询 价 函

各报价人：

江苏有线通州分公司因等保建设需要，现邀请有意向的供货单位进行报价，报价不得高于预算控制价，预算控制价为人民币捌拾伍万伍仟元（￥855000元）。报价为完成该服务所有内容的价格，结算时不再进行调整，请各报价人认真研究服务内容慎重报价。

**一、项目基本情况**

项目名称：等保项目

项目类型：货物

所属行业：软件和信息技术服务业

预算金额：人民币约85.5万元

最高限价：人民币85.5万元, 报价超过最高限价者按无效处理。

采购需求：见项目需求。

合同履行期限：2023年12月15日前交货并安装调试结束。

本项目不接受联合体投标。

本项目不接受分包。

**二、项目需求**

报价人在制作报价文件时仔细研究项目需求说明，报价即代表报价人全部满足该项目所有需求，包括技术要求和商务要求:技术要求是指对采购标的功能和质量要求，包括性能、材料、结构、外观、安全，或者服务内容和标准等;商务要求是指取得采购标的的时间、地点、财务和服务要求，包括交付（实施）的时间（期限）和地点（范围），付款条件（进度和方法），包装和运输，售后服务，保险等。

设备清单如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 规格、品牌 | 配置参数 | 数量 |
|  | 下一代  防火墙 | 奇安信NSG5000-TG15 | 下一代防火墙系统；含应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN、SSL VPN等功能；多核AMP+架构，网络层吞吐量≥8G，并发连接≥200万，每秒新建连接数12万， 标准配置≥6个10/100/1000M自适应电口，支持液晶屏，3年入侵防御模块和3年防病毒模块。3年质保。 | 5 |
|  | 日志审计 | 奇安信  LAS-R32P | ≥6个千兆电口，2个扩展插槽（可选2万兆光、4千兆电、4千兆光），1个Console接口，4T硬盘。支持≥50个审计对象授权。3年原厂商质保和系统升级服务。 | 2 |
|  | 数据库审计 | 网御星云  LA-DAP-4000 | 设备配置≥6个千兆自适应电口（含1个管理口，1个HA口），1个接口扩展槽位，硬盘2T，1个RJ45串口； | 1 |
|  | 堡垒机 | 奇安信  C6100-BH-TF10 | ≥6个千兆电口；支持2个接口扩展槽位；内置≥4TB硬盘，≥50个管理授权。3年原厂商质保和系统升级服务 | 2 |
|  | 终端及其服务器杀毒软件 | 奇安信  ESM-FL；  火绒终端安全管理系统 | 企业版终端和服务器杀毒软件。3年原厂服务和售后 | 1 |
|  | 工作站汇聚交换机 | 锐捷  RG-S5300-24GT2SFP2XS-E | 交换容量≥336Gbps，转发性能≥69Mpps，固化10/100/1000M以太网端口≥24，1000M SFP光接口≥4个，3年原厂服务和售后 | 4 |
|  | 网络准入 | 金盾  ID-MST-03 | 支持国产化操作系统与Windows操作系统：对入网终端进行安全项目检查，不符合安全规范的终端不允许接入网络，检查项目包括网络监听端口检测、系统服务检测、系统时间检测、防病毒软件检测等，3年原厂服务和售后 | 1 |
|  | 上网行为管理 | 奇安信  NI3200-10A | 最大并发连接数为16万，最大新建连接数为11000个/秒；标配≥4个千兆电接口（其中含1个管理接口和1个HA接口），≥128G SSD硬盘； | 1 |
|  | 云防服务 | 国产 | 通过云WAF方式，对用户的访问请求进行监控过滤，能够抵御通用类型的SQL注入、文件包含、远程命令、WEBSHELL、XSS跨站、代码执行、文件注入等攻击威胁。 | 3 |
|  | 安全运维服务 | 国产 | 安全运维、漏洞扫描、安全培训、应急响应等 | 3 |
|  | 系统集成服务 | 国产 | 提供所有设备的安装调试服务及所需要的辅材等与本次项目相关的配件，另外增加一台标准机柜。 | 1 |

具体参数要求如下：

1、下一代防火墙

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| 硬件和性能 | 硬件和性能 | ★多核AMP+架构，网络层吞吐量≥8G，并发连接≥200万，每秒新建连接数12万， 标准2U机箱，冗余电源，标准配置≥6个10/100/1000M自适应电口，另有2个接口板卡扩展插槽，1个Console口，支持液晶屏，含三年硬件维保服务。加配：2口万兆光口板卡（选配）：2个SFP+插槽 |
| 功能授权 | ▲包含下一代防火墙系统软件；支持应用控制、URL过滤、病毒防护、入侵防御、威胁情报检测、IPSec VPN、SSL VPN等功能。配置三年病毒防护特征库、入侵防御特征库升级服务 |
| 基础组网 | 部署模式 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求，支持旁路模式； |
| 网络协议 | 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定； |
| 所投产品必须支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能。 |
| 路由协议 | 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。 |
| 地址转换 | 所投产品必须支持全面的NAT转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL\_CONE模式和SYMMETRIC模式。 |
| IPv6支持 | 所投产品必须设备接口支持配置IPv6地址，并可使用IPv6地址管理设备；支持IPv6手动及自动的IP/MAC探测及绑定。 |
| 高可靠性 | ★所投产品必须支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；支持链路探测。 |
| 虚拟化防火墙功能 | 所投产品必须支持对虚系统进行系统配置，包括管理设定、管理主机、证书管理、配置文件导入导出、日志配置；虚系统管理员可分权管理； |
| 所投产品必须支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。 |
| 访问控制 | 访问控制 | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查。 |
| 应用识别与控制 | 所投产品必须支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类。 |
| 流量管理 | ★所投产品必须支持多调度类相互嵌套最大5级的带宽管理设置。支持设置每IP最大或最小带宽，支持对每IP进行带宽配额管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。 |
| 攻击防护 | 网络攻击防护 | 所投产品必须支持基于不同安全区域防御DNS Flood、HTTP Flood攻击，并支持警告、阻断、首包丢弃、TC反弹技术、NS重定向、自动重定向、手工确认等多种防护措施。 |
| 所投产品必须支持基于安全区域的异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、IP选项、TCP异常、Smurf、Fraggle、Land、Winnuke、DNS异常、IP分片等；并可在设备页面显示每种攻击类型的丢包统计结果。 |
| 所投产品必须支持防御基于安全域的IP地址欺骗攻击，指定IP或网段必须从特定安全域流入。 |
| 病毒防护 | 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀； |
| 所投产品必须支持对最多6级的压缩文件进行解压查杀； |
| 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀。 |
|
| 入侵防御 | 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护。 |
| ★所投产品必须支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、严重性、影响的平台、类型、描述等详细信息。 |
| 协同防御 | 云端协同 | ★所投产品必须支持与互联网云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能。 |

