DATA SHEET

Thunder SSLi

TLS/SSL Decryption for Real-time Visibility into Encrypted Traffic

A comprehensive TLS/SSL decryption solution, A10 Thunder® SSL Insight® (SSLi®) decrypts traffic across all ports, enabling third-party security devices to analyze all enterprise traffic without compromising performance.

Eliminate the Blind Spot

Thunder SSLi eliminates the blind spot introduced by TLS/SSL encryption by offloading CPU-intensive decryption and encryption functions from third-party security devices, while ensuring compliance with privacy standards.

While dedicated security devices provide in-depth inspection and analysis of network traffic, they are not designed to decrypt and encrypt traffic at high speeds. In fact, many security products do not have the ability to decrypt traffic at all. Thus, Thunder SSLi helps augment the existing security devices, secure your investments for security infrastructure and further strength your Zero Trust strategy.

Thunder SSLi boosts the performance of the security infrastructure by decrypting traffic and forwarding it to one or more third-party security devices, such as a next-gen firewall, intrusion prevention system (IPS), advanced threat protection (ATP) or other solution. Thunder SSLi re-encrypts traffic and forwards it to the intended destination. Response traffic is also inspected in the same way.

A10 Control can streamline operations and management for Thunder SSLi across multiple sites. Equipped with comprehensive dashboards, A10 Control provides real-time actionable insigts into network traffic characteristics, and rich analytics based on service, application types, URL categories and so on, that enable the visibility and control needed to augment Zero Trust strategies.

Platforms

Physical Appliance

Virtual Appliance

Management

A10 Control
Centralized Analytics and Management

Learn More

A10Networks.com/ssli

Benefits

Decrypt Once

Inspect Multiple Times

Leverage A10's SSL Insight technology to decrypt SSL traffic and forward it to third-party security devices for inspection.

Maximize uptime and increase security infrastructure capacity with integrated load balancing and unburden firewalls and other security devices from computationally intensive SSL decryption, enabling them to detect and stop attacks.

Decrypt Traffic

for Any Security Devices

To truly secure an enterprise network, from both internal and external threats, organizations require the help of a variety of security devices.

Thunder SSLi works with the major security vendors, which may be deployed in a number of ways in the "secure decrypt zone," ensuring that the whole network is secure against encrypted threats. Thunder SSLi interoperates with:

- Firewalls
- Secure web gateways (SWG)
- Intrusion prevention systems (IPS)
- Unified threat management (UTM) platforms
- Data loss prevention (DLP) products
- Threat prevention platforms
- Network forensics and web monitoring tools

Reduce

Operational Costs

Thunder SSLi offers a centralized point to decrypt enterprise traffic, forwarding it to many inline and non-inline security devices. This eliminates the decryption overhead of each security device, improving performance while maintaining proper security diligence. It also eliminates the need to purchase bigger security devices just to support resource-exhausting decryption and encryption functions.

Gain Full Visibility

Into The Blind Spot

Thunder SSLi decrypts traffic across all ports and multiple protocols, eliminating the encryption blind spot and enabling the security infrastructure to inspect previously invisible traffic, detect hidden threats and defend against them.

Validate

Certificate Status

Attackers can use invalid certificates to infiltrate networks. If these attacks are not blocked, users can be at risk of multiple attacks.

Thunder SSLi helps the system confirm the validity of certificates it receives from the server by supporting certificate revocation lists (CRL) and Online Certificate Status Protocol (OCSP). These help verify the origin certificate is valid.

