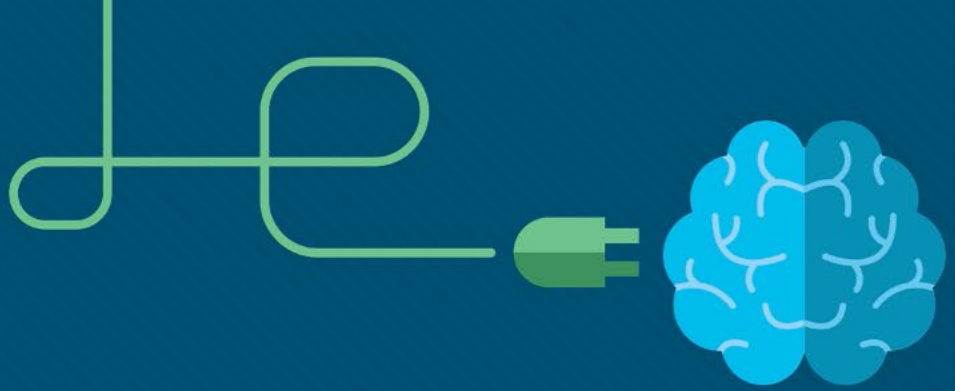


Module 13: Access Control

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Access Control

Module Objective: Configure local and server-based access control.

Topic Title	Topic Objective
Access Controls	Configure secure access on a host.
Access Control Concepts	Explain how access control protects network data.
Account Management	Explain the need for account management and access control strategies.
AAA Usage and Operation	Configure server-based authentication with TACACS+ and RADIUS.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.1 Access Controls

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Physical Access Controls

- **Physical access controls** are actual barriers deployed to prevent direct physical contact with systems.

- The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets.

- Some examples of physical access controls are:
  - Guards to monitor the facility
  - Fences to protect the perimeter
  - Motion detectors to detect moving objects
  - Laptop locks to safeguard portable equipment
  - Locked doors to prevent unauthorized access
  - Swipe cards to allow access to restricted areas
  - Guard dogs to protect the facility
  - Video cameras to monitor a facility by collecting and recording images
  - Mantrap-style entry systems to stagger the flow of people into the secured area and trap any unwanted visitors
  - Alarms to detect intrusion

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Logical Access Controls

- **Logical access controls** are the hardware and software solutions used to manage access to resources and systems.

- These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.

- Logical access control examples
  - Encryption is the process of taking plaintext and creating ciphertext.
  - Smart cards have an embedded microchip.
  - Passwords are protected strings of characters.
  - Biometrics are users' physical characteristics.
  - Access control lists (ACLs) define the type of traffic allowed on a network.
  - Protocols are sets of rules that govern the exchange of data between devices.
  - Firewalls prevent unwanted network traffic.
  - Routers connect at least two networks.
  - Intrusion detection systems monitor a network for suspicious activities.
  - Clipping levels are certain allowed thresholds for errors before triggering a red flag.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Administrative Access Controls

- **Administrative access controls** are the policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access.

- Administrative controls focus on personnel and business practices.

- Examples of administrative controls
  - Policies are statements of intent.
  - Procedures are the detailed steps required to perform an activity.
  - Hiring practices define the steps an organization takes to find qualified employees.
  - Background checks are a type of employee screening that includes information of past employment verification, credit history, and criminal history.
  - Data classification categorizes data based on its sensitivity.
  - Security training educates employees about the security policies at an organization.
  - Reviews evaluate an employee's job performance.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Administrative Access Controls in Detail

- The concept of administrative access controls involves three security services: authentication, authorization, and accounting (AAA).

- These services provide the primary framework to control access, preventing unauthorized access to a computer, network, database, or other data resource.

- **Authentication:**
  - It verifies the identity of each user, to prevent unauthorized access.
  - Users prove their identity with a username or ID.
  - In addition, users need to verify their identity by providing one of the following:
    - Something they know (such as a password)
    - Something they have (such as a token or card)
    - Something they are (such as a fingerprint)
    - In the case of two factor authentication, which is increasingly becoming the norm, the system requires a combination of two of the above rather than just one to verify someone's identity.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Administrative Access Controls in Detail (Cont.)

