**招标参数**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 功能参数 | 数量 | 金额 |
| 1 | 服务器 | 1. 国产化CPU，处理器：≥1个服务器专用处理器，其中CPU的主频≥2.2GHz，核心数≥16C；
2. 内存≥DDR4 64G ，内存频率≥2933 ,硬盘≥2块 2T HDD SATA 硬盘;
3. 配备≥1块Raid卡，支持raid 0,1,5,6,10,50,60,JBOD ， 不少于2G缓存，550W单电源；
4. 提供≥2个万兆光口、2个SFP+万兆多模光模块，
5. 从服务器安全方面考虑，要求服务器厂家拥有具备自主知识产权的防勒索组件，提供计算机软件著作权登记证书证明，证书中需明确含“防勒索”字样。并需提供国家计算机病毒应急处理中心出具的产品检验报告，产品检验报告中至少可以体现“勒索行为监测”、“勒索病毒诱捕”、“关键业务保护”和“核心数据保护”等勒索病毒主流防护功能；
6. 售后服务：原厂三年免费整机保修，三年免费原厂工程师上门服务提供证明材料
 | 3 | 240000 |
| 2 | 防火墙 | 1. 标准2U机架式设备，千兆电接口≥12个(其中包含2组bypass)，千兆光接口≥12个，万兆SFP+光口≥2个，2个USB3.0，冗余电源，提供不少于2个扩展插槽，网络吞吐率≥18G，并发连接数不少于500W，需含URL过滤、防病毒、防攻击、上网行为管理、Web安全防护等增强特性；至少提供三年维保和三年全特征库升级授权服务；
2. 支持7元组的链路负载均衡策略，负载均衡接口支持接口和接口组，支持基于域名进行链路负载，负载算法包括但不少于优先级和权重，负载均衡接口支持pppoe、dhcp、tunnel等三层接口。提供功能截图证明；
3. 支持基于全局或链路进行DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载；
4. 支持进行DNS探测，针对探测失败情况，支持选择禁用dns-dnat功能或禁用负载链路出接口。提供功能截图证明；
5. IPS特征库支持超过8500+条主流攻击规则，包含但不限于用户提取、任意代码执行、木马/后门、WEB攻击、拒绝服务、信息泄露、蠕虫/病毒、挖矿、缓冲区溢出、目录遍历、SQL注入、WEB序列化、WEBSHELL、木马外联、间谍软件等攻击类别；
6. 支持异常包防御，包括但不少于：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP选项、IP Spoof、Jolt2、Fraggle等。提供功能截图证明；
7. 内置Web防护特征库，提供HTTP协议检查、XSS攻击、恶意扫描与爬虫、服务器防护、CMS漏洞防护等不少于11种的防护类型；
8. 支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等；
9. 支持应用特征不少于5000个，移动应用不少于450个。支持根据标签选择应用，预置标签分类至少包含安全风险、高带宽消耗、降低工作效率等10大类；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。提供功能截图证明；
10. 支持网络共享接入监控，针对私接路由器和非法无线热点行为进行识别和阻断。针对共享接入网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长；
11. 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒检测，支持检测邮件正文/附件、网页及下载文件中包含的病毒，支持300万余种病毒的检测；
12. ★支持多种用户认证方式，包含本地WEB认证、微信公众号认证、互联网钉钉认证、短信认证、免认证、Portal认证、SAM认证、二维码认证、IC卡认证、APP认证、POP3认证、混合认证和LDAP认证，其中微信公众号认证支持通过小程序获取手机号。提供功能截图证明；
