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+认证可以为FTP，Telnet和HTTP连接执行通过Cisco Secure PIX防火墙。其他较不普通的协议的验证通常使工作。支持TACACS+授权。不支持RADIUS授权。在PIX 5.2验证、授权和统计(AAA)上的变化在更早版本包括AAA访问列表支持控制谁验证，并且什么资源用户访问。在PIX 5 3和以后，在代码更早版本的验证、授权和统计(AAA)更改是RADIUS端口可配置。

注意： PIX 6.x能执行核算穿过流量，但是不流量的destinated对PIX。

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：

- Cisco Secure 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。

注意： 如果运行PIX/ASA软件版本7.x和以后，参考配置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

这是验证、授权和核算的说明：

- 认证就是用户是谁。
- 授权是什么用户。
- 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。
- 核算是什么用户。

开启验证/授权时用户看到的信息

当用户设法去从里向外(或反之亦然) Authentication/Authorization开启：

- **Telnet** —用户为密码看到用户名提示出来，然后请求。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来。用户需要输入“local_username@remote_username” 为用户名和“local_password@remote_password的”为密码。PIX发送“local_username”和“local_password”到本地安全服务器。如果验证(和授权)是成功的在PIX/服务器，“remote_username”和“remote_password”通过到目的地FTP服务器以远。
- **HTTP** —窗口在浏览器请求用户名和密码显示。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**。如果看起来PIX应该计时HTTP连接，但是不如此执行，很可能再验证用浏览器“射击”实际上发生缓存的用户名和密码对PIX。PIX转发此到认证服务器。PIX系统日志和服务器调试显示此现象。如果Telnet和FTP似乎“正常”工作，但是HTTP连接不，这是原因。

调试步骤

- 在您添加AAA认证和特许前，请确保PIX配置工作。如果无法通过流量，在您创立认证和授权前，您无法那么之后执行。
- 启用登陆PIX。发出**logging console debug命令**打开操作日志控制台调试。**注意：** 请勿大量地使用在一个加载的系统的操作日志控制台调试。请使用**logging monitor debug命令**记录远程登录会话。可以使用Logging buffered debugging，然后执行**show logging命令**。记录日志可能也发送到系统日志服务器和被检查那里。
- 启用调试在TACACS+或RADIUS服务器。

只有认证

网络图

服务器设置- 仅认证

Cisco Secure UNIX TACACS服务器配置

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

Cisco Secure UNIX RADIUS服务器配置

注意： 添加PIX IP地址和密钥到网络接入服务器(NAS)列表在高级GUI帮助下。

```
user=bill {
radius=Cisco {
check_items= {
2="foo"
}
reply_attributes= {
6=6
```

```
}
}
}
```

Cisco Secure Windows RADIUS

请使用这些步骤设置Cisco Secure Windows RADIUS塞弗。

1. 得到在**User Setup部分的**一个密码。
2. 从**Group Setup部分**，请设置属性6 (服务类型)**登陆**或**管理**。
3. 添加在GUI的**NAS Configuration部分的**PIX IP地址。

Cisco Secure Windows TACACS+

用户获得在**User Setup部分的**一个密码。

Livingston RADIUS 服务器配置

注意： 添加PIX IP地址并且锁上到客户端文件。

- 发单Password= " foo” user-service-type = Shell用户

Merit RADIUS 服务器配置

注意： 添加PIX IP地址并且锁上到客户端文件。

- 发单Password= " foo”服务类型= Shell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-仅验证

PIX初始配置-仅验证

```
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和以后， RADIUS验证和计费端口可以更改到某事除默认1645/1646之外用这些命令：

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

PIX 认证Debug示例

关于如何启用调试的信息，请参阅调试步骤。这些是初始化流量对内部的172.18.124.114用户的示例在99.99.99.2 (99.99.99.99)反之亦然。入站数据流TACACS验证的，并且出站RADIUS验证的。

成功认证- 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)
```

不成功验证由于错误的用户名/密码- TACACS+ (入站)。用户看到“Error:超出的尝试最大数”。

```
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
```

