在运行 Cisco IOS 的路由器与交换机上配置 Secure Shell

目录

简介

安全壳 (SSH) 是一种提供到网络设备的安全远程访问连接的协议。在 SSH 版本 1 和 SSH 版本 2 中，客户端与服务器之间的通信是加密的。如有可能，请实施 SSH 版本 2，因为它采用的安全加密算法更强。

本文档讨论如何在运行支持 SSH 的 Cisco IOS® 软件版本的 Cisco 路由器或交换机上配置和调试 SSH。本文档包含有关特定版本和软件映像的详细信息。

先决条件

要求

使用的Cisco IOS镜像必须是**k9(crypto)**镜像为了支持SSH。例如**c3750e-universalk9-tar.122-35.SE5.tar**是k9 (crypto)镜像。

使用的组件

本文档中的信息基于 Cisco IOS 3600 软件 (C3640-IK9S-M) 版本 12.2(2)T1。

SSH介绍到这些Cisco IOS平台并且制作镜像：

SSH版本1.0 (SSH v1)服务器在Cisco IOS软件版本12.0.5.S启动的一些Cisco IOS平台和镜像介绍。

SSH客户端在一些Cisco IOS平台介绍并且制作镜像开始在Cisco IOS软件版本12.1.3.T。

SSH终端线路接入(亦称reverse-telnet)在一些Cisco IOS平台介绍并且制作镜像开始在Cisco IOS软件版本12.2.2.T。

SSH版本2.0 (SSH v2)支持在一些Cisco IOS平台介绍并且制作镜像开始在Cisco IOS软件版本12.1(19)E。

参考如何配置在运行CatOS的Catalyst交换机的SSH关于在交换机的SSH支持的更多信息。

有关不同 Cisco IOS 软件版本和不同平台支持的功能集的完整列表，请参阅 Software Advisor（仅限注册用户）。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您在使用任何命令前已经了解其潜在影响。

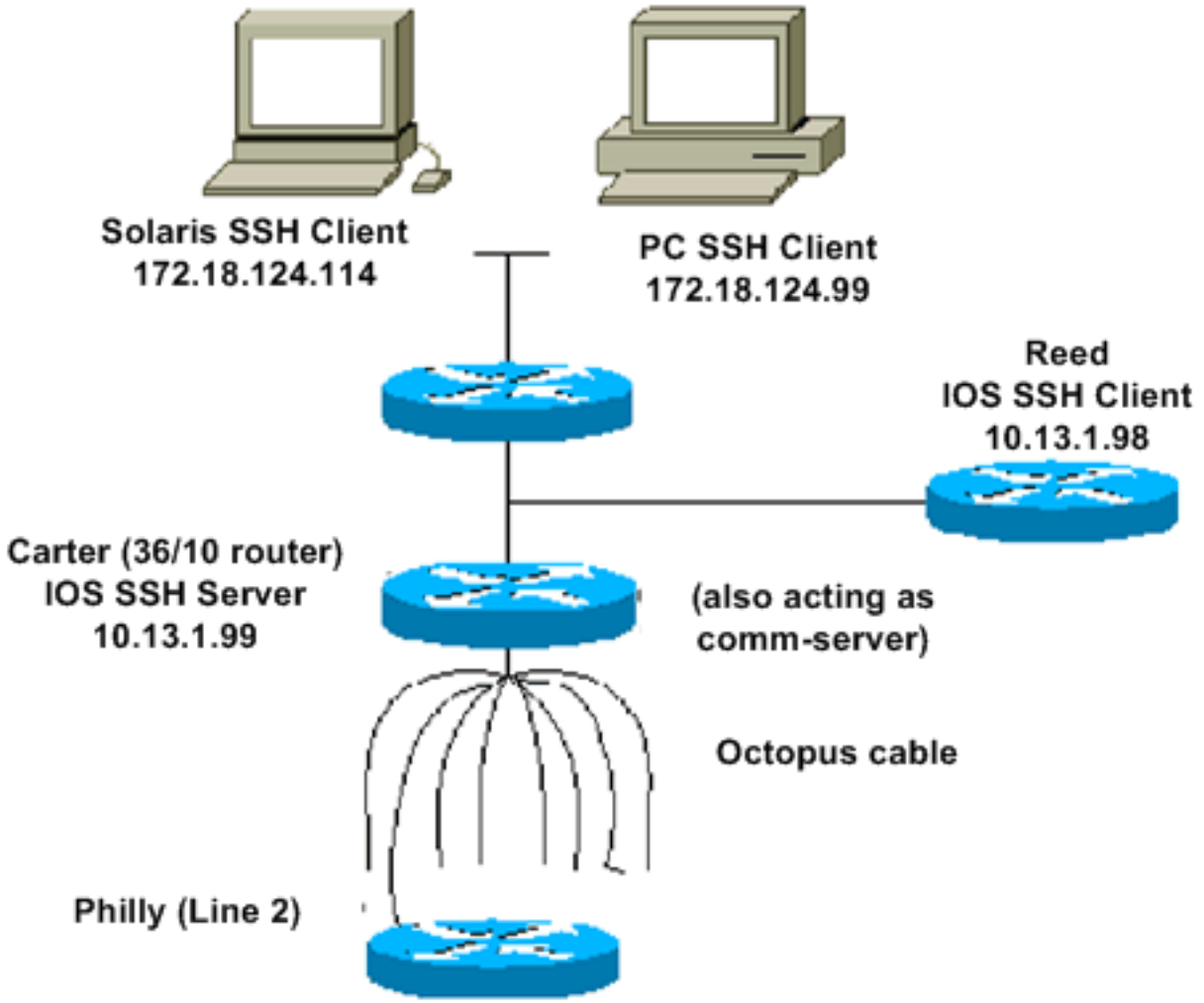
规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

