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

Ce document décrit comment créer un tunnel entre réseaux locaux d'IPsec entre une gamme Cisco Catalyst 6500 commutent avec le module de service d'accélération VPN et un routeur de Cisco IOS®.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version du logiciel Cisco IOS 12.2(14)SY2 pour l'engine de superviseur du Catalyst 6000, avec le module de service d'IPsec VPN

- Routeur de Cisco 3640 qui exécute le Logiciel Cisco IOS version 12.3(4)T

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Informations générales

Le module de service du Catalyst 6500 VPN a deux ports de Gigabit Ethernet (GE) sans les connecteurs extérieurement visibles. Ces ports sont adressables pour des raisons de configuration seulement. Le port 1 est toujours le port d'intérieur. Ce port traite tout le trafic et derrière le réseau intérieur. Le deuxième port (le port 2) traite tout le trafic et derrière les réseaux de WAN ou d'extérieur. Ces deux ports sont toujours configurés en mode de jonction de 802.1Q. Le module de service VPN utilise une technique appelée le bosse sur le fil (BITW) pour l'écoulement de paquet.

Des paquets sont traités par une paire des VLAN, d'une une couche 3 VLAN intérieur et d'une une couche 2 VLAN extérieur. Les paquets, de l'intérieur à l'extérieur, sont conduits par une méthode appelée la logique de reconnaissance d'adresses encodées (EARL) au VLAN intérieur. Après qu'il chiffre les paquets, le module de service VPN utilise la correspondance en dehors du VLAN. Dans le procédé de déchiffrement, les paquets de l'extérieur à l'intérieur pont au module de service VPN utilisant le VLAN extérieur. Après que le module de service VPN déchiffre le paquet et trace le VLAN à la correspondance à l'intérieur du VLAN, l'EARL conduit le paquet au port LAN approprié. La couche 3 VLAN intérieur et la couche 2 VLAN extérieurs sont jointes ensemble en émettant la commande de **crypto connect vlan**. Il y a trois types de ports dans les Commutateurs de gamme Catalyst 6500 :

- **Ports conduits** — Par défaut, tous les ports Ethernet sont les ports conduits. Ces ports ont un VLAN masqué associé avec eux.
- **Ports d'accès** — Ces ports ont un externe ou le protocole VTP (VLAN Trunk Protocol) VLAN associé avec eux. Vous pouvez associer plus d'un port à un VLAN défini.
- **Ports de joncteur réseau** — Ces ports portent beaucoup d'externe ou VTP VLAN, sur lesquels tous les paquets sont encapsulés avec une en-tête de 802.1Q.

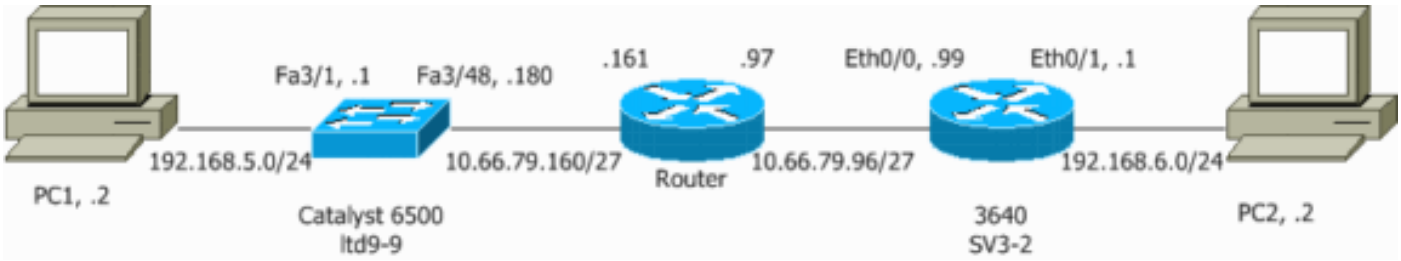
Configurer

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

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

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



Configuration pour IPsec utilisant une couche 2 Access ou port de joncteur réseau

Exécutez ces étapes pour configurer IPsec avec l'aide des 2 ports d'accès ou de joncteur réseau de la couche pour l'interface physique extérieure.

1. Ajoutez les VLAN intérieurs au port d'intérieur du module de service VPN.Supposez que le module de service VPN est sur l'emplacement 4. Utilisez VLAN 100 comme VLAN intérieur et VLAN 209 comme VLAN extérieur. Configurez les ports de GE de module de service VPN comme ceci :

```
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 le VLAN 100 relient et l'interface où le tunnel est terminé (qui, dans ce cas, est l'`interface vlan 209`, comme affiché 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 extérieur comme port d'accès ou de joncteur réseau (qui, dans ce cas, est `FastEthernet 3/48`, comme affiché 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 le contournement NAT. Ajoutez ces entrées à l'aucune déclaration nat afin d'exempter nating entre ces réseaux :

```
!--- 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. Créez votre crypto configuration et la liste de contrôle d'accès (ACL) qui définit le trafic à chiffrer.Créez un ACL (dans ce cas, ACL 100) qui définit le trafic du réseau intérieur 192.168.5.0/24 au réseau distant 192.168.6.0/24, comme ceci :

```
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 stratégie de Protocole ISAKMP (Internet Security Association and Key Management Protocol), comme ceci :

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

Fournissez cette commande (dans cet exemple) à utiliser-et définissent des clés pré-partagées.

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

Définissez vos propositions d'IPsec, comme ceci :

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

Créez votre déclaration de 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 le crypto map au VLAN 100 relient, 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 utilisant un port conduit

Exécutez ces étapes pour configurer IPsec avec l'aide d'un port conduit de la couche 3 pour l'interface physique extérieure.

1. Ajoutez les VLAN intérieurs au port d'intérieur du module de service VPN.Supposez que le module de service VPN est sur l'emplacement 4. Utilisez VLAN 100 comme VLAN intérieur et VLAN 209 comme VLAN extérieur. Configurez les ports de GE de module de service VPN comme ceci :

```
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 le VLAN 100 relient et l'interface où le tunnel est terminé (qui, dans ce cas, est `FastEthernet3/48`, comme affiché 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 le contournement NAT. Ajoutez ces entrées à l'aucune déclaration nat afin d'exempter nating entre ces réseaux :

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

4. Créez votre crypto configuration et l'ACL qui définit le trafic à chiffrer.Créez un ACL (dans ce cas, ACL 100) qui définit le trafic du réseau intérieur 192.168.5.0/24 au réseau distant 192.168.6.0/24, comme ceci :

```
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 stratégie ISAKMP, comme ceci :

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

Fournissez cette commande (dans cet exemple) à utiliser-et définissent des clés pré-partagées :

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

Définissez vos propositions d'IPsec, comme ceci :

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

Créez votre déclaration de 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 le crypto map au VLAN 100 relient, 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
```

Vérifier

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 configurations utilisées par l'IPsec en cours SAS.
- **show crypto isakmp sa** — Affiche tout l'IKE en cours SAS à un pair.
- **show crypto vlan** — Affiche le VLAN associé avec la crypto configuration.
- **show crypto eli** — Affiche les statistiques de module de service VPN.

Pour des informations supplémentaires sur vérifier et dépanner IPsec, référez-vous au dépannage de sécurité IP - en comprenant et en utilisant des commandes de débogage.

Dépanner

Cette section fournit les informations pour dépanner votre configuration.

Dépannage des commandes

Remarque: Avant d'émettre des commandes **debug**, reportez-vous aux Informations importantes sur les commandes de débogage.

- **debug crypto ipsec** — Affiche les négociations IPSecs du Phase 2.
- **debug crypto isakmp** — Affiche les négociations ISAKMP du Phase 1.
- **debug crypto engine** - Montre le trafic crypté.
- **clear crypto isakmp** — Efface SAS liée au Phase 1.
- **clear crypto sa** — Efface SAS liée au Phase 2.

Pour des informations supplémentaires sur vérifier et dépanner IPsec, référez-vous au dépannage de sécurité IP - en comprenant et en utilisant des commandes de débogage.

Informations connexes

- Page d'assistance IPsec
- Sécurité des réseaux de configuration d'IPSec
- Configurer le protocole de sécurité IKE
- Support technique - Cisco Systems