# PIX 6.2 :驗證與授權命令組態範例

## 目錄



## 簡介

6.2版引入了PIX命令授權和本地身份驗證的擴展。本文檔提供了如何在PIX上設定此功能的示例。以前提供的身份驗證功能仍然可用，但本文檔中未討論(例如，安全外殼(SSH)、從PC進行的IPsec客戶端連線等)。 執行的命令可以在PIX本地控制，也可以通過TACACS+遠端控制。不支援RADIUS命令授權；這是RADIUS通訊協定的限制。

本地命令授權通過將命令和使用者分配到許可權級別來完成。

遠端命令授權是透過TACACS+驗證、授權及計量(AAA)伺服器完成。在無法訪問一個AAA伺服器的情況下，可以定義多個AAA伺服器。

身份驗證也適用於以前配置的IPSec和SSH連線。SSH身份驗證要求您發出以下命令：

```
aaa authentication ssh console <LOCAL | server_tag>
```

**注意：**如果使用TACACS+或RADIUS伺服器組進行身份驗證，則可以配置PIX，在AAA伺服器不可用時將本地資料庫用作**回**方法。

例如

```
pix(config)#aaa authentication ssh console TACACS+ LOCAL
```

如果您單獨輸入LOCAL，也可以使用本地資料庫作為主要身份驗證方法（無回退）。

例如，發出以下命令以在本地資料庫中定義使用者帳戶並為SSH連線執行本地身份驗證：

```
pix(config)#aaa authentication ssh console LOCAL
```

請參閱如何在Cisco安全PIX防火牆（5.2至6.2）上執行身份驗證和啟用，以瞭解有關如何對運行PIX軟體5.2至6.2版的PIX防火牆建立AAA身份驗證訪問的更多資訊，以及有關AAA伺服器關閉時啟用身份驗證、系統日誌記錄和獲取訪問許可權的詳細資訊。

請參閱PIX/ASA:使用TACACS+和RADIUS伺服器進行網路訪問的直通代理配置示例以瞭解有關如何對運行PIX軟體6.3版及更高版本的PIX防火牆建立AAA身份驗證（直通代理）訪問的更多資訊。

如果配置正確完成，則不應將您鎖定在PIX之外。如果未儲存配置，重新引導PIX應使其返回到預配置狀態。如果由於配置錯誤而無法訪問PIX，請參閱PIX的密碼恢復和AAA配置恢復過程。

# 開始之前

## 慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

## 必要條件

本文件沒有特定先決條件。

## 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6.2
- 適用於Windows的Cisco Secure ACS版本3.0(ACS)
- 適用於UNIX的Cisco安全ACS(CSUnix)版本2.3.6

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。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

# 新增身份驗證/授權之前進行測試

在實施新的6.2身份驗證/授權功能之前，確保您當前能夠使用這些命令訪問PIX:

```
!--- IP range allowed to Telnet to the PIX (values depend on network). telnet 172.18.124.0
255.255.255.0
```

```
!--- Telnet password. passwd <password>
!--- Enable password. enable password <password>
```

## 瞭解許可權設定

PIX中的大多數命令位於15級，但少數命令位於0級。要檢視所有命令的當前設定，請使用以下命令：

```
show privilege all
```

預設情況下，大多數命令處於第15級，如下例所示：

```
privilege configure level 15 command route
```

一些命令位於0級，如以下示例所示：

```
privilege show level 0 command curpriv
```

PIX可以在啟用和配置模式下運行。某些命令(例如show logging)在兩個模式下均可用。要設定這些命令的許可權，必須指定命令所在的模式，如示例所示。另一種模式選項是enable。您會收到logging is a command available in multiple modes消息。如果未配置模式，請使用mode [enable|configure]命令：

```
privilege show level 5 mode configure command logging
```

