採用VPN服務模組的Catalyst 6500和Cisco IOS路由器之間的IPsec LAN到LAN通道組態範例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[背景資訊](#)
[設定](#)
[網路圖表](#)
[使用第2層接入或中繼埠配置IPsec](#)
[使用路由埠配置IPsec](#)
[驗證](#)
[疑難排解](#)
[疑難排解指令](#)
[相關資訊](#)

簡介

本文描述如何在具有VPN加速服務模組的Cisco Catalyst 6500系列交換機和Cisco IOS®路由器之間建立IPsec LAN到LAN隧道。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 適用於Catalyst 6000 Supervisor Engine的Cisco IOS軟體版本12.2(14)SY2，含IPsec VPN服務模組
- 執行Cisco IOS軟體版本12.3(4)T的Cisco 3640路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

Catalyst 6500 VPN服務模組具有兩個千兆乙太網(GE)埠，沒有外部可見聯結器。這些埠可定址僅用於配置。連線埠1一律是內部連線埠。此埠處理來自和流向內部網路的所有流量。第二個埠（埠2）處理來自WAN或外部網路的所有流量。這兩個埠始終在802.1Q中繼模式下配置。VPN服務模組使用一種稱為線路中凸點(BITW)的技術來傳輸封包。

資料包由一對VLAN處理，一個VLAN內部的第3層和一個外部VLAN的第2層。封包從內部到外部，透過稱為編碼位址識別邏輯(EARL)的方法路由到內部VLAN。在對資料包進行加密後，VPN服務模組將使用相應的外部VLAN。在解密過程中，使用外部VLAN將來自外部的封包橋接到VPN服務模組。VPN服務模組解密封包並將該VLAN對應到內部VLAN後，EARL會將封包路由到適當的LAN連線埠。發出**crypto connect vlan**命令，將第3層內部VLAN和第2層外部VLAN連線在一起。Catalyst 6500系列交換器中有三種型別的連線埠：

- **路由埠** — 預設情況下，所有乙太網埠都是路由埠。這些連線埠具有與其相關聯的隱藏VLAN。
- **存取連**接埠 — 這些連線埠具有與其相關的外部或VLAN中繼線通訊協定(VTP)VLAN。您可以將多個埠與定義的VLAN關聯。
- **中繼埠** — 這些埠承載許多外部或VTP VLAN，所有資料包都以802.1Q報頭封裝在這些埠上。

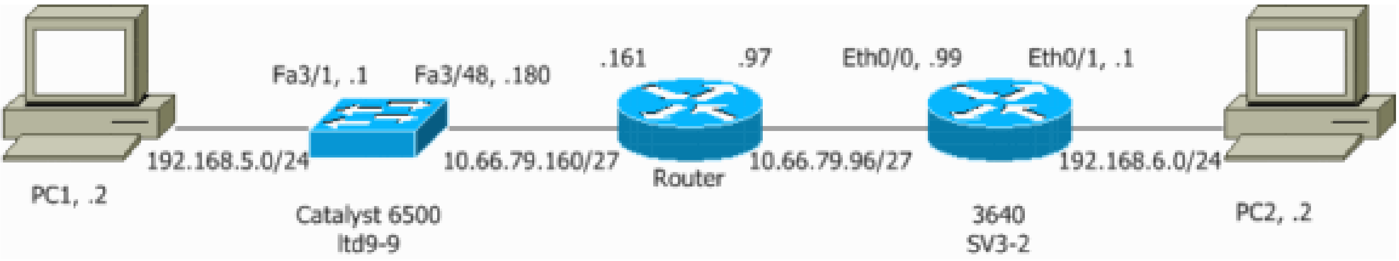
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用下圖所示的網路設定：



使用第2層接入或中繼埠配置IPsec

執行以下步驟，藉助外部物理介面的第2層接入或中繼埠配置IPsec。

1. 將內部VLAN新增到VPN服務模組的內部埠。假設VPN服務模組位於插槽4中。使用VLAN 100作為內部VLAN，使用VLAN 209作為外部VLAN。按如下方式配置VPN服務模組GE埠：

```
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. 新增VLAN 100介面和隧道終止的介面(在本例中為`Vlan 209`，如下所示)。

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

3. 將外部實體連線埠設定為存取或主干連線埠(在此案例中為`FastEthernet 3/48`，如此處所示)。

```
!--- 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. 建立旁路NAT。將這些條目新增到no nat語句中，以免除在這些網路之間的命名：

```
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. 建立密碼編譯組態以及定義要加密的流量的存取控制清單(ACL)。建立一個ACL（在本例中為ACL 100），定義從內部網路192.168.5.0/24到遠端網路192.168.6.0/24的流量，如下所示：

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

定義您的Internet安全關聯和金鑰管理協定(ISAKMP)策略提案，如下所示：

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

發出此命令（在本例中）以使用和定義預共用金鑰。

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

定義您的IPsec方案，如下所示：

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

建立加密對映語句，如下所示：

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

6. 將密碼編譯對應套用到VLAN 100介面，如下所示：

```
interface vlan100
crypto map cisco
```

使用的是這些配置。

- Catalyst 6500
- Cisco IOS路由器

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路由器

```
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
```

使用路由埠配置IPsec

執行以下步驟，藉助外部物理介面的第3層路由埠配置IPsec。

1. 將內部VLAN新增到VPN服務模組的內部埠。假設VPN服務模組位於插槽4中。使用VLAN 100作為內部VLAN，使用VLAN 209作為外部VLAN。按如下方式配置VPN服務模組GE埠：

```
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. 新增VLAN 100介面和隧道終止的介面(在本例中為`FastEthernet3/48`，如下所示)。

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

3. 建立旁路NAT。將這些條目新增到no nat語句中，以免除在這些網路之間的命名：

```
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. 建立密碼編譯組態和定義要加密的流量的ACL。建立一個ACL（在本例中為ACL 100），定義從內部網路192.168.5.0/24到遠端網路192.168.6.0/24的流量，如下所示：

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

定義您的ISAKMP策略建議，如下所示：

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

發出以下命令（在本例中）以使用和定義預共用金鑰：

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

定義您的IPsec方案，如下所示：

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

建立加密對映語句，如下所示：

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

5. 將密碼編譯對應套用到VLAN 100介面，如下所示：

```
interface vlan100
crypto map cisco
```

使用的是這些配置。

- Catalyst 6500
- Cisco IOS路由器

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路由器

```

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
```

驗證

本節提供的資訊用於確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show crypto ipsec sa** — 顯示當前IPsec SA使用的設定。
- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE SA。
- **show crypto vlan** — 顯示與加密配置關聯的VLAN。
- **show crypto eli** — 顯示VPN服務模組統計資訊。

有關驗證和排除IPsec故障的其他資訊，請參閱IP安全故障排除 — 瞭解和使用debug命令。

疑難排解

本節提供的資訊用於對組態進行疑難排解。

疑難排解指令

注意：發出**debug**指令之前，**請參閱**有關Debug指令的重要資訊**。**

- **debug crypto ipsec** — 顯示第2階段的IPsec協商。
- **debug crypto isakmp** — 顯示第1階段的ISAKMP協商。
- **debug crypto engine** — 顯示加密的流量。
- **clear crypto isakmp** — 清除與第1階段相關的SA。
- **clear crypto sa** — 清除與第2階段相關的SA。

有關驗證和排除IPsec故障的其他資訊，請參閱IP安全故障排除 — 瞭解和使用debug命令。

相關資訊

- IPSec支援頁面
- 配置IPSec網路安全
- 配置Internet金鑰交換安全協定
- 技術支援 - Cisco Systems