磋商内容及技术要求

序号	设备类型	技术指标	设备数量	单位	备注
1	服务器及网络设备				
1.1	业务网/管理网交换机	24 个 10/100/1000Base-T 自适应电口，4 个万兆 SFP+光口；交换容量≥336Gbps/3.36Tbps，包转发率≥108Mpps/126Mpps，支持全端口线速转发；支持 NAC 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。	2	台	
1.2	存储同步交换机	1. 设备高度要求≤2U，节约机柜空间 2. 交换容量≥2.5Tbps，包转发率≥700Mpps； 3. 设备固化万兆光口≥24 个，40G 光口≥2 个，扩展槽位≥2 个； 4. 实配可拔插模块化双电源和可拔插模块化双风扇； 5. 支持跨设备链路聚合，单一 IP 管理，统一的路由表项，支持通过标准以太端口进行堆叠；支持远距离堆叠； 6. 支持静态路由、RIP v1/2、OSPF、BGP 等动态路由协议，支持 RIPng、OSPF V3、IS-IS V6、BGP+ FOR IPV6、IPV6 策略路由，支持 VRRP，支持等价路由；	6	台	
1.3	光模块	万兆多模光模块	162	个	
1.4	辅材	辅材一批	1	批	
2	虚拟化及异地容灾备份软件				
2.1	云计算管理平台	1.★支持对我院 2019 年建成的超融合平台进行统一管理(注：目前是日立品牌服务器及深信服、VMware 等品牌的虚拟化软件)。(提供相关证明) 2.支持多超融合服务器集群统一管理,含本次建设高性能集群和大容量集群以及现有的集群； 3.★虚拟机、虚拟存储、虚拟网络资源能够在同一管理平台下实现集中式的管理和运维，无需在多个管理平台软件之间切换即可实现虚拟机、虚拟存储、虚拟网络等资源等分配、回收、利用率监控，简化运维管理； 4.云平台具备功能，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； 5.支持业务整体可靠性指标的集中展示，包括业务可靠性、平台可靠性和硬件可靠性，方便管理员能直观地掌握整个数据中心的可靠性状态。(需提对应大屏展示功能截图，并加盖厂商公章) 6.★云厂商通过可信云评估，提供相应的可信云认证报告；	76	CPU	**其中 40 颗 CPU 授权用于纳管医院本地机房 20 台服务器**

2.2	计算服务器虚拟化软件	实现基础虚拟化和平台，简单、经济、快速的实现业务应用软件与底层服务器的解耦合，封装并隔离各个业务软件，从而实现服务器的基础虚拟化，同时提高应用平台的整体可用性，可管理性。 1.需要满足业务高可用功能（HA）和虚拟机热迁移（vMotion）等基本功能，保障业务连续性； 2.★满足集群动态资源分配（DRX）功能，包括但不限于热添加CPU和内存，根据需要为虚拟机在线添加更多资源，满足业务高可用性要求； 3.★管理架构去中心化，管理平台不依赖于某一个虚拟机或物理机部署，消除简单点故障隐患（须提供厂商支持分布式管理平台的参数确认函，加盖厂商公章）； 4.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支持需要包括Windows、 Linux，并且支持国产操作系统包括：红旗linux、中标麒麟、中标普华等（需提供包括以上操作系统列表的产品功能截图，并加盖厂商公章） 5.支持通过专用的快虚/快速还原工具，实现快速将物理机转换为虚拟化平台，并且可实现虚拟化平台快速还原为物理机原有操作系统。 6.支持在线的带存储的虚拟机迁移功能，可以在不停机状态下和非共享存储的环境中，实现虚拟机在集群内的不同物理机和上迁移，保障业务连续性。 7. 需要满足纳管第三方主流虚拟化平台，提供对现有的Vmware虚拟化及深信服超融合平台上的虚拟机进行管理，支持在本地管理平台实现对VMware vCenter中的虚拟机备份，并能够在超融合的平台实现VMware虚拟机的启动恢复(提供产品功能界面截图)； 8. ★支持双向迁移，可将VMware、深信服超融合虚拟机在运行状态下迁移到超融合平台上，也可将超融合平台上的虚拟机在运行状态下迁移到VMware vCenter的集群中(提供产品功能界面截图)； 9.★服务：提供原厂工程师实施，提供3年原厂升级服务，3年原厂工程师上门服务，提供3年原厂专属技术服务经理7×24小时400/800及在线响应服务，3年内提供原厂工程师每半年一次巡检服务；提供厂商针对此项目的项目授权书及售后服务承诺函加盖原厂公章。	36	CPU	
2.3	网络虚拟化软件	以软件形式创建整个网络，容灾机房服务器的虚拟化授权。 1.在管理平台上可提供大屏展示功能，展示数据中心业务运行状态。 2.★满足支持主流数据库，2种以上（如oracle、sqlserver、Weblogic数据库及中间件监控）的应用性能监控，实现数据库的语句故障定位排错，时延分析。（需提供产品功能截图，并加盖厂商公章） 3.提供分布式虚拟交换机功能，实现虚拟机之间或与物理机之间的网络调度，通过分布式虚拟交换机对虚拟化集群环境进行统一的网络管理。 4.提供分布式防火墙功能，实时拦截日志显示，以及支持“数据直通ByPass”功能，出现问题快速定位问题。 5.★提供故障排查功能，虚拟网络设备故障可以快速定位，保障业务连续性（需提供产品功能截图，并加盖厂商公章）。 6.★服务：提供原厂工程师实施，提供3年原厂升级服务，3年原厂	36	CPU	