Ensure

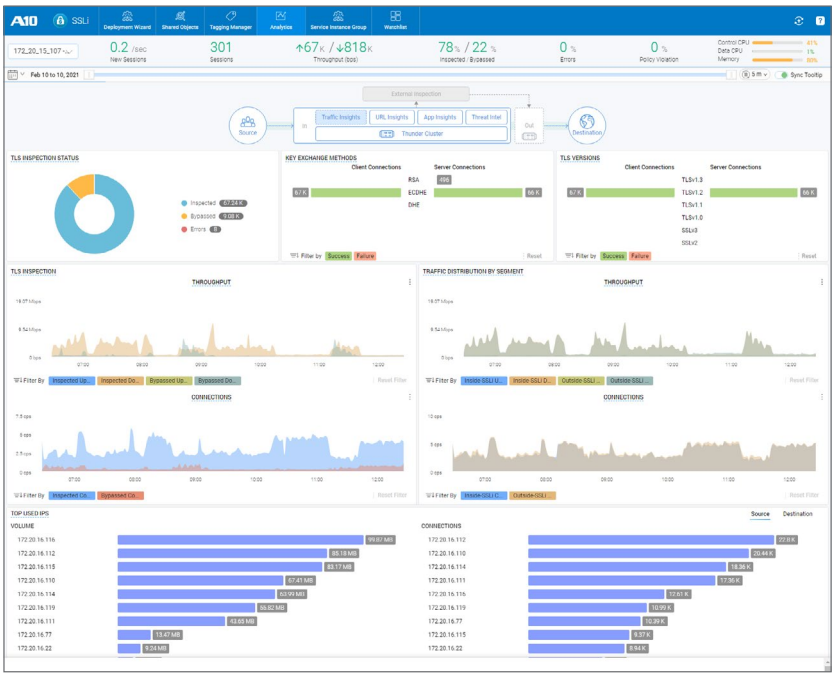
Compliance and Privacy

Thunder SSLi allows for selective decryption, making sure that organizations can keep up with industry, government and other compliance and privacy standards. For example, HIPAA compliance may forbid the decryption of private and sensitive healthcare information.

Centralized

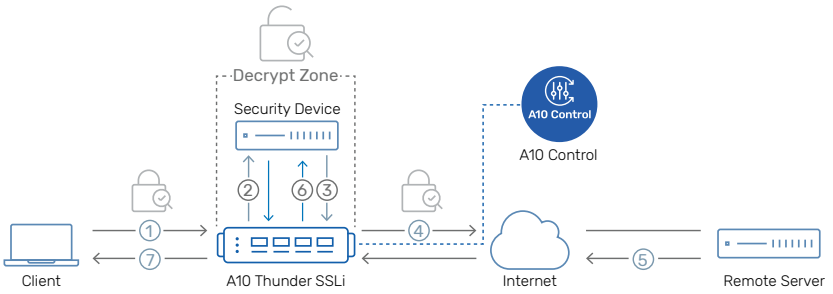
Analytics and Management

A10 Control provides centralized management and rich analytics for multiple Thunder devices from multiple branch offices into one centralized and condensed console. Distributed Thunder devices can be configured and managed through A10 Control from a central location. A10 Control can display either individual Thunder device statistics or aggregated into an intuitive dashboard for faster troubleshooting and rich analytics.



A10 Control SSLi app provides comprehensive analytics for complete visibility into all SSLi deployment, intuitive deployment wizard adn troubleshooting tools. The analytics dashboard can be populated for each SSLi instance individually or in aggregated fashion providing a holistic view into traffic patterns.

