配置PIX 5.1.x ：TACACS+和RADIUS

目录

简介

RADIUS和TACACS+认证可能为FTP、Telnet和HTTP连接执行。其他较不普通的协议的验证可能通常使工作。支持 TACACS+ 授权；RADIUS授权不是。在PIX 5.1验证、授权和统计(AAA)上的变化在以前版本包括扩展认证--IPSec隧道的验证从思科安全VPN客户端1.1的。

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。

背景信息

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。
- 核算是什么用户。

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。您会告诉PIX验证出站流量和给所有六个用户在TACACS+/RADIUS安全服务器的id's。使用简单验证，这六个用户可能验证与用户名和密码，然后出去。其他九十四个用户不可能出去。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。这六个用户可能执行FTP，Telnet或者HTTP。

但是请假设这六个用户之一，“Festus”，不是委托。您希望允许Festus执行FTP，但是不是HTTP或者Telnet到外部。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。这只是有效与TACACS+。当我们添加*特许*到PIX时， PIX首先发送Festus'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*” Festus尝试执行。使用适当服务器设置，Festus能允许到“ftp 1.2.3.4”，但是拒绝对任何地方HTTP或Telnet的能力。

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出来，然后请求。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。用户需要进入用户名的密码的**local_username@remote_username**和**local_password@remote_password**。PIX发送local_username和local_password到本地安全服务器和，如果验证(和授权)是成功的在PIX/服务器， remote_username，并且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。如果认证(和授权)成功，用户将能访问上面的目的网站。请记住，**浏览器会缓存用户名和口令**。如果看起来应该时间PIX HTTP连接，但是不如此执行，很可能再验证用射击缓存的用户名和密码的浏览器实际上发生对PIX，然后转发此到认证服务器。PIX系统日志和服务器调试显示此现象。如果Telnet和FTP似乎工作正常，但HTTP不连接，这是为什么？
- **通道**-当尝试以隧道传输IPSec数据流到与VPN客户端和Xauth的网络时，“用户认证的一个灰色方框新连接的”为用户名/密码显示。**注意：** 此验证从思科安全VPN客户端1.1开始支持。如果**Help > About**菜单不show version 2.1.x或以后，这不工作。

用于所有情形的服务器安全配置

Cisco Secure UNIX TACACS服务器配置

在此部分，您提交以信息配置您的安全服务器。

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 .*
}
}
```

```
}
```

Cisco Secure UNIX RADIUS服务器配置

请使用GUI添加PIX IP地址和密钥对网络接入服务器(NAS)列表。

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

Cisco Secure ACS for Windows 2.x RADIUS

请使用这些步骤配置Cisco Secure ACS for Windows 2.x RADIUS。

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 Configuration部分GUI的PIX IP地址。

EasyACS TACACS+

EasyACS文档描述设置。

1. 在组部分，请点击**Shell exec**给EXEC权限。
2. 对PIX的添加授权，点击**Deny不匹配IOS at命令**组建立的底部。
3. 选择**add/edit new命令**您希望允许的每命令的，例如， **Telnet**。
4. 如果远程登录到特定站点允许，请填写在参数部分的IP地址以形式“permit #.#.#.#”。否则，允许远程登录，请单击**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。

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**给EXEC权限。
2. 对PIX的添加授权，在组建立的底部，单击**拒绝不匹配IOS命令**。
3. 选择**add/edit new命令**例如您希望允许的每命令的(**Telnet**)。
4. 要允许远程登录到特定站点，请输入在参数部分的IP地址以形式“permit #.#.#.#”。要允许远程登录到所有站点，请单击**允许所有未列出的参数**。
5. **编辑指令的**单击**完成**。
6. 执行其中每一的步骤1至5允许命令(例如， Telnet、HTTP或者FTP)。
7. 保证PIX IP地址被添加在NAS Configuration GUI部分。

Livingston RADIUS 服务器配置

添加PIX IP地址并且锁上到客户端文件。

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

Merit RADIUS 服务器配置

添加PIX IP地址并且锁上到客户端文件。

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

TACACS+ 免费软件服务器配置

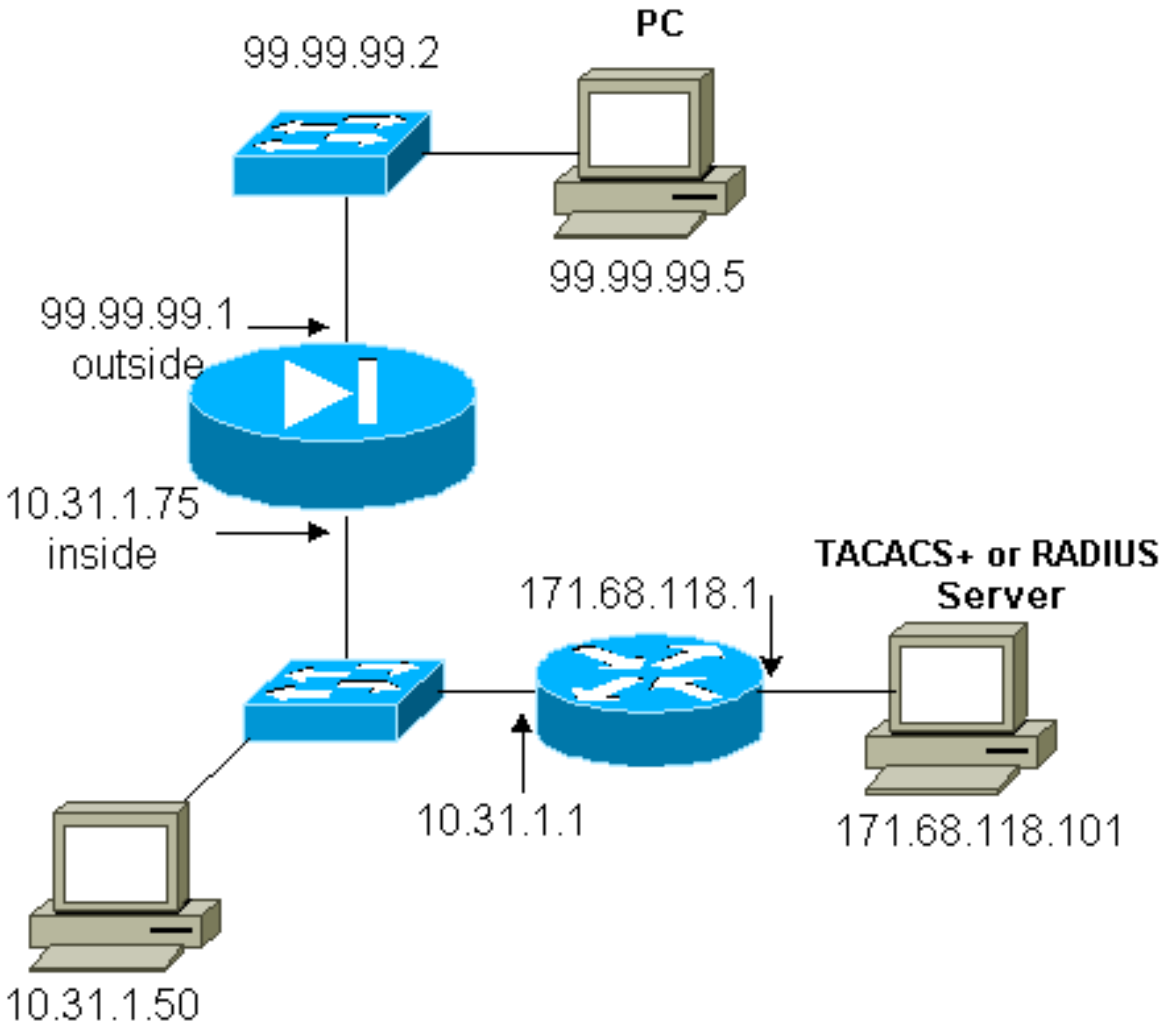
```
key = "cisco"
user = adminuser {
login = cleartext "all"
default service = permit
}

