IPv6 网络规模部署的安全风险隐患探讨

（南京证券供稿 江苏局指导）

一、前言

目前，我国正处于 IPv6 改造升级的关键时期，IPv6 规模部署工作是网络强国战略的重要部分。根据国家 IPv6 发展监测平台数据显示，截止 2022 年 9 月，我国 IPv6 互联网活跃用户数量已达 7.137 亿，占我国互联网用户总数的 67.9%。随着 IPv6 网络开始投入使用，针对 IPv6 网络的攻击数量急剧增加，影响范围也呈现出向各行业领域扩大趋势。根据 2021 年 CNCERT 抽样监测数据[1]显示，境外约 1.2 万个 IPv6 地址控制了我国境内约 2.3 万台 IPv6 主机，攻击源、攻击目标为 IPv6 地址的网站后门事件有 486 起，共涉及攻击源 IPv6 地址 114 个，被攻击的 IPv6 地址解析网站域名累计 78 个。截至 2022 年 9 月，在 CVE 漏洞库中已有 553 个与 IPv6 相关的安全漏洞被发布，覆盖系统漏洞、应用漏洞、硬件漏洞、协议漏洞等不同层面，涉及华为、思科等网络设备，Linux、Windows 等操作系统的各个发行版本，以及 Wireshark 等网络维护应用程序等。

2021 年 7 月，中央网信办等部委发文明确要求持续提高金融服务机构面向公众服务的互联网应用系统 IPv6 支持能力，加强 IPv6 安全防护体系建设，强化复杂场景下 IPv6 安全保障能力；通过依托国家网络与信息安全信息通报机制，

构建 IPv6 安全监测体系，提高 IPv6 安全态势感知、通报预警和应急响应能力。2021 年 11 月，中央网信办等十二部发文指出要提高 IPv6 环境下漏洞监测发现与处置能力；推动 IPv6 网络安全产品和服务研发应用，探索在 IPv6 环境下新兴领域的网络安全技术、管理及机制创新。在国家大力推进 IPv6 规模部署的行动中，证券行业必须走在前列。由于证券经营机构对网络安全运行有极高的要求，在保障现有 IPv4 网络连续安全稳定运行的情况下，如何实现应用系统的 IPv6 规模部署存在诸多挑战。

因此，本文旨在通过分析探讨 IPv6 可能存在的安全风险隐患，提出相应的安全防护建议，从技术和管理上为后续 IPv6 大规模部署打好安全基础。本文首先分析 IPv6 协议的安全优势，接着分析 IPv6 规模部署后将会面临的主要安全问题，最后提出针对 IPv6 的安全部署建议。本文的探讨将有利于促进证券行业 IPv6 网络的安全建设与健康发展。

二、IPv6 的网络安全优势

网络层协议是互联网体系结构特别是 TCP/IP 架构的基本要素之一，IPv6 相对于 IPv4 具有一定的安全优势。

作为上一代协议，IPv4 存在以下安全问题[2]：一是私有地址重复，安全监测和溯源难度大。由于公网地址缺乏，数据中心及办公场所内网主机通常会采用私有地址，经过 NAT 转换后接入外网，多台设备、多个用户共享外网 IP 地址，当安全检测平台监测到攻击后，并不能精准定位到具体是哪台主机，无法进行取证，造成溯源排查困难，难以实施进一步

阻断策略。二是公网地址错误私用，存在数据泄露风险。在IPv4地址不足时，有些组织可能会把非私网的IP地址作为私有地址使用，例如172.10.0.0/16网段，这些地址一旦后续在公网重新启用，由于内网已使用该地址，导致内网主机根据私网路由无法正常访问公网启用的相应服务，同时，当内网业务路由发生变化（不可达等），可能将IP数据包按照默认路由转发到外网，造成内部信息泄漏。

IPv6定义了下一代的网络层传输格式，具有以下优势[3][4][5]：

一是IPv6拥有128位的地址空间，约有3.4×1038个IP地址（IPv4地址总量为43亿个），加上移动IPv6技术实现了完整的IP层的移动性，能为每个设备分配一个永久的全球IP地址，真正实现全球任意点到任意点的连接，并有利于事后追查溯源，提高安全保障。

二是IPv6地址分配遵循聚类的原则，可以在路由表中用1条记录表示一个巨大的自治域网络和大量的子网，从而大大减少了路由表长度，在实现网络扁平化的基础上进行地址分层规划，不需要再使用NAT协议进行地址转换，减少了网络时延，提高信息传输效率。

