IPv6 技术安全防护应用与实践

（上交所技术有限责任公司供稿）

摘要：IPv6 技术是未来互联网的发展方向，随着 IPv6 网络的广泛应用和部署，IPv6 技术带来便利的同时也引入许多新的安全风险，包括 IPsec 漏洞、ICMPv6 漏洞等。引入 IPv6 技术安全防护，可以推动 IPv6 技术的发展和应用，保障 IPv6 网络的安全性，全面提升企业安全防护能力，有效保护企业业务、数据和财产安全。IPv6 技术安全防护落地需要依据现有安全防护体系，由外到内，统筹考虑基础设施安全配置、互联网侧安全监测、防护设备安全策略、应用流量安全加密等，结合 IPv6 技术，形成可落地的防护方案。

一、概述

IPv6 技术是下一代互联网协议，具有地址空间大、安全性高等优点，已经成为未来互联网的发展方向[1]。随着 IPv6 网络的广泛应用和部署，也面临着许多安全挑战，如地址扫描、中间人欺骗、漏洞利用等，这些攻击手段可能使企业遭受威胁和损失。

IPv6 技术是未来互联网的发展方向，IPv6 网络的广泛应用和部署是互联网发展的必然趋势。IPv6 技术防护落地实践是为进一步推动 IPv6 技术的发展和应用，可以有效避免各种网络攻击和恶意行为，降低网络延迟和丢包率，提高网络的效率和性能，保障 IPv6 网络的安全性，全面提升企业安全防护能力，有效保护企业业务、数据、财产安全。

二、IPv6 改造难点

(一) 协议兼容性

IPv6 与 IPv4 协议栈不兼容，需要考虑现有网络设备，如路由器、交换机、防火墙、负载均衡等，以及软件基础设施操作系统、数据库、Web 中间件等，对 IPv6 的支持情况，对于无法支持的现有系统协议栈需要进行升级。升级需考虑操作系统版本、应用程序兼容性等问题，确保升级后系统可正常运行。但由于部分老旧的应用程序仅支持 IPv4，需要对程序的配置文件进行优化。

(二) 网络架构

IPv6 网络规模部署后需申请专用地址段，由于地址规模较大，既要保证与当前 IPv4 网络设计吻合，又要考虑业务类型增加和用户数增长，合理分配地址空间，同时还要考虑地址使用的安全性。

(三) 安全性

当前金融机构基本都在 IPv4 网络下建立了相对完整的安全防护体系，但 IPv6 相关软硬件仍处应用初期，尚不具备完善的安全机制，IPv6 地址标识较为复杂，流量清洗、入侵检测等基于网络地址标识解析的传统防护手段将面临挑战，同时 IPv6 的新特性也可能带来扩展头攻击等新型安全风险。

三、IPv6 改造方案

在当前的网络环境中，IPv6 协议并不能立即取代 IPv4 协议，在未来很长一段时间中，二者将共存在同一网络环境

中。在这段过渡时期，主要有三种技术方案可用于二者的兼容：

方案一是隧道技术，将局部 IPv6 网络的 IPv6 数据包作为数据封装到 IPv4 数据包，使得 IPv6 数据包可以在 IPv4 网络中传输。在隧道机制中，IPv6 数据包被封装在 IPv4 数据包中，实现在 IPv4 网络中传输。此方式适用于孤立的 IPv6 网络，通过 IPv4 网络通信，沿途经过的网络设备不需要改造。

方案二是双协议栈技术，通过保有一个 IPv4 协议栈以及一个 IPv6 协议栈，实现并轨运行；双协议栈是 IPv4 和 IPv6 同时存在于一台设备上的方式，设备可以同时使用 IPv4 和 IPv6 协议栈，从而实现 IPv4 和 IPv6 的共存[2]。双协议栈可以保证 IPv6 网络的逐步部署和升级，并且不会影响 IPv4 网络的正常运行，是改造最为彻底的方案。

