**第二章项目采购需求**

一、说明

**1 总则**

1.1 供应商应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由供应商自行负责。

1.2 供应商提供的货物和服务应当符合磋商文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。所提供的货物应当是全新的、未使用过的。

1.3 供应商在磋商前应认真了解项目的实施背景、应提供的服务内容和质量、项目考核管理要求等，一旦成交，应按照磋商文件和合同规定的要求提供相关服务。

1.4供应商对所提供的货物和服务应当享有合法的所有权，没有侵犯任何第三方的知识产权、商业秘密、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。如采购人使用该服务构成上述侵权的，则由成交供应商承担全部责任。

1.5供应商应如实准确地填写参加磋商货物的规格型号、技术参数、品牌、产地等相关信息，因上述信息内容填写不完整、不准确，而导致响应文件被误读、漏读，由供应商自行负责，为此供应商需承担其响应文件在评审时被扣分甚至被认定为无效响应的风险。

★1.6若本项目涉及国家强制认证产品（信息安全产品、3C认证产品、强制节能产品、电信设备进网许可证等），则根据国家有关规定，供应商提供的产品必须满足强制认证要求。（详见第一章磋商须知及前附表17.2（6））

★1.7供应商提供的产品和服务必须符合国家强制性标准。

1.8采购人在技术需求和图纸或图片（如果有）中指出的工艺、材料和货物的标准以及参照的技术参数或型号仅起说明作用，并没有任何限制性和排他性，供应商在响应文件中可以选用其他替代标准、技术参数或型号，但这些替代要在不影响功能实现的前提下，并在可接受范围内接受偏离。

1.9供应商应根据本章节中详细技术规格要求，采用市场主流产品或按照要求提供定制产品参加磋商。同时，请供应商务必注意：无论是正偏离还是负偏离，都不得与磋商要求相差太大，否则将可能影响供应商的得分。一旦成交，供应商应按响应文件的承诺签订合同并提供相应的产品和服务。

1.10本项目如涉及软件开发，则开发软件（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）的全部知识产权归采购人所有。供应商向采购人交付使用的软件系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。支撑该系统开发和运行的第三方编制的软件的知识产权仍属于第三方。如采购人使用该软件系统构成上述侵权的，则由供应商承担全部责任。

1.11供应商认为磋商文件（包括磋商补充文件）存在排他性或歧视性条款，可在收到或下载磋商文件之日起五个工作日内提出，并附相关证据。

二、项目概况

**2磋商范围与内容**

2.1 项目背景及现状

浦东新区生态环境局中心机房（以下称局中心机房）包括灵山路28号一楼核心机房和二楼小机房，面积约为40㎡。局中心机房按照二级机房标准建造，于2008年建成投入使用。局中心机房所处房屋为公园附属临时建筑，该建筑为两层钢架结构简易用房，系统升级改造时应考虑到房屋结构的特殊性，提前做好房屋承重情况的调查，并在保证整体建筑安全的情况下进行升级改造，过程中应对建筑薄弱部分结构进行加固处理。

局中心机房于2008年建成投入使用，承载着9个综合应用及业务系统，由40余台服务器，60余台虚拟机，3套异构存储系统，6个异构集群系统（VMware集群、Hyper-v集群和数据库集群），网络安全设备，不间断电源以及精密空调组成。对保障局业务工作正常开展、确保局信息安全起着重要的支撑作用。为提升局中心机房的服务能力和稳定运行能力，拟对局中心机房内与信息化系统运行相关的机房设施系统、安全系统、网络系统、存储系统和局财务系统进行全面升级改造。

2.2 项目磋商范围及内容

本项目为生态环境局中心机房安全升级改造，包含机房设施系统升级改造、机房网络安全系统升级改造、机房网络系统升级改造、机房存储系统升级改造、局财务系统机房区域升级改造等。

2.3 本项目服务期限为自合同签订后90天内完成系统的升级改造工作并通过验收，相关的备货工作在合同签订后15天内完成。。

**3承包方式**

3.1 依照本项目的磋商范围和内容，成交供应商以包质包量、包安全可靠的方式实施项目承包。

3.2 本项目不允许分包。

**4合同签订方式**

4.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与磋商文件和成交供应商响应文件的内容一致，并互相补充和解释。

**5结算原则和支付方式**

5.1 结算原则

5.1.1 本项目合同总价不变，采购人不会因政策性调价、人工成本、材料、设备使用年限增长引起的维修成本增加和效能衰减等因素（不可抗力除外）的变动而进行调整。

5.1.2发生设备维修的，如该设备尚在质保期内的，采购人不另行支付相关费用；如在质保期外的，单价按照响应文件中明确的备品备件单价（含维修人工费）计取，数量按实结算。如响应文件中没有类似备品备件单价可参照的，则有合同双方协商确定维修单价。

5.2 支付方式

5.2.1 本项目合同金额采用**分期付款**方式，在采购人和成交供应商合同签订后，按下款要求支付相应的合同款项。

5.2.2 分期付款的时间进度要求和支付比例具体如下：

（1）合同签订后30日内，支付合同金额50%的预付款；

（2）项目所需所有货物到货后30日内，支付合同金额的40%。

（3）项目验收结束后30日内，支付合同尾款。

5.3成交供应商因自身原因造成返工的工作量，采购人将不予计量和支付。

5.4采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时1年期贷款市场报价利率。

三、技术质量要求

**6适用技术规范与规范性文件**

各供应商应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本磋商文件中列明，供应商应无条件执行。标准、规范等不一致的，以要求高者为准。

**7磋商内容与要求**

7.1 工作目标与总体要求

（1）以先进成熟的计算机和通信技术为主要手段，在新区生态环境局已有网络信息系统的基础上，加强网络管理，提高新区生态环境局业务系统内各个单位的业务应用的高可用性，避免单点故障可能性。提高整体网络的稳定和可靠性。选择安全可靠的服务器、存储设备并充分利用现有资源重新搭建新区生态环境局各业务系统，实现虚拟化数据中心和备份中心。使其既能满足现有业务需求，又能满足未来3-5年业务发展需求。

（2）通过局中心机房安全升级改造项目的规划建设，使得新区生态环境局业务系统性能达到一定的高可用性、稳定性，从而保证相关的内部系统能够在一个高效、安全、稳定的平台上运行，从而为新区生态环境局业务信息化的推进和发展奠定坚实的基础和保障。

（3）根据上级部门相关文件要求，要求各单位对重要信息系统安全开展等级保护定级工作。通过此次局中心机房安全升级改造，改善局财务系统的硬件环境和网络环境，提高系统安全性，以符合等级保护的相关要求，做好我局财务系统的安全等级保护定级工作。

7.2 本项目磋商内容与具体质量要求（但不仅限于）详见下表。

**服务内容一览表（工作量清单）**

项目名称及包件号：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **具体内容** | **数量** | **工期** | **备注** |
| 1 | 机房设施系统升级改造 | 1项 | 90天内 |  |
| 2 | 机房网络安全系统升级改造 | 1项 | 90天内 |  |
| 3 | 机房网络系统升级改造 | 1项 | 90天内 |  |
| 4 | 机房存储系统升级改造 | 1项 | 90天内 |  |
| 5 | 局财务系统机房区域升级改造 | 1项 | 90天内 |  |

**说明：此表所列内容为本次磋商核心工作内容，供应商不得缩减。**

7.3具体服务内容

7.3.1建设要求

（1）机房设施系统升级改造

1）机房防静电系统和安全设施系统升级改造

目前机房设施系统已经超过14年，系统设备的稳定性大幅下降。机房防静电系统、机房照明系统、机房供配电系统和机房消防系统都存在老化和缺失现象。对现有的机房防静电系统、机房照明系统、机房供配电系统和机房消防系统进行升级改造，替换所有机房设施系统，保证机房设施系统安全，稳定运行。

2）UPS系统和供配电系统升级改造

根据局财务系统机房区域布局需要，负责调整UPS系统、配电系统和空调系统等系统位置；本系统升级改造涉及采购新的蓄电池替换现有蓄电池，并对蓄电池的电路接线、供电线路、供配电箱和相关电气系统全部进行升级改造，保证机房UPS和供配电系统安全，稳定运行；为2F机房单独采购一套UPS系统和电池，并完成相关供配电线路升级改造。

（2）机房网络安全系统升级改造

根据网络安全等级保护测评的要求，对机房的网络安全系统进行升级改造。本系统升级改造涉及到安全网关系统、采购日志审计平台、堡垒机系统、数据库审计平台、主机安全管理系统和APT攻击预警平台，根据采购人要求完成安全系统的升级改造工作，保证网络边界的安全性。

（3）机房网络系统升级改造

本系统升级改造包括通信网络系统和光纤存储网络系统升级改造，优化机房网络架构，扩容机房网络资源。

（4）机房存储系统升级改造

本系统升级改造包括分布式存储系统和现有存储系统升级改造，优化机房存储架构，扩容机房存储资源，老系统数据迁移。

（5）局财务系统机房区域改造

对机房布局需要重新规划，升级改造局财务系统专用区域，为局财务系统配备专用设备和网络。机房区域改造需要将机房配电柜、UPS主机和电池柜、机房空调和现有机柜位置进行调整。局财务系统专用区域内需要新采购2个标准机柜（含KVM系统）和1台财务系统专用交换机，并负责新机柜的强、弱电系统和硬件设备安装调试工作；还要预留精密空调的专用区域。

7.3.2具体升级改造要求

（1）机房设施系统升级改造内容

1）机房防静电系统和安全设施系统升级改造要求

对现有的机房防静电系统、机房照明系统、机房供配电系统和机房消防系统进行升级改造，替换所有机房设施系统，保证机房设施系统安全，稳定运行。本系统升级改造涉及到更换吊顶、防静电地板、LED照明灯（带应急照明）及照明电缆、市电配电柜及电缆、消防气瓶及阀门和消防药剂，升级改造要求如下：

①升级改造前要求制定切实可行的升级改造方案，充分考虑现场环境和升级改造难度；升级改造前要求制定切实可行的机房断电、断网和系统意外中断等突发事件的应急预案。升级改造期间要求供应商对机房各信息系统和机房硬件设备的运行状况进行实时监控，做好故障预防和风险排除工作，确保在工作时间机房内所有信息系统正常运行。

②升级改造期间机房需要断电或者断网的，供应商必须将升级改造放到周末、节假日进行，且连续断电（断网）时间不能超过24小时；供应商必须全面负责由于升级改造原因停电（断网）而造成的机房内所有系统和设备的停机和启动工作，保证机房内所有系统数据安全，保证数据的一致性和完整性，保证机房内所有系统设备启动、运行正常。如果因为断电（断网）给采购方及用户造成损失和影响的，由供应商负责消除影响，由此造成的损失，采购方有权要求供应商赔偿。

③升级改造期间涉及局中心机房信息系统需要暂停的，供应商应负责协调相关应用软件服务商，制定切实可行的系统暂停方案，确保系统暂停安全顺利实施，供应商不得以应用软件服务商不配合为由进行推脱。如果因为系统暂停给采购人及用户造成损失和影响的，由供应商负责消除影响，由此造成的损失，采购人有权要求供应商赔偿。对于供应商以此为推脱，或者由此造成升级改造延误的，采购人有权终止合同，扣除全部项目费用，并要求供应商承担违约责任，并赔偿相应的损失。

④升级改造期间涉及局中心机房硬件设备需要移机的，供应商应负责协调相关硬件服务商，制定切实可行的硬件移机方案，确保系统暂停安全顺利实施，供应商不得以硬件服务商不配合为由进行推脱。如果因为硬件移机给采购人及用户造成损失和影响的，由供应商负责消除影响，由此造成的损失，采购人有权要求供应商赔偿。对于供应商以此为推脱，或者由此造成升级改造延误的，采购人有权终止合同，扣除全部项目费用，并要求供应商承担违约责任，并赔偿相应的损失。

2）UPS和供配电系统升级改造要求

根据局财务系统机房区域布局需要，负责调整UPS系统、配电系统和空调系统等系统位置；本系统升级改造涉及采购新的蓄电池替换现有蓄电池，并对蓄电池的电路接线、供电线路、供配电箱和相关电气系统全部进行更换，保证机房UPS和供配电系统安全，稳定运行；为2F机房单独采购一套UPS系统和电池，并完成相关供配电线路升级改造。升级改造要求如下：

