SSL INSIGHT FOR QRADAR INCIDENT FORENSICS

Uncover Security Incidents Concealed In SSL Traffic

Challenge:

Forensics tools must have full visibility into all network traffic. QRadar Incident Forensics customers need a solution that can decrypt SSL traffic at high speeds to analyze malicious activity hidden in SSL communications.

Solution:

A10 Networks enables QRadar customers to analyze all data, including encrypted data, by intercepting SSL traffic and sending it to their QRadar Incident Forensics appliances in decrypted form for inspection.

Benefits:

- Eliminate the blind spot in forensics investigations by decrypting SSL traffic at high speeds
- Retrace the step-by-step actions of cyber criminals to understand the magnitude of a breach
- Resolve incidents in minutes or hours instead of weeks with advanced forensics intelligence
- Maximize uptime and scale using best-in-class load balancing and clustering

Advanced Business Partner IBM

Ready For
Security Intelligence

Encryption Complicates Forensics Investigations

Inundated with data – such as never-ending alerts from security devices, network log messages, vulnerability reports and more – many IT security teams cannot prioritize or even keep up with enterprise threats. With too few analysts to manually investigate and remediate incidents, organizations need a solution that can identify high profile events, quickly search network logs, and reconstruct raw network data to isolate malicious activity.

Besides sifting through a mountain of security and networking events, security teams must also contend with encrypted traffic. To prevent snooping, manipulation and theft, an increasing number of applications encrypt data using Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS). SSL usage has become ubiquitous; many leading websites today encrypt every web request and response. In fact, 48% more of the million most popular websites were using SSL in January 2014 than a year earlier.[1]

To protect users, 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 blind spots in corporate defenses.

SSL Insight and QRadar Incident Forensics

A10 Networks has partnered with IBM Security to analyze security incidents and reconstruct events that would otherwise be hidden in SSL traffic. The A10 Networks® Thunder™ ADC, with its integrated SSL Insight™ technology, terminates and decrypts SSL traffic. Thunder ADC then sends decrypted traffic to IBM® Security QRadar® Incident Forensics for inspection and forensics analysis.

Thunder ADC functions as an SSL forward proxy to intercept SSL traffic. In a QRadar Incident Forensics 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 the QRadar Incident Forensics appliance 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 QRadar Incident Forensics appliance for inspection and analysis.
5. Thunder ADC encrypts the web server response and sends it to the client.

