Ejemplo de configuración de contraseñas de puerto auxiliar, consola y Telnet en routers Cisco

Contenido

Introducción

En este documento, se ofrecen ejemplos de configuraciones de protección con contraseña para conexiones EXEC entrantes al router.

prerrequisitos

Requisitos

Para realizar las tareas descritas en este documento, debe disponer de acceso EXEC privilegiado a la interfaz de línea de comandos (CLI) del router. Para obtener información sobre el uso de la línea de comandos y para comprender los modos de comandos, vea Uso de la Interfaz de Línea de Comandos de Cisco IOS.

Para obtener instrucciones sobre cómo conectar una consola al router, consulte la documentación que se suministra con su router o la documentación en línea relativa a su equipo.

Componentes Utilizados

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

- Router 2509 de Cisco
- 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

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Antecedentes

El uso de protección con contraseña para controlar o restringir el acceso a la interfaz de línea de comandos (CLI) del router es uno de los elementos fundamentales de un plan de seguridad general.

La protección del router contra el acceso remoto no autorizado, generalmente Telnet, es el tipo de seguridad más común que debe configurar, aunque la protección del router contra el acceso local no autorizado no se puede pasar por alto.

Nota: La protección mediante contraseña es sólo uno de los muchos pasos que debe seguir en un régimen de seguridad de red eficaz y en profundidad. 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.

El acceso a la línea de comando o EXEC en un router puede realizarse de distintas maneras, pero en todos los casos, la conexión interna al router se realiza en una línea TTY. Existen cuatro tipos principales de líneas TTY, como se puede ver en este ejemplo de resultado del comando **show line:**

```
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 tipo de línea **CTY es el Puerto de la Consola.** En cualquier router, aparece en la configuración de router como **line con 0 y, en el resultado 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 TTY son asíncronas y se utilizan para conexiones entrantes y salientes de módem y terminal. Pueden encontrarse en una configuración de router o de servidor de acceso 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 **line vty 0 4.**

Cada uno de estos tipos de líneas puede configurarse con protección con contraseña. Las líneas pueden configurarse para utilizar una misma contraseña para todos los usuarios o para contraseñas específicas de los usuarios. Las contraseñas específicas de los usuarios se pueden configurar de manera local en el router, o bien puede utilizar un servidor de autenticación para proporcionar 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.

A continuación, se presenta un ejemplo de resultado de router para el **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
```

Configuración de Contraseñas en la Línea

Para especificar una contraseña en una línea, use el **comando password en el modo de configuración de línea.** Para habilitar la verificación de la contraseña durante el inicio de sesión, utilice el **comando login en el modo de configuración de línea.**

Procedimiento de Configuración

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

1. En el mensaje de EXEC privilegiado (o "enable"), ingrese al modo de configuración y luego cambie al modo de configuración de línea utilizando los siguientes comandos. 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 habilite la verificación de contraseñas durante el inicio de sesión.
```
router(config-line)#password letmein
router(config-line)#login
```
3. Salga del modo de configuración.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```
Nota: No guarde los cambios de configuración en la **línea con 0** hasta que se haya verificado su capacidad para iniciar sesión.

Nota: En la configuración de la consola de línea, **login** es un comando de configuración obligatorio para habilitar la verificación de contraseña al iniciar sesión. La autenticación de la consola requiere los **comandos password y login para su correcto funcionamiento.**

Verifique la Configuración

Examine la configuración del router para verificar que los comandos hayan sido ingresados correctamente:

