通過PIX 5.2及更高版本執行使用者身份驗證、授權和記帳

目錄

簡介

RADIUS和TACACS+身份驗證可通過Cisco Secure PIX防火牆為FTP、Telnet和HTTP連線完成。對其他不太常用的協定的身份驗證通常能夠正常工作。支援TACACS+授權。不支援RADIUS授權。PIX 5.2身份驗證、授權和記帳(AAA)在早期版本上的更改包括AAA訪問清單支援，用於控制誰經過身份驗證，使用者訪問哪些資源。在PIX 5.3及更高版本中，身份驗證、授權和記帳(AAA)與早期代碼版本相比的變化是RADIUS埠是可配置的。

附註： PIX 6.x可以對通過流量進行記帳，但對目的地為PIX的流量則不進行記帳。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本檔案中的資訊是根據以下軟體版本：

- Cisco Secure PIX防火牆軟體版本5.2.0.205和5.2.0.207

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。

註：如果運行PIX/ASA軟體版本7.x及更高版本，請參閱配置AAA伺服器和本地資料庫**。**

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、授權及記帳

以下是驗證、授權和記帳的解釋：

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

- 記帳是使用者執行的操作。

使用者透過開啟驗證/授權看到的專案

當使用者嘗試從內部到外部（反之亦然）並且身份驗證/授權開啟時：

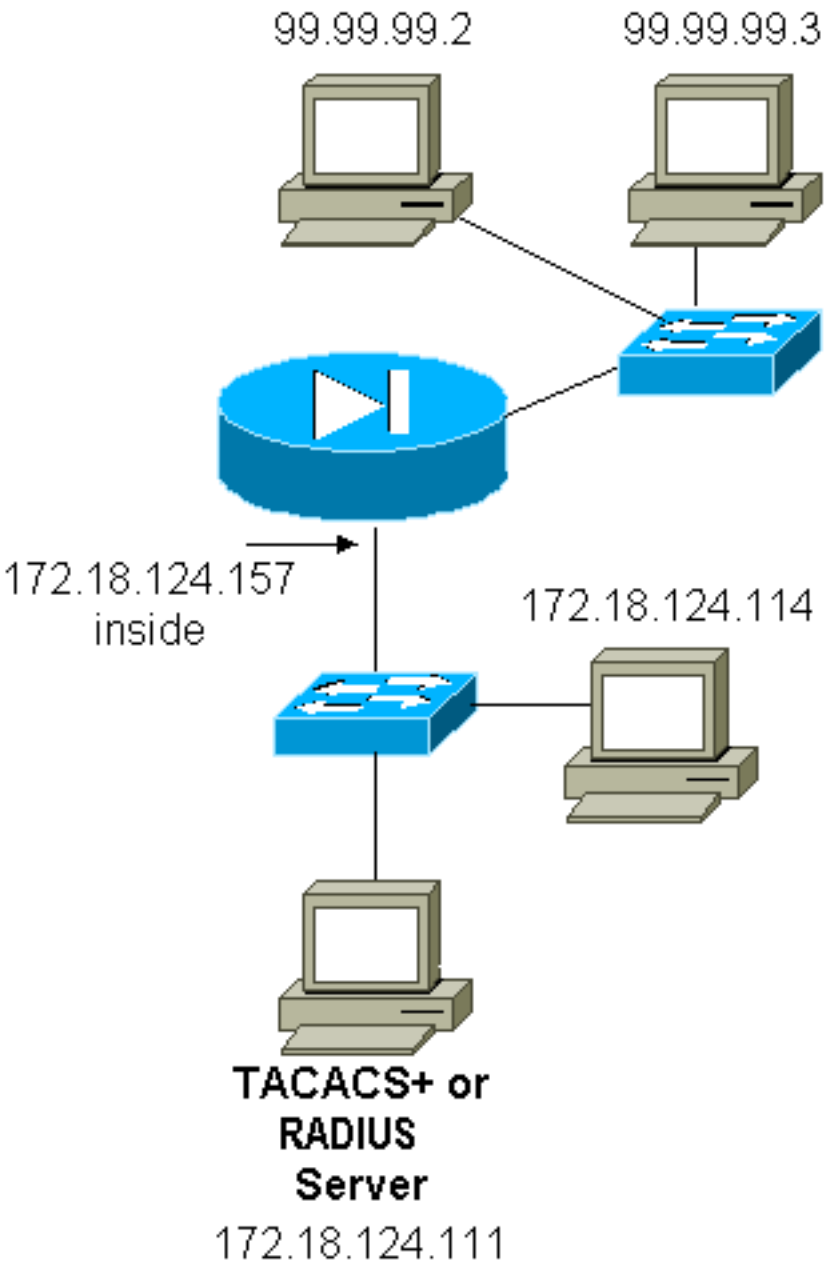
- **Telnet** — 使用者看到使用者名稱提示出現，然後請求密碼。如果在PIX/伺服器上成功進行身份驗證（和授權），則目標主機將提示使用者輸入使用者名稱和密碼。
- **FTP** — 使用者看到出現使用者名稱提示。使用者需要輸入「local_username@remote_username」作為使用者名稱，輸入「local_password@remote_password」作為密碼。PIX將「local_username」和「local_password」傳送到本地安全伺服器。如果在PIX/伺服器上成功進行身份驗證（和授權），則「remote_username」和「remote_password」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似乎應該使HTTP連線超時，但是沒有超時，則可能實際上通過瀏覽器「拍攝」快取的PIX使用者名稱和密碼來進行重新身份驗證。PIX將這個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「正常」工作，但HTTP連線不工作，這就是原因。

調試步驟

- 在新增AAA身份驗證和授權之前，請確保PIX配置工作正常。如果您在設定驗證和授權之前無法傳遞流量，則之後您將無法傳遞流量。
- 在PIX中啟用某種日誌記錄。發出**logging console debug**命令以啟用日誌記錄控制檯調試。**注意**：請勿在負載較重的系統上使用日誌控制檯調試。使用**logging monitor debug** 命令記錄Telnet作業階段。可以使用logging buffered debugging，然後執行**show logging**命令。日誌記錄還可以傳送到系統日誌伺服器並在那裡檢視。
- 開啟TACACS+或RADIUS伺服器的調試。

僅身份驗證

網路圖表



伺服器設定 — 僅身份驗證

Cisco Secure UNIX TACACS伺服器配置

```
User = cse {
password = clear "cse"
default service = permit
}
```

Cisco Secure UNIX RADIUS伺服器配置

附註： 藉助高級GUI，將PIX IP地址和金鑰新增到網路訪問伺服器(NAS)清單中。

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
```

```
}
reply_attributes= {
6=6
}
}
}
```

Cisco安全Windows RADIUS

使用以下步驟設定Cisco Secure Windows RADIUS伺服器。

1. 在**User Setup**部分獲取密碼。
2. 在**Group Setup**部分，將屬性6(Service-Type)設定為**Login**或**Administrative**。
3. 在GUI的**NAS配置**部分新增PIX IP地址。

Cisco安全Windows TACACS+

使用者在**User Setup**（使用者設定）**部分獲得**密碼。

Livingston RADIUS伺服器配置

附註： 將PIX IP地址和金鑰新增到*client*檔案。

- bill Password="foo" User-Service-Type = Shell-User

價值RADIUS伺服器配置

附註： 將PIX IP地址和金鑰新增到*client*檔案。

- bill Password="foo" Service-Type = Shell-User

TACACS+免費軟體伺服器配置

```
key = "cisco"
user = cse {
login = cleartext "cse"
default service = permit
}
```

PIX初始配置 — 僅身份驗證

PIX初始配置 — 僅身份驗證

```
PIX Version 5.2(0)205
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd OnTrBUG1Tp0edmkr encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
```

```
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
!
!--- These lines are necessary !--- if the new feature
in 5.2 is used to define which !--- target/source IP
addresses are to be authenticated. access-list 101
permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
!
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 99.99.99.1 255.255.255.0
ip address inside 172.18.124.157 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 99.99.99.10-99.99.99.20 netmask
255.255.255.0
nat (inside) 1 172.18.124.0 255.255.255.0 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
conduit permit udp any any
conduit permit icmp any any
route inside 172.18.0.0 255.255.0.0 172.18.124.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323 0:05:00
si p 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
!--- For the purposes of illustration, the TACACS+
process is used !--- to authenticate inbound users and
RADIUS is used to authenticate outbound users. aaa-
server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server AuthInbound protocol tacacs+
aaa-server AuthInbound (inside) host 172.18.124.111
cisco timeout 5
aaa-server AuthOutbound protocol radius
aaa-server AuthOutbound (inside) host 172.18.124.111
cisco timeout 5
!
```

