IOS Security

- When a Cisco router or switch is received from the factory no security is configured
- You can access the command line via a console cable with no password required
- One of the first tasks is to configure security to ensure that only authorised administrators can access the device

IOS Command Hierarchy

- > = User Exec mode
- # = Privileged Exec moe (“Enable”)
- (config)# = Global Confuration mode (“Configure Terminal”)
- (config-if)# = Interface Configuration mode (“Interface x”)

Basic Line Level Security

- Minimal password security can be configured through the use of static, locally defined passwords at three different levels:
    - Console line – accessing User Exec mode when connecting via a console cable
    - Virtual terminal VTY line – accessing User Exec mode when connecting remotely via Telnet or SSH Secure Shell
    - Privileged Exec Mode – entering the ‘enable’ command

- The levels can be used independently or in combination with each other.
- They can use the same or different passwords.

Basic Console Security

- Only one administrator can connect over a console cable at a time so the line number is always 0.
- ‘Login’ with no following keywords requires the administrator to enter the password configured at the line level to log in

    - *R1(config)#line console 0*
    - *R1(config-line)#password Flackbox1*
    - *R1(config-line)#login*

Switch Management IP Address

- A Layer 2 Switch is not IP routing aware
- It does however support a single IP address for management
- A default gateway also needs to be configured to allow connectivity to other subnets

Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.0.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway 192.168.0.1

Basic Telnet Security

- An administrator can use Telnet to connect to the CLI of a router or switch remotely over an IP connection
- IOS devices do not accept incoming Telnet sessions by default
- An IP address and virtual terminal VTY line access must be configured
- Multiple administrators can connect at the same time. Lines are allocated on a first come first served basis
- If all configured lines are in use then additional administrators will not be able to login

R1(config)#line vty 0 15
R1(config-line)#password Flackbox2
R1(config-line)#login

Exec Timeout

- An administrator will be logged out after 10 minutes of inactivity by default. This applies to both the console and VTY lines
- You can edit this value with the exec-timeout command
- *no exec-timeout* or *exec-timeout 0* allows an administrator to stay logged in indefinitely

R1(config)#line con 0
R1(config-line)#exec-timeout 15
R1(config)#line vty 0 15
R1(config-line)#exec-timeout 5 30

Securing VTY Lines with Access Lists

- You can apply an Access List to control access to the VTY lines
- This can be used to limit Telnet and SSH access to only your administrator workstations

R1(config)#access-list 1 permit host 10.0.0.10
R1(config)#line vty 0 15
R1(config-line)#login
R1(config-line)#password Flackbox3
R1(config-line)#access-class 1 in

Basic Privileged Exec Security

- When you connect over the console or a VTY line you will land at the User Exec prompt which has a very limited set of commands available
- To get superuser access you use the 'enable' command to invoke Privileged Exec mode
- This can be secured with a password
- Disadvantage: enable password can be viewed in the show run config

R1(config)#enable password Flackbox3

Enable Secret

- An enable secret performs the **same function as the enable password**
- The enable secret is always shown **in an encrypted format** in the running configuration
- If both an enable password and enable secret are configured, the enable secret supersedes the enable password which is no longer used
- **Best practice is to configure an enable secret but not an enable password**

Encrypting Passwords

Line level passwords can also be viewed in plain text in the running configuration by default.

```
R1#show run
!
enable secret 5 $1$mERr$ABB9Y2FkwbWuPLfUgLUxf1
enable password Flackbox3
!
line con 0
password Flackbox1
login
!
line vty 0 4
password Flackbox2
login
line vty 5 15
password Flackbox2
login
```

Service Password-Encryption

- The service password encryption command encrypts all passwords in the running configuration
- **It is best practice to enable this**

R1(config)#service password-encryption

```
R1#show run
!
service password-encryption
!
enable secret 5 $1$mERr$ABB9Y2FkwbWuPLfUgLUxf1
enable password 7 0807404F0A1207180A58
!
line con 0
password 7 0807404F0A1207180A5A
login
!
line vty 0 4
password 7 0807404F0A1207180A59
login
line vty 5 15
password 7 0807404F0A1207180A59
login
```

