浦东300号集中办公点信息系统（2025年升级改造）项目

采购需求

# 项目概况

浦东300号上海市政府浦东集中办公点位于上海市浦东世博园区世博村路、雪野路、沂南路和华丰路之间，共由7幢高层建筑（1-7号楼）和综合楼（8号楼）组成。园区入驻委办局包括上海市知识产权局、上海市交通委员会、上海市人力资源和社会保障局、上海市审计局、上海市卫生健康委员会、上海市经济和信息化委员会、上海市机管事务管理局、上海市房屋管理局、上海市民政局、上海市民族和宗教事务局、上海市商务委员会、上海市人民政府合作交流办公室、上海市生态环境局、上海市疾病预防控制局等多家委办局单位并对外提供市民办事公共服务功能。

浦东300号集中办公点信息系统网络为双链路方式。按照分区进行管理，整体分为互联网统一出口区、政务外网统一出口区、网络管理区、公共服务区、委办接入区、IDC区、DC区7个区域。自2013年使用以来已有11年多的时间，部分网络安全设备陆续开始出现故障，虽然对其及时进行了维修与保养，但是因配件过时及故障率等原因，若长此以往可能会造成用户体验度下降、整体系统故障等情况。

近年来的等保三级测评对安全设备不能满足现有等保要求提出了整改要求，包括信息系统各区域边界防火墙、IDC防火墙、安全审计产品、安全管理平台等。

综上，信息系统运行至今，已有相当数量的安全设备严重老化，功能、性能不能满足安全需要，且部分设备不能完全符合国家、上海市关于安全等保、信创的管理和技术要求，存在较大的安全隐患，急需进行升级改造，提升现有系统的安全性、稳定性和合规性。

本项目是对园区UPS电池升级改造、机房安全设备升级改造、信息系统安全管理升级改造进行升级改造，旨在采用性价比最高的方案确保网络状态及机房电力供应安全可靠，解决目前300号集中办公点由于部分设备老化，导致的设备性能下降、问题频出、安全风险增加等问题，用以保障整个集中办公点信息系统网络安全稳定运行。通过本项目建设，重点拟实现以下三个建设目标：

一是解决目前存在的设备问题，支撑信息系统安全稳定运行。

二是提升关键核心设备的性能，符合信息系统等保三级要求。

三是适应现代信息技术的趋势，满足信息系统合规可用要求。

建设期限：自合同签订之日起12个月内完成项目建设和验收工作。

建设地点：上海市

预算金额：5397859元（2025年预算4315859元）

采购金额（最高限价）：5397859元

组织形式：集中采购

采购方式：公开招标

是否接受联合体投标：否

是否按信创要求建设：是

运维后所属大系统：集中办公点信息化基础设施

# 建设目标

**2.1、建设目标**

根据国家及上海市推动网络安全和信息化工作的要求，按照系统安全管理、信息系统信创改造等工作要求，对浦东300号集中办公点的UPS电池、网络安全设备、信息系统网络和安全管理系统进行升级改造，确保浦东300号网络状态及机房电力供应安全可靠，为浦东300号内各信息系统提供安全稳定的系统运行环境。

对UPS电池、网络安全设备、信息系统网络和安全管理系统采用性价比最高的方案确保网络状态及机房电力供应安全可靠。

**2.2、项目规划指标参数**

本项目建设需满足以下指标：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 总体目标 | | 对浦东300号集中办公点的UPS电池、信息系统网络安全设备、信息系统安全管理系统进行升级改造，确保浦东300号网络状态及机房电力供应安全可靠，为浦东300号内各信息系统提供安全稳定的系统运行环境。 | | |
| 规划指标参数 | 一级指标 | 二级指标 | 三级指标 | 目标值 |
| 通用指标 | 产出质量 | 一次性验收合格率 | 100% |
| 系统可靠性 | ≥99.99% |
| 安全测试 | 通过 |
| 网络安全等级保护 | 等保三级 |
| 故障修复时间 | ≤1小时 |
| 安全事件 | 数据安全事件发生次数 | 0次 |
| 时效指标 | 项目建设周期 | 12个月 |
| 业务指标 | 产出数量 | UPS采购数量（节） | 308 |
| 防火墙设备采购数量（台） | 34 |
| 审计设备采购数量（台） | 1 |
| 信息安全管理系统采购数量（台） | 2 |
| 服务器采购数量（台） | 1 |
| 产出质量 | 防护墙整体吞吐量 | ≥10Gbps |
| 网络与安全设备的日志留存保留时间 | ≥6个月 |
| 支撑日志审计整体授权许可量（个） | ≥150 |
| 支撑日志审计存储量（TB） | ≥4 |
| 产出效益 | 支撑浦东300号集中办公点政务外网正常运行时间（天） | 365 |
| 提供流量采集分析的委办单位数量（个） | 14 |
| 提供网络安全防护服务的委办单位数量（个） | 14 |

# 项目建设内容

## 技术路线需求

具体技术路线需求如下：

本次需针对浦东300号集中办公点的UPS电池、网络安全设备、信息系统网络和安全管理系统进行升级改造。

其中，UPS电池部分需替换符合目前UPS系统匹配共计308节电池及配套配件等，并按采购方要求对更换后的旧设备进行堆放处置。网络安全设备，需升级改造各边界、区域防火墙共计34台以及日志审计1台。信息系统网络和安全管理部分需升级改造1台安全管理中心，1台流量采集主机和1台冗余服务器。

## 硬件购置清单

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品大类 | 产品小类 | 产品配置 | 保修年限 | 数量 | 备注 |
| 1 | 动力设备 | UPS电池 | 电池：12V 100AH | 1 | 60 | / |
| 2 | 动力设备 | UPS电池 | 连接线及配套：50mm²BV线 | 1 | 1 | 序号1的设备配套 |
| 3 | 动力设备 | UPS电池 | 电池：12V 200AH | 1 | 208 | / |
| 4 | 动力设备 | UPS电池 | 电池：12V 24AH | 1 | 40 | / |
| 5 | 动力设备 | UPS电池 | 连接线及配套：50mm²BV线 | 1 | 1 | 序号3和序号4的设备配套 |

