智能电网信息内外网边界安全监测模型的设计

夏颖　范金强　李西治　陈宏佑　邱继付　顾志奇
国网思极网安科技(北京)有限公司
DOI:10.12238/acair.v2i4.10287

[摘　要] 在智能电网快速发展的时代背景下,信息内外网边界的安全监测工作尤为重要。本文基于此,设计一款信息内外网间安全设备,实现对交互对象的安全过滤和访问,并在此基础上对信息内外网边界安全的防御方法展开系统性研究,构建信息内外网边界交互信息安全监测模型。该模型的应用,能够实现边界交互数据信息实时监控、网络行为和数据流的实时采集以及数据库访问行为的追溯与控制等目标,从而为评估和预测信息内外网边界安全状态提供依据,提升信息内外网边界状态的整体检测水平。
[关键词] 内外网边界；智能电网；信息安全；监测模型
中图分类号：V242.3+1　文献标识码：A

Design of a Security Monitoring Model for the Inner and Outer Network Boundaries of Smart Grid Information

Ying Xia　Jinqiang Fan　Xizhi Li　Hongyou Chen　Jifu Qiu　Zhiqi Gu
State Grid Siji Network Security Technology (Beijing) Co., Ltd.

[Abstract] In the context of the rapid development of the smart grid, the security monitoring of the information internal and external network boundaries is particularly important. Based on this, this article designs a security device for information between internal and external networks, which realizes secure filtering and access to interactive objects. On this basis, a systematic study is conducted on the defense methods of information internal and external network boundary security, and an information security monitoring model for information internal and external network boundary content interaction is constructed. The application of this model can achieve real-time monitoring of boundary interaction data information, real-time collection of network behavior and data flow, and traceability and control of database access behavior, providing a basis for evaluating and predicting the security status of information internal and external network boundaries, and improving the overall detection level of information internal and external network boundary status.
[Key words] internal and external network boundaries; Smart grid; Information security; Monitoring Model

智能电网在运行服务期间,高度集成通信、信息和控制技术,从而实现电力系统自动化、互动化和智能化。但是,随着智能电网开放性和互联性持续增加,关于信息安全方面的问题日渐凸显[1]。作为智能电网与外部网络交互的接口,信息内外网边界安全性与智能电网稳定运行之间存在最为直接的联系。近年来,黑客入侵、恶意代码传播等网络攻击事件频频发生,严重威胁智能电网信息安全。设计可靠、高效的信息内外网边界安全监测模型,对保障智能电网信息安全具有重要意义。

1 设计目标

信息内外网边界安全监测模型的设计,其最为关键的目标是构建安全且高效的防护体系。在模型构建期间,要充分保障信息内外网所覆盖的所有设备始终保持高效、稳定运行状态,严格过滤交互对象信息,保证信息安全。只有经过安全验证的信息,方能通过访问限制,有效阻挡潜在的安全威胁。在设计信息内外网边界安全监测模型时,要对边界安全防御展开深入研究,保证模型兼具实时交互和数据监控能力,快速捕捉并分析网络行为的数据流。详细追溯和控制数据库访问行为,保证所有的数据访问都能够有据可查,规避非法访问和数据泄露等问题出现[2]。

2 模型架构

2.1数据采集模块。作为安全监测模型的基础,数据采集模块在设计与开发时,要求其准确且实时的收集边界交互的数据、网络行为以及数据流,为后续全面及时分析数据提供支持。使用Wireshark网络嗅探器抓取网络流量,获取HTTP请求、FTP传输和SMTP邮件等经过网络接口的数据包。利用PRTG作为流量分析工具,动态监测网络流量,准确识别出带宽使用混合异常连接行为,及时发现网络拥塞和攻击行为。ELKStack作为日志收集系统,

