While remote delivery of applications to a mobile workforce is essential to enterprise success, it increases the opportunity for data theft and network attacks. In order to protect their business, organizations are increasingly turning to solutions that allow them to detect and stop potentially harmful SSL/TLS (Secure Sockets Layer/Transport Layer Security)-encrypted traffic that traverses their networks. Implementing a firewall that can mitigate threats posed by malicious SSL traffic can be effective, but the implementation changes the hierarchy of trust on which SSL traditionally depends.

The Palo Alto Networks Firewall Platform gives enterprises the ability to secure, identify, control, and inspect SSL- and SSH (Secure Shell)-encrypted traffic to prevent data corruption, theft, and unauthorized data transfer. When integrated with a Palo Alto Networks Firewall, SafeNet Luna Network hardware security modules (HSMs) act as a trust anchor that helps to protect the integrity of SSL communications.

The Solution: SafeNet Luna HSMs for Palo Alto Networks Firewall and Web Firewall Gateways

SafeNet Luna HSMs integrate with Palo Alto Networks Next-Generation Firewalls to provide the logical and physical protection of the keys used in SSL encryption. The dedicated HSM manages certificate-signing functions for SSL forward proxy and SSL inbound inspection, as well as master key storage functions. SafeNet Luna HSMs also secure the encryption keys during their entire lifecycle—from key creation to storage to deployment to destruction. HSM support is generally needed when FIPS 140-2 Level 3 protection for Certificate Authority (CA) keys is required.

Palo Alto Networks Gateway Firewalls

Palo Alto Networks offers a full line of advanced web firewall-gateway appliances that protect network traffic and the remote delivery of enterprise applications. The firewall’s traffic classification system—unique to the Palo Alto Network platform—inspects network traffic for threats outside (not inside) the firewall, even if that traffic is secured with SSL encryption. As it is decrypted and inspected, traffic is tied to a specific user. That information, along with the context of the traffic, application, and associated content are used to make delivery decisions based on defined security policies. Policies allow administrators to choose which traffic is decrypted and which remains secured and compliant—exempting HR and finance operations to maintain regulatory compliance. When combined, these features allow enterprises to focus on business operations without sacrificing overall enterprise security.

Key Benefits

High-Performance Processing
SafeNet Luna Network HSMs are capable of processing up to 10,000 RSA and 22,000 ECC transactions per second. High processing speeds allow administrators to offload cryptographic functions to improve server performance.

Robust Security that Meets Compliance Standards
SafeNet Luna HSMs offer the highest level of tamper-resistant security and are validated to be compliant with FIPS 140-2 Level 3 and Common Criteria EAL 4+ [AVA_VAN.5] standards.

Next-Generation Data Security
Palo Alto Networks Next-Generation Firewalls create, store, process, and encrypt both keys and data in SafeNet Luna HSMs. Palo Alto Networks appliances are separate from the firewall and provide the strongest cryptographic algorithms to guard digital identities.

Multi-Level Access Control
SafeNet Luna HSMs offer partitioning for signing/key management. Remote backup features allow administrators to securely move copies of their sensitive cryptographic material to the SafeNet Luna Backup HSM.

SafeNet Network Luna HSM

SafeNet Network Luna 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-resistant 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 important encryption keys. A single SafeNet Luna HSM can manage keys and accelerate operations to significantly improve the reliability, security, and scale of encryption performance. With SafeNet Luna Network HSMs as a security infrastructure’s trusted root, administrators can ensure the integrity of their cryptographic operations.
Key features

Robust security
SafeNet Luna HSMs safeguard the private keys and associated certificates used by Palo Alto Networks platforms to authenticate the endpoints involved in SSL operations. When Palo Alto Networks platforms decrypt SSL traffic to inspect for threatening activity, they alter the trust hierarchy. SafeNet Luna HSM serves as a root of trust to ensure the integrity of network traffic as it is decrypted, reviewed and re-encrypted. The private key essential to SSL encryption never leaves the hardware appliance, making it impossible for unauthorized users to steal the keys needed to decrypt secured traffic or masquerade as network servers. The appliance’s tamper-proof design also provides significant physical security in addition to the logical security protecting the keys.

Centralized Management and Operations
Palo Alto Networks next-generation firewalls allow for a number of management options, ranging from individually using a command line interface to device/group-based management using a web interface. Palo Alto Networks centralizes policy, reporting, visibility, and logging features to reduce management overhead. SafeNet Luna HSMs can be clustered into high-availability configurations that can be managed as one unit. In addition, SafeNet Luna HSMs can perform multiple operations—such as key generation, export, and root functions—where enterprises would normally require multiple appliances or solutions to manage the PKI infrastructure.

Logging and auditability features
SafeNet Luna Network HSM 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.

Product Integrations

Palo Alto Networks Next-Generation Firewall Platforms
- PA-3000 Series
- PA-3200 Series
- PA-5000 Series
- PA-5200 Series
- PA-7000 Series
- VM-Series firewalls
- Panorama management server (Virtual and M-Series appliance)

SafeNet Luna HSM
- SafeNet Luna Network HSM

Partition to Easily Scale
SafeNet Luna Network HSMs can be separated into 100 cryptographically isolated partitions, with each partition acting as if it were an independent HSM. Partitions provide a tremendous amount of scalability and flexibility, as a single HSM can act as the root of trust that protects the cryptographic key lifecycle of one hundred dependent Palo Alto Networks firewalls.

What’s more, the partitions are designed to protect key material from other tenants on the appliance, meaning different lines of business can leverage the same appliance without fear of losing their keys to other tenants. Enterprises with large-scale Palo Alto Networks deployments can use SafeNet Luna HSM as a cost-effective solution to hardware key storage.

Conclusion
Gemalto and Palo Alto Networks work together to enhance network security so businesses can focus on the initiatives that drive their success. Palo Alto Networks preserves network traffic privacy where needed while eliminating threats to the enterprise resources on which businesses depend. SafeNet Luna Network HSMs support these efforts by ensuring that all operations occur within a trusted infrastructure. For more information on the Palo Alto Networks partnership, visit: https://safenet.gemalto.com/partners/palo-alto-networks/.

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us
Follow Us: blog.gemalto.com/security

Secure SSL Keys: Palo Alto Networks Firewall Platforms with SafeNet Luna HSM - Solution Brief