CLOUDFLARE

Cloudflare Spectrum

Overview

Today, an increasing number of organizations are subject to layer 3 and 4 (L3/L4) DDoS attacks on their Internet-facing network properties. It's not just web servers that are under attack — game servers, email and file servers, and VPN concentrators have also been targeted on a frequent basis.

Cloudflare Spectrum is a reverse proxy service that provides DDoS protection for any application. Services such as MQTT, email, FTP, SSH, VoIP, gaming, or any application running over a TCP/UDP protocol use Cloudflare Spectrum to mask the origin server, protect it from DDoS attacks, and get performance benefits.

How Cloudflare Spectrum protects applications

When a request to the TCP/UDP application comes in, it first hits the closest Cloudflare data center. The connection is proxied and all traffic is inspected for threats. Clean traffic is then forwarded over Cloudflare's global network to the origin server.

Cloudflare automatically detects and mitigates stateful or stateless DDoS attacks using a dual-pronged DDoS protection approach:

- **Gatebot:** Gatebot is Cloudflare's centralized DDoS protection system for detecting and mitigating volumetric, globally-distributed DDoS attacks. Gatebot runs in our network's core data center. It receives samples from every one of our edge data centers, analyzes them, and automatically sends mitigation instructions when attacks are detected. Gatebot is also synchronized with each of our customers' web servers to identify the health and triggers of the servers and provide tailored protection against attacks.

- **dosd (denial of service daemon):** dosd is Cloudflare's decentralized DDoS protection system. dosd runs autonomously in each server in every Cloudflare data center around the world. It analyzes traffic and applies local mitigation rules when needed. In addition to quickly detecting and mitigating attacks, dosd significantly improves our network resilience by delegating the detection and mitigation capabilities to the edge.

Key integrations with Cloudflare Spectrum

- **Cloudflare Load Balancing**: When downtime occurs, all active TCP connections and UDP traffic automatically fail over to an alternate healthy server in a configured load balancing pool. By dynamically distributing traffic to the most available and responsive server pools, Cloudflare Spectrum and Load Balancing help increase the uptime of your services. They also provide TCP health checks and traffic steering to bolster the resiliency of your Spectrum-enabled applications.

- **Argo Smart Routing**: Applications such as RDP, VoIP, RTMP, and custom financial and gaming applications require low end-to-end network latency to deliver consistent, reliable, and 'real-time' experiences to end-users.

  Cloudflare Spectrum integrates with Argo Smart Routing to send TCP traffic faster than the 'best-effort' Internet. Cloudflare's network learns from the traffic that spans over 25,000,000+ Internet properties, enabling machine-learning (ML) based routing around network congestion in real-time.

  Based on synthetic measurement tests between Western America and Singapore, we saw a nearly 17% decrease in the TCP roundtrip time (RTT) on Cloudflare's network when compared to sending the traffic directly on the Internet.

- **IP firewall**: Spectrum comes with a completely software-defined IP firewall that can be configured right from your dashboard or API. You can allow or deny individual IPs or IP ranges in order to control traffic to your application server. You can also configure rules to block visitors from a specified country or even an Autonomous System Number (ASN).

- **Logshare**: Connection logs help customers debug, generate reports, and monitor service usage. With Cloudflare Spectrum, you can request detailed log data on every single connection event using a RESTful API. Spectrum also enables you to automate log data delivery to a cloud storage provider of your choice. We currently support Amazon S3, Google Cloud Storage, Sumo Logic, and Microsoft Azure Blob Storage.

Get the most out of Cloudflare Spectrum

There are three main benefits of using Spectrum:

- **Robust security**: With over 51 Tbps of network capacity, Cloudflare is equipped to mitigate DDoS attacks of any size and kind on your application servers.

- **Integrated security and performance**: When used in tandem with Argo Smart Routing, Spectrum ensures your traffic is protected *and* fast.

- **Easy implementation**: Onboard applications within minutes right from your Cloudflare dashboard. Setting up Spectrum does not need dedicated teams or support staff.

Real-world applications

Learn how companies like yours are leveraging our platform

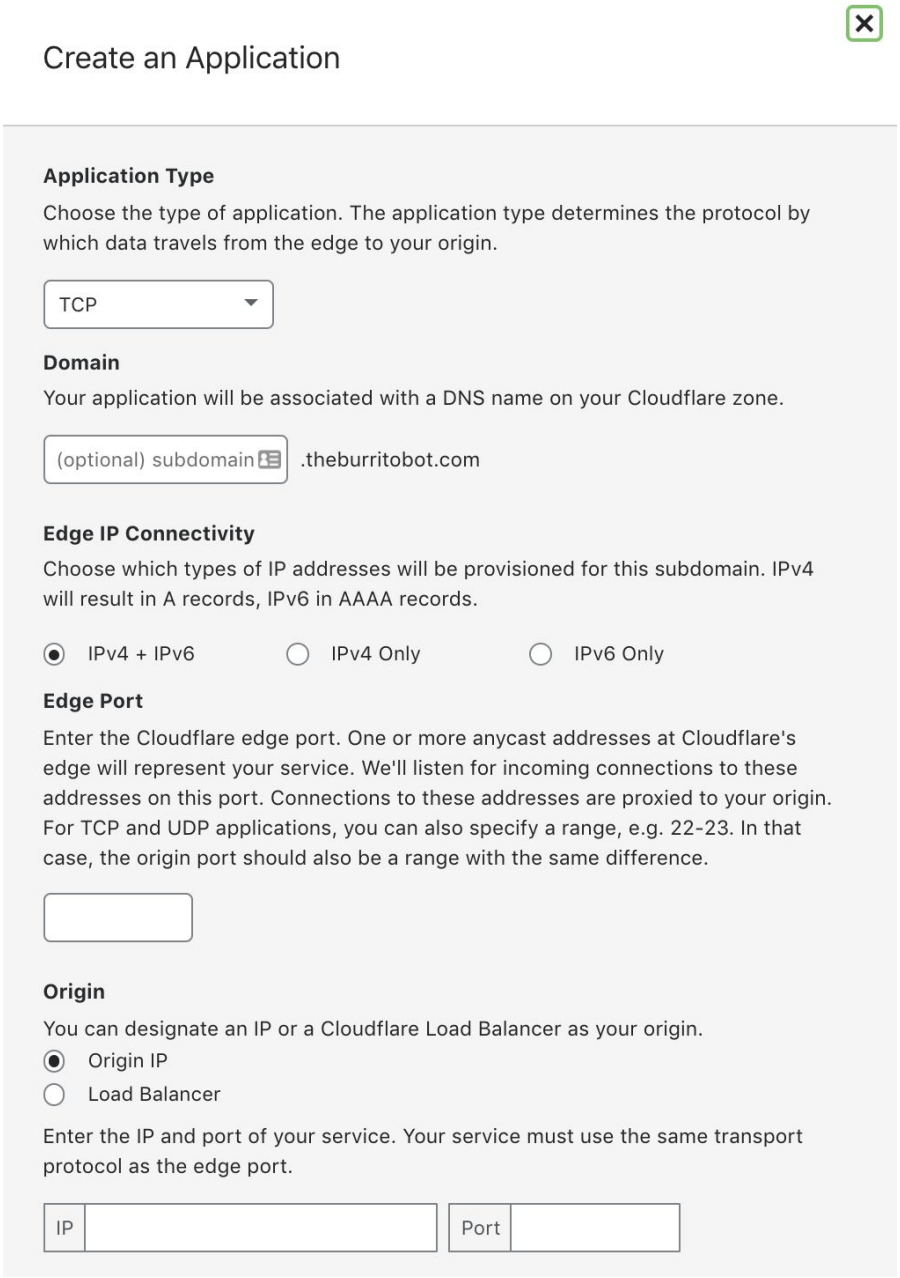
- When Shift Markets experienced connectivity issues for some of their globally-distributed clientele, they turned to Cloudflare. Now, they use Cloudflare Spectrum to protect their traffic routed over a proprietary TCP protocol.

- A cloud-based aquarium monitoring company used Cloudflare Spectrum to secure their IoT devices from attacks. When compared to competing products, Spectrum proved simpler to implement and easier to manage.

How to implement Cloudflare Spectrum

In the Dashboard, navigate to the **Spectrum tab → Create an Application**. Configure your application here.

Once created, the application will show up in the list within the tab:



Edge TLS Termination

When enabled, Cloudflare will encrypt traffic for your application at the edge. TLS may not be used with UDP applications.

Off

Argo Smart Routing

Enables Argo Smart Routing for this application. Argo Smart Routing routes traffic across the internet using the fastest network paths available. Argo Smart Routing is only available for TCP applications.

Off

IP Access Rules

If enabled, access rules with a Block or Allow action will be enforced for this Spectrum application.

On

Proxy Protocols

Enable the protocol version that your origin supports, if any. This relays the client's original IP and port information to your origin. It is only supported for TCP and UDP.

Off

Add