PIX、TACACS+和RADIUS配置示例：4.4.x

目錄

簡介

可以對FTP、Telnet和HTTP連線執行RADIUS和TACACS+身份驗證。通常可以驗證其它不太常見的TCP協定。

支援TACACS+授權；RADIUS授權不是。與先前版本相比，PIX 4.4.1身份驗證、授權和記帳(AAA)中的更改包括：AAA伺服器組和故障切換、啟用和串列控制檯訪問的身份驗證，以及接受和拒絕提示消息。

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。

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。
- 授權是使用者可以執行的操作。
- 未經授權，身份驗證有效。
- 未經身份驗證，授權無效。

假設您內部有100個使用者，並且只希望其中的6個使用者能夠在網路外部執行FTP、Telnet或HTTP。您會通知PIX驗證出站流量，並為TACACS+/RADIUS安全伺服器上的所有6個使用者ID提供證書。使用簡單身份驗證，這6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個使用者無法出站。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，並根據響應開啟或拒絕連線。這6位使用者可能執行FTP、Telnet或HTTP。

但假設三個使用者中的一個「Terry」不可信。您想允許Terry執行FTP，但不要使用HTTP或Telnet到外部。這意味著必須新增授權，即，除了驗證使用者身份之外，還要對使用者能夠執行的操作進行授權。當我們向PIX新增授權時，PIX將首先將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Terry正在嘗試執行什麼「命令」。正確設定伺服器後，可以允許Terry使用「FTP 1.2.3.4」，但會拒絕在任何地方使用HTTP或Telnet。

使用者透過開啟驗證/授權看到的專案

當嘗試從內部到外部（反之亦然）並且身份驗證/授權開啟時：

- **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請求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正在將快取的使用者名稱和密碼「拍攝」到PIX，然後PIX再將此資訊轉發到身份驗證伺服器，從而重新進行身份驗證。PIX系統日誌和/或伺服器調試將顯示此現象。如果Telnet和FTP似乎「正常」工作，但HTTP連線不工作，這就是原因。

適用於所有場景的安全伺服器配置

CiscoSecure UNIX TACACS伺服器配置

確保您在CSU.cfg檔案中具有PIX IP地址或完全限定域名和金鑰。

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

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

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

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

CiscoSecure 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。

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
```

CiscoSecure NT 2.x RADIUS

請完成以下步驟。

1. 在使用者設定GUI部分獲取密碼。
2. 在Group Setup GUI部分，將屬性6(Service-Type)設定為Login或Administrative。
3. 在NAS配置GUI中新增PIX IP。

EasyACS TACACS+

EasyACS文檔描述了設定。

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. 為要允許的每個命令（例如Telnet）選擇**Add/Edit** new命令。
4. 如果要允許Telnet到特定站點，請在引數部分以「permit #.#.#.#」的形式輸入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**完成編輯命令**。
6. 對每個允許的命令（例如Telnet、HTTP和/或FTP）執行步驟1至5。
7. 在NAS配置GUI部分新增PIX IP。

CiscoSecure 2.x TACACS+

使用者在GUI的「使用者設定」部分獲得密碼。

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. 為要允許的每個命令（例如Telnet）選擇**Add/Edit**。
4. 如果要允許Telnet到特定站點，請在引數矩形中輸入允許IP（例如，「permit 1.2.3.4」）。 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**完成編輯命令**。
6. 對每個允許的命令（例如Telnet、HTTP或FTP）執行步驟1至5。
7. 在NAS配置GUI部分新增PIX IP。

Livingston RADIUS伺服器配置

將PIX IP和金鑰新增到客戶端檔案。

```
adminuser 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。

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

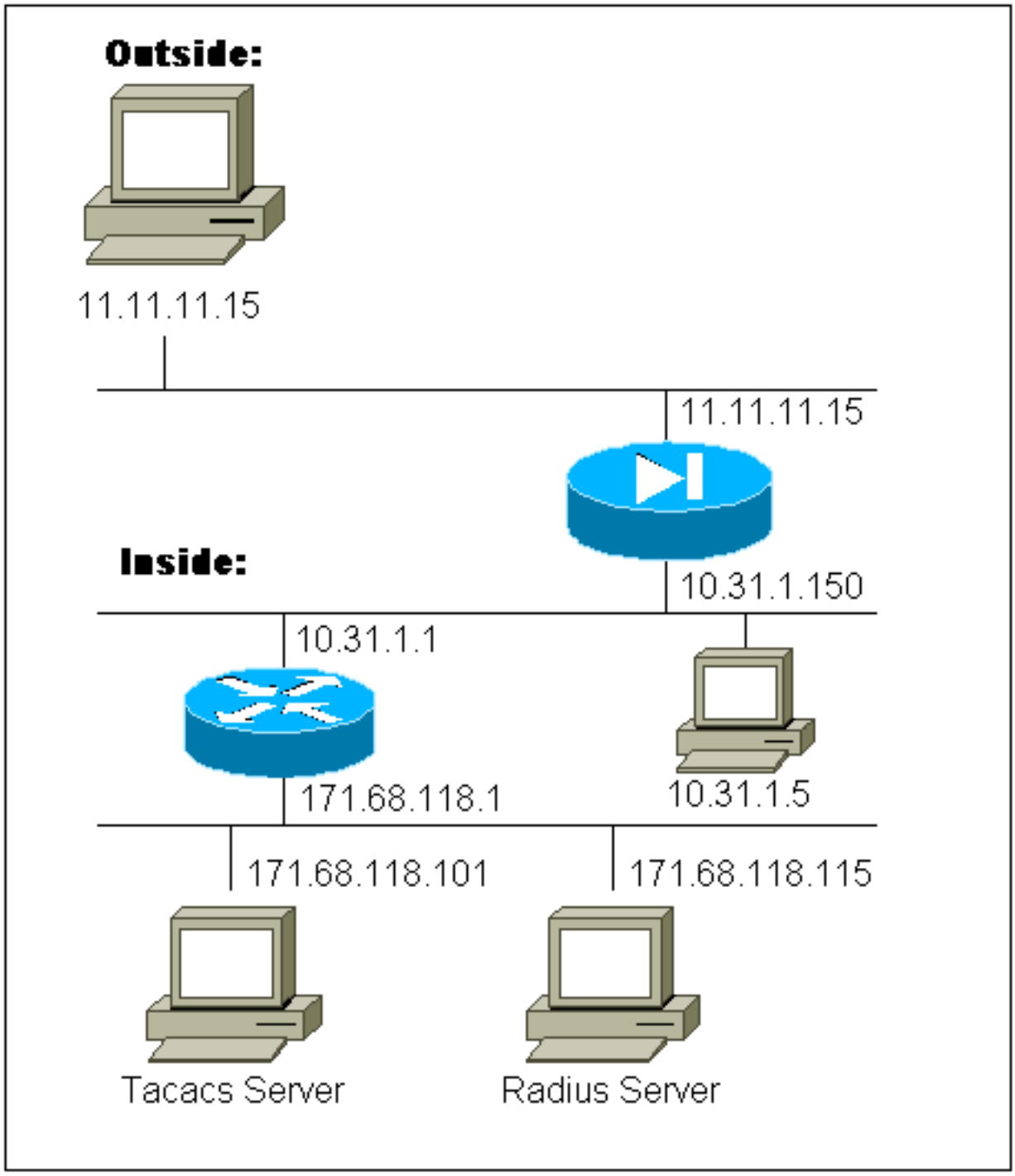
TACACS+免費軟體伺服器配置

```
key = "cisco"

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

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

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

user = can_only_do_ftp {
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。如果您無法在發起身份驗證和授權之前傳遞流量，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。

網路圖表



PIX配置

```
pix-5# write terminal
 Building configuration...
 : Saved
 :
 PIX Version 4.4(1)
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 nameif ethernet2 pix/intf2 security10
 nameif ethernet3 pix/intf3 security15
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pix-5
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol smtp 25
 fixup protocol h323 1720
```

```
 fixup protocol rsh 514
 fixup protocol sqlnet 1521
 names
 pager lines 24
 no logging timestamp
 logging console debugging
 no logging monitor
 no logging buffered
 logging trap debugging
 logging facility 20
 interface ethernet0 auto
 interface ethernet1 auto
 interface ethernet2 auto
 interface ethernet3 auto
 mtu outside 1500
 mtu inside 1500
 mtu pix/intf2 1500
 mtu pix/intf3 1500
 ip address outside 11.11.11.1 255.255.255.0
 ip address inside 10.31.1.150 255.255.255.0
 ip address pix/intf2 127.0.0.1 255.255.255.255
 ip address pix/intf3 127.0.0.1 255.255.255.255
 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 pix/intf2 0.0.0.0
 failover ip address pix/intf3 0.0.0.0
 arp timeout 14400
 global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0
 static (inside,outside) 11.11.11.20 171.68.118.115
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.21 171.68.118.101
netmask 255.255.255.255 0 0
 static (inside,outside) 11.11.11.22 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit icmp any any
 conduit permit tcp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 no rip pix/intf2 passive
 no rip pix/intf2 default
 no rip pix/intf3 passive
 no rip pix/intf3 default
 route inside 0.0.0.0 0.0.0.0 10.31.1.1 1
 timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
 timeout rpc 0:10:00 h323 0:05:00
 timeout uauth 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
!
!--- For any given list, multiple AAA servers can !---
be configured. They will be !--- tried sequentially if
any one of them is down. ! aaa-server Outgoing protocol
tacacs+ aaa-server Outgoing (inside) host 171.68.118.101
cisco timeout 10 aaa-server Incoming protocol radius
aaa-server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
```

