SOLUTION BRIEF

SSL INSIGHT FOR FIREEYE

ENCRYPTION REDUCES VISIBILITY AND SECURITY

THE CHALLENGE

Attackers have set their sights on vulnerable enterprises, leveraging malware to compromise end-users. Once infected, these end-users become unwitting members of botnets that relay information to command and control servers by exposing not only one machine, but potentially the entire network to reconnaissance, infiltration and data exfiltration.

At the same time, an increasing number of 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; but today, many web applications encrypt every web request and response with SSL.

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 keep pace with growing SSL encryption demands, resulting in blind spots in corporate defenses.

CHALLENGE

The rising volume of encrypted traffic on the Internet provides an opportunity for attackers to stealthily infiltrate networks, using encrypted attacks to install malware. Traditional security devices are not designed to decrypt/encrypt traffic at high speeds, resulting in performance degradation and other network issues.

SOLUTION

A10 Networks has partnered with FireEye to deliver a solution that intercepts and decrypts SSL traffic, enabling the FireEye Threat Prevention Platform to inspect encrypted traffic for hidden malware and perform advanced threat analysis.

BENEFITS

- Eliminates the blind spot and counters encrypted cyberattacks on corporate defenses.
- Prevents costly data breaches and loss of intellectual property by detecting advanced threats.
- Maximizes uptime and scale performance by load balancing multiple FireEye Threat Prevention appliances.

THE A10 THUNDER SSLI AND FIREEYE THREAT PREVENTION SOLUTION

A10 Thunder® SSL Insight® (SSLi®) provides high-speed SSL decryption to eliminate the blind spot and ensure that the FireEye® infrastructure, including devices such as FireEye NX Series, EX Series and FX Series, can look at encrypted and unencrypted threats alike, defending against sophisticated cyberattacks. Thunder SSLi can decrypt traffic for multiple FireEye devices at the same time using the intrinsic load-balancing capabilities, ensuring that the security infrastructure is used in an efficient way.

SSL Insight consists of two SSL termination points that have separate SSL-secured sessions between the client and the server. Figure 1 shows how SSL Insight deploys and integrates with FireEye NX. When configured for inline deployment:

- A Thunder SSLi appliance is deployed on the enterprise perimeter between client machines and FireEye appliances. The Thunder SSLi intercepts outgoing SSL traffic, decrypts it and sends the unencrypted traffic to the FireEye appliances.
- The FireEye appliances inspect traffic for advanced threats and forward the legitimate traffic on.
- The Thunder SSLi appliance receives the inspected traffic back from the FireEye appliances, re-encrypts the data and sends it to the internet via the gateway.

From both the client's and the server's points 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 in 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.

Following the "***decrypt once, inspect many times***" approach, Thunder SSLi can decrypt traffic for multiple devices simultaneously, enabling organizations to deploy multiple FireEye platforms and distribute traffic between them using Firewall load balancing (FWLB). Customers can also deploy the FireEye platforms in an active-standby configuration for high availability (HA) so that in the event of a software, hardware or network failure, traffic can be routed around the failed devices. For full redundancy, customers can install multiple Thunder SSLi appliances between clients and FireEye platforms and between FireEye platforms and external servers.

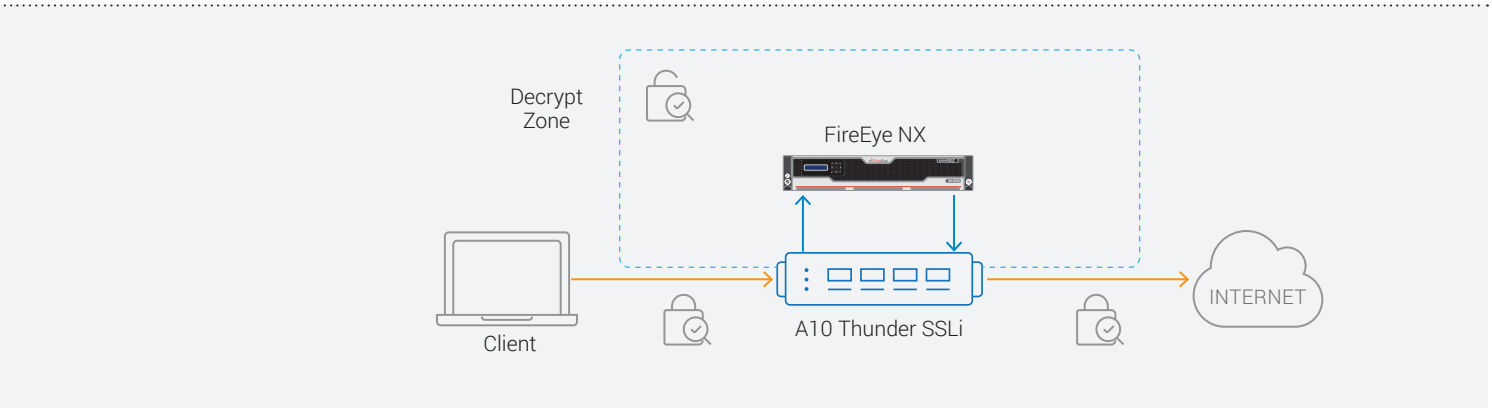

Figure 1: Thunder SSLi decrypts encrypted traffic and enables the FireEye NX appliance to defend against hidden threats

