Supported Platforms _____

Thunder SSLi
physical appliance

Overview _____

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.

THUNDER SSLi
High-Performance Visibility in Encrypted Traffic

The A10 Networks Thunder® SSLi® products feature A10's SSL Insight® technology, which eliminates the blind spot imposed by SSL encryption by offloading CPU-intensive SSL decryption functions from third-party security devices. Thunder SSLi decrypts SSL-encrypted traffic and forwards it to one or more third-party security devices such as a firewall, for deep packet inspection (DPI). Once the traffic has been analyzed and scrubbed, Thunder SSLi re-encrypts it and forwards to the intended destination.

Features and Benefits

Full Visibility into SSL Traffic

While dedicated security devices provide in-depth inspection and analysis of network traffic, they are rarely designed to decrypt and re-encrypt SSL traffic at high speeds. In fact, some security products cannot inspect SSL traffic at all. SSL Insight offloads CPU-intensive decryption and re-encryption tasks from dedicated security devices, boosting performance.

Thunder SSLi functions as a forward proxy for SSL traffic, or as an explicit proxy to intercept SSL traffic. Organizations can simply deploy Thunder SSLi appliances to safeguard their communications efficiently.

In addition to inline deployment, organizations can deploy security devices, such as intrusion detection systems and forensics tools, in passive mode. Thunder SSLi decrypts SSL traffic and sends a copy of the unencrypted traffic to the non-inline security device for inspection. Thunder SSLi devices can provide visibility to proxy servers and can also act as a proxy server. A single Thunder SSLi appliance can provide SSL visibility to the entire security stack.

With SSL Insight, organizations can:

- **Achieve high performance with SSL acceleration hardware** – A10 Thunder SSLi comes equipped with powerful, dedicated SSL security processors that can scale to meet high-volume traffic demands. With SSL acceleration hardware, Thunder SSLi 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. Multiple cipher suites are available including DHE and ECDHE for perfect forward secrecy (PFS) support.
- **Scale security with load balancing** – Besides offloading SSL encryption, Thunder SSLi can load balance multiple firewalls or other security devices. A Thunder SSLi 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.
- **Selectively manage traffic -** Using the ICAP protocol, Thunder SSLi can interact with third-party devices to decide if traffic should be subject to SSL Insight. In addition, the URL classification service can enforce privacy policies so data to medical or financial organizations is not inspected.

- **Reduce load on security infrastructure by controlling which types of traffic to decrypt** – Thunder SSLi can selectively redirect traffic based on application type to security devices and security service chains with fine-grained policies. For example, Thunder SSLi 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, Thunder SSLi 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 offers complete control over application traffic, allowing customers to solve almost any type of application challenge.

- **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 SSLi 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 SSLi can interoperate with:

- Firewalls
- Secure Web Gateways
- 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 SSLi enables these devices to inspect SSL-encrypted data without burdening the devices with computationally intensive SSL processing. Thunder SSLi 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 SSLi includes 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, the aGalaxy® centralized management system ensures routine tasks can be

performed at scale across multiple Thunder appliances, regardless of physical location.

