Table of Contents

What to Expect from a DDoS attack 1
   What to Expect under DDoS Attack: Panic 1
   How the DDoS Attack Landscape has Changed 1

8 Best Practices for Building and Maintaining a DDoS Protection Plan 2
   1. Anticipate these Single Points of Failure 2
   2. Verify your ISP’s Capability to Provide DDoS Protection 2
   3. Don’t Overestimate your Infrastructure 3
   4. Identify What you Need to Protect and the Business Impact of its Loss 3
   5. Identify Acceptable Time to Mitigation 3
   6. Deploy a DDoS Protection Service before you Need it 4
   7. Develop a DDoS Response Runbook 4
      Roles and Responsibilities of Key Personnel, and the Escalation Path 4
      Who to Contact and How to Contact Them 4
      How to Manage Internal Communications 4
      How to Manage Public Relations and Customer Relationships 4
      Plan Post-attack Reviews 5
      Keep the DDoS Runbook up to Date 5
   8. Tabletop your DDoS Runbook to Ensure Operational Readiness 5

Conclusion 5
What to Expect from a DDoS Attack

The impact of a distributed denial of service (DDoS) attack is easy to see – your websites and applications are unavailable or slow. Your call center lights up urgently with unhappy, frustrated customers. Your IT dashboards alert and indicate an ominous and confusing situation.

What to Expect under DDoS Attack: Panic

Panic ensues at unprepared organizations when a DDoS attack hits. IT teams scramble in an attempt to keep websites and applications available in the face of malicious actors and multiple attack vectors. As the attacker changes denial of service vectors to exploit different network vulnerabilities, IT personnel attempt to triage the unfolding situation and figure out why network anomalies are occurring, such as:

- Why are routers passing traffic, while load balancers are freezing?
- Why is the web server responding, but the database is not?
- Why is the database up, but the web server unresponsive?
- Why is traffic being deflected, when everything seems to be working?

Multiple people within the organization scurry to place calls to the Internet Service Provider (ISP) and application vendors, seeking an explanation and help, but no one really knows who to call first and what questions to ask. Meanwhile, senior managers want clear answers as to why operations have ground to a halt and when business as usual will resume. That’s when panic really sets in.

When a DDoS attack strikes, having a DDoS protection plan in place will make the difference between organization-wide panic and an orderly and timely response that keeps business as usual.

How the DDoS Attack Landscape has Changed

Organizations of all sizes with an Internet presence need to be concerned about cyberattacks. Attackers can target any components of your Internet-facing systems, such as:

- Website
- Web application
- API
- Domain name (DNS) server
- Origin server
- Data center and network infrastructure

DDoS attacks have changed over time. Some of the DDoS attack trends over the past year highlighted in Akamai’s State of the Internet / Security Report include the following:

- Internet of Things (IoT) devices\(^1\) are a source of massive botnet resources. Mirai malware and its progeny are evolving and spreading,\(^2\) and older malware is being updated\(^3\) to take advantage of the proliferation of insecure IoT devices.
- The largest DDoS attacks have doubled in size year-over-year, to exceed 600 gigabits per second (Gbps).\(^4\)
- Even a typical DDoS attack of less than 4 Gbps\(^5\) can cause denial of service at an unprotected site or one that relies upon on-premise DDoS mitigation hardware.
- DDoS attacks can be powerful with a duration of minutes or days, repeatedly target the same site (on average 32 attacks per victim per quarter\(^6\)), and cause chronic, low-level response degradation.
- The emergence of new DDoS attack vectors\(^7\) and new types of botnet malware infections\(^8\) are frequent.
- DDoS-for-hire services\(^9\) are readily available, and anyone – even without technical skills – can launch a damaging DDoS attack.
Many organizations include DDoS in a disaster recovery plan, but that is a mistake. Disaster implies an event that is unlikely and unavoidable. **Attackers deliberately launch hundreds of DDoS attacks every day.** DDoS attacks are common for many organizations.

Every organization that depends on its Internet-facing assets should have a DDoS protection plan. When fully prepared for a DDoS attack with **DDoS protection already in place**, and a **DDoS response runbook**, it is easy to respond effectively to DDoS incidents and quickly mitigate operational, financial, regulatory and reputational damage.

**Planning ahead and being prepared** is a best practice for business operations and your best defense against DDoS attacks.

---

**8 Best Practices for Building and Maintaining a DDoS Protection Plan**

If their initial efforts are blocked, DDoS attackers will typically change attack vectors or move on to easier targets. Think like an attacker. Consider all types of and targets of DDoS attacks, and fully understand your DDoS protection options. Develop and implement a DDoS protection plan that includes the following eight best practices to mitigate the business impact of DDoS attacks.

