DATA SHEET

THUNDER SSLi

REAL-TIME VISIBILITY INTO ENCRYPTED TRAFFIC

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

PLATFORM

THUNDER SSLi
Physical Appliance

ELIMINATE THE BLIND SPOT

Thunder SSLi eliminates the blind spot introduced by SSL encryption by offloading CPU-intensive SSL 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.

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 firewall for deep packet inspection (DPI).

Thunder SSLi re-encrypts traffic and forwards it to the intended destination. Response traffic is also inspected in the same way.

TALK WITH A10

WEB
a10networks.com/SSLi

CONTACT US
a10networks.com/contact

BENEFITS

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.

DECRYPT TRAFFIC
FOR ALL 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, 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

SECURE
KEY STORAGE

Storing encryption keys on many appliances in the network can introduce serious vulnerabilities. Threat actors can acquire keys from vulnerable points and use them for encrypted attacks or data extraction.

With FIPS 140-2 Level 3-validated internal and external Hardware Security Module (HSM) support, Thunder SSLi reduces decryption points so encryption keys are stored securely.

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 protocols help verify the origin certificate is valid.

ENSURE
COMPLIANCE AND PRIVACY

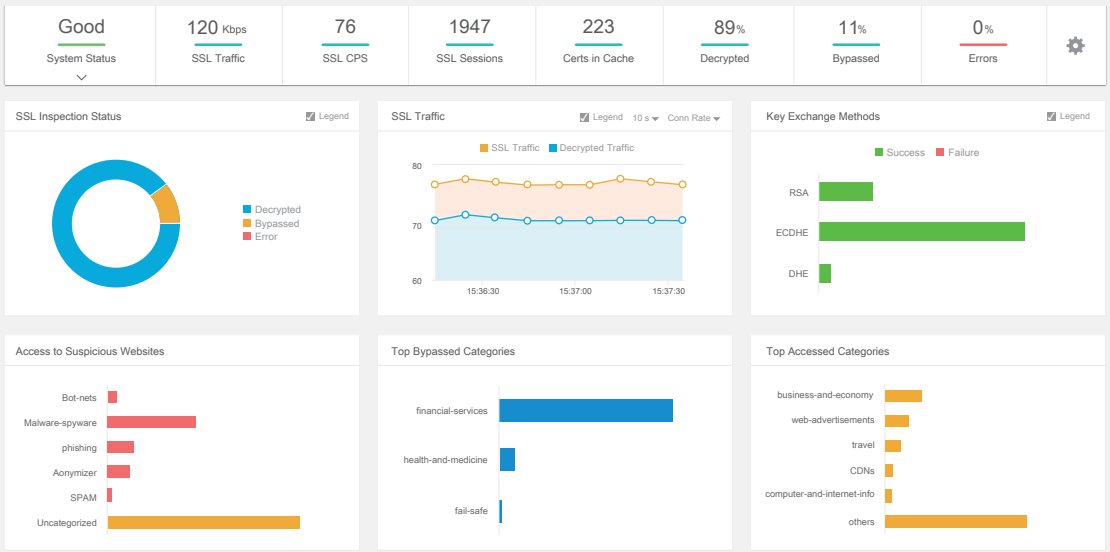
Thunder SSLi allows for selective decryption, making sure that organizations can keep up with industry, government and other compliance and privacy standards. For example, HIPAA compliance may forbid the decryption of private and sensitive healthcare information.

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.

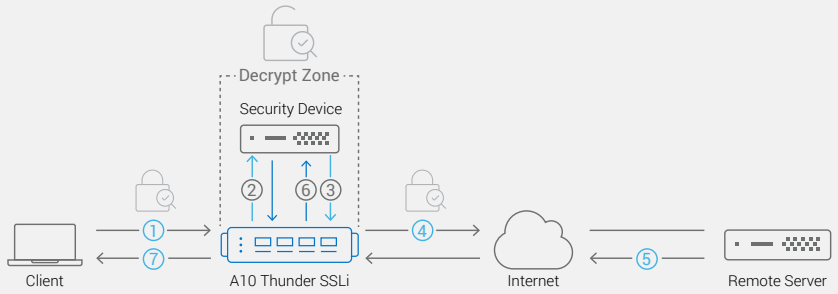
SIMPLIFY OPERATIONS
AND MANAGEMENT

A wizard-based configuration, deployment and management tool, AppCentric Templates make Thunder SSLi the easiest-to-use decryption solution in the industry. With informative dashboards, organizations can track their network with ease. Thunder SSLi also includes an industry-standard CLI, a web user interface and a RESTful API (aXAPI®), which integrates with third-party or custom management consoles.



