Dispelling DDoS Myths

Block Unwanted Traffic at Every Level with F5 and AWS

Multi-layered DDoS protection from F5 and AWS keeps your applications secure and available to support your business. AWS provides secure and resilient services with several forms of DDoS mitigation built in. Protect against L3-L7 attacks in every environment, including AWS, with F5® Distributed Cloud DDoS Mitigation. With consistent cloud-based network perimeter security, you can simplify management and reduce costs.

Learn more at f5.com or find F5 Distributed Cloud Services on AWS Marketplace.

Distributed denial-of-service (DDoS) attacks have escalated in scale and sophistication, with one notable attack in 2023 reaching a peak of 120,000 requests per second. Attackers now leverage virtual private servers to create massive, high-performance botnets that overwhelm defenses and even extort ransoms from victims.

Are you prepared for today's sophisticated, hyper-volumetric attacks? Check your knowledge against these common DDoS myths.

Myth #1

Most DDoS attacks are at the network layer.

Truth: Application layer attacks are up by 165% and are now the largest single vector used in DDoS attacks.[2] Volumetric and multi-vector attacks have decreased, possibly because defenses against these more typical attack vectors have improved. DDoS protection now must cover from L3 to L7 to be effective.

Myth #2

A web application firewall (WAF) will stop L7 DDoS attacks.

Truth: While a WAF is an important solution in your security stack, DDoS protection can identify and block malicious traffic at L3/4 and L7 before it reaches your applications. A cloud-based DDoS mitigation solution can handle today's large and complex attacks on a global scale.

Myth #3

Distributed architectures are immune to DDoS attacks.

Truth: Modern multi-cloud environments, content delivery networks (CDNs), and distributed app architectures can reduce the impact of volumetric attacks, but without a DDoS mitigation solution, you're still at risk of performance degradation, outages, or increased costs. The massive scale of sophisticated botnets are capable of overwhelming distributed environments.

[1] F5, What's a Distributed Denial-of-Service Attack?
[2] F5 Labs, 2023 DDoS Attack Trends, February 2023

DC 12.2023 | JOB-CODE-1263869349

aws PARTNER