SSH V1 与 SSH V2

请使用Cisco Software Advisor (仅限注册用户)为了帮助您查找与适当的支持的编码版本SSH v1或SSH的v2。

网络图



测试身份验证

不使用 SSH 时的身份验证测试

首先在不使用 SSH 的情况下测试身份验证，以确保在您添加 SSH 之前，路由器 Carter 的身份验证工作正常。可以使用本地用户名和口令进行身份验证，也可以使用运行 TACACS+ 或 RADIUS 的身份验证、授权和记账 (AAA) 服务器进行身份验证。（对于 SSH，不能使用线路密码进行身份认证。）本示例说明了本地身份验证，本地身份验证允许您使用用户名“cisco”和口令“cisco”通过 Telnet 登录路由器。

```
!--- 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.
```

使用 SSH 时的身份验证测试

为了在使用 SSH 的情况下测试身份验证，必须添加之前的语句，才能在 Carter 上启用 SSH 并从 PC 和 UNIX 工作站测试 SSH。

```
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
```

这时， **show crypto key mypubkey rsa命令**必须显示生成的密钥。在添加 SSH 配置后，请测试从

PC 和 UNIX 工作站访问路由器的能力。如果不能进行访问，请参阅本文档的调试部分。

可选配置设置

阻止非 SSH 连接

如果要阻止非 SSH 连接，请在语句行的下面添加 **transport input ssh** 命令，将路由器限制为只能使用 SSH 连接。直接（非 SSH）Telnet 将被拒绝。

```
line vty 0 4
!--- Prevent non-SSH Telnets. transport input ssh
```

进行测试以确保非 SSH 用户不能通过 Telnet 登录路由器 Carter。

设置 IOS 路由器或交换机作为 SSH 客户端

有要求的四个步骤启用在Cisco IOS路由器的SSH支持：

配置 **hostname** 命令。

配置 DNS 域。

生成要使用的 SSH 密钥。

对虚拟类型终端 (vty) 启用 SSH 传输支持。

如果要让一台设备充当另一台设备的 SSH 客户端，可以在称为 Reed 的第二台设备上添加 SSH。然后，这些设备将处于客户端服务器布局中，其中 Carter 充当服务器，而 Reed 充当客户端。在Reed的Cisco IOS SSH客户端配置是相同的如所需求为在卡特的SSH服务器配置。

```
!--- 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.
```

