Configuration urlrewrite sur l'accélérateur de contenu sécurisé

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Théorie générale](#)
[Configurez](#)
[Diagramme du réseau](#)
[Configurations](#)
[Vérifiez](#)
[Dépannez](#)
[Procédure de dépannage](#)
[Dépannage des commandes](#)
[Informations connexes](#)

Introduction

Ce document fournit une configuration d'échantillon pour la caractéristique d'urlrewrite de l'accélérateur de contenu sécurisé (SCA). SCA offre une solution facile pour migrer des web server traditionnels avec le HTTP aux serveurs de contenu sécurisé avec le HTTP sécurisé (HTTPS).

La mise en place du SCA devant le serveur HTTP permet au SCA de remplir toutes les fonctions sécurisées nécessaires pour chiffrer le document HTML. Le SCA est transparent aux clients et serveurs.

Le but de ce document est d'afficher comment la fonction d'urlrewrite peut remplacer quelques liens à un document de HTTP avec un lien au même document par l'intermédiaire de HTTPS. Cette caractéristique est utile quand vous voulez être sûr qu'un utilisateur qui se connecte à votre serveur par l'intermédiaire de HTTPS par le SCA ne fait pas redirect to un document nonsecure (de HTTP).

Conditions préalables

Conditions requises

Avant que vous tentiez cette configuration, assurez-vous que vous comprenez ces concepts :

- Commutateur de services de contenu (CSS) et configuration de base SCA
- Protocoles de HTTP et HTTPS

Composants utilisés

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

- Cisco CSS 11000 ou CSS 11500 qui exécutent n'importe quelle version de logiciel de Cisco WebNS
- Cisco SCA ou SCA2 qui exécutent 3.2.x ou 4.x

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Théorie générale

La syntaxe de commande est la suivante :

- *Domain Name d'***urlrewrite [***portid de* **sslport] [***portid de* **clearport]** *redirectonly*

Quand vous avez configuré la commande d'**urlrewrite**, le SCA peut examiner la pleine réponse HTML pour remplacer tous les liens à un document nonsecure avec un lien au même document par l'intermédiaire de HTTPS. Par exemple, si le document HTML contient le <A HREF= " **http://mycompany.com/images/index.html** " >images</A> *e*, le SCA le remplace par le <A HREF= " **https://mycompany.com/images/index.html** " >images</A>.

