PIX、TACACS+和RADIUS配置示例：4.2.x

目录

简介

RADIUS和TACACS+认证可能为FTP、Telnet和HTTP连接执行。支持 TACACS+ 授权；RADIUS授权不是。

验证的语法在PIX软件4.2.2方面轻微更改。本文使用语法软件版本4.2.2。

先决条件

要求

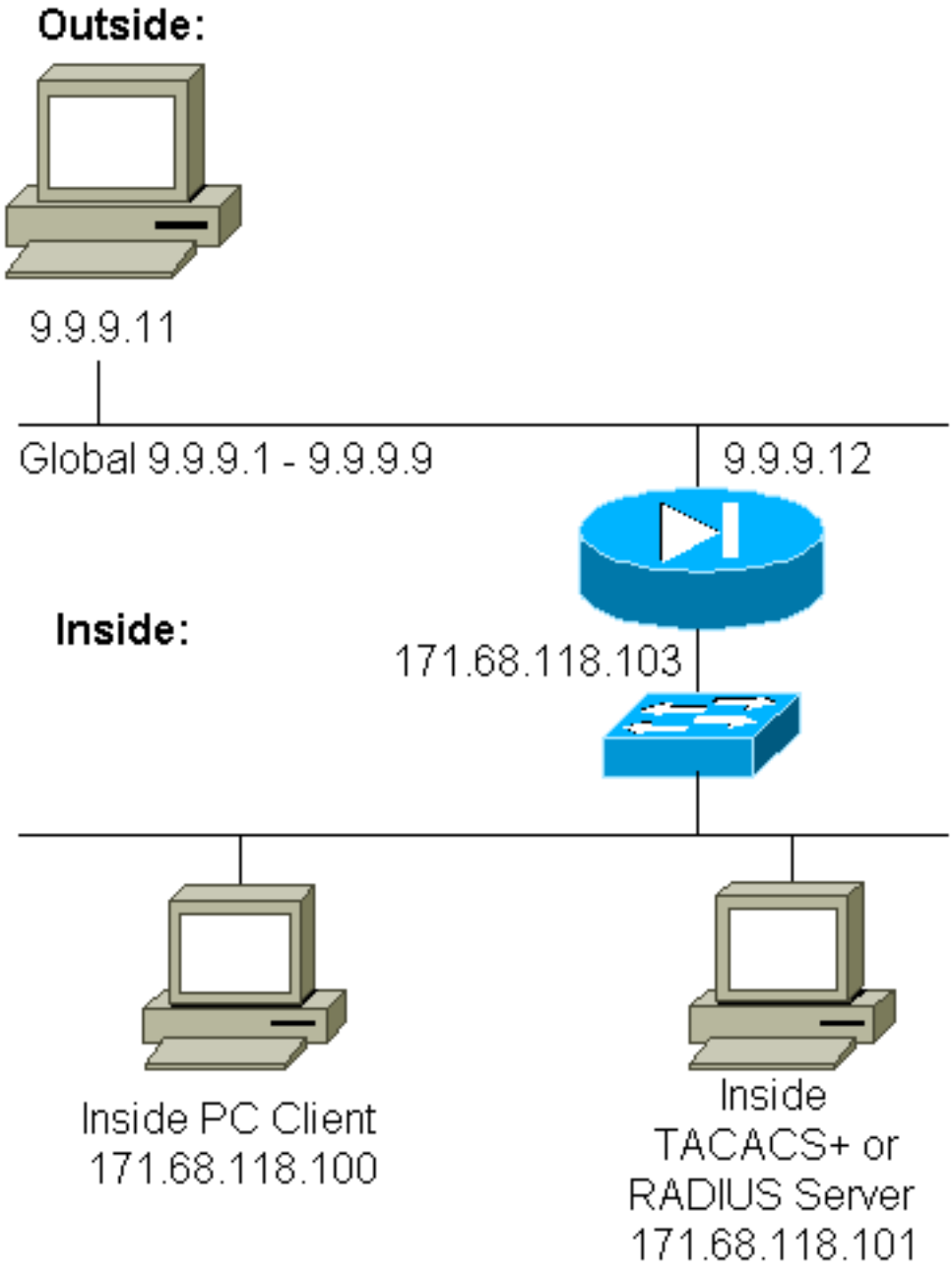
本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

