|  |
| --- |
| **赣州市中医院机房改造项目清单** |
| **序号** | **产品名称** | **参数要求** | **单位** | **数量** |
| **一、超融合数据中心** |
| 1 | 超融合一体机 | 1、标准2U机架式服务器，配置≥2颗Silver 4114 2.2GHz，10核20T； 2、配置≥160G内存，ECC DDR4；3、配置≥1块 128GB SSD系统盘（不占槽位），≥2块480G SSD硬盘，≥4块 6T SATA数据盘，≥12个数据盘槽位；4、配置≥2个万兆光口，≥6个千兆电口；5、配置1+1冗余电源； 6、为了方便后期运维及管理，要求超融合一体机、超融合软件、备份一体机、虚拟化防火墙为同一品牌。  | 台 | 4 |
| 2 | 超融合软件 | 1. 软件按照物理CPU颗数进行授权，本次项目包含8颗CPU超融合授权数

2、超融合软件采用裸金属架构，无需绑定操作系统即可搭建超融合平台，底层内核基于KVM技术开发； 3、能够提供平台整体性能监控功能，对资源池中CPU、网络、磁盘使用率等指标进行实时的数据统计，并能反映现阶段物理机、虚拟机的资源瓶颈； 1. 支持通过延伸集群的方式实现跨数据中心的数据双活，每个数据中心均保存完整的数据副本，数据同时写入到两个数据中心，任何一个数据中心故障，数据零丢失，业务分钟级别恢复；
2. 为了防止误操作导致的数据丢失，要求产品具备快速浏览指定CDP备份内的文件，可快速的从CDP备份中找回数据文件，查看虚拟机文件目录的操作可做安全审计；

6、每个虚拟机都可以安装独立的操作系统。为获得良好的兼容性，操作系统需支持包括Windows、 Linux，并且支持国产操作系统包括：红旗linux、中标麒麟、中标普华、深度linux等；7、产品支持无代理跨物理主机的虚拟机USB映射，当需使用USB KEY时，无需在虚拟机上安装客户端插件，且虚拟机迁移到其它物理主机后，仍能正常使用迁移前所在物理主机上的USB资源；8、支持虚拟机的HA功能。当物理服务器发生故障时，该物理服务器上的所有虚拟机，可以实现在集群之内的其它物理服务器上重新启动，保障业务连续性；9、支持数据写入优化机制，将高速SSD作为写缓存，数据先写到SSD，再回写到机械硬盘，提升写IO性能； 10、为了缩短我院新业务系统的上线时间并提升IT管理人员的工作效率，要求产品在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，快速的实现整个业务逻辑，并且可以连接、开启、关闭虚拟网络设备，支持对整个平台虚拟设备实现统一的管理； 11、为了实现虚拟机秒级启动，要求支持多种克隆方式，可根据需求选择克隆方式，包括节省空间的基于源虚拟机镜像文件生成链接克隆虚拟机；和保证业务高性能的基于源虚拟机镜像文件生成链接克隆虚拟机, 后进行源虚拟机数据的完整拷贝;(需提供功能界面截图并加盖厂商公章) | 套 | 1 |
| 3 | 备份一体机 | 1、硬件参数：CPU型号：E3-1230 v6 3.50GHz，CPU个数：1，内存：2\*16GB，系统盘：1\*64GB，缓存盘：2\*480G SSD，数据盘：6\*4T SATA，标配盘位数：12，电源：单电源，接口：2千兆电口+2万兆光口。2、通过标准服务器和软件定义技术构建存储资源池，实现弹性扩展、按需分配，为不同业务分配不同存储资源（高性能存储资源、低成本大容量存储资源等）。EDS存储可提供软硬一体化交付或纯软件交付两种方式，一个平台支持块、文件、对象多种存储服务。 | 套 | 1 |
| 4 | 虚拟化防火墙 | 1. 虚拟防火墙网络层吞吐量3600Mbps,应用层吞吐量240Mbps,并发会话数400W;为了保障产品兼容性及易管理性，要求所投超融合一体机、超融合软件、虚拟化防火墙为同一品牌；2、支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；3、具备对常见网络协议（SSH、FTP、RDP、VNC、Netbios）和数据库（MySQL、Oracle、MSSQL）的弱密码扫描功能；4、支持受保护业务和用户的关联安全事件展示；支持以攻击链方式来匹配和展示资产遭受到的攻击行为；

5、支持DDoS攻击防护、Web应用安全防护、入侵防护功能、支持URL过滤和文件过滤功能、僵尸主机检测、网页篡改防护等功能，保障业务的高安全性； 6、为了保证在发现问题后能够及时的进行安全防护并全面保障业务安全，所投产品可提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测并一键生成防护规则；（需提供产品功能截图，并加盖厂商公章） 7、为了保证IT运维人员能全面的了解到当前网络中的安全风险及时提前处理，要求产品能自动生成综合安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的统计，具备有效攻击行为次数统计和攻击举证；（需提供产品功能截图，并加盖厂商公章） | 套 | 1 |
