Contenido

Introducción

Este documento proporciona una configuración de muestra para la característica del urlrewrite del Acelerador de contenido seguro (SCA). El SCA ofrece una fácil solución para emigrar de los servidores Web tradicional con el HTTP a los servidores del contenido seguro con HTTP seguro (HTTPS).

La inserción del SCA delante del servidor HTTP permite al SCA para realizar todas las funciones seguras necesarias cifrar el documento HTML. El SCA es transparente a los clientes y servidores.

El propósito de este documento es mostrar cómo la función del urlrewrite puede sobregrabar algunos links a un documento HTTP con un link al mismo documento vía el HTTPS. Esta característica es útil cuando usted quiere estar seguro que un usuario que conecta con su servidor vía el HTTPS con el SCA no reorienta a un documento nonsecure (HTTP).

prerrequisitos

Requisitos

Antes de que usted intente esta configuración, asegúrese de que usted entienda estos conceptos:

- Content Services Switch (CSS) y configuración básica SCA
- HTTP y protocolos HTTP

Componentes Utilizados

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

- Cisco CSS 11000 o CSS11500 que funcionan con cualquier versión de software de Cisco WebNS
- Cisco SCA o SCA2 que ejecutan 3.2.x o 4.x

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

Convenciones

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

Teoría Precedente

La sintaxis del comando es la siguiente:

- *Domain Name del* **urlrewrite [sslport portid] [clearport portid]** *redirectonly*

Cuando usted ha configurado el **comando urlrewrite**, el SCA puede examinar la respuesta completa HTML para substituir todos los links a un documento nonsecure con un link al mismo documento vía el HTTPS. Por ejemplo, si el documento HTML contiene *e* <A HREF= " **http://mycompany.com/images/index.html** " >images</A>, el SCA la substituye por <A HREF= " **https://mycompany.com/images/index.html** " >images</A>.

El SCA puede examinar la encabezado solamente, en vez del documento completo HTML, y substituye el URL que está presente en la `ubicación:` campo. El ejemplo abajo muestra la `ubicación:` coloque y el URL esas puntas a una página nonsecure. Especifique la **opción de sólo redirección** para que el SCA substituya solamente el URL en la `ubicación:` campo.

Configurar

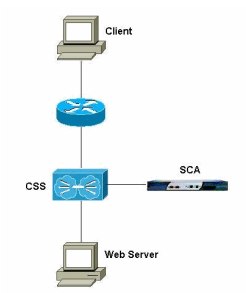
Esta sección presenta la información para configurar las características que este documento describe.

La configuración de su servidor debe ser reorientar a los usuarios a http://tension.mycompany.com:70. La configuración de SCA, es por consiguiente interceptar la ubicación de campo del encabezado, http://tension.mycompany.com:70, y lo substituye por https://tension.mycompany.com.

Nota: Para encontrar la información adicional en los comandos en este documento, utilice la herramienta de búsqueda de comandos (clientes registrados solamente).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

