在路由器和交換器上設定 SSH

目錄

簡介

本文件說明如何在執行 Cisco IOS® 軟體的思科路由器或交換器上設定安全殼層 (SSH)，以及為這

些 SSH 偵錯的方法。

必要條件

需求

使用的 Cisco IOS 映像必須是 k9（密碼編譯）映像才能支援 SSH。例如 c3750e-universalk9-tar.122-35.SE5.tar 就是 k9（密碼編譯）映像。

採用元件

本文提供的資訊以 Cisco IOS 3600 軟體 (C3640-IK9S-M) 的 12.2(2)T1 版為主。

SSH 已導入這些 Cisco IOS 平台和映像中：

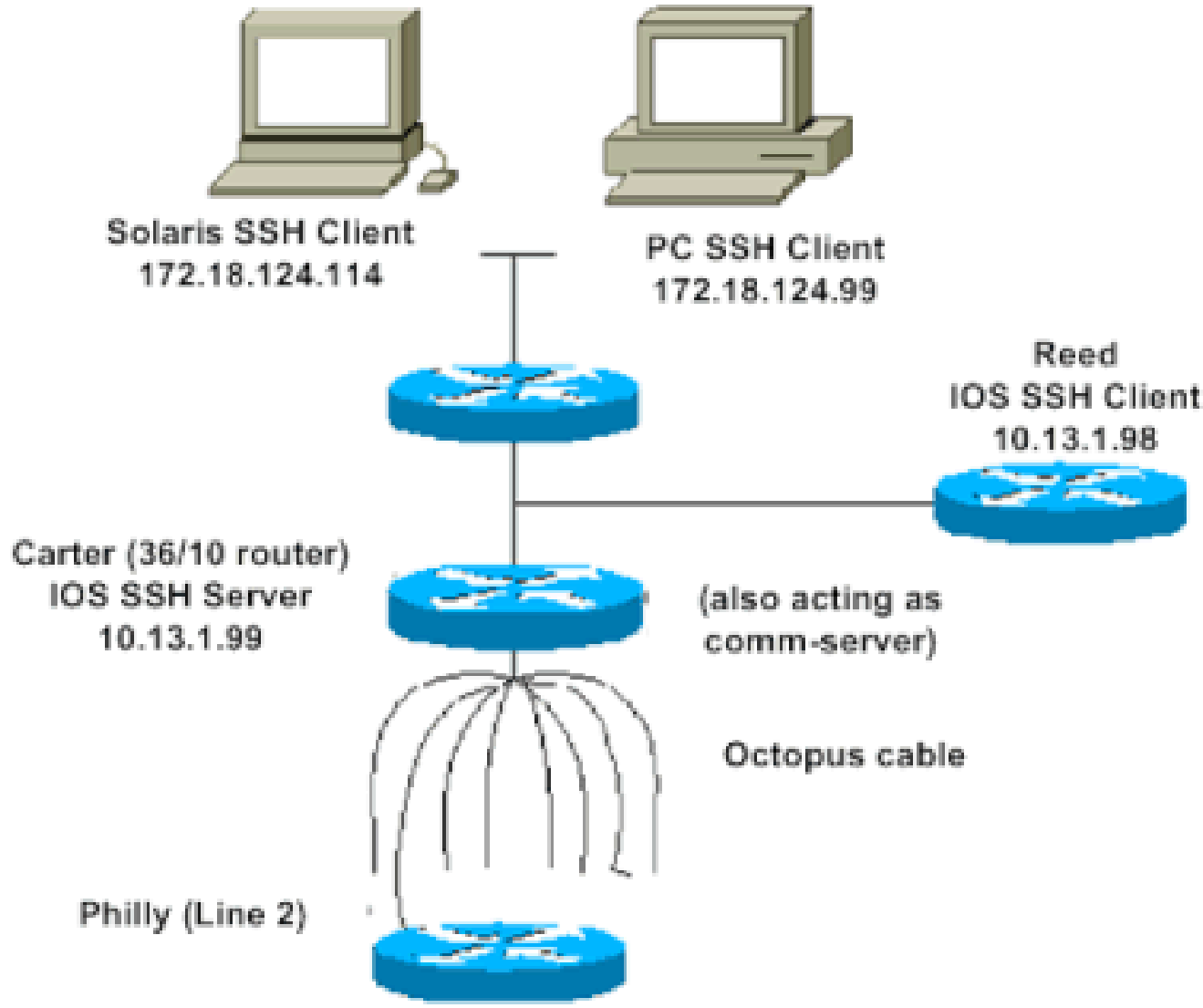
- 從 Cisco IOS 軟體 12.2.2.T 版開始，Cisco IOS 平台和映像已導入 SSH 終端線路存取（又稱為反向 Telnet）。
- 從 Cisco IOS 軟體 12.1(19) E 版開始，Cisco IOS 平台和映像已導入 SSH 2.0 (SSH v2) 支援。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需更多資訊，請參閱思科技術提示慣例。

