更正后第三部分 技术要求

一、内网 C86-DMZ 区

1、国产化超融合服务器 3 台

1) 2U 标准机架式服务器，含超融合所需云计算管理平台、计算虚拟化软件、存储虚拟化软件、网络虚拟化软件、连续数据保护软件，采用国产化 CPU 和操作系统。

2) 每节点 CPU 配置≥2 颗 Hygon 5480 2.5GHz 及以上、核心数≥32C，每节点≥24*32GB DDR5 5600 内存；每节点系统盘≥2*480GB SATA SSD；每节点配备≥2 块 1.92T SATA SSD 企业级固态硬盘+6 块 8T SATA HDD 企业级机械硬盘；每节点盘位数≥12；电源：1+1 冗余电源；设备接口≥4 千兆电口+4 万兆光口。含本项目所需多模万兆 SFP 光模块、线缆等配件。

3) ▲提供≥20 台核心虚拟机的连续实时数据保护授权；允许将恢复点目标配置为 5 秒内；连续实时数据保护无需安装插件。**(提供承诺函加盖公章)**

4) 系统需支持在管理界面中通过点击操作栏中的相关按钮来执行备份文件的恢复操作。文件恢复后可以进行下载，系统会记录文件找回日志。

5) 平台需具备以下功能：能够自动识别出现假死状态的主机，并将其标记为“问题主机”，运维人员可通过邮件或短信接收告警信息；平台在此情况下需限制重要虚拟机在“问题主机”上运行，保障核心业务的连续性和稳定性。

6) ▲平台可定期升级，平台需支持在线升级功能，管理员可自定义暂停升级，并允许灵活制定升级顺序计划。**（提供承诺函加盖公章）**

7) 管理平台具备资源监控能力，可实时查看集群 CPU、网络和磁盘的使用情况，探测扫描频率可达到每 20 秒一次。系统管理员可通过告警设置界面，对 CPU、网络和磁盘的占用率阈值进行自定义配置，一旦超出设定上限，管理平台将自动发出告警通知。

8) ▲超融合平台可定期自动检测平台漏洞及版本信息，需第一时间自动推送相关升级通知；支持自动安装补丁、更新系统，并可在必要时执行补丁回退操作。**（提供承诺函加盖公章）**

9) 虚拟机迁移支持指定网口迁移、限制速度、压缩传输迁移，同时虚拟机迁移过程中如因数据写入量过大迁移不能完成，支持迁移强制切换。

10) ▲为保障超融合架构内部横向通信的访问安全及隔离，需支持无数量限制的虚拟路由器和虚拟交换机部署，且分布式防火墙的授权数量应≥100 个，分布式防火墙策略可以自动跟随虚拟机迁移配置。**（提供承诺函加**