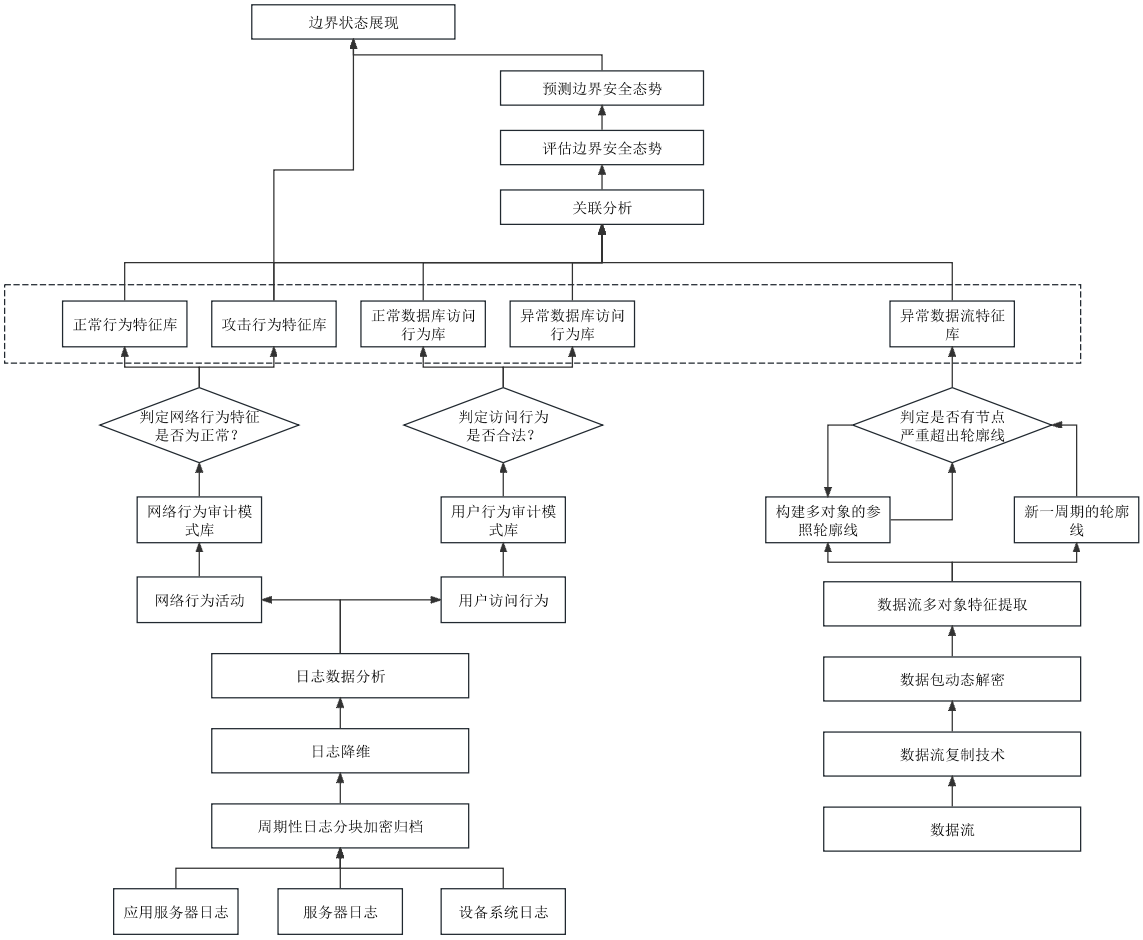

图 1 信息内外网边界交互信息安全监测系统

用于集中收集与分析防火墙、路由器、交换机等网络设备日志信息,详细记录与发现设备运行状态和网络活动详情。对于某些应用或服务,数据采集模块还通过API接口直接获取交互数据,如云服务提供商的安全日志和Web应用的访问日志,丰富数据源。综合数据清洗、格式化和去重等预处理步骤,对采集到的原始数据进行处理,消除噪声和冗余信息,提高数据质量[3]。

