如何在Cisco Secure PIX防火牆（5.2至6.2）上執行身份驗證和啟用

目錄

簡介

本文檔介紹如何對運行PIX軟體版本5.2至6.2的PIX防火牆建立AAA身份驗證訪問，並且還提供了有關enable authentication、syslogging和AAA伺服器關閉時獲取訪問的資訊。在PIX 5.3及更高版本中，與先前版本的代碼相比，身份驗證、授權和記帳(AAA)的變化是RADIUS埠是可配置的。

在PIX軟體版本5.2及更高版本中，您可以通過五種不同方式建立對PIX的AAA身份驗證訪問：

- Telnet驗證 — 內部
- 控制檯埠身份驗證
- 通過身份驗證的Cisco安全VPN客戶端1.1 — 外部
- 已驗證VPN 3000 2.5 — 外部
- 驗證安全殼層(SSH) — 內部或外部

注意：對於最後三種方法，必須在PIX上啟用DES或3DES(發出**show version**命令進行驗證)。在PIX軟體版本6.0及更高版本中，還可以載入PIX裝置管理器(PDM)以啟用GUI管理。PDM不屬於本文檔的範圍。

有關PIX 6.2的身份驗證和授權命令的詳細資訊，請參閱PIX 6.2 :驗證和授權命令配置示例。

要建立對運行PIX軟體6.3版及更高版本的PIX防火牆的AAA身份驗證（直通代理）訪問，請參閱PIX/ASA:使用TACACS+和RADIUS伺服器進行網路存取的直通代理組態範例。

必要條件

需求

在新增AAA身份驗證之前執行以下任務：

- 發出以下命令，以便為PIX新增密碼：**passwd wwtelnet <local_ip> [<mask>] [<if_name>]**PIX自動加密此密碼，以形成加密字串，其中關鍵字**encrypted**如下：
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  您無需新增**encrypted**關鍵字。
- 在新增這些語句後，確保您可以Telnet從內部網路到PIX的內部介面，*而不*需要AAA身份驗證。
- 當您新增身份驗證語句時，如果必須退出命令，請始終開啟與PIX的連線。

在AAA驗證上（SSH除外，其順序取決於使用者端），使用者會看到要求PIX密碼(如*passwd <whatever>*)，然後是要求RADIUS或TACACS使用者名稱和密碼。

注意：您無法Telnet至PIX的外部介面。如果從外部SSH客戶端連線，則可以在外部介面上使用SSH。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX軟體版本5.2、5.3、6.0、6.1或6.2
- Cisco安全VPN使用者端1.1
- Cisco VPN 3000使用者端2.5
- Cisco VPN Client 3.0.x（需要PIX 6.0代碼）

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

可配置的RADIUS埠（5.3及更高版本）

某些RADIUS伺服器使用RADIUS連線埠而不是1645/1646（通常為1812/1813）。 在PIX 5.3中，可以使用以下命令將RADIUS身份驗證和記帳埠更改為除預設1645/1646之外的其他埠：

