fastly

Fastly DDoS Protection and Mitigation

CUSTOMER FAQ

This document provides answers to some of the most frequently asked questions about Fastly's DDoS protection service.

What kind of DDoS services do you offer?

Fastly's DDoS services provide protection of HTTP (port 80) and HTTPS (port 443, TLS) with unlimited overage protection. We offer these services as an add-on to your edge cloud service, with annual renewal terms. Our DDoS protection service provides the following:

- **Immediate onboarding:** If you're not already a customer, we'll work directly with you to immediately transition you to Fastly's edge cloud platform.
- **Access to Fastly IP space and API endpoints:** This will allow you to filter traffic at your origin to ensure only Fastly cache systems can send requests directly to your data center's HTTP / HTTPS servers.
- **Emergency configuration and deployment support:** We'll actively work with you to configure your service map and set an initial filter policy to immediately block an attack.
- **Ongoing attack mitigation support:** We'll work directly with you to write custom filters in Varnish Configuration Language (VCL) to deal with changing attacks or new attacks. We'll also isolate malicious traffic on your behalf.
- **Layer 7 DDoS protection:** We protect your application layer without requiring BGP or DNS routing changes which can introduce latency and IT complexity.
- **A personalized Incident Response plan:** We'll deliver a plan identifying how communication and escalation will occur between you and Fastly if an attack occurs. This plan will also describe mitigation and defense details such as any DDoS filters that we can insert into VCL prior to, or during an attack.
- **Direct mitigation support:** We'll provide direct DDoS mitigation support for attacks that attempt to impact your origin availability or stability.
- **Unlimited traffic overage protection:** As a Fastly edge cloud platform customer, when you experience a DDoS attack and spike in traffic during an attack, we'll provide you with unlimited overage insurance. We'll forgive the charges to your bill that result from the attack. There are no overage protection limits based on the number of events or size of the attacks that can occur within any month.

What if I am not a Fastly customer?

If you're not already a customer, we'll work directly with you to immediately transition you to Fastly's edge cloud platform.

How does your DDoS service work?

We provide a fully integrated, always on, security aware platform. By building enforcement into our platform, we're able to rapidly mitigate attacks:

- We leverage our massive global network and server capacity to absorb much of the attack. For attacks targeting layer 3 or 4, we filter out traffic based on port and protocol, inspecting only HTTP or HTTPS requests. ICMP, UDP, and other network born attacks are dropped at our network edge. This includes reflection and amplification attacks which use UDP services like SSDP or NTP. By providing this level of protection, we effectively block multiple common attacks like Ping of Death, Smurf attacks, as well as other ICMP-based floods.
- We manage the TCP level attacks at the cache layer, addressing the necessary scale and context per client to deal with SYN flood and its many variants, including TCP stack, resource attacks, and TLS attacks within our systems.
- By leveraging the power of VCL, we can inspect for and filter out malicious layer 7 requests based on header, payload, Geo-IP, or the combination of attributes that identify attack traffic.
- Our application provides traffic insights to your service allowing you to manipulate your logs directly with advanced monitoring for rapid troubleshooting.

Can you protect against cloud piercing?

Yes. Fastly publishes our IP address space and encourages you to use those addresses to update whitelist Access Control Lists (ACLs) at your origin data center. This will allow you to ensure that only Fastly cache nodes can access the HTTP and HTTPS services and prevent traffic from the Internet accessing these services directly. Additionally, with our Origin Cloaking capabilities, we are able to hide the origin IP, forcing all attack traffic through our edge cloud platform, where we apply DDoS mitigation rules. We connect directly with your origin server using private network interconnections (PNI), hiding the IP address from the public internet and thwarting any attempts to bypass Fastly. If the origin site is not well architected (e.g. using a public IP all the way through to the origin) it will be harder to cloak. In this case, it may be worthwhile to connect your network to ours through a direct peering connection or via PNI, forcing traffic to pass through the Fastly network first. The direct connection to our network will help protect your data center during an attack that is actively trying to bypass our platform, making it easier than changing your data center IP address.