Username Level Security

- More granular security can be provided by configuring individual usernames and passwords for different administrators

R1(config)#username admin1 secret Flackbox1
R1(config)#username admin2 secret Flackbox2
R1(config)#line console 0
R1(config-line)#login local (use local usernames)
R1(config)#line vty 0 15
R1(config-line)#login local

```
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open

User Access Verification

Username: admin1
Password: <Flackbox1>
R1>
```

Privilege Levels

- There are 16 privilege levels of admin access (0-15) available on a Cisco router or switch
- Usernames can be assigned a privilege level. The default level is 1.
- You can also configure different passwords for direct access to the different privilege levels
- Each available command in IOS can be assigned a privilege level. An administrator must be logged in with that privilege level or higher to run the command
- By default, three levels of privilege are used - zero, user, and privileged. All commands are at one of these three levels by default
- Zero-level access allows only five commands—logout, enable, disable, help, and exit.
- User level (level 1) provides very limited read-only access to the router. When you enter User Exec Mode you're at Privilege Level 1 by default
- Privileged level (level 15) provides complete control over the router. When you enter Privileged Exec Mode with the 'enable' command you're at Level 15 by default

R1(config)#username admin1 secret Flackbox1
R1(config)#username admin2 privilege 15 secret Flackbox2
R1(config)#line console 0
R1(config-line)#login local
R1(config)#line vty 0 15
R1(config-line)#login local

```
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open

User Access Verification

Username: admin1
Password: <Flackbox1>
R1>
R1>show privilege
Current privilege level is 1
```

Configuring Command Privilege Levels Example

Only admin2 has *superuser* privileges
R1(config)#username admin1 secret Flackbox1
R1(config)#username admin2 privilege 15 secret Flackbox2
R1(config)#username admin3 privilege 5 secret Flackbox3

Change command privilege level. Now also admin3 can execute *show run conf*

R1(config)#privilege exec level 5 show running-config

R1(config)#enable secret secret1 (sets password for privilege level 15)
R1(config)#enable secret level 5 secret2 (sets password for privilege level 5)

```
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open
User Access Verification
Username: admin1
Password: <Flackbox1>

R1>show run
^
% Invalid input detected at '^' marker.

R1>enable 5
Password: <secret2>
R1#show run
Building configuration...


Current configuration : 1380 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
```

Telnet vs SSH

- All Telnet communications cross the network in plain text
- If somebody sniffs the traffic using a tool such as Wireshark they can see all the commands you enter including your username and password
- All SSH Secure Shell traffic is encrypted
- If somebody sniffs the traffic they cannot read it
- Best practice is to disable Telnet and only allow SSH for administrator CLI access

Enable SSH

- A digital certificate with a key length of at least 768 bits must be generated to enable SSH encryption

```
R1(config)#ip domain-name flackbox.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.flackbox.com
Choose the size of the key modulus in the range of 360 to 2048
for your General Purpose Keys. Choosing a key modulus greater
than 512 may take a few minutes.

How many bits in the modulus [512]: 768
% Generating 768 bit RSA keys, keys will be non-
exportable...[OK]
```

Disable Telnet

- VTY lines are used for both Telnet and SSH connections
- Access is allowed for both by default
- A username is required for SSH access (line level passwords are not supported)

R1(config)#username Flackbox secret Flackbox1
R1(config)#line vty 0 15
R1(config-line)#transport input ssh (telnet not added)
R1(config-line)#login local (use local usernames)
R1(config-line)#exit
R1(config)#ip ssh version 2 (limit SSH to v2)

AAA Server

- Configuring line level security or local usernames on each device has a serious scalability limitation
- If a password has to be added, changed or removed it needs to be done on all devices
- An external AAA server can be used to centralise this instead
- Multiple AAA servers can be implemented for redundancy

- AAA servers provide Authentication, Authorization and Accounting.
- Authentication verifies somebody is who they say they are. This is most commonly achieved with a username and password.
- Authorization specifies what a particular user is allowed to do, such as running a particular command.
- Accounting keeps track of the actions a user has carried out.
- Authorization and Accounting are optional. Authentication is mandatory if Authorization and/or Accounting are used.

