附件1：

网络安全等级保护系统技术参数

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类别** | **设备名称** | **主要技术参数** |
| 1 | 外网出口防火墙 | 出口防火墙主机 | 1.标准1U设备，配置≥6个千兆电口，≥2个千兆光口，≥2个扩展槽位，单电源；防火墙吞吐≥6G，并发连接≥220万，每秒新建连接≥5万；配置≥5年入侵防御、防病毒规则库升级许可。 2.支持手动和LACP链路聚合，可根据源/目的mac、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法。 3.支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式；支持StickyNAT开关，使相同源IP的数据包经过地址转换后为其转换的源IP地址相同； 4.提供策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查、策略包含分析，可在WEB界面显示检测结果。 5.支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置。 6.支持基于TCP协议的检测清洗，包括但不限于：TCPFlood、SYNFlood、FINFlood、RSTFlood、新建SESSIONFlood、SESSIONFlood等；支持SYN源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击。（提供截图，并加盖制造商公章） 7.支持对HTTP/SMTP/POP3/FTP/IM等协议进行病毒防御。 8.支持在一台物理设备上划分出128个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源。 9.支持防暴力破解、密码复杂度、密码有效性设置，如认证失败次数及锁定时间、密码格式、密码长度、密码找回、首次登录修改密码、密码定期修改、密码有效时间等设置。 10.内置动态黑名单功能，可与URL过滤、病毒过滤、防代理功能实现联动封锁；支持静态和动态黑名单命中统计和监控。（提供截图，并加盖制造商公章） 11.支持在WEB界面进行网络诊断，支持PING、TRACEROUTE、TCP、HTTP、DNS诊断方式。 12.支持根据应用对通过设备的数据进行统计，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速。 13.支持对设备状态、威胁信息、接口流量、连接信息、应用流量、用户流量、服务器流量、网站类型流量、VPN流量、在线用户等对象进行监控展示。 14.支持与本次招标采购终端威胁防御系统设备进行联动，提高安全事件响应与处置能力，构建立体防御体系。 15.投标产品具有中国信息安全测评中心颁发的《信息技术产品安全测评证书》且级别达到EAL4+级或以上（提供证书复印件，并加盖制造商公章） 16.为保证项目信息系统建设过程的安全，要求投标产品制造商具有中国信息安全测评中心颁发的《信息安全服务资质证书》（安全工程类三级）（提供证书复印件，并加盖制造商公章） 17.为保证产品质量，要求投标产品制造商具有电讯业质量管理体系认证证书TL9000认证；（提供证书复印件并，加盖制造商公章） |
| 特征库 | IDP攻击规则特征库5年升级许可 |
| 病毒库 | 专业版快速扫描查杀病毒库5年升级服务许可； |
| 规则库 | 5年规则库升级许可 |
| 2 | 入侵防御 | 入侵防御系统主机 | 1.标准1U设备，配置≥8个千兆电口（含1个管理口，支持1组Bypass），≥4个千兆光口插槽，冗余电源；配置≥2个扩展槽位；整机吞吐率≥6.5Gbps，最大并发连接数≥150万，IPS吞吐率≥2.2Gbps，配置≥5年攻击检测规则库、应用识别库、地理信息库升级许可； 2.要求能够检测包括扫描探测、暴力猜解、拒绝服务攻击、后门控制、溢出攻击、代码执行、非授权访问、注入攻击、URL跳转、跨站攻击、WebShell、浏览器劫持、文件漏洞攻击、工控漏洞攻击、物联网漏洞攻击等在内的15大类超过9000种网络攻击事件。 3.支持暴力破解检测，包括SMTP、IMAP、POP3、FTP、SMB、TELENT、LDAP、ORACLE、MYSQL、MSSQL、MONGODB、POSTGRESQL、DB2、REDIS、HTTP等协议的口令暴力破解和登录成功行为检测。支持自定义检测周期和检测次数。支持对发生的暴力破解行为事件进行取证。（提供截图，并加盖公章） 4.支持对DDoS攻击的全局参数配置，如：统计采样比、动态源节点超时、动态保护节点超时、攻击开始抖动时间、攻击结束抖动时间、攻击日志源最大个数等。 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10000种以上僵尸主机行为进行检测，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。 6.支持隐蔽通信检测，支持对HTTP、FTP、SMTP、IMAP、POP3、Telnet等服务的隐蔽通信检测。 7.要求应支持DDoS防护模板，提供包括100M/1000M/10000M的WEB服务器、DNS授权服务器、DNS缓存服务器、FTP服务器等模板选择，模板可设置。 8.支持对恶意程序实现特征检测、机器学习检测、内置虚拟沙箱检测等多种检测方式，并且多种检测方式相互独立、互不影响；支持专业沙箱设备联动检测。（提供截图，并加盖公章） 9.机器学习检测能够对目标文件实时检测实时还原效果，不依赖规则库检测实现对未知恶意程序检测。 10.支持对传统协议生成流量审计日志：如TCP/UDP、ICMP、HTTP、邮件、FTP、SMB、NFS、文件、数据库、SSL、RDP、DNS、SNMP、TFTP、IKEV2、LDAP、SIP等。 11.支持根据IP地址添加IP黑名单、IP白名单；支持动态IP黑名单（黑名单IP地址数据包阻断，白名单IP地址不做检测。）、动态URL黑名单；支持根据文件hash添加文件白名单；根据规则编号+IP+端口添加事件白名单。支持批量导入IP黑白名单和文件白名单。 12.支持与同品牌防火墙联动处置，支持设置联动防火墙名称、地址、共享密钥；支持设置防火墙阻塞时间。 13.为保证项目信息系统建设过程的安全，要求投标产品具有中国信息安全测评中心颁发的《信息安全服务资质证书》（安全工程类三级）（提供证书复印件，并加盖公章） 14.为保证产品质量，要求投标产品具有电讯业质量管理体系认证证书TL9000认证；（提供证书复印件并，加盖公章） |
