**公安信息通信网边界接入-电子政务外网和公安视频传输网接入通道子系统建设项目**

**一、建设目标**

本项目是按照部局公安信息通信网边界接入相关规范要求，结合上海公安实际工作需要，通过建设电子政务外网与公安信息网之间安全边界接入平台及公安视频传输网与公安信息网之间安全边界接入平台，提供高效、安全的跨网信息交换服务。

**二、建设内容**

本项目建设内容包括：

一是搭建公安信息通信网边界接入平台—上海公安信息网与电子政务外网接入通道，该通道提供双单向交换能力，并支持不少于100个业务数据，采购设备包括2台交换机、2台应用服务器、1台防火墙、1台入侵防御、1台边界安全网关、1台集控探针、2套数据安全交换系统、4台单向光闸、1套请求服务系统。

二是搭建公安信息通信网边界接入平台—上海公安信息网与上海公安视频传输网接入通道，为公安视频传输网与公安信息网提供图像数据资源单向接入及视频资源接入的合规通道，该通道提供视频流和图像数据单向导入，并支持并发3000路视频资源接入能力，采购设备包括2台交换机、2台应用服务器、2台防火墙、1台入侵防御、1台边界安全网关、2台集控探针、2套数据安全交换系统、2套视频安全交换系统、2台单向光闸、2台网闸、1台流量监测探针、1台边界安全集中管控平台。

供应商应当针对本项目需求提供专门的设计方案、选型方案、兼容对接方案等。

**三、建设需求**

本项目采购设备类型、数量及技术要求如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 单位 | 数量 | 技术要求 |
| 交换机 | 台 | 4 | 见3.1 |
| 应用服务器 | 台 | 4 | 见3.2 |
| 防火墙 | 台 | 3 | 见3.3 |
| 入侵防御 | 台 | 2 | 见3.4 |
| 边界安全网关 | 台 | 2 | 见3.5 |
| 集控探针 | 台 | 3 | 见3.6 |
| 数据安全交换系统 | 套 | 4 | 见3.7 |
| 视频安全交换系统 | 套 | 2 | 见3.8 |
| 单向光闸 | 台 | 6 | 见3.9 |
| 网闸 | 台 | 2 | 见3.10 |
| 请求服务系统 | 套 | 1 | 见3.11 |
| 流量监测探针 | 台 | 1 | 见3.12 |
| 边界安全集中管控平台 | 台 | 1 | 见3.13 |

**以下参数要求中标注▲指标的为关键指标，供应商需提供专门的▲技术参数偏离表，标明偏离情况，并且提供满足该指标的相关证明材料（如需提供相应的第三方测试报告、适配证明、加盖原厂公章的产品官方技术资料白皮书或网页截图、专门承诺函等相关证明文件），需标明证明材料在响应文件中的位置，并明确标示出满足▲的内容，未提供证明材料或者证明材料不符合指标要求的视为该项负偏离**

3.1 交换机

|  |  |
| --- | --- |
| 指标项 | 技术要求 |
| 交换容量 | 交换容量≥700Gbps |
| 包转发率 | 包转发率≥200Mpps |
| 电源 | 为了提高设备可靠性，支持并配置模块化可插拔双电源 |
| 端口 | 固定端口不少于48个10/100/1000Base-T以太网端口、4个万兆SFP+（满配万兆多模光模块） |
| 支持业务扩展插槽数≥1，配置1块不少于8端口万兆光口接口板（满配万兆多模光模块） |
| 二层功能 | 支持4K VLAN，支持QinQ，灵活QinQ、支持端口VLAN、协议VLAN、IP子网VLAN，支持Super VLAN、支持Voice VLAN、支持组播VLAN，支持IEEE 802.1d(STP), 802.w(RSTP), 802.1s(MSTP) |
| 支持策略VLAN，支持PVLAN/MUX VLAN |
| 支持IGMP v1/v2/v3、PIM-SM、PIM-DM、PIM-SSM |
| 支持MAC地址≥220K |
| 三层功能 | 支持静态路由、RIP v1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+ |
| 支持策略路由、路由策略、VRRP、BFD for OSPF、BGP、IS-IS、Static Route，支持IPv6、支持IPv4/IPv6双栈、IPv6 over IPv4隧道、IPv4 over IPv6隧道 |
| 支持IPv4 路由表≥512K，支持IPv6 路由表≥64K |
| 镜像功能 | 支持多个物理端口的流量镜像到一个端口，支持流镜像、远程端口镜像 |
| 访问控制 | 支持基于第二层、第三层和第四层的ACL |
| 支持双向ACL |
| 支持VLAN ACL和IPv6 ACL |
| 支持IP/Port/MAC的绑定功能 |
| VxLAN | 支持VxLAN二层网关、三层网关，支持BGP EVPN，支持通过Netconf进行配置 |
| QoS | 支持对端口接收报文速率和发送报文速率进行限制，支持SP、WRR、SP+WRR等队列调度算法 |
| 安全 | 支持DHCP Snooping，IP Source Guard，SAVI等安全特性 |
| 支持防ARP攻击、DOS攻击、ICMP防攻击、CPU防攻击 |
| 支持dot1X、MAC认证和Portal认证 |
| 可靠性 | 支持G.8032标准以太环网协议，倒换时间≤50ms |
| 支持真实业务流实时检测技术，实时检测网络故障 |
| 堆叠 | 支持堆叠，主机堆叠数不小于9台 |
| 管理维护 | 支持SNMP v1/v2/v3、Telnet、RMON、SSH |
| 支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理 |

