Configurando a urlrewrite no acelerador de conteúdo seguro

Índice

Introdução

Este documento fornece uma configuração de exemplo para a característica da urlrewrite do acelerador de conteúdo seguro (SCA). O SCA oferece uma solução fácil migrar dos servidores de rede tradicionais com o HTTP aos server do conteúdo seguro com HTTP seguro (HTTPS).

A inserção do SCA na frente do Server do HTTP permite o SCA de executar todas as funções seguras necessárias cifrar o documento HTML. O SCA é transparente aos clientes e servidor.

A finalidade deste documento é mostrar como a função da urlrewrite pode overwrite alguns links a um documento HTTP com um link ao mesmo documento através do HTTPS. Esta característica é útil quando você quer para ter certeza que um usuário que conecte a seu server através do HTTPS com o SCA não reorienta a um documento (HTTP) não-seguro.

Pré-requisitos

Requisitos

Antes que você tente esta configuração, assegure-se de que você compreenda estes conceitos:

- Content Services Switch (CSS) e configuração básica SCA
- HTTP e protocolos de HTTPS

Componentes Utilizados

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

- Cisco CSS 11000 ou CSS11500 que executam toda a versão de software webns de Cisco
- Cisco SCA ou SCA2 que executam 3.2.x ou 4.x

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos neste documento começaram com uma configuração esclarecida (PADRÃO). Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Material de Suporte

A sintaxe do comando é:

- **[clearport portid] do [sslport portid] do** *Domain Name da* **urlrewrite** *redirectonly*

Quando você configurou o **comando urlrewrite**, o SCA pode inspecionar a resposta completa HTML para substituir todos os links a um documento não-seguro com um link ao mesmo documento através do HTTPS. Por exemplo, se o documento HTML contém o <A HREF= " **http://mycompany.com/images/index.html** " >images</A> *e*, o SCA substitui-o com o <A HREF= " **https://mycompany.com/images/index.html** " >images</A>.

O SCA pode inspecionar o encabeçamento somente, em vez do documento completo HTML, e substitui a URL que esta presente no `lugar:` campo. O exemplo abaixo mostra o `lugar:` coloque e a URL esses pontos a uma página não-seguro. Especifique a **opção redirecionar somente** para que o SCA substitua somente a URL no `lugar:` campo.

```
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
```

Configurar

Esta seção apresenta a informação para configurar as características que este documento descreve.

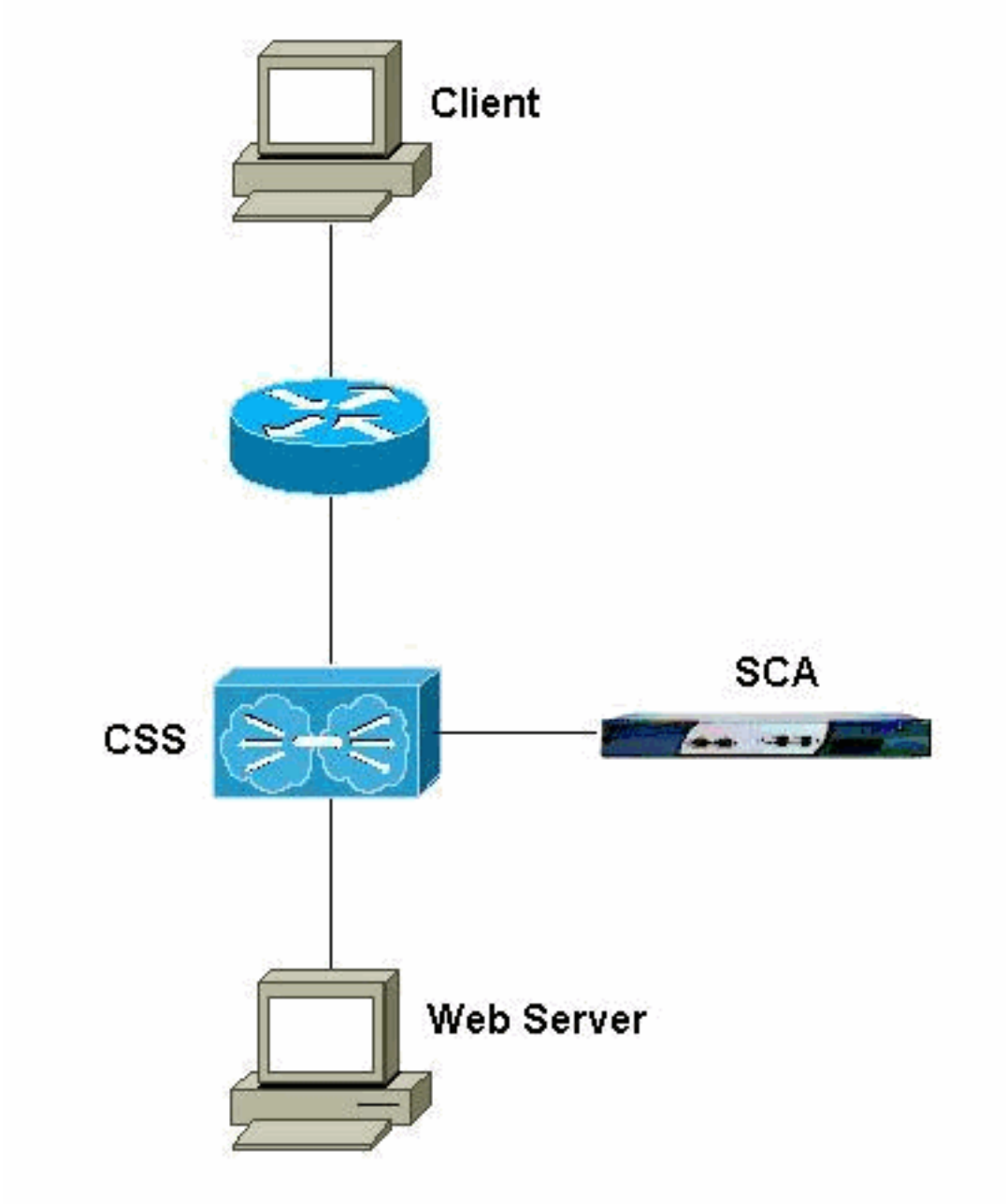
A configuração de seu server deve ser reorientar usuários a http://tension.mycompany.com:70. A configuração de SCA, em conformidade, é interceptar o lugar de campo de cabeçalho, http://tension.mycompany.com:70, e substitui-o com https://tension.mycompany.com.