How would we initiate support for a DDoS attack or a DDoS threat?

Support is initiated through simple communication between your IT team and Fastly. A ticket, phone call, or email to **support@fastly.com** will trigger the process. Fastly will respond within 15 minutes and begin to prepare for the event or deal with an ongoing event.

How does Fastly handle attacks?

(see also **"How does your DDoS service work?"**)

With our massive aggregate network capacity as well as transactional capacity, we can defend against large attacks and accelerate TLS sessions to your origin site by keeping sessions alive and pipelining requests to your data center. Our network scales to the volume of inbound TLS sessions, particularly under an attack scenario.

We highly recommend building proactive filters during provisioning, where appropriate. However, if there is a problem detected or if the existing mitigations are being bypassed, it may be necessary to update or change the filters to block any current event or poor usage.

What should we do if we receive a threat?

If you receive a threat such as an extortion notice, you should file an attack report with Fastly support through our ticketing process (contact **support@fastly.com** to learn more), as it's valuable for us to understand if there is an escalated risk to your service that we may not be aware of. Please include the following in the attack report:

- Details about the severity of the threat
- Size of the attack threatened or previously observed
- Type and vector of any attack traffic seen or threatened
- Duration of previous attacks and vector behavior, including major source IP addresses, if known
- Attack history for the last 24 months, if we don't know already
- Threat specifics with details of any attacks that the protected services or sites have experienced in the past

Do you provide proactive detection?

Today, our service does not provide proactive detection for DDoS attacks. We filter most DDoS attacks at the network edge so they won't hit your origin in the first place. For smarter attacks that try to circumvent us, we can use Origin Cloaking to hide your IP address. If you have a dedicated IP address and we see attack traffic targeting it, we again leverage all of our platform defenses to stop the attack and maintain availability for your services. If the attack happens to be in stealth mode we may need your help in deciphering what the best path of mitigation should be. It is recommended that you maintain points of contact with us to ensure that we can reach someone on your team to work with through the technical details of one approach or another. In all cases, we want to keep your services running as fast as possible, so if there are issues you are concerned about please reach out to our **support team** to get started.

Does Fastly have a Security Operations Center?

Fastly has a virtual Security Operations Center. The SOC team works with Technical Account Managers who are assigned to customers during incidents and analysis.

Most DDoS incidents are mitigated through our infrastructure in an automated and transparent way, as Fastly maintains significant excess capacity to deal with these events. For major incidents, Fastly maintains an Incident Command (IC) structure which engages during events with customers that have experienced noticeable impact.

Fastly's cache operations are distributed by design. The IC structure enables the right Fastly engineers to be engaged, within minutes, to rapidly redirect traffic away from affected points of presence (POP) to other POP locations. Our data centers also have connections with multiple Internet service providers, and we can actively balance across internet connections to avoid being affected by an outage at one provider. Our team of incident commanders and engineers responding to incidents, is globally distributed.

Do you offer DDoS reports and dashboards?

Yes. Fastly provides information about status code responses, traffic volumes, and service specifics through our application. Login and take a look **here**.

We also stream all of the usage logs directly to you through our log streaming services. We think you probably know more about your web site or application than we do, so we work hard to get you as much visibility as possible from our platform within a second or two. We aim to ensure that you have immediate data and visibility needed to see what's happening with your service at all times. We highly recommend that you also take advantage of Fastly's ability to deliver real-time streaming logs. These logs can be used to generate statistics, reports and alerts about events within our platform before they impact your site. Fastly logs can be streamed to almost any major logging endpoint, including syslog servers, logging-as-a-service providers (like Sumo Logic, Papertrail, or Logentries), and Amazon S3 buckets. We also support encryption of log traffic using Transport Layer Security (TLS), so you can send sensitive information to log files without exposing data.

More Questions?

If you have any questions that are not answered in this FAQ please contact **support@fastly.com**