AppCentric Templates help users manage their encrypted traffic using a dashboard to visualize SSL traffic, decryption and encryption, bypassing, traffic management using categorization, and more.

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.

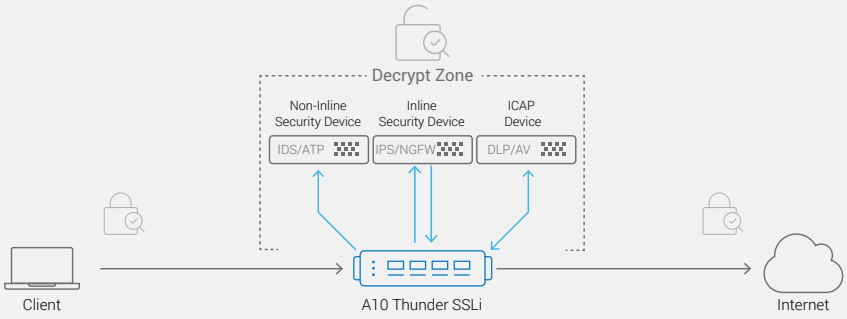
⑤ The server processes the request and sends an encrypted response to Thunder SSLi.

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 & 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 *SSLi*

THUNDER 840 *SSLi* | **500 Mbps**

THUNDER 5840S *SSLi* | **20 Gbps**

SMALL — MEDIUM — LARGE

Thunder SSLi provides decryption solutions that cater to the needs of small, medium and large enterprises.

DECRYPTED TRAFFIC SOLUTIONS FOR ANY SECURITY DEVICE

Thunder SSLi decrypts traffic for security devices from the top vendors.

FIREWALLS

- Cisco ASA with FirePOWER
- Palo Alto Networks Next Generation Firewalls
- Check Point Next Generation Firewalls

SECURE WEB GATEWAYS

- Symantec ProxySG
- Forcepoint Trusted Gateway System

ADVANCED THREAT PROTECTION

- FireEye Network Security
- Fidelis Network

FORENSICS AND SECURITY SYSTEMS

- RSA NetWitness
- IBM QRadar

OTHERS

- Symantec Data Loss Prevention (DLP)
- Bivio Networks Cybersecurity
- Trend Micro Deep Security
- Cyphort Advanced Threat Detection
- Vectra Networks Cybersecurity

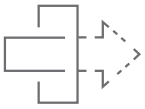
FEATURES

DECRYPT

ACROSS MULTIPLE PORTS AND PROTOCOLS

Using Dynamic Port Inspection, Thunder SSLi decrypts traffic across all TCP ports. Decryption for protocols like STARTTLS, XMPP, SMTP and POP3 are also supported.

However, the decryption functionalities are not limited to only SSL/TLS, encrypted traffic and decryption for SSH traffic is supported as well.



FULL-PROXY

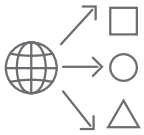
ARCHITECTURE

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 multiple cipher suites, including DHE and ECDHE, for perfect forward secrecy (PFS) support.



URL CLASSIFICATION

FOR SELECTIVE DECRYPTION

Thunder SSLi URL classification categorizes the traffic of more than 460 million 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.

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.

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.

SECURE HSM

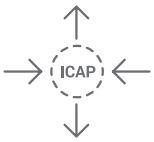
FOR FIPS COMPLIANCE

Thunder SSLi supports both internal and external network HSMs to ensure private keys are securely stored. With industry-leading support for up to four internal HSMs (FIPS 140-2 Level 3-validated), Thunder SSLi provides high performance with better security. Thunder SSLi interoperates with existing external HSMs deployed in the network.

EXPLICIT

PROXY 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.



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.

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.

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.