- El comando **show running-config muestra 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, desconecte la consola y vuelva a conectarla, utilizando la contraseña configurada para acceder 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>
```
Nota: Antes de realizar esta prueba, asegúrese de tener una conexión alternativa en el router, como Telnet o dial-in, en caso de que haya un problema al volver a iniciar sesión en el router.

Troubleshooting de Errores de Inicio de Sesión

Si no puede volver a iniciar sesión en el router y no ha guardado la configuración, la recarga del router eliminará todos los cambios 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. Para obtener instrucciones sobre una plataforma en particular, consulte Procedimientos para Recuperación de Contraseña.

Configure Contraseñas Locales Específicas para cada Usuario

Para establecer un sistema de autenticación basado en el nombre de usuario, utilice el **comando username en el modo de configuración global.** Para habilitar la verificación de contraseñas durante el inicio de sesión, utilice el **comando login local en el modo de configuración de línea.**

Procedimiento de Configuración

En este ejemplo, se configuran contraseñas para los usuarios que intenten conectarse al router en las líneas VTY mediante 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 la verificación de contraseñas durante el inicio de sesión.
```
router(config-line)#login local
```

4. Salga del modo de configuración.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```
Nota: Para inhabilitar el Telnet automático cuando escribe un nombre en la CLI, configure **no logging preferido** 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 router para verificar que los comandos hayan sido ingresados correctamente:

- El comando **show running-config muestra 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. Para ello, conéctese desde un host diferente en la red, aunque también puede realizar la prueba desde el mismo router conectándose mediante la red Telnet a la dirección IP de cualquier interfaz en el router cuyo estado sea up/up, como se puede ver en el resultado del **comando show interfaces.**Este es un ejemplo de resultado si la dirección de la **interfaz Ethernet 0 fuese 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
```

Troubleshooting de Errores de Contraseñas Específicas de los Usuarios

Los nombres de usuario y las contraseñas distinguen entre mayúsculas y minúsculas. Se rechazará todo usuario que intente iniciar sesión con un nombre de usuario o una contraseña con el tipo de letra incorrecto.

Si los usuarios no pueden iniciar sesión en el router con sus contraseñas específicas, reconfigure el nombre de usuario y la contraseña en el router.

Configuración de la contraseña de línea AUX

Para especificar una contraseña en la línea AUX, ejecute el comando **password** en el modo de configuración de línea. Para habilitar la verificación de contraseña al iniciar sesión, ejecute el comando **login** en el modo de configuración de línea.

Procedimiento de Configuración

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

1. Ejecute el comando **show line** para verificar la línea utilizada 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. Ejecute 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#
```

Verificar configuración

Examine la configuración del router para verificar que los comandos se hayan ingresado correctamente:

- El comando **show running-config** muestra 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 Atneticación AAA para el Inicio de Sesión

Para habilitar la autenticación de autenticación, autorización y contabilización (AAA) para los inicios de sesión, utilice el **comando login authentication en el modo de configuración de línea.** También se deben configurar los servicios AAA.

Procedimiento de Configuración

En este ejemplo, el router está configurado para recuperar las contraseñas de los usuarios de un servidor TACACS+ cuando estos intenten conectarse al router.

Nota: La configuración del router para utilizar otros tipos de servidores AAA (RADIUS, por ejemplo) es similar. Para obtener más información, consulte Configuración de la Autenticación.

Nota: Este documento no aborda la configuración del propio servidor AAA.

1. En el mensaje de EXEC privilegiado (o "habilitado"), ingrese configuration mode luego ejecute los comandos para configurar el router para usar los servicios AAA para la 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 con los siguientes comandos. Tenga en cuenta que el mensaje cambia para reflejar el modo actual.
```
router(config)#line 1 8
router(config-line)#
```
3. Configure la verificación de contraseñas durante el inicio de sesión.
```
router(config-line)#login authentication my-auth-list
```
4. Salga del modo de configuración.
```
router(config-line)#end
router#
%SYS-5-CONFIG_I: Configured from console by console
```

Verifique la Configuración

Examine la configuración del router para verificar que los comandos hayan sido ingresados correctamente:

- El comando **show running-config muestra 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. Consulte Guía de Conexión del Módem al Router para obtener información específica sobre la configuración de líneas asíncronas para conexiones de módem.

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

Troubleshooting de Errores de Inicio de Sesión de AAA

Antes de ejecutar un **comando debug, consulte** Información Importante sobre Comandos de Debug.

Para resolver problemas de un intento de inicio de sesión fallido, use el **comando debug que**

corresponda a su configuración:

- debug aaa authentication
- debug radius
- debug kerberos

Información Relacionada

- Referencia de Comandos de Debug del Cisco IOS
- Soporte Técnico - Cisco Systems