

人工智能大数据在专网通信安全防护中的运用

孙景国

内蒙古广播电视网络科技有限公司 内蒙古 呼和浩特 010010

摘要: 专网通信依托封闭化运行模式保障业务通信安全,但传统防护模式存在明显短板,静态防御机制难以适配动态多变的网络运行场景。本文结合专网通信的架构特征与防护逻辑,分析传统防护模式在数据处理、风险识别、场景适配等方面的运行局限,探究人工智能大数据技术在专网安全感知、异常研判、主动防御、态势监测中的具体应用路径,从数据体系搭建、防护架构升级、技术融合优化、运维机制完善等多个角度,提出智能化安全防护的系统性实施路径,可为专网通信安全防护体系升级提供技术参考。

关键词: 专网通信;安全防护;人工智能;大数据;智能风控

引言

专网通信凭借独立闭环的组网优势,广泛应用于各类专属业务场景,网络运行的安全性与稳定性直接关系专项业务的有序开展。网络业务场景持续拓展,终端接入形式愈发多元,各类隐性、新型网络安全风险不断增加。传统安全防护模式以静态被动防御为主,数据处理能力薄弱,风险识别存在明显滞后性,难以应对复杂动态的网络安全隐患。引入人工智能大数据技术重构安全防护体系,能够突破传统防护的运行瓶颈,提升专网风险感知、识别与处置能力,对强化专网通信安全管控质量具备重要现实意义。

1 专网通信安全防护整体架构与运行逻辑

1.1 专网通信网络架构与运行模式

专网通信网络采用封闭的拓扑结构,整体架构分为核心交换层、汇聚传输层、终端接入层三个部分。核心交换层部署专属交换设备,统筹全网的数据调度和指令分发工作,划定独立的数据传输区域,从源头隔绝外部网络的非法数据^[1]。汇聚传输层依靠专用光缆、专属无线频段完成数据中转,对全网传输链路做分段管理,固定数据的传输通路。终端接入层涵盖各类业务终端与管控设备,设置严格的入网权限标准。整套网络运行自成闭环,完全独立于公共互联网。所有设备的数据交互、指令传递都在专属链路内部完成,外部网络无法触碰专网内部运行节点。运维工作采用分级管控模式,设备和工作人员只能使用自身权限范围内的网络功能。

1.2 专网通信安全防护核心场景

专网通信安全防护工作,主要针对日常运行中高发的安全风险场景部署防护手段。终端接入环节严格核查设备入网资质,无论是新接入设备还是离线后重新连接的设备,都会完成全面的身份核验和安全检测,杜绝非

法设备接入网络。数据传输环节重点防范明文传输、数据篡改、链路窃听等常见风险,对各类业务数据统一做加密处理,持续监测数据传输的实时状态。边界交互环节针对专网和外部系统的少量数据交互,部署专用边界防护设备,逐一筛查所有跨网传输数据。业务运行环节持续监测业务系统运行状态,及时发现异常访问、频繁操作、违规调用等问题,有效防范业务数据被篡改、核心信息泄漏等安全问题。

1.3 专网通信安全防护运行逻辑

专网通信安全防护依托前置防御、实时管控、事后溯源的完整思路运转。系统会提前录入合法设备、合规传输链路、授权访问主体的白名单数据,搭建基础的安全防护壁垒。网络正常运行期间,防护模块持续采集全网运行数据,对照预设的白名单规则和安全标准,主动甄别各类异常行为。一旦监测到风险隐患,系统会自动启动拦截机制,阻断风险传输链路、限制违规操作行为,阻止安全问题持续扩散。网络运行中的访问行为、数据传输过程、设备操作记录都会完整留存。工作人员可以依托留存日志排查风险来源,锁定问题节点,为整改安全隐患、优化访问权限提供可靠的依据。

2 专网通信传统安全防护模式现存短板

2.1 传统防护模式的运行机制

传统专网安全防护以静态规则为核心开展防护工作。技术部署以硬件防火墙、准入控制系统、加密网关等固定设备为主。整套防护体系依靠预设的静态策略、固定权限清单和固有防护规则完成网络防护。设备只会按照既定参数筛查网络数据,执行准入判定和风险拦截操作。防护规则长期保持固定状态,仅依靠人工定期更新策略条目。整体防护逻辑偏向被动防御,只对数据库内登记的已知风险做出响应,无法主动挖掘网络环境中

