

Túnel LAN a LAN IPsec entre um Catalyst 6500 com o módulo de serviço VPN e um exemplo de configuração do roteador Cisco IOS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

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

[Configuração de IPsec usando uma porta roteada](#)

[Verificar](#)

[Troubleshoot](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como criar um túnel IPsec LAN-to-LAN entre um switch Cisco Catalyst 6500 Series com o módulo de serviço de aceleração de VPN e um roteador Cisco IOS®.

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Software Cisco IOS versão 12.2(14)SY2 para o Supervisor Engine do Catalyst 6000, com o módulo de serviço VPN IPsec
- Roteador Cisco 3640 que executa o Software Cisco IOS versão 12.3(4)T

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações de Apoio

O módulo de serviço de VPN do Catalyst 6500 tem duas portas Gigabit Ethernet (GE) sem conectores visíveis externamente. Essas portas são endereçáveis apenas para fins de configuração. A porta 1 é sempre a porta interna. Esta porta lida com todo o tráfego de e para a rede interna. A segunda porta (porta 2) trata todo o tráfego de e para a WAN ou redes externas. Essas duas portas são sempre configuradas no modo de entroncamento 802.1Q. O módulo de serviço VPN usa uma técnica chamada Bump In The Wire (BITW) para fluxo de pacote.

Os pacotes são processados por um par de VLANs, uma camada 3 dentro da VLAN e uma camada 2 fora da VLAN. Os pacotes, de dentro para fora, são roteados por meio de um método chamado de Lógica de Reconhecimento de Endereço Codificado (EARL - Encoded Address Recognition Logic) para a VLAN interna. Depois de criptografar os pacotes, o módulo de serviço VPN usa a VLAN externa correspondente. No processo de descriptografia, os pacotes de fora para dentro são ligados ao módulo de serviço VPN usando a VLAN externa. Depois que o módulo de serviço VPN descriptografa o pacote e mapeia a VLAN para a VLAN interna correspondente, o EARL encaminha o pacote para a porta LAN apropriada. A Camada 3 dentro da VLAN e as VLANs externas da Camada 2 são unidas emitindo o comando **crypto connect vlan**. Há três tipos de portas nos switches da série Catalyst 6500:

- **Portas roteadas** — Por padrão, todas as portas Ethernet são portas roteadas. Essas portas têm uma VLAN oculta associada a elas.
- **Portas de acesso** —Essas portas têm uma VLAN externa ou VLAN Trunk Protocol (VTP) associada a elas. Você pode associar mais de uma porta a uma VLAN definida.
- **Portas de tronco**—Essas portas transportam muitas VLANs externas ou VTP, nas quais todos os pacotes são encapsulados com um cabeçalho 802.1Q.

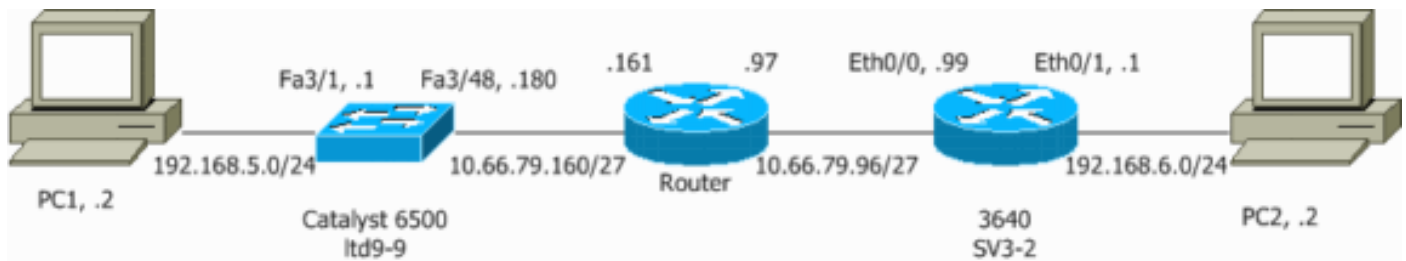
Configurar

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

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama:



Configuração para IPsec usando uma porta de tronco ou acesso de camada 2

Execute estas etapas para configurar o IPsec com a ajuda de uma porta de tronco ou de acesso de Camada 2 para a interface física externa.

1. Adicione as VLANs internas à porta interna do módulo de serviço VPN. Suponha que o módulo de serviço VPN esteja no slot 4. Use a VLAN 100 como a VLAN interna e a VLAN 209 como a VLAN externa. Configure as portas GE do módulo de serviço VPN como esta:

```
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. Adicione a interface VLAN 100 e a interface onde o túnel é terminado (que, neste caso, é a interface 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. Configure a porta física externa como uma porta de tronco ou de acesso (que, nesse caso, é FastEthernet 3/48, como mostrado aqui).

```
!--- This is the configuration that uses an access port. interface FastEthernet3/48
no ip address
switchport
switchport access vlan 209
switchport mode access
```

```
!--- This is the configuration that uses a trunk port. interface FastEthernet3/48
no ip address switchport
```

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

4. Crie o NAT de desvio. Adicione estas entradas à instrução no nat para isentar a nação entre estas redes:

```
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. Crie sua configuração de criptografia e a lista de controle de acesso (ACL) que define o tráfego a ser criptografado. Crie uma ACL (neste caso, ACL 100) que defina o tráfego da rede interna 192.168.5.0/24 para a rede remota 192.168.6.0/24, como esta:

```
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 de Internet Security Association and Key Management Protocol (ISAKMP), como esta:

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

Emita este comando (neste exemplo) para usar e definir chaves pré-compartilhadas.

```
crypto isakmp key cisco address 10.66.79.99
```

Defina suas propostas de IPsec, como esta:

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

Crie sua instrução de mapa de criptografia, como esta:

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.99
set transform-set cisco
match address 100
```

6. Aplique o mapa de criptografia à interface da VLAN 100, assim:

```
interface vlan100
crypto map cisco
```

Essas configurações são usadas.

- [Catalyst 6500](#)
- [Cisco IOS Router](#)

Catalyst 6500

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

```

group 2
crypto isakmp key cisco address 10.66.79.99
!
!
!--- 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 10.66.79.99
  set transform-set cisco
  match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet3/1
  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 FastEthernet3/48 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 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
!--- 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
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 !--- 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
```

Cisco IOS Router

```
SV3-2#show run
Building configuration...

Current configuration : 1268 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.180
!
```

```

!
!--- 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 10.66.79.180
  set transform-set cisco
  match address 100
!
!
!--- Apply the crypto map to the interface. interface
Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-
duplex crypto map cisco
!
interface Ethernet0/1
  ip address 192.168.6.1 255.255.255.0
  half-duplex
  no keepalive
!
!
ip http server
no ip http secure-server
ip classless
!--- Configure the routing so that the device !--- is
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.97
!
!
!--- This is the crypto ACL. access-list 100 permit ip
192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end

```

Configuração de IPsec usando uma porta roteada

Execute estas etapas para configurar o IPsec com a ajuda de uma porta roteada de Camada 3 para a interface física externa.

1. Adicione as VLANs internas à porta interna do módulo de serviço VPN. Suponha que o módulo de serviço VPN esteja no slot 4. Use a VLAN 100 como a VLAN interna e a VLAN 209 como a VLAN externa. Configure as portas GE do módulo de serviço VPN como esta:

```

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. Adicione a interface VLAN 100 e a interface onde o túnel é terminado (que, neste caso, é FastEthernet3/48, como mostrado aqui).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224

interface FastEthernet3/48
no ip address
crypto connect vlan 100
```

3. Crie o NAT de desvio. Adicione estas entradas à instrução no nat para isentar a nação entre estas redes:

```
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. Crie sua configuração de criptografia e a ACL que define o tráfego a ser criptografado. Crie uma ACL (neste caso, ACL 100) que defina o tráfego da rede interna 192.168.5.0/24 para a rede remota 192.168.6.0/24, como esta:

```
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 esta:

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

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

```
crypto isakmp key cisco address 10.66.79.99
```

Defina suas propostas de IPsec, como esta:

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

Crie sua instrução de mapa de criptografia, como esta:

```
crypto map cisco 10 ipsec-isakmp
set peer 10.66.79.99
set transform-set cisco
match address 100
```


5. Aplique o mapa de criptografia à interface da VLAN 100, assim:

```
interface vlan100
crypto map cisco
```

Essas configurações são usadas.

- [Catalyst 6500](#)
- [Cisco IOS Router](#)

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
hash md5
authentication pre-share
group 2
crypto isakmp key cisco address 10.66.79.99
!
!
!--- 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 10.66.79.99
set transform-set cisco
match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet3/1
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 FastEthernet3/48 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
  !
  ip classless
  !--- 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
  !
  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 !--- 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

```

Cisco IOS Router

```

SV3-2# show run
Building configuration...

Current configuration : 1268 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

```

```
!  
hostname SV3-2  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
ip subnet-zero  
!  
ip audit notify log  
ip audit po max-events 100  
ip ssh break-string  
no ftp-server write-enable  
!  
!--- Define the Phase 1 policy. crypto isakmp policy 1  
hash md5  
authentication pre-share  
group 2  
crypto isakmp key cisco address 10.66.79.180  
!  
!  
!--- 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 10.66.79.180  
set transform-set cisco  
match address 100  
!  
!  
!--- Apply the crypto map to the interface. interface  
Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-  
duplex crypto map cisco  
!  
interface Ethernet0/1  
ip address 192.168.6.1 255.255.255.0  
half-duplex  
no keepalive  
!  
!  
ip http server  
no ip http secure-server  
ip classless  
!--- Configure the routing so that the device !--- is  
directed to reach its destination network. ip route  
0.0.0.0 0.0.0.0 10.66.79.97  
!  
!  
!--- This is the crypto ACL. access-list 100 permit ip  
192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255  
!  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!
```

Verificar

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

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

- **show crypto ipsec sa** — Mostra as configurações usadas pelas SAs IPsec atuais.
- **show crypto isakmp sa** — Mostra todas as SAs IKE atuais em um peer.
- **show crypto vlan** — Mostra a VLAN associada à configuração de criptografia.
- **show crypto eli** — Mostra as estatísticas do módulo de serviço VPN.

Para obter informações adicionais sobre como verificar e solucionar problemas de IPsec, consulte [IP Security Troubleshooting - Understanding and Using debug Commands](#).

Troubleshoot

Esta seção fornece as informações para solucionar problemas de configuração.

Comandos para Troubleshooting

Observação: antes de emitir comandos **debug**, consulte [Informações Importantes sobre Comandos Debug](#).

- **debug crypto ipsec** —Mostra as negociações de IPsec da Fase 2.
- **debug crypto ipsec - Exibe as negociações ISAKMP da fase 1.**
- **debug crypto engine** —Mostra o tráfego que está criptografado.
- **clear crypto isakmp** — Limpa as SAs relacionadas à Fase 1.
- **clear crypto sa** —Limpa as SAs relacionadas à Fase 2.

Para obter informações adicionais sobre como verificar e solucionar problemas de IPsec, consulte [IP Security Troubleshooting - Understanding and Using debug Commands](#).

Informações Relacionadas

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