```
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

來自PIX的身份驗證調試示例

在這些偵錯範例中：

出站

10.31.1.5的內部使用者向外部11.11.15發起流量，並通過TACACS+進行身份驗證（出站流量使用包括TACACS伺服器171.68.118.101的伺服器清單「傳出」）。

傳入

11.11.11.15的外部使用者向內部10.31.1.5(11.11.22)發起流量，並通過RADIUS進行身份驗證（入站流量使用伺服器清單「傳入」，包括RADIUS伺服器171.68.118.115）。

PIX調試 — 良好身份驗證 — TACACS+

以下示例顯示具有良好身份驗證的PIX調試：

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼）— TACACS+

以下示例顯示帶有錯誤身份驗證（使用者名稱或密碼）的PIX調試。 使用者看到四個使用者名稱/密碼集。將顯示以下消息："錯誤：超出最大嘗試次數」。

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

PIX調試 — 可以Ping通，但沒有響應 — TACACS+

以下示例顯示未與PIX進行通訊的ping伺服器的PIX調試。使用者只看到一次使用者名稱，而PIX從不要求密碼（此在Telnet上）。

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
```

```
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

PIX調試 — 無法Ping伺服器 — TACACS+

以下示例顯示不可執行ping操作的伺服器的PIX調試。使用者會看到使用者名稱一次。PIX從不要求密碼（此命令在Telnet上）。 將顯示以下消息：「TACACS+伺服器超時」和「錯誤：超出最大嘗試次數」（此範例中的組態反映虛假伺服器）。

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

PIX調試 — 良好身份驗證 — RADIUS

以下示例顯示具有良好身份驗證的PIX調試：

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼） — RADIUS

以下示例顯示帶有錯誤身份驗證（使用者名稱或密碼）的PIX調試。 使用者看到使用者名稱和密碼請求。如果其中任何一項錯誤，則消息「Incorrect password」顯示四次。然後，使用者斷開連線。此問題已分配錯誤ID #CSCdm46934。

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

PIX調試 — 停機，將不會與PIX通訊 — RADIUS

以下示例顯示使用可執行ping操作的伺服器進行PIX調試，但守護進程已關閉。伺服器不會與PIX通訊。使用者看到使用者名稱後跟密碼。將顯示以下消息：「RADIUS伺服器失敗」和「錯誤：超出最大嘗試次數」。

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
```

```
(server 171.68.118.115 failed)
304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
(server 171.68.118.115 failed)
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

PIX調試 — 無法Ping伺服器或金鑰/客戶端不匹配 — RADIUS

以下示例顯示不可執行ping操作或存在金鑰/客戶端不匹配的伺服器的PIX調試。使用者看到使用者名稱和密碼。將顯示以下消息：「RADIUS伺服器超時」和「錯誤：超出最大嘗試次數」（配置中的伺服器僅供範例使用）。

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
(server 171.68.118.199 failed)
109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

新增授權

由於未經身份驗證授權無效，我們將要求對相同的源和目標範圍進行授權：

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
```

傳出

請注意，我們不為「incoming」新增授權，因為傳入流量使用RADIUS進行身份驗證，且RADIUS授權無效

來自PIX的身份驗證和授權調試示例

使用良好身份驗證和成功授權的PIX調試 — TACACS+

以下示例顯示具有良好身份驗證和成功授權的PIX調試：

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_telnet', sid 7
109005: Authentication succeeded for user 'can_only_do_telnet'
from 10.31.1.5/11002 to 11.11.11.15/23
109011: Authen Session Start: user 'can_only_do_telnet', sid 7
109007: Authorization permitted for user 'can_only_do_telnet'
from 10.31.1.5/11002 to 11.11.11.15/23
109012: Authen Session End: user 'can_only_do_telnet', sid 7,
elapsed 1 seconds
302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

PIX調試 — 身份驗證良好，授權失敗 — TACACS+

以下示例顯示了具有良好身份驗證但授權失敗的PIX調試：

使用者在此處還會看到消息「錯誤：拒絕授權」

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

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 Outgoing
```

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

TACACS+記帳記錄如下所示(這些記錄來自CiscoSecure UNIX;ciscoSecure NT中的可以改為使用逗號分隔):

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

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

RADIUS記帳記錄如下所示：(這些產品來自CiscoSecure UNIX;ciscoSecure NT中的可以改為使用逗號分隔):

