AVX SERIES SOLUTION BRIEF

SSL Intercept

Array SSLi Gives 3rd-Party Security Devices Visibility into Encrypted Traffic for Improved Security and Performance

Background

The majority of the world's web traffic is now encrypted via SSL, which vastly increases security for users. For enterprises, xSPs and others, however, SSL encryption is a double-edged sword. While SSL improves security overall, hackers are increasingly using the 'cloak' of SSL encryption to deliver malicious payloads directly into data centers and enterprises.

Often, firewalls, IDS/IPS, data loss prevention and other security appliances do not have visibility into encrypted traffic and thus can allow malware and other threats to traverse the network uninspected. For those security devices that do support SSL decryption and inspection, the sheer volume of SSL traffic can overwhelm resources and thus impact performance. In addition, to meet HIPAA, banking and other regulations, certain traffic is required to be passed through without decryption or inspection in order to preserve user privacy.

Array's SSL intercept (SSLi) feature set, acting as a proxy, decrypts SSL traffic to allow 3rd-party security appliances to perform inspection, then re-encrypts the traffic before forwarding it to its final destination. Built-in SSL resources offload compute-intensive SSL processing, allowing security appliances to operate at their peak performance level. 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, Array's SSLi solution can load balance and/or service chain traffic across multiple 3rd-party security appliances to help assure high performance and availability of these critical security mechanisms.

Key SSLi Solution Benefits

Using Array to decrypt and re-encrypt SSL traffic allows security appliances to do what they do best – with complete visibility into network traffic – while maintaining high availability and performance and easily adapting to changing deployment modes.

Array's SSLi solution decrypts SSL traffic to allow inspection and remediation by 3rd-party security devices to protect against attacks,

intrusion and data exfiltration attempts, and then optionally re-encrypts the data before sending the traffic on to its final destination. Array's high-performance hardware-based SSL resources process SSL traffic far more efficiently than most security appliances, thus helping assure their performance. APV Series ADC can operate as a Webagent service to implement explicit forward proxy mode, which adds an additional layer of security by anonymizing internal user IPs and network structures, and by providing firewalling via Array's WebWall web application firewall.

Forward proxy works in tandem with the Webroot BrightCloud Threat Intelligence Service feature option, which offers a diverse set of threat protections across multiple vectors. BrightCloud includes reputation services to protect users from malicious sites, as well as a web classification service to blacklist inappropriate sites and/or whitelist sites for which traffic must flow uninspected for regulatory or other requirements (such as financial or medical sites that contain sensitive personal information).

Array's SSLi solution offers multiple deployment modes to accommodate different environments, including L2 or L3 mode, integrated or distributed mode, and forward or reverse proxy. The Array solution can load balance traffic across multiple security appliances, and/or service-chain different appliance types in turn to assure high availability and continued protection under load.

SSLi on the AVX Series Network Functions Platforms

Array's AVX Series Network Functions Platforms support multiple Array and 3rd-party networking and security functions on a single platform, and abstracts the complexities of network functions virtualization – taking the guesswork and risk out of NFV adoption. In addition, the AVX Series offers the best of both worlds – the agility of virtualization coupled with the performance of dedicated appliances, and mix-and-match sizing to optimize VA performance.

The AVX Series provides dedicated resources per VA instance, including hardware SSL processing, CPU, memory and I/O resources. In addition, dedicated resources are reserved for hypervisor management to minimize virtual machine contention and enable SLAs for business-critical customers and applications.

The AVX Series supports Array's vAPV virtual application delivery controller (ADC), with the SSLi feature license and optional URL classification subscription, to provide SSL intercept decryption and re-encryption for security appliances like next-gen firewalls, IDS/IPS and others. In addition, the AVX Series can support multiple 3rd-party security virtual appliances on-board, allowing service chaining for maximum flexibility in security design, as well as reducing CAPEX, space, energy and other costs.

