IPv6 环境下水利业务网安全防护技术研究与实现

李　莹　葛召华　庄　磊

山东省水利综合事业服务中心　山东济南　250004

摘　要：IPv6 环境下水利业务网安全防护技术的应用，直接关乎着水利网络系统能否稳定运行、敏感数据的安全性以及网络系统应对各类攻击、风险的能力。本文从事 IPv6 环境下水利业务网安全防护技术研究与实现策略探讨，在对 IPv6 环境下水利业务网络安全风险类型加以分析后，围绕 IPv6 网络边界保护技术、IPv6 网络终端安全加固技术开展深度研究，从而为我国水利管理部门提供借鉴与参考的价值，促进其合理打造网络安全防护体系，为水利业务网安全运行作出有效推动。

关键词：IPv6；网络安全；IPv6 网络终端安全加固；IPv6 网络边界保护

Research and implementation of water conservancy service network security protection technology under IPv6 environment

Li Ying Ge Zhaohua Zhuang Lei

Shandong Water Conservancy Comprehensive Service Center，Jinan 250004，China

Abstract：The application of security protection technology of water conservancy service network under IPv6 environment is directly related to the stable operation of water conservancy network system，the security of sensitive data and the ability of network system to deal with various attacks and risks. This paper is engaged in the research of security protection technology and implementation strategy of water conservancy service network under IPv6 environment. After analyzing the types of security risks of water conservancy service network under IPv6 environment，in-depth research is carried out around IPv6 network boundary protection technology and IPv6 network terminal security reinforcement technology，so as to provide reference value for Chinese water conservancy management departments. Promote its reasonable construction of network security protection system，and effectively promote the safe operation of water conservancy business network.

Key words：IPv6；Network security；IPv6 network terminal security hardening；IPv6 network boundary protection

在 IPv6 环境下配置完善的水利业务网络安全防护技术，可以有效保护水利业务系统，保障资源的安全利用，提高水利业务系统的稳定性和可靠性，同时可以降低水利业务网络遭受攻击和数据泄露等风险的可能性，为水利业务系统的健康可持续发展提供更加可靠的技术保护。因此，从事 IPv6 环境下水利业务网安全防护技术研究与实现探讨，是进一步促进水利业务网安全性，保障水利系统各项业务稳定运行的重要研究行为。

一、IPv6 环境下水利业务网络安全风险类型分析

（一）数据泄露风险

IPv6 环境下的网络协议对于安全防护措施，提出了更高更详细的要求，在数据传输过程中，应用程序基于 IPv6 协议合理性，会存在较多软件漏洞，从而面临更多数据泄露风险。一旦水利业务系统被入侵后，攻击者可通过非法获取数据的方式，实现对水利数据的窃取，对水利设备、水文仪器等进行远攻击，给水利系统的正常运行带来严重威胁。

（二）远程攻击风险

由于 IPv6 的特性和广泛的连接性，水利系统可能成为攻击者的目标。这些攻击可能导致以下风险：①拒绝服务攻击：攻击者可能通过洪水攻击或资源耗尽攻击来占用水利业务网的带宽和资源，使其无法正常工作，导致服务中断和系统瘫痪。②网络侦听和窃听：IPv6 的地址空间庞大，攻击者可以利用这一特点进行网络侦听和窃听操作，截取敏感信息和控制指令，造成严重的数据泄露风险。③远程控制攻击：攻击者可能利用安全漏洞或弱密码对水利业务网进行远程控制，篡改操作、损坏设备，甚至导致事故发生，造成人员伤亡和财产损失。④恶意软件和病毒攻击：通过恶意软件和病毒感染，攻击者可以在水利业务网中传播恶意代码，破坏系统功能，篡改或破坏数据，影响水利系统的正常运行。⑤社会工程攻击：攻击者可能利用社交工程手段，通过诱骗、钓鱼等手段获取合法用户的敏感信息，入侵水利业务网，进而发起远程攻击。

（三）路由器攻击与 DDoS 攻击

IPv6 网段有更大的地址空间，而路由器也需要处理更多的数据包，因此攻击者可以针对路由器进行攻击，对网络带宽和稳定性造成威胁。同时，Pv6 环境下的地址数量比 IPv4 更多，因此 DDoS 攻击者可以对网络进行更强的攻击，从而对水利业务造成更严重的威胁。

二、IPv6 环境下水利业务网安全防护技术研究与实现

（一）IPv6 网络边界保护技术研究与实现

1.技术研究

IPv6 网络边界保护技术的工作是通过设置访问控制列表（ACL）和使用访问保护技术，拒绝来自非法和未经授权的访问，只允许被认可的访问进入或离开 IPv6 网络。其在工作阶段的具体防护策略包括 IP 地址筛选和源地址验证，限制 IP 数据包的流向，两项功能的融合，可有效防止黑客攻击和网络病毒的侵入，防止网络流量被滥用，消除网络攻击和数据泄露的风险，提高网络的稳定性和业务的安全性。

水利业务网 IPv6 网络边界保护技术的实现思路是首先识别出水利业务网络的网络边界，包括物理边界和逻辑边界。物理边界是具有实际地理位置的网络硬件设备，如路由器、交换机、防火墙等，逻辑边界是指定义的可接入和不可接入网络的界限。其次，根据水利业务需求，定义访问控制列表（ACL）规则，制定访问控制策略。最后，IPv6 网络边界保护技术会配置防火墙设备，实现系统运行阶段的访问控制。

2.实现方法

实现水利业务网下的 IPv6 网络边界保护，其具体步骤包括确定网络边界→→制定访问控制策略→→配置网络防火墙→→源地址认证。

步骤 1：确定网络边界。识别和确定水利业务网的网络边界。网络边界主要包括硬件设备（如防火墙、路由器等）和逻辑边界，包括确定哪些网络是可信任的，允许接入，哪些网络是不被信任的。这样能够形成一道清晰的防线，有效地隔离互联网和内部网络。

步骤 2：制定访问控制策略。根据水利业务网业务需求，制定访问控制策略，明确哪些访问是允许的，哪些是禁止的。具体可以通过定义访问控制列表（ACL），明确指出源 IP 地址、目的 IP 地址、源端口、目的端口、协议类型、接口等条件，来对数据包进行筛选。

步骤 3：配置网络防火墙。在防火墙上实施预先制定的访问控制策略。该步骤需要对边界防火墙或路由器进行具体的配置，实施 ACL 的规则。同时，考虑到 IPv6 的新特性，如地址自动配置和邻居发现等，技术人员对防火墙的配置也要相应做出调整。

步骤 4：实施源地址认证。对水利业务网络内的设备实施源地址认证，防止地址欺骗和欺诈。具体可以通过开启 IPv6 的源地址验证机制（如 BCP38，对出口流量进行过滤），禁止非法的地址或者伪造的地址进入网络。

此外，在建设水利业务网 IPv6 网络边界保护系统过程中，技术部门需注意如下要点。第一，除了确保可靠的来源地址和封闭未授权的访问之外，还需要对内部和外部的网络流量进行严密的分割，以避免恶意流量穿越网络边界。第二，定期对边界设备进行检查和维护，以防新出现的威胁和漏洞。第三，网络信息管理部门应设立监控制度，实时发现并处理网络中的异常事件和攻击行为。

（二）IPv6 网络终端安全加固技术研究与实现

1.技术研究

IPv6 网络终端安全是指在 IPv6 环境下，防护对网络终端设备（如计算机，服务器等）的各种攻击，重点考虑 IPv6 独特的特性，如大量地址空间，自动配置，邻居发现等。其核心原理是通过对网络终端的配置寻址，网络接入，数据传输等环节的安全管理，达到防范和抵御潜在攻击的目标。防护效果表现在保证网络终端的正常运行，维护数据的完整性，确保网络的畅通性，提升网络的稳定性。

2.实现方法

水利业务网 IPv6 网络终端安全加固技术应用思路包含五部分，第一是地址安全，即通过禁用不必要的 IPv6 地址和服务，减少攻击面。第二是访问控制，通过配置访问控制策略，限制非法访问。第三是数据保护，通过数据传输中的加密和完整性校验，保护数据安全。第四是设备管理，即通过设备的身份验证和安全更新，保证设备的安全。第五异常监测，通过实时的异常监测和应急处置，防止和解决安全问题。