```
!--- The next six statements are used to authenticate
all inbound !--- and outbound FTP, Telnet, and HTTP
traffic. aaa authentication include ftp outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include telnet outside 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http outside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthInbound
aaa authentication include http inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include telnet inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
aaa authentication include ftp inside 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0
   AuthOutbound
!
!--- OR the new 5.2 feature allows these two statements
in !--- conjunction with access-list 101 to replace the
previous six statements. !--- Note: Do not mix the old
and new verbiage.

aaa authentication match 101 outside AuthInbound
aaa authentication match 101 inside AuthOutbound
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
no sysopt route dnat
isakmp identity hostname
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:5882f514247589d784a0d74c800907b8
: end
```

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及更高版本中，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 #
```

PIX身份驗證調試示例

有關如何開啟調試的資訊，請參閱調試步驟。以下是位於99.99.99.2的使用者向172.18.124.114(99.99.99)內部發起流量的範例，反之亦然。傳入流量通過TACACS驗證，而傳出流量通過RADIUS驗證。

成功的身份驗證 — TACACS+（入站）

```
109001: Auth start for user '???' from 99.99.99.2/11003 to 172.18.124.114/23
109011: Authen Session Start: user 'cse', sid 2
109005: Authentication succeeded for user 'cse' from 172.18.124.114/23
  to 99.99. 99.2/11003 on interface outside
302001: Built inbound TCP connection 4 for faddr 99.99.99.2/11003
  gaddr 99.99.99 .99/23 laddr 172.18.124.114/23 (cse)
```

由於使用者名稱/密碼錯誤，身份驗證失敗 — TACACS+（入站）。 使用者看到「錯誤：超出最大嘗試次數。"

```
109001: Auth start for user '???' from 99.99.99.2/11004 to 172.18.1 24.114/23
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1004 on interface outside
```

伺服器無法與PIX通話 — TACACS+（入站）。 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）。 使用者看到「錯誤：超出最大嘗試次數。"

```
109001: Auth start for user '???' from 99.99.99.2/11005 to 172.18.124.114/23
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109002: Auth from 172.18.124.114/23 to 99.99.99.2/11005 failed
  (server 172.18.12 4.111 failed) on interface outside
109006: Authentication failed for user '' from 172.18.124.114/23
  to 99.99.99.2/1 1005 on interface outside
```

良好驗證 — RADIUS（傳出）

```
109001: Auth start for user '???' from 172.18.124.114/35931 to 99.99.99.2/23
109011: Authen Session Start: user 'bill', Sid 0
109005: Authentication succeeded for user 'bill' from 172.18.124.114/35931
  to 99 .99.99.2/23 on interface inside
```

身份驗證錯誤（使用者名稱或密碼） — RADIUS（出站）。 使用者看到使用者名稱請求，然後是密碼請求，有三種機會輸入這些資訊，如果失敗，請參閱「錯誤：超出最大嘗試次數。"

```
109001: Auth start for user '???' from 172.18.124.114/35932 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35932 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35932
  to 99.99.99. 2/23 on interface inside
```

伺服器ping但守護程式關閉、伺服器無法ping通，或者金鑰/客戶端不匹配 — 不會與PIX通訊 — RADIUS（出站）。 使用者先看到使用者名稱，再看到密碼，然後顯示「RADIUS伺服器失敗」，最後顯示「錯誤：超出最大嘗試次數。"

```
109001: Auth start for user '???' from 172.18.124.114/35933 to 99.99.99.2/23
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109002: Auth from 172.18.124.114/35933 to 99.99.99.2/23 failed
  (server 172.18.12 4.111 failed) on interface inside
109006: Authentication failed for user '' from 172.18.124.114/35933
  to 99.99.99. 2/23 on interface inside
```

驗證與授權

如果您希望允許所有經過身份驗證的使用者通過PIX執行所有操作（HTTP、FTP和Telnet），則身份驗證就足夠了，不需要授權。但是，如果您希望允許某些使用者的某些服務子集或限制使用者訪問某些站點，則需要授權。RADIUS授權對通過PIX的流量無效。在此案例中，TACACS+授權有效。

如果身份驗證通過，並且授權開啟，PIX會將使用者正在執行的命令傳送到伺服器。例如，「http 1.2.3.4」。 在PIX的5.2版中，TACACS+授權與存取清單結合使用，以控制使用者前往的位置。

如果要為HTTP（已訪問的網站）實施授權，請使用諸如Websense之類的軟體，因為單個網站可能有大量IP地址與其關聯。

伺服器設定 — 身份驗證和授權

Cisco Secure UNIX TACACS伺服器配置

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

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

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

Cisco安全Windows TACACS+

完成以下步驟以設定Cisco Secure Windows TACACS+伺服器。

1. 按一下組設定底部的**Deny unmatched IOS commands**。
2. 按一下「**Add/Edit New Command(FTP、HTTP、Telnet)**」。例如，如果要允許Telnet到特定站點(「telnet 1.2.3.4」)，命令是**telnet**。引數是*1.2.3.4*。填寫「command=**telnet**」後，在引數矩形中填寫「permit」IP地址（例如，「permit 1.2.3.4」）。 如果要允許所有Telnet，該命令仍為**telnet**，但按一下**Allow all unlisted arguments**。然後按一下**完成編輯命令**。
3. 對每個允許的命令（例如Telnet、HTTP和FTP）執行步驟2。

4. 藉助GUI在「NAS配置」部分新增PIX IP地址。

TACACS+免費軟體伺服器配置

```
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 .*
   }
   }
```

PIX配置 — 新增授權

新增需要授權的命令：

```
aaa authorization include telnet outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include http outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include ftp outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
```

新的5.2功能允許此語句與先前定義的訪問清單101一起替換先前的三個語句。新舊措辭不應混為一談。

```
aaa authorization match 101 outside AuthInbound
```

PIX身份驗證和授權調試示例

身份驗證和授權成功 — TACACS+

```
 109001: Auth start for user '???' from
    99.99.99.2/11010 to 172.18.124.114/23
 109011: Authen Session Start: user 'cse', Sid 3
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/23 to 99.99.99.2/11010
    on interface outside
```

```
109011: Authen Session Start: user 'cse', Sid 3
109007: Authorization permitted for user 'cse'
   from 99.99.99.2/11010 to 172.18.1  24.114/23
   on interface outside
302001: Built inbound TCP connection 2 for faddr
   99.99.99.2/11010 gaddr 99.99.99.99/23 laddr
   172.18.124.114/23 (cse)
```

身份驗證成功，但授權失敗 — TACACS+。使用者還會看到消息「錯誤：拒絕授權。"

```
109001: Auth start for user '???' from
   99.99.99.2/11011 to 172.18.124.114/23
109011: Authen Session Start: user 'httponly', Sid 4
109005: Authentication succeeded for user 'httponly'
   from 172.18.124.114/23 to  9 9.99.99.2/11011
   on interface outside
109008: Authorization denied for user 'httponly'
   from 172.18.124.114/23 to 99.99.99.2/11011
   on interface outside
```

新存取清單功能

在PIX軟體版本5.2及更高版本中，定義PIX上的訪問清單。根據伺服器上的使用者配置檔案逐個應用它們。TACACS+需要驗證和授權。RADIUS僅要求驗證。在本範例中，TACACS+的傳出驗證和授權已變更。在PIX上設定訪問清單。

注意：在PIX版本6.0.1及更高版本中，如果使用RADIUS，則通過在標準IETF RADIUS屬性11(Filter-Id)[CSCdt50422]中輸入該清單來實現訪問清單。在本例中，屬性11設定為115，而不是執行特定於供應商的「acl=115」措辭。

PIX配置

```
access-list 115 permit tcp any host 99.99.99.2 eq telnet
access-list 115 permit tcp any host 99.99.99.2 eq www
access-list 115 permit tcp any host 99.99.99.2 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq www
access-list 115 deny tcp any host 99.99.99.3 eq ftp
access-list 115 deny tcp any host 99.99.99.3 eq telnet
```

伺服器配置檔案

註：2.1版本的TACACS+免費軟體無法識別「acl」措辭。

Cisco Secure UNIX TACACS+伺服器配置

```
user = pixa{
  password = clear "********"
  service=shell {
  set acl=115
  }
  }
```

Cisco安全Windows TACACS+

為了向PIX新增授權以控制使用者使用訪問清單的位置，請選中**shell/exec**，選中**Access control list**框，並填寫數字（與PIX上的訪問清單編號匹配）。

Cisco安全UNIX RADIUS

```
user = pixa{
  password = clear "********"
  radius=Cisco {
  reply_attributes= {
  9,1="acl=115"
  }
  }
  }
```

