# 招标需求

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **货物名称** | **是否为核心产品** | **单位** | **数量** |
|
|
| 1 | 边界防火墙 | 否 | 台 | 3 |
| 2 | 运维审计系统 | 否 | 台 | 1 |
| 3 | 高级威胁检测系统 | 否 | 台 | 1 |
| 4 | 日志管理系统 | 是 | 套 | 1 |

**第一部分 货物采购需求一览表**

**第二部分 技术要求**

重要性分为“★”、“#”和一般无标示指标。★代表最关键指标，不满足该指标项将导致投标被拒绝，#代表重要指标，无标识则表示一般指标项。

**1技术指标要求**

1. **边界防火墙**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标** | **指标项** | **详细要求** |
| 1 | **硬件配置** | 产品形态 | 1U |
| 2 | ★电源 | 冗余电源 |
| 3 | CPU | 飞腾 |
| 4 | 操作系统 | 银河麒麟 |
| 5 | ★内存 | ≥16G |
| 6 | ★硬盘 | ≥1TB |
| 7 | ★接口配置 | 最大配置为26个接口，默认含1个管理口、5个千兆电口、4个千兆光口 |
| 8 | **★系统性能** | 整机网络层吞吐量(双向) | IPv4≥7121.831Mbps |
| IPv6≥7198.180Gbps |
| 9 | 整机应用层吞吐量(单向) | IPv4≥2076.333Mbps |
| IPv6≥2079.667Mbps |
| 10 | 整机TCP新建 | IPv4≥10.666万/秒 |
| IPv6≥9.998万/秒 |
| 11 | 整机TCP并发 | IPv4≥300万 |
| IPv6≥300万 |
| 12 | **基本要求** | **★**系统结构 | 产品由专用的国产化硬件平台、国产化安全操作系统及功能软件构成；支持飞腾处理器、银河麒麟等操作系统或兆芯处理器、中标麒麟操作系统；不低于4核CPU，主频不低于1.5GHz，CF不低于4G； |
| 13 | **★**操作系统 | 安全操作系统采用冗余设计 |
| 14 | **★**系统软件 | 系统具有良好的扩展性，支持扩展病毒防御、入侵防御、应用识别、网站分类库过滤、IPSEC VPN等功能。 配置web过滤功能模块，不少于3年规则库升级许可。配置应用识别功能模块，不少于3年规则库升级许可。 |
| 15 | **网络接入** | 工作模式 | #支持路由、交换、虚拟线、Listening、混合工作模式（需提供截图或其他证明材料，加盖投标人公章） |
| 16 | 路由交换 | #支持RIP、OSPF、BGP4、802.1q、QinQ； |
| 17 | #支持策略略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；  |
| 18 | 链路聚合 | #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。（需提供截图或其他证明材料，加盖投标人公章） |
| 19 | IP/MAC绑定 | #支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作； |
| 20 | 地址转换 | #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；支持源IP转换同一性；  |
| 21 | DNS Doctoring | #支持DNS Doctoring功能（需提供截图或其他证明材料，加盖投标人公章）； |
| 22 | **访问控制** | 访问控制 | #支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、邮件安全、数据过滤、文件过滤、审计、APT等功能配置,简化用户管理； |
| 23 | #支持域名控制，支持对多级域名进行控制，域名对象支持通配符； |
| 24 | #访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址； （需提供截图或其他证明材料，加盖投标人公章） |
| 25 | #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； |
| 26 | #提供策略查询功能，支持五元组快速查询以及针对策略名、源/目的区域、源/目的地址、服务、对象、未命中时间等条件进行细粒度检索； |
| 27 | **IPv6** | 双栈模式 | 支持IPv4/IPv6双栈工作模式，支持RADVD、ND、RIPng、OSPFv3、BGP4+；  |
| 28 | 访问控制 | #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 |
| 29 | #支持IPv6域名控制，支持对多级域名进行控制，域名对象支持通配符； |
| 30 | 安全防护 | #支持对IPv6报文进行病毒防御、入侵防御、URL过滤、抗DDOS、流量控制、连接限制、文件过滤、数据过滤等； （需提供截图或其他证明材料，加盖投标人公章） |
| 31 | **用户管控** | 认证方式 | #内置用户身份管理系统，支持本地认证、外部认证及免认证等方式，支持RADIUS、LDAP、TACACS等第三方外部认证；（需提供截图或其他证明材料，加盖投标人公章）  |
| 32 | 用户管控 | #综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控；支持手动创建用户、批量导入导出用户，同时支持设备扫描方式创建用户；  |
| 33 | #支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；  |
| 34 | #支持查看在线用户情况和用户流量，可显示用户流量、会话、新建连接列表及趋势图，支持用户流量排名； |
| 35 | #支持本地CA和第三方CA，支持作为CA认证中心为其他人签发证书（需提供截图或其他证明材料，加盖投标人公章）；支持标准CRL列表，支持CRL手工更新（需提供截图或其他证明材料，加盖投标人公章），  |
