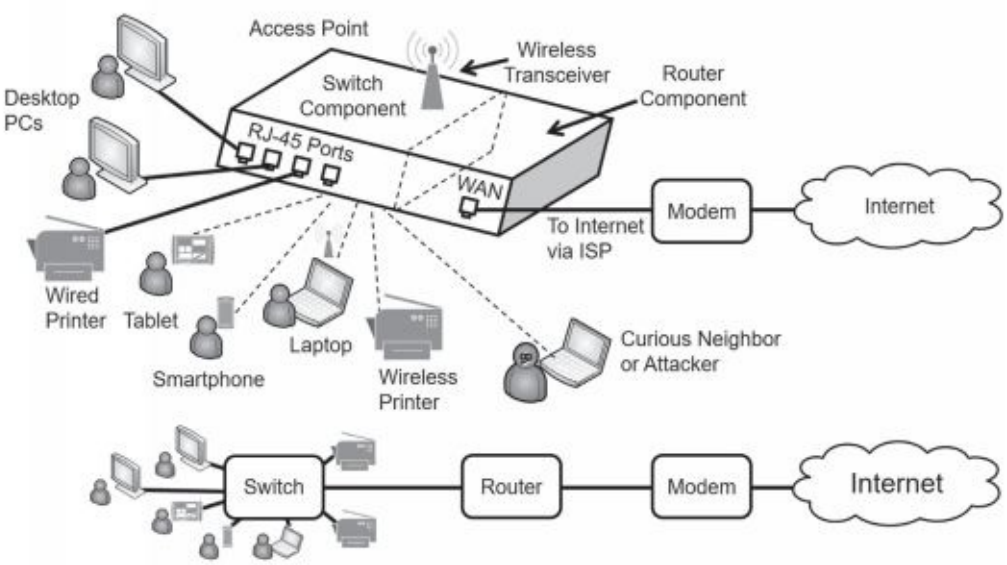


Figure 4.3 shows a diagram of a wireless router providing connectivity to multiple systems. Notice that the wireless router has both a switch component and a router component, and the drawing at the bottom of Figure 4.3 shows the logical configuration of the network. The devices connect to the switch component and the router component provides connectivity to the Internet through a broadband modem or similar device depending on the Internet Service Provider (ISP) requirements.

Figure 4.3: Wireless access point with routing capabilities (wireless

router)

Most APs include physical ports for wired access (labeled as “RJ-45 Ports” in the diagram) and a wireless transceiver for wireless clients. In other words, some users can connect with regular twisted-pair cable, and other users can connect using wireless transmissions. The wired ports and wireless connections all connect through the switch component of the wireless router. Many vendors label the Internet connection WAN for wide area network, but some vendors label this port as “Internet.”

When used as shown in Figure 4.3, the AP also includes extra services and capabilities, such as routing, Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), and more. These extra services reduce the setup time required for the WLAN.

Because wireless networks broadcast on known frequency bands, other wireless users can often see them. This includes authorized users, curious neighbors, and attackers.

Fat Versus Thin Access Points

A ***fat AP***, also known as a stand-alone, intelligent, or autonomous AP, includes everything needed to connect wireless clients to a wireless network. It typically includes features such as a routing component, NAT, DHCP, wireless security options, access control lists (ACLs), and more. If you’re running a wireless network at your home or in a small office network, you are probably using a fat access point. Fat APs must be configured separately from each other, which isn’t really a problem if you’re only configuring a single AP.

Consider a network that has a dozen APs spread around the organization. If these were all fat APs, administrators would need to configure each one separately, which is highly inefficient. Enter the ***thin AP***. A thin AP is a ***controller-based AP***, meaning that it isn’t a stand-alone AP, but rather an AP managed by a controller. Administrators use a wireless controller to configure and manage thin-based APs. This streamlines the administration by consolidating it in one place.

Thin APs are also making their way into small office and home networks. For example, NETGEAR’s Orbi wireless router includes one fat AP and one or more thin satellite APs. You configure the single AP and it then configures the satellite APs.

Remember this

A fat AP is also known as a stand-alone AP and is managed independently. A thin AP is also known as a controller-based AP and is managed by a wireless controller. The wireless controller configures the thin AP.

Band Selection and Channel Widths

Wireless networks use two primary radio bands: 2.4 GHz and 5 GHz. However, wireless devices don't transmit exactly on 2.4 GHz or 5 GHz. Instead, the two bands have multiple channels starting at about 2.4 GHz and 5 GHz. There isn't a single standard that applies to every country, so you'll find that the number of channels within each band varies from country to country.

The Institute of Electrical and Electronics Engineers (IEEE) defines many standards, including the IEEE 802.11 group of wireless network protocols. Table 4.1 shows some common wireless standards along with the frequency band (or bands) they support. It also shows the channel widths supported by each. However, the channel widths are somewhat misleading. For example, 802.11n supports channel widths of both 20 MHz and 40 MHz. However, a 40 MHz channel is two combined 20 MHz channels.

IEEE Standard	Frequency Band	Channel Width
802.11b	2.4 GHz	22 MHz
802.11g	2.4 GHz	20 MHz
802.11n	2.4 GHz and 5 GHz	20 MHz and 40 MHz
802.11ac	5 GHz	20 MHZ, 40 MHz, 80 MHz, and 160 MHz

Table 4.1: Common wireless standards, frequencies, and channel widths

Theoretically, wider channels allow you to transfer more data through the channel. Unfortunately, there are two challenges. First, when you increase the channel width, you decrease the distance of the radio transmissions. A device that connects with a 20 MHz channel at a specific distance away might not be able to connect at 40 MHz from the same location. Second, you

increase the possibility of interference. Wider channels are more likely to overlap with other wireless devices and this interference affects overall performance.

These challenges are much more prevalent in the 2.4 GHz band because there are more technologies operating in this band. For example, Bluetooth devices, microwave ovens, and cordless phones operate in this range. Additionally, the 2.4 GHz range has only three nonoverlapping channels. APs typically allow you to choose the frequency band (2.4 GHz and/or 5 GHz). Additionally, most APs allow you to manually select a channel or allow the AP to pick the best channel. The "PSK, Enterprise, and Open Modes" section (found later in this chapter) shows a screenshot of an AP with some of these selections.

Access Point SSID

Wireless networks are identified by a service set identifier (***SSID***), which is simply the name of the wireless network. Some APs still come with default SSIDs, though most vendors have moved away from this practice. For example, the default SSID of some older Linksys APs is "Linksys." Some newer APs force you to enter a name for the SSID when you first install it and do not include a default. From a defense-in-depth perspective, it's a good idea to change the name of the SSID if a default is used. It simply gives attackers less information.

For example, if an attacker sees a wireless network with an SSID of Linksys, the attacker has a good idea that the network is using a Linksys AP. If the attacker knows about specific weaknesses with this AP, he can start exploiting these weaknesses. On the other hand, an AP with an SSID of "Success" doesn't give the attacker any clues about the AP.

Disable SSID Broadcasting or Not

One of the goals of 802.11 wireless networks is ease of use. The designers wanted wireless computers to be able to easily find each other and work together. They were successful with this goal. Unfortunately, attackers can also easily find your networks. By default, APs broadcast the SSID in cleartext, making it easy to locate wireless networks.

At some point years ago, someone stated that the SSID was a password (not true!), and many information technology (IT) professionals latched onto

the idea that you can increase security by disabling the SSID broadcast. Others say that the SSID has nothing to do with security and disabling the broadcast reduces usability but does not increase security.

As background, APs must regularly send out a beacon frame to ensure interoperability with other devices in the wireless network. This beacon frame includes the SSID, and if the SSID broadcast is disabled, the SSID entry is blank. However, even if the SSID broadcast is disabled, the AP includes the SSID in Probe responses sent in response to Probe requests from authorized wireless clients. Because of this, it's easy for an attacker with a wireless protocol analyzer to listen for the Probe responses and detect the SSID.

In other words, disabling the SSID makes it a little more difficult for attackers to find your network, but not much. It's almost like locking the front door of your house, but leaving the key in the lock.

Steve Riley wrote in a security blog titled "Myth vs. Reality: Wireless SSIDs" that disabling the SSID for security "is a myth that needs to be forcibly dragged out behind the woodshed, strangled until it wheezes its last labored breath, then shot several times for good measure." In case it isn't clear, Mr. Riley is in the camp that says you should not disable the SSID for security. For the record, I agree with him.

For the CompTIA Security+ exam, you should know that it is possible to disable the SSID broadcast and hide the network from casual users. However, an attacker with a wireless protocol analyzer can easily discover the SSID even if SSID broadcast is disabled.

Remember this

The service set identifier (SSID) identifies the name of the wireless network. You should change the SSID from the default name. Disabling SSID broadcast can hide the network from casual users, but an attacker can easily discover it with a wireless sniffer.

Enable MAC Filtering

Enabling media access control (MAC) filtering provides a small measure of security to a wireless network. As a reminder from your networking studies, the MAC address (also called a physical address or hardware address) is a 48-bit address used to identify network interface cards

(NICs). You will usually see the MAC address displayed as six pairs of hexadecimal characters such as 00-16-EA-DD-A6-60. Every NIC, including wireless NICs, has a MAC address.

MAC filtering is a form of network access control. It's used with port security on switches (covered in Chapter 3) and you can use it to restrict access to wireless networks.

For example, Figure 4.4 shows the MAC filter on a NETGEAR Orbi AP. In the figure, you can see that the system is set to Permit PCs Listed Below to Access the Wireless Network. The MAC Address column shows the MAC addresses of the allowed devices. The Status column shows that each of these devices is set to Allows, granting them access. The Block all new devices from connecting setting prevents any other devices from connecting. It's also possible to select the check box for any device, and click on Block to change its status to Blocked.

