**网络安全设备项目采购需求**

**一、采购需求及预算明细**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **单价（元）** | **数量** | **合计（元）** | **质保** |
| 1 | 日志审计系统 |  | 1台 |  | 原厂三年 |
| 2 | 40G边界安全视频网关 |  | 1台 |  | 原厂三年 |
| 3 | 20G边界安全视频网关 |  | 2台 |  | 原厂三年 |
| 4 | 集成服务 |  | 1项 |  | 3年服务 |
| **5** | **合计** |  |  | **370000** |  |

**二、参数要求**

**1.安全设备**

|  |  |
| --- | --- |
| **设备名称** | **技术参数** |
| 日志审计系统 | 1.采用中国自主创新的龙芯3A4000处理器，配套统信UOS V20操作系统，标准机架式设备,1+1冗余电源。（投标人所投的设备参数应满足或优于采购需求中的技术参数）  2.主机业务端口需求：千兆电口≥4个，千兆光口≥4个，内存≥16G,存储硬盘≥4T（企业级），板卡扩展槽位≥2个,配套日志授权≥40个；  3.均值EPS≥1300，峰值EPS≥1500；  4.独立完成审计日志采集，不依赖于设备或系统自身的日志系统；审计工作不影响被审计对象的性能、稳定性或日常管理流程；审计结果存储于独立存储空间；自身用户管理与设备或主机的管理、使用、权限无关联；全中文WEB管理界面，无需安装任意客户端软件或插件。  5.日志采集设备支持厂家包括但不限于：Cisco(思科)、Juniper、联想网御/网御神州、F5、华为、H3C、微软、绿盟、飞塔(Fortinet)、Foundry、天融信、启明星辰、天网、趋势、东软、Nokia、CheckPoint、Hillstone(山石)、安恒信息、珠海伟思、BEA、中国电信、安氏、帕拉迪、APC、Arbor、Clam、戴尔（Dell）、Digium、东方电子、EMC、中国电力科学研究院、Eudora、Google、冠群金辰、Linksys、McAFee、Netapp、NAS、永达、Sonicwall、Vigor、天存、Symantec（赛门铁克）、Hardened-PHP、Foundertech(方正)、三零盛安、Allot、蓝盾、IBM、金诺网安、网威、Nortel(北电)、Citrix(思杰)、Watchguard、中兴、阿帕奇、Windows系统日志、Linux/UNIX syslog、IIS、Apache等；  6.支持Syslog、SNMP Trap、HTTP、ODBC/JDBC、WMI、FTP、SFTP、kafka等协议方式进行日志收集,支持阿里云SLS日志的采集；  7.可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。  8.支持使用代理(Agent)方式提取日志并收集，安装包支持界面下载，且安装支持可视化向导。  9.支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等。  ★10.内置5000+解析规则，支持对收集的5000+设备类型日志进行解析（标准化、归一化），解析维度多达200+，解析规则可以根据客户要求定制扩展；  11、可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况）；  ★12、具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件（提供截图证明）；  ★13、内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景（提供截图证明）；  ★14、日志syslog转发：支持将收集到的日志进行加密(国密算法SM4)、签名(国密算法SM3)转发传输，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备；(提供截图证明)  15、通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息（提供第三方检测报告）；  16、支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据（提供截图证明）；  ★17、需提供产品的《计算机信息系统安全专用产品销售许可证》。  ★18、产品需入围信创。 |
| 40G边界安全视频网关 | 1、具备传统防火墙、入侵防御、僵尸网络检测、应用识别与流控等功能，通过IPS签名拦截被感染的摄像头，防止摄像头将病毒带入视频监控网络中。  2、支持有效防御蠕虫、木马、僵尸网络、跨站攻击等常见攻击；支持自定义签名，灵活快速应对突发威胁；支持对主流摄像头厂家的私有视频协议的漏洞检测及防护。  ★3、主机网络层吞吐量≥40G，应用层吞吐量≥20G，防病毒吞吐量≥3.5G，IPS吞吐量≥3.5G，全威胁吞吐量≥2G，并发连接数≥420万，新建连接数≥19万。（提供技术参数证明）  ★4、主机内存大小≥16G，硬盘容量≥480G SSD，电源：冗余电源，千兆业务电口≥12，千兆业务光口≥4，万兆业务光口SFP+≥6。  5、支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。  6、支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。  7、支持IPsec VPN和SSL VPN功能。  ★8、支持应用管控功能，应用特征识别库数量大于9000种。（需提供产品功能截图证明）  9、支持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。  ★10、支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。（需提供产品功能截图证明）  ★11、产品需支持勒索病毒检测与防御功能，所投产品须提供具备CMA（中国国家认证认可监督管理委员会）认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告证明。  ★12、产品内置不低于10000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明）  ★13、产品内置超过4580种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。  ★14、产品支持未知威胁检测能力，需提供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、公安部信息安全产品检测中心之中任意一家检测机构出具关于“未知威胁检测”的证书或检测报告。  ★15、配备3年防病毒、IPS、URL特征库安全授权，SSL VPN接入授权50个。 |
| 20G边界安全视频网关 | 1、具备传统防火墙、入侵防御、僵尸网络检测、应用识别与流控等功能，通过IPS签名拦截被感染的摄像头，防止摄像头将病毒带入视频监控网络中。  2、支持有效防御蠕虫、木马、僵尸网络、跨站攻击等常见攻击；支持自定义签名，灵活快速应对突发威胁；支持对主流摄像头厂家的私有视频协议的漏洞检测及防护。  ★3、主机网络层吞吐量≥20G，应用层吞吐量≥8G，防病毒吞吐量≥1.5G，IPS吞吐量≥1.3G，全威胁吞吐量≥1G，并发连接数≥220万，HTTP新建连接数≥15万。（提供技术参数证明）  ★4、主机内存大小≥8G，硬盘容量≥128G SSD，电源：冗余电源，千兆业务电口≥6，万兆业务光口SFP+≥2。  5、支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。  6、支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。  7、支持IPsec VPN和SSL VPN功能。  ★8、支持应用管控功能，应用特征识别库数量大于9000种。（需提供产品功能截图证明）  9、支持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。  ★10、支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上。（需提供产品功能截图证明）  ★11、产品需支持勒索病毒检测与防御功能，所投产品须提供具备CMA（中国国家认证认可监督管理委员会）认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告。  ★12、产品内置不低于10000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明）  ★13、产品内置超过4580种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。（需提供产品功能截图证明）  ★14、产品支持未知威胁检测能力，需提供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、公安部信息安全产品检测中心之中任意一家检测机构出具关于“未知威胁检测”的证书或检测报告。  ★15、配备3年防病毒、IPS、URL特征库安全授权。 |