服务器不发言对PIX - 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：超出的尝试最大数”。

```
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
```

成功验证- 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
```

未成功认证(用户名或密码) - RADIUS (出站)。用户为用户名看到请求，然后密码，有三个机会输入这些，和，如果不成功，参见“Error:超出的尝试最大数”。

```
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：超出的尝试最大数”。

```
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

如果要允许所有已认证的用户通过PIX执行所有操作(HTTP、FTP和Telnet)，则验证是满足的，并且授权不是需要的。然而，如果要允许服务的某子集对某些用户或对某些站点限制从去的用户，授权是需要的。RADIUS授权为流量是无效通过PIX。TACACS+授权在这种情况下有效。

如果验证通过，并且授权打开， PIX发送用户执行到服务器的命令。例如，“在PIX版本5.2的http 1.2.3.4."， TACACS+授权与访问列表一道用于控制用户去的地方。

如果要实现HTTP的(访问的网站授权)，请使用软件例如Websense，因为单个网站能有很大数量的IP地址关联与它。

服务器设置- 认证和授权

Cisco Secure 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 .*
}
}
}
```

Cisco Secure Windows TACACS+

完成这些步骤设置Cisco Secure Windows TACACS+服务器。

1. 单击**拒绝不匹配IOS at命令**组建立的底部。
2. 点击**add/edit new命令(FTP， HTTP， Telnet)**。例如，如果要允许Telnet到一个特定站点(“telnet 1.2.3.4")，命令是**telnet**。参数是*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。然后请单击**editing命令的完成**。
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帮助下添加在NAS Configuration部分的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功能与定义的访问控制列表101一道以前允许此语句替换上一个三个语句。不应该混合旧有和新的冗余。

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

PIX 认证和授权Debug示例

成功验证和授权成功- 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)
```

成功验证，但是授权发生故障- TACACS+.用户也看到消息“Error:拒绝的授权”。

```
 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及以上版本，请定义在PIX的访问列表。应用他们逐个用户根据在服务器的用户配置文件。TACACS+要求认证和授权。RADIUS要求仅验证。在本例中，出局验证和授权对TACACS+更改。在PIX的一访问列表设置。

注意： 在PIX版本6.0.1中及以后，如果使用RADIUS，访问列表通过输入在标准IETF RADIUS属性11 (过滤器ID) [CSCdt50422]的列表实现。在本例中，属性11设置到115代替执行根据厂商的"acl=115"冗余。

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版本不认可“ACL”冗余。

Cisco Secure UNIX TACACS+服务器配置

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

Cisco Secure Windows TACACS+

为了添加特许到PIX控制用户连同访问列表的地方，请检查**shell/exec**，检查**存取控制序列逻辑单元**，并且填写编号(匹配在PIX的访问列表编号)。

Cisco Secure UNIX RADIUS

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

Cisco Secure Windows RADIUS

RADIUS/Cisco是设备类型。“pixa”用户需要一用户名、一个密码和一检查和"acl=115"在说009\001 AV对的Cisco/RADIUS矩形框(根据厂商的)。

输出

出局用户“pixa”与"acl=115"在配置文件验证并且授权。服务器通过在acl=115下对PIX，并且PIX显示此：

```
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”设法去99.99.99.3 (或除了99.99.99.2的所有IP地址，因为隐式时请拒绝)，用户看到此：

```
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和以上中，访问列表在访问控制服务器(ACS)定义下载到PIX在验证以后。这仅与RADIUS协议一起使用。没有需要配置在PIX的访问列表。组模板应用给多个用户。

在更早版本中，访问列表在PIX定义。在验证， ACS推送访问列表名称对PIX。新版本允许ACS推送访问列表直接地到PIX。

注意： 如果故障切换发生， uauth表不是复制的用户重新鉴别。访问列表再下载。

ACS设置

点击**组建立**并且选择**RADIUS (思科IOS/PIX)**设备类型设置用户帐户。为用户分配用户名(“cse”，在本例中)和密码。从Attributes列表，请选择选项配置**[009\001] vendor-av-pair**。定义访问列表如此示例所示：

