Esempio di configurazione del bilanciamento del carico VPN sul CSM in modalità diretta

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per il bilanciamento del carico VPN su un modulo CSM (Content Switching Module). Il bilanciamento del carico VPN è un meccanismo che distribuisce in modo intelligente le sessioni VPN su un set di concentratori VPN o dispositivi headend VPN. Il bilanciamento del carico VPN viene implementato per i seguenti motivi:

- superare i limiti di prestazioni o scalabilità dei dispositivi VPN; ad esempio, pacchetti al secondo, connessioni al secondo e throughput
- per fornire ridondanza (rimuovere un singolo punto di errore)

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Implementare Reverse Route Injection (RRI) sui dispositivi headend per propagare automaticamente le informazioni di routing dai raggi.
- Abilitare le VLAN 61 e 51 per condividere la stessa subnet.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

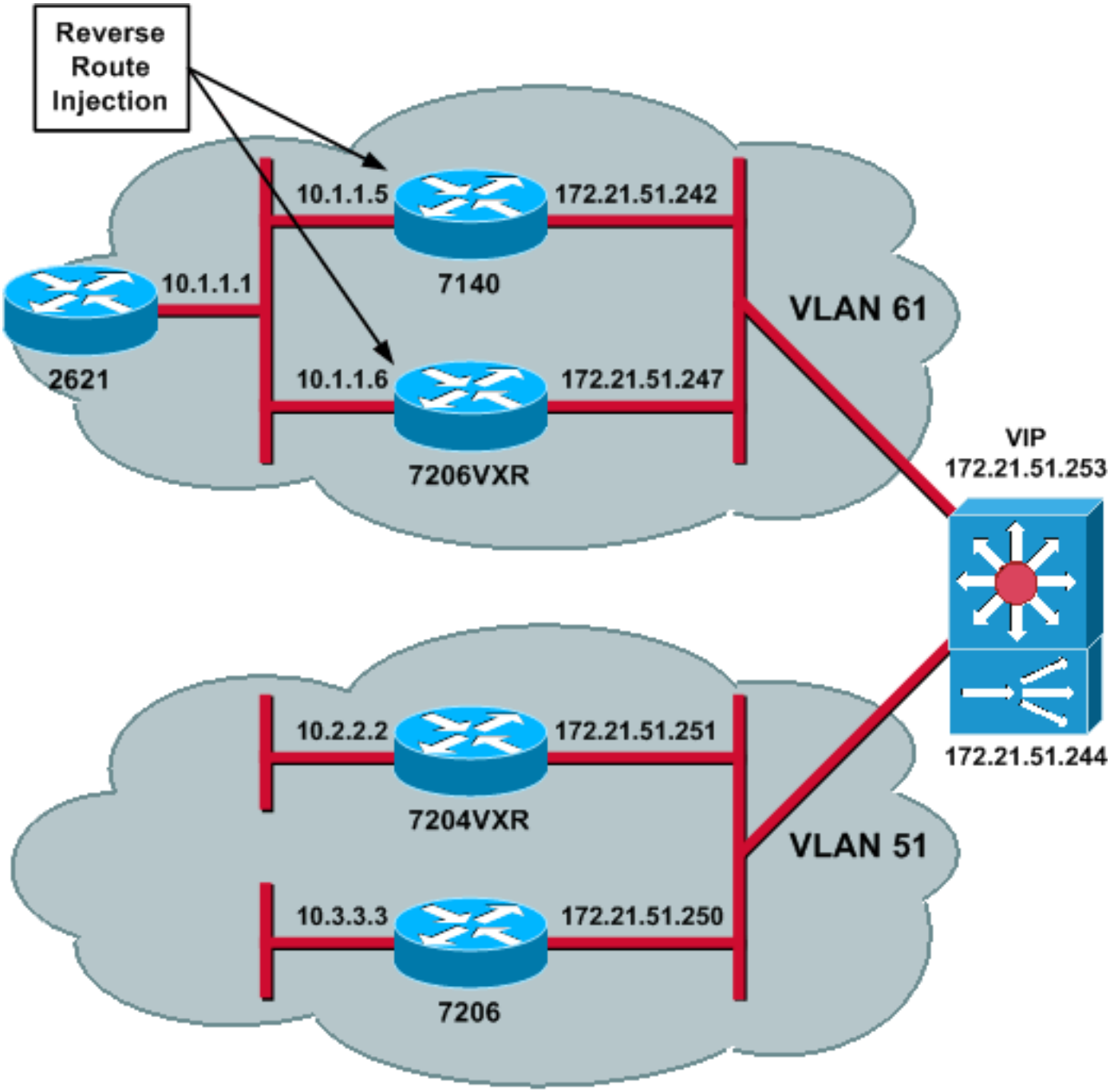
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Configurazioni

Nel documento vengono usate queste configurazioni:

- Configurazione CSM
- Configurazione router headend - 7206VXR
- Configurazione router spoke - 7206

Configurazione CSM

Attenersi alla seguente procedura:

1. Implementare RRI sui dispositivi headend per propagare automaticamente le informazioni di routing dagli spoke.**Nota: la** VLAN 61 e la VLAN 51 condividono la stessa subnet.
2. Definire il client VLAN e il server VLAN.

3. Definire il probe utilizzato per controllare lo stato dei server 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. Definire la **server farm** con i veri server IPSec.
5. Configurare la **rimozione degli errori** per scaricare le connessioni che appartengono ai server inattivi.
6. Definire il criterio di Sticky Notes.

```
!--- 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. Definire i server VS, uno per flusso di traffico.

```
!--- 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 !
```

Configurazione router headend - 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
!
```

Configurazione router spoke - 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
!
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- Eseguire il comando **show module csm all** o **show module contentSwitchingModule all**; entrambi i comandi generano le stesse informazioni.Il comando **show module contentSwitchingModule all vservers** mostra le informazioni sul server virtuale 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
```

Il comando **show module contentSwitchingModule all conns** visualizza le informazioni sulla connessione 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
```

Il comando **show module contentSwitchingModule all sticky** consente di visualizzare il database 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
```

- Eseguire il comando **show ip route** sul 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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Esempio di configurazione del bilanciamento del carico VPN sul CSM in modalità di invio
- Guida di riferimento ai comandi di Catalyst serie 6500 Switch Content Switching Module, 4.1(2)
- Documentazione e supporto tecnico – Cisco Systems