| 36 | **安全防护** | 入侵防御 | #支持独立的入侵防护规则特征库，特征总数在5500条以上（需提供截图或其他证明材料，加盖投标人公章），能对常见漏洞进行安全防护，兼容国家信息安全漏洞库； |
| 37 | #规则库支持根据攻击类型、风险等级、流行程度、操作系统等进行分类，防护动作包括告警、阻断、记录攻击报文； |
| 38 | #支持针对地址、应用设置入侵防御白名单，支持攻击规则搜索以及自定义规则，自定义规则支持导入导出；  |
| 39 | 支持对威胁事件、攻击来源、受威胁主机、威胁趋势等进行监控统计，并可进行可视化展示； （需提供截图或其他证明材料，加盖投标人公章） |
| 40 |  |
| 41 | 行为分析 | #内置行为分析功能，对会话、流量等数据进行统计分析，建立业务行为基线，对异常行为进行告警；支持行为分析监控展示，可展示不同行为分析策略的实时数据和基线数据趋势； |
| 42 | DDOS防御 | #支持针对IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议进行DDOS防护（需提供截图或其他证明材料，加盖投标人公章）  |
| 43 | #支持IP DDOS防护，可对IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke等异常报文攻击；  |
| 44 | #支持TCP DDOS防护，可对TCP Flood、SYN Flood、FIN Flood、RST Flood、新建SESSION Flood、SESSION Flood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； |
| 45 | #支持UDP DDOS防护，采用报文大小限制、阀值检查、源/目的限流方式综合进行UDP FLOOD防护；（需提供截图或其他证明材料，加盖投标人公章）  |
| 46 | #支持DNS DDOS防护，可对DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒攻击、DNS格式检查、DNS NX异常比率检测等；  |
| 47 | #支持HTTP DDOS防护，可对HTTP Flood、HTTP新建连接Flood、HTTP并发连接Flood、HTTP URI CC等攻击检测 |
| 48 | #支持NTP DDOS防护（需提供截图或其他证明材料，加盖投标人公章） |
| 49 | #支持根据DOS/DDOS攻击行为自动添加动态黑名单功能； |
| 50 | 病毒过滤 | #支持对HTTP/SMTP/POP3/FTP/IM等协议进行病毒防御，病毒特征库规模超过200万；  |
| 51 | 文件过滤 | #内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM文件传输等应用类型以及HTTP/FTP/SMTP/POP3等标准协议进行检测； |
| 52 | 内容过滤 | 内置内容过滤功能，支持基于HTTP、FTP、TELNET、SNMP、POP3、IMAP等协议的内容过滤策略；  |
| 53 | #支持对HTTP命令进行过滤；  |
| 54 | #支持对FTP信令进行过滤 |
| 55 | #支持对邮件内容进行过滤 |
| 56 | 黑名单 | #内置静态黑名单功能（需提供截图或其他证明材料，加盖投标人公章） |
| 57 | #内置动态黑名单功能（需提供截图或其他证明材料，加盖投标人公章） |
| 58 | 白名单 | 内置白名单功能，支持针对入侵防御、抗DDOS、审计、流量管理等功能自定义IP、应用白名单； |
| 59 | **系统管理** | 配置维护 | #支持配置文件本地备份和回滚，支持≥3个配置文件备份，支持对访问控制策略、NAT策略等关键配置进行单独及加密备份和恢复；支持对配置命令及配置文件的操作行为进行审计；（需提供截图或其他证明材料，加盖投标人公章）  |
| 60 | 升级维护 | #支持软件版本本地备份，支持对软件版本进行快速升级及回滚；（需提供截图或其他证明材料，加盖投标人公章）  |
| 61 | 系统诊断 | #支持在WEB界面进行网络诊断，支持PING、TRACEROUTE、TCP、HTTP、DNS诊断方式 |
| 62 | #支持在WEB界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出；  |
| 63 | **数据中心** | 报表 | #内置16种预定义报表模板，支持应用流量、用户流量、上网行为、威胁统计等报表，支持报表自定义；（需提供截图或其他证明材料，加盖投标人公章）  |
| 64 | #支持一次性报表及周期性报表 |
| 65 | 审计 | #支持独立审计策略，支持审计白名单；（需提供截图或其他证明材料，加盖投标人公章）  |
| 66 | #支持访问网站URL 地址、网页标题和网页内容审计；  |
| 67 | #支持对接收/发送邮件内容进行审计；对FTP上传/下载文件内容进行审计；  |
| 68 | #提供审计数据查询功能 |
| 69 | 日志 | #支持日志本地存储（需提供截图或其他证明材料，加盖投标人公章） |
| 70 | #支持日志外发（需提供截图或其他证明材料，加盖投标人公章） |
| 71 | **显示监控** | 设备状态 | #支持硬件资源实时利用率及其历史使用情况追踪；  |
| 72 | 流量统计 | 支持根据应用对通过设备的数据进行统计 |
| 73 | 支持根据用户对通过设备的数据报文流量进行统计 |
| 74 | #支持根据服务器对通过设备的数据报文流量进行统计（需提供截图或其他证明材料，加盖投标人公章） |
| 75 | 威胁统计 | #支持对病毒防御、入侵防御、DDOS攻击等按照威胁类型/攻击主机/受攻击主机三种维度结合威胁等级和时间周期进行统计、排名。（需提供截图或其他证明材料，加盖投标人公章） |
| 76 | **管理员** | 三权分立 | 系统内置系统管理员、安全操作员和安全审计员三类管理员角色，管理员权限相互制约； |
| 77 | 管理员设置 | #支持系统管理员本地认证、外部认证和证书认证 |
| 78 | 支持设置管理员首次登录是否强制修改密码，支持密码强度、有效期设置； |
| 79 | 其他要求 | 目录要求 | 设备厂商需承诺所投产品在最新一期《安可替代工程核心产品名录》、《安可替代工程适配产品清单》中，提供承诺函。 |

