White Paper

SSL Offloading and Acceleration in Virtualized Environments

Assuring High Performance in the Cloud

APV Series Application Delivery Controllers

Introduction

The move to the cloud has brought a quantum shift in data center design, as well as the delivery mechanisms for resources and applications. In order to consolidate resources and enable rapid scaling, data centers often deploy a virtualized infrastructure including virtualized servers, firewalls, and application delivery controllers (ADCs).

However, the same quantum shift brought by cloud computing has also changed the way that business-critical information is shared and used – it is no longer confined to the traditional IT environment. In these circumstances, SSL/TLS data encryption is frequently employed to secure mission-critical and sensitive data across the Internet.

Securing Data in Transit

SSL/TLS data encryption has become the *de facto* standard for securing data in transit. Cloud-based virtual ADC appliances support software-based SSL/TLS data encryption by leveraging the host CPU's resources, and in many cases those resources provide enough performance and throughput via enhancements. For example, Intel-based CPUs recently added support for the Advanced Encryption Standard new instructions (AES-NI) to improve SSL/TLS encryption and decryption speeds.

However, software-based (i.e. virtual) SSL/TLS performance is typically much lower than that of hardware-based (i.e. dedicated physical appliance) solutions. For example, for Array's vAPV virtual application delivery controller the average SSL/TLS transactions per second (TPS) for 2048-bit keys is around 600 TPS. If other virtual machines are sharing the same CPU, resource competition and contention could further reduce throughput.

In addition, there's one very important proviso: In terminating SSL/TLS, it is necessary to see clear text for devices and functions to allow deep packet inspection, such as an ADC looking for application session IDs, cookies and URLs for intelligent application routing, filtering and/or server persistency. SSL/TLS termination thus requires additional processing power, especially for new session ID exchanges.

Adding multiple vAPV virtual ADC appliances can help scale up SSL/TLS performance, but cost and set-up complexity is increased as well. In addition, virtual ADC appliances running on a common CPU will not be able to fulfill the FIPS hardware security module (HSM) requirements. FIPS, the U.S. government's Federal Information Processing Standard, has also been adopted by governments and other entities worldwide as a standard for data security.

A Hybrid Virtual/Dedicated Model for SSL/TLS Offloading

In circumstances where SSL/TLS performance must be assured in a virtual environment, and scaling requirements preclude an all-virtual model, a hybrid virtual/dedicated application delivery controller model can be of benefit. This model combines the economies and flexibility of one or more virtual ADC appliances with the proven performance and throughput of one or more dedicated ADC appliances.

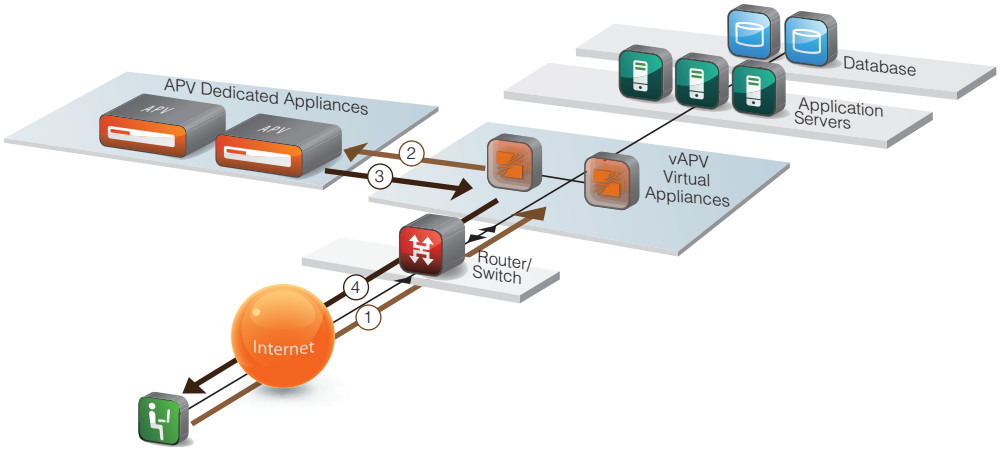

Figure 1: Hybrid Virtual/Dedicated ADC Model using vAPV SLB Virtual Service

Depending on the model, Array dedicated APV Series application delivery controllers can support 2k to 70k SSL/TLS transactions per second for 2048-bit SSL processing. In addition, up to 4 million SSL/TLS connections/sessions, and 25Gbps encrypted data throughput per unit are supported. The hybrid model not only speeds up SSL/TLS processing (and thus reduces load on the virtual ADC appliance and servers), but also increases application capacity by supporting more secure connections via SSL/TLS when needed. In addition, a dedicated Array APV Series appliance can provide FIPS HSM compliance, if needed.

