# What to Look for When Choosing a CDN for DDoS Protection

Written by Bizety

WHITE PAPER

## Introduction

Every online company should be familiar with Distributed Denial of Service (DDoS) attacks and the risk they pose to business. But while DDoS threats are a cause for concern, actionable DDoS solutions are available and new security approaches are regularly developed. By understanding the different categories of DDoS attacks and the methods of DDoS prevention, your company can select the best options for your needs.

This paper will introduce the basics of DDoS attacks, starting with earlier **flood** style attacks, and covering emerging trends in attack patterns, most notably the rise of **reflection** and **amplification** attacks. We will explore the different solutions available, including DDoS appliances, cloud-based mitigation services and hybrid solutions. In doing so, we will also cover the strengths and weaknesses of each approach. Finally, we will take a closer look at how a Content Delivery Network (CDN) vendor can help protect you against DDoS attacks and what to look for when choosing one.

## DDoS attacks

Every DDoS attack shares a common objective — to block users from online resources. To accomplish this, attackers use multiple hosts to overwhelm targeted networks. Modern attacks typically rely on botnets — collections of compromised computers running assorted malware. These botnets provide attackers the computing power needed to carry out resource intensive DDoS attacks.

Each of the past five years has seen a sharp rise in the volume, frequency, and intensity of DDoS attacks targeting both American and international companies. According to Arbor Network's Worldwide Infrastructure Security Report, in 2015 attacks reached peaks of over 400 Gbps, with DDoS remaining the number one threat to service providers[1]. Forrester Research predicts that more than 60% of American companies will have to deal with a breach of sensitive data in the coming year, with DDoS attacks identified as a principal vector.[2]

Corporate data centers have become a favorite target for attacks. The Ponemon Institute reports that cybercrime, including DDoS attacks, represents the fastest growing cause of data center outages.[3] Major attacks have already disrupted popular online gaming sites, as well as targets in the media, telecom and financial sectors.

## Common DDoS attack types: flood attacks

The most common form of DDoS attacks has historically been **flood attacks**, which take advantage of the Transmission Control Protocol (TCP) handshake procedure. The attacker sends a synchronization request (SYN) to the targeted server (often with a spoofed or faked source address), which then responds with a synchronization acknowledgement (SYN-ACK), an open invitation to form a connection. The attacker leaves the invitation open filling the list of open connections with these false requests and blocking any new legitimate connections.

This process is then repeated thousands, millions or even billions of times. The flood of open or false requests eventually overwhelms system resources, at which point the target network starts denying access to legitimate users. Attacks can target a variety of resources at several different layers.

Variants of flood attacks include those that target the Internet Control Message Protocol (ICMP) with Echo Request (ping) packets, the User Datagram Protocol (UDP), or HTTP with GET or POST requests. These constitute complex flood attacks, requiring comprehensive filtering and network management expertise.

Initially, flood attacks followed a 'dumb' attack pattern targeting Layers 3 and 4. These attacks were primarily blocked by big networks and big, IP-based filtering (maintaining a blacklist of attacking IP addresses). While brute force flood attacks can successfully deny service to legitimate customers, they require a sizable network of attacking hosts to shut down major websites. System developers and network engineers are also very familiar with these forms of attacks, and have become increasingly adept at recognizing attack patterns and blocking malicious access before the network is overloaded.

Recently, Layer 7 attacks with 'real user' simulation have gained in popularity and sophistication. Managing these attacks requires separate inspection of headers and data requests, which can only be accomplished through Layer 7 application platforms like Varnish.

## Emerging attack patterns: reflection and amplification

The past three years have seen a shift in the nature of DDoS attacks, as basic flood-style attacks gradually grew less effective. Currently, **reflection** and **amplification** attacks are rising in popularity. Reflection and amplification attacks are also evolving past DNS based attack vectors, branching out to exploit NDP, SSDP and other UDP protocols as well.

Reflection attacks, like flood attacks, begin with a query to a target server. The original request is sent with a spoofed source address. When the target responds, this response is altered and returned (reflected) back to the target as a new query, along with a response to the original request. By exploiting vulnerabilities and the lack of authentication protocols, these reflected responses soon present a huge burden to the target network, without requiring the same level of infrastructure as flood attacks.

Amplification attacks focus on sending out seemingly harmless queries to multiple hosts (compromised or not), then directing the response to a targeted server. As the response is designed to be exponentially larger than the query, and originates from trusted locations, amplification attacks outpace basic flood attacks in both severity and difficulty of mitigation. Amplification attacks originally used DNS level queries that take advantage of large DNS responses (for example the large size of DNSSEC keys) and the widespread availability of open DNS resolvers.

These vulnerabilities allowed for attack amplification of over 4000 times the original query rate. Amplification attacks can target NTP and SSDP, as well as any UDP-based protocol. The largest modern DDoS outbreaks use elements of both reflection and amplification types of attacks to achieve ever increasing rates of attack.

## DDoS solutions

While the news regarding DDoS often appears grim, there are several different approaches your company can take to mitigate DDoS risk. Due to the constantly changing nature of attacks, there is no silver bullet solution for all attacks, but every DDoS threat can be recognized and defeated with sufficient preparation.

### DDoS appliances

DDoS appliances are often the first line of defense against DDoS attacks. They can typically handle minor attacks of up to 1 Gbps and can initially seem like good value. However, in high traffic situations, bottlenecks quickly appear in the bandwidth in front of the appliance, blocking most legitimate traffic at that point.

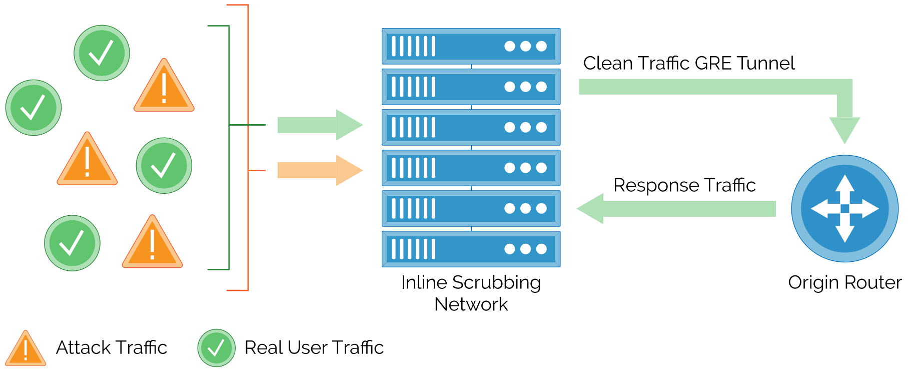
The price of keeping a DDoS proficient engineer on staff can also quickly add up, and it can be inefficient to have employees simply waiting for attacks to happen. Corporate datacenters can struggle even with normal DDoS attacks, and risk high rates of failure against larger or sustained attacks. The need for more appliances and highly skilled DDoS engineers quickly makes this solution cost prohibitive.

### Cloud-based DDoS mitigation services

As full-scale, on-site DDoS protection is generally not cost effective, many companies are turning to cloud service providers for DDoS protection. By using edge-based filtering, malicious requests can be blocked before they become a problem. Content Delivery Network (CDN) vendors in particular offer a powerful and scalable option, due to their robust networks, high capacity, and distributed resources.

CDNs offer two main forms of cloud-based DDoS solutions — always-on solutions, which provide symmetric protection for regular operations, and on-demand solutions, which offer asymmetric protection for elevated threat situations.

**Always-on solutions** use inline scrubbing to monitor traffic and remove suspicious requests without routing through specialized servers. With bidirectional intelligence, the point of presence (POP) servers can drop flood traffic before it impacts the customer. And since scrubbing takes place at the POP, there is little impact on application latency.



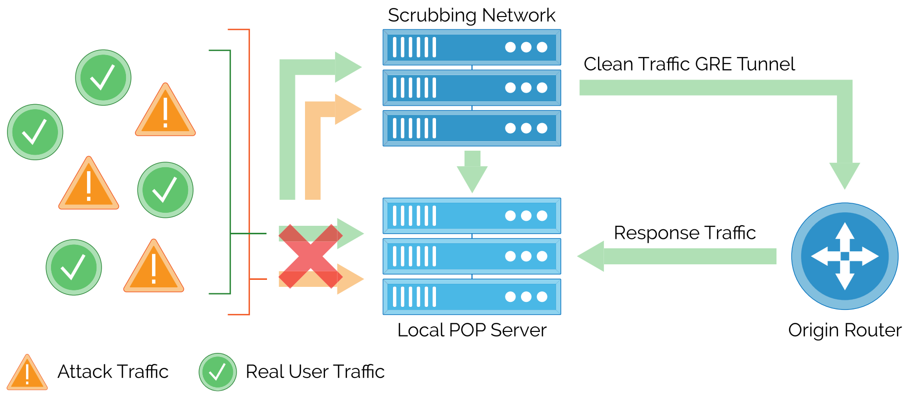
Some CDNs potentially offer visibility into all bidirectional traffic (encrypted and unencrypted), giving them an ideal position for consistent mitigation policy across open and encrypted traffic flows. By using edge cache nodes as enforcement points, the scope of attacks can be recognized and constrained from the start, limiting the resources required for an adequate security response. By situating the mitigation enforcement at the cache edge, always-on solutions can immediately identify Layer 7 attacks, and can better implement origin health monitoring.

CDN nodes can be very effective for continuous scrubbing, but require a CDN with the right network architecture, and sufficient transactional capacity to handle massive attacks. There may be emergent issues with 'cloud piercing', where attackers relay DDoS type requests directly to the origin servers, attacking around the CDN. When choosing an always-on solution, make sure the CDN provider has both the capacity and security protocols to address these issues.

With an always-on solution, 'cloud piercing' attacks can best be avoided by hiding the IP addresses of the origin servers. Some CDNs only provide CDN IP addresses without actively concealing the origin IP, so that enterprises can "filter" any traffic that isn't from that address. This a stop-gap solution, as the attackers can still saturate the bandwidth in front of the origin server. Truly "hiding" the origin IP addresses from the public Internet routing tables is the only guaranteed solution.

**On-demand solutions** focus on rerouting traffic through network-based scrubbing centers. BGP route changes and DNS redirection can deal with threats at different layers, without dropping actual user requests.

BGP allows for the deployment of network changes for the entire netblock (the range of IP addresses controlled by the CDN), preventing any possibility of bypass. This wholesale redirection can immediately shut down even the largest of attacks, but risks slowing legitimate traffic.



Furthermore, BGP solutions rely on netflow based detection that is blind to Layer 7 information - the mitigator doesn't have information at the application layer until the traffic flows through it. Without application layer data, on-demand solutions can be less agile in identifying and responding to threats.

These solutions require enough IP address space to be "routable," which means that blocks smaller than 256 addresses may not be eligible for this type of service. Such solutions can be ideal for large scale mitigations, but remain unavailable for smaller sections of network address space.

On-demand protection is an essential tool for dealing with large volume attacks, but is not very efficient when it comes to other forms of DDoS attacks. Examples include SlowLoris or SNMP-based attacks, which exploit loopholes in traditional intrusion detection. In addition, on-demand solutions completely miss complex Layer 7 attacks.

**Hybrid solutions**
Highly risk-adverse companies often end up with a hybrid solution, deploying both DDoS appliances in conjunction with cloud-based mitigation services to address security threats. To many, hybrid solutions seem to offer the best of both worlds, with accessible on-site integration, and cloud-supported attack management.

However, hybrid solutions are notoriously difficult to implement and can become exceedingly complex to maintain. Incorporating DDoS appliances into a cloud-based protection system requires specialized expertise and continuous supervision. Conflicting attack recognition methods also risk interrupting legitimate high-volume traffic, and can be delayed in reacting to actual threats.

When improperly deployed, hybrid solutions can be less effective than correctly architected always-on solutions. The cost can quickly skyrocket, as a company finds itself paying for two conflicting methods of DDOS protection, instead of superior cloud-based protection on its own.

## Solution summary

Coordinating a DDoS mitigation system starts with understanding your company's IT infrastructure, and planning your protection accordingly. For low and slow attacks, up-to-date and secure DDoS appliances — with properly integrated reverse proxies, firewalls and content switches — offer mitigation without affecting legitimate traffic.

For larger, faster attacks requiring massive scrubbing efforts, cloud-based rerouting can be crucial. Cloud-based vendors are often best prepared to deal with the size and severity of current reflection and amplification attacks, with system-wide white/black lists and monitored threshold settings.

When establishing your company's DDoS response strategy, it is important to properly incorporate all elements of protection. Your datacenter should be prepared for its role, and the CDN you choose should have the essential components to meet any threat.

## What to look for when choosing a CDN for DDoS

The market for cloud-based DDoS protection can be complex and confusing, but when choosing a CDN for this service there are four essentials elements to look for:

(1) **High network capacity**
(2) **Single secure network**
(3) **Real-time configuration changes**
(4) **Protection at all layers**

**High network capacity**
Massive attacks can require massive mitigation facilities – that's why your company needs a CDN with significant aggregate network capacity to withstand and repel large and sustained DDoS attacks. Verisign[4] reports an average attack size of over 7 Gbps, but this number is diluted by the thousands of low-level extortion attempts that target small web enterprises.

Sustained attacks targeting large corporations can reach 300 Gbps, making full-scale proxy solutions a necessity for websites with high baseline traffic. A CDN with high capacity network architecture is better positioned to deliver coverage in the case of an attack, because these networks regularly operate under substantial constant traffic.

Best practices require scrubbing the attack traffic as close to the source of the attack as possible. This creates a premium on distributed infrastructure capable of operating at scale. If massive quantities of attack and legitimate traffic collect in one location, the CDN scrubbing capabilities optimize filtering while also optimizing load across multiple POPs. A CDN with large-capacity POP locations, co-located at the major Internet exchange points (or IXPs) will have the resources to scrub attack traffic right at the edge, as far from the customer's origin server as possible.

**Single secure network**
By choosing a CDN with an integrated network, you ensure consistent traffic mitigation paths and rule application. While some CDNs provide separate networks for delivery and security traffic (or even worse, for PCI and non-PCI traffic), this approach risks dropping legitimate traffic and mishandling attacks.

With dependable routing and network behavior, a CDN with a single network for delivery and security can more easily spot security anomalies, and respond appropriately. A single network allows your company to make comprehensive scaling decisions as attacks intensify. The entire CDN network can also serve as a scrubbing center for symmetric and asymmetric solutions, meaning operations can reliably continue even during high threat situations.

With caching and security rules centralized, responsive adjustments and updates are also much easier to coordinate. Due to clear traffic architecture, these coherent networks are better prepared to mask origin IP addresses, and prevent any issues with cloud-piercing attacks. A single secure network enables uniform traffic flow, and handles encrypted traffic with the same stability as clear traffic.

**Real-time configuration changes**
Real-Time configuration changes allow you to responsively adapt to network conditions, including DDoS attacks. There are two sides to the configuration equation: data analytics and client-side change settings.

*Data monitoring and analytics*
To implement optimal security practices, your company requires a CDN that gives you real-time access to streaming logs, performance analytics, and global traffic profile. You should also look for comprehensive tracking of historical statistics like  percentage of requests per second, average and elevated data rates, and location-based demographics. By monitoring current and past usage patterns, attacks are easier to detect, and easier to mitigate.

Real-time logs and statistics allow you to have a non-filtered view of the attack, so you can tell exactly what the provider is doing for you. More than just high-level graphs, you need granular attack data that helps you understand how and why your mitigation strategy is working. Don't settle for "black-box" dashboards – make sure you get the full picture.

*Client-side change settings*
While CDN vendors staff DDoS experts to monitor and manage your website traffic, it can be beneficial to have the ability to make configuration changes on

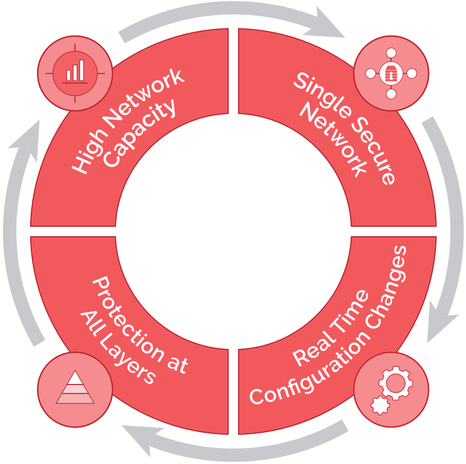
the fly, so that you can respond to real-time events. When deciding on a CDN vendor, check out the settings structure. Can you make necessary configuration changes? Can you make those changes quickly and easily, without having to rely on the vendor's professional services department? The ability to craft custom DDoS rules, roll back changes and adjust network behavior using a customer-facing UI or API will help you avoid slowdowns or unnecessary charges.

### Protection at all layers

Perhaps the most critical element of CDN DDoS mitigation is the ability to provide comprehensive protection at all layers. Many DDoS attacks take place at Layer 3 and Layer 4, the Network and Transport layers, respectively. Here, your CDN vendor should be prepared for NTP and DNS attacks, as well as the different flavors of floods: PING, ICMP, UDP, etc. A CDN should also be prepared for the latest styles of amplification and reflection attacks, and the various amalgams that regularly pop up.

A CDN-based DDoS mitigation service should be ready for common Layer 7 or application layer attacks. These attacks revolve around security loopholes in network interaction, and include LOIC/HOIC and SlowLoris-style function interference. Application layer attacks are particularly endemic to the financial industry, and can be deployed as a distraction technique for more penetrative attacks. A CDN can be pivotal in correctly differentiating between human, bot, and malicious bot access, and routing it accordingly.

### Elements of Evaluation



## Conclusion

The appropriate response to the rising DDoS threat is preparation. By understanding the different DDoS solutions available, you can choose the options that best prepare your company to mitigate any attack. A CDN-based DDoS mitigation service can be an essential element in your security program.

## More Information

For more information on how Fastly can help with DDoS protection, please visit fastly.com/DDoS

[1] Arbor Networks, *11th Annual Worldwide Infrastructure Security Report*, www.arbornetworks.com, 2016

[2] Forrester Research, *Predictions 2015: Security Budgets Will Increase, As Will Breach Costs, Fines, And Lawsuits*, www.forrester.com, 2015.

[3] Ponemon Institute, Cost of Data Center Outages, www.emersonnetworkpower.com, 2016

[4] Verisign Distributed Denial-of-Service Trends Report. www.verisign.com December 2014.