

Luna[®] SA

for SSL Acceleration



High-performance SSL acceleration and hardware key management combined with the flexibility and scalability of a network-attached security appliance.



SafeNet Luna SA
Security, integrity, and performance
for all your SSL applications

Luna SA[®] for SSL Acceleration

Luna SA delivers SSL acceleration to multiple web servers with network-shareable, FIPS 140-2 Level 2 validated SSL acceleration that is cost-effective, easy to deploy, and highly scalable.

High Performance Hardware SSL Acceleration

Luna SA offloads computationally intensive SSL connection setups from web servers with dedicated hardware SSL acceleration. Luna SA delivers up to 1200 SSL session setups per second (RSA 1024-bit decryptions) to your web servers and provides future-proofed performance headroom as transaction volumes and key sizes increase.

Shareable and Scalable

Luna SA changes the economics of adding hardware-accelerated SSL to web servers and Internet applications with a cost-effective shareable deployment: share a single Luna SA between up to 10 web servers on a network. Luna SA delivers SSL acceleration capacity, ensuring that connected web servers receive performance when it is needed.

Luna SA scales to over 3600 transactions per second in high availability load-sharing configurations to ensure that even the most demanding applications receive the performance they need while allowing fewer web servers to handle larger traffic loads.

Network Attached — Easy to Deploy and Easy to Manage

Luna SA features Ethernet connectivity to simplify deployment, administration, and management across a network. Built-in support for TCP/IP (Internet Protocol) ensures that Luna SA deploys easily into existing network infrastructures allowing you to add SSL acceleration without the need to install additional hardware into your web servers. Secure network configuration and administration tools permit easy remote configuration and monitoring of the Luna SA.

Shareable SSL Acceleration to Reduce Costs and Simplify Administration

Luna SA's network shareable deployment model dramatically reduces the cost of adding SSL acceleration to web server farms by allowing easy sharing of hardware between multiple web servers. Luna SA allows up to 10 web servers to easily share hardware security and SSL performance, decreasing capital costs by eliminating the need to install SSL acceleration hardware in every web server reducing the hardware costs associated with traditional direct connected SSL accelerators.

Protect Your Website's Identity with Secure Hardware Key Management

SSL relies on digital certificates to identify secure web servers. Each certificate is tied to a secret Private Key stored on the web server. If a web server's Private Key is stolen it can be used to tap into online transactions or impersonate your legitimate web site.

To protect the identity of your web servers, Luna SA performs all cryptographic functions within a tamper-resistant cryptographic hardware module, ensuring that Private Keys are stored and managed in a secure environment. The Luna SA's cryptographic module is validated to FIPS 140-2 Level 2* for customers, like healthcare, government, and finance, that require top-level security for web applications and services.

Luna SA for SSL Features

Integrated with Leading Web Servers

Luna SA is fully integrated with the most popular web server platforms for easy deployment:

- Microsoft® IIS 5.0, IIS 6.0, and Windows ISA Server for Microsoft Windows® 2000 Server and Windows Server 2003
- Apache Web Server 1.3.27 and 2.0.46
- Sun One Web Server 4.1, 6.0

For custom application development, Luna SA offers API support for PKCS#11, Microsoft CryptoAPI 2.0, JCA (Java Cryptographic Architecture), JCE (Java Cryptographic Extensions), and OpenSSL.

Hardware Accelerated Performance

Luna SA delivers up to 1200 SSL setups per second. Combine multiple Luna SAs to achieve up to 3600 transactions per second in high availability load-sharing configurations

Industry Standard Rackmount Chassis

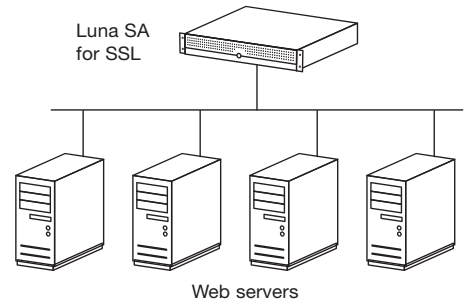
Luna SA features a 2U, 19" rackmount chassis optimized for security and dependability to meet the high processing density and manageability needs of web farms and data centers.

Integrated Physical Security and Built-in Hardware Security Module (HSM)

Luna SA includes an integrated K3 Cryptographic Engine, a dedicated FIPS 140-2 Level 2 validated* HSM. The K3 is integrated into the Luna SA's secure chassis that includes tamper-evident screws, intrusion detection switches, and shielded connectors to minimize exposure to direct physical attack.

