CCNA Cyber Ops (Version 1.1) – Chapter 8: Protecting the Network

itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-8-protecting-the-network.html

June 13, 2019

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- How is the defense-in-depth strategy used to protect networks?
- What are common security policies, regulations, and standards?
- What are access control policies?
- How is AAA used to control network access?
- What information sources are used to communicate emerging network security threats?
- What threat intelligence is used to identify threats and vulnerabilities?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

asset
edge router
security onion
security artichoke
company policies
employee policies
security policies
acceptable use policy (AUP)
Bring Your Own Device (BYOD)
confidentiality
integrity
availability
mandatory access control (MAC)
discretionary access control (DAC)
non-discretionary access control
attribute-based access control (ABAC)
privilege escalation
Authentication, Authorization, and Accounting (AAA)

Introduction (8.0)

Protecting our networks will continue to be a challenge. Millions of new devices are joining our networks every year as the Internet of Things (IoT) continues to expand. In addition, with wireless capabilities those devices can be almost anywhere. Threat actors will continue to look for vulnerabilities that can be exploited.

We use a variety of methods to protect our networks, devices, and data. This chapter covers approaches to network security defense, access control methods, and the various sources cybersecurity analysts rely on for threat intelligence.

Understanding Defense (8.1)

In this section, you will learn about a variety of approaches to network securitydefense.

Defense-in-Depth (8.1.1)

In this topic, you will learn how the defense-in-depth strategy is used to protect networks.

Assets, Vulnerabilities, Threats (8.1.1.1)

Cybersecurity analysts must prepare for any type of attack. It is their job to secure the assets of the organization's network. To do this, cybersecurity analysts must first identify:

Asset: Anything of value to an organization that must be protected, including servers, infrastructure devices, end devices, and the greatest asset, data.
Vulnerability: A weakness in a system or its design that could be exploited by a threat.
Threat: Any potential danger to an asset.

Identify Assets (8.1.1.2)

As an organization grows, so do its assets. Consider the number of assets a large organization would have to protect. It may also acquire other assets through mergers with other companies. The result is that many organizations only have a general idea of the assets that need to be protected.

The collection of all the devices and information owned or managed by the organization are the assets. The assets constitute the attack surface that threat actors could target. These assets must be inventoried and assessed for the level of protection needed to thwart potential attacks.

Asset management consists of inventorying all assets, and then developing and implementing policies and procedures to protect them. This task can be daunting considering many organizations must protect internal users and resources, mobile workers, and cloud-based and virtual services.

Further, organizations need to identify where critical information assets are stored, and how access is gained to that information. Information assets vary, asdo the threats against them. For example, a retail business may store customer credit card information. An engineering firm will store competition-sensitive designs and software. A bank will store customer data, account information, and other sensitive financial information. Each of these assets can attract different threat actors who have different skill levels and motivations.

Identify Vulnerabilities (8.1.1.3)

Threat identification provides an organization with a list of likely threats for a particular environment. When identifying threats, it is important to ask several questions:

- What are the possible vulnerabilities of a system?
- Who may want to exploit those vulnerabilities to access specific information assets?
- What are the consequences if system vulnerabilities are exploited and assets are lost?

For example, as highlighted in Figure 8-1, threat identification for an e-banking system would include:

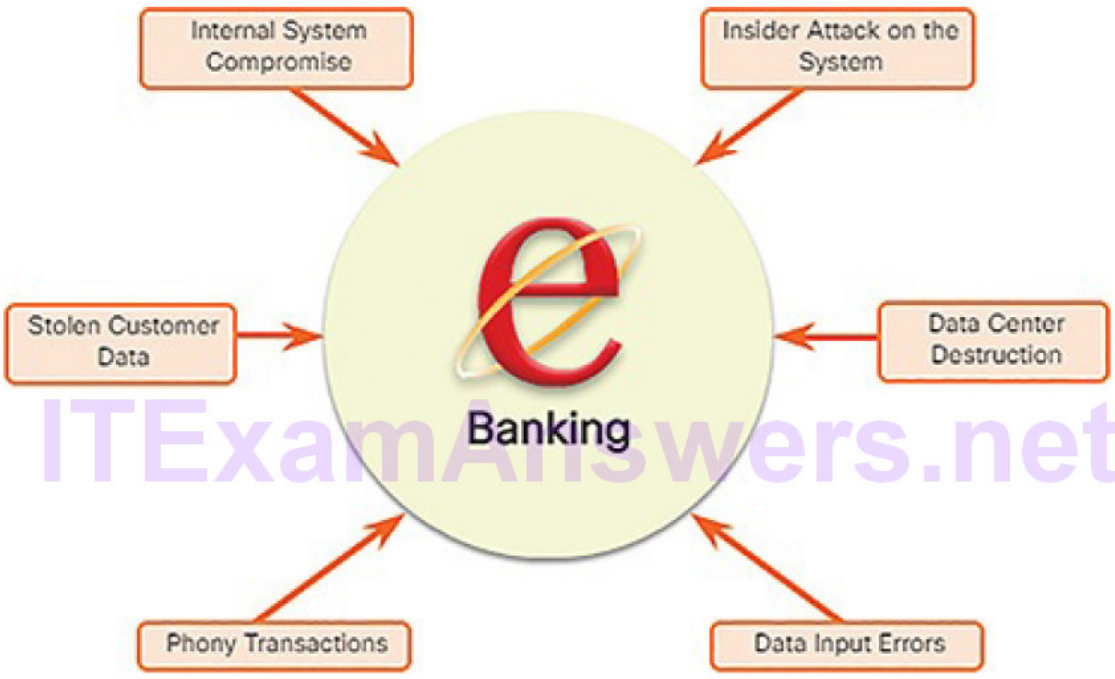

Figure 8-1 Identified Electronic Banking Threats

Internal system compromise: The attacker uses the exposed e-bankingservers to break into an internal bank system.

