



Preface	xiii
Audience	xiii
Organization	xiv
Conventions	xv
Safety Overview	xvi
Related Documentation	xxi
Obtaining Documentation	xxii
Cisco.com	xxii
Documentation DVD	xxii
Ordering Documentation	xxiii
Documentation Feedback	xxiii
Cisco Product Security Overview	xxiii
Reporting Security Problems in Cisco Products	xxiv
Obtaining Technical Assistance	xxiv
Cisco Technical Support Website	xxiv
Submitting a Service Request	xxv
Definitions of Service Request Severity	xxv
Obtaining Additional Publications and Information	xxvi
Licenses	xxvi
CHAPTER 1	
Product Overview	1-1
Features	1-2
Front Panel Description	1-8
LEDs	1-8
RJ-45 Connector	1-9
SSL Connector	1-9
CSM-S and SSL Services Module Command Differences	1-10
Software Version Information	1-10
Configuration Restrictions	1-12
CSM-S Operation Overview	1-12
CSM-S Operation with SSL	1-14
Client-Side Configuration Traffic Flow	1-15
Server-Side Configuration Traffic Flow	1-17

Configuring the CSM as the Back-End Server 1-17
 Configuring the Real Server as the Back-End Server 1-18

CHAPTER 2

Networking with the Content Switching Module with SSL 2-1

Configuring Modes for Networking 2-1
 Configuring the Single Subnet (Bridge) Mode 2-1
 Configuring the Secure (Router) Mode 2-3
 CSM-S Networking Topologies 2-4
 CSM-S Inline and MSFC Not Involved 2-4
 CSM-S Inline and MSFC on Server Side 2-5
 CSM-S Inline and MSFC on Client Side 2-5
 CSM-S in Aggregate Mode 2-6
 Direct Server Return 2-6
 Routing with the CSM-S 2-7
 Protecting Against Denial-of-Service Attacks 2-7

CHAPTER 3

Getting Started 3-1

Configuration Overview 3-1
 Operating System Support 3-4
 Preparing to Configure the CSM-S 3-4
 Using the Command-Line Interface 3-5
 Accessing Online Help 3-6
 Saving and Restoring Configurations 3-6
 Configuring SLB Modes 3-6
 Mode Command Syntax 3-6
 Migrating Between Modes 3-7
 Differences Between the CSM and RP Modes 3-8
 CSM Mode 3-8
 RP Mode 3-9
 Changing Modes 3-9
 CSM Mode to RP Mode 3-10
 RP Mode to CSM Mode 3-10
 Verifying the Configuration 3-11
 Upgrading to a New Software Release 3-12
 Upgrading from the Supervisor Engine Bootflash 3-12
 Upgrading from a PCMCIA Card 3-13
 Upgrading from an External TFTP Server 3-14
 Recovering a Lost Password 3-14

CHAPTER 4

Configuring VLANs 4-1

- Configuring Client-Side VLANs 4-2
- Configuring Server-Side VLANs 4-3

CHAPTER 5

Configuring Real Servers and Server Farms 5-1

- Configuring Server Farms 5-1
- Configuring Real Servers 5-3
- Configuring Dynamic Feedback Protocol 5-5
- Configuring Client NAT Pools 5-6
- Configuring Server-Initiated Connections 5-7
- Configuring URL Hashing 5-7
 - Configuring a URL Hashing Predictor 5-8
 - Configuring Beginning and Ending Patterns 5-9

CHAPTER 6

Configuring Virtual Servers, Maps, and Policies 6-1

- Configuring Virtual Servers 6-1
 - Configuring TCP Parameters 6-4
 - Configuring Partial Serverfarm Failover 6-5
 - Configuring Virtual Server Dependency 6-6
 - Configuring Redirect Virtual Servers 6-6
- Configuring Maps 6-8
- Configuring Policies 6-10
- Configuring Generic Header Parsing 6-12
 - Understanding Generic Header Parsing 6-12
 - Generic Header Parsing Configuration 6-12
 - Creating a Map for the HTTP Header 6-13
 - Specifying Header Fields and Match Values 6-13
 - Assigning an HTTP Header Map to a Policy 6-13
 - Assigning the Policy to a Virtual Server 6-14
 - Generic Header Parsing Example 6-14

CHAPTER 7

Configuring the CSM-S SSL Services 7-1

- Initial SSL Daughter Card Configuration 7-2
 - Configuring VLANs on the SSL Daughter Card 7-2
- Configuring Telnet Remote Access 7-3
- Configuring the Fully Qualified Domain Name 7-3
- Configuring SSH 7-4
 - Enabling SSH on the Module 7-4