| 5 | 存储网交换机 | 15个10G SFP+万兆光口，1个SFP千兆光口，8个千兆电口；交换容量1.28Tbps/12.8Tbps，包转发率420Mpps，支持全端口线速转发；支持aNAC统一管理、统一查看状态、VLAN等配置管理；支持终端识别、终端准入、安全防护及安全画像可视；支持胖瘦一体化 | 台 | 2 |
| 6 | 业务网交换机 | 24个10/100/1000Base-T自适应电口，4个万兆SFP+光口，交换性能：336Gbps/3.36Tbps包转发率：108Mpps/126Mpps，支持全端口线速转发；支持M-LAG、IGMP snooping、ACL、QoS、802.1x、Portal认证等； | 台 | 2 |
| 7 | 核心交换机 | 24个10G SFP+万兆光口，24个千兆电口，2个40GE QSFP+光口；交换容量≥2.56Tbps/23.04Tbps，包转发率≥720Mpps，支持全端口线速转发；支持aNAC统一管理、统一查看状态、VLAN等配置管理；支持终端识别、终端准入、安全防护及安全画像可视；支持胖瘦一体化；支持双电源模块，默认 1个150W可插拔AC交流电源，并预留一个扩展可插拔电源槽位 | 台 | 1 |
| 8 | 20KVA UPS电源 | MF100-12/12V100AH 蓄电池32节；C16电池柜2套；满足1-2小时备用电源要求。 | 套 | 1 |
|  |
| **二、安全等保建设** |
| 1 | 内网应用防火墙 | 1、网络层吞吐量：5.5G，应用层吞吐量：700M，并发连接数：1800000，新建连接数（CPS）：50000，硬件参数：规格：1U，内存大小：4G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP；具备WEB应用防护、入侵防御、实时漏洞分析、防僵尸网络等功能 2、支持路由，网桥，单臂，旁路，虚拟网线部署模式。3、含传统防火墙功能（NAT、路由、访问控制ACL、IPSec VPN、DDoS、会话控制、用户认证、流控、双机）。4、内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护5、内置Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后面攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为; 6、支持对HTTP异常请求协议检测和防护攻击，检测内容包含HTTP请求信息的方法及参数长度等；具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵；（需提供功能界面截图并加盖厂商公章） | 台 | 1 |
| 2 | 全流量威胁分析系统 | 1、性能参数：应用吞吐量：600Mbps。硬件参数：规格：1U，内存大小：16G，硬盘容量：128GB SSD+2TB SATA，电源：单电源，接口：6千兆电口+2千兆光口SFP。2、定位异常网络行为，及时检测和响应NDR，可联动EDR，在网络和端点之间实现设备间智能联动，单点发现风险，全局响应风险，并自动建立免疫系统，为用户提供完整有效的安全保护； 3、支持通过云端沙盒对全球威胁情报源进行验证，提取有效信息形成规则定期更新到僵尸网络识别库，增量提升检测能力。4、支持对平台的CPU、内存、磁盘利用率进行实时监控，同时支持对核心进程的资源占用率进行实时分析。5、支持自动识别网络内部主机网段和外网网段；支持通过流量中的应用内容自动区分网络内部网段IP是属于PC还是服务器； 支持自动识别已知服务器，通过被动检测机制，对经过探针的流量进行分析，识别已知服务器对外提供的所有服务、已开放端口及端口传输的协议/应用等。6、支持感知业务/服务器资产，可定义IP地址、所属分支、主机名、责任人、责任人邮箱、所属业务、操作系统、服务与端口等信息，并支持基于流量支持识别操作系统、开放的服务与端口。 7、支持与同品牌防火墙进行联动响应，支持平台自动下发安全策略到防火墙上，阻断攻击流量（需提供功能界面截图并加盖厂商公章） | 台 | 1 |