2、日志审计

|  |  |
| --- | --- |
| 功能 | 指标要求 |
| 产品形态 | ★硬件规格：标准1U机箱，≥6个千兆电口，2个扩展插槽（可选2万兆光、4千兆电、4千兆光），1个Console接口，单电源，4T硬盘。包含50个日志源授权，三年硬件维保服务。性能：事件处理最高3000EPS |
| 使用模式 | 采用B/S模式，无需安装客户端，使用WEB浏览器访问管理中心，浏览器端无需安装Java运行环境。支持chrome浏览。 |
| 管理范围 | 能够对企业和组织的IT资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。 |
| 审计对象 | 支持审计各种网络设备（路由器、交换机等）配置日志、运行日志、告警日志等；  支持审计各种安全设备（防火墙、IDS、IPS、VPN、防病毒网关，网闸，防DDOS攻击，Web应用防火墙、等）配置日志、运行日志、告警日志等；  支持审计各种主机操作系统（包括Windows\Solaris\Linux\AIX\HP-UX\UNIX\AS400）配置日志、运行日志、告警日志等；  支持审计各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）配置日志、运行日志、告警日志等；  支持审计各种中间件（Tomcat、Apache、Webshpere、 Weblogic等）配置日志、运行日志、告警日志等；  支持各种应用各种应用系统（邮件，Web，FTP，Telnet、等）配置日志、运行日志、告警日志等；  以及用户自己的业务系统的日志、事件、告警等安全信息. |
| 日志采集与转发 | 支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能，支持多行日志采集合并为一行； |
| 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； |
| 资产管理 | 能够将资产按照多种维度进行分组、分域管理，如地理位置、组织结构、业务系统等，提供便捷的添加、修改、删除、查询与统计功能，支持资产组可以在页面不同的分组中移动。  支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行CIA赋值，自动计算资产价值，设置等保等级；在资产管理界面可查看每个资产的属性信息，情境信息，本身产生的事件信息、关联告警信息；  支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警。 |
| ★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。 |
| 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 |
| 日志归一化 | 支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； |
| 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。 |
| 日志解析字段内置130个字段，属性字段可扩展，用户可根据审计需要自行创建字段，字段类型包括IP、字符串、整型等6种，可设定字段长度、选择字段操作符集，选择映射函数等。内置及新增的所有字段均可参与查询、关联分析和报表统计。； |
| 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；  支持对选中的日志内容自动生成正则表达式来提取日志属性。 |
| 日志交互式分析 | 系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理，可将原始信息进行自动索引，快速搜索分析各类安全事件。系统提供即席查询功能，支持归一化字段及关键字搜索，从海量事件原始信息中获取与关键字匹配或部分匹配的所有事件。系统支持基于正则表达式的检索功能，用户可在搜索栏内输入正则表达式，系统可搜索出原始信息中与正则表达式相匹配的所有事件； |
| 用户可自定义事件搜索查询条件，并可保存为策略，以树形结构进行组织，形成一个搜索分析策略树；每个查询场景都可以查询策略的形式进行存储。 |
| 可以显示一段时间的动态事件移动图，能够在图上显示每个时间切片的事件数量，点击该时间切片，可以查看该切片内的所有事件；动态事件移动图可设置动态刷新频率，根据刷新时间显示实时事件； |
| 可以以图形化的方式形象的展示一段时间内的日志中IP节点之间的访问行为和关系。 |
| ★能够在世界地图上实时定位事件源/目的IP地址（内网IP）的地理位置； |
| 采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别(无须范化)，使审计人员清晰了解采集的日志构成。 |
| 日志统计分析 | 可自定义统计场景，统计的字段条件和时间段以及过滤器等可自由设定； |
| 支持柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图、3D地球等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报表等。图表数据支持数据下钻。 |
| 支持将统计结果保存为仪表板、报表和策略。 |
| 日志综合展现 | 系统提供可编辑的灵活强大的自定义仪表板； |
| 系统内置仪表板至少包括日志源事件分析仪表板，Windows事件分析仪表板，网络设备分析仪表板，防火墙事件总览分析仪表板，WEB事件总览分析仪表板，FTP服务器日志分析等； |
| 仪表板支持自定义创建框架，用户根据需要在框架内添加不同的仪表板组件（数值、折线、面积、柱图、饼图、环状图、地图、组件、URL、文本、图片、列表等），支持组件位置自由摆放，组件大小自由拖曳等。 |
| 关联分析 | 具备完善的基于规则的关联分析引擎，能够提供逻辑关联、统计关联和递归关联三种关联分析能力。其中，逻辑关联支持与、或、非逻辑，支持丰富的逻辑表达式（包括并不限于大于、大于等于、小于、小于等于、不等于、包含、在……之间、属于、开始于、结束于、是否为空、通配符匹配、正则匹配等），支持逻辑嵌套；统计关联支持在统计的时候针对特定的一个或多个字段进行相同计数和不同计数，支持统计时长设置和触发次数设置，具备重复触发的抑制设置功能； |
| 提供基于图形化方式的规则编辑器，能够对规则进行各种编辑和自定义，规则可实时启用和停用 |
| 关联规则能够引用外部资源，包括地址资源、时间资源、端口资源，以及用户自定义资源； |
| 关联规则支持规则嵌套和引用，通过多规则联合，可精确识别复杂安全事件和场景； |
| 必须具备单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析； |
| 系统支持动态活动列表，通过关联规则将关注的日志信息保存入活动列表中，并将活动列表中的内容应用到关联规则中。活动列表可根据分析需要创建，可赋予活动列表寿命。 |
| 支持对保存在系统中的历史日志进行回溯关联分析，发现历史日志中的安全事件 |
| 关联规则支持导入导出；支持关联规则复制； |
| ★支持对关联规则进行监控，了解该规则命中历史情况（投标文件需要提供能够体现上述功能及配置选项的截图）； |
| 支持分布式关联分析引擎，可以弹性扩展分析能力，最大可达10万EPS以上 |

3、数据库审计

|  |  |
| --- | --- |
| 功能 | 指标要求 |
| 硬件规格 | ★1U标准机架设备；设备配置≥6个千兆自适应电口（含1个管理口，1个HA口），1个接口扩展槽位，硬盘2T，1个RJ45串口； |
| 此次配置三个被审计数据库授权，三年硬件质保和技术支持服务 |
| 性能要求 | 可审计流量≥500Mbps |
| 审计协议 | 支持对Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis、Hbase、hive等数据库进行审计 |
| 支持人大金仓KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) |
| 支持MongoDB、Redis、Hbase、hive等数据库进行审计（提供截图证明） |
| 支持FTP、Rlogin、Radius、NFS、X11等协议审计 |
| 审计能力与效果 | 审计策略支持时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件。 |
| 审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件（非正则表达式方式）； |
| 支持对数据库DML、DCL、DDL语句的审计 |
| ★提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别 |
| 审计策略支持时间、源IP、目的IP、协议、端口、登陆账号、命令作为响应条件 |
| 支持审计网络邻居的用户名、读写操作、文件名等（提供截图证明） |
| ★产品采用先进的报文过滤的方法和功能装置，可有效防范针对数据库的网络攻击 |
| 数据库异常行为审计 | 数据库操作行为基线包括数据库账号、操作类型、源IP、客户端程序等行为特征 |
| 支持对超出数据库操作行为基线的操作可自动识别，并及时告警 |
| 产品采用先进的异常处理的方法和技术，告效识别数据库异常访问行为 |
| 事件查询统计与报表 | 支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多IP登录、上下班操作量对比异常、操作响应时间分析；支持疑似暴力破解、疑似撞库攻击场景的操作异常分析；行为周期与阀值可按需定义 |
| 数据库审计支持用户数据库中敏感信息的自动发现，方便针对敏感信息配置针对性的审计策略，敏感信息发现支持探测器和正则表达式两种方式，探测器至少包含：姓名、地名、银行卡、身份证、IP地址、密码等多种探测器 |
| 支持按每天、每周、每月、时刻生成报表 |
| 支持生成Word、PDF、xls、HTML、WPS格式的报表导出 |
| 自身管理 | 提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能 |
| 审计系统上存在大量敏感信息，必须对审计管理员进行强度更高的认证，管理员登陆支持硬件令牌认证 。 |
| 响应方式 | 记录审计事件、记录会话数据、忽略、界面告警、Syslog告警、SNMP trap告警、邮件告警、短信告警 |
| 资质 | 产品具有公安部销售许可证（增强级） |
| 产品具有《中国国家信息安全产品认证证书》（增强级） |
| ★产品具有《中国信息安全测评中心的信息技术产品安全测评证书》EAL3+ |

