Configuración del SSH en routers y switches

Contenido

Introducción

En este documento se describe la configuración y depuración de shell seguro (SSH) en los

routers o switches de Cisco que ejecutan el software Cisco IOS®.

Prerequisites

Requirements

La imagen del Cisco IOS utilizada debe ser una imagen k9 (crypto) para que pueda soportar SSH. Por ejemplo, c3750e-universalk9-tar.122-35.SE5.tar es una imagen k9 (criptográfica).

Componentes Utilizados

La información de este documento se basa en el Cisco IOS 3600 Software (C3640-IK9S-M), versión 12.2(2)T1.

SSH se introdujo en las siguientes imágenes y plataformas del Cisco IOS:

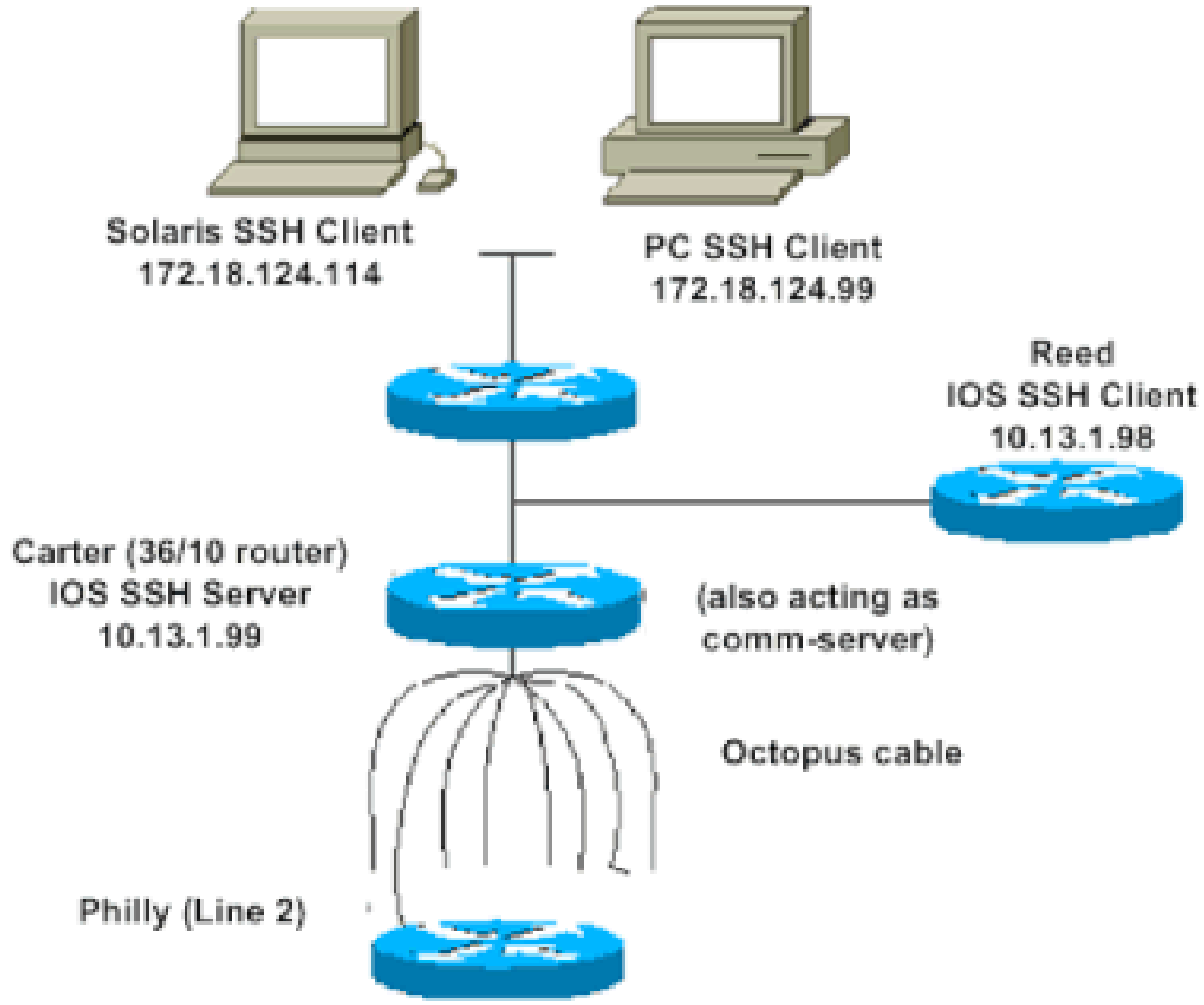
- El acceso a línea de terminal SSH (también denominado Telnet inverso) se comenzó a incluir en plataformas e imágenes IOS de Cisco desde la versión 12.2.2.T del software Cisco IOS.
- La compatibilidad con la versión 2.0 de SSH (SSH v2) se comenzó a incluir en plataformas e imágenes IOS de Cisco desde la versión 12.1(19)E del software Cisco IOS.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Para más información, consulte las Convenciones sobre consejos técnicos de Cisco.