盖公章）

2、超融合存储交换机 2 台

1、▲性能要求：交换容量≥2.3Tbps，包转发率≥700Mpps，以官网最小值为准；**（提供相关佐证材料,不限于产品彩页、官网截图、白皮书等）**

2、接口要求：万兆光 SFP+口≥24（含 SFP+模块≥24），QSFP+光接口≥2（含光模块≥2），扩展槽位≥2；

3、扩展性要求：支持万兆、40G 接口，支持防火墙插卡扩展；

4、支持 IPv4、IPv6 静态路由、RIP V1/V2、OSPF、BGP 等路由；支持 IPv4 和 IPv6 环境下的策略路由；

5、支持 VxLAN 二层网关，支持 EVPN；

6、双交流电源、双风扇；

3、超融合管理交换机 2 台

1、▲交换容量≥650Gbps，包转发率≥150Mpps，静音无风扇，以官网最小值为准；**（提供相关佐证材料,不限于产品彩页、官网截图、白皮书等）**

2、提供≥24 个 10/100/1000BASE-T 电口，提供≥4 个 1/10GE SFP+端口（含模块≥4）；

3、支持基于端口的 VLAN，支持基于协议的 VLAN；

4、堆叠链路冗余保护能够快速收敛，收敛时间≤50ms；

5、支持 IPv4/IPV6 双栈管理和转发，支持静态路由协议和 RIP、OSPF 等路由协议，支持丰富的管理和安全特性；

二、东院区内网超融合区（扩容）

1、超融合服务器 4 台

1) 2U 标准机架式服务器，含超融合所需云计算管理平台、计算虚拟化软件、存储虚拟化软件、网络虚拟化软件。

2) 每节点 CPU 配置≥2 颗 intel(R) CPU 主频≥2.10GHZ 核心数≥24C；每节点≥24*32GB DDR4 3200 内存；每节点系统盘≥2*240GB SATA SSD；每节点配备≥12 块 1.92T SATA SSD 固态硬盘；每节点盘位数≥12；电源：1+1 冗余电源；设备接口≥4 千兆电口+4 万兆光口；含本项目所需万兆 SFP 光模块、线缆等配件。

3) ▲本次新增节点须与现有超融合集群平滑扩容，实现业务灵活部署和整体超融合资源池的统一管理，同时在扩容过程中无需停机即可实现超融合资源线性扩展。**（提供承诺函加盖公章）**

2、超融合业务交换机 2 台

1、性能要求：交换容量≥2.3Tbps，包转发率≥700Mpps；

2、接口要求：万兆光 SFP+口≥24（含模块），QSFP+光接口≥2（含模块），扩展槽位≥2；

3、扩展性要求：支持万兆、40G 接口，防火墙插卡扩展；

4、支持 IPv4、IPv6 静态路由、RIP V1/V2、OSPF、BGP 等路由；支持 IPv4 和 IPv6 环境下的策略路由；

5、支持 VxLAN 二层网关，支持 EVPN；

6、双交流电源、双风扇；

3、超融合存储交换机 2 台

1、▲性能要求：交换容量≥2.3Tbps，包转发率≥700Mpps；**（提供相关佐证材料,不限于产品彩页、官网截图、白皮书等）**

2、接口要求：万兆光 SFP+口≥24（含 SFP+模块≥24），QSFP+光接口≥2（含光模块≥2），扩展槽位≥2,；

3、扩展性要求：支持万兆、40G 接口，防火墙插卡扩展；

4、支持 IPv4、IPv6 静态路由、RIP V1/V2、OSPF、BGP 等路由；支持 IPv4 和 IPv6 环境下的策略路由；

5、支持 VxLAN 二层网关，支持 EVPN；

6、双交流电源、双风扇；

4、超融合管理交换机 2 台

1、▲交换容量≥650Gbps，包转发率≥150Mpps，静音无风扇；**（提供相关佐证材料,不限于产品彩页、官网截图、白皮书等）**

2、提供≥24 个 10/100/1000BASE-T 电口，提供≥4 个 1/10GE SFP+端口（含模块≥4）；

3、支持基于端口的 VLAN，支持基于协议的 VLAN；

4、堆叠链路冗余保护能够快速收敛，收敛时间≤50ms；

5、支持 IPv4/IPV6 双栈管理和转发，支持静态路由协议和 RIP、OSPF 等路由协议，支持丰富的管理和安全特性；

三、西院区备份超融合区

1、超融合一体机 8 台

1) 2U 标准机架式服务器，含超融合所需云计算管理平台、计算虚拟化软件、存储虚拟化软件、网络虚拟化软件。

2) 每节点 CPU 配置≥2 颗 intel(R) Xeon(R) Gold 及以上 CPU、主频≥2.10GHZ 核心数≥24C，每节点≥24*32GB DDR4 3200 内存；每节点系统

盘≥2*240GB SATA SSD；每节点配备≥2 块 1.92T SSD 固态硬盘，每节点配备≥6 块 8T 机械硬盘；每节点盘位数≥12。电源：1+1 冗余电源；设备接口≥4 千兆电口+4 万兆光口。所需万兆 SFP 光模块、线缆等配件。