网络图

本文档使用以下网络设置：



PIX 配置
pix2# **write terminal** Building configuration : Saved :

```
PIX Version 4.2(2) nameif ethernet0 outside security0
nameif ethernet1 inside security100 enable password
8Ry2YjIyt7RRXU24 encrypted passwd OnTrBUG1Tp0edmkr
encrypted hostname pix2 fixup protocol http 80 fixup
protocol smtp 25 no fixup protocol ftp 21 no fixup
protocol h323 1720 no fixup protocol rsh 514 no fixup
protocol sqlnet 1521 no failover failover timeout
0:00:00 failover ip address outside 0.0.0.0 failover ip
address inside 0.0.0.0 failover ip address 0.0.0.0 names
pager lines 24 logging console debugging no logging
monitor logging buffered debugging logging trap
debugging logging facility 20 interface ethernet0 auto
interface ethernet1 auto interface ethernet2 auto ip
address outside 9.9.9.12 255.255.255.0 ip address inside
171.68.118.103 255.255.255.0 ip address 0.0.0.0 0.0.0.0
arp timeout 14400 global (outside) 1 9.9.9.1-9.9.9.9
netmask 255.0.0.0 static (inside,outside) 9.9.9.10
171.68.118.100 netmask 255.255.255.255 0 0 conduit
permit icmp any any conduit permit tcp host 9.9.9.10 eq
telnet any no rip outside passive no rip outside default
no rip inside passive no rip inside default timeout
xlate 3:00:00 conn 1:00:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:00:00 absolute ! !-
-- The next entry depends on whether TACACS+ or RADIUS
is used. ! tacacs-server (inside) host 171.68.118.101
cisco timeout 5 radius-server (inside) host
171.68.118.101 cisco timeout 10 ! !--- The focus of
concern is with hosts on the inside network !---
accessing a particular outside host. ! aaa
authentication any outbound 171.68.118.0 255.255.255.0
9.9.9.11 255.255.255.255 tacacs+|radius ! !--- It is
possible to be less granular and authenticate !--- all
outbound FTP, HTTP, Telnet traffic with: aaa
authentication ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius aaa authentication http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs+|radius ! !--- Accounting records are
sent for !--- successful authentications to the TACACS+
or RADIUS server. ! aaa accounting any outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius ! no snmp-server
location no snmp-server contact snmp-server community
public no snmp-server enable traps telnet 171.68.118.100
255.255.255.255 mtu outside 1500 mtu inside 1500 mtu
1500 Smallest mtu: 1500 floodguard 0 tcpchecksum silent
Cryptochecksum:be28c9827e13baf89a937c617cfe6da0 : end
[OK]
```

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

认证与授权

- 认证就是用户是谁。
- 授权是告诉用户什么能执行。
- 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。

和作为示例，假设您只安排内部一百个的用户和您希望六这些用户能执行FTP，Telnet或者HTTP网

络的外部。告诉PIX验证出站流量和给所有六个用户在TACACS+/RADIUS安全服务器的ID。使用简单验证，这六个用户可以验证与用户名和密码，然后出去。其他九十四个用户不能出去。PIX提示用户提供用户名/密码，然后将用户名和密码发送到TACACS+/RADIUS安全服务器。并且，根据答复，它打开或拒绝连接。这六个用户可能执行FTP，Telnet或者HTTP。

然而，假设这三个用户之一，“特里”，不是委托。您希望允许特里执行FTP，而不是HTTP或者Telnet到外界。这意味着您需要添加授权。即授权什么用户能执行除他们是的正在验证之外。当您添加特许到PIX时， PIX首先发送特里的用户名和密码到安全服务器，然后发送告诉安全服务器的授权请求什么“命令”特里尝试执行。适当的设置服务器，特里可以允许到“FTP 1.2.3.4"，但是拒绝“HTTP”或“Telnet”到任何地方。

