配置PIX 5.0.x:TACACS+和RADIUS

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。PIX 5.0身份驗證、授權和記帳(AAA)與先前版本相比的更改包括除HTTP、FTP和Telnet之外的流量的AAA記帳。

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。
- 未經驗*證*，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。使用簡單的*驗證*，這六個使用者可以使用使用者名稱和密碼進行驗證，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。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。

另一方面，假設*這*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。這意味著您需要新增*授權*。即，授權用*戶*除了驗證*身份*之外還能做*什麼*的事情。當您將*authorization*新增到PIX時，PIX會先將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正在嘗試執行的「*command*」操作。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** -瀏覽器中顯示的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似乎工作正常，但HTTP連線不正常，這就是原因。

適用於所有場景的安全伺服器配置

Cisco Secure 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 .*
}
}
}
```

Cisco Secure UNIX RADIUS伺服器配置

使用圖形使用者介面(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
}
}
```

Cisco安全Windows 2.x RADIUS

請遵循以下步驟：

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. 為您希望允許的每個命令（例如Telnet）選擇**Add/Edit new command**。
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或FTP）執行步驟1至5。
7. 在NAS配置GUI部分新增PIX IP。

Cisco Secure 2.x TACACS+

使用者在「使用者設定GUI」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 new command**。
4. 如果要允許Telnet到特定站點，請在引數矩形中輸入permit IP(s)（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**finish editing**命令。
6. 對每個允許的命令（例如Telnet、HTTP和/或FTP）執行上述步驟。
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。

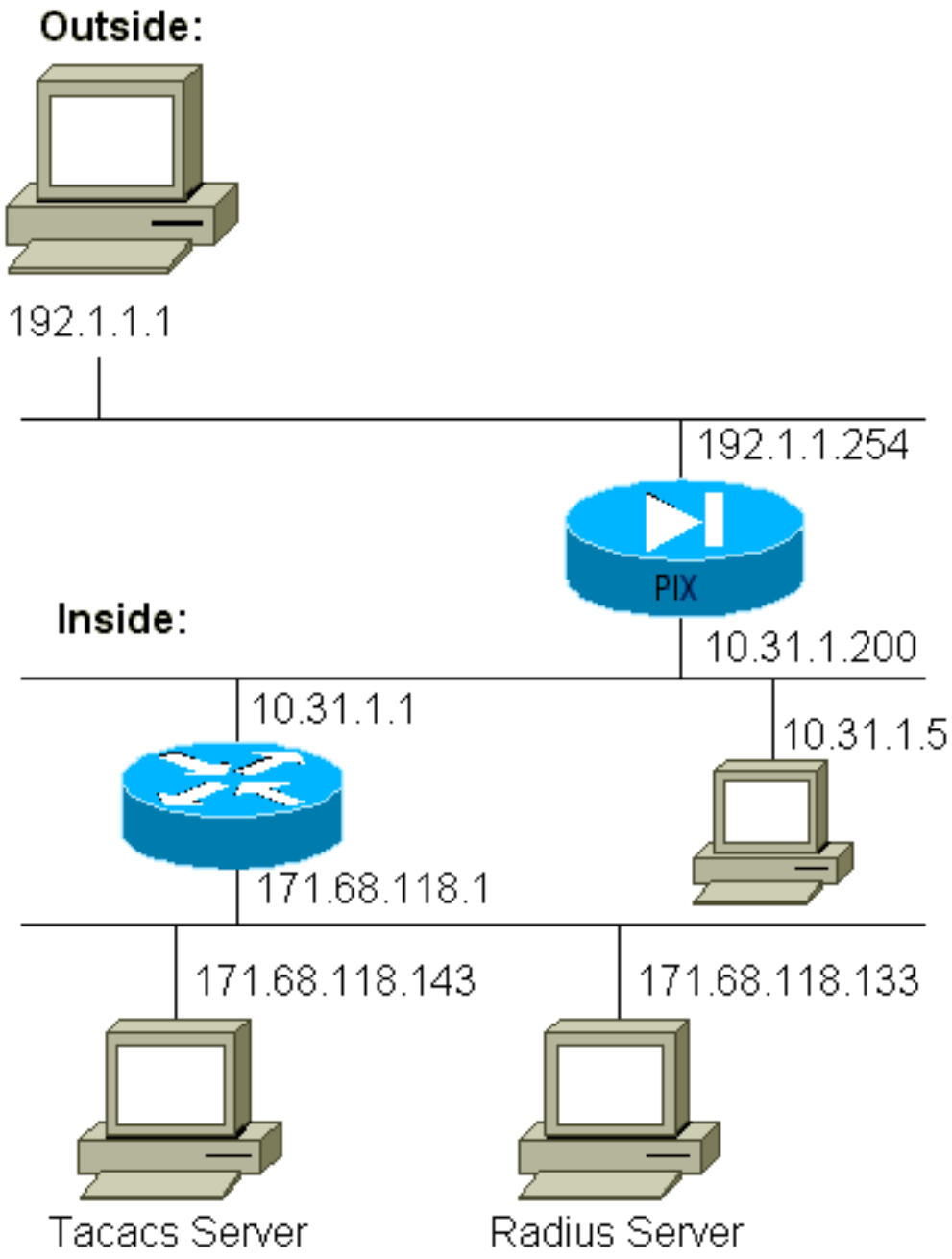
```
adminuser Password="all"
Service-Type = Shell-User

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
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 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
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask
255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143
netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 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
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143
cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133
```

```
cisco timeout 5
 aaa authentication telnet outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication telnet inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound
 aaa authentication http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound
 aaa authentication http inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 aaa authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthOutbound
 aaa authentication ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 AuthInbound
 no snmp-server location
 no snmp-server contact
 snmp-server community public
 no snmp-server enable traps
 telnet timeout 5
 terminal width 80
 Cryptochecksum:fef4bfc9801d7692dce0cf227fe7859b
 : end
```

