基于物断单导系统实现的异构网络数据传输

王伟怡
台山核电合营有限公司
DOI:10.12238/pe.v2i4.8346

[摘　要] 本论文基于物理隔离的两个异构网络,通过部署物断单导系统,进行安全、可靠、单向的数据传输,以增加网络安全,保护敏感数据,满足法规要求和业务对异构网络环境的数据利用需求。
[关键词] 物断单导；网络隔离；数据传输；传输验证
中图分类号：TN405.95　**文献标识码**：A

Heterogeneous network data transmission based on the single conduction system

Weiyi Wang
Taishan Nuclear Power Joint venture Co., LTD

[Abstract] This paper is based on the isolation of two physically isolated heterogeneous networks, through the deployment of single guide system, safe, reliable, one-way data transmission, in order to increase network security, protect sensitive data, meet the regulatory requirements and business for heterogeneous network environment data utilization needs.
[Key words] material breaking and single guide; network isolation; data transmission; verification

引言

为提升电站的网络安全水平,控制网络应用规模,某电站的生产管理信息区和办公管理信息区进行了网络物理隔离,消除了外部直接网络攻击风险,确保了电力监控系统的安全。同时为满足办公网对生产数据的利用,通过部署物断单导系统,利用激光的单向传输特性,安全、可靠、有效传递生产数据。本文通过介绍某电站物断单导系统项目的实施,结合物断设备的物理特性和安全属性,论证了物断设备单向传输的技术要点,解决了异构网络生产数据单向传输的问题,为生产数据的进一步利用和价值发挥打下坚实基础。

1 网络安全隔离的概述

1.1背景

国务院第745号令《关键信息基础设施安全保护条例》自2021年9月1日正式施行,要求“安全保护措施未与关键信息基础设施同步规划、同步建设、同步实施的”,运营者要承担相应的法律责任。

随着网络攻防对抗持续升级,能源企业已成为网络攻击的主战场之一。为了提升电站的网络安全水平,加强纵深防御,消除来自外部直接网络攻击风险,确保电力监控系统等关键生产信息系统的安全,某电站对生产管理信息区和办公管理信息区进行了网络物理隔离,降低了攻击成功的可能性,防止外部直接网络攻击,提升网络的安全性能。

1.2网络物理隔离的意义

实现网络物理隔离后,企业可以将不同级别的数据(如公开信息、内部信息、敏感信息等)存放在不同的网络中,并应用不同的安全策略,这样可以防止敏感数据被未授权的用户访问。通过敏感重要系统、数据的物理隔离,减少了外部攻击面,保护关键信息资产;加上防火墙策略,可以限制内部网络中不同系统之间的直接通信及用户对系统的直接访问,限制了攻击点的横向移动。同时,隔离后生产管理信息区和办公管理信息区形成相对较小的网络区域,相对来说更容易监控,进而提高监测和响应安全事件的能力。网络物理隔离可以防止某个部分的网络问题如(广播风暴、网络堵塞、故障等)等影响到其他部分,提高整个网络的稳定性和可靠性。而且不同的隔离网络可以根据业务的需要,实现不同的安全策略；当安全事件发生时,隔离的网络区域可以快速被处理,而不影响到其他网络。

2 基于物断单导系统实现的异构网络数据传输原理

2.1技术概述

物断单导(物理断开激光信息单向导入系统)部署在两个不同安全等级或异构网络之间,通过利用激光的单向传输特性,将数据单向、无反馈地从发送端导入到接收端；从而提供安全可靠的网络安全措施,实现异构网络之间提供单向数据传输,同时保持网络的物理隔离,确保数据的安全和系统的稳定运行。

通过部署物断单导系统,进行安全、可靠、单向的数据传输,从而起到保护敏感数据、满足法律法规要求和业务对异构网络环境的数据利用需求。

2.2安全属性和工作原理

物断单导的安全性能有以下几方面：

(1)物理隔离：物断设备可以在不同安全等级的网络之间实现物理上的断开，意味着两个网络之间没有直接的物理连接，从而避免了任何形式的电磁波、电信号或物理接触的传输路径；

(2)单向激光传输：以红外激光为信息载体、空气为传输介质，实现设备间无物理线缆连接的信息传输，满足网络间物理断开的要求；

(3)国密算法：通过使用国产密码技术和可信计算技术对传输的数据进行加密，确保即使数据在传输过程中被截获，也无法被未授权的第三方解读；

(4)无反馈机制：单向传输不会有任何反馈信号从接收端传回到发射端，进一步增强了系统的安全性，避免任何形式的逆向通信，从而减少潜在的攻击面；且发送端机向接收端机传输数据必须是原始数据，所有数据解析到应用层，需要传输的数据全部是应用还原的完成格式，不携带任何协议信息。