Cisco安全Windows RADIUS

RADIUS/Cisco是裝置型別。在Cisco/RADIUS矩形框中，「pixa」使用者需要使用者名稱、密碼、檢查和「acl=115」，其中顯示009\001 AV配對（特定於供應商）。

輸出

配置檔案中具有「acl=115」的出站使用者「pixa」驗證和授權。伺服器將acl=115傳遞到PIX，PIX將顯示以下資訊：

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          2
user 'pixa' at 172.18.124.114, authenticated
   access-list 115
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

使用者「pixa」嘗試前往99.99.99.3（或除99.99.99.2以外的任何IP位址，因為存在隱含的deny）時，使用者會看到以下情況：

```
Error: acl authorization denied
```

6.2版新的按使用者可下載訪問清單

在PIX防火牆的軟體版本6.2及更高版本中，訪問控制伺服器(ACS)上定義訪問清單，以便在身份驗證後下載到PIX。這僅適用於RADIUS通訊協定。無需在PIX本身上配置訪問清單。組模板應用於多個使用者。

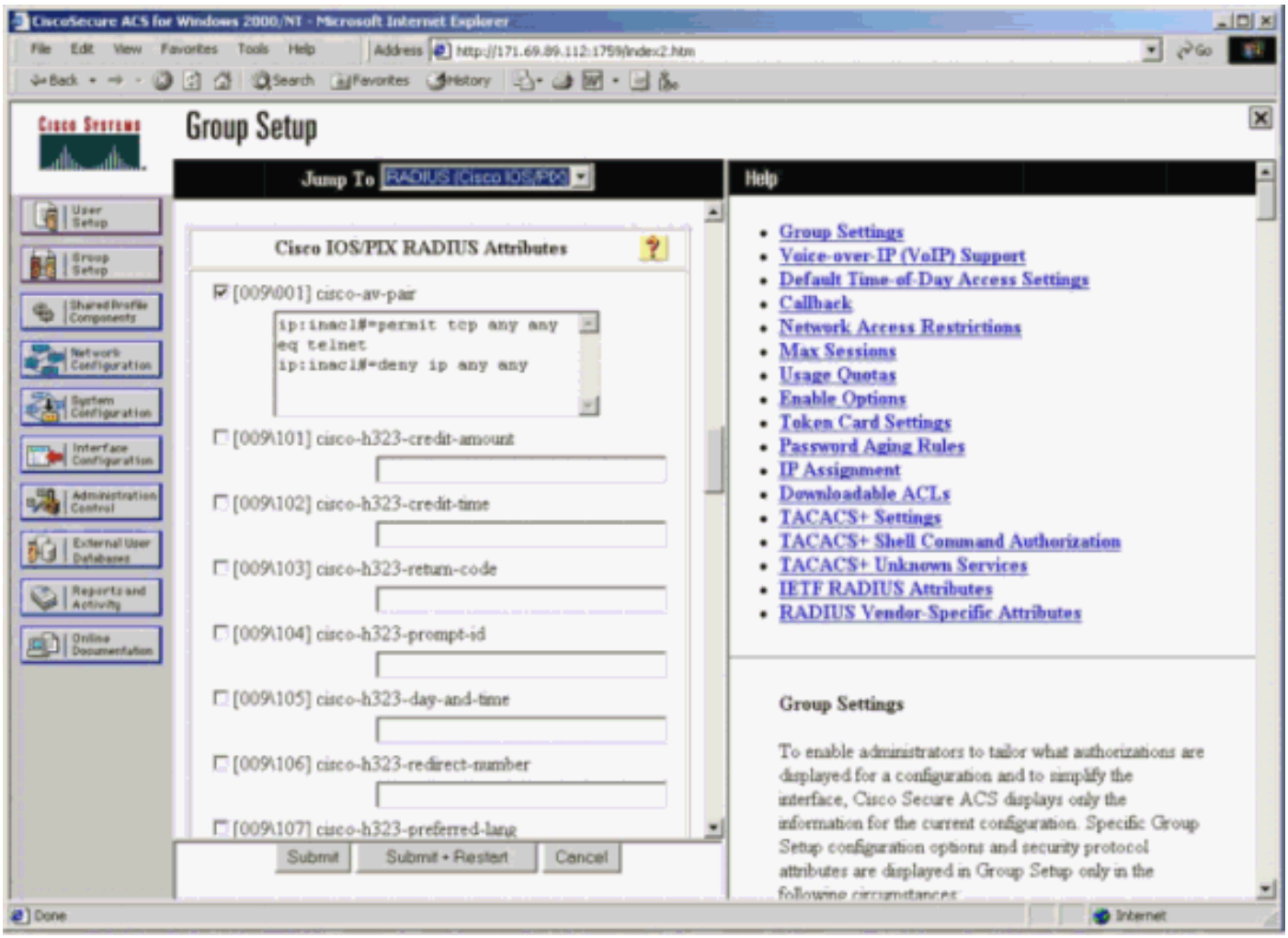
在早期版本中，訪問清單是在PIX上定義的。身份驗證後，ACS將訪問清單名稱推送到PIX。新版本允許ACS將訪問清單直接推送到PIX。

注意：如果發生故障轉移，則不會複製uauth表使用者將重新進行身份驗證。再次下載訪問清單。

ACS設定

按一下**Group Setup**並選擇**RADIUS(Cisco IOS/PIX)裝置**型別以設定使用者帳戶。為使用者分配使用者名稱（在本例中為「cse」）和密碼。從「屬性」清單中，選擇配置**[009\001]** ***vendor-av-pair*****的選**

項。定義訪問清單，如以下示例所示：



PIX調試：有效身份驗證和下載的訪問清單

- 僅允許Telnet並拒絕其他流量。

```
pix# 305011: Built dynamic TCP translation from inside:
  172.16.171.33/11063 to outside:172.16.171.201/1049
109001: Auth start for user '???' from 172.16.171.33/11063
   to 172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11063
   to 172.16.171.202/23 on interface inside

302013: Built outbound TCP connection 123 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11063 (172.16.171.201/1049) (cse)
```

show uauth命令的輸出。

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

show access-list命令的輸出。

```
pix#show access-list
access-list AAA-user-cse; 2 elements
```

```
access-list AAA-user-cse permit tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse deny ip any any (hitcnt=0)
```

- 僅拒絕Telnet並允許其他流量。

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11064 to outside:172.16.171.201/1050
109001: Auth start for user '???' from 172.16.171.33/11064 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 11
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11064
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl= AAA-user-cse) for user 'cse'
  from 172.16.171.33/11064 to 172.16.171.202/23 on interface inside
```

show uauth命令的輸出。

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list AAA-user-cse
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
```

show access-list命令的輸出。

```
pix#show access-list
access-list AAA-user-cse; 2 elements
access-list AAA-user-cse deny tcp any any eq telnet (hitcnt=1)
access-list AAA-user-cse permit ip any any (hitcnt=0)
```