How the Hybrid Virtual/Dedicated SSL Offloading Model Works

As shown in the diagram above, the hybrid virtual/dedicated SSL offloading model works as follows:

1. Similar to an HTTP request, the client starts an HTTPS request (TCP destination: port 443), which is forwarded to the vAPV virtual appliance
2. With external HW SSL offloading, the HTTPS service request is forwarded to the dedicated APV Series appliance by using the vAPV virtual appliances' server load balancing (SLB) virtual service (TCP port 443) or by the router/switch (policy-based routing)
3. Using an SLB virtual service (TCPS port 443), the dedicated APV Series appliance terminates and decrypts the client HTTPS request and initiates an HTTP connection/forward request to the vAPV virtual appliance (HTTP port 80)
4. Based upon its SLB configuration, the vAPV virtual appliance selects a Real Server and forwards the client HTTP request

5. In the reversed path, once the server responds to the vAPV, it forwards the response to the dedicated APV Series appliance, which encrypts the server response and then sends the HTTPS response to the client through the vAPV (or, if the request was routed via the router/switch the response will be routed via that path).

The description and diagram above are typical for an enterprise deployment. However, for a service provider deploying SSL offload as a service (Infrastructure-as-a-Service model), the dedicated APV Series appliances can be located at the data center edge managed by the service provider and shared by multiple tenants to offload and accelerate SSL processing, thus allowing scaling as needed.

Key Features of the Hybrid Virtual/Dedicated SSL Offloading Model

The hybrid virtual/dedicated SSL offloading model includes several key features that improve performance, support scaling and enhance application security:

- **Accelerate Secured Applications** – Because compute-intensive SSL processing is performed in high-performance, dedicated APV Series hardware, the time delays for key exchange, encryption/decryption and other functions are greatly reduced.
- **Improved Scaling Capability** – The hybrid model offers a simple means of scaling up secured application capacity and availability through SSL offloading. In addition, the hybrid model provides redundancy and application health checks to improve application availability.
- **Enhance Application Security** – Array dedicated and virtual ADC appliances feature a proprietary, high-performance SSL processing stack that mitigates potential SSL/TLS protocol attacks. Most vendors' ADC products are based on OpenSSL, which has suffered multiple vulnerabilities such as Heartbleed, Bash and Man-in-the-Middle (MitM). In addition, the hybrid model provides multi-layered network security, with full reverse proxy functions that serve as application firewalls with deep scanning of client requests.

Simplified Deployment and Management

The combined virtual vAPV and dedicated APV Series appliances are tightly integrated, running on the same underlying software. This provides additional benefits for deployment and management of the hybrid model, including:

- **ADC Integration** – The virtual and dedicated ADC appliances are integrated, with advanced Layer 4-Layer 7 server load balancing, application scripting, caching and compression, Layer 7 session persistence, Web application firewall and access control lists (ACLs).
- **SSL Bridge Mode** – This capability provides end-to-end security with simple network integration without major network reconfiguration.

- **SSL Client Certificate Management** – The combined solution provides high-performance client certificate verification, international language support, access control, and flexible client information-forward functions. It also includes full-functioned support for certificate validation via an external certificate authority (CA) via certificate revocation lists (CRLs) and online certificate status protocol (OCSP)
- **Supports Other Secure Protocols** – In addition to HTTPS, the solution supports many other protocols that can run over TCPS using SSL encryption functions. These protocols include FTPS, POPS, SMTPS, IMAPS, LDAPS, NNTPS and others.

Conclusion

In virtualized cloud and data center environments, performance and scaling of SSL/TLS processing can be assured through a hybrid virtual/dedicated ADC model. This model leverages the economies and flexibility of one or more virtual vAPV ADC appliances with the proven performance of one or more dedicated APV Series application delivery controllers. Through the model, SSL/TLS processing can be offloaded from both the servers and the virtual ADC appliances, and application capacity and availability can also be increased by supporting more SSL/TLS secure connections than otherwise could be processed. In addition, dedicated APV Series appliances can also meet requirements for FIPS HSM compliance.

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 250 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Feb-2017 rev. a