nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

High assurance protection of master keys

- Protect website and applications against fraud, data theft and other cyberattacks
- 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
- Facilitate auditing and compliance with data security regulations

NFINITY
STRATEGIC TECHNOLOGY
PARTNER PROGRAM

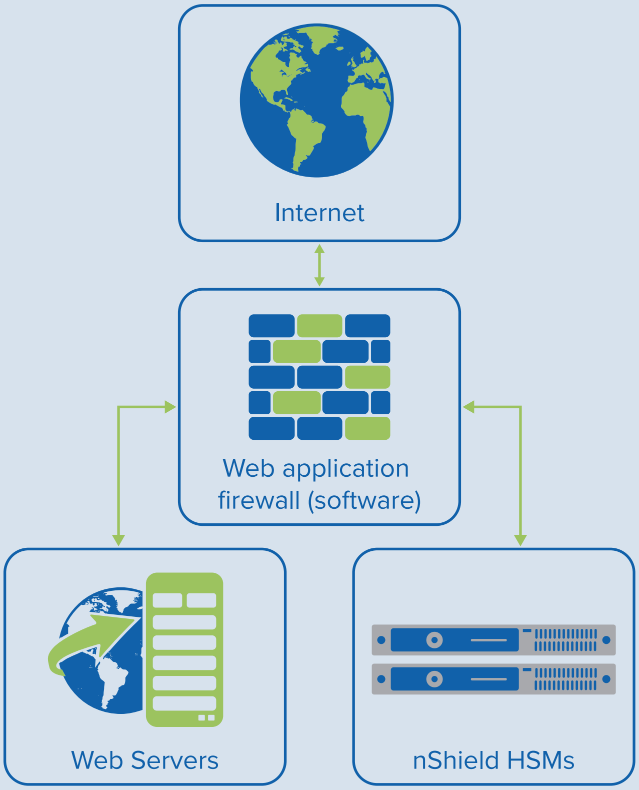
nShield HSMs enhance the security of web application firewalls

THE CHALLENGE: INCREASED CONNECTIVITY LEADS TO NEW ATTACKS

Web applications and cloud-based services are essential tools for today's enterprise but they create additional exposure to data security risks. To help address these risks, organizations implement web application firewalls (WAFs), which filter and monitor traffic and can detect, block, and prevent attacks such as cross-site scripting, SQL injection, zero-day exploits, malware infections, impersonation, and other threats.

While WAFs use encryption to ensure validated connections and protect the confidentiality and integrity of data, this must be coupled with strong protection of the encryption keys. Storing encryption keys outside of a cryptographic boundary can leave an organization vulnerable to attacks while creating a false sense of security.

Additionally, many compliance mandates, such as PCI DSS and national critical infrastructure regulations, call for strong safeguarding of encryption keys. The use of hardware security modules (HSMs) for key protection not only meets compliance standards but is also an accepted security industry best practice.



Leading web application firewalls use nShield HSMs to protect the master key used to encrypt private keys and passwords.

nShield HSMs enhance the security of web application firewalls

THE SOLUTION: WEB APPLICATION FIREWALLS INTEGRATED WITH NSHIELD HSMs

Next-generation web application firewalls help enterprises block, detect and prevent attacks, as well as encrypt content to ensure validated connections and protection of sensitive data. nCipher hardware security modules (HSMs) integrate with leading web application firewalls to protect the master key used to encrypt all private keys and passwords, as well as the private keys used for SSL/TLS encryption, providing unassailable roots of trust and enhanced network security. The nShield line of HSMs have earned both FIPS 140-2 and Common Criteria certifications, ensuring that the web application firewall environment meets compliance requirements.

THE NSHIELD DIFFERENCE

nCipher nShield HSMs protect privileged account keys and passwords in a dedicated, hardened environment. Keys handled outside the cryptographic boundary of certified HSMs are significantly more vulnerable to attacks, which can lead to disclosure of confidential information. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield HSMs:

- Secure keys and certificates within carefully designed cryptographic boundaries
- 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
- Support compliance with mandates related to critical infrastructure, government, banking and other industries

nCipher has worked with solution and application providers for decades to address a wide range of data protection-related business issues including:

- Device credentialing for the Internet of Things
- Cloud computing, big data, and application security
- Regulatory compliance and industry mandates
- Intellectual property protection
- Secure credentialing

NFINITY PARTNERS

Palo Alto Networks® Next-Generation Firewall integrates with nShield Connect HSMs to enhance the security of the master key used to encrypt private keys and passwords. The HSM also safeguards and manages private keys used in the SSL/TLS decryption process – providing a root of trust that enhances the complete network security posture.

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com

STRATEGIC TECHNOLOGY PARTNER PROGRAM

Search: nCipherSecurity

www.ncipher.com

AN ENTRUST DATACARD COMPANY