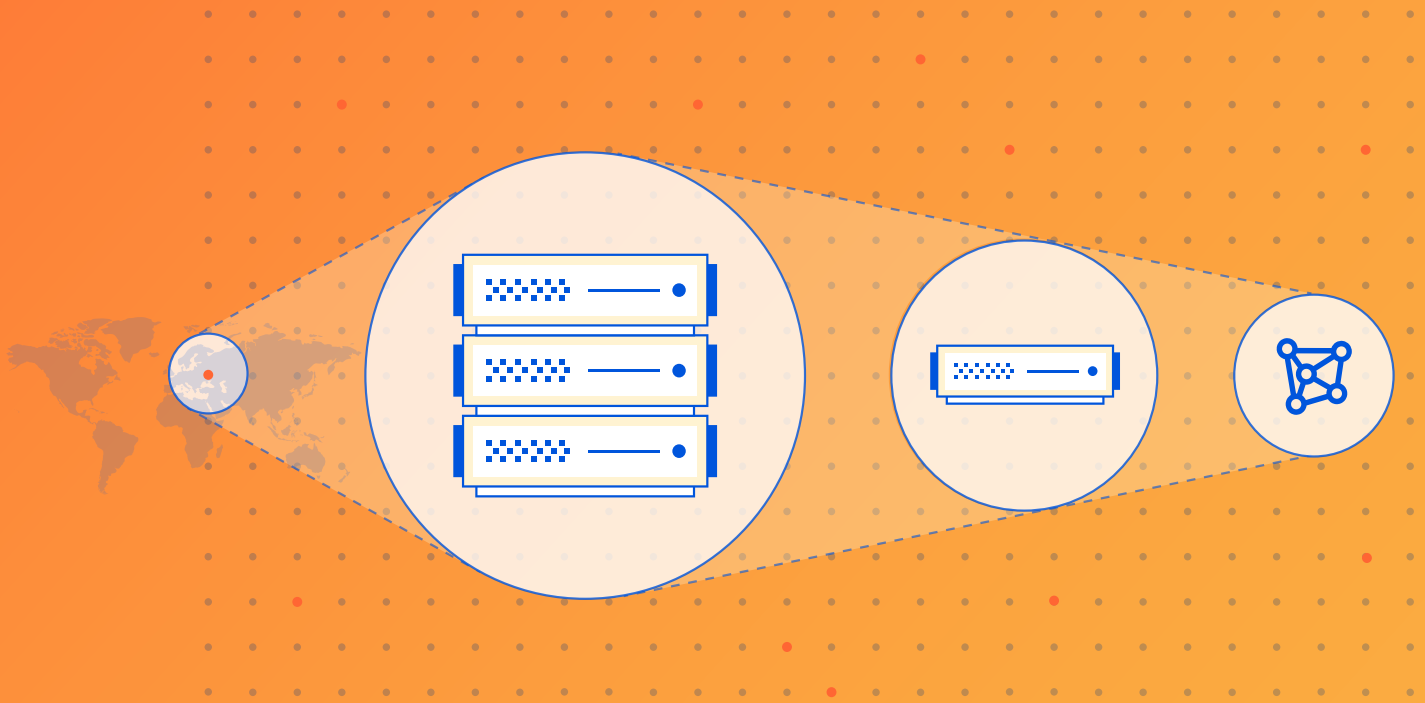
CLOUDFLARE

WHITEPAPER

DNS and the Threat of DDoS



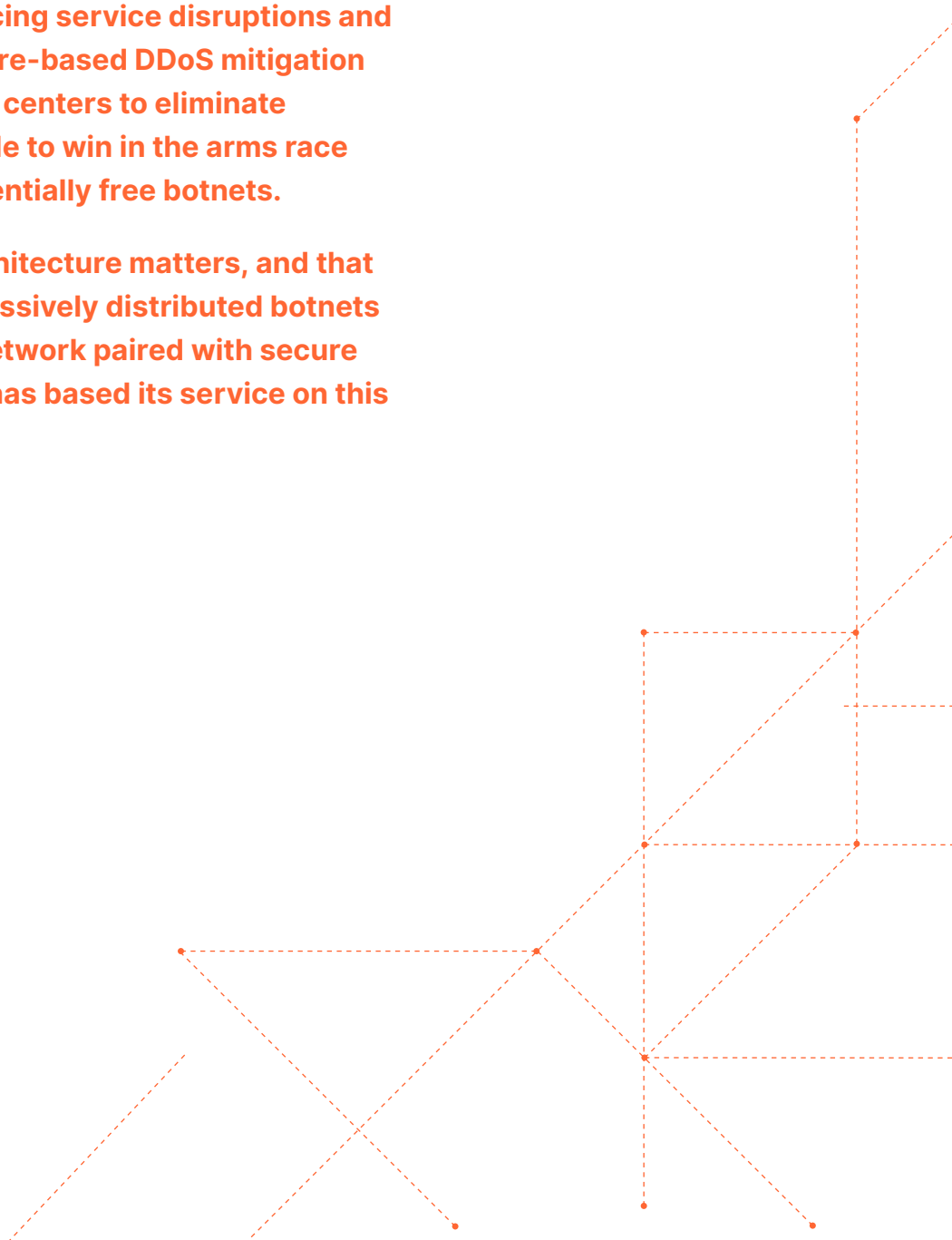
Content

Executive Summary

The Domain Name System (DNS) was one of the major innovations that made the Internet possible. But today, massive botnets are being used to stage ever-larger cyber attacks using, and targeting, DNS infrastructure.

In recent years, attackers have been able to take down essential services and huge patches of the Internet using large distributed denial-of-service (DDoS) attacks against DNS, with a large number of high-profile sites and organizations experiencing service disruptions and outages. Traditional hardware-based DDoS mitigation services that use scrubbing centers to eliminate malicious traffic cannot scale to win in the arms race against distributed and essentially free botnets.

Cloudflare believes that architecture matters, and that the only solution against massively distributed botnets is a massively distributed network paired with secure DNS resolution. Cloudflare has based its service on this architectural approach.



Large, growing attacks pose a new degree of threat to DNS

On October 21, 2016, a massive and sustained distributed denial-of-service (DDoS) attack impacted huge parts of the Internet, interrupting or bringing down dozens of high-profile websites and services. The direct target of the attack was Dyn, a DNS service provider, which maps domain names to their Internet Protocol (IP) addresses so that traffic can be routed to a specific site. The attack took hours to mitigate.[1]

But that was just the beginning of a growing wave of extremely large DDoS attacks. In the years since, attacks have increased in scale and scope, culminating in some of the biggest cyber attacks on record. AWS reported mitigating a massive DDoS attack in February of 2020. At its peak, this attack saw incoming traffic at a rate of 2.3 terabits per second (Tbps).[2] And In June 2022, Cloudflare mitigated a 26 million request per second DDoS attack — the largest HTTPS DDoS attack on record to that point.[3]

How are attackers able to scale up their attacks to these heights?

