# 基于行为分析的港口网络边界入侵防御策略

岳 皓 牛文奇 刘卓岑
山东港口科技集团青岛有限公司 山东 青岛 266000

**摘 要：**港口作为贸易与物流的核心枢纽，在数字化进程中，其网络边界的安全防护直接关系到运营稳定与数据安全。当前，港口网络边界面临外部攻击、内部操作风险、设备软件漏洞及数据传输隐患等多重挑战，传统依赖特征库的入侵防御方式，对新型攻击的识别能力有限，已难以满足防护需求。本文探讨基于行为分析的港口网络边界入侵防御策略，解析行为分析技术的基本原理与应用优势，说明其在用户操作、设备运行及应用程序行为监测中的具体实践。通过构建网络行为基线、识别异常行为、采取针对性防御措施，经实验验证，该策略在提升入侵检测精准度、降低误报漏报率及加快响应速度等方面成效显著，可为港口网络边界安全提供可靠支撑。

**关键词：**港口网络；行为分析；入侵防御；网络安全

## 引言

港口是重要的贸易和物流枢纽，在现代数字化时代发展下容易遭受网络攻击，这就会造成港口生产中断、数据泄露、设备故障等产生巨大经济损失，也会给国家经济安全以及社会稳定发展造成不利影响。在现代网络技术高速发展的背景下，港口网络边界面临入侵手段日益多样化和复杂性的风险。以往基于特征库的入侵检测和防御方法，因为对未知攻击检测能力有限，所以，无法适应当前极为严峻的网络安全形势。基于行为分析的港口网络边界入侵防御策略能够精准监测、分析以及识别网络风险，及时发现异常行为和潜在威胁以保证港口网络边界安全性达到要求。

## 1 港口网络边界安全现状

### 1.1 港口网络边界的构成

港口网络边界作为港口内部网络，它需要和合作伙伴网络、互联网等外部网络连接，也是重要的节点与分界线，这时系统内包含路由器、防火墙、交换机、入侵检测等网络设备，还涉及到服务器终端设备等。通过对这些设备展开分析，它们和系统共同组成港口网络的第一道安全防线，这就能够确保进出港口网络的数据流量实现全面监管与防控。

### 1.2 面临的安全威胁

（1）外部攻击。港口网络边界的威胁中，这时的外部攻击是面临的首要威胁，如果黑客攻击网络漏洞、恶意软件等，就会直接进入到港口网络内部获取敏感信息，进而直接破坏网络安全或者进行勒索，从而就会出现港口网络运行存在风险以及经济损失[1]。

（2）内部威胁。如果港口网络运行的环节发生了误操作或恶意行为，这就会导致网络的安全性无法达到要求。

（3）设备和软件漏洞。港口网络系统内安装有大量的的软件系统、网络设备等，如果这些设备设计与安装中存在设计缺陷，或者未能及时更新而导致网络安全的漏洞，进而导致港口网络系统的安全性无法保证。

（4）数据传输安全。港口网络在运行过程中，需要和监管部门、外部合作伙伴等时刻保持数据传输与应用，这样就会导致数据传输时存在数据窃取、篡改、拦截等风险。

## 2 行为分析技术在港口网络边界入侵防御中的应用

### 2.1 行为分析技术的原理

行为分析技术作为先进网络安全技术，它需要利用对网络用户、设备以及应用程序，能够完成数据信息的采集、分析以及建模，进而构成正常行为基线，然后再利用对比实际行为和正常行为基线的差异，就能够精准实现异常行为和潜在威胁。该技术的核心在于认为正常网络行为具备一定的规律性和稳定性，这时利用分析确定的异常行为则和正常行为对比，就能快速判定网络外部攻击行为。

行为分析技术能够从用户登录行为、数据访问行为、网络连接行为、应用程序行为等获取信息，这时通过多个维度掌握数据信息，进而能够实现风险的精准识别。通过对网络行为的长期监测和分析，能够建设准确的正常行为模型，一旦存在异常行为立即采取处理措施。

### 2.2 行为分析技术的优势

（1）检测未知攻击。基于特征库的入侵检测方法只

**作者简介：**岳皓，1996年8月23日，山东港口科技集团青岛有限公司，山东省青岛市，本科，266000，男，汉，山西省长治市，中级工程师，大学本科，网络及网络安全。

是通过预设特征码识别已知攻击行为，所以该系统运行时对于新型未知的攻击行为不能精准识别和分析。行为分析技术利用建设网络正常行为模型，它能够连续监测并分析各种操作行为的偏离度，如果系统监测发现存在超出极限的异常模式，就能够有效的判定为潜在攻击。经过上述模式能够快速识别异常的行为，它可以利用系统精准识别变种恶意代码、零日攻击等方面提高未知威胁识别能力，从而可以实现港口网络攻击的快速识别。