使用ACS 3.0新建每使用者可下載訪問清單

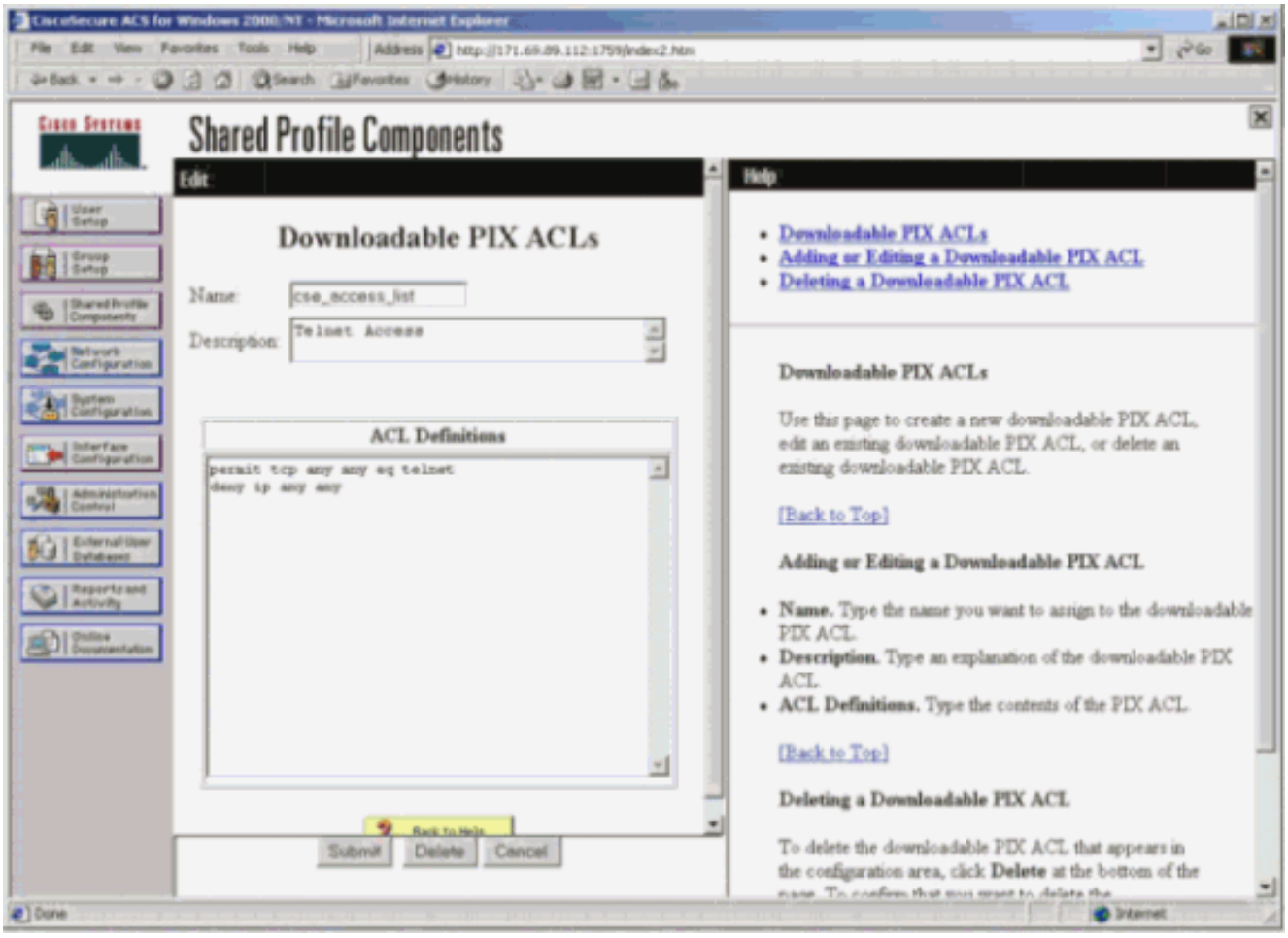
在ACS版本3.0中，共用配置檔案元件允許使用者建立訪問清單模板並為特定使用者或組定義模板名稱。模板名稱可以與所需數量的使用者或組一起使用。這樣就無需為每個使用者配置相同的訪問清單。

注意：如果發生故障轉移，則uauth不會複製到輔助PIX。在狀態故障切換中，會話是持續的。但是，必須重新驗證新連線，並再次下載訪問清單。

使用共用配置檔案

使用共用配置檔案時，請完成以下步驟。

1. 按一下「Interface Configuration」。
2. 檢查**使用者級可下載ACL**和/或**組級可下載ACL**。
3. 按一下Shared Profile Components。按一下「User-Level Downloadable ACLs」。
4. 定義可下載ACL。
5. 按一下Group Setup。在Downloadable ACLs下，將PIX訪問清單分配到之前建立的訪問清單。



PIX調試：使用共用配置檔案的有效身份驗證和下載的訪問清單

- 僅允許Telnet並拒絕其他流量。

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11065 to outside:172.16.171.201/1051
109001: Auth start for user '???' from 172.16.171.33/11065 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 12
109005: Authentication succeeded for user 'cse' from
   172.16.171.33/11065 to 172.16.171.202/23 on interface inside
302013: Built outbound TCP connection 124 for outside:
   172.16.171.202/23 (172.16.171.202/23) to inside:
   172.16.171.33/11065 (172.16.171.201/1051) (cse)
```

show uauth命令的輸出。

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
pix#
```

show access-list命令的輸出。

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   permit tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1bb3
   deny ip any any (hitcnt=0)
```

```
pix# 111009: User 'enable_15' executed cmd: show access-list
```

- 僅拒絕Telnet並允許其他流量。

```
pix# 305011: Built dynamic TCP translation from inside:
   172.16.171.33/11066 to outside:172.16.171.201/1052
109001: Auth start for user '???' from 172.16.171.33/11066 to
   172.16.171.202/23
109011: Authen Session Start: user 'cse', sid 13
109005: Authentication succeeded for user 'cse'
   from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
109015: Authorization denied (acl=#ACSACL#-PIX-cse_access_list-3cff1dd6)
   for user 'cse' from 172.16.171.33/11066
   to 172.16.171.202/23 on interface inside
```

show uauth命令的輸出。

```
pix#show uauth
Current Most Seen
Authenticated Users 1 1
Authen In Progress 0 1
user 'cse' at 172.16.171.33, authenticated
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
absolute timeout: 0:05:00
inactivity timeout: 0:00:00
pix# 111009: User 'enable_15' executed cmd: show uauth
```

show access-list命令的輸出。

```
pix#show access-list
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6; 2 elements
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   deny tcp any any eq telnet (hitcnt=1)
access-list #ACSACL#-PIX-cse_access_list-3cff1dd6
   permit ip any any (hitcnt=0)
pix# 111009: User 'enable_15' executed cmd: show access-listpix#
```

新增記帳

PIX配置 — 新增記帳

TACACS(AuthInbound=tacacs)

新增此命令。

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthInbound
```

或者，使用5.2中的新功能定義訪問清單要計算的內容。

```
aaa accounting match 101 outside AuthInbound
```

注意：訪問清單101是單獨定義的。

RADIUS(AuthOutbound=radius)

新增此命令。

```
aaa accounting include any inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound
```

或者，使用5.2中的新功能定義訪問清單要計算的內容。

```
aaa accounting match 101 outside AuthOutbound
```

注意：訪問清單101是單獨定義的。

注意：從PIX 7.0代碼開始，可以為PIX上的管理會話生成記帳記錄。

記帳示例

- TACACS說明從99.99.99.2 outside到172.18.124.114 inside(99.99.99)的Telnet例項。

```
172.18.124.157 pixuser PIX 99.99.99.2 start server=rtp-cherry
   time=10:36:16 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114 cmd=telnet
172.18.124.157 pixuser PIX 99.99.99.2 stop server=rtp-cherry
   time=10:37:50 date=08/23/2000 task_id=0x0 foreign_ip=99.99.99.2
   local_ip=172.18.124.114
   cmd=telnet elapsed_time=94 bytes_in=61 bytes_out=254
```

- 從172.18.124.114內部到99.99.99.2外部(Telnet)和99.99.99.3外部(HTTP)的連線的RADIUS記帳示例。

```
Sun Aug  6 03:59:28 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
        User-Name = cse
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 03:59:32 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000004
         Username = cse
        Acct-Session-Time = 4
        Acct-Input-Octets = 101
        Acct-Output-Octets = 143
        Vendor-Specific = Source-IP=172.18.124.114
        Vendor-Specific = Source-Port=35937
        Vendor-Specific = Destination-IP=99.99.99.2
        Vendor-Specific = Destination-Port=23

Sun Aug  6 04:05:02 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 172.18.124.157
        Login-IP-Host = 172.18.124.114
        Login-TCP-Port = 80
```

```
            Username = cse
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80

    Sun Aug  6 04:05:02 2000
            Acct-Status-Type = Stop
            NAS-IP-Address = 172.18.124.157
            Login-IP-Host = 172.18.124.114
            Login-TCP-Port = 80
            Acct-Session-Id = 0x0000000a
            Username = cse
            Acct-Session-Time = 0
            Acct-Input-Octets = 1277
            Acct-Output-Octets = 310
            Vendor-Specific = Source-IP=172.18.124.114
            Vendor-Specific = Source-Port=35949
            Vendor-Specific = Destination-IP=99.99.99.3
            Vendor-Specific = Destination-Port=80
```

使用exclude命令

在此網路中，如果您確定特定源或目標不需要身份驗證、授權或記帳，請發出以下命令。

```
aaa authentication exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa authorization exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
aaa accounting exclude telnet outside 172.18.124.114 255.255.255.255
  99.99.99.3 255.255.255.255 AuthInbound
```

附註： 您已經具有include命令。

```
aaa authentication|authorization|accounting include http|ftp|telnet
```

或者，使用5.2中的新功能，定義要排除的內容。

```
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq telnet
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq ftp
access-list 101 deny tcp host 99.99.99.3 host 172.18.124.114 eq www
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq ftp
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
aaa accounting match 101 outside AuthInbound
```

注意：如果您從驗證中排除一個框，並且您具有授權，則還必須從授權中排除該框。

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伺服器會假定該使用者仍然登入（即，使用者通過PIX具有會話）。 由於連線的性質，這非常適用於Telnet和FTP連線。但是，這並不適合HTTP。本範例中使用的是不同的網路組態，但概念是相同的。