具体实现期间，步骤 1：进行 IPv6 地址管理。在 IPv6 环境下，网络地址数量可以达到天文数字级别，但这也带来了新的安全威胁，如地址扫描、地址欺骗等等。因此，必须建立完善的 IPv6 地址管理策略和流程，对网络中的 IPv6 地址进行管理和监控。第一，严格控制 IPv6 地址分配和使用，在水利业务网络规模较大的情况下，应采用 DHCPv6 来进行地址分配，同时配置地址池和地址范围，以达到有效控制地址分配的目的。第二，采用地址管理方案，对 IPv6 地址进行分类和组织，便于快速识别和管理。第三，对重要网络资源，如服务器、路由器、交换机等设备进行 IPv6 地址指定，避免使用自动分配的地址，以提高网络的安全性。第四，进行 IPv6 地址跟踪和收集，及时进行地址池的清理和更新操作，以保证网络稳定和安全。

步骤 2：访问控制配置。第一，对不同级别的 IPv6 用户进行身份认证和授权，实施网络访问控制。第二，控制 IPv6 用户和设备的网络访问，规定用户和设备可访问的网络服务以及可访问的目标地址和端口。第三，配置 IPv6 访问控制列表（ACL），对流量进行规则匹配和过滤。第四，采用 IPv6 防火墙、入侵检测和防护系统（IDS/IPS）等技术实现网络安全访问控制。

步骤 3：数据传输安全配置。第一，设置加密和解密数据，采用 IPv6 加密技术，如 IPsec 等实现 IP 层的加密传输，保证数据传输的安全性。第二，对敏感数据进行加密，如密码、账户信息等，采用 SSL、TLS 等技术实现数据的加密传输。第三，限制敏感数据的传输范围，通过 IPv6 ACL 控制敏感数据的传输范围，避免数据泄露的风险。

步骤 4：设备安全管理。在水利业务 IPv6 网络中，设备安全管理是非常重要的一环，包括实现设备健康状态的监控、设备漏洞的修复和设备的安全管理等方面。第一，对设备进行安全加固，包括关闭不必要的服务、更新设备的操作系统和相关软件、实现强密码授权等。第二，配置日志监控，SDK logs 以及系统日志进行完整记录，及时掌握设备状态和漏洞情况。第三，进行设备的弱点扫描、漏洞扫描等操作，及时进行修复。第四，设备管理采用统一身份认证、访问控制、流量限制等技术，以确保设备管理安全。

步骤 5：安全监测和应急处置配置。针对 IPv6 网络安全风险的不断变化和增长，水利管理部门必须建立完善的网络安全监测系统，对网络安全威胁和攻击监测，并及时采取应急处置措施。具体实践阶段，第一，水利部门信息技术中心/网络管理部门需要建立完善的安全事件管理系统，及时监测和分析网络中的安全事件。第二，在系统中应用、自动化监测技术，及时发现并应对网络安全威胁和攻击。第三，在信息技术中心或网络安全管理部门中成立网络应急响应组，及时响应网络安全事件，在最短时间内恢复网络服务。第四，建立网络安全备份和灾难恢复机制，定期备份重要数据和系统信息，以保网络数据安全性。

结语：

随着 IPv6 的广泛应用，水利业务网的安全威胁逐渐增加。针对当前这一高风险的环境，配置 IPv6 环境下水利业务网的安全防护技术，不论是对于业务运行还是未来组织机构的可持续发展而言均至关重要。因此，水利管理部门可借鉴本文研究成果，结合组织机构自身特点，合理在 IPv6 环境下配置网络安全技术，以最大化降低网络安全风险的发生概率，为水利业务网络安全、稳定运行提供坚实技术保障。

参考文献：

[1]王吉昌，张连成，杨剑波等.基于多类型威胁的 IPv6 安全防护有效性检测方法[J/OL].郑州大学学报（理学版）：1-8[2023-10-12].

[2]刘汉刚，王宾启，赵文竹等. 基于 IPv6 技术的智慧水利感知应用研究[C]//河海大学，武汉大学，长江水利委员会网络与信息中心，湖北省水利水电科学研究院.2023（第十一届）中国水利信息化技术论坛论文集.[出版者不详]，2023：20.

[3]张然.高校 IPv6 网络安全风险与应对措施[J].网络安全技术与应用，2022（05）：100-101.

[4]牟舵，肖尧轩，张飞等.珠江流域水利网络安全能力提升探析[J].水利信息化，2020（05）：41-45.

[5]林坚.福建省水利厅 CNGI 驻地网建设探讨[J].水利科技，2006（03）：50-52.