使用 Cloudflare 進行 DDoS 保護

現今 DDoS 攻擊的演進

2016
每秒 1 Tb
IoT 殭屍網路第 7 層攻擊

前所未有規模最大的第 7 層攻擊 (使用 Mirai IoT 殭屍網路)。攻擊不但會進行流量攻擊，還會耗盡伺服器資源。

2014
每秒 400 Gb
NTP 放大攻擊

攻擊者只從一部頻寬為每秒 87 Mb 的來源伺服器，就利用 4,529 部 NTP 伺服器將攻擊放大。

2013
每秒 120 Gb
第 3/4 層 DDoS 攻擊

Spamhaus 攻擊被視為當時規模最大的攻擊之一，而且背上「幾乎造成整個網際網路停擺的威脅」之惡名。

分散式阻斷服務 (DDoS) 攻擊日益普遍，且已演化為讓組織疲於因應的複雜安全性挑戰。雖然 DDoS 攻擊並非近來才有的現象，用於進行並屏蔽此類攻擊的手法與資源已大幅演進。DDoS 攻擊的一個演進里程碑是 Mirai 殭屍網路的形成；此殭屍網路由超過 300,000 部受駭 IoT 裝置所組成，並用於產生目前已知規模最大的 DDoS 攻擊，而其尖峰攻擊流量超過每秒 1 Tb 的輸送量。此種規模的攻擊已成為後續攻擊者意欲達到的新標準。

DDoS 攻擊通常不是一次性事件，受害者在一年內通常會遭到多次攻擊。根據 Cloudflare 的經驗，不論是大型或小型組織，都有可能成為攻擊目標。即使許多管轄機構的法律都將 DDOS 攻擊視為非法，仍有「DDOS 即服務」提供者提供訂閱方案，有些甚至每個月只要 5 - 10 美金就能取得這種服務。

收入損失只是此類型攻擊會對您的網站或企業造成的眾多威脅之一。即便是 Amazon 網站 (2015 年零售收入為 990 億美金)，過去也曾因為未知的原因停機數次。例如，在 2013 年，Amazon.com 停機大約 15-45 分鐘，造成該公司 180 - 530 萬美金的營業額損失 (以該公司每分鐘平均營業額 117,882 美金計算)。此外，網站無法存取等問題會造成較無法量化的損失，例如品牌忠誠度與客戶滿意度降低。

規模可調整且精確的 DDoS 解決方案

Cloudflare 每秒 10 Tb 的全球 Anycast™ 網路速度是有記錄以來規模最大 DDoS 攻擊的 10 倍之，因此可確保 Cloudflare 網路上的所有網際網路資產都能承受現今大規模的 DDoS 攻擊。Cloudflare 針對第 3、4 與 7 層提供的 DDoS 保護是以網路前緣服務的方式提供，可協助您抵擋現今大規模的威脅，而且可用來減輕任何形式與規模的 DDoS 攻擊。「速率限制」讓 Cloudflare 的 DDoS 防護功能更為完整，因為它可以讓您精確地減輕針對應用程式層的最複雜攻擊所帶來的影響。

針對第 3 與 4 層 DDOS 攻擊提供保護

第 3 與 4 層 DDOS 攻擊通常是流量攻擊，例如 DDoS 放大、DDoS 洪水與 DDOS SYN 洪水攻擊。雖然這些攻擊可以癱瘓典型的單點傳播型網路，但是 Cloudflare 的 Anycast 型網路本質上會透過將攻擊流量分散到每個 Cloudflare 資料中心 (全球有 102 個以上) 並分散到與其他網路彼此之間的高頻寬連線以將受攻擊面分散，進而完全吸收攻擊流量。

DDoS 保護功能

- 第 3、4 與 7 層 DDoS 保護
- DNS 攻擊保護
- 使用「速率限制」進行精細的威脅封鎖
- 透過 IP 信譽資料庫獲得預測性安全性

「知道我們不用擔心 API 與閘道伺服器會遭受 DDoS 攻擊的威脅，讓我們可以放心地專注在改進產品上。」

- Jake Heinz，
Discord 軟體工程師

Cloudflare 的網路

- 擁有超過 102 個資料中心的全球 Anycast™ 網路
- 每秒 10 Tb 的輸送量足以吸收流量攻擊
- 6 百萬個網際網路資產
- 實惠的頻寬訂價

「我們使用 Cloudflare 的原因在於安全性功能卓越、CDN 效能極佳，且套件式解決方案真的很方便。它讓我們可以輕鬆地管理所有項目，而且讓我們可以專注在核心業務上。」

- Amanda Kleha，Zendesk
Online Business Unit 總經理

針對第 7 層 (應用程式層) 弱點提供保護

常見的第 7 層攻擊類型包括 SQL 插入與跨網站指令碼 (XSS)，這可能可讓攻擊者取得客戶資源或任何其他類型應用程式資料的存取權並予以竄改。Cloudflare 透過其 Web 應用程式防火牆 (WAF) 抵擋此類威脅。WAF 會自動封鎖在前 10 個 OWASP 規則集、Cloudflare 應用程式規則集與社群/客戶建立之自訂規則中發現的威脅。Cloudflare 已協助客戶抵擋主要零時差弱點攻擊，包括 Shellshock 弱點攻擊與 Heartbleed Bug。

速率限制

啟用 Cloudflare 的「速率限制」即可設定更為精細的流量控制，以讓 Cloudflare 的 DDoS 防護功能與 Web 應用程式防火牆 (WAF) 服務功能更為完整。「速率限制」可協助抵擋阻斷服務攻擊、暴力密碼破解嘗試以及其他以應用程式層為目標的惡意行為。設定要求閾值、定義自訂回應 (例如攻擊緩和動作 (查問或 CAPTCHA)) 或回應碼，並取得您網站、應用程式或 API 端點的深入洞察分析。

預測性安全性

Cloudflare 提供自動學習平台，系統會即時分析其中的網路流量，以識別異常或惡意要求。一旦識別新的攻擊，Cloudflare 會自動開始針對特定網站與整個社群封鎖該攻擊類型。因為 Cloudflare 的網路與社群持續成長，所以針對 Cloudflare 使用者發動有效的 DDoS 攻擊將會越來越困難。

實惠的頻寬訂價

Cloudflare 以實惠的月費提供無限制的企業級 DDoS 保護。Cloudflare 認為客戶不應該因為 DDoS 攻擊相關網路流量暴增而多繳費用。使用 Cloudflare 的 DDoS 保護時，客戶可以不用擔心其網站是否會因為遭受攻擊而離線，而且每月帳單上也不會有暴增的費用。

註冊 Cloudflare

註冊 Cloudflare 並啟用「速率限制」以保護您的網站、應用程式或 API 使其免於 DDoS 攻擊的威脅，同時降低延遲並發揮最新 Web 技術的完整功能。設定方式非常簡單，而且通常只需要不到 5 分鐘的時間就能讓功能順利運作。瀏覽 www.cloudflare.com 以查看從 Free (免費) 到 Enterprise (企業) 等方案。