セキュア コンテンツ アクセラレータでの urlrewrite の設定

目次

概要

このドキュメントでは、セキュア コンテンツ アクセラレータ（SCA）の urlrewrite 機能の設定例を紹介します。 SCA は、HTTP を使用した従来の Web サーバからセキュア HTTP（HTTPS）を使用したセキュア コンテンツ サーバに移行するための簡単な解決方法を提供します。

HTTP サーバの前に SCA を挿入することで、SCA は、HTML ドキュメントの暗号化に必要なすべての安全な機能を実行できます。 SCA は、クライアントおよびサーバに対してトランスペアレントです。

このドキュメントでは、urlrewrite 機能により HTTP ドキュメントへのリンクが、HTTPS を介した同じドキュメントへのリンクにどのように上書きされるかを示します。 この機能は、SCA を使用して HTTPS を介してサーバに接続するユーザが、非セキュア（HTTP）ドキュメントにリダイレクトされないようにする場合に役に立ちます。

前提条件

要件

この設定を開始する前に、次の概念について理解しておく必要があります。

- コンテンツ サービス スイッチ（CSS）および SCA の基本構成

- HTTP および HTTPS プロトコル

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 任意の Cisco WebNS ソフトウェア バージョンを実行する Cisco CSS 11000 または CSS 11500
- 3.2.x または 4.x を実行する Cisco SCA または SCA2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントのすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景理論

コマンドの構文は次のとおりです。

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

urlrewrite コマンドが設定されている場合、SCA は、フル HTML アンサーを検査し、非セキュア ドキュメントへのすべてのリンクを、HTTPS を介した同じドキュメントへのリンクに置換できます。 たとえば、HTML ドキュメントに *e* <A HREF="**http**://mycompany.com/images/index.html">images</A> が含まれている場合、SCA は、このリンクを <A HREF="**https**://mycompany.com/images/index.html">images</A> に置換します。

SCA は、フル HTML ドキュメントではなく、ヘッダーのみを検査して、Location: フィールドの URL のみが置換されます。 次の例では、非セキュア ページにリンクされた Location: フィールドおよび URL を示します。 SCA の **redirectonly** オプションを指定すると、Location: フィールドの URL のみが置換されます。

```
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
```

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

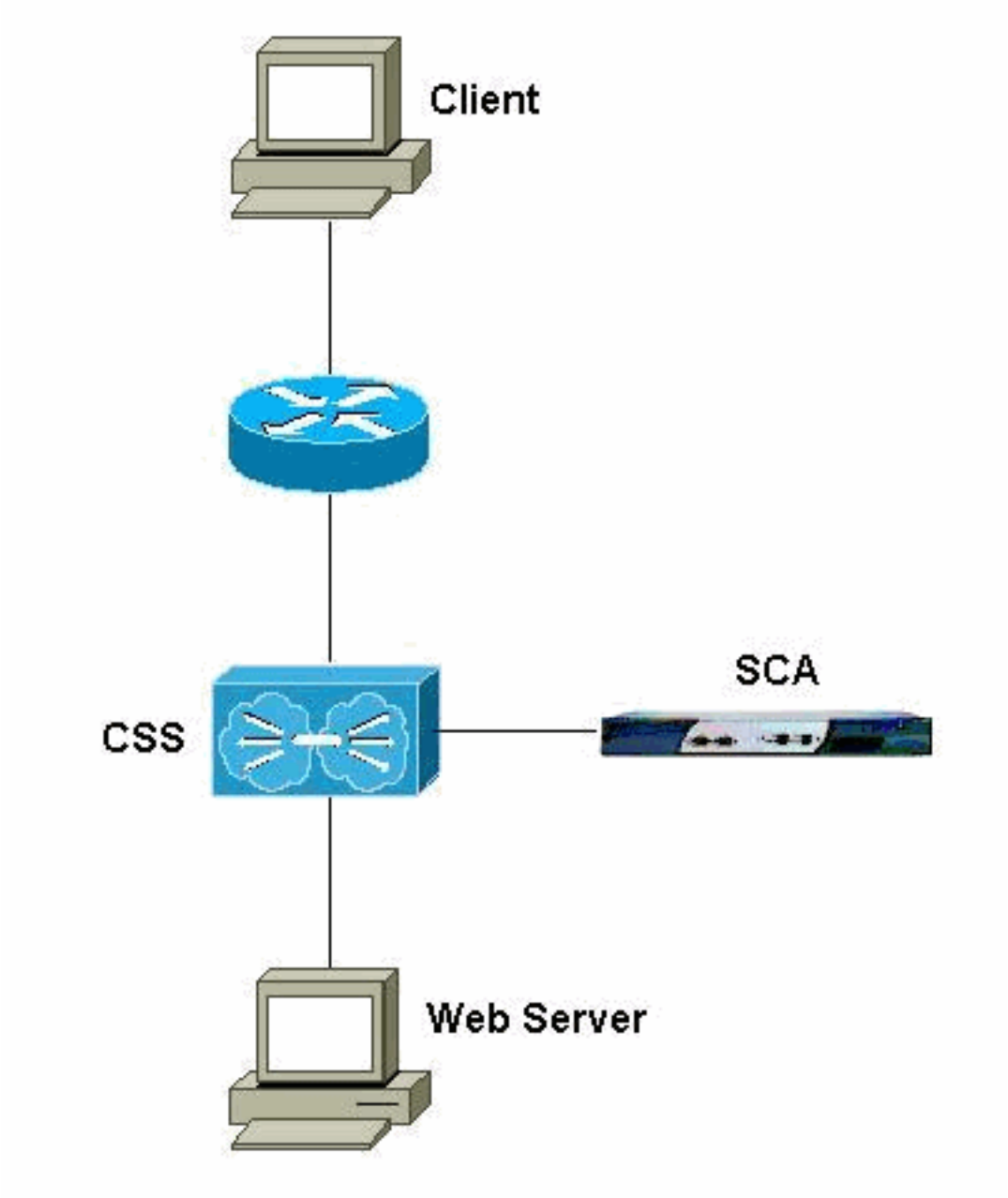
サーバは、ユーザを http://tension.mycompany.com:70 にリダイレクトするように設定する必要があります。 これにより、SCA 設定は、ヘッダー フィールド ロケーション

