一、 项目概述

1、项目名称：上海戏剧学院 XC 虚拟云子系统建设项目

2、采购内容：本项目拟通过建成具备互联互通、虚拟计算、数据存储、安全防护、数据备份等综合服务能力的 XC 云平台，实现校园公共基础设施的统建共用，支撑学校高质量数据集建设，包括高质量数据集基础支撑系统、XC 云平台系统、安全系统及满足多个业务应用迁移上云或新建业务上云。建设内容包括云网络系统、云存储系统、安全系统等，各系统可以保证各自独立并实现兼容和互联互通，在 XC 云整体方案中能够实现融合，保证整体技术架构的灵活性、先进性、合理性、高可用、高安全和可扩展性。

3、交付地点：上海市静安区华山路 630 号

4、合同履约期限：合同签订后 30 个日历天内到货并完成检验签收，5 个日历天内完成设备安装、调试、连通、测试等工作。

二、 项目背景

按照本市 XC 工作部署，有序推进信息系统安全可靠替代改造，逐步完成相关业务系统自主产品适配。应用系统基于国产技术平台稳定运行，信息安全基础更加牢固，安全防护能力整体增强。上海戏剧学院将逐步实现信息系统自主产品替代，包括国产服务器、国产网络安全设备、国产终端设备、国产基础软件替代以及信息系统安全的提升。

三、 建设目标

本项目拟通过建成具备互联互通、虚拟计算、数据存储、安全防护、数据备份等综合服务能力的 XC 云平台，实现校园公共基础设施的统建共用，支撑学校信息化业务协同和数据共享汇聚，显著提升校园治理精准化、服务便捷化、基础设施集约化等水平。

四、建设原则

1、按照相关产品需求配置确定技术路线，在满足需求的前提下，保证采用国产自主可控的安全可靠信息化设备。

2、在满足安全可靠信息化要求的前提下，结合我市信息化现状和产业发展实际，优先选择性能佳、兼容性好、稳定性高、适配性强且具有良好的保障和服务能力的产品及服务。

3、选择符合相关标准协议的产品，确保产品间可互联互通及今后扩展。

4、相关安全设备选择符合相关部门认证的产品。

5、软件产品优先选用体系架构成熟的软件产品，尽量减少自行开发工作，确保系统工作稳定。

6、选择低能耗的设备，优先采用一类能耗标准的获得“中国节能/环保产品”标识/证书的产品。

五、项目建设内容

本项目拟通过建成具备互联互通、虚拟计算、数据存储、安全防护、数据备份等综合服务能力的XC云平台，实现校园公共基础设施的统建共用，支撑学校高质量数据集建设，包括高质量数据集基础支撑系统、XC云平台系统、安全系统及满足多个业务应用迁移上云或新建业务上云。建设内容包括云网络系统、云存储系统、安全系统等，各系统可以保证各自独立并实现兼容和互联互通，在XC云整体方案中能够实现融合，保证整体技术架构的灵活性、先进性、合理性、高可用、高安全和可扩展性。

本项目核心产品：云汇聚交换机

1、XC虚拟云平台软硬件采购

主要包括存储设备3台、融合云存储软件1套。

序号	产品大类	产品小类	产品配置	数量
1	主机	存储设备	分布式块存储设备采用国产处理器，主频≥2.5GHz，单颗处理器≥32 核、三级缓存≥64MB，配置 2 颗；CPU 内置密码模块或密码协处理器；整机内存容量≥256GB；配置冗余系统盘，单块系统 SSD≥480G；NVMe 缓存盘总容量≥3.84TB；SATA 数据盘裸总容量≥80TB；板载 GE 电口≥4，万兆光口≥6。	3
2	工具软件	工具软件	融合云存储软件，240T 许可；含部署服务和三年技术服务	1

2、网络及安全产品采购

主要包括云汇聚交换机2台、云业务交换机2台、云存储交换机2台、云存储后端交换机1台、云管理交换机1台、云带外管理交换机1台、核心域防火墙2台、堡垒机1台、日志审计系统1台、数据库审计系统1台、应用域防火墙1台、 WEB应用防火墙2台。

序号	产品大类	产品小类	产品名称	产品配置	数量
1	网络设备	交换机	云汇聚交换机	24个万兆光口，2个QSFP 40G端口，14个SFP+ 万兆模块，冗余电源及风扇;3个业务插槽；交换容量不低于6.4Tbps；	2
2	网络设备	交换机	云业务接入交换机	48个万兆光口，2个40G光口，7个SFP+ 万兆模块，QSFP+ 电缆，配置冗余电源及风扇；交换容量不低于4.8Tbps；	2
3	网络设备	交换机	云存储交换机	48个万兆光口，2个40G光口，7个SFP+ 万兆模块，QSFP+ 电缆，配置冗余电源及风扇；交换容量不低于4.8Tbps；	2
4	网络设备	交换机	云存储后	云存储后端交换机48个万兆光口，2	1

			端交换机	个 40G 光口，5 个 SFP+ 万兆模块，QSFP+ 5m 电缆，配置冗余电源及风扇；交换容量不低于 4.8Tbps；	
5	网络设备	交换机	云管理交换机	48 个万兆光口，2 个 40G 光口，22 个 SFP+ 万兆模块，QSFP+ 电缆，配置冗余电源及风扇；交换容量不低于 4.8Tbps；	1
6	网络设备	交换机	云带外管理交换机	48 个千兆电口，4 个万兆光口，配置冗余电源及风扇；交换容量不低于 2.4Tbps ；	1
7	边界安全	防火墙	核心域防火墙	采用国产化硬件平台和国产操作系统；应用层吞吐量：10Gpbs；1 个管理口、8 个千兆电口、4 个千兆光口和 4 个万兆光口，包含专业版快速查杀病毒库 3 年升级许可和 IDP 攻击规则特征库 3 年升级许可；	2
8	安全管理与支持	安全审计产品	堡垒机	采用国产化硬件平台和国产操作系统。外观：标准机架式，支持 6 个千兆电口，4 个千兆光口，含 2 个万兆光口，支持 1 个扩展槽，内置 4TB 企业级硬盘，冗余电源。最大支持 400 路图形会话或 2000 路字符会话并发，授权 500 个被管资源数，最大可选 1000 授权许可；	1
9	安全管理与支持	安全审计产品	日志审计系统	采用国产化硬件平台和国产操作系统。1 个管理口、1 个 HA 口、4T 硬盘，8 个千兆电口、8 个千兆光口和 2 个万兆光口,冗余电源,日志采集处理均值 5000EPS，包含 50 日志源；	1
10	安全管理与支持	安全审计产品	数据库审计系统	采用国产化硬件平台和国产操作系统。2U,内存 32G，机械硬盘 4T，6 个千兆电口（1 个管理，1 个 HA），4 个千兆光口，2 个万兆光口,冗余电源,2 个扩展槽位,每秒新建连接：5W，整机吞吐：5.47Gbps；	1
11	边界安全	防火墙	应用域防火墙	采用国产化硬件平台和国产操作系统；2U,1 个管理口、1 个 HA 口、8 个千兆电口、4 个千兆光口和 4 个万兆光口,冗余电源,应用层吞吐量：8Gpbs；包含专业版快速查杀病毒库 3 年升级许可和 IDP 攻击规则特征库 3 年升级许可；	1
12	应用安全	WEB 应用防火墙	WEB 应用防火墙	采用国产化硬件平台和国产操作系统；2U,内存：16GB；硬盘：2TB；4 个千兆电口,4 个千兆光口,2 个万兆光口;HTTP 吞吐量：8Gbps，HTTP 并发连接数：100 万；	2

六、项目建设要求

项目建设需符合 XC 要求。在产品选择上，采用具有开放性好、兼容性强、可扩展的符合国产要求的国内主流产品。应采用目前符合国产要求的行业领先技术，保证在满足功能要求的基础上，应能够满足个性化需求的定制。

XC 产品：本产品为自主可控信息技术产品，核心技术由国内主体掌握，适配国内自研芯片、操作系统、数据库等技术底座，满足网络与数据安全相关规范要求，可在自主信息技术体系内稳定部署、协同运行等要求。

