**HIS、LIS、PACS、EMRS三级等级保护认证参数**

项目内容

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目内容** | **频率/数量** | **服务期限** |
| 1 | 网络安全设备巡检服务 | 四次 | 一年 |
| 2 | 系统漏洞扫描及加固服务 | 二次 | 一年 |
| 3 | 网络安全培训服务 | 一次 | 一年 |
| 4 | 网络安全加固服务/建议 | 不限次数 | 一年 |
| 5 | 网络安全应急响应服务 | 不限次数 | 一年 |
| 6 | 防火墙边界安全保护系统服务 | 不限次数 | 一年 |
| 7 | 核心业务系统等级保护达标检测服务 | 一次 | 一年 |

项目内容说明：

1 、网络安全设备巡检服务

利用工具或人工方式对内网主要网络安全设备的运行状况、连通状况、设备性能等进行综合巡检。以医院核心业务系统为重点，全面梳理与之相连的网络安全资产、端口、服务，排查风险隐患，保障系统正常运行。

巡检对象：安全设备、网络设备、操作系统、数据库、应用平台等系统，交付物：《网络安全巡检报告》

2 、系统漏洞扫描及加固服务

通过漏洞扫描和持续监控来发现核心业务系统的安全隐患，探测发现无主资产、闲置资产，并对资产进行全生命周期的管理。利用漏洞扫描工具对网络层、操作系统层、应用层等范围以本地化扫描的方式对核心业务系统涉及范围内的系统和网络进行资产梳理、漏洞发现，根据发现的漏洞提供漏洞修复、安全加固、安全建议等服务。

检测对象：包括安全设备、操作系统、应用中间件、网络设备、数据库等系统，交付物：《漏洞扫描报告》及《漏洞加固报告》

3 、网络安全培训服务

通过大量的当前典型网络安全事件导入，对网络安全威胁给予直观描述，加强员工安全意识，尤其防范社会工程学攻击。包括全员安全意识宣传、内部安全意识培训以及第三方安全意识宣贯等。

培训内容：网络安全意识、网络安全等级保护知识、网络安全攻防内容（含网络攻击演示），培训时间：不小于6小时，交付物：培训材料及PPT

4 、网络安全加固服务/建议

对核心业务系统按照最新标准进行等级保护差距分析，根据差距分析结果对安全漏洞进行加固、安全缺陷进行弥补、安全策略进行调整、安全管理进行提升，确保经过等级保护安全加固使各核心业务系统达到相应级别的等级保护标准要求。，交付物：《网络安全等级保护差距分析报告》、《网络安全加固整改方案》。

5 、网络安全应急响应服务

按照相关应急响应流程和规范对系统日常运行过程中出现的网络安全事件，提供安全专家协助进行事件分析、恢复、根除以及总结等一系列工作，确保安全事件得到迅速妥善处置，并使影响降到最低。交付物：《网络安全应急处置报告》

