***医院
网络安全等级保护解决方案

2020 年 03 月

目 录

一、 项目概述

1.1、项目背景

2016 年 4 月 19 日，总书记在北京主持召开网络安全和信息化工作座谈会并发表重要讲话，并明确指出：“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。”

2017 年 6 月 1 日，我国的网络安全法正式实施。《网络安全法》第二十一条规定，网络运营者的网络安全等级保护义务：网络运营者有义务制定内部安全管理制度和操作规程、确定网络安全负责人；并应当采取防范病毒、攻击、入侵等危害网络安全行为的技术措施；网络运营者的日志留存时间必须不少于 6 个月；并有义务采取数据分类、重要数据备份和加密等措施。《网络安全法》规定对于网络运营者拒不履行安全的责任，明确处罚措施，包括暂停业务活动、严重的违法行为将导致停业整顿或吊销执照、处罚金额最高可至 100 万元、对于直接负责人进行罚款等。构成犯罪的会依法追究刑事责任。

医院是一个信息和技术密集型的行业，其计算机网络是一个完善的办公网络系统，作为一个现代化的医疗机构网络,除了要满足高效的内部自动化办公需求以外,还应对外界的通讯保证畅通。结合医院复杂的 HIS、RIS、PACS 等应用系统，要求网络必须能够满足数据、语音、图像等综合业务的传输要求，所以在这样的网络上应运用多种高性能设备和先进技术来保证系统的正常运作和稳定的效率。同时医院的网络系统连接着 Internet、医保网和卫生局等，访问人员比较复杂，所以如何保证医院网络系统中的数据安全问题尤为重要。

在医院行业的信息化建设过程中，信息安全的建设虽然只是一个很小的部分，但其重要性不容忽视。便捷、开放的网络环境，是医院信息化建设的基础，在数据传递和共享的过程当中，数据的安全性要切实地得到保障，才能保障医院信息化业务的正常运行。然而，我们的数据却面临着越来越多的安全风险，时刻对业务的正常运行带来威胁。

为此， 2011 年 12 月，卫生部发布《卫生部办公厅关于全面开展卫生行业信息安全等级保护工作的通知》，要求卫生行业“全面开展信息安全等级保护工作”，

《中华人民共和国网络安全法》（以下简称《网络安全法》）自2017年6月1日开始施行。其中，《网络安全法》第21条明确规定了“国家实行网络安全等级保护制度”。《网络安全法》是从国家层面对等级保护工作的法律认可，简单点就是单位不做等级保护工作就是违法。医院信息系统的安全性直接关系到医院医疗工作的正常运行，一旦网络瘫痪或数据丢失，将会给医院和病人带来巨大的灾难和难以弥补的损失。同时，医院信息系统涉及大量医院经营和患者医疗等私密信息，信息的泄露和传播将会给医院、社会和患者带来安全风险。

所以在***医院的信息化建设过程中，我们应当正视可能面临的各种安全风险，对网络威胁给予充分的重视。为了***医院信息网络的安全稳定运行，确保信息系统安全，根据***医院目前的计算机信息网网络特点及安全需求，本着切合实际、保护投资、着眼未来的原则，提出本技术方案。

1.2、建设依据

1.2.1、 国家相关政策文件

1)《中华人民共和国网络安全法》

2)《中华人民共和国计算机信息系统安全保护条例》（国务院令 147 号）

3)《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）

4)《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）

5)《信息安全等级保护管理办法》（公通字[2007]43 号）

6)《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号）

7)《信息安全等级保护备案实施细则》（公信安[2007]1360 号）

8)《公安机关信息安全等级保护检查工作规范》（公信安[2008]736 号）

9)《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）

10)《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）

11)《关于加快推进国家电子政务外网安全等级保护工作的通知》(政务外网[2011]15 号)

