# 上海化工区局域网（一期）子系统建设项目

# 采购需求

# 项目概况

本次上海化工区局域网（一期）子系统建设项目旨在化工区范围内构建一个完整、安全、高效的局域网，进一步建立局域网 “运维管理体系”和“安全防护体系”，为化工区实现跨部门跨层级的网络互通、数据共享、应用协同提供有力支撑。主要包含硬件产品购置、运行管理平台、安全产品购置等。

# 建设目标

上海化工区局域网升级改造的目标是在化工区范围内构建一个完整、安全、高效的局域网，以满足未来电子政务发展需求为导向，建成一张标准统一、技术先进、管理智能、安全可靠、坚强有力的新型局域网。充分利用现有资源，按照国家、上海市统一规划和标准规范，进一步建立局域网 “运维管理体系”和“安全防护体系”，实现局域网在网络架构、基础链路、网络资源、网络运维、网络安全等方面的统一管理，为实现跨部门跨层级的网络互通、数据共享、应用协同提供有力支撑。

1) 全网建设符合信息系统安全等级保护2.0三级基本要求的安全防护体系及运行管理平台；

2) 建设的局域网支持IPv4/IPv6双栈技术及网络传输能力。

3) 基于大数据分析技术和智能检测技术，对网络中不同业务的运行状态、服务质量，做到实时监控、主动运维。

4) 建立专业高效的运维服务体系，对升级后的上海化学工业区局域网进行整体系统维护，保障网络系统的正常运行。

5) 预留升级构建基于SDN功能的骨干数据通信网络，满足网络业务和链路策略的快速下发、业务快速部署、流量工程和智能流量调整的整网能力。

# 交付时间

2025年11月10日前完成供货、安装和调试，实现网络组网，并支持相关系统正常运行。

# 网络拓扑情况

系统网络设计如下图所示，投标人应结合采购设备设施与管委会实际情况，对网络拓扑情况进行优化设计，以满足管委会完整、安全、高效的局域网建设目标。



# 运行管理平台建设

## 项目设备清单

以下为本项目主要软硬件参考清单，如硬件设备涉及到除项目内所列明成品软件外配套软件的则供应商必须在报价中已涵盖，项目建设内容质保期（含设备原厂质保期）不得少于3年，此外本项目为“交钥匙工程”，采购人不再另外支付相关任何费用。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 技术指标要求 | 数量 | 单位 |
| 一 | 硬件产品-网络设备 |  |  |  |
| 1 | 核心交换机 | 请详见5.2.1的技术指标规格要求 | 2 | 台 |
| 2 | 接入区千兆接入交换机 | 请详见5.2.1的技术指标规格要求 | 11 | 台 |
| 3 | 接入区万兆接入交换机 | 请详见5.2.1的技术指标规格要求 | 5 | 台 |
| 4 | 市政务外网区接入路由器 | 请详见5.2.1的技术指标规格要求 | 2 | 台 |
| 5 | 安全管理区接入交换机 | 请详见5.2.1的技术指标规格要求 | 2 | 台 |
| 二 | 安全产品 |  |  |  |
| 1 | 各单位接入政务外网-探针 | 请详见5.2.2的技术指标规格要求 | 1 | 台 |
| 2 | 市政务外网边界区-防火墙（IPS+AV） | 请详见5.2.2的技术指标规格要求 | 2 | 台 |
| 3 | 政务云及信创云边界区-防火墙（IPS+AV） | 请详见5.2.2的技术指标规格要求 | 2 | 台 |
| 4 | 安全管理区-态势感知 | 请详见5.2.2的技术指标规格要求 | 1 | 台 |
| 5 | 安全管理区-堡垒机 | 请详见5.2.2的技术指标规格要求 | 1 | 台 |
| 6 | 日志审计 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 7 | 安全管理区-数据库审计 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 8 | 安全管理区-防火墙（IPS+AV） | 请详见5.2.2的技术指标规格要求 | 2 | 台 |
| 9 | 签名验签服务器 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 10 | 密钥管理系统 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 11 | 安全认证网关 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 12 | SSL VPN网关 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 13 | 站点证书 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 14 | 设备证书 | 请详见5.2.2的技术指标规格要求 | 1 | 项 |
| 三 | 产品软件 |  |  |  |
| 1 | 运行管理平台 | 请详见5.2.3的技术指标规格要求 | 1 | 项 |