①设计规划：根据局财务系统专用区域规划情况，升级改造同时调整相关系统位置，需要调整的系统涉及到配电柜、UPS主机和电池柜、机房空调和现有机柜。

②升级改造要求：同上“1）机房防静电系统和安全设施系统升级改造要求”相关升级改造要求。

（2）机房网络安全系统升级改造内容

本系统升级改造涉及到安全网关系统、日志审计平台、堡垒机系统、数据库审计平台、主机安全管理系统和APT攻击预警平台，保证网络边界的安全性。

采购的所有安全系统都要能够相互联动，组成一个安全联动防护系统。

在安全系统升级改造完成后，供应商需要对采购人指定人员进行培训，培训主要内容包括安全系统安装、安全系统配置、安全系统管理、安全技术培训等方面。

1）安全网关系统升级改造要求

①安全网关系统建立双活冗余架构，完成对安全网关系统的安装部署和调试工作，并确保机房所有信息系统在不变动自身网络设置的情况下都正常运行。

②在安全网关系统安装前，供应商需要将现有安全设备进行拆卸。要求将现有安全设备的相关设置和安全策略全部导出保存并移植到采购安全网关系统中，并确保所有安全设置能够正常作用。

③现有安全设备利旧

将替换下来的现有防火墙布置到临港机房内环评公示网站前端，根据现有系统情况设置相关安全防护功能。

2）日志审计平台升级改造要求

完成对日志审计平台的安装部署和调试工作，并确保机房所有信息系统在不变动自身网络设置的情况下日志审计平台都正常收集日志。

3）堡垒机系统升级改造要求

完成对堡垒机系统的安装部署和调试工作，并确保机房所有信息系统在不变动自身网络设置的情况下堡垒机系统都正常运行。

4）数据库审计平台升级改造要求

完成对数据库审计平台的安装部署和调试工作，并确保机房所有信息系统在不变动自身网络设置的情况下数据库审计平台都正常收集日志。

5）APT攻击预警平台升级改造要求

完成对APT攻击预警平台的安装部署和调试工作，并确保机房所有信息系统在不变动自身网络设置的情况下APT攻击预警平台都正常运行。

6）主机安全管理系统升级改造要求

完成对主机安全管理系统的安装部署和调试工作，并确保机房所有信息系统在不变动自身网络设置的情况下主机安全管理系统都正常运行。

（3）机房网络系统升级改造内容

本系统升级改造包括通信网络系统和光纤存储网络系统的升级改造，优化机房网络架构，扩容机房网络资源。

通信网络系统升级改造涉及的网络交换机系统必须与现有网络交换机相互兼容，并支持IRF2智能弹性架构, 与现有核心网络设备虚拟化为一台逻辑设备。负责将机房现有系统设备接入网络交换机系统，升级改造过程中确保系统数据安全。

光纤存储网络系统升级改造涉及的光纤存储网络交换机系统必须与所有存储系统和关联服务器相互兼容。负责将机房所有存储系统和关联服务器接入光纤存储网络交换机系统，升级改造过程中保证存储系统和关联服务器数据安全。

在网络系统升级改造完成后，供应商需要对采购人指定人员进行培训，培训主要内容包括系统安装、系统配置、系统管理等方面。

1） 通信网络系统升级改造要求

完成对通信网络系统的升级改造工作，要求将网络交换机系统接入到现有核心交换机中，通过IRF2技术虚拟化为一台逻辑设备。对机房网络进行优化、分级，增加核心交换机处理性能，并确保机房所有信息系统在不变动自身网络设置的情况下都正常运行。

2）光纤存储网络系统升级改造要求

完成对光纤存储网络系统的升级改造工作，光纤存储网络交换机系统做双链路冗余替换现有的光纤存储网络交换机，确保存储数据链路正常运作，同时兼容现有存储系统和服务器，确保机房所有信息系统在不变动自身系统设置的情况下都正常运行。

（4）机房存储系统升级改造内容

本系统升级改造包括分布式存储系统和现有存储系统升级改造，优化机房存储架构，扩容机房存储资源。

分布式存储系统需要兼容现有的硬件设备，支持在异构存储系统环境中从现有存储系统上复制、迁移数据，对云和虚拟化技术进行优化，后台易用易管理。

分布式存储系统升级改造要结合业务系统的实际情况，合理规划部署新老存储系统，保证数据存储安全，保证数据的一致性和完整性。分布式存储系统必须与现有服务器相互兼容。供应商负责将机房服务器接入分布式存储系统，完成新老存储系统之间的数据迁移工作，升级改造过程中必须保证存储系统和服务器数据安全。

在存储系统升级改造完成后，供应商需要对采购人指定人员进行培训，培训主要内容包括系统安装、系统配置、系统管理等方面。

1）分布式存储系统升级改造要求

完成对分布式存储系统的升级改造工作，通过 iSCSI 协议完成挂载，数据保护方式采用三副本保护，需要同时支持DAS、NAS、SAN、融合架构等技术，还需要保证VMware集群、Hyper-V集群和SQL Server集群的系统服务正常使用。

2）分布式存储网络系统升级改造要求

完成对分布式存储网络系统的升级改造工作，负责分布式存储系统与前端应用通过 iSCSI 协议完成挂载，同时兼容现有服务器。

3）现有存储系统升级改造要求

完成对现有存储系统的升级改造工作，增加现有存储系统的容量，同时保证现有存储系统和关联服务器的数据安全。

4）数据迁移要求

完成新老存储系统之间的数据迁移工作，升级改造过程中保证存储系统和服务器数据安全。数据迁移整体实施时间为周末2天，其中36小时为存储设备迁移服务商实施时间，剩余时间为数据迁移涉及到的第三方维护公司恢复和验证时间。如单次无法完成全部数据迁移工作将按照涉及业务系统分多次进行实时。每次实时均需要联系数据所涉及系统的第三方运维公司配合，配合工作所产生的所有费用均包含在本项目内。

（5）局财务系统机房区域升级改造内容

对机房布局需要重新规划，升级改造局财务系统专用区域，为局财务系统配备专用系统和网络。机房区域改造需要将机房配电柜、UPS主机和电池柜、机房空调和现有机柜位置进行调整。局财务系统专用区域内需要新采购2个标准机柜（含KVM系统）和1台财务系统专用交换机，并负责新机柜的强、弱电系统和硬件设备安装调试工作；还要预留精密空调的专用区域。

7.3.3具体技术指标

7.3.3.1机房设施系统升级改造

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **主要性能指标** | **数量** |
| 1 | 全钢防静电地板 | 600×600×32防火A1级 | 40平米 |
| 2 | LED平板灯(带应急照明） | 600×600LED | 14套 |
| 3 | 照明系统电缆管线 | 国产 | 150米 |
| 4 | 吊顶 | 国产 | 40平米 |
| 5 | 消防气瓶 | 更换消防气瓶及阀门和消防药剂 | 1套 |
| 6 | 二楼UPS主机 | 10KVA（含6节12V 65AH 蓄电池） | 1套 |
| 7 | 一楼UPS蓄电池 | 12V200AH 铅蓄免维护电池 | 60节 |
| 8 | 电池柜 | 定制A6电池柜(含开关） | 1项 |
| 9 | 市电自切柜（市电智能数显版安全门配电柜） | 定制 800\*450\*1600(含开关） | 1台 |
| 10 | UPS配电柜（一体化智能数显版安全型配电柜） | 定制 800\*450\*1600(含开关） | 1台 |
| 11 | 电气系统电缆管线 | 国产 | 200米 |

7.3.3.2机房网络安全系统升级改造

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **主要性能指标** | **数量** |
| 1 | 安全网关系统 | 详见“（1）安全网关系统参数要求”。 | 2台 |
| 2 | 日志审计平台 | 详见“（2）日志审计平台系统参数要求”。 | 1台 |
| 3 | 堡垒机系统 | 详见“（3）堡垒机系统参数要求”。 | 1台 |
| 4 | 数据库审计平台 | 详见“（4）数据库审计平台系统参数要求”。 | 1台 |
| 5 | APT攻击预警平台 | 详见“（5）APT攻击预警平台系统参数要求”。 | 1台 |
| 6 | 主机安全管理系统 | 包含1套主机安全及管理系统管理中心软件和14套主机安全及管理系统防护端软件，详见“（6）主机安全管理系统参数要求”。 | 1套 |

（1）安全网关系统参数要求如下：

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 性能要求 | 设备最大吞吐量≥3.5Gbps，HTTP吞吐量≥1.5 Gbps，IPS吞吐量≥600 Mbps，AV吞吐量≥600 Mbps，IPSec VPN性能≥900 Mbps，最大并发连接数≥140万，每秒新建连接数≥3万，IPSec VPN隧道数≥1000，SSL VPN接入数≥350 |
| 系统要求 | 标准1U专用千兆硬件平台，内置交流单电源，硬盘≥480GB HDD |
| ≥9\*GE电口，1\*Combo口；支持千兆接口总数≥10个 |

