# 在 PIX 5.2 及更高版本中执行用户身份验证、授权和记账

## 目录

# 简介

RADIUS和TACACS+身份验证可通过Cisco Secure PIX防火墙对FTP、Telnet和HTTP连接进行。对其他较不常见协议的身份验证通常都要工作。支持TACACS+授权。不支持RADIUS授权。PIX 5.2身份验证、授权和记帐(AAA)在早期版本中的更改包括AAA访问列表支持，以控制身份验证对象和用户访问的资源。在PIX 5.3及更高版本中，与早期版本的代码相比，身份验证、授权和记帐(AAA)更改是RADIUS端口是可配置的。

**注意：** PIX 6.x可以对通过的流量进行记帐，但不能对流向PIX的流量进行记帐。

# 先决条件

## 要求

本文档没有任何特定的前提条件。

## 使用的组件

本文档中的信息基于以下软件版本：

- 思科安全PIX防火墙软件版本5.2.0.205和5.2.0.207

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

**注：如**果运行PIX/ASA软件版本7.x及更高版本，请参阅配置AAA服务器和本地数据库。

## 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

## 验证、授权和记帐

以下是身份验证、授权和记帐的说明：

- 认证就是用户是谁。
- 授权是用户的操作。
- 没有授权的身份验证是有效的。
- 没有身份验证的授权是无效的。

- 记帐是用户所做的。

## 开启验证/授权时用户看到的信息

当用户尝试在以下位置进行身份验证/授权时从内部到外部（反之亦然）：

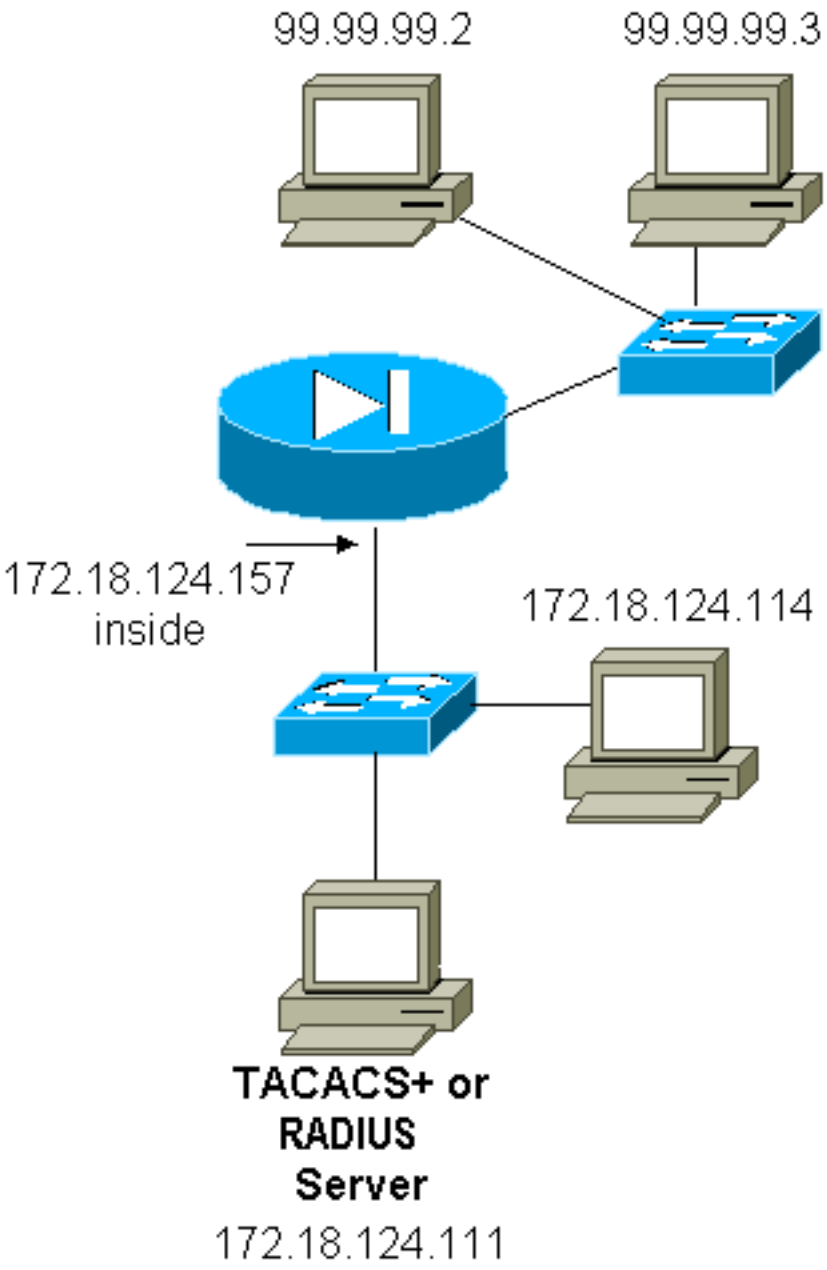
- **Telnet** — 用户看到出现用户名提示，然后出现密码请求。如果PIX/服务器上的认证（授权）成功，目的地主机将提示用户输入用户名和密码。
- **FTP** — 用户看到用户名提示出现。用户需要输入“local_username@remote_username” 为用户名和“local_password@remote_password的”为密码。PIX将“local_username”和“local_password”发送到本地安全服务器。如果PIX/服务器上的身份验证（和授权）成功，则“remote_username”和“remote_password”会传递到外部的目标FTP服务器。
- **HTTP** — 在请求用户名和密码的浏览器中显示一个窗口。如果认证(和授权)成功，用户将能访问上面的目的网站。请记住，*浏览器会缓存用户名和口令*。如果PIX似乎应超时HTTP连接，但不超时，则很可能会通过浏览器将缓存的用户名和密码“打开”到PIX，来实际进行重新身份验证。PIX将此转发到身份验证服务器。PIX系统日志和/或服务器调试显示了此现象。如果Telnet和FTP似乎“正常”工作，但HTTP连接不正常，这就是原因。

## 调试步骤

- 在添加AAA身份验证和授权之前，请确保PIX配置工作正常。如果在启动身份验证和授权之前无法传递流量，则以后无法传递。
- 在PIX中启用某种日志记录。发出**logging console debug**命令以打开日志记录控制台调试。**注意**：请勿在负载较重的系统上使用日志记录控制台调试。使用logging monitor **debug命**令记录Telnet会话。可以使用日志记录缓冲调试，然后执**行show logging** 命令。日志记录也可以发送到系统日志服务器并在那里进行检查。
- 在TACACS+或RADIUS服务器上启用调试。