Architecture and Key Components

SSL Insight Traffic Flow

1. Encrypted traffic from the client is decrypted by the internal, client-side Thunder SSLi.
2. Thunder SSLi sends the unencrypted data to a security appliance which inspects the data in clear text.
3. The external Thunder SSLi re-encrypts the data and sends it to the server.
4. The server sends an encrypted response to the external Thunder SSLi.
5. Thunder SSLi decrypts the response and forwards it to the security device for inspection.
6. The internal SSLi receives traffic from the security device, re-encrypts it and sends it to the client.
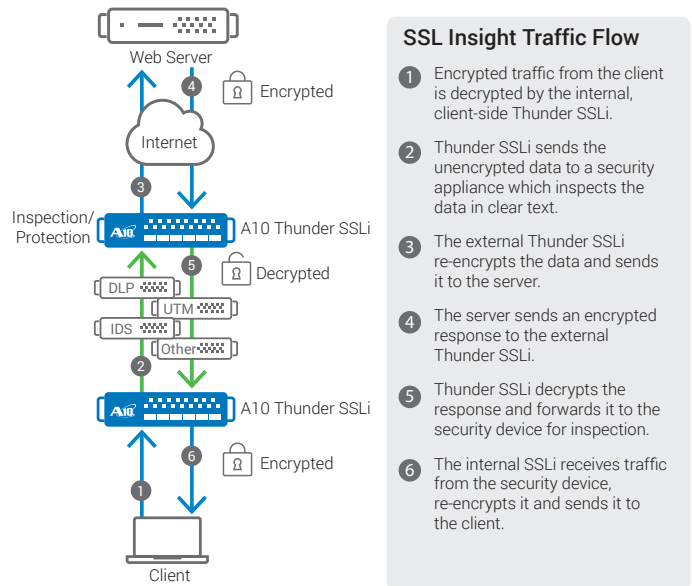
Figure 1: A10 Thunder SSLi helps protect internal users from web-based threats.
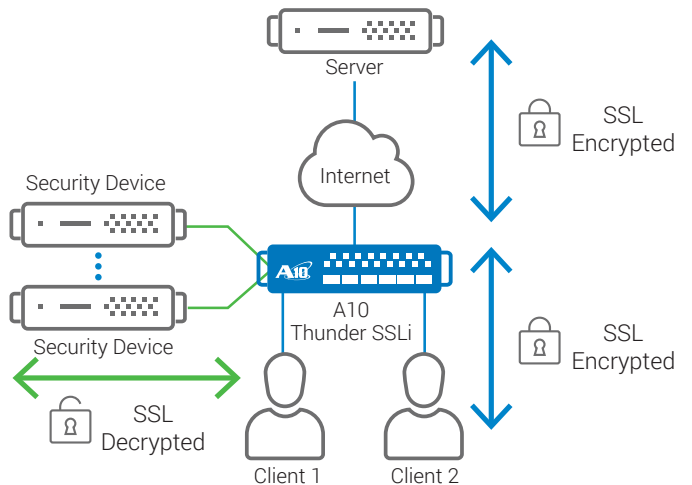

Figure 2: A10 Thunder SSLi can decrypt and forward traffic to security devices that are non-inline passively deployed.

Product Description

Thunder SSLi Product Line

Thunder SSLi appliances support any deployment need. Each Thunder SSLi appliance is powered by A10 Networks Advanced Core Operating System (ACOS®), which brings a unique combination of shared memory accuracy and efficiency, 64-bit scalability and advanced flow processing.

- Thunder SSLi Hardware Appliances:
  - The A10 Thunder SSLi line of appliances fits all size networks in a single, rack-mountable appliance to address the most demanding requirements.
  - All models are dual power supply-capable, feature solid-state drives (SSDs) and use no inaccessible moving parts for high availability.
  - All models benefit from A10's Flexible Traffic Accelerator (FTA) technology, with select models featuring Field Programmable Gate Arrays (FPGAs) for hardware optimized FTA processing; this provides highly scalable flow distribution and DDoS protection capabilities.
  - Select models include switching and routing processors for high-speed network processing, dedicated security processors for SSL offload, and lights-out management (LOM) for out-of-band monitoring and management.
  - Each appliance offers exceptional performance per rack unit to reduce power consumption costs and ensure a green solution. Coupled with high density 1 GbE, 10 GbE and 40 GbE port options, Thunder SSLi meets the highest networking bandwidth demands.