這些示例針對clock命令。使用以下命令確定clock命令的當前設定：

```
show privilege command clock
```

show privilege command clock命令的輸出顯示clock命令以以下三種格式存在：

```
!--- Users at level 15 can use the show clock command.

privilege show level 15 command clock
!--- Users at level 15 can use the clear clock command.

Privilege clear level 15 command clock
!--- Users at level 15 can configure the clock !--- (for example, clock set 12:00:00 Jan 01
2001).

privilege configure level 15 command clock
```

## 身份驗證/授權 — 本地使用者名稱

在更改**clock**命令的許可權級別之前，您應該前往控制檯埠配置管理使用者並啟用LOCAL登入身份驗證，如以下示例所示：

```
GOSS(config)# username poweruser password poweruser privilege 15
GOSS(config)# aaa-server LOCAL protocol local
GOSS(config)# aaa authentication telnet console LOCAL
```

PIX確認新增使用者，如以下示例所示：

```
GOSS(config)# 502101: New user added to local dbase:
      Uname: poweruser Priv: 15 Encpass: Nimjl8wRa7VAmpm5
```

使用者「poweruser」應該能夠通過Telnet訪問PIX並使用現有的本地PIX啟用密碼(**enable password *<password>***命令中的密碼)**啟用**。

您可以通過新增用於啟用的身份驗證來新增更多安全性，如以下示例所示：

```
GOSS(config)# aaa authentication enable console LOCAL
```

這要求使用者輸入密碼以進行登入和啟用。在本例中，密碼「poweruser」用於登入和啟用。使用者「poweruser」應該能夠通過Telnet訪問PIX，並且使用本地PIX密碼啟用。

如果您希望某些使用者只能使用某些命令，則必須設定許可權較低的使用者，如以下示例所示：

```
GOSS(config)# username ordinary password ordinary privilege 9
```

由於實際上預設情況下您的所有命令都處於第15級，因此您必須將某些命令向下移動到第9級，以便「普通」使用者能夠發出這些命令。在這種情況下，您希望9級使用者能夠使用**show clock**命令，但不能重新配置時鐘，如以下示例所示：

```
GOSS(config)# privilege show level 9 command clock
```

您還需要您的使用者能夠註銷PIX（使用者希望這樣做時可能處於級別1或9），如以下示例所示：

```
GOSS(config)# privilege configure level 1 command logout
```

您需要使用者能夠使用**enable**命令（使用者嘗試此命令時處於第1級），如以下範例所示：

```
GOSS(config)# privilege configure level 1 mode enable command enable
```

將**disable**命令移動到級別1後，級別2-15之間的任何使用者都可以退出啟用模式，如下例所示：

```
GOSS(config)# privilege configure level 1 command disable
```

如果您以「normal」使用者身份遠端登入並以同一使用者身份啟用（密碼也是「normal」），則應使用**privilege configure level 1命令disable**，如以下示例所示：

```
GOSS# show curpriv
Username : ordinary
Current privilege level : 9
Current Mode/s : P_PRIV
```

如果您仍開啟原始會話（新增任何身份驗證之前的會話），PIX可能不知道您是誰，因為您最初沒有使用使用者名稱登入。如果是這種情況，請使用**debug**命令檢視有關使用者「enable_15」或「enable_1」的消息（如果沒有關聯的使用者名稱）。因此，在配置命令授權之前，請以「poweruser」使用者（「15級」使用者）身份通過Telnet登入到PIX，因為您需要確保PIX可以將使用者名稱與嘗試的命令相關聯。您已準備好使用以下命令測試命令授權：

```
GOSS(config)# aaa authorization command LOCAL
```

使用者「poweruser」應能通過Telnet登入、啟用和執行所有命令。使用者「normal」應該能夠使用**show clock**、**enable**、**disable**和**logout**指令，但是不能使用其他指令，如以下範例所示：

```
GOSS# show xlate
Command authorization failed
```

