 DOI: https://doi.org/10.12349/iser.v6i7.6711

Research on network security technology of cloud application system in IPv4/IPv6 dual-stack network environment

Baoqi Zhang Xudong Du Wei Li Jun Chang

Chuanqing Drilling Engineering Co., Ltd., Changqing Drilling Corporation, Xi'an, Shaanxi, 710018, China

Abstract

With the rapid development of the Internet, IPv4 address resources are gradually being depleted, and IPv6, as the next-generation Internet protocol, is increasingly being widely used. The IPv4/IPv6 dual-stack network environment has become an important form during the network transition period. This paper first analyzes the current status of cloud application system network security in IPv4 network environments, using data from authoritative institutions and companies to illustrate the challenges faced. It then explores the cutting-edge technologies related to network security in IPv4/IPv6 dual-stack network environments for cloud application systems, including the dual-stack support capabilities of cloud platforms such as Azure and Google Cloud. Finally, by combining the production scenarios of petroleum enterprises, the practical application of dual-stack network security technology is studied, and targeted solutions are proposed to enhance the security and reliability of the production networks of petroleum enterprises.

Keywords

IPv4/IPv6; Cloud Application System; Network Security; Dual Stack Network

IPv4/IPv6 双栈网络环境下云应用系统网络安全技术研究

张宝奇 杜旭东 李卫 常军

川庆钻探工程有限公司长庆钻井总公司，中国 · 陕西 西安 710018

摘 要

随着互联网的快速发展，IPv4地址资源逐渐枯竭，IPv6作为下一代互联网协议逐渐被广泛应用。IPv4/IPv6双栈网络环境成为当前网络过渡阶段的重要形态。本文首先分析了IPv4网络环境下云应用系统的网络安全现状，通过权威机构和公司的数据展示了当前面临的挑战。接着，探讨了IPv4/IPv6双栈网络环境下云应用系统网络安全相关的前沿技术，包括Azure、Google Cloud等云平台的双栈支持能力。最后，结合石油企业生产场景，研究了双栈网络安全技术的实际应用，提出了针对性的解决方案，以提升石油企业生产网络的安全性和可靠性。

关键词

IPv4/IPv6；云应用系统；网络安全；双栈网络

1 引言

随着云计算和物联网技术的飞速发展，云应用系统在各个行业的应用越来越广泛。然而，IPv4 地址资源的有限性逐渐成为制约网络发展的瓶颈。IPv6 作为下一代互联网协议，以其巨大的地址空间和更好的安全性逐渐被接受和推广。在 IPv4/IPv6 双栈网络环境下，云应用系统的网络安全面临着新的挑战和机遇。本文将深入研究双栈网络环境下云应用系统的网络安全技术，并结合石油企业生产场景进行实际应用分析。

2 Pv4 网络环境下云应用系统网络安全现状

我国高度重视 IPv6 的规模部署和应用，以推动互联网技术的升级和网络安全的提升。2025 年，中央网信办、国家发展改革委、工业和信息化部联合印发了《2025 年深入推进 IPv6 规模部署和应用工作要点》，到 2025 年末，我国将全面建成全球领先的 IPv6 技术、产业、设施、应用和安全体系。

近年来，随着国家对信创产业的支持力度不断加大，石油企业等相关能源企业纷纷加大信创投入，推动信息技术应用创新，积极推进 IPv6 在网络基础设施中的广泛应用。基于 IPv6 技术全面开展云网融合改造与混合云办公服务体系升级，探索快速、高效、灵活的信息化服务模式，以满足云数据安全及生产实时数据高速传输的可持续发展要求，从而适应 IPv4 到 IPv6+ 网络的平滑过渡。

2.1 IPv4 地址资源短缺

IPv4 采用 32 位地址空间，仅能提供约 43 亿个地址。随着互联网设备的爆炸性增长，IPv4 地址资源短缺问题日益严重。根据互联网协会（Internet Society）的报告，全球

【作者简介】张宝奇（1978–），男，中国甘肃宁县人，硕士，高级工程师，从事信息安全研究。

IPv4 地址分配已接近饱和。地址短缺导致企业大量使用网络地址转换（NAT）技术，虽然 NAT 在一定程度上缓解了地址不足的问题，但也带来了安全挑战，例如隐藏了真实的网络流量来源，增加了安全监控的难度。

2.2 网络安全威胁

IPv4 网络面临着多种安全威胁，包括 IP 欺骗、分布式拒绝服务（DDoS）攻击和端口扫描等。根据 Cyscale 的报告，IPv4 地址的公共暴露增加了网络攻击的风险，而减少公共 IP 地址数量不仅可以降低成本，还可以通过缩小攻击面来增强安全性。

2.3 云平台的安全措施

云服务提供商（CSP）通过多种方式增强 IPv4 网络的安全性。例如，AWS 通过 NAT 网关支持 NAT64 和 DNS64 技术，以实现 IPv6 和 IPv4 之间的通信。然而，这些转换机制也引入了新的安全问题，需要仔细配置和持续监控。

2.4 制约物联网发展

随着物联网的蓬勃发展，设备数量呈爆发式增长，IPv4 网络的局限性愈发凸显。IPv4 地址资源有限，仅能提供约 43 亿个地址，难以满足海量物联网设备的连接需求。此外，其在安全性、可扩展性及对移动设备的支持等方面也存在不足。物联网的广泛应用场景，如智能家居、智能交通、工业自动化等，对网络的稳定性、高效性和安全性提出了更高要求。因此，IPv4 网络已无法完全适应物联网的发展，急需更先进的网络技术来解决地址短缺等问题，以推动物联网的持续进步。

3 IPv4/IPv6 双栈网络环境下云应用系统网络安全前沿技术

3.1 IPv6 在网络溯源方面的优势

3.1.1 地址空间巨大易于溯源

IPv6 拥有 128 位的地址空间，理论上可以提供几乎无限的地址数量。这使得每个用户和设备都可以分配到唯一的 IPv6 地址，无需像 IPv4 那样依赖 NAT（网络地址转换）设备。因此，IPv6 地址可以直接与用户身份绑定，便于溯源。IPv6 地址分为 64 位的网络前缀和 64 位的接口地址。这种结构使得地址分配更加有规律，便于管理和溯源。

3.1.2 协议设计增强溯源能力

IPv6 取消了 IPv4 中的 ARP（地址解析协议），改为使用邻居发现协议（NDP），增强了地址解析的安全性。NDP 还增加了邻居不可达发现（NUD）功能，进一步提高了网络的健壮性。IPv6 支持无状态自动配置和有状态自动配置。无状态自动配置通过 EUI-64 算法将 MAC 地址转换为接口标识符，结合网络前缀生成全局单播地址。这种自动配置方式使得地址的生成和分配更加透明，便于溯源。

3.1.3 安全性增强，支持端到端加密

IPv6 协议中默认集成了 IPSec（Internet Protocol Security）安全机制。IPSec 通过扩展认证报头（AH）和封装安全载荷报头（ESP）实现数据加密和验证功能。这种端到端的安全机制使得数据在传输过程中更加安全，同时也便于在发生安全事件时进行溯源。IPv6 的扩展报头还可以插入染色比特、时间标签等信息，用于随流检测和路径还原。这些功能可以实时监测信道性能，还原数据路径，从而帮助快速定位攻击源。

3.1.4 网络扫描难度增加

IPv6 的地址空间巨大，攻击者难以扫描一个 IPv6 网段内所有可能的主机。假设攻击者以每秒扫描 100 万个主机的速度扫描，大约需要 50 万年才能遍历一个 64 位前缀内所有的主机地址。这大大增加了攻击的难度和代价，同时也使得溯源更加容易。

