Service Description

Cloudflare Magic Transit DDoS

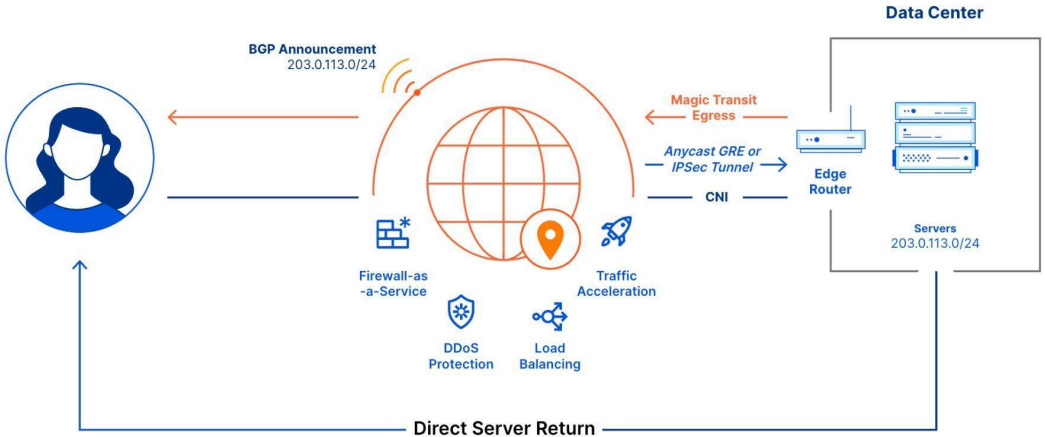
G-Cloud 15

CLOUDFLARE

Magic Transit

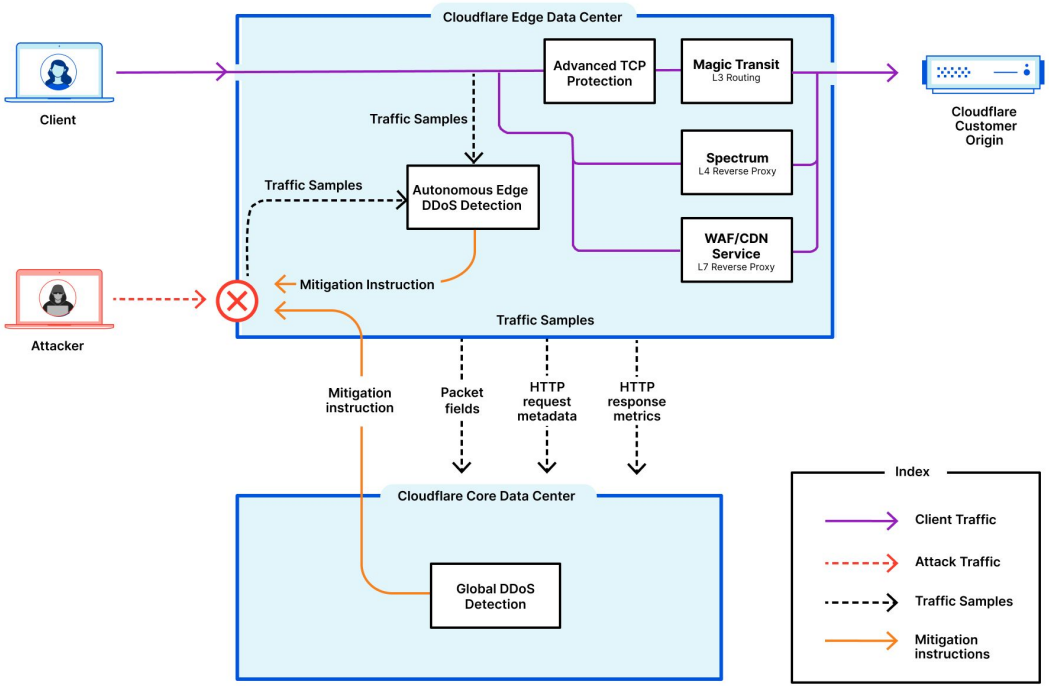
Protect your network infrastructure, data centers and public cloud services against DDoS attacks