- **Authorization**:
  - It determines which resources users can access, along with the operations that users can perform.
  - Some systems accomplish this by using an access control list, or an ACL.
    - An ACL determines whether a user has certain access privileges once the user authenticates.
    - It can also control when a user has access to a specific resource.

- **Accounting:**
  - It keeps track of what users do — including what they access, the amount of time they access resources, and any changes they make.
  - Cybersecurity accounting services track each data transaction and provide auditing results.
  - System administrators can set up computer policies to enable system auditing.
  - Cybersecurity accounting tracks and monitors in real time.

- The concept of AAA is like using a credit card that identifies who can use it, how much that user can spend, and accounts for items or services the user purchased.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Is Identification?

- It enforces the rules established by the authorization policy.
- Every time access to a resource is requested, the access controls determine whether to grant or deny access.
- A unique identifier ensures the proper association between allowed activities and subjects.
- A username is the most common method used to identify a user.
- A username can be an alphanumeric combination, a personal identification number (PIN), a smart card or biometric — such as a fingerprint, retina scan, or voice recognition.
- A unique identifier ensures that a system can identify each user individually, therefore allowing an authorized user to perform the appropriate actions on a particular resource.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Federated Identity Management

- It refers to multiple enterprises that let their users use the same identification credentials to gain access to the networks of all enterprises in the group.
- Unfortunately, this broadens the scope and increases the probability of a cascading effect should an attack occur.
- A federated identity links a subject's electronic identity across separate identity management systems, such as being able to access several websites using the same social login credentials.
- The goal of federated identity management is to share identity information automatically across castle boundaries.
- From the individual user's perspective, this means a single sign-on to the web.
- It is imperative that organizations scrutinize the identifying information shared with partners, even within the same corporate group, for example.
- The sharing of social security numbers, names, and addresses may allow identity thieves the opportunity to steal this information from a partner to perpetrate fraud.
- The most common way to protect federated identity is to tie login ability to an authorized device.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Methods

- Users prove their identity with a username or ID and need to verify their identity by providing one of the following.

What you know:

- Passwords, passphrases, or PINs are all examples of something that the user knows.
- The terms passphrase, passcode, passkey, and PIN are all generically referred to as password — a string of characters used to prove a user's identity.
- A password should be at least eight characters and contain a combination of upper and lowercase letters, numbers, and special characters.
- Users need to use different passwords for different systems because if a criminal cracks the user's password once, the criminal will have access to all the user's accounts.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Methods (Cont.)

What you have:

- Smart cards and security key fobs are examples of something that users possess that can be used for authentication purposes.
- A smart card is a small plastic card, about the size of a credit card, with a small chip embedded in it that is capable of processing, storing, and safeguarding data.
- A security key fob is a device that is small enough to attach to a keyring.
- In most cases, security key fobs are used for two factor authentication (2FA), which is much more secure than a username and password combination.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Methods (Cont.)

Who you are:

- Biometric security compares unique physical characteristics against stored profiles to authenticate users.

- There are two types of biometric identifiers:
  - **Physiological characteristics** — fingerprints, DNA, face, hands, retina, or ear features.
  - **Behavioral characteristics** — patterns of behavior such as gestures, voice, gait, or typing rhythm.

- Biometrics is becoming increasingly popular in public security systems, consumer electronics and point-of-sale applications.

- Implementing biometrics involves a reader or scanning device, software that converts the scanned information into digital form and a database that has biometric data stored for comparison.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Multi-Factor Authentication

- It uses at least two methods of verification — such as a password and something you have, for example, a security key fob.
- This can be taken a step further by adding something you are, such as a fingerprint scan.
- Multi-factor authentication can reduce the incidence of online identity theft because it means knowing a password will not give cybercriminals access to a user's account.
- Note that two-factor authentication (2FA) is a method of multi-factor authentication that entails two factors, but the two terms are often used interchangeably.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authorization

Authorization controls what a user can and cannot do on the network after successful authentication.