（2）提高检测准确性。行为分析技术能够精准识别港口网络系统运行环节的正常行为规律，它能够建设形成完善且准确的行为基线。根据行为分析技术检测要求可以对比基线与异常行为之间的差异或者不同之处，这样能够快速掌握异常攻击行为，也能够通过细微的差异快速判定异常攻击行为以便及时进行防护处理。对于各个网络端口运行环节的异常行为达到精准化防控以及应对的目的。该机制可以快速掌握系统运行的状态，它能够提高系统识别的精确性和稳定性，最终能够保证港口网络边界达到安全运行的标准[2]。

（3）实时监测和响应。行为分析技术通过分布式传感以及实时计算架构，它们就能够精准进行网络流量、设备操作、用户行为的分析，这时系统运行环节的分析速度能够达到毫秒级。如果系统监测存在异常行为则立即进行特征提取、风险评级，这时就能自动触发告警机制再联动防火墙、入侵防御设备等实现网络攻击的阻断与隔离。这种监测装置从响应到闭环流程能够大幅缩短网络攻击识别与处置时间差，从而能够防止传统策略中因为人工介入延迟导致损失增大。

2.3 在港口网络边界中的具体应用

（1）用户行为分析。通过对港口网络用户登录时间、登录地点、登录行为、操作行为方面的全面监控，此时就能根据系统防控要求构建完善的用户行为模型。如果系统监测用户的异常登录、频繁访问敏感数据等异常行为则立即发出告警，并提醒安全人员尽快进行核实。

（2）设备行为分析。行为分析技术能够充分分析港口网络中网络设备、服务器、终端设备等，这时就能快速的掌握运行状态、网络连接、数据传输等进而精准识别异常行为。例如，港口网络设备运行环节必然存在大量的网络请求、数据传输体量异常增大等，这时可以在系统判定为攻击的表现以提前进行安全防御。

（3）应用程序行为分析。通过对港口网络运行的应用程序进行启动、关闭、数据交互等行为的监测与分析，这时就能建设更具精准性的应用程序正常行为模型而发出告警。

## 3 基于行为分析的港口网络边界入侵防御策略

3.1 建立网络行为基线

港口网络边界系统内部设置入侵检测系统、网络流量分析仪等设备，此时就能实时掌握网络用户、设备和应用程序的用户登录日志、网络连接日志、数据访问日志、应用程序运行日志等行为。然后通过系统进行原始数据的清洗、过滤以及转换，从而将数据内噪声数据、冗余数据去除使其转换成为适宜分析的格式。例如，通过对港口网络系统日志数据进行标准化处理，能够及时获取时间、源IP地址、目标IP地址、操作类型等关键信息以掌握是否存在攻击行为。

3.2 异常行为检测与识别

行为分析技术应用后能够时刻监测港口网络运行行为的各项数据信息，并且将监测后的数据信息和正常行为基线进行对比，从而能够精准识别港口网络系统的用户行为、设备行为、应用程序的异常行为情况。然后利用统计分析算法、机器学习算法、深度学习算法进行多种异常行为的精准识别，这样就能实现网络行为的精准分析与识别。统计分析算法能够计算系统内获取的数值均值、方差、标准差等统计量，从而判定网络行为是否存在异常情况；机器学习算法通过不断训练网络监测数据信息构建形成等行为模型，再利用行为数据的分类和预测以实现行异常行为的精准识别；深度学习算法能够处理复杂的非线性关系，从而使得异常识别达到准确性、科学性要求[3]。

行为分析技术能够时刻监测港口网络边界的异常行为，并根据异常行为的严重程度发出异常行为的发生时间、源IP地址、目标IP地址、行为类型等不同级别的告警以便安全人员及时了解情况，并采取相应的安全应对措施。这种情况下能够使得安全行为精准识别，也能够确保港口网络边界入侵防御效果达到要求。

3.3 入侵防御措施

港口网络边界入侵防御措施在应用时，这就能够精准识别用户的身份和权限，能够通过对用户访问港口网络资源的行为实现整个系统的严格控制以提高系统安全性。该系统中设置必要的访问控制策略，就能够通过限制未授权用户访问、防止敏感信息泄露以及网络攻击等方式保证港口网络边界运行达到安全性要求。例如，通过基于角色访问控制模型给不同角色用户分配不同权限，利用分析不同权限的特性就能够使得用户只能在自己权限内访问工作所需的资源。同时，港口网络中传输、存储敏感信息时，系统内部的安全防护时利用对称加密、非对称加密等先进加密技术实现数据信息的加密

