VPN Load Balancing on the CSM in Dispatched Mode Configuration Example

Contents

- Introduction
- Before You Begin
  - Requirements
  - Components Used
  - Conventions
- Configurations Tasks
  - Network Diagram
  - CSM Configuration - Dispatched Mode
  - Head-End Router Configuration - Dispatch Mode
  - Spoke Router Configuration - Dispatch Mode
- Verify
- Troubleshoot
- Related Information

Introduction

This document provides a sample configuration for configuring VPN load balancing on the Content Switching Module (CSM) in dispatched mode. 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 to:

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

Before You Begin

Requirements

Before attempting this configuration, ensure that you meet these requirements:

- Both hub routers are configured with the same loopback IP address (VIP).
- Reverse Route Injection (RRI) is implemented at the head-end routers.
- Use Authentication Headers (AH).

Components Used

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

- Cisco 7140 and 7206
- Cisco 7206VXR and 7204VXR
- Cisco Catalyst 6500 CSM

Conventions

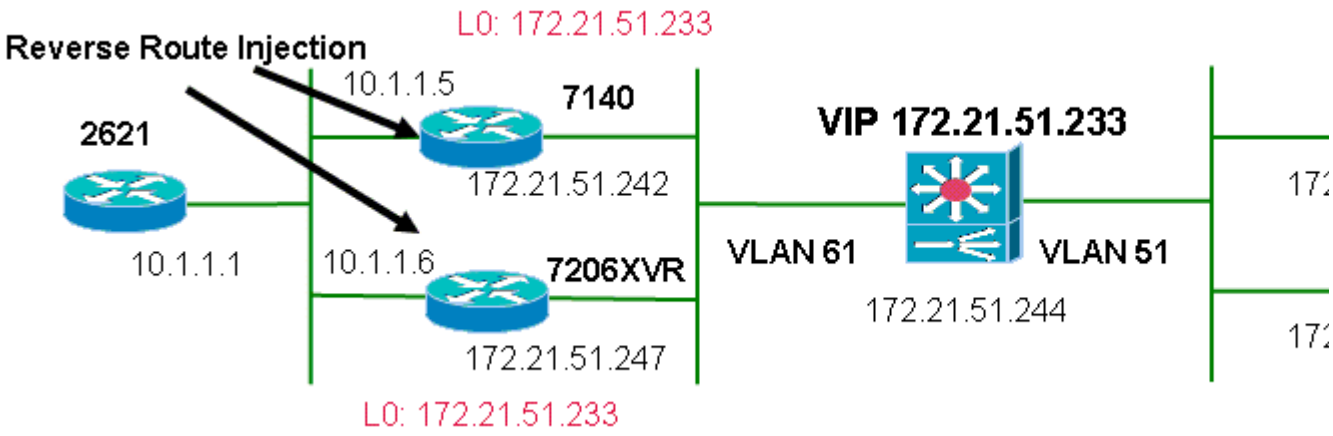
For more information on document conventions, refer to Cisco Technical Tips Conventions.

Configurations Tasks

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

Network Diagram

This document uses this network setup:



CSM Configuration - Dispatched Mode

Complete these steps.

1. Define the VLAN client and the VLAN server.

2. Define the probe used to check the health of the IPSec servers. Use the **module csm** or **module contentSwitchingModule** command; both generate the same information.

```
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. Define the severfarm with the real IPSec servers

4. Issue the **no nat server** command to indicate dispatch mode.

5. Indicate **failaction purge** to flush the connections belonging to dead servers.

6. Define the sticky policy.

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

```
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
    !
```

Head-End Router Configuration - Dispatch Mode

```
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
```

Spoke Router Configuration - Dispatch Mode

```
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
!
```

Verify

This section provides information you can use to confirm your configuration is working properly.

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

```
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
```

Troubleshoot

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

Related Information

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