SOLUTION BRIEF

Fortinet and Thales Luna HSM Security Solution

Enhanced security for private keys used in SSL/TLS decryption

Executive Summary

Fortinet and Thales have partnered to deliver unparalleled, highly performant network security solutions by ensuring private keys used in SSL/TLS decryption are tightly secured and tamper-proof. Integrations between multiple Fortinet and Thales Luna HSM solutions provide several options to secure applications, workloads, networks, and clouds to meet business and regulatory needs.

The Challenges

Data is often most vulnerable to attackers as it moves across communications channels like SSL/TLS, requiring private keys for decryption. The combined integration between Fortinet and Thales can help protect organizations by integrating multiple security layers around software infrastructure.

Joint Solution

Fortinet's integration with Thales Luna Hardware Security Modules (HSMs) ensures and enhances high-performance network security solutions. It improves security for the private keys used for HTTPS inspection. In addition, you can use the Luna HSM to encrypt, generate, and store master keys.

Luna HSMs prevent an application from loading a copy of a private key into the memory of a web server. This is useful because your security keys are vulnerable to hackers while loaded into device memory. If an attacker gains access to the inspecting device, they can locate your key and then use it to access sensitive data. By deploying Luna HSMs (either on-premises, as a service, in the cloud, or across hybrid environments), you close the door to hackers attempting to get their hands on your organization's data.

The cryptographic functions in securing data during transmission occur within the secure Luna HSM environment, where data is shielded from attackers. How a Luna HSM is designed makes it impossible for an attacker to impact the operations inside the device. In other words, although an HSM can accept user input, users cannot access its inner workings. This makes HSMs a secure solution for both storing your cryptographic keys and performing encryption and decryption procedures.

Luna HSMs use common interfaces and encryption algorithms with crypto wallets, public critical infrastructure (PKI), and basic primary sensitive data security. Luna HSMs support CAPI, PKCS#11, CNG, and other interfaces.

Solution Components

- Thales Luna HSMs
- Fortinet FortiGate Next-Generation Firewalls
- Fortinet FortiWeb
- Fortinet FortiADC

Solution Benefits

- Industry-leading WAF performance for enterprise mission-critical applications
- Tamper-proof FIPS 140-2 Level 3 and Common Criteria (EAL 4+) security compliance provided by Luna HSMs
- Centralized management of SSL/TLS security certificates and encryption keys
- Enhanced security through a single set of certificates used on multiple devices to maximize performance, scale, and and essential critical durability
- Many deployment options, including hardware and virtual appliances, to meet enterprise network needs

FORTINET FABRIC-READY

Solution Components

Thales Luna HSMs secure sensitive data and critical applications by storing, protecting, and managing cryptographic keys. Luna HSMs are FIPS 140-2 Level 3 and Common Criteria certified high-assurance, tamper-resistant solutions that help organizations meet compliance and audit needs for GDPR, eIDAS, , HIPAA, PCI-DSS, and others, in highly regulated industries, including financial services, healthcare, and government.

FortiGate Next-Generation Firewalls (NGFWs) combine the functionality of traditional firewalls with deep packet inspection (DPI) and machine learning to enhance your network's security. In this way, FortiGate can identify malware, attacks by hackers, and many other threats and block them.

FortiWeb web application firewalls (WAFs) protect hosted web applications from OWASP Top 10 threats, DDoS attacks, and malicious bot attacks.

FortiADC is an advanced application delivery controller (ADC) that optimizes enterprise application delivery availability, user experience, and scalability. It enables fast, secure, intelligent acceleration and distribution of even the most demanding enterprise applications.

Joint Solution Integration

The integration of Thales Luna HSMs and Fortinet FortiGate, FortiWeb, and FortiADC enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers unparalleled, highly performant network security solutions by ensuring private keys used in SSL/TLS decryption are tightly secured and tamper-proof. Additionally, the joint Fortinet and Thales integration helps organizations conform to regulatory standards, manage encryption keys, and ensure authorized authentication and identity credentials.

