

SSL SERVICES MODULE FOR THE CISCO CATALYST 6500 SERIES AND CISCO 7600 SERIES

The SSL Service Module is an integrated service module for the Cisco® Catalyst® 6500 Series and Cisco 7600 Series Internet Routers that offloads processor-intensive tasks related to securing traffic with Secure Sockets Layer (SSL), increases the number of secure connections supported by a Web site, and reduces the operational complexity of high-performance, Web server farms.

KEY FEATURES OF THE SSL SERVICE MODULE INCLUDE:

- *Server SSL offload*—performs all SSL-related tasks, allowing servers to handle high-speed clear text traffic
- *Scalable performance*—provides a simple means of addressing increased performance requirements by installing additional SSL modules in a Cisco Catalyst 6500 switch
- *Stickiness*—maintains persistence even when clients request new session IDs, in Integrated Mode with Content Switching Module (CSM)
- *Certificate optimization*—provides cost savings by requiring only a single certificate copy vs. a copy for each server subject to customer and certificate authority agreement
- *Backend encryption*—SSL Module offers end to end security by also encrypting the communication between Module and servers as well.

Up to four SSL service modules can be installed in each chassis providing the fastest SSL session setup rates and bulk encrypted throughput in the industry and supporting the highest number of concurrent connections:

- *3000 connection setups/second per module*—10,000 per Chassis fully-populated with SSL modules
- *300 Mbps bulk encrypted throughput per chassis module*—1.2 Gbps per fully-populated with SSL modules
- *64,000 concurrent client connections*—256,000 per chassis fully-populated with SSL modules

Figure 1



The SSL Service Module offloads all SSL processing, allowing the end Web and eCommerce servers to process more requests for content and handle more e-transactions—providing a multifold increase in the performance of eCommerce and secure sites using encryption.

As eCommerce continues to grow and involve more applications, security in business-to-consumer (B2C) and business-to-business (B2B) transactions becomes essential. In B2C transactions, analysts estimate that more than 70 percent of consumers avoid making online transactions for fear that someone will steal their credit card numbers. As a result, SSL has become the de facto standard for securing e-commerce transactions.

Businesses use the Internet to streamline operations, improve customer service, and close sales. Businesses are also moving legacy applications to the Web and opening them to intranet and extranet use—requiring them to provide high-speed, secure, authenticated access to confidential information. Increasingly, businesses are using SSL accelerators to perform authentication, encryption, and decryption processing.

MAJOR SSL SERVICE MODULE BENEFITS

In the old client/server SSL model, SSL processing is embedded within servers via SSL NIC cards. Drawbacks to this older model include:

- Persistent connections cannot be established and sessions are lost when clients request new SSL IDs, resulting in lost revenue
- Certificate copies must be purchased for each server in the server farm, increasing costs unnecessarily
- Web servers must be added to scale SSL transaction capacity, increasing costs and spreading disruption throughout the server farms
- Web servers waste processing capacity in establishing SSL sessions, driving up costs

Cisco responded to these drawbacks by introducing the integrated SSL Service Module, providing the following benefits:

Cost-Effective Solution

The SSL Service Module provides the best price/performance of any SSL accelerator on the market. Cost of maintenance is included in the maintenance contract of the Cisco Catalyst chassis, providing cost savings on annual service contracts. By offloading the processing-intensive SSL termination burden from the Web servers, the SSL Service Module eliminates the need to purchase additional servers. Multiple modules can be installed in a chassis, conserving rack space, which is especially important where rack space is at a premium.

Server SSL Offload

The SSL Service Module offloads the SSL termination function from the Web server, allowing the Web server to increase its performance accordingly. Further performance increases occur when a content switch, such as the Cisco CSM, load balances SSL traffic among SSL modules, using standard load balancing algorithms, and maintains SSL session ID stickiness with SSL modules.

Scalability Performance

Integrated Content Switching Modules or external load balancing appliances can load balance secure HTTPS content requests to multiple Cisco SSL service modules—maximizing SSL termination performance and providing SSL scalability. SSL modules offload SSL processing from Web servers allowing them to handle peak traffic demands without degrading the user experience. Because SSL processing is centralized in the switch, it can be scaled easily by adding additional modules, without interrupting processing.

