

Túnel de LAN para LAN de IPSec entre um Catalyst 6500 com o módulo de serviço VPN e um exemplo de configuração do PIX Firewall

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração para o IPsec usando um acesso ou uma porta de tronco da camada 2](#)

[Configuração para o IPsec usando uma porta roteada](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos de solução de problemas](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como criar um túnel de LAN para LAN de IPSec entre um Cisco Catalyst 6500 Series Switch com o módulo de serviço do IPSec VPN (W) e um Cisco PIX Firewall.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Release 12.2(14)SY2 de Cisco IOS® para o Supervisor Engine do Catalyst 6000 Series, com o módulo de serviço do IPSec VPN
- Versão 6.3(3) do Software do firewall Cisco PIX

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

[Informações de Apoio](#)

O módulo de serviço do Catalyst 6500 VPN tem duas portas de gigabit Ethernet sem externamente conectores visíveis. Estas portas são endereçáveis para propósitos de configuração somente. A porta 1 é sempre a porta interna. Esta porta segura todo o tráfego e à rede interna. A segunda porta (porta 2) segura todo o tráfego e a WAN ou às redes externas. Estas duas portas são configuradas sempre no modo de entroncamento do 802.1Q. O módulo de serviço VPN usa uma técnica chamada o Bump In The Wire (BITW) para o fluxo de pacote de informação.

Os pacotes são processados por um par de VLAN, de uma camada 3 VLAN interno e de uma camada 2 VLAN exterior. Os pacotes, do interior à parte externa, são distribuídos com um método chamado lógica de reconhecimento de endereço codificado (EARL) ao VLAN interno. Depois que cifra os pacotes, o módulo de serviço VPN usa a correspondência fora do VLAN. No processo de descriptografia, os pacotes da parte externa ao interior são construídos uma ponte sobre ao módulo de serviço VPN usando o VLAN exterior. Depois que o módulo de serviço VPN decifra o pacote e traça o VLAN à correspondência dentro do VLAN, o EARL distribui o pacote à porta de LAN apropriada. A camada 3 VLAN interno e a camada 2 VLAN exteriores são juntadas junto com o comando **crypto connect vlan**. Há três tipos de portas nos Catalyst 6500 Series Switch:

- **Portas roteada** — À revelia, todas as portas Ethernet são portas roteada no Cisco IOS. Estas portas têm um vlan oculta associado com elas.
- **Portas de acesso** — Estas portas têm um externo ou um protocolo VLAN Trunk (VTP) VLAN associado com eles. Você pode associar mais de uma porta a um vlan definida.
- **Portas de tronco** — Estas portas levam muito externos ou o VTP VLAN, em que todos os pacotes são encapsulados com um encabeçamento do 802.1Q.

[Configurar](#)

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:

[Configuração para o IPsec usando um acesso ou uma porta de tronco da camada 2](#)

Execute estas etapas para configurar o IPsec com a ajuda de um acesso da camada 2 ou a porta de tronco para a interface física exterior.

1. Adicionar os VLAN internos à porta interna do módulo de serviço VPN. Supõe que o módulo de serviço VPN está no entalhe 4. Use o VLAN 100 como o VLAN interno e VLAN 209 como o VLAN exterior. Configurar as portas do módulo de serviço GE VPN como este:

```
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. Adicionar a relação do VLAN 100 e a relação onde o túnel é terminado (que, neste caso, é relação Vlan 209, como mostrado aqui).

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

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

3. Configurar a porta física exterior como um acesso ou uma porta de tronco (neste caso, FastEthernet 2/48, como mostrado aqui).

```
!--- 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. Crie o desvio NAT. Adicionar estas entradas a nenhuma indicação nat a fim isentar nating entre estas redes:

```
!--- 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
```

5. Crie sua configuração de criptografia e o Access Control List (ACL) que define o tráfego a

ser cifrado. Crie um ACL cripto (neste caso, ACL 100 - tráfego interessante) que define o tráfego da rede interna 192.168.5.0/24 à rede remota 192.168.6.0/24, como isto:

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

Defina suas propostas da política do Internet Security Association and Key Management Protocol (ISAKMP), como este:

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

Emita este comando (neste exemplo) usar e definir chaves pré-compartilhada:

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

Defina seus propósitos de IPsec, como isto:

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

Crie sua instrução de mapa de criptografia, como isto:

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

6. Aplique o crypto map à relação do VLAN 100, como este:

```
interface vlan100
crypto map cisco
```

Estas configurações são usadas:

- [Catalyst 6500](#)
- [Firewall de PIX](#)

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
```

Firewall de PIX

```
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

```

[Configuração para o IPsec usando uma porta roteada](#)

Execute estas etapas para configurar o IPsec com a ajuda de uma porta roteada da camada 3 para a interface física exterior.

1. Adicionar os VLAN internos à porta interna do módulo de serviço VPN. Supõe que o módulo de serviço VPN está no entalhe 4. Use o VLAN 100 como o VLAN interno e VLAN 209 como o VLAN exterior. Configurar as portas do módulo de serviço GE VPN como este:

```

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. Adicionar a relação do VLAN 100 e a relação onde o túnel é terminado (que, neste caso, é FastEthernet2/48, como mostrado aqui).

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

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

3. Crie o desvio NAT. Adicionar estas entradas a nenhuma indicação nat a fim isentar nating entre estas redes:

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

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

4. Crie sua configuração de criptografia e o ACL que define o tráfego a ser cifrado. Crie um ACL (neste caso, ACL 100) que define o tráfego da rede interna 192.168.5.0/24 à rede remota 192.168.6.0/24, como isto:

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

Defina suas propostas de política ISAKMP, como isto:

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

Emita este comando (neste exemplo) usar e definir chaves pré-compartilhada:

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

Defina seus propósitos de IPsec, como isto:

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

Crie sua instrução de mapa de criptografia, como isto:

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

5. Aplique o crypto map à relação do VLAN 100, como este:

```
interface vlan100
crypto map cisco
```

Estas configurações são usadas:

- [Catalyst 6500](#)

- [Firewall de PIX](#)

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
```

Firewall de PIX

```
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
```

Verificar

Esta seção fornece as informações para confirmar que sua configuração funciona adequadamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre IPsec cripto sa** — Mostra os ajustes usados pelo IPsec atual SA.
- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.
- **show crypto vlan** — Mostra o VLAN associado com a configuração de criptografia.
- **show crypto eli** — Mostra as estatísticas do módulo de serviço VPN.

Para obter informações adicionais sobre a verificação e pesquisar defeitos o IPsec, referem o [Troubleshooting de Segurança IP - compreendendo e usando comandos debug](#).

Troubleshooting

Esta seção fornece a informação para pesquisar defeitos sua configuração.

Comandos de solução de problemas

Nota: [Antes de emitir comandos de depuração, consulte Informações Importantes sobre Comandos de Depuração.](#)

- **IPsec do debug crypto** — Mostra as negociações de IPSEC de fase 2.
- **debug crypto ipsec** - Exibe as negociações ISAKMP da fase 1.
- **motor do debug crypto** — Mostra o tráfego que é cifrado.
- **cancela o isakmp crypto** — Cancela os SA relativos à fase 1.
- **cancela o sa crypto** — Cancela os SA relativos à fase 2.

Para obter informações adicionais sobre a verificação e pesquisar defeitos o IPsec, referem o [Troubleshooting de Segurança IP - compreendendo e usando comandos debug.](#)

[Informações Relacionadas](#)

- [Página de suporte do IPsec](#)
- [Configurando a segurança da rede IPsec](#)
- [Configurando o protocolo de segurança do intercâmbio chave de Internet](#)
- [Suporte Técnico - Cisco Systems](#)