Packet Tracer: Configuración de SSH

Topología

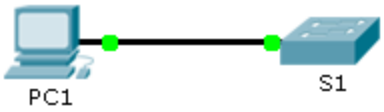


Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	NIC	10.10.10.10	255.255.255.0

Objetivos

Parte 1: Configuración del acceso para la administración remota por IPv4

Parte 2: Proteger las contraseñas

Parte 3: Cifrar las comunicaciones

Parte 4: Verificar la implementación de SSH

Aspectos básicos

Para el acceso a la administración remota de un switch, este se debe configurar con una dirección IP y una máscara de subred. Recuerde que para administrar un switch desde una red remota, se lo debe configurar con un gateway predeterminado. Se debe asignar una dirección IP a la interfaz virtual del switch (SVI). De manera predeterminada, el switch está configurado para que el control de la administración del switch se realice mediante la VLAN 1. Todos los puertos se asignan a la VLAN 1 de manera predeterminada. Por motivos de seguridad, se recomienda usar una VLAN de administración distinta de la VLAN 1.

SSH debe reemplazar a Telnet para las conexiones de administración. Telnet usa comunicaciones inseguras de texto no cifrado. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro de todos los datos transmitidos entre los dispositivos. En esta actividad, protegerá un switch remoto con el cifrado de contraseñas y SSH.

Parte 1: Configuración del acceso para la administración remota por IPv4

a. Configure contraseña **cisco** para acceder al modo privilegiado.

```
Switch(config)#enable secret cisco
Switch(config)#
```

Se va asignar una IP y un gateway predeterminado a la SVI configurando una VLAN cualquiera como VLAN de administración distinta de la VLAN 1. Todos los pasos siguientes se harán desde el CLI del switch.

b. Cree o dé de alta la **VLAN 99** con el nombre **administracion**.

```
Switch(config)#interface vlan 99
Switch(config-if)#ip address 10.10.10.2 255.255.255.0
```

```
Switch(config)#vlan 99
Switch(config-vlan)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

Switch(config-vlan)#name administracion
Switch(config-vlan)#
```

c. Asigne la IP, la máscara y el Gateway predeterminado (**10.10.10.1**).

```
Switch(config)#ip default-gateway 10.10.10.1
```

d. Asigne el puerto Fa0/1 a Vlan 99.

```
Switch(config)#interface fa0/1
Switch(config-if)#switch
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode a
Switch(config-if)#switchport mode access v
Switch(config-if)#switchport mode access vlan 99
                                        ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport a
Switch(config-if)#switchport access vlan 99
Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

Switch(config-if)#end
Switch#
```

e. Configure la VTY para que el switch permita el acceso por Telnet. Si no configura una contraseña de VTY, no podrá acceder al switch mediante Telnet.

```
Switch(config)#line vty 0 15
Switch(config-line)#pass
Switch(config-line)#password cisco
Switch(config-line)#exit
Switch(config)#line vty 0 15
Switch(config-line)#transport input telnet
Switch(config-line)#login
Switch(config-line)#exit
```

Parte 2: Proteger las contraseñas

a. Desde el símbolo del sistema en la **PC1**, acceda al **S1** mediante Telnet. La contraseña de los modos EXEC del usuario y EXEC privilegiado es **cisco**.

```
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open


User Access Verification

Password:
Switch>ena
Password:
Switch#
```

b. Guarde la configuración actual, de manera que pueda revertir cualquier error que cometa reiniciando el **S1**.

```
Switch#copy running-config star
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

c. Muestre la configuración actual y observe que las contraseñas están en texto no cifrado.

Show running config.

```
line con 0
!
line vty 0 4
 password cisco
 login
 transport input telnet
line vty 5 15
 password cisco
 login
 transport input telnet
```

d. Introduzca el comando para cifrar las contraseñas de texto no cifrado.

```
Switch(config)#service password-encryption
Switch(config)#
```

e. Verifique que las contraseñas estén cifradas.

```
line con 0
!
line vty 0 4
 password 7 0822455D0A16
 login
 transport input telnet
line vty 5 15
 password 7 0822455D0A16
 login
 transport input telnet
!
```

Parte 3: Cifrar las comunicaciones

Paso 1: Establecer el nombre de dominio IP y generar claves seguras

En general no es seguro utilizar Telnet, porque los datos se transfieren como texto no cifrado. Por lo tanto, utilice SSH siempre que esté disponible.

a. Configure el nombre de dominio **netacad.pka.**

```
Switch(config)#ip domain-name netacad.pka
Switch(config)#
```

b. Se necesitan claves seguras para cifrar los datos. Genere las claves RSA con la longitud de clave 1024.

Tenemos que poner un nombre al switch antes de poner generar las claves.

```
Switch(config)#crypto key generate rsa
% Please define a hostname other than Switch.
Switch(config)#hostname S1
S1(config)#crypto key generate rsa
The name for the keys will be: S1.netacad.pka
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]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#
```

Paso 2: Crear un usuario de SSH y reconfigurar las líneas VTY para que solo admitan acceso por SSH

a. Cree un usuario **administrador** con **cisco** como contraseña secreta.

```
S1(config)#username administrador password cisco
*Mar 1 0:40:49.834: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#
```

b. Configure las líneas VTY para que revisen la base de datos local de nombres de usuario en busca de las credenciales de inicio de sesión y para que solo permitan el acceso remoto mediante SSH. Elimine la contraseña existente de la línea vty.

Se ha borrado correctamente las contraseñas.

```
line con 0
!
line vty 0 4
 login
 transport input telnet
line vty 5 15
 login
 transport input telnet
```

Antes teníamos puesto transport input telnet, ahora lo cambiaremos por ssh.

```
S1(config)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
```

c. Habilite la versión 2 SSH.

```
S1(config)#ip ssh version 2
S1(config)#
```

Parte 4: Verificar la implementación de SSH

a. Cierre la sesión de Telnet e intente iniciar sesión nuevamente con Telnet. El intento debería fallar.

```
C:\>telnet 10.10.10.2
Trying 10.10.10.2 ...Open

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

b. Intente iniciar sesión mediante SSH. Escriba **ssh** y presione la tecla **Enter**, sin incluir ningún parámetro que revele las instrucciones de uso de comandos. Sugerencia: la opción **-l** representa la letra “L”, no el número 1.

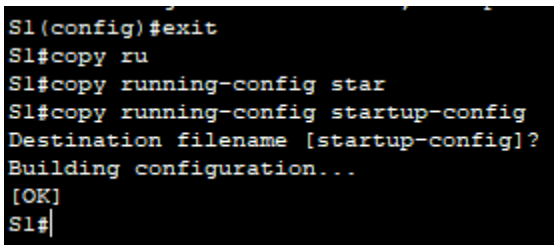
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l administrador 10.10.10.2

Password:



S1>
```

c. Cuando inicie sesión de forma correcta, ingrese al modo EXEC privilegiado y guarde la configuración. Si no pudo acceder de forma correcta al **S1**, reinicie y comience de nuevo en la parte 1.



AVISAR AL PROFESOR PARA COMPROBAR LA PRÁCTICA.

VISTO POR EL PROFESOR