

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de muestra para los Productos y las aplicaciones de Web CSS 11xxx para mantener a un cliente pegado al mismo servidor, si usted utiliza el HTTP o el SSL.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Entienda los fundamentos del HTTP y del SSL.
- Tenga conocimiento sobre los Productos y las aplicaciones de Web CSS 11xxx.

[Componentes Utilizados](#)

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

- Software Release 5.00 y Posterior de Cisco WebNS
- Todos los Content Services Switches de las 11xxx Series del Cisco CSS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las

convenciones sobre documentos.

Antecedentes

Muchos Web site tienen los clientes ingresar su sitio con la ayuda del puerto 80 del Hypertext Transfer Protocol (HTTP), pero quieren a los clientes a la transición al protocolo del Secure Socket Layer (SSL) durante la sesión para las transacciones seguras. Aquí está una manera de mantener a un cliente pegado al mismo servidor, si usted utiliza el HTTP o el SSL.

El tráfico HTTP de los pedidos de cliente destinado al IP virtual (VIP). El switch toma una decisión de equilibrio de carga. En este documento, el tráfico va al s1 del servidor. Entonces pegan al cliente al s1 del servidor basado en uno de los métodos de la avance-balanza, tales como Sticky-srip, Sticky-srcip-dstport, y Cookie. Refiera a [configurar los parámetros fijos para las reglas de contenido](#) para más información.

Durante la sesión del cliente, la transición se hace al puerto SSL 443 cuando el cliente selecciona un link en la página que reorienta al https. Esto ocasiona que se elija una nueva regla de contenido y es posible que se desvíe al cliente a otro servidor por equilibrio de carga. Pues el tráfico ahora es el https cifrado (SSL/TLS), el CSS no puede marcar sobre la capa 4 (el número del puerto TCP) para los Cookie, URL etc., porque se cifran las peticiones cuando la información pasa el CSS. Para prevenir el acontecimiento de este problema, configure el HREF de reorientación en cada servidor para señalar de nuevo al https en la misma dirección pública de los servidores, no el direccionamiento VIP, como se muestra aquí:

Si sus servidores están en un espacio de dirección privada, configure las reglas de contenido SSL para cada servidor con un HREF en cada servidor esas puntas a las reglas de contenido VIP SSL.

Usted puede también necesitar hacer algunas modificaciones a las configuraciones de las aplicaciones de Web en el s1 asegurado y el s2 de los servidores.

También una regla de contenido con un conjunto de la configuración fija a las cookies de equilibrio avanzado requiere a todos los clientes habilitar los Cookie en su navegador.

Configurar

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

Nota: Utilice la herramienta [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos utilizados en esta sección.

Configuraciones

Este documento usa esta configuración:

- CSS11XXX con WebNS 5.00 y posterior - Configuración corriente

CSS11XXX con WebNS 5.00 y posterior - Configuración corriente
--

!Generated on 10/10/2001 18:12:17 !Active version:
--

```

ap0500015s configure !*****
SERVICE***** service s1 ip
address 10.10.1.101 active service s2 ip
address 10.10.1.102 active
!*****
OWNER***** owner cookie-ssl
content layer5cookie vip address 10.10.1.66
protocol tcp port 80 url "/"
advanced-balance arrowpoint-cookie !--- Specify a
port in the content rule to use this option. !--- Port
80 traffic is used here. !--- All clients must enable
cookies on their browser. add service s1
add service s2 active content s1-ssl
vip address 10.10.1.88 protocol tcp port
443 application ssl add service s1
active content s2-ssl vip address 10.10.1.99
protocol tcp port 443 application
ssl add service s2 active !--- Use this
HREF on server S1 where switching from http to https:
<A HREF="https://10.10.1.101/applicationpath1/"> secure
site s1 </A> !--- Use this HREF on server S2 where
switching from http to https: <A
HREF="https://10.10.1.102/applicationpath2"> secure site
s2 </A> !--- In the example, the addresses for servers
s1 and s2 must be !--- reachable from the client. If
this is not the case, you must add a !--- content rule
for each server with a unique publicly routable VIP !---
address and one service for each SSL server, as shown
here: content s1-ssl vip address 10.10.1.88 protocol tcp
port 443 application ssl add service s1 active content
s2-ssl vip address 10.10.1.99 protocol tcp port 443
application ssl add service s2 active!--- Use this HREF
on server s1 where the switch from http to https occurs:
<A HREF=https://10.10.1.88/applicationpath1/> secure
site s1 </A> !--- Use this HREF on server s2 where the
switch from http to https occurs: <A
HREF=https://10.10.1.99/applicationpath2> secure site s2
</A>

```

[Verificación](#)

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

[Troubleshooting](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

[Información Relacionada](#)

- [Página de soporte al producto Cisco CSS de la serie 11000](#)
- [Configuración de Parámetros fijos para reglas de contenido](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)