[1] Netcraft, January 2014 Web Server Survey

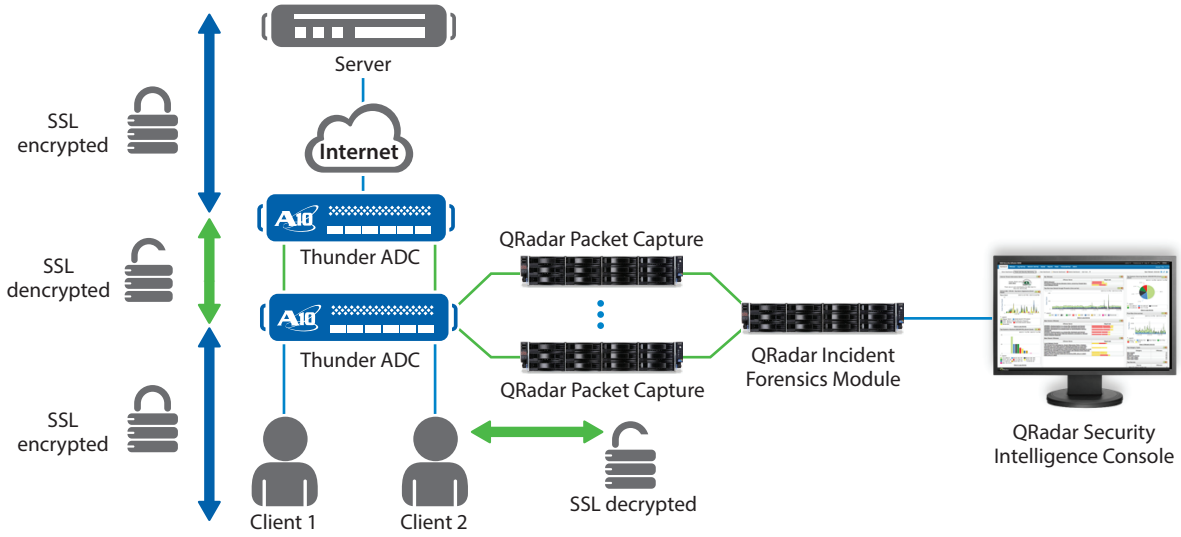

Figure 1: Thunder ADC decrypts and forward traffic to QRadar Packet Capture appliances. QRadar Incident Forensics retrieves packet captures and reconstructs sessions for forensics.

SSL Insight ensures that connections between internal clients and servers are encrypted to prevent unwanted snooping and data theft. SSL Insight ensures that all inbound and outbound network traffic can be properly inspected and analyzed, eliminating SSL blind spots and offering IT security teams peace of mind.

With its inbuilt load-balancing capabilities, Thunder ADC also provides high availability and scale, enabling organizations to deploy multiple QRadar platforms in non-inline mode and, in the event of a hardware or network failure, to send network data to an available QRadar appliance. Select Thunder ADC models can distribute SSL Insight traffic streams to up to four QRadar appliances. For example, Thunder ADC can forward intercepted traffic from one group of internal IP addresses to a specific QRadar appliance and from a second group of IP addresses to a second QRadar appliance. By segmenting out traffic, Thunder ADC can efficiently complement QRadar deployments as multiple packet capture devices are added to scale the solution.

SSL Challenges

SSL termination, which involves setting up and tearing down secure sessions and 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 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, to establish many SSL connections per second (CPS), and to handle larger SSL keys sizes.

A10 ADCs with SSL Acceleration Hardware

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 the 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 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.

[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.

IBM Security QRadar Incident Forensics

IBM Security QRadar Incident Forensics is an integrated forensic search technology designed to complement IBM® QRadar® Security Intelligence Platform by helping IT security teams reduce the time spent investigating security incidents from days or hours to minutes and even seconds, in most cases, while also reducing the need for specialized technical training.

The solution expands security data collection capabilities beyond log events and network flows to include full packet captures and digitally stored text, voice and image documents, presenting better clarity around what happened when, who was involved, and what data was accessed or transferred. As a result, it also helps better remediate a network breach and prevent it from succeeding again.

Conclusion

With more and more applications using encryption to secure communications and data – in fact, SSL now accounts for 25 to 35% of all Internet traffic[3] – SSL exposes dangerous blind spots in corporate defenses. A10 Thunder ADC, combined with QRadar Incident Forensics from IBM Security, 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 QRadar Incident Forensics and A10 Thunder ADC. Using SSL Insight, organizations can:

- Maximize performance, availability and scalability using A10's 64-bit Advanced Core Operating System, ACOS, and specialized security processors.
- Integrate with best-of-breed content inspection solutions like QRadar Incidents Forensics for event analysis.
- Analyze all network data, including encrypted data, as part of forensics investigations.

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

- Eliminate blind spots in corporate defenses. A10 Thunder ADCs provide a wide range of options in CPU performance and hardware acceleration so that customers can choose the right model for their environment.
- Future-proof their investment as SSL usage expands and organizations transition to 2048- and 4096-bit SSL keys.
- Decrypt traffic and send it to multiple inspection devices, using Thunder ADC as a centralized point for decryption and security.

About IBM Security

The IBM QRadar Security Intelligence Platform helps organizations holistically protect their people, data, applications and infrastructure. IBM's broader security portfolio offers solutions for identity and access management, security information and event management, database security, application development, risk management, endpoint management, next-generation intrusion protection and more. IBM operates one of the world's broadest security research and development, and delivery organizations. IBM monitors 15 billion security events per day in more than 130 countries and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

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**

[3] NSS Labs, "SSL Performance Problems"

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-19116-EN-02
Sep 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.