Cloudflare network with built-in DDoS protection



- DDoS mitigation from every single data center
- **Every server** in every data center runs the **full stack of services** incl. DDoS mitigation, CDN, WAF inspection, etc.
- Cloudflare **network capacity = DDoS mitigation capacity** = 405 Tbps

How it works



Connect

Using BGP route announcements customer network traffic is ingested by Cloudflare

Protect and Process

All traffic inspected for attacks automatically and immediately

Accelerate

Clean traffic is routed back to the customer network over Cloudflare. Anycast GRE tunnels deliver traffic to the customer network

Options for connecting to the Cloudflare network

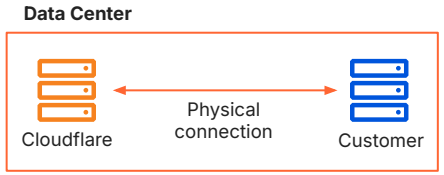
- **Cloudflare Network Interconnect (CNI)**

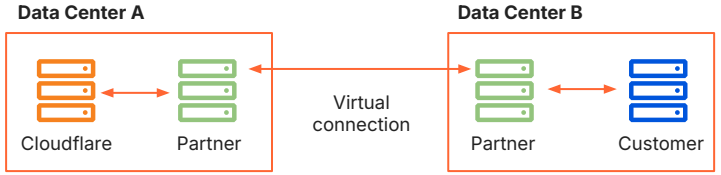
  Direct — layer 1

  - Direct connection to Cloudflare routers
  - Available in over 330 Cloudflare cities

  Partner — layer 2

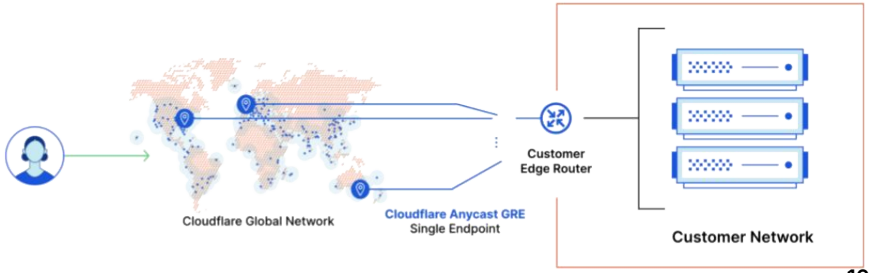
  - Use an intermediary *network fabric* partner in between your network and Cloudflare
  - Available in over +1,600 data centers: *[Equinix, Megaport, PacketFabric, Console Connect, Coresite and Epsilon]*



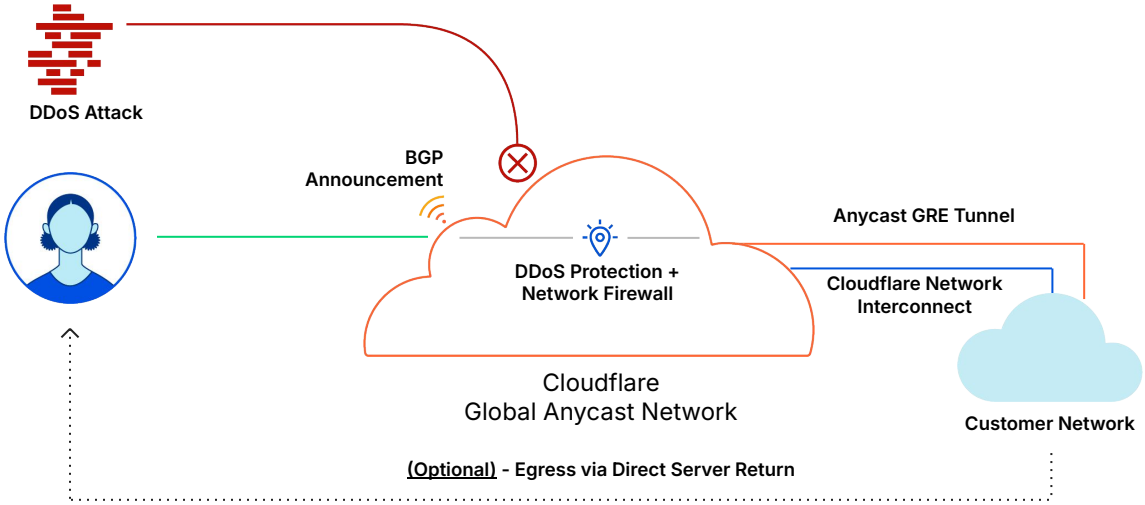


- **Internet (Anycast GRE or IPsec Tunnel)**

  - Available in any location with an Internet connection
  - Fast setup and no single point of failure with redundant Anycast GRE or IPsec tunnels



