

Configurar SSH nos roteadores e switches

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conventions](#)

[Diagrama de rede SSH v2](#)

[Autenticação de teste](#)

[Teste da autenticação sem SSH](#)

[Teste da autenticação com SSH](#)

[Conjuntos de configurações opcionais](#)

[Previna conexões não-SSH](#)

[Estabelecer um IOS Router ou um interruptor como o cliente SSH](#)

[Configurar um roteador IOS como servidor SSH que executa a autenticação de usuário de RSA](#)

[Adicionar o acesso de linha terminal SSH](#)

[Restrinja o acesso SSH a uma sub-rede](#)

[Configurar o SSH versão 2](#)

[Variações na saída do comando da bandeira](#)

[Opções de comando de banner](#)

[Telnet](#)

[SSH v2](#)

[Não é possível exibir o LoginBanner](#)

[comandos debug e show](#)

[Exemplo de saída de depuração](#)

[Debug de Roteador](#)

[Depuração do servidor](#)

[Configurações incorretas](#)

[SSH de um cliente SSH não compilado com padrão de criptografia de dados \(DES\)](#)

[Senha incorreta](#)

[Debug de Roteador](#)

[O cliente SSH envia a cifra não suportada \(Blowfish\)](#)

[Debug de Roteador](#)

[Obter erro "%SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for"](#)

[Dicas](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar e depurar o Secure Shell (SSH) nos roteadores ou

switches Cisco que executam o software Cisco IOS®.

Pré-requisitos

Requisitos

A imagem IOS Cisco usada deve ser uma k9(crypto) imagem a fim de dar suporte ao SSH. Por exemplo, c3750e-universalk9-tar.122-35.SE5.tar é uma imagem k9 (criptografia).

Componentes Utilizados

A informação neste documento é baseada no software do Cisco IOS 3600 (C3640-IK9S-M), a liberação 12.2(2)T1.

O SSH foi introduzido nestas plataformas do Cisco IOS e imagens:

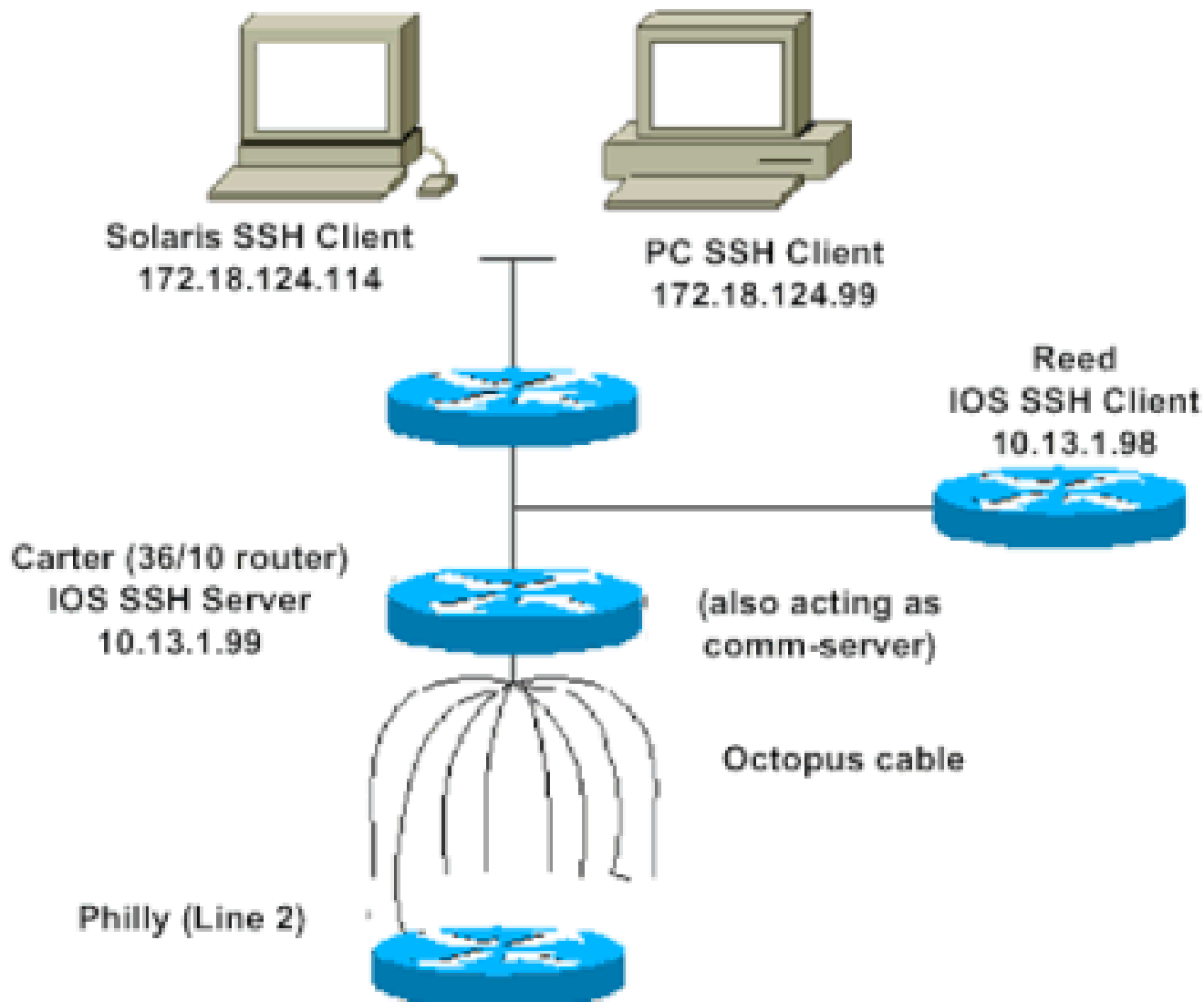
- O acesso de linha de terminal SSH (também conhecido como Telnet reverso) foi lançado nas plataformas e imagens do Cisco IOS a partir do software Cisco IOS versão 12.2.2.T.
- O suporte ao SSH versão 2.0 (SSH v2) foi lançado nas plataformas e imagens do Cisco IOS a partir do software Cisco IOS versão 12.1(19)E.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Consulte as [Convenções de dicas técnicas da Cisco](#) para obter mais informações.

Diagrama de rede SSH v2



Autenticação de teste

Teste da autenticação sem SSH

Teste primeiramente a autenticação sem SSH para certificar-se de que a autenticação trabalha com o roteador Carter antes que você adicione o SSH. A autenticação pode ser com um nome de usuário e uma senha locais ou com um servidor de autenticação, autorização e contabilização (AAA) que executa o TACACS+ ou RADIUS. (A autenticação por meio da senha de linha não é possível com o SSH.) Este exemplo mostra a autenticação local, que permite executar o Telnet no roteador com o nome de usuário cisco e a senha cisco.

 Observação: ao longo deste documento, vty é usado para indicar o tipo de terminal virtual.

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

```
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.

Teste da autenticação com SSH

Para testar a autenticação com o SSH, você precisa adicionar às instruções anteriores para ativar o SSH no Carter e testar o SSH nas estações PC e 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
```

Neste momento, o comando `show crypto key mypubkey rsa` deve mostrar a chave gerada. Depois que você adiciona a configuração SSH, teste sua capacidade para acessar o roteador do PC e da estação Unix.

Conjuntos de configurações opcionais

Previna conexões não-SSH

Se você quer prevenir conexões não-SSH, adicione o comando `transport input ssh` sob as linhas limitar o roteador somente às conexões de SSH. Telnets (não-SSH) diretos são recusados.

```
line vty 0 4
```

!--- Prevent non-SSH Telnets.

```
transport input ssh
```

Teste para garantir que usuários não SSH não possam executar o Telnet no Carter do roteador.