4、堡垒机

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| 硬件和性能 | 硬件和性能 | ★采用专用千兆多核硬件平台和安全操作系统；外观：标准1U机架式；6个千兆电口；支持2个接口扩展槽位；内置4TB硬盘；单电源；支持液晶屏；最大支持150路图形会话或400路字符会话并发；最大可选300授权许可。（本次配备不少于100个授权。）含三年标准售后服务。 |
| 身份认证 | 多因子认证 | ★支持多因子认证，方式包括手机令牌、手机短信、动态令牌、USBKey、指纹识别等多因子认证方式 |
| 多因子灵活配置 | 支持不同的用户配置不同的多因子认证方式，例如user01配置USB Key，user02配置动态令牌 |
| 认证方式配置 | ★支持配置登录页面展示的默认登录方式，其他登录方式用户可点击“更多登录方式”按钮进入 |
| 登录锁定 | 支持登录失败次数锁定设置，可锁定主账户或IP，可配置解锁时长，到期自动解锁，也可以手动解锁 |
| 登录限制 | 支持用户的登录时间、来源IP地址和来源MAC地址限制（黑名单或白名单），限制非法时间和非法地址登录堡垒机 |
| 用户管理 | 用户角色 | ★支持按模块和功能自定义角色权限，便于管理，用于复杂的业务场景需求 |
| 批量管理 | 支持用户信息的批量修改，包括重置密码、移动部门、更改角色、修改多因子配置、修改有效期、修改IP限制、修改MAC限制 |
| 资源管理 | 支持的协议 | 支持的运维协议包含SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、Rlogin |
| 自动发现 | 支持按IP范围、端口进行资源设备自动发现，实现快速批量添加资源设备 |
| 登录模式 | 支持资源账户自动登录（包含提权登录，TELNET、SSH协议资源使用普通账户自动切换到root或enable账户）和手动登录方式，其中手动登录方式又区分全手动（手动输入账户和密码）和半自动模式（手动输入密码） |
| 资源标签 | 支持资源按标签管理，并可以对资源批量添加和删除标签 |
| 策略管理 | 访问控制 | 支持同时以用户、用户组、账户、账户组为核心要素，来设置多对多的资源访问授权，用户组和账户组内的新增成员可自动继承授权关系 |
| 细粒度权限控制 | 可根据用户、用户组、账户、账户组、有效期、文件管理控制、文件传输控制（上传、下载）、RDP剪切板控制、时间限制、IP限制为条件，细粒度地进行访问控制 |
| 自定义命令 | 预制主机和网络设备的基本命令，支持正则表达式和通配符方式设置自定义命令 |
| 资源账户改密 | 自动改密 | 支持以账户、账户组、时间、改密周期、改密方式生成详细的改密计划，到期自动执行 |
| 密码分段外发 | ★改密完成之后，通过邮件将密码发送给指定的管理员，需要指定2个管理员，管理员A收到前半段密码，管理员B收到后半段密码 |
| 密码生成方式 | 支持随机生成不同、相同密码或者手动指定密码，改密日志内容包括改密账户总数，成功、失败和未修改数量 |
| 资源运维 | H5运维 | 不限操作系统类型，无需安装任何客户端插件，使用浏览器通过H5方式即可直接运维SSH、RDP、Telnet、VNC资源 |
| 批量登录 | 支持SSH、RDP、TELNET、VNC协议资源的批量登录功能，并且支持混合协议的批量登录，支持同时在一个页面运维不同协议的资源 |
| 会话协同 | ★支持运维过程中邀请其他用户参与、协助操作；会话协同过程中，协同者可以申请控制会话，创建者可以强制获取控制权 |
| 工单管理 | 工单申请范围设置 | 可设置用户申请工单时，可以查看的待选资源的范围，支持设置为全部、本部门及下级部门、本部门；同时，可设置高级模式，指定某类角色或某个部门的人员可以申请指定部门的资源 |
| 审计日志 | 实时监控 | 支持对实时会话进行无延时的实时监控和切断 |
| 在线回放 | 支持在线回放运维人员对资源的操作过程，并可以对播放速度进行调整，支持拖动、暂停、停止、跳过空闲、重新播放、切换会话等操作 |