3.2 应用服务器

|  |  |
| --- | --- |
| 指标项 | 技术要求 |
| 硬件要求 | 1、服务器CPU 和操作系统等关键部件应当符合安全可靠测评要求，并提供中国信息安全测评中心官网截图证明2、国产化ARM处理器CPU≥2，单CPU主频≥2.6GHz、核数≥323、内存≥DDR4 8\*32GB4、硬盘≥8\*480GB SATA SSD5、网络接口：千兆电口≥2个， 2\*双端口10GE光口网卡（满配10GE多模光模块）6、配置独立RAID卡,4GB缓存，支持RAID 0,1,5,6,10,50,607、电源：配置冗余电源8、操作系统：配置统信服务器操作系统V209、服务器BMC系统软件为国产自主开发，硬件为国产自研管理芯片，且软硬件为同一品牌10、集成系统管理支持：电源启动和关闭、风扇监视和控制、电源监控、温度监控、本地固件更新、错误日志11、配置独立的远程管理控制端口，支持远程监控图形界面, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作 |

3.3 防火墙

|  |  |
| --- | --- |
| 指标项 | 技术要求 |
| 架构 | 软硬一体化设备，符合信创要求，冗余电源 |
| 端口 | 千兆光口≥8个，千兆电口≥8个，万兆光口≥10个，端口可扩展，提供管理口和双机心跳口，配备至少4个千兆多模光模块、4个千兆单模10km光模块、6个万兆多模光模块、4个万兆单模10km光模块 |
| 性能 | 网络层吞吐量（双向，IPv4）≥80Gbps，应用层吞吐量（单向，IPv4）≥50Gbps |
| TCP新建连接速率（IPv4）≥126万/秒 |
| TCP并发连接数（IPv4）≥3000万  |
| 硬盘 | 硬盘≥1TB |
| 访问控制 | 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，并重复策略的检查 |
| 支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向 |
| 基于状态检测技术的访问控制 |
| 深度包检测 |
| 网络攻击防御 | 抵御地址欺骗、拒绝服务、网络扫描等网络攻击行为 |
| 支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 |
| 应用攻击防御 | 提供应用攻击防御能力 |
| 防病毒 | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万 |
| 支持对最多6级的压缩文件进行解压查杀 |
| ▲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 | 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 |
| 支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围 |
| NAT | 一对一、地址池等NAT方式；支持多种应用协议，如SIP、H.232、FTP、RAS、NBT的NAT ALG功能 |
| 支持在源地址转换过程中，对SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过SNMP Trap、邮件等方式告警。 |
| 带宽管理 | 提供带宽管理功能 |
| IP/MAC绑定 | 手工或自动IP/MAC地址绑定 |
| 应用层控制 | 提供应用类型控制、应用关键内容控制 |
| 网络 | 透明、路由、混合模式 |
| 支持802.1q、RIP、OSPF、BGP、SNMP等协议 |
| 提供对IPv4和IPv6的支持 |
| 提供策略路由 |
| IPv6支持 | 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 |
| 支持IPv6下静态路由及策略路由、动态路由，动态路由应包括RIPng、OSPFv3、BGP4+ |
| 支持NAT64，NAT66、NAT-PT等种IPv4/v6过渡技术，支持针对ICMPv6以及IPv6扩展头防护功能 |
| 高可用性 | 提供双机热备，包括主-主模式和主-备模式 |
| 安全审计 | 提供对日志事件的记录、存储和管理功能，提供以syslog等标准方式输出日志信息 |
| 对日志的统计分析和报表功能 |
| 日志存储至少6个月 |
| 流量异常检测功能 |
| 升级 | 在线、离线等升级方式 |
| 管理 | 远程和本地管理，保障远程管理安全 |
| NTP时间同步，准确记录日志时间 |
| 提供用户身份鉴别等功能 |
| 提供对安全策略等配置的管理，界面友好 |
| 病毒库、应用特征库至少5年免费升级服务 |
| 资质要求 | ▲所投防火墙产品平均无故障时间MTBF≥5000H，满足 GB/T 5080.7-1986《设备可靠性试验 恒定失效率假设下的失效率与平均无故障时间的验证试验方案》要求。 |
| ▲所投防火墙产品环境适应性良好，能够在-40°至70°环境中稳定运行，能够在环境湿度25%至95%环境中稳定运行，满足GB/T2423.1-2008要求。 |
| 具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（达到EAL4或以上级别），投标文件需提供证书复印件 |
| 其他要求 | 提供产品原厂商的授权书和质保服务承诺函 |

