SOLUTION BRIEF

A10 AND nCIPHER STRENGTHEN THE SECURITY OF APPLICATION DELIVERY PLATFORMS

A10 THUNDER INTEGRATES WITH nCIPHER nSHIELD TO DELIVER FIPS 140-2 LEVEL 3 PROTECTION OF TLS/SSL KEYS

Organizations increasingly depend on application networking solutions to run critical business processes that involve private and sensitive information. To fulfill demands of businesses, data centers, networks and applications must not only be available 24-7 and run at optimum speeds, but must also protect against attacks that could compromise the confidentiality and integrity of the data they process.

With the reliance on web application services, sensitive information exchanged online and in the cloud is at risk of interception and exploitation. Transport layer security/ secure sockets layer (TLS/SSL) is used to protect sensitive information by encrypting the data. However, a compromise of the encryption keys can lead to a breach of the data flowing between end-user devices and Web servers. With growing use of TLS/SSL, protecting and managing the underpinning cryptographic keys is a vital function.

THE CHALLENGE

As organizations and businesses increasingly deliver services through Web and cloud-based applications, more sensitive data is transacted over TLS/SSL tunnels to protect confidentiality. TLS/SSL is a resource-intensive process that demands high utilization of servers to meet application performance and availability requirements.

Application delivery controllers (ADC) are designed to optimize an organization's ability to deliver services and meet customer demands, providing high availability, acceleration and

CHALLENGE

Protecting and managing the increasing numbers of TLS/SSL keys—without impacting application delivery, performance or compliance requirements—is critically important in today's business environment.

SOLUTION

A10 Thunder ADC integrates with nCipher nShield hardware security modules (HSMs) to protect and manage the TLS/SSL keys. As part of this integration, keys are stored in the hardware of nShield HSMs, and encryption- and signature-processing (involving private keys) are executed within its protected boundary. This provides robust protection and management of the cryptographic keys and encryption process.

BENEFITS

- Delivers secure application availability and acceleration
- Strengthens TLS/SSL cryptographic key management
- Enables robust FIPS 140-2 Level 3-certified security
- Provides high-performance TLS/SSL transactions
- Supports virtual and cloud-based environments

security. Increased volumes of TLS/SSL-encrypted traffic across networks requires careful safeguarding and management of the keys to ensure their availability and security.

Protecting and managing large numbers of TLS/SSL keys — without impacting the application delivery process and in a manner that is transparent to the user — is critically important for security. As organizations are increasingly required to comply with regulatory mandates for the protection of sensitive data, solutions that provide a root of trust, enable compliance and facilitate security auditing help fulfil operational demands.

THE A10 & nCIPHER SOLUTION

A10 Thunder ADC enables customer applications to be highly available, accelerated and secure. Able to run as a dedicated appliance or in a clustered configuration, Thunder ADC delivers high throughput to fulfill the most demanding needs of today's business.

Deployed in dedicated, hosted or cloud environments, Thunder ADC scales to meet customer demand and ensure business continuity. The ADCs provide application acceleration for efficient operations and reduced infrastructure requirements to drive down capital and operational costs.

Employing robust key protection and management features through the integration with nCipher nShield HSMs, Thunder ADC provides security for compliance and risk reduction. The solution supports TLS/SSL acceleration features by offloading processing from the application servers to the ADC. Supporting various protocols, including HTTP/HTTPS and FIX, this solution delivers security and high performance to ensure end-users have a positive online experience.

Protecting and managing large numbers of TLS/SSL keys within a FIPS 140-2 Level 3-certified environment, the combined A10 and nCipher solution optimizes traffic flow and eliminates the exposure of sensitive data within the IT infrastructure. This protects against advanced and emerging attacks for uninterrupted operations while meeting required regulatory compliance obligations.

