全国公安大数据智能化建设应用基础环境（上海部分）(2026 年升级改造)用户需求

一、建设目标与任务

（一）建设目标

本项目建设目标将采用更安全合规、更成熟、更具备推广性的技术手段，通过建设通道 1、通道 2、访问模式以及相应配套服务，充分释放大数据智能化应用服务实战能力，更好服务和促进大数据实战。

（二）建设任务

通道 1：新建专网-数据域业务协同通道，用于用户接入区应用、移动信息网应用、视频传输网应用、电子政务外网应用等与数据接入区业务协同场景。分为外部发起的和数据接入区（内部）发起的。

通道 2：新建视频传输网至数据接入区的视频流单向导入通道，构建高效、稳定、安全的视频传输网与新一代公安信息网数据接入区的视频交换链路。

访问模式：通过安全方案提供的管控能力，构建方便、安全、可靠的接入与访问方式，并融合现有公安大数据零信任体系的基础，提升大数据安全措施。

配套服务：分别在视频传输网接入侧以及数据域接入侧增设 DNS 引流设备，以满足安全访问需求。

二、技术性能指标与配置要求

名称	单位	数量	技术要求
核心交换机	台	2	见 2.1
视频接入交换机	台	8	见 2.2
TAP 及接入交换机	台	4	见 2.3
沙箱系统控制中心软件	套	1	见 2.4
沙箱系统接入授权软件	个	1500	见 2.5
沙箱系统接入网关软件	套	1	见 2.6
防火墙	台	10	见 2.7
负载均衡	台	2	见 2.8
攻击诱捕	台	1	见 2.9
流量威胁监测探针	台	1	见 2.10
流量采集探针	台	2	见 2.11
日志审计	台	1	见 2.12
检控集中管控	台	3	见 2.13
认证代理	套	2	见 2.14
权限代理	套	2	见 2.15
集控探针	台	2	见 2.16
视频安全交换系统（前后置）	套	3	见 2.17
单向光闸	台	6	见 2.18
流量监测探针	台	2	见 2.19
堡垒机	台	1	见 2.20

运维防火墙	台	1	见 2.21
DNS 设备	台	4	见 2.22
系统集成	套	1	见 2.23

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、或系统功能截图证明、或功能实现技术证明等相关证明文件），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。

2.1 核心交换机

指标项	技术要求
硬件要求	交换容量≥1904Tbps
	包转发率≥460800Mpps
	主控板槽位数≥2；业务板槽位数≥8；独立交换网板槽位数≥4
	支持颗粒化电源，整机电源槽位数≥6
	为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，独立风扇框数≥3
	为适应机柜并排部署，设备机箱（包括业务板卡区）采用后出风风道设计
配置要求	单台配置冗余引擎板卡、交换网板≥4，满足单槽位支持最大单向线速处理能力≥480Gbps
	单台配置风扇模块≥3、电源模块≥4，且为冗余配置
	单台实配业务板卡： 40G 以太网光接口板（单块板卡光口数量≥12，接口类型 QSFP+）≥1 块； 百兆/千兆自适应以太网电接口板（单块板卡光口数量≥48，接口类型 RJ45）≥1 块； 万兆/千兆自适应以太网光接口板（单块板卡光口数量≥48，接口类型 SFP+ / SFP）≥1 块；
	单台实配光模块： 40G 多模光模块≥8 个；40G 单模 10km 光模块

	≥4 个，万兆单模 10km 光模块≥20 个；万兆多模光模块≥20 个。要求 40G 光模块要求 QSFP+封装类型，10G 光模块要求 SFP+封装类型，所配光模块需满足本项目实际配置板卡接口类型和距离需求，所有光模块与交换机互相兼容，并能在线检测收发光功率。
	单台实配 40G 堆叠线缆（长度≥5 米）≥2 根(含两端模块)
	配置必需的软件、主机和辅助部件，授权和 license 周期为永久，
缓存容量	支持每端口≥200ms 数据缓存
数据中心特性	支持大带宽高密板卡，满足海量数据吞吐能力，具有高性能、高可靠、低延时等数据中心特性
VLAN	支持 4K VLAN
	支持 Access、Trunk、Hybrid 方式，支持 LNP 链路型自协商
	支持 default VLAN；
	支持 VLAN 交换；
	支持基于 MAC 的动态 VLAN 分配；
MAC	支持整机 MAC 地址≥1M
IP 路由	支持 RIP、OSPF、ISIS、BGP 等 IPV4 动态路由协议
	支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPV6 动态路由协议
	支持 IPv4 路由转发表 FIB 规格≥3M，支持 Ipv6 路由转发表 FIB 规格≥1M
组播协议	支持 IGMP Snooping V1,V2,V3；
	支持 PIM-SM/DM/SSM；
	支持 MSDP、MBGP；
MPLS	支持 MPLS 基本功能；支持 MPLS OAM、MPLS VPN(VPLS,VLL)、MPLS-TE
QoS	支持 PQ、WRR、DRR、PQ+WRR、PQ+DRR 等队列调度方式；
	支持基于 Layer2 协议头、Layer3 协议、Layer4 协议、802.1p 优先级等级的组合流分类；
	支持 ACL、CAR、Remark、Schedule 等动作；
	支持 WRED、尾丢弃等拥塞避免机制；
	支持 HQoS
	支持流量整形
可靠性	支持硬件 BFD/OAM，稳定均匀发包检测，故障倒换时间小于 50ms
用户管理	支持 802.1X、MAC、Portal 等认证方式
管理维护	支持 SNMP V1/V2/V3、Telnet、RMON、SSHV2
	支持通过命令行、中文图形化配置软件等方式进行配置和管理

2.2 视频接入交换机

指标项	技术要求
交换容量	交换容量≥4.8Tbps
包转发率	包转发率≥1620Mpps
硬件	端口不少于 24 个 10G SFP+接口（配置 12 个万兆多模光模块）、不少于 6 个 40/100GE QSFP28 接口（配置 4 个 40G 多模光模块）
	为了提高设备可靠性，支持并配置模块化可插拔双电源
	实配冗余风扇

二层	支持 MAC 表项≥384K
	支持 4K 个 VLAN，支 QinQ、灵活 QinQ、VLAN Stacking、支持静态、动态、黑洞 MAC
三层	支持静态路由、RIP 、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6
	支持 IPv4 路由表项≥256k
	支持 IPv6 路由表项≥80k
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（RSPAN）
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
QOS/ACL	ACL 硬件规格支持 6K
	支持 PQ、WDRR、DRR、PQ+WDRR、PQ+DRR 等队列调度方式
	支持 WRED、尾丢弃、流量整形等拥塞避免机制
	支持基于 Layer2 协议头、Layer3 协议、Layer4 协议、802.1p 优先级等的组合流分类
	设备支持大缓存模式应对流量突发，整机缓存大于 13.5M
安全	支持命令行分级保护，未授权用户无法侵入
	支持防 DOS 攻击、TCP 的 SYN Flood 攻击、UDP Flood 攻击、广播风暴攻击、大流量攻击
管理维护	支持 SNMPv1/v2c/v3，支持 RMON
	支持网管系统、支持 WEB 网管特性
智能运维	支持 Netstream
	支持 Telemetry 技术

2.3 TAP 及接入交换机

指标项	技术要求
交换容量	交换容量≥4.8Tbps
包转发率	包转发率≥1620Mpps
硬件	端口不少于 24 个 10G SFP+接口（配置 12 个万兆 单模 10km 光模块）、不少于 6 个 40/100GE QSFP28 接口（配置 4 个 40G 单模 10km 光模块）
	为了提高设备可靠性，支持并配置模块化可插拔双电源
	实配冗余风扇
二层	支持 MAC 表项≥384K
	支持 4K 个 VLAN，支 QinQ、灵活 QinQ、VLAN Stacking、支持静态、动态、黑洞 MAC
三层	支持静态路由、RIP 、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6
	支持 IPv4 路由表项≥256k
	支持 IPv6 路由表项≥80k

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（RSPAN）
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
QOS/ACL	ACL 硬件规格支持 6K
	支持 PQ、WDRR、DRR、PQ+WDRR、PQ+DRR 等队列调度方式
	支持 WRED、尾丢弃、流量整形等拥塞避免机制
	支持基于 Layer2 协议头、Layer3 协议、Layer4 协议、802.1p 优先级等的组合流分类
	设备支持大缓存模式应对流量突发，整机缓存大于 13.5M
安全	支持命令行分级保护，未授权用户无法侵入
	支持防 DOS 攻击、TCP 的 SYN Flood 攻击、UDP Flood 攻击、广播风暴攻击、大流量攻击
管理维护	支持 SNMPv1/v2c/v3，支持 RMON
	支持网管系统、支持 WEB 网管特性
智能运维	支持 Netstream
	支持 Telemetry 技术