Stolen customer data: An attacker steals the personal and financial data of bank customers from the customer database.

Phony transactions from an external server: An attacker alters the code of the e-banking application and makes transactions by impersonating a legitimate user.

Phony transactions using a stolen customer PIN or smart card: An attacker steals the identity of a customer and completes malicious transactions from the compromised account.

Insider attack on the system: A bank employee finds a flaw in the system from which to mount an attack.

Data input errors: A user inputs incorrect data or makes incorrect transaction requests.

Data center destruction: A cataclysmic event severely damages or destroys the data center.

Identifying vulnerabilities on a network requires an understanding of the important applications that are used, as well as the different vulnerabilities of those applications and the network hardware. This can require a significant amount of research on the part of the network administrator.

Identify Threats (8.1.1.4)

Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets. This approach uses multiple layers of security at the network edge, within the network, and on network endpoints.

For example, Figure 8-2 displays a simple topology of a defense-in-depth approach:

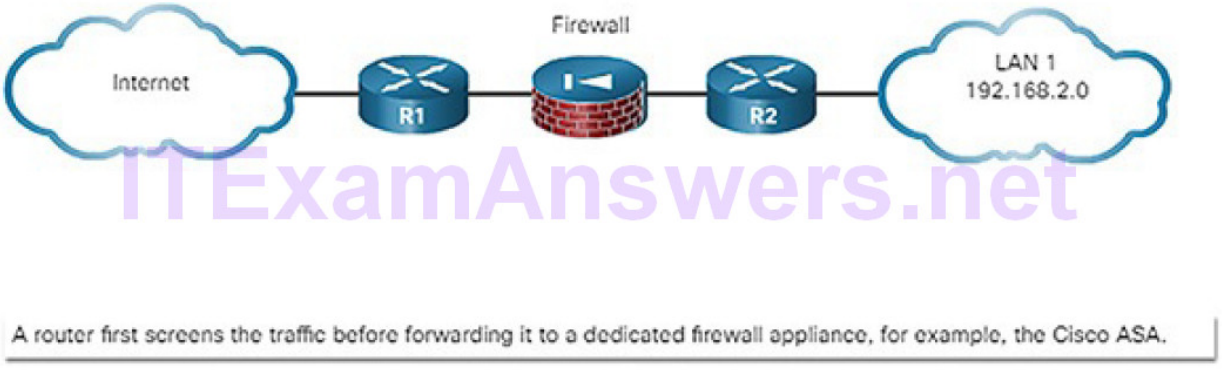

Figure 8-2 Defense-in-Depth Approach

Edge router: The first line of defense is known as an edge router (R1 in Figure 8-2). The edge router has a set of rules specifying which traffic it allows or denies. It passes all connections that are intended for the internal LAN to the firewall.

Firewall: A second line of defense is the firewall. The firewall is a checkpoint device that performs additional filtering and tracks the state of the connections. It denies the initiation of connections from the outside (untrusted) networks to the inside (trusted) network while enabling internal users to establish two-way connections to the untrusted networks. It can also perform user authentication (authentication proxy) to grant external remote users access to internal network resources.

Internal router: Another line of defense is the internal router (R2 in Figure 8-2). It can apply final filtering rules on the traffic before it is forwarded to its destination.

Routers and firewalls are not the only devices that are used in a defense-in-depth approach. Other security devices include intrusion prevention systems (IPSs), advanced malware protection (AMP), web and email content security systems, identity services, network access controls, and more.

In the layered defense-in-depth security approach, the different layers work together to create a security architecture in which the failure of one safeguard does not affect the effectiveness of the other safeguards.

Security Onion and Security Artichoke Approaches (8.1.1.5)

A common analogy used to describe a defense-in-depth approach is called the security onion. As illustrated in Figure 8-3, a threat actor would have to peel away at a network's defense mechanisms in a manner similar to peeling an onion.

