PIX、TACACS+和RADIUS配置示例：4.4.x

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
验证和授权
什么用户看到Authentication/Authorization开启
用于所有情形的服务器安全配置
CiscoSecure UNIX TACACS服务器配置
CiscoSecure UNIX RADIUS服务器配置
CiscoSecure NT 2.x RADIUS
EasyACS TACACS+
CiscoSecure 2.x TACACS+
Livingston RADIUS服务器配置
Merit RADIUS服务器配置
TACACS+免费软件服务器配置
调试步骤
Network Diagram
PIX验证调试示例
添加特许
认证和授权从PIX的调试示例
增加记帐功能
TACACS+
RADIUS
Except命令的使用
最大会话数与查看登录用户
在PIX的认证并启用
在串行控制台的认证
更改提示用户看见
定制消息用户请参阅在成功/故障
单个用户的空闲和绝对超时
虚拟HTTP
Virtual telnet
虚拟Telnet注销
端口认证
Related Information

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。在PIX 4.4.1验证、授权和统计(AAA)上的变化在老版本包括：AAA服务器组和故障切换， enable (event)和串行控制台访问的认证，和接受并且拒绝及时消息。

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。

假设您有内部100个的用户，并且您希望只希望6这些用户能执行FTP、Telnet或者HTTP网络的外部。您会告诉PIX验证出局流量和产生所有6个用户在TACACS+/RADIUS安全服务器的ID。使用简单验证，这6个用户可能用用户名和密码验证，然后出去。其他94个用户不可能出去。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安全服务器和根据回应，打开或拒绝连接。这6个用户可能执行FTP、Telnet或者HTTP。

但是请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。这意味着必须添加特许，即，核准什么用户能执行除验证谁之外他们是。当我们添加特许到PIX时， PIX首先将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，特里可能允许到“FTP 1.2.3.4”，但是会拒绝了能力对任何地方HTTP或Telnet。

什么用户看到Authentication/Authorization开启

当设法去从里向外(或反之亦然)时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 -窗口在浏览器请求用户名和密码显示。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

CiscoSecure 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 .*
}
}
}
```

CiscoSecure UNIX RADIUS服务器配置

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

```
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. 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. 对添加特许到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和FTP)。
7. 添加在NAS Configuration GUI部分的PIX IP。

CiscoSecure 2.x TACACS+

用户得到在GUI的User Setup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. 选择为例如您要允许的每个命令**添加/编辑**(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。