12)《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发[2016]55 号）

13）卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知卫办发[2011]85 号

14）卫生部办公厅《关于全面开展卫生行业信息安全等级保护工作》的通知卫办综函[2011]1126 号

1.2.2、 相关标准及规范

1)《计算机信息系统安全等级保护划分准则》（GB 17859-1999）

2)《信息安全技术 信息系统物理安全技术要求》（GB/T 21052-2007）

3)《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）

4)《信息安全技术 网络基础安全技术要求》（GB/T 20270-2006）

5)《信息安全技术 信息系统安全通用技术要求》（GB/T 20271-2006）

6)《信息安全技术 信息系统安全等级保护体系框架》（GA/T 708-2007）

7)《信息安全技术 信息系统安全等级保护基本模型》（GA/T 709-2007）

8)《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）

9)《信息安全技术 信息安全风险评估实施指南》（GB/T 31509-2015）

10)《信息技术 安全技术 信息安全风险管理》（GB/T 31722-2015）

11)《信息安全技术 信息安全风险处理实施指南》（GB/T 33132-2016）

12)《信息安全技术 信息系统安全等级保护定级指南》（GB/T 22240-2008）

13)《信息安全技术 信息系统安全等级保护实施指南》（GB/T 25058-2010）

14)《信息技术 安全技术 信息安全管理体系 要求》（GB/T 22080-2016）

15)《数据中心设计规范》（GB 50174-2017）

16)《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）

17)《信息安全技术 网络安全等级保护测试评估技术指南》(GB/T 36627-2018)

18)《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018）

19)《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

20)《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

21)《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

22)《信息安全管理体系要求》（ISO/IEC 27001-2013）、

1.2.3、 行业标准

卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知卫办发[2011]85 号

卫生部办公厅《关于全面开展卫生行业信息安全等级保护工作》的通知卫办综函[2011]1126 号

国家卫健委《国家健康医疗大数据标准、安全和服务管理办法（试行）》

国家卫健委《互联网医院管理办法（试行）》

国家卫健委《互联网诊疗管理办法（试行）》

国家卫健委《远程医疗服务管理规范（试行）》

1.3、建设目标

依照《卫生部办公厅关于全面开展卫生行业信息安全等级保护工作的通知》、《中华人民共和国网络安全法》《网络安全等级保护基本要求》等标准，以及医院对信息系统等级保护工作的有关规定和要求，对医院的网络和信息系统进行等级保护定级，通过实现基于安全策略模型和标记的强制访问控制以及增强系统的审计机制，使得系统具有在统一安全策略管控下，保护敏感资源的能力。

通过技术体系和管理体系建设，使得医院网络系统的等级保护建设既可以满足等级保护的相关要求，又能够全方面为医院的业务系统提供持续的安全保护。

本项目建设将完成以下目标：

1、建立完善的安全技术防护体系。根据网络安全等级保护的要求，建立满足等级保护要求的安全技术防护体系，在满足安全合规基础上实现医院网络安全持续保护。

2、建立符合医院实际的安全管理组织机构，健全信息系统安全管理制度。根据网络安全等级保护的要求，制定各项信息系统安全管理制度，对安全管理人员或操作人员执行的重要管理操作建立操作规程和执行记录文档。

3、制定医院网络安全应急预案。应急预案是网络安全等级保护的重要组成部分，按可能出现问题的不同情形制定相应的应急措施，在系统出现故障和意外且无法短时间恢复的情况下能确保生产活动持续进行。