5、终端及其服务器杀毒软件

5.1、终端杀毒软件

|  |  |  |
| --- | --- | --- |
| 技术指标项 | | 指标要求 |
| 平台环境要求 | 产品要求 | ▲软件形态，包含管理控制中心、客户端软件，共200个客户端授权；其中160个客户端支持：windows，40个支持：银河麒麟V10(龙芯、飞腾、X86)、银河麒麟(龙芯、飞腾、X86)V10.1、UOS20 sp1(龙芯、龙芯3A5000、鲲鹏920、麒麟9006C、飞腾、X86、兆芯)、中科方德（龙芯、飞腾、申威、X86），TencentOS Server3 |
| 控制中心要求 | 控制中心支持单机部署和集群部署两种方式，控制中心根据客户端点数的增加支持横向扩展； 操作系统支持Windows Server 2012/2012 R2/2016的64位版本（简体中文版）； 支持CentOS 7系统； |
| 控制中心支持安装在虚拟机上； |
| 客户端要求 | 操作系统：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10；Windows Server 2008/Windows Server 2012/Windows Server 2016/Windows Server 2019；macOS X 10.11/macOS X 10.12/macOS X 10.13/macOS X 10.14/macOS X 10.15/macOS X 10.16/macOS X 11.0；CentOS 5~8/Red Hat Enterprise Linux 5~8； |
| 基础功能 | 语言要求 | ★产品全功能支持简体中文/繁体中体/英语自由切换。 |
| 控制中心管理 | 支持控制中心迁移、数据备份、数据恢复；支持多升级服务器； |
| 支持通过高级筛选方式对终端概况进行筛选查看指定范围终端实时统计数据，支持“与或”组合筛选。 |
| 管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，且可设置锁定时间，该时间内账号登录请求不被接受。同时应支持双因子认证登录方式，提高安全性。 |
| 客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。当检测到新版本将从第一批次重新观察。 |
| 支持终端用户和管理员是一套账号管理系统，简化账号管理复杂度，一个账号解决所有身份认证，既可以用于终端登录，也可以用于管理管理中心。 |
| 支持不同分组，客户端轻量化模式一键切换功能。 |
| 客户端管理 | 支持终端密码保护功能，支持终端“防退出”密码保护、“防卸载”密码保护、防安装密码保护。支持设置自我保护功能，可有效防止客户端进程被恶意终止、注入、提高客户端进程、数据、配置的安全性。 |
| 支持自定义定制客户端标题、皮肤、语言、产品LOGO、企业LOGO、认证弹窗LOGO。 |
| 病毒防护 | 病毒防护概况 | 病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本 |
| 病毒扫描 | 支持信任区设置，病毒扫描或实时防护时不扫描目录或文件。 |
| 病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件。 |
| 支持对终端当扫描到感染型病毒、顽固木马时，自动进入深度查模式，可设置禁止终端用户管理路径或文件白名单、禁止终端用户管理扩展名白名单、扫描时不允许终端用户暂停或停止扫描任务。 |
| 支持扫描资源占用设置，可设置不限制、均衡型、低资源三种模式。 |
| ★支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描。 |
| 主动防御 | ★支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护。 |
| 网络防护 | 支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。 |
| 支持僵尸网络攻击防护，对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2连接等威胁。 |
| 终端病毒处理弹窗 | 客户端弹窗支持免打扰模式和智能模式，使用免打扰模式可以对不能弹窗的终端设备中避免弹窗。使用智能模式是智能调整弹窗，对已知的病毒自动处理，对未知的病毒提示处理。 |
| 杀毒引擎 | 支持不少于三个杀毒引擎混合使用，提高病毒检出率。 |
| 补丁管理 | 补丁类型 | 支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复。 |
| 支持按补丁类型和级别修复，补丁级别需包括：安全更新、重要补丁、功能补丁、可选补丁。支持仅安装指定补丁设置。 |
| 支持精细配置按照操作系统版本修复漏洞，支持精细配置按照Office版本修复漏洞。 |
| 灰度发布 | ★支持管理员预先设置好灰度发布批次和漏洞修复策略（分时间段、按级别、排除有兼容性问题的补丁等），每当控制台更新补丁库，自动化编排完成漏洞修复——将全网终端划分为由小到大的多个批次，根据企业环境，自动先推送给第一个小批次分组，如无问题自动推送给下一个批次，直到推送给全网。如有问题，只需将有问题的补丁添加到排除列表和卸载已安装的终端即可。整个推送安装过程自动化编排，无需管理员过多参与，只需在有问题时添加排除列表和下发卸载补丁任务。 |
| 终端管控 | 外设管理 | 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMIA）设置使用权限，并支持生效时间设置。 |
| 支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源。 |
| ★支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。 |
| 进程管理 | 支持对单点维护功能，可远程查看终端实时运行的进程，需要包含进程名称，进程用户、命令行（执行路径+执行参数）、内存占用、签名、产品名称、公司名称等，支持远程结束进程。 支持远程查看计算机各个网卡配置信息。 |
| 支持终端进程红名单、黑名单、白名单功能。可设置核心进程必须运行，也可保护核心进程不被结束，违规并告警。 |
| 违规外联 | 支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理。支持例外白名单添加。 |

5.2、服务器杀毒软件（windows版）

|  |  |
| --- | --- |
| 模块 | 功能要求 |
| 技术要求 | ★支持终端发现可以通过扫描发现需要安装但没有安装终端的计算机，以免出现漏管漏控的情况； |
| ▲要求客户端安装后占用硬盘空间60M以内， 病毒库大小不超过10M，日常使用内存占用30M左右，有效节省电脑资源，共50台设备授权。 |
| ★要求中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将顶替宕机的主中心且同步数据 |
| ★要求支持备用中心查看和审批，支持通过本地安装的配置工具申请成为主中心的备用中心，主中心审批通过后，显示备用中心的相关信息 |
| ★要求支持邮件预警功能，当全网发现病毒事件、网络攻击事件、超过一周未更新时发送邮件通知 |
| 要求支持备份终端信息,分组及规则,防护策略,事件日志,管理员信息,系统设置；支持自动备份，按照月/周/时间设置自动备份 |
| 要求支持按全网终端迁移或部分终端迁移，当网络环境发生变化或物理设备出现故障时可转移终端 |
| ★要求支持可对终端添加多个中心地址,当终端接入网络环境时,中心可对终端实施管控 |
| 要求支持第三方软件调用API接口，包括调用漏洞修复信息查看、下发查杀任务、查看、创建、修改和删除分组信息、查询终端详情、终端资产信息、调用接口修改终端名称等 |
| 要求中心可统计全网操作系统版本信息、安装时间、激活状态且具有操作系统占比可视化数据图；可统计全网终端硬件信息包括CPU、内存、硬盘、硬盘序列号、硬盘ID、网卡、显卡、主板、主机序列号、显示器且支持硬件清单导出、支持全网终端硬件、软件变更历史记录包括变更时间等其他信息 |
| ★要求支持热补丁机制，利用产品自身防御功能，防护其他软件以及系统出现的漏洞，阻止对计算机造成损害与入侵 |
| ★要求具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库，却有较强的病毒查杀能力 |
| ★要求支持勒索病毒诱捕，可在根目录生成txt、pem、sql、xlsx、mdb、jpg、rtf、xls、doc、docx等格式的诱捕文件，当出现勒索行为，对其进行捕获并进行隔离 |
| ★要求支持恶意行为监控，通过监控程序运行过程中是否存在恶意操作来判断程序是否安全，从而可以作为传统特征查杀的补充，极大提升电脑反病毒能力 |
| ★要求支持暴破攻击防护，阻止黑客通过SMBv1、SMBv2、 RPC、SQLServer、PDP协议进行暴力破解攻击 |
| ★要求支持横向渗透防护，防护内网中已中毒机器感染其他主机，阻止横向传播、病毒以及木马的扩散防护项包括默认共享访问、远程服务创建、远程计划任务创建、远程注册表篡改、远程MMC调用、远程DCOM调用、远程WMI调用有效阻止病毒横向渗透 |
| ★要求支持系统加固，针对病毒会利用或修改的系统脆弱点，设置相应的防护规则，有效保护系统关键文件不被篡改、破坏或恶意创建，防止特定注册表项目不被恶意篡改，监控针对系统的敏感行为，拦截高风险动作，阻止特定命令行被恶意利用的行为，保护系统关键进程不被攻击利用，针对病毒特殊行为进行免疫等 |
| ★要求支持应用加固，通过对容易被恶意代码攻击的软件进行行为限制，防止这些软件被恶意代码利用 |
| ★支持软件禁用功能，可以设置使用违规软件的处理方式，包括记录、提示卸载以及隔离，可添加软件黑白名单，设置软件是否可用； |
| ★支持违规外联设置，探测终端用户是否有违规连接外部网络的行为； |
| ★要求具有终端动态口令验证功能，当终端用户登录计算机时都将弹出动态口令安全认证窗口，若用户设置了计算机密码，该弹窗将在用户输入正确的账户密码后弹出用户需再次输入正确的动态口令才可登入计算机且可设置应用范围：远程登录时启用或本地登录时启用 |
| ★要求终端具有弹窗拦截工具，具备自动拦截方式，手动截图拦截方式，可拦截流氓、广告、以及恶意弹窗等 |
| 要求支持导出安全分析报告，对当前中心进行安全状况分析并生成分析报告，可按照最近7天、最近30天、最近一年等时间范围生成报告，也可自定义时间范围生成报告；安全报告支持邮件订阅功能，可给管理员配置订阅功能 |
| 要求管理中心支持对Windows、linux、Mac各种不同操作系统版本的客户端统一运维管控 |
| ★要求产品完全自主研发，不涉及OEM，并对国内三家知名安全厂商提供技术赋能 |