aaa-server radius-authport #

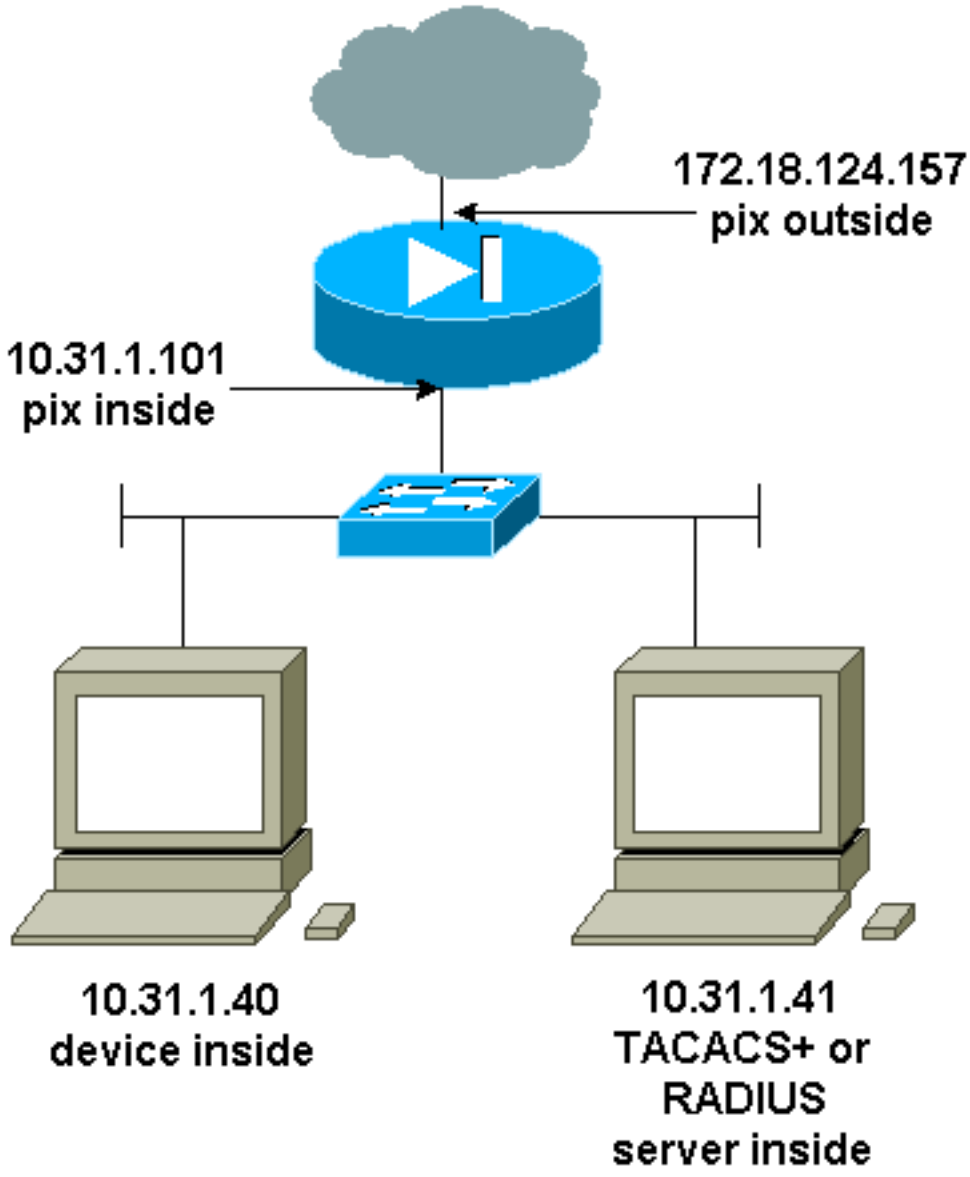
aaa-server radius-acctport #

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

Telnet驗證 — 內部

網路圖表



新增到PIX配置的命令

將以下命令新增到您的配置：

aaa伺服器topix通訊協定tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication telnet console topix

使用者看到一個請求PIX密碼(如`passwd <whatever>`)，然後是一個請求RADIUS或TACACS使用者名稱和密碼（儲存在10.31.1.41 TACACS或RADIUS伺服器上）。

