Device Security

16.4.1

Cisco AutoSecure

One area of networks that requires special attention to maintain security is the devices. You probably already have a password for your computer, smart phone, or tablet. Is it as strong as it could be? Are you using other tools to enhance the security of your devices? This topic tells you how.

The security settings are set to the default values when a new operating system is installed on a device. In most cases, this level of security is inadequate. For Cisco routers, the Cisco AutoSecure feature can be used to assist securing the system, as shown in the example.

```
Router# auto secure
                --- AutoSecure Configuration ---
*** AutoSecure configuration enhances the security of
the router but it will not make router absolutely secure
from all security attacks ***
```

In addition, there are some simple steps that should be taken that apply to most operating systems:

- Default usernames and passwords should be changed immediately.
- Access to system resources should be restricted to only the individuals that are authorized to use those resources.
- Any unnecessary services and applications should be turned off and uninstalled when possible.

Often, devices shipped from the manufacturer have been sitting in a warehouse for a period of time and do not have the most up-to-date patches installed. It is important to update any software and install any security patches prior to implementation.

16.4.2

Passwords

To protect network devices, it is important to use strong passwords. Here are standard guidelines to follow:

- Use a password length of at least eight characters, preferably 10 or more characters. A longer password is a more secure password.
- Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces, if allowed.
- Avoid passwords based on repetition, common dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
- Deliberately misspell a password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Change passwords often. If a password is unknowingly compromised, the window of opportunity for the threat actor to use the password is limited.
- Do not write passwords down and leave them in obvious places such as on the desk or monitor.

The tables show examples of strong and weak passwords.

Weak Passwords

Weak Password	Why it is Weak
secret	Simple dictionary password
smith	Maiden name of mother
toyota	Make of a car
bob1967	Name and birthday of the user
Blueleaf23	Simple words and numbers

Strong Passwords

Strong Password	Why it is Strong
b67n42d39c	Combines alphanumeric characters
12^h u4@1p7	Combines alphanumeric characters, symbols, and includes a space

On Cisco routers, leading spaces are ignored for passwords, but spaces after the first character are not. Therefore, one method to create a strong password is to use the space bar and create a phrase made of many words. This is called a passphrase. A passphrase is often easier to remember than a simple password. It is also longer and harder to guess.

16.4.3

Additional Password Security

Strong passwords are only useful if they are secret. There are several steps that can be taken to help ensure that passwords remain secret on a Cisco router and switch including these:

- Encrypting all plaintext passwords
- Setting a minimum acceptable password length
- Deterring brute-force password guessing attacks
- Disabling an inactive privileged EXEC mode access after a specified amount of time.

As shown in the sample configuration in the figure, the **service password-encryption** global configuration command prevents unauthorized individuals from viewing plaintext passwords in the configuration file. This command encrypts all plaintext passwords. Notice in the example, that the password “cisco” has been encrypted as “03095A0F034F”.

To ensure that all configured passwords are a minimum of a specified length, use the **security passwords min-length** *length* command in global configuration mode. In the figure, any new password configured would have to have a minimum length of eight characters.

Threat actors may use password cracking software to conduct a brute-force attack on a network device. This attack continuously attempts to guess the valid passwords until one works. Use the **login block-for # attempts # within #** global configuration command to deter this type of attack. In the figure for example, the **login block-for 120 attempts 3 within 60** command will block vty login attempts for 120 seconds if there are three failed login attempts within 60 seconds.

Network administrators can become distracted and accidently leave a privileged EXEC mode session open on a terminal. This could enable an internal threat actor access to change or erase the device configuration.

By default, Cisco routers will logout an EXEC session after 10 minutes of inactivity. However, you can reduce this setting using the **exec-timeout** *minutes seconds* line configuration command. This command can be applied online console, auxiliary, and vty lines. In the figure, we are telling the Cisco device to automatically disconnect an inactive user on a vty line after the user has been idle for 5 minutes and 30 seconds.

```
R1(config)# service password-encryption
R1(config)# security passwords min-length 8
R1(config)# login block-for 120 attempts 3 within 60
R1(config)# line vty 0 4
R1(config-line)# password cisco123
R1(config-line)# exec-timeout 5 30
R1(config-line)# transport input ssh
R1(config-line)# end
R1#
R1# show running-config | section line vty
line vty 0 4
 password 7 094F471A1A0A
 exec-timeout 5 30
 login
 transport input ssh
R1#
```

16.4.4

Enable SSH

Telnet simplifies remote device access, but it is not secure. Data contained within a Telnet packet is transmitted unencrypted. For this reason, it is highly recommended to enable Secure Shell (SSH) on devices for secure remote access.