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

注意： 命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

- 确保PIX配置在添加AAA前工作。如果不能在创立认证和授权之前通过流量，您不能那么之后执行。
- 登陆PIX的Enable (event)。在一个加载的系统不应该大量地使用操作日志控制台调试。可以使用Logging buffered debugging，然后执行**show logging命令**。记录日志可能也发送到系统日志服务器和被检查那里。
- 启用调试在TACACS+或RADIUS服务器(所有服务器有此选项)。

网络图



PIX 配置
PIX Version 5.1(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 pix/intf2 security10 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix3 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 no logging standby **logging console debugging** no logging monitor no logging buffered no logging trap no logging history logging facility 20 logging queue 512 interface ethernet0 auto interface ethernet1 auto interface ethernet2 auto shutdown mtu outside 1500 mtu inside 1500 mtu pix/intf2 1500 **ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0** ip address pix/intf2 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 arp timeout 14400 **global (outside) 1**

```
99.99.99.7-99.99.99.10 netmask 255.255.255.0 nat
(inside) 1 10.31.1.0 255.255.255.0 0 0 static
(inside,outside) 99.99.99.99 10.31.1.50 netmask
255.255.255.255 0 0 conduit permit icmp any any conduit
permit tcp any any conduit permit udp any any route
outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route inside
171.68.118.0 255.255.255.0 10.31.1.1 1 route inside
171.68.120.0 255.255.255.0 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 0:05:00
absolute aaa-server TACACS+ protocol tacacs+ aaa-server
RADIUS protocol radius aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host
171.68.118.101 cisco timeout 5 aaa-server AuthOutbound
protocol radius aaa-server AuthOutbound (inside) host
171.68.118.101 cisco timeout 5 aaa authentication
include telnet outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
AuthOutbound aaa authentication include telnet inbound
0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa
authentication include http outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
http inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
aaa authentication include ftp outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include
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
floodguard enable telnet timeout 5 terminal width 80
Cryptochecksum:b26b560b20e625c9e23743082484caca : end
[OK]
```

PIX 验证调试示例

此部分显示验证调试示例多种方案的。

入站

99.99.99.2的外部用户初始化流量对内部的10.31.1.50 (99.99.99.99)和通过TACACS验证(即入站数据流使用包括TACACS服务器171.68.118.101)的服务器列表“AuthInbound”。

PIX 调试 - 身份验证成功 - TACACS+

下面的示例显示与成功验证的PIX调试：

```
109001: Auth start for user '???' from
    99.99.99.2/11008 to 10.31.1.50/23
109011: Authen Session Start: user 'cse', sid 4
109005: Authentication succeeded for user 'cse'
    from 10.31.1.50/23 to 99.99.99.e
302001: Built inbound TCP connection 10 for
    faddr 99.99.99.2/11008 gaddr 99.99.)
```

PIX 调试 - 身份验证失败（用户名或口令有误）- TACACS+

下面的示例显示与未成功认证的PIX调试(用户名或密码)。用户看到三个用户名/密码集合，跟随由此消息：`Error:`。

```
109001: Auth start for user '???' from
     99.99.99.2/11010 to 10.31.1.50/23
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11010 on
     interface outside
```

