radware

Remove Blind Spots with Radware's SSL Traffic Inspection Solution

Whitepaper

SHARE THIS WHITEPAPER

Table of Contents

SSL Encrypted Traffic Creates New Security Challenges for the Enterprise

Most web applications used for private, commercial or business purposes encrypt the transactions based on SSL/HTTPS protocol to ensure the privacy of data transfer between user and server. Recent surveys show that enterprise communication sent through its LAN and WAN infrastructure contains 25%-35% of SSL encrypted traffic on average. Certain vertical segments (such as finance or medical) can reach 70% of SSL encrypted traffic in the network due to the information communicated. SSL technology continues to improve the security it provides, with more complex and longer keys used to encrypt data.

SSL solves the privacy problem and secures the communication of sensitive information in and out of the enterprise. However, it has created new blind spots in the visibility of traffic that goes in and out of the enterprise. SSL has also become a vehicle to carry malicious programs into the enterprise IT infrastructure and allows sensitive information to leak out of the enterprise unnoticed.

The use of cloud applications has exacerbated matters even more. Many enterprises have clear security policies on what information is allowed to be stored in the cloud and what information must remain inside the enterprise's private datacenter. However, as cloud services often utilize secured connections, it makes the enforcement of these policies impossible as data leakage prevention solutions can't analyze the SSL encrypted traffic sent out to the cloud application and storage.

Even private emails or innocent collaboration tools have become a security hazard as malicious programs can cross through the enterprises' advanced, anti-virus solution unchecked, hide in the SSL connection established between the two ends and infect the end user's computer with malicious programs. This can lead to an infection with Trojan horses that sends sensitive information outside the organization over encrypted connections creating another blindspot for the enterprise's data leakage prevention (DLP) solutions.

Industry and Government Regulation Compliance

Organizations subjected to industry and government regulations, such as Health Insurance Portability and Accounting Act (HIPAA) or the Sarbanes-Oxley (SOX), have strict rules on accessing sensitive information and requires all traffic in the datacenter to be visible. This requirement poses a new challenge when facing the inherent need to keep data transmission encrypted and ensure privacy.

Things to Consider When Addressing the Visibility of SSL Traffic Challenges

IT administrators seeking a solution that enables visibility into SSL encrypted traffic should consider several things to ensure a long lasting, cost effective and efficient solution.

1. Decryption/re-encryption of SSL sessions to enable inspection of both clear and encrypted traffic for security purposes while keeping the privacy of the traffic content in its journey to its destination.

2. The solution should be optimized for SSL traffic and to be able to handle a high (and scalable) volumen of SSL encrypted traffic with minimal impact or delays.

3. Network topology: Eliminate the need to re-engineer the network or reconfigure the client devices with a new proxy address to pass relevant traffic through the SSL traffic inspection device.

4. Many organizations own more than one security solution that requires visibility into SSL traffic (i.e., intrusion detection, next generation firewalls, data leakage prevention, etc.). Any outbound SSL inspection solution needs to be able to selectively forward traffic to one or more security solution, without adding unnecessary latency along the way.

5. End-user privacy considerations: In many countries it is forbidden for employers to inspect private information such as the data in browsing sessions to banking sites or on-line healthcare services. This poses another requirement from the outbound SSL inspection solution to be able to identify such private sessions and bypass the inspection of it.

6. Scalability: As the amount of traffic/SSL traffic continuously grows, SSL traffic inspection solutions must seamlessly scale and eliminate forklift upgrades as much as possible.

7. High availability: To avoid downtime due to outages, the SSL traffic inspection solution should always ensure traffic is only forwarded to the available value added security server, and automatically bypass service servers.

Radware's SSL Traffic Inspection Solution

Radware offers one unified solution that uniquely addresses all challenges and requirements. Alteon NG can be implemented as a bump in the wire, overseeing all of the organization's traffic to and from the internet. Based on its advanced Layer 4-7 classification capabilities, Alteon seamlessly intercepts SSL sessions and terminates it as if it were the authentication server. It opens a new SSL session on its other side, on behalf of the end-user, towards the original destination server.

Alteon's advanced transparent traffic steering capabilities are put to action in order to forward the decrypted traffic to one or more security server solutions (such as firewalls, anti-malware, data leakage protection, etc.), providing full visibility into the content of both encrypted and clear text sessions.

