Mitigating the Encrypted Threat

With encrypted traffic in today's organizations accounting for 25-35% of all inbound and outbound Internet traffic, it should come as no surprise that SSL-based cyber-attacks are on the rise. Industry trends, including the migration to cloud computing environments and the transition to pushing customer interactions and transactions online, are forcing organizations to use encrypted connections to ensure privacy. New HTTP/2 internet protocols also mandate encrypted communications between browsers and servers. As the use of encrypted connections continues to rise, so has the volume of SSL-based attacks.

According to Radware's 2015-2016 Global Application & Network Security Report, over 25% of cyber assaults leverage SSL-based attack vectors. Today's hackers are increasingly using encrypted connections to hide attack traffic and infiltrate datacenters and applications. Many attack mitigation solutions lack the ability to decrypt encrypted traffic and inspect its content, leaving them vulnerable to these camouflaged cyber assaults. Even for solutions capable of detecting these types of attacks, there is heavy processing time for the decryption and encryption, which places a significant burden on servers.

Traditional Protection Provides Limited Coverage

In recent years, SSL-based assaults have broadened to include three types of attacks. The first is web attacks over an encrypted connection. Second is the ability to attack SSL infrastructure and exhaust SSL processing resources. The third is denial of service attacks via an encrypted session targeting both network and application-layer infrastructure.

While the majority of organizations have a solution that addresses the first issue, these solutions typically rely on an inline decryption device – a stateful device that is susceptible to attacks and cannot handle the higher volume encrypted DDoS attacks.

Encrypted Attacks Span across Layers

Provisioning of encrypted applications involves three infrastructure layers. Each layer is vulnerable to a different set of attacks and therefore is optimally protected by a different set of tools. Any breakage in the toolset or failure in protection can result in failure of the entire infrastructure.

- The TCP layer is vulnerable to network infrastructure and server attacks. It is important not to expose the system to such attacks while trying to protect it from other layers' threats.
- The SSL layer is inherently vulnerable to session saturation and renegotiation attacks due to the protocol structure, which requires more computing resources from the server than from the client in any session creation. Moreover, it is vulnerable to SSL-related protocol anomaly attacks and implementation vulnerabilities.
- The Encrypted Application Layer is vulnerable to application layer floods, application protocol and non-vulnerability attacks and application vulnerabilities.

Radware SSL/TLS Mitigation Solution

As part of its hybrid attack mitigation solution, Radware offers a patent-protected mitigation solution called DefenseSSL. DefenseSSL supports all common versions of SSL and TLS and protects from all types of encrypted attacks - including TCP SYN Floods, SSL Negotiation Floods, HTTPS Floods and Encrypted Web Attacks. Radware's SSL solution is deployed using Radware patented SSL DDoS protection technology which enables the SSL decryption agent to be deployed out-of-path and triggered only when suspicious activity starts.

It is the only solution that supports asymmetric deployment environments where only ingress traffic flows through the solution. This capability is crucial in cloud-based deployments such as within scrubbing centers or service provides, and multi-homed deployments.