THUNDER SSLi PHYSICAL APPLIANCE

PERFORMANCE*1	THUNDER 840 SSLi	THUNDER 1030S SSLi	THUNDER 3030S SSLi	THUNDER 3040S SSLi	THUNDER 3230S SSLi
SSLi Throughput	0.5 Gbps	1.5 Gbps	2.5 Gbps	2.5 Gbps	3.5 Gbps
SSLi CPS	RSA (1K): 500 RSA (2K): 300	RSA (1K): 4K RSA (2K): 3K	RSA (1K): 8K RSA (2K): 6K	RSA: 8K ECDHE: 4.5K	RSA: 12.5K ECDHE: 7K
SSLi Concurrent Sessions	40K	125K	200K	200K	200K
NETWORK INTERFACE					
1 GE Copper	5	6	6	6	0
1 GE Fiber (SFP)	0	2	2	2	4
1/10 GE Fiber (SFP+)	2	2	4	4	4
Management Ports	1 x Ethernet Management Port, 1 x RJ-45 Console Port				
HARDWARE SPECIFICATIONS					
Processor	Intel Communications Processor	Intel Xeon 4-core	Intel Xeon 4-core	Intel Xeon 4-core	Intel Xeon 4-core
Memory (ECC RAM)	8 GB	8 GB	16 GB	16 GB	16 GB
Storage	SSD	SSD	SSD	SSD	SSD
Hardware Acceleration	Software	Software	Software	Software	1 x FTA-4
SSL Security Processor ('S' Models)	N/A	Yes	Yes	Yes	Yes
Dimensions (Inches)	1.75 (H) x 17.0 (W) x 12 (D)	1.75 (H) x 17.5 (W) x 17.45 (D)	1.75 (H) x 17.5 (W) x 17.45 (D)	1.75 (H) x 17.5 (W) x 17.45 (D)	1.75 (H) x 17.5 (W) x 17.15 (D)
Rack Units (Mountable)	1U	1U	1U	1U	1U
Unit Weight	8.8 lbs	18.0 lbs 20.1 lbs (RPS)	20.1 lbs	20.6 lbs	23 lbs
Power Supply (DC option available)	Single 150W (AC only)	Single 600W*3	Dual 600W RPS	Dual 600W RPS	Dual 600W RPS
	100 - 240 VAC, 50-60Hz	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz			
Power Consumption (Typical/Max)*2	57W / 75W	98W / 108W	180W / 240W	180W / 240W	190W / 240W
Heat in BTU/Hour (Typical/Max)*2	195 / 256	334 / 369	615 / 819	615 / 819	648 / 819
Cooling Fan	Single Fixed Fan	Hot Swap Smart Fans			
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%				
Regulatory Certifications	FCC Class A, UL, CE, TUV, CB, VCCI, CCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, CCC, KCC BSMI, RCM, FAC | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, CCC, KCC, BSMI, RCM, EAC, FAC | RoHS, FIPS 140-2*1+	FCC Class A, UL, CE, CB, GS*, VCCI, CCC*, KCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, TUV, CB, VCCI, CCC, KCC, BSMI, RCM, NEBS | RoHS
Standard Warranty	90-Day Hardware and Software				

Thunder SSLi Physical Appliance Specifications (Cont.)

PERFORMANCE*1	THUNDER 3430S SSLi	THUNDER 4440S SSLi	THUNDER 5330S SSLi	THUNDER 5440S SSLi	THUNDER 5840S SSLi
SSLi Throughput	5.5 Gbps	8 Gbps	10 Gbps	15 Gbps	20 Gbps
SSLi CPS	RSA: 18K ECDHE: 10K	RSA: 22K ECDHE: 10K	RSA: 30K ECDHE: 15K	RSA: 35K ECDHE: 20K	RSA: 50K ECDHE: 25K
SSLi Concurrent Sessions	400K	400K	400K	1 Million	1 Million
NETWORK INTERFACE					
1 GE Fiber (SFP)	4	0	0	0	0
1/10 GE Fiber (SFP+)	4	24	8	24	24
40 GE Fiber (QSFP+)	0	4	0	4	4
Management Ports	1 x Ethernet Management Port, 1 x RJ-45 Console Port				
HARDWARE SPECIFICATIONS					
Processor	Intel Xeon 6-core	Intel Xeon 6-core	Intel Xeon 10-core	Intel Xeon 12-core	Intel Xeon 18-core
Memory (ECC RAM)	32 GB	32 GB	32 GB	64 GB	64 GB
Storage	SSD	SSD	SSD	SSD	SSD
Hardware Acceleration	1 x FTA-4	2 x FTA-4	1 x FTA-4	2 x FTA-4	2x FTA-4
SSL Security Processor ('S' Models)	Yes	Yes	Yes	Yes	Yes
Dimensions (Inches)	1.75 (H) x 17.5 (W) x 17.15 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 17.15 (D)	1.75 (H) x 17.5 (W) x 30 (D)	1.75 (H) x 17.5 (W) x 30 (D)
Rack Units (Mountable)	1U	1U	1U	1U	1U
Unit Weight	23 lbs	32.5 lbs	23 lbs	32.5 lbs	32.5 lbs
Power Supply (DC option available)	Dual 600W RPS	Dual 1100W RPS	Dual 600W RPS	Dual 1100W RPS	Dual 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz				
Power Consumption (Typical/Max)*2	210W / 260W	360W / 445W	210W / 260W	360W / 445W	375W / 470W
Heat in BTU/Hour (Typical/Max)*2	717 / 887	1,229 / 1,519	717 / 887	1,229 / 1,519	1,280 / 1,604
Cooling Fan	Hot Swap Smart Fans				
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%				
Regulatory Certifications	FCC Class A, UL, CE, GS, CB, VCCI, CCC, KCC, BSMI, RCM, NEBS | RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC, KCC, BSMI, RCM | RoHS, FIPS 140-2^+	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM, NEBS | RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM | RoHS	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM | RoHS
Standard Warranty	90-Day Hardware and Software				

