如何在 Cisco 安全 PIX 防火墙（5.2 到 6.2）中执行并启用身份验证

目录

简介

本文档介绍了如何对运行 PIX 软件（5.2 版到 6.2 版）的 PIX 防火墙建立经 AAA 身份验证的访问，并提供了有关启用身份验证、系统日志记录以及在 AAA 服务器发生故障时进行访问的信息。与以前的版本代码相比，在PIX 5 3和更新版本中，认证、授权和记帐(AAA)发生的变化是：RADIUS端口是可配置的。

在PIX软件5.2以上的版本中，您可以用五种不同的方式创建AAA验证访问：

- Telnet 验证 - 内部
- 控制台端口认证
- 经认证的 Cisco Secure VPN 客户端 1.1 - 外部
- 经身份验证的 VPN 3000 2.5 - 外部
- 经身份验证的安全壳 (SSH) - 内部或外部

注意：对于最后三种方法，必须在PIX上启用DES或3DES(发**出show** version命令进行验证)。在 PIX 软件 6.0 及更高版本中，也可以加载 PIX 设备管理器 (PDM) 来启用 GUI 管理。PDM 不在本文档讨论范围之内。

有关 PIX 6.2 的身份验证和授权命令的详细信息，请参阅 PIX 6.2：身份验证和授权命令配置示例。

要对运行 PIX 软件 6.3 版本及更高版本的 PIX 防火墙建立经 AAA 身份验证的（直通代理）访问，请参阅 PIX/ASA：使用 TACACS+ 和 RADIUS 服务器进行网络访问的直通代理配置示例。

先决条件

要求

在添加 AAA 身份验证之前，请执行下述任务：

- 发出以下命令以添加PIX的口令：**passwd wwtelnet <local_ip> [<mask>] [<if_name>]**如下例所示，PIX 会自动加密此口令，以生成一个带有关键字 **encrypted** 的加密字符串：
  ```
  passwd OnTrBUG1Tp0edmkr encrypted
  ```
  您不需要添加 **encrypted 关键字。**
- 请确保在添加上述语句后可以通过 Telnet 从内部网络连接到 PIX 的内部接口而*无需 经过 AAA 身份验证。*
- 在必须取消命令的情况下，请在添加身份验证语句时始终让某个连接对 PIX 开放。

通过AAA鉴权(除顺序取决于客户端的SSH以外），用户可以查看PIX密码请求(无论密码是<什么>)，然后请求RADIUS或TACACS用户名和密码。

注意：您无法Telnet至PIX的外部接口。如果是从外部 SSH 客户端连接的，则可在外部接口上使用 SSH。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX 软件版本 5.2、5.3、6.0、6.1 或 6.2
- Cisco 安全 VPN 客户端 1.1
- Cisco VPN 3000 Client 2.5
- Cisco VPN Client 3.0.x（要求使用 PIX 6.0 代码）

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

可配置 RADIUS 端口（5.3 和更高版本）

某些 RADIUS 服务器使用除 1645/1646 之外的 RADIUS 端口（通常为 1812/1813）。 在 PIX 5.3 中，可使用以下命令将 RADIUS 身份验证和记帐端口更改为默认端口 1645/1646 以外的其他端口：