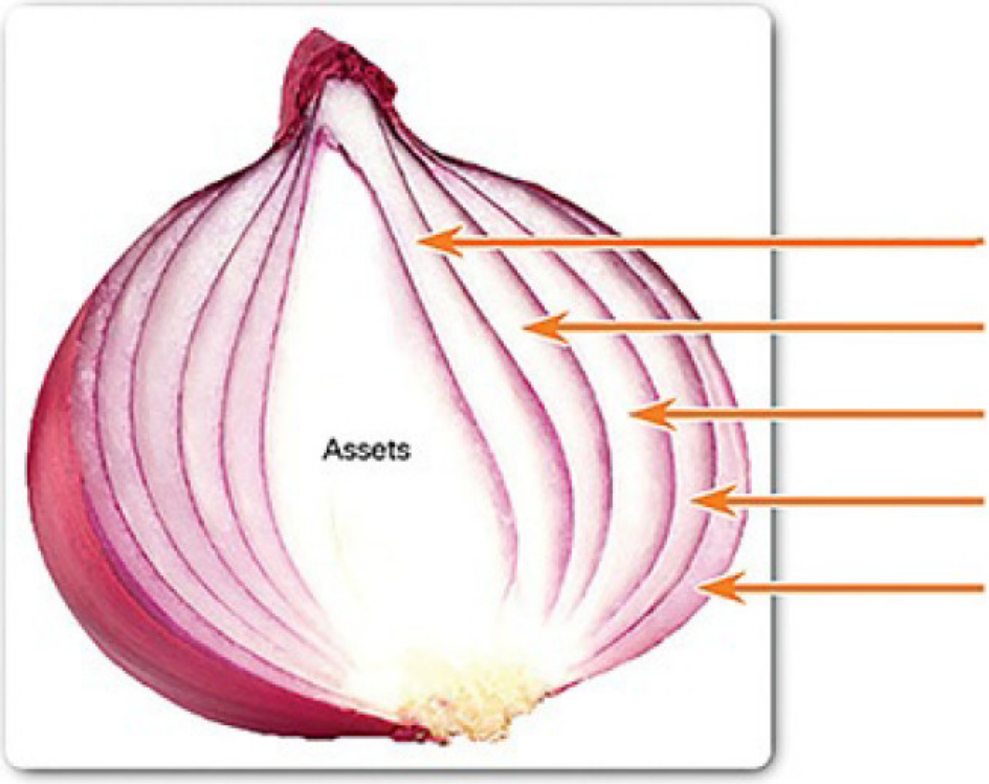

Figure 8-3 Security Onion Layers

However, the changing landscape of networking, such as the evolution of borderless networks, has changed this analogy to the security artichoke, which benefits the threat actor. As illustrated in Figure 8-4, threat actors no longer have to peel away each layer.

They only need to remove certain "artichoke leaves." The bonus is that each "leaf" of the network may reveal sensitive data that is not well secured. For example, it's easier for a threat actor to compromise a mobile device than it is to compromise an internal computer or server that is protected by layers of defense. Each mobile device is a leaf. And leaf after leaf, it all leads the hacker to more data. The heart of the artichoke is where the most confidential data is found. Each leaf provides a layer of protection while simultaneously providing a path to attack.

Not every leaf needs to be removed in order to get at the heart of the artichoke. The hacker chips away at the security armor along the perimeter to get to the "heart" of the enterprise.

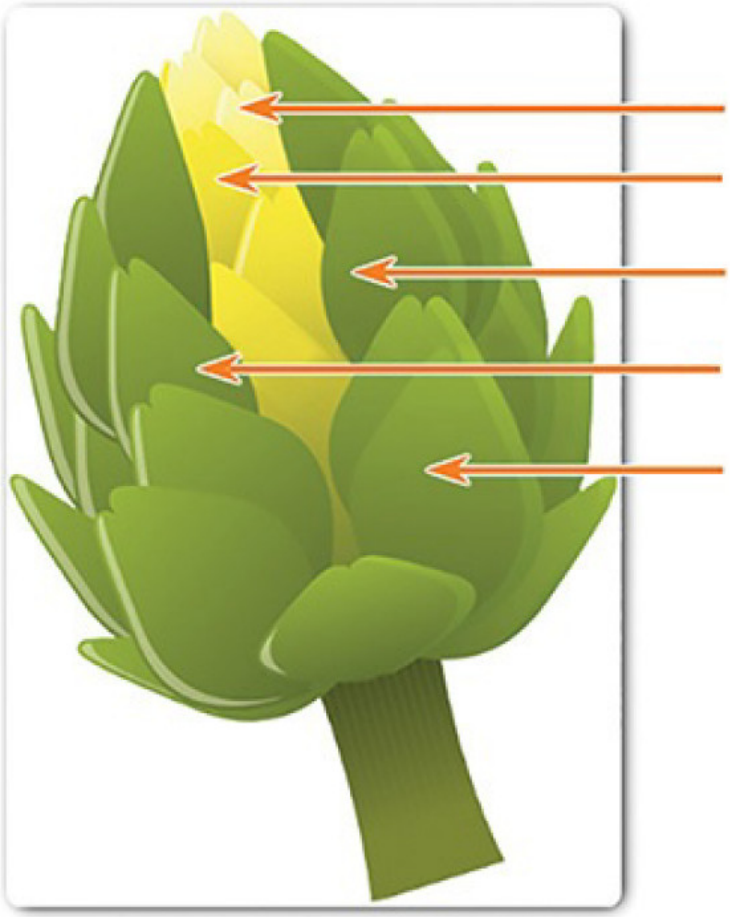

Figure 8-4 Security Artichoke Leaves

While Internet-facing systems are usually very well protected and boundary protections are typically solid, persistent hackers, aided by a mix of skill and luck, do eventually find a gap in that hard-core exterior through which they can enter and go where they please.

Note
The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.

Security Policies (8.1.2)

In this topic, you will learn about security policies, regulations, and standards.

Business Policies (8.1.2.1)

Business policies are the guidelines developed by an organization to govern its actions. The policies define standards of correct behavior for the business and its employees. In networking, policies define the activities that are allowed on the network. This sets a baseline of acceptable use. If behavior that violates business policy is detected on the network, it is possible that a security breach has occurred.

An organization may have several guiding policies:

Company policies: These policies establish the rules of conduct and the responsibilities of both employees and employers. Policies protect the rights of workers as well as the business interests of employers. Depending on the needs of the organization, various policies and procedures establish rules regarding employee conduct, attendance, dress code, privacy, and other areas related to the terms and conditions of employment.

Employee policies: These policies are created and maintained by human resources staff to identify employee salary, pay schedule, employee benefits, work schedule, vacations, and more. They are often provided to new employees to review and sign.

