基于 GAP 技术的地震信息网络系统改造方案①

付荣国, 陈兴东, 章熙海, 肖 飞

(江苏省地震局 应急救援中心, 南京 210014)

摘 要: 江苏省地震信息网络系统是全省区域地震数据传输、数据交换、数据存储及信息服务的统一平台. 针对网络系统目前存在的问题, 提出了改造方案, 即通过使用隔离网闸将业务传输系统和互连网进行物理隔离, 升级网络关键设备和链路带宽, 增加网络安全设备等技术手段, 使网络系统达到了安全、稳定运行的目标, 既满足了地震信息数据传输、交换、存储及多元化应用等的需求, 又符合信息系统三级安全管理要求, 可以为地震行业信息网络系统优化建设提供有益参考.

关键词: 地震信息网络; 信息系统; 网络改造; 隔离网闸; 信息安全; 网络安全

Reconstruction Scheme of Earthquake Information Network System Based on GAP Technology

FU Rong-Guo, CHEN Xing-Dong, ZHANG Xi-Hai, XIAO Fei

(Emergency Rescue Center, Administrator of Jiangsu Province, Nanjing 210014, China)

Abstract: Earthquake information network system of Jiangsu province is a unified platform of regional seismic data transmission, data exchange, and data storage and information service. Aiming at the existing problems of the network system, an updating scheme is put forward. There are mainly: to physically separate the transmission system and Internet by GAP, to upgrade the key equipment and links bandwidth of the network, to increase network security equipment. Through those technical means, the network system achieves a safe, stable operation target, both to satisfy the needs of the information and data transmission, exchange, storage and diversified applications of seismic, and to meet the requirements of three level safety management of information system. The scheme can provide a useful reference for optimizing the seismic information network system.

Key words: earthquake information network; information system; network reconstruction; gap; information security; network security

地震事件发生后, 社会公众对地震部门的网络访问量骤然增加, 容易造成网络堵塞, 甚至瘫痪; 而地震部门也需要快速发布相关的信息服务产品、顺利地开展应急协调联动等工作, 因此, 应有可靠的网络平台.

江苏省地震局“十五”期间建设的重点工程“江苏省数字地震观测网络”(简称“行业网”)是中国地震局“十五”重点项目“中国数字地震观测网络”[1]和江苏省“十五”重点项目“江苏省防灾减灾预警信息系统一期工程”[2]的重要组成部分. 通过项目的建设实施, 使全省形成了以计算机网络为架构的, 集地震信息采集、传输、处理和服务于一体的现代化数字地震前兆、测震和强震观测系统, 地震活断层探测及危险性评价服务系统, 地震应急指挥技术支撑系统, 以及地震信息网络系统等 6 个业务子系统. 这 6 个子系统承担着全省地震监测预报、震灾预防、应急救援、公众宣传与服务等工作, 而地震信息网络系统作为其它 5 个子系统的网络传输平台, 能否稳定运行, 对江苏省防震减灾工作有着重要意义.

近几年来, 随着全省防震减灾工作的不断开展, 现

① 基金项目:国家地震专业基础设施项目(2012BAK15B05);江苏省地震局青年科技基金(201010)
收稿时间:2014-09-11;收到修改稿时间:2014-11-13

有的网络传输平台已不能完全满足地震信息传输、数据存储等业务和信息安全的要求, 需要进行升级改造. 本文对该网络传输平台的升级改造方案进行了总体设计, 详细说明了实施策略, 总结了方案的优点, 并对方案下一步工作做了说明.

1 江苏省地震信息网络系统

1.1 网络系统简介

网络系统全省共建设信息节点 30 个, 其中省级区域中心节点 1 个, 大中城市节点 3 个, 县级节点 15 个, 台站节点 11 个, 节点分布如图 1 所示.