潜藏的新型安全威胁。

2.2 网络数据海量处理能力的局限性

专网业务场景持续拓展,终端设备接入数量稳步增长。网络日常运行产生的流量数据、业务日志、交互信息体量持续攀升^[2]。传统防护设备的数据算力和存储容量存在固定上限。设备仅能完成小体量、结构化数据的筛查与分析。面对高频次、大流量的碎片化数据和瞬时爆发的网络流量,设备会出现数据筛查不全面、分析精度下降的问题。大量边缘数据、短时流量数据无法得到有效解析,部分潜在风险数据会直接穿过防护设备,留存网络安全隐患。

2.3 异常网络行为识别的滞后性问题

传统防护手段依托特征库比对方式识别网络风险。识别工作需要完成数据采集、特征比对、风险判定的完整流程,耗费一定网络运行时长。新型网络攻击、变异违规操作没有对应特征数据,系统无法第一时间完成风险判定。隐蔽性较强的渐进式违规行为,会以正常流量形式长期驻留网络内部。系统只会在风险造成明显异常数据波动后,完成识别和处置。前期潜伏的违规操作会持续侵蚀网络安全边界,破坏专网运行稳定性。

2.4 动态网络环境适配能力不足

当下专网业务模式、接入场景处于持续变动状态。移动终端接入、跨区域业务交互、临时业务开通等场景愈发普遍,网络拓扑结构会随业务调整随时改变。传统防护策略固化性较强,无法跟随网络场景变化调整防护标准。新的业务链路、临时接入节点缺少匹配的防护规则覆盖。原有管控策略无法适配灵活多变的专网运行场景,漏洞排查、权限管控、流量监测都会出现管控盲区,大幅降低整体防护成效。

3 人工智能大数据在专网通信安全防护中的应用维度

3.1 基于大数据的专网通信数据全方位感知与采集

大数据技术打破了传统专网数据采集范围狭窄的局限,拓展了全网数据采集的覆盖范围。采集对象不再局限于核心流量与业务日志,可全面覆盖专网链路流量、终端操作记录、设备运行参数、边界交互数据、业务操作轨迹等各类网络信息。技术架构支持分布式采集模式,能够对接专网各层级、各节点设备,捕捉常规筛查中容易遗漏的碎片化数据、短时波动数据和边缘节点数据。采集过程采用轻量化抓取方式,不会对专网正常业务运行造成干扰^[3]。采集后的原始数据会经过分类清洗、去重过滤、格式统一处理,剔除无效冗余信息。规整后的高质量数据,可为后续深度分析与风险研判提供完整、真实的基础数据源,补齐传统数据采集覆盖面不足

的短板。

3.2 依托人工智能的网络异常行为深度分析

人工智能技术改变了传统特征比对的单一分析模式,实现专网网络行为的深度挖掘与精准研判。机器学习模型可依托海量历史专网运行数据开展自主训练,梳理总结合法网络行为的运行规律,建立常态化行为基线。模型能够精准分辨常规操作与细微违规行为的差异,针对无特征的新型攻击、变异违规操作、渐进式入侵行为展开深度拆解。可以精准识别越权访问、异常流量跳转、隐蔽数据传输、终端违规操作等各类风险行为。智能分析体系摒弃了固定判定标准,可结合不同业务场景、不同接入终端的运行特点灵活调整分析逻辑。精细化的分析模式,能够捕捉传统防护手段无法识别的隐性风险,提升专网异常行为识别的精准度。

3.3 智能算法驱动的专网通信风险主动防御

智能算法为专网安全防护搭建主动防御体系,扭转了传统被动应对风险的防护局面。深度学习、聚类分析等智能算法可实时解析专网运行数据,对比常态化运行基线捕捉数据偏差。系统能够提前预判网络链路异常、终端风险接入、数据违规传输等潜在隐患,在风险形成危害前完成预警处置。针对不同等级、不同类型的安全风险,算法可自动匹配对应的处置策略,完成风险链路阻断、违规权限冻结、异常终端隔离等操作。算法具备持续迭代能力,会根据专网新增业务、新型风险类型不断优化判定规则和处置逻辑。动态更新的防御体系,可适配专网多变的运行场景,持续压缩网络安全风险的生存空间。

3.4 大数据赋能的专网安全态势动态感知

大数据技术可整合专网全网安全数据,实现安全态势的实时感知与动态研判。技术能够汇总全网各区域、各节点、各业务模块的安全状态信息,完成整体安全数据的统一整合分析。通过对风险数量、漏洞分布、攻击类型、违规频次等数据的量化统计,直观呈现专网当下的安全运行状态。数据动态更新机制可实时同步网络场景、业务运行、风险状态的变化情况,精准定位网络防护薄弱区域。运维人员可依托量化数据掌握专网安全整体状态,清晰把控防护工作的重点方向,有针对性开展漏洞修复、权限优化、风险防控工作,实现专网安全防护的精细化、动态化管控。