It is possible to configure a Cisco device to support SSH using the following six steps:

Step 1. Configure a unique device hostname. A device must have a unique hostname other than the default.

Step 2. Configure the IP domain name. Configure the IP domain name of the network by using the global configuration mode command **ip domain name** *name*.

Step 3. Generate a key to encrypt SSH traffic. SSH encrypts traffic between source and destination. However, to do so, a unique authentication key must be generated by using the global configuration command **crypto key generate rsa general-keys modulus** *bits*. The modulus *bits* determines the size of the key and can be configured from 360 bits to 2048 bits. The larger the bit value, the more secure the key. However, larger bit values also take longer to encrypt and decrypt information. The minimum recommended modulus length is 1024 bits.

Step 4. Verify or create a local database entry. Create a local database username entry using the **username** global configuration command. In the example, the parameter **secret** is used so that the password will be encrypted using MD5.

Step 5. Authenticate against the local database. Use the **login local** line configuration command to authenticate the vty line against the local database.

Step 6. Enable vty inbound SSH sessions. By default, no input session is allowed on vty lines. You can specify multiple input protocols including Telnet and SSH using the **transport input {ssh | telnet}** command.

As shown in the example, router R1 is configured in the span.com domain. This information is used along with the bit value specified in the **crypto key generate rsa general-keys modulus** command to create an encryption key.

Next, a local database entry for a user named Bob is created. Finally, the vty lines are configured to authenticate against the local database and to only accept incoming SSH sessions.

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# ip domain name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com % The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#
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
R1(config)#
```

16.4.5

Disable Unused Services

Cisco routers and switches start with a list of active services that may or may not be required in your network. Disable any unused services to preserve system resources, such as CPU cycles and RAM, and prevent threat actors from exploiting these services. The type of services that are on by default will vary depending on the IOS version. For example, IOS-XE typically will have only HTTPS and DHCP ports open. You can verify this with the **show ip ports all** command, as shown in the example.

```
Router# show ip ports all
Proto Local Address              Foreign Address            State       PID/Program Name
TCB       Local Address              Foreign Address            (state)
tcp   :::443                    :::*                       LISTEN      309/[IOS]HTTP CORE
tcp   *:443                      *:*                        LISTEN      309/[IOS]HTTP CORE
udp   *:67                        0.0.0.0:0                              387/[IOS]DHCPD Receive
Router#
```

IOS versions prior to IOS-XE use the **show control-plane host open-ports** command. We mention this command because you may see it on older devices. The output is similar. However, notice that this older router has an insecure HTTP server and Telnet running. Both of these services should be disabled. As shown in the example, disable HTTP with the **no ip http server** global configuration command. Disable Telnet by specifying only SSH in the line configuration command, **transport input ssh**.

```
Router# show control-plane host open-ports
Active internet connections (servers and established)
Prot        Local Address      Foreign Address                Service    State
 tcp                *:23                *:0                  Telnet   LISTEN
 tcp                *:80                *:0              HTTP CORE    LISTEN
 udp                *:67                *:0           DHCPD Receive   LISTEN
Router# configure terminal
Router(config)# no ip http server
Router(config)# line vty 0 15
Router(config-line)# transport input ssh
```

16.4.6

Packet Tracer - Configure Secure Passwords and SSH

The network administrator has asked you to prepare RTA and SW1 for deployment. Before they can be connected to the network, security measures must be enabled.

Configure Secure Passwords and SSH

Configure Secure Passwords and SSH

16.4.7

Lab - Configure Network Devices with SSH

In this lab, you will complete the following objectives:

- Part 1: Configure Basic Device Settings
- Part 2: Configure the Router for SSH Access
- Part 3: Configure the Switch for SSH Access
- Part 4: SSH from the CLI on the Switch

Configure Network Devices with SSH