Diagrama de red SSH v2



Prueba de Autenticación

Prueba de Autenticación Sin SSH

Primero, pruebe la autenticación sin SSH para asegurarse de que la autenticación trabaje con el router Carter antes de que se agregue SSH. La autenticación se puede realizar con un nombre de usuario y contraseña locales, o con un servidor de autenticación, autorización y contabilidad (AAA) que ejecute TACACS+ o RADIUS. (Con SSH no se puede realizar la autenticación mediante contraseña de línea.) Este ejemplo muestra la autenticación local, que permite realizar Telnet al router con el nombre de usuario cisco y la contraseña cisco.

Nota: En este documento, vty se utiliza para indicar el tipo de terminal virtual.

```
!--- The aaa new-model command causes the local username and password on the router to be used in the al

aaa new-model
username cisco password 0 cisco
line vty 0 4
```

```
transport input telnet

!--- Instead of aaa new-model, you can use the login local command.
```

Prueba de Autenticación Con SSH

Para poder probar la autenticación con SSH, debe agregar elementos a las sentencias anteriores para poder habilitar SSH en Carter y probar SSH desde el PC y las estaciones UNIX.

```
ip domain-name rtp.cisco.com

!--- Generate an SSH key to be used with SSH.

crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
```

En este punto, el comando show crypto key mypubkey rsa debe mostrar la llave generada. Una vez agregada la configuración de SSH, pruebe su capacidad para acceder al router desde las estaciones UNIX y las PC.

Conjuntos de configuraciones optativas

Prevención de Conexiones No SSH

Si usted desea prevenir conexiones no SSH, agregue el comando transport input ssh en las líneas para limitar el router a conexiones SSH solamente. Se rechaza Telnet recto (no SSH).

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

Realice una prueba para asegurarse de que los usuarios sin SSH no pueden realizar Telnet al router Carter.

Configuración de un Switch o un Router del IOS Como Cliente de SSH

Hay cuatro pasos obligatorios para habilitar el soporte de SSH en un router del Cisco IOS:

1. Configure el comando hostname.

2. Configure el dominio DNS.

3. Genere la clave SSH.

4. Habilite la compatibilidad con el transporte SSH para el vtys.

Si desea que un dispositivo actúe como cliente de SSH al otro, puede agregar SSH a un segundo dispositivo llamado Reed. Esto pone a estos dispositivos en una configuración de cliente y servidor, en la que Carter actúa como servidor y Reed como cliente. La configuración de cliente de SSH del Cisco IOS en Reed es la misma que la requerida para la configuración de servidor de SSH en Carter.

```
!--- Step 1: Configure the hostname if you have not previously done so.

hostname carter

!--- The aaa new-model command causes the local username and password on the router to be used in the al

aaa new-model
username cisco password 0 cisco

!--- Step 2: Configure the DNS domain of the router.

ip domain-name rtp.cisco.com

!--- Step 3: Generate an SSH key to be used with SSH.

crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2

!--- Step 4: By default the vty transport is Telnet. In this case, Telnet is disabled and only SSH is su

line vty 0 4
transport input ssh

!--- Instead of aaa new-model, you can use the login local command.
```