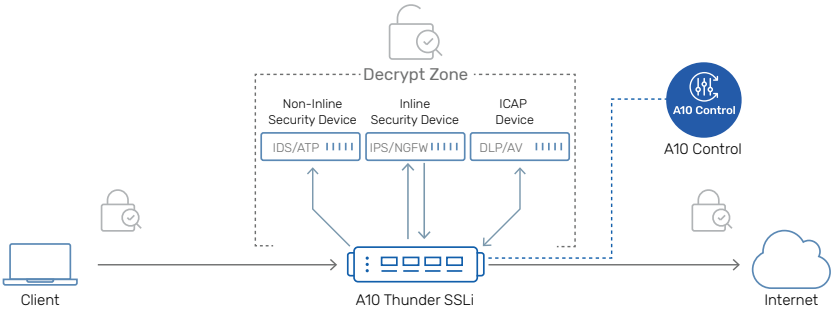
Reference Architectures



1. Encrypted traffic from the client is intercepted by Thunder SSLi and decrypted.
2. Thunder SSLi sends the decrypted traffic to a security device, which inspects it in clear-text.
3. The security device, after inspection, sends the traffic back to Thunder SSLi, which intercepts and re-encrypts it.
4. Thunder SSLi sends the re-encrypted traffic to the server.
5. The server processes the request and sends an encrypted response to Thunder SSLi.
6. Thunder SSLi decrypts the response traffic and forwards it to the same security device for inspection.
7. Thunder SSLi receives the traffic from the security device, re-encrypts it and sends it to the client.

Traffic Flow Through the Decrypt Zone

Thunder SSLi provides visibility via a logical decrypt zone where third-party security devices inspect traffic for threats. Thunder SSLi can be deployed in a one- or two-appliance configuration.



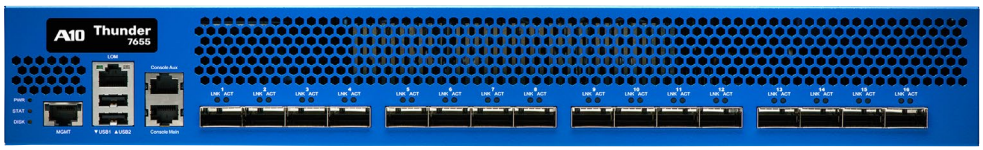
Multiple Deployment and Decryption Options

Thunder SSLi may be deployed inline, on the enterprise perimeter, and can decrypt traffic for a variety of security products simultaneously, including inline, non-inline (passive/TAP) and ICAP-enabled devices.

Thunder 7655S SSLi

by the Numbers

72 Gbps SSLi Throughput	145 Gbps SSL Bulk Throughput	4M SSLi Concurrent Sessions	100 GbE Ports



RSA: 100K
ECDHE: 70K
SSLi CPS

Decrypted Traffic Solutions for any Security Device

Firewalls

- Cisco FirePOWER
- Palo Alto Networks next-generation firewalls
- Check Point next-generation firewalls

Secure Web Gateways

- Symantec Edge SWG
- Forcepoint Trusted Gateway System

Advanced Threat Protection

- FireEye Network Security
- Fidelis Network

Forensics and Security Systems

- RSA NetWitness
- IBM Security QRadar

Intrusion Prevention Systems

- Trellix IPS (McAfee NSP)
- Secureworks iSensor

Others

- OPSWAT MetaDefender
- Trend Micro Deep Security
- Vectra NDR
- Garland Technology NPB
- Niagara Networks NPB/Bypass Switch

Features

Decrypt

Across Multiple Ports and Protocols

Using dynamic port inspection, Thunder SSLi decrypts regular TLS traffic on any TCP ports.

Decryption for other secure service protocols like STARTTLS, XMPP, SMTP and POP3 are supported. However, the decryption functionalities are not limited to SSL/TLS, encrypted traffic and decryption for SSH traffic is supported as well.

Full-proxy

Architecture

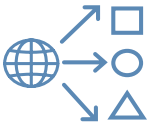
Thunder SSLi operates as a full-proxy, which enables adjusting of cipher suite selection for encryption. Thunder SSLi can re-negotiate to a different cipher suite of similar strength, making the solution future-proof against new ciphers or TLS versions that might be introduced to the network without notice. Thunder SSLi can ensure traffic is encrypted using the most secure ciphers, eliminating the use of compromised ciphers.

Multiple Ciphers
for PFS Support

With dedicated SSL acceleration hardware, Thunder SSLi delivers high performance with 2048-bit and 4096-bit key sizes, while supporting advanced cipher suites, including DHE DHE, ECDHE, ECDSA, ChaCha-Poly and more, for perfect forward secrecy (PFS) support.

