Computer Science and Application 计算机科学与应用, 2022, 12(12), 2706-2711
Published Online December 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.1212274

Hans汉斯

校园网IPv4向IPv6过渡的安全分析

——以伊犁师范大学为例

张体谅，张　斌*，刘新茂，李　杨，王彦同

伊犁师范大学，信号检测与控制技术重点实验平台，新疆　伊宁

收稿日期：2022年11月1日；录用日期：2022年11月30日；发布日期：2022年12月7日

摘　要

本文以伊犁师范大学为例，分析IPv4向IPv6过渡时存在安全风险，旨在降低安全风险点，树立四位一体安全防护体系，以双栈安全通信网络、双栈零信任安全区域边界、双栈安全计算环境、双栈安全管理中心四个维度为出发点，通过相关技术手段和创新思维理念，建立一体化防护运维体系和网络安全建设，提高了学校双栈网络安全性；也为其它高校IPv4/IPv6双栈安全运营提供借鉴。

关键词

伊犁师范大学，数据中心，双栈，IPv4，IPv6，安全

Security Analysis of IPv4 to IPv6 Transition in Campus Networks

—Taking Yili Normal University as an Example

Tiliang Zhang, Bin Zhang*, Xinmao Liu, Yang Li, Yantong Wang

Key Experimental Platform for Signal Detection and Control Technology, Yili Normal University, Yining Xinjiang

Received: Nov. 1st, 2022; accepted: Nov. 30th, 2022; published: Dec. 7th, 2022

Abstract

Taking Yili Normal University as an example, this paper analyzes the security risks in the transition from IPv4 to IPv6, aiming to reduce security risk points, establish a four-in-one security pro-

*通讯作者。

文章引用: 张体谅, 张斌, 刘新茂, 李杨, 王彦同. 校园网 IPv4 向 IPv6 过渡的安全分析[J]. 计算机科学与应用, 2022, 12(12): 2706-2711. DOI: 10.12677/csa.2022.1212274

tection system, take the four dimensions of dual-stack secure communication network, dual-stack zero-trust security zone boundary, dual-stack secure computing environment, and dual-stack security management center as the starting point, establish an integrated protection operation and maintenance system and network security construction through relevant technical means and innovative thinking concepts, and improve the security of the school's dual-stack network. It also provides reference for IPv4/IPv6 dual-stack security operations in other universities.

Keywords

Yili Normal University, Data Centers, Dual-Stack, IPv4, IPv6, Safe

1. 引言

伊犁师范大学数据中心采用平台双栈融合建设与运营模式，相比于专线与裸光纤的教育专网组网方案，降低组网成本，提高了网络接入的灵活性。基于这种融合的建设模式，必须加快学校数据跨区域资源安全整合，实现数据共享。但是近年来安全态势不容乐观，双栈的安全风险，制约伊犁师范大学数字化校园的发展和 IPv6 的建设速度，因此必须建设一套完善双栈的安全防护体系。

IPv6 比 IPv4 有更多的信息和数据源，针对这些风险，我们采取一系列举措进行应对：从技术上，加大对 IPv6 安全威胁和防护技术的研究投入和前瞻部署。二是分阶段部署研究 IPv6，降低安全风险点，加强管理维护并对 IPv6 进行深入分析和研究。三是采用扁平化的网络架构，建立四位一体的双栈安全防护体系，通过数据中心防火墙建立 DDOS 防护、SLB 安全防护、主机 IPv6 安全防护；防护策略实施先外网后内网，先边缘后核心，先简单后复杂，先双栈后纯 IPv6 的安全架构。

2. 双栈数据中心面临的安全挑战

2.1. 传统威胁

传统攻击事件(DOS 攻击、路由选择攻击、应用层攻击)依然存在。

1) 病毒木马查杀，通过检测并清除网络终端、节点或系统软硬件中插入植入的恶意代码，并设法迭代检出恶意代码并删除，报警、隔离、人工接入、防止传播扩散。

2) 漏洞发现与修补，用补丁方式修补目标系统软硬件代码设计中存在的安全缺陷，引入不同层次的动态技术，避免病毒木马注入或者降低漏洞的可利用率。

3) 攻击感知与阻断，发现不规范的蓄意行为和特征，通过攻击行为的特征感知，阻断攻击链或者降低攻击链的可靠性，借助大数据和人工智能等技术发现或者抑制可能的攻击行为。

