行业概况

- 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。结合医院关键系统HIS系统（医院管理信息系统）、LIS系统（实验室管理系统）、CIS系统（临床信息系统）、PACS/RIS系统（影响存储和通信管理系统）等业务系统，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省医保、市医保、新农合以及区域卫生平台等，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。在日新月异的现代化社会进程中，计算机网络几乎延伸到了世界每一个角落，它不停的改变着我们的工作生活方式和思维方式，但是，计算机信息网络安全的脆弱性和易受攻击性是不容忽视的。由于网络设备、计算机操作系统、网络协议等安全技术上的漏洞和管理体制上的不严密，都会使计算机网络受到威胁。我们可以想象一下，对于一个需要高速信息传达的现代化医院，如果遭到致命攻击，会给社会造成多大的影响。

- 为此，国家公安部、保密局、国家密码管理局、国务院信息化领导小组办公室于2007年联合颁布了861号文件《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》和《信息安全等级保护管理办法》。国家卫生部也在2011年11月发布85号文《卫生行业信息安全等级保护工作的指导意见》，要求涉及国计民生的信息系统应达到一定的安全等级。

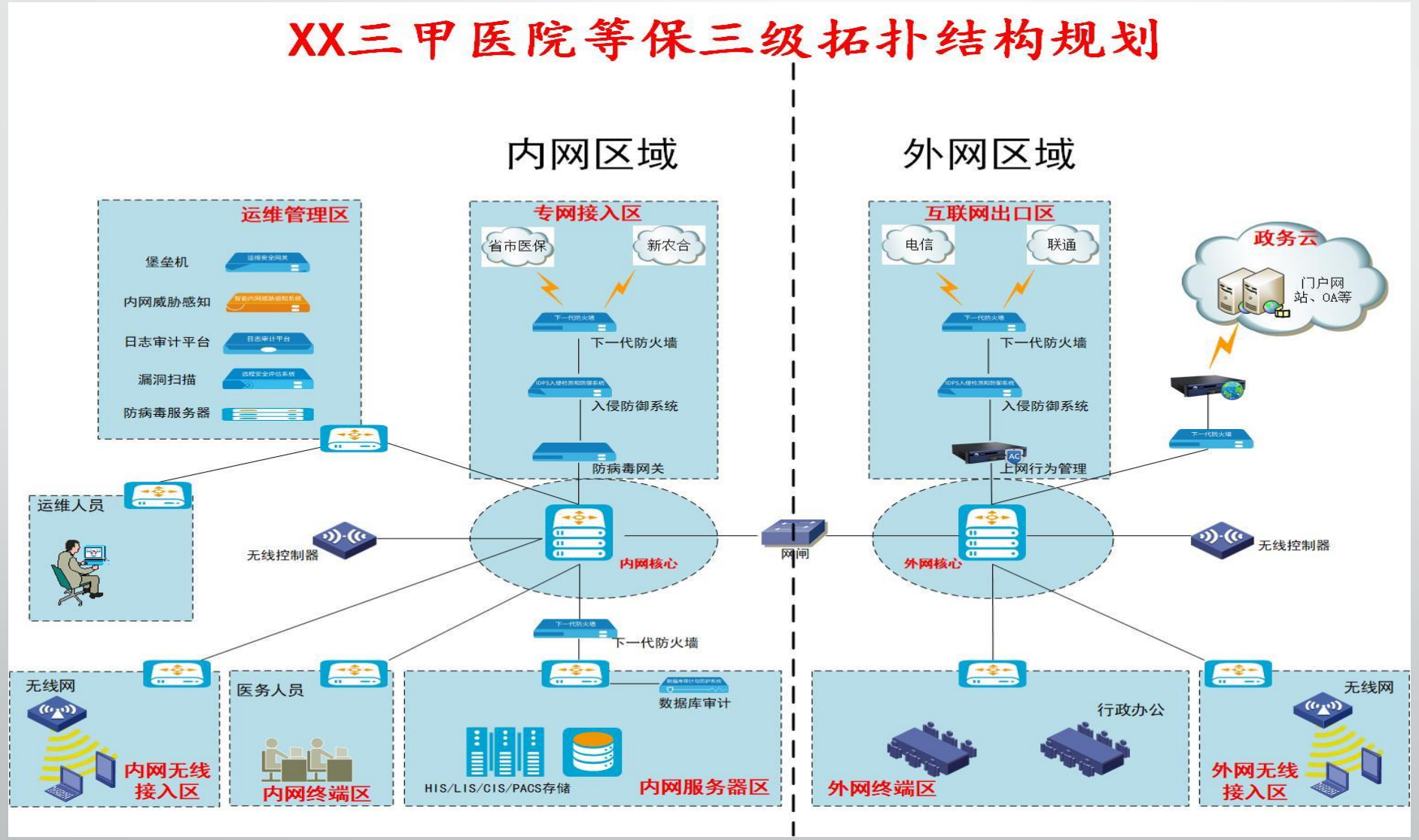
- 2016年，国家卫健委发布《2016 三级综合医院评审标准考评办法 (完整版)》规定了重要业务系统必须达到等保三级标准才满足三级医院评审标准中对于网络安全的要求。

2018年，国家卫健委发布《互联网医院管理办法(试行)》规定了承载互联网医院的平台必须通过等保三级测评。

XX医院安全风险及建设目标

- 防范来自互联网的威胁
- 防范外网与内网数据交互带来的威胁
- 移动办公数据传输的保护
- 保障互联网诊疗业务的开展
- 防范来自外联单位的访问行为
- 防范内网感染主机对核心业务系统的破坏
- 针对核心业务数据访问的防护和审计
- 满足政策合规性要求
- 本方案的建设目标是在国家信息系统安全等级保护相关政策和标准的指导下，结合XX医院信息系统的安全需求分析，确定XX医院信息系统安全等级保护的级别，对信息系统进行差距分析并提出整改建议，对XX医院信息系统进行安全整改，达到国家信息安全等级保护相关标准的要求，并通过信息系统等级测评，更好地保障XX医院各业务系统的正常运行，全面提升XX医院信息系统的安全保护水平，并顺利的通过三级等级保护。

解决方案


XX三甲医院等保三级拓扑结构规划
内网区域
外网区域
运维管理区
堡垒机
内网威胁感知
日志审计平台
漏洞扫描
防病毒服务器
专网接入区
省市医保
新农合
下一代防火墙
入侵防御系统
防病毒网关
互联网出口区
电信
联通
下一代防火墙
入侵防御系统
上网行为管理
政务云
门户网站、OA等
运维人员
无线控制器
内网核心
网闸
外网核心
无线控制器
下一代防火墙
无线网
内网无线接入区
医务人员
内网终端区
数据库审计
HIS/LIS/CIS/PACS存储
内网服务器区
行政办公
外网终端区
无线网
外网无线接入区

方案说明

- 在本解决方案中，将严格按照信息系统的重要性和网络使用的逻辑特性划分安全域，根据XX医院网络与信息系统各节点的网络结构、具体的应用以及安全等级的需求，按照技术体系中网络安全规划，将XX医院系统划分为六个安全域。

- 依据安全域划分原则，同一安全域拥有相同的安全等级和属性，专线接入区、内网服务器区、运维管理区、内网终端区、内网无线区；互联网接入区、外网终端区、无线接入区是相互信任的，安全风险主要来自不同的安全域互访，需要加强安全域边界的安全防护。区域之间依据业务及安全的需要配置安全策略，有效实现信息系统合理安全域划分。

- 专线接入区：由于专线连接区域，需要进行安全隔离，包括医保专网等。

- 内网服务器区：XX网络中的内网服务器区域，包括信息系统所在的服务器，主要有HIS、LIS等系统等，同时包括系统所涉及的配套基础，如数据库、存储等设备。跟进等级保护建设基本要求，对重要区域进行划分和防护，如果服务器就直接接在核心交换机上，将会存在很大的安全风险。

- 运维管理区：运维管理区是指通过数据库审计、堡垒机、防病毒软件、内昂威胁感知、漏洞扫描设备对全网进行安全管理的区域。

- 互联网出口区：提供统一的对互联网威胁的防护能力，通过下一代防火墙、入侵防御、上网行为管理等设备进行网络边界的安全防护，提供外网用户对网内数据访问的安全保障。

方案价值

- 通过引入多款安全产品，综合采用多种安全技术来实现了以下安全防护需求：

- 防范来自互联网的威胁：通过在医院的互联网出口部署下一代防火墙、入侵防御系统、上网行为管理等安全设备，综合采取多种安全防护检测手段，很好的防范来自互联网的非法的访问、攻击行为和病毒的传入。

- 防范外网与内网数据交换带来的威胁：通过在医院内网数据中心出口部署下一代防火墙、入侵防御系统、防病毒网关，实时检测专网到内网、内网之间的访问行为，并对其中的非授权访问、攻击行为、携带的恶意代码病毒进行过滤，有效防止了威胁在医院内网的蔓延扩散。

- 定位内网感染主机，发现内网潜在威胁：在医院内网运维管理区部署内网威胁感知系统，聚焦于医院内网风险态势感知，采用山石智能安全技术，重点监控医院核心资产服务器，检测发现已知及未知网络威胁，精准定位内网风险终端和服务器，同时提供完整的攻击链行为细节还原，帮助医院构建可视、可管理、可信任的安全内网。

- 针对访问核心业务数据行为进行防护和审计：通过在医院内网服务器区接入交换机处部署数据库审计与防护系统，通过对访问数据库的行为等采集、分析，实现独立于数据库的审计功能，同时也可以作为数据库防火墙，实时监控、识别、阻断外部黑客攻击以及内部高权限用户的数据窃取行为。

- 满足合规性要求：针对山西省第二人民医院医院，本安全建设方案在满足《网络安全法》要求的同时，也根据等级保护制度的相关要求，落实了医院核心业务信息系统安全保护等级达到三级要求。