Security policies: These policies identify a set of security objectives for a company, define the rules of behavior for users and administrators, and specify system requirements. These objectives, rules, and requirements collectively ensure the security of a network and the computer systems in an organization. Much like a continuity plan, a security policy is a constantly evolving document based on changes in the threat landscape, vulnerabilities, and business and employee requirements.

Security Policy (8.1.2.2)

A comprehensive security policy has a number of benefits:

- Demonstrates an organization's commitment to security
- Sets the rules for expected behavior
- Ensures consistency in system operations, software and hardware acquisition and use, and maintenance
- Defines the legal consequences of violations
- Gives security staff the backing of management

Security policies are used to inform users, staff, and managers of an organization's requirements for protecting technology and information assets. A security policy also specifies the mechanisms that are needed to meet security requirements and provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance.

A security policy may include the following:

Identification and authentication policy: Specifies authorized persons that can have access to network resources and identity verification procedures.

Password policy: Ensures passwords meet minimum requirements and are changed regularly.

Acceptable use policy (AUP): Identifies network applications and uses that are acceptable to the organization. It may also identify ramifications if this policy is violated.

Remote access policy: Identifies how remote users can access a network and what is accessible via remote connectivity.

Network maintenance policy: Specifies network device operating systems and end user application update procedures.

Incident handling procedures: Describes how security incidents are handled.

One of the most common security policy components is an acceptable use policy (AUP). This can also be referred to as an appropriate use policy. This component defines what users are allowed and not allowed to do on the various system components. This includes the type of traffic that is allowed on the network. TheAUP should be as explicit as possible to avoid misunderstanding. For example, an AUP might list specific websites, newsgroups, or bandwidth-intensive applications that are prohibited from being accessed by company computers or from the company network. Every employee should be required to sign an AUP, and the signed AUPs should be retained for the duration of employment.

BYOD Policies (8.1.2.3)

Many organizations must now also support Bring Your Own Device (BYOD).
This enables employees to use their own mobile devices to access company systems, software, networks, or information. BYOD provides several key benefits to enterprises, including increased productivity, reduced IT and operating costs, better mobility for employees, and greater appeal when it comes to hiring and retaining employees.

However, these benefits also bring an increased information security risk, because BYOD can lead to data breaches and greater liability for the organization.

A BYOD security policy should be developed to accomplish the following:

- Specify the goals of the BYOD program.
- Identify which employees can bring their own devices.
- Identify which devices will be supported.
- Identify the level of access employees are granted when using personal devices.
- Describe the rights to access and activities permitted to security personnel on the device.

- Identify which regulations must be adhered to when using employee devices.
- Identify safeguards to put in place if a device is compromised.

The following BYOD security best practices help mitigate BYOD risks:

Password protect access: Use unique passwords for each device and account.

Manually control wireless connectivity: Turn off Wi-Fi and Bluetooth connectivity when not in use. Connect only to trusted networks.

Keep updated: Always keep the device OS and other software updated. Updated software often contains security patches to mitigate against the latest threats or exploits.

Back up data: Enable backup of the device in case it is lost or stolen.

Enable "Find my Device": Subscribe to a device locator service with remote wipe feature.

Provide antivirus software: Provide antivirus software for approved BYOD devices.

Use Mobile Device Management (MDM) software: MDM software enables IT teams to implement security settings and software configurations on all devices that connect to company networks.

Regulatory and Standard Compliance (8.1.2.4)

There are also external regulations regarding network security. Network security professionals must be familiar with the laws and codes of ethics that are binding on Information Systems Security (INFOSEC) professionals.

Many organizations are mandated to develop and implement security policies. Compliance regulations define what organizations are responsible for providing and the liability if they fail to comply. The compliance regulations that an organization is obligated to follow depend on the type of organization and the data that the organization handles. Specific compliance regulations will be discussed later in the course.

Access Control (8.2)

In this section, you will learn about access control as a method of protecting a network.

Access Control Concepts (8.2.1)

In this topic, you will learn about access control policies.

Communications Security: CIA (8.2.1.1)

Information security deals with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

As shown in Figure 8-5, the CIA triad consists of three components of information security:

Confidentiality: Only authorized individuals, entities, or processes can access sensitive information.
Integrity: Refers to the protection of data from unauthorized alteration.
Availability: Authorized users must have uninterrupted access to important resources and data.

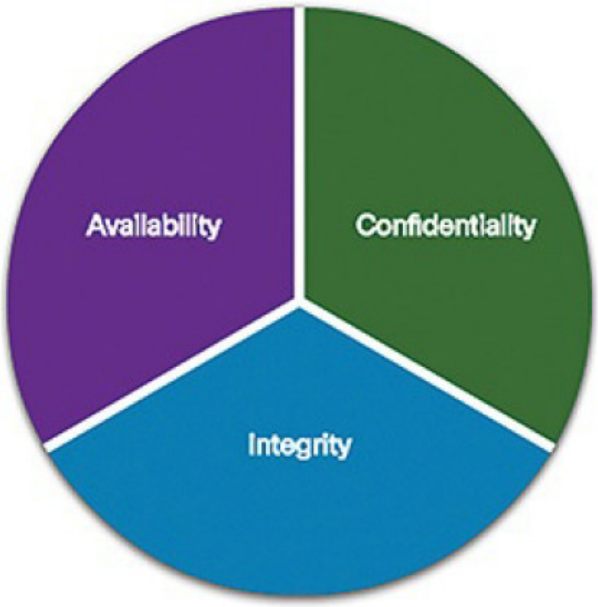

Figure 8-5 CIA Triad

Network data can be encrypted (made unreadable to unauthorized users) using various cryptography applications. The conversation between two IP phone users can be encrypted. The files on a computer can also be encrypted. These are just a few examples. Cryptography can be used almost anywhere that there is data communication. In fact, the trend is toward all communication being encrypted.

