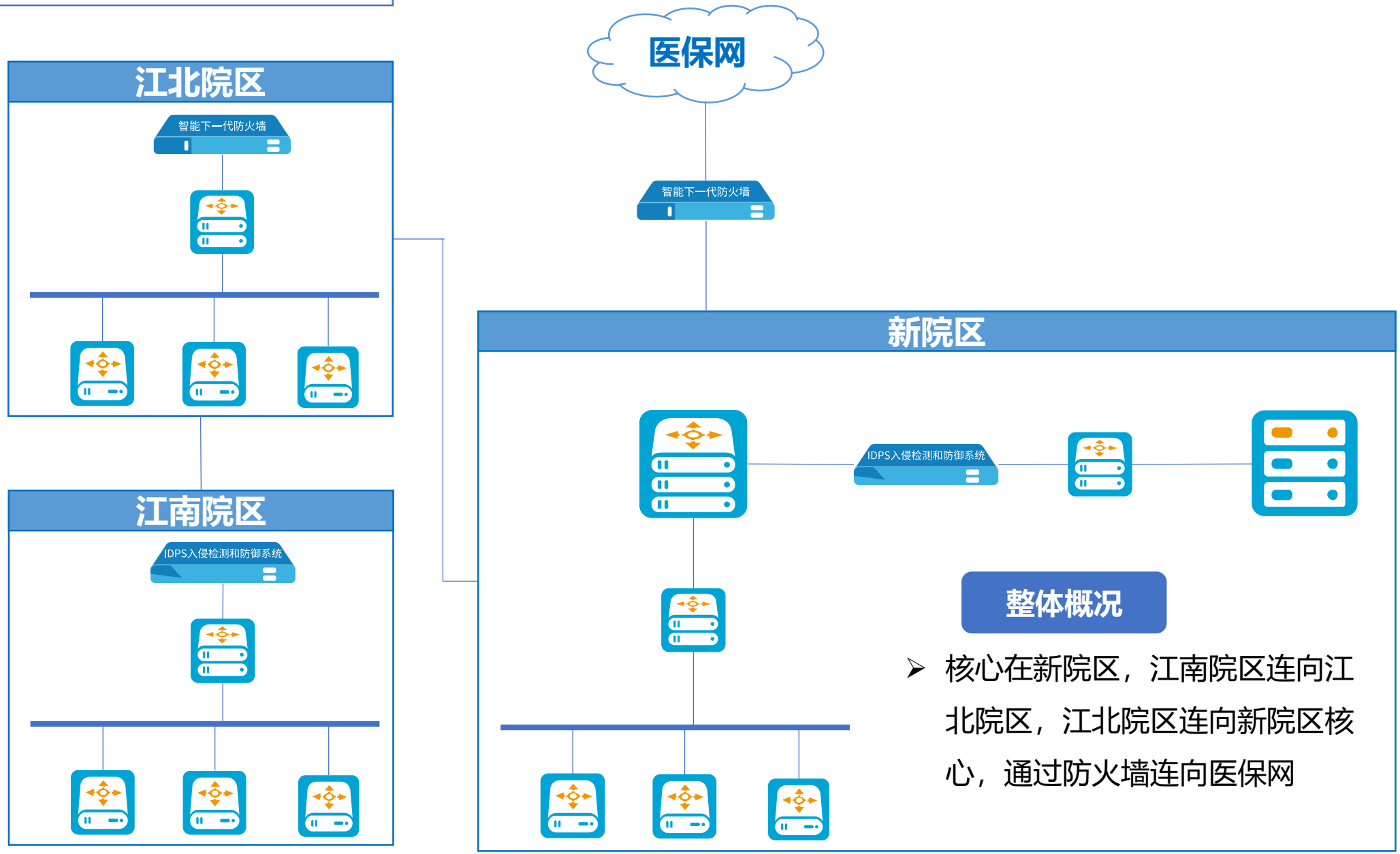
方案名称：某医院等保二级建设解决方案

个人信息：罗茂平-四川泰丰源信息工程有限公司

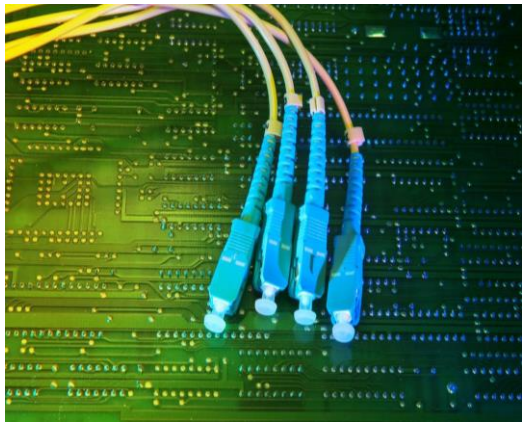
背景介绍—医院网络现状



整体概况

- 核心在新院区，江南院区连向江北院区，江北院区连向新院区核心，通过防火墙连向医保网

需求分析—医院面临挑战



数据安全难防护

数据库作为医院核心业务系统的重要组成部分，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。

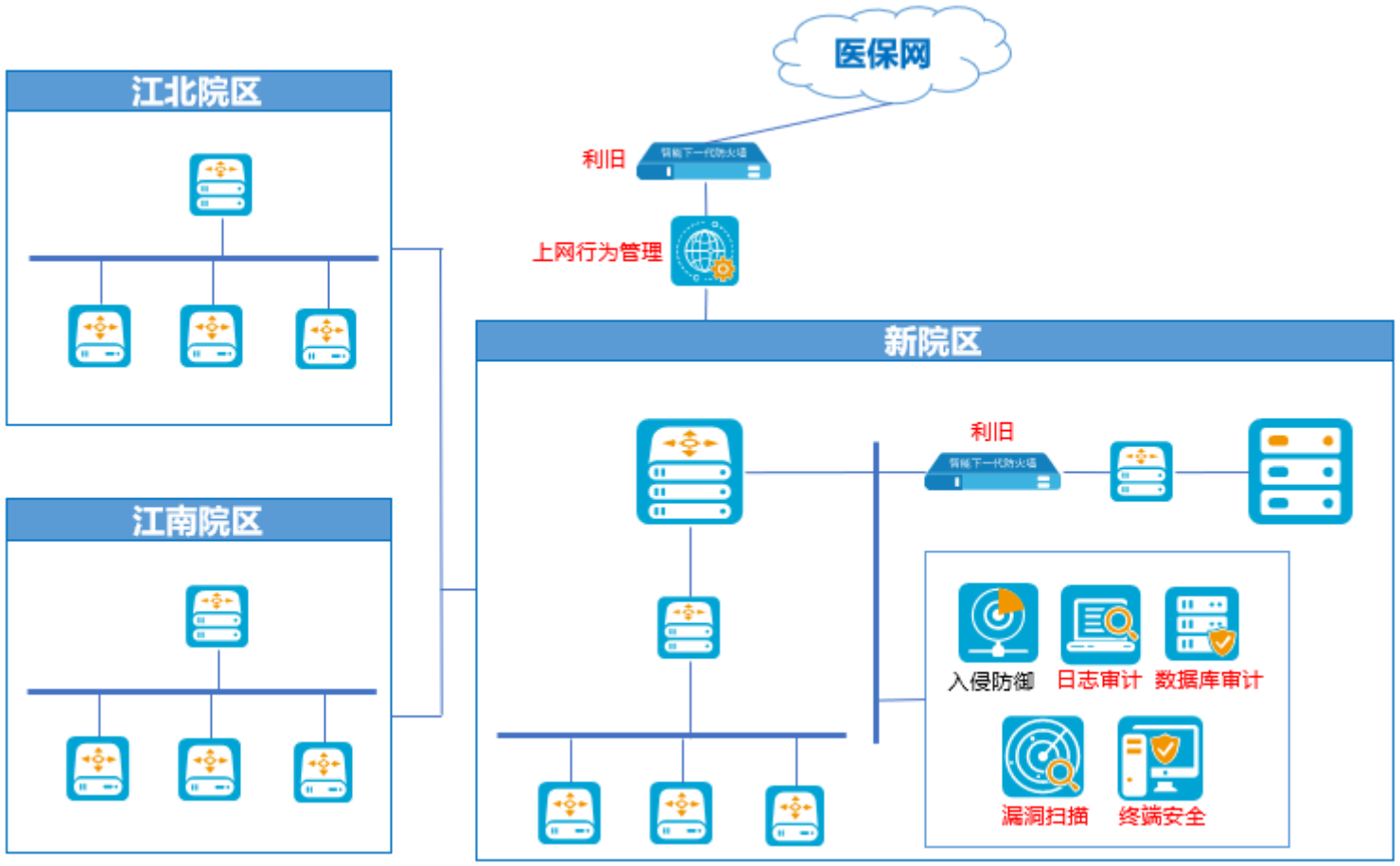
事后追溯困难

设备日志没有专门的设备存放，无法做到相关日志存放6个月以上，发生安全事件后，事后追溯很困难。

运维管理困难

网络内部结构不透明，发生数据泄露、网页篡改等安全事件，无法第一时间知晓，极有可能错过最佳修复时间。

解决方案—山石等保二级解决方案



互联网出口区

部署下一代防火墙，开启IDS、僵尸网络、AV模块（利旧）
部署上网行为管理（新增）

服务器区

部署下一代防火墙，开启WAF模块（利旧）

运维管理区

部署入侵防御（利旧）
部署日志审计、数据库审计、漏洞扫描、终端安全防护（新增）

内网安全可控

全网状态可视，流量管理，带宽控制，行为审计，应用封堵，准入控制。结合终端安全管理，接入内部网络时需准入认证。

提高数据安全防护

实时检测出用户对数据库进行的SQL注入和缓冲区溢出攻击，替换或者阻断高危SQL语句并报警，同时详细的审计下攻击操作发生的时间、来源IP、登录数据库的用户名、攻击代码等详细信息。

事后追溯有证可查

网络数据存放6个月以上，出现数据泄露等网络威胁事件留有记录，事后有证可查。

等保合规

符合《网络安全法》等级保护2.0二级标准。