SSH v2 網路圖表



測試驗證

不使用 SSH 執行驗證測試

首先，在不使用 SSH 的情況下測試驗證，確保驗證適用於路由器 Carter，再新增 SSH。驗證可以使用本機使用者名稱和密碼，也可以使用執行 TACACS+ 或 RADIUS 的驗證、授權及帳戶處理 (AAA) 伺服器。（SSH 無法透過線路密碼進行驗證。）此範例為本機驗證，您可輸入使用者名稱 cisco 和密碼 cisco，透過 Telnet 連入路由器。

附註：本文中，「vty」是指「虛擬終端類型」。

```
!--- 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.
```

使用 SSH 執行驗證測試

如要使用 SSH 測試驗證，您必須新增至先前的陳述式，才能在 Carter 上啟用 SSH，然後從電腦和 UNIX 工作站測試 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
```

此時，show crypto key mypubkey rsa 命令必須顯示所產生的金鑰。新增 SSH 設定後，測試您是否能從電腦和 UNIX 工作站存取路由器。

選用的組態集

防止非 SSH 連線

如要防止非 SSH 的連線，可在該行下方新增 transport input ssh 命令，限制路由器只能使用 SSH 連線。直接（非 SSH）Telnet 會遭到拒絕。

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

測試非 SSH 使用者是否無法透過 Telnet 連線至路由器 Carter。

將 IOS 路由器或交換器設為 SSH 用戶端

在 Cisco IOS 路由器上啟用 SSH 支援需要四個步驟：

1. 設定 hostname 命令。

2. 設定 DNS 網域。

3. 產生 SSH 金鑰。

4. 針對 vty 啟用 SSH 傳輸支援。

若要讓裝置擔任其他裝置的 SSH 用戶端，您可以將 SSH 新增至命名為 Reed 的第二個裝置。這樣

做會讓裝置建立用戶端與伺服器的關係，其中 Carter 擔任伺服器，Reed 則是用戶端。Reed 上的 Cisco IOS SSH 用戶端組態與 Carter 上的 SSH 伺服器組態所需的相同。

```
!--- 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.
```

將此命令從 Cisco IOS SSH 用戶端 (Reed) 發出至 Cisco IOS SSH 伺服器 (Carter) 的 SSH，以進行以下測試：

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

將 IOS 路由器設定為執行基於 RSA 之使用者驗證的 SSH 伺服器

完成以下步驟即可設定 SSH 伺服器以執行基於 RSA 的驗證。

1. 指定主機名稱。

```
Router(config)#hostname
```

2. 定義預設網域名稱。

```
Router(config)#ip domain-name
```

3. 產生 RSA 金鑰配對。

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

4. 為使用者和伺服器驗證設定 SSH-RSA 金鑰。

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

5. 設定 SSH 使用者名稱。

```
Router(conf-ssh-pubkey)#username
```

6. 指定遠端對等點的 RSA 公開金鑰。

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

7. 指定 SSH 金鑰類型和版本。（此為選用步驟）

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

8. 退出目前模式並返回特權 EXEC 模式。

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

新增 SSH 終端線路存取

如果您需要傳出 SSH 終端線路驗證，可透過 Carter 設定及測試傳出反向 Telnet 的 SSH（Carter 作為 Philly 的 comm 伺服器）。

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

如果 Philly 已連接到 Carter 連接埠 2，您便可透過以下命令，從 Reed 透過 Carter 將 SSH 設定至 Philly ：

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

您可以透過 Solaris 使用這項命令：

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

限制對子網路的 SSH 存取

您需要將 SSH 連線限制為特定子網路；在該子網路中，應捨棄來自子網外 IP 的所有其他 SSH 嘗試。

您可以按照下列步驟進行相同工作：

1. 定義允許來自該特定子網路之流量的存取清單。
2. 使用 access-class 限制對 VTY 線路介面的存取。

以下是組態範例。此範例僅允許透過 SSH 存取 10.10.10.0 255.255.255.0 子網路，其他任何存取作業都會遭拒。