3.4 入侵防御

|  |  |
| --- | --- |
| 指标项 | 技术要求 |
| 架构 | 软硬一体化设备，符合信创要求，冗余电源 |
| 端口 | 万兆光口≥8，千兆光口≥8，千兆电口≥8，配备至少4个千兆多模光模块、4个千兆单模10km光模块、4个万兆多模光模块、4个万兆单模10km光模块 |
| 性能 | 满检速率≥59000Mbps  |
| TCP并发连接数≥2000万 |
| 硬盘 | ≥1TB |
| 路由支持 | 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 OSPFv2/v3 |
| 提供对IPv4和IPv6的支持 |
| 支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别、反间谍软件等安全功能； |
| 访问控制 | 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、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 |
| 支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向 |
| 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 |
| 网络攻击防护 | ▲支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。 |
| 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 |
| 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 | 能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀 |
| 支持对最多6级的压缩文件进行解压查杀 |
| 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 | 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；支持针对应用协议的漏洞防护 |
| 支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号 |
| 支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围 |
| 事件处置 | 提供统计分析面板，可将展示，威胁统计、恶意URL、恶意域名、恶意地址的TOP5、TOP10、TOP15内容展示；并支持15分钟、1小时、6小时、12小时、1天、7天等多时间维度筛选 |
| 可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项 |
| 运维管理 | 支持双系统备份，且在系统切换中可实现配置的自动迁移；可记录不同时间点的历史配置文件。 |
| 支持三权分立管理 ，权限设置至少包括全部权限，仅具有策略变更权限和仅具有日志审计权限、仅具有账户配置权限、虚系统配置管理权限以及虚系统审计权限；并支持以读写、只读、无权限的方式自定义权限管理，权限管理的范围至少包括策略配置、对象配置、网络配置、系统配置、统计分析、威胁处置等 |
| 支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括配置、时间、流量、URL过滤、内容过滤、邮件过滤、行为、威胁等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试八种 |
| 资质要求 | ▲所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》（万兆EAL4+），投标文件需提供证书复印件； |
| ▲具备中国信息安全测评中心颁发的“CNNVD兼容性认证”，投标文件提需供证书复印件 |
| 其他要求 | 5年全量特征库免费升级服务 |
| 提供产品原厂商的授权书和质保服务承诺函 |

3.5 边界安全网关

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 内存≥64GB，硬盘≥1TB，千兆电口≥4，万兆光口≥2个（满配万兆多模光模块），支持扩展。 |
| 性能要求 | 吞吐量≥30Gbps；加密带宽吞吐量≥6Gbps。 |
| 功能要求 | 支持串联部署、旁路部署、策略路由部署。 |
| 具备对接第三方PKI/CA系统，支持跨CA证书认证，支持导入根证书，支持CRL同步。支持数字证书的身份认证。 |
| 具备802.1X认证，支持portal认证。 |
| 具备对接入的终端设备进行认证的能力，能够基于终端数字证书、终端令牌、口令密码、硬件指纹等标识进行终端身份认证和准入控制。 |
| 具备多维度访问控制能力，包括基于访问时间、访问IP、访问动作、URL、访问内容、访问次数、访问频次的限制能力。 |
| 能够通过无客户端方式（响应嵌入方式）实现终端非法外联探测；能够通过客户端检测方式，实现终端非法外联探测告警。 |
| 具备用户管理、角色管理和权限分配功能。 |
| 具备加密隧道功能，支持与客户端之间使用IPSec、SSL协议对通信过程进行加密和完整性保护，保证数据传输的安全性。 |
| 具备对接入设备、用户的认证、访问控制过程进行详细的记录，并实时报送给边界安全集中管控平台进行审计和行为分析。 |
| 具有应用安全代理、服务隐藏、服务路由、单点登录功能。 |
| 具备高可用功能，双机部署时，能够双机热备、双主负载均衡部署。 |
| 具备接收边界安全集中管控平台统一监控管理、策略管理、策略下发。 |
| 具备向集中监控管理系统上报信息，包括但不限于业务访问日志、运营状态等信息。 |
| 客户端 | 提供设备客户端数量≥150个，客户端支持适配信创软硬件环境适配，支持安装在统信UOS、麒麟操作系统终端上 |

3.6 集控探针

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | 内存≥16GB，硬盘≥128GB，千兆电口≥4个，数据存储空间≥1TB。 |
| 性能要求 | 吞吐量≥8000Mbps，日志采集速率≥1200EPS，镜像流量处理性能≥1Gbps。 |
| 功能要求 | 支持通过Syslog，SNMP，ICMP采集安全设备、应用系统、网络设备的安全事件日志，配置操作日志，运行状态信息等数据。 |
| 支持将日志统一报送边界安全集中管控平台。 |

