LEVERAGING SYMANTEC CIC AND A10 THUNDER ADC TO SIMPLIFY CERTIFICATE MANAGEMENT

Identify, Monitor and Manage All Digital Certificates Present

Challenge:

Many IT environments encounter decentralized SSL key deployments. To ensure proper key and certificate management, administrators must identify every certificate present, including those on network infrastructure solutions such as application delivery controllers (ADCs).

Solution:

A10 Thunder ADC is fully interoperable with Symantec's Certificate Intelligence Center (CIC) and provides visibility over all digital certificates installed on these A10 network-aware appliances.

Benefits:

- Administrators can track thousands of SSL certificates from multiple providers to protect websites and visitors.
- Fully discoverable certificates can be stored on the Thunder ADC appliance to eliminate certificate duplication.
- Consolidates and simplifies critical security information such as the location of certificates, key sizes, ciphers used and validity dates.
- Supports the creation of self-signed certificates. In the event of an SSL vulnerability outbreak, administrators can avoid patching web servers.
- A10's aXAPI supports the integration and programmability to Symantec's CIC to ensure the necessary visibility.

The information explosion and the accelerating adoption of cloud computing and e-commerce are making Internet security a critical priority. As more and more applications become web-based and require encryption, privacy for computing transactions such as online shopping sites, portals, email and other applications is now more important than ever. Users must feel confident that they are at legitimate websites before sharing valuable information. Additionally, the popularity of social media and online collaboration in the modern enterprise makes the use of Secure Sockets Layer (SSL) and Transport Layer Security (TLS) encrypted sessions essential. Online users are sharing increasingly large volumes of personal and professional information, and they need to know that their accounts will not be compromised.

The Challenge

Organizations are challenged to keep up with threats and evolving standards and need real-time, aggregated data to continually assess and strengthen their security posture. Management and organization of digital certificates and their keys is a critical component of that. SSL certificates make it possible for users around the world to communicate sensitive information with the confidence that it is safe from snooping by malicious hackers, allowing anyone to confidently use the web for business and personal interactions, including banking, shopping, social media and product development.

As SSL certificates are deployed to secure transactions and information through these different activities, the management of SSL certificates becomes more challenging. This is especially true in a mixed environment where SSL certificates are from different Certificate Authorities (CAs) or include self-signed certificates. Organizations are constantly adding, removing or redeploying servers to meet business needs. At the same time, business units within an organization might be executing their own SSL certificate initiatives. This fluid and dynamic environment creates challenges for organizations to account for all SSL certificates at any given time, including self-signed certificates and certificates from any CAs across ten, to hundreds, to thousands of servers and the associated applications.

Without proper certificate management, organizations can have SSL certificates in their systems that have expired or are noncompliant. This situation can adversely affect business continuity and erode brand value. A robust, easy-to-use SSL certificate management system can help an enterprise avoid the consequences of loss of business, productivity, noncompliance and risks of security breach.

The A10 Networks Symantec Solution

Through its partnership with Symantec, A10 Networks simplifies and consolidates key management, allowing customers to dramatically reduce the number of keys required by centralizing certificates for thousands of web servers at a time, versus provisioning a certificate for each server directly. Through the Symantec Certificate Intelligence Center (CIC) integration with A10 Networks® Thunder® ADC line of Application Delivery Controllers,

customers can gain real-time visibility of all certificates, including all of those present on A10 devices in the network. Other benefits include expiration alerts to avoid disruption, optimizing certificate usage, eliminating gaps in security coverage and reducing operational costs.

Symantec Certificate Intelligence Center

Symantec CIC helps discover, catalog and track all SSL certificates so that organizations can mitigate the risks of having SSL certificates coming from breached or high-risk CAs or that are incompatible with industry best practices. Rich and detailed information, including security ratings on all SSL certificates, help administrators ensure that they are compliant with corporate policies and industry standards. CIC allows the auto renewal of SSL certificates to greatly simplify operations.

Discover and monitor all SSL certificates to help avoid certificate expiration

Expired, high-risk, rogue or unknown certificates can adversely affect business and erode brand value. Most prospective consumers or other visitors will not continue an online transaction if they see a browser warning page on the SSL security of that website. The Symantec CIC cloud-based service helps organizations have central control over all of their SSL certificates. Administrators can get summary and detailed information via a central, easy-to-use dashboard. Notifications, alerts and reports help facilitate timely interventions to prevent business disruptions.

Get security ratings on all SSL certificates to mitigate noncompliance and security risks

Organizations are continually adding, removing or redeploying servers to meet business needs. At the same time, business units within an organization could be executing their own SSL certificate initiatives. This constantly changing environment creates challenges for organizations to account for all SSL certificates at any given time, including self-signed certificates, and certificates, including those based on PFS and ECHDE, from any CAs. Symantec CIC helps discover, catalog and track all SSL certificates so that organizations can mitigate the risks of having SSL certificates from breached or high-risk CAs, or those that are incompatible with industry best practices. Rich and detailed information, including security ratings on all SSL certificates, encryption cyphers and key sizes, help administrators ensure that all SSL certificates in the organization are compliant with corporate policies and industry standards.