三是提高了网络转发效率，RFC 2460中定义了IPv6协议头部格式，一些不重要的扩展字段都被放在了IPv6头部之后的扩展头部之中，使IPv6的头部信息更加简单清晰，因此路由器可以更高效地处理，从而显著提高数据包转发效率。通过引入灵活的扩展报头，可以按照不同协议要求增加

扩展报头种类，对网络加载新的应用提供了充分的支持。

四是IPv6使用无状态地址自动配置协议（SLAAC）和IPv6动态主机配置协议自动配置协议，可不需要服务器或使用DHCPv6服务器管理地址池对地址进行管理，使得网络（尤其是局域网）的管理更加方便和快捷，增强了移动终端的移动特性、安全特性、路由特性，降低了管理网络地址的难度。

五是IPv6中ARP的功能被邻居发现协议（NDP）所代替。邻居发现协议通过发现链路上的其他节点，判断其他节点的地址，寻找可用路由。对比ARP，NDP仅在链路层实现，更加独立于传输介质。此外，下一代互联网的安全邻居发现（SEND）协议通过独立于IPSec的另一种加密方式，使用密码生成地址方法，并用公私钥对身份进行验证，防止假冒，保证了传输的安全性。

六是协议安全性有所提高。首先，IPv6地址空间庞大，极大地增加了入侵者扫描检测的难度，在一定程度上降低了DDoS攻击发生的可能性。其次，在IPv6协议中支持IP Sec，为通信双方提供数据完整性保护、数据内容的机密性验证、有限的数据流机密性保证和数据起源验证，并提供了抗重播保护。因而可将用户、报文和攻击一一对应，防止用户抵赖，实现对用户行为的安全监控。再次，IPv6增加了增强的组播支持并废除了广播地址，为QoS控制提供了良好的网络平台，避免利用广播地址发起的广播风暴和DDoS攻击。最后，IPv6协议禁用了链路层组播、广播数据包和源地址不是唯一

识别的单个节点的数据包，因此能减少由ICMPv6报文造成的放大攻击。

七是IPv6地址费用极低。目前IPv4地址的二手市场转让价格约15美元/个，而ISP、政府、企业和家庭用户几乎可以零成本获得海量IPv6地址. 对于大量使用公网IP地址的证券行业，部署IPv6可以大大降低IP地址的成本。

三、IPv6面临安全风险隐患分析

（一）IPv6协议安全

从协议本身来看，IPv6与IPv4并没有太大的区别：它是一个无连接的网络协议，使用与IPv4相同的下层服务，并向上层提供相同的服务。本节将从IPv6与IPv4共有的安全风险、IPv6特有的安全风险、IPv6过渡机制的安全风险三个方面进行探讨。

1. IPv6与IPv4共有的安全风险

有多种攻击同时作用于IPv6与IPv4[6]，包括：

（1）应用层攻击：如跨站脚本、SQL注入、DDoS等；

（2）恶意设备：如恶意Wi-Fi接入点；

（3）泛洪和所有基于流量的拒绝服务：比如RFC 6192中描述了一种使用非法IPv6流量攻击路由器控制平面的方法。

此外，作为一个在实践中应用较少的网络协议，很多实践过程中的IPv6相关安全隐患还没有被发现和修复，而且具备安全维护IPv6网络的专业人士较少。

关于IPv6有很多误解，例如：由于其巨大的地址空间，

无法通过枚举/64 子网中所有的 IPv6 地址来进行网络扫描，因此黑客无法定位攻击目标。但是 RFC 5157 描述了可用来寻找网络上潜在目标的替代技术，例如枚举区域内所有的 DNS 名称。RFC 7707 中也给出了有关 IPv6 网络探测的其他做法。

另一个误解是由于 IPv6 强制要求使用 IPsec，因此它更安全。虽然最初的 IPv6 规范可能暗示了这一点，但 RFC 6434 明确指出：并不强制性要求支持 IPsec。此外，如果企业内部的所有流量都被加密，那么不仅是恶意软件，那些依靠检测 Payload 的安全工具——如入侵防御系统、防火墙、访问控制列表、IP 流信息导出（IPFIX，见 RFC 7011 和 RFC 7012 等）——都会受到影响。因此，IPsec 在 IPv6 中的用法与 IPv4 一致，如用于在非可信网络上建立 VPN 通道，或为某些特定应用预留。

