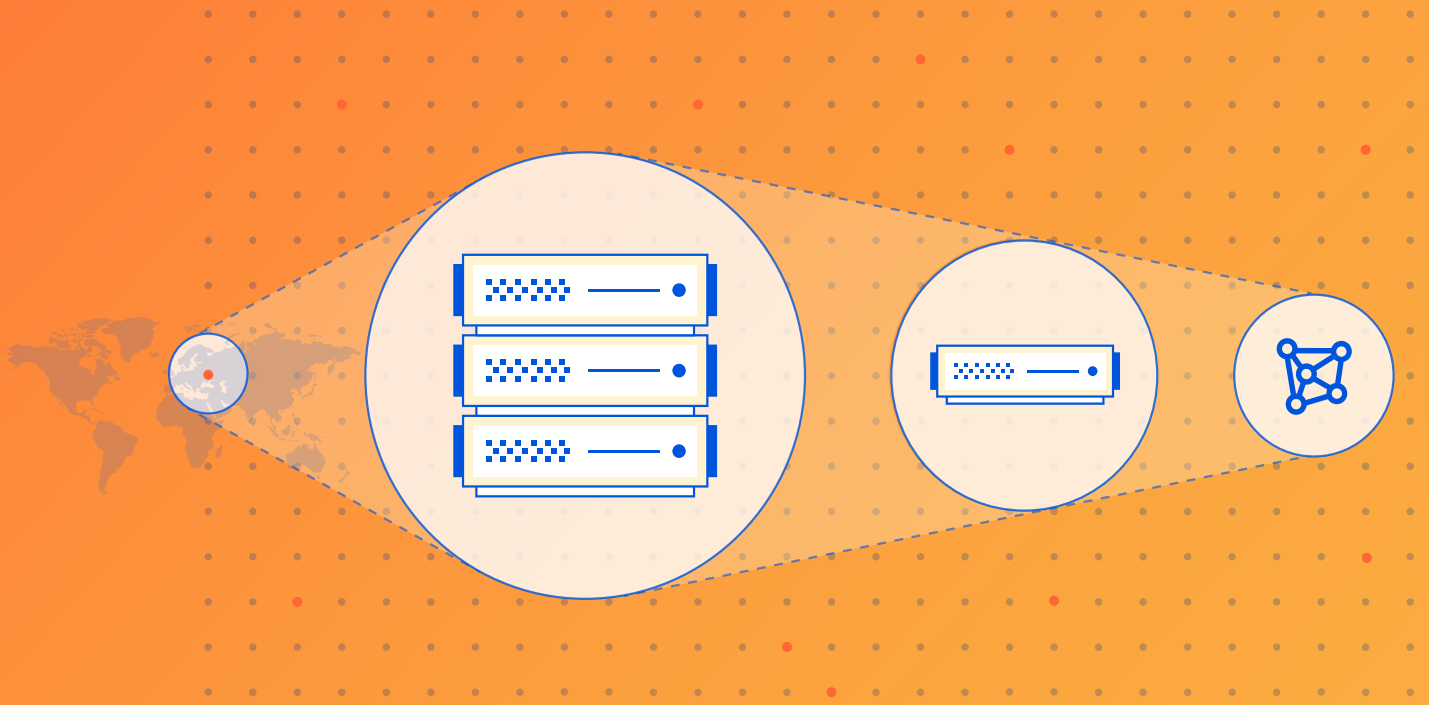
CLOUDFLARE

白皮書

DNS 和 DDoS 威脅



目錄

報告摘要

網域名稱系統 (DNS) 是一項重大創新，讓網際網路成為了可能。但今天，大規模機器人網路卻被用來發起更大規模的網路攻擊，這些攻擊或者使用 DNS 基礎架構，或者以 DNS 基礎架構為目標。

近年來，攻擊者透過針對 DNS 使用大規模的分散式阻斷服務 (DDoS) 攻擊，能夠摧毀基本服務和大面積的網際網路，讓大量的知名網站和組織遭遇了服務中斷。使用清理中心來消除惡意流量的傳統硬體型 DDoS 緩解服務無法擴展，進而無法在軍備競賽中擊敗基本免費的分散式機器人網路。

