

# Table of Contents

<b><u>SSL Module with a CSM in Bridge Mode Configuration Example</u></b> .....	<b>1</b>
<u>Document ID: 59741</u> .....	1
<u>Introduction</u> .....	1
<u>Before You Begin</u> .....	1
<u>Requirements</u> .....	1
<u>Components Used</u> .....	1
<u>Conventions</u> .....	1
<u>Configure</u> .....	2
<u>Network Diagram</u> .....	2
<u>Configurations</u> .....	4
<u>Verify</u> .....	7
<u>Troubleshoot</u> .....	8
<u>Related Information</u> .....	8

# SSL Module with a CSM in Bridge Mode Configuration Example

Document ID: 59741

---

## Introduction

### Before You Begin

Requirements

Components Used

Conventions

### Configure

Network Diagram

Configurations

### Verify

### Troubleshoot

### Related Information

---

## Introduction

This document provides a sample configuration for handling HTTPS traffic with a Secure Socket Layer Module (SSLM) and load balancing the decrypted traffic with a Content Switch Module (CSM).

In this example, the CSM is configured in bridge mode. The client VLAN and server VLAN share the same IP address. The same virtual IP address is also configured on the CSM and on the SSLM. This requires some special attention, which you see later in this document.

## Before You Begin

### Requirements

Before attempting this configuration, please ensure that you meet these requirements:

- The SSL module is accessible via console or Telnet.

### Components Used

The information in this document is based on these hardware and software versions.

- CSM version 3.x or higher
- SSL module version 2.1

### Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

# Configure

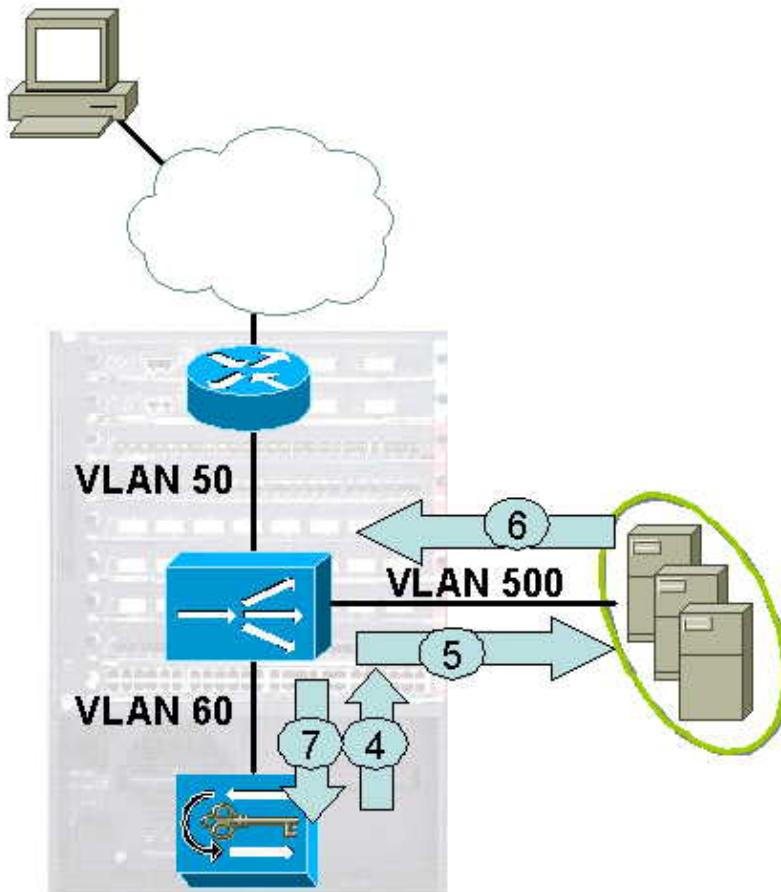
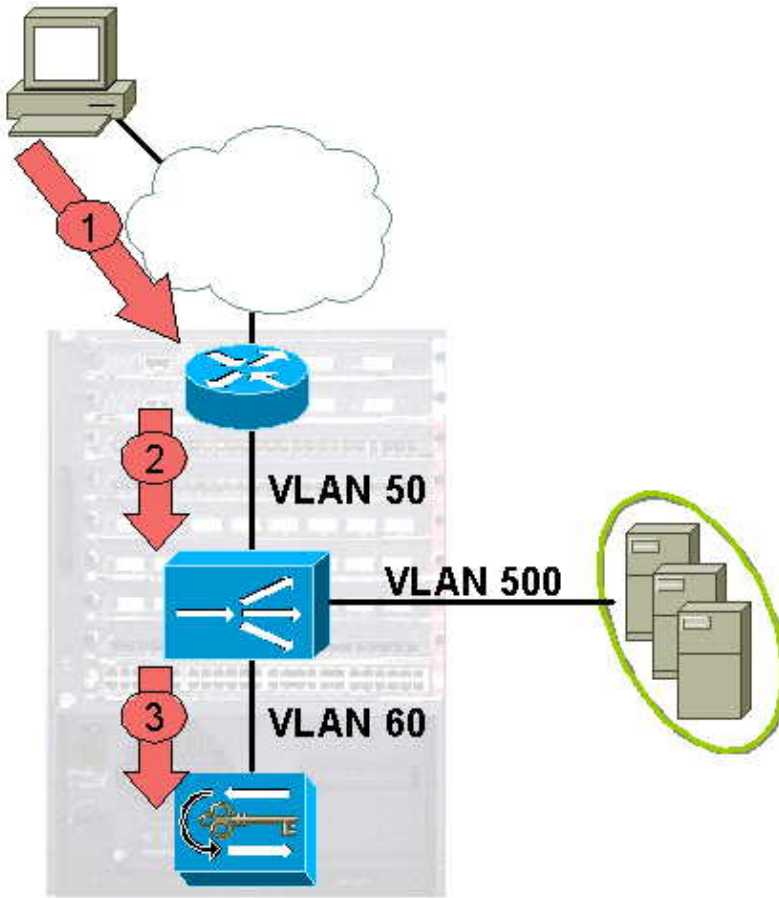
In this section, you are presented with the information to configure the features described in this document.