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
```

```
        Login-TCP-Port = 23
        Acct-Session-Id = "0x00000008"
        User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
        Acct-Status-Type = Stop
        Client-Id = 10.31.1.150
        Login-Host = 10.31.1.5
        Login-TCP-Port = 23
        Acct-Session-Id = "0x00000008"
        User-Name = "adminuser"
        Acct-Session-Time = 73
        Acct-Input-Octets = 27
        Acct-Output-Octets = 73
```

使用Except命令

在我們的網路中，如果我們確定特定源和/或目標不需要身份驗證、授權或記帳，我們可以執行以下操作：

```
aaa authentication except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
aaa authorization except outbound 10.31.1.60 255.255.255.255
11.11.11.15 255.255.255.255 Outgoing
```

如果您「例外」IP地址進行身份驗證並且啟用授權，您還必須禁止這些地址進行授權！

最大會話數和檢視登入使用者

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。當生成記帳「開始」記錄但沒有「停止」記錄時，TACACS+或RADIUS伺服器會假定該人員仍登入（即通過PIX具有會話）。

由於連線的性質，這非常適用於Telnet和FTP連線。由於連線的性質，HTTP無法順利運作。在以下示例中，使用了不同的網路配置，但概念是相同的。

使用者通過PIX進行遠端通訊，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），因此伺服器會顯示「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（可能從另一台PC進行），並且如果在此使用者的伺服器上將max-sessions設定為「1」（假定伺服器支援max-sessions），伺服器將拒絕該連線。

使用者繼續在目標主機上進行Telnet或FTP業務，然後退出（在那裡花費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
```

無論uauth是0（每次進行驗證）還是更多（在uauth期間反複進行驗證），都會為存取的每個網站剪下一條記帳記錄。

但是，由於協定的性質，HTTP的工作方式有所不同。以下是HTTP的示例。

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。

16:35:34張貼的起始記錄，16:35:35張貼的終止記錄。此下載僅需一秒(即；開始和停止記錄之間只有不到一秒的時間)。 使用者是否仍登入到該網站，並且在他們閱讀該網頁時連線仍然開啟？否。最大會話數或檢視登入的使用者是否在此處工作？否，因為HTTP中的連線時間（「已建立」和「拆除」之間的時間）太短。「開始」和「停止」記錄是次秒級。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。無論是否將uauth設定為0或更大，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，最大會話數和檢視登入使用者數將無法工作。

在PIX本身進行身份驗證和啟用

之前的討論是驗證通過PIX的Telnet（以及HTTP、FTP）流量。在下面的示例中，我們確保Telnet至pix在未經身份驗證的情況下工作：

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

然後，我們將新增命令來向PIX驗證使用者Telnet:

aaa authentication telnet console Outgoing

當使用者Telnet至PIX時，系統會提示他們輸入Telnet口令(「ww」)。 在這種情況下，PIX還會請求TACACS+（因為使用了「傳出」伺服器清單）或RADIUS使用者名稱和密碼。

aaa authentication enable console Outgoing

使用此命令，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。在這種情況下，由於使用了「傳出」伺服器清單，因此請求將轉到TACACS伺服器。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，因此使用者可以使用相同使用者名稱/密碼通過TACACS或RADIUS啟用（假定使用者可以使用TACACS或RADIUS登入到PIX）。此問題已分配錯誤ID #CSCdm47044。

在伺服器關閉時，使用者可以通過輸入PIX的使用者名稱的「PIX」和來自PIX的普通啟用密碼(「enable password whatever」)來訪問PIX啟用模式。 如果「enable password whatever」不在PIX配置中，使用者應輸入「PIX」作為使用者名稱並按Enter鍵。如果已設定啟用密碼但不知道該密碼，則需要使用密碼恢復磁碟進行重置。

串列控制檯上的身份驗證

aaa authentication serial console命令需要身份驗證驗證才能訪問PIX的串列控制檯。當使用者從控制檯執行配置命令時，系統日誌消息將被切斷（如果PIX配置為在調試級別將系統日誌傳送到系統日誌主機）。 以下是syslog伺服器的示例：

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

更改提示使用者檢視

如果我們有命令：

auth-prompt THIS_IS_PIX_5

通過PIX的使用者可以看到以下順序：

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

然後，到達最終目標框後，顯示「使用者名稱：」和「密碼：」提示目標框。

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。

自定義使用者在成功/失敗時看到的消息

如果有命令：

```
auth-prompt accept "You're allowed through the pix"
auth-prompt reject "You blew it"
```