开启验证/授权时用户看到的信息

当您设法去从里向外(或反之亦然) Authentication/Authorization开启：

- **Telnet** -用户为密码看到用户名提示显示，跟随着的是对密码的请求。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向本地安全服务器发送“local_username”和“local_password”命令，如果PIX/服务器上的认证（和授权）成功，“remote_username”和“remote_password”将传输到目的地FTP服务器。
- **HTTP** -窗口在请求用户名和密码的浏览器显示。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**。如果看起来应该时间PIX 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。它然后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。

用于所有情形的服务器配置

在TACACS+服务器配置示例中，只要启动认证，用户"all"， "telnetonly" "，httponly"，和"ftponly"都工作。在RADIUS服务器配置示例中，用户“所有”工作。

增加授权后，PIX除向TACACS+认证服务发送用户名和密码外，还向TACACS+服务器发送命令(Telnet、HTTP或FTP)。TACACS+服务器然后检查发现是否用户被授权该命令。

在一最新示例中， 171.68.118.100的用户发出telnet命令**9.9.9.11**。当这在PIX接收时，向TACACS+服务器发送用户名、密码和命令，并进行处理。

因此与授权除验证之外，用户“telnetonly”可通过PIX执行Telnet操作。然而，用户“httponly”和“ftponly”不可通过PIX执行Telnet操作。

(再，授权不支持与RADIUS由于协议规格描述的本质)。

Cisco Secure UNIX TACACS+服务器配置

Cisco Secure 2.x

- 用户节显示此处。
- 添加PIX IP地址或完全限定域名并且锁上对CSU.cfg。`user = all {`

```
password = clear "all"
default service = permit
}

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

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

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

Cisco Secure UNIX RADIUS服务器配置

请使用先进的图形用户界面(GUI)添加PIX IP和密钥对网络接入服务器(NAS)列表。用户节出现如被看到此处：

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

CiscoSecure NT 2.x RADIUS

联机的CiscoSecure 2.1的Sample Configurations部分和Web文档描述设置;属性6 (服务类型)是洛金或管理的。

使用GUI，添加PIX的IP在NAS Configuration部分的。

EasyACS TACACS+

EasyACS文档提供设置信息。

1. 在组部分，单击**Shell exec** (产生EXEC权限)。
2. 要添加特权到PIX，在组建立的底层单击**拒绝不匹配IOS指令**。
3. 选择为例如您要允许的每命令**添加/编辑**(Telnet)。
4. 如果您想要允许Telnet到特定站点，在参数部分输入IP。要允许Telnet到整个场地，单击**允许所有未列出的参数**。
5. 点击**editing命令的完成**。
6. 执行步骤其中每一的1through 5允许命令例如(Telnet、HTTP和FTP)。

7. 使用GUI，添加PIX的IP在NAS Configuration部分的。

CiscoSecure NT 2.x TACACS+

Cisco Secure 2.x文档提供设置信息。

1. 在组部分，单击**Shell exec** (产生EXEC权限)。
2. 要添加特权到PIX，在组建立的底层单击**拒绝不匹配IOS指令**。
3. 在底部选择命令复选框，输入您允许的命令(如Telnet)。
4. 如果您想允许Telnet到达特定站点，请在参数部分输入IP(例如“permit 1.2.3.4“)。要允许Telnet到整个场地，请点击**Permit未列出的参数**。
5. 单击 **submit**。
6. 执行步骤其中每一的1through 5允许命令例如(Telnet、FTP，并且/或者HTTP)。
7. 使用GUI，添加PIX的IP在NAS Configuration部分的。

Livingston RADIUS 服务器配置

添加PIX IP并且锁上到客户端文件。

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

Merit RADIUS 服务器配置

添加PIX IP和密匙给客户端文件。

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

TACACS+ 免费软件服务器配置

```
# Handshake with router--PIX needs 'tacacs-server host #.#.#.# cisco':
key = "cisco"

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

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

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

user = ftponly {
login = cleartext "ftponly"
cmd = ftp {
permit .*
```

```
}
}
```

调试步骤

- 请确保 PIX 配置在添加身份验证、授权和记帐 (AAA) 之前有效。如果您在设立AAA之前不能传输数据流，您以后也将不能传输。
- 启用 PIX 中的日志记录：不应该在高负载系统上使用 **logging console debugging** 命令。可以使用**logging buffered debugging**指令。从**show logging**的输出或**记录日志**命令可能然后被发送到系统日志服务器和被检查。
- 切记调试打开为TACACS+或RADIUS服务器。所有服务器有此选项。

PIX 验证调试示例

PIX 调试 - 身份验证成功 - RADIUS

这是PIX调试的示例与成功验证的：

