

Manipulación del tráfico HTTPS con el módulo CSS5-SSL

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de muestra para el módulo CSS5-SSL. El módulo CSS5-SSL se introduce con la estructura 1. de la WebNS versión 5.20.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

[Convenciones](#)

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este

documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

[Diagrama de la red](#)

Este documento utiliza esta configuración de red:

[Configuraciones](#)

Este documento utiliza esta configuración.

- [POMPÓN \(CSS11506\)](#)

```
POMPÓN (CSS11506)
POMPON#show running-config !Generated on 10/09/2002
12:46:25 !Active version: sg0520002s configure
|***** GLOBAL
***** logging buffer 64000 ssl
associate rsakey keyrsa CompanyX-rsa-key ssl associate
cert rsacert CompanyX-cert ssl associate dhparam
CompanyX-dh CompanyX-dh ssl associate dsakey CompanyXdsa
CompanyX-dsa-key ip route 0.0.0.0 0.0.0.0 10.48.66.1 1
|***** INTERFACE
***** interface Ethernet-Mgmt phy
10Mbits-HD interface 3/1 bridge vlan 10 interface 3/3
bridge vlan 149 !***** CIRCUIT
***** circuit VLAN10 ip address
10.48.67.8 255.255.254.0 circuit VLAN149 ip address
192.168.150.199 255.255.255.0 !--- Server VLAN.
|***** SSL PROXY LIST
***** ssl-proxy-list ssl-list ssl-
server 90 ssl-server 90 vip address 10.48.67.22 !--- The
VIP address must be the same as in the content rule
defined here. !--- The default port is 443. !--- You can
change the default port when you issue the !--- ssl-
server 90 port <0-65535> command. ssl-server 90 cipher
rsa-with-des-cbc-sha 192.168.150.15 80 ssl-server 90
cipher rsa-with-3des-ede-cbc-sha 192.168.150.15 80 ssl-
server 90 cipher rsa-with-rc4-128-sha 192.168.150.15 80
ssl-server 90 cipher rsa-with-rc4-128-md5 192.168.150.15
80 !--- Note: The IP address in the cipher suite can be
the VIP address or !--- the address of a real server
that is available to the CSS. !--- Select which cipher
mode you want the CSS to accept and define to which
server !--- deciphered (clear) traffic should be sent.
!--- You can select different servers/ports for each
cipher mode. ssl-server 90 rsacert rsacert ssl-server 90
rsakey keyrsa !--- Define which certificate and key to
use. active !***** SERVICE
***** service WWW type ssl-accel !-
-- Define that the SSL module is used. add ssl-proxy-
list ssl-list keepalive type none !--- Disable keepalive
- internal heartbeat is used. slot 5 !--- Define which
SSL module to use (issue the show chassis !--- command
to see in which slot the SSL module is. active
|***** OWNER
***** owner CompanyX !--- The
```

```
content rule definition is the same as for any other
service. content ssl port 443 vip address 10.48.67.22 !-
-- The ssl-proxy-list VIP address and port must match
with those defined here. protocol tcp application ssl
add service WWW active POMPON#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre el chasis** POMPON#**show chassis** Configuration for CSS11506-2AC A0: Product Name: CSS11506-2AC A0 SW Version: 5.20 Build 2 Serial Number: PL505500237 Base Mac Address: 00-07-85-43-8d-96 Slot Number Module Name Status 1 CSS5-SCM-2GE primary 2 CSS5-SAM primary 3 CSS5-IOM-8FE primary 4 CSS5-IOM-2GE primary 5 **CSS5-SSL primary** 6 empty slot 7 CSS506-SM powered-on 8 CSS506-SM powered-on
- **show version** POMPON#**show version** Version: sg0520002s (5.20 Build 2) Flash (Locked): 5.10 Build 1 Flash (Operational): 5.20 Build 2 Type: PRIMARY Licensed Cmd Set(s): Standard Feature Set Secure Management POMPON#
- **muestre el archivo SSL** POMPON#**show ssl file** File Name File Type File Size -----
----- CompanyX-rsa-key PEM 688 CompanyX-cert PEM 871 CompanyX-dh PEM 201
CompanyX-dsa-key PEM 404 POMPON#
- **muestre los flujos SSL** POMPON#**show ssl flows** SSL Acceleration Flows for slot 5 Virtual Port
TCP Proxy Flows Active SSL Flows SSL Flows in Handshake -----
----- 10.48.67.22 443 0 0 0 POMPON#
- **muestre al socio SSL** POMPON#**show ssl associate** Certificate Name File Name Used by List ----
----- rsacert CompanyX-cert yes RSA Key Name File Name Used by
List ----- CompanyXrsa CompanyX-rsa-key yes DH Param Name File
Name Used by List ----- CompanyX-dh CompanyX-dh no DSA Key
Name File Name Used by List ----- CompanyXdsa CompanyX-dsa-key
no POMPON#
- **muestre las estadísticas SSL** POMPON#**show ssl statistics** SSL Acceleration Statistics 0 DSA
Sign Failed 0 DSA Verify Failed 0 SSL MAC Failed 0 TLS HMAC Failed 0 3DES Failed 0 ARC4
Failed 0 HASH Failed 0 Hardware Device Not Found 0 Hardware Device Timed Out 0 Invalid
Crypto Parameter 0 Hardware Device Failed 313 SSL received non-application data bytes 992
SSL transmitted non-application data bytes 0 RSA Private Decrypt failures 0 MAC failures for
packets received 0 Re-handshake TimerAlloc failed 0 Blocks SSL could not allocate 0 Dup
Blocks SSL could not allocate 0 Too many blocks for Block2AccelFragmentArray 0 Too many
blocks in a SSL message POMPON#
- **show summary** POMPON#**show summary** Global Bypass Counters: No Rule Bypass Count: 0 Acl
Bypass Count: 0 Owner Content Rules State Services Service Hits CompanyX ssl Master WWW 2
POMPON#
- **show flows** POMPON#**show flows** -----
----- Src Address SPort Dst Address DPort NAT Dst Address Prt InPort OutPort -----
----- 192.168.150.15 80
10.254.8.98 38460 0.0.0.0 TCP 3/3 3/1 POMPON#
- **muestre el contenido todo del propietario de la regla** POMPON#**show rule CompanyX ssl all** Name:
ssl Owner: CompanyX State: Active Type: SSL Balance: Round Robin Failover: N/A Persistence:
Enabled Param-Bypass: Disabled Session Redundancy: Disabled PrimarySorryServer: None
SecondSorryServer: None Name: Hits: Wgt: State: Ld: KAlive: Conn: DNS: -----
-- --- WWW 16 S-1 Alive 2 None 0 0 Rule DNS Information DNS Balance:
roundrobin DNS Names: DNS TTL: Rule Hotlist Information Hotlist: Disabled Size: 10, Type:
HitCount, Threshold 0, Interval 1 Associated ACLs: NONE
- **muestre el SSL-proxy-servidor de las estadísticas SSL** POMPON#**show ssl statistics ssl-proxy-server** SSL Acceleration Statistics Component: SSL Proxy Server Slot: 5 Count Description ---