管控[4]。

港口网络边界在面临入侵时需要采取必要防御措施，这时主要利用发现和修复港口网络的设备与软件漏洞的方式避免受到攻击者入侵。同时，建设完善的漏洞防控机制进行网络设备和软件的漏洞扫描与评估能够及时安装补丁程序达到漏洞快速修复的目的。此外，通过制定完善的应急组织架构、应急处置流程、应急救援措施等应急预案，一旦发现港口网络被外部攻击则立即启动应急预案以保障资金和信息的安全性[5]。

## 4 实验验证与分析

### 4.1 实验环境搭建

为了检验基于行为分析的港口网络边界入侵防御策略是否达到应用要求，需要建设模拟的港口网络环境验证其防御效果。在实验环境中配置8台服务器、40台终端设备、15台网络设备、入侵检测系统、网络流量分析仪等。通过模拟港口网络和外部网络连接，其网络带宽为1000Mbps，划分为6个子网，分别模拟港口不同功能区域。在本次实验中连续48h运行，环境温度24℃~26℃，湿度控制48%~52%，并且模拟不同攻击场景以测验防御策略的效能。

### 4.2 实验方案设计

在本次试验攻击场景模拟设置SQL注入攻击、缓冲区溢出攻击、端口扫描攻击、恶意代码攻击等多种网络攻击场景。每种攻击执行8次，SQL注入攻击每秒发起6~9次请求，缓冲区溢出攻击单次数据包大小1200~1800字节，端口扫描攻击速率80~120端口/s，恶意代码攻击传播频率为2~4台设备/min。

本次实验过程中每6min需要进行一次网络行为数据的监控，利用行为分析确定入侵防御策略并进行数据分析，从而记录入侵检测率、误报率、漏报率、响应时间等各项指标。而后根据行为分析的入侵防护策略与传统基于特征库的入侵防御策略进行对比试验，传统策略特征库每日更新一次，两种策略运行在相同配置设备中对比不同攻击场景下性能表现。

### 4.3 实验结果分析

（1）入侵检测率。行为分析以基础建设的入侵防御策略在SQL注入攻击策略检测效率为97.8%，缓冲区溢出攻击为96.5%、端口扫描攻击为98.9%、恶意代码攻击95.7%；传统对应攻击检测率为81.2%、78.5%、87.6%、74.2%。行为分析策略检测未知攻击行为比例为91.3%，传统策略只有60.8%。

（2）误报率和漏报率。通过行为分析建设的攻击防御策略误报率为1.3%，漏报率平均为0.9%；传统策略误报率4.6%，漏报率5.8%。通过上述结果就说明行为分析的港口网络边界入侵防御策略能够有效识别异常性潜在威胁，并且降低误报率、漏报率。

（3）实时性。通过行为分析建设的港口网络边界入侵防御策略的平均响应时间为0.4s，传统策略1.3s，能够在攻击发生后立即发出告警并采取防御措施具备较高的实时性。

从上述实验结果进行分析，基于行为分析的港口网络边界入侵防御系统能够提高检测准确率、降低误报率以及漏报率，并且具备较高的实时性，能够保证港口网络边界运行达到安全性要求，进而有效抵抗网络攻击的影响。

## 5 结语

基于行为分析的港口网络边界入侵防御策略能够保证港口网络运行的安全性，这比传统的入侵防御策略具备较高的优势。同时，本文以实际案例提出建立网络行为基线、异常行为检测与识别、入侵防御措施及动态调整与优化的多样化防御策略，能够提高港口网络边界入侵防御水平。

而在本文中进行实验分析后得出基于行为分析的港口网络边界入侵防御策略能够有效抵抗各种网络攻击，提高响应速度、降低误报率、漏报率，并且能够提高实时性以满足港口网络安全运行需求。

## 参考文献

[1]余娟.互联网背景下的港口网络信息安全对策研究[J].舰船科学技术,2019,41(14):169-171.

[2]张华,岳皓.基于SDN的港口安全资源池建设[J].网络空间安全,2020,11(03):39-43.

[3]沈朗捷.基于人工智能的港口网络安全威胁检测与防御技术[J].中国信息界,2024,(09):30-32.

[4]王娟娟,崔枭飞,崔赫,等.全力筑牢港口网络安全防线近期海外港口网络安全事件对我国的启示[J].中国电信业,2023,(10):61-63.

[5]杨惠云,邱云鹏,刘广会,等.智慧港口网络安全保障体系框架[J].港口科技,2022,(12):22-26