

# VPN サービス モジュール搭載 Catalyst 6500 と PIX ファイアウォール間の IPSec LAN-to-LAN トンネルの設定例

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[レイヤ2のアクセスポートまたはトランクポートを使用したIPSecの設定](#)

[ルーテッドポートを使用したIPSecの設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

## 概要

このドキュメントでは、IPSec VPN サービス モジュール ( W ) を搭載した Cisco Catalyst 6500 シリーズ スイッチと Cisco PIX Firewall の間に IPSec LAN-to-LAN トンネルを作成する方法について説明します。

## 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。

- IPSec VPN サービスモジュールを搭載した Catalyst 6000 シリーズスーパーバイザエンジン用 Cisco IOS® ソフトウェア リリース 12.2(14)SY2
- Cisco PIX Firewall ソフトウェアバージョン 6.3(3)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## [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](#)

Catalyst 6500 VPN サービス モジュールには 2 つの Gigabit Ethernet ( GE; ギガビット イーサネット ) ポートがありますが、外部から見えるコネクタはありません。これらのポートは、設定の目的にのみアドレスを指定できます。ポート 1 は、常に内部ポートです。このポートでは、内部ネットワークと送受信されるすべてのトラフィックが処理されます。2 つ目のポート ( ポート 2 ) では、WAN や外部ネットワークと送受信されるすべてのトラフィックが処理されます。2 つのポートは常に 802.1Q トランキング モードに設定されます。VPN サービス モジュールでは、パケット フローに Bump In The Wire ( BITW ) と呼ばれる技術が使用されます。

パケットは、1 対の VLAN、1 つのレイヤ 3 内部 VLAN、および 1 つのレイヤ 2 外部 VLAN によって処理されます。内部から外部へ伝送されるパケットは、Encoded Address Recognition Logic ( EARL ) という方式で内部 VLAN ヘルレーティングされます。VPN サービス モジュールでは、パケットを暗号化した後、対応する外部 VLAN が使用されます。復号化プロセスでは、外部から内部へ入るパケットは外部 VLAN を使用して VPN サービス モジュールにブリッジされます。VPN サービス モジュールがパケットを復号化し、VLAN を対応する内部 VLAN にマッピングすると、パケットは EARL によって適切な LAN ポートヘルレーティングされます。レイヤ 3 内部 VLAN とレイヤ 2 外部 VLAN は、`crypto connect vlan` コマンドで結合されます。Catalyst 6500 シリーズ スイッチには、3 種類のポートがあります。

- **ルーテッドポート**：デフォルトでは、すべてのイーサネットポートは Cisco IOS のルーテッドポートです。これらのポートには、隠し VLAN が 1 つ関連付けられています。
- **アクセスポート**：これらのポートには、外部または VLAN トランク プロトコル (VTP) VLAN が関連付けられています。定義済み VLAN には、複数のポートを関連付けることができます。
- **トランクポート**：これらのポートは多数の外部 VLAN または VTP VLAN を伝送し、すべてのパケットが 802.1Q ヘッダーでカプセル化されます。

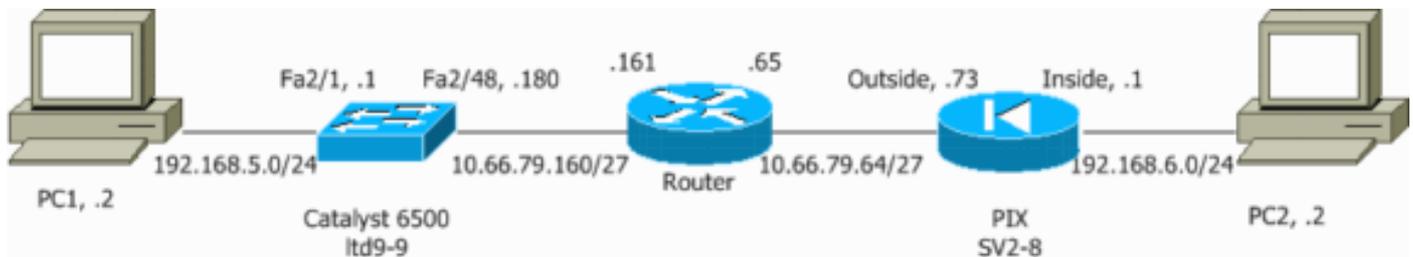
## [設定](#)

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ているコマンドの詳細を調べるには、[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 セットアップを使用します。



## レイヤ2のアクセスポートまたはトランクポートを使用したIPSecの設定

外部物理インターフェイスにレイヤ2のアクセスポートまたはトランクポートを使用してIPSecを設定するには、次のステップを実行します。

1. 内部VLANをVPNサービスモジュールの内部ポートに追加します。VPNサービスモジュールがスロット4にあるとします。内部VLANとしてVLAN 100を、外部VLANとしてVLAN 209を使用します。VPNサービスモジュールのGEポートを次のように設定します。

```
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. VLAN 100インターフェイスと、トンネルが終端するインターフェイス(この場合はinterface Vlan 209)を追加します。

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface Vlan209
no ip address
crypto connect vlan 100
```

3. 外部物理ポートをアクセスポートまたはトランクポートとして設定します(この場合は、FastEthernet 2/48を次に示します)。

```
!--- This is the configuration that uses an access port. interface FastEthernet2/48
no ip address
switchport
switchport access vlan 209
switchport mode access
```

```
!--- This is the configuration that uses a trunk port. interface FastEthernet2/48
no ip address switchport
```

```
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. バイパスNATを作成します。次のネットワーク間で NAT を免除するには、no nat ステートメントにこれらのエントリを追加します。

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

5. 暗号設定と、暗号化するトラフィックを定義するための Access Control List ( ACL; アクセスコントロール リスト ) を作成します。次のように、内部ネットワーク192.168.5.0/24からリモートネットワーク192.168.6.0/24へのトラフィックを定義するクリプトACL ( この場合はACL 100 – 対象トラフィック ) を作成します。

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

次のように、Internet Security Association and Key Management Protocol ( ISAKMP ) ポリシーのプロポーザルを定義します。

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

事前共有キーを使用し、定義するために、( この例では ) 次のコマンドを発行します。

```
crypto isakmp key cisco address 10.66.79.73
```

次のように、IPSec プロポーザルを定義します。

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

次のように、crypto map 文を作成します。

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.73
set transform-set cisco
match address 100
```

6. 次のように、暗号マップを VLAN 100 インターフェイスに適用します。

```
interface vlan100
crypto map cisco
```

次の設定が使用されます。

- [Catalyst 6500](#)
- [PIX ファイアウォール](#)

#### Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
```

```

authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.73
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that
Internet Key Exchange (IKE) !--- is used to establish
the IPsec !--- security associations (SAs) to protect
the traffic !--- specified by this crypto map entry.
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.73
set transform-set cisco
match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
ip address 192.168.5.1 255.255.255.0
!
!--- This is the outside Layer 2 port that allows !---
VLAN 209 traffic to enter. interface FastEthernet2/48 no
ip address switchport switchport trunk encapsulation
dot1q switchport mode trunk ! interface
GigabitEthernet4/1 no ip address flowcontrol receive on
flowcontrol send off switchport switchport trunk
encapsulation dot1q !--- VLAN 100 is defined as the
Interface VLAN (IVLAN). switchport trunk allowed vlan
1,100,1002-1005
switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
!--- The Port VLAN (PVLAN) configuration is handled
transparently by !--- the VPN service module without
user configuration !--- or involvement. It also is not
shown in the configuration. !--- Note: For every IVLAN,
a corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port !--- of the VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco

```

```
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
interface Vlan209 no ip address crypto connect vlan 100
!
ip classless

global (outside) 1 interface
!--- NAT 0 prevents NAT for networks specified in the
ACL inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.5.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration. access-list inside_nat0_outbound permit
ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

## PIX ファイアウォール

```
SV2-8(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
domain-name cisco.com
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 ils 389
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
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
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
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 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 uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- These are IPsec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address 100
```

```
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ***** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end
```

## ルーテッド ポートを使用した IPsec の設定

外部物理インターフェイスにレイヤ 3 ルーテッド ポートを使用して IPsec を設定するには、次のステップを実行します。

1. 内部 VLAN を VPN サービス モジュールの内部ポートに追加します。VPN サービスモジュールがスロット4にあるとします。内部VLANとしてVLAN 100を、外部VLANとしてVLAN 209を使用します。VPN サービス モジュールの GE ポートを次のように設定します。

```
interface GigabitEthernet4/1
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,100,1002-1005
switchport mode trunk
cdp enable
```

```
interface GigabitEthernet4/2
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,209,1002-1005
switchport mode trunk
cdp enable
spanning-tree portfast trunk
```

2. VLAN 100 インターフェイスと、トンネルが終端するインターフェイス ( 次に示すように、この場合は FastEthernet2/48 ) を追加します。

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

```
interface FastEthernet2/48
no ip address
crypto connect vlan 100
```

3. バイパスNATを作成します。次のネットワーク間で NAT を免除するには、no nat ステートメントにこれらのエントリを追加します。

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

4. 暗号設定と、暗号化するトラフィックを定義するための ACL を作成します。次のように、内部ネットワーク 192.168.5.0/24 からリモート ネットワーク 192.168.6.0/24 へ送信されるトラフィックを定義する ACL ( この場合は ACL 100 ) を作成します。

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

次のように、ISAKMP ポリシー のプロポーザルを定義します。

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

事前共有キーを使用し、定義するために、( この例では ) 次のコマンドを発行します。

```
crypto isakmp key cisco address 10.66.79.73
```

次のように、IPSec プロポーザルを定義します。

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

次のように、crypto map 文を作成します。

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.73
set transform-set cisco
match address 100
```

5. 次のように、暗号マップを VLAN 100 インターフェイスに適用します。

```
interface vlan100
crypto map cisco
```

次の設定が使用されます。

- [Catalyst 6500](#)
- [PIX ファイアウォール](#)

### Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.73
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
```

```

with mode ipsec-isakmp. !--- This indicates that IKE is
used to establish the !--- IPsec SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
  set peer 10.66.79.73
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
  ip address 192.168.5.1 255.255.255.0
!
!--- This is the secure port that is configured in
routed port mode. !--- This routed port mode does not
have a Layer 3 IP address !--- configured. This is
normal for the BITW process. !--- The IP address is
moved from this interface to the VLAN 100 to !---
accomplish BITW. This brings the VPN service module into
!--- the packet path. This is the Layer 2 port VLAN on
which the !--- outside port of the VPN service module
also belongs. ! interface FastEthernet2/48 no ip address
crypto connect vlan 100
!
interface GigabitEthernet4/1
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
!--- VLAN 100 is defined as the IVLAN. switchport trunk
allowed vlan 1,100,1002-1005
  switchport mode trunk
  cdp enable
!
interface GigabitEthernet4/2
  no ip address
  flowcontrol receive on
  flowcontrol send off
  switchport
  switchport trunk encapsulation dot1q
!--- The PVLAN configuration is handled transparently by
the !--- VPN service module without user configuration
!--- or involvement. It also is not shown in the
configuration. !--- Note: For every IVLAN, a
corresponding PVLAN exists.

switchport trunk allowed vlan 1,209,1002-1005
  switchport mode trunk
  cdp enable
  spanning-tree portfast trunk
!
interface Vlan1
  no ip address
  shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port of the !--- VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224 crypto map cisco

```

```

!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
! ip classless global (outside) 1 interface !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.6.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration.

access-list inside_nat0_outbound permit ip 192.168.5.0
0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

## PIX ファイアウォール

```

SV2-8(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
domain-name cisco.com
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 ils 389
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
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
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
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 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 uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- These are IPsec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
```

```
crypto map cisco 10 match address 100
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ***** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end
```

## 確認

このセクションでは、設定が正常に動作しているかどうかを確認するための情報について説明しています。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- `show crypto ipsec sa` : 現在のIPSec SAで使用されている設定を表示します。
- `show crypto isakmp sa` : ピアにある現在のすべてのIKE SAを表示します。
- `show crypto vlan` : 暗号設定に関連付けられたVLANを表示します。
- `show crypto eli:VPN` : VPNサービスモジュールの統計情報を表示します。

IPSec の確認とトラブルシューティングの詳細については、『[IP Security のトラブルシューティング - debug コマンドの理解と使用](#)』を参照してください。

## トラブルシューティング

このセクションでは、設定のトラブルシューティングを行うための情報について説明します。

### トラブルシューティングのためのコマンド

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` : フェーズ 2 の IPSec ネゴシエーションを表示します。
- `debug crypto isakmp` : フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- `debug crypto engine` : 暗号化されたトラフィックを表示します。
- `clear crypto isakmp` : フェーズ 1 に関連する SA をクリアします。
- `clear crypto ipsec` : フェーズ 2 に関連する SA をクリアします。

IPSec の確認とトラブルシューティングの詳細については、『[IP Security のトラブルシューティング - debug コマンドの理解と使用](#)』を参照してください。

## 関連情報

- [IPSec に関するサポート ページ](#)
- [IPSec ネットワーク セキュリティの設定](#)
- [Internet Key Exchange セキュリティ プロトコルの設定](#)
- [テクニカルサポート - Cisco Systems](#)