

directed モードの CSM での VPN ロード バランシング設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、コンテンツ スイッチング モジュール (CSM) での VPN のロード バランシングの設定例を紹介します。VPN ロード バランシングは、一連の VPN コンセントレータまたは VPN ヘッドエンド デバイスに VPN のセッションをインテリジェントに分散させるメカニズムです。VPN のロード バランシングは、次の理由により実装されます。

- VPN デバイスのパフォーマンスまたは拡張性の制限を克服するためたとえば、パケット/秒、接続/秒、スループットなどです
- 冗長性を提供するため (シングルポイント障害を排除)

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- スポークからルーティング情報を自動的に伝搬するために、ヘッドエンドデバイスで Reverse Route Injection (RRI) を実装します。
- VLAN 61 と 51 が同じサブネットを共有できるようにします。

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いています。

- CSM搭載Cisco Catalyst 6500
- Cisco 2621 ルータ
- Cisco 7206
- Cisco 7206VXR
- Cisco 7204VXR
- Cisco 7140

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実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。

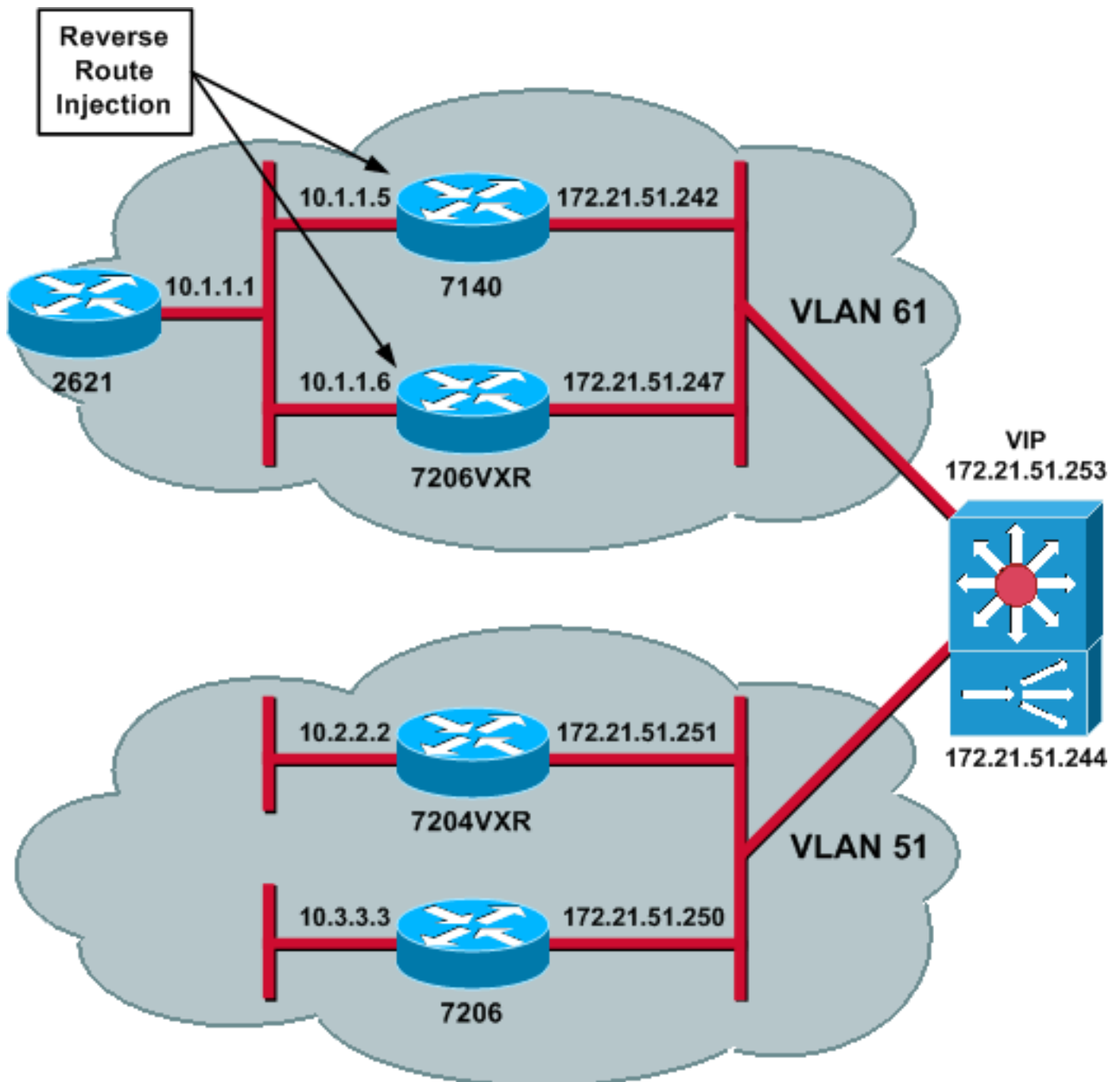
[設定](#)

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクション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）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

[ネットワーク図](#)

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- [CSMの設定](#)
- [ヘッドエンドルータの設定 - 7206VXR](#)
- [スポークルータの設定 : 7206](#)

CSMの設定

次のステップを実行します。

1. スポークからルーティング情報を自動的に伝播するために、ヘッドエンドデバイスでRRIを実装します。注：VLAN 61とVLAN 51は同じサブネットを共有します。
2. VLANクライアントとVLANサーバを定義します。

3. IPSecサーバの状態を確認するために使用するプローブを定義します。

```
!--- The CSM is located in slot 4. module ContentSwitchingModule 4 vlan 51 client ip
address 172.21.51.244 255.255.255.240 ! vlan 61 server ip address 172.21.51.244
255.255.255.240 ! probe ICMP_PROBE icmp interval 5 retries 2 !
```

4. 実際のIPSecサーバを使用してserverfarmを定義します。

5. 停止したサーバに属する接続をフラッシュするように、失敗の消去を構成します。

6. ステイッキポリシーを定義します。

```
!--- Serverfarm VPN_IOS and real server members. serverfarm VPN_IOS
nat server
no nat client
!--- Set the behavior of connections when the real servers have failed. failaction purge
real 172.21.51.242
inservice
real 172.21.51.247
inservice
probe ICMP_PROBE
!--- Ensure that connections from the same client match the same server !--- load
balancing (SLB) policy. !--- Use the same real server on subsequent connections; issue the
!--- sticky command.

sticky 5 netmask 255.255.255.255 timeout 60
!
policy VPNIOS
sticky-group 5
serverfarm VPN_IOS
!
```

7. トラフィックフローごとに1つずつ、VServersを定義します。

```
!--- Virtual server VPN_IOS_ESP. vserver VPN_IOS_ESP
!--- The virtual server IP address is specified. virtual 172.21.51.253 50 !--- Persistence
rebalance is used for HTTP 1.1, to rebalance the connection !--- to a new server using the
load balancing policy. persistent rebalance !--- Associate the load balancing policy with
the VPNIOS virtual server. slb-policy VPNIOS inservice ! vserver VPN_IOS_IKE virtual
172.21.51.253 udp 500 persistent rebalance slb-policy VPNIOS inservice !
```

ヘッドエンドルータの設定 - 7206VXR

```
crypto isakmp policy 10
authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
crypto dynamic-map mydyn 10
set transform-set myset
reverse-route
!
crypto map mymap 10 ipsec-isakmp dynamic mydyn
!
interface FastEthernet0/0
ip address 172.21.51.247 255.255.255.240
crypto map mymap
!
interface FastEthernet2/0
```

```
ip address 10.1.1.6 255.255.255.0

router eigrp 1
 redistribute static
 network 10.0.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip default-gateway 172.21.51.241
ip classless
ip route 0.0.0.0 0.0.0.0 172.21.51.241
no ip http server
!
```

スポークルータの設定 : 7206

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 172.21.51.253
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
crypto map mymap 10 ipsec-isakmp
 set peer 172.21.51.253
 set transform-set myset
 match address 101
!
interface Loopback0
 ip address 10.3.3.3 255.255.255.0
!
interface Ethernet0/0
 ip address 172.21.51.250 255.255.255.240
 duplex auto
 crypto map mymap
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.21.51.241
no ip http server
!
access-list 101 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255
!
```

確認

ここでは、設定が正常に機能しているかどうかを確認します。

[アウトプット インタープリタ ツール \(登録ユーザ専用 \) \(OIT \) は、特定の show コマンドをサポートします。](#) OIT を使用して、show コマンドの出力の分析を表示します。

- **show module csm all** または **show module contentSwitchingModule all** コマンドを発行します。どちらのコマンドも同じ情報を生成します。 **show module contentSwitchingModule all vservers** コマンドは、SLB 仮想サーバ情報を表示します。

```
Cat6506-1-Native# show module contentSwitchingModule all vservers
```

```
----- CSM in slot 4 -----
```

```
slb vserver      prot      virtual      vlan      state      conns
```

```
-----
```

```
VPN_IOS_ESP      50      172.21.51.253/32:0      ALL  OPERATIONAL  2
VPN_IOS_IKE      UDP     172.21.51.253/32:500   ALL  OPERATIONAL  2
```

show module contentSwitchingModule all conns コマンドは、SLB接続情報を表示します。

```
Cat6506-1-Native# show module contentSwitchingModule all conns
```

```
----- CSM in slot 4 -----
```

	prot	vlan	source	destination	state
In	UDP	51	172.21.51.250:500	172.21.51.253:500	ESTAB
Out	UDP	61	172.21.51.242:500	172.21.51.250:500	ESTAB
In	50	51	172.21.51.251	172.21.51.253	ESTAB
Out	50	61	172.21.51.247	172.21.51.251	ESTAB
In	50	51	172.21.51.250	172.21.51.253	ESTAB
Out	50	61	172.21.51.242	172.21.51.250	ESTAB
In	UDP	51	172.21.51.251:500	172.21.51.253:500	ESTAB
Out	UDP	61	172.21.51.247:500	172.21.51.251:500	ESTAB

show module contentSwitchingModule all sticky コマンドは、SLBスティッキデータベースを表示します。

```
Cat6506-1-Native# show module contentSwitchingModule all sticky
```

```
----- CSM in slot 4 -----
```

```
client IP:      172.21.51.250
real server:    172.21.51.242
connections:    0
group id:       5
timeout:        38
sticky type:    netmask 255.255.255.255
```

```
client IP:      172.21.51.251
real server:    172.21.51.247
connections:    0
group id:       5
timeout:        40
sticky type:    netmask 255.255.255.255
```

- ルータで**show ip route**コマンドを発行します。

```
2621VPN# show ip route
```

```
!--- Output suppressed. 10.0.0.0/24 is subnetted, 3 subnets D EX 10.2.2.0 [170/30720] via
10.1.1.6, 00:13:57, FastEthernet0/0 D EX 10.3.3.0 [170/30720] via 10.1.1.5, 00:16:15,
FastEthernet0/0 C 10.1.1.0 is directly connected, FastEthernet0/0 D*EX 0.0.0.0/0 [170/30720]
via 10.1.1.5, 00:37:58, FastEthernet0/0 [170/30720] via 10.1.1.6, 00:37:58, FastEthernet0/0
```

```
2621VPN# 7206VXR# show ip route
```

```
!--- Output suppressed. 172.21.0.0/28 is subnetted, 1 subnets C 172.21.51.240 is directly
connected, FastEthernet0/0 10.0.0.0/24 is subnetted, 3 subnets S 10.2.2.0 [1/0] via 0.0.0.0,
FastEthernet0/0 D EX 10.3.3.0 [170/30720] via 10.1.1.5, 00:16:45, FastEthernet2/0 C 10.1.1.0
is directly connected, FastEthernet2/0 S* 0.0.0.0/0 [1/0] via 172.21.51.241
```

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [dispatched モードの CSM での VPN ロード バランシング設定例](#)
- [Catalyst 6500シリーズスイッチコンテンツスイッチングモジュールコマンドリファレンス](#)

4.1(2)

- [テクニカル サポートとドキュメント – Cisco Systems](#)