配置PIX 5.0.x ：TACACS+和RADIUS

目录

简介
先决条件
要求
使用的组件
规则
认证与授权
开启验证/授权时用户看到的信息
用于所有情形的服务器安全配置
思科安全UNIX TACACS服务器配置
思科安全UNIX RADIUS服务器配置
思科安全Windows 2.x RADIUS
EasyACS TACACS+
思科安全2.x TACACS+
Livingston RADIUS 服务器配置
Merit RADIUS 服务器配置
调试步骤
网络图
PIX身份验证调试示例PIX身份验证调试示例
出站
入站
PIX 调试 - 身份验证成功 - TACACS+
PIX 调试 - 身份验证失败（用户名或口令有误）- TACACS+
PIX调试 — 能ping通服务器，无响应 — TACACS+
PIX调试 — 无法ping服务器 — TACACS+
PIX 调试 - 身份验证成功 - RADIUS
PIX 调试 - 身份验证失败（用户名或口令有误）- RADIUS
Ping调试 — 可以Ping服务器，守护程序关闭 — RADIUS
PIX调试 — 无法ping服务器或密钥/客户端不匹配 — RADIUS
添加授权
PIX 认证和授权调试示例
PIX调试 — 良好的身份验证和成功的授权 — TACACS+
PIX 调试 - 身份验证成功，授权失败 - TACACS+
添加记帐
TACACS+
RADIUS
Except 命令的使用
最大会话数与查看登录用户

对 PIX 自身进行验证并启用
串行 控制台上的认证
更改用户看到的提示
自定义用户在成功/失败时看到的消息
每用户空闲超时与绝对超时
虚拟 HTTP
虚拟HTTP出站图
PIX配置虚拟HTTP出站
虚拟 Telnet
虚拟Telnet入站图
PIX配置虚拟Telnet入站
TACACS+服务器用户配置虚拟Telnet入站
PIX调试虚拟Telnet入站
虚拟 Telnet 出站
PIX配置虚拟Telnet出站
PIX调试虚拟Telnet出站
虚拟 Telnet 注销
端口授权
PIX 配置
TACACS+ 免费软件服务器配置
在PIX上调试
AAA计费HTTP、FTP和Telnet以外的流量
相关信息

简介

RADIUS和TACACS+认证可能为FTP、Telnet和HTTP连接执行。通常，可以对其他不太常见的TCP 协议进行身份验证。

支持TACACS+授权。RADIUS授权不是。对老版本在PIX 5.0验证、授权和记帐(AAA)上的更改包括针对除HTTP 、FTP和Telnet外的其他数据流的AAA记账。

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。

规则

有关文件规则的更多信息请参见“ 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。

例如，假设您内部有100个用户，并且您只希望其中6个用户能够在网络外部执行FTP、Telnet或HTTP。告诉PIX对出站流量进行身份验证，并在TACACS+/RADIUS安全服务器上为所有六个用户ID。通过简单*的身*份验证，这六个用户可以使用用户名和密码进行身份验证，然后退出。其他94个用户无法外出。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。根据响应，它会打开或拒绝连接。这六个用户可以执行FTP、Telnet或HTTP。

另一方面，假设这三个用户中的一个“Terry”不可信。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*。也就是说，授权*用*户除了验证身份外还能*做什*么工作。当您向PIX添加*授权*时，PIX首先将Terry的用户名和密码发送到安全服务器，然后发送授权请求，告知安全服务器Terry尝试执行的*“命*令”。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** — 浏览器中显示的请求用户名和密码的窗口。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**器会缓存用户名和密码**。如果PIX应该暂停HTTP连接，但它并没有这样做，则很可能进行再次认证，方法是浏览器将缓存的用户名和密码“发射”到PIX，然后将它们转发到认证服务器。PIX Syslog 和/或服务器调试将显示此现象。如果Telnet和FTP似乎工作正常，但HTTP不连接，这是为什么？

用于所有情形的服务器安全配置

思科安全UNIX TACACS服务器配置

切记您有PIX IP地址，或完全合格的域名和CSU.cfg文件密钥。

```
user = ddunlap {
password = clear "rtp"
default service = permit
}

user = can_only_do_telnet {
password = clear "telnetonly"
service = shell {
```

```
cmd = telnet {
permit .*
}
}
}

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

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

思科安全UNIX RADIUS服务器配置

使用图形用户界面(GUI)添加PIX IP和网络接入服务器(NAS)列表密匙。

```
user=adminuser {
radius=Cisco {
check_items= {
2="all"
}
reply_attributes= {
6=6
}
}
```

思科安全Windows 2.x RADIUS

执行下列步骤：

1. 在“用户设置GUI”部分获取密码。
2. 从Group Setup GUI部分，将属性6(Service-Type)设置为Login或Administrative。
3. 在 NAS Configuration GUI 中，添加 PIX IP。

EasyACS TACACS+

EasyACS文档描述设置。

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. 为要**允许的每个命**令（例如，Telnet）选择Add/Edit new command。
4. 如果要允许Telnet至特定站点，请在参数部分以“permit #.#.#.#”的形式输入IP。 要允许Telnet到整个场地，单击**允许所有未列出的参数。**
5. **编辑指令的**单击**完成。**

6. 对每个允许的命令（例如Telnet、HTTP或FTP）执行步骤1到步骤5。
7. 在NAS Configuration GUI部分添加PIX IP。

思科安全2.x TACACS+

用户在“用户设置GUI”部分获取密码。

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. 为要**允许的每个命**令（例如，Telnet）选择Add/Edit new command。
4. 如果要允许Telnet至特定站点，请在参数矩形中输入permit IP(s)（例如，“permit 1.2.3.4”）。要允许Telnet到整个场地，单击**允许所有未列出的参数。**
5. **编辑指令的**单击**完成。**
6. 每个允许命令(如Telnet 、FTP，和/或HTTP)均要执行前面的步骤。
7. 在NAS Configuration GUI部分添加PIX IP。

Livingston RADIUS 服务器配置

将PIX IP和密钥添加到客户端文件。