Estabelecer um IOS Router ou um interruptor como o cliente SSH

Há quatro etapas exigidas para permitir o apoio SSH em um roteador do Cisco IOS:

1. Configure o comando `hostname`.
2. Configure o domínio DNS.

3. Gere a chave SSH.

4. Ative o suporte ao transporte SSH do vty.

Se você quer mandar um dispositivo atuar como um cliente SSH ao outro, você pode adicionar o SSH a um segundo dispositivo chamado Reed. Isso coloca esses dispositivos em uma disposição de cliente-servidor, em que Carter atua como o servidor, e Reed atua como o cliente. A configuração do cliente SSH do Cisco IOS em Reed é a mesma como necessário para a configuração do servidor SSH em 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 a

```
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 s

```
line vty 0 4  
transport input ssh
```

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

Emita este comando para o SSH, do cliente SSH do Cisco IOS (Reed) para o servidor SSH do Cisco IOS (Carter), para testar o seguinte:

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

Configurar um roteador IOS como servidor SSH que executa a autenticação de usuário de RSA

Siga estas etapas para configurar o servidor SSH para executar a autenticação de RSA.

1. Especifique o nome de host.

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

2. Defina o nome de domínio padrão.

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

3. Gere pares de chaves RSA.

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

4. Configure as chaves SSH-RSA para autenticação de usuário e servidor.

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

5. Configure o nome do usuário SSH.

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

6. Especifique a chave pública RSA do par remoto.

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

7. Especifique o tipo e a versão da chave SSH. (Essa etapa é opcional.)

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

8. Saia do modo atual e retorne ao modo EXEC com privilégios.

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

Adicionar o acesso de linha terminal SSH

Se você precisa a autenticação de linha terminal SSH de saída, você pode configurar e testar o SSH para Telnets reverso de partida através de Carter, que actua como um servidor comm para 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
```

Se o Philly estiver conectado à Porta 2 do Carter, você poderá configurar o SSH para o Philly por meio do Carter no Reed com este comando:

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

Você pode usar este comando do Solaris:

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

Restrinja o acesso SSH a uma sub-rede

Você precisa limitar a conectividade SSH a uma sub-rede específica, em que todas as outras tentativas de SSH dos IPs fora da sub-rede são descartadas.


Você pode usar estas etapas para fazer o mesmo:

1. Defina uma lista de acesso que permita o tráfego dessa sub-rede específica.
2. Restrinja o acesso à interface de linha VTY com um acesso-classe.

Este é um exemplo de configuração. Neste exemplo, apenas o acesso SSH à sub-rede 10.10.10.0 255.255.255.0 é permitido; outro acesso será negado.

```
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
```

 Observação: o mesmo procedimento para bloquear o acesso SSH também é usado para plataformas de switch.


Configurar o SSH versão 2

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

Variações na saída do comando da bandeira

A saída do comando banner varia entre o Telnet e diferentes versões das conexões de SSH. Esta tabela ilustra como diferentes opções de comando do banner funcionam com vários tipos de conexões.

Opções de comando de banner	Telnet	SSH v2
registro de banner	Exibido antes de fazer login no dispositivo.	Exibido antes de fazer login no dispositivo.
banner motd	Exibido antes de fazer login no dispositivo.	Exibido após fazer login no dispositivo.
banner exec	Exibido após fazer login no dispositivo.	Exibido após fazer login no dispositivo.

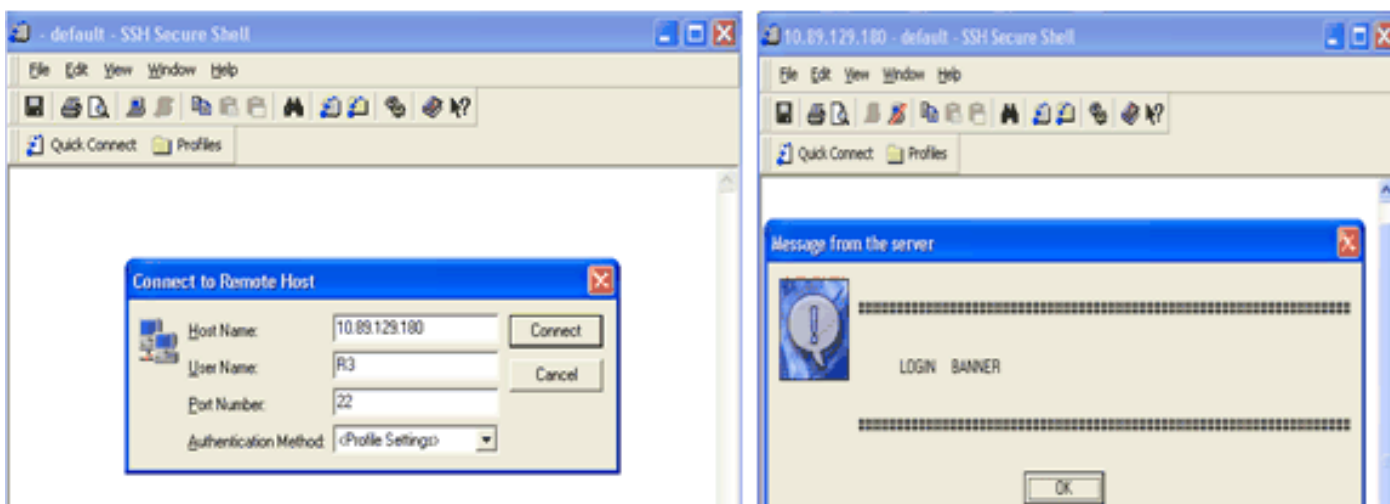
 Observação: o SSH versão 1 não é mais recomendado.

Incapaz de indicar o banner de login

O SSH versão 2 é compatível com o banner de login. Ao iniciar a sessão SSH com o roteador Cisco, o banner de login será exibido se o cliente SSH enviar o nome de usuário. Por exemplo, quando o cliente SSH do Secure Shell é usado, o banner de login é exibido. Quando o cliente SSH do PuTTY é usado, o banner de login não é exibido. Isso ocorre porque o SSH envia o nome de usuário por padrão e o PuTTY não envia o nome de usuário por padrão.

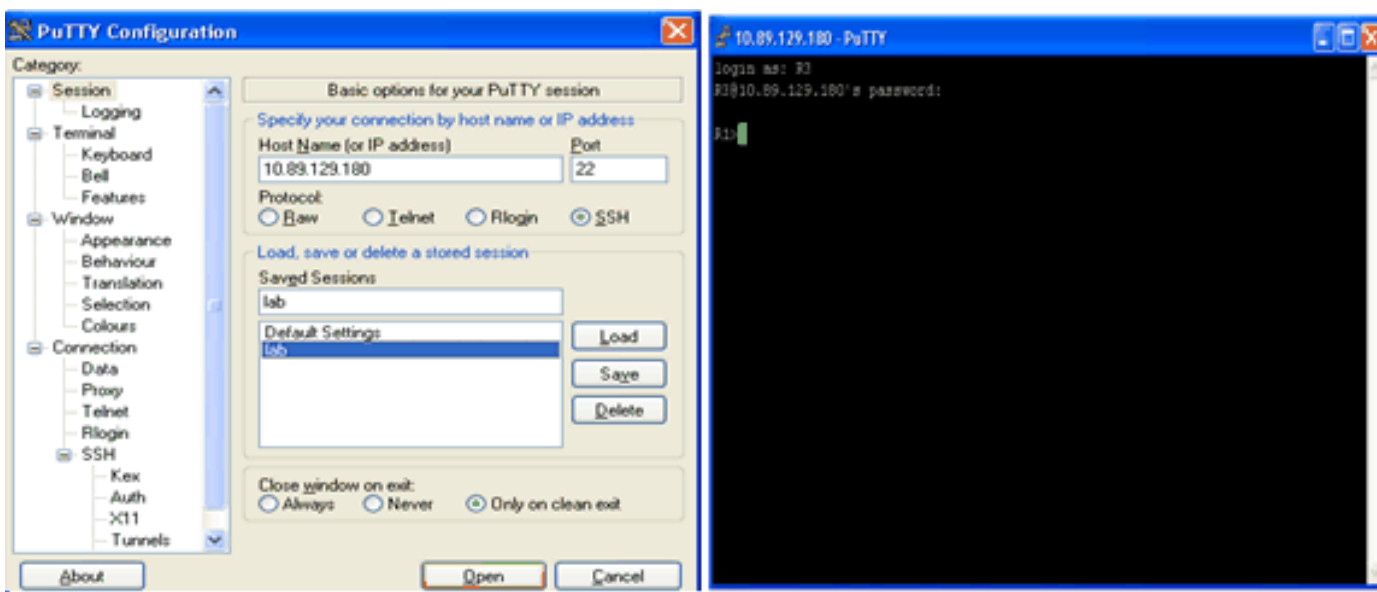
O cliente SSH precisa do nome de usuário para iniciar a conexão com o dispositivo compatível com SSH. O botão connect não está habilitado se você não digitar o nome de host e nome de