物断单导系统包含以下基础组件：

(1)应用适配器：分为发送端和接收端，以软件形态安装在物理断开激光信息单向导入设备两侧服务器中；对接各种应用系统协议，剥离应用系统数据，在模块中重新封装为内部通信协议，支持文件(FTP、SFTP、webservice接口调用)，邮件(建立SMTP中继)，数据库、数据流(TCP)的传输。

(2)物理断开激光信息单向导入设备：是物断单导的核心组件，部署在应用适配器中间，内部也有发送端和接收端，但彼此间无任何电气连接，仅通过激光传输数据。如图1所示：

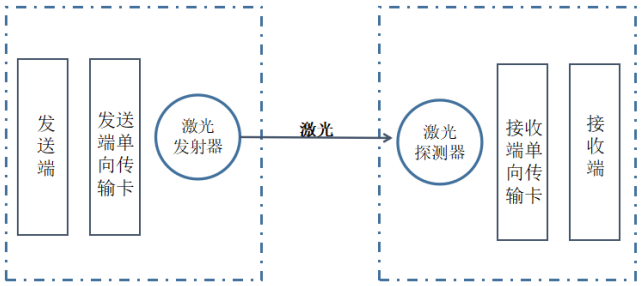

图1　物断单导逻辑组成

通过服务器上安装的发送应用发送数据，应用将数据传输给应用适配器，应用适配器对数据进行合规性检查。

包括需传输的文件大小、类型、内容等信息进行检查，合规的文件才允许传输；基于五元组的网络防护功能(包括源IP、目的IP、协议、源端口、目的端口)，合规的应用才允许接入；检查通过后，在发送端对传输数据进行分包，按照内部专用协议进行封装和通信；应用适配器根据策略将数据传输至接收端应用，到了接收端应用适配器，对专用协议传输的数据包进行解析，重新还原成应用协议。

3 某电厂物断单导单向传输数据应用实例

物断单导系统适用于需要高度安全隔离的网络环境，如能源、电力企业的安全通信等；数据从发射端到接收端的延迟非常低，能够实现数据的实时传输，适用于需要实时数据传输的应用场景。

某电站的生产管理信息区和办公管理信息区进行了网络物理隔离后，办公区对生产区的数据仍有访问需求，而从安全的角度上，已无法实现直接访问需求。其中，生产管理区对数据的实时性和准确性要求比较高，业务系统的主要使用对象是生产一线人员；办公管理区主要是处理企业内部业务和经营管理信息的计算机网络区域。以某指定生产信息系统数据库的数据通过物断单导传输为例，通过部署物断单导系统连接两个异构的网络，并实现前后端数据库的单向安全读取、传输，满足办公区对生产信息区的数据利用需求；物理断开的数据摆渡设备也满足了网络安全的要求。

3.1整体的架构设计

系统整体架构设计如图2所示：

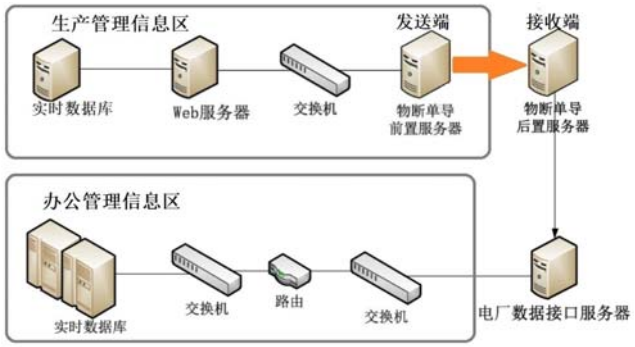

图2　某电站物断单导整体架构和数据流向

部署在生产管理信息区的应用服务器，主要是通过数据库的API接口获取实时数据，进行数据打包，并通过TCP/IP发送到物断单导前置服务器；部署在办公管理信息区的应用服务器，主要是通过接收物断单导后置服务器发送的TCP/IP数据包，进行数据包的解包，并通过数据库API接口写入到实时数据库。

系统根据TCP流代理的配置在发送端应用适配器上监听TCP端口，接收发送端的TCP连接和数据，并对TCP数据进行剥离与重新组包，单向导入至接收端，接收端的应用适配根据配置把这些数据重组为TCP流发送给相应的接收端服务器。

3.2资源需求

系统实施所需资源如下：

硬件方面包括：物断单导设备(配置双电源冗余，实现不停机切换；采用符合信创标准的高性能CPU处理器和操作系统)应用服务器2套(物理机虚拟机均可，分别对应发送端、接收端应用软件安装)以上设备均需满足7*24小时不间断运行。

辅助设备包括：机柜机架预留6U空间；交换机、路由器等网络设备(根据前后两个网络组网的情况配置)；显示器1套，鼠标键盘1套，专用笔记本电脑1台(作为配置附属设备)，RJ45网线若干。

软件：发送端/接收端应用软件，实时数据库专用客户端软件。

3.3系统单向数据通道实现

某电厂通过物断单导设备,实现特定频段的激光信号传输,满足数据的高性能传输要求:在发射端,通过信号处理电路将太网信号转换为串行信号、将串行电信号转换为光信号；接收端信号处理电路将光信号转换为串行电信号、将串行电信号转换为以太网信号。

4 技术实现和验证

4.1关注点和流程处理机制

整个系统的部署涉及物断设备的上架、配置,服务器的软件安装、调试,网络策略的开通等、网络配置等,还需提前完成机柜上架准备、服务器资源申请、固定IP地址申请、账号申请等工作。

生产管理信息区和办公管理信息区处于不同的网络环境,需要提前为发送端和接收端应用配置IP/端口,并在发送端、接收端进行配置:通过发送端和接收端提供的Web服务和可视化的系统管理软件,系统管理员可进行发送端、接收端的应用适配,包括网络接口、系统参数、安全规则等；还要完成两台应用服务器的配置和权限开通,包括:读取发送端生产信息系统数据库的权限(账号和密码),接收端写入办公信息系统的数据库权限(账号和密码);另外,根据目标IP/端口和源IP/端口需提前进行防火墙策略放行,避免数据受制无法传输;发送端应用适配与接收端应用适配软件结构一致,在系统运行时根据部署不同加载相应模块提供服务。

4.2 Web服务管理

物断单导前置和后置服务器,提供了web服务器管理系统,允许系统管理员对系统的发送端、接收端的应用适配进行配置,提高了系统的灵活性和可用性。配置内容包括接口、参数、传输任务等。系统管理员登录认证支持商密算法,支持用户名口令,UsbKey等多因子认证方式。

4.3安全控制功能指标和性能指标

整个系统实现基于IP地址、网络端口的访问控制,通过设置可接入系统的源IP地址及服务端口,阻止非法IP接入系统,并支持深度病毒检测；通过系统的业务日志记录数据中的各个环节状态,通过操作日志对应用的交换信息、安全控制信息等进行记录实现审计功能。

能实现信息单向导入功能,具体包括文档、邮件、数据库、数据流的单向传输和同步。实现协议剥离和原始数据传输,即发送端向接收端传输数据必须是原始数据,不携带任何协议信息。所有数据解析到应用层,需要传输的数据全部是应用还原的完整格式。提供对数据库的单向同步功能,数据库同步支持开源数据库和主流国产化数据库,及支持数据库全表同步、增量同步及全表后增量同步功能。支持邮件的单向中继功能,支持SMTP和POP3协议。

4.4测试和验证

某电厂通过物断单导实施的生产管理信息区和办公管理信息区的实时数据库同步,其中传输路径经过数据包的解析、激光传导、重组,需要验证数据是否实现了实时同步,以保障数据传输的及时性和有效性。不同的传输内容(如邮件、文件、数据流)测试方案,本项目传输内容为将结构化数据,以下为实际采用的验证方法。

生产管理区实时数据库增加新表、新表字段,识别增量同步及全表后增量同步功能,在办公管理信息区实时数据库能实现映射关系,识别新增字段和创建映射规则。

通过生产管理区和办公管理区的专用授权客户端进行有效性验证,分别访问两侧实时数据库,抽取和对比随机实时数据,比较相同字段的实时数据变化情况,包括数据值和变化趋势;两侧数据要线性一致且无缺漏；稳定性验证：物断单导连续运行24小时,运行过程中定期对数据进行抽样对比,确保数据无丢失。

安全测试方面,使用自动化扫描、端口扫描、动静态分析工作、漏扫工具等对接口服务器部署的应用进行测试,并需完全通过。

5 结论

某电厂基于物断单导设备,在生产管理信息区和办公管理信息区的物理隔离的基础上,实现了实时数据安全、有效传输;既满足了网络安全管控要求,又保证了办公系统对生产管理数据的及时利用,为后续发挥生产数据的价值打下坚实基础。

[参考文献]

[1]吴亚铭,李璐,何伟光,等.一种提高网络隔离单向传输系统可靠性的方法[J].网络空间安全,2021,12(Z5):39-43.

[2]程少良.高速网络多模式相似数据串隔离式传输仿真[J].计算机仿真,2021,38(06):117-120.

[3]李建臣.单向传输技术研究与展望[J].电子技术与软件工程,2022(06):17-20.

作者简介：

王伟怡(1979--),女,汉族,广东省广州市人,大学本科,台山核电合营有限公司,工程师,研究方向：基础设施和信息化管理。