1. **Anticipate these Single Points of Failure**

DDoS attackers will target any potential point of failure, such as:

- **Domain Name System (DNS) Servers** – DNS infrastructure is a ripe target for malicious actors, because it provides a necessary service for end users’ browsers to look up your IP address and find your website. **Learn more about DNS attacks.**

- **Origin Server** – The servers that host your websites, web applications and web content are targets. Attackers can bypass your other protections if they can directly access your origin server, which may be in the cloud or in a data center.

- **Website** – Even a simple DDoS attack can flood an unprotected website with a high volume of requests that exceeds its capacity.

- **Web Application** – A web application can’t easily tell the difference between a DDoS attack and legitimate user requests. Login pages are often targeted, because they trigger back-end processes that consume CPU cycles on the web server, such as fraud prevention, database access, and authentication routines.

- **Application Programming Interfaces (APIs)** – APIs are being targeted more frequently, in part because more and more websites are enabling communications through APIs. APIs may feed information to mobile apps or pull content from third-party content sources into a web application.

- **Data Center & Network Infrastructure** – Network and data center infrastructure, and network bandwidth into a data center, are targets. If an attacker can fill your network pipes or overwhelm routers and switches, legitimate traffic can’t get through.

2. **Verify your ISP’s Capability to Provide DDoS Protection**

Your ISP may be your single point of failure. 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. Therefore, here are some questions to ask your ISP:

1. Have you ever **blackholed traffic to a customer site** under DDoS attack?

2. **What DDoS protection do you have in place?**

3. **Do you have the capability to decrypt TLS/SSL** to inspect for application DDoS attacks encrypted in SSL sessions?
4. How are you prepared for zero-day attacks and new attack vectors?

5. How much available capacity do you have across your network, in excess of normal peak traffic?

6. 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)?

7. How large of a DDoS attack will you attempt to mitigate before you decide to blackhole all traffic to that site?

8. If a customer’s traffic is blackholed due to a DDoS attack, what requirements do you have before you restore their Internet service?

Learn more about DDoS protection options and the importance of available capacity in the eBook, **Why Cloud: The Buyer’s Guide to Cloud Security**.

3. Don’t Overestimate your Infrastructure

Your current 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.

- Determine and ensure that your infrastructure has sufficient balance with headroom above and beyond legitimate peak requirements.
- Consider your tolerance for risk. A typical DDoS attack generates less than 4 Gbps, but peak DDoS traffic can exceed 600 Gbps.

4. Identify What you Need to Protect and the Business Impact of its Loss

Every organization’s needs are different. What Internet-facing assets do you need to protect from DDoS attacks? If you didn’t protect them and they became unavailable, what business impact and costs would you incur, including operational, financial, regulatory and reputational costs?

- Do you only care to protect your website? Web applications? APIs?
- How about your origin server? DNS servers?
- Can a business case be made to protect your data center and network infrastructure?

Knowing what you need to protect will affect the type of DDoS protection. Not all attacks target ports 80 and 443.

- Protecting a data center, network infrastructure and other non-website assets such as email servers requires a DDoS scrubbing network.
- A content delivery network (CDN) with DDoS mitigation and web application firewall capabilities can protect web assets, including websites, web applications, and APIs. A CDN can also protect origin servers, and primary and secondary DNS infrastructure.

5. Identify Acceptable Time to Mitigation

Some DDoS protection services are always on: you won’t even notice most DDoS attacks. Others are activated on demand: after a manual request or automated DDoS detection. How quickly do you need your DDoS protection service activated?

DDoS scrubbing services are usually on-demand – your network traffic is only routed through the scrubbing center when needed. With professional flow monitoring and a direct, high-bandwidth connection to the DDoS scrubbing network, the switchover can be so fast that the DDoS attack would have little to no impact on site availability. Other organizations choose to lower costs by relying on their own staff to identify a DDoS attack and to activate the scrubbing service manually. CDN-based DDoS protection services are always-on and instantaneous, but they only protect websites, not infrastructure. Vendors offer flexibility, so it is important to understand your business risk tolerance and use this to guide your architectural choices.
6. Deploy a DDoS Protection Service before you Need it

Select a DDoS protection service before you need it. Avoiding the chaos, delays and panic of looking for DDoS protection when under attack has several additional advantages:

- **Have time to choose the best solution.** Your DDoS protection provider can explain the approaches to DDoS protection that would meet your specific needs. They can look for gaps to ensure you are fully protected.
- **Know who to call and what to do.** Develop a relationship with your DDoS protection provider and know what to do and whom to call when under attack.
- **Get ready for DDoS protection.** Lay the groundwork and set up your DDoS protection service. For example, setting DNS time-to-live (TTL) to a short duration will speed time to mitigation when routing traffic to a scrubbing service.
- **Test and optimize:** Work with your DDoS protection provider to test and validate your DDoS scrubbing service. Test the process, ensure that your applications continue to work as expected, and optimize settings.

