附件 2

技术要求

（一）总体要求

根据项目总体建设要求，遵循信息安全建设标准，构建云数融合、架构清晰、资源高效、扩展灵活、信息安全的一体化信息平台，为实现数据安全存储、充分利用，有效纳入平台体系奠定环境基础。为满足系统需求，系统架构包括网络架构及安全部署、计算安全、应用与数据安全三个方面，主要开展信息系统安全建设、基础配套硬件及环境建设。本项目建设内容需与上级单位总体系统兼容，满足《XX 大数据典型应用（XX 大数据应用建设）安全保密建设方案》要求。

1.网络架构及安全部署

此次项目将使用 2 台核心交换机作为项目的核心网络承载，并使用多台交换机完成设备接入。系统建设通过部署 UTM、网络防火墙的方式控制到系统内的数据传输。系统边界通过部署网络防火墙实现网络访问控制。

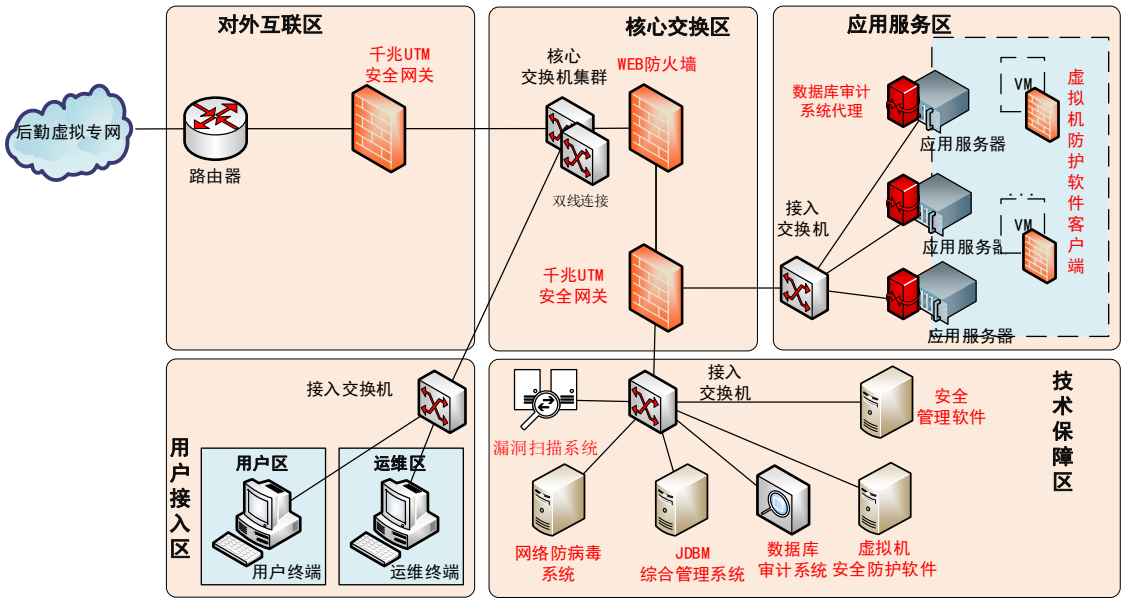
2.计算安全

通过部署主机管控系统实现主机层网络访问控制、外设管控、非法外联告警、用户操作审计、系统登录认证、程序完整性验证。同时部署漏洞扫描系统，定期定时对系统内存在的漏洞风险进行查验，提高整体系统的防护力。通过部署防病毒系统，实现病毒查杀。通过部署虚拟机安全防护软件提供虚拟机安全防护功能，实现对虚拟机的网络包过滤、流量监测、攻击检测等。

3.应用与数据安全

通过部署 Web 应用防火墙，实现针对应用服务攻击行为的检测阻断。通过部署数据库审计系统，实现针对数据库攻击行为的检测与告警。

通过上述三方面的安全技术手段，构成相互协调、适应性强的安全体系结构，为系统建设提供完整安全支撑。



项目整体建设示意图

4.依据文件

《军用关键软硬件自主可控产品名录》

《安可替代工程核心产品名录》

《XX 大数据典型应用（XX 大数据应用建设）安全保密建设方案》

（二）设备清单

序号	设备名称	数量	单位
1	千兆 UTM 安全网关 1（根据“同一链路上相同功能的安全产品应符合异构设计的要求，选用不同架构或品牌产品”这一原则防火墙应选用 2 种以上架构或品牌产品）	1	台