aaa-server radius-authport #

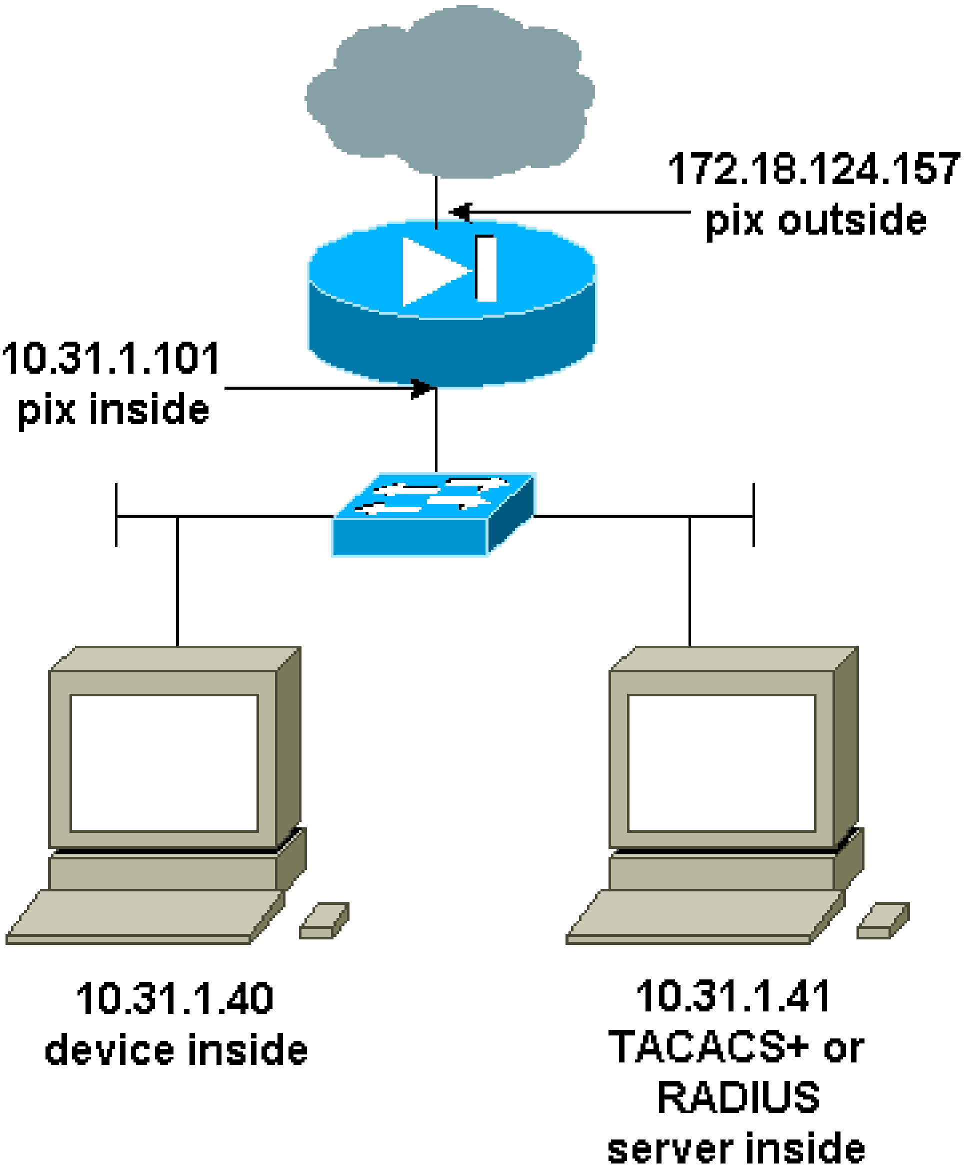
aaa-server radius-acctport #

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Telnet 验证 - 内部

网络图



添加到 PIX 配置的命令

将以下命令添加到配置中：

aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

```
aaa authentication telnet console topix
```

用户可看见PIX密码请求(无论密码是<什么>)，然后看见RADIUS或TACACS用户名和密码请求(存储在10.31.1.41TACACS或RADIUS服务器)。