## 安全产品购置清单

| 序号 | 产品大类 | 产品小类 | 产品配置 | 保修年限 | 数量 |
| --- | --- | --- | --- | --- | --- |
| 1 | 边界安全 | 防火墙A | 信创防火墙：三年入侵防护，云威胁软件更新。 性能参数：网络层吞吐量：10G，应用层吞吐量：4G，防病毒吞吐量：1G，IPS吞吐量：1G，全威胁吞吐量：800M，并发连接数：400万，HTTP新建连接数：10万。 硬件参数：规格：1U，内存大小：8G，硬盘容量：128G SSD，电源：单电源，接口：6千兆电口。 | 1 | 2 |
| 2 | 边界安全 | 防火墙B | 信创防火墙：网络层吞吐量：10G，应用层吞吐量：4G，防病毒吞吐量：1G，IPS吞吐量：1G，全威胁吞吐量：800M，并发连接数：400万，HTTP新建连接数：10万。 硬件参数：规格：1U，内存大小：8G，硬盘容量：128G SSD，电源：单电源，接口：6千兆电口。包含：三年入侵防御规则库更新。 | 1 | 2 |
| 3 | 边界安全 | 防火墙C | 信创防火墙：网络层吞吐量：10G，应用层吞吐量：4G，防病毒吞吐量：1G，IPS吞吐量：1G，全威胁吞吐量：800M，并发连接数：400万，HTTP新建连接数：10万。 硬件参数：规格：1U，内存大小：8G，硬盘容量：128G SSD，电源：单电源，接口：6千兆电口。包含：三年入侵防御规则库更新。 | 1 | 2 |
| 4 | 边界安全 | 防火墙D | 信创防火墙：接口：6千兆电口+4万兆光口。 网络层吞吐量：10G，应用层吞吐量：4G，防病毒吞吐量：1G，IPS吞吐量：1G。 含防病毒功能，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；支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略。 含云查功能，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。 包含：三年入侵防御规则库、防病毒规则库更新、云威胁软件更新。 | 1 | 20 |
| 5 | 边界安全 | 防火墙E | 信创防火墙：网络层吞吐量：4G，应用层吞吐量：2G，防病毒吞吐量：600M，IPS吞吐量：600M，全威胁吞吐量：400M，并发连接数：200W，HTTP新建连接数：4.5W。 硬件参数：规格：1U，内存大小：8G，硬盘容量：128G SSD，电源：单电源，接口：6千兆电口。包含：三年入侵防护，网关杀毒，云威胁软件更新。 | 1 | 8 |
| 6 | 安全管理与支持 | 安全审计产品 | 信创产品：包含主机审计许可证书数量：150，可用存储量：4TB（RAID0 模式），平均每秒处理日志数（eps）最大性能：2500。 硬件参数：规格：2U，内存大小：16G，硬盘容量：128G SSD+4T SATA，电源：冗余电源，接口：6千兆电口+2万兆光口SFP+。包含：三年软硬件质保服务。 | 1 | 1 |
| 7 | 其他安全产品 | 流量采集主机 | 流量采集主机：冗余双电源，整机IO性能320Gbps，最大支持16\*千兆电、16\*SFP+、 1\* QSFP、1\*QSFP28；支持MATRIX-SDN 控制器统一管理；接受 MATRIX-SDN-CENT 平台统一管控策略实现流量的输入、分类识别输出、负载均衡输出；支持基于IP五元组分流，支持vlan标签，支持过滤、切片、打纳秒级时间戳，支持隧道封装剥离，支持协议识别，支持基于端口流量标识分流，支持基于协议头关键标记的流量标识策略分流等功能；包括安装调试服务，硬件设备保修/更换服务（含备件先行服务），管理软件升级服务，软硬件故障定位和故障排查服务，模块满配 设备出厂已包括3年免费硬件设备保修/更换服务（含备件先行服务），管理软件升级服务，软硬件故障定位和故障排查服务， | 1 | 1 |
| 8 | 安全管理与支持 | 安全管理平台产品 | 信创产品：部署一套安全管理中心，接入探针流量进行分析，实现深度监测与联动闭环；管理各安全设备，通过实时监控发现并立即处置安全设备的紧急状况。安全管理中心包括态势感知、威胁情报共享、通报预警、安全管理等系统。性能参数：存储容量：36T，在带宽性能1Gbps时存储时长：1800天/1Gbps。 硬件参数：规格：2U，内存：8\*32GB DDR4 3200，系统盘：1\*240GB SATA SSD，缓存盘：无缓存盘，数据盘：12\*4TB，标配盘位数：12，电源：白金，冗余电源，接口：4千兆电口+2万兆光口。 | 1 | 1 |
| 9 | 其他安全产品 | 服务器 | 冗余服务器：信创服务器机架式2U、处理器32核 、国产操作系统 内存:32G\*16 、Raid卡、硬盘:960G\*2+12T\*10 用于支持安全管理中心，提升整体信息系统性能、可以提升系统的整体处理能力，改善用户体验 | 1 | 1 |

## 实施要求

1）本次项目实施过程应满足上海市大数据中心对设备配置、施工规范、集成文档、施工人员管理等要求。

2）供应商应提供针对本项目的测试方案。测试方案内容包括但不限于测试拓扑、测试设备要求、软件版本信息、测试用例、测试周期等。测试共分为离线测试部分和在线联网测试部分，其中针对在线联网测试部分需额外提供风险评估和应急预案。在实际测试过程中，涉及的所有仪器、仪表设备均由成交供应商提供。测试报告需由成交供应商和设备原厂共同盖章确认。

3）供应商应提供针对本项目的实施方案。具体内容包括但不限于网络拓扑、网络和安全协议、网络和安全配置、网络冗余方式、网络诊断方案、安全事件发现、诊断、处理及验证方案等。

4）成交供应商负责本次采购设备的到货免费安装，包括并不仅限于上架、上电、设备侧线缆等辅材、电源插头改造等工程等（工程所产生的相关线缆、电源插头等耗材由成交供应商免费提供）。

5）供应商应提供针对本项目的联调方案。须落实本次采购采购设备与现有相关网络设备、安全设备和支撑系统的联调工作，内容包括但不限于网络实施、测试验证等工作。

6）供应商必须依据采购要求，结合采购人的需求，提供相关产品的扩容、更新或替代方案。成交供应商应对采购人的现有网络情况，包括但不仅限于功能和性能进行充分分析，并提出可兼容现有网络功能和性能，同时满足此次扩容要求的完整的解决方案。

7）供应商应提供针对本项目的迁移方案。内容包括但不限于网络拓扑、施工材料、迁移实施步骤、网络和安全配置、线路切换、应急演练、验证方式、迁移时间、回退方案和保障计划等。如迁移方案中涉及本次采购之外的物资采购（例如光模块等）均由成交供应商免费提供。

8）成交供应商负责根据迁移方案完成业务的迁移工作，迁移工作成功率须为100%（包含因不可预见的情况而导致的迁移回退，迁移回退必须在申请的割接窗口时间内完成），如发生迁移回退的，须在当日向采购人提供盖章的回退报告，内容包括但不限于具体回退原因和对应的解决方案。

9）成交供应商负责在每次业务迁移完成后，安排各相关设备原厂至少1名资深技术人员现场保障48个小时。保障人员在接到采购人的报修通知后须做到5分钟内响应、15分钟内恢复运营，并于当日向采购人提供盖章的故障报告，内容包括但不限于具体故障原因和对应的解决方案。