Access Control Models (8.2.1.2)

An organization must implement proper access controls to protect its network resources, information system resources, and information.

A security analyst should understand the different basic access control models to have a better understanding of how attackers can break the access controls.

Mandatory access control (MAC): Applies the strictest access control and is typically used in military or mission-critical applications. It assigns security level labels to information and enables users with access based on their security level clearance.

Discretionary access control (DAC): Allows users to control access to their data as owners of that data. DAC may use ACLs or other methods to specify which users or groups of users have access to the information.

Non-discretionary access control: Access decisions are based on an individual's roles and responsibilities within the organization, also known as role-based access control (RBAC).

Attribute-based access control (ABAC): Allows access based on attributes of the object (resource) to be accessed, the subject (user) accessing the resource, and environmental factors regarding how the object is to be accessed, such as time of day.

Another access control model is the principle of least privilege, which specifies a limited, as-needed approach to granting user and process access rights to specific information and tools. The principle of least privilege states that users should be granted the minimum amount of access required to perform their work function.

A common exploit is known as privilege escalation. In this exploit, vulnerabilities in servers or access control systems are exploited to grant an unauthorized user, or software process, higher levels of privilege than they should have. After the privilege is granted, the threat actor can access sensitive information or take control of a system.

Activity 8.2.1.3: Identify the Access Control Model
Refer to the online course to complete this Activity.

AAA Usage and Operation (8.2.2)

In this topic, you will learn how AAA is used to control network access.

AAA Operation (8.2.2.1)

A network must be designed to control who is allowed to connect to it and what they are allowed to do when they are connected. These design requirements are identified in the network security policy. The policy specifies how network administrators, corporate users, remote users, business partners, and clients access network resources. The network security policy can also mandate the implementation of an accounting system that tracks who logged in and when and what they did while logged in. Some compliance regulations may specify that access must be logged and the logs retained for a set period of time.

The Authentication, Authorization, and Accounting (AAA) protocol provides the necessary framework to enable scalable access security.

Network and administrative AAA security has several functional components:

Authentication: Users and administrators must prove that they are who they say they are. Authentication can be established using username and password combinations, challenge and response questions, token cards, and other methods. For example: “I am user ‘student’. I know the password to prove that I am user ‘student’.”

Authorization: After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform. An example is “User ‘student’ can access host serverXYZ using Telnet only.”

Accounting and auditing: Accounting records what the user does and when they do it, including what is accessed, the amount of time the resource is accessed, and any changes that were made. Accounting keeps track of how network resources are used. An example is "User 'student' accessed host serverXYZ using Telnet for 15 minutes."

This concept is similar to the use of a credit card, as indicated by Figure 8-6. The credit card identifies who can use it, identifies how much that user can spend, and keeps account of what items the user spent money on.