PIX调试-能ping服务器，无响应- TACACS+

下面的示例显示服务器可ping通的PIX调试，但是不发言对PIX。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Error:。

```
109001: Auth start for user '???' from 99.99.99.2/11011
     to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11011 failed
     (server 171.68.118.101 failed) on interface outside
  109006: Authentication failed for user '' from 10.31.1.50/23
     to 99.99.99.2/11011 on interface outside
```

PIX调试-无法ping服务器- TACACS+

下面的示例显示PIX调试服务器不可ping通的地方。用户一次看到用户名，但是PIX从未请求密码(这在Telnet)。下列信息显示：TACACS+和Error:(伪装服务器被交换了配置)。

```
111005: console end configuration: OK
  109001: Auth start for user '???' from
     99.99.99.2/11012 to 10.31.1.50/23
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109002: Auth from 10.31.1.50/23 to 99.99.99.2/11012
     failed (server 1.1.1.1 failed) on interface outside
  109006: Authentication failed for user '' from
     10.31.1.50/23 to 99.99.99.2/11012 on interface
     outside
```

PIX 调试 - 身份验证成功 - RADIUS

下面的示例显示与成功验证的PIX调试：

```
109001: Auth start for user '???' from
     10.31.1.50/11008 to 99.99.99.2/23
  109011: Authen Session Start: user 'pixuser', sid 8
  109005: Authentication succeeded for user
     'pixuser' from 10.31.1.50/11008 to
     99.99.99.2/23 on interface inside
  302001: Built outbound TCP connection 16 for faddr
     99.99.99.2/23 gaddr 99.99.99.99/11008
     laddr 10.31.1.50/11008 (pixuser)
```

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，并且有三个机会输入这些。当条目不成功时，下列信息显示：Error:。

```
109001: Auth start for user '???' from 10.31.1.50/11010
     to 99.99.99.2/23
```

```
  109006: Authentication failed for user ''
     from 10.31.1.50/11010 to 99.99.99.2/23
     on interface inside
```

PIX调试-能ping服务器，守护程序下来- RADIUS

下面的示例显示PIX调试服务器可ping通的地方，但是守护程序发生故障和不会与PIX联络。用户看到用户名，然后密码、RADIUS和Error:。错误消息。

```
109001: Auth start for user '???' from 10.31.1.50/11011
     to 99.99.99.2/23
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  1ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  ICMP unreachable (code 3) 171.68.118.101 > 10.31.1.75
  09002: Auth from 10.31.1.50/11011 to 99.99.99.2/23
     failed (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109002: Auth from 10.31.1.50/11011 to 99.99.99.2/23 failed
     (server 171.68.118.101 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11011
     to 99.99.99.2/23 on interface inside
```

PIX调试-无法ping服务器或密匙/客户端不匹配- RADIUS

下面的示例显示PIX调试服务器不可ping通的地方或有客户端/主要不匹配。用户看到用户名、密码、RADIUS消息和Error:消息伪装服务器被交换了配置)。

```
109001: Auth start for user '???' from 10.31.1.50/11012
     to 99.99.99.2/23
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109002: Auth from 10.31.1.50/11012 to 99.99.99.2/23 failed
     (server 1.1.1.1 failed) on interface inside
  109006: Authentication failed for user '' from 10.31.1.50/11012
     to 99.99.99.2/23 on interface inside
```

增加授权

如果决定添加授权，因为授权是无效没有验证，您需要需要同一个源及目的地范围的授权。

```
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
```

注意您不添加流出的特许，因为流出流量验证与RADIUS，并且RADIUS授权无效。

PIX 认证和授权调试示例

PIX调试-成功验证和成功的授权- TACACS+

下面的示例显示与成功验证和成功的授权的PIX调试：

```
109001: Auth start for user '???' from 99.99.99.2/11016
   to 10.31.1.50/23
```

```
109011: Authen Session Start: user 'cse', Sid 11
109005: Authentication succeeded for user 'cse'
   from 10.31.1.50/23 to 99.99.99.2/11016 on interface outside
109011: Authen Session Start: user 'cse', Sid 11
109007: Authorization permitted for user 'cse' from
   99.99.99.2/11016 to 10.31.1.50/23 on interface outside
302001: Built inbound TCP connection 19 for faddr 99.99.99.2/11016
   gaddr 99.99.99.99/23 laddr 10.31.1.50/23 (cse)
```

PIX 调试 - 身份验证成功，授权失败 - TACACS+

下面的示例显示与成功验证，但是失败的授权的PIX调试。此处用户也看到Message错误。

```
109001: Auth start for user '???' from
    99.99.99.2/11017 to 10.31.1.50/23
109011: Authen Session Start: user 'httponly',
   Sid 12
109005: Authentication succeeded for user 'httponly'
   from 10.31.1.50/23 to 99.99.99.2/11017 on
   interface outside
109008: Authorization denied for user 'httponly' from
   10.31.1.50/23 to 99.99.99.2/11017 on interface outside
```

增加记账功能

TACACS+

aaa accounting include any inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
输出的TACACS+免费软件：

```
Tue Feb 22 08:52:20 2000  10.31.1.75 cse PIX
   99.99.99.2 start task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet
Tue Feb 22 08:52:25 2000  10.31.1.75 cse PIX
   99.99.99.2 stop task_id=0x14
   foreign_ip=99.99.99.2 local_ip=10.31.1.50
   cmd=telnet elapsed_time=5
   bytes_in=39 bytes_out=126
```