10)成交供应商负责提供并收集本次采购范围内设备应纳入采购人指定网管平台、安管平台和展示所需的SNMP MIB、日志解析文档、日志样本、配置命令集、接口文档等材料，并协助对本次采购范围内设备的SNMP MIB、日志样本、配置命令集、接口进行解析和适配（如产生相关费用由成交供应商免费提供）。

11)成交供应商负责根据采购人的要求提供项目实施日报和周报，内容包括但不限于当日/当周已完成工作内容、下一步计划、遗留问题/困难等。

12)成交供应商负责根据采购人对于资源管理的要求完成相关资源管理文档的编制，内容包括但不限于设备安装位置、设备面板图、设备槽位图、设备连线关系等。

13)成交供应商负责在项目到货之日起至项目终验完成前，应根据采购人要求，提供基于本次采购的安全设备等的各类安全分析报告，包括但不仅限于设备运行日志分析、用户风险分析和安全评估分析及对应的整改建议方案，并负责根据采购人要求完成整改工作。

14）在实施前须做好设备材料及备品备件准备工作，并做好演练及应急预案。在实施过程中，应充分考虑与原系统的联动，不得影响业务设备的正常运行。在实施过程中及质保期间如果发现其他故障及问题，成交供应商须免费提供原厂配件一并解决。

## 技术参数

### 动力设备-UPS电池

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| 额定容量 | 12V24Ah/12V100Ah/12V200Ah |
| 组件结构 | 蓄电池应由正极板、负极板、隔板、槽、盖、安全阀、回流条、端子、电解液等组成。蓄电池结构应保证在使用寿命期间，不得渗漏电解液 |
| 配件要求 | 蓄电池间接线板、终端接头应选择导电性能优良的材料，并具有防腐蚀措施。蓄电池槽、盖、安全阀、极柱封口剂等材料应具有阻燃性。 |
| 密封要求 | 蓄电池必须采用全密封防泄漏结构，外壳无异常变形、裂纹及污迹，上盖及端子无损伤，正常工作时无酸雾溢出。 |
| 使用寿命 | 蓄电池在环境温度20～25℃时的浮充运行寿命应不低于10年。 |
| 安全阀性能 | 蓄电池使用期间安全阀应能自动开启闭合，闭阀压力应在10-30kPa范围内，开阀压力应在10-35kPa范围内。 |
| 其他要求 | 蓄电池除安全阀外，应能承受50kPa的正压或负压而不破裂、不开胶，压力释放后壳体无残余变形。 |
| 静置28天后，容量不低于98%。 |
| 蓄电池正负极性及端子应有明显标志，蓄电池极性应与极性标志一直。正极板厚度应与使用寿命相适应。 |
| 两个蓄电池之间连接条的压降，5.5I10时不超过5mV。提供第三方报告。 |
| 蓄电池需具有较强的耐过充能力。以0.3I10电流连续充电160h后，外观应无明显变形及渗液。 |
| 电池进行10h率容量试验，实际容量的最大值和最小值的差值应不大于2％。 |
| 密封反应效率＞98％。 |
| 蓄电池在-30℃和65℃温度范围内时，封口剂应无裂纹和溢流，密封性应符合规定要求。 |
| 蓄电池在充电过程中，蓄电池外部遇明火时，不应内部爆炸。 |

### 边界安全-防火墙A

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| 硬件要求 | 硬件参数：产品不少于6个千兆电口。内存≥8G，硬盘容量≥128G SSD。 |
| 性能要求 | 网络层吞吐量≥10 Gbps，应用层吞吐量≥4 Gbps，并发连接数≥400万，每秒新建连接数≥10万。 |
| 授权模块 | 提供入侵防御能力、云威胁情报网关能力模块 |
| 服务要求 | 提供三年规则库更新和三年软硬件质保服务。 |
| 硬件平台 | 产品应用多核并行处理架构，并采用国产处理器和国产操作系统。 |
| 链路状态探测 | 产品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。 |
| 路由功能 | 产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。 |
| 地址转换 | 产品支持多种地址转换功能，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持IPv4／IPv6下地址转换，至少包括NAT64和NAT46两种方式。 |
| 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 安全防护 | 产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持超过7200种特征规则数量。 |
| 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀。 |
| 产品支持勒索病毒检测与防御功能（需提供产品功能截图证明）。 |
| 产品支持对多重压缩文件的病毒检测能力，支持不小于15层压缩文件病毒检测与处置。 |
| 产品具备Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为。 |
| 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。 |
| 产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。（需提供产品功能截图证明） |
| 对象识别 | 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 |
| 云威胁情报网关 | ▲1产品支持云威胁情报网关技术，通过全球超过30+pop节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品功能截图证明、提供POP节点在线查询链接并） |
| 安全策略管理 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 |
| 用户管理 | 产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。 |

### 边界安全-防火墙B

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| 硬件要求 | 硬件参数：产品不少于6个千兆电口。内存≥8G，硬盘容量≥128G SSD。 |
| 性能要求 | 网络层吞吐量≥10 Gbps，应用层吞吐量≥4Gbps，并发连接数≥400万，每秒新建连接数≥10万。 |
| 授权模块 | 提供入侵防御能力模块。 |
| 服务要求 | 提供三年规则库更新和三年软硬件质保服务。 |
| 硬件平台 | 产品应用多核并行处理架构，并采用国产处理器和国产操作系统。 |
| 链路状态探测 | 产品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。 |
| 路由功能 | 产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。 |
| 地址转换 | 产品支持多种地址转换功能，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持IPv4／IPv6下地址转换，至少包括NAT64和NAT46两种方式。 |
| 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 安全防护 | 产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持超过7200种特征规则数量。 |
| 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀。 |
| ▲2产品支持勒索病毒检测与防御功能（需提供产品功能截图证明）。 |
| 产品支持对多重压缩文件的病毒检测能力，支持不小于15层压缩文件病毒检测与处置。 |
| 产品具备Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为。 |
| 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。 |
| 产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。（需提供产品功能截图证明） |
| 对象识别 | 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 |
| 安全策略管理 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 |
| 用户管理 | 产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。 |