Send & receive all traffic through Cloudflare



Previously

Ingress traffic steered through the Cloudflare network. Egress traffic goes direct to Internet.

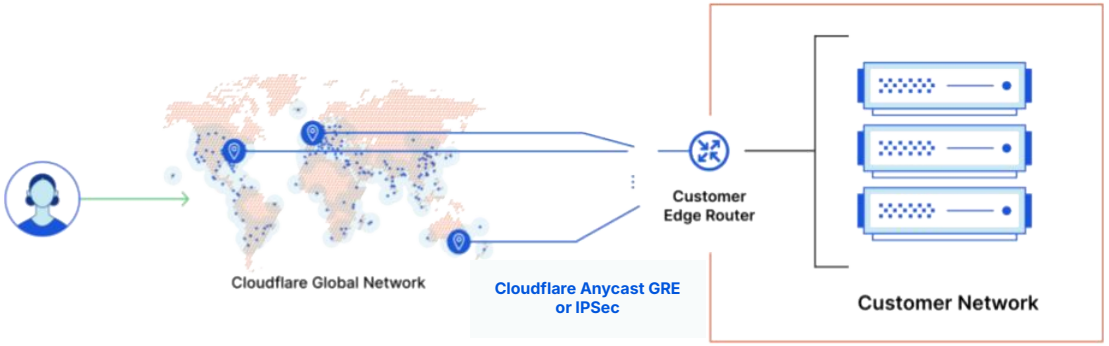
Supported

Customers can send return traffic **through Cloudflare** to the Internet, over the same paths used for incoming traffic.

Benefits

- Flow symmetry
- Enhanced performance in both directions
- Improved security for egress traffic (if directly connected)

Anycast routing for L3-L7 traffic



Connect via GRE or IPsec

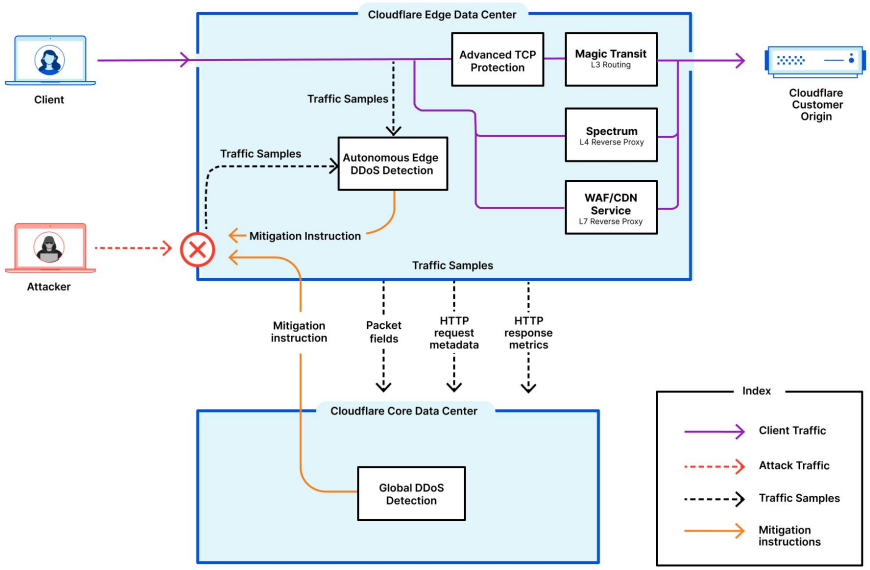
- The tunnel is bound to an IP address, not a specific device or data center location
- GRE provides easy connectivity from any network device
- IPSec provides privacy and easy integration with public cloud VPCs

Set it & forget it

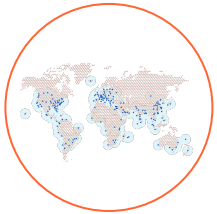
- Health checks from all Cloudflare data centers used to route traffic over healthy tunnels
- ECMP-based load balancing (set weights & priorities for tunnels)

Multi-tiered defense

- **Autonomous Edge:** ***Decentralized*** system, runs autonomously in each server in every Cloudflare data center around the world, analyzing traffic and applying local mitigation rules when needed.
- **Coordinated Global Defense:** ***Centralized*** system, runs in Cloudflare's core data centers; detects and mitigates globally distributed volumetric DDoS attacks.
- **Advanced TCP Protection:** ***TCP state tracking*** machine, using only the ingress traffic that routes through Cloudflare, detects and mitigated sophisticated TCP attacks.
- **Behavioral DDoS Protection:** ***Traffic profiling*** based on various dimensions to detect and mitigation deviations.
- **Magic Firewall:** Granular ***rules-based filtering*** with IP lists, threat-intel, geo-blocking and more.

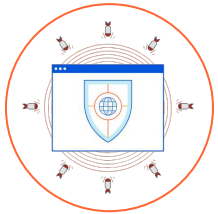


The Cloudflare DDoS difference



Modern Architecture

- Global 480 Tbps Anycast network
- Unified L3-7 protection
- In-line detection and mitigation, no Scrubbing Centers/3rd party boxes
- Cloud/on-prem Agnostic
- Traffic acceleration via real-time smart routing



Comprehensive Protection

- Real-time fingerprinting
- Adaptive DDoS protection
- Novel TCP state classification engine & traffic profiling
- Time to mitigate <3 sec
- Magic Firewall for additional layer of protection

Easy to use

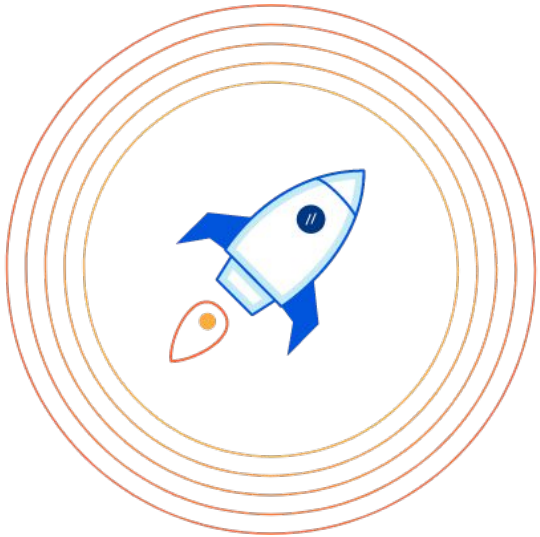
- Fully self-service and configurable
- API first, Terraform and Logs support
- Single analytics and management pane
- BYOIP or Cloudflare leased IP

CLOUDFLARE

Argo Smart Routing for Packets

Detect and route around real-time network congestion for faster web app performance

Supercharge your network performance using the Cloudflare network



Argo improves your network performance

10%
faster network performance using dynamic intelligence from real time network probes across 325+ cities

Improved reliability
by rerouting traffic around congestion points in the network and choosing the most reliable links

Improved security
by encrypting traffic across the Cloudflare network

Latency metrics: https://blog.cloudflare.com/argo-v2/

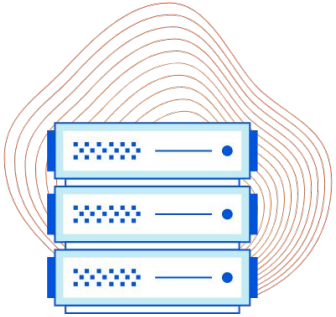
CLOUDFLARE

How does Argo work?

Using network analytics to make better routing decisions

- Argo periodically polls your network locations from every Cloudflare data center and examines every available path through the Cloudflare network
- Argo dynamically chooses the best possible path to route traffic to your network location
- Your traffic is delivered to its destination over the Cloudflare network using encrypted tunnels
- Argo improves latency and reduces packet loss resulting in **10%** improved performance

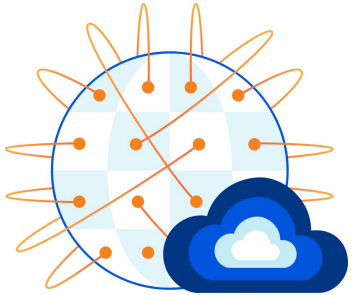
Argo is available to all Magic Transit and Magic WAN customers. Contact your account manager to upgrade your service.



Magic Transit

Network-layer DDoS Protection as-a-service

DDoS protection for entire IP subnets across on-premise, cloud-hosted, and hybrid networks. The Cloudflare network advertises your IP address space via BGP to accept, process and accelerate traffic destined for your network



Magic WAN

WAN-as-a-service

Replace legacy WAN architectures such as MPLS. Securely connect any traffic source - data centers, offices, devices, cloud properties - to Cloudflare's network and configure routing policies to get the bits where they need to go

Magic Firewall

Network Firewall-as-a-service

Enforce centrally-managed firewall policies at the edge, across traffic to/from any entity within your network. Integrates seamlessly with Magic Transit and Magic WAN

Customer Success Resources

CLOUDFLARE

Ensuring your success

 Community	 Docs	 Resource Hub	 Help Center	 Discord
 Blog	 theNET	 Cloudflare Radar	 CloudflareTV	 YouTube

CLOUDFLARE

Service Product Definitions

Network Services Definitions

CLOUDFLARE

Network Security	The **Cloudflare network security portfolio** exists to secure the networks of modern enterprises, helping to mitigate DDoS attacks, identify malicious traffic patterns, and monitor new and emerging threats. Our solutions offer unified, layered security and can be applied across all endpoints and users — no matter where they're located. Our network solutions are delivered from our global network which operates at massive scale. Every network service - like every Cloudflare service - runs on every server in every data center over our global Anycast network. All are easy to manage from the Cloudflare dashboard, the one pane of glass for all our services.
Magic WAN	Extends the benefits of our network to customers' private networks. **Magic WAN** enables IP level connectivity as well as a full suite of virtual network functions, including IP packet filtering and firewalling, load balancing, and traffic management tools.
Advanced Magic Firewall	**Magic Firewall** is a cloud-based firewall enabling administrators to set policies for all traffic entering and leaving the network.
Magic Transit	Cloudflare **Magic Transit** provides near-instant mitigation of network-layer threats (L3 DDoS attacks) from the Cloudflare global network, alongside next-generation firewall and traffic acceleration.
Network Interconnect	**Cloudflare Network Interconnect** allows our customers to interconnect branch and HQ location directly with Cloudflare wherever they are, bringing Cloudflare's full suite of network functions to their physical network edge.
Smart Routing	**Smart Routing** improves Internet performance by intelligently routing end users through less congested and more reliable paths over the Internet using our network.
Intrusion Detection Systems	**Intrusion Detection Systems (IDS)** is an Advanced Magic Firewall feature you can use to actively monitor for a wide range of known threat signatures in your traffic.

Network Services Definition

CLOUDFLARE

Access

Access determines who can reach your application by applying the Access policies you configure.

Gateway

Gateway, our comprehensive Secure Web Gateway, allows you to set up policies to inspect DNS, Network, HTTP, and Egress traffic.

Advanced Browser Isolation

Browser Isolation complements the Secure Web Gateway and Zero Trust Network Access solutions by executing active webpage content in a secure isolated browser. Executing active content remotely from the endpoint protects users from zero-day attacks and malware.

Cloud Email Security

Cloud Email Security solution crawls the Internet to stop phishing, Business Email Compromise (BEC), and email supply chain attacks at the earliest stage of the attack cycle, and enhances built-in security from cloud email providers.

CASB

Cloudflare's **Cloud Access Security Broker (CASB)** service gives comprehensive visibility and control over SaaS apps, so you can easily prevent data leaks and compliance violations. With Zero Trust security, block insider threats, Shadow IT, risky data sharing, and bad actors.

Data Loss Prevention

Cloudflare **Data Loss Prevention (DLP)** allows you to scan your web traffic and SaaS applications for the presence of sensitive data such as social security numbers, financial information, secret keys, and source code.