3.2 IPv6 网络溯源的关键技术

3.2.1 地址分析技术

通过分析 IPv6 地址的分配记录、路由信息和使用情况来实现溯源。IPv6 地址由互联网注册机构分配给各级运营商，接口标识则由设备自行生成或由网络管理员分配。通过查询这些信息，可以追溯到 IP 地址的注册机构和实际使用者的地理位置。地址编码技术可用于识别 IP 地址类型，进一步支持溯源。

3.2.2 日志分析技术

日志分析是网络溯源的重要手段之一。通过收集和分析网络设备的日志信息，可以获取攻击路径和攻击源的相关信息。在 IPv6 网络中，由于地址空间大，日志记录更加详细，有助于提高溯源的准确性。

3.2.3 数据报文分析技术

基于网络层数据报文分析方法的溯源技术可以通过提取和分析 TCP 五元组（源地址、目的地址、源端口、目的端口、协议类型）等信息来追踪攻击源。在 IPv6 网络中，数据报文的格式和内容更加丰富，为溯源提供了更多的信息。

3.2.4 随流检测技术

iFIT（随流检测）技术利用 IPv6 扩展报头中的染色比特，可以实时监测信道性能并还原数据路径。这种技术可以在业务出现异常时，自动在业务路径上逐级收集业务质量信息，定位故障位置，从而实现攻击源的精准溯源。

3.2.5 安全邻居发现（SEND）技术

SEND 协议通过独立于 IPSec 的另一种加密方式（Cryptographically Generated Address）保证了传输的安全性。这种技术可以防止攻击者伪造地址，从而提高溯源的可靠性。

3.2.6 双重触发机制

在一些 IPv6 网络攻击溯源方案中，采用双重触发机制可以提高溯源包生成的效率。这种机制能够在显著减少对攻击持续时间依赖的情况下完成攻击路径的还原，从而提高溯源的速度和准确性。

3.3 云平台的双栈支持

IPv4/IPv6 双栈技术是指在同一台设备或网络节点上同时支持 IPv4 和 IPv6 协议栈，允许设备同时处理 IPv4 和 IPv6 数据包。在云平台中，双栈支持通过在虚拟化层、网

络设备和应用程序中同时启用 IPv4 和 IPv6 协议来实现。云平台的虚拟机、容器和网络接口都可以配置为支持两种协议栈，从而实现无缝的网络通信。

云平台的网络设备（如虚拟交换机和路由器）也需要支持双栈，能够正确转发 IPv4 和 IPv6 数据包；客户端在解析域名时，DNS 服务器会根据客户端支持的协议返回相应的 IPv4 或 IPv6 地址；云平台的负载均衡器需要支持 IPv4 和 IPv6 双栈，能够将流量转发到 IPv4 或 IPv6 后端服务。

云平台的 IPv4/IPv6 双栈支持是网络演进的重要技术手段。云平台可以实现 IPv4 和 IPv6 的无缝互操作，确保业务的平滑过渡和兼容性。双栈技术不仅提升了网络性能和安全性，还为未来网络的全面 IPv6 化奠定了基础。

3.4 IPv6 网络安全阻断机制

在 IPv6 网络环境中，攻击者常常利用地址频繁变更的特性来逃避安全策略的封堵。为了应对这种情况，可以通过基于 MAC 地址或端口的阻断机制来精准识别并阻断威胁终端。在地址相对稳定的场景下，这种阻断方式能够精确地拦截威胁流量，同时不影响正常业务的运行 [1]。

通过上述多种阻断机制的结合使用，可以有效应对网络威胁，确保网络的安全性和可用性。这在很大程度上解决了 IPv6 地址随机性大导致静态安全策略失效的问题。

4 IPv4/IPv6 双栈网络环境下云应用系统网络安全技术在石油企业生产中的应用

4.1 石油企业网络基础架构改造

石油企业云平台整体以构建“万物互联”的云服务体系为数字化转型目标，助力企业智能化发展，逐步完成 IPv6 规模化部署和应用，做到云服务体系 IPv4-IPv6 的平滑过渡，包括：核心层、汇聚层、接入层。采用针对接入层的 IPv6 安全准入，对接入云平台的设备进行身份验证和访问控制，进一步保证企业云服务体系网络安全 [2]。

4.2 构建企业 IPv6+ 云桌面服务数据中心

通过部署 IPv6（互联网协议第 6 版），构建一个企业 IPv6+ 云桌面服务数据中心（即云服务器、PC 桌面、移动端访问三种办公环境），石油企业云服务体系全面进入数据云办公服务体系，提升了办公终端设备资源效率，提高了现有数据中心资源利用率，促进企业云计算资源实现动态管理及可持续发展。

云桌面服务采用虚拟化技术，将桌面环境部署在虚拟机（VM）中。每个虚拟机分配一个或多个 IPv6 地址，通过虚拟交换机与企业内部专网连接；采用负载均衡技术，根据用户的请求动态分配云桌面资源，确保云服务系统的高可用性；通过 IPv6 的流量工程（TE）技术，优化云桌面服务的网络路径，减少延迟和丢包率，提升用户体验和数据转发效率 [3]。

4.3 IPv6 零信任接入

IPv6 零信任接入结合了基于 SDP（软件定义边界）的访问控制机制，并禁用了自动生成地址和隐私扩展地址功能。在这种机制下，用户在尝试访问网络资源之前，必须先通过身份认证。同时，交换机可以通过维护一个动态的 MAC 地址表来管理接入设备。该表记录了连接到各个端口的设备的 MAC 地址。当新设备尝试接入网络时，交换机会检查其 MAC 地址是否已存在于表中。如果新设备的 MAC 地址不在表中，交换机可以根据预先配置的策略采取相应的阻断措施，例如关闭端口或发送警告信息。MAC 地址表可以通过手动配置生成，也可以通过网络管理协议（如 SNMP）自动更新。这种机制有效解决了 IPv6 地址频繁变更导致基于 IP 地址的访问控制失效、地址可读性差以及人工处置难度大等问题。

5 总结

5.1 IPv6 部署效益分析

IPv6 的推广和部署将优化现有的网络规划与管理流程，随着我国信息技术产业的持续进步和国产化替代进程的不断推进，国产服务器、存储设备以及操作系统、国产芯片等产品的性能和品质显著提升，已具备进行市场化推广核心竞争力。通过选用国产信息化产品，石油企业可以大幅度降低采购成本。同时，IPv6 的广泛应用可以显著增强网络的安全性与稳定性，为企业数字化转型和智能化发展提供坚实网络基础保障。

5.2 提升生产管理效能，为企业减负增效

IPv6 企业专网能够有效满足 EISC 中心在油气生产、远程指挥和应急救援等方面的实际需求。首先，在网络质量和成本方面，与传统有线组网模式相比，工业视频生产专网的网络传输速率提高了 30%，传输时延减少了 20%。不仅显著提升了网络性能，还大幅降低了生产运营成本，满足了基层员工在不同区域和工况下对网络的多样化需求。其次，在生产管理和数据应用方面，通过工业视频专网，作业现场的实时数据能够快速回传至 EISC 中心，实现数据的高效存储、分析和应用，助力业务从传统的经验型管理向基于大数据的精益管理转变。

6 结语

本文主要围绕石油企业在 IPv4/IPv6 双栈网络环境下，开展网络安全技术研究，通过分析双栈网络架构特性与云环境安全挑战，提出了立足于石油企业的网络安全和云技术解决方案，为企业数字化转型贡献力量。IPv6 的成功实践将进一步推动物联网技术、AI 大模型在石油勘探和钻井生产领域深入发展。

参考文献

[1] 胡佑东 朱豫川 徐睿等.基于IPv6的油气矿生产网侧自主可控自动控制系统应用[J].自动化应用.2025,04(04):252-256

[2] 宋恒利 卫乾 马赟等.油气生产物联网中IPv6与IPv4技术共存分析[J].中国石油和化工,2012, 06(06):46-47

[3] 薛彩霞 庄佳 沈晨普.基于云桌面系统的大数据智慧互动实训室建设研究[J].电脑知识与技术.2025，05(05):70-73