http://tension.mycompany.com:70 をインターセプトして、https://tension.mycompany.com に置換します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

このドキュメントでは、次の設定を使用します。

- 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
=636973636f2e636f6d301e170d303330313330303730303030 5a170
d30343031
=33303037303030305a308187311a3018060355040313116764756 66
f75722e63
=6973636f2e636f6d310b3009060355040613025553310b300906035
504081302
=434f310f300d060355040713064656e766572310f300d060355040
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#
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

Output Interpreter Tool（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。このツールを使用すると、**show** コマンドの出力を分析できます。一部ツールについては、ゲスト登録のお客様はアクセスできない場合があることをご了承ください。

- **show summary**：各ルールでのヒット数をチェックします。

```
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**：SCA が正しいポートでリスニングされ、接続が確立されているか確認します。

```
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#
```

ESTAB（確立）接続を参照してください。 一方はクライアントとの接続（192.168.2.15）で、もう一方は CSS を介した Web サーバとの接続です（10.48.67.1）。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

クライアントから SCA へのすべてのトラフィックが暗号化されているため、このシナリオのトラブルシューティングは困難です。

トラブルシューティングの手順

設定をトラブルシューティングするには、次の手順を実行します。

1. HTTP を介したサーバとの接続をチェックします。リダイレクトが正しく機能することを確認します。
2. CSS/SCA により HTTPS を介してサーバにアクセスできるかチェックします。リダイレクションを必要としないページを使用します。 このチェックに失敗した場合、CSS にトラフィックがある場合は **show summary** コマンドを実行します。SSL ルールにヒットしない場合、サービスおよびコンテンツ ルール ステータスをチェックします。 必要な場合、CSS の前でスニファを使用して、トラフィックが着信するか確認します。SSL2WWW ルールではなく、SSL ルールにヒットすれば、SSL ポートのクライアントと接続が確立されている場合、SCA で **show netstat** コマンドを実行します。 接続がない場合、**show ssl statistics** コマンドおよび **show ssl errors** コマンドを実行して、SSL エラーがないかチェックします。SSL および SSL2WW ルールにヒットするが、サーバにアクセスできない場合、クライアントのスニファを使用して、Web サーバからメッセージが直接送信されるか確認します。

3. HTTPS 接続は機能するが、リダイレクションが機能しない場合、サーバの前にスニファを挿入して、Location: フィールドの値を確認し、SCA 設定と一致するか検証します。

トラブルシューティングのためのコマンド

- **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
------------------------------
```

関連情報

- コンテンツ ネットワーキング ダウンロード (登録ユーザ専用)
- コンテンツ ネットワーキング デバイスに関するテクニカル サポート
- テクニカルサポート - Cisco Systems