

CS y ejemplo de la configuración inicial del módulo de servicios SSL

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento suministra una configuración de ejemplo para configurar el Content Switching Module (CSM) con Secure Socket Layer (SSL).

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ® corriente 12.1 del Cisco IOS del Cisco 7202 Router
- Cisco Catalyst 6509 IOS12.1 que se ejecuta
- CS con el conjunto de características del Motor de terminación SSL (STE) que ejecuta IOS 12.2(11) y SSL(0.86)
- Cisco 7606 Router que ejecuta el IOS12.1
- Estructura CS 3.1(0.119)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

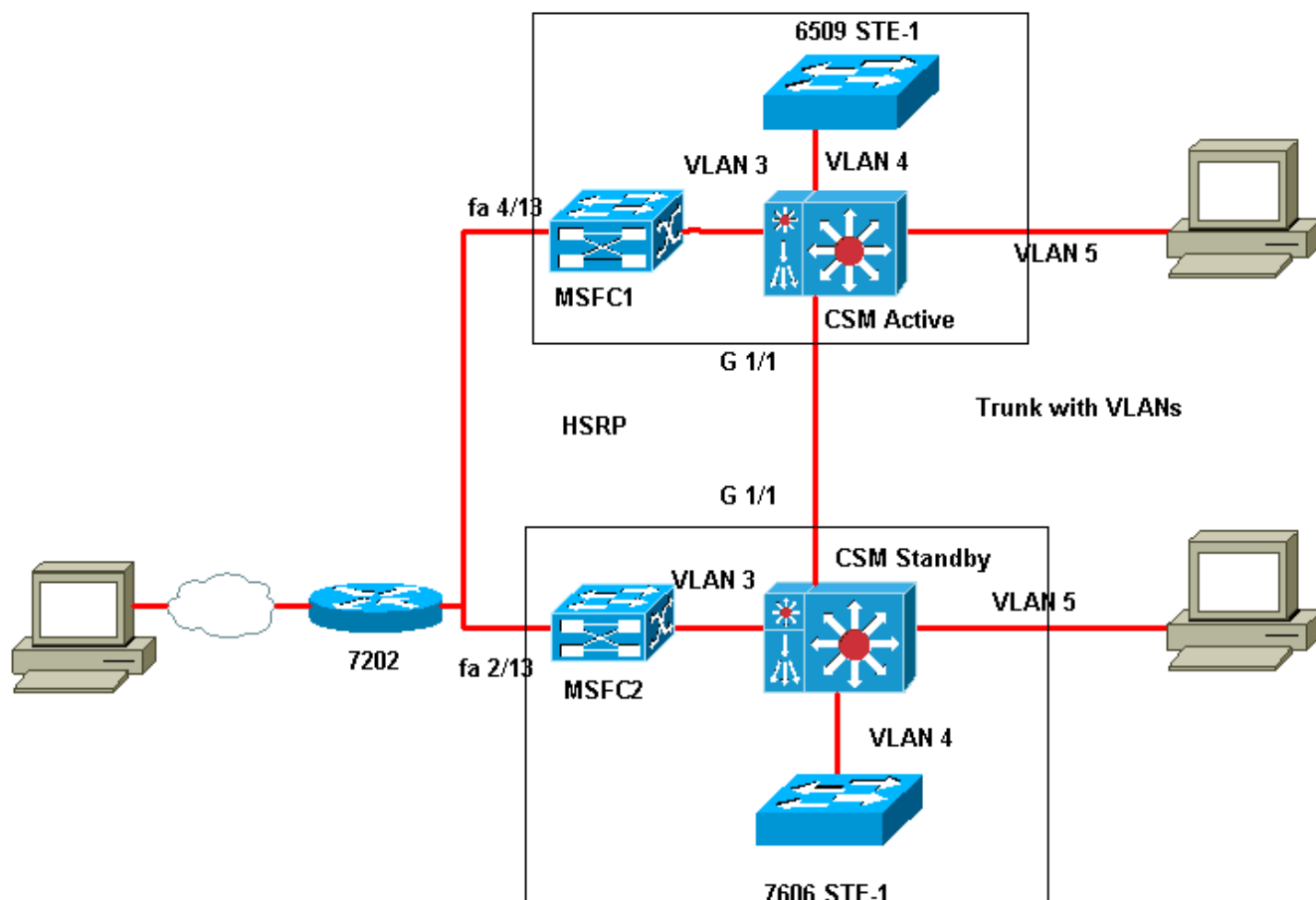
Configurar

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

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

Diagrama de la red

En este documento, se utiliza esta configuración de red:



En esta topología, el Hot Standby Router Protocol (HSRP) se está ejecutando sobre la Multilayer Switch Feature Card 1 (MSFC1) y la Multilayer Switch Feature Card 2 (MSFC2). Hay dos grupos del HSRP, uno en el lado del cliente y otro en el lado CS. El CS se configura como el modo enviado entre el MSFC y el Motor de terminación SSL (STE), y modo dirigido entre el STE y los servidores reales. El CS es conexiones SSL del Equilibrio de carga entre dos STE.

