Cache transparente com o exemplo de configuração do módulo content switching

Índice

Introdução

Este documento fornece uma configuração de exemplo para o cache transparente usando os motores do Cisco Cache e o módulo content switching (CS). O cache transparente é a técnica usada para interceptar o tráfego do um navegador da Web e para reorientá-lo transparentemente a um dispositivo do esconderijo para recuperar o índice que foi posto em esconderijo previamente.

Um outro método para fazer o cache transparente é Web Cache Communications Protocol (WCCP). A vantagem do cache transparente sobre o WCCP é que o CS olha a URL pedida pelo cliente e decide se o tráfego for enviado ao esconderijo ou não. Os pedidos para arquivos estáticos tais como imagens GIF ou JPEG estão recuperados do esconderijo, quando as páginas dinâmicas (resultado de um script) forem recuperadas diretamente do server sem ir ao esconderijo.

Antes de Começar

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas seguintes versões de hardware e software:

- Versão de CSM 3.x
- Versão 5.1 do Content Networking Software do aplicativo (ACNS)

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.

Configurações

Este documento utiliza esta configuração:

```
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 !
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

- mostre o detalhe do *nome do* nome do vserver modificação csm X

- mostre o detalhe dos conns modificação 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
```

Verifique que o tráfego combinou a política (tráfego reorientado aos esconderijos), ou se o tráfego foi enviado (fósforo na política padrão).

```
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
```

O esconderijo foi configurado para a falsificação de IP. Você pode ver na saída acima daquele lá é uma conexão do cliente 192.168.11.41 ao server 192.168.21.4 visto em VLAN 499, e uma conexão similar vista em VLAN 501. Primeiro é a conexão real do cliente que foi reorientado ao esconderijo (a saída VLAN é 501), e segundo é a conexão do esconderijo (endereço IP cliente da falsificação) ao servidor de origem.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Informações Relacionadas

- Configurando o modo seguro (do roteador) no módulo content switching
- Suporte a hardware do módulo content switching
- Cat 6000 de Cisco a outra transferência do módulo inteligente SW (clientes registrados somente)
- Suporte Técnico e Documentação - Cisco Systems