配置PIX 5.0.x ：TACACS+和RADIUS

Contents

Introduction

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。除HTTP、FTP和Telnet之外，在PIX 5.0验证、授权和统计(AAA)上的变化在老版本包括数据流的Aaa accounting。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

验证和授权

- 认证是谁用户是。
- 授权是什么用户能执行。
- 认证*是*有效的没有授权。
- 授权是*无效*没有认证。

为例，假设您有内部一百个的用户，并且您希望只希望六这些用户能执行FTP、Telnet或者HTTP网络的外部。告诉PIX验证出局流量和产生所有六个用户在TACACS+/RADIUS安全服务器的ID。使用*简单验证*，这六个用户可以用用户名和密码验证，然后出去。其他九十四个用户无法出去。用户名/密码的PIX提示用户，然后通过他们的用户名和密码到TACACS+/RADIUS安全服务器。根据回应，它打开或拒绝连接。这六个用户能执行FTP、Telnet或者HTTP。

另一方面，假设这三个用户之一，“特里”，不是将委托。您希望允许特里执行FTP，但是不是HTTP或者Telnet到外部。这意味着您需要添加*特许*。即核准*什么*用户能执行除验证*谁之*外他们是。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，然后发送告诉的授权请求安全服务器什么“*命令*”特里设法执行。使用适当服务器安装，特里可以允许到“FTP 1.2.3.4”，但是被拒绝对“HTTP”或“Telnet的”能力任何地方。

什么用户看到Authentication/Authorization开启

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，跟随由请求。如果认证(和授权)是成功的在PIX/服务器，提示用户输入用户名和密码由目的地主机以远。
- **FTP** -用户看到用户名提示出来。用户需要输入“local_username@remote_username”用户名和“local_password@remote_password的”密码的。PIX发送“local_username”和“local_password”到本地安全服务器，并且，如果认证(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** -窗口在请求用户名和密码的浏览器显示了。如果认证(和授权)是成功的，用户目的地网站到达以远。记住**浏览器缓存用户名和密码**。如果看来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，然后转发此到认证服务器。PIX系统日志和服务器调试将显示此现象。如果Telnet和FTP似乎正常工作，但是HTTP连接不，这就是为什么。

用于所有情形的服务器安全配置

Cisco Secure UNIX TACACS服务器配置

切记您有PIX IP地址或全限定域名并且锁上在CSU.cfg文件。

```
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 .*
}
}
}
```

Cisco Secure UNIX RADIUS服务器配置

请使用图形用户界面(GUI)添加PIX IP和键到网络接入服务器(NAS)列表。

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

Cisco Secure Windows 2.x RADIUS

执行下列步骤：

1. 得到在User Setup GUI部分的一个密码。
2. 从Group Setup GUI部分，请设置属性6 (服务类型)登陆或管理。
3. 添加在NAS配置GUI的PIX IP。

EasyACS TACACS+

EasyACS文档描述设置。

1. 在组部分，请点击**Shell exec** (产生exec权限)。
2. 要添加特许到PIX，请点击**拒绝不匹配IOS at命令**组建立的底部。
3. 为例如您希望允许的每个命令选择**add/edit new命令**(Telnet)。
4. 如果要允许Telnet到特定站点，请输入IP在参数部分以形式“许可证#.#.#.#”。要允许Telnet到整个场地，请点击**允许所有未列出的参数**。
5. 点击**editing命令的完成**。

6. 执行其中每一的第1步至第5步允许的操作(例如， Telnet、HTTP或者FTP)。
7. 添加在NAS Configuration GUI部分的PIX IP。

Cisco Secure 2.x TACACS+

用户得到在User Setup GUI部分的一个密码。

1. 在组部分，请点击**Shell exec** (产生exec权限)。
2. 要添加特许到PIX，请点击**拒绝不匹配IOS at命令**组建立的底部。
3. 为例如您要允许的每个命令选择**add/edit new命令**(Telnet)。
4. 如果要允许Telnet到特定站点，请送进permit ip在参数方框(例如， “许可证1.2.3.4")。要允许Telnet到整个场地，请点击**允许所有未列出的参数**。
5. 点击**editing命令的完成**。
6. 执行其中每一的早先步骤允许的操作(例如， Telnet、HTTP和FTP)。
7. 添加在NAS Configuration GUI部分的PIX IP。

