dispatched 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、ディスパッチ モードのコンテンツ スイッチング モジュール（CSM）で VPN ロード バランシングを設定するため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 ロード バランシングは、次のものに実装されます。

- VPN デバイス、たとえば、パケット毎秒、接続毎秒およびスループットのパフォーマンス/スケーラビリティ 制限を克服して下さい。
- 冗長性を提供します（シングル ポイント障害を取除いて下さい）。

はじめに

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- ハブルータは両方とも同じループバックIPアドレス（VIP）で設定されます。
- Reverse Route Injection （RRI）はヘッドエンドルータで設定されています。
- 認証ヘッダー（AH）を使用して下さい。

使用するコンポーネント

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

- Cisco 7140 および 7206
- Cisco 7206VXR および 7204VXR
- Cisco Catalyst 6500 CSM

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。

コンフィギュレーション タスク

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。

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。

CSM 設定- Dispatchedモード

次の手順を実行します。

1. VLAN クライアントおよび VLAN サーバを定義して下さい。
2. 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。 **モジュール csm かモジュール contentSwitchingModule** コマンドを使用して下さい; 両方とも同じ情報を生成します。
```
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
!
```
3. 実質 IPSecサーバが付いている severfarm を定義して下さい
4. 発送モードを示すために **no nat server** コマンドを発行して下さい。
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**示して下さい。
6. スティッキ ポリシーを定義して下さい。
```
serverfarm VPN_IOS
  no nat server no nat client failaction purge real 172.21.51.242 inservice real
172.21.51.247 inservice probe ICMP_PROBE ! 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。
```
vserver VPN_IOS_AH_2
  virtual 172.21.51.233 51
  persistent rebalance
  slb-policy VPNIOS
```

```
  inservice
!
 vserver VPN_IOS_ESP_2
  virtual 172.21.51.233 50
  persistent rebalance
  slb-policy VPNIOS
  inservice
!
vserver VPN_IOS_IKE_2
  virtual 172.21.51.233 udp 500
  persistent rebalance
  slb-policy VPNIOS
  inservice
!
```

ヘッドエンドルータ 設定-ディスパッチ モード

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 0.0.0.0
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set myset ah-sha-hmac 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 local-address Loopback0
crypto map mymap 10 ipsec-isakmp dynamic mydyn
interface Loopback0
 ip address 172.21.51.233 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.1.5 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.21.51.242 255.255.255.240
 crypto map mymap
!
router eigrp 1
 redistribute static
 network 10.0.0.0
 no auto-summary
 no eigrp log-neighbor-changes
!
ip route 0.0.0.0 0.0.0.0 172.21.51.241
```

スポークルータ 設定-ディスパッチ モード

```
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 172.21.51.233
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set myset ah-sha-hmac 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 172.21.51.233
 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 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際に役立つ情報を提供しています。

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。

```
Cat6506-1-Native#sh module c 4 vser slb vserver prot virtual vlan state conns ------------------
---------------------------------------------------------- VPN_IOS_ESP 50 172.21.51.253/32:0 ALL
OPERATIONAL 0 VPN_IOS_IKE UDP 172.21.51.253/32:500 ALL OPERATIONAL 0 VPN_IOS_ESP_2 50
172.21.51.233/32:0 ALL OPERATIONAL 0 VPN_IOS_IKE_2 UDP 172.21.51.233/32:500 ALL OPERATIONAL 2
VPN_IOS_AH_2 51 172.21.51.233/32:0 ALL OPERATIONAL 2
Cat6506-1-Native#sh module c 4 sticky client IP: 172.21.51.250 real server: 172.21.51.247
connections: 0 group id: 5 timeout: 39 sticky type: netmask 255.255.255.255 client IP:
172.21.51.251 real server: 172.21.51.242 connections: 0 group id: 5 timeout: 39 sticky type:
netmask 255.255.255.255
2621VPN#sh ip ro ÂÂ… 10.0.0.0/24 is subnetted, 3 subnets D EX 10.3.3.0 [170/30720] via 10.1.1.6,
00:00:05, FastEthernet0/0 D EX 10.2.2.0 [170/30720] via 10.1.1.5, 00:00:30, FastEthernet0/0 C
10.1.1.0 is directly connected, FastEthernet0/0 D*EX 0.0.0.0/0 [170/30720] via 10.1.1.6,
00:18:15, FastEthernet0/0 [170/30720] via 10.1.1.5, 00:18:15, FastEthernet0/0 2621VPN# 7140-
2FE#sh ip route ÂÂ… 172.21.0.0/16 is variably subnetted, 2 subnets, 2 masks C 172.21.51.233/32
is directly connected, Loopback0 C 172.21.51.240/28 is directly connected, FastEthernet0/1
10.0.0.0/24 is subnetted, 3 subnets D EX 10.3.3.0 [170/30720] via 10.1.1.6, 00:01:01,
FastEthernet0/0 S 10.2.2.0 [1/0] via 0.0.0.0, FastEthernet0/1 C 10.1.1.0 is directly connected,
FastEthernet0/0 S* 0.0.0.0/0 [1/0] via 172.21.51.241 7140-2FE#sh cry ip sa interface:
FastEthernet0/1 Crypto map tag: mymap, local addr. 172.21.51.233 local ident
(addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(10.2.2.0/255.255.255.0/0/0) current_peer: 172.21.51.251 PERMIT, flags={} #pkts encaps: 4, #pkts
encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4 #pkts compressed:
0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress
failed: 0 #send errors 0, #recv errors 0
     local crypto endpt.: 172.21.51.233, remote crypto endpt.: 172.21.51.251
     path mtu 1500, media mtu 1500
     current outbound spi: 3280D368

     ….
     inbound ah sas:
      spi: 0xB259E0C1(2992234689)
        transform: ah-sha-hmac ,
```

```
in use settings ={Tunnel, }
slot: 0, conn id: 5141, flow_id: 19, crypto map: mymap
sa timing: remaining key lifetime (k/sec): (4607999/3474)
replay detection support: Y
```

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

- directed モードの CSM での VPN ロード バランシング設定例
- テクニカルサポート - Cisco Systems