配置在安全内容加速器上的urlrewrite

目录

简介

本文为安全内容加速器(SCA) urlrewrite功能提供一配置示例。SCA提供一容易解决方案从有HTTP的传统Web服务器移植到有安全HTTP的(HTTPS)安全内容服务器。

SCA的插入在HTTP服务器前面的使SCA执行必要所有安全的功能加密HTML文档。SCA是透明对客户端和服务器。

本文目的将显示urlrewrite功能如何能覆盖一些链路到HTTP文档与链路到同一个文档通过HTTPS。此功能是有用的，当您要肯定时连接到您的服务器通过HTTPS通过SCA的用户不重定向对一个不安全的(HTTP)文档。

先决条件

要求

在您尝试此配置前，请保证您了解这些概念：

- 内容服务交换机(CSS)和SCA基本配置
- HTTP和HTTPS协议

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行所有Cisco WebNS软件版本的Cisco CSS 11000或CSS11500
- 运行3.2.x或4.x的Cisco SCA或SCA2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景理论

命令语法为：

- **urlrewrite***域名***[sslport portid] [clearport portid]** *redirectonly*

当您配置**urlrewrite命令时**，SCA能检查全双工HTML答案替换所有链路到一个不安全的文档与链路到同一个文档通过HTTPS。例如，如果HTML文档包含*e* <A HREF= " **http://mycompany.com/images/index.html** " >images</A>，SCA用<A HREF= " **https://mycompany.com/images/index.html** " >images</A>替换它。

SCA能检查仅报头，而不是存在完整HTML文档，并且替换URL 字段。下面的示例显示字段和URL对一个不安全的页的该点。在指定SCA的**redirectonly**选项能只替换URL 字段。

```
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
```