2	千兆 UTM 安全网关 2（根据“同一链路上相同功能的安全产品应符合异构设计的要求，选用不同架构或品牌产品”这一原则防火墙应选用 2 种以上架构或品牌产品）	1	台
3	局域网可信接入鉴权设备	1	套
4	漏洞扫描系统	1	套
5	网络防病毒系统	1	套
6	JDBM 综合管理系统	1	套
7	数据库审计系统	1	台
8	虚拟机安全防护软件	1	套
9	WEB 应用防火墙	1	台
10	安全管理软件	1	套
11	安全服务器	3	台
12	升级带宽	1	套
13	扩展网络端口（出口路由）	1	套
14	核心交换机	2	台
15	业务服务器	1	台
16	存储服务器	1	台
17	管理终端	5	台
18	业务终端	5	台
19	接入交换机	2	台
20	消防系统	1	套
21	精密空调	1	台
22	UPS 系统	1	套
23	视频监控系统	1	套
24	移动运维手推车	1	台
25	42U 机柜	5	套
26	UPS 设备	1	套

（三）技术参数

1.UTM 安全网关 1

序号	指标项
1	▲军用关键软硬件自主可控名录（2022 年版）产品。
2	支持状态检测包过滤，能够基于 IP 地址、端口、协议、时间等属性进行规则设定；
3	支持透明、路由、混合三种工作模式，支持大多数网络服务协议，保障原有网络正常运行，能够提供应用层透明代理，包括 http、ftp、smtp 等；
4	可识别和防御 synflood、pingflood、udpflood、teardrop、sweep、land-base、pingofdeath、smurf、winnuke、圣诞树、碎片等多种攻击；

5	支持端口联动，支持自定义单个或多个端口间的端口联动；
6	整机吞吐量≥10Gbps；
7	最大并发连接≥350 万。
8	全功能开启条件下，吞吐率≥1G ，千兆以太网口数量≥4；
9	★与 UTM 安全网关 2 不能选用同样架构或品牌；

2.UTM 安全网关 2

序号	指标项
1	▲军用关键软硬件自主可控名录（2022 年版）产品。
2	支持状态检测包过滤，能够基于 IP 地址、端口、协议、时间等属性进行规则设定；
3	支持透明、路由、混合三种工作模式，支持大多数网络服务协议，保障原有网络正常运行，能够提供应用层透明代理，包括 http、ftp、smtp 等；
4	可识别和防御 synflood、pingflood、udpflood、teardrop、sweep、land-base、pingofdeath、smurf、winnuke、圣诞树、碎片等多种攻击；
5	支持端口联动，支持自定义单个或多个端口间的端口联动；
6	整机吞吐量≥10Gbps；
7	最大并发连接≥350 万。
8	全功能开启条件下，吞吐率≥1G ，千兆以太网口数量≥4；
9	★与 UTM 安全网关 1 不能选用同样架构或品牌；

3.局域网可信接入鉴权系统

序号	指标项
1	支持基于硬件特征的主机身份注册、注销；
2	提供主机接入策略的制定和分发功能；
3	提供基于硬件特征的主机身份认证功能；
4	能根据主机准入策略和主机安全状态核查结果，实现主机局域网接入时的权限判决功能；
5	能与支持 802.1x 的交换机配合，完成主机局域网准入控制；
6	能对主机接入局域网的行为进行日志记录、告警提示，能按照时间范围对主机上线、下线、认证失败等日志进行汇总统计；
7	能通过图形、表格的方式对主机入网行为进行可视化展现和动态更新；
8	能基于多条件组合对主机入网日志进行查询；
9	支持安全管理系统统一管理、安全审计系统统一审计；
10	支持主机管理数量≥100 台；
11	并发鉴权请求≥400 个。
12	本次项目提供 100 点位授权。
13	▲产品需提供《军用信息安全产品认证证书》

