

CSM和SSL服务模块初始配置示例

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Configure](#)

[Network Diagram](#)

[配置](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

[Introduction](#)

本文为配置内容交换模块(CSM)提供一配置示例用安全套接字层SSL。

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

本文档中的信息基于以下软件和硬件版本：

- 运行Cisco IOS 12.1的Cisco 7202路由器
- 运行IOS 12.1的Cisco Catalyst 6509
- 与SSL终端引擎(STE)运行IOS 12.2(11)和SSL(0.86)的功能集的CSM
- 运行IOS 12.1的Cisco 7606 Router
- CSM修造3.1(0.119)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

[Conventions](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

1. SSL在CSM的连接复制
2. 在CSM的SSL粘贴复制
3. CSM故障切换与SSL的连接的打开
4. 活动MSFC故障切换与开放SSL的连接
5. 机箱故障切换与SSL连接的打开
6. SSL在同一连接的连接重新协商和恢复与新的SSL连接(新功能)
7. 与多SSL连接的CSM粘贴功能与恢复

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 csrpf sticky  
!--- Replicates connections to the backup CSM.  
replicate csrpf 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$7dNm7l7l.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

```

Verify

请使用此信息验证您的配置：

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

- **显示SSL代理服务服务器/客户端**—此命令显示如何显示SSL服务器代理服务的状况。
- **show mod** —此命令显示VLAN的状态在SSL服务模块和Supervisor引擎之间的。
- **显示SSL代理stats hdr** —此命令显示如何显示报头插入信息。
- **显示SSL代理stats ssl** —此命令显示如何显示SSL统计数据。

- [显示SSL代理stats服务和show standby](#) —这些show命令如何显示统计数据表示，负载均衡在两SSL服务模块发生。
- [显示SSL代理联系人](#)—，当连接是活跃的时，此命令显示如何显示统计数据。

[Troubleshoot](#)

参考[测试SSL代理服务故障检修提示](#)的。

[Related Information](#)

- [内容交换模块硬件技术支持](#)
- [内容交换模块软件下载\(仅限注册用户\)](#)
- [Technical Support & Documentation - Cisco Systems](#)