
Hillstone
山 石 网 科
方案名称：XX医院信息安全建设方案
个人信息：张强-佳杰科技

医疗行业信息安全痛点

01

- 病毒木马威胁
- 外部网络连通带来的威胁
- 内部违规导致患者隐私泄露（医生，服务商，下游链条）

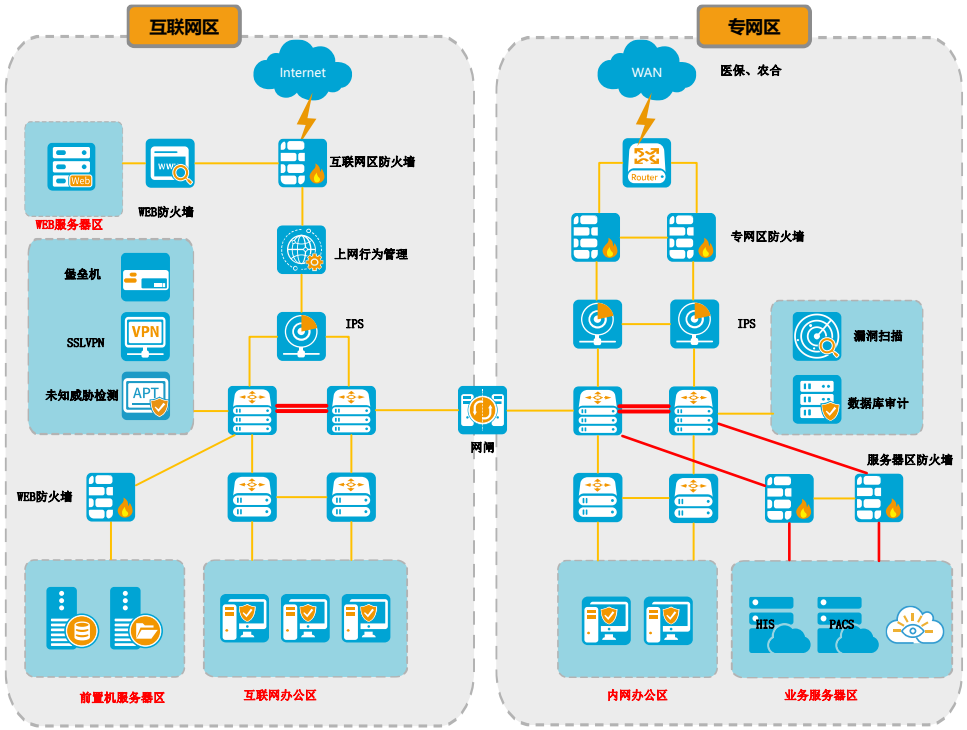
02

- 面临来自互联网的威胁
- 主机安全管控不足，且医院应用HOOK行为较多的特殊性

03

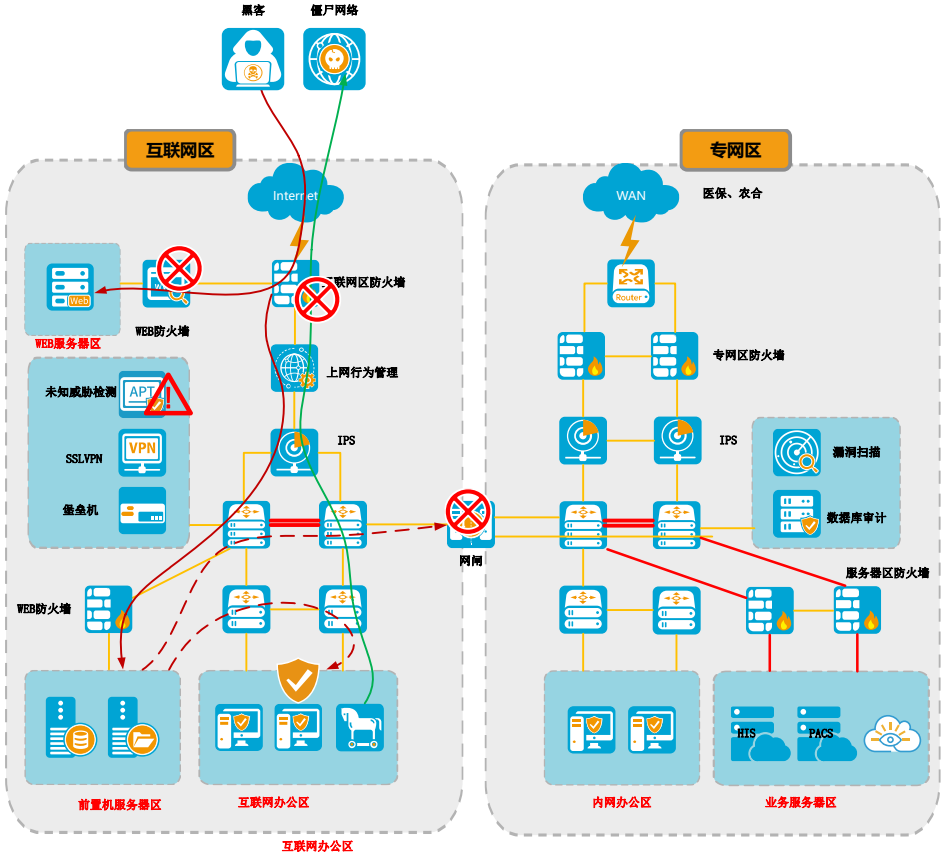
- 信息安全技术力量不足
- 虚拟化平台的脆弱性