4.漏洞扫描系统

序号	指标项
1	▲军用关键软硬件自主可控名录（2022 年版）产品。
2	支持对各种网络主机、操作系统、网络设备（如交换机、路由器等）、常用软件以及应用系统的识别和漏洞扫描；
3	支持对各种 WEB 应用系统的扫描，支持检测 SQL 注入漏洞、命令注入漏洞、CRLF 注入漏洞、LDAP 注入漏洞、XSS 跨站脚本漏洞、路径遍历漏洞、信息泄漏漏洞、URL 跳转漏洞、文件包含漏洞、应用程序漏洞、文件上传漏洞等；
4	支持对主流网络设备的安全配置核查；
5	漏洞知识库数量≥25000 个；
6	支持的最大并发扫描 IP≥100 个；
7	支持安全管理系统统一管理、安全审计系统统一审计。
8	支持 IPv4 和 IPv6 环境的部署和扫描，可扫描 IP 地址的范围无限制。
9	支持丰富的扫描任务参数设置，包括执行方式、扫描策略、扫描方法、任务优先级、插件超时、模糊扫描等（提供截图证明）。
10	支持对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、Debian、深度、红旗、麒麟、新支点等。
11	支持对主流数据库的识别与扫描，包括：Oracle、Sybase、GBASE、GaussDB、神通、达梦、人大金仓、优炫等，能够扫描的数据库漏洞扫描方法不小于 3000 种（提供截图证明）。
12	支持多种协议口令猜测，包括 SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM、REDIS、SMTP 等（提供截图证明）。
13	支持灵活的扫描策略自定义功能，提供策略编辑向导和详细漏洞信息，支持以插件名称、漏洞编号、CNCVE 编号、CNNVD 编号、BugTraq 编号、CVE 编号、CNVD 编号、安全性、影响平台、简短描述、详细描述、修补建议等进行筛选，支持策略的导入、导出、修改以及合并。

5.网络防病毒系统

序号	指标项
1	能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质；
2	能对本地系统中存在的恶意程序进行有效的识别和查杀；
3	支持对压缩文件的病毒查杀；
4	支持文件监控、手动扫描、定时扫描，以及全盘扫描、快速扫描和自定义扫描等，支持清除、删除、重启清除、重启删除、询问用户处理等恶意代码处理方式；

5	能自动将本地系统中发现、处理的恶意代码样本及处置情况，上报到服务端，并可以接收、执行服务端下发的策略；
6	支持分组下发策略，策略内容包括客户端病毒扫描配置、实时监控配置、定时查毒配置、病毒库升级方式等；
7	支持对补丁进行验证，可以设定补丁自动下载安装和手动安装方式；
8	客户端部署方式支持推送安装、本地安装、WEB 安装；
9	支持客户端软件、恶意代码特征库的在线和离线升级，支持增量升级；
10	支持安全管理系统统一管理、安全审计系统统一审计。
11	本次配备 20 个服务器、主机客户端授权，其中服务器授权数量≥5 个。
12	▲支持部署在国产自主硬件平台和国产自主操作系统上。（提供截图证明）

6.JDBM 综合管理系统

序号	指标项
1	需满足网络安全保密系统建设标准和要求。
2	建设交付的产品包括基础平台、集中管控、终端管控、文印监管、标签管理等子系统软件。
3	能够配合建设方开展保密综合管理系统集成。
4	能够提供适用性强、自动程度高的技术方案，将旧标签文件转换为新标签文件。

7.数据库审计系统

序号	指标项
1	能够分析不同应用访问数据库的方式、行为和主要特征；
2	能够实时监测、识别数据库异常访问和攻击行为；
3	能够智能识别数据库高危操作行为，进行实时告警；
4	能够对数据库导出和数据加工过程中产生的非结构化数据文件提供行为分析与访问控制；
5	支持国产主流数据库和 Oracle 数据库等；
6	支持旁路、代理等部署方式；
7	并发数≥10000；吞吐量≥3GB；SQL 解析能力≥5 万；
8	支持安全管理系统统一管理、安全审计系统统一审计。

8.虚拟机安全防护软件

序号	指标项
1	支持网络包过滤，支持基于状态检测的访问控制功能；支持基于 MAC 地址、传输层五元组（源地址、源端口、目的地址、目的端口、协议）、时间周期特征进行网络数据过滤；