**2）运维审计系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标** | **指标项** | **详细要求** |
| 1 | 硬件配置 | 机箱 | 2U标准高度； |
| 2 | ★电源 | 配置模块化冗余电源； |
| 3 | ★接口配置 | 配置可扩展为不少于26个接口,投标产品配置6个千兆电口、4个千兆光口,2个扩展槽位 |
| 4 | ★授权许可 | 主机许可 | 不少于200个主机/设备许可，用户数不限制。 |
| 5 | 部署方式 | 工作模式 | 采用物理旁路部署 |
| 6 | 高可用性 | 支持双机部署 |
| 7 | 用户管理 | 用户管理 | 支持用户的增删改查、锁定、激活，进行用户全生命周期管理，支持用户批量导入和导出 |
| 8 | 角色管理 | 采用三员管理 |
| 9 | 认证管理 | 支持本地认证和三方认证服务器接入认证 |
| 10 | #支持数字证书等方式进行双因子认证。、等（需提供截图或其他证明材料，加盖投标人公章） |
| 11 | 用户组管理 | 支持用户组的增删改查 |
| 12 | 资产管理 | 资产管理 | 支持中标麒麟、银河麒麟、Windows等操作系统，支持网络设备、安全设备、数据库等的资产管理 |
| 13 | #支持修改管理协议默认端口（需提供截图或其他证明材料，加盖投标人公章） |
| 14 | #支持资产的批量导入导出（需提供截图或其他证明材料，加盖投标人公章） |
| 15 | 资产组管理 | 支持资产组的增删改查 |
| 16 | 资产账号 | 账号添加 | 支持资产账号手动添加，支持账号的批量导入导出 |
| 17 | 账号改密 | #自动对Windows、Linux等设备进行账号改密，改密支持手动和定期任务，密码配置支持全局策略和手工指定，密码复杂度支持按策略随机生成（需提供截图或其他证明材料，加盖投标人公章） |
| 18 | 权限管理 | 授权管理 | 支持按照用户、用户组、资产、资产组、管理协议、资产账号进行一对一、一对多、多对一、多对多授权 |
| 19 | 运维策略 | 支持会话、指令、剪切板上下行、文件上传下载的约束行为； |
| 20 | 登录策略 | 支持用户会话超时退出；支持用户密码连续鉴权失败锁定，到期自动解锁；支持用户强密码策略，密码长度8位以上，包含字母、数字、特殊字符等；支持对用户登录IP地址、MAC地址、时间的限定 |
| 21 | 运维工单 | 支持内置工单运维 |
| 22 | 访问策略 | 支持对运维时间、运维地址、运维操作指令的限定，触发策略后进行告警 |
| 23 | 单点登录 | 登录方式 | 支持访问SSH、RDP、Telnet、FTP、SFTP、VNC、数据库等资产；支持账号密码的自动代填登录，支持半自动登录和手动登录；支持进行协议/工具扩展 |
| 24 | Html5技术 | 设备访问支持最新的html5技术； |
| 25 | C/S运维 | 支持SecureCRT、XShell、WinSCP等客户端直接连接堡垒机进行代理运维目标资产 |
| 26 | 审计管理 | 操作审计 | 支持对用户和管理员的认证登录、操作和配置管理进行日志记录 |
| 27 | 图形审计 | 支持对Windows、VNC等图形界面的运维操作进行录屏审计，支持图形和字符协议的视频回放 |
| 28 | 文本审计 | #支持对图形和字符协议的操作进行文本记录（需提供截图或其他证明材料，加盖投标人公章） |
| 29 | 监控阻断 | 支持对在线会话的实时监控和即时阻断 |
| 30 | 全文检索 | #支持全文审计检索。 |
| 31 | 审计报表 | #报表针从会话、指令等多个维度进行统计； |
| 32 | 　 | #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。 |
| 33 | 自动化运维 | 运维脚本 | #支持上传脚本文件（需提供截图或其他证明材料，加盖投标人公章） |
| 34 | 定时任务 | 支持创建定时任务 |
| 35 | 系统管理 | 安全管理 | 支持HTTPS方式和Console方式进行管理 |
| 36 | #支持管理口与业务口分离（需提供截图或其他证明材料，加盖投标人公章） |
| 37 | 日志管理 | 支持将本机日志、告警日志通过SYSLOG、邮箱等进行外发和告警 |
| 38 | 数据维护 | 支持配置数据和审计数据的备份、自动清理，支持备份数据通过FTP方式远程备份 |
| 39 | 时间同步 | 支持配置时间同步服务器，进行时间自动校对，保障审计的有效性和准确性 |
| 40 | 其他要求 | 目录要求 | 设备厂商需承诺所投产品在最新一期《安可替代工程核心产品名录》、《安可替代工程适配产品清单》中，提供承诺函。 |

