

网络保护

利用 Cloudflare 的全球连通云保护面向公众的基础设施

问题：在安全性和性能之间权衡

面向公众的基础设施面临安全漏洞，因其可在互联网上访问而成为各种攻击的目标。威胁行为者可以扫描可发现的服务，利用未修补的漏洞，并在安全团队做出反应之前发起毁灭性的 DDoS 攻击，造成经济损失。

企业已部署大量防火墙辅助工具和网络设备，但这些工具往往会造成效率低下，同时在面对复杂威胁时仍然无法提供有效防护。

解决方案：网络保护

使用 Cloudflare [全球连通云](#) 增强企业网络，简化架构并使其更加安全。通过启用云交付的服务来轻松添加功能，而无需插入设备，借助一个同时满足当前需求和未来新场景的平台，支持您的网络现代化转型。

Cloudflare 全球覆盖的一次通过安全防护，包括针对容量耗尽、协议或应用层攻击的多层保护，以及有关网络状态、行为和性能的可见性。

恶意流量

网络侦察、端口扫描、漏洞利用

容量耗尽攻击

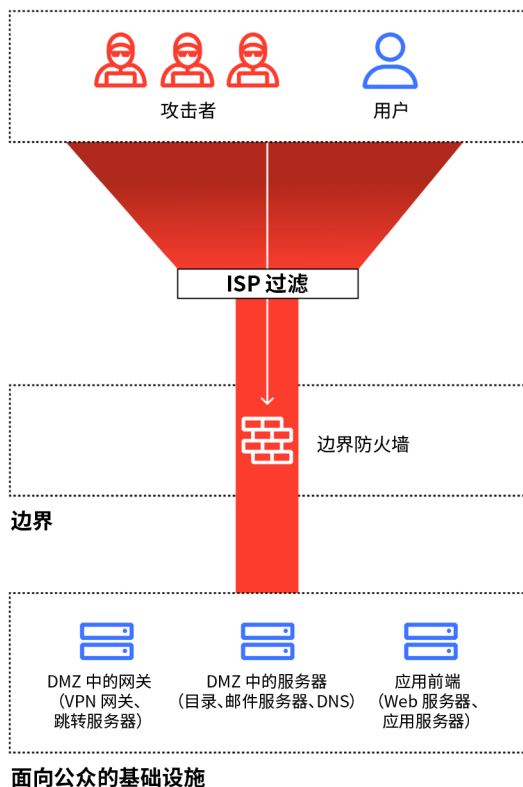
僵尸网络、流量洪水、分布式拒绝服务

协议攻击

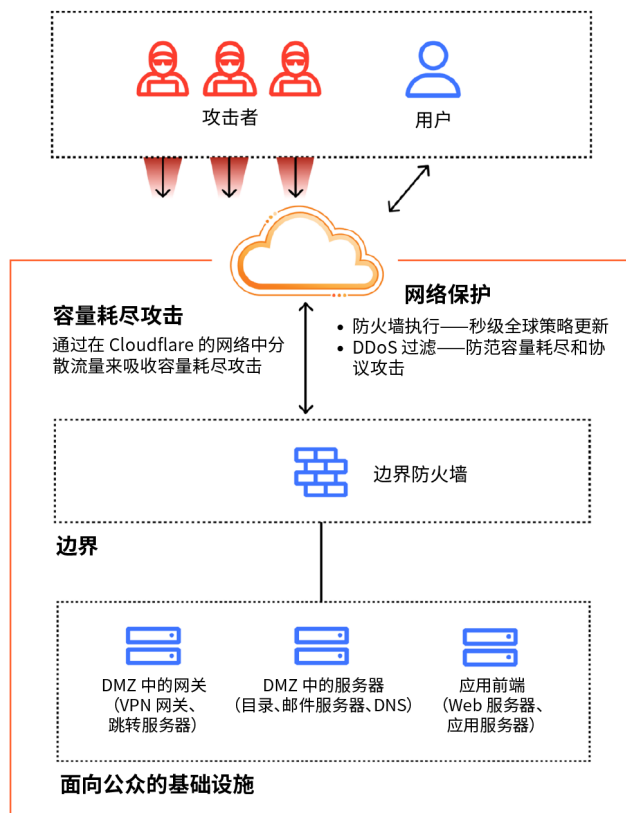
SYN 洪水，DNS 放大，ICMP 洪水

应用层攻击

XSS, HTTP 协议攻击 / Rapid Reset, API 滥用



部署 Cloudflare 网络保护后



工作方式

1. 通过 IPSec 隧道、GRE 隧道或使用 Cloudflare 网络互连 (CNI) 建立接入 Cloudflare Anycast 网络的流量路径
2. 通过 [Magic Transit](#) 和 [Magic Firewall](#) 以最少配置获得自动保护
3. 秒级全球策略部署

[详细了解](#)如何设计 Cloudflare 的架构以保护的您的现有网络基础设施。

优势

- **弹性资源**：从第一天起即实现全球部署，避免资本支出
- **简化管理**：所有服务通过统一控制平面管理，无需管理硬件或改造网络
- **性能提升**：优化流量路由，避免拥塞
- **全球威胁响应**：Cloudflare 的网络保护约 20% 的 Web 资产，每天阻止 2270 亿次网络威胁，并使用 AI 分析全球流量模式以实时调整防御。

全球网络覆盖

与全球 95% 互联网用户的延迟在 50 毫秒以内

经验证的成功记录

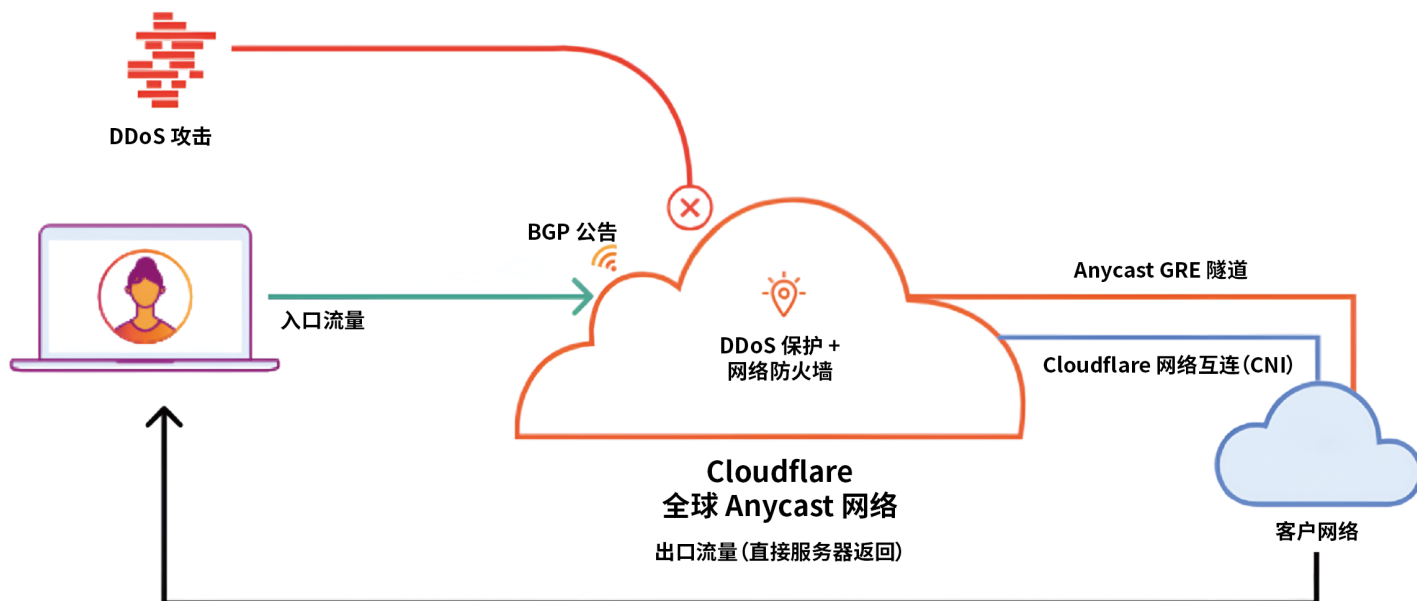
保护数百万个互联网资产，覆盖 35% 的财富 500 强企业

持续创新

Cloudflare 网络服务提供 100% 可用性 SLA

高性价比整合

以单一集成平台取代多个单点解决方案



为什么选择 Cloudflare?



每个数据中心，每项服务

尽可能靠近源头处理流量，以减少防火墙的负担



单次通过，多层保护

使用 Cloudflare 的全球 Anycast 网络避免不必要的延迟并打造韧性



直连 Cloudflare

绕过公共互联网，使用我们的网络互连能力直接接入

请求演示

欢迎观看导览演示，体验 Cloudflare 的网络防护工作实况。

[请求演示](#)

下载网络保护白皮书

了解保护面向公众的网络基础设施面临的挑战，以及防火墙辅助工具的局限性

[下载](#)

其他资源

- 网络研讨会：[“告别传统的防火墙辅助工具：为您的网络获得应有的保护”](#)
- 参考架构：<https://developers.cloudflare.com/reference-architecture/architectures/magic-transit/>