Automate SSL certificate lifecycle management to increase operational efficiency

Organizations are facing increasing demands for their IT services to manage industry trends that add to the complexity of their environments. Simultaneously, budgets are constrained and resources are reduced or have remained the same. Symantec CIC end-to-end SSL certificate lifecycle management includes the automation of manual, routine actions to help ensure efficiency, consistency and accuracy. This capability gives IT teams the time to focus on other mission-critical tasks while providing auditable records for accountability. In addition, administrators can run automated upgrades of non-Symantec to Symantec SSL certificates, allowing management to further streamline the SSL environment and take advantage of vendor consolidation.

Deliver and maintain SSL security by leveraging best-in-class SSL certificate management service

Organizations rely on SSL certificates to protect information and assure customers of their authenticity. Maintaining a secure environment with 24x7 SSL protection requires a dependable and scalable certificate management service. Symantec CIC helps enterprises maintain SSL protection with best-in-class service delivered on a proven and robust infrastructure. Symantec was the first Certificate Authority to provide commercial SSL protection, and has experienced 100% uptime since 2004 with its validation infrastructure. Easy deployment, configurable controls and fast scanning are capabilities ideal for large and growing organizations. In addition, Symantec CIC for Mobile, the first mobile capability for SSL certificate management, provides actionable intelligence anytime, anyplace.

A10 Thunder Application Delivery Controllers and SSL Support

Comprehensive application delivery optimization

A10 Thunder ADC platforms solve many of the challenges facing organizations of all types, including enterprises, cloud service providers, telecommunications, cloud computing and government. These all-in-one solutions help IT administrators realize the potential of their network infrastructure investments while dramatically lowering overall costs. Thunder ADC consolidates numerous "point products" into one scalable ultra-high capacity appliance by providing application acceleration via caching, compression and TCP optimization, server availability with local and global Layer 4-7 load balancing and security with web application and DNS firewalls, Distributed Denial of Service (DDoS) protection, authentication support and A10 Networks SSL Insight™ technology.

SSL offloading and centralized key management

The widespread use of SSL encrypted data strains firewalls, intrusion prevention systems, and many other infrastructure components that are used to inspect traffic, deflect intrusions and quarantine or drop malware. Decentralizing SSL key management to each of these solutions further complicates security management and potentially reduces certificate visibility. A10 Thunder ADC leverages SSL Insight to offload CPU-intensive SSL decryption functions and enable security devices to inspect all traffic, not just clear text.

Features and Benefits

Thunder ADC's SSL Insight feature provides a forward proxy to allow inspection of SSL traffic. These purpose-built appliances with SSL hardware acceleration process traffic with 1024-, 2048- or 4096-bit certificates at sustainable SSL encryption rates exceeding 40 Gbps and over 170,000 new SSL connections per second (with 2048-bit certificates). Thunder ADC decrypts SSL-encrypted traffic and forwards it to a third-party security device like a firewall for deep packet inspection (DPI). Once the traffic has been analyzed and scrubbed, Thunder ADC re-encrypts it and forwards it to the intended destination.

Thunder ADC appliances not only offload SSL traffic to reduce the load on application servers with reverse proxy functionality, they also streamline SSL key management and lower certificate overhead. Certificates are stored on the Thunder ADC appliance with its hardened operating system to enhance security, reduce the expense of costly duplication of certificates on the application servers and minimize management complexity. Administrators avoid procuring and handling SSL certificates for each individual server. A10 also supports the creation of self-signed certificates for simplification. In the event of an SSL vulnerability outbreak such as Heartbleed, administrators can avoid patching countless web servers. Organizations provision an SSL certificate automatically or manually to prevent users from seeing an "untrusted root" error typically generated from an internal untrusted certificate server.

Symantec's CIC demonstrates proven interoperability with A10 Thunder ADC, providing customers with a consolidated and simplified method for managing critical security information such as the location of certificates, key sizes, ciphers used and validity dates. Combining these two solutions provides a complete view of an organization's digital certificates and keys for efficient operations.

Symantec's CIC provides the necessary visibility and reporting to ensure that Thunder ADC is using the latest standards supported, via the A10 Networks aXAPI® REST-based API integration and programmability. Emerging standards in SSL/TLS supported include:

- Perfect Forward Secrecy (PFS) and Elliptic Curve Diffie–Hellman Exchange (ECDHE)
- Risk assessment of SHA-1 certificates and vulnerabilities similar to Heartbleed and SSL 3.0
- Key size migration status compliance from 1024- to 2048-bit keys
- Emerging use case of 4096-bit keys, where usage can top twenty percent

Summary – Simplify Certificate Management with Symantec CIC and A10 Thunder ADC

Together, Symantec CIC and Thunder ADC overcome the pitfalls of SSL certificate management. IT administrators can be confident that their online data communications are protected. And, by combining these tools, the following benefits can be realized:

- Simplifies the discovery of all certificates throughout the network, including all those installed on A10 Thunder networking and security devices
- Efficiently tracks thousands of SSL certificates from multiple providers with up-to-date knowledge of critical parameters, including expiration times; ensures that websites are protected and visitors safeguarded from hacking
- Manages self-signed certificates, preventing them from being unaccounted for and ensuring that there are no violations of organizational policy
- Automates and ensures correctly installed SSL certificates and business continuity; eliminates browser popup warnings when users try to access the site

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment – from the smallest mobile device to the enterprise data center to cloud-based systems. Our industry leading expertise in protecting data, identities, and interactions gives our customer's confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-SB-19130-EN-01
Nov 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.