- After a user proves their identity, the system checks to see what network resources the user can access and what they can do with the resources.

When to implement authorization

- Authorization uses a set of attributes that describes the user's access to the network, to answer the question, 'What read, copy, edit, create, and delete privileges does this user have?'

- The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local device where the user is connected.

- Authorization is automatic and does not require users to perform additional steps after authentication.

- System administrators have set the network up to implement authorization immediately after the user authenticates.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authorization (Cont.)

Using authorization

- Defining authorization rules is the first step in controlling access.
- An authorization policy establishes these rules.
- A group membership policy defines authorization based on users' membership in a specific group.
- All employees of an organization may have a swipe card, for example, which provides access to the premises, but it might not allow access to a server room.
- An authority-level policy defines access permissions based on an employee's position within the organization.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer - Configure Access Control

In the following Packet Tracer activity, you will complete the following objectives:

Part 1: Configure and Use AAA Authentication Credentials
Part 2: Configure and Use Email Services
Part 3: Configure and Use FTP Services

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Implementing Accountability

- **What is accountability?**
  - Accountability traces an action back to a person or process making this change to a system.
  - It then collects this information and reports the usage data.
  - The organization can use this data for such purposes as auditing or billing.
- **Implementing accountability**
  - Implementing accountability consists of technologies, policies, procedures, and education.
  - Log files provide detailed information based on the parameters chosen.
  - The organization's policies and procedures spell out what actions should be recorded and how the log files are generated, reviewed, and stored.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Implementing Accountability (Cont.)

- **Providing accountability**
  - Data retention, media disposal, and compliance requirements all provide accountability.
  - Many laws require the implementation of measures to secure different data types.
  - These laws guide an organization on the right way to handle, store, and dispose of data.
  - The education and awareness of an organization's policies, procedures, and related laws can also contribute to accountability.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab - Configure Authentication and Authorization in Linux

In the following Lab, you will complete the following objectives:

Part 1: Add a New Group for Users
Part 2: Add Users to the New Group
Part 3: Switch Users and Modify Permissions
Part 4: Modify Permissions in Absolute Mode

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.2 Access Control Concepts

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zero Trust Security

- **Zero trust** is a comprehensive approach to securing all access across networks, applications, and environments.
- This approach helps secure access from users, end-user devices, APIs, IoT, microservices, containers, and more.
- A zero trust security framework helps to prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement through a network.
- Traditionally, the network perimeter (edge) was the boundary between inside and outside, or trusted and untrusted.
- In a zero trust approach, any place at which an access control decision is required should be considered a perimeter.
- This means that although a user or other entity may have successfully passed access control previously, they are not trusted to access another area or resource until they are authenticated.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Zero Trust Security (Cont.)

The three pillars of zero trust are **workforce, workloads,** and **workplace:**

Zero Trust for the Workforce

- This pillar consists of people (e.g., employees, contractors, partners, and vendors) who access work applications by using their personal or corporate-managed devices.
- It ensures only the right users and secure devices can access applications, regardless of location.

Zero Trust for Workloads

- This pillar is concerned with applications that are running in the cloud, in data centers, and other virtualized environments that interact with one another.
- It focuses on secure access when an API, a microservice, or a container is accessing a database within an application.

Zero Trust for the Workplace

- This pillar focuses on secure access for all devices, including on the internet of things (IoT), that connect to enterprise networks, such as user endpoints, physical and virtual servers, printers, cameras, HVAC systems, kiosks, infusion pumps, industrial control systems, and more.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Access Control Models

- 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.
- One 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.
- A common exploit is known as privilege escalation.
  - 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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Access Control Models (Cont.)