來自PIX的身份驗證調試示例來自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192.1.1.1發起流量，並通過TACACS+進行身份驗證。傳出流量使用伺服器清單「AuthOutbound」，其中包括RADIUS伺服器171.68.118.133。

傳入

192.1.1.1的外部使用者向內部10.31.1.5(192.1.1.30)發起流量，並通過TACACS進行身份驗證。傳入流量使用伺服器清單「AuthInbound」(包括TACACS伺服器(171.68.118.143)。

PIX調試 — 良好身份驗證 — TACACS+

此示例顯示具有良好身份驗證的PIX調試：

```
pixfirewall# 109001: Auth start for user "???" from 192.1.1.1/13155
    to 10.31.1.5/23
 109011: Authen Session Start: user 'pixuser', sid 6
 109005: Authentication succeeded for user 'pixuser' from 10.31.1.5/23
    to 192.1.1.1/13155
 109012: Authen Session End: user 'pixuser', Sid 6, elapsed 1 seconds
 302001: Built inbound TCP connection 6 for faddr 192.1.1.1/13155
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼） — TACACS+

此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/密碼集和消息「Error:數。"

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

PIX調試 — 可以Ping伺服器，無響應 — TACACS+

此示例顯示PIX調試，在該調試中，伺服器可以ping通，但不會與PIX通訊。使用者只看到一次使用者名稱，但PIX從不要求密碼（此在Telnet上）。 使用者看到「Error:」

```
Auth start for user '???' from 192.1.1.1/13159 to
    10.31.1.5/23
 pixfirewall# 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159
    failed (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13159 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13159
```

PIX調試 — 無法Ping伺服器 — TACACS+

此示例顯示伺服器無法ping通的PIX調試。使用者只看到一次使用者名稱，但PIX從不要求密碼（這是Telnet）。 將顯示以下消息："Timeout to TACACS+server"和"Error:數」（我們在配置中的假伺服器中交換）。

```
109001: Auth start for user '???' from 192.1.1.1/13158
    to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109002: Auth from 10.31.1.5/23 to 192.1.1.1/13158 failed
    (server 171.68.118.143 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13158
```

PIX調試 — 良好身份驗證 — RADIUS

此示例顯示具有良好身份驗證的PIX調試：

