SSL Insight

Uncover Hidden Threats in Encrypted Traffic

Challenge:

Malicious users leverage SSL encryption to conceal their exploits. Organizations need a powerful, high-performance platform to decrypt SSL traffic.

Solution:

A10 Networks enables organizations to analyze all data, including encrypted data, by intercepting SSL communications and sending it to third-party security devices such as firewalls, threat prevention platforms and forensic tools for inspection.

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 third-party security appliances
- Scale performance and throughput to successfully counter cyber attacks

SSL Encryption Challenges

To prevent attacks, intrusions and malware, enterprises need to inspect incoming and outgoing traffic for threats. Unfortunately, attackers are increasingly turning to encryption to evade detection. With more and more applications supporting SSL – in fact, is expected to account for 67% of Internet traffic by the end of 2016.[1] SSL encryption represents not just a chink in enterprises' proverbial armor, but an enormous crater that malicious actors can exploit.

SSL Use Exposes a Blind Spot in Corporate Defenses

Organizations rely on a dizzying array of security products to inspect traffic, block intrusions, stop malware and control which applications users can access. To keep users safe inside the organization, these products must inspect all communications, not just clear-text traffic. Unfortunately, many firewalls, intrusion prevention and threat prevention products can't keep pace with growing SSL encryption demands.

In its report, *SSL Performance Problems*, NSS Labs found that eight leading next-generation firewall vendors experienced significant performance degradation when decrypting 2048-bit encrypted traffic. This led NSS Labs to assert that it had "concerns for the viability of SSL inspection in enterprise networks without the use of dedicated SSL decryption devices."[2]

As organizations move key applications—like email, CRM, business intelligence, and file storage—to the cloud, they need to monitor and protect these applications just as they would internally-hosted applications. Many of these cloud-based applications use SSL, exposing gaping holes in organizations' defenses. For end-to-end security, organizations need to inspect outbound SSL traffic originating from internal users, as well as inbound SSL traffic originating from external users to corporate-owned application servers, in order to eliminate the blind spot in corporate defenses.

High-Speed SSL Decryption with SSL Insight

The A10 Networks Thunder® SSLi and CFW product line's SSL Insight® technology, which eliminates the blind spot imposed by SSL encryption, offloading CPU-intensive SSL decryption and encryption functions that enable security devices to inspect encrypted traffic – not just clear text. SSL Insight 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, SSL Insight re-encrypts it and forwards it to the intended destination.

[1] Sandvine Global Internet Phenomena Spotlight: Encrypted Internet Traffic report, May 2015.

[2] NSS Labs, "SSL Performance Problems," https://www.nsslabs.com/research-advisory/library/infrastructure-security/next-generation-firewall/ssl-performance-problems/.

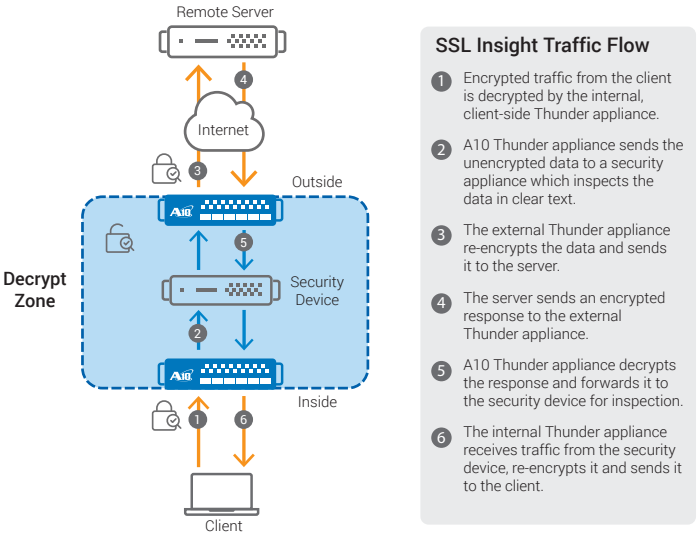

Figure 1: Logical view of traffic flow through the SSL Insight decrypt zone.

Full Visibility into SSL Traffic

While dedicated security devices provide in-depth inspection and analysis of network traffic, they are rarely designed to encrypt SSL traffic at high speeds. In fact, some security products cannot decrypt SSL traffic at all. SSL Insight, included standard with A10 Thunder CFW and SSLi appliances, offloads CPU-intensive encryption and decryption tasks from dedicated security devices, boosting application performance.