2.4 沙箱系统控制中心软件

指标项	技术要求
兼容性要求	沙箱系统控制中心软件版本要求能兼容华为、曙光等国产服务器，及阿里云、华为云等云平台，支持国产 ARM 芯片及 x86 芯片双栈架构统一管理统一运维，国产 ARM 芯片架构下支持统信、银河麒麟等操作系统，x86 芯片架构下支持 Windows 等操作系统；
云化部署	可支持云化部署方案，可以直接通过云上的基础服务资源搭建安全沙箱系统，并发放沙箱空间，支持云上平滑升级扩容。
高可靠保障	为了提高系统可靠性，保障单台设备故障时系统仍可正常运行，控制中心应支持本地集群部署，集群中的节点可承载工作负载功能，不需要依赖其它外置设备。
	为了使系统资源利用最大化，集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和。为了保障系统的稳定性，集群节点故障后剩余节点仍能接管所有业务，集群均需支持授权漂移机制：集群中的单节点故障后，集群的总授权数跟故障前保持一致。
资源发布能力	通过 WEB 模式,可以支持基于 http 或 https 协议代理访问业务资源，支持发布 IPv4、IPv6 地址或域名形式的后端服务器地址，可配置业务应用的具体访问 URL 路径。
	为方便维护人员管理，支持直接在应用授权界面为单一应用或某个应用分类分配用户授权，授权方式支持直接授权给用户所在的组织架构、用户关联的角色或用户本身，并展示应用直接授权的组织架构、授权角色或用户数量。
	为提升业务应用的数据安全性,应支持针对发布的 WEB 应用开启 WEB

	水印，水印内容至少包括：用户名+当前年月日，起到威慑与溯源作用，有效预防数据泄露。
	▲为提升 WEB 业务的数据安全性，应支持禁止对 WEB 应用禁止复制、禁止打印、禁止下载、禁止鼠标右键、禁止浏览器调试，以保护应用的数据安全。
认证管理	支持本地账号密码认证、OAuth2.0 标准协议的票据认证、CAS 标准协议的票据认证、证书主认证、证书辅认证、标准 Radius 令牌认证、第三方令牌认证、TOTP 动态令牌认证等认证方式；
	支持在满足条件的情况下，可配置成即使是关机重启，也能自动拉起客户端并自动登录一键上线（强制注销情况除外），可配置的条件包括但不限于：授信终端、Windows 域环境、自定义网络环境等。
用户管理	支持通过组织架构、角色等方式进行本地用户管理。新增或修改本地用户时，可编辑的用户属性应包括但不限于：用户名、显示名、组织信息、关联角色、手机号码、密码、用户有效期、帐号是否启用、应用授权等。
	支持与外部用户管理服务器进行对接，包括但不限于 LDAP 用户目录、AD 域用户目录等。
动态上线准入控制	支持配置动态上线准入规则，可配置化的 ACL 规则引擎，可以灵活地将终端环境、用户身份、处置动作等进行配置，为单位不同用户不同部门提供灵活丰富的访问控制策略。 1、动态访问控制策略可指定适用用户范围和排除用户； 2、动态访问控制策略支持针对操作系统单独设定或多系统设定访问控制策略，操作系统需包括 Windows、统信/麒麟等； 3、动态访问控制策略支持“与”、“或”条件嵌套，并可通过单一条件或条件组的方式灵活组合嵌套，可支持的条件变量应包括但不限于：终端名称、MAC 地址、终端本地 IP 列表、操作系统版本、终端资产类型、终端标签类型、运行进程、运行天擎杀毒软件、安装指定软件、开启系统防火墙、开放的操作系统端口、windows 操作系统注册表、用户登录时间、弱密码、授信终端、授信域环境、闲置帐号、帐号首次登录、帐号在该终端首次登录、异常时间登录、非常用地点登录等。
审计能力	支持将用户访问沙箱系统的认证及策略类请求加密流量解密后镜像给外部系统，如态势感知等设备，以完善系统的用户行为审计溯源能力。
	支持个人空间向工作空间和工作空间到个人空间的数据拷贝控制。
	支持用户安全日志提取，审计中心应将具有异常登录行为的用户日志自动打标签为用户安全日志，便于管理员快速审计定位。用户安全日志包括但不限于：帐号安全、中间人、SPA 安全（应包含 SPA Fuzz 攻击、SPA 爆破攻击、SPA 敲门伪造、SPA 重放攻击、SPA 安全码泄漏等）、会话劫持等。

监控中心	支持管理员直接在控制台查看接入沙箱系统的安全概览，包括但不限于 TOP5 的风险 IP、风险账号、风险终端等风险实体，以及账号、终端相关的风险事件分布、风险事件趋势、TOP5 风险事件类型等展示。
	支持查看当前在线用户终端总数；可查看当前在线用户，用户信息至少包括用户名、组织架构、终端类型、浏览器类型、接入 IP、最后接入时间、认证方式等。
	对于创建后长时间未使用、长时间不登录或登录后长时间不使用的用户帐号，支持检测并判定为闲置帐号。闲置帐号的时长可自定义配置，可配置范围不得小于 1-365 天。可设置检测闲置账号后是否自动锁定，支持锁定后手动恢复帐号状态。
设备健康检查	为方便管理员统筹查看管理沙箱系统的整体运行状态，支持对设备自身的安全状态和策略配置进行巡检，对设备的整体状态进行打分，统计所有检查的正常项、异常项和告警项，并输出巡检报告。可在设备上查看及下载巡检报告。报告应至少包含检测项、检查状态、存在的问题描述、建议改进措施等。
	设备稳定性检查，包括但不限于： 1、应支持系统黑匣子及核心进程的状态检测。 2、应支持 CPU 负载、内存负载、磁盘空间、网卡健康、硬盘健康、网卡日志、BIOS 固件等硬件相关状态的检测。 3、应支持软件版本及补丁修复状态等检测。
分权管理能力	支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权。
	内容权限管理模块支持按应用和用户粒度划分权限，如指定某管理员仅能管理指定的应用和指定的用户
	支持至少 15 级用户目录、200 万规格用户帐号数、10 万隧道应用数、10 万 WEB 应用数等。
	最大并发用户≥1700
	新建用户数（个/秒）≥50； 支持外部认证模式，该模式下新建用户数（个/秒）≥25
	理论应用鉴权请求新建 TPS（个/秒）≥270
	沙箱系统可同时管理的在线沙箱数量≥1500
其他要求	满足个性化服务扩展权益、持续强化安全功能
	实现与当前零信任体系适配
	在 3 年质保期内免费软件升级服务

2.5 沙箱系统接入授权软件

指标项	**技术要求**
授权要求	本次采购的安全沙箱客户端终端接入授权数≥1500 个。
用户体验	支持在个人空间浏览器中访问特定链接时，自动启动相应工作空间的浏览器，确保链接在正确的环境中加载访问；支持在个人空间运行指定进程自动拉起到工作空间运行。

功能要求	实现在终端创建具备安全链路、落地文件加密、网络隔离、剪切板隔离、进程保护、屏幕水印等数据保护能力的安全工作空间。
安全能力	为了满足 PC 端数据防泄密需求，沙箱系统接入授权软件需支持在 PC 终端上生成隔离的安全工作空间（非容器类型），在 PC 上使用沙箱应支持 Windows 系统、统信 UOS、麒麟 Kylin 等国产化系统。
	支持工作空间与个人空间文件隔离，用户在个人空间指定路径无法查看工作空间的文件
	支持以文件为单位，对工作应用产生的数据进行加密保存；支持透明加解密技术，加解密过程对用户无感知，在工作空间内可直接打开文档进行预览和编辑。
	文件加密支持“一文一密”即每个文件独立密钥，以确保沙箱系统接入授权软件组件被卸载、模块驱动被摘除的情况下，终端用户仍无法明文取出文件。
	支持个人空间向工作空间和工作空间到个人空间的数据拷贝控制；支持启用剪切板内容审计，开启后将对工作空间到个人空间的拷贝行为进行审计。
	支持配置允许/禁止工作空间文件导出到个人空间；支持配置允许/禁止个人空间文件导入到工作空间；
	支持对工作空间添加屏幕水印，水印至少包含自定义提醒、用户名、时间、空间名称、手机号后四位、终端 MAC 地址等信息；支持为工作空间配置禁止截屏策略，启用后任何截屏程序都无法对工作空间打开的窗口截屏或录屏；支持工作空间内允许使用截图工具进行截屏时，或对工作空间拍照时，截图和照片带有水印信息。
	支持终端用户在客户端上自行查看所关联工作空间的权限，包括但不限于剪切板拷贝权限、文件导入导出权限、打印权限、截屏权限、水印等。
可靠性	支持终端环境诊断排查，可针对客户端接入失败、客户端服务异常、工作空间启动失败进行诊断，便于用户自行排查修复终端问题，减少运维工作。
	为了方便快速运维排障，支持管理员在控制台远程获取在线终端的日志，若终端不在线时支持加入排队列表，排队列表中的终端上线后自动收集日志。
	为了满足用户单位有序平滑、推广沙箱系统接入授权软件接入，需支持客户端的按需灰度升级。 1、支持区分 Windows、macOS、Linux 等不同系统配置灰度升级策略，并支持查看灰度升级进度。 2、为保障客户端升级阶段的稳定性，降低运维工作量，应支持上传新版本客户端独立更新，不需要跟服务端的升级捆绑；且应支持指定用户/用户组进行客户端灰度升级。
业务承载	需配套提供支撑不少于 1500 个安全沙箱客户端，并兼容支持正常使用的物理机操作系统和软件运行环境。同时，要求客户端能够在符合国产化要求的服务器和操作系统环境进行部署。
其他要求	满足个性化服务扩展权益