发出此命令对从Cisco IOS SSH客户端(Reed)的SSH到Cisco IOS SSH服务器(卡特)为了测试此：

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
```

设置IOS路由器作为进行RSA基于用户认证的SSH服务器

完成这些步骤为了配置SSH服务器执行RSA基于验证。

指定主机名。

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

定义默认域名。

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

生成RSA密钥对。

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

配置用户和服务器验证的SSH-RSA密钥。

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

配置SSH用户名。

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

指定远端对等体的RSA公共密钥。

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

指定SSH密钥类型和版本。(可选)

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

退出电流模式和回归对特权EXEC模式。

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

注意： 参考的Secure Shell版本2支持欲知更多信息。

添加 SSH 终端线路接入

如果需要进行出站 SSH 终端线路身份验证，可以配置并测试通过 Carter（充当 Philly 的通信服务器）进行出站反向 Telnet 的 SSH。

```
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
```

如果 Philly 连接到 Carter 的端口 2，则可以在 Reed 中使用以下命令配置通过 Carter 以 SSH 方式

登录 Philly：

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
```

在 Solaris 上，可以使用以下命令：

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

限制对子网的SSH访问

您需要对应该丢弃从IP的其他SSH尝试子网的外部的一特定子网限制SSH连接。

您能使用这些步骤完成同样：

定义access-list该许可证从该特定子网的流量。

限制对VTY线路接口的访问与access-class。

这是配置示例。仅在对10.10.10.0 255.255.255.0子网的此示例SSH访问允许，任何其他是拒绝访问。

```
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
```

注意： 锁定的同一个步骤在SSH访问下也是可适用的在交换机平台。

配置 SSH 版本

配置 SSH V1：

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

配置 SSH V2：

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

配置 SSH V1 和 SSH V2：

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

注意： 当您使用SSHv1时，您收到此错误消息：

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

注意： Cisco Bug ID CSCsu51740 (仅限注册用户)为此问题被归档。应急方案是配置SSHv2。

banner 命令输出的变化

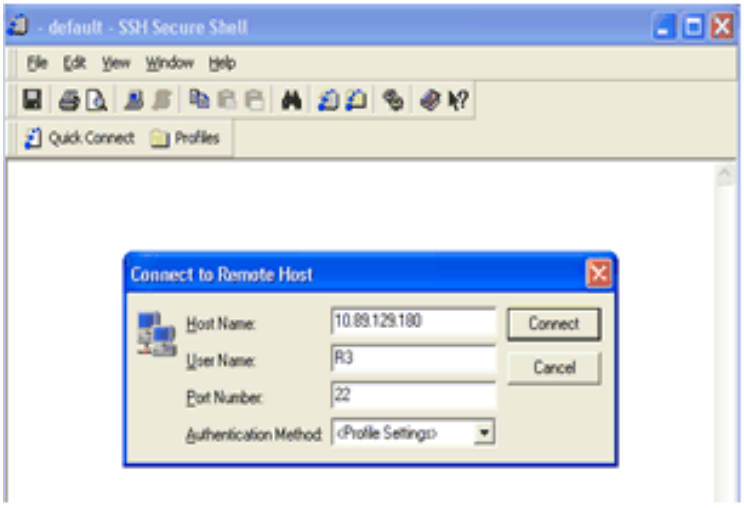
使用 Telnet 和不同版本的 SSH 连接时，**banner** 命令的输出会有所不同。下表说明了不同的 **banner** 命令选项如何处理各种类型的连接。

