Secure Web Gateway with SSL Insight

Safeguard Web Access and Eliminate SSL Blind Spots

Challenge:

Malicious users leverage SSL encryption to conceal their exploits. Organizations need a powerful, high-performance platform to decrypt SSL traffic, so access to malicious websites can be restricted.

Solution:

A10 Networks Secure Web Gateway with SSL Insight technology enables organizations to block access to undesirable sites and analyze encrypted data by intercepting and sending SSL communications to third-party security devices such as firewalls and threat prevention platforms for inspection.

Benefits:

- Eliminate the blind spot in corporate defenses by decrypting SSL traffic at high speeds
- Prevent malware infections and phishing attacks by blocking malicious websites
- Avoid costly data breaches and loss of intellectual property by detecting advanced threats
- Maximize uptime by load-balancing multiple third-party security appliances

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

The Challenge

The increasing use of SSL to avoid detection exposes a gap 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 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]

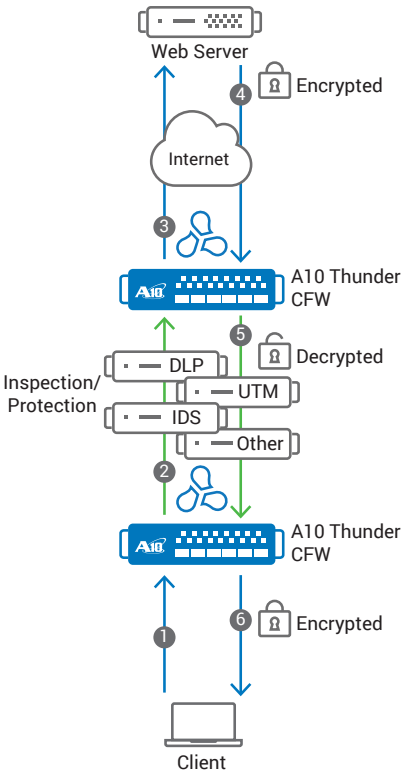
As organizations move key applications such as email, CRM, business intelligence and file storage to the cloud, they need to monitor and protect these applications just as they would internally hosted applications. Many of these cloud-based applications use SSL, exposing gaping holes in an organization's 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 spots in corporate defenses.

[1] Sandvine Global Internet Phenomena Spotlight: Encrypted Internet Traffic report, May 2015.
[2] NSS Labs, "SSL Performance Problems," https://www.nsslabs.com/reports/ssl-performance-problems.

The A10 Networks Secure Web Gateway with SSL Insight Solution

High-Speed SSL Decryption

The A10 Networks® Secure Web Gateway with SSL Insight® technology eliminates the blind spots imposed by SSL encryption, offloading CPU-intensive SSL decryption functions that enable security devices to inspect encrypted traffic – not just clear text. The Secure Web Gateway feature, which comes standard in A10 Networks Thunder® CFW product line, 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, the Secure Web Gateway re-encrypts it and forwards it to the intended destination.



SSL Insight Traffic Flow

1. Encrypted traffic from the client is decrypted by the internal, client-side Thunder CFW.
2. Thunder CFW sends the unencrypted data to a security appliance which inspects the data in clear text.
3. The external Thunder CFW re-encrypts the data and sends it to the server.
4. The server sends an encrypted response to the external Thunder CFW.
5. Thunder CFW decrypts the response and forwards it to the security device for inspection.
6. The internal Thunder CFW receives traffic from the security device, re-encrypts it and sends it to the client.

Figure 1: Thunder CFW helps protect internal users from web-based threats.

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. The Secure Web Gateway offloads CPU-intensive encryption and decryption tasks from dedicated security devices, boosting application performance.

The Secure Web Gateway functions as an SSL forward proxy or an explicit proxy to intercept SSL traffic. Organizations can simply deploy Thunder CFW appliances to safeguard their communications efficiently.

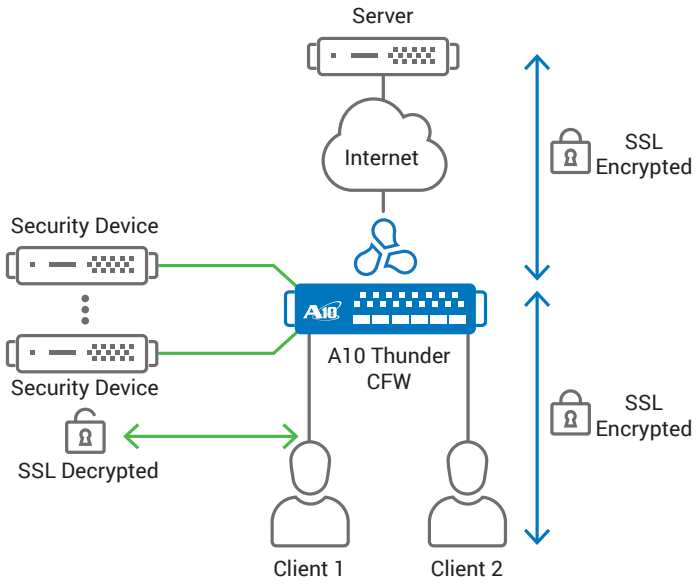


Figure 2: Thunder CFW can decrypt and forward traffic to security devices that are non-inline and passively deployed.

In addition to inline deployment, organizations can deploy security devices, such as intrusion detection systems and forensics tools, in passive mode. The Secure Web Gateway with 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 into 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.