控制台端口认证

将以下命令添加到配置中：

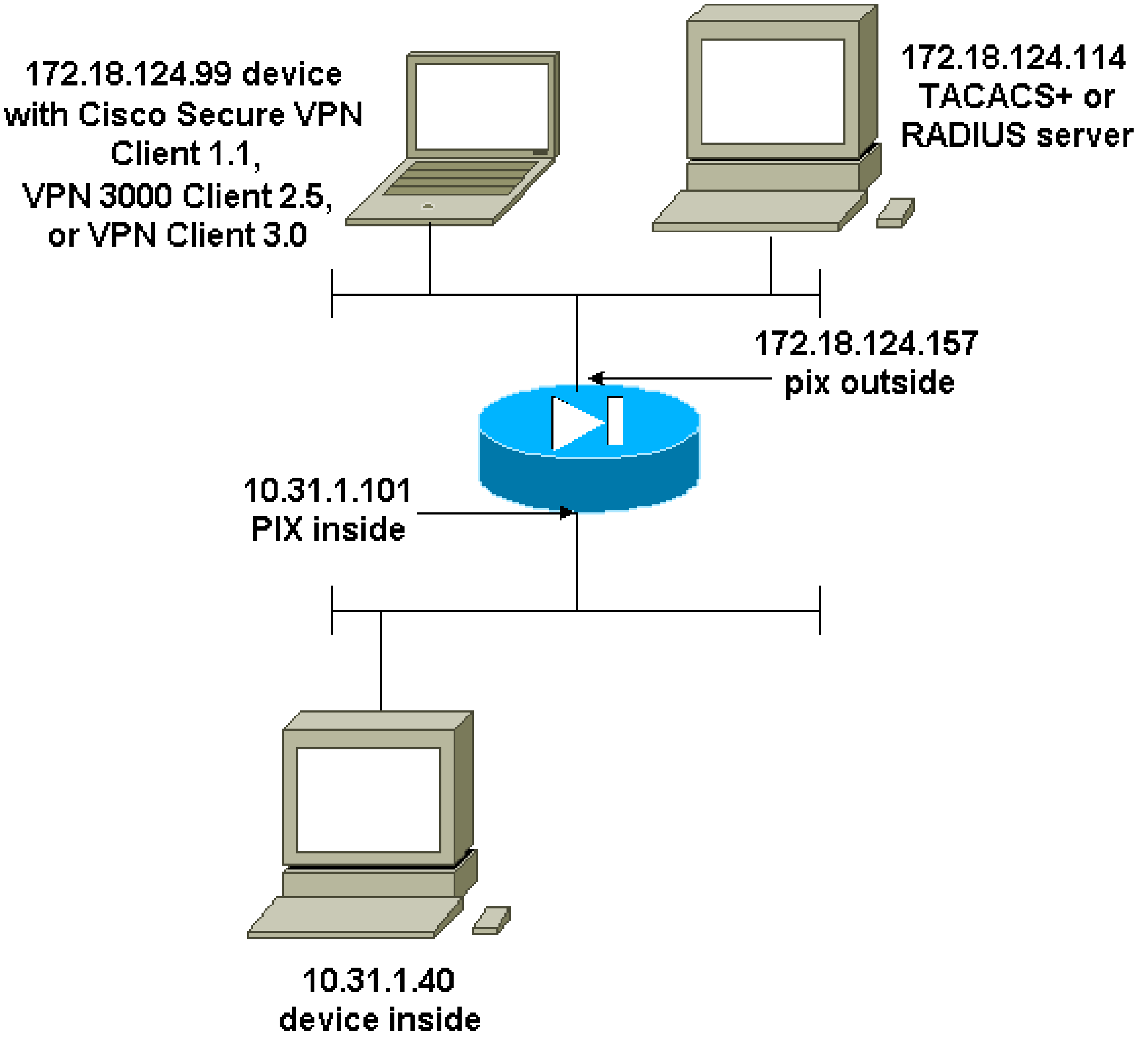
```
aaa-server topix protocol tacacs+

aaa-server topix host 10.31.1.41 cisco timeout 5

aaa authentication serial console topix
```

用户可看见PIX密码请求(无论密码是<什么>)，然后看见RADIUS/TACACS用户名/密码请求(存储在RADIUS或TACACS 10.31.1.41服务器)。

图表 - VPN Client 1.1、VPN 3000 2.5 或 VPN Client 3.0 - 外部



经认证的 Cisco Secure VPN 客户端 1.1 - 外部

经身份验证的 Cisco 安全 VPN 客户端 1.1 - 外部 - 客户端配置

```
1- Myconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP address
          Port all Protocol all
          Pre-shared key (matches that on PIX)

     Connect using secure tunnel
          ID Type: IP address
          172.18.124.157

     Authentication (Phase 1)
     Proposal 1

         Authentication method: Preshared key
         Encryp Alg: DES
         Hash Alg: MD5
         SA life:  Unspecified
         Key Group: DH 1

     Key exchange (Phase 2)
     Proposal 1
         Encapsulation ESP
         Encrypt Alg: DES
         Hash Alg: MD5
         Encap: tunnel
         SA life: Unspecified
         no AH

 2- Other Connections
        Connection security: Non-secure
        Local Network Interface
          Name: Any
          IP Addr: Any
          Port: All
```