RADIUS

aaa accounting include any outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound
输出的Merit RADIUS ：

```
Tue Feb 22 08:56:17 2000
        Acct-Status-Type = Start
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
        Acct-Session-Id = 0x00000015
        User-Name = pixuser

        Tue Feb 22 08:56:24 2000
        Acct-Status-Type = Stop
        NAS-IP-Address = 10.31.1.75
        Login-IP-Host = 10.31.1.50
        Login-TCP-Port = 23
```

```
        Acct-Session-Id = 0x00000015
        Username = pixuser
        Acct-Session-Time = 6
        Acct-Input-Octets = 139
        Acct-Output-Octets = 36
```

Exclude 命令的使用

如果我们添加另一主机外部(在99.99.99.100)自我们的网络，并且此主机是委托，您能从认证和授权排除他们用以下命令：

```
aaa authentication exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100 255.255.255.255
AuthInbound aaa authorization exclude telnet inbound 0.0.0.0 0.0.0.0 99.99.99.100
255.255.255.255 AuthInbound
```

最大会话数与查看登录用户

一些TACACS+和RADIUS服务器有“最大会话”（max-session）或“查看已登陆用户”（view logged-in users）功能。能力执行最大会话或检查登录用户依靠计费记录。当有记帐“开始”记录生成，但没有“终止”记录生成时，TACACS+或RADIUS服务器则假设仍然有人登录(用户有一个会话通过PIX)。

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，使用不同的网络配置，但概念却相同。

用户通过PIX远程登录，验证在途中：

```
   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
```

由于服务器未看到开始录制，但是终止记录，此时此刻，服务器显示Telnet用户登陆。如果用户尝试要求验证的另一连接(或许从另一个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。

用户去他们的Telnet或FTP业务在目标主机，然后退出(度过十分钟那里)：

```
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是否为0 (指每次认证)或更大值(在uauth期间，一次认证后便不再鉴权))，每一个被访站点的计费记录都会被剪切。

HTTP工作不同地由于协议的本质。下面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。

开始录制被张贴在16:35:34和在16:35:35的终止记录。此次下载用了一秒时间(即在开始和终止记录之间的时间不足一秒)。在用户阅读网页时，用户是否仍然登录到网站，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。开始和停止记录分秒。因为记录同时，出现没有开始录制没有终止记录。将有开始和停止记录发送对每处理的服务器uauth是否为更加大0或的事设置。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

验证Telnet (和HTTP， FTP)流量的先前的讨论注意事项通过PIX。保证Telnet对PIX工作，不用验证：

```
telnet 10.31.1.5 255.255.255.255 passwd ww
```

然后请添加命令验证远程登录到PIX的用户：

```
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**)。PIX也请求TACACS+或RADIUS用户名和密码。在这种情况下，因为使用AuthInbound服务器列表， PIX请求TACACS+用户名和密码。

如果服务器发生故障，您能通过输入用户名的**PIX**访问PIX，然后特权密码(**无论何种形式的特权密码**)。使用以下命令：

```
aaa authentication enable console AuthInbound
```

提示用户输入发送到TACACS或RADIUS服务器的用户名和密码。在这种情况下，因为使用AuthInbound服务器列表， PIX请求TACACS+用户名和密码。

由于启用认证 信息包与登录认证 信息包相同，假设用户可以通过TACACS或RADIUS登录PIX，那们他们也可以利用相同用户名/密码，通过TACACS或RADIUS启用。此问题分配Cisco Bug ID

CSCdm47044 (仅限注册用户)。

如果服务器发生故障，您能通过输入用户名和正常特权密码的**PIX**访问PIX特权模式从PIX (**无论何种形式的特权密码**)。如果enable password不在PIX的配置中，请输入PIX作为用户名，并按回车键。如果特权密码设置，但是不知道，密码复原盘需要被构件重置密码。

修改用户看到的提示

如果有命令：

auth-prompt PIX_PIX_PIX
通过PIX的用户看到以下顺序：

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

在最终目的地的到达，用户会看到用户名：并且密码：目的地框显示的提示符。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youh有命令：

auth-prompt accept "GOOD_AUTH" auth-prompt reject "BAD_AUTH"
然后用户通过PIX看到在失败/成功登录的以下顺序：