Thunder SSLi Hardware Appliance Specifications Table

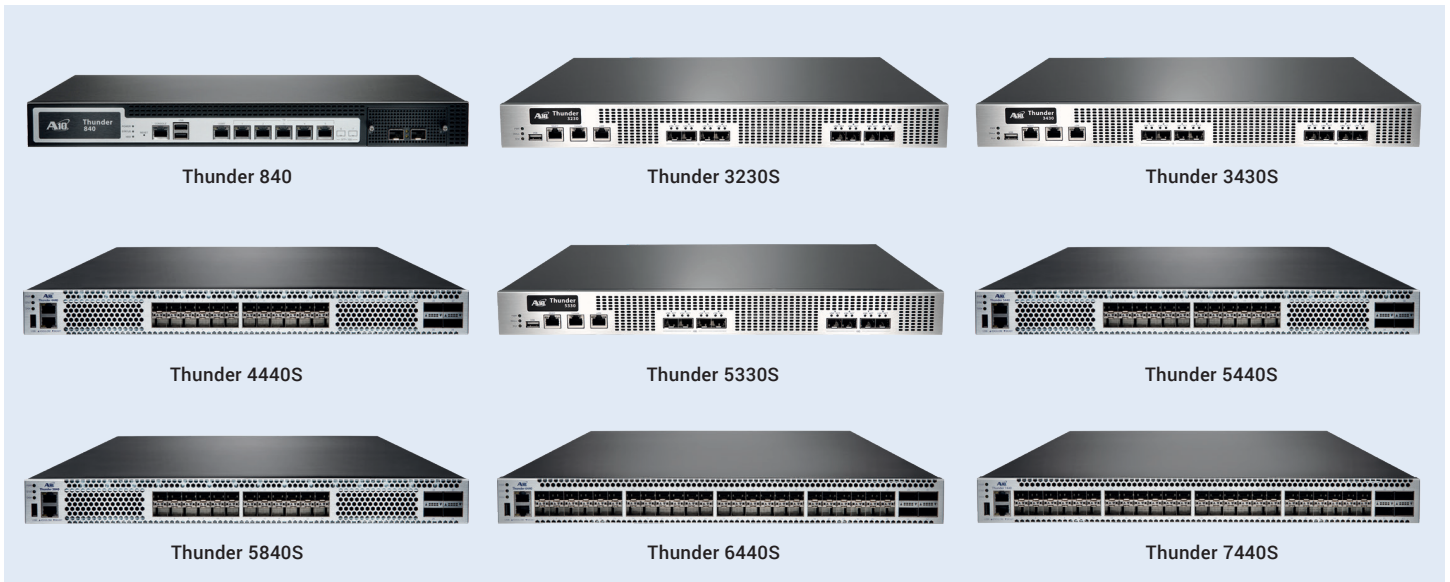|	Thunder 840	Thunder 3230S	Thunder 3430S
SSLi Throughput (2k key)[1][2]	0.5 Gbps	3.5 Gbps	5.5 Gbps
SSLi CPS (2k key)[1][2]	300	12.5k	18k
Network Interface			
1 GE Copper	5	0	0
1 GE Fiber (SFP)	0	4	4
1/10 GE Fiber (SFP+)	2	4	4
40 GE Fiber (QSFP+)	0	0	0
Management Interface	Yes	Yes	Yes
Lights Out Management	No	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Communication Processor	Intel Xeon 4-core	Intel Xeon 6-core
Memory (ECC RAM)	8 GB	16 GB	32 GB
Hardware Acceleration			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	Software	1 x FTA-4 FPGA	1 x FTA-4 FPGA
Switching/Routing	Software	Hybrid[4]	Hybrid[4]
SSL Security Processor	N/A	Dual	Dual or Quad
Power Consumption (Typical/Max)[3]	57W / 75W	210W / 265W	240W / 288W
Heat in BTU/hour (Typical/Max)[3]	195 / 256	717 / 904	819 / 983
Power Supply (DC option available)	Single 150W (AC only)	Dual 600W RPS	Dual 600W RPS
	100 - 240 VAC, 50-60 Hz	80 Plus Platinum efficiency, 100 - 240 VAC, Frequency 50 − 60 Hz	
Cooling Fan	Single Fixed Fan	Hot Swap Smart Fans	
Dimensions	1.75 in (H), 17.0 (W), 12 in (D)	1.75 in (H), 17.5 in (W), 17.15 in (D)	1.75 in (H), 17.5 in (W), 17.15 in (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	8.8 lbs	23 lbs	23 lbs
Operating Ranges	Temperature 0° - 40° C	Humidity 5% - 95%		
Regulatory Certifications	FCC Class A^, UL, CE^, TUV^, CB^, VCCI^, China CCC, BSMI^, RCM^	RoHS^	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, MSIP, BSMI, RCM, NEBS	RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, MSIP, BSMI, RCM, NEBS	RoHS, FIPS 140-2^[+]
Standard Warranty	90-day Hardware and Software		

[1] SSLi performance are measured in single appliance SSLi deployment. | [2] With maximum SSL | [3] With base model. Number varies by SSL model
[4] No dedicated hardware but FTA-4 FPGA handles select switching/routing functions | ^ Certification in process | + FIPS model must be purchased

Thunder SSLi Hardware Appliance Specifications Table (continued)

	Thunder 4440S	Thunder 5330S	Thunder 5440S
SSLi Throughput (2k key)*1 | *2	8 Gbps	8 Gbps	12.5 Gbps
SSLi CPS (2k key)*1 | *2	22k	24k	28k
Network Interface			
1 GE Copper	0	0	0
1 GE Fiber (SFP)	0	0	0
1/10 GE Fiber (SFP+)	24	8	24
40 GE Fiber (QSFP+)	4	0	4
Management Interface	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Xeon 6-core	Intel Xeon 10-core	Intel Xeon 12-core
Memory (ECC RAM)	32 GB	32 GB	64 GB
Hardware Acceleration			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	2 x FTA-4 FPGA	1 x FTA-4 FPGA	2 x FTA-4 FPGA
Switching/Routing	Hardware	Hybrid*4	Hardware
SSL Security Processor	Dual or Quad	Dual or Quad	Dual or Quad
Power Consumption (Typical/Max)*3	400W / 485W	240W / 288W	400W / 485W
Heat in BTU/hour (Typical/Max)*3	1,365 / 1,655	819 / 983	1,365 / 1,655
Power Supply (DC option available)	Dual 1100W RPS	Dual 600W RPS	Dual 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, Frequency 50 − 60 Hz		
Cooling Fan	Hot Swap Smart Fans		
Dimensions	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 17.15 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	32.5 lbs	23 lbs	32.5 lbs
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A^, UL^, CE^, TUV^, CB^, VCCI^, China CCC, BSMI^, RCM^ | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, China CCC, BSMI, RCM, NEBS | RoHS	FCC Class A^, UL^, CE^, TUV^, CB^, VCCI^, China CCC, BSMI^, RCM^ | RoHS, FIPS 140-2^|+
Standard Warranty	90-day Hardware and Software		