2	支持流量监测，能对进出虚拟计算环境和虚拟机之间的流量进行监控，针对前50 名的通信量，支持对传输层协议、地址、服务端口、平均包长进行流量统计，流量单位包括：包数/单位时间、比特/单位时间；
3	支持攻击检测，支持基于内置规则库对虚拟网络环境中的异常报文攻击、拒绝服务攻击行为进行检测；
4	支持恶意代码检测，能基于内置特征库对进出虚拟计算环境和虚拟机之间的网络流量进行病毒、木马、蠕虫的过滤检测；
5	支持事件管理，支持将攻击事件分为防火墙、入侵检测、恶意代码检测三类，能将事件告警信息上报到管理端，支持上报事件类型的自定义功能；
6	支持策略同步，在虚拟机创建、迁移、复制时，能够保持虚拟机安全防护软件的安全策略同步生效；
7	支持安全管理系统统一管理、安全审计系统统一审计。
8	▲本次配置的虚拟机安全防护授权数量≥10 个。

9.Web 应用防火墙

序号	指标项
1	支持 Web 应用数据包安全检测和过滤，包括 HTTP 协议过滤、SQL 注入攻击防御、跨站脚本（XSS）、跨站请求伪造（CSRF）、XML 恶意代码等；
2	新建连接速率不低于 2.4 万次/秒，网络吞吐量不低于 5Gbps，HTTP 吞吐量不低于 2.5Gbps，最大并发 HTTP 连接数不少于 280 万，攻击检测漏报率小于 5%，支持应用访问控制规则分组管理，规则不少于 2000 条；
3	支持网页防篡改功能；
4	支持安全管理系统的统一管理。
5	包含 3 年特征库升级。

10.安全管理软件

序号	指标项
1	支持设备的运行状态检测，对监控设备的工作状态进行评估。主要监测目标为资源占用情况（CPU、内存、硬盘使用），硬件工作状态，带宽使用状态，故障报警等等；
2	支持安全策略预置，支持网络安全设备策略模板功能，能将安全策略预先制作成模板进行存储和管理，并能根据需要通过策略导入功能加载执行；
3	支持安全策略监察，能对所辖范围及下级的安全防护设备策略状态进行监察，发现变化时能进行提示，给出变化内容，并记录策略变更日志（时间、操作人员、操作的安全设备、变化内容）；
4	支持拓扑管理，能半自动绘制生成所辖范围安全防护设备的网络拓扑图和安全管理级联关系，并以安全管理级联关系和拓扑图的形式实时显示各安全防护设备基本状态，包含正常、告警、故障、失连等；
5	支持状态监控，能基于网络拓扑图选择安全设备显示其运行状态详细信息，包括在线情况、资源占用（CPU、内存、硬盘）、网络接口状态（数量、启用状态、

	带宽消耗）、故障报警、操作日志、安全策略等，并能对设备实施关停和重启操作；
6	支持设备信息管理，能录入、存储、查询安全设备的详细信息，包括类型、来源、管理地址、负责人、所属单位、技术状态（主用、备用、维修、报废）等，并提供所辖安全设备情况的统计报表功能；
7	支持故障告警，能实时显示、记录安全防护设备的故障告警信息，提供故障告警综合条件查询能力，故障告警内容包含告警源、告警时间、故障类型、故障设备信息等；故障告警信息支持标注、处理操作，可与值班日志绑定，在填写值班日志时自动生成故障告警信息的统计信息和处理情况；
8	支持事件告警，能实时显示安全设备的告警信息，能对报警进行过滤和归并处理，告警内容包含告警源、告警时间、告警事件、告警级别、告警数量等；
9	安全管理级联深度≥6 级；
10	单级被管安全设备数≥100 台；
11	最大局域网管理终端数≥1000 台；
12	本级设备和终端状态刷新周期≤60 秒；
13	本级告警信息接收速率≥20000 条/分钟；
14	对攻击事件进行统计和关联分析的服务响应时间≤5 秒。
15	本次项目提供 50 点位授权。

11.安全服务器

1	▲军用关键软硬件自主可控名录（2022 年版）产品。
2	处理器：国产，至少双路 CPU，单颗 CPU 主频不低于 2.0GHz；
3	内存：不小于 128GB；
4	硬盘：不小于 960G SSD，机械硬盘不小于 2TB；
5	不少于 2 路 10Gbps 光口，不少于 2 路千兆网口；
6	至少支持 1+1 冗余电源；
7	外形尺寸：机架式服务器，不高于 4U；
8	支持带外管理。
9	配备国产服务器操作系统