4 人工智能大数据赋能专网通信安全的实施路径与优化方向

4.1 构建专网通信安全智能数据处理体系

智能数据处理体系是落地专网智能安全防护的核心

基础,需要针对专网数据特性搭建专属化处理流程。依托分布式数据采集架构,覆盖专网核心链路、汇聚节点、终端接入端、业务系统等全维度数据来源,收录流量报文、设备运行日志、业务操作记录、边界交互数据等多类型信息。搭建标准化数据处理流程,通过智能筛选、自动去重、格式归一化、噪声剔除等工序,清理无效、错乱的原始数据^[4]。结合专网业务属性搭建专属数据标签体系,对正常流量、合规操作、风险行为、异常链路等数据进行分类标注。依托大数据存储技术搭建分级存储资源池,区分高频分析数据、历史归档数据的存储模式,适配不同场景的数据分析需求。持续迭代数据处理规则,匹配专网业务更新节奏,为智能安全分析和风险研判提供可靠的数据底座。

4.2 搭建智能化分层安全防护架构

结合专网闭环运行的网络特征,搭建分层、分级的智能安全防护架构,替代传统单一的硬件防护模式。在终端接入层部署智能检测模块,依托训练成熟的AI模型筛查入网设备状态,自动识别终端固件漏洞、非法改装、风险程序等问题。在传输汇聚层配置智能流量管控单元,对全网传输数据进行逐段监测,自主识别数据篡改、隐秘传输、链路异常等风险行为。在核心交换层搭建智能风控中心,统筹全网安全数据的分析研判,统一下发风险处置指令。在业务应用层对接智能防护接口,监测业务系统的访问操作、数据调用、权限使用等行为。各层级防护模块独立承载对应防护工作,依托数据链路完成信息互通,全方位填补传统分层防护存在的管控空白。

4.3 优化智能防护技术与专网系统的融合模式

传统智能技术落地存在适配度低、兼容性弱的问题,需要针对性优化技术与专网系统的融合方式。摒弃通用化智能防护部署方案,依据专网专属拓扑结构、业务运行规则、设备参数特性,定制轻量化智能防护算法模型。删减冗余运算模块,降低智能分析技术对专网算力资源的占用,避免影响常规业务运转。打通智能防护系统与专网原有硬件设备、业务系统的数据接口,破除数据交互壁垒,实现网络运行数据的顺畅流转与调用。针对专网高频业务场景调试算法参数,优化风险识别、

预警、处置的响应流程。结合新型网络攻击手段与专网违规行为,定期完成算法模型的迭代训练,有效提升智能防护技术在专网场景的落地实效。

4.4 完善专网通信智能安全防护运维体系

科学完善的运维体系,是智能防护技术长效稳定运行的关键支撑。建立智能化设备运维机制,定期核查防护模块、数据采集设备、算法运行平台的工作状态,自动排查设备故障、数据断连、算法卡顿等问题。搭建分级运维管理机制,划分设备运维、数据运维、算法运维、安全风控等不同工作板块,明确各板块工作内容与执行标准。建立安全风险复盘机制,针对专网出现的安全隐患、预警信息、处置记录,定期开展数据分析,梳理防护短板。结合运维数据优化防护策略,调整算法判定阈值、数据采集范围、风险处置标准^[5]。同步完善运维人员技能体系,匹配智能防护技术的迭代节奏,夯实专网智能安全防护的运维保障能力。

结束语

专网通信传统安全防护体系的静态化、被动化特征,逐渐无法适配日趋复杂的网络运行环境与业务需求。人工智能大数据技术能够深度融入专网安全防护全流程,拓宽网络数据感知范围,提升异常行为识别精度,构建主动化、动态化的安全防御模式。通过搭建智能数据处理体系、分层防护架构、优化技术融合方式、完善配套运维机制,可全方位补齐传统防护短板,持续提升专网通信安全防护的精细化与智能化水平,稳固专网业务安全稳定的运行根基。

参考文献

- [1]王允昕.基于人工智能的网络通信信息数据安全加密技术[J].互联网周刊,2025(14):35-37.
- [2]朱杰.基于人工智能的网络通信信息数据安全加密技术研究[J].信息记录材料,2025,26(2):144-146.
- [3]杨嘉.基于人工智能的网络通信信息数据安全加密技术研究[J].信息记录材料,2025,26(3):120-122.
- [4]徐焕.基于人工智能的网络通信信息数据安全加密技术研究[J].中国高新科技,2025(12):109-111.
- [5]杨阳,费晓琛.面向物联网通信的人工智能安全机制与防护技术研究[J].微型计算机,2025(19):184-186.