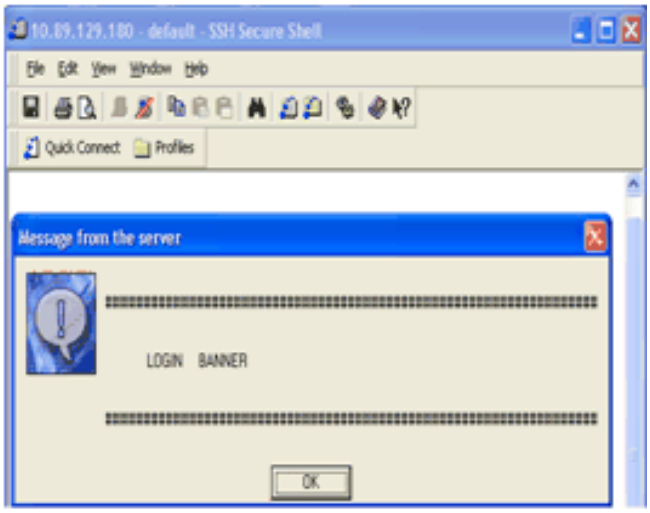
Banner 命令选项	Telnet	仅 SSH V1	SSH V1 和 SSH V2	仅 SSH V2
banner login	在登录设备**之前**显示。	不显示。	在登录设备**之前**显示。	在登录设备**之前**显示。
banner motd	在登录设备**之前**显示。	在登录设备**之后**显示。	在登录设备**之后**显示。	在登录设备**之后**显示。
banner exec	在登录设备**之后**显示。	在登录设备**之后**显示。	在登录设备**之后**显示。	在登录设备**之后**显示。

无法显示登录标语

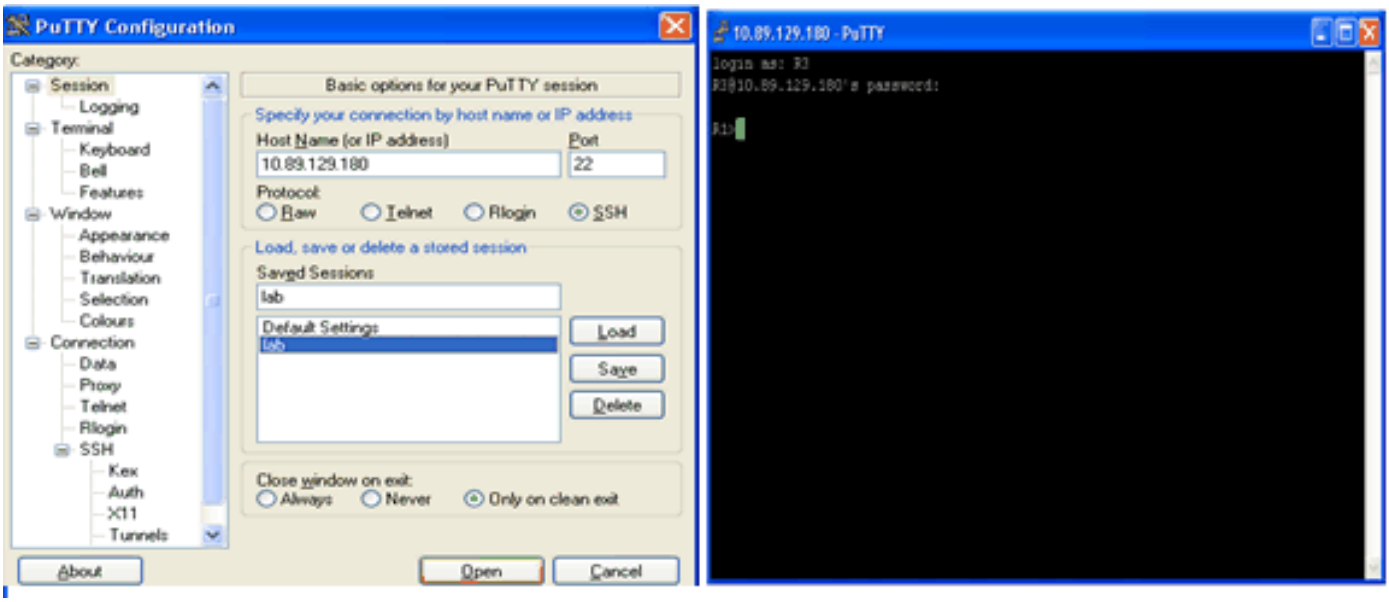
SSH 版本 2 支持登录标语。如果 SSH 客户端在向 Cisco 路由器发起 SSH 会话时发送用户名，则会显示登录标语。例如，当使用Secure Shell SSH 客户端时，会显示登录标语。使用 PuTTY SSH 客户端时，不会显示登录标语。这是因为默认情况下Secure Shell SSH 发送用户名，而 PuTTY 不发送用户名。