# 只有认证

## 网络图




## 服务器设置- 仅认证

### 思科安全UNIX TACACS服务器配置

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

### 思科安全UNIX RADIUS服务器配置

**注意：** 在高级GUI的帮助下，将PIX IP地址和密钥添加到网络接入服务器(NAS)列表。

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

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

### 思科安全Windows RADIUS

使用以下步骤设置Cisco Secure Windows RADIUS服务器。

1. 在“用户设置”部**分中获**取密码。
2. 从“组**设置”**部分，将属性6（服务类型）设置为“登录”**或“管理”**。
3. 在GUI的“NAS配置”部**分添**加PIX IP地址。

### 思科安全Windows TACACS+

用户在“用户设置”部分**获取密**码。

### Livingston RADIUS 服务器配置

**注意：** 将PIX IP地址和密钥添加到客*户端*文件。

- bill password="foo"用户 — 服务 — 类型=外壳 — 用户

### Merit RADIUS 服务器配置

**注意：** 将PIX IP地址和密钥添加到客*户端*文件。

- bill password="foo"服务类型=外壳用户

### TACACS+ 免费软件服务器配置

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

### PIX初始配置 — 仅身份验证

**PIX初始配置 — 仅身份验证**

```
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 RADIUS 端口（5.3 和更高版本）

某些 RADIUS 服务器使用除 1645/1646 之外的 RADIUS 端口（通常为 1812/1813）。 在PIX 5.3及更高版本中，可使用以下命令将RADIUS身份验证和记帐端口更改为默认1645/1646以外的端口：

```
aaa-server radius-authport #
aaa-server radius-acctport #
```

## PIX 认证Debug示例

有关如何打开调试的信息，请参阅调试步骤。以下是99.99.99.2用户发起到172.18.124.114(99.99.99)内部流量的示例，反之亦然。入站流量通过TACACS身份验证，出站流量通过RADIUS身份验证。

### 身份验证成功 — 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)
```

由于用户名/密码错误，身份验证失败 — TACACS+（入站）。 用户看到“Error:已超出最大尝试次数。”

```
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
```

服务器不与PIX通话 — TACACS+（入站）。 用户看见一次用户名，PIX从未请求密码(远程登陆密码)。 用户看到“错误：已超出最大尝试次数。”

```
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
```

良好的身份验证 — RADIUS（出站）

```
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
```

身份验证错误（用户名或密码）— RADIUS（出站）。 用户看到用户名请求，然后看到密码，有三个机会输入这些，如果失败，请参阅“错误：已超出最大尝试次数。”

```
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
```

服务器可ping通，但daemon程序中断，服务器不可ping通，或密匙/客户端不匹配，都不能与PIX-RADIUS (向外)接通。 用户看到用户名，然后看到密码，然后看到“RADIUS服务器发生故障”，最后看到“错误：已超出最大尝试次数。”

```
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
```

# 认证和授权

如果要允许所有经过身份验证的用户通过PIX执行所有操作（HTTP、FTP和Telnet），则身份验证已足够，无需授权。但是，如果要允许某些服务子集访问特定用户或限制用户访问特定站点，则需要授权。RADIUS授权对通过PIX的流量无效。TACACS+授权在本例中有效。

如果身份验证通过且授权已启用，PIX会向服务器发送用户正在执行的命令。例如，“http 1.2.3.4”。在PIX版本5.2中，TACACS+授权与访问列表一起使用，以控制用户的去向。

如果要对HTTP（访问的网站）实施授权，请使用Websense等软件，因为单个网站可能具有大量与其关联的IP地址。

## 服务器设置- 认证和授权

### 思科安全UNIX TACACS服务器配置

```
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 .*
}
}
}
```

### 思科安全Windows TACACS+

完成以下步骤以设置Cisco Secure Windows TACACS+服务器。

1. 单击**Deny unmatched IOS命令**在Group Setup（组设置）底部。
2. 单击**Add/Edit New Command(FTP、HTTP、Telnet)**。例如，如果要允许Telnet到特定站点（“telnet 1.2.3.4”），则命令为**telnet**。参数为*1.2.3.4*。在填写"command=telnet"之后，在"Argument"方框内填写"petmit" +IP地址(例如，permit 1.2.3.4")。 如果允许所有远程登录，命令仍然是telnet，但单击Allow，则允许所有未列出的参数。然后单击“完**成编辑”命**令。
3. 执行每一个允许命令(例如Telnet、HTTP和FTP)的第二步操作。
4. 在GUI的帮助下，在“NAS配置”部分添加PIX IP地址。

## TACACS+ 免费软件服务器配置

```
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- 添加授权

添加命令以要求授权：

```
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功能允许此语句与先前定义的访问列表101一起替换前三个语句。新旧语言不应混为一谈。

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

## PIX 认证和授权Debug示例

### 良好的身份验证和授权成功 — 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)
```

### 身份验证良好，但授权失败 — TACACS+。用户还看到消息“Error:授权被拒绝。”

```
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
```

## 新的访问列表功能

在PIX软件版本5.2及更高版本中，定义PIX上的访问列表。根据服务器上的用户配置文件按用户应用这些配置。TACACS+需要身份验证和授权。RADIUS仅需要身份验证。在本示例中，对TACACS+的出站身份验证和授权已更改。在PIX上设置访问列表。

**注意**：在PIX版本6.0.1及更高版本中，如果使用RADIUS，则访问列表通过在标准IETF RADIUS属性11(Filter-Id)[CSCdt50422]中输入列表来实现。在本示例中，属性11设置为115，而不是执行供应商特定的“acl=115”语法。

## 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
```

## 服务器配置文件

**注意**：TACACS+免费软件的2.1版无法识别“acl”语法。

### 思科安全UNIX TACACS+服务器配置

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

### 思科安全Windows TACACS+

要向PIX添加授权以控制用户访问访问列表的位置，请选中**shell/exec**，选中**访问控制列表**框，并填写该号码（与PIX上的访问列表编号匹配）。

## Cisco Secure UNIX RADIUS

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

## 思科安全Windows RADIUS

RADIUS/Cisco是设备类型。“pixa”用户需要Cisco/RADIUS矩形框中的用户名、密码和复选项和“acl=115”，其中显示009\001 AV-Pair（供应商特定）。

## 输出

配置文件中带有“acl=115”的出站用户“pixa”进行身份验证和授权。服务器将acl=115向下传递到PIX，PIX显示如下：

```
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
```

当用户“pixa”尝试转到99.99.99.3（或除99.99.99.2外的任何IP地址，因为存在隐式拒绝）时，用户会看到：

```
Error: acl authorization denied
```