Access Control Models	Description
Discretionary access control (DAC)	This is the least restrictive model and 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.
Mandatory access control (MAC)	This 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.
Role-based access control (RBAC)	Access decisions are based on an individual's roles and responsibilities within the organization. Different roles are assigned security privileges, and individuals are assigned to the RBAC profile for the role. Roles may include different positions, job classifications, or groups of job classifications. Also known as a type of non-discretionary access control.
Attribute-based access control (ABAC)	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.
Rule-based access control (RBAC)	Network security staff specify sets of rules regarding or conditions that are associated with access to data or systems. These rules may specify permitted or denied IP addresses, or certain protocols and other conditions. Also known as Rule-Based RBAC.
Time-based access control (TAC)	TAC Allows access to network resources based on time and day.

Network Access Control (NAC) Systems

- They support access management by enforcing organizational policies regarding the people and devices that are attempting to access the network.

- NAC systems allow cybersecurity professionals to monitor the users and devices that are attached to the network, and manually control access as required.

- Network access control systems provide the following capabilities:
  - Rapidly enforcing access policies that have been created for different operational conditions.
  - Recognizing and profiling connected users and devices to prevent malicious software on non-compliant systems from causing damage.
  - Providing secure access to network guests, often through registration portals.
  - Evaluating device compliance with security policies by user type, device type, and operating system prior to permitting network access.
  - Mitigating security incidents by blocking, isolating, or repairing non-compliant devices.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Network Access Control (NAC) Systems (Cont.)

- Because BYOD and IoT networking greatly expand the network attack surface, NAC system automation features make focused control of network access by such devices practical.
- The NAC system is configured to enforce organizational policies.
- The relevant policies are enacted to permit or deny network access according to a wide range of factors that the NAC system detects on the devices that are attempting access.
- Without NAC systems it would be impossible for cybersecurity personnel to evaluate the thousands of devices that could attempt to access the network.
- NAC is an important component of a zero-trust security architecture that enforces security policy compliance with all devices and users that attempt to access the network.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.3 Account Management

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Account Types

- An organization should not share accounts for privileged users, administrators, or applications.
- The administrator account should only be used to administer a system.
- If a user accesses a malware-infected website or opens a malicious email while using the administrator account, this would put the organization at risk.
- Administrators must be aware of the default group and user accounts that might be installed by an operating system.
- Knowing about these accounts will help an administrator decide which should be permitted and which of these accounts should be disabled.
- Default accounts such as the guest or administrator accounts can be a security risk in older systems as attackers are familiar with the default settings used.
- To improve security, always replace any default accounts and make sure that all account types require a password.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Account Types (Cont.)

It's important to properly manage accounts to maintain security.

- On hiring a new employee, create an identity profile, register the employee's computer and mobile devices, and enable access to the organization's network. As the Identity Provider (IdP), the organization is responsible for authenticating their identity.
- Disable or deactivate any accounts that are no longer needed and retrieve any organizational data or applications from the user's devices.
- Grant a user no more access than is necessary to perform assigned tasks (least privilege).
- Review user access to identify any access control adjustments that need to be made.
- Use time of day restrictions to control when a user can log in.
- Use location restrictions to control where a device or user can log in from.
    - Geofencing is used to trigger an action when a user enters or exits a geographic boundary.
    - Geolocation identifies a device based on its geographic location.
    - Geotagging adds an identifier to something based on the location (like a photo taken on a smartphone tagged with the coordinates of where the photo was taken).

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Privileged Accounts

- Cybercriminals target privileged accounts because these are the most powerful accounts in the organization with elevated, unrestricted access to systems.
- Administrators use these accounts to deploy and manage operating systems, applications, and network devices.
- Continuously securing and locking down privileged accounts is critical to the security of the organization. Regularly evaluate this process and adjust to improve protection.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Privileged Accounts (Cont.)

Organizations should adopt robust practices for securing privileged accounts.