3) 平台虚拟机应具备恢复回收站中项目的功能，且应能够自定义设置回收站内文件的保留期限。平台还应提供查看回收站中文件的详细信息，包括但不限于文件的描述、名称、所占用的存储空间以及删除的具体时间等。

4) 超融合平台必须支持在虚拟机运行时动态调整磁盘分配策略（例如从精简配置切换到预分配模式），且调整应当能够即时生效，无需对虚拟机进行重启。

5) ▲为提升灾备数据中心首次数据同步速率并降低对带宽的压力，可利用数据资源包功能，将需要容灾的云主机备份生成数据资源包存储于外置存储设备中。通过将外置存储设备介质送至灾备数据中心，再导入数据资源包，从而实现灾备数据快速同步。**（提供产品功能截图加盖公章）**

6) 支持容灾状态可视化和状态监控，可以查看异地容灾页面信息，包括容灾状态、站点管理、容灾策略和受保护业务组和恢复计划等信息。

7) 容灾软件需具备模拟灾难恢复演练能力，能够在不影响正常业务运行的情况下，支持按业务分组进行演练，并依据业务访问关系实现联动切换，确保容灾系统的可靠运行与数据的有效可用。

8) ▲为了保证能提供可靠的备份数据管理功能，并满足业务系统对数据保留周期的要求。要求支持对异地容灾的备份数据设置保留周期操作，可以按照不同时间周期保留备份文件；提供≥200 套容灾软件的虚拟机使用授权。**（提供承诺函加盖公章）**

9) ▲为保障超融合架构内部横向通信的访问安全及隔离，需支持无数量限制的虚拟路由器和虚拟交换机部署，且分布式防火墙的授权数量应≥300 个，分布式防火墙策略可以自动跟随虚拟机迁移配置，避免安全防护策略失效。**（提供佐证材料或承诺函）**

10) ▲新增超融合平台需与原有集群兼容；可实现原有集群、容灾集群的容灾业务统一管理。**（提供承诺函加盖公章）**

11) ▲提供≥15 个集群专属监控运维软件许可；平台需具备运维专属桌面数据外发的内容监控功能。可禁止虚拟机通过复制粘贴、外置存储设备进行数据外发操作。如果有数据外发需求，可通过运维专属软件内部的数据外发工具完成。如果有可疑数据外发行为，系统会及时告警通知管理