Cloudflare 認為架構是非常重要的，並且唯一能夠抵禦大規模分散式機器人網路的解決方案就是將大規模分散式網路與安全的 DNS 解析搭配使用。Cloudflare 就是基於這一架構方法提供服務的。

不斷增長的大規模攻擊對 DNS 構成了新的威脅度

2016 年 10 月 21 日，持續的大規模分散式阻斷服務 (DDoS) 攻擊影響了大部分的網際網路，導致幾十個知名網站及服務中斷或質量下降。該攻擊的直接目標是 Dyn，這是一個 DNS 服務提供者，可將網域名稱對應至網際網路通訊協定 (IP) 位址，以便流量能夠路由至特定的網站。該攻擊花了幾個小時才得以緩解。[1]

但這只是越來越多的極大規模 DDoS 攻擊的開始。在那以後的幾年裡，攻擊規模及範圍均有所擴大，最終爆發了有史以來規模最大的幾起網路攻擊。AWS 報告於 2020 年 2 月緩解了一起大規模 DDoS 攻擊。這次攻擊傳入流量的峰值速率達到 2.3 Tbps（太比特/秒）。[2] 2022 年 6 月，Cloudflare 緩解了一起每秒 2600 萬個要求的 DDoS 攻擊 — 這是截止當時有史以來規模最大的 HTTPS DDoS 攻擊。[3]

攻擊者何以能夠發起規模如此龐大的攻擊呢？

基於 IoT 和基於伺服器的大規模機器人網路

產生大規模攻擊的一個主要方式是透過接管保護不力的物聯網 (IoT) 裝置。Mirai 機器人網路可能是最知名的 IoT 裝置網路遭到惡意利用的例子。Mirai 的建立者入侵了 100,000 多個已連線的裝置（例如，家用路由器、智慧型家用小工具、監視攝影機或影像錄影機）來建立巨大的機器人網路，並使用該網路發起 Dyn 攻擊（以及其他攻擊），其流量最多可能達到 1.2 Tbps。

這一龐大的機器人網路讓 Dyn 不堪重負，針對依賴它的所有網站及應用程式關閉了 DNS 解析服務。

該機器人網路是使用惡意軟體 Mirai 建立的。Mirai 會掃描網際網路，尋找仍然具有原廠預設使用者名稱和密碼設定的裝置，然後即可輕鬆地加以感染、登入並控制裝置。而裝置擁有者除了偶爾的效能遲緩，並不會注意到裝置遭到入侵。

「假設一台裝置可以公開存取，則遭到駭客入侵的機率可能就是 100%。IPv4 位址空間並沒有那麼大。現在，您只需幾個小時就能對整個空間執行一次掃描，特別是在您有一個大型機器人網路的情況下。漏洞掃描從未間斷過，如果非要說有什麼不同，那就是在過去幾年內加速了。」

- Cloudflare CEO，Matthew Prince

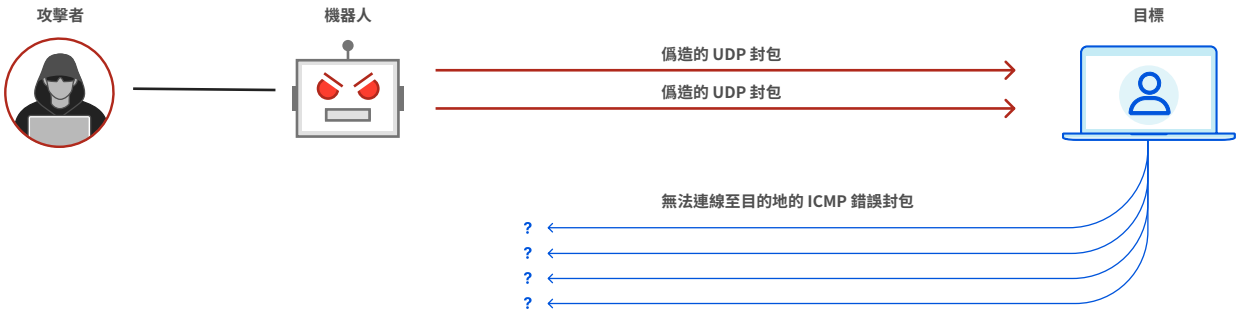
目前，Mirai 機器人網路仍是一種威脅，並且遠非唯一一個正在 DDoS 攻擊中使用的機器人網路：

