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 public key of the entity, and the time stamps that indicate the certificate 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.

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] • Supervisor Engine 720 with MSFC3 and PFC3
Supported Software
• Supervisor Engine 2: – 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 2.1(1) or later on the SSL Services Module • Supervisor Engine 720: – Cisco IOS Release 12.2(14)SX1 or later on the MSFC3 – Cisco IOS Release 12.2(17)SX1 or later on the MSFC3 and Catalyst software release 8.2(1) or later on the Supervisor Engine 720 – SSL Services Module software release 2.1(1) or later on the SSL Services Module
SSL Features
SSL initiation[3]
SSL version 2.0 forwarding[3]
URL rewrite[3]
HTTP header insertion[3]
Wildcard proxy[3]
Handshake Protocol
SSL 3.0
SSL 3.1/TLS 1.0
SSL 2.0 (only ClientHello support)
Session reuse
Session renegotiation
Session timeout
Symmetric Algorithms
ARC4
DES
3DES
Asymmetric Algorithms
RSA

Table 1-1 Feature Set Description (continued)

Features
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 certificates up to 2048-bit
Secure key storage in SSL Services Module Flash memory device
Certificate enrollment for client and server-type proxy services
Importing and exporting of key and certificate (PKCS12 and PEM)
Duplicating keys and certificates on standby SSL Services Module using the key and certificate import and export mechanism
Manual key archival, recovery, and backup
Key and certificate renewal using the CLI
Graceful rollover of expiring keys and certificates
Auto-enrollment and auto-renewal of certificates
Importing of certificate authority certificates by cut-and-paste or TFTP
Up to 8 levels of certificate authority in a certificate chain
Generating of self-signed certificate
Manual certificate enrollment using cut-and-paste or TFTP of PKCS10 CSR file
Peer (client and server) certificate authentication[3]
Peer (client and server) certificates[3]
Certificate security attribute-based access control lists[3]
Certificate revocation lists (CRL)[3]
Certificate expiration warning[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

Table 1-1 Feature Set Description (continued)

Features
NAT[5]/PAT[6]
Client and server
Scalability
Multiple modules in a single chassis when used with the CSM[7]; the CSM provides server load balancing (SLB[8])
High Availability
Failure detection (SLB health monitoring schemes)
System-level redundancy (stateless) (when used with the CSM)
Module-level redundancy (stateless) (when used with the CSM or with multiple SSL modules configured with HSRP[3, 9])
Serviceability
OIR[10] (after properly shutdown)
Graceful shutdown
Password recovery[3]
Statistics and Accounting
Total SSL connections attempt per proxy service
Total SSL connections successfully established per proxy service
Total SSL connections failed per proxy service
Total SSL alert errors per proxy service
Total SSL resumed sessions per proxy service
Total encrypted/decrypted packets/bytes per proxy service
Statistics displayed at 1 second, 1 minute, and 5 minutes traffic rate for CPU utilization and SSL-specific counters
Certificate authentication and caching statistics[3]
Configuration and Management
Direct connection to the module console port
Secure Shell (SSHv1) session
TACACS/TACACS+/RADIUS[3]
Telnet
Automatic backup and restore of configuration file to NVRAM
System Capacity and Performance
Supports the following RSA key sizes: – 512-bits – 768-bits – 1024-bits – 1536-bits – 2048-bits

Table 1-1 Feature Set Description (continued)

Features
System Capacity and Performance (continued)
Up to 300 Mbps throughput
Up to 256 proxy services
Up to 64,000 simultaneous sessions
Up to 3000 sessions per second
Stores up to 356 certificates
Stores up to 356 key pairs
SNMP Support
CISCO-SSL-PROXY-MIB[3, 11]
– cspGlobalConfigGroup
Version string
Supported cipher suites
Trap configuration setting
– cspProxyServiceConfigGroup
Type of proxy service
IP addresses and TCP ports
Policy names
Keys and certificates
– cspProxyServiceNotificationGroup
Proxy service operational status change
Proxy service certificate expiration warning
– cspSslGroup
Protocol counters
Error counters
Cumulative total values are reported in get responses, even if counters are cleared using CLI commands.
– cspSsl3Group
– cspTls1Group
– cspSslErrorGroup
– cspCpuStatusGroup
Utilization of each CPU
If counters have been cleared using CLI commands, the current values are reported in get responses, and the time of the last **clear** command are reported.
CISCO-SSL-PROXY-CAPABILITY

1. MSFC = Multilayer Switch Feature Card
2. PFC = Policy Feature Card
3. New feature in SSL software release 2.1(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. HSRP = Hot Standby Router Protocol
10. OIR = Online Insertion and Removal
11. All objects are read-only