usuário. Esta imagem da tela mostra que o banner de login é exibido quando o SSH se conecta ao roteador. O banner solicitará uma senha.



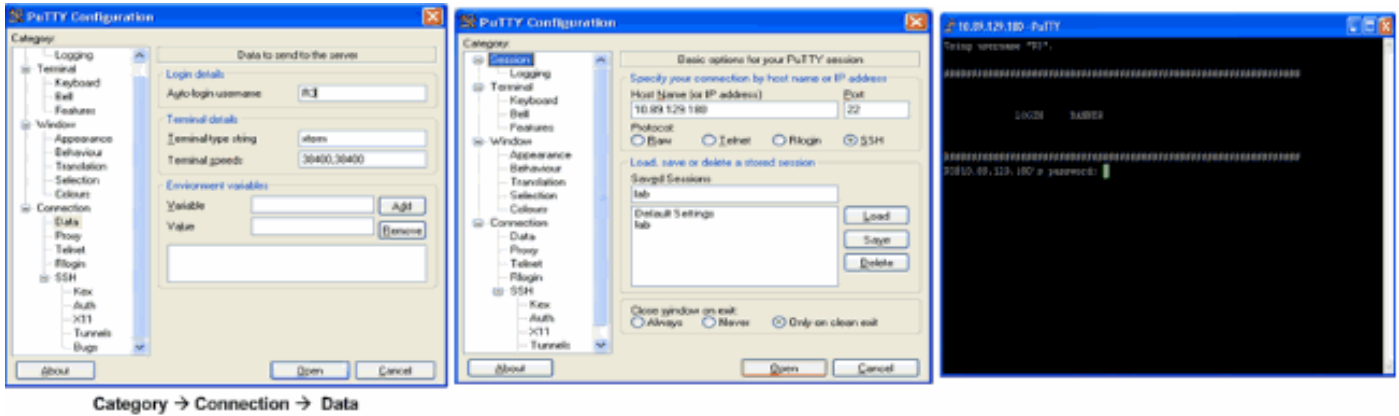
Prompts de banner para uma senha

O cliente PuTTY não requer o nome de usuário para iniciar a conexão SSH ao roteador. Esta imagem da tela mostra que o cliente PuTTY se conecta ao roteador e solicita o nome de usuário e a senha. Ela não exibe o banner de login.



Conexão SSH com o roteador

Esta captura de tela mostra que o banner de login é exibido quando o PuTTY é configurado para enviar o nome de usuário ao roteador.



Enviar nome de usuário para o roteador

comandos debug e show

Antes de emitir os comandos debug descritos aqui, consulte [Informações importantes sobre os comandos debug](#). Alguns comandos show são compatíveis com a [ferramenta Interpretador Externo](#) (registrada somente para clientes), que permite visualizar uma análise da saída do comando show.

- debug ip ssh Exibe mensagens de depuração para SSH.
- show ssh Exibe o status das conexões do servidor SSH.

