Entrust enhances security of F5 BIG-IP platforms

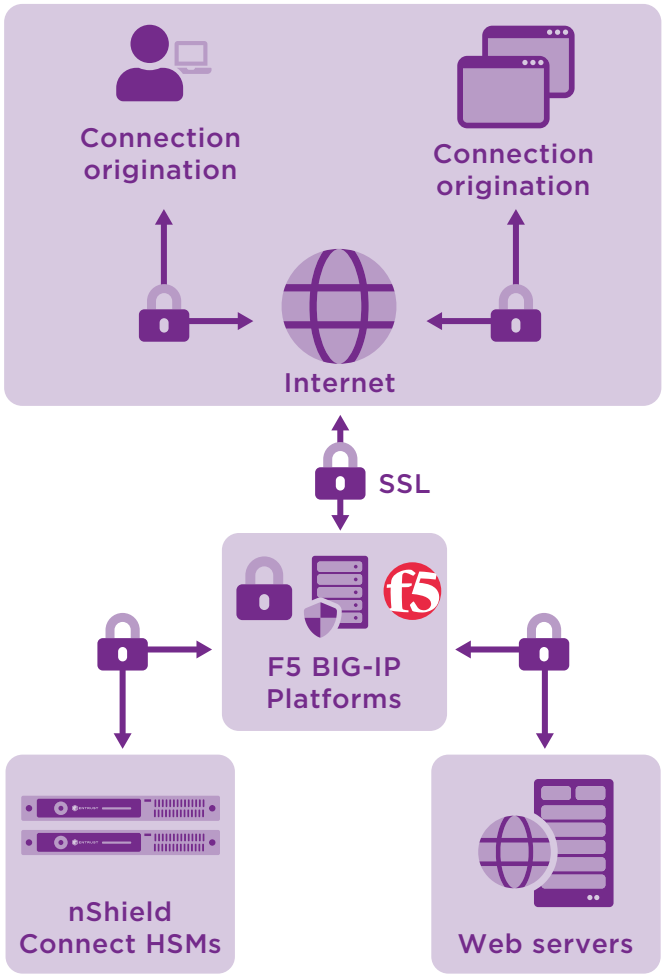
F5 and Entrust provide dedicated SSL termination, offload and acceleration with certified tamper-resistant key generation and management

HIGHLIGHTS

- 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 Distributed Denial of Service (DDoS) and web application attacks
- FIPS 140-2 Level 3 platform secures keys and certificates
- Easy setup enhances performance and traffic volume

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.



Entrust nShield® Connect hardware security modules (HSMs) integrate with F5 BIG-IP application delivery controllers (ADCs) to protect SSL encryption/decryption keys and certificates. nShield HSMs can be deployed on-premises or as a service.

LEARN MORE AT ENTRUST.COM/HSM

Entrust enhances security of F5 BIG-IP platforms

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 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.

The solution: F5 and Entrust 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 Entrust network-based HSMs to achieve operational efficiency and high assurance. Entrust 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 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, nShield HSMs 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 Entrust nShield Connect HSMs 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. 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

Entrust enhances security of F5 BIG-IP platforms

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial and government organizations. Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

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

Entrust nShield HSMs are available in several form-factors: as an appliance, PCIe, USB, and as a service.

www.f5.com

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

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com