13. 为确保产品安全性，产品应通过ARP缓存感染、ARP异常测试、IP语法异常测试、TCP异常测试等多项测试要求并异常数量为0。具有由 ISCI（ISA Security Compliance Institute 国际自动化协会安全合规学会）或其官方认证工具制造商颁发的ISASecure EDSA CRT产品检测报告证明，提供证明材料；
14. 售后服务：原厂三年免费整机保修，三年免费原厂工程师上门服务提供证明材料
 | 1 | 86000 |
| 3 | 网闸 | 1. 2U机架式设备，吞吐≥500Mbps，最大并发连接数≥2万，内网千兆电口≥6个（其中包含1个管理口），外网千兆电口≥6个（其中包含1个HA口），内外网至少各提供1个串口和2个USB口，双电源，至少提供三年维保；
2. 系统基本架构 “2+1”系统结构，内外端机之间采用专用硬件和专用协议进行连接，网闸以软硬件结合的方式，有效地隔断内外网络间直接的连接，防止信息无限制交换，支持IPV4/IPV6双栈接入；
3. 产品支持各类应用协议，包括HTTP、FTP、SMTP、IMAP、POP3、SQL、SMB、RTSP、SIP、RFB、OPC、ModbusTCP、S7、IEC104、DNP3、MQTT等各类协议，提供产品功能截图；
4. 支持SMB/CIFS、FTP、SFTP、NFS等多种文件协议，可以实现内网到外网、外网到内网的文件传送，提供证明截图；
5. 支持文件增量传输、删除同步等传输策略；支持目录内子目录同步，子目录级别不受限制；
6. 支持数据库同步，支持ORACLE、SQLSERVER、MYSQL、POSTGRESQL、DB2、 Sybase等多种主流数据库单、双向数据交换；
7. 支持SIP、RSTP协议视频交换，SMTP、POP3协议邮件交换，支持符合GB/ T28181标准的视频业务；
8. 支持同构、异构数据库之间的同步，如Mysql同步至Oracle，提供产品功能截图；
9. 支持自定义的TCP、UDP协议的数据隔离交换，以用户定制的命令、参数等来限定隔离通道内的数据内容；
10. 可实时监控CPU、内存、存储、隔离通道、活动链接、实时吞吐量等信息；
11. 产品应具有公安部计算机信息系统安全产品质量监督检验中心颁发的网络安全专用产品安全检测证书，提供证明材料；
12. ★为确保产品安全性，产品应通过ARP缓存感染、ARP异常测试、IP语法异常测试、TCP异常测试等多项测试要求并异常数量为0。具有由 ISCI（ISA Security Compliance Institute 国际自动化协会安全合规学会）或其官方认证工具制造商颁发的ISASecure EDSA CRT产品检测报告证明，提供证明材料；
13. 售后服务：原厂三年免费整机保修，三年免费原厂工程师上门服务提供证明材料
 | 1 | 80000 |
| 4 | 入侵防御 | 1. 1U机架式，千兆电口≥12个，千兆光口≥12个，1个专用带外管理口，1\*USB3.0.冗余电源，网络吞吐率≥10 Gbps，并发连接数不少于300万，至少包含三年维保和三年全特征库授权服务；
2. 系统定义超过8500+条主流攻击规则，包含但不限于用户提取、任意代码执行、木马/后门、WEB攻击、拒绝服务、信息泄露、蠕虫/病毒、挖矿、缓冲区溢出、目录遍历、SQL注入、WEB序列化、WEBSHELL、木马外联、间谍软件等攻击类别；
3. 支持自定义IPS特征，支持针对8种协议自定义入侵攻击特征，包括IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等协议。提供功能截图证明；
4. 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀，支持查杀邮件正文/附件、网页及下载文件中包含的病毒，支持300万余种病毒的查杀；
5. 支持ZIP、TAR等压缩打包文件的病毒查杀，压缩：默认5层，最大20层。提供功能截图证明；
6. 内置Web防护特征库，提供HTTP协议检查、XSS攻击、恶意扫描与爬虫、服务器防护、CMS漏洞防护等不少于11种的防护类型；
