SSL INSIGHT FOR RSA SECURITY ANALYTICS

Discover Threats Lurking in SSL Traffic

Challenge:

To gain full visibility into threats, RSA Security Analytics® customers must be able to inspect all traffic, including encrypted traffic.

Solution:

A10 Thunder ADC empowers RSA customers to gain SSL visibility by intercepting SSL traffic and sending it unencrypted to RSA Security Analytics for inspection and analysis.

Benefits:

- Uncover threats concealed in encrypted traffic by decrypting SSL traffic at high speeds
- Investigate, prioritize and remediate incidents with unprecedented precision and speed
- Detect and analyze even the most advanced attacks before they can impact the business
- Scale RSA Security Analytics deployments with load balancing

Encryption Reduces Visibility

Threats continually evolve. Today, attackers conduct extensive reconnaissance on targeted organizations, identifying employee names and email addresses, business applications and more. To stay ahead of attackers, security teams must adapt. Unfortunately, many security teams miss attacks or they don't have the expertise needed to keep up with new attack techniques.

On top of these threats, organizations must contend with growing SSL bandwidth use. To prevent snooping, manipulation and theft, an increasing number of applications encrypt data using SSL or TLS. While many web applications used to only encrypt sensitive communications such as credit card transactions and user logins, now, they encrypt every web request and response. In fact, according to NSS research, 25 - 35% of enterprise traffic is SSL and, depending on the industry vertical, the percentage of SSL traffic can approach 70%[1].

To protect applications and data, organizations must inspect all traffic, including encrypted data. Unfortunately, many security devices cannot inspect encrypted traffic, and the few that can decrypt SSL traffic often cannot keep pace with growing SSL bandwidth demands, exposing dangerous gaps in corporate defenses.

SSL Insight and RSA Security Analytics

A10 Networks has partnered with RSA, the Security Division of EMC, to uncover malicious activity that would otherwise be hidden in SSL traffic. The A10 Networks® Thunder™ ADC line of high-performance, next-generation application delivery controllers, with its integrated SSL Insight™ technology, terminates and decrypts SSL traffic. Thunder ADC then sends decrypted traffic to RSA Security Analytics for inspection and analysis.

Thunder ADC functions as an SSL forward proxy to intercept SSL traffic. In an RSA Security Analytics and Thunder ADC deployment, the Thunder ADC appliance is installed between internal clients and the Internet. As shown in Figure 1:

1. Thunder ADC decrypts outbound SSL traffic and sends a copy of the unencrypted traffic to RSA Security Analytics for forensics analysis.
2. Thunder ADC encrypts the HTTP request and forwards it to a web server.
3. The web server sends an encrypted response to Thunder ADC.
4. Thunder ADC decrypts the response and forwards a copy of the unencrypted traffic to the RSA Security Analytics for inspection and analysis.
5. Thunder ADC encrypts the web server response and sends it to the client.

[1] NSS Labs, SSL Performance Problems, https://www.nsslabs.com/system/files/public-report/files/SSL%20Performance%20Problems.pdf

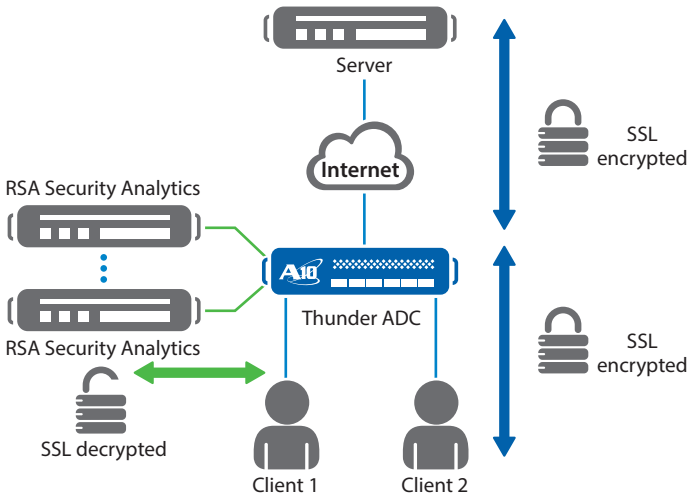

Figure 1: Thunder ADC decrypts and forwards traffic to RSA Security Analytics.

A10 Networks' SSL Insight ensures that connections between internal clients and servers are encrypted to prevent unwanted snooping and data theft. It also ensures that all inbound and outbound network traffic can be properly inspected and analyzed, providing complete visibility into network activity.

With its load balancing capabilities, Thunder ADC also provides high availability and scale, enabling organizations to deploy multiple RSA Security Analytics platforms in non-inline mode and, in the event of a hardware or network failure, to send network data to an available RSA Security Analytics platform. Select Thunder ADC models can distribute SSL Insight traffic streams to up to four RSA Security Analytics servers. For example, Thunder ADC can forward intercepted traffic from one group of internal IP addresses to a specific RSA Security Analytics server and from a second group of IP addresses to a second RSA Security Analytics server. By segmenting out traffic, Thunder ADC can efficiently scale RSA Security Analytics deployments.

SSL Challenges

SSL termination, which involves encrypting and decrypting many sessions simultaneously, is an extremely CPU-intensive task. Increasing security strength calls for an exponential increase in CPU power.