控制檯埠身份驗證

將以下命令新增到您的配置：

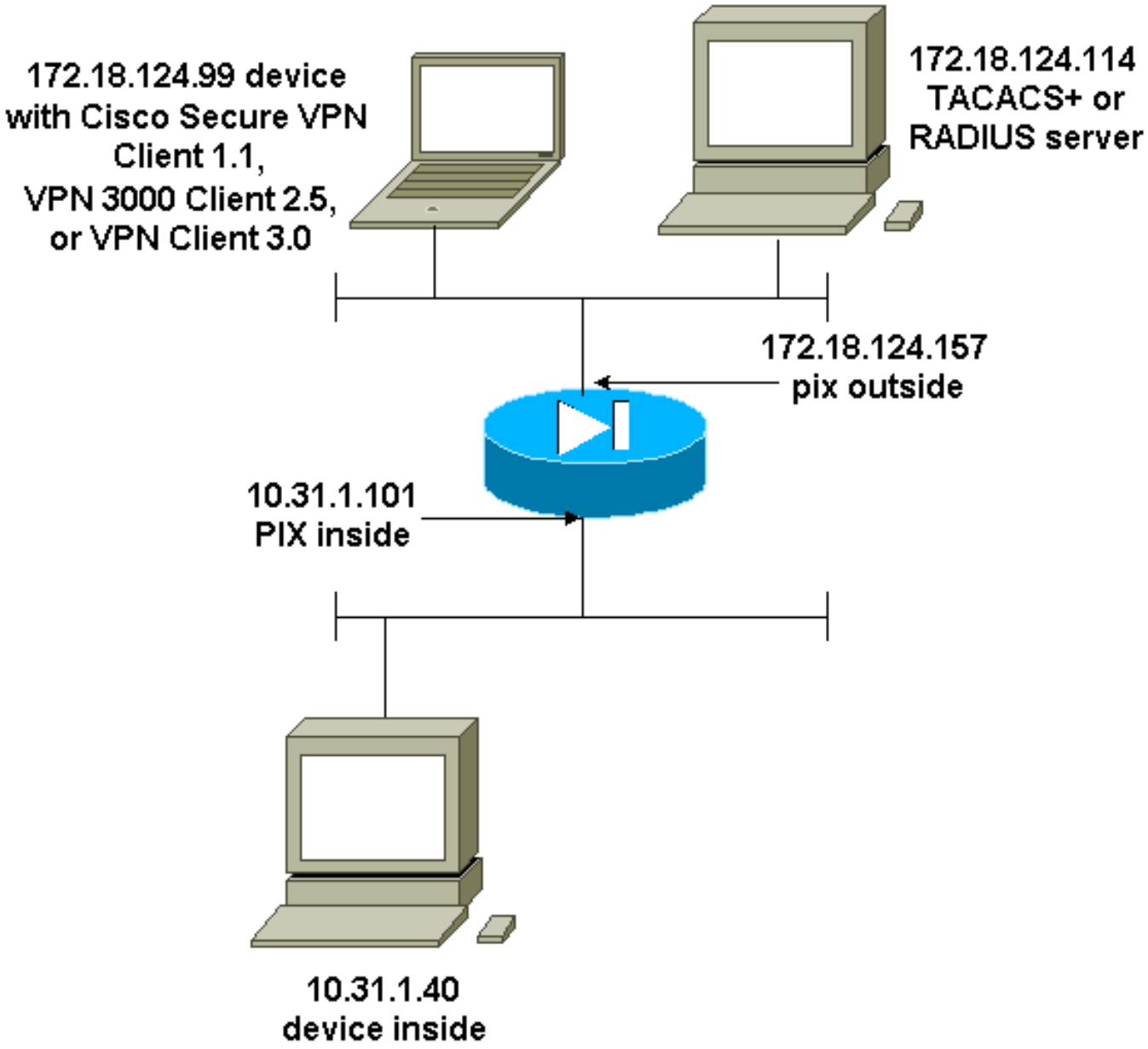
aaa伺服器topix通訊協定tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication serial console topix

使用者看到一個請求PIX密碼(如`passwd <whatever>`)，然後是一個請求RADIUS/TACACS使用者名稱/密碼（儲存在RADIUS或TACACS 10.31.1.41伺服器上）。

圖 — VPN Client 1.1、VPN 3000 2.5或VPN Client 3.0 — 外部



通過身份驗證的Cisco安全VPN客戶端1.1 — 外部

通過身份驗證的Cisco安全VPN客戶端1.1 — 外部 — 客戶端配置

```
1- Myconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP address
          Port all Protocol all
          Pre-shared key (matches that on PIX)

     Connect using secure tunnel
          ID Type: IP address
          172.18.124.157

     Authentication (Phase 1)
     Proposal 1

         Authentication method: Preshared key
         Encryp Alg: DES
         Hash Alg: MD5
         SA life:  Unspecified
         Key Group: DH 1

     Key exchange (Phase 2)
     Proposal 1
         Encapsulation ESP
         Encrypt Alg: DES
         Hash Alg: MD5
         Encap: tunnel
         SA life: Unspecified
         no AH

 2- Other Connections
        Connection security: Non-secure
        Local Network Interface
          Name: Any
          IP Addr: Any
          Port: All
```

