# Túnel ipsec de LAN a LAN entre un Catalyst 6500 con el módulo de servicio VPN y un ejemplo de la configuración del router del Cisco IOS

## Contenido



# Introducción

Este documento describe cómo crear un túnel ipsec de LAN a LAN entre un Cisco Catalyst 6500 Series Switch con el módulo de servicio de la aceleración de VPN y un router de Cisco IOS®.

# prerrequisitos

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco IOS Software Release 12.2(14)SY2 para el Catalyst 6000 Supervisor Engine, con el módulo de servicio del IPSec VPN

- Cisco 3640 Router que funciona con el Cisco IOS Software Release 12.3(4)T

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

### Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

## Antecedentes

El módulo de servicio del Catalyst 6500 VPN tiene dos puertos del Gigabit Ethernet (GE) sin externamente los conectores visibles. Estos puertos son direccionables para los fines de la configuración solamente. El puerto 1 es siempre el puerto del interior. Este puerto maneja todo el tráfico y a la red interna. El segundo puerto (el puerto 2) maneja todo el tráfico y a WAN o a las redes externas. Estos dos puertos se configuran siempre en el modo de concentración links del 802.1Q. El módulo de servicio VPN utiliza una técnica llamada el Bump In The Wire (BITW) para el flujo de paquetes.

Los paquetes son procesados por un par de VLA N, de un VLA N interior de la capa 3 y de un VLA N exterior de la capa 2. Los paquetes, del interior al exterior, se rutean con un método llamado Lógica de reconocimiento de dirección codificada (EARL) al VLA N interior. Después de que cifre los paquetes, el módulo de servicio VPN utiliza la correspondencia fuera del VLA N. En el proceso de descifrado, los paquetes del exterior al interior se interligan al módulo de servicio VPN usando el VLA N exterior. Después de que el módulo de servicio VPN desencripte el paquete y asocie el VLA N a la correspondencia dentro del VLA N, el CONDE rutea el paquete al puerto LAN apropiado. El VLA N interior de la capa 3 y los VLA N exteriores de la capa 2 son unidos a juntos publicando el **comando crypto connect vlan**. Hay tres tipos de puertos en los Catalyst 6500 Series Switch:

- **Puertos ruteados** — Por abandono, todos los accesos de Ethernet son puertos ruteados. Estos puertos tienen un VLAN oculta asociado a ellos.
- **Puertos de acceso** — Estos puertos tienen un externo o un VLA N del VLAN Trunk Protocol (VTP) asociado a ellos. Usted puede asociar más de un puerto a un VLAN definido.
- **Puertos troncales** — Estos puertos llevan mucho el externo o los VLA N VTP, en los cuales todos los paquetes se encapsulan con una encabezado del 802.1Q.

## Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

**Nota:** Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

### Diagrama de la red

Este documento utiliza la configuración de red que se muestra en este diagrama:

## Configuración para el IPSec usando un acceso o un puerto troncal de la capa 2

Realice estos pasos para configurar el IPSec con la ayuda de un acceso de la capa 2 o el puerto troncal para la interfaz física exterior.

1. Agregue los VLA N interiores al puerto del interior del módulo de servicio VPN.Asuma que el módulo de servicio VPN está en el slot 4. Utilice el VLAN 100 como el VLA N interior y el VLA N 209 como el VLA N exterior. Configure los puertos de GE del módulo de servicio VPN como esto:

```
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. Agregue la interfaz del VLAN 100 y la interfaz donde el túnel se termina (que, en este caso, es `interfaz Vlan 209`, como se muestra aquí).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

3. Configure el puerto físico exterior como un acceso o puerto troncal (que, en este caso, sean el `FastEthernet 3/48`, como se muestra aquí).

```
!--- 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. Cree puente NAT. Agregue estas entradas a la ninguna sentencia NAT para eximir nating entre estas redes:

```
!--- 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
```

5. Cree su configuración de criptografía y el Access Control List (ACL) que defina el tráfico que se cifrará.Cree un ACL (en este caso, ACL 100) que define el tráfico de la red interna 192.168.5.0/24 a la red remota 192.168.6.0/24, como esto:
   ```
   access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
   ```
   Defina sus propuestas de política del Internet Security Association and Key Management Protocol (ISAKMP), como esto:
   ```
   crypto isakmp policy 1
   hash md5
   authentication pre-share
   group 2
   ```
   Publique este comando (en este ejemplo) de utilizar y de definir las claves previamente compartidas.
   ```
   crypto isakmp key cisco address 10.66.79.99
   ```
   Defina sus ofertas del IPSec, como esto:
   ```
   crypto ipsec transform-set cisco esp-des esp-md5-hmac
   ```
   Cree su sentencia de correspondencia de criptografía, como esto:
   ```
   crypto map cisco 10 ipsec-isakmp
   set peer 10.66.79.99
   set transform-set cisco
   match address 100
   ```
6. Aplique la correspondencia de criptografía a la interfaz del VLAN 100, como esto:
   ```
   interface vlan100
   crypto map cisco
   ```

Se utilizan estas configuraciones.

- Catalyst 6500
- Router del Cisco IOS

**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
```

## Router del Cisco IOS

```
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
```

## Configuración para el IPSec usando un puerto ruteado

Realice estos pasos para configurar el IPSec con la ayuda de un puerto ruteado de la capa 3 para la interfaz física exterior.

1. Agregue los VLA N interiores al puerto del interior del módulo de servicio VPN.Asuma que el módulo de servicio VPN está en el slot 4. Utilice el VLAN 100 como el VLA N interior y el VLA N 209 como el VLA N exterior. Configure los puertos de GE del módulo de servicio VPN como esto:

```
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. Agregue la interfaz del VLAN 100 y la interfaz donde el túnel se termina (que, en este caso, es `FastEthernet3/48`, como se muestra aquí).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

3. Cree puente NAT. Agregue estas entradas a la ninguna sentencia NAT para eximir nating entre estas redes:

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

4. Cree su configuración de criptografía y el ACL que define el tráfico que se cifrará.Cree un ACL (en este caso, ACL 100) que define el tráfico de la red interna 192.168.5.0/24 a la red remota 192.168.6.0/24, como esto:

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

Defina sus propuestas de política ISAKMP, como esto:

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

Publique este comando (en este ejemplo) de utilizar y de definir las claves previamente compartidas:

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

Defina sus ofertas del IPSec, como esto:

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

Cree su sentencia de correspondencia de criptografía, como esto:

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

5. Aplique la correspondencia de criptografía a la interfaz del VLAN 100, como esto:

```
interface vlan100
crypto map cisco
```

Se utilizan estas configuraciones.

- Catalyst 6500
- Router del Cisco IOS

**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
```

## Router del Cisco IOS

```
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
```

# Verificación

En esta sección encontrará información que le permitirá confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre IPSec crypto sa** — Muestra las configuraciones usadas por el SA de IPSec actual.
- **muestre isakmp crypto sa** — Muestra todo el IKE actual SA en un par.
- **show crypto vlan** — Muestra el VLA N asociado a la configuración de criptografía.
- **show crypto eli** — Muestra las estadísticas del módulo de servicio VPN.

Para más información sobre verificar y resolver problemas el IPSec, refiera al Troubleshooting de IP Security - entendiendo y con los comandos debug.

# Troubleshooting

Esta sección proporciona la información para resolver problemas su configuración.

## Comandos para resolución de problemas

**Nota:** Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

- **IPSec del debug crypto** — Muestra los IPSec Negotiations de la fase 2.
- debug crypto isakmp — muestra las negociaciones ISAKMP para la fase 1.
- debug crypto engine — muestra el tráfico codificado.

- **borre el isakmp crypto** — Borra los SA relacionados con la fase 1.
- **borre el sa crypto** — Borra los SA relacionados con la fase 2.

Para más información sobre verificar y resolver problemas el IPSec, refiera al Troubleshooting de IP Security - entendiendo y con los comandos debug.

## Información Relacionada

- Página de soporte de IPSec
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico - Cisco Systems