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

每用户空闲超时与绝对超时

此功能当前不工作，并且问题分配Cisco Bug ID CSCdp93492 (仅限注册用户)。

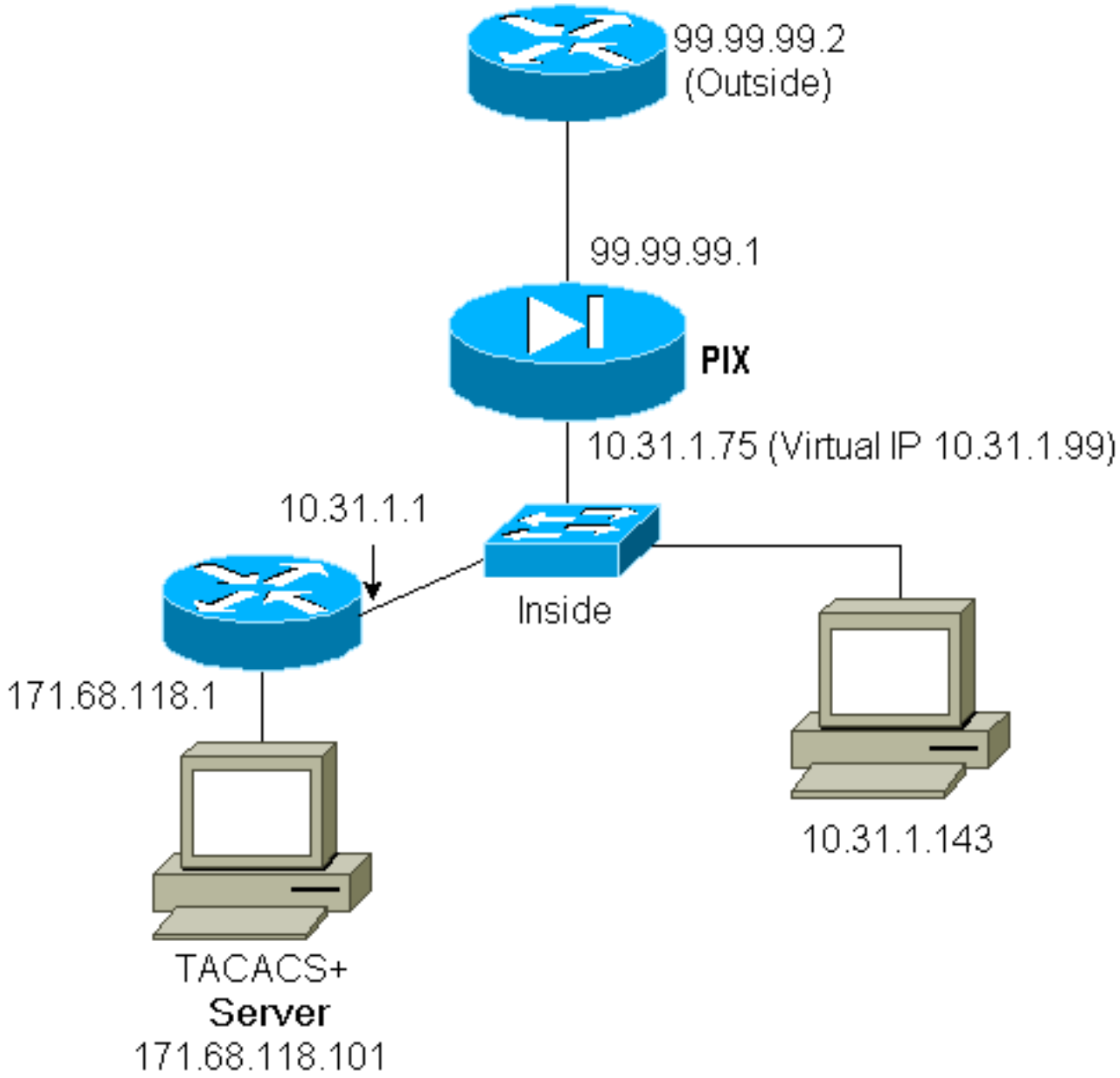
虚拟 HTTP

如果PIX以外的站点和PIX本身需要认证，异常浏览器行为有时可以看到，因为浏览器可以缓存用户名和密码。

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 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 01:00:00 aaa
authentication include http outbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa-server
RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound (inside)
host 171.68.118.101 cisco timeout 5 virtual http 10.31.1.99
```

虚拟 Telnet

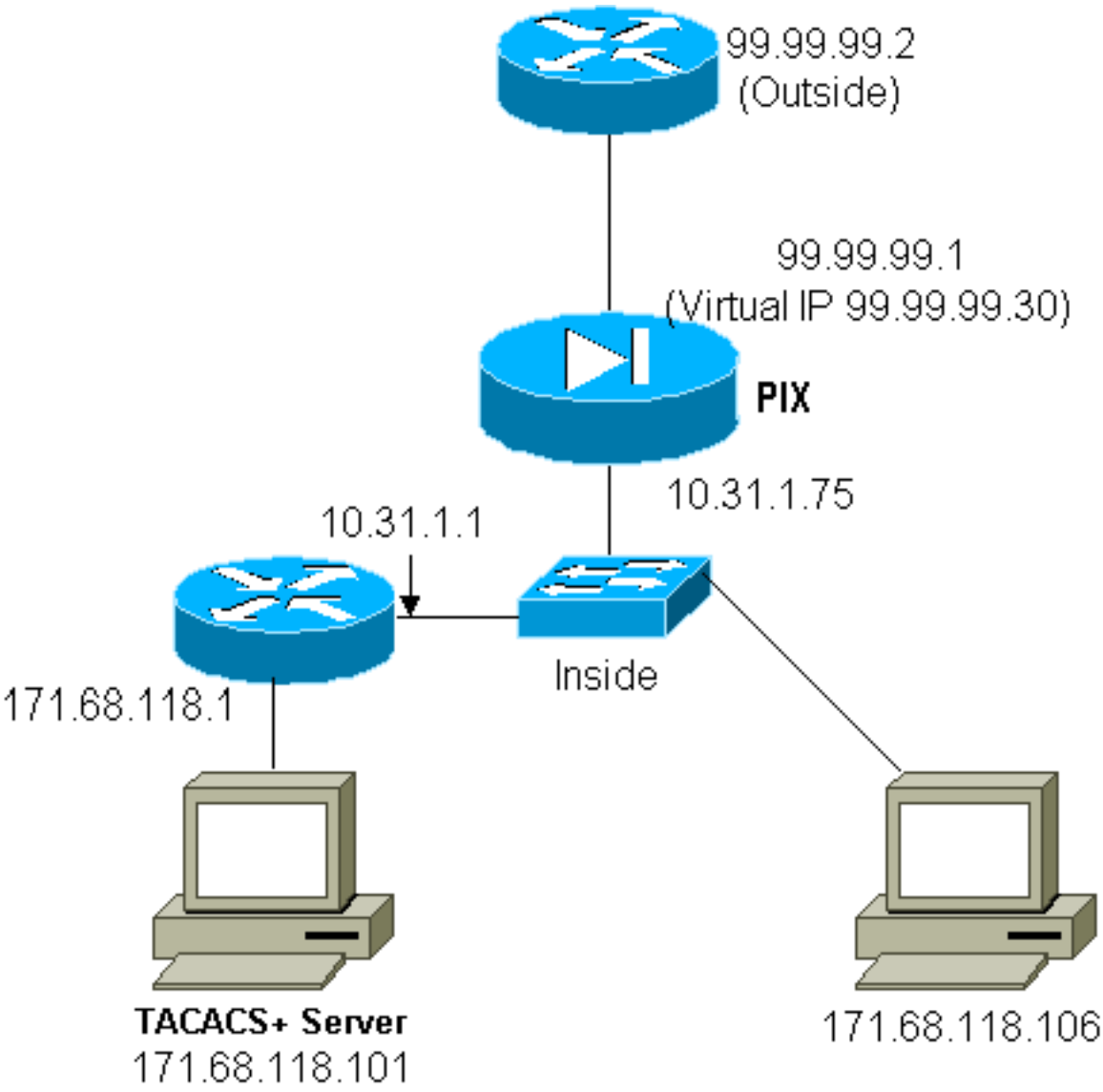
配置PIX验证所有入站和出站是可能的，但是它不是一个好想法，因为一些协议，例如邮件，没有容易地验证。当邮件服务器和客户端设法通过PIX时通信，当所有流量通过PIX验证时，无法认证的协议的PIX系统日志表示消息例如：

