采购技术参数说明书

1. 项目名称：安全保密软硬件
2. 最高限价（或项目预算）：475万元
3. 采购项目需求
4. 带“★”号条款均为实质性响应指标要求，必须全部响应。若有一项带“★”条款未响应或不满足，均视为非实质性响应招标文件，按无效投标处理；。“▲”为重要参数，允许正偏离，负偏离超过2条按无效投标处理。
5. 技术要求
6. 硬件技术要求

优先选用进入《中国人民解放军信息安全认证产品目录》内产品；厂家投标需备注该设备是否进入《中国人民解放军信息安全认证产品目录》

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **单位** | **数量** | **参数建议 ▲ ★** |
| **（一）外网安全保密** | | | | |
| 1 | 下一代防火墙 | 台 | 1 | 1.国产化CPU、国产操作系统、≥16个千兆电口，≥16个万兆光口，≥2个100GE光口，≥2个扩展槽，冗余电源，网络处理能力≥35Gbps，并发连接≥1000万，每秒新建连接≥40万/秒； 2.访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 3.支持二层模式（透明模式）、三层模式（路由和NAT模式）和混合模式； 4.支持链路聚合功能、接口状态同步功能； 5.支持静态路由、等价路由，支持RIP、RIPng；OSPFv2/v3动态路由协议； 6.支持自动生成安全策略。统一管理平台可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率； 7.支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查； 8.支持基于不同安全策略设定会话长连接老化时间； 9.支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备； 10.支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的CPU和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙； 11.需与现网统一安全管理平台无缝对接，实现联动处置，确保服务器区域安全；支持与态势感知平台无缝对接，实现应急联动处置； 为保证产品质量，投标产品须在《军用关键软硬件自主可控产品名录（最新版）》，且具备《军用信息安全产品认证证书》 |
| 2 | 下一代防火墙 | 台 | 1 | 1.国产化CPU、国产操作系统、≥16个千兆电口，≥16个万兆光口，≥2个100GE光口，≥2个扩展槽，冗余电源，网络处理能力≥35Gbps，并发连接≥1000万，每秒新建连接≥40万/秒； 2.访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 3.支持二层模式（透明模式）、三层模式（路由和NAT模式）和混合模式； 4.支持链路聚合功能、接口状态同步功能； 5.支持静态路由、等价路由，支持RIP、RIPng；OSPFv2/v3动态路由协议； 6.支持自动生成安全策略。统一管理平台可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率； 7.支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查； 8.支持基于不同安全策略设定会话长连接老化时间； 9.支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备； 10.支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的CPU和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙； 11.需与现网出口安全防护设备实现双机虚拟化，提高冗余高可靠性，确保学术网出口安全；支持与态势感知平台无缝对接，实现应急联动处置； 为保证产品质量，投标产品须在《军用关键软硬件自主可控产品名录（最新版）》，且具备《军用信息安全产品认证证书》。 |
| 3 | 入侵检测 | 台 | 1 | 1.国产化CPU、国产操作系统、≥16个千兆电口，≥16个万兆光口，≥2个100GE光口，≥2个扩展槽，冗余电源，处理性能≥35G，并发连接数≥1000万，每秒新建连接数≥40万； 2.内置丰富的入侵检测特征库，可针对SQL注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量不少于9000条； 3.内置丰富的病毒特征库，可针对文件感染型、蠕虫、木马等类型病毒进行检测和阻断，特征规则数量不少于250万条； 4.支持对HTTP协议进行检测，检测JAVA Applets、ActiveX等插件，检测上传或者下载的文件大小以及文件类型，支持自定义关键字检测； 5.支持暴力破解检测，至少支持数据库、RDP、POP3、HTTP、VNC、Rlogin、Weblogic、SMB、SMTP、FTP、IMAP、Telnet、SSH等协议的检测 6.支持对挖矿行为进行检测与防护，能够对挖矿通信、矿池连接、挖矿病毒传播行为进行统计，能够展示挖矿通信源IP、挖矿通信服务器IP、矿池IP、矿池域名、中毒地址、投毒地址等信息top排行，支持按最近一天、最近两天、最近一周、最近一个月进行排行展示，展示的内容包括IP/域名以及攻击数量； 7.支持对DNS的Request Flood、Reply Flood、IP、域名等形式的DDoS检测； 8.支持指纹方式的DDoS检测，可以根据报文长度、报文ID、TTL、源IP、目的IP、序列号、确认号、源端口、目的端口、flag标记等指纹进行检测设定； 9.支持威胁情报功能，需包含恶意软件、C&C节点、钓鱼网址、僵尸网络、数字货币、垃圾邮件等情报，数量不少于1000万，支持自定义基于域名和IP的威胁情报，支持配置基于域名和IP的白名单，减少情报误报的影响； 10.支持与防火墙进行联动，可以设定阻断方向为源到目的、目的到源、双向，自定义阻断时间； 11.支持与漏洞扫描设备进行联动，可以获取主机的漏洞信息； 为保证产品质量，投标产品须在《军用关键软硬件自主可控产品名录（最新版）》，且具备《军用信息安全产品认证证书》。 |
| 4 | Web应用防火墙 | 台 | 1 | 1.标准机架式1U设备，网络层吞吐量：≥35G，并发连接数：≥410万；配置≥3年入侵防御特征库升级，≥3年Web应用防护规则库升级，≥3年产品质保和软件升级。 2.配置双电源；接口要求：≥16千兆电口、≥6万兆光口（配置4个万兆多模光模块）。 3.为适应IPV6网络改造，须同时支持IPV4及IPV6协议。 4.支持自定义安全策略，安全策略组功能；可针对源、目的、协议、用户、时间等进行访问控制策略配置。 5.路由协议：支持动态地址转换、静态地址转换以及端口地址转换功能，支持 OSPFv2/v3 等路由协议。 ▲6.为应对严峻的勒索病毒攻击，支持针对勒索病毒进行检测并开展防御。（提供对应功能截图及“勒索病毒”相关知识产权证书） 7.支持通过TCP代理及SSL代理等方式对https进行解密。 8.支持ftp协议命令控制功能，避免互联网服务遭受篡改等攻击。 ▲9.为应对最新的网络攻击，产品应支持对最新的勒索、挖矿、无文件攻击等未知威胁进行检测，产品需具备未知威胁检测能力。（提供“未知威胁”相关知识产权证书） ▲10.为防止学校内网业务受扫描攻击，产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁，所投产品须具备漏洞防扫描功能。（需提供提供具备CNAS资质认证的第三方检测机构的关于“漏洞防扫描”功能项的产品检测报告，附带CNAS对检测机构的认证证明并加盖投标人公章） 11.产品支持X-Forworded-For字段检测，并对非法源IP进行日志记录和联动封锁。 |