3.7 数据安全交换系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件配置 | 包括数据交换前置设备和数据交换后置设备各1台，含配套数据交换系统软件。 |
| 每台数据交换前置设备和数据交换后置设备分别配置端口：千兆电口≥4个、万兆光口≥4个（满配万兆多模光模块），支持扩展。 |
| 每台数据交换前置设备和数据交换后置设备分别配置:CPU≥2路8核，≥2.2GHz，内存≥768GB，硬盘≥6TB。 |
| 每台数据交换前置设备和数据交换后置设备均配置冗余电源。 |
| 性能要求 | ▲吞吐量≥8Gbps。数据库同步速率（1KB）≥45000条/秒。FTP文件同步速率（40KB）≥6000个/秒。消息同步速率（1KB）≥15万个/秒。API请求服务交换速度（40KB数据大小，1000并发）≥19000个/秒，传输时延≤1ms。。 |
| 无任务数限制。 |
| 功能要求 | 支持集群扩展，无需独立集群管理节点，具备集群高可用和负载均衡能力。具备集群节点并行交换、负载均衡和容灾切换功能。 |
| 具备文件交换功能，兼容FTP、SFTP、SMB、NFS协议，支持文件断点续传，支持大文件（GB级）同步。 |
| 具备数据库同步功能，兼容常用关系数据库、非关系型数据库、MPP数据库、国产数据库等。能够将数据库数据转格式化文件落地交换。支持异构数据库同步，提供新增数据库适配能力。 |
| 内置请求服务功能，能够将请求和响应转文件落地交换。 |
| ▲具备分布式多通道高速数据总线引擎，能够对格式化消息进行交换。具备对消息数据进行格式检查、敏感信息过滤、内容替换、加插数据水印、水印内容加密，水印溯源功能。 |
| ▲能够设置消息同步的起始位置和起始时间，指定消费位置进行分区分配，读写消息总线进行消息同步。 |
| 支持对文本文件、数据库格式化数据、API 请求/响应报文基于安全策略进行内容过滤。 |
| ▲具备应用认证能力，包括 Basic认证、Soap头认证、JWT认证、HMAC 签名认证、数字证书、口令密码、动态令牌、Token等认证方式。 |
| 具备数据签名验证能力，确保交换数据的真实性、完整性和不可抵赖性。 |
| 具备敏感信息过滤功能，通过关键字字典（如数据库字段名、手机号、车牌号等）和正则表达式方式，实现对交换的文本数据进行内容过滤、报警和阻断。 |
| 具备多种访问控制能力，支持基于 IP、端口、协议、时间、流量、频次的访问控制。 |
| 支持前端API用户对后端Web资源访问、API反向代理；支持API调用方Token身份认证、数据格式检查、关键字过滤、请求报文完整性验证功能 |
| ▲具备文件水印功能，包括添加显性和隐性水印，能够设置水印大小、水印颜色、水印位置等，能够基于水印标签进行泄漏溯源。 |
| 具备数据库数据单列、多列、单列多行、列顺序等方式添加水印。具备插入文字、空格、变更全角等方式插入水印。具备添加水印时指定水印位置、水印长度、水印前缀分隔符等功能。 |
| 具有任务优先级设置和控制功能，在网络带宽或设备高负荷时保障高优先级业务交换。 |
| 具备集群式交换能力，可获取隔离设备的通道配置并根据通道配置选择最优可用通道。 |
| 支持交叉热备功能，能在双机热备功能下提供一端的故障切换（如主设备发送端故障，切换至备用设备发送端，主设备接收端正常工作）。 |
| 兼容IPv4和IPv6网络环境。 |

3.8 视频安全交换系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件配置 | 包括视频交换前置设备和视频交换后置设备各1台，含配套视频交换系统软件。 |
| 视频交换前置设备和视频交换后置设备分别配置端口：千兆电口≥4个、万兆光口≥4个（满配万兆多模光模块），支持扩展。 |
| 视频交换前置设备和视频交换后置设备分别配置：CPU≥2路8核，≥2.2GHz，内存≥64GB。 |
| 视频交换前置设备和视频交换后置设备均配置冗余电源。 |
| 性能要求 | 吞吐量≥8Gbps。并发路数D1标清≥3000路或D4高清≥1500路。 |
| 功能要求 | ▲视频交换前置设备和视频交换后置设备支持集群部署和横向扩展，集群对外提供统一虚拟 IP 地址入口。具备SIP协议的七层集群负载功能。 |
| ▲支持对集群媒体流提供负载均衡和动态容灾功能。 |
| 支持对 RTSP、SIP、GB/T28181、GB35114、RTP 等指定协议的信令和数据流数据基于安全策略进行格式检查，对不符合格式的信令和数据流数据进行拦截丢弃，并进行日志报警。 |
| 支持对指定协议的信令和数据流数据基于安全策略进行内容过滤，对含有敏感信息的信令和数据流数据进行拦截丢弃，并进行日志报警。 |
| 支持基于GB35114的设备认证准入控制、信令签名验证、加密视频流传输。 |
| 支持动态端口控制，在不存在视频媒体流时可关闭端口，减小攻击暴露面。 |
| 支持对接入的视频摄像头、视频平台、信令网关等设备进行认证，支持 IP/MAC 认证、口令密码认证、GB/T28181 设备 ID 认证准入。 |
| 支持访问用户限制、访问内容限制、访问动作限制、访问时间限制、访问地址限制、访问次数限制等访问控制能力。 |
| 支持视频访问日志审计，审计内容包括时间、源 IP、源端口、目标 IP、 目标端口、设备编码、操作动作等信息，支持日志数据存储空间报警和转发报送。 |
| ▲具备对H.264、H.265视频流添加水印,可以配置水印文字内容、水印大小、水印颜色、水印透明度等。 |
| 兼容IPv4和IPv6网络环境。 |

3.9 单向光闸

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件配置 | 采用“2+1”硬件系统架构，单台设备由内、外网两个独立主机模块和一个单向传输专用硬件模块三部分组成。配置冗余电源。 |
| 内外主机分别配置接口：千兆电口≥4个，万兆光口≥4个（满配万兆多模光模块）。 |
| 内外主机分别配置： CPU≥8核，内存≥64GB,硬盘≥512GB；内置国产CPU和国产操作系统。 |
| 性能要求 | 吞吐量≥6Gbps。 |
| 功能要求 | 具备交叉热备功能，能在双机热备功能下提供一端的故障切换（如主设备发送端故障，切换至备用设备发送端，主设备接收端正常工作） |
| 具备数据库同步，兼容适配Oracle、MySQL、MariaDB、PostgreSQL、SQL Server等多种主流数据库。 |
| 具备FTP、SFTP文件同步功能。 |
| 具备对数据文件完整性进行校验和病毒查杀功能，可针对文件后缀名、内容格式、关键字等过滤配置，支持任务调度策略配置 |
| 文件交换模块支持病毒检测功能，支持通过文件大小控制病毒查杀 |
| 具备UDP通道功能，包括通道管理、查看通道的基本信息，通道名称、通道类型、数据发送间隔等，访问策略配置等 |
| 兼容IPv4协议和IPv6网络环境。 |