**3）高级威胁检测系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标** | **指标项** | **详细要求** |
| 1 | **★基本配置** | 接口配置 | 标配4个SFP插槽和4个10/100/1000BASE-T端口，其中包含2个10/100/1000BASE-T接口（作为HA口和管理口） |
| 2 | 系统存储空间 | ≥250G SSD |
| 3 | 日志存储空间 | ≥2T |
| 4 | 授权 | 不少于3年License升级许可 |
| 5 | **功能要求** | 恶意文件检测 | 支持从HTTP、FTP、POP3、SMTP、IMAP、SMB/CIFS、HTTP Proxy协议中还原出指定格式文件 |
| 6 | #文件静态检测支持检测包括邮件文件（需提供截图或其他证明材料，加盖投标人公章） |
| 7 | #支持检测文件格式自定义（需提供截图或其他证明材料，加盖投标人公章） |
| 8 | #具备独立的文件HASH库检测引擎（需提供截图或其他证明材料，加盖投标人公章） |
| 9 | #具备独立的文件内容分析特征库分析引擎（需提供截图或其他证明材料），加盖投标人公章 |
| 10 | 支持手工提交EML格式文件，自动提取附件并进行检测（需提供截图或其他证明材料，加盖投标人公章） |
| 11 | #支持从指定URL地址下载文件（需提供截图或其他证明材料，加盖投标人公章） |
| 12 | #对于系统还原出的文件，系统自动存储，支持对加文件加密下载，加密密码可以策略自定义设定。（需提供截图或其他证明材料，加盖投标人公章） |
| 13 | 支持对所有已检测过的文件HASH进行统一存储，并提供搜索、查看、重新检测功能（需提供截图或其他证明材料，加盖投标人公章） |
| 14 | 支持动态沙箱检测技术来检测文件，分析文件威胁，发现已知/未知的漏洞漏洞利用行为，识别木马、僵尸、蠕虫、病毒等恶意代码文件。 |
| 15 | #沙箱引擎的虚拟机系统支持Windows等常见操作系统模板，支持实时切换检测用的虚拟机操作系统。（需提供截图或其他证明材料，加盖投标人公章） |
| 16 | 支持沙箱逃逸技术的检测分析，能够针对特种木马等恶意代码反虚拟机检测技术进行检测和处理，避免恶意代码的绕过。支持200种以上沙箱逃逸技术检测规则（需提供截图或其他证明材料，加盖投标人公章）。 |
| 17 | #支持用户自定义沙箱虚拟机联网设置，至少支持不联网、可联网以、使用虚拟网络联网几种模式（需提供截图或其他证明材料，加盖投标人公章） |
| 18 | 沙箱支持监控恶意软件对文件系统的操作 |
| 19 | 沙箱支持监控恶意软件对系统注册表的操作 |
| 20 | 沙箱支持对进程操作进行监控 |
| 21 | 沙箱支持对模块行为的监测，分析出模块调用的进程ID以及模块名和模块路径等信息 |
| 22 | 沙箱支持对进程调用API情况的监测，并能提供调用的基本信息，如API名称、调用地址、进程名、基本参数等 |
| 23 | 沙箱支持进程对窗口的操作行为监测 |
| 24 | 对于进程的异常处理情况进行监测 |
| 25 | #沙箱支持对文件样本的网络行为检测 |
| 26 | #支持联网会话PCAP文件在线查看功能（需提供截图或其他证明材料，加盖投标人公章） |
| 27 | #沙箱支持对样本文件的PE信息、证书信息、字符串信息的检测分析功能。（需提供截图或其他证明材料，加盖投标人公章） |
| 28 | 支持对带有自运行恶意宏的样本文件产生的行为进行分析 |
| 29 | #支持对样本的数字签名状态信息进行分析（需提供截图或其他证明材料，加盖投标人公章） |
| 30 | 支持签名伪装行为分析能够识别样本过期、伪造、盗用、恶意签名等信息 |
| 31 | 支持LNK文件修改监测，支持对修改快捷方式（LNK）文件中的目标属性（LNK文件指向的文件）的操作监测 |
| 32 | 支持文件伪装识别，能够识别出伪装成图片以及其它正常文件的恶意代码文件 |
| 33 | #支持shellcode提取，能将shellcode反汇编成汇编代码（需提供截图或其他证明材料，加盖投标人公章） |
| 34 | #支持3种以上机器学习算法模型对文件进行威胁判定，输出文件样本的威胁概率。（需提供截图或其他证明材料，加盖投标人公章） |
| 35 | 支持多种机器学习算法生成的多个模型同时对文件进行威胁判定。支持机器学习模型的导入、更新、新增。  |
