COST EFFECTIVELY HANDLING ENCRYPTED TRAFFIC ACROSS THE IT INFRASTRUCTURE

As more websites, enterprise applications and web services are mandating the use of traffic encryption in communications, the load for processing this encryption on the various parts of the IT infrastructure is growing exponentially. 2016 marked an important milestone around traffic encryption: over 50% of overall internet traffic was encrypted, after more than 10% growth in encrypted traffic in the previous 12 months. Moreover, to overcome newly discovered vulnerabilities in encrypted communication protocols, new cyphers and key exchange mechanisms were introduced, delivering higher level of security.

While this trend provides increased privacy to end users and organizations, it also introduces a new set of challenges, for example, the need to refresh an existing infrastructure, which does not support new encryption standards, or the growing percentage of cyber-attacks, which are taking advantage of the encrypted traffic tunnels to hide malicious activity.

When Handling Encrypted Traffic Processing on the Server Becomes Impractical

Application servers were not originally designed to handle communication encryption and decryption. This is why in many cases (especially when the amount of encrypted traffic is high) the application's infrastructure architecture include an application delivery controller (ADC) with dedicated hardware for encrypted traffic processing, to offload this task from the servers.

However, with the need to now support new cyphers and a rapidly growing capacity of encrypted traffic, most organizations are forced to shop for an ADC solution that can handle current and future needs.

Radware's new Alteon D-line provides an industry-leading solution that addresses all the above-mentioned challenges for offloading the processing of encrypted traffic from the servers. Its software is optimized to handle the latest traffic encryption protocols and cyphers, and its embedded dedicated hardware, based on the latest chipset in the industry for processing traffic encryption and decryption, provides unmatched price-performance ratio for any size application.

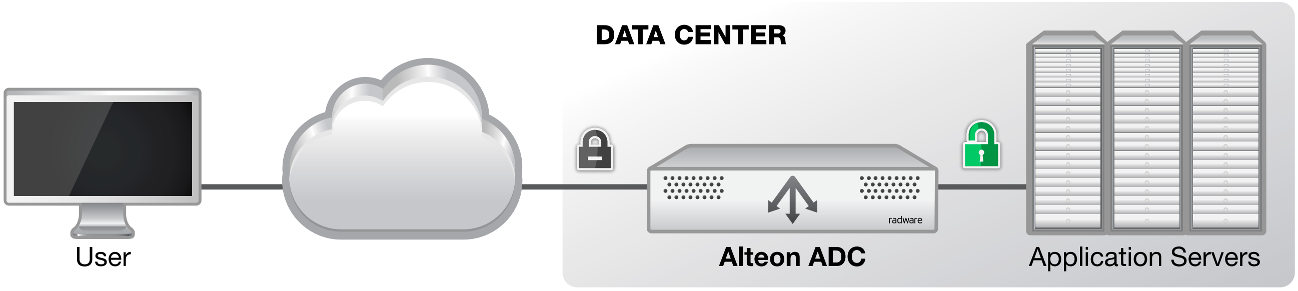

Figure 1- Encrypted traffic processing offload - network diagram

Whether the application infrastructure architecture includes physical ADC appliances or virtual appliances deployed in the cloud, the Alteon D-line delivers advanced ADC capabilities for guaranteeing the application's service level and user experience, coupled with a high performance and cost-effective engine for encrypted traffic processing.

As a result, organizations now have the option to reduce their applications' total cost of ownership by using the same application servers together with the new Alteon D-line to handle more users while handling much larger capacities of encrypted traffic with the latest cyphers.

Changing the Business Case for Removing the Blind Spot from Perimeter Security Devices

Another area in the datacenter that needs to consider the rising use of encrypted traffic is the perimeter security devices, which today are mostly blind to cyber threats that are passing through them, in an encrypted format. The main reason why many organizations do not inspect encrypted traffic (according to Gartner, 80% of organizations as of end of 2016) is the performance penalty those devices suffered from when trying to decrypt and re-encrypt the data passing through them (about 80% of reduced performance in most cases).

Additionally, organizations that tried to address this problem directly on these perimeter security devices ultimately found it very costly. First because they had to over-provision because end security devices like servers have traditionally not been optimized for handing SSL. Second, because each security device that needed said visibility had to be overprovisioned i.e. firewall, IPS , WAF , DDOS , DLP etc. The other major problem was the unacceptable introduction of latency the decrypt encrypt process takes time doing it over and over again can add unacceptable levels of latency.

Radware's SSL Inspect solution provides the ability to gain visibility both to encrypted traffic in the inbound direction (initiated by a client across the internet towards a server inside the organization) and in the outbound direction (initiated by a client inside the organization towards a server in the cloud / internet).

