

SOLUTION BRIEF



Ensuring Trust in Encrypted SSL-secured Web Gateways: Blue Coat ProxySG and Gemalto SafeNet Luna SP

As advanced attacks on enterprise networks become more common and costly, organizations are increasingly turning to SSL encryption to secure their applications and networks, and preserve data privacy. Yet, SSL encryption can hide malware and viruses from security administrators, making it a vulnerability to the applications and networks it protects. Additionally, should the encryption keys protecting SSL traffic ever fall into the hands of skilled hackers or malicious users, entire applications and networks could be compromised without anyone knowing. To complicate matters, enterprises must demonstrate their compliance with regulatory regimes and best practices as they establish defense-in-depth security postures.

The Solution: Blue Coat ProxySG and SafeNet Luna SP

SafeNet Luna SP hardware security modules (HSMs) by Gemalto integrate with Blue Coat's ProxySG appliance to enhance the security of SSL traffic in enterprise networks. SafeNet Luna SP stores the CA certificates and private keys used by the ProxySG appliance to carry out SSL inspection using certificate re-sign. The CA certificate and key are stored in the Luna SP's secure, tamper-proof hardware to make them inaccessible to unauthorized users, and easy to manage and scale as SSL use grows. The ProxySG appliance identifies and manages all SSL-encrypted traffic to effectively enable protected communications based on acceptable use policies.

Blue Coat ProxySG appliance

ProxySG is a web access gateway that both secures web communications through SSL encryption and accelerates the delivery of business applications. Security teams can also use it to control web traffic through encrypted content inspection, and traffic optimization and validation. ProxySG's hardware design has increased performance over previous generations and now offers increased throughput for quick delivery times in encrypted, high-availability deployments. Coupled with content caching and bandwidth management features, ProxySG speeds remote application deployment while protecting network resources from malicious threats.

Key Benefits

Best-in-class security

ProxySG and SafeNet Luna SP HSMs combine to provide a best-in-class enterprise encrypted traffic management solution.

Robust security

SafeNet Luna SP HSMs offer the highest level of tamper resistance and security commercially available. They have been validated to be compliant with FIPS 140-2 Level 3 and Common Criteria EAL 4+ standards. Proxy SG appliances are FIPS 140-2 certified.

Meet compliance requirements

High-assurance hardware key storage is an important part of meeting data governance requirements. ProxySG appliances can exclude regulated data streams from inspection to protect privacy and accommodate regulatory requirements, such as HIPAA, PCI, FISMA, and SOX.

Integrates seamlessly with existing infrastructure

Both SafeNet Luna SP HSM and ProxySG connect to standard networks to ensure ease of deployment into existing network infrastructure. Easy network attachment reduces setup time so administrators can deploy their security quickly with reduced resource investments.

SafeNet Luna SP HSM

SafeNet Luna SP HSMs are robust, high-availability, and high-performance appliances that store cryptographic materials (e.g., certificates, encryption keys, etc.) in a secure FIPS 140-2 Level 3, tamper-proof hardware appliance. In addition, Luna SP can conduct all cryptographic operations itself within the hardware appliance so ProxySG can offload SSL transactions and improve server performance. Storing these materials in a hardware appliance keeps them out of harm's way and ensures that only authorized administrators have access to important encryption keys. Since the keys never leave the device and cryptographic operations take place in the module, Luna SP can serve as a trusted root that ensures the integrity of an organization's cryptographic operations.

Key features

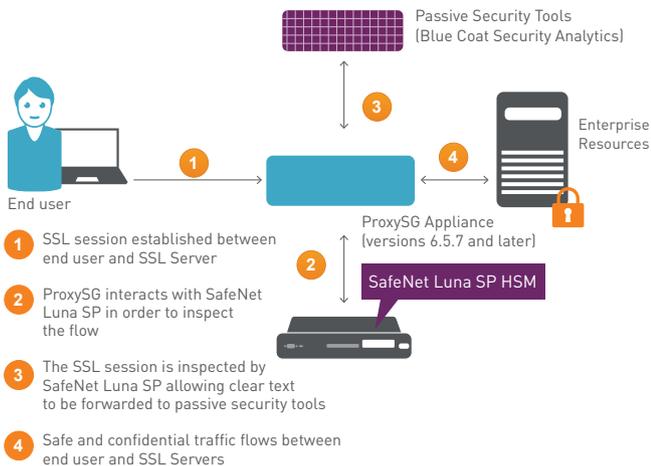
Robust security

SafeNet Luna SP HSMs store the private keys and associated CA certificates used to authenticate servers involved in SSL transactions. The ProxySG appliance then applies policies to selectively determine which secure communications should be inspected. Data required to stay private continues to its destination while suspect traffic is inspected – all according to custom-defined policies. For flows that need to be inspected, ProxySG requires access to CA/private keys in order to obtain access to encrypted content. Storing the CA/private key in a hardware appliance prevents unauthorized physical or logical access to the keys and certificates used for SSL, thus preserving the integrity of the cryptographic infrastructure.

Centralized, scalable security management

Centralizing key storage and management in SafeNet Luna SP allows administrators to keep a close eye on the CA/private keys used by ProxySG. As SSL use increases, administrators can grow their security capability simply without multiplying management consoles and complicating their security environment. ProxySG offers 1Gbps throughput so an increase in traffic does not equate to a decrease in performance. Luna SP can serve multiple appliances, further reducing management overhead as SSL use increases. ProxySG and Luna SP offer a scalable, secure solution that addresses SSL's blind spot and preserves overall performance.

ProxySG Appliance and SafeNet Luna SP Architecture Diagram



Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: data-protection.safenet-inc.com

GEMALTO.COM

Quickly deploy a security solution without impacting server performance

ProxySG is transparent to end systems, and does not require network reconfiguration or modifications to client and web browser configurations. Likewise, SafeNet Luna SP uses standard development tools and protocols to attach anywhere in the network for quick deployment.

Once installed, ProxySG and Luna SP combine to provide policy-based encryption security without impacting overall performance. ProxySG delivers non-SSL-protected data directly to end users while separating SSL-encrypted data for examination. Separating encrypted from unencrypted data eliminates unnecessary processes to maintain server performance.

SafeNet Luna SP offloads SSL transactions to further reduce the number of processes asked of the server. Since it is specially designed for encryption operations, Luna SP is capable of processing up to 7,000 RSA transactions per second, giving enterprises a purpose-built option that reduces strain on server resources.

With the combined solution, security administrators can quickly secure their networks with a key storage solution that also accelerates the speed at which they can deliver secured network traffic.

Logging and auditability features

SafeNet Luna SP combines proven hardware key management with rigorous logging features to provide non-repudiable audit records of access and cryptographic key usage. Separated administrative roles and flexible security policy management allows security teams to maintain tight control over sensitive administrative functions, such as the management of cryptographic keys. Knowing who is accessing keys, and being able to easily demonstrate detailed log records, makes reporting for audits easier on security teams.

Conclusion

SSL-encrypted traffic is pervasive in today's enterprises and predicted to grow rapidly over the next several years. While providing data privacy, SSL also presents a blind spot for current security tools and applications as malware and advanced threats increasingly use SSL to hide from detection. Organizations must effectively address this dilemma to reduce risk and avoid damaged reputations. Gemalto and Blue Coat join together to provide enhanced security and visibility to enterprises using SSL applications. With SafeNet Luna SP, organizations can trust that the data traveling in its ProxySG-secured network is encrypted and protected from unauthorized users. For more information, visit: <http://www.safenet-inc.com/partners/bluecoat>

gemalto
security to be free