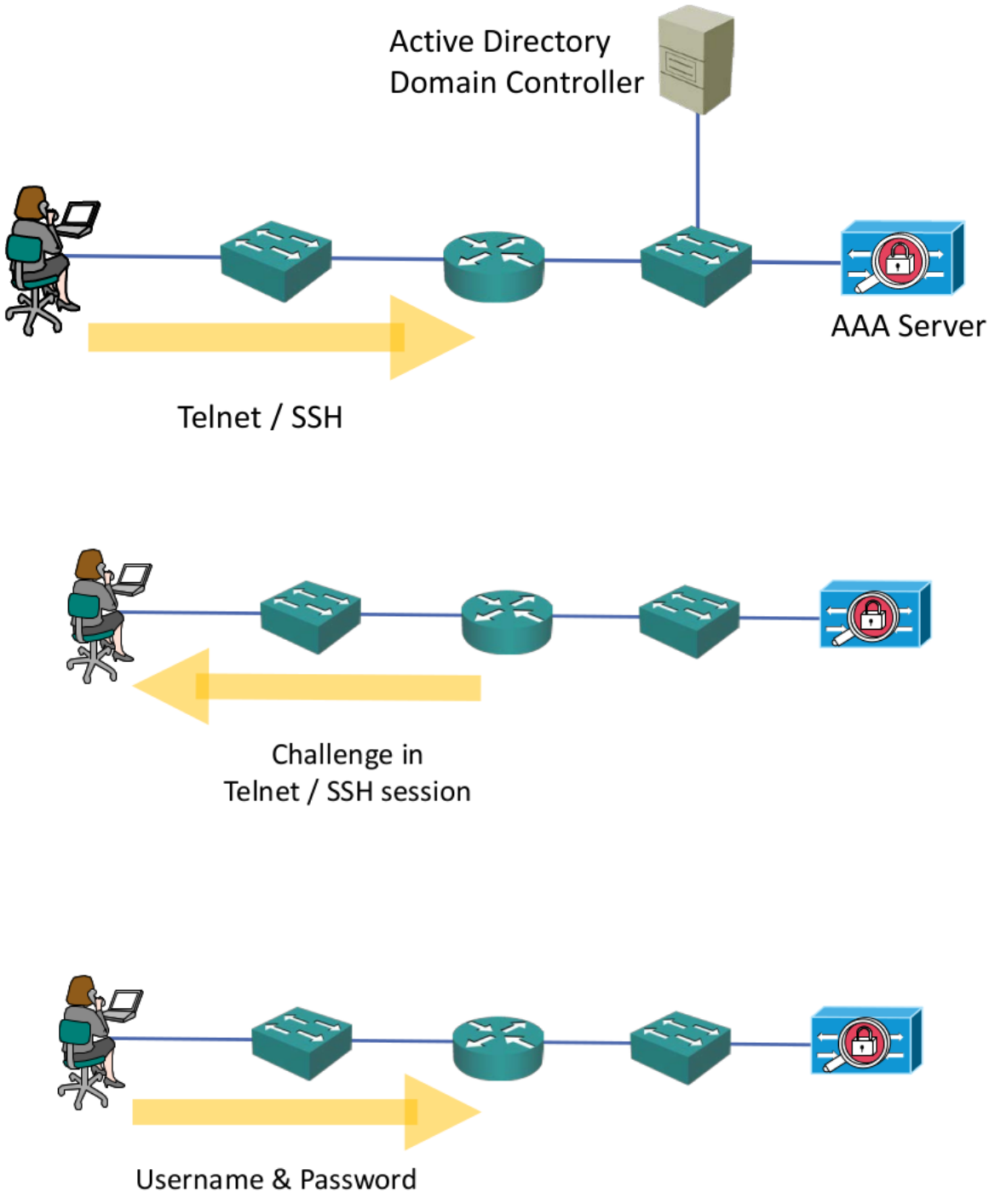
RADIUS and TACACS+

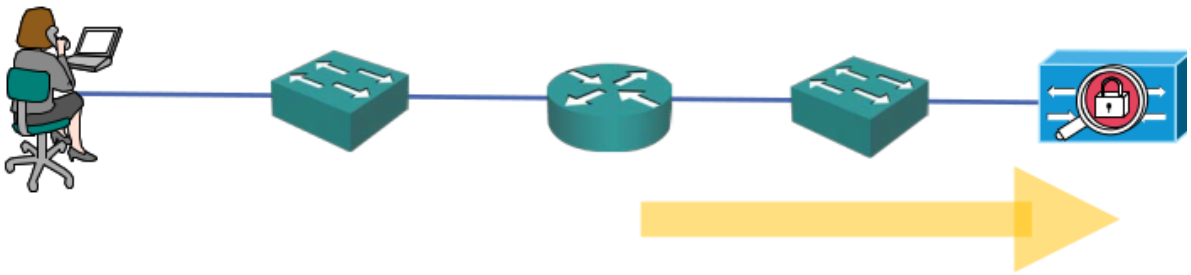
- The protocols which are used for AAA services are RADIUS and TACACS+
- Both are open standards, although vendors may add their own proprietary extensions
- Many vendor’s AAA servers support both protocols
- RADIUS is commonly used for end user level services, such as VPN access