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

- show ip ssh Exibe a versão e os dados de configuração do SSH.

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

Exemplo de saída de depuração

Debug de Roteador

```
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_MSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_MSG_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
```

Depuração do servidor



Observação: esta é a saída do computador 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.
```

Configurações incorretas

Estas seções têm o exemplo de debug de diversas configurações incorretas.

SSH de um cliente SSH não compilado com padrão de criptografia de dados (DES)

Senha incorreta

Debug de Roteador

```
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_MSG_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_MSG_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_MSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

O cliente SSH envia a cifra não suportada (Blowfish)

Debug de Roteador

```
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_MSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

Obter erro "%SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for"

Uma alteração no nome de domínio ou no nome de host pode acionar essa mensagem de erro. Use estas soluções alternativas:

- Zere as chaves RSA e regenere as chaves.

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

- Se a ação alternativa precedente não funcionar, tente estas etapas:
 1. Zere todas as chaves RSA.
 2. Recarregue o dispositivo.
 3. Crie chaves etiquetadas novas para o SSH.

Dicas

- Se seus comandos de configuração SSH são rejeitados como comandos ilegais, você não gerou com sucesso um par de chaves RSA para seu roteador. Verifique se você especificou um nome de host e um domínio. Em seguida, use o comando `crypto key generate rsa` para gerar pares de chaves RSA e ativar o servidor SSH.
- Ao configurar os pares de chaves RSA, você pode obter estas mensagens de erro:

1. Nenhum hostname especificado.

Use o comando de configuração global `hostname` para configurar um nome de host para o roteador.

2. Nenhum domínio especificado.

Use o comando de configuração global `ip domain-name` para configurar um domínio de host para o roteador.

- O número de conexões SSH permitidas é limitado ao número máximo de conexões `vtty` configuradas para o roteador. Cada conexão SSH usa um `vtty` recurso.

-

O SSH usa a segurança local ou o protocolo de segurança configurado por meio de AAA no roteador para autenticação do usuário. Ao configurar o AAA, você deve garantir que o console não seja executado no AAA. Aplique uma palavra-chave no modo de configuração global para desativar o AAA no console.

-

No SSH server connections running:

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

Esta saída sugere que o servidor de SSH seja desabilitado ou não habilitado corretamente. Se você já configurou o SSH, recomenda-se que você reconfigure o servidor de SSH no dispositivo. Siga estas etapas para reconfigurar o servidor SSH no dispositivo.

- Exclua os pares de chaves RSA. Depois que os pares de chaves RSA são excluídos, o servidor SSH é desativado automaticamente.

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



Observação: é importante gerar pares de chaves com um tamanho de bit de pelo menos 768 quando você ativa o SSH v2.



Cuidado: este comando não poderá ser desfeito depois que você salvar a configuração. Além disso, após a exclusão das chaves RSA, você não pode usar certificados ou a CA nem participar de trocas de certificados com outros pares de segurança IP (IPSec), a menos que gere novamente as chaves RSA para reconfigurar a interoperabilidade de CA, obter o certificado de CA e solicitar seu próprio certificado novamente.

2. Reconfigure o nome de host e o nome de domínio do dispositivo.

```
carter(config)#hostname hostname
```

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

3. Gere os pares de chaves RSA para o roteador. Isso ativa o SSH automaticamente.

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



Observação: consulte [crypto key generate rsa – Referência de comando de segurança do Cisco IOS, versão 12.3](#) para obter mais informações sobre o uso desse comando.



Observação: você pode receber a mensagem de erro SSH2 0: Unexpected mesg type received devido a um pacote recebido que o roteador não pode entender. Aumente o comprimento da chave quando você gerar chaves RSA para o ssh a fim resolver este problema.

4. Configure o servidor SSH.

5. Para ativar e configurar um roteador/switch Cisco para o servidor SSH, configure os parâmetros SSH. Se você não configurar parâmetros SSH, os valores padrão serão usados.

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

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

Informações Relacionadas

- [Página de Suporte ao Produto SSH](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.