```
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
```

附註：鎖定 SSH 存取的相同程序也用於交換器平台。

設定 SSH 第 2 版

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

banner 命令輸出內容的變化版本

Telnet 和不同版本 SSH 連線之間的 banner 命令輸出內容有所不同。下表列出不同 banner 命令選項與各種連線類型的運作情形。

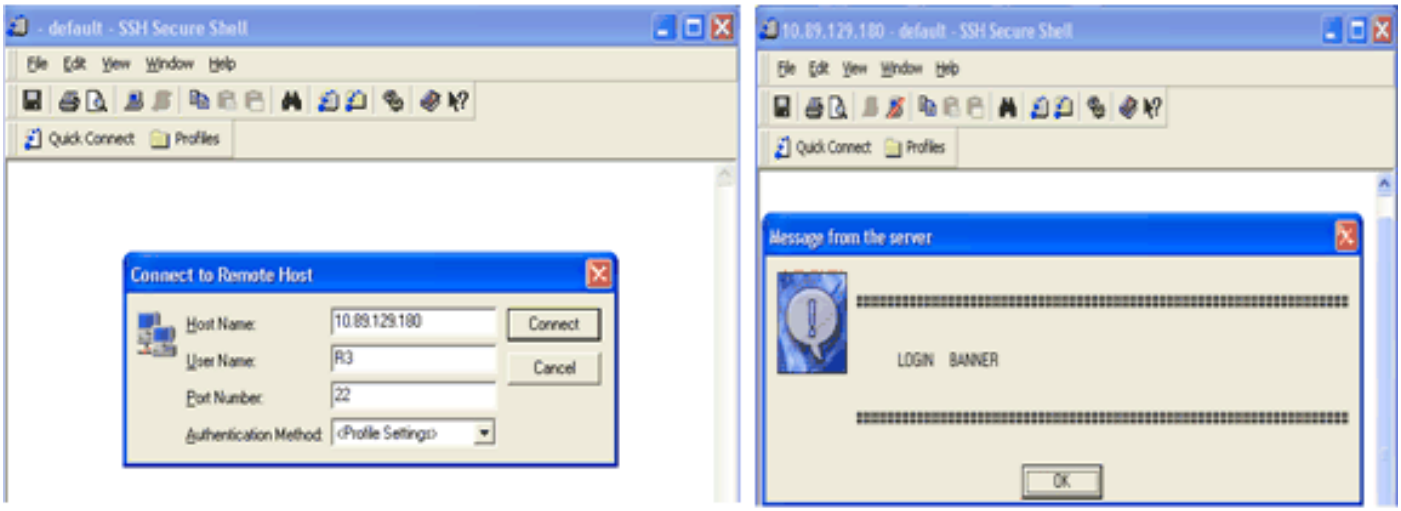
橫幅命令選項	Telnet	SSH v2
banner log	在登入裝置前顯示。	在登入裝置前顯示。
banner motd	在登入裝置前顯示。	在登入裝置後顯示。
banner exec	在登入裝置後顯示。	在登入裝置後顯示。

附註：不建議您繼續 SSH 1。

無法顯示登入橫幅

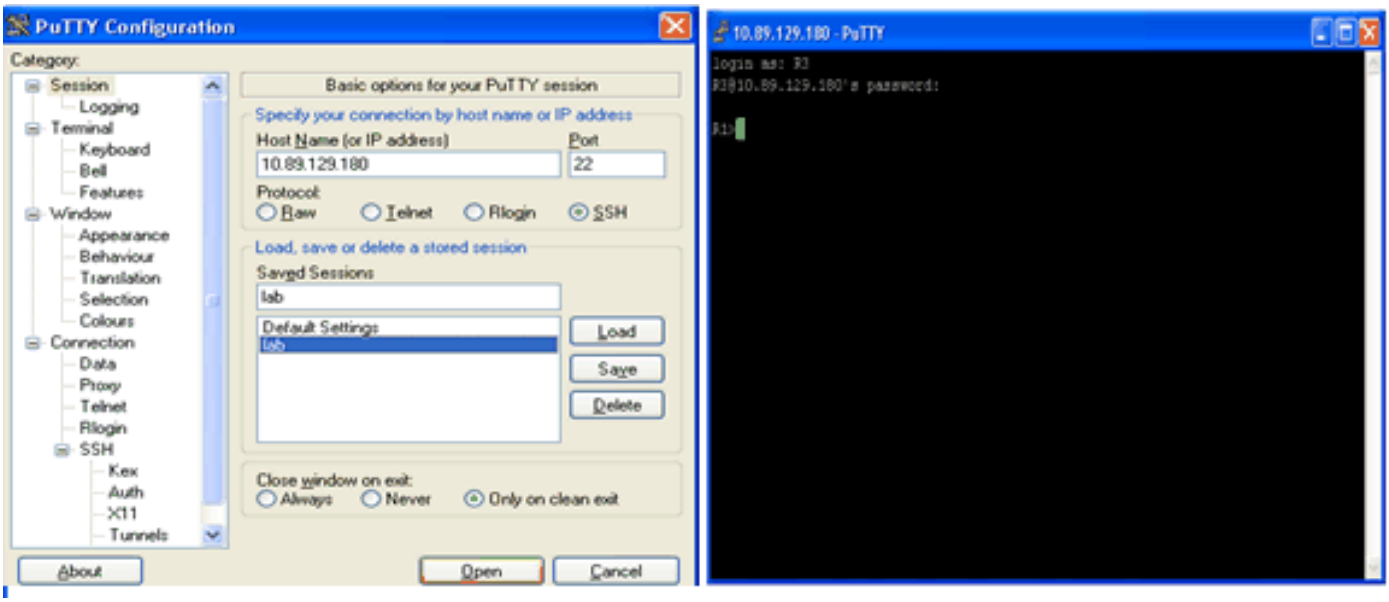
SSH 2 支援登入橫幅。使用思科路由器啟動 SSH 工作階段時，如果 SSH 用戶端傳送使用者名稱，系統會顯示登入橫幅。例如，如果使用安全殼層 (SSH) 用戶端，系統會顯示登入橫幅；如果使用 PuTTY (SSH) 用戶端，系統不會顯示登入橫幅。這是因為 SSH 預設會傳送使用者名稱，而 PuTTY 預設不會傳送使用者名稱。