Configuraciones

En este documento, se utilizan estas configuraciones:

- 7202 Router
- 6509 Switch
- STE-1
- 7606 Switch
- STE-2

Éstos son los casos de prueba:

1. Copia de la conexión SSL en el CS
2. Copia fija de SSL en el CS
3. Conmutación por falla del CS con la conexión SSL dejada abierta
4. Conmutación por falla del MSFC activo con la conexión SSL abierta
5. La Conmutación por falla del chasis con las conexiones SSL dejadas se abre
6. Renegociación de la conexión SSL en la misma conexión y reanudación con la nueva conexión SSL (nueva función)
7. Funcionalidad fija CSM con las conexiones SSL múltiples con la reanudación

7202

```
7202-Reg#show run
Building configuration...
Current configuration : 1042 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 7202-Reg
!
boot system flash disk0:c7200-jk2o3s-mz.121-11b.E
enable password lab
!
ip subnet-zero
!
!
no ip domain-lookup
ip host defib 223.255.254.242
!
ip cef
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
controller ISA 1/1
!
controller ISA 2/1
!
interface Loopback0
 ip address 192.10.10.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 15.10.10.21 255.0.0.0
 duplex auto
 speed auto
```

```

!
interface FastEthernet0/1
 ip address 11.0.0.1 255.0.0.0
 duplex auto
 speed auto
!
interface GigabitEthernet5/0
 ip address 10.0.0.100 255.0.0.0
 negotiation auto
!
ip classless
ip route 12.0.0.0 255.0.0.0 11.0.0.100
ip route 192.0.0.0 255.0.0.0 147.10.10.1
ip route 223.255.254.0 255.255.255.0 15.0.100.1
no ip http server
no ip http secure-server
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password lab
 login
line vty 5 15
 login
!
end

```

6509

```

6509-1#show run
Building configuration...
Current configuration : 7932 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname 6509-1
!
boot system flash slot0:
logging buffered 50000000 debugging
enable password lab
!
!--- Configures the VLANs allowed over the trunk to the
SSL services module. !--- The admin VLAN is included.
The SSL module is located in slot 9. !
ssl-proxy module 9 allowed-vlan 4,15
diagnostic level complete
ip subnet-zero
!
!
no ip domain-lookup
!
mls flow ip destination
mls flow ipx destination
!
spanning-tree extend system-id
no spanning-tree vlan 2
!

```

```

!--- The CSM is located in slot 7. The module is
running as Active. !
module ContentSwitchingModule 7
  vlan 3 client
    ip address 12.0.0.23 255.0.0.0
    gateway 12.0.0.100
  !
  vlan 4 server
    ip address 12.0.0.23 255.0.0.0
  !
  vlan 5 server
    ip address 20.0.0.23 255.0.0.0
    alias 20.0.0.100 255.0.0.0
  !
  probe ICMP icmp
    interval 5
    failed 10
  !
  !--- These are the server farm HTTP and real server
members. serverfarm HTTP
    nat server
    no nat client
    real 20.0.0.7
      inservice
    real 20.0.0.8
      inservice
    real 20.0.0.9
      inservice
    real 20.0.0.10
      inservice
    real 20.0.0.11
      inservice
    real 20.0.0.12
      inservice
  !
  !--- These are the server farm HTTPS and real server
members. serverfarm HTTPS
    no nat server
    no nat client
    real 12.0.0.50
      inservice
    real 12.0.0.51
      inservice
    probe ICMP
  !
  sticky 1 ssl timeout 5
  sticky 2 netmask 255.0.0.0 timeout 5
  !
  !--- Virtual server HTTP. vserver HTTP
!--- The virtual server IP address is specified with TCP
port www.
virtual 12.0.0.124 tcp www
  !--- The VLAN from where the CSM accepts traffic for a
specified virtual server.
vlan 4
  !--- Destination server farm.
serverfarm HTTP
sticky 5 group 2
  !--- Enables connection redundancy. !--- Replicates the
sticky database to the backup CSM.
replicate csrp sticky
  !--- Replicates connections to the backup CSM.
replicate csrp connection
  persistent rebalance