```
109001: Auth start for user '???' from 10.31.1.5/11074
    to 192.1.1.1/23
 109011: Authen Session Start: user 'pixuser', Sid 7
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.5/11074 to 192.1.1.1/23
 109012: Authen Session End: user 'pixuser', Sid 7,
    elapsed 1 seconds
 302001: Built outbound TCP connection 7 for faddr 192.1.1.1/23
    gaddr 192.1.1.30/11074 laddr 10.31.1.5/11074 (pixuser)
```

PIX調試 — 身份驗證錯誤（使用者名稱或密碼）— RADIUS

此示例顯示具有錯誤身份驗證（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。使用者有三個成功輸入使用者名稱/密碼的機會。

```
- 'Error: max number of tries exceeded'
 pixfirewall# 109001: Auth start for user '???' from
    192.1.1.1/13157 to 10.31.1.5/23
 109001: Auth start for user '???' from 10.31.1.5/11075
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11075 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11075
    to 192.1.1.1/23
```

Ping調試 — 可以Ping伺服器，守護程式關閉 — RADIUS

此示例顯示了一個PIX調試，其中伺服器可以執行ping操作，但守護進程已關閉，不會與PIX通訊。使用者看到使用者名稱、密碼，以及訊息「`RADIUS server failed`」和「`Error:`」

```
pixfirewall# 109001: Auth start for user '???'
    from 10.31.1.5/11076 to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109002: Auth from 10.31.1.5/11076 to 192.1.1.1/23 failed
    (server 171.68.118.133 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11076
    to 192.1.1.1/23
```

PIX調試 — 無法Ping伺服器或金鑰/客戶端不匹配 — RADIUS

此示例引導一個PIX調試，在該調試中伺服器無法ping通或存在金鑰/客戶端不匹配。使用者看到使用者名稱、密碼，以及訊息「`Timeout to RADIUS server`」和「`Error:`數」（配置中交換了假伺服器）。

```
109001: Auth start for user '???' from 10.31.1.5/11077
    to 192.1.1.1/23
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109002: Auth from 10.31.1.5/11077 to 192.1.1.1/23 failed
    (server 100.100.100.100 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11077
    to 192.1.1.1/23
```

新增授權

如果您決定新增授權，您將需要同一源和目標範圍的授權（因為未經身份驗證授權無效）：

```
aaa authorization telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization HTTP inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authorization ftp inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

請注意，未為「傳出」新增授權，因為傳出流量使用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

PIX調試 — 良好身份驗證和成功授權 — TACACS+

此示例顯示了具有良好身份驗證和成功授權的PIX調試：

```
109011: Authen Session Start: user 'pixuser', Sid 8
 109007: Authorization permitted for user 'pixuser'
    from 192.1.1.1/13160 to 10.31.1.5/23
 109012: Authen Session End: user 'pixuser', Sid 8,
    elapsed 1 seconds
 302001: Built inbound TCP connection 8 for faddr 192.1.1.1/13160
    gaddr 192.1.1.30/23 laddr 10.31.1.5/23 (pixuser)
```

PIX調試 — 身份驗證良好，授權失敗 — TACACS+

此示例顯示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「Error:」

```
109001: Auth start for user '???' from 192.1.1.1/13162
    to 10.31.1.5/23
 109011: Authen Session Start: user 'userhttp', Sid 10
 109005: Authentication succeeded for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109008: Authorization denied for user 'userhttp'
    from 10.31.1.5/23 to 192.1.1.1/13162
 109012: Authen Session End: user 'userhttp', Sid 10,
    elapsed 1 seconds
 302010: 0 in use, 2 most used
```

新增記帳

TACACS+

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

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。在「拆除」時，傳送「停止」記帳記錄。

TACACS+記帳記錄類似於以下輸出（這些記錄來自Cisco Secure NT，因此使用逗號分隔格式）：

```
04/26/2000,01:31:22,pixuser,Default Group,192.1.1.1,
  start,,,,,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1.1,
  ,, ,,,,,,,,,zekie,,,,,,,,^
04/26/2000,01:31:26,pixuser,Default Group,192.1.1.1,stop,4,
  ,36,82,,,0x2a,,PIX,10.31.1.200,telnet,6,
  Login,1,,,1,,,,,,,,,,,local_ip=10.31.1.5 foreign_ip=192.1.1. 1,
  ,,,,,,,,,,,zekie,,,,,,,,
```