# 新的每用户可下载访问列表 6.2 版本

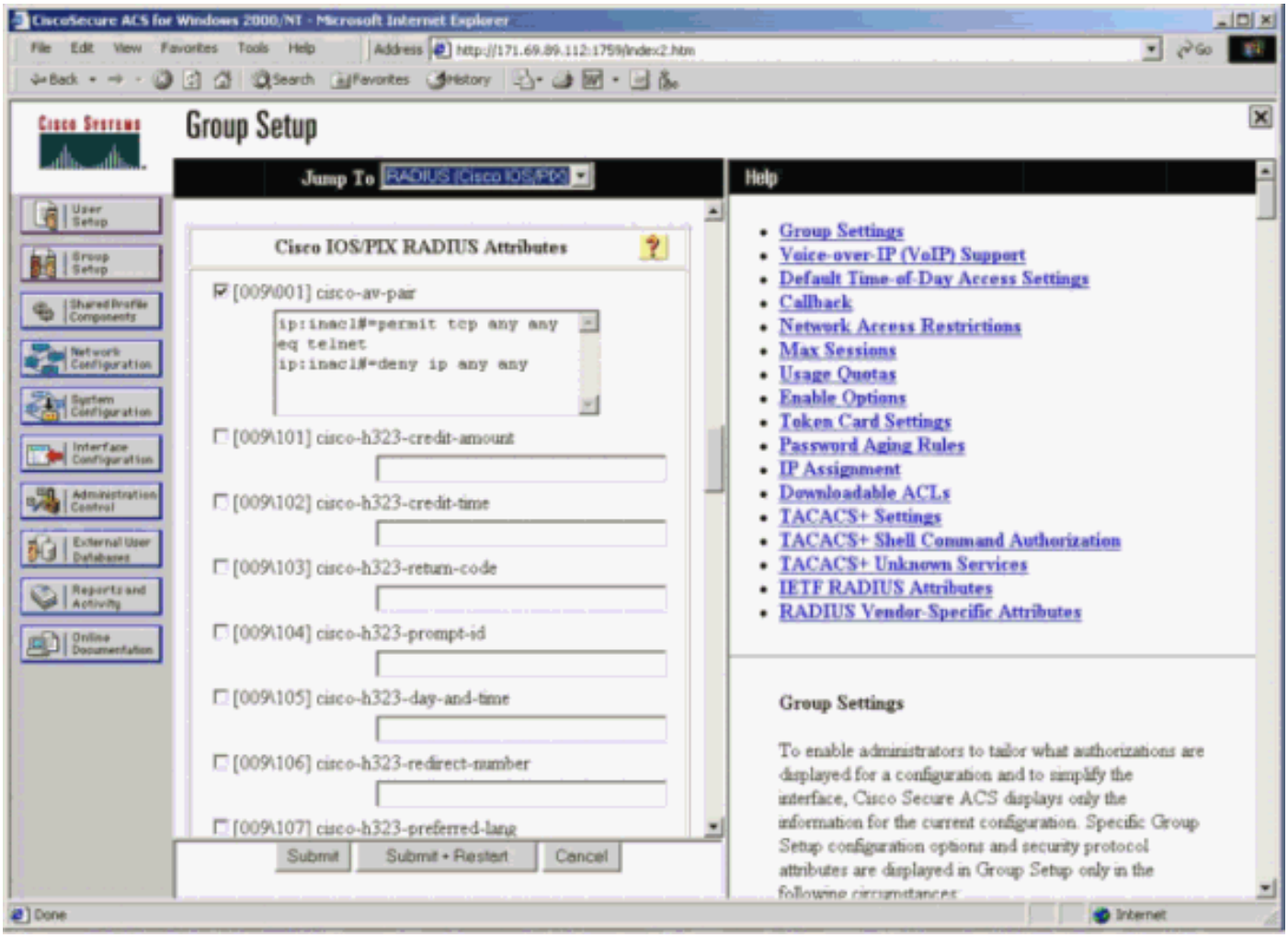
在PIX防火墙的软件版本6.2及更高版本中，访问列表在访问控制服务器(ACS)上定义，以在身份验证后下载到PIX。这仅适用于RADIUS协议。无需在PIX本身上配置访问列表。组模板应用于多个用户。

在早期版本中，访问列表在PIX上定义。身份验证后，ACS将访问列表名称推送到PIX。新版本允许ACS将访问列表直接推送到PIX。

**注意：如**果发生故障转移，则不复制uauth表用户将重新进行身份验证。访问列表将再次下载。

## ACS设置

单击Group Setup并选择RADIUS(Cisco IOS/PIX)设备类型以设置用户帐户。为用户分配用户名（本例中为“cse”）和密码。从属性列表中，选择用于配置[009\001] *vendor-av*-pair的选项。定义访问列表，如本例所示：




## PIX 调试:有效身份验证和下载的访问列表

- 仅允许Telnet并拒绝其他流量。

```
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命令的输出。

```
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命令的输出。

```
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)
```

- 仅拒绝Telnet并允许其他流量。

```
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命令的输出。