### 边界安全-防火墙C

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| 硬件要求 | 硬件参数：产品不少于6个千兆电口。内存≥8 G，硬盘容量≥128G SSD。 |
| 性能要求 | 网络层吞吐量≥10 Gbps，应用层吞吐量≥4 Gbps，并发连接数≥400万，每秒新建连接数≥10万。 |
| 授权模块 | 提供入侵防御能力模块。 |
| 服务要求 | 提供三年规则库更新和三年软硬件质保服务。 |
| 硬件平台 | 产品应用多核并行处理架构，并采用国产处理器和国产操作系统。 |
| 链路状态探测 | 产品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。 |
| 路由功能 | 产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。 |
| 地址转换 | 产品支持多种地址转换功能，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持IPv4／IPv6下地址转换，至少包括NAT64和NAT46两种方式。 |
| 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 安全防护 | 产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持超过7200种特征规则数量。 |
| 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀。 |
| 产品支持勒索病毒检测与防御功能（需提供产品功能截图证明）。 |
| 产品支持对多重压缩文件的病毒检测能力，支持不小于15层压缩文件病毒检测与处置。 |
| 产品具备Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为。 |
| ▲3产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。需提供相关证明。 |
| 产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。（需提供产品功能截图证明） |
| 对象识别 | 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 |
| 安全策略管理 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 |
| 用户管理 | 产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。 |

### 边界安全-防火墙D

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| 硬件要求 | 硬件参数：产品不少于6个千兆电口，4个万兆光口。内存≥8 G，硬盘容量≥128G SSD。 |
| 性能要求 | 网络层吞吐量≥10 Gbps，应用层吞吐量≥4 Gbps，并发连接数≥400万，每秒新建连接数≥10万。 |
| 授权模块 | 提供入侵防御、网关杀毒能力模块。 |
| 服务要求 | 提供三年规则库更新和三年软硬件质保服务。 |
| 硬件平台 | 产品应用多核并行处理架构，并采用国产处理器和国产操作系统。 |
| 链路状态探测 | 产品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。 |
| 路由功能 | 产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。 |
| 地址转换 | 产品支持多种地址转换功能，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持IPv4／IPv6下地址转换，至少包括NAT64和NAT46两种方式。 |
| 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 安全防护 | 产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持超过7200种特征规则数量。 |
| 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀。 |
| 产品支持勒索病毒检测与防御功能（需提供产品功能截图证明）。 |
| 产品支持对多重压缩文件的病毒检测能力，支持不小于15层压缩文件病毒检测与处置。 |
| 产品具备Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为。 |
| 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。需提供相关证明。 |
| 产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。（需提供产品功能截图证明） |
| 对象识别 | 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 |
| 安全策略管理 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 |
| 用户管理 | 产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。 |

### 边界安全-防火墙E

|  |  |
| --- | --- |
| **功能项** | **功能要求说明** |
| 硬件要求 | 硬件参数：产品不少于6个千兆电口。内存≥8 G，硬盘容量≥128G SSD。 |
| 性能要求 | 网络层吞吐量≥4 Gbps，应用层吞吐量≥2 Gbps，并发连接数≥200万，每秒新建连接数≥4.5万。 |
| 授权模块 | 提供入侵防御能力、网关杀毒能力、云威胁情报网关能力模块。 |
| 服务要求 | 提供三年规则库更新和三年软硬件质保服务。 |
| 硬件平台 | 产品应用多核并行处理架构，并采用国产处理器和国产操作系统。 |
| 链路状态探测 | 产品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。 |
| 路由功能 | 产品支持静态路由、策略路由和多播路由协议，并支持BGP、RIP、OSPF等动态路由协议。 |
| 地址转换 | 产品支持多种地址转换功能，支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT，支持IPv4／IPv6下地址转换，至少包括NAT64和NAT46两种方式。 |
| 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 安全防护 | 产品具备入侵防御检测引擎，支持对各类漏洞利用攻击进行检测与防护，产品支持超过7200种特征规则数量。 |
| 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持杀毒白名单设置，可以例外排除特定MD5和URL的病毒文件，针对特定文件不进行查杀。 |
| 产品支持勒索病毒检测与防御功能（需提供产品功能截图证明）。 |
| 产品支持对多重压缩文件的病毒检测能力，支持不小于15层压缩文件病毒检测与处置。 |
| 产品具备Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为。 |
| 产品支持Cookie攻击防护功能，并通过日志记录Cookie被篡改。需提供相关证明。 |
| 产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁。（需提供产品功能截图证明） |
| 对象识别 | 产品支持服务器自动侦测功能，采用双向流量检测技术识别网络中的服务器对象。 |
| 云威胁情报网关 | 产品支持云威胁情报网关技术，通过全球超过30+pop节点，实现对威胁流量就近进行实时检测&拦截，实现失陷外联实时阻断，保护资产安全。（需提供产品功能截图证明、提供POP节点在线查询链接） |
| 安全策略管理 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。 |
| 用户管理 | 产品支持三权分立功能，根据用户权限可设置为安全管理员、审计员和系统管理员三种角色。 |

### 安全审计产品

|  |  |
| --- | --- |
| 功能项 | 功能要求说明 |
| 硬件要求 | 不少于6个千兆电口，2个万兆光口，2U机箱，内存≥16G，硬盘容量≥128G SSD+4TB SATA。 |
| 性能要求 | 可用存储量≥4TB，平均每秒处理日志数（eps)最大性能≥2500。默认包含主机审计许可证书数量≥150 |
| 服务要求 | 提供三年软硬件质保服务。 |
| 日志采集 | 支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka等多种方式完成日志收集； |
| 支持接入TLS加密方式的日志，支持对日志传输状态、最近同步时间进行监控，可统计每个日志源的今日传输量和传输总量。（需提供截图证明） |
| 日志标准化 | 支持通过正则、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。 |
| 日志过滤 | 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。 |
| 日志转发 | 支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志。 |
| 日志存储 | 支持日志文件备份到外置存储节点，支持ISCSI存储方式，并可查看外置存储容量、状态等信息。支持以FTP方式将日志数据备份至外部存储空间，支持备份数据的恢复和查询；（需提供截图证明） |
| 全文检索 | ▲4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；（需提供截图证明） |
| 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； |
| 日志分析 | 支持自定义审计规则与关联规则，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。 |
| 日志告警 | 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。 |
| 系统管理 | 提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持IP免登录，指定IP免认证直接进入平台；支持只允许某些IP登录平台；支持页面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持usb-key认证。 |
| 支持POC测试工具一键生成日志数据。 |