Explicit Proxy
Deployment Support

In addition to the standard transparent proxy deployment, Thunder SSLi can also be deployed as an explicit proxy, giving more control over traffic management. Thunder SSLi can connect to multiple upstream proxy servers using proxy chaining.



URL Classification
for Selective Decryption

Thunder SSLi URL classification categorizes the traffic of more than one billion domains, selectively bypassing traffic decryption to enforce privacy policies so private/sensitive data (e.g., medical or financial records) is not decrypted, in adherence to compliance standards like HIPAA.

Application Traffic
Recognition and Control

Identify and categorize traffic on the application level, allowing for more granular controls and policies to be defined, with application visibility and control. Along with comprehensive user and group awareness, this provids deep insights into application traffic for effective security planning and sanctioning of allowed business applications.

URL Filtering
for Access Control

URL filtering is used to maximize employee productivity and reduce risks by blocking access to malicious websites, including malware, spam and phishing sources.

ICAP
Support

Data loss prevention (DLP) systems typically use ICAP to connect to the network and help prevent unauthorized data exfiltration. Thunder SSLi supports ICAP connectivity simultaneously with other decryption modes. This enables a network's existing DLP systems without the purchase of extra solutions.

Load Balance
Security Devices

With load-balancing support, Thunder SSLi dramatically increases performance of firewalls and other security devices. Easily add security capacity and extend the life of existing security devices. Flexible weighted traffic priorities can be assigned.

Granular
Traffic Control

Examine, update, modify or drop requests DPI using A10 aFleX® scripting. 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.

Intelligent Service Chaining

for High-performance Security

Selectively redirect traffic, based on application type, to different service chains with fine-grained policies. Thunder SSLi reduces latency and potential bottlenecks with the **decrypt once, inspect many times** approach, consolidating decryption and encryption duties.

User Authentication and User-based Policies

Create security policies for users, making sure no unauthorized access is allowed, with the identity and access management feature. This also enables you to define user-ID-based traffic and inspection policies to maintain granular control.

Threat Intelligence

IP threat intelligence feeds help identify and block traffic going out to and coming in from known bad IP addresses, even before going into decryption process.

With the Threat Investigator, explore and confirm the trustworthiness of websites, based on threat reputation and confidence scores. This can be accessed via A10 Control.

Centralized Analytics and Management

A10 Control provides performance monitoring and faster troubleshooting with device health status, logs and traffic pattern analysis.

Deep insights into anomalies and threats enable enterprises to set adaptive controls and policy updates through behavior analysis.

Thunder SSLi Physical Appliance Specifications

Performance	Thunder 1060S-10G SSLi	Thunder 1060S SSLi	Thunder 3350S SSLi
SSLi Throughput	1 Gbps	2 Gbps	5.5 Gbps
SSLi CPS	RSA: 2K ECDHE: 1.2K	RSA: 6K ECDHE: 4K	RSA: 20K ECDHE: 10K
SSLi Concurrent Sessions	50K	100K	300K
SSL Bulk Throughput*5	10 Gbps	15 Gbps	30 Gbps
Network Interface			
1 GE (BASE-T)	7	7	6
1 GE Fiber (SFP)	0	0	2
10/1 GE Fiber (SFP+/SFP)	4	4	8 + 4*4
25/10 GE Fiber (SFP28/SFP+)	2	2	0
40 GE Fiber (QSFP+)	0	0	0
100/40 GE Fiber (QSFP28/QSFP+)	0	0	0
Management Ports	Ethernet mgmt port, RJ-45 console port		
Hardware Specifications			
Processor	Intel communications processor 20-core [9-core active]	Intel communications processor 20-core	Intel Xeon 14-core
Memory (ECC RAM)	32 GB [24 GB active]	32 GB	64 GB
Storage	SSD		SSD
Hardware Acceleration	Software		Software
TLS/SSL Security Acceleration	Hardware		Hardware
Dimensions (inches)	1.75 (H) x 17.5 (W) x 17(D)		1.75 (H) x 17.5 (W) x 18(D)
Rack Units (mountable)	1U		1U
Unit Weight	12 lbs		18 lbs
Power Supply (DC option available)	Dual 300W RPS		Dual 750W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz		
Power Consumption (typical/max)*2	112W / 127W		175W / 222W
Heat in BTU/hour (typical/max)*2	383 / 434		598 / 758
Cooling Fan (front-to-back airflow)	Removable fans		Hot swap smart fans
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%		
Regulatory Certifications	FCC Class A, UL, ICES, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS		FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI, RCM | RoHS, FIPS 140-2*
Standard Warranty	90-day hardware and software		