7. 支持HTTP协议的精确访问控制，可针对IP、URL、Method、Referer、User-Agent、Cookie、Url-args等字段设置内容，匹配内容包括但不少于：等于、不等于、包含、不包含、长度小于、长度等于、长度大于、正则匹配等。提供功能截图证明；
8. 支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等；
9. 支持7元组的链路负载均衡策略，负载均衡接口支持接口和接口组，支持基于域名进行链路负载，负载算法包括但不少于优先级和权重；
10. 支持进行DNS探测，针对探测失败情况，支持选择禁用dns-dnat功能或禁用负载链路出接口；
11. 支持针对IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能；
12. 支持弱口令扫描能力，可设置立即扫描或定期扫描，弱口令字典可自定义设置。提供功能截图证明；
13. 支持以攻击者的视角从攻击的四个阶段进行安全事件分析，包括但不限于：扫描探测、入侵尝试、内网渗透、数据盗取。支持统计每个攻击阶段的次数和攻击目的，支持针对每个攻击阶段进行数据下钻，以便了解详细的攻击内容。提供功能截图证明；
14. 支持多种用户认证方式，包含本地认证、短信认证、微信公众号认证、互联网钉钉认证和免认证，其中微信公众号认证支持通过小程序获取手机号。提供功能截图证明；
 | 1 | 65000 |
| 5 | 日志审计 | 1. ★2U机架式，千兆电口≥6个，万兆光口≥2个，2\*USB，1个console，不小于4T硬盘，双电源，不少于50点授权，日志处理能力不低于10000EPS，至少提供三年软件升级维保和硬件质保服务, 包含产品系统升级授权、远程支持服务、产品保修服务、硬件故障上门支持；
2. 软件授权：内置采集器，含日志收集、日志查询、日志存储、报表管理、事件管理、资产管理、用户管理、系统配置等功能；

3.支持采集日志种类有主机和服务器、网络设备、安全设备数据库、中间件等，支持通过Syslog、SNMP Trap、(S)FTP、JDBC、SMB等方式进行数据采集；4. ★支持采集主机和服务器日志：支持采集Window、linux、AIX、麒麟、凝思操作系统日志，能够对用户登录、用户权限变更、关键文件变更、USB插入和拔出、操作记录回显、串口占用事件、并口占用事件、非法外联、光驱事件、开放端口、网卡up和down、后台进程等主机事件进行收集和分析，提供相关证明文件，如功能截图或资质扫描件或官网发布的功能描述或具有相关功能描述的检测报告并加盖制造商公章；5. ★支持采集网络设备日志：支持采集包括但不限于华为、华三、思科等网络设备日志收集，包括（通用日志、http登录日志、VTY远程登录、snmp登录、登录超时、设备故障、设备性能、接口状态、操作命令日志），提供相关证明文件，如功能截图或资质扫描件或官网发布的功能描述或具有相关功能描述的检测报告并加盖制造商公章；6.系统应能够按照多种维度统计日志信息，包括但不限于攻击日志、审计过滤、恶意程序、防火墙、主机报表、应用服务器、网络设备、Windows审计、Linux审计、终端审计、SOX合规、PCI合规、VPN账号异常等多种场景；7.支持为重点关注的日志设置不同的查询条件和显示条件；8. ★内置不少于1100种日志解析规则，支持7大类百种常见设备日志范化规则，支持自定义配置范化规则，可满足常见应用场景的日志解析需求，支持对已范化日志进行二次解析，可自定义二次解析规则。提供相关证明文件，如功能截图或资质扫描件或官网发布的功能描述或具有相关功能描述的检测报告并加盖制造商公章；9.支持逻辑关联、事件关联、时序关联、统计关联分析逻辑关联支持与、或、非逻辑；事件关联支持丰富的逻辑表达式（等于、大于、小于、大于等于、小于等于、不等于）；统计关联支持按照统计条件的次数进行分析；10.支持用户行为审计：实时记录系统中各设备的登录、账号、外设、命令指令、配置变更等活动，对各类活动进行统计分析，筛选出可能存在风险的行为操作；11.