| **模块** | **指标项** | **技术参数** |
| --- | --- | --- |
| 系统部署 | 部署模式 | 支持网关模式、网桥模式、旁路模式、虚拟网线工作模式、混合模式；部署模式切换无需重启系统 |
| 双机热备 | 支持双机热备，支持主备模式和主主模式；支持同步配置、运行状态、特征库等；支持配置抢占模式和抢占延时 |
| 网络特性 | NAT | 支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换。 |
| 路由支持 | 支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目的地址、用户、服务、应用、时间、域名的策略路由 |
| 链路负载均衡 | 支持基于7元组、域名的链路负载均衡策略；负载方式支持带宽、优先级和权重；支持接口过载保护、会话保持和链路健康检查，会话保持可实现用户的访问请求均分配至同一出口。 |
| 支持基于负载链路的出接口的DNS请求，主动完成DNS服务器替换，解决用户主机配置DNS解析结果与实际转发运营商链路解析结果有冲突，从而导致跨运营商访问慢的问题；支持进行DNS探测，针对探测失败情况，可选择禁用DNS-DNAT功能或禁用负载链路出接口。 |
| DNS | 支持DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载。 |
| IPv6 | 支持IPv6/IPv4双栈，支持IPv6安全策略、包括审计策略、NAT策略、流量控制策略、会话控制策略、黑名单、白名单、认证策略等 |
| 支持IPv6策略路由、OSPFv3、静态路由、IPv6隧道，包括IPv6手工隧道、ISATAP、6to4等隧道模式、支持IPv6网络下的DHCPv6、DNSv6、SNMPv6、NTPv6、PPPoE等基础协议 |
| 支持IPv6入侵防御、病毒防护、Web防护、风险扫描、安全分析、资产发现、弱密码防护等安全功能 |
| 安全防护 | 访问控制 | 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能。 |
| 入侵防御 | 系统定义超过8600+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型；以及对应IPS规则的攻击类型、严重程度、CVE编号、CNNVD编号、协议、操作系统、发布年份、漏洞厂商等详细信息；并支持在线升级和手动升级。 |
| 预置防护模板，可基于常见场景进行一键式的安全加固；支持基于常见协议进行异常检查，包括但不限于：HTTP、DNS、SMTP、POP3、FTP；检查内容支持自定义，包括但不限于：URL长度、请求长度、目录长度、Host字段、Version字段、字符检测、文本长度、文件名长度、命令参数长度，支持针对每协议设置处置动作和事件等级。 |
| 支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容；支持选择包含、等于、不等于、大于、正则匹配等匹配方式；可选择多种匹配条件，支持设置“与”和“或”的匹配顺序；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择重要等级。 |
| 支持日志聚合，可按照源IP、目的IP、防护规则和源目IP等维度进行聚合，方便管理员快速进行攻击事件统计和回溯。 |
| 支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者Syslog告警，不同告警规则可以发送给不同的用户。 |
| 支持针对攻击进行本地报文存储，方便管理员事后回溯攻击事件，支持针对某一个和某一类攻击设置报文存储机制；支持针对某一个和某一类攻击的源地址进行隔离，隔离时间可自定义。 |
| 病毒防护 | 支持HTTP，FTP，POP3，SMTP，IMAP协议的病毒查杀，支持查杀邮件正文/附件、网页及下载文件中包含的病毒，支持400万余种病毒的查杀，并支持在线升级和手动升级病毒库 |
| 支持对最多20级的压缩文件进行解压查杀。 |
| 端口扫描 | 支持针对IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能。 |
| 其他防护 | 支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，实现自动拦截；学习时长可选择1小时、12小时、一天、一周等。 |
| 失陷主机 | 支持通过木马、数据外传、间谍软件、病毒、挖矿等行为判断主机是否失陷；支持手动或者自动的方式将失陷主机加入到黑名单中，避免威胁在内网进一步扩散。 |
| 威胁情报 | 支持与多个威胁情报中心订阅，帮助产品实现检测、预警和防御。 |
| 提供在设备端上的全网威胁情报的搜索查询，包括IP、域名、文件（MD5/SHA1等）情报的查询。 |
| 支持针对内网进行威胁情报安全分析，支持以饼状图、柱状图等形式展示网络安全态势。支持针对资产维度进行数据下钻，分析维度包括但不限于资产、目的地址、威胁类型、威胁信息、威胁风险、命中次数、命中时间等，支持跳转至威胁情报平台，查看详细的威胁情报内容。 |
| 支持展示全球热门和新型的威胁事件，支持数据下钻查看该威胁事件的时间、威胁级别、描述、类型、应用措施和指示器等信息。支持针对威胁事件提供安全防护的配置向导，通过引导方式帮助用户完成安全加固，规避威胁风险。 |
| 协同防御 | 支持与EDR产品协同工作，实现终端在访问特定IP/网段时必须安装EDR，否则拒绝访问并重定向EDR的安装页面；可实时阻断EDR同步的风险主机的访问；并在与EDR产品联动后，增强防火墙对木马特征、内网资产的识别能力。 |
| 支持所投的APT产品协同工作，实现将APT分析到的SMB远程溢出攻击、扫描行为、Web后门访问、隐蔽信道通信、暴力破解、挖矿、远控工具利用、Web特征攻击等外部攻击源IP同步到本设备，通过本设备的黑名单功能实现自动阻断 |
| 安全分析 | 资产安全分析 | 支持内网资产自动发现功能，支持手动创建、导入和导出资产信息；支持展示内网资产的风险级别、IP、用户、部门、操作系统、重要程度、受攻击总数、来源等内容。 |
| 支持数据下钻至单资产风险详情，可自动关联该资产所有安全信息，安全信息包括但不少于：入侵防御、威胁情报、Web防护、病毒防护、防暴力破解、非法外联防护、弱密码防护、扫描攻击防御和行为模型等，支持以趋势图方式按时间展示各类安全事件的趋势，方便管理员快速了解资产安全状况，以便进行准确的安全防护。 |
| 攻击链可视 | 支持安全事件攻击链分析，以资产和攻击者两种角度关联所有安全事件，将攻击过程阶段化，分析和统计每个攻击阶段的攻击内容和攻击次数，支持针对每个攻击阶段进行数据下钻，支持分析攻击时间、攻击源、攻击目的、攻击事件、检测模块、攻击级别等信息，帮助管理员清晰了解APT攻击的攻击进度，及时在数据泄露前加固网络，针对已经数据泄露的情况，进行事件回溯，为后续网络加固提供数据支撑。 |
| 行为管控 | 应用识别 | 应用特征不少于7000个，移动应用不少于2200个。 |
| 可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（ZIP、RAR、GZ、BZ2、Z、TGZ、TBZ、7Z、CAB、BZ等）、应用程序、Office系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。 |
| URL识别与控制 | 内置URL分类库，支持≥56个URL分类，URL库可在线升级  支持自定义URL过滤，包括恶意URL白名单、恶意URL黑名单、URL白名单等，并支持URL的模糊匹配。 |
| 支持基于DNS前置技术实现在DNS解析阶段针对HTTP和HTTPS域名进行过滤，防止HTTPS域名过滤逃逸情况。 |
| 防私接路由 | 支持防网络共享行为，针对私接路由器和非法无线热点行为进行识别和阻断。 |
| 针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长。 |
| 数据分析 | 数据分析 | 支持用户全天行为分析，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息。 |
| 支持监控用户和应用实时流速，包括用户名、应用名、用户组、上行速率、下行速率、总速率、会话数等信息，帮助管理员快速甄别网络异常行为；支持数据下钻跳转至详细列表，针对用户支持通过趋势图形式，按照时间顺序展示该用户网络会话和流量趋势，支持下钻跳转至详细列表访问的应用组成和流速情况。针对应用支持通过趋势图形式，按照时间顺序展示该应用会话和流量趋势，支持下钻跳转至详细列表使用该应用的用户、速率和会话数等情况。 |
| 身份认证 | 用户认证 | 本地认证、Portal认证、Radius认证、LDAP认证、POP3认证、AD域单点登录、短信认证、微信认证、APP认证、二维码认证、互联网钉钉认证、混合认证和免认证，其中微信认证支持通过小程序获取手机号。 |
| 支持对接AC Controller、IMC、AAS、SMP、深澜、城市热点、PPPoE、安美等常见认证服务器。 |
| VPN | VPN | 支持标准IPSec VPN和快速IPSec VPN；同品牌设备快速IPSec VPN对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址。 |
| 支持IPSec VPN、SSL VPN、GRE VPN，支持手机、平板电脑等移动终端VPN接入，功能标配，无需增加功能授权即可使用 |
| 系统管理员支持与第三方服务器联动认证，第三方服务器包括但不限于Radius服务器、LDAP服务器。支持第三方服务器状态探测，根据服务器状态自动切换认证方式，服务器异常时，切换为本地认证，服务器恢复后使用外部认证。 |
| Web管理界面支持Ping、Traceroute、TCP SYN诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析 |

（2）日志审计平台系统参数要求如下：

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 性能要求 | 支持≥20个日志源（不支持扩展）；  日志处理能力≥EPS：150/秒 |
| 系统要求 | 标准1U硬件，1个console口  网口类别：≥5个千兆工作管理口(1管理口+1HA口+3审计口)  硬盘：≥1,5T\*1  内存：≥4G |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需代码开发。 |
| 支持kafka日志接收转发、大数据安全域同步、APT沙箱报告转发等大数据联调功能。Kafka收发支持SSL加密。 |
| 可通过接收协议限制日志接收速率，包括Http接收、syslog接收、SNMPtrap接收、TCP接收、WMI接收、aliyun接收。 |
| 支持对Agent进行统一管控，包括卸载、升级、启动及停止操作，支持将日志收集策略统一分发。 |
| 对日志样例可进行划词辅助解析，一键生成正则表达式 |
| 支持解析规则性能以界面列表形式显示，可了解解析耗时、解析成功或失败次数等信息 |
| 支持关联规则性能以界面列表形式显示，可了解触发次数、最近一周监控状态等信息 |
| 支持基于跨设备的多事件关联分析； |
| 具备安全评估模型，评估模型基于设备故障、认证登录、攻击威胁、可用性、系统脆弱性等纬度加权平均计算总体安全指数。安全评估模型可以显示总体评分、历史评分趋势。安全评估模型各项指标可钻取具体的评分扣分事件。 |
| 内置设备异常、漏洞利用、横向渗透、权限提升、命令执行、可疑行为6大类50+子类的安全分析场景。 |
| 三维关联分析；支持通过资产、安全知识库、弱点库三个维度分析事件是否存在威胁，并形成关联事件 |
| 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询 |
| 支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果 |
| 通过在目标主机上安装Agent程序，支持监测目标主机的CPU利用率、内存使用率、磁盘使用率、磁盘使用情况、流量等信息 |
| 支持磁盘空间阈值告警，当磁盘使用率达到设定的阈值时可产生并外发告警；资产性能监控异常告警，对于监控的资产系统资源进行监测当指定指标使用率达到设定的阈值时可产生并外发告警；资产状态监控，当资产处于不活跃状态时可产生并外发告警；远程仓库状态监测可告警，当远程仓库可用性检测失败或备份包自动上传失败时可产生并外发告警。 |
| 综合查询及报表管理 | 内置合规性报表1000+种 |
| 内置SOX、ISO27001、WEB安全等解决方案包 |
| 内置完善的等级保护合规报表 |
| 资产管理 | 注册用户资产时，提供自动发现识别能力 |
| 资产拓扑支持按照实际的用户环境进行编辑发布并可以和资产进行绑定，拓扑可以显示资产采集的事件数量被采集资产的状态等信息 |
| 部署方式 | 支持分布式部署，支持页面一键添加子节点，自动进行绑定添加，采集器可以选择同步日志范围，按需转发数据。 |

（3）堡垒机系统参数要求如下：

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 性能要求 | 授权资产：≥80个  硬件性能：并发字符连接≥60个  并发图形连接≥10个 |
| 系统要求 | 机箱高度：1U  标配网口：≥1\*GE电管理口，≥3\*GE电业务口  硬盘容量：≥1.5T  USB口：≥USB2.0\*2  串口：≥RJ45口\*1  电源：单电源 |

| **模块** | **指标项** | **技术参数** |
| --- | --- | --- |
| 登录认证 | 身份认证方式 | 支持手机APP动态口令认证方式登录堡垒机，新用户首次登录后需强制绑定APP动态口令；支持AD、LDAP、RADIUS、吉大正元、北京CA认证系统联动登录堡垒机，支持自动同步AD/LDAP用户。 |
| 单点登录认证 | 支持标准化对接CAS、JWT单点登录认证，且支持配置是否自动创建堡垒机中不存在用户。 |
| 短信口令认证对接 | 支持与Get、Post、Soap发送方式的HTTP短信网关平台进行联动，实现短信动态口令双因素认证机制，如与阿里云短信服务、SendCloud联动。 |
| 双因子认证 | 堡垒机内嵌动态令牌和USBkey认证引擎，可使用动态令牌或USBkey进行双因子认证。 |
| 密码存储 | 支持采用国密加密算法进行核心敏感数据加密存储。 |
| 多用户双因子认证 | 基于不同的用户设置不同的双因子认证模式，如user1用动态令牌、user2用USBkey、user3手机APP动态口令认证。 |
| 兼容客户端类型 | 单点登录支持调用多种本地客户端工具：字符：xshell、secureCRT、putty，图形：mstsc、realvnc，文件传输：secureEX、flashFXP、filezilla、winscp，数据库：ssms、sqlwb、mysqlworkbench、mysql、dbvisualizer、plsql、sqlplus、toad、db2cmd、quest central，无需应用发布服务器。 |
| IE/谷歌浏览器代填 | IE或谷歌浏览器代填应用发布：HTTP/HTTPS协议的web设备，且可以直接代填账号和密码。 |
| 自动收集和自动授权 | 支持自动收集设备IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。 |
| 数据库管理 | 数据库兼容性 | 标准支持DB2、Oracle、MySQL、sqlserver、PG、人大金仓、达梦数据库的协议运维代理，可实现自动登录，自动登录可直接调用本地Windows系统的数据库客户端工具（包括ssms、sqlwb、workbench、mysql、DbVisualizer、plsql、sqlplus、toad、dbcmd、Quest Central、pgadmin3、psql、ksql、Isql、DIsql、DMmanger等），无需应用发布前置机。 |
| macOS兼容性 | 支持在MacOS操作系统下调用Navicat工具运维MySQL、Oracle等数据库资产。 |
| 数据库命令管控 | 数据库支持命令阻断功能，精确到数据库，表、字段级别。 |
| 数据库双重审计 | 支持同时对数据库会话记录图形审计及命令提取。 |
| 数据库双向审计 | 支持对数据库运维会话的上行和下行命令进行审计。 |
| 数据库/web  自动改密 | 支持对数据库及Web应用的自动改密功能。 |
| 账号切换改密 | 支持Unix/Linux系统账号自动改密功能。并支持账号切换改密功能，当root不能直接远程登录时，依旧可以修改root密码。 |
| 专用客户端运维 | 支持Windows/macOS操作系统下C/S架构的堡垒机专用客户端，可通过此专用客户端登录堡垒机，对堡垒机进行简单的管理及运维资产操作。 |
| 运维客户端自带运维工具，可不依赖 xshell/Securecrt/mstsc等工具进行运维操作。 |
| 客户端至少支持资产分组、资产连通性检测，批量运维、资产运维审批、命令审批、二次运维审批等能力。其中资产分组操作支持个性化设置，即每个运维人员可单独设置分组，相互之间独立。 |
| 客户端支持VPN登录功能。 |
| H5运维 | H5运维方式：支持SSH、Telnet、Rlogin、RDP、VNC协议的H5运维，无需本地运维客户端工具。 |
| H5运维方式下，可支持RDP/SSH在线文件传输，无需借助第三方客户端工具，通过web页面即可。 |
| 客户端工具登录 | 客户端访问方式：支持使用本地的mstsc/Xshell/SecureCRT/Putty/winscp/Xftp等客户端工具登录堡垒机访问图形、字符或SFTP、FTP设备。 |
| SSH网关代理直连 | 支持使用本地的SecurCRT/Xshell/OpenSSH工具通过SSH网关代理方式直接登录字符设备。 |
| SQL记录 | 支持审计主流数据库（如DB2、oracle、mysql、sql server、PG、人大金仓、达梦）运维中的SQL语句，可进行关键信息定位查询，并可过滤数据库客户端自动发起的语句，方便查询真实人为的数据库操作。 |
| 文件传输要求 | 实时监控 | 支持对文件传输会话的实时监控。 |
| 命令审批 | 支持对重要命令进行审核：运维人员执行命令后，需等到管理员审批通过后才可执行成功。可选择性设置自定义时间内未审批，对命令自动放行。执行命令的运维人员在运维待审批命令时，可选择终止此命令。 |
| 存储管理 | 支持NAS存储。 |
| 部署架构要求 | 安全接入 | 支持内置VPN模块，无需与其他VPN设备联动，实现运维入口安全接入。 |
| 跨地域部署 | 支持多台堡垒机异地备份部署，每台设备都能提供运维和审计服务，配置数据自动同步。 |