PIX 调试：有效验证和下载的访问列表

- 允许仅Telnet并且否决其他流量。
```
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)
```
从**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
```
从**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)
```
- 拒绝仅Telnet并且允许其他流量。
```
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
```

从**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`从**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)`

新的每个用户可下载访问控制列表使用ACS 3.0

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。模板名称可以与许多用户或组一起使用当必要时。这排除需要配置每个用户的相同的访问列表。

注意： 如果故障切换发生， uauth没有复制对备用PIX。在有状态故障切换，会话持续。然而，必须重新鉴别新连接，并且必须再下载访问列表。

使用共享配置文件

当您使用共享配置文件时，请完成这些步骤。

1. 点击**接口配置**。
2. 检查**用户级可下载的ACLs**和**组级可下载的ACLs**。
3. 点击**共享配置文件组件**。点击**用户级可下载的ACLs**。
4. 定义可下载的ACLs。
5. 单击 **Group Setup**。在可下载的ACLs下，请分配PIX访问列表到创建的访问列表前。

PIX 调试：有效验证和下载的访问列表使用共享配置文件

- 允许仅Telnet并且否决其他流量。`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)`从**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#`从**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`
- 拒绝仅Telnet并且允许其他流量。`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
```

从**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
```

从**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-添加核算

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分开定义。

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分开定义。

注意： 计费记录可以为PIX的管理会话生成从PIX 7.0代码开始。

统计示例

- Telnet的TACACS统计示例从99.99.99.2从外部对172.18.124.114里面(99.99.99.99)。

```
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
```

- 连接的RADIUS记帐示例从172.18.124.114里面对从外部99.99.99.2的外部(Telnet)和99.99.99.3(HTTP)。

```
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，如果决定特定来源或目的地不需要验证，授权或者认为，请发出这些命令。

```
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： 您已经有**包括**命令。

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

或者，与在5.2的新特性，请定义什么您要排除。

```
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： 如果从验证排除方框，并且有授权，您必须从授权也排除方框。

注册用户最大会话与观点

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。然而，这不为HTTP工作良好。在本例中，使用不同的网络配置，但是概念是相同的。

用户通过PIX远程登录，验证在途中。

```
(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
```

由于服务器未看到“启动”记录，但是“终止”记录，此时此刻，服务器显示“Telnet”用户登陆。如果用户尝试要求验证的另一连接(或许从另一个PC)，并且，如果最大会话设置到"1"在此用户的服务器(假设服务器支持最大会话)，连接由服务器拒绝。用户去他们的Telnet或FTP业务在目标主机，然后退出(度过十分钟那里)。

```
    (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。

HTTP工作不同地由于协议的本质。这是HTTP的示例用户从171.68.118.100浏览到9.9.9.25通过PIX的地方。

```
(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。开始录制被张贴在16:35:34和在16:35:35的终止记录。此次下载用了一秒时间(即在开始和终止记录之间的时间不足一秒)。用户没有登陆到网站。当用户读网页时，连接不是开放的。注册用户最大会话或观点不运作此处。这是因为连接时间(“被构件的”和“卸载之间的”时间)在HTTP是太短的。“启动”和“终止”记录分秒。因为记录同时，出现没有“启动”记录没有“终止”记录。仍有“启动”和“终止”记录发送对每处理的服务器uauth是否为更加大0或的事设置。然而，注册用户最大会话与观点不工作由于HTTP连接种类。

用户界面

更改提示用户看到

如果有命令：

auth-prompt prompt PIX515B

然后通过PIX的用户看到此提示符。

```
PIX515B
```

定制消息用户看到

如果有命令：

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

然后用户看到关于认证状态的一个消息在失败/成功登录。

```
  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命令控制重新验证多频繁要求。如果TACACS+认证/授权打开，这逐个用户被控制。此用户配置文件设置控制超时(这在TACACS+免费软件服务器，并且超时是以分钟)。

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

在认证/授权以后：

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

在两分钟结束时：

绝对超时-被切断的会话获得：

```
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

如果验证要求在站点PIX的外部以及在PIX，异常浏览器行为从浏览器缓存有时被观察，用户名和密码。

为了避免此，请通过添加一个RFC 1918地址实现虚拟 HTTP (在互联网的地址不可路由，但是有效和唯一为PIX网络内部)对在格式的PIX配置。

virtual http #.#.#.# <warn>

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，请勿设置**timeout uauth命令**持续时间为0与虚拟HTTP的秒。这避免HTTP连接到真正的网络服务器。

注意： 在**AAA认证**语句必须包括虚拟HTTP和virtual telnet IP地址。在本例中，指定0.0.0.0包括这些地址。

在PIX配置中请添加此命令。

virtual http 172.18.124.47

用户点浏览器99.99.99.3。此消息显示。

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

在验证以后，流量重定向对99.99.99.3。

虚拟 Telnet

注意： 在**AAA认证**语句必须包括虚拟HTTP和virtual telnet IP地址。在本例中，指定0.0.0.0包括这些地址。

虚拟 Telnet 入站

因为窗口没有显示为了邮件能发送的入站，它不是好主意验证入站的邮件。请使用**exclude命令**。但是对于例证目的，这些命令被添加。

```
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 .*
  }
  }
```

如果仅验证打开，两个用户发送邮件入站在验证在Telnet以后对IP地址99.99.99.30。如果授权启用，用户“cse”远程登录到99.99.99.30，并且输入TACACS+用户名/密码。Telnet连接丢包。用户“cse”然后发送邮件对99.99.99.99 (172.18.124.114)。验证为用户“pixuser”成功。然而，当PIX发送授权请求cmd=tcp/25和cmd-arg=172.18.124.114时，如此输出所显示，请求失效。

```
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

因为窗口没有显示为了邮件能发送的入站，它不是好主意验证入站的邮件。请使用**exclude命令**。但是对于例证目的，这些命令被添加。

因为窗口没有显示为了邮件能发送的出站，它不是好主意验证出站的邮件。请使用**exclude命令**。但是为图示的目的，这些命令被添加。

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.*

为了发送从里向外邮件，请启动在邮件主机的一prompt命令并且远程登录到99.99.99.30。这打开邮件的孔能经历。邮件从172.18.124.114被发送到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。这是由此示例说明的。

第一验证

```
 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
```

在第一验证以后

```
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
```

在第二验证以后

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

端口授权

网络图

授权为端口范围允许。如果virtual telnet在PIX配置，并且授权为端口范围配置，用户打开与virtual telnet的孔。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。此示例显示在端口范围的Inbound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
  }
  }
```

用户必须首先远程登录到虚拟IP地址99.99.99.99。在验证以后，当用户设法穿过在端口40-50范围的TCP数据流PIX到99.99.99.99 (172.18.124.114)时， cmd=tcp/40-50发送到有cmd-arg=172.18.124.114的TACACS+服务器如说明此处：

```
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
```

流量的Aaa accounting除HTTP、FTP和Telnet之外

在您确保virtual telnet工作允许TCP/40-50流量到主机在网络里面后，请添加此流量的核算用这些命令。

```
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

为了验证从一个DMZ接口去别的用户，请告诉PIX验证指定接口的流量。在PIX，安排是象这样：

```
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，如被展示此处。

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
```

报告TAC案例应收集的信息

如果在遵从上面故障排除步骤以后还需要援助并且要开有Cisco TAC的一个Case，请务必包括排除故障的您的PIX防火墙此信息。

- 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
- (若有)展示问题从**show log命令的**输出，在您以**logging buffered debugging命令后**运行或者控制台获取

请以非压缩的纯文本格式 (.txt) 将收集的数据附加到请求中。附上信息到情况通过上传它在案例查询工具(仅限注册用户)帮助下。如果无法访问案例查询工具，请发送在一个电子邮件附件的信息对attach@cisco.com同您的案例编号在您的消息标题栏。

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