A10 Thunder appliances function as an SSL forward proxy or an explicit proxy to intercept SSL traffic. Organizations can simply deploy Thunder appliances with SSL Insight to safeguard their communications efficiently.

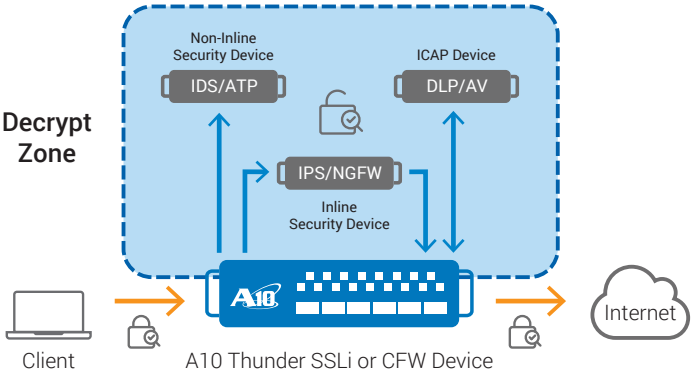

Figure 2: A10 Thunder SSLi or CFW devices can decrypt traffic for a variety of security products, including inline, non-inline (passive/TAP) and ICAP enabled devices.

In addition to inline deployment, organizations can deploy security devices, such as intrusion detection systems and forensics tools, in passive mode. SSL Insight decrypts SSL traffic and sends a copy of the unencrypted traffic to the non-inline security device for inspection. In passive mode, the security device can easily be integrated in a production environment without requiring network changes or introducing a single point of failure in the network. Non-inline deployment is ideal for security devices that inspect, alert and report on events rather than actively block attacks.

With SSL Insight, organizations can:

- **Achieve high performance with SSL acceleration hardware** – A10 Thunder appliances come equipped with powerful, dedicated SSL security processors that can scale to handle up to 174,000 2048-bit SSL handshakes per second. With SSL acceleration hardware, Thunder appliances deliver near parity performance between 1024-bit and 2048-bit key sizes and has the extreme power needed to handle 4096-bit keys at high-performance production levels.
- **Scale security with load balancing** – Besides offloading SSL decryption and encryption, Thunder appliances can load balance multiple firewalls or other security devices, dramatically increasing their performance, and can track each connection to ensure that requests and responses are directed to the same device that inspected the traffic.
- **Reduce load on security infrastructure by controlling which types of traffic to decrypt** – SSL Insight can selectively redirect traffic based on application type to security devices and security service chains with fine-grained policies for effective traffic management. For example, SSL Insight can decrypt and forward email traffic and web traffic to a threat prevention platform, but not burden the device with other types of traffic.
- **Granularly control traffic with aFleX policies** – Using A10 Networks aFleX® scripting, users can examine, update, modify or drop traffic. aFleX scripting enables organizations to fully control which traffic is intercepted and forwarded to a third-party security device and which traffic should be sanitized before being sent to the intended destination. aFleX offers complete control over application traffic, allowing customers to solve almost any type of application challenge. aFleX also enables users to handle data modified by third-party security devices and secure web gateways, instead of dropping connections.
- **Bypass sensitive applications and block known malicious websites** – To meet compliance requirements and ensure data privacy, SSL Insight can bypass trusted communications, such as traffic to banking and healthcare applications. With a URL classification subscription, SSL Insight can categorize traffic to over 460 million domains, ensuring confidential data remains encrypted. The optional URL classification subscription can also maximize employee productivity and reduce security risks by blocking access to malicious websites, including malware, spam, and phishing sites.

A Single Point for Decryption and Analysis

Organizations often deploy multiple security solutions to analyze and filter application traffic. SSL Insight offers a centralized point to decrypt SSL traffic and send it in clear text to a myriad of devices, eliminating the need to decrypt traffic multiple times. Thunder appliances can interoperate with:

- Firewalls
- Intrusion Prevention Systems (IPS)
- Unified Threat Management (UTM) platforms
- Data Loss Prevention (DLP) products
- Threat prevention platforms
- Network forensics and web monitoring tools

Many security devices are not designed for inline deployment or for high-speed SSL decryption. Thunder appliances enable these devices to inspect SSL-encrypted data without burdening the devices with computationally intensive SSL processing. SSL Insight can decrypt traffic once and forward traffic to a multitude of inline and non-inline security devices.