Le SCA peut examiner l'en-tête seulement, au lieu du document HTML complet, et remplace l'URL qui est présent dans l'`emplacement :` champ. L'exemple ci-dessous affiche l'`emplacement :` mettez en place et l'URL ces points à une page nonsecure. Spécifiez **redirectonly l'**option pour que le SCA remplace seulement l'URL dans l'`emplacement :` champ.

```
HTTP/1.1 302 Found
Date: Wed, 05 Feb 2003 16:11:58 GMT
Server: Apache/2.0.40 (Red Hat Linux)
Location: http://tension.mycompany.com:70/images
Content-Length: 326
Keep-Alive: timeout=15, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

Configurez

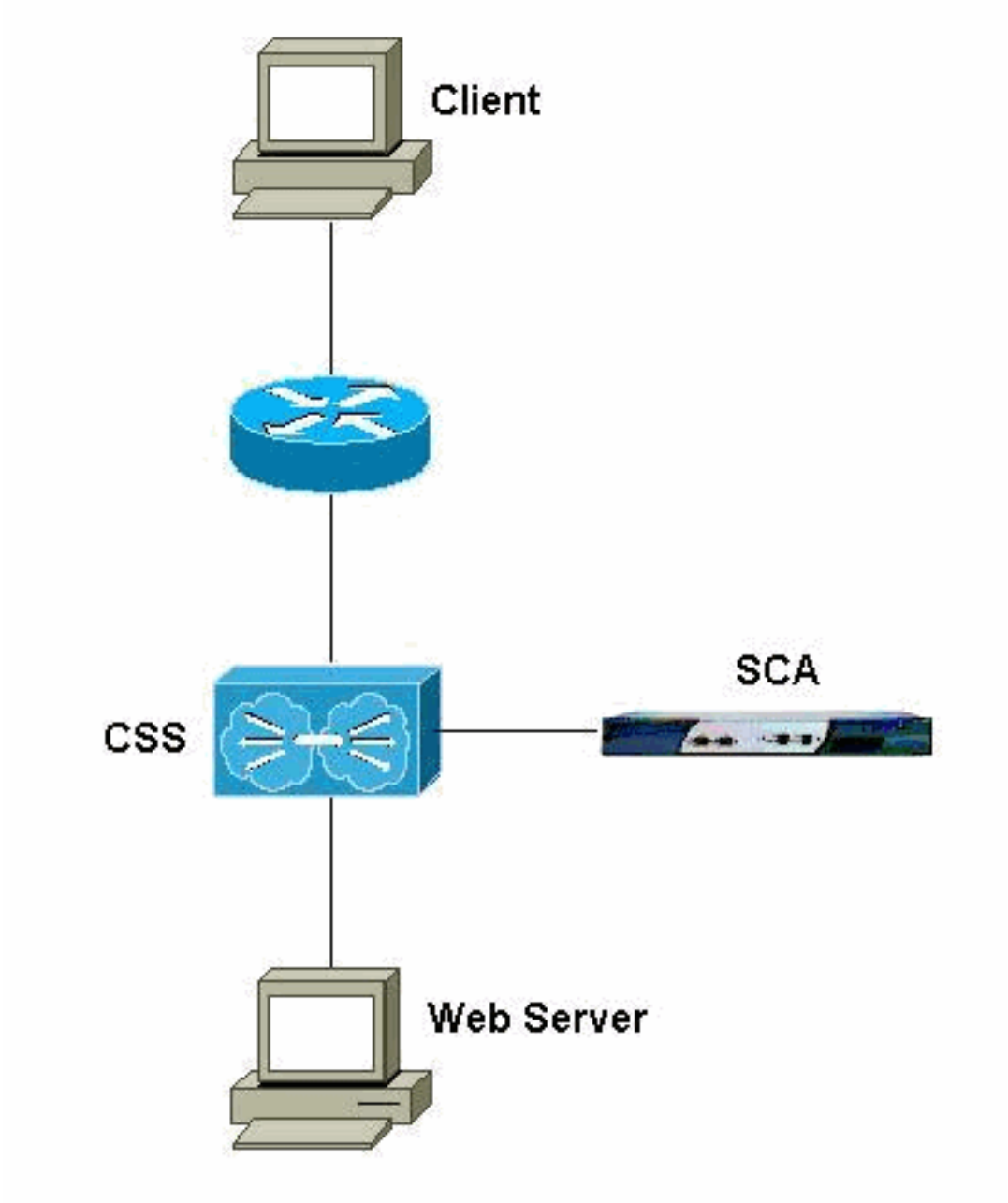
Cette section présente les informations pour configurer les caractéristiques que ce document décrit.

La configuration de votre serveur devrait être de réorienter des utilisateurs à http://tension.mycompany.com:70. La configuration SCA, en conséquence, est d'intercepter l'emplacement de champ d'en-tête, http://tension.mycompany.com:70, et le remplace par https://tension.mycompany.com.

Remarque: Pour trouver les informations complémentaires sur les commandes dans ce document, utilisez le Command Lookup Tool (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- 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
  auto
end
interface server
  auto
end

### Device ###

ip address 192.168.1.2 netmask 255.255.255.0
hostname sca
timezone "MST7MDT"

### Password ###

password access
"2431244C362461476C67654D485269494C4634772E586A374E39472
F"
password enable
"2431246E6324386D437A6E714B44567174306565386A77556653693
1"

### 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 10.10.10.1 ip domain-name
mycompany.com ### Remote Management ### no remote-
management access-list remote-management enable ###
Telnet ### telnet enable ### Web Management ### web-mgmt
port 80 web-mgmt enable ### SNMP Subsystem ### no snmp
### SSL Subsystem ### ssl !--- This is the certificate
definition. cert my-cert create binhex 579
=3082023f308201c9a0030201020201003 00d06092a864886f70d010
104050030
=8187311a3018060355040313116764756 66f75722e636973636f2e6
36f6d310b
```

=300906035504061302555331 0b300906035504081302434f310f300
d06035504
=07130644656e766572310f300d060355040a13065441432d6d65310
b30090603
=55040b130243413120301e06092a864886f70d01090116116764756
66f757240
=636973636f2e636f6d301e170d303330313330303730303 0305a170
d30343031
=33303037303030305a308187311a3018060355040313116764756 66
f75722e63
=6973636f2e636f6d310b300906035504061302555331 0b300906035
504081302
=434f310f300d060355040713064465e766572310f300d060355040
a13065441
=432d6d65310b3009060355040b130243413120301e06092a864886f
70d010901
=1611676475666f757240636973636f2e636f6d307c300d06092a864
886f70d01
=01010500036b003068026100aff358226467ed77f0278750048557d
e683291af
=47fceb89f40572e7d312623581a1d9f9a3d2087cbaeb2e30c402676
a7f8c7a6b
=02dc89e45d40d799d38ac93a20fa054809b2692b24bc3742285396c
8b91a66e1
=852aa9a23d6b1da0a95083850203010001300d06092a864886f70d0
1010405 00
=0361006fc579e08b00d5981c7d30f2d6219cb90ac0c203918ae2e96
1697de7bf
=85e57fbc0db3fa8a73e48bde1127926b780f127abfe7cd13283c8ad
4d45f0178
=b8fb2e3aba62622f8127ee1fd840b0738120fc38cf745d72c179331
913b1e87b =f4d3b4 end *!--- 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.

```
  end
end
sca#
```