	实现与当前零信任体系适配
	在 3 年质保期内免费软件升级服务

2.6 沙箱系统接入网关软件

指标项	技术要求
兼容性要求	沙箱系统接入网关软件版本要求能兼容华为、曙光等国产服务器，及阿里云、华为云等云平台，支持国产 ARM 芯片及 x86 芯片双栈架构统一管理统一运维，国产 ARM 芯片架构下支持统信、银河麒麟等操作系统，x86 芯片架构下支持 Windows 等操作系统；
云化部署	可支持云化部署方案，可以直接通过云上的基础服务资源搭建沙箱系统接入网关软件，支持云上平滑升级扩容。
性能指标	接入零信任代理网关流量，需支持不低于 3000M，需支持用户总数为需达到 50000 人
	单虚拟机需支持用户量 5000 人以上
设备检查	支持认证配置检查，包括控制台超时时间配置检查；管理员登录防爆破、管理员首次登录强制修改密码等管理员安全性登录配置检查。
	支持 API 防护检查，包括但不限于 API 接口爆破检查、API 接口越权调用、API 接口扫描、API Web Shell 攻击。
分权管理能力	支持新增/删除/修改管理组，内置审计管理员、安全管理员、系统管理员等管理组；通过管理组管理权限的配置，实现管理员分级分权。
	内容权限管理模块支持按应用和用户粒度划分权限，如指定某管理员仅能管理指定的应用和指定的用户
其他要求	在 3 年质保期内免费软件升级服务

2.7 防火墙

指标项	技术要求
硬件	≥4 个千兆电口，≥4 个万兆光口，≥2 个 40G 光口，冗余电源；三年质保。
性能参数	网络层吞吐量≥70G，并发连接≥3000 万，每秒新建连接数≥68 万；
工作模式	支持路由、交换、混合、IPv4/IPv6 双栈工作模式；
路由交换	支持静态路由、ISP 路由及动态路由协议，支持 802.1q 模式，支持 RIP、OSPF、BGP4、QinQ（VLAN VPN）、PIM-SM、PIM-DM；
	支持基于源/目的地址、源/目的端口、协议、度量值、应用、权重、时间、BFD、选路算法的策略路由；
链路聚合	支持手工链路聚合及 LACP 链路聚合，支持不少于 11 种负载分担算法；
带外管理	支持独立管理接口实现管理流量和业务流量处理隔离；
IP/MAC 绑定	支持手动添加绑定，支持基于 IP、接口的动态探测绑定，支

	持 IP/MAC 绑定表可导入导出；
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；
	支持全面 NAT 功能，对多种应用层协议支持 ALG 功能，包括 DNS、FTP、SIP、H323、MSN、Netbios、PPTP、RSH、RTSP、SIP、SQLnet 等
	支持 NAT66、NAT64、NAT46 功能；
功能虚拟化	支持配置文件、系统服务等系统功能虚拟化；
应用识别和管控	支持运用端口识别、行为识别、特征识别、关联识别等技术手段准确识别和管控传统应用、web 应用、移动应用、云应用、加密应用等；
连接控制	支持对单条访问控制策略进行最大并发连接数限制；
	支持每 IP 连接总数限制，支持所有 IP 连接总数限制，支持每 IP 每秒新建连接数限制；
	支持监控显示最近被拦截的 IP、地址对象及应用的节点信息，支持对连接数限制策略匹配信息进行分类统计；
访问控制策略	支持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、并发会话等功能配置；
	支持针对 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；
	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；
	支持策略命中分析、策略冗余分析、策略冲突检查，支持在 WEB 界面显示检测结果；
	支持策略导入导出，支持策略变更信息查询，支持一键恢复策略；
	支持 IPv4/IPv6 黑名单功能，支持根据五元组、MAC、地址范围、应用组、角色配置黑名单，支持配置生效时间；（提供截图）
DDOS 防御	支持基于 IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、NTP、SIP 等众多协议类型的 DDOS 防护策略，支持对各种协议数据流进行源、目的限流，支持策略模板自定义，支持配置白名单、动态黑名单；
信息防泄漏	支持自定义关键字进行过滤；
	支持对多种类型的文件进行过滤；
黑白名单	支持基于 IPV4/V6 的静态黑名单功能，支持设置 IP 地址、五元组信息、MAC 地址、地址范围、应用组、角色等信息；

	支持基于 IPV4/V6 源地址、目的地址动态五元组黑名单功能；
工作模式	支持双机热备、负载均衡、连接保护等高可用配置；
日志管理	支持日志本地存储，支持对不同类型日志设置存储空间。支持外发日志至 SYSLOG 服务器，支持对日志传输进行加密保护。
其他	病毒库在 3 年质保期内需提供免费升级服务

另：10 台防火墙总计需配置光模块如下：

40G 单模 10KM 光模块 12 个；10G 单模 40KM 光模块 14 个（其中 4 个需适配市局公安网核心网络设备）；10G 多模光模块 14 个；10G 单模 10KM 光模块 14 个。

2.8 负载均衡

指标项	技术要求
性能参数	L4 层吞吐量≥40Gbps，L4 层新建连接数为≥16 万/秒，L4 层并发连接数≥8000 万/秒；≥4TB 硬盘，≥4 个万兆光口，≥2 个 40G 光口，冗余电源；三年质保。
其他硬件参数	CPU≥8 核，内存≥16G
部署模式	支持路由、旁路部署，以及三角传输
高可用性	支持 AA，AP 工作模式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换。
	支持基于 vlan 链路的零流量状态进行高可用故障切换
	支持会话保持表项与连接表项独立同步功能,可根据使用需要定义同步的会话保持表
多合一功能集成	单一设备即可同时支持包括链路负载均衡、服务器负载均衡，全局负载等功能
系统管理与配置	支持备份配置与备份管理，并支持从备份中恢复、从本地文件中恢复的功能
服务器业务负载	支持 SNMP 方式动态读取服务器运行状态进行算法调节；支持随机算法、最快响应时间、动态反馈、加权源 IP 哈希等算法
	支持在 WEB 页面配置主动健康检查,支持常见的主动式健康检查类别至少包括 SNMP、ICMP、SIP、ICMPv6、TCP、UDP、FTP、HTTP、DNS、RADIUS、HTTPS、LDAP、HTTP2、ORACLE、MSSQL、MYSQL 数据库的探测判断机制；
	支持在 WEB 页面配置负载均衡算法，负载均衡算法至少包括轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应时间、加权最小流量、最小流量、最少连接、主机-最小流量、主机-最少连接调度、动态反馈、按主机加权最小流量、源 IP 源端口哈希、源 IP 哈希、URI 哈希和 HOST 哈希。
	支持 cookie 作用域和作用路径的自定义，支持 cookie 加密，提升 cookie 安全性。
	支持 HTTP 被动健康检查，可配置指定检查 URL、响应状态码、响应超时时间、统计时间以及可设置异常 URL 上限，并且能开启/关闭调试日志功能。