## 产品技术指标要求

重点技术条款▲15个，须提供产品功能截图或者相关材料（彩页、官网截图、实物照片、检测报告等）作为证明，未提供视为负偏离。

### 硬件产品

|  |  |  |
| --- | --- | --- |
| 序号 | 产品名称 | 技术规格要求 |
| 1 | 核心交换机 | 1. 交换容量≥1000Tbps；
2. 包转发率≥460000Mpps；
3. 主控引擎与交换网板物理分离；
4. 主控引擎≥2；
5. 独立交换网板≥4；
6. 整机业务板槽位数≥6；
7. 支持颗粒化电源，电源插槽个数≥6，万兆光模块≥15个；
8. 以太网支持千兆电口，千兆光口，万兆光口、万兆电口、25G端口、40G端口；
9. 支持精细化的流量监管，粒度可达8K；支持WRED拥塞避免；
10. ▲支持全端口256bits MACsec加密（提供第三方检测报告）
11. 支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由；
12. ▲支持四框堆叠及统一管理（IRF2），最大堆叠带宽能达到双向3.2T（提供第三方检测报告）
13. 支持RIPng、OSPFv3、BGP4+、IS-ISv6协议；
14. 支持基于IPv6的VRRP功能；
15. 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，支持 Telemetry 技术。
16. 包含三年质保服务。
 |
| 2 | 接入区千兆接入交换机 | 1. 交换容量≥670Gbps，转发能力≥200Mpps ；
2. 千兆电口≥48，万兆光口≥4；
3. 冗余电源；
4. 整机最大MAC地址表≥32K；支持基于端口的VLAN，支持基于协议的VLAN；
5. 支持基于MAC的VLAN；
6. 支持链路聚合基本功能及聚合零丢包；
7. 支持远程镜像、流镜像、端口镜像；
8. 支持IPv4静态路由、RIP V1/V2、OSPF；支持IPv6静态路由、RIPng、OSPF v3；
9. 支持基于第二层、第三层和第四层的ACL；
10. 支持出方向ACL，以便于灵活实现数据包过滤；
11. 支持802.1x认证，支持集中式MAC地址认证。
12. 包含三年质保服务。
 |
| 3 | 接入区万兆接入交换机 | 1. 交换容量≥2.56Gbps，转发能力≥1600Mpps ；
2. 万兆光口≥48，40G QSFP28光口≥6；
3. 模块化电源；
4. 支持基于端口的VLAN，支持基于协议的VLAN；
5. 支持基于MAC的VLAN；
6. 支持链路聚合基本功能及聚合零丢包；
7. 支持远程镜像、流镜像、端口镜像；
8. ▲支持基于端口、流量N:M复制,M或N≥48（提供第三方测试报告）
9. 支持IPv4静态路由、RIP V1/V2、OSPF；
10. 支持IPv6静态路由、RIPng、OSPF v3；
11. 支持基于第二层、第三层和第四层的ACL；
12. 支持出方向ACL，以便于灵活实现数据包过滤；
13. 包含三年质保服务。
 |
| 4 | 市政务外网区接入路由器 | 1. 交换容量≥340Gbps；
2. 转发性能≥250Mpps ；
3. 万兆SFP+光口≥6，GE口≥8；
4. 支持RIP、OSPF、IS-IS、BGP等路由协议支持VxLAN二层网关；
5. 支持VxLAN三层网关；
6. ▲支持web cache功能（提供第三方检测报告）
7. 支持L2VPN、L3VPN、EVPN等VPN技术支持ISIS for SRv6支持Console、Telnet、SSH、SNMP等管理方式
8. 包含三年质保服务。
 |
| 5 | 安全管理区接入交换机 | 1. 交换容量≥2.56Tbps，转发能力≥1620Mpps；
2. 万兆光口≥48，40G QSFP28光口≥6；
3. 模块化电源；
4. 支持基于端口的VLAN，支持基于协议的VLAN；
5. 支持基于MAC的VLAN；
6. 支持链路聚合基本功能及聚合零丢包；
7. 支持远程镜像、流镜像、端口镜像RSPAN；
8. ▲支持基于端口、流量N:M复制,M或N≥48（提供第三方测试报告）
9. 支持IGMP v1/v2/v3，MLD v1/v2 。
10. 支持IPv4静态路由、RIP V1/V2、OSPF；
11. 支持IPv6静态路由、RIPng、OSPF v3；
12. 支持基于第二层、第三层和第四层的ACL；
13. 支持出方向ACL，以便于灵活实现数据包过滤；
14. 包含三年质保服务。
 |