Simplified Remote Administration

Luna SA features a network accessible Secure Command Line Interface (SCLI) to simplify remote system administration and streamline maintenance. A local console port is offered for secure initial configuration or direct system administration.



Share one Luna SA between multiple web servers

Luna SA for SSL Benefits

Lower Cost Per Web Server

Luna SA's shareable network attached deployment model reduces the cost-per-web server by allowing up to 10 web servers to utilize one Luna SA for high-performance SSL acceleration. Compared to competing direct-connected SSL accelerators, initial hardware costs and ongoing maintenance expenses are dramatically reduced without sacrificing security or performance.

More Performance from Your Web Servers

Luna SA eliminates SSL bottlenecks on host web servers, allowing you to use fewer web servers to serve more secure sessions, handle peak traffic loads without faltering, and reduce failed connection attempts that produce customer frustration. Luna SA provides capacity on demand to significantly increase the value of your revenue-generating web servers by enabling dramatically higher transaction throughput.

Easy to Deploy

Add hardware SSL acceleration without the need to install additional hardware in your web servers. Luna SA delivers flexible, easy-to-deploy Ethernet-attached connectivity that easily integrates into existing network infrastructures.

Easy to Scale

As your needs grow, add additional Luna SAs to increase performance, achieve high-availability and load balancing capabilities to simplify advanced network architectures without having to add new web servers or add-in cards to handle SSL traffic.

Easy Integration

The Luna SA simplifies integration and ensures application compatibility with support for PKCS#11, Microsoft CryptoAPI 2.0, JCA (Java Cryptographic Architecture), JCE (Java Cryptographic Extensions), and OpenSSL cryptographic APIs. A full Software Developer Kit is available for custom development.

Technical Specifications

Supported SSL Protocols

SSL v2.0, SSL v3.0, TLS

Cryptographic APIs

PKCS#11 v2.01, Microsoft CAPI v2.0, JCA (Java Cryptographic Architecture), JCE (Java Cryptographic Extensions), OpenSSL

Cryptographic Acceleration Hardware Features

- FIPS 140-2 Level 2 Validated
- True hardware accelerated random number generation (Annex C of ANSI X9.17)
- Symmetric and asymmetric key pair generation
- RSA Encryption and decryption (RSA 512-bit to 4096-bit key lengths)

Cryptographic Algorithms

Asymmetric Key

Diffie-Hellman (1024-4096 bit)

RSA (512-4096 bit) (PKCS#1 v1.5, OAEP PKCS#1 v2.0)

Digital Signing

RSA (1024-4096-bit), DSA (512-1024-bit), (PKCS#1 v1.5)

Symmetric Keys

3DES, (double & triple key lengths), AES, RC2, RC4, RC5, CAST-128

Hash Digest

SHA-1, SHA-2 (160, 256, 512), MD-5

Message Authentication Codes (MAC)

HMAC-MD5, HMAC-SHA-1, SSL3-MD5-MAC, SSL3-SHA-1-MAC

Physical Characteristics

Connectivity

2 x 10/100 Ethernet, CAT5, UTP
Local serial console port

Dimensions

2U full-length 19" rackmount chassis (ANSI/EIA-310-D compliant)
19.0" x 20.6" x 3.45" (482.6mm x 523.2mm x 87.7mm)
35lb (15.9kg)

Temperature

Operating 0°C to 40°C, Storage -20°C to +65°C

Regulatory Standards Certification

U/L 1950 & CSA C22.2 safety compliant
FCC Part 15 - Class B
ISO - 9002 Certification

Configurations and Options

Luna SA 600 for SSL

600 Transactions per second
1 client; upgradeable to up to 10 clients
1 HSM Partition with up to 80 key objects

Luna SA 1200 for SSL

1200 Transactions per second
1 client; upgradeable to up to 10 clients
1 HSM Partition with up to 80 key objects

NTLS Client License

Add up to 9 additional client licenses to the single license that is included in the configuration.

Luna SA High-Availability Array License

Add multiple Luna SA to a high-availability, load balancing, redundant array.



- 1 Indicator Lights
- 2 Console Port
- 4 Token Ports
- 5 Power Socket
- 6 Ethernet Ports



Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or **800.533.3958** eMail: **info@safenet-inc.com**