SCALABLE AND HIGHLY-AVAILABLE SECURITY SERVICES INFRASTRUCTURE WITH ALTEON SSL INSPECT

Alteon SSL Inspect provides policy-based, security services chaining for seamless traffic steering through multiple security solutions while eliminating the SSL blindspot.

Designing and building an enterprise security solution which protects users and servers from all threat vectors that exist today is a complex task. It requires advanced traffic engineering through a chain of multiple protection solutions. Much of the traffic on the Internet is encrypted and all of those security solutions pay a steep performance penalty when decrypting and re-encrypting traffic to identify and block the threats. Radware offers the Alteon SSL Inspect as a security service chaining gateway that simplifies deployment of enterprise security services, enables higher availability, seamless scalability, granular control of traffic protection and offloads SSL traffic processing from security solutions.

BACKGROUND

Businesses must protect their network from network-based cyber-attacks. They are required to deploy, design and build a tight enterprise security solution which protects the users and servers from all threat vectors that exist today. This requires multiple attack detection and prevention tools including network firewall, intrusion detection or prevention system (IDS/IPS), anti-malware, data leak prevention (DLP) and more. To add to that, the growth of SSL encrypted traffic results in a steep performance penalty that these security tools have to pay when decrypting and re-encrypting traffic to detect and block attacks. This decryption/re-encryption process also adds latency to the communications. Designing, provisioning and managing enterprise security services becomes extremely challenging.

THE CHALLENGE

The enterprise IT network and security teams face multiple challenges involved in designing, managing and provisioning security services:

- Complex network configurations are required to ensure that only relevant traffic flows through the various security inspection devices. Managing and provisioning security services is even more challenging as each security tool has its own requirements and properties.
- High availability is costly (often require 1+1 redundancy) and complex to configure when each inspection solution has its own proprietary redundancy model.
- Performance and scalability are costly: users suffer from increased latency; security tools run out of capacity when SSL encrypted traffic grows; scaling capacity often results in forklift hardware upgrades.

THE SOLUTION

Radware's Alteon SSL Inspect provides a simple one-box solution for intelligent, policy-based security services chaining for seamless traffic steering through multiple security solutions. SSL Inspect acts as a central switching point for all perimeter network security tools. Security managers can chain and provision security services with highly granular policy options per user profile. SSL Inspect supports highly available, scalable and flexible security services deployment and reduces overall security solution costs via offloading decryption and re-encryption of SSL encrypted traffic.

FEATURES AND BENEFITS

Policy-based Security Services Chaining

SSL Inspect uses simple wizards to define user or traffic profiles and the corresponding policies to transparently steer traffic through the various security inspection servers in the chain. SSL Inspect service chaining enables simplified security services provisioning and reduces the administrative tasks involved in service management and maintenance.

Flexible Deployment Options

SSL Inspect can be implemented as a bump in the wire device, overseeing all of the organization's traffic to and from the Internet or as a two instance solution with virtual/physical separation between the DMZ and the enterprise's internal network. Based on its advanced application classification capabilities, SSL Inspect seamlessly intercepts and steers traffic to the various security solutions for in-depth inspection before allowing it to continue to its destination. It also allows combining steering traffic to active inline devices as well as forwarding a copy of the traffic to out-of-path passive devices.