Furthermore, Alteon can be programed with different security policies for various groups of end users and types of browsing destinations. Each security policy can include any combination of the following actions:

1. Intercept and decrypt/re-sign the SSL session
2. Pass the traffic through untouched
3. Forward the traffic to security server 1, and/or server 2, and/or server 3, etc.
4. Send a copy of the traffic to a predefined destination (for passive monitoring)

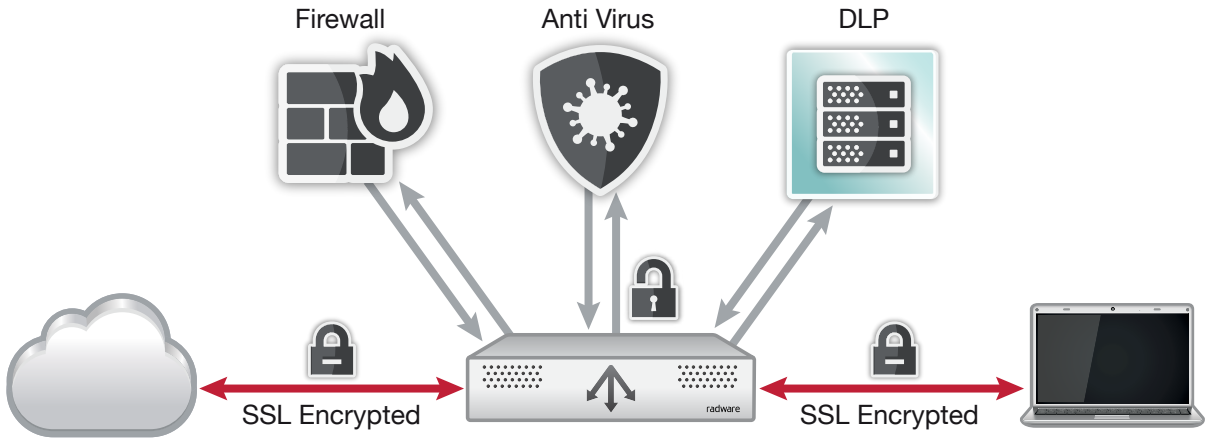

Figure 1: Radware's SSL Traffic Inspection Solution

By leveraging Alteon ADC capabilities and combining Radware's patented SSL inspection technology and transparent traffic steering, the solution delivers an advanced and flexible SSL traffic inspection solution that is simple to deploy.

High Availability and Scalability

Alteon can be deployed in a high availability configuration that eliminates any single point of failure. Its load balancing functionality guarantees high availability for security solutions and ensures the enterprise's connectivity by:

- Providing advanced health-check options to ensure traffic is only forwarded to available and responding servers.
- Alteon ADC can be programed (per service/application) to bypass unresponsive security solutions, or block the traffic in case the organization's security requirements requires it – for a specific application

High Volume SSL Traffic Inspection and Scalability

Radware's Alteon NG contains hardware based SSL engines for high capacity processing of SSL traffic. Alteon NG and its SSL engine enable initiation of several new connection setups per second and processing of multi gigabit per second of SSL traffic.

It allows customers to purchase a solution optimized in size to its current requirement, and grow on demand with a simple license application to the device purchased only when required - making it a cost-effective solution for any size organization.

To support scalability of the security solution, customers can use the inherent load balancing functionality in Alteon NG to add more servers for greater traffic inspection and protection power, and load balance between servers. Alteon NG also ensures a certain session will always reach the same physical server, allowing the security solution continuous analysis of full sessions and not just packet by packet.

Complete Outbound Traffic Management

Alteon NG provides three added value modules to complete the outbound traffic management for encrypted traffic inspection. Based on its inherent ability to analyze Layer 7 information, Alteon NG can parse the URLs employees are browsing and cross-match it with a live database of URL classes, providing the following capabilities:

Employee privacy module: Not all employees' outbound traffic should be inspected and sometimes the organization is required to maintain employees' privacy and avoid inspection of sessions to sites such as online banking, online healthcare services or insurance services. Alteon NG provides a privacy module which bypasses inspection of user sessions going to a predefined list of website classes, to ensure complete employee privacy.

Browsing protection module: There are several threats to end-user browsing which may direct users to malicious websites for phishing or pushing unwanted malware programs to the end-user's device. Alternatively, if a malware that is already installed and running on one the devices inside the organization's network tries to communicate with its Command &Control, it may result in sensitive data leakage from the organization. Alteon NG provides a browsing protection module which identifies and blocks access attempts to known malicious sites on the fly, based on a real time database of malicious sites' URLs.

Productivity module: Some organizations prefer to limit the type of sites employees are allowed to browse over its network in order to increase productivity of both the employee and of the network. Blocking access to social sites such as Facebook, Google+, news sites or torrent sites (which abuse the organization's internet bandwidth) can deliver both significant employees productivity improvement as well as increased network efficiency.

Benefits of Using Radware's Alteon for SSL Traffic Inspection

Radware's Alteon solution for SSL traffic inspection provides several benefits and advantages for organizations that wish to eliminate the security blind spots that exist in SSL encrypted traffic.

Enables visibility to all SSL traffic: Alteon can decrypt the SSL traffic on the fly, and forward the traffic for inspection in real time, to one or more security inspection and logging solutions.