- SCA
- CSS

SCA

```
sca# show running-configuration ## Cisco SCA Device
Configuration File## Written:      Sun Jun 20 17:56:41 1970
MDT# Inxcfg:       version 3.2 build 200204302030# Device
Type:  CSS-SCA# Device Id:    S/N 118140# Device OS:    MaxOS
version 3.2.0 build 200204302029 by reading### Mode ###mode
one-port### Interfaces ###interface network  autoendinterface
server  autoend### Device ###ip address 192.168.1.2 netmask
255.255.255.0hostname scatimezone "MST7MDT"### Password
###password access
"2431244C362461476C67654D485269494C4634772E586A374E39472F"pas
sword enable
"2431246E6324386D437A6E714B44567174306565386A775566536931"###
SNTP ###sntp interval 86400### Static Routes ###ip route
0.0.0.0 0.0.0.0 192.168.1.1 metric 1!--- The default route
points to the CSS.### RIP ###rip### DNS ###ip name-server
10.10.10.1ip domain-name mycompany.com### Remote Management
###no remote-management access-listremote-management
enable### Telnet ###telnet enable### Web Management ###web-
mgmt port 80web-mgmt enable### SNMP Subsystem ###no snmp###
SSL Subsystem ###ssl!--- This is the certificate definition.
cert my-cert createbinhex
579=3082023f308201c9a003020102020100300d06092a864886f70d01010
4050030=8187311a3018060355040313116764756666f75722e636973636f2
e636f6d310b=300906035504061302555310b300906035504081302434f3
10f300d06035504=07130644656e766572310f300d060355040a130654414
32d6d65310b30090603=55040b130243413120301e06092a864886f70d010
9011611676475666f757240=636973636f2e636f6d301e170d30333031333
03037303030305a170d30343031=33303037303030305a308187311a30180
603550403131167647566f75722e63=6973636f2e636f6d310b300906035
5040613025553310b300906035504081302=434f310f300d0603550407130
644656e766572310f300d060355040a13065441=432d6d65310b300906035
5040b130243413120301e06092a864886f70d010901=1611676475666f757
240636973636f2e636f6d307c300d06092a864886f70d01=01010500036b0
03068026100aff358226467ed77f0278750048557de683291af=47fceb89f
40572e7d312623581a1d9f9a3d2087cbaeb2e30c402676a7f8c7a6b=02dc8
9e45d40d799d38ac93a20fa054809b2692b24bc3742285396c8b91a66e1=8
52aa9a23d6b1da0a9508385020301000130 0d06092a864886f70d01010405
00=0361006fc579e08b00d5981c7d30f2d6219cb90ac0c203918ae2e96169
7de7bf=85e57fbc0db3fa8a73e48bde1127926b780f127abfe7cd13283c8a
d4d45f0178=b8fb2e3aba62622f8127ee1fd840b0738120fc38cf745d72c1
79331913b1e87b=f4d3b4end!--- This is the web server
configuration. server webserver create ip address
10.48.67.1!--- This is the server IP address. localport 443!-
-- This is the localport on which the CSS accepts connection.
remoteport 81 !--- This is the port to which the SCA connects
with the server. !--- The configuration of the CSS is to
intercept connection to this port !--- and load balance over
the different servers. !--- This example uses only one
server. key MyKey cert my-cert secpolicy default session-
cache size 20480 session-cache timeout 300 session-cache
enable no transparent no clientauth enable clientauth
verifydepth 1 clientauth error cert-other-error fail
clientauth error cert-not-provided fail clientauth error
```

```
cert-has-expired fail clientauth error cert-not-yet-valid
fail clientauth error cert-has-invalid-ca fail clientauth
error cert-has-signature-failure fail clientauth error cert-
revoked fail certgroup clientauth defaultCA no httpheader
client-cert no httpheader server-cert no httpheader session
no httpheader pre-filter httpheader prefix "SSL" ephrsa
urlrewrite tension.mycompany.com clearport 70 redirectonly!--
- This is the urlrewrite command. !--- This command matches
the http://tension.mycompany.com:70 location !--- and
replaces it with the https://tension.mycompany.com location.
!--- The redirectonly keyword indicates that the only !---
rewrite should be in the "Location:" field in the HTTP 30x
redirect header. !--- Without the redirectonly keyword, all
references to !--- http://tension.mycompany.com:70 in the
server answer convert to HTTPS.  endendsca#
```

CSS

```
 css# show running-config !Generated on 02/04/2003
13:31:17!Active version:
ap0503026sconfigure!************************** GLOBAL
**************************  dns primary 144.254.6.77   dns
suffix cisco.com.   ip route 0.0.0.0 0.0.0.0 192.168.1.2 1
ip route 0.0.0.0 0.0.0.0 192.168.150.2 1 !--- These are two
default routes. !--- The transparent design requires these
routes. !--- Refer to the !--- Cisco CSS 11000 Secure Content
Accelerator Configuration Guide Index !--- for more
information. ip route 144.254.0.0 255.255.0.0 10.48.66.1 1
!************************* INTERFACE
*************************interface e2 bridge vlan 149
interface e3 bridge vlan 161 !*************************
CIRCUIT **************************circuit VLAN1 ip address
10.48.66.6 255.255.254.0 !--- This is the servers
VLAN.circuit VLAN149 ip address 192.168.1.1 255.255.255.0 !--
- This is the SCA VLAN.circuit VLAN161 ip address
192.168.150.1 255.255.255.0 !--- This is the clients
VLAN.!************************** SERVICE
**************************service SSL1 ip address 192.168.1.2
active !--- This is the definition of the SCA.service tension
ip address 10.48.66.123 protocol tcp port 80 active !--- This
is the definition of the web
server.!************************** OWNER
**************************owner MyCompany content SSL !---
This is the SSL rule to intercept HTTPS traffic !--- and
forward it to the SCA. protocol tcp vip address 10.48.67.1
add service SSL1 port 443 active content SSL2WWW !--- This is
decrypted traffic from the SCA to the !--- HTTP web server.
vip address 10.48.67.1 protocol tcp port 81 add service
tension active content WWW !--- This part of the
configuration allows you access !--- to the server in
nonsecure mode, if desired. vip address 10.48.67.1 protocol
tcp port 80 add service tension active CSS#
```

Verificación

En esta sección encontrará información que puede utilizar para comprobar que su configuración funcione correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) proporciona los **comandos show del** soporte con certeza. La herramienta permite que usted vea una análisis de la salida del comando show.