```
109013: User must authenticate before using
    this service
109009: Authorization denied from 171.68.118.106/49
    to 9.9.9.10/11094    (not authenticated)
```

然而，如果确实有需要验证特殊服务，这可以利用**virtual telnet命令**执行。此命令允许验证发生到虚拟Telnet IP地址。在此验证以后，特殊服务的流量可以去真实服务器。

在本例中，您希望TCP端口49流量从外部主机99.99.99.2流到内部主机171.68.118.106。因为此流量不确实authenticatable，请设置virtual telnet。virtual telnet，必须有一相关的静态。这里，99.99.99.20和171.68.118.20是虚拟地址。

虚拟 Telnet 入站



入站PIX的配置虚拟远程登录

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 static
(inside,outside) 99.99.99.20 171.68.118.20 netmask 255.255.255.255 0 0 static (inside,outside)
99.99.99.30 171.68.118.106 netmask 255.255.255.255 0 0 conduit permit tcp host 99.99.99.20 eq
telnet any conduit permit tcp host 99.99.99.30 eq tacacs any aaa-server TACACS+ protocol tacacs+
aaa-server Incoming protocol tacacs+ aaa-server Incoming (inside) host 171.68.118.101 cisco
timeout 5 aaa authentication include telnet inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming aaa
authentication include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 Incoming virtual telnet
99.99.99.20
```

PIX调试虚拟Telnet入站

99.99.99.2的用户必须通过远程登录首先验证到在PIX的99.99.99.20地址：

```
109001: Auth start for user '???' from
```

```
    99.99.99.2/22530 to 171.68.118.20/23
 109011: Authen Session Start: user 'cse', Sid 13
 109005: Authentication succeeded for user
    'cse' from 171.68.118.20/23 to
    99.99.99.2/22530 on interface outside
```

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 2 Authen In Progress 0 1 user
'cse' at 99.99.99.2, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
```

并且，当在99.99.99.2的设备要发送TCP/49流量到设备在171.68.118.106 ：

```
302001: Built inbound TCP connection 16
    for faddr 99.99.99.2/11054 gaddr
    99.99.99.30/49 laddr 171.68.118.106/49 (cse)
```

特许可以被添加：