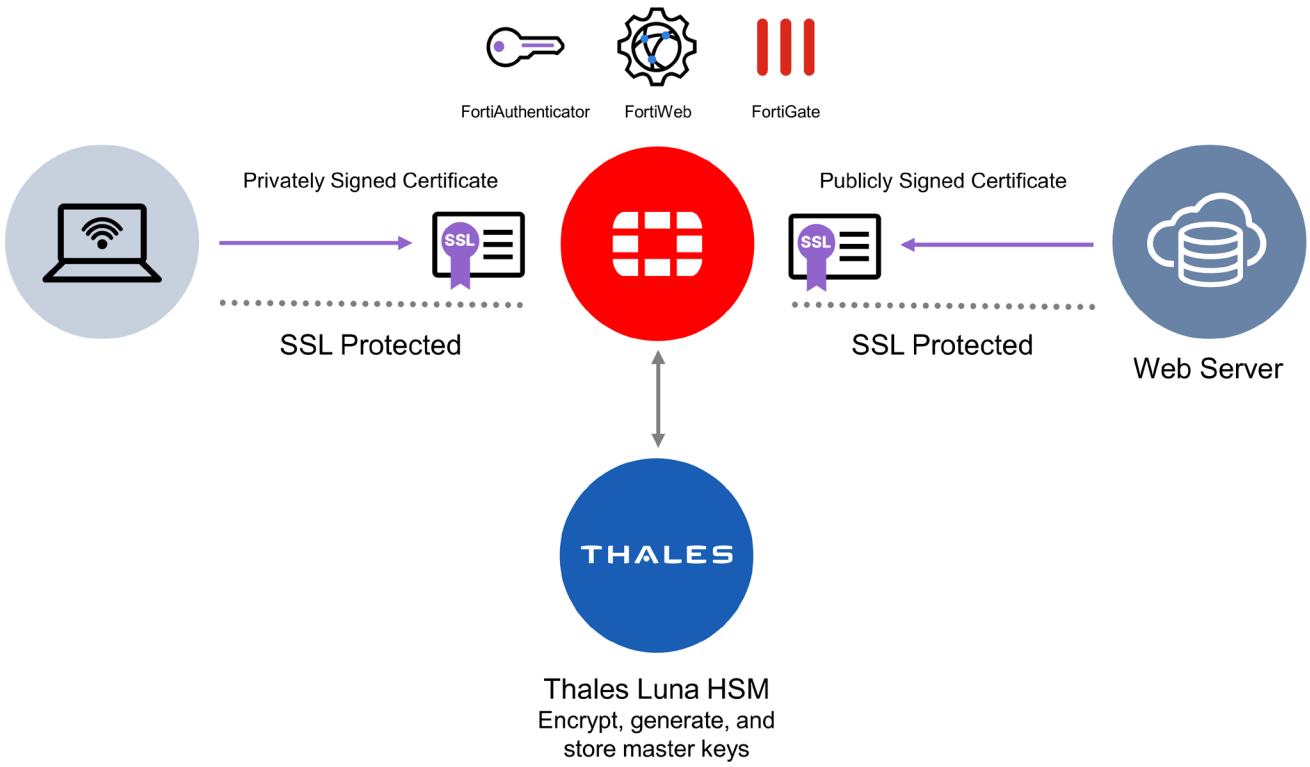

Figure 1: The Fortinet and Thales Luna HSM integration architecture

Joint Use Cases

There are many use cases for Luna HSMs; all involve encrypting and decrypting sensitive or private information. Some of the more popular examples include:

Protection of privileged access and company secrets: You can limit the effectiveness of insider threats with an HSM. That is because no one can tangle with what is happening inside an HSM—not even a capable internal hacker. Also, if your DevOps team needs to access private information, you can manage that access using an HSM to prevent exfiltration.

Keys management: Luna HSMs are very effective at managing cryptography keys. Whether deployed on-premises or in a cloud environment, Luna HSMs allow you to manage multiple keys.

Strong access controls: Luna HSM authenticates each user against required credentials and facilitates the creation of trustworthy identity credentials for securing your organization's infrastructure.

About Thales

Thales is the worldwide leader in data protection, providing everything an organization needs to protect and manage its data, identities, and intellectual property: encryption, advanced key management, tokenization, and authentication and access management. Whether it's securing the cloud, digital payments, blockchain, or the Internet of Things, security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales Cloud Protection & Licensing is part of Thales Group.

October 20, 2023 7:53 AM

2406200-0-0-EN