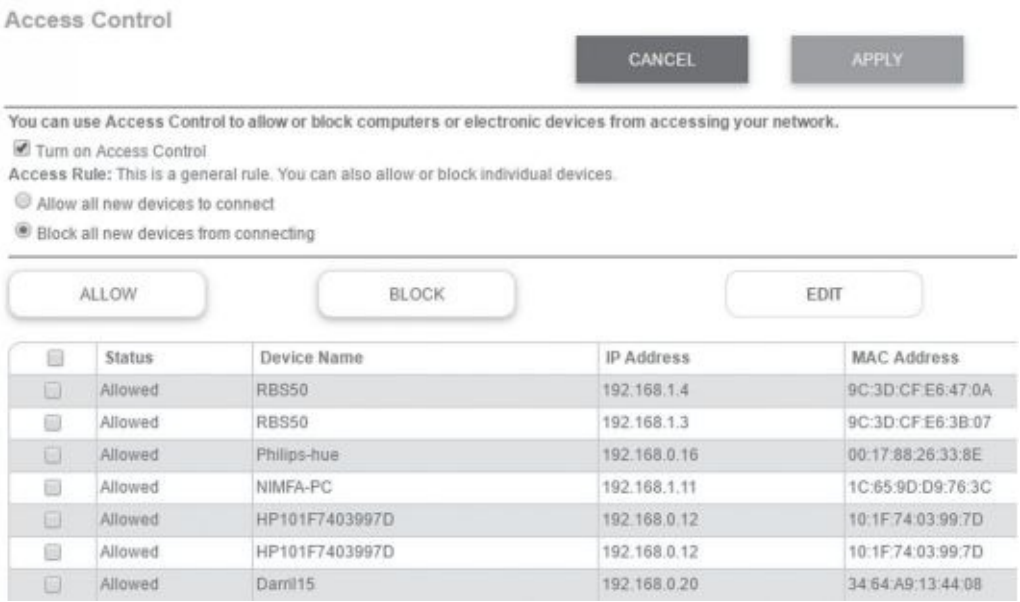


Figure 4.4: MAC filter on an AP

Theoretically, MAC addresses are unique. The MAC filter in Figure 4.4 limits access to only the devices with these MAC addresses. This might sound secure, but an attacker with a wireless sniffer can easily identify the MAC addresses allowed in a wireless network. Additionally, it's very easy to change a MAC address. An attacker can launch a spoofing attack by changing the MAC address on his laptop to impersonate one of the allowed MAC addresses.

Many operating systems include built-in functionality to change a NIC's MAC address. For example, in Windows 10 you can access the NIC's

properties from Device Manager, click the Advanced tab, and configure the Network Address setting with a new MAC.

Remember this

MAC filtering can restrict access to a wireless network to specific clients. However, an attacker can use a sniffer to discover allowed MAC addresses and circumvent this form of network access control. It's relatively simple for an attacker to spoof a MAC address.

Antenna Types and Placement

The most commonly used wireless antenna on both APs and wireless devices is an omnidirectional (or omni) antenna. Omnidirectional antennas transmit and receive signals in all directions at the same time. This allows wireless devices to connect to an AP from any direction. Another type of antenna is a directional antenna. A directional antenna transmits in a single direction and receives signals back from the same direction. Because the power of the antenna is focused in a single direction, the directional antenna has greater gain than an omni antenna, and it can transmit and receive signals over greater distances. The directional antenna also has a very narrow radiation pattern, focusing the signal in a specific area.

When considering antenna placement, you should also configure the antenna orientation. Many APs have adjustable antennas. Should you orient them vertically, pointed straight up? Or, should you orient them horizontally, pointed straight out, even with the floor? It depends. Reception is maximized when your AP's antenna orientation matches the orientation used by your wireless devices. However, you'll find that antenna orientation isn't consistent in all devices. Some place them horizontally and others place them vertically. If your AP has two antennas, some experts recommend orienting one of them horizontally and one of them vertically.

Administrators often perform a site survey while planning and deploying a wireless network. The site survey examines the wireless environment to identify potential issues, such as areas with noise or other devices operating on the same frequency bands. Administrators and security personnel periodically repeat the site survey to verify the environment hasn't changed and to detect potential security issues.

One method of performing a site survey is to configure an AP and position the antenna within the organization. Administrators then measure the power levels of the AP from different areas to determine if it provides the desired coverage. If the AP doesn't provide adequate coverage, administrators might try to modify the placement of the AP and/or its antenna, or add additional APs.

Antenna Power and Signal Strength

Youcannotmodifythegainofanantennawithoutchangingitsphysicalpropert However, many wireless access points include a power setting that you can manipulate to increase or decrease the transmit power. Administrators sometimes reduce the power level to restrict access to a small area such as a conference room, or to prevent wireless users from connecting from the parking lot or somewhere else outside the building. Similarly, administrators sometimes increase the power level to increase the range of the AP.

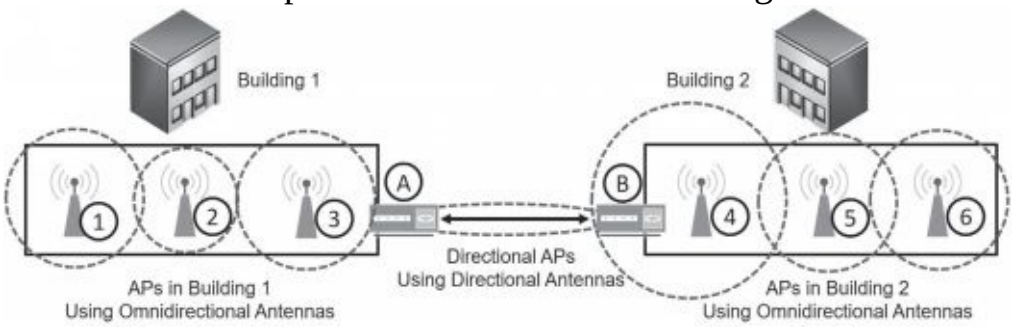


Figure 4.5 shows several APs in two buildings. The dotted circles around APs 1 through 6 show their range. They are each using omnidirectional antennas. AP 4 has a larger circle than the others, indicating the power level is the highest in this AP. The two APs labeled A and B are using directional antennas. Organizations sometimes use this configuration to connect networks between two buildings.

Figure 4.5: Omnidirectional and directional APs

Remember this

You can limit the range of an AP to a room or building by reducing the AP's power level. This prevents people from connecting because they will be out of the AP's range.

Network Architecture Zones

Chapter 3 introduces several zones and topologies used within a network. These commonly provide separation for networks based on usage. Some additional zones and topologies are:

- **Wireless.** Many organizations provide wireless networks for both employees and guests. Wireless networks for employees provide a bridge to a wired network, allowing employees access to all network resources just as if they were connected from a wired PC at their desk.
- **Guest.** A guest network is typically a wireless network used to provide guests with Internet access. The guest network rarely gives guests access to network resources, but instead gives them a simple way to check their email or access web sites.
- **Ad hoc.** In ***ad hoc*** mode, wireless devices connect to each other without an AP. For example, if you and another user have wireless laptops, you can create an ad hoc wireless network to connect your two computers. Ad hoc is Latin for "as needed," which is a good way to think about an ad hoc wireless network. You create it as needed. In contrast, when you connect to a wireless network via an AP, you are using infrastructure mode.

Wireless Cryptographic Protocols

Because wireless networks broadcast over the air, anyone who has a wireless transceiver can intercept the transmissions. You can secure wireless networks with several different steps, but the most important step is to implement a strong security protocol, such as Wi-Fi Protected Access II (WPA2). The following sections describe the primary security protocols available for wireless networks.

WPA

Wi-Fi Protected Access (***WPA***) was an interim replacement for Wired Equivalent Privacy (WEP). WEP has known vulnerabilities and should not be used. WPA provided an immediate solution to the weaknesses of WEP without requiring users to upgrade their hardware. Even when WPA replaced WEP, its developers recognized that WPA wasn't solid enough to last for an

extended period. Instead, WPA improved wireless security by giving users an alternative to WEP with existing hardware while the developers worked on creating the stronger WPA2 protocol.

WPA is susceptible to password-cracking attacks, especially when the AP has a weak passphrase. The attacker uses a wireless protocol analyzer to capture the authentication traffic and then uses an offline brute force attack to discover the passphrase. Attackers often use a disassociation attack (discussed later in this chapter) to force the user to reauthenticate.

WPA2

Wi-Fi Protected Access II (***WPA2***) is the permanent replacement for WPA. WPA2 (also known as IEEE 802.11i) uses stronger cryptography than WPA. The Wi-Fi Alliance requires all devices carrying its WI-FI CERTIFIED logo to meet WPA2 standards, including the use of the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (***CCMP***).

Although WPA2 provides significant security improvements over previous wireless encryption techniques, some enterprises need stronger security. Another step you can take is to enable authentication with Enterprise mode, described later in this chapter.

TKIP Versus CCMP

Temporal Key Integrity Protocol (***TKIP***) is an older encryption protocol used with WPA, and CCMP is a newer encryption protocol used with WPA2. IEEE has deprecated WPA and TKIP due to various security issues, but many wireless networks are still using these older protocols. IEEE recommends using WPA2 with CCMP because it provides significantly more security.

A benefit of TKIP is that it didn't require new hardware. WEP users could upgrade software and/or firmware and implement WPA with TKIP without the need to replace the hardware. Newer hardware supports WPA2, so the usage of WPA and TKIP is waning. However, you might still see some legacy hardware using WPA and TKIP.

Later implementations of WPA support Advanced Encryption Standard (***AES***) instead of TKIP. Chapter 10 presents AES in more depth, but, in short, it is a very strong and efficient encryption algorithm. Many applications beyond WPA/WPA2 use AES to provide secure encryption and ensure confidentiality. Several people have been successful at cracking WPA with

TKIP, so whenever possible, it's best to upgrade WPA to WPA2, or at least upgrade TKIP to use AES.

WPA2 supports CCMP, which is based on AES and is much stronger than WPA using TKIP. WPA2 also employs much more secure methods of managing the encryption keys than WPA.

Remember this

WPA provided an immediate replacement for WEP and originally used TKIP, which was compatible with older hardware. Later implementations support the stronger AES encryption algorithm. WPA2 is the permanent replacement for WEP and WPA. WPA2 supports CCMP (based on AES), which is much stronger than the older TKIP protocol and CCMP should be used instead of TKIP.

PSK, Enterprise, and Open Modes

Both WPA and WPA2 can operate in either pre-shared key (PSK) or Enterprise modes. When using ***PSK*** mode, users access the wireless network anonymously with a PSK or passphrase. This doesn't provide authentication. As a reminder, authentication proves a user's identity with the use of credentials such as a username and password. Users claim an identity with a username and prove their identity with a password. Just a passphrase without a username provides authorization without authentication.