1、总设计技术要求

投标人应负责本项目总体设计和软硬件系统安装调试集成。并满足以下要求：

1.1 投标人应负责本项目的总体设计和软硬件系统安装调试集成。

1.2 负责按照要求编制总体设计方案和总体实施方案。

1.3 负责落实网络安全等级保护制度，总体系统安全需达到各应用系统对应的等级保护等级要求。

1.4 负责项目整体管理协调工作，按照确定的项目管理方法和信息系统工程标准规范，完成项目建设目标。

2、设计原则

系统在设计时遵循以下设计原则：

建设应以“实用、可靠、先进、经济、开放、安全”为指导思想，并综合考虑施工、维护以及操作因素，使得设计方案具有科学性、合理性、可操作性。

3、XC虚拟云平台软硬件要求

3.1存储设备

要求采购、安装、集成实施 3 台存储设备，具体参数要求如下：

指标分类	详细技术参数
品牌要求	国内厂商
服务器外型	机架式，≥2U，标配原厂导轨
▲CPU 要求	≥2 颗国产 CPU 处理器，单颗 CPU 核数≥32 核，主频≥2.5GHz。CPU 内置密码模块或密码协处理器，可实现 SM2、SM3 和 SM4 国密算法的硬件加速。
▲内存要求	配置 32GB 5600MT/s DDR5≥8 根，可支持≥16 个内存插槽，支持最大内存容量 1.5TB
▲硬盘要求	配置≥2 块 480GB SSD 硬盘，≥10 块 8TB HDD 硬盘，≥2 块 1.92TB NVME SSD 缓存盘；支持扩展至≥33 个 2.5 寸热插拔硬盘槽位
阵列控制器要求	≥1 个 SAS RAID 阵列卡，≥4GB 缓存，支持缓存数据保护，且后备保护时间不受限制，支持 RAID0/1/10/5/6/50/60

▲I/O 插槽要求	最大提供≥10 个标准 PCIe 5.0 插槽
▲网卡要求	配置≥4 个 GE 电口，≥3 个 10GE 双端口光口网卡（含光模块）
▲接口要求	≥5 个 USB 3.0 接口，1 个 USB 2.0 接口；标配 1 个 VGA，可选配支持最高 2 个 VGA 接口；标配 1 个串口；支持后部独立的管理端口
电源要求	2 个≥1300W 白金版热插拔冗余电源，支持 94%能效比的白金级电源选件
风扇要求	热插拔冗余风扇
工作温度	在允许的配置条件下，可支持 5℃～40℃
嵌入式管理	配置≥1Gb 独立的远程管理控制端口
硬件加密	支持虚拟化加速，支持加密虚拟化和内存，支持国密算法
▲BMC 芯片	BMC 管理芯片通过安全可靠测评
入侵侦测	可配置机箱入侵侦测，在外部打开机箱时提供报警功能

3.2融合云存储软件

要求采购、安装、集成实施 1 套融合云存储软件，具体参数要求如下：

指标项	详细技术参数
▲授权配置	本次配置≥240TB 的裸容量授权，包含所有功能特性，不额外收费。
IO 聚合	支持将随机小 IO 聚合为顺序大 IO，提升读写性能，降低硬盘磨损。
▲部署能力	支持多种部署方式，既独立部署作为 IP SAN 使用，也可与厂商计算虚拟化平台实现内核级超融合部署。与本项目提供的存储设备完全兼容。提供原厂官网证明。
部署	单节点池可同时部署文件、对象和块存储类型服务。
多子集群管理	支持多子集群管理功能，将多套存储集群信息集成到统一运维界面，清晰直观地向用户展示多套集群的 IOPS，带宽，硬盘池信息，异常主机，实时告警等数据
反磨损均衡	对系统中的盘磨损度进行检测，当盘达到设计的磨损度后增大到该盘的 IO 数量，使其提前磨损并重构，避免系统中多个盘寿命同时到达后同时故障。
分布式架构	Scale-out 横向扩展的分布式架构，最高支持 8192 节点。节点间完全对称，无独立的元数据物理服务器或索引服务器；元数据、数据均采用集群方式部署，满足任何一个节点出现故障，不影响数据的正常访问功能
分布式架构	采用全分布式架构和数据冗余技术，随着存储节点数的增加，分布式存储性能和容量也随着线性增长，性能误差小于 10%。
负载均衡	支持节点间智能负载均衡功能，支持按照轮询、CPU 使用率、剩余内存容量、客户端连接数、网络吞吐量、综合负载等多种方式，实时选择最优的节点用于业务分担；
可靠性	支持分布式存储基本的可靠性保障，如集群扩容、硬盘故障、节点故障均不影响数据完整性。

扩容	支持构建存储集群，集群内节点可在线添加，并且可支持添加硬盘并实现硬盘在线/离线扩容、更换功能，并能实现磁盘的批量扩容，新增磁盘或者节点后，系统可自动实现数据均衡，保障资源的平衡利用。
数据加密	支持存储加密，数据通过标准的商密和国密算法（AES、SM4）以密文落盘进行存储，裸盘直接读取的文件为密文。
数据冗余机制	支持纠删码特性，支持 N+1 到 N+4 的纠删码保护，最大支持任意 4 个节点故障而数据不丢失、系统不停机。
▲数据重构	磁盘或者节点故障之后无需人工干预，数据在集群内硬盘的剩余空间中自动重构，所有硬盘并发重构，提升重构效率，可以做到<=15min/TB。

4、网络及安全产品要求

4.1云汇聚交换机

要求采购、安装、集成实施 2 台设备，具体参数要求如下：

指标分类	详细技术参数
▲交换容量	≥ 6.4Tbps
▲转发性能	≥2030Mpps
硬件规格	高度 2U，扩展插槽≥4。 支持模块化四电源，双风扇框。
软件规格	整机最大路由地址表≥320K
▲端口实配要求	实配 24 个 10G SFP+接口，2 个 40G QSFP+接口；配置 14 个 10G 多模光模块。
二层功能	支持基于端口、基于协议、基于 MAC 的 VLAN。 支持动态 MAC、静态 MAC 和黑洞 MAC 表项。
三层功能	支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 动态路由协议。 支持 IPv6 ND、支持路径 MTU 发现。
可靠性	支持 VRRP 功能。提供第三方权威机构测试报告。 ▲支持 BFD 功能，支持最小 3 毫秒检测时间；收敛时间≤10ms，会话数可达 256。提供第三方权威机构测试报告。 支持跨设备链路聚合技术 M-LAG/DRNI,支持二三层组播、快速收敛和一致性检查。 支持 STP/RSTP/MSTP。
▲智能无损	支持无损网络 RoCE(RoCEv1/RoCEv2 功能)/RDMA,支持 PFC、ECN、ETS、DCB。提供第三方权威机构测试报告。
可视化	支持 sFlow/Netstream 功能。提供第三方权威机构测试报告。 ▲支持 MOD 功能，不占用路由资源。提供第三方权威机构测试报告。
DC 特性	支持二层、三层 Vxlan 网关和 BGP EVPN 特性。
安全性	支持端口隔离。 ▲支持 MACSec 功能测试，支持 128bit 和 256bit MACSec 加密，提供第三方权威机构测试报告。
配置和维护	支持 ERSPAN/RSPAN/ERSPANv3（ERSPAN 增强）功能