- 操作系统自身存在的脆弱性

网络安全整体规划



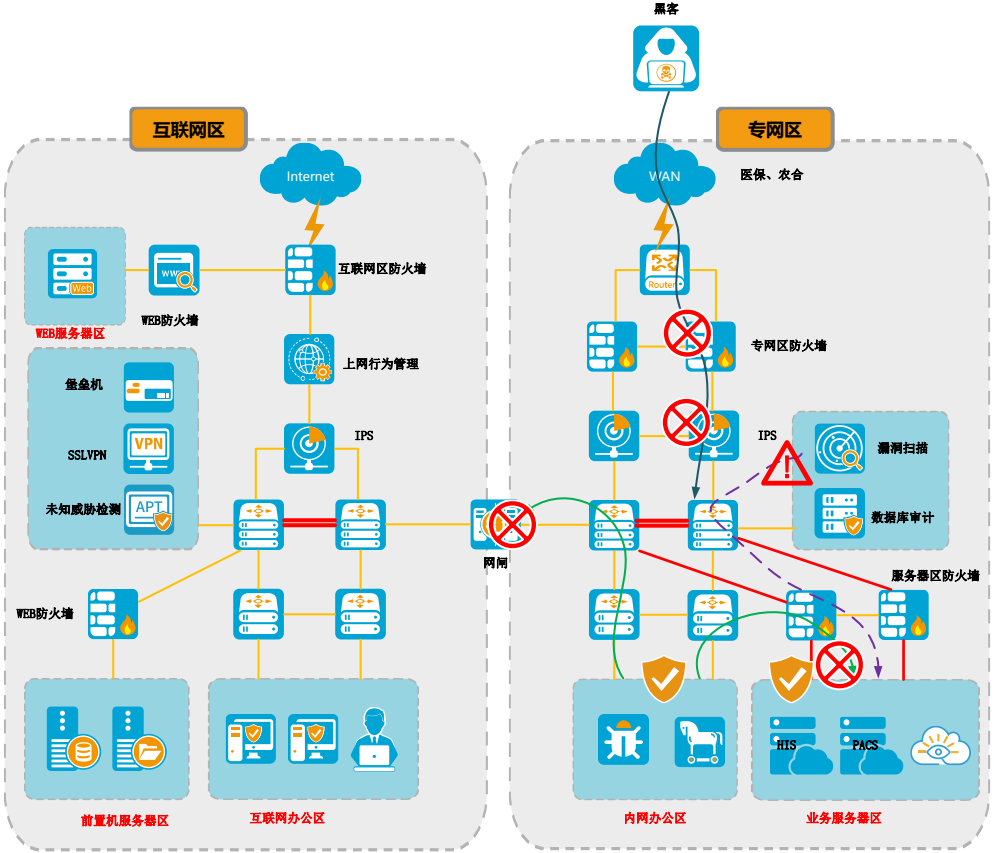
- 整体规划为两张网，进行物理隔离，中间使用网闸进行必要的信息交互。
- 互联网区的业务有WEB服务、前置机服务
- 互联网区出口采用防火墙、上网行为管理、IPS对出入互联网的流量进行控制。
- 在各个区域边界采用相应的防护设备做隔离，如防火墙、WAF
- 在服务器终端和PC终端分别部署终端安全软件。
- 在专网区边界采用防火墙、IPS对访问业务服务器的流量做控制
- 在业务服务器边界采用防火设备作隔离。
- 在内网各终端部署终端安全软件