In contrast, ***Enterprise*** mode forces users to authenticate with unique credentials before granting them access to the wireless network. Enterprise mode uses an 802.1x server, often implemented as a RADIUS server, which accesses a database of accounts. If users don't have the proper credentials, Enterprise mode (using an 802.1x server) blocks their access. Also, an 802.1x server can provide certificate-based authentication to increase the security of the authentication process. The authentication protocol (discussed later in this chapter) determines if the 802.1x server will use a certificate or not.

Figure 4.6 shows a screenshot of a NETGEAR Orbi router web page. The Wireless Network section shows the SSID (Success) and selections for 2.4 GHz and 5 GHz channels. The Auto selection for 2.4 GHz allows the AP to automatically select the best channel to use. The 5 GHz Channel selection indicates the device will pick from 48 available channels in this band.

Figure 4.6: Configuring wireless security

The Security Options section shows that it's selected to use WPA2-PSK with AES and the password (the passphrase or PSK) is IC@nP@ssSecurity+. It can be as many as 63 characters long and the passphrase you enter here is the same passphrase you would enter on all the wireless devices. Many security experts recommend using a passphrase at least 20 characters long, with a mix of uppercase, lowercase, numbers, and special characters. This device also supports the use of WPA for backward compatibility.

Note that the Security Options section also includes a choice of None. If you select None, the AP will operate in ***Open*** mode, meaning that it doesn't have any security.

Some APs support Enterprise mode, but the one shown in Figure 4.6 doesn't. If it did, it would include a check box to implement WPA2 Enterprise. When you select Enterprise mode, you'll need to enter three pieces of information:

- **RADIUS Server.** You enter the IP address assigned to the 802.1x server, which is often a RADIUS server. This is sometimes referred to as an AAA server.
- **RADIUS port.** You enter the port used by the RADIUS server. The official default port for RADIUS is 1812. However, some vendors have used other ports such as 1645. The key is that you must enter the same port here that the server is using.
- **Shared Secret.** The shared secret is similar to a password and you

must enter it here exactly as it is entered on the RADIUS server.

Check out the online labs for this chapter to see how to configure a wireless router using WPA2 Enterprise mode. You can access them at *http://gcgapremium.com/501labs/.*

After configuring WPA2 Enterprise on an AP, it redirects all attempts to connect to the RADIUS server to authenticate. After users authenticate, the RADIUS server tells the AP to grant them access.

Wireless authentication systems using an 802.1x server are more advanced than most home networks need, but many larger organizations use them. In other words, most home networks use Personal mode, but organizations that want to increase wireless security use Enterprise mode. A combination of both a security protocol such as WPA2 and an 802.1x authentication server significantly reduces the chance of a successful access attack against a wireless system.

Remember this

PSK mode (or WPA-PSK and WPA2-PSK) uses a pre-shared key and does not provide individual authentication. Open mode doesn't use any security and allows all users to access the AP. Enterprise mode is more secure than Personal mode, and it provides strong authentication. Enterprise mode uses an 802.1x server (implemented as a RADIUS server) to add authentication.

Authentication Protocols

Wireless networks support several different authentication protocols. Many are built on the Extensible Authentication Protocol (EAP), an authentication framework that provides general guidance for authentication methods. IEEE 802.1x servers typically use one of these methods to increase the level of security during the authentication process. Additionally, while they are often used in wireless networks, they can also be used anywhere an 802.1x server is implemented.

A key point to remember for each of these methods is if they support or require certificates.

Some methods are:

- **EAP.** ***EAP*** provides a method for two systems to create a secure encryption key, also known as a Pairwise Master Key (PMK). Systems then use this key to encrypt all data transmitted between the devices. Both TKIP and AES-based CCMP use this key, though CCMP is much more secure.
- **EAP-Flexible Authentication via Secure Tunneling (EAP-FAST).** Cisco designed ***EAP- FAST*** as a secure replacement for Lightweight EAP (LEAP) that Cisco also designed. EAP- FAST supports certificates, but they are optional.
- **Protected EAP (PEAP).** ***PEAP*** provides an extra layer of protection for EAP. The EAP designers assumed that EAP would be used with adequate physical security to ensure the communication channel was secure. In practice, that wasn't always the case, but PEAP protects the channel. PEAP encapsulates and encrypts the EAP conversation in a Transport Layer Security (TLS) tunnel. PEAP

requires a certificate on the server, but not the clients. A common implementation is with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2).

- **EAP-Tunneled TLS (EAP-TTLS).** This is an extension of PEAP, allowing systems to use some older authentication methods such as Password Authentication Protocol (PAP) within a TLS tunnel. ***EAP-TTLS*** requires a certificate on the 802.1x server but not the clients.
- **EAP-TLS.** This is one of the most secure EAP standards and is widely implemented. The primary difference between PEAP and ***EAP-TLS*** is that it requires certificates on the 802.1x server and on each of the wireless clients.
- **RADIUS Federation.** Chapter 2 covers federations used for single sign-on (SSO). As a reminder, a federation includes two or more entities (such as companies) that share the same identity management system. Users can log on once and access shared resources with the other entity without logging on again. Similarly, it's possible to create a federation using 802.1x and RADIUS servers.

Note that EAP-FAST supports digital certificates, but they are optional. PEAP and EAP-TTLS require a certificate on the server, but not the clients. EAP-TLS requires certificates on both the

servers and the clients. Chapter 10 digs into certificates much deeper, but as an introduction, certificates help provide strong authentication and encryption services. However, a Certificate Authority (CA) must issue certificates, so an organization must either purchase certificates from a public CA, or implement a private CA within the network.

Remember this

Enterprise mode requires an 802.1x server. EAP-FAST supports certificates. PEAP and EAP-TTLS require a certificate on the 802.1x server. EAP-TLS also uses TLS, but it requires certificates on both the 802.1x server and each of the clients.

Captive Portals

A ***captive portal*** is a technical solution that forces clients using web browsers to complete a specific process before it allows them access to the network. Organizations commonly use it as a hot spot that requires users to log on or agree to specific terms before they can access the Internet. Here are three common examples:

- **Free Internet access.** Many hospitals and other medical facilities provide free Internet access to patients and visitors. The captive portal requires users to acknowledge and agree to abide by an acceptable use policy (AUP). Free captive portals rarely require users to log on, but instead just require them to check a box indicating they agree, and then click a button to continue.
- **Paid Internet access.** Many hotels, resorts, cruise ships, and airlines provide Internet access to customers, but on a pay-as-you-go basis. When users attempt to access the Internet, they are redirected to the captive portal and must successfully log on with a pre-created account or enter credit card information to pay for access.
- **Alternative to IEEE 802.1x.** Adding an 802.1x server can be expensive and is sometimes not a feasible option. Organizations can use captive portals as an alternative. It requires users to authenticate before granting them access.

Understanding Wireless Attacks

There are several known attacks against wireless networks. Most can be avoided by using strong security protocols such as WPA2 with CCMP. In contrast, WPA is vulnerable to many attacks, especially if it is using TKIP.

Disassociation Attacks

A ***disassociation attack*** effectively removes a wireless client from a wireless network. To understand the attack, it's valuable to first understand the normal operation.

After a wireless client authenticates with a wireless AP, the two devices exchange frames, causing the client to be associated with the AP. At any point, a wireless device can send a disassociation frame to the AP to terminate the connection. This frame includes the wireless client's MAC address. When the AP receives the disassociation frame, it deallocates all the memory it was using for the connection.

In a disassociation attack, attackers send a disassociation frame to the AP with a spoofed MAC address of the victim. The AP receives the frame and shuts down the connection. The victim is now disconnected from the AP and must go through the authentication process again to reconnect.

Interestingly, many hotels were using this attack to prevent guests from using their own personal wireless networks. For example, if you have an iPhone with cellular access to the Internet, you can enable the Personal Hotspot feature. This lets you share the connection with other devices, such as a laptop. Some hotels looked for these personal wireless networks, and launched disassociation attacks against them. Customers were then forced to pay for the hotel's wireless services. As an example, the Federal Communications Commission (FCC) fined Marriott Hotel Services $600,000 for launching attacks on its customers that prevented them from using their personal wireless networks.

Remember this

A disassociation attack effectively removes a wireless client from a wireless network, forcing it to reauthenticate. WPS allows users to easily configure a wireless device by entering an eight-digit

PIN. A WPS attack guesses all possible PINs until it finds the correct one. It will typically discover the PIN within hours and use it to discover the passphrase.

WPS and WPS Attacks

Wi-Fi Protected Setup (***WPS***) allows users to configure wireless devices without typing in the passphrase. Instead, users can configure devices by pressing buttons or by entering a short eight-digit personal identification number (PIN).

For example, a user can configure a new wireless device by pressing a button on the AP and on the wireless device. It will automatically configure the device within about 30 seconds with no other actions needed. These buttons can be physical buttons on the devices, or virtual buttons that the user clicks via an application or web page. When using the PIN method, users first identify the eight-digit PIN on the AP and then enter the PIN on the new wireless device.

Unfortunately, WPS is susceptible to brute force attacks. A ***WPS attack*** keeps trying different PINs until it succeeds. As an example, Reaver is an open source tool freely available that allows attackers to discover the PIN within 10 hours, and often much quicker. Once it discovers the PIN, it can then discover the passphrase in both WPA and WPA2 wireless networks.

Security experts recommend disabling WPS on all devices. This is typically possible via the AP configuration page. Even if you choose to enable WPS to easily connect some devices, you should immediately turn it off once you're done.

Rogue AP

A rogue access point (***rogue AP***) is an AP placed within a network without official authorization. It might be an employee who is bypassing security or installed by an attacker. If an employee installs a rogue AP, the chances are higher that this AP will not be managed properly, increasing vulnerabilities to the network.

Generically, you can think of a rogue as a scoundrel, a crook, or a villain. Clearly, if a rogue is a crook or villain, then rogue access points are

not an administrator's friend. You might also see them called counterfeit access points, which is also a clear indication they aren't legitimate.

Attackers may connect a rogue access point to network devices in wireless closets that lack adequate physical security. This access point acts as a sniffer to capture traffic passing through the wired network device, and then broadcasts the traffic using the wireless capability of the AP. The attacker can then capture the exfiltrated data files while sitting in the parking lot. Data exfiltration is the unauthorized transfer of data from an organization to a location controlled by an attacker.

Additionally, attackers may be able to use the rogue access point to connect into the wired network. This works the same way that regular users can connect to a wired network via a wireless network. The difference is that the attacker configures all the security for the counterfeit access point and can use it for malicious purposes.

