# 8 steps to creating a DDoS mitigation plan

When a Distributed Denial of Service (DDos) attack strikes, panic ensues. Having a DDoS mitigation plan in place can make the difference between hours or days of organizational 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 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.

## FIS™ Web Application Protection

FIS™ Web Application Protection (WAP) protects websites and applications from downtime and data theft caused by opportunistic and targeted web attacks, as well as (DDoS) attacks. DDoS-defense capabilities are always on, so traffic does not have to be re-routed before mitigation begins. Moreover, WAP visibility into 15-30% of the world's web traffic provides intelligence into the threat landscape that allows us to constantly evolve rules to thwart the latest attacks. WAP stops sources with poor reputation from accessing your web applications that may negatively impact performance and customer experience.  For more information, please reach out to **getinfo@fisglobal.com**.

## About FIS

FIS is a global leader in financial services technology, with a focus on retail and institutional banking, payments, asset and wealth management, risk and compliance, consulting and outsourcing solutions. Through the depth and breadth of our solutions portfolio, global capabilities and domain expertise, FIS serves more than 20,000 clients in over 130 countries. Headquartered in Jacksonville, Florida, FIS employs more than 53,000 people worldwide and holds leadership positions in payment processing, financial software and banking solutions. Providing software, services and outsourcing of the technology that empowers the financial world, FIS is a Fortune 500 company and is a member of Standard & Poor's 500® Index. For more information about FIS, visit **www.fisglobal.com**.

www.fisglobal.com

getinfo@fisglobal.com

twitter.com/fisglobal

linkedin.com/company/fisglobal