The specifications, performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions.

*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.

^ Certification in process.

+ FIPS model must be purchased.

THUNDER SSLi PHYSICAL APPLIANCE WITH HSM

PERFORMANCE*1,*2	THUNDER 5440 SSLi with HSM	THUNDER 6630 SSLi with HSM
SSLi Throughput (RSA 2K keys)	15 Gbps	40 Gbps
SSLi CPS (RSA 2K keys)	50K	100K
NETWORK INTERFACE		
1/10 GE Fiber (SFP+)	24	12
40 GE Fiber (QSFP+)	4	0
100 GE Fiber (CXP)	0	4
Management Ports	1 x Ethernet Mgmt port, 1 x RJ-45 console port	
HARDWARE SPECIFICATIONS		
Processor	Intel Xeon 12-core	2 x Intel Xeon 12-core
Memory (ECC RAM)	64 GB	128 GB
Storage	SSD	SSD
Hardware Acceleration	2 x FTA-4	4 x FTA-3
SSL Security Processor ('S' Models)	1 or 2	1, 2 or 4
Dimensions (Inches)	1.75 (H) x 17.5 (W) x 30 (D)	5.3 (H) x 16.9 (W) x 30 (D)
Rack Units (Mountable)	1U	3U
Unit Weight	32.5 lbs	74.5 lbs
Power Supply (DC option available)	Dual 1100W RPS	2+2 1100W RPS
	80 Plus Platinum efficiency, 100 - 240 VAC, 50 – 60 Hz	
Power Consumption (Typical/Max)*2	400W / 485W	995W / 1,150W
Heat in BTU/Hour (Typical/Max)*2	1,365 / 1,655	3,395 / 3,924
Cooling Fan	Hot Swap Smart Fans	
Operating Ranges	Temperature 0° - 40° C | Humidity 5% - 95%	
Regulatory Certifications	FCC Class A, UL, CE, GS, CB, VCCI, CCC, BSMI, RCM | RoHS, FIPS 140-2 Level 3	FCC Class A, UL, CE, TUV, CB, VCCI, KCC^, EAC, FAC | RoHS, FIPS 140-2 Level 3
Standard Warranty	90-Day Hardware and Software	

The specifications, performance numbers are subject to change without notice, and may vary depending on configuration and environmental conditions.

*1 Tested with maximum HSM cards in two appliances SSLi deployment. Cipher "TLS_RSA_WITH_AES_128_CBC_SHA" with RSA 2K keys are used.

*2 With base model. Number varies by HSM card option.

^ Certification in process.

DETAILED FEATURE LIST

Features may vary by appliance.

Decryption

- High-performance SSL decryption and encryption as a forward proxy
- Full-proxy architecture
- Internet Content Adaption Protocol (ICAP) support for data loss prevention (DLP) and antivirus 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
- 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
  - RSA/DHE/ECDHE 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)
- 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)

Hardware Security Module (HSM)

- FIPS 140-2 Level 3-validated on-board HSM (Up to four cards on a single platform)**
- External network HSM with Thales nShield

URL Classification***

- URL Bypassing for web category-based selective decryption
- URL Filtering for blocking of known malicious or undesirable websites
- URL Classification Service powered by Webroot

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

Management

- Dedicated on-box management interface (GUI, CLI, SSH, Telnet)
- Web-based AppCentric Templates (ACT) support
- SNMP, syslog, email alerts
- RESTful API (aXAPI)
- LDAP, TACACS+, RADIUS support
- Configurable control CPUs

* Features may vary by appliance.
** Available on select models.
*** URL Classification for URL Filtering and Bypassing subscriptions are available as an additional paid service.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-DS-15113-EN-11 JUN 2017