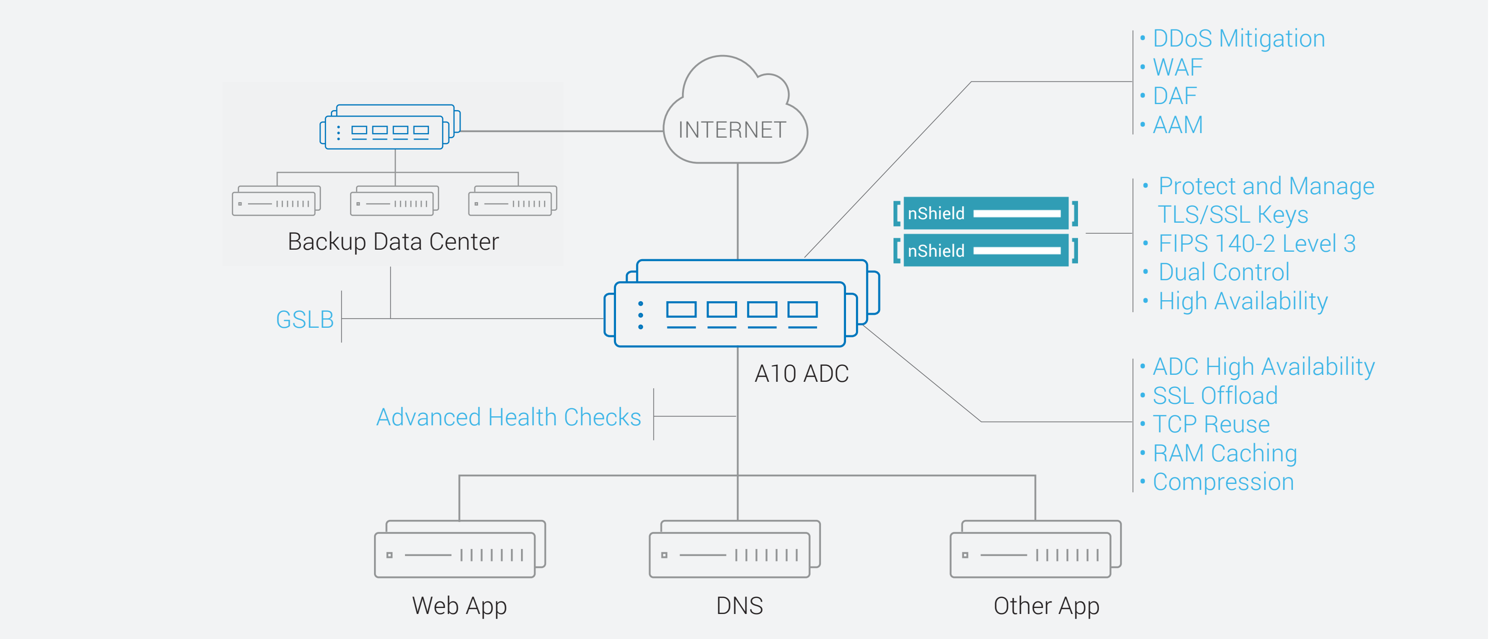

Figure 1: A10 Thunder ADC integrates with nCipher nShield HSM to secure and manage TLS/SSL keys inside a FIPS 140-2 Level 3 environment.

FEATURES AND BENEFITS

With the A10 Thunder and nCipher nShield HSMs, customers enjoy high availability, accelerated performance, and robust security, complying with FIPS 140-2 Level 3. TLS/SSL keys handled outside the cryptographic boundary of a certified HSM tend to be more vulnerable to attacks, which could result in a disclosure of confidential information. HSMs are the only proven and auditable way to secure valuable cryptographic material such as TLS/SSL keys. 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 increasing transaction rates

nCipher nShield HSMs are high-performance, network-attached HSMs for high-availability Web server and data center environments. Certified to stringent security standards, nShield HSMs:

- Store TLS/SSL keys in a secure and tamper-resistant environment
- Comply with regulatory requirements for public sectors, financial services and enterprises
- Manage administrator access with smartcard-based policy and two-factor authentication
- Administer unattended HSMs in remote locations and eliminate need to delegate authority

SOLUTION COMPONENTS

The joint A10 and nCipher solution includes:

- A10 Thunder Series ADC or CFW running ACOS 4.1 (verified with ACOS 4.1.1-P1)
- nCipher nShield Connect HSM

INCREASE PERFORMANCE AND LOWER OPERATIONAL COSTS WITH A10 AND nCIPHER SECURITY SOLUTION

A10 provides a range of high-performance application networking solutions that help organizations ensure that their applications and networks are always available, operate at peak speed, and that the data they process is always secured.

TLS/SSL is used to protect sensitive information, robust security requires the protection and management of the underpinning keys used to encrypt the data.

A10 Thunder ADC integrates with nCipher nShield HSM to protect and manage critical TLS/SSL keys within a robust FIPS 140-2 Level 3 security boundary for high-assurance protection and to facilitate regulatory compliance.

NEXT STEPS

To learn more about the joint A10 Networks and nCipher solution, please contact your A10 representative or visit a10networks.com.

ABOUT nCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) enables service providers, cloud providers and enterprises to ensure their 5G networks and multi-cloud applications are secure. With advanced analytics, machine learning and intelligent automation, business-critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers in 117 countries worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19172-EN-03 MAR 2020