```
adminuser 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。

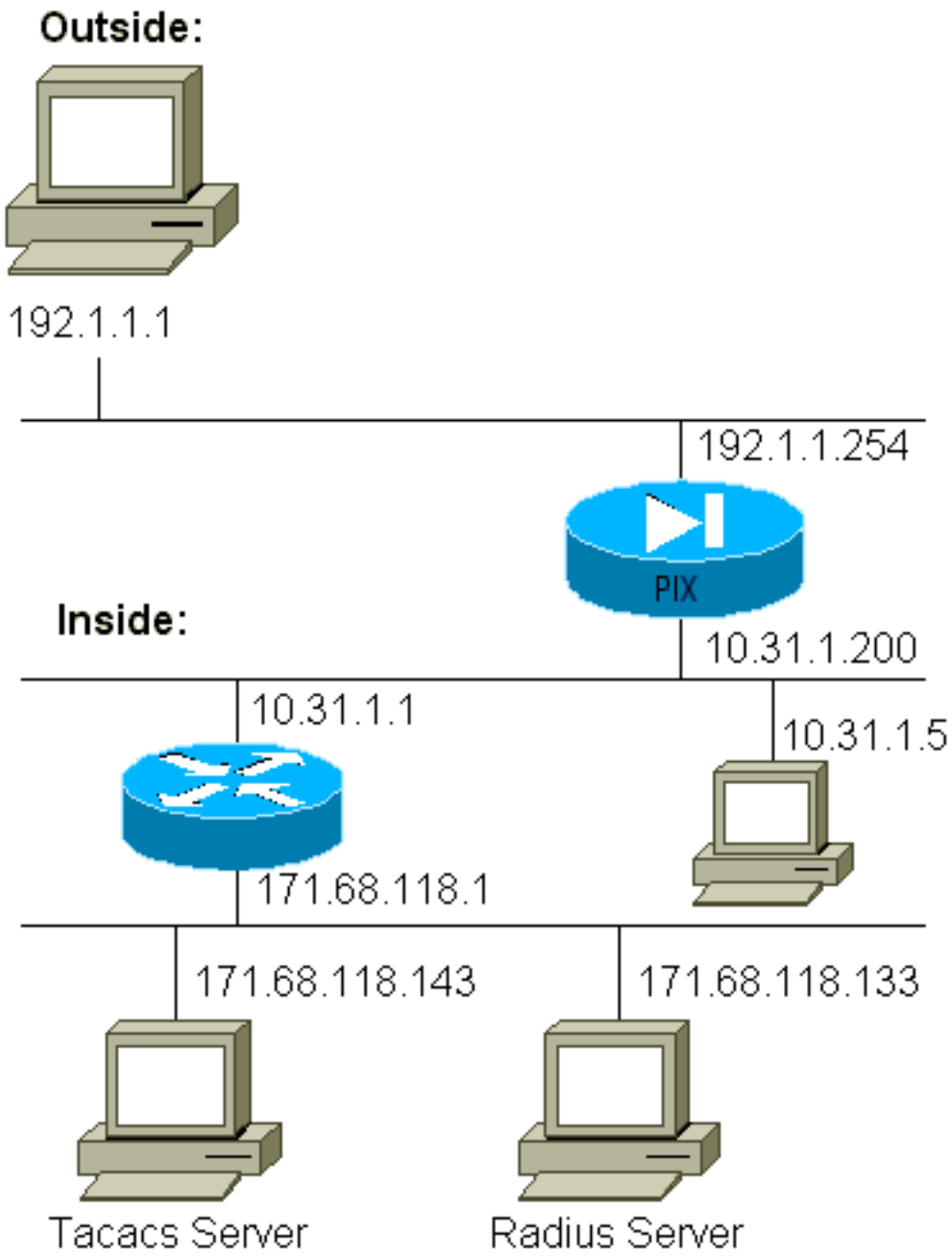
```
adminuser Password="all"
Service-Type = Shell-User

key = "cisco"

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

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

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

user = can_only_do_ftp {
login = cleartext "ftponly"
cmd = ftp {
```

```
permit .*
}
}
```

调试步骤

- 在添加AAA之前，请确保PIX配置有效。如果您在创立认证和授权之前没有通过数据流，您以后便不能执行该操作了。
- 在PIX中启用日志记录在负载**较重的系**统*上不*应使用logging console debugging命令。可以使用**logging buffered debugging指令。**可以将 **show logging 或 logging 命令的输出发送到 Syslog 服务器并进行检查。**
- 切记调试打开为TACACS+或RADIUS服务器。所有服务器有此选项。