| 36 | #支持CVE漏洞检测，具备独立的CVE漏洞检测引擎，对已知的文档类漏洞（PDF、OFFICE）进行独立检测，识别出CVE信息（需提供截图或其他证明材料，加盖投标人公章） |
| 37 | 支持CVE漏洞编码识别，能够识别恶意代码的所对应的CVE信息，并给出CVE相关的信息 |
| 38 | #支持FLASH漏洞检测，具备独立的引擎对FLASH文件进行检测，对其中包含的ABC进行分析提取，识别恶意行为（需提供截图或其他证明材料，加盖投标人公章） |
| 39 | #沙箱检测报告具有检测信息概要功能（需提供截图或其他证明材料，加盖投标人公章） |
| 40 | #沙箱检测报告具备样本分类趋势图功能（需提供截图或其他证明材料，加盖投标人公章） |
| 41 | 沙箱引擎支持以可视化的对象实体图的方式来查看样本的威胁行为信息 |
| 42 | #沙箱引擎支持对样本主要活动行为自动截图并保存，提供查看使用。（需提供截图或其他证明材料，加盖投标人公章） |
| 43 | #文件检测支持YARA格式的自定义规则（需提供截图或其他证明材料，加盖投标人公章） |
| 44 | 支持文件样本报告批量导出功能（需提供截图或其他证明材料，加盖投标人公章） |
| 45 | 失陷主机检测 | 支持信誉检测机制 |
| 46 | #支持通信流量特征检测（需提供截图或其他证明材料，加盖投标人公章） |
| 47 | #支持基于威胁情报&流量特征的威胁事件会话PCAP文件记录、存储和PCAP文件在线查看功能（需提供截图或其他证明材料，加盖投标人公章） |
| 48 |  |
| 49 | 远程漏洞攻击检测 | 支持远程溢出漏洞检测，基于流量特征来检测远程漏洞扫描及利用的攻击行为 |
| 50 | #支持远程漏洞攻击事件会话PCAP文件记录、存储和PCAP文件在线查看功能（需提供截图或其他证明材料，加盖投标人公章） |
| 51 | 为每一条漏洞检测信息提供详细的知识库说明 |
| 52 | Web攻击检测 | 支持Web攻击检测，能够检测Web漏洞扫描及利用行为 |
| 53 | #支持Webshell控制检测，能够检测Webshell控制行为 |
| 54 | #支持Web攻击事件会话PCAP文件记录、存储和PCAP文件在线查看功能（需提供截图或其他证明材料，加盖投标人公章） |
| 55 | 为每一条攻击检测事件提供详细的知识库说明 |
| 56 | 异常行为检测 | 支持隐蔽信道检测功能。支持基于协议冗余字段和伪装通信两类隐蔽信道通信技术在看似正常的流量中识别木马的隐藏传输行为。 |
| 57 | #隐蔽信道检测功能至少支持DNS、HTTP、ICMP协议的隐蔽信道检测。（需提供截图或其他证明材料，加盖投标人公章） |
| 58 | #支持DGA检测。（需提供截图或其他证明材料，加盖投标人公章） |
| 60 | 支持协议异常检测，能够检测通信不符合相关协议规范的可疑行为，包括DNS、HTTP协议。 |
| 61 | #支持异常心跳检测，检测周期性重复数据包疑似心跳的可疑行为。（需提供截图或其他证明材料，加盖投标人公章） |
| 62 | 可视化关联分析 | 支持时间序列关联分析，以内网资产(必选)或者指定的外部IP地址作为基础，以时间、检测事件作为条件呈现当前资产或者IP的威胁态势情况。需要支持交互式操作，用户可以按照时间段、威胁类别、攻击次数、外网IP进行过滤筛选 |
| 63 | #支持KILLCHAIN关联分析（需提供截图或其他证明材料，加盖投标人公章） |
| 64 | 知识库功能 | 提供网络威胁知识库 |
| 65 | 威胁感知地图 | #支持对实时攻击态势进行动态地图展示 |
| 66 | 资产威胁统计 | #支持以资产维度，展示资产的威胁信息 |
| 67 | 告警策略 | 支持以时间轴的方式展示实时威胁告警信息 |
| 68 | 提供告警策略管理功能 |
| 69 | #支持告警信息支持以邮件形式发送到策略设定的接收人查收（需提供截图或其他证明材料，加盖投标人公章） |
| 70 | 统计报表 | 支持自定义时间和类型统计报表查询 |
| 71 | #支持自动发送导出报表） |
| 72 | 支持对定时导出报表进行管理，包括查询、删除、下载等 |
| 73 | 配置管理 | 支持动态开启/停用系统文件检测、WEB检测、流量检测功能 |
| 74 | #支持将日志发送给第三方Syslog服务器 |
| 75 | 支持组件升级功能，能够对系统组件进行在线或者离线更新 |
| 76 | **资质要求** | 检验报告 | 。 |
| 77 | 销售许可证 | #产品具有《计算机信息系统安全专用产品销售许可证》 |

