铁路计算机应用
RAILWAY COMPUTER APPLICATION

铁路设计企业安全态势感知技术研究与实践

刘　峰，韩　寓

Security situation awareness technology of railway design corporations

LIU Feng and HAN Yu

引用本文:
刘峰, 韩寓. 铁路设计企业安全态势感知技术研究与实践[J]. 铁路计算机应用, 2021, 30(11): 68-72.
LIU Feng, HAN Yu. Security situation awareness technology of railway design corporations[J]. Railway Computer Application, 2021, 30(11): 68-72.

在线阅读 View online: http://tljsjyy.xml-journal.net/2021/I11/68

文章编号：1005-8451（2021）11-0068-05

铁路设计企业安全态势感知技术研究与实践

刘　峰，韩　寓
（中国铁路设计集团有限公司　信息化院，天津　300308）

摘　要：分析了铁路设计企业网络安全防护现状，对比并制定了安全态势感知技术方案，重点阐述铁路设计企业态势感知技术实践中遇到的问题和对既有网络及安全防控体系的适应性调整。实现企业网络流量安全态势监测及安全自动化，使安全态势感知技术在网络安全综合防控体系中发挥出核心价值，可以切实提升企业整体安全水平。

关键词：态势感知；全网流量分析；安全自动化；安全管理平台；铁路设计企业
中图分类号：U29 : TP393　**文献标识码：**A　**DOI：**10.3969/j.issn.1005-8451.2021.11.14

Security situation awareness technology of railway design corporations

LIU Feng, HAN Yu
(Information Design Research Institute, China Railway Design Corporation, Tianjin　300308, China)

Abstract: This paper analyzed the current situation of network security protection in railway design corporations, compared and formulated the security situation awareness technology scheme, focused on the problems encountered in the practice of situation awareness technology in railway design corporations, the adaptive adjustment of the existing network and security prevention and control system, implemented network wide traffic security situation monitoring and security automation, made the security situation awareness technology play a core value in the comprehensive network security prevention and control system, and effectively improved the overall security level of the corporations.

Keywords: situation awareness；network wide traffic analysis；security automation；security management platform；railway design corporations

《信息安全技术 网络安全等级保护基本要求》[1]中提出应采取技术措施对网络行为进行分析，实现对网络攻击特别是新兴网络攻击行为的分析。作为可满足该项要求的主要技术措施，安全态势感知[2]在大规模信息系统环境中，对系统环境因素进行获取、理解，结合全网网络流量、设备日志及威胁情报等数据进行安全大数据分析，实现对信息系统安全状态和趋势的显示及预测[3]，以便有效应对高级持续性威胁（APT，Advanced Persistent Threat）等复杂形式的攻击。

为满足网络安全等级保护的需要，本文以构建企业网络安全综合防控体系为目标[4]，在某铁路设计企业的自建网络中，研究并应用安全态势感知技术，补足网络安全短板，为提升铁路设计企业网络整体安全防护提供支撑[5]。

收稿日期：2021-08-31
作者简介：刘　峰，工程师；韩　寓，高级工程师。

1　网络安全现状分析

1.1　网络架构概述

某铁路设计企业内部局域网络规划 5 个物理网络分区，分别为骨干区、业务区、园区、运维区、边界区，如图 1 所示。骨干区通过高性能交换设备承载各分区流量转发；业务区提供服务器及存储设备的网络接入环境，同时，根据纵深防御要求，区域内部基于 VxLAN 虚拟网络划分多个虚拟网络分区，包括内部服务区、隔离区（DMZ，Demilitarized Zone）、测试研发区，并通过防火墙实现安全隔离；园区承载用户办公网络接入；运维区部署数据中心监控运维相关的平台软件；边界区提供互联网应用发布服务。

