Hillstone 山石网科

Hillstone 山石网科

方案名称：医院信息化建设

个人信息：盛志凯-江西创瑞电子有限公司

医疗数据中心边界安全解决方案

方案背景

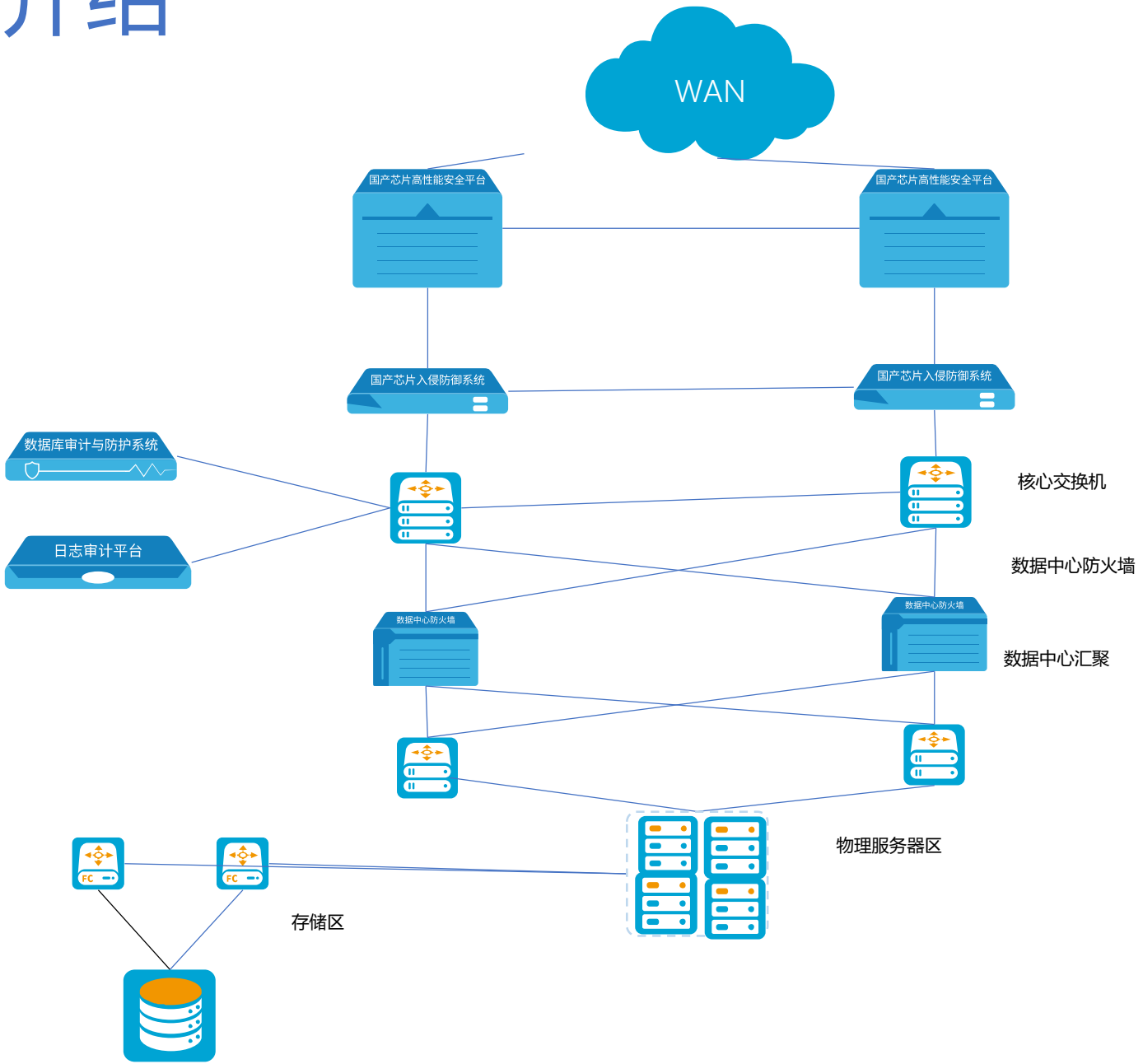
随着医疗信息化建设的逐步深入，网络业务应用和网络系统日益复杂，医疗的带宽大规模升级，网络结构不断优化，数据中心流量剧增，而原有安全设备往往老化严重，吞吐、并发能力有限，网络抗风险性差，数据中心安全设备往往成为性能瓶颈，有单点故障风险，更无法满足未来的带宽扩展需求。

由于医院数据中心往往面临着黑客的攻击，这些攻击轻者引起访问业务中断，严重的将造成重要信息的泄露，并且数据中心集中了医院最重要的信息资产，一旦发生安全事件将对医院的正常业务造成极大的损失，因此需要采取必要的安全防护手段进行保护。

医疗数据中心常见的安全需求：

- 边界隔离、身份识别与访问控制；
- 有效对抗攻击、防范网络入侵和恶意代码、检测与防护未知威胁；
- 流量管理、带宽控制，保障健康的互联网访问；
- 高性能、高可靠性要求；
- 数据中心虚拟化攻击防护；
- 有效防护网站被攻击和篡改；
- 满足等级保护合规性需求；
- 企业多出口运营商线路智能选路；
- 深度应用识别与管控，实现应用层安全防护；

方案介绍


WAN
国产芯片高性能安全平台
国产芯片高性能安全平台
国产芯片入侵防御系统
国产芯片入侵防御系统
数据库审计与防护系统
日志审计平台
核心交换机
数据中心防火墙
数据中心防火墙
数据中心防火墙
数据中心汇聚
FC
FC
存储区
物理服务器区

方案优势

通过在医疗数据中心部署山石网科下一代防火墙、IPS、WAF等设备，满足大流量、高并发环境的部署要求，同时还提供了链路负载、NAT、应用识别、流量管理、访问控制和攻击防护等安全功能，全面保障了企业数据中心网络的安全：

- 在数据中心边界区域部署两台下一代防火墙设备，防火墙设备采用HA的主备方式部署，开启防火墙基本功能、访问控制策略等功能，实现数据中心区域的访问控制、安全防护的功能；
- 下一代防火墙下联两台入侵防御设备，实现对出入数据中心的 2-7 层网络攻击流量的安全防护，保证数据中心区域服务器的安全；
- 在数据中心区域核心交换机处，采用旁挂的方式部署两台WEB应用防火墙设备， 通过在数据中心核心交换机上，将 WEB 流量采用流量牵引方式引流到 WEB 应用防火墙上，进行 WEB 流量的过滤，开启相应的防护策略，保障数据中心 WEB 服务器的安全。

Hillstone®
山 石 网 科

为您的安全竭尽全力！

Thanks

400-828-6655

https://www.hillstonenet.com.cn