PulseSupply

CLOUDFLARE

Cloudflare Magic Transit

DDoS Protection for on-premise, cloud-hosted, and hybrid networks

Protecting network infrastructure from DDoS attacks demands a unique combination of strength and speed. Volumetric attacks can easily overwhelm hardware boxes and their bandwidth-constrained Internet links. And most cloud-based solutions redirect traffic to centralized scrubbing centers, which impacts network performance significantly.

Cloudflare Magic Transit provides DDoS protection and traffic acceleration for on-premise, cloud, and hybrid networks. With data centers spanning 200 cities and over 90 Tbps in mitigation capacity, Magic Transit can detect and mitigate attacks close to their source of origin in under 3 seconds globally on average — all while routing traffic faster than the public Internet.

The Cloudflare Advantage

Recognized Leader in DDoS mitigation

Top analyst research firms consistently rank Cloudflare as a leader in DDoS mitigation because of Cloudflare's recorded ability to block attacks of all sizes and kinds, unique architecture, rapid onboarding, and fine-grained controls.

Robust security with integrated performance

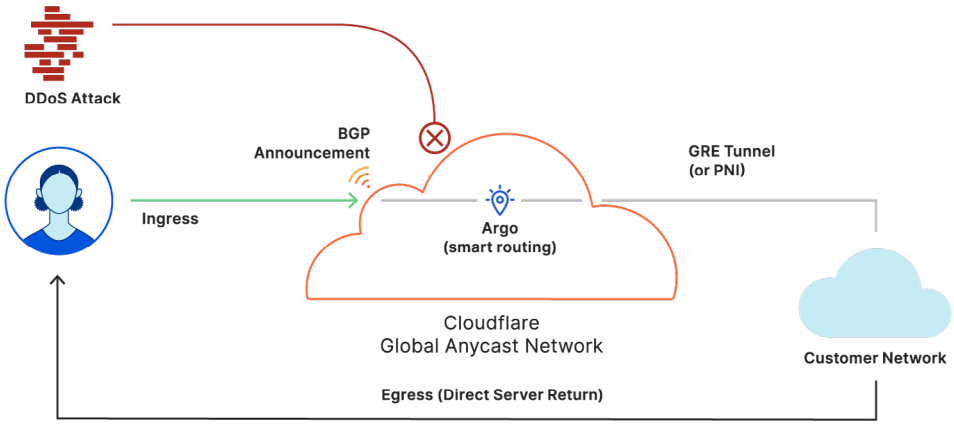
Magic Transit runs as a service on every server in the Cloudflare network—meaning there's no need to divert traffic to latency-inducing scrubbing centers. Better yet, traffic routed over the Cloudflare network benefits from faster routing than over the public Internet.

Lower TCO by combining DDoS, WAF, CDN, Bot Mitigation (and more)

Our security, performance and reliability functions are built on the same global anycast network spanning over 200 cities. They are designed to integrate seamlessly and can be managed from the same dashboard. With zero CAPEX required, security and performance functions can be deployed easily with increased operational agility.

Feature Comparison	Cloudflare	Others
Use BGP and BYOIPs	✓	✓
Return traffic over GRE	✓	✓
Global network > 90 Tbps network capacity	✓	✗
Sub-second threat detection and TTM < 3 sec	✓	✗
Integrated performance benefits	✓	✗
Native integration of L3/4/7 products	✓	✗
Built-in L3 firewall	✓	✗

How Magic Transit works



1. Connect

Using Border Gateway Protocol (BGP) route announcements to the Internet, and Cloudflare's anycast network, customer traffic is ingested at a Cloudflare data center closest to the source.

2. Protect and Process

All customer traffic is inspected for attacks. Advanced and automated mitigation techniques are applied immediately upon detecting an attack. Additional functions such as load balancing, next-gen firewall, content caching and serverless compute are also delivered as a service.

3. Accelerate

Clean traffic is routed over Cloudflare's low-latency network links for optimal throughput and handed-off over anycast GRE tunnels, private network interconnects (PNI) or other forms or peering to the origin network.

Threat intelligence at scale

Cloudflare DDoS protection is fueled by intelligence from our global network, which protects millions of websites. This reach gives us a unique vantage point to deploy learnings globally and constantly protect against the newest and most sophisticated attacks.

Analyze your data, your way

Network analytics enable you to analyze DDoS events through Cloudflare's dashboard or the GraphQL API. Get real-time visibility into network- and transport-layer traffic patterns and DDoS attacks that are blocked.

Flexible deployment options

Magic Transit is available in on-demand and always-on deployment options. With Cloudflare, you don't have to worry about added latency in either option — pick what suits your network architecture best.