SOLUTION BRIEF

Ensuring Trust in SSL-encrypted Networks: Blue Coat SSL Visibility Appliance and Gemalto SafeNet Luna SP

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

The Solution: Blue Coat SSL Visibility Appliance and Gemalto SafeNet Luna SP

SafeNet Luna SP hardware security modules (HSMs) by Gemalto integrate with Blue Coat's SSL Visibility Appliance to enhance the security of SSL traffic in enterprise networks while maintaining the privacy needs of the organization. SafeNet Luna SP stores CA certificates and private keys used by the SSL Visibility 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 appliance to make them inaccessible to unauthorized users, as well as easy to manage and scale as the capacity needs grow. The SSL Visibility Appliance identifies and manages all SSL-encrypted traffic to effectively enable protected communications based on acceptable use policies.

Blue Coat SSL Visability Appliance

The SSL Visibility Appliance is a powerful, purpose-built solution that decrypts incoming or outgoing SSL traffic and provides that content to multiple security appliances (e.g., next-generation firewalls (NGFW), intrusion detection and prevention systems (IDS/IPS), and data loss prevention (DLP) solutions) based on defined policies for further processing and analysis. This provides IT security administrators with the necessary visibility and control of all SSL-encrypted traffic entering and exiting their organization. Once traffic is inspected and assured based on the established policies, the SSL Visibility Appliance re-encrypts the data before sending it to its final destination. The Blue Coat appliance empowers existing security tools with visibility into formerly hidden traffic and potential threats without hindering device or

Key Benefits

Encrypted Traffic Management (ETM) is becoming essential for enterprises to manage potential threats within SSL traffic

Together, the SSL Visibility Appliance and Gemalto SafeNet Luna SP HSMs provide a best-in-class enterprise ETM solution

Robust and certified security

SafeNet Luna SP hardware security modules (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. The SSL Visibility Appliance SV2800 is FIPS 140-2 Level 2 certified.

Helps meet compliance requirements

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

Seamless integration with existing infrastructure

Both the SSL Visibility Appliance and SafeNet Luna SP HSM connect to standard networks to ensure ease of deployment into existing network infrastructure.

network performance, thus extending the existing investment in the security infrastructure. Blue Coat's comprehensive SSL inspection capabilities are easy to add to any network security infrastructure so administrators can plug the security loopholes created by SSL.

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. Storing these materials in a hardware appliance keeps them out of harm's way and ensures that only authorized administrators have access to the keys that unlock all enterprise communications. 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. Additionally, Luna SP conducts all cryptographic operations within the hardware appliance so that the SSL Visibility Appliance can offload SSL transactions and improve server performance.

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 SSL Visibility 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 according to custom-defined policies. For inspected flows, the SSL Visibility Appliance uses CAs/private keys to access encrypted content. With Luna SP as the root of trust, organizations can securely send and inspect data without worrying about attackers impersonating network servers.

Quickly deploy a security solution without impacting server performance

The SSL Visibility Appliance 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, the SSL Visibility Appliance and Luna SP HSM combine to provide policy-based encryption security without impacting overall performance. The SSL Visibility Appliance 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.

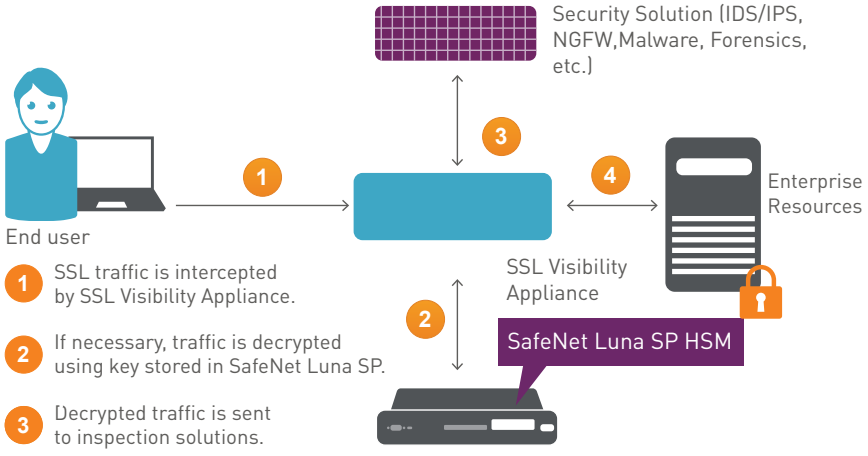
SafeNet Luna SP offloads SSL transactions to further reduce the number of processes asked of the server. Since it is specially designed for encryption operations, Luna SP is capable of processing up to 7,000 RSA transactions per second, giving enterprises a purpose-built option that reduces strain on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

Centralized, scalable security management

Centralizing key storage and management in SafeNet Luna SP allows administrators to keep a close eye on the keys being used by SSL Visibility Appliances. As SSL use continues to increase, administrators can grow their security capability simply without multiplying management consoles and complicating their security environment. The SSL Visibility Appliance manages multiple SSL streams so an increase in traffic does not equate to a decrease in performance or security. Luna SP can serve multiple SSL Visibility Appliances, further reducing management overhead as SSL use increases. When combined, the SSL Visibility Appliance and Luna SP HSM offer a scalable, secure solution that addresses SSL's blind spot.

SSL Visibility Appliance and SafeNet Luna SP Architecture Diagram



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 the management of cryptographic keys. Knowing who is accessing the SSL Visibility Appliance's private 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 use SSL to hide from detection. Organizations must effectively address this dilemma to reduce risk and avoid damage. Gemalto and Blue Coat provide enhanced security and visibility to enterprises using SSL applications. For more information, visit: http://www.safenet-inc.com/partners/bluecoat

About Gemalto's SafeNet Identity and Data Protection Solutions

Gemalto's portfolio of Identity and Data Protection solutions offers one of the most complete portfolios of enterprise security solutions in the world, enabling its customers to enjoy industry-leading protection of data, digital identities, payments and transactions–from the edge to the core. Gemalto's SafeNet Identity and Data Protection solutions enable enterprises across many verticals, including major financial institutions and governments, to take a data-centric approach to security by utilizing innovative encryption methods, best-in-class crypto management techniques, and strong authentication and identity management solutions to protect what matters, where it matters. Through these solutions, Gemalto helps organizations achieve compliance with stringent data privacy regulations and ensure that sensitive corporate assets, customer information, and digital transactions are safe from exposure and manipulation in order to protect customer trust in an increasingly digital world.

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

GEMALTO.COM

gemalto
security to be free