	支持在同一个虚拟服务下同时配置多个 IPv4 和 IPv6 地址；
	支持 TCP 被动健康检查，可配置统计时间、监视类型、保护时间等，并且能开启/关闭调试日志功能。
	支持基于主机的健康检查功能，实现当主机健康状态异常时，会影响到其关联的每一个节点。
全局负载	支持标准 DNS 服务，支持正向解析和反向解析功能，支持常用的记录类型如 A、AAAA、CNAME、DNAME、MX、NS、TXT、PTR、SRV、DS、CAA、HINFO 和 NAPTR 等。
	支持 DNS 缓存，可配置全局缓存最小时间和最大时间，并可设置 MSG 缓存大小、RR 缓存大小、密钥缓存大小、否定记录缓存大小和否定记录最大缓存时间
	支持 TCP 和 UDP DNS 解析能力，支持设置 EDNS 缓冲区大小
链路负载均衡	支持通过 Web 页面进行智能选路的路由测试功能,支持基于应用协议的智能选路。
	支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。
运维管理	IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66、FTP ALG、DNS64 等协议转换。
	支持端口枯竭告警功能,并支持针对告警阈值和告警间隔时间进行设置。
	支持 Web 页面抓包，并且可设置抓包时间。
	支持 SNMP V1/V2/V3 协议，支持 snmp ipv6
其他	3 年质保期内需提供免费升级服务
	单台配置：不少于 4 个万兆单模 10km 光模块，不少于 2 个 40G 单模 10km 光模块

2.9 攻击诱捕

指标项	技术要求
性能参数	具备同时启用≥10 个（2C2G）蜜罐实例的能力；≥4 个千兆电口，≥4 个万兆光口，≥960G SSD 存储，≥4TB SATA 存储，冗余电源；三年质保。
数据统计	统计蜜罐实例部署数量、监听 IP 数量、诱捕节点数量、遗留文件数量、溯源成功次数和反制成功次数的数据，支持按照当天、7 天、30 天和自定义方式进行选择
攻击者行为链	支持展示 ATT&CK 模型构建的攻击者行为链
代理流量	支持按照线形图查看被动代理的流量趋势
攻击事件	支持按照攻击 IP、攻击者类型、威胁级别、攻击者归属地、告警类型、XFF 最新值、时间筛选告警
	支持按照攻击 IP、攻击者类型、威胁级别、告警数量、攻击者归属地等数量统计告警
	支持查看攻击者画像详情，基本信息(攻击 IP、自定义标签、攻击者类型、社交信息数、设备数量、溯源反制阶段、告警数量、告警

	类型、初次攻击时间、最近攻击时间、攻击者威胁等级、攻击者归属地)、攻击事件热力图、攻击分析环形图、受害 IP、XFF 代理、PDNS、RDNS、攻击者社交信息、攻击者设备信息、诱饵下载列表、反制成功信息、交互式反制(文件上传、文件下载、桌面截图、命令执行)、攻击轨迹(行为分析、溯源反制)、遗留文件等攻击者信息
行为分析	支持按照攻击 IP、受害 IP、实例名称、攻击结果、告警类型、攻击者归属地、威胁级别、攻击行为、XFF 代理、子网名称、时间筛选告警
	支持按照危急、高危、中危、低危的威胁级别统计告警
	支持查看攻击回放，包括最初攻击时间、最近攻击时间、攻击 IP、实例名称、子网名称、攻击者类型、RDP 实例视频回放
	支持查看单条告警记录详情，包括告警基本信息、原始数据(请求、响应)
溯源反制	支持按照攻击 IP、反制类型、攻击者归属地、攻击者信息、时间筛选告警
	支持按照浏览器指纹、JSONP 溯源、MySQL 反制、反制文件、诱饵命中的反制类型统计告警
	支持查看溯源反制告警详情
遗留文件	支持按照文件名称、攻击 IP、文件类型、关联实例、时间筛选文件
	支持按照高危、中危、低危、安全的威胁级别统计文件数量
蜜罐管理-实例管理	支持按照实例名称、交互类型、模板名称、监听 IP、实例状态、子网名称、诱捕状态筛选实例
	支持对实例进行编辑、停止、启用、暂停、重启、查看、删除操作
	支持查看实时监控蜜罐实例运行状态：启动中、运行中、关闭中、已停止等
	支持查看蜜罐实例诱捕情况：未被攻击、受到攻击
	支持按照高中低交互类型创建实例
	支持登录钓鱼反制实例，用于定制网站的登录界面仿真，并含有反制与钓鱼功能
	支持在指定的实例上配置反制功能,通过反制功能获取攻击者的浏览器指纹、JSONP 社交信息等
	支持实例添加监听 IP 数量不受限
	支持新增快照，将当前状态的蜜罐实例保存为快照，进行下载、删除和恢复等操作
诱捕节点管理	支持通过下载安装包感知节点,通过感知节点接收诱饵相关的回连信息
	支持通过下载安装包或复制安装脚本的方式部署诱捕节点,支持在 windows 和 Linux 的操作系统上部署
	支持查看诱捕节点详情，包括：基本信息、服务信息、诱饵信息等
	支持诱捕节点开启智能推荐常用服务配置监听规则
诱饵配置	支持自定义诱饵文件，诱捕节点客户端自动投放诱饵文件

	支持添加主机诱饵，利用主机发布的虚假用户信息迷惑攻击者，包括 Xshell 连接诱饵、SSH 历史命令诱饵、远程桌面诱饵
主动引流	支持通过 SDN 的方式进行攻击力量的牵引,支持对 SDN 交换机的链路和接口进行管理
	支持通过代理模式进行流量牵引，无需外置硬件探针
	支持按照攻击 IP、受害 IP、威胁名称、威胁等级、告警名称等信息筛选告警
蜜网拓扑	支持按照星型拓扑，展示攻击诱捕系统、实例、蜜点、诱捕节点的各节点关系网
基础配置	支持证书管理（标准功能证书、主动引流授权），导入/导出、获取权限
	支持网络配置：可进行管理 IP 配置和 DNS 配置
蜜罐模板	支持按照模板名称、交互类型、服务协议筛选模板
	支持通过模板的方式导入实例的定制模版
	支持内置实例模板，数量不少于 50 个
	支持常见中低交互仿真服务如：网络安全系统仿真、网络设备与服务仿真、行业软件仿真等
	支持常见的漏洞靶场如：Spring V5、Struts2、Tomcat、Apache Log4j2、thinkphp V5 等
JSONP 设置	支持通过 JSONP 获取 10 余种 JSONP 溯源网站攻击者社交信息，
	支持添加自定义 JSONP 溯源接口
黑白名单管理	支持设置告警白名单，触发白名单则不会产生告警。支持对名单进行增删改查，支持根据名单细节筛选
	支持设置蜜罐黑名单，触发黑名单则不会访问到蜜罐。支持对名单进行增删改查，支持根据名单细节筛选
	支持设置登录黑白名单，触发黑名单则不会访问和管理到蜜罐设备；触发白名单则仅白名单内用户可访问和管理到蜜罐设备。支持对名单进行增删改查，支持根据名单细节筛选
状态与监控	支持展示系统的运行状态，包括 CPU 利用率、内存利用率、存储空间使用率、网络流量，日志外发情况的展示
	支持通过页面对设备进行设备关机、设备重启、恢复出厂、服务自检等操作
其他	3 年质保期内需提供免费升级服务
	单台配置：不少于 4 个万兆-单模-LC 10km 光模块

2.10 流量威胁监测探针

指标项	技术要求
性能参数	≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆光口，冗余电源，1TB SATA 硬盘；三年质保。
	网络流量处理能力≥10Gbps
抓包分析	支持展示本地 PCAP 会话数据用于告警分析，可以查看会话数量，会话时间、源/目的 IP、协议、会话信息等。