A10 THUNDER SSLI 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 Thunder SSLi models. The A10 Thunder SSLi appliances 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. Thunder SSLi provides visibility into encrypted traffic to stop potential threats by decrypting the traffic and allowing it to be inspected before it is re-encrypted and sent to its destination. This helps reveal malicious traffic that may be hidden in encrypted traffic. With dedicated SSL acceleration hardware, Thunder SSLi delivers high performance with 2048-bit and 4096-bit key sizes, while supporting multiple cipher suites, including DHE and ECDHE, for perfect forward secrecy (PFS) support.

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 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.

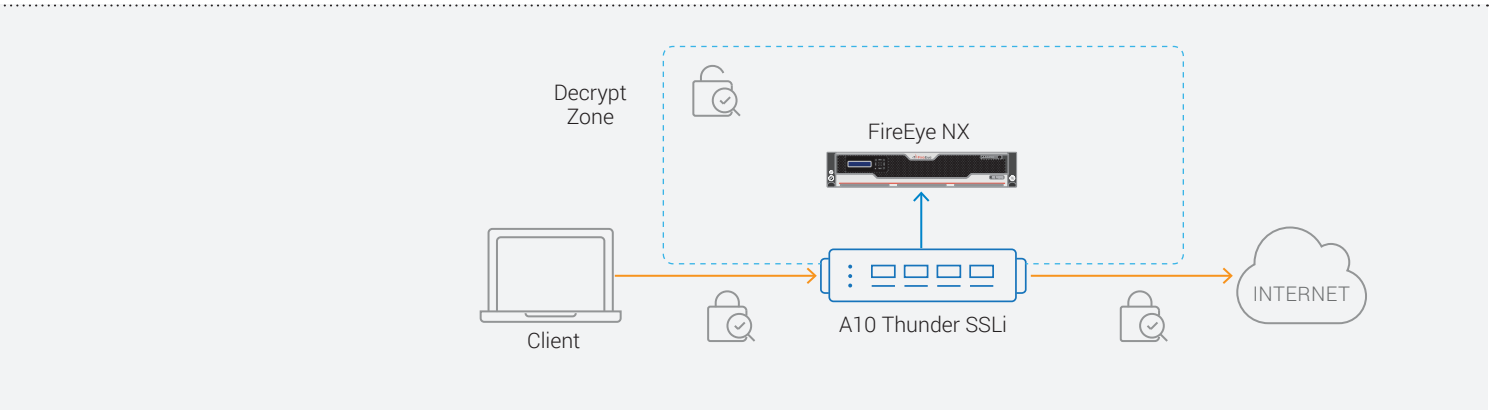

Figure 2: FireEye NX series deployed in passive mode

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.

SUMMARY

A10 Thunder SSLi combined with the FireEye Threat Prevention Platform is a superior solution for corporations that want to complete their online defense strategies. 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 Thunder SSLi models.

Using Thunder SSLi, 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.
- Enable the best-of-breed content inspection solutions to fend off encrypted cyberattacks.

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

- Future-proof their investments against expanding SSL usage and higher encryption standards, including 2048- and 4096-bit SSL keys.
- Decrypt SSL/TLS traffic on all ports and protocols with full control over the cipher suites used for encryption, including advanced DHE and ECDHE ciphers for perfect forward secrecy (PFS) support.
- Ensure that private keys are securely stored with up to four FIPS 140-2 Level 3 internal hardware security modules (HSM).
- Maximize employee productivity and reduce security risks by blocking access to known malicious websites with URL filtering.
- Adhere to compliance standards by selectively decrypting traffic based on categories using URL classification.
- Lower CAPEX and OPEX by providing high-speed SSL decryption without requiring the purchase of additional security appliances.
- Simultaneously decrypt traffic for, and load balance between, multiple devices deployed in the decrypt zone.

ABOUT FIREEYE, INC.

FireEye has a purpose-built security platform that provides real-time threat protection to enterprises and governments against the next generation of cyberattacks, such as advanced persistent threats and spear phishing. These highly sophisticated cyberattacks easily circumvent traditional signature-based defenses, such as next-generation firewalls, IPS, antivirus 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 multi-vector virtual execution engine, complemented by dynamic threat intelligence, to identify and block cyberattacks in real time. FireEye has over 5,800 customers across 67 countries, including more than 40 percent of the Forbes Global 2000.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

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

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19112-EN-03 FEB 2018