```

```

inservice
!
!--- Virtual server HTTPS. vserver HTTPS
!--- The virtual server IP address is specified with
TCP port HTTP over SSL. virtual 12.0.0.123 tcp https
!--- The VLAN from where the CSM accepts traffic for a
specified virtual server. vlan 3
!--- Destination server farm.
serverfarm HTTPS
ssl-sticky offset 20 length 6
sticky 5 group 1
!--- Enables connection redundancy. !--- Replicates the
sticky database to the backup CSM.
replicate csrp sticky
!--- Replicates connections to the backup CSM.
replicate csrp connection
!--- Disables HTTP 1.1 persistence for connections in
the virtual server.
no persistent rebalance
inservice
!
  ft group 1 vlan 2
!
!
redundancy
  mode rpr-plus
  main-cpu
    auto-sync running-config
    auto-sync standard
!
power redundancy-mode combined
!
interface Loopback0
  ip address 192.10.10.2 255.255.255.255
!
interface GigabitEthernet1/1
  no ip address
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1-5,1002-1005
  switchport mode trunk
!
interface GigabitEthernet1/2
  no ip address
  shutdown
!
interface FastEthernet4/13
  ip address 11.0.0.5 255.0.0.0
  no ip redirects
  standby 2 ip 11.0.0.100
  standby 2 priority 101
  standby 2 preempt
  standby 2 name Client-Side
!
interface FastEthernet4/14
  no ip address
  shutdown
!
interface FastEthernet4/48
  no ip address
  switchport
  switchport access vlan 15
  switchport mode access
!

```

```

interface GigabitEthernet5/1
  no ip address
  switchport
  switchport access vlan 5
  switchport mode access
!
interface GigabitEthernet5/2
  no ip address
  switchport
  switchport access vlan 5
  switchport mode access
!
interface GigabitEthernet5/3
  no ip address
  switchport
  switchport access vlan 5
  switchport mode access
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan3
  ip address 12.0.0.1 255.0.0.0
  no ip redirects
  standby 1 ip 12.0.0.100
  standby 1 priority 101
  standby 1 preempt
  standby 1 name CSM-Side
  standby 1 track FastEthernet4/13
!
interface Vlan15
  ip address 15.0.1.1 255.0.0.0
!
ip classless
ip route 10.0.0.0 255.0.0.0 11.0.0.1
no ip http server
!
alias exec sc show module csm 7
!
line con 0
  exec-timeout 0 0
line vty 0 4
  password lab
  login
  transport input lat pad mop telnet rlogin udptn nasi
!
scheduler runtime netinput 300
end

```

STE-1

```

ssl-proxy-9#show run brief
Building configuration...
Current configuration : 1437 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!

```

```

hostname ssl-proxy-9
!
enable password lab
!
username braghu secret 5 $1$7Pdr$7dNm7l71.BJzELfi.QUzp/
ip subnet-zero
ip tftp source-interface Ethernet0/0.15
no ip domain lookup
!
ip ssh rsa keypair-name ssh-key
!
!
!--- Adds a proxy service HTTPS that identifies a
virtual IP address !--- and a server IP address for each
proxy.
ssl-proxy service https
  virtual ipaddr 12.0.0.123 protocol tcp port 443
secondary
  server ipaddr 12.0.0.124 protocol tcp port 80
  certificate rsa general-purpose trustpoint TP-2048-
pkcs12
  inservice
  !--- Configures this VLAN as administrative.
ssl-proxy vlan 15
  ipaddr 15.0.10.4 255.0.0.0
  gateway 15.0.100.1
  admin
  !--- Adds an interface to VLAN 4 on the SSL services
module.
ssl-proxy vlan 4
  ipaddr 12.0.0.50 255.0.0.0
  gateway 12.0.0.100
ssl-proxy mac address 00e0.b0ff.f0c4
!
!--- Declares the trustpoint that the module is to use.
crypto ca trustpoint TP-2048-pkcs12
  !--- Specifies the key pair to associate with the
certificate.
rsakeypair TP-2048-pkcs12
!
!--- Declares the trustpoint that the module is to use.
crypto ca trustpoint TP-1024-pkcs12
  !--- Specifies the key pair to associate with the
certificate.
rsakeypair TP-1024-pkcs12
  !--- Specifies the certificate and key to be
associated.
crypto ca certificate chain TP-2048-pkcs12
  certificate ca 313AD6510D25ABAE4626E96305511AC4
  certificate 3C2DF2E50001000000DC
crypto ca certificate chain TP-1024-pkcs12
  certificate 3C2CD2330001000000DB
  certificate ca 313AD6510D25ABAE4626E96305511AC4
!
ip classless
ip route 0.0.0.0 0.0.0.0 15.0.100.1
ip http server
!
no cdp run
!
line con 0
  exec-timeout 0 0
line 1 3
no exec