旁路阻断	支持基于 IP 和域名的旁路阻断,能够在实时镜像的流量中发现恶意 IP 并实现实时阻断,支持 24 小时/7 天/最近 30 天/永久或者自定义时间阻断威胁。
日志传输	支持传输协议审计日志，包括 https、http、DNS、邮件协议审计日志、SMB、AD 域、WEB 登录、FTP、TELNET、ICMP 、SNMP 、SSL 、SSH、SIP 、ONVIF 、NFS 、SOCKS 、dhcp、netbios_nbns、流量元数据审计、数据库审计协议等
系统管理	提供三权分立的用户管理能力：系统管理员、审计管理员、操作员，角色相互独立；同时支持 IP 绑定的登录安全设置。普通管理员角色的权限可自定义模块页面的编辑和查看权限
	可实时监控设备的 CPU、内存、存储空间使用情况；能够监控监听接口的实时流量情况
对象识别	1.支持根据数据包方向、协议、端口、IP 地址等信息自定义应用规则来识别应用类型。 2.支持通过规则 ID、名称、攻击影响、危险等级、字符串、正则表达式及匹配方向来自定义 web 应用检测规则库、自定义 IPS 规则库，支持自定义登录规则库。 3.支持自定义内网服务器 IP 组、客户端 IP 组
应用安全专项分析	支持命令注入检测、PHP 代码检测、XSS 攻击检测、Webshell 上传检测、SQL 注入检测、XXE 攻击检测、JAVA 代码检测、SQL 非注入型检测、MYSQL 解析增强、php 反序列化检测等自定义配置启用，针对命令注入检测、SQL 注入检测等类型支持自定义高检出、低误报模式
	支持新增白名单、黑名单等策略，且可通过列表形式展示已有策略（含名称、类型、目标 IP 组、开放的服务、允许访问的 IP 组/时间、禁止访问的 IP 组/时间、状态等。）白名单策略只允许白名单里的 IP（组）在指定的时间内访问，其他时间或其他 IP 的访问均被视为违规，黑名单策略禁止黑名单里的 IP（组）在指定的时间内访问，否则将被视为违规
	支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Media 漏洞攻击、Network Device、Shellcode 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击、IPS 云防护等服务漏洞攻击检测。
	支持基于数据库威胁的分析，发现受攻击的数据库及详细的数据库危险操作。
系统安全专项分析	支持从暴力破解，弱口令，未授权维度分析系统安全
	内置 IPS 漏洞特征识别库、应用识别库、WEB 应用防护库、僵尸网络识别库、实时漏洞分析识别库
	支持基于自定义配置弱口令字典，支持自定义 FTP 弱口令检测，规则设置如空口令、用户名和密码相同、长度、弱口令列表等；支持口令暴力破解检测不同类型（FTP/WEB 登录）的爆破次数。
其他	3 年质保期内需提供免费升级服务
	单台配置：不少于 4 个万兆-单模-LC 10km 光模块

	系统免费提供二次开发，将解析后的数据输出给市局网络安全运营管理平台

2.11 流量采集探针

指标项	技术要求
性能指标	流量处理≥20Gbps，数据包处理能力≥1000 万 pps，≥TCP／UDP 会话处理 100 万／秒；存储空间≥96TB，≥2 个千兆电口，≥4 个万兆光口，冗余电源；三年质保。
服务要求	免费提供补丁修复及版本升级服务。
分布式部署模式	支持“分布部署、集中监控管理”架构，能够实现横向扩展。集中监控管理服务器能够采集各分布式采集设备的性能分析数据，并实现统一监控、分析，并支持流量镜像、TAP 等方式部署，要求能够对镜像数据的集中管理。
国产化支持	设备支持与鲲鹏、海光等国芯硬件平台的适配、设备支持麒麟、统信、欧拉等国产操作系统。
数据加密专用客户端提取数据包	支持加密存储数据，为确保所采集的数据流量安全，系统所存储的数据包格式为自有加密格式，非传统 cap 及 pcap 格式，且系统同时支持 B/S 及 C/S 架构，用户可通过浏览器便捷的进行可视化监控及分析配置，当需要调取流量中的原始数据包的时候，出于安全考虑只能通过专用的控制台软件才能调取并下载数据包至操作电脑本地，同时控制台软件的数据传输模式支持加密，防止数据外泄。
流量过滤	支持根据 mac 地址、IP 地址、IP 地址段、通讯协议、TCP/UDP 端口或应用进行流量捕获和存储过滤(或以上条件的组合过滤策略)，被过滤流量不存储原始数据包，也不进行实时分析与统计；以及被过滤流量不存储原始数据包，但需要进行实时分析与统计。
基础分析功能	支持截断数据包的分析,即数据包经过 TAP 截断后输入探针服务器，由分析探针进行原始流量的速率及数据量还原统计； 能够统计分析链路捕获的流量的趋势，包括总体流量的趋势，可区分网络的上行流量和下行流量；数据包趋势，可区分网络的上行数据包和下行数据包；TCP 参数趋势，包括 TCP 同步数据包个数、TCP 同步确认数据包个数、TCP 同步重置数据包个数；利用率趋势，可区分网络的上行利用率和下行利用率。
数据链路层采集分析	系统支持基于原始数据包的 mac 层地址统计分析，分析维度包括 mac 地址、mac 会话 基于 mac 地址支持统计以下 KPI： 总字节数、发送/接收字节数、发送/接收比特率、发送/接收数据包数、广播数据包数、组播数据包数、发送 ARP 请求/响应数； 基于 mac 会话支持统计以下 KPI： 源、目 mac 地址的总字节数、双向发送/接收字节数、双向发送/接收比特率、双向发送/接收数据包数 以上指标均支持一秒级颗粒度统计
IP 层采集分析	系统支持基于原始数据包的 IP 层地址统计分析，分析维度包括 IP 地址、IP 会话、IP 网段（ip site）、IP 网段与网段间 能够统计分析所有 IP 主机的通讯流量信息，包括接收发送流量，

	接收发送数据包，比特率，数据包率，tcp 连接请求数量，tcp 同步响应数量，tcp 同步重置数量，数据包的发收比，tcp 连接请求无响应次数，tcp 连接请求被重置次数等流量参数，并能够根据参数的大小进行排序。支持二次挖掘指定 IP 的应用成分、IP 会话、TCP/UDP 会话等关联统计分析表 以上指标均支持一秒级颗粒度统计
	支持将 IP 地址与资产及现网功能区进行关联，并使用别名标识，提升故障对象的识别与分析效率
	支持 IP 地理位置标定，包含源目 IP 详细地理位置，自带 IP 地址库，能够准确区分省，市，区县，以及运营商,数据准确度需达到 99%，满足地址流量统计需求
传输层协议采集分析	系统支持统计分析网络中所有 TCP/UDP 会话五元组、服务节点开放的 TCP/UDP 的服务端口、客户端到服务器服务端口的全量访问统计。系统能够统计基于传输层的接收发送流量,接收发送数据包等 KPI。对 tcp/udp 五元组会话,需要能够分析会话的开始时间,持续时间,会话状态，应用协议类型，重传数量，分段丢失数量，重传率，分段丢失率，平均 ACK 时延，TCP 交易数量，最大响应时间，平均响应时间等。且指标均支持秒级统计
指定对象检索	提供全局搜索功能，针对任意 IP、应用、通讯对、网段、TCP/UDP 服务端口、TCP/UDP5 元组以及数据包特定值搜索能够自动发现所经过的监控链路，支持显示检索对象的流量、比特率、连接状态、会话数等曲线，针对 IP 及 IP 会话的检索条件支持连续和非连续 IP 范围检索两种方式。
NAT 会话缝合关联	在 NAT 地址转化场景下，支持会话缝合展示，全链路 NAT 会话自动关联，可根据流量特征自动关联 NAT 会话转换前后会话，对比分析相关指标数据、发现前后时延、丢包、穿透时间等指标变化。
预警组合指标	可以根据自己的需求对业务节点定制告警规则功能，能够对各种 KPI 指标的多种参数逻辑或、逻辑与的灵活组合警报，能够支持告警排除时间范围设置，触发时间支持 1 秒、10 秒、1 分钟等样本评估间隔。
协议内容统计报警	具备指定流量、地址及协议内容的统计报警功能，支持针对 ASCII 及 HEX16 进制特征值内容警报，并配置源和目的 IP 地址、端口、协议及 ICMP 标志位等多种特征条件，为确保特征统计警报的准确性，协议支持 http、ftp 和 ETHERNET_II 等常见协议外，还支持 Modbus_TCP、S7、IEC_MMS、IEC_101、DNP3、CoAP、AMQP、GTP_U 和 XMPP 等 5G 物联网、工控网络协议。
其它	3 年质保期内需提供免费补丁修复及版本升级服务。
	单台配置：不少于 4 个万兆-单模-LC 10km 光模块

2.12 日志审计

指标项	技术要求
性能参数	综合日志处理性能≥6000EPS，日志采集处理≥10000EPS，至少包含 135 个日志源授权； ≥6 个千兆电口，≥4 个千兆光口，冗余电源，≥16GB

	minisata+8TB 硬盘。三年质保。
日志采集与转发	支持通过 syslog、SNMP Trap、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。
资产管理	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。
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；
	持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析
	支持正则表达式、JSON、分隔符等解析方案，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；
	支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数,减少对网络带宽和数据库存储空间的占用
	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。
	系统支持即席在线查询,支持嵌套查询,可针对查询结果任意回退，收敛事件范围；用户可根据需要配置事件显示的字段内容等。
	用户点击事件任意属性字段,可以该字段为条件对事件进行统计分析，并展示 Top 20 排序，排序支持正序和倒序，并可对统计内容进行点击下钻
	用户点击单条事件，可对该事件进行展开，显示事件详细信息和原始信息
	用户点击事件的某一字段,可以该字段及内容为条件在当前事件集中进行事件搜索，显示相应结果；
日志检索	支持自定义过滤条件检索，支持对模糊 ip、多个 ip、ip 地址段、应用、协议、MAC 地址等其他字段精准检索，至少支持 AND、OR、NOT 三种运算符；
	支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件