最后一个误解是因为不再有广播，因此在 IPv6 中不存在放大攻击（如 SMURF）。可惜这也是不对的，因为路由器和主机在转发或接收组播消息时，在某些情况下会产生 ICMP 错误或信息消息（见 RFC 4443 的 2.4 节）。因此，必须像 IPv4 一样限制 ICMPv6 报文的生成和转发速率。

2. IPv6 协议安全风险特点

IPv6 协议的安全风险主要包括其协议本身特点以及针对 IPv6 特有的攻击[7][8][9]：

（1）协议本身的安全特点：IPv6 报文结构中引入的新字段（如流标签、RH0、路由头等）、IPv6 协议族中引入的

新协议（如邻居发现协议等）可能存在漏洞，可能被用于发起嗅探、DoS 等攻击。此外，不同类型设备在实现 IPv6 协议栈时，存在因编码、实施造成的安全风险。

（2）IPv6 特有的攻击风险：逐跳扩展头攻击、邻居发现协议攻击、DAD 攻击、前缀欺骗攻击、MLD 攻击、使用嵌入 IPv4 地址的 IPv6 地址绕过防护问题、不使用 NAT 导致的端到端透明性问题、将 IPv6 隐藏于 IPv6 隧道带来的绕过安全检查问题等。

3. IPv6 过渡机制可能引发的安全风险

在从 IPv4 向 IPv6 过渡的过程中，“双栈”、“隧道”、“翻译”是三种可能采用的方案，均可能带来新的安全威胁[8][9]：

（1）双栈机制安全风险

过渡期间双栈部署的网络中同时运行着 IPv4、IPv6 两个逻辑通道，增加了设备/系统的暴露面，也意味着防火墙、安全网关等防护设备需同时配置双栈策略，导致策略管理复杂度加倍，防护被穿透的机会加倍。IPv4 网络中，部分操作系统缺省启动了 IPv6 自动地址配置功能，使得 IPv4 网络中存在隐蔽的 IPv6 通道，由于该 IPv6 通道并没有进行防护配置，攻击者可以利用 IPv6 通道实施攻击。此外，双栈系统的复杂性也会增加网络节点的数据转发负担，导致网络节点的故障率增加。

（2）隧道机制安全风险

在隧道环境下，部分隧道机制仅要求隧道出入口节点对报文进行简单的封装和解封，缺乏内置认证、加密等安全功

能，导致攻击者可能截取隧道报文，伪造用户地址并伪装成合法用户发起攻击。以 IPv6 Over IPv4 为例，攻击者可伪造内层、外层地址发起仿冒攻击等安全风险。此外，由于部分隧道机制未采取对隧道封装内容的检查，因此，攻击者可将 IPv4 流量承载在 IPv6 报文中，导致原来 IPv4 网络的攻击流量经由 IPv6 的“掩护”后穿越防护造成威胁。

（3）翻译机制安全风险

翻译机制（协议转换）是为 IPv6 网络节点与 IPv4 网络节点相互通信提供透明的路由。翻译设备作为 IPv6 与 IPv4 互连节点，易成为安全瓶颈，面临地址池耗尽等常见 DDoS 攻击威胁，攻击者可通过伪造大量 IPv6 地址向翻译节点发起地址转换请求，消耗地址池 IPv4 资源，同时导致合法用户无法获取 IPv4 地址，进而引发 IPv4 网络无法正常访问，导致网络瘫痪。

（二）IPv6 设备安全

随着全球范围内的 IPv6 部署发展，网络设备主流厂家研发了大量的 IPv6 产品，产品类型丰富，基本涵盖了所有的网络产品（包括路由器、交换机、接入服务器、防火墙、VPN 网关、域名服务器等），能够满足基本商用部署需求。根据《2021 全球 IPv6 支持度白皮书》[10]，获得 IPv6 Ready Logo 测试认证的设备中，交换机和路由器等网络设备的数量已超过 900 个，而防火墙、IDS、WAF 等安全设备获得认证较少。

根据实际使用情况，启用 IPv6/v4 双协议栈后，部分网

络设备和安全设备的处理能力明显降低。除此之外，不同类型的网络安全防护设备还存在以下问题[8]:

1. 网络层安全防护设备

IPv6 环境下所有设备均可使用全球单播地址,不需要使用 NAT 即可实现互通，同时也可能缺少 NAT 设备形成的防护。因此，防火墙（或其他安全防护设备）的安全域划分与访问控制策略需要更加严格管理，一旦出现如“可以访问任意目标 IP 与端口”的错误配置将会造成更大风险。

在 IPv6 与 IPv4 混合网络中，防火墙/安全网关等防护设备需要同时配置双栈策略保障安全性，对设备的功能、性能的要求更高，出现单点故障的概率增加。

此外，由于 IPv6 地址长度大于 IPv4，因此原有 IPv4 防火墙升级版本支持 IPv6 后，在硬件规格不变的情况下，防火墙会话表容量、地址簿容量等内部数据结构的条目数量可能减少，影响性能或安全防护能力。

混合使用支持和不支持 IPv6 的设备也可能带来安全风险[11]。RFC 7359 提到了一个不容易想到的情况——远程访问 VPN 在客户端环境有原生 IPv6 时对流量失去控制。远程访问 VPN 客户端可以操纵本地路由表，重定向所有或是指定目的地的流量到隧道。然而由于有些 VPN 客户端软件不支持 IPv6 或是未配置 IPv6 的 Split Tunnel，结果等于它们无视 IPv6 路由表的存在，任由应该流经隧道的流量利用本地 IPv6 到达互联网，造成网络安全事件。

2. 应用层安全防护设备

WAF、IPS、IDS 等应用层安全防护设备的 IPv6 报文解析能力、IPv6 地址格式配置（如黑白名单等）功能可能不完善；包含安全功能的网络系统（如流量控制系统等）也可能存在类似风险。

在 IPv4 环境下，系统漏洞扫描、WEB 漏洞扫描等设备一般按照 C 段/B 段地址进行扫描，目前主流的网络扫描设备可对外网或内网 IPv4 资产进行全面扫描。但 IPv6 地址长达 128 位，是 IPv4 的 296 倍，即使按 IPv6 默认的最小前缀划分区域（264 个地址）进行扫描，也难以实施。

上网日志留存系统在进行日志生成的过程中，需将 Radius 等设备的用户上网认证记录和防火墙 NAT 日志进行关联，可能存在不同系统间 IPv4、IPv6 匹配不一致的情况，导致日志缺失。

（三）IPv6 管理安全

由于目前还缺少相配套的安全管理措施，IPv6 网络的部署实施将对现网的 IP 资产监控、网络安全管理系统会产生影响，并对现有安全管理工作提出挑战[8]。

1. 资产暴露面安全管理

IPv4 网络广泛使用 NAT 技术，所有节点隐藏在 NAT 设备后面。部署 IPv6 后，如果网络出口未能部署有效的安全防护设备和访问控制策略，那么意味着内网主机 IPv6 地址裸露在全球互联网上，外网 IPv6 地址可以直接端到端连接访问内网 IPv6 设备，从而带来极大的安全风险[4]。

此外当前互联网资产暴露面以“IP 地址+端口”作为标识，IPv6 规模部署后资产暴露面的标识发生变化，相关的情报获取及分析工作将受到影响，包括如下方面：

a) 资产暴露面的探测：目前的资产发现主要是通过扫描工具对 IPv4 地址段进行逐个扫描，在 IPv6 环境下广泛的地址扫描已不可行。当业务系统采用 IPv6 部署时，对资产暴露面的远程探测能力提出了更高的要求。

b)资产暴露面指纹的获取：IPv6 条件下，需要资产指纹扫描工具具备对 IPv6 的支持，部分设备与系统需改造升级。

c)基础威胁情报的缺失：恶意 IP 地址及 IP 归属地是当前威胁情报分析中用到的最基本的情报。在 IPv4 条件下，这类情报易得、准确率高。但根据前期调研，现有的威胁情报库很少包括恶意 IPv6 情报，甚至存在地理位置归属不完善、定位不准确的现象。因此在 IPv6 规模部署过程中，IPv6 地址情报需要重新积累；这类信息的缺失将影响情报分析、可视化展现。

2. 域名解析安全管理

在 IPv4 网络应用编程中，程序员经常在代码中直接写入服务器固定 IPv4 地址，以提高数据通信效率。由于 IPv6 地址比较长，难以记忆，所以 IPv6 网络应用编程主要使用域名和 DNS 进行访问调度，取代在程序代码中写入固定地址。所以 IPv6 网络中 DNS 的重要性和价值将显著提高，成为最核心和最重要的基础设施[4]。

首先，IPv4 网络 DNS 系统记录的域名解析请求主要来

自于 NAT 设备的 IP 地址。而在 IPv6 网络中 DNS 解析请求主要来自于用户设备的 IPv6 地址，因此 DNS 系统日志将保存大量用户真实 IPv6 源地址信息。入侵 DNS 获取 DNS 系统日志数据，将成为黑客获得用户真实 IPv6 地址的重要方式。一旦 DNS 系统日志被窃取，可能造成大量用户的 IPv6 真实地址数据泄露。

其次，IPv4 网络中 DNS 系统重点防护 DDoS 攻击。而在 IPv6 网络上，DNS 安全防护的重点不仅是 DDoS，还要包括 DNS 系统自身安全和日志数据安全，防止数据泄露。预计未来 DNS 服务器将成为黑客的主要攻击目标。IPv6 网络安全管理必须要高度重视 IPv6 DNS 系统的数据安全防护。

最后，虽然目前主流操作系统都已支持 IPv6 的 DNS 解析，但行为有所区别，包括：优先使用 IPv4 还是 IPv6 发起 DNS 查询请求、优先查询 A 记录还是 AAAA、记录查询得到 2 个记录时优先使用 A 记录还是 AAAA 发起连接、IPv6 不可达时终端是否可以回退到使用 IPv4。经过实际测试，微软系列的 OS 优先使用 DNSv6，优先查询 A 记录（除 XP）。苹果系列 OS 优先使用 DNSv4，优先查询 AAAA 记录。全部 OS 优先使用 IPv6（AAAA 记录）发起网络连接。当 IPv6 不可达时，微软 IE 回退较慢，最长达 70 秒，用户体验差，苹果浏览器能够快速回退。因此，为满足监管机构技术指标要求，应针对不同客户端进行 IPv6 DNS 解析的详细测试。

3. 安全运营管理系统

除基础网络和安全防护设备之外，安全态势感知、SIEM、

SOC、堡垒机、零信任网关、邮件安全网关、统一身份认证等安全运营管理系统，此前均运行在 IPv4 网络环境中，同样需针对 IPv6 环境进行改造。对于 SIEM、SOC 等具备日志收集功能的系统，需要特别注意是否具备 IPv6 地址日志收集以及同一设备 IPv4 和 IPv6 双地址关联分析能力。

此外，在 IPv6 规模部署过程中，网站监控、防毒墙、数据库审计系系统、应用安全系统、网络 DLP 系统等系统需及时升级支持 IPv6，否则将存在业务系统提前改造而无法进行安全监管的风险。

四、IPv6 安全风险应对

综上分析，IPv6 的规模部署可能会带来一定的安全风险，RFC 9099[12]从多个方面提出了通用的 IPv6 安全运营注意事项。作为证券经营机构，建议从以下几个方面应对 IPv6 规模部署带来的安全风险：

（一）做好 IPv6 安全规划建设

对于新建 IPv6 网络区域，应提前做好 IPv6 网络安全规划，制定具体实施方案和推进工作计划，明确涉及的关键产品、网络及业务范畴，按照优先级分步骤实施。统筹 IPv6 地址申请、分配等管理工作，严格落实 IPv6 网络地址编码规划方案。应充分利用 IPv6 逐级、层次化分配密码生成地址的方法，对生成地址进行加密认证，防止设备仿冒接入和中间人攻击，从而消除源地址欺骗和利用邻居发现协议攻击的隐患。针对 IPv6 网络没有地址转换而带来的内网结构及相关信息暴露问题，可以利用 IPv6 新增的隐私扩展机制，

隐藏真实的通信地址，防止关键信息暴露，确保网络安全。

应结合相关网络与系统的建设需求，全面梳理 IPv6 带来的安全风险。同时系统规划和设计方案中，应包含整体 IPv6 安全方案，加强项目管理，确保按设计实时交付。新上线设备应采用行业最佳 IPv6 安全实践进行配置，不得使用默认配置，避免带来安全隐患。

对于已有 IPv4 网络改造，应深入了解各种 IPv4/IPv6 过渡机制可能带来的安全隐患，与设备厂商充分沟通，制定合理改造方案。如升级设备固件，应考虑升级后为兼容 IPv6 地址空间而可能带来的问题，如防火墙会话表容量、地址簿容量、新建连接速率、网络吞吐率可能会出现不同程度的减少；如更新设备型号，应考虑新型号设备中新特性可能引入的兼容性问题。同时应做好相应 IPv6 安全配置，避免应错误配置引入风险。

在设备选型方面，安全防护设备需支持纯 IPv6 环境下、过渡期间 IPv4/IPv6 双栈部署等场景的功能需求，具体可参考人行科技司印发的“银科技〔2019〕33 号文”《金融行业 IPv6 规模部署技术验证指标体系 V1.0》中“IPv6 自身安全”及“IPv6 部署安全”两个验证项。下一代防火墙设备需要支持 IPv4/IPv6 双栈协议及过渡时期的常用隧道技术，同时其集成的应用层网关需支持 IPv6 解析，应用识别、病毒检测、入侵防御等功能所需的规则库均需要升级，以支持纯 IPv6 或 IPv4/IPv6 双栈场景。在双栈网络中，须充分考虑 IPv4 和 IPv6 两个逻辑通道的安全需求，防火墙、WAF

等防护设备应具备对安全策略配置进行一致性检查等能力。应进行 IPv6 性能测试，验证 IPv6 网络区域的二三层网络设备、负载均衡、防火墙、WAF 等系统或设备的性能（CPU、内存、IO）不高于影响系统运行的阈值。

（二）加强 IPv6 网络安全运营

在 IPv6 运营过程中，对于新业务上线前严格开展 IPv6 安全风险评估，根据评估结果进行整改复核，未经评估不得上线。构建安全态势感知和重点业务安全保障两方面能力，通过构建针对 IPv6 网络的态势感知、威胁情报分析能力，开展主动防御。运行阶段，开展周期性风险评估检查、监测和审计，保证 IPv6 安全能力持续符合国家及监管机构管理要求。研究新型资产暴露面探测方式，以应对 IPv6 网络中难以进行全量扫描的情况。定期更新防病毒、恶意软件、IPS、WAF、态势感知等安全管控系统中的各类规则库和 IOC 库（如恶意攻击 IPv6 地址等）。及时与安全服务商沟通需求，确保其具备针对 IPv6 的设备维保、漏洞挖掘和渗透测试能力，及时发现 IPv6 安全隐患，提升 IPv6 环境下网络和系统安全能力。应定期开展 IPv6 安全测试工作，及时发现设备及信息系统 IPv6 相关脆弱性，避免设备“带病”入网。

在安全策略方面[3]，由于 IPv6 的地址、协议与 IPv4 有所不同，需要在防火墙、路由器、入侵检测和上网行为管理系统等安全设备上配置合乎业务需要的访问控制策略，关闭不必要的服务、禁止源路由，并实施单播反向路由查找技术，防止基于源地址欺骗的网络攻击行为。要根据网络使用实际，

管理 IPv6 协议各层通信，做好安全域的访问与隔离控制，采用恰当的网络过滤机制，实施网络接入许可。需谨慎设置 ICMPv6 报文的访问策略，根据实际情况选择合适的安全措施，例如配置 ACL 白名单，仅允许必须的 ICMPv6 等报文通过，接口关闭 ICMPv6 重定向、端口停止发送 RA 消息，关闭发送 ICMP 不可达信息，关闭源路由，防止 Type 0 Routing Header 攻击等，以免影响正常的服务和应用。在防火墙上需设置扩展头检查规则，设置具有选择发送和重组到网络中间设备的分片的能力，并支持防范 DDoS 攻击，能识别、过滤 type0 类型的路由扩展头报文。要在防火墙和边界设备上启用入口过滤机制，以减少网络间的源地址伪造威胁，做好边界防护。

在传统安全风险方面[3]，IPv6 继承了 IPv4 网络的一些应用层面的安全风险，因此传统的网络整体安全保障体系同样适用于 IPv6。一要未雨绸缪，安装防病毒软件，在用户终端建立防护之盾。二要筑牢防线，配备堡垒机、入侵检测、上网行为管理器和防火墙等网络防护系统，防止外部攻击，管控上网行为，严格实现内外网隔离。三要防止泄密与欺诈，使用数据加密和身份认证技术，确保数据完整可靠。最好采用混合加密和权威认证相结合的方式，提高网络安全防护级别。四要选用有自主知识产权自主可控的软件和硬件系统，提高系统与设备自身的安全可靠性。五要提高人员安全意识，整章立制，合理分配权限，严防内部作案。六要做好 IPv6 及相关应用的安全质量评估、健壮性和渗透性测试，不断进