RADIUS

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
```

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。在「拆除」時，傳送「停止」記帳記錄。

RADIUS記賬記錄類似於此輸出(這些記錄來自Cisco Secure UNIX;cisco Secure NT中的1可以改為用逗號分隔):

```
radrecv: Request from host a1f01c8 code=4, id=18, length=65
Acct-Status-Type = Start
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
User-Name = "pixuser"
Sending Accounting Ack of id 18 to a1f01c8 (10.31.1.200)
radrecv: Request from host a1f01c8 code=4, id=19, length=83
Acct-Status-Type = Stop
Client-Id = 10.31.1.200
Login-Host = 10.31.1.5
Login-TCP-Port = 23
Acct-Session-Id = "0x0000002f"
Username = "pixuser"
Acct-Session-Time = 7
```

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，我們可以執行如下輸出：

```
aaa authentication except inbound 192.1.1.1 255.255.255.255
   0.0.0.0 0.0.0.0 AuthInbound
```

如果您「例外」一個盒子進行身份驗證並啟用授權，您還必須將盒子排除在授權之外。

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處於登入狀態（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。在此範例輸出中，使用不同的網路組態，但概念相同。

使用者通過PIX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），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），並且此使用者的max-sessions在伺服器上設定為「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（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
```

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。

由於通訊協定的性質，HTTP的運作方式不同。以下輸出顯示HTTP的範例：

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。

開始記錄發佈於16:35:34，停止記錄發佈於16:35:35。此下載用了一秒鐘（即，開始記錄與停止記錄之間不到一秒）。 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無法工作。

在PIX本身進行身份驗證和啟用

之前的討論描述了通過PIX對Telnet（和HTTP、FTP）流*量進*行身份驗證。我們確保Telnet至*PIX在*以下位置不進*行身份*驗證的情況下運行：

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

當使用者Telnet至PIX時，系統會提示他們輸入Telnet密碼(**ww**)。 接下來PIX也會請求TACACS+（在本例中，因為使用了「AuthInbound」伺服器清單）或RADIUS使用者名稱和密碼。如果伺服器關閉，您可以通過輸入**pix**作為使用者名稱，然後輸入enable password(**enable password**隨意)來訪問PIX。

使用以下命令：

```
aaa authentication enable console AuthInbound
```

系統會提示使用者輸入使用者名稱和密碼，並將其傳送到TACACS（在這種情況下，由於使用了「AuthInbound」伺服器清單，因此要求會傳送到TACACS伺服器）或RADIUS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，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。此問題已分配有Cisco錯誤ID CSCdm47044(僅限註冊客戶)。

串列控制檯上的身份驗證

aaa authentication serial console AuthInbound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，系統日誌消息被切斷（假設PIX配置為在調試級別將系統日誌傳送到系統日誌主機）。 以下是系統日誌伺服器上所顯示的範例：

```
logmsg: pri 245, flags 0, from [10.31.1.200.2.2], msg Nov 01 1999
 03:21:14: %PIX-5-111008: User 'pixuser' executed the 'logging' command.
```

更改使用者看到的提示

如果使用**auth-prompt PIX_PIX_PIX**命令，通過PIX的使用者將看到以下順序：

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

到達最終目標框後，將顯示「使用者名稱：」和「密碼：」提示。此提示僅影響通過PIX*的*使用者，而不*影響*到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

如果您有以下命令：

```
auth-prompt accept "GOOD_AUTH"
auth-prompt reject "BAD_AUTH"
```

使用者通過PIX登入失敗/成功時看到以下序列：

```
PIX_PIX_PIX
 Username: asjdkl
 Password:
 "BAD_AUTH"
 "PIX_PIX_PIX"
 Username: cse
 Password:
 "GOOD_AUTH"
```

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」，請勿實作此功能！但是，如果每個使用者需要不同的使用者，請繼續閱讀。

在本範例中，使用**timeout uauth 3:00:00**指令。一個人一旦進行身份驗證，就不必再重新進行身份驗證三小時。但是，如果您使用此配置檔案設定使用者並在PIX中啟用TACACS AAA *authorization*，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。

