 

“AZƏRBAYCAN HAVA YOLLARI” CJSC NATIONAL AVIATION ACADEMY”

**Topic:** DDOS prevention. Cloudflare

**Subject:** Operating system

**Teacher:** Sahmaliyev Memmed

**Student:** Aliyeva Qumru

**Group:** 2450-I

**Date:** 19.11.22

**Signature:**

**Baku 2022**

***DDOS prevention. Cloudflare***

A DDoS attack enables a hacker to flood a network or server with bogus traffic. Too much traffic overloads resources and disrupts connectivity, stopping the system from processing genuine user requests. Services become unavailable, and the target company suffers prolonged downtime, lost revenue, and dissatisfied customers.

This article explains how a business can prevent DDoS attacks and stay a step ahead of would-be hackers. The practices we show below help minimize the impact of a DDoS and ensure a quick recovery from an attack attempt.

What Is a DDoS Attack?

A DDoS (Distributed Denial of Service) is a cyberattack that aims to crash a network, service, or server by flooding the system with fake traffic. The sudden spike in messages, connection requests, or packets overwhelms the target's infrastructure and causes the system to slow down or crash.

While some hackers use DDoS attacks to blackmail a business into paying a ransom (similar to ransomware), more common motives behind a DDoS are to:

Disrupt services or communications.

Inflict brand damage.

Gain a business advantage while a competitor's website is down.

Distract the incident response team.

DDoS attacks are a danger to businesses of all sizes, from Fortune 500 companies to small e-retailers. Statistically, DDoS hackers most often target:

* Online retailers.
* IT service providers.
* Financial and fintech companies.
* Government entities.
* Online gaming and gambling companies.

Attackers typically use a botnet to cause a DDoS. A botnet is a linked network of malware-infected computers, mobile devices, and IoT gadgets under the attacker's control. Hackers use these "zombie" devices to send excessive numbers of requests to a target website or server's IP address.

Once the botnet sends enough requests, online services (emails, websites, web apps, etc.) slow down or fail. According to a Radware report, these are the average lengths of a DDoS attack:

33% keep services unavailable for an hour.

60% last less than a full day.

15% last for a month.

While a DDoS typically does not directly lead to a data breach or leakage, the victim spends time and money getting services back online. Loss of business, abandoned shopping carts, frustrated users, and reputational harm are usual consequences of failing to prevent DDoS attacks.

***Types of DDoS Attacks***

While all DDoS attacks aim to overwhelm a system with too much activity, hackers have different strategies they rely on to cause a distributed denial of service.

The three main types of attack are:

* Application-layer attacks.
* Protocol attacks.
* Volumetric attacks.

The three approaches rely on different techniques, but a skilled hacker can employ all three strategies to overwhelm a single target.

All pNAP servers come with DDoS protection at no additional cost. Stay online 24/7 with our automated traffic filtering and lightning-fast DDoS mitigation infrastructure.

Application-Layer Attacks

An application-layer attack targets and disrupts a specific app, not an entire network. A hacker generates a high number of HTTP requests that exhaust the target server's ability to respond.

Cybersecurity specialists measure app-layer attacks in requests per second (RPS). Common targets of these attacks include:

Web apps.

Internet-connected apps.

Cloud services.

Trying to prevent DDoS attacks of this type is challenging as security teams often struggle to distinguish between legitimate and malicious HTTP requests. These attacks use fewer resources than other DDoS strategies, and some hackers can even use only a single device to orchestrate an application-layer attack.

Another common name for an app-level DDoS is a layer 7 attack.

Protocol Attacks

Protocol DDoS attacks (or network-layer attacks) exploit weaknesses in the protocols or procedures that govern internet communications. While an app-level DDoS targets a specific app, the goal of a protocol attack is to slow down the entire network.

The two most common types of protocol-based DDoS attacks are:

SYN floods: This attack exploits the TCP handshake procedure. An attacker sends TCP requests with fake IP addresses to the target. The target system responds and waits for the sender to confirm the handshake. As the attacker never sends the response to complete the handshake, the incomplete processes pile up and eventually crash the server.

Smurf DDoS: A hacker uses malware to create a network packet attached to a false IP address (spoofing). The package contains an ICMP ping message that asks the network to send back a reply. The hacker sends the responses (echos) back to the network IP address again, creating an infinite loop that eventually crashes the system.

Cybersecurity experts measure protocol attacks in packets per second (PPS) or bits per second (BPS). The main reason why protocol DDoS is so widespread is that these attacks can easily bypass poorly configured firewalls.

Volumetric Attacks

A volume-based DDoS attack consumes a target's available bandwidth with false data requests and creates network congestion. The attacker's traffic blocks legitimate users from accessing services, preventing traffic from flowing in or out.

The most common types of volumetric DDoS attack types are:

UDP floods: These attacks allow a hacker to overwhelm ports on the target host with IP packets containing the stateless UDP protocol.

DNS amplification (or DNS reflection): This attack redirects high amounts of DNS requests to the target's IP address.

ICMP flood: This strategy uses ICMP false error requests to overload the network's bandwidth.

All volumetric attacks rely on botnets. Hackers use armies of malware-infected devices to cause traffic spikes and use up all available bandwidth. Volumetric attacks are the most common type of DDoS.