网络图



PIX 配置

```
pix-5# write terminal
 nameif ethernet0 outside security0
 nameif ethernet1 inside security100
 enable password 8Ry2YjIyt7RRXU24 encrypted
 passwd 2KFQnbNIdI.2KYOU encrypted
 hostname pixfirewall
 fixup protocol ftp 21
 fixup protocol http 80
 fixup protocol smtp 25
 fixup protocol h323 1720
 fixup protocol rsh 514
 fixup protocol sqlnet 1521
 names
 name 1.1.1.1 abcd
 name 1.1.1.2 a123456789
 name 1.1.1.3 a123456789123456
 pager lines 24
 logging timestamp
 no logging standby
 logging console debugging
 no logging monitor
 logging buffered debugging
 no logging trap
 logging facility 20
 logging queue 512
 interface ethernet0 auto
 interface ethernet1 auto
 mtu outside 1500
 mtu inside 1500
 ip address outside 192.1.1.254 255.255.255.0
 ip address inside 10.31.1.200 255.255.255.0
 no failover
 failover timeout 0:00:00
 failover ip address outside 0.0.0.0
 failover ip address inside 0.0.0.0
 arp timeout 14400
 global (outside) 1 192.1.1.10-192.1.1.20 netmask
255.255.255.0
 static (inside,outside) 192.1.1.25 171.68.118.143
netmask 255.255.255.255 0 0
 static (inside,outside) 192.1.1.30 10.31.1.5 netmask
255.255.255.255 0 0
 conduit permit tcp any any
 conduit permit icmp any any
 conduit permit udp any any
 no rip outside passive
 no rip outside default
 no rip inside passive
 no rip inside default
 route inside 171.68.118.0 255.255.255.0 10.31.1.1 1
 timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
 timeout rpc 0:10:00 h323 0:05:00
 timeout uauth 0:00:00 absolute
 aaa-server TACACS+ protocol tacacs+
 aaa-server RADIUS protocol radius
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.143
cisco timeout 5
 aaa-server AuthOutbound protocol radius
 aaa-server AuthOutbound (inside) host 171.68.118.133
cisco timeout 5
```

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

PIX身份验证调试示例PIX身份验证调试示例

在这些调试示例中：

出站

在10.31.1.5的内部的用户向外192.1.1.1 发出数据流，并通过TACACS+进行验证。出站流量使用服务器列表“AuthOutbound”，其中包括RADIUS服务器171.68.118.133。

入站

在192.1.1.1的外部用户向10.31.1.5 (192.1.1.30)发起数据流，并通过了TACACS的验证。入站流量使用服务器列表“AuthInbound”（包括TACACS服务器171.68.118.143）。

PIX 调试 - 身份验证成功 - TACACS+

此示例显示具有良好身份验证的PIX调试：

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

PIX 调试 - 身份验证失败（用户名或口令有误）- TACACS+

此示例显示PIX调试，身份验证错误（用户名或密码）。 用户看到四个用户名/密码集，并显示消息“Error:次数。”

```
pixfirewall# 109001: Auth start for user '???' from 192.1.1.1/13157
```

```
    to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23
    to 192.1.1.1/13157
```

PIX调试 — 能ping通服务器，无响应 — TACACS+

此示例显示PIX调试，其中服务器可以ping通但不与PIX通信。用户看过用户名，但PIX从不询问密码(这是在Telnet上)。 用户看到“Error:”

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

PIX调试 — 无法ping服务器 — TACACS+

此示例显示服务器无法ping通的PIX调试。用户看过用户名，PIX从不询问密码(这是在Telnet上)。显示以下消息：“Timeout to TACACS+ server”和“Error:次数”（我们在配置中交换了一个伪造服务器）。

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

PIX 调试 - 身份验证成功 - RADIUS

此示例显示具有良好身份验证的PIX调试：

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

PIX 调试 - 身份验证失败（用户名或口令有误）- RADIUS

此示例显示PIX调试，身份验证错误（用户名或密码）。 用户会看到要求输入用户名和口令。用户有三个成功输入用户名/密码的机会。

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

Ping调试 — 可以Ping服务器，守护程序关闭 — RADIUS

此示例显示PIX调试，其中服务器可ping通，但守护程序关闭，并且不与PIX通信。用户看到用户名、密码和消息“RADIUS server failed”和“Error:”

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

PIX调试 — 无法ping服务器或密钥/客户端不匹配 — RADIUS

此示例为PIX调试设置，其中服务器无法ping通或密钥/客户端不匹配。用户看到用户名、密码和消息“Timeout to RADIUS server”“Error：”Max number of tries exceeded”（在配置中交换了伪造服务器）。

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

添加授权

如果您决定添加授权，则需要对相同的源和目标范围进行授权（因为授权在未经身份验证的情况下无效）：

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

请注意，未为“传出”添加授权，因为传出流量使用RADIUS进行身份验证，并且RADIUS授权无效。

PIX 认证和授权调试示例

PIX调试 — 良好的身份验证和成功的授权 — TACACS+

此示例显示具有良好身份验证和成功授权的PIX调试：

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

PIX 调试 - 身份验证成功，授权失败 - TACACS+

此示例显示了身份验证良好但授权失败的PIX调试。在这里，用户也会看到消息“Error:”

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

添加记帐

TACACS+

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

无论记帐是打开还是关闭，调试都看起来相同。但是，在“已构建”时，会发送“开始”会计记录。在“拆除”时，会发送“停止”记帐记录。

TACACS+记帐记录类似于以下输出（这些记录来自Cisco Secure NT，因此采用逗号分隔格式）：

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

RADIUS

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

无论记帐是打开还是关闭，Debug的外观都相同。但是，在“已构建”时，会发送“开始”会计记录。在“拆除”时，会发送“停止”记帐记录。

RADIUS记帐记录类似于此输出(这些来自Cisco Secure UNIX;Cisco Secure NT中的1可以用逗号分隔):

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

Except 命令的使用

在我们的网络中，如果我们确定特定源和/或目标不需要身份验证、授权或记帐，我们可以执行如下输出：

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

如果您正在去除机箱的鉴权而机箱同时具有授权功能，那么您还必须在机箱中取消授权.