员。**（提供相关佐证材料，不限于产品彩页、官网截图、白皮书等）**

3、业务交换机 2 台

1、性能要求：交换容量≥2.3Tbps，包转发率≥700Mpps；

2、接口要求：万兆光 SFP+口≥24（含模块），QSFP+光接口≥2（含模块），扩展槽位≥2；

3、扩展性要求：支持万兆、40G 接口，防火墙插卡扩展；

4、支持 IPv4、IPv6 静态路由、RIP V1/V2、OSPF、BGP 等路由；支持 IPv4 和 IPv6 环境下的策略路由；

5、支持 VxLAN 二层网关，支持 EVPN；

6、双交流电源、双风扇；

4、存储交换机 2 台

1、性能要求：交换容量≥2.3Tbps，包转发率≥700Mpps；

2、接口要求：万兆光 SFP+口≥24（含模块），QSFP+光接口≥2（含模块），扩展槽位≥2；

3、扩展性要求：支持万兆、40G 接口，防火墙插卡扩展；

4、支持 IPv4、IPv6 静态路由、RIP V1/V2、OSPF、BGP 等路由；支持 IPv4 和 IPv6 环境下的策略路由；

5、支持 VxLAN 二层网关，支持 EVPN；

6、双交流电源、双风扇；

5、管理交换机 2 台

1、▲交换容量≥650Gbps，包转发率≥150Mpps，静音无风扇;**（提供相关佐证材料,不限于产品彩页、官网截图、白皮书等）**

2、提供≥24 个 10/100/1000BASE-T 电口，提供≥4 个 1/10GE SFP+端口（含模块≥4）；

3、支持基于端口的 VLAN，支持基于协议的 VLAN；

4、堆叠链路冗余保护能够快速收敛，收敛时间≤50ms；

5、支持 IPv4/IPV6 双栈管理和转发，支持静态路由协议和 RIP、OSPF 等路由协议，支持丰富的管理和安全特性；

四、网络安全扩容

1、终端安全软件

1） ▲提供≥120 套服务器版终端安全软件，≥1000 套 PC 版终端安全软件；支持通过单位现网终端安全软件控制中心统一管理。**（提供承诺函加盖公章）**

2) 定期梳理高可利用漏洞，并在控制中心上进行展示。同时支持对资产进行统一漏洞检测，并支持设置热点漏洞的定时检测功能。
3) 针对单位无法确认的威胁文件，可通过控制平台接入云端专家进行研判分析。
4) 提供 U 盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马。
5) ▲当现有网络中的下一代防火墙检测到某台终端存在僵尸病毒、蠕虫病毒、木马病毒等的恶意指令通信行为、命令与控制通信行为时，可以手动或自动方式将相关信息推送至现网中的下一代防火墙，由现网中的下一代防火墙负责对该恶意指令通信行为、命令与控制通信行为进行封锁拦截，从而实现对远程控制通信行为的精准防护。同时，防火墙针对此类事件后续可自动化处置。**（提供承诺函加盖公章）**
6) ▲服务器版终端安全软件提供三年软件升级，PC 版终端安全软件提供一年软件升级。**（提供承诺函加盖公章）**

2、全网行为管理 1 台

1) 网络层吞吐量≥10Gbps，应用层吞吐量≥1.2Gbps，带宽性能≥1Gbps；支持用户数≥6000；每秒新建连接数≥1 万,最大并发连接数≥50 万；接口≥4 千兆电口+2 万兆光口 SFP+；≥1T SSD 硬盘。
2) ▲支持与现有全网行为管理双机部署，降低单点故障风险。**（提供承诺函加盖公章）**
3) 支持首页分析显示接入用户人数、终端类型；带宽质量分析、实时流量排名；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行。
4) 支持针对特定用户和管理员配置免认证、审计和控制密钥。
5) 支持基于端口的网络接入控制，可对接本地和 AD 域用户源，同步账号到本地，可对接外部 CA 认证服务器进行证书认证，可在线查询证书状态。
6) 支持通过改善网络中的其他设备到本地设备链路中的丢包现象，来减缓网络中的其他设备到本地设备流量，从而解决网络流量压力大的问题。
7) 支持主流云服务应用管控，内置云服务应用分类库，帮助管理员统一配置策略。
8) 支持与零信任产品实现联动，能够向零信任系统同步上报日志。
9) ▲本系统能够与现有的下一代防火墙进行认证协同工作，支持将用户的认证信息传递至下一代防火墙，从而实现用户的统一身份认证。**（提供**

承诺函加盖公章）

3、零信任综合网关 1 台

1) 最大加密流量≥400Mbps，最大并发用户数≥700；接口≥6 千兆电口+2 千兆光口 SFP；提供≥500 套零信任接入授权软件。

2) 为适应组织灵活多变的管理需求，平台支持配置动态访问规则，配备可定制的访问控制列表规则引擎。该引擎能够根据终端环境、用户身份、用户动作等因素进行配置策略，并可根据现使用的不同操作系统制定专门的或多系统的访问控制策略。当检测到不符合安全条件的情况时，平台可执行如短信增强认证、系统告警等灵活的处理措施，实现分级管控处理，从而在保障接入访问体验的同时，确保安全防护的有效性。

3) 为增强业务应用的数据安全防护能力，零信任系统需支持为已发布的网页应用启用水印功能。水印内容可涵盖用户名及当前年月日，以此实现威慑与便于事后调查的效果。同时，该系统应具备对网页应用的多重安全管控能力，包括禁止复制、打印、下载操作，管控鼠标右键功能，以及屏蔽浏览器开发工具调试功能，全面保障数据安全与设备自身运行安全。