此配置檔案來自TACACS+免費軟體：

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

身份驗證後，在PIX上執行**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

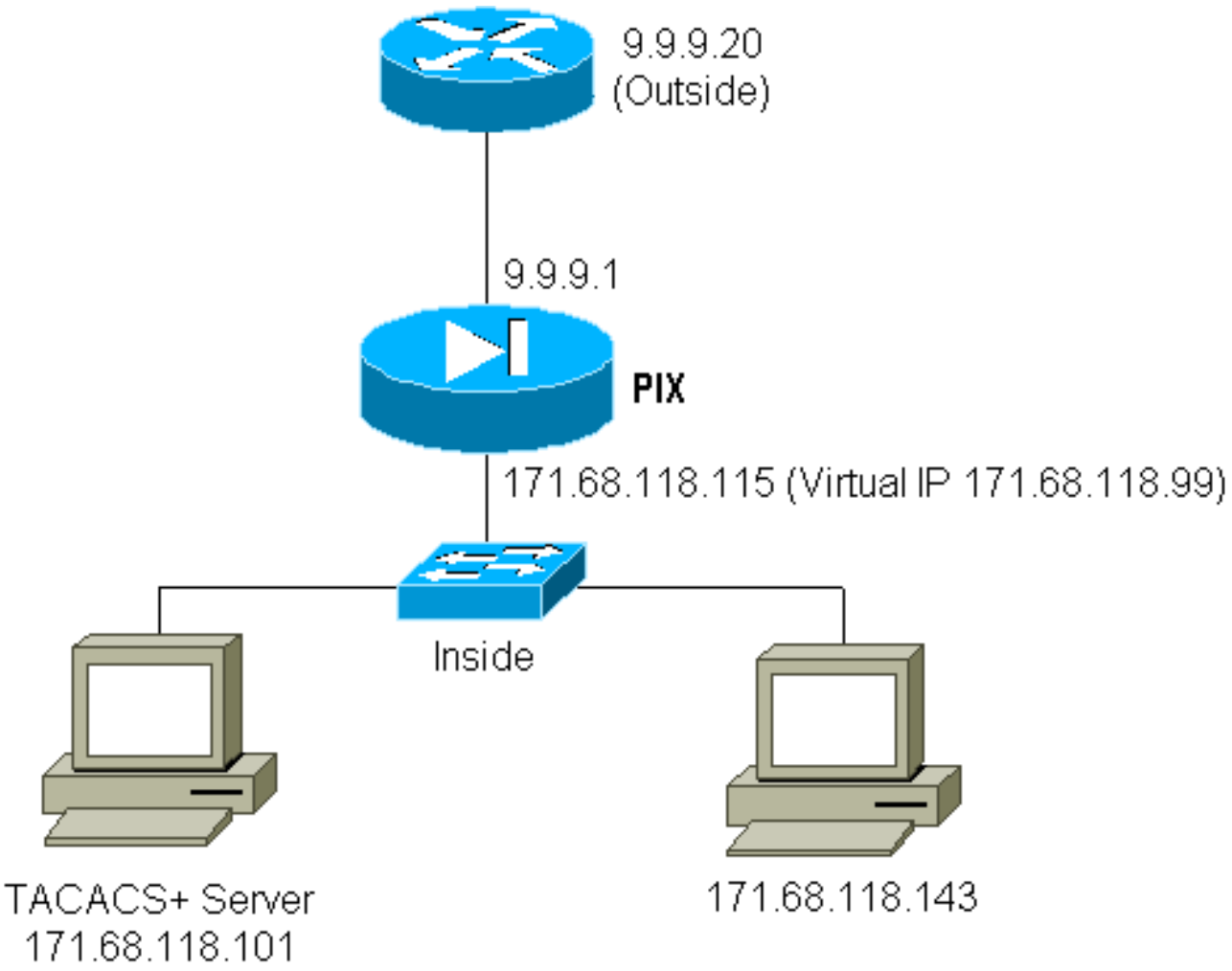
如果在PIX外部的站點以及PIX本身需要身份驗證，有時會觀察到異常的瀏覽器行為，因為瀏覽器會快取使用者名稱和密碼。