Massive IoT-based and server-based botnets

One major way that large attacks are generated is through taking over poorly protected Internet of Things (IoT) devices. The Mirai botnet is perhaps the highest-profile example of a network of IoT devices exploited for malicious purposes. The creators of Mirai compromised over 100,000 connected devices, such as home routers, smart home gadgets, security cameras, or video recorders, to create a huge botnet, which was used to launch the Dyn attack (among others) with potentially as much as 1.2 Tbps of traffic.

This massive botnet overwhelmed Dyn, which shut down DNS resolution for all the websites and applications relying on it.

> **"Assuming a device is publicly accessible, the chance of being hacked is probably 100 percent. The IPv4 address space just isn't that big. You can now run a scan across that entire space in hours, especially if you have a big botnet. The scans for vulnerability are continuous, and if anything, have accelerated over the last couple of years."**
>
> - Matthew Prince, CEO of Cloudflare

The botnet was created using a malware called Mirai. Mirai scans the Internet for devices that still have the factory-default username and password settings, making it easy to then infect it, log in, and take control of the device. The owner of the devices will not notice that the device was compromised, other than occasional sluggish performance.

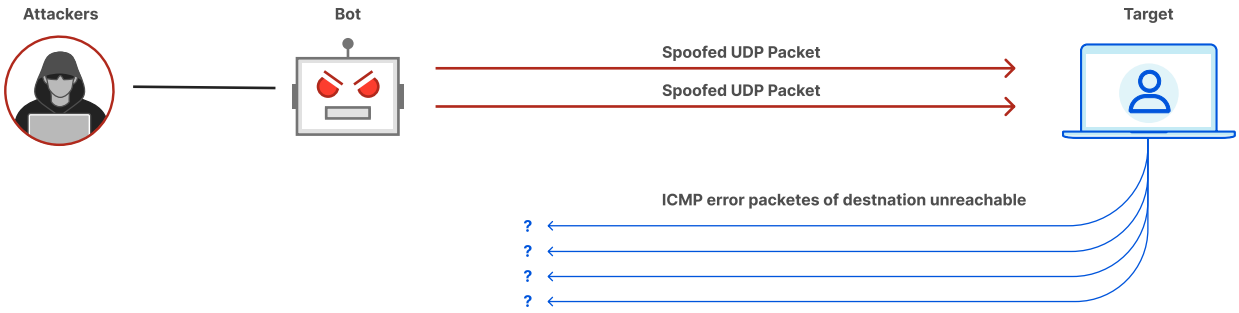
The Mirai botnet, which is still a threat today, is far from the only one that is actively used in DDoS attacks:

- The **Meris botnet** was first detected in June 2021. While researchers identified at least 30,000 bots within the botnet, the actual number of bots is believed to be much higher.[4]
- The **Mantis botnet** uses hijacked virtual machines and powerful servers instead of IoT devices. This means that each bot has far more computational resources than the devices in Mirai or Meris. The botnet is able to create massive DDoS attacks, as large as 26 million requests per second in some cases.[5]

The two most common methods for exploiting how DNS works are DNS amplification (or "reflection") attacks and UDP flood attacks.

Overwhelming DNS servers: UDP floods

UDP flood attacks send a large number of UDP packets to a targeted server with the aim of overwhelming that device's ability to process and respond. The firewall protecting the targeted server can also become exhausted as a result of UDP flooding, resulting in a denial-of-service to legitimate traffic.



Such attacks are particularly relevant to DNS resolvers, since all DNS traffic is generally sent over UDP (not TCP is only used in some specific use cases like zone transfers). Because UDP requires no handshake to open a connection, large volumes of junk UDP packets can be sent to the target, which will then do its best to respond to each one. (The Mirai attack on Dyn, for example, was a UDP flood attack — when such attacks target DNS, they may be called a "DNS flood".)