CSS

```
css# show running-config
!Generated on 02/04/2003 13:31:17
!Active version: ap0503026s

configure


!*************************** 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#
```

Vérifiez

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

L'Output Interpreter Tool (clients enregistrés seulement) fournit le support pour certaines **commandes show**. L'outil te permet pour visualiser une analyse de sortie de commande show.

- **résumé d'exposition** — Vérifie le nombre de hits sur les différentes règles.

```
css# show summary
Global Bypass Counters:
   No Rule Bypass Count:     102
   Acl Bypass Count:         0

Owner            Content Rules    State     Services         Service Hits

MyCompany          SSL              Active    SSL1             17

                   WWW              Active    tension          11

                   SSL2WWW          Active    tension          19


css#
```

- **show netstat** — Détermine si le SCA écoute sur le port droit, et s'il y a des connexions.`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  6432
tcp ESTAB      0      0 192.168.1.2:443       192.168.2.15:3106     33580 16560
udp            0      0 *:4099                *:*                       0     0
udp            0      0 *:4098                *:*                       0     0
tcp LISTN      0      0 *:2932                *:*                       0     0
udp            0      0 *:2932                *:*                       0     0
udp            0      0 *:520                 *:*                       0     0
udp            0      0 *:514                 *:*                       0     0
tcp LISTN      0      0 *:443                 *:*                   32768     0
tcp LISTN      0      0 *:80                  *:*                   32768     0
tcp LISTN      0      0 *:23                  *:*                       0     0
```

`sca#` Référez-vous aux connexions d'`ÉTABLISSEMENT` (établi). On est une connexion avec le client (192.168.2.15), et on est une connexion avec le web server par le CSS (10.48.67.1)

Dépannez

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

Un dépannage de ce scénario est difficile en raison du cryptage de tout le trafic du client jusqu'au SCA.

Procédure de dépannage

Suivez ces instructions de dépanner votre configuration :

1. Vérifiez la Connectivité au serveur par l'intermédiaire du HTTP.Soyez sûr que la réorientation fonctionne correctement.
2. Vérifiez pour être sûr que vous pouvez accéder au serveur par l'intermédiaire de HTTPS par le CSS/SCA.Utilisez une page qui n'exige pas la redirection. Si ce contrôle échoue, émettez la commande **récapitulative d'exposition** s'il y a du trafic sur le CSS.Si vous ne voyez pas que tous les hit sur le SSL ordonnent, vérifiez l'état de service et de règle de contenu. S'il y a lieu, employez un renifleur devant le CSS pour déterminer si le trafic entre.Si vous voyez des hit sur la règle SSL mais pas sur la règle SSL2WWW, émettez la commande de **show netstat** sur le SCA s'il y a une connexion avec le client sur le port SSL. Sinon, vérifiez les erreurs possibles SSL avec la question de la commande de **statistiques de show ssl** et les **erreurs de show ssl** commandent.Si vous voyez les hit sur les règles SSL et SSL2WW, mais vous ne

pouvez toujours pas accéder au serveur, employez un renifleur du client pour déterminer si les messages ne sont pas livré directement du web server.

3. Si les connexions HTTPS fonctionnent mais la redirection ne fait pas, placer un renifleur devant le serveur pour déterminer l'`emplacement :` mettez en place la valeur et si elle apparie celui dans la configuration SCA.

Dépannage des commandes

- **erreurs de show ssl**

```
sca# show ssl errors
------------------------------

For 'sca':
SSL Negotiation Errors (SNE)                     :        0
Total SSL Connections Rejected no resources      :        0
Ssl Accept Errors                                :        0
SSL System Write Errors to client                :        0
SSL Write Broken Connection Errors to client     :        0
SSL System Read Errors from client               :        0
SSL Read Broken Connection Errors from client    :        0
System Write Errors to remote server             :        0
Broken Connection Write Errors to remote server  :        0
System Read Errors from remote server            :        0
Broken Connection Read Errors from remote server :        0
System Call Error Histogram for Client SSL Connections
System Call Error Histogram for Server Connections
------------------------------
```

- **statistiques de show 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
------------------------------
```

Informations connexes

- Téléchargements réseaux de diffusion de contenu) (clients enregistrés seulement)
- Soutien technique de périphériques de Réseau de diffusion de contenu
- Support technique - Cisco Systems