Array

SSL Intercept

DATASHEET

Array SSL Intercept provides industry-leading 3rd-Party Security Devices with Visibility into Encrypted Traffic for Improved Security and Performance.

In today's hi-tech world, Internet security for users is considered critical. Hence, most of the world's web traffic has been encrypted via SSL/TLS. However, SSL/TLS encryption is considered as a double-edged sword for all the enterprises as well as for xSPs. Let's understand why?

At the time when SSL/TLS is improvising the security, hackers are trying to break through using the cloak of SSL/TLS encryption. SSL/TLS is used to protect millions of network users, but we shouldn't forget the fact of how vulnerable it is. There are times when firewalls, IDS/IPS, APT and other data loss prevention techniques do not have the required visibility into encrypted traffic, which often leads to malware and other data attacks. There will be application traffic slow down when the security devices installed performs SSL/TLS traffic inspection as the added decryption/encryption processing and the volume of SSL/TLS traffic can easily overpower security device resources.

Additionally, for data privacy policy and compliance, such as HIPAA, banking and several other regulations, certain types/destinations of SSL/TLS traffic are mandatory to bypass inspection to comply and preserve data privacy.

To resolve this, Array's SSL intercept acts as a proxy that can decrypt SSL/TLS traffic to allow third-party security application to perform an inspection, which then re-encrypts the traffic before it is forwarded to its destination. built-in SSL/TLS high performance SW and HW relieve the compute-intensive SSL/TLS processing from the security application to allow it to perform at its peak. Array's whitelisting ensures that sensitive information to and from trusted sites is not decrypted, and web classification helps ensure that banking, healthcare and other regulated information is processed appropriately.

In addition to this, the Array's SSLi solution can assure transparent deployment, high performance and critical security mechanisms across several third-party security applications.

Highlights And Benefits

- Onboarding a powerful SSL/TLS SW/HW helps you decrypt and re-encrypt web traffic that allows better visibility for security devices.
- Unburdening the compute-intensive SSL/TLS processing from security devices, allows them to operate at peak performance and support advanced SSL/TLS features.
- Processing all the sensitive information appropriately via whitelisting & web classification
- Accommodating various network configurations via several deployment modes, such as: SSL/TLS Bridge ADC setup in front of known HTTPS/TCPS services
- Operates as a Web agent to enable explicit forward proxy with outbound Web access control/Monitoring.
- Supports simple and transparent L2 Bridge inline deployment for selected traffic, and SSL/TLS bridge support for protocol conversion.
- Protecting against a diverse set of threats and offers a web classification service for blacklisting/whitelisting via Optional Webroot BrightCloud Threat Intelligence Service
- Stabilizing traffic across numerous security devices for high a vailability and more efficient operation.
- Direct support for active and passive security devices such as FW, IPS/IDS, WAF, and DLP.
- Service chaining allows maximum security competence by 'cascading' traffic across multiple security device types in sequence.
- Decrypting traffic across all TCP ports using Dynamic Port Inspection as well as providing decryption for protocols such as SMTP and POP3
- Deploying encryption and decryption on single Array device (integrated mode) or on multiple devices (distributed mode)
- 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, APV 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

With dedicated SSL/TLS acceleration hardware of Array's SSLi solution on APV and AVX appliance 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).

Multiple Deployment Modes

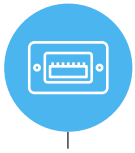
As per the customer environment, Array SSLi solution can be deployed in Layer-2 or Layer-3 mode, on single device or multiple as required. Layer-2 mode is called the bridge mode. With an L2 bridge configuration, the APV appliance function as an L2 device to bridge SSL traffic, allocate it to the upper 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 APV 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 APV 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 APV appliance can function as a forward or reverse proxy.

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 for protocols such as SMTPS and POP3S are also supported.



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 (bidirectional).

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 ciphers.

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 thirdparty or custom management consoles, includes SSL/TLS keys and certificates management. It helps the enterprises and cloud service providers efficiently manages and monitor multiple Array Networks products among other applications/devices from a central point. The centralized management provides an easy way to lay down administrative privileges to different types of administrators, streamlines and speeds-up configuration management of multiple local or geographically distributed appliances.

Traffic Management

Array SSLi includes APV Series ADC traffic management functions that can manage nonencrypted traffic as well, with options available such as, block/drop and redirect to assure appropriate handling of the traffic.

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 APV appliances) then send 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.