- ¿**muestre el resumen**? Marca la cantidad de aciertos en las diversas reglas.`css# show summary`
```
Global Bypass Counters:   No Rule Bypass Count:     102   Acl Bypass Count:         0Owner
Content Rules     State     Services         Service HitsMyCompany          SSL               Active
SSL1              17                                                                  WWW
Active     tension          11                                                              SSL2WWW
Active     tension          19                                                            css#
```
- ¿**muestre el netstat**? Determina si el SCA escucha en el puerto derecho, y si hay algunas conexiones.`sca# show netstat`
```
Pro State Recv-Q Send-Q Local Address          Remote Address        R-
Win S-Win-------------------------------------------------------------------------------tcp ESTAB      0
0 192.168.1.2:4156      10.48.67.1:81          33304  6432tcp ESTAB      0      0 192.168.1.2:443
192.168.2.15:3106     33580 16560udp             0      0 *:4099                *:*
0     0udp              0      0 *:4098                *:*                           0     0tcp LISTN
0      0 *:2932                 *:*                        0     0udp             0      0 *:2932
*:*                         0     0udp             0      0 *:520                 *:*
0     0udp              0      0 *:514                 *:*                           0     0tcp LISTN
0      0 *:443                  *:*                     32768     0tcp LISTN      0      0 *:80
*:*                    32768     0tcp LISTN       0      0 *:23                  *:*
0     0sca#
```
Refiera a las conexiones del `ESTABLECIMIENTO` (establecido). Uno es una conexión con el cliente (192.168.2.15), y uno es una conexión con el servidor Web con el CSS (10.48.67.1)

Troubleshooting

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

Un Troubleshooting de este escenario es difícil debido al cifrado de todo el tráfico del cliente hasta el SCA.

Procedimiento de resolución de problemas

Siga estas instrucciones para resolver problemas de su configuración:

1. Marque para saber si hay Conectividad al servidor vía el HTTP.Esté seguro que la reorientación trabaja correctamente.
2. Marque para estar seguro que usted puede acceder el servidor vía el HTTPS con el CSS/SCA.Utilice una página que no requiera el cambio de dirección. Si este control falla, publique el **comando show summary** si hay tráfico en el CSS.Si usted no ve que cualquier golpe en el SSL gobierna, marque el estatus del servicio y de la regla de contenido. En caso necesario, utilice un sniffer delante del CSS para determinar si viene el tráfico adentro.Si usted ve que los golpes en el SSL gobiernan pero no en la regla SSL2WWW, publique el **comando show netstat** en el SCA si hay una conexión con el cliente en el puerto SSL. Si no, marque para saber si hay errores posibles SSL con la aplicación el **comando show ssl statistics** y el **comando show ssl errors**.Si usted ve los golpes en las reglas SSL y SSL2WW, pero le todavía no puede acceder el servidor, utilice un sniffer del cliente para determinar si los mensajes no vienen directamente del servidor Web.
3. Si las conexiones HTTPS funcionan pero no lo hace el cambio de dirección, colocar un sniffer delante del servidor para determinar la `ubicación:` valor de campo y si hace juego el que está en la configuración de SCA.

Comandos para Troubleshooting

- **muestre los errores SSL**
```
sca# show ssl errors ------------------------------For 'sca':SSL
Negotiation Errors (SNE)                        :        0Total SSL Connections Rejected no resources
:        0Ssl Accept Errors                             :        0SSL System Write Errors to
client                 :        0SSL Write Broken Connection Errors to client      :        0SSL
System Read Errors from client                 :        0SSL Read Broken Connection Errors from client
:        0System Write Errors to remote server              :        0Broken Connection Write Errors
to remote server    :        0System Read Errors from remote server             :        0Broken
Connection Read Errors from remote server  :        0System Call Error Histogram for Client SSL
ConnectionsSystem Call Error Histogram for Server Connections-----------------------------
```
- **muestre las estadísticas SSL**
```
sca# show ssl statistics ----------------------------  For 'sca':
Active Client Connections (AC):                         0  Active Server Connections:
0  Active Sockets (AS):                                    1  SSL Negotiation Errors (SNE):
0  Total Socket Errors (TSE):                              0  Connection Errors to remote Server (CES):
0  Total Connection Block Errors (TCBE):                   0  Total SSL Connections Refused:
0  Total SSL Connections Rejected (TSCR):                  0  Total Connections Accepted (TCA):
41  Total RSA Operations in Hardware (TROH):               15  Total SSL Negotiations Succeeded (TSNS):
41-----------------------------
```

Información Relacionada

- Descargas de las Redes de contenido (clientes registrados solamente)
- Soporte técnico de dispositivos de interconexión de redes de contenido
- Soporte Técnico - Cisco Systems