```
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命令的输出。

```
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的新每用户可下载访问列表

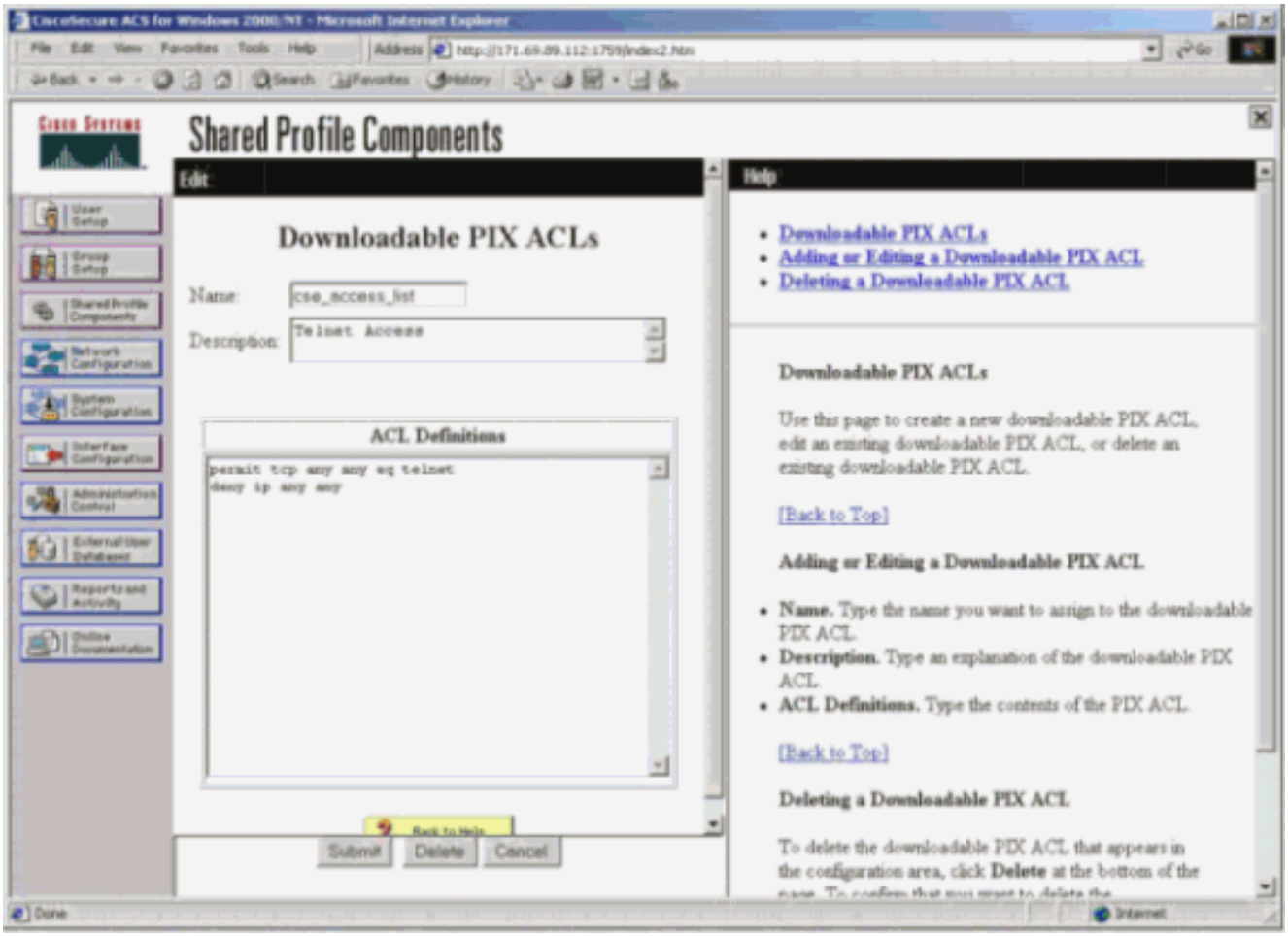
在ACS版本3.0中，共享配置文件组件允许用户创建访问控制列表模板，并为特定用户或组定义模板名称。模板名称可以根据需要与多个用户或组一起使用。这样就无需为每个用户配置相同的访问列表。

**注意：**如果发生故障转移，uauth不会复制到辅助PIX。在状态故障切换中，会话持续。但是，必须重新对新连接进行身份验证，并且必须再次下载访问列表。

## 使用共享配置文件

使用共享配置文件时，请完成以下步骤。

1. 单击**接口配置**。
2. 检查**用户级可下载ACL**和/或**组级可下载ACL**。
3. 单击“共**享配置文件组件**”。单击**User-Level Downloadable ACLs**。
4. 定义可下载ACL。
5. 单击 **Group Setup**。在可下载ACL下，将PIX访问列表分配给之前创建的访问列表。




## PIX 调试:使用共享配置文件的有效身份验证和下载的访问列表

- 仅允许Telnet并拒绝其他流量。

```
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命令的输出。

```
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命令的输出。

```
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
```

- 仅拒绝Telnet并允许其他流量。

```
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命令的输出。

```
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命令的输出。

```
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#
```

# 添加记帐

## PIX配置 — 添加记帐

### TACACS(AuthInbound=tacacs)

添加此命令。

```
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版本中的新功能，定义访问控制列表将说明的内容。

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

**注意：访**问列表101单独定义。

### RADIUS(AuthOutbound=radius)

添加此命令。

```
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版本中的新功能，定义访问控制列表将说明的内容。

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

**注意：访**问列表101单独定义。

**注意**：可以为从PIX 7.0代码开始的PIX上的管理会话生成记帐记录。

## 统计示例

- TACACS记帐示例，用于从99.99.99.2外部到172.18.124.114内部(99.99.99)的Telnet。

```
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
```

- RADIUS记帐示例，用于从内部172.18.124.114到外部99.99.99.2(Telnet)和外部99.99.99.3(HTTP)的连接。

```
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
```

## exclude 命令的使用

在此网络中，如果您确定特定源或目标不需要身份验证、授权或记帐，请发出以下命令。

```
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
```

**注意：** 您已经拥有include命令。

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

或者，在5.2中使用新功能，定义要排除的内容。

```
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：如**果从身份验证中排除框，并且您有授权，则还必须从授权中排除框。

## 最大会话数和查看登录用户

一些TACACS+和RADIUS服务器有“最大会话”（max-session）或“查看已登陆用户”（view logged-in users）功能。能力执行最大会话或检查登录用户依靠计费记录。当有记帐“开始”记录生成，但没有“终止”记录生成时，TACACS+或RADIUS服务器则假设仍然有人登录(用户有一个会话通过PIX)。由于连接性质，它非常适合于Telnet和FTP连接。但是，这对HTTP并不适用。在本例中，使用了不同的网络配置，但概念相同。

用户通过PIX Telnet，在路上进行身份验证。

```
(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
```

由于服务器看到“start”记录，但没有“stop”记录，因此此时服务器显示“Telnet”用户已登录。如果用户尝试需要身份验证的另一连接（可能来自另一台PC），并且如果此用户的服务器上的max-sessions设置为“1”（假设服务器支持max-sessions），则服务器拒绝该连接。用户在目标主机上执行其Telnet或FTP业务，然后退出（在此花费10分钟）。

```
    (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
```

无论uauth是否为0 (指每次认证)或更大值(在uauth期间，一次认证后便不再鉴权）），每一个被访站点的计费记录都会被剪切。

由于协议的性质，HTTP的工作方式不同。以下是HTTP的示例，其中用户通过PIX从171.68.118.100浏览到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
```

用户读下载的网页。开始记录发布在16:35:34，停止记录发布在16:35:35。此下载需要一秒（即，开始记录和停止记录之间不到一秒）。 用户未登录网站。当用户正在读取网页时，连接未打开。最大会话数或查看登录用户不在此处工作。这是因为HTTP中的连接时间（“Built”和“Teardown”之间的时间）太短。“启动”和“终止”记录分秒。没有没有“停止”记录的“开始”记录，因为记录几乎在同一时间发生。无论uauth设置为0还是更大值，每个事务仍会向服务器发送“开始”和“停止”记录。但是，由于HTTP连接的性质，最大会话数和查看登录用户不工作。

# 用户界面

## 更改提示用户请参阅

如果您有命令：

