PIX 6.x：簡単な PIX-to-PIX VPN トンネルの設定例

内容

概要

この設定により、2 つの Cisco Secure PIX Firewall は、インターネットまたは IP Security（IPsec）を使用する任意のパブリック ネットワーク経由で PIX 間の簡単なバーチャル プライベート ネットワーク（VPN）トンネルを稼働できます。IPSec とは、IPSec ピア間でデータの機密性、データの完全性、およびデータの発信元の認証を提供するオープン スタンダードを組み合わせたものです。

ソフトウェア バージョン 7.x が稼働する Cisco セキュリティ アプライアンスでのサイト間 IPSec VPN の設定方法の詳細については、『PIX/ASA 7.x：Ciscoセキュリティアプライアンスでソフトウェアバージョン7.xが稼働している同じシナリオの詳細は、『PIX-to-PIX VPNトンネルの簡単な設定例』を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアバージョン6.3が稼働するCisco Secure PIX 515E Firewall
- ソフトウェアバージョン6.3が稼働するCisco Secure PIX 515E Firewall

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

IPSecネゴシエーションは、2つのインターネットキーエクスチェンジ(IKE)フェーズを含む5つのステップに分けることができます。

1. 対象トラフィックによって IPSec トンネルが開始されます。IPsec ピアの間を転送されるトラフィックは、対象トラフィックとみなされます。
2. IKE フェーズ 1 では、IPSec ピア同士が、IKE Security Association（SA; セキュリティ結合）ポリシーについてネゴシエートします。ピアが認証されると、Internet Security Association and Key Management Protocol（ISAKMP）を使用して安全なトンネルが作成されます。
3. IKE フェーズ 2 では、IPSec ピア同士が認証済みの安全なトンネルを使用して、IPSec SA トランスフォームをネゴシエートします。共有ポリシーのネゴシエーションによって、IPsec トンネルの確立方法が決まります。
4. IPSec トンネルが作成され、IPSec トランスフォーム セットに設定された IPSec パラメータに基づいて、IPSec 間でデータが伝送されます。
5. IPsec SA が削除されるか、そのライフタイムの有効期限が切れると、IPsec トンネルは終了します。

注：ピアで両方のIKEフェーズのSAが一致しない場合、2つのPIX間のIPSecネゴシエーションは失敗します。

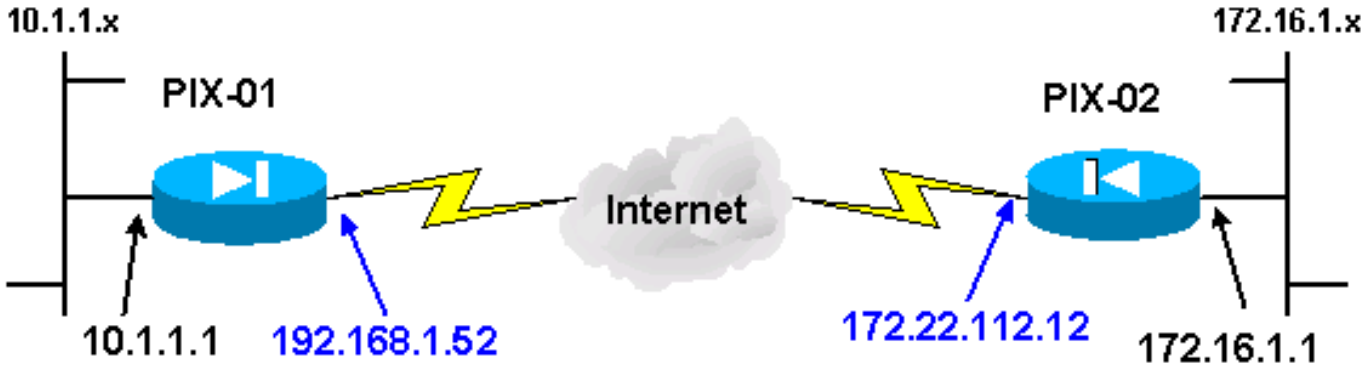
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このドキュメントで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワークダイアグラムを使用します。



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 でのアドレスであり、ラボ環境で使用されたものです。

IKE と IPSec 設定

各PIXのIPSec設定は、ピア情報と、暗号マップとトランスフォームセットに対して選択された命名規則を挿入した場合にのみ異なります。設定は、**write terminal**コマンドまたは**show**コマンドを使用して確認できます。該当するコマンドは、show isakmp、show isakmp policy、show access-list、show crypto ipsec transform-set、および show crypto map です。これらのコマンドの詳細は、『Cisco Secure PIX Firewallコマンドリファレンス』を参照してください。

IPSecを設定するには、次の手順を実行します。

1. 事前共有キーのIKEの設定
2. IPSec の設定
3. ネットワークアドレス変換(NAT)の設定
4. PIXシステムオプションの設定

事前共有キーのIKEの設定

IPSec終端インターフェイスでIKEを有効にするには、**isakmp enable**コマンドを発行します。このシナリオでは、両 PIX の外部インターフェイスが IPSec 終端インターフェイスになります。IKEは両方のPIXで設定されます。これらのコマンドは、PIX-01のみを表示します。

```
isakmp enable outside
```

また、IKEネゴシエーション中に使用されるIKEポリシーを定義する必要があります。これを行うには、**isakmp policy**コマンドを発行します。このコマンドを発行する場合は、ポリシーが一意に識別されるようにプライオリティレベルを割り当てる必要があります。このケースでは、最もプライオリティの高い 1 をポリシーに割り当てます。ポリシーは、事前共有キー、データ認証用のMD5ハッシュアルゴリズム、Encapsulating Security Payload(ESP)用のDES、およびDiffie-Hellman group1を使用するように設定されます。また、SAライフタイムを使用するように設定されます。

```
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
```

IKE コンフィギュレーションは、show isakmp policy コマンドで確認できます。

```
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
```

最後に、**isakmp key**コマンドを発行して、事前共有キーを設定し、ピアアドレスを割り当てます。事前共有鍵を使用する場合は、IPSec ピアに同じ共有鍵を設定する必要があります。アドレスは、リモートピアのIPアドレスによって異なります。

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

ポリシーは、write terminal コマンドまたは show isakmp コマンドを使用して確認できます。

```
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
```

IPSec の設定

IPSecは、一方のPIXが他方のPIX内部ネットワークを宛先とするトラフィックを受信すると開始されます。このトラフィックは、IPSec による保護が必要な対象トラフィックと見なされます。アクセス リストを使用することにより、IKE と IPsec のネゴシエーションを開始させるトラフィックを指定できます。このアクセスリストは、IPSecトンネルを介して10.1.1.xネットワークから172.16.1.xネットワークにトラフィックを送信することを許可します。反対のPIX設定のアクセスリストは、このアクセスリストをミラーリングしています。これはPIX-01に適しています。

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

IPSec トランスフォーム セットは、データ フローを保護するためにピアで使用されるセキュリティポリシーを定義します。IPsec トランスフォームを定義するには、**crypto ipsec transform-set コマンドを使用します。**トランスフォーム セットには一意の名前を付ける必要があり、IPSec セキ

ユリティ プロトコルを定義するために最大 3 つのトランスフォームを選択できます。この設定は、2 つの変換だけを使用します。**esp-hmac-md5**と**esp-des**。

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

暗号マップは、暗号化トラフィック用の IPSec SA を設定します。暗号マップを作成するには、マップ名とシーケンス番号を割り当てる必要があります。次に、暗号マップパラメータを定義します。表示される暗号マップtransamは、IKEを使用してIPSec SAを確立し、アクセスリスト101に一致するすべてのトラフィックを暗号化し、セットピアを持ち、**chevelle** transform-setを使用してトラフィックのセキュリティポリシーを確立します。

```
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
```

暗号マップを定義したら、暗号マップをインターフェイスに適用します。選択するインターフェイスは、IPSec終端インターフェイスである必要があります。

```
crypto map transam interface outside
```

show crypto mapコマンドを発行して、クリプトマップの属性を確認します。

```
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, }
```

NAT の設定

このコマンドは、IPSecの対象と見なされるトラフィックをNAT処理しないようにPIXに指示します。したがって、**access-list**コマンド文に一致するすべてのトラフィックは、NATサービスから除外されます。

```
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
```

PIXシステムオプションの設定

着信セッションはすべて、アクセス リストまたはコンジットによって明示的に許可される必要があるため、sysopt connection permit-ipsec コマンドを使用して、すべての着信 IPSec 認証済み暗号化セッションを許可します。IPSecで保護されたトラフィックでは、セカンダリコンジットチェックが冗長になり、トンネルの作成が失敗する可能性があります。sysoptコマンド**は、さまざまな**PIXファイアウォールのセキュリティ機能と設定機能を調整します。

```
sysopt connection permit-IPSec
```

設定

ご使用のシスコ デバイスの **write terminal コマンドの出力データがある場合は、**アウトプット インタープリタ（登録ユーザ専用）を使用して、今後予想される障害や修正を表示できます。 アウトプットインタープリタ（登録ユーザ専用）を使用するには、ログインして、JavaScriptを有効にする必要があります 。

PIX-01(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(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
```

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- **show crypto IPSec sa**：このコマンドは、IPSec SAの現在のステータスを表示し、トラフィックが暗号化されているかどうかを判別するのに役立ちます。
- **show crypto isakmp sa**：このコマンドは、IKE SAの現在の状態を表示します。

PIX-01 showコマンド

PIX-01 showコマンド

```
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コマンド

PIX-02 showコマンド

```
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#
```

グローバルコンフィギュレーションモードでmanagement-accessコマンドを設定しない限り、PIXの内部インターフェイスにpingを発行してトンネルを形成することはできません。

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

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

注：clearコマンドは設定モードで実行する必要があります。

- **clear crypto IPSec sa**：このコマンドは、VPNトンネルのネゴシエートに失敗した後で、IPSec SAをリセットします。
- **clear crypto isakmp sa**：このコマンドは、VPNトンネルのネゴシエートに失敗した後でISAKMP SAをリセットします。

注：debugコマンドを発行する前に、『debugコマンドの重要な情報』を参照してください。

- **debug crypto IPSec**：クライアントがVPN接続のIPSec部分をネゴシエートしているかどうかを表示します。
- **debug crypto isakmp**：ピアがVPN接続のISAKMP部分をネゴシエートしているかどうかを表示します。

接続が完了したら、**show**コマンドを使用して確認できます。

関連情報

- PIX に関するサポート ページ
- PIX コマンド リファレンス
- Request for Comments (RFC)
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- テクニカル サポートとドキュメント – Cisco Systems