1. Securing Configuration Access to Network Devices:

Protecting users starts with securing the devices that carry user information.

1. Secure the Network Infrastructure:

Critical to overall network security, includes routers, switches, servers, endpoints, and other devices. Routers direct traffic and are primary attack targets. Types of network setups:

* + Single Router: Connects the protected network to the internet.
  + Defense-in-Depth: Uses multiple layers of security, including edge router, firewall, and internal router.
  + DMZ: Used for servers accessible from the internet, set up between two routers.

1. Three Areas of Router Security:
   * Physical: Place router in a secure, locked room accessible only to authorized personnel. Use UPS or backup power generator.
   * Operating System: Configure router with maximum memory, use the latest stable OS version, and keep secure backups of OS images and configuration files.
   * Router Hardening: Ensure only authorized personnel have access, disable unused ports and interfaces, and disable unnecessary services.
2. Secure Administrative Access:

Important to prevent unauthorized access that could alter routing parameters or gain access to other systems.

* + Restrict device accessibility
  + Log and account for all access
  + Authenticate access
  + Authorize actions
  + Present legal notification
  + Ensure data confidentiality

1. Secure Local and Remote Access:
   * Local Access: Requires physical access to the router using a console cable.
   * Remote Access: Uses Telnet, SSH, HTTP, HTTPS, or SNMP connections from a local or remote computer.
2. Passwords:
   * Use a mix of upper and lower case letters, numbers, and special characters, with a recommended length of 12 characters.
   * Configuring passwords for different access levels:
     + Console password: Secures user EXEC mode access.
     + Privileged Access or Enable mode password: Provides access to all IOS commands.
     + Remote Access through SSH/Telnet: Secures vty lines.
3. Encrypt Passwords:

Ensure passwords remain secret by encrypting all plaintext passwords, setting a minimum password length, deterring brute-force attacks, and disabling inactive privileged EXEC mode access.

* + Example:

**Sw-Flocr-1(config)#** service password-encryption

1. Password Security:

Ensure all configured passwords have a minimum length and deter brute-force attacks using login block-for. Example configuration:

* + Set minimum password length and block login attempts:

**RI(config)# service password-encryption**

**RI(config)# security passwords min-length 8**

**RI(config)# login block-for 120 attempts 3 within 60**

1. Hash Function for Storing Passwords:

Use hash functions to store passwords securely by creating a Message Digest. The enable secret command generates an MD5 hash and stores it instead of the actual password.

* + Example command:

**Router(config)# enable secret fred**

1. Alternate Secret Password Algorithms:

Use type 8 or type 9 passwords for better security. These types use SHA encryption.

* + Example command:

**Router(config)# enable algorithm-type {md5 | scrypt | sha256 | secret} unencrypted password**

1. Enhance the Login Process:
   * Login blocking to react to repeated failed login attempts.
   * Use ACLs to permit legitimate connections.
   * Display banners for legal notification.
2. Login Enhancement Features:
   * login block-for to defend against DoS attacks.
   * login quiet-mode to allow logins only from permitted hosts.
   * login delay to specify wait time between unsuccessful attempts.
   * login on-success and login on-failure to log login attempts.
   * Example commands:

**RI(config)#** **login block-for seconds attempts tries within seconds**

**RI(config)#** **login quiet-mode access-class {acl-name | acl-number}**

**RI(config)# login delay seconds**

**RI(config)# login on-success log [every login]**

**RI(config)# login on-failure log [every login]**

1. Configuring SSH (Secure Shell):

Always use SSH for secure remote access. Steps to enable SSH:

* + Step 1: Configure a unique device hostname.
  + Step 2: Configure the IP domain name.
  + Step 3: Generate a key to encrypt SSH traffic.
  + Step 4: Verify or create a local database entry.
  + Step 5: Authenticate against the local database.
  + Step 6: Enable vty inbound SSH sessions.
  + Example configuration:

**Router#** configure terminal

**Router(config**)# **hostname R1**

**R1(config)#** **ip domain name span.com**

**R1(config)#** **crypto key generate rsa general-keys modulus 1024**

**R1(config)#** **username Bob secret cisco**

**R1(config)#** **line vty 0 4**

**R1(config-line)# login local**

**R1(config-line)# transport input ssh**

**R1(config-line)# exit**

1. Enhance SSH Login Security:
   * Verify optional SSH command settings using show ip ssh.
   * Modify timeout interval and number of consecutive retries.
   * Example commands:

**Router(config)#** **ip ssh time-out 60**

**Router(config)#** **ip ssh authentication-retries 2**

1. Connecting to an SSH-Enabled Router:

Verify client connections using show ssh. Routers can act as both SSH servers and clients.

* + Example command:

**R2#** **ssh -l Bob 152.168.2.101**