Almacenamiento en memoria caché transparente con el ejemplo de configuración del módulo content switching

Contenido

Introducción

Este documento proporciona una configuración de muestra para el Almacenamiento en memoria caché transparente usando los motores y el módulo content switching (CS) del Cisco Cache. El Almacenamiento en memoria caché transparente es la técnica usada transparente para interceptar el tráfico del un buscador Web y para reorientarlo a un dispositivo del caché para extraer el contenido que fue ocultado previamente.

Otro método para hacer el Almacenamiento en memoria caché transparente es Web Cache Communications Protocol (WCCP). La ventaja del Almacenamiento en memoria caché transparente sobre el WCCP es que el CS mira el URL pedido por el cliente y decide a si el tráfico se envía al caché o no. Las peticiones los archivos estáticos tales como GIF o las imágenes jpeges se extraen del caché, mientras que las páginas dinámicas (resultado de un script) se extraen directamente del servidor sin ir al caché.

Antes de comenzar

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- CSM versión 3.x
- Versión 5.1 del Content Networking Software de la aplicación (ACNS)

Convenciones

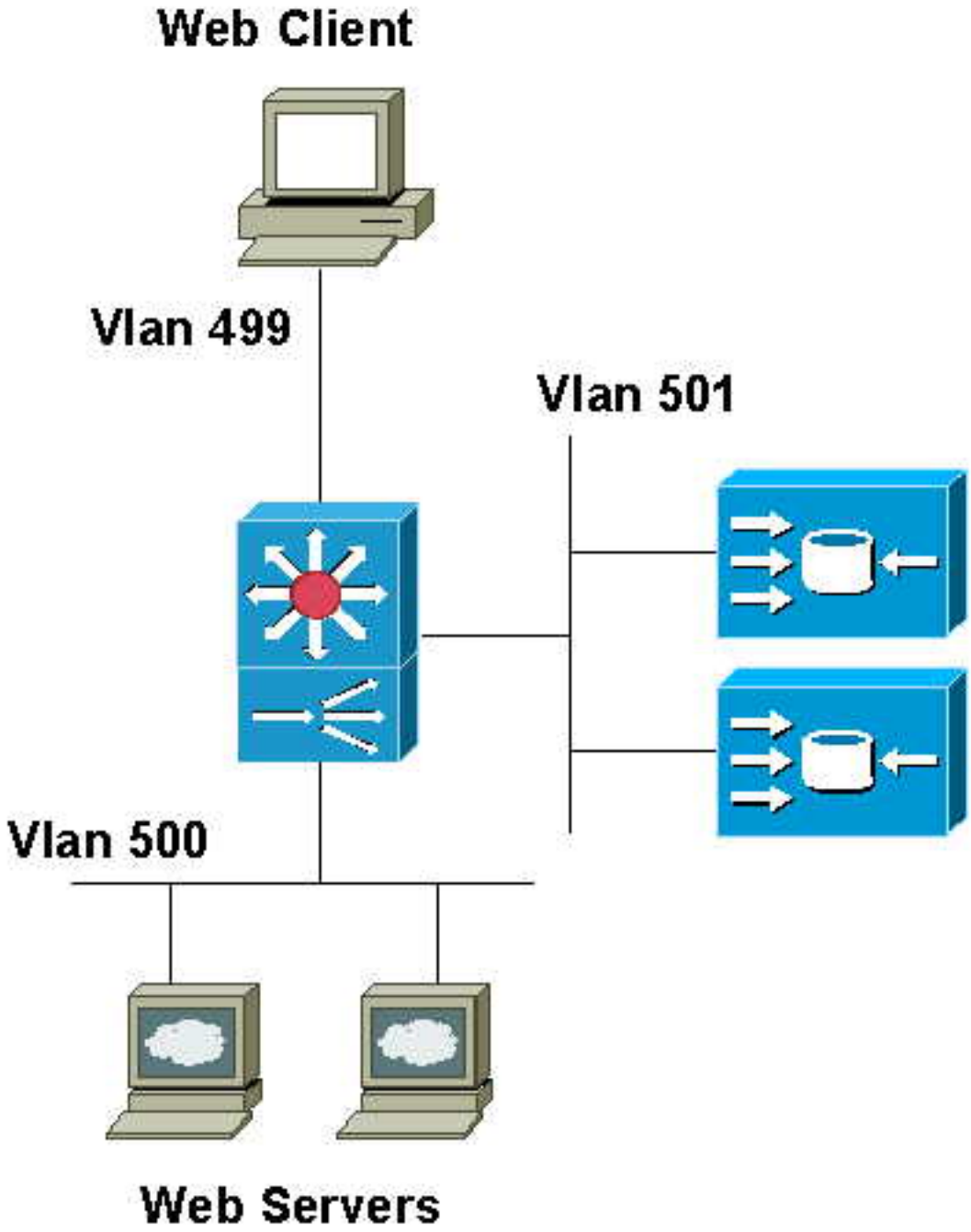
Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa esta configuración:

```
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 !
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

- **muestre el detalle del** *nombre del* **nombre del vserver Mod csm X**
- **muestre el detalle del conns Mod 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 el tráfico correspondiera con la directiva (tráfico reorientado a los cachés), o si el tráfico fue remitido (coincidencia en la política predeterminada).

```
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
```

El caché fue configurado para el IP spoofing. Usted puede ver en la salida sobre eso allí es una conexión del cliente 192.168.11.41 al servidor 192.168.21.4 visto en el VLA N 499, y una conexión similar vista en el VLA N 501. Primer es la conexión real del cliente que fue reorientado al caché (el VLA N de la salida es 501), y segundo es la conexión del caché (dirección IP del cliente del spoofing) al servidor de origen.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Información Relacionada

- Configurar el modo seguro (del router) en el módulo content switching

- Soporte del hardware del módulo content switching
- Cat6000 de Cisco la otra descarga del módulo inteligente SW (clientes registrados solamente)
- Soporte Técnico y Documentación - Cisco Systems