

Barracuda Active DDoS Prevention

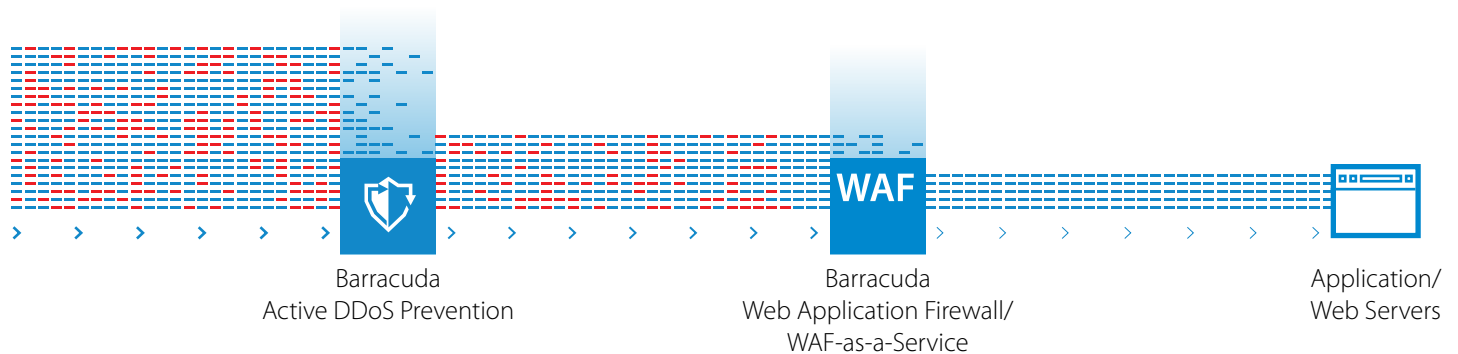


Always-On DDoS Protection That Identifies and Mitigates Attacks Before They Reach Your Network and Crash Your Apps

Businesses of all Sizes in Nearly Every Industry are Vulnerable to DDoS Attacks¹

Today's distributed denial-of-service (DDoS) attacks not only interrupt the availability of websites and applications, but also serve to distract security teams from even greater threats. Attackers combine a variety of attack types—including volumetric floods, stealthy application-targeted strikes, and role/authentication-type strategies—in hope of discovering vulnerabilities in an organization's defense.

Build a Comprehensive Attack Mitigation Strategy With Proactive, Always-On DDoS Defense



Cloud for Volumetric Defense

Can your network handle hundreds of gigabits per second? Volumetric attacks are sufficiently large enough to overflow most organizations inbound capacity. To defend against these attacks, incoming traffic is first re-routed through Barracuda's high-bandwidth data centers that scrub the traffic clean before returning it to Barracuda WAF or WAF-as-a-Service.

WAF for Layer 7 Defense

Sneaky application layer level DDoS attacks such as Slowloris can slow down apps for everyone. HTTP floods or heavy URL resource attacks, including complex database queries can quickly overwhelm applications. Technologies built into the Barracuda Web Application Firewall and WAF-as-a-Service mitigate the numerous application-layer and bot driven DDoS attacks.

¹ 2018 Verizon Data Breach Report

Complete Visibility. Complete Control.



Active DDoS Prevention

Volumetric DDoS attacks including:

- DNS Amplification Attacks
- TCP SYN Floods
- UDP / ICMP Floods
- FIN / RST Floods
- Network Protocol Abuse

Barracuda WAF/WAF-as-a-Service

Application DDoS attacks including:

- SlowLoris Attacks, RUDY, Slow Read
- Bot Detection
- GET Floods
- HTTP Cache Bypass Flood Mitigation
- SSL Floods
- SSL Protocol attacks

Seamless Integration

Add complete L3–L7 DDoS protection to any Barracuda WAF



- ✓ Delivered as high-performance hardware or virtual machines
- ✓ Comprehensive platform protects apps, and accelerates their availability
- ✓ Centralized management for enterprise-scale deployments



- ✓ Comprehensive protection with near-native experience
- ✓ Well-architected for public cloud eliminates deployment friction
- ✓ Fully-featured API enables dev-ops/sec-ops to automate security controls using familiar tools



- ✓ Deploy enterprise-proven security in minutes
- ✓ Cloud delivered with zero hardware to install or manage
- ✓ Complete control over building specific policies
- ✓ Industry leading SLA and support

Visit barracuda.com/WAF to learn more.