国泰君安 IPv6 安全防护体系实践
（国泰君安证券供稿，上海局指导）

一、项目背景

伴随着近年来国内外 IPv6 规模部署加速推进，IPv6 环境下的网络安全问题逐渐突出并呈现复杂化、多元化发展等趋势。企业在开展 IPv6 改造工作的同时，需要高度重视落实网络安全战略规划，考虑依托技术手段及工具加快 IPv6 人才培养、安全运营流程建设，为 IPv6 流量占比加速提升夯实网络安全基石。我司在近年发布数字化转型等公司战略时，同步制定了网络安全战略规划，明确提出内部安全发展方向，以随时应对公司转型不同阶段中可能带来的新的安全风险。在公司战略指导下，IPv6 工作小组在致力于打造具有行业示范效应的 IPv6 规模部署案例时，始终把网络安全作为 IPv6 改造顶层设计中重要指导方针之一。本篇文章主要围绕企业推进 IPv6 规模部署中的系列问题，展开介绍我司如何通过多重 IPv6 网络安全防御手段保障 IPv6 网络整体安全性。

二、项目难点

（一）IPv4/IPv6 过渡期安全风险

证券行业具有交易时间集中、市场高速变化、交易应用软件形态多样等特点，系统改造适配的环境较为复杂。在开展 IPv6 规模部署时需同步保障业务稳定性，全面支持 IPv6 升级演进将是个长期的过程，在此期间 IPv4 网络和 IPv6 网络将长期并存。为保障两类网络协议的相互通信，通常采用双栈、隧道、翻译等过渡机制，部分过度机制本身可能存在一定的安全隐患，如使用嵌入 IPv4 地址的 IPv6 地址绕过防护等。

（二）IPv6 协议新特性带来的挑战

安全防护手段的挑战：IPv6 协议的特性，如路由头、移动 IPv6、站点范围的多播地址等，使得传统基于地址资源的安全防护手段面临多重挑战。IPv6 地址标识的复杂性大幅增加，增加了安全防护的难度。

IPv6 地址暴露风险：IPv6 地址空间的巨大扩展性使得攻击者更容易进行地址扫描和发现漏洞，进而获取敏感信息。同时 IPv6 地址直接暴露为恶意攻击提供了更多机会，如 DDoS 攻击、僵尸网络构建等，可能导致网络服务中断、系统崩溃。

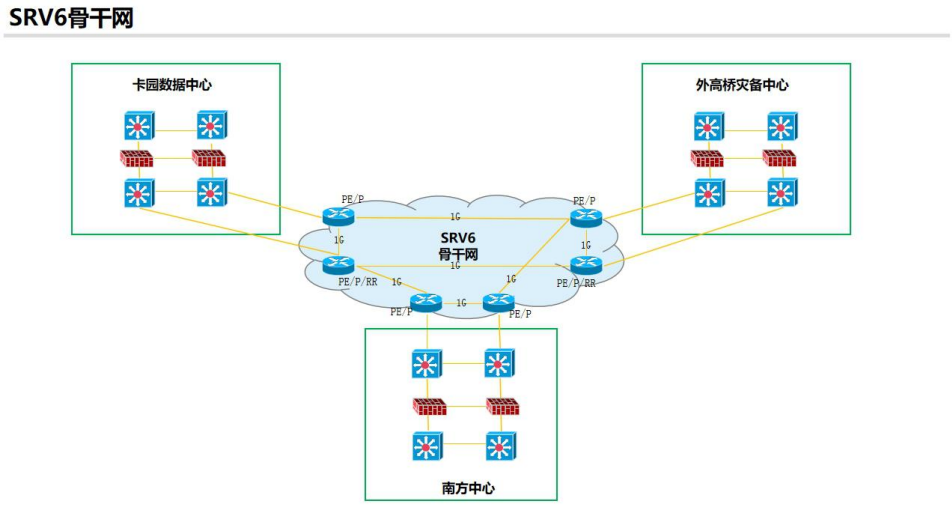
（三）IPv6 安全运营风险

IPv6 威胁情报缺失：随着数字化转型的深入及网络安全的形势复杂化，企业的安全防御需要部署提前预警的主动式安全防护措施，这就要求能够基于精准的情报信息提前发现威胁并溯源攻击行为。当前威胁情报研究还主要围绕 IPv4 开展，由于 IPv6 协议本身特性及威胁情报分析收集环节等复杂原因导致 IPv6 威胁情报数据有较大缺口，伴随着网络安全的演变，企业对 IPv6 威胁情报的需求也越来越紧迫。

三、项目方案

（一）多举措“纵深防御”保障双栈 IPv6 网络安全

在网络安全防护方面，我司利用基于 IPv6 的 SRv6 新一代路由技术，搭建了新一代骨干网，发挥 IPv6 骨干网在全网流量调优、拥塞保护、运维等方面的优势。同时采用 BGP 多线路的网络技术方案，可为不同运营商的用户提供最优的运营商网络获得服务，为企业提供了一种相对隐蔽的网络接入方式。在遭受 DDoS 等网络攻击时，BGP 多线路可以将攻击流量分散到不同的网络线路上，降低单一线路的负载压力，结合实时流量清洗技术，BGP 多线路方案可以进一步保障正常业务流量的顺畅传输并有效抵御攻击。



图一 国泰君安 SRV6 骨干网

在主机安全防护方面，由于 IPv6 服务器的安全性同样依赖于其内部环境的稳定和安全，HIDS 能够深入到系统内部，监测到从网络层面难以发现的安全问题，如后门、反弹 shell、恶意操作、主机组件安全漏洞、系统用户管理安全问题以及主机基线安全风险等。我司在推进 IPv6 规模部署同时持续推进 IPv6 主机 HIDS 覆盖度，截止目前已完成包括 1581 台 IPv6 主机的 HIDS 全面覆盖，具备实时感知 IPv6 主机环境下的各类威胁能力。

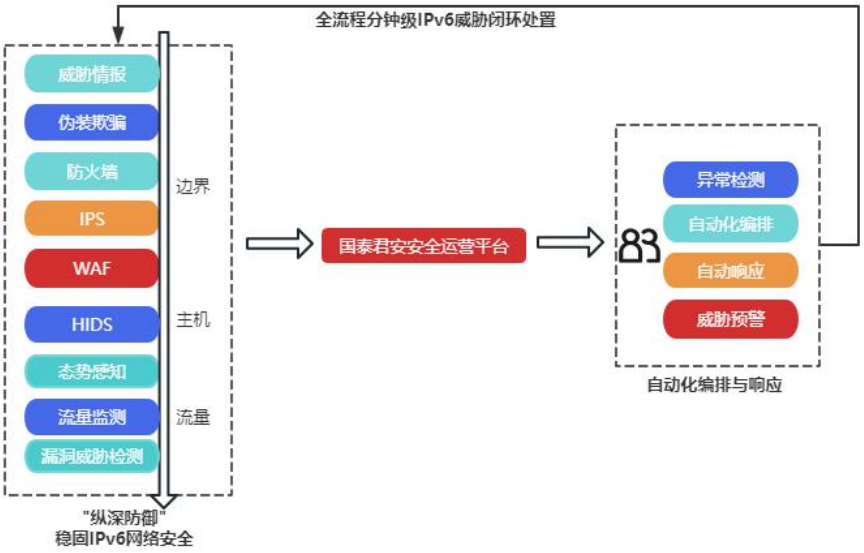
在应用安全防护方面，我司共计约 76 个对客服务应用，均已完成 IPv6 改造。基于传统防火墙和 Web 应用防火墙为 IPv6 应用提供网络层及七层防护能力，包括对恶意威胁的实时告警与拦截能力。为积极应对移动环境下的各类威胁，我司建设了移动 APP 线上威胁感知平台，能够对 IPv6 环境运行过程中的系统环境、应用行为、第三方 SDK 行为、用户

行为进行监测和审计，实时监测和阻断 APP 在线上运行过程中的各类安全风险。

在流量安全防护方面，我司基于现有两地三中心流量安全防护网全面升级覆盖 IPv6 网络，具备针对全量 IPv6 流量实时展开威胁检测、预警能力。

（二）建设“一体多面”IPv6 安全运营管理体系

安全运营平台是我司常态化安全运营体系建设的重要抓手，以“看得清、守得住、当沉淀、促发展、赢未来”15 字方针为指导思想。依托该平台，覆盖包括全量 IPv6 网络环境在内，具备全面扎实的数据能力底座、实战级的安全场景建设、自动化的安全事件编排与响应、可量化的安全运营成效展现，能多维感知安全态势，持续提升 IPv6 网络安全防御韧性。



图二 国泰君安安全运营管理体系

为积极展开IPv6威胁的主动防御，我司构建面向攻击溯源的行业威胁情报共享体系时，重点将IPv6情报纳入建设方向，通过“一套机制、一个中心”打通行业威胁情报共享通道，结合多源威胁情报信息数据的采集上报，利用机器学习算法关联分析出具备行业特色的IPv6攻击溯源情报。威胁情报体系建设以来，日均产生500-1000条情报数据，包括16条IPv6情报数据。

为加强IPv6安全知识技能培训并保障IPv6规模部署工作顺利进行，我司各成员部门指定专人开展IPv6相关工作，网站应用及君弘APP应用指定专项对接人，并与多家第三方服务商持续进行技术交流与方案讨论。同时，持续安排核心技术人员参与CNNIC、监管部门等组织的IPv6培训会议，并积极与人行上海总部、上海证监局、上海市国资委、上海市委网信办报告和沟通，确保工作安排符合网络安全要求及整体IPv6改造要求。

（三）加速推进自主掌控的IPv6规模部署环境

作为行业信息技术创新的领头羊，我司始终坚持自主掌控策略策略，承担了多项行业创新示范任务，作为首批行业信创示范单位，坚持“前瞻布局、先进替代、框架先行、客户无感”的信创改造方针，确保信创环境下的IPv6规模建设有序推进、平稳运行。2019年，我司开始着手研究、布局信创环境下的IPv6安全体系建设，截止目前覆盖IPv6应

用的网络基础设施及Web应用防火墙已部分完成信创替换，主机安全检测工具具备纳管信创服务器能力，安全运营体系已具备为基于信创的业务系统提供自主掌控的安全防护能力。

四、成效总结

（一）项目成效

通过近五年的IPv6部署摸索实践，我司已形成一整套成熟有效的IPv6网络安全防护方案，灵活适用于常态化安全运营及重要时期的网络安全保障，切实为公司IPv6规模部署及数字化转型保驾护航。安全运营体系实践以来，日均检测IPv6攻击约29万次，占整体互联网侧攻击量约4%。

（二）项目展望

未来，我司仍将紧跟国家IPv6战略规划发展步伐，在推进IPv6整体占比提升时始终高度重视保护企业信息资产安全及个人用户隐私安全。在已构建的IPv6网络安全纵深防御体系中，不断优化提升防御能力及安全运营能力，持续勇敢面对公司发展不同阶段的不同安全挑战，为行业持续输出IPv6网络安全建设解决方案，保持行业安全标杆地位。