If you discover an unauthorized AP, you should disconnect it as quickly as possible. A basic first step to take when you discover any attack is to contain or isolate the threat. By simply unplugging the Ethernet cable, you can stop the unauthorized AP from capturing network traffic.

Evil Twin

An ***evil twin*** is a rogue access point with the same SSID as a legitimate access point. For example, many public places such as coffee shops, hotels, and airports include free Wi-Fi as a service. An attacker can set up an AP using the same SSID as the public Wi-Fi network, and many unsuspecting users will connect to this evil twin.

Once a user connects to an evil twin, wireless traffic goes through the evil twin instead of the legitimate AP. Often, the attacker presents bogus logon pages to users to capture usernames and passwords. Other times, they simply capture traffic from the connection, such as email or text typed into web page text boxes, and analyze it to detect sensitive information they can exploit.

Although it might sound complex to set up an evil twin, it's rather easy. Attackers can configure a laptop that has a wireless access card as an AP. With it running, the attackers look just like any other user in a coffee shop or airport waiting area. They'll have their laptop open and appear to be working (just like you perhaps), and you'll have no idea they are trying to steal your

credentials or other personal data that you send over the Internet via the evil twin. Similarly, attackers can set one up in a parking lot or another location close to an organization and try to trick employees or visitors.

Often, administrators will use wireless scanners to perform site surveys. In addition to detecting noise on frequency bands, they can also detect rogue APs, including evil twins. The site survey can help them identify the physical location of access points because the signal will get stronger as the administrator gets closer.

Remember this

Rogue access points are often used to capture and exfiltrate data. An evil twin is a rogue access point using the same SSID as a legitimate access point. A secure AP blocks unauthorized users, but a rogue access point provides access to unauthorized users.

Jamming Attacks

Attackers can transmit noise or another radio signal on the same frequency used by a wireless network. This interferes with the wireless transmissions and can seriously degrade performance. This type of denial-of-service attack is commonly called ***jamming*** and it usually prevents all users from connecting to a wireless network. In some cases, users have intermittent connectivity because the interference causes them to lose their association with the AP and forces them to try to reconnect.

In some cases, you can increase the power levels of the AP to overcome the attack. Another method of overcoming the attack is to use different wireless channels. Each wireless standard has several channels you can use, and if one channel is too noisy, you can use another one. Although this is useful to overcome interference in home networks, it won't be as effective to combat an interference attack. If you switch channels, the attacker can also switch channels.

IV Attacks

A wireless initialization vector (IV) attack attempts to discover the pre-shared key from the IV. The IV is simply a number. Some wireless protocols use an IV by combining it with the pre-shared key to encrypt data-in-transit.

An ***IV attack*** is successful when an encryption system reuses the same IV. Unfortunately, WEP uses a relatively small 24-bit number for the IV. This small IV results in wireless networks reusing keys.

In many IV attacks, the attacker uses packet injection techniques to add additional packets into the data stream. The AP responds with more packets, increasing the probability that it will reuse a key. An IV attack using packet injection decreases the time it takes to crack a WEP key to a very short time, sometimes less than a minute. It's worth repeating that WEP has been deprecated and should not be used.

NFC Attacks

Near field communication (NFC) is a group of standards used on mobile devices that allow them to communicate with other mobile devices when they are close to them. For example, you can share pictures, contacts, and other data with friends. One person shares the data, and after placing the smartphones close to each other, the other person selects it to download.

During an ***NFC attack***, an attacker uses an NFC reader to capture data from another NFC device. One method is an eavesdropping attack. The NFC reader uses an antenna to boost its range, and intercepts the data transfer between two other devices.

A more advanced attack was discovered by security researchers in 2012. They designed Trojan malware and installed it on an Android-based smartphone. They used the Trojan to initiate a payment. The NFC reader was then able to capture the payment data and use it in a live payment transaction. Google quickly modified Google Wallet to prevent this type of attack.

Bluetooth Attacks

Bluetooth is a short-range wireless system used in personal area networks (PANs) and within networks. A PAN is a network of devices close to a single person. Bluetooth devices include smartphones, headsets, and computer devices.

The range of Bluetooth was originally designed for about three meters (about 10 feet), but the range is often farther, and ultimately extends beyond a person's personal space. Attackers have discovered methods of exploiting these networks. Some common attacks are bluejacking, bluesnarfing, and

bluebugging:

- ***Bluejacking*** is the practice of sending unsolicited messages to nearby Bluetooth devices. Bluejacking messages are typically text, but can also be images or sounds. Bluejacking is relatively harmless, but does cause some confusion when users start receiving messages.
- ***Bluesnarfing*** refers to the unauthorized access to, or theft of information from, a Bluetooth device. A bluesnarfing attack can access information, such as email, contact lists, calendars, and text messages. Attackers use tools such as hcitool and obexftp.
- Bluebugging is like bluesnarfing, but it goes a step further. In addition to gaining full access to the phone, the attacker installs a backdoor. The attacker can have the phone call the attacker at any time, allowing the attacker to listen in on conversations within a room. Attackers can also listen in on phone conversations, enable call forwarding, send messages, and more.

When Bluetooth devices are first configured, they are configured in Discovery mode. Bluetooth devices use MAC addresses, and in Discovery mode the Bluetooth device broadcasts its MAC address, allowing other devices to see it and connect to it. This is required when pairing Bluetooth devices.

In earlier versions of Bluetooth, this pairing process could happen any time a device is in Discovery mode. However, most software vendors have rewritten their software to prevent this. Today, users typically manually pair the device. If a user doesn't acknowledge an attempted pairing, it fails. As a result, Bluetooth attacks are rare today. However, if a device doesn't require a user to manually pair a device, it is still susceptible to these attacks.

Remember this

Bluejacking is the unauthorized sending of text messages to a nearby Bluetooth device. Bluesnarfing is the unauthorized access to, or theft of information from, a Bluetooth device. Ensuring devices cannot be paired without manual user intervention prevents these attacks.

Wireless Replay Attacks

In a ***replay attack***, an attacker captures data sent between two entities, modifies it, and then attempts to impersonate one of the parties by replaying the data. WPA2 using CCMP and AES is not vulnerable to replay attacks. However, WPA using TKIP is vulnerable to replay attacks.

WPA uses a sequence counter to number the packets and an access point will reject packets received out of order. Additionally, TKIP uses a 64-bit Message Integrity Check (MIC) to verify the integrity of the packets. While this sounds secure, security experts identified a method to discover the MIC key. After discovering the key, an attacker can transmit and decrypt packets. Later, other security experts improved this attack allowing them to launch a replay attack. This is one of the reasons that TKIP was deprecated in 2012 and should not be used.

RFID Attacks

Radio-frequency identification (RFID) systems include an RFID reader and RFID tags placed on objects. They are used to track and manage inventory, and any type of valuable assets, including objects and animals.

There's an almost endless assortment of tags available for multiple purposes. This includes tags implanted into animals, packaging for any type of product (such as computers), pharmaceuticals, transportation systems (such as shipping containers, railcars, and busses), and controlled substances (such as pharmaceutical containers). Some tags are only slightly larger than a grain of rice.

Tags do not have a power source. Instead, they include electronics that allow them to collect and use power to transmit data stored on the device. This is similar to how a proximity card (described in Chapter 9, "Implementing Controls to Protect Assets") receives a charge from a proximity card reader and then transmits data to the reader. One difference is that RFID transmitters can transmit to and from tags from a much greater distance than proximity readers.

Some of the common ***RFID attacks*** are:

- **Sniffing or eavesdropping.** Because RFID transmits data over the air, it's possible for an attacker to collect it by listening. A key requirement is to know the frequency used by the RFID system and have a receiver that can be tuned to that frequency. The attacker also needs to know the protocols used by the RFID system to interpret the

data.

- **Replay.** Successful eavesdropping attacks allow the attacker to perform a replay attack. For example, an attacker can configure a bogus tag to mimic the tag attached to a valuable object. The attacker can then steal the valuable object without the theft being easily detected.
- **DoS.** A denial-of-service (DoS) attack attempts to disrupt services. If an attacker knows the frequency used by the RFID system, it's possible to launch a jamming or interference attack, flooding the frequency with noise. This prevents the RFID system from operating normally.

Remember this

WPA2 using CCMP and AES prevents wireless replay attacks. TKIP is vulnerable and should not be used. Radio-frequency identification (RFID) attacks include eavesdropping, replay, and DoS.

Misconfigured Access Points

One of the primary reasons that wireless attacks are successful is because APs are misconfigured. For example, if an AP is not using WPA2 with AES and CCMP, it is susceptible to many attacks. Similarly, if WPS is enabled on an AP, a WPS attack can discover the PIN in a few hours simply by guessing. After it discovers the PIN, it can discover the passphrase.

The Configuring a Wireless Router Lab shows how to configure several security settings on a wireless router. Although your wireless router might be a little different, you'll still be able to see many of the typical configuration settings. You can access this lab and other online exercises for this book at *http://gcgapremium.com/501labs/.*

Using VPNs for Remote Access

Chapter 3 covers several use cases for remote access, including the use of Secure Shell (SSH) and Remote Desktop Protocol (RDP). A virtual private network (***VPN***) is another method used for remote access. VPNs allow users to access private networks via a public network. The public

network is most commonly the Internet, but it can also be a semiprivate leased line from a telecommunications company. Because the telecommunications company will often lease access to one physical line to several companies, the leased line is not truly private.

Access over a public network is a core security concern with VPNs. Different tunneling protocols encapsulate and encrypt the traffic to protect the data from unauthorized disclosure. The tunnel prevents anyone from reading the data transferred through it.

VPNs and VPN Concentrators

It's possible to create a VPN by enabling services on a server. For example, if you have a Windows server, you can enable the Direct Access VPN role and configure the Routing and Remote Access console. The only additional hardware requirement is that the server has two network interface cards (NICs). One NIC is accessible from the Internet, and the second NIC provides access to the private network. If you are only supporting a few VPN clients, this might be the perfect solution.

Larger organizations often use a VPN concentrator, which is a dedicated device used for VPNs. A VPN concentrator includes all the services needed to create a VPN, including strong encryption and authentication techniques, and it supports many clients.

When using a VPN concentrator, you would typically place it in the DMZ. The firewall between the Internet and the DMZ would forward VPN traffic to the VPN concentrator. The concentrator would route all private VPN traffic to the firewall between the DMZ and the intranet.