- Identify and reduce the number of privileged accounts.
- Enforce the principle of least privilege. The principle means that users, systems, and processes only have access to resources (networks, systems, and files) that are necessary to perform their assigned function.
- Revoke access rights when employees leave or change jobs.
- Eliminate shared accounts with passwords that do not expire.
- Secure password storage.
- Eliminate shared credentials for multiple administrators.
- Automatically change privileged account passwords every 30 or 60 days.
- Record privileged sessions.
- Implement a process to change embedded passwords for scripts and service accounts.
- Log all user activity.
- Generate alerts for unusual behavior.
- Disable inactive privileged accounts.
- Use multi-factor authentication for all administrative access.
- Implement a gateway between the end user and sensitive assets to limit network exposure to malware.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

File Access Control

- **Permissions** are rules configured to limit folder or file access for an individual or a group and can help secure data.
- Users should be limited to only the resources they need on a computer system or network.
- It may be easier to provide access to the entire drive, but it is more secure to limit access to only the folder they need.
- This is the principle of **least privilege** and closely connected to the concept of ‘need to know’ access.
- Limiting access to resources also prevents cybercriminals from accessing those resources if the user’s computer becomes infected.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

File Access Control (Cont.)

Permission levels available for files and folders

Full Control: Users can:

- See the contents of a file or folder.
- Change and delete existing files and folders.
- Create new files and folders.
- Run programs in a folder.

Modify: Users can change and delete existing files and folders but cannot create new ones.

Read and execute: Users can see the contents of existing files and folders and can run programs in a folder.

Write: Users can create new files and folders and make changes to existing files and folders.

Read: Users can see the contents of a folder and open files and folders.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

File Access Control (Cont.)

- If an administrator denies an individual or group permissions to a network share, this will override any other permission settings.
  - The user cannot access that share, even if the user is the administrator or part of the administrator group.

- The local security policy must outline the resources and the type of access allowed for each user and group.

- After parent folder permissions have been set, folders and files created inside the parent folder inherit its permissions.

- The location of data and the action performed on it also determine the permission propagation:
  - Data moved to the same volume will keep the original permissions.
  - Data copied to the same volume will inherit new permissions.
  - Data moved to a different volume will inherit new permissions.
  - Data copied to a different volume will inherit new permission.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Account Policies in Windows

- In most networks that use Windows computers, an administrator configures Active Directory with domains on a Windows server.
- Windows computers that join the domain become domain members.
- The administrator configures a **domain security policy** that applies to all domain members.
- When a computer is not part of an Active Directory domain, the user configures policies through Windows Local Security Policy.
- In all versions of Windows except Home edition, enter ‘secpol.msc’ at the Run command to open the Local Security Policy tool.

Configuring Security Policies:

- **Password Policy**
  - An administrator can configure user account policies such as password policies and lockout policies.
  - Passwords must contain eight characters and three of the following four categories: uppercase letters, lowercase letters, numbers, and symbols.
  - Lastly, the user can reuse a password after 24 unique passwords.
  - Different password policies can be set, depending on organizational requirements and needs.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Account Policies in Windows (Cont.)

- **Account Lockout Policy**
  - An account lockout policy locks an account for a set duration when too many incorrect login attempts occur.
  - For example, a policy allows a user to enter the wrong username and/or password five times.
    - After five attempts, the account locks users out for 30 minutes.
    - After 30 minutes, the number of attempts resets to zero and the user can attempt to log in again.

- **Audit Policies**
  - More security settings are available by selecting the ‘local policies’ folder in Windows.
  - An audit policy creates a security log file used to track the following events:
    - Account logon events
    - Audit account management
    - Directory service access
    - Object access
    - Policy changes
    - Privilege use
    - Process tracking
    - System events

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Management

- Authentication and authorization issues include unencrypted credentials, incorrect permissions, and access violations.

- Authentication management aims to ensure secure sign in while still providing ease of use:
  - A **Single Sign On (SSO)** solution allows the user to use one set of login credentials to authenticate across multiple applications. This way, the user only needs to remember one strong password.
  - **OAuth** is a standard that enables a user's account information to be used by third-party services such as Facebook or Google.
  - A **password vault** can protect and store the user's credentials with a single strong password required to access them.
  - Many organizations implement **Knowledge-Based Authentication (KBA)** to provide a password reset should a user forget their password. KBA is based on personal information known by the user or a series of questions.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hash-Based Message Authentication Code (HMAC)

- HMAC uses an encryption key with a hash function to authenticate a web user.
  - Using HMAC, the user sends a private key identifier and an HMAC.
  - The server looks up the user's private key and creates an HMAC.
  - The user's HMAC must match the one calculated by the server.

