SSL INSIGHT FOR FIREEYE

Encryption Reduces Visibility and Security

Challenge:

To stop cyber threats like malware and targeted attacks, organizations need to inspect all types of traffic, including encrypted SSL communications. With the transition from 1024- to 2048-bit SSL keys and growing SSL usage, organizations need a powerful, high performance platform that can decrypt and inspect encrypted data.

Solution:

A10 Networks has partnered with FireEye to deliver a solution that intercepts SSL traffic and performs advanced threat analysis. SSL Insight, a feature of A10 Thunder ADC, offloads CPU-intensive decryption functions, enabling the FireEye Threat Prevention Platform to inspect encrypted traffic.

Benefits:

- Eliminate the blind spot in corporate defenses by decrypting SSL traffic at high speeds
- Prevent costly data breaches and loss of intellectual property by detecting advanced threats
- Maximize uptime by load balancing multiple FireEye Threat Prevention appliances
- Scale performance and throughput to successfully counter cyber attacks

Attackers have set their sights on vulnerable end users, leveraging malware to compromise client computers. Once infected, client computers become unwitting members of botnets, relaying information to command and control servers and exposing not only one machine, but potentially an entire network to reconnaissance and infiltration.

At the same time, more and more applications are encrypting data to prevent third parties from accessing sensitive information. Technologies such as Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are being used to secure web and email traffic. SSL usage has become ubiquitous; not long ago, popular websites only encrypted sensitive transactions such as credit card transactions or user logins, while today, many web applications encrypt every web request and response with SSL. In fact, 48% more of the million most popular websites were using SSL in January 2014 than a year earlier.[1]

Increasing SSL usage poses a problem when organizations wish to inspect traffic for malicious content such as malware, viruses or targeted phishing attacks. Many products that secure web, email and file transactions cannot inspect encrypted traffic or cannot keep pace with growing SSL encryption demands, resulting in blind spots in corporate defenses.

The A10 Thunder™ Application Delivery Controller (ADC) simultaneously provides load balancing capabilities to scale out and ensure resiliency of FireEye® infrastructure while also delivering visibility into encrypted traffic, enabling security devices such as FireEye NX Series, EX Series and FX Series platforms to inspect all traffic and to detect sophisticated cyber attacks.

SSL Insight and FireEye

SSL Insight™, also known as an SSL forward proxy, is a technology that consists of two SSL termination points that have separate SSL-secured sessions between the server and the client. Figure 1 on page 2 shows the SSL Insight feature. When configured for inline deployment:

- A Thunder ADC appliance deployed between clients and FireEye appliances intercepts outgoing SSL traffic and sends the traffic unencrypted to the FireEye appliances.
- The FireEye appliances inspect traffic for advanced threats and forward legitimate traffic on.
- A second Thunder ADC appliance, deployed between the FireEye appliances and the Internet, receives traffic from the FireEye appliances, encrypts the data and sends it to an external server.

From both the client's and the server's point of view, there still is an end-to-end encrypted session that is only decrypted within the client's network, in a contained environment. Customers can have peace of mind knowing that security blind spots created by SSL are eliminated. Now all inbound and outbound network traffic can be properly inspected and threats can be mitigated.

With its inbuilt load-balancing capabilities, Thunder ADC also provides high availability and scale, enabling organizations to deploy multiple FireEye platforms and, in the event of a software, hardware or network failure, to route around failed devices. For full redundancy, customers can install multiple Thunder ADC appliances between clients and FireEye platforms, and between FireEye platforms and external servers.

[1] Netcraft, January 2014 Web Server Survey

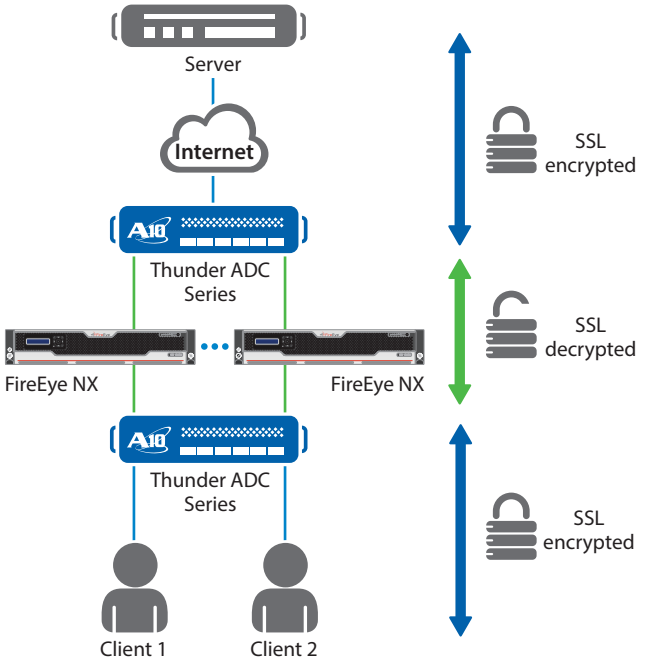

Figure 1: Thunder ADC decrypts SSL traffic and load balances multiple FireEye NX Series platforms

Alternatively, if hardware consolidation is desired, Thunder ADC's powerful Application Delivery Partitions (ADPs) allow organizations to configure multiple layer 3 virtual (L3V) partitions on a single appliance. Thunder ADC partitions can be hosted on a single hardware platform, allowing one Thunder ADC device to both decrypt and then re-encrypt the traffic. By leveraging ADPs, organizations can reduce hardware and operating expenses.