| 3 | 日志审计 | 1、含50个主机审计许可证书（可扩展到150个主机审计许可），配备2\*1T的硬盘，采用raid1的技术，实际可用是1T，6个千兆电口，接口可扩展；2、支持获取各种主流网络及数据库访问行为，支持Syslog、WMI、OPSEC Lea、SNMP trap和LAS-1000专用协议等协议事件日志； 3、支持通过Http、Https、FTP、SFTP、SMB等协议获取各类文件型日志，支持基于SQL/XML标准内容获取； 4、支持通过页面直接将日志文件导入或以syslog方式接收日志信息，支持日志类型：UNIX、WINDOWS事件[2000、2003、2008、XP、VISTA、Win7及以上版本]、网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]、AS400日志、数据库访问[Mysql]、WEB访问[Apache、IIS、Tomcat、Nginx、Weblogic、Resin、Websphere]、文件访问[VSftpd、Pureftpd、NCftpd、IISftpd、Proftpd、Glftpd、Serv-u]、数据库服务[Oracle、Mssql、Mysql、DB2、Informix、Sybase]、WEB服务[Apache、Tomcat、Nginx、Weblogic、Resin、Websphere]、FTP服务[VSftpd、NCftpd、Proftpd、Glftpd、Serv-u]； 5、支持SNMP日志采集，支持日志类型：网络及安全设备[深信服、Cisco、Array、Juniper、H3C、神州数码、绿盟、天融信、安氏领信、网神]； 6、支持挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，需支持GUI方式的关联规则设置功能，关联的类型包括基于规则和基于统计的；（需提供功能界面截图并加盖厂商公章） | 台 | 1 |
| 4 | 杀毒软件 | 1. 配置300点PC终端防病毒功能；3年升级服务；配置≥20点服务器端防病毒功能；3年升级服务； 2. 产品采用B/S架构管理端，具备终端防病毒和终端安全管控一体化的功能。支持设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能； | 套 | 1 |
| 5 | 网闸 | 1、吞吐量300Mbps,标配提供文件交换、数据库访问和同步、视频交换、组播代理、访问交换等功能模块； 2、采用2+1系统架构即内网单元+外网单元+FPGA专用隔离硬件。不能采用网线等形式直通； 3、产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC模块、MODBUS模块、组播代理模块、用户自定义应用模块等各类应用模块，并可控制相应应用协议的动作、参数、内容； 4、支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名；支持文件内容深度检测，对包含关键字内容的文件进行过滤； 5、同步功能由网闸主动发起并完成，无需在数据库安装方软件，支持Windows、Linux、Unix 等多种数据库操作系统，且网闸无需开放端口以杜绝安全隐患； | 台 | 1 |
| 6 | 终端准入 | 1、网络层吞吐量（大包）：3Gb，应用层吞吐量：300Mb，带宽性能：200Mb，准入终端数：400，包转发率：27Kpps，每秒新建连接数：1600，最大并发连接数：80000。硬件参数：规格：1U，内存大小：4G，硬盘容量：128G minisata SSD，电源：单电源，接口：4千兆电口。2、实现全网资产、身份、行为可视可控，智能感知内部威胁风险，帮助用户构建有效防御体系。 | 台 | 1 |
| 7 | 堡垒机 | 默认含50个运维资源授权（可扩展到150个），提供运维人员单点登录、用户权限细粒度授权及访问控制、运维过程审计等功能，并满足等级保护三级建设要求，含三年硬件保修和软件升级服务。 | 台 | 1 |
| 8 | 外网下一代防火墙 | 1、性能参数：网络层吞吐量：4G，应用层吞吐量：1G，并发连接数：100万，新建连接数（CPS）：2万，硬件参数：规格：1U，内存大小：4G，硬盘容量：64G minisata SSD，电源：单电源，接口：6千兆电口+2千兆光口SFP。2、提供L2-L7层各类威胁的检测和防护，是一款能够有效应对传统网络攻击和未知威胁攻击的网络安全产品,具备入侵防御、网页防篡改、实时漏洞分析、防僵尸网络等功能. | 台 | 1 |
|  |
| **三、环境改造** |
| 1 | 机房门禁系统 | 指静脉门禁系统设备，满足机房门禁安全要求。 | 套 | 1 |
| 2 | 机房消防系统 | 七氟丙烷机房消防系统，满足机房消防要求。 | 套 | 1 |
| 3 | 项目集成 | 包含各系统安装、调试，机房整理等费用。 | 项 | 1 |
|  |  |  |  |  |