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
```

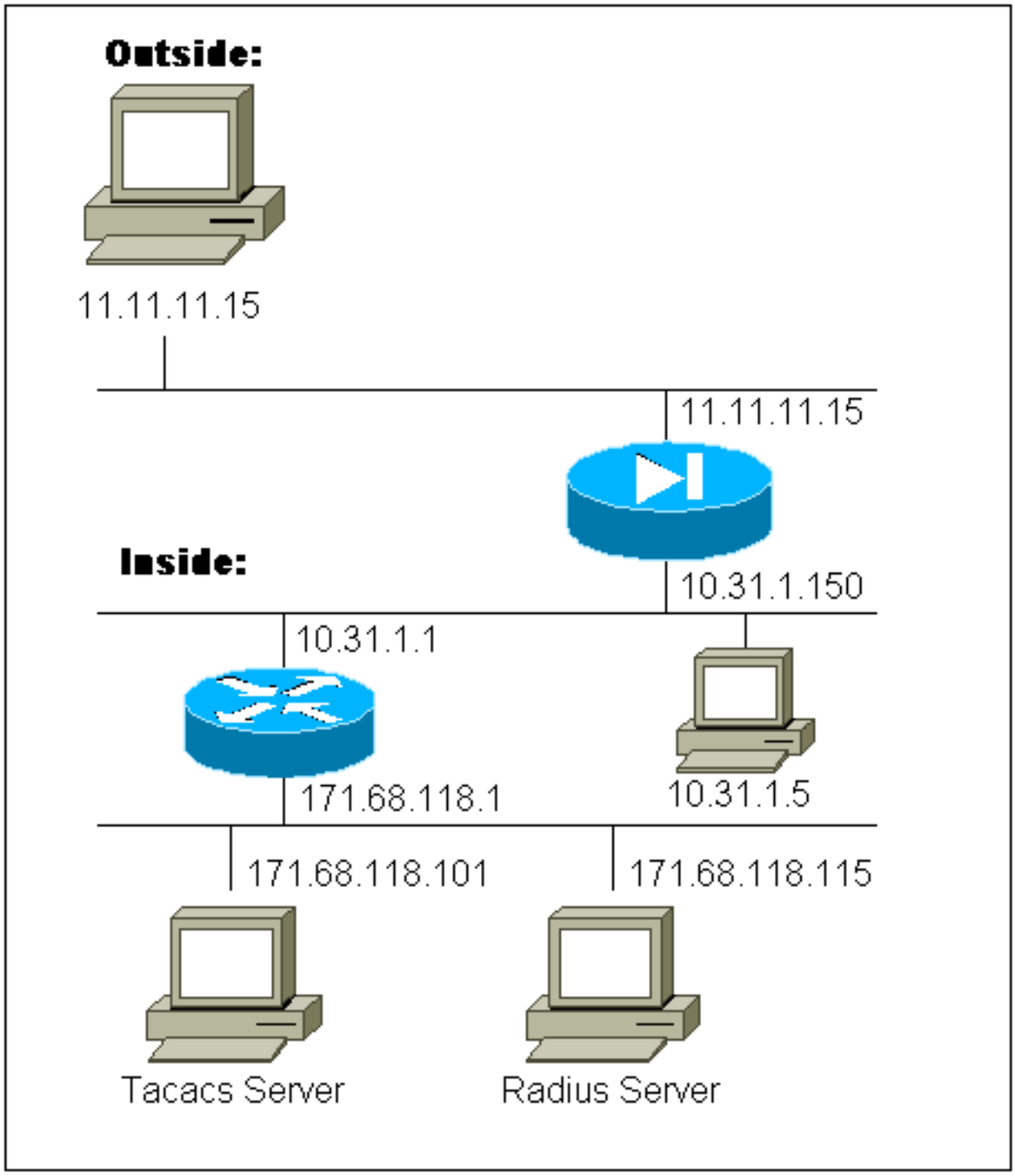
TACACS+免费软件服务器配置

```
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

- 切记PIX配置在添加验证、授权和统计(AAA)前工作。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
 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：

outbound

10.31.1.5的内部的用户初始化数据流对外部11.11.11.15和通过TACACS+验证(出局流量使用包括TACACS服务器171.68.118.101) “流出”的服务器列表。

入站

11.11.11.15的外部用户初始化数据流对内部的10.31.1.5 (11.11.11.22)和通过RADIUS验证(Inbound数据流使用包括RADIUS服务器171.68.118.115) “流入”的服务器列表。

PIX调试-良好的验证- TACACS+

下面的示例显示与良好的验证的PIX调试：

```
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调试-未成功认证(用户名或密码) - TACACS+

下面的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。下列信息显示：“错误：超出的尝试的最大数量”。

```
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调试-能连接，但是无响应- TACACS+

下面的示例显示与PIX不讲话的一个可PING的服务器的PIX调试。用户一次看到用户名，并且PIX从未请求密码(这在Telnet)。

```
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调试-不能连接服务器- TACACS+

下面的示例显示不可ping通的服务器的PIX调试。用户一次看到用户名。PIX从未请求密码(这在Telnet)。下列信息显示：“对TACACS+服务器”和“错误的超时：超出的尝试的最大数量” (在本例中的配置反射伪装服务器)。

```
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调试-良好的验证- RADIUS

下面的示例显示与良好的验证的PIX调试：

```
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调试-未成功认证(用户名或密码) - RADIUS

下面的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。如果二者之一是错误的，消息“不正确的密码”显示四次。然后，用户是断开的。此问题分配Bug ID #CSCdm46934。

```
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调试- Deamon下来，不会与PIX联络- RADIUS

下面的示例显示PIX调试用一个可PING的服务器，但是守护程序发生故障。服务器不会与PIX联络。用户看到用户名，跟随由密码。下列信息显示：“RADIUS服务器被放弃的”和“错误：超出的尝试的最大数量”。

```
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调试-不能连接服务器或键/客户端不匹配- RADIUS

下面的示例显示不可ping通的或的PIX调试有键/客户端不匹配的服务器。用户看到用户名和密码。下列信息显示：“对RADIUS服务器”和“错误的超时：超出的尝试的最大数量” (在配置的服务器是只为示例目的)。