2.2. 双栈威胁

1) 跳板威胁

伊犁师范大学 IPv4 向 IPv6 过渡网络建设采用双逻辑通道的双栈模式，以 IPv4 网络为跳板，双栈网络潜在存在传统的 DDOS、注入、勒索病毒等攻击威胁。

2) 区域边界出口安全威胁

IPv6 环境下设备使用全球唯一单播地址，无需经过 NAT 转换，双栈数据导致真实的地址暴露——内网主机 IPv6 裸露在互联网上，互联网和教育网可以直接端到端访问学校内网双栈资源，增加了系统暴露性和安全管理复杂度，攻击者可以利用隐蔽 IPv6 通道攻击。

3) 协议本身威胁

IPv6 报文结构中引入的扩展字段、协议族中新协议可能存在漏洞，可被用于发起嗅探、DOS、MLD 仿冒及泛洪攻击。

利用 IPv6 的特性进行无状态地址扫描。大量物联设备使用 EUI-64 标准为设备无状态自动配置 IPv6，使黑客可以有针对性的扫描。部分 DPI 设备存在对 IPv6 报文解析和输出不完备的风险，同时 DPI 识别规则库(如 IP 地址归属)在 IPv6 场景下可能存在缺失，影响设备功能用户认证系统与其他系统之间 IPv4 与 IPv6 匹配不一致，会导致上网日志缺失。

4) 数据泄露威胁

DNS 系统、站群系统是数据中心 IPv6 网络安全防护的核心，一旦 IPv6 系统日志窃取，可能造成大量用户的 IPv6 基本数据泄露。

5) 安全运维体系不健全

安全管理人员不足，对双栈网络安全态势感知与预判能力有限，没有完整的智能化主动防御体系。缺乏体系化运维，一体化协同防御的手段；存在传统安全防御模式的弊端，表现为单点防御、单边防御、单片防御、头疼医头、脚疼医脚。

3. 树立四位一体安全防护运维体系

树立四位一体安全防护体系，建立双栈安全通信网络、双栈零信任安全区域边界、双栈安全计算环境、双栈安全管理中心四个维度，打破传统思维模式，建立一体化防护运维体系，创新安全联动机制，实现全域感知、精准预测、立体纵深、敏捷可变、智能进化。

3.1. 双栈安全通信网络体系

1) 端到端安全传输通道

建立端到端 IPSec 的认证和加密，利用 IPv6 逐跳选项头、选路头、目的地选项头、身份验证头(AH)、封装安全性净荷(ESP)头等扩展选项，使用 IPv6 扩展头和目的地节点建立连接，使用 IPv6 Flow Label 字段域建立流标记通道进行数据包传输，对流的精准识别，匹配流转发策略，避免三角路由。并通过 IPv6 邻居发现[1]机制实现本区域内其它网络的发现并转交，建立端到端传输，增安全性和透明度，通过 SRv6、随流检测、流量工程、分段路由实现端到端安全传输。

2) 建立隐私保护机制

海量的 IPv6 地址使每一个设备都可以获得一个唯一的地址，隐藏了巨大的隐私风险。对于终端用户，由于每个 IPv6 地址包含计算机的 MAC 地址，为了避免 MAC 地址暴露主机的隐私性，其隐私性是基于 RA 路由前缀通过网络前缀产生一个基于 64 位扩展唯一标识 SLAAC 地址，地址组成是网络前缀 + MAC 地址。终端获取的 IPv6 地址在一定时间内自动改变。目前主流操作系统一般以隐私地址[2]的优先级别最高，即优先以隐私地址向外网发起连接，同时由于隐私策略生效，终端每隔一段时间都变更临时地址，这样攻击者很难准确进行攻击，攻击难度增大。在路由侧通过双栈路由器自动发现功能识别本地链路相连的设备，实现前缀自动绑定，避免类似于 IPv4 网络的 ARP 攻击，同时路由设备开启 NDP 重复地址检测功能，使用三层的安全机制避免地址解析攻击，提供隐私保护。

3) 建立加密体系

利用 IPv6 身份验证头(AH)、封装安全性净荷(ESP)头等扩展选项增加 IPSec 端到端的加密，抵御扫描类型网络攻击，提供 IPv6 的 HttpsWEB 认证，采用国密算法使用 WEBSDK 的加密调用站群接口。