| 5 | 堡垒机 | 台 | 1 | 1、配置≥6个千兆电口，≥4个千兆光口，≥2个扩展槽位，16G内存，4T存储空间，冗余电源；配置300个主机/设备许可，最大可扩容到1000，用户数不限制，最大字符并发连接≥400，最大图型并发连接≥150。 2、支持第三方证书用户自行上传用作校验的CA证书和CRL列表。 3、支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长TOP10、今日告警总数、今日运维指令TOP10等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况。（提供功能截图并加盖制造商鲜章） 4、支持改密结果可通过邮箱、FTP方式外发；密码采用密码信封加密保存，以保证安全性；支持密钥加密和明文分段发送。 5、提供授权关系查看功能，图形化直观展示用户、资产、协议、账号的授权关系。 6、支持Xshell、Xftp、SecureCRT客户端的session文件导出。 7、支持会话请求远程协助，且协同会话保持实时同步。 8、支持全文审计检索，可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。 9、支持图形化查看用户的运维记录，查询结果以鱼骨图按照时间倒序自上而下而下展示，每个时间点详细记录运维资产、运维用户、账号、协议、会话时长等详细信息。 10、系统内置丰富报表统计模板：协议运维排名、资产运维次数top10、资产运维趋势top10、用户运维趋势top10、协议运维趋势、用户运维次数top10、指令分布top10、top10指令资产分布、指令用户分布top10、指令资产账号分布、指令排名、指令趋势、风险指令次数、风险指令top10等多种类型报表模板。 11、投标产品制造厂商应具备中国电子信息行业联合会颁发的《信息系统建设和服务能力等级证书》，且达到优秀级（CS4）；（提供证书复印件并加盖制造商鲜章） |
| 6 | 邮件防泄漏 | 台 | 1 | 1、配置≥6个千兆电口，≥4个千兆光口，冗余电源，2个扩展槽位，64G内存，2T存储空间，7层吞吐率：1Gbps，7层应用检测率：300Mbps/S。 2、支持与防火墙联动，支持旁路部署与防火墙联动配置，基于内容检测然后反馈给防火墙需要阻断的地址或者URL，且通过防火墙实现阻断效果。（提供功能截图并加盖制造商鲜章） 3、支持MTA（邮件代理）模式解析邮件数据，支持MTA转发、反射模式配置。 ▲4、支持识别解析邮件头、主题、正文、附件、发件人、收件人、抄送人、密送人等；阻断模式支持SSL加密协议解析，支持加密邮件（TLS）敏感信息检测。（提供功能截图并加盖制造商鲜章） 5、支持文档指纹检测，支持对固定内容格式的文档生成文档指纹，识别外发相似文档。 6、支持识别邮件密送行为，识别邮件中是否包含密送人；支持邮件阻断，发现邮件违规数据后，阻断原始邮件发送，并且发送退信通知发放方，支持自定义退信通知信息、支持重定向退信收件人。 7、支持违规邮件的主题、正文修改，支持解析SMTP、POP、IMAP协议传输违规邮件中主题、正文的内容修改。 8、支持增加、删除邮件收件人；支持违规邮件附件删除。 9、支持邮件审核，支持解析阻断SMTP、POP、IMAP协议传输邮件，并发送审核邮件给管理者，管理者审核通过后，邮件正常外发；支持多级（3级）邮件审批；支持填写审批意见。（提供功能截图并加盖制造商鲜章） 10、支持对FTP、SMTP、HTTP下载的WPS文件（PDF WORD excel ppt格式）添加水印信息，水印信息包括源IP、目标IP、数据传输类型、时间、自定义文本。（提供功能截图并加盖制造商鲜章） |
| 7 | 网络防泄漏系统 | 台 | 1 | 1、配置≥6个千兆电口，≥4个千兆光口，冗余电源，2个扩展槽位，64G内存，2T存储空间，7层吞吐率：1Gbps，7层应用检测率：300Mbps/S。 2、支持与防火墙联动，支持旁路部署与防火墙联动配置，基于内容检测然后反馈给防火墙需要阻断的地址或者URL，且通过防火墙实现阻断效果。（提供功能截图并加盖制造商鲜章） 3、支持nginx代理转发能力，支持SMTP、POP、IMAP、HTTP、HTTPS、FTP协议代理。 4、支持对HTTPS、HTTP、SMTP、POP3、IMAP、FTP、SMB、TELNET、DNS等协议的解析、还原、识别。 5、支持识别文件格式，包括文字格式、图片格式、电子表格格式、演示格式、多媒体格式、封装格式类型；支持自定义添加未预置的文件格式进行识别。（提供功能截图并加盖制造商鲜章） 6、支持图片内容检测，支持通过OCR技术对bmp，jpg，tif，tif2，png、jpeg、pjx、PSD等格式，支持对windows截屏、身份证或者其他证件的扫描件、身份证拍照、快递单扫描件或拍照、海关关单扫描件、保单扫描件、保单拍照、税单扫描件进行识别。（提供功能截图并加盖制造商鲜章） 7、支持机器聚类，手动、自动抓取大量无序文档样本进行聚类分析，生成推荐规则；支持通过上传训练样本（ZIP格式正向、反向源文件），建立检测模型，来判断有违规内容的文件。 ▲8、支持识别文档多层（10层）嵌套方式逃避检测行为：支持的压缩文件类型rar、zip、gz、Bzip2、7z,rar5压缩层数最大10层；支持的word、excle、ppt、pdf、压缩包（rar、zip、gz、Bzip2、7z,rar5）相互嵌套，嵌套层数最大3层。（提供功能截图并加盖制造商鲜章） 9、支持对用户越权访问行为进行审计，通过备案应用的访问账户、账户角色、API接口信息三者关联关系，匹配API调用过程中的字段信息，对违规访问行为进行监控。 10、支持对接第三方水印服务，支持调用第三方水印系统的restful api 添加水印信息。 |
| 8 | 态势感知（含探针） | 台 | 1 | 1.平台数据处理能力≥10G；CPU≥10核X 2颗，≥256G内存，≥480G SSD，≥36T SATA，≥2个千兆电口，≥2个万兆光口，冗余电源； 2.实现对全网数据的采集与分析，同时接受各类设备的告警日志进行关联分析，展现全网的安全状况； ★3.与本次新建安全设备、现网安全设备无缝对接，实现联动处置，自动下发处置命令到各安全设备，实现秒级应急处置，确保学术网各边界安全； 4.支持攻击关系分析，以攻击者视角展示针对每个攻击目标所采用的攻击手段的攻击关系视图，同时展示攻击事件的攻击手段TOP统计，以及每种攻击手段的描述说明，并支持下钻； 5.支持攻击详情分析，基于受害者、目的端口、时间段、攻击手段、攻击类型、攻击级别、攻击名称等七个维度进行网络攻击日志检索，可查看本次攻击事件涉及的网络攻击的详细情况，以及下载原始攻击数据包； 6.支持AI判真功能，存在多个攻击手段的攻击事件显示为AI判真事件，AI判真事件存在AI判真标识； 7.支持资产画像功能，可显示资产的外部访问的流量统计信息、访问的源IP、目的IP、访问方式和流量趋势；内部访问的流量统计信息、访问的源IP、目的IP、访问方式和流量趋势；外连访问的流量统计信息、访问的源IP、目的IP、访问方式和流量趋势； 8.支持AI自动处置功能，当处置列表有昨天的处置信息，今天没有处置信息时，攻击事件支持自动按照昨天的处置历史信息进行处置，攻击事件被盖上相应的处置标签，历史处置记录按时间轴形式显示处置时间、设备信息或备注信息，处置列表新增一条处置信息，显示处置目标、所属机构、数据来源、威胁等级、威胁资产数量、事件类型、处置来源、处置手段、处置时间、生效日期和备注信息； 9.全流量探针：CPU≥8核X 2颗，≥64G内存，≥4T SATA，≥2个千兆电口，≥2个万兆光口，冗余电源； 10.通过旁路镜像采集网络全部流量，支持在线支持同时接入多个镜像口，每个口相互独立不影响，设备部署不影响原有网络结构； 11.支持主机渗透攻击检测、支持Web渗透攻击检测、支持隐匿隧道通信检测、支持挖矿病毒检测； 12.支持全流量报文的存储，以及远程调取、查看和下载功能； 支持全流量存储规则配置，至少包括：会话保存天数和深度、系统预留空间、协议保存优先级，其中能设置优先级的协议有ICMP、ICMP6、TCP、UDP、SSH、SMTP、IMAP、SMB、SNMP、HTTP、TLS等。 |
| 9 | 数据库审计 | 台 | 1 | 1.吞吐量≥2Gbps，纯数据库流量≥400Mb/s，数据库实例个数≥30个，SQL处理性能≥3W条SQL/s，日志检索性能≥50W条/秒。 2.硬件参数：内存大小≥8G，硬盘容量≥2 TSATA，千兆电口≥6个，万兆光口SFP+≥2个（配置2个万兆多模光模块）。 3.为适应多种数据库，支持市面上主流的数据库，包括Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache，以及国产数据库达梦、人大金仓、南大通用。 ▲4.为方便对数据库操作日志进行查询，支持TB级的日志级查询，过滤选项包括：源IP、客户端程序、源MAC、业务系统、业务主机端口、数据库用户、数据库名、操作类型、表名，并且支持按照时间进行排序和查询。（提供产品界面截图证明并加盖投标人公章） 5.支持完整记录用户数据库会话细节，包括源IP、源端口、源MAC、目的IP、目的端口、数据库用户、数据库类型、操作类型、SQL语句、SQL模版、客户端程序名、响应码、影响行数、返回行数、SQL预计响应时间。 6.支持吞吐量整体状况展示，展示类型包括SQL语句吞吐量排行和变化趋势、SQL操作类型吞吐量排行和变化趋势、数据库用户吞吐量排行和趋势、业务主机吞吐量排行和变化趋势。 7.为多样化展示数据库安全形势，支持实时监控内网数据威胁态势，监控纬度包括通过自定义交互分析设置正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数。 8.支持国产数据库：达梦、人大金仓、南大通用。 9.支持进行管理员权限设置，支持分权管理，并且支持三权分立功能，同时具备管理员操作自我审计功能。 10.支持日志导出到Excel。 11.支持HTTP请求审计，可指定GET、POST、URL、响应码进行精细审计。 12.支持同时审计多种数据库及跨多种数据库平台操作。 ▲13.为进行不同安全规则的检测，规则包括导出可执行程序、系统命令执行、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp\_addrolemember提权、web端sp\_addrolemember提权、查询内置敏感表、篡改内置敏感表导出方式窃取、备份方式窃取、读写注册表等。（提供产品界面截图证明并加盖投标人公章） ▲14.为直观显示数据库访问来源，以曲线连接多点的形式展示用户的访问来源、访问目标、操作类型、操作对象的行为轨迹图。（提供产品界面截图证明并加盖投标人公章） |