```
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
```

添加特许

因为授权是无效没有认证，我们为同一个源及目的地范围将需要授权：

```
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

注意我们不添加“流入的”特许，因为流入的数据流用RADIUS验证，并且RADIUS授权无效

认证和授权从PIX的调试示例

与良好的验证和成功的授权的PIX调试- TACACS+

下面的示例显示与良好的验证和成功的授权的PIX调试：

```
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
```

PIX调试-良好的验证，失败的授权- TACACS+

下面的示例显示与良好的验证的PIX调试，但是失败的授权：

这里用户也看到消息“错误：被拒绝的授权”

```
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
```

增加记帐功能

TACACS+

```
aaa accounting any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

调试将查找同样认为是否开/关。然而，在被发送的“构件”，将有“启动”计费记录时。在被发送的“卸载”，将有“终止”计费记录时。

TACACS+计费记录看起来象以下(这些是从CiscoSecure UNIX;那个在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 Outgoing
```

RADIUS

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

调试将查找同样认为是否开/关。然而，在“构件”，“启动”计费记录时被发送。在，“终止”计费记录时发送“卸载”：

RADIUS计费记录看起来象以下：(这些是从CiscoSecure UNIX;那个在CiscoSecure NT可能逗号分隔的)：

```
aaa accounting any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming
```

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，我们能执行某事类似以下：

```
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
```

如果是“除了”从认证的IP地址并且有授权，您必须从授权也除去他们!

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(即有一次会话通过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。在以下示例中，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 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
```

由于服务器未看到“启动”记录，但是“终止”记录(此时此刻)，服务器表示， “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)，连接将由服务器拒绝。

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

```
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
```

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。

然而， HTTP工作不同地由于协议的本质。下面HTTP的示例。

用户从171.68.118.100访问到9.9.9.25通过PIX ：

```
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
```

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。此下载用是的一秒钟(;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会工作由于HTTP连接种类。

在PIX的认证并启用

先前的讨论是验证Telnet (和HTTP， FTP)数据流通过PIX。在下面的示例中的，我们确信，对PIX的Telnet运作，不用认证：

```
telnet 10.31.1.5 255.255.255.255
passwd ww
```

然后，我们添加命令验证远程登录到PIX的用户：

```
aaa authentication telnet console Outgoing
```

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

```
aaa authentication enable console Outgoing
```

用此命令，提示用户输入被发送到TACACS或RADIUS服务器的用户名和密码。在这种情况下，因为使用“流出的”服务器列表，请求去TACACS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，用户通过TACACS能enable (event)或RADIUS用相同用户名/密码，假设用户能登陆到与TACACS或RADIUS的PIX。此问题分配Bug ID #CSCdm47044。

在服务器发生故障情况下，用户能获得访问到PIX特权模式通过输入“PIX”用户名和正常特权密码的从PIX (“无论何种形式的特权密码”)。如果“无论何种形式的特权密码”不在PIX配置，用户应该输入“PIX”用户名的和按enter键。如果设置特权密码，但是不知道，将要求密码复原盘为了重置。

在串行控制台的认证

aaa authentication serial console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的配置命令，系统消息将被削减(如果配置PIX发送系统日志在调试级别到系统日志主机)。下面从系统日志服务器的一个示例：