配置和维护	支持 SNMP、Telnet、RMON、SSH

4.2云业务交换机

要求采购、安装、集成实施 2 台设备，具体参数要求如下：

指标分类	详细技术参数
▲交换容量	≥4.8Tbps/80Tbps
▲包转发率	≥2000Mpps
▲硬件架构	48*10G+8*40G/100G ,8 个 100G 口支持拆分 10G/25G 模块化风扇≥4 电源冗余 风扇冗余，支持故障任意风扇，设备工作正常
软件规格	MAC 表项 ≥440K IPv4 FIB ≥480K，IPv6 FIB≥240K ARP 表项≥94K
二层功能	支持 802.1Q（VLAN），数目不小于 4k；支持 802.1ad（QinQ）。 支持基于端口、协议、IP 子网、MAC 地址 VLAN 划分。 支持端口聚合，802.3ad，支持二,三层聚合。
三层功能	支持 IPv4 静态路由、RIP、OSPF、ISISv4 及加密、BGP 及加密。 支持 IPv6 静态路由、RIPng、OSPFv3 及加密、ISISv6 及加密、BGP4+及加密。
MPLS	MPLS VPLS、 SRv6 功能。 MPLS L3VPN 功能。
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备。 支持跨框链路聚合（M-LAG)。 M-Lag 支持 VXLAN，M-LAG 支持三层组播。
镜像	支持本地端口镜像和远程端口镜像；支持流镜像。
tap	支持基于端口 N:M 复制。 支持 GRE 隧道剥离封装，支持同源同宿。
流量调度	支持 ACL、CAR、Remark 等动作。 支持 Diff-serv/QoS。 支持 PQ（SP）、WFQ、PQ+WFQ 等队列调度方式。
可靠性	支持微分段。 支持 BFD FOR VRRP 功能。 硬件 BFD, 最小检测间隔 3ms。 支持组播 FRR。 支持电源的告警监视；电压和环境温度的监视。 支持风扇模块热拔插。
管理和监控	支持 SNMP V1/V2/V3、Telnet、RMON、SSH2.0 功能。 支持缓存微突发监控。 支持缓存状态监控，识别流量微突发情况。 ▲支持 SLICE 切片功能。 支持配置回滚。 支持 sflow。 ▲微分段支持 65535 个组，支持 131060 个成员。 支持 INT 流量可视化功能。 支持 ERSPAN 增强，支持采样和截断测试。 支持 Telemetry（GRPC）。

安全特性	支持 IP/ARP/ICMP 安全。 支持配置文件国密加密； 支持安全 boot，主用 boot 故障时，采用备用 boot 进行启动。 支持硬件层级双 boot，采用两个 FLASH 芯片存储 boot 软件（系统引导程序），实现硬件级 boot 冗余备份，避免因 FLASH 芯片故障导致交换机无法启动。 设备的端口安全支持授权双栈自定义 ACL 功能。 支持 MOD：丢包镜像。 支持全端口 256bits MACsec 加密。 支持国密算法、具备国密检测能力 端口光功率异常检测。
网络分析	支持 10G/25G/40G/100G/400G IPFIX/Netstream 1:1 采样功能。 支持基于会话的 Netstream 功能。 Netstream 支持出入方向过滤。
VxLAN	支持 VXLAN over IPv6。 支持 IPv6 VXLAN over IPv4。 支持 VxLAN OAM: VxLAN ping, VxLAN tracert。 支持 BGP EVPN 协议。 微分段实现 IPv4 服务链（Service chain）功能。 微分段实现 IPv6 服务链（Service chain）功能。
▲实配	满配电源、风扇，配置 7 个 10G 多模光模块，一根 5m 40G QSFP+堆叠线 。

4.3 云存储交换机

要求采购、安装、集成实施 2 台设备，具体参数要求如下：

指标分类	详细技术参数
▲交换容量	≥4.8Tbps/80Tbps
▲包转发率	≥2000Mpps
▲硬件架构	48*10G+8*40G/100G ,8 个 100G 口支持拆分 10G/25G 模块化风扇≥4 电源冗余 风扇冗余，支持故障任意风扇，设备工作正常
软件规格	MAC 表项 ≥440K IPv4 FIB ≥480K，IPv6 FIB≥240K ARP 表项≥94K
二层功能	支持 802.1Q（VLAN），数目不小于 4k；支持 802.1ad（QinQ） 支持基于端口、协议、IP 子网、MAC 地址 VLAN 划分 支持端口聚合，802.3ad，支持二,三层聚合
三层功能	支持 IPv4 静态路由、RIP、OSPF、ISISv4 及加密、BGP 及加密 支持 IPv6 静态路由、RIPng、OSPFv3 及加密、ISISv6 及加密、BGP4+及加密
MPLS	MPLS VPLS、 SRv6 功能 MPLS L3VPN 功能
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备 支持跨框链路聚合（M-LAG) M-Lag 支持 VXLAN，M-LAG 支持三层组播

镜像	支持本地端口镜像和远程端口镜像；支持流镜像
tap	支持基于端口 N:M 复制 支持 GRE 隧道剥离封装，支持同源同宿
流量调度	支持 ACL、CAR、Remark 等动作 支持 Diff-serv/QoS 支持 PQ（SP）、WFQ、PQ+WFQ 等队列调度方式
可靠性	支持微分段 支持 BFD FOR VRRP 功能 硬件 BFD，最小检测间隔 3ms 支持组播 FRR 支持电源的告警监视；电压和环境温度的监视 支持风扇模块热拔插
管理和监控	支持 SNMP V1/V2/V3、Telnet、RMON、SSH2.0 功能 支持缓存微突发监控 支持缓存状态监控，识别流量微突发情况 ▲支持 SLICE 切片功能； 支持配置回滚 支持 sflow ▲微分段支持 65535 个组，支持 131060 个成员； 支持 INT 流量可视化功能 支持 ERSPAN 增强，支持采样和截断测试 支持 Telemetry（GRPC）
安全特性	支持 IP/ARP/ICMP 安全 支持配置文件国密加密； 支持安全 boot，主用 boot 故障时，采用备用 boot 进行启动； 支持硬件层级双 boot，采用两个 FLASH 芯片存储 boot 软件（系统引导程序），实现硬件级 boot 冗余备份，避免因 FLASH 芯片故障导致交换机无法启动； 设备的端口安全支持授权双栈自定义 ACL 功能； 支持 MOD：丢包镜像 支持全端口 256bits MACsec 加密 支持国密认证 端口光功率异常检测
网络分析	支持 10G/25G/40G/100G/400G IPFIX/Netstream 1:1 采样功能； 支持基于会话的 Netstream 功能； Netstream 支持出入方向过滤；
VxLAN	支持 VXLAN over IPv6 支持 IPv6 VXLAN over IPv4 支持 VxLAN OAM: VxLAN ping, VxLAN tracert 支持 BGP EVPN 协议 微分段实现 IPv4 服务链（Service chain）功能 微分段实现 IPv6 服务链（Service chain）功能
▲实配	满配电源、风扇，配置 7 个 10G 多模光模块，一根 5m 40G QSFP+堆叠线

4.4云存储后端交换机

要求采购、安装、集成实施 1 台设备，具体参数要求如下：

指标分类	详细技术参数

▲交换容量	≥4.8Tbps/80Tbps
▲包转发率	≥2000Mpps
▲硬件架构	48*10G+8*40G/100G ,8 个 100G 口支持拆分 10G/25G 模块化风扇≥4 电源冗余 风扇冗余，支持故障任意风扇，设备工作正常
软件规格	MAC 表项 ≥440K IPv4 FIB ≥480K，IPv6 FIB≥240K ARP 表项≥94K
二层功能	支持 802.1Q（VLAN），数目不小于 4k；支持 802.1ad（QinQ） 支持基于端口、协议、IP 子网、MAC 地址 VLAN 划分 支持端口聚合，802.3ad，支持二,三层聚合
三层功能	支持 IPv4 静态路由、RIP、OSPF、ISISv4 及加密、BGP 及加密 支持 IPv6 静态路由、RIPng、OSPFv3 及加密、ISISv6 及加密、BGP4+及加密
MPLS	MPLS VPLS、 SRv6 功能 MPLS L3VPN 功能
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备 支持跨框链路聚合（M-LAG) M-Lag 支持 VXLAN，M-LAG 支持三层组播
镜像	支持本地端口镜像和远程端口镜像；支持流镜像
tap	支持基于端口 N:M 复制 支持 GRE 隧道剥离封装，支持同源同宿
流量调度	支持 ACL、CAR、Remark 等动作 支持 Diff-serv/QoS 支持 PQ（SP）、WFQ、PQ+WFQ 等队列调度方式
可靠性	支持微分段 支持 BFD FOR VRRP 功能 硬件 BFD, 最小检测间隔 3ms 支持组播 FRR 支持电源的告警监视；电压和环境温度的监视 支持风扇模块热拔插
管理和监控	支持 SNMP V1/V2/V3、Telnet、RMON、SSH2.0 功能 支持缓存微突发监控 支持缓存状态监控，识别流量微突发情况 ▲支持 SLICE 切片功能； 支持配置回滚 支持 sflow ▲微分段支持 65535 个组，支持 131060 个成员； 支持 INT 流量可视化功能 支持 ERSPAN 增强，支持采样和截断测试 支持 Telemetry（GRPC）
安全特性	支持 IP/ARP/ICMP 安全 支持配置文件国密加密； 支持安全 boot，主用 boot 故障时，采用备用 boot 进行启动； 支持硬件层级双 boot，采用两个 FLASH 芯片存储 boot 软件（系统引导程序），实现硬件级 boot 冗余备份，避免因 FLASH 芯片故障导致交换机无法启动； 设备的端口安全支持授权双栈自定义 ACL 功能；