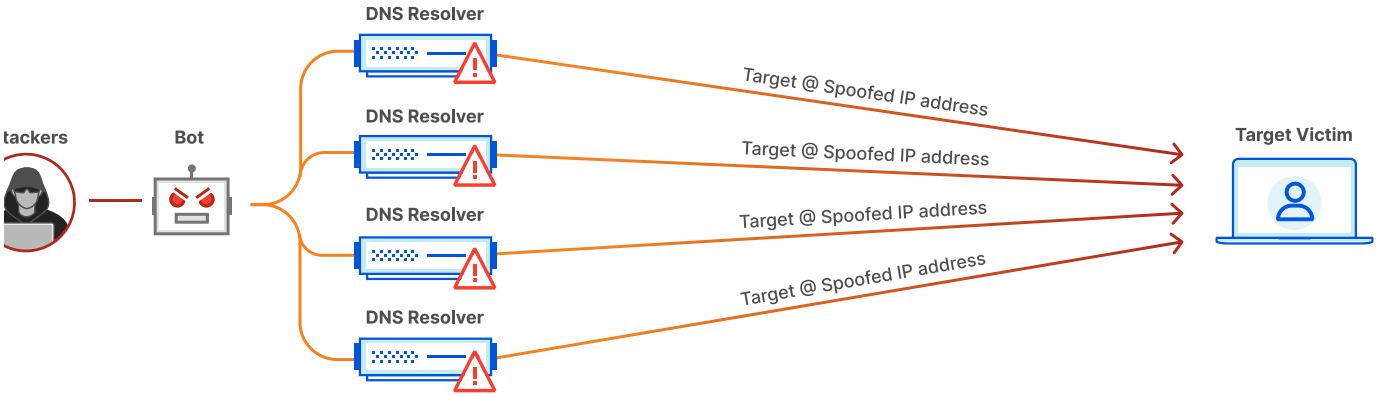
A UDP flood works primarily by exploiting the steps that a server takes when it responds to a UDP packet sent to one of its ports. If no programs are receiving packets at that port, the server responds with a ICMP (ping) packet to inform the sender that the destination was unreachable. As each new UDP packet is received by the server, it goes through steps in order to process the request, utilizing server resources in the process. As a result of the targeted server utilizing resources to check and then respond to each received UDP packet, the target's resources can become quickly exhausted when a large flood of UDP packets are received.

Exploiting how DNS works: DNS amplification

In addition to targeting DNS service providers directly, attackers can also weaponize their infrastructure and use the way DNS works to conduct crippling DDoS attacks to target others.

DNS amplification attacks leverage the functionality of open DNS resolvers in order to overwhelm a target server or network with an amplified amount of traffic. Instead of targeting the victim directly, each bot in the attack sends requests to open DNS resolvers with a spoofed IP address, which has been changed to the real source IP address of the targeted victim. The target then receives a response from the DNS resolvers.

The attacker structures the request in a way that generates as large a response from the DNS resolvers as possible. As a result, the target receives an amplification of the attacker's initial traffic. The Cybersecurity & Infrastructure Security Agency (CISA) estimates that DNS amplification attacks can allow an attacker to send traffic up to 54 times the bandwidth of the spoofed packets they sent.[6]



DNS amplification was a crucial piece of the 2013 attack that knocked Spamhaus offline,[7] and has been used in many other attacks in the wild as well.

While DNS resolvers are not directly responsible for these attacks, such exploitation of their systems can and should be prevented. Organizations with self-hosted DNS may also find their system working against them to take down their internal networks.

The impacts of large DDoS attacks on DNS resolvers and downstream victims

Organizations that have experienced DDoS attacks are well aware of their far-reaching negative impacts, which include downtime, lost business, reputational damage, and heavy financial burdens. One source found that on average, the total cost of a DDoS attack for enterprises was $2 million, and the cost of a DDoS attack for small and medium-sized businesses was $120,000. The cost of reacting to a DDoS attack could reach $2.3 million for enterprises (as measured in 2017).[8]

Attacks directly on DNS providers can have even more far-reaching impacts for both the organizations that rely on them and the providers themselves: if their DNS goes down, organizations may look for a new provider.

Websites and applications are not the only targets of DDoS attacks. Attackers often target on-premise networks as well. Organizations with self-hosted DNS can be crippled while the attack goes on, with client devices unable to load needed resources. Such an attack can severely hinder an organization's operations, or stop them altogether.

How to stop the coming threats targeting DNS infrastructure

Ultimately only the right architecture can stop DDoS attacks that are growing in size with each passing year.

Legacy DDoS mitigation via hardware vs. scalable mitigation via software

Traditionally, the way to stop an attack was to buy or build a big box and use it to filter incoming traffic. Most legacy DDoS mitigation service vendors used hardware from companies like Cisco, Arbor Networks, and Radware clustered together into "scrubbing centers."

There were tricks to get these behemoth mitigation boxes to work together, but it was awkward. Physical limits on the number of packets a single box could absorb became the effective limit on the total volume that could be mitigated by a service provider. In very large DDoS attack situations, most of the attack traffic never reached the scrubbing center because, with only a few locations, upstream ISPs become the bottleneck.

The expense of the equipment meant that it was not cost effective to distribute scrubbing hardware broadly. It was typical for legacy DDoS vendors to only provision their service when a customer came

under attack; it never made sense to have capacity beyond a certain margin over the largest attack previously seen.

It seemed rational to assume that any investment beyond that was a waste. But that assumption is proving ultimately fatal to this traditional model.

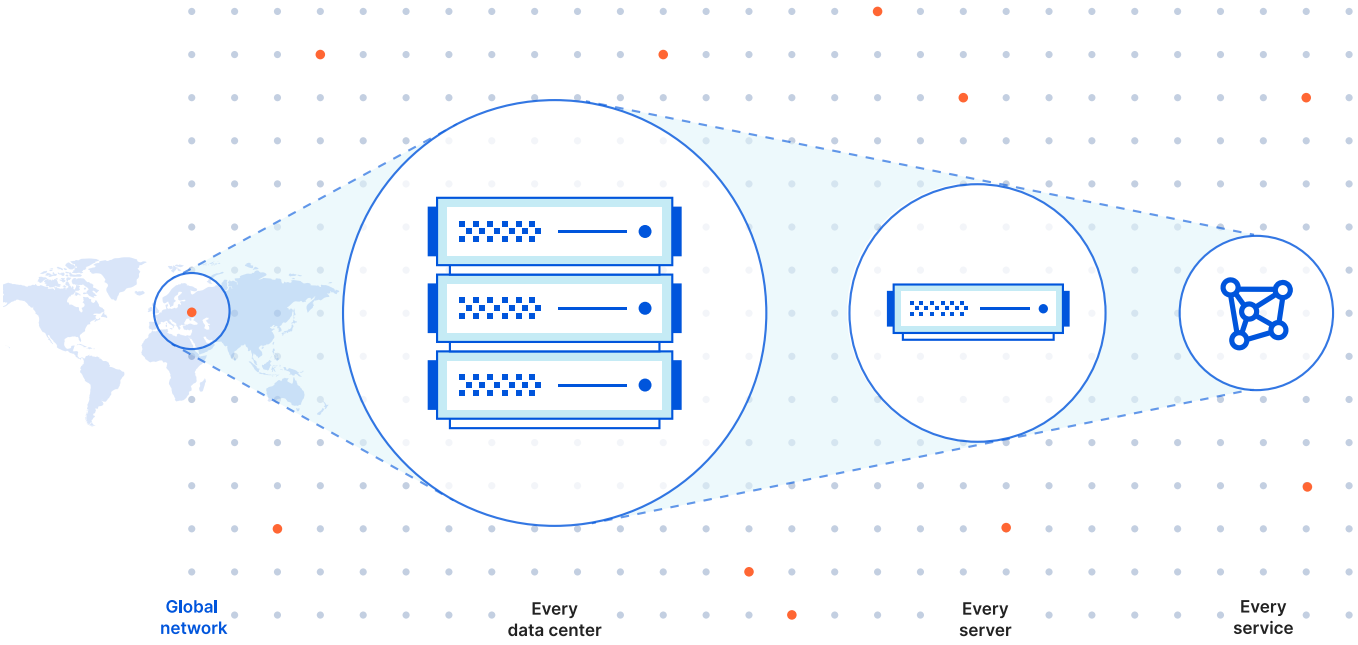
The future does not come in a box

Instead of investing in hardware boxes for DDoS mitigation, from its earliest days Cloudflare started with a very simple architecture. Cloudflare's first racks had only three components: router, switch, server. Today the rack is even simpler, often dropping the router entirely and using switches that can also handle enough of the routing table to route packets across the geographic region the data center serves.

Rather than using load balancers or dedicated mitigation hardware, which could become bottlenecks in an attack, Cloudflare wrote software that uses Border Gateway Protocol (BGP), the fundamental routing protocol of the Internet, to distribute load geographically, and within each data center in the network. Every server in every rack is able to answer every type of request. Cloudflare's software dynamically allocates traffic load based on what is needed for a particular customer at a particular time — meaning, Cloudflare automatically spreads load across literally tens of thousands of servers during large attacks.

It also means that Cloudflare can cost-effectively continue to invest in its network. For example, if a city needs 10% more capacity, Cloudflare can ship 10% more servers there, rather than having to make the step-function decision of whether to buy or build another scrubbing box.

Since every core, in every server, in every data center can help mitigate attacks, each new data center Cloudflare brings online makes the service better and more capable of stopping attacks nearer to the source. In other words, the solution to massively distributed botnets is a massively distributed network. This is how the Internet was meant to work: distributed strength, not focused brawn within a few scrubbing locations.



How Cloudflare easily scales up DNS security

But not only does Cloudflare use a distributed network to block and absorb malicious traffic efficiently, Cloudflare also provides authoritative DNS and DNS resolution from all of these locations. Serving DNS responses from any data center means DNS queries are resolved with minimal latency. It also means Cloudflare's DNS benefits from the entire network's capacity and distributed nature.

The Cloudflare network's efficient use of resources comes with operating savings as well as capital savings. Because Cloudflare uses the same equipment and networks to provide all of its functionality, Cloudflare rarely has any additional bandwidth costs associated with stopping an attack or providing any other service.

As Cloudflare's functionalities continue to expand, the capacity to stop attacks increases proportionately. Cloudflare can provide DDoS mitigation at a fixed cost to customers, regardless of the size of the attack, because attacks do not increase the largest of Cloudflare's unit costs.

This vast, distributed network of servers that all have the same capabilities also makes it simple for Cloudflare to offer functionalities at a massive scale and with minimal latency. One of the most core services is authoritative and secondary DNS; Cloudflare is the fastest DNS resolver in the world.[9]

The Cloudflare global Anycast network allows DNS resolution at the network edge in each data center across 275+ cities, resulting in unparalleled redundancy and 100% uptime. As Cloudflare's network capacity is well able to absorb DDoS attacks, the result is DNS that is resilient in the face of attacks of any size and type.

Winning the arms race and remaining resilient in the face of DDoS attacks

- Cloudflare's network capacity as of Q4 2022: **172 Tbps** (and growing)
- The largest DDoS attack ever recorded: less than **2.5 Tbps**

The size of DDoS attacks may continue to grow rapidly, even exponentially, in the coming years. But Cloudflare is positioned to continue winning the arms race for decades to come.

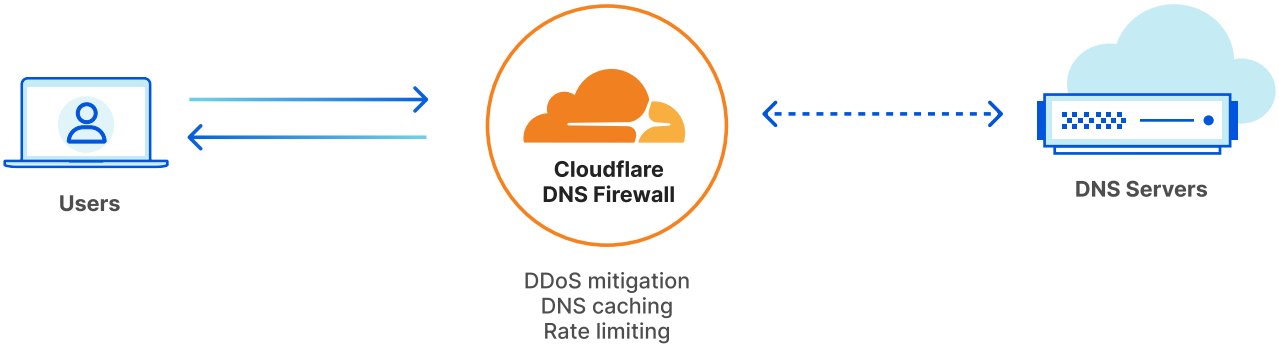
Cloudflare is the only provider that was designed from the beginning to mitigate large-scale DDoS attacks. Just as DDoS attacks are by their very nature distributed, Cloudflare's DDoS mitigation system is also distributed across its massive global network.

Against most legacy service providers, attackers have an advantage: providers' costs are high because they have to buy expensive boxes and bandwidth, while attackers' costs are low because they use an overwhelming number of hacked devices and generate an asymmetrical amount of traffic against their targets. That is why Cloudflare's secret sauce is the software that allocates the load across Cloudflare's massively distributed network of commodity hardware.

Protecting DNS from all kinds of attacks and exploitation

Cloudflare processes approximately 22.6 million DNS queries per second (both authoritative and resolution requests), as of Q4 2022 — all while mitigating growing DDoS attacks. Cloudflare DNS remains resilient against DDoS and bot attacks of any scale, from the large DDoS attacks of today to DNS water torture and other exploits.

For DNS service providers and organizations that host their own DNS infrastructure, the Cloudflare DNS Firewall provides a solution that not only helps them protect their infrastructure and users from large scale DDoS attacks, but also improves their performance by caching DNS records and responding on their behalf.



By natively integrating with DDoS mitigation, Cloudflare's DNS and DNS Firewall solutions ensure that your applications are always protected and available, even when facing some of the largest DDoS attacks on record.

Takeaways

Cloudflare continues to expand, adding more cities and countries to its network regularly. Cloudflare remains ever-vigilant for new attacks, but is confident that its architecture is ultimately the right way to stop whatever comes next. Start partnering with the network that's built to stop attacks on DNS both now and in the years to come:

- Protect yourself against all DDoS attacks, including large botnet-based DDoS attacks as well as amplification attacks, by setting up Cloudflare
- Keep your DNS up and running despite attacks by relying on Cloudflare as your authoritative DNS provider
- Protect your DNS infrastructure and potential DDoS victims by using Cloudflare's DNS Firewall to rate limit and deflect attacks

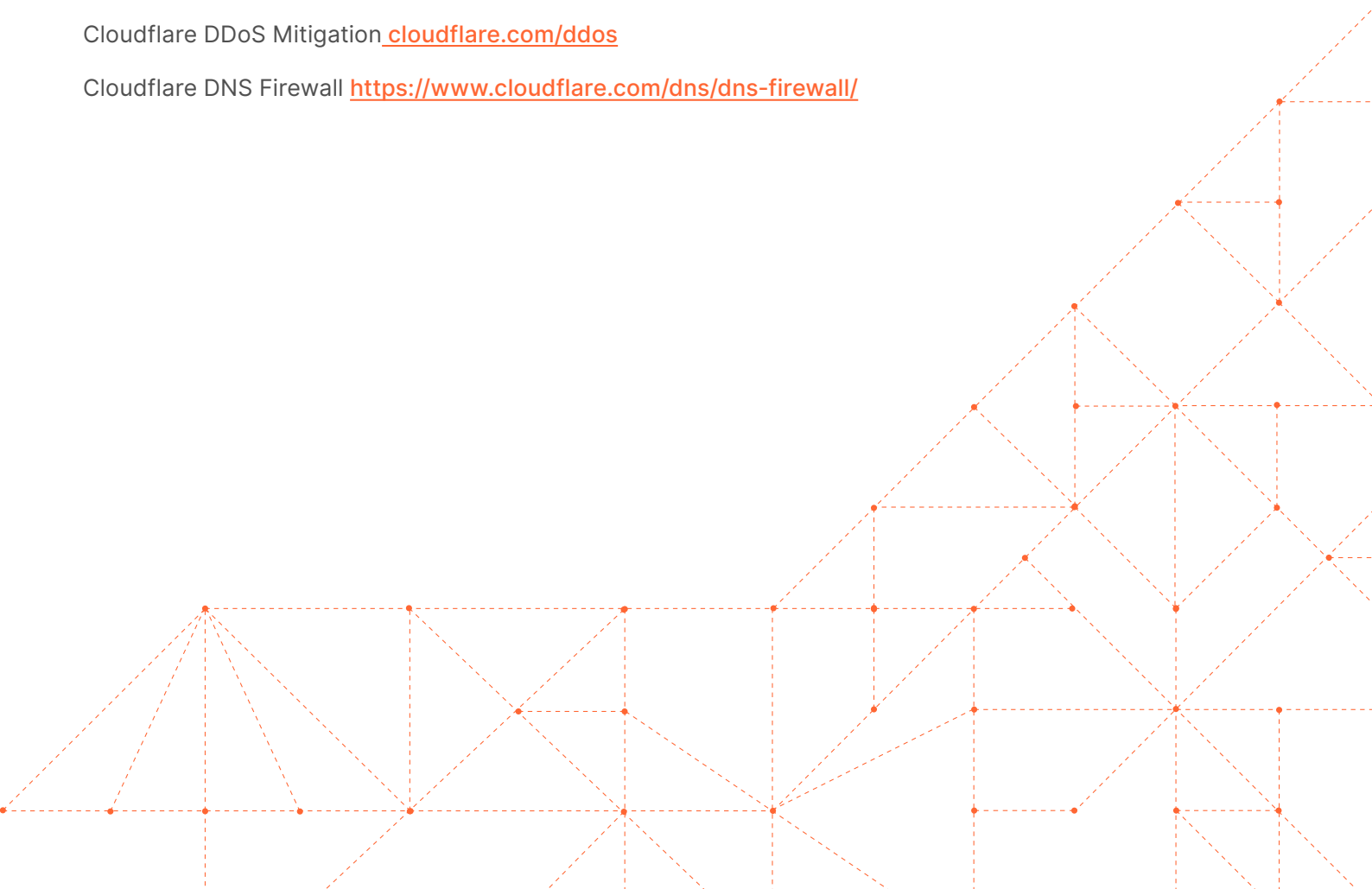
The setup is very simple and usually takes less than 5 minute to get up and running. See the plans, ranging from Free to Enterprise, at cloudflare.com/plans.

To learn more about Cloudflare's solutions, visit:

Cloudflare DNS https://www.cloudflare.com/dns/

Cloudflare DDoS Mitigation cloudflare.com/ddos

Cloudflare DNS Firewall https://www.cloudflare.com/dns/dns-firewall/



References

1. “DDoS Attack Against Dyn Managed DNS.” Dyn Statue Updates, 21 October 2016, https://www.dynstatus.com/incidents/nlr4yrr162t8. Accessed 3 October 2022.
2. Cimpanu, Catalin. “AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever.” ZDNET, 17 June 2020, https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/. Accessed 3 October 2022.
3. Yoachimik, Omer. “Cloudflare mitigates 26 million request per second DDoS attack.” Cloudflare, 14 June 2022, https://blog.cloudflare.com/26m-rps-ddos/. Accessed 3 October 2022.
4. Ganti, Vivek and Omer Yoachimik. “A Brief History of the Meris Botnet.” Cloudflare, 9 November 2021, https://blog.cloudflare.com/meris-botnet/. Accessed 3 October 2022.
5. Yoachimik, Omer. “Mantis - the most powerful botnet to date.” Cloudflare, 14 July 2022, https://blog.cloudflare.com/mantis-botnet/. Accessed 3 October 2022.
6. “Alert (TA14-017A): UDP-Based Amplification Attacks.” CISA, 18 December 2019, https://www.cisa.gov/uscert/ncas/alerts/TA14-017A. Accessed 24 October 2022.
7. Prince, Matthew. “The DDoS That Knocked Spamhaus Offline (And How We Mitigated It).” Cloudflare, 20 March 2013, https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/. Accessed 24 October 2022.
8. Kobialka, Dan. “Kaspersky Lab Study: Average Cost of Enterprise DDoS Attack Totals $2M.” MSSP Alert, 25 February 2018, https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/. Accessed 3 October 2022.
9. “DNS Performance Analytics and Comparison.” DNSPerf, https://www.dnsperf.com/. Accessed 24 October 2022.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES/3855.20221104