Thunder SSLi Physical Appliance Specifications (cont.)

Performance	Thunder 6655S SSLi	Thunder 7655S SSLi
SSLi Throughput	36 Gbps	72 Gbps
SSLi CPS	RSA: 50K ECDHE: 35K	RSA: 100K ECDHE: 70K
SSLi Concurrent Sessions	2 Million	4 Million
SSL Bulk Throughput*5	72.5 Gbps	145 Gbps
Network Interface		
1 GE (BASE-T)	0	0
1 GE Fiber (SFP)	0	0
10/1 GE Fiber (SFP+/SFP)	0	0
25/10 GE Fiber (SFP28/SFP+)	0	0
40 GE Fiber (QSFP+)	0	0
100/40 GE Fiber (QSFP28/QSFP+)	16	16
Management Ports	Ethernet mgmt. port, RJ-45 console port, Lights out management	
Hardware Specifications		
Processor	Intel Xeon 28-core	2 x Intel Xeon 28-core
Memory (ECC RAM)	192 GB	384 GB
Storage	SSD	SSD
Hardware Acceleration	FTA-5, SPE	2 x FTA-5, SPE
TLS/SSL Security Acceleration	Hardware	Hardware
Dimensions (inches)	2.625 (H) x 17.5 (W) x 30 (D)	2.625 (H) x 17.5 (W) x 30 (D)
Rack Units (mountable)	1.5U	1.5U
Unit Weight	39 lbs	44.2 lbs
Power Supply (DC option available)	Dual 1500W RPS	
	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz	
Power Consumption (typical/max)*2	667W / 856W	1,121W / 1,300W
Heat in BTU/hour (typical/max)*2	2,276 /2,921	3,826 / 4,436
Cooling Fan (front-to-back airflow)	Hot swap smart fans	
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%	
Regulatory Certifications	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS, FIPS 140-2+	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM | RoHS, FIPS 140-2+
Standard Warranty	90-day hardware and software	

Thunder SSLi has been completely merged to into the A10 Thunder CFW product line. Please refer to the Thunder CFW data sheet for more SSL Insight solution products.

Hardware specifications and performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions. As for network interface, it's highly recommended to use A10 Networks qualified optics/transceivers to ensure network reliability and stability.

All SSLi products are also available in CFW license. For SWG use cases (e.g., application-aware firewall and IP threat intelligence), CFW product line is required.

*1 Tested in single appliance SSLi deployment with maximum SSL option. Cipher "TLS_RSA_WITH_AES_128_CBC_SHA256" with RSA 2K keys are used for RSA cases, "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256" with EC P-256 and RSA 2K keys are used for ECDHE case.
*2 With base model. Number varies by SSL model | *3 Optional RPS available | *4 10Gbps speed only | *5 Total SSL (transaction) capacity with maximum SSL option | ^ Certification in process | + FIPS model must be purchased

Thunder SSLi Virtual Appliance Specifications

vThunder SSLi	
Supported Hypervisors	VMware ESXi (VMXNET3, SR-IOV, PCI Passthrough), KVM QEMU (SR-IOV, PCI Passthrough)
Hardware Requirements	See installation guide
License*	• BYOL bandwidth license • FlexPool license
Standard Warranty	90-day software

* Bandwidth license needs to be applied based on the total traffic passing through the SSLi appliance. For example, single appliance SSLi deployment transacts traffic twice (for decryption and the re-encryption), therefore the actual bandwidth would be double of the SSLi throughput or more.twice (for decryption and then re-encryption) in one transaction.