10 ways to prevent a DDoS attack

1. Know your network’s traffic

Every organization’s infrastructure has typical Internet traffic patterns — know yours. When you understand your organization’s normal traffic pattern, you’ll have a baseline. That way, when unusual activity occurs, you can identify the symptoms of a DDoS attack.

2. Create a Denial-of-Service Response Plan

Do you know what will happen when and if a DDoS attack happens? How will your organization respond? By defining a plan in advance, you’ll be able to respond quickly and efficiently when your network is targeted.

This can take some planning; the more complex your infrastructure, the more detailed your DDoS response plan will be. Regardless of your company’s size, however, your plan should include the following:

A systems checklist

A trained response team

Well-defined notification and escalation procedures.

A list of internal and external contacts that should be informed about the attack

A communication plan for all other stakeholders, like customers, or vendors

3. Make your network resilient

Your infrastructure should be as resilient as possible against DDoS attacks. That means more than firewalls because some DDoS attacks target firewalls. Instead consider making sure you’re not keeping all your eggs in the same basket — put data centers on different networks, make sure that not all your data centers are in the same physical location, put servers in different data centers, and be sure that there aren’t places where traffic bottlenecks in your network.

4. Practice good cyber hygiene

It goes without saying that your users should be engaging in best security practices, including changing passwords, secure authentication practices, knowing to avoid phishing attacks, and so on. The less user error your organization demonstrates, the safer you’ll be, even if there’s an attack.

5. Scale up your bandwidth

If DDoS is creating a traffic jam in your network, one way to make that traffic jam less severe is to widen the highway. By adding more bandwidth, your organization will be able to absorb more to absorb a larger volume of traffic. This solution won’t stop all DDoS attacks, however. The size of volumetric DDoS attacks is increasing; in 2018, for example, a DDoS attack topped 1 Tbps in size for the first time. That was a record… until a few days later, when a 1.7 Tbps attack occurred.

6. Take advantage of anti-DDoS hardware and software

DDoS attacks have been around for a while and some kinds of attacks are very common. There are plenty of products that are prepared to repel or mitigate certain protocol and application attacks, for example. Take advantage of those tools.

7. Move to the cloud

While this won’t eliminate DDoS attacks, moving to the cloud can mitigate attacks. The cloud has more bandwidth than on-premise resources, for example, and the nature of the cloud means many servers are not located in the same place.

8. Know the symptoms of an attack

Your network slows down inexplicably. The website shuts down. All of a sudden, you’re getting a lot of spam. These can all be signs of a DDoS attack. If so, the organization should investigate.

9. Outsource your DDoS protection

Some companies offer DDoS-as-a-Service. Some of these companies specialize in scaling resources to respond to an attack, others bolster defenses, and still, others mitigate the damage of an ongoing attack.

10. Monitor for unusual activity

Once you know your typical activity and the signs of an attack, monitor your network for odd traffic. By monitoring traffic in real-time, your organization will be able to spot a DDoS attack when it starts and mitigate it.

Cloudflare is on a mission to help build a better Internet.

Cloudflare is one of the world’s largest networks. Today, businesses, non-profits, bloggers, and anyone with an Internet presence boast faster, more secure websites and apps thanks to Cloudflare.

Cloudflare network map

Millions of Internet properties are on Cloudflare, and our network is growing by tens of thousands each day. Cloudflare powers Internet requests for millions of websites and serves 39 million HTTP requests per second on average.

Here’s how it works:

In the early days of the Internet, when you wanted to load a website, your request would go from your computer to a server, which would then return the web page you requested.

Connection Between Computer And Server

If too many requests came in at once, that server could be overwhelmed and crash, becoming unresponsive to anyone trying to access the resources it hosted.

Overwhelmed server

This made it difficult for owners of Internet properties to provide content that was fast, safe, and reliable. Cloudflare was created to ease these difficulties and empower users with the resources to make their sites, apps, and blogs safe and performant. This is done through the use of a powerful edge network that provides content and other services as close to you as possible, so you get the information as fast as possible.

Website with Cloudflare

You see, Einstein figured out some time ago that the speed of light is a hard upper limit on how fast you can communicate; there comes a point when the only thing you can do is move the content and computation closer! That’s why we put data centers in more than 275 cities all across the world: to give you what you’re looking for quickly!

Einstein's speed of light

Cloudflare also provides security by protecting Internet properties from malicious activity like DDoS attacks, malicious bots, and other nefarious intrusions.

Cloudflare protection

And allows website owners to easily insert applications into their websites without needing to be a developer.

Application being dropped onto a website using Cloudflare

If you’re a developer, we allow you to run Javascript code on our powerful edge network, so that you can get as close to a user as possible. This eliminates delays, and improves the experience for users like you!

Hello world

We provide security and performance for millions of Internet properties and offer great functionality such as SSL and content distribution to every website on our network.

Our services run silently in the background, keeping many of the websites and services you depend on up and running.

Your Internet provider, and anyone else listening in on the Internet, can see every site you visit and every app you use — even if their content is encrypted. Cloudflare offers a free DNS service called 1.1.1.1 that you can use on any device. Cloudflare’s 1.1.1.1 protects your data from being analysed or used for targeting you with ads.

Above all, we are mission-driven. That’s why we protect organizations working on behalf of the arts, human rights, civil society, or democracy with Project Galileo, giving them Cloudflare’s highest level of protection for free.