5 Steps to Protecting Your Organization from a DDoS Attack

Introduction

Distributed denial of service (DDoS) attacks flood the network with malicious traffic, impacting the availability of applications and preventing legitimate users from accessing business-critical services. Today's sophisticated DDoS attacks frequently result in lost sales, abandoned shopping carts, damage to reputation and brand, and dissatisfied customers. The motivations for DDoS attacks vary widely from hacktivism to cybercrime to espionage. Given the sophistication and determination of today's attackers, chances are that your organization will eventually suffer a damaging DDoS attack.

Fortunately, with proper planning and proactive deployment of a scalable DDoS protection solution, there is a great deal that can be done to reduce the risk and potential impact of a DDoS attack. While there's no way to predict when an attack will happen, following the steps outlined in this guide will allow you to minimize the impact of the attack, recover quickly, and ensure it doesn't happen again.

1 Map vulnerable assets

The ancient Greeks said that knowing thyself is the beginning of wisdom. The same logic applies to protection against DDoS attacks.

The first step to securing your assets against a DDoS attack is to know which assets are most at risk. Begin by listing all external-facing assets that could be attacked. This list should include both physical and virtual assets:

- Physical locations and offices
- Data centers
- Servers
- Applications
- IP addresses and subnets
- Domains, subdomains, and specific FQDNs

Mapping external-facing assets will help you construct a threat surface and identify points of vulnerability.

2 Assess risk

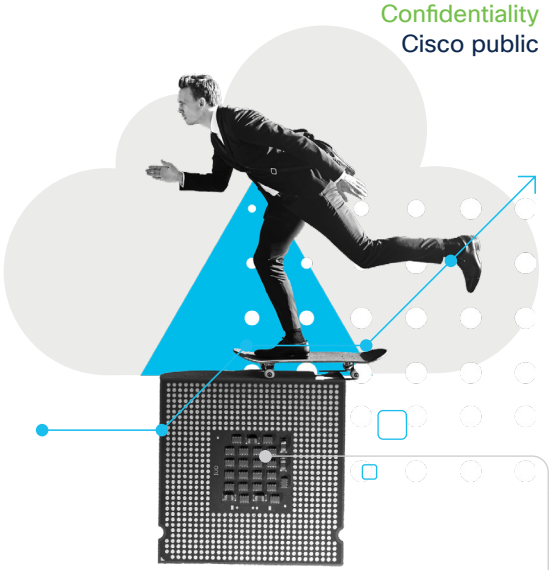
Determine the value of each asset and allocate appropriate budget and resources for protection. Keep in mind that some damages are direct, while others may be indirect. Some of the potential damages that can result from a DDoS attack include:

Direct loss of revenue – If your website or applications are generating revenue, any loss of availability will cause a direct loss of revenue. For example, if your website generates $1 million a day, then every hour of downtime, on average, will cause over $40,000 in damages.

Loss of productivity – For organizations that rely on online services, such as email, scheduling, storage, CRM, or databases, any loss of availability to any of these services will directly result in loss of productivity.

SLA obligations – For applications and services that are bound by service commitments, any downtime can lead to breach of SLA, resulting in refunding customers for lost services, granting service credits, and even potentially facing lawsuits.

Damage to brand and reputation – Availability and the digital experience are increasingly tied to a company's brand. Any loss of availability as a result of a cyber attack can directly impact a company's brand and reputation. Damage to brand is often hard to calculate, and it can take years to rebuild brand equity.



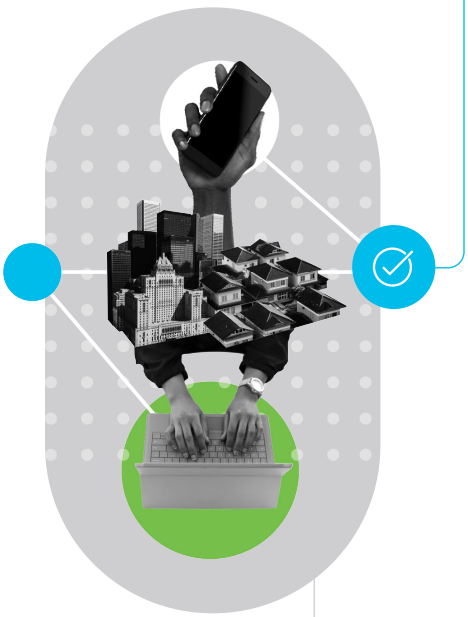
Loss of customers – One of the biggest potential impacts of a successful DDoS attack is loss of customers. This includes both customers who are unable to reach your website during an attack and customers who choose to stop doing business with you as a result of a cyber attack.