Remember this

A virtual private network (VPN) provides remote access to a private network via a public network. VPN concentrators are dedicated devices used for VPNS. They include all the services needed to create a secure VPN supporting many clients.

Remote Access VPN

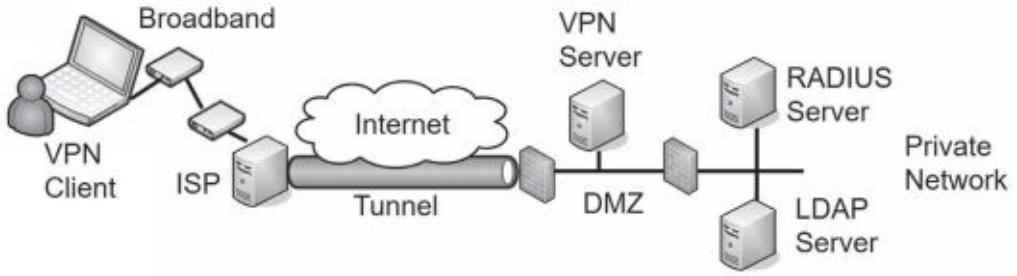


Figure 4.7 shows an example of how users can connect to internal networks from remote locations. The VPN client first connects to the Internet using a broadband connection to an Internet Service Provider (ISP). After connecting to the Internet, the VPN client can then initiate the VPN connection.

Figure 4.7: Connecting to a VPN server

The VPN server is in the DMZ and reachable through a public IP address. This makes it accessible from any other host on the Internet. A VPN server needs to authenticate clients. A common method is to use an internal Remote Authentication Dial-in User Service (RADIUS) server. When a user logs on, the VPN server sends the user's credentials to the RADIUS server.

While the RADIUS server might have a database of users and passwords, it's more common for it to pass the credentials on to another server to validate them. For example, the RADIUS server can pass the credentials on to a Lightweight Directory Access Protocol (LDAP) server during the authentication process. In a Microsoft domain, the LDAP server is a domain controller.

IPsec as a Tunneling Protocol

Chapter 3 introduces Internet Protocol security (***IPsec***) as a method of encrypting data-in- transit. IPsec supports both Tunnel mode and Transport mode.

Tunnel mode encrypts the entire IP packet used in the internal network, and is the mode used with VPNs transmitted over the Internet. The benefit is that the IP addressing used within the internal network is encrypted and not visible to anyone who intercepts the traffic. If someone does intercept the traffic, he can see the source IP address from the client and the destination address to the VPN server, but the internal IP address information remains hidden.

Transport mode only encrypts the payload and is commonly used in private networks, but not with VPNs. If traffic is transmitted and used only

within a private network, there isn't any need to hide the IP addresses by encrypting them.

IPsec provides security in two ways:

- **Authentication.** IPsec includes an Authentication Header (***AH***) to allow each of the hosts in the IPsec conversation to authenticate with each other before exchanging data. AH provides authentication and integrity. AH uses protocol number 51.
- **Encryption.** IPsec includes Encapsulating Security Payload (***ESP***) to encrypt the data and provide confidentiality. ESP includes AH so it provides confidentiality, authentication, and integrity. ESP uses protocol number 50.

The term protocol number might look like a typo, but it isn't. AH and ESP are identified with protocol numbers, not port numbers. Chapter 3 discusses routers and firewalls. You may remember from Chapter 3 that a basic packet-filtering firewall can filter packets based on IP addresses, ports, and some protocols, such as Internet Control Message Protocol (ICMP) and IPsec. Packet filters use the protocol numbers to identify AH and ESP traffic.

IPsec uses Internet Key Exchange (IKE) over port 500 to authenticate clients in the IPsec conversation. IKE creates security associations (SAs) for the VPN and uses these to set up a secure channel between the client and the VPN server.

TLS as a Tunneling Protocol

Some tunneling protocols use Transport Layer Security (TLS) to secure the VPN channel. As an example, Secure Socket Tunneling Protocol (SSTP) encrypts VPN traffic using TLS over port 443. Using port 443 provides a lot of flexibility for many administrators and rarely requires opening additional firewall ports. It is a useful alternative when the VPN tunnel must go through a device using NAT, and IPsec is not feasible. OpenVPN and OpenConnect are two open source applications that can use TLS to create a secure channel. While this can also use Secure Sockets Layer (SSL), SSL has known weaknesses and TLS is the designated replacement.

Split Tunnel Versus Full Tunnel

Imagine that Lisa connects to a company VPN server using IPsec from her home computer. The VPN is using ESP so all traffic in the tunnel is

encrypted. Now, Lisa wants to do an Internet search on saxophones. Will her computer connect directly to the Internet for her search? Or will her computer make a connection through the VPN server first? It depends on how the VPN is configured.

In a ***split tunnel***, a VPN administrator determines what traffic should use the encrypted tunnel. For example, it's possible to configure the tunnel to only encrypt traffic going to private IP addresses used within the private network. If Lisa did an Internet search with the VPN server configured in a split tunnel configuration, her Internet search traffic will not go through the encrypted tunnel. Instead, her search will go directly to Internet sites via her ISP.

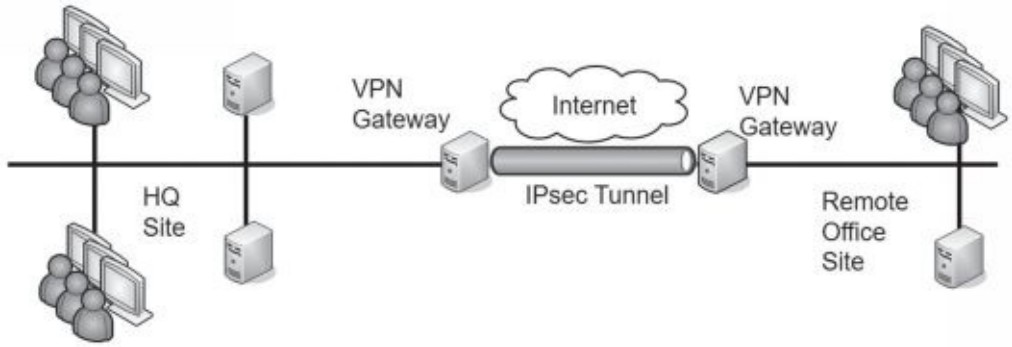
In a ***full tunnel***, all traffic goes through the encrypted tunnel while the user is connected to the VPN. If Lisa was connected to the VPN and then tried to connect to a public web site, the traffic would first go through the encrypted tunnel and then out to the public web site from within the private network. If the private network routed Internet traffic through a unified threat management (***UTM***) device, Lisa's traffic would go through the UTM device. The web site would send web pages back to the UTM device and the VPN server would encrypt it and send it back to Lisa via the encrypted tunnel.

Chapter 3 discusses UTM devices. As a reminder, a UTM device can perform URL filtering, malware inspection, and content inspection of all traffic sent through it. This is one of the reasons why an organization may choose to use a full tunnel for users connected to a VPN server. A disadvantage is that it can be slow. Not only is the Internet traffic taking an indirect route through the VPN server, but it's also being encrypted and decrypted a couple of times.

Remember this

IPsec is a secure encryption protocol used with VPNs. Encapsulating Security Payload (ESP) provides confidentiality, integrity, and authentication for VPN traffic. IPsec uses Tunnel mode for VPN traffic and can be identified with protocol ID 50 for ESP. It uses IKE over port 500. A full tunnel encrypts all traffic after a user has connected to a VPN. A split tunnel only encrypts traffic destined for the VPN's private network.

Site-to-Site VPNs



A site-to-site VPN includes two VPN servers that act as gateways for two networks separated geographically. For example, an organization can have two locations. One is its headquarters and the other is a remote office. It can use two VPN servers to act as gateways to connect the networks at the two locations together, as shown in Figure 4.8.

Figure 4.8: Site-to-site VPN

A benefit of the site-to-site model is that it connects both networks without requiring additional steps on the part of the user. Users in the remote office can connect to servers in the headquarters location as easily as if the servers were in the remote office. Connecting to the remote server might be slower than connecting to a local server, but, otherwise, it's transparent to end users.

In contrast, in a traditional remote access VPN (also called a host-to-gateway model), the end user makes the direct connection to the VPN server and is very much aware of the process.

Always-On VPN

Some VPNs are always-on VPNs. They can be used with both site-to-site VPNs and remote access VPNs. When used with a site-to-site VPN, the two VPN gateways maintain the VPN connection. In contrast, some site-to-site VPNs use an on-demand connection. The VPN connection is only established when a user connects to a remote system.

Several vendors have always-on VPNs for remote access VPNs. They attempt to create the VPN connection as soon as the user's device connects to the Internet. For a home user, this might be right after the user turns on a desktop PC or laptop computer.

When configured on mobile devices, such as cell phones, the device will connect to the always-on VPN anytime the device connects to an Internet connection. As an example, if a user visits a coffee shop that has free Internet access and the user connects to the network, the device will automatically connect to the always-on VPN.

Network Access Control

Allowing remote access to your private network can expose your network to a significant number of risks from the clients. If a user logs on to a VPN with a malware-infected computer, this computer can then infect other computers on the internal network. Network access control (***NAC***) methods provide continuous security monitoring by inspecting computers and preventing them from accessing the network if they don't pass the inspection.

Most administrators have complete control over computers in their network. For example, they can ensure the clients have up-to-date antivirus software installed, operating systems have current patches applied, and their firewalls are enabled. However, administrators don't have complete control of computers employees use at home or on the road.

NAC provides a measure of control for these other computers. It ensures that clients meet predetermined characteristics prior to accessing a network. NAC systems often use *health* as a metaphor, indicating that a client meets these predetermined characteristics. Just as doctors can quarantine patients with certain illnesses, NAC can quarantine or isolate unhealthy clients that don't meet the predefined NAC conditions.

