PIX、TACACS+和RADIUS配置示例：4.2.x

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[網路圖表](#)
[慣例](#)
[驗證與授權](#)
[使用者透過開啟驗證/授權看到的專案](#)
[用於所有方案的伺服器配置](#)
[Cisco Secure UNIX TACACS+伺服器配置](#)
[Cisco Secure UNIX RADIUS伺服器配置](#)
[Cisco安全NT 2.x RADIUS](#)
[EasyACS TACACS+](#)
[Cisco安全NT 2.x TACACS+](#)
[Livingston RADIUS伺服器配置](#)
[價值RADIUS伺服器配置](#)
[TACACS+免費軟體伺服器配置](#)
[調試步驟](#)
[來自PIX的身份驗證調試示例](#)
[新增授權](#)
[來自PIX的身份驗證和授權調試示例](#)
[新增記帳](#)
[TACACS+](#)
[RADIUS](#)
[最大會話數和檢視登入使用者數](#)
[使用Except命令](#)
[對PIX本身的身份驗證](#)
[更改使用者看到的提示](#)
[相關資訊](#)

簡介

可以對FTP、Telnet和HTTP連線執行RADIUS和TACACS+身份驗證。支援TACACS+授權；RADIUS授權不是。

在PIX軟體4.2.2中，身份驗證的語法略有更改。本文檔使用軟體版本4.2.2的語法。

必要條件

需求

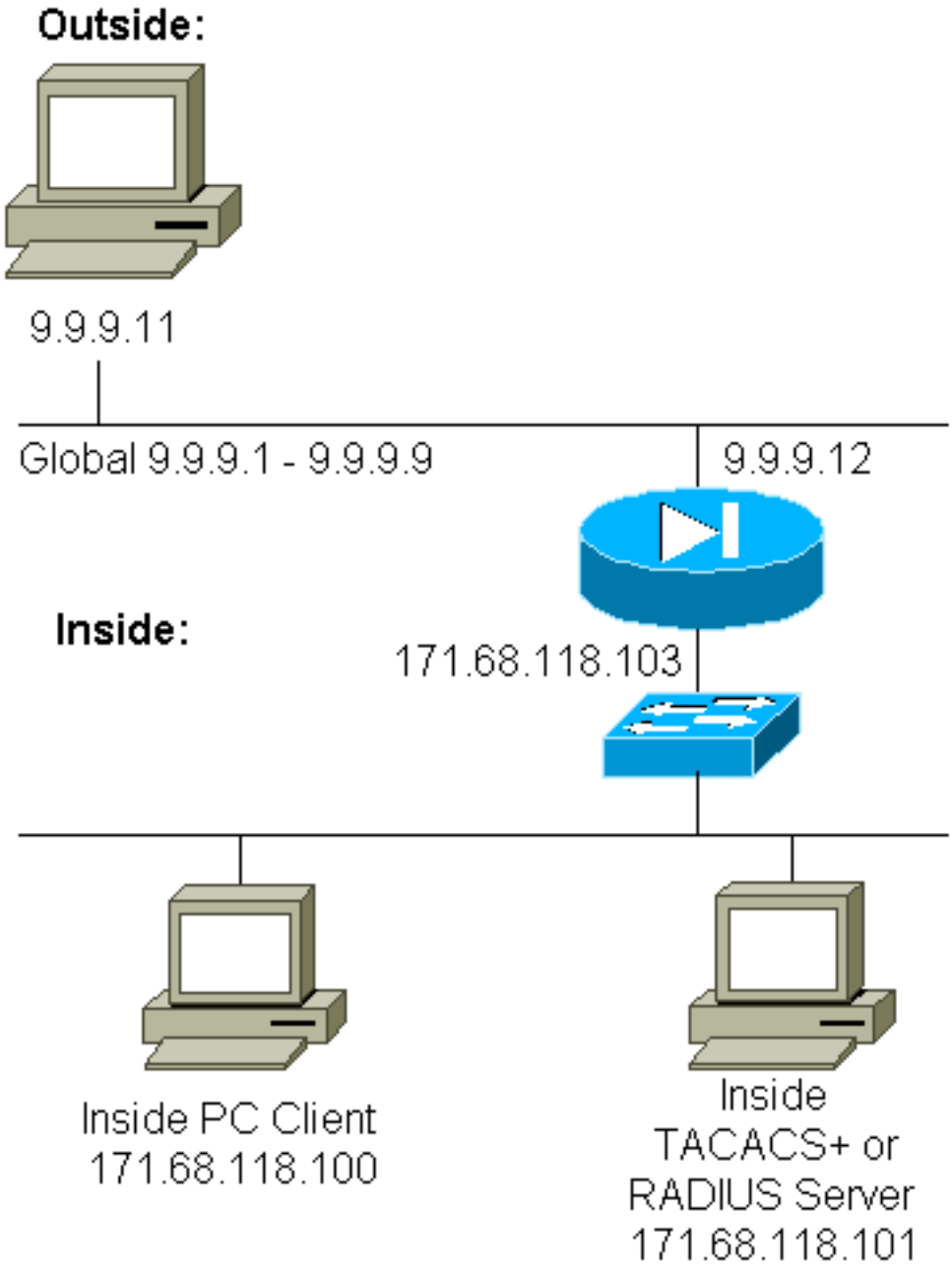
本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