When evaluating the potential damage of a DDoS attack, assess vulnerable assets individually. A DDoS attack against a customer-facing e-commerce site will have a different impact than an attack against a field office.

Example: A large car brand evaluated the potential impact of their "brochure" website being unavailable for a few hours and determined this to be an acceptable loss. Much of the information was available from other online resources, and the reputational/brand risk was minimal. However, the potential loss of their financial services infrastructure and the ability to process customer loan applications was deemed unacceptable, since this would potentially result in millions in lost revenue per hour.

After you assess the risk to each asset, prioritize them according to risk and potential damages. This allows you to prioritize protection and determine which type of protection is required.

3 Assign responsibility



After a monetary value is defined for each asset, determine who is responsible for protecting them from a DDoS attack.

- Is DDoS protection the responsibility of the network administrator since it affects network performance?
- Is it the responsibility of application owners since it impacts application availability?
- Is it the responsibility of the business manager since it affects revenue?
- Is it the responsibility of the CISO because it is a type of cyber attack?

A surprising number of organizations don't have defined areas of responsibility regarding DDoS protection. This often results in exposed assets because DDoS defenses "fall between the cracks."

4 Set up detection mechanisms

Once you've evaluated which assets require protection and assign responsibility, next establish detection and alert protocols within your organization. After all, you don't want your customers – or worse, your boss – to be the ones to tell you that your services and applications are offline.

Detection measures can be deployed either at the network or application level. Make sure these measures are configured so that they don't just detect attacks, but also alert you when something bad happens.

5 Deploy effective DDoS protection

Finally, after you've assessed your vulnerabilities and costs and established attack detection mechanisms, it's time to evaluate how best to protect your organization from attack. Obviously, this step is best accomplished before you are attacked.

DDoS protection is not a one-size-fits-all proposition. There are many types of protection available and multiple deployment options based on the needs of the business and the characteristics, risk, and value of the assets being protected.

DDoS deployment options:

- **On-demand cloud DDoS mitigation services** are activated only after an attack is detected. On-demand cloud DDoS is the lowest cost solution and requires the least overhead. However, traffic must be diverted for protection to be activated. As a result, on-demand cloud DDoS is best suited for cost-sensitive customers, for business services that are not mission critical, and for customers who have never been (or are infrequently) attacked, but want a basic DDoS protection.
- **Always-on cloud services** always route all traffic through a cloud scrubbing center. No diversion is required, but there is minor added latency. This type of protection is best for mission-critical applications that cannot afford any downtime and organizations that are frequently attacked or are concerned about being attacked.
- **Hardware-based, on-premises DDoS appliances** provide advanced capabilities and fast response times. However, an on-premises appliance alone (i.e., no cloud-based mitigation) may have capacity limitations and have difficulty scaling to handle a large "volumetric" DDoS attack. On-premises appliances are best suited to service providers who are building their own scrubbing capabilities or in combination with a cloud service.
- **Hybrid (on-premises + cloud) DDoS protection** combines the scalability of cloud services with the advanced capabilities and fast response times of hardware-based appliances. Hybrid protection is best for mission-critical and latency-sensitive services that require protection against volumetric, application-layer, and encrypted traffic attacks and cannot afford any downtime at all.

Cisco offers advanced DDoS solutions that protect networks from malicious attacks and ensure network resilience and application availability. To learn more, see our Cisco Secure DDoS Protection At-A-Glance at https://www.cisco.com/c/en/us/products/collateral/security/secure-ddos-protect-aag.html

Contact your Cisco sales representative today to learn more about Cisco® Secure DDoS Protection.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.