**苏州市第九人民医院院安全设备续保扩容及安全服务项目调研**

1. **设备维保及扩容服务目标**
2. 通过设备维保服务可获得7\*24小时远程和现场支持服务，确保一旦发生故障，迅速得到技术专家的技术支持。
3. 维保服务期内设备软件故障可得到原厂代码级支持，确保设备在运维中遇到任何问题，故障隐患都可以完善处置、定位并解决。
4. 在维保服务期内原厂发布重要、重大软件更新，能够及时得到原厂技术支持，包括软件和版本升级服务，确保我院网络安全设备在维保服务期间的安全、可靠、稳定和扩展性。
5. 提供7\*24整体网络环境、链路和网络安全系统的日常运维保障。包含安全规划、日常巡检、安全加固、应急响应、风险评估、渗透测试和安全培训服务。
6. **维保及扩容网络安全设备清单**
7. 维保清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **产品型号** | **质保类型** | **续至时间** |
| 1 | 深信服 外网负载均衡 主 | AD-1000-D620 | 特征库 | 2024年5月30日 |
| 2 | 深信服 外网负载均衡 备 | AD-1000-D620 | 特征库 | 2024年5月30日 |
| 3 | 山石网科 专网防火墙 | SG-6000 E5168 | 特征库 | 2024年5月30日 |
| 4 | 深信服 防火墙 | AF-1000-FA40-GL | 特征库 | 2024年5月30日 |
| 5 | 网御 行为流控 主 | LeadsecACM-N6010 | 特征库 | 2024年5月30日 |
| 6 | 网御 行为流控 备 | LeadsecACM-N6010 | 特征库 | 2024年5月30日 |
| 7 | 锐捷 外网防火墙 主 | RG-WALL 1600-X8500 | 特征库 | 2024年5月30日 |
| 8 | 锐捷 外网防火墙 备 | RG-WALL 1600-X8500 | 特征库 | 2024年5月30日 |
| 9 | 天融信 软件木马检查 | （TI-51428-TVD） | 软件授权 | 2024年5月30日 |
| 10 | 网御WEB防护 主 | Leadsec-6000WAF-A | 特征库 | 2024年5月30日 |
| 11 | 网御WEB防护 备 | Leadsec-6000WAF-A | 特征库 | 2024年5月30日 |
| 12 | 网御 漏洞扫描 | TS-SC-S1100 | 特征库 | 2024年5月30日 |
| 13 | 山石网科备用墙 | SG-6000 E5168 | 特征库 | 2024年5月30日 |
| 14 | 360杀毒软件 | 1500个终端安全 | 特征库 | 2024年12月31日 |
| 15 | 360杀毒软件 | 150windows服务器终端 | 软件授权 | 2024年12月31日 |
| 16 | 360杀毒软件 | 1000个终端安全 | 特征库 | 2024年12月31日 |

1. 扩容清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **产品型号** | **扩容点数** | **质保类型** | **备注** |
| 1 | 锐捷堡垒机 | RG-DAS 1000E | 200点授权 | 扩容授权 | 永久有效 |
| 2 | 360杀毒软件 | 服务器终端（40\*W+10\*L) | 50点授权 | 扩容授权 | 2024年12月31日 |

1. 服务清单及要求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **标的物名称** | **服务要求** | **单位** | **服务期限** |
| 1 | 网络、信息安全运维服务 | 提供7\*24整体网络环境、链路和网络安全系统的日常运维保障。包含安全规划、日常巡检、安全加固、应急响应、风险评估、渗透测试和安全培训服务 | 项 | 2年 |

1. **网络安全设备维保及扩容要求**
2. 基础要求

* 对延保设备提供至对应年限的原厂延保服务（根据合同要求对相关设备进行特征库升级），并针对购买了延保服务的设备，提供完整的日常应用维护和技术支持服务；
* 对扩容设备提供原厂扩容授权（根据合同要求对相关设备进行库容升级），并针对购买了扩容授权的设备，提供完整的授权导入升级、新增扩容项初始化上线、调试和相关的技术支持服务；
* 电话基本服务提供7×24小时不间断热线电话支持服务，通过电话可以直接联络专门技术工程师，寻求问题的解决方案、技术文档以及技术指导，电话支持需及时响应。
* 因为设备故障等原因，采购方需要进行数据恢复时，安排工程师值守配合采购方的需求，提供系统的备份以及恢复的咨询，帮助采购方制定系统的备份方案，并且能在采购方进行备份恢复测试时提供辅助。另外，应根据采购方需要，进行相关的软硬件配置、调整等。
* 对采购方在不同阶段遇到的各种具体问题提供服务支持，包括现场服务，非工作时间技术支持服务。如系统宕机，性能的下降，系统配置的等问题。
* 提供可靠的服务保障，能提供正常的技术、备品备件服务。拥有本地备件库。技术服务运行维护符合相关标准。

1. 网络、信息安全运维要求
2. 网络、信息安全巡检要求

* 日常安全监控运维服务
* 安全设备日常巡检：安全设备软、硬件健康性检查，安全策略检查、及安全日志分析等。

（包括防火墙、WEB 应用防火墙、基线管理系统、安全运维，堡垒机、漏洞扫描以及与安全运维有关的服务器及存储设备。监控相关硬件设备使用是否正常、系统日志是否有报错、网络连通性是否正常等。）

* 协助完成安全策略的核查与整改
* 优化整理关键业务平台的安全设备的拓扑资料，保持相关资料的更新
* 维护更新安全运维文档，应急响应流程
* 对新设备进场进行安全配置核查系统使用状况和运行趋势分析
* 定期提供系统的资源使用统计、相关日志进行归档和历史运行趋势分析，并提交报告。监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月，满足《网络安全法》和相关法律法规要求。
* 协助处理相关部门端口开放等业务申请
* 根据客户业务需求配合调整网络安全设备端口权限和策略设置。
* 防火墙策略优化
* 安全配置核查服务
* 补丁升级（含服务器操作系统和终端操作系统）
* 重大节假日保障支撑服务

1. 应急响应要求

* 建立应急响应机制，在保证快速响应的前提下，通过流程化、标准化的机制保障客户各应用系统出现信息安全事件，网络安全系统遇到重大故障时，需及时提供应急响应服务。同时协助客户每年修订完善网络与信息安全预案及各系统专项应急预案，并配合实施年度应急演练做好相关过程记录形成应急演练报告。
* 2年内提供不限次数“7×24小时”快速响应的紧急服务。我院随时随地可立即得到本公司工程师的电话响应。一旦用户遇到紧急情况（如意外停机），本公司工程师会立即通过电话通知用户有关应急处理方法（如在线恢复、生产切换等），一方面与用户保持热线联系，另一方面安排工程师用最快的方式抵达现场进行紧急维护。