USE CASE

Stop Application-layer Downtime with Adaptive Layer 7 DDoS Protection

The Scenario that Modern Organizations are Facing

An eCommerce business relies heavily on web applications and APIs to deliver services, enable customer engagement, and drive business transactions. However, the organization has begun experiencing occasional slowdowns, page timeouts, and even application downtime, heavily impacting their ability to generate revenue, and impacting user experience. One of the main causes could be Layer 7 (application-layer) DDoS attacks designed to appear as legitimate traffic while overwhelming backend systems and draining server resources.

Unlike traditional volumetric network-layer DDoS attacks, these attacks can be disguised in a variety of methods. For starters, Layer 7 DDoS attacks often appear like legitimate traffic, so the only way to examine if the traffic is malicious or not is to decrypt it, which is a very resource-intensive and expensive task. While innovations like cloud computing have made it possible to scale, it is costly and resource-intensive to decrypt all this traffic in real time. Layer 7 DDoS attacks can also be fragmented, in the sense that part of an attack is sent in one packet, and the other part of an attack is sent in another. When combined, they can become malicious, but separately, they each look like legitimate traffic. By mimicking user behavior and blending in with normal traffic, Layer 7 DDoS attacks can deplete application-layer resources while avoiding detection. Additionally, Layer 7 DDoS is often combined with other tactics to create multi-vector threats targeting APIs, credentials, or sensitive data. Because most existing security solutions operate in silos, they won't be able to correlate the data properly and stop attacks across differing vectors.

SECURITY SOLUTION

ThreatX, A Web Application Protection Platform

CRITICAL ISSUES

- **Performance Impact**: Slowdowns and downtime hurt revenue and user experience
- **Layer 7 DDoS Attacks**: Mimics real traffic, overwhelms backend systems, and evades detection
- **Detection Limits**: Decryption is costly; fragmented attacks appear legitimate

THREATX™
by A10 Networks

Without advanced detection and mitigation techniques, organizations will struggle to identify malicious traffic from normal traffic. The result is a sharp decline in resource availability, performance, brand reputation, customer experience, and even revenue generation.

Key Challenges

In-house SOCs usually lack integrated/comprehensive visibility and are too hamstrung to quickly prioritize crucial threats in the event of a flood of false positives

Advanced techniques, like fragmentation or slow-and-low, can deplete resources while making detection very difficult

Siloed defenses make complex, multi-vector L7 DDoS attacks more effective, especially when information from different attack vectors are not correlated

Potential Risks

The Risks of this Scenario

- **Application downtime** – Due to resource exhaustion and slowdowns, halting revenue, damaging brand reputation, and eroding customer trust.
- **Weaponizing the system against itself** – Without a streamlined approach of decryption and the ability to decrypt L7 traffic to inspection, the risk of successful L7 DDoS attacks greatly increases, raising the likelihood of downtime.
- **False positives** – Could block legitimate users, or allow malicious users, degrading customer experience, and introducing downtime.
- **Ineffective mitigation** – Because traditional methods like rate-limiting or stale block lists fail to stop more intelligent, dynamic, and adaptive DDoS attack methods; Stop-gap techniques like TCP progression tracking have limited visibility and result in a large amount of false positives.

How ThreatX by A10 Networks Secures Organizations

ThreatX by A10 Networks, a web application protection platform (WAPP), defends against sophisticated Layer 7 DDoS attacks by combining entity-based and transaction-based tracking to dynamically and intelligently perform threat mitigation.

Below are key techniques ThreatX uses to neutralize Layer 7 DDoS attacks.

- **Entity and transaction-based tracking** – Tracks users, bots, transactions, and attackers over time, correlating the data to find malicious patterns, behaviors, and entities.
- **Adaptive risk scoring** – The ThreatX decision engine, Hacker Mind, builds adaptive risk scores based on multiple points of data, enhancing blocking precision without introducing false positives.
- **Dynamic mitigation techniques** – Based on real-time risk levels from the ThreatX adaptive risk scoring, it intelligently flags, alerts, throttles, or downright blocks threats, minimizing strain on infrastructure.
- **Real-time selective decryption** – Traffic can be selectively decrypted based on profile, ensuring system resources are efficiently used for decryption.

Impact

By leveraging Layer 7 DDoS protection in ThreatX, organizations can maintain uptime by implementing real-time defense against one of the most evasive and resource-draining attack vectors.

L7 DDoS protection provides:

- Application uptime, even against multi-vector L7 DDoS attacks
- Scalable DDoS protection that decrypts traffic efficiently, so that it can stop large DDoS attacks without straining your organizations' existing infrastructure
- Minimized false positives, which reduces workload on the security team, and ensures access for legitimate users while stopping attackers
- Intelligent mitigation, with adaptive risk scoring, entity- and transaction-based tracking, and dynamic mitigation techniques
- Enhanced brand reputation by maintaining customer trust and uptime of digital services

With the L7 DDoS protection in ThreatX, security teams will be able to mitigate the most frequent attack vectors, before they start impacting customers and the organization's bottom line.

About A10

A10Networks.com

Contact Us
A10Networks.com/contact

Part Number: A10-CS-80255-EN-01 Aug 2025