PIX 6.x ：简单的PIX间的VPN隧道配置示例

目录

简介
先决条件
要求
使用的组件
规则
背景信息
配置
网络图
IKE 与 IPSec 配置
配置
验证
PIX-01 show 命令
PIX-02 show 命令
故障排除
故障排除命令
相关信息

简介

此配置允许两个 Cisco Secure PIX 防火墙在 Internet 或任何使用 IP Security (IPSec) 的公共网络上运行从 PIX 到 PIX 的简单虚拟私有网络 (VPN) 隧道。IPSec由多个开放标准组成，能够在IPSec对端之间提供数据保密性、数据完整性和数据源鉴权。

请参阅 PIX/ASA 7.x：简单的 PIX 到 PIX VPN 隧道配置示例，以了解有关 Cisco 安全设备运行软件版本 7.x 的相同方案的详细信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 具有软件版本 6.3(5) 的 Cisco 安全 PIX 515E 防火墙
- 具有软件版本 6.3(5) 的 Cisco 安全 PIX 515E 防火墙

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

IPSec 协商可分为五个步骤，其中包括两个 Internet Key Exchange (IKE) 阶段。

1. IPsec 隧道由相关数据流启动。如果数据流在 IPsec 对等体之间传输，则它会被认为是相关数据流。
2. 在 IKE 第 1 阶段中，IPsec 对等体对建立的 IKE 安全关联 (SA) 策略进行协商。对等体经过身份验证后，会使用 Internet 安全关联和密钥管理协议 (ISAKMP) 创建安全隧道。
3. 在 IKE 第 2 阶段中，IPsec 对等体使用经身份验证的安全隧道对 IPsec SA 转换进行协商。共享策略的协商决定建立 IPsec 隧道的方式。
4. 根据 IPsec 转换集中配置的 IPsec 参数，将在 IPsec 对等体之间创建 IPsec 隧道并传输数据。
5. 如果删除了 IPsec SA，或者 IPsec SA 的生存时间到期，则 IPsec 隧道将终止。

注意： 如果两个 IKE 阶段的 SA 在对等体上不匹配，则两个 PIX 之间的 IPsec 协商会失败。

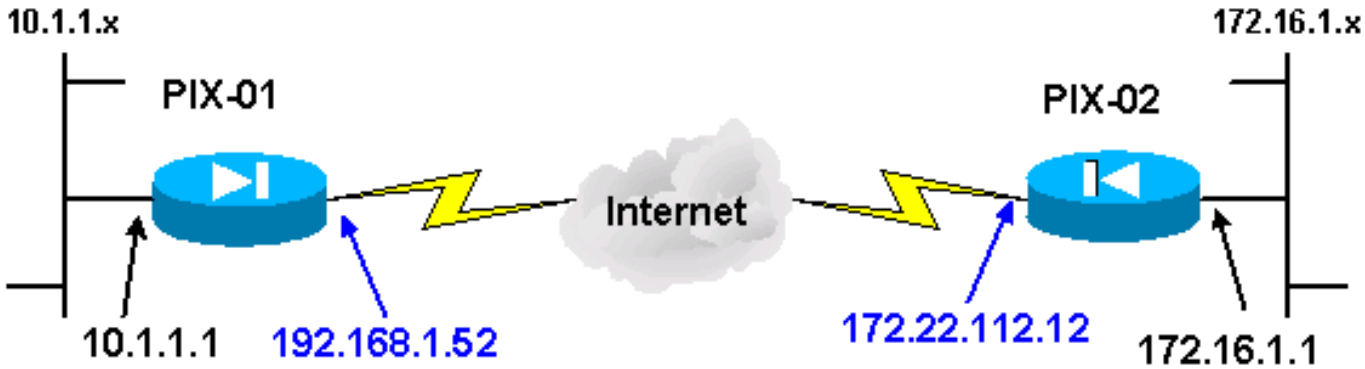
配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可了解有关本文档所使用命令的详细信息。

网络图

本文档使用此网络图：



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些是已在实验室环境中使用的 RFC 1918 地址。

IKE 与 IPSec 配置

仅当插入为加密映射和转换集选择的对等体信息和命名规则时，每个 PIX 上的 IPSec 配置才有所不同。使用 **write terminal** 或 **show** 命令可以验证配置。相关命令包括 **show isakmp**、**show isakmp policy**、**show access-list**、**show crypto IPSec transform-set** 和 **show crypto map**。有关这些命令的详细信息，请参阅 Cisco Secure PIX 防火墙命令参考。

完成以下步骤以配置 IPSec：

1. 配置预共享密钥的 IKE
2. **配置 IPsec**
3. 配置网络地址转换 (NAT)
4. 配置 PIX 系统选项

配置预共享密钥的 IKE

发出 **isakmp enable 命令**以便在 IPSec 终接接口上启用 IKE。在此情况下，外部接口为两个PIX上的IPSec终接接口。需在两个 PIX 上都配置 IKE。这些命令只显示 PIX-01。

```
isakmp enable outside
```

还需要定义在 IKE 协商期间使用的 IKE 策略。为此，请发出 **isakmp policy 命令**。发出此命令时，必须分配优先级，以便唯一地标识策略。在这种情况下，最高优先级1被分配给该策略。该策略还设置为使用预共享密钥、将 MD5 哈希算法用于数据认证、将 DES 用于 Encapsulating Security Payload (ESP) 并使用 Diffie-Hellman 组 1。该策略还设置为使用 SA 生存时间。

```
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

可使用 **show isakmp policy** 命令检验 IKE 配置：

```
PIX-01#show isakmp policy
Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 1000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

最后，发出 **isakmp key 命令**以配置预共享密钥并分配对等体地址。使用预共享密钥时，相同的预共享密钥必须在IPSec对端上匹配。地址会因远程对等体的 IP 地址而异。

```
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
PIX-01#
```

可使用 **write terminal** 或 **show isakmp** 命令检验策略：

```
PIX-01#show isakmp
isakmp enable outside
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp identity address
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

配置 IPsec

当一个 PIX 收到以网络内另一个 PIX 为目标的流量时，会启动 IPsec。此流量被视为需要受 IPsec 保护的相关流量。访问列表用于确定哪些流量启动了 IKE 和 IPsec 协商。此访问列表允许流量从 10.1.1.x 网络通过 IPSec 隧道发送到 172.16.1.x 网络。相反 PIX 配置的访问列表是此访问列表的镜像。这适用于 PIX-01。

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

IPsec 转换集定义对等体用于保护数据流的安全策略。通过使用 **crypto ipsec transform-set** 命令定义 IPsec 转换。必须为转换集选择一个唯一的名称，并且最多可以选择三个转换用于定义 IPsec 安全协议。此配置只使用了两个转换：**esp-hmac-md5** 和 **esp-des**。

```
crypto IPSec transform-set chevelle esp-des esp-md5-hmac
```

加密映射设置加密流量的 IPsec SA。必须分配映射名称和序号才能创建加密映射。然后定义加密映射参数。显示的 crypto map transam 使用 IKE 建立 IPSec SA，加密与访问列表 101 匹配的所有对象，具有 set peer，并且使用 **chevelle transform-set** 规定针对流量的安全策略。

```
crypto map transam 1 IPSec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle
```

定义加密映射后，将加密映射应用于接口。所选的接口必须是 IPsec 终接接口。

```
crypto map transam interface outside
```

发出 **show crypto map 命令**以验证加密映射属性。

```
PIX-01#show crypto map

Crypto Map: "transam" interfaces: { outside }

Crypto Map "transam" 1 IPSec-isakmp
Peer = 172.22.112.12
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255
Current peer: 172.22.112.12
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ chevelle, }
```

配置 NAT

此命令告知 PIX 不要对视为与 IPSec 相关的任何流量进行 NAT。因此，会从 NAT 服务中排除与 **access-list 命令**语句匹配的所有流量。

```
access-list NoNAT permit ip 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0
nat (inside) 0 access-list NoNAT
```

配置 PIX 系统选项

由于所有入局会话都必须经过访问列表或管道的明确许可，因此，使用 **sysopt connection permit-ipsec** 命令允许所有经过 IPSec 鉴权的入局加密会话。对于受 IPSec 保护的流量，第二次管道检查可能没有必要，而且会导致隧道创建失败。**sysopt 命令**可调节各种 PIX 防火墙安全和配置功能。

```
sysopt connection permit-IPSec
```

配置

如果从 Cisco 设备中获得write terminal 命令的输出，则可使用命令输出解释程序（仅限注册用户）显示潜在问题和解决方法。 您必须登录并启用 JavaScript 才能使用命令输出解释程序（仅限注册用户）。

PIX-01（地址为 192.68.1.52）

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-01
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
!--- Sets the outside address on the PIX Firewall. ip
address outside 192.168.1.52 255.255.255.0
!--- Sets the inside address on the PIX Firewall. ip
address inside 10.1.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
```

```
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2: !--- The IPSec transform-set
"chevelle" uses esp-md5-hmac to provide !--- data
authentication.

crypto IPSec transform-set chevelle esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map transam 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 172.22.112.12.
crypto map transam 1 match address 101
!--- Sets the IPSec peer. crypto map transam 1 set peer
172.22.112.12
!--- Sets the IPSec transform set "chevelle" !--- to be
used with the crypto map entry "transam". crypto map
transam 1 set transform-set chevelle
!--- Assigns the crypto map transam to the interface.
crypto map transam interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate the IPSec tunnel

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the pre-shared key between the IPSec peers. !--- The
same preshared key must be configured on the !--- IPSec
peers for IKE authentication. isakmp key ********
address 172.22.112.12 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
!--- The show isakmp policy command shows the
differences in !--- the default and configured policy.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
```

```
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX-02（地址为 172.22.112.12）

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-02
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
!--- Sets the outside address on the PIX Firewall. ip
address outside 172.22.112.12 255.255.255.0
!--- Sets the inside address on the PIX Firewall. ip
address inside 172.16.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 172.22.112.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
```

```
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2:  !--- The IPSec transform set defines
the negotiated security policy !--- that the peers use
to protect the data flow. !--- The IPSec transform-set
"toyota" uses hmac-md5 authentication header !--- and
encapsulates the payload with des.

crypto IPSec transform-set toyota esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map bmw 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 192.168.1.52.
crypto map bmw 1 match address 101
!--- Sets IPSec peer. crypto map bmw 1 set peer
192.168.1.52
!--- Sets the IPSec transform set "toyota" !--- to be
used with the crypto map entry "bmw". crypto map bmw 1
set transform-set toyota
!--- Assigns the crypto map bmw to the interface. crypto
map bmw interface outside
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate IPSec tunnel.

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the preshared key between the IPSec peers. !--- The same
preshared key must be configured on the !--- IPSec peers
for IKE authentication. isakmp key ******** address
192.168.1.52 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
```

```
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

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。

- **show crypto IPSec sa** — 此命令显示 IPSec SA 的当前状态，可用于确定流量是否加密。
- **show crypto isakmp sa** — 此命令显示 IKE SA 的当前状态。

PIX-01 show 命令

PIX-01 show 命令

```
PIX-01#show crypto IPSec sa
interface: outside
Crypto map tag: transam, local addr. 192.168.1.52

local ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
current peer: 172.22.112.12
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are being sent
!--- and received without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 192.168.1.52, remote crypto endpt.:
172.22.112.12
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 6f09cbf1
!--- Shows inbound SAs that are established. inbound esp
sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:
!--- Shows outbound SAs that are established. outbound
ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
```

```
slot: 0, conn id: 2, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-01#show
crypto isakmp sa
     dst             src          state       pending
created
172.22.112.12    192.168.1.52    QM_IDLE          0
1Maui-PIX-01#
```

PIX-02 show 命令

PIX-02 show 命令

```
PIX-02#show crypto IPSec sa

interface: outside
Crypto map tag: bmw, local addr. 172.22.112.12

local ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
current_peer: 192.168.1.52
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are !--- being
sent and recede without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts
decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.22.112.12, remote crypto
endpt.: 192.168.1.52
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 70be0c04
!--- Shows inbound SAs that are established. Inbound ESP
sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:
!--- Shows outbound SAs that are established. Outbound
```

```
ESP sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-02#show
crypto isakmp sa
     dst             src          state       pending
created
172.22.112.12    192.168.1.52    QM_IDLE          0
PIX-02#
```

除非在全局配置模式下配置 management-access 命令，否则无法对 PIX 的内部接口执行 ping 操作以形成隧道。

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

注意： clear 命令必须在配置模式下执行。

- **clear crypto ipsec sa** — 此命令在尝试对 VPN 隧道进行协商失败后重置 IPSec SA。
- **clear crypto isakmp sa** — 此命令在尝试对 VPN 隧道进行协商失败后重置 ISAKMP SA。

注意： 发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **debug crypto ipsec** — 此命令显示客户端是否在对 VPN 连接的 IPSec 部分进行协商。
- **debug crypto isakmp** — 此命令显示对等体是否在对 VPN 连接的 ISAKMP 部分进行协商。

在连接完成后，可以使用 **show** 命令进行验证。

相关信息

- PIX 支持页
- PIX 命令参考
- 请求注解 (RFC)
- IPsec 协商/IKE 协议支持页
- 技术支持和文档 - Cisco Systems