```
auth-prompt prompt PIX515B
```

然后，通过PIX的用户会看到此提示。

```
PIX515B
```

## 自定义用户查看的消息

如果您有以下命令：

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

然后，用户将看到有关失败/成功登录的身份验证状态的消息。

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

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

# 每用户空闲超时与绝对超时

PIX timeout uauth**命令**控制需要重新身份验证的频率。如果TACACS+身份验证/授权已启用，则按用户控制。此用户配置文件设置为控制超时（这位于TACACS+免费软件服务器上，超时以分钟为单位）。

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

身份验证/授权后：

```
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
```

两分钟后：

绝对超时 — 会话断开：

```
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)
```

## 向外的虚拟 HTTP

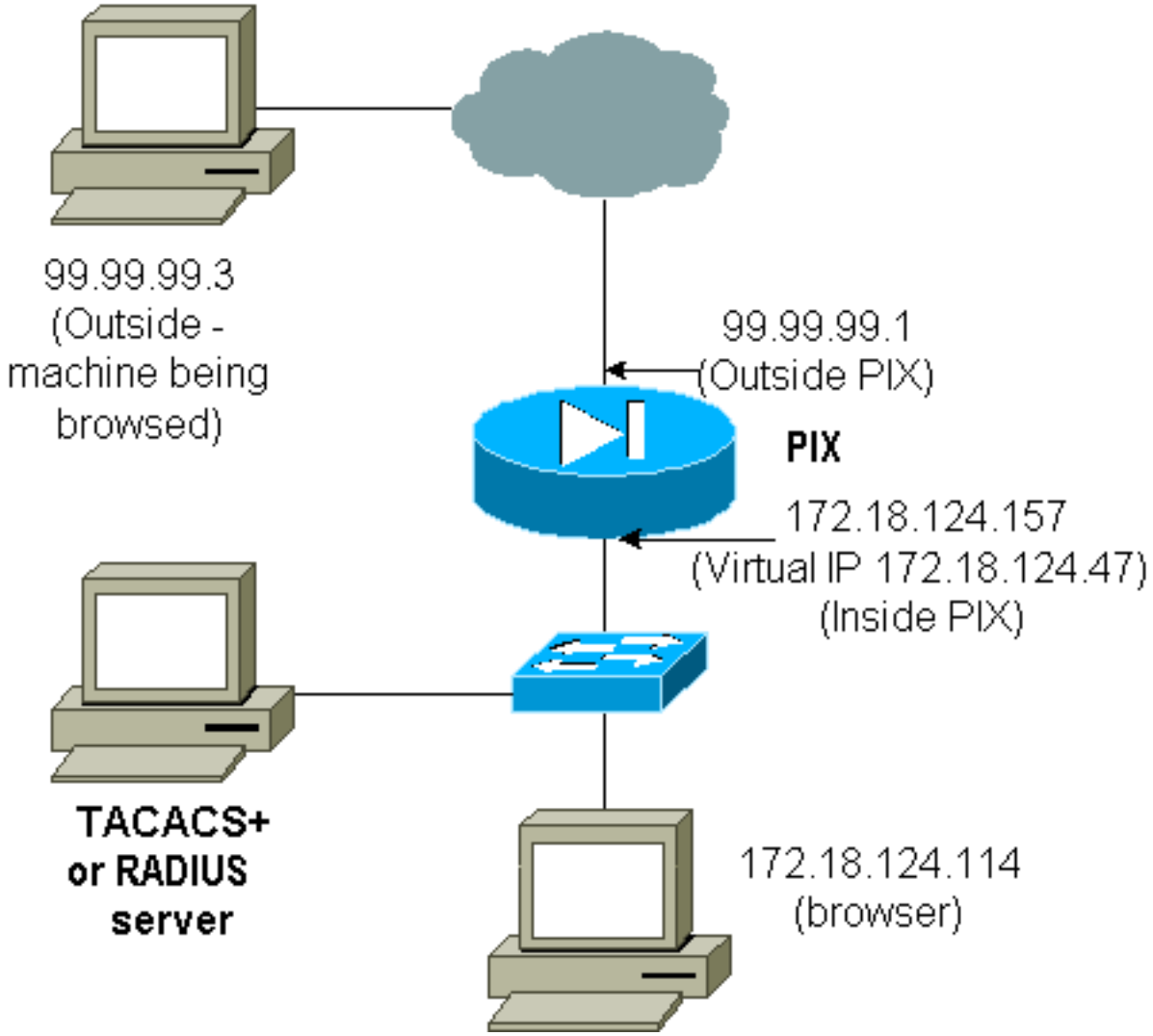
如果在PIX外部的站点以及PIX本身上需要身份验证，则有时会观察到异常的浏览器行为，因为浏览器缓存用户名和密码。

为避免这种情况，请通过将RFC 1918（在Internet上不可路由，但对于PIX内部网络有效且唯一的地址）添加到PIX配置中，以格式实施虚拟HTTP。

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

当用户设法访问PIX之外的时候，需要认证。如果警告参数存在，用户收到一个更改方向消息。认证对UAUTH的时间长度是好的。如文档所示，请勿使用虚拟HTTP将**timeout uauth**命令持续时间设置为0秒。这避免HTTP连接到真正的网络服务器。

**注意**：虚拟HTTP和虚拟Telnet IP地址必须包含在aaa authentication语**句中**。在本例中，指定0.0.0.0包含这些地址。




在PIX配置中添加此命令。