3.10 网闸

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件配置 | 采用“2+1”硬件系统架构，单台设备由内、外网两个独立主机模块和一个隔离交换硬件模块三部分组成。配置冗余电源。 |
| 内外主机分别配置接口：千兆电口≥4个，万兆光口≥4个（满配万兆多模光模块）。 |
| 内外主机分别配置：CPU≥8核，内存≥64GB，硬盘≥512GB；内置国产CPU和国产操作系统。 |
| 性能要求 | 吞吐量≥6Gbps。 |
| 功能要求 | 具备交叉热备功能，能在双机热备功能下提供一端的故障切换（如主设备发送端故障，切换至备用设备发送端，主设备接收端正常工作） |
| 提供实时监控功能，可针对设备资源情况、任务运行情况、设备流量情况、异常时间情况进行实时统计监控；  |
| 具备数据库同步功能，兼容适配Oracle、MySQL、MariaDB、PostgreSQL、SQL Server等多种主流数据库。 |
| 具备FTP、SFTP文件同步功能。 |
| 具备对数据文件完整性进行校验和病毒查杀功能，可针对文件后缀名、内容格式、关键字等过滤配置，支持任务调度策略配置 |
| 支持文件源端删除同步、全量同步、增量同步、文件同步重名等同步策略。 |
| 兼容IPV4协议和IPV6网络环境。 |

3.11 请求服务系统

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件配置 | 包括请求服务前置设备和请求服务后置设备，含配套请求服务系统软件。 |
| 请求服务前置设备和请求服务后置设备分别配置端口：千兆电口≥4个，万兆光口≥4个（满配万兆多模光模块），支持扩展。 |
| 请求服务前置设备和请求服务后置设备分别配置：CPU≥8核，≥2.2GHz，内存≥256GB，硬盘≥6TB。 |
| 请求服务前置设备和请求服务后置设备均配置冗余电源。 |
| 性能要求 | 吞吐量≥6Gbps。 |
| 功能要求 | 具备对请求报文、响应报文转文件，对接边界数据交换系统进行隔离交换。 |
| 具备webservice、REST API接口类型，支持XML、JSON数据格式。 |
| 具备对后端真实服务的URL进行隐藏，通过系统以新的URL对外提供访问入口。 |
| 具备对应用方进行身份认证，支持HTTP Basic基本认证、AK/SK认证、Token认证、数字证书认证、签名认证、SOAP头认证、动态令牌认证等方式，并支持多因子认证。 |
| 具备静态服务路由方式，通过配置path和具体URL的映射关系，把对URL的请求固定转发给服务提供方的path。 |
| 具备接口复用，实现统一接口服务。统一接口服务根据操作方法、作用用途等进行归类，为所有应用服务请求方提供统一的调用接口URL，用于数据上传、数据删除、数据更新、数据查询等操作，以达到减少暴露面的目的。统一接口服务应支持同步调用、异步调用。 |
| 具备请求限额控制，包括频次限制、次数限制、流量大小限制、时间范围限制、IP限制等，可以防护爬虫程序攻击、拒绝服务攻击等行为。 |
| 协议清洗，支持对请求报文、响应报文进行URL编码、header字段、MIME类型、长度大小的校验，只允许符合白名单策略的数据通过。 |
| 支持负载均衡集群，支持虚拟VIP服务和会话持续。 |
| 兼容IPv4和IPv6网络环境 |