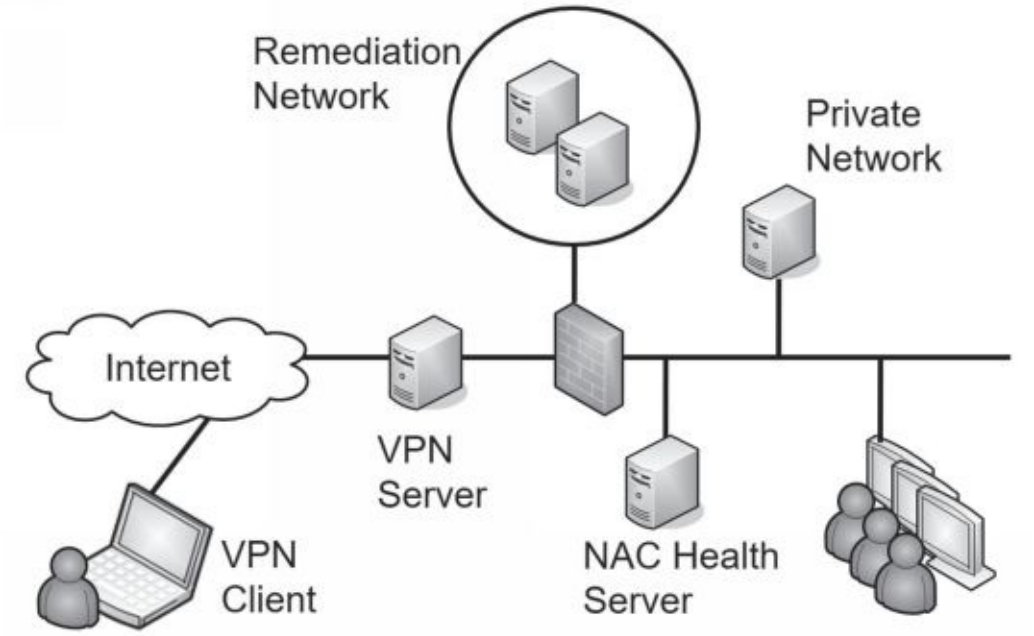
Host Health Checks

Administrators set predefined conditions for healthy clients and those that meet these preset conditions can access the network. The NAC system isolates computers that don't meet the conditions. Common health conditions checked by a NAC are:

- Up-to-date antivirus software, including updated signature definitions
- Up-to-date operating system, including current patches and fixes
- Firewall enabled on the client

NAC systems use authentication agents (sometimes called health agents) to inspect NAC clients. These agents are applications or services that check different conditions on the computer and document the status in a

statement of health. When a client connects to a NAC-controlled network, the agent reports the health status of the NAC client.



Consider Figure 4.9. When a VPN client accesses the network, the VPN server queries the NAC health server to determine required health conditions. The VPN server also queries the client for a statement of the client's health. If the client meets all health requirements, the NAC system allows the client to access the network.

Figure 4.9: Using network access control

However, if a client doesn't meet the health conditions mandated by the NAC server, the VPN server redirects the client to a remediation network (also called a quarantine network). The remediation network includes resources the client can use to get healthy. For example, it would include current approved patches, antivirus software, and updated virus signatures. The client can use these resources to improve its health and then try to access the network again.

While NAC can inspect the health of VPN clients, you can also use it to inspect the health of internal clients. For example, internal computers may occasionally miss patches and be vulnerable. NAC will detect the unpatched system and quarantine it. If you use this feature, it's important that the detection is accurate. A false positive by the NAC system can quarantine a healthy client, and prevent it from accessing the network.

Similarly, your organization may allow visitors or employees to plug in

their mobile computers to live wall jacks for connectivity, or connect to a wireless network. NAC inspects the clients, and if they don't meet health conditions, they may be granted Internet access through the network but remain isolated from any other network activity.

Permanent Versus Dissolvable

Agents on clients can be either dissolvable or permanent. A ***permanent agent*** (sometimes called a persistent NAC agent) is installed on the client and stays on the client. NAC uses the agent when the client attempts to log on remotely. This is the most common implementation for corporate-owned devices, and for approved laptops and PCs that employees use to connect remotely.

A ***dissolvable agent*** is downloaded and run on the client when the client logs on remotely. It collects the information it needs, identifies the client as healthy or not healthy, and reports the status back to the NAC system. Some dissolvable NAC agents remove themselves immediately after they report back to the NAC system. Others remove themselves after the remote session ends.

Dissolvableagentsareoftenusedonmobiledeviceswhenanorganizationhasi a bring your own device (BYOD) policy. Employee-owned devices are inspected for health, but the organization doesn't require users to install extra software on their devices. However, these dissolvable agents can detect vulnerabilities on mobile devices, such as a jail-broken or rooted device. A jail-broken Apple device removes software restrictions, such as the ability to install software from sources other than the Apple store. A rooted Android device has been modified, allowing root-level access to, and the ability to modify, the Android operating system.

Many NAC vendors refer to dissolvable agents as an agentless capability, though this is somewhat of a misnomer. The NAC is still using an agent to inspect the client, but it is not installing the agent on the client.

Remember this

Network access control (NAC) includes methods to inspect clients for health, such as having up-to-date antivirus software. NAC can restrict access of unhealthy clients to a remediation network. You can use NAC for VPN clients and for internal clients. Permanent

agents are installed on the clients. Dissolvable agents (sometimes called agentless) are not installed on the clients and are often used to inspect employee-owned mobile devices.

Identity and Access Services

An important step when implementing a VPN is to ensure only authorized entities can access it. Authorization begins with authentication, and VPNs support multiple methods of authentication. The following sections describe the different remote access authentication mechanisms in more depth, but here's a quick introduction:

- **Password Authentication Protocol (PAP).** PAP sends passwords in cleartext so PAP is used only as a last resort.
- **Challenge Handshake Authentication Protocol (CHAP).** CHAP uses a handshake process where the server challenges the client. The client then responds with appropriate authentication information.
- **Microsoft CHAP (MS-CHAP).** This is the Microsoft implementation of CHAP, which is used only by Microsoft clients.
- **MS-CHAPv2.** MS-CHAP is deprecated in favor of MS-CHAPv2. It includes several improvements, including the ability to perform mutual authentication.
- **Remote Authentication Dial-In User Service (RADIUS).** RADIUS provides a centralized method of authentication for multiple remote access servers. RADIUS encrypts the password packets, but not the entire authentication process.
- **Diameter.** Diameter was created to overcome some of the limitations of RADIUS and is often used instead of RADIUS.
- **Terminal Access Controller Access-Control System Plus (TACACS+).** TACACS+ is an alternative to RADIUS, but it is proprietary to Cisco systems. A benefit of TACACS+ is that it can interact with Kerberos, allowing it to work with a broader range of environments, including Microsoft domains using Kerberos. Additionally, TACACS+ encrypts the entire authentication process, whereas RADIUS encrypts only the password.

PAP

Password Authentication Protocol (***PAP***) is used with Point-to-Point Protocol (PPP) to authenticate clients. A significant weakness of PAP is that it sends passwords over a network in cleartext, representing a significant security risk.

PPP was primarily used with dial-up connections. Believe it or not, there was a time when the thought of someone wiretapping a phone was rather remote. Because of this, security was an afterthought with PPP. Today, PPP is only used as a last resort due to passwords being passed in cleartext, or it is used with another protocol that provides encryption.

CHAP

Challenge Handshake Authentication Protocol (***CHAP***) also uses PPP and authenticates remote users, but it is more secure than PAP. The goal of CHAP is to allow the client to pass credentials over a public network (such as a phone or the Internet) without allowing attackers to intercept the data and later use it in an attack.

The client and server both know a shared secret (similar to a password) used in the authentication process. However, the client doesn't send the shared secret over the network in plaintext as PAP does. Instead, the client hashes it after combining it with a nonce (number used once) provided by the server. This handshake process is used when the client initially tries to connect to the server, and at different times during the connection.

Remember this

PAP authentication uses a password or a PIN. A significant weakness is that PAP sends the information across a network in cleartext, making it susceptible to sniffing attacks. CHAP is more secure than PAP because passwords are not sent over the network in cleartext.

MS-CHAP and MS-CHAPv2

Microsoft introduced Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) as an improvement over CHAP for Microsoft clients. MS-CHAP supported clients as old as Windows 95. Later, Microsoft improved MS-CHAP with MS-CHAPv2.

A significant improvement of ***MS-CHAPv2*** over MS-CHAP is the

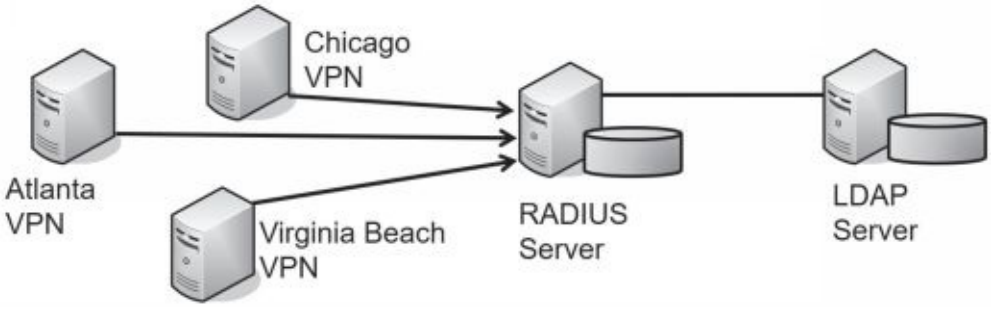
ability to perform mutual authentication. Not only does the client authenticate to the server, but the server also authenticates to the client. Chapter 7, “Protecting Against Advanced Attacks,” covers different types of attacks, including attacks in which an attacker may try to impersonate a server. Mutual authentication provides assurances of the server’s identity before the client transmits data, which reduces the risk of a client sending sensitive data to a rogue server.

RADIUS

Remote Authentication Dial-In User Service (***RADIUS***) is a centralized authentication service. Instead of each individual VPN server needing a separate database to identify who can authenticate, the VPN servers forward the authentication requests to a central RADIUS server. RADIUS can also be used as an 802.1x server with WPA2 Enterprise mode (described earlier in this chapter).

Imagine your company has locations in Virginia Beach, Atlanta, and Chicago. Each location has a VPN server that users can access. Bart is a traveling salesman, and he can connect to any of these VPN servers. When entering sales data, he connects to the Atlanta VPN. When using the company-sponsored always-on VPN for his mobile devices, he connects to the Virginia Beach VPN server. Bart has one account for all company access and today he was prompted to change his password.

If each VPN server has a separate database with Bart’s username and password, each of these databases must be updated. This can be labor intensive and result in needless errors.



However, the company could use a centralized RADIUS server, as shown in Figure 4.10, instead. Each VPN server is configured with a shared secret (similar to a password) and the RADIUS server is configured with a matching shared secret for each of the VPN servers.

