執行摘要

網路安全神話：

為什麼漸進式修復方法效果不佳—以及 EzIP 如何提供更簡單、更安全的解決方案

網路是現代社會運作的基石，但它仍然脆弱不堪。最近 Cloudflare（2025 年 11 月）發生的全球性故障以及亞馬遜網路服務 (AWS) 頻繁中斷，都凸顯了即使是旨在增強安全性和可靠性的頂級服務提供商，也仍然存在持續的脆弱性。聯邦政府的努力（FCC NPRM，2024 年）和白宮發布的《增強互聯網路由安全路線圖》（2024 年）都將目標鎖定在邊界網關協定 (BGP)，旨在加強對其的監控和驗證。這些措施雖然有效，但只是治標不治本，未能解決更深層的問題：IPv4 位址最初的短缺。為了因應地址資源有限的問題：

- 動態分配（DHCP）使 IP 位址變成臨時位址。
- DNS 負責追蹤這些變化。
- 網路被分割成數千個域（自治系統），並依賴 BGP 協定連接這些域。
- 內容傳遞網路（CDN）集中管理流量，以因應網路複雜度。

這種架構會造成混亂、單點故障，並給攻擊者帶來優勢：偽造地址易於使用且難以追踪，而合法用戶卻會留下清晰的記錄。集中式 CDN 成為主要攻擊目標，而修補漏洞只會增加更多層級，卻無法解決根本原因。 EzIP（簡易 IPv4）透過重新利用長期保留的 IPv4 240/4 位址區塊來解決這個問題，為數百萬個場所提供唯一的靜態公用位址——足以服務整個區域，而無需動態重新分配或過度依賴存在問題的協定。主要優勢：

- 更強的固有安全性－靜態位址使欺騙行為更容易被偵測到，提高了可追溯性，並從設計上縮小了攻擊面。
- 更高的可靠性－降低複雜性可減少中斷風險；精確的地理位置資訊有助於管理和回應。
- 最小的干擾－此系統疊加在現有網路之上，透過增強區域路由器逐步部署，無需大規模設備升級。
- 更廣泛的優勢－降低了中心化風險，改善了網路架構，並有助於更好地進行執法追溯。

EzIP 透過解決導致網路脆弱的根本性資源稀缺問題，對 IPv6 和現有工具進行了補充。它符合建立更具韌性、更公平的數位基礎設施的目標。如需完整分析，請造訪：

https://avinta.com/gallery/CyberSecurityMyth-RoC.pdf

編制： Abraham Y. Chen / Avinta Communications, Inc.
接觸：AYChen@Avinta.com / +1(650)248-1829
2026 年 1 月