	支持 MOD：丢包镜像 支持全端口 256bits MACsec 加密 支持国密算法、具备国密检测能力。 端口光功率异常检测
网络分析	支持 10G/25G/40G/100G/400G IPFIX/Netstream 1:1 采样功能； 支持基于会话的 Netstream 功能； Netstream 支持出入方向过滤；
VxLAN	支持 VXLAN over IPv6 支持 IPv6 VXLAN over IPv4 支持 VxLAN OAM: VxLAN ping, VxLAN tracert 支持 BGP EVPN 协议 微分段实现 IPv4 服务链（Service chain）功能 微分段实现 IPv6 服务链（Service chain）功能
▲实配	满配电源、风扇，配置 5 个 10G 多模光模块，一根 5m 40G QSFP+堆叠线

4.5云管理交换机

要求采购、安装、集成实施 1 台设备，具体参数要求如下：

指标分类	详细技术参数
▲交换容量	≥4.8Tbps/80Tbps
▲包转发率	≥2000Mpps
▲硬件架构	48*10G+8*40G/100G ,8 个 100G 口支持拆分 10G/25G 模块化风扇≥4 电源冗余 风扇冗余，支持故障任意风扇，设备工作正常
软件规格	MAC 表项 ≥440K IPv4 FIB ≥480K，IPv6 FIB≥240K ARP 表项≥94K
二层功能	支持 802.1Q（VLAN），数目不小于 4k；支持 802.1ad（QinQ） 支持基于端口、协议、IP 子网、MAC 地址 VLAN 划分 支持端口聚合，802.3ad，支持二,三层聚合
三层功能	支持 IPv4 静态路由、RIP、OSPF、ISISv4 及加密、BGP 及加密 支持 IPv6 静态路由、RIPng、OSPFv3 及加密、ISISv6 及加密、BGP4+及加密
MPLS	MPLS VPLS、 SRv6 功能 MPLS L3VPN 功能
虚拟化	支持集群或堆叠多虚一技术，实现单一界面管理多台设备 支持跨框链路聚合（M-LAG) M-Lag 支持 VXLAN，M-LAG 支持三层组播
镜像	支持本地端口镜像和远程端口镜像；支持流镜像
tap	支持基于端口 N:M 复制 支持 GRE 隧道剥离封装，支持同源同宿
流量调度	支持 ACL、CAR、Remark 等动作 支持 Diff-serv/QoS 支持 PQ（SP）、WFQ、PQ+WFQ 等队列调度方式
可靠性	支持微分段 支持 BFD FOR VRRP 功能

	硬件 BFD，最小检测间隔 3ms 支持组播 FRR 支持电源的告警监视；电压和环境温度的监视 支持风扇模块热拔插
管理和监控	支持 SNMP V1/V2/V3、Telnet、RMON、SSH2.0 功能 支持缓存微突发监控 支持缓存状态监控，识别流量微突发情况 ▲支持 SLICE 切片功能； 支持配置回滚 支持 sflow ▲微分段支持 65535 个组，支持 131060 个成员； 支持 INT 流量可视化功能 支持 ERSPAN 增强，支持采样和截断测试 支持 Telemetry（GRPC）
安全特性	支持 IP/ARP/ICMP 安全 支持配置文件国密加密； 支持安全 boot，主用 boot 故障时，采用备用 boot 进行启动； 支持硬件层级双 boot，采用两个 FLASH 芯片存储 boot 软件（系统引导程序），实现硬件级 boot 冗余备份，避免因 FLASH 芯片故障导致交换机无法启动； 设备的端口安全支持授权双栈自定义 ACL 功能； 支持 MOD：丢包镜像 支持全端口 256bits MACsec 加密 支持国密算法、具备国密检测能力 端口光功率异常检测
网络分析	支持 10G/25G/40G/100G/400G IPFIX/Netstream 1:1 采样功能； 支持基于会话的 Netstream 功能； Netstream 支持出入方向过滤；
VxLAN	支持 VXLAN over IPv6 支持 IPv6 VXLAN over IPv4 支持 VxLAN OAM: VxLAN ping, VxLAN tracert 支持 BGP EVPN 协议 微分段实现 IPv4 服务链（Service chain）功能 微分段实现 IPv6 服务链（Service chain）功能
▲实配	满配电源、风扇，配置 22 个 10G 多模光模块，一根 5m 40G QSFP+堆叠线

4.6 云带外管理交换机

要求采购、安装、集成实施 1 台设备，具体参数要求如下：

指标分类	详细技术参数
▲交换容量	≥2.4Tbps
▲转发性能	≥660Mpps
硬件规格	高度 1U，固定接口交换机 支持双电源，2 风扇模块 1 扩展插槽
▲软件规格	整机最大路由地址表≥80K 整机最大 ARP 地址表≥64K

	整机最大 MAC 地址表≥320K
▲端口实配	实配 100/1000Base-T 电接口≥48 个，1/10 GE 光接口≥4 个，满配电源、风扇
三层功能	支持 IPv4 静态路由、RIP、OSPF、ISIS、BGP 支持 IPv6 静态路由、RIPng、OSPFv3、ISISv6、BGP4+ 支持 IPv4 和 IPv6 环境下的策略路由 支持 IPv6 手动隧道、6to4 隧道和 ISATAP 隧道
▲防火墙插卡	要求设备支持防火墙插卡，提供证明材料
▲多类型插卡	要求设备支持不同种类的业务插卡，提供证明材料
可靠性	支持 Smartlink、RSTP、MSTP、PVST 功能
访问控制策略	支持基于第二层、第三层和第四层的 ACL 支持基于端口和 VLAN 的 ACL
堆叠	最大堆叠台数≥4 台 支持通过标准以太端口进行堆叠 支持远程堆叠
VLAN	支持基于端口的 VLAN,支持基于协议的 VLAN;支持基于 MAC 的 VLAN 最大 VLAN 数(不是 VLAN ID)≥4094
链路聚合	支持链路聚合基本功能及聚合零丢包
镜像功能	支持本地端口镜像和远程端口镜像；支持流镜像
▲MACsec	支持全端口 256bit MACsec 加密功能，提供证明材料
M-LAG	支持跨设备链路聚合技术 DRNI/M-LAG
配置和维护	支持 SNMP V1/V2/V3、RMON、SSHV2 支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准

4.7核心域防火墙

要求采购、安装、集成实施 2 台设备，具体参数要求如下：

指标项	详细要求
▲硬件规格	采用国产化软硬件平台； 1U,内存≥8G、存储空间≥256G SSD，8 个千兆电口、4 个千兆光口和 4 个万兆光口,冗余电源,2 个扩展槽位；
▲性能指标	防火墙吞吐≥12G，并发连接≥300 万，应用层吞吐量≥10G，FW+IPS 吞吐量≥5G，FW+AV 吞吐量≥5G，FW+WAF 吞吐量≥1G，全威胁吞吐量≥2G，IPSEC VPN 吞吐≥700M；
路由交换	支持 RIP、RIPng、OSPF、OSPFv3、BGP4、QinQ、PIM-SM、PIM-DM、IPv6 静态和动态组播路由；
链路聚合	支持根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口轮询等条件进行链路聚合，提供不少于 10 种链路负载算法;
▲地址转换	支持源/目的 NAT、双向 NAT，支持源 IP 转换同一性；支持端口块地址转换和 EIM 地址转换，支持 NAT64、NAT46、NAT66 地址

