

# Exemple de configuration de tunnel IPSec LAN à LAN entre un Catalyst 6500 avec le module de service VPN et un routeur Cisco IOS

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configuration pour IPsec à l'aide d'un port d'accès ou de liaison de couche 2](#)

[Configuration pour IPsec à l'aide d'un port routé](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment créer un tunnel LAN à LAN IPsec entre un commutateur de la gamme Cisco Catalyst 6500 avec le module de service VPN Acceleration et un routeur Cisco IOS®.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS Version 12.2(14)SY2 pour le Supervisor Engine Catalyst 6000, avec le module de service VPN IPsec

- Routeur Cisco 3640 qui exécute le logiciel Cisco IOS Version 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

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

## Informations générales

Le module de service VPN Catalyst 6500 est équipé de deux ports Gigabit Ethernet (GE) sans connecteurs externes visibles. Ces ports sont adressables uniquement à des fins de configuration. Le port 1 est toujours le port interne. Ce port gère tout le trafic en provenance et à destination du réseau interne. Le second port (port 2) gère tout le trafic en provenance et à destination du WAN ou des réseaux externes. Ces deux ports sont toujours configurés en mode d'agrégation 802.1Q. Le module de service VPN utilise une technique appelée Bump In The Wire (BITW) pour le flux de paquets.

Les paquets sont traités par une paire de VLAN, une couche 3 à l'intérieur du VLAN et une couche 2 à l'extérieur du VLAN. Les paquets, de l'intérieur vers l'extérieur, sont acheminés via une méthode appelée Encoded Address Recognition Logic (EARL) vers le VLAN interne. Après avoir chiffré les paquets, le module de service VPN utilise le VLAN externe correspondant. Dans le processus de déchiffrement, les paquets de l'extérieur vers l'intérieur sont pontés au module de service VPN à l'aide du VLAN externe. Une fois que le module de service VPN déchiffre le paquet et mappe le VLAN au VLAN interne correspondant, EARL achemine le paquet vers le port LAN approprié. Les VLAN internes de couche 3 et les VLAN externes de couche 2 sont regroupés par l'émission de la commande **crypto connect vlan**. Il existe trois types de ports dans les commutateurs de la gamme Catalyst 6500 :

- **Routed ports** - Par défaut, tous les ports Ethernet sont des ports routés. Ces ports sont associés à un VLAN masqué.
- **Ports d'accès** - Ces ports sont associés à un VLAN externe ou VTP (VLAN Trunk Protocol). Vous pouvez associer plusieurs ports à un VLAN défini.
- **Ports agrégés** - Ces ports transportent de nombreux VLAN externes ou VTP, sur lesquels tous les paquets sont encapsulés avec un en-tête 802.1Q.

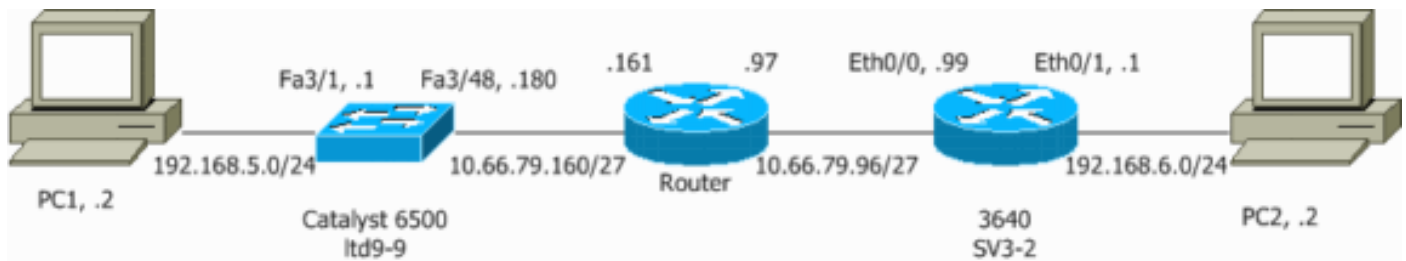
## Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

**Remarque** : Utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement) pour en savoir plus sur les commandes figurant dans le présent document.

## Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



## Configuration pour IPsec à l'aide d'un port d'accès ou de liaison de couche 2

Procédez comme suit pour configurer IPsec à l'aide d'un port d'accès ou de liaison de couche 2 pour l'interface physique externe.

1. Ajoutez les VLAN internes au port interne du module de service VPN. Supposez que le module de service VPN se trouve sur le logement 4. Utilisez VLAN 100 comme VLAN interne et VLAN 209 comme VLAN externe. Configurez les ports GE du module de service VPN comme suit :

```
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. Ajoutez l'interface VLAN 100 et l'interface où le tunnel est terminé (qui, dans ce cas, est l'interface Vlan 209, comme indiqué ici).

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

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

3. Configurez le port physique externe en tant que port d'accès ou de liaison (qui, dans ce cas, est FastEthernet 3/48, comme indiqué ici).

```
!--- 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. Créez la NAT de contournement. Ajoutez ces entrées à l'instruction `no nat` afin d'exempter la liaison entre ces réseaux :

```
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. Créez votre configuration de chiffrement et la liste de contrôle d'accès (ACL) qui définit le trafic à chiffrer. Créez une liste de contrôle d'accès (dans ce cas, la liste de contrôle d'accès 100) qui définit le trafic du réseau interne 192.168.5.0/24 vers le réseau distant 192.168.6.0/24, comme suit :

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

Définissez vos propositions de politique ISAKMP (Internet Security Association and Key Management Protocol), comme suit :

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

Émettez cette commande (dans cet exemple) pour utiliser et définir des clés pré-partagées.

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

Définissez vos propositions IPsec, comme ceci :

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

Créez votre instruction crypto map, comme ceci :

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

6. Appliquez la crypto-carte à l'interface VLAN 100, comme ceci :

```
interface vlan100
crypto map cisco
```

Ces configurations sont utilisées.

- [Catalyst 6500](#)
- [Routeur 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

```

## Routeur 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

```

## Configuration pour IPsec à l'aide d'un port routé

Procédez comme suit pour configurer IPsec à l'aide d'un port routé de couche 3 pour l'interface physique externe.

1. Ajoutez les VLAN internes au port interne du module de service VPN. Supposez que le module de service VPN se trouve sur le logement 4. Utilisez VLAN 100 comme VLAN interne et VLAN 209 comme VLAN externe. Configurez les ports GE du module de service VPN comme suit :

```

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. Ajoutez l'interface VLAN 100 et l'interface où le tunnel est terminé (qui, dans ce cas, est FastEthernet3/48, comme indiqué ici).

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

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

3. Créez la NAT de contournement. Ajoutez ces entrées à l'instruction no nat afin d'exempter la liaison entre ces réseaux :

```
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. Créez votre configuration de chiffrement et la liste de contrôle d'accès qui définit le trafic à chiffrer. Créez une liste de contrôle d'accès (dans ce cas, la liste de contrôle d'accès 100) qui définit le trafic du réseau interne 192.168.5.0/24 vers le réseau distant 192.168.6.0/24, comme suit :

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

Définissez vos propositions de politique ISAKMP, comme ceci :

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

Émettez cette commande (dans cet exemple) pour utiliser et définir des clés pré-partagées :

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

Définissez vos propositions IPsec, comme ceci :

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

Créez votre instruction crypto map, comme ceci :



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

5. Appliquez la crypto-carte à l'interface VLAN 100, comme ceci :

```
interface vlan100
  crypto map cisco
```

Ces configurations sont utilisées.

- [Catalyst 6500](#)
- [Routeur 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

```

## Routeur 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
```

## Vérification

Cette section fournit les informations pour confirmer que votre configuration fonctionne correctement.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines [commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- **show crypto ipsec sa** - Affiche les paramètres utilisés par les SA IPsec actuelles.
- **show crypto isakmp sa** - Affiche toutes les SA IKE actuelles sur un homologue.
- **show crypto vlan** - Affiche le VLAN associé à la configuration de chiffrement.
- **show crypto eli** - Affiche les statistiques du module de service VPN.

Pour plus d'informations sur la vérification et le dépannage d'IPsec, référez-vous à [Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage](#).

## Dépannage

Cette section fournit les informations nécessaires au dépannage de votre configuration.

### Dépannage des commandes

**Remarque** : Avant d'émettre des commandes **debug**, reportez-vous à [Informations importantes sur les commandes de débogage](#).

- **debug crypto ipsec** : Cette commande affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** - Affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Montre le trafic crypté.
- **clear crypto isakmp** : efface les SA liées à la phase 1.
- **clear crypto sa** : efface les SA liées à la phase 2.

Pour plus d'informations sur la vérification et le dépannage d'IPsec, référez-vous à [Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage](#).

## Informations connexes

- [Page d'assistance IPsec](#)
- [Configuration de la sécurité des réseaux IPsec](#)
- [Configuration du protocole IKE \(Internet Key Exchange\)](#)
- [Support technique - Cisco Systems](#)