Radware’s DefenseSSL System Features Behavioral-Based Algorithms To Prevent HTTPS Flood Attacks

Published on 24 Jul 2019

Radware® a provider of cyber security and application delivery solutions, announces that its SSL DDoS attack protection, DefenseSSL®, now features behavioral-based algorithms for keyless protection against HTTPS flood attacks. For the first time, organizations have the scale needed to effectively mitigate HTTPS floods.

According to Google, the majority of internet traffic is now encrypted and accounts for more than 70% of internet pages. 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.

**Simplifying key management**

SSL/TLS connections require up to 15 times more resources from the destination server than of the requesting host, meaning that threat actors can launch devastating DDoS attacks using only
a relatively small number of connections. Radware’s keyless DDoS mitigation solution now makes it possible to protect from SSL-based HTTP DDoS attacks at scale without adding latency to customer communications, and while preserving user privacy and simplifying key management.

“Service providers and carriers serve many tenants on their network and provide them with cyber-attack protections

Service providers and carriers serve many tenants on their network and provide them with cyber-attack protections. Due to their own security policies, network tenants cannot provide their decryption keys to the service provider’s or carrier’s network administrators, which leaves the providers or carriers vulnerable to HTTPS flood attacks. With no decryption capabilities, service providers and carriers are left with no effective solution to provide HTTPS flood protection to their tenants.

Managing decryption keys

Radware’s Chief Marketing officer, Anna Convery-Pelletier, said, “Our new DefenseSSL capabilities support carriers and service providers in protecting themselves and their customers against HTTPS flood attacks even when they don’t have access to their tenants’ decryption keys. This unique capability eliminates the massive operational complexity that comes with managing decryption keys. Further, with this solution, enterprises have the flexibility to opt for the most suitable protection to match their needs. Enterprises that have access to decryption keys can still choose to use those keys to decrypt suspected traffic and increase the accuracy of their mitigation.”

Radware’s solution for keyless protection against HTTPS flood attacks is based on a stateless architecture. Traditional solutions are stateful and thus themselves vulnerable to DDoS attacks. With advanced behavioral algorithms and the combination of rate-based and non-rate-based parameters, Radware can identify DDoS attacks over encrypted traffic, even without inspection of the traffic’s content. Radware’s DefenseSSL functionality is currently available across its DefensePro advanced protection product suite.
Radware’s Global Application And Network Security Report Indicates Ave...

Radware, a provider of cybersecurity and application delivery solutions, announced it has released its 2018-2019 Global Application and Netw...

What Is The Role Of Ethical Hackers To Ensure Cybersecurity?

Ethical hackers are familiar to the world of cybersecurity. As cybersecurity awareness increases in physical security, they are also playing...

Four Emerging App Security Challenges Every CTO Needs To Know About

In the next three years, software as a service ‘SaaS’ is likely to grow by around 23%. That’s according to reports by Cogn...