網路圖表

本檔案會使用以下網路設定：



PIX配置

```
pix2# write terminal
Building configuration
: Saved
:
PIX Version 4.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pix2
fixup protocol http 80
fixup protocol smtp 25
no fixup protocol ftp 21
no fixup protocol h323 1720
no fixup protocol rsh 514
no fixup protocol sqlnet 1521
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address  0.0.0.0
names
pager lines 24
logging console debugging
no logging monitor
logging buffered debugging
logging trap debugging
logging facility 20
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
ip address outside 9.9.9.12 255.255.255.0
ip address inside 171.68.118.103 255.255.255.0
ip address  0.0.0.0 0.0.0.0
arp timeout 14400
global (outside) 1 9.9.9.1-9.9.9.9 netmask 255.0.0.0
static (inside,outside) 9.9.9.10 171.68.118.100 netmask
255.255.255.255 0 0
conduit permit icmp any any
conduit permit tcp host 9.9.9.10 eq telnet any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
timeout xlate 3:00:00 conn 1:00:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:00:00 absolute
!
!--- The next entry depends on whether TACACS+ or RADIUS
is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5
radius-server (inside) host 171.68.118.101 cisco timeout
10
!
!--- The focus of concern is with hosts on the inside
network !--- accessing a particular outside host. ! aaa
authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11
   255.255.255.255 tacacs+|radius
!
!--- It is possible to be less granular and authenticate
!--- all outbound FTP, HTTP, Telnet traffic with: aaa
authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
```

```
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius ! !--- Accounting records are
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
[OK]
```

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

驗證與授權

- 身份驗證*是*使用者的身份。
- 授權是*用戶*可以做的。
- 未經授權,身份驗證有效。
- 未經*驗證的*授權無效。

例如，假設您內部有100個使用者，並且您只希望其中六個使用者能夠在網路外部執行FTP、Telnet或HTTP。告訴PIX驗證出站流量，並為TACACS+/RADIUS安全伺服器上的所有六個使用者ID提供證書。使用簡單身份驗證時，這六個使用者可以使用使用者名稱和密碼進行身份驗證，然後退出。其他94個使用者無法外出。PIX提示使用者輸入使用者名稱/密碼，然後將其使用者名稱和密碼傳遞到TACACS+/RADIUS安全伺服器。此外，根據響應，它會開啟或拒絕連線。這六個使用者可以執行FTP、Telnet或HTTP。