| 10 | 漏洞扫描 | 台 | 1 | 1．系统漏扫授权IP数≥1000，WEB漏扫授权URL数≥200；主机漏扫最大并发IP数≥300，WEB漏扫最大并发URL数≥10。含三年产品质保、三年软件。 2．硬件参数：规格：2U，硬盘≥128GB SSD+ 2TB SATA，电源：冗余电源，接口≥6\*GE口+2\*SFP+口（配置2个万兆多模光模块）。 3．为高效进行风险展示，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。 ▲4．为适应不同扫描需求，产品支持全面扫描、资产发现、系统漏洞扫描、弱口令扫描、WEB漏洞扫描、基线配置核查六种任务类型，其中全面扫描支持系统漏洞扫描、WEB漏洞扫描、弱口令扫描同时执行。（提供产品界面截图证明并加盖投标人公章） 5．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。（提供产品界面截图证明并加盖投标人公章） ▲6．为适应等级保护测评规则，按“一个中心、三重防护”的架构展示检测结果，每个检测结果呈现具体问题及整改建议，系统支持手动核查确认、整改后重新检测、以及手动导入全局分析和人工核查报告来对测评报告中的结果进行核查确认，其中手动核查确认支持单项核查确认和批量核查确认。（提供产品界面截图证明并加盖投标人公章） 7．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。 8．支持报表过滤功能，支持从任务类型、任务/资产、风险等级、漏洞/基线类型等角度筛选和过滤报表生成条件。 9．为方便等保管理，支持业务系统登记功能，保护等级支持第二级和第三级，可根据不同域类别添加资产到业务系统中。 ▲10．为帮助学校进行等保初步评估，产品支持提供检测结果综述分析，按照等保2.0的检测项要求，统计客户业务系统存在的不符合、部分符合、符合、待确认、不适用检测项，直观了解自身业务系统合规情况。（提供产品界面截图证明并加盖投标人公章） 11．支持统一管理所有业务系统的合规情况，合规报告可导出业务系统差距报告量化、可视化整改前后的符合情况和安全问题。 |
| 11 | 网络准入系统 | 台 | 1 | 1.物联网场景吞吐（传统FW）≥18G，物联网场景吞吐（开通IPS）≥5.5G；每秒新建连接数≥ 35w；每秒并发连接数≥2000w；视频网接入路数（4M码流，传统FW）≥5000，视频网接入路数（4M码流，开通IPS）≥1500。提供3年质保、3年软件升级。 2.2U，冗余电源，接口:≥16千兆电口+6万兆光口SFP+（配置6个万兆多模光模块）。 3.支持路由、网桥、旁路三种部署模式；支持主备模式的双机部署，设备或网络故障时可自动进行切换。 4.为具有最佳的资产探测效果，须支持主动探测和流量分析两种资产发现方式，可通过SNMP等协议发起探测，并设定探测的目标IP、SNMP版本、团体名等。 5.为保证资产识别准确率，产品可识别IT和IoT混合资产，获取IP、MAC、操作系统、类型、厂商等信息，终端类型包括但不限于： （1）PC、瘦客户机、手机、平板、交换机、路由器、防火墙、无线控制器、服务器等IT资产 （2）摄像头、门禁、打印机、投影仪、VOIP设备、条形码扫描仪等IoT资产。 ▲6.为排查物联网设备中存在的非法外联风险，支持对IT和IoT混合终端进行HTTP流量重定向，通过对其重定向后的访问请求判断其是否存在违规外联行为，可配置流量重定向的时间间隔，支持根据源IP或目标IP进行白名单豁免。（提供产品界面截图证明并加盖投标人公章） ▲7.为根据学校现有视频协议进行准入配置，产品须支持视频协议准入，可识别SIP、RTP、RTCP、RTSP等视频协议，基于协议进行应用层准入，仅允许指定协议入网通信（提供产品界面截图和第三方检测机构出具的检测报告） 8.支持连接外网检查，自动检查PC终端是否能PING通互联网地址，对不满足检查要求的终端强制断网，支持向管理员告警，并弹窗提示用户。 9.支持对IT和IoT混合终端进行主动网络探测，通过终端的响应数据包判断其是否存在违规外联行为，可配置定期检测任务。 10.支持ACL访问控制，基于区域、IP、网络协议、端口号等因素对访问权限进行管控。 ▲11.为对IOT设备进行精准准入，支持IoT协议准入，可识别ONVIF、MQTT等IoT协议基于协议进行应用层准入，仅允许指定协议入网通信。（提供产品界面截图和第三方检测机构出具的检测报告） 12.支持私有视频协议准入，可识别海康、大华、华为等主流IPC摄像头的私有协议，仅允许指定协议入网通信。 13.支持IPS入侵防御，可针对IoT终端和业务进行保护，响应动作包括记录日志、行为拦截、联动封锁等。 14.支持非法外联管控，可设置PC终端访问地址白名单和黑名单，写入终端防火墙ACL策略，实现强访问管控。 15.支持对IT和IoT混合终端进行HTTP流量重定向，通过对其重定向后的访问请求判断其是否存在违规外联行为，并封堵违规外联终端，终端可配置流量重定向的时间间隔，支持根据源IP或目标IP进行白名单豁免。 16.支持对SYN Flood、ICMP Flood、UDP Flood等泛洪攻击检测。 |
| 12 | 入侵防御 | 台 | 1 | 1.机架式设备，冗余电源，配置≥16个千兆电口，≥6个万兆光口(配置4个万兆多模光模块和跳线)。 2、网络层吞吐量≥35G，应用层吞吐量≥20G，防病毒吞吐量≥3.5G，IPS吞吐量≥2.5G，全威胁吞吐量≥1.8G。并发连接数≥410万，HTTP新建连接数≥18万，开启IPS、WAF授权模块，提供三年产品质保，三年软件升级，开启IPS授权模块，提供三年产品质保，三年软件升级，三年包括WEB应用防护识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和URL&应用识别库定期更新。 ▲3.为有效保护学校各项IT资产，产品支持云威胁情报网关技术，通过全球超过30+pop节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品功能截图证明并提供POP节点在线查询链接和具备CMA/CNAS标识的第三方检测报告，加盖投标人公章） 4.为防止核心专业如药理学专业学生访问特殊药物符号被误阻断，支持自定义语义引擎白名单功能，包含通过Web应用防护规则、URL参数、IP地址、Webshell上传防护、SQL、XSS、后门扫描的方式排除，防止访问特殊符号被误阻断。 5.新型高级攻击手段可能将异常攻击手段隐藏在HTTP头部字段，为实现特殊字段检测能力，支持识别HTTP异常，包含HTTP方法过滤、HTTP头部字段Referer、User-Agent等注入检测、Host检测、URL溢出检测、POST实体溢出检测、HTTP头部溢出检测、range字段防护、multipart头部字段异常检测，防范异常攻击手段隐藏在HTTP头部字段，实现特殊字段检测能力。 6.支持自定义Web应用防护规则，通过正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。 7.支持超过6200种防护规则，其中Web应用防护规则超过4900种，Web应用漏洞攻击防护规则超过1300种，提升业务系统应用层防护能力。 8.支持语义引擎用于检测Web攻击，能针对不同类型的Web攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测，保证应用层特殊语法攻击准确识别（提供产品功能截图，加盖投标人公章）。 9.支持https解密功能，TCP、SSL两种代理都要求支持。 10.为提前防护勒索病毒加密学校教学、实验核心数据，支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略，提前防护勒索病毒加密核心数据（出具公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局之中任意一家检测机构出具关于“勒索病毒”的相关证书复印件证明功能有效性，加盖投标人公章）。 11.为了方便学校运维老师灵活设置策略路由，支持路由类型、协议类型、网络对象、国家地区等条件进行自动选路的策略路由，支持不少于3种的调度算法，至少包括带宽比例、加权流量、线路优先等，方便管理部门灵活设置策略路由。 