方案三是网络地址转换（Network Address Translator，NAT）技术，通过 NAT 实现 IPv4 和 IPv6 主机的互通。目前常用的 IPv6/IPv4 转换技术为 NAT64，可实现 TCP、UDP、ICMP 协议下的 IPv6 与 IPv4 网络地址和协议转换[2]。

结合上海证券交易所实际情况，选用方案三即网络地址转换技术方案作为 IPv6 改造方案。在 IPv6 和 IPv4 网络间部署协议转换设备（如 NAT64 协议转换设备）作为网络网关，IPv6 和 IPv4 网络流量通过此网络网关进行地址转换，从而建立、维护 IPv6/IPv4 之间地址和端口的映射关系，以

实现透明的 IPv6 和 IPv4 互访，并能够获取到并记录真实的访问源地址。

四、IPv6 技术安全防护

随着 IPv6 技术的广泛应用，其安全问题也逐渐凸显。IPv6 网络的攻击方式多样，攻击技巧不断更新，企业需要采取相应的措施来保护网络安全。

(一) 基础配置

IPv6 基础配置通常包括以下几个方面：IPv6 地址、路由器、接入控制、DNS、DHCPv6,管理员需要对这些组成部分进行合理的配置和管理，以确保 IPv6 网络的安全和稳定运行。

1、IPv6 地址：IPv6 地址是 IPv6 网络中的唯一标识符，与 IPv4 地址相比，IPv6 地址具有更加丰富的地址空间，可以为更多的设备提供唯一的地址。管理员需要配置 IPv6 地址，限制 IPv6 地址的使用范围，以确保 IPv6 地址的安全性。

2、路由器：IPv6 路由器在传递数据包时，需要确保数据包的来源和目标是可信的。管理员需要配置 IPv6 路由器，启用路由器安全功能，防止路由器被攻击或篡改，导致网络安全问题。

3、接入控制：管理员需要限制接入 IPv6 网络的设备类型和数量，设置访问控制策略等[3]。可以采用 ACL（Access Control List）等技术，实现对 IPv6 网络的访问控制，保护网络安全。

4、DNS:IPv6 网络需要使用 IPv6 地址解析服务（DNS）

来解析IPv6地址和主机名之间的映射关系。管理员需要配置IPv6 DNS服务器，确保IPv6网络中的DNS服务正常运行。

5、DHCPv6：动态主机配置协议（DHCPv6）用于自动为IPv6设备分配IPv6地址和其他网络参数。管理员需要配置IPv6 DHCPv6服务器，确保IPv6设备能够自动获取正确的IPv6地址和其他网络参数。

(二)防火墙策略优化

防火墙是IPv6网络安全防护的重要组成部分，可以实现对IPv6网络的访问控制和流量过滤，防火墙的配置全面与否是关系到IPv6安全性重要的环节：

1、启用IPv6防火墙，需要启用IPv6防火墙，并对其进行配置。可以采用现有的防火墙技术对IPv6网络进行访问控制和流量过滤。

2、确定防火墙策略，需要根据实际情况，确定防火墙的策略。需要考虑IPv6网络的特点和安全威胁，对网络流量进行过滤，保护网络安全。

3、定期更新防火墙规则，需要定期更新防火墙规则，确保防火墙的有效性并及时监测网络威胁，对新出现的威胁进行规则更新。

(三)入侵检测和入侵防御部署

入侵检测和入侵防御是保护IPv6网络安全的重要手段。管理员需要定期检测网络入侵事件，并及时采取相应的防御措施。所有IPv6应用均不低于原有IPv4的防护标准。

1、启用入侵检测系统，需要启用入侵检测系统（IDS），对网络流量进行实时监测，及时发现潜在的攻击威胁。IDS可以识别各种攻击类型，如DDoS攻击、漏洞利用等，并发出警报通知管理员。

2、启用入侵防御系统，需要启用入侵防御系统（IPS），对网络流量进行实时监测，并对恶意流量进行拦截和过滤。IPS可以防止各种攻击类型，如DDoS攻击、拒绝服务攻击等，并在攻击发生时及时采取相应的防御措施。

3、定期更新入侵检测和入侵防御规则，需要定期更新入侵检测和入侵防御规则，确保系统的有效性。需要及时监测网络威胁，对新出现的威胁进行规则更新。

(四)加密和身份认证

加密和身份认证是保护IPv6网络安全的另一重要手段。管理员需要对敏感数据进行加密，并采取身份认证措施，防止未经授权的用户接入网络。加密和身份认证需要注意以下几点：

1、启用加密协议，管理员需要启用加密协议，对敏感数据进行加密传输。可以采用TLS/SSL等加密协议，确保数据传输的机密性和完整性。

2、启用身份认证机制，管理员需要启用身份认证机制，防止未经授权的用户接入网络。可以采用AAA（Authentication、Authorization、Accounting）等身份认证技术，对用户进行身份认证，确保网络安全。

3、定期更新加密和身份认证规则，管理员需要定期更

新加密和身份认证规则，确保系统的有效性。需要及时监测网络威胁，对新出现的威胁进行规则更新。

(五)制度保障和运维

1、制定 IPv6 改造实施制定的应急预案，定期组织相关的应急演练。制定较为完备的业务连续性方案，定期对相关的预案进行评估修订。

2、IPv6 相关网络、系统和应用信息建立监控运维体系、部署日志审计系统，所有 IPv6 应用监控和日志保存标准均不低于原有 IPv4。

五、IPv6 技术防护实践应用

本所目前对使用的网络及网站进行了 IPv6 的升级防护，取得了显著性的效果，同时也积累了相关经验。整个防护的落地实践，提高了网络性能，简化了网络管理，增强了网络的安全性，使得 IPv6 网络更难遭到网络扫描和恶意攻击的威胁。具体体现在以下方面：

1、通过对 IPv6 进行合理的配置和管理，设置访问网络控制权限，目前已实现互联网重要业务系统支持 IPv6 网站访问，其中门户网站支持率达到 100%。www 域名及二级以上域名具备 AAAA 解析记录，公众递归服务器能够得到解析并且整个递归解析过程全部通过 IPv6 完成，同时 IPv4 的域名和支持 IPV6 的域名为同一域名。

2、IPv6 技术改造后，网站支持 IPv4 和 IPv6 访问，网站监测云防护已从原始的 IPv4 监测，变更为 IPv4 到 IPv6 同步检测，通过更改网站策略，增加漏洞以及攻击面的识别，

漏洞数量较之前明显降低。

3、在 NAT 转换设备上配置安全防护，抵御 NAT 相关攻击。使用 IPv6 路由协议时，在路由设备上配置路由协议安全，抵御路由协议攻击。且针对 IPv6 相关网络、系统和应用信息部署了日志系统，及时更新防火墙规则，实时反馈系统异常行为，增强系统可用性。

六、总结

IPv6 改造是一项复杂的系统性工程，推进 IPv6 规模化部署是一项长期的工作。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，是构建安全可信 IPv6 网络的方法论。IPv6 规模化部署要实现所有应用的迁移，并确保所有迁移应用能够安全稳定的运行，需要系统性的开展建设工作。构建 IPv6 安全防护体系，需推动加强运维支撑平台对 IPv6 的支持能力，不断完善 IPv6 基础设施，确保应用系统在完成 IPv6 迁移后能够安全稳定运行。同时，结合 IPv6 技术防护方案，从设备安全管理、流量安全监测、安全策略配置等方面进行全面推进，确保 IPv6 网络的安全性和稳定性，持续推动应用系统 IPv6 技术安全防护落地实践[3]。

七、参考文献

[1]李伟.金融行业 IPv6 规模部署取得阶段性成效[J].金融电子化,2020(2):11-12.

[2]吴达旻.金融机构 IPv6 改造方案分析[J].金融电子化,2020(2):25-26.

[3]刘萌.金融业 IPv6 规模部署应对思考[J].金融科技时代,2021,29(10):90-93.