*1 SSLi performance are measured in single appliance SSLi deployment. | *2 With maximum SSL | *3 With base model. Number varies by SSL model
*4 No dedicated hardware but FTA-4 FPGA handles select switching/routing functions | ^ Certification in process | + FIPS model must be purchased

Thunder SSLi Hardware Appliance Specifications Table (continued)

	Thunder 5840S	Thunder 6440S	Thunder 7440S
SSLi Throughput (2k key)[1][2]*	17.5 Gbps	TBD	TBD
SSLi CPS (2k key)[1][2]*	50k	TBD	TBD
Network Interface			
1 GE Copper	0	0	0
1 GE Fiber (SFP)	0	0	0
1/10 GE Fiber (SFP+)	24	48	48
40 GE Fiber (QSFP+)	4	4	4
Management Interface	Yes	Yes	Yes
Lights Out Management	Yes	Yes	Yes
Console Port	Yes	Yes	Yes
Solid-state Drive (SSD)	Yes	Yes	Yes
Processor	Intel Xeon 18-core	Intel Xeon Dual 8-core	Intel Xeon Dual 18-core
Memory (ECC RAM)	64 GB	128 GB	128 GB
Hardware Acceleration			
64-bit Linear Decoupled Architecture	Yes	Yes	Yes
Flexible Traffic Acceleration	2x FTA-4 FPGA	3 x FTA-4 FPGA	3 x FTA-4 FPGA
Switching/Routing	Hardware	Hardware	Hardware
SSL Security Processor	Dual or Quad	2 x Dual	2 x Dual
Power Consumption (Typical/Max)[3]	415W / 510W	560W / 630W	770W / 900W
Heat in BTU/hour (Typical/Max)[3]	1,417 / 1,741	1,911 / 2,150	2,628 / 3,071
Power Supply (DC option available)	Dual 1100W RPS	Dual 1100W RPS	Dual 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, Frequency 50 − 60 Hz		
Cooling Fan	Hot Swap Smart Fans		
Dimensions	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)	1.75 in (H), 17.5 in (W), 30 in (D)
Rack Units (Mountable)	1U	1U	1U
Unit Weight	32.5 lbs	36 lbs	36 lbs
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A^, UL^, CE^, TUV^, CB^, VCCI^, China CCC, BSMI^, RCM^ | RoHS	FCC Class A^, UL^, CE^, TUV^, CB^, VCCI^, China CCC^, BSMI^, RCM^ | RoHS	FCC Class A^, UL^, CE^, TUV^, CB^, VCCI^, China CCC^, BSMI^, RCM^ | RoHS, FIPS 140-2^|+
Standard Warranty	90-day Hardware and Software		

*1 SSLi performance are measured in single appliance SSLi deployment. | *2 With maximum SSL | *3 With base model. Number varies by SSL model
*4 No dedicated hardware but FTA-4 FPGA handles select switching/routing functions | ^ Certification in process | + FIPS model must be purchased

Thunder 840	Thunder 3230S	Thunder 3430S
Thunder 4440S	Thunder 5330S	Thunder 5440S
Thunder 5840S	Thunder 6440S	Thunder 7440S

Detailed Feature List

SSL Insight

- High-performance SSL decryption and encryption as a forward proxy
- Internet Content Adaption Protocol (ICAP) support for data loss prevention
- 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
- Decryption of HTTPS, STARTTLS, SMTP, XMPP
- 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
- Firewall Load Balancing (FWLB)

URL Filtering

- URL Classification Service powered by Webroot to selectively bypass trusted websites for SSL decryption*
- Optional monitoring and blocking of malicious or undesirable websites

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

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, Syslog, 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 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.

*Additional paid service

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

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.