Persistent Connections

In Integrated Mode, the SSL Service Module and CSM maintain persistent client-to-SSL device sessions when client browsers renegotiate SSL IDs or when the source IP addresses are modified—events that often occur in wireless traffic flows and when traffic moves through gateways. The SSL Service Module and CSM also maintain persistence by using cookie sticky to stick clients to Web servers—optimizing overall user experience. Additionally, when SSL modules are installed in redundant configurations, user session state is maintained even when hardware failures occur.

Ease of Management and Configuration

Additionally, the SSL Service Module integrates SSL processing within the infrastructure and allows any port on the Cisco Catalyst 6500 Switch to operate as an SSL port. The SSL Service Module simplifies security management while encrypting user data to the Web servers, providing privacy, confidentiality, and authentication using a wide range of certificates, including Netscape and VeriSign.

High Availability

When SSL modules and a CSM are installed in a Cisco Catalyst 6500 configuration, SSL traffic is maintained if failures occur. The failover capabilities of the SSL Module, and the Content Switching Module provide an extremely fault-tolerant solution.

Certificate Cost Reduction

SSL certificates reside on the Cisco SSL module that ‘front ends’ multiple Web servers, centralizing certificate management, eliminating the need to purchase/manage certificates for individual servers, and reducing licensing costs.

Table 1 SSL Service Module Features

Key Features	Benefits
System Capacity and Performance	<ul style="list-style-type: none">• 2500 connection setups/sec per module—10K per chassis• 60K concurrent client connections—240K per chassis• 300 Mbps bulk rate encryption—1.2 Gbps per chassis• 256 key pairs• 256 certificates• 512-bit, 768-bit, 1024-bit, 1536-bit, and 2048-bit• 256 proxy servers
Hash Algorithms	<ul style="list-style-type: none">• Message Digest 5 (MD5)• SHA1
Cipher Suites	<ul style="list-style-type: none">• SSL_RSA_WITH_RC4_128_MD5• SSL_RSA_WITH_RC4_128_SHA• SSL_RSA_WITH_DES_CBC_SHA• SSL_RSA_WITH_3DES_EDE_CBC_SHA
Handshake Protocol	<ul style="list-style-type: none">• SSL 3.0• SSL 3.1/TLS 1.0• SSL 2.0 (Client Hello)• Session reuse• Session renegotiation

Table 1 SSL Service Module Features (Continued)

Key Features	Benefits
Algorithms	<ul style="list-style-type: none"> • ARC4 • DES • 3DES • RSA
Public Key Infrastructure	<ul style="list-style-type: none"> • RSA key pair generation • Server certificate enrollment • Server key and certificate import • Server key and certificate export • Key and certificate renewal • Auto-enrollment of server certificates
Network Address Translation	<ul style="list-style-type: none"> • Client NAT • Server NAT/Port Address Translation (PAT)
Scalability	<ul style="list-style-type: none"> • Multiple SSL modules in the same box
High Availability	<ul style="list-style-type: none"> • CSM can balance traffic among multiple SSL modules
Integration with Server Load Balancing	<ul style="list-style-type: none"> • Tightly integrated in the Cisco Catalyst 6500 Switch with the CSM
Monitoring	<ul style="list-style-type: none"> • Various statistics and monitoring available for SSL sessions
Hot Swappable	<ul style="list-style-type: none"> • Online insertion and removal
Secure Key Storage	<ul style="list-style-type: none"> • Keys stored in private NVRAM storage
Standalone Mode	<ul style="list-style-type: none"> • Can be used in standalone configuration along with external server load balancing device
SSL Session ID Stickiness	<ul style="list-style-type: none"> • SSL module maintains the stickiness of the session
Backend encryption	This feature allows you to configure the SSL Services Module as an SSL client. When you configure an SSL proxy service for SSL client functionality, the SSL Services Module negotiates an SSL session with the server and uses that session to encrypt the clear-text data coming from the client connection.
Client Authentication	This feature allows you to configure the option to request and authenticate the client certificate when the SSL Services Module acts as a SSL server. The SSL Services Module automatically authenticates the server certificate when it acts as a SSL client. The feature specifies a set of trusted certificate authorities and the scope of validation for each proxy service.
Client Certificates	This feature allows you to configure a certificate for a client-type proxy service. When acting as an SSL client, the SSL Services Module sends this certificate for authentication if the SSL server requests it, and the issuer of this certificate is on the server's list of acceptable certificate authorities.
SSL 2.0 forwarding	This feature allows you to configure the SSL Services Module to forward SSLv2 connections to another server. When you configure the SSLv2 server IP address, the SSL Services Module transparently forwards all SSLv2 connections to that server.
Certificate revocation lists (CRL)	A CRL is a time-stamped list that identifies certificates that should no longer be trusted. When a participating peer device uses a certificate, that device not only checks the certificate signature and validity but also checks that the certificate serial number is not on that CRL.
HSRP based Redundancy	You can configure HSRP to provide redundancy when the SSL Services Module is used in a standalone configuration (using policy-based routing).

