Making a DDoS Protection Plan

8 Best Practices

When a DDoS attack strikes, panic ensues. Having a DDoS mitigation plan in place will make the difference between hours or days of organization-wide chaos and an orderly and timely response that keeps business as usual. Follow these steps to develop a DDoS mitigation plan for your organization.

1 **Anticipate single points of failure.** DDoS attackers will target any potential point of failure, such as websites, web applications, application programming interfaces (APIs), domain name system (DNS) and origin servers, and data center and network infrastructure.

2 **Verify your ISP's capability to provide DDoS mitigation.** If a DDoS attack on your website puts your ISP's other customers at risk, the ISP will almost certainly blackhole (dump) your traffic — and your website will be down indefinitely. Ask your ISP:

- How large of a DDoS attack will you attempt to mitigate before you blackhole all traffic to the site? And what requirements will you have before restoring Internet service?
- How much available capacity do you have across your network, in excess of normal peak traffic?
- Can you decrypt TLS/SSL to inspect for application DDoS attacks encrypted in SSL sessions?
- If your network is hit with 10 Gbps of traffic from a reflection DDoS attack with hundreds of sources, how long will it take you to block it using an access control list (ACL)?

3 **Don't overestimate your infrastructure.** Your edge network hardware may serve you well in daily use but may fail rapidly during a DDoS attack, if the network edge has been under-resourced for a malicious event. A typical DDoS attack generates 0.5–4 Gbps, and peak DDoS traffic can exceed 600 Gbps.

4 **Identify what you need to protect and the business impact of its loss.** This may include websites, web applications, APIs, DNS and origin servers, and data center and network infrastructure. What business impact and operational, financial, regulatory, and reputational costs would you incur from their loss?

5 **Identify acceptable time to mitigation.** How quickly do you need your DDoS protection service activated? Some DDoS protection services are always on, and others are activated on demand, after a manual request or automated DDoS detection. There are two types of DDoS protection services:

- **CDN-based DDoS protection services** are always-on and instantaneous but they do not protect data centers or network infrastructure.
- **DDoS scrubbing services** are usually on-demand. Some organizations choose professional flow monitoring and a direct, high-bandwidth connection to make switchover so fast that there is little to no impact on site availability. Other organizations choose to identify a DDoS attack on their own and to activate the service manually.

6 **Deploy a DDoS protection service before you need it.** Talk to DDoS protection service providers before an attack, and select a service before you need it. Ask questions and prepare for all of the possible DDoS scenarios that your organization could experience.

7 **Develop a DDoS response runbook.** A DDoS runbook allows your organization to experience a controlled, streamlined response to an attack. The runbook should include incident response processes, escalation paths, points of contact, roles and responsibilities, and internal and external communications plans.

8 **Tabletop your DDoS runbook to ensure operational readiness.** An annual tabletop drill can review attack scenarios to help ensure the information in the runbook is documented properly, and escalation paths, best practices, and procedures are followed.

Learn about some of Akamai's Cloud Security Solutions

Kona Site Defender: Customizable CDN-based website protection service to secure brand-critical, revenue-generating, and performance-sensitive websites from DDoS and web application attacks.

DDoS and Application Protection: Learn how you can stay ahead of the changing threat landscape and be prepared for emerging attack vectors.

Web Application Protector: Powerfully simple CDN-based web application firewall and DDoS protection service to easily safeguard web assets while improving performance.

Prolexic Routed: Dedicated DDoS protection service with globally distributed scrubbing centers to secure your network and data center infrastructure against the broadest range of DDoS attacks.

Fast DNS: Cloud-based DNS service to protect against DDoS attacks and to improve performance. Optional DNSSEC support protects against DNS forgery and manipulations.

Akamai

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at www.akamai.com/locations. Published 09/17.