

Packet Tracer – Configure o SSH

Tabela de Endereçamento

Dispositivo	Interface	Endereço IP	Máscara de sub-rede
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objetivos

- ☒ ~~Parte 1: Proteger senhas~~
- ☒ ~~Parte 2: Criptografar comunicações~~
- ☒ ~~Parte 3: Verificar a implementação SSH~~

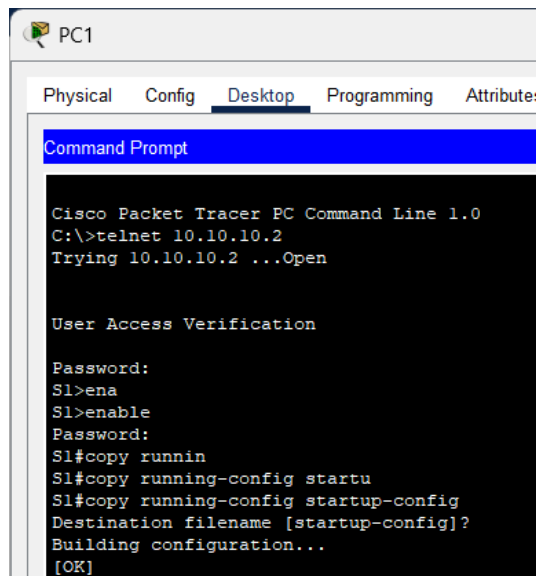
Histórico

O SSH deve substituir o Telnet nas conexões de gerenciamento. O Telnet utiliza a comunicação em texto claro de forma não segura. O SSH fornece segurança para conexões remotas, fornecendo criptografia forte de todos os dados transmitidos entre os dispositivos. Nesta atividade, você protegerá um switch remoto com criptografia de senha e SSH.

Instruções

Parte 1: Proteger senhas

- a. Usando o prompt de comando em **PC1**, execute Telnet para **S1**. A senha do EXEC do usuário e do EXEC privilegiado é **cisco**.
- b. Salve a configuração atual de forma que todos os erros que você cometa possam ser revertidos ligando e desligando **S1**.

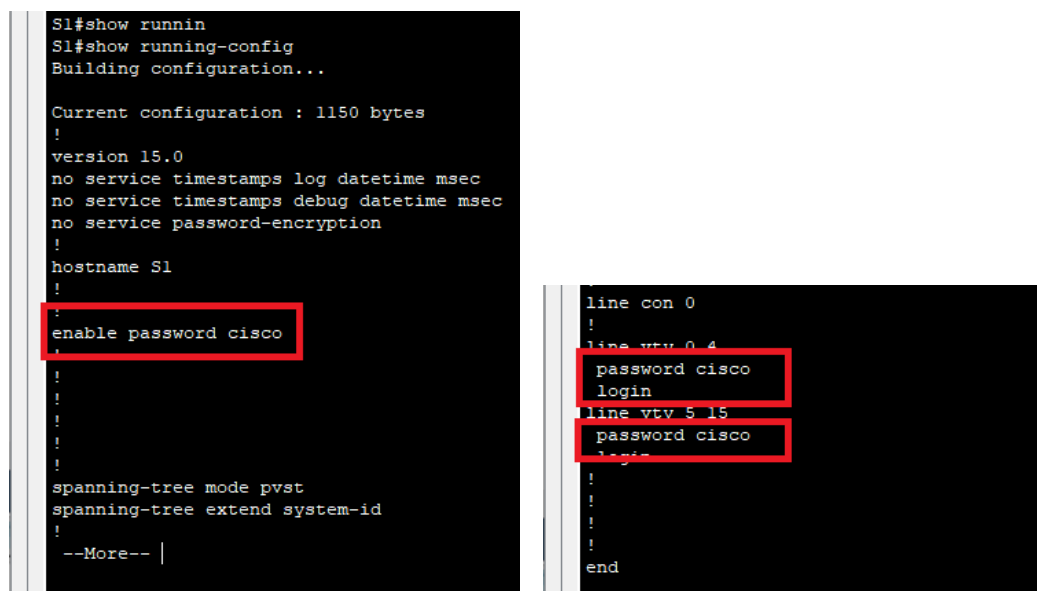


```
PC1
Physical Config Desktop Programming Attribute:
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open

User Access Verification

Password:
S1>ena
S1>enable
Password:
S1#copy runnin
S1#copy running-config startu
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

c. Exiba a configuração atual e observe que as senhas estão em texto claro.



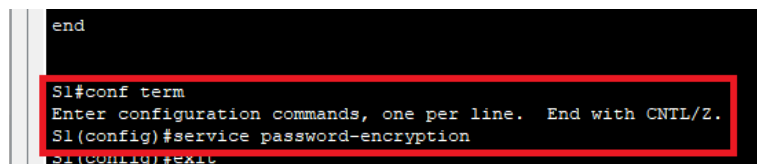
```
S1#show runnin
S1#show running-config
Building configuration...