Table 1 SSL Service Module Features (Continued)

Key Features	Benefits
URL rewrite	URL rewrite rules resolve the problem of a Web site redirecting you to a nonsecure HTTP URL by rewriting the domain from http:// to https://. By configuring URL rewrite, all client connections to the Web server are SSL connections, ensuring the secure delivery of HTTPS content back to the client.
Header Insertion	This feature provides support for servers that require information inserted into an HTTP header.
Password Recovery	This feature allows you to access the SSL Services Module without any authentication using the password recovery script.
Wildcard Proxy	Wildcard SSL proxy provides a flexible network configuration interface if you have a large number of servers in your network.
TACACS/ACACS+/RADIUS	The feature allows you to configure external servers for authentication, authorization and accounting (AAA).
SNMP MIBs	Supports various MIBs using SNMP.
Certificate security attribute-based access control lists	This feature allows you to configure an access control list (ACL) that filters certificates based on certificate attribute values.
Certificate expiration warning	When you enable certificate expiration warnings, the SSL Services Module checks every 30 minutes for expiration information. The SSL Services Module can log warning messages and send SNMP traps when certificates have expired or will expire within a specified amount of time.

CONFIGURATION MODES AND TRAFFIC FLOW

The Cisco SSL Service Module can be installed in two basic configurations:

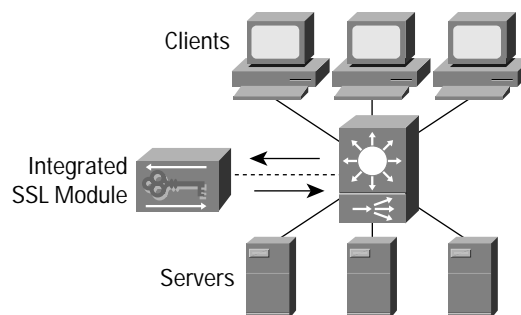
- *Integrated mode*—Integrated with the CSM
- *Standalone mode*—Using external server load balancer

Integrated Mode Configuration

As shown in Figure 2 the SSL Module when integrated with the CSM provides encrypted traffic flow and load-balanced connections between a client and server.

Figure 2

SSL Module Integrated Mode Configuration



The Clients send encrypted traffic on port 443, the standard SSL port. The CSM listens on port 443 and load balances the encrypted traffic to an internal “server farm” of SSL modules. The selected SSL Service Module decrypts the traffic, stamps it with a SSL Session ID, opens a clear-text connection to a Versatile Interface Processor (VIP) on the CSM, and sends the traffic to a port that has been configured to receive “decrypted SSL traffic”, for examples port 81.

The CSM receives the decrypted traffic, makes a load balancing decision to select a Web server, and forwards the traffic. When the CSM receives return traffic from the Web server, it sends it to the SSL Service Module that opened the connection.

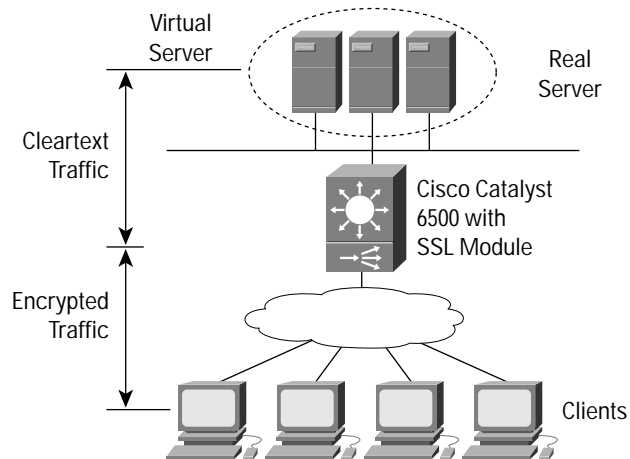
The SSL Module receives the unencrypted traffic, encrypts it, and sends it back to the CSM from port 443. The CSM receives the encrypted traffic and sends it back to the client.

