Comprehensive SSL DDoS Attack Protection

Over 99% of internet traffic is now encrypted. Fraud, hacking activities and a long list of privacy regulations have caused organizations to use HTTPS and encrypted communication as a default communication method. The good news is that data is safer when encrypted. The bad news is that attacks are easily camouflaged when encrypted. Attackers use encrypted messages as an evasive technique so frontline network security tools (anti DoS/DDoS, firewall and IPS/IDS tools) are blind to the attack.

Considerations For Selecting An SSL Protection Solution

There is no one-size-fits-all solution for SSL protection. Each organization has its unique priorities, business needs, sensitivities and privacy issues. Organizations should ask themselves the following questions:

- Do they have access to the SSL certificate?
- If there is access to the certificate, where and when should the traffic be decrypted?
- Are their services overly sensitive to latency?
- Do they use content delivery networks (CDN) for their services?

DefenseSSL Solutions

Radware understands the considerations and challenges around SSL security and offers a comprehensive and flexible solution for all types of organizations and deployments.

KEYLESS SSL PROTECTION

Detects, characterizes and mitigates SSL attacks without requiring any SSL decryption. The algorithm learns and automatically creates a baseline during peacetime based on applicative traffic characteristics that go beyond the network layer.

FIRST REQUEST SSL PROTECTION

Detects and characterizes the suspicious sessions without decryption and applies decryption only under attack and only on the first request of every session to authenticate legitimate users.

SELECTIVE FULL SSL PROTECTION

Detects and characterizes the suspicious sessions of the attack without any decryption and then applies decryption only under attack and fully decrypts all suspicious sessions.

FULL SSL PROTECTION

Decrypts all SSL sessions towards a protected object and applies all protections on the cleartext traffic. A choice can be made to decrypt SSL traffic always, only under attack conditions or on-demand.

What DefenseSSL Solution Is Best For You?

DefenseSSL Solution	Best for
Keyless SSL Protection	▸ MSSPs ▸ Enterprises requiring protection with no access to certificates ▸ Organizations that are overly sensitive to latency
First Request SSL Protection	▸ Organizations that have strict requirements on latency ▸ Organization that prefer to minimize decryption operations at perimeter level ▸ MSSPs or cloud scrubbing services that have access to certificate only under attack
Selective Full SSL Protection	▸ Security teams (NOC/SOC) ▸ Organizations needing to mitigate attacks behind CDNs ▸ Organizations that have access to ingress traffic only
Full SSL Protection	▸ Enterprise data center protection with access to certificate and full two-way traffic visibility

Why Radware?

MAXIMUM FLEXIBILITY

Robust & tailor-made to match multiple defense strategies and not delivered as one-size-fits-all solution.

MINIMUM LATENCY

The perfect solutions for organizations with strict requirements on latency, wishing to open the certificate for security benefits.

UNIQUE KEYLESS PROTECTION

The only solution in the market to offer SSL attack detection, characterization and mitigation without requiring any SSL decryption.

BEHAVIORAL-BASED PROTECTION

Adaptive algorithms that learn and create baselines automatically during peacetime based on applicative traffic characteristics that go beyond the network layer.