VPN Load Balancing on the CSM in Directed Mode Configuration Example

Document ID: 63390

Contents

Introduction

This document provides a sample configuration for VPN load balancing on a Content Switching Module (CSM). VPN load balancing is a mechanism that intelligently distributes VPN sessions along a set of VPN concentrators or VPN head−end devices. VPN load balancing is implemented for these reasons:

- to overcome performance or scalability limitations on VPN devices; for example, packets per second, connections per second, and throughput
- to provide redundancy (remove a single point of failure)

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Implement Reverse Route Injection (RRI) at the head−end devices, to propagate the routing information from the spokes automatically.
- Enable VLAN 61 and 51 to share the same subnet.

Components Used

The information in this document is based on these software and hardware versions:

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

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.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

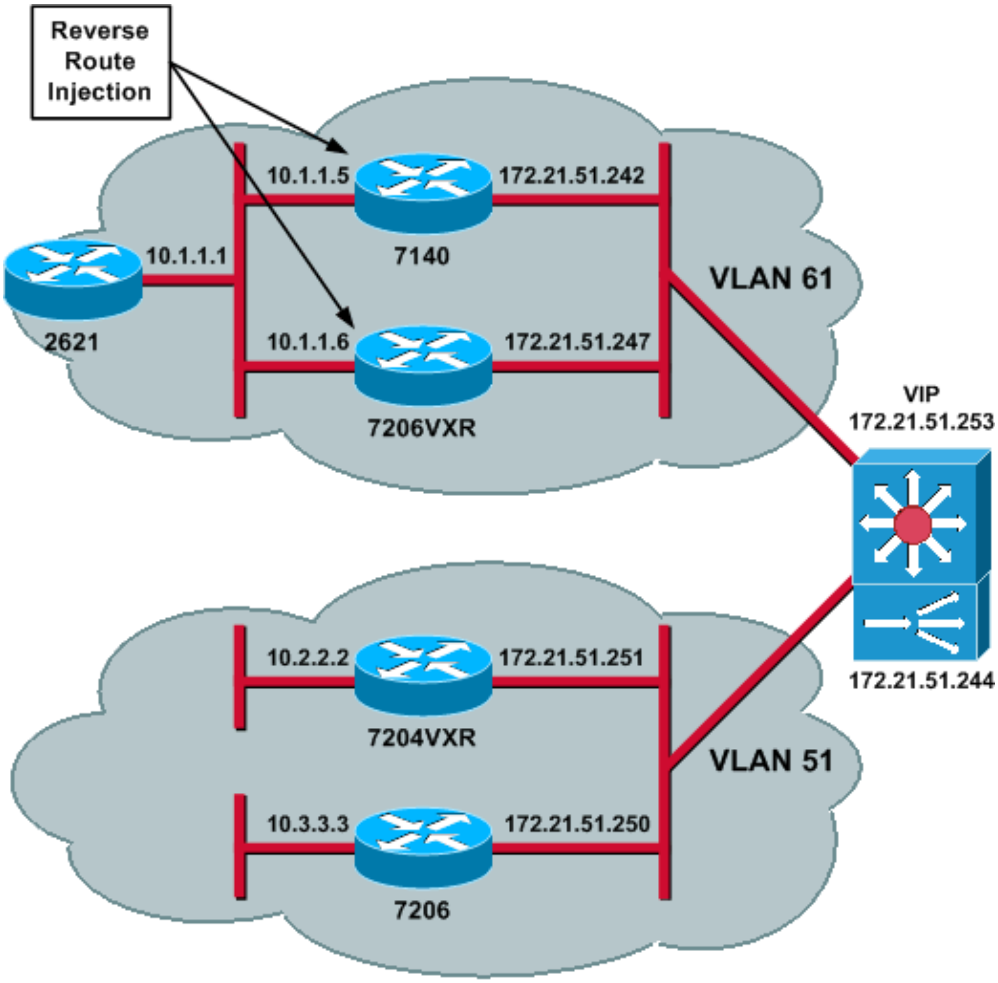
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- CSM Configuration

- Head−End Router Configuration − 7206VXR
- Spoke Router Configuration − 7206

CSM Configuration

Complete these steps:

1. Implement RRI at the head−end devices, to propagate the routing information from the spokes automatically.

   Note: VLAN 61 and VLAN 51 share the same subnet.
2. Define the VLAN client and the VLAN server.
3. Define the probe used to check the health of the IPSec servers.

   ```
   !--- 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. Define the **serverfarm** with the real IPSec servers.
5. Configure **failaction purge**, to flush the connections that belong to dead servers.
6. Define the sticky policy.

   ```
   !--- 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. Define VServers, one per traffic flow.

```
      !−−− 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
      !
```

Head−End Router Configuration − 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
!
```

Spoke Router Configuration − 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
!
```

Verify

Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- Issue the **show module csm all** or **show module contentSwitchingModule all** command; both commands generate the same information.

  The **show module contentSwitchingModule all vservers** command shows the SLB virtual server information.

  ```
  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
  ```

  The **show module contentSwitchingModule all conns** command shows SLB connection information.

  ```
  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
```

The **show module contentSwitchingModule all sticky** command shows the SLB sticky database.

```
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
```

- Issue the **show ip route** command on the 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

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **VPN Load Balancing on the CSM in Dispatched Mode Configuration Example**
- **Catalyst 6500 Series Switch Content Switching Module Command Reference, 4.1(2)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Nov 30, 2005 Document ID: 63390