### 安全产品

|  |  |  |
| --- | --- | --- |
| 序号 | 产品名称 | 技术规格要求 |
| 1 | 各单位接入政务外网-探针 | 1. ▲性能参数：网络层吞吐量≥8Gbps
2. 硬件参数：规格：2U，内存大小：16G，硬盘容量：480G SSD，电源：冗余电源，接口：4千兆电口+4千兆光口SFP+2万兆光口SFP+。
3. 旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响
4. 支持与第三方安全分析平台kafka对接，将采集的数据上报至第三方安全分析平台。
5. 包含：三年探针规则库更新，三年软硬件质保服务。
 |
| 2 | 市政务外网边界区-防火墙（IPS+AV） | 1. ▲安全处理性能≥10Gbps，网络层吞吐量≥40Gbps。
2. 硬件参数：规格：2U，产品不少于4个千兆电口，4个千兆光口SFP，4个万兆光口SFP+，内存32GB，硬盘总容量不小于960GB SSD；
3. 支持IPv4/IPv6双栈工作模式。
4. 支持基于应用、服务、时间、域名、IPv6对象等维度的访问控制。
5. 产品支持杀毒白名单设置，可以针对特定MD5和URL的病毒文件，不进行查杀。
6. 包含：IPS、网关杀毒，三年软硬件质保服务。
 |
| 3 | 政务云及信创云边界区-防火墙（IPS+AV） | 1. ▲安全处理性能≥10Gbps，网络层吞吐量≥40Gbps；
2. 硬件参数：规格：2U，产品不少于4个千兆电口，4个千兆光口SFP，4个万兆光口SFP+；内存32GB，硬盘总容量不小于960GB SSD；
3. 支持IPv4/IPv6双栈工作模式。
4. 支持基于应用、服务、时间、域名、IPv6对象等维度的访问控制。
5. 包含：IPS、网关杀毒，三年软硬件质保服务。
 |
| 4 | 安全管理区-态势感知 | 1. ▲性能参数：在带宽性能1Gbps时存储时长：1500天/1Gbps。
2. 硬件参数：规格：2U，CPU：2颗Kunpeng 920 3210 2.6GHz（24C），内存：4\*32GB DDR4 3200，系统盘：1\*480GB SATA SSD，数据盘：4\*4T，电源：冗余电源，接口不低于4千兆电口。
3. 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。
4. 支持DNS服务器日志导入，可以接入DNS服务器的日志，安全分析引擎将结合DNS服务器的日志，定位出DNS服务器代理风险外连场景下的真实源IP，从而有效地进行风险处置闭环。支持对导入DNS服务器进行展示，展示内容至少包含日志源名称、日志源IP、接入类型、今日日志传输量、传输日志总量、最近同步时间、运营状态等。
5. 包含：三年态势感知平台规则库更新，三年软硬件质保服务。
 |
| 5 | 安全管理区-堡垒机 | 1. ▲性能参数：包含运维授权数≥200，最大可扩展资产数≥1000，图形运维最大并发数≥200，字符运维最大并发数≥550。
2. 硬件参数：规格：2U，内存大小：32G，硬盘容量：480G SSD+4T，电源：冗余电源，接口不低于8千兆电口、4千兆光口SFP、2万兆光口SFP+；
3. 电源：冗余电源；
4. 全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计
5. 包含：三年软硬件质保服务。
 |
| 6 | 日志审计 | 1. 性能参数：包含主机审计许可证书数量≥100，可用存储量≥4TB（RAID0 模式），平均每秒处理日志数最大性能≥2500EPS。
2. 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，接口不少于6千兆电口、2万兆光口SFP+。
3. 支持主流国产操作系统日志接入。
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、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
5. 包含：三年软硬件质保服务。
 |
| 7 | 安全管理区-数据库审计 | 1. ▲性能参数：最大硬件吞吐量≥2Gbps，最大数据库纯SQL流量≥400Mb/s，数据库实例个数≥30个，SQL处理性能≥30000条SQL/s，日志检索性能≥400000条/秒，配置国产化系统。