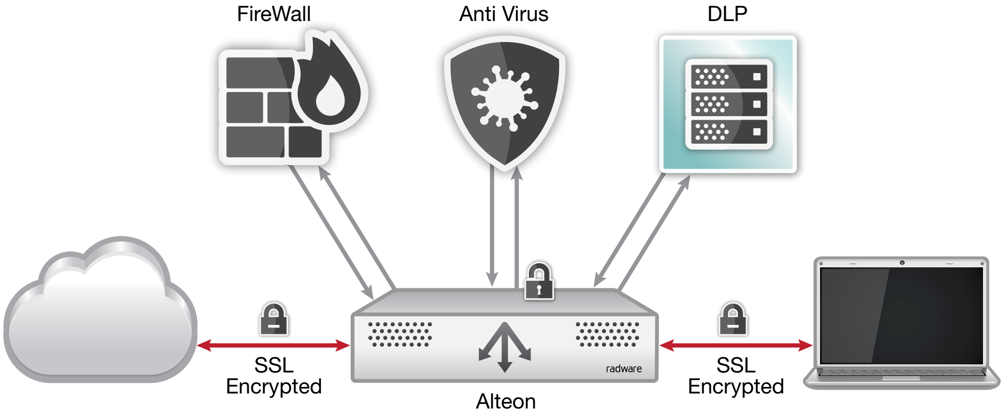

Figure 2 - SSL Inspect Solution Diagram (outbound direction example)

Radware's SSL Inspect solution, based on the Alteon D-line with its advanced and highly efficient SSL processing engine, provides a high capacity and a cost effective alternative to processing encrypted traffic on perimeter security devices such as firewalls, data leakage prevention (DLP) servers, anti-malware, IDS/IPS, and other devices. By offloading the processing of encrypted traffic from those devices, the SSL Inspect solution simplifies deployment and reduces latency applied on the traffic to a minimum, ensuring the fastest, highly secured user experience.

Using the Alteon D-line's SSL inspect functionality enables organizations to remove the blind spot that most perimeter security devices have today, at a fraction of the cost and effort of doing it in their existing security devices (up to 60% less). This makes the business case around securing their internet communication much more attractive and reasonable.

Adding Visibility into Encrypted Traffic for DDoS Protection Solutions

One of the ways for cyber attackers to get through DDoS mitigation solutions is to replace their HTTP flood attacks with HTTPs attacks (encrypting the HTTP flood sessions). This is why most vendors in the market have added an SSL proxy as part of their DDoS mitigation solution, to open the HTTPs encrypted sessions and allow the DDoS mitigation device to detect and block the attack. The problem with this approach is that the same proxy device used to open the encrypted sessions becomes a vulnerability point by itself, as it is a stateful device, with session tables, which can easily be flooded with session (the essence of a DDoS attack), filling its table and causing it to choke.

Radware's Defense SSL solution, based on the same traffic encryption processing engine in the Alteon D-line, provides a stateless solution on one hand for handling SSL traffic, and a high capacity engine supporting all the latest cyphers on the other hand.

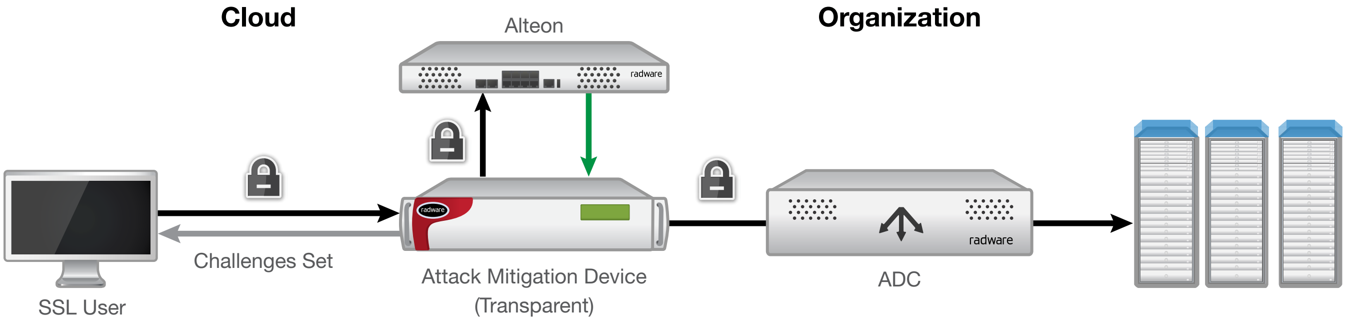

Figure 3 - Defense SSL solution Architecture

The unique architecture of the defense SSL solution, which hides the SSL proxy behind the DefensePro DDoS mitigatory, coupled with the Alteon D-Line's powerful traffic encryption processing engine, provide customers a high capacity DDoS solution. It is capable of handling encrypted attacks at the same volume as non-encrypted attacks in the most cost effective manner, while supporting the latest cyphers and eliminating any possible choke point.

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.