3.2. 双栈零信任安全区域边界体系

1) 边缘管控

收敛互联网络双栈暴露面，加强双栈攻击点管控；网络边缘通过出口防火墙、IVI 翻译设备，第二代蜜罐、沙箱、诱捕等方式做好精准防控，建立 DDOS 防护、SLB 安全防护、主机 IPv6 安全防护；防护策略实施先外网后内网，先边缘后核心，先简单后复杂，先双栈后纯 IPv6 的零信任区域边界安全架构。

2) 身份管控

经过身份准入准出，双栈认证、网络流量加密实现区域边界零信任。使用 IP 地址、物理位置、身份标识为依据，访问双栈资源，攻击者发起主动攻击或者被动攻击的行为，通过监听网络流量获取相关信息，进行风险处置。

通过与校园统一身份认证系统的单点登陆对接，用户使用统一身份认证系统账号完成实名绑定 MAC，获取到双栈地址接入网络，实现 IPv6 的统一分配管理和用户认证整合，有效精确识别和跟踪同一用户的 IP 地址状态，在 IPv6 隐私策略配合校内智能 DHCP [3]系统下实现无感知认证、计费和审计，记录双栈用户的登陆信息。

目前伊犁师范大学大量终端采用 PPPoE 代拨方式，认证平台基于 IPoE 和 Portal 的架构，双栈认证基于 BRAS 的 Radius 报文交互实现 IPv4/IPv6 联动上下线。将 IPv6 的统一分配管理和用户认证整合，有效精确识别和跟踪同一用户的 IP 地址状态，实现无感知认证、计费和审计。

3.3. 双栈安全计算环境理念

双栈安全计算环境，结合人工智能、网络欺骗及博弈论等相关方法，对大量安全威胁数据进行关联性分析，通过软硬件安全防护相结合，对各类网络安全威胁的有效检测，提升安全检测效率、精准度和自动化程度。建立计算模型快速理解、识别和检测复杂的攻击链和潜在威胁，通过双栈网络及安全设备的实时测试和数据包分析提出安全对策。

3.4. 双栈安全管理中心体系

建立双栈安全管理中心，管理人员必须进行政治考核和具备相关技术能力。实行权限最小分配原则，划分系统管理员、操作员、审计员，权限不交叉；网络和系统设置双重 ACL 防控列表，允许特定主机和特定人员通过指定账号登录堡垒机，由堡垒机进行统一登录和管理双栈设备；日志溯源能力，堡垒机提供接口连接至日志审计平台，对视频及操作日志进行标准化存储，方便及时调取和解析。最终面向管理人员对双栈资源调取和操作使用流程的各个环节，实现可管、可控和可追溯的双栈网络安全管理。

4. 安全建设

4.1. 安全体系

以四位一体安全防护体系为基础，做好 IPv4/IPv6 双栈防护，实现防护多层次、多维度，加固关键点，感知全方位。

1) 建立完善双栈技术安全体系[4]

包括基础设施安全、系统安全、服务安全、数据安全、应用安全和固件安全，明确相关主题的行为

安全保护权限和访问控制机制，避免被泄露数据、篡改数据、未授权数据的流传，形成权数据生命周期的安全防护体系。利用 IPv6 随流检测、应用感知能力提供先进安全风险管理方向和风险量化管控安全精细化策略降低传统和双栈网络的威胁。

2) 建立联动机制

安全产品相关联，联动处理安全风险，利用学校态势感知平台、上网行为、防火墙做联动，及时预防处置双栈风险，预警信息的自动分发、安全威胁的智能分析、响应措施的联动处置，构建集威胁检测、实时防护、动态响应、态势预测为一体的智能网络安全主动防御体系。

3) 集中化管控

集中管控双栈安全产品，搜集所有网内资产的安全信息，集中化管控并通过对收集到的各种安全事件进行深层的分析、统计、和关联，及时反映被管理资产的安全情况，定位安全风险，对各类安全事件及时发现和定位，并及时提供处理方法和建议，协助管理员进行事件分析、风险分析、预警管理和应急响应处理。