12. 支持Cookie攻击防护功能，并通过日志记录Cookie被篡改，保障学校业务的安全性（出具符合功能要求的承诺函或者证明文件并加盖投标人公章，签订合同前需提供具备CMA/CNAS认证的第三方权威机构关于“Cookie攻击防护”功能项的产品检测报告，加盖原投标人公章。） 13.支持对压缩病毒文件进行检测和拦截，且压缩层数支持15层（含）以上，保障业务系统互访过程中各种压缩文件的识别能力，避免压缩文件中存在病毒导致业务中断。 14.支持各类异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护、WinNuke攻击防护等攻击类型。 15.支持管理员双因子认证，可以通过用户密码和Key等不同方式登陆产品管理界面，提升管理员认证的安全性和灵活性。 16、产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁（需提供产品功能截图证明和具备CMA/CNAS标识的第三方检测报告，加盖投标人公章）。 17.产品支持云端未知威胁主动探测技术，实现5min内未知威胁情报全网设备下发（需提供产品功能截图证明并提供具备CMA/CNAS标识的第三方检测报告，加盖投标人公章） 18.满足等保要求：安全区域边界-访问控制、安全计算环境-入侵防范的要求。 |
| 13 | 日志审计 | 台 | 1 | 1.2U，产品不少于6个千兆SFP口，2个万兆SFP+口（配置2个万兆多模光模块），冗余电源。 2.配置不少于 300 个日志接入授权，支持扩展为450个接入授权，日志处理性能不少于 3500 EPS.，硬盘容量不少于128G minisata+4T SATA\*2，可用存储量不低于4TB（RAID1 模式） 3.支持自动识别采集设备、支持设备异常告警、设备异常告警发送邮件或第三方接口。 4.支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志(提供截图证明文件，并加盖投标人公章)。 5.支持TLS加密方式进行日志传输，支持日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量(提供证明材料并加盖投标人公章)。 6.支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括base64、Unicode、GBK、HEX、UTF-8等(提供证明材料并加盖投标人公章)。 7.支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析。 8.支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件。 9.支持资产全生命周期管理，资产入库审核、资产离线风险识别、资产退库、资产数据更新，责任人管理机制等，支持自定义资产标签、属性。 10.支持对IPv4/ipv6对象的自动发现功能，对自动发现的设备可以修改、删除或转为资产。 11.支持可视化展示，包括数据分布、安全事件趋势图、关联规则告警趋势图、接入设备概况等，可提供设备专项分析场景。如防火墙外部攻击场景分析、VPN账号异常场景分析、Windows服务器主机异常场景分析等，通过设备专项页面对每一台设备安全情况深度专业化分析(提供证明材料并加盖投标人公章) 12.支持POC测试工具一键生成数据,验证日志数据采集是否成功，避免设备部署后采集失效但不被发现等风险(提供证明材料并加盖投标人公章)。 13.支持等保合规检测，用户可自查设备是否满足等保要求。 14.支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射(提供截图证明文件，并加盖投标人公章) |
| 14 | 零信任 | 台 | 1 | 1.加密流量≥480Mbps，并发用户数（个）≥4800，https并发连接数（个）≥48000，新建连接数（个/秒）≥320。提供3年质保和软件升级、1套零信任访问控制系统软件。 2.内存大小≥16G，硬盘容量≥128G SSD，电源：冗余电源，接口≥6千兆电口+4千兆光口SFP。 3.支持首次登录强制修改密码，支持配置密码最长使用周期（到期后需要修改密码）。 4.为了提高系统可靠性，保障单台设备故障时系统仍可正常运行，代理网关应支持本地集群部署，且最少2台设备即可组建集群，单集群的最大节点数量不得少于4台；本地集群组建时，集群中的节点可承载工作负载功能，不需要依赖其它外置设备。 5.支持通过域名访问内网业务，以及内外网访问业务时，使用内网的DNS解析，内外网访问统一(提供证明材料并加盖投标人公章)。 6.支持接入IP限制（即接入控制台的IP白名单），限制后，从浏览器、SSH或SNMP等方式接入管理台时，都必须在上述IP白名单范围内接入。 ★7.支持用户访问日志（用户、源IP、URL、时间、get请求、post请求、端口）。支持管理员操作日志（含管理员、接入IP、时间、管理行为、对象）。支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，以便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全（应包含帐号首次登录、异常时间登录、非常用地点登录、弱密码登录、爆破登录、闲置帐号登录、帐号在新终端登录等）、中间人攻击、SPA安全（应包含SPA端口扫描、SPA爆破攻击、SPA敲门伪造、SPA重放攻击、SPA安全码泄漏等）、cookie劫持等。支持将设备安全事件单独记录在设备安全日志中，事件类型包括但不限于：接口扫描、接口webshall攻击、接口参数爆破、接口越权调用等设备API防护日志。(提供证明材料并加盖投标人公章) 8.支持将用户访问零信任系统的WEB资源访问流量解密后镜像给外部网络流量分析系统，如态势感知等设备，以完善系统的用户行为审计溯源能力，提升设备自身的安全性。(提供证明材料并加盖投标人公章) 9.为方便管理员统筹查看管理零信任系统的整体运行状态，支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告。支持在设备上查看及下载巡检报告。报告应至少包含检测项、检查状态、存在的问题描述、建议改进措施等。 10.支持API防护检查：包括但不限于：支持API接口爆破检查；支持API接口越权调用；支持API接口扫描；支持API Web Shell攻击。 11.提供国家密码管理局商用密码检测中心出具的含有“访问控制系统”字样，符合GM/T 0024标准或GM/T 0025标准要求，以及符合GM/T 0028《密码模块安全技术要求》第二级的《商用密码产品认证证书》。(提供证明材料并加盖投标人公章) 12.为保证零信任产品的架构规范性，应提供中国信通院认证的零信任SDP设备Zero Trust Ready证书。(提供证明材料并加盖投标人公章) 13.为证明产品的软件成熟性与先进性，应提供由中国软件协会颁发的年度优秀软件产品证书。(提供证明材料并加盖投标人公章) 零信任控制中心 1.并发用户数（个）≥8000，新建用户数（个/秒，本地认证）≥200；规格：2U，内存大小≥16 G，硬盘容量≥240G SSD，冗余电源，接口≥6千兆电口+4千兆光口SFP+2万兆光口SFP+（配置2个万兆多模光模块）。提供3年质保和软件升级、1套零信任访问控制系统软件、2000个零信任接入授权。 2.为了满足灵活部署的要求，控制中心应支持单臂模式、路由模式部署。 3.为了提升师生使用体验，便于用户无感接入，控制中心应支持跨平台免插件访问，支持多资源（http/https/websocket等）免客户端接入。 4.支持新增/删除/修改管理员角色，内置审计管理员、安全管理员、系统管理员角色；通过管理员角色配置，实现管理员分级分权。 5.支持虚拟IP池，用户首次连接时分配虚拟IP，后续用户与虚拟IP绑定，便于用户访问行为可追溯。 6.为了保障学校当前或者后期在国产化终端上的正常业务访问，零信任客户端应兼容主流国产硬件CPU的国产操作系统终端，需提供国产操作系统与零信任投标人的兼容性证明，包括但不限于麒麟V10×龙芯、麒麟V10×龙芯LoongArch、麒麟V10×飞腾、麒麟V10×鲲鹏、麒麟V10×兆芯、麒麟V10×海光、麒麟V10×海思麒麟；统信V20×龙芯（3A3000、3A4000）、统信V20×龙芯（3A5000）、统信V20×飞腾、统信V20×鲲鹏、统信V20×海光、统信V20×兆芯等。（提供证明材料并加盖投标人公章） 7.支持终端环境诊断排查，提供终端诊断工具，支持对当前终端的基本环境进行扫描和一键修复，便于员工自行排查修复终端问题，减少IT运维人员工作。 8.防机器人输入，提供强安全性的点击图像校验码机制，图形校验码支持中文和英文。 9.支持防爆破、配置同IP用户连续登录错误超过上限时锁定IP，并于指定时长后自动恢复。 ▲10.为了提高系统可靠性，保障单台设备故障时系统仍可正常运行，控制中心应支持本地集群部署，且最少2台设备即可组建集群，单集群的最大节点数量不得少于4台；本地集群组建时，集群中的节点可承载工作负载功能，不需要依赖其它外置设备。（提供证明材料并加盖投标人公章） 11.为提升终端用户使用的便利性，零信任系统应支持跟同品牌桌面云服务器进行单点登录对接，实现仅需在零信任进行认证即可直接进入云桌面进行业务办公，无需重复验证。 12.通过WEB模式，可以支持基于http或https协议代理访问业务资源，支持发布IP或域名形式的后端服务器地址，可配置业务应用的具体访问URL路径。为了保持用户访问应用体验的一致性，后端服务器地址需支持多地址配置；为适应较复杂的内外网访问场景，WEB应用的前端访问地址应支持多地址访问。存在前置代理设备的场景，还应支持从XFF字段获取源IP。 13.为提升业务应用的数据安全性，零信任系统应支持针对发布的WEB应用开启WEB水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用，有效预防数据泄露。 14.对于一些主要在主站点中点击使用的子站点WEB业务系统，且子站点跟主站点业务系统权限一致的场景，为简化管理员配置，零信任系统应支持开启依赖站点功能。为方便业务快速上线，还应支持自动采集站点功能对依赖站点进行梳理。（提供证明材料并加盖投标人公章） 15.为了不改变师生原有使用习惯，保障师生的使用体验，需支持以下主流浏览器访问WEB资源： a、支持IE8及以上版本浏览器访问WEB资源 b、支持Chrome 69及以上版本访问WEB资源 c、支持Edge、Firefox、Opera、Safari等其他主流浏览器访问WEB资源 d、支持微信内置浏览器、钉钉内置浏览器访问WEB资源 e、支持Android、iOS各大手机投标人的自带浏览器访问WEB资源 f、支持国产操作系统浏览器接入并访问WEB资源 （要求提供实际效果演示截图证明） 16.支持配置单位的CDN作为零信任客户端下载地址，以降低设备本身的非业务访问带宽压力。当客户端通过CDN加速等代理方式接入访问业务系统时，支持获取CDN加速前的访问IP，并在日志中记录此IP为客户端IP。 17.为了方便快速运维排障，支持用户在客户端自助进行日志收集。支持管理员在控制台远程获取在线终端的日志，若终端不在线时支持加入排队列表，排队列表中的终端上线后自动收集日志。 |
| **（二）内网安全保密** | | | | |
| 1 | 下一代防火墙 | 台 | 2 | 1.国产化CPU、国产操作系统、≥16个千兆电口，≥16个万兆光口，≥2个100GE光口，≥2个扩展槽，冗余电源，网络处理能力≥35Gbps，并发连接≥1000万，每秒新建连接≥40万/秒； 2.访问控制策略支持基于源/目的IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式； 3.支持二层模式（透明模式）、三层模式（路由和NAT模式）和混合模式； 4.支持链路聚合功能、接口状态同步功能； 5.支持静态路由、等价路由，支持RIP、RIPng；OSPFv2/v3动态路由协议； 6.支持自动生成安全策略。统一管理平台可通过对流量日志的统计整理，自动生成安全策略，并下发给防火墙设备，提高运维人员工作效率； 7.支持通过命令行的方式对设备内部数据流进行分析，可快速定位造成故障的防火墙内部功能模块，便于进行故障排查； 8.支持基于不同安全策略设定会话长连接老化时间； 9.支持多虚一部署，可将两台物理设备虚拟化成一台逻辑上的设备； 10.支持将一台逻辑上的设备虚拟化成多个虚拟防火墙，并可查看各虚拟防火墙的CPU和内存利用率、新建、并发和吞吐信息，并可单独重启特定虚拟防火墙； 11.需与现网统一安全管理平台无缝对接，实现联动处置，确保服务器区域安全；支持与态势感知平台无缝对接，实现应急联动处置； 为保证产品质量，投标产品须在《军用关键软硬件自主可控产品名录（最新版）》，且具备《军用信息安全产品认证证书》 |
| 2 | 入侵防御 | 台 | 1 | 1.国产化CPU、国产操作系统、≥16个千兆电口，≥16个万兆光口，≥2个100GE光口，≥2个扩展槽，冗余电源，处理性能≥35G，并发连接数≥1000万，每秒新建连接数≥40万； 2.内置丰富的入侵检测特征库，可针对SQL注入、木马后门、漏洞利用等恶意攻击进行检测和阻断，特征规则数量不少于9000条； 3.内置丰富的病毒特征库，可针对文件感染型、蠕虫、木马等类型病毒进行检测和阻断，特征规则数量不少于250万条； 4.支持对HTTP协议进行检测，检测JAVA Applets、ActiveX等插件，检测上传或者下载的文件大小以及文件类型，支持自定义关键字检测； 5.支持暴力破解检测，至少支持数据库、RDP、POP3、HTTP、VNC、Rlogin、Weblogic、SMB、SMTP、FTP、IMAP、Telnet、SSH等协议的检测 6.支持对挖矿行为进行检测与防护，能够对挖矿通信、矿池连接、挖矿病毒传播行为进行统计，能够展示挖矿通信源IP、挖矿通信服务器IP、矿池IP、矿池域名、中毒地址、投毒地址等信息top排行，支持按最近一天、最近两天、最近一周、最近一个月进行排行展示，展示的内容包括IP/域名以及攻击数量； 7.支持对DNS的Request Flood、Reply Flood、IP、域名等形式的DDoS检测； 8.支持指纹方式的DDoS检测，可以根据报文长度、报文ID、TTL、源IP、目的IP、序列号、确认号、源端口、目的端口、flag标记等指纹进行检测设定； 9.支持威胁情报功能，需包含恶意软件、C&C节点、钓鱼网址、僵尸网络、数字货币、垃圾邮件等情报，数量不少于1000万，支持自定义基于域名和IP的威胁情报，支持配置基于域名和IP的白名单，减少情报误报的影响； 10.支持与防火墙进行联动，可以设定阻断方向为源到目的、目的到源、双向，自定义阻断时间； 11.支持与漏洞扫描设备进行联动，可以获取主机的漏洞信息； 为保证产品质量，投标产品须在《军用关键软硬件自主可控产品名录（最新版）》，且具备《军用信息安全产品认证证书》。 |
| 3 | 数据库防火墙 | 台 | 1 | 1、配置≥6个千兆电口，≥4个千兆光口，≥2个扩展槽位，1个HA口，冗余电源；DB最大并发数≥30000；SQL处理能力≥35000/s。 2、能够按照SQL操作类型包括Select、Insert、Update、Delete,对象拥有者，及基于表、视图对象、列进行权限控制，支持黑白名单的访问控制，能够以IP地址、用户、应用程序、时间段为授权单位，进行访问控制。 ★3、可以对指定的数据库基于名称、基于数据内容进行敏感数据扫描，发现数据库中存在的敏感数据的字段及其在服务器、数据库的分布情况（提供功能截图，并加盖制造商鲜章） 4、审计记录应包括：会话的终端信息（IP、MAC、Port、工具名、数据库用户名）、会话的主机信息（IP、MAC、Port、数据库名（实例名））、操作信息：操作类型（DDL、DML、DCL等）、操作时间、执行时长、操作成功与失败、受影响行数、操作对象（表、函数、存储过程等名称）、SQL语句等。 5、支持变量绑定值的记录，能够记录查询中Bind Variable的变量的名字和Bind Variable的数值；能够支持跨语句、跨多包的绑定变量审计，可以实现交叉关联分析 6、支持对数据库进行健康评分，系统界面可以显示数据库的用户、缓冲区击中率、共享内存、索引效率、查询统计、查询缓冲命中率等信息，支持设置数据库状态参数阈值，触发阈值时可快速告警。 7、可以根据常用端口号、自定义端口号发现指定网段范围内存在的数据库服务，并可直接将发现的数据库服务直接加入到防护引擎（提供功能截图，并加盖制造商鲜章） 8、内置自动告警设置，支持系统资源监控与告警；支持敏感语句告警策略；支持风险操作、SQL注入、漏洞攻击告警等等。告警必须提供级别设定，至少提供致命、高风险、中风险、低风险4种告警级别，支持短信、SYSLOG、SNMP 、邮件、FTP等多种事件告警和提示方式 9、支持主主、主备模式部署，支持HA双机主备自动切换，支持策略同步、会话同步机制，保障多设备间的一致性，支持软硬件bypass功能，可自动启动和关闭网口间bypass导通，保障系统异常环境下的网络畅通。 |