经身份验证的 Cisco 安全 VPN 客户端 1.1 - 外部 - 部分 PIX 配置

```
ip address outside 172.18.124.157 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap interface outside
isakmp enable outside
!--- If you know the IP address of the outside client,
use that !--- IP address in this statement. isakmp key
******** address 0.0.0.0 netmask 0.0.0.0 ! isakmp
identity address isakmp policy 10 authentication pre-
share isakmp policy 10 encryption des isakmp policy 10
```

```
hash md5 isakmp policy 10 group 1 isakmp policy 10
lifetime 86400 !--- We knew our client would access the
PIX from this !--- network. If you know the IP address
of the client, use that IP address !--- in this
statement. telnet 172.18.124.0 255.255.255.0 outside
```

经认证的 VPN 3000 2.5 或 VPN 客户端 3.0 - 外部

验证的 VPN 3000 2.5 或 VPN Client 3.0 - 外部- 客户端配置

1. 从 VPN 3000 中选择 **VPN Dialer > Properties > Name the connection。**
2. 选择 **Authentication > Group Access Information**。组名和密码应该与vpngroup < group_name >密码********语句中PIX上的组名和密码相匹配。

当您点击Connect，会出现加密隧道，并且PIX将从测试池分配IP地址(VPN3000客户端仅支持模式配置)。 然后会出现一个终端窗口，您可以通过 Telnet 连接到 172.18.124.157，并且可以通过 AAA 身份验证。PIX上的telnet 192.168.1.x命令允许池中的用户连接到外部接口。

经身份验证的 VPN 3000 2.5 - 外部 - 部分 PIX 配置

```

ip address outside 172.18.124.157 255.255.255.0
ip address inside 10.31.1.101 255.255.255.0
aaa-server topix (outside) host 172.18.124.114 cisco
timeout 5
aaa authentication telnet console topix
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside
isakmp identity address
!!--- ISAKMP Policy for VPN 3000 Client runs 2.5 code.
isakmp policy 10 authentication pre-share isakmp policy
10 encryption des isakmp policy 10 hash md5 !--- The 2.5
client uses group 1 policy (PIX default). isakmp policy
10 group 1 isakmp policy 10 lifetime 86400 !--- ISAKMP
Policy for VPN Client runs 3.0 code. isakmp policy 20
authentication pre-share isakmp policy 20 encryption des
isakmp policy 20 hash md5 !--- The 3.0 clients use D-H
group 2 policy and require PIX 6.0 code. isakmp policy
20 group 2 isakmp policy 20 lifetime 86400 ! vpngroup
vpn3000 address-pool test vpngroup vpn3000 idle-time
1800 vpngroup vpn3000 password ******** telnet
192.168.1.0 255.255.255.0 outside
```