**2.集成服务：**

|  |  |
| --- | --- |
| **服务内容** | **技术要求** |
| 1. 技术集成 | 1. 安装日志审计系统与分局视频专网侧，对涉及的服务器、交换机等设备进行安全管控。 2. 安装40G边界安全视频网关设备至视频共享平台各局办业务对接侧，更换原有设备，配置安全数据，需与现有平台的技术人员沟通进行现有平台对接数据业务的割接迁移工作。 3. 安装20G边界安全视频网关设备至公安视频专网平台及公安信息内网对接边界，配置安全数据，需与现有网闸系统的技术人员沟通进行现有平台对接数据业务的割接工作。 4. 项目涉及共享总平台、视频专网平台、公安信息内网平台的安全数据更改配置，及原有系统、网路、交换机等对接需重新对接。本次项目实施需与分局平台升级同步实施，需现有核心交换机维护单位、各平台原厂技术、网闸等原厂技术配合实施。投标人需配套专业技术人员进行项目设备割接及业务对接，项目验收后技术运维服务三年。 5. 提供一年一次的系统漏洞扫描服务，共计3次。 6. 对安全设备提供一个月一次的现场病毒库、特征库及规则库等的现场离线更新服务 |

**三、商务要求：**

★1.投标人需具备本项目的实施技术能力，需具备至少一名高级网络工程师（H3CIE、HCIE等），一名注册信息安全工程师，提供证书复印件及截止当前连续三个月的社保证明。

★2.报价含投标商供应产品到达买方并能正常使用的一切费用，含税金，运输费，装卸费，保险费，安装调试费，技术服务费，系统联调费，测试费，保修费等等。

★3.采购需求文件（含附件）中标有“★”的技术指标不容许发生偏离，如发生偏离或其他技术指标如有明显不符合采购文件（附件）参数标明的，采购单位有权取消其中标资格，验收时发现产品不符合采购文件（附件）参数要求或中标单位提供的中标产品详细参数则不予验收通过。

★4.考虑项目采购的设备需与现有的各平台业务系统对接，涉及兼容性及技术要求符合性问题，各投标商必须同步上传产品明细价格表（包括品牌、型号、规格、价格）、产品技术参数偏离表（格式自设）及打“★”技术参数的检测报告或技术功能证明材料或其他要求提供的证明材料，否则视投标无效。

★5、投标人所交付的产品应是交付前未被使用过的全新产品，同时必须具有在中国境内的合法使用权，并提供随机配件。中标供应商需在项目验收中提供中标产品原厂保修证明材料，不能提供的预中标供应商放弃成交资格。

★6.货款结算：

①甲方应于本合同生效后10个工作日内向乙方支付合同总价款的60 %作为预付款；

②全部货物验收合格后 10 个工作日内，甲方向乙方支付至结算审定金额的100%。

7.履约保证金：

①本合同签订后  7 个工作日内，乙方应向甲方支付合同总价  1  %的履约保证金（履约保证金可以是银行或保险公司出具的履约保函），作为乙方认真履行合同条款的保证。

②在无质量问题的情况下，履约保证金待项目验收结束后无息返还 。

8.工期要求：签订合同后30天内完成安装调试，试运行1个月后乙方可申请终验。

9.设备原厂免费质保三年，在保修期内每季度提供一次上门巡检，原厂保修服务内容必须是其标准的产品服务和投标承诺的服务，质保期满后，必须配合采购单位做好后续衔接工作。

10. 项目验收：设备提供符合采购技术需求，到货数量完整，技术集成服务完成并满足相关要求，系统运行正常视作验收合格。

★11.售后：提供现场安装及培训服务，安装、调试时中标人必须指派专业技术人员现场值守，直至验收合格。接到用户报修电话，10分钟内响应，0.5小时内赶到现场排除故障。