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 171.68.118.100/1200 to 9.9.9.25/23
    (pix) 302001: Built TCP connection 5 for
        faddr 9.9.9.25/23 gaddr 9.9.9.10/1200 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，因此此時伺服器會顯示「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），並且此使用者的伺服器上的max-sessions設定為「1」（假定伺服器支援max-sessions），伺服器將拒絕該連線。使用者在目標主機上進行Telnet或FTP業務，然後退出（在此停留十分鐘）。

```
    (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（即每次進行身份驗證）還是更多（在uauth期間進行一次身份驗證），都會為每個訪問的站點剪下記帳記錄。

由於通訊協定的性質，HTTP的運作方式不同。以下是HTTP的示例，其中使用者通過PIX瀏覽從171.68.118.100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。開始記錄發佈時間為16:35:34，停止記錄發佈時間為16:35:35。此下載僅需一秒（即，開始記錄與停止記錄之間的間隔不到一秒）。 使用者未登入網站。使用者讀取網頁時未開啟連線。Max-sessions或view logged-in users在此不工作。這是因為HTTP中的連線時間（「建立」和「卸除」之間的時間）太短。「開始」和「停止」記錄是次秒級。沒有沒有「停止」記錄的「開始」記錄不存在，因為這些記錄實際上發生在同一時刻。無論是否將uauth設定為0或更大，仍會針對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。

使用者介面

更改提示使用者看到的內容

如果您有以下命令：

```
auth-prompt prompt PIX515B
```

然後使用者通過PIX看到此提示。

```
PIX515B
```

自定義使用者看到的消息

如果您有以下命令：

```
auth-prompt accept "GOOD_AUTHENTICATION"
auth-prompt reject "BAD_AUTHENTICATION"
```

然後，使用者會看到有關登入失敗/成功時身份驗證狀態的消息。

```
  PIX515B
  Username: junk
  Password:
  "BAD_AUTHENTICATION"

  PIX515B
  Username: cse
  Password:
  "GOOD_AUTHENTICATION"
```

每使用者空閒和絕對超時

PIX timeout uauth命令控制需要重新身份驗證的頻率。如果已開啟TACACS+驗證/授權，則會針對每個使用者進行控制。此使用者配置檔案設定為控制超時（在TACACS+免費軟體伺服器上，超時以分鐘為單位）。

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

驗證/授權後：

```
show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 99.99.99.3, authorized to:
   port 172.18.124.114/telnet
   absolute   timeout: 0:02:00
   inactivity timeout: 0:01:00
```

在兩分鐘結束時：

絕對逾時 — 作業階段關閉：

```
109012: Authen Session End: user 'cse', Sid 20, elapsed 122 seconds
302002: Teardown TCP connection 32 faddr 99.99.99.3/11025
   gaddr 99.99.99.99/23 l addr 172.18.124.114/23 duration 0:02:26
   bytes 7547 (TCP FINs)
```

虛擬HTTP出站

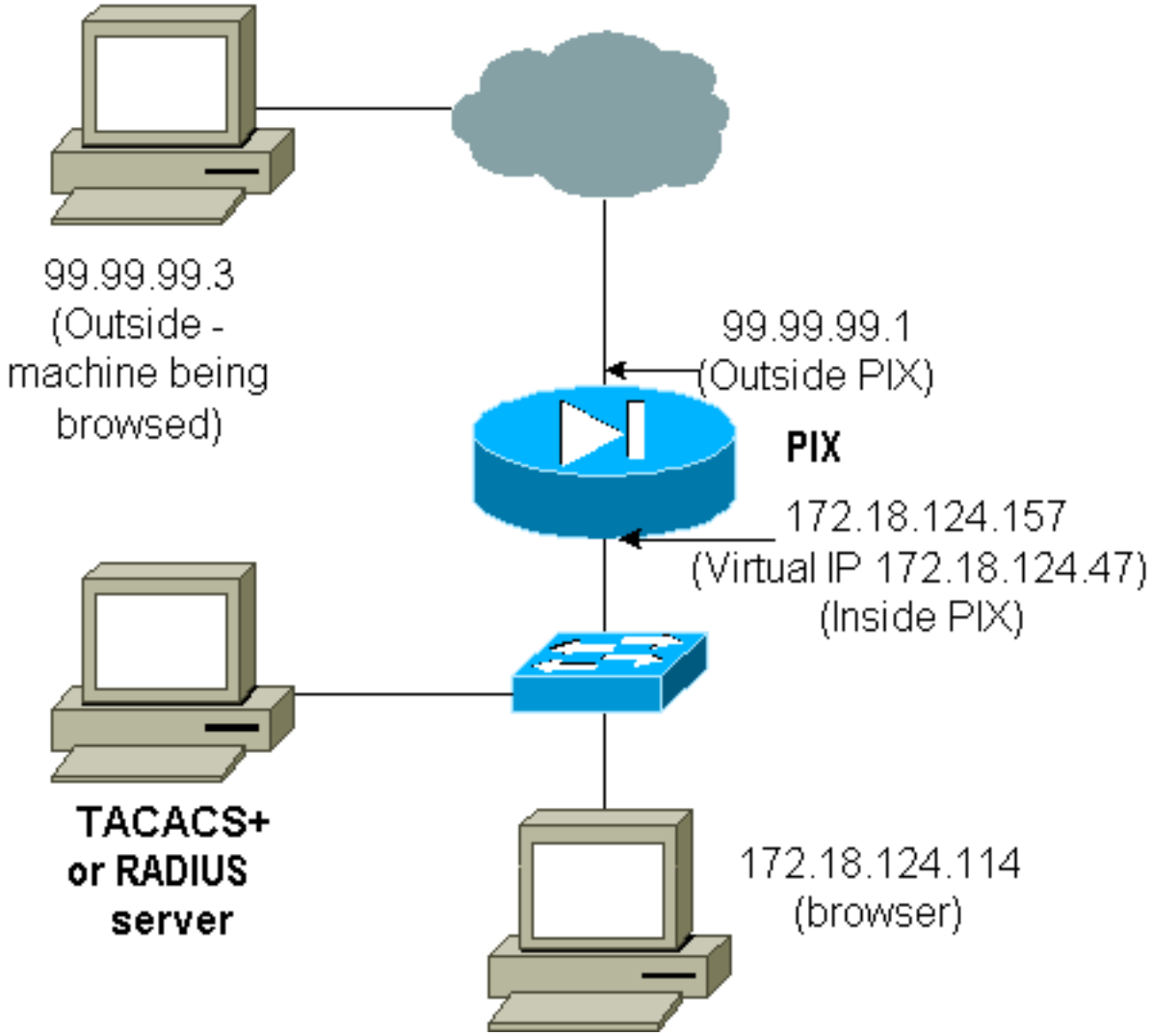
如果在PIX外部和PIX本身需要身份驗證，有時會觀察到異常的瀏覽器行為，因為瀏覽器會快取使用者名稱和密碼。

為了避免這種情況，請通過將RFC 1918 地址（在Internet上不可路由但對PIX內部網路有效且唯一的地址）以格式新增到PIX配置中來實施虛擬HTTP。

```
virtual http #.#.#.#
```

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。

注意：虛擬HTTP和虛擬Telnet IP地址必須包含在aaa身份驗證**語句**中。在本示例中，指定0.0.0.0確實包含這些地址。



在PIX配置中新增此命令。