SSH - 内部或外部

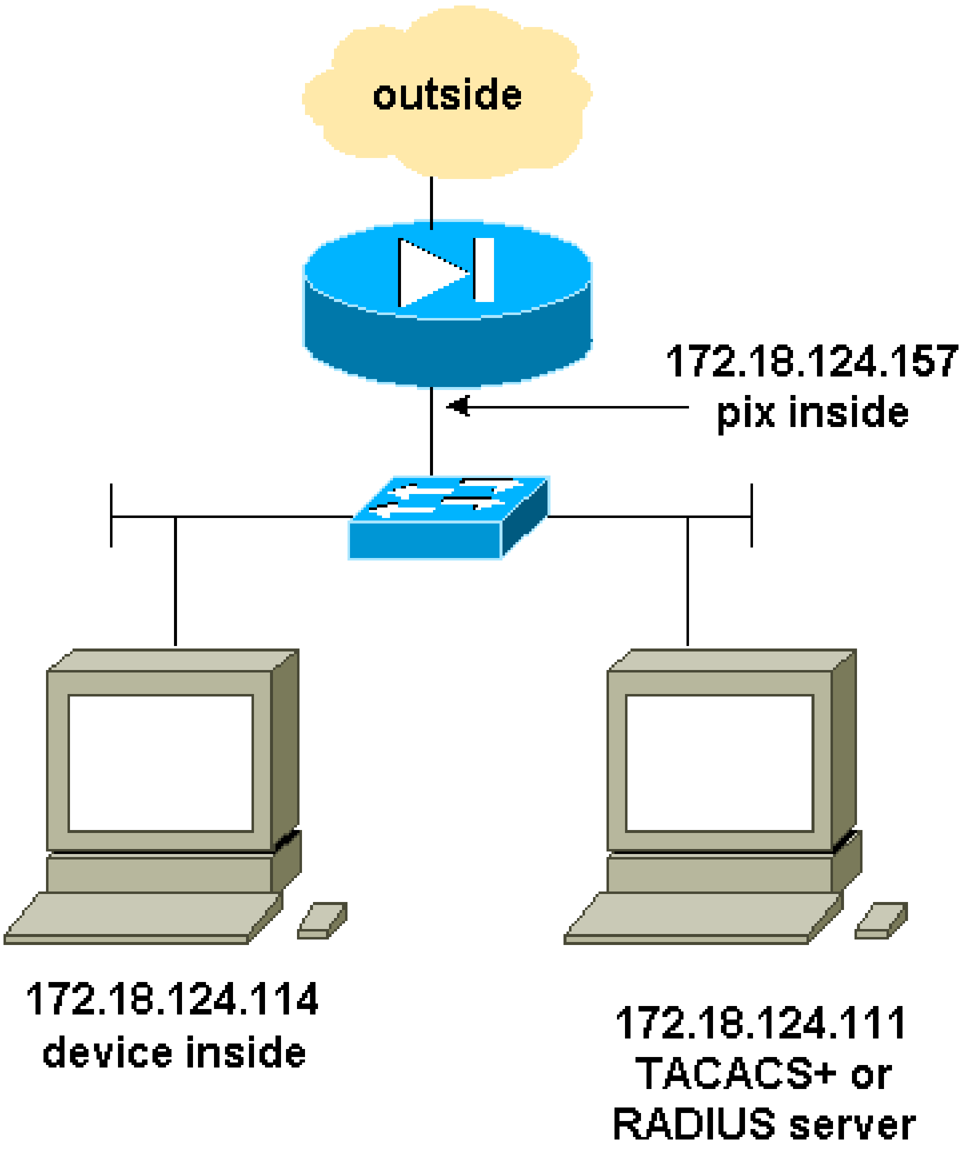
PIX 5.2 添加了对安全壳 (SSH) 版本 1 的支持。SSH 1 以 1995 年 11 月的一份 IETF 草案为基础。SSH 版本 1 和版本 2 互不兼容。有关 SSH 的详细信息，请参阅安全壳 (SSH) 常见问题。

PIX 被视为 SSH 服务器。从SSH客户端（即运行 SSH 的机箱）传输到 SSH 服务器 (PIX) 的数据流将被加密。某些 SSH 第 1 版客户端在 PIX 5.2 发行版本注释中列出。实验室中的测试是使用

NT上的F-Secure SSH 1.1或Solaris版本1.2.26进行的。

注意：对于PIX 7.x，请参阅管理系统访问的允许SSH访问部分。

网络图



配置经 AAA 身份验证的 SSH

要配置经 AAA 身份验证的 SSH，请完成以下步骤：

1. 确保在 AAA 处于打开状态但不使用 SSH 时可以通过 Telnet 连接到 PIX：

   ```
   aaa-server AuthOutbound protocol radius (or tacacs+)
   aaa authentication telnet console AuthOutbound
   aaa-server AuthOutbound host 172.18.124.111 cisco
   ```

   注意：配置SSH时，不需要**telnet 172.18.124.114 255.255.255.255** 命令，因为**SSH 172.18.124.114 255PIX上发**出。255.255.255。加入这两个命令是出于测试目的。
2. 使用以下命令添加 SSH：