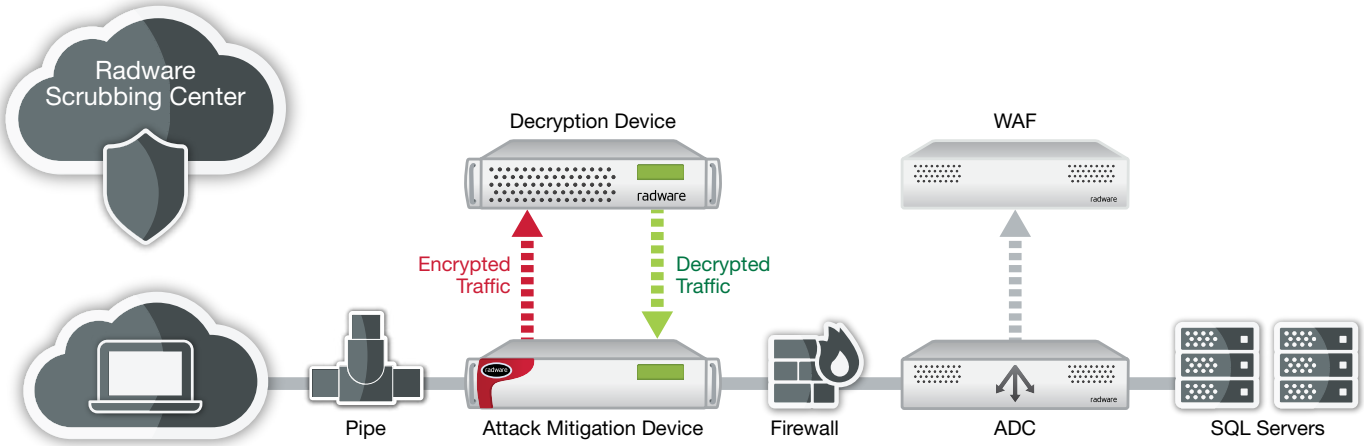

Figure 1: DefenseSSL deployed within the enterprise perimeter to detect/mitigate both clear and encrypted traffic.

Complete SSL Protection

Radware's SSL mitigation solution includes the following components:

- **TCP attack protection** includes Radware's behavioral-based network protection, TCP state saturation attacks protection, TCP challenge response mechanisms and TCP vulnerabilities and anomalies protection.
- **SSL vulnerabilities protection** includes SSL renegotiation attacks protection, state and session saturation protections, and SSL vulnerabilities protection signatures.
- **Encrypted challenge response technology** includes protection from HTTP floods and botnets. The HTTP challenge includes the capability to thwart advanced tools which are able to overcome standard challenge response mechanisms.
- **Encrypted applications signature protections** are applied to application traffic and protect from known attack tools and application vulnerabilities.
- **Encrypted web application protection** enables negative security while it applies decryption, normalization and decoding of application traffic – thus enabling complex known attacks protection. Positive security is applied by learning normal application behavior and patterns and enables zero-day web application protection.

Smart Certificate Management

Radware's SSL mitigation solution works to maintain user data confidentiality by performing the HTTPS validation with independent certificate management. This means that once a user is validated as legitimate, the HTTPS session resumes with the customer's certificate, which is unknown to Radware. As a result, user data remains

fully encrypted and confidential and customer certificate management remains unchanged. This also removes operational dependencies between the service provider and the organization when keys are changed. In addition, the solution allows usage of wildcard certificates to reduce operational complexity when required to protect a large number of subdomains.

Here are two use cases that demonstrate the unique benefits of Radware's SSL mitigation solution.

Use Case 1: Out-of Path Deployment

In the case of an HTTPS flood attack, Radware's perimeter attack mitigation identifies suspicious traffic using behavioral analysis and then sends only that traffic to the out-of-path decryption device for decryption. Via a set of challenge response mechanisms, applied only to the suspicious traffic, the attack is identified and mitigated. If the user passes all the challenges and is authenticated, a new SSL or TLS session is created which is allowed to reach the origin server directly.

This unique deployment model enables a solution which introduces zero latency in peace time and minimal latency under attack – only on the first session per each client.

Use Case 2: Detect at the Application, Mitigate at the Perimeter

In the case of an encrypted web attack, slow attack, evasive attack or encoded attack carried over HTTPS, Radware's WAF, deployed out of path, analyzes the advanced encrypted attack and uses unique messaging to send attack footprint for high speed mitigation at the perimeter - enabling full WAF level HTTPS protection at line speed with no added latency or risk to legitimate users.

Through its patent-protect, unique technology, Radware offers the only mitigation solution in the industry that provides full, scalable, lowest latency protection from encrypted attacks.

Benefits of Utilizing Radware DefenseSSL

Leveraging Radware's mitigation solution provides numerous benefits to organizations that wish to eliminate security blind spots that exist due to SSL encrypted traffic.

- **Enable visibility to all SSL & TLS traffic** for real-time inspection of outbound encrypted traffic via one or more content-based security and logging solutions.
- **Advanced detection and mitigation** from the increasing number of encrypted attacks targeting organizations using SSL & TLS.
- **Transparent deployment** eliminates the need to re-engineer the network or configure end user clients to pass all traffic through a predefined SSL proxy.
- **Flexible security policies** including URL class-based classification ensures user privacy is kept (i.e. traffic to banking sites is not inspected) based on class.
- **Reduced latency** through service chaining so that SSL traffic only needs to be decrypted and re-encrypt once, and not for each security solution.
- **Helps maintain user data confidentiality** by performing the HTTPS validation with independent certificate management.
- **Removes operational dependencies** between the service provider and the organization when keys are changed.

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.