

# 在具有 VPN 服务模块的 Catalyst 6500 和 PIX 防火墙之间配置 IPSec LAN 到 LAN 隧道的配置示例

## 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](#)

[使用第 2 层接入或中继端口配置 IPSec](#)

[使用路由端口配置 IPSec](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

## 简介

本文档介绍如何在含有 IPSec VPN 服务模块 (W) 的 Cisco Catalyst 6500 系列交换机与 Cisco PIX 防火墙之间创建 IPSec LAN 到 LAN 隧道。

## 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：

- 适用于含 IPSec VPN 服务模块的 Catalyst 6000 系列 Supervisor 引擎的 Cisco IOS® 软件 12.2(14)SY2 版
- Cisco PIX 防火墙软件 6.3(3) 版

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。

## 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

Catalyst 6500 VPN 服务模块有两个千兆以太网 (GE) 端口，无外部可见的接头。这些端口只在配置时是可寻址的。端口 1 始终为内部端口。此端口处理从和到网络内部的所有业务量。第二个端口(端口2)处理所有业务量从和对广域网或外部网络。这两个端口在802.1q中继模式下总是配置。VPN服务模块对数据包流使用称线内冲突(BITW)的技术。

数据包由一对 VLAN 处理：一个第 3 层内部 VLAN 和一个第 2 层外部 VLAN。从内部传到外部的包，通过一种称为对内部VLAN的编码地址识别逻辑(EARL)的方法进行寻址。该方法将数据包加密之后，VPN 服务模块将使用相应的外部 VLAN。在解密过程中，使用外部 VLAN 将从外部到内部的数据包桥接到 VPN 服务模块。VPN 服务模块将数据包解密并将 VLAN 映射到相应的内部 VLAN 之后，EARL 将数据包路由到适当的 LAN 端口。第 3 层内部 VLAN 和第 2 层外部 VLAN 通过 **crypto connect vlan** 命令连接在一起。在Catalyst 6500系列交换机中有三种类型的端口：

- **路由端口** - 默认情况下，在 Cisco IOS 中所有以太网端口都是路由端口。这些端口有一个与它联系的隐藏VLAN。
- **接入端口** - 这些端口有一个外部 VLAN 或 VLAN 中继协议 (VTP) VLAN 与其关联。您能关联超过一个端口到默认的VLAN。
- **中继端口** - 这些端口承载许多外部 VLAN 或 VTP VLAN，上面所有数据包都以 802.1Q 报头进行封装。

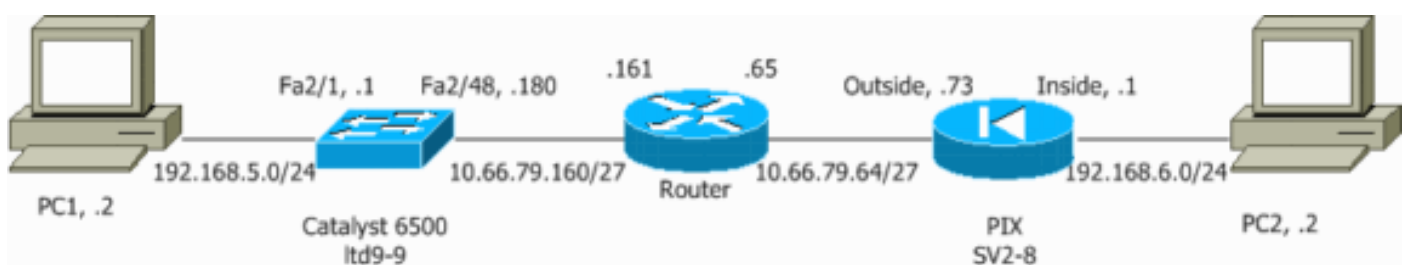
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：**有关本文档所用命令的详细信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

## 网络图

本文档使用以下网络设置：



## 使用第 2 层接入或中继端口配置 IPsec

执行以下这些步骤，在外部物理接口作为第 2 层接入或中继端口的情况下配置 IPsec。

1. 将内部 VLAN 添加到 VPN 服务模块的内部端口。假设 VPN 服务模块在插槽 4 上。使用 VLAN 100 作为内部 VLAN，VLAN 209 作为外部 VLAN。按如下所示配置 VPN 服务模块的 GE 端口：

```
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. 添加 VLAN 100 接口和隧道终止处的接口（本例中为 interface Vlan 209，如下所示）。  
interface Vlan100 ip address 10.66.79.180 255.255.255.224 interface Vlan209 no ip address  
crypto connect vlan 100

3. 配置外部物理端口作为接入或中继端口（本例中为 FastEthernet 2/48，如下所示）。  
*!--- 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. 创建旁路 NAT。将以下条目添加到 no nat 语句以免除在这些网络之间的 NAT：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. 创建您的加密配置以及定义将被加密的流量的访问控制列表 (ACL)。按如下所示，创建用于定义从内部网络 192.168.5.0/24 到远程网络 192.168.6.0/24 的流量的加密 ACL（本例中为 ACL 100 - 关注流量）：

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255 按如下所示定义您的  
Internet 安全连接和密钥管理协议 (ISAKMP) 策略方案：
```

```
crypto isakmp policy 1 hash md5 authentication pre-share group 2 发出下面这个命令（在本  
例中）以使用和定义预共享密钥：
```

```
crypto isakmp key cisco address 10.66.79.73 按如下所示定义您的 IPsec 方案：
```

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac 按如下所示创建您的加密映射语句：
```

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

6. 按如下所示将加密映射应用于 VLAN 100 接口：

```
interface vlan100 crypto map cisco
```

使用以下这些配置：

- [Catalyst 6500](#)
- [PIX 防火墙](#)

### 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 防火墙

```

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

```

## 使用路由端口配置 IPsec

执行以下这些步骤，在外部物理接口作为第 3 层路由端口的情况下配置 IPsec。

1. 将内部 VLAN 添加到 VPN 服务模块的内部端口。假设 VPN 服务模块在插槽 4 上。使用 VLAN 100 作为内部 VLAN，VLAN 209 作为外部 VLAN。按如下所示配置 VPN 服务模块的 GE 端口：

```

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. 添加 VLAN 100 接口和隧道终止处的接口 ( 本例中为 FastEthernet2/48 , 如下所示 ) 。

```
interface Vlan100 ip address 10.66.79.180 255.255.255.224 interface FastEthernet2/48 no ip
address crypto connect vlan 100
```

3. 创建旁路 NAT。将以下条目添加到 no nat 语句以免除在这些网络之间的 NAT : 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. 创建您的加密配置以及用于定义被加密的流量的 ACL。按如下所示, 创建用于定义从内部网络 192.168.5.0/24 到远程网络 192.168.6.0/24 的流量的 ACL ( 本例中为 ACL 100 ) :

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255 按如下所示定义您的
ISAKMP 策略方案 :
```

```
crypto isakmp policy 1 hash md5 authentication pre-share group 2 发出下面这个命令 ( 在本
例中 ) 以使用和定义预共享密钥 :
```

```
crypto isakmp key cisco address 10.66.79.73 按如下所示定义您的 IPsec 方案 :
```

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac 按如下所示创建您的加密映射语句 :
crypto map cisco 10 ipsec-isakmp set peer 10.66.79.73 set transform-set cisco match address
100
```

5. 按如下所示将加密映射应用于 VLAN 100 接口 :

```
interface vlan100 crypto map cisco
```

使用以下这些配置 :

- [Catalyst 6500](#)
- [PIX 防火墙](#)

## 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 防火墙

```

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
```

## 验证

本部分提供的信息有助于确认配置是否正常运行。

[命令输出解释程序 \( 仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto ipsec sa** — 显示当前 IPsec SA 所使用的设置。
- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。
- **show crypto vlan** - 显示与加密配置关联的 VLAN。
- **show crypto eli** - 显示 VPN 服务模块的统计信息。

有关验证和排除 IPsec 故障的其他信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

## 故障排除

此部分提供信息故障排除您的配置。

### 故障排除命令

**注意：** 在发出 **debug** 命令之前，请参阅 [有关 debug 命令的重要信息](#)。



- `debug crypto ipsec` - 显示第 2 阶段的 IPsec 协商。
- `debug crypto isakmp` - 显示第 1 阶段的 ISAKMP 协商。
- `debug crypto engine` - 显示已加密的数据流。
- `clear crypto isakmp` - 清除与第 1 阶段相关的 SA。
- [clear crypto sa](#) - 清除与第 2 阶段相关的 SA。

有关验证和排除 IPsec 故障的其他信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

## [相关信息](#)

- [IPSec 支持页面](#)
- [配置 IPSec 网络安全](#)
- [配置 Internet 密钥交换安全协议](#)
- [技术支持 - Cisco Systems](#)