1. 边界安全防护系统服务

安全防护需要人工与工具接合，部署安全防护工具，实时对边界安全进行检测与防护，工具最终为甲方所有。

|  |  |
| --- | --- |
| 服务能力 | 1. 硬件参数：标准1U机架；配备9个千兆电口；配备独立的1个CON口，1个USB2.0口。
2. 硬件平台采用非X86的专业嵌入式多核安全架构。
3. 性能参数：吞吐量≥4Gbps，AV吞吐量≥1Gbps， IPS吞吐量≥1.5Gbps，IPsec VPN吞吐率≥1.5Gbps；最大并发连接数≥180万；最大IPsec VPN隧道数≥2000，每秒新建会话≥4.5万，SSL VPN并发用户数可扩展到至1000个；
4. ★支持策略助手支持生成基于服务的安全策略，SNAT/DNAT支持策略命中数分析，显示策略创建时间、命中数、首次命中时间、最近一次命中时间、未命中天数等信息，并可针对分析结果，对策略进行删除或禁用。提供相关截图证明加盖公章
5. 支持透明、路由、混合、旁路4种工作模式。
6. ★建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，隔离技术，用以及时发现并处理企业计算机网络运行时可能存在的安全风险、[数据传输](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E4%BC%A0%E8%BE%93/2987565%22%20%5Ct%20%22/Users/mac/Documentsx/_blank)、操作实施记录与检测，以确保计算机网络运行的安全性。连续7年入选权威机构Gartner防火墙魔力象限，提供证明文件加盖公章
 |
| 攻击防护 | 1. 支持多种畸形报文攻击防护，SYN Flood、DNS Query Flood等多种DoS/DDoS攻击防护，支持ARP攻击防护。
2. DNS query flood支持IPv6，DNS reply flood支持IPv4和IPv6，AD支持目的IP地址白名单。
3. 支持与云端威胁情报中心联动。
4. 支持威胁情报与防火墙威胁事件、威胁日志检测结果加强与取证，用户可通过手动触发与自动触发将日志元素上送威胁情报平台进行上下文查询。
5. 支持自动聚焦重点威胁，热点情报推送到设备，并提供配置向导协助用户生成安全防护策略。
 |
| 故障诊断工具 | 1. 可模拟数据包流经设备的每个功能模块，并以逻辑图的方式呈现每个功能模块的对数据包的处理结果，非命令行debug抓包功能。便于管理员排查故障。
2. 智能分析诊断：支持数据包路径检测工具通过在线检测、模拟检测、已有检测源等检测手段，图形化展现数据包经过的每个防火墙功能模块的处理过程，图形化检测项包括：报文合法性检查、攻击防护、会话匹配、MAC检查等，以便快速定位异常功能模块。
 |
| 数据安全 | 1. 支持基于文件类型、文件大小、文件名称进行数据传输安全控制。
2. 支持HTTP、FTP、SMTP、POP3协议文件传输的识别。
3. 支持近百种主流文件类型的特征码及后缀名双重识别。
4. 支持对网页关键字、Web外发信息、邮件等内容进行过滤。
5. 支持微博、微信UID和QQ虚拟身份的识别及相关上网行为的审计记录。
6. 文件过滤支持SMB协议。
7. ★支持NAT转换扩展技术，使每个公网IP地址支持的NAT转换端口突破65535端口的限制，支持NAT资源地址池可用性检测；要求提供产品软件界面截图以证明，并加盖厂商公章
 |
| 扩展功能 | 1. 支持扩展入侵防御IPS2. 支持扩展病毒过滤AV3. 支持扩展虚拟化VSYS4. 支持扩展云沙箱sandbox5. 支持扩展僵尸网络C2防御C2C6. 支持扩展IP信誉库7. 支持扩展带宽管理QOS8. 支持扩展网页控制URL |
| 满足的安全资质要求 | 1. 具备公安部颁发的第二代防火墙《计算机信息系统安全专用产品销售许可证》（增强级）；
2. ★具备国家网络与信息系统安全产品质量监督检验中心颁发的信息技术产品安全分级评估证书（EAL4+级）；提供证明材料加盖公章
3. ★具备中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》（增强级）；提供证明材料加盖公章
4. ★要求设备厂商获得了NGFW下一代防火墙产品的NSS Labs最高的评价推荐级；提供证明材料加盖公章
5. ★要求设备厂商连续三年进入了Gartner IDPS魔力象限（市场指南）；提供证明材料加盖公章
6. 7、要求设备厂商通过全球IPv6测试中心的“IPv6 Ready”金牌认证，并提供认证证书；
7. 8、具备国家保密科技测评中心颁发的防火墙《涉密信息系统产品检测证书》
8. ★必须提供原厂商1年的硬件保修和软件升级服务，1年应用识别特征库升级；并提供原厂商售后服务承诺函原件。
 |

7 、核心业务系统等级保护达标检测服务

完成核心业务系统的安全等级保护达标检测。

★取得至少4个系统（至少分4个单独文档）第三级的信息系统安全等级保护备案证明文档，证明文档中相关系统的确认以医院最终说明为准。交付《网络安全等级保护测评报告》及《网络安全等级保护系统备案证书》