### 流量采集主机

| 功能项 | 功能要求说明 |
| --- | --- |
| 硬件规格 | 网络接口：至少16\*RJ45千兆电接口、16\*SFP+插槽、1\*QSFP28插槽、1\*QSFP插槽；支持单、多模光纤；整机规格：1U机箱 电源:双电源设备质保：3年质保 |
| 性能要求 | 整机IO性能吞吐量要求在310Gbps及以上。 |
| 硬件架构 | 设备的中央处理器（CPU）、交换芯片、接口扩展芯片（如有）、操作系统须全部为国产。  提供设备cpu、交换芯片、接口扩展芯片（如有）的拆机核验照片，体现元器件的厂商、型号。  需提供相关证明。 |
| 组网能力 | 设备支持基于Openflow/Netconf协议的控制面接口与流量数据集中采集管控平台通信，具备SDN组网能力。 |
| 设备应支持基于LLDP机制的设备邻居发现。 |
| 设备可支持多互连端口组成链路聚合组，增长互连传输带宽，且所生成的链路聚合组可支持双向数据传输。 |
| 设备支持基于SDN架构的流量数据管理平台集中管理与调度。 |
| 基础流量转发功能 | 支持流量复制/汇聚/分流功能，支持一对多，多对一，多对多的流量复制汇聚功能。 |
| 支持聚合策略功能，单条聚合策略可包含多条规则，并可根据需求快速添加批量规则。（需提供截图证明） |
| 在定义流量分发策略时，可根据需求选择“途经点接口”，以实现对流量数据的灵活调度与处理。（需提供截图证明） |
| ▲5支持按策略名称、输入接口、输出接口、途经点、ACL类型、规则使能状态、以及基于五元组信息快速检索策略条目。可对策略条目状态进行一键切换，即ON或OFF，实现对应策略条目的一键启用或停用。（需提供截图证明） |
| 支持基于五元组、以太网类型字段、VLAN ID、VNI、TCP Flag、DSCP等参数或多个参数组合定义过滤条件，同时支持报文过滤方向的灵活选择，即可以选择报文输入方向、报文输出方向进行筛选与过滤。 |
| 支持根据报文的内层、外层字段信息灵活定义哈希分流策略选项，如支持基于L2的src.mac、dst.mac、vlanid、ethertype；支持基于L3的protocol；支持基于L4的src.port、dst.port；支持基于IPv4的src.ip、dst.ip；支持基于IPv6的src.ip、dst.ip； |
| 支持报文vlan tag的添加、删除、修改。 |
| 设备支持接口组的配置与引用功能，包含但不限于组播组、负载均衡组、接口热备组及输入接口组，以提高接口引用配置效率。（需提供截图证明） |
| 设备支持隧道封装剥离功能，支持对VxLAN、MPLS、NVGRE等隧道协议类型的解封装。 |
| 设备支持隧道内层、外层数据的匹配能力，可根据需要快速切换端口的内层或外层匹配方式。 |
| 支持 IP 隧道终结，能够充当用于 IP 隧道协议封装流量的远程镜像目标，接收隧道流量，并结合汇聚、复制、负载均衡功能，将流量输出至监测和安全工具；每个端口均能够单独配置 IP 地址用于 IP 隧道终结，单端口不少于 16 个。 |
| 设备支持对任意多个接口的统计信息进行累加与计数对比的功能。（需提供截图证明） |
| 支持数据包在入端口根据业务重要程度定义优先级，对于高优先级报文在输出时优先被转发。（需提供截图证明） |
| 设备支持镜像配置功能，即可以把设备收到的流量数据通过ERSPAN隧道封装的方式传输至远端设备，支持源/目的IP地址的配置。（需提供截图证明） |
| 流量可视化 | 提供策略执行状态可视化监控能力，每条策略可通过不同的颜色表示策略的下发状态，如策略下发成功或下发失败，且可用图形的方式分别展示每条策略的流量趋势及策略关联的设备接口等信息。（需提供截图证明） |
| 支持对任意输入接口的当前或历史统计信息进行图形化展示，至少包含接收字节数、接收包数、接收错误包数、输出字节数、输出包数、输出错误包数、包长分布、包类型统计、接口流量趋势，以及当前接口命中策略实时流量趋势图形化展示。（需提供截图证明） |
| 支持对任意输出接口的当前或历史统计信息进行图形化展示，至少包含接收字节数、接收包数、接收错误包数、输出字节数、输出包数、输出错误包数、包长分布、包类型统计、接口流量趋势，以及当前接口命中策略实时流量趋势图形化展示。（需提供截图证明） |
| 系统管理 | 设备支持系统信息展示功能，支持设备温度、风扇转速、CPU使用率、内存使用率、系统时间、运行时间、软件版本信息等设备运行状态信息的展示。 |
| 设备支持预警管理功能，可针对流量阈值或设备健康度进行阈值的配置，可实现阈值小于、小于等于、大于、大于等于的条件设定；当超过阈值时可基于弹窗、语音、Http接口以及syslog等方式进行告警，同时针对告警事件触发流量快照。（需提供截图证明） |
| 设备支持LDAP、RADIUS、TACACS+远程接入认证能力。 |
| 支持基于角色的用户管理能力，不同的用户可归属于不同的用户组，不同的用户组具有不同的管理权限，可根据用户角色分配不同的功能模块管理能力。 |
| 支持基于NTP的时钟同步能力。 |
| 支持syslog本地、远程日志记录和syslog服务配置 |
| 支持基于流量数据集中管控平台进行设备升级；支持基于独立的FTP/TFTP方式升级 |