Secure Shell SSH 客户端需要用户名来发起到启用了 SSH 的设备的连接。如果不输入主机名和用户名，则不会启用 Connect 按钮。以下屏幕截图表明当Secure Shell SSH 连接到路由器时会显示登录标语。然后，会显示登录标语口令提示。

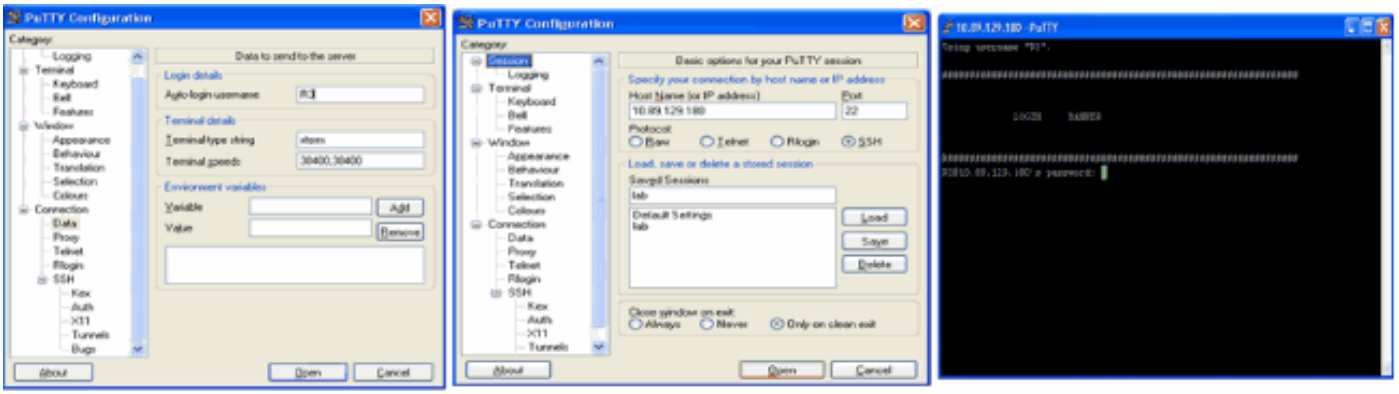




PuTTY 客户端不需要用户名来发起到路由器的 SSH 连接。以下屏幕截图表明当 PuTTY 客户端连接到路由器时会提示输入用户名和口令。它不显示登录标语。



此屏幕画面显示登录标识显示，当PuTTY配置发送用户名到路由器时。



Category → Connection → Data

debug 和 show 命令

在发出此处说明和演示的 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

debug ip sshâ 显示调试SSH的消息。

显示sshâ 显示SSH服务器连接状态。

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

显示ip sshâ 显示版本和配置数据SSH的。

版本 1 连接，没有版本 2

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

版本 2 连接，没有版本 1

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

```
Authentication retries: 3
```

版本 1 和版本 2 连接

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

调试输出示例

路由器调试

注意： 由于空间限制，某些正确的调试输出分若干行显示。

```
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
```

