

VPN负载均衡在分派模式的CSM配置示例

目录

[简介](#)

[开始使用前](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置任务](#)

[网络图](#)

[CSM配置-分派模式](#)

[数据转发路由器配置-分派模式](#)

[分支路由器配置-分派模式](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文为配置VPN负载均衡提供一配置示例在分派模式的内容交换模块(CSM)。VPN负载均衡是智能分配沿一套的VPN会话VPN集中器或VPN数据转发设备的机制。VPN负载均衡实现对：

- 解决在VPN设备，例如，数据包每秒，连接每秒和吞吐量的性能/可扩展性限制。
- 提供冗余(删除单点故障)。

开始使用前

要求

在尝试此配置前，请保证您符合这些要求：

- 两中心路由器配置与同样环回IP地址(VIP)。
- 反向路由注入(RRI)实现在数据转发路由器。
- 请使用认证报头(AH)。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- Cisco 7140和7206
- Cisco 7206VXR和7204VXR

- 思科Catalyst 6500 CSM

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

配置任务

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：

CSM配置-分派模式

完成下面这些步骤。

1. 定义VLAN客户端和VLAN服务器。
2. 定义用于的探测器检查IPSec服务器的健康。请使用**模块csm**或**模块contentSwitchingModule**命令;两个生成同一信息。

```
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. 定义serverfarm用实时IPSec服务器
4. 发出**no nat server**命令指示分派模式。
5. 指示**failaction**清除冲洗属于死机服务器的连接。
6. 定义粘贴策略。

```
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. 定义Vserver，一个每通信流。

```
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
!
```

数据转发路由器配置-分派模式

```
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
```

分支路由器配置-分派模式

```
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
!

```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

发出**show module csm全部**或**show module contentSwitchingModule all命令**;两命令生成同一信息。

```

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 ... 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 ... 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

```

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- [VPN负载均衡在定向模式的CSM配置示例的](#)
- [技术支持 - Cisco Systems](#)