

網路保護

使用 Cloudflare 的全球連通雲保護面向公眾的 基礎架構

問題:安全性和效能之間的權衡

面向公眾的基礎架構因具備網際網路可存取性,成為了各類攻擊的目標,從而面臨多種安全漏洞威脅。威脅執行者可以掃描可發現的服務、利用未修補的漏洞,並發起毀滅性的 DDoS 攻擊,在安全團隊得以做出回應之前造成財務損失。

組織已經部署了大量的防火牆協助程式和網路設備,但 這些措施通常會導致效率低下,同時仍然無法抵禦複雜 的威脅。

解決方案:網路保護

透過使用 Cloudflare 的全球連通雲擴充您的網路,簡化您的架構並提高安全性。透過啟用雲端交付的服務(而不是插入設備)輕鬆新增功能,並藉助一個同時滿足當前需求與未來新應用場景的平台,推動網路現代化進程。

Cloudflare 透過單遍實施提供全球覆蓋,其中包括針對巨流量、通訊協定或應用程式層攻擊的多層保護,以及對網路狀態、行為和效能的可見性。

之後:Cloudflare 網路保護

惡意流量 2 偵察、連接埠掃描、 漏洞利用 巨流量攻擊 殭屍網路、流量洪水、 分散式阻斷服務 ISP 篩選 通訊協定攻擊 Svn 洪水、DNS 放大、 週邊防火牆 ICMP 洪水 邊界 應用程式層攻擊 XSS、HTTP 通訊協定攻擊/ DMZ 中的閘道 DMZ 中的伺服器 應用程式前端 (VPN 閘道、跳板機) (Web 伺服器 快速重設、API 濫用 伺服器、DNS) App 伺服器) 面向公眾的基礎架構

使用者 網路保護 巨流量攻擊 可在幾秒內完成全域原則更新的 透過在 Cloudflare 網路中散佈 防火牆強制執行 流量來化解巨流量攻擊 針對巨流量和通訊協定攻擊的 DDoS 篩選 週邊防火牆 邊界 DMZ 中的閘道 DMZ 中的伺服器 應用程式前端 (Web 伺服器 (VPN 閘道、跳板機) 伺服器、DNS) App 伺服器) 面向公眾的基礎架構

運作方式

- 1. 透過 IPsec VPN 通道、GRE 通道或使用 Cloudflare 網路互連 (CNI) 建立到 Cloudflare Anycast 網路的流量路徑
- 2. 透過 Magic Transit 和 Magic Firewall 以最少的設定獲得自動保護
- 3. 數秒內在全球部署原則

深入瞭解如何部署 Cloudflare 以保護現有網路基礎架構。

優點

- 彈性資源:首日即享全球部署,免去資本支出
- **簡化管理:**所有服務採用統一的控制平面,無需進行硬體管理或網路重新設計
- **提高效能:**最佳化流量路由,避免壅塞
- 全球威脅回應: Cloudflare 的網路保護約 20%的 Web 流量,每日 封鎖 2270 億次網路威脅,並使用 AI 分析全球流量模式以進行即時 防禦調整。

全球網路覆蓋

在約50毫秒內連線至全球95%的網際網路人口

可靠的追蹤記錄

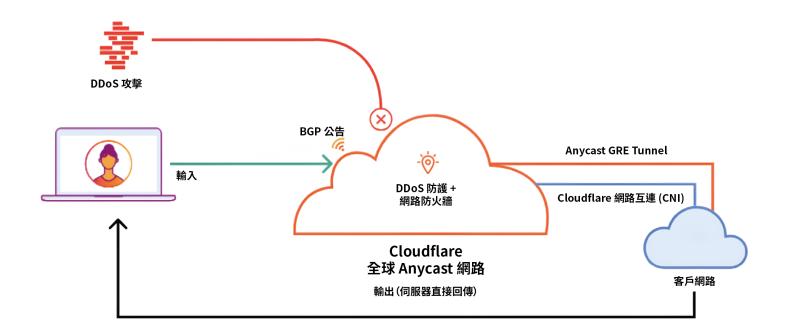
保護數百萬筆網際網路內容以及 35%的《財星》500強企業

持續創新

Cloudflare 網路服務提供 100% 正常運作時間 SLA 的保證

經濟高效的整合

使用單一整合式平台取代多個單點 解決方案



為什麼選擇 Cloudflare?



每一個資料中心提供每一項服務

在盡可能靠近來源的位置處理流量, 以減少防火牆的工作負載



單遍多層防護

使用 Cloudflare 的全球 Anycast 網路 避免不必要的延遲並建立韌性



直接連線至 Cloudflare

繞過公用網際網路,直接使用我們的 網路互連進行連線

請求示範

透過引導式即時示範,即時瞭解 Cloudflare 的網路保護。

請求示範

下載《網路保護》白皮書

瞭解保護面向公眾的網路基礎架構所面臨的挑戰, 以及防火牆協助程式的局限性

下載

其他資源

網路研討會: 「告別傳統防火牆協助程式:為您的網路提供應有的保護」

● 参考架構:https://developers.cloudflare.com/reference-architecture/architectures/magic-transit/

