PIX 6.x:簡單PIX到PIX VPN隧道配置示例

目錄

簡介

此配置允許兩個Cisco Secure PIX防火牆通過Internet或任何使用IP安全(IPSec)的公共網路運行從PIX到PIX的簡單虛擬專用網路(VPN)隧道。IPSec是開放標準的組合，可在IPSec對等體之間提供資料機密性、資料完整性和資料來源身份驗證。

請參閱PIX/ASA 7.x:簡單的PIX到PIX VPN隧道配置示例，瞭解有關思科安全裝置運行軟體版本7.x的相同方案的詳細資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco安全PIX 515E防火牆，軟體版本6.3(5)
- Cisco安全PIX 515E防火牆，軟體版本6.3(5)

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

IPSec交涉可分為五個步驟，其中包括兩個網際網路金鑰交換(IKE)階段。

1. IPSec隧道由相關流量發起。流量在IPSec對等體之間傳輸時被認為很有趣。
2. 在IKE第1階段，IPSec對等體協商已建立的IKE安全關聯(SA)策略。對等點通過驗證後，會使用網際網路安全性關聯和金鑰管理通訊協定(ISAKMP)建立安全通道。
3. 在IKE第2階段，IPSec對等體使用經過身份驗證的安全隧道協商IPSec SA轉換。共用策略的協商決定如何建立IPSec隧道。
4. 系統將建立IPSec隧道，並根據IPSec轉換集中配置的IPSec引數在IPSec對等體之間傳輸資料。
5. IPSec SA被刪除或其生存期到期時，IPSec隧道將終止。

注意：如果兩個IKE階段上的SA在對等體上不匹配，則兩個PIX之間的IPSec協商將失敗。

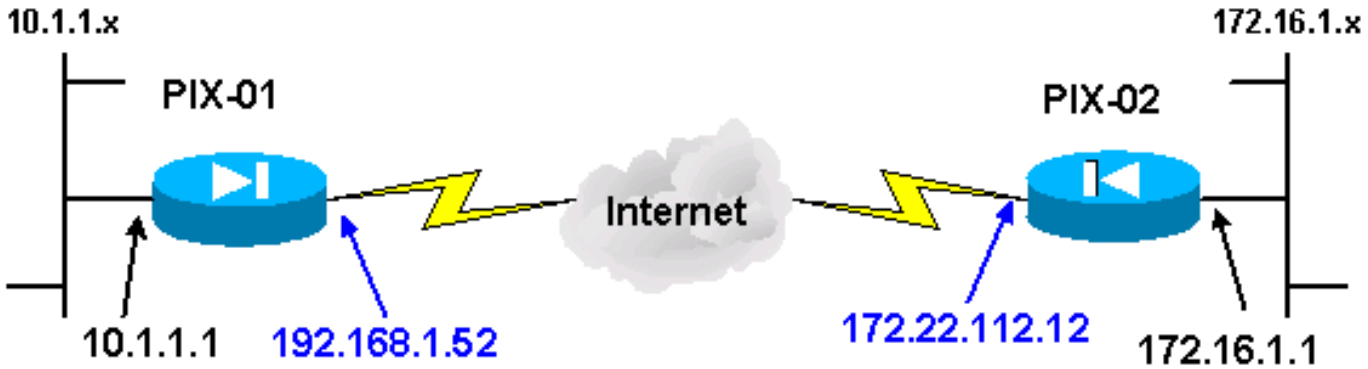
設定

本節提供用於設定本文件中所述功能的資訊。

附註：使用命令查詢工具(僅限註冊客戶)以瞭解有關本文檔中所用命令的更多資訊。

網路圖表

本檔案會使用以下網路圖表：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。以下是RFC 1918 位址，已在實驗室環境中使用。

IKE和IPSec配置

只有在插入對等體資訊以及為加密對映和轉換集選擇的命名約定時，每個PIX上的IPSec配置才會變化。可使用**write terminal**或**show**命令驗證配置。相關命令包括show isakmp、**show isakmp policy**、**show access-list**、**show crypto IPSec transform-set**和**show crypto map**。有關這些命令的詳細資訊，請參閱Cisco Secure PIX防火牆命令參考。

完成以下步驟即可配置IPSec:

1. 為預共用金鑰配置IKE
2. 配置IPSec
3. 設定網路位址轉譯(NAT)
4. 配置PIX系統選項

為預共用金鑰配置IKE

發出**isakmp enable**命令，以便在IPSec終端介面上啟用IKE。在此方案中，外部介面是兩個PIX上的IPSec終端介面。兩個PIX上都配置了IKE。這些命令僅顯示PIX-01。

```
isakmp enable outside
```

您還需要定義IKE協商期間使用的IKE策略。發出**isakmp policy**命令可執行此操作。發出此命令時，必須分配優先順序以便唯一標識策略。在這種情況下，將最高優先順序1分配給策略。此策略還設定為使用預共用金鑰、用於資料身份驗證的MD5雜湊演算法、用於封裝安全負載(ESP)的DES以及Diffie-Hellman組1。此策略還設定為使用SA生存期。

```
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
```

可以使用**show isakmp policy**命令驗證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
```

最後，發出**isakmp key**命令以配置預共用金鑰並分配對等體地址。使用預共用金鑰時，IPSec對等體上的同一預共用金鑰必須匹配。地址不同，這取決於遠端對等裝置的IP地址。

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

可以使用**write terminal**或**show isakmp**命令驗證策略：

```
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

當其中一個PIX收到發往另一個PIX內部網路的流量時，會啟動IPSec。此流量被視為需要由IPSec保護的感興趣流量。訪問清單用於確定哪些流量發起IKE和IPSec協商。此存取清單允許流量從10.1.1.x網路透過IPSec通道傳送到172.16.1.x網路。相反的PIX配置上的訪問清單將映象此訪問清單。這適用於PIX-01。

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

IPSec轉換集定義對等體用於保護資料流的安全策略。IPSec轉換通過使用**crypto IPSec transform-set**命令定義。必須為轉換集選擇唯一的名稱，並且最多可以選擇三個轉換來定義IPSec安全協定。此配置僅使用兩種轉換：**esp-hmac-md5**和**esp-des**。

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

加密對映為加密流量設定IPSec SA。您必須分配對映名稱和序列號才能建立加密對映。然後定義加密對映引數。顯示的加密對映轉換使用IKE建立IPSec SA，加密任何與訪問清單101匹配的內容，具有設定的對等體，並使用**chevelle** transform-set為流量實施其安全策略。

```
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
```

定義密碼編譯對應後，請將該密碼編譯對應套用到介面。您選擇的介面必須是IPSec終端介面。

```
crypto map transam interface outside
```

發出**show crypto map**命令以驗證加密對映屬性。

```
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不要對IPSec感興趣的任何流量進行NAT。因此，與**access-list**命令語句匹配的所有流量都免於NAT服務。

```
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系統選項

由於所有入站會話都必須由訪問清單或管道明確允許，因此**sysopt connection permit-IPSec**命令用於允許所有入站IPSec驗證的密碼會話。使用IPSec保護的流量時，輔助管道檢查可以是冗餘的，並導致隧道建立失敗。**sysopt**命令可調整各種PIX防火牆安全和配置功能。

```
sysopt connection permit-IPSec
```

組態

如果您的Cisco裝置具有**write terminal**命令的輸出，可以使用Output Interpreter (僅限註冊客戶)顯示潛在問題和修正程式。您必須登入並啟用JavaScript才能使用Output Interpreter (僅限註冊客戶)。

192.68.1.52的PIX-01

```
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位於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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

Output Interpreter Tool (僅供註冊客戶使用)支援某些**show**命令，這允許您檢視show命令輸出的分析。

- **show crypto IPSec sa** — 此命令顯示IPSec SA的當前狀態，在確定流量是否正在加密時很有用。
- **show crypto isakmp sa** — 此命令顯示IKE SA的當前狀態。

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#
```

除非在全域性配置模式下配置了management-access 命令，否則無法ping通PIX的內部介面以形成隧道。

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

注意：clear命令必須在配置模式下執行。

- **clear crypto IPSec sa** — 此命令在嘗試協商VPN隧道失敗後重置IPSec SA。
- **clear crypto isakmp sa** — 此命令在嘗試協商VPN隧道失敗後重置ISAKMP SA。

註：發出debug指令之前，請先參閱有關Debug指令的**重要**資訊。

- **debug crypto IPSec** — 此命令顯示客戶端是否正在協商VPN連線的IPSec部分。
- **debug crypto isakmp** — 此命令顯示對等體是否正在協商VPN連線的ISAKMP部分。

連線完成後，可以使用**show**命令進行驗證。

相關資訊

- PIX支援頁
- PIX命令參考
- 要求建議(RFC)
- IPSec協商/IKE通訊協定支援頁面
- 技術支援與文件 - Cisco Systems