### 安全管理平台产品

|  |  |
| --- | --- |
| 功能项 | 功能要求说明 |
| 硬件与性能要求 | 存储容量≥36T；在带宽性能1Gbps时存储时长≥1800天/1Gbps；内存≥8\*32GB，硬盘≥12\*4TB，冗余电源，规格2U，不少于4个千兆电口、2个万兆光口。 |
| 服务要求 | 提供三年规则库更新和三年软硬件质保服务。 |
| 大屏可视化 | 支持安全态势的可视化呈现，帮助更直观的看清风险、看懂威胁，产品内置综合安全态势、物联网安全态势、分支安全态势、安全事件、通报预警态势、脆弱性态势、资产态势、全球网络攻击态势、资产监控、告警实时监控、设备运行态势、重大活动网络安全指挥调度大屏、正常外连监控等不少于17块大屏展示界面证明；支持大屏轮播及自定义大屏顺序设置和轮播间隔设置，方便结合自身业务需求进行个性化设置（需提供截图打印） |
| ATT&CK能力图谱可视化 | ▲6支持基于ATT&CK能力图谱将网络安全现状映射到模型的各个阶段，支持命中攻击技术统计展示，支持基于规则检测引擎、情报检测引擎、文件分析引擎、攻击行为分析引擎以及异常行为引擎查看攻击技术分布，支持针对具体攻击技术展示检测能力图谱以及受影响的风险资产。（需提供截图） |
| 资产识别 | 支持主机类资产识别，能够识别资产数据来源、IP地址、主机名、MAC地址、基线异常、操作系统、操作系统详请、主机类型、服务与端口、状态、责任人、EDR状态、标签、最近上线时间、所属资产组织、资产名称、应用、IP类型、识别方式、首次发现时间等。 |
| 支持跨三层取MAC地址，识别资产MAC地址，并能够解决不同资产IP冲突问题，以及DHCP场景IP变更的问题。 |
| 资产全生命周期管理 | 支持责任人管理功能，可对资产进行全生命周期管理，包括自动识别资产、入库审核、离线资产识别、自动识别资产图库、手动导入资产退库、自定义资产名称等。针对自动识别资产退库功能，可设置全局退库时间，数据更新时间。支持主机资产分级管理，责任人管理。 |
| 脆弱性风险 | 支持整体展示服务器脆弱性风险分析、热点漏洞情况、脆弱性风险详情（漏洞风险、配置风险、弱密码、web明文传输、可用性风险），支持第三方漏扫报告导入和解析，可按资产组分类上传，支持上传文件。 |
| 弱密码检测 | ▲7支持弱密码主动扫描，支持SMB、MySQL、Oracle、RDP、SSH、Redis、MongoDB、ElasticSearch、MSSQL等扫描协议，支持自定义扫描周期、发包频率、扫描时间段、扫描优先级、扫描对象等。弱密码检测规则支持高度自定义，包括规则名称、生效域名、规则配置、账号白名单、密码白名单、弱密码内容导入文件，其中规则配置至少支持密码长度、字符种类、字典序、密码与账号相同、web空密码等。 |
| 实体行为分析 | 支持EBA实体行为分析功能，通过对这些对象进行持续的行为分析和行为画像构建，识别服务器异常，包括DGA解析请求、外联C&C服务器、异常协议利用、下载可疑文件、异常横向访问等。（需提供截图打印） |
| 日志接入 | 支持对800+网络安全设备接入类型，接入方式支持文件、数据库、API、Syslog、FTP、Snmp trap、Kafka、WMI、webservice、winlogbeat等方式进日志行接入，并支持用户对日志进行自定义解析规则。 |
| 挖矿专项检测 | ▲8支持挖矿专项检测页面，帮助客户更好的应对日益严峻的挖矿风险，避免数据窃取和监管通报，支持基于规则的本地挖矿检测和基于主动探测技术的云端挖矿检测，以实现挖矿病毒的全面检测，支持挖矿实时检测播报本地和云端的挖矿检测分析结果，支持基于攻击阶段展示挖矿主机数量，便于掌握各阶段挖矿主机分布情况，支持以列表的形式展示挖矿事件，包括最近发生时间、威胁描述、威胁定性、挖矿阶段、威胁等级、受害者IP、攻击次数、威胁情报等信息（需提供截图证明） |
| 文件威胁分析 | 文件威胁分析支持平台内置的恶意脚本分析引擎、webshellkiller智能引擎、save智能分析引擎以及云端分析引擎组合进行综合研判，协议类型有HTTP、FTP、SMB、SMTP、POP3、IMAP多种类型，支持展示查杀数据统计、受害资产攻击数TOP5，支持以列表的形式展示文件威胁信息，包括最近发生时间、威胁描述、威胁定性、威胁类型、攻击阶段、受害者IP、攻击次数等信息。 |
| 威胁定性 | 支持威胁定性引擎以分析告警的上下文关联、时序关系、历史告警发生的频率规律性，结合威胁情报与安全专家经验对当前的安全告警进行目的性确认，从而确认安全告警的优先级顺序，支持基于人工渗透、程序自动化、业务相关风险、其它4个维度对告警进行分类，帮助安全人员快速定位高危告警并及时处置。 |
| 预警中心 | 支持向下级单位推送预警，支持自定义预警内容，包括：标题、预警类型、内容、添加附件等，推送方式支持平台推送、邮件和短信3种方式，下级平台可收到上级平台的预警信息。 |
| 实战攻防能力 | 具备实时告警分析能力，支持备战阶段的对外服务器外网暴露面分析、内网服务器暴露面分析；支持实战阶段的实时告警分析和攻击者分析，支持全过程可视溯源分析。 |
| 实时告警分析 | 实时检测到关注告警类型的威胁可以发出声音告警提醒用户。支持受害者IP/攻击者IP/代理服务器IP/威胁描述/威胁类型等维度自定义告警复制，支持基于威胁定性、重点关注资产以及威胁类型排行等维度对告警进行筛选。 |

### 服务器

|  |  |
| --- | --- |
| 功能指标 | 指标要求 |
| 设备规格 | 硬件设备采用国产机架式服务器，国产品牌，采用国产芯片，设备规格≥2U，适用于通用机房环境，支持标准机柜。免工具开箱和部件维护设计，安装维护简便，无需额外工具。 |
| CPU | 每节点配置≥2颗国产CPU；核数≥32核。 |
| 系统盘 | 每节点配置2块960G SATA SSD企业级硬盘，支持免工具热插拔维护。支持RAID1，可用于安装操作系统。 |
| 存储 | 整机支持≥12块3.5" SATA/SAS热插拔硬盘，支持服务器磁盘盘序查看、点亮磁盘灯灯等功能。本次每节点配置10块12TB 7.2K RPM SATA HDD 企业级机械硬盘。 |
| 内存插槽 | 支持RDIMM、LDIMM内存，单条最大64GB DDR4-3200MHz内存，可以支持扩展≥16 个内存插槽。 |
| 内存条 | 每节点配置16 根 32GB RECC DDR4 3200MHz内存条，支持内存ECC自动纠错机制。 |
| 阵列控制器（Raid卡） | 配置独立高性能磁盘阵列控制器，≥1张，8通道，12Gbps带宽，no Cache，x8 PCIe Gen 4.0，支持JBOD/ RAID0/RAID1/RAID10，支持SATA\SAS\NVME存储。 |
| 网络接口 | 配置4口千兆以太网卡和2 个10Gb 万兆光口，网卡芯片需要支持RSS和TSO，含满配原厂多模光模块。 |
| PCIe扩展 | 支持PCIE 4.0，PCI-E I/O插槽总数：≥3 |
| I/O 插槽 | 支持≥1个IPMI 2.0 RJ45管理口、4 个USB3.0接口、1 个VGA接口、1 个COM串口 |
| 电源及外设 | 配置高效能热插拔 1+1 冗余电源，可选直流方式电源；设备附带机架安装导轨。 |
| 风扇 | 配置冗余热插拔风扇（双转子），风扇数量≥4个，支持单风扇失效。 |
| 嵌入式管理 | 集成系统管理芯片，提供ikvm和KVM Over IP高级管理功能，本地固件更新、错误日志，提供系统状况的可视显示；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，包括远程开机、关机、重启、虚拟设备挂在等操作；可实现监控服务器内部主要部件的状态，包括CPU、内存、硬盘、风扇、电源等。 |
| BMC功能 | 标配BMC诊断模块，可实现对CPU/内存/硬盘/网卡/风扇/温度/电源等关键部件的故障诊断 |
| 售后维保服务 | 产品报警前置，支持设备故障快速定位，快速排障，支持及时更换配件和硬件设备。 |
| 提供三年免费整机硬件有限保修，原厂工程师上门服务。 |