	支持解码小工具，按照不同的解码方式解码成不同的目标内容，编码格式包括 base64、Unicode、GBK、HEX、UTF-8 等
日志统计分析	支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到 350 条以上，支持自定义关联分析规则
	支持内置规则作为模板新建规则，支持调整规则等级，支持通过事件的任意字段制定规则创建策略,支持审计策略命中后可以定义告警并通过相应方式转发，如：邮件、短信等
	支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件

2.13 检控集中管控

指标项	技术要求
性能参数	并发用户数不少于 5000，并发在线用户授权至少 500 个；≥4 个千兆电口，≥4 个万兆光口，冗余电源；三年质保。
	CPU≥16 核，内存≥64G
检控集中管控平台	▲支持对可信接入检控、可信应用检控提供集中配置、令牌管理、资源监控等服务；
	支持集中查看 web 应用、API 资源的访问日志
	支持查看令牌核验日志,查看核验通过的用户令牌、应用令牌信息
	支持与认证代理和认证服务联动，提供用户令牌、应用令牌检查能力，将核验结果同步接入检控、应用检控，根据核验结果阻断或放行
	支持与权限服务联动，提供用户对应用访问检查能力，根据检查结果阻断或放行
	支持与业务安全策略控制服务联动，提供风险上报、策略指令联动能力，并将阻断指令同步到接入检控、应用检控。
	支持与审计服务联动，上报令牌核验日志，应用访问日志，API 访问日志；
	支持可信接入检控、可信应用检控的集群管理。
	提供 SSL/TLS 加密流量解密能力，支持 SM2、SM3、SM4 国密算法；选配国密卡，支持硬件加密；
	针对设备本身的安全，提供文件防护、暴力破解防护、操作系统加固；
	高可用性：支持集群水平扩展能力；
	支持与可信应用检控、可信接入检控实现通道安全：SSL/TLS 加密流量解密能力，支持国密算法；
其它	3 年质保期内需提供免费升级服务
	单台配置：不少于 4 个万兆-单模-LC 10km 光模块

2.14 认证代理

指标项	技术要求

配置要求	SM2 加密吞吐率≥5Gbps，SM2 每秒新建连接：单向≥12K，并发连接数≥12W，SM2 HTTPTPS≥30W； 至少单颗八核、16G 内存、256G 硬盘，≥2 万兆光口，≥6 千兆电口，双电源；三年质保。
组织机构及人员管理	根据《全国公安机关机构代码编制规则》的要求，提供符合编制规则的公安组织机构管理功能， 保证公安组织机构合规、真实、有效的同时，尽量保证它的灵活性、实用性。系统应具备人员信息管理功能，通过现行各种规则，如身份证号编制规则、公安机关机构代码编制规则等，维护公安工作人员身份信息，建立健全管理员管理机制，保证警员信息的真实有效。
应用认证方式	根据不同公安业务应用系统的安全等级分别配置不同的认证方式， 最大限度的保证各业务系统数据的安全性和有效访问，防止通过越权、冒仿等手段非法进行数据访问的情况出现。
认证方式及认证因子管理	支持不同维度、不同安全等级认证因子定制组合，生成多因子认证方式，满足不同敏感级别应用的不同强度认证需求。支持标准化接入不同认证因子，并其进行统一管理。认证因子包括声纹、人脸、数字证书等。
令牌管理	▲提供令牌全生命周期的管理，包括生成、发布、撤销、延续等。
统计分析及日志管理	统计用户注册、认证情况，以此分析用户使用情况、系统压力等，根据分析结果调整认证策略，优化系统性能，保证用户使用体验、系统高效稳定运行，持续提供服务等。支持记录用户行为日志，供系统自己分析的同时，向审计输出日志信息，配合审计工作的顺利开展。
接入管理服务	接入管理提供标准化的对接服务，用于认证因子接入、数据同步等。
运维监控服务	支持使用情况监控预警，并进行监测情况的展示。
统一认证服务	支持向接入零信任体系的应用提供用户的身份认证，实现单点登录、敏感应用进行安全级别较高的认证等业务需求。
数据安全传输	认证服务中组织机构数据、人员数据、令牌都与相关服务或应用进行交互发挥作用，出于安全考虑，需要支持对数据进行加密传输，并最小化原则进行输出。
协议解析服务	数据传输、存储等过程中，为了保证数据的安全、完整，进行数据加密等操作，数据接收方接收到数据后，调用协议解析服务转化数据， 保证数据的可读性、可识别性。
数据库管理	要求数据库管理采用统一的数据结构方式，使数据结构化，全局数据结构由多个程序共用，各程序调用局部结构数据，全局和局部的数据构成集合，使得数据高度共享，低冗余，同时数据独立性高，不影响程序对数据的使用。
风险传递服务	认证服务识别到的风险除基于自身逻辑进行处理外，还要向零信任相关服务进行风险传递，用于综合风险评估判定。
日志推送服务	认证服务记录的日志除基于自身逻辑、业务需要进行统计分析、审计等处理外，要求向零信任体系相关服务进行日志输出。
授权要求	要求认证服务用户数量、终端数量无限制授权；机构数量≥1 万

	条；应用数量≥500 个。
性能要求	身份信息查询响应时间≤1 秒;如需为其他系统提供身份信息时，响应时间≤1 秒；双因素身份鉴别能力≥300TPS；单因素身份鉴别能力≥500TPS；签发票据能力≥1000TPS；验证票据能力≥1000TPS。
业务承载	支撑不少于 50000 点权限服务实时正常使用的客户端运行环境。同时，要求软件能够在符合国产化要求的服务器和操作系统环境进行软件部署。
其它	3 年质保期内需提供免费升级服务
	单台配置：不少于 4 个万兆-单模-LC 10km 光模块

2.15 权限代理

指标项	技术要求
配置要求	SM2 加密吞吐率≥5Gbps，SM2 每秒新建连接：单向≥12K，并发连接数≥12W，SM2 HTTPTPS≥30W; 至少单颗八核、16G 内存、256G 硬盘，≥2 万兆光口，≥6 千兆电口，双电源；三年质保。
角色管理	支持角色与对象属性一对一的关系，一个对象会对应多个常态属性，在网络中可以拥有多个角色，角色则是按照对象属性在网络中的资源集合，通过属性与角色的对应关系，完成主客体之间的自动匹配，实现权限的形成。
应用管理	提供应用管理服务。
资源管理及授权管理	提供资源管理服务，提供资源授权管理服务。
流程管理	流程管理是为权限管理服务提供与业务安全审批服务子系统相互联动的入口。包括但不限于流程申请、流程删除、流程查询。
权限监测预警及同步	提供权限监测预警服务。提供权限同步服务。
机构、用户对接服务	提供机构、用户对接服务。
系统管理	系统管理主要是用于系统的日常管理，便于管理员随时了解系统运行状态，管理原通过系统完成对系统的配置、系统运行情况的监测、权限管理员的分配等。
令牌使用管理	▲令牌使用管理是指授权管理和认证服务以及应用交互时，需要通过用户令牌及应用令牌进行安全校验，令牌中存储部分鉴权条件信息。
在线鉴权	在线鉴权是指鉴权服务本身将为第三方开放接口，实时响应第三方应用的鉴权请求。可通过同步的方式，获取到授权管理的权限结果。
鉴权监测预警服务	包括但不限于异常 IP 鉴权预警、异常时间鉴权预警、异常鉴权预警处理。
系统管理	系统管理主要是针对管理员，可对系统进行配置、对系统运行情况进行监测等。

接口服务	包括但不限于角色维护服务、角色查询服务、角色与资源绑定服务、角色与资源绑定查询服务、推送授权结果服务、应用级鉴权服务、功能级鉴权服务、服务级鉴权服务、数据级鉴权服务、外部应用接口级鉴权、权限策略变更通知服务、白名单查询服务。
授权要求	要求权限服务用户数量、终端数量无限制授权。资源条目、权限策略、权限集合无限制授权。
性能要求	在线授权≥300 次/TPS；在线鉴权≥500 次/TPS。
业务承载	支撑不少于 50000 点权限服务实时正常使用的客户端运行环境。同时，要求软件能够在符合国产化要求的服务器和操作系统环境进行软件部署。
其它	3 年质保期内需提供免费升级服务
	单台配置：不少于 4 个万兆-单模-LC 10km 光模块

2.16 集控探针

指标项	技术要求
硬件要求	内存≥16GB，硬盘≥2TB，千兆电口≥6 个，万兆光口≥2 个（满配万兆多模光模块）。三年质保。
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。