12.升级带宽

将现有 10M 带宽光纤升级为至少满足 1G 带宽光纤，将现有 1 个专用出口，扩展为至少 20 个设备可用接口。

13.扩展网络接口（出口路由）

指标项	详细要求
国产化	▲军用关键软硬件自主可控名录（2022 年版）产品。
主要功能	具备三层转发功能； 支持 VLAN 功能； 支持 ARP、IP、TCP、UDP、ICMP 协议；

	支持严格 URPF 功能； 支持 IGMPv1/v2/v3、PIM-SM、PIM-DM 组播功能； 支持 IPv4 静态路由、OSPFv2、RIP、IS-ISv4 路由功能； 支持 ACL 访问控制列表功能；具备流量控制及流分类；具备 QoS 队列调度能力； 支持 SNMPv1/v2/v3 网管功能、支持 RMON 协议； 具备抗攻击能力； 支持 RIPv2、OSPFv2、IS-ISv4 的路由安全认证； 支持 NTP 功能； 支持用户访问控制功能； 支持 FTP、Ping、Traceroute 功能； 支持 CLI、Telnet、SSH、WEB 管理。
可靠性	无故障连续工作时间：MTBF＞10 万小时； 支持交流电源模块冗余；
性能指标	IPv4 包转发率（64Bytes）：大于 3Mpps； IPv4 转发表容量（FIB）：大于 5000 条； 端口缓存：大于 1500KB； ACL 容量：大于 4000 条；

14.核心交换机

指标项	详细要求
国产化	▲军用关键软硬件自主可控名录（2022 年版）产品。
主要功能	具备二层交换及三层转发功能； 支持 STP、RSTP、MSTP 生成树协议，支持 ERPS 环网保护； 支持 VLAN 协议； 支持横向堆叠虚拟化功能； 支持 ARP、IP、TCP、UDP、ICMP 协议； 支持全双工流控，支持 802.3ad 多链路聚合功能； 支持端口镜像、端口 MAC 绑定、MAC 地址限制； 支持 IGMPv1/v2/v3、PIM-SM、PIM-DM 组播功能； 支持静态、OSPFv2、RIPv1/v2 路由功能； 支持 ACL 访问控制列表；具备流量控制及流分类；具备 QoS 队列调度能力； 支持 SNMPv1/v2/v3 网管功能、支持 RMON 协议； 具备抗攻击能力，支持 uRPF 功能； 支持 802.1x 协议； 支持 RIPv2、OSPFv2 的路由安全认证； 支持用户访问控制、Telnet 访问安全、安全审计功能； 支持 FTP、TFTP、Ping、Traceroute 功能； 支持 VRRP 保护功能；

	支持 NTP 协议； 支持 NETCONF、Openflow
可靠性	无故障连续工作时间：MTBF＞10 万小时； 支持交流电源模块冗余； 支持风扇模块冗余； 支持主控板卡冗余； 支持主控板卡、电源模块、风扇模块热插拔。
性能指标	整机交换容量（双向）大于 1.5Tbps； 支持 256 及以上字节线速转发； IPv4 包转发率（64Bytes）：大于 1100Mpps； 最大 MAC 容量：65535 条； VLAN 条目数：大于 4000 个； 转发表容量（FIB）：65536 条； 端口缓存：大于 4200KB； ACL 容量：大于 4500 条；

15.业务服务器

1	▲军用关键软硬件自主可控名录（2022 年版）产品。
2	处理器：国产，至少双路 CPU，单颗 CPU 主频不低于 2.0GHz；
3	内存：不小于 128GB；
4	硬盘：不小于 3 块 960GB SSD 硬盘；
5	不少于 4 路千兆网口；
6	至少支持 1+1 冗余电源；
7	外形尺寸：机架式服务器，不高于 4U；
8	支持带外管理。
9	配备国产服务器操作系统

16.存储服务器

1	▲军用关键软硬件自主可控名录（2022 年版）产品。
2	处理器：国产，至少双路 CPU，单颗 CPU 主频不低于 2.0GHz；
3	内存：不小于 64GB；
4	硬盘：不小于 2 块 960GB SSD 硬盘；不少于 4 块 8TB 机械硬盘；
5	不少于 4 路千兆网口；
6	至少支持 1+1 冗余电源；
7	外形尺寸：机架式服务器，不高于 4U；
8	支持带外管理。
9	配备国产服务器操作系统

17.管理终端

指标项	详细要求

cpu	核心数≥4，主频≥2.2GHz
内存	≥8G
操作系统	需配备国产桌面端操作系统
硬盘容量	≥1T
软件需求	需安装国产流式软件
	需安装国产版式软件

18.业务终端

指标项	详细要求
cpu	核心数≥4，主频≥2.2GHz
内存	≥8G
操作系统	需配备国产桌面端操作系统
硬盘容量	≥1T
软件需求	需安装国产流式软件
	需安装国产版式软件

19.接入交换机

指标项	详细要求
国产化	▲军用关键软硬件自主可控名录（2022 年版）产品。
主要功能	具备二层交换及三层转发功能； 支持 STP、RSTP、MSTP 生成树协议，支持 ERPS 环网保护； 支持 VLAN 协议； 支持横向堆叠虚拟化功能； 支持 ARP、IP、TCP、UDP、ICMP 协议； 支持全双工流控，支持 802.3ad 多链路聚合功能； 支持端口镜像、端口 MAC 绑定、MAC 地址限制； 支持 IGMPv1/v2/v3、PIM-SM、PIM-DM 组播功能； 支持静态、OSPFv2、RIPv1/v2 路由功能； 支持 ACL 访问控制列表；具备流量控制及流分类；具备 QoS 队列调度能力； 支持 SNMPv1/v2/v3 网管功能、支持 RMON 协议； 具备抗攻击能力，支持 uRPF 功能； 支持 802.1x 协议； 支持 RIPv2、OSPFv2 的路由安全认证； 支持用户访问控制、Telnet 访问安全、安全审计功能； 支持 FTP、TFTP、Ping、Traceroute 功能。
可靠性	无故障连续工作时间：MTBF＞10 万小时；
性能指标	整机交换容量（双向）大于 200Gbps； 支持 256 及以上字节线速转发； IPv4 包转发率（64Bytes）：大于 40Mpps；

	最大 MAC 容量：大于 30000 条； VLAN 条目数：大于 4000 个； 转发表容量（FIB）：大于 15000 条； 端口缓存：大于 2000KB； ACL 容量：大于 900 条；

20.消防系统

指标项	详细要求
气体灭火形态	固定式钢瓶
气体	七氟丙烷
启动	自动控制/手动控制
气体灭火保护面积	≥45m³

21.精密空调

指标项	详细要求
样式	一体化机柜式
精密空调制冷量要求	≥20KW
风量	≥2000m³ /h
送风方式	上送风
制冷方式	风冷
压缩机数量	1
风机数量	1
制冷作用体积	≥45m³
系统温度、湿度控制性能	能按要求自动调节室内温、湿度，具有制冷、加热、加湿、除湿等功能。

22.UPS 系统

指标项	详细要求
额定输入电压	380/400/415
接线制式	三相五线
输入功率因数	≥0.99
输出电压	380/400/415
输出功率因数	0.9
波形	正弦波
切换时间	0ms

过载能力	≤110%负载，持续 60 分钟切换旁路；≤125%负载，持续 10 分钟切换旁路；≤150%负载，持续 1 分钟切换旁路；＞150%负载，立即切换旁路
告警功能	过载、市电异常、UPS 故障、电池欠压等
保护功能	短路、过载、过温、电池欠压、输出过欠压、风扇故障等

23.视频监控系统

指标项	详细要求
存储方式	硬盘
存储容量	≥12T
支持路数	4 路及以上
视频录制分辨率	≥720P
摄像头分辨率	≥720P
硬盘接口	SATA
NVR 功能支持	支持循环写入及非循环写入 支持回放时的暂停，快放，慢放等。 支持常规备份，冗余备份功能。
视频编码	支持 H.264 或更高规格
音频输出	单路
网络协议	支持 IPV4-NTP,DHCP 服务

24.移动运维手推车

指标项	详细要求
移动运维手推车	机房内运维用手推车，含运维使用键盘（USB），鼠标(USB)，显示器(VGA 接口)

25.42U 标准机柜

指标项	详细要求
机柜 U 数	42U
机柜类型	服务器机柜
侧板规格	可拆卸侧板

26.UPS 设备

指标项	详细要求
UPS 机头	输出功率不小于 100kw
UPS 电池组	40 节 100A

（四）其他要求

本项目产品如属于《军用关键软硬件自主可控产品名录》或《安可替代工程核心产品名录》规定类目，必须选用名录中产品；如不属于名录规定产品类目，选用的产品也必须为国产可控品牌。