# 其他工作要求

## 售后服务要求

本项目从系统验收通过之日起三年提供7\*24小时免费技术支持和售后服务，其中动力设备UPS电池免费维护期为1年，安全产品免费维护期为1年。

在质量保证期内，供应商将按照售后服务的承诺提供保修和运行维护服务，如果厂商对信息系统中软、硬件设备等产品中的部分保修期超过上述期限的，则按照厂商的规定进行免费保修。

在质量保证期内，供应商负责信息系统的运行维护工作，确保信息系统安全、稳定、可靠地运行。本项目涉及的运行维护工作范围为：本次招标的功能范围。

## 应急响应要求

供应商对系统故障应能够实时响应，若系统发生故障，接到通知后30分钟之内响应，专业工程师2小时内到达现场。特殊故障与客户沟通协商后，按照协商的方式制定解决方案并进行处理。

具体故障级别及对应的应急响应要求如下：

一级故障：在1小时内确诊，总故障解决时间不超过4小时。

二级故障：在2小时内确诊，并在4小时内由专家到达现场确诊并解决，总故障解决时间不超过8小时；

三、四级故障：在4小时内确诊故障，总故障解决时间不超过16小时。

## 培训要求

对系统使用单位提供业务操作培训，应提供详细培训方案。

1、在质量保证期内，提供2次与项目相关的必要培训。

2、供应商需要评估培训成果，培训应具有培训教材、培训环境和高水平的培训讲师。

3、供应商应提供一般用户的基础操作培训和部门信息管理员的日常应用维护的培训，确保用户对象能够掌握对应的操作技能。

## 验收要求

本项目按下述方式开展验收。

（1）验收分初验和终验。

（2）初验前，供应商须完成软硬件安装和信息系统的调试等，并对本项目进行功能和运行检测，确保所有模块能够正常运行且已达到本项目约定的各类标准要求。供应商应以书面形式向招标方递交初验通知书。招标方应当在接到通知后的5个工作日内确定初验的具体日期，由双方按照本项目的约定完成本项目的初验。招标方有权委托第三方检测机构进行验收，对此供应商应当配合。

（3）初验时，供应商须提供文档包括用户要求的相关验收文档及可安装的程序运行文件。所交付的文档与文件应当是可供自然人阅读的书面和电子文档。软件文档及可安装的程序运行文件验收通过后，视为初验通过。如有缺陷，招标方应向供应商出具书面报告，陈述需要改进的缺陷。供应商应立即严格依照招标方的书面报告中的要求改进缺陷，并再次进行初验。

（4）自初验通过之日起，招标方享有供应商免费提供的30天的信息系统试运行现场驻场服务期。该期间内，供应商应当按照招标方的要求提供现场技术支持服务，解决信息系统试运行期间可能出现的各类问题，或进一步提高与完善信息系统运行水平。

（5）初验通过且信息系统试运行期已经达到本项目约定的时间，经供应商确认信息系统具备正常运行条件，且信息系统通过运行测试，供应商应以书面形式通知招标方信息系统已准备就绪等待终验。招标方在收到终验通知后的10个工作日内发起组织专家验收会。

（6）如果属于供应商原因致使本项目未能通过终验，供应商应当排除缺陷，直至本项目完全符合验收标准，由上述情形而产生的相关费用应由供应商自行承担。

（7）如果由于招标方原因导致本项目在终验通过前出现故障或问题，供应商应及时配合排除该方面的故障或问题。

（8）如本项目连续3次验收未通过（含初验未通过或终验未通过），招标方有权解除项目，并有权依照本项目约定的违约条款追究供应商的违约责任。

## 进度要求

供应商应根据建设内容，分阶段制定合理的时间进度，并且应根据采购人要求进行调整和细化。本项目于合同签订后12个月内，完成项目建设和验收工作。

总建设周期预计分为五个阶段，预估时间如下：

第一阶段为T+60天，完成规划设计；

第二阶段为T+120天,完成系统设计设备选型；

第三阶段为T+240天，完成系统建设；

第四阶段为T+300天，完成系统测试、试运行；

第五阶段为T+360天，完成验收。

## 企业综合能力要求

供应商具有ISO9001质量管理体系认证证书、ISO45001 职业健康安全管理体系认证证书、ISO20000信息技术服务管理体系认证证书、ISO27001信息安全管理体系认证证书、信息安全服务资质证书、信息系统建设和服务能力证书的优先考虑。

## 项目团队及驻场人员要求

1）投标人须具有稳定的在职技术保障力量，能够提供及时的技术支援或服务，应针对本项目提供不少于13人的项目服务团队（包括项目负责人、生产经理、质量员、安全员、材料员、资料员等），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。

项目主要负责人要求：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 项目负责人 | 负责项目总体质量和进度控制 | 1人 | 本科以上学历，具备信息系统高级项目管理师证书、高级工程师、注册信息安全管理人员（CISP），10年及以上类似项目的实施经验 | 驻场 |
| 技术负责人 | 全面技术相关问题解决 | 1人 | 本科以上学历，具备一级建造师（机电）、高级工程师资质证书 | 驻场 |
| 技术工程师 | 现场计算机网络技术相关问题解决 | 3人 | 具备注册信息安全管理人员（CISP）或注册渗透测试工程师（CISP-PTE）资格 | 驻场 |
| 技术工程师 | 现场实施 | 3人 | 大学学历，相关证书（需含电工作业资格至少1名） | 驻场 |
| 生产经理（施工员） | 负责现场实施人员安排，处理现场问题，上报施工进度、质量情况 | 1人 | 本科以上学历，具备政务行业工作经验。 | 驻场 |
| 质量员 | 负责现场施工质量管理 | 1人 | 具备相关证书 | 驻场 |
| 安全员 | 负责现场施工安全管理 | 1人 | 具备相关证书 | 驻场 |
| 材料员 | 负责组织材料进场、掌握材料使用情况 | 1人 | 具备相关证书 | 驻场 |
| 资料员 | 负责资料的编写 | 1人 | 具备相关证书 | 不驻场 |

2）投标人应针对本项目提供不少于6人的质保期间支撑团队（其中运维经理1人，技术工程师2人，维护工程师不少于2人）；投标人的相关服务人员需具备相应的服务能力，需提供相关证明（最近一个季度依法缴纳社保费的证明）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 项目经理 | 负责项目总体质量和进度控制 | 1人 | 本科以上学历，具备信息系统高级项目管理师证书、高级工程师、注册信息安全管理人员（CISP） | 驻场 |
| 技术负责人 | 全面技术相关问题解决 | 1人 | 具备一级建造师、高级工程师 | 不驻场 |
| 技术工程师 | 现场计算机网络技术相关问题解决 | 2人 | 具备注册信息安全管理人员（CISP）资格 | 不驻场 |
| 维护工程师 | 负责计算机网络运行维护 | 1人 | 熟悉产品性能，熟悉软硬件基本维护 | 驻场 |
| 维护工程师 | 负责电气技术问题解决 | 1人 | 具备相关资质（电工作业特种操作证） | 驻场 |

