Solution Brief

Secure and Manage SSL/TLS Keys: Palo Alto Networks Next-Generation Firewalls with Thales CipherTrust Manager

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

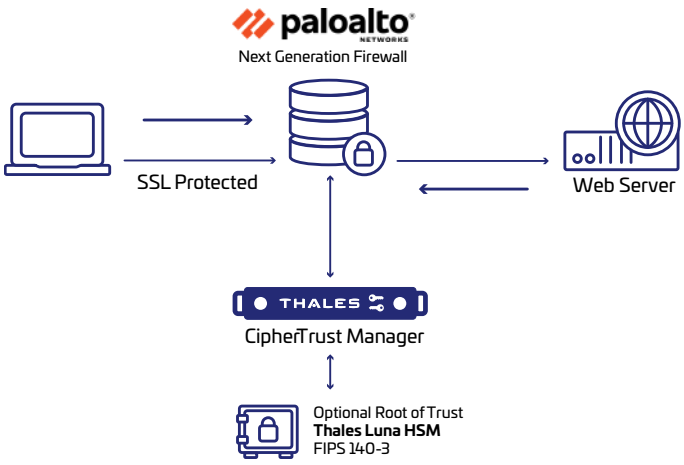
The Challenge

While remote application delivery to a mobile workforce is essential to enterprise success, it increases the opportunity for data theft and network attacks. 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 Solution

Centralized encryption key management is essential for safeguarding the keys involved in SSL encryption and decryption. It consolidates and protects master keys and secures keys from various third-party encryption solutions.

Together, the next-generation firewalls and encryption management solutions empower organizations to strengthen their security posture by centralizing and simplifying key management and data security policies.



Benefits of the Integration:

Integrating Thales CipherTrust Manager with Palo Alto Networks Next-Generation Firewalls (NGFW) offers several advantages:

1. **Centralized Key Management:** Enables centralized control of cryptographic keys, easing policy enforcement and reducing risks.
2. **Improved Compliance:** Helps meet regulatory requirements with strong data encryption.
3. **Tamper-Resistant Key Storage:** Optional embedded HSM provides robust security measures for encryption keys, minimizing exposure to unauthorized access.
4. **Operations:** Integrating key management and cryptographic functions into the NGFW cuts operational complexity and hardware needs.
5. **Monitoring/Auditing:** Comprehensive monitoring and logging of cryptographic activities enhances insights and incident response capabilities.

Thales CipherTrust Manager

Thales CipherTrust Manager provides a leading enterprise key management solution, allowing organizations to centrally manage encryption keys, enforce granular access controls, and set security policies. Serving as the core of the CipherTrust Data Security Platform, is managing tasks like key generation, rotation, destruction, and import/export. The platform features role-based access control, robust auditing, reporting, and user-friendly automation interfaces (REST API, CLI, Terraform).

CipherTrust Manager comes in both virtual and physical appliances that can integrate with FIPS 140-3 Level 3 compliant Thales Luna HSM for secure key storage. These can be deployed on-premises or in public cloud environments, meeting compliance requirements and industry best practices for data security. A unified management console simplifies policy management, data discovery, classification, and protection of sensitive data across various locations using CipherTrust Data Security Platform Connectors.

Palo Alto Networks Next Generation Firewall

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.

Secure and Manage SSL/TLS Keys: Palo Alto Networks and Thales CipherTrust Manager

As cyber threats rise and regulatory demands increase, safeguarding SSL/TLS keys is essential for enterprises. The challenge is to protect private keys and avoid unauthorized access and data breaches. The secure management of master keys and certificate-signing functions is critical, requiring a tamper-proof design to ensure the integrity of encrypted communications.

Thales CipherTrust Manager, integrated with Palo Alto Networks NGFW, addresses these challenges. It serves to ensure the integrity of network traffic during decryption, analysis, and re-encryption by securing private keys within a protected external appliance. The solution prevents unauthorized access and enhances physical security.

This integration meets compliance needs with a centralized platform for managing encryption keys and policies. Together, Thales and Palo Alto Networks empower enterprises to proactively protect sensitive information and maintain operational integrity.

Secure and Manage SSL/TLS Keys

Challenge

The challenge with SSL encryption is protecting the private key, which must remain secure to prevent unauthorized access. If the private key is ever exposed, it becomes vulnerable to theft, allowing attackers to decrypt secured traffic or impersonate network servers. Securing these keys in an external appliance is essential to safeguard their security, ensuring keys and certificates remain protected.

Solution

Thales CipherTrust Manager is crucial for safeguarding private keys and certificates used by Palo Alto Networks NGFW platforms during SSL operations. When these platforms decrypt SSL traffic for threat inspection, the trust hierarchy changes. CipherTrust Manager provides protection and management for keys used in SSL communications, ensuring the integrity of network traffic throughout decryption, analysis, and re-encryption. The private key for SSL encryption is secured within the CipherTrust Manager, preventing unauthorized access and potential impersonation of network servers.

Insuring Data Security and Privacy Compliance

Challenge

Enterprises face growing regulatory demands for hardware key storage to protect sensitive data. As cyber threats become more sophisticated, secure encryption key management is crucial to prevent unauthorized access and breaches. Proper key storage helps keep customers out of breach notification requirements, easing compliance burdens. Ensuring compliance and data security is essential for operational integrity today.

Solution

Thales CipherTrust Manager, integrated with Palo Alto Networks NGFW, effectively addresses data security, privacy, and compliance challenges for enterprises. This integration provides a centralized platform for managing encryption keys and policies, ensuring robust protection for sensitive data both at rest and in transit. CipherTrust Manager enhances administrative visibility over SSL keys, making all actions transparent. Together, these solutions ensure robust protection for sensitive data while reinforcing overall network integrity.

Thales Luna HSM and Palo Alto Next-Generation Firewall Integrations

Palo Alto Networks - Thales Luna HSM - Solution Brief

Palo Alto Networks (PAN) OS Integration Guide Luna HSM - Integration Guide

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. For more information, visit www.paloaltonetworks.com.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us

© Thales - November 2024 • EHv3