| 4 | 堡垒机 | 台 | 1 | 1、配置≥6个千兆电口，≥4个千兆光口，≥2个扩展槽位，16G内存，4T存储空间，冗余电源；配置300个主机/设备许可，最大可扩容到1000，用户数不限制，最大字符并发连接≥400，最大图型并发连接≥150。 2、支持第三方证书用户自行上传用作校验的CA证书和CRL列表。 3、支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长TOP10、今日告警总数、今日运维指令TOP10等信息，方便管理员实时查看系统运行情况掌握资产会话连接情况。（提供功能截图并加盖制造商鲜章） 4、支持改密结果可通过邮箱、FTP方式外发；密码采用密码信封加密保存，以保证安全性；支持密钥加密和明文分段发送。 5、提供授权关系查看功能，图形化直观展示用户、资产、协议、账号的授权关系。 6、支持Xshell、Xftp、SecureCRT客户端的session文件导出。 7、支持会话请求远程协助，且协同会话保持实时同步。 8、支持全文审计检索，可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。 9、支持图形化查看用户的运维记录，查询结果以鱼骨图按照时间倒序自上而下而下展示，每个时间点详细记录运维资产、运维用户、账号、协议、会话时长等详细信息。 10、系统内置丰富报表统计模板：协议运维排名、资产运维次数top10、资产运维趋势top10、用户运维趋势top10、协议运维趋势、用户运维次数top10、指令分布top10、top10指令资产分布、指令用户分布top10、指令资产账号分布、指令排名、指令趋势、风险指令次数、风险指令top10等多种类型报表模板。 11、投标产品制造厂商应具备中国电子信息行业联合会颁发的《信息系统建设和服务能力等级证书》，且达到优秀级（CS4）；（提供证书复印件并加盖制造商鲜章） |
| 5 | API安全监测 | 台 | 1 | ▲1.应用层数据处理能力≥3Gbps，CPU≥10核X 2颗，≥256G内存，硬盘≥16T，≥2个千兆电口，≥2个万兆光口，冗余电源； 2.实现系统全局API接口调用数据的检测，发现潜在的API资产并可进行安全评估； 3.支持资产的汇总分析，包含应用、接口、接口状态、接口类型等维度的统计分析，同时支持应用、接口的联动展示； 4.支持基于接口监测审计结果，形成接口资产清单，并统计每天接口的访问情况； 5.支持根据接口访问情况，对接口状态进行分析、自动变更； 6.支持对接口进行画像分析，自动关联接口的访问审计样例信息，包含请求头、请求参数、请求体、响应头、响应体等信息； 7.支持从接口的统计概览、访问日志、关联风险等维度进行接口画像，了解接口的访问源、数据标签、访问情况和风险情况等信息； 8.支持对应用进行画像分析，了解应用的接口、账号、风险情况； 9.支持查看应用下的接口状态、接口类型、数据标签、当天的访问者分布情况，以及风险Top5分布情况； 10.支持多维度的追踪溯源分析，包括线索溯源、账号溯源、源IP溯源、条件溯源等，并支持溯源分析结果下载； 11.支持基于具体数据内容的线索溯源，溯源结果从访问者、访问接口、访问轨迹等维度进行分析呈现，可以查看不同访问者、访问不同接口的轨迹溯源信息，同时支持对线索轨迹种的数据进行举证分析； 12.支持对账号进行追踪溯源，了解目标账号在溯源期间所发生的风险、访问的接口/数据情况，掌握目标账号的风险与访问轨迹； 13.支持对访问源地址进行追踪，从时间溯源、风险概况、访问接口、数据传输等多个维度进行溯源总览，同时列举该源IP在溯源期间产生的风险清单以及访问日志清单； 14.支持源IP、应用、账号、接口为条件的追踪溯源，将溯源期间内的风险、访问接口、数据传输等进行汇总分析，了解溯源期间发生的访问行为和风险情况； 支持与态势感知平台无缝对接，支持资产、风险、攻击威胁自动关联； |
| 6 | 上网行为管理 | 台 | 1 | 1.国产CPU，产品不少于6个以太网电口，2个SFP+口（配置2个万兆多模光模块），支持2个USB口和1个RJ45串口，冗余电源，128G SSD+960G SSD固态硬盘；含三年产品质保、三年软件升级、三年规则库升级 2.网络层吞吐量≥ 18Gbps，应用层吞吐量≥4.5 Gbps，支持用户数≥25000，每秒新建连接数≥4万,最大并发连接数≥180万。 3.为适应用户侧环境，支持路由模式（NAT、路由转发、DHCP、GRE、OSPF）、网桥模式（多路桥接模式）、旁路模式。 4.为满足后期扩展，支持两台及两台以上设备同时做主机的部署模式。 2．为适应IPV6改造，支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6。 3．为进行上网质量评估，支持针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示访问质量差的用户名单，支持对单用户进行定向web访问质量检测。（提供产品界面截图证明并加盖投标人公章） ▲4.为保障可视化分析展示，支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行。（提供产品界面截图证明并加盖投标人公章） 5．为保证应用识别率，设备内置应用识别规则库，支持超过9000条应用规则数、支持超过6000种以上的应用；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制。 ▲6．为抑制P2P下载对网络的影响，支持减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题。（提供产品界面截图证明并加盖投标人公章） 7.设备内置海量预分类的URL地址库，能够针对各种URL类型做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制；（提供产品界面截图证明并加盖投标人公章） 8．基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中。（提供产品界面截图证明并加盖投标人公章） 9．支持应用管理，设备内置应用识别规则库，支持超过9000条应用规则数，支持超过6000种以上的应用，并保持每两个星期更新一次，保证应用识别的准确率；支持根据标签选择应用，并支持给每个应用自定义标签；支持根据标签选择一类应用做控制。（提供产品界面截图证明并加盖投标人公章） 10．支持针对特权用户配置免认证key、免审计key、免控制key。（提供产品界面截图证明并加盖投标人公章） 支持发现私接路由（或者共享软件等）共享网络的行为；支持自定义配置终端数量和冻结时间；支持“仅统计电脑”和“统计所有终端”两种模式;；支持可选“冻结IP”还是“冻结用户名”；支持添加信任列表；支持显示以IP或用户名的维度统计一段时间内的趋势图。  11.支持首页分析显示接入用户人数、终端类型。 12.支持根据访问的URL和网页关键字进行网页过滤。 13.可设置四类管理员，分别为系统管理员、安全管理员、审计管理员，以及多种权限的超级管理员。 ▲14.为避免校内人员访问钓鱼网站，产品须支持在上网终端与被访问网站中间通过SSL解密，使经过SSL加密的数据可被安全网关捕获，从而防范钓鱼网站访问。（须提供关于“防范钓鱼网站”相关的自主知识产权证明，并加盖投标人公章） ▲15.为遏制私接路由进行共享上网的行为，产品须支持发现私接路由（或者共享软件等）共享网络的行为（须提供关于“防止共享上网”相关的自主知识产权证明，并加盖投标人公章） |
| 7 | 数据库审计 | 台 | 1 | 1、配置≥6个千兆电口，≥4个千兆光口，≥2个扩展槽，32G内存，2T存储空间，可审计流量：500Mbps/S，SQL处理能力：30000条/s，日处理能力1000万条，不限制数据库实例。 2、支持Oracle、SQLServer、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata等数据库系统；支持Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis等国际主流数据库系统；支持KingBase、DaMeng、Oscar、GBase、Inspur\_KDB、Highgo、GaussDB等国内主流数据库系统。 3、HTTP协议支持按HTTP访问域、URL、请求类型、请求文件、Cookie、返回码等34个分项作为查询和统计的条件。 4、支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。 5、支持数据库请求和返回的双向审计，特别是返回字段和结果集、返回码、SQL错误信息、返回行数、执行时长等内容。 6、支持自定义时间条件进行各个数据库的会话趋势、SQL操作趋势、安全趋势、访问源趋势的图表展示。 7、以饼图展示正常SQL与慢SQL占比情况、TOP10慢SQL的详细分析：TOP排名信息、事件ID、数据库名、目的ip、协议类型、源ip、sql响应时间、操作类型、具体sql语句等要素。 8、支持以姓名、部门、域名、主机名、源MAC、邮箱、电话、数据来源等要素为条件的实名审计。 9、支持会话回放功能,并至少支持0.5倍速、1倍速、1.5倍速、2倍速、4倍速五级播放速度调节。（提供功能截图并加盖制造商鲜章） 10、支持历史版本回退功能，系统内建历史版本库不少于3个。 11、支持国密算法SM2/SM3/SM4的红莲花、密信等安全浏览器登录管理设备。（提供功能截图并加盖制造商鲜章） |