Livingston RADIUS服务器配置

添加PIX IP并且锁上对客户端文件。

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

Merit RADIUS服务器配置

添加PIX IP并且锁上对客户端文件。

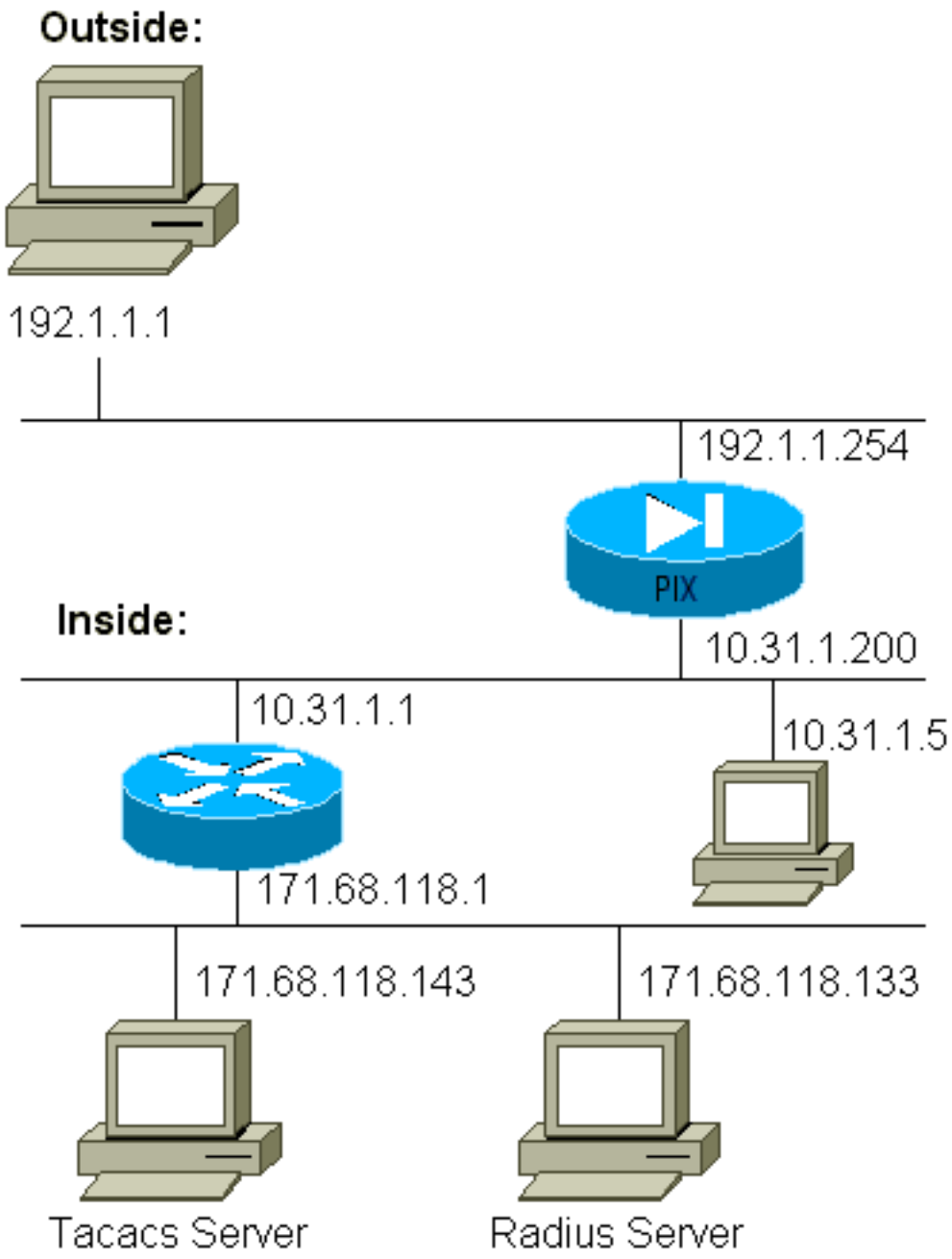
```
adminuser Password="all"
Service-Type = Shell-User

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

- 切记PIX配置工作，在您添加AAA前。如果不能在创立认证和授权前通过数据流，您不能那么之后执行。
- 登陆PIX的Enable (event)在一个高负荷系统不应该使用**logging console debugging命令**。可以使用**logging buffered debugging命令**。**show logging的**输出或**记录**命令可以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。

Network Diagram



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
```

