Configuring Secure Shell on Routers and Switches Running Cisco IOS

Índice

Introdução

O Secure Shell (SSH) é um protocolo que fornece uma conexão segura de acesso remoto aos dispositivos de rede. Uma comunicação entre o cliente e servidor é criptografada na versão de SSH 2 do instrumento da versão de SSH 1 e da versão de SSH 2. quando possível porque usa um algoritmo avançado de criptografia da segurança.

Este documento discute como configurar e debugar o SSH nos roteadores Cisco ou no Switches

que executam uma versão do Cisco IOS ® Software que apoie o SSH. Este original contem mais informação em versões específicas e imagens do software.

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 (cripto).

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 servidor SSH Versão 1.0 (SSH v1) foi introduzido em algumas plataformas do Cisco IOS e imagens que começam no Cisco IOS Software Release 12.0.5.S.

- O cliente SSH foi introduzido em algumas plataformas do Cisco IOS e imagens que começam no Cisco IOS Software Release 12.1.3.T.

- O acesso de linha terminal SSH (igualmente conhecido como o reverso-Telnet) foi introduzido em algumas plataformas do Cisco IOS e imagens que começam no Cisco IOS Software Release 12.2.2.T.

- O suporte do SSH 2.0 (SSH v2) foi introduzido em algumas plataformas do Cisco IOS e imagens que começam no Cisco IOS Software Release 12.1(19)E.

- Refira a Como configurar o SSH nos Catalyst Switches que executam CatOS para mais informações sobre o suporte SSH nos interruptores.

Refira o Software Advisor (somente clientes registrados) para uma lista completa dos conjuntos de recursos apoiados em Cisco IOS Software Release diferentes e em plataformas diferentes.

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 você está em uma rede ao vivo, certifique-se de que você compreende o impacto potencial de qualquer comando antes que você o use.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

SSH v1 ss. SSH v2

Use o Cisco Software Advisor (somente clientes registrados) a fim ajudá-lo a encontrar a versão de código com suporte apropriado para o SSH v1 ou o SSH v2.

Diagrama de Rede

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 local e uma senha ou com um server do autenticação, autorização e relatório (AAA) que execute o TACACS+ ou o RAIO. (A autenticação com a senha de linha não é possível com SSH.) Este exemplo mostra a autenticação local, que o deixa Telnet no roteador com usuário “Cisco” e senha “Cisco.”

```
!--- The aaa new-model command causes the local username and password on the router !--- to be used in the absence of other AAA statements. 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

Autenticação de teste com SSH, você deve adicionar às declarações precedente a fim de permitir o SSH em Carter e testar o SSH do PC e das estações 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. Se isto não funcionar, veja a seção debugar deste documento.

Definições de configuração opcional

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 certificar-se de que os usuários não-SSH não podem utilizar o Telnet ao roteador Carter.

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:

Configurar o **comando hostname**.

Configure o domínio do DNS.

Gere a chave SSH a ser usada.

Permita o suporte de transporte SSH para o terminal de tipo virtual (vtys).

Se você quer mandar um dispositivo atuar como um cliente SSH ao outro, você pode adicionar o SSH a um segundo dispositivo chamado Reed. Estes dispositivos estão então em uma organização cliente/servidor, onde 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 absence of other AAA statements. 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 vtys' transport is Telnet. In this case, !--- Telnet is
disabled and only SSH is supported. line vty 0 4 transport input SSH !--- Instead of aaa new-
model, you can use the login local command.
```

Emita este comando ao SSH do cliente SSH do Cisco IOS (Reed) ao servidor SSH do Cisco IOS (Carter) para testar isto:

SSH v1:

```
ssh -l cisco -c 3des 10.13.1.99
```

SSH v2:

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

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

Complete estas etapas a fim configurar o servidor SSH para executar a autenticação baseada RSA.

Especifique o nome de host.

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

Defina um nome de domínio padrão.

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

Gere pares de chaves RSA.

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

Configurar chaves SSH-RSA para o usuário e a autenticação de servidor.

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

Configurar o nome de usuário SSH.

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

Especifique a chave pública RSA do peer remoto.

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

Especifique o tipo e a versão da chave SSH. (opcional)

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

Retire o modo atual e retorne ao modo privilegiado EXEC.

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

Nota: Refira o apoio da versão 2 do Secure Shell para mais informação.

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 In Out
   Stopbits 1
```

Se Philly for anexado à porta 2 de Carter, a seguir você pode configurar o SSH a Philly através de Carter de Reed com a ajuda deste comando:

SSH v1:

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

SSH v2:

```
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 onde todas tentativas SSH restantes dos IP fora da sub-rede devam ser deixadas cair.

