

# Exemple de configuration de mise en cache transparente avec le module de commutation de contenu

## Contenu

[Introduction](#)

[Avant de commencer](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

## [Introduction](#)

Ce document fournit une configuration d'échantillon pour la mise en cache transparente utilisant les moteurs de cache de Cisco et le module de commutation de contenu (CSM). La mise en cache transparente est la technique utilisée d'une manière transparente pour intercepter le trafic de l'un navigateur Web et pour le réorienter à un périphérique de cache pour récupérer le contenu qui a été précédemment caché.

Une autre méthode pour faire la mise en cache transparente est Protocole WCCP (Web Cache Communications Protocol). L'avantage de la mise en cache transparente au-dessus du WCCP est que le CSM regarde l'URL demandé par le client et décide si le trafic est envoyé dans le cache ou pas. Des demandes des fichiers statiques tels que des images GIF ou JPEG sont récupérées du cache, alors que les pages dynamiques (résultat d'un script) sont récupérées directement du serveur sans aller dans le cache.

## [Avant de commencer](#)

### [Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

### [Composants utilisés](#)

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

- Version 3.x CSM
- Version 5.1 du logiciel réseau de Réseau de diffusion de contenu d'application (ACNS)

## Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

## Configurez

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

## Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :

## Configurations

Ce document utilise la configuration suivante :

```
module ContentSwitchingModule 4 vlan 501 server ip address 192.168.30.97 255.255.254.0 ! vlan
499 client ip address 192.168.10.97 255.255.254.0 gateway 192.168.10.1 ! vlan 500 server ip
address 192.168.20.97 255.255.254.0 ! serverfarm CACHES no nat server !--- This is a transparent
redirect; do not change the destination IP address. no nat client predictor hash url !--- Use
URL hashing to make sure the request for a specific URL always goes to the same server. real
192.168.30.200 inservice real 192.168.30.201 inservice ! serverfarm FORWARD no nat server no nat
client predictor forward !--- This serverfarm tells the CSM not to load balance. !--- The CSM
instead uses its routing table to forward the traffic. ! map CACHEABLE url !--- In this example,
you want to only redirect requests for certain file types. !--- This is not mandatory. !--- You
can also adjust this to something more realistic. match protocol http url *.html match protocol
http url *.gif match protocol http url *.jpg match protocol http url *.exe match protocol http
url *.zip ! policy CACHEABLE !--- The policy is the way to link the map with a serverfarm. url-
map CACHEABLE serverfarm CACHES ! vserver FROMCACHE !--- This rule is for traffic originating
from the caches (when they have !--- to retrieve content from the origin server). virtual
0.0.0.0 0.0.0.0 any vlan 501 !--- The VLAN command guarantees that you limit this vserver to the
cache VLAN. serverfarm FORWARD !--- Use the serverfarm FORWARD command to disable load balancing
for this traffic. !--- In this example, you need forward requests from the caches to the origin
server. !--- You could, however, load balance this traffic to a series of Web servers, that is,
!--- when doing reverse proxy caching. persistent rebalance inservice ! vserver INTERCEPT !---
This is the rule to transparently redirect requests from the client to the caches. virtual
0.0.0.0 0.0.0.0 tcp www vlan 499 serverfarm FORWARD !--- The default action is forward; no load
balancing. !--- This is for requests that do not match the policy. persistent rebalance slb-
policy CACHEABLE !--- Traffic matching the policy is load balanced to the caches. inservice !
vserver NONHTTP !--- Non-HTTP traffic from the clients is forwarded. virtual 0.0.0.0 0.0.0.0 any
vlan 499 serverfarm FORWARD persistent rebalance inservice !
```

## Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre

configuration fonctionne correctement.

- affichez le détail de *nom de nom de vserver* modèle *csM X*
- affichez le détail de *conns* modèle *csM X*

```
EOMER#show mod csm 4 vser name intercept det INTERCEPT, type = SLB, state = OPERATIONAL, v_index = 22 virtual = 0.0.0.0/0:80 bidir, TCP, service = NONE, advertise = FALSE idle = 3600, replicate csrp = none, vlan = 499, pending = 30, layer 4 max parse len = 2000, persist rebalance = TRUE ssl sticky offset = 0, length = 32 conns = 0, total conns = 3 Default policy: server farm = FORWARD, backup = <not assigned> sticky: timer = 0, subnet = 0.0.0.0, group id = 0 Policy Tot matches Client pkts Server pkts ----- CACHEABLE 2 410 926 (default) 5 20 17
```

Vérifiez que le trafic a apparié la stratégie (le trafic réorienté dans les caches), ou si le trafic était expédié (correspondance sur la stratégie par défaut).

```
EOMER#show mod csm 4 conn det prot vlan source destination state -----
----- In ICMP 499 192.168.11.41 192.168.21.4 ESTAB Out ICMP
500 192.168.21.4 192.168.11.41 ESTAB vs = NONHTTP, ftp = No, csrp = False In ICMP 501
192.168.10.107 10.48.66.102 ESTAB Out ICMP 499 10.48.66.102 192.168.10.107 ESTAB vs = FROMCACHE,
ftp = No, csrp = False In TCP 499 192.168.11.41:4402 192.168.21.4:80 REQ_WAIT Out TCP 501
192.168.21.4:80 192.168.11.41:4402 REQ_WAIT vs = INTERCEPT, ftp = No, csrp = False In TCP 501
192.168.11.41:32784 192.168.21.4:80 ESTAB Out TCP 500 192.168.21.4:80 192.168.11.41:32784 ESTAB
vs = FROMCACHE, ftp = No, csrp = False
```

Le cache a été configuré pour l'usurpation d'adresse IP. Vous pouvez voir dans la sortie au-dessus de cela il y a une connexion de client 192.168.11.41 au serveur 192.168.21.4 vu sur VLAN 499, et une connexion semblable vue sur VLAN 501. Le premier est la vraie connexion du client qui a été réorienté dans le cache (la sortie VLAN est 501), et le second est la connexion du cache (adresse IP de client de mystification) au serveur d'origine.

## [Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

## [Informations connexes](#)

- [Configuration du mode \(routeur\) sécurisé sur le module de commutation de contenu](#)
- [Support matériel de module de commutation de contenu](#)
- [Cat de Cisco 6000 l'autre téléchargement de SW de module intelligent \(clients enregistrés seulement\)](#)
- [Support et documentation techniques - Cisco Systems](#)