```
aaa authentication enable console Outgoing
```

更改提示用户看见

如果我们有命令：

```
auth-prompt THIS_IS_PIX_5
```

通过PIX的用户看到顺序：

```
auth-prompt THIS_IS_PIX_5
```

然后，在最后目的地设备的到达，“用户名：”并且“密码：”请提示目的地框被提交。

此提示只影响去通过PIX，不PIX的用户。

Note: 没有为对PIX的访问削减的计费记录。

定制消息用户请参阅在成功/故障

如果我们有命令：

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

用户通过PIX将看到以下在一个失败/成功的登录：


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


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”，然后请勿实现此!但是，如果需要单个用户不同的uauth，请读。

在我们的在PIX的示例中，我们使用**timeout uauth 3:00:00命令**。这意味着，一旦人验证，他们不会必须重新鉴别3小时。但是，如果我们设置有以下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/绝对超时以后断开。它控制再验证是否发生。


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


在认证以后，请发出一**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

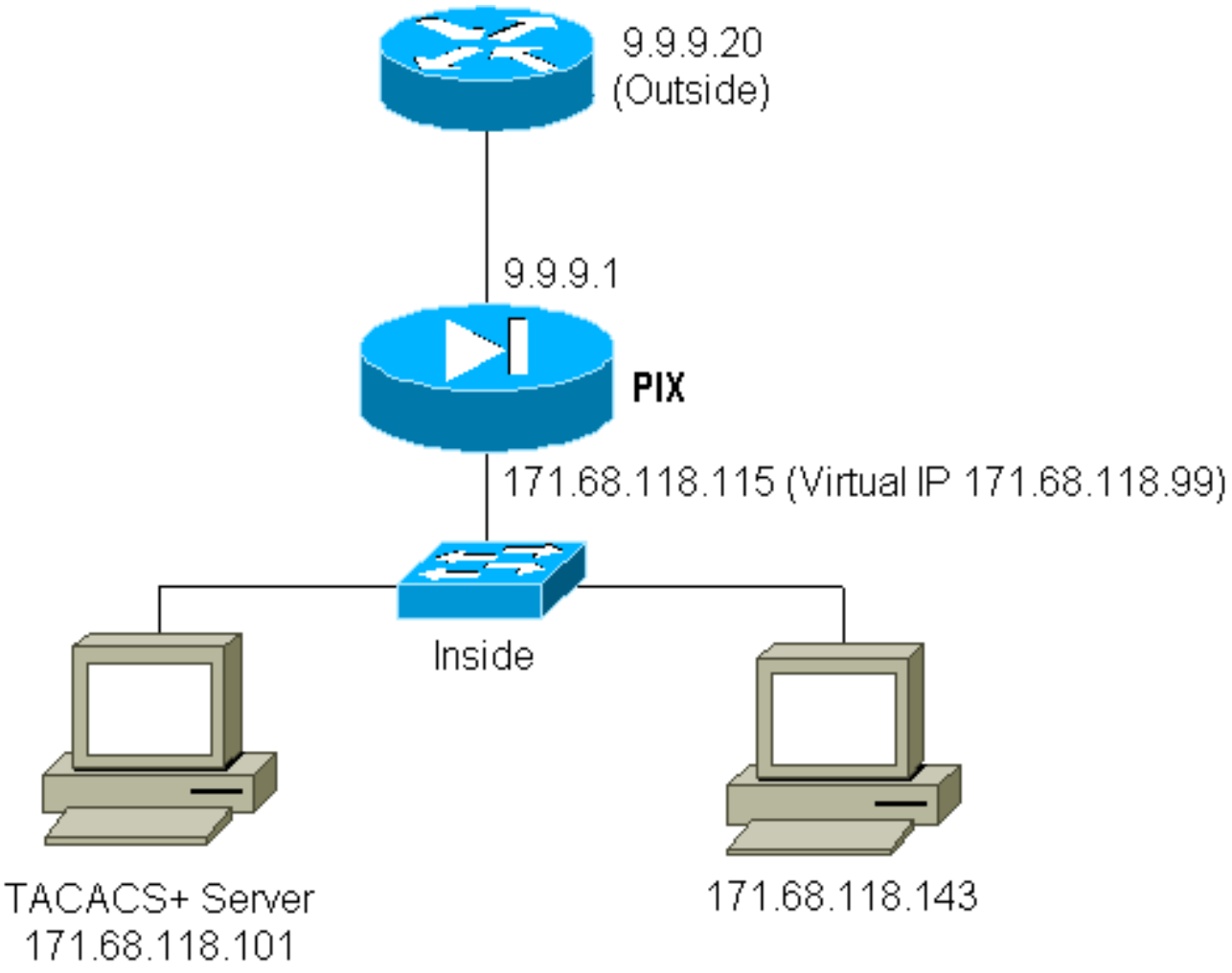
如果认证需要在站点PIX的外部，以及在PIX，异常浏览器行为可能从浏览器缓存有时被观察用户名和密码。

