

F5 AND THALES SOLUTION PROVIDES DEDICATED SSL TERMINATION, OFFLOAD AND ACCELERATION WITH CERTIFIED TAMPER-RESISTANT KEY GENERATION AND MANAGEMENT

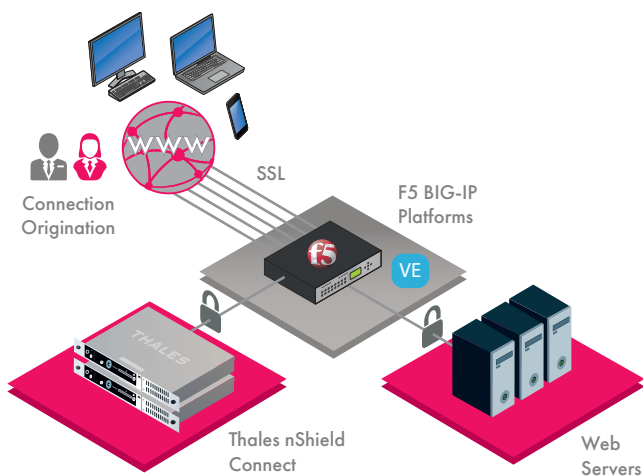
► Solution Benefits:

- Intelligent traffic management reduces burden on servers for speed and high availability
- Real-time analysis of network and applications delivers greater visibility and control
- Data center and web firewalls protect against Layer 7 DDoS and web application attacks
- Trusted FIPS 140-2 Level 3 certified platform secures keys and certificates
- Easy setup enhances performance and meets traffic volume requirements



Thales e-Security

Thales Enhances Security of F5 BIG-IP Platforms



Thales nShield Connect HSMs integrate with F5 BIG-IP to protect SSL encryption/decryption keys and certificates within a high assurance environment.

The Problem: Growing volumes of security-sensitive Internet traffic require protection

- Increasing use of web applications and cloud-based services is driving growth in numbers of secure sockets layer (SSL) connections. Web traffic, including user IDs, login passwords and sensitive account numbers is commonly encrypted and transported using SSL.

The Challenge: Increasing SSL connections impact operational performance

- High volume SSL encryption/decryption is a resource-intensive process that impacts web server performance. F5 BIG-IP efficiently manages high volume SSL traffic by terminating connections in a dedicated appliance. BIG-IP optimizes the network infrastructure to deliver high availability and security for critical business applications.

Increasing SSL traffic results in higher numbers of keys and certificates. Safeguarding and managing these critical components represents an additional challenge in traditional software environments where they might be exposed to targeted threats.



THALES ENHANCES SECURITY OF F5 BIG-IP PLATFORMS

The Solution: F5 and Thales together deliver high performance and enhanced security

With F5, customers can simultaneously manage high volume SSL connections to deliver secure connectivity while meeting operational demands. Organizations looking to further extend the security of SSL-based operations can deploy F5 BIG-IP with Thales network-based hardware security modules (HSMs) to achieve operational efficiency and high assurance. Thales nShield Connect HSMs safeguard and manage large numbers of critical SSL keys and certificates within a dedicated, hardened device, ensuring that keys are never exposed to unauthorized entities.

Regulated customers in government, financial services, healthcare and other industries require high assurance solutions that are independently certified to internationally recognized security standards. Integration of BIG-IP with nShield Connects provide FIPS 140-2 Level 3 certified protection, which enables organizations to deliver a high assurance environment and comply with industry best practices. Thales nShield Connects also enable auditable key and certification validation per established security policies, including enforcement of dual controls and separation of duties. Regulated customers are often required to use FIPS-approved HSMs, and Ponemon Institute research shows that auditors recommend the use of HSMs to facilitate audit and regulatory compliance.

Why use HSMs for SSL connections?

While it's possible to terminate SSL connections in a dedicated appliance, SSL keys handled outside the cryptographic boundary of certified HSMs are significantly more vulnerable to attacks which could lead to disclosure of confidential information. HSMs are the only proven and auditable way to secure valuable cryptographic material. HSMs enable organizations to:

- Secure keys and certificates within carefully designed cryptographic boundaries that use robust access control mechanisms so keys are only used for their authorized purpose
- Ensure availability by using sophisticated key management, storage and redundancy features to guarantee keys are always accessible when needed
- Deliver high performance to support increasingly demanding transaction rates

Thales

nShield Connect is a high performance, network-attached HSM for high-availability web server and data center environments. Certified to stringent security standards, nShield Connect:

- Stores keys for signing and issuing digital certificates in secure and tamper resistant environment
- Complies with regulatory requirements for public sector, financial services and enterprises
- Manages administrator access with smart card based policy and two-factor authentication
- Administers unattended HSMs in remote locations and eliminates need to delegate authority
- Supports high performance elliptic curve cryptography (ECC)

F5

BIG-IP is an application delivery controller that provides load balancing, acceleration and security for hardware platforms or virtual instances to ensure applications are fast, secure and available. Using a shared and flexible architecture, BIG-IP:

- Provides application health monitoring and ensures availability
- Controls application acceleration, security and availability using F5 **TMOS**
- Manages application networking services using F5 **iApps**
- Delivers scalable incremental functions as needed using flexible modular **BIG-IP application delivery services**
- Manages workloads between on-premises and cloud environments using F5 **ScaleN**

For more detailed technical specifications, please visit www.thales-esecurity.com or www.f5.com

F5 and Thales deliver enhanced security for application delivery controllers, enabling effective management of high volume SSL traffic while protecting critical SSL keys.

Follow us on:

