

Cloudflare Magic Transit 既保護網路，又提升效能

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。憑藉遍佈 200 個城市的資料中心和超過 51 Tbps 的 DDoS 緩解容量，Magic Transit 能在接近源頭的位置偵測和緩解攻擊，平均用時不足 3 秒，而且還附帶了效能方面的效益。

本文將展示對我們網路執行的 [Catchpoint](#) 測試的結果，以量化 Magic Transit 對延遲的影響。測試結果表明，當流量透過 Cloudflare Magic Transit 路由時，測試客戶的網路效能 (延遲和封包遺失) 得以改善。具體而言，我們在測試結果中發現，流量透過 Magic Transit 路由時延遲縮短了 3 毫秒，封包遺失則幾乎為零。

Cloudflare Magic Transit 如何做到在不影響效能的前提下保護網路基礎結構？

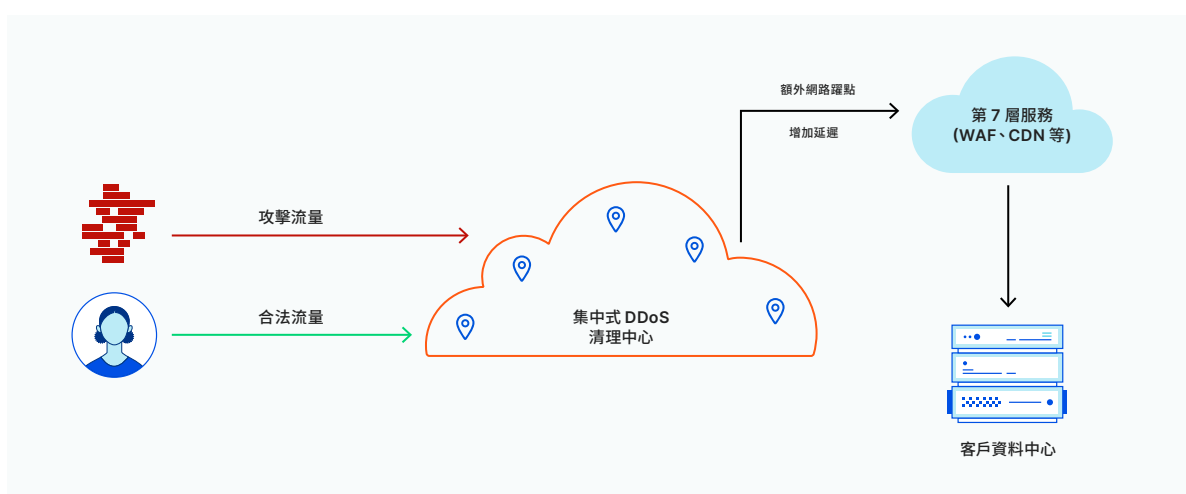
在 Magic Transit 誕生之前，保護網路基礎結構免受 DDoS 攻擊的策略主要有兩種：內部部署硬體 DDoS 防護設備和雲端清理解決方案。

在一定程度上，內部部署硬體設備可以妥善地保護您的基礎結構。但這些設備的頻寬有限，可能會被規模較大或同時發生的攻擊壓垮。硬體還需要大量前期投資，並耗費大量資源來管理和維護。

雲端清理中心應運而生，提供了一種更簡單的替代選擇：使流量經由清理中心進行路由，並在清理中心篩選掉攻擊流量。這解決了內部部署硬體引起的財務負擔和維護難題。

然而，這也造成了新的問題：顯著的延遲。

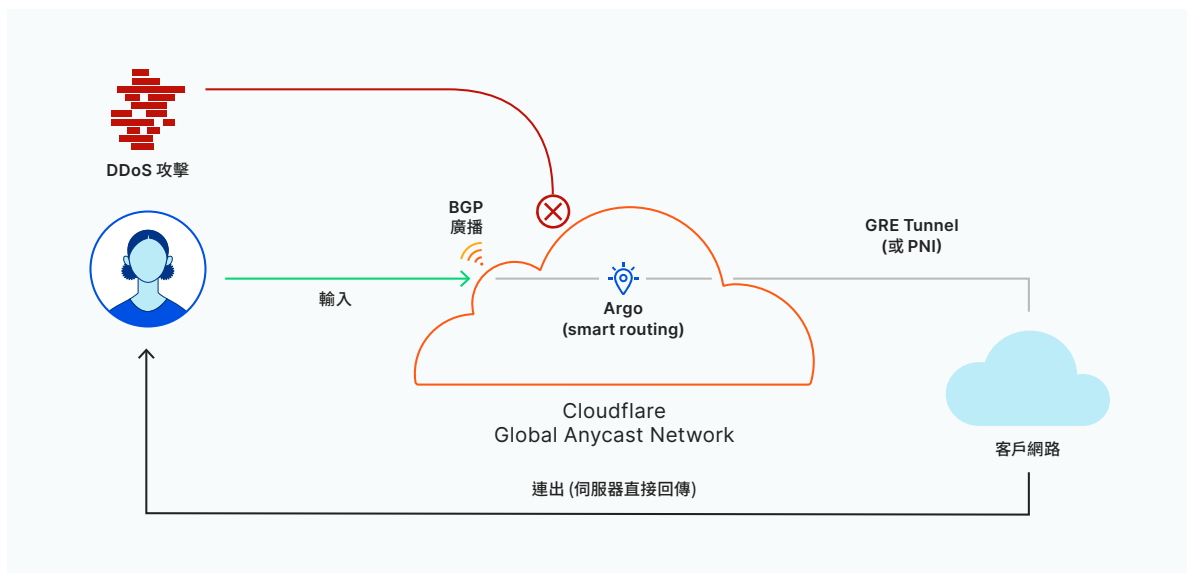
由於這些雲端提供者的清理中心數量有限，並且分散於不同的地理位置，因此流量可能必須傳輸很長距離進行清理，然後才能到達最終目的地。雲端提供者通常只有屈指可數的清理中心，如果您或最終使用者與所有清理中心都相隔甚遠，即使最終目的地就在附近，流量也必須傳輸很長一段距離。這是所謂的長號效應，通常會引起明顯且惱人的延遲。(之所以稱為「長號效應」，是因為如果您在地圖上標出路途較長的往返路線，就能看到這條路線的形狀很像長號)。



「清理中心」距離遠、數量少，專門用於緩解 DDoS。這需要網路流量傳輸到備用資料中心，以進行額外的 L4-7 處理，導致更多的延遲。

假設在上述情境中，您需要在第 3-4 層以及第 7 層服務 (例如 WAF 和 Bot Management 等) 中處理流量。——這時，您的流量首先到達遙遠的 L3 清理中心在 L3 內緩解 DDoS，然後傳送到輔助資料中心以進行其他 L7 處理，這對點對點流量增添了網路躍點，增加了不必要的延遲。如果雲端供應商的清理中心數量有限，並且與網路流量的源頭相距很遠，那麼延遲就會特別明顯。

Magic Transit 帶來了更好的解決方案。我們不使用專門的清理中心，而是讓 Cloudflare 全球網路中的每個資料中心都能處理清理工作。實際上，每個 Cloudflare 資料中心都執行完整的 Cloudflare 服務堆疊。這樣一來，您的流量只需傳到最近的 Cloudflare 資料中心便可；我們在 100 多個國家/地區的 200 多個城市設立了資料中心，因此距離有可能會很近。

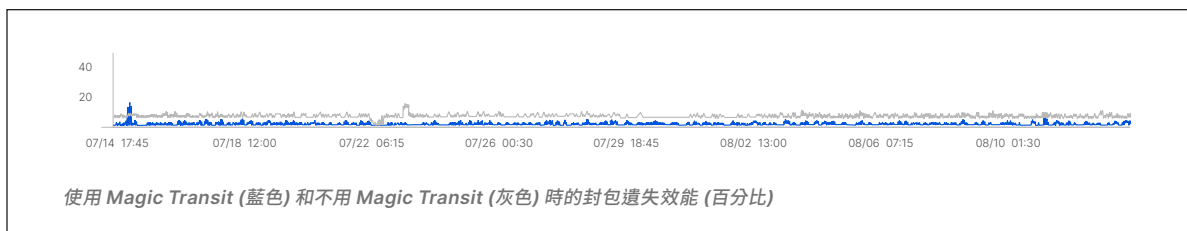
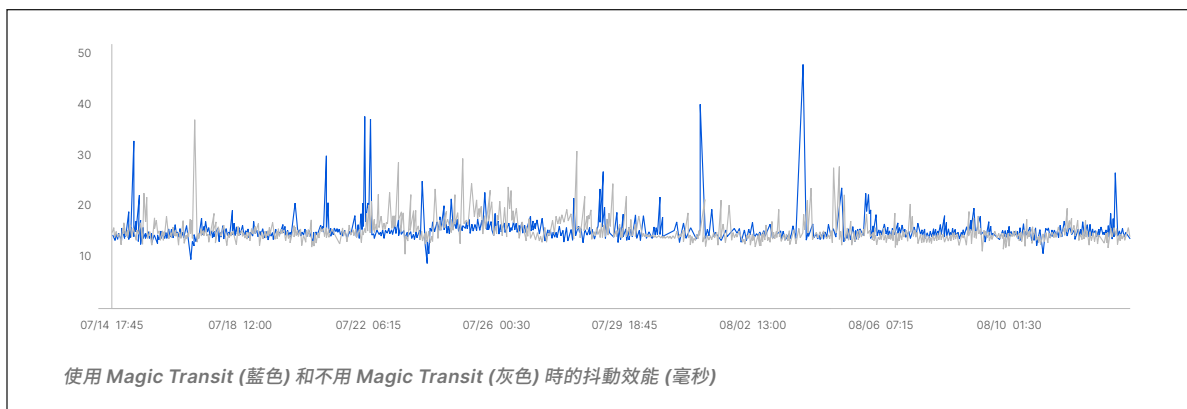
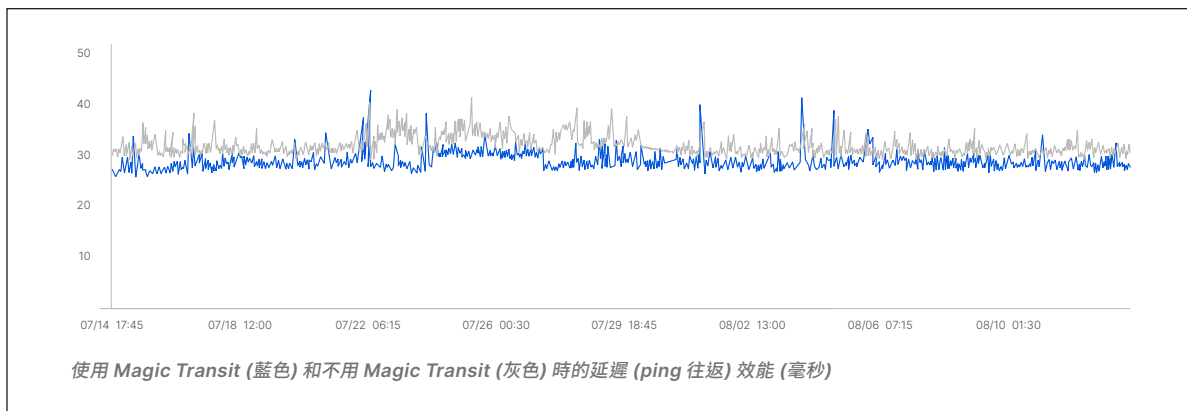


每個 Cloudflare 資料中心執行 L3-7 服務的完整堆疊，因此網路流量可在同一位置進行處理。

這表示，沒有長號效應，延遲也很短。網路效能是我們開發 Magic Transit 的首要顧慮事項；我們想確保使用者不必為了安全性而犧牲效能。

Catchpoint 測試

為了驗證這一點，我們使用 Catchpoint 進行了一些測試，以判斷使用 Magic Transit 對整體網路效能的影響。透過全域散發探針，我們對位於 Magic Transit 後方的 IP 位址和不用 Magic Transit 的另一個位址執行 ICMP ping 測試，這兩個位址都託管在同一網路基礎結構上。這樣，我們能夠同時測量延遲、封包遺失和抖動，以查看效能差異。



在上述測試中，藍線代表使用 Magic Transit 時的效能，灰線則代表不用 Magic Transit 時的效能。

測試結果

效能	使用 Magic Transit (藍色)	不用 Magic Transit (灰色)
延遲	28.96 毫秒	31.98 毫秒
抖動	28.96 毫秒	28.96 毫秒
封包遺失	0.52%	5.26%

從這些測試中得出的重要結論

- 使用 Magic Transit 時延遲縮短了 3 毫秒
- 使用 Magic Transit 時抖動增加了 0.36 毫秒
- 使用 Magic Transit 時封包遺失幾乎為零 (0.52%)，而不用 Magic Transit 時則為 5.26%

這些結果代表什麼？

延遲：延遲是封包從網路上的一個點傳輸到另一點所花費的時間。在我們的測試中，我們觀察到 Cloudflare 網路的延遲較低。

Cloudflare 根據不同網路路徑的狀態不斷最佳化流量路由，因此封包從 Cloudflare 到客戶網路的傳出路徑效率通常高於那些未經 Cloudflare 最佳化的封包。

這可確保網路延遲不會延長，而且如我們的測試結果所示，許多情形中甚至可以縮短。這對於對延遲敏感 (即時) 的應用程式尤為重要，例如線上遊戲和 IP 語音 (VoIP) 服務。

抖動：網路抖動是指網路上封包傳遞之間的延遲量。減少抖動對於 VoIP 等應用程式尤其重要。使用 Magic Transit 時，抖動增加了 0.36 毫秒。即使對抖動敏感的應用程式，這也可以忽略不計。

封包遺失：網路傳輸中若有一個或多個封包未能到達目的地，就會發生封包遺失。根據具體的通訊協定，封包遺失可能需要花費額外時間來重新傳輸，或者導致品質下降。對於像視訊會議這樣對時間極為敏感的傳輸，封包遺失率低於 1% 被認為可以接受*。在我們的測試中，我們觀察到 Cloudflare 網路上的封包遺失率幾乎降到了零 (相比之下，不用 Magic Transit 時的封包遺失率超過了 5%)

總之，Magic Transit 對延遲、抖動和封包遺失的影響不會損害使用者體驗，而且在許多情況下甚至還能改善體驗。換言之，Cloudflare 客戶在使用 Magic Transit 時不必為網路效能「權衡取捨」而操心。

此外，Cloudflare Magic Transit 可與 Cloudflare 的所有安全性、效能和可靠性產品整合，進一步最佳化國際網路設備的效能。

若要瞭解有關 Cloudflare Magic Transit 的更多資訊，請瀏覽 www.cloudflare.com/magic-transit 或透過以下地址聯絡我們：sales@cloudflare.com

*<https://web.archive.org/web/20131010010244/http://sdu.ictp.it/pinger/pinger.html>

© 2021 Cloudflare, Inc. 並保留一切權利。Cloudflare 標誌是 Cloudflare 的商標。
所有其他公司與產品名稱可能是各個相關公司的商標。