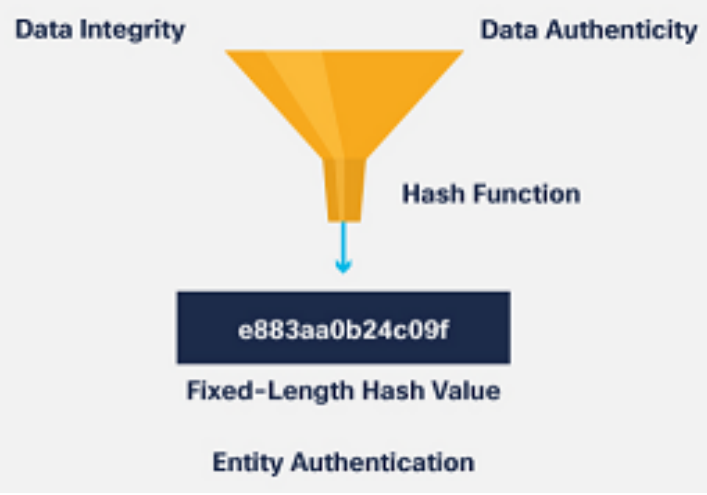
- Many web services use basic authentication, which does not encrypt the username and password during transmission.

- VPNs using IPsec rely on HMAC functions to authenticate the origin of every packet and provide data integrity checking.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Hash-Based Message Authentication Code (HMAC) (Cont.)

- Cisco products use hashing for entity authentication, data integrity, and data authenticity purposes.
- Cisco IOS routers use hashing with secret keys in an HMAC-like manner to add authentication information to routing protocol updates.
- IPsec gateways and clients use hashing algorithms, such as MD5 and SHA-1 in HMAC mode, to provide packet integrity and authenticity.
- Cisco software images on Cisco.com have an MD5-based checksum available so that customers can check the integrity of downloaded images.



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Protocols and Technologies

- An authentication protocol authenticates data between two entities to prevent unauthorized access.
- The word ‘entity’ can refer to any device or system within an organization.
- A protocol outlines the type of information that needs to be shared to authenticate and connect.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Authentication Protocols and Technologies

Extensible Authentication Protocol (EAP)	A password from the client is sent using a hash to the authentication server. The authentication server has a certificate (the client does not need a certificate).
Password Authentication Protocol (PAP)	A username and password are sent to a remote access server in plaintext. Most network operating system remote servers support PAP.
Challenge Handshake Authentication Protocol (CHAP)	It validates the identity of remote clients using a one-way hashing function created by the client. The service also calculates the expected hash value. The server (the authenticator) compares the two values. If the values match, transmission continues.
802.1X	An organization authenticates your identity and authorizes access to the network. Your identity is determined based on credentials or a certificate which is confirmed by a RADIUS server.
RADIUS	Use it to either accept or deny access when simple username/password authentication is needed. It only encrypts the user's password from client to the server.
TACACS+	It encrypts all data (username, password, accounting and authorized services) between the client and the server.
Kerberos	It uses strong encryption, requesting a client to prove its identity to a server, with the server in turn authenticating itself to the client.

Applications of Cryptographic Hash Functions

- Cryptographic hash functions help us to ensure data integrity and verify authentication.

- Cryptographic hash functions are used in the following situations:
  - To provide proof of authenticity when used with a symmetric secret authentication key such as IP security (IPsec) or routing protocol authentication.
  - To provide authentication by generating one-time and one-way responses to challenges in authentication protocols.
  - To provide message integrity check proof (such as those used in digitally signed contracts) and Public Key Infrastructure (PKI) certificates (like those accepted when accessing a secure website).