Enables regulatory compliance: Alteon SSL traffic inspection solution enables organizations to meet various types of regulatory compliance requirements such as logging details of encrypted transactions, while ensuring and maintaining data exchange privacy.

Transparent deployment: Eliminate the need to re-engineer the network or configure end user clients to pass all traffic through a predefined SSL proxy. Alteon SSL traffic inspection solution can be deployed in transparent mode – as a bump in the wire, intercepting all traffic passing through it. As a result, it avoids the risk of becoming another element in the network that is prone to cyber-attacks.

Complete end-user privacy: Alteon NG can quickly decide which traffic to send for inspection and which traffic should be kept private and bypass the security inspection tools. This is based on the type of site the user is accessing (i.e. banking), device being used and other parameters.

Simple one box solution: A single Alteon provides a holistic solution for both inbound (SSL offload) and outbound (SSL inspection) transaction analysis, security solutions, load balancing and scalability - supporting multiple security value added services.

Seamless scalability: Alteon's on-demand approach, increasing SSL inspection capacity, is as easy as applying a higher capacity license on the Alteon unit. As the security inspection server reaches capacity limits, Alteon NG's load balancing function allows seamless addition of servers for more inspection and protection capacity.

Optimized resource utilization on Alteon: By defining which services are SSL encrypted, Alteon can process only encrypted traffic, passing through all the rest of the traffic, without over utilizing SSL encryption/decryption resources.

Reduced latency: Using Alteon SSL inspection solution, an organization will only need to decrypt and re-encrypt traffic once, even if it has multiple solutions that require SSL inspection. This is achieved through Alteon's transparent traffic steering and service chaining capability, where only relevant traffic per security service is passed to each of the services in a row.

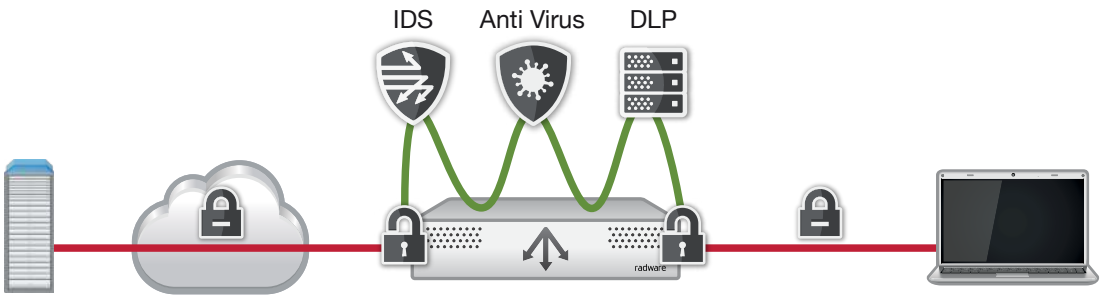

Figure 2 - Service Chaining

Guarantee connectivity at all times: Eliminate any single point of failure with High Availability (HA) Alteon topology, and use advanced health checks to ensure traffic is only forwarded to the security inspection servers that are fast responding and operational (or bypass them in case of congestion/high delays or complete failures).

Increased protection: Alteon NG provides additional layers of protection for outbound traffic to protect employees from reaching malicious sites (i.e. phishing sites or sites that may install malwares on your device), and other malware from connecting C&C, delivering another layer of protection to the organization.

Increased productivity: Alteon NG increases employee productivity by simply preventing browsing to social and news sites and increase network efficiency by preventing unwanted high bandwidth downloads from torrent sites and alike.

Mature patent protected solution: Radware's solution for content inspection of SSL/TLS (and non-SSL/TLS) traffic is a mature solution that has developed and evolved for over 10 years, and is fully patent protected (US Patent 7769994 B2).

Summary

As SSL traffic continuously gains momentum and increases in volume, so does the amount of security threats that take advantage of this new "invisibility" tunnel in the organization's network and datacenters. Security and network administrators need scalable solutions that will regain visibility into potential threats that may "hide" in SSL sessions.

Radware's SSL traffic inspection solution enables transparent high capacity SSL traffic interception and decryption, with a strong traffic steering engine that can flexibly steer the unencrypted traffic to several relevant security solutions for deep packet inspection. With Alteon's unique integrated capabilities, Radware offers a simple one box solution that is easy to deploy and eliminates the need to reconfigure end user clients' network configuration or reengineer the network to steer traffic through the Radware solution.

Radware's solution offers many additional benefits of scalability and high availability, both at the SSL traffic processing level and at the security services' capacity level.

Radware's SSL traffic inspection is the only solution on the market to combine a patent protected technology for SSL/TLS traffic inspection with transparent (and non-transparent) traffic steering, and load balancing technologies. It is only with this unique combination of capabilities that enterprises can benefit from uncompromised visibility into encrypted content, data security and regulatory compliance, all while maintaining high resource utilization efficiency and seamless scalability.