		工程师上门服务，提供3年原厂专属技术服务经理7×24小时400/800及在线响应服务，3年内提供原厂工程师每半年一次巡检服务；提供厂商针对此项目的项目授权书及售后服务承诺函加盖原厂公章。			
2.4	存储虚拟化软件	存储虚拟化软件，能够实现存储多副本，高性能读写缓存，存储弹性扩展，数据故障切换，磁盘故障告警，软件平台升级更新等功能。 1.★支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能； 2.采用分布式架构设计，由多台物理服务器组成分布式存储集群，通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out架构），扩容过程保证业务零中断； 3、★支持数据重建智能保护业务性能，可以对数据重建速度进行智能限速，避免数据重建过程中IO性能占用导致对业务的性能造成影响。（需提供产品功能截图，并加盖厂商公章） 4、分布式存储能够提供超高性能，性能随着节点数增加线性增长，能够提供百万级IOPS和12GB/s以上的带宽能力。(需提供产品功能截图，并加盖厂商公章） 5、★支持2个或以上多副本冗余功能，副本互斥地保存在集群的不同节点. 当1个或多个主机或者磁盘故障，确保数据依旧正常访问；并能够根据业务的重要程度，按需选择不同的副本策略，满足用户灵活的可靠性需求。(需提供产品功能截图，并加盖厂商公章） 6.★服务：提供原厂工程师实施，提供3年原厂升级服务，3年原厂工程师上门服务，提供3年原厂专属技术服务经理7×24小时400/800及在线响应服务，3年内提供原厂工程师每半年一次巡检服务；提供厂商针对此项目的项目授权书及售后服务承诺函加盖原厂公章。	36	CPU	
2.5	容灾软件	本次配置容灾软件，需要与存储虚拟化软件同一品牌，实现良好的兼容性和异地业务容灾。 1.★容灾软件模块需采用无代理的方案，以简化部署和运维，并避免虚拟机安装代理软件后对稳定性和性能产生影响。 2.支持提供RPO可配置的虚拟机级容灾，RPO值范围从1秒到1周。 3.★为提高数据传输效率、减少对带宽的消耗，灾备软件需要支持压缩传输功能，对同步到备站点的数据先压缩再进行传输。 4.容灾软件具备仿真容灾演练能力，在不影响业务的前提下，验证容灾系统的可靠性。 5.当主站点恢复正常后，容灾软件支持一键回迁功能，并可根据业务需求回迁全量数据或增量数据。 6.支持种子文件功能，用户可以在主站点使用种子文件功能将需要容灾的云主机备份制作成种子文件存放到外置存储（U盘，移动硬盘）中，使用物理方式将存储介质运输到灾备数据中心，然后导入主站点云主机的种子文件，以此来提到容灾首次数据同步的速度，降低对带宽的要求。 7.★容灾要求：实现本次项目配置的2个超融合服务器集群与数据中心现有的20台服务器承载的业务实现相互容灾，可通过WEB控制台快速切换业务运行地点，故障后能快速拉起业务；业务恢复时间：核心	1	套	

