执行摘要

网络安全神话：

为什么渐进式修复方法效果不佳—以及 EzIP 如何提供更简单、更安全的解决方案

互联网是现代社会运转的基石，但它仍然脆弱不堪。最近 Cloudflare（2025 年 11 月）发生的全球性故障以及亚马逊网络服务 (AWS) 频繁中断，都凸显了即使是旨在增强安全性和可靠性的顶级服务提供商，也仍然存在持续的脆弱性。联邦政府的努力（FCC NPRM，2024 年）和白宫发布的《增强互联网路由安全路线图》（2024 年）都将目标锁定在边界网关协议 (BGP)，旨在加强对其的监控和验证。这些措施虽然有效，但只是治标不治本，未能解决更深层次的问题：IPv4 地址最初的短缺。为了应对地址资源有限的问题：

- 动态分配（DHCP）使 IP 地址变为临时地址。
- DNS 负责跟踪这些变化。
- 网络被分割成数千个域（自治系统），并依靠 BGP 协议连接这些域。
- 内容分发网络（CDN）集中管理流量，以应对网络复杂性。

这种架构会造成混乱、单点故障，并给攻击者带来优势：伪造地址易于使用且难以追踪，而合法用户却会留下清晰的记录。集中式 CDN 成为主要攻击目标，而修补漏洞只会增加更多层级，却无法解决根本原因。EzIP（简易 IPv4）通过重新利用长期保留的 IPv4 240/4 地址块来解决这个问题，为数百万个场所提供唯一的静态公共地址——足以服务整个区域，而无需动态重新分配或过度依赖存在问题的协议。主要优势：

- 更强的固有安全性——静态地址使欺骗行为更容易被检测到，提高了可追溯性，并从设计上缩小了攻击面。
- 更高的可靠性——降低复杂性可减少中断风险；精确的地理位置信息有助于管理和响应。
- 最小的干扰——该系统叠加在现有互联网之上，通过增强型区域路由器逐步部署，无需大规模设备升级。
- 更广泛的优势——降低了中心化风险，改进了互联网架构，并有助于更好地进行执法追溯。

EzIP 通过解决导致互联网脆弱的根本性资源稀缺问题，对 IPv6 和现有工具进行了补充。它符合构建更具韧性、更加公平的数字基础设施的目标。如需完整分析，请访问：

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

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