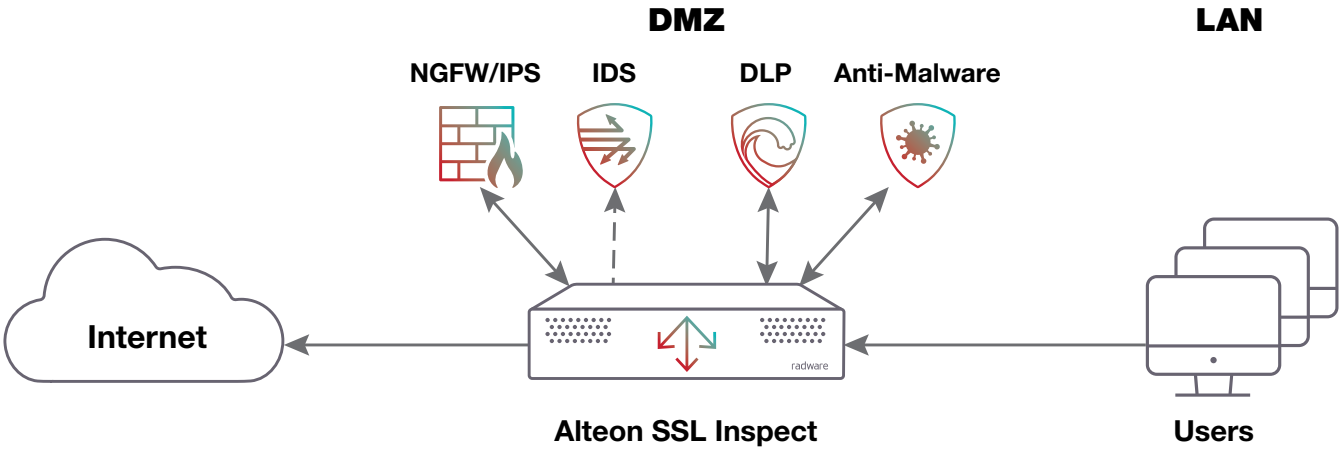

Figure 1: SSL Inspect steers traffic to active inline security inspection tools (NGFW, IPS, DLP) as well as to passive, out-of-path, security inspection tools (IDS)

Furthermore, SSL Inspect has a unique ability to connect to any type of value-add security service (VAS) including 1 or 2-leg solution, L2 and L3 solutions, or out-of-path solutions that read network traffic in TAP mode.

Advanced High Availability

The unique deployment architecture of SSL Inspect and its inherent load balancing capabilities enables it to load balance each of the security server farms separately and thus ensure traffic will always flow through the most available server. Even in cases where servers are down, SSL Inspect provides a simple way to define a policy which decides whether to bypass to an unresponsive security service, ensuring continuous internet connectivity, or to block the traffic and avoid cyber threats.

SSL Visibility and Offloading

As a smart centralized traffic steering solution, the SSL Inspect, with its high capacity SSL hardware engine, decrypts all relevant SSL encrypted traffic before forwarding it to the various security solutions and re-encrypts the traffic before forwarding it to the final destination. Offloading traffic decryption and re-encryption delivers the following key benefits:

- Lower latency for all transactions as traffic is only decrypted/re-encrypted once for all solutions and not by each security solution separately
- Reduce costs of the overall solution, reducing the performance penalty up to 70% versus activating SSL traffic inspection in each of the security solutions

Multi-Vendor Certified Solution

Alteon SSL Inspect has been tested to validate full integration and performance improvement with following vendor solutions:

Solution Type	Vendor	Certified Product
Firewall / NGFW	Check Point SOFTWARE TECHNOLOGIES LTD.	Next generation Firewall
Firewall / NGFW	CISCO	Cisco ASA 5500-X Cisco Firepower 4100 Series Cisco Firepower 9000 Series
IPS/ NGIPS	CISCO	Cisco FirePOWER 8000 Series Cisco FirePOWER 7000 Series
Anti-Malware	FireEye	FireEye Network Security NX Series
Anti-malware	BlueCoat	Blue Coat Malware Analysis S400/S500
DLP	Symantec	Symantec Vontu

Improved Security Solutions Capacity

SSL Inspect provides several capabilities which improve the utilization of the enterprise's security devices:

- By steering only the relevant traffic to the security server for inspection, the load on that sever can be controlled and reduced, enabling cost effective sizing.
- SSL Inspect enables redundant security inspection solution servers to operate in an active-active mode through persistent load balancing to increase the traffic inspection capacity of the entire deployed solution.
- Centralized hardware based encrypted traffic processing offloads decryption/re-encryption from the multiple security inspection servers, thereby reducing their processing requirements and increasing their capacity, thus reducing their cost.

Outbound Traffic Management for Complete Privacy, Increased Security and Higher Productivity

SSL Inspect provides three additional modules to complete the outbound traffic management based on its embedded URL classification engine:

- **Employee privacy module**: In cases where the employee is browsing sites with private personal information, such as consumer banking or healthcare, the privacy module automatically designates that session as private, avoids its decryption and bypasses all inspection servers and sends the traffic directly to its destination, ensuring user privacy.

- **Browsing protection module**: Identifies access attempts to known malicious sites and blocks them on the fly, based on real time information from a database of malicious site URLs.

- **Productivity module**: Blocks access to various content categories including social sites such as Facebook, Google+ or to peer-to-peer file sharing sites (which abuse the organization's internet bandwidth) and delivers employee productivity improvements and increased network efficiency.

ABOUT RADWARE

Radware® (NASDAQ: RDWR), is a global leader of cyber security and application delivery solutions for physical, cloud, and software defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application, and corporate IT protection services to enterprises globally. Radware's solutions empower more than 12,500 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: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, 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.