Current configuration : 1150 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
:
enable password cisco
:
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
--More-- |

line con 0
!
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
!
!
!
end
```

Digite o comando que criptografa senhas em texto simples:

`S1(config)# service password-encryption`



```
end

S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#exit
```

d. Verifique se as senhas estão criptografadas.

```
S1#show running-config
Building configuration...

Current configuration : 1174 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
!
enable password 7 0822455D0A16
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
--More--

!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 10.10.10.2 255.255.255.0
!
!
!
!
!
line con 0
!
!
line vty 0 4
password 7 0822455D0A16
login
line vty 5 15
password 7 0822455D0A16
login
!
!
end
```

Parte 2: Criptografar comunicações

Etapa 1: Defina o nome de domínio IP e gere chaves de segurança.

Geralmente não é seguro usar o Telnet, pois os dados são transferidos em texto claro. Portanto, use SSH sempre que estiver disponível.

- Configure o nome de domínio como **netacad.pka**.

```
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#ip domain-name netacad-gabifreitas.pka
S1(config)#
S1(config)#
S1(config)#
S1(config)#
S1(config)#
S1(config)#
```

- As chaves seguras são necessárias para criptografar os dados. Gere as chaves RSA usando um comprimento de chave de 1024.

```
S1#
S1#
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#ip domain-name netacad-gabifreitas.pka
S1(config)#
S1(config)#
S1(config)#
S1(config)#
S1(config)#
S1(config)#crypto key generate rsa
The name for the keys will be: S1.netacad-gabifreitas.pka
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
S1(config)#
```

Etapa 2: Crie um usuário do SSH e configure as linhas de VTY para somente acesso SSH.

- a. Crie um usuário **administrator** com a senha **cisco**.

```
S1(config)#crypto key generate rsa
The name for the keys will be: S1.netacad-gabifreitas.pka
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#username administrator secret cisco
*Mar 1 4:4:35.672: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
S1(config)#
```

- b. Configure as linhas VTY para verificar o banco de dados de nome de usuário local para ver se há credenciais de login e para permitir acesso remoto apenas para SSH. Remova a senha da linha vty existente.

```
S1(config)#username administrator secret cisco
*Mar 1 4:4:35.672: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#no password cisco
S1(config-line)#exit
S1(config)#
```

Parte 3: Verificar a implementação SSH

- a. Saia da sessão Telnet e tente fazer login novamente usando o Telnet. A tentativa deverá falhar.

```
S1(config-line)#exit
S1(config)#exit
S1#exit

[Connection to 10.10.10.2 closed by foreign host]
C:\>
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open

[Connection to 10.10.10.2 closed by foreign host]
C:\>
```

- b. Tente fazer login usando o SSH. Digite **ssh** e pressione **Enter** sem nenhum parâmetro para revelar as instruções de uso de comando.

Dica: a opção **-l** é a letra “L”, não o número 1.

```
[Connection to 10.10.10.2 closed by foreign host]
C:\>
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open

[Connection to 10.10.10.2 closed by foreign host]
C:\>
C:\>
C:\>
C:\>
C:\>ssh
Cisco Packet Tracer PC SSH

Usage: SSH -l username target

C:\>ssh -l administrator 10.10.10.2

Password:

S1>
```

☐ Top

- c. Após o login com êxito, entre no modo EXEC privilegiado e salve as configurações. Se você não conseguir acessar o **S1**, desligue e ligue **S1** e comece novamente na Parte 1.