| 8 | 漏洞扫描 | 台 | 1 | 1、配置≥6个千兆电口，≥4个千兆光口，配置≥2个扩展槽位，2个USB接口，32G内存，1T硬盘，1个console，冗余电源；支持无限制Web域名扫描授权，并发扫描12个web扫描任务，支持分布式部署。 2、扫描对象支持手动输入、批量文件导入及站点组导入，支持填写排除目标。 3、支持站点分组管理功能，可批量导入站点信息，并支持在站点管理下针对站点组或者单个站点直接开启扫描任务。 4、支持站点管理，显示站点树，包括站点目录信息、文件信息。（提供功能截图并加盖制造商鲜章） 5、支持自定义路径，对有爬取限制链接进行深度扫描，添加指定的站点url，便于爬取到更多的页面。 6、支持排除路径名，可自定义无需爬取的URL链接。 7、支持排除后缀名，可自定义无需爬取的文件后缀名，即引擎爬虫不对如下特定的链接爬取。 8、站点报表支持展示危险级别、站点信息、漏洞信息、外部站点，支持基于站点树展示漏洞分布及漏洞信息。 9、支持漏洞生命周期管理，包括未修复、确定、忽略、修复、已验证五种状态。（提供功能截图并加盖制造商鲜章） |
| 9 | 入侵检测 | 台 | 1 | ▲1、国产化CPU，国产化操作系统，配置≥4个千兆电口，≥4个千兆SFP光口（含光模块），≥2个万兆SFP+光口（含光模块），2个千兆管理口，2个扩展槽，冗余电源；设备满检速率：24000.000Mbps，TCP并发连接数：500.000万，4T存储空间，三年质保。 2、支持独立的攻击检测引擎，涵盖13000种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式进行分类。 3、智慧引擎检测功能能够实现对目标文件实时检测实时还原的效果，不依赖规则库即可实现对未知恶意程序检测。（提供功能截图并加盖制造商鲜章） 4、支持对文件还原捕获，可自定义捕获文件大小，最大支持还原100M大小的文件；支持对恶意文件、疑似恶意文件、无风险文件还原。 5、采用僵尸主机与控制主机异常通信行为检测的方式，具有独立的僵尸主机特征库，能够对11000种以上僵尸主机行为进行监测，包括僵尸网络、木马控制、蠕虫、挖矿、勒索、移动端木马控制、APT等多类型的僵尸主机行为。支持对Windows、Linux、IOS、Android、Unix、MacOS等多种操作系统的僵尸主机检测，并对规则可设置相应警告、联动阻断动作。 6、支持卸载SSL，实现对HTTPS、IMAPS、SMTPS、POP3S、FTPS、RDP、MQTT、SIP等加密流量的分析检测。 7、支持对传统协议元数据提取，包括TCP/UDP、ICMP、HTTP、SMTP、POP3、IMAP、FTP、SMB、NFS、文件、MYSQL、MSSQL、ORACLE、POSTGRESQL、DB2、REDIS、MONGODB、达梦、南大通用、人大金仓、SSL、RDP、DNS、SNMP、TFTP、IKEV2、LDAP、SIP、SSDP、SOCKS4、SOCKS5、AFP、VNC、SSH、DHCP、RADIUS、NTP、认证、SPICE、FEIQ、WAP等协议。 8、支持支持攻击取证、僵尸主机取证、恶意程序样本、恶意程序无风险样本、威胁情报样本、威胁情报取证、WEB防护取证、异常流量取证，取证类型支持报文取证和样本文件取证两种形式。 9、投标产品需入围《军用关键软硬件自主可控产品名录（最新版）》。 |
| 10 | 虚拟化平台防护系统 | 套 | 1 | 1. 支持所有Hypervisor，支持主流虚拟化平台，此次配置120个点授权，三年免费升级服务 2.基本防护功能：防恶意程序，可以阻止用户访问恶意Web站点，实时检测并报告对文件和系统注册表的恶意及意外更改，减少物理和虚拟服务器的攻击面，在已知漏洞修复之前屏蔽漏洞以免遭受无限制的入侵，捕获和分析系统日志，为组织提供审计证据，可以将日志审计配置为将可疑事件转发到SIEM系统。 3.通过预测性机器学习为未知威胁和零日攻击提供增强的恶意软件防护。 4.管理中心支持多租户，支持不同租户widget、事件、安全策略、管理、日志文件相互隔离，同时支持不同租户计算机、终端、安全配置相互隔离； 5.支持不少于100种异常监控和告警规则，应支持不少于700种系统事件，记录包括管理员、审计员、系统等所有审计日志； 6 .应提供至少19个报表模板，覆盖所有功能，包括数量排名、图形展示，可指定任意虚拟机/终端、计算机组、策略、时间段和标记进行报表生成，支持定义报表保密级别，支持生成报表加密。 |
| 11 | Web防火墙 | 台 | 1 | 1、国产化CPU，国产化操作系统，配置≥6个千兆电口(带2组bypass)、≥4个千兆光口、≥2个万兆光口、2个扩展槽、16G内存、4T机械硬盘+16G Msata,冗余电源,HTTP吞吐量：3529.965Mbps。 HTTP请求速率：5.004万/秒。 HTTP并发连接数：350.000万，三年质保。 2、采用专用国产化硬件架构与专用安全操作系统，基于操作系统内核的完全检测技术；硬件设备可以机架安装，产品必须为专业性 WEB 应用防火墙硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能。 3、支持对HTTP/HTTPS Flood攻击源的发包速度、源新建连接数、源并发连接数做源限速控制配置，且可以阻断攻击或者将攻击IP加动态入黑名单。 4、对ddos流量支持检测清洗和强制防御两种模式，检测清洗根据是否到达阈值对流量进行清洗，强制清洗对所有流量直接进行流量清洗判断。（提供功能截图并加盖制造商鲜章） 5、网关型网页防篡改，无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容。 6、持对防护的WEB服务器进行健康检查，支持 ICMP、TCP、HTTP、HTTPS 类型的健康检查。 7、针对攻击日志，可对任意一条编辑其行为动作，包括阻断记录日志、阻断不记录日志、继续、警告、临时或永久跳转到某一重定向页面等动作。 8、支持与防火墙联动，提供闭环的Web安全解决方案。 |
| 12 | 日志审计 | 台 | 1 | 1、国产化CPU，国产化操作系统，配置≥6个千兆电口、≥4个千兆光口、≥2个万兆光口、4T硬盘，内存：32GB，系统盘：256GB Msata,冗余电源,日志采集处理均值30000EPS，三年质保。 2、数据存储能力：压缩加密存储，压缩比不低10:1；日志存储不低于10000条/M 。 3、支持百亿级数据交互式多条件查询，百亿级数据查询响应时间小于10s。 4、支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于26类300种日志对象的日志数据采集。 5、支持对日志流量非常大但是日志重要程度低的syslog类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集。（提供功能截图并加盖制造商鲜章） 6、支持对常用查询条件进行保存，可重复使用；支持查询条件缓存，通过快速调用系统右侧隐藏栏中缓存的查询条件，提升常用条件的检索速度。 7、支持为不同类型日志设置不同的查询条件和显示条件。 8、支持基于时间轴展示日志数据分布，能够通过时间轴进行查询分析。 9、支持多种运维管理工具，可对日志源进行HTTP、HTTPS、SSH、SCP、SFTP、FTP、MYSQL、ORACLE、SQLSERVER等操作。（提供功能截图并加盖制造商鲜章） 10、系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。 |
| 13 | 蜜罐（潜听威胁发现系统） | 台 | 1 | 1、配置≥6个千兆电口，≥4个SFP光口,冗余双电源,32GB内存，240G SSD系统盘 +1TB数据存储盘，50个进程级虚拟主机IP+1个容器级虚拟主机。 ▲2、支持以攻击源-虚拟主机、中国地图、世界地图三种方式对主动防御态势进行展示，包括攻击源IP TOP10、被攻击虚拟主机IP TOP10、攻击趋势、攻击拓扑、攻击类型分布等信息。（提供功能截图并加盖制造商鲜章） 3、支持攻击事件关联漏洞信息展示，包括漏洞名称、漏洞类型、漏洞级别、CVE编号、漏洞简介信息。 漏洞至少包含（CVE-2017-12636、CVE-2018-7600、CVE-2017-17562、CVE-2021-44228、CVE-2022-22965、CVE-2017-5638、CVE-2017-10271、CVE-2018-2628）。 4、支持3000种以上操作系统伪装，包括Windows、Linux。macOS等。 5、支持20000种以上设备指纹伪装，包括DELL、HP、联想等。 6、支持智能一键添加蜜网，自动生成虚拟主机，支持添加多个蜜网模拟真实网络区域。（提供功能截图并加盖制造商鲜章） 7、支持文件诱饵，对虚拟主机的目标路径下发、删除诱饵文件，当黑客访问诱饵文件时，捕获感知文件变动信息。（提供功能截图并加盖制造商鲜章） 8、支持爬取和自定义上传两种方式创建网站模板，并生成对应的web仿真服务。 9、支持添加防火墙自动封禁策略。 10、支持联动沙箱中检测攻击者的遗留文件。 |