經過身份驗證的Cisco安全VPN客戶端1.1 — 外部 — 部分PIX配置

```
ip address outside 172.18.124.157 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
!--- If you know the IP address of the outside client,
use that !--- IP address in this statement. isakmp key
******** address 0.0.0.0 netmask 0.0.0.0 ! isakmp
identity address isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
hash md5 isakmp policy 10 group 1 isakmp policy 10
lifetime 86400 !--- We knew our client would access the
PIX from this !--- network. If you know the IP address
```

```
of the client, use that IP address !--- in this
statement. telnet 172.18.124.0 255.255.255.0 outside
```

已驗證VPN 3000 2.5或VPN使用者端3.0 — 外部

已驗證VPN 3000 2.5或VPN客戶端3.0 — 外部 — 客戶端配置

1. 從VPN 3000中選擇**VPN Dialer > Properties > Name**。
2. 選擇**Authentication > Group Access Information**。組名稱和密碼應與vpngroup <*group_name*> password *****語句中PIX上的內容匹配。

當您按一下**Connect**時，加密隧道將啟動，PIX從測試池分配IP地址（VPN 3000客戶端僅支援模式配置）。 然後，您可以開啟終端視窗，Telnet至172.18.124.157，並進行AAA身份驗證。PIX上的**telnet 192.168.1.x**命令允許從池中的使用者連線到外部介面。

已驗證VPN 3000 2.5 — 外部 — 部分PIX配置

```
ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.31.1.101 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
!!--- ISAKMP Policy for VPN 3000 Client runs 2.5 code.
isakmp policy 10 authentication pre-share isakmp policy
10 encryption des isakmp policy 10 hash md5 !--- The 2.5
client uses group 1 policy (PIX default). isakmp policy
10 group 1 isakmp policy 10 lifetime 86400 !--- ISAKMP
Policy for VPN Client runs 3.0 code. isakmp policy 20
authentication pre-share isakmp policy 20 encryption des
isakmp policy 20 hash md5 !--- The 3.0 clients use D-H
group 2 policy and require PIX 6.0 code. isakmp policy
20 group 2 isakmp policy 20 lifetime 86400 ! vpngroup
vpn3000 address-pool test vpngroup vpn3000 idle-time
1800 vpngroup vpn3000 password ******** telnet
192.168.1.0 255.255.255.0 outside
```