**4）日志管理系统**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **指标** | **指标项** | **详细要求** |
| 1 | **基本要求** | 系统部署 | 支持单级部署；支持代理分布式部署采集日志； |
| 2 | 数据采集 | 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； |
| 3 | 数据存储 | 对所管理设备的日志原始数据完整存储，支持数据本地集中存储； |
| 4 | 数据查询 | 基于时间轴展示数据分布，能够通过时间轴进行查询分析； |
| 5 | 告警 | 内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则； |
| 6 | ★授权 | 不少于100个授权 |
| 7 | **功能要求** | 系统性能 | 日志采集峰值：35000EPS；日志采集均值：20000EPS；综合处理峰值：35000EPS；综合处理均值：20000EPS |
| 8 | 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 ； |
| 9 | 数据采集 | 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。 |
| 10 | 对于尚未支持的设备类型日志进行新增采集支持，在页面上传升级文件或增加配置文件即可； |
| 11 | 支持Syslog、SNMP Trap、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。 |
| 12 | 系统内置已支持设备种类清单，提供设备日志外发配置建议指导； |
| 13 | 支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者； |
| 14 | 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； |
| 15 | 支持首页展示日志采集总量统计，可按不同日志源种类分类显示日志总量及大小，并支持导出； |
| 16 | #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，  |
| 17 | #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；  |
| 18 | #支持对文本类型日志源进行限速采集，匀速采集日志，防止对系统资源产生突发冲击； |
| 19 | 支持对每个日志源设置过滤条件规则，自动过滤无用日志； |
| 20 | 支持日志转发给第三方系统平台，支持设置多个日志转发IP地址，支持转发格式化日志或仅转发原始日志； |
| 21 | #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； |
| 22 | 数据存储 | 支持对所管理设备的日志原始数据完整存储，支持数据本地集中存储、网络存储； |
| 23 | #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； |
| 24 | 支持自定义存储位置，支持多盘并行存储，当磁盘满后自动切换存储位置，支持磁盘阵列、SAN、DAS等外部高性能存储； |
| 25 | 支持存储空间图像化、动态监控，超过阀值进行告警。支持从存储空间、存储时间多维度进行动态监控； |
| 26 | 支持日志备份功能，支持本地备份和FTP备份方式，支持自动备份和手动备份。 |
| 27 | #支持IPv6日志的全量存储。 |
| 28 | 数据查询 | #支持首页以全国地图、全球地图展示最近24小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息； |
| 29 | 支持实时日志查询，支持历史备份文件导入查询； |
| 30 | #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； |
| 31 | #支持为不同类型日志设置不同的查询条件和显示条件； |
| 32 | 支持展示日志查询情况，包括查询条件命中数、日志总量、查询耗时等信息； |
| 33 | 查询结果支持分页显示； |
| 34 | 支持查询结果格式化日志、原始日志导出； |
| 35 | 支持查询结果快速统计，可自定义统计主题规则，支持将多个主题添加为一个统计任务，以分、时、周、月、年定时执行自动统计，将统计结果报表发送到指定邮箱； |
| 36 | #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； |
| 37 | 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。 |
| 38 | #支持IPv6日志的多条件高速查询检索及统计分析。 |
| 39 | 告警管理 | 支持首页展示当日告警情况统计；支持展示当日最新告警TOP10、TOP30和TOP50； |
| 40 | 内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则； |
| 41 | 支持安全告警概况、安全告警趋势的统一展示，实时告警可根据级别、规则类型等进行分类；  |
| 42 | 支持实时告警展示，可根据告警规则、告警级别两个维度进行实时告警监视，并可对刷新事件间隔进行设定； |
| 43 | 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； |
| 44 | #支持基于时间轴展示告警数据分布，能够通过时间轴进行查询分析； |
| 45 | 支持在告警事件查询界面直接显示触发告警的关联日志，也支持点击跳转到日志查询界面。 |
| 46 | 支持告警抑制规则设定，防止报警信息短时间内大量发送。 |
| 47 | 告警响应方式 | 支持邮件、Snmp Trap、声音、声光、短信、一信通响应、数据库响应等多种告警方式，支持报警内容引用字段变量参数。 |
| 48 | 可以针对不同类型、不同种类以及不同安全级别的安全事件制定不同的告警方式。 |
| 49 | 统计报表管理 | #系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应； |
| 50 | 报表支持基于全国地图、全球地图进行访问源、访问目的追踪。 |
| 51 | 支持自定义统计日志数据形成报表，支持统计分析报表以PDF、word、execl、html等方式导出；支持实时报表、计划报表。 |
| 52 | 日志源管理 | 支持手动添加日志源，管理员可以对日志源进行查看、批量修改、添加、编辑、删除以及启\禁用的操作； |
| 53 | #支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息； |
| 54 | 支持按照日志源名称、IP地址、日志源类型、接受时间及状态等维度对日志源列表进行排序； |
| 55 | 支持为日志源指定类型、名称、IP地址、收集节点、收集方式、以及日志源启停状态等属性信息； |
| 56 | 支持日志源在线状态监测告警，实时监测日志源的可用性，可显示每个日志源采集日志的最近时间，实时展示每个日志源最近一天日志趋势变化； |
| 57 | 支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示； |
| 58 | #支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据。 |
| 59 | 日志分析 | 系统内置常见安全事件关联分析规则； |
| 60 | 内置系统运行相关告警规则，包括检测到新日志源、节点掉线、主动日志源长期不外发日志、存储上限告警、主机认证失败等，可启用/禁用规则； |
| 61 | 支持基于策略的多日志源海量日志实时关联分析，发现安全事件实时告警。 |
| 62 | 提供可视化关联分析规则编辑视图，可根据实际业务编辑关联分析规则； |
| 63 | 系统内置安全知识库，支持自定义增加安全知识内容，可在关联分析规则中关联知识。 |
| 64 | #系统内置多种维度的数据在线分析模型，在数据查询结果界面直接对查询结果数据进行多维度在线数据分析，分析结果实时展示，分析模型包括但不限于树图、散点图、关系图、折线图、时序图、柱状图等。 |
| 65 | 知识库管理 | 知识库包含常见典型日志事件描述，支持自定义增加日志时间内容描述，支持在配置告警规则时关联知识库内规则。 |
| 66 | 系统管理 | 支持用户按角色管理，支持三权分立； |
| 67 | 支持将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日志，互不干扰； |
| 68 | #支持将常用IP地址或IP地址网段标记为自定义名称，在日志查询界面可以在IP列中对应悬浮显示自定义名称； |

**第三部分 项目其它需求**

重要性分为“★”、“#”和一般无标示指标。★代表最关键指标，不满足该指标项将导致投标被拒绝，#代表重要指标，无标识则表示一般指标项。

**(一)系统集成要求**

★本项目中，所有软硬件产品实施部署时需与目前财政网络系统兼容，确保项目实施后所有系统安全稳定的运行，若对接中所产生额外的开发费用，均由中标方自行提供，招标方不另外支付任何费用。（须提供投标人承诺函）

**(二)测试服务要求**

★本项目涉及多种安全产品，属于本系统核心安全产品，为保障网络系统安全稳定，要求投标人能够配合采购方对本项目投标产品进行功能及稳定性测试，测试内容不超过本项目技术需求。要求投标人必须提供**项目测试服务承诺函**，内容包括但不限于：在采购方提出测试要求后，投标人应在5个工作日内，按照采购方测试要求，提供测试设备。（须提供投标人承诺函）

**(三)项目实施相关要求**

1.投标人要统筹考虑、协调本项目建设内容及进度，负责提出实施方案，实施方案内容包括但不限于实施目标与任务、实施内容、工作计划、人员安排等，并根据项目总体时间以及招标人工作安排完成项目实施。

2.有完整的设备安装调试记录、测试验收文档、安装手册、用户使用手册等

3.项目实施需具备完整、有序的组织架构，项目经理负责项目的工期、质量、安全、物资等实施计划、组织、协调、控制和决策，投标人须提供项目施工组织方案。

4.明确设备安装先后次序，中标方及厂商实施人员现场工作安排计划。

**(四)项目售后服务需求**

1.原厂售后服务

要求对所有设备硬件三年质保、软件3年免费升级，电话报修后2小时内上门服务、2小时内排除故障。

2.投标人服务标准

投标人承诺所有设备硬件三年质保、软件3年免费升级，电话报修后1小时内上门服务、1小时内排除故障。（须提供投标人承诺函）

# 评标标准和方法前附表

**1、初步评审**

**资格性检查**

|  |  |  |
| --- | --- | --- |
| 资格性检查 | 评审因素 | 评审标准 |
| 营业执照 | 是否有效 |
| 财务审计报告或银行资信证明 | 符合招标文件要求 |
| 依法纳税证明 | 符合招标文件要求 |
| 依法缴纳社保证明 | 符合招标文件要求 |
| 无违法违纪行为声明 | 符合招标文件要求 |
| 信用记录 | 符合招标文件要求 |
| 结 论 | 合格/不合格 |
| 采购人代表签字：年 月 日 |

备注:有一项不合格，即为资格性检查不合格

|  |  |
| --- | --- |
| 符合性检查 | 法定代表人身份证明及授权书符合招标文件要求 |
| 投标书及投标一览表加盖投标人公章，法定代表人或其委托代理人签字或盖章 |
| 投标报价不超出招标控制价 |
| 投标人不存在提交两份或多份内容不同的投标文件，或在一份投标文件中对本招标项目报有两个或多个报价 |
| 保密承诺函符合招标文件要求 |
| 承诺函符合招标文件要求 |
| 投标保证金符合招标文件要求 |
| 投标有效期符合招标文件要求 |
| 商务偏离表中不存在负偏离条款 |
| 技术偏离表★号条款中不存在负偏离 |
| 不存在对招标文件的实质性条款不响应的情形 |
| 投标人不存在《政府采购法》等相关法律法规等规定的废标条件 |