```
109001: Auth start for user '???' from 171.68.118.100/1116 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 1
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1116 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 1, elapsed 1 seconds
 302001: Built TCP connection 1 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1116
   laddr 171.68.118.100/1116 (bill)
```

PIX 调试 - 身份验证失败（用户名或口令有误）- RADIUS

这是PIX调试的示例与未成功认证的(用户名或密码)。用户看到四个用户名/密码集合。“Error:重试次数超出的”消息最大数显示。

注意： 如果这是FTP尝试，一个尝试允许。对于HTTP，无限重试次数允许。

```
109001: Auth start for user '???' from 171.68.118.100/1132 to 9.9.9.11/23
 109006: Authentication failed for user '' from
   171.68.118.100/1132 to 9.9.9.11/23
```

PIX调试-下来服务器- RADIUS

这是PIX调试的示例用下来服务器。用户看到一次username。服务器“然后暂停”并且请求密码(三次)。

```
109001: Auth start for user '???' from 171.68.118.100/1151 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1151 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
```

PIX 调试 - 身份验证成功 - TACACS+

这是PIX调试的示例与成功验证的：

```
109001: Auth start for user '???' from 171.68.118.100/1200 to 9.9.9.11/23
 109011: Authen Session Start: user 'cse', sid 3
 109005: Authentication succeeded for user 'cse'
   from 171.68.118.100/1200 to 9.9.9.11/23
 109012: Authen Session End: user 'cse', sid 3, elapsed 1 seconds
 302001: Built TCP connection 3 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1200
```

```
  laddr 171.68.118.100/1200 (cse)
```

PIX 调试 - 身份验证失败（用户名或口令有误）- TACACS+

这是PIX调试的示例与未成功认证的(用户名或密码)。用户看到四个用户名/密码集合。“Error:重试次数超出的”消息最大数显示。

注意： 如果这是FTP尝试，一个尝试允许。对于HTTP，无限重试次数允许。

```
109001: Auth start for user '???' from 171.68.118.100/1203 to 9.9.9.11/23
 109006: Authentication failed for user ''
   from 171.68.118.100/1203 to 9.9.9.11/23
```

PIX调试-下来服务器- TACACS+

这是PIX调试的示例用下来服务器。用户看到一次username。立即，“Error:尝试超出的”消息最大数显示。

```
109001: Auth start for user '???' from 171.68.118.100/1212 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1212 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1212 to 9.9.9.11/23
```

增加授权

由于授权是无效没有验证，授权为同一源和目的要求：

```
aaa authorization any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255
tacacs+|radius
```

或者，如果所有三项出局的服务最初验证：

```
aaa authorization http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization
ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius aaa authorization telnet outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 tacacs+|radius
```

PIX 认证和授权调试示例

PIX调试-成功验证和授权- TACACS+

这是PIX调试的示例与成功验证和授权的：

```
109001: Auth start for user '???' from 171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109005: Authentication succeeded for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 5
 109007: Authorization permitted for user 'telnetonly' from
   171.68.118.100/1218 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 5, elapsed 1 seconds
 302001: Built TCP connection 4 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1218
   laddr 171.68.118.100/1218 (telnetonly)
```

PIX调试-成功验证，但是失败授权的- TACACS+

这是PIX调试的示例与成功验证，但是失败的授权的：

```
109001: Auth start for user '???' from 171.68.118.100/1223 to 9.9.9.11/23
 109011: Authen Session Start: user 'httponly', sid 6
 109005: Authentication succeeded for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
 109008: Authorization denied for user 'httponly'
   from 171.68.118.100/1223 to 9.9.9.11/23
```

PIX调试-未成功认证，没尝试的授权- TACACS+

这PIX调试的示例与认证和授权的，但是授权没尝试的归结于未成功认证(用户名或密码)。用户看到四个用户名/密码集合。“Error:超出的重试次数最大数”。消息显示

注意： 如果这是FTP尝试，一个尝试允许。对于HTTP，无限重试次数允许。