```
S1>en
Password:
S1#copy running-config start
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Conclusão

Cisco Packet Tracer - D:\02_Areas\studies\FATEC\2025-1\IRC011 - Protocolos e Roteamento em Redes de Computa

File Edit Options View Tools Extensions Window Help

Activity Results

You did not complete the activity. Please close this window and try again.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All Show Incorrect Items

Assessment Items	Status	Points	Component(s)	Feedback
Network				
S1				
DNS		0	Other	
IP Domain Name	Incorrect	20	Device Hardening ...	
Security		0	Other	
Modulus Bits	Correct	20	Device Hardening ...	
Service Password Encryption	Correct	20	Device Hardening ...	
User Names		0	Other	
(deprecated) Username	Correct	20	Device Hardening ...	
VTY Lines				
VTY Line 0				
Login	Correct	7	Device Hardening ...	
Password	Correct	6	Device Hardening ...	
Transport Input	Correct	7	Device Hardening ...	

Como eu adicionei meu nome ao IP Domain, ficou marcado como incompleto. Foi só alterar isso para concluir o exercício.

Cisco Packet Tracer - D:\02_Areas\studies\FATEC\2025-1\IRC011 - Protocolos e Roteamento em Re

File Edit Options View Tools Extensions Window Help

Activity Results

You did not complete the activity. Please close this window and try again.

Overall Feedback Assessment Items Connectivity Tests

Expand/Collapse All Show Only Incorrect Item

Assessment Items	Status	Points	Component(s)
Network			
S1			
DNS		0	Other
IP Domain Name	Correct	20	Device Hardening ...
Security		0	Other
Modulus Bits	Correct	20	Device Hardening ...
Service Password Encryption	Correct	20	Device Hardening ...
User Names		0	Other
(deprecated) Username	Correct	20	Device Hardening ...
VTY Lines			
VTY Line 0			
Login	Correct	7	Device Hardening ...
Password	Correct	6	Device Hardening ...
Transport Input	Correct	7	Device Hardening ...

Instruções

Parte 1: Senhas seguras

- Usando o prompt de comando em PC1, Telnet para S1. O usuário EXEC e a senha EXEC privilegiada são cisco.
- Salve a configuração atual para que quaisquer erros que você possa cometer possam ser revertidos, alternando o poder de S1.
- Mostre a configuração atual e observe que as senhas estão em texto sem formatação. Digite o comando que criptografa senhas em texto simples:
`S1(config)# service password-encryption`
- Verifique se as senhas estão criptografadas.

Parte 2: Criptografar as comunicações

Etapa 1: defina o nome do domínio IP e gere chaves seguras.

Geralmente, não é seguro usar o Telnet, porque os dados são transferidos em texto sem formatação. Portanto, use SSH sempre que estiver disponível.

- Configure o nome do domínio para ser **netacad.pka**.
- Chaves seguras são necessárias para criptografar os dados. Gere as chaves RSA usando um comprimento de chave 1024.

Etapa 2: Crie um usuário SSH e reconfigure as linhas VTY para acesso somente SSH.

- Crie um usuário **administrador** com **cisco** como a senha secreta.
- Configure as linhas VTY para verificar o banco de dados de nome de usuário local quanto a credenciais de login e permitir apenas o acesso remoto ao SSH. Remova a senha da linha vty existente.

Etapa 3: verificar a implementação do SSH

- Saia da sessão Telnet e tente efetuar login novamente usando o Telnet. A tentativa deve falhar.
- Tente fazer login usando SSH. Digite **ssh** e pressione **Enter** without any parameters to reveal the command usage instructions. Dica: A opção **-l** é a letra "l", não é o número 1.
- Após o login bem-sucedido, entre no modo EXEC privilegiado e salve a configuração. Se você não conseguiu acessar com êxito o S1, altere o poder e comece novamente na Parte 1.

Time Elapsed: 00:00:00 Completion: 100%

☒ Dock 1/1