5.3服务器杀毒软件（Linux版）

|  |  |
| --- | --- |
| 功能模块 | 功能要求 |
| 体系架构  系统部署 | 要求支持中/英文界面，系统部署采用 C/S 架构，管理采用 B/S 架构，管理员只需通过浏览器登录控制中心，即可对系统进行管理 |
| 要求端支持Windows XP、Windows 7、Windows 8、Windows 8.1、Windows 10、Windows、11、Windows Server 2003、Windows Server 2008、Windows Server 2012、Windows Server 2016、Windows Server 2019 |
| 要求支持CentOS、Ubuntu、SUSE、Deepin、中科红旗、银河麒麟、优麒麟、中标麒麟、龙芯（loongnix）、统信UOS等发行版 |
| 要求管理中心支持对Windows、linux、Mac各种不同操作系统版本的客户端统一运维管控 |
| ▲要求客户端安装后占用硬盘空间较少，病毒库大小不超过10M，日常使用内存占用较小，有效节省电脑资源，共十台设备授权。 |
| ★中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将顶替宕机的主中心且同步数据 |
| ★要求支持备用中心查看和审批，支持通过本地安装的配置工具申请成为主中心的备用中心，主中心审批通过后，显示备用中心的相关信息 |
| 要求支持级联部署及管理，可实时查看下级终端威胁及在线情况，上级可对下级灵活分配授权，上级可登陆下级中心直接进行管理，同时可实现分级管理中心能够通过一级管理中心升级病毒库和客户端版本 |
| 中心基础设置 | 要求支持展示全网终端安全概览：终端在线数量、最新安全动态、终端操作系统概览 |
| 要求支持展示全网终端安全事件可视化数据：7/30天病毒查杀事件 |
| 要求支持监控中心服务器性能：CPU使用率、内存使用率、磁盘占用率、网络流量使用状况 |
| 要求中心可启用SysLog日志导出功能，支持导出安全日志、升级日志 |
| ★要求中心支持任务通知，可在任务完成时、子中心连入时、子中心脱离时接收通知 |
| ★要求支持邮件预警功能，当全网发现病毒事件、超过一周未更新时发送邮件通知 |
| 要求中心具备事件日志模块，包含病毒查杀日志、终端管理日志、系统管理日志 |
| 要求中心支持全局信任区可通过信任文件路径、信任文件校验和方法添加信任文件以及添加信任网址 |
| 中心管理 | 要求支持中心定制功能，可将产品显示的LOGO替换为企业LOGO，按需自定义配置LOGO展示 |
| 要求可按照不同分组创建管理员以及设置管理员更换密码周期且管理权限可按模块划分，支持管理员接收邮件预警 |
| 要求支持中心无操作自动登出设置，防止管理后台闲置时自动退出，避免频繁登录 |
| ★要求中心具有登陆二次验证功能，开启该功能后，通过登录中心时进行二次验证的方式，阻止中心遭遇密码泄露、弱口令暴破、撞库等黑客破解行为带来的危害，达到保护控制中心的目的 |
| ★要求管理员可设置高危操作动态认证，添加信任文件时需要管理员进行二次动态认证后才可执行高危操作 |
| 要求支持备份终端信息,分组及规则,防护策略,事件日志,管理员信息,系统设置；支持自动备份，按照月/周/时间设置自动备份 |
| 要求支持按全网终端迁移或部分终端迁移，当网络环境发生变化或物理设备出现故障时可转移终端 |
| 要求支持离线终端可设置过期时间，过期终端超时后将自动从中心删除 |
| ★要求支持中心地址屏蔽来自搜索引擎的页面访问，当中心架设在公网时防止他人恶意访问 |
| 要求支持中心升级可配置手动、自动以及指定升级代理服务器 |
| 要求支持第三方软件调用API接口，包括调用接口获取全部分组信息、调用接口创建分组、调用接口修改分组名称、调用接口删除分组、调用接口查询上线终端情况、调用接口查询终端详情、调用接口修改终端名称、调用接口修改终端分组、调用接口查询终端详情 |
| ★要求支持可对终端添加多个中心地址,当终端接入网络环境时,中心可对终端实施管控 |
| 资产管理 | 要求中心可统计全网操作系统版本信息、安装时间、激活状态且具有操作系统占比可视化数据图 |
| 要求中心可统计全网终端硬件信息包括CPU、内存、硬盘、网卡、显卡、主板且支持硬件清单导出 |
| 终端运维管控 | 要求展示终端基本信息：终端名称、计算机名称、终端分组、本地IP、通信IP、MAC地址、终端类型、操作系统版本、病毒库版本、终端版本、唯一标识、最后上线时间、首次上线时间以及终端标签；可组合检索项进行全方位查询、定位、展示 |
| 要求中心支持对终端下发快速查杀、全盘查杀、自定查杀任务，可推送终端升级等任务，支持将终端拉黑，避免占用授权点数 |
| 要求中心可预览终端系统用户信息 |
| ★要求支持自定义标签内容，将标签自定义给予终端，可灵活对终端进行标记 |
| 要求可设置定时任务，支持快速查杀、全盘查杀、自定义查杀、终端升级且配置执行方式：自定义计划、单次执行、开机执行计划任务 |
| 要求中心可查看下发任务详情，包括任务执行状态、任务创建时间、过期时间且可终止已下发任务 |
| 反病毒引擎 | ★要求具有反病毒底层技术，反病毒引擎为本地反病毒引擎，不依赖云（联网时的病毒查杀能力与断网时的病毒查杀能力一致）具有轻量级的病毒库，却有较强的病毒查杀能力 |
| ★要求反病毒引擎具备全文哈希、分段哈希、局部敏感哈希、关键数据特征等扫描技术，可提取恶意代码中关键代码或数据片段来标识恶意代码 |
| ★要求反病毒引擎具有虚拟沙盒技术，能对待扫描的PE样本应用通用脱壳和动态行为扫描技术，用较少的记录，长期、有效地检出家族性样本且虚拟沙盒接近真实 CPU 的执行效率和高还原度的操作系统环境仿真且具有很强的抗干扰能力 |
| ★要求反病毒引擎具有基于虚拟沙盒的动态行为分析，可以跟踪和记录运行在其中程序的行为，通过行为记录，可以通过启发式分析算法对程序的恶意性进行评估 |
| ★要求反病毒引擎具有代码级修复能力，对寄生类恶意代码拥有完善的解决方案 |
| ★要求具有脚本动态行为启发查杀，无需静态特征，在可控虚拟沙盒中还原脚本病毒执行逻辑并评估恶意性 |
| ★要求支持对各种加壳的病毒文件进行病毒查杀，包括病毒使用的自定义壳、代码混淆器在内的所有其他代码级对抗技术，均可解决 |
| ★要求特征库具备轻巧性，将特征高度复用、重组恶意代码 DNA 片段来描述不同的恶意代码，最大限度减少特征库中的冗余数据 |
| ★要求支持病毒库更新周期为一天一更新，紧急或重大事故出现可及时升级 |
| ★要求支持十万多种家族类型病毒，亿级别以上样本数量 |
|  | ★要求产品完全自主研发，不涉及OEM，并对国内三家知名安全厂商提供技术赋能 |
| 日志报表 | 要求支持导出安全分析报告，对当前中心进行安全状况分析并生成分析报告，可按照最近7天、最近30天、最近一年等时间范围生成报告，也可自定义时间范围生成报告；安全报告支持邮件订阅功能，可给管理员配置订阅功能 |
| 要求支持内网环境中心使用离线增量包更新病毒库与组件版本 |
| 要求支持客户端主动升级及平台推送升级任务 |
| 要求病毒查杀日志可按照时间、系统类型、终端名称、终端分组、本地IP、病毒ID、病毒名称、病毒路径、查杀类型、处理结果、病毒库版本等检索项进行检索且可导出 |
| 要求终端日志可按照时间、终端名称、终端分组、本地IP、升级前版本、升级后版本、升级结果、操作描述等检索项进行检索且可导出 |
| 要求系统日志可按照时间、升级模块、升级前版本、升级后版本、升级地址、升级结果、管理员名称、管理员类型、管理员IP、操作模块、操作描述等检索项进行检索且可导出 |