This is a description of the traffic path based on the network diagram below:

1. The HTTPS connection is opened by the client 192.168.11.41 to the vserver IP address 192.168.21.246 on port 443.
2. Traffic is forwarded by the MSFC to the CSM on VLAN 50.
3. Traffic hits the CSM vserver SSL 21 (see configuration), and is load balanced between the SSL module (in this case, only one). Only MAC addresses are modified; the IP addresses are not changed.
4. The SSL module decrypts the HTTPS request from the client and opens an HTTP connection with the CSM VIP 192.168.21.246 on port 80.
5. The CSM load balances this connection to one of the servers.
6. The server response is sent to the CSM.
7. The CSM forwards the response to the SSLM.
8. The SSLM encrypts the traffic from the server, and forwards it to the client through the CSM.

## Network Diagram

This document uses this network setup



Cisco – SSL Module with a CSM in Bridge Mode Configuration Example



# Configurations

This document uses this configuration:

```
msfc1#show running-config
Building configuration...
.

!--- On the MSFC, you need to configure the VLANs that are
!--- used by the SSL module. This automatically sets up the
!--- trunk between the Cat6k and the SSLM.

ssl-proxy module 1 allowed-vlan 60,499-501

!--- This is the CSM configuration.

module ContentSwitchingModule 4
  vlan 50 client

!--- This is the VLAN between MSFC and CSM. This VLAN is bridged
!--- by the CSM with the server VLAN 500.

  ip address 192.168.20.97 255.255.254.0
  gateway 192.168.21.97
  !
  vlan 500 server
  ip address 192.168.20.97 255.255.254.0
  !
  vlan 60 server

!--- This is the VLAN between CSM and SSLM.

  ip address 192.168.60.1 255.255.255.0
  alias 192.168.60.254 255.255.255.0
  !
  serverfarm MYLINUX

!--- These are the HTTP servers.

  nat server

!--- A NAT server is required to translate the VIP address to the
!--- server IP address.

  no nat client
  real 192.168.21.3
  inservice
  real 192.168.21.4
  inservice
  !
  serverfarm SSLACC

!--- This is the SSL module serverfarm. You can list more than one module
!--- here.

  no nat server
```

*!--- You do not want to NAT the server IP address because the SSLM uses  
!--- the same VIP as the CSM.*

```
no nat client
real 192.168.60.2
inservice
```

*!--- This is the SSLM interface IP address.*

```
!
vserver SSL21
```

*!--- The vserver handles the HTTPS traffic from the client.*

```
virtual 192.168.21.246 tcp https
vlan 50
```

*!--- The **vlan 50** command limits the access to this VIP  
!--- to traffic coming from the MSFC vlan 50.*

```
serverfarm SSLACC
```

*!--- You need to link the SSL modules to this vserver.*

```
no persistent rebalance
```

*!--- HTTPS traffic cannot be rebalanced due to encryption.*

```
inservice
!
vserver WWW21
```

*!--- The vserver handles HTTP traffic from VLAN 60.  
!--- This is the decrypted traffic forwarded by the SSLM.*

```
virtual 192.168.21.246 tcp www
```

*!--- You can reuse the same VIP address, but a different TCP port.*

```
vlan 60
serverfarm MYLINUX
```

*!--- You can link the servers to this VIP.*

```
persistent rebalance
```

*!--- Persistent rebalance is possible for HTTP traffic.*

```
inservice
!
interface Vlan499
```

*!--- This is the MSFC interface to the clients.*

```
ip address 192.168.11.97 255.255.254.0
!  
interface Vlan50
```

*!--- This is the MSFC interface to the CSM.*

```
ip address 192.168.21.97 255.255.254.0
!
```

This is the SSLM configuration:

```
ssl-proxy#sho run  
Building configuration...  
  
Current configuration : 23095 bytes  
!  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname ssl-proxy  
!  
logging queue-limit 100  
enable password ww  
!  
spd headroom 512  
ip subnet-zero  
ip tftp source-interface Ethernet0/0.499  
ip domain name cisco.com  
!  
!  
ssl-proxy service ssl21  
virtual ipaddr 192.168.21.246 protocol tcp port 443 secondary
```