	转换；（提供功能界面截图）
IPv4/IPv6访问控制	支持一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、时间、长连接、并发会话、IPv6扩展头、WEB认证、IPS、AV、URL过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、防代理、APT等功能调度,简化用户管理；
▲策略管理	提供策略变更信息管理功能，支持查看变更策略、变更动作、变更时间、修改人、登陆IP，支持对变更前后的策略进行直观对比，并能一键还原配置；（提供功能界面截图）
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，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库； ▲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；（提供功能界面截图）
DDOS防御	支持针对IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP等协议进行DDOS防护；支持预定义和自定义策略模板； ▲支持NTP DDOS防护，采用阀值检查、源/目的限流、源认证等方式综合进行NTP QUERY FLOOD、NTP REPLY FLOOD攻击防护；（提供功能界面截图）
病毒过滤	▲支持对HTTP/SMTP/POP3/FTP/IMAP/IM等协议进行病毒防御；支持对6级以上的压缩文件进行解压查杀；（提供功能界面截图） 包含专业版快速查杀病毒库3年升级许可和IDP攻击规则特征库3年升级许可；
僵木蠕防御	▲支持独立的僵木蠕检测防御引擎，支持预定义僵木蠕规则库，特征总数在6000条以上，可对僵尸、木马、蠕虫、勒索软件进行防护；（提供功能界面截图）
黑名单	内置静态黑名单功能，可设置多个对象条件，如：五元组信息、源MAC、地址范围、应用、用户，实现对特定报文进行快速过滤；支持封禁HTTP代理X-Forward-For字段IP；
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，支持配置定时保存，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；
日志管理	支持日志本地存储，支持管理日志、系统日志、连接日志等日志类型存储，可对不同类型日志设置存储空间；可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数；
产品要求	具备防火墙密码检测证书；提供有效证书复印件 具备信息安全产品分级评估（EAL4+）；提供有效证书复印件

4.8堡垒机

要求采购、安装、集成实施 1 台设备，具体参数要求如下：

指标项	详细要求
▲硬件规格	采用国产化软硬件平台； 标准 2U 机架式，不少于 6 个千兆电口、4 个千兆光口、2 个万兆光口，硬盘容量≥4T，内存≥16G，USB 接口≥2 个，支持液晶屏，配备热插拔冗余电源；
性能指标	提供不小于 500 个资产管理授权许可；
▲身份认证	支持多因子认证，方式包括手机令牌、手机短信、动态令牌、国密 USBKey、指纹识别等；支持自动根据用户访问的源 IP 地址关联不同的认证方式，例如内网可直接密码登录、外网 VPN 拨号接入需使用双因子认证；（提供功能界面截图）
▲策略管理	支持对数据库协议访问操作进行控制，可基于库、表、命令实现对数据库操作的细粒度访问控制，执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行；（提供功能界面截图）
▲系统安全	支持内置文件病毒扫描，对本地上传文件到堡垒机网盘、主机上传文件到堡垒机网盘的传输过程进行病毒扫描；针对病毒文件可执行信任、删除等操作，并生成审计记录，防止运维场景下传输病毒文件威胁系统安全；（提供功能界面截图）
运维协议兼容	支持的运维协议包含 SSH、RDP、Telnet、VNC、FTP、SFTP、SCP、DB2、MySQL、SQL Server、Oracle、Rlogin、DM、Redis、PostgreSQL 等；支持 SSH、RDP、Telnet、VNC、FTP、SFTP、SCP 等协议资源账户密码自动登录（单点登录），无需用户手动输入账号或密码。
访问控制	支持同时以用户、用户组、账户、账户组为核心要素，设置多对多的资源访问授权，用户组和账户组内的新增成员可自动继承授权关系；支持按部门、用户、有效期、文件传输控制（上传、下载）、剪切板、水印、时间限制、IP 限制（黑、白名单）等条件进行细粒度访问控制。
命令控制	支持按用户、用户组、资源账户、账户组、操作命令、命令集、有效期、生效时段等条件，细粒度地设置命令操作权限；执行动作包括但不限于断开连接、拒绝执行、动态授权、允许执行、双人复核；支持通配符和正则表达式两种匹配方式。
资源账户改密	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；支持改密计划立即执行，执行前需要输入用户密码以确认身份。
审计与回放	支持对实时会话进行无延时的实时监控和切断；支持在线回放运维人员对资源的操作过程，播放速度支持最快 16X 快进，支持拖动、

	暂停、停止、跳过空闲、重新播放、截屏、切换会话等操作。
工单审批	支持通过访问授权工单向管理员申请需要访问的资源的权限，工单支持申请文件管理、剪切板、磁盘映射、水印、上传、下载等权限；支持设置多人审批模式或会签审批模式，支持开启终审节点审批，支持多级审批模式（最大支持 5 级）。
产品要求	具备网络安全专用产品安全检测报告/证书；提供有效复印件 具备计算机软件著作权登记证书；提供有效证书复印件 具备国家信息安全测评信息技术产品安全测评证书（EAL3+）；提供有效证书复印件

4.9日志审计系统

要求采购、安装、集成实施 1 台设备，具体参数要求如下：

指标项	详细要求
▲硬件规格	采用国产化软硬件平台； 2U，至少 8 个千兆电口、至少 8 个千兆光口和至少 2 个万兆光口，冗余电源,内存≥32G，系统盘≥256G Msata，数据盘≥4T，冗余电源；
▲性能指标	日志采集处理均值≥5000EPS。默认包含至少 50 个日志源授权；
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； 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； 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； ▲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；（提供功能界面截图） 支持对每个日志源设置过滤条件规则，自动过滤无用日志； 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；
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； ▲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；（提供功能界面截图） 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；
数据查询	▲支持为不同类型日志设置不同的查询条件和显示条件；（提供功能界面截图） ▲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；（提供功能界面截图） 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；
告警管理	▲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；（提供功能界面截图）
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。
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；

	▲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；（提供功能界面截图）
系统管理	支持用户按角色管理，支持三权分立； ▲系统具有防恶意暴力破解账号与口令功能，口令错误次数可设置，超过错误次数锁定，锁定时间可设置。（提供功能界面截图）
产品要求	具备信息技术产品安全测评证书 EAL3+；提供有效证书复印件 具备网络关键设备和网络安全专用产品安全认证证书；提供有效证书复印件

