fastly

Fastly DDoS Protection & Mitigation Service

QUICK REFERENCE GUIDE

This document is for customers who have purchased Fastly's DDoS Protection and Mitigation Service. It provides details of our service, the onboarding process and guidelines on how to contact Fastly in the event of an attack.

Need to report a DDoS attack now?	Let us know ASAP! Create a support ticket by sending an emergency email to emergency@fastly.com. Filing this ticket will trigger Fastly's promised SLA response time.

Fastly DDoS Protection and Mitigation Service

What this service entails

Fastly offers basic DDoS protection as part of our core delivery service. By default, our network is designed to provide always-on DDoS, acting as a scrubbing center for Layer 3 and Layer 4 network attacks. You never see these attacks — they are automatically filtered at our network edge.

We can apply countermeasures at Layer 7 to protect HTTP and HTTPS traffic without requiring BGP or DNS routing changes. This service includes ongoing attack mitigation and 24/7 access to our security experts to mitigate an attack. It also includes service overage protection — Fastly will waive all bandwidth and request charges associated with DDoS attack traffic and provide invoice credits or adjustments for the same.

How Fastly's DDoS service works

Tapping into our security expertise and visibility of internet traffic throughout our network, we analyze all DDoS attack vectors using techniques such as VCL statements, network filters, and bulk traffic filtering through regional sinks.

For smarter attacks that try to circumvent Fastly, we can use private network interconnections, to connect directly with your origin server, hiding your IP address from the public internet. This forces all attack traffic to go through our network, where we apply security policies to protect applications hosted at your data centers.

Access to Fastly's IP ranges

We also provide access to the list of Fastly's assigned IP ranges via an API call, allowing you to whitelist Fastly's services through your firewall. You can then automate the API call (by running a script as a cron job) to request the list of IPs to detect when the IP ranges change. When using cloud hosted applications, you can dynamically update source IP-based Network Access Control Lists.

Onboarding for Fastly's DDoS Service

Included in onboarding

As a new subscriber of Fastly's DDoS Protection and Mitigation Service, we will engage with you to provide the following:

- **Best practices** outlining steps you can take to help avoid a DDOS attack
- An **incident response process** identifying how communication and escalation will occur during an attack
- A dedicated phone number to contact Fastly Support Engineers
- A **Slack channel** (unless one already exist for you) which can be used for real-time communications with Fastly's Security Support Engineers in the event of an attack
- A **questionnaire** which we will work with you to complete in order to gather more details about your network environment. This information will help us better protect you should an attack occur. This includes requesting two points of contact for Fastly to connect with in the event of a DDoS attack. You should include names, email addresses, and phone numbers for each point of contact and keep this information up-to-date with Fastly. If you are an existing Fastly customer and would like to check what contact information we currently have on file for you, please reach out to support@fastly.com.

During an Attack

Reporting a DDoS attack

When reporting a DDoS attack, we ask that you try to provide us with as much of the below background information as possible. While not required, it will greatly assist us in helping you faster:

- Estimate of attack severity
- Size of the attack threatened or previously observed
- Type and vector of attack traffic seen or threatened
- Duration of previous attacks and vector behavior including major source
- IP addresses
- Your organization's attack history for the past 24 months
- Threat specifics including all details of any attacks that the protected services or sites have experienced in the past
- Any available logs for the time of the attack

Emergency response times

When reporting a DDoS attack to emergency@fastly.com, you can expect a response to your ticket within 15 minutes. Tickets for communication between Fastly Support Engineers and our customers are tracked using a ticketing application. This application maintains a time-stamped transcript of all communications with Fastly staff and automatically sends you an email every time your ticket is updated.

Working with Fastly during an attack

In the event of a DDoS attack, we will provide you with the following services:

- **Emergency configuration and deployment support:** We will 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 will work directly with you to write custom filters in Varnish Configuration Language (VCL) to deal with changing attacks or new attacks. We will also isolate malicious traffic on your behalf.
- **Access to Fastly IP space and API endpoints:** This access 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.
- **Attack Investigation:** During the investigation of some attacks the Fastly team might require detailed knowledge of the targeted system and its architecture in order to develop the best possible mitigation signature/ strategy for it. Fastly may request introductions to additional contacts at your company in order to gather the full technical scope of an attack and it's impact. Examples of ideal contacts include system architects, application developers, and or network engineers.
- **An 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.

Responding to the threat of an attack

If you receive a threat of a DDoS attack, you can let us know by filing a support ticket — simply send an email to support@fastly.com. We will assign resources to monitor your service with extra attention. The Fastly Support Engineer that receives notification of your attack threat will reach out to you with actionable next steps.

Additional resources

At-a-glance communications table

METHOD	DETAILS	GUIDELINES
Emergency ticket email	emergency@fastly.com Available 24 / 7 / 365	For emergency cases requiring immediate response. The email triggers a page to an on-call support team member who will respond promptly. Please use your *company* email address when contacting us.
Emergency phone line	+1 (855) 378-0444 (toll free) Available 24 / 7 / 365	For emergency situations requiring an immediate conversation with a Fastly Support Engineer. If we miss your call, leave us a voicemail. This will page a support engineer, who will promptly call back to begin helping you.
General DDoS inquiries	support@fastly.com	Use this email for non-emergency or non-attack communications (e.g. general questions about DDoS). Submitting a support ticket via support@fastly.com will trigger a system-generated acknowledgement within minutes containing the ticket number and a direct link to the ticket.
Chat	https://fastly-support.slack.com @support – to reach support team directly Alternative options – @here or @channel	After you file a ticket, you can use Slack to communicate with your Fastly Support Engineer on topics requiring real-time interaction. Examples include questions on your TTL, setting up shielding, etc. Support engineers from the nearest time zone will be available during business hours to answer your questions, per the SLAs. Email support@fastly.com for help getting set up or for logins for additional team members.

Useful links

Fastly DDoS Protection and Mitigation Service FAQ

Fastly DDoS Protection and Mitigation Service Docs