6、工作站汇聚交换机

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 基本要求 | 1）★交换容量≥336Gbps，转发性能≥69Mpps，固化10/100/1000M以太网端口≥24，1000M SFP光接口≥4个；  2）★要求所投产品端口浪涌抗扰度≥10KV（即具备10KV的防雷能力）；  3）支持RIP/RIPng、OSPFv2/OSPFv3等三层路由协议；  4）支持CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作。  5）★支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行；  6）★支持快速链路检测协议（RLDP），可快速检测链路的通断和光纤链路的单向性，并支持端口下的环路检测功能；  7）支持虚拟化功能，可将多台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤50ms；  8）支持SNMP、CLI(Telnet/Console)、RMON、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web；  9）MAC地址表项≥32K； |

7、网络准入

|  |  |
| --- | --- |
| 指标类型 | 指标要求 |
| 客户端管控 | 支持客户端首次登录修改密码，可设定最小长度，数字、大小写组合以及非法登录尝试次数和锁定时间；▲本次客户端要求不少于200点。 |
| 安全测评 | ▲针对国产化操作系统与Windows操作系统：支持以弹窗方式自动对入网终端进行安全项目检查，不符合安全规范的终端不允许接入网络，检查项目包括网络监听端口检测、TELNET检测等； |
| ★支持安全测评项目的在线一键检测及一键全部修复功能；  ★支持自动检测、循环评测及后台自动修复功能。 |
| USB禁止使用 | 针对国产化操作系统与Windows操作系统：支持对存储类USB设备进行禁用，不影响非存储类USB外设使用；支持对USB设备进行禁止、只读或读写等权限控制。国产化操作系统支持禁止、读写控制。 |
| USB使用申请 | ★针对Windows操作系统，终端使用USB时可以主动发起申请操作，申请通过前不允许使用USB存储介质；★管理员可以对USB使用申请进行批准或拒绝操作。 |
| USB使用审计 | 针对国产化操作系统与Windows操作系统，支持对USB存储介质的插拔行为进行记录；Windows操作系统也支持对USB存储介质内的文件操作行为进行详细记录。 |
| 终端安全规范 | 针对国产化操作系统与Windows操作系统：  支持禁用终端所有USB存储设备、蓝牙设备、打印机、光驱介质使用；  支持禁用终端所有无线网卡、其它网卡（含虚拟网卡，除与服务器连接应用的网卡）外联设备；  支持IP/MAC绑定（可设定允许修改DNS）、共享等安全功能；  支持设置终端用户的应用程序黑名单；  支持定时关机、水印设置、终端信息显示功能；  ★支持邮件/FTP服务器访问控制，可根据域名、IP、端口进行管控配置； |
| 针对Windows操作系统：  支持禁用便携式设备介质使用；  支持禁止3G无线上网卡、手机代理上网、无线热点、调制解调器等外联设备；  禁止进入windows系统的安全模式、注册表设置；  ★支持禁用组策略、控制面板等安全功能；  支持指定版本和授权码的正版化软件检测；  支持禁止桌面弹窗；  支持设置终端用户的网站黑白名单以及SSID黑白名单；  ★支持垃圾清理，可清理回收站、缩略图缓存、临时文件、最近打开文件、系统日志、缺失的共享dll、chrome浏览器缓存、ie浏览器缓存、firefox浏览器缓存、Microsoft edge浏览器缓存、无效的快捷方式； |
| 终端行为审计 | 针对国产化操作系统与Windows操作系统，支持终端USB插拔审计功能； |
| ★支持审计数据的汇总分析功能，并支持通过图表的形式进行分析展现及导出、打印功能。 |
| 文件分发 | 针对国产化操作系统与Windows操作系统，实现从服务器端向客户端分发文件功能，支持单点、多点、分组、全终端推送；实现查看分发状态以及根据状态进行筛选再次发送； |
| 水印信息 | ★针对国产化操作系统与Windows操作系统，支持屏幕水印防护，内容包含用户名、所属部门等，同时支持自定义水印内容；  ★支持水印自定义展示样式，可设置平铺、左上角、右上角、左下角、右下角和居中展示，支持设定颜色、透明度、方向和字体； |
| 远程协助 | 远程控制不依赖于用户是否登录，也可以通过远程控制进行用户的注销和切换。管理端在控制用户端时，可以远程关闭用户端键鼠，实现完全控制，远程桌面管理发起时，应保证画面的实时性，实现操作和响应画面传输在1秒之内完成，支持全局热键远程执行的应用； |