4.10数据库审计系统

要求采购、安装、集成实施 1 台设备，具体参数要求如下：

指标项	详细要求
▲硬件规格	采用国产化软硬件平台； 2U,内存≥32G，机械硬盘≥4T，至少 6 个千兆电口、4 个千兆光口、2 个万兆光口，冗余电源,至少 2 个扩展槽位；
▲性能指标	每秒新建连接：≥5W，整机吞吐：≥5.47Gbps；
数据库类型	支持国内外 40 余种主流数据库协议，包括国产化/非国产化的关系型数据库、非关系型数据库等； 支持 Cache、Hive、Hana、clickhouse、Tibero、Solr、MongoDB、HBase、ElasticSearch、Redis 等国际主流数据库系统；
细粒度审计日志	系统支持详细的审计日志，审计字段包括访问数据库的时间、源目 IP、源目端口、事件 ID、源目 MAC、应用协议、实名用户、规则名称、告警描述、数据库名、客户端程序、数据库用户名、SQL 语句、返回码、SQL 错误信息、影响行数、响应时间、返回结果集、业务 URL、业务用户名、SQL 操作类型、数据库表名、表影响字段、敏感类型等；
▲应用流量监控	支持审计各个应用协议的流量大小和数据包数量，并以图表形式进行排名；（提供功能界面截图）
▲会话回放	支持查看会话回放，支持倍速回放，至少包括 2 倍速、3 倍速、4 倍速等，完整还原数据库操作情况；（提供功能界面截图）
SQL 操作统计	支持以柱状图形式展示各类 SQL 操作数量情况。
▲SQL 效率分析	以饼图展示正常 SQL 与慢 SQL 分布占比情况、TOP10 慢 SQL 的详细分析：数据库用户名、源 ip、SQL 语句、SQL 操作类型、SQL 语句响应时间等要素；（提供功能界面截图）
▲敏感数据扫描与访问审计	支持用户数据库中敏感信息的自动发现和手动添加，可定位敏感数据所在数据库名、实例名、表名、列名，并形成针对敏感信息的检测规则；（提供功能界面截图）
高危异常操作行为分析	统计图表展示数据库高危操作行为统计，可直观展示针对数据库删库、删表等高危风险操作，并展示受影响数据库详情；
攻击行为分析	支持以折线图的方式实时展示 SQL 注入风险发生趋势和数据库漏洞攻击趋势，并以表格的方式展示 SQL 和数据库漏洞攻击注入统计信息和攻击详情；
数据库自动发现	支持从数据库流量中自动识别数据库，从流量分析结果中自动判别包含的数据库类型、版本、地址、端口、发现时间、会话时长、总事件数等信息，并且自动添加到待监控审计列表，无需用户提供网段、数据库地址等信息。
数据库监控	支持依据数据库实例监控各个数据的数据库类型、活跃会话数、

	总会话数、负载等信息
▲操作系统	安全操作系统采用冗余设计，可在设备命令行启动过程中选择主备系统。（提供功能界面截图）
安全浏览器管理	支持红莲花、密信等安全浏览器登录管理设备，该类浏览器支持国密算法 SM2/SM3/SM4，安全性非常高。
产品要求	具备网络关键设备和网络安全专用产品安全认证证书；提供有效证书复印件

4.11应用域防火墙

要求采购、安装、集成实施 1 台设备，具体参数要求如下：

指标项	详细要求
▲硬件规格	采用国产化软硬件平台； 2U,内存≥16G、机械硬盘≥4T，1 个 MGMT 口、1 个 HA 口、8 个千兆电口、4 个千兆光口和 4 个万兆光口,冗余电源,1 个扩展槽位；
▲性能指标	防火墙吞吐≥10G，并发连接≥300 万，每秒新建连接≥15 万，应用层吞吐量≥8G,FW+IPS 吞吐量≥1.5G,FW+AV 吞吐量≥1.5G，FW+WAF 吞吐量≥1.5G，全威胁吞吐量≥1G，IPSEC VPN 吞吐≥700M，IPSEC VPN 隧道数≥2000；
路由交换	支持 RIP、RIPng、OSPF、OSPFv3、BGP4、QinQ、PIM-SM、PIM-DM、IPv6 静态和动态组播路由；
链路聚合	支持根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口轮询等条件进行链路聚合，提供不少于 10 种链路负载算法；
地址转换	▲支持源/目的 NAT、双向 NAT，支持源 IP 转换同一性；支持端口块地址转换和 EIM 地址转换，支持 NAT64、NAT46、NAT66 地址转换；（提供功能界面截图）
IPv4/IPv6 访问控制	支持一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、时间、长连接、并发会话、IPv6 扩展头、WEB 认证、IPS、AV、URL 过滤、高级威胁防护、WAF、邮件安全、数据过滤、文件过滤、僵木蠕防御、审计、防代理、APT 等功能调度,简化用户管理；
▲策略管理	提供策略变更信息管理功能，支持查看变更策略、变更动作、变更时间、修改人、登陆 IP，支持对变更前后的策略进行直观对比，并能一键还原配置；（提供功能界面截图）
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，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库；

	▲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；（提供功能界面截图）
DDOS 防御	支持针对 IP、ICMP、TCP、UDP、DNS、HTTP、HTTPS、SIP、NTP 等协议进行 DDOS 防护；支持预定义和自定义策略模板； ▲支持 NTP DDOS 防护，采用阀值检查、源/目的限流、源认证等方式综合进行 NTP QUERY FLOOD、NTP REPLY FLOOD 攻击防护；（提供功能界面截图）
病毒过滤	▲支持对 HTTP/SMTP/POP3/FTP/IMAP/IM 等协议进行病毒防御；支持对 6 级以上的压缩文件进行解压查杀；（提供功能界面截图） 包含专业版快速查杀病毒库 3 年升级许可和 IDP 攻击规则特征库 3 年升级许可；
僵木蠕防御	▲支持独立的僵木蠕检测防御引擎，支持预定义僵木蠕规则库，特征总数在 6000 条以上，可对僵尸、木马、蠕虫、勒索软件进行防护；（提供功能界面截图）
黑名单	内置静态黑名单功能，可设置多个对象条件，如：五元组信息、源 MAC、地址范围、应用、用户，实现对特定报文进行快速过滤；支持封禁 HTTP 代理 X-Forward-For 字段 IP；
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，支持配置定时保存，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；
日志管理	支持日志本地存储，支持管理日志、系统日志、连接日志等日志类型存储，可对不同类型日志设置存储空间；可设置日志传输协议、外发时间类型、日志语言、合并传输、加密传输等参数；
产品要求	信息安全产品自主原创证明；提供有效证书复印件 防火墙密码检测证书；提供有效证书复印件 信息安全产品分级评估（EAL4+）；提供有效证书复印件

4.12WEB应用防火墙

要求采购、安装、集成实施 2 台设备，具体参数要求如下：

指标项	详细要求

▲硬件规格	采用国产化软硬件平台； 2U 机架式，内存≥16GB，硬盘≥2TB，1+1 冗余电源，千兆电口≥4 个，千兆光口≥4 个，万兆光口≥2 个；
▲性能指标	整机吞吐≥10Gbps，HTTP 应用层吞吐量≥8Gbps；HTTP 最大新建数≥30000 个；HTTP 最大并发数≥1000000 个；
数据防护	支持多条链路数据的防护，防护网段数量不限；支持 ipv4/ipv6 双协议栈；支持 4 层和 7 层服务器健康状态检查，7 层健康检查支持检测时间间隔配置、支持检测状态码选择（包括 2XX、3XX、4XX、5XX）、支持请求方法的配置（GET/OPTION）、支持健康检查路径及检查时间阀值的配置； ▲支持自动发现网络环境中存在的 Web 服务器，包括 HTTP 业务、HTTPS 业务。可记录服务器的 IP、端口、协议、IP 类型域名等信息。并且针对 HTTP 业务，可设置侦测后的自动部署，自动部署时，可选择防护模板、处理方式以及可选择开启阻断或观察模式；（提供功能界面截图） ▲支持 HTTPS 站点 SSL 算法自动探测功能。探测时可以设置指定站点及端口，可以显示探测结果。（提供功能界面截图）
攻击防护	支持注入式攻击防护，应包括 SQL 注入、PHP 代码注入、VBScript 注入、JavaScript 注入、OGNL 注入、SpringEL 注入、Csharp 注入、命令注入、文件注入、LDAP 注入、SSI 注入、Email 注入、Java 代码注入、SSTI 注入等。支持跨站脚本（XSS）防护。
敏感数据管理	支持对身份证、银行卡、手机号、信用卡号等个人敏感信息数据，可通过星号进行隐藏。支持自定义敏感词，防止提交政治敏感、违反法规相关的言论信息，保障网站的内容健康呈现。
客户端安全防护	▲支持客户端安全防护，能够通过 WAF 向服务器返回信息插入特殊的 HTTP 报头（包括 X-Frame-Options、X-Content-Type-Options、Content-Security-Policy，以客户端免受相应攻击。（提供功能界面截图）
CC 攻击检测	▲支持对 CC 攻击进行检测和防护，能够配置 URL 参数、请求头部字段、目的 IP、请求方法、地理位置组成的匹配条件；能够对请求速率、请求集中度、请求离散度进行检测。（提供功能界面截图）
盗链识别	支持多种盗链识别算法能有效解决单一来源盗链、分布式盗链、网站数据恶意采集等信息盗取行为，从而确保网站的资源只能通过本站才能访问。支持配置域名白名单。
Cookie 防护	支持针对特定的域名和 URL 进行无头浏览器、脚本扫描等行为的检测和阻断。支持通过签名、加密等方式防止 Cookie 被篡改。支持 Cookie 防劫持。
自定义检测	▲可对至少 20 种检测字段进行自定义规则，可选择匹配检测字段值或匹配检测字段个数。对于检测的字段支持解码能力，包括字母小写化、长度计算、路径归一化。（提供功能界面截图）
智能识别	支持语义分析能力，可对 SQL 注入、XSS、代码注入等攻击行为进行防护。支持智能识别攻击者，对发起攻击的 IP 进行自动阻塞，禁止其进行访问，可配置阻塞时间。
网页防篡改	支持网页防篡改，可选择需要防护的文件类型，应至少支持 30 种类型。防篡改能力需支持运行模式的选择，可选择学习模式，对网页内容进行学习；选择保护模式，对篡改后的网页进行恢复；选择仅检测模式对篡改行为进行告警。