要避免這種情況，您可以實施虛擬HTTP，方法是使用以下命令向PIX配置中新增一個RFC 1918 地址（該地址在Internet上不可路由，但對PIX內部網路而言有效且唯一）：

```
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出站圖



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 AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (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 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

虛擬Telnet

可以將PIX配置為對所有入站和出站流量進行身份驗證，但是這樣做並不理想。這是因為某些通訊協定（例如「mail」）無法輕易進行驗證。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，不可驗證協定的PIX系統日誌顯示以下消息：

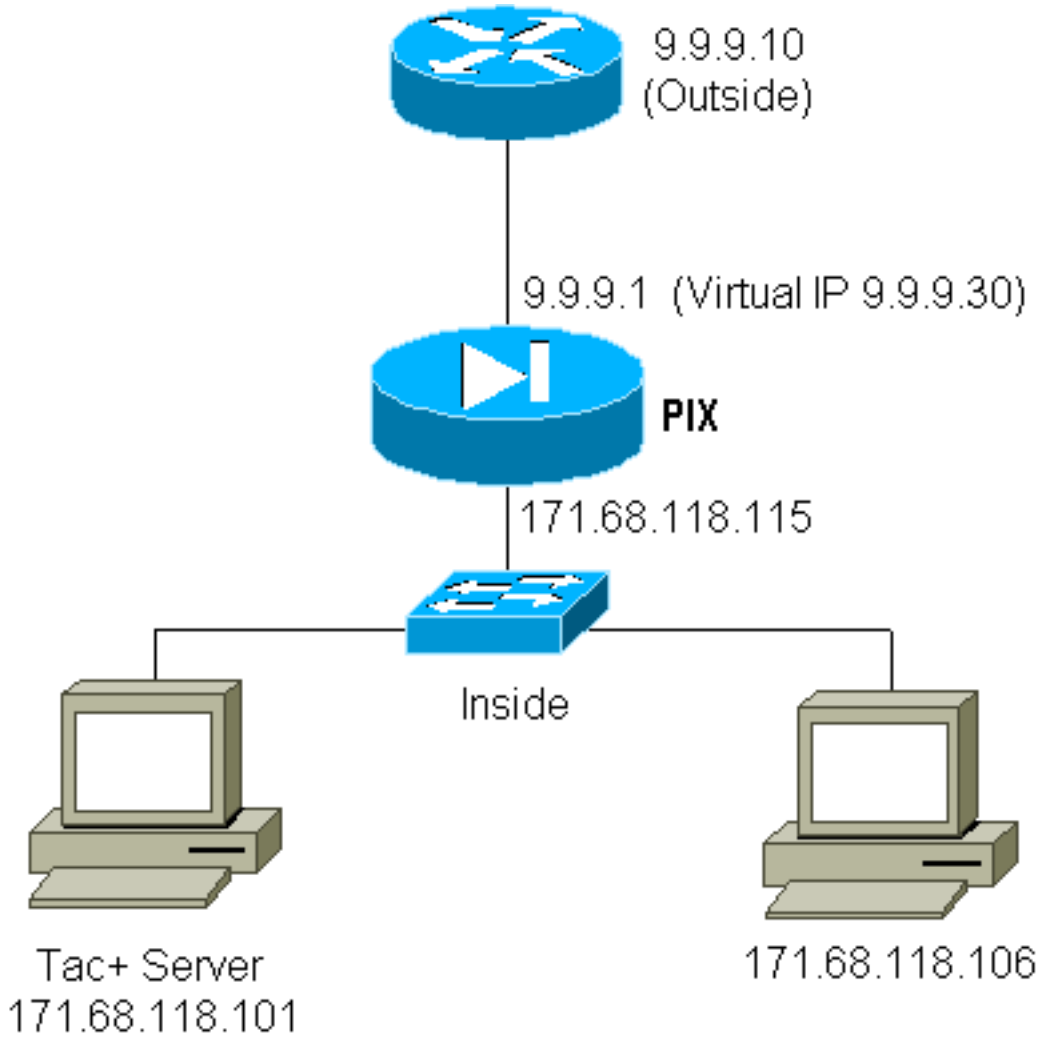
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

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）。

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進入實際伺服器。

在本例中，我們想讓TCP埠49流量從外部主機9.9.9.10流向內部主機171.68.118.106。由於此流量並非真正可身份驗證，因此我們設定了一個虛擬Telnet。對於入站虛擬Telnet，必須存在關聯的靜態。這裡，9.9.9.20和171.68.118.20都是虛擬地址。

虛擬Telnet傳入圖表



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) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (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 AuthInbound
 virtual telnet 9.9.9.20
```