8、上网行为管理

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| 硬件规格 | 多核处理 | 采用国际先进的多核处理器硬件架构及多核并行处理系统。 |
| 硬件与性能 | ★不少于200人网络环境使用；最大并发连接数为16万，最大新建连接数为11000个/秒；1U硬件，标配4个千兆电接口（其中含1个管理接口和1个HA接口），128G SSD硬盘。提供1个扩展插槽，单交流电源 |
| 管理口 | 设备必须具备独立的（具备标识的）网络管理接口。所有接业务接口均被用满后，仍然可以存在独立的管理口可以访问设备。 |
| 硬件Bypass按钮 | 设备必须提供物理硬件bypass按钮，便于设备巡检、设备故障时管理员无需重启、关机、断电即可恢复网络通畅。 |
| 设备部署 | 部署模式 | 设备可支持网关模式、镜像旁路模式、网桥模式、多路桥接模式部署。 |
| Portal模式 | ★设备在部署时支持模式选择，可设置为Portal模式，实现Portal服务器功能； |
| 网络支持 | IPv6支持 | 能够支持IPv6环境下的网址访问审计、生成分析报表等功能；能够在IPv6环境下，正确审计显示用户的IPv6地址。 |
| IPSec VPN | 支持标准IPSec协议的VPN功能，能够实现隧道建立于配置、隧道状态监视、证书管理等内容。 |
| IPSEC冗余 | ★IPSEC VPN支持冗余隧道设置，支持对冗余隧道按优先级或权重的分配方式进行配置 |
| 系统监控 | 设备状态 | 能够实时提供产品CPU、内存、磁盘使用率、网口状态、授权状态、系统情况等信息。 |
| 网络状态 | 能够实时提供在线用户趋势、设备流速趋势、用户流量排名、应用流量排名、用户实时流量和应用实时流量等信息。 |
| 安全管理 | 支持对病毒的查杀 | 支持配置病毒查杀策略，检查网络中传输的文件是否是病毒，支持记录日志、病毒过滤。 |
| 病毒云查 | ★支持与云端杀毒平台联动，对网络中传输的文件进行特征比对，以便减少对本地计算资源的消耗。至少应支持对以下几类网络应用传输的文件进行病毒云查杀：HTTP/FTP/IMAP/SMTP/POP3。 |
| 支持对恶意URL的云查杀 | 支持基于云端大数据安全平台，对恶意URL访问进行封堵和记录日志。 |
| 应用管理 | 应用审计及控制 | 应用协议库包含的应用数量不低于7100种，应用规则总数不低于30000种。 |
| 应用分类 | 可以对下载工具、视频播放、网络游戏、金融理财、即时消息、移动应用有独立的分类进行识别控制；为覆盖工作无关应用，移动应用不少于1000种，即时消息应不低于150种，虚拟货币交易平台不低于40种；为规避外发类风险，论坛发帖应不低于3000种，网络存储不低于100种，代理隧道不低于100种。 |
| 网页管理 | 网站分类库 | ★≥2.8亿条URL数据，在官网上有公开的URL库更新情况详细说明。 |
| 流量管理 | 多级虚拟通道 | 支持多级虚拟通道，可以将物理带宽分成至少7级虚拟通道，合理分配物理带宽资源。 |
| 流控策略 | 支持基于用户、时间、应用、源IP、目的IP和服务创建流量控制策略。 |
| 用户管理 | 组织架构建立 | 可通过手工方式、LDAP导入、数据库导入（SQL Server、MySQL、ORACLE）、文件导入、IP扫描等方式建立组织架构。 |
| web认证 | 支持本地、LDAP、Radius、邮件认证方式的WEB认证。支持在界面上通过配置，将一台设备作为独立的认证服务器配合审计设备使用，提升认证性能。 |
| 短信认证 | 支持短信认证方式，用户输入手机号作为用户名，设备通过短信网关为用户手机发送密码。短信认证能够根据不同用户推送不同认证页面，该认证页面可自定义。支持白名单。支持完整短信认证功能，无需额外购买短信网关。 |
| 微信认证 | 支持通过微信“扫一扫”二维码方式，快速连接Wi-Fi。 |
| 支持利用微信公众号进行网络接入的身份准入认证。 |
| 二维码认证 | ★支持接待人员扫描访客二维码方式授权访客使用网络；支持配置接待用户列表避免越权授权。 |
| 日志统计与报表 | 日志查询 | 可查询到网页访问、论坛发帖，webmail、邮件收发、应用访问、应用流量历史日志。 |
| 综合分析报告 | 支持上网行为分析报表、网络带宽分析报表、合规分析报表、效率分析报表、安全分析报表。 |
| 系统管理 | 支持三权制衡管理机制 | 支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端。系统管理员和审计员的账号创建，权限变更需要审核员审批才能生效。管理员和审计员的操作会形成日志受审核员监督。 |
| 产品资质 | 产品资质和服务 | 公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》。 |

9、云防服务

|  |  |
| --- | --- |
| 序号 | 技术参数功能要求 |
| 1 | 通过云WAF方式，对用户的访问请求进行监控过滤，能够抵御通用类型的SQL注入、文件包含、远程命令、WEBSHELL、XSS跨站、代码执行、文件注入等攻击威胁。 |
| 2 | 支持上传SSL证书； |
| 3 | 支持自主设置特定IP的WAF拦截要求；并支持自主设置WAF拦截IP白名单； |
| 4 | 能够支持端口设置功能，进行支持配置80、443端口以外的端口及端口转发策略；提供证明材料 |
| 5 | 能够识别Web攻击者的IP所在地区，如是境外IP，可限制境外IP访问，并支持设定限制时间 |
| 6 | 能够按照访问时间进行防御，允许或者阻止一定时间段内的访问； |
| 7 | 能够识别出各种Web扫描器的自动化扫描和攻击行为，并进行扫描阻断； |
| 8 | 能够定义给定的URL作为网站后台管理页面，允许特定IP进行访问，同时可以对URL访问进行限速； |
| 9 | 能够爬取网站的所有静态页面，并据此代替网站提供服务； |
| 10 | 能够检查网站内容，发现敏感信息、反动言论和淫秽内容进行屏蔽；能够提供自定义敏感信息功能； |
| 11 | 能够支持报表自定义日期查询数据和日志下载功能。 |
| 12 | 支持网站缓存功能，即使网站源站内容被篡改，访客访问到的内容也是网站原来缓存的内容 |
| 13 | 支持网站可用性监控功能，在网站异常无法提供服务时进行告警 |
| 14 | 全平台支持IPv6，支持IPv4/IPv6DNS解析服务、支持IPv4/IPv6访问服务、支持IPv4/IPv6攻击流量进行清洗，均需支持在不改变源站配置的情况下实现。支持无感知解决天窗问题，保障网站访问者在纯IPv6网络环境下访问网站不出现天窗问题。 |
| 15 | 支持云端https，并回源http；https支持SNI（Server Name Indication）取源。 |
| 16 | 支持全网协同防御，拥有不少于五种以上的数据分类。支持洋葱路由IP、IDC IP，代理IP一键拦截能力，相关IP数据库提供动态更新能力。 |
| 17 | 支持保护网站图片、压缩包等资源文件不被其它站点盗用。 |
| 18 | 支持一键关停网站服务功能。 |
| 19 | 支持网站永久在线 |
| 20 | 最少支持10个以上地区的节点同时提供防御服务，支持全国范围内的节点无缝调配。 |
| 21 | 协议支持http、https、HSTS、websocket。 |
| 22 | 支持按照域名取源和IP取源方式 |
| 23 | 由信息安全等级保护关键技术国家工程实验室提供服务支撑 |
| 24 | 支持攻击态势可视化，应包括：  实时获取网络攻击行为，实时发现、分析、报警；  根据关联请求日志分析黑客攻击手段、攻击IP定位属性信息；  对发现的新黑客攻击进行分析，历史攻击行为进行描绘，做到黑客追踪的分析能力；  以地图形式实时显示网站遭受攻击的情况；  展示内容包括攻击的具体来源、IP地址、所属国家（地区）并标示攻击类型，并对威胁程度大的攻击行为及时报警，展示页面。 |
| 25 | ▲由信息安全等级保护关键技术国家工程实验室分实验室提供技术支撑。 |