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.

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 setup of a secure connection is the most CPU demanding part of establishing an SSL connection. Encrypting and decrypting the bulk data of a session is still CPU-intensive but to a lesser degree. Managing many secure connections simultaneously is a perfect task for A10's ADC models. A10 Networks – the first vendor to introduce SSL Insight in an ADC – provides exceptional SSL connection rates with the powerful, feature-rich Thunder ADC platforms. The A10 ADCs are powered by the 64-bit Advanced Core Operating System (ACOS®), which provides linear scalability and is designed to get the maximum performance levels from the application and traffic acceleration hardware. All models have powerful CPUs and can support SSL offloading, but select models are available with a wide range of high-performance, multi-chip SSL acceleration modules that are exceptionally well suited for managing many SSL sessions simultaneously.

When using conventional CPU resources for establishing SSL connections, the performance hit is significant when SSL key sizes increase. With the new SSL acceleration hardware, A10 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.

The wide range of A10 ACOS features allows Thunder ADC customers to control which secure sessions to intercept and which to leave encrypted.

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 and performance are included without licensing fees.

FireEye Threat Prevention Platforms

FireEye Threat Prevention Platforms include all FireEye appliance- and cloud-based products. These include network, email, content, mobile, forensics and endpoint solutions that address today's advanced cyber threats. The FireEye Threat Prevention Platforms also use the patented and proven Multi-Vector Virtual Execution™ (MVX) technology to enable real-time detection and prevention of advanced threats.

The MVX engine captures and confirms zero-day and targeted advanced persistent threat (APT) attacks by detonating suspicious web objects, email attachments, content files and mobile apps within instrumented virtual machine environments. The MVX engine is designed to provide scalable, accurate and timely protection across the primary threat vectors (web, email, file and mobile), and it also provides actionable threat intelligence to enable rapid event prioritization and incident response.

[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.

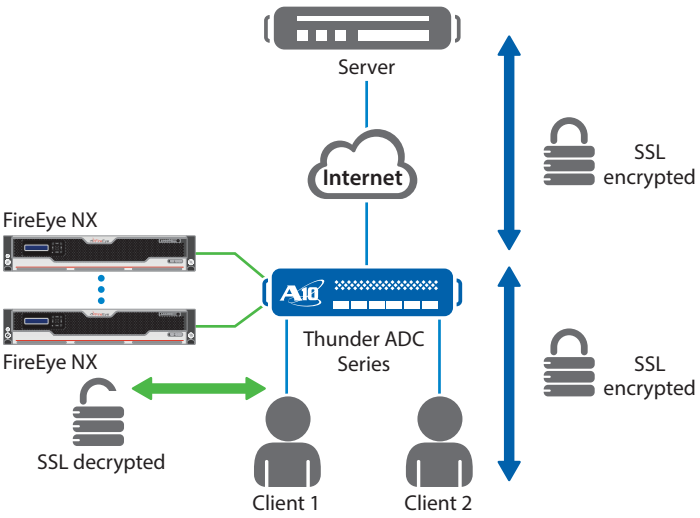

Figure 2: FireEye Threat Prevention Platforms in passive mode

FireEye platforms can also be deployed in passive mode, as shown in Figure 2. The decrypted traffic is duplicated towards the FireEye device, so it can inspect the traffic and even mitigate certain threats if desired. In passive mode, the FireEye unit can easily be integrated in a production network, without disruption. This is a non-impacting setup; the FireEye Threat Prevention Platform is not involved in the path of the network traffic flow, which makes it perfect for an evaluation phase.

Conclusion

A10 Thunder ADC with SSL Insight, combined with FireEye Threat Prevention Platform, is a superior solution for corporations that want to complete their online defense strategy. When a significant amount of traffic cannot be inspected, dangerous blind spots occur in corporate defenses. FireEye's Threat Prevention Platform has been successfully tested and proven to work in combination with A10's ADC models. Using SSL Insight, organizations can:

- Maximize performance, availability and scalability using A10's 64-bit Advanced Core Operating System, ACOS, and specialized security processors
- Analyze all network data, including encrypted data, for complete threat protection
- Deploy best-of-breed content inspection solutions to fend off cyber attacks

A10 offers extremely powerful SSL offloading solutions, enabling businesses to:

- Future-proof their investment against expanding SSL usage and higher encryption standards, including 2048 and 4096-bit SSL keys.
- Lower CAPEX by providing high-speed SSL decryption without requiring the purchase of additional security appliances. A10 Thunder ADC can decrypt traffic and send it to multiple inspection devices – FireEye Threat Prevention Platforms, as well as data leak prevention devices, network firewalls and URL content filtering products – providing a centralized point for decryption and security.
- 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. A10 Thunder ADC delivers critical services, maximizes rack space and reduces power consumption.

About FireEye Inc.

FireEye has invented a purpose-built, virtual machine-based security platform that provides real-time threat protection to enterprises and governments worldwide against the next generation of cyber attacks. These highly sophisticated cyber attacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, anti-virus, and gateways. The FireEye Threat Prevention Platform provides real-time, dynamic threat protection without the use of signatures to protect an organization across the primary threat vectors and across the different stages of an attack life cycle. The core of the FireEye platform is a virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyber attacks in real time. FireEye has over 2,200 customers across more than 60 countries, including over 130 of the Fortune 500.

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-19112-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.