Ejemplo de Balanceo de Carga VPN en el CSM en la Configuración del Modo Directo

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para el balanceo de carga VPN en un Content Switching Module (CSM). El balanceo de carga VPN es un mecanismo que distribuye de forma inteligente sesiones VPN a lo largo de un conjunto de concentradores VPN o dispositivos de cabecera VPN. El balanceo de carga VPN se implementa por estas razones:

- para superar las limitaciones de rendimiento o escalabilidad en los dispositivos VPN; por ejemplo, paquetes por segundo, conexiones por segundo y rendimiento
- para proporcionar redundancia (eliminar un único punto de fallo)

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Implemente Reverse Route Injection (RRI) en los dispositivos de cabecera para propagar automáticamente la información de routing de los radios.
- Habilite VLAN 61 y 51 para compartir la misma subred.

Componentes Utilizados

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

- Cisco Catalyst 6500 con CSM
- Cisco 2621 Router
- 7206 de Cisco
- Cisco 7206VXR
- Cisco 7204VXR
- 7140 de Cisco

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

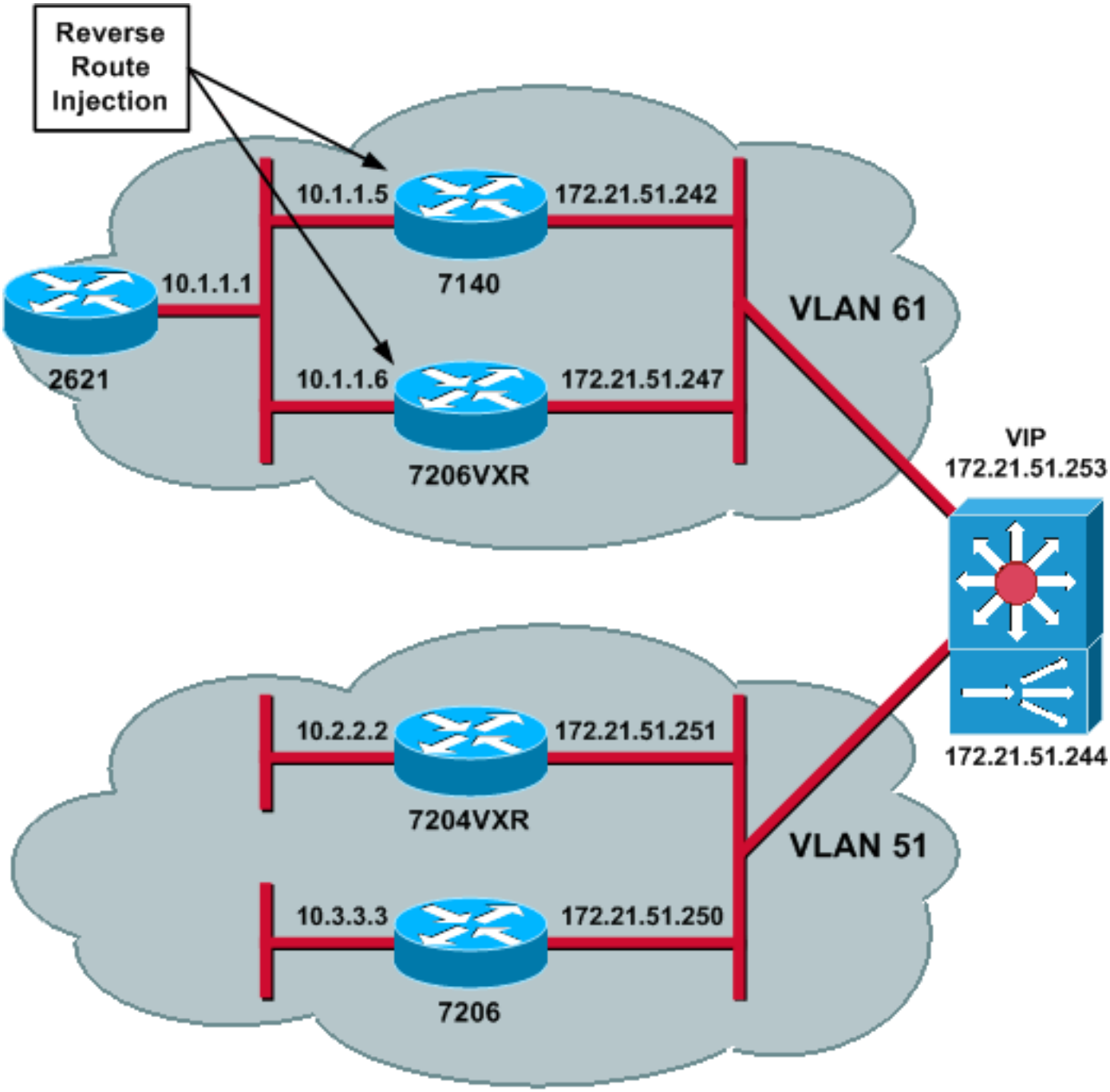
Configurar

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- Configuración de CSM
- Configuración del router de cabecera - 7206VXR
- Configuración del router de radio - 7206

Configuración de CSM

Complete estos pasos:

1. Implemente RRI en los dispositivos de cabecera para propagar la información de ruteo de los radios automáticamente.**Nota:** VLAN 61 y VLAN 51 comparten la misma subred.
2. Defina el cliente VLAN y el servidor VLAN.

3. Defina la sonda utilizada para verificar el estado de los servidores IPSec.

```
!--- 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. Defina el **serverfarm** con los servidores IPSec reales.
5. Configure **failaction purge**, para vaciar las conexiones que pertenecen a los servidores muertos.
6. Defina la política fija.

```
!--- 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. Defina VServers, uno por flujo de tráfico.

```
!--- 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 !
```

Configuración del router de cabecera - 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
!
```

Configuración del router de radio - 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
!
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- Ejecute el comando **show module csm all** o **show module contentSwitchingModule all**; ambos comandos generan la misma información.El comando **show module contentSwitchingModule all vservers** muestra la información del servidor virtual SLB.

```
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
```

El comando **show module contentSwitchingModule all conns** muestra la información de conexión SLB.

```
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
```

El comando **show module contentSwitchingModule all sticky** muestra la base de datos SLB sticky.

```
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
```

- Ejecute el comando **show ip route** en el router.

```
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
```

Troubleshoot

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

Información Relacionada

- Ejemplo de Configuración de Balanceo de Carga VPN en el CSM en el Modo Enviado
- Referencia de Comandos del Módulo de Switching de Contenido de Catalyst 6500 Series Switch, 4.1(2)
- Soporte Técnico y Documentación - Cisco Systems