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”（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。当生成记帐“开始”记录但没有“停止”记录时，TACACS+或RADIUS服务器假定该人仍登录（通过PIX有会话）。

由于连接性质，它非常适合于Telnet和FTP连接。由于连接的本质这在HTTP上运行的不是很好。在本示例输出中，使用了不同的网络配置，但概念相同。

用户通过 PIX 进行远程登录，正在进行身份验证：

```
(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 171.68.118.100/12 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
```

由于服务器看到“start”记录，但没有“stop”记录（此时），因此服务器显示“Telnet”用户已登录。"如果用户尝试要求认证的另一个连接(可能来自另一台PC)，并且如果在服务器上为该用户设置的最大会话为""1""（假设服器支持最大会话），此时服务器拒绝该连接。"

用户在目标主机上继续进行Telnet或FTP业务，然后退出（在此处花费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0 (每次认证)或更大值(一次认证，并且在uauth 期间不再重复执行)，每个计费记录都被剪切用于每个接入站点。

由于协议的性质，HTTP的工作方式不同。此输出显示HTTP的示例：

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。

开始记录发布于16:35:34，停止记录发布于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）。 用户是否仍要登录到网站，并且在他们读取网页内容时，此连接是否仍然打开？否。最大会话数或查看登录用户是否在此工作？不，因为HTTP的连接时间(“建立”和“拆卸”之间的时间)太短。“启动”和“终止”记录分秒。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。"无论uauth设置为0或更大值，每次处理都有""开始""和""停止""记录发送至服务器。"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。

对 PIX 自身进行验证并启用

前面的讨论介绍如何通过PIX对Telnet（和HTTP、FTP）流*量进行*身份验证。我们确保Telnet至*PIX*工作，*而不*进行身份验证：

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

当用户Telnet到PIX时，会提示他们输入Telnet密码(**ww**)。 然后，PIX还请求TACACS+（在本例中，由于使用“AuthInbound”服务器列表）或RADIUS用户名和密码。如果服务器发生故障，您能用“pix”作为用户名进入PIX，并以特权密码(enable password)（无论何种形式的特权密码）获得访问权限

使用此命令：

```
aaa authentication enable console AuthInbound
```

由于"AuthInbound"服务器列表已被使用，用户被提示使用用户名和密码，并发送到TACACS (本例已使用"AuthInbound" 服务器列表，所以该请求被发送至TACACS服务器)或RADIUS服务器。由于启用认证 信息包与登录认证 信息包相同，假设用户可以通过TACACS或RADIUS登录PIX，那们他们也可以利用相同用户名/密码，通过TACACS或RADIUS启用。此问题已分配Cisco Bug ID CSCdm47044(仅限注册客户)。

串行 控制台上的认证

aaa authentication serial console AuthInbound命令需要进行身份验证验证才能访问PIX的串行控制台。

用户从控制台执行配置命令时，系统日志消息将被剪切(假设PIX被配置来向系统日志主机发送调试级别的系统日志)。 以下是系统日志服务器上显示内容的示例：

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

更改用户看到的提示

如果您有**auth-prompt PIX_PIX_PIX命令**，则通过PIX的用户会看到以下序列：

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

到达最终目标框后，将显示“用户名：”和“密码：”提示。此提示仅影响通过*PIX*的用户，而不*影响*PIX。

注意：没有为访问PIX而剪切的记帐记录。

自定义用户在成功/失败时看到的消息

如果您有以下命令：

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

用户在通过PIX登录失败/成功时看到以下序列：

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

每用户空闲超时与绝对超时

空闲和绝对UAUTH超时，可以按照用户，从TACACS+服务器发出。如果您的网络的所有用户将有同一"超时Uauth"，请勿执行它!但是，如果每个用户需要不同的身份验证，请继续阅读。

在本示例中，**使用timeout uauth 3:00:**00命令。一个人经过身份验证后，他们无需在三小时内重新进行身份验证。但是，如果您使用此配置文件设置用户，并在PIX中启用TACACS AAA授权，则用户配置文件中的空闲和绝对超时将覆盖该用户在PIX中的超时uauth。这不意味着通过PIX的Telnet会话在idle/absolute超时后断开。它只控制是否进行重新身份验证。

此配置文件来自TACACS+免费软件：

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

身份验证后，在PIX上执**行show uauth**命令：

```
pix-5# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'timeout' at 10.31.1.5, authorized to:
    port 11.11.11.15/telnet
    absolute   timeout: 0:02:00
    inactivity timeout: 0:01:00
```

在用户等待一分钟之后，PIX 上的调试会显示：

```
109012: Authen Session End: user 'timeout', Sid 19, elapsed 91 seconds
```