   ```
   hostname goss-d3-pix515b
   domain-name rtp.cisco.com
   ca gen rsa key 1024!--- Caution: The RSA key is not be saved without !--- the ca save all
   command. !--- The write mem command does not save it. !--- In addition, if the PIX has
   undergone a write erase !--- or has been replaced, then cutting and pasting !--- the old
   ```

```
configuration does not generate the key. !--- You must re-enter the ca gen rsa key command.
!--- If there is a secondary PIX in a failover pair, the write standby !--- command does
not copy the key from the primary to the secondary. !--- You must also generate and save
the key on the secondary device.

ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
aaa authen ssh console AuthOutbound
logging trap debug
logging console debug
```

3. 在配置模式下发出 **show ca mypubkey rsa 命令。**

```
goss-d3-pix(config)#show ca mypubkey rsa
 % Key pair was generated at: 08:22:25 Aug 14 2000
 Key name: goss-d3-pix.rtp.cisco.com
  Usage: General Purpose Key
  Key Data:
   30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ad4bcb
   e9c174d5 0657a0f3 c94e4b6d 32ac8500 6b84e754 59e20df4 f28c257d 131af21d
   4c0a8f4c e79d8b6d a3520faa 1a42d577 c6adfe51 9d96fa62 f3be07fb 01e082d7
   133cecff bf24f653 bc690b11 ee222070 413c1920 d02321f8 4fc3c5f1 f0c6e077
   81e93184 af55438b dcdcda34 c0a5f5ad 87c435ef
      67170674 4d5ba51e 6d020301 0001
 % Key pair was generated at: 08:27:18 Aug 14 2000
 Key name: goss-d3-pix.rtp.cisco.com.server
  Usage: Encryption Key
  Key Data:
   307c300d 06092a86 4886f70d 01010105 00036b00 30680261 00d4f61b ec45843a
   4ad9266d b125ee26 efc63cc4 e5e9cda4 9418ee53 6e4d16cf 3d0dc864 4d4830c8
   fa7f110e 8a5761ed 4ca73ea7 5d405862 6f3150df 9eb0d11e 9c4d3563 95ff51ae
   6711d60b 9a1415e4 19201d3f 03b455ea c1df9a41 b3a5a73f 4f020301 0001
```

4. 从 Solaris 工作站尝试进行 Telnet 连接：

```
rtp-evergreen#./ssh -c 3des -l cisco -v 172.18.124.157
```

注意：“cisco”是RADIUS/TACACS+服务器上的用户名，172.18.124.157是目标。

配置本地 SSH（没有 AAA 身份验证）

也可以在没有 AAA 服务器的情况下，设置使用本地身份验证的与 PIX 的 SSH 连接。不过，并非每个用户都有独立的用户名。用户名始终为“pix”。

可使用以下命令在 PIX 上配置本地 SSH：

```
hostname goss-d3-pix515b
domain-name rtp.cisco.com
ca gen rsa key 1024!--- Caution: The RSA key is not saved without !--- the ca save all command.
!--- The write mem command does not save it. !--- In addition, if the PIX has undergone a write
erase !--- or has been replaced, then cutting and pasting !--- the old configuration does not
generate the key. !--- You must re-enter the ca gen rsa key command. !--- If there is a
secondary PIX in a failover pair, a write standby !--- command does not copy the key from the
primary to the secondary. !--- You must also generate and save the key on the secondary device.
ssh 172.18.124.114 255.255.255.255 inside
ssh timeout 60
passwd cisco123
```

由于默认用户名在此安排中总是为“PIX”，因此连接到PIX的命令 (该命令是从Solaris设备发出的3DES)是：

```
./ssh -c 3des -1 pix -v <ip_of_pix>
```

SSH 调试

在不使用 debug ssh 命令时进行调试 - 3DES 和 512 位密码

```
109005: Authentication succeeded for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
109011: Authen Session Start: user 'cse', sid 0
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
315011: SSH session from 172.18.124.114 on interface inside
   for user "cse" terminated normally
```

使用 debug ssh 命令进行调试 - 3DES 和 512 位密码

```
goss-d3-pix#debug ssh
SSH debugging on
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - msg type 0x03, length 112
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

调试 - 3DES 和 1024 位密码

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-1.2.26
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse109005:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
```

```
   from 0.0.0.0/0 to 172.18.124.114/0 on interface SSH
315002: Permitted SSH session from 172.18.124.114 on interface inside
   for user "cse"
```

调试 - DES 和 1024 位密码

注意：此输出来自具有SSH的PC，而不是Solaris。

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.99' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-W1.0
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests DES cipher: 2
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid ssh
SSH(ssh): user authen method is 'use AAA', aaa server group ID = 4
SSH(ssh): starting user authentication request,
   and waiting for reply from AAA server
SSH(ssh): user 'ssh' is authenticated
SSH(ssh): user authentication request completed
SSH0: authentication successful for ssh109
SSH0: invalid request - 0x2500
SSH0: starting exec shell5: Authentication succeeded for user 'ssh'
   from 0.0.0.0/0 to 172.18.124.99/0 on interface SSH
109011: Authen Session Start: user 'ssh', sid 1
315002: Permitted SSH session from 172.18.124.99 on interface outside
   for user "ssh"
```

调试 - 3DES 和 2048 位密码

注意：此输出来自具有SSH的PC，而不是Solaris。

```
goss-d3-pix# Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3.
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server
SSH(cse): user 'cse' is authenticated
SSH(cse): user authentication request completed
SSH1: authentication successful for cse10900
SSH1: invalid request - 0x255:
SSH1: starting exec shellAuthentication succeeded for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
109011: Authen Session Start: user 'cse', Sid 2
315002: Permitted SSH session from 161.44.17.151 on interface inside
   for user "cse"
```

可能出现的错误

Solaris 调试 - 2048 位密码和 Solaris SSH

注意：Solaris无法处理2048密码。

```
rtp-evergreen.cisco.com: Initializing random;
seed file /export/home/cse/.ssh/random_seed
RSA key has too many bits for RSAREF to handle (max 1024).
```

RADIUS/TACACS+ 服务器上的口令或用户名错误

```
Device opened successfully.
SSH: host key initialised.
SSH: SSH client: IP = '161.44.17.151' interface # = 1
SSH1: starting SSH control process
SSH1: Exchanging versions - SSH-1.5-Cisco-1.25
SSH1: client version is - SSH-1.5-W1.0
SSH1: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH1: SSH_SMSG_PUBLIC_KEY message sent
SSH1: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 272
SSH1: client requests 3DES cipher: 3
SSH1: keys exchanged and encryption on
SSH1: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA serverss-d3-pix#
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH1: password authentication failed for cse
109006: Authentication failed for user 'cse'
   from 0.0.0.0/0 to 161.44.17.151/0 on interface SSH
```

无法通过以下命令对用户进行授权：

ssh 172.18.124.114 255.255.255.255 inside

尝试连接：

315001：已拒绝内部接口上 161.44.17.151 的 SSH 会话

使用从PIX中删除的密钥(使用ca zero rsa命令)，或使用ca save all命令，取消保存。

```
Device opened successfully.
SSH: unable to retrieve host public key for 'goss-d3-pix.rtp.cisco.com',
   terminate SSH connection.
SSH-2145462416: Session disconnected by SSH server - error 0x00 "Internal error"
315004: Fail to establish SSH session because PIX RSA host key retrieval failed.
315011: SSH session from 0.0.0.0 on interface outside for user ""
   disconnected by SSH server, reason: "Internal error" (0x00)
```

AAA 服务器发生故障：

```
SSH: host key initialised.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
```

```
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x0c
SSH0: SSH_SMSG_PUBLIC_KEY message sent302010: 0 in use, 0 most used
SSH0: SSH_CMSG_SESSION_KEY message received - MSG type 0x03, length 144
SSH0: client requests 3DES cipher: 3
SSH0: keys exchanged and encryption on
SSH0: authentication request for userid cse
SSH(cse): user authen method is 'use AAA', aaa server group ID = 3
SSH(cse): starting user authentication request,
   and waiting for reply from AAA server1090
SSH(cse): user authentication for 'cse' failed
SSH(cse): user authentication request completed
SSH0: password authentication failed for cse0
SSH0: authentication failed for cse
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
2: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109002: Auth from 0.0.0.0/0 to 172.18.124.114/0 failed
   (server 172.18.124.111 failed) on interface outside
109006: Authentication failed for user 'cse' from 0.0.0.0/0
   to 172.18.124.114/0 on interface SSH
315003: SSH login session failed from 172.18.124.114 (1 attempts)
   on interface outside by user "cse"
315011: SSH session from 172.18.124.114 on interface outside for user "cse"
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
109012: Authen Session End: user 'cse', Sid 0, elapsed 352 seconds
```

客户端设置用于3DES，但PIX中只有DES键：

注意：客户端是不支持DES的Solaris。

