Настройка функции urlrewrite на Secure Content Accelerator

Содержание

Введение

Этот документ предоставляет пример конфигурации для функции urlrewrite Защищенного акселератора контента (SCA). SCA предлагает простое решение для миграции от традиционных вебов - серверов с HTTP для обеспечения серверов содержания с Безопасным HTTP (HTTPS).

Вставка SCA перед HTTP server позволяет SCA выполнить все безопасные функции, необходимые для шифрования документа HTML. SCA очевиден для клиентов и серверов.

Цель этого документа состоит в том, чтобы показать, как функция urlrewrite может перезаписать некоторые ссылки на документ HTTP со ссылкой на тот же документ через HTTPS. Эта функция полезна, когда вы хотите быть уверенными, что пользователь, который соединяется с вашим сервером через HTTPS через SCA, не перенаправляет к незащищенному (HTTP) документ.

Предварительные условия

Требования

Прежде чем вы будете делать попытку этой конфигурации, будете гарантировать понимание этих понятий:

- Коммутатор контент-сервисов (CSS) и базовая конфигурация SCA
- HTTP и протоколы HTTPS

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco CSS 11000 или CSS 11500, который выполняет любую версию Программного обеспечения webns Cisco
- SCA Cisco или SCA2, который выполняется 3.2.x или 4. x

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, указанные в этом документе, начинали работу с чистой (стандартной) конфигурацией. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Теоретические сведения

Синтаксис команды:

- *доменное имя* **urlrewrite [sslport** *портируемый*] **[clearport** *портируемый*] *redirectonly*

При настройке **команды urlrewrite** SCA может осмотреть полный ответ HTML для замены всех ссылок на незащищенный документ со ссылкой на тот же документ через HTTPS. Например, если документ HTML содержит *e* <HREF = "**http:**//mycompany.com/images/index.html"> образы </A>, SCA заменяет его <HREF = "**https:**//mycompany.com/images/index.html"> образы </A>.

SCA может осмотреть заголовок только, вместо полного документа HTML, и заменить URL, который присутствует в поле `Location:`. Пример ниже показов поле `Location:` и URL, который указывает к незащищенной странице. Задайте **параметр redirectonly** для SCA, чтобы только заменить URL в поле `Location:`.

```
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
```

Настройка

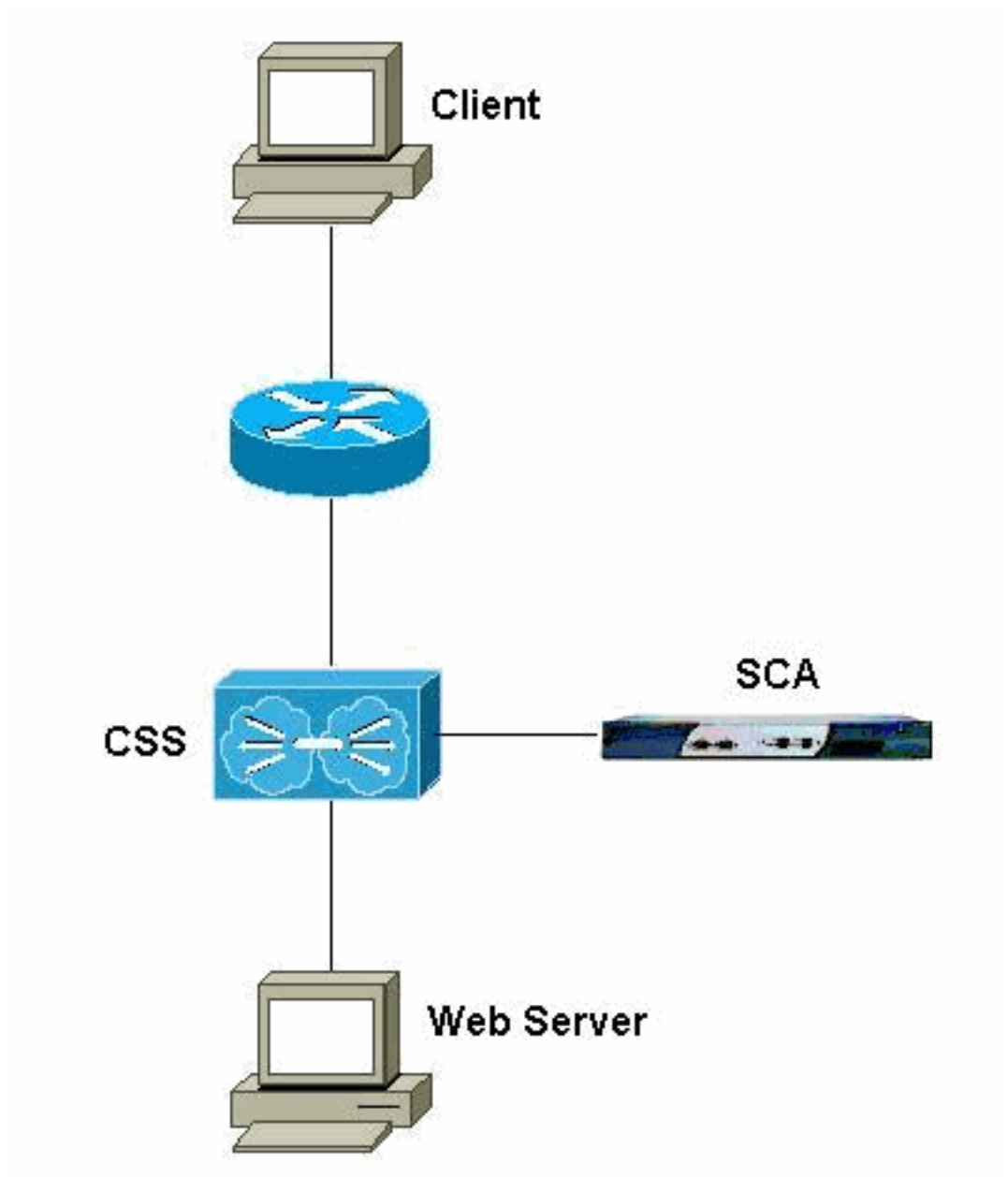
Этот раздел представляет информацию по настройке функций, которую описывает этот документ.