| 升级许可 | 5年攻击检测规则库、应用识别库、地理信息库升级许可 |
| 3 | 日志审计 | | 1.标准1U设备，配置≥7个千兆电口，单电源，240GSSD系统盘，数据盘≥12T，日志采集处理速度≥10000EPS，配置≥105个日志源授权。 2.数据存储能力：压缩加密存储，压缩比不低于10:1；日志存储不低于10000条/M；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。 3.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。 4.支持Syslog、SNMPTrap、Netflow、JDBC、WMI、FTP、SFTP、SCP、文件等方式进行数据采集；支持通过Agent采集日志数据。 5.支持实时自动刷新每个日志源的实时日志列表，支持在实时日志界面通过选择过滤器来监视所关注的特定类型的日志。 6.支持独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态。 7.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。（提供截图并加盖厂商公章） 8.支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数。 9.支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源IP和目的IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果。 10.支持IPv6/IPv4双栈环境部署，对IPv6/IPv4日志源的日志进行高速采集，支持IPv6日志的全量存储，支持IPv6日志的多条件高速查询检索及统计分析；（提供第三方检测报告，并加盖公章） 11.支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备IP、源IP、目的IP等方式快速检索安全事件告警，检索结果支持Excel等格式导出。 12.为保证项目信息系统建设过程的安全，要求投标产品具有中国信息安全测评中心颁发的《信息安全服务资质证书》（安全工程类三级）（提供证书复印件，并加盖公章） 13.为保证产品质量，要求投标产品具有电讯业质量管理体系认证证书TL9000认证；（提供证书复印件并，加盖公章） |
| 4 | 堡垒机 | | 1.标准1U设备，配置≥6个千兆电口，≥2个SFP插槽，单电源，配置≥2个扩展槽位；配置≥200个主机/设备许可，用户数不限制，图形并发≥100，字符并发≥200。 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。 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，更方便地进行用户关联追溯。 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。（提供截图并加盖厂商公章） 11.支持对堡垒机虚拟为多台逻辑堡垒机，虚拟堡垒机之间实现独立配置、独立数据。实现IT资源的动态分配、灵活调度、跨域共享，提高IT资源利用率。 12.为保证项目信息系统建设过程的安全，要求投标产品具有中国信息安全测评中心颁发的《信息安全服务资质证书》（安全工程类三级）（提供证书复印件，并加盖公章） 13.为保证产品质量，要求投标产品具有电讯业质量管理体系认证证书TL9000认证；（提供证书复印件并，加盖公章） |
| 5 | 网闸 | | 1.标准2U设备，内外端机双侧液晶屏；内端机配置≥6个10/100/1000Base-T接口（含1个管理口），≥2个千兆光口插槽，≥1个扩展槽位；外端机配置≥6个10/100/1000Base-T接口（含1个HA口），≥2个千兆光口插槽，≥1个扩展槽位，冗余电源；网络吞吐量≥800Mbps，并发连接数≥12万，延时≤5ms。 2.支持http消息头、消息体，上下行方向，命令及关键字的管控，支持允许、阻断、告警三种处理方式。 3.内置FTP安全模块，支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制。 4.支持文件名和文件类型的黑白名单过滤，文件类型过滤基于文件特征识别，非扩展名识别，且支持不小于50种文件类型识别。支持文件同步信息统计，包括每个任务的开始时间、同步数据量、同步成功数、同步失败数，并能够以图表的方式进行实时可视化展现。 5.支持网闸同侧数据库之间的数据同步，网闸可旁路部署实现数据库同步。 6.支持企业版和专业版双病毒防御引擎，采用国内外知名厂商病毒库，支持病毒库升级，并提供后续升级服务。 7.支持HTTP攻击类，RPC攻击类，WEBCGI攻击类，拒绝服务类、木马类、蠕虫类等11大类不少于4000条的攻击规则知识库。 8.支持DOS攻击防御，支持端口扫描防御、IP扫描防御、支持IP\TCP\UDP源限速和目的限速，可手动设置相关阈值。 9.提供服务器负载均衡功能，支持轮询、加权轮询、最少连接、加权最少连接等负载均衡算法。 10.提供在线用户监控，可实时展现内外端机在线用户名称、IP地址、认证服务器名称、客户端类型和在线时间信息，并可根据管理需要手动强制指定用户下线。 11.管理端通过独立的管理口与网闸内端机相连，策略统一从内端机下发，不允许采用外端机上的任何网络接口进行管理。 12.为保证项目信息系统建设过程的安全，要求投标产品具有中国信息安全测评中心颁发的《信息安全服务资质证书》（安全工程类三级）（提供证书复印件，并加盖公章） 13.为保证产品质量，要求投标产品具有电讯业质量管理体系认证证书TL9000认证；（提供证书复印件并，加盖公章） |
