

Balanceamento de carga VPN no CS no exemplo de configuração do modo despachado

Índice

[Introdução](#)

[Antes de Começar](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Tarefas das configurações](#)

[Diagrama de Rede](#)

[Configuração de CSM - Modo despachado](#)

[Configuração do roteador de extremidade principal - Modo da expedição](#)

[Configuração do Spoke Router - Modo da expedição](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece uma configuração de exemplo configurando o Balanceamento de carga VPN no módulo content switching (CS) no modo despachado. O Balanceamento de carga VPN é um mecanismo que distribua inteligentemente sessões de VPN ao longo de um grupo de concentradores VPN ou de dispositivos de extremidade principais VPN. O Balanceamento de carga VPN é executado a:

- supere o desempenho/limitações de escalabilidade em dispositivos VPN, por exemplo, em pacotes por segundo, em conexões por segundo, e em taxa de transferência.
- forneça a Redundância (remova o ponto de falha único).

[Antes de Começar](#)

[Requisitos](#)

Antes de tentar esta configuração, verifique se estes requisitos são atendidos:

- Ambos os roteadores de hub são configurados com o mesmo endereço IP de loopback (VIP).
- O Reverse Route Injection (RRI) é executado nos roteadores de extremidade principais.
- Use os cabeçalhos de autenticação (AH).

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Cisco 7140 e 7206
- Cisco 7206VXR e 7204VXR
- Cisco catalyst 6500 CS

Convenções

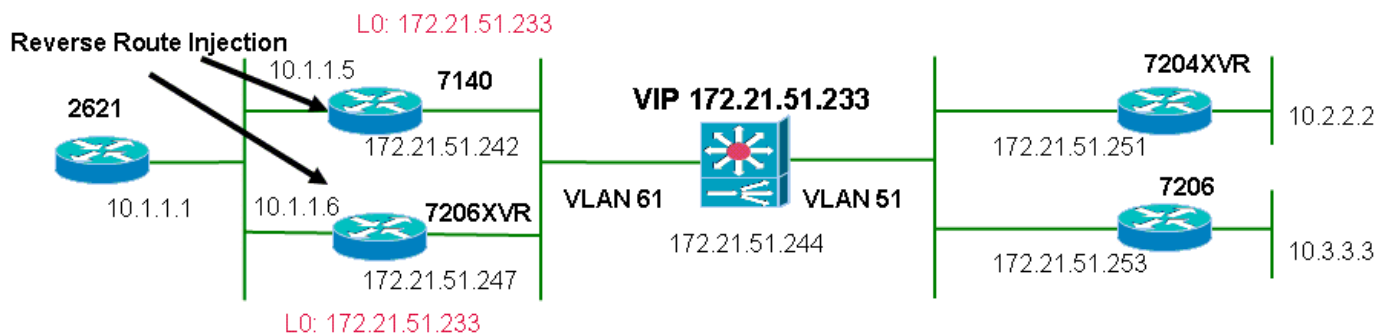
Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Tarefas das configurações

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configuração de CSM - Modo despachado

Termine estas etapas.

1. Defina o VLAN cliente e o servidor de VLAN.
2. Defina a ponta de prova usada para verificar a saúde dos servidores IPsec. Use o **módulo csm** ou o comando do **contentSwitchingModule** do **módulo**; ambos gerenciem a mesma informação.

```
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. Defina o severfarm com os servidores reais de IPSec
4. Emita o **comando no nat server** indicar o modo da expedição.
5. Indique a **remoção do failaction** para nivelar as conexões que pertencem aos servidores inoperantes.
6. Defina a política de dificuldades.

```
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. Defina vserveres, um pelo fluxo de tráfego.

```
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
!
```

Configuração do roteador de extremidade principal - Modo da expedição

```
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
```

Configuração do Spoke Router - Modo da expedição

```
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
!
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

Emita o comando **show module csm all** ou **show module contentSwitchingModule all**; os comandos **both** gerenciam a mesma informação.

```
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 ... 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 ... 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
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Balanceamento de carga VPN no CS no exemplo de configuração do modo direcionado](#)
- [Suporte Técnico - Cisco Systems](#)