行攻防演练，测试和堵塞IPv6协议漏洞，从根本上防范协议自身带来的风险。

（三）培养IPv6专业人才队伍

在部署IPv6的过程中，最大的威胁就是缺乏专业运营知识。IPv6环境下引入了扩展头攻击、NDP攻击等安全新威胁，使现有IPv4安全知识和经验难以直接应用到IPv6环境中，给企业安全技术人员带来新的挑战，导致IPv6相关业务的运维工作存在安全隐患，大量防御薄弱的IPv6协议栈成为攻击者实施网络攻击的新突破口。安全专业人员的IPv6知识储备不足，将引发无法充分认识和理解IPv6安全问题，无法有效应对IPv6安全防护需求等现实问题。如我司曾遇到过负载均衡设备无法正常探测IPv6业务端口的问题，经排查是由于防火墙默认阻断了ICMPv6协议的邻居发现报文所致。因此，应当加强IPv6安全知识和技能培训，提升IPv6相关工作人员安全能力。

IPv6将彻底改变原来IPv4时代的网络形态，特别是纯IPv6（IPv6-Only）网络将变得彻底扁平化，因此，证券行业IPv6规模部署要坚持发展与安全并举，网络安全系统同步规划、同步建设、同步运行，从而打造行业自主可控、安全可靠的IPv6网络。

五、参考文献

[1] 2021年上半年我国互联网网络安全监测数据分析报告[EB/OL]. 国家计算机网络应急技术处理协调中

心 .[2021.7].https://www.cert.org.cn/publish/main/upload/File/first-half%20%20year%20cyberseurity%20report%202021.pdf

[2] 政务外网 IPv6 发展演进白皮书[EB/OL].国家电子政务外网管理中心办公室.[2021.8]. http://www.sic.gov.cn/News/622/11031.htm

[3] 何淑玲，陈世清.IPv6 规模部署下网络安全风险防范[J].金融科技时代,2021,29(04):64-67.

[4] 赵肃波.中国 IPv6 发展与网络安全挑战[J].信息安全研究,2019,5(3):261-272.

[5] IPv6 规模部署下的网络安全防护[EB/OL].华为技术有限公司.[2018.1]. http://www.cnbp.net/events/2018huawei/pdf/szzf/IPv6%E8%A7%84%E6%A8%A1%E9%83%A8%E7%BD%B2%E4%B8%8B%E7%9A%84%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E9%98%B2%E6%8A%A4.pdf

[6] K. Chittimaneni, T. Chown, L. Howard, et al. Enterprise IPv6 Deployment Guidelines[EB/OL]. IETF RFC 7381. [2014.10]; www.rfc-editor.org/rfc/rfc7381.txt

[7] E. Davies, S. Krishnan and P. Savola. IPv6 Transition/Co-existence Security Considerations [EB/OL]. IETF RFC 4942.[2007.9]; www.rfc-editor.org/rfc/rfc4942.txt

[8] IPv6 安全白皮书[EB/OL].中国移动通信集团有限公司.[2018.12]. http://iot.10086.cn:81/Uploads/file/news/20181205/20181205173726_92618.pdf

[9] 筑牢下一代互联网安全防线—IPv6 网络安全白皮书[EB/OL].中国信息通信研究院.[2019.9].http://www.caict.ac.cn/kxyj/qwfb/bps/201909/t20190918_211484.htm

[10] 2021 全球 IPv6 支持度白皮书[EB/OL].下一代互联网国家工程中心.[2021.8].

https://www.ipv6ready.org.cn/public/download/ipv62.pdf

[11] IPv6 安全隐患的第一大来源[EB/OL]. 宋崟川.[2018.7].https://www.ipv6-cn.com/2018/07/10/IPv6-security-reflections-1.html

[12] É. Vyncke, Chittimaneni, K., Kaeo, M., and E. Rey. Operational Security Considerations for IPv6 Networks[EB/OL]. IETF RFC 9099.[2021.8] ; www.rfc-editor.org/rfc/rfc9099.txt