Detailed Feature List

Features may vary by appliance.

Detection/Analysis

- High-performance SSL decryption and encryption as a forward proxy
- Full-proxy architecture
- Internet Content Adaption Protocol (ICAP) support with pre-filtering for data loss prevention (DLP) and antivirus solutions
- Dynamic port decryption to detect and intercept SSL or TLS traffic regardless of TCP port number
- Bi-directional inspection for protection against incoming web threats
- Forward proxy failsafe to bypass traffic when there is a handshake failure
- Decryption 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 1.0/1.1/1.2/1.3*3
  - RSA/DHE/ECDHE/ECDSA/ChaCha-Poly ciphers with Perfect Forward Secrecy (PFS) support
  - SHA, SHA-2, MD5 Message Authentication Code (MAC) algorithms
  - IPv4 and IPv6
  - HTTP 1.1, HTTP/2
- Decryption of HTTPS, STARTTLS, SMTP, XMPP, POP3, SSH, SCP, sFTP
- Client certificate detection and optional bypass
- Untrusted/expired certificate handling using:
  - Online certificate status protocol (OCSP)
  - Certificate revocation lists (CRL)
- Detailed user and session logging
- User authentication and authorization service for identity based access control
- SaaS local breakout and access control
- Next hop load distribution (NHLD) for internet traffic load distribution and optimization
- TLS alert logging to log flow information from SSLi events
- SSL session ID reuse
- aFleX scripting for customizable, application-aware switching
- High availability: active-active, active-standby configurations
- Firewall load-balancing (FWLB)

URL Classification*2

- URL bypassing for web category-based selective decryption
- URL filtering for blocking of known malicious or undesirable websites

Threat Intelligence*2

- IP threat intelligence service*1 prevents malicious traffic from entering your network, based on customizable risk score and tolerance
- Threat investigator provides rich and contextual analytics for object such as URL, IP, app etc.

Application-aware Firewall*1|*2

- Recognition of thousands protocol signatures with identification of service types within applications
- Support custom rules that run real-time

Deployment

- Inline transparent proxy or explicit proxy deployment with non-inline third-party devices
- Inline transparent proxy or explicit proxy deployment with 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

Virtualization

- vThunder virtual appliance for VMware vSphere ESXi, Microsoft Hyper-V and KVM
- A10 Thunder on Dell Technologies OEM solution bundle

Management

- Dedicated on-box management interface (GUI, CLI, SSH, Telnet)
- SNMP, syslog, email alerts
- RESTful API (aXAPI)
- LDAP, TACACS+, RADIUS support
- Configurable control CPUs
- Interoperable with A10 Control for centralized management, configuration and analytics

Centralized Management and Analytics with A10 Control

- Device and configuration management across multiple sites
- Deployment wizard with guided configuration
- Centralized security policy management and enforcement
- Rich TLS/SSL traffic and decryption analytics for traffic insight, application insight, URL insight, source and destination insight and more
- Threat investigator view
- Session log drill-down
- Troubleshooting tools

* Features may vary by appliance.
*1 Available on CFW platform/license.
*2 Software and service subscriptions are required.
*3 Available on Thunder 1060S, 3350S, 6655S and 7655S.

About A10

A10Networks.com

Contact Us

A10Networks.com/contact

Part Number: A10-DS-15113-EN-30 November 2025