```
aaa authorization include tcp/49 inbound 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound
```

因此，当TCP/49流量通过PIX尝试， PIX也发送授权查询到服务器：

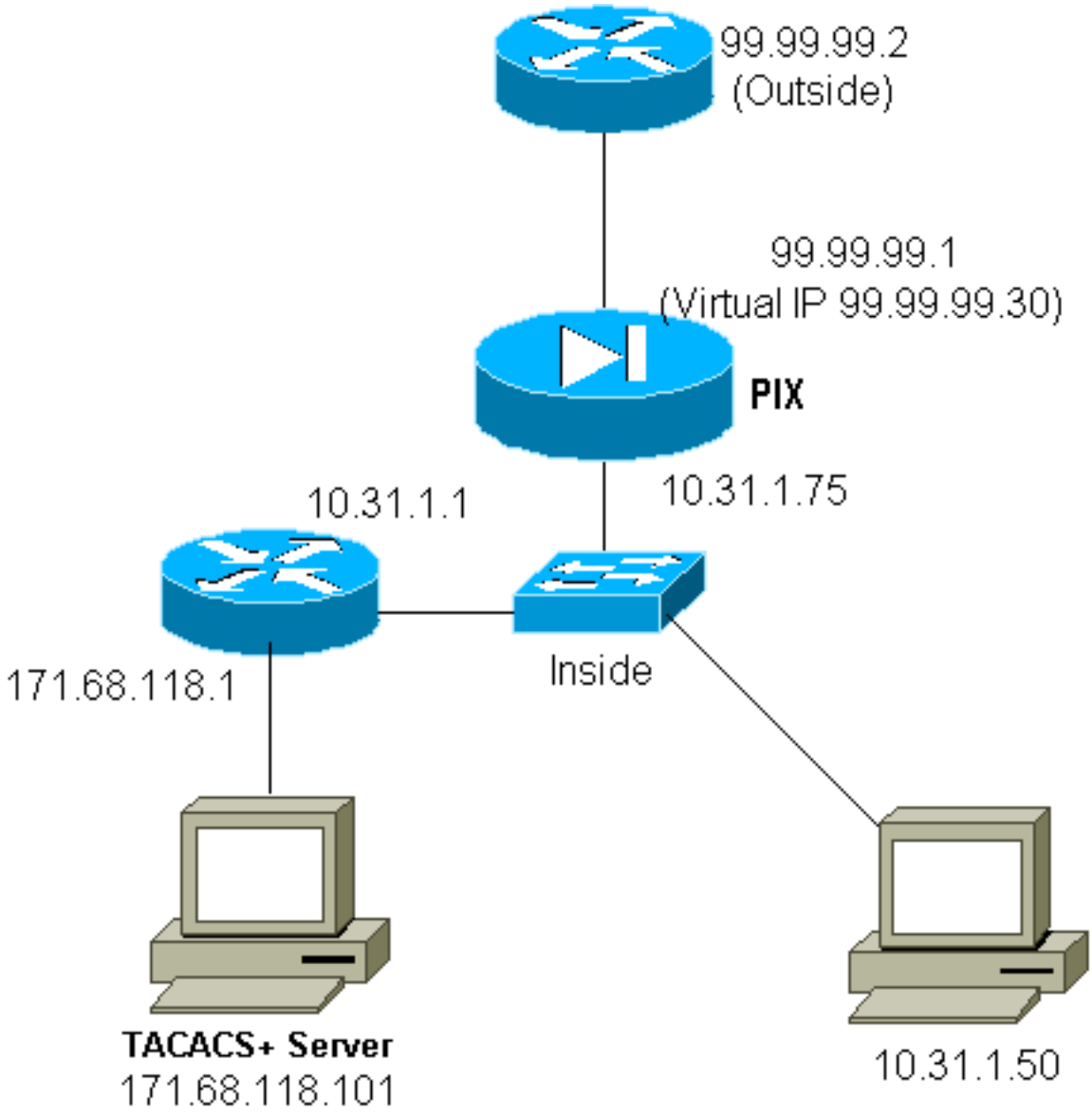
```
109007: Authorization permitted for user 'cse'
    from 99.99.99.2/11057 to 171.68.118.106/49
    on interface outside
```

在TACACS+服务器上，这被看到如下：

```
service=shell,
  cmd=tcp/49,
  cmd-arg=171.68.118.106
```

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。在以下示例中，10.31.1.50的内部的用户远程登录到虚拟99.99.99.30并且验证;Telnet连接立即丢弃。一旦验证，TCP数据流从10.31.1.50允许到在99.99.99.2的服务器：



PIX 配置虚拟 Telnet 出站：

```
ip address outside 99.99.99.1 255.255.255.0 ip address inside 10.31.1.75 255.255.255.0 global
(outside) 1 99.99.99.7-99.99.99.10 netmask 255.255.255.0 timeout uauth 0:05:00 absolute aaa-
server RADIUS protocol radius aaa-server AuthOutbound protocol radius aaa-server AuthOutbound
(inside) host 171.68.118.101 cisco timeout 5 aaa authentication include telnet outbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthOutbound aaa authentication include tcp/49 outbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthOutbound virtual telnet 99.99.99.30
```

注意： 因为这是RADIUS，没有授权。

PIX 调试虚拟 Telnet 出站：

```
109001: Auth start for user '???' from 10.31.1.50/11034
    to 99.99.99.30/23
 109011: Authen Session Start: user 'pixuser', Sid 16
 109005: Authentication succeeded for user 'pixuser'
    from 10.31.1.50/11034 to 99.99.99.30/23 on interface
    inside
 302001: Built outbound TCP connection 18 for faddr
    99.99.99.2/49 gaddr 99.99.99.8/11036 laddr
    10.31.1.50/11036 (pixuser)
 302002: Teardown TCP connection 18 faddr 99.99.99.2/49
```

```
    gaddr 99.99.99.8/11036 laddr 10.31.1.50/11036
    duration 0:00:02 bytes 0 (pixuser)
```

虚拟 Telnet 注销

当用户远程登录到虚拟Telnet IP地址时， **show uauth命令**显示他们的uauth。如果用户要防止流量经历，在他们的会话完成后，当有在uauth时留下的时间，他们需要再远程登录到虚拟Telnet IP地址。这将断开会话。

在第一验证以后：

```
 pix3# show uauth Current Most Seen Authenticated Users 1 2 Authen In Progress 0 1 user
'pixuser' at 10.31.1.50, authenticated absolute timeout: 0:05:00 inactivity timeout: 0:00:00
pix3# 109001: Auth start for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 109005:
Authentication succeeded for user 'pixuser' from 10.31.1.50/11038 to 99.99.99.30/23 on interface
inside
```

在第二验证以后(即孔再按乒乓键的已关闭) ：

```
 pix3# show uauth Current Most Seen Authenticated Users 0 2 Authen In Progress 0 1
```

端口授权

授权为端口范围允许(类似TCP/30-100)。如果virtual telnet在PIX和授权配置端口范围的，一旦孔打开与virtual telnet， PIX问题**tcp/30-100命令**对TACACS+服务器授权的：