Ejecute este comando para SSH desde el cliente SSH de Cisco IOS (Reed) hasta el servidor SSH de Cisco IOS (Carter) para probar esto:

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99
```

Configurar un router IOS como servidor SSH que realiza autenticación de usuario basada en RSA

Complete estos pasos para configurar el servidor SSH para realizar la autenticación basada en RSA.

1. Especifique el nombre del host.

```
Router(config)#hostname <host name>
```

2. Nombre de dominio predeterminado.

```
Router(config)#ip domain-name <Domain Name>
```

3. Generar pares de claves RSA

```
Router(config)#crypto key generate rsa
```

4. Configure las claves SSH-RSA para la autenticación de usuarios y servidores.

```
Router(config)#ip ssh pubkey-chain
```

5. Configura el nombre de usuario SSH.

```
Router(conf-ssh-pubkey)#username <user name>
```

6. Especifique la clave pública RSA del par remoto.

```
Router(conf-ssh-pubkey-user)#key-string
```

7. Especifique el tipo y la versión de la clave SSH. (Este paso es opcional).

```
Router(conf-ssh-pubkey-data)#key-hash ssh-rsa <key ID>
```

8. Salga del modo actual y regrese al modo EXEC privilegiado.

```
Router(conf-ssh-pubkey-data)#end
```

Adición de Acceso de Línea de Terminal de SSH

Si necesita autenticación de línea de terminal de SSH saliente, puede configurar y probar SSH para Telnet inverso saliente a través de Carter, que actúa como un servidor de comunicaciones a Philly.

```
ip ssh port 2001 rotary 1
line 1 16
   no exec
   rotary 1
   transport input ssh
   exec-timeout 0 0
   modem InOut
   stopbits 1
```

Si Philly está conectado al puerto 2 de Carter, puede configurar SSH para Philly a través de Carter desde Reed con la ayuda de este comando:

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -p 2002 10.31.1.99
```

Puede utilizar este comando de Solaris:

```
ssh -c 3des -p 2002 -x -v 10.13.1.99
```

Restricción del Acceso de SSH a una Subred

Debe limitar la conectividad SSH a una subred específica donde se descartan todos los demás intentos de SSH de IP fuera de la subred.

Puede seguir estos pasos para hacer lo mismo:

1. Defina una lista de acceso que permita el tráfico de esa subred específica.
2. Restrinja el acceso a la interfaz de línea VTY con access-class.

Este es un ejemplo de configuración. En este ejemplo, solo se permite el acceso SSH a la subred 10.10.10.0 255.255.255.0; se niega el acceso a cualquier otra subred.

```
Router(config)#access-list 23 permit 10.10.10.0 0.0.0.255
Router(config)#line vty 5 15
Router(config-line)#transport input ssh
Router(config-line)#access-class 23 in
Router(config-line)#exit
```

Nota: el mismo procedimiento para bloquear el acceso SSH también se utiliza para las plataformas de switch.

Configuración de la versión 2 de SSH

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

Variaciones en el Resultado del Comando de Banner

El resultado del comando banner varía entre Telnet y las diversas versiones de las conexiones de SSH. En esta tabla, se ilustra cómo funcionan las diferentes opciones del comando banner con varios tipos de conexiones.