- TACACS+ is commonly used for administrator access on Cisco devices as it has more granular authorization capabilities

Cisco AAA Servers

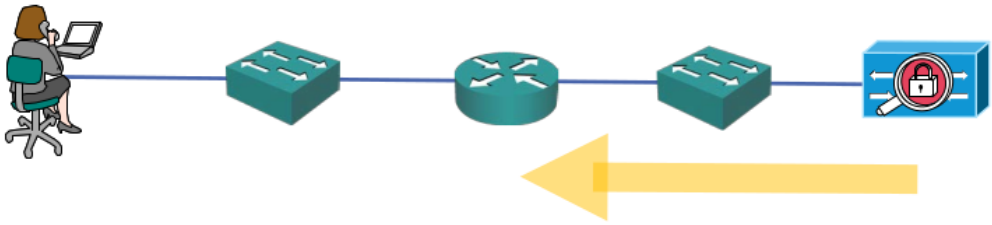
- Cisco's AAA server is the Identity Services Engine (ISE)
- They also offered the Access Control Server (ACS) for a long time but it is now end of sale

Active Directory Integration

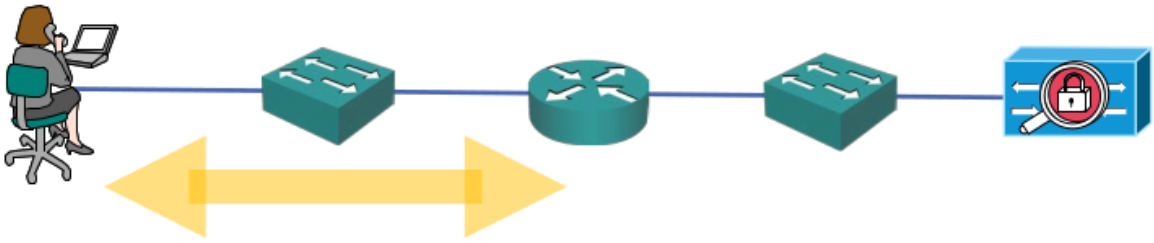




Username & Password
(RADIUS / TACACS+)

