cpl.thalesgroup.com

THALES

Secure SSL/TLS Keys: Palo Alto Networks Next-Generation Firewalls with Thales Luna HSM

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 TLS/SSL (Transport Layer Security/Secure Sockets Layer)-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 Next-Generation Firewall (NGFW) 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 NGFW, Luna Network hardware security modules (HSMs) act as a trust anchor that helps to protect the integrity of SSL communications.

The Solution: Luna HSMs for Palo Alto Networks NGFW

Luna HSMs integrate with Palo Alto Networks NGFWs to provide the logical and physical protection of the keys used in SSL encryption. The dedicated Luna HSM manages certificate-signing functions for SSL forward proxy and SSL inbound inspection, as well as master key storage functions. 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-validated hardware protection for Certificate Authority (CA) keys is required.

Palo Alto Networks NGFW

Palo Alto Networks NGFWs detect known and unknown threats, including in encrypted traffic, using intelligence generated across many thousands of customer deployments. That means they reduce risks and prevent a broad range of attacks. For example, they enable users to access data and applications based on business requirements. As traffic 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.

Luna Network HSM

Luna Network HSMs are robust, high-availability, and high-performance network appliances that store cryptographic materials (e.g., certificates, encryption keys, etc.) in a secure FIPS 140-3 Level 3 tamper-resistant hardware appliance. Storing these materials in hardware keeps them out of harm's way and ensures that only authorized administrators have access to important encryption keys. A single Luna HSM can manage keys and accelerate operations to significantly improve the reliability, security, and scale of encryption performance. With Luna Network HSMs as a security infrastructure's trusted root, administrators can ensure the integrity of their cryptographic operations.

Key Benefits

High-Performance Processing

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

Luna HSMs offer the highest level of tamper-resistant security and are FIPS 140-3 Level 3 validated and Common Criteria EAL 4+ certified.

Next-Generation Data Security

Palo Alto Networks NGFW create, store, process, and encrypt both keys and data in Luna HSMs. Luna HSMs are separate from the Palo Alto Networks NGFW and provide the strongest cryptographic algorithms and hardware key management to guard digital identities.

Multi-Level Access Control

Luna HSMs offer partitioning for signing/key management. Remote backup features allow administrators to securely move copies of their sensitive cryptographic material to a backup HSM solution from Thales, available as-a-service from Thales Data Protection on Demand, or as an accessory to Luna Network HSMs.

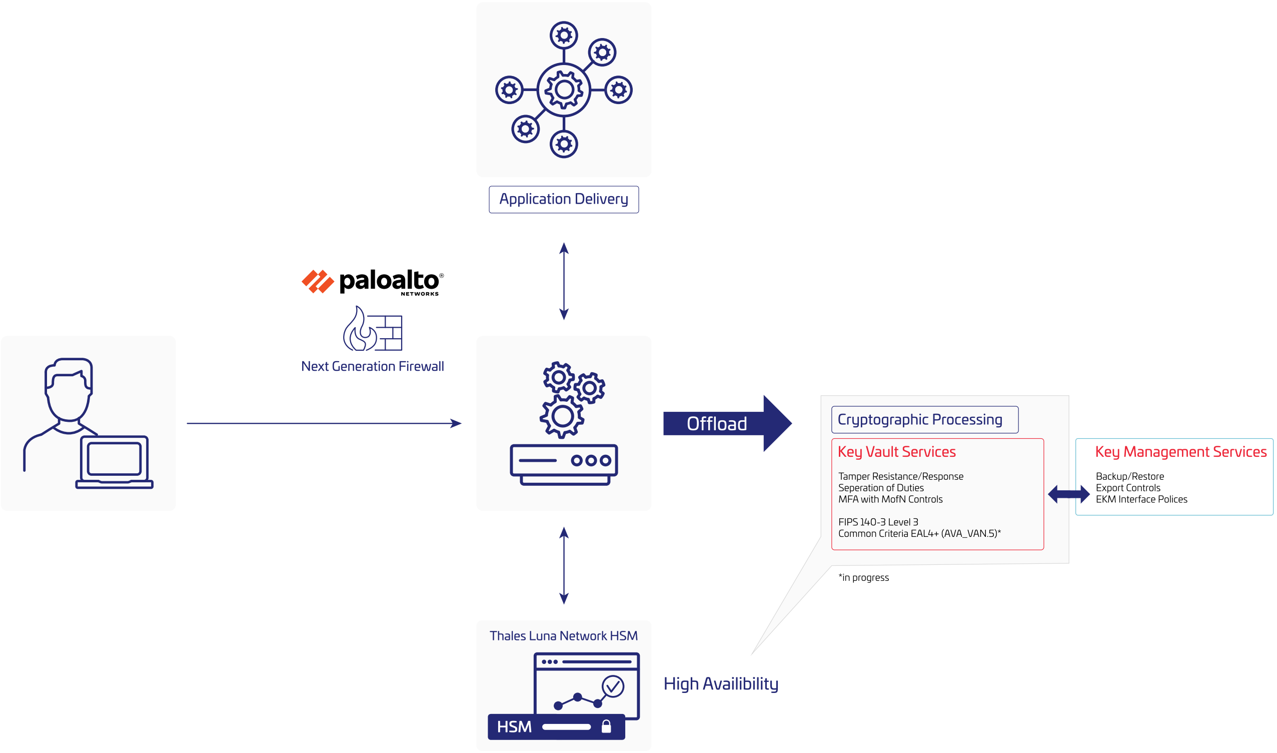
Key Features

Robust security

Luna HSMs safeguard the private keys and associated certificates used by the Palo Alto Networks NGFW platforms to authenticate the endpoints involved in SSL operations. When Palo Alto Networks NGFW platforms decrypts SSL traffic to inspect for threatening activity, it alters the trust hierarchy. Luna HSMs serve 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 NGFW allows 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 NGFW centralizes policy, reporting, visibility, and logging features to reduce management overhead. Luna HSMs can be clustered into high-availability configurations that can be managed as one unit. In addition, 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

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.

Partition to Easily Scale

Luna Network HSMs can be separated into one hundred 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 NGFWs.

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 NGFW deployments can use Luna HSM as a cost-effective solution to hardware key storage.

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)

Thales Luna HSM

- Thales Luna Network HSM

Conclusion

Thales 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. 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://cpl.thalesgroup.com/partners/palo-alto-networks

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.