使用者通過PIX登入失敗/成功時將會看到以下內容：

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
 "You blew it"
 "THIS_IS_PIX_5"
 Username: cse
 Password:
 "You're allowed through the pix"
```

每使用者空閒和絕對超時

可以針對每個使用者從TACACS+伺服器向下傳送空閒和絕對uauth超時。如果您的網路中的所有使用者都有相同的「timeout uauth」，則不要實作此功能！但是，如果每個使用者需要不同的使用者授權，請繼續閱讀。

在PIX的示例中，我們使用**timeout uauth 3:00:00**命令。這表示一個人一旦進行身份驗證，在3小時內將不必重新進行身份驗證。但是，如果我們使用以下配置檔案設定使用者，並在PIX中啟用TACACS AAA授權，則使用者配置檔案中的空閒和絕對超時將覆蓋該使用者在PIX中的超時uauth。這並不意味著通過PIX的Telnet會話在空閒/絕對超時後斷開。它只控制是否發生重新身份驗證。

```
user = timeout {
default service = permit
login = cleartext "timeout"
service = exec {
timeout = 2
idletime = 1
}
}
```

身份驗證後，在PIX上發出**show uauth**命令：

```
pix-5# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'timeout' at 10.31.1.5, authorized to:
    port 11.11.11.15/telnet
    absolute   timeout: 0:02:00
    inactivity timeout: 0:01:00
```

使用者空閒一分鐘後，PIX上的調試顯示：

```
109012: Authen Session End: user 'timeout', sid 19, elapsed 91 seconds
```

使用者返回同一目標主機或其他主機時必須重新進行身份驗證。

虛擬HTTP

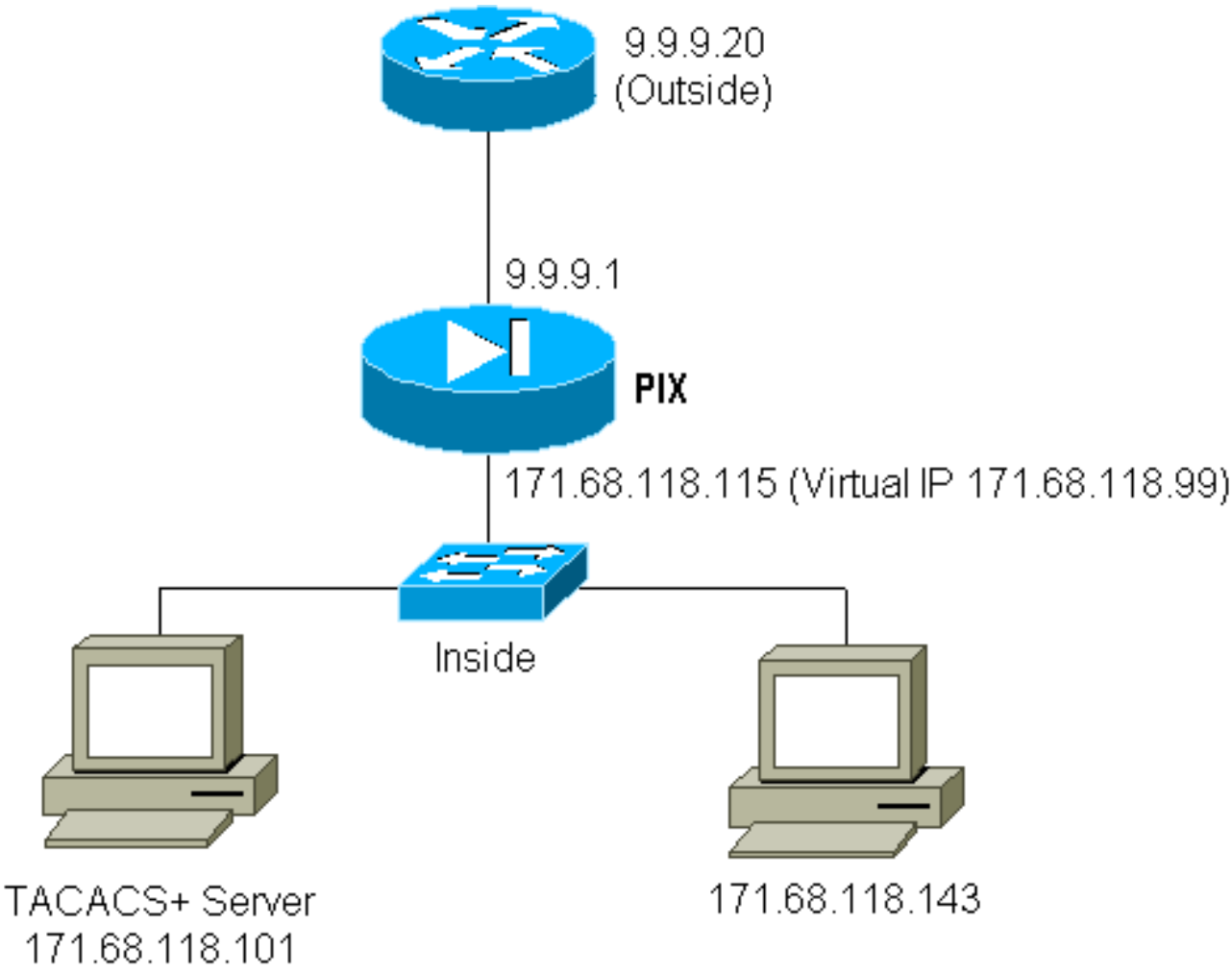
如果在PIX外部的站點以及PIX本身需要身份驗證，有時會觀察到異常的瀏覽器行為，因為瀏覽器會快取使用者名稱和密碼。

要避免這種情況，可以使用以下命令向PIX配置中新增一個RFC 1918 地址（即，在Internet上不可路由，但對PIX內部網路有效且唯一的地址）來實施虛擬HTTP:

```
virtual http #.#.#.# [warn]
```

當使用者嘗試離開PIX時，需要進行身份驗證。如果存在warn引數，則使用者會收到重新導向訊息。驗證對uauth中的時間長度沒有影響。如文檔所示，請勿使用虛擬HTTP將**timeout uauth**命令持續時間設定為0秒；這可以防止與實際Web伺服器的HTTP連線。

虛擬HTTP出站示例：



PIX配置虛擬HTTP出站：

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server Outgoing protocol tacacs+
 aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
  aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

```
virtual http 171.68.118.99
auth-prompt THIS_IS_PIX_5
```

虛擬Telnet

將PIX配置為對所有入站和出站流量進行身份驗證不是個好主意，因為某些協定（如「郵件」）不容易進行身份驗證。當通過PIX的所有流量都經過身份驗證時，郵件伺服器和客戶端嘗試通過PIX通訊時，用於不可驗證協定的PIX系統日誌將顯示以下消息：

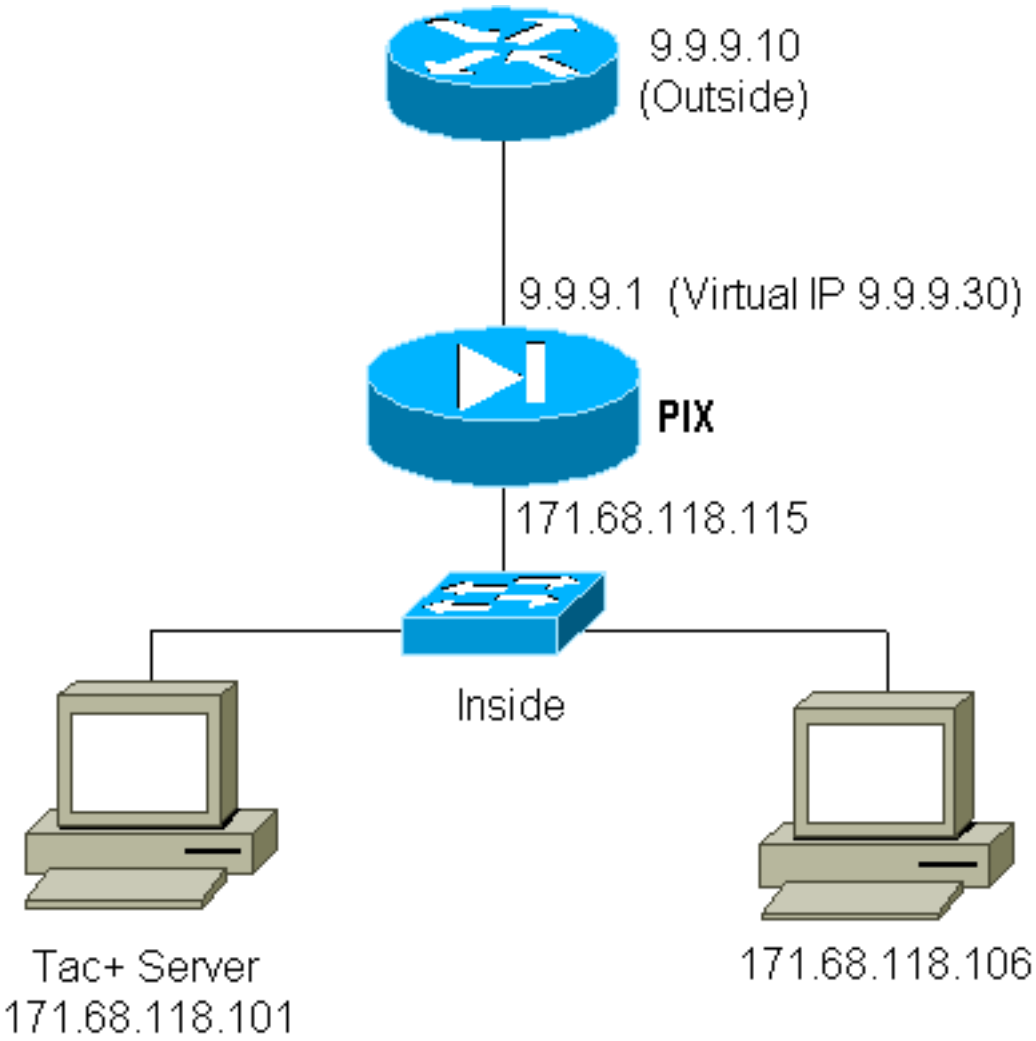
```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated
```

由於郵件和某些其他服務的互動性不足以進行身份驗證，因此一個解決方案是使用**except**命令進行身份驗證/授權（對郵件伺服器/客戶端的源/目標以外的所有服務進行身份驗證）。

但是，如果確實需要對某種異常服務進行身份驗證，可以使用**virtual telnet**命令完成此操作。此命令允許對虛擬Telnet IP進行身份驗證。進行此驗證後，異常服務的流量可以流向與虛擬IP關聯的真實伺服器。

在我們的示例中，我們想要允許TCP埠49流量從外部主機9.9.9.10流向內部主機171.68.118.106。由於此流量實際上不可驗證，因此我們設定了虛擬Telnet。

虛擬Telnet入站：



PIX配置虛擬Telnet入站：

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
 aaa-server Incoming (inside) host 171.68.118.101 cisco timeout 5
 aaa authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
 virtual telnet 9.9.9.30
```