- 2021 年 6 月首次偵測到了 **Meris 機器人網路**。儘管研究人員在該機器人網路中識別出至少 30,000 個機器人，但據信實際機器人數量更多。[4]
- **Mantis 機器人網路**使用遭劫持的虛擬機器以及功能強大的伺服器而非 IoT 裝置。這表示，每個機器人都有更多的計算資源，遠遠超出 Mirai 或 Meris 中的裝置數。該機器人網路能夠建立大規模 DDoS 攻擊，在部分情況下，可達到每秒 2600 萬個要求。[5]

利用 DNS 工作方式有兩種最常用的方法：DNS 放大（或「反射」）攻擊和 UDP 洪水攻擊。

不堪重負的 DNS 伺服器：UDP 洪水

UDP 洪水攻擊會將大量 UDP 封包傳送至目標伺服器，旨在擊垮該裝置的處理及回應能力。保護該目標伺服器的防火牆也會因 UDP 洪水攻擊而變得精疲力盡，導致阻斷為合法流量提供服務。



此類攻擊與 DNS 解析程式特別相關，這是因為所有 DNS 流量通常透過 UDP（而不是僅在區域傳輸等部分特定使用案例中使用的 TCP）來傳送。由於 UDP 不需要握手即可開啟連線，因此，可將大量垃圾 UDP 封包傳送至目標，然後該目標就會竭盡全力去回應每個封包。（例如，針對 Dyn 的 Mirai 攻擊是一個 UDP 洪水攻擊 — 當此類攻擊將 DNS 作為目標時，就可以將其稱為「DNS 洪水」。）

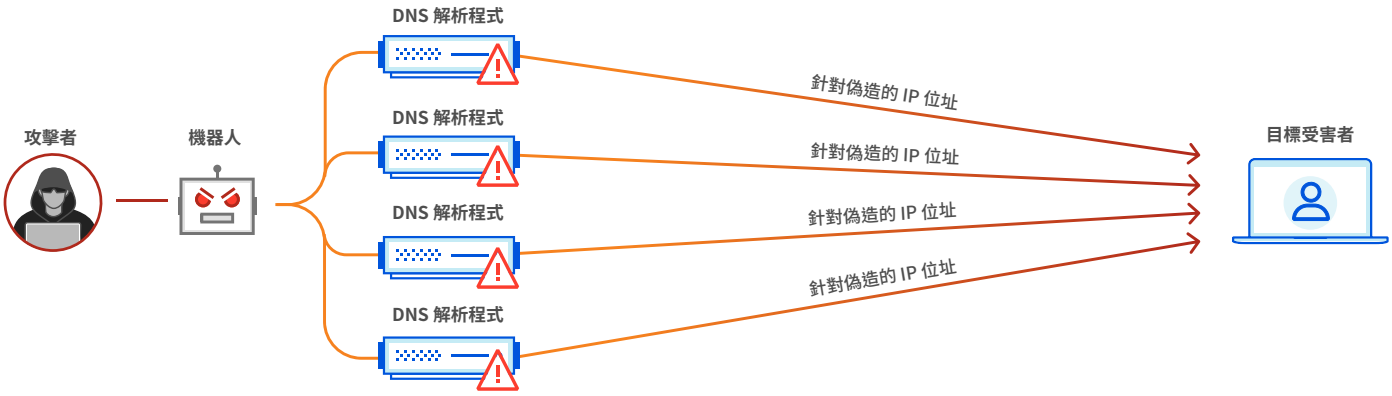
UDP 洪水的主要工作方式為：在伺服器回應傳送至其中一個連接埠的 UDP 封包時，入侵其採取的步驟。如果任何程式在該連接埠都未收到封包，則伺服器會使用 ICMP (ping) 封包進行回應，來通知傳送者無法連線至目的地。當伺服器收到每個新的 UDP 封包，它會完成這些步驟以處理要求，從而在這個過程中利用伺服器資源。由於目標伺服器利用資源來檢查每個收到的 UDP 封包，然後進行回應，因此，當收到大量 UDP 封包時，目標的資源就會快速耗盡。