| 6 | 杀毒软件 | 杀毒软件系统 | 1.配置满足用户需求的Windows、Linux终端杀毒授权许可，终端防病毒功能授权，含5年升级服务。防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS病毒等进行查杀，提供主动防御系统防护等功能。 2.客户端至少支持WindowsXP、Windows7、Windows8、Windows10、Windows11等32位/64位终端操作系统，支持Windowsserver2003、Windowsserver2008、Windowsserver2012、Windowsserver2016、Windowsserver2019、RedHatLinux、UbuntuLinux、SuSELinux、CentOS、Debian、支持中标麒麟、银河麒麟、中科方德、深度、UOS等操作系统。 3.客户端安装后至多占用50M硬盘资源，日常内存占用不到30M，有效节省PC/Server资源。 4.全网安全态势展示，统计运行概况及客户端概况，包括终端信息、使用授权信息、待处理威胁、当日防护、全网风险趋势、威胁终端排行、病毒风险排行、安全事件、服务器信息等统计情况，点击统计数据可跳转查看详细信息。 5.可以展示全网补丁情况，包括补丁编号、补丁类型、操作系统、下载状态等，支持补丁忽略功能。 6.支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控、白名单）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP协议控制、恶意网站拦截、IP黑名单）；合规管控（文档检测、文档跟踪、USB存储、设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、补丁配置、弹窗配置、通信管理中心）。 7.支持通过PING、ARP、NMAP方式扫描，发现尚未纳入管控的终端，支持展示终端的终端在线、离线、安装情况（要求提供具备CNAS/CMA资质的第三方测试机构测试报告证明材料，至少包含报告首页，对应功能测试页和报告尾页并加盖公章） 8.支持不同终端组、不同IP、不同服务之间的安全隔离和访问控制，规范内部网络不同对象的访问行为。支持协议包括但不限于TCP、UDP、TCP/UDP、ICMP、IGMP、GGP、PUP、IDP、ND、ESP、AH、RDP、GRE、SKIP、RAW。 9.支持对webshell后门进行扫描检测，webshell后门规则数量大于100000。 10.支持开启勒索诱捕功能，设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。 11.支持系统加固，从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。（要求提供具备CNAS/CMA资质的第三方测试机构测试报告证明材料，至少包含报告首页，对应功能测试页和报告尾页并加盖公章） 12.支持文档检测功能，针对txt,doc,docx,xls,xlsx,ppt,pptx,rtf,pdf等格式文档的名称、内容进行包含关键字检查，对含有指定关键字的文档进行禁止发送、禁止拷贝等管控，消息提醒的同时将文档违规信息上报管理平台。 13.能够与同品牌的防火墙、态势感知和上网行为管理实现协同联动。 14.投标产品具有中国信息安全测评中心颁发的《信息技术产品安全测评证书》且级别达到EAL3+级或以上（提供证书复印件，并加盖公章） 15.为保证项目信息系统建设过程的安全，要求投标产品具有中国信息安全测评中心颁发的《信息安全服务资质证书》（安全工程类三级）（提供证书复印件，并加盖公章） 16.为保证产品质量，要求投标产品具有电讯业质量管理体系认证证书TL9000认证；（提供证书复印件并，加盖公章） |
| WindowsServer授权 | 10个WindowsServer客户端防病毒功能授权，含5年升级服务。针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能。系统默认支持WindowsServer。 |
| LinuxServer授权 | 10个LinuxServer客户端防病毒功能授权，含5年升级服务。针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能。系统默认支持LinuxServer，含5年升级服务。 |
| 7 | 认证系统 | | 支持802.1X、Portal、VPN等多种认证接入方式 支持短信验证码/URL认证、二维码授权认证、授权码认证、公共二维码/二维码名片认证、Web免责认证、邮件开户认证、双因子认证（用户名密码+短信校验码）、BYOD无感知认证（802.1X无感知、WEB+MAB无感知）、昵称认证、学生信息作为机房账号认证等多种认证方式 支持PAP、CHAP、MS-CHAPV1/V2、EAP-MD5、EAP-TLS、PEAP(MsCHAPV2/GTC/MD5)、证书认证等多种身份验证 支持基于场景感知（用户、时间、地点、接入方式）的身份认证 支持基于用户身份的网络访问权限控制、应用安全域分时切换、自定义Radius属性授权 支持基于包括用户名、密码、IP地址、MAC地址、网络设备IP、网络设备端口号、主机硬盘序列号、IMSI/手机号、SSID等在内的元素灵活绑定 支持配合RG-EG网关设备进行实名审计 支持配合RG-ACE流量控制引擎进行流量控制 支持锐捷3G/4G解决方案，配合3G/4G路由器进行IMSI卡号认证和IP地址下发 支持在线时长控制：包括每天在线时长、单次在线时长、累计在线时长控制 支持用户自助服务平台：包括用户基本信息、密码、密保、移动终端、访客开户、二维码名片、授权码生成、上网历史记录、认证失败日志、在线信息的灵活管理 用户短消息、修复程序自动下发功能，用户上下线日志功能，用户黑名单功能，定期销户功能 |
| 8 | 机房运维平台 | | 软件参数：采用业内领先的嵌入式技术和开发的网络架构平台，内嵌WEB服务器、多种智能设备采集协议、3D图形，可适配多种传感器、电量仪、UPS、精密空调等智能设备。 |
| 9 | 温湿监测器 | | 测量范围：温度：-10℃~50℃湿度：0～95%rh；测量精度：温度：±0.5℃在25℃时湿度：±3%rh在25℃时；安装方式：机柜磁吸式安装或壁挂安装；RS485通讯输出，标准的MODBUS协议； |
| 10 | 烟雾传感器 | | 光电探测方式，吸顶安装，光学迷宫，采用低功耗CMOS微处理器， |
| 11 | 声光报警器 | | 机房专用声光联网报警器 |
| 12 | 测评 | | 二级等保测评费用，含评测咨询、资料制作等评测所有费用 |