当用户返回到同一目标主机或不同主机时，必须重新进行身份验证。

虚拟 HTTP

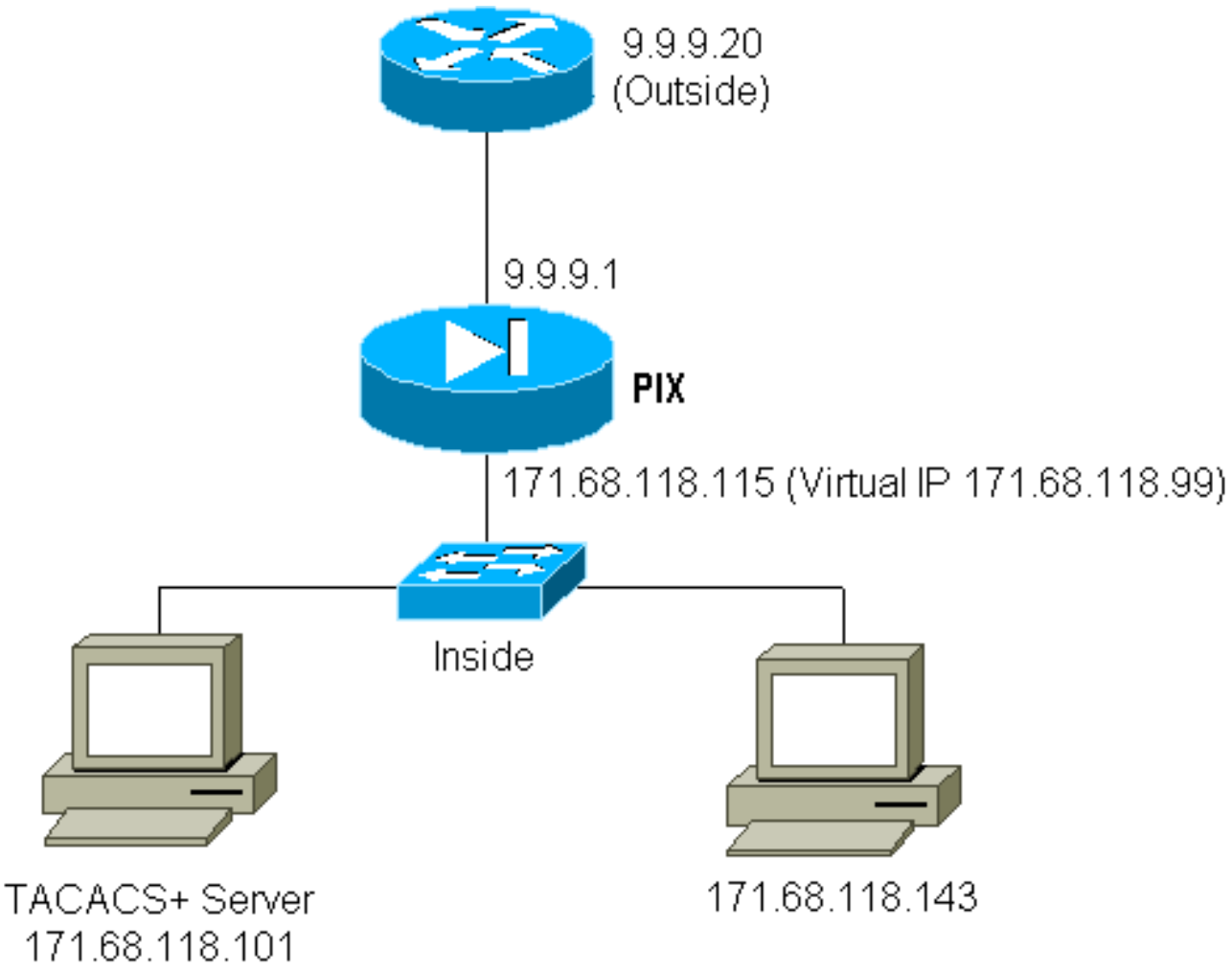
如果PIX外部的站点和PIX自身均要求认证，由于浏览器缓存用户名和密码，所以有时可以观察到浏览器工作异常的情况。