支持告警归并，能够按照时间周期、类型、级别、受影响IP进行归并；12.支持通过Syslog或IEC104协议向对三方系统报送日志和告警；13.为确保产品安全性，产品应通过ARP缓存感染、ARP异常测试、IP语法异常测试、TCP异常测试等多项测试要求并异常数量为0。具有由 ISCI（ISA Security Compliance Institute 国际自动化协会安全合规学会）或其官方认证工具制造商颁发的ISASecure EDSA CRT产品检测报告证明，提供证明材料；14.所投产品应具有CNAS机构的振动测试和跌落测试报告，提供证明材料；15.服务要求：若因质量问题发生争议的，应邀请国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由采购方承担，货物不符合标准的，鉴定费用由供货方承担；16.需提供合法来源渠道证明，包含销售协议或代理协议或其他能证明合法来源的证明材料。 | 1 | 73000 |
| 6 | 运维审计 | 1. 标准机架式设备，1U，单电源，8G CF卡，4T硬盘，4\*GE电口，2\*USB，1\*串口，1\*GE管理口，1\*扩展插槽。提供授权管理25台设备和3个SDP远程接入授权。
2. 堡垒机具不同用户角色划分功能，如系统管理员、审计员、运维主管、设备管理员、普通用户等，对各类角色需要进行细粒度的权限管理。
3. 支持密钥登录方式，登录目标服务器时，可以自由选择密钥或密码的登录认证方式。
4. 支持运维人员依据个人的运维习惯自定义设置，如自定义的配置运维参数，提高运维效率；首页设备分组的默认方式自由选择：可配置本地客户端路径、可配置默认账号的登录参数、可配置图形、文件、应用的运维默认值。
5. 策略访问支持设备和用户等视图，视图可以按照表格格式导出，方便管理员管理。
6. 支持设备自动发现，通过IP地址扫描地址段内主机、服务器和网络设备，并自动识别启用服务和端口，方便管理员快速添加资产。

7. ★支持自动化运维，支持自定义自动化脚本，包含但不限于：支持window bat脚本、windows ps脚本、linux shell脚本、python脚本等脚本类型。可在线编辑和本地导入。提供截图证明。8. ★支持设定运维任务为手动、定时和周期执行方式，周期执行可按天、小时、周、月等设置，支持自动执行脚本执行后设备留存脚本记录，包括脚本名称、执行时间、统计结果，执行结果等，提供截图证明。9. 支持工单系统：包括运维工单的流程，运维人员通过提前工单申请，审批员可提前审批加大自由度，降低时间限制，提高工作效率；工单系统流程包括：工单申请创建、审批、完成。10. 需提供合法来源渠道证明，包含销售协议或代理协议或其他能证明合法来源的证明材料。 | 1 | 75000 |
| 7 | 漏洞扫描 | 1. 1U机架式，千兆电口≥6个，1\*USB，1个console，不小于1T硬盘，双电源，IP授权≥300点，IP扫描并发≥128点，至少提供三年维保及三年漏洞库升级授权服务；
2. 集成系统漏洞扫描、Web应用扫描、镜像扫描、移动扫描于一体；
3. 系统漏洞库数大于260000条，支持通过多种维度对漏洞进行检索，包括：CVE 、BUGTRAQ ID、CNCVE、CNVD、CNNVD 、MSID 、风险等级、漏洞名称、是否使用危险插件、漏洞发布日期等信息。提供截图证明；
4. 系统内置23种以上的系统漏洞扫描模板，如针对Windows操作系统、数据库、云平台（虚拟化）、工控系统、物联网、大数据组件、DNS、网络设备、弱密码等，同时允许用户自定义扫描模板；
5. 支持的操作系统包括：Windows系列：NT、2000、XP、2003、Win7、Win10、2008、2012、2016等。Linux系列：Amazon Linux、CentOS、Debian、Fedora、Red Hat、SuSE、Ubuntu等。Unix系列：AIX、FreeBSD、HP—UX、Solaris、Mac OS X等。国产操作系统（深度、银河麒麟、中标麒麟、凝思、欧拉、红旗等）等；
