## 附件:晴隆县人民医院网络安全等级保护合规性整改项目采购清单及技术参数

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 出口防火墙 | 1、产品网络层吞吐量≥6Gbps，应用层吞吐量≥2Gbps，最大七层并发连接数≥180万，HTTP新建连接数≥6万；  2、产品配置千兆电口≥6个，千兆光口SFP≥4个；配置64G SSD硬盘；配置三年的WEB应用防护识别库、IPS特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和URL&应用识别库升级授权；  3、产品支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型；  4、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；  5、产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议；支持策略路由负载，支持基于服务、ISP地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法；  6、产品支持支持源地址转换SNAT，目的地址转换DNAT和双向NAT等功能， 支持一对一、一对多、多对一等形式的NAT；支持NAT64和NAT46 地址转换方式，满足IPv6改造要求；  7、产品支持IPsec VPN和SSL VPN功能，IPSec VPN需支持IKEv1和IKEv2协议，支持基于主模式和野蛮模式建立加密隧道；  ★8、产品支持对不少于9880种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制（提供产品功能截图并加盖厂商公章）；  ★9、产品支持僵尸主机检测功能，产品预定义僵尸特征库超过110万种，可识别主机的异常外联行为（提供产品功能截图并加盖厂商公章）；  10、产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制；  ★11、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（提供产品功能截图并加盖厂商公章）；  ★12、产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生（提供产品功能截图并加盖厂商公章）； | 1 | 台 |
| 2 | 数据中心防火墙 | 1、产品网络层吞吐量≥20Gbps，应用层吞吐量≥8Gbps，最大七层并发连接数≥220万，HTTP新建连接数≥15万；  2、产品配置千兆电口≥6个，万兆光口SFP+≥2个；配置128G SSD硬盘；配置三年的WEB应用防护识别库、IPS特征库、僵尸网络与病毒防护库、实时漏洞分析识别库和URL&应用识别库升级授权；  3、产品支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型；  4、产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式；  5、产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议；支持策略路由负载，支持基于服务、ISP地址、应用、地域等维度进行智能选路，保证关键业务流量通过优质链路转发，支持加权流量、带宽比例、线路优先等负载均衡调度算法；  6、产品支持支持源地址转换SNAT，目的地址转换DNAT和双向NAT等功能， 支持一对一、一对多、多对一等形式的NAT；支持NAT64和NAT46 地址转换方式，满足IPv6改造要求；  7、产品支持IPsec VPN和SSL VPN功能，IPSec VPN需支持IKEv1和IKEv2协议，支持基于主模式和野蛮模式建立加密隧道；  ★8、产品支持对不少于9880种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制（提供产品功能截图并加盖厂商公章）；  ★9、产品支持僵尸主机检测功能，产品预定义僵尸特征库超过110万种，可识别主机的异常外联行为（提供产品功能截图并加盖厂商公章）；  10、产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制；  ★11、产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（提供产品功能截图并加盖厂商公章）；  ★12、产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生（提供产品功能截图并加盖厂商公章）； | 1 | 台 |
| 3 | 漏洞扫描系统 | 1、1U设备，配置≥6千兆电口，≥2个千兆光口；配置单交流电源，配置硬盘容量≥128GB SSD+2TB SATA；  2、设备支持资产发现最大并发IP数1024个，支持主机漏扫最大并发IP数75个，支持WEB漏扫最大并发URL数5个，支持基线核查最大并发IP数5个，支持弱口令扫描最大并发IP数25个；本次要求配置系统漏扫授权IP数100个，WEB漏扫授权URL数20个；  3、支持同时开启全插件系统漏洞扫描、WEB漏洞扫描、弱口令扫描、基线配置核查，扫描速度不低于1000ip/h；  ★4、支持全局风险统计功能，通过扇形图、条状图、标签、表格等形式直观展示资产风险分布、漏洞风险等级分布、紧急漏洞、风险资产清单等信息，并可查看详情（提供产品功能截图并加盖厂商公章）；  5、支持资产发现功能，可基于IP地址、IP网段、IP范围、URL等方式进行资产发现扫描，支持EXCEL格式批量导入；  6、支持系统漏洞扫描检测的漏洞数大于14000条，兼容CVE、CNNVD、CNVD、Bugtraq等主流标准；  ★7、支持行业通用标准OWASP，支持通用WEB漏洞检测，如：SQL注入、XSS、目录遍历、本地/远程文件包含漏洞、安全配置错误、命令执行、敏感信息泄露等（提供产品功能截图并加盖厂商公章）；  8、支持对多种服务协议的弱口令猜解，包括FTP、IMAP、Microsoft SQL、MySQL、PcAnywhere、POP3、SMB、Telnet、VNC、SSH、RDP、ORACLE、Rsync、SMTP、VMware等；  9、支持对Windows、Linux等操作系统按照等保二级、等保三级要求实施基线配置核查；  ★10、产品支持对系统漏洞、WEB漏洞、基线配置、弱口令进行扫描和分析，可同时输出包含系统漏洞扫描、WEB漏洞扫描、基线配置核查、弱口令扫描结果的报表（提供产品功能截图并加盖厂商公章）；  11、支持查看系统CPU、内存、磁盘资源的使用情况，支持系统设备状态的实时监控、一键式关机和重启； | 1 | 台 |
| 4 | 漏水检测绳 | 漏水检测绳30米，带声光报警器 | 1 | 套 |
| 5 | 静电消除器 | 静电消除器，带声光报警器 | 1 | 套 |
| 6 | 技术服务 | 1、实施三级等保技术整改，解决所有高风险选项，包含：数据库高危漏洞修复、操作系统高危漏洞修复、中间件高危漏洞修复、基线合规等内容，确保测评分数达到70分以上；  2、远程巡检，服务期内每季度1次。  3、现场巡检，服务期内每年2次以上，质保期后每年1次。  4、安全培训，服务期内每年1次以上。  5、应急演练，服务期内每年1次。  6、应急支撑 甲方遭受网络攻击事件时提供远程、现场应急支撑，服务期内无限次。  7、安全加固，服务期内每年2次。  8、迎检支撑，服务期内无限次。 | 1 | 批 |