```
109001: Auth start for user '???' from 171.68.118.100/1228 to 9.9.9.11/23
 109006: Authentication failed for user '' from 171.68.118.100/1228
   to 9.9.9.11/23
```

PIX Debug authentication/授权，服务器下来- TACACS+

这是PIX调试的示例与认证和授权的。服务器发生故障。用户一次看到用户名。立即，“Error:超出的尝试最大数”。显示。

```
109001: Auth start for user '???' from 171.68.118.100/1237 to 9.9.9.11/23
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109002: Auth from 171.68.118.100/1237 to 9.9.9.11/23 failed
   (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 171.68.118.100/1237
   to 9.9.9.11/23
```

添加记帐

TACACS+

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0: tacacs+

调试查找同样认为是否开/关。然而，在时“构件”，a“启动”计费记录发送。并且，在“卸载时”，a“终止”计费记录发送：

```
109011: Authen Session Start: user 'telnetonly', sid 13
 109005: Authentication succeeded for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109011: Authen Session Start: user 'telnetonly', sid 13
 109007: Authorization permitted for user 'telnetonly'
   from 171.68.118.100/1299 to 9.9.9.11/23
 109012: Authen Session End: user 'telnetonly', sid 13, elapsed 1 seconds
 302001: Built TCP connection 11 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 (telnetonly)
 302002: Teardown TCP connection 11 faddr 9.9.9.11/23 gaddr 9.9.9.10/1299
  laddr 171.68.118.100/1299 duration 0:00:02 bytes 112
```

TACACS+计费记录看起来象此输出(这些是从CiscoSecure UNIX;在Cisco Secure Windows的记录可能逗号分隔的)：

```
Tue Sep 29 11:00:18 1998 redclay cse PIX 171.68.118.103
   start task_id=0x8 foreign_ip=9.9.9.11
```

```
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:00:36 1998 redclay cse PIX 171.68.118.103
   stop task_id=0x8 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=17
   bytes_in=1198 bytes_out=62
 Tue Sep 29 11:02:08 1998 redclay telnetonly PIX 171.68.118.103
   start task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet
 Tue Sep 29 11:02:27 1998 redclay telnetonly PIX 171.68.118.103
   stop task_id=0x9 foreign_ip=9.9.9.11
  local_ip=171.68.118.100 cmd=telnet elapsed_time=19
   bytes_in=2223 bytes_out=64
```

字段划分如被看到此处：

```
DAY MO DATE TIME YEAR NAME_OF_PIX USER SENDER PIX_IP START/STOP
   UNIQUE_TASK_ID DESTINATION SOURCE
   SERVICE <TIME> <BYTES_IN> <BYTES_OUT>
```

RADIUS

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 radius

调试查找同样认为是否开/关。然而，在时“构件”，a“启动”计费记录发送。并且，在“卸载时”，a“终止”计费记录发送：

```
109001: Auth start for user '???' from 171.68.118.100/1316 to 9.9.9.11/23
 109011: Authen Session Start: user 'bill', sid 16
 109005: Authentication succeeded for user 'bill'
   from 171.68.118.100/1316 to 9.9.9.11/23
 109012: Authen Session End: user 'bill', sid 16, elapsed 1 seconds
 302001: Built TCP connection 14 for faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 (bill)
 302002: Teardown TCP connection 14 faddr 9.9.9.11/23 gaddr 9.9.9.10/1316
  laddr 171.68.118.100/1316 duration 0:00:03 bytes 112
```

RADIUS计费记录看起来象此输出(这些是从Cisco Secure UNIX;那个在Cisco Secure Windows逗号分隔的)：

```
Mon Sep 28 10:47:01 1998
Acct-Status-Type = Start
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"

Mon Sep 28 10:47:07 1998
Acct-Status-Type = Stop
Client-Id = 171.68.118.103
Login-Host = 171.68.118.100
Login-TCP-Port = 23
Acct-Session-Id = "0x00000004"
User-Name = "bill"
Acct-Session-Time = 5
```

字段划分如被看到此处：