认证从PIXAuthentication调试示例的调试示例从PIX

在这些调试示例中：

outbound

10.31.1.5的内部的用户初始化数据流对外部192.1.1.1和通过TACACS+验证。出局流量使用包括RADIUS服务器171.68.118.133的服务器列表“AuthOutbound”。

入站

192.1.1.1的外部用户初始化数据流对内部的10.31.1.5 (192.1.1.30)和通过TACACS验证。Inbound数据流使用包括TACACS服务器171.68.118.143)的服务器列表“AuthInbound”。

PIX调试-良好的验证- TACACS+

此示例显示与良好的验证的PIX调试：

```
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调试-未成功认证(用户名或密码) - TACACS+

此示例显示与未成功认证的PIX调试(用户名或密码)。用户看到四个用户名/密码集合和消息“”。

```
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调试-能连接服务器，无响应- TACACS+

此示例显示服务器可以连接的PIX调试，但是与PIX不讲话。用户一次看到用户名，但是PIX从未请求密码(这在Telnet)。用户看到“”。

```
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调试-无法连接服务器- TACACS+

此示例显示PIX调试服务器哪里不可ping通的。用户一次看到用户名，但是PIX从未请求密码(这在Telnet)。这些消息显示："TACACS+"和"" (我们交换了在配置的一个伪装服务器)。

```
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调试-良好的验证- RADIUS

此示例显示与良好的验证的PIX调试：

```
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调试-未成功认证(用户名或密码) - RADIUS

此示例显示与未成功认证的PIX调试(用户名或密码)。用户为用户名和密码看到请求。用户有成功的用户名/密码条目的三个机会。

```
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
```

Ping调试-能连接服务器，守护程序下来- RADIUS

此示例显示PIX调试服务器哪里可ping通的，但是守护程序发生故障和不会与PIX联络。用户看到用户名、密码和消息“RADIUS”和“”。

```
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调试-无法连接服务器或键/客户端不匹配- RADIUS

此示例穿上鞋子服务器不可ping通的PIX调试或有键/客户端不匹配。用户看到用户名、密码和消息“RADIUS”和“” (伪装服务器被交换了配置)。

```
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
```

添加特许

如果决定添加特许，您为同一个源及目的地范围将需要授权(因为授权是无效没有认证)：

```
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
```

注意特许没有为“流出”被添加，因为流出的数据流用RADIUS验证，并且RADIUS授权无效。

认证和授权从PIX的调试示例

PIX调试-良好的验证和成功的授权- TACACS+

此示例显示与良好的验证和成功的授权的PIX调试：

```
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
```

PIX调试-良好的验证，失败的授权- TACACS+

此示例显示PIX调试与良好的验证，但是与失败的授权。这里用户也看到消息“”。

```
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
```

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
```

调试查看同样认为是否开/关。然而，在时“构件”， a “启动”计费记录被发送。在“卸载时”， a “发送终止”计费记录。

TACACS+计费记录看起来象此输出因此(这些是从CiscoSecure NT，逗号分隔的格式) ：

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

RADIUS

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

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

RADIUS计费记录看起来象此输出(这些是从Cisco Secure UNIX;部分在CiscoSecure NT可能逗号分隔的) ：

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

Except命令的使用

在我们的网络中，如果我们决定一个特定来源和目的地不需要认证，授权或者认为，我们能执行输出的如此物：

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

如果是“除了”从认证的一个机箱并且有授权，您必须也除去从授权的机箱。

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陆的用户依靠计费记录。当有记帐“启动”记录生成的，但是没有“终止”记录时， TACACS+或RADIUS服务器假设人仍然登陆(有一次会话通过PIX)。

这为Telnet和FTP连接工作良好由于连接的本质。这不为HTTP工作良好由于连接的本质。在此输出示例中，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：

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

因为服务器未看到“启动”记录，但是“终止”记录(此时此刻)，服务器表示， “Telnet”用户登陆。或许如果用户尝试要求认证的另一连接(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。

用户连同Telnet或FTP业务在目标主机，然后退出(度过10分钟那里) ：

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

uauth是否是0 (每次请验证)或更多(一次和不再请验证在uauth期间)，计费记录为被获取的每个站点被削减。

HTTP工作不同地由于协议的本质。此输出显示HTTP的示例：

用户从171.68.118.100访问到9.9.9.25通过PIX ：

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

用户读下载的网页。

开始记录被张贴在16:35:34和终止记录被张贴在16:35:35。此下载用一秒钟(即少于在开始和终止记录之间的一秒钟有)。当他们读网页时，用户仍然登陆对的网站和开放的连接？No.注册用户最大会话或观点是否将运作得这里？不，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“终止”记录，将没有“启动”记录。将有“开始”，并且“请终止”记录被发送到每处理的服务器， uauth是否为更大0或事设置。然而，注册用户最大会话与观点不工作由于HTTP连接种类。

在PIX的认证并启用

先前的讨论描述验证Telnet (和HTTP， FTP)数据流*通过*PIX。我们确定Telnet*对*PIX工作，*不用*认证：

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