Figure 4.10: RADIUS configuration

This centralized RADIUS server could hold a centralized database of user accounts. However, it is more common for the RADIUS server to access an LDAP server that holds the accounts. For example, in a Microsoft domain, the RADIUS server would pass the credentials to a domain controller. A significant benefit is that there is only one account for the user. If Bart changes his password, the domain controller knows the new password.

RADIUS uses the User Datagram Protocol (UDP), which provides a best-effort delivery mechanism. As a result, RADIUS includes logic to detect communication problems. In contrast, RADIUS alternatives use TCP, which provides guaranteed delivery. These alternatives allow TCP to detect and handle communication issues. Also, RADIUS only encrypts the password, while alternatives encrypt the entire authentication process.

Even though RADIUS was created before Extensible Authentication Protocol (EAP) was developed, RADIUS does work with EAP. RFC 3579 “RADIUS Support for EAP” is an informational RFC and describes how to do so. However, alternatives make it easier to extend the use of EAP.

TACACS+

Terminal Access Controller Access-Control System Plus (***TACACS+***) is the Cisco alternative to RADIUS. It provides two important security benefits over RADIUS. First, it encrypts the entire authentication process, whereas RADIUS encrypts only the password. Second, TACACS+ uses multiple challenges and responses between the client and the server.

Although TACACS+ is proprietary to Cisco, it can interact with Kerberos. This allows a Cisco VPN concentrator to interact in a Microsoft Active Directory environment. As a reminder, Microsoft Active Directory uses Kerberos for authentication.

Organizations also use TACACS+ as an authentication service for network devices. In other words, you can use it to authenticate users before they are able to access a configuration page for a router or a switch. The network devices must be TACACS+ enabled, and a TACACS+ server provides the authentication services.

Diameter

Diameter is an extension of RADIUS and many organizations have switched to it due to its extra capabilities. Diameter adds several other commands beyond the capabilities of RADIUS, along with adding new commands that can be used with EAP. Diameter uses TCP instead of UDP used by RADIUS. A key benefit is that it is backwards compatible with RADIUS and provides an upgrade path from RADIUS to Diameter.

In geometry, the diameter of a circle is a straight line between the two edges of a circle, whereas the radius is a straight line from the center to an edge. In other words, the diameter of a circle is twice as long as the radius. The designers considered this when naming Diameter to indicate indirectly that it is twice as good as RADIUS.

Remember this

RADIUS, TACACS+, and Diameter all provide centralized authentication. TACACS+ is proprietary to Cisco, but can be used with Kerberos. Diameter is an improvement over RADIUS, and it supports many additional capabilities, including securing transmissions with EAP.

AAA Protocols

AAA protocols provide authentication, authorization, and accounting. Authentication verifies a user's identification. Authorization determines if a user should have access. Accounting tracks user access with logs.

As an example, RADIUS, TACACS+, and Diameter are considered AAA protocols because they provide all three services. They authenticate users who attempt remote access, determine if the user is authorized for remote access by checking a database, and then record the user's activity. TACACS+ uses multiple challenges and responses during a session. Kerberos is sometimes referred to as an AAA protocol, but it does not provide any accounting services.

Chapter 4 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Exploring Advanced Security Devices

- Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) inspect traffic using the same functionality as a protocol analyzer.
- A host-based IDS (HIDS) can detect attacks on local systems such as workstations and servers. The HIDS protects local resources on the host and can detect some malware that isn't detected by traditional antivirus software. A network-based IDS (NIDS) detects attacks on networks.
- A signature-based IDS or IPS uses signatures to detect known attacks or vulnerabilities.
- Heuristic-based or behavioral-based IDSs (also called anomaly-based IDSs) require a baseline and detect attacks based on anomalies or when traffic is outside expected boundaries.
- A false positive incorrectly raises an alert indicating an attack when an attack is not active. False positives increase the workload of administrators. A false negative is when an attack is active, but not reported.
- An IPS is similar to an active IDS except that it's placed inline with the traffic (sometimes called in-band) and can stop attacks before they reach the internal network. An IPS can actively monitor data streams, detect malicious content, and prevent it from reaching a network. In contrast, an IDS is out-of-band.
- IDSs and IPSs can also protect internal private networks, such as private supervisory control and data acquisition (SCADA) networks.
- SSL/TLS accelerators are dedicated hardware devices that handle Transport Layer Security (TLS) traffic. Other devices, such as a web server, can off-load TLS traffic handling to the accelerator.
- SSL decryptors allow an organization to inspect traffic, even when

traffic is using SSL or TLS.

- A software defined network (SDN) uses virtualization technologies to route traffic instead of using hardware routers and switches. It separates the data and control planes.
- Honeypots and honeynets appear to have valuable data and attempt to divert attackers away from live networks. Security personnel use them to observe current attack methodologies and gather intelligence on attacks.
- An 802.1x server provides strong port security using port-based authentication. It prevents rogue devices from connecting to a network by ensuring that only authorized clients can connect.

Securing Wireless Networks

- Wireless access points (APs) connect wireless clients to a wired network.
- A fat AP, also known as a stand-alone AP, includes everything needed to connect wireless clients to a wireless network.
- Thin APs are controller-based APs. A controller configures and manages a thin AP.
- The service set identifier (SSID) is the name of the wireless network. Disabling the SSID broadcast hides a wireless network from casual users.
- You can restrict access to wireless networks with media access control (MAC) filtering. However, attackers can discover authorized MACs and spoof an authorized MAC address.
- Most WAPs have omnidirectional antennas. Directional antennas have narrower beams and longer ranges.
- An ad hoc wireless network is two or more devices connected together without an AP.
- Wi-Fi Protected Access (WPA) can use Temporal Key Integrity Protocol (TKIP) or Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Both WPA and TKIP have been deprecated.
- Personal mode uses a pre-shared key (PSK). It is easy to implement and is used in many smaller wireless networks.

- Enterprise mode is more secure than Personal mode because it adds authentication. It uses an 802.1x authentication server implemented as a RADIUS server.
- Open mode doesn't use a PSK or an 802.1x server. Many hot spots use Open mode when providing free wireless access to customers.
- 802.1x servers use one of the Extensible Authentication Protocol (EAP) versions, such as Protected EAP (PEAP), EAP-Tunneled TLS (EAP-TTLS), EAP-TLS, or EAP-Flexible Authentication via Secure Tunneling (EAP-FAST).
- The most secure EAP method is EAP-TLS, and it requires a certificate on the server and on each of the wireless clients. PEAP and EAP-TTLS require a certificate on the server, but not the client. PEAP is often implemented with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). LEAP is proprietary to Cisco and does not require a certificate. Cisco designed EAP-FAST to replace Lightweight EAP (LEAP).
- A captive portal forces wireless clients to complete a process, such as acknowledging a policy or paying for access, before it grants them access to the network.

Understanding Wireless Attacks

- A disassociation attack effectively removes a wireless client from a wireless network, forcing it to reauthenticate.
- Wi-Fi Protected Setup (WPS) allows users to easily configure a wireless device by pressing a button or entering a short PIN. WPS is not secure. A WPS attack can discover the PIN within hours. It then uses the PIN to discover the passphrase.
- A rogue access point (rogue AP) is an AP placed within a network without official authorization. An evil twin is a rogue access point with the same SSID as a legitimate access point.
- A jamming attack floods a wireless frequency with noise, blocking wireless traffic.
- An initialization vector (IV) attack attempts to discover the IV and uses it to discover the passphrase.
- Near field communication (NFC) attacks use an NFC reader to read data from mobile devices.
- Bluejacking is the practice of sending unsolicited messages to a

phone. Bluesnarfing is the unauthorized access to, or theft of information from, a Bluetooth device.

- In a wireless replay attack, an attacker captures data sent between two entities, modifies it, and then impersonates one of the parties by replaying the data. WPA2 using CCMP and AES prevents wireless replay attacks.
- Radio-frequency identification (RFID) attacks include eavesdropping, replay, and DoS.

Using VPNs for Remote Access

- A virtual private network (VPN) provides access to private networks via a public network, such as the Internet. VPN concentrators are dedicated devices that provide secure remote access to remote users.
- IPsec is a common tunneling protocol used with VPNs. It secures traffic within a tunnel. IPsec provides authentication with an Authentication Header (AH). Encapsulating Security Payload (ESP) encrypts VPN traffic and provides confidentiality, integrity, and authentication.
- IPsec Tunnel mode encrypts the entire IP packet used in the internal network. IPsec Transport mode only encrypts the payload and is commonly used in private networks, but not with VPNs.
- Some VPNs use TLS to encrypt traffic within the VPN tunnel.
- A full tunnel encrypts all traffic after a user has connected to a VPN. A split tunnel only encrypts traffic destined for the VPN's private network.
- Site-to-site VPNs provide secure access between two networks. These can be on- demand VPNs or always-on VPNs.
- Mobile devices can also use always-on VPNs to protect traffic when users connect to public hot spots.
- Network access control (NAC) inspects clients for specific health conditions such as up- to-date antivirus software, and can redirect unhealthy clients to a remediation network.
- A permanent NAC agent (sometimes called a persistent NAC agent) is installed on the client and stays on the client. A dissolvable NAC agent (sometimes called agentless) is downloaded and run on the

client when the client logs on, and deleted after the session ends. Dissolvable agents are commonly used for employee-owned mobile devices.

- Remote access authentication is used when a user accesses a private network from a remote location, such as with a VPN connection.
- Password Authentication Protocol (PAP) uses a password or PIN for authentication. A significant weakness is that PAP sends passwords across a network in cleartext.
- Challenge Handshake Authentication Protocol (CHAP) is more secure than PAP and uses a handshake process when authenticating clients.
- MS-CHAP and MS-CHAPv2 are the Microsoft improvement over CHAP. MS-CHAPv2 provides mutual authentication.
- RADIUS provides central authentication for multiple remote access services. RADIUS relies on the use of shared secrets and only encrypts the password during the authentication process. It uses UDP.
- TACACS+ is used by some Cisco systems as an alternative to RADIUS. TACACS+ uses TCP, encrypts the entire authentication process, and supports multiple challenges and responses.
- Diameter is an improvement over RADIUS. Diameter uses TCP, encrypts the entire authentication process, and supports many additional capabilities.
- RADIUS, TACACS+, and Diameter are all authentication, authorization, and accounting (AAA) protocols.