利用 DNS 的工作方式：DNS 放大

除了直接對 DNS 服務提供者發起攻擊以外，攻擊者也可以將其基礎架構裝備成武器，並使用 DNS 的工作方式對其他服務提供者進行嚴重的 DDoS 攻擊。

DNS 放大攻擊會利用開放的 DNS 解析程式的功能，用放大的流量壓垮目標伺服器或網路。攻擊中的每個機器人不會直接針對受害者發起攻擊，而是使用欺騙性 IP 位址（已變更為目標受害者的實際來源 IP 位址）將要求傳送至開放的 DNS 解析程式。然後，目標會從 DNS 解析程式收到回應。

攻擊者會採取盡量從 DNS 解析程式產生大規模回應的方式，來建立要求。因此，目標會收到放大的攻擊者起始流量。網路安全和基礎結構署 (CISA) 估計，DNS 放大攻擊允許攻擊者傳送的流量最多為所傳送欺騙性封包之頻寬的 54 倍。[6]



DNS 放大是讓 Spamhaus 離線的 2013 年攻擊的關鍵部分，[7] 也在許多其他外部攻擊中有所使用。

雖然 DNS 解析程式不會直接對這些攻擊負責，但可以也應該防止對其系統進行此類入侵。具有自託管 DNS 的組織也會發現，他們的系統正在與其進行對抗，來摧毀其內部網路。

大規模 DDoS 攻擊對 DNS 解析程式及下游受害者的影響

遭遇 DDoS 攻擊的組織清楚地瞭解這些攻擊會造成深遠的負面影響，包括停機、失去業務、聲譽受損以及沉重的財務負擔。一位知情人士發現，平均而言，企業 DDoS 攻擊的總成本為 200 萬美元，而中小企業 DDoS 攻擊的成本為 12 萬美元。企業回應 DDoS 攻擊的成本可達到 230 萬美元（2017 年測量資料）。[8]

直接針對 DNS 提供者發起的攻擊可能會對依賴他們的組織以及提供者本身造成更為深遠的影響：如果他們的 DNS 發生故障，則組織可能會尋找新的提供者。

網站和應用程式並非 DDoS 攻擊的唯一目標。攻擊者通常也會針對內部部署網路發起攻擊。當攻擊持續進行，且用戶端裝置無法載入所需資源時，具有自託管 DNS 的組織也會遭受嚴重損失。此類攻擊可能會嚴重地阻礙組織的正常營運，甚至使其全部停止。

如何阻止即將到來的針對 DNS 基礎架構的威脅

最終，只有正確的架構才能阻止規模逐年增長的 DDoS 攻擊。

透過硬體的傳統 DDoS 緩解與透過軟體的可擴充緩解

以往，阻止攻擊的方式就是購買或構建一個大盒子，然後用它來篩選傳入的流量。大多數傳統 DDoS 緩解服務廠商使用 Cisco、Arbor Networks 及 Radware 等公司的硬體，並將其一起叢集到「清理中心」。

讓這些龐大的緩解盒子一起工作是有技巧的，但很不方便。單個盒子可以吸收的封包數量的實際限制成為服務提供者可緩解的總量的有效限制。在規模非常大的 DDoS 攻擊情況中，大部分攻擊流量從未到達清理中心，因為只有幾個位置，上游 ISP 成為瓶頸。

設備的費用意味著廣泛地分佈清理硬體並不具有成本效益。傳統 DDoS 廠商通常僅在客戶遭受攻擊時才會提供服務；

讓處理能力超出以往最大規模攻擊一定程度則毫無意義。

似乎可以認為，除此以外的任何投資都是一種浪費。但最終事實證明，這種想法對這種傳統模式而言是致命的。

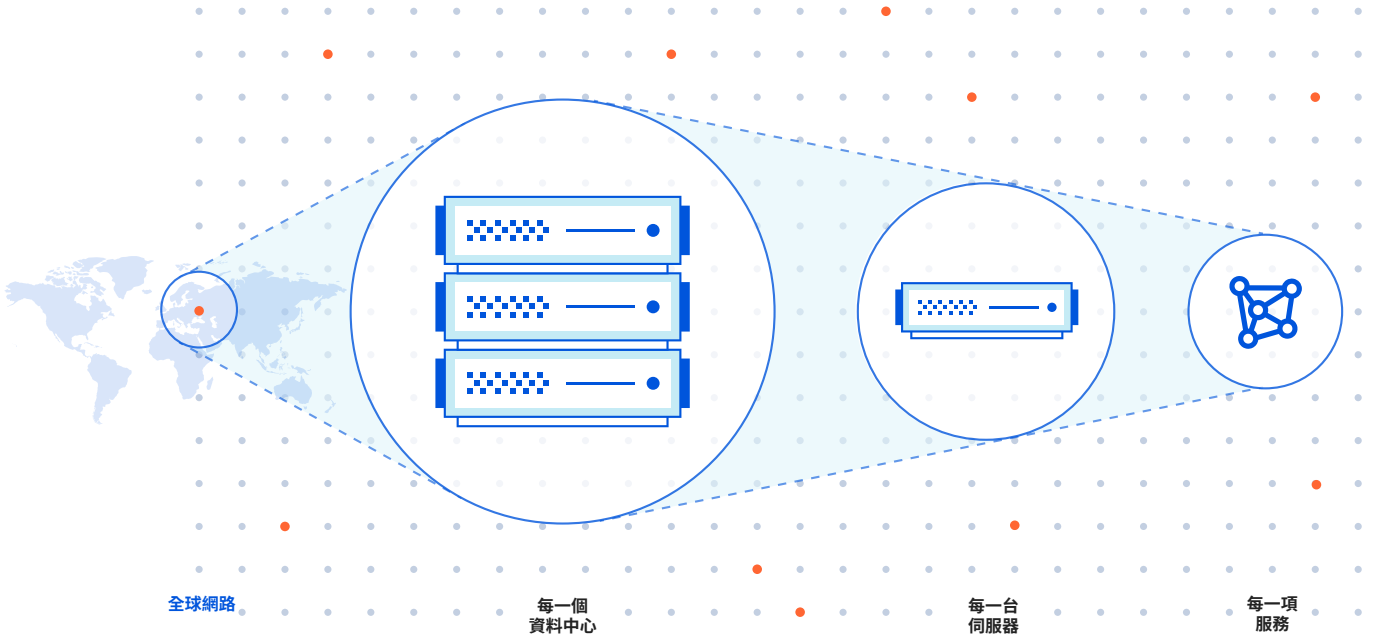
未來不會裝在盒子裡

從早期開始，Cloudflare 就開始部署一個非常簡單的架構，而不是投資硬體盒子進行 DDoS 緩解。起初，Cloudflare 的機架只有三個元件：路由器、交換器、伺服器。如今，機架變得更簡單了，通常完全捨棄了路由器，使用也可以處理足夠路由表的交換器，在資料中心所服務的地理區域內路由封包。

Cloudflare 並未使用負載平衡器或專用緩解硬體（可能會成為攻擊中的瓶頸），而是撰寫了使用邊界閘道協定 (BGP)（這是基本的網際網路路由通訊協定）的軟體，在網路中的每個資料中心內依地理位置分散負載。每個機架中的每台伺服器都能夠應答每種類型的要求。Cloudflare 的軟體會根據特定客戶在特定時間的需求動態分配流量負載 — 這表示，Cloudflare 會在大規模攻擊期間自動在實際數萬台伺服器之間分配負載。

這也表示，Cloudflare 可以經濟高效地繼續進行網路投資。例如，如果一座城市需要增加 10% 的處理能力，Cloudflare 就可以向那裡額外運送 10% 的伺服器，而不必做出購買還是構建另一個清理盒子的階躍性決定。

由於每一個核心、每一台伺服器、每一個資料中心都可以協助緩解攻擊，因此，Cloudflare 所連線的每一個新的資料中心都會提供更好的服務，並且阻止更接近來源的攻擊的能力也會增強。換言之，針對大規模分散式機器人網路的解決方案就是大規模分散式網路。這就是網際網路的工作方式：在幾個清理位置將力量分散，而不是聚焦。



Cloudflare 如何輕鬆擴展 DNS 安全性

但是，Cloudflare 不僅使用分散式網路來高效地封鎖並吸收惡意流量，Cloudflare 還會從所有這些位置提供權威 DNS 及 DNS 解析。從任何資料中心提供 DNS 回應都意味著以最短的等待時間解析了 DNS 查詢。這也意味著，Cloudflare 的 DNS 會從整個網路的處理能力和分散性質中獲益。

Cloudflare 網路的資源使用非常高效，從而節約了大量的作業和資本。由於 Cloudflare 使用相同的設備及網路來提供所有功能，因此 Cloudflare 很少會因為阻止攻擊或提供任何其他服務而產生其他頻寬成本。

隨著 Cloudflare 的功能不斷擴充，用來阻止攻擊的處理能力也相應增加。不管攻擊規模大小，Cloudflare 都能夠以固定成本提供 DDoS 緩解，因為攻擊不會增加 Cloudflare 的最大單位成本。

這一龐大的分散式網路由具有相同功能的伺服器組成，也可以讓 Cloudflare 輕鬆地以最短的等待時間和較大的規模提供功能。其中一個最核心的服務是權威和次要 DNS；Cloudflare 是世界上最快的 DNS 解析程式。[9]

Cloudflare 全球 Anycast 網路允許在超過 275 座城市的每個資料中心的網路邊緣進行 DNS 解析，從而實現無與倫比的備援和 100% 正常運作時間。由於 Cloudflare 的網路處理能力能夠很好地吸收 DDoS 攻擊，因此，DNS 在面對任何大小和類型的攻擊時都具有復原能力。

贏得軍備競賽並在面對 DDoS 攻擊時保持復原能力

- Cloudflare 的網路處理能力（截至 2022 年第四季度）：**172 Tbps**（且在不斷增長）
- 有史以來規模最大的 DDoS 攻擊：小於 **2.5 Tbps**

在未來幾年內，DDoS 攻擊的規模可能會繼續快速增長，甚至呈指數性增長。但 Cloudflare 已做好準備，在未來幾十年內繼續贏得軍備競賽。

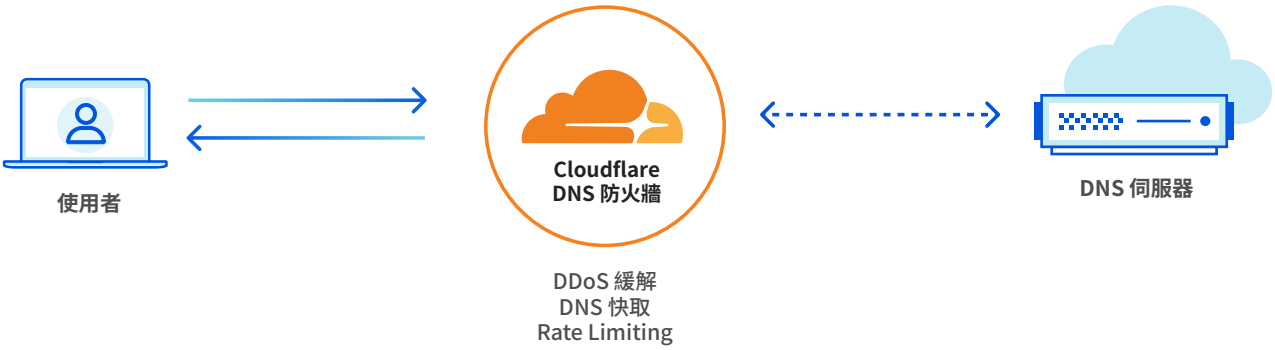
Cloudflare 是唯一從開始就旨在緩解大規模 DDoS 攻擊的提供者。正如 DDoS 攻擊本來就是分散性的，Cloudflare 的 DDoS 緩解系統在其龐大的全球網路中也是分散的。

與大多數傳統服務提供者相比，攻擊者有一項優勢：提供者的成本較高，因為他們必須購買價格昂貴的盒子和頻寬，而攻擊者的成本卻很低，因為他們使用數量驚人的遭到駭客入侵的裝置，並產生不對稱的流量來攻擊其目標。正因為如此，Cloudflare 的祕密武器就是在 Cloudflare 的大規模分散式商用硬體網路中分配負載的軟體。