```
GOSS-PIX# Device opened successfully.
SSH: host key initialised
SSH: license supports DES: 1.
SSH: SSH client: IP = '172.18.124.114' interface # = 0
SSH0: starting SSH control process
SSH0: Exchanging versions - SSH-1.5-Cisco-1.25
SSH0: client version is - SSH-1.5-1.2.26
SSH0: declare what cipher(s) we support: 0x00 0x00 0x00 0x04
SSH0: SSH_SMSG_PUBLIC_KEY message sent
SSH0: Session disconnected by SSH server - error 0x03 "status code: 0x03"
315011: SSH session from 172.18.124.114 on interface outside for user ""
   disconnected by SSH server, reason: "status code: 0x03" (0x03)
```

在我们的 Solaris CLI 上：

```
Selected cipher type 3DES not supported by server.
```

如何从 PIX 删除 RSA 密钥

ca zero rsa

如何将 RSA 密钥保存到 PIX

ca save all

如何允许 SSH 客户端外部的 SSH

ssh outside_ip *255.255.255.255 outside*

启用认证

使用以下命令：

aaa authentication enable console topix

(topix位于我们的服务器列表时)，将提示用户输入发送到TACACS或RADIUS服务器的用户名和密码。由于启用的身份验证数据包与登录的身份验证数据包相同，如果用户可以使用TACACS或RADIUS登录PIX，则他们可以使用相同的用户名/密码通过TACACS或RADIUS启用。

可通过 Cisco Bug ID CSCdm47044（仅限注册用户）获取有关这些问题的详细信息。

Syslogg 信息

当AAA记帐只对通过PIX的连接有效时（对于到达PIX的连接无效），如果设置了系统日志，认证用户的行为信息将被发送到系统日志服务器(和网络管理服务器，如果通过系统日志MIB配置了网络管理服务器)。

如果设置了系统日志记录，则 syslog 服务器上会显示类似如下内容的消息：

日志记录陷阱通知级别：

```
111006: Console Login from pixuser at console
111007: Begin configuration: 10.31.1.40 reading from terminal
111008: User 'pixuser' executed the 'conf' command.
111008: User 'pixuser' executed the 'hostname' command.
```

日志记录陷阱信息级别（包括通知级别）：

307002：来自 10.31.1.40 的经允许的 Telnet 登录会话

在 AAA 服务器发生故障时进行访问

如果 AAA 服务器发生故障，可以先输入 Telnet 口令以访问 PIX，然后输入 **pix 作为用户名，然后再输入启用口令 (enable password whatever)** 作为口令。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。如果启用口令已设置但却未知，则需使用口令恢复磁盘来重置口令。

报告TAC案例应收集的信息

如果在执行以上故障检修步骤后，您还需要援助，希望 Cisco TAC打开一个案例，请确保提供以下信息。
• 问题说明和相关拓扑详细信息 • 在建立案例前所执行的故障诊断及处理措施 • **show tech-support 命令的输出** • 运行 logging buffered debugging 命令后 **show log 命令的输出，或演示问题的控制台捕获信息（如果可用**

)
请将您所收集到的上述数据附加在一个非压缩的、纯文本格式（.txt）文件中。 通过使用Case Query工具进行上载，您可以将此信息附加到您的案例(仅限于注册用户)。 如果您不能访问案例查询工具，您也可以将相关信息发送到attach@cisco.com，请将您的案例编号注在邮件的标题栏上。

相关信息

- Cisco Secure PIX 防火墙命令参考
- PIX RADIUS TACACS+