Encryption strength is determined in part by SSL key length. 2048-bit SSL certificates require approximately 3.4 times more processing power to encrypt and 6.3 times more processing power to decrypt than 1024-bit certificates[2], whereas 4096-bit certificates require roughly 25 times more processing power than 1024-bit certificates to decrypt.

The transition from 1024- to 2048-bit key lengths, spurred on by NIST Special Publication 800-131A, has burdened devices that encrypt and decrypt SSL traffic. Customers who want to increase their security beyond minimum SSL certificate key lengths should expect a dramatic performance impact on their servers and their load balancers. A device used to intercept and inspect SSL traffic, therefore, must possess the computing power needed to manage multiple sessions simultaneously, establish many SSL connections per second and handle larger SSL keys sizes.

High Performance with Powerful Security Processors

The initial SSL handshake is the most computationally demanding part of SSL encryption. Encrypting and decrypting the bulk data of a session is still CPU-intensive, but to a lesser degree. A10 Thunder ADC has been architected to manage many secure connections simultaneously. A10 Networks – the first vendor to introduce SSL Insight in an application delivery controller – provides exceptional SSL connection and throughput rates.

Powered by A10 Networks' 64-bit Advanced Core Operating System (ACOS®), Thunder ADC provides linear scalability and offers the maximum performance available from dedicated security processors and switching and routing processors. All models can support SSL offloading, but select models include dedicated high-performance security processors that are exceptionally well suited for managing many SSL sessions simultaneously.

When using conventional CPU resources for establishing SSL connections, performance degrades drastically as SSL key sizes increase. With its next-generation security processors, Thunder ADC delivers near parity performance between 1024- and 2048-bit key sizes, and has the extreme power needed to handle 4096-bit keys at high-rate production levels.

Due to Thunder ADC's granular policies, customers can control which secure sessions to intercept and which to leave encrypted based on the type of traffic, the source or destination IP address and other attributes.

The A10 Thunder ADC product line of high-performance, next-generation application delivery controllers enables customers' applications to be highly available, accelerated and secure. As an added benefit, all features, including SSL Insight, are included without licensing fees.

RSA Security Analytics

RSA Security Analytics is a single security monitoring platform providing the extended visibility that organizations need, by combining logs, network (both packets and NetFlow) and endpoint visibility to see what is happening across the enterprise. This makes it easier to view the environment in totality, rather than in piecemeal, making the analyst more efficient with a much greater chance of detecting attacks.

RSA Security Analytics provides the security team a flexible, modular approach to meet several use cases:

- Complete visibility and rapid investigations through network forensics
- Analytic capabilities way beyond security information and event management (SIEM) and its log-centric approach
- Built-in compliance to keep organizations current with compliance mandates

[2] On commodity hardware, 2048-bit RSA certificates require 6.3x and 3.4x more computational effort, to decrypt and encrypt respectively, than 1024-bit RSA certificates according to a StackExchange analysis.

Conclusion

As more and more applications encrypt data in transit, SSL exposes dangerous blind spots in corporate defenses. A10 Thunder ADC, combined with RSA Security Analytics, offers organizations an ideal, easy-to-deploy and scalable solution for intercepting and securing encrypted traffic. A10 Networks has successfully tested and validated interoperability between RSA Security Analytics and A10 Thunder ADC. Using A10's SSL Insight technology, organizations can:

- Maximize performance, availability and scalability using A10's 64-bit Advanced Core Operating System and specialized security processors
- Integrate with advanced security monitoring platforms such as RSA Security Analytics for event management, forensics and compliance
- Combine security logs, network packet captures and endpoint visibility to see what is happening across the enterprise

A10's powerful SSL Insight capability, included as a standard feature of Thunder ADC, enables businesses to:

- Gain complete visibility into network activity, including encrypted traffic, to uncover attacks and infiltrations
- Use Thunder ADC as a centralized point for load balancing and decryption, intercepting SSL traffic and sending it to multiple security devices, such as security analytics, data loss prevention (DLP), threat protection and intrusion detection appliances, for inspection
- Optionally bypass traffic to sensitive websites, such as communications to banking and healthcare sites, to prevent confidential data from being decrypted
- Future-proof their investment as SSL usage expands and encryption key lengths increase

About RSA Security

RSA, The Security Division of EMC, is the premier provider of intelligence-driven security solutions. RSA helps the world's leading organizations solve their most complex and sensitive security challenges: managing organizational risk, safeguarding mobile access and collaboration, preventing online fraud, and defending against advanced threats. RSA delivers agile controls for identity assurance, fraud detection, and data protection; robust Security Analytics and industry-leading GRC capabilities; and expert consulting and advisory services. For more information, visit: **www.emc.com/rsa**

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-19125-EN-02
Mar 2015

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.

©2015 A10 Networks, Inc. All rights reserved. The A10 logo, A10 Harmony, A10 Lightning, A10 Networks, A10 Thunder, aCloud, ACOS, ACOS Policy Engine, Affinity, aFleX, aFlow, aGalaxy, aVCS, AX, aXAPI, IDaccess, IDsentrie, IP-to-ID, SoftAX, SSL Insight, Thunder, Thunder TPS, UASG, VirtualN, and vThunder are trademarks or registered trademarks of A10 Networks, Inc. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.