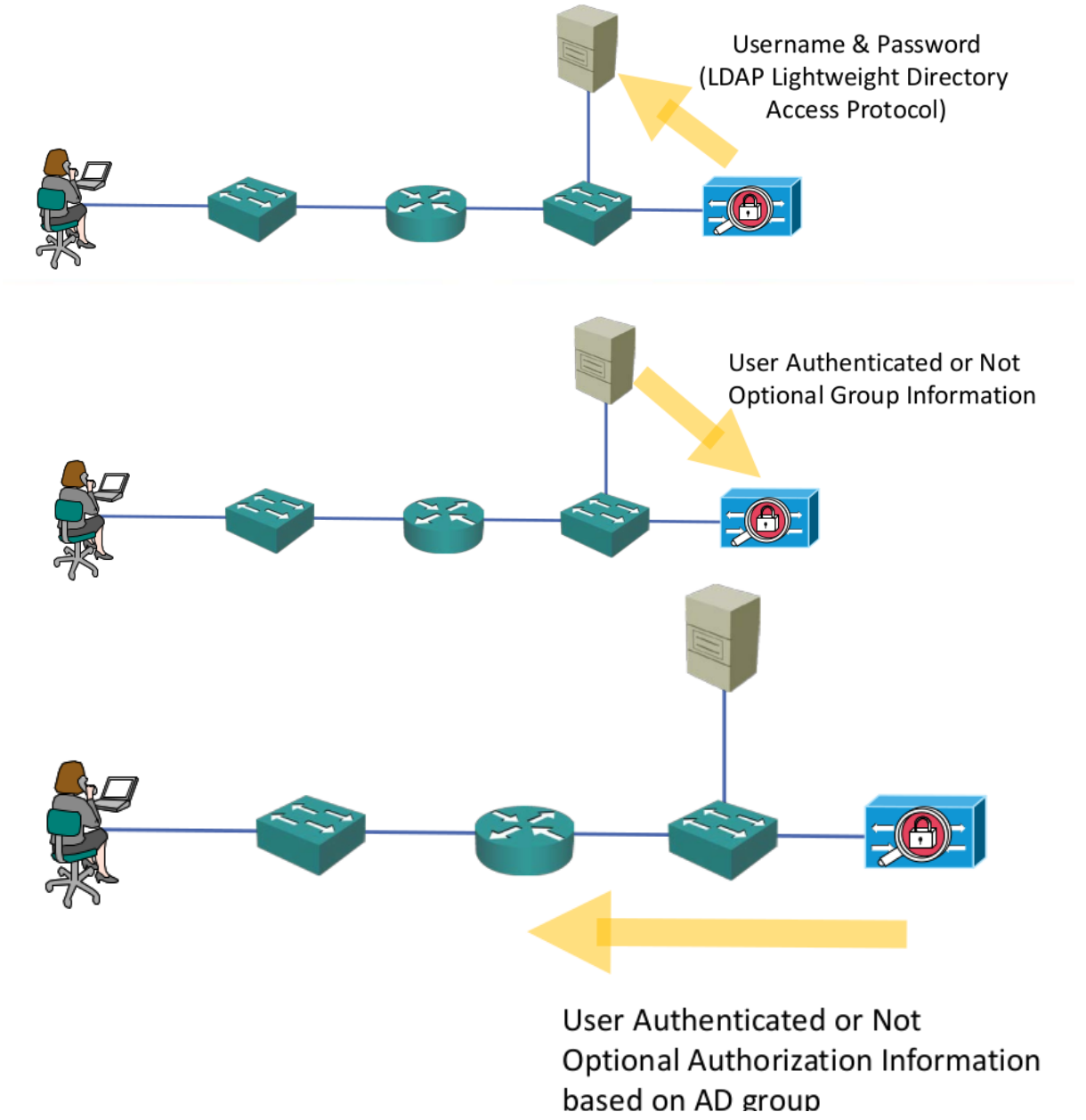


User Authenticated or Not
Optional Authorization Information



Telnet / SSH

OR


Username & Password
(LDAP Lightweight Directory
Access Protocol)
User Authenticated or Not
Optional Group Information
User Authenticated or Not
Optional Authorization Information
based on AD group
Telnet / SSH

RADIUS/TACACS+ Configuration

Old RADIUS Configuration

R1(config)#username BackupAdmin secret Flackbox1 (configure a local user in case connectivity to the AAA server is lost)

R1(config)#aaa new-model

R1(config)#radius-server host 10.10.10.10 key Flackbox1
R1(config)#radius-server host 10.10.10.11 key Flackbox2

R1(config)#aaa group server radius FB-RG (optional)
R1(config-sg-radius)#server 10.10.10.10
R1(config-sg-radius)#server 10.10.10.11

R1(config)#aaa authentication login default group radius local
(Use all RADIUS servers) OR:
R1(config)#aaa authentication login default group FB-RG local
(Use servers in specified group)

New RADIUS Configuration

R1(config)#radius-server host 10.10.10.10
Warning: This CLI will be deprecated soon. Please move to radius server <name> CLI.

