Equilibrio de carga VPN en el CS en el ejemplo de configuración del modo enviado

Contenido

Introducción

Este documento proporciona una configuración de muestra para configurar el Equilibrio de carga VPN en el módulo content switching (CS) en el modo enviado. El Equilibrio de carga VPN es un mecanismo que distribuye inteligente a las sesiones de VPN a lo largo de un conjunto de los concentradores VPN o de los dispositivos de centro de distribuidor VPN. El Equilibrio de carga VPN se implementa a:

- supere el funcionamiento/las limitaciones de escalabilidad en los dispositivos VPN, por ejemplo, los paquetes por segundo, las conexiones por segundo, y la producción.
- proporcione la Redundancia (quite el solo punto de falla).

Antes de comenzar

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con estos requisitos:

- Configuran a ambos routeres de eje de conexión con el mismo Loopback IP Address (VIP).
- El Reverse Route Injection (RRI) se implementa en los routeres de centro distribuidor.
- Utilice los encabezados de autenticación (AH).

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cisco 7140 y 7206
- Cisco 7206VXR y 7204VXR
- Cisco Catalyst 6500 CS

Convenciones

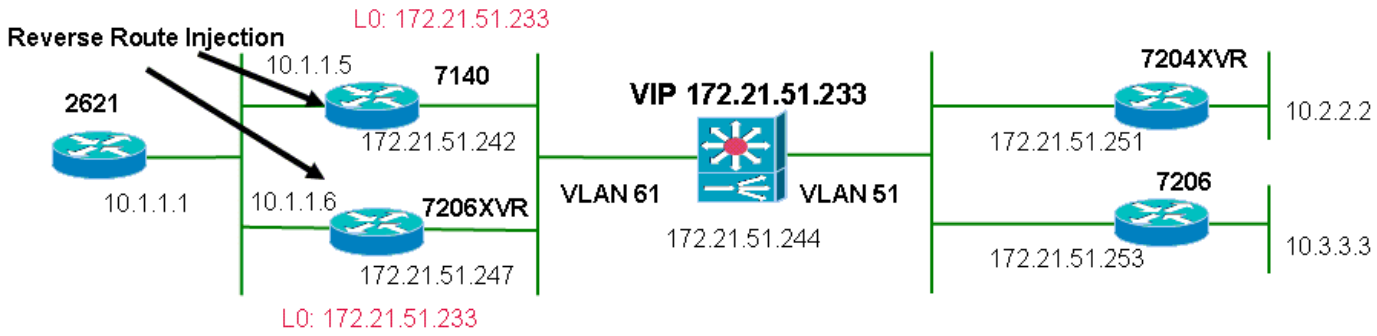
Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Tareas de las configuraciones

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración de CSM - Modo enviado

Complete estos pasos.

1. Defina el cliente VLAN y al servidor VLAN.
2. Defina la sonda usada para marcar la salud de los servidores del IPSec. Utilice el comando del **contentSwitchingModule del módulo csm** o del **módulo**; ambos generan la misma información.

```
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 el severfarm con los servidores IPSec reales
4. Publique el **comando no nat server** de indicar el modo del envío.
5. Indique la **purgación del failaction** para vaciar las conexiones que pertenecen a los servidores muertos.
6. Defina la política de cumplimiento.

```
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 el vservers, uno por el flujo de tráfico.

```
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
!
```

Configuración del router de centro distribuidor - Modo del envío

```
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
```

Configuración del router radial - Modo del envío

```
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
!
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

Publique el **comando show module csm all o show module contentSwitchingModule all**; los comandos both generan la misma información.

```
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
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Equilibrio de carga VPN en el CS en el ejemplo de configuración del modo dirigido
- Soporte Técnico - Cisco Systems