除需要提供技术参数中指定的相关证书证明外，还需要提供以下证明文件：

1、本次采购的防火墙系统须符合GB/T18336-2015《信息技术安全技术信息技术安全评估准则》标准要求，通过EAL4+及以上等级评估，具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（EAL4+级）。（提供证书复印件，并加盖制造商公章）

2、本次投标防火墙产品具有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CCRC（增强级）。（提供证书复印件，并加盖制造商公章）

3、本次采购的日志审计系统须符合GB/T18336-2015《信息技术安全技术信息技术安全评估准则》标准要求，通过EAL3+及以上等级评估，具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（EAL3+级）。（提供证书复印件，并加盖制造商公章）

4、本次采购的堡垒机系统须符合GB/T18336-2015《信息技术安全技术信息技术安全评估准则》标准要求，通过EAL3+及以上等级评估，具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（EAL3+级）。（提供证书复印件，并加盖公章）

5、本次采购的杀毒软件系统须符合GB/T18336-2015《信息技术安全技术信息技术安全评估准则》标准要求，通过EAL3+及以上等级评估，具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书》（EAL3+级）。（提供证书复印件，并加盖公章）

6、为保证项目网络安全应急服务能力，要求投标安全产品制造商获得第九届CNCERT网络安全应急服务支撑单位（国家级）（提供官网截图）；同时具备国家互联网应急中心（CNCERT）颁发的网络安全应急服务支撑单位证书（国家级）。（提供证书复印件，并加盖制造商公章）

7、为保证产品代码质量与稳定性，要求投标安全产品制造商能力成熟度集成模型CMMI达到成熟度五级。（提供证书复印件，并加盖制造商公章）

8、投标安全产品制造厂商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），得4分。（提供证书复印件，并加盖制造商公章）

9、投标安全产品制造商具有国家信息安全测评中心信息安全服务资质安全开发类二级。（提供证书复印件，并加盖制造商公章）