```
----- 20 Handshake started for incoming SSL connections 19 Handshake
completed for incoming SSL connections 0 Handshake started for outgoing SSL connections 0
Handshake completed for outgoing SSL connections 1 Active SSL flows high water mark 0
Current number of TCP Proxy flows 2 Maximum number of TCP Proxy flows POMPON#
```

- **muestre el SSL de las estadísticas SSL**

```
POMPON#show ssl statistics ssl
```

 SSL Acceleration
Statistics Component: SSL Slot: 5 Count Description ----- 5 RSA
Private Decrypt calls 0 RSA Public Decrypt calls 0 DH Compute key calls 0 DH Generate key
calls 0 DSA Verify calls 0 DSA Sign calls 335 MD5 raw hash calls
- **muestre las estadísticas de cifrado SSL**

```
POMPON#show ssl statistics crypto
```

 SSL Acceleration
Statistics Component: Crypto Slot: 5 Count Description ----- 5 RSA
Private 0 RSA Public 0 DH Shared 0 DH Public 0 DSA Sign 0 DSA Verify 192 SSL MAC 257 TLS
HMAC 451 3DES 0 ARC4 3,303 HASH 0 RSA Private Failed 0 RSA Public Failed 0 DH Shared Failed
0 DH Public Failed 0 DSA Sign Failed 0 DSA Verify Failed 0 SSL MAC Failed 0 TLS HMAC Failed
0 3DES Failed 0 ARC4 Failed 0 HASH Failed 0 Hardware Device Not Found 0 Hardware Device
Timed Out 0 Invalid Crypto Parameter 0 Hardware Device Failed 0 Hardware Device Busy 0 Out
Of Resources 0 Cancelled -- Device Reset POMPON#

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Centro del software de Content Networking \(sólo para clientes registrados\)](#)
- [‘Soporte técnico para hardware de dispositivos de redes de contenido’](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)