保護 DNS 免受各種攻擊和入侵

截至 2022 年第四季度，Cloudflare 每秒可處理約 2260 萬個 DNS 查詢（權威要求和解析要求）— 同時緩解不斷增長的 DDoS 攻擊。Cloudflare DNS 仍然能夠防禦任何規模的 DDoS 及機器人攻擊，從目前的大規模 DDoS 攻擊到 DNS 水刑及其他入侵。

針對託管自己的 DNS 基礎架構的 DNS 服務提供者及組織，Cloudflare DNS 防火牆可提供一個解決方案，不僅會協助他們保護自己的基礎架構及使用者免受大規模 DDoS 攻擊，而且會透過快取 DNS 記錄及代表他們回應來提高效能。



透過與 DDoS 緩解原生整合，Cloudflare 的 DNS 及 DNS 防火牆解決方案可確保您的應用程式一律受到保護並可用，甚至在面對有史以來最大規模的幾起 DDoS 攻擊時亦是如此。

重點

Cloudflare 繼續發展，不斷地將更多的城市和國家/地區加入其網路。Cloudflare 對新攻擊時刻保持警惕，但非常確信，最終他們的架構會是阻止接下來任何攻擊的正確方式。開始與旨在現在以及未來幾年阻止針對 DNS 的攻擊的網路合作：

- 透過設定 Cloudflare，保護自己免受所有 DDoS 攻擊，包括大規模基於機器人網路的 DDoS 攻擊以及放大攻擊
- 透過依賴 Cloudflare 作為您的權威 DNS 供應商，讓 DNS 在受到攻擊的情況下保持正常運作
- 透過使用 Cloudflare 的 DNS 防火牆來限速和抵禦攻擊，保護您的 DNS 基礎架構和潛在的 DDoS 受害者

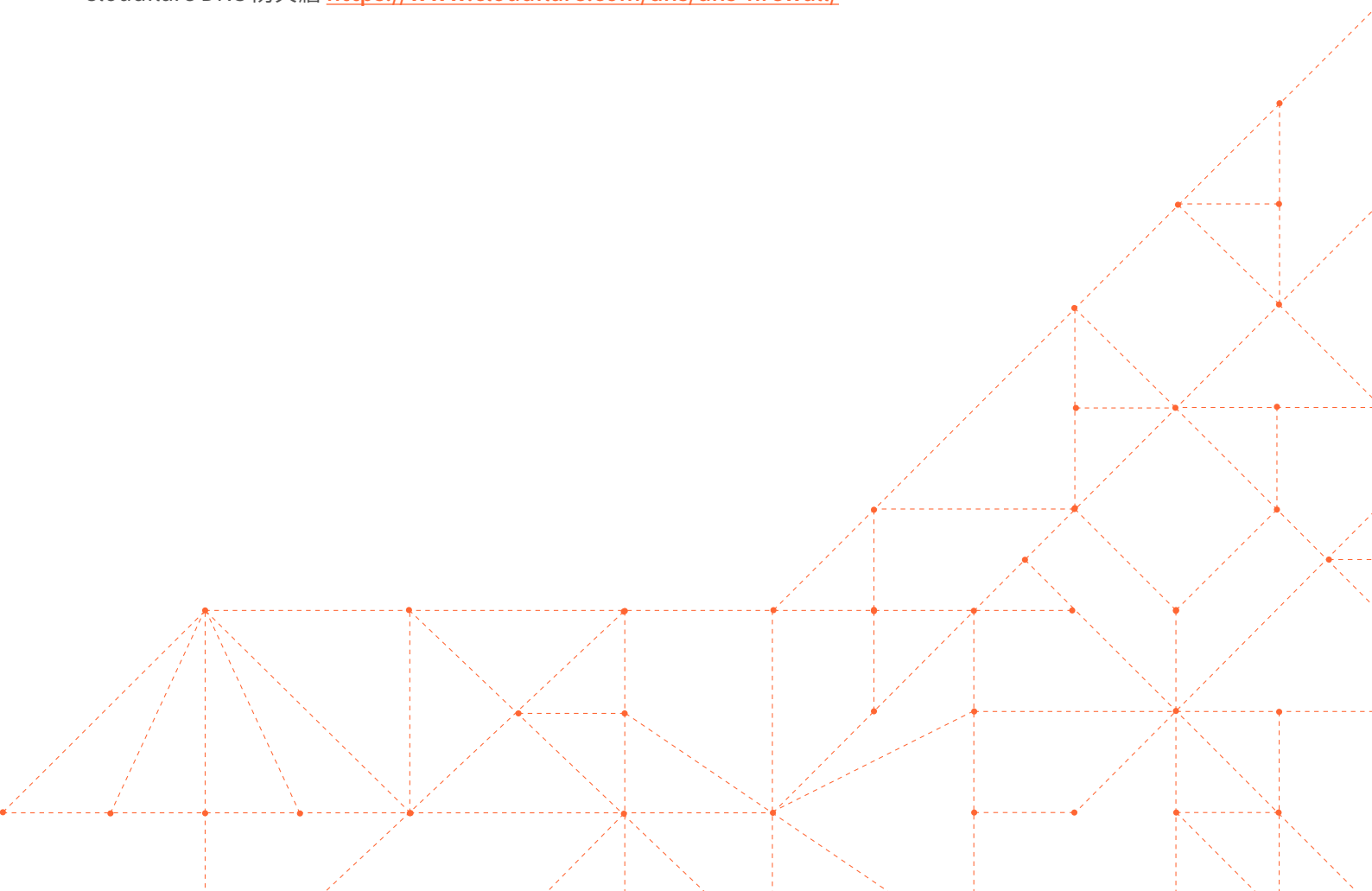
設定非常簡單，通常只需不到 5 分鐘就可以啟動並執行。請造訪 cloudflare.com/plans，查看各種方案（從 Free 到 Enterprise）。