```
virtual http 172.18.124.47
```

使用者將瀏覽器指向99.99.99.3。將顯示此消息。

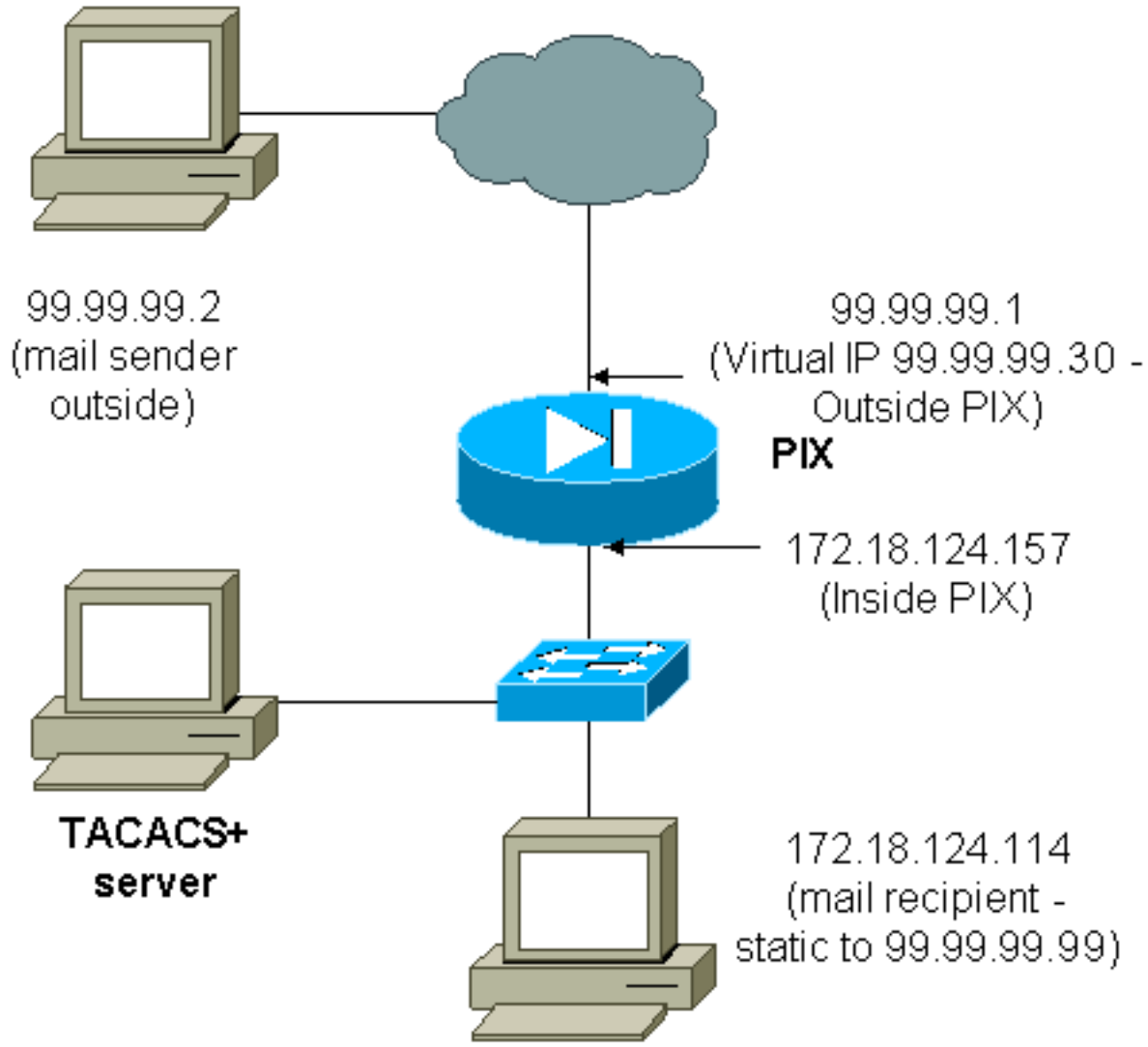
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

驗證後，流量將重新導向到99.99.99.3。

虛擬Telnet

注意：虛擬HTTP和虛擬Telnet IP地址必須包含在aaa身份驗證**語句**中。在本示例中，指定0.0.0.0確實包含這些地址。

虛擬Telnet傳入



對入站郵件進行身份驗證不是很好的主意，因為不會顯示要入站傳送的郵件的視窗。請改用**exclude**命令。但為了便於說明，新增了這些命令。

```
aaa authentication include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/25 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these !--- four statements to perform the same function. !---
Note: The old and new verbiage should not be mixed.

access-list 101 permit tcp any any eq smtp
!--- The "mail" was a Telnet to port 25. access-list 101 permit tcp any any eq telnet
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
!
!--- plus ! virtual telnet 99.99.99.30
static (inside,outside) 99.99.99.30 172.18.124.30
   netmask 255.255.255.255 0 0
static (inside,outside) 99.99.99.99 172.18.124.114
   netmask 255.255.255.255 0 0
conduit permit tcp host 99.99.99.30 eq telnet any
conduit permit tcp host 99.99.99.99 eq telnet any
conduit permit tcp host 99.99.99.99 eq smtp any
```

使用者（這是TACACS+免費軟體）：

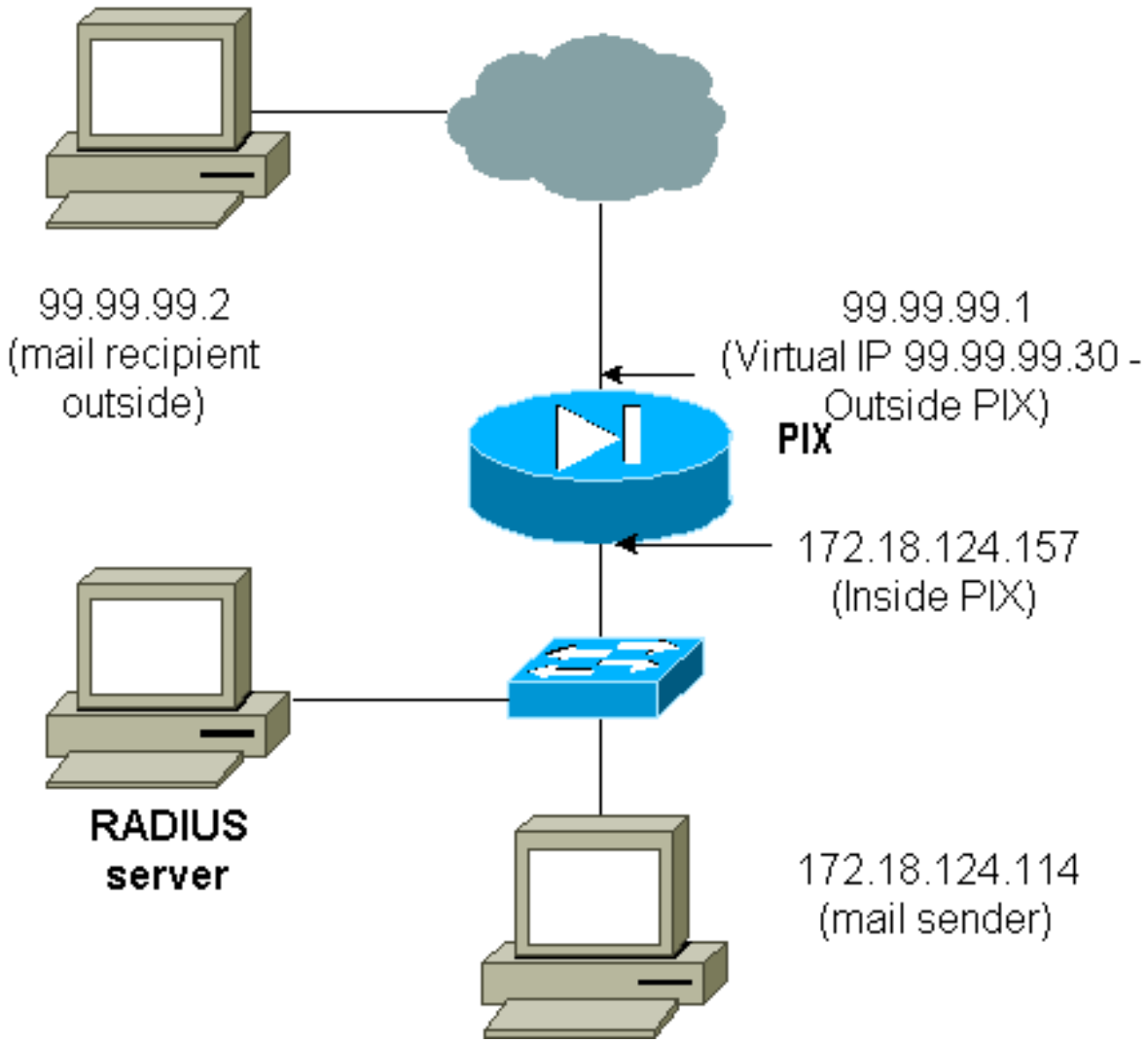
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


  user = pixuser {
  login = cleartext "pixuser"
  service = exec {
  }
  cmd = telnet {
  permit .*
  }
  }
```