Detailed Feature List*

(* Features may vary by appliance.)

SSL Insight

- High-performance SSL decryption and encryption as a forward proxy
- Internet Content Adaption Protocol (ICAP) support for data loss prevention (DLP) and anti-virus solutions
- Dynamic port decryption to detect and intercept SSL or TLS traffic regardless of TCP port number
- Forward proxy failsafe to bypass traffic when there is a handshake failure
- SSL Insight bypass based on hostname; bypass list scales up to 1 million Server Name Indication (SNI) values
- Multi-bypass list support
- Extensive cipher and protocol support
  - SSL 3.0, TLS 1.0/1.1/1.2
  - RSA/DHE/ECDHE ciphers with Perfect Forward Secrecy (PFS) support
  - SHA, SHA-2, MD5 Message Authentication Code (MAC) algorithms
- Decryption of HTTPS, STARTTLS, SMTP, XMPP, POP3, SSH, SCP, sFTP
- Client certificate detection and optional bypass
- Untrusted certificate handling using the Online Certificate Status Protocol (OCSP)
- TLS alert logging to log flow information from SSL Insight events
- SSL session ID reuse
- aFleX scripting for deep packet inspection and customizable, application-aware switching
- High Availability – Active-Active, Active-Standby configurations
- Firewall Load Balancing (FWLB)
- Hardware Security Module (HSM) FIPS 140-2 Level 3**

URL Classification and Filtering***

- URL Classification Service powered by Webroot to monitor, block, or selectively bypass websites based on web-categories
- Optional monitoring and blocking of known malicious or undesirable websites using URL Filtering

Operation Modes

- Inline transparent proxy or explicit proxy deployment with passive, non-inline third-party devices
- Inline transparent proxy or explicit proxy deployment with active, inline third-party devices
- Inline transparent proxy or explicit proxy deployment with ICAP-connected devices
- Inline transparent proxy or explicit proxy deployment with third-party transparent and explicit proxy devices using proxy chaining

Management

- Dedicated management interface (Console, SSH, Telnet, HTTPS)
- Web-based Graphical User Interface (GUI) with Language Localization
- Industry-standard Command Line Interface (CLI) support
- Web-based AppCentric Templates (ACT) support****
- SNMP, Syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
- Port mirroring
- RESTful API (aXAPI)
- LDAP, TACACS+, RADIUS support

Carrier-grade Hardware

- Dedicated SSL security processors for high performance
- 40 GE ports
- Tamper Detection
- For non-inline deployments, traffic flows can be segmented by traffic type and broadcast through up to four network interfaces, enabling organizations to filter relevant traffic and to scale out security deployments
- For inline deployments, Thunder SSLi can offload SSL decryption functions and load balance multiple security devices

* Features may vary by appliance.
** Available on select models
*** URL Classification subscriptions are available as an additional paid service
**** Available as an early availability feature

Comprehensive and Scalable Management

To streamline and automate management, Thunder appliances include an industry standard CLI, a web user interface, and a RESTful API (aXAPI®) which can integrate with third party or custom management consoles. For larger deployments, A10 Networks aGalaxy® centralized management system ensures routine tasks can be performed at scale across multiple Thunder appliances, regardless of physical location.

Logging and Reporting

SSL Insight supports high-speed syslog logging as well as email alerts and NetFlow and sFlow statistics for traffic analysis. A real-time dashboard in the Thunder appliances web user interface displays system information, memory and CPU usage, and network status.

Summary

SSL Insight offers organizations a powerful load-balancing, high availability and SSL decryption solution. Using SSL Insight, organizations can:

- Analyze all network data, including encrypted data, for complete threat protection
- Deploy best-of-breed content inspection solutions to fend off cyber attacks
- Maximize the performance, availability and scalability of corporate networks by leveraging A10 Networks Advanced Core Operating System (ACOS®) platform, Flexible Traffic Acceleration (FTA) technology and specialized security processors

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

- Eliminate blind spots in corporate defenses using SSL Insight, with a wide range of deployment options delivering scalable performance and hardware acceleration so that customers can choose the right model for their environment
- 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
- Decrypt traffic and send it to multiple inspection devices, providing a centralized point for decryption and security

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-19113-EN-07
Nov 2016

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
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
southasia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at **a10networks.com/contact** or call to speak with an A10 sales representative.