Cloudflare Magic Transit

適用於現場部署、雲端託管和混合網路的 DDoS 保護

保護網路基礎結構免受 DDoS 攻擊需要力量與速度的特殊組合。巨流量攻擊能夠輕鬆淹沒硬體工具及其頻寬受限的網際網路連結。大多數基於雲端的解決方案將流量重新導向到集中式的流量清理中心 (scrubbing center)，而這會大幅影響網路效能。

Cloudflare Magic Transit 為內部部署、雲端和混合網路提供 DDoS 保護和流量加速。憑藉遍布 275 個城市的資料中心和超過172Tbps的緩解容量，Magic Transit 能在接近源頭的位置偵測和緩解攻擊，全球平均用時不到 3 秒，而且流量路由速度比公用網際網路更快。

Cloudflare 的優勢

在 DDoS 緩解受認可的領導者

頂尖的分析師研究公司 一致將 Cloudflare 排名為 DDoS 緩解的領導者，因為 Cloudflare 素來擁有阻擋所有規模攻擊的能力，還具備各種獨特的架構、快速導入和精細的控制功能。

具備整合效能的穩健安全性

Magic Transit 會在 Cloudflare 網路中的所有伺服器上以即服務執行；也就是說，不需要將流量分流至會導致延遲的清理中心。更棒的是，透過 Cloudflare 網路路由的流量會因為路由速度比公有網際網路更快而受益。

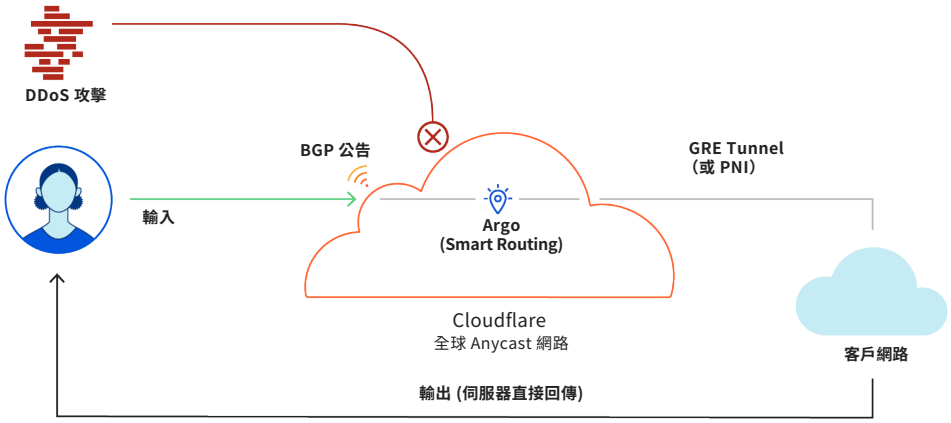
透過結合 DDoS、WAF、CDN、機器人緩解等功能，降低 TCO

我們的網路安全效能和可靠性功能建置在遍佈超過 200 個城市的相同全球 Anycast 網路上，旨在順暢整合且能夠從相同儀表板進行管理。不需要任何資本支出，就能夠輕鬆透過提升的操作靈活度來部署網路安全與效能功能。

功能比較	Cloudflare	其他
使用 BGP 和 BYOIP	✓	✓
透過 GRE 返回流量	✓	✓
全球網路 > 90 Tbps 網路容量	✓	✗
亞秒級威脅偵測和 TTM < 3 秒	✓	✗
綜合效能優勢	✓	✗
L3/4/7 產品的原生整合	✓	✗
內建第 3 層防火牆	✓	✗

+ 886 8 0185 7030 | enterprise@cloudflare.com | www.cloudflare.com

Magic Transit 的運作方式



1. 連線

使用邊界閘道通訊協定 (BGP) 將公告路由到網際網路和 Cloudflare 的 Anycast 網路，在最靠近來源的 Cloudflare 資料中心處接收客戶流量。

2. 保護和處理

檢查所有客戶流量是否存在攻擊。在偵測到攻擊時立即套用先進的自動緩解技術。負載平衡、下一代防火牆、內容快取和無伺服器運算等其他功能也以即服務提供。

3. 加速

乾淨的流量透過 Cloudflare 的網路進行路由，以獲得最佳輸送量，並透過 Anycast GRE 通道、私人網路互連 (PNI) 或其他形式的對等連接切換到原始網路。

Cloudflare 協助保護 Web 資產、應用程式和整個網路免受 DDoS 攻擊。如需更多資訊，請造訪 cloudflare.com/magic-transit

大規模威脅情報

Cloudflare 的 DDoS 保護借助我們全球網路的情報，能夠保護數百萬個網站。這種涵蓋範圍提供了獨一無二的優勢，讓我們能夠在全球範圍內部署機器學習，持續不斷地抵禦最新、最複雜的攻擊。

以自訂方式分析自有資料

網路分析使您可以透過Cloudflare的儀表板或 GraphQL API 分析 DDoS 事件。獲得對網路層和傳輸層流量模式及遭封鎖之 DDoS 攻擊近乎即時的洞察能力。

彈性的部署選項

Magic Transit 可透過隨需和永遠連線的選項提供。有了 Cloudflare，您就不需要擔心上述任一選項會增加延遲，因此可以挑選最符合您網路架構的選項。