若要進一步瞭解 Cloudflare 的解決方案，請造訪：

Cloudflare DNS https://www.cloudflare.com/dns/

Cloudflare DDoS 緩解 cloudflare.com/ddos

Cloudflare DNS 防火牆 https://www.cloudflare.com/dns/dns-firewall/



參考文獻

1. 「針對 Dyn 受管 DNS 的 DDoS 攻擊。」Dyn Statue Updates，2016 年 10 月 21 日，https://www.dynstatus.com/incidents/nlr4yrr162t8。2022 年 10 月 3 日存取。
2. Catalin Cimpanu。「AWS 稱，它緩解了有史以來規模最大的一個 2.3 Tbps 的 DDoS 攻擊。」ZDNET，2020 年 6 月 17 日，https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/。2022 年 10 月 3 日存取。
3. Omer Yoachimik。「Cloudflare 緩解了每秒 2600 萬個要求的 DDoS 攻擊。」Cloudflare，2022 年 6 月 14 日，https://blog.cloudflare.com/zh-tw/26m-rps-ddos-zh-tw/。2022 年 10 月 3 日存取。
4. Vivek Ganti 和 Omer Yoachimik。「Meris 機器人網路簡史。」Cloudflare，2021 年 11 月 9 日，https://blog.cloudflare.com/meris-botnet/。2022 年 10 月 3 日存取。
5. Omer Yoachimik。「Mantis — 迄今為止最強大的機器人網路。」Cloudflare，2022 年 7 月 14 日，https://blog.cloudflare.com/zh-tw/mantis-botnet-zh-tw/。2022 年 10 月 3 日存取。
6. 「警示 (TA14-017A)：基於 UDP 的放大攻擊。」CISA，2019 年 12 月 18 日，https://www.cisa.gov/uscert/ncas/alerts/TA14-017A。2022 年 10 月 24 日存取。
7. Matthew Prince。「讓 Spamhaus 離線的 DDoS（以及如何緩解）。」Cloudflare，2013 年 3 月 20 日，https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/。2022 年 10 月 24 日存取。
8. Dan Kobialka。「Kaspersky Lab 研究：企業 DDoS 攻擊的平均成本總計為 200 萬美元。」MSSP Alert，2018 年 2 月 25 日，https://www.msspalert.com/cybersecurity-research/kaspersky-lab-study-average-cost-of-enterprise-ddos-attack-totals-2m/。2022 年 10 月 3 日存取。
9. 「DNS 效能分析與對比。」DNSPerf，https://www.dnsperf.com/。2022 年 10 月 24 日存取。

CLOUDFLARE

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

REV:BDES/3855.20221104