如果僅啟用身份驗證，則兩個使用者在Telnet向IP地址99.99.99.30進行身份驗證後，傳送入站郵件。如果啟用了授權，則使用者「訪問」向99.99.99.30進行Telnet訪問，並輸入TACACS+使用者名稱/密碼。Telnet連線將會捨棄。然後，使用者「cse」將郵件傳送到99.99.99.99(172.18.124.114)。使用者「pixuser」的身份驗證成功。 但是，當PIX傳送對cmd=tcp/25和cmd-arg=172.18.124.114的授權請求時，請求將失敗，如以下輸出所示。

```
109001: Auth start for user '???' from
   99.99.99.2/11036 to 172.18.124.114/23
109005: Authentication succeeded for user
   'cse' from 172.18.124.114/23 to
   99.99.99.2/11036 on interface outside

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          1
Authen In Progress        0          1
user 'cse' at 99.99.99.2, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00

pixfirewall# 109001: Auth start for user '???' from
    99.99.99.2/11173 to 172.18.124.30/23
109011: Authen Session Start: user 'cse', sid 10
109005: Authentication succeeded for user 'cse' from 99.99.99.2/23
    to 172.18.124.30/11173 on interface outside
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11173
    to 172.18.124.30/23 on interface outside
109001: Auth start for user 'cse' from 99.99.99.2/11174 to
    172.18.124.114/25
109011: Authen Session Start: user 'cse', sid 10
109007: Authorization permitted for user 'cse' from 99.99.99.2/11174
    to 172.18.124.114/25 on interface outside
302001: Built inbound TCP connection 5 for faddr 99.99.99.2/11174
    gaddr 99.99.99.99/25 laddr 172.18.124.114/25 (cse)

pixfirewall# 109001: Auth start for user '???' from 99.99.99.2/11175
    to 172.18.124.30/23
109011: Authen Session Start: user 'pixuser', sid 11
109005: Authentication succeeded for user 'pixuser' from 99.99.99.2/23
    to 172.18.124.30/11175 on interface outside
109011: Authen Session Start: user 'pixuser', sid 11
109007: Authorization permitted for user 'pixuser' from 99.99.99.2/11175
    to 172.18.124.30/23 on interface outside
```

```
109001: Auth start for user 'pixuser' from 99.99.99.2/11176
    to 172.18.124.114/25
109008: Authorization denied for user 'pixuser' from 99.99.99.2/25
    to 172.18.124.114/11176 on interface outside
```

虛擬Telnet出站



對入站郵件進行身份驗證不是很好的主意，因為不會顯示要入站傳送的郵件的視窗。請改用**exclude**命令。但為了便於說明，新增了這些命令。

對出站郵件進行身份驗證不是個好主意，因為不會顯示要出站郵件的視窗。請改用**exclude**命令。但是為了便於說明，新增了這些命令。

```
aaa authentication include tcp/25 inside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthOutbound
!--- OR the new 5.2 feature allows these three statements !--- to replace the previous
statements. !--- Note: Do not mix the old and new verbiage.

access-list 101 permit tcp any any eq smtp
access-list 101 permit tcp any any eq telnet
aaa authentication match 101 inside AuthOutbound
!
!--- plus ! virtual telnet 99.99.99.30
!--- The IP address on the outside of PIX is not used for anything else.
```

若要將郵件從內部傳送到外部，請在郵件主機上開啟命令提示符，然後Telnet至99.99.99.30。這會

開啟郵件通過的漏洞。郵件從172.18.124.114傳送到99.99.99.2:

```
   305002: Translation built for gaddr 99.99.99.99
      to laddr 172.18.124.114
   109001: Auth start for user '???' from
      172.18.124.114/32860 to 99.99.99.30/23
   109011: Authen Session Start: user 'cse', Sid 14
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32860 to    99.99.99.30/23
      on interface inside
   302001: Built outbound TCP connection 22 for faddr
      99.99.99.2/25 gaddr 99.99.99.99/32861
      laddr 172.18.124.114/32861 (cse)

pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

虛擬Telnet註銷

當使用者通過Telnet連線至虛擬Telnet IP位址時，**show uauth**指令會顯示開啟洞穴的時間。如果使用者希望在其會話完成後（時間仍停留在uauth中）阻止流量通過，則需要再次通過Telnet訪問虛擬Telnet IP地址。這會關閉作業階段。本示例說明了這一點。

第一個身份驗證

```
 109001: Auth start for user '???'
    from 172.18.124.114/32862 to 99.99.99.30/23
 109011: Authen Session Start: user 'cse', Sid 15
 109005: Authentication succeeded for user
    'cse' from 172.18.124.114/32862 to
    99.99.99.30/23 on interface inside
```

第一次驗證後

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       1          2
Authen In Progress        0          1
user 'cse' at 172.18.124.114, authenticated
   absolute   timeout: 0:05:00
   inactivity timeout: 0:00:00
```

第二次身份驗證

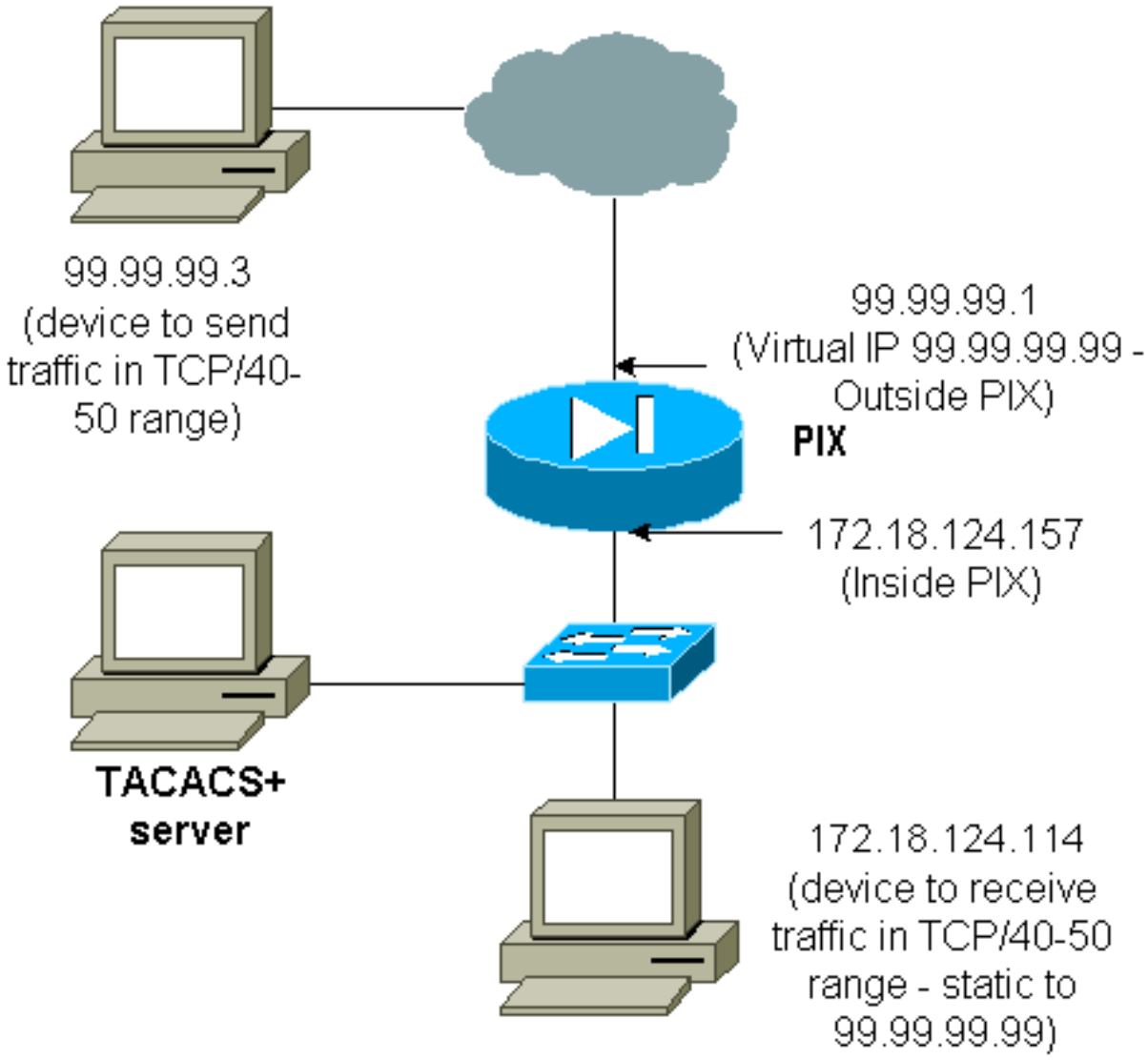
```
   pixfirewall# 109001: Auth start for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
      on interface inside
```

第二次身份驗證之後

```
pixfirewall#show uauth
                        Current    Most Seen
Authenticated Users       0          2
Authen In Progress        0          1
```

連線埠授權

網路圖表



允許對埠範圍進行授權。如果在PIX上配置了虛擬Telnet，並且為一系列埠配置了授權，則使用者使用虛擬Telnet開啟該孔。然後，如果某個埠範圍的授權開啟，且該範圍內的流量命中PIX，則PIX會將命令傳送到TACACS+伺服器以進行授權。此範例顯示連線埠範圍上的傳入授權。

```
aaa authentication include any outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
aaa authorization include tcp/40-50 outside 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   AuthInbound
!--- OR the new 5.2 feature allows these three statements !--- to perform the same function as
the previous two statements. !--- Note: The old and new verbiage should not be mixed.

access-list 116 permit tcp any any range 40 50
aaa authentication match 116 outside AuthInbound
aaa authorization match 116 outside AuthInbound
```

```
!
!--- plus ! static (inside,outside) 99.99.99.99 172.18.124.114
netmask 255.255.255.255 0 0
conduit permit tcp any any
virtual telnet 99.99.99.99
```

