CLOUDFLARE

SOLUTION BRIEF

Network Protection

Protect public-facing infrastructure with Cloudflare's connectivity cloud

Problem: Tradeoffs between security and performance

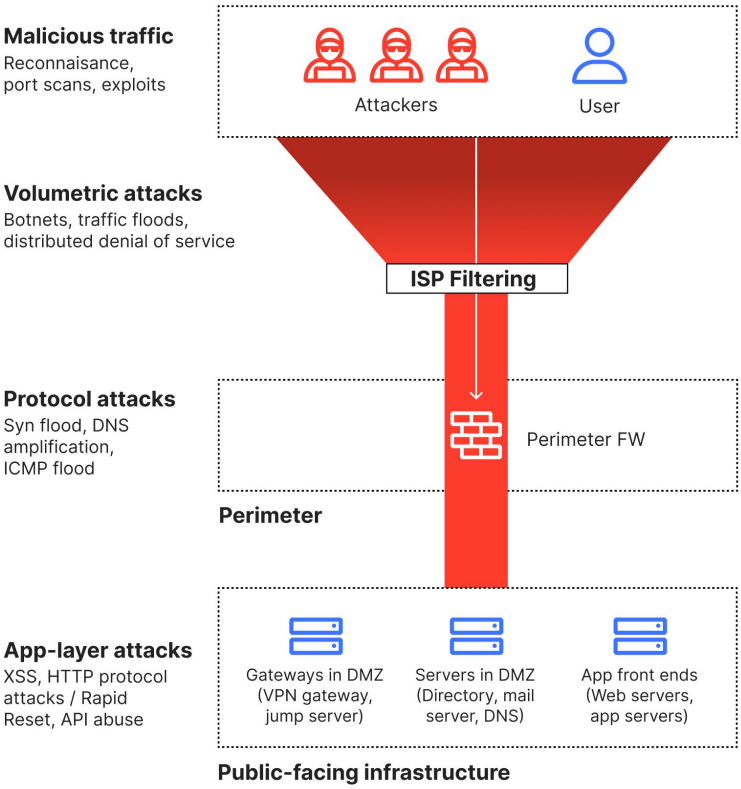
Public-facing infrastructure faces security vulnerabilities as its Internet accessibility makes it a target for various types of attacks. Threat actors can scan for discoverable services, exploit unpatched vulnerabilities, and launch devastating DDoS attacks that cause financial damage before security teams can respond.

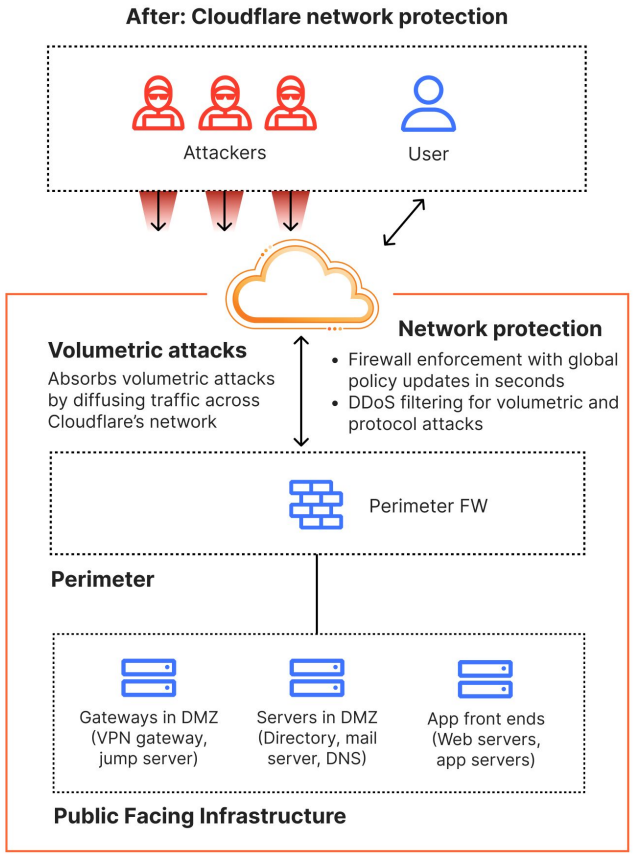
Organizations have deployed numerous firewall helpers and network appliances, but these often create inefficiencies while still failing against sophisticated threats.

Solution: Network Protection

Simplify your architecture and make it more secure by augmenting your network with Cloudflare's connectivity cloud. Easily add functionality by enabling cloud-delivered services — rather than inserting appliances — and support your network modernization journey with a platform that addresses both current needs and new, future use cases.

Cloudflare provides global coverage with single-pass enforcement that includes multi-layered protection for volumetric, protocol or app-layer based attacks – alongside visibility into network state, behavior and performance.





How it works

1. Establish a traffic path to Cloudflare's Anycast network via IPSec tunnels, GRE tunnels or using Cloudflare Network Interconnect (CNI)
2. Gain automatic protection via Magic Transit and Magic Firewall with minimal configuration
3. Deploy policies globally within seconds

Learn more about architecting Cloudflare to protect your existing network infrastructure.

Benefits

- **Elastic resources**: Avoid CapEx by being global on day 1
- **Simplified management**: Unified control plane for all services, with no hardware management or network re-engineering required
- **Improved performance**: Optimized traffic routing avoiding congestion
- **Global threat response**: Cloudflare's network protects ~20% of the web, blocks 227 billion daily cyber threats, and uses AI to analyze global traffic patterns for real-time defense adaptation.

Global network presence

Within ~50ms of 95% of the world's Internet population

Proven track record

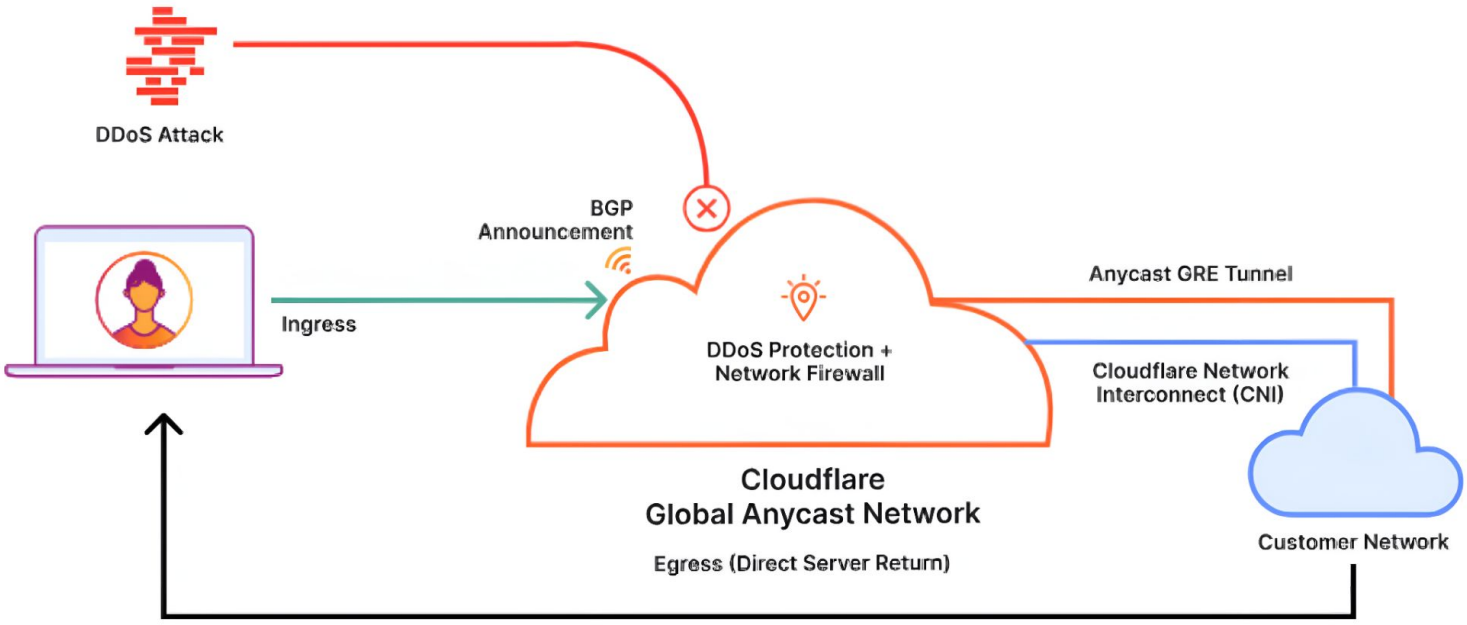
Protecting millions of Internet properties plus 35% of the Fortune 500

Continuous innovation

Cloudflare network services backed by 100% uptime SLA

Cost-effective consolidation

Replace multiple point solutions with a single, integrated platform



Why Cloudflare?

Every data center, every service

Process traffic as close to the source as possible to reduce the workload on your firewalls

Single-pass, multi-layer protection

Avoid unwanted latency and build resiliency using Cloudflare's global Anycast network

Direct connection to Cloudflare

Bypass the public internet and connect directly using our Network Interconnect

Learn more

Cloudflare Magic Transit protects network infrastructure, data centers, and public cloud services against DDoS attacks and other malicious traffic.

Watch the demo

Download the Network Protection whitepaper

Learn about the challenges of securing public-facing network infrastructure and the limitations of firewall helpers

Download

Additional resources

- Webinar: 'A farewell to legacy firewall helpers: Getting the protection your network deserves'
- Reference Architecture: https://developers.cloudflare.com/reference-architecture/architectures/magic-transit/