TACACS+伺服器使用者配置虛擬Telnet入站：

```
user = pinecone {
default service = permit
        login = cleartext "pinecone"
service = exec {
        timeout = 10
        idletime = 10
        }
}
```

PIX調試虛擬Telnet入站：

9.9.9.10上的使用者必須先通過遠端登入到PIX上的9.9.9.30地址進行身份驗證：

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
 to 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

成功驗證後，**show uauth**命令會顯示使用者有「計量器上的時間」：

```
pixfirewall# show uauth
                         Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

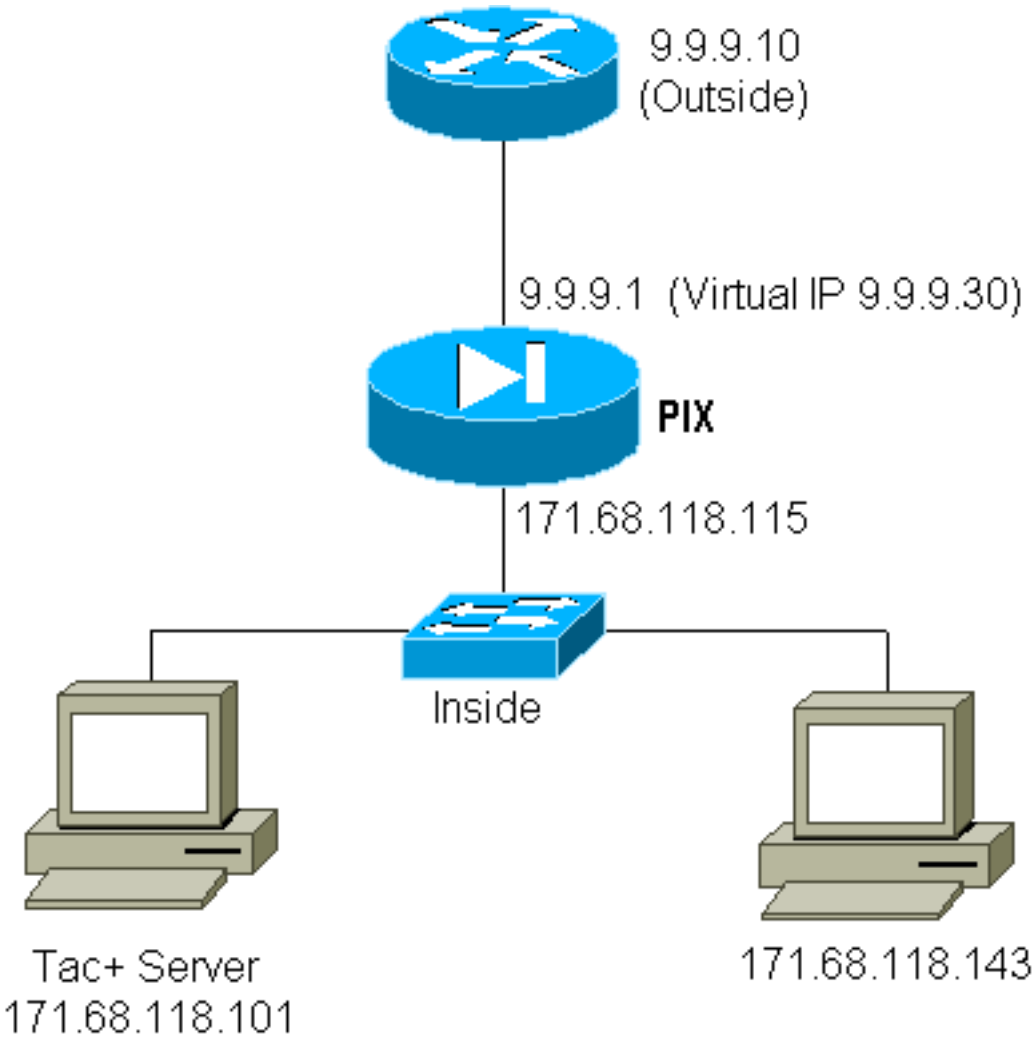
當位於9.9.9.10的裝置要向位於171.68.118.106的裝置傳送TCP/49流量時：

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr
 9.9.9.30/49 laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

虛擬Telnet出站：

由於預設情況下允許出站流量，因此使用虛擬Telnet出站不需要靜態。在以下示例中，位於171.68.118.143的內部使用者將Telnet到虛擬9.9.9.30並進行身份驗證。Telnet連線會立即捨棄。

通過身份驗證後，允許從171.68.118.143到伺服器9.9.9.10的TCP流量：



PIX配置虛擬Telnet出站：