为避免这种情况，您可以使用以下命令将RFC 1918（在Internet上不可路由，但对PIX内部网络有效且唯一的地址）添加到PIX配置中，以实现虚拟HTTP:

```
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。

虚拟HTTP出站图



PIX配置虚拟HTTP出站

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 01:00:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

虚拟 Telnet

可以配置PIX来验证所有入站和出站流量，但是这样做不是个好主意。这是因为某些协议（如“mail”）不易进行身份验证。如果PIX的所有数据流在进行认证时，邮件服务器和客户端试图通过PIX进行通信，这时无法认证的协议在PIX系统日志中显示如下消息：

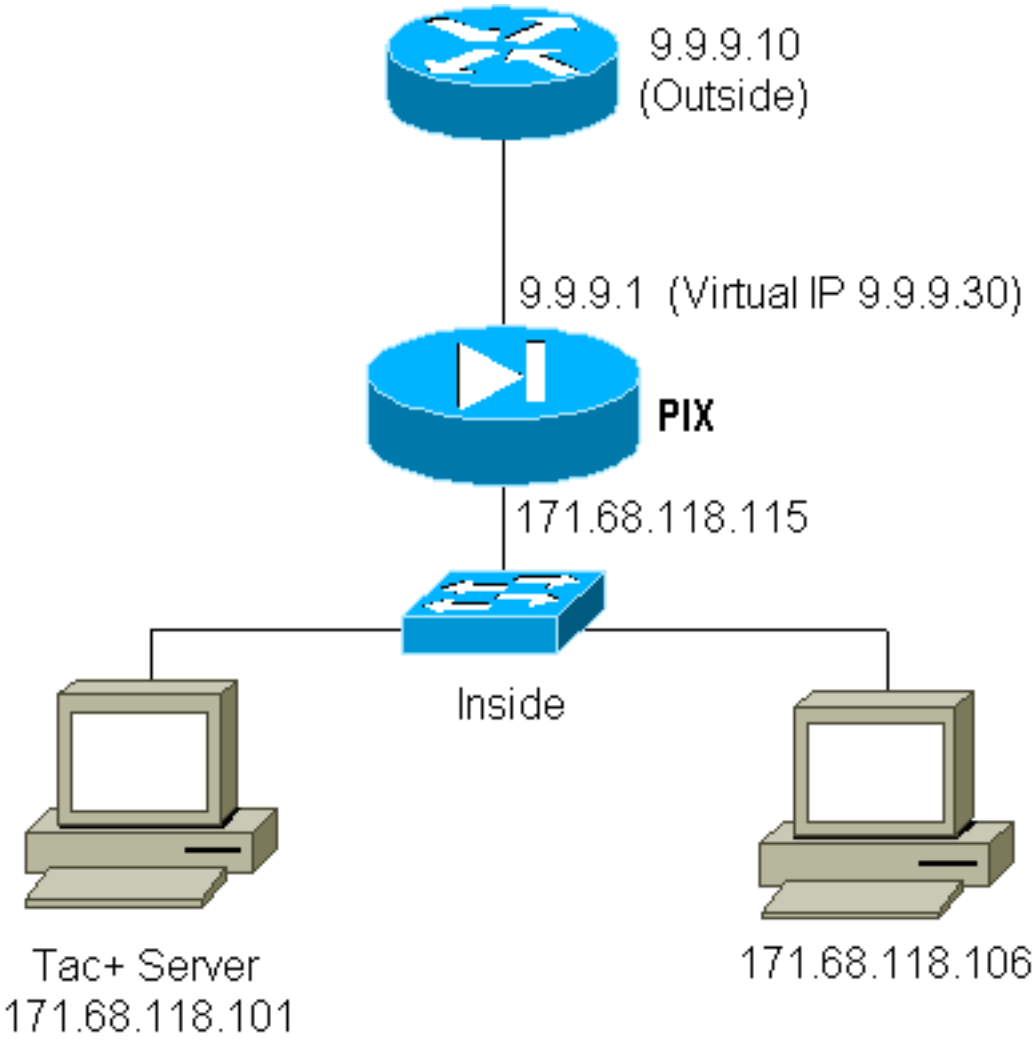
```
109001: Auth start for user '???' from 9.9.9.10/11094
    to 171.68.118.106/25
 109009: Authorization denied from 171.68.118.106/49 to
    9.9.9.10/11094 (not authenticated
```

由于邮件和部分其他服务在认证时互动不充分，这时需要一个特殊命令进行认证和授权(邮件服务器/客户端源/目的地认证除外)。

如果确实需要对某种异常服务进行身份验证，可使用virtual telnet命令**来完**成。此指令允许认证发生到虚拟Telnet IP。经过此身份验证后，异常服务的流量可以转到实际服务器。

在本例中，我们希望TCP端口49流量从外部主机9.9.9.10流到内部主机171.68.118.106。由于此流量实际上不可验证，因此我们设置了虚拟Telnet。对于入站虚拟Telnet，必须存在关联的静态。此处，9.9.9.20和171.68.118.20都是虚拟地址。

虚拟Telnet入站图



PIX配置虚拟Telnet入站

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 static (inside,outside) 9.9.9.20 171.68.118.20 netmask 255.255.255.255 0 0
 static (inside,outside) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.20 eq telnet any
 conduit permit tcp host 9.9.9.30 eq tacacs any
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthInbound protocol tacacs+
 aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
 AAA authentication any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
 virtual telnet 9.9.9.20
```

TACACS+服务器用户配置虚拟Telnet入站

```
user = pinecone {
default service = permit
        login = cleartext "pinecone"
service = exec {
        timeout = 10
        idletime = 10
        }
}
```

PIX调试虚拟Telnet入站

在9.9.9.10的用户首先必须远程登录到PIX的地址9.9.9.20进行验证：

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

"在成功地进行了认证后，show uauth命令显示用户有""time on the meter""："