2. 硬件参数：规格：2U，内存大小：内存≥8G，硬盘容量≥128G SSD+4T SATA，接口：千兆电口≥6。
3. 支持告警日志审阅，可设置同时审阅规则对同类事件进行同时审阅，同时审阅规则条件包含服务端IP、数据库实例名、数据库账号、客户端IP、匹配规则、操作对象名、操作命令、客户端APP和SQL模板等，支持选择多条告警日志进行批量审阅。
4. 支持定义黑白名单策略，匹配条件至少包括数据库账号、策略周期、来源IP、客户端工具、SQL命令、操作对象名、SQL语句等条件。白名单命中后识别为信任行为，黑名单命中后可识别为非法行为。
5. 支持旁路阻断功能（非串联方式）
6. 包含：三年软硬件质保服务。
 |
| 8 | 安全管理区-防火墙（IPS+AV） | 1. ▲安全处理性能≥10Gbps，网络层吞吐量≥40Gbps。
2. 硬件参数：2U，产品不少于4个千兆电口，4个千兆光口SFP，4个万兆光口SFP+，内存32GB，硬盘总容量不小于960GB SSD。
3. 产品支持IPv4/IPv6双栈工作模式。
4. 产品支持独立的账号安全防护模块，具备事前账号脆弱性、事中账号爆破、事后账号失陷的全生命周期安全防护，在设备界面可以详细展示账号安全相关信息，包括风险业务、风险等级、存在账号入口、存在弱口令、遭受口令爆破、异常登录账号登。
5. 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。
6. 产品支持多种安全日志存储方式，至少包括防火墙本机、日志服务器等不同方式。支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间。
7. 包含：IPS、网关杀毒，三年软硬件质保服务。
 |
| 9 | 签名验签服务器 | 1. 支持国产密码算法SM2、SM3、SM4，支持基于数字证书的身份认证，提供数据签名与签名验证功能、数字信封功能，实现数据的完整性和行为的不可否认性保护。
2. 性能：SM2签名效率不低于97000，SM2验签效率不低于42000。
3. 支持三员管理：支持安全管理员、系统管理员、审计管理员的分角色管理。
4. 全面系统管理及审计功能：支持日志SYSLOG远程发送、日志归档、系统备份恢复、支持IPV6、三权管理、SNMP监控。支持时间服务管理。
5. 包含三年质保服务。
 |
| 10 | 密钥管理系统 | 1. 密钥管理系统支持SM2、SM3、SM4算法，具有密钥生成、分发、存储、管理等功能，提供密钥生命周期管理，提供创建密钥，禁用密钥，删除密钥，导入密钥（密钥来源为外部导入），查看密钥轮转历史，搜索指定密钥等功能，还支持应用数据加解密和数据库加解功能。
2. 支持集群部署、服务设备动态扩展。
3. 应用数据加解密：支持基于密钥管理系统的接口或客户端工具，获取数据密钥实现。对应用数据的加解密数据库加解密码：支持在数据库系统中内置密钥管理系统的数据库加密引擎工具，实现对数据库数据的加解密等密钥运算服务。
4. 包含三年质保服务。
 |
| 11 | 安全认证网关 | 1. 支持SM2、SM3、SM4算法，具有密钥协商、身份认证、SSL隧道加密等功能，支持基于数字证书实现用户访问业务系统时的安全身份认证，支持双向身份验证功能，支持动态黑名单，支持多种业务应用：B/S应用、C/S应用。
2. 性能：并发连接数不低于50000，SM2 HTTP TPS不低于30000，加密吞吐率不低于1Gbps。
3. 支持证书认证，实现网关和客户端的双向强身份认证，保证接入用户身份的真实性。支持 SSL3.0、TLS1.0、TLS1.1、TLS1.2、TL.S1.3、TLCP协议，适应多样化的网络环境；可以根据客户端发起访问的类型自适应国密或者国际算法加密。
4. SM2加密吞吐率≥4Gbps。SM2每秒新建连接：单向≥ 8K。并发连接数 ≥8W。SM2 HTTP TPS≥10W。
5. 包含三年质保服务。
 |
| 12 | SSL VPN网关 | 1. 实现安全运维通道保护。
2. 包含三年质保服务。
 |
| 13 | 站点证书 | 1. 安全认证网关使用。
 |
| 14 | 设备证书 | 1. 签名验签服务器使用。
 |