要避免此，您能通过添加RFC 1918地址实现虚拟 HTTP (即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)使用以下命令，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出站示例：



PIX配置虚拟HTTP出站：

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

Virtual telnet

因为一些协议，例如“邮件”，没有容易验证，配置PIX验证所有Inbound与Outbound数据流不是一个好想法。当邮件服务器和客户端设法通过PIX沟通，当所有数据流通过PIX验证，无法认证的协议的PIX系统日志将表示消息例如：

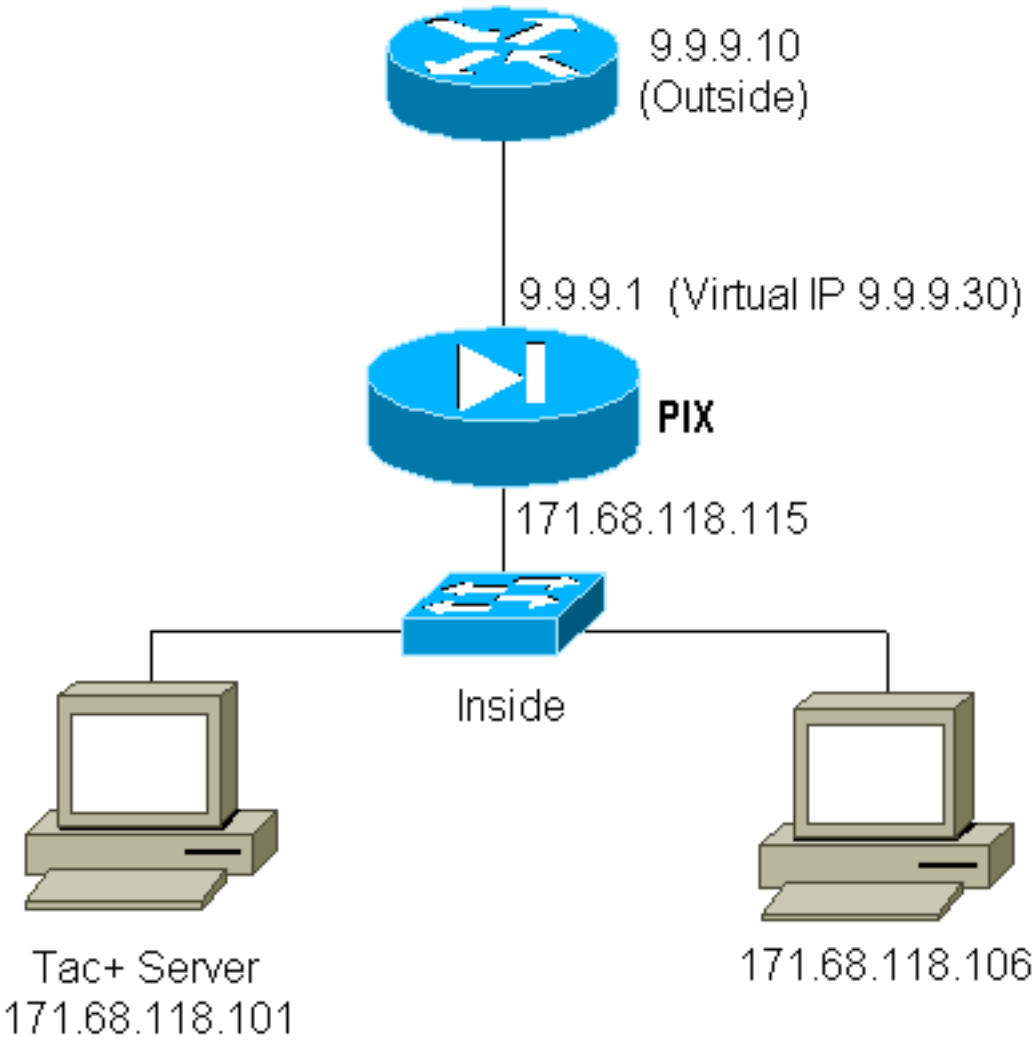
```
virtual http #.#.#.# [warn]
```

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)。

但是，如果确实有需要验证特殊服务，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附加对虚拟IP的真实服务器。

在我们的示例中，我们要允许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。

虚拟Telnet入站：



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9.9.9.30地址：

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

在成功的验证以后， **show uauth命令**显示用户有“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
```