1.2　网络安全防护现状

网络安全防控策略依各分区内防护对象做出针对性部署。边界区为第一道安全防护屏障，采取包括访问控制、入侵防御系统（IPS，Intrusion Prevention

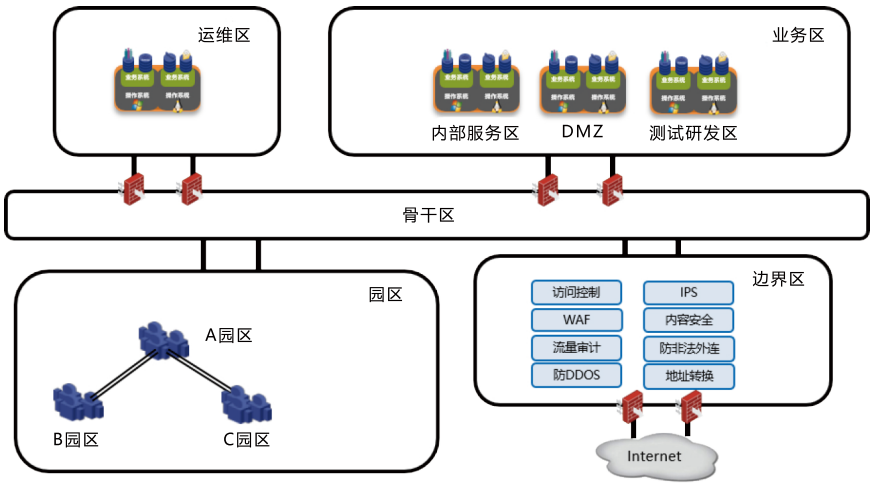

图1　企业网络拓扑

System）、Web 应用防护系统（WAF，Web Application Firewall）、内容安全、防非法外连、防 DDoS、流量审计等安全措施；业务区网络采取访问控制、IPS、防病毒、网页防篡改等安全措施；运维区网络边界提供访问控制、统一资源定位（URL，Uniform Resource Locator）过滤、漏洞扫描防护措施，并部署监控、审计、配置等运维作业平台；园区网络边界采取路由隔离、访问控制、终端防病毒、准入认证等防护手段。

1.3　现状分析

分析发现，该铁路设计企业的网络安全防护依然偏重于边界防护，实际安全运营过程中存在以下问题：

（1）安全监控系统有死角，没有覆盖到全网的网络安全运行情况；

（2）不同的安全系统互不兼容，缺乏集中检查和管理的手段；

（3）安全事件分析能力不足，利用人工检查发现安全事件的方式，导致安全事件响应处置滞后，效率较低。

2　安全态势感知技术研究

本文以安全态势感知技术为核心，搭建一套可监控、发现全网安全事件的安全管理平台，补强流量监控、集中管理及威胁态势分析方面的短板，同时，把安全管理摆在网络安全综合防控体系的核心位置上。

2.1　态势感知技术分析

网络安全态势感知技术分为基于网络流量数据和基于设备日志数据两种。该技术结合安全领域知识，使用大数据和机器学习关联分析实现全网安全状态的可视化度量。基于流量分析的态势感知对网络流量中的异常安全事件进行解析，包括攻击流量特征、威胁文件传输等，把结果实时同步到管理平台，进行深度关联分析及问题定位呈现；基于设备日志分析的态势感知通过采集安全设备、网络设备、服务器、中间件、业务系统等的日志，进行统一日志标准处理，对安全问题进行关联分析[6-8]。2 种态势感知的优劣势分析如表 1 所示。

2.2　态势感知方案制定

表1　态势感知技术对比

态势感知技术类型	优势	劣势
基于流量分析	1. 不需要其他设备对接配合，可实现快速部署，可复制性强 2. 借助原始流量关键信息的还原、存储，可提供更多的原始数据回溯支持，便于深度分析	1. 不能整合已有设备的安全信息，包括已经部署的安全设备 2. 流量分析能力受限于一家厂商的研发水平，不能集各家所长 3. 无法建立需要终端日志的分析模型，例如本地异常登录、网络地址转换（NAT，Network Address Translation）溯源等
基于日志分析	1. 能充分整合全网络安全相关信息，采集分析维度更全面 2. 可采集各安全设备的分析日志结果，不受限于一家厂商的分析能力 3. 满足网络安全等级保护的要求	1. 不同设备因厂商、类型的差异，采集的信息不可控，分析模型的复制性受限，对接优化周期较长 2. 由于没有原始流量数据支撑，对安全问题的回溯、深度排查受限

本文选择集成流量分析与日志分析功能的技术路线，以实现覆盖网到端的全面安全管理。基于安全态势感知技术的安全管理平台由数据分析系统、流量采集探针、日志审计系统构成。其中，数据分析系统实现流量与日志数据的集中安全关联分析与可视化展示；流量采集探针实现网络流量的捕获、初步攻击识别及威胁检测；日志审计系统实现终端日志收集及分类。数据分析系统和日志审计系统部署于网络运维区，流量采集探针部署于网络骨干区，如图 2 所示。