### 产品软件

|  |  |  |
| --- | --- | --- |
| 序号 | 产品名称 | 技术规格要求 |
| 1 | 运行管理平台 | 1. 提供对核心交换机、汇聚交换机、边界路由器、关键业务的统一监控管理、统一告警管理、统一报表管理；
2. 支持设备基本信息展示：设备标签、管理状态、IP地址、掩码、sysOID、类型、系统名称、联系人、位置、设备型号、最后轮询时间、接口数量、运行时间、系统描述等。所有新建网络设备管理授权及满足需求局域网准入授权；
3. ▲支持自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等；（提供第三方测试报告）
4. 可以为不同的管理员设置不同的用户名、密码，并限制管理员的管理权限和管理范围，实现用户分权管理；
5. 支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时，根据不同的阈值发送不同级别的告警；
6. 支持对全网设备告警的实时监控和统一浏览；支持多种提醒方式，如告警实时提醒（告警板）、告警音响提示；支持多种转发方式，比如转E-mail，转短信，转上级网管或其它网管等。支持告警分析，可以屏蔽重复告警、闪断告警，支持告警自动确认功能；
7. 支持批量的设备配置备份和恢复。支持向导方式或者任务方式（周期性任务、一次性任务或立即任务）批量的备份、恢复完整的配置文件，也可以批量的下发配置片断；
8. ▲VLAN拓扑功能以可视的方式对网络中的VLAN资源进行管理，查看拓扑视图中所有设备节点和链路是否允许某个特定VLAN通过；（提供第三方测试报告）
9. 支持分析多告警关系，找到根源告警及兄弟告警。并提供关联分析，分析和当前告警相关的告警，可自定义配置分析的维度和时间窗进行手动分析；
10. 支持基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警；
11. ▲实配：网络管理和终端准入授权，网络管理授权数不小于100个，终端准入授权数不小于200个。（提供第三方测试报告）
 |

# 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1年内提供7\*24小时免费技术支持和售后服务，1年后进入有偿维护期。

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：系统技术支持、系统使用支持、运行环境的维护及漏洞修复等。

## 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12个月的质量保证期内，提供2次与项目相关的必要培训。

(2)供应商需要开展分层次的人员培训工作，每次培训后应对参加培训人员进行测试，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。

## 进度要求

投标人应根据建设内容，分阶段制定合理的时间进度，并且应根据招标方要求进行调整和细化。

2025年11月10日前完成供货、安装和调试。

## 等级保护要求

本项目软件开发部分按照等保2.0第三级进行建设。

## 商业密码应用需求

本项目软件开发部分依据商用密码应用三级信息系统要求建设。

## 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，供应商具有ISO20000IT信息技术服务管理体系认证、ISO27001信息安全管理体系认证、ISO9001质量管理体系认证的.
2. 投标人应提供不少于10人的项目服务团队（包括项目经理、技术负责人、工程师等）；其中项目负责人应具备高级工程师资质认证，技术负责人、工程师应具备中级及以上工程师资质认证。
3. 供应商在质保期内投入不少于3人驻场服务团队。

## 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)产品使用说明书

(2) 系统总体设计说明书

(3)软硬件产品功能清单

(4) 安全管理方案、应急方案

提供全套技术文件纸介质3套以及电子文件1套。