**符合性检查**

备注:有一项不合格，即为符合性审查不合格。

**2、详细评审**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 评审项目 | 评审细则 | 评审标准 |
| 1 | 价格部分（30分） | 投标报价（30分） | 满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=(评标基准价／投标报价)×30； 对小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审，须提供小型和微型企业证明(残疾人福利性单位、监狱企业视同小型、微型企业)。 |
| 2 | 商务部分（12分） | 业绩（5分） | 投标人提供近3年（2017年10月1日至今，以合同签约日期为准）所从事类似项目业绩，每提供一个业绩得1分，最高得5分。没有不得分。须提供（以实际合同为依据，须提供合同首页、签字盖章页、合同金额页的复印件并加盖公章。） |
| 企业情况（5分） | 具有国家信息安全测评信息安全服务资质证书（安全工程类一级）证书得2分；具有信息安全管理体系认证证书27001得1分；具有环境管理体系认证证书得1分；具有职业健康安全管理体系认证证书得1分。 |
| 投标文件编制情况（2分） | 投标文件内容完整、简洁明了、字迹清晰、编排有序、页码连贯，按招标文件要求进行装订，双面打印得2分；非双面打印得1分；未按招标文件要求装订、内容缺漏、重复繁琐、文字或图片不清晰或者编排混乱的，每有一项在上述得分基础上扣0.2分，最多扣2分。 |
| 3 | 技术部分（58分） | 货物参数 （40分） | 投标人所报货物参数全部响应技术需求文件中服务要求的全部指标得40分，★代表最关键指标，不满足该指标项将导致投标被拒绝；无负偏离不扣分。#代表重要指标，每有一项不满足技术需求指标，每项扣1分；无标识则表示一般指标项，每有一项不满足技术需求指标，每扣0.5分；扣完为止。 |
| 实施方案合理性和完整性（8分） | 投标人能统筹考虑、协调本项目建设内容及进度，负责提出实施方案，实施方案内容包括但不限于实施目标与任务、实施内容、工作计划、人员安排等，并根据项目总体时间以及招标人工作安排完成项目实施。投标人有完整的设备安装调试记录、测试验收文档、安装手册、用户使用手册等，项目实施需具备完整、有序的组织架构，明确设备安装先后次序，中标方及厂商实施人员现场工作安排计划。综合考察投标人针对本项目提出的完备的项目技术实施方案并提供出科学、合理、先进、可行、适合采购人实际情况施方案，方案优秀，服务质量措施强、实施性及可操作性好得8分；针对本项目提出的项目技术实施方案较好，较科学合理，基本适合采购人实际情况，方案良好得4分；提出的技术实施方案一般，服务质量措施一般，有待完善得1分。 |
| 售后服务方案合理性和完整性（6分） | 综合考察投标人售后服务及培训服务方案，提供完善解决方案。方案内容周到、细致，科学合理的得6分；方案常规、简单，基本满足项目需要，得3分；方案略有欠缺，有待完善得1分。 |
| 原厂售后服务承诺函（4分） | 对所提投产品提供原厂售后服务承诺函，每提供一个产品原厂售后服务承诺函加1分，总分4分。 |