SSH 用戶端需要使用者名稱，才能初始化與已啟用 SSH 裝置的連線。如果您未輸入主機名稱和使用者名稱，「連線」按鈕不會啟用。此畫面圖片顯示，SSH 連線到路由器時，畫面會顯示登入橫幅。橫幅會提示要求輸入密碼。



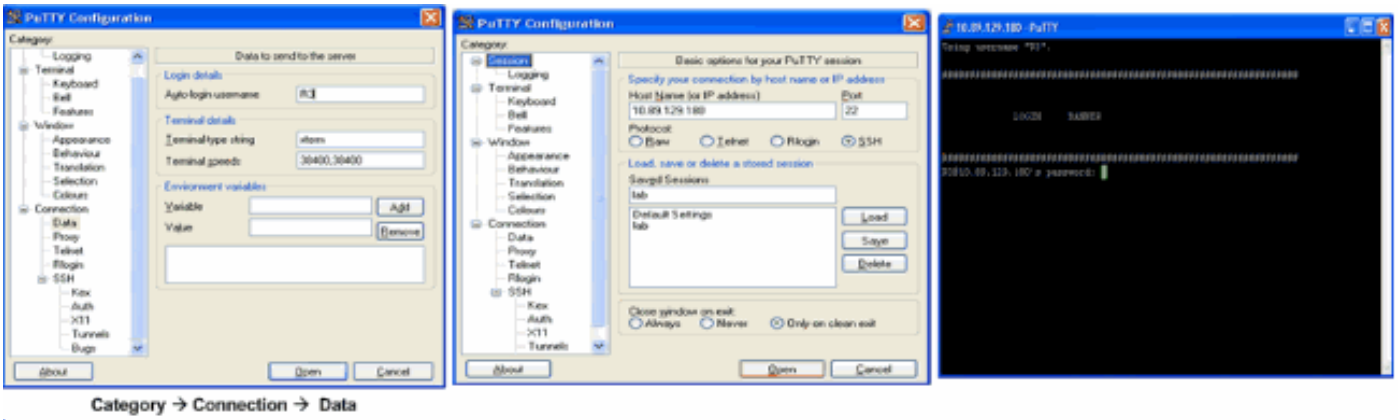
橫幅提示要求輸入密碼

PuTTY 用戶端不需使用者名稱，就能啟動連至路由器的 SSH 連線。此畫面圖片顯示 PuTTY 用戶端連線至路由器，並提示輸入使用者名稱和密碼，畫面並未顯示登入橫幅。



SSH 連線至路由器

此螢幕截圖顯示，將 PuTTY 設定為將使用者名稱傳送到路由器時，畫面會顯示登入橫幅。



Category → Connection → Data

偵錯和顯示命令

發出此處所說的 debug 命令前，請先參閱有關偵錯命令的重要資訊。輸出直譯器工具支援某些 show 命令（僅限註冊客戶），它允許您查看 show 命令輸出的分析。

- debug ip ssh 顯示 SSH 的偵錯訊息。
- show ssh 顯示 SSH 伺服器連線的狀態。

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

- show ip ssh 顯示 SSH 的版本和組態資料。

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

範例偵錯輸出

路由器偵錯

