Defend, Adapt, and Mitigate Against Layer 7 DoS Attacks

Enhance Security, Automate Defense, and Accelerate Protection with NGINX

Distributed denial-of-service (DDoS) attacks continue to grow in size and complexity, with application-layer attacks up by 165% in 2022 over the previous two years. Threat actors use multi-vector attacks that include targeting the application layer (Layer 7) to maximize damage, knowing that even a short service interruption can cause revenue loss, reputational damage, and exposure to other types of attacks.

How can you protect your apps and APIs from hard-to-detect Layer 7 DDoS attacks across hybrid and multi-cloud environments?

NGINX makes it easy with NGINX App Protect DoS, which provides a configurable, robust, multi-layered defense for a comprehensive mitigation strategy. Running across distributed architectures and environments, it delivers adaptive and consistent protection.

With NGINX App Protect DoS you can:

- Implement a multi-layered DDoS defense strategy that includes blocking IP addresses of bad actors, blocking bad requests with attack signatures, and global rate limiting as needed
- Significantly reduce operating costs and false positives with machine learning-based algorithms which observe normal traffic patterns to establish a baseline, then detect anomalies and block malicious traffic without affecting legitimate traffic
- Protect HTTP/S and HTTP/2 apps – including gRPC and WebSocket – against various DDoS attacks including Slow POST, Slowloris, flood attacks, Challenger Collapsar, and more
- Continuously measure mitigation effectiveness with adaptive learning for no-touch policy configuration that enables cost-effective DDoS protection at scale
- Seamlessly integrate security posture config changes into DevOps environments to enable security-as-code as a Layer 7 DoS defense across platforms, architectures, and clouds
Implement Multi-Layered Defense
Mitigate against Layer 7 DoS attacks with comprehensive and adaptive protection:
- Track over 300 metrics of user and app behavior used to build a unique algorithm that reduces false positives
- Deploy dynamic signatures to automatically mitigate attacks
- Measure mitigation effectiveness and adapt to changing behavior or health conditions
- Use adaptive learning for no-touch policy configuration and protection from zero-day attacks

Mitigate DoS Attack Types
Protect against multiple types of sophisticated DoS attacks:
- Block GET and POST flood attacks which overwhelm the server with a high volume of requests
- Mitigate low and slow attacks which tie up resources, including Slowloris, Slow Read, and Slow POST
- Block Challenger Collapsar attacks which aim to exhaust targeted server resources
- Protect against targeted SSL/TLS attacks and ensure app uptime using signature mechanisms for mitigation based on the CLIENT HELLO message

Deploy Platform-Agnostic Protection
Enable DoS protection controls wherever NGINX Plus and NGINX Ingress Controller are deployed:
- Deploy DoS protection on the load balancer, API gateway, Ingress Controller, or per-pod/per-service proxies
- Achieve lightweight, high-performance, low-latency attack mitigation
- Easily integrate platform-agnostic protection into any architecture and across multi-cloud environments
- Reduce complexity and tool sprawl using the NGINX portfolio for single-vendor DoS mitigation

Automate Security for DevSecOps
Incorporate DoS attack mitigation into the software development lifecycle (SDLC):
- Apply consistent protection with declarative security policies created by SecOps and deployed by DevOps
- Automate security-as-code seamlessly into CI/CD pipelines for DevSecOps
- Enable cost-effective DDoS protection at scale with no-touch configuration
- Leverage easy policy integration via the Kubernetes API to keep developers agile

To learn more, visit nginx.com/dos