Telnet, consola y contraseñas AUX. del puerto en el ejemplo de la configuración del Routers de Cisco

Contenido

Introducción

Este documento proporciona a las configuraciones de muestra para configurar la protección de la contraseña para las conexiones EXEC entrantes al router.

Prerequisites

Requisitos

Para realizar las tareas descritas en este documento, usted debe haber privilegiado el Acceso a Exec al comando line interface(cli) del router. Para la información sobre usar la línea de comando

y para los modos de comando de comprensión, vea con el software del Cisco IOS.

Para las instrucciones en la conexión de una consola con su router, refiera a la documentación que acompañó a su router, o refiera a la documentación en línea para su equipo.

Componentes usados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2509 Router
- Cisco IOS® Software, versión 12.2(19)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para más información sobre los convenios del documento, refiera a los convenios de los consejos técnicos de Cisco.

Antecedentes

El uso de la protección de la contraseña de controlar o de restringir el acceso al comando line interface(cli) de su router es uno de los elementos fundamentales de un plan de la seguridad general.

Protegiendo al router contra el Acceso Remoto desautorizado, típicamente Telnet, es la mayoría de la seguridad común que necesita configurar, pero la protección del router contra el Acceso local desautorizado no puede ser pasada por alto.

Note: La protección de la contraseña es apenas una de los muchos pasos que usted debe utilizar en un régimen profundizado eficaz de la seguridad de la red. Los firewalls, las listas de acceso y el control del acceso físico al equipo son otros elementos que se deben considerar al implementar su plan de seguridad.

La línea de comando, o el EXEC, acceso a un router se puede hacer de varias maneras, pero en todos los casos la conexión hacia adentro al router se hace en una línea equipo teleescritor. Hay cuatro tipos principales de líneas equipo teleescritor, como se ve en esta **salida de línea de la demostración de la** muestra:

```
2509#show line
   Tty Typ     Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns   Int
*    0 CTY              -    -      -    -    -      0       0     0/0       -
     1 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     2 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     3 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     4 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     5 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
     6 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
```

```
  7 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
  8 TTY   9600/9600  -    -      -    -    -      0       0     0/0       -
  9 AUX   9600/9600  -    -      -    -    -      0       0     0/0       -
 10 VTY              -    -      -    -    -      0       0     0/0       -
 11 VTY              -    -      -    -    -      0       0     0/0       -
 12 VTY              -    -      -    -    -      0       0     0/0       -
 13 VTY              -    -      -    -    -      0       0     0/0       -
 14 VTY              -    -      -    -    -      0       0     0/0       -

2509#
```

El CTY de canalización es el puerto de la consola. En cualquier router, aparece en la configuración del router como **línea estafa 0** y en la salida del **comando show line** como **cty**. El puerto de la consola se usa principalmente para el acceso al sistema local mediante un terminal de consola.

Las líneas **equipo teleescritor** son líneas asíncronas usadas para entrante o módem de salida y los conexión de la terminal y se pueden considerar en un router o una configuración del Access Server como **línea x.** Los números de líneas específicas son una función del hardware incorporada o instalada en el router o en el servidor de acceso.

La línea **AUX** es el puerto auxiliar, que aparece en la configuración como **line aux 0**.

Las líneas **VTY** son las líneas de terminal virtual del router, que se utilizan solamente para controlar las conexiones Telnet entrantes. Son virtuales en el sentido que son una función de software; no hay hardware relacionado con ellas. Aparecen en la configuración como **línea 0 4. vty.**

Cada uno de estos tipos de líneas se puede configurar con la protección de la contraseña. Las líneas pueden configurarse para utilizar una misma contraseña para todos los usuarios o para contraseñas específicas de los usuarios. las contraseñas Usuario-específicas se pueden configurar localmente en el router, o usted puede utilizar un servidor de la autenticación para proporcionar a la autenticación.

No hay prohibición de configuración de diferentes líneas con diferentes tipos de protección con contraseña. De hecho, es común ver routers con una sola contraseña para la consola y contraseñas específicas de los usuarios para otras conexiones entrantes.

Abajo está un ejemplo del router hecho salir del **comando show running-config**:

```
2509#show running-config
Building configuration...

Current configuration : 655 bytes
!
version 12.2
.
.
.
!--- Configuration edited for brevity line con 0 line 1 8 line aux 0 line vty 0 4 ! end
```

Configure las contraseñas en la línea

Para especificar una contraseña en una línea, utilice el **comando password** en el modo de configuración de línea. Para activar el control de contraseña en la clave, utilice el **comando login** en el modo de configuración de línea.

Note: Para encontrar la información adicional sobre los comandos usados en este documento, utilice la herramienta de búsqueda de comandos (clientes registrados solamente).

Procedimiento de configuración

En este ejemplo, una contraseña se configura para todos los usuarios que intentan utilizar la consola.