```
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
```

伺服器偵錯

附註：這是 Solaris 電腦的輸出內容。

```
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.
```

組態不正確

以下提供幾個設定錯誤所產生的偵錯輸出內容範例。

SSH 來自未使用資料加密標準 (DES) 編譯的 SSH 用戶端

密碼錯誤

路由器偵錯

```
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
```

SSH 用戶端傳送不支援的 (Blowfish) 密碼

路由器偵錯

```
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
```

收到「%SSH-3-PRIVATEKEY：無法擷取 RSA 私密金鑰」錯誤

變更網域或主機名稱可能會觸發此錯誤訊息。請使用以下因應措施處理：

- **將 RSA 金鑰歸零並重新產生金鑰。**

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

- **如果先前的解決方法無效，請嘗試以下步驟：**
    1. **將所有 RSA 金鑰歸零。**
    2. **重新載入裝置。**
    3. **為 SSH 建立新的標籤金鑰。**

秘訣

- 如果系統將您的 SSH 設定命令視為非法命令而予以拒絕，表示您尚未成功產生路由器的 RSA 金鑰配對。確認您已指定主機名稱和網域。然後使用 crypto key generate rsa 命令產生 RSA 金鑰配對，並啟用 SSH 伺服器。
- 設定 RSA 金鑰配對時，可能會收到這些錯誤訊息：

  1. 未指定主機名稱。

     您必須使用 hostname 全域組態命令來設定路由器的主機名稱。

  2. 未指定網域。

     您必須使用 ip domain-name 全域組態命令來設定路由器的主機網域。

- 允許的SSH連線數限製為路由器配置vty 的最大數量。每個SSH連線都使用一個vty資源。
- SSH 在進行使用者驗證時，會使用本機安全性或透過路由器 AAA 設定的安全性通訊協定。當您設定 AAA 時，必須確認主控台並未在 AAA 下執行。請在全域組態模式中套用關鍵字以停用主控台的 AAA。
- No SSH server connections running:

```
carter#show ssh

%No SSHv2 server connections running.
```

此輸出內容表示 SSH 伺服器已停用或未正確啟用。如果您已設定 SSH，建議您在裝置上重新設定 SSH。完成這些步驟以重新設定裝置上的 SSH 伺服器。

1. 刪除 RSA 金鑰配對。刪除 RSA 金鑰配對後，SSH 伺服器會自動停用。

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

附註：啟用 SSH v2 時，請務必產生至少 768 位元的金鑰配對。

注意：這項命令在儲存設定後無法復原。另外，刪除 RSA 金鑰後，除非您重新產生 RSA 金鑰以重新設定 CA 互通性、取得 CA 憑證，並重新索取您自己的憑證，否則無法使用憑證或 CA，也無法參與與其他 IP 安全 (IPSec) 對等點的憑證交換。

---

2. 重新設定裝置的主機名稱和網域名稱。

```
carter(config)#hostname hostname

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

3. 為您的路由器產生 RSA 金鑰配對。這樣做會自動啟用 SSH。

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

附註：如要瞭解更多有關使用這項命令的資訊，請參閱 crypto key generate rsa - Cisco IOS 安全命令參考（12.3 版）。

附註：由於路由器無法理解收到的封包，您可能會收到 `SSH2 0: Unexpected mesg type received` 錯誤訊息。如要解決這項問題，請在為 SSH 產生 RSA 金鑰時增加金鑰長度。

---

4. 設定 SSH 伺服器。

5. 若要為 SSH 伺服器啟用及設定思科路由器/交換器，您必須設定 SSH 參數。如未設定 SSH 參數，則會使用預設值。

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

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

相關資訊

- SSH 產品支援頁面

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。