PIX、TACACS+和RADIUS配置示例：4.4.x

目录

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。基于以前版本的 PIX 4.4.1 身份验证、授权和记帐 (AAA) 中的更改包括：AAA服务器组和故障切换、认证启用及串行控制台访问、接受和拒绝提示消息。

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。

假设您有100个内部用户，并希望只有6个用户能在网络外部执行FTP、Telnet或HTTP。您会告知PIX检验出站流量，并提供TACACS+/RADIUS安全服务器上的所有6个用户ID。基于简单身份验证，可以使用用户名和口令对这 6 个用户进行身份验证，然后传出。其他 94 个用户无法传出。PIX提示用户输入用户名/密码，然后通过用户名和密码进入TACACS+/RADIUS安全服务器（取决于响应情况），打开或拒绝连接。这 6 个用户可以执行 FTP、Telnet 或 HTTP。

不过，这里假设这三个用户之一“Terry”不受信任。您希望允许特里执行FTP，而不是HTTP或者Telnet到外界。这意味着必须添加授权，即除了认证用户是谁之外，还授权哪些用户能做。当我们进行PIX授权时，PIX首先向安全服务器发送特里的用户名和密码，然后发送授权请求，告诉安全服务器特里想执行什么"命令"。"如果已经正确安装服务器，Terry可以允许到达""FTP 1.2.3.4""，但不能在任何地方到达“HTTP""或""Telnet""。"

开启验证/授权时用户看到的信息

当认证/授权开启式设法从里向外(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看似“正常”运行，但却没有HTTP连接，这便是故障原因。

用于所有情形的服务器安全配置

CiscoSecure 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 .*
}
}
}
```

CiscoSecure UNIX RADIUS 服务器配置

使用先进的图形用户界面(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
}
}
```

CiscoSecure NT 2.x RADIUS

完成下面这些步骤。

1. 在 User Setup GUI 部分取得口令。
2. 在 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**（提供 EXEC 权限）。
2. 要在PIX上添加授权，请在组建立的底部单击**Deny unmatched IOS命令**。
3. 针对您要允许的每个命令（例如，Telnet），选择 **Add/Edit new** 命令。
4. 如果您希望允许对特定站点进行 Telnet，请在参数部分以“permit #.#.#.#”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. 针对每个允许的命令（例如，Telnet、HTTP 和/或 FTP）执行步骤 1 到 5。
7. 在NAS Configuration GUI部分添加PIX IP。

CiscoSecure 2.x TACACS+

用户可在 GUI 的 User Setup 部分取得口令。

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. 针对您要允许的每个命令（例如，Telnet），选择 **Add/Edit**。
4. 如果您希望允许对特定站点进行 Telnet，请在参数方框中输入许可的 IP（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. 针对每个允许的命令（例如，Telnet、HTTP 或 FTP）执行步骤 1 到 5。
7. 在NAS Configuration GUI部分添加PIX IP。

Livingston RADIUS 服务器配置

添加PIX IP和密匙给客户端文件。

```
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
```

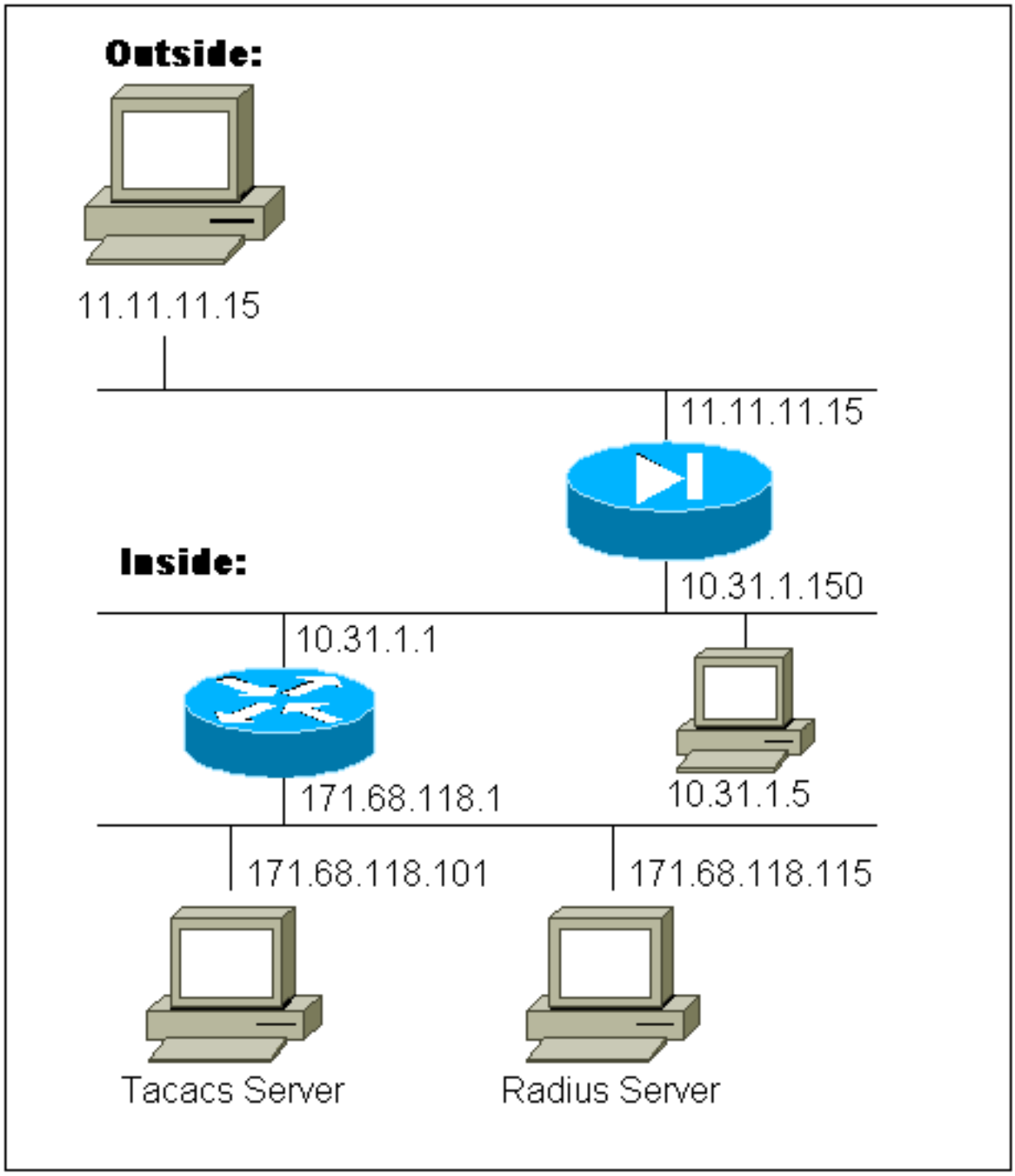
TACACS+ 免费软件服务器配置

```
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

- 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。
- 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。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 Building configuration... : Saved
: PIX Version 4.4(1) nameif ethernet0 outside security0
nameif ethernet1 inside security100 nameif ethernet2
pix/intf2 security10 nameif ethernet3 pix/intf3
security15 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix-5 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 pager lines 24 no
logging timestamp logging console debugging no logging
monitor no logging buffered logging trap debugging
logging facility 20 interface ethernet0 auto interface
ethernet1 auto interface ethernet2 auto interface
ethernet3 auto mtu outside 1500 mtu inside 1500 mtu
pix/intf2 1500 mtu pix/intf3 1500 ip address outside
11.11.11.1 255.255.255.0 ip address inside 10.31.1.150
255.255.255.0 ip address pix/intf2 127.0.0.1
```

```
255.255.255.255 ip address pix/intf3 127.0.0.1
255.255.255.255 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 pix/intf2 0.0.0.0
failover ip address pix/intf3 0.0.0.0 arp timeout 14400
global (outside) 1 11.11.11.10-11.11.11.14 netmask
255.255.255.0 static (inside,outside) 11.11.11.20
171.68.118.115 netmask 255.255.255.255 0 0 static
(inside,outside) 11.11.11.21 171.68.118.101 netmask
255.255.255.255 0 0 static (inside,outside) 11.11.11.22
10.31.1.5 netmask 255.255.255.255 0 0 conduit permit
icmp any any conduit permit tcp any any no rip outside
passive no rip outside default no rip inside passive no
rip inside default no rip pix/intf2 passive no rip
pix/intf2 default no rip pix/intf3 passive no rip
pix/intf3 default route inside 0.0.0.0 0.0.0.0 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 ! !--- For any
given list, multiple AAA servers can !--- be configured.
They will be !--- tried sequentially if any one of them
is down. ! aaa-server Outgoing protocol tacacs+ aaa-
server Outgoing (inside) host 171.68.118.101 cisco
timeout 10 aaa-server Incoming protocol radius aaa-
server Incoming (inside) host 171.68.118.115 cisco
timeout 10 aaa authentication ftp outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authentication http
outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa
authentication telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Outgoing aaa authentication ftp inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa authentication http
inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 Incoming no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps telnet timeout 5 terminal width 80
Cryptochecksum:b287a37a676262275a4201cac52399ca : end
```

PIX 验证调试示例

在这些调试示例中：

出站

"在10.31.1.5的内部用户向外部11.11.11.15发起数据流，并通过TACACS+(出站流量使用包括TACACS服务器171.68.118.101的服务器列表""流出"")进行认证。"

入站

"在11.11.11.15的外部用户向内部10.31.1.5 (11.11.11.22)发起数据流，并通过RADIUS(入站流量使用包括RADIUS 服务器 171.68.118.115的服务器列表 ""Incoming"")进行认证。"

PIX 调试 - 身份验证成功 - TACACS+

下面的示例显示身份验证成功的 PIX 调试：

```
109001: Auth start for user '???' from 10.31.1.5/11004 to 11.11.11.15/23
```

```
 109011: Authen Session Start: user 'ddunlap', sid 3
 109005: Authentication succeeded for user 'ddunlap'
 from 10.31.1.5/11004 to 11.11.11.15/23
 109012: Authen Session End: user 'ddunlap', sid 3, elapsed 1 seconds
 302001: Built outbound TCP connection 4 for faddr 11.11.11.15/23 gaddr
11.11.11.22/11004 laddr 10.31.1.5/11004
```

PIX 调试 - 身份验证失败（用户名或口令有误）- TACACS+

下面的示例显示身份验证失败的 PIX 调试（用户名或口令有误）。用户看到四个用户名/密码集合。显示以下消息：“Error:max number of tries exceeded”。

```
109001: Auth start for user '???' from 10.31.1.5/11005 to 11.11.11.15/23
 109006: Authentication failed for user '' from 10.31.1.5/11005 to 11.11.11.15/23
```

PIX 调试 - 可以 Ping 通，但是无响应 - TACACS+

以下示例显示了不与PIX对话的可PING通服务器的PIX调试。用户看过用户名，但PIX从不询问密码(这是在Telnet上)。

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 10.31.1.5/11006 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 304006: URL Server 171.68.118.101 not responding, trying 171.68.118.101
 109002: Auth from 10.31.1.5/11006 to 11.11.11.15/23 failed
 (server 171.68.118.101 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11006 to 11.11.11.15/23
```

PIX 调试 - 不能 Ping 通服务器 - TACACS+

下面的示例显示不能 ping 通的服务器的 PIX 调试。用户看到一次username。PIX 从不会要求输入口令（这是在 Telnet 上）。显示以下消息：“Timeout to TACACS+ server”和“Error:Max number of tries exceeded”（在本示例中的配置反映了伪装服务器）。

```
109001: Auth start for user '???' from 10.31.1.5/11007 to 11.11.11.15/23
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/11007 to 11.11.11.15/23 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/11007 to 11.11.11.15/23
```

PIX 调试 - 身份验证成功 - RADIUS

下面的示例显示身份验证成功的 PIX 调试：

```
109001: Auth start for user '???' from 11.11.11.15/11003 to 10.31.1.5/23
 109011: Authen Session Start: user 'adminuser', sid 4
 109005: Authentication succeeded for user 'adminuser'
 from 10.31.1.5/23 to 11.11.11.15/11003
 109012: Authen Session End: user 'adminuser', sid 4, elapsed 1 seconds
 302001: Built inbound TCP connection 5 for faddr
 11.11.11.15/11003 gaddr 11.11.11.22/23 laddr 10.31.1.5/23
```

PIX 调试 - 身份验证失败（用户名或口令有误）- RADIUS

下面的示例显示身份验证失败的 PIX 调试（用户名或口令有误）。用户会看到要求输入用户名和口令。如果二者之一是错误的，消息“Incorrect password”会显示四次。然后，用户会断开连接。此问题已分配 Bug ID #CSCdm46934。

```
'Error: Max number of tries exceeded'
 109001: Auth start for user '???' from 11.11.11.15/11007 to 10.31.1.5/23
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11007
```

PIX 调试 - 后台程序关闭，不与 PIX 通信 - RADIUS

下面的示例显示服务器可 ping 通，但是后台程序已关闭的 PIX 调试。服务器不会与 PIX 通信。用户会看到用户名，后面是口令。显示以下消息：“RADIUS server failed”和“Error:Max number of tries exceeded”。

```
109001: Auth start for user '???' from 11.11.11.15/11008 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 304006: URL Server 171.68.118.115 not responding, trying 171.68.118.115
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11008 failed
 (server 171.68.118.115 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11008
```

PIX 调试 - 不能 Ping 通服务器或密匙/客户端不匹配 - RADIUS

下面的示例为不能ping通或密匙/客户端不匹配的服务器显示PIX调试。用户会看到用户名和口令。显示以下消息：“Timeout to RADIUS server”和“Error:Max number of tries exceeded”（该配置中的服务器仅供参考）。

```
109001: Auth start for user '???' from 11.11.11.15/11009 to 10.31.1.5/23
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 304006: URL Server 171.68.118.199 not responding, trying 171.68.118.199
 109002: Auth from 10.31.1.5/23 to 11.11.11.15/11009 failed
 (server 171.68.118.199 failed)
 109006: Authentication failed for user '' from 10.31.1.5/23 to 11.11.11.15/11009
```

增加授权

因为授权无效，没有经过认证，因此我们需要对相同源和目的地范围的授权。

```
aaa authorization ftp outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 aaa authorization http outbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 aaa authorization telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0
```

流出的

"请注意我们不为""incoming""添加授权，因为流入数据流采用RADIUS认证，并且RADIUS授权无效。"

PIX 认证和授权调试示例

PIX 调试 - 身份验证成功和授权成功 - TACACS+

下面的示例显示身份验证成功和授权成功的 PIX 调试：

```
109001: Auth start for user '???' from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109005: Authentication succeeded for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_telnet', sid 7
 109007: Authorization permitted for user 'can_only_do_telnet'
 from 10.31.1.5/11002 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_telnet', sid 7,
 elapsed 1 seconds
 302001: Built outbound TCP connection 6 for faddr 11.11.11.15/23
 gaddr 11.11.11.22/11002 laddr 10.31.1.5/11002 (can_only_do_telnet)
```

PIX 调试 - 身份验证成功，授权失败 - TACACS+

下面的示例显示身份验证成功，但是授权失败的 PIX 调试：

在这里，用户也会看到消息“Error:Authorization Denied”

```
109001: Auth start for user '???' from 10.31.1.5/11000 to 11.11.11.15/23
 109011: Authen Session Start: user 'can_only_do_ftp', sid 5
 109005: Authentication succeeded for user 'can_only_do_ftp'
 from 10.31.1.5/11000 to 11.11.11.15/23
 109008: Authorization denied for user 'can_only_do_ftp' from
 10.31.1.5/11000 to 11.11.11.15/23
 109012: Authen Session End: user 'can_only_do_ftp', sid 5, elapsed 33 seconds
```

增加记账功能

TACACS+

aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
无论记帐是开启还是关闭，调试看上去都相同。但是，在“建立”时，会发送“开始”记帐记录。在“断开”时，会发送“停止”记帐记录。

TACACS+ 记帐记录与下列内容类似（这些内容来自 CiscoSecure UNIX；在 CiscoSecure NT 中的记录可能是逗号分隔的）：

```
Thu Jun  3 10:41:50 1999 10.31.1.150 can_only_do_telnet
 PIX 10.31.1.5 start task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5  cmd=telnet
Thu Jun  3 10:41:55 1999 10.31.1.150 can_only_do_telnet PIX 10.31.1.5
 stop task_id=0x7 foreign_ip=11.11.11.15
local_ip=10.31.1.5 cmd=telnet elapsed_time=4 bytes_in=74 bytes_out=27
```

RADIUS

aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
无论记帐是开启还是关闭，调试看上去都相同。但是，在“建立”时，会发送“开始”记帐记录。在“断开”时，会发送“停止”记帐记录：

RADIUS 记帐记录与下列内容类似：（这些内容来自 CiscoSecure UNIX；在 CiscoSecure NT 中的记录可能是逗号分隔的）：

```
10.31.1.150adminuser -- start server=rtp-evergreen.rtp.cisco.com
```

```
time=14:53:11 date=06/3/1999 task_id=0x00000008
 Thu Jun  3 15:53:11 1999
         Acct-Status-Type = Start
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
 10.31.1.150 adminuser -- stop server=rtp-evergreen.rtp.cisco.com
time=14:54:24 date=06/ 3/1999 task_id=0x00000008
 Thu Jun  3 15:54:24 1999
         Acct-Status-Type = Stop
         Client-Id = 10.31.1.150
         Login-Host = 10.31.1.5
         Login-TCP-Port = 23
         Acct-Session-Id = "0x00000008"
         User-Name = "adminuser"
         Acct-Session-Time = 73
         Acct-Input-Octets = 27
         Acct-Output-Octets = 73
```

Except 命令的使用

在网络中，如果我们决定某个特定的源或目的地不需要认证，授权和计费，可以进行如下操作：

```
aaa authentication except outbound 10.31.1.60 255.255.255.255 11.11.11.15 255.255.255.255
Outgoing aaa authorization except outbound 10.31.1.60 255.255.255.255 11.11.11.15
255.255.255.255 Outgoing
```

如果您要使您的IP地址免于认证，且授权又处于开启状况，那么您必须还让它们免于授权。

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。"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）;"

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。在以下示例中，使用了不同网络配置，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
```

由于服务器已经找到"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（假设服务器支持最大会话）用户设置的最大会话为""1""，此时服务器拒绝该连接。"

用户在目标主机继续Telnet 或FTP业务，然后退出(等待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。

但是，由于协议本质的不同，HTTP 的工作方式也不相同。下面是 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。

开始记录放置在16:35:34，终止记录放置在16:35:35。此下载需要一秒钟（即，开始和停止记录之间少于一秒钟）。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？不能。max-sessions或 view logged-in users在这里是否工作？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 连接的本质，将无法使用最大会话且不能查看登录的用户。

对 PIX 自身进行验证并启用

先前的讨论是通过PIX对Telnet (和HTTP，FTP) 数据流认证。在下面的示例中，我们确保对一下项目不进行认证也可远程登录到PIX

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

然后，我们可以添加命令，对远程登录到 PIX 的用户进行身份验证：

```
aaa authentication telnet console Outgoing
```

当用户远程登录到 PIX 时，会提示他们输入远程登录口令（“ww”）。"在这种情况下，PIX也请求TACACS+ (因为使用了””流出的””服务器列表)或RADIUS用户名及密码。"

```
aaa authentication enable console Outgoing
```

在此命令下，用户被提示使用用户名和密码，并发送到TACACS或RADIUS服务器上。在这种情况下，因为使用了“传出”服务器列表，请求会转到 TACACS 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，那他便可以利用相同用户名/密码，通过TACACS或RADIUS启用认证信息包。此问题已分配 Bug ID #CSCdm47044。

"在服务器发生故障的情形下，用户能够通过输入""PIX""作为用户名，接入PIX特权模式，并从PIX(支持任何密码)获得一般特权密码 。"如果"enable password whatever"不在PIX配置里，用户应该登录"PIX"，查找用户名，然后按Enter键。如果设置特权密码但并不知道，那么将需要密码恢复原盘以便重置。

串行 控制台上的认证

aaa authentication serial console 命令要求先进行身份验证，然后才能访问 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)。下面是 Syslog 服务器的示例：

```
Jun  5 07:24:09 [10.31.1.150.2.2] %PIX-5-111008: User 'cse' executed
the 'hostname' command.
```

修改用户看到的提示

如果我们有命令：

auth-prompt THIS_IS_PIX_5

通过 PIX 的用户会看到序列：

```
THIS_IS_PIX_5 [at which point one would enter the username]
 Password:[at which point one would enter the password]
```

然后，在到达最后的目标框时，“Username:”和“Password:”会提示已显示目标框。

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。

自定义用户看到的成功/失败消息

如果我们有命令：

auth-prompt accept "You're allowed through the pix" auth-prompt reject "You blew it"

用户将通过 PIX 看到有关登录失败/成功的下列消息：

```
THIS_IS_PIX_5
 Username: asjdkl
 Password:
 "You blew it"
 "THIS_IS_PIX_5"
 Username: cse
 Password:
 "You're allowed through the pix"
```

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。如果网络中的所有用户将有同

一个"超时Uauth"，那么请勿执行它!但是，如果您需要对每个用户进行不同的身份验证，请继续读取。

在我们有关 PIX 的示例中，我们使用了 **timeout uauth 3:00:00** 命令。这意味着一旦一个人经过验证，他们将3小时不用重新验证。但如果我们利用下列配置文件设置用户，并在PIX上进行TACACS AAA授权，用户配置文件的空闲和绝对超时设定将覆盖该用户的PIX中的超时Uauth。这不意味着通过PIX的Telnet会话在idle/absolute超时以后断开。它只控制是否重新进行身份验证。

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

在身份验证之后，在 PIX 上发出 **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
```

当返回到同一台目标主机或一台不同的主机时，用户将必须重新授权。

虚拟 HTTP

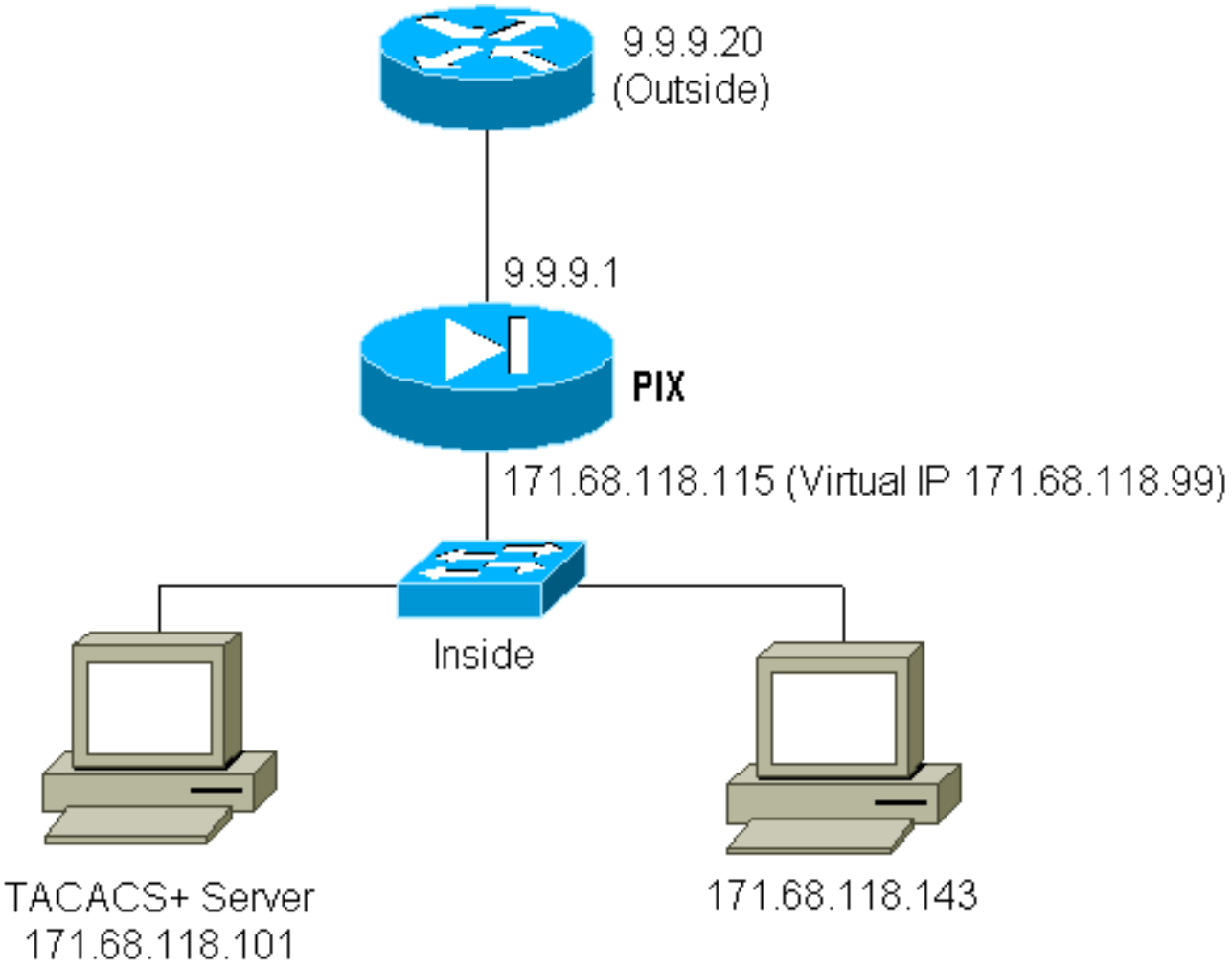
如果PIX外部的站点和PIX自身均要求认证，由于浏览器缓存用户名和密码，所以有时可以观察到浏览器工作异常的情况。

为避免此问题，您可以通过在PIX配置上添加RFC1918地址 (在互联网上不能路由，但对网络内部的PIX是有效的而且是唯一的)来实施虚拟HTTP 。操作命令如下：

```
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。如说明文档中的指示，在使用虚拟 HTTP 时请勿将 **timeout uauth 命令**期限设置为 0 秒；这避免HTTP连接到真正的网络服务器。

虚拟 HTTP 出站示例：



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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 virtual http 171.68.118.99
 auth-prompt THIS_IS_PIX_5
```

虚拟 Telnet

配置PIX，来验证所有入站和出站数据流并不是什么好主意，因为一些协议（如“邮件”）不容易验证。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：

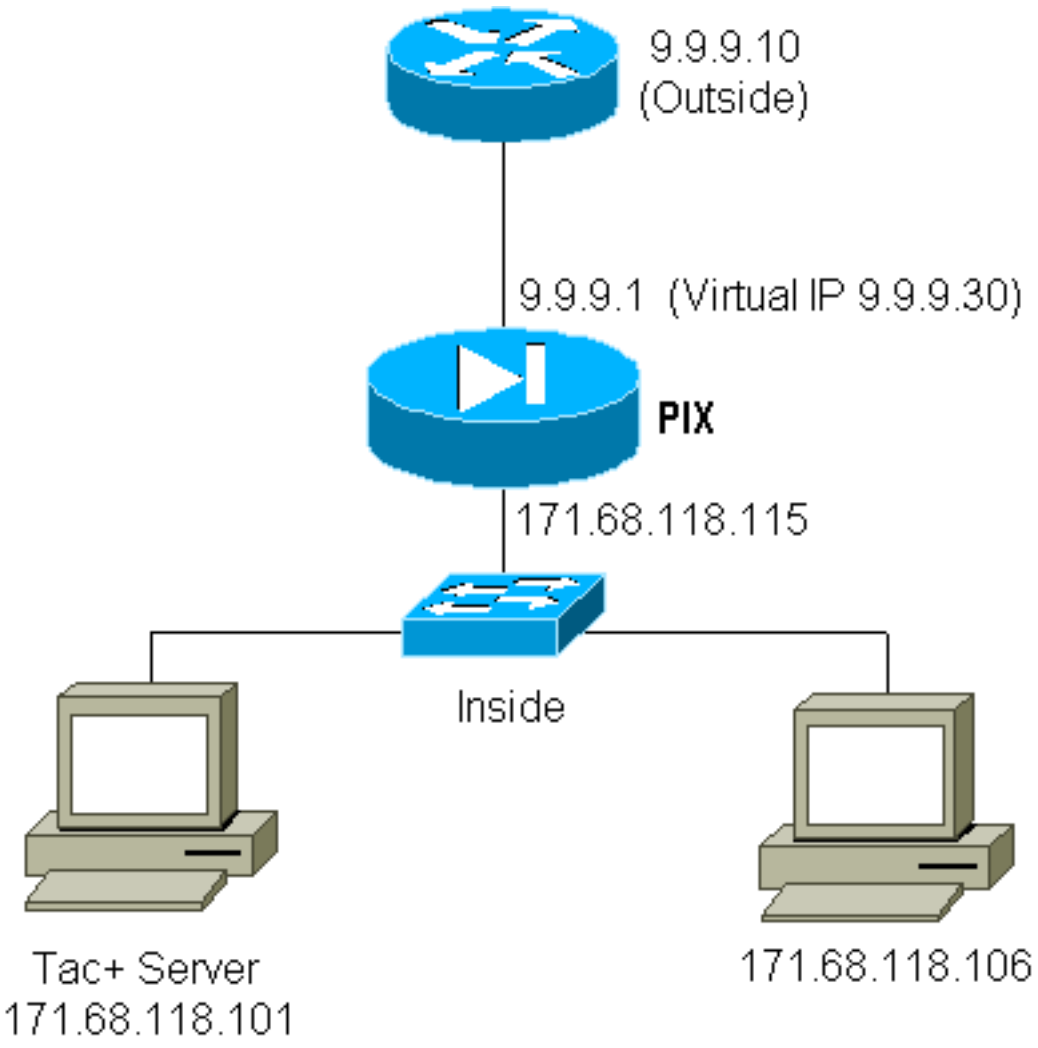
```
109001: Auth start for user '???' from 9.9.9.10/11094 to 171.68.118.106/25
109009: Authorization denied from 171.68.118.106/49 to 9.9.9.10/11094
(not authenticated
```

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)。

但是如果确实需要对部分异常的服务执行验证，这可以利用 virtual telnet 命令完成。此指令允许认证发生到虚拟Telnet IP。经过认证后，特殊服务数据流可以到达与虚拟IP连接的服务器。

在我们的示例中，我们想要允许TCP端口49的数据流从外部主机9.9.9.10流到内部主机171.68.118.106。因为此流量无法进行真正的身份验证，所以我们设置了虚拟 Telnet。

虚拟 Telnet 入站：



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) 9.9.9.30 171.68.118.106 netmask 255.255.255.255 0 0
 conduit permit tcp host 9.9.9.30 host 9.9.9.10
 aaa-server TACACS+ protocol tacacs+
 aaa-server Incoming protocol tacacs+
 aaa-server Incoming (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 Incoming
 virtual telnet 9.9.9.30
```

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的用户必须首先通过远程登录到PIX的9.9.9.30地址进行认证：

```
pixfirewall# 109001: Auth start for user '???' from 9.9.9.10/11099
 to 171.68.118.106/23
 109011: Authen Session Start: user 'pinecone', sid 13
 109005: Authentication succeeded for user 'pinecone' from
 171.68.118.106/23 to 9.9.9.10/11099
```

在成功进行身份验证之后，**show uauth** 命令显示用户“在计量表上有时间显示”：

```
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
```

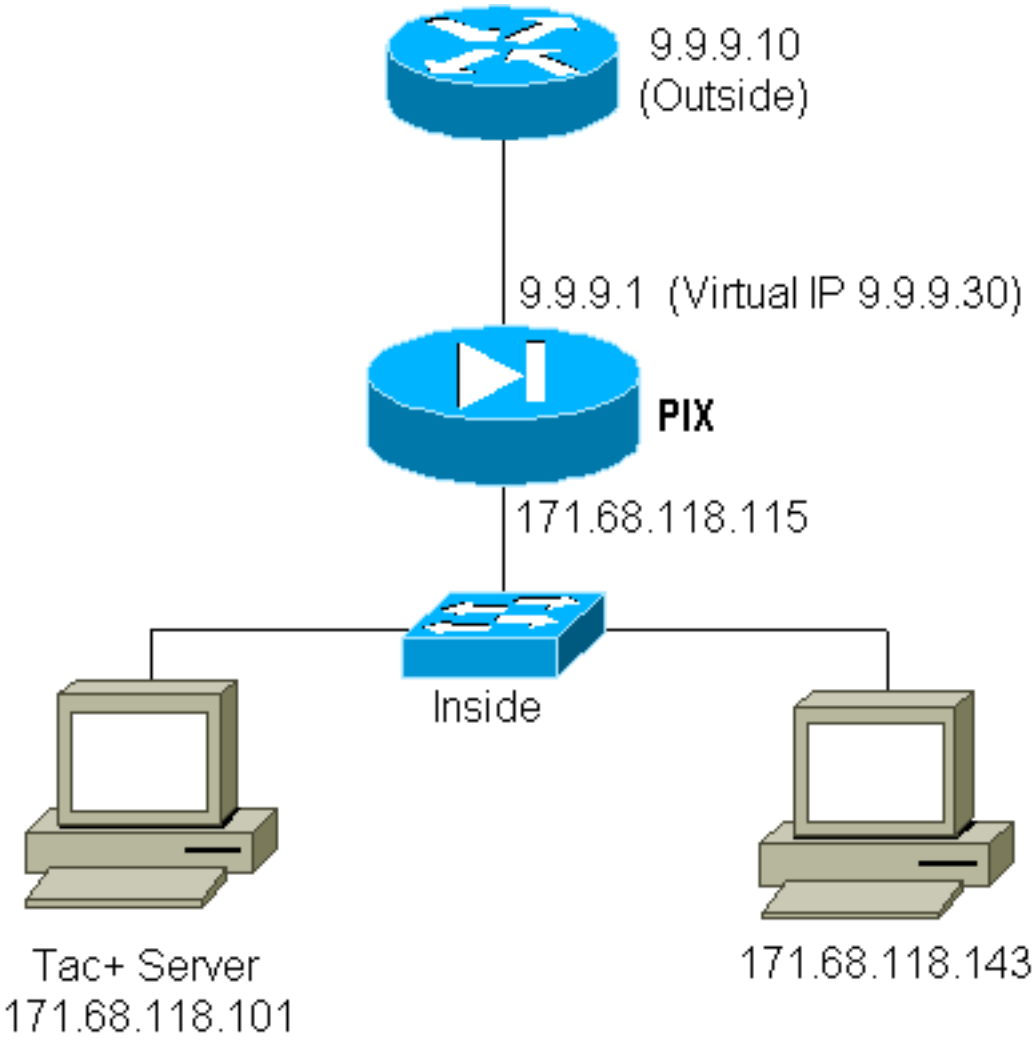
当9.9.9.10地址上的设备要向171.68.118.106上的设备发送TCP/49数据流时：

```
pixfirewall# 109001: Auth start for user 'pinecone'
 from 9.9.9.10/11104 to 171.68.118.106/49
 109011: Authen Session Start: user 'pinecone', sid 14
 109007: Authorization permitted for user 'pinecone' from 9.9.9.10/11104
 to 171.68.118.106/49
 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。在下例中，位于171.68.118.143的内部用户将远程登录到虚拟9.9.9.30并且进行认证。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 Outgoing protocol tacacs+
 aaa-server Outgoing (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 Outgoing
 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

当用户远程登录到虚拟 Telnet IP 时，**show uauth** 命令会显示其用户身份验证情况。如果用户要防止会话结束后(uauth内没有剩余时间)数据流流出，他需要再次远程登录到虚拟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。在下面的例子中，仍然要对所有的出站呼叫进行认证，但只有TCP端口23-49要求授权。

PIX 配置：

aaa authentication any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing

因此，当我们在171.68.118.143和9.9.9.10之间Telnet时，由于Telnet端口23处于23-49之间，所以会发生认证和授权。如果从171.68.118.143向9.9.9.10发起HTTP会话，我们仍必须进行鉴权，但由于80不在23-49范围内，所以PIX不要求TACACS+s服务器对HTTP进行授权。

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 正在将“cmd=tcp/23-49”和“cmd-arg=9.9.9.10”发送到 TACACS+ 服务器。

在 PIX 上的调试：

```
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)
```

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