1. 实施服务要求
2. 投标人负责提供硬件设备的现场安装、调测、开通。
3. 投标人在设备安装实施前，须向招标人提供详细的进度安排及项目实施组织方案。
4. 投标人在完成施工安装后续提供技术支持文档，包括热线服务电话、技术支持联系方式、技术支持联系人、故障处理流程、用户使用操作文档等内容。
5. 设备割接不得影响大学正常使用网络。
6. 经济要求
7. 采购项目预算安排情况

475万元

1. 实施周期和服务地点

项目实施周期：合同签订后6个月。

服务地点：重庆市沙坪坝区。

1. 售后服务要求
2. 项目综合验收之日起投标人提供硬件原厂≥3年售后维保。
3. 在售后服务期内，投标人免费提供检测、维修、更换及升级服务，确保大学网络不中断，不影响正常使用。
4. 投标人在实施及维保期间须提供核心交换机备件服务，确保在故障发生后24小时内进行替换，保障网络通畅。
5. 投标人须保证技术服务响应时间不超过20分钟，到达现场时间不超过1小时，修复时间不超过24小时。
6. 投标人在故障解决后三个工作日内提供详细的书面报告，包括故障形成原因、故障历时、故障影响面、故障解决过程、故障解决办法、经验教训、防止故障重复发生的措施等。
7. 投标人提供每周7天、每天24小时(7x24)的技术支持服务。
8. 投标人在网络及本次项目所采购的设备出现重大技术故障时，组织并提供相关专家技术服务。
9. 验收方法

中标方提供网络性能测试报告，招标人按采购清单逐一验收。

（三）实施意见

1. 采购方式选择

公开招标

1. 采购包划分

不分包

1. 付款方式

投入使用并通过验收支付货款90%，质保期完成支付10%货款。

1. 供应商资格条件设定
2. 符合《中华人民共和国政府采购法》第二十二条资格条件:

①具有独立承担民事责任的能力:

②具有良好的商业信誉和健全的财务会计制度:

③具有履行合同所必需的设备和专业技术能力:

④有依法缴纳税收和社会保障资金的良好记录:

⑤参加政府采购活动前3年内，在经营活动中没有重大违法记录:

⑥法律、行政法规规定的其他条件。

1. 国有企业;事业单位;成立3年以上的非外资独资企业或控股企业。
2. 单位负责人为同一人或存在直接控股或管理关系的不间供应商，不得同时参加同一包的采购活动。生产场经营地址或注册登记地址为同一地址的不同生产型企业，股东和管理人员(法定代表人、董事或监事)之间存在近亲属或相互占股等关联关系的不同非国有销售型企业，也不得同时参加同一包的采购活动。近亲属指夫妻、直系血亲、三代以内旁系血亲或近姻亲关系。
3. 未被中国政府采购网 (www.ccgp.gov.cn) 列入政府采购严重违法失信行为记录名单，未在军队采购网 (www.plap.mil.cn)军队采购暂停名单处罚范围内或军队采购失信名单禁入处罚期和处罚范围内，以及未被“信用中国” (www.creditchina.gov.cn)列入严重失信主体名单或国家企业信用信息公示系统(www.gsxt.gov.cn)列入严重违法失信名单(处罚期内)。
4. 评审方式选择

价格优先法

1. 安全保密措施

投标人须与大学签订保密协议，项目成员须与大学签订保密承诺书。

1. 其他实施意见（如采购类别）

物资类采购