```
aaa authentication telnet console AuthInbound
```

当用户远程登录到PIX时，提示他们输入远程登录密码(**ww**)。然后PIX也请求TACACS+ (在这种情况

下，因为使用“AuthInbound”服务器列表)或RADIUS用户名和密码。如果服务器发生故障，您能进入PIX通过输入用户名的**PIX**，特权密码(**无论何种形式的特权密码**)然后获得访问。

用此命令：

```
aaa authentication enable console AuthInbound
```

提示用户输入用户名和密码，被发送到TACACS (在这种情况下，因为使用“AuthInbound”服务器列表，请求去TACACS服务器)或RADIUS服务器。因为enable (event)的认证信息包是相同的象登录的认证信息包，如果用户能登录到与TACACS或RADIUS的PIX，他们通过TACACS或RADIUS能enable (event)用相同用户名/密码。此问题分配Cisco Bug ID CSCdm47044 (仅限注册用户)。

在串行控制台的认证

aaa authentication serial console AuthInbound命令要求验证认证为了访问PIX的串行控制台。

当用户执行从控制台时的配置命令，系统消息被削减(PIX配置假设发送系统日志在调试级别到系统日志主机)。这是什么的示例在系统日志服务器显示：

```
aaa authentication enable console AuthInbound
```

更改用户看到的提示

如果有**auth-prompt PIX_PIX_PIX命令**，通过PIX的用户看到此顺序：

```
aaa authentication enable console AuthInbound
```

在最后目的地设备的到达时，“用户名：”并且“密码：”提示显示。此提示影响去*通过*PIX，不PIX的只有用户。

Note: 没有为对PIX的访问削减的计费记录。

定制消息用户看到在成功/故障

如果有命令：

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

用户通过PIX看到在一个失败/成功的登录的此顺序：

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

单个用户的空闲和绝对超时

空闲和绝对UAUTH超时可以逐个用户从TACACS+服务器被发送下来。如果您的网络的所有用户将有同样“超时Uauth”，请勿实现此!但是，如果需要单个用户不同的uauth，请继续读。

在本例中，使用**timeout uauth 3:00:00命令**。一旦人验证，他们不必须重新鉴别三小时。然而，如果设置有此配置文件的一个用户并且有TACACS AAA授权在PIX，空闲和绝对超时在用户配置文件改写超时Uauth在PIX该用户的。这不意味着远程登录会话通过PIX在空闲/绝对超时以后是断开的。它控制再验证是否发生。

此配置文件来自TACACS+免费软件：

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

在认证以后，请执行一**show uauth命令**在PIX ：

```
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
```

在用户坐一分钟的后空闲，在PIX的调试显示：