```



```
transport input all
flowcontrol software
line vty 0 1
  exec-timeout 0 0
  password lab
  login
line vty 2 4
  exec-timeout 0 0
  password lab
  login
  no exec
  flowcontrol software
!
end
```

7606

```
7606-2#show run
Building configuration...
Current configuration : 7375 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 7606-2
!
boot system flash slot0:
enable password lab
!
!--- Configures the VLANs allowed over the trunk to the
SSL services module. !--- The admin VLAN is included.
The SSL module is located in slot 3.
ssl-proxy module 3 allowed-vlan 4,15
ip subnet-zero
!
no ip domain-lookup
ip host mat 223.255.254.228
ip host defib 223.255.254.242
!
mls flow ip destination
mls flow ipx destination
!
spanning-tree extend system-id
no spanning-tree vlan 2,10
!--- The CSM is located in slot 5. The module running
as Active.
module ContentSwitchingModule 5
  vlan 3 client
    ip address 12.0.0.24 255.0.0.0
    gateway 12.0.0.100
  !
  vlan 4 server
    ip address 12.0.0.24 255.0.0.0
  !
  vlan 5 server
    ip address 20.0.0.24 255.0.0.0
    alias 20.0.0.100 255.0.0.0
  !
  probe ICMP icmp
    interval 5
```

```
failed 10
!
!--- These are the server farm HTTP and real server
members. serverfarm HTTP
  nat server
  no nat client
  real 20.0.0.7
  inservice
  real 20.0.0.8
  inservice
  real 20.0.0.9
  inservice
  real 20.0.0.10
  inservice
  real 20.0.0.11
  inservice
  real 20.0.0.12
  inservice
!
!--- These are the server farm HTTPS and real server
members. serverfarm HTTPS
  no nat server
  no nat client
  real 12.0.0.50
  inservice
  real 12.0.0.51
  inservice
  probe ICMP
!
sticky 1 ssl timeout 5
sticky 2 netmask 255.0.0.0 timeout 5
!
!--- Virtual server HTTP.
vserver HTTP
  !--- The virtual server IP address is specified with
  TCP port www.
  virtual 12.0.0.124 tcp www
!--- This is the VLAN from where the CSM accepts traffic
for a specified !--- virtual server.
  vlan 4
  !--- This is the destination server farm.
  serverfarm HTTP
  sticky 5 group 2
  !--- Enables connection redundancy. !--- Replicates
the sticky database to the backup CSM.
  replicate csrp sticky
  !--- Replicates connections to the backup CSM.
  replicate csrp connection
  persistent rebalance
  inservice
!
!--- This is the virtual server HTTPS.
vserver HTTPS
  !--- The virtual server IP address is specified with
  TCP port HTTP over SSL.
  virtual 12.0.0.123 tcp https
  !--- This is the VLAN from where the CSM accepts
traffic for a specified !--- virtual server.
  vlan 3
  !--- Destination server farm.
  serverfarm HTTPS
  !--- The CSM load balances an incoming SSL connection
to the SSL !--- termination engine that generated that
SSL ID.
```

```
ssl-sticky offset 20 length 6
sticky 5 group 1
  !--- Enables connection redundancy. !--- Replicates
the sticky database to the backup CSM.
  replicate csrp sticky
    !--- Replicates connections to the backup CSM.
  replicate csrp connection
    no persistent rebalance
    inservice
!
ft group 1 vlan 2
!
redundancy
mode rpr-plus
main-cpu
  auto-sync running-config
  auto-sync standard
!
interface Loopback0
ip address 192.10.10.3 255.255.255.0
!
interface GigabitEthernet1/1
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-5,1002-1005
switchport mode trunk
no cdp enable
!
interface GigabitEthernet1/2
no ip address
shutdown
no cdp enable
!
interface FastEthernet2/1
no ip address
switchport
switchport access vlan 5
switchport mode access
no cdp enable
!
interface FastEthernet2/2
no ip address
switchport
switchport access vlan 5
switchport mode access
no cdp enable
!
interface FastEthernet2/3
no ip address
switchport
switchport access vlan 5
switchport mode access
no cdp enable
!
interface FastEthernet2/13
ip address 11.0.0.6 255.0.0.0
no ip redirects
no cdp enable
standby 2 ip 11.0.0.100
standby 2 preempt
standby 2 name Client-Side
!
interface FastEthernet2/48
```

```
no ip address
switchport
switchport access vlan 15
switchport mode access
no cdp enable
!
interface Vlan1
no ip address
shutdown
!
interface Vlan3
ip address 12.0.0.2 255.0.0.0
no ip redirects
standby 1 ip 12.0.0.100
standby 1 preempt
standby 1 name CSM-Side
standby 1 track FastEthernet2/13
!
interface Vlan15
ip address 15.0.1.2 255.0.0.0
!
ip classless
ip route 10.0.0.0 255.0.0.0 11.0.0.1
no ip http server
!
no cdp run
!
alias exec sc show module csm 5
!
line con 0
exec-timeout 0 0
line vty 0 4
password lab
login
transport input lat pad mop telnet rlogin udptn nasi
!
end
```

