Konfigurationsbeispiel für VPN-Lastenausgleich auf dem CSM im Directed Mode

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für den VPN-Lastenausgleich auf einem Content Switching Module (CSM). VPN-Lastenausgleich ist ein Mechanismus, der VPN-Sitzungen auf intelligente Weise über eine Reihe von VPN-Konzentratoren oder VPN-Headend-Geräten verteilt. Der VPN-Lastenausgleich wird aus folgenden Gründen implementiert:

- Überwindung von Performance- oder Skalierbarkeitseinschränkungen bei VPN-Geräten; beispielsweise Pakete pro Sekunde, Verbindungen pro Sekunde und Durchsatz
- Redundanz bereitstellen (Entfernen eines Single Point of Failure)

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Implementieren Sie RRI (Reverse Route Injection) auf den Headend-Geräten, um die Routing-Informationen automatisch von den Stationen zu übertragen.
- Aktivieren Sie VLAN 61 und 51, um dasselbe Subnetz gemeinsam zu nutzen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und

Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

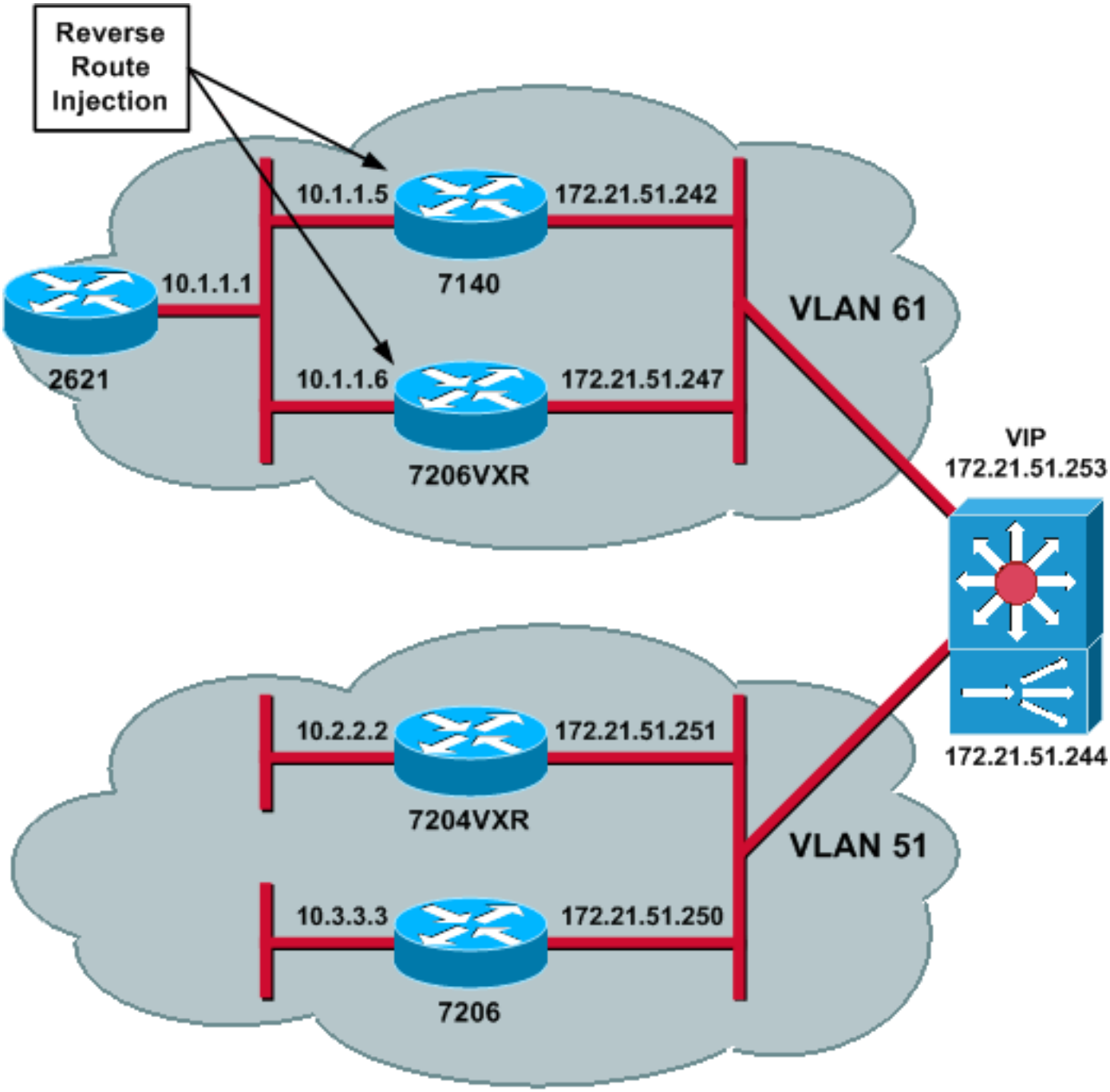
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- CSM-Konfiguration
- Konfiguration des Head-End-Routers - 7206VXR
- Konfiguration des Spoke-Routers - 7206

CSM-Konfiguration

Gehen Sie wie folgt vor:

1. Implementieren Sie RRI auf den Head-End-Geräten, um die Routing-Informationen automatisch von den Stationen weiterzuleiten.**Hinweis:** VLAN 61 und VLAN 51 nutzen dasselbe Subnetz.

2. Definieren Sie den VLAN-Client und den VLAN-Server.
3. Definieren Sie die Messsonde, die zur Überprüfung der Integrität der IPSec-Server verwendet wird.

```
!--- 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. Definieren Sie den **Serverfarm** mit den echten IPSec-Servern.
5. Konfigurieren Sie **eine Fehlerbehebung**, um die Verbindungen zu fehlerhaften Servern zu löschen.
6. Definieren Sie die Haftrichtlinie.

```
!--- 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. Definieren Sie VServer, einen pro Datenverkehrsfluss.

```
!--- 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 !
```

Konfiguration des Head-End-Routers - 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
!
```

Konfiguration des Spoke-Routers - 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
!
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- Geben Sie den Befehl **show module csm all** oder **show module contentSwitchingModule all** ein. Beide Befehle generieren die gleichen Informationen.Der Befehl **show module contentSwitchingModule all vservers** zeigt die Informationen zum virtuellen SLB-Server an.
  `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
```

Der Befehl **show module contentSwitchingModule all conns** zeigt SLB-Verbindungsinformationen an.

```
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
```

Der Befehl **show module contentSwitchingModule all stick** zeigt die SLB-Haftdatenbank.

```
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
```

- Geben Sie den Befehl **show ip route** auf dem Router ein.

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Konfigurationsbeispiel für VPN-Lastenausgleich auf dem CSM im Dispatched Mode
- Catalyst Switch der Serie 6500 - Content-Switching-Modul-Befehlsreferenz, 4.1(2)
- Technischer Support und Dokumentation - Cisco Systems