2.17 视频安全交换系统（前后置）

指标项	技术要求
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。三年质保。
	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≥128GB。支持国产操作系统、国产 CPU 芯片。
	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≥9Gbps。并发路数 D1 标清≥4000 路或 D4 高清≥2000 路。传输时延≤50ms。
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，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。

2.18 单向光闸

指标项	技术要求
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。三年质保。
	内外主机分别配置接口：千兆电口≥6 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≥16 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≥9Gbps。传输时延≤50ms。
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。

2.19 流量监测探针

指标项	技术要求
硬件要求	双 CPU（每个 CPU≥16 核，≥2.2GHz），内存≥64G；硬盘≥SSD 512G。千兆电口≥6 个，万兆光口≥2 个（满配万兆多模光模块）；40GE 光口≥1 个（满配光模块）；冗余电源．三年质保。
性能要求	可处理网络流量≥15Gbps
功能要求	含有流量采集、扫描监测、内容解析、边界安全预警告警及数据输出功能
	支持端口镜像与被动接收两种采集方式，支持多种应用协议的解析并范式化为应用协议结构化数据。
	综合采用端口服务扫描、漏洞扫描、访问探测等方式，对包括边界所有设备信息、所有业务运行信息、边界平台中的网络访问信息、安全设备的日志信息以及边界平台的使用安全和运行安全风险进行监测。
	支持对边界设备信息进行扫描，包括漏洞信息、弱口令信息。
	对绕过边界隔离措施、直接穿透边界等高危风险进行监测与预警，包括端口映射、TCP/UDP 端口代理、SOCKS 代理、HTTP 反向代理、隐蔽通道等。
	对数据盗取、敏感数据泄露等数据安全风险进行监测与预警，包括数据流出异常、长时间无数据交换、API 业务调用异常、视频业务调阅异常等。
	对边界平台自身安全隐患进行监测、预警，缩小边界平台受攻击面，提升整体安全防御能力，主要包括发现僵尸资产、高危端口、未注册用户访问、访问控制策略不严、安全措施失效等问题。
	对来自外部网络的攻击行为进行检测，防止资产风险面受到攻击，包括：漏洞扫描、口令破解等功能。
	备案信息校验：识别边界设备、边界业务相关信息，与备案信息比对，校验备案信息与实际建设、使用是否相符，提升边界备案信息的准确性和时效性，包括发现未备案资产、未审批业务、未备案的业务用户账号、业务类型与备案不一致、数据交换方向与备案不一致、业务访问源 IP 与备案不一致等。

2.20 堡垒机

指标项	技术要求
性能参数	含至少 100 个授权接入许可； ≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆光口，冗余电源，1TBSATA 硬盘；三年质保。
部署要求	设备采用旁路部署，不得影响业务环境，支持 HA 双机部署
用户角色	系统内置组织管理员、策略管理员、审计管理员、运维员等角色，并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；支持角色权限细粒度划分，包括新建部门、安全配置、网络配置、HA 配置、端口配置、外发配置、认证配置、工单配置、告警配置、系统风格等权限划分

用户管理	支持细颗粒度设置登录安全规则，登录失败次数、源 IP 黑名单失败次数、登录时间间隔等，支持自动禁用长时间未登录的用户。配置不活跃用户自动禁用有效期，将长时间未登录的用户更改为失效状态。
支持的协议	支持的运维协议包含 SSH、RDP、VNC、Telnet、SCP、SFTP、DB2、MySQL、Oracle、SQL Server、DM、Redis、PostgreSQL 等
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
细粒度权限控制	可根据部门、用户、用户组、资源账户、账户组、双人~~授权~~复核、动态令牌、有效期、文件管理控制、文件传输控制（上传、下载）、上行剪切板、下行剪切板、水印、磁盘映射、RDP 剪切板控制、时间限制（允许登陆、禁止登陆）、IP 限制（黑白名单）为条件，细粒度地进行访问控制
数据库控制	支持对 MySQL、Oracle 和达梦数据库的访问操作进行控制，支持数据脱敏，用户可自定义脱敏规则
账户同步策略	支持账户同步策略，执行方式支持手动同步、定期执行、周期执行同步策略支持拉取账户和推送账户，当账户密码不一致时允许更新账户密码，账户不存在时允许创建账户，执行日志支持查看账户执行结果（主机执行结果，更新密码、新建账户）并支持结果下载
自动改密	支持以部门、资源账户、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
水印	支持水印功能，用户在运维或者是监控、查看会话时，H5 页面会将用户的登录名作为水印展示，避免数据泄露无法追责，支持在 H5 运维 SSH、RDP、TELNET、VNC、应用发布等资源时显示水印
审计日志	支持记录用户登录资源的操作行为，包含：资源名称、协议类型、主机或应用地址、资源账户、起止时间、会话时长、操作用户、来源 IP、操作记录、文件传输记录、会话协同记录、以及会话结束状态的审计
协同操作审计	支持对协同用户的操作审计，所有操作关联到实际的操作人员
其他	3 年质保期内需提供免费升级服务
	单台配置：不少于 4 个万兆-单模-LC 10km 光模块

2.21 运维防火墙

指标项	技术要求
性能参数	网络层吞吐量≥40G，并发连接≥1200 万，每秒新建连接数 25 万；≥4 个千兆光口，≥4 个万兆光口，冗余电源，1T 硬盘； 三年质保。
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	所投产品需支持支持通过 802.3ad 协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的 MAC 组合、MAC 和 IP 组合或 TCP/UDP 端口组合等方式实现负载和备份

路由协议	所投产品需支持支持静态路由、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，；需支持静态和动态多播路由，动态多播路由需支持稀疏模式
	所投产品需支持基于策略的路由负载,支持根据应用和服务进行智能选路，支持轮询、带宽比例、加权最小流量、优先使用前面线路 4 种负载均衡算法来智能选路，支持通过 ARP、DNS、PING 协议方式进行链路探测。
地址转换	所投产品需支持全面的 NAT 转换配置，包括一对一，一对多，多对一的源、目的地址转换
	所投产品需支持在会话的源、目的地址同为 IPv4 地址时，可将目的地址转换至指定服务器地址
IPv6 支持	所投产品需设备接口支持配置 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；
	所投产品需支持 IPv6 下静态路由及策略路由、动态路由，动态路由应包括 OSPFv3、BGP4+
	所投产品需支持 NAT64，NAT66 等 IPv4/v6 过渡技术
	所投产品需支持配置基于 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；
高可靠性	所投产品需支持路由模式、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
虚拟防火墙功能	所投产品需支持将物理防火墙资源，如会话数、安全策略数、源 NAT 数、目的 NAT 数，日志存储数量以保留值及最大值的形式自动分配。
	所投产品需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
访问控制	所投产品需支持基于源安全域、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
	所投产品需支持命中时间分析和安全策略推荐。命中时间分析展示被命中的安全策略的名称、状态、命中数、策略创建时间、首次命中时间和最近命中时间。

流量管理	所投产品支持设置每 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。
	支持配置基于 IP、用户、应用的流量管理规则
引流策略	所投产品支持引流策略的添加、删除支持引流策略的启用和禁用功能。
	所投产品支持灵活的细粒度引流策略，可基于源区域、目的区域、源地址、目的地址、服务的策略路由，并详细记录日志。
网络攻击防护	所投产品需支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、Frag Flood、DNS Flood、HTTP Flood，并支持日志记录和阻断丢弃等多种防护措施
	所投产品需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
病毒防护	所投产品需能够对 HTTP/FTP/POP3/SMTP/IMAP/SMB 六种协议进行病毒查杀；
	所投产品需支持对最多 16 级的压缩文件进行解压查杀
	产品应具备独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略。
入侵防御	所投产品需支持漏洞防护功能，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
其他	产品内置不低于 16000 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
	3 年质保期内需提供免费升级服务 单台配置：不少于 8 个~~万兆~~-单模-LC 10km 光模块

2.22 DNS 设备

指标项	**技术要求**
平台	为保证设备运行稳定，DNS 为专用一体化设备
配置	硬盘≥1TB*2，支持 raid 0，1；内存≥16G；支持热插拔双冗余电源，电口≥8 个；千兆光口≥2 个