```
 ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server Outgoing protocol tacacs+
 aaa-server Outgoing (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
 virtual telnet 9.9.9.30
```

PIX調試虛擬Telnet出站：

```
109001: Auth start for user '???' from 171.68.118.143/1536 to 9.9.9.30/23
 109011: Authen Session Start: user 'timeout_143', sid 25
 109005: Authentication succeeded for user 'timeout_143' from
171.68.118.143/1536 to 9.9.9.30/23
 302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
  laddr 171.68 .118.143/1537 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
  laddr 171.68 .118.143/1538 (timeout_143)
 302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr 9.9.9.30/1537
  laddr 171.68. 118.143/1537 duration 0:00:03 bytes 625 (timeout_143)
```

```
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr 9.9.9.30/1538
 laddr 171.68. 118.143/1538 duration 0:00:01 bytes 2281 (timeout_143)
302009: 0 in use, 1 most used
```

虛擬Telnet註銷

使用者Telnet到虛擬Telnet IP時，**show uauth**指令會顯示其uauth。如果使用者想要在其作業階段完成之後防止流量通過（當uauth中還有時間時），他需要再次Telnet到虛擬Telnet IP。這會關閉作業階段。

連線埠授權

您可以要求對一系列埠進行授權。在以下示例中，所有出站仍然需要身份驗證，但僅對TCP埠23-49需要授權。

PIX配置：

```
aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

因此，當我們從171.68.118.143到9.9.9.10 Telnet時，由於Telnet埠23位於23-49範圍內，因此發生了身份驗證和授權。執行從171.68.118.143到9.9.9.10的HTTP會話時，我們仍需進行身份驗證，但是PIX不會要求TACACS+伺服器授權HTTP，因為80不在23-49範圍內。

TACACS+免費軟體伺服器配置

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
        }
        }
```

請注意，PIX正在將「cmd=tcp/23-49」和「cmd-arg=9.9.9.10」傳送到TACACS+伺服器。

在PIX上進行調試：

```
109001: Auth start for user '???' from 171.68.118.143/1051 to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', sid 0
 109005: Authentication succeeded for user 'telnetrange' from
 171.68.118.143/1051 to 9. 9.9.10/23
 109011: Authen Session Start: user 'telnetrange', sid 0
 109007: Authorization permitted for user 'telnetrange' from
 171.68.118.143/1051 to 9.9 .9.10/23
 302001: Built TCP connection 0 for faddr 9.9.9.10/23 gaddr 9.9.9.5/1051
 laddr 171.68.1 18.143/1051 (telnetrange)
 109001: Auth start for user '???' from 171.68.118.143/1105 to 9.9.9.10/80
 109001: Auth start for user '???' from 171.68.118.143/1110 to 9.9.9.10/80
 109011: Authen Session Start: user 'telnetrange', sid 1
 109005: Authentication succeeded for user 'telnetrange' from
 171.68.118.143/1110 to 9. 9.9.10/80
 302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
```

```
 laddr 171.68.1 18.143/1110 (telnetrange)
 302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.1 18.143/1111 (telnetrange)
 302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111 laddr
171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

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