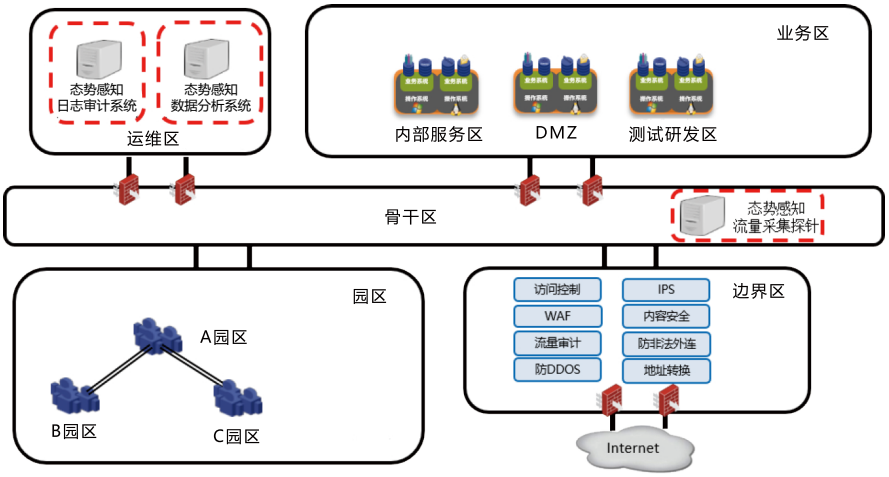

图2　安全管理平台部署示意

3　态势感知技术应用研究

3.1　数据中心虚拟网络流量监控

态势感知流量采集探针通常选取网络骨干区交换机作为流量采集节点，实现全网流量分析，解决各物理网络分区互访流量的安全监控、检测问题。然而，该企业数据中心业务网的内部虚拟网络分区间互访流量在设计之初不经过骨干网，导致流量捕获存在盲区。虚拟网络分区间访问流量由网关路由至业务区防火墙对应接口上，通过防火墙内部安全过滤后，流量从防火墙另一接口转发至目标虚拟网络分区中，不经过骨干区，也就无法被网络骨干区有效捕获，如图 3 所示。

为解决流量覆盖不全的问题，利用物理防火墙虚拟化技术，将每个业务区逻辑子网作为独立租户网络，单独分配虚拟防火墙，由此每台虚拟防火墙作为租户网络边界直接与骨干网建立路由，从而实现逻辑子网互访流量统一流经骨干网络，解决了业务区内部互访流量监测盲点问题，切实做到全网流量安全监控、检测，如图 4 所示。