Opción del comando banner	TELNET	SSH v2
registro de banner	Aparece antes de iniciar sesión en el dispositivo.	Aparece antes de iniciar sesión en el dispositivo.
banner motd	Aparece antes de iniciar sesión en el dispositivo.	Aparece después de iniciar sesión en el dispositivo.
banner exec	Aparece después de iniciar sesión en el dispositivo.	Aparece después de iniciar sesión en el dispositivo.

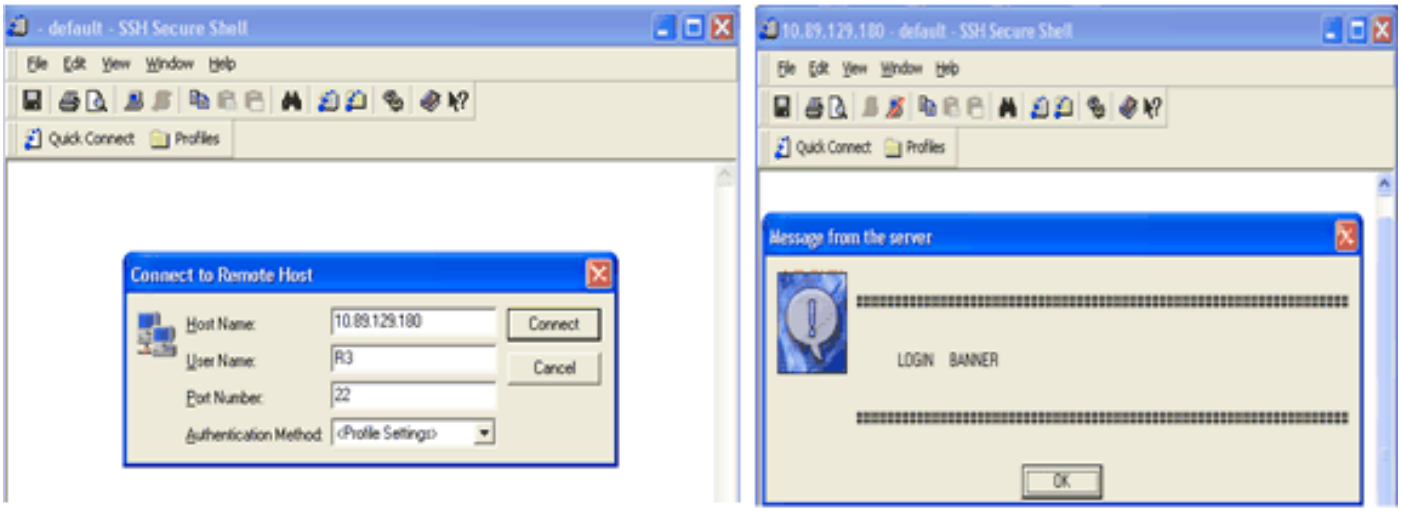
Nota: Ya no se recomienda el uso de la versión 1 de SSH.

Incapacidad para Mostrar el Banner de Inicio de Sesión

La versión 2 de SSH admite el banner de inicio de sesión. Cuando inicia la sesión SSH con el router Cisco, se muestra el banner de inicio de sesión si el cliente SSH envía el nombre de usuario. Por ejemplo, cuando se utiliza el cliente SSH Shell seguro, se muestra el anuncio de inicio de sesión. Cuando se utiliza el cliente SSH PuTTY, no se muestra el anuncio de inicio de

