
Networkforyou
Welcome
To
Network for you
Lines and password protection
Networkforyou

Cisco Routers Security:

- Cisco Routers are not security device and it is made for Routing.
- There are many features present in Cisco Routers, which can be misused.
- Attacker can easily gain access to router and can take control over the network.
- Network infrastructure devices routers are the assets of an enterprise.
- Router plays an important role & thus need to be protected & configured accordingly.
- Cisco routers can be secure using many methods such as Physical Security.
- Enterprises focus on protecting data, servers; applications etc but forget about Router.

Enable Mode Passwords
R1(config)# enable password cisco R1(config)# do show run | include password R1(config)# service password-encryption https://www.ifm.net.nz/cookbooks/passwordcracker.html R1(config)# enable secret cisco R1(config)# do show run | include secret https://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html R1(config)# enable algorithm-type sha256 secret cisco R1(config)# do show running-config | include secret R1(config)# enable algorithm-type scrypt secret cisco R1(config)# do show running-config | include secret

Virtual Terminal Line (VTY):

- VTY stand for Virtual Terminal Lines or Virtual Teletype.
- We are access network device virtually so we will use Virtual Terminal line.
- VTY is a Command Line Interface (CLI) created in a router
- VTY is just way to access Router or switch CLI Remotely.
- VTY are logical connections from the network to the switch or routers.

Telnet:

- Telnet is a network protocol that provides a command - line interface to communicate with a device remotely.
- In simple words we can say Telnet is use to access device remotely from different location.

- Telnet is an application layer protocol which is use to remotely access network devices.
- Telnet is work on Protocol TCP & Port # 23.
- First, we need to configure Telnet in network device then we can do Telnet from different place

Router Telnet configuration:

Config t
Enable password 12345
Line vty 0 4 ---------- if we want to allow 5 people to access device remotely then we will use vty 0 4 i.e. Qty 5

Password cisco
Login

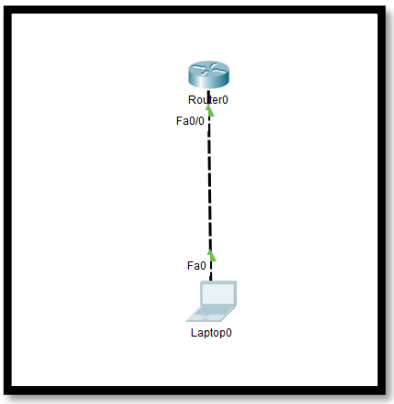
Or

Other Method

Config t
Username abc password abc

Enable password 12345
Line vty 0 4 ---------- if we want to allow 5 people to access device remotely then we will use vty 0 4 i.e. Qty 5

Password cisco
Login local



SSH: SSH (Secure Shell):

- SSH (Secure Shell) is a secure method for remote access as is include authentication and encryption. To do this, it uses an RSA public/private key pair.
- It works on Port number 22
- Very Secure Protocol
- SSH are two versions SSH Version 1 and SSH Version 2.
- Communication between server and client is encrypted in both SSH Version.
- SSH Version 2 is more Secure then SSH Version 1.

How to Configure SSH on CISCO IOS:

En
Config t
Hostname R1
Ip domain-name Networkforyou
Now we can generate the RSA Keypair:
Crypto key generate rsa
Then it will ask
The name for the keys will be: Branch2.Networkforyou
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]:

So we will choose let me choose 2048
Then we get

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

Then it will enable SSH

*Mar 1 5:21:55.540: %SSH-5-ENABLED: SSH 1.99 has been enabled

By default version 1 is enable . Now I am enabling to shh version 2

Then we will type ip ssh version 2

line vty 0 4
transport input ssh
login local
username admin password admin

How to access ssh:

Type
Ssh -l username IP
Password

Different between Telnet and SSH:

- Telnet and SSH protocols have the same purpose and both of them used to communicate to a remote device.
- Telnet is not secure because all the data would be sent in clear text including the passwords without authentication and encryption.
- where SSH is a Secure Protocol because it encrypts the data using authentication.

Cisco Routers Password Types:

Cisco Password	Crackability
Type 0	instant
Type 7	instant
Type 4	easy
Type 5	medium
Type 8	hard
Type 9	very hard

Type 0: The password will not be encrypted when router store it in Run/Start Files**: enable password cisco123**

Type 4: The password will be encrypted when router store it in Run/Start Files using SHA-256. Can be crack but will take long time. This is not the password string itself but the hash of the password. This type is deprecated starting from **IOS 15.3(3). enable secret 4 Rv4kArhts7yA2xd8BD2YTVbts**

Type 5: The password will be encrypted when router store it in Run/Start Files using MD5. Can be crack but will take long time. This is not the password string itself but the hash of the password. enable secret 5 00271A5307542A02D22842 OR enable secret cisco123

Type 7: The password will be encrypted when router store it in Run/Start Files using Vigenere cipher which any website with type7 reverser can crack it in less than one second. enable password cisco123 service password-encryption

Type 8:

The password will be encrypted when router store it in Run/Start Files using PBKDF2-SHA-256 starting from IOS 15.3(3). Password-Based Key Derivation Function 2 (PBKDF2) with Secure Hash Algorithm, 26-bits (SHA-256) as the hashing algorithm

enable algorithm-type sha256 secret cisco

show run | include enable

enable secret 8 8mTj4RZG8N9ZDOk$elY/asfm8kD3iDmkBe3hD2r4xcA/0oWS5V3os.O91u.

Type 9:

The password will be encrypted when router store it in Run/Start Files using scrypt as the hashing algorithm. Starting from IOS 15.3(3).

enable algorithm-type scrypt secret cisco

show run | include enable

enable secret 9 9WnArItcQHW/uuE$x5WTLbu7PbzGDuv0fSwGKS/KURsy5a3WCQckmJp0MbE