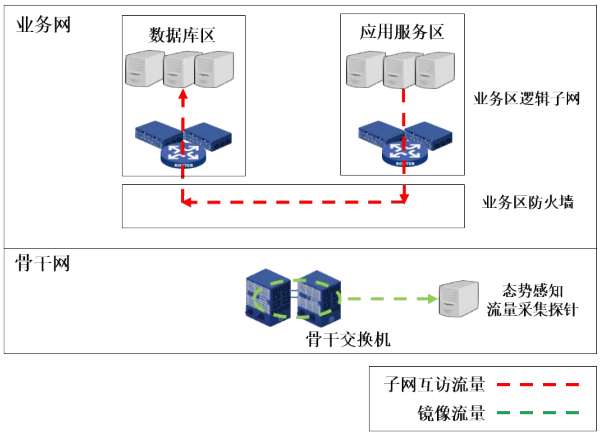

图3　业务区逻辑子网互访流量不经过骨干网示意

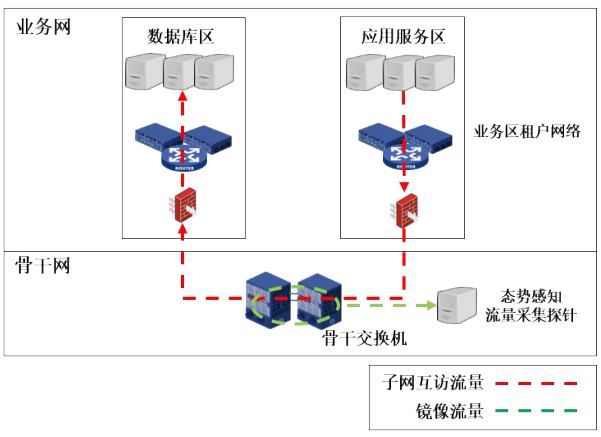

图4　业务区逻辑子网互访流量经过骨干网示意

3.2　SSL/TLS 加密流量的监测分析

安全套接字层（SSL，Secure Sockets Layer）/传输层安全（TLS，Transport Layer Security）密钥交换协议有 RSA 和 ECDHE两种。在 RSA 密钥交换协议中，通信密钥由客户端计算出来后，再传递给服务端，密钥交换和服务端认证在一步内完成，因此存在前向安全性问题，即拥有服务端私钥即可对历史加密流量进行解密；在 ECDHE 密钥交换协议中，通信密钥由通信双方各自算出，避免协商阶段直接传递，将密钥交换和服务端认证步骤分离，因此具备前向安全性。

信息系统普遍采用 SSL/TLS 加密向互联网发布，确保通信安全，同时使用 ECDHE 密钥交换避免前向安全性问题。但 ECDHE 的前向安全性导致旁路部署的态势感知流量采集探针无法解密流量，产生监控盲区。用于 SSL 加密的证书通常在服务器上部署，使得流量在抵达服务器之前均保持加密状态，如图 5 所示。

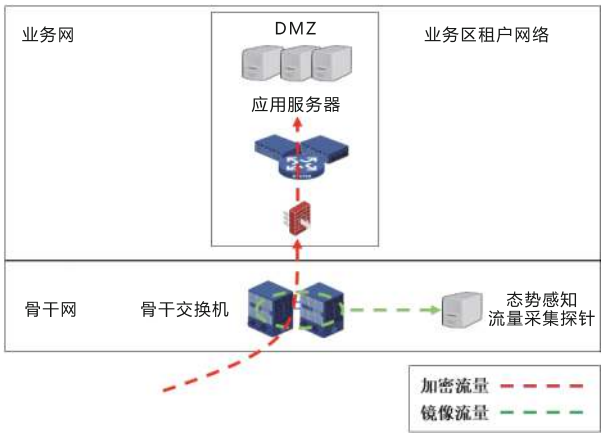

图5　SSL 证书部署于应用服务器导致无法检测加密流量示意

为解决 SSL/TLS 加密流量分析问题，该铁路设计企业通过自建互联网信息系统发布平台，统一为互联网应用提供反向代理、负载均衡、SSL 证书加解密、URL 过滤、协议优化等服务，同时在业务网络规划上，为互联网信息系统发布平台规划单独虚拟网络分区，具体是将 DMZ 更名为 DMZ 后端，新建 DMZ 前端部署互联网信息系统发布平台，如图 6 所示。经过改造调整，应用访问的加密流量先统一在发布平台做 SSL/TLS 解密。解密后，流量再经骨干网络路由到应用服务器所在逻辑业务分区。由此，态势感知流量采集探针即可捕获解密后的流量，实现对 SSL/TLS 加密互联网流量的分析检查。

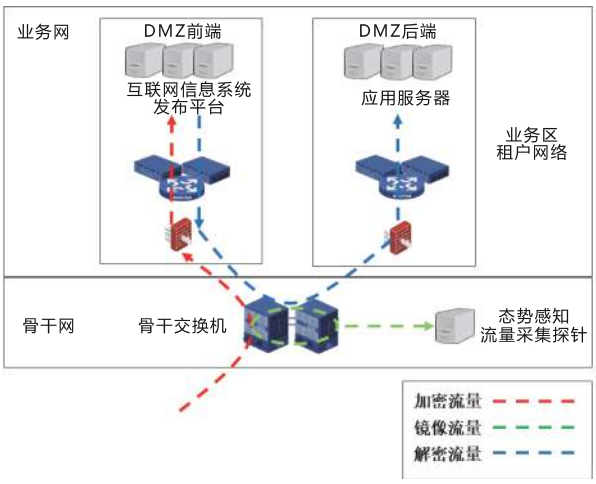

图6　通过互联网信息系统发布平台解决加密流量检测示意

3.3　基于态势感知的安全自动化

基于态势感知和大数据技术，能够实现部分安全事务的自动化处理，有效解决安全设备巡检、海量安全事件甄别等难题。

3.3.1　集中日志审计

应用态势感知技术实现网络安全设备及重要信息系统日志的统一收集，涉及定制适配各安全厂商、各系统日志模板等问题。后续根据安全需要，对日志进行分级分类，例如，标记系统后台登录等敏感行为日志，为追踪溯源提供统一日志查询入口。