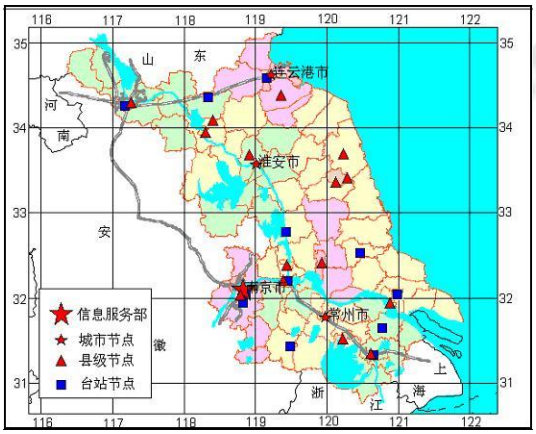

图 1 江苏省地震信息节点分布图

作为全省地震行业专网, 系统采用二层点对点星型结构, 省级区域中心与全省 29 个信息节点以 2M SDH 专线为主, VPN 为辅的方式实现全省广域网连接; 省级区域中心与国家地震台网中心通过以 3 条 2M SDH 专线为主, VPN 为辅的方式互联, 从而与全国其他省市地震系统间实现互联互通. 省级区域中心采用双核心交换负载均衡方式, 统一进行信道、路由、地址、域名、子网、网络安全等整体规划, 并对各分业务系统制定必要的子网策略, 对数据存储和数据库进行统一设计、整体规划, 实现了数据的集中管理和存储; 另外, 在省级区域中心统一部署了公用服务器, 而专用服务器划归各业务部门工作区, 方便了设备运行和维护的统一管理. 网络系统使全省实现了省内测震、前兆、应急、强震等各技术系统的网络集成, 并为全省区域地震信息服务、数据交换、数据存储提供了统一的平台, 其拓扑结构如图 2 所示.

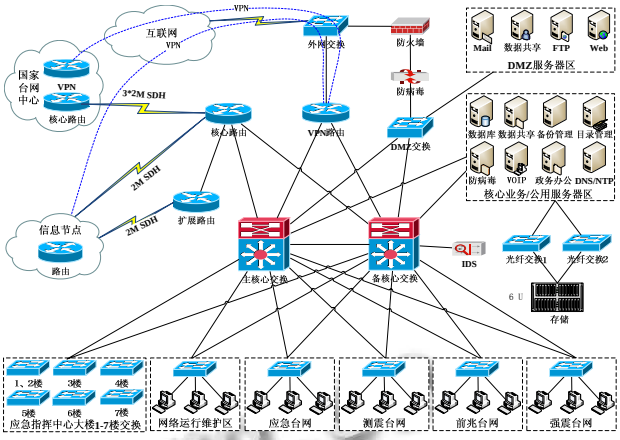

图 2 江苏省数字地震观测网络拓扑图

1.2 目前存在主要问题

网络系统自投入使用以来, 已取得明显的社会和经济效益, 但随着近几年全省防震减灾事业的发展, 暴露出以下问题:

(1)网络的建设没有考虑业务数据传输与互联网的物理隔离, 网络中的安全设备较少, 且设备陈旧, 存在较大的安全隐患;

(2)近几年“陆态网络”、“社会服务工程”、“背景场探测”和“监测台站加密”等重大建设项目的实施, 全省台站接入数量不断增加, 观测数据数量成倍增加, 导致网络的核心路由器、核心交换机和存储设备在保障台站接入、数据存储等方面已接近能力上限;

(3)网络核心设备是“十五”配置, 其使用寿命已超过 6 年, 目前已出现故障率上升等问题, 影响整个网络的稳定运行;

(4)网络中视频会商、应急联动等多元化应用不断增加, 省级区域中心与国家台网中心的 3 条 2M SDH 链路其带宽已远远不能满足这些应用的需求, 且链路运行商只有 1 家, 缺少备份;

(5)网络中上联台网中心的核心路由器只有 1 台, 存在单点故障隐患; 存储系统只有 1 套, 且存储能力有限, 数据的存储备份存在安全隐患;

(6)缺少统一的网络和安全管理平台, 无法实现对各种网络设备和安全设备的管理与监控.

2 改造方案设计

借助中国地震局“十二五”《国家地震专业基础设施专项建设规划首批项目-全国各省级地震信息支撑平台建设项目》支持, 对网络系统进行升级改造, 将网络划分为外网区(互联网)和内网区(业务数据传输网),

内外网之间使用隔离网闸(简称 GAP)[3], 利用网闸来实现内外网间的数据交互和安全防护, 升级改造后的网络拓扑如图 3 所示.

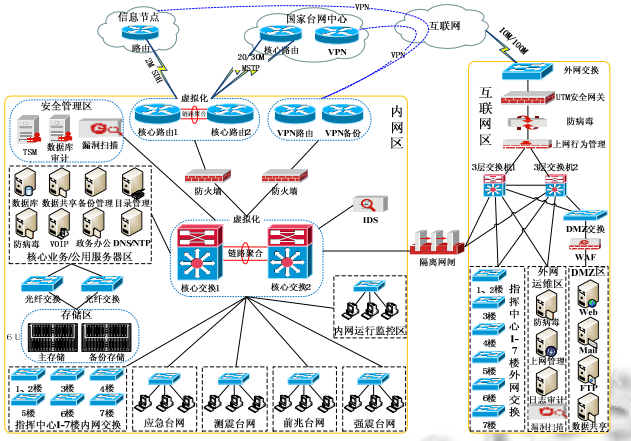

图 3　优化改造后网络拓扑图

2.1 内外网数据交换

隔离网闸(GAP)是使用带有多种控制功能的固态开关读写介质连接两个独立网络的信息安全设备, 能够隔断两个接入网络之间的所有连接, 不光检查所有协议, 还把协议给剥离掉, 直接还原成最原始数据, 对数据可以检查和扫描, 防止恶意代码和病毒, 甚至对数据的属性进行要求, 不支持 TCP / IP, 不依赖操作系统, 数据传输机制在文件和数据信息的交换过程中不可编程. 也就是 GAP 对 OSI 模型的七层(物理层、数据链路层、网络层、传输层、会话层、表现层、应用层)进行全面检查, 在异构介质上重组所有的数据. 隔离网闸的物理隔离或网络隔离是对 OSI 全部七层的断开, 在断开的基础上首先进行防病毒检查处理和安全审查管理, 然后以“摆渡”文件或数据信息的交换方式, 在应用层将原始数据通过存储介质的“写入”与“读出”完成数据转发, 并能够在阻断各种网络攻击及入侵的前提下, 提供安全浏览、收发邮件及基于文件和数据库的信息交换[4].

内外网之间部署采用透明方式的 GAP 进行内外网数据交换, 当内网与外网之间无信息交换时, GAP 与内网, GAP 与外网, 内网与外网之间是完全断开的, 即三者之间不存在物理连接和逻辑连接.

当内网数据需要传输到外网时, GAP 主动向内网服务器数据交换代理发起非 TCP/IP 协议的数据连接请求, 并发出“写”命令, 将写入开关合上, 并把所有的协议剥离, 将原始数据写入存储介质. 在此过程中, 外网服务器与 GAP 始终处于断开状态.

一旦数据完全写入 GAP 的存储介质, 开关立即打开, 中断与内网的连接. 转而发起对外网的非 TCP/IP 协议的数据连接请求, 当外网服务器收到请求后, 发出“读取”命令, 将 GAP 存储介质内的数据导向外网服务器. 外网服务器收到数据后, 按 TCP/IP 协议重新封装接收到的数据, 交给应用系统, 完成了内网到外网的信息交换.

从外网到内网的信息交换, 与上述类似, 只是方向相反. 每一次数据交换, GAP 都经历数据的写入、数据读出两个过程; 内网与外网永不连接; 内网和外网在同一时刻最多只有一个同隔离网闸建立非 TCP/IP 协议的数据连接, 从而实现数据安全防护功能.

2.2 互联网区

互联网区域采取的主要措施:

(1)增加网络安全设备. 新增 1 台集 IPS、IDS、防火墙等功能于一身的 UTM 一体化安全网关取代原防火墙, 从而实现对网络的访问控制、垃圾邮件拦截、病毒防护、入侵检测、入侵防御等功能; 增加漏洞扫描, 及时发现网络中各种安全隐患及漏洞, 通知相关人员进行升级修补;

(2)加强网络安全管理. 增加上网行为管理系统, 实时监控用户的网络流量和对互联网的上网行为, 并实现对用户互联网访问的控制和管理; 增加日志审计系统, 留存互联网区域网络设备和安全设备日志, 便于日后安全事件审计与追查;

(3)加强 DMZ 区安全防护. DMZ 交换机划分 Vlan, 进行端口保护, 禁止不同 Vlan 间相互通信, 并新增 1 套 Web 应用防护系统(WAF), 加强外部用户对 Web 的访问安全性, 防止 SQL 注入、网页篡改、网页挂马等安全事件发生;

(4)部署统一的病毒主动防御软件. 统一部署东方微点网络版主动防御软件, 对各类病毒进行主动防御, 保护全网终端及服务器, 从而抑制来自外部或内部网络的恶意病毒传播, 并建立全网统一的升级服务中心, 实现全网统一升级管理;

(5)调整网络结构. 将原 2 台核心交换作为外网三层交换与网闸连接, 在内外网数据交换时进行路由选择; DMZ 交换不再与防病毒直接相连; 原 1 至 7 楼内网交换变更为 1 至 7 楼外网交换, 从而整个大楼互联网网络拓扑结构不需大的改变.

2.3 内网区

内网区采取的主要措施:

(1)上行链路进行扩容备份. 省级区域中心到国家台网中心之间的链路由原 3 条 SDH 线路升级为 2 条 MSTP 线路(1 条 30M 的电信和 1 条 20M 的联通), 从

而为多元化的应用和信息共享提供带宽保证;

(2)核心设备升级更新. 新增 2 台支持链路聚合的核心路由替换原核心路由(作为备份路由), 新增2台支持链路聚合的核心交换替换原 2 台核心交换, 核心路由和交换聚合后各虚拟化为 1 台, 从而加速内网(地震行业网)区域的收敛速度; 新增 1 套 80T 的存储系统作为主存储, 原存储系统作为备份存储, 从而加强对业务数据的实时备份和及时恢复;

(3)VPN 路由备份及线路调整. 将原扩展核心路由作为 VPN 备份路由, 增加 1 条 VPN 备份线路(与原 ISP 运行商不同), 并将原网络防火墙接入 VPN 线路中, 加强 VPN 线路的边界安全防护;

(4)加强网络安全管理. 在核心路由和核心交换间新增 1 台防火墙, 用来加强内网与国家台网中心和省内信息节点间的安全防护; 新增漏洞扫描、数据库审计系统和终端安全管理平台(TSM)等设备, 实现对网内各种网络设备和安全设备的管理与监控;

(5)网络结构调整. 在不新增交换机的情况下, 将现物理隔离的政务系统和权力阳光系统交换接到新核心交换上, 修改交换机配置后即可作为指挥中心大楼 1 至 7 层内网交换, 整个内网网络拓扑结构不需大的改变.

3 方案创新

(1)针对原业务网和互联网逻辑隔离存在的安全隐患, 利用 GAP 技术进行物理隔离, 保护了业务数据的安全, 并实现了内外网数据的交互;

(2)将原上行 SDH 线路升级为 MSTP 线路, 保障了内网(地震行业网)业务数据传输的高速、及时, 且满足了业务系统的多元化应用需求;

(3)对核心路由和交换的升级更新, 网络可以满足今后信息节点及台站等接入点不断增加的需求;

(4)增加存储系统, 实现了对业务数据备份能力的扩容, 满足了今后地震信息数据不断增长的备份需求;

(5)对 VPN 设备及线路的备份, 实现了网络与国家台网中心、信息节点之间的多种连接方式, 增加了网络的可靠性与稳定性;

(6)通过增加安全技术手段, 加强了内外网访问的边界安全防护, 实现了对内外网访问的控制, 留存了日志审计, 做到事后可追查, 从而提高了内外网安全管理水平和对安全风险的抵抗能力;

(7)将原政务系统和权力阳光系统接入内网, 省局、市县及台站三者间的办公可直接在地震行业网内进行, 从而节省资源, 并大大提升了办公效率;

(8)实现了网络安全防护、系统安全防护、应用安全防护及系统安全管理, 达到了信息系统等级保护三级[5]的相关要求.

4 进一步工作

按照改造方案实施后, 网络系统已能满足地震信息传输和安全管理要求, 但还有一些地方可以进一步改进, 主要有:

(1)需要增加信息数据的异地容灾备份;

(2)增加 3 台防火墙, 1 台用于互联网防火墙备份, 1 台用于内网核心路由防火墙备份, 1 台用于内网 VPN 路由防火墙备份;

(3)利用虚拟技术, 实现对全部服务器的虚拟化和备份, 这是今后网络优化建设的重点;

(4)增加 1 台隔离网闸, 用于内外网数据交互时备份;

(5)对重要设备如应急台网交换、测震台网交换、DMZ 交换等进行备份, 从而保障所有业务部门的工作顺利开展;

(6)在 29 个信息节点中选取部分节点变更为中间节点, 减少信息节点与省级区域中心节点间的 SDH 区间线路(变更为区内线路), 从而降低全省通信信道的费用[6].

5 结语

江苏省地震信息网络系统既承担了地震观测数据从台站到省局区域中心和国家中心, 地震应急数据从地震现场到各级应急指挥部的传输、汇聚、交换、共享等功能, 又是省局互联网和门户网站、邮件、数据存储等信息服务的管理中心, 按照上述升级改造方案实施后, 网络具有高速带宽、快速收敛、实时备份、容易管理等优点, 且具备了层层设防, 重点突出, 策略联动, 管理为上的目标和优势, 能够满足江苏防震减灾工作未来几年的发展需求.

参考文献

1 刘瑞丰,高景春,陈运泰,吴忠良,黄志斌,徐志国,孙丽.中国数字地震台网的建设与发展.地震学报,2008,30(5):533–539.
2 付荣国,章熙海,肖飞,刘鹏飞.地震应急卫星通信指挥车通信系统设计.通信技术,2014,47(2):215–220.
3 万平国.网络隔离与网闸.北京:机械工业出版社,2004.
4 张骁,李红信.信息安全建设中的隔离网闸技术应用研究.山西师范大学学报(自然科学版),2010,24(2):43–47.
5 胡志昂.信息系统等级保护安全建设技术方案设计实现与应用.北京:电子工业出版社,2010.
6 张宇翔,罗词建,罗治国,李媛媛.陕西地震监测台网恢复重建与通讯网络改造.地磁地震观测与研究,2011,32(5):123–127.