4) 对于多线路接入单网关访问业务的场景，支持时延优先的选路模式，支持周期性探测线路时延和多次探测确认恶化后切换。多网关接入访问业务的场景，支持最低时延+相对时延阈值随机选择策略。

5) 为改善在网络质量较差环境中的连接访问性能，需支持对传输控制协议进行优化，增强传输隧道的丢包和抖动抵抗能力，从而实现网络质量较差的环境下的加速访问效果。

6) 为了最大限度减少网络和业务的暴露风险，零信任平台应具备单包认证控制功能，支持结合 TCP/UDP 协议的单包认证控制技术。未经授权的用户将无法连接到零信任平台，也无法探测到平台服务端口。

7) 可自动为出现异常登录行为的用户日志添加标识，并将其归类至用户安全日志。用户安全日志所包含的内容应涵盖账号安全问题、中间人攻击、单包授权安全风险事件、Cookie 劫持等。

8) ▲产品可联动现网终端安全软件的检测评分作为入网准入的策略条件，针对终端入网进行管理，防止违规终端入网。**（提供产品功能截图加盖公章）**

9) ▲提供三年产品质保和软件升级，提供移动应用自动封装服务三年。**（提供承诺函加盖公章）**

4、安全托管服务

1) 提供50个核心业务系统IP资产的7*24小时安全监测及应急响应处置服务。

2) ▲服务提供方的云端服务平台应与现有以及本次采购的主要安全设备（如下一代防火墙、安全态势感知平台等）进行对接，能够实时接收并借助这些安全设备所检测到的安全事件信息和安全日志数据，提供全天候（7×24小时）的服务支持。**（提供承诺函加盖公章）**

3) 针对资产扫描所发现的高危、可能被黑客利用漏洞，服务方须为采购人针对每个漏洞采取有效的技术防护，以保障采购人不会因这些漏洞导致重大安全事件或产生损失;服务方对上述漏洞防护的有效率需达到 99%。

4) 服务方应当具备云端监测与分析系统，通过采集采购人单位各类网络安全设备的告警日志，为采购人单位提供全天候（7×24小时）的云端安全威胁监测和分析能力，系统用户界面应支持对安全事件的跟踪与分析功能。

5) 服务方需配备一名专业的安全专家担任专属服务经理，随时响应使用方关于网络安全的各类咨询问题，并提供全天候（7×24小时）的在线服务支持。此外，在节假日期间，服务方还需每日向我单位提供《节假日值守报告》，确保网络安全保障不间断。

6) 服务方需提供移动端服务门户，通过清晰可视化的风险或漏洞的消减过程，直观实时了解当前网络安全隐患和威胁闭环情况。

五、接入交换机

1、接入交换机4台

1、交换容量≥650Gbps，包转发率≥110Mpps，静音无风扇；

2、提供≥24个10/100/1000BASE-T电口，提供≥4个1000 BASE-X SFP端口；

3、支持基于端口的VLAN，支持基于协议的VLAN;

4、堆叠链路冗余保护能够快速收敛，收敛时间≤50ms；

5、支持IPv4/IPV6双栈管理和转发，支持静态路由协议和RIP、OSPF等路由协议，支持丰富的管理和安全特性；

六、核心交换机2台（核心产品）

1、▲基本要求：交换容量≥1000Tbps（以最小值为准），包转发率≥300000Mpps；主控引擎槽位≥2，交换网板槽位≥4，业务插槽数≥6，1+1冗余电源模块；**（提供相关佐证材料）**

2、为保证产品散热契合机房风道，严格前后风道设计；

3、扩展性要求：为满足不同接口互联的需求，要求设备支持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、100G 端口且单槽位万兆端口密度≥48；