```
virtual http 172.18.124.47
```

用户指向浏览器99.99.99.3。显示此消息。

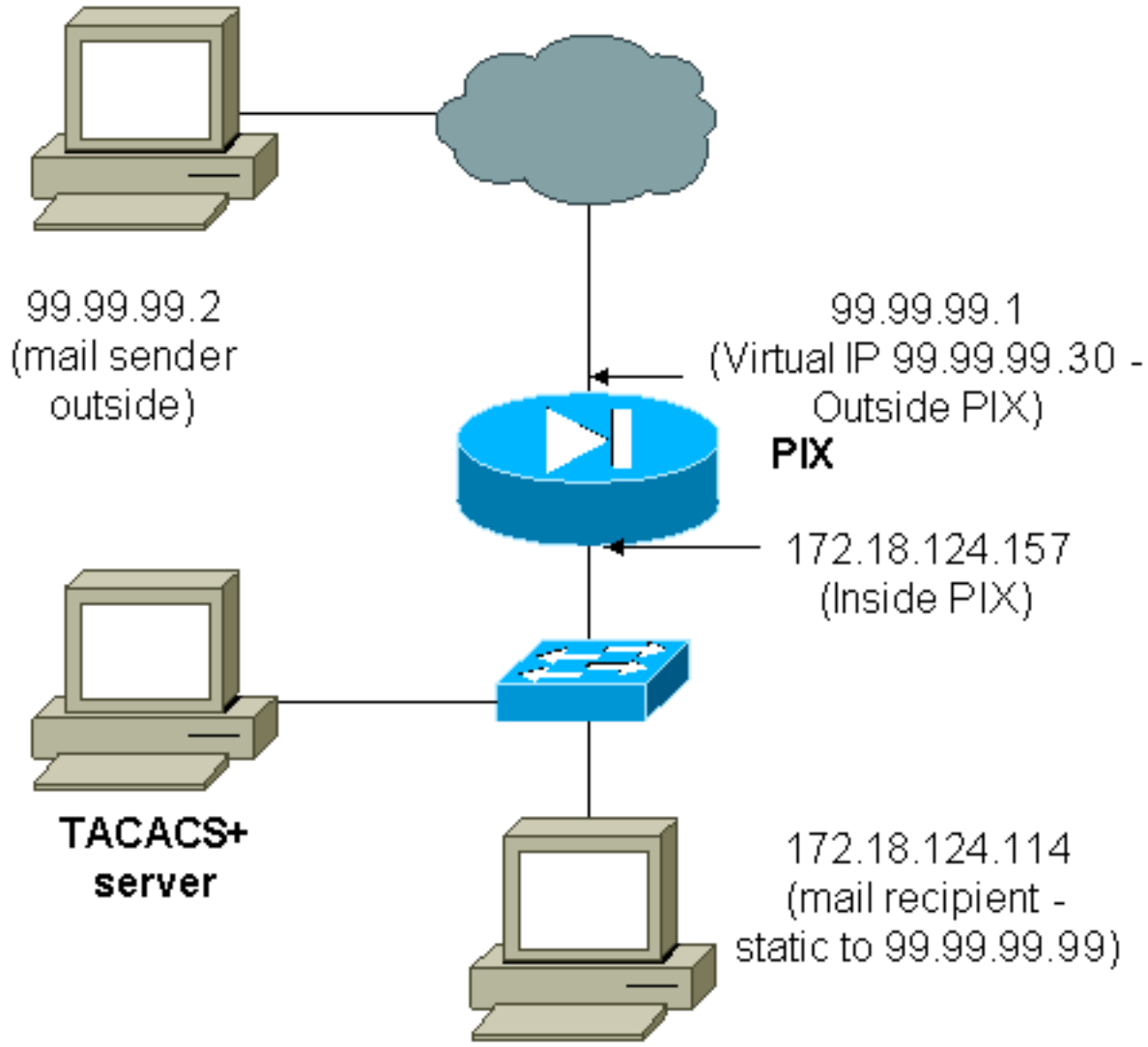
```
Enter username for PIX515B (IDXXX) at 172.18.124.47
```

身份验证后，流量被重定向到99.99.99.3。

## 虚拟 Telnet

**注意**：虚拟HTTP和虚拟Telnet IP地址必须包含在aaa authentication语**句中**。在本例中，指定0.0.0.0包含这些地址。

### 虚拟 Telnet 入站




对入站邮件进行身份验证不是一个好主意，因为不会显示将入站邮件发送到的窗口。请改用**exclude**命令。但为了便于说明，添加了这些命令。

```
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
```

用户（这是TACACS+免费软件）：

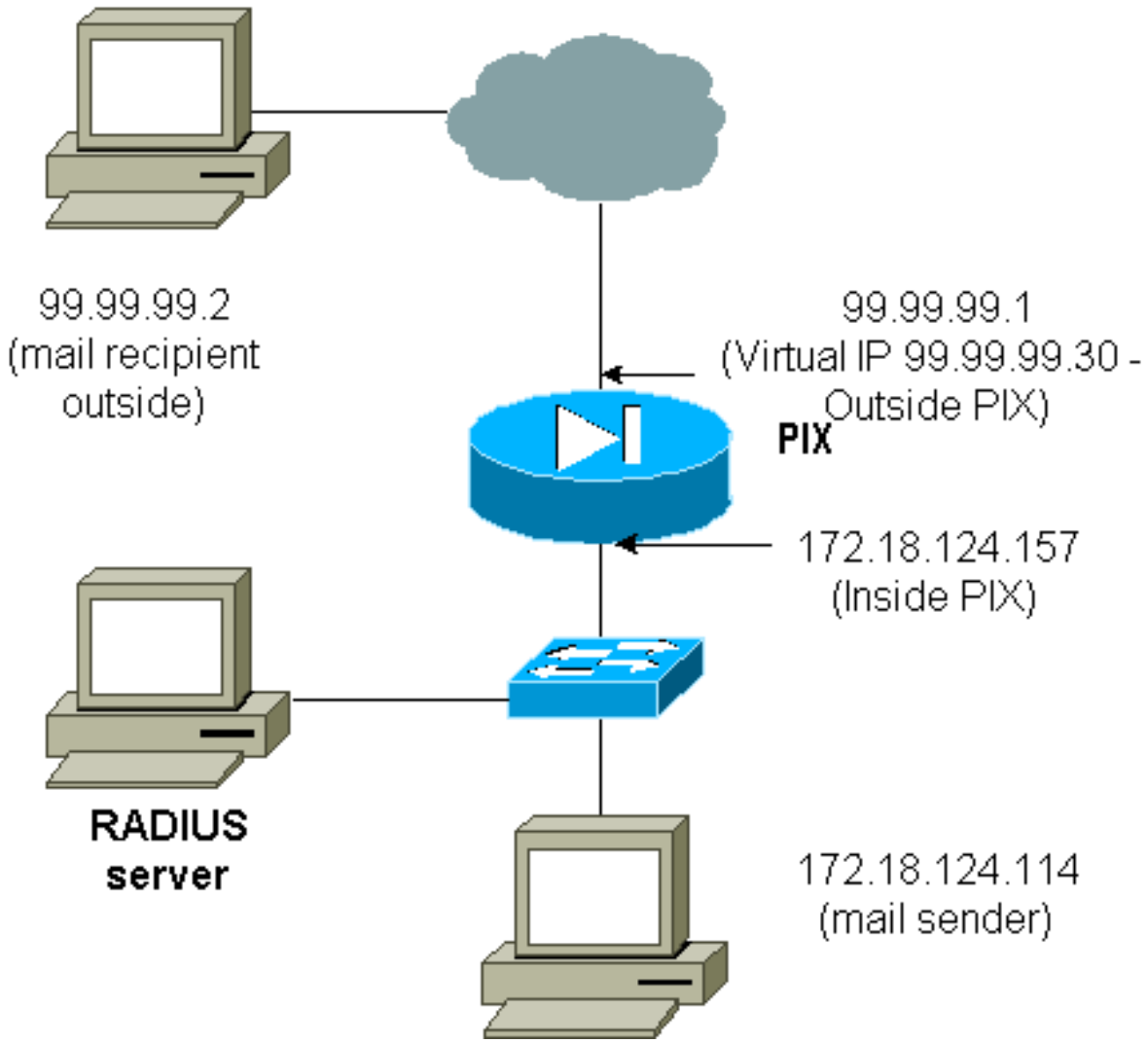
```
  user = cse {
  default service = permit
  login = cleartext "csecse"
  }


