

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

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

## [Introduction](#)

Ce document fournit un exemple de configuration pour l'équilibrage de charge VPN sur un module de commutation de contenu (CSM). L'équilibrage de charge VPN est un mécanisme qui distribue intelligemment les sessions VPN le long d'un ensemble de concentrateurs VPN ou de périphériques tête de réseau VPN. L'équilibrage de charge VPN est mis en oeuvre pour les raisons suivantes :

- pour surmonter les limitations de performances ou d'évolutivité sur les périphériques VPN ; par exemple, les paquets par seconde, les connexions par seconde et le débit
- Pour fournir une redondance (supprimer un point de défaillance unique)

## [Conditions préalables](#)

### [Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Implémenter l'injection de route inverse (RRI) au niveau des périphériques de tête de réseau, pour propager automatiquement les informations de routage à partir des rayons.
- Activez les VLAN 61 et 51 pour partager le même sous-réseau.

### [Components Used](#)

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

logiciel suivantes :

- Cisco Catalyst 6500 avec CSM
- Routeur Cisco 2621
- 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](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

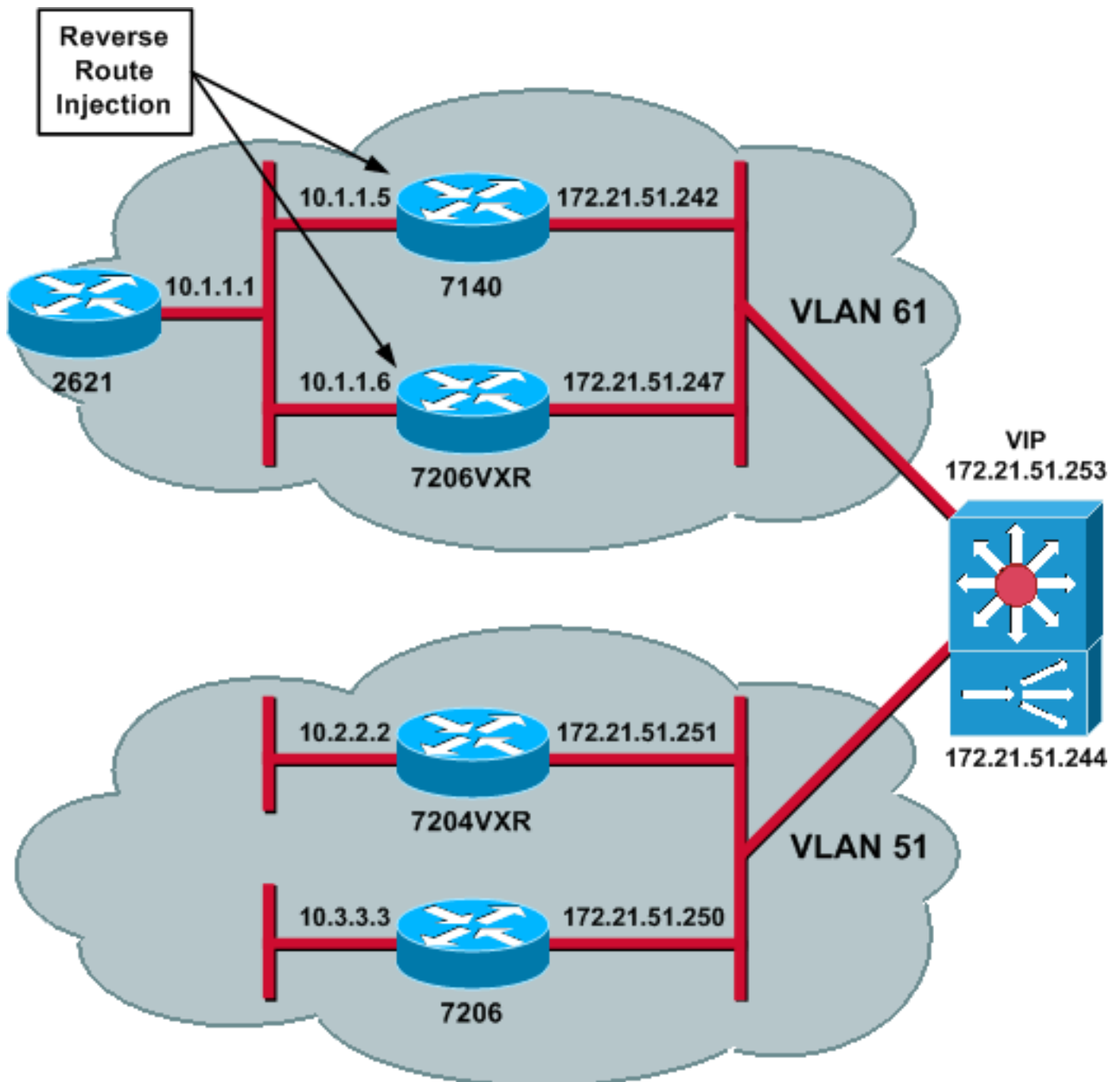
## [Configuration](#)

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

**Remarque** : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

## [Diagramme du réseau](#)

Ce document utilise la configuration réseau suivante :



## Configurations

Ce document utilise les configurations suivantes :

- [Configuration CSM](#)
- [Configuration du routeur principal - 7206VXR](#)
- [Configuration du routeur satellite - 7206](#)

## Configuration CSM

Procédez comme suit :

1. Implémentez RRI au niveau des périphériques de tête de réseau, pour propager automatiquement les informations de routage à partir des rayons. **Remarque** : VLAN 61 et VLAN 51 partagent le même sous-réseau.

2. Définissez le client VLAN et le serveur VLAN.
3. Définissez la sonde utilisée pour vérifier l'état des serveurs IPSec.

```
!--- 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. Définissez la **batterie de serveurs** avec les vrais serveurs IPSec.
5. Configurez la **purge des échecs**, pour vider les connexions qui appartiennent aux serveurs morts.
6. Définissez la politique rémanente.

```
!--- 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. Définissez VServers, un par flux de trafic.

```
!--- 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 !
```

## Configuration du routeur principal - 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
!

```

## Configuration du routeur satellite - 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
!

```

## Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

[L'Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show.](#) Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- Émettez la commande **show module csm all** ou **show module contentSwitchingModule all** ; les deux commandes génèrent les mêmes informations. La commande **show module contentSwitchingModule all vservers** affiche les informations du serveur virtuel SLB.

```
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

```

La commande **show module contentSwitchingModule all conns** affiche les informations de connexion SLB.

```
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

```

La commande **show module contentSwitchingModule all sticky** affiche la base de données sticky SLB.

```
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

```

- Exécutez la commande **show ip route** sur le routeur.

```

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

```

## Dépannage

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 distribué](#)
- [Guide de référence des commandes du module de commutation de contenu des commutateurs de la gamme Catalyst 6500, 4.1\(2\)](#)
- [Support et documentation techniques - Cisco Systems](#)