（4）数据库审计平台系统参数要求如下：

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 性能要求 | 支持的数据库实例个数：≥2；  审计性能：峰值SQL处理能力≥2000条/秒；  硬件最大吞吐量≥400Mbps；  双向审计数据库流量≥40Mbps；  标配日志存储数≥8亿条；  审计日志检索能力≥1000万条/秒。 |
| 系统要求 | 1U机架式；  内置交流单电源；  产品采用专用工控机硬件架构，非普通PC服务器，MTBF(平均故障间隔时间)≥65000小时；  处理器采用Intel高性能CPU，内存≥4GB DDR3 1600Mhz，硬盘≥1.5TB；  网络端口：配备至少2个千兆电口管理口；支持千兆网络环境下的监听能力，配备至少4个千兆业务电口。 |

| **模块** | **指标项** | **技术参数** |
| --- | --- | --- |
| 功能项 | 部署方式 | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计； |
| 可在云环境操作系统中安装软件代理； |
| 支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询、一键批量升级所有节点； |
| 协议支持 | 支持Oracle（包括21C版本）、PostgreSQL、SQL Server、DB2、Informix、Sybase、MySQL、MariaDB、Sybase IQ、Vertica、Tidb、PolarDB、PolarDB-X等主流数据库的审计。 |
| 支持MongoDB、Hbase、Hive、impala、Elastic Search、HDFS、Cassandra、greenplum、LibrA、graphbase、cache、Redis、HANA、ArangoDB、Neo4j、OrientDB等非关系型数据库的审计。 |
| 审计信息能够记录执行时长，影响行数、执行结果描述与返回结果集。 |
| 支持超长SQL语句（最长4M）审计。 |
| 产品具有内置规则，规则类型有sql注入、账号安全、数据泄露和违规操作等，并可依据规则进行邮件告警。 |
| 内置安全规则不少于900条，如SQL注入、缓冲区溢出等。 |
| 可自定义审计规则，审计规则至少支持18个条件。 |
| 支持内置安全规则单独升级。 |
| 支持在审计日志中一键添加过滤规则，支持在告警规则中一键添加信任规则和规则白名单。 |
| 设置日志检索条件时，检索条件可根据历史信息自动弹出，检索条件支持源IP、目的IP、客户端工具、数据库名、数据库账号等，输入检索条件时支持智能联想。 |
| 支持告警分析功能，告警支持按照源IP和数据库账号对SQL模板维度进行排行，支持在页面一键去除规则、添加规则白名单。 |
| 支持自定义报表，自定义报表支持客户端IP、数据库账号、客户端工具等10种统计维度，支持审计日志数量、告警日志数量、SQL注入告警数量、会话请求流量等29种统计指标。 |
| 模型分析 | 可依据客户端工具名、数据库用户名、客户端IP、操作系统用户名、客户端主机名、数据库名、操作类型、服务器IP等配置行为模型，并可查看相应告警日志。 |
| 系统管理 | 支持用户界面告警、邮件、短信、钉钉、SYSLOG、企业微信方式告警。 |
| 支持系统资源使用率超阈值、agent状态异常、长时间无审计日志时触发系统告警，且告警支持通过页面、SYSLOG、邮件、短信、钉钉、企业微信方式输出。 |
| Agent管理 | 支持在审计管理端批量安装、卸载、重新安装审计代理； |
| 支持在审计页面直接升级或回退已安装在数据库服务器上的Agent，且升级或回退不需要输入数据库服务器的账号、密码 |
| Agent支持设置CPU亲和性、最大资源使用率限制（CPU、内存） |
| 可监控Agent的转发速率，以及Agent所在数据库服务器的CPU、内存利用率，并可设置CPU、内存利用率的上线阈值，超阈值时Agent将自动停止转发数据。 |
| 支持根据系统CPU使用率、系统内存使用率、系统I/O使用率自动熔断。 |
| Agent支持按照客户端工具、数据库账号过滤审计日志，Agent支持设置抓包过滤串、回环网口抓包。 |
| 支持Agent和审计服务端流量加密传输。 |
| 支持管理中心和审计节点手工同步配置信息。 |
| 支持在管理中心直接升级审计节点。 |
| 管理中心和审计节点统一license。 |
| 三层关联 | 可提供客户端访问Web服务器的URL和应用服务器访问数据库的SQL语句关联功能。 |
| 支持通过部署agent实现java web环境100%准确关联。 |
| 支持配置过滤规则，过滤规则包含IP过滤、SQL模板过滤和自定义过滤，自定义过滤条件不少于28个条件。 |
| 在页面支持ping、traceroute、nc命令测试连通性，支持配置路由信息。 |
| 内置运维终端，可实现日志查看、设备状态检查、执行SQL语句、执行常用命令、特权运维等能力。 |

（5）APT攻击预警平台系统参数要求如下：

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 性能要求 | **性能参数：**  MTBF ≥60000小时  吞吐率：网络层≥400Mbps，应用层≥80Mbps  WEB检测：HTTP最大并发数≥1.5万/秒  邮件检测：邮件处理数≥40万封/24小时  文件检测：≥1万个/24小时  支持管理节点≥4个 |
| 系统要求 | 电源：单电源  CPU≥2核4线程\*1  内存≥8G  硬盘容量：≥1.5T\*1  接口数量：标配≥5个  接口类型：千兆RJ45网口≥2(管理口≥2)、千兆RJ45网口≥3  接口扩展：不可扩展 |

| **指标项** | **技术参数** |
| --- | --- |
| 综合能力 | 支持全流量检测  支持双向流量审计，可对请求和响应内容进行审计 |
| 支持风险数据包保存功能，可存留会话的请求和相应数据包，帮助用户还原攻击过程，进行取证和关联分析；并支持系统内置wireshark组件在线预览风险数据包 |
| 支持解析HTTP、FTP、SMTP、POP3、SMB、IMAP、DNS、HTTPS、SMTPS、POP3S、IMAPS、RADIUS、KRB5、SNMP、NETFLOW V9、TFTP等协议报文（HTTPS、SMTPS、POP3S、IMAPS加密协议解析需要导入服务器私钥证书），  支持GTP、PFCP、NGAP等5G协议解析和审计  支持识别QQ、WEB、LDAP、FTP、TELNET、邮件、SMB、RADMIN、ORACLE、MSSQL、SYBASE、MYSQL、DB2、PostgreSQL、REDIS、MQTT等登录行为；  支持多层 VLAN、VXLAN、MPLS、GRE、VN-Tag、Capwap等网络流量的解析检测 |
| 支持检测WEB攻击、恶意文件攻击、远程控制、WEB后门访问、行为分析、DGA域名请求、SMB远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP欺骗、密码明文形式传输等行为 |
| 支持IP、端口、SMB、Radmin、ICMP、ARP、传输层协议和漏洞扫描行为检测 |
| 支持IP过滤配置，可配置IP、端口或IP对和端口的方式对网络流量进行过滤；可通过新增、批量导入等方式完成IP过滤的配置  支持对指定IP进行流量检测，可通过新增、批量导入等方式完成指定IP检测的配置 |
| 支持识别流量中的个人敏感信息，包括身份证、银行卡、手机号、港澳通行证等，并展示传输信息的协议、网站域名、URL、客户端IP、服务端IP，便于用户发现敏感信息的传输安全隐患和处置 |
| 支持将分析到的WEBSHELL攻击、木马回连和恶意攻击行为同步到WAF，实现APT深度威胁分析与WAF联动阻断 |
| 支持将分析到的恶意文件攻击行为同步到EDR，实现APT深度威胁分析与EDR联动查杀  支持自定义与EDR联动的等待扫描时长，并将联动状态、样本执行结果、样本路径、EDR病毒木马扫描结果等同步到APT设备 |
| 支持将分析到的SMB远程溢出攻击、扫描行为、Web后门访问、隧道通信、暴力破解、挖矿、远控工具利用等攻击成功事件同步到防火墙，实现APT深度威胁分析与防火墙联动阻断  支持自定义防火墙阻断的风险告警类型，时长，并展示最新联动状态、状态更新时间  支持查看阻断信息，阻断信息包括阻断IP、阻断开始时间、阻断结束时间、阻断状态等  支持自定义添加防火墙阻断IP白名单 |
| 支持 HTTP、HTTPS（需要导入服务器私钥证书）协议解析，检测WEB攻击 |
| Web攻击检测 | 支持SQL注入、命令注入、跨站脚本、代码注入、WEB扫描或爬虫、网页篡改、服务错误攻击检测  支持通过智能语义分析引擎，对XSS跨站脚本、SQL注入攻击和OGNL注入攻击进行检测  支持通过智能语义分析引擎，检测JSP脚本文件上传和PHP脚本文件上传  支持30个以上的深度检测模块，对流量进行二次分析，提高攻击检测的准确性 |
| 支持WEBSHELL检测，可检测访问webshell的行为，包含具体对应的URL、返回码、返回数据包内容等，可显示一句话类webshell后门是否植入成功 |
| 支持根据规则类型、协议、源IP/端口、目的IP/端口、流量方向、流量状态、风险类别、风险等级、风险阶段、攻击者、攻击状态、阈值、Flowbits、规则内容等自定义审计规则  支持自定义配置旁路阻断规则，阻断TCP会话 |
| mail攻击检测 | 对社工类攻击进行检测，检测内容包括：邮件头欺骗、邮件发件人欺骗、邮件钓鱼欺骗、邮件恶意链接 |
| 支持邮件恶意附件行为检测 |
| 支持 HTTP、FTP、SMB、SMTP、POP3、IMAP、NFS、TFTP、HTTPS、SMTPS、POP3S、IMAPS（加密协议需要导入服务器私钥证书）等协议传输文件检测 |
| 文件攻击检测 | 支持doc, xls, ppt, swf, pdf, rar, zip, rar, exe, vbs, scr、ps1、elf、mach-O等多种文件解析 |
| 通过分析文件中的二进制代码，找到文件溢出攻击的代码，并能找到APT攻击中的0day攻击 |
| 支持沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现采用多并发沙箱检测技术，集成主流的操作系统winXP、win7、win10、linux等多种检测环境，拥有多项自主研发技术和专利。结合平台内置反病毒引擎和静态分析技术对恶意特征文件、文件漏洞、未知威胁等深度关联分析 |
| 威胁情报与APT云端 | 支持对IP、域名、恶意文件SHA256进行威胁情报检索，或跳转第三方链接进行检索  支持在告警详情页面直接查询与告警IP、域名相关的威胁情报，获取样本通信记录、情报画像等信息 |
| 支持自动从APT云端获取最新的威胁情报  支持域名白名单同步云端 |
| 支持将本地恶意文件攻击的病毒类型等信息上传到APT云端，提升协同防御能力 |
| 支持自动从APT云端更新软件版本和策略库  支持从第三方FTP/SFTP等服务器进行软件版本和策略库更新 |
| 大屏导航 | 导航：支持大屏展示网络攻击态势，包括攻击地图、紧急事件数/总数、恶意文件数/扫描总数、风险趋势（高、中、低风险）、流量分析（吞吐量、HTTP流量、DNS流量）、高危风险类别排名、攻击源区域排名、紧急事件/高危事件，并支持全球地图、中国地图切换展示  失陷主机：支持大屏展示失陷主机风险态势，包括失陷主机视角/横向攻击视角、失陷主机/黑客组织TOP5、风险类别排名、回连区域排名、失陷主机事件统计柱状图、最新事件、失陷主机数，支持实时数据自动刷新  攻击溯源：支持大屏展示风险较为严重的事件，并进行攻击溯源，包括攻击主机个数最多的情报事件TOP10、威胁情报告警类型分布、3D攻击关系图、威胁活动（弱点探测、渗透入侵、获取权限、命令与控制、数据盗取）；支持按IP搜索关联的攻击事件，包括攻击拓扑图、攻击者基本信息、被攻击者信息、攻击过程（攻击过程列表内容包括时间、攻击者、被攻击者、攻击链阶段、风险标签、攻击次数） |