1. De la guía privilegiada del EXEC (o “enable”), ingrese el modo de la configuración y después cambie al modo de configuración de línea que usa los comandos siguientes. Tenga en cuenta que el mensaje cambia para reflejar el modo actual.
   ```
   router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#line con 0
   router(config-line)#
   ```
2. Configure la contraseña, y active el control de contraseña en la clave.
   ```
   router(config-line)#password letmein
   router(config-line)#login
   ```
3. Dé salida al modo de la configuración.
   ```
   router(config-line)#end
   router#
   %SYS-5-CONFIG_I: Configured from console by console
   ```
   Note: No guarde los cambios de configuración para **line con 0** hasta que se verifique su capacidad para iniciar sesión.

Note: En la configuración de la consola de líneas, **login** es un comando de configuración obligatorio para habilitar la verificación de contraseñas durante el inicio de sesión. La autenticación de la consola requiere los **comandos password** y **login** para su correcto funcionamiento.

Verifique la configuración

Examine la configuración del ranurador para verificar que los comandos se han ingresado correctamente:

La herramienta intérprete de la salida apoyan a los ciertos comandos show (clientes registrados solamente), que permite que usted vea un análisis de la **salida del comando show**.

- **los ejecutar-config de la demostración** - visualiza la configuración actual del router.
  ```
  router#show running-config
  Building configuration...
  ...
  !--- Lines omitted for brevity ! line con 0 password letmein
  login
  line 1 8
  line aux 0
  line vty 0 4
  !
  end
  ```
  Para probar la configuración, terminar una sesión la consola y abrirse una sesión otra vez, usando la contraseña configurada para tener acceso al router:
  ```
  router#exit

  router con0 is now available
  ```

```
Press RETURN to get started.

User Access Verification
Password:
!--- Password entered here is not displayed by the router router>
```

Note: Antes de realizar esta prueba, asegúrese de que usted tiene una conexión alterna en el router, tal como Telnet o dial-en, en caso de que haya un registro de problema nuevamente dentro del router.

Resuelva problemas la falla de registro

Si usted no puede registrar nuevamente dentro del router y usted no ha guardado la configuración, recargar al router eliminará cualquier cambio de configuración que usted haya realizado.

Si los cambios de configuración se guardaron y no puede iniciar sesión en el router, deberá realizar una recuperación de contraseña. Vea los procedimientos para recuperación de contraseña para encontrar las instrucciones para su plataforma particular.

Configure las contraseñas Usuario-específicas locales

Para establecer un sistema de autenticación basado en el nombre de usuario, utilice el **comando username** en el modo de configuración global. Para activar el control de contraseña en la clave, utilice el **comando login local** en el modo de configuración de línea.

Procedimiento de configuración

En este ejemplo, las contraseñas se configuran para los usuarios que intentan conectar con el router en las líneas VTY usando Telnet.

1. En el mensaje de EXEC privilegiado (o "enable"), ingrese al modo de configuración y luego ingrese las combinaciones de nombre de usuario/contraseña, una para cada usuario para el cual desea permitir el acceso al router:
   ```
   router#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   router(config)#username russ password montecito
   router(config)#username cindy password belgium
   router(config)#username mike password rottweiler
   ```

2. Cambie al modo de configuración de línea mediante los siguientes comandos. Tenga en cuenta que el mensaje cambia para reflejar el modo actual.
   ```
   router(config)#line vty 0 4
   router(config-line)#
   ```
3. Configure el control de contraseña en la clave.
   ```
   router(config-line)#login local
   ```

4. Dé salida al modo de la configuración.
   ```
   router(config-line)#end
   router#
   %SYS-5-CONFIG_I: Configured from console by console
   ```

Note: Para inhabilitar el uso automático de Telnet cuando escribe un nombre en la CLI,

configure **no logging preferred** en la línea que se utiliza. Si bien **transport preferred none** proporciona el mismo resultado, también inhabilita el uso automático de Telnet para el host definido que se configura con el **comando ip host**. Esto difiere del comando **no logging preferred**, que lo detiene para hosts indefinidos y lo deja funcionar para los definidos.

Verifique la configuración

Examine la configuración del ranurador para verificar que los comandos se han ingresado correctamente:

- **los ejecutar-config de la demostración** - visualiza la configuración actual del router.

```
router#show running-config
Building configuration...
!
!--- Lines omitted for brevity ! username russ password 0 montecito
username cindy password 0 belgium
username mike password 0 rottweiler
!
!--- Lines omitted for brevity ! line con 0 line 1 8 line aux 0 line vty 0 4 login local
!
end
```

Para probar esta configuración, se debe establecer una conexión Telnet al router. Esto puede ser hecha conectando de un diverso host en la red, pero usted puede también probar del router sí mismo telnetting a la dirección IP de cualquier interfaz en el router que está en un estado up-up como se ve en la salida del **comando show interfaces**.Aquí está una salida de muestra si el direccionamiento de las **interfaces Ethernet 0** era 10.1.1.1:

```
router#telnet 10.1.1.1
Trying 10.1.1.1 ... Open


User Access Verification


Username: mike
Password:
!--- Password entered here is not displayed by the router router
```

Falla de contraseña Usuario-específica del Troubleshooting

Los nombres de usuario y las contraseñas distinguen entre mayúsculas y minúsculas. Rechazarán a los usuarios que intentan abrirse una sesión con un username o una contraseña incorrectamente encajonado.

