VPN サービス モジュールを搭載した Catalyst 6500 と Cisco ルータ間の IPSec LAN-to-LAN トンネルの設定例

目次

概要

このドキュメントは、VPN Acceleration サービス モジュールを搭載した Cisco Catalyst 6500 シリーズ スイッチと Cisco IOS® ルータの間に IPSec LAN-to-LAN トンネルを作成する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- IPSec VPN サービスモジュールが付いている Catalyst 6000 Supervisor Engine のための Cisco IOS ソフトウェア リリース 12.2(14)sy2、
- Cisco IOS ソフトウェア リリース 12.3(4)T を実行する Cisco 3640 ルータ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

Catalyst 6500 VPN サービス モジュールには 2 つの Gigabit Ethernet（GE; ギガビット イーサネット）ポートがありますが、外部から見えるコネクタはありません。 これらのポートは、設定の目的にのみアドレスを指定できます。 ポート 1 は、常に内部ポートです。 このポートでは、内部ネットワークと送受信されるすべてのトラフィックが処理されます。 2 つ目のポート（ポート 2）では、WAN や外部ネットワークと送受信されるすべてのトラフィックが処理されます。 2 つのポートは常に 802.1Q トランキング モードに設定されます。 VPN サービス モジュールでは、パケット フローに Bump In The Wire （BITW）と呼ばれる技術が使用されます。

パケットは、1 対の VLAN、1 つのレイヤ 3 内部 VLAN、および 1 つのレイヤ 2 外部 VLAN によって処理されます。 内部から外部へ伝送されるパケットは、Encoded Address Recognition Logic（EARL）という方式で内部 VLAN へルーティングされます。 VPN サービス モジュールでは、パケットを暗号化した後、対応する外部 VLAN が使用されます。 復号化プロセスでは、外部から内部へ入るパケットは外部 VLAN を使用して VPN サービス モジュールにブリッジされます。 VPN サービス モジュールがパケットを復号化し、VLAN を対応する内部 VLAN にマッピングすると、パケットは EARL によって適切な LAN ポートへルーティングされます。 crypto connect vlan コマンドを発行することによって、レイヤ 3 内部 VLAN とレイヤ 2 外部 VLAN が接続されます。 Catalyst 6500 シリーズ スイッチには、3 種類のポートがあります。

- ルーテッド ポート - デフォルトでは、すべてのイーサネット ポートはルーテッド ポートです。 これらのポートには、隠し VLAN が 1 つ関連付けられています。
- アクセス ポート - これらのポートには、外部 VLAN または VLAN Trunk Protocol（VTP）VLAN が 1 つ関連付けられています。 定義済み VLAN には、複数のポートを関連付けることができます。
- トランク ポート - これらのポートは多数の外部 VLAN または VTP VLAN を保持しており、すべてのパケットが 802.1Q ヘッダーによってカプセル化されます。

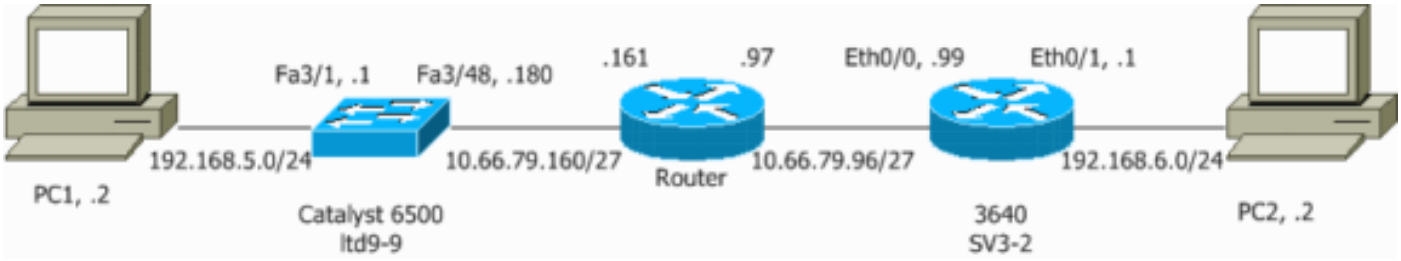
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

この文書では、次のダイヤグラムに示すネットワーク設定を使用します。



レイヤ2 アクセスまたはトランク ポートを使用した IPsec のための設定

外部物理インターフェイスのためのレイヤ2 アクセスかトランク ポートの助けによって IPsec を設定するためにこれらのステップを実行して下さい。

1. 内部 VLAN を VPN サービス モジュールの内部ポートに追加します。VPN サービスモジュールがスロット 4.にあると仮定して下さい。 外部 VLAN として内部 VLAN および VLAN 209 として VLAN 100 を使用して下さい。 VPN サービス モジュールの GE ポートを次のように設定します。

```
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. VLAN 100 インターフェイスをおよびトンネルが終わる（、この場合、 VLAN 209 であるインターフェイスをここに示されている追加して下さい、）。

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

3. 外部物理ポートをアクセス ポートまたはトランク ポート（次に示すように、この場合は FastEthernet 3/48）に設定します。

```
!--- 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. バイパス NAT を作成して下さい。 次のネットワーク間で NAT を免除するには、no nat ス

テートメントにこれらのエントリを追加します。

```
!--- 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. 暗号設定と、暗号化するトラフィックを定義するための Access Control List（ACL; アクセス コントロール リスト）を作成します。次のように、内部ネットワーク 192.168.5.0/24 からリモート ネットワーク 192.168.6.0/24 へ送信されるトラフィックを定義する ACL（この場合は ACL 100）を作成します。

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

   次のように、Internet Security Association and Key Management Protocol（ISAKMP）ポリシーのプロポーザルを定義します。

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

   事前共有キーを使用し、定義するために、（この例では）次のコマンドを発行します。

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

   このような IPsec 提案を、定義して下さい:

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

   次のように、crypto map 文を作成します。

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

6. 次のように、暗号マップを VLAN 100 インターフェイスに適用します。

   ```
   interface vlan100
   crypto map cisco
   ```

次の設定が使用されます。

- Catalyst 6500
- Cisco IOS ルータ

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 ルータ

```
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
```

ルーテッドポートを使用した IPsec のための設定

外部物理インターフェイスのためのレイヤ3 ルーテッドポートの助けによって IPsec を設定するためにこれらのステップを実行して下さい。

1. 内部 VLAN を VPN サービス モジュールの内部ポートに追加します。VPN サービスモジュールがスロット 4.にあると仮定して下さい。 外部 VLAN として内部 VLAN および VLAN 209 として VLAN 100 を使用して下さい。 VPN サービス モジュールの GE ポートを次のように設定します。

   ```
   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. VLAN 100 インターフェイスと、トンネルが終端するインターフェイス (次に示すように、この場合は FastEthernet3/48) を追加します。

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

3. バイパス NAT を作成して下さい。 次のネットワーク間で NAT を免除するには、no nat ステートメントにこれらのエントリを追加します。

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

4. 暗号設定と、暗号化するトラフィックを定義するための ACL を作成します。次のように、内部ネットワーク 192.168.5.0/24 からリモート ネットワーク 192.168.6.0/24 へ送信されるトラフィックを定義する ACL（この場合は ACL 100）を作成します。

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

次のように、ISAKMP ポリシー のプロポーザルを定義します。

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

事前共有キーを使用し、定義するために、（この例では）次のコマンドを発行します。

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

このような IPsec 提案を、定義して下さい:

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

次のように、crypto map 文を作成します。

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

5. 次のように、暗号マップを VLAN 100 インターフェイスに適用します。

```
interface vlan100
crypto map cisco
```

次の設定が使用されます。

- Catalyst 6500
- Cisco IOS ルータ

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 ルータ

```
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
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認するための情報について説明しています。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto ipsec sa** —現在の IPSec SA によって使用される設定を示します。
- show crypto isakmp sa - 現在ピアにあるすべての IKE SA を表示します。
- show crypto vlan - 暗号設定に関連付けられている VLAN を表示します。
- show crypto eli - VPN サービス モジュールの統計を表示します。

IPsec の検証およびトラブルシューティングのその他の情報に関しては、IP Security Troubleshooting - Understanding and Using debug Commands を参照して下さい。

トラブルシューティング

このセクションでは、設定のトラブルシューティングを行うための情報について説明します。

トラブルシューティングのためのコマンド

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

- **debug crypto ipsec**：フェーズ 2 の IPSec ネゴシエーションを表示します。
- **debug crypto isakmp**：フェーズ 1 の ISAKMP ネゴシエーションを表示します。
- **debug crypto engine**：暗号化されたトラフィックを表示します。
- **clear crypto isakmp**：フェーズ 1 に関連する SA をクリアします。
- **clear crypto sa**：フェーズ 2 に関連する SA をクリアします。

IPsec の検証およびトラブルシューティングのその他の情報に関しては、IP Security Troubleshooting - Understanding and Using debug Commands を参照して下さい。

関連情報

- **IPSec に関するサポート ページ**
- **IPsec ネットワーク セキュリティの設定**
- **インターネット キー交換セキュリティ プロトコルの設定**
- **テクニカルサポート - Cisco Systems**