4、安全培训：为医院信息化技术人员提供信息安全相关专业技术知识培训和全员安全意识培训。

5、完善医院整体安全规划，建立服务+技术+管理的整体安全体系，让医院安全规划更全面，安全更持续有效。

二、 现状分析

2.1、现状描述

***医院是一个星型的快速以太交换网，内网核心为一台三层交换机，下接接入交换机，无其他安全防护措施，主要安全设备为去年采购的两台防火墙。

如上拓扑所示，现状问题描述如下：

1、没有明显的安全域划分，一旦爆发病毒（如勒索病毒）将很快传染扩算，另外一旦内网某台主机被黑客控制，很容易进行横向攻击。

2、除服务器区域外，内网攻击行为无法监控处理，一旦出问题导致无法访问，数据丢失。

3、单位办公网没有做终端准入认证，内部没有做安全区域隔离划分，容易被利用攻击；

4、无日志审计设备，尤其是 WEB 服务器没有外置日志存储中心，一旦服务器被攻击控制后被不法份子清除日志内容，会导致安全事件难以定位。

5、数据安全层面建设薄弱，没有数据库审计设备，缺乏特权账号管控、数据防泄漏、数据脱敏加密等安全产品；

6、主机安全层面缺乏漏洞扫描系统，缺乏通过风险评估发现了漏洞以及高危漏洞。

7、无集中的安全运维管理平台，导致安全事件无法集中管理、运维。

除以上几点外还存在以下安全风险：

1、全网安全不可视：缺乏有效的可视化手段，过去主要简单边界防火墙隔离的方式进行安全防御，内部的都是安全的，外部的都是不安全的，但由于移动化、虚拟化、互联网化的下的 IT 趋势的发展，安全边界变得模糊了，好的坏的混在一起，只有通过可视化的手段，看见威胁和风险才能实现安全保护；

2、全局安全事件难定位：一旦出现了安全事故，总部的运维人员由于缺乏基础数据和日志难以对安全事件进行定位，到底是哪个分支机构还是总部哪个业务系统被攻击了。

3、更高级的威胁：总有一些攻击手段可以绕过现有的基于静态特征的防御体系，如 0Day 攻击、APT 攻击等可能导致基于静态特征的防御失效；

4、内网的潜藏威胁：黑客一旦进入到内网，位于边界的防御体系就失效了，如通过社会工程学、钓鱼等欺骗手段进入到了内部，位于边界的防御便失效了；

5、内网的横向攻击：发生在内部的横向移动攻击边界防御无法进行检测，如通过失陷主机向内网业务资产发起的横向移动或者跳板攻击。

6、缺乏对业务与应用的可视化：过往安全设备的保护对象大多是 IT 设备与资产，缺乏对关键业务、关键数据的安全保护。更难以捕捉洞察对关键应用、关键数据的攻击行为。

7、重防护，轻检测、响应、加固：传统的安全解决方案以拼凑防御产品为目的，重防御、轻检测，事后审计、追责收效甚微，难以满足安全保障的实际需求。

8、重产品，轻服务，难以适应动态发展的攻防安全形势：简陋的安全告警和报表，使得安全运维管理人员陷于海量的攻击日志中，工作量巨大且容易忽略重要安全事件。安全运维人员缺乏安全专业咨询与支持服务支撑其日常的“预防，检测，响应，加固”活动，使得在出现突发安全事件时后知后觉，安全攻击窗口期过长，出现安全事件后疲于应付。

基于上述风险，***医院极需加强内外部的持续检测来发现这些新的安全问题，并基于可视化的平台将这些潜在的问题进行展现，以便于对可能发生或者已经发生的安全事件进行快速的响应。从技术、管理、运维多个角度，平衡防护、检测、响应的投资，建设立体化的安全框架。

2.2、 问题分析

1、信息技术体系需要进一步完善。虽然***医院出口部署了下一代防火，但难以满足当前复杂的安全形势。单位将进行现有安全体系的升级建设，从单纯被动防御层次向“持续检测、快速响应”迈进，打造一站式的“预测，防御，检测，响应，加固”的五位一体服务，真正做到“安全防御可见效、安全态势可感知、安全威胁可预警、异常行为可监控、安全价值可呈现”的安全建设效果。

2、信息安全管理制度急待梳理完善。由于管理模式、环境要求等方面的不同，引用的制度还不能完全满足建立等保、ISO27001 等成熟体系的要求。并且各项制度也还未达到合适的推行力度，仍存在基层技术人员对制度不知情的情况。同时各业务部门往往还拥有自己的内部制度，在执行时可能与单位制度造成优先级或内容上的实质性冲突，因此需要对制度进行全面梳理，建立文件化的管理体系，力争每位职员日常工作中遵循唯一的标准，使制度的执行和考核能落实下去。

3、信息安全管理工作尚未落实到基层。单位现有信息安全管理组织主要是信息安全领导组和信息化部门，但是没有明确指定开展信息安全各项具体工作的执行层面的人员，同时也未按照国际成熟标准和业界惯例把三类互相制衡、互相配合的人员职能（信息安全技术、信息安全管理、信息安全审计）落实到相关部门人员，最终导致单位领导虽然高度重视信息安全工作，但是具体工作却难以深入开展下去。

4、单位骨干运维人员尚未掌握信息资产、风险管理的理念。在之前开展安全评估活动过程中，发现目前的员工包括骨干岗位人员普遍缺乏对威胁、弱点等基础理论知识的正确认识，对国内外成熟标准和最佳实践不了解，在日常工作中主动用风险管理指导自己也不了解。因此建立真正可持续改进、以风险管理理念为出发点的信息安全管理体系仍任重而道远。

5、流程尚未实现规范化。本次认证范围内的各部门均拥有各自的信息系统和重要数据或信息资产，但从国内外信息安全最佳实践的角度来看，所依据的制度流程也是少量信息技术部的 IT 类管理制度，操作记录层面居多，缺少提炼为可优化可重复的管理制度，也尚未提升到目前业界推崇的“流程建设”的高度。服务质量仍主要依赖于技术人员和管理人员的自身经验，而缺少具有继承性的操作规范，在为客户提供持续的、稳定的高质量方面存在相当大的风险。

6、对内部第三方的管理仍需要加强。对于外部第三方这三类人员，还未出台针对此类人员具体工作内容的信息安全管理制度细则，也没有在第三方职责和合同中对信息安全责任进行进一步的明确界定，对此类人员的信息安全管理全部依赖接口人员的个人意识和能力，缺乏统一的管理标准。

7、信息安全内外部审计检查机制尚未形成。单位尚未建立信息安全内外部审计检查机制，信息安全审计审核工作也未开展。需要把内部审计检查与外部审

计检查结合起来，建立内外部审计检查制度，落实相关组织建设和人员责任，参照国际成熟标准和业界最佳实践，定期组织内外部审计检查活动，确保信息安全建设覆盖各个领域。

2.3、新形势下的安全挑战

2.3.1、 “黑灰产”产业化趋势明显

从中国网络安全漏洞的数据来看，2016 年漏洞数量有 10822 个，这个趋势图一直往上涨。这些只是通用基础漏洞，还有业务漏洞以及逻辑设计上的漏洞。在中国大陆从事黑灰产人员在 100 万到 200 万之间，有一条数据获取、洗钱担保的完整地下利益链条。黑灰产业相互依附，形成了各种各样的产业链，其中如恶意注册、虚假认证、虚假交易等部分黑灰产业甚至已经发展成了“一条龙服务”，从前期骗取农村、工厂等人口的身份信息，到后期网络交易平台虚假认证和虚假交易的整个过程，都有跨境跨地区的专人或公司负责。

2.3.2、 黑客攻击手段更加智能、复杂

从上个世纪九十时代到现在，黑客的攻击手段在发生重要变化，总体上呈现更加智能化、复杂化的趋势。

图 2.1 黑客攻击手法向智能化、复杂化转变

从攻击目的来看，从最初的黑客炫耀、破坏、窃取数据，转向以牟利为主的黑灰产产业化运作为主，如僵尸网络、挖矿程序、用户数据窃取等；从攻击技术手段来看，在最开始的僵木蠕、漏洞利用、口令入侵为主，演变成更加复杂的攻击方式，例如 APT 攻击、社会工程学、水坑攻击等；从攻击层面来看，从最初的网络层攻击如 DDOS、身份冒仿、数据窃取方式，向应用层的攻击如应用层漏洞利用、SQL 注入、XSS 攻击等演进。

2.3.3、 勒索病毒，未知恶意代码具备较强的破坏能力

勒索病毒也在不停的创新，邮件钓鱼、口令传播、最新漏洞蠕虫传播、MBR篡改等无所不用其极，此外勒索病毒也利用 Exploit Kit 等黑色产业链进行攻击。

2017 年 5 月 12 日开始，在全球蔓延的 WannaCry 勒索病毒已经席卷了至少150个国家的20万台电脑。病毒要求用户在被感染后的三天内交纳相当于300美元的比特币，三天后“赎金”将翻倍。七天内不缴纳赎金的电脑数据将被全部删除。2019 年 3 月，勒索病毒再一次席卷国内医疗行业，尤其是***，多达几十家医院遭受感染，部分医院业务无法开展，病人看病无法正常进行，造成了不小的经济损失以及极其恶劣的社会影响。

另外，当前防病毒软件或硬件网关，基本上以依靠病毒特征库为主，而针对经过变种的病毒、木马或者未知恶意代码，不具备监测能力。从而，未知恶意代码能够都计算机系统或网络设备带来很大的危害。

2.3.4、 内鬼隐藏较深，难以发现

与新闻媒体大规模宣传、大家耳熟能详的外部黑客攻击相比，内部作案才是信息安全事件的主要来源，更是各种信息安全事件的重灾区。因此美军的IATF(信息保障技术框架)中早就把内部威胁和第三方威胁(有各种合作关系的组织或者个人)当作是信息安全威胁的重要来源。

总之，新形势下，***医院面临更加严峻的信息安全挑战。

三、 需求分析

经过前期调研，依据***医院对安全保障工作的要求，需要强化网络信息安全服务保障，建设数据中心、办公网、及业务平台安全防护体系，加强大数据安全保障。***医院信息安全防护体系建设的总体安全需求汇总如下：

一是强化网络安全保障体系建设。健全安全体系，建立安全管控制度，形成“三员”（系统管理员、安全保密管理员、安全审计员）分立机制；推进***医院信息安全技术体系建设，完善安全事件快速响应和处置手段；建成感知、处置、响应一体化的安全运营机制，加强事前预防、事中审计、事后响应的安全应急服务能力，形成发现、阻断、取证、溯源、研判、拓展的安全业务闭环；开展安全组织与职责建设、安全技术设计、安全管理设计，确定第三方机构，统一实施网络安全等级防护和风险评估。

二是建设业务平台安全防护体系。建设网络安全接入管控系统，提供面内部用户、合作伙伴、运维人员的强身份认证、用户管理和访问控制服务；强化数据中心网、办公网、以及互联网各网络区域的安全防护；构建云计算虚拟化平台安全保障系统，实时监测识别恶意代码、安全漏洞、非授权访问等安全风险，提供隔离、防护、监测及审计服务。

三是加强以数据安全为核心的安全保障体系。加强数据中心边界安全防护，建立统一的平台认证与身份管理机制；实施平台级访问控制和授权管理，实现细粒度的访问控制；建设操作审计系统，形成集中审计报告；强化大数据安全防护及隐私保护，实现高效可靠的数据防泄露。

3.1、安全物理环境需求

目前整体系统内的多有服务器、网络设备、UPS 等设备均在一个区域，需要做到区域与区域间的物理隔离或者交付过度机制；对于现有机房监控报警系统，需要配备相应的电子门禁系统与相应的人员进出登记管理机制；在防火，防雷，防电，防水，防潮，电力供应和电磁防护上需要进行进一步的建设与检测报警机制，对于现有机房需要进一步升级以满足等级保护需求。

3.2、安全计算环境需求

目前整体网络计算环境存在诸多问题，需要进行相应的安全改造，就目前调研来看，现有网络存在操作系统管理、身份鉴别机制不完善，核心业务或者数据库存在多人共同维护，并且为定期生成相应的审计报表和保存措施，对于服务器入侵防范能力不足，存在安全漏洞，对于服务器的资源控制也需要进一步加强，种种问题还需进一步解决和完善。

3.3、安全通信网络需求

目前整网的主要安全防护设备为防火墙以保障数据的完整性，保密性。存在一定的安全隐患，基于现有情况。需尽快解决系统之间安全隔离，重要网段访问控制，远程设备合理限制，网络日志安全审计，身份识别认证方式多样，网络数据传输明文传输等问题，一次达到整体网络体系的安全。

3.4、安全区域边界需求

在边界安全建设中相对于其他区域比较完整，但是也存在着一些问题，对于边界的安全审计，边界访问控制，边界访问控制，边界完整性检查，边界入侵防范都需要进一步加强，以此保障各区域的安全防护效果。

3.5、安全管理中心需求

对于现有网络，管理体系相对薄弱，需进一步加强，基于用户身份基于分工不同，权限不同的统一管理，基于资源配置（包括数据库日志空间，数据库空间，服务器内存，磁盘使用情况等等）的统一监控，基于系统运行状态数据备份恢复，恶意代码防范，系统补丁管理等等统一运维管理。

通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括：根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等；对安全审计员进行严格的身份鉴别，并只允许其通过特定的命令或界面进行安全审计操作。

3.6、安全管理体系需求

安全体系管理层面设计主要是依据《信息系统安全等级保护基本要求》中的管理要求而设计。对于***医院目前的安全管理制度需考虑一下一些问题：

安全管理制度

根据安全管理制度的基本要求制定各类管理规定、管理办法和暂行规定。制定相应的信息安全管理制度，加强《密码管理制度》与《变更管理制度》，拟定细节性的安全管理制度，相应安全策略，安全检查和审定。

安全管理机构

根据基本要求设置安全管理机构的组织形式和运作方式，明确岗位职责；对于关键岗位需安排多人共同管理，基于现有业务重要程度，需聘请安全顾问定期知道安全建设思路，并且定期进行安全检查与审核。

人员安全管理

根据基本要求制定人员录用，离岗、考核、培训几个方面的规定，并严格执行；规定外部人员访问流程，并严格执行，定期开展安全意识培训等。

系统建设管理

根据基本要求制定系统建设管理制度，包括：系统定级、安全方案设计、产品采购和使用、外包软件开发、工程实施、测试验收、系统交付、安全服务商选择等方面。从工程实施的前、中、后三个方面，从初始定级设计到验收评测完整的工程周期角度进行系统建设管理。

系统运维管理

根据基本要求进行信息系统日常运行维护管理，利用管理制度以及安全管理中心进行，包括：环境管理、资产管理、介质管理、设备管理、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等，使系统始终处于相应等级安全状态中。

四、 建设目标

***医院整体安全规划项目也应满足其要求，全面实现一体化安全保障体系，深入结合先的 IT 基础设施、业务系统、网络运行平台的外部安全保障与内部环境的安全保障需求，基于云计算、大数据、互联网+等特点、系统软件特点、应用特点和数据特点，全面推进整体安全保障体系的构建、系统平台优化、分层纵深设计和安全运营能力提升，形成“技术可落地、管理可执行、平台可扩展、安全可运营”的安全保障体系规划。以总体安全策略为核心，明确信息安全工作的目标、原则和规范；以信息安全管理体系、信息安全技术体系、信息安全运维体系和安全管理中心为支撑，通过各种安全控制措施落实安全策略，进一步实现在区域边界、计算环境和通信网络的安全防护；使网络与信息系统在物理安全、网络安全、主机安全、应用安全、数据安全、管理安全各个层面不仅达到国家信息安全相关标准要求，且最终实现“看得见、用得好、管得住”的安全目标。

贯彻以人为本的管理理念，引进国际先进的安全管理的技术体系、管理标准，补充和完善所需的设备和系统，以 ISO27001、等保三级为建设基准，构筑立体化、纵深、可追溯的网络安全预警防控系统，形成安全、合规、全面、稳定、高效网络安全纵深防御体系，充分发挥和全面提升存量系统的作用，夯实网络安全的基本防线。

五、 建设方案

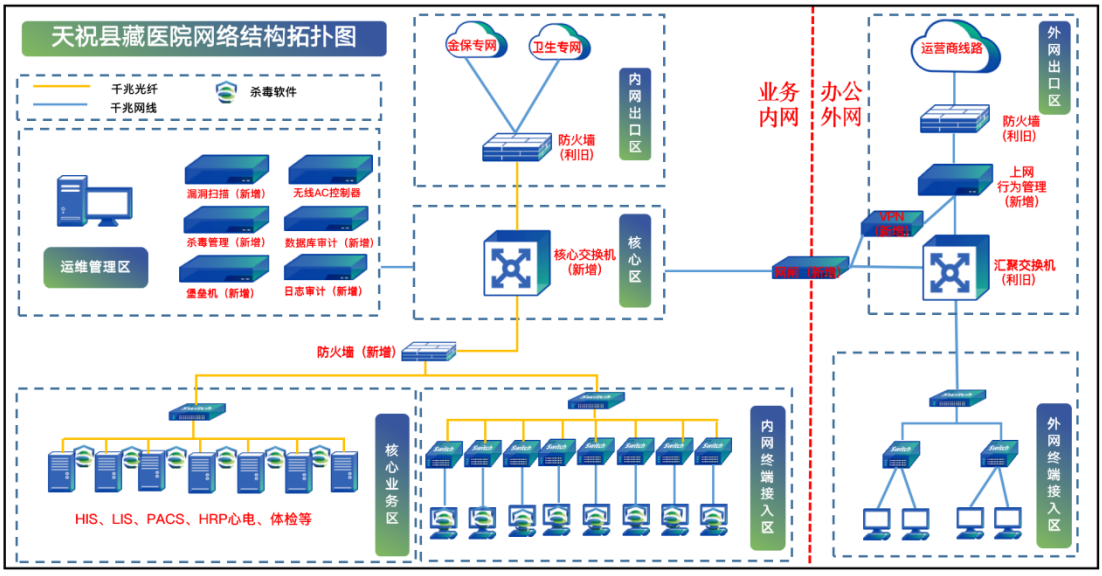
5.1、 构建以全局安全可视为核心的安全治理能力

在网络安全的世界里，可视化有着不可忽视的作用，安全的可视化能够保证对信息资产、人、行为三者之间的风险点进行实时观测，在发生威胁时能够果断进行安全处置，有效防止了安全威胁的渗透。

“***医院整体安全规划项目”在流量可视、行为可视的基础上，可实现全局安全可视化，可以结合攻击趋势、有效攻击、业务资产脆弱性对全网安全态势进行整体评价，以业务系统的视角进行呈现，可有效的把握整体安全态势进行安全决策分析。

在全局安全可视的基础上，基于人工智能、大数据技术能够显著提升安全运维能力，通过失陷主机检测和访问关系可视等技术帮助运维人员快速发现安全风险，并提供处理建议，简化运维。进一步可以在客户侧建立起深度分析、威胁检测、防御联动和服务响应的安全运营中心。

*****医院网络改造拓扑：**



5.2、 详细方案设计安全技术体系

5.2.1、 整体安全环境设计

安全域划分

安全域是指同一系统内根据信息的性质、使用主体、安全目标和策略等元素的不同来划分的不同逻辑子网或网络，每一个逻辑区域有相同的安全保护需求，具有相同的安全访问控制和边界控制策略，区域间具有相互信任关系，而且相同的网络安全域共享同样的安全策略。一个安全域内可进一步被划分为安全子域，安全子域也可继续依次细化。根据***医院业务访问的需要，结合定级对象分等级保护的思想，将***医院整体网络分为内外网出口区、运维管理区、核心业务区、内外网终端接入区等。

安全防护设计

***医院全网安全防护设计方案将严格按照区域功能的重要性和网络使用的逻辑特性划分安全域，并基于安全域之间的边界隔离及访问控制要求，各安全域出口推荐部署下一代防火墙进行 2-7 层访问控制。各安全域需求及解决方案如下：

网络出口区：该区域说明如下：需在互联网出口边界利旧使用下一代防火墙进行隔离和访问控制，保护内部网络，从 2-7 层对攻击进行防护，实现对入侵事件的监控、阻断，保护整体网络各个安全域免受外网常见恶意攻击，利用网络防病毒，主动扫描 web 和电子邮件流量、阻止恶意软件到达并感染网络上主机等防护功能。

核心业务区：通过部署下一代防火墙（增强级），实现基于应用层的边界隔离与访问控制，通过可视化展示基于事前风险发现，系统漏洞检测，基于人工智能引擎基于事中安全防护，有效防止未知威胁、勒索病毒、挖矿病毒等攻击，基于事后的联动响应联动原有终端检测与响应设备，实现网端一体的有效联动防御体系实时保障网端边界及终端安全。

运维管理区域：（使用使用日志审计系统，堡垒主机，漏洞扫描系统，数据库审计等）。日志审计系统、数据库审计等安全设备的部署实现设备和计算的安全审计，同时对主机系统、安全设备、交换机等根据需求开启设备自身审计功能，审计设备连接至政法委 NTP 服务器保证了审计记录产生时的时间由系统范围内唯一确定的时钟产生，以确保审计分析的正确性。对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计日志保存 6 个月以上，应对审计进程进行保护，防止未经授权的中断。审核员帐号（角色）与系统管理员帐号（角色）应独立分开，且互相制约，并通过设备或相关措施对审计进程进行保护，防止未经授权的中断。

日志审计设备通过旁路镜像模式一体式部署，实现网络内各设备的安全信息采集及分析，分析的安全告警信息在首页进行统一集中展示，主要采集设备包括系统满足设备的信息采集要求，主要包含各类主机、安全设备、网络设备、数据库、中间件等主流设备，无需安装任何代理支持 Syslog、Syslog-ng、SNMPTrap、文件、WMI、SFTP、数据库等方式采集日志，并且日志采集器可实时或按设定的时间将指定的日志送到审计中心；

对于用户管理侧，可实现根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理，通过可视化列表的方式展示告警、告警声音设置、告警过滤策略，通过 GUI 设置告警策略，具备丰富关联/审计类告警策略，并可以灵活自定义策略。

数据库审计设备通过镜像、软件探针等多种部署方式，对数据库进行多因子精准审计，可准确评估数据库所面临的风险，并可以通过日志记录提供事后追查机制，可有效保障数据库访问安全。

审计内容全面，可实现单双向审计、绑定变量审计、删改留痕审计、三层、四层审计，能最大程度审计到各种访问源头对数据库的访问内容，并可基于精准的策略规则进行报警；可实现支持主流数据库：ORACLE、MYSQL、MSSQL、SYBASE、DB2、达梦 7、达梦 6、人大金仓、神州通用、INFORMIX、PostgreSQL、Gbase、Hive、MongoDB、Redis、TereData、Kafka、Cache、ES、HANA；达梦、人大金仓、神州通用、南大通用；

通过授予不同管理员权限，进行分工，（1）安全管理员（负责配置规则，无查看日志权限)；（2）系统管理员（负责系统配置，包括授权、时间配置、接口配置、升级配置、用户安全、服务配置、日志配置、报表配置、告警配置、备份还原配置、系统监控等，无查看日志权限）；（3）审计管理员（负责查看审计日志；并可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能；仅有日志查看权限）；通过可视化维度直观报表展示现有数据库整体安全状况。

漏洞扫描设备通过旁路模式部署，通过安全基线管理、变更基线管理，漏洞问题管理、WEB 漏扫、等方式实现全面集中检查及分析各类系统本地安全配置问题，实现监控计算机文件、端口、系统、进程等变化信息，发现系统异常；通过全面集中化扫描和用户各类信息系统分析以及设备存在的安全漏洞，尤其是通

过深度探测端口与服务扫描网站站点信息遍历整个 WEB 框架目录结构，自动分析实现 WEB 漏洞扫描，提供全面详尽的报告管理，实现整网业务系统的全面，详尽的业务风险评估。