R1(config)#aaa new-model

R1(config)#radius server Server1
R1(config-radius-server)# address ipv4 10.10.10.10
R1(config-radius-server)# key Flackbox1

R1(config)#radius server Server2
R1(config-radius-server)# address ipv4 10.10.10.11
R1(config-radius-server)# key Flackbox2

R1(config-radius-server)#aaa group server radius FB-RG
R1(config-sg-radius)# server name Server1
R1(config-sg-radius)# server name Server2

R1(config-sg-radius)#aaa authentication login default group FB-RG local

Old TACACS+ Configuration

R1(config)#username BackupAdmin secret Flackbox1

R1(config)#aaa new-model

R1(config)#tacacs-server host 10.10.10.10 key Flackbox1
R1(config)#tacacs-server host 10.10.10.11 key Flackbox2

R1(config)#aaa group server tacacs+ FB-TG
R1(config-sg-tacacs+)#server 10.10.10.10
R1(config-sg-tacacs+)#server 10.10.10.11

R1(config)#aaa authentication login default group FB-TG local

New TACACS+ Configuration

R1(config)#tacacs-server host 10.10.10.10
Warning: This CLI will be deprecated soon. Please move to tacacs server <name> CLI.

R1(config)#username BackupAdmin secret Flackbox1

R1(config)#aaa new-model
R1(config)#tacacs server Server1
R1(config-server-tacacs)# address ipv4 10.10.10.10
R1(config-server-tacacs)# key Flackbox1

R1(config)#tacacs server Server2
R1(config-server-tacacs)# address ipv4 10.10.10.11
R1(config-server-tacacs)# key Flackbox2

R1(config-radius-server)#aaa group server tacacs+ FB-TG
R1(config-sg-tacacs+)# server name Server1
R1(config-sg-tacacs+)# server name Server2

R1(config-sg-tacacs+)#aaa authentication login default group FB-TG local

Best Practices

Login and Exec Banners

- Messages can be displayed in the CLI before and/or after an administrator logs in to a Cisco IOS device
- This is most commonly used to display security warnings

```
R1(config)#banner login ‟ (hit enter here)
Enter TEXT message. End with the character '"'.
Authorized users only‟

R1(config)#banner exec "
Enter TEXT message. End with the character '"'.
Please log out immediately if you are not an authorized
administrator"

C:\> telnet 10.0.0.1
Trying 10.0.0.1 …Open

Authorized users only

User Access Verification
Password: Flackbox3
Please log out immediately if you are not an authorized
administrator
R1>enable
```

Disable Unused Services

- It is best practice to disable unused services
- This reduces the attack surface and also the load on the device
- HTTPS is sometimes used by GUI administration tools but HTTP should be disabled
- CDP should also be disabled in highly secure environments

R1(config)#no ip http server
R1(config)#no cdp run

Time Synchronisation - NTP

- All servers and infrastructure devices in your network should be synchronised to the same time
- This aids in troubleshooting as logs will report the correct time that events occurred
- It is also required by several security features such as Kerberos authentication and digital certificates

NTP Network Time Protocol

- Servers and infrastructure devices can use their own internal clock or synchronise with an external NTP server
- An NTP server should be used to ensure all devices have the same time
- A Cisco router can function as an NTP server and/or client

```
R1(config)#clock timezone PST -8
R1(config)#ntp server 10.0.1.100 (configures router to be NTP client)
R1(config)#ntp master (configures router to be NTP server)

R1#show clock
16:19:36.51 PST Mon Oct 2 2017

R1#show ntp status
Clock is synchronized, stratum 2, reference is 10.0.1.100
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19
reference time is DD53255C.0000039C (00:16:28.924 UTC Tue Jan 2 2018)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.02 msec, peer dispersion is 0.02 msec.
```