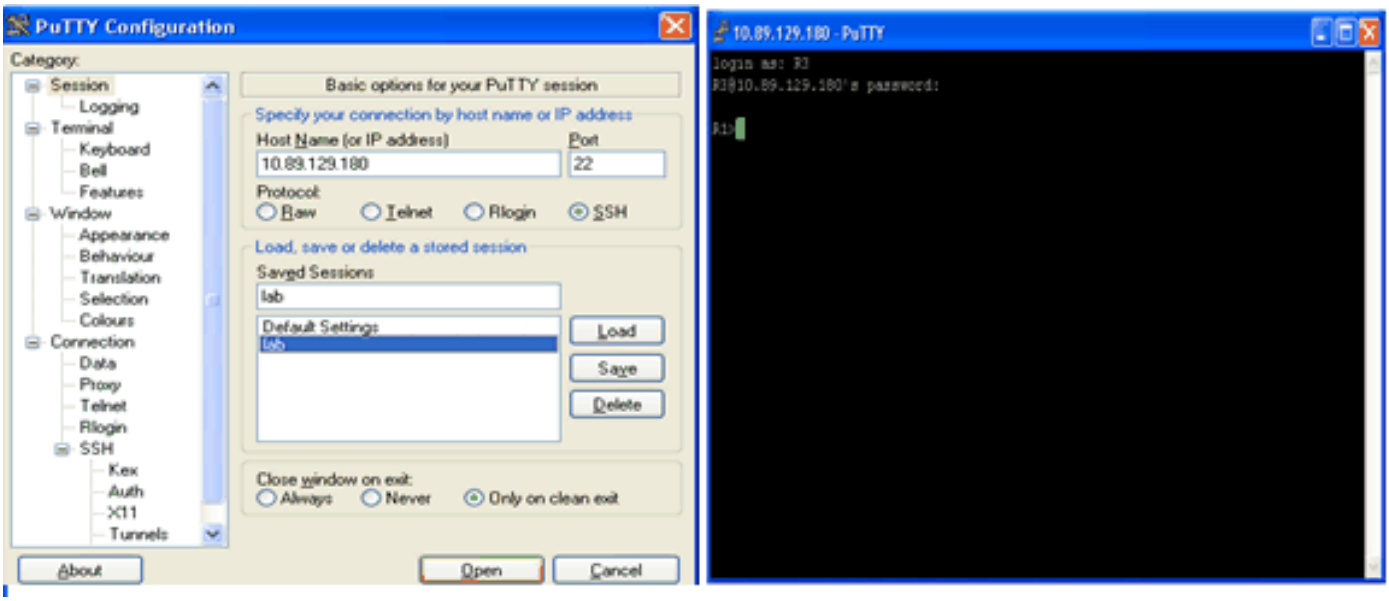
sesión. Esto se debe a que SSH envía el nombre de usuario de manera predeterminada y PuTTY no envía el nombre de usuario de manera predeterminada.

El cliente SSH necesita el nombre de usuario para iniciar la conexión al dispositivo habilitado para SSH. El botón Connect no se habilita si usted no ingresa el nombre de host y el nombre de usuario. Esta imagen de pantalla muestra que el banner de inicio de sesión se muestra cuando SSH se conecta al router. El banner solicita una contraseña.



