|  |  |
| --- | --- |
| 产品名称 | 技术要求 |
| 下一代防火墙一台 | 1. 性能参数：网络层吞吐量≥3G，应用层吞吐量≥1G，防病毒吞吐量≥500M，IPS吞吐量≥400M。 2. 硬件参数：规格：1U，内存≥4G，硬盘容量≥64G SSD，电源：单电源，接口：≥6个千兆电口，≥4个千兆光口SFP。   3、支持IPv4／v6 NAT地址转换，支持源地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制，支持NAT64、NAT46 地址转换；  4、支持基于五元组的访问功能，在重点保护期间，能够通过国家地域的方式进行访问控制；访问控制规则支持模拟策略匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；  5、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。（需提供产品功能截图证明并加盖厂商公章）  6、为保障各地域的访问管控能力，支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。所投产品必须提供具备CMA认证的第三方权威机构关于“国家/地区的流量管理”功能项的产品检测报告。（需提供相关证明材料并加盖厂商公章）  7、为保障病毒防护效果，支持对多重压缩文件的病毒检测能力，支持不小于15层压缩文件病毒检测与处置。（需提供产品功能截图证明并加盖厂商公章）  8、为避免单位因遭遇近期多种变种勒索病毒的攻击，支持勒索病毒检测与防御功能  9、支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。（需提供产品功能截图证明并加盖厂商公章）  10、为避免单位遭到挖矿病毒攻击，支持CC通信检测防护，支持CC攻击防护功能，为保障勒CC攻击的检测效果。 |
| 杀毒软件aES | 1、产品可以纯软件交付，包含管理控制中心软件及终端客户端软件，其中管理控制中心可云化部署，需配置≥150点PC授权，≥10点服务器授权；  2、具备高兼容性，在识别到终端存在非适配的第三方软件时可使用兼容模式进行安装，灵活调整agent策略，提供流畅的终端体验。  3、Windows服务器 客户端支持Windows Server 2008、 R2/Windows Server 2012/Windows Server 2016/Windows Server 2022；Linux服务器 客户端支持 CentOS/UbuntuDebian/RHEL/SUSE/Red Flag Asianux Server/Oracle Linux。  4、采用B/S架构的管理控制中心，具备终端安全可视，终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能。  5、支持全网风险展示，包括但不限于未处理的勒索病毒数量、高级威胁、暴力破解、僵尸网络、WebShell后门、高危漏洞及其各自影响的终端数量。（需提供产品功能截图证明并加盖厂商公章）  6、提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数。（需提供产品功能截图证明并加盖厂商公章）  7、支持同时展示跟同品牌下一代防火墙进行联动处；置理员可以在防火墙管理界面下发快速查杀任务，并查看任务状态、结果并进行处置，支持在管理平台查询和统计联动信息。（需提供产品功能截图证明并加盖厂商公章）  8、支持跳转链接至云端安全威胁响应系统，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析。  9、支持终端自动分组管理，新接入的终端可以根据网段自动分配到对应的分组。  10、支持全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件、监听端口和终端账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示。  11、支持基于系统内置弱密码字典和自定义弱密码字典的检查功能，弱密码检测支持至少包括SSH、RDP、MySQL、Tomcat、Redis等应用类型，可按照空密码、自定义弱密码、密码长度小于8、字符种类小于3等常见弱密码类型进行分类查看。  12、支持勒索风险管理功能，持续跟踪最新的勒索情报和技战法，实时展示出资产中的入侵风险，包括勒索风险端口、勒索应用弱密码和勒索风险漏洞，为用户做勒索风险加固提供数据支撑。 |
| 日志审计一台 | 1、性能：综合每秒处理日志数(EPS)最大性能：2600。硬件规格：1U机箱，6个千兆电口，2个扩展插槽，1个Console接口，单电源，2TB硬盘。包含60个日志源授权，三年硬件维保服务和3年软件升级维护服务。 2、支持按照Syslog-NG标准及自有格式进行转发，转发时包含原始日志源IP地址；  3、支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示（提供证明截图并加盖原厂公章）  4、支持自定义资产类型及资产属性；支持对资产自定义标签，支持对标签内容进行查询和管理。  5、系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。  6、支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化。  7、支持以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，且支持图片大小调整。（提供证明截图并加盖原厂公章）  8、支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息  9、系统提供页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略，所见即所得，也支持通过归一化文件的导入来支持归一化,不需修改系统程序。 |
| 安全托管服务 | 1、告警数据与云端运营中心联动，云端安全专家提供7\*24小时的安全运营托管服务。  2、定期发送安全运营报告，让用户清晰了解安全运营态势、安全运营工作情况。  3、探测互联网边界资产，包含IP、端口、漏洞、域名、API接口、弱口令、敏感代码、敏感文档、邮箱、微信公众号、微信小程序等（提供证明截图并加盖公章）。  4、对主机、网络设备、操作系统、数据库、中间件等进行常态化的漏洞与弱口令扫描，提供漏洞、弱口令扫描结果与整改建议。  5、监测互联网出口与服务器区域边界流量，及时发现包括非法外联、外网攻击、内网传播、暴力破解、利用成功等攻击行为。  6、发生相关风险告警，通过邮件、飞书、钉钉、企业微信等形式及时通知用户。  7、支持高交互蜜罐，精准诱捕攻击蜜罐的失陷主机，深挖各种内网潜伏威胁：勒索病毒传播、内网主机被远控后横向攻击（提供证明截图并加盖公章）。 |
| 探针安服工具一体机一台 | 机架式设备，配置≥4个千兆电口，≥64G内存，≥2T硬盘存储空间，冗余电源，三年有效期。  1、扫描次数授权：无限制；  2、扫描IP/域名范围授权：无限制；  3、提供仿真业务陷阱授权数：无限制；  4、提供出口流量监测带宽授权：2Gbps |
| 堡垒机一台 | 1、标准1U机架式硬件、单电源、硬盘容量≥2T、标配≥2个电管理口，标配≥4个电业务口，字符连接数≥50，图形连接数≥10，授权资产数量≥50，RJ45串口1个，USB接口≥2个，运维用户无限制。  2、支持常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin、X11；可通过应用发布的方式进行协议扩展，如数据库Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具。  3、支持标准化对接CAS、JWT、SAML2、OAuth2单点登录认证，且支持配置是否自动创建堡垒机用户（需提供相关截图证明并加盖原厂公章）。  4、支持基于国密算法的动态令牌进行双因子认证。  5、支持IE、谷歌或火狐浏览器代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码（提供证明截图并加盖原厂公章）。  6、支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权（需提供国家权威机构证明并加盖原厂公章）。  7、支持对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段（需提供相关截图证明并加盖原厂公章）。 |