Note: The selected SSL Module and the client use SSL Session IDs for all the TCP connections that make up that flow. The CSM also uses a portion of that SSL Session ID to stick the selected SSL Service Module to that client. If a client requests a new SSL session ID from the SSL Service Module, the CSM is able to keep the client and the selected SSL Service Module “stuck” together.

Standalone Mode with a CSS or Other Server Load Balancer

In Standalone mode, shown in Figure 3, the SSL Service Module is installed in the Cisco Catalyst 6500 chassis without server load balancing (either hardware or software) inside the chassis.

Figure 3
SSL Module Standalone Mode Configuration



The Cisco Catalyst 6500 uses ACLs containing entries that associate IP addresses and port numbers to direct traffic flows from clients to SSL modules and from servers to SSL modules. In the client-to-server direction, the ACL identifies data flows that need to be directed to server port 443, the SSL port. The Cisco Catalyst 6500 allows normal data traffic that is not associated with an ACL entry to go directly to a server, without first directing it to the SSL module.

The Standalone mode traffic flow is very similar to the flow in Integrated Mode, with the following exceptions:

- The SSL session ID sticky feature is not available
- Clients and servers must be on separate subnets
- The server may be a real server address, or the virtual address of a cluster of real servers
- Depending on the capability of the server load balancer, the cookie sticky feature may or may not be available

ORDERING INFORMATION

Product Number	Description
WS-SVC-SSL-1-K9	SSL Service Module
WS-SVC-SSL-1-K9=	Spare SSL Service Module
SC-SVC-SSL-1.1-K9	SSL Service Module Software Release 1.1
SC-SVC-SSL-1.1-K9=	Spare SSL Service Module Software Release 1.1
SC-SVC-SSL-2.1-K9	SSL Service Module Software Release 2.1
SC-SVC-SSL-2.1-K9=	Spare SSL Service Module Software Release 2.1

LICENSING

No licensing is required.

SYSTEM REQUIREMENTS

- Supervisor 720 or Supervisor 2/Multilayer Switch Feature Card 2 (MSFC2)
- Native Cisco IOS[®] software release 12.1(13)E or higher
- Hybrid CatOS minimum software release 7.5(1)
- Occupies one slot in a Cisco Catalyst 6500 Series Switch or Cisco 7600 Series Internet Router
- Max of four SSL modules in the same chassis

ENVIRONMENTAL CONDITIONS

Operating temperature: 32 to 104 F (0 to 40 C)

Storage temperature: -40 to 167 F (-40 to 75 C)

Relative humidity: 10% to 90%, noncondensing

Operating altitude: -60 to 4000 m

REGULATORY COMPLIANCE

Safety

UL 1950

CSA C22.2 No. 950-95

EN60950

EN60825-1

TS001

CE Marking

IEC 60950

AS/NZS3260

EMI	ITU-T G.826
FCC Part 15 Class A	ITU-T G.841
ICES-003 Class A	ITU-T G.957 Table 3
VCCI Class B	ITU-T G.958
EN55022 Class B	ITU-T I.361
CISPR22 Class B	ITU-T I.363
CE Marking	ITU I.432
AS/NZS3548 Class B	ITU-T Q.2110
NEBS	ITU-T Q.2130
SR-3580—NEBS: Criteria Levels (Level 3 Compliant)	ITU-T Q.2140
GR-63-CORE—NEBS: Physical Protection	ITU-T Q.2931
GR-1089-CORE—NEBS: EMC and Safety	ITU-T O.151
ETSI	ITU-T O.171
ETS-300386-2 Switching Equipment	ETSI ETS 300 417-1-1
Telecommunications	TAS SC BISDN (1998)
ITU-T G.610	ACA TS 026 (1997)
ITU-T G.703	BABT /TC/139 (Draft 1e)
ITU-T G.707	
ITU-T G.783 Sections 9-10	
ITU-T G.784	
ITU-T G.803	
ITU-T G.813	
ITU-T G.825	



Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Catalyst, Cisco, Cisco Systems, the Cisco Systems logo, Catalyst, and Cisco IOS are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0402R)
KC/WH/LW5833 0304