3.12 流量监测探针

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | CPU≥4核，内存≥32GB，硬盘≥128GB。千兆电口≥2个，万兆光口≥4个（满配万兆多模光模块），支持扩展。 |
| 性能要求 | 同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流吞吐量10Gbps，HTTP并发连接数800万，HTTP新建连接速率30万/秒 |
| 旁路部署 | 支持通过流量镜像的方式旁路部署在网络中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断TCP威胁会话连接，支持通过流量被动识别资产 |
| 流量采集 | 采集过滤条件支持但不限于源地址、目的地址、服务、流量采样比、时间等 |
| ▲支持空载荷过滤，支持对采集的流量的上下行载荷长度设置。 |
| 支持离线采集，可通过手动PCAP导入或FTP等协议批量上传导入等方式对离线流量进行采集 |
| 流量识别与解析 | 支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类等多类别的应用识别，应用识别库3000+ |
| 支持VXLAN、GRE 、VLAN 、MPLS的流量接入与解析，日志中可提现响应标识信息 |
| 支持Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2等数据库行为的解析 |
| 支持WebMail、SMTP、POP3、IMAP邮件行为解析 |
| 支持ICMP、DHCP、HTTP、TELNET、DNS、SSL等基础协议的解析 |
| 支持如ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp的登录动作解析 |
| 具有自定义解析流量能力，支持基于正则表达式、TLV格式、固定长度等提取模式对应用流量解析 |
| 文件还原 | 支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP |
| 支持多种文件类型的筛选，可执行文件还原格式包含：bin、exe、bat、dll、sys、com、ax、acm、drv等；压缩文件还原格式包含：rar、zip、gz、7z、tar等；文档类型的还原格式包含：doc、docx、xls、txt、pptx、pdf、rtf、ppt等 |
| 威胁检测 | 系统具备全面的间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等 |
| 系统具备全面的漏洞检测能力，可检测常见的溢出攻击、跨站脚本、SQL注入、拒绝服务、跨站请求伪造、目录遍历、webshell上传等 |
| 系统支持Flood攻击检测，包括SYN Flood、ICMP Flood、UDP Flood和IP Flood；支持应用层Flood攻击检测，包括DNS Flood和HTTP Flood |
| 支持按照协议类型对攻击事件规则的设置检测有效性，协议类型包括HTTP、DNS、FTP、ICMP、IMAP、IRC、Mongodb、NNTP、POP3、RIP、RLOGIN、SMTP、SNMP、TDS、TELNET、TFTP、TNS等  |
| 提供的攻击特征不应少于10000条有效最新攻击规则，特征库需支持自动及手动升级 |
| 本地集成威胁情报库，支持实现基于威胁情报的失陷主机检测，情报不少于200万 |
| 需具备专业的查毒引擎，独立的病毒库，支持通过对HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS协议进行恶意文件检测 |
| 支持恶意文件例外，对指定特征的恶意文件及文件类型不进行查杀 |
| 数据外发 | ▲通信模式支持但不限于KAFKA、ZMQ、SYSLOG等协议，需支持多路外发，并支持外发多地址的负载均衡处理。 |
| 支持灵活配置外发策略，日志类别可配置 |
| 外发类别支持但不限于流量日志、威胁日志、资产日志、样本文件、威胁相关pcap等 |
| 旁路阻断 | 支持旁路IPv4和IPv6的IP阻断、URL重定向、DNS重定向 |
| 资产识别 | 系统具有资产识别能力，能够根据流量识别资产的操作系统、服务、开放端口、banner信息等 |
| 支持 资产识别范围配置、支持资产识别展示及导出 |
| 流量及样本取证 | 支持威胁告警的相关pcap数据留存，支持本地下载及外发，外发通信协议包括但不限于KAFKA、FTP、SFTP等 |
| 支持威胁告警的相关文件留存，支持本地下载及外发，外发通信协议包括但不限于FTP、SFTP等 |
| 支持可疑流量的留存，留存条件支持但不限于数据方向、地址、端口、应用、URL、时间等；抓取的流量支持本地留存、定时或实时上传 |
| 业务统计和状态监控 | 支持失陷主机、恶意文件检测、漏洞攻击检测的数量统计 |
| 基于应用维度的TOP5、TOP10的24小时/7天的实时流量统计和可视化展示 |
| 基于接口维度的发送、接收和总数的实时流量统计和可视化展示 |
| 基于会话维度并发、新建的24小时/7天的统计和可视化 |
| 网络流量日志数和威胁检测日志数的实时统计及可视化展示 |
| 其他要求 | 5年全量特征库免费升级服务 |
| 系统免费提供二次开发，将解析后的数据输出给边界安全集中管控平台 |

3.13 边界安全集中管控平台

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 硬件要求 | CPU≥2路8核，内存≥128GB，硬盘≥4TB\*2，千兆电口≥6个，支持扩展。 |
| 性能要求 | 支持多台服务器实现多节点集群管控。监管链路数支持扩展。 |
| 功能要求 | 通过 Syslog、SNMP 获取边界安全设备、网络设备、应用的状态信息、告警信息，包括防火墙、入侵防御、边界安全网关、网闸、单向光闸、数据交换系统、视频交换系统等。  |
| 具备边界安全设备资产管理能力，实现信息注册、资产维护、知识管理、漏洞管理等功能，支持页面表单注册、模版上传注册两种方式。 |
| 具备对边界安全交互系统内设备运行状态进行检测和展现能力。能够对业务运行状态进行统计。实现依据业务审批信息设置业务监控报警阈值。具有违规业务告警和应用访问异常告警等业务监控报警功能。 |
| 具备对数据交换系统、视频交换系统的策略管理能力，实现安全策略配置下发、策略变更、策略删除、策略查询等功能。 |
| 具备边界安全设备级联管理，实现数据报送、审批、通报等能力。 |
| 具备边界资产的查询搜索、信息编辑、修改、删除等管理功能。 |
| ▲具备各种边界设备发现能力，支持通过发包探测、端口扫描、WEB扫描和镜像流量方式，获取边界设备的品牌型号、在线状态、端口和服务列表、设备类型（包括网闸、单向光闸、数据交换系统、代理服务器、NAT网关、可信认证接入网关、视频交换系统等资产类型）。。 |
| ▲具备边界僵尸设备、僵尸业务、隐蔽通道、未注册协议、未注册资产、未注册应用服务的监控功能。 |
| ▲具备边界中断、业务中断、设备超负荷、数据拥塞、应用服务器故障指标监控功能。 |
| 具备资产变更替换设备的自动检测和手动稽核，可展示相同 IP 的变更前后设备列表。 |
| 具有安全事件管理能力，具有安全事件分类分级、安全事件分布、安全事件趋势、安全事件关联、时间序列关系等态势展现功能。 |
| 异常流量分析：根据流量监测数据，支持发现边界非注册业务、与注册信息不符的业务、僵尸业务，支持发现边界违规协议，支持发现违规外联行为。 |
| 具备采集边界设备日志、格式化处理能力，并可提供安全事件分类分级、安全事件分布、安全事件趋势、安全事件关联、安全事件时间序列关系展现，提供对于安全事件的入侵分析报告。 |
| 支持集中审计，可对设备的配置操作、视频交换行为、数据交换行为进行审计，审计内容至少包括：日期、时间、IP、端口、协议、用户 (应用) 、字节数、URL、操作动作、操作结果等。 |
| 提供在线绘制边界拓扑图的功能，支持在编辑器中进行各种安全设备网元图标拖拉、连线、信息标注等操作。 |
| 事件处置功能模块中可以对告警事件进行处置动作，并支持填报告警事件处理意见。 |
| ▲兼容IPV4和IPV6网络环境。 |