6. 支持的大数据组件包括：Cassandra、Elasticsearch、Flume、Hadoop、Hbase、Hive、 Kafka、Mongodb、Oozie、Redis、Spark、Storm、Splunk等，提供截图证明；
7. 支持资产主动探测，识别协议、智能识别端口对应的服务以及软件版本等，一键添加到资产；
8. 应用漏洞知识库数大于10000种，支持对主流Web漏洞的识别与扫描，包括：SQL注入漏洞、命令注入漏洞、CRLF注入漏洞、LDAP注入漏洞、XSS跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞等；
9. 扫描结果可展示原始数据包和测试数据包；
10. 支持Android、iOS移动应用静态扫描；支持获取APP相关信息：包括应用名称、版本信息、文件大小、文件md5、第三方sdk数量等,提供截图证明；
11. 支持输出的报表格式包括：HTML、DOC、PDF、XLSX等；
12. 支持编码解码（BASE64、URL、HEX等），哈希散列（MD5、SHA1、SHA224、SHA256、SHA384、SHA512等），加密解密（RC4、AES等）等辅助功能。提供功能截图证明；
 | 1 | 76000 |
| 8 | 入侵检测 | 1. 1U机架式，千兆电口≥8个，千兆光口≥2个，1个专用带外管理口，2\*USB2.0，冗余电源，网络吞吐率≥8Gbps，并发连接数不少于150万，每秒新建数不少于150000，至少包含三年维保和三年全特征库授权；
2. 支持基于流量的白名单自学习，可以通过自动学习生成协议白名单列表；支持学习后的白名单智能合并功能，降低白名单维护工作量；
3. 支持不少于12种工业协议的深度解析；支持对OPC UA/DA、Modbus、S7的值域级细粒度工业协议解析能力，提供功能截图；
4. 支持不少于10000条特征库，且支持工业安全事件特征库，如PLC程序上载下载、PLC变量写入、CPU状态设置等；
5. 异常报文检测支持：Teardrop、Land、WinNuke、fraggle和Smurf、TCP Flag、Jolt2；

6.支持将日志以syslog格式同时发送至最多三个日志服务器平台；7.支持IPv6的全局配置，支持基于IPv6的IDS；8.支持1个镜像流量转出接口，在不影响工业入侵检测系统对原始报文正常处理的情况下，将采集到的流量复制一份，通过镜像转出接口发送给监控设备；9.产品具有中国电力科学研究院的检测报告，提供证明材料； | 1 | 80000 |
| 9 | 等保测评 | 测评机构需取得国家网络安全等级保护工作协调小组办公室颁发的《网络安全等级保护测评机构推荐证书》。提供测评机构针对本项目的相关授权。 | 1 | 96000 |
| 10 | 不间断电源主机 | 电压范围：305~478 VAC ± @ 100% 负载，190~520 VAC （3-相）@50% 负载频率范围：46~54HZ or 56~64HZ 功率因数：≥0.99@100%负载输出电压：3\*360/380/400/415VAC (3相+N）电压范围（电池模式）：±1%频率范围（同步校正范围）：46~54Hz或56~64Hz频率范围（电池模式）：50 Hz±0.1 Hz或60 Hz±0.1Hz浪涌比率：3:1（最大）谐波失真：≤2% THD（线性负载）；≤5%THD（非线性负载）市电转换电池：0逆变到旁路：0波形（电池模式）：纯正弦波市电模式：95.0%CEO模式效率：98.0%电池模式：92.0%最大充电电流:4A 充电电压：±13.65V\*电池节数（16-20）LCD或LED：负载大小、电池容量、市电模式、电池模式、旁路模式、故障指示 | 1 | 7000 |
| 11 | 蓄电池 | 容量（A·h):100AH | 16 | 14400 |
| 说明 打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。 |  |