- When choosing a hashing algorithm, use SHA-256 or higher, as they are currently the most secure. Avoid SHA-1 and MD5 due to security flaws that have been discovered.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Access Control Strategies

Mandatory access control	It restricts the actions that a user can perform on an object (a file, a port or a device). An authorization rule enforces whether a user can access the object. Organizations use it where different levels of security classifications exist. Every object has a label, and every user has a clearance. Its system restricts a user based on the security classification of the object and the label attached to the user.
Discretionary access control	In systems that employ them, the owner of an object can decide which users can access that object and what specific access they may have. Permissions and access control lists can be used to implement it. The owner of a file can specify what permissions (read, write, or execute) other users may have. An ACL uses rules to determine what traffic can enter or exit a network.
Role-based access control	It depends on the role or job function of the user. It can work in combination with discretionary access controls or mandatory access controls by enforcing the policies of either one. It helps to implement security administration in large organizations with hundreds of users and thousands of possible permissions.
Rule-based access control	It uses ACLs to help determine whether to grant access. A series of rules is contained in the ACL and the decision to grant access depends on these rules. As with mandatory access control, users cannot change the access rules. Organizations can combine rule-based access control with other strategies for implementing access restrictions.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.4 AAA usage and operation

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AAA Operation

- 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, when, and what they did while logged in.
- The **Authentication, Authorization, and Accounting (AAA)** protocol provides the necessary framework to enable scalable access security.
- The three independent security functions provided by the AAA architectural framework are authentication, authorization, and accounting.
- This concept is like the use of a credit card.
    - The credit card identifies who can use it, how much that user can spend, and keeps account of what items the user spent money on.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AAA Operation (Cont.)

The three independent security functions provided by the AAA architectural framework:

AAA Component	Description
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. AAA authentication provides a centralized way to control access to the network.
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 server XYZ using SSH only.”
Accounting	Accounting records what the user does, 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 server XYZ using SSH for 15 minutes."

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AAA Authentication

- AAA Authentication can be used to authenticate users for administrative access or remote network access.

- Cisco provides two common methods of implementing AAA services:
  - **Local AAA Authentication:** It is sometimes known as self-contained authentication because it authenticates users against locally stored usernames and passwords. Ideal for small networks.
  - **Server-Based AAA Authentication:** This method authenticates against a central AAA server that contains the usernames and passwords for all users. It is appropriate for medium-to-large networks.

- Centralized AAA is more scalable and manageable than local AAA authentication and it is the preferred AAA implementation.
  - Its system may independently maintain databases for authentication, authorization, and accounting.
  - It can leverage Active Directory or 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 RADIUS or TACACS+ protocols.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AAA Authentication (Cont.)

The table lists the differences between the two protocols.

	TACACS+	RADIUS
Functionality	It separates authentication, authorization, and accounting functions according to the AAA architecture, allowing modularity of the security server implementation.	It combines authentication and authorization but separates accounting, allowing less flexibility in implementation than TACACS+.
Standard	Mostly Cisco supported	Open/RFC standard
Transport	TCP port 49	UDP ports 1812/1813, or 1645/1646
Protocol CHAP	Bidirectional challenge and response as used in CHAP.	Unidirectional challenge and response from the RADIUS security server to the RADIUS client.
Confidentiality	Encrypts the entire body of the packet but leaves a standard TACACS+ header.	Encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted.
Customization	Provides authorization of router commands on a per-user or per-group basis.	Has no option to authorize router commands on a per-user or per-group basis.
Accounting	Limited	Extensive