互联网区防御体系



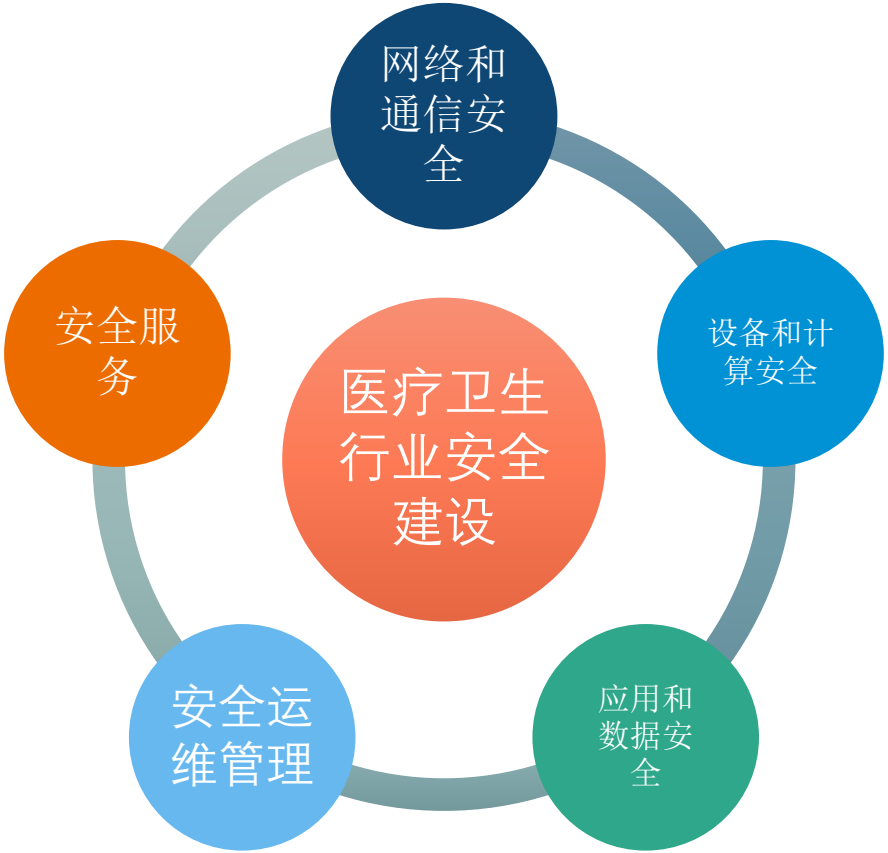
- 互联网区的威胁主要为黑客从外部进行攻击；内部终端的病毒、木马威胁。
- WAF可以有效的阻断黑客对WEB服务器的SQL注入、xss、webshell等攻击。
- 防火墙和IPS可以有效阻断黑客对服务器操作系统、中间件的漏洞攻击。
- 未知威胁检测系统能更细致的检测出特征不明显或隐藏的攻击行为。
- 即使黑客通过某些技术手段或管理员的疏忽，攻破某台内部服务器，在做横向渗透时也会被网闸和终端安全软件所拦截。
- 如果某些主机感染病毒或被植入了木马成为肉机，当肉机进行外联时，防火墙可以检测出失陷主机，并对外联请求做阻断
- 在运维区部署堡垒机和SSL VPN能对应用系统做更安全、便捷的管理

专网区防御体系



- WAN边界的防火墙可以有效阻断从外部到内部的攻击行为。
- 网闸可以阻断木马的外联请求并且终端安全软件可以对木马、病毒进行有效的查杀
- 业务服务器区防火墙可以有效阻断南北向威胁和横向渗透威胁。
- 漏扫定期扫描业务服务器、PC机、网络设备的最新漏洞，并且第一时间更新漏洞，缩小攻击面。
- 堡垒机系统对访问、操作业务服务器的运维人员做限制。
- 数据库审计系统对数据库的所有操作做记录。
- 虚拟化安全系统对虚拟主机进行保护

方案优势



本安全建设方案符合医疗行业信息化安全要求，促进行业信息化安全建设健康、稳定的持续运营。

Thanks

Hillstone
山石网科

为您的安全竭尽全力！

400-828-6655

https://www.hillstonenet.com.cn