（6）主机安全管理系统参数要求如下：

| **指标项** | **技术参数** |
| --- | --- |
| 全网风险可视 | 支持展示当前待处理的高危风险信息，包括弱口令、待处理病毒、待处理漏洞数据，支持一键跳转到对应处理页面。 |
| 支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、在线终端数、防护中终端数、异常设备数。 |
| 支持查看当前安全防护信息数据，包括渗透追踪防护、勒索深度防护、病毒实时防护、系统登录防护、Web请求防护。 |
| 支持查看当前TOP 5风险资产、TOP 5威胁IP、TOP 5威胁区域。支持实时查看当前安全动态。 |
| 系统性能监控 | 支持监控CPU使用率、内存占用率、磁盘读写以及上下行流量。 |
| 支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。支持对CPU、内存达到一定阈值时客户端自动进行熔断。 |
| 资产指纹 | 支持自动收集终端资产信息，包括：计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡、终端版本、病毒库版本、最近更新时间。 |
| 基线检查 | 支持等保1级到等保4级的系统基线检查，支持的操作系统包括Debian、Linux、Oracle Linux、Suse、Windows。 |
| 主机发现 | 支持自定义扫描指定网段，清点、发现未安装EDR的资产信息，资产信息包括主机名、IP、设备类型、操作系统、发现时间等 |
| 高级威胁防御模块 | 支持对本机的扩展行为（信息收集、权限提升）进行监测，防止提权行为和信息泄露。 |
| 识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。 |
| 对失陷后主机远控持久化行为进行检测（反弹Shell、远程控制），可阻断远控。 |
| 对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。 |
| 可对渗透的收尾阶段的数据清除行为进行识别和阻断。 |
| 系统安全性模块 | 支持防端口扫描，锁定恶意的端口扫描，并记录告警。 |
| 支持网络分域访问，在服务端设置不同网络访问域，资产在同一时间只能访问任意一个网络域，支持资产自主切换不同网络访问域。 |
| 支持基于IP及域名设置探测地址，实时感知违规外联行为，针对违规外联行为支持多种处置方式，包括不做处理、弹窗提醒用户并关机、弹窗提醒用户并断网。 |
| 支持反渗透监控，包括横向渗透的危险操作等。 |
| 支持网站漏洞防护，防护内容包括SQL注入、XSS攻击、应用程序漏洞及自定义规则。 |
| 内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。 |
| 支持登录防护，包括以系统账号为粒度的异常登录防护、支持4个任意维度（任意IP，任意域名，任意计算机名，任意时间）的系统登录访问策略设置。 |
| 移动存储介质管理：  1.支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、导出注册列表、行为监控及审计等。  2.支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。  3.支持管理员设置自动审批客户端注册请求。  4.支持从资产维度、设备维度对存储介质的权限进行精细化设置，同一设备可针对不同的资产设置不同的读写权限，有效控制不明来历的移动存储可能带来的病毒传播等隐患。 |
| 云端威胁鉴定 | 支持对文件HASH、IP、域名、邮箱等IOC指标进行动静态鉴定，通过和云端威胁情报进行碰撞，实时返回威胁结果。 |
| 联动威胁情报，支持对外联IP、DNS解析、可疑文件进行实时情报鉴定，实现风险一站式实时监测。 |
| 防病毒模块 | 针对Windows系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程。 |
| 支持多引擎设置，包括默认引擎、深度扫描引擎。 |
| 提供专门的勒索风险评估功能。 |
| 提供专门的针对未知勒索病毒的防御引擎，并提供功能开关项。对于未知勒索病毒确保无法加密。同时支持白名单设置。 |
| 提供专门的挖矿风险评估工具。 |
| 提供专门的挖矿实时防御工具，并提供功能开关。 |
| 无文件检测 | 针对流行的无文件病毒进行实时监测，支持对powershell、rundll32、cmd、register等类型进行参数分析检查 |
| 微隔离 | 支持基于主机维度和业务维度的网络五元组策略下发、并支持混合模式、黑名单、白名单3种模式切换 |
| 支持一键封堵IP和端口 |
| 支持对微隔离策略进行导入和导出 |
| 支持按照资产标签、协议、端口、时间等维度筛选、展示业务和主机的访问关系 |
| 屏幕水印 | 支持对屏幕拍照泄密数据的行为进行溯源。 |
| 升级系统 | 支持病毒库、Windows补丁库的离线升级及在线升级；支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库、弱口令库的离线升级。 |
| 客户端程序支持在线热升级，升级之后旧版本驱动等程序无残留。 |
| 集中管控 | 管理平台支持一键设置客户端卸载密码、一键卸载监控端、一键解除绑定、一键停止/启动防护、一键关闭/重启主机、一键重启客户端、一键迁移资产。 |
| 支持多级中心部署，查看所有下级控制中心的资产部署情况以及风险数据。 |
| 支持通过Web页面进行客户端推广部署，推广页面支持自定义。 |
| 应急响应 | 对于新发现的病毒、零日漏洞，厂商能够于24小时内作出响应，及时通知用户，并提供专门应急预案、处置工具或专杀工具。 |
| 技术支持 | 支持7天\*24小时全天候威胁溯源服务。 |

7.3.3.3机房网络系统升级改造

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **主要性能指标** | **数量** |
| 1 | 网络交换机系统1 | 详见“（1）网络交换机系统1参数要求”。 | 2台 |
| 2 | 网络交换机系统1光模块 | SFP+ 万兆模块(850nm,300m,LC) | 62个 |
| 3 | 网络交换机系统1光纤 | 配套光纤跳线 | 90根 |
| 4 | 网络交换机系统2 | 详见“（2）网络交换机系统2参数要求”。 | 4台 |
| 5 | 网络交换机系统2光模块 | SFP+ 万兆模块(850nm,300m,LC) | 15个 |
| 6 | 网络交换机系统2光纤 | 配套光纤跳线 | 18根 |
| 7 | 网络交换机系统2以太网网线 | 配套六类以太网网线 | 180根 |
| 8 | 光纤存储网络交换机系统 | 详见“（3）光纤存储网络交换机系统参数要求”。 | 2台 |

（1）网络交换机系统1参数要求如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 交换容量 | | ≥2 Tbps | 包转发率 | ≥1000Mpps |
| Console口 | | ≥1个 | 管理用以太网口 | ≥1个 |
| USB口 | | ≥1个 | SFP+ | ≥48 |
| 扩展插槽 | | ≥2个 | | |
| 电源模块 | | 双模块化电源 | | |
| 风扇模块 | | 双模块化风扇，前后或后前通风 | | |
| 横向虚拟化 | 支持IRF2智能弹性架构 | | | |
| 支持分布式设备管理，分布式链路聚合，分布式弹性路由 | | | |
| 支持通过标准以太网接口进行堆叠 | | | |
| 支持本地堆叠和远程堆叠 | | | |
| 支持基于LACP、BFD、ARP的MAD堆叠分裂检测机制 | | | |
| 最大堆叠9台 | | | |
| 链路聚合 | 支持10GE端口聚合 | | | |
| 支持40GE端口聚合 | | | |
| 支持静态聚合、动态聚合 | | | |
| Jumbo Frame | 支持 | | | |
| MAC地址表 | 支持静态MAC地址 | | | |
| 支持黑洞MAC地址 | | | |
| 支持设置端口MAC地址学习最大个数 | | | |
| SDN/Openflow | 支持OpenFlow 1.3标准 | | | |
| 支持多控制器（EQUAL模式、主备模式） | | | |
| 支持多表流水线 | | | |
| 支持Group table | | | |
| 支持Meter | | | |
| VLAN | 支持基于端口的VLAN（4094个） | | | |
| 支持Default VLAN | | | |
| 支持QINQ | | | |
| 支持灵活QINQ | | | |
| 支持VLAN MAPPING | | | |
| 支持PVST+ 支持RPVST+ | | | |
| 支持基于IP、MAC的VLAN划分 | | | |
| 流量监控 | 支持SFLOW、NetStream\* | | | |
| MPLS | 支持MPLS | | | |
| 支持MCE | | | |
| 支持MPLS VPN、VPLS | | | |
| 支持MPLS TE | | | |
| DHCP | DHCP Client | | | |
| DHCP Snooping | | | |
| DHCP Relay | | | |
| DHCP Server | | | |
| DHCP Snooping option82/DHCP Relay option82 | | | |
| ARP | 支持静态表项 | | | |
| 支持免费ARP | | | |
| 支持标准代理ARP和本地代理ARP | | | |
| 支持Dynamic ARP Inspection | | | |
| 支持ARP anti-attack | | | |
| 支持ARP源抑制 | | | |
| 支持ARP Detection功能（能够根据DHCP Snooping安全表项、802.1x表项，或IP/MAC静态绑定表项进行检查） | | | |
| 路由协议 | 支持静态路由 | | | |
| 支持RIPv1/v2，RIPng | | | |
| 支持OSPFv1/v2，OSPFv3 | | | |
| 支持BGP4，BGP4+ for IPv6 | | | |
| 支持IS-IS，IS-IS V6 | | | |
| 支持等价路由，策略路由 | | | |
| 支持VRRP/VRRPv3 | | | |
| IPV6特性 | 支持ND（Neighbor Discovery） | | | |
| 支持PMTU | | | |
| 支持 ICMP v6、Telnet v6、SFTP v6、SNMP v6、BFD v6、VRRP v3、IS-ISv6、BGP4+ for IPv6 | | | |
| 支持IPv6 Portal | | | |
| 支持IPv6 tunnel | | | |
| VxLAN | 支持VXLAN 二层交换 | | | |
| 支持VXLAN 路由交换 | | | |
| 支持VXLAN 网关 | | | |
| 支持OpenFlow+Netconf的VxLAN集中式控制平面 | | | |
| 组播协议 | 支持IGMP Snooping v2/v3 | | | |
| 支持IGMP Snooping Fast-leave | | | |
| 支持IGMP Snooping Group-policy | | | |
| 支持PIM-SM,PIM-DM，PIM-SSM | | | |
| 支持PIM snooping | | | |
| 支持MVRP | | | |
| 支持MFF | | | |
| 支持增强三层组播协议 | | | |
| 零配置 | 支持DHCP auto-config及CWMP-TR069等零配置方式 | | | |
| 广播/组播/单播风暴抑制 | 支持基于端口速率百分比的风暴抑制 | | | |
| 支持基于pps的风暴抑制 | | | |
| 支持基于bps的风暴抑制 | | | |
| 二层环网协议 | 支持STP/RSTP/MSTP协议 | | | |
| 支持STP Root Guard | | | |
| 支持BPDU Guard | | | |
| 支持ERPS以太环保护协议（G.8032） | | | |
| QoS/ACL | 支持对端口接收报文的速率和发送报文的速率进行限制 | | | |
| 支持CAR功能 | | | |
| 每个端口支持8个输出队列 | | | |
| 支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持SP、WDRR、WRR、WFQ、SP+WDRR等多种模式 | | | |
| 支持报文的802.1p和DSCP优先级重新标记 | | | |
| 支持L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源MAC地址、目的MAC地址、源IP(IPv4/IPv6)地址、目的IP(IPv4/IPv6)地址、端口、协议、VLAN的流分类 | | | |
| 支持时间段（Time Range） | | | |
| 支持WRED | | | |
| 镜像 | 支持流镜像 | | | |
| 支持N:4端口镜像 | | | |
| 支持本地和远程端口镜像 | | | |
| 支持ERSPAN | | | |
| 安全特性 | 支持用户分级管理和口令保护 | | | |
| 支持集中MAC认证 | | | |
| 支持802.1X | | | |
| 支持storm constrain | | | |
| 支持AAA认证 | | | |
| 支持Portal认证 | | | |
| 支持RADIUS认证 | | | |
| 支持HWTACACS | | | |
| 支持SSH 2.0 | | | |
| 支持端口隔离 | | | |
| 支持IP+MAC+端口绑定 | | | |
| 支持IP Source Guard | | | |
| 支持HTTPs | | | |
| 支持SSL | | | |
| 支持PKI(Public Key Infrastructure，公钥基础设施) | | | |
| 支持CPU防护 | | | |
| 加载与升级 | 支持XModem协议实现加载升级 | | | |
| 支持FTP（File Transfer Protocol）加载升级 | | | |
| 支持TFTP（Trivial File Transfer Protocol）加载升级 | | | |
| 管理和维护 | 支持命令行接口（CLI）配置 | | | |
| 支持Telnet远程配置 | | | |
| 支持通过Console口配置 | | | |
| 支持schedule job | | | |
| 支持ISSU | | | |
| 支持802.1AG及802.3AH | | | |
| 支持SNMP（Simple Network Management Protocol） | | | |
| 支持NetStream功能，流量分析采样比1：1 | | | |
| 支持IMC网管系统 | | | |
| 支持系统日志 | | | |
| 支持分级告警 | | | |
| 支持NTP | | | |
| 支持电源的告警功能 | | | |
| 支持风扇、温度告警 | | | |
| 支持调试信息输出 | | | |
| 支持Ping、Tracert | | | |
| 支持Track | | | |
| 支持Telnet远程维护 | | | |
| 支持USB进行文件上传和下载 | | | |

