nCipher
AN ENTRUST DATACARD COMPANY

www.ncipher.com

F5 and nCipher provide dedicated SSL termination, offload and acceleration with certified tamper-resistant key generation and management

- Intelligent traffic management delivers speed and high availability
- Network and application analytics provide visibility and control
- Data center and web firewalls protect against Layer 7 DDoS and web application attacks
- FIPS 140-2 Level 3 platform secures keys and certificates
- Easy setup enhances performance and traffic volume

nCipher enhances security of F5 BIG-IP platforms

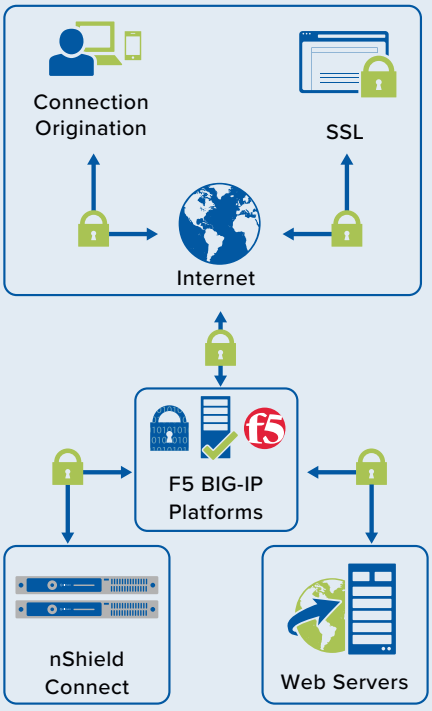
THE PROBLEM: GROWING VOLUMES OF SECURITY-SENSITIVE INTERNET TRAFFIC REQUIRE PROTECTION

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. F5 BIG-IP application delivery controllers (ADCs) optimize the network infrastructure to deliver high availability and security for critical business applications.

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



nCipher nShield Connect HSMs integrate with F5 BIG-IP ADCs to protect SSL encryption/decryption keys and certificates within a high security environment. nCipher nShield can be deployed on-premises or as a service.

nCipher enhances security of F5 BIG-IP platforms

THE SOLUTION: F5 AND NCIPHER 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 nCipher network-based hardware security modules (HSMs) to achieve operational efficiency and high assurance. nCipher 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 security solutions that are independently certified to internationally recognized security standards. Integration of F5 BIG-IP platforms including LTM, APM, ASM (WAF), AFM, and GTM (DNSSEC), with nCipher nShield Connect HSMs, provide FIPS 140-2 Level 3 certified protection, which enables organizations to deliver a high security environment and comply with industry best practices. Deployed on-premises or as a service, nCipher nShield also enables 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 NCIPHER NSHIELD CONNECT WITH F5 BIG-IP ADCS?

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. nCipher nShield Connect 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

NCIPHER

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:

- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, CNG, nCore, and nShield Web Services Crypto API)
- 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)

nCipher nShield is available in several form-factors: as an appliance, PCIe, USB, and as a service.

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

nCipher nShield is available in several form-factors: as an appliance, PCIe, USB, and and as a service.

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

For more detailed technical specifications, please visit www.ncipher.com or www.f5.com

Search: nCipherSecurity

www.ncipher.com

nCipher AN ENTRUST DATACARD COMPANY