## 使用AAA伺服器的驗證/授權

您也可以使用AAA伺服器對使用者進行驗證和授權。TACACS+的運作效果最佳，因為可能會使用指令授權，但也可使用RADIUS。檢查PIX上是否有以前的AAA Telnet/控制檯命令(在以前使用**LOCAL AAA**命令的情況下)，如以下示例所示：

```
GOSS(config)# show aaa
AAA authentication telnet console LOCAL
AAA authentication enable console LOCAL
AAA authorization command LOCAL
```

如果有以前的AAA Telnet/控制檯命令，請使用以下命令將其刪除：

```
GOSS(config)# no aaa authorization command LOCAL
GOSS(config)# no aaa authentication telnet console LOCAL
GOSS(config)# no aaa authentication enable console LOCAL
```

與配置本地身份驗證一樣，測試以確保使用者可以使用這些命令Telnet至PIX。

```
telnet 172.18.124.0 255.255.255.0
!--- IP range allowed to telnet to the PIX (values would depend on network). passwd <password>
!--- Telnet password. Enable password <password>
!--- Enable password.
```

根據您使用的伺服器，配置PIX以使用AAA伺服器進行身份驗證/授權。

## ACS - TACACS+

配置ACS以與PIX通訊，方法是使用「Authenticate Using」 TACACS+在網路配置中定義PIX(適用於Cisco IOS®軟體)。 ACS使用者的配置取決於PIX的配置。至少應為ACS使用者設定使用者名稱和密碼。

在PIX上，使用以下命令：

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host   timeout 10
GOSS(config)# aaa authentication telnet console TACSERVER
```

此時，ACS使用者應該能夠通過Telnet訪問PIX，使用PIX上的現有啟用密碼啟用它，並執行所有命令。請完成以下步驟：

1. 如果需要對ACS執行PIX啟用身份驗證，請選擇**Interface Configuration > Advanced TACACS+ Settings**。
2. 選中**Advanced Configuration Options中的Advanced TACACS+功能**框。
3. 按一下「**Submit**」。「高級TACACS+設定」現在顯示在使用者配置下。
4. 將任何AAA客戶端的Max Privilege設定為Level 15。
5. 為使用者選擇啟用密碼方案（這可能涉及配置單獨的啟用密碼）。
6. 按一下「**Submit**」。

要在PIX中啟用通過TACACS+的身份驗證，請使用以下命令：

```
GOSS(config)# aaa authentication enable console TACSERVER
```

此時，ACS使用者應該能夠通過Telnet連線到PIX並使用在ACS中配置的使能密碼啟用。

在新增PIX命令授權之前，必須修補ACS 3.0。您可以從Software Center（僅限註冊客戶）下載修補程式。 您還可以通過訪問思科錯誤ID CSCdw78255(僅限註冊客戶)來檢視有關此修補程式的更多資訊。

進行命令授權之前，驗證必須工作正常。如果需要使用ACS執行命令授權，請為使用者和/或組選擇**Interface Configuration > TACACS+(Cisco)> Shell(exec)，然後單擊Submit**。外殼命令授權設定現在在使用者（或組）配置下可見。

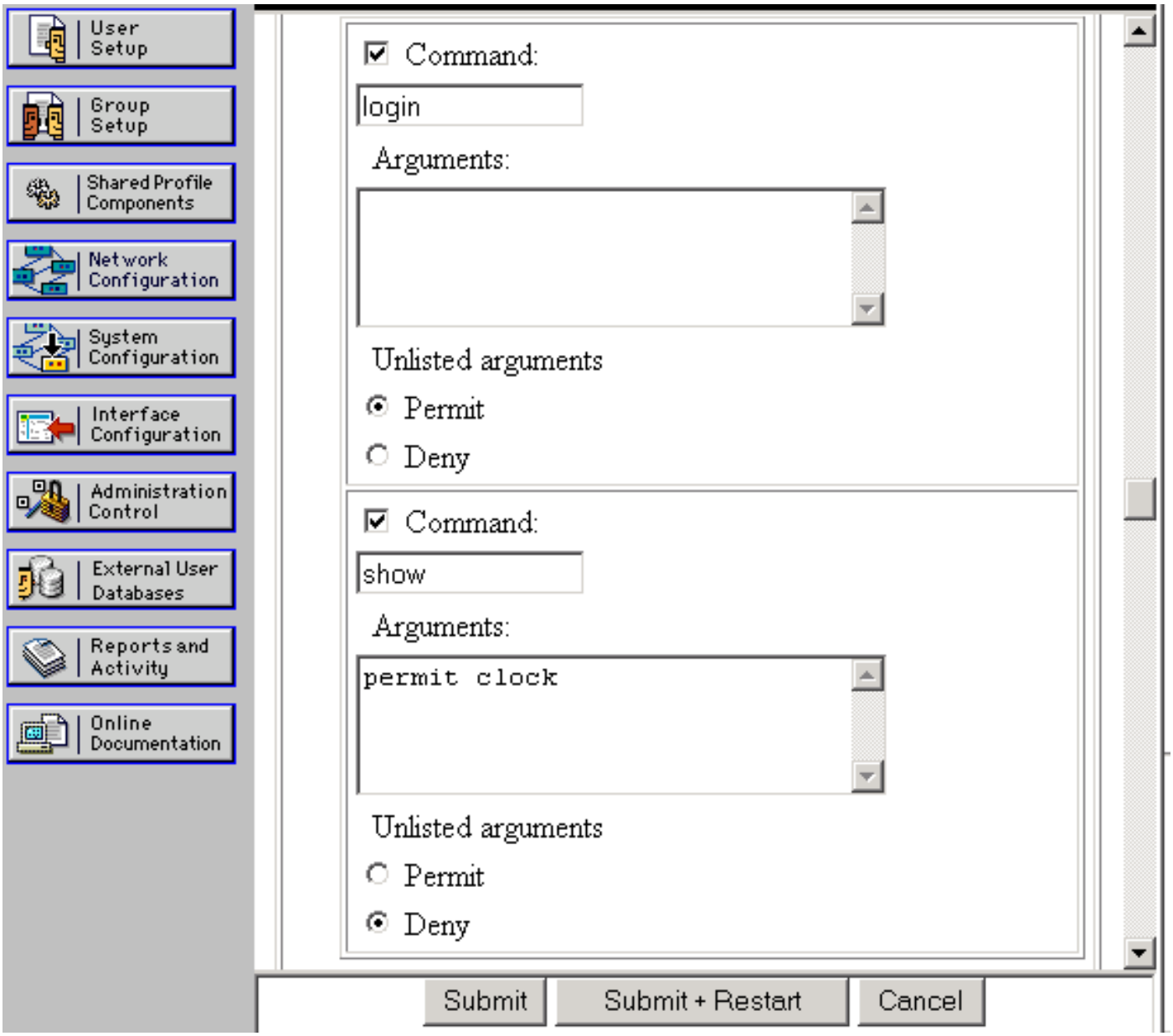
最好至少設定一個強大的ACS使用者用於命令授權和允許不匹配的Cisco IOS命令。

通過允許命令子集，可以通過命令授權設定其他ACS使用者。此範例使用以下步驟：

1. 選擇Group Settings以從下拉框查詢所需的組。
2. 按一下「**Edit Settings**」。
3. 選擇**Shell Command Authorization Set**。
4. 按一下**Command**按鈕。
5. 輸入**login**。

6. 在Unlisted Arguments下選擇Permit。
7. 對**logout**、**enable**和**disable**命令重複此過程。
8. 選擇Shell Command Authorization Set。
9. 按一下**Command**按鈕。
10. **Entershow**。
11. 在引數下，輸入**permit clock**。
12. 為未列出的引數選擇deny。
13. 按一下「**Submit**」。

以下是這些步驟的範例：




如果您仍然開啟了原始會話（新增任何身份驗證之前的會話），PIX可能不知道您是誰，因為您最初沒有使用ACS使用者名稱登入。如果是這種情況，請使用**debug**命令檢視有關使用者「enable_15」或「enable_1」的消息（如果沒有關聯使用者名稱）。您需要確保PIX可以將使用者名稱與正在嘗試的命令相關聯。您可以在配置命令授權之前，以15級ACS使用者的身份通過Telnet連線到PIX。您已準備好使用以下命令測試命令授權：

```
aaa authorization command TACSERVER
```

此時，您應該有一個能夠Telnet、啟用和使用所有命令的使用者，和一個只能執行五個命令的使用者。

## CSUnix - TACACS+

配置CSUnix以像與任何其他網路裝置一樣與PIX通訊。CSUnix使用者的配置取決於PIX的配置。CSUnix使用者至少應設定使用者名稱和密碼。在此示例中，設定了三個使用者：

```
!--- This is our "poweruser" who can enable, use all commands, and log in. !--- The login
password is in the 'clear "********"' statement. !--- The enable password is in the 'clear
"********" 15' statement. user = pixtest{ password = clear "********" privilege = clear
"********" 15 service=shell { default cmd=permit default attribute=permit } } !--- This user can
Telnet in, enable, and use four commands !--- (such as show clock, logout, exit, and enable). !-
-- The login password is in the 'clear "********"' statement. !--- The enable password is in the
'clear "********" 15' statement.

user = limitpix{
password = clear "********"
privilege = clear "********" 15
service=shell {
cmd=show {
permit "clock"
}
cmd=logout {
permit ".*"
}
cmd=enable {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}

 !--- This user can Telnet in, but not enable. This user can use any !--- show commands in non-
enable mode as well as logout, exit, and ?.

user = oneuser{
password = clear "********"
service=shell {
cmd=show {
permit ".*"
}
cmd=logout {
permit ".*"
}
cmd="?" {
permit ".*"
}
cmd=exit {
permit ".*"
}
}
}
```

在PIX上，使用以下命令：

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server TACSERVER protocol tacacs+
GOSS(config)# aaa-server TACSERVER (inside) host
```

```
GOSS(config)# aaa authentication telnet console TACSERVER
```

此時，任何CSUnix使用者都應能夠通過Telnet登入到PIX，使用PIX上的現有啟用密碼啟用，並使用所有命令。

通過PIX中的TACACS+啟用身份驗證：

```
GOSS(config)# aaa authentication enable console TACSERVER
```

此時，具有「特權15」密碼的CSUnix使用者應該能夠通過Telnet登入到PIX並使用這些「啟用」密碼啟用。

如果您仍然開啟了原始會話（新增任何身份驗證之前的會話），PIX可能不知道您是誰，因為您最初沒有使用使用者名稱登入。如果是這種情況，如果沒有關聯使用者名稱，發出**debug**命令可能會顯示有關使用者「enable_15」或「enable_1」的消息。在配置命令授權之前，以「pixtest」使用者（我們的「15級」使用者）的身份遠端登入到PIX，因為我們需要確保PIX可以將使用者名稱與嘗試的命令相關聯。在執行命令授權之前，必須啟用身份驗證。如果需要使用CSUnix執行命令授權，請新增以下命令：

```
GOSS(config)# aaa authorization command TACSERVER
```

在這三個使用者中，「pixtest」可以執行所有操作，而另外兩個使用者可以執行命令的子集。

## ACS - RADIUS

不支援RADIUS命令授權。可以使用ACS進行Telnet和啟用身份驗證。ACS可通過使用「Authenticate Using」 RADIUS（任何種類）在網路配置中定義PIX來配置，以便與PIX通訊。ACS使用者的配置取決於PIX的配置。至少應為ACS使用者設定使用者名稱和密碼。

在PIX上，使用以下命令：

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius GOSS(config)
            # aaa-server RADSERVER (inside)
              host
```

```
GOSS(config)# aaa authentication telnet console RADSERVER
```

此時，ACS使用者應該能夠通過Telnet連線到PIX，使用PIX上的現有啟用密碼啟用，並使用所有命令(PIX不向RADIUS伺服器傳送命令；不支援RADIUS命令授權)。

如果要在PIX上使用ACS和RADIUS啟用，請新增以下命令：

```
aaa authentication enable console RADSERVER
```

與TACACS+不同的是，RADIUS啟用和RADIUS登入使用的密碼相同。

## CSUnix - RADIUS

配置CSUnix以像與任何其他網路裝置一樣與PIX通訊。CSUnix使用者的配置取決於PIX的配置。此配置檔案適用於身份驗證和啟用：

```
user = pixradius{
profile_id = 26
profile_cycle = 1
!--- The login password is in the 'clear "*********"' statement; !--- this is used for the login,
enable, and non-enable commands.

password = clear "*********" < pixradius
}
```

在PIX上，使用以下命令：

```
GOSS(config)# enable password cisco123
GOSS(config)# aaa-server RADSERVER protocol radius
GOSS(config)# aaa-server RADSERVER (inside) host
```

如果要在PIX上使用ACS和RADIUS啟用，請使用以下命令：

```
GOSS(config)# aaa authentication enable console RADSERVER
```

與TACACS+不同的是，RADIUS啟用和RADIUS登入使用的密碼相同。

# 網路訪問限制

網路訪問限制可在ACS和CSUnix中使用，以限製出於管理目的可以連線到PIX的人員。

- **ACS** — 將在組設定的「網路訪問限制」區域中配置PIX。PIX配置為「拒絕的呼叫/接入點位置」或「允許的呼叫/接入點位置」（取決於安全計畫）。
- **CSUnix** — 這是允許訪問PIX（但不允許訪問其他裝置）的使用者的示例：

```
user = naruser{
profile_id = 119
```

```
profile_cycle = 1
password = clear "*********"
privilege = clear "*********" 15
service=shell {
allow "10.98.21.50" ".*" ".*"
refuse ".*" ".*" ".*"
default cmd=permit
default attribute=permit
}
}
```

## 調試

要啟用debug，請使用以下命令：

```
logging on
logging
```

以下是調試的好壞示例：

- **Good debug** — 使用者能夠使用**登入、enable和執行**命令。
  ```
  307002: Permitted Telnet login session from 172.18.124.111
  111006: Console Login from pixpartial at console
  502103: User priv level changed: Uname: pixpartial From: 1 To: 15
  111009: User 'pixpartial' executed cmd: show clock
  ```
- **錯誤偵錯** — 使用者的授權失敗，如以下示例所示：
  ```
  610101: Authorization failed: Cmd: uauth Cmdtype: show
  ```
- **遠端AAA伺服器無法連線：**
  ```
  AAA server host machine not responding
  ```

## 會計

沒有可用的實際命令記帳，但是通過在PIX上啟用系統日誌，您可以看到執行了哪些操作，如以下示例所示：

```
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
611103: User logged out: Uname: pixtest
307002: Permitted Telnet login session from 172.18.124.111
111006: Console Login from pixtest at console
502103: User priv level changed: Uname: pixtest From: 1 To: 15
111008: User 'pixtest' executed the 'enable' command.
111007: Begin configuration: 172.18.124.111 reading from terminal
111008: User 'pixtest' executed the 'configure t' command.
111008: User 'pixtest' executed the 'write t' command.
```

## 建立TAC案例時要收集的資訊

| **如果在執行上述故障排除步驟後仍需要幫助，並且希望通過Cisco TAC建立案例，請確保包含以下資訊，用於排除PIX防火牆故障。** |
| --- |
| • 問題描述和相關拓撲詳細資訊<br>• 開啟案例之前執行的故障排除<br>• **show tech-support**命令的輸出<br>• 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）<br>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

- PIX命令參考
- Cisco PIX防火牆軟體 — 技術支援與檔案
- 思科安全存取控制伺服器（Windows專用） — 技術支援與檔案
- Unix版Cisco安全存取控制伺服器 — 技術支援與檔案