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

如果仅启用身份验证，则两个用户在Telnet上对IP地址99.99.99.30进行身份验证后都会发送入站邮件。如果启用了授权，则用户“cse”会Telnet到99.99.99.30，并输入TACACS+用户名/密码。Telnet连接将断开。用户“cse”随后将邮件发送到99.99.99.99(172.18.124.114)。 用户“pixuser”的身份验证成功。 但是，当PIX发送cmd=tcp/25和cmd-arg=172.18.124.114的授权请求时，请求失败，如此输出所示。

```
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
```

## 虚拟 Telnet 出站




对入站邮件进行身份验证不是一个好主意，因为不会显示将入站邮件发送到的窗口。请改用**exclude**命令。但为了便于说明，添加了这些命令。

对出站邮件进行身份验证并不是个好主意，因为出站邮件不会显示一个窗口。请改用**exclude**命令。但为了便于说明，添加了这些命令。

```
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.
```

要从内部向外部发送邮件，请在邮件主机上打开命令提示符，然后Telnet至99.99.99.30。这打开了

邮件通过的洞。邮件从172.18.124.114发送到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
```

## 虚拟 Telnet 注销

当用户远程登录到虚拟Telnet IP地址时，show uauth命令将显示孔开放的时间。如果用户想在他们的会话结束之后阻止数据流经过(时间仍然保持在uauth)，他们需要再次远程登录到虚拟Telnet IP地址。这将断开会话。本示例说明了这一点。

### 第一个身份验证

```
 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
```

### 在第一次身份验证后

```
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
```

### 第二个身份验证

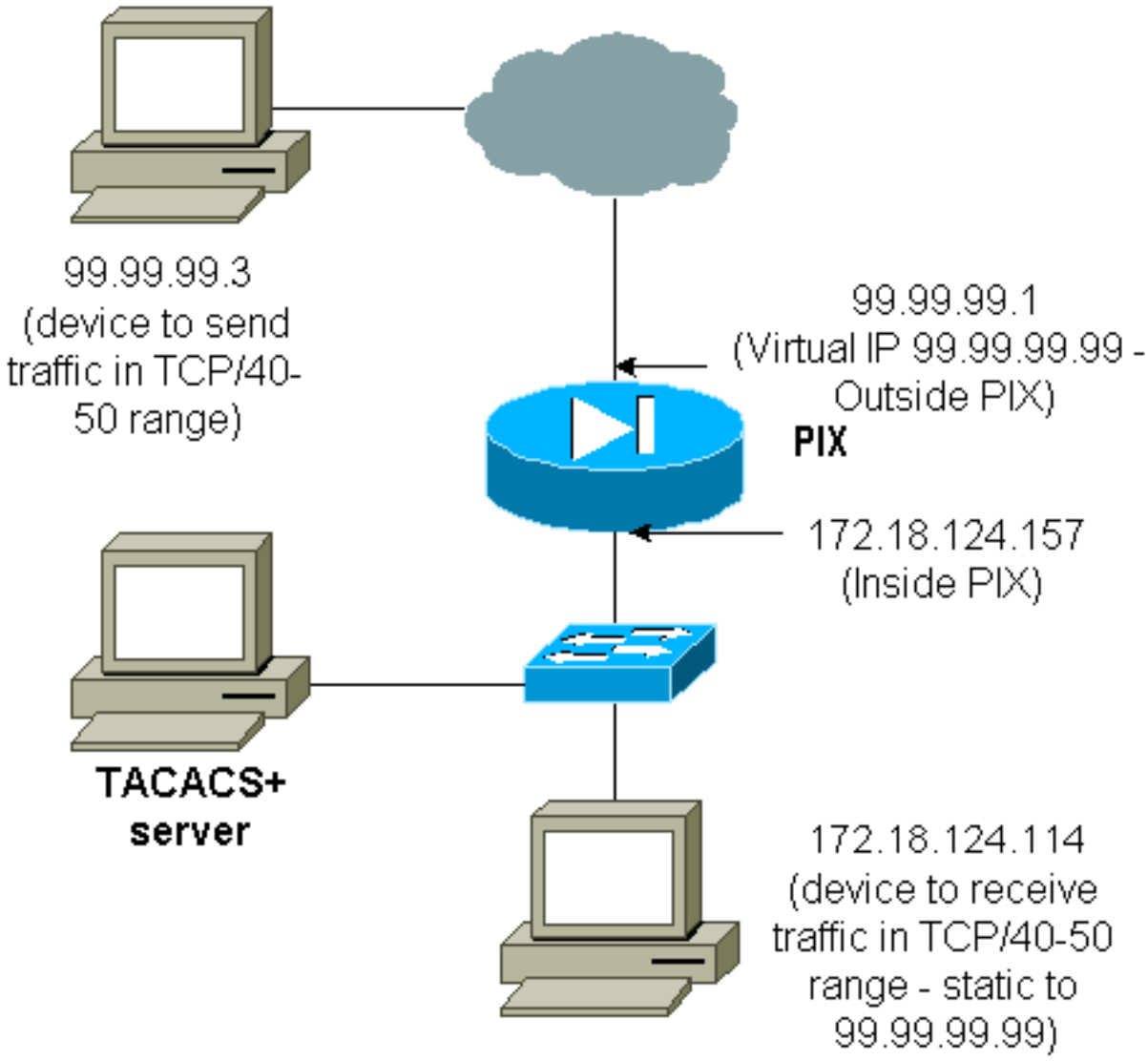
```
   pixfirewall# 109001: Auth start for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
   109005: Authentication succeeded for user 'cse'
      from 172.18.124.114/32863 to    99.99.99.30/23
      on interface inside
```

### 第二次身份验证后

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

# 端口授权

## 网络图




允许对端口范围进行授权。如果在PIX上配置了虚拟Telnet，并且为一系列端口配置了授权，则用户会通过虚拟Telnet打开洞。如果端口范围授权在启动状态，该范围的数据流传输到PIX，PIX则发送命令到TACACS+服务器进行授权。此示例显示端口范围上的入站授权。