A Single Point for Decryption and Analysis

Organizations often deploy multiple security solutions to analyze and filter application traffic. The Secure Web Gateway with 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. The Secure Web Gateway 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 CFW's Secure Web Gateway with SSL Insight enables these devices to inspect SSL-encrypted data without burdening the devices with computationally intensive SSL processing. Thunder CFW can decrypt traffic once and forward traffic to a multitude of inline and non-inline security devices.

Comprehensive and Scalable Management

To streamline and automate management, Thunder CFW includes an industry standard CLI, a web user interface and A10 Networks aXAPI® REST-based API, which can integrate with third-party or custom management consoles. For larger deployments, the A10 Networks aGalaxy® Centralized Management System ensures that routine tasks can be performed at scale across multiple Thunder CFW appliances, regardless of physical location.

Logging and Reporting

Thunder CFW 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 CFW web user interface displays system information, memory and CPU usage, as well as network status.

Features and Benefits

Benefits

With the Thunder CFW Secure Web Gateway, organizations can:

- **Achieve high performance with SSL acceleration hardware** – A10 Thunder CFW comes equipped with powerful, dedicated SSL security processors that can scale to handle hundreds of thousands of SSL handshakes per second. With SSL acceleration hardware, Thunder CFW delivers 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.
- **Block malicious websites and bypass sensitive applications** – 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, Thunder CFW can categorize traffic to over 460 million domains, ensuring that 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.[3]
- **Scale security with load balancing** – Besides offloading SSL encryption, Thunder CFW can load balance multiple firewalls or other security devices. A Thunder CFW high availability pair can load balance multiple security devices and can track each connection to ensure that requests and responses are directed to the same device.
- **Reduce the load on security infrastructure by controlling which types of traffic to decrypt** – Thunder CFW can selectively redirect traffic to security devices and security service chains with fine-grained policies based on application type. For example, Thunder CFW 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® TCL Scripting Technology, customers can examine, update, modify or drop requests. 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 TCL scripting offers complete control over application traffic, allowing customers to solve almost any type of application challenge.

Features[4]

Secure Web Gateway with SSL Insight:

- URL classification service powered by Webroot to monitor, block or selectively bypass specific websites; URL classification service requires a subscription license (see footnote 3)
- SSL Insight bypass based on hostname; bypass list scales up to 1 million Server Name Indication (SNI) values
- Multi-bypass list support
- Decryption of HTTPS, SMTP, XMPP
- Extensive cipher and protocol support (TLS 1.0, TLS 1.1, TLS 1.2, SSLv3); RSA, DHE, ECDHE ciphers with Perfect Forward Secrecy (PFS) support; SHA, SHA-2, MD5 hashing algorithms
- 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
- Forward proxy failsafe to bypass traffic when there is a handshake failure
- Dynamic port decryption to detect and intercept SSL or TLS traffic regardless of the protocol running on top of TCP
- SSL session ID reuse

Application Delivery:

- Advanced Layer 4/Layer 7 server load balancing
- aFleX TCL scripting for deep packet inspection and transformation for customizable, application-aware switching
- High availability for active/active and active/standby configurations
- Firewall Load Balancing (FWLB)

Deployment:

- 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

[3] URL Classification subscriptions are available in 4.0.1 to bypass sensitive websites. URL filtering is supported in A10 Networks Advance Core Operating System (ACOS® 4.1.0).
[4] Features vary by appliance model. See the Thunder CFW datasheet for a complete list of features and certifications.

Management:

- Dedicated management interface (console, SSH, telnet, HTTPS)
- Web-based graphical user interface (GUI) with language localization
- Industry-standard command-line interface (CLI) support
- SNMP, system logging, email alerts, NetFlow v9 and v10 (IPFIX), sFlow
- Port mirroring
- REST-style XML API (aXAPI)
- LDAP, TACACS+, RADIUS support

Carrier-Grade Hardware:

- Dedicated SSL security processors for high performance
- 40 GbE and 100 GbE 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, A10 Thunder CFW can offload SSL decryption functions and load balance multiple security devices
- Security and capability assurance

Certifications:

- Common Criteria EAL 2+
- FIPS 140-2 Level 2
- Joint Interoperability Test Command (JITC)

Solution Components

- Thunder CFW Secure Web Gateway with SSL Insight
- aGalaxy® Centralized Management System
- aFleX TCL Scripting Technology
- aXAPI® REST-based API

Summary – Safeguard Web Access and Eliminate SSL Blind Spots

Thunder CFW's Secure Web Gateway with SSL Insight offers organizations a powerful load-balancing, URL filtering and SSL decryption solution. Using SSL Insight, organizations can:

- Analyze all network data, including encrypted data, for complete threat protection
- Monitor and control web access based on over 83 URL classification categories
- Deploy best-of-breed content inspection solutions to fend off cyber attacks

Thunder CFW physical and virtual appliances enable businesses to:

- Maximize the performance, availability and scalability of their networks by leveraging A10's 64-bit ACOS platform, Flexible Traffic Acceleration (FTA) technology and specialized security processors
- Future-proof their investment against expanding SSL usage and higher encryption standards, including 2048- and 4096-bit SSL keys
- Decrypt traffic and send it to multiple inspection devices, providing a centralized point for decryption and security

Next Steps

For more information, please contact your A10 representative and visit: www.a10networks.com/news/security-solutions-with-new-A10-thunder-convergent-firewall

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-19154-EN-01
May 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 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.