3.3.2　全网流量实时分析

基于流量采集探针，对网络流量的深度解析、多维度威胁检测及对告警的数据聚合处理能力，可在海量流量监测数据中有效提炼风险隐患。对 Web 代码脆弱检测（如 SQL 注入、明文传输）、僵木蠕检测（如网内恶意域名请求）、文件沙箱分析（如网盘恶意文件检测）、横向渗透检测（如服务器间异常访问）等安全威胁，能够替代或辅助安全人员完成威胁的前期甄别筛查，使安全人员聚焦于后续隐患分析及处理，提高工作效率。

3.3.3　安全自动化联动

以安全态势感知为安全管理平台、防火墙为防护屏障、漏洞扫描器为脆弱检查机制，三者联动，

构建综合防控体系。在实践中，通过与防火墙接口联动实现安全管理平台自动向防火墙下达 IP 封锁、访问控制策略增删功能，串通了监测、分析与处置的环节。同时，基于态势感知自定义规则模板功能，可灵活定制不同的安全策略需求。例如，对重要防护对象实施更严格的安全策略，一旦发现攻击行为即进行攻击源 IP 封锁；对未登录堡垒机访问后台的流量行为，一经发现即进行 IP 封锁等。随着安全工作的不断深入，安全场景会不断丰富，围绕态势感知的自动化定制规则能够减少安全人员的重复性工作，提高风险处置效率。

4 结束语

该铁路设计企业通过建设基于态势感知技术的安全管理平台，实现了从边界防御、被动式防御向全网主动式防御的发展；通过数据分析系统不断优化对已知、未知威胁的发现及回溯能力；通过深化扩展安全设备联动范围，不断提高安全自动化水平。让安全技术人员将更多精力投入到关键安全事件分析中。

从企业安全态势感知系统部署、应用阶段的实践过程中不难发现，企业安全防控体系建设无法一蹴而就，信息安全技术理论的综合性及复杂性决定了态势感知技术在铁路设计企业落地过程中难免遇到前期规划无法覆盖的问题，而这些盲点问题往往更应得到安全工作人员的重视，积极采取措施化解，不仅能促进态势感知项目更好地落地应用，也是全面提升企业安全水平的有效途径。

下一步，该铁路设计企业仍需围绕态势感知系统磨合安全管理体系，建立与之相适应的措施，将态势感知系统的作用纳入安全闭环管理中，切实落实到安全规划、建设及使用中去。

参考文献

[1] 全国信息安全标准化技术委员会. 信息安全技术 网络安全等级保护基本要求：GB/T 22239—2019[S]. 北京：全国信息安全标准化技术委员会，2019.

[2] 王斯梁，冯 暄，蔡友保，等. 等保2.0下的网络安全态势感知方案研究[J]. 信息安全研究，2019（9）.

[3] 施卫忠. 铁路领域重要信息系统安全保障的创新与实践 [J]. 中国铁路，2020（4）：2-6.

[4] 王 磊，冯铁民. 关于国家电网公司网络与信息安全态势感知的思考 [J]. 工程技术（文摘版）·建筑，2017（10）：111-112.

[5] 丘惠军，陈 昊. 供电企业网络与信息安全态势感知的实践 [J]. 数字通信世界，2020（4）：246，255.

[6] 蒋 凡，程绍银，贾振宏，等. 信息网络安全态势感知研究与实践 [J]. 中国信息安全，2011（2）：36-40.

[7] 邓 鑫，田 征，李 楠，等. 浅析网络安全态势感知技术在气象网络中的实践与应用 [J]. 网络安全技术与应用，2020（5）：139-143.

[8] 陈春霖，屠正伟，郭 靓. 国家电网公司网络与信息安全态势感知的实践 [J]. 电力信息与通信技术，2017，15（6）：3-8.

责任编辑 李依诺