```
static (inside,outside) 99.99.99.75 10.31.1.50 netmask 255.255.255.255 0 0 conduit permit tcp
host 99.99.99.75 host 99.99.99.2 static (inside,outside) 99.99.99.75 10.31.1.50 netmask
255.255.255.255 0 0 virtual telnet 99.99.99.75 aaa authentication include any inbound 0.0.0.0
0.0.0.0 0.0.0.0 0.0.0.0 AuthInbound aaa authorization include tcp/30-100 inbound 0.0.0.0 0.0.0.0
0.0.0.0 0.0.0.0 AuthInbound virtual telnet 99.99.99.30
```

TACACS+免费软件服务器配置：

```
user = anyone {
         login = cleartext "anyone"
         cmd = tcp/30-100 {
         permit 10.31.1.50
         }
         }
```

流量的Aaa accounting除HTTP、FTP和Telnet之外

在确保工作的virtual telnet以后允许TCP/49流量到主机在网络里面，我们决定我们想要此的核算，因此我们补充说：

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

这导致安排计费记录被削减，当tcp/49流量经历时(此示例是从TACACS+免费软件) ：

```
Sun Feb 27 05:24:44 2000 10.31.1.75 cse PIX
    99.99.99.2 start task_id=0x14 foreign_ip=99.99.99.2 local_ip=171.68.118.106
    cmd=tcp/49
```

扩展认证 (Xauth)

示例配置

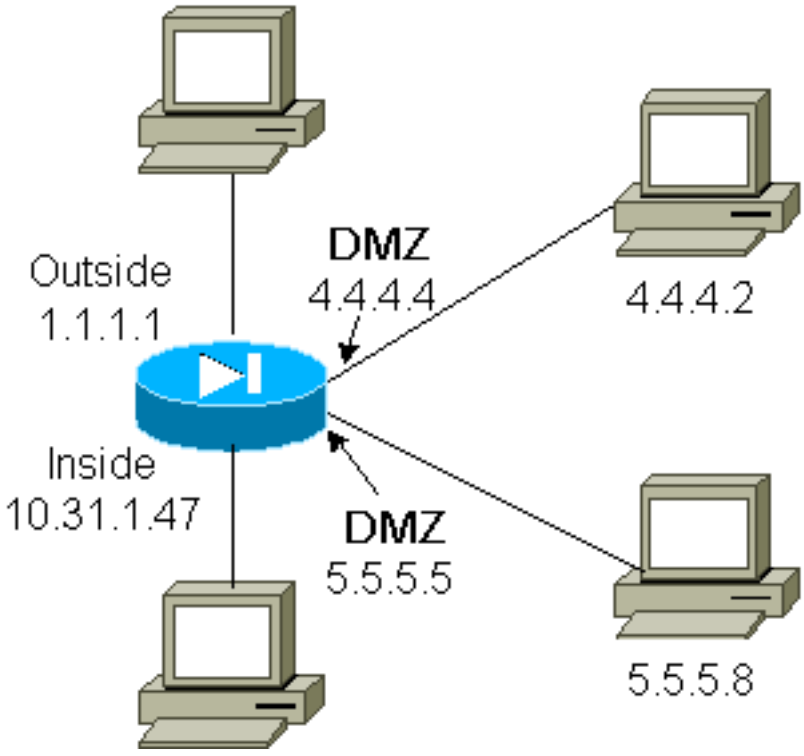
- 终止使用多个 Xauth 的 Cisco 安全 PIX 防火墙接口上的 IPSec 隧道
- 在Cisco Secure PIX防火墙和一VPN客户端之间的IPSec有扩展认证的

DMZ 上的认证

要验证去从一个DMZ接口的用户别的，请告诉PIX验证指定接口的流量。在我们的PIX安排是：

```
least secure

PIX outside (security0) = 1.1.1.1

pix/intf4 (DMZ - security20) = 4.4.4.4 & device 4.4.4.2

pix/intf5 (DMZ - security25) = 5.5.5.5 & device 5.5.5.8

(static to 4.4.4.15)

PIX inside (security100) = 10.31.1.47

 most secure
```

网络图



PIX 配置

我们要验证pix/intf4和pix/intf5之间的Telnet流量：

```
nameif ethernet0 outside security0 nameif ethernet1 inside security100 (nameif ethernet2
pix/intf2 security10 nameif ethernet3 pix/intf3 security15) nameif ethernet4 pix/intf4
security20 nameif ethernet5 pix/intf5 security25 ip address outside 1.1.1.1 255.255.255.0 ip
address inside 10.31.1.47 255.255.255.0 (ip address pix/intf2 127.0.0.1 255.255.255.255 ip
```

```
address pix/intf3 127.0.0.1 255.255.255.255) ip address pix/intf4 4.4.4.4 255.255.255.0 ip
address pix/intf5 5.5.5.5 255.255.255.0 static (pix/intf5,pix/intf4) 4.4.4.15 5.5.5.8 netmask
255.255.255.255 0 0 aaa authentication telnet pix/intf4 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa authentication telnet pix/intf5 5.5.5.0 255.255.255.0 4.4.4.0
255.255.255.0 AuthInbound aaa-server TACACS+ protocol tacacs+ aaa-server AuthInbound protocol
tacacs+ aaa-server AuthInbound (inside) host 171.68.118.101 cisco timeout 5
```

Xauth 记帐

如果**sysopt connection permit-ipsec命令**，不是**sysopt ipsec pl-compatible命令**，在与Xauth的PIX配置，认为为TCP连接，但是不是ICMP或者UDP是有效。

相关信息

- PIX 产品支持页面
- PIX 命令参考
- RADIUS 支持页
- 请求注解 (RFC)
- Cisco Secure UNIX 支持页
- Cisco Secure ACS for Windows 支持页
- 技术支持 - Cisco Systems