

# 在一台使用VPN服务模块的Catalyst 6500和Cisco IOS路由器之间的IPSec LAN到LAN隧道配置示例

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[背景信息](#)

[配置](#)

[网络图](#)

[IPsec的配置使用Layer2访问或中继端口](#)

[使用路由端口配置 IPsec](#)

[验证](#)

[故障排除](#)

[故障排除命令](#)

[相关信息](#)

## 简介

本文档介绍如何在含有 VPN 加速服务模块的 Cisco Catalyst 6500 系列交换机与 Cisco IOS® 路由器之间创建 IPsec LAN 到 LAN 隧道。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 适用于含 IPsec VPN 服务模块的 Catalyst 6000 Supervisor 引擎的 Cisco IOS 软件 12.2(14)SY2 版
- 运行 Cisco IOS 软件 12.3(4)T 版的 Cisco 3640 路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

## 规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

## 背景信息

Catalyst 6500 VPN 服务模块有两个千兆以太网 (GE) 端口，无外部可见的接头。这些端口只在配置时是可寻址的。端口 1 始终为内部端口。此端口处理从和到网络内部的所有业务量。第二个端口(端口2)处理所有业务量从和对广域网或外部网络。这两个端口在802.1q中继模式下总是配置。VPN服务模块对数据包流使用称线内冲突(BITW)的技术。

数据包由一对 VLAN 处理：一个第 3 层内部 VLAN 和一个第 2 层外部 VLAN。从内部传到外部的包，通过一种称为对内部VLAN的编码地址识别逻辑(EARL)的方法进行寻址。该方法将数据包加密之后，VPN 服务模块将使用相应的外部 VLAN。在解密过程中，使用外部 VLAN 将从外部到内部的数据包桥接到 VPN 服务模块。VPN 服务模块将数据包解密并将 VLAN 映射到相应的内部 VLAN 之后，EARL 将数据包路由到适当的 LAN 端口。第 3 层内部 VLAN 和第 2 层外部 VLAN 通过发出 `crypto connect vlan` 命令连接在一起。在Catalyst 6500系列交换机中有三种类型的端口：

- **路由端口**—默认情况下，所有以太网端口是路由端口。这些端口有一个与它联系的隐藏VLAN。
- **接入端口** - 这些端口有一个外部 VLAN 或 VLAN 中继协议 (VTP) VLAN 与其关联。您能关联超过一个端口到默认的VLAN。
- **中继端口** - 这些端口承载许多外部 VLAN 或 VTP VLAN，上面所有数据包都以 802.1Q 报头进行封装。

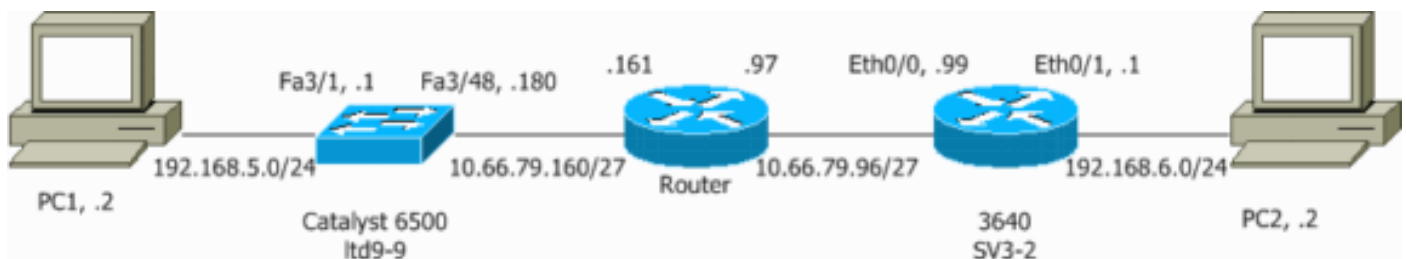
## 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：**有关本文档所用命令的详细信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

## 网络图

本文档使用此图中所示的网络设置：



## IPsec的配置使用Layer2访问或中继端口

执行以下这些步骤，在外部物理接口作为第 2 层接入或中继端口的情况下配置 IPsec。

1. 将内部 VLAN 添加到 VPN 服务模块的内部端口。假设 VPN 服务模块在插槽 4 上。使用 VLAN 100 作为内部 VLAN，VLAN 209 作为外部 VLAN。按如下所示配置 VPN 服务模块的 GE 端口：

```

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. 添加 VLAN 100 接口和隧道终止处的接口 ( 本例中为 interface 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. 配置外部物理端口作为接入或中继端口 ( 本例中为 FastEthernet 3/48 , 如下所示 ) 。

```

!--- 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. 创建旁路 NAT。将以下条目添加到 no nat 语句以免除在这些网络之间的 NAT :

```

!--- 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. 创建您的加密配置以及定义将被加密的流量的访问控制列表 (ACL)。按如下所示, 创建用于定义从内部网络 192.168.5.0/24 到远程网络 192.168.6.0/24 的流量的 ACL ( 本例中为 ACL 100 ) :

```

access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

```

按如下所示定义您的 Internet 安全连接和密钥管理协议 (ISAKMP) 策略方案 :

```

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

```

发出下面这个命令 ( 在本例中 ) 以使用和定义预共享密钥。

```

crypto isakmp key cisco address 10.66.79.99

```

定义您的IPsec建议, 象这样 :

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

按如下所示创建您的加密映射语句：

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

6. 按如下所示将加密映射应用于 VLAN 100 接口：

```
interface vlan100
crypto map cisco
```

使用以下这些配置。

- [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
```

## 使用路由端口配置 IPsec

执行以下这些步骤，在外部物理接口作为第 3 层路由端口的情况下配置 IPsec。

1. 将内部 VLAN 添加到 VPN 服务模块的内部端口。假设 VPN 服务模块在插槽 4 上。使用 VLAN 100 作为内部 VLAN，VLAN 209 作为外部 VLAN。按如下所示配置 VPN 服务模块的 GE 端口：

```
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. 添加 VLAN 100 接口和隧道终止处的接口（本例中为 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. 创建旁路 NAT。将以下条目添加到 no nat 语句以免除在这些网络之间的 NAT：

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

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

4. 创建您的加密配置以及用于定义被加密的流量的 ACL。按如下所示，创建用于定义从内部网络 192.168.5.0/24 到远程网络 192.168.6.0/24 的流量的 ACL（本例中为 ACL 100）：

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

按如下所示定义您的 ISAKMP 策略方案：

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

发出下面这个命令（在本例中）以使用和定义预共享密钥：

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

定义您的 IPsec 建议，象这样：

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

按如下所示创建您的加密映射语句：

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

5. 按如下所示将加密映射应用于 VLAN 100 接口：

```
interface vlan100
crypto map cisco
```

使用以下这些配置。

- [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

```

**验证**

本部分提供的信息有助于确认配置是否正常运行。

[命令输出解释程序 \( 仅限注册用户 \)](#) (OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show crypto ipsec sa** — 显示当前 IPsec SA 所使用的设置。
- **show crypto isakmp sa** — 显示所有当前IKE SAS在对等体。
- **show crypto vlan** - 显示与加密配置关联的 VLAN。
- **show crypto eli** - 显示 VPN 服务模块的统计信息。

有关验证和排除 IPsec 故障的其他信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

## 故障排除

此部分提供信息故障排除您的配置。

### 故障排除命令

**注意：** 在发出 **debug** 命令之前，请参阅[有关 debug 命令的重要信息](#)。

- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。
- **debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。
- **debug crypto engine** - 显示已加密的数据流。
- **clear crypto isakmp** - 清除与第 1 阶段相关的 SA。
- [clear crypto sa](#) - 清除与第 2 阶段相关的 SA。

有关验证和排除 IPsec 故障的其他信息，请参阅 [IP 安全故障排除 - 了解和使用 debug 命令](#)。

## 相关信息

- [IPSec 支持页面](#)
- [配置 IPSec 网络安全](#)
- [配置 Internet 密钥交换安全协议](#)
- [技术支持 - Cisco Systems](#)