10、安全运维服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 安全服务项目 | 服务内容 | 服务说明 | 服务频率 |
|  | 安全巡检 | 安全配置核查 | 1、对安全设备、网络设备、服务器、存储等设备的配置进行等保合规性检查；  2、对配置核查过程中发现的问题进行总结，并出具相关配置核查服务报告。 | 每月一次 |
| 安全日志分析 | 1、对防火墙、入侵防御、安全审计产品、终端防护产品等安全设备进行事件审计和日志分析，检查审计日志是否正常，是否有可疑事件发生；  2、一旦发现网络入侵事件或者尝试入侵事件，及时通知客户并提供阻止入侵的技术手段建议。 |
|  | 漏洞扫描服务 | 对网络设备、安全设备、应用系统等提供漏洞扫描服务 | 1、对网络设备、安全设备、服务器操作系统和业务应用系统进行漏洞扫描服务，并出具相关报告；  2、有新设备或新业务上线时，对业务及设备进行安全扫描检查，并提供结果报告。 | 每月一次 |
|  | 安全加固服务 | 针对安全巡检、漏洞扫描、测评报告中发现的各种安全隐患提供安全加固。 | 1、针对巡检过程中发现问题，如特征库更新、策略无效等，进行安全策略调整；  2、针对漏洞扫描、渗透测试和安全评估过程中发现的各种安全隐患，进行安全加固和安全优化。 | 每季度一次 |
|  | 攻防演练 | 对单位的重要信息系统进行攻防演练 | 对单位的重要信息系统进行攻防演练，由攻击组开始对网络和系统实施模拟攻击。  攻击手段主要有注入攻击、脚本攻击、拒绝服务攻击、密码爆破、利用漏洞（溢出，逻辑）、旁注攻击、社会工程攻击、数据传输攻击等等  最终由防护组和攻击组将各自结果形成报告，并开展安全防护工作。 | 每年一次 |
|  | 应急响应服务 | 当发生黑客入侵、系统崩溃或其它影响业务正常运行的安全事件时，第一时间对安全事件进行应急响应处理 | 1、在15分钟内电话响应，在2小时内到达现场，并在4小时候内使安全事件的事态得到控制，给出相应的解决方案；  2、针对在应急响应服务的所遇到的安全问题、安全事故处理过程、处理结果，48小时汇总形成应急响应服务结果报告，提交给客户。 | 按需 |
|  | 网络安全培训 | 组织单位人员进行网络安全意识培训 | 通过ppt的方式，结合当下的网络情况，及单位的自身需求，对单位的网络情况进行分析，提高单位人员的整体网络安全意识。 | 每年一次 |

三、相关要求

1、合同履行期限：

2023年12月15日前交货并安装调试结束。

2、标的验收：

建设完成后由供货单位提请验收，以通过业主单位验收合格为准，供货单位须确保一次性通过验收，如通不过验收或因验收事项造成采购单位损失的，由供货单位承担相关责任及经济损失。

3、质保期（验收合格后）：

质保三年。

4、付款方式：

合同签订后5个工作日内付至合同经额的90%，项目完成安装、调试并经验收合格、等保测试合格后30天内,甲方向乙方支付至合同金额的95%，验收合格满三年后付清。

5、售后服务及其他（含安装、调试、培训、维护等）：

（1）投标人具有良好的信誉，售后服务及时到位。

（2）供方免费送货上门、安装调试、人员培训。

（3）供应商应具备完善售后服务体系，在南通地区有办事处及有固定的维护人员并有能力及时处理所有可能发生的故障。

（4）售后响应速度为12小时内登门服务。24小时内修复，24小时不能修复的须免费提供备用设备至修复。提供培训及售后服务计划方案。

（5）超出保修期后，仍需提供维护服务，并承诺只收取成本费。

报价响应文件所需文件（需加盖公章）

1、企业有效营业执照副本复印件

2、法人身份证明书和授权委托书

3、主要设备厂商奇安信公司针对本项目授权书

4、报价函（含分项报价表）

报价请于2023年10月26日前密封后递交（可邮寄或现场递交）。

询价人联系方式：盛开，电话：19201774877，地址：南通市通州区金沙街道新金西路68号。

江苏有线网络发展有限责任公司通州分公司

2023年10月19日

一、法定代表人身份证明书

投标人：

单位性质：

地址：

成立时间：年 月 日

经营期限：

姓名：性别：

年龄：职务：

系 （报价供应商名称）的法定代表人。

特此证明。

报价人：（盖单位章）

年 月 日

附法定代表人（负责人）身份证复印件

二、授权委托书

本人 系 的法定代表人，现委托 （身份证号： ）为我方代理人。代理人根据授权，以我方名义签署、澄清、说明、补正、递交、撤回、修改  项目的报价响应文件，签订合同和处理有关事宜，其法律后果由我方承担。

代理人无转委托权。

被委托人： 性别： 年龄： 岁

被委托人单位：

部门： 职务：

报价人： （盖单位公章）

法定代表人（签字或印鉴）：

附授权委托人身份证复印件

三、报价函

致：（询价人）

1、依据贵单位项目询价文件，我方愿意按照询价文件的要求，我单位愿以人民币 （大写） 元的价格，完成本项目的全部服务内容。

2、本询价有效期为自报价文件落款日起10天。

3、同意并接受询价文件的各项要求，遵守询价文件中的各项规定，按询价文件的要求提供报价。

4、我公司已经详细阅读了全部询价文件，我方已完全清晰理解询价文件的要求，不存在任何含糊不清和误解之处，同意放弃对这些文件所提出的异议和质疑的权利。

5、我公司已毫无保留地向贵方提供一切所需的证明材料。

6、一旦我方中选，我方将根据询价文件的要求签订合同，严格履行合同的责任和义务，并保证在询价文件规定的时间完成服务。

报价人：（加盖公章）

法定代表人：（签字或盖章）

年 月 日

附：分项报价单

分项报价表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 规格、配置参数、品牌 | 数量 | 单位 | 单价  （元） | 金额  （元） | 备注 |
| 1 | 下一代防火墙 | 奇安信  NSG5000-TG15 | 5 | 台 |  |  |  |
| 2 | 日志审计 | 奇安信 LAS-R32P | 2 | 台 |  |  |  |
| 3 | 数据库审计 | 网御星云  LA-DAP-4000 | 1 | 台 |  |  |  |
| 4 | 堡垒机 | 奇安信 C6100-BH-TF10 | 2 | 台 |  |  |  |
| 5 | 终端及其服务器杀毒软件 | 奇安信ESM-FL；  火绒 终端安全管理系统 | 1 | 套 |  |  | 200台终端；服务器端：windows50台，linux 10台 |
| 6 | 工作站汇聚交换机 | 锐捷 RG-S5300-24GT2SFP2XS-E | 4 | 台 |  |  |  |
| 7 | 网络准入 | 金盾 ID-MST-03 | 1 | 台 |  |  |  |
| 8 | 上网行为管理 | 奇安信NI3200-10A | 1 | 台 |  |  |  |
| 9 | 云防服务 | 国产 | 3 | 年 |  |  |  |
| 10 | 安全运维服务 | 国产 | 3 | 年 |  |  |  |
| 11 | 系统集成服务 | 国产 | 1 | 次 |  |  |  |
|  | 合计：大写 小写： | | | | | | |