配置

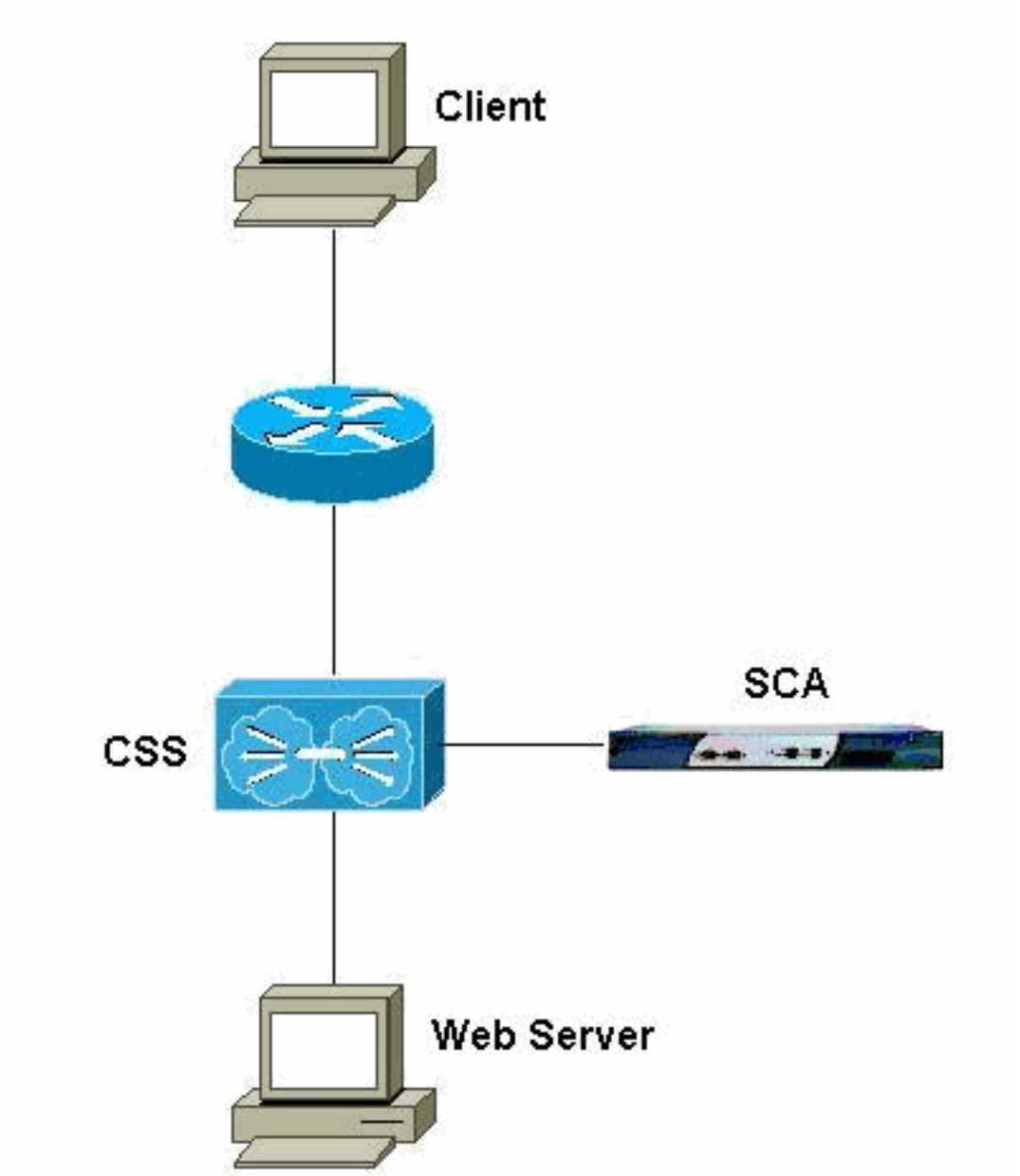
此部分引见信息配置本文描述的功能。

您的服务器的配置应该是重定向用户对http://tension.mycompany.com:70。SCA配置，相应地，是拦截报头字段字段位置，http://tension.mycompany.com:70，并且用https://tension.mycompany.com替换它。

注意： 要寻找关于in命令的其他信息本文，使用命令查找工具(仅限注册用户)。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

- 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
=3009060355040613025553310b3009060 3550408130243 4f310f300
d06035504
=07130644656e766572310f300d060355040a13065441432d6d65310
b30090603
=55040b130243413120301e06092a864886f70d01090116116764756
66f757240
=636973636f2e636f6d301e170d3033303133303037303030305a170
d30343031
=3330303730303030 5a308187311a3018060355040313116764756 66
f75722e63
=6973636f2e636f6d310b3009060355040613025553310b300906035
504081302
=434f310f300d060355040713064465 6e766572310f300d060355040
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#
```

验证

本部分提供的信息可帮助您确认您的配置是否可正常运行。

Output Interpreter Tool (仅限注册用户)提供支持肯定**显示**命令。工具允许您查看show命令输出分析。

- **show summary** —检查命中数数量在不同的规则的。

```
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** —确定SCA是否在正确端口侦听，并且是否有任何连接。

```
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# 参考(已建立)连接。一个是与客户端(192.168.2.15)的一连接，并且一个是一连接用Web服务器通过CSS (10.48.67.1)

故障排除

本部分提供的信息可用于对配置进行故障排除。

此方案排除故障是困难由于所有流量的加密从客户端的至SCA。

故障排除步骤

遵从这些说明排除故障您的配置：

1. 检查连接到服务器通过HTTP。请务必重定向适当地运作。
2. 检查肯定您能通过HTTPS访问服务器通过CSS/SCA。请使用不要求重定向的一个页。如果此检查发生故障，请发出**show summary命令**是否有在CSS的流量。如果看不到在SSL的所有命中数规定，请检查服务和内容规则状态。如果需要，请使用在CSS前面的一个嗅探器确定流量是否进来。如果看到命中数在SSL规则，但是不在SSL2WWW规则，请发出**show netstat命令**在SCA，如果有与客户端的一连接SSL端口的。否则，请检查可能的SSL错误与问题**show ssl statistics命令**和**show ssl errors命令**。如果看到在SSL和SSL2WW规则的命中数，但是您仍然不能访问服务器，请使用客户端的嗅探器确定消息是否不来自直接地Web服务器。
3. 如果HTTPS连接工作，但是重定向不，放置在服务器前面的一个嗅探器确定字段值，并且，如果匹配那个在SCA配置里。

故障排除命令

- **显示ssl错误**

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

相关信息

- 内容网络下载(注册用户)
- 内容网络设备技术支持
- 技术支持 - Cisco Systems