```
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
```

当它回到同一台目标主机或一台不同的主机时，用户必须重新鉴别。

虚拟HTTP

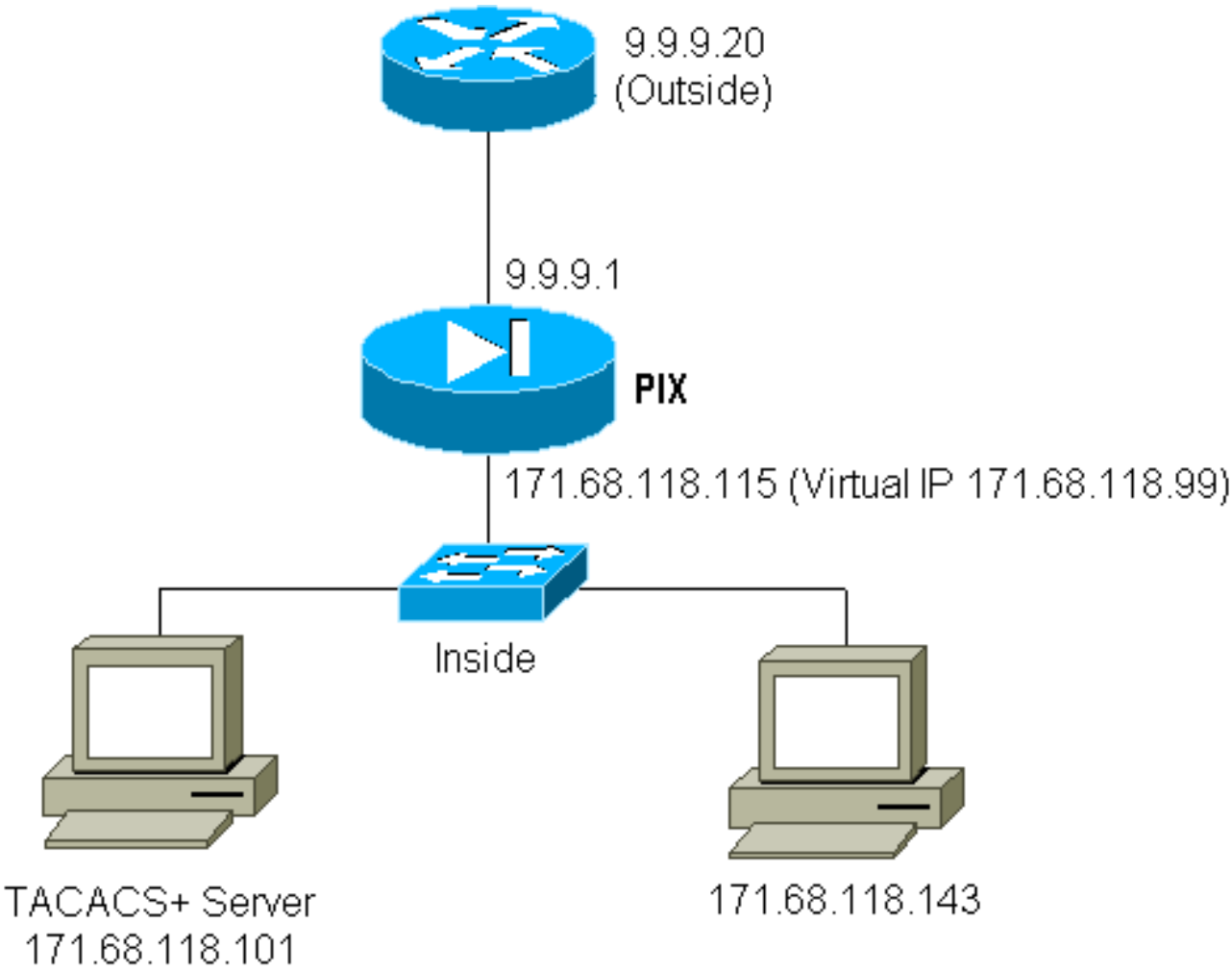
如果认证需要在站点PIX的外部，以及在PIX，异常浏览器行为可能从浏览器缓存有时被观察用户名和密码。

要避免此，您能通过添加RFC 1918地址实现虚拟 HTTP (是不能路由的在互联网的一地址，但是有效和唯一为PIX内部网络)使用此命令，到PIX配置：

```
virtual http #.#.#.# [warn]
```

当用户设法PIX的外部时去，需要认证。如果警告参数存在，用户收到重定向消息。认证是有效对于时间长度在uauth。如文档所示，请勿设置**timeout uauth命令**期限为0与虚拟HTTP的秒。这防止与真正的网络服务器的HTTP连接。

虚拟HTTP出站图表



PIX配置虚拟HTTP出站

```
virtual http #.#.#.# [warn]
```

Virtual telnet

配置PIX验证所有Inbound与Outbound数据流是可能的，但是它不是一个好想法如此执行。这是因为一些协议，例如“邮件”，没有容易验证。当邮件服务器和客户端设法通过PIX时沟通，当所有数据流通过PIX验证时，未经证实的协议的PIX系统日志表示消息例如：

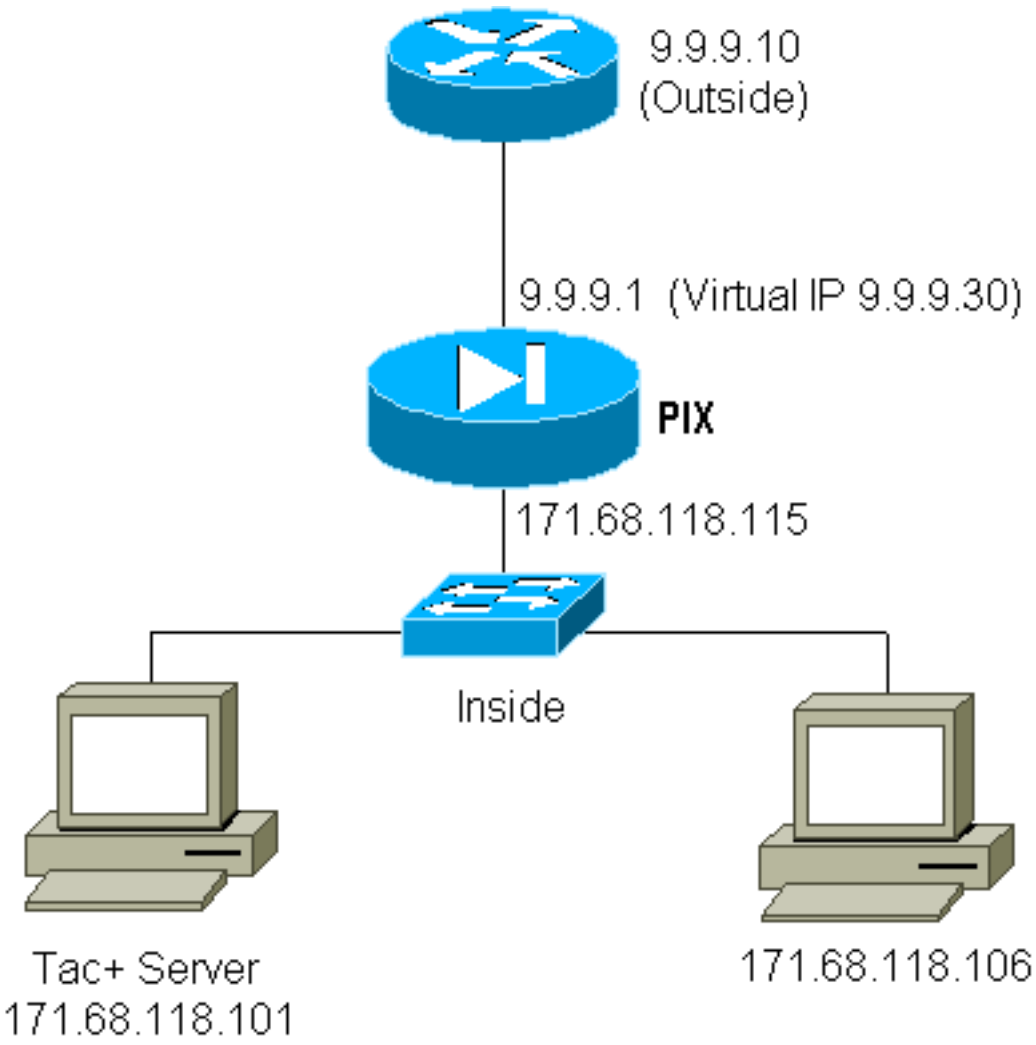
```
virtual http #.#.#.# [warn]
```

因为邮件和一些其他服务不是足够交互验证，一个解决方案将使用**except命令**认证/授权(请验证所有除了邮件服务器/客户端的来源/目的地)。

如果有验证的实际需求特殊服务，这可以利用**virtual telnet命令**执行。此命令允许认证发生到虚拟Telnet IP。在此认证以后，特殊服务的数据流可以去真实服务器。

在本例中，我们希望TCP端口49数据流从外部主机9.9.9.10流到内部主机171.68.118.106。因为此数据流不确实authenticatable，我们设置virtual telnet。入站virtual telnet，必须有相关的静态。这里，9.9.9.20和171.68.118.20是虚拟地址。

虚拟Telnet入站图表



PIX配置虚拟Telnet入站

```
virtual http #.#.#.# [warn]
```

入站TACACS+的服务器用户配置虚拟Telnet

```
virtual http #.#.#.# [warn]
```

PIX调试虚拟Telnet入站

9.9.9.10的用户必须通过远程登录首先验证到在PIX的9.9.9.20地址：

```
virtual http #.#.#.# [warn]
```

在成功的验证以后， **show uauth命令**表示，用户有“在公尺的时间”：

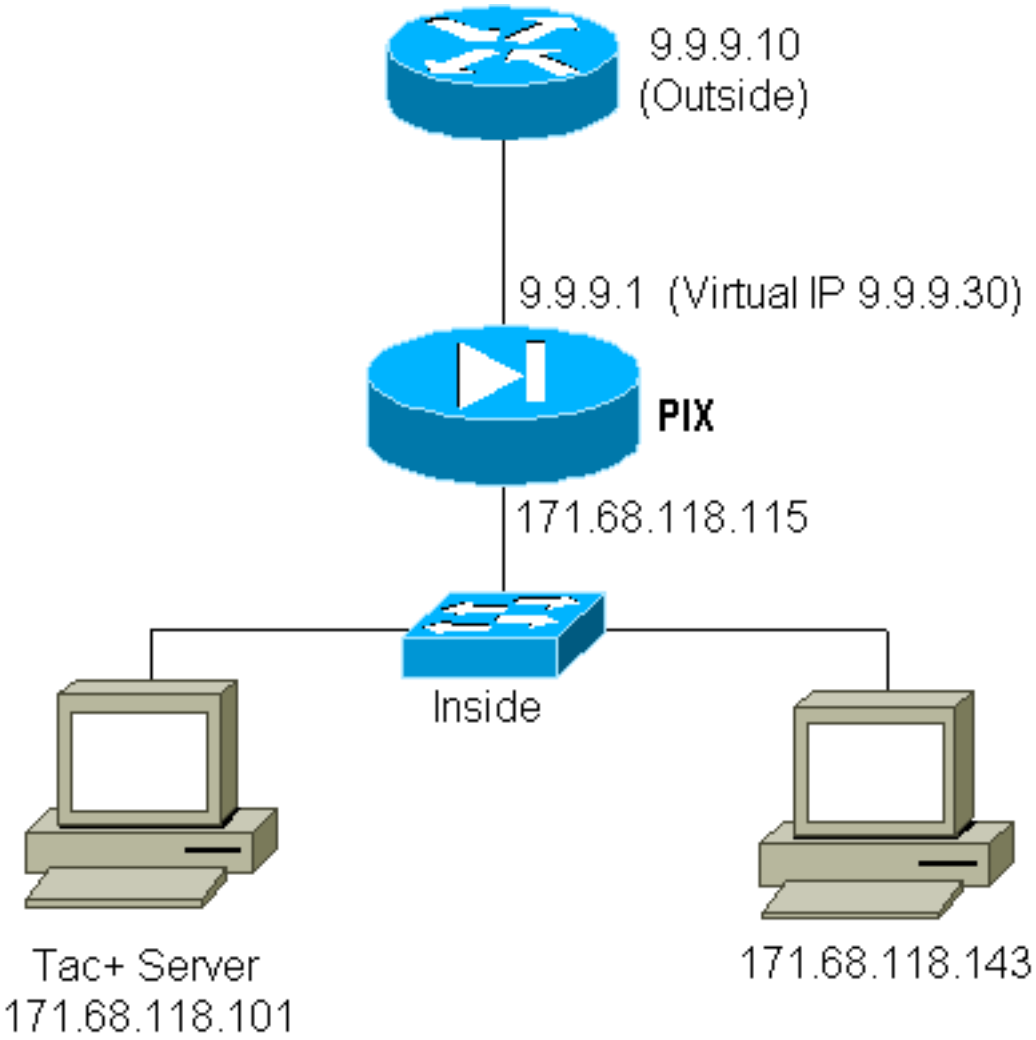
```
pixfirewall# show uauth
                        Current    Most Seen
 Authenticated Users       1          1
 Authen In Progress        0          1
 user 'pinecone' at 9.9.9.10, authenticated
    absolute   timeout: 0:10:00
    inactivity timeout: 0:10:00
```

这里，在9.9.9.10的设备要发送TCP/49数据流到设备在171.68.118.106 ：

```
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
```

虚拟Telnet出站

默认情况下因为出局流量允许，没有静态对于使用虚拟Telnet出站是必需的。在本例中，171.68.118.143的内部的用户远程登录到虚拟9.9.9.30并且验证。Telnet连接立即切。一旦验证，TCP通信流从171.68.118.143允许到在9.9.9.10的服务器：



PIX配置虚拟Telnet出站

```
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
```

PIX调试虚拟Telnet出站

```
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
```

虚拟Telnet注销

当用户远程登录到虚拟Telnet IP时， **show uauth命令**显示uauth。

如果用户要防止数据流经历，在会话完成后(当有在uauth留给的时间)，用户需要再远程登录到虚拟

Telnet IP。这再按乒乓键会话。

端口认证

您能需要在端口范围的授权。在本例中，认证对于所有outbound仍然是必需的，但是仅授权对于TCP端口是必需的23-49。

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
```

当Telnet从171.68.118.143执行到9.9.9.10，认证和授权出现，因为Telnet端口23在23-49范围。

当HTTP会话从171.68.118.143完成到9.9.9.10时，您必须仍然验证，但是PIX不请求TACACS+服务器核准HTTP，因为80不在23-49范围。

TACACS+免费软件服务器配置

```
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
```

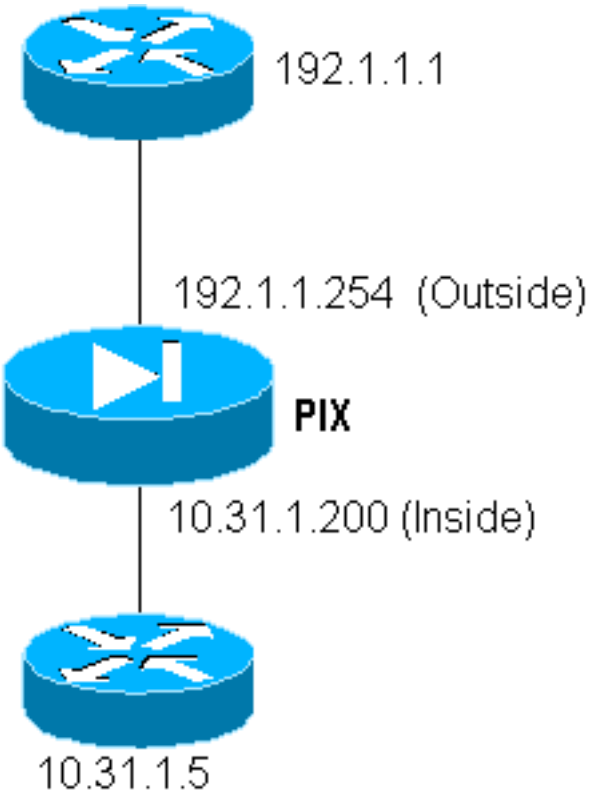
注意PIX发送“cmd=tcp/23-49"和“cmd-arg=9.9.9.10"到TACACS+服务器。

在PIX的调试

```
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
```

数据流的Aaa accounting除HTTP、FTP和Telnet之外

PIX软件版本5.0更改数据流记帐功能。一旦认证完成，除HTTP、FTP和Telnet之外，计费记录可能为数据流当前被削减。



从外部路由器(192.1.1.1)要TFTP副本文件到内部路由器(10.31.1.5)，请添加virtual telnet打开TFTP进程的一个孔：

```
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，从外部路由器的Telnet在对虚拟IP 192.1.1.30的192.1.1.1和验证对允许UDP横断PIX的虚拟地址。在本例中， **copy tftp flash**进程开始了从外向里：

```
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
```

对于在PIX的每**copy tftp flash** (有三在此IOS复制期间)，计费记录被削减并且被发送到认证服务器。以下一个TACACS记录的示例在Cisco Secure Windows)的：

```
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
```

Related Information

- pix命令参考资料
- PIX 产品支持页面