Si los usuarios no pueden registrar en el router con sus contraseñas específicas, configure de nuevo el nombre de usuario y contraseña en el router.

Configure la contraseña de línea AUX.

Para especificar una contraseña en la línea AUX., publique el **comando password** en el modo de configuración de línea. Para activar el control de contraseña en la clave, publique el **comando login** en el modo de configuración de línea.

Procedimiento de configuración

En este ejemplo, una contraseña se configura para todos los usuarios que intentan utilizar el puerto AUX.

1. Publique el **comando show line** para verificar la línea usada por el puerto AUX.
```
R1#show line

   Tty Typ     Tx/Rx    A Modem Roty AccO AccI  Uses  Noise  Overruns  Int
*    0 CTY                  -    -     -    -    -     0      0     0/0       -
    65 AUX  9600/9600  -    -     -    -    -    0     1     0/0             -
    66 VTY                 -    -     -    -    -     0      0     0/0       -
    67 VTY                 -    -     -    -    -     0      0     0/0       -
```
2. En este ejemplo, el puerto AUX. está en la línea 65. Publique estos comandos para configurar la línea AUX. del router:
```
R1# conf t
R1(config)# line 65
R1(config-line)#modem inout
R1(config-line)#speed 115200
R1(config-line)#transport input all
R1(config-line)#flowcontrol hardware
R1(config-line)#login
R1(config-line)#password cisco
R1(config-line)#end
R1#
```

Verifique la configuración

Examine la configuración del ranurador para verificar que los comandos se han ingresado correctamente:

- **El comando show running-config** visualiza la configuración actual del router:
```
R1#show running-config
Building configuration...
!
!--- Lines omitted for brevity. line aux 0
 password cisco
 login
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware

!--- Lines omitted for brevity. ! end
```

Configure la autenticación AAA para la clave

Para activar la autenticación para inicios de sesión del Authentication, Authorization, and Accounting (AAA), utilice el **comando login authentication** en el modo de configuración de línea. Los servicios AAA deben también ser configurados.

Procedimiento de configuración

En este ejemplo, configuran al router para extraer las contraseñas de usuarios de un servidor TACACS+ cuando los usuarios intentan conectar con el router.

Note: La configuración del router para utilizar otros tipos de servidores AAA (RADIUS, por ejemplo) es similar. Vea configurar la autenticación para la información adicional.

Note: En este documento, no se trata la configuración del servidor AAA en sí. Refiera a los protocolos para información del servidor de seguridad en configurar el servidor AAA.

1. De la guía privilegiada del EXEC (o “enable”), ingrese el modo de la configuración y ingrese los comandos de configurar el ranurador para utilizar los servicios AAA para autenticación:
```
router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#aaa new-model
router(config)#aaa authentication login my-auth-list tacacs+
router(config)#tacacs-server host 192.168.1.101
router(config)#tacacs-server key letmein
```

2. Cambie al modo de configuración de línea que usa los comandos siguientes. Tenga en cuenta que el mensaje cambia para reflejar el modo actual.
```
router(config)#line 1 8
router(config-line)#
```
3. Configure el control de contraseña en la clave.
```
router(config)#line 1 8
router(config-line)#
```
4. Dé salida al modo de la configuración.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

Verifique la configuración

Examine la configuración del ranurador para verificar que los comandos se han ingresado correctamente:

- **los ejecutar-config de la demostración** - visualiza la configuración actual del router.

```
router#write terminal
Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
aaa new-model
aaa authentication login my-auth-list tacacs+
!
!--- Lines omitted for brevity ... ! tacacs-server host 192.168.1.101
tacacs-server key letmein
!
line con 0
line 1 8
 login authentication my-auth-list
line aux 0
line vty 0 4
!
end
```

Para probar esta configuración en particular, se debe establecer una conexión entrante o saliente a la línea. Vea la guía para la conexión del módem-router para información específica sobre configurar las líneas del async para las conexiones del módem.

De forma alternativa, puede configurar una o más líneas VTY para realizar la autenticación de AAA y para realizar su prueba allí.

Falla de registro AAA del Troubleshooting

Antes de publicar los **comandos debug**, vea la información importante en los comandos Debug.

Para resolver problemas un intento de inicio de sesión fallido, utilice el **comando debug** apropiado a su configuración:

- debug aaa authentication
- debug radius
- debug kerberos

Información Relacionada

- Configurar la autenticación
- Referencia de Comandos de Debug del Cisco IOS
- Soporte técnico - Cisco Systems