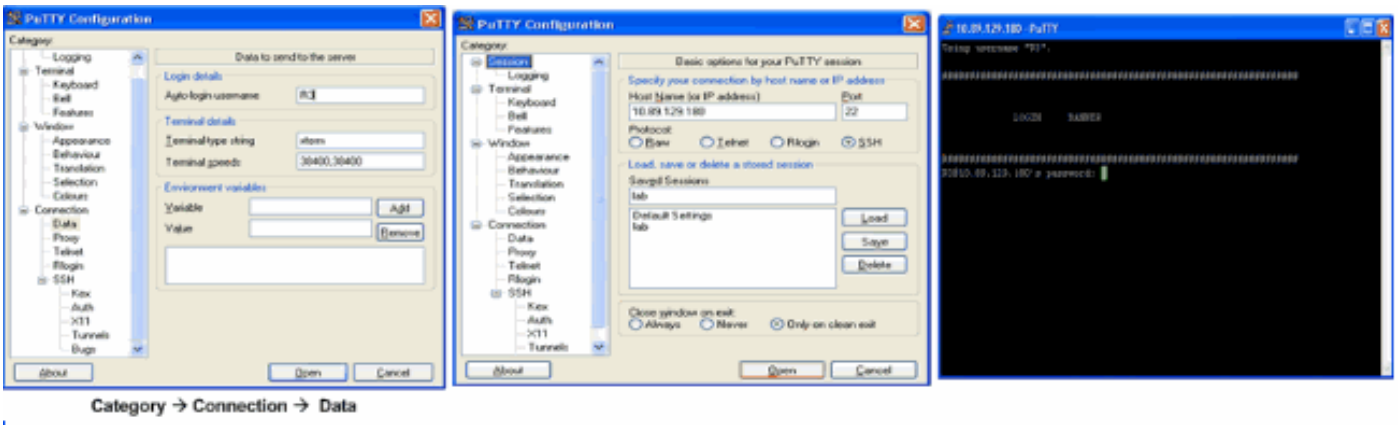
Banner solicita una contraseña

El cliente de PuTTY no requiere el nombre de usuario para iniciar la conexión de SSH al router. Esta imagen de pantalla muestra que el cliente PuTTY se conecta al router y solicita el nombre de usuario y la contraseña. No muestra el banner de inicio de sesión.



Conexión SSH al router

Esta captura de pantalla muestra que el banner de inicio de sesión se muestra cuando PuTTY está configurada para enviar el nombre de usuario al router.



Enviar nombre de usuario al router

Comandos debug y show

Antes de ejecutar los comandosdebugque se describen aquí, consulte Información importante sobre comandos de depuración. La herramientaOutput Interpreter (sólo para clientes registrados) admite los comandosshow, lo cual le permitirá ver un análisis del resultado de dichos comandos.

- debug ip ssh muestra los mensajes de depuración para SSH.
- show ssh muestra el estado de las conexiones SSH del servidor.

```
carter#show ssh
  Connection     Version Encryption    State               Username
   0             2.0     DES           Session started     cisco
```

- show ip ssh muestra los datos de versión y configuración de SSH.

```
carter#show ip ssh
  SSH Enabled - version 2.0
  Authentication timeout: 120 secs; Authentication retries: 3
```

Ejemplo de resultado del comando debug

Depuración de Router

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-2.0-1.2.26
00:23:20: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
```

```
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH0: sending encryption confirmation
00:23:21: SSH0: keys exchanged and encryption on
00:23:21: SSH0: SSH_CMSG_USER message received
00:23:21: SSH0: authentication request for userid cisco
00:23:21: SSH0: SSH_SMSG_FAILURE message sent
00:23:23: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:23:23: SSH0: authentication successful for cisco
00:23:23: SSH0: requesting TTY
00:23:23: SSH0: setting TTY - requested: length 24, width 80; set:
   length 24, width 80
00:23:23: SSH0: invalid request - 0x22
00:23:23: SSH0: SSH_CMSG_EXEC_SHELL message received
00:23:23: SSH0: starting shell for vty
```

Debug de Servidor

Nota: Este es el resultado de la máquina Solaris.

```
rtp-evergreen.rtp.cisco.com#ssh -c 3des -l cisco -v 10.31.1.99
rtp-evergreen#/opt/CISssh/bin/ssh -c 3des -l cisco -v 10.13.1.99
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.13.1.99 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 2.0,
   remote software version Cisco-1.25
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits)
   and host key (512 bits).
rtp-evergreen: Host '10.13.1.99' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
cisco@10.13.1.99's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.
```

Configuraciones incorrectas

En estas secciones, hay ejemplos de resultado de debug de varias configuraciones incorrectas.

SSH desde un cliente de SSH no compilado con el estándar de cifrado de datos (DES)

Contraseña Incorrecta

Depuración de Router

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-2.0-1.2.26
00:26:52: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_SMSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

El Cliente de SSH Envía Encripción No Soportada (Blowfish)

Depuración de Router

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-2.0-W1.0
00:39:26: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

Recibir el error “%SSH-3-PRIVATEKEY: No se puede recuperar la clave privada RSA para”

Un cambio en el nombre de dominio o el nombre de host puede activar este mensaje de error. Utilice estas soluciones alternativas:

- Ponga en cero las llaves RSA y vuelva a generar las llaves.