7. Develop a DDoS Response Runbook

A DDoS response runbook (also called a playbook) allows your organization to experience a controlled, streamlined response to a DDoS attack.

- If you choose on-demand mitigation with manual activation, your organization needs to know what to look for, what to do, and whom to call in order to activate the DDoS service.
- If you have an always-on or automatically triggered DDoS protection service, your organization needs to know how to respond if hit by a **zero-day attack** or a DDoS attack that targets an **unanticipated failure point** for which your organization is unprotected.

A DDoS response runbook should include incident response processes, escalation paths, and points of contact including:

**Roles and Responsibilities of Key Personnel, and the Escalation Path**

Identify what decisions and actions need to be taken and who is responsible. Include members of the IT team, application owners in each line of business, customer service, communications teams, and executives, among others. Include any special details of your configuration. Identify the communication channels that will be opened and who will participate.

DDoS attacks impact much more than IT. In order to minimize business disruption, include step-by-step roles and responsibilities of every department across your organization.

**Who to Contact and How to Contact Them**

Storing in one place all the names and phone numbers of key contacts – in your organization and at the DDoS protection provider – can save valuable time.

**How to Manage Internal Communications**

Help company employees and key partners understand what is going on during the attack so that they don’t panic and create an additional internal crisis. Have a single point of contact for relaying information and prepare confidential, short Twitter-style updates for use across the organization.

**How to Manage Public Relations and Customer Relationships**

If the DDoS attack affects partners, customers or the public, consider how your organization will respond to them, and to the media.
Plan Post-attack Reviews
Your organization can learn from every attack. Have a post-attack review process.

Keep the DDoS Runbook up to Date
Review and update the runbook procedures and points of contact frequently – at least quarterly.

8. Tabletop your DDoS Runbook to Ensure Operational Readiness
The best way to determine operational readiness is through testing and a simulated DDoS attack. An annual tabletop drill can review various attack scenarios with the goal of ensuring that escalation paths, best practices, and procedures will be followed. It can also validate that the information in the runbook is properly documented and current.

Conclusion
Emergency DDoS mitigation can be deployed within an hour in typical cases, but that will be after an unprepared organization has accumulated hours or days of downtime and chaos. The best way to avoid DDoS downtime is to implement a DDoS protection plan before your organization is targeted by a DDoS attack.

Be prepared is a classic motto that is relevant for an online organization in a world where DDoS and web attacks pose a pervasive threat. You need robust, intelligent and easy-to-use solutions to keep your infrastructure, data, applications and APIs safe, without overtaxing internal resources.

Akamai advises security leaders and IT management to talk to DDoS protection service providers before an attack. Ask questions and discuss all of the possible DDoS scenarios that your organization could experience. Implement a solution and understand how to use the vendor’s DDoS protection services to your best advantage. Prepare a DDoS response runbook and test it.

With DDoS protection planning, instead of panic and chaos, your DDoS experience can be business as usual, as experienced by these organizations:

- An international commercial bank with 50,000 member logins per day identified its DDoS protection requirements, implemented Akamai Cloud Security Solutions, tested the system, prepared a DDoS mitigation runbook, and made modifications to its existing incident response plan. When later targeted by DDoS attacks against its DNS infrastructure, the attacks were mitigated and did not affect the bank’s services. Read the case study on Akamai.com

- A government agency planning a crowd-sourced bug bounty program engaged Akamai in advance to thwart Internet-based attacks and to ensure the availability of the sites it offered up for vulnerability testing. During the hackathon, Akamai denied more than 19 million malicious requests and a DDoS attack originating from IP addresses in 83 countries without site interruption. Read the case study on Akamai.com

Sources

1) Q3 2016, Section 2.3
2) Q2 2017, Section 4.2
3) Q4 2016, Section 2.3
4) Q3 2016, Section 2.3
5) Q1 2017, Section 1.0
6) Q2 2017, Section 2.0
7) Q1 2017, Section 2.3
8) Q2 2017, Section 2.5
9) Q2 2016, Section 2.9