Comprehensive SSL DDoS Attack Protection

The majority of internet traffic is now encrypted and accounts for as much as 85% of internet pages. Ironically, while SSL/TLS encryption is critical for many aspects of security, it also opens the door to a new generation of powerful distributed denial-of-service (DDoS) attacks. SSL/TLS connections require up to 15 times more resources from the destination server than of the requesting host, meaning that cyberattackers can launch devastating DDoS attacks using only a small number of connections. Radware's encrypted DDoS mitigation solution offers industry-leading protection from SSL-based DDoS attacks without adding latency to customer communications while preserving user privacy and simplifying key management.

BEHAVIORAL-BASED DETECTION

Industry-leading, machine learning algorithms to detect HTTPS-based DDoS attacks using both rate-based parameters, as well as behavioral parameters not dependent on rates.

KEYLESS PROTECTION

This allows Radware to identify and block potentially malicious hosts, even without having to decrypt user communications and without the customer having to provide Radware with a copy of SSL certificates.

DOES NOT ADD LATENCY

Radware uses a unique, asymmetric challenge-response mechanism that enables it to block malicious connections without impacting legitimate users.

PRESERVES USER PRIVACY

A unique approach that blocks malicious SSL connections without having to decrypt all customer traffic, thereby preserving user privacy and meeting compliance requirements.

Unique Asymmetric Approach

Radware's SSL DDoS mitigation solution is based on a unique asymmetric approach that does not require full decryption of all traffic and requires only ingress traffic to flow through the solution. Whenever a suspicious connection is identified, the solution applies a challenge-response mechanism to block potentially malicious hosts. This allows Radware to mitigate suspicious traffic without impacting legitimate users.

Smart Key Management

For customers interested in a deeper level of inspection, Radware's SSL mitigation solution maintains user data confidentiality by performing HTTPS validation with independent certificate management. To reduce operational complexity when protecting large numbers of applications and subdomains, Radware's solution supports usage of TLS server name indication (SNI) and of wild-card and subject alternative name (SAN) certificates.

Premise-Based, Cloud and Hybrid Deployments

Radware's encrypted DDoS mitigation solution offers flexible SSL protection deployment models, including cloud-based SSL protection with Radware's Cloud DDoS Protection Service, on-premise protection using a Radware DefensePro appliance or hybrid deployments that combine both premise-based and cloud-based protection.

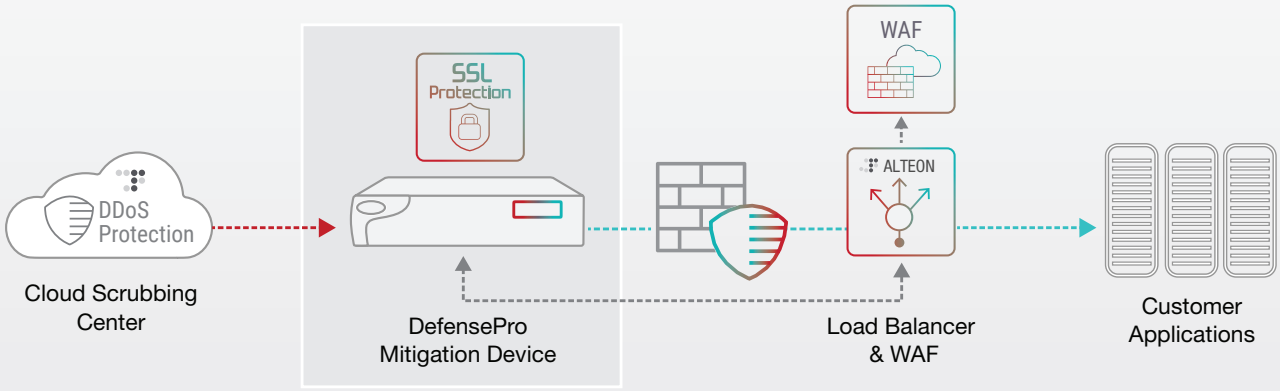

Figure 1: How Radware's solution works

Comprehensive SSL Protection

Radware's SSL mitigation solution provides the following key protections:

- **Network protection** includes Radware's behavioral-based network protection, transmission control protocol (TCP) nonsession-based attack protection, TCP challenge-response mechanisms and TCP vulnerabilities and anomalies protection.
- **Protection against HTTPS Floods and botnets** based on an innovative algorithm that inspects encrypted ingress traffic to detect attacks. This unique technology allows for keyless detection and smart, surgical mitigation without having to decrypt the traffic.
- **Known attack tools and vulnerabilities** using signatures to protect from known attack tools and application vulnerabilities.
- **Encrypted web application protection** in combination with Radware's web application firewall (WAF) to detect and block penetration attempts hiding beneath the encryption layer.

Attack Vector	Details
HTTPS Flood	• Flood of requests toward an HTTPS server • Single or multiple requests per connection • Botnet with variable request rate per source • Any HTTP Command (GET/POST/HEAD/etc.) • Randomized URL/User Agent/Cookie/etc.
HTTP Large Page Attack	• Egress pipe saturation (large responses)
SSL Vulnerabilities	• Malformed SSL packets • SSL Renegotiation
TCP Floods	• TCP flood on port 443 • Nonsession-based TCP attacks • DDoS SSL tools