基于安全等级保护的医院网络安全优化方案实践

臧 璆 汪春亮

（苏州大学附属第二医院信息处 苏州 215000）

〔摘要〕 介绍安全等级保护要求，以苏州大学附属第二医院网络安全改造实践为例，详细阐述网络安全规划路径及方法、优化改造方案、实施情况和效果，为相关研究提供参考。

〔关键词〕 网络安全；物理隔离；安全等保；安全改造

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2022.03.016

Practice of the Optimization Scheme of Hospital Network Security Based on Classified Security Protection *ZANG Qiu, WANG Chunliang, Information Department, The Second Affiliated Hospital of Suzhou University, Suzhou 215000, China*

〔**Abstract**〕 The paper introduces the requirements of classified security protection and takes the network security reconstruction practice of the Second Affiliated Hospital of Suzhou University as an example to elaborate the network security planning path and method, optimization reconstruction scheme, specific implementation and effect, so as to provide references for related study.

〔**Keywords**〕 network security; physical isolation; classified security protection; security reconstruction

1 引言

苏州大学附属第二医院信息化建设工作全方位覆盖运营管控、决策分析、临床业务、科研教学等业务活动，应通过信息化手段推进医院医疗水平和业务流程创新和持续优化[1]。医院信息化建设不断推进对网络的可靠性和安全性提出更高要求。苏州大学附属第二医院目前网络稳定性和安全性较低，已无法满足医院现有应用业务要求，需要重新规划、设计和改造实施[2]。

〔修回日期〕 2021－07－22

〔作者简介〕 臧璆，硕士，工程师，发表论文 5 篇；通讯作者：汪春亮，高级工程师。

2 等保 2.0 安全要求

2019 年 5 月《信息安全技术网络安全等级保护基本要求》2.0 版本（以下简称等保 2.0）发布。同年 12 月等保 2.0 正式实施，为医疗行业提供更完善的安全规范和技术要求。等保 2.0 的安全要求从内容上可以分成技术和管理两部分。技术要求和管理要求分别包括 5 个方面。技术要求可分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心；管理要求可分为安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理。本项目侧重安全通信网络、安全区域边界和安全管理中心建设。在安全通信网络方面，对整体网络架构提出更详细要求。网络带宽和

关键网络设施处理能力需要满足业务高峰期的需求。安全区域边界可能涉及多条网络边界，包括互联网、社保单位、卫健委等上级单位、合作银行和附属大学边界等。不同网络边界分属不同安全设备。安全管理中心是等保 2.0 全新规划节点，该节点包括对各项设备系统运维情况、各类日志、策略配置、监控情况、恶意代码等的集中管理。

3 网络安全规划

3.1 网络安全现状分析

3.1.1 医院现有网络安全建设情况 本院网络包括两个院区园区网、数据中心以及安全设施区域。网络设备和安全设备等已经使用较长时间，呈老化状态。承载网核心和汇聚、数据中心核心和汇聚都采用智能弹性架构（Intelligent Resilient Framework，IRF）虚拟化技术进行冗余配置，链路采用聚合技术，达到设备和链路冗余状态。医院网络采用内外网混合模式，即内网和外网使用一套物理网络进行转发。

3.1.2 医院现行网络存在的问题 内外网未进行有效隔离，仍采用内外网混合的旧模式；网络设备和安全设备部分老化，未及时更新升级；骨干网未全部升级到万兆，业务高峰时期流量转发慢；未完全按照新的安全等保技术要求配置。

3.1.3 网络安全改造升级需求 医院现阶段业务正在逐步与互联网接轨，以患者为中心，APP、微信公众号、微信小程序为服务载体，逐步建设互联网医院。随着越来越丰富的互联网应用推进，医院需要应对来自互联网的安全隐患问题，亟需进行网络安全改造升级[3]。

3.2 优化改造目标

一是内网和外网需进行物理隔离。医院根据实际情况搭建一套完整的、与内网完全物理隔离的外网。二是内网和外网需要安全加固。根据安全等级保护要求，内网和外网结合不同业务需求和技术要求，进行有效安全加固。三是更新升级已有部分内网。网络和安全设备使得承载网骨干部分全部达到万兆带宽，桌面带宽达到千兆速率。

4 优化改造方案

4.1 内网方案

4.1.1 概述 首先对内网现有网络和安全设备进行更新升级。将现行网络建设成为内网网络，见图 1。根据安全等级保护要求调整内网架构，加固边界和内网安全，使医院安全体系从被动防御转为主动防御[4]。

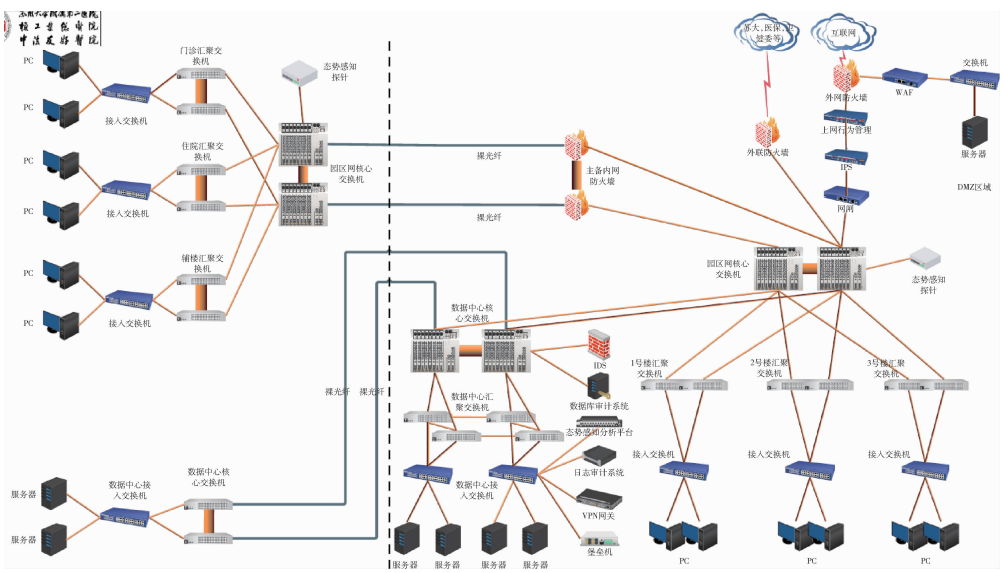

图 1 医院内网网络安全拓扑结构

4.1.2 安全通信网络区域 涉及医院内网网络安全拓扑结构中所有交换机和路由器设备，虚拟专用网络（Virtual Private Network，VPN）以及终端接入安全防护体系（准入、桌管）。核心层和汇聚皆由两台交换机 Switch 做双机双活冗余配置并进行负载均衡，实现高性能转发能力和较高网络稳定性[5]。数据中心利用 4 对万兆光纤链路将主备机房汇聚交换机进行连接，实现主备数据中心汇聚 4 框虚拟化，形成环形网络物理拓扑[6]。VPN 设备使用户可以安全地通过互联网访问内网服务。终端接入安全防护体系主要涉及终端安全防护技术，包括准入控制接入和桌管系统等，旨在避免非法终端接入内网以及提高终端自身安全性。

4.1.3 安全区域边界 分为互联网边界、专线边界[7]。具体设备涉及医院内网网络安全拓扑结构各防火墙，上网行为管理，入侵防御系统（Intrusion Prevention System，IPS），Web 应用防火墙（Web Application Firewall，WAF）等设备。在规划业务网络框架时，在互联网边界划分隔离区（Demilitarized Zone，DMZ）用于互联网应用业务。医院采用防火墙将互联网边界分割为 3 个区域：DMZ、内网区域和外网区域。内网区域是通往内网方向，后置上网行为管理、IPS、网闸等专用安全设备防护[8]。外网区域是互联网方向。在 DMZ 中将不涉及敏感数据的业务系统部署在该区前置机上。而重要敏感数据则在内网核心数据中心存储，以确保重要数据安全性。医院业务涉及医保单位以及各上级单位通信交互。在规划此类业务时主要通过独立防火墙划分出专线边界区域并在其中设置规范、严谨的安全策略将医保、银行等有业务交互的单位网络独立开。

4.1.4 安全管理中心 包括安全预警体系、审计追溯体系和安全防御体系[9]。内网安全预警体系涉及入侵检测系统（Intrusion Detection System，IDS）以及态势感知平台、杀毒预警平台、可视化统一网络管理运维平台等，实时监测预警，属于主动防御。内网审计追溯体系涉及数据库审计平台、日志审计平台等，旨在产生安全事件后对事件审计追溯，以便发现漏洞并完善加固。内网安全防御体系涉及杀毒系统等，在安全事件发生过程中处理其不良反应，阻止产生更大危害。

4.2 外网方案

4.2.1 概述 考虑到本次改造重点在于内外网物理隔离，因此在已有网络基础上，重新搭建一套新的承载网作为外网使用。

4.2.2 承载网 外网承载网采用物理 2 层结构，结构同内网类似，见图 2。承载网分为骨干层和接入层。骨干层采用开放式最短路径优先（Open Shortest Path First，OSPF）TCP/IP 3 层路由协议，自动生成并分发路由表项。

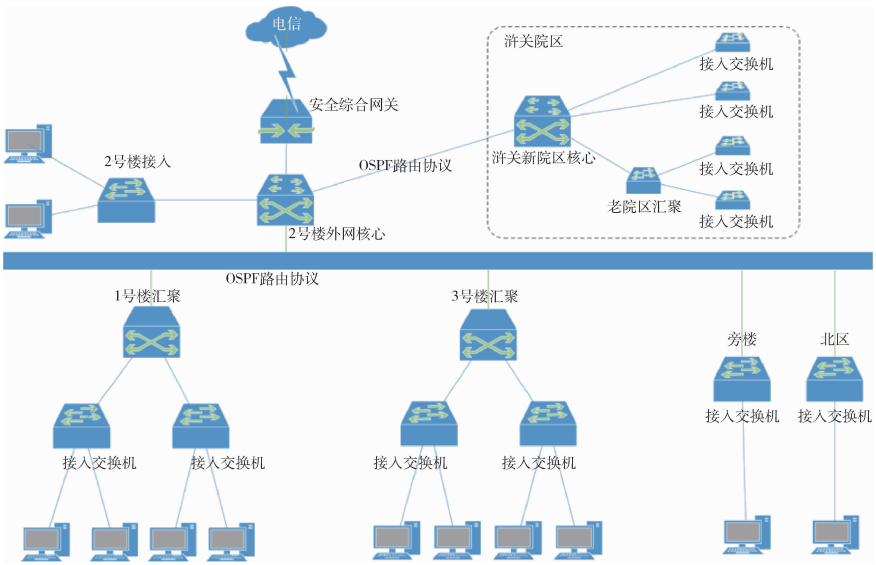

图 2 医院外网和外网安全拓扑结构

4.2.3 安全防护 互联网出口方面以防火墙作为出口安全网关，内联应用控制网关（Application Control Gateway，ACG）。ACG 对外网使用用户进行合法性认证。用户通过无线或有线方式连入外网后，利用手机号获取验证码，从而判断是否可以合法使用互联网。

5 优化改造方案实施

5.1 安全通信网络

5.1.1 承载网设备 网络设备实施时，骨干核心和汇聚皆采用 IRF 虚拟化技术保证设备多机冗余性。设备和物理线路高度冗余保证了网络稳定性和可靠性[10]。医院建立可视化统一网络运维管理平台，该平台能够实时监控网络设备运行情况并记录日志，能够定期对设备配置进行统一备份。

5.1.2 VPN 通过对通讯数据加密使会话能够在加密通道内进行，进而保障用户进行安全通讯而不被窃听。

5.1.3 终端接入安全防护体系 包括准入系统、桌管。主要对象是各类终端设备。医院内网终端和外网终端禁止交叉使用。管理部门需要通过技术手段禁止非法外联终端连入内网，同时禁止内网终端连入外网。本项目通过准入控制系统禁止外联终端连入内网。同时安装桌管系统客户端以保证内网电脑无法连入外网使用，开启禁外网功能。桌管系统还可以禁止终端使用移动硬盘、无线网卡等，有效预防内网终端中毒事件。

5.2 安全区域边界

5.2.1 防火墙 需按照一定要求升级到功能稳定的新版本。设备采用端口级别的安全策略对交互业务进行访问控制。通过业务访问权限最小化[11]对访问行为中的源目 IP 和端口、传输层协议进行严格过滤，阻断未经授权的数据流，有效防范互联网非法用户对医院业务的恶意访问、网络攻击。

5.2.2 ACG 网络框架设计中，在防火墙后端各部署 1 套独立 ACG，以管理监控和记录医院互联网访问行为。ACG 进行有效带宽分配以保证医院业务应用以及网络用户用网速率。

5.2.3 IPS 与 WAF 设备部署在互联网出口处。IPS 用以防范来自互联网、针对内网的木马蠕虫病毒、缓冲溢出攻击、穷举探测以及公共网关接口（Common Gateway Interface，CGI）攻击等入侵行为。WAF 部署在 DMZ 区域应用前置服务器前端，可以实时拦截应用层非法访问和攻击行为，例如中间件攻击、挂马行为、CMS 攻击以及分布式拒绝服务（Distributed Denial of Service，DDOS）等。

5.2.4 网闸 部署在交换机前端、IPS 后端。对通信进行完整采集、深层解析、应用重建，在网络间采用专有协议进行数据交换。同时本系统对网络通信的主体、客体进行综合认证，确保通信安全可靠，从而在保证内外网络相互隔离的基础上进行适度、可靠的数据交换。

5.3 安全管理中心

5.3.1 内网安全预警体系 包括态势感知平台、入侵检测平台、杀毒预警平台以及可视化网络管理运维平台[12]。态势感知以安全大数据为基础，从全局视角搭建综合网络安全运维平台，包括防御、监测、提前预知、事件处理以及事后日志记录等功能。态势感知平台包括感知探针和综合分析平台。医院采用 1 平台 3 探针的网络部署模式，3 个感知探针分别放置在主院区、分院区以及数据中心核心，实时抓取网络上的流量，通过特征库匹配得出基本流量分析日志并将日志发送至综合分析平台，形成可视化报告。入侵检测平台采用镜像模式，旁路部署在数据中心内部，对数据中心流量进行监控，严密监测数据中心是否被木马后门等攻击渗透。一旦发生渗透 IDS 立即推送告警信息至相关安全责任人。杀毒预警平台专职监控园区网和数据中心是否存在木马、勒索、蠕虫等网络病毒。如果出现网络病毒立即报警并通过与终端杀毒客户端联动方式联动杀毒。

5.3.2 内网审计追溯体系 包括日志审计系统、数据库审计系统等。网络和安全设备会将自身产生的操作日志、网络日志以及安全日志等发送至日志审计平台。日志审计系统对收集到的日志进行存

储、分析。通过对日志分析可以对事件进行追溯，帮助运维人员找到安全漏洞并弥补，杜绝未来发生同样类型的安全事件[13]。数据库审计系统通过镜像方式旁路部署在数据中心，通抓取进出数据中心的流量，分析、审计和记录业务人员对数据库的操作行为。当数据库发生异常情况时管理人员可以通过审计分析其操作过程，解决异常操作带来的问题。

5.3.3 安全防御体系 全院内网和外网终端都安装网络版杀毒软件。该软件客户端与杀毒预警平台联动，实时对终端计算机扫描杀毒[14]。

5.4 实施效果

经过改造医院整体网络安全防御体系更加完善。有效加强通讯、边界安全性。医院在此次优化改造过程中建立安全管理中心，具体包括安全预警体系、审计追溯体系、安全防御体系。医院网络安全从被动防御转为主动防御阶段，较大程度提高安全事件预警和应对能力。优化后的网络架构达到等保 2.0 技术要求，加强系统安全和集中管控能力。通过对出口策略进行端口级别控制大幅提高内外网数据交互安全性。

6 结语

医院通过内外网物理隔离手段提高自身网络安全防护能力[15]。本文主要阐述医院内外网隔离的技术要点、方案设计以及具体实施。此次改造已实施完毕，但仍存在改进空间。互联网出口和专线出口仍然存在单点故障问题。在未来安全改造过程中可以通过增加设备和线路方式解决该问题，提高互联网出口、专线出口稳定性和可靠性。医院需要根据安全等保各方面技术要求建设完善的网络安全架构，保证医院各业务系统安全稳定运行。

参考文献

1 杨旋，周小甲．医院信息系统安全等级保护定级与整改结果探讨［J］．中国医疗设备，2017，32（6）：166－169.

2 开拓．基于网络安全视角的医院网络管理研究［J］．网络空间安全，2016，7（8）：21－23.

3 王玉珍，李洪威，武旭红．医院网络及数据中心升级改造研究［J］．中国医疗设备，2018，33（9）：141－143，157.

4 陈拥军，肖新文，陈泓伶，等．医院网络安全体系构建与实现［J］．中国数字医学，2016，11（7）：105－107.

5 吴长安，胡延林，任明．双核心、全路由 3 层网络架构的医院网络系统改造［J］．医学信息学杂志，2014，35（10）：27－29.

6 刘海林．基于三层架构的医院网络改造与实施方案［J］．中国医学教育技术，2012，26（4）：451－454.

7 严比卓．大型综合医院数据中心机房设计与建设研究［J］．电脑与信息技术，2017（3）：43－46.

8 刘鑫，张锦．编码在医用耗材管理中的作用［J］．中国医疗设备，2016，31（6）：134－136.

9 黄成兵．计算机网络安全与防御分析［J］．福建电脑，2011，27（6）：39－40.

10 王波．基于等级保护的医院信息网络平台安全体系设计与实现［J］．医学信息学杂志，2014，35（7）：30－32.

11 汤斌，黄玉成．三级等保下医院信息系统安全优化方案实践［J］．中国医疗设备，2018，33（9）：136－140.

12 梁子炘．试论基于网络安全视角的医院网络管理方略［J］．科技创新与应用，2017（11）：86.

13 韩作为．医院信息安全等级保护三级建设流程与要点［J］．中国数字医学，2013，8（9）：33－35.

14 张伟丽．信息安全等级保护现状浅析［J］．信息安全与技术，2014（9）：9－13.

15 朱贤斌，常乐．基于等级保护基本要求的网站群安全体系研究［J］．信息技术与信息化，2015（9）：107－108.