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上的使用者必須首先通過Telnet向PIX上的9.9.9.20地址進行身份驗證：

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
    to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 13
 109005: Authentication succeeded for user 'pinecone'
    from 171.68.118.20/23 to 9.9.9.10/1470
```

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

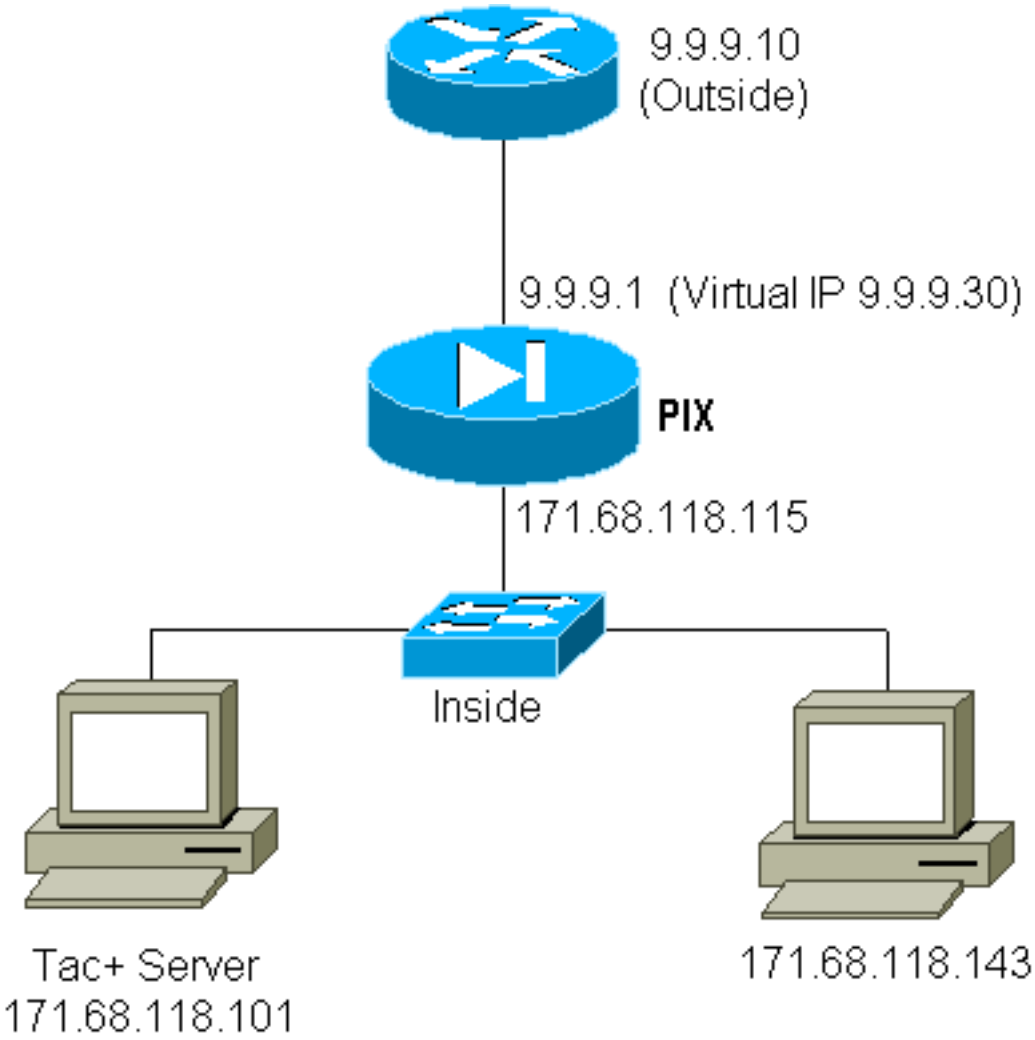
```
pixfirewall# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