产品要求	具备网络关键设备和网络安全专用产品安全认证证书；提供有效证书复印件 具备《信息技术产品适配性证书（XC 版）》；提供有效证书复印件

5、安全防护要求

本项目按照等级保护 2.0 三级要求进行设计和建设。根据云资源情况设计符合等级保护三级的相关安全防护措施并配合通过三级等保测试。

七、项目实施要求

1、实施原则

为保障项目的顺利实施，在项目实施过程应遵循以下原则：

1）规范性原则：投标人应采用项目管理方法，按照采购单位的要求在人员、质量和时间进度等方面进行严格管控。

2）标准化原则：项目实施过程应严格遵守国家、市和有关部门的相关法规、标准。

3）完整性原则：投标人应按照招标人的要求，保证实施内容、实施流程的完整性，保证实施过程科学完整。

4）保密性原则：在进行集成和实施过程中，投标人及实施工作人员应按照招标人的要求签署相关的保密协议，采取严格的管理措施，确保实施中涉及到的任何信息，不会泄露给第三方单位或个人，或利用这些信息损害招标人利益。

5）最小影响原则：投标人在实施过程中，应充分考虑项目实施对目标系统的正常运行可能产生的不利影响，并采取必要的措施将风险降到最低。

2、实施要求

1）在项目正式实施前，投标人应会同招标人及具体使用部门明确相关的实施方案、实施进度安排、过渡迁移对接方案和应急处置方案等内容，确保相关业务的正常有序运行。

2）投标人应按照项目技术要求和产品技术操作规范在合同签订后在承诺的时间内完成设备供货；5 个日历天内完成所有设备内完成设备安装、调试、连通、测试等工作。

3）安装过程中所需要的工具、配件、线缆、各类器件辅材、设备端口的使用许可等均由投标人负责提供。线缆部署需遵照招标人布线规范。

4）投标人负责协调解决本项目集成过程中出现的各类问题，对集成的进度、质量负总责，并牵头负责与既有软件投标人、集成商、运维服务投标人的沟通协调以及配合其他项目的建设实施。

5）投标人需提供与现有网络、安全、服务器、存储等设备的联调工作。

6）招标文件中硬件设备的配置或要求中出现不合理或不完整的问题时，投标人有责任和义务提出补充修改方案并征得招标人的同意后付与实施。

7）招标人聘请第三方监理单位参与项目全过程管理，投标人要接受监理单位的全程监管。

8）投标人应成立项目管理组织，严格遵守相关的业务管控、架构管控、项目管控的要求。

9）投标人应依据合同（含招标文件、投标文件等）完成设备到货点验文档的编制，并接受第三方监理单位的审核。

10）各节点设备到货点验、安装、加电、集成实施期间，第三方监理单位将对实施情况进行随机现场检查，投标人应配合完成相关工作。

11）投标人应提供合理的技术力量配置。

12）投标人应依据合同（含招标文件、投标文件等）完成最终验收文档的收集，接受第三方监理单位的审核。

13）项目建设期间，第三方监理单位将对投标人各项工作进行全程指导。

3、项目需求说明

1）投标人应充分理解开发需求的多样性，需求主要分类如下：

（1）业务流程、服务与管理创新导致的业务需求变化。

（2）技术创新或架构优化导致的架构变化。

（3）系统运行过程发现的问题。

（4）系统功能完善涉及的相关需求。

（5）招标人提出的其他优化需求。

2）投标人应严格遵守招标人的进度要求，按期保质保量完成，未经招标人同意完不成的，招标人有权追究投标人的相关责任。

4、技术要求

1） 投标人提供的产品必须是符合 XC 要求的产品。

2） 投标人在系统设计开发时，须至少满足如下技术标准：

GB/T 22239-2019 信息系统安全等级保护三级基本要求；

GB/T 25070-2019 网络安全等级保护三级安全设计技术要求；

5、项目团队及驻场人员要求

投标人必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 5 人的项目服务团队（包括项目经理、工程师等），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	项目管理，项目进度控制，组织各类资源申请流程，审核技术文档，汇报项目进度	1 人	具备信息技术应用创新专业人员证书或具备信息系统项目管理师（高级）或 PMP 证书，承担过同类工程项目的实践经历。	驻场
技术负责人	负责项目整体技术指导	1 人	具备信息技术应用创新专业人员证书或具备信息系统项	不驻场

			目管理师(高级)或 PMP 证书，近 3 年承担过同类项目的实践经历，指导工程师完成实施部署。	
实施工程师	负责项目实施工作，服务器上架、网络配置等	3 人	熟悉 XC 信息化软硬件，并能熟练完成部署，协助项目经理完成项目实施工作。	驻场

6、质量保证要求

投标人需采用国际通用的信息化项目实施和项目管理方法，提供完整的质量保证体系，对项目实施的全过程进行监控和管理，对项目进度和工程实施进度进行控制；所有的技术文件应是中文，并且本项目所有文档应该按照所使用的质量管理体系要求编写。投标方应提出对所投产品质量的承诺。

1、投标人应成立专门的质量保证组，明确质量保证组所要进行的质量保证活动。投标书中需详细列明项目实施单位（或办事处、技术支持服务中心等）地址、负责人、联系电话（包括手机和固定电话）、人员状况和相关证明文件等。

2、投标人应制定专门质量保证计划，明确质量保证活动与整个系统生命周期中各个阶段的关系，并选择合适的质量保证工具。

3、投标人需承诺在质量保证期向招标人提供质量保证，并提供有关证明。

4、投标人在应答时应详细阐述所提供技术支持的内容与范围。技术支持范围至少包括运维支持、软件升级、性能调优、设备维修、备品备件、技术咨询、各种突发事件的应急策略、定期巡检等。

5、投标人应向招标人提供一站式服务，即一点受理后，应负责全程跟踪服务。

6、投标人在招标人事先告知的关键服务期，应提供重点保障服务。

7、投标人应承诺按照采购单位系统运维体系的管理规定，不断调整和优化其运维服务的方式，确保满足系统运维管理的要求。

8、原厂商需有完善的质量保证体系，能够向设备所在地用户提供统一快捷的技术质量保证支持服务。

9、在质量保证期内应对设备及系统运行情况进行巡检，提供预防性维护服务。

10、应有完善的备品备件库体系，以满足本项目中最终用户单位建设期内对备品备件的需求，为完成本项目技术支持服务需求提供可靠保证； 投标人需提供备品备件库负责人、联系方式（包括手机和固定电话）和相关证明文件（照片等）

11、投标人和原厂商应向招标人提供电话、E-Mail 和 Internet 网站技术支持方式，并应建立提供专门的服务号码和账户，原厂商应向用户单位提供 7×24 小时授权工程师电话响应服务。能够在互联网站上查询、下载相关技术资料、提交问题并获得支持。E-MAIL 最迟次日回复。用户需要时应提供现场服务。