		业务不高于5分钟，非核心业务不高于30分钟的快速恢复的异地容灾能力。（提供原厂商技术支持承诺函）			
2.6		虚拟机容灾授权	60	个	
2.7	一体化备份存储	1、用于虚拟化应用的存储备份，三节点分布式存储一体机（含备份软件），与虚拟存储软件同一品牌，单节点配置不低于：高度2U，32G内存，12个3.5寸盘位，4×10G+4x1G网口，双电源。集群配置不少于100T容量授权，9块固态硬盘-960G-SSD，24块机械硬盘4T SATA。 2.支持提供SAN、NAS+Object统一存储系统，一套系统同时支持iSCSI、NFS、CIFS、S3、Swift存储服务，实现统一管理。 3.★提供高性能块存储，可实现单节点（配置2块960GB SSD，两副本）提供至少10万IOPS。（要求厂家提供第三方测试报告，并提供集群的相应测试数据，加盖厂家公章） 4.★智能监控平台，能够清楚展示当前存储的关键硬件和逻辑资源，包含存储池、块存储、文件存储、对象存储、服务器硬件状态，并且能够在监控视图中根据当前状态给予客户提示，以达到快速清晰告警的目的。同时为了方便客户排错，支持点击各个资源和硬件等，能够展示当前选中单元的详细信息。（需提供产品功能截图，并加盖厂商公章）。 5.★支持一键检测功能，支持用户自行检测系统健康状态，检测包括CPU、内存、硬盘、网口等硬件故障、告警等问题，同时支持检测各类存储服务是否正常启动。针对问题能够提出解决推荐办法。（需提供产品功能截图，并加盖厂商公章）。	1	套	
2.8	虚拟应用负载均衡组件	1、软件版，实现业务高可用负载均衡，与计算虚拟化软件同一品牌，组件性能要求：授权带宽（吞吐率）3G，不限制新建和并发，最低要求4核CPU 8G内存。 2、支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、带宽比例、哈希、主备、首个可用、优先级等算法； 3、★支持非对称式部署的TCP协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果（提供第三方评测报告，证明所投产品厂商可提供此类技术）； 4、支持节点智能恢复，当节点出现故障时，负载均衡能自动重启服务器上的相关进程或重启服务器，使其恢复正常状态并继续提供服务；如无法使其恢复正常，则将其从节点池中移除，保证业务正常访问。（需提供产品功能截图，并加盖厂商公章）。 5、★支持面向服务器健康度的弹性调控机制，可通过监控业务流中的TCP传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载（需提供产品功能截图，并加盖厂商公章）。 6、支持实时漏洞被动检测功能，通过对实时流量进行安全性分析的方式来评估业务系统的漏洞风险，结合黑客攻击行为进行关联分析，并通过报表的方式展现安全风险和解决方法。	2	套	