這裡，位於9.9.9.10的裝置要將TCP/49流量傳送到位於171.68.118.106的裝置：

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 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。在本示例中，位於171.68.118.143 Telnet的內部使用者連線到虛擬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 AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (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 AuthOutbound
 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uauth。

如果使用者想要在會話完成後（當uauth中還有時間時）阻止流量通過，則使用者需要再次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。在本示例中，所有出站仍然需要身份驗證，但TCP埠23-49只需要授權。

PIX配置

```
AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
AAA authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0
   0.0.0.0 0.0.0.0 AuthOutbound
```

從171.68.118.143到9.9.9.10執行Telnet時，由於Telnet埠23在23-49範圍內，因此發生了身份驗證和授權。

從171.68.118.143到9.9.9.10完成HTTP會話時，您仍然必須進行身份驗證，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。

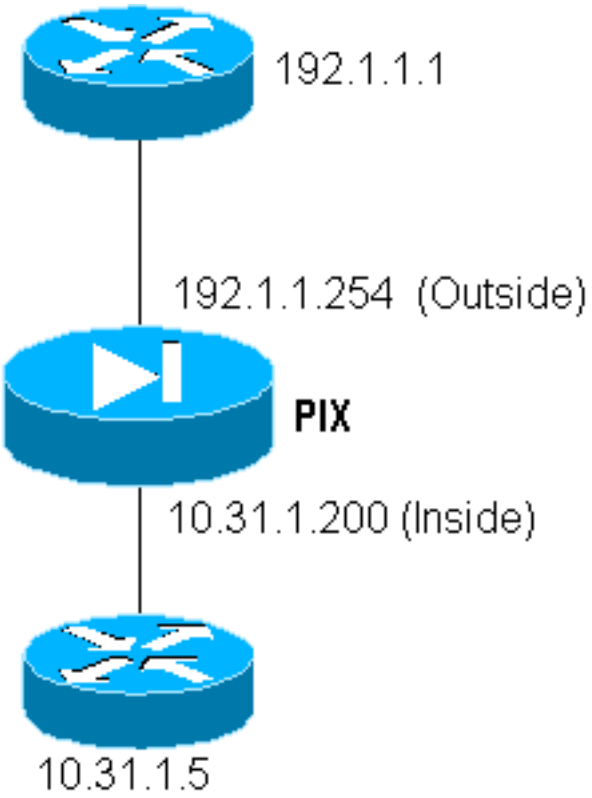
在PIX上進行調試

```
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)
```

除HTTP、FTP和Telnet以外的流量的AAA記帳

PIX軟體5.0版更改流量計費功能。完成驗證後，現在可以為HTTP、FTP和Telnet以外的流量剪下記帳記錄。



若要將檔案從外部路由器(192.1.1.1)複製到內部路由器(10.31.1.5)，請新增虛擬Telnet以開啟TFTP程式的漏洞：

```
virtual telnet 192.1.1.30
static (inside,outside) 192.1.1.30 10.31.1.5 netmask 255.255.255.255 0 0
conduit permit udp any any
AAA authentication udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
AAA authorization udp/69 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

```
AAA accounting udp/0 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

接下來，從位於192.1.1.1的外部路由器Telnet至虛擬IP 192.1.1.30，並向允許UDP通過PIX的虛擬地址進行身份驗證。在本範例中， **copy tftp flash**程式是從外部啟動到內部的：

```
302006: Teardown UDP connection for faddr 192.1.1.1/7680
    gaddr 192.1.1.30/69 laddr 10.31.1.5/69
```

對於PIX上的每個**copy tftp flash**（在此IOS複製期間有三個快閃記憶體），都會剪下記賬記錄並將其傳送到身份驗證伺服器。以下是Cisco Secure Windows上的TACACS記錄示例):

```
Date,Time,Username,Group-Name,Caller-Id,Acct-Flags,elapsed_time,
    service,bytes_in,bytes_out,paks_in,paks_out,
    task_id,addr,NAS-Portname,NAS-IP-Address,cmd
 04/28/2000,03:08:26,pixuser,Default Group,192.1.1.1,start,,,,,,,
    0x3c,,PIX,10.31.1.200,udp/69
```

相關資訊

- PIX命令參考
- PIX產品支援頁