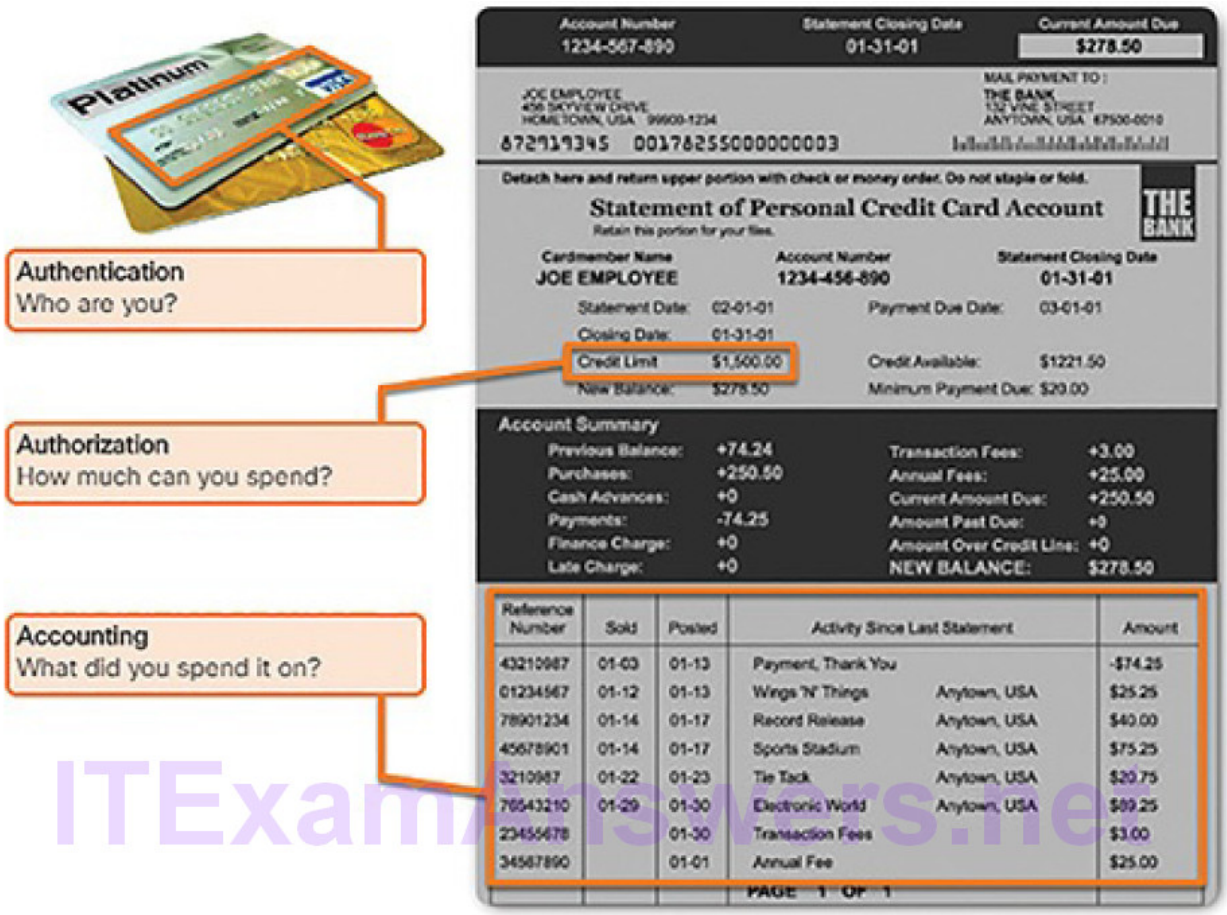

Figure 8-6 The AAA Concept Is Similar to Using a Credit Card

AAA Authentication (8.2.2.2)

AAA authentication can be used to authenticate users for administrative access or it can be used to authenticate users for remote network access. Cisco provides two common methods of implementing AAA services.

Local AAA Authentication

This method is sometimes known as self-contained authentication because it authenticates users against locally stored usernames and passwords, as shown in Figure 8-7. Local AAA is ideal for small networks.

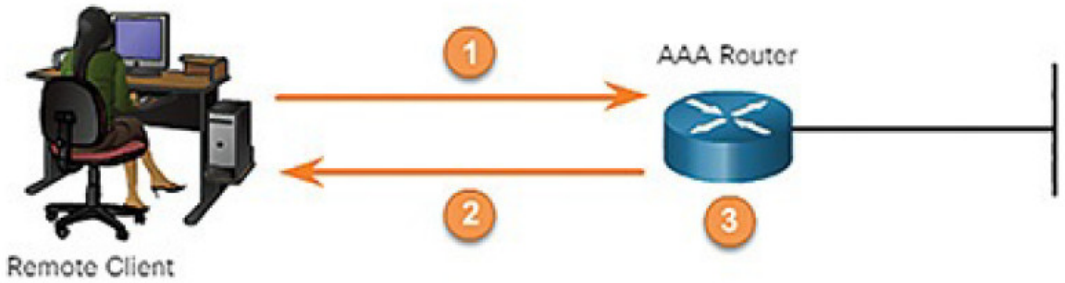

Figure 8-7 Local AAA Authentication

In Figure 8-7...

1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using the local database and the user is authorized to access the network based on information in the local database.

Server-Based AAA Authentication

This method authenticates against a central AAA server that contains the usernames and passwords for all users, as shown in Figure 8-8. Server-based AAA authentication is appropriate for medium-to-large networks.

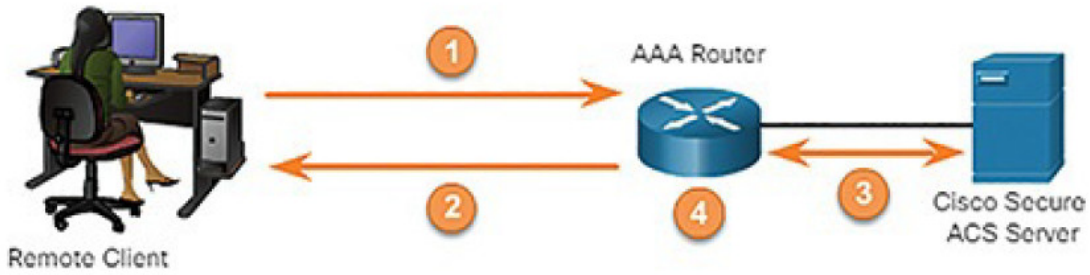

Figure 8-8 Server-Based AAA Authentication

In Figure 8-8...

1. The client establishes a connection with the router.
2. The AAA router prompts the user for a username and password.
3. The router authenticates the username and password using a remote AAA server such as a Cisco Secure ACS Server.
4. The user is authorized to access the network based on information on the remote AAA Server.

Centralized AAA is more scalable and manageable than local AAA authentication and, therefore, is the preferred AAA implementation.

A centralized AAA system may independently maintain databases for authentication, authorization, and accounting. It can leverage Active Directory or Lightweight Directory Access Protocol (LDAP) for user authentication and group membership, while maintaining its own authorization and accounting databases.

Devices communicate with the centralized AAA server using either the Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System Plus (TACACS+) protocols.

The following are specifics of the RADIUS protocol:

- RADIUS uses UDP ports 1812 and 1813, or 1645 and 1646.
- RADIUS combines authentication and authorization.
- RADIUS encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted, leaving the username, authorized services, and accounting unprotected.

The following are specifics of the TACACS+ protocol:

- TACACS+ uses TCP port 49.
- TACACS+ separates authentication, authorization, and accounting.
- TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.

AAA Accounting Logs (8.2.2.3)

Centralized AAA also enables the use of the accounting method. Accounting records from all devices are sent to centralized repositories, enabling simplified auditing of user actions.

AAA accounting collects and reports usage data in AAA logs. These logs are useful for security auditing. The collected data might include the start and stop connection times, executed commands, number of packets, and number of bytes.

One widely deployed use of accounting is to combine it with AAA authentication. This helps with managing access to internetworking devices by network administrative staff. Accounting provides more security than just authentication. The AAA servers keep a detailed log of exactly what the authenticated user does on the device, as shown in Figure 8-9.