```
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+服务器配置示例（免费软件）：

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

用户必须首先Telnet至虚拟IP地址99.99.99.99。身份验证后，当用户尝试通过PIX将端口40-50范围内的TCP流量推送至99.99.99.99(172.18.124.114)时，cmd=tcp/40-50被发送到TACACS+服务器，其中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
```

## AAA计费HTTP、FTP和Telnet以外的流量

在确保虚拟Telnet工作以允许TCP/40-50流量传输到网络内部的主机后，请使用以下命令添加此流量的记帐。

```
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+ 计费记录示例

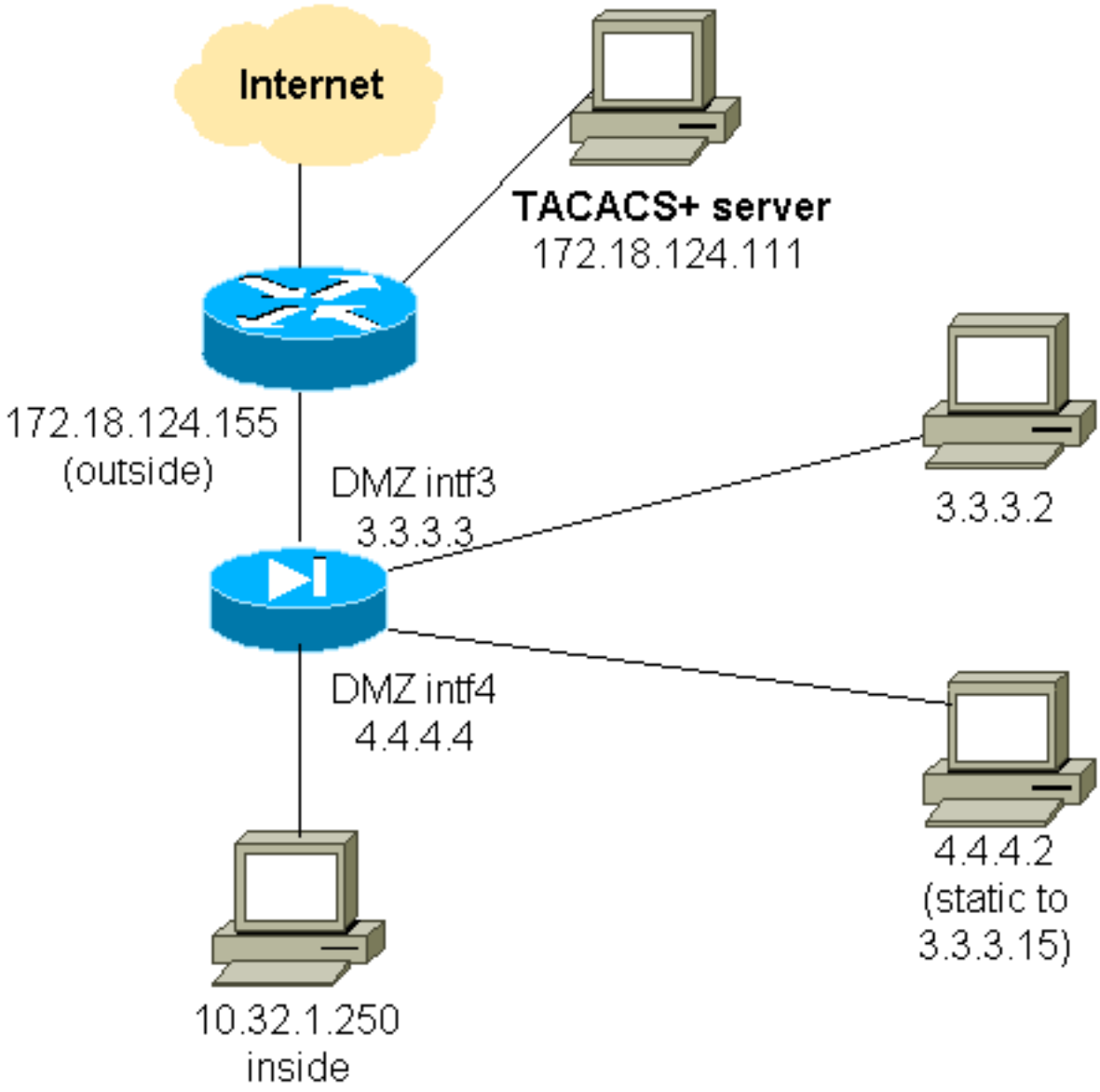
```
   Thu Aug 24 08:06:09 2000 172.18.124.157 cse PIX 99.99.99.3
   start task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50
   Thu Aug 24 08:06:17 2000 172.18.124.157 cse PIX 99.99.99.3
   stop task_id=0x17 foreign_ip=99.99.99.3 local_ip=172.18.124.114
   cmd=tcp/40-50 elapsed_time=8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

## DMZ 上的认证

要验证从一个DMZ接口到另一个DMZ接口的用户，请告诉PIX验证指定接口的流量。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
```

## 网络图




## 部分 PIX 配置

验证pix/intf3和pix/intf4之间的Telnet流量，如下所示。

| 部分 PIX 配置 |
| --- |
| nameif ethernet0 outside security0<br>nameif ethernet1 inside security100<br>(nameif ethernet2 pix/intf2 security10)<br>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
```

# 报告TAC案例应收集的信息

**如果在执行上述故障排除步骤后仍需要帮助，并希望向Cisco TAC提交问题，请确保包含此信息以排除PIX防火墙故障。**

- 问题说明和相关拓扑详细信息
- 在打开案例之前，请进行故障排除
- **show tech-support 命令的输出**
- 使用logging buffered debugging命令**运行后**,show log命令的输出，或演示问题**的控制台捕**获（如果可用）

请以非压缩的纯文本格式 (.txt) 将收集的数据附加到请求中。 在案例查询工具（仅限注册客户）的帮助下，通过上载案例将信息附加到您的案例。 如果无法访问案例查询工具，请将邮件附件中的信息发送到attach@cisco.com，并在邮件的主题行中注明案例编号。

# 相关信息

- Cisco PIX 防火墙软件

- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 用于 Windows 的 Cisco 安全访问控制服务器
- 用于 Unix 的 Cisco 安全访问控制服务器
- 终端访问控制器访问控制系统 (TACACS+)
- 远程用户拨入认证系统(RADIUS)
- 技术支持和文档 - Cisco Systems