TACACS+伺服器配置示例（免費軟體）：

```
  user = cse {
  login = cleartext "numeric"
  cmd = tcp/40-50 {
  permit 172.18.124.114
  }
  }
```

使用者必須首先Telnet到虛擬IP地址99.99.99。身份驗證後，當使用者嘗試通過PIX推送埠40-50範圍內的TCP流量到99.99.99.99(172.18.124.114)時，cmd=tcp/40-50將傳送到TACACS+伺服器，其命令是cmd-arg=172.18.124.114，如下所示：

```
109001: Auth start for user '???' from 99.99.99.3/11075
    to 172.18.124.114/23
109011: Authen Session Start: user 'cse', Sid 13
109005: Authentication succeeded for user 'cse'
    from 172.18.124.114/23 to 99.99.99.3/11075
    on interface outside
109001: Auth start for user 'cse' from 99.99.99.3/11077
    to 172.18.124.114/49
109011: Authen Session Start: user 'cse', Sid 13
109007: Authorization permitted for user 'cse'
    from 99.99.99.3/11077 to 172.18.124.114/49
    on interface outside
```

除HTTP、FTP和Telnet以外的流量的AAA記帳

確保虛擬Telnet的工作方式是允許TCP/40-50流量到達網路內部的主機後，請使用以下命令為此流量新增記帳。

```
aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
!--- OR the new 5.2 feature allows these !--- two statements to replace the previous statement.
!--- Note: Do not mix the old and new verbiage.

aaa accounting match 116 outside AuthInbound
access-list 116 permit ip any any
```

TACACS+記帳記錄範例

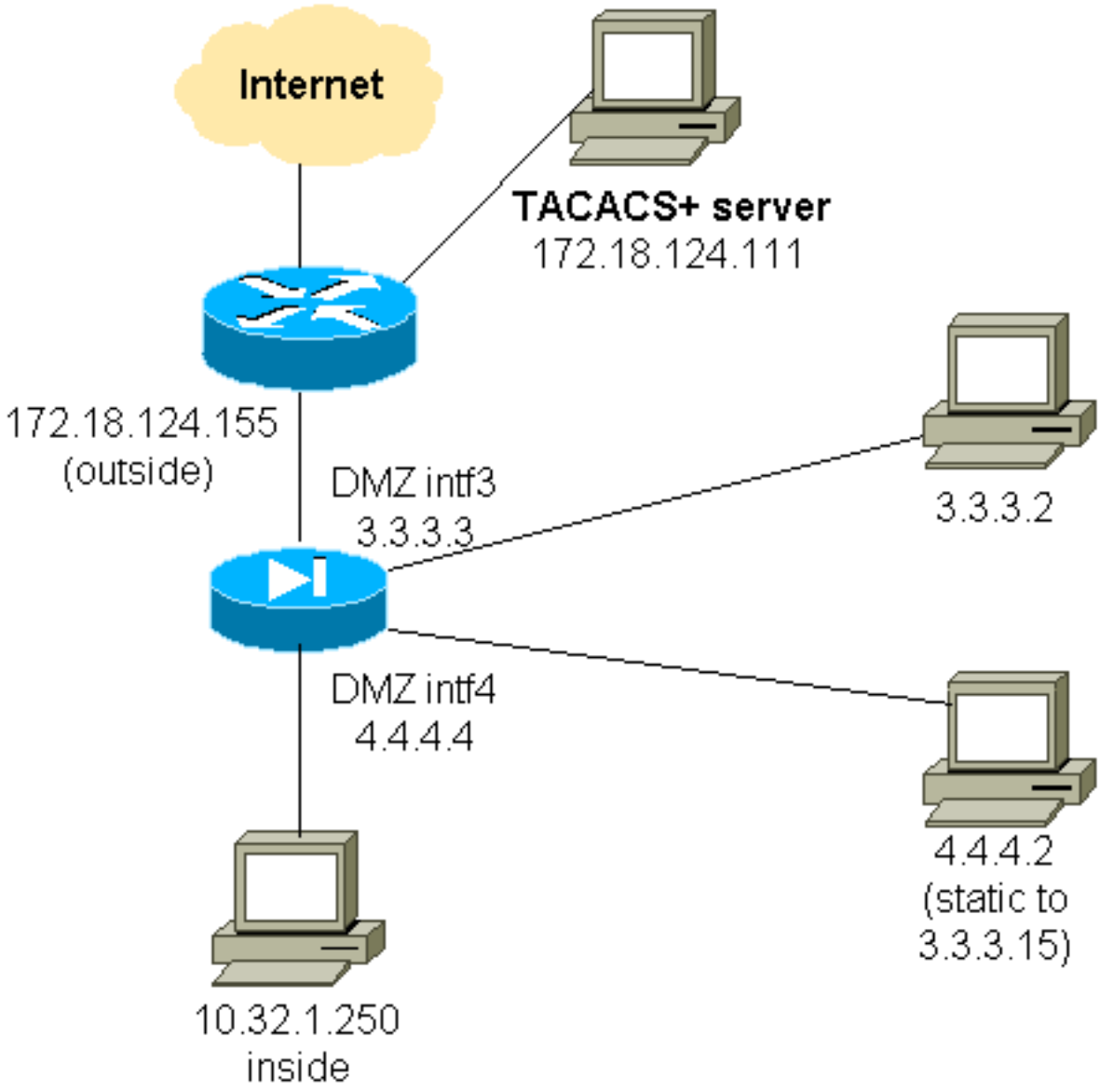
```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
   stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50 elapsed_time=8 bytes_in=80 bytes_out=101
```

DMZ上的身份驗證

為了對從一個DMZ介面到另一個介面的使用者進行身份驗證，請告知PIX對指定介面的流量進行身份驗證。在PIX上，安排如下：

```
least secure
PIX outside (security0) = 172.18.124.155
pix/intf3 (DMZ - security15) = 3.3.3.3 & device 3.3.3.2
pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2 (static to 3.3.3.15)
PIX inside (security100) = 10.32.1.250
most secure
```

網路圖表



部分PIX配置

驗證pix/intf3和pix/intf4之間的Telnet流量，如此處所示。

部分PIX配置
nameif ethernet0 outside security0 nameif ethernet1 inside security100 (nameif ethernet2 pix/intf2 security10) nameif ethernet3 pix/intf3 security15

```
  nameif ethernet4 pix/intf4 security20
  (nameif ethernet5 pix/intf5 security25)
  interface ethernet0 auto
  interface ethernet1 auto
  (interface ethernet2 auto shutdown)
  interface ethernet3 auto
  interface ethernet4 auto
  (interface ethernet5 auto shutdown)
  ip address outside 172.18.124.155 255.255.255.0
  ip address inside 10.32.1.250 255.255.255.0
  ip address pix/intf3 3.3.3.3 255.255.255.0
  ip address pix/intf4 4.4.4.4 255.255.255.0
  static (pix/intf4,pix/intf3) 3.3.3.15 4.4.4.2 netmask
255.255.255.255 0 0
  conduit permit tcp host 3.3.3.15 host 3.3.3.2
  aaa-server xway protocol tacacs+
  aaa-server xway (outside) host 172.18.124.111 timeout
5
  aaa authentication include telnet pix/intf4 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
  aaa authentication include telnet pix/intf3 4.4.4.0
255.255.255.0 3.3.3.0
  255.255.255.0 3.3.3.0 255.255.255.0 xway
!--- OR the new 5.2 feature allows these four statements
!--- to replace the previous two statements. !--- Note:
Do not mix the old and new verbiage.

  access-list 103 permit tcp 3.3.3.0 255.255.255.0
4.4.4.0 255.255.255.0 eq telnet
  access-list 104 permit tcp 4.4.4.0 255.255.255.0
3.3.3.0 255.255.255.0 eq telnet
  aaa authentication match 103 pix/intf3 xway
  aaa authentication match 104 pix/intf4 xway
```

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，並且希望向Cisco TAC提交案例，請確保提供此資訊以排除PIX防火牆故障。

- 問題描述和相關拓撲詳細資訊
- 開啟案例之前先進行疑難排解
- 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）

將收集的資料以非壓縮純文字檔案格式(.txt)附加到您的案例。 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，請將電子郵件附件中的資訊傳送到attach@cisco.com，並將您的案件編號填寫在郵件主題行。

相關資訊

- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 思科安全存取控制伺服器（Windows專用）
- Cisco Secure Access Control Server for UNIX
- 終端存取控制器存取控制系統(TACACS+)
- 遠端驗證撥入使用者服務(RADIUS)
- 技術支援與文件 - Cisco Systems