Online References

- Have you done any of the online labs at *http://gcgapremium.com/501-extras?* Online resources also include sample practice test questions, including performance-based questions.

Chapter 4 Practice Questions

1. You are preparing to deploy a heuristic-based detection system to monitor network activity. Which of the following would you create first?
   A. Flood guards
   B. Signatures
   C. Baseline
   D. Honeypot

2. Attackers have recently launched several attacks against servers in your organization's DMZ. You are tasked with identifying a solution that will have the best chance at preventing these attacks in the future. Which of the following is the BEST choice?
   A. An out-of-band IPS
   B. An in-band IPS
   C. A passive IDS
   D. An out-of-band IDS

3. Lisa oversees and monitors processes at a water treatment plant using SCADA systems. Administrators recently discovered malware on her system that was connecting to the SCADA systems. Although they removed the malware, management is still concerned. Lisa needs to continue using her system and it's not possible to update the SCADA systems. Which of the following can mitigate this risk?
   A. Install HIPS on the SCADA systems.
   B. Install a firewall on the border of the SCADA network.
   C. Install a NIPS on the border of the SCADA network.
   D. Install a honeypot on the SCADA network.

4. Which of the following BEST describes a false negative?
   A. An IDS falsely indicates a buffer overflow attack occurred.
   B. Antivirus software reports that a valid application is malware.
   C. A heuristic-based IDS detects a previously unknown attack.
   D. An IDS does not detect a buffer overflow attack.

5. Your wireless network includes one centralized AP that you configure. This AP forwards the configuration to other APs in your wireless network. Which of the following BEST describes these APs?
   A. The centralized AP is a stand-alone AP and it configures fat APs

in your network.

B. The centralized AP is a thin AP and it configures fat APs in your network.

C. The centralized AP is a controller-based AP and it configures stand-alone APs in your network.

D. The centralized AP is a fat AP and it configures thin APs in your network.

6. You need to provide connectivity between two buildings without running any cables. You decide to use two 802.11ac APs to provide wireless connectivity between the buildings. Which of the following is the BEST choice to support this need?

A. Use omnidirectional antennas on both APs.

B. Use wide channels.

C. Use the 2.4 GHz frequency band.

D. Use directional antennas on both APs.

7. You want to implement the STRONGEST level of security on a wireless network. Which of the following supports this goal?

A. Implementing WPA with TKIP

B. Disabling SSID broadcast

C. Enabling MAC filtering

D. Implementing WPA2 with CCMP

8. Your organization is planning to implement a wireless network using WPA2 Enterprise. Of the following choices, what is required?

A. An authentication server with a digital certificate installed on the authentication server

B. An authentication server with DHCP installed on the authentication server

C. An authentication server with DNS installed on the authentication server

D. An authentication server with WEP running on the access point

9. A security administrator is testing the security of an AP. The AP is using WPA2. She ran an automated program for several hours and discovered the AP's passphrase. Which of the following methods was she MOST likely using?

A. IV attack

B. Disassociation attack

C. WPS attack
D. Evil twin attack

10. Your wireless network name is myoffice. You disabled the SSID broadcast several days ago. Today, you notice that a wireless network named myoffice is available to wireless users. You verified that SSID broadcast is still disabled. Which of the following is the MOST likely reason for this behavior?

A. Evil twin attack
B. Disassociation attack
C. WPS attack
D. Jamming attack

11. Mobile users in your network report that they frequently lose connectivity with the wireless network on some days, but on other days they don't have any problems. You suspect this is due to an attack. Which of the following attacks is MOST likely causing this problem?

A. Wireless jamming
B. IV
C. Replay
D. Bluesnarfing

12. Management within your organization wants some users to be able to access internal network resources from remote locations. Which of the following is the BEST choice to meet this need?

A. NAC
B. VPN
C. IDS
D. IPS

13. Your organization is planning to implement a VPN. They want to ensure that after a VPN client connects to the VPN server, all traffic from the VPN client is encrypted. Which of the following would BEST meet this goal?

A. Split tunnel
B. Full tunnel
C. IPsec using Tunnel mode
D. IPsec using Transport mode

14. You are tasked with configuring authentication services settings on computers in your network. You are entering shared secrets on different

servers. Which of the following services are you MOST likely configuring? (Select TWO.)

A. RADIUS
B. Kerberos
C. LDAP
D. EAP-TLS

15. Your organization recently implemented a BYOD policy. However, management wants to ensure that mobile devices meet minimum standards for security before they can access any network resources. Which of the following agents would the NAC MOST likely have?

A. Permanent
B. Health
C. RADIUS
D. Dissolvable

Chapter 4 Practice Question Answers

1. **C.** A heuristic-based (also called anomaly-based or behavior-based) detection system compares current activity with a previously created baseline to detect any anomalies or changes. Flood guards help protect against flood attacks (such as a SYN flood attack). Signature-based systems (also called definition-based) use signatures of known attack patterns to detect attacks. A honeypot is a server designed to look valuable to an attacker and can divert attacks.

2. **B.** The best solution of the given choices is an in-band intrusion prevention system (IPS). Traffic goes through the IPS and the IPS has the best chance of preventing attacks from reaching internal systems. An IPS is in-band not out-of-band. An intrusion detection system (IDS) is passive and not in-band, so it can only detect and react to the attacks, not block them.

3. **C.** A network intrusion prevention system (NIPS) installed on the supervisory control and data acquisition (SCADA) network can intercept malicious traffic coming into the network and is the best choice of those given. The scenario states you cannot update the SCADA systems, so you cannot install a host-based IPS (HIPS) on any of them. A firewall provides a level of protection. However, it wouldn't

be able to differentiate between valid traffic sent by Lisa and malicious traffic sent by malware from Lisa's system. A honeypot might be useful to observe malicious traffic, but wouldn't prevent it.

4. **D.** If an intrusion detection system (IDS) does not detect and report a buffer overflow attack, it is a false negative. It is a false positive if the IDS falsely (incorrectly) indicates an attack occurred. If antivirus software indicates a valid application is malware, it is also a false positive. If a heuristic-based IDS accurately detects a previously unknown attack, it is working correctly.

5. **D.** The centralized access point (AP) is a fat AP and it configures thin APs in the network. The fat AP could also be called a stand-alone, intelligent, or autonomous AP and it is used to configure thin APs, not fat APs. Thin APs do not configure other APs. Stand-alone APs are not configured by other APs.

6. **D.** Using directional antennas on both access points (APs) is the best choice to meet this need because they have high gain with a very narrow radiation pattern. Omnidirectional antennas transmit the signal in all directions at the same time and are not a good choice when connecting networks between two buildings. Wider channels reduce the range of wireless transmissions and aren't a good choice here. Because 802.11ac uses only the 5 GHz frequency band, you can't use 2.4 GHz.

7. **D.** Wi-Fi Protected Access II (WPA2) with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) provides the strongest level of security of the given choices. Temporal Key Integrity Protocol (TKIP) is an older encryption protocol used with WPA and it isn't as strong as CCMP. Disabling service set identifier (SSID) broadcast hides the network from casual users, but attackers can still discover it because the SSID is still included in some packets in plaintext. Attackers can bypass media access control (MAC) address filtering by spoofing authorized MAC addresses.

8. **A.** WPA2 Enterprise requires an 802.1x authentication server and most implementations require a digital certificate installed on the server. The network will likely have Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) services, but it isn't necessary to install them on the authentication server. Wired Equivalent Privacy

(WEP) provides poor security and is not compatible with WPA2 Enterprise.

9. **C.** This is most likely a Wi-Fi Protected Setup (WPS) attack. Reaver is an automated program that will discover the WPS PIN and after it discovers the PIN, it can discover the passphrase or secret key used by the access point (AP). While an initialization vector (IV) attack can discover the passphrase in legacy wireless security protocols, Wi-Fi Protected Access II (WPA2) isn't susceptible to an IV attack. A disassociation attack effectively removes a wireless client from a wireless network, but it doesn't discover the passphrase. An evil twin attack uses a separate AP with the same name as an existing AP with the goal of tricking users into connecting to it.

10. **A.** The scenario indicates an evil twin attack is in progress. An attacker can easily discover the service set identifier (SSID) even with SSID broadcast disabled and can then create another access point with the same SSID. A disassociation attack disconnects wireless clients from the wireless network. A Wi-Fi Protected Setup (WPS) attack discovers the eight-digit PIN and then uses it to discover the passphrase. A jamming attack floods the frequency channel with noise to prevent connections.

11. **A.** A wireless jamming attack is a type of denial-of-service (DoS) attack that can cause wireless devices to lose their association with access points and disconnect them from the network. None of the other attacks are DoS attacks. An initialization vector (IV) attack attempts to discover the passphrase. A replay attack captures traffic with the goal of replaying it later to impersonate one of the parties in the original transmission. Bluesnarfing is a Bluetooth attack that attempts to access information on Bluetooth devices.

12. **B.** A virtual private network (VPN) provides access to a private network over a public network such as the Internet via remote locations and is the best choice. Network access control (NAC) methods can check VPN clients for health before allowing them access to the network, but it doesn't directly provide the access. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) protect networks, but do not control remote access.

13. **B.** A full tunnel encrypts all traffic after a user has connected to a VPN using a tunnel. A split tunnel only encrypts traffic destined for the VPN's private network. Traffic from the client directly to another Internet site is not encrypted. Internet Protocol security (IPsec) Tunnel mode encrypts the entire IP packet used in the internal network. It encrypts all traffic used within the VPN's private network, but not all traffic from the VPN client. IPsec Transport mode only encrypts the payload and is used within private networks, not for VPN traffic.

14. **A, C.** Remote Authentication Dial-in User Service (RADIUS) servers use shared secrets. You can configure them to interact with Lightweight Directory Access Protocol (LDAP)–based systems by entering the same shared secret on both a RADIUS server and an LDAP server. A shared secret is basically just an identical password on both systems. Kerberos uses tickets for authentication, not shared secrets. Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) is an authentication protocol that requires the use of certificates on both clients and servers, not shared secrets.

15. **D.** A dissolvable agent is often used on employee-owned devices and would be appropriate if an organization implemented a bring your own device (BYOD) policy. A permanent network access control (NAC) agent is installed on the device permanently, but this might cause problems for employee-owned devices. Any NAC agent is a health agent. Remote Authentication Dial-In User Service (RADIUS) is used for authentication, not to inspect clients.