Other Deployment Options

Array's APV Series physical ADC appliances also support the SSLi feature license as well as the optional URL classification feature license, and can be used for SSLi deployments that require a very large number of SSL transactions per second (greater than 20K RSA 2K, for example). For smaller deployments where performance is less of a concern, Array's vAPV virtual application delivery controllers, with software-based SSL processing, may be utilized.

Summary

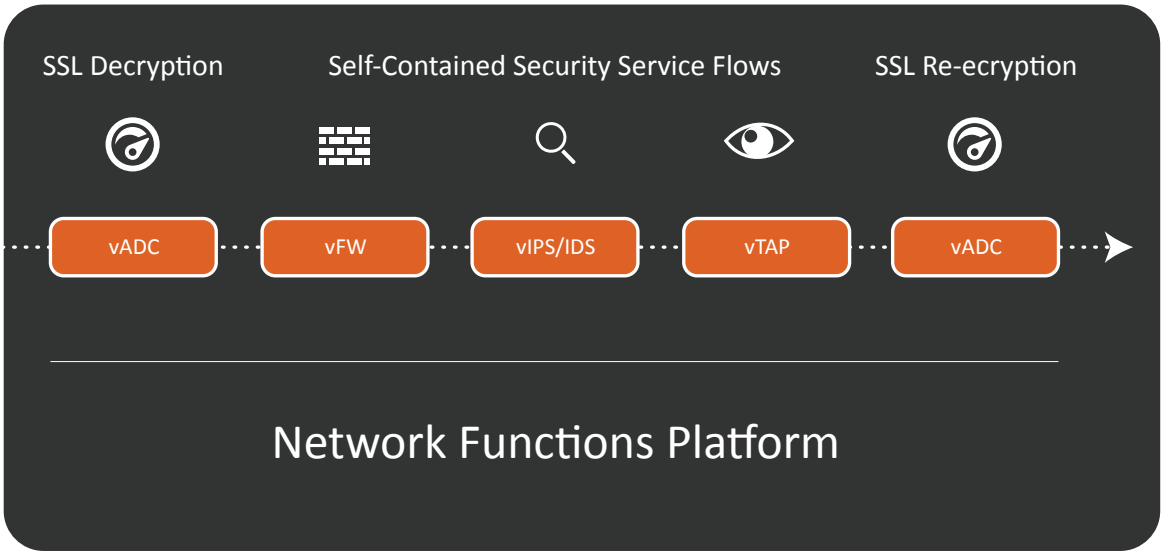
As SSL-encrypted traffic becomes the norm, the effectiveness of security devices such as next-gen firewalls, IDS/IPS and others can be compromised by lack of visibility into encrypted traffic, as well as by the resource-intensive nature of SSL processing. Array's SSLi solution efficiently and securely handles the decryption and re-encryption needed to allow visibility into SSL

SSLi Benefits

- Powerful onboard SSL processing efficiently decrypts and re-encrypts SSL traffic to allow visibility for security devices
- Offloads compute-intensive SSL processing from security devices, allowing them to operate at peak performance
- Whitelisting and optional web classification to ensure that sensitive information is processed appropriately
- Multiple deployment modes to accommodate different environments and requirements
- Can operate as a Webagent to enable explicit forward proxy
- Optional Webroot BrightCloud Threat Intelligence Service protects against a diverse set of threats
- Load balances traffic across multiple security devices for more efficient operation
- Service chaining allows maximum flexibility in security design
- Multiple deployment options: on Array's Network Functions Platform, on Array APV Series dedicated load balancers or vAPV virtual load balancers

traffic, and offers white listing and web classification to ensure that sensitive information is processed appropriately. In addition, the Array solution load balances and/or service chains across multiple security appliances to allow the greatest possible flexibility in security design, as well as ensuring high performance and availability of security devices.

A step-by-step deployment guide for the SSL Intercept solution is available on our website.



For more information about how Array Networks can help you provide visibility into SSL-encrypted traffic while providing high availability and high performance for security devices, visit us at array-networks.co.in or send us an email at sales-india@arraynetworks.com.

www.array-networks.co.in