Nota: Para encontrar a informação adicional nos comandos neste documento, use a ferramenta

de consulta de comandos (clientes registrados somente).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- 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
=8187311a30180603550403131167647 5666f75722e636973636f2e6
36f6d310b
=300906035504061302555331 0b300906035504081302434f310f300
d06035504
=07130644656e766572310f300d060355040a13065441432d6d65310
b30090603
=55040b130243413120301e06092a864886f70d01090116116764756
66f757240
=636973636f2e636f6d301e170d303330313330303730303030 5a170
d30343031
=3330303730303030 5a308187311a30180603550403131167647 5666
f75722e63
=6973636f2e636f6d310b300906035504061302555331 0b300906035
504081302
=434f310f300d060355040713064465 6e766572310f300d060355040
a13065441
=432d6d65310b3009060355040b130243413120301e06092a864886f
70d010901
=1611676475666f757240636973636f2e636f6d307c300d06092a864
886f70d01
=01010500036b003068026100aff358226467ed77f0278750048557d
e683291af
=47fceb89f40572e7d312623581a1d9f9a3d2087cbaeb2e30c402676
a7f8c7a6b
=02dc89e45d40d799d38ac93a20fa054809b2692b24bc3742285396c
8b91a66e1
=852aa9a23d6b1da0a9508385020301000 1300d06092a864886f70d0
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#
```

Verificar

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

A ferramenta Output Interpreter (clientes registrados somente) fornece **comandos show do** apoio com certeza. A ferramenta permite que você ver uma análise do emissor de comando de execução.

- **sumário da mostra** — Verifica o número de pressionamentos nas regras diferentes.
  ```
  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#
  ```
- **netstat da mostra** — Determina se o SCA escuta na porta direita, e se há alguma conexão.`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#` Refira as conexões do `ESTABELECIMENTO` (estabelecido). Um é uma conexão com o cliente (192.168.2.15), e um é uma conexão com o servidor de Web com o CSS (10.48.67.1)

Troubleshooting

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

Uma pesquisa de defeitos desta encenação é difícil devido à criptografia de todo o tráfego do cliente até o SCA.

Procedimento de solução de problemas

Siga estas instruções para fazer troubleshooting com sua configuração.

1. Verifique para ver se há a Conectividade ao server através do HTTP.Seja certo que a reorientação trabalha corretamente.
2. Verifique para ter certeza que você possa alcançar o server através do HTTPS com o CSS/SCA.Use uma página que não exija a reorientação. Se esta verificação falha, emita o **comando show summary** se há um tráfego no CSS.Se você não vê que todas as batidas no SSL ordenam, verifique o estado do serviço e da regra de conteúdo. Caso necessário, use um sniffer na frente do CSS para determinar se o tráfego entra.Se você vê que as batidas no SSL ordenam mas não na regra SSL2WWW, emita o **comando show netstat no** SCA se há uma conexão com o cliente na porta SSL. Se não, verifique para ver se há erros possíveis SSL com a introdução do **comando show ssl statistics** e do **comando show ssl errors**.Se você o vê batidas nas regras SSL e SSL2WW, mas não pode ainda alcançar o server, use um sniffer do cliente para determinar se as mensagens não vêm diretamente do servidor de Web.
3. Se as conexões de HTTPS funcionam mas a reorientação não faz, para colocar um sniffer na frente do server para determinar o `lugar:` valor de campo e se combina esse na configuração de SCA.

Comandos de solução de problemas

- **mostre erros 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 ------------------------------
```

- **mostre estatísticas 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 ------------------------------
```

Informações Relacionadas

- Transferências da Rede de conteúdo (clientes registrados somente)
- Suporte técnico de dispositivos de redes de conteúdo
- Suporte Técnico - Cisco Systems