SSLi - URL Categorization

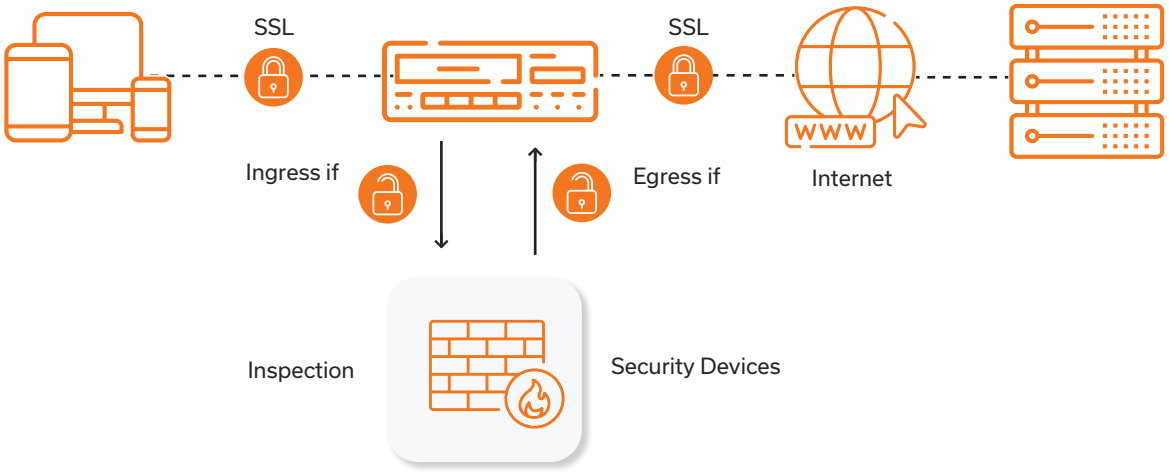
Array's optional SSLi URL classification uses Webroot BrightCloud to categorize URLs (such as financial or health web sites) across 82 categories.

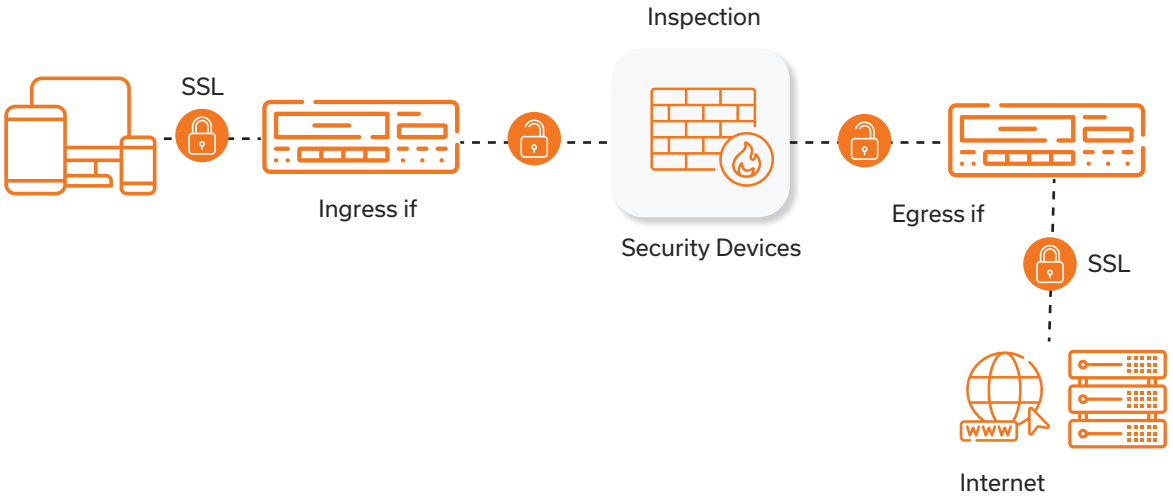
Thereafter the traffic is selectively bypassed or decrypted depending on the compliance standards and risk factors. With this functionality enabled, the APV appliance determines the category of a given website via the local cache, the local database or an online connection to the Webroot server.

Privacy and Compliance Initiatives

The SSL Intercept 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 to meet their business needs (Example: "Do not decrypt financial or banking traffic going out of the business")

Typical Development





Dedicated and Virtual ASI Appliances

Array's ASI Series physical 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 utilized. Array 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 2800	ASI 5800	ASI 7800	ASI 9800	ASI 12800
Max. L4 Throughput	20 Gbps	40 Gbps	100 Gbps	160 Gbps	200Gbps
Max. SSL Throughput	10 Gbps	25 Gbps	45 Gbps	90 Gbps	90/120Gbps
Max. SSL TPS (RSA 2K)	20K	40K	53K	110K	110/220K
Max. ECC TPS (ECDSA P256)	14K	28K	38K	76K	76/142K
1 GbE Copper	•	•			
1 GbE Fiber		o			
10 GbE Fiber	•	•	•	•	o
40 GbE Fiber			o	o	o
100 GbE Fiber					•
Power Supply	ASI2800 ASI5800 ASI7800, 9800		Dual Power: 100-240VAC, 8-4A, 50-60Hz Dual Power: 100-240VAC, 8-4A, 50-60Hz Dual Power: 100-240VAC, 10-5A, 50-60Hz		
Dimensions	ASI1800, 2800. 5800 ASI7800, 9800		1U – 17" W x 19.875" D x 1.75" H 2U – 17" W x 22.5" D x 3.5" H		
Weight	ASI2800, 5800 ASI7800, 9800		18.4 lbs. 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				

VERSION: OCT-2019-REV-A

1371 McCarthy Blvd.
Milpitas, CA 95035

www.arraynetworks.com

+1-866-MY-ARRAY
+1 408-240-8700