**四、进度要求**

本项目自合同签订之日起12个月内完成项目建设、试运行并通过验收。

（一）交货

合同签订后，45个自然日内全部设备到货，要求：

1、设备到货后将提供的货物全部运抵用户指定地点，由招标方进行货物查验。如果发现数量不足或有质量、技术等问题，中标方应负责按照用户的要求采取补足、更换或退货等处理措施，并承担由此发生的一切损失和费用。

2、设备到货清点时，中标方必须提供设备制造商对该项目采购的所有设备（含配件）出具的订货证明（即须有设备制造商对订购设备提供的产品序列号）。如果未提供，用户有权终止合同，并且中标方将承担合同金额20%的违约金。

3、中标方在交货的同时提供关于项目的详细设计方案、设备安装调试方案、回退方案和运行维护等方面齐全有效的技术资料。

 （二）安装和调试

全部设备到货后，按照用户要求完成所有设备的部署、配置、调试，保证系统满足用户需求和部局规范。

（三）试运行

在完成软硬件系统安装、调试后进入试运行，试运行期为1个月。试运行无重大缺陷、无重大故障且解决所有发现的缺陷后进行正式验收。

（四）验收

1、验收形式由用户指定，中标方必须配合验收相关工作，验收所需费用由中标方承担。

2、中标方需提供整个系统包括设备的测试与验收的方案和详细的验收计划。中标方应提供验收相关资料：所有验收文件、测试报告、配置文档、设备技术资料及使用说明书等，资料要提交完整的四套，以作设备留档备案。

3、根据部局边界规范要求，本项目建设边界应经公安部授权的测评单位进行边界测评。边界测评合格后予以验收，相关测评费由中标方承担。

4、中标方应当配合第三方测评单位开展安全测评（测评费用由采购人承担），若安全测评不通过，中标方应根据要求整改（整改所需费用由中标方自行承担），直至安全测评通过。

**五、工程技术服务要求**

（一）中标方须提供成功实施其技术方案所必须的技术支持和工程服务，包括系统设计、工程设计、项目管理、工程实施、验收、培训等，并须提交详细的工程服务方案。

（二）中标方不得将工程分包、转包。

（三）中标方应接受招标方的统一管理。招标方根据实际情况委托监理单位、咨询机构或行业专家参与本项目相关工作，中标人应积极配合并遵循相应指令。

（四）本项目系统集成质量控制和文档需满足国家标准要求。

（五）中标方需组建素质高、专业性强、经验丰富、稳定的团队负责项目建设。需建设严格的、有组织有纪律的管理流程，并指定项目经理负责本项目的实施活动，需要及时响应建设需求，并负责接收、处理、跟踪、结果汇报等工作。

（六）中标方建设期间需提交项目人员参与清单。项目建设期间，项目参与人员不得参与其他项目建设工作。中标方应保持项目团队稳定，未经招标方同意，项目参与人员在项目整体验收前一般不得更换。确因特殊原因更换的，应当经招标方同意。同时，项目参与人员需签订保密承诺书，明确其应当承担的保密责任和义务。

（七）中标方负责项目性能的优化指导、故障诊断等工作；根据实际运行情况，定期调整软件硬件配置策略；定期对软硬件的运行情况进行专业巡检，向招标方提出相关建议。

（八）中标方应协助招标方制定运行相关规范，并提供相关咨询、建议服务。

（九）设备安装和调试

中标方负责所有设备的安装调试，具体要求如下：

1、要求中标方负责设备安装机房的环境检测和电路测试，对于不满足设备安装要求的机房环境和电源、电路等，中标方负责提出符合设备安装条件的解决方案。

2、设备安装和联网调试由中标方负责，提交用户一个可使用、稳定可靠的系统。

3、设备安装过程中所需的网线、光纤、电缆、接头、工具及仪器仪表均由中标方提供，所需费用由中标方自行承担。

（十）培训

针对项目中建设的系统和软硬件设备，中标方应对用户进行免费培训，提供相应的操作手册，使用户能够独立进行日常管理和维护。

**六、投标要求**

（一）该项目为“交钥匙”工程，项目中涉及的各个环节需在方案中一并考虑。

（二）投标方应针对用户需求书逐条应对，需提供详细的响应方案，包括设备配置、设备部署、业务流程、运行维护、人员培训、售后服务等内容。方案内容需符合用户实际需求，其中技术方案需满足公安部边界相关规范要求。

（三）投标方在标书中需制作详细的设备规格、技术参数偏离表。

（四）投标方需提供投标产品中下述设备的原厂授权和质保服务承诺（均需加盖原厂公章）。

|  |  |
| --- | --- |
| 1 | 防火墙 |
| 2 | 入侵防御 |
| 3 | 边界安全网关 |
| 4 | 数据安全交换系统 |
| 5 | 视频安全交换系统 |
| 6 | 单向光闸 |
| 7 | 网闸 |
| 8 | 请求服务系统 |
| 9 | 流量监测探针 |
| 10 | 边界安全集中管控平台 |