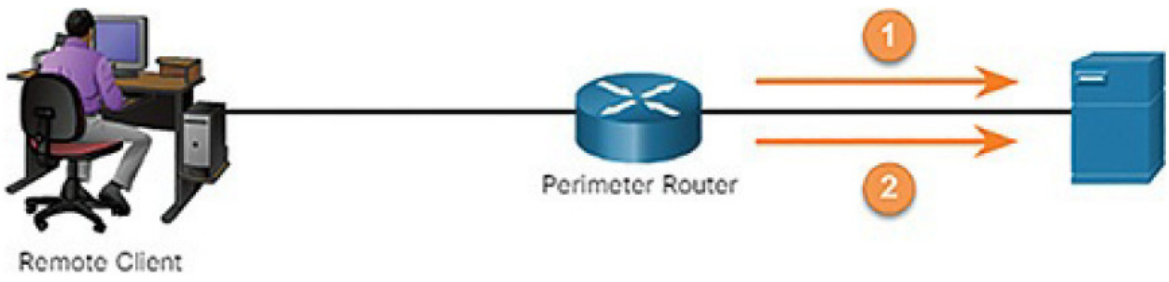

Figure 8-9 AAA Accounting

In Figure 8-9…

1. When a user has been authenticated, the AAA accounting process generates a start message to begin the accounting process.
2. When the user finishes, a stop message is recorded and the accounting process ends.

This includes all EXEC and configuration commands issued by the user. The log contains numerous data fields, including the username, the date and time, and the actual command that was entered by the user. This information is useful when troubleshooting devices. It also provides evidence against individuals who perform malicious actions.

The various types of accounting information that can be collected include:

Network accounting: Network accounting captures information for all Point-to-Point Protocol (PPP) sessions, including packet and byte counts.

Connection accounting: Connection accounting captures information about all outbound connections made from the AAA client, such as Telnet or SSH.

EXEC accounting: EXEC accounting captures information about user EXEC terminal sessions (user shells) on the network access server, including username, date, start and stop times, and the access server IP address.

System accounting: System accounting captures information about all system-level events (for example, when the system reboots or when accounting is turned on or off).

Command accounting: Command accounting captures information about the EXEC shell commands for a specified privilege level that are being executed on a network access server. Each command accounting record includes a list of the commands executed for that privilege level, as well asthe date and time each command was executed, and the user who executed it.

Resource accounting: The Cisco implementation of AAA accounting captures “start” and “stop” record support for calls that have passed user authentication. The additional feature of generating “stop” records for calls that fail to authenticate as part of user authentication is also supported. Such records are necessary for users employing accounting records to manage and monitor their networks.

Activity 8.2.2.4: Identify the Characteristic of AAA
Refer to the online course to complete this Activity.

Threat Intelligence (8.3)

In this section, you will learn how to use various intelligence sources to locate current security threats.

Information Sources (8.3.1)

In this topic, you will learn how information sources are used to communicate emerging network security threats.

Network Intelligence Communities (8.3.1.1)

To effectively protect a network, security professionals must stay informed and gain network intelligence. There are many security organizations which provide network intelligence. They provide resources, workshops, and conferences to help security professionals. These organizations often have the latest information on threats and vulnerabilities.

Figure 8-10 shows a few important network security organizations, described here:

Figure 8-10 Network Security Organizations

CERT: Computer Emergency Response Team (CERT) is a U.S. federally funded initiative chartered to work with the Internet community in detecting and resolving computer security incidents. The CERT Coordination Center (CERT/CC) coordinates communication among experts during security emergencies to help prevent future incidents. CERT also responds to major security incidents and analyzes product vulnerabilities. CERT manages changes relating to progressive intruder techniques and to the difficulty of detecting attacks and

catching attackers. It also develops and promotes the use of appropriate technology and systems management practices to resist attacks on networked systems, to limit damage, and to ensure continuity of services.

SANS: SysAdmin, Audit, Network, Security (SANS) Institute resources are largely free upon request and include the popular Internet Storm Center, the Internet's early warning system; NewsBites, the weekly news digest; @RISK, the weekly vulnerability digest; flash security alerts; and more than 1,200 award-winning, original research papers. SANS also develops security courses.

MITRE: The MITRE Corporation maintains a list of CommonVulnerabilities and Exposures (CVE) used by prominent security organizations.

(ISC)2: International Information Systems Security Certification Consortium (ISC)2 provides vendor-neutral education products and career services in more than 135 countries, to 75,000+ certified industry professionals. Their mission is to make the cyber world a safer place by elevating information security to the public domain, and supporting and developing network security professionals around the world. They also provide information security certifications including the Certified Information Systems Security Professional (CISSP).

INFOSYSSEC: Information Systems Security (InfoSysSec) is a network security organization that hosts a security news portal, providing the latest breaking news pertaining to alerts, exploits, and vulnerabilities.

FIRST: Forum of Incident Response and Security Teams (FIRST) is a security organization that brings together a variety of computer security incident response teams from government, commercial, and educational organizations to foster cooperation and coordination in information sharing, incident prevention, and rapid reaction.

MS-ISAC: The Multi-State Information Sharing & Analysis Center (MS-ISAC) is the focal point for cyberthreat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24×7 cybersecurity operations center provides real-time network monitoring, early cyberthreat warnings and advisories, vulnerability identification and mitigation, and incident response.

To remain effective, a network security professional must:

Keep abreast of the latest threats: This includes subscribing to real-time feeds regarding threats, routinely perusing security-related websites, following security blogs and podcasts, and more.