- Configuring the Username and Password for SSH 7-5
 - Configuring Authentication, Authorization, and Accounting for SSH 7-6
- Configuring SSL for Client-Side and Server-Side Operation 7-6
 - Configuring the Client Side 7-7
 - Configuring the Server Side 7-8
 - Configuring the CSM as the Back-End Server 7-8
 - Configuring the Real Server as the Back-End Server 7-9
- Configuring Policies 7-9
 - Configuring SSL Policy 7-10
 - Configuring TCP Policy 7-11
 - HTTP Header Insertion 7-13
 - Prefix 7-13
 - Client Certificate Headers 7-13
 - Client IP and Port Address Headers 7-14
 - Custom Headers 7-14
 - SSL Session Headers 7-15
 - Configuring the HTTP Header Insertion 7-15
 - Configuring URL Rewrite 7-16
- Configuring the SSL Proxy Services 7-18
 - SSL Server Proxy Services 7-18
 - SSL Version 2.0 Forwarding 7-20
 - SSL Client Proxy Services 7-20
- Configuring NAT 7-22
 - Server NAT 7-22
 - Client NAT 7-23
- Configuring TACACS, TACACS+, and RADIUS 7-23
- Configuring SNMP Traps 7-24
- Enabling the Cryptographic Self-Test 7-25
 - Displaying Statistics Information 7-25
- Collecting Crash Information 7-28
- Enabling VTS Debugging 7-30

CHAPTER 8

- Configuring SSL Services Secure Transactions 8-1**
 - Configuring the Public Key Infrastructure 8-1
 - Configuring the Keys and the Certificates 8-2
 - Configuring the Trustpoint Using SCEP 8-5
 - Manual Certificate Enrollment 8-11
 - Importing and Exporting the Key Pairs and Certificates 8-19

Importing the PEM Files for Three Levels of Certificate Authority	8-23
Verifying the Certificates and the Trustpoints	8-27
Sharing the Keys and the Certificates	8-27
Configuring a Root CA (Trusted Root)	8-28
Saving Your Configuration	8-29
Oversized Configuration	8-29
Verifying the Saved Configuration	8-30
Erasing the Saved Configuration	8-30
Backing Up the Keys and the Certificates	8-30
Security Guidelines	8-30
Monitoring and Maintaining the Keys and Certificates	8-31
Deleting the RSA Keys from the Module	8-31
Displaying the Keys and Certificates	8-32
Deleting the Certificates from the Configuration	8-32
Assigning a Certificate to a Proxy Service	8-32
Renewing a Certificate	8-34
Configuring the Automatic Certificate Renewal and Enrollment	8-36
Enabling the Key and Certificate History	8-37
Caching the Peer Certificates	8-37
Configuring the Certificate Expiration Warning	8-38
Configuring the Certificate Authentication	8-40
Client Certificate Authentication	8-41
Server Certificate Authentication	8-43
Certificate Revocation List	8-47
Downloading the CRL	8-47
Configuring the CRL Options	8-48
Updating a CRL	8-49
Entering the X.500 CDP Information	8-49
Entering a CRL Manually	8-50
Displaying the CRL Information	8-51
Deleting a CRL	8-51
Certificate Security Attribute-Based Access Control	8-51

CHAPTER 9

Configuring Redundancy 9-1

Configuring Fault Tolerance	9-1
Configuring HSRP	9-5
HSRP Configuration Overview	9-5
Creating the HSRP Gateway	9-6
Creating Fault-Tolerant HSRP Configurations	9-7

- Configuring Interface and Device Tracking 9-8
 - Tracking an HSRP Group 9-8
 - Tracking a Gateway 9-9
 - Tracking an Interface 9-9
 - Configure the Tracking Mode 9-9
- Configuring Connection Redundancy 9-9
- Synchronizing the Configuration 9-11
- Configuring a Hitless Upgrade 9-12

CHAPTER 10

- Configuring Additional Features and Options 10-1**
 - Configuring Session Persistence (Stickiness) 10-1
 - Configuring Sticky Groups 10-3
 - Cookie Insert 10-4
 - Cookie Sticky Offset and Length 10-4
 - URL-Learn 10-4
 - Configuring Route Health Injection 10-5
 - Understanding RHI 10-5
 - RHI Overview 10-6
 - Routing to VIP Addresses Without RHI 10-6
 - Routing to VIP Addresses With RHI 10-7
 - Understanding How the CSM-S Determines VIP Availability 10-7
 - Understanding Propagation of VIP Availability Information 10-7
 - Configuring RHI for Virtual Servers 10-7
 - Environmental Variables 10-8
 - Configuring Persistent Connections 10-14
 - HTTP Header Insert 10-15
 - Configuring Global Server Load Balancing 10-16
 - Using the GSLB Advanced Feature Set Option 10-16
 - Configuring GSLB 10-17
 - Configuring Network Management 10-21
 - Configuring SNMP Traps for Real Servers 10-21
 - Configuring the XML Interface 10-21
 - Configuring Server Application State Protocol 10-25
 - Configuring SASP Groups 10-25
 - Configuring a GWM 10-25
 - Configuring Alternate bind_ids 10-26
 - Configuring a Unique ID for the CSM-S 10-26
 - Configuring Weight Scaling 10-27