4、支持命令行采用分级保护方式，防止未授权用户的非法侵入，为不同级别的用户有不同的配置权限；

5、双栈：支持 IPv4 Portal、IPv6 Portal 及 Portal 双协议栈功能；

6、支持设备在线状态监测机制，实现对包括主控引擎，背板，芯片和存储等关键元器件进行检测；

7、支持 Portal 认证，支持 MAC 认证，支持 IEEE 802.1x 和 IEEE 802.1x SERVER；

8、支持 IP 地址、VLAN ID、MAC 地址和端口等多种组合绑定；

9、配置要求：配置双主控，双交换网板，双交流电源模块，满配风扇模块；配置≥48 端口万兆以太光接口（含模块），≥48 端口千兆以太网电接口，≥24 端口万兆以太网光接口，≥2 端口 40G 以太网光接口（含模块）；

11、3 年原厂质保。

七、运维管理平台

1、支持对网络设备的性能异常、可用性故障的探测与管理；

2、支持物理拓扑图及逻辑协议视图管理；

3、支持网络设备的 IP、MAC、路由表；

4、对于未识别的网络设备快速开发；

5、操作系统管理：提供对常见操作系统的监控管理，包括 Windows、AIX、IBM AS400 / iSeries、FreeBSD/OpenBSD、Linux、Mac OS 等，同时支持对国产操作系统如中标麒麟、银河麒麟、凝思磐石等的监管；

6、支持对 ORACLE、DB2、Sybase、SQLServer 等主流数据库的管理；

7、数据库管理：提供对常见数据库服务器的监控管理，包括 MySQL、Oracle、MS SQL、DB2、PostgreSQL、MongoDB、ElasticSearch、MemCached、达梦、人大金仓、Redis 等；

8、中间件管理：提供对常见中间件服务器的监控管理，支持对性能、状态等信息的监控，包括 WebLogic、WebSphere、Tomcat、JBoss、GlassFish、RabbitMQ、TongLINKQ、WebSphere MQ、Tuxedo、Active MQ 等；

9、Web 应用管理：提供对常见 Web 服务器的监控管理，包括 Apache、IIS、Nginx、PHP 服务；

10、存储管理：可通过 SMI-S 协议、SNMP 协议或者 RESTful 协议对华为、HP、

H3C、DELL、IBM、EMC、Hitachi 等存储设备进行集中监控管理；

11、服务器硬件管理：必须支持通过 IPMI、SNMP、RESTful 和 Redfish 协议带外方式对主流厂商服务器进行硬件层面的精细化管理，包括服务器序列号、硬件型号、产品 ID、风扇状态/风速、温度、电源功率/状态/模式、处理器状态/缓存/速度、内存大小/状态/频率、网卡状态相关信息的监控。同时支持服务器硬件系统事件的采集，包括硬件错误事件，并支持将服务器系统事件转换为运维平台的告警信息；

12、监控模板：对同类型监控对象支持按需自定义监控模板，包括采集哪些指标、采集间隔、阈值、告警级别、触发次数，实现灵活高效的个性化监控需求；

13、▲远程监控：支持远程 URL 探测；支持远程 Ping 探测；支持远程 Telnet 探测；**（提供相关佐证材料）**

14、支持服务器通用 vKVM 远程控制台能力，可以实现带外登录管理功能，提供产品功能截图证明；

15、支持实例级阈值：针对单个资源单个指标的指定实例设置阈值，包括实例值变化阈值以及实例丢失阈值；

17、▲本次配置网络设备管理授权≥25 个，服务器硬件管理授权≥20 个，存储硬件，操作系统，数据库，中间件管理授权共≥25 个；**（提供承诺函加盖公章）**

八、技术服务

1、网络及安全设备、存储优化服务

1、对现有安全设备使用情况进行梳理，安全设备策略精细化调整配置，终端杀毒部署。

2、对网络架构进行优化，包括东院区、西院区所有网络设备的配置，架构调整，链路调整等

3、对原 PACS 老数据进行梳理,存储故障维修。