STE-2

```
ssl-proxy-3#show run br
Building configuration...
Current configuration : 1216 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ssl-proxy-3
!
enable password lab
!
ip subnet-zero
ip tftp source-interface Ethernet0/0.15
no ip domain lookup
ip host defib 223.255.254.242
ip host mat 223.255.254.228
!
!
!
```

```
!--- Adds a proxy service HTTPS that identifies a
virtual IP address !--- and a server IP address for each
proxy.
ssl-proxy service https
  virtual ipaddr 12.0.0.123 protocol tcp port 443
secondary
  server ipaddr 12.0.0.124 protocol tcp port 80
  certificate rsa general-purpose trustpoint TP-2048-
pkcs12
  inservice
!--- Configures this VLAN as administrative.
ssl-proxy vlan 15
  ipaddr 15.0.10.5 255.0.0.0
  gateway 15.0.100.1
  admin
!--- Adds an interface to VLAN 4 on the SSL services
module.
ssl-proxy vlan 4
  ipaddr 12.0.0.51 255.0.0.0
  gateway 12.0.0.100
ssl-proxy mac address 0001.6446.a1c0
!
!--- Declares the trustpoint that the module is to use.
crypto ca trustpoint TP-2048-pkcs12
  !--- Specifies key pair to associate with the
certificate.
  rsakeypair TP-2048-pkcs12
  !--- Specifies the certificate and key to be
associated.
  crypto ca certificate chain TP-2048-pkcs12
    certificate 3C2DF2E50001000000DC
    certificate ca 313AD6510D25ABAE4626E96305511AC4
  !
  !
  !
  !
ip classless
ip route 0.0.0.0 0.0.0.0 15.0.100.1
ip http server
!
!
no cdp run
!
line con 0
  exec-timeout 0 0
line 1 3
  no exec
  transport input all
  flowcontrol software
line vty 0 1
  exec-timeout 0 0
  password lab
  login
line vty 2 4
  exec-timeout 0 0
  password lab
  login
  no exec
  flowcontrol software
!
end
```

Verificación

Utilice esta información para verificar su configuración:

```
Router# sh module contentSwitchingModule all vservers
```

- **muestre a proxy SSL el servidor/el cliente del servicio** — Este comando muestra cómo visualizar el estatus del servicio de representación del servidor SSL.
- **Mod de la demostración** — Este comando muestra el estatus del VLA N entre el módulo de servicios SSL y el Supervisor Engine.
- **muestre al proxy SSL stats hdr** — Este comando muestra cómo visualizar la información de inserción de encabezado.
- **muestre a proxy SSL el SSL stats** — Este comando muestra cómo visualizar las estadísticas del SSL.
- **muestre a proxy SSL el servicio stats y muestre el recurso seguro** — estos comandos show cómo visualizar las estadísticas para mostrar que el Equilibrio de carga está ocurriendo en dos módulos de servicios SSL.
- **muestre a proxy SSL la estafa** — Este comando muestra cómo visualizar las estadísticas cuando las conexiones son activas.

Troubleshooting

Refiera a los [servicios del proxy SSL de la prueba](#) para los consejos de Troubleshooting.

Información Relacionada

- [Soporte del hardware del módulo content switching](#)
- [Descargas del software del módulo content switching \(clientes registrados solamente\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)