（五）投标方对任何陈述的条款答复都需符合实际指标与客观事实，任何隐瞒或不尊重事实的阐述均有可能承担被拒绝接受或废除投标资格或合同的风险。在采购过程中，招标方将在认为必要时，对投标方所响应满足的某项功能或指标要求投标方配合进行测试、检查并核实（所需相关费用由投标方承担）。本需求书将作为合同主体的重要依据，严格体现投标方对本项目的技术与服务承诺。

（六）投标方应提供详细的报价，包括设备费用及系统集成费用。报价应提供详细的报价清单，包括：产品名称、型号、单价、数量、总价。报价按单项开列，最终费用以人民币报价、结算。

（七）投标方如具有类似项目的成功实施经验，需提供相应的合同复印件等相关证明材料；投标方组建的项目组负责人及项目组主要成员参与类似项目建设，需提供相关证明材料。

（八）投标方应该保证所提供的所有产品皆不侵犯任何第三方的版权、知识产权和其他合法权利。

**七、运维及售后服务要求**

（一）系统及设备的保修、维护期从本项目验收通过之日起计算。

（二）要求投标方须免费提供本项目采购的所有设备4年或以上原厂保修以及7×24×4的备件先行服务（即每周7天每天24小时响应用户硬件故障申请，并保证在接到用户申请4小时内备件到达用户现场）。同时提供设备制造商出具的本项目采购的所有设备4年或以上原厂保修以及7×24×4的备件先行保修服务承诺，内容包括但不限于保修期限、保修条件、保修范围和备件先行服务等方面。

（三）要求投标方提供4年或以上免费的维护服务，免费维护期内，投标方需提供5人以上固定的维护队伍（附名单简介及社保缴纳证明材料），提供2名专业运维人员开展驻场运维服务（驻场地点：武宁南路128号，至少5\*8小时驻场服务，节假日或重大活动保障期间应根据科技处的要求，提供驻场保障），提供这名工程师的工作简历，并得到最终用户的确认。中标方如需更换驻场工程师必须事先与最终用户协商确定。

免费维护期内，投标方须提供每周7天、每天24小时的技术支持服务，故障响应时间不超过30分钟，到达现场时间不超过1小时，2小时内排除故障或提出解决方案。

免费维护期内，投标方必须接受用户方的需求更改要求（在不增硬件的基础上），免费进行系统及软件升级、整体优化，并对于各应用开发对接提供技术支持，不另行收费。

（四）保修期内当设备故障时，故障设备维修返回时间不超过3个月，在这期间，必须提供同型号的备件顶替，不得影响系统的正常运行，同时设备中硬盘等存储介质必须交由用户方保管。

（五）免费维护期间，投标方须承诺提供巡检服务，定期（每月至少1次）对用户的系统进行巡检，并协助用户对隐患和故障进行解决和追查，最终以报告形式提交用户。

**八、供应商与项目团队要求**

（一）供应商应当具有类似项目建设经验，通过ISO9001质量管理体系认证、ISO20000信息技术服务管理体系认证、ISO27001信息安全管理体系认证、ISO22301业务连续性管理体系认证、ISO27701隐私信息管理体系认证；具有CNCERT网络安全应急服务支撑单位乙级及以上资质。

（二）项目建设与免费维护期间，投标人需提供素质高、专业性强、经验丰富、稳定的项目服务团队。针对本项目提供不少于11人的项目服务团队（包括项目经理、驻场运维工程师、技术支持工程师、产品技术支持工程师等）。

投标单位的项目服务团队应对本项目具备较深的理解，熟悉边界接入平台的技术架构、安全体系。具备公安边界接入平台项目服务经验，能够掌握平台整体技术架构、安全体系、网络环境等各类内容。

投标单位的相关服务人员需具备相应的服务能力，需提供相关证明（最近一个季度任意一个月依法缴纳社保费用的证明）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量下限** | **人员要求** | **驻场要求** |
| 项目经理 | 项目服务人员的总体组织和管理，与用户及时沟通，对服务团队进行内部考核。 | 1人 | 1、硕士及以上学历，通信工程、信息安全、电子信息、计算机、等相关专业；2、具有信息系统项目管理师（高级）证书；3、具有担任5年（含）以上网络安全项目项目经理职务的工作经验；4、具有类似项目管理经验。 | / |
| 驻场运维工程师 | 负责项目维护期内至少5\*8小时现场驻场运维服务，节假日或重大保障期间根据用户要求提供驻场服务。 | 2人 | 1、本科及以上学历，通信工程、信息安全、电子信息、计算机、等相关专业；2、具有信息系统项目管理师（高级）证书；3、具备5年（含）以上网络安全项目运维经验。 | 驻场 |
| 技术支持工程师 | 提供项目技术服务，协助项目经理管理项目服务人员，与用户及时沟通；提供设备安装调试、策略调优、定期巡检、故障诊断、应急响应、培训等服务。 | 4人 | 1、本科及以上学历，通信工程、信息安全、电子信息、计算机、等相关专业；2、具备1年以上网络安全项目经验； | / |
| 产品技术支持工程师 | 负责项目产品技术对接、技术测试等工作。 | 4人 | 1、本科及以上学历，通信工程、信息安全、电子信息、计算机、等相关专业；2、具有3年以上网络安全项目产品技术支持经验。 | / |