2.2数据分析模块。在安全监测模型中,数据分析模块负责深入剖析采集的数据,识别潜在的安全威胁。数据分析模块为实现此功能,必须具备强大的数据处理能力和智能分析算法,精准区分异常行为和正常行为。模块集成支持向量机(SVM)、随机森林(RandomForest)及神经网络等多种技术,从而训练模型并快速识别恶意行为。机器学习算法可从海量数据中学习并提取特征,准确预测未知威胁。综合已知的恶意IP地址、域名、哈希值等信息构建威胁情报库,快速匹配并识别已知威胁,并定期更新以保持有效性。作为数据分析模块的另一关键手段,行为分析通过监控用户或者系统的行为,识别异常登录时间、频繁访问敏感数据等异常行为。对于未知文件或代码,此模块利用沙箱技术进行隔离,观察在沙箱中的行为,判断是否存在恶意。另外,数据分析模块还配备PowerBI可视化工具,图形化、直观化处理复杂的分析结果,帮助安全人员快速理解存在的威胁态势,并及时做出响应调整[4]。

2.3安全过滤模块与访问控制模块。安全过滤模块与访问控制模块协同作业,共同构建坚固防线,旨在确保合法数据和信息能穿越内外网边界,有效阻止未授权访问及数据泄露。两模块紧密合作,实现对网络流量的精细管控,为网络安全提供坚实保障。防火墙作为首道防线,依据预设安全策略对进出网络的数据包进行过滤。现代防火墙除基本过滤功能外,还支持状态检测、深度包检查等高级功能,提供全面且高级的安全保护。入侵检测和防御系统(IDS/IPS)的加入,进一步增强了网络安全防护。IDS监控网络活动,识别并报告潜在攻击;IPS则在IDS基础上,增加自动响应功能,如阻断连接、重置会话,实时检测与防御网络攻击。Web过滤、邮件过滤等内容过滤技术,利用黑名单、白名单或正则表达式等方法,拦截恶意内容,防止其进入网络,保护网络环境的清洁与安全。应用身份认证和授权系统,则确保仅合法用户能访问敏感资源。系统如RADIUS、LDAP、Kerberos等,通过验证用户身份并授予访问权限,有效防止未授权访问。SSL/TLS、IPSec等数据加密技术,确保数据在传输中不被窃听或篡改,保护数据的完整性和机密性。

2.4实时监控模块。设计开发实时监控模块的思路旨在全面保障边界安全状态,利用高效技术集成与自动化流程,实现安全事件的即时发现与快速处理。此模块的核心是构建一套快速响应且高度自动化的系统,以减少人工干预并大幅缩短响应时间。在技术选

型与设备部署上,引入IBMQRadar安全事件管理系统(SIEM),集中管理和深入分析来自各安全组件的警报与事件。通过自动关联与智能分析,SIEM系统提供统一视图和报警机制,有助于全面掌握安全态势。为提升自动化水平,整合Ansible自动化响应系统,结合自定义脚本或第三方服务,实现安全事件的自动化响应。系统检测到安全事件时,立即触发预设响应操作,如隔离受感染主机、阻断恶意连接等,有效遏制安全威胁扩散。设计可视化监控界面,基于Web技术展示实时网络拓扑图、安全事件分布图等,便于安全人员远程访问和协作,快速掌握网络运行状况。集成Grafana监控工具实时监控网络性能、系统资源等关键指标,帮助安全人员及时发现潜在性能问题或安全风险,为预防安全事件提供支持。

3 关键技术

3.1加密/解密技术：数据安全的基石。加密/解密技术是保护数据在传输中不被窃取或篡改的关键。采用AES、RSA等先进加密算法对敏感数据加密,即便数据被截获,攻击者也难以破解,从而保障数据的机密性和完整性。解密过程只允许授权用户访问原始数据,进一步增强数据安全。设计内外网边界安全监测模型时,所有重要数据传输都应加密,无论内网向外网发送还是外部访问内网资源,均需遵循此原则。

3.2身份认证/数字签名技术：确保访问合法性。身份认证和数字签名技术是验证用户或设备身份,防止未授权访问的机制。实施多因素认证,如密码、生物特征、硬件令牌等,可大幅提高访问控制的安全性。数字签名则验证数据完整性和来源真实性,确保接收数据未被篡改且来自声称的发送者。在内外网边界安全监测模型中,这些技术应广泛应用于用户登录、数据交换、服务访问等,确保只有合法用户和设备能跨越边界进行安全交互。