## 等级保护要求

本项目等级保护要求：

拟按照信息系统安全等级保护三级进行建设。

## 技术文件要求

投标人提供的书面技术资料应能确保系统正常运行所需的管理、运营及维护有关的全套文件。技术文件应该全面、完整、详细。投标人提供的技术文件至少应包括：

－系统说明文件；

－技术手册(安装、测试、操作、维护、故障排除等)；

－项目文档，应该包括：

(1)竣工图

(2)项目过程文件

(3)设备移交清单

提供全套技术文件纸介质3套以及电子文件1套。

# 供应商资质要求

1、符合《中华人民共和国政府采购法》第二十二条规定的供应商。

2、根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。

3、其他资格要求：

3.1本项目面向大、中、小、微型等各类供应商采购。

3.2未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单。

# 供应商管理要求

1、在项目实施期间，中标人应严格执行国家、地方、行业有关本项目业务管理和安全作业的法律、法规和制度并按规定承担相应的费用。中标人因违反规定等原因造成的一切损失和责任由中标人自行承担。

2、中标人在响应文件中承诺并经采购人认定的项目负责人及专业技术人员必须是本单位职工（在本单位缴纳社会保障金）和该项目实施现场的实际操作者，应具有类似本项目的实施经验，并应在软件应用调研、安装、试运行等期间常驻项目现场。未经采购人同意，中标人不得调换或撤离上述人员。如采购人认为有必要，可要求中标人对上述人员中的部分人员作出更好的调整。

3、中标人在项目实施期间，应按项目实际进度与环节落实所对应项目整体及各环节管理工作，按照规范做好项目实施期间相关管理与实施记录。

4、参与本项目的工作人员应严格遵循采购人的安全制度，保障采购人资料和设备的安全。中标人如需进入采购人机房工作，只能在采购人规定的工作区域内对项目涉及的设备进行操作，严禁触动与项目无关的任何设备（包括任何操作行为），如需跨区操作必须得到采购人项目联系人确认。

5、中标人在项目实施期间必须遵守采购人的规章制度并提供实施人员名单。

6、各供应商在响应文件中要结合本项目的特点和采购人上述的具体要求制定相应的管理措施，并在报价中列支相应的费用清单，供应商报价中未列支上述费用清单的，上述费用视为已包含在供应商的投标总报价中。

7、本项目软件开发及调试将纳入采购人的管理范围，中标人在此过程中须服从上述单位的管理协调。

# 关于转让和分包的规定

本项目不得转让、不得分包。

# 知识产权及保密要求

1、中标人数据、文件、资料知识产权

中标人保证其所提供的服务和交付的成果以及在履行本项目义务中使用到的所有数据、文件、信息不会引起任何第三方在专利权、著作权、商标权等知识产权方面向采购人或采购人的关联方及合作方（包括但不限于采购人的主管单位和采购人的合作单位等）发出侵权指控或提出索赔。若有，中标人应负责与第三方解决纠纷，若因此导致采购人损失的，采购人有权要求中标人赔偿采购人因此遭受的全部损失，包括但不限于直接损失、间接损失、诉讼费／仲裁费、律师费、公证费、鉴定费等。

中标人因履行本项目而产生的所有成果的知识产权等权利均归采购人所有，中标人应配合采购人进行相关权利登记或申请。未经采购人书面同意，中标人不得以任何形式使用或许可他人使用本项目成果的相关内容，不得擅自对外公开发表或向任何第三方透露。

在不影响上述条款规定的由采购人取得所有成果的知识产权的前提下，双方因履行本项目而被授权接触或使用对方之知识产权（包括但不限于商标、专利、著作权等），和/或任何其他相关资料、数据等涉及的任何权利，均不视为向另一方转让上述权利或在本项目范围外授权许可另一方使用上述权利，上述权利仍应属于提供方，并仅可使用于本项目，被授权接触或使用方未经提供方书面同意，不得擅自挪作他用。

2、项目保密要求

中标人因履行本项目而知悉的所有数据、信息和资料（包括但不限于账号信息、图表、文字、计算过程、任何形式的文件、访谈记录、现场实测数据、采购人相关工作程序等）以及因履行本项目而形成的数据、信息和任何形式的工作成果，均是采购人要求保密的信息。未经采购人书面同意，中标人不得对外泄露采购人要求保密的信息，不得用于其他用途，否则中标人需承担由此引起的法律责任和经济责任，包括但不限于直接损失、间接损失、律师费、诉讼费/仲裁费、调查费、公证费等。

中标人应采取必要的有效措施保证其参与本项目的人员（包括中标人聘用的人员、借调的人员、实习的人员）无论是在职或离职后，以及中标人的合作方无论是合作中或合作终止后，都能够履行本项目约定的保密义务。若中标人人员或中标人合作方违反保密规定，中标人应承担连带责任。

中标人（含中标人参与本项目的人员以及其合作方）未经采购方书面许可，不得以任何形式自行使用或以任何方式向第三方披露、转让、授权、出售与本项目有关的技术成果、计算机软件、源代码、策划文档、技术诀窍、秘密信息、技术资料和其他文件。

以上内容的保密期限自中标人知悉保密信息起始至保密信息被合法公开之日止。

3、临时账号等使用要求

中标人对采购人提拱的临时使用账号要保密，不得公开，对组件开发的账号密码需进行加密，避免信息安全的泄露。未经采购人的同意不得利用采购人的网络及平台进行短信、彩信、微信发送,造成的一切后果由中标人负责。

# 项目的变更、解除和终止

如果中标人丧失履约能力、发生资不抵债或进入破产程序，采购人可在任何时候以书面形式通知中标人终止本项目的执行而不给予中标人补偿。该终止本项目将不损害或影响采购人已经采取或将要采取任何行动或补救措施的权利。

如遇国家、行业管理部门等机构的有关标准和规定调整的，导致本项目内容须做相应调整时，双方应按照公平、合理的原则共同协商修改本项目对应的合同的相关条款。

# 付款方式

如中标金额高于4315859元整，a.合同签订生效后且甲方收到乙方开具的等额发票后的 10个工作日内，支付合同总价款的 50%;b.本项目中期验收(即初验)通过且甲方收到约定的项目工作成果、乙方开具的等额发票后的 10个工作日内，支付人民币4315859元扣除第一笔支付金额的剩余金额;c.本项目通过最终验收且甲方收到约定的项目工作成果、乙方开具的等额发票后的10个工作日内，支付合同尾款。如中标金额等于或低于4315859元，a.合同签订生效且收到发票后10个工作日内，支付合同总价款的50 %；b.本项目通过最终验收且收到发票后10个工作日内，支付合同总价款的尾款。