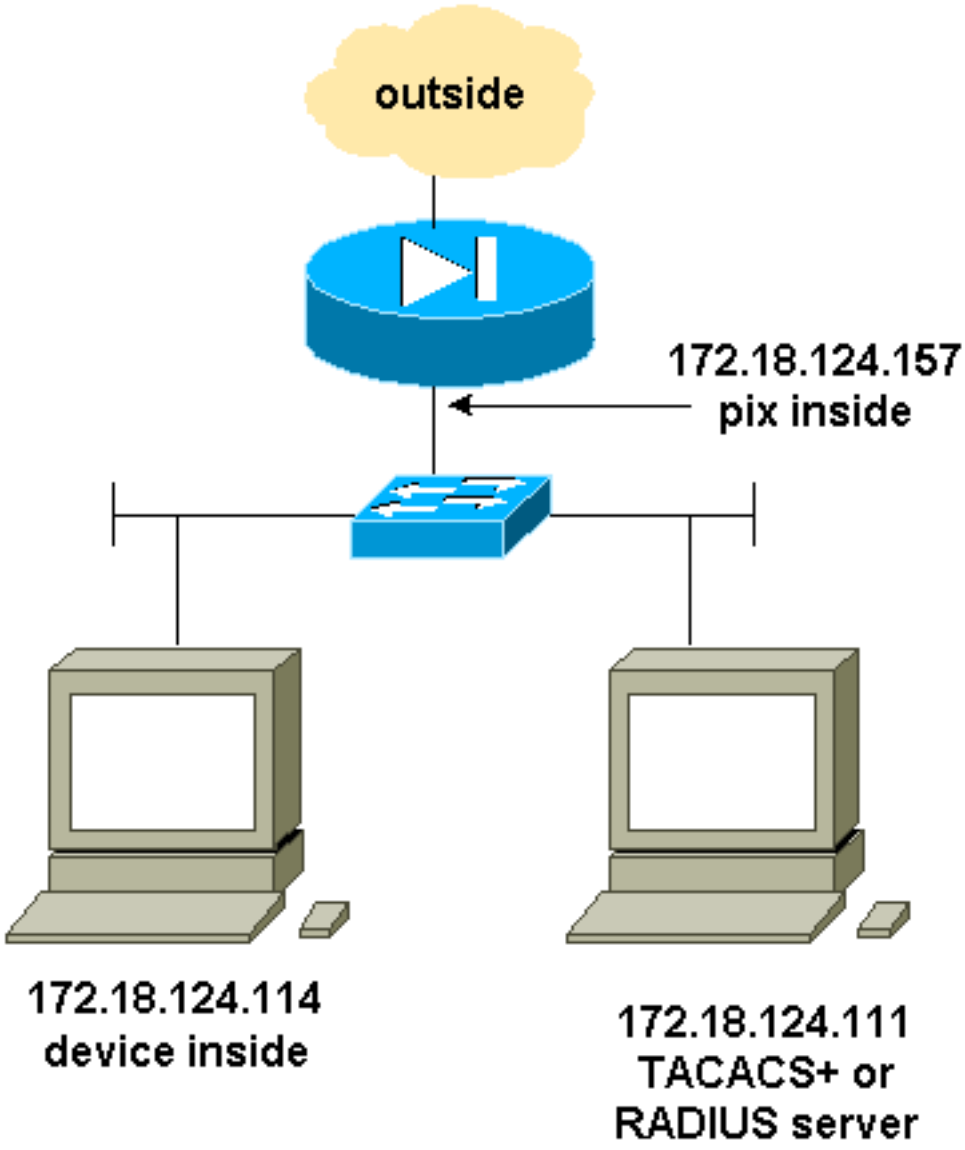
SSH — 內部或外部

PIX 5.2增加了安全殼層(SSH)版本1支援。SSH 1基於1995年11月的IETF草案。SSH第1版和第2版彼此不相容。有關SSH的詳細資訊，請參閱安全外殼(SSH)常見問題。

PIX被認為是SSH伺服器。從SSH客戶端（即運行SSH的框）到SSH伺服器(PIX)的流量將加密。PIX 5.2版本說明中列出了某些SSH版本1客戶端。我們實驗室中的測試是使用NT上的F-secure SSH 1.1和Solaris的1.2.26版完成的。

注意：對於PIX 7.x，請參閱管理系統訪問的允許SSH訪問部分。

網路圖表



配置AAA身份驗證SSH

完成以下步驟以配置AAA身份驗證SSH:

1. 確保可以在啟用AAA但不使用SSH的情況下Telnet至PIX:
   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```
   注意：配置SSH時，不需要使用**telnet 172.18.124.114 255.255.255.255**命令，因為PIX上發出**ssh 172.18.124.114 255.255.255.255**inside命令。這兩個命令都包含於測試中。
2. 使用以下命令新增SSH:
   ```
   hostname goss-d3-pix515b
   domain-name rtp.cisco.com
   ca gen rsa key 1024!--- Caution: The RSA key is not be saved without !--- the ca save all
   command. !--- The write mem command does not save it. !--- In addition, if the PIX has
   undergone a write erase !--- or has been replaced, then cutting and pasting !--- the old
   configuration does not generate the key. !--- You must re-enter the ca gen rsa key command.
   !--- If there is a secondary PIX in a failover pair, the write standby !--- command does
   not copy the key from the primary to the secondary. !--- You must also generate and save
   the key on the secondary device.
   ```

```
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
aaa authen ssh console AuthOutbound
logging trap debug
logging console debug
```

3. 在配置模式下發出**show ca mypubkey rsa**命令。

```
goss-d3-pix(config)#show ca mypubkey rsa
 % Key pair was generated at: 08:22:25 Aug 14 2000
 Key name: goss-d3-pix.rtp.cisco.com
  Usage: General Purpose Key
  Key Data:
   30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ad4bcb
   e9c174d5 0657a0f3 c94e4b6d 32ac8500 6b84e754 59e20df4 f28c257d 131af21d
   4c0a8f4c e79d8b6d a3520faa 1a42d577 c6adfe51 9d96fa62 f3be07fb 01e082d7
   133cecff bf24f653 bc690b11 ee222070 413c1920 d02321f8 4fc3c5f1 f0c6e077
   81e93184 af55438b dcdcda34 c0a5f5ad 87c435ef
      67170674 4d5ba51e 6d020301 0001
 % Key pair was generated at: 08:27:18 Aug 14 2000
 Key name: goss-d3-pix.rtp.cisco.com.server
  Usage: Encryption Key
  Key Data:
   307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00d4f61b ec45843a
   4ad9266d b125ee26 efc63cc4 e5e9cda4 9418ee53 6e4d16cf 3d0dc864 4d4830c8
   fa7f110e 8a5761ed 4ca73ea7 5d405862 6f3150df 9eb0d11e 9c4d3563 95ff51ae
   6711d60b 9a1415e4 19201d3f 03b455ea c1df9a41 b3a5a73f 4f020301 0001
```