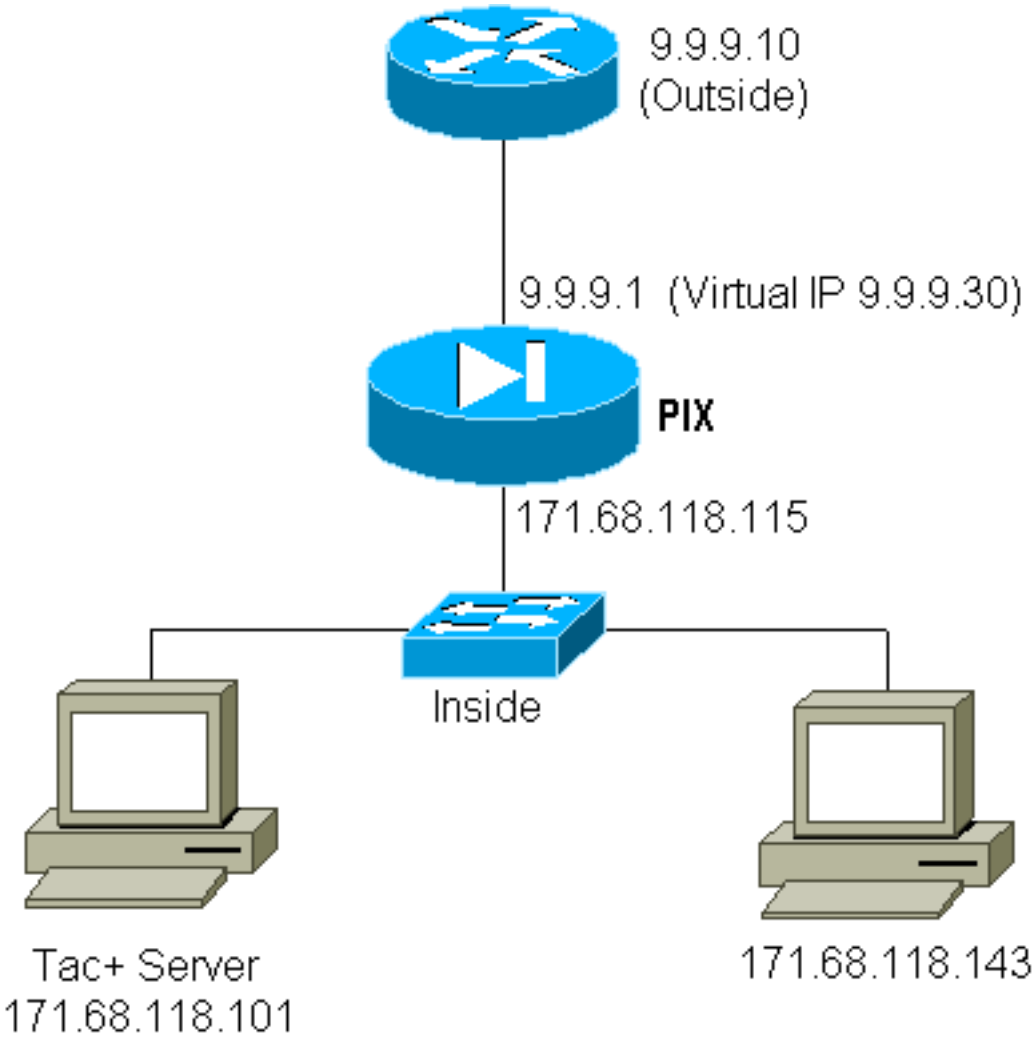
```
pixfirewall# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

此处，9.9.9.10的设备要向171.68.118.106的设备发送TCP/49流量：

```
pixfirewall# 109001: Auth start for user 'pinecone' from 9.9.9.10/11104
     to 171.68.118.20/23
 109011: Authen Session Start: user 'pinecone', Sid 14
 109005: Authentication succeeded for user 'pinecone' from 171.68.118.20/23
     to 9.9.9.10/1470
 302001: Built TCP connection 23 for faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 (pinecone)
 302002: Teardown TCP connection 23 faddr 9.9.9.10/11104 gaddr 9.9.9.30/49
  laddr 171.68.118.106/49 duration 0:00:10 bytes 179 (pinecone)
```

虚拟 Telnet 出站

默认情况下因为出站流量允许，没有静态对于对虚拟Telnet出站的使用是必需的。在本示例中，位于171.68.118.143 Telnet的内部用户到虚拟9.9.9.30并进行身份验证。Telnet 连接立即丢弃。在进行身份验证之后，允许 TCP 流量从 171.68.118.143 流到 9.9.9.10 处的服务器：



PIX配置虚拟Telnet出站

```
ip address outside 9.9.9.1 255.255.255.0
 ip address inside 171.68.118.115 255.255.255.0
 global (outside) 1 9.9.9.5-9.9.9.9 netmask 255.0.0.0
 timeout uauth 00:05:00
 aaa-server TACACS+ protocol tacacs+
 aaa-server AuthOutbound protocol tacacs+
 aaa-server AuthOutbound (inside) host 171.68.118.101 cisco timeout 10
 AAA authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
 virtual telnet 9.9.9.30
```

PIX调试虚拟Telnet出站

```
109001: Auth start for user '???' from 171.68.118.143/1536
     to 9.9.9.30/23
 109011: Authen Session Start: user 'timeout_143', Sid 25
 109005: Authentication succeeded for user 'timeout_143' from
    171.68.118.143/1536 to 9. 9.9.30/23
 302001: Built TCP connection 46 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68 .118.143/1537 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302001: Built TCP connection 47 for faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68 .118.143/1538 (timeout_143)
 302002: Teardown TCP connection 46 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1537 laddr 171.68. 118.143/1537 duration 0:00:03
```