```
Acct-Status-Type = START or STOP
Client-ID = IP_OF_PIX
Login_Host = SOURCE_OF_TRAFFIC
Login-TCP-Port = #
Acct-Session-ID = UNIQUE_ID_PER_RADIUS_RFC
User-name = <whatever>
```

<Acct-Session-Time = #>

最大会话数与查看登录用户

一些TACACS和RADIUS服务器有最大会话或“显示登陆用户”功能。能力执行最大会话或检查登录用户依靠计费记录。如果有记帐"开始"记录生成，但没有"停止"记录生成时，TACACS或RADIUS服务器假设此人仍在登录(即PIX在传输会话）;有一会话通过PIX)。由于连接性质，它非常适合于Telnet和FTP连接。为例：

用户从171.68.118.100远程登录到9.9.9.25通过PIX，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 171.68.118.100/12
00 to 9.9.9.25/23
(pix) 302001: Built TCP connection 5 for faddr 9.9.9.25/23 gaddr 9.9.9.10/12
00 laddr 171.68.118.100/1200 (cse)
(server start account) Sun Nov  8 16:31:10 1998 rtp-pinecone.rtp.cisco.com
    cse PIX     171.68.118.100  start   task_id=0x3     foreign_ip=9.9.9.25
    local_ip=171.68.118.100     cmd=telnet
```

由于服务器已找到"开始"记录，但没找到“停止”记录(此时此刻)，服务器显示"Telnet"用户在登录。"如果用户尝试另一连接来请求认证(可能来自另一台PC)，并且如果在服务器上为该用户将max-sessions设置为″″1″″，此时服务器拒绝该连接。″

用户在目标主机上处理业务，然后退出主机（在那里花费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
```

uauth是否是的0 (;无论uauth是0 (每次鉴权)或更大值(一次鉴权，并且在uauth 期间不再重复执行)，每个接入站点都将拥有一个记帐记录剪切。

但是HTTP工作不同地由于协议的本质。示例如下：

用户从171.68.118.100浏览到9.9.9.25通过PIX。

```
(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。

注释时间。此下载用一秒钟(少于在开始和终止记录之间的一秒钟有)。用户仍然登陆对的网站和开放的连接？不能。

max-sessions或 view logged-in users在这里是否工作？不，因为在HTTP的连接时间是太短的。"Built" 和"Teardown" (“启动”和“终止”记录) 之间的时间是分秒。因为记录实际上在同一瞬间发生，如果没有“终止”记录，将没有“开始”"记录。每一次处理都会向服务器发送“开始”和“终止”记录，无论uauth是否设置为0或更大值。然而，注册用户最大会话与观点不会工作由于HTTP连接种类。

Except 命令的使用

在我们的网络中，如果我们决定一个流出的用户(171.68.118.100)不需要验证，我们能执行此：

```
aaa authentication any outbound 171.68.118.0 255.255.255.0 9.9.9.11 255.255.255.255 tacacs+ aaa
authentication except outbound 171.68.118.100 255.255.255.255 9.9.9.11 255.255.255.255 tacacs+
```

对 PIX 自身 的 认证

先前的讨论是通过PIX对Telnet (和HTTP，FTP) 数据流进行鉴权。对于4.2.2，对PIX的Telnet连接可能也验证。这里，我们定义了能远程登录到PIX方框的IP ：

```
telnet 171.68.118.100 255.255.255.255
```

然后请供应远程登录密码：**passwd ww**。

添加new命令验证远程登录到PIX的用户：

```
aaa authentication telnet console tacacs+|radius
```

当用户远程登录到 PIX 时，会提示他们输入远程登录口令 (“ww”) 。PIX也请求TACACS+或RADIUS用户名和密码。

修改用户看到的提示

如果添加命令：**鉴别提示YOU_ARE_AT_THE_PIX**，通过PIX的用户将看到顺序：

```
YOU_ARE_AT_THE_PIX [at which point you enter the username] Password:[at which point you enter
the password]
```

在最终目的地的到达时，“用户名：”和“Password:”提示符将显示。此提示只影响通过 PIX 的用户，而不影响转到 PIX 的用户。

注意： 访问PIX的计费记录没有减少。

相关信息

- 思科PIX防火墙软件产品支持
- Cisco Secure PIX 防火墙命令参考
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems