

方案名称：医院等保三级安全解决方案

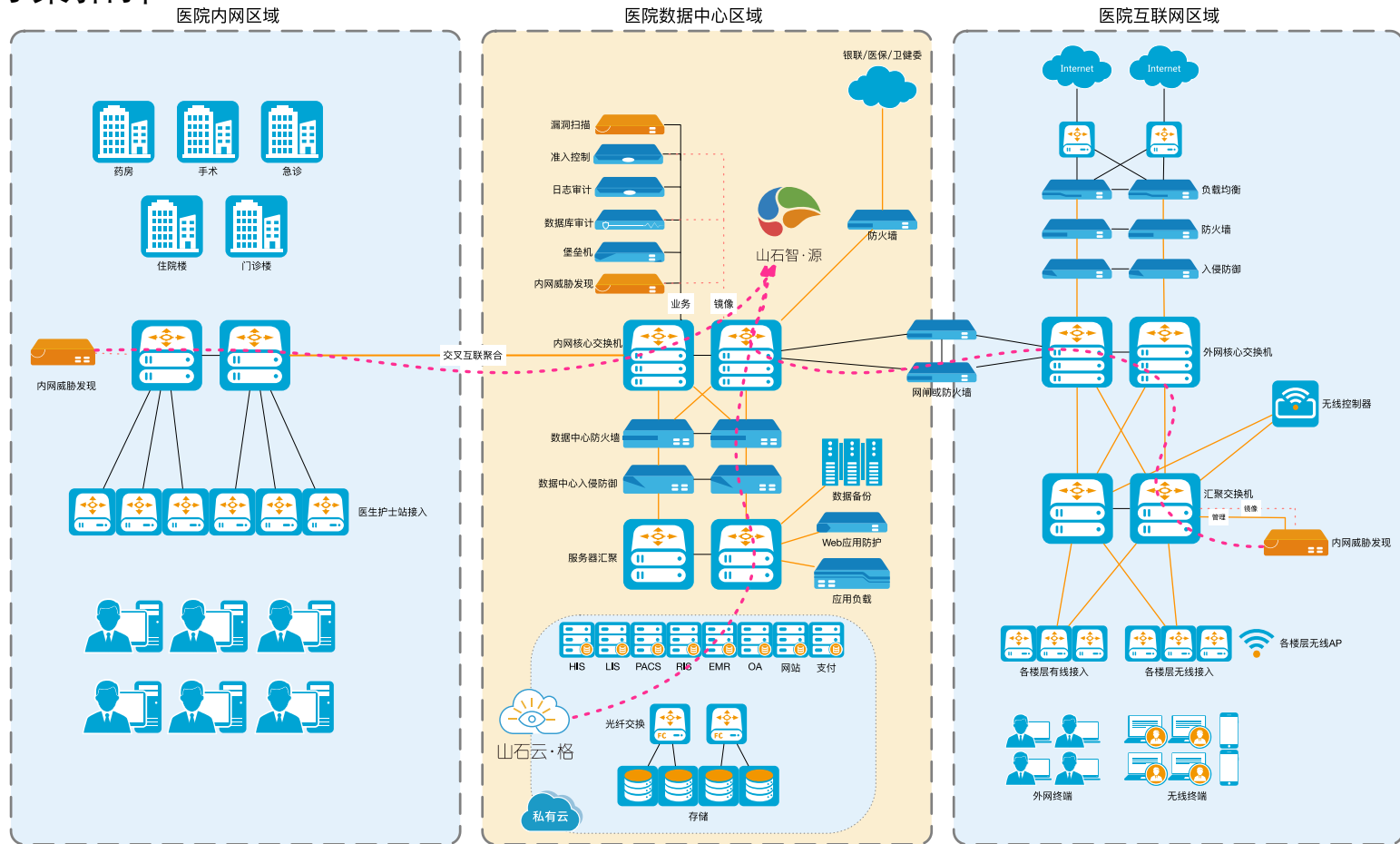
个人信息：高德-青岛盛铂信息技术有限公司

方案背景

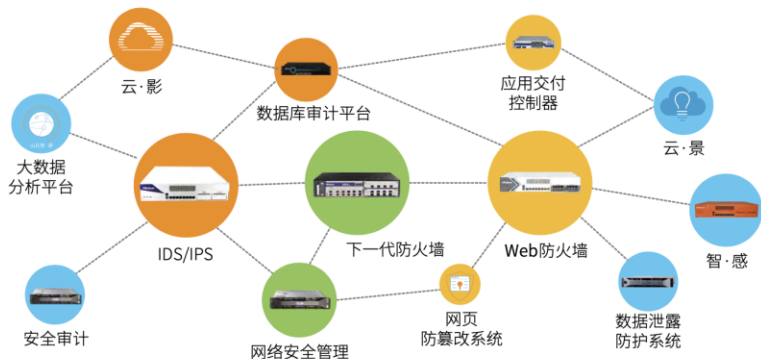


网络技术飞速发展，全球数据量爆炸式增长，信息网络和信息安全成为国家安全重要组成部分之一。根据2017年6月1日实行的《中华人民共和国网络安全法》，第二十一条明确要求：国家实行网络安全等级保护制度。而针对医疗卫生行业，卫生部于2011年11月分别发布《卫生部办公厅关于全面开展卫生行业信息安全等级保护工作的通知》(卫办综函〔2011〕1126号)，卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知(卫办发〔2011〕85号)，明确要求全国所有三甲医院核心业务信息系统的安全保护等级原则上不低于第三级，等级保护成为医院安全建设的重要标准。

不论从合规性角度上还是从自身信息系统安全角度考虑，医疗卫生行业都需要加强自己的安全管理体系和技术体系的建设，切实提升整体信息系统及数据的安全性。



方案介绍



Hillstone
山石网科

覆盖安全通用技术要求

安全管理中心

控制点

系统管理
审计管理
安全管理
集中管控

安全通信网络

控制点

网络架构
通信传输

安全区域边界

控制点

边界防护
访问控制
入侵防范
恶意代码和垃圾邮件防范
安全审计

安全计算环境

控制点

访问控制
安全审计
入侵防范

• 外网区域安全方案设计

在外网区域部署山石网科下一代防火墙、入侵防御 IPS 设备，对进出网络的数据进行 L2-L7 层安全检测，有效防御来自内外网的 DDOS 攻击、应用层等攻击。同时在外网交换机镜像部署山石网科流量 / 威胁探针，通过和安全管理中心的智源管理平台联动，实现对网络内东西南北流量的分析，让管理员直观了解当前的网络风险态势。

• 外联区域安全方案设计

在外联区域部署山石网科下一代防火墙、入侵防御 IPS 设备，对进出网络的数据进行 L2-L7 层安全检测，有效防御来自内外网的 DDOS 攻击、应用层等攻击。

• 服务器区域安全方案设计

在服务器区域边界部署山石网科下一代防火墙设备，实现对进出流量进行精细化的策略管控功能，同时配置 AV/IPS 等功能模块实现对应用层攻击的过滤；在虚拟化内部部署山石云格虚拟化安全防护软件，实现对虚拟化内部的可视、隔离防护作用；镜像模式部署山石网科流量 / 威胁探针，通过和安全管理中心的智源管理平台联动，实现对网络内东西南北流量的分析，让管理员直观了解当前的网络风险态势；部署数据库审计设备对操作数据库的行为进行有效审计；部署应用交付设备为大流量业务系统提供高可靠性冗余能力。

• 核心交换区域安全方案设计

镜像模式部署山石网科流量 / 威胁探针，通过和安全管理中心的山石智源管理平台联动，实现对网络内东西南北流量的分析，让管理员直观了解当前的网络风险态势；部署山石网科下一代防火墙设备实现基层医疗单位的接入控制。

• 内外网办公区域安全方案设计

在终端设备上面以代理模式部署终端探针设备，通过和安全管理中心的山石智源管理平台联动，实时分析监控终端的风险态势。

• 安全管理中心安全方案设计

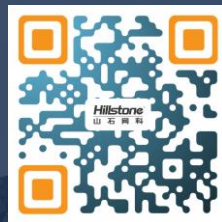
配置日志审计类、集中管控类、运维审计类产品实现全网的安全审计和集中管控等能力，通过智源大数据分析平台呈现全局网络安全及业务流量态势。

通过在不同的安全区域全面部署山石网科的下一代防火墙、入侵防御 / 检测、WEB 防护、内网安全、数据安全、智能分析平台、应用交付、云计算安全、运维管理等各大类设备对医疗行业整体网络提供安全可视、协同防御、持续监测的能力，通过综合部署山石网科硬件安全设备和虚拟化安全防护软件，满足网络安全等级保护基本要求中的通用安全要求和云计算安全扩展要求的技术部分要求。

Hillstone[®]
山石网科

为您的安全竭尽全力!

Thanks



400-828-6655
<https://www.hillstonenet.com.cn>