THALES

Secure Your Network Traffic with F5 BIG-IP and Thales Luna Network HSM

Downtime for corporate applications delivered through networks is not an option. Since organizations use these applications to generate revenue and manage operations, disruption and compromise directly impacts the bottom line. With the stakes so high, securing these resources and ensuring their availability is essential. Sophisticated attacks – such as Distributed Denial of Service (DDoS) attacks – can disrupt the availability of corporate applications or compromise the sensitive data traveling within a network. Protecting these resources is required to protect an organization's success.

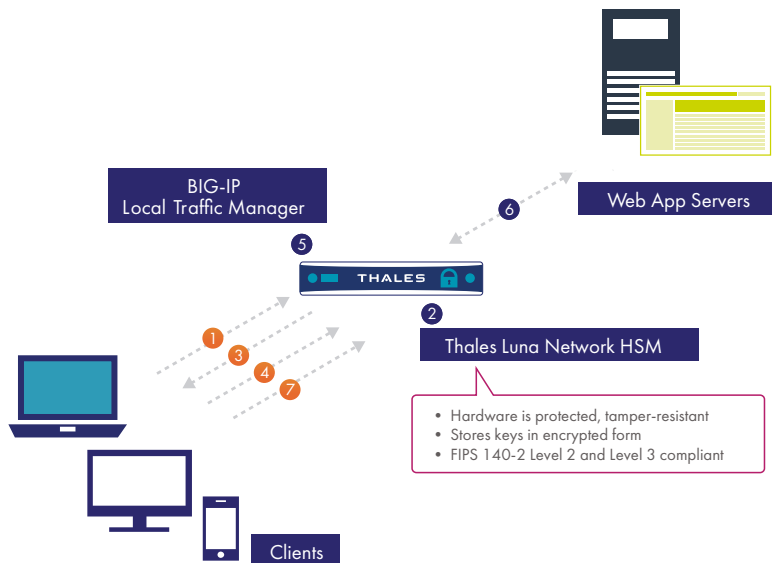## Solution: BIG-IP and Thales Luna Network HSM

Thales's Luna Network HSMs integrate with BIG-IP's Local Traffic Manager (LTM) and Access Manager to secure the network over which BIG-IP delivers applications. Luna Network HSM stores the certificates and encryption keys at the heart of BIG-IP's SSL/TLS (Secure Sockets Layer / Transport Layer Security) transactions in FIPS-validated hardware, ensuring high-assurance crypto protection. LTM and Access Manager intelligently deliver applications from data centers to authorized users in an effort to optimize network resources according to pre-defined business policies. Thales ensures that the network activity managed by BIG-IP occurs in tunnels secured by robust encryption and server authentication.

F5 BIG-IP Local Traffic Manager

BIG-IP LTM is a high performance application delivery system that intelligently manages network traffic in order to optimize performance. Its ability to balance loads and offload cryptographic operations eliminates single points of failure while maintaining security and high performance. Managing traffic across physical, virtual and cloud environments makes it easy to move applications across cloud and traditional physical architectures.

F5 BIG-IP Access Manager

BIG-IP Access Manager is a flexible, high-performance access and security solution that consolidates remote and LAN access, as well as wireless connections within a single management interface. Access Manager unifies access to corporate applications and networks, and controls entry to those unified resources through easy-to-manage access policies. When LTM centralizes application delivery and adds BIG-IP Access Manager, enterprises simplify the implementation of authentication and authorization controls ultimately protecting the organization from unauthorized access and sophisticated attacks.

BIG-IP Local Traffic Manager

Web App Servers

THALES

Thales Luna Network HSM

- Hardware is protected, tamper-resistant
- Stores keys in encrypted form
- FIPS 140-2 Level 2 and Level 3 compliant

Clients

1. Client requests a page with TLS
2. BIG-IP LTM retrieves public key
3. Server responds with the certificate (public key)
4. Client creates a pre-master secret, encrypts it with the F5 public key, and sends it to BIG-IP LTM
5. BIG-IP sends the pre-master secret (encrypted key) in the HSM, decrypts it with the F5 private key on HSM
6. BIG-IP LTM retrieves page from app server
7. Client and BIG-IP LTM communicate using the symmetric key

Thales Luna Network HSM

Luna Network 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 2, Level 3, or Common Criteria EAL 4+ certified, 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. With Luna Network HSM as a security infrastructure's trusted root, administrators can ensure the integrity of their cryptographic operations.

Key Benefits

Virtual editions available for the cloud

- Benefit from a flexible solution to meet your enterprise needs regardless of the environment
- BIG-IP and Luna Network HSMs are available for deployment in enterprise, private, hybrid and public clouds

High-performance processing

- Offload cryptographic functions to improve data center performance with high processing speeds
- Luna Network HSMs are capable of processing up to 10,000 RSA and 22,000 ECC transactions per second

Robust security

- Security is of utmost importance to protecting network activity
- Luna Network HSMs offer the highest level of tamper-resistant security, and have been validated to be compliant with FIPS 140-2 Level 2, Level 3 and Common Criteria EAL 4+ standards

Meet compliance standards

- Help meet data governance requirements with high-assurance hardware key storage
- Luna Network HSM's high performance and high-assurance protection make demonstrating compliance easier
- Generating, managing, and storing keys in a centralized, FIPS-validated, secure environment ensures complete key and data ownership

Key features

Robust security

BIG-IP stores in Luna Network HSMs the private keys and associated certificates used by BIG-IP LTM to authenticate servers involved in SSL transactions. With Luna Network HSM as the root of trust, organizations can securely send data and deliver applications through protected SSL tunnels. Data is encrypted before it travels and the keys necessary to decrypt that data never leave the hardware appliance, thus eliminating the possibility that data will be intercepted while in clear text. Together, the solution mitigates risk from attacks by both deflecting them and securing the internal resources so that data is not in legible if a breach occurs.

High availability

BIG-IP LTM ensures high availability by redirecting traffic to separate, functioning data centers in the case of a site's disruption. Because BIG-IP ensures that there can be no single point of failure, applications remain persistently accessible. As a complement, multiple Luna Network HSMs can be configured for high availability so encryption keys are always available to secure SSL transactions. Multiple HSMs can be grouped in high availability (HA) configurations to scale performance to process tens of thousands of transactions per second. Luna Network HSM's integration in BIG-IP environments ensures that encryption keys and certificates are always protected and available to identify servers and secure the transport layer.

Secure the transport layer while improving data center performance

BIG-IP stores, processes and encrypts both keys and data in Luna Network HSMs. By offloading these cryptographic functions from general servers, Luna Network HSMs free valuable compute resources. Capable of performing thousands of cryptographic transactions per second, Luna Network HSMs support the most demanding SSL operations. Not only does Luna Network HSM secure valuable encryption materials in a tamper-resistant appliance, it adds value to any environment by taking on resource intensive cryptographic operations, improving overall data center performance.

Conclusion

Thales and F5 join together to secure and optimize the delivery of corporate applications. With Luna Network HSMs, organizations can trust that the data traveling in its BIG-IP managed network is encrypted and secure from unauthorized users. Whether the attack is aimed at denying service or stealing valuable data, the BIG-IP/ Luna Network HSM solution provides a high-performance, robust and reliable answer for security administrators.

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.