Você pode usar estas etapas para realizar o mesmos:

Defina uma lista de acesso que permita o tráfego dessa sub-rede específica.

Restrinja o acesso à interface de linha VTY com um acesso-classe.

Este é um exemplo de configuração. Neste exemplo somente o SSH é permitido acesso à sub-rede 10.10.10.0 255.255.255.0, a qualquer outro é negado o acesso.

```
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: O mesmo procedimento para travar o acesso SSH é igualmente aplicável em plataformas do switch.

Configurar a versão de SSH

Configurar o SSH v1:

```
carter(config)#ip ssh version 1
```

Configurar o SSH v2:

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

Configurar o SSH v1 e v2:

```
carter(config)#no ip ssh version
```

Nota: Você recebe esta mensagem de erro quando você usa SSHv1:

```
%SCHED-3-THRASHING: Process thrashing on watched message event.
```

Nota: A ID de bug Cisco CSCsu51740 (somente clientes registrados) são arquivada para este problema. O Workaround é configurar SSHv2.

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.

Opção de Comando de Banner	Telnet	Somente SSH v1	SSH v1 e v2	Somente SSH v2
banner login	Indicado **antes de** registrar	Não indicado.	Indicado **antes de** registrar	Indicado **antes de** registrar

	no dispositivo.		no dispositivo.	no dispositivo.
banner motd	Indicado **antes de** registrar no dispositivo.	Indicado **após o** registo no dispositivo.	Indicado **após o** registo no dispositivo.	Indicado **após o** registo no dispositivo.
banner exec	Indicado **após o** registo no dispositivo.	Indicado **após o** registo no dispositivo.	Indicado **após o** registo no dispositivo.	Indicado **após o** registo no dispositivo.

Incapaz de indicar o banner de login

O SSH versão 2 suporta o banner de login. O banner de login está indicado se o cliente SSH envia o nome de usuário quando inicia a sessão SSH com o roteador Cisco. Por exemplo, quando o cliente SSH do Secure Shell é usado, o banner de login é indicado. Quando o cliente SSH da massa de vidraceiro é usado, o banner de login não está indicado. Isto é porque o Secure Shell envia o nome de usuário por padrão e PuTTY não envia o nome por padrão.

O cliente do Secure Shell precisa o nome de usuário para iniciar a conexão ao dispositivo SSH habilitado. O botão connect não está habilitado se você não digitar o nome de host e nome de usuário. Este screenshot mostra que o banner de login é mostrado quando o Secure Shell se conectar ao roteador. Então, o prompt da senha do banner de login é mostrado.

O cliente PuTTY não requer o nome de usuário para iniciar a conexão SSH ao roteador. Este screenshot mostra que o cliente PuTTY se conecta ao roteador e às alertas para o nome de usuário e senha. Ele não mostra o banner de login.

Este screen shot mostra que o banner de login está indicado quando a massa de vidraceiro é configurada para enviar o username ao roteador.

comandos debug e show

Antes que você emita os **comandos debug** descritos e ilustrados aqui, refira a informação importante em comandos Debug. A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

debugar indicadores do do do **sshâ IP** debugam mensagens para o SSH.

mostre que do do **sshâ** indica os status da conexão de servidor SSH.

```
carter#show ssh Connection Version Encryption State Username 0 1.5 DES Session started cisco
```

mostre que do do **sshâ IP** indica a versão e os dados de configuração para o SSH.

Conexão da versão 1 e nenhuma versão 2

```
carter#show ip ssh SSH Enabled - version 1.5 Authentication timeout: 60 secs;
Authentication retries: 2
```

Conexão da versão 2 e nenhuma versão 1

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

Conexões da versão 1 e da versão 2

```
carter#show ip ssh SSH Enabled - version 1.99 Authentication timeout: 120 secs;
Authentication retries: 3
```

Exemplo de debug

Debug de Roteador

Nota: Algumas destas saídas do debug correto é envolvida em múltiplas linhas devido à considerações espaciais.

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-1.5-1.2.26
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
```

Depuração do servidor

Nota: Esta saída foi capturada em uma máquina de 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 1.5, 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.

que pode dar errado

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

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

Solaris Debug

rtp-evergreen#**/opt/CISssh/bin/ssh -c des -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 1.5, 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: des rtp-evergreen: Sent encrypted session key. cipher_set_key: unknown cipher: 2