服务器调试

注意： 此输出是在 Solaris 计算机上捕获的。

```
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.

可能出现的错误

以下部分列出了几种不正确的配置导致的调试输出示例。

来自 SSH 客户端的 SSH 不是使用数据加密标准 (DES) 编译的

Solaris 调试

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

路由器调试

```
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
```

错误密码

路由器调试

```
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
```

SSH 客户端发送不支持的 (Blowfish) 密码

路由器调试

```
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
```

获得"%SSH-3-PRIVATEKEY ：无法获取”错误的RSA专用密钥

如果收到此错误消息，可能导致由于在域名或主机名上的所有变化。为了解决此，请尝试这些应急方案。

调零RSA密钥并且重新生成密钥。

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

如果上一个应急方案不工作，请尝试这些步骤：

调零所有RSA密钥。

重新启动设备。

创建SSH的新的被标记的密钥。

归档Cisco Bug ID CSCsa83601 (仅限注册用户)寻址此行为。

故障排除提示

如果 SSH 配置命令被作为非法命令拒绝，则说明您没有成功地为路由器生成 RSA 密钥对。请确保指定了主机名和域。然后，使用 **crypto key generate rsa** 命令生成 RSA 密钥对并启用 SSH 服务器。

配置 RSA 密钥对时，可能会遇到下列错误消息：

```
No hostname specified
```

此时，必须使用 **hostname** 全局配置命令为路由器配置一个主机名。

```
No domain specified
```

此时，必须使用 **ip domain-name** 全局配置命令为路由器配置一个主机域。

允许的 SSH 连接数受为路由器配置的 vty 的最大数目限制。每个 SSH 连接使用一个 vty 资源。

SSH 使用本地安全协议或通过路由器上的 AAA 配置的安全协议进行用户身份验证。配置 AAA 时，必须通过在全局配置模式下应用关键字来禁用控制台上的 AAA，确保控制台不在 AAA 系统下运行。

```
No SSH server connections running.
```

```
carter#show ssh %No SSHv2 server connections running. %No SSHv1 server connections running.
```

此输出表明 SSH 服务器被禁用或未正确启用。如果已经配置了 SSH，建议您在设备中重新配置 SSH 服务器。完成下列步骤在设备上重新配置 SSH 服务器。

删除 RSA 密钥对。在删除 RSA 密钥对后，SSH 服务器将自动禁用。

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

注意： 当您启用SSH v2时，生成与至少768的一密钥对作为比特大小是重要的。

警告： 在保存配置后，此命令将无法撤消。而且，在删除 RSA 密钥对后，您不能使用证书或 CA 与其他 IP 安全 (IPSec) 对等体进行证书交换，除非您通过重新生成 RSA 密钥、获取 CA 的证书并再次请求自己的证书重新配置 CA 互操作性。有关此命令的详细信息，请参阅 crypto key zeroize rsa - Cisco IOS 安全命令参考 12.3 版。

重新配置设备的主机名和域名。

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

为路由器生成 RSA 密钥对，这将自动启用 SSH。

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

有关此命令用法的详细信息，请参阅 crypto key generate rsa - Cisco IOS 安全命令参考 12.3 版。

注意： 您可能会收到如下错误消息：SSH2 0:Unexpected mesg type received，这是因为路由器无法理解接收到的数据包。要解决此问题，请在生成用于 SSH 的 RSA 密钥时增加密钥长度。

配置 SSH 服务器。为了启动并设定一Cisco路由器/交换机SSH服务器的，您能配置SSH参数。如果不配置 SSH 参数，将使用默认值。

ip ssh {[timeout seconds]|[[authentication-retries integer]} `carter(config)# ip ssh`
有关此命令用法的详细信息，请参阅 ip ssh - Cisco IOS 安全命令参考 12.3 版。

相关信息

- 如何在运行 CatOS 的 Catalyst 交换机上配置 SSH
- Secure Shell SSH 版本 2 支持
- SSH 产品支持页面
- 技术支持和文档 - Cisco Systems