- Acting as a SSL/TLS proxy that adjusts the cipher suite selection for encryption, such as protocol conversion for down level client or server.
- Multiple deployment options on Array's AVX Series Network Functions Platform, ASI Series dedicated ADCs or vAPV virtual ADCs.
- Offering configuration, deployment and management of multiple Array appliances via optional AMP centralized management platform.
- Providing comprehensive reporting and analytics for SSL/TLS based traffic via optional MARS virtual appliance.
- Industry-standard CLI, a web user interface and a RESTful API that integrates with third-party or custom management consoles.
- Integration with VMware Orchestrator and Microsoft System Center, as well as OpenStack.
- Space-efficient, redundant-power hardware appliances that consume 10-35% less power versus alternative solutions.
- Familiar CLI, intuitive cloud-friendly WebUI and centralized management for ease of use and configuration.

FEATURES

High Performance, Best-in-Class Ciphers

Array's SSLI solution on dedicated appliances - ASI and AVX can be accelerated for high throughput of RSA 2048-bit and 4096-bit key sizes as well as ECC ciphers, Array SSLI delivers high performance while supporting multiple cipher suites, including DHE and ECDHE, for Perfect Forward Secrecy (PFS).

Decryption across Multiple TCP Ports

If the application is using SSL/TLS, Array SSLI decrypts application traffic across all TCPS ports using Deep Packet Inspection (DPI). Decryption of protocols such as SMTPS and POP3S are also supported.

Multiple Deployment Modes

As per the customer environment, Array SSLI solution can be deployed in Layer-2 or Layer-3 mode, on single device or multiple as required.

Layer-2 mode is called the bridge mode. With an L2 bridge configuration, the APV appliance function as an L2 device to bridge SSL traffic, allocate it to the upper layer within the APV appliance for decryption and then forward the decrypted traffic to the security device(s) for inspection.

Layer-3 mode is called the routing mode. In this configuration, the ASI appliance working in L3 mode forwards all the packet that is not destined for any of its IP addresses by looking up in its routing table. Packets that are left and are not meant for any of its MAC addresses are forwarded by looking up its MAC address table. When the ASI appliance works in L3 mode, it can cooperate with two or more security devices working in L2 or L3 mode to implement SSL interception.

For inbound, known domains, encrypted network packets can be intercepted and decrypted by deploying the server private key on SSLI.

On the other hand, for outbound SSL traffic originating from clients is sent out to the internet or cloud hosted infrastructure which in turn proves that ASI appliance can function as a forward or reverse proxy.

SPAN Port Support

The Array SSLI SPAN Port feature integrated filter

lists to filter the traffic that needs to be captured. With the help of filter lists, the system is configured to capture traffic with specific source IPs, source ports, destination IPs and destination ports. Furthermore, it allows the definition of packets to be captured that is flowing in the inbound, outbound or both directions.

Complete Proxy Architecture

Array SSLI acts as a proxy that can adjust the cipher suite selected for encryption. It can re-negotiate to a different cipher suite of a similar strength, which makes the solution future-proof against new ciphers or TLS versions that might occur in the network without notice. It also ensures the traffic is encrypted using the most secure ciphers, discarding the use of compromised ones.

SSLI - URL Categorization

Array's optional SSLI URL classification uses Webroot BrightCloud to categorize URLs (such as financial or health web sites) across 82 categories.

Thereafter the traffic is selectively bypassed or decrypted depending on the compliance standards and risk factors. With this functionality enabled, the ASI appliance determines the category of a given website via the local cache, the local database or an online connection to the Webroot server.

Load Balancing of Multiple Security Devices

Array's industry-leading ADC load balancing capabilities can be utilized with the SSLI solution to help improve the availability and performance of the security devices. The system (either one or two ASI appliances) sends captured packets to multiple security devices, either of the same or different types.

If the security devices are of the same type, the system can be configured to send the captured packets to the security devices in a load balancing manner based on the hash value of the packets' source IP and destination IP addresses.

Traffic Management

Array SSLI includes ADC traffic management functions that can manage non-encrypted traffic with options available such as, block/drop and redirect to assure appropriate handling of the traffic.