*!--- The keyword secondary is necessary since the VIP address  
!--- is not part of any VLAN configured on the SSLM.*

```
server ipaddr 192.168.60.254 protocol tcp port 80
```

*!--- The server IP address is the alias IP address of the CSM.*

```
certificate rsa general-purpose trustpoint stefano  
no nat server
```

*!--- You need to disable server NAT; this is traffic that is forwarded back  
!--- to the CSM MAC address with the VIP address as the destination.*

```
trusted-ca ca-servidor-pool  
inservice  
ssl-proxy vlan 60  
ipaddr 192.168.60.2 255.255.255.0  
gateway 192.168.60.254  
!  
crypto ca trustpoint stefano  
crl optional  
rsakeypair stefano
```

```

!
crypto ca certificate chain stefano
  certificate 02
  certificate ca 00
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.60.254
no ip http server
no ip http secure-server
!
!
no cdp run
!
line con 0
  exec-timeout 0 0
line 1 3
  no exec
  transport input all
  flowcontrol software
line vty 0 4
  password ww
  login
!
end

```

## Verify

This section provides information you can use to confirm your configuration is working properly.

- **show mod csm X vserver name name detail** issue this command to verify that traffic hits the vserver. Make sure packets are received from both direction client and server. If you do not see any hits, try to ping the VIP. Make sure the VIP status is OPERATIONAL. If you do not see server packets, check the connectivity between CSM and SSLM.

```

msfc1#sho mod csm 4 vser name ssl21 det
SSL21, type = SLB, state = OPERATIONAL, v_index = 21
  virtual = 192.168.21.246/32:443 bidir, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = none, vlan = 50, pending = 30, layer 4
  max parse len = 2000, persist rebalance = TRUE
  ssl sticky offset = 0, length = 32
  conns = 0, total conns = 2
  Default policy:
    server farm = SSLACC, backup = <not assigned>
    sticky: timer = 0, subnet = 0.0.0.0, group id = 0
  Policy          Tot matches  Client pkts  Server pkts
  -----
  (default)      2             18           12

```

```

msfc1#sho mod csm 4 vser name www21 det
WWW21, type = SLB, state = OPERATIONAL, v_index = 22
  virtual = 192.168.21.246/32:80 bidir, TCP, service = NONE, advertise = FALSE
  idle = 3600, replicate csrp = none, vlan = 60, pending = 30, layer 4
  max parse len = 2000, persist rebalance = TRUE
  ssl sticky offset = 0, length = 32
  conns = 0, total conns = 2
  Default policy:
    server farm = MYLINUX, backup = <not assigned>
    sticky: timer = 0, subnet = 0.0.0.0, group id = 0
  Policy          Tot matches  Client pkts  Server pkts
  -----
  (default)      2             11           7

```

- **show mod csm X conns detail** issue this command to verify that packets are seen from client and server. Failure to see packets from the server could be an indication that the server has the wrong default gateway, and traffic is bypassing the CSM on the return path.

This command verifies that there are connections on the CSM. In this example, you can see that client 192.168.11.41 opened a connection from TCP port 1741 to the VIP 192.168.21.246:443 on VLAN 50. This traffic was forwarded with an IP address that was not changed (no NAT server and no nat client) to the SSLM. The SSLM opened an HTTP connection on behalf of the client to the vserver www21, and the CSM load balanced the connection to the server 192.168.21.4.

```
msfc1#show mod csm 4 conn det
```

	prot	vlan	source	destination	state
In	TCP	50	192.168.11.41:1741	ESTAB	
Out	TCP	60	192.168.21.246:443	192.168.11.41:1741	ESTAB
vs = SSL21, ftp = No, csrp = False					
In	TCP	60	192.168.11.41:1741	192.168.21.246:80	ESTAB
Out	TCP	500	192.168.21.4:80	192.168.11.41:1741	ESTAB
vs = WWW21, ftp = No, csrp = False					

- **show ssl-proxy service name** this SSL module command is very important. This command provides the status of the SSL-proxy service. Make sure the Admin and Operation Status are both up.

```
ssl-proxy#show ssl-proxy service ssl21
Service id: 3, bound_service_id: 259
Virtual IP: 192.168.21.246, port: 443 (secondary configured)
Server IP: 192.168.60.254, port: 80
Certificate authority pool: ca-servidor-pool
CA pool complete
rsa-general-purpose certificate trustpoint: stefano
Certificate chain for new connections:
Certificate:
  Key Label: stefano, 1024-bit, not exportable
  Key Timestamp: 13:52:23 UTC Apr 27 2004
  Serial Number: 02
Root CA Certificate:
  Serial Number: 00
Certificate chain complete

Admin Status: up
Operation Status: up
```

## Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

## Related Information

- [Content Switching Module Hardware Support](#)
- [Cisco Cat 6000 Other Intelligent Module SW Software Downloads \(registered customers only\)](#)
- [Technical Support – Cisco Systems](#)

