Overview

The SSL Services Module is a Layer 4-through-Layer 7 service module that you can install into the Catalyst 6500 series switch. The module terminates secure sockets layer (SSL) transactions and accelerates the encryption and decryption of data used in SSL sessions.

The module operates either in a standalone configuration or with the Content Switching Module (CSM). In a standalone configuration, secure traffic is directed to the module using policy-based routing (PBR). When used with the CSM, only encrypted client traffic is forwarded to the module, while clear text traffic is forwarded to the real servers.

The SSL Services Module uses the SSL protocol to enable secure transactions of data through privacy, authentication, and data integrity; the protocol relies upon certificates, public keys, and private keys.

The certificates, which are similar to digital ID cards, verify the identity of the server to the clients. The certificates, which are issued by certificate authorities, include the name of the entity to which the certificate was issued, the entity's public key, and the time stamps that indicate the certificate's expiration date.

The public and private keys are the ciphers that are used to encrypt and decrypt information. The public key is shared without any restrictions, but the private key is never shared. Each public-private key pair works together; data that is encrypted with the public key can only be decrypted with the corresponding private key.

These sections describe the SSL Services Module:

Features

The SSL Services Module has these features:

- Accelerates SSL transactions to help alleviate the server processing load
- Enables intelligent content switching using the CSM to load balance traffic through the server
- Provides centralized management (for the key, certificate, and configuration management)

Table 1-1 lists the available features.

Table 1-1 Feature Set Description

Features
Supported Hardware
Supervisor Engine 2 with MSFC2[1] and PFC2[2]
Supported Software
– Cisco IOS Release 12.1(13)E or later on the MSFC2 – Cisco IOS Release 12.1(13)E3 or later on the MSFC2 and Catalyst software release 7.5(1) or later on the Supervisor Engine 2 – SSL Services Module software release 1.1(1) or later on the SSL Services Module
Handshake Protocol
SSL 3.0
SSL 3.1/TLS 1.0
SSL 2.0 (only ClientHello support)
Session reuse
Session renegotiation
Session timeout[3]
Symmetric Algorithms
ARC4
DES
3DES
Asymmetric Algorithms
RSA
Hash Algorithms
MD5
SHA1
Cipher Suites
SSL_RSA_WITH_RC4_128_MD5
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_DES_CSC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
Public Key Infrastructure
RSA key pair generation for server certificates up to 2048-bit
Secure server key storage in SSL Services Module Flash memory device
Server certificate enrollment
Importing and exporting of server key and certificate (PKCS12 and PEM[3])
Duplicating keys and certificates on standby SSL Services Module using the key and certificate import and export mechanism

Table 1-1 Feature Set Description (continued)

Features
Public Key Infrastructure (continued)
Manual key archival, recovery, and backup
Key and certificate renewal using the CLI
Graceful rollover of expiring server keys and certificates
Auto-enrollment of server certificates
Exporting of PKCS10 CRT file for manual or offline certificate enrollment[3]
Importing of CA certificates by cut-and-paste or TFTP[3]
Up to 8 levels of Certificate Authority in a certificate chain[3]
Generating of self-signed certificate[3]
Manual certificate enrollment using cut-and-paste or TFTP[3]
TCP Termination
RFC 1323
Connection aging
Connection rate
Up to 64,000 concurrent client connections
Up to 192,000 concurrent connections (includes 2 MSL[4])
Up to 300 Mbps throughput
NAT[5]
Client NAT
Server NAT/PAT[6]
Scalability
Multiple modules in a single chassis when used with the CSM[7]; the CSM provides server load balancing (SLB)
High Availability
Failure detection (SLB[8] health monitoring schemes)
System-level redundancy (stateless) (when used with the CSM)
Module-level redundancy (stateless) (when used with the CSM)
Serviceability
OIR[9] (after properly shutdown)
Graceful shutdown
Statistics and Accounting
Total SSL connections attempt per virtual server
Total SSL connections successfully established per virtual server
Total SSL connections failed per virtual server
Total SSL alert errors per virtual server

Table 1-1 Feature Set Description (continued)

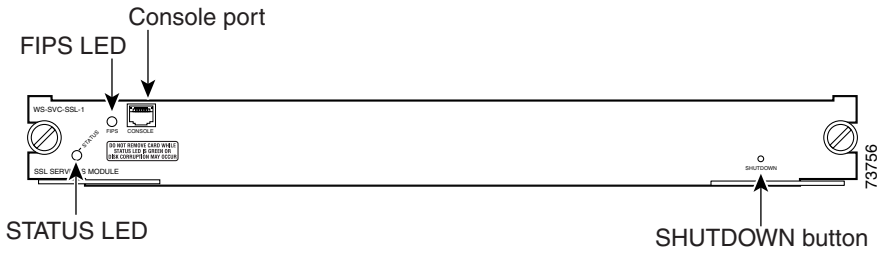
Features
Statistics and Accounting (continued)
Total SSL resumed sessions per virtual server
Total encrypted/decrypted packets/bytes per virtual server
Statistics displayed at 1 second, 1 minute, and 5 minutes traffic rate for CPU utilization and SSL-specific counters
Configuration and Management
Direct connection to the module console port
Secure Shell (SSHv1) session
Telnet
Automatic backup and restore of configuration file to NVRAM[3]
System Capacity and Performance
Up to 300 Mbps throughput
Up to 256 proxy servers
Up to 64,000 simultaneous sessions
Stores up to 356 key pairs
Stores up to 356 certificates
Supports the following RSA key sizes: – 512-bits – 768-bits – 1024-bits – 1536-bits – 2048-bits
Up to 3000 sessions per second

1. MSFC = Multilayer Switch Feature Card
2. PFC = Policy Feature Card
3. New feature in SSL software release 1.2(1).
4. MSL = Maximum Segment Lifetime
5. NAT = Network Address Translation
6. PAT = Port Address Translation
7. CSM = Content Switching Module
8. SLB = Server Load Balancing
9. OIR = Online Insertion and Removal

Front Panel Description

The SSL Services Module front panel (see Figure 1-1) includes a STATUS LED, a Federal Information Processing Standards (FIPS) LED, a SHUTDOWN button, and a console port.

Figure 1-1 SSL Services Module Front Panel



These sections describe the SSL Services Module front panel:

- STATUS LED, page 1-5
- FIPS LED, page 1-5
- SHUTDOWN Button, page 1-6

STATUS LED

The STATUS LED indicates the operating states of the module. Table 1-2 describes the LED operation.

Table 1-2 STATUS LED Description

Color	State	Description
Green	On	All diagnostic tests pass. The module is receiving power.
Red	On	A diagnostic other than an individual port test failed.
Orange	On	Indicates one of three conditions: • The module is running through its boot and self-test diagnostic sequence. • The module is disabled. • The module is in the shutdown state.
	Off	The module power is off.

FIPS LED

The FIPS LED currently is not used.

SHUTDOWN Button

Caution Do not remove the SSL Services Module from the switch until the module has shut down completely and the STATUS LED is orange. You can damage the module if you remove it from the switch before it completely shuts down.

To avoid corrupting the SSL Services Module hard disk, you must correctly shut down the SSL Services Module before you remove it from the chassis or disconnect the power. You can shut down the module by entering the **hw-mod module** *mod* **shutdown** command in privileged mode from the router CLI.

If the SSL Services Module fails to respond to this command, shut down the module by pressing the SHUTDOWN button on the front panel.

The shutdown procedure may require several minutes. The STATUS LED turns off when the module shuts down.