Centralized Management and Analytics

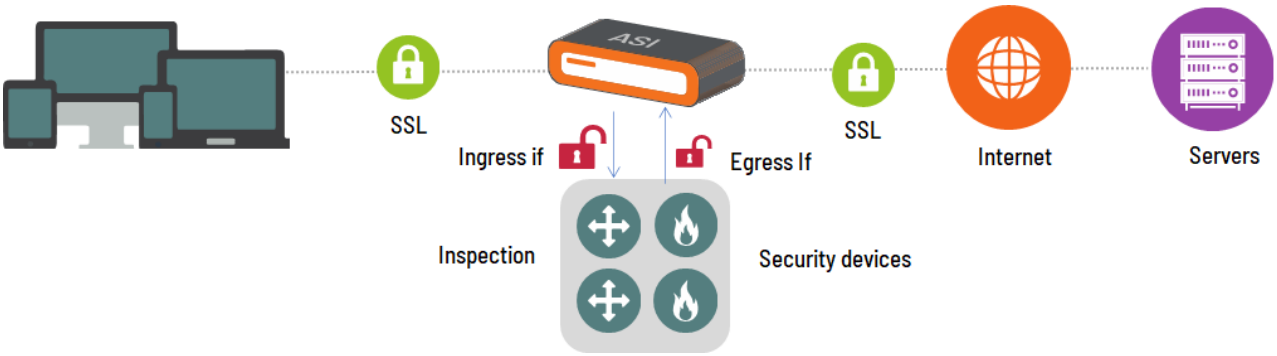
Centralized management and analytics can be used for configuration, monitoring and reporting. Array SSLI includes industry standard CLIs, RESTful APIs and System Logs that can be easily integrated with third-party or custom management consoles, including SSL/TLS keys and certificate management. It helps enterprises and cloud service providers to efficiently manage and monitor multiple Array products among other applications/ devices from a central point. It provides an easy way to lay down administrative privileges with different types of administrators, streamlines and speeds-up configuration management of multiple local or geographically distributed appliances.

Privacy and Compliance Initiatives

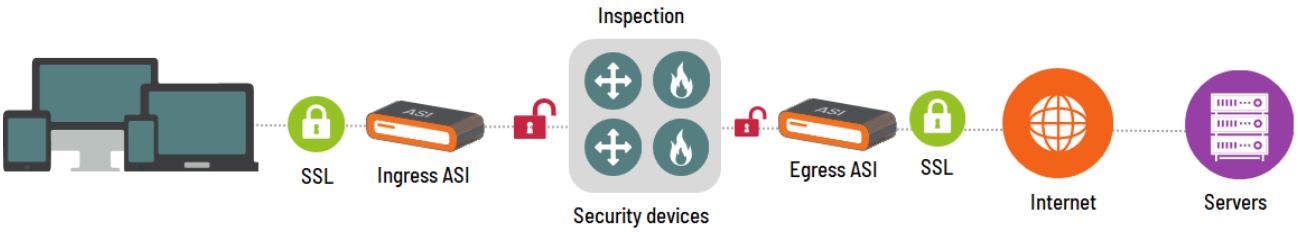
The SSL Interceptor serves as an effective policy enforcement point to control SSL traffic throughout the enterprise. It reduces risks posed by encrypted traffic while maintaining compliance with relevant privacy policies and regulatory requirements. Using URL Classifications, organizations can easily create granular policies to selectively decrypt traffic and meet their business requirements. (Example: "Do not decrypt financial or banking traffic going out of the business"

Typical Deployment

Option 1: Integrated Mode



Option 2: Distributed Mode



Dedicated and Virtual ASI Appliances

Array's ASI Series dedicated appliances support the SSLI as well as the optional URL classification feature license. It can be used for SSLI deployments that require a very large number of SSL transactions per second (greater than 20K RSA-2K Key, for example). For smaller deployments where performance is less of a concern, Array's vAPV virtual application delivery controllers with software-based SSL processing can be used. Array's SSLI can be deployed either on a single device or multiple for encryption and decryption, also known as the integrated model.

Product Specifications – ASI Platform

• **STANDARD** o **OPTIONAL**

	ASI 1800	ASI 2800	ASI 5800	ASI 7800	ASI 9800
Max. L4 Throughput	7 Gbps	20 Gbps	40 Gbps	100 Gbps	160 Gbps
Max. SSL Throughput	7 Gbps	10 Gbps	25 Gbps	45 Gbps	90 Gbps
Max. SSL TPS (RSA 2K)	20K	20K	40K	53K	110K
Max. ECC TPS (ECDSA P256)	14K	14K	28K	38K	76K
1 GbE Copper	•	•	•		
1 GbE Fiber			o		
10 GbE Fiber		•	•	•	•
40 GbE Fiber				o	o
Power Supply	ASI1800, 2800			Dual Power: 100-240VAC, 8-4A, 50-60Hz	
	ASI5800			Dual Power: 100-240VAC, 8-4A, 50-60Hz	
	ASI7800, 9800			Dual Power: 100-240VAC, 10-5A, 50-60Hz	
Dimensions	ASI1800, 2800. 5800			1U – 17" W x 19.875" D x 1.75" H	
	ASI7800, 9800			2U – 17" W x 22.5" D x 3.5" H	
Weight	ASI1800, 2800, 5800			18.4 lbs.	
	ASI7800, 9800			29.6 lbs.	
Environmental	Operating Temperature: 0˚ to 45˚C, Humidity: 0% to 90%, Non condensing				
Regulatory Compliance	ICES-003, EN 55024, CISPR 22, AS/NZS 3548, FCC, 47FR part 15 Class A, VCCI-A.				
Safety	CSA, C/US, CE, IEC 60950-1, CSA 60950-1, EN 60950-1				
Support	Gold, Silver and Bronze Level Support Plans				
Warranty	1 Year Hardware, 90 Days Software				

1371 McCarthy Blvd. Milpitas, CA 95035 | Phone: (408) 240-8700 Toll Free: 1-866-MY-ARRAY | www.arraynetworks.com

VERSION: MAY-2020-REV-A