Exemple de configuration d'équilibrage de charge VPN sur le CSM en mode distribué

Contenu

Introduction
Avant de commencer
Conditions requises
Composants utilisés
Conventions
Tâches de configurations
Diagramme du réseau
Configuration CSM - Mode acheminé
Configuration de routeur de tête de réseau - Mode de répartition
Configuration de routeur en étoile - Mode de répartition
Vérifiez
Dépannez
Informations connexes

Introduction

Ce document fournit une configuration d'échantillon pour configurer l'Équilibrage de charge VPN sur le module de commutation de contenu (CSM) en mode acheminé. L'Équilibrage de charge VPN est un mécanisme qui distribue intelligemment des sessions VPN le long d'un ensemble de périphériques de concentrateurs VPN ou de tête de réseau VPN. L'Équilibrage de charge VPN est mis en application à :

- surmontez les limites de représentation/évolutivité sur des périphériques VPN, par exemple, des paquets par seconde, des connexions par seconde, et le débit.
- fournissez la Redondance (enlevez le point de défaillance unique).

Avant de commencer

Conditions requises

Avant de tenter cette configuration, assurez-vous que vous répondez à ces exigences :

- Les deux routeurs concentrateur sont configurés avec la même adresse IP de bouclage (VIP).
- L'Injection inversée de routes (RRI) est mis en application aux routeurs de tête de réseau.
- En-têtes d'authentification d'utilisation (OH).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Tâches de configurations

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configuration CSM - Mode acheminé

Procédez comme suit :

1. Définissez le client VLAN et le serveur VLAN.
2. Définissez la sonde utilisée pour vérifier les santés des serveurs d'IPSec. Utilisez le **module csm** ou la commande de **contentSwitchingModule de module** ; chacun des deux génèrent les mêmes informations.

```
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. Définissez le severfarm avec les vrais serveurs d'IPSec
4. N'émettez l'**aucun** ordre **nat de serveur** d'indiquer le mode de répartition.
5. Indiquez la **purge de failaction** pour vider les connexions appartenant aux serveurs morts.
6. Définissez la stratégie Rémanente.

```
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. Définissez VServers, un par circulation.

```
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
!
```

Configuration de routeur de tête de réseau - Mode de répartition

```
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
```

Configuration de routeur en étoile - Mode de répartition

```
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
!
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Émettez le **show module csm tout** ou le **contentSwitchingModule de show module toute la** commande ; les deux commandes génèrent les mêmes informations.

```
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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Exemple de configuration d'équilibrage de charge VPN sur le CSM en mode dirigé
- Support technique - Cisco Systems