（2）网络交换机系统2参数要求如下:

|  |  |  |  |
| --- | --- | --- | --- |
| 交换容量 | ≥500Gbps | 包转发率 | ≥100Mpps |
| 管理网口 | ≥1 | 管理串口 | ≥1个RJ-45 Console口，≥1个 USB及MIRCO USB口（不能同时工作，MICRO USB优先） |
| 前面板 | ≥48个10/100/1000Base-T自适应以太网端口 | 业务端口描述 | ≥4个万兆SFP+口 |
| 电源模块 | 双模块化电源 | | |
| IRF2智能弹性架构 | 支持IRF2智能弹性架构 | | |
| 支持分布式设备管理，分布式链路聚合，分布式弹性路由 | | |
| 支持通过标准以太网接口等方式进行堆叠 | | |
| 支持本地堆叠和远程堆叠 | | |
| SDN/Openflow | 支持OpenFlow 1.3标准 | | |
| 支持多控制器（EQUAL模式、主备模式） | | |
| 支持多表流水线 | | |
| 支持Group table | | |
| 支持Meter | | |
| 端口聚合 | 支持GE端口聚合 | | |
| 支持10GE端口聚合 | | |
| 支持40G聚合 | | |
| 支持静态聚合 | | |
| 支持动态聚合 | | |
| 支持跨设备聚合 | | |
| 端口特性 | 支持IEEE802.3x 流量控制（全双工） | | |
| 支持基于端口速率百分比的风暴抑制 | | |
| 支持基于PPS的风暴抑制 | | |
| 支持基于bps的风暴抑制 | | |
| Jumbo Frame | 支持 | | |
| MAC地址表 | 支持黑洞MAC地址 | | |
| 支持设置端口MAC地址学习最大个数 | | |
| VLAN | 支持基于端口的VLAN | | |
| 支持基于MAC的VLAN | | |
| 基于协议的VLAN | | |
| 基于IP子网的VLAN | | |
| 支持QinQ，灵活QinQ | | |
| 支持VLAN Mapping | | |
| 支持Voice VLAN | | |
| 支持MVRP | | |
| 二层环网协议 | 支持STP/RSTP/MSTP、PVST | | |
| 支持SmartLink | | |
| 支持RRPP | | |
| 支持ERPS以太环保护协议（G.8032） | | |
| DHCP | DHCP Client | | |
| DHCP Snooping | | |
| DHCP Relay | | |
| DHCP Server | | |
| DHCP Snooping option82/DHCP Relay option82 | | |
| IP路由 | 支持静态路由 | | |
| 支持RIPv1/v2，RIPng | | |
| 支持OSPFv1/v2，OSPFv3 | | |
| 支持BGP4，BGP4+ for IPv6 | | |
| 支持IS-IS | | |
| 支持VRRP/VRRPv3 | | |
| IPv6 | 支持ND（Neighbor Discovery） | | |
| 支持PMTU | | |
| 支持IPv6-Ping，IPv6-Tracert，IPv6-Telnet，IPv6-TFTP | | |
| 支持手动配置Tunnel | | |
| 支持6to4 tunnel | | |
| 支持ISATAP tunnel | | |
| 组播 | 支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2 | | |
| 支持PIM Snooping | | |
| 支持MLD Proxy | | |
| 支持组播VLAN | | |
| 支持IGMP v1/v2/v3，MLD v1/v2 | | |
| 支持PIM-DM，PIM-SM，PIM-SSM | | |
| 支持MSDP，MSDP for IPv6 | | |
| 支持MBGP，MBGP for Ipv6 | | |
| 镜像 | 支持流镜像 | | |
| 支持N:4端口镜像 | | |
| 支持本地和远程端口镜像 | | |
| OAM | 支持802.1ag | | |
| 支持802.3ah | | |
| 支持ACL\QoS | 支持L2（Layer 2）~L4（Layer 4）包过滤功能，提供基于源MAC地址、目的MAC地址、源IP(IPv4/IPv6)地址、目的IP(IPv4/IPv6)地址、TCP/UDP端口号、VLAN的流分类 | | |
| 支持时间段（Time Range）ACL | | |
| 支持入方向和出方向的双向ACL策略 | | |
| 支持基于VLAN下发ACL | | |
| 支持对端口接收报文的速率和发送报文的速率进行限制，最小粒度为8Kbps | | |
| 支持报文重定向 | | |
| 支持报文的802.1p和DSCP优先级重新标记 | | |
| 支持CAR（Committed Access Rate）功能 | | |
| 每个端口支持8个输出队列，CPU口支持48个队列 | | |
| 支持灵活的队列调度算法，可以同时基于端口和队列进行设置，支持SP、WRR、WFQ、SP+WRR、WDRR五种模式 | | |
| 安全特性 | 支持用户分级管理和口令保护 | | |
| 支持802.1X认证/集中式MAC地址认证 | | |
| 支持Guest VLAN | | |
| 支持RADIUS认证 | | |
| 支持SSH 2.0 | | |
| 支持端口隔离 | | |
| 支持端口安全 | | |
| 支持PORTAL认证 | | |
| 支持EAD | | |
| 可支持DHCP Snooping，防止欺骗的DHCP服务器 | | |
| 支持动态ARP检测，防止中间人攻击和ARP拒绝服务 | | |
| 支持BPDU guard， Root guard | | |
| 支持uRPF(单播反向路径检测)，杜绝IP源地址欺骗，防范病毒和攻击 | | |
| 支持IP/Port/MAC的绑定功能 | | |
| 支持OSPF、RIPv2报文的明文及MD5密文认证 | | |
| 支持PKI（Public Key Infrastructure，公钥基础设施） | | |
| 管理与维护 | 支持XModem/FTP/TFTP加载升级 | | |
| 支持命令行接口（CLI），Telnet，Console口进行配置 | | |
| 支持SNMPv1/v2/v3 | | |
| 支持RMON （Remote Monitoring）告警、事件、历史记录 | | |
| 支持iMC智能管理中心 | | |
| 支持系统日志，分级告警，调试信息输出 | | |
| 支持NTP | | |
| 支持电源的告警功能，风扇、温度告警 | | |
| 支持Ping、Tracert | | |
| 支持VCT（Virtual Cable Test）电缆检测功能 | | |
| 支持DLDP（Device Link Detection Protocol）单向链路检测协议 | | |
| 支持LLDP | | |
| 支持Loopback-detection 端口环回检测 | | |

（3）光纤存储网络交换机系统参数要求如下：

|  |  |
| --- | --- |
| **参数** | **要求** |
| 性能 | ≥16 Gb FC |
| 端口数量 | 24–48 个光纤通道设备端口，要求具有36个活动端口，具有36个活动端口许可。 |
| 交换机总带宽 | 300–700 Gbps |
| 交换机光模块 | 配置不少于36个16Gb SFP+ 光模块 |
| 交换机专用光纤线 | 配置不少于36根LC/LC Multi-mode OM4 2 fiber 15m Cable |
| 加密功能 | 是；动态加密；AES-GCM 256 位 |
| 协议支持 | 4/8/10/16 Gb FC，路由 |
| 可用性 | • 热码加载；按需配置端口，无停机时间  • 带有集成冷却风扇的可选集成冗余热插拔电源  • 所有数据路径和系统内存上的增强型故障检测逻辑奇偶校验保护 |
| 介质类型 | B 系列 16 Gb SFP+、8 Gb SFP+ |

7.3.3.4机房存储系统升级改造

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **主要性能指标** | **数量** |
| 1 | 存储硬盘 | 4TB 12G SAS 7.2K LFF(3.5in），适配现有存储设备 | 8块 |
| 2 | 分布式存储系统 | 详见“（1）分布式存储系统参数要求”。 | 1套 |
| 3 | 分布式存储网络系统交换机 | 详见“（2）分布式存储网络系统交换机系统参数要求”。 | 2台 |