Continue to upgrade skills: This includes attending security-related training, workshops, and conferences.

Note
Network security has a very steep learning curve and requires a commitment to continuous professional development.

Cisco Cybersecurity Reports (8.3.1.2)

A resource to help security professionals stay abreast of the latest threats is the Cisco Annual Cybersecurity Report, and the Mid-Year Cybersecurity Report. These reports provide an update on the state of security preparedness, expert analysis of top vulnerabilities, factors behind the explosion of attacks using adware and spam, and more.

Cybersecurity analysts should subscribe to and read these reports to learn how threat actors are targeting their networks, and what can be done to mitigate these attacks.

Security Blogs and Podcasts (8.3.1.3)

Another method for keeping up-to-date on the latest threats is to read blogs and listen to podcasts. Blogs and podcasts also provide advice, research, and recommended mitigation techniques.

There are several security blogs and podcasts available that a cybersecurity analyst should follow to learn about the latest threats, vulnerabilities, and exploits.

Search the Internet for Cisco's podcast and blog from the Cisco Talos group.

Threat Intelligence Services (8.3.2)

In this topic, you will learn how to use threat intelligence to identify threats and vulnerabilities.

Cisco Talos (8.3.2.1)

Threat intelligence services allow the exchange of threat information such as vulnerabilities, indicators of compromise (IOCs), and mitigation techniques. This information is shared not only with personnel, but also with security systems. As threats emerge, threat intelligence services create and distribute firewall rules and IOCs to the devices that have subscribed to the service.

One such service is the Cisco Talos group. Talos is a world-leading threat intelligence team with a goal to help protect enterprise users, data, and infrastructure from active adversaries. The Talos team collects information aboutactive, existing, and emerging threats. Talos then provides comprehensive protection against these attacks and malware to its subscribers.

Cisco Security products can use Talos threat intelligence in real time to provide fast and effective security solutions.

Cisco Talos also provides free software, services, resources, and data.

FireEye (8.3.2.2)

FireEye is another security company that offers services to help enterprises secure their networks. FireEye uses a three-pronged approach combining security intelligence, security expertise, and technology.

The FireEye Malware Analysis product blocks attacks across web and email threat vectors, and latent malware that resides on file shares. It can block advanced malware that easily bypasses traditional signature-based defenses and compromises the majority of enterprise networks. It addresses all stages of an attack lifecycle with a signature-less engine utilizing stateful attack analysis to detect zero-day threats.

Automated Indicator Sharing (8.3.2.3)

The U.S. Department of Homeland Security (DHS) offers a free service called Automated Indicator Sharing (AIS). AIS enables the real-time exchange of cyberthreat indicators (e.g., malicious IP addresses, the sender address of a phishing email, etc.) between the U.S. federal government and the private sector.

AIS creates an ecosystem where, as soon as a threat is recognized, it is immediately shared with the community to help them protect their networks from that particular threat.

Common Vulnerabilities and Exposures Database (8.3.2.4)

The U.S. government sponsored the MITRE Corporation to create and maintain a catalog of known security threats called Common Vulnerabilities and Exposures (CVE). The CVE serves as a dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

The MITRE Corporation defines unique CVE Identifiers for publicly known information-security vulnerabilities to make it easier to share data.

Threat Intelligence Communication Standards (8.3.2.5)

Network organizations and professionals must share information to increase knowledge about threat actors and the assets they want to access. Several intelligence sharing open standards have evolved to enable communication across multiple networking platforms. These standards enable the exchange of cyberthreat intelligence (CTI) in an automated, consistent, and machine-readable format.

Two common threat intelligence sharing standards include

Structured Threat Information Expression (STIX): This is a set of specifications for exchanging cyberthreat information between organizations. The Cyber Observable Expression (CybOX) standard has been incorporated into STIX.

Trusted Automated Exchange of Indicator Information (TAXII): This is the specification for an application layer protocol that allows the communication of CTI over HTTPS. TAXII is designed to support STIX.

These open standards provide the specifications that aid in the automated exchange of cyberthreat intelligence information in a standardized format.

Activity 8.3.2.6: Identify the Threat Intelligence Information Source
Refer to the online course to complete this Activity.

Summary (8.4)

In this chapter, you learned the importance of protecting our networks, devices, and data from threat actors.

Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets. This approach uses multiple layers of security at the network edge, within the network, and on network endpoints.Organizations must also have a set of policies that define the activities that are allowed on the network. These include business policies, security policies, BYOD policies, and policies that ensure the organization complies with governmental regulations.

Access control methods are used to protect the confidentiality, integrity, and availability of our networks, devices, and data. Access control models include:

- Mandatory access control
- Discretionary access control
- Non-discretionary access control
- Attribute-based access control

AAA security provides the necessary framework to enable scalable access security:

Authentication: Users and administrators must prove that they are who they say they are.

Authorization: After the user is authenticated, authorization services determine which resources the user can access and which operations the user is allowed to perform.

Accounting: Records what the user does and when they do it, including what is accessed, the amount of time the resource is accessed, and any changes that were made.

Security experts and cybersecurity analysts rely on various information sources to keep abreast of the latest threats and continue to upgrade their skills. Threat intelligences services, such as Cisco Talos, FireEye, DHS AIS, and the CVE database, allow the exchange of threat information such as vulnerabilities, indicators of compromise (IOCs), and mitigation techniques. These services are guided by the threat intelligence sharing standards STIX and TAXII.

Practice

The chapter does not have any Labs or Packet Tracer activities.