4. 從Solaris工作站嘗試Telnet:

```
rtp-evergreen#./ssh -c 3des -l cisco -v 172.18.124.157
```

注意：「cisco」是RADIUS/TACACS+伺服器上的使用者名稱，而172.18.124.157是目標。

配置本地SSH（無AAA身份驗證）

也可以使用本地身份驗證設定與PIX的SSH連線，而不使用AAA伺服器。但是，沒有離散的每使用者使用者名稱。使用者名稱始終為「pix」。

使用以下命令在PIX上配置本地SSH:

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024!--- Caution: The RSA key is not saved without !--- the ca save all command.
!--- The write mem command does not save it. !--- In addition, if the PIX has undergone a write
erase !--- or has been replaced, then cutting and pasting !--- the old configuration does not
generate the key. !--- You must re-enter the ca gen rsa key command. !--- If there is a
secondary PIX in a failover pair, a write standby !--- command does not copy the key from the
primary to the secondary. !--- You must also generate and save the key on the secondary device.
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
passwd cisco123
```

由於此配置中的預設使用者名稱始終是「pix」，因此連線到PIX的命令（這是Solaris框中的3DES）為：

```
./ssh -c 3des -1 pix -v <ip_of_pix>
```

SSH調試

不使用debug ssh命令進行調試 — 3DES和512-cipher

```
109005: Authentication succeeded for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
109011: Authen Session Start: user 'cse', sid 0
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
315011: SSH session from 172.18.124.114 on interface inside
   for user "cse" terminated normally
```

使用debug ssh命令進行調試 — 3DES和512-cipher

```
goss-d3-pix#debug ssh
SSH debugging on
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - msg type 0x03, length 112
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

調試 — 3DES和1024密碼

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

Debug - DES和1024-cipher

注意：此輸出來自使用SSH的PC，而不是Solaris。

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.99' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-W1.0
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests DES cipher: 2
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid ssh
SSH(ssh): user authen method is 'use AAA', aaa server group ID = 4
SSH(ssh): starting user authentication request,
   and waiting for reply from AAA server
SSH(ssh): user 'ssh' is authenticated
SSH(ssh): user authentication request completed
SSH0: authentication successful for ssh109
SSH0: invalid request - 0x2500
SSH0: starting exec shell5: Authentication succeeded for user 'ssh'
   from 0.0.0.0/0 to 172.18.124.99/0 on interface SSH
109011: Authen Session Start: user 'ssh', sid 1
315002: Permitted SSH session from 172.18.124.99 on interface outside
   for user "ssh"
```

調試 — 3DES和2048密碼

注意：此輸出來自使用SSH的PC，而不是Solaris。

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3.
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse10900
SSH1: invalid request - 0x255:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
109011: Authen Session Start: user 'cse', Sid 2
315002: Permitted SSH session from 161.44.17.151 on interface inside
   for user "cse"
```

可能出錯的地方

Solaris debug - 2048-cipher和Solaris SSH

注意：Solaris無法處理2048加密口令。

```
rtp-evergreen.cisco.com: Initializing random;
seed file /export/home/cse/.ssh/random_seed
RSA key has too many bits for RSAREF to handle (max 1024).
```

RADIUS/TACACS+伺服器上的密碼或使用者名稱錯誤

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA serverss-d3-pix#
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH1: password authentication failed for cse
109006: Authentication failed for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

不允許使用者通過命令：

ssh 172.18.124.114 255.255.255.255內部

嘗試連線：

315001:拒絕來自內部介面上161.44.17.151的SSH會話

從PIX中刪除金鑰時(使用**ca zero rsa命令**)，或者不使用**ca save all命令保**存

```
Device opened successfully.
SSH: unable to retrieve host public key for 'goss-d3-pix.rtp.cisco.com',
   terminate SSH connection.
SSH-2145462416: Session disconnected by SSH server - error 0x00 "Internal error"
315004: Fail to establish SSH session because PIX RSA host key retrieval failed.
315011: SSH session from 0.0.0.0 on interface outside for user ""
   disconnected by SSH server, reason: "Internal error" (0x00)
```