（1）分布式存储系统参数要求如下：

|  | **类别** | **参数** | **描述** |
| --- | --- | --- | --- |
| 系统要求 | 存储设备 | | 1套（≥3个节点） |
| 安装要求 | | 机架式，可安装到42U标准机柜中，含安全面板和滚珠导轨 |
| 高可靠性 | | 所有部件采用冗余设计，如电源、风扇等，采用内存保护技术  在任何一部件发生故障时，系统仍能正常运行 |
| 硬件配置 | 每集群控制器数量 | ≥3个 |
| 每集群的处理器 | 采用Intel Xeon 可扩展处理器，内核总数≥60核 |
| 每集群的内存 | ≥350GB |
| 每集群的SSD缓存 | ≥5500GB |
| SSD五年耐久性 | ≥3 DWPD |
| 每集群的HDD容量 | ≥170TB |
| 每集群的10GbE/iSCSI端口 | ≥6个10Gb Bonding |
| 每集群的1GbE端口 | ≥4个 |
| 每集群的电源 | ≥6个热插拔冗余电源模块 |
| 多协议支持 | 支持协议 | 支持RBD、iSCSI、FC、FTP、NFS 、SMB 、S3、POSIX、HDFS、CSI |
| 软件要求 | 多管理接口 | RESTful API | 支持RESTful 管理接口，以利于上层应用无缝整合存储系统 |
| CLI命令行工具 | 支持CLI命令行工具，最大化管理效率 |
| GUI管理接口 | 支持可视化GUI管理接口 |
| VMware web client | 支持VMware Web Client，在 VMware 侧统一管理计算和存储，大幅度提升管理运维的便捷度 |
| 运行管理分析 | 全方位性能指标监控 | 支持物理服务器CPU、内存、网络、负载监控 |
| 支持存储介质读写IOPS、带宽和延迟监控 |
| 支持存储池读写IOPS、带宽和延迟监控 |
| 支持卷、文件目录读写IOPS、带宽和延迟监控 |
| 支持上述指标统计保留天数自定义设置 |
| 实时健康管理 | 支持对物理服务器、存储介质、存储池数据冗余状态监控及管理 |
| 支持块和文件的网关和链路健康检测 |
| 支持存储介质根据SMART信息预测设备寿命，提醒坏盘可能 |
| 容量预警 | 根据智能算法预测未来容量使用增长，可以预测剩余容量将在几天后被写满，并在容量使用天数剩余30天内给与提示和告警 |
| 可视化硬盘拓扑 | 以可视化的视图展示硬盘的基本信息及从属关系，基本信息包括：硬盘名称、状态、容量、已使用容量、数据恢复情况、硬盘介质、IO利用率等。从属关系包括从属服务器视图和从属存储池视图。同时支持鼠标hover时显示硬盘详细信息 |
| 自动重平衡 | 闲时做自动重平衡，当发现集群内OSD容量不均衡的时候，会自动以最低速进行重平衡 |
| 可视化网络拓扑 | 可视化硬件网络拓扑，直观展现集群网络情况、数据中心、机架、服务器、网卡信息。同时可以可视化展现集群网络中各个模块的异常情况。支持不同网卡的监控信息及监控历史 |
| 事件通知 | 支持系统和用户触发产生的及关键事件日志，包括记录重要的系统触发、操作员行为触发及系统关键事件等（系统触发如服务器、硬盘离线上线、存储池重平衡等，用户行为触发如创建、修改、删除资源等），便于排错、审计和跟踪，方便用户全方面掌控存储运行情况。同时支持事件日志导出 |
| 告警管理 | 支持集群内所有资源的告警，在存储系统的各级软硬件产生故障时，由管理控制台向管理员提示告警，有助于及时了解资源使用情况和处理突发事件；支持自定义告警通知，同时支持邮件告警 |
| SNMP | 支持SNMP V2/V3，支持TRAP，GET，SET操作 |
| 自定义容量阈值 | 自定义集群中硬盘的容量阈值，该阈值是硬盘被安全写满的阈值。达到该阈值后改硬盘将不可再写入数据，但该阈值可以根据业务需求调整 |
| 块存储 | 卷和快照管理 | 支持卷管理操作，精简配置，在线扩容 |
| 支持秒级快照，定时快照 |
| 支持链接克隆，支持独立克隆 |
| 卷QoS | 支持卷QoS，支持在线调整QoS，实时生效 |
| 精简配置 | 支持精简配置，安写入有效数据容量分配实际空间 |
| 多协议支持 | 支持RBD和iSCSI协议，可选支持FC协议 |
| VAAI | 支持VMware VAAI，并通过VMware VAAI 认证 |
| 无损快照技术 | 使用 ROW(Redirect on Write)快照技术，在连续快照/克隆负载下，性能变化幅度小于5% |
| 数据链路高可用（MPIO） | 支持iSCSI冗余链路，业务链路更安全 |
| IP链路高可用 | 在用户无感知的情况下，将故障端口上的业务，快速自动地切换到其它可用端口上，保障业务不中断，提高iSCSI路径的可靠性 |
| 支持多虚拟化和容器平台 | 支持VMware，HyperV，Citrix等主流虚拟化平台，支持Kubernetes CSI接口驱动，同时支持iSCSI和NFS |
| 文件存储 | 接口支持 | 支持支持FTP、NFS 、SMB 、POSIX、HDFS、CSI |
| 在线整池扩容 | 持文件系统在线扩容。已创建的命名空间支持按池扩容，避免存储池大规模扩容导致海量数据重平衡，进而长时间影响业务可用性。 |
| 文件目录共享 | 支持同一个目录多种访问协议同时访问 |
| 数据迁移 | 支持对象到对象，对象到文件及文件到对象间的数据迁移服务，同时支持断点续传及增量迁移。 |
| 对象存储 | 数据生命周期管理 | 存储桶数据生命周期管理支持，可以对存储桶内的数据通过数据前缀或整桶进行删除，支持延时删除。 |
| 海量小文件管理 | 支持针对海量小文件存取优化。 |
| 分级存储 | 可以根据数据性质选择数据持久化存储级别，需要提供存储空间利用率时选择EC存储。 |
| 数据分层 | 支持本地存储到公有云、私有云及蓝光存储等的数据分层功能，根据数据的访问需求，通过不同的策略对于不经常访问或需要做归档的数据自动分层到不同存储要求的公有云或蓝光存储。分层归档到远端存储的数据可以直接访问，对于分层归档后的数据在某个时间段如果有频繁访问的需求还可以直接缓存到本地存储。 |
| 图片处理 | 在线图片处理，支持图片缩放、裁剪、格式转换、水印、旋转、质量调节等十几种图片处理功能 |
| 多站点全局统一命名空间 | 多站点统一命名空间通过跨多集群建立统一的用户和桶管理视图，桶中对象数据在多个站点间异步复制，实现数据异地容灾、就近访问、负载跨站点分布。数据桶需以存储桶为粒度，可以按需将数据同步到指定的数据中心，在本地数据中心就近读、写数据。 |
| 数据可靠 | 数据多副本 | 支持1-6副本，且支持在线修改副本 |
| EC纠删码 | 全场景支持EC |
| 拓扑规划及故障域隔离 | 支持自主规划集群物理设备拓扑，使允许多级故障隔离，包含主机、机柜级故障隔离能力 |
| 数据恢复QoS控制 | 在数据较长时间处于降级状态时，例如节点丢失或副本丢失，系统会自动触发数据重建恢复 |
| 用户可设定数据恢复的带宽规则，最小化对业务的影响 |
| 硬盘维护模式 | 硬盘维护模式是辅助对硬盘进行维护操作时数据不进行重平衡，为保证系统可用性，建议维护时间不要过长 |
| 利用该模式可用于硬件设备下线维护场景 |
| 端到端校验和自动恢复 | 针对在线实时读写数据时做CRC（Cyclic Redundancy Check）校验，防止静默数据错误。 |
| 智能缓存 | 内存读缓存 | 通过流预测算法在内存中提前获取目标数据，大大提高读性能 |
| SSD 读写缓存 | 实现SSD和HDD分层，支持大容量分布式缓存 |
| 单控制器支持高达960GB持久高性能读写缓存 |
| SSD与HDD Tier分层聚合模式 | 整体架构采用Tier分层模式，缓存层由高速介质组成，采用创新性的IO聚合技术，将小块随机IO聚合成大块顺序IO，可支持高并发和高负载下的持续稳定的性能。 |
| 扩展性 | 线性扩展 | 支持随着系统规模（节点数量）的增加，系统性能和容量线性提升 |
| 卷在线扩展 | 支持不中断业务的情况下进行卷级扩容 |
| 多资源池 | 支持集群中不同存储介质分别建立资源池 |
| 一致性组异步复制（快照复制） | 支持一致性组异步复制，一致性组中的卷同时复制到目标端，确保相同时间点的快照复制，支持数据库容灾 |
|  | 支持将块数据归档到Amazon S3、阿里云、腾讯云、电信天翼云等公有云 |

（2）分布式存储网络系统交换机系统参数要求如下：

| **功能及技术指标** | **详细技术参数** |
| --- | --- |
| 系统性能 | 交换性能≥2.5Tbps，转发性能≥450Mpps |
| 接口要求 | ≥20个1/10G SFP Plus端口，含不少于20个光模块 |
| 电源 | 模块化双电源 |
| 风扇 | 模块化风扇 |
| 扩展插槽 | 扩展插槽≥1，支持8端口万兆SFP+光接口板卡；2端口40GE QSFP+光接口板卡，2端口25G SFP28以太网光接口模块，8端口 1/2.5/5G BASE-T以太网电接口模块，8端口 1/2.5/5/10G BASE-T 以太网电接口模块 |
| 性能指标 | MAC地址表 ≥32K，路由表容量（max）≥16K，ARP≥16K，ACL≥1K（入）/256（出） |
| VxLAN | 支持VxLAN二层网关  支持VxLAN三层网关  支持EVPN |
| 堆叠 | 最大堆叠台数>=9台 |
| 最大堆叠带宽>=160G |
| 可要求堆叠带宽，并要求实配接口的基础上额外满配堆叠带宽所需的接口和互联模块 |
| 支持跨设备链路聚合，单一IP管理，分布式弹性路由 |
| 支持通过标准以太端口进行堆叠（万兆或40G均支持） |
| 支持完善的堆叠分裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预 |
| 支持远程堆叠 |
| VLAN特性 | 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 | 支持最多16个端口聚合；支持最多128个聚合组（IRF2）；支持LACP |
| 镜像功能 | 支持本地端口镜像和远程端口镜像RSPAN； |
| 支持流镜像 |
| 同时支持N：M的端口镜像（M大于1） |
| 可靠性 | 支持VRRPv2/v3（虚拟路由冗余协议)； |
| 支持RRPP（快速环网保护协议），环网故障恢复时间不超过200ms； |

7.3.3.5局财务系统机房区域升级改造

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **内容** | **主要性能指标** | **数量** |
| 1 | 机柜 | 标准机柜+KVM | 2台 |
| 2 | 网络交换机系统2 | 详见“（2）网络交换机系统2参数要求”。 | 1台 |
| 3 | 网络交换机系统2光模块 | SFP+ 万兆模块(850nm,300m,LC) | 4个 |

7.3.4与原系统的兼容与接口要求

（1）机房内现有两台核心交换机以热备模式功运行，用于核心机房与二楼办公楼层机房两部分，两个C类IP地址段，接入服务器等设备40余台，办公电脑和办公设备50余台，业务流量包括视频会议、网站、内外网系统数据交换等。

机房网络交换机系统升级改造与现有网络交换机相互兼容，并支持IRF2智能弹性架构, 与现有核心网络设备虚拟化为一台逻辑设备，保证现有设备运行和业务流程都正常。负责将机房现有系统设备接入采购交换机，施工过程中确保系统数据安全。

光纤存储交换机系统与所有存储设备和关联服务器设备相互兼容。负责将机房所有存储设备和关联服务器设备接入光纤存储交换机，施工过程中保证存储设备和关联服务器数据安全。

（2）机房现有3套不同型号异构的存储设备，且设备之间存在较大的代差，上面存储有10余个业务系统的数据，存储数据总量约100TB。机房存储系统升级改造需要兼容现有的硬件设备，支持在异构环境中从现有存储设备上复制、迁移数据，保证数据存储安全，保证数据的一致性和完整性。分布式存储系统与现有服务器相互兼容。供应商负责将机房服务器接入分布式存储系统，完成新老存储系统之间的数据迁移工作，升级改造过程中保证存储系统和服务器数据安全。

7.4质量标准和验收方案

（1）货物的数量不足或表面瑕疵采购人应在验收时当面提出，对质量问题之异议应在安装调试后七日内提出。

（2）采购人收货后根据货物的技术规格要求和质量标准，对货物进行检查验收，如果发现数量不足或有质量、技术等问题，供应商应负责按照采购人的要求采取补足、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。

（3）系统升级改造完成后，应交付采购人所要求的相关文档，并按照要求配合其他相关服务方完成项目有关交接。

（4）供应商应按验收标准配合采购人验收。系统的各项测试应独立进行，并逐项进行检验。

（5）供应商根据国家的有关标准和由供应商拟定并经采购人确认的验收大纲进行项目验收，验收由采购人最后确认，验收工作前供应商必须先进行自检工作，并向采购人提供自检报告。若合同系统的试运行处于非良好状态下，采购人有权拒绝验收，由此引起的损失由供应商负责。

（6）零件更换时间：一般零件2天之内，特殊零件4天之内。

7.5人员及设备要求

（1）人员要求

本项目运维团队人员配置7名，供应商根据本项目实际情况组建独立的项目团队，并指定1名专职项目经理提供项目管理工作。本项目指派5名项目团队成员负责实施系统升级改造；1名驻场维护人员在系统升级改造期间，以及改造完成后3年维保服务期内，提供5（天）×8（小时）驻场维护服务。

本项目中人员岗位要求详见下表：

| **序号** | **岗位名称** | **建议配置岗位人数** | **基本要求** | **备注** |
| --- | --- | --- | --- | --- |
| 1 | 项目经理 | 1 | 负责项目管理 | 请在响应文件中提供在职证明材料 |
| 2 | 项目团队  成员 | 5 | 负责实施系统升级改造 |
| 3 | 驻场维护人员 | 1 | 在系统升级改造期间，以及改造完成后3年维保服务期内，提供每周5（天）×8（小时）驻场维护服务。 |
| 4 | 合计 | 7 | 专业实施管理团队 |

7.6其他

供应商要负责全部系统的升级改造工作。升级改造前要求制定切实可行的升级改造方案，充分考虑现场环境和升级改造难度；升级改造前要求制定切实可行的机房断电、断网和系统意外中断等突发事件的应急预案。升级改造期间要求供应商对机房各信息系统和机房硬件设备的运行状况进行实时监控，做好故障预防和风险排除工作。整个升级改造过程不能对机房其他设备和系统造成影响，升级改造过程中要保证采购人工作时间机房其他设备和系统的正常运行。

本项目中涉及机房需要断电或者断网的，供应商将升级改造放到周末、节假日进行，且连续断电（断网）时间不能超过24小时；供应商全面负责由于升级改造原因停电（断网）而造成的机房内所有系统和设备的停机和启动工作，保证机房内所有系统数据安全，保证数据的一致性和完整性，保证机房内所有系统设备启动、运行正常。如果因为断电（断网）给采购方及用户造成损失和影响的，由供应商负责消除影响，由此造成的损失，采购方有权要求供应商赔偿。