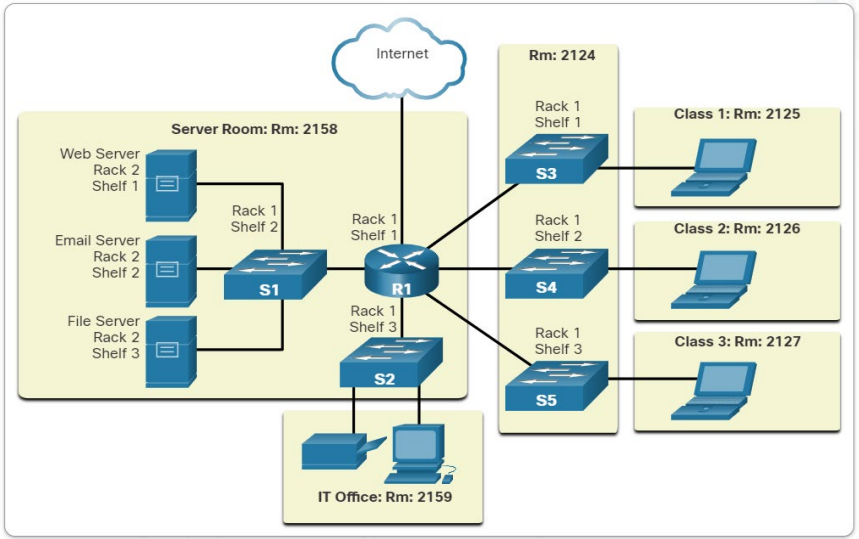
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AAA Accounting Logs

- Centralized AAA also enables the use of the Accounting method.
- Accounting records from all devices are sent to centralized repositories, which simplifies auditing of user actions.
- AAA Accounting collects and reports usage data in AAA logs that 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.
- 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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AAA Accounting Logs (Cont.)



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.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

AAA Accounting Logs (Cont.)

The table displays the various types of accounting information that can be collected:

Type of Accounting Information	Description
Network Accounting	It captures information for all PPP sessions, including packet and byte counts.
Connection Accounting	It captures information about all outbound connections made from the AAA client, such as by SSH
EXEC Accounting	It 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	It captures information about all system-level events (for example, when the system reboots or when accounting is turned on or off).
Command Accounting	It captures information about the EXEC shell commands for a specified privilege level, as well as the 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 connections that have passed user authentication. The additional feature of generating “stop” records for connections that fail to authenticate as part of user authentication is also supported.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Packet Tracer - Configure Server-Based Authentication with TACACS+ and RADIUS

In this Packet Tracer activity, you will complete the following objectives:

- Configure server-based AAA authentication using TACACS+.
- Verify server-based AAA authentication from the PC-B client.
- Configure server-based AAA authentication using RADIUS.
- Verify server-based AAA authentication from the PC-C client.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

13.5 Access Control Summary

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module?

- Physical access controls are actual barriers deployed to prevent direct physical contact with systems.
- Logical access controls are hardware and software solutions used to manage access resources and systems.
- Administrative access controls involves three security services: authentication, authorization, and accounting.
- Identification enforces the rules established by the authorization process.
- Authorization controls what a user can and cannot do on the network after successful authentication.
- Accountability traces an action back to a person or process making the change to the system.
- The CIA triad consists of confidentiality, integrity, and availability.
- Zero trust is a comprehensive approach to securing all access across networks, applications, and environments.
- Access control methods include DAC, MAC, RBAC, ABAC, RBAC, and TAC.
- Privilege escalation is a common exploit where vulnerabilities in servers or access control systems are exploited to grant access to an unauthorized user or software process.
- Account types can include administrator accounts, user accounts, service accounts, and guest accounts.
- Permission levels can be assigned to files and folders to include full control, modify, read and execute, write, and read.
- Robust practices for securing privileged accounts must be taken because they are often the target of cybercriminals.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What Did I Learn in this Module?

- Authentication management aims to ensure secure sign in while still providing ease of use.
- HMAC uses an encryption key with a hash function to authenticate a web user.
- An authentication protocol authenticates data between two entities to prevent unauthorized access.
- 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.
- AAA systems provide the necessary framework to enable scalable security.
- AAA authentication can be used to authenticate users for local 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 and Server-based AAA Authentication.
- Centralized AAA is more scalable and manageable than local AAA and is the preferred AAA implementation.
- A centralized AAA system can leverage Active Directory or LDAP for user authentication and group membership, while maintaining its own authorization and accounting databases.
- Devices communicate with the centralized AAA server using with the RADIUS or TACACS+ protocols.
- Centralized AAA also enables the use of the accounting method that reports usage data in AAA logs.
- Various types of accounting information that can be collected are network accounting, connection accounting, EXEC accounting, system accounting, command accounting, and resource accounting.

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential