白皮書

最佳化中國的網站效能與安全性

探索規模龐大、複雜且快速成長的中國網際網路經濟的策略

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

報告摘要

中國擁有世界最多的連網人口。然而網路的複雜性以及始終存在的網路攻擊威脅，提高進入這個市場的困難度。為協助企業組織解決這些困難，並優化中國使用者的網站使用經驗，Cloudflare 已將其全球效能和安全性網路服務無縫擴展到中國。

在中國拓展線上業務的挑戰

中國規模巨大且快速成長的線上經濟，使其成為眾多企業組織想進入的潛力市場。連線至網際網路的中國公民超過十億，是全球網民最多的國家，其中超過 8.12 億人在 2021 年上半年進行了網購。這段時間內的整體線上購物支出與前年相比稍微有下降趨勢，主要原因是出於 COVID-19（新冠肺炎）疫情所導致的不穩定狀況，然而中國經濟在後疫情時代仍呈現兩位數成長，而電子商務市場在 2020 年成長 12.5%。

與進入任何區域性市場一樣，跨國企業要在中國營運必須調整自家服務和線上體驗，以符合當地文化和期望。然而中國的網際網路監管政策、底層基礎結構和威脅狀況都帶來各種特殊挑戰，使得想要提供符合當地消費者期望之優質體驗服務的跨國企業打入市場難上加難。挑戰包括：

- 因網際網路瓶頸和品質不佳的本地點對點連線導致的延遲
- 行動網站效能折損
- 持續性國內網路攻擊

這份白皮書中會詳細說明這些挑戰，闡述克服挑戰的因應策略，展示 Cloudflare 可如何提供幫助。

因網際網路瓶頸和品質不佳的本地點對點連線導致的延遲

和許多消費者一樣，中國民眾對線上體驗抱有很高的期望。根據滙豐銀行 (HSBC) 的報告，中國在全球電子商務市場處於領先地位並佔據主導地位。根據 business.com 的分析，中國是全世界最大的電子商務市場。

遺憾的是，組織往往難以讓他們的網站快速且可靠地為中國使用者提供服務。

其中一個原因是網路瓶頸。所有進出中國的網際網路流量，皆需經過三個網際網路交換點 (IXP) 中的一個：分別位於北京、上海或廣州。在高峰使用時段，這些 IXP 可能會壅塞並大幅增加中國境外託管網站的載入時間。在一系列測試中發現 TED 網站在上海網路瀏覽高峰時段，第一次載入時間需要長達 8 到 38 秒，而相同時段在紐約只需要 5 到 8 秒。

為避免此類瓶頸，部分跨國公司選擇將他們的網站託管在最靠近的中國三個 IXP 之一的資料中心中（例如：香港網站最靠近廣州 IXP）或是中國境內的伺服器上。不過這些方法仍會面臨另一個重大網路挑戰：品質不佳的且數量有限的本地網際網路服務提供者 (ISP)。

熟悉中國網際網路狀況的公司可能已經很清楚主導市場的三家國有 ISP：中國電信、中國移動和中國聯通。每家 ISP 分別主導中國境內不同區域，同時也參與相對弱的點對點連接，或透過 IXP 與個別網路連線。一份 2017 年的 Mlytics 調查研究發現，相較於北美的 66 個以及歐洲的 71 個，中國最多點對點網路僅連線至兩個 IXP。

這意味著即便是國內的網際網路也必須覆蓋較長的網路距離，以便途經相對短的地理距離，這會導致使用者出現更長的延遲。

如何克服瓶頸和品質不佳的本機對等

面對這些 Web 效能挑戰，許多在中國開展業務的跨國企業選擇使用內容傳遞網路 (CDN) 在靠近終端使用者的資料中心中快取靜態（或非特定於使用者的）網站內容，如此一來大多數的請求便不需傳回來源伺服器。組織對於 CDN 的考量：

- **擁有大型且優質對等網路。**CDN 的資料中心數量越多，就能距離終端使用者更近。並且當中國的三個主要 ISP 對 CDN 的覆蓋範圍更廣時，也會減少終端使用者的請求需要經歷的網路躍點。
- **能在中國境內解析 DNS 查詢。**如果流量必須出入中國，即使已本地快取網站內容，DNS 解析過程（將網域名稱轉成 IP 位址的過程）也會增加延遲。
- **最小化使用網站 HTML、CSS 和 Javascript 程式碼。**這些程式碼類型是大多數網站使用的建置區塊，用於將網站外觀告知終端使用者的瀏覽器。極簡化是指將不必要的字元從程式碼中移除的過程，目的是縮小網站整體大小——進而在通過網路時減少頻寬使用；頻寬越小代表網站的載入速度會更快。
- **在網路邊緣使用無伺服器程式碼，建立自訂規則來回應請求。**無伺服器程式碼是一種不侷限於開發者控制特定伺服器的程式碼。當無伺服器程式碼在網路邊緣執行時，無伺服器程式碼存在於資料中心的整個大型網路中，這代表此類程式碼可以輕鬆且快速地將規則套用至特定終端使用者。例如：組織可以在中國網路上編寫無伺服器程式碼，針對行動使用者、慢速網際網路連線和許多其他使用案例強制執行特殊規則。

Cloudflare 網路與京東雲的夥伴關係連同我們的全球效能服務，有助於客戶流量瓶頸和品質不佳的點對點連線挑戰。請跳至此白皮書的下個章節瞭解方式詳情。

持續性國內網路攻擊

與在其他地區一樣，在中國經營網站也會面臨各種網路安全威脅。

其中一種威脅便是分散式阻絕服務 (DDoS) 攻擊，利用大量垃圾流量轟炸伺服器或網路基礎結構，使其無法回應合法請求。Talos Intelligence 2017 年的一份報告中發現，國內的受雇型 DDoS (DDoS-for-hire) 服務（能讓非專家使用者透過包含受感染裝置的現有殭屍網路輕鬆發動攻擊）正在中國快速蔓延。

自那時起，中國執法部門機關已關閉數個主要 DDoS 殭屍網路，其中包含一個在 2019 年感染超過 20 萬台裝置並發動高達 200 Gbps 流量攻擊的殭屍網路。然而其他殭屍網路仍在運作中——例如 DoubleGuns，截至這份報告發表，其背後經營者依舊逍遙法外。

中國境內網站同時必須避免試圖存取私人資料和開發環境。2018 年曾有攻擊者利用常見 PHP 架構的漏洞，試圖存取超過 4 萬 5 千個中文網站的伺服器。攻擊在發現架構漏洞不到 24 小時即刻發動。2020 年兩名中國籍攻擊者因非法存取數百家公司私人網路遭到起訴，判刑長達十年，也是利用各種 Web 應用程式漏洞發動攻擊。

此外，想在中國境內保護私人資料的組織可能無法使用一般常用的方法，因為中國網路不支援現代加密標準（例如 TLS 1.3 和加密伺服器名稱指示 (ESNI)），讓未經授權的觀察者有更多機會窺探流量。

如何在中國防禦持續性國內網路攻擊

全世界日益增加的 DDoS 攻擊已使得 DDoS 防護服務和其他應用程式安全工具（如 Web 應用程式防火牆 (WAF)）成為所有營運中網站的必備安全要求，在中國也毫無例外。在中國市場尋找此類防護服務的組織應當考量：

- **從網路邊緣（而非受限的「清理中心」）進行 DDoS 防護。**僅管幾乎所有的現代 DDoS 防護服務都在雲端運作，仍有許多仰賴數量有限的資料中心來篩選，或者說「清理」惡意流量。將流量回傳至這些「清理中心」進行檢測會增加額外網路躍點，並因此導致延遲和對使用者的干擾，鑒於中國的網路限制，此類延遲更加嚴重。在中國若想兼顧 DDoS 防護和網際網路效能，企業組織應考量既不會增加額外網路躍點，又能在每個邊緣資料中心提供 DDoS 防護的雲端服務。
- **限速以封鎖濫用。**必須進行精細控制，以緩解高精度第 7 層 DDoS 攻擊，阻止 API 濫用以確保可用性，保護敏感的客戶資訊免受暴力登入攻擊，並保護原始伺服器免於資源耗盡，同時避免因流量暴增而產生的不可預測的成本。

- **能夠自動更新且十分快速的 WAF。**中國境內的攻擊者已證明他們有能力快速利用新的 Web 應用程式漏洞。企業組織大多希望能夠建立自有的 WAF 規則，但不應大幅仰賴自家威脅情報和能力來進行更新。企業組織應考慮採用 Web 應用程式防火牆，它能根據觀察到的大量威脅集區自動更新；而當企業組織想要進行自己的規則更新時，也能充分相信這些變更能夠盡快散播。
- **可自訂加密選項。**要在沒有 TLS 1.3 和 ESNI 的情況下保護傳輸中的資料，組織應當考慮可提供更多可自訂加密方法選項的安全服務。

Cloudflare 的安全服務是我們中國網路的一部分，提供零延遲 DDoS 防護以及能取得全球威脅情報的快速更新 WAF。請跳至此白皮書的下個章節瞭解詳情。

Cloudflare 如何支援在中國經營跨國網站

Cloudflare 運營的資料中心網路遍佈全球 100 多個國家/地區的 200 多個城市。截至 2022 年 3 月，已有 45 個資料中心遍及中國 38 個城市。每個資料中心都提供大量網路安全、效能和可靠性服務，包含內容傳遞、DNS 解析、DDoS 緩解、WAF 強制執行、無伺服器程式碼執行等眾多服務。由於每項服務是在單一資料中心中運作，因此可以近距離服務終端使用者——協助減少延遲，讓我們的網路對最新安全威脅和網路狀況能有詳細、最新的瞭解掌控。此外，組織可以從單一儀表板集中管理所有服務。

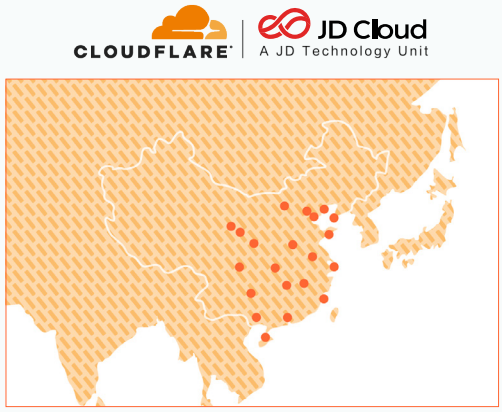
自 2015 年起，Cloudflare 已協助多家企業組織為中國訪客提供安全、快速且可靠的網際網路體驗。為了更進一步改良這些服務，我們近期已開始與京東雲 (中國網際網路巨人 JD.com 的雲端智慧科技事業部門) 建立夥伴關係。

下面將介紹此網路如何協助組織克服上個章節中講述的挑戰。

Cloudflare 如何幫助克服延遲

Cloudflare 與中國的京東雲網路可攜手提供：

- **Argo Smart Routing：** 將資料從用戶端傳送到原點並傳回會導致延遲。運用快取，靜態內容可以避免網路擁塞，但動態內容依賴於網際網路的可用性、可靠性和效能。這可能會導致載入緩慢、逾時、連線中斷和終端使用者體驗降級。**Argo Smart Routing** 具有獨特功能，**可即時偵測擁塞**並透過**最快且最可靠的網路路徑路由 Web 流量**。Cloudflare 客戶及其使用者對 Cloudflare 網路的請求有助於我們瞭解網際網路的不同部分在任何給定時間的效能。Argo Smart Routing 使用 Cloudflare 收集的計時資料，**將流量沿最快路徑動態路由回原點，**從而提高效能。平均而言，Argo 將 Web 資產效能提高約 30%。這隨後將提高您的銷售額和回客率。
- **可從中國境內的多個資料中心快取和提供靜態內容**，降低延遲時間並加速頁面載入時間——無論使用者身在何處。我們的網路與中國的 ISP 密切互連，減少必要的網路躍點流量。



中國大陸資料中心

- **可選中國境內的 DNS 解析**，同樣可以加快回應速度。
- 使用**網際網路通訊協定版本 6** (IPv6) 的能力，可提升路由和封包處理的效率。
- 透過 Auto Minify 功能（在 Cloudflare 儀表板中選中相應方塊即可輕鬆啟用）**極簡化網站程式碼**的能力。
- 經由 Cloudflare Workers 服務（在我們的中國網路中的每個資料中心運作）提供的**無伺服器計算**，可讓您以自訂方式回應要求和擴充現有應用程式。甚至不需維護基礎架構即可建立全新的應用程式。

Cloudflare 如何幫助對抗持續性國內網路攻擊

與中國網路相整合的安全服務，可協助組織：

- **緩解 DDoS 攻擊。**我們在中國的每處資料中心皆可緩解攻擊，為網路提供巨大容量來吸收最強大的攻擊，同時不影響合法請求——並且不需仰賴 Cloudflare 在世界其他位置的資料中心。由於執行流量檢查的位置靠近使用者，可以免去使用者回傳流量至遠端「清理中心」的冗長程序。此外針對中國境內的網路挑戰，Cloudflare 提供獨特的自動化流量工程功能，可以自動重新路由攻擊流量。這些功能都是為了避免中國境內外的合法流量受到惡意流量的拖累。
- 利用 Cloudflare WAF **防禦 Web 應用程式漏洞**。除了透過受管理規則集（例如實施 OWASP 和 Cloudflare 專有規則）阻止已知的攻擊手段之外，WAF 還利用來自我們網路的持續威脅情報流來自動阻止最新威脅。此外，組織可以輕鬆建立自己的規則，並在幾分鐘內將其傳播到整個網路。2021 年所做的改進使 WAF 能夠更快地部署，並輕鬆擴展以覆蓋更多流量。WAF 還更新了規則集，透過將規則狀態與操作分開進行更好的控制。使用者現在可以透過進階篩選、大量編輯、規則標籤等更有效地瀏覽規則。
- **限速**與我們的 WAF 自訂規則整合，可防止 DDoS 攻擊、暴力登入嘗試、原始伺服器過載以及其他類型針對 API 和應用程式的濫用行為。使用者可以設定閾值、定義流量、自訂回應，並獲得有關特定網站 URL、應用程式或 API 端點的寶貴見解。
- **使用 TLS 1.2 加密資料**，並從 Cloudflare 儀表板輕鬆管理自有憑證。

瞭解更多

Cloudflare 中國網路服務向所有 Cloudflare Enterprise 客戶開放，並且完全符合中國法律與法規，包括中國網路服務上線必須獲得有效的網際網路內容提供者 (ICP) 授權。

隨著中國網際網路經濟持續成長，新的安全和效能挑戰勢必會浮現。Cloudflare 針對中國的持續成長作出規劃，將各公司放在我們網路上的適當位置，以便快速回應這些挑戰並持續提升順暢使用者體驗等級平。

聯絡 Cloudflare 立即開始最佳化您在中國的網路空間！

如需進一步瞭解 Cloudflare 中國網路，請造訪：cloudflare.com/network/china/，或與您的 Cloudflare 代表聯繫。