3.3入侵检测和防御技术：主动防御的利剑。入侵检测和防御技术是保护内外网边界免受外部攻击的关键。入侵检测系统(IDS)实时监控网络流量,识别并报告潜在攻击行为,如恶意软件入侵、DDoS攻击等。入侵防御系统(IPS)更进一步,不仅能检测攻击,还能自动采取防御措施,如阻断攻击流量、隔离受感染主机等,有效阻止攻击。设计安全监测模型时,应将这些技术融入边界防护体系,形成多层次、立体化的防御架构,确保边界安全稳定。

3.4防火墙技术：数据流过滤的守门员。防火墙技术是内外网边界安全的第一道屏障。设置防火墙可对进出边界的数据流进行精细化过滤和控制,根据安全策略允许或拒绝特定数据包通过。现代防火墙具备包过滤、状态检测、应用层过滤等高级特性,能有效抵御多种网络攻击。设计安全监测模型时,应合理配置防火墙规则,既不妨碍正常业务通信,又能有效阻挡恶意流量,保护内网资源安全。

3.5安全隔离技术：网络间的安全屏障。安全隔离技术,尤其是安全隔离装置(如网闸),是实现内外网物理隔离的重要手段。这类装置在电路上切断网络间的链路层连接,确保内外网间不存在直接数据通道,从根本上隔绝安全风险。同时,安全隔离装置支持基于内容的安全检查和数据交换,确保隔离不影响必要业务数据传输。设计内外网边界安全监测模型时,应充分考虑安全隔离技术的应用,将其作为整体安全策略的重要组成部分,为内外网间安全交互提供坚实保障。

4 实际应用

在实际应用中,信息内外网边界安全监测模型可以应用于智能电网的各个环节,如发电、输电、变电、配电、用电和调度等。通过对各个环节的信息安全进行监测和防护,可以有效提升智能电网的整体安全水平。

表1 实际应用效果对比表

环节	应用前安全事件数量(次/年)	应用后安全事件数量(次/年)	安全提升比例(%)
发电	17	3	82.4
输电	21	4	81
变电	13	2	84.6
配电	29	6	79.3
用电	31	8	74.2
调度	18	5	72.2
总计	129	28	78.3

5 结语

本文设计了一款针对智能电网信息内外网边界的安全监测模型,该模型构建数据采集、数据分析、安全过滤与访问控制及实时监控四大模块,实现对边界交互数据的全面监测与高效防护。模型采用先进的加密/解密、身份认证/数字签名、入侵检测和防御、防火墙及安全隔离等技术,保障数据的机密性、完整性和合法性,有效抵御外部攻击和未授权访问。实际应用中,该模型在智能电网各环节均取得显著安全提升效果,整体安全事件数量大幅下降,安全提升比例高达78.3%。这一成果证明该模型在保障智能电网信息安全方面的有效性和实用性。未来,将继续优化和完善该模型,以适应智能电网不断发展变化的安全需求,为智能电网的稳定运行和可靠供电提供坚实安全保障。

[参考文献]

[1]鞠睿.基于内外网协同的售电公司差额电费智能结算管理应用[J].市场瞭望,2023,(23):82-84.

[2]何立民.泛在电力物联网中的智能电表[J].单片机与嵌入式系统应用,2022,22(08):4-6.

[3]周泽元,严彬元,刘俊荣.基于未知威胁感知的电网内外网边界信息安全监测[J].电力大数据,2022,25(04):18-25.

[4]何立民.从智能电网、物联网到泛在电力物联网[J].单片机与嵌入式系统应用,2022,22(04):3-5+10.

作者简介：

夏颖(1978--),女,汉族,安徽铜陵人,硕士,高级工程师,国网思极网安科技(北京)有限公司,研究方向：电力行业信息系统安全防护,信息化项目安全管理,安全生产技术标准。