4) 建立安全应急响应

提前规范进行防范，做好安全人才技术储备，做好修补，提高有效的安全人力保障和双栈网络技术支撑，对互联网暴露面资产列表及资产的相关指纹信息的管控。

5) 搭建双栈辅助平台

利用 IPv6 扩展性和可变成行，构造 IPv4/IPv6 双栈辅助工具快速定位故障，事半功倍完成 IPv6 的维护工作。

4.2. 安全业务

在缺乏先进经验的条件下，应对双栈网络空间基于未知漏洞后门通过 IPv6 的应用感知能力、网络编程能力、实时监测能力，加强策略部署保证伊犁师范大学数据中心重要业务的安全运行。

1) 在站群优优化方面

利用资源分发、Nginx 反代技术加固站群系统安全。对于双栈站群服务器，定期主动扫描安全漏洞，关闭不必要端口，通过防火墙、WAF 提高站群服务器安全等级，部署内容发布 CDN 平台，防止 DDOS 攻击；优化网站代码，防注入式攻击；使用静态 URL，实现认证校验并过滤 IP。针对 IPv6 网络特点一键部署 SSL 证书，实现网站资源一键上下线；针对双栈网站资源发布的面向对象，实现网站资源的访问权限控制。如：部分网站仅为内部用户访问，如内部知识交流资源系统；个别网站仅供特定用户访问，如财务系统等。

2) 在 DNS 解析体系方面

使用域名泛解析[5]，子域名和外部 URL 泛解析指向授权的 IPv4-IPv6 互通网关，通过互通网关智能分析 URL，解析真实 URL，提高 DNS 解析安全性。伊犁师范大学一级域名 www.ylnu.edu.cn，配置 A/AAAA 用*作为通配符，*代表任何的合法子域名，在 DNS 系统中，不用为每个子域名配置 DNS 的 A 和 AAAA 记录，允许任何域名解析为泛解析所指向地址，设置 *.ylnu.edu.cn 指向 219.247.32.34 和 2001:250:1813:1003::3 的，其余的子站也指向这两个地址，通过泛解析为域名解析提供一条缺省路由，针对泛解析中存在的入侵、报文拦截、篡改，进行安全加固。

具体为进行智能 DNS 的双栈权威解析和 A/AAAA 过滤，动态监测采用 Radius、Syslog 协议，实时侦听 NDP 报文 IPv6-MAC 信息、NS/NA 报文，分析和确定用户终端真实的 IPv6 地址，侦听 DAD 过程的 NS 报文，获取终端更新时的无状态地址和 MAC 地址，同时 DNS 的地址库加入四大运营商的 IPv6 地址，做到 IPv6 的分线路智能解析。

5. 效果与展望

本文通过突破传统安全思维，形成新思维模式，并建立安全体系。通过相关技术创新、思维理念创新，转变传统安全模式，建立四位一体安全防护体系，有效加固我校 IPv4/IPv6 双栈网络安全，降低了安全风险，实现无感知认证、核心数据加固，数据安全传输，提高了双栈系统的网络安全运维，为其它高校网络安全扩展思维模式。但是 IPv6 对于管理者和使用者来说都是新事物，缺乏使用经验，双栈网络各个环节的管控、风险处置还很薄弱，在推动 IPv6 发展的同时不断研究 IPv6 可编程技术，结合软件层面开发自适应的网络安全模型。伊犁师范大学数据中心下阶段的重点方向由双栈回归 IPv6 单栈，实现全生命周期管控，通过精细化的地址管理，实现地址溯源规模部署及平滑演进。

基金项目

伊犁师范大学校级科研项目(2021YSYB094)。

参考文献

[1] 崔北亮, 岳阳. IPv6 中邻居发现协议剖析及攻防探索[J]. 南京工业大学学报(自然科学版), 2021, 43(6): 746-754.

[2] 张军. 移动 IPv6 网络安全问题及解决对策[J]. 信息系统工程, 2022(9): 115-118.

[3] 黄宏志, 路懿, 刘娜. IPv4/IPv6 双栈 + DHCP 环境下的用户网络流量监测[J]. 现代计算机, 2021(11): 145-149+160.

[4] 高浪, 马峥. IPv6 环境下校园网安全防护技术研究与应用[J]. 网络安全技术与应用, 2022(7): 72-73.

[5] 何黎明, 曾靓, 蔡敏. 网站 IPv6 升级中域名泛解析的安全分析[J]. 江西通信科技, 2020(3): 38-41.