```
    bytes 625 (timeout_143)
 304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
 302002: Teardown TCP connection 47 faddr 9.9.9.10/80 gaddr
    9.9.9.30/1538 laddr 171.68. 118.143/1538 duration 0:00:01
    bytes 2281 (timeout_143)
 302009: 0 in use, 1 most used
```

虚拟 Telnet 注销

当用户Telnet到虚拟Telnet IP时，**show uauth**命令显示uauth。

如果用户希望在会话完成后（在uauth中剩余时间时）阻止流量通过，则用户需要再次Telnet至虚拟Telnet IP。这将断开会话。

端口授权

您可以要求在端口范围内进行授权。在本示例中，所有出站仍需要身份验证，但TCP端口23-49仅需要授权。

PIX 配置

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

从171.68.118.143到9.9.9.10执行Telnet时，由于Telnet端口23在23-49范围内，因此会进行身份验证和授权。

当从171.68.118.143到9.9.9.10完成HTTP会话时，您仍然必须进行身份验证，但PIX不会要求TACACS+服务器授权HTTP，因为80不在23-49范围内。

TACACS+ 免费软件服务器配置

```
user = telnetrange {
        login = cleartext "telnetrange"
        cmd = tcp/23-49 {
        permit 9.9.9.10
        }
        }
```

请注意，PIX将“cmd=tcp/23-49”和“cmd-arg=9.9.9.10”发送到TACACS+服务器。

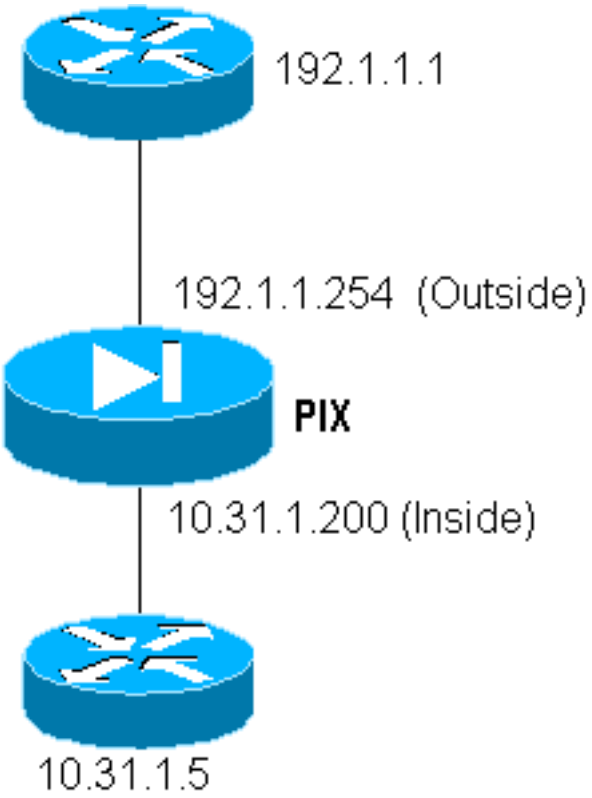
在PIX上调试

```
109001: Auth start for user '???' from 171.68.118.143/1051
    to 9.9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109005: Authentication succeeded for user 'telnetrange'
    from 171.68.118.143/1051 to 9. 9.9.10/23
 109011: Authen Session Start: user 'telnetrange', Sid 0
 109007: Authorization permitted for user 'telnetrange'
```

```
   from 171.68.118.143/1051 to 9.9 .9.10/23
302001: Built TCP connection 0 for faddr 9.9.9.10/23
   gaddr 9.9.9.5/1051 laddr 171.68.1 18.143/1051 (telnetrange)
109001: Auth start for user '???' from 171.68.118.143/1105
   to 9.9.9.10/80
109001: Auth start for user '???' from 171.68.118.143/1110
   to 9.9.9.10/80
109011: Authen Session Start: user 'telnetrange', Sid 1
109005: Authentication succeeded for user 'telnetrange'
   from 171.68.118.143/1110 to 9. 9.9.10/80
302001: Built TCP connection 1 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.1 18.143/1110 (telnetrange)
302001: Built TCP connection 2 for faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.1 18.143/1111 (telnetrange)
302002: Teardown TCP connection 1 faddr 9.9.9.10/80 gaddr 9.9.9.5/1110
 laddr 171.68.11 8.143/1110 duration 0:00:08 bytes 338 (telnetrange)
304001: timeout_143@171.68.118.143 Accessed URL 9.9.9.10:/
302002: Teardown TCP connection 2 faddr 9.9.9.10/80 gaddr 9.9.9.5/1111
 laddr 171.68.11 8.143/1111 duration 0:00:01 bytes 2329 (telnetrange)
```

AAA计费HTTP、FTP和Telnet以外的流量

PIX软件版本5.0更改了流量记帐功能。一旦认证完成，可以削减HTTP、FTP和Telnet数据流以外的其他记账记录。



要通过TFTP将文件从外部路由器(192.1.1.1)复制到内部路由器(10.31.1.5)，请添加虚拟Telnet以打开TFTP 流程通道：

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

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

其次，从192.1.1.1外部路由器远程登录到虚拟IP 192.1.1.30，对允许UDP通过PIX的虚拟地址进行认证。在本示例中，从外部**到内部**启动了copy tftp flash进程：

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

PIX上的每个复制tftp flash（IOS复制期间有三个）都能获得一个计费 记录，并发送到认证服务器上。以下是思科安全Windows上的TACACS记录示例):

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

相关信息

- PIX 命令参考
- PIX 产品支持页面