但是，假設三個使用者之一「Terry」不可信。您想允許Terry執行FTP，但不要使用HTTP或Telnet到外部。這意味著您需要新增授權。也就是說，除了驗證使用者身份之外，還要授權使用者能做什麼。當您向PIX新增授權時，PIX首先將Terry的使用者名稱和密碼傳送到安全伺服器，然後傳送授權請求，告訴安全伺服器Terry嘗試執行哪些「命令」。正確設定伺服器後，可以允許Terry使用「FTP 1.2.3.4」，但拒絕在任何地方使用「HTTP」或「Telnet」。

使用者透過開啟驗證/授權看到的事案

當您嘗試從內部到外部（反之亦然）時，身份驗證/授權開啟：

- **Telnet** — 使用者看到顯示的使用者名稱提示，然後請求密碼。如果在PIX/伺服器上成功進行身份驗證（和授權），則目標主機將提示使用者輸入使用者名稱和密碼。
- **FTP** — 使用者看到使用者名稱提示啟動。使用者需要輸入「local_username@remote_username」作為使用者名稱，輸入「local_password@remote_password」作為密碼。PIX將「local_username」和「local_password」傳送到本地安全伺服器，如果在PIX/伺服器上成功進行身份驗證（和授權），則「remote_username」和「remote_password」將傳遞到目標FTP伺服器。
- **HTTP** -瀏覽器中將顯示一個要求輸入使用者名稱和密碼的視窗。如果身份驗證（和授權）成功，則使用者將超出該時間到達目標網站。請記住，瀏覽器**會快取使用者名稱和密碼**。如果PIX似乎應該對HTTP連線進行超時，但並未這樣做，則瀏覽器實際上很可能在進行重新身份驗證，將快取的使用者名稱和密碼「拍攝」到PIX。然後將其轉發到身份驗證伺服器。PIX系統日誌和/或

伺服器調試顯示了此現象。如果Telnet和FTP似乎工作正常，但HTTP連線不正常，這就是原因。

用於所有方案的伺服器配置

在TACACS+伺服器組態範例中，如果僅開啟驗證，則使用者「all」、「telnetonly」、「httponly」和「ftponly」都正常運作。在RADIUS伺服器組態範例中，使用者「all」正常運作。

向PIX新增授權後，除了向TACACS+身份驗證伺服器傳送使用者名稱和密碼外，PIX還會向TACACS+伺服器傳送命令（Telnet、HTTP或FTP）。然後，TACACS+伺服器會檢查該使用者是否獲得該指令的授權。

在稍後的示例中，171.68.118.100上的使用者發出命令**telnet 9.9.9.11**。在PIX收到此命令時，PIX會將使用者名稱、密碼和命令傳遞給TACACS+伺服器進行處理。

因此，如果除了身份驗證之外還啟用授權，使用者「telnetonly」可以通過PIX執行Telnet操作。但是，使用者「httponly」和「ftponly」無法通過PIX執行Telnet操作。

（同樣地，由於通訊協定規範的性質，RADIUS不支援授權）。

Cisco Secure UNIX TACACS+伺服器配置

Cisco Secure 2.x

- 此處顯示使用者標準。
- 將PIX IP地址或完全限定域名和金鑰新增到CSU.cfg。

```
user = all {
password = clear "all"
default service = permit
}

user = telnetonly {
password = clear "telnetonly"
service = shell {
cmd = telnet {
permit .*
}
}
}

user = ftponly {
password = clear "ftponly"
service = shell {
cmd = ftp {
permit .*
}
}
}

user = httponly {
password = clear "httponly"
service = shell {
cmd = http {
permit .*
}
}
```

```
}
```

Cisco Secure UNIX RADIUS伺服器配置

使用高級圖形使用者介面(GUI)將PIX IP和金鑰新增到網路訪問伺服器(NAS)清單。此時將顯示使用者stanza，如下所示：

```
all Password="all"
User-Service-Type = Shell-User
```

Cisco安全NT 2.x RADIUS

CiscoSecure 2.1線上和Web文檔的「配置示例」部分描述了設定；屬性6（服務型別）為「登入」或「管理」。

使用GUI在「NAS配置」部分新增PIX的IP。

EasyACS TACACS+

EasyACS文檔提供了設定資訊。

1. 在組部分中，按一下**Shell exec**（以授予exec許可權）。
2. 要向PIX新增授權，請按一下組設定底部的**Deny unmatched IOS commands**。
3. 為每個要允許的命令（例如Telnet）選擇**Add/Edit**。
4. 如果要允許Telnet到特定站點，請在引數部分輸入IP。要允許Telnet到所有站點，請按一下**允許所有未列出的引數**。
5. 按一下**finish editing**命令。
6. 對每個允許的命令（例如Telnet、HTTP和/或FTP）執行步驟1至5。
7. 使用GUI在「NAS配置」部分新增PIX的IP。

Cisco安全NT 2.x TACACS+

Cisco Secure 2.x文檔提供了設定資訊。

1. 在組部分中，按一下**Shell exec**（以授予exec許可權）。
2. 要向PIX新增授權，請按一下組設定底部的**Deny unmatched IOS commands**。
3. 選中底部的**command**覈取方塊，然後輸入您要允許的命令（例如Telnet）。
4. 如果要允許Telnet到特定站點，請在引數部分輸入IP（例如，「permit 1.2.3.4」）。 要允許Telnet到所有站點，請按一下**允許未列出的引數**。
5. 按一下「**Submit**」。
6. 對每個允許的命令（例如Telnet、FTP和/或HTTP）執行步驟1至5。
7. 使用GUI在「NAS配置」部分新增PIX的IP。

Livingston RADIUS伺服器配置

將PIX IP和金鑰新增到客戶端檔案。

```
all Password="all"
```

```
User-Service-Type = Shell-User
```

價值RADIUS伺服器配置

將PIX IP和金鑰新增到客戶端檔案。

```
all Password="all"
Service-Type = Shell-User
```

TACACS+免費軟體伺服器配置

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

user = all {
default service = permit
login = cleartext "all"
}

user = telnetonly {
login = cleartext "telnetonly"
cmd = telnet {
permit .*
}
}

user = httponly {
login = cleartext "httponly"
cmd = http {
permit .*
}
}

user = ftponly {
login = cleartext "ftponly"
cmd = ftp {
permit .*
}
}
```

調試步驟

- 在新增身份驗證、授權和記帳(AAA)之前，確保PIX配置工作正常。如果您在建立AAA之前無法傳遞流量，則以後將無法這樣做。
- 在PIX中啟用日誌記錄：在負載較重的系統上不應使用**logging console debugging**命令。可以使用**logging buffered debugging**命令。**show logging**或**logging**命令的輸出隨後可以傳送到系統日誌伺服器並進行檢查。
- 確保TACACS+或RADIUS伺服器的調試已開啟。所有伺服器均具有此選項。

來自PIX的身份驗證調試示例

PIX調試 — 良好身份驗證 — RADIUS

以下是具有良好驗證的PIX調試示例：

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼） — RADIUS

以下是具有錯誤身份驗證（使用者名稱或密碼）的PIX調試示例。 使用者看到四個使用者名稱/密碼集。「錯誤：超出最大重試次數」消息隨即顯示。

注意：如果這是FTP嘗試，則允許嘗試。對於HTTP，允許無限次重試。

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

PIX調試 — 伺服器關閉 — RADIUS

以下是伺服器關閉的PIX偵錯範例。使用者會看到使用者名稱一次。然後伺服器「掛起」並請求密碼（三次）。

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

PIX調試 — 良好身份驗證 — TACACS+

以下是具有良好驗證的PIX調試示例：

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
  laddr 171.68.118.100/1200 (cse)
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼） — TACACS+

以下是具有錯誤身份驗證（使用者名稱或密碼）的PIX調試示例。 使用者看到四個使用者名稱/密碼集。「錯誤：超出最大重試次數」消息隨即顯示。

注意：如果這是FTP嘗試，則允許嘗試。對於HTTP，允許無限次重試。

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

PIX調試 — 伺服器關閉 — TACACS+

以下是伺服器關閉的PIX偵錯範例。使用者會看到使用者名稱一次。立即輸入「Error:顯示「超出最大嘗試次數」消息。

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

新增授權

因為未經身份驗證授權無效，所以同一源和目標需要授權：

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+|radius
```