AAA伺服器已關閉：

```
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH0: SSH_SMSG_PUBLIC_KEY message sent302010: 0 in use, 0 most used
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests 3DES cipher: 3
```

```
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server1090
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH0: password authentication failed for cse0
SSH0: authentication failed for cse
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
2: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109006: Authentication failed for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
315003: SSH login session failed from 172.18.124.114 (1 attempts)
   on interface outside by user "cse"
315011: SSH session from 172.18.124.114 on interface outside for user "cse"
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
109012: Authen Session End: user 'cse', Sid 0, elapsed 352 seconds
```

客戶端已為3DES設定，但PIX中只有DES金鑰：

註：客戶端是Solaris不支援DES。

```
GOSS-PIX# Device opened successfully.
SSH: host key initialised
SSH: license supports DES: 1.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
315011: SSH session from 172.18.124.114 on interface outside for user ""
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
```

在Solaris CLI上：

```
Selected cipher type 3DES not supported by server.
```

如何從PIX中刪除RSA金鑰

ca zero rsa

如何將RSA金鑰儲存到PIX

ca save all

如何允許來自外部SSH客戶端的SSH

ssh outside_ip *255.255.255.255* outside

啟用身份驗證

使用以下命令：

aaa authentication enable console topix

其中*topix*是我們的伺服器清單)，系統會提示使用者輸入傳送到TACACS或RADIUS伺服器的使用者名稱和密碼。由於用於啟用的身份驗證資料包與用於登入的身份驗證資料包相同，因此，如果使用者可以使用TACACS或RADIUS登入到PIX，則可以使用相同的使用者名稱/密碼通過TACACS或RADIUS啟用這些身份驗證資料包。

有關這些問題的詳細資訊請參閱Cisco錯誤ID CSCdm4704(僅限註冊客戶)。

Syslogg資訊

雖然AAA記賬僅對通過PIX的連線有效，而不對PIX有效，但是，如果設定了syslogging，則有關經過身份驗證的使用者所執行操作的資訊將傳送到syslog伺服器（如果進行了配置，則通過syslog MIB傳送到網路管理伺服器）。

如果設定了syslogging，則系統日誌伺服器上將顯示以下消息：

日誌記錄陷阱通知級別：

```
111006: Console Login from pixuser at console
111007: Begin configuration: 10.31.1.40 reading from terminal
111008: User 'pixuser' executed the 'conf' command.
111008: User 'pixuser' executed the 'hostname' command.
```

日誌記錄陷阱資訊級別（包括通知級別）：

307002:允許的10.31.1.40的Telnet登入會話

在AAA伺服器關閉時取得存取許可權

如果AAA伺服器關閉，您可以先輸入Telnet密碼訪問PIX，然後輸入使用者名稱的**pix**，最後輸入密碼的啟用密碼(**enable password** 無論)。如果**enable password** 不包含PIX配置中的任何值，請輸入**pix**作為使用者名稱，然後按**Enter**。如果使能口令已設定但未知，則需要口令恢復盤來重置口令。

建立TAC案例時要收集的資訊

如果在完成上述故障排除步驟後仍然需要幫助，並且希望通過Cisco TAC建立案例，請確保包含以下資訊。
• 問題描述和相關拓撲詳細資訊 • 開啟案例之前執行的故障排除 • **show tech-support**命令的輸出 • 使用**logging buffered debugging**命令運行後**show log**命令的輸出，或顯示問題的控制檯捕獲（如果可用） 請將收集到的資料以非壓縮純文字檔案格式(.txt)附加到您

的案例。 您可以使用案件查詢工具（僅限註冊客戶）將資訊上傳到您的案件（僅限註冊客戶）。 如果您無法訪問案件查詢工具，可以將電子郵件附件中的資訊傳送到attach@cisco.com，並將案例編號填寫在郵件主題行。

相關資訊

- Cisco Secure PIX防火牆命令參考
- PIX RADIUS TACACS+