设备参数	QPS≥8 万 QPS；LPS≥500
智能递归调度	支持智能出口流量调度技术，实现多出口链路的充分合理利用和快速的自动容灾切换
TTL 值优化功能	具备缓存管理技术，支持不同视图对应不同的缓存模块，支持缓存模块容量大小、缓存 TTL 的设置，支持缓存内容的查询、删除功能，并可以通过前台立即刷新对应的缓存结果
视图功能	用户根据源 IP 匹配视图，根据视图可以定义不同的 DNS 策略，支持系统默认视图：对所有源 IP 都生效，支持普通视图：具有明确的源 IP 地址范围，普通视图地址范围可以重叠，普通视图具有优先级，DNS 解析按优先级来选择匹配普通视图，系统视图优先级最低
内置域名库	内置域名库包括但不限于游戏网站、视频动漫、购物网站、下载网站、新闻媒体、网银、国际域名和教育网资源等，同时域名库可进行主动编辑和更新升级；可以通过库调节流量，将不同网站应用类别的应调配到特定出口，提供相关产品功能截图
	可支持不低于 100 万自定义域名库，提供第三方测试机构出具的专业测试报告
域名请求转发	支持 First/RTT、First/Order、Only/RTT、Only/Order 和 No 的转发方式；支持对 Forward 服务器进行健康检查
自定义属性	支持为权威记录等资源列表动态添加多个自定义属性列，方便用户为域名记录灵活添加备注信息
支持会话保持技术	支持会话保持时间设置，实现会话保持时间自主定义
源 IP 限速、域名限速	全局源 IP 限速、特定源 IP 限速、限制其 DNS 查询速率，超过速率的部分丢弃；全局域名限速、精确域名限速、泛域名限速，限制其 DNS 查询速率，超过速率的部分丢弃
地址分组	支持对地址池进行分组，方便根据使用目的不同进行地址池归类管理支持对地址池进行分组，方便根据使用目的不同进行地址池归类管理，支持手动创建分组和基于自定义属性自动分组两种方式
高可用	设备支持 IPv6 DHCP Failover 技术，提供 DHCP 服务异地备灾的功能，当一台异常时另外一台支持一键接管全部租赁服务，支持调整 MCLT 和负载比例
地址模板	支持 DHCP 模板，可根据模板批量生成地址池，模板可指定地址池起止地址，可按规则指定网关；
地址管理	支持进行网络的缩放、拆分、合并

三重绑定	支持 IP、MAC、交换机端口的三重绑定，支持绑定违规发现和提示
设备联动	支持与主流网络设备联动，通过配置脚本模板的方式，实现对终端的一键绑定、一键阻断；提供相关产品功能截图
僵尸地址	对自定义设定时间内未上线的地址进行僵尸地址类型标记，并可以产生告警。可界面指定此类地址自动回收容忍时间。实现 IP 地址动态管理需要
报表	支持自定义报表定制，自定义报表分析类型包括但不限于 TOP 总量、TOP 百分比、百分比及次数/秒；分析项目包括但不限于源 IP、源端口、查询区、查询记录类型、查询域名、应答状态、RD 位状态、请求签名、是否包含 EDNS、是否 TCP 请求、DO 位状态、CD 位状态、是否命中缓存、ISP、国家、省、市；匹配规则包括但不限于所有、等于、不等于、包含、不包含；需支持统计项目内的二层分析；数据统计分析需支持省、国家地理位置的数据统计，且统计报告支持定时自动生成及定时邮件推送功能
统一管理	（1）支持多节点统一管理。（2）支持不同用户组统一的分权管理。（3）支持 HA 模式主备管理
全局搜索	支持通过全局搜索自定义属性值的方式筛选所有视图中的权威资源记录，搜索方式包括：等于、不等于、包含、以...开头、以...结尾 几种方式，搜索结果可以全选编辑解析结果、TTL、属性值等，并且支持以 csv 格式导出搜索结果（结果中包含自定义列和内容）
告警	可以设置各种阀值、事件告警，支持邮件告警、回调告警、SNMP 告警、syslog 告警、短信告警及声音告警。告警记录内容包括但不限于告警时间，节点名称及 IP、告警事件原因
IPV4/IPV6 双栈支持	系统支持 IPV4 及 IPV6 数据中心调度策略
AAAA 记录控制	支持 AAAA 应答控制，在解析结果同时存在 A 与 AAAA 记录时，针对部分 AAAA 记录进行过滤，支持 A、AAAA 记录同 PTR 的操作联动

2.23 系统集成

指标项	**技术要求**
系统集成	1、完成所有硬件设备的安装与调试，完成所有软件产品部署、联调等工作，应可根据用户要求进行定制。在项目集成和实施过程中需保证不影响现有系统的稳定运行。 2、需根据公安部建设要求，充分考虑、设计并提供安全保障系统日常管理运维所需的整体技术保障软硬件环境。 3、在项目实施过程中，应同步考虑并提供系统整体部署上线所需的数据库及中间件等，需提供项目实施所需（不限于）六类网线、光纤线以及系统搭建所需各类辅助材料。

	4、应全面适配并兼容新一代公安信息网基于国产化环境的服务器或虚拟化平台。 5、本项目采集的日志要满足部局规范、满足用户提出的采集规范，按要求上传至日志审计平台。

三、进度要求

（一）交货

合同签订后，1 个月内全部设备到货，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，中标方需提供合法获得该项目采购的所有设备（含配件）的相关证明（例如: 设备制造商对订购设备提供的产品序列号等有效证明材料）。

3、中标方在交货的同时提供关于项目详细设计方案、设备安装调试方案、应急方案、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

合同签订后，3 个月内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符合部局规范及技术要求。

（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

合同签订后，4 个月内完成全部建设内容并通过验收，要求:

1、验收形式由用户指定，中标方需配合验收相关工作。

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。中标方应对每个设备及整体系统进行完善的测试（包括系统功能测试和性能测试）和自验收，提供测试文档和自验收文档。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，资料要提交完整的四套，以作设备留档备案。

3、中标方应当配合第三方测评单位开展安全测评，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。

四、工程技术服务需求

（一）中标方需提供成功实施其技术方案所需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，并需提交详细的工程服务方案。

（二）中标方应接受用户方的统一管理。用户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。

（三）本项目系统集成质量控制和文档需满足国家标准要求。

（四）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。

（五）中标方建设期间需提交项目人员参与清单。项目建设期间，项目负责人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。

（六）本项目系统建设应符合等级保护三级安全性评估的要求。

（七）设备安装和调试

1、软硬件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。

2、在设备安装调试时，如涉及到现有软硬件设备地理位置调整的（具体位置由用户方指定），中标方需负责设备下架、地理位置调整和安装等工作。

3、软硬件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。

4、中标方安装前负责提供下列详细资料:

设备机架（柜）布局、进出线方式；设备所需电源种类、功耗、电压、地线要求；设备安装方式和抗震措施；设备及线缆等的维护标识方式；上述资料需提供电子文档。

（八）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。

五、投标材料要求

（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，需保证系统符合部局规范及技术要求。

（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。

（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）投标方需提供合法获得投标产品的相关证明，由原厂商提供质保期内服务。

（五）本项目不接受联合投标，投标方不得分包、转包。

（六）投标单位具备专业工程师服务团队（附名单简介及社保缴纳证明材料）。投标人需提供专业的项目实施团队，项目经理 1 名，具备信息系统项目管理师证书，且有相关项目经验；现场工程师不少于 3 名，具备相应能力，提供相关证书等。

六、报价要求

（一）投标方应提供详细的报价，包括软硬件设备费用及系统集成费用。投标方应提供详细的报价清单，包括：每个项目的名称、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。

（二）投标方应详细说明集成费等费用的组成、比例和计取方法。

（三）投标方报价应为含税价。

七、运维及售后服务要求

（一）系统及设备的保修、维护期应从本项目验收通过之日起计算。

（二）要求投标方免费提供本项目采购的所有设备 3 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）。

（三）要求投标方提供 3 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（驻场地点由用户方指定，至少 7*8 小时驻场服务，节假日或重大活动保障期间应根据用户的要求，提供驻场保障），提供驻场工程师的工作简历（附名单简介及社保缴纳证明材料），并得到最终用户的确认。中标方如需更换驻场工程师需事先与最终用户协商确定。

免费维护期内，投标方需提供每周 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。

免费维护期内，投标方需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）故障设备维修无法在 24 小时内恢复的，需提供同型号的备件顶替，不得影响系统的正常运行。

（五）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，需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需交由用户方保管。

（六）若用户在免费质保期内对软硬件环境进行调整，中标方应免费完成相关集成工作，包括但不限于将硬件设备及应用软件部署至不同公安业务网络等。

（七）免费维护期间，投标方需承诺提供巡检服务，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。中标方应在用户方指定的重大节点前对系统全面巡检，提供应急方案等。

（八）按照 GB/T 22239《信息安全技术 网络安全等级保护基本要求》，在三年质保期内，中标方每年度应聘请第三方具有资质的测评机构，对本次项目升级改造涉及的全国公安大数据智能化建设应用基础环境整体项目部分按照等保三级要求进行等保测评，提供测评报告，并对相关问题开展即时整改。

投标人具备CCRC信息系统安全集成服务资质认证证书的予以优先考虑。