或者，如果所有三個出站服務最初均經過身份驗證：

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
   0.0.0.0 tacacs+|radius
```

來自PIX的身份驗證和授權調試示例

PIX調試 — 身份驗證和授權正常 — TACACS+

以下是具有良好驗證和授權的PIX調試示例：

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

PIX調試 — 身份驗證良好，但授權失敗 — TACACS+

以下是具有良好身份驗證但授權失敗的PIX調試示例：

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
```

```
   from 171.68.118.100/1223 to 9.9.9.11/23
```

PIX調試 — 身份驗證錯誤，未嘗試授權 — TACACS+

這是一個使用身份驗證和授權的PIX調試示例，但由於身份驗證錯誤（使用者名稱或密碼），未嘗試授權。 使用者看到四個使用者名稱/密碼集。「錯誤：超出最大重試次數。" 顯示消息

注意：如果這是FTP嘗試，則允許嘗試。對於HTTP，允許無限次重試。

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

PIX調試 — 身份驗證/授權，伺服器關閉 — TACACS+

以下是使用驗證和授權的PIX調試示例。伺服器已關閉。使用者只能看到使用者名稱。立即輸入「Error:超出最大嘗試次數。" 顯示。

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

新增記帳

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+
```

無論記帳是開啟還是關閉，調試看起來都相同。但是，在「構建」時，會傳送「開始」記帳記錄。此外，在「拆除」時，會傳送「停止」會計記錄：

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

TACACS+記帳記錄類似於以下輸出(這些記錄來自CiscoSecure UNIX;思科安全Windows中的記錄可以用逗號分隔):

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
```

```
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

欄位按如下所示進行細分：

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RADIUS

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

無論記帳是開啟還是關閉，調試看起來都相同。但是，在「構建」時，會傳送「開始」記帳記錄。此外，在「拆除」時，會傳送「停止」會計記錄：

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

RADIUS記賬記錄類似於此輸出(這些記錄來自Cisco Secure UNIX;cisco Secure Windows中的選項以逗號分隔):

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

欄位按如下所示進行細分：

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
<Acct-Session-Time = #>
```

最大會話數和檢視登入使用者數

有些TACACS和RADIUS伺服器具有「max-session」或「view logged-in users」功能。執行max-sessions或check logged-in使用者的功能取決於記帳記錄。當產生記帳「開始」記錄但沒有「停止」記錄時，TACACS或RADIUS伺服器會假設該人員仍然登入(即；通過PIX有一個會話)。 由於連線的性質，這非常適用於Telnet和FTP連線。例如：

使用者通過PIX從171.68.118.100到9.9.9.25進行Telnet，在途中進行身份驗證：

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1200
   to 9.9.9.25/23
(pix) 109011: Authen Session Start: user 'cse', sid 3
(pix) 109005: Authentication succeeded for user 'cse' from 171.68.118.100/12
00 to 9.9.9.25/23
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23 gaddr 9.9.9.10/12
00 laddr 171.68.118.100/1200 (cse)
(server start account) Sun Nov  8 16:31:10 1998 rtp-pinecone.rtp.cisco.com
    cse PIX     171.68.118.100  start   task_id=0x3     foreign_ip=9.9.9.25
    local_ip=171.68.118.100     cmd=telnet
```

由於伺服器已看到「開始」記錄但沒有「停止」記錄（此時此刻），因此伺服器顯示「Telnet」使用者已登入。如果使用者嘗試需要身份驗證的另一連線（可能來自另一台PC），並且此使用者的max-sessions在伺服器上設定為「1」，伺服器將拒絕該連線。

使用者在目標主機上開展業務，然後退出（需要10分鐘）。

```
(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr 9.9.9.10/128 1
  laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)

 (server stop account) Sun Nov  8 16:41:17 1998
   rtp-pinecone.rtp.cisco.com cse PIX
   171.68.118.100  stop task_id=0x3 foreign_ip=9.9.9.25
   local_ip=171.68.118.100
   cmd=telnet elapsed_time=5  bytes_in=98 bytes_out=36
```

uauth是否為0(即；每次進行身份驗證)或更多（在uauth期間進行一次身份驗證）時，將為每個訪問的站點剪下記賬記錄。

但是由於協定的性質，HTTP的工作方式有所不同。範例如下：

使用者通過PIX從171.68.118.100瀏覽到9.9.9.25。

```
(pix) 109001: Auth start for user '???' from 171.68.118.100/1281
   to 9.9.9.25 /80 (pix) 109011: Authen Session Start: user 'cse', sid 5

 (pix) 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/12 81 to 9.9.9.25/80
```

```
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/80 gaddr 9.9.9.10/12 81
  laddr 171.68.118.100/1281 (cse)

(server start account) Sun Nov  8 16:35:34 1998 rtp-pinecone.rtp.cisco.com
  cse PIX     171.68.118.100  start   task_id=0x9     foreign_ip=9.9.9.25
  local_ip=171.68.118.100     cmd=http

(pix) 302002: Teardown TCP connection 5 faddr 9.9.9.25/80 gaddr 9.9.9.10/128 1
  laddr 171.68.118.100/1281 duration 0:00:00 bytes 1907 (cse)

(server stop account) Sun Nov  8 16:35.35 1998 rtp-pinecone.rtp.cisco .com
  cse     PIX     171.68.118.100  stop  task_id=0x9   foreign_ip =9.9.9.25

  local_ip=171.68.118.100 cmd=http   elapsed_time=0
     bytes_ in=1907   bytes_out=223
```

使用者讀取下載的網頁。

注意時間。此下載用時為一秒（開始和停止記錄之間不到一秒）。 使用者是否仍登入到網站，並且連線仍然開啟？編號

最大會話數或檢視登入使用者是否在此處工作？否，因為HTTP中的連線時間太短。「已建立」和「拆除」（「開始」和「停止」記錄）之間的時間為次秒。如果沒有「停止」記錄，則不會出現「開始」記錄，因為這些記錄實際上在同一時刻發生。無論uauth設定為0還是大於或等於0，仍會為每個事務向伺服器傳送「開始」和「停止」記錄。但是，由於HTTP連線的性質，最大會話數和檢視已登入使用者將無法工作。

使用Except命令

在我們的網路中，如果我們確定一個傳出使用者(171.68.118.100)不需要進行身份驗證，我們可以執行以下操作：

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11
   255.255.255.255 tacacs+
aaa authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11
   255.255.255.255 tacacs+
```

對PIX本身的身份驗證

前面討論的是通過PIX對Telnet（以及HTTP、FTP）流量進行身份驗證。在4.2.2中，與PIX的Telnet連線也可以通過身份驗證。在這裡，我們定義可以Telnet至PIX的框的IP:

```
telnet 171.68.118.100 255.255.255.255
```

然後提供Telnet密碼：**passwd ww**.

新增新的命令，驗證使用者通過Telnet連線到PIX:

```
aaa authentication telnet console tacacs+|radius
```

當使用者Telnet至PIX時，系統會提示他們輸入Telnet口令(「ww」)。 PIX還請求TACACS+或RADIUS使用者名稱和密碼。

更改使用者看到的提示

如果新增命令：**auth-prompt YOU_ARE_AT_THE_PIX**，通過PIX的使用者將看到以下順序：

```
YOU_ARE_AT_THE_PIX [at which point you enter the username] Password:[at which point you enter the password]
```

到達最終目的地後，將顯示「使用者名稱：」和「密碼：」提示。此提示僅影響使用者通過PIX，而不影響PIX。

注意：沒有針對訪問PIX而削減的記帳記錄。

相關資訊

- Cisco PIX防火牆軟體產品支援
- Cisco Secure PIX防火牆命令參考
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems