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

目次

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スケーラビリティ 制限を克服するため; たとえば、パケット毎秒、接続毎秒およびスループット
- 冗長性を提供するため（シングル ポイント障害を取除いて下さい）

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。

- スポークからの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、設定して下さい。
- 同じ サブネットを共有することを VLAN 61 および 51 が可能にして下さい。

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。

- CSM の 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。

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）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

このドキュメントでは、次の設定を使用します。

- CSM 設定
- ヘッドエンドルータ 設定- 7206VXR
- スポークルータ 設定- 7206

CSM 設定

次の手順を実行します。

1. スポークからの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 RRI を、設定して下さい。**注:** VLAN 61 および VLAN 51 の共有 同じ サブネット。
2. VLAN クライアントおよび VLAN サーバを定義して下さい。
3. IPSecサーバの健全性をチェックするのに使用されるプローブを定義して下さい。

```
!--- 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. 実質 IPSecサーバが付いている**サーバファームを**定義して下さい。
5. デッド サーバに属する接続をフラッシュするために **failaction パージを**、設定して下さい。
6. スティッキ ポリシーを定義して下さい。

```
!--- 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. Vserver を、トラフィックフローごとに 1 定義して下さい。

```
!--- 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 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 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、設定が正常に動作していることを確認します。

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 module csm をすべて**発行すれば **show module contentSwitchingModule はすべて**命じます; コマンドは両方とも同じ情報を生成します。**show module contentSwitchingModule はすべての vserver** コマンド SLB 仮想サーバ 情報を示します。`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 はすべての conns** コマンド SLB 接続 情報を示します。`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 はすべての sticky コマンド** SLB スティッキー データベースを示します。`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`
- ルータの **show ip route コマンドを**発行して下さい。`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

現在のところ、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 Content Switching Module コマンドレファレンス、4.1(2)
- テクニカルサポートとドキュメント - Cisco Systems