Debug de Roteador

```
00:24:41: SSH0: Session terminated normally
00:24:55: SSH0: starting SSH control process
00:24:55: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:24:55: SSH0: protocol version id is - SSH-1.5-1.2.26
00:24:55: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:24:55: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:24:55: SSH: RSA decrypt started
00:24:56: SSH: RSA decrypt finished
00:24:56: SSH: RSA decrypt started
00:24:56: SSH: RSA decrypt finished
00:24:56: SSH0: sending encryption confirmation
00:24:56: SSH0: Session disconnected - error 0x07
```

Senha incorreta

Debug de Roteador

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-1.5-1.2.26
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
```

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-1.5-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-1.5-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
```

Obtendo o "%SSH-3-PRIVATEKEY: Incapaz de recuperar a chave privada RSA para o" erro

Se você recebe este Mensagem de Erro, esta pode ser causada devido a qualquer alteração no Nome de Domínio ou no nome de host. A fim resolver isto, tente estas ações 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:

Zere todas as chaves RSA.

Recarregue o dispositivo.

Crie chaves etiquetadas novas para o SSH.

A identificação de bug Cisco CSCsa83601 (somente clientes registrados) foi arquivada para endereçar este comportamento.

Dicas para Troubleshooting

Se seus comandos de configuração SSH são rejeitados como comandos ilegais, você não gerou com sucesso um par de chaves RSA para seu roteador. Certifique-se de você ter especificado um nome de host e um domínio. Use então o **comando crypto key generate rsa** para gerar um par de chaves RSA e habilitar o servidor SSH.

Quando você configura o par de chaves RSA, você pode encontrar estas Mensagens de Erro:

`Nenhum hostname especificado`

Você deve configurar um nome de host para o roteador que usa o comando global configuration do **hostname**.

`Nenhum domínio especificado`

Você deve configurar um domínio do host para o roteador usando o **comando ip domain-name global configuration**.

O número de conexões SSH permitidas é limitado ao número máximo de vtys configurados para o roteador. Cada conexão SSH usa um recurso vty.

O SSH usa a segurança local ou o protocolo de segurança que é configurado com o AAA em seu roteador para a autenticação de usuário. Quando você configura o AAA, você deve assegurar-se de que o console não esteja sendo executado sob o AAA aplicando uma palavra-chave no modo de configuração global para desabilitar o AAA no console.

`Nenhuma conexão do servidor SSH está sendo executado.`

`carter#`**`show ssh`** `%No SSHv2 server connections running. %No SSHv1 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. Termine estas etapas a fim reconfigurar o servidor de SSH no dispositivo.

Suprima do par de chaves RSA. Depois que o par de chaves RSA é suprimido, o servidor de SSH é desabilitado automaticamente.

`carter(config)#`**`crypto key zeroize rsa`**
Nota: É importante gerar um par de chaves com tamanho de bit de pelo menos 768 quando você permite o SSH v2.

Cuidado: Este comando não pode ser desfeito depois que você salvar sua configuração, e depois que as chaves RSA estiveram suprimidas, você não pode usar certificados ou o CA ou participar em trocas do certificado com outros pares da Segurança IP (IPSec) a menos que você reconfigure a interoperabilidade CA regenerando as chaves RSA, obtendo o certificado de CA, e pedindo seu próprio certificado outra vez. Refira ao crypto key zeroize rsa - Cisco IOS Security Command Reference, Release 12.3 para obter mais informações sobre este comando.

Reconfigure o hostname e o Domain Name do dispositivo.

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

Gere um par de chaves RSA para seu roteador, que habilite automaticamente o SSH.

`carter(config)#`**`crypto key generate rsa`**
Refira a crypto key generate rsa - Cisco IOS Security Command Reference, Release 12.3 para obter mais informações sobre o uso deste comando.

Nota: Você pode receber o SSH2 0: A mensagem de erro Unexpected msdg type recieved devido ao pacote recebido que não é compreendido pelo roteador. Aumente o comprimento da chave quando você gerar chaves RSA para o ssh a fim resolver este problema.

Configurar o servidor SSH. A fim permitir e configurar um roteador Cisco/interruptor para o servidor de SSH, você pode configurar parâmetros SSH. Se você não configurar parâmetros SSH, os valores padrão serão usados.

ip ssh {[timeout seconds] | [[authentication-retries integer]} `carter(config)#` **`ip ssh`**
Refira a ip ssh - Cisco IOS Security Command reference, Release 12.3 para mais informações sobre do uso deste comando.

Informações Relacionadas

- Como configurar o SSH nos Catalyst Switches que executam CatOS
- Secure Shell Version 2 Support
- Página de Suporte ao Produto SSH
- Suporte Técnico e Documentação - Cisco Systems