```
crypto key zeroize rsa label key_name
crypto key generate rsa label key_name modulus key_size
```

- Si la solución temporal anterior no funciona, intente estos pasos:
    1. Ponga en cero todas las llaves RSA.
    2. Recargue el dispositivo.
    3. Cree llaves nuevas etiquetadas para SSH.

Consejos

- Si los comandos de configuración de SSH se rechazan como comandos ilegales, usted no ha generado correctamente un par de llaves RSA para el router. Asegúrese de haber especificado un nombre de host y un dominio. Luego use el comandocrypto key generate rsapara generar pares de claves RSA y habilitar el servidor SSH.
- Al configurar pares de claves RSA, pueden aparecer estos mensajes de error:
    1. `No se especificó ningún nombre de host.`

       Debe utilizar el comando de configuración global hostname para configurar un nombre de host para el router.
    2. `No se especificó ningún dominio.`

       Debe utilizar el comando de configuración global ip domain-name para configurar un dominio de host para el router.
- El número de conexiones SSH permitidas está limitado al número máximo de conexiones vty configuradas para el router. Cada conexión SSH utiliza un vty recurso.

•

SSH utiliza la seguridad local o el protocolo de seguridad configurado a través de AAA en su router para la autenticación de usuarios. Al configurar AAA, debe asegurarse de que la consola no se ejecute en AAA. Aplique una palabra clave en el modo de configuración global para deshabilitar AAA en la consola.

•

No SSH server connections running:

```
carter#show ssh %No SSHv2 server connections running.
```

Este resultado sugiere que el servidor de SSH está inhabilitado o que no está habilitado correctamente. Si usted ya ha configurado SSH, se recomienda reconfigurar el servidor de SSH en el dispositivo. Complete estos pasos para volver a configurar el servidor SSH en el dispositivo.

- Elimine los pares de claves RSA. Después de eliminarse los pares de claves RSA, el servidor SSH se deshabilita automáticamente.

```
carter(config)#crypto key zeroize rsa
```

Nota: Es importante generar pares de claves con al menos 768 de tamaño de bits cuando habilita SSH v2.

Precaución: Este comando no se puede deshacer después de guardar la configuración. Además, después de que se eliminan las claves RSA, no puede utilizar certificados ni la CA ni participar en intercambios de certificados con otros pares de seguridad IP (IPSec) a menos que vuelva a generar las claves RSA para volver a configurar la interoperabilidad de la CA, obtener el certificado de CA y volver a solicitar su propio certificado.

2. Vuelva a configurar el nombre de host y el nombre de dominio del dispositivo.

```
carter(config)#hostname hostname

carter(config)#ip domain-name domainname
```

3.Genere pares de claves RSA para su router. Esto activa SSH automáticamente.

```
carter(config)#crypto key generate rsa
```

Nota: Consulte Crypto Key Generate rsa - Referencia de comandos de seguridad de Cisco IOS, versión 12.3 para obtener más información sobre el uso de este comando.

Nota: Puede recibir el mensaje de error `SSH2 0: Tipo de mensaje recibido inesperado` debido a un paquete recibido que el router no puede comprender. Aumente la longitud de la llave cuando genere llaves RSA para SSH a fin de resolver este problema.

4. Configure el servidor de SSH.

5. Para habilitar y configurar un router/switch Cisco para el servidor SSH, debe configurar los parámetros de SSH. Si no configura los parámetros de SSH, se utilizarán los valores predeterminados.

ip ssh {[timeout seconds] | [authentication-retries integer]}

```
carter(config)# ip ssh
```

Información Relacionada

- **Página de Soporte de Productos de SSH**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).