Конфигурация вашего сервера должна быть должна перенаправить пользователей к http://сила mycompany.com:70. Конфигурация SCA, соответственно, должна перехватить местоположение поля заголовка, http://сила mycompany.com:70, и заменить его https://tension.mycompany.com.

Примечание: Для обнаружения дополнительных сведений о командах в этом документе используйте Средство поиска команд Command Lookup Tool (только зарегистрированные клиенты).

Схема сети

В настоящем документе используется следующая схема сети:



Конфигурации

Эти конфигурации используются в данном документе:

- 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
=300906035504061302553310b300906035504081302434f310f300
d06035504
=07130644656e766572310f300d060355040a13065441432d6d65310
b30090603
=55040b130243413120301e06092a864886f70d01090116116764756
66f757240
=636973636f2e636f6d301e170d303330313330303730303030305a170
d30343031
=333030373030303035a308187311a3018060355040313116764756666
f75722e63
=6973636f2e636f6d310b300906035504061302553310b300906035
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#
```

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Средство интерпретации выходных данных (только зарегистрированные клиенты) оказывает поддержку для определенных **команд показа**. Программное средство позволяет вам **просматривать аналитику выходных данных команды show**.

- **show summary** количество соответствий на других правилах.

```
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** — Определяет, слушает ли SCA на правильном порту, и если существуют любые соединения.

```
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#` См. `ESTAB` (установил) соединения. Каждый - соединение с клиентом (192.168.2.15), и каждый - соединение с Web-сервером через CSS (10.48.67.1)

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Устранение неполадок этого сценария является трудным из-за шифрования всего трафика от клиента до SCA.

Процедура устранения неполадок

Для устранения неполадок конфигурации выполните следующие действия:

1. Проверьте для подключения к серверу через HTTP.Убедитесь, что перенаправление работает должным образом.
2. Проверьте, чтобы быть уверенными, что можно обратиться к серверу через HTTPS через CSS/SCA.Используйте страницу, которая не требует перенаправления. Если эта проверка отказывает, выполните **команду show summary**, если существует трафик на CSS.Если вы не видите соответствий на правиле SSL, проверьте статус правила содержимого и сервис. Если необходимо, используйте анализатор перед CSS, чтобы определить, входит ли трафик.Если существует соединение с клиентом на порту SSL, если вы видите соответствия на правиле SSL, но не на правиле SSL2WWW,

выполняете **команду show netstat** на SCA. В противном случае проверьте для возможных ошибок SSL с проблемой команды **show ssl statistics** и **команды show ssl errors**.Если вы видите соответствия на SSL и правилах SSL2WW, но вы все еще не в состоянии обратиться к серверу, используйте анализатор клиента, чтобы определить, не прибывают ли сообщения непосредственно из Web-сервера.

3. Если Подключения HTTPS работают, но перенаправление не делает, разместите анализатор перед сервером для определения значения поля `Location:` и если это совпадает с тем в конфигурации SCA.

Команды устранения неполадок

- **show ssl errors**

```
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
------------------------------
```

- **show ssl statistics**

```
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
------------------------------
```

Дополнительные сведения

- Загрузки Сетей передачи контента (только зарегистрированные клиенты)
- Техническая поддержка оборудования Управления Контентом
- Техническая поддержка - Cisco Systems