本项目中涉及局中心机房信息系统需要暂停的，供应商负责协调相关应用软件服务商，制定切实可行的系统暂停方案，确保系统暂停安全顺利实施，供应商不得以应用软件服务商不配合为由进行推脱。如果因为系统暂停给采购人及用户造成损失和影响的，由供应商负责消除影响，由此造成的损失，采购人有权要求供应商赔偿。对于供应商以此为推脱，或者由此造成升级改造延误的，采购人有权终止合同，扣除全部项目费用，并要求供应商承担违约责任，并赔偿相应的损失。

本项目中涉及局中心机房硬件设备需要移机的，供应商应负责协调相关硬件服务商，制定切实可行的硬件移机方案，确保系统暂停安全顺利实施，供应商不得以硬件服务商不配合为由进行推脱。如果因为硬件移机给采购人及用户造成损失和影响的，由供应商负责消除影响，由此造成的损失，采购人有权要求供应商赔偿。对于供应商以此为推脱，或者由此造成升级改造延误的，采购人有权终止合同，扣除全部项目费用，并要求供应商承担违约责任，并赔偿相应的损失。

本项目中涉及局中心机房应用系统数据迁移的，供应商应负责协调相关应用软件服务商，制定切实可行的迁移计划和技术迁移方案，确保迁移安全顺利实施，供应商不得以应用软件服务商不配合为由进行推脱。如果因为数据迁移给采购方及用户造成损失和影响的，由供应商负责消除影响，由此造成的损失，采购方有权要求供应商赔偿。对于供应商以此为推脱，或者由此造成升级改造延误的，采购人有权终止合同，扣除全部项目集成费，并要求供应商承担违约责任。

供应商应充分考虑到本项目中系统升级改造的实施难度，包括但不限于新旧系统的替换，与其他系统间的兼容性问题，减少系统中断时间问题，新旧系统间的数据迁移问题等，在升级改造过程中如涉及到其他系统的调试费用全部由供应商承担。供应商不得以原系统非供应商开发或原建设方不配合为由进行推脱，拒不履行设备安装要求内容，否则视作延误服务，采购人有权按合同相关条款追究违约责任。

供应商应认真踏勘项目现场，熟悉项目现场及周围地形、地貌、水文、地质、施工空间、交通道路等情况，并在响应文件中考虑可能影响报价的一切因素。成交后，不得以不完全了解现场及周边等情况为理由要求提出经济补偿，否则，由此引起的一切后果由供应商负责。

本项目为机房改造项目，供应商应充分考虑机房现有条件，充分利用现有设备，充分考虑采购系统与现有设备的兼容性，进行一体化改造，项目升级改造过程中不得以对于原设备配置不清，技术不掌握为由进行推脱。对于新采购系统与现有设备不兼容所造成的损失由供应商负责。

升级改造期间供应商须严格遵守机房所在公园和采购人单位相关防疫要求，听从现场工作人员指挥，文明施工。

供应商在项目现场就货物的安装、启动、运营、维护对采购人进行培训。

供应商在验收时提供完整的项目竣工资料，包括但不限于（机房平面图、电路图、设备使用手册等）。

供应商全面负责合同系统设备到货后的保管工作，确保到货时完整无损的合同系统设备包装箱体在开箱前维持原样；如在系统设备到货以后开箱前发现到货时完整无损的箱体有损坏，则由供应商负责承担由此引起的一切责任。供应商在系统设备送到采购人指定地点后，3天内派工程技术人员达到现场，在采购人人员在场的情况下开箱清点货物，并根据安装要求进行系统设备的安装、辅件配件的组装、调试及相关软件的安装调试。

供应商派出专业人员在采购人现场负责系统的安装、调试与检验，自备必要的工具，所产生的费用由供应商自理。现场的安装、调试工作由制造商或制造商授权的工程师进行。

在系统升级改造过程中,如因供应商技术人员的错误，造成升级改造进度延误或设备安装质量达不到合同要求，供应商对此承担全部责任。

在系统调试过程中，供应商技术人员负责向采购人技术人员详细解释系统调试方法及调试过程中可能发生问题的处理方法，使采购人技术人员能够完全掌握系统调试的专业技术及操作技能。

本项目为机房改造项目，供应商充分考虑机房现有条件，充分利用现有设备，充分考虑采购系统与现有设备的兼容性，进行一体化改造，项目升级改造过程中不得以对于原系统配置不清，技术不掌握为由进行推脱。对于新采购系统与现有设备不兼容所造成的损失由供应商负责。

由供应商提供货物组装和维修所需的专用工具和辅助材料。

供应商提供本系统的详细技术文件。

供应商在响应文件中详细说明技术指导和技术支持的范围和程度。

供应商在响应文件中提出保修期之后的设备返修流程，包括返修时间，替用设备，以及返修价格。

**8****安全生产、文明施工（安装）与环境保护要求**

8.1供应商应具备上海市或有关行业管理部门规定的在本市进行相关安装、调试服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由供应商自行负责。

8.2在项目安装、调试实施期间为确保安装作业区域及周围环境的整洁和不影响其他活动正常进行，供应商应严格执行国家与上海市有关安全文明施工（安装）管理的法律、法规和政策，积极主动加强和落实安全文明施工（安装）及环境保护等有关管理工作，并按规定承担相应的费用。供应商若违反规定野蛮施工、违章作业等原因造成的一切损失和责任由供应商承担。

8.3供应商在项目供货、安装实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

8.4供应商现场设备安装负责人应具有专业证书，安装人员必须持证上岗。供应商应对设备安装、调试期间自身和第三方安全与财产负责。

8.5供应商在组织项目实施时必须按安装施工计划协调好现场施工（安装）工作，在项目验收合格移交前对到场货物承担保管责任。供应商在项目实施期间必须保护好施工区域内的环境和原有建筑、装饰与设施，保证环境和原有建筑、装饰与设施完好。

8.6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安全文明施工（安装）和安全生产管理措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价措施费中列支必须的费用清单。

**9****售后服务要求（包括延伸服务要求）**

（1）质量保证期：系统升级改造完成，由采购人负责组织验收，自通过验收之日起对本项目提供整体系统3年维保服务，维保经费含在本项目中。

（2）质保期满后，供应商提供系统的终身维修承诺，供应商提供系统维修仅向采购人收取维护的成本费用。在系统出现采购人难以修复的故障时，供应商保证提供必要的技术支持。

（3）在项目完工后3年内，如因用户应用系统做等保测评等需要，供应商对所采购的网络安全系统等提供后续技术支持服务，协助用户完成等保测评工作。

（4）供应商需要对采购人指定人员进行培训，应使采购人相关人员可以独立操作、维护、管理，从而使采购人相关人员能独立进行管理、故障处理、日常维护等工作，确保系统能正常安全的运行。

（5）质保期内系统维修响应时间：接到采购人报修通知后，供应商工程师应立即做出响应，若需要到系统现场维修，工程师要在1小时内到达现场，8小时内排除故障，并提供7天\*24小时全天候维修服务电话。

**10保密要求和知识产权**

10.1 成交供应商应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。成交供应商不得利用工作之便外泄资料或做其他用途，否则成交供应商需承担由此引起的法律责任和赔偿采购人的经济损失。本款规定的效力及于成交供应商及成交供应商的所有雇用人员。

10.2 成交供应商保证对其提供的服务及出售的标的物享有合法的权利，应保证在其出售的标的物上不存在任何未曾向采购人透露的担保物权，如抵押权、质押权、留置权等。

10.3采购人委托开发软件的知识产权归采购人所有。成交供应商向采购人交付使用的信息系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。

10.4在本合同项下的任何权利和义务不因成交供应商发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则成交供应商的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对采购人承担连带责任。

10.5成交供应商应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。

10.6采购人具有源代码修改权和永久使用权。采购人对本次开发的软件拥有产权，具有软件开发平台的永久使用权，成交供应商在售后维护期内（包括续签的售后服务期）应提供软件开发平台的后续升级及因开发平台升级导致的应用软件升级服务。

10.7如采购人使用该标的物构成上述侵权的，则成交供应商承担全部责任。

四、报价须知

**11磋商报价依据**

11.1 磋商报价计算依据包括本项目的磋商文件（包括提供的附件）、磋商文件答疑或修改的补充文书、磋商过程中实质性变动的内容、服务内容一览表（工作量清单）、项目现场条件等。

11.2磋商文件明确的项目范围、实施内容、实施期限、质量要求、售后服务（如果有）、管理要求与标准及考核要求等。

11.3服务内容一览表（工作量清单）说明

11.3.1服务内容一览表（工作量清单）应与供应商须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

11.3.2采购人提供的服务内容一览表（工作量清单）是依照采购需求测算出的主要工作内容，允许供应商对服务内容一览表（工作量清单）内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各供应商应认真了解采购需求，如发现核心工作内容和实际采购需求不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件、补充文件或磋商过程中实质性内容对磋商文件予以更正，否则，应以服务内容一览表（工作量清单）为准。

11.4岗位设置说明

11.4.1 岗位设置应与磋商须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

11.4.2 采购人提供的**岗位设置**是依照采购需求测算出的**各岗位最低配置要求**，与最终的实际履约可能存在小的出入，各供应商应自行认真踏勘现场，了解采购需求。供应商如发现**该表**和实际工作内容不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件、补充文件或磋商过程中实质性内容对磋商文件予以更正，否则，供应商不得**对岗位设置中的岗位类别和数量进行缩减**。

**1****2磋商报价内容**

12.1 本项目报价为全费用报价，是履行合同的最终价格，除采购需求中另有说明外，磋商报价（即磋商总价）应包括项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、硬件集成实施、软件集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。

12.2 磋商报价中供应商应考虑本项目可能存在的风险因素。磋商报价应将所有工作内容考虑在内，如有漏项或缺项，均属于供应商的风险，其费用视作已分配在磋商报价明细表内单价或总价之中。供应商应逐项计算并填写单价、合计价和总价。

12.3在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，供应商应自行考虑，在合同履约期内成交价不作调整。

12.4 供应商按照响应文件格式中所附的表式完整地填写《磋商报价一览表》及各类磋商报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

12.5供应商按照磋商文件格式中所附的表式完整地填写磋商一览表及各类磋商报价明细表，说明其拟提供服务的内容、数量、价格构成等。

供应商只需在《磋商一览表》中报出对应服务期限的磋商价格即可。

13磋商报价控制性条款

13.1 磋商最后报价不得超过公布的预算金额或最高限价。

13.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

13.3 供应商提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。不得违反法规标准规定或合同约定，不得通过降低服务质量、减少服务内容等手段进行恶性低价竞争，扰乱正常市场秩序。

**★**13.4 经磋商小组审定，磋商报价存在下列情形之一的，该响应文件作无效处理：

13.4.1 磋商最后报价和技术方案明显不相符的；

13.4.2 磋商最后报价中缩减磋商小组最终确定的服务内容的；

13.4.3 磋商报价中员工的基本工资低于本市职工最新的最低工资标准的。

**14其他**

无

五、政府采购政策

**15节能产品政府采购（本项目不适用）**

15.1 按照财政部、发改委发布的《关于印发〈节能产品政府采购实施意见〉的通知》（财库[2004]185号）和《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“节能产品品目清单”中的，在技术、服务等指标同等条件下，应当优先采购节能产品。采购人需购买的材料产品属于政府强制采购节能产品品目的，供应商必须选用节能产品。

15.2供应商如选用节能产品的，则应在响应文件中提供国家确定的认证机构出具的、处于有效期之内的节能产品的认证证书；反之，该产品在评审时不被认定为节能产品。

**16环境标志产品政府采购（本项目不适用）**

16.1 按照财政部、环保总局联合印发的《关于环境标志产品政府采购实施的意见》（财库[2006]90号）和《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“环境标志产品品目清单”中的，在性能、技术、服务等指标同等条件下，应当优先采购环境标志产品。

16.2供应商如选用环境标志产品的，则应在响应文件中提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书；反之，该产品在评审时不被认定为环境标志产品。

**17促进中小企业发展**

17.1中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业【2011】300号）执行，参加磋商的中小企业应当提供《中小企业声明函》（具体格式见“磋商文件格式”），反之，视作非中、小微企业，不具备参与磋商资格。如项目允许联合体参与竞争的，则联合体中各方均应为中小企业，并按本款要求提供《中小企业声明函》。

17.2 事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

17.3 如项目允许联合体参与竞争的，组成联合体的中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

17.4供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

**18** **促进残疾人就业**

18.1 符合财库【2017】141号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

18.2 残疾人福利性单位在参加政府采购活动时，应当按财库【2017】141号规定的《残疾人福利性单位声明函》（具体格式详见“磋商文件格式”），并对声明的真实性负责。