12、质量保证期（所有软件质保 3 年，硬件设备质保 5 年）内，应由专业技术人员负

责对设备进行现场维修更换，更换的设备或部件应是来自原厂商的全新同型设备或备件，不得以其它方式替代。

13、现场维修时含有数据的硬盘、磁带等存储类零部件不得带出机房，维修更换下来的此类部件所有权归用户单位所有。

14、故障解决后 12 小时内，投标人及原厂商应向用户单位提交故障处理报告。说明故障种类、故障原因、故障解决中使用的方法及故障损失等情况。按季向招标人提交上期故障受理报告、故障分析报告和汇总情况。

15、以上质量保证内容在合同规定的质量保证期内提供(上门费、备件费、人工费及相关费用含在产品报价中)。

16、设备的扩容升级：招标人如对设备进行扩容时，投标人应提供所需配件和相应服务，费用不高于本次中标协议中的价格和折扣优惠。

17、后续追加采购：在本项目质量保证期内，招标人如对本项目所涉及的设备及软件进行后续追加采购时，所需软硬件、系统集成和质量保证期服务价格均应不高于本次中标协议中的价格和折扣优惠。

7、技术文档要求

1、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。

2、所有的技术文件应用中文书写或有完整的中文注释，并符合有关归档要求。项目最终验收后全部移交招标人进行归档。

8、培训要求

1、投标人应提供本项目相关的各类软硬件产品及相关技术培训，以确保招标人指定的运维管理人员能完全掌握本项目所建内容的整体架构、设备配置和部署情况、日常管理、操作使用为最终目标。

2、投标人应根据以上培训目标提出具体的培训方案与计划，在中标后提供全套培训教材及课件。

3、培训方式：培训方式可包括集中讲课、操作示范、参观学习和其他相应的业务指导和技术咨询等形式。2 次集中授课，需要涵盖各应用系统、软硬件设备的操作与使用等。

4、集中授课培训师资要求：中级工程师以上，具备相关项目建设和实际授课经验。

5、集中授课培训人数：招标人可根据不同课程按需增减人数。

6、培训地点：由招标人与中标单位另行商定。

7、培训完成时间要求：集中培训应在项目交付使用后两个月内完成，招标人要求推迟的情况除外。

8、培训费用：本项目所有培训相关费用应已包含在总报价中。

9、验收要求

本项目按下述方式开展验收。

1、验收前，投标人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，确保所有设备能够正常运行且已达到本项目约定的各类标准要求。

硬件设备需上架加电测试通过，并完成网络布线。按项目实施计划进行设备到货、点验、开机加电、测试、布线、调试等，保证硬件设备运行正常。

满足验收条件后，投标人应以书面形式向招标人递交验收申请，由招标人按照本项目的约定组织本项目的验收。

2、软硬件设备验收需要按标书要求对全部设备的型号、规格、数量、外型、包装及资料、文件（如装箱单、保修单、随箱介质等）进行验收。在设备及配套软件验收时发现产品损坏、数量不全、型号规格不符等问题，投标人应及时解决。招标人有拒收和追究赔偿责任的权利。

3、投标人须保质保量、按整体解决方案如期完成该项目全部工作，并满足相关要求。

投标人应按照招标人要求，移交本项目实施过程中的各类文档，并经过招标人验收签字。

4、如果属于投标人原因致使本项目未能通过验收，投标人应当排除缺陷，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投标人自行承担。

5、如果由于招标人原因导致本项目在验收通过前出现故障或问题，投标人应及时配合排除该方面的故障或问题。

6、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），招标人有权解除项目，并有权依照本项目约定的违约条款追究投标人的违约责任。

八、其他要求

1、投标人及参与项目的所有人员应严格遵守招标人的保密要求签订保密协议,参与人员由投标人担保。保密期限不受本项目期限的限制，在本项目履行完毕后，保密信息接受方仍应按照国家有关规定承担保密义务。

2、投标人应自行配备必要的硬件设备和软件工具，如计算机、工具软件等。

3、投标人应协助用户制定本项目所建设系统相关运行、维护、管理规范，并提供相关咨询、建议服务。

4、投标人应熟悉我国政府以及企业信息化发展要求和国产相关要求，并具备类似信息化建设项目实际经验。

5、投标人应在合同约定的时间内提供本项目中规定的全部内容，承诺与本项目的相关单位，进行积极主动的合作。

6、投标人在实施过程中应服从招标人的统一协调，招标人有权裁决项目执行各方的

责任范围，投标人应无条件执行，并在规定的时间内解决问题。如果任意一方不配合招标人工作，严重影响工程进度、造成严重后果，招标人有权退货、索赔或拒付款项。

7、对本项目内由投标人采购的第三方工具软件，投标人应提供原厂商售后服务承诺，并承诺提供本项目实施过程中所需的原厂商服务，同时承诺不得有知识产权纠纷。

8、为保障项目能够及时完成，并保证项目完成的质量，减少建设风险，投标人所提供的主要设备系统应为成熟产品，并在投标方案中提供该产品在类似项目中的成功应用案例。

9、投标人投标报价应至少满足本软硬件清单，对于未列出的但对系统的正常运行和维护必不可少的设备、配件、软件、线缆及其它辅助材料等，投标人有责任给予补充，并应同其它设备一并报价，且包含在投标总报价中。

10、项目采购产品必须采用 XC 产品，并符合信息系统安全可靠管理要求。

九、售后服务要求

1、投标人是本项目技术支持与售后服务的主要承担者和责任人。在服务的实施过程中，要求投标人应能提供及时、高效的技术支持与售后服务，确保工程能按设计方案的各项指标要求和实施计划顺利完成，并在工程验收合格后，系统能长期稳定运行。

2、技术支持与售后服务的范围包括本项目所涉及的所有软硬件产品。本项目涉及的所有软件产品提供三年质保服务，硬件产品提供五年质保服务，需出具承诺函。

3、投标人在本项目验收通过之日起一年内需提供一名运维工程师驻场技术支持，且未经招标人同意不得更换，需提交具体驻场人员名单及资质、近三个月社保缴纳证明，以及加盖单位公章的承诺函。投标人对本项目内涉及的所有软硬件产品提供 7*24 小时免费技术支持和售后服务，对产品故障做到 15 分钟响应，30 分钟到现场，2 小时内解决。不能解决的提供替代解决方案。

十、投标人资质要求

1、符合《中华人民共和国政府采购法》第二十二条规定的投标人。

2、根据《上海市政府采购投标人登记及诚信管理办法》已登记入库的合格投标人。

3、本项目面向大、中、小、微型等各类投标人采购。

4、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。

十一、违约责任

1、如投标人未按约定的时间或服务标准完成建设工作，招标人可要求投标人在规定

的时间内采取补救措施。投标人还应向招标人支付本项目费用总额10%的违约金，违约金不足以弥补招标人损失的，招标人有权要求投标人赔偿超过部分。

2、因投标人违反保密义务或知识产权约定的，招标人有权要求投标人支付本项目费用总额10%的违约金，违约金不足以弥补招标人损失的，招标人有权要求投标人赔偿超过部分。若投标人违反保密义务，招标人还有权立即单方解除合同而不承担任何违约责任。

3、投标人有其他违反本项目合同约定的行为，投标人应当支付本项目总价款金额的10%作为违约金，违约金不足以弥补招标人损失的，招标人有权要求投标人赔偿超过部分。

4、投标人有下列情形之一，招标人有权解除合同：

因投标人服务质量问题导致招标人无法实现目的。

擅自转让或者分包其应履行的义务的。

违反或者未履行本项目合同约定的其他相关义务，且在招标人要求的合理时间内未能纠正的。

十二、付款方式

1、合同签订生效后且招标人收到中标人开具的等额[增值税普通]发票后的五个工作日内，支付合同总价款的30%。

2、所有设备到货通过验收且招标人收到中标人开具的等额[增值税普通]发票后十个工作日内支付合同总价款的 50 %。

3、本项目通过终验后且招标人收到中标人开具的等额[增值税普通]发票后的十个工作日内，支付合同总价款的 20 %。