Back-End Encryption	10-28
Configuring the Client Side	10-28
Configuring the Server Side	10-29
Configuring the CSM-S as the Back-End Server	10-30
Configuring the Real Server as the Back-End Server	10-31

CHAPTER 11

Configuring Health Monitoring	11-1
Configuring Probes for Health Monitoring	11-1
Probe Configuration Commands	11-3
Configuring an HTTP Probe	11-4
Configuring an ICMP Probe	11-5
Configuring a UDP Probe	11-5
Configuring a TCP Probe	11-6
Configuring FTP, SMTP, and Telnet Probes	11-6
Specifying the DNS Resolve Request	11-7
Configuring GSLB Probes	11-7
Understanding and Configuring Inband Health Monitoring	11-8
Understanding Inband Health Monitoring	11-8
Configuring Inband Health Monitoring	11-8
Understanding and Configuring HTTP Return Code Checking	11-9
Understanding HTTP Return Code Checking	11-9
Configuring HTTP Return Code Checking	11-10

CHAPTER 12

Using TCL Scripts with the CSM-S	12-1
Loading Scripts	12-2
Examples for Loading Scripts	12-2
Reloading TCL Scripts	12-3
TCL Scripts and the CSM-S	12-3
Probe Scripts	12-7
Example for Writing a Probe Script	12-8
Environment Variables	12-9
Exit Codes	12-9
EXIT_MSG Variable	12-10
Running Probe Scripts	12-11
Debugging Probe Scripts	12-13
Standalone Scripts	12-15
Example for Writing Standalone Scripts	12-15
Running Standalone Scripts	12-16
Debugging Standalone Scripts	12-16

TCL Script Frequently Asked Questions (FAQs) 12-17

CHAPTER 13

Configuring Firewall Load Balancing 13-1

- Understanding How Firewalls Work 13-1
 - Firewall Types 13-2
 - How the CSM-S Distributes Traffic to Firewalls 13-2
 - Supported Firewalls 13-2
 - Layer 3 Load Balancing to Firewalls 13-2
 - Types of Firewall Configurations 13-3
 - IP Reverse-Sticky for Firewalls 13-3
 - CSM-S Firewall Configurations 13-3
 - Fault-Tolerant CSM-S Firewall Configurations 13-6
- Configuring Stealth Firewall Load Balancing 13-7
 - Stealth Firewall Configuration 13-7
 - Stealth Firewall Configuration Example 13-8
 - Configuring CSM-S A (Stealth Firewall Example) 13-9
 - Configuring CSM-S B (Stealth Firewall Example) 13-12
- Configuring Regular Firewall Load Balancing 13-16
 - Packet Flow in a Regular Firewall Configuration 13-16
 - Regular Firewall Configuration Example 13-17
 - Configuring CSM-S A (Regular Firewall Example) 13-18
 - Configuring CSM-S B (Regular Firewall Example) 13-21
- Configuring Reverse-Sticky for Firewalls 13-24
 - Understanding Reverse-Sticky for Firewalls 13-24
 - Configuring Reverse-Sticky for Firewalls 13-26
- Configuring Stateful Firewall Connection Remapping 13-26

APPENDIX A

CSM-S Configuration Examples A-1

- Configuring the Router Mode with the MSFC on the Client Side A-1
- Configuring the Bridged Mode with the MSFC on the Client Side A-4
- Configuring the Probes A-5
- Configuring the Source NAT for Server-Originated Connections to the VIP A-7
- Configuring Session Persistence (Stickiness) A-9
- Configuring Direct Access to Servers in Router Mode A-10
- Configuring Server-to-Server Load-Balanced Connections A-12
- Configuring Route Health Injection A-14
- Configuring the Server Names A-16
- Configuring a Backup Server Farm A-19

Configuring a Load-Balancing Decision Based on the Source IP Address	A-24
Configuring Layer 7 Load Balancing	A-27
Configuring HTTP Redirect	A-29

 APPENDIX B

SSL Configuration Examples B-1

CSM-S Configuration Example (Bridge Mode, No NAT)	B-1
CSM-S Configuration Example (Router Mode, Server NAT)	B-7
CSM-S and SSLM Configuration Example (Router Mode, Server NAT)	B-12
Integrated Secure Content-Switching Service Example	B-16
Configuring the CSM	B-17
Configuring the SSL Daughter Card	B-18
Certificate Security Attribute-Based Access Control Examples	B-19
HTTP Header Insertion Examples	B-21
Example 1	B-21
Example 2	B-23
Example 3	B-24
URL Rewrite Examples	B-26
Example 1	B-26
Example 2	B-26
Example 3	B-27
Example 4	B-27

 APPENDIX C

Troubleshooting and System Messages C-1

Troubleshooting	C-1
System Messages	C-1
Server and Gateway Health Monitoring	C-5
Diagnostic Messages	C-5
Fault Tolerance Messages	C-6
Regular Expression Errors	C-6
XML Errors	C-7

 APPENDIX D

CSM XML Document Type Definition D-1

 INDEX