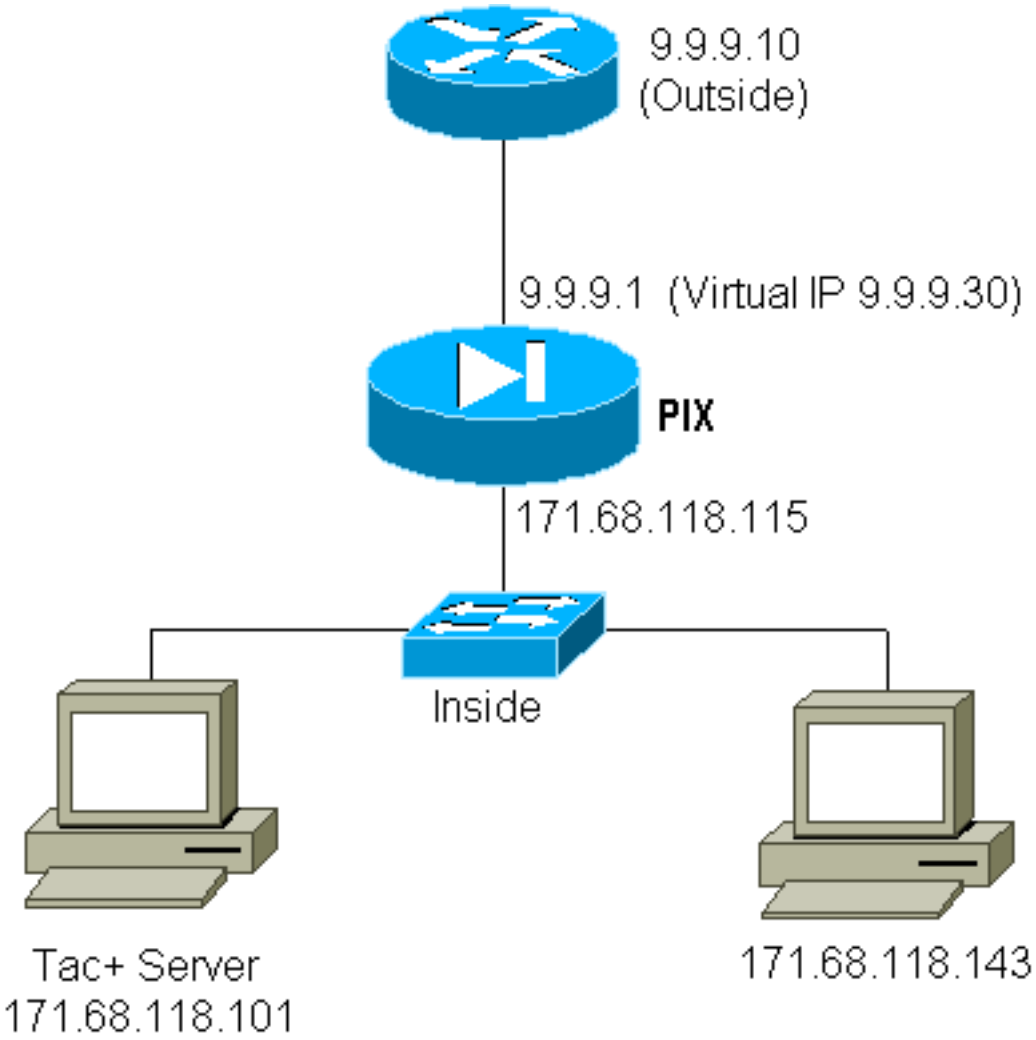
并且，当在9.9.9.10的设备要发送TCP/49数据流到设备在171.68.118.106 ：

```
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。在以下示例中，171.68.118.143的内部的用户将远程登录到虚拟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**显示他的uauth。如果用户要防止数据流经历，在他的会话完成后(当有在uauth留给的时间)，他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。在以下示例中，认证对于所有outbound仍然是必需的，但是授权对于TCP端口只是必需的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 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，当我们从171.68.118.143远程登录到9.9.9.10时，认证和授权出现，因为Telnet端口23在23-49范围。当我们执行从171.68.118.143的HTTP会话到9.9.9.10时，我们必须仍然验证，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 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

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 Outgoing
aaa authorization tcp/23-49 outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Outgoing
```

Related Information

- 思科PIX防火墙软件产品技术支持
- Cisco Secure PIX防火墙命令参考