3	网络安全等保配置（按照三甲医院等保三级要求配置）				
3.1	终端安全检测与响应软件（含杀毒）	安全检测与响应系统1套，主机授权（至少含50个Windows Server、20个Linux客户端 ）。 1.包含管理平台和终端Agent软件； 2.具备终端管理、终端病毒查杀、文件实时监控防护、东西向访问微隔离、暴力破解检测响应、WebShell检测响应、设备联动响应等功能组件，保障平台的扩展性和兼容性； 3.支持控制台显示当前平台终端总数、在线/离线数量、服务器终端/PC终端数量； 4.支持Vmware、Ctrix、Hyper-V、华为云、华三云、阿里云、腾讯云、KVM等国内主流云平台的虚拟机防护； 5.支持热点安全事件动态更新和展示及全网终端已发生的热点安全事件及其数量； 6.★支持安全策略一体化配置，通过一条策略即可实现不同安全功能的配置，包括：终端病毒查杀的文件扫描配置、WebShell检测的检测和威胁处置方式、暴力破解的威胁处置方式和Windows系统下信任区文件目录配置；（提供界面截图并加盖厂商公章） 7.基于多维度轻量级的无特征检测技术，多引擎协同工作； 8.支持展示勒索病毒事件、木马病毒事件、蠕虫病毒事件和其他病毒文件事件及其详情，包括：病毒文件名称，事件等级，受感染的文件，发现时间，检测引擎，文件Hash值，文件大小，文件创建时间。	1	套	
3.2	数据中心虚拟下一代防火墙NFV组件	1、软件版，与虚拟化软件同一品牌，8*vCPU+16G RAM资源使用授权，防火墙+IPS漏洞防护+服务器防护功能模块+僵尸网络检测；含全部功能使用授权及三年特征更新。 2、具备独立的Web应用防护规则库，Web应用防护规则总数在3000条以上；具备独立的僵尸主机识别特征库，恶意软件识别特征总数在50万条以上； 3、★支持对常见应用服务(FTP、SSH、SMTP、IMAP)和数据库软件(MySQL、Oracle、MSSQL）的口令暴力破解防护功能，全面保障业务的安全（需提供产品功能截图，并加盖厂商公章） 4、★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，全面保障业务的安全（需提供产品功能截图，并加盖厂商公章） 5、★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，发现问题后支持一键生成防护规则，能够及时的进行安全防护，全面保障业务的安全（需提供产品功能截图，并加盖厂商公章） 6、★支持B/S服务漏洞扫描功能，可扫描WEB网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞，全面保障业务的安全（需提供产品功能截图，并加盖厂商公章） 7、提供安全报表，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漏洞统计，可以查看到有效攻击行为次数和攻击趋势	2	套	

3.3	虚拟数据库审计NFV组件	1、软件版，组件性能要求：纯SQL流量≥600Mb/s，日志检索≥40000条/秒；含三年软件更新。 2、支持采用B/S管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；支持IPv6协议，可识别IPv6协议的数据流，支持基于IPv6地址格式的审计策略； 3、内置大量SQL安全规则，包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用grant、业务系统使用grant、客户端sp_addrolemember提权、web端sp_addrolemember提权、查询内置敏感表、篡改内置敏感表等；（需提供产品截图证明并加盖制造商公章）； 4、支持提供web审计日志的查询页面，支持通过日期、源IP、业务系统、以及指定url地址作为搜索关键字进行过滤查询，查询结果包括源区域、目的区域、操作对象、影响结果及其web三层关联信息 5、★支持基于SQL命令的webshell检测，提供webshell日志查询，可通过查看webshell攻击的时间、源IP、业务系统、webshell规则发现威胁（需提供产品截图证明并加盖制造商公章）； 6、支持统一的分析入口，可以设置和分析正常访问和异常访问视图、数据库泄密分析、图形化泄密轨迹分析、数据窃取、数据库风险、外发数据人员、受攻击业务系统、风险总次数这几个维度实时监控内网数据威胁态势并且提供交互式分析视图帮助企业快速溯源；	1	套	
3.4	虚拟SSL VPN NFV组件	1、软件版，组件性能要求：至少支持50个并发用户授权。 2、★支持PC终端使用包括32/64位的Windows （10、8.1、8、7、Vista、XP）、Mac OS、Linux等主流操作系统登录SSLVPN，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持终端使用包括IE（6、7、8、10、11）或其他IE内核的浏览器以及非IE内核浏览器如Firefox，Safari，Google Chrome，Opera来登录SSLVPN； 3、支持断线重连自动技术，防止用户误操作关闭浏览器导致VPN隧道断开，防止用户在无线网络环境下网络正常切换时VPN隧道断开；支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访； 4、产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象；支持SSL VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接； 5、支持业务系统账号和VPN账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统；（需提供截图证明并加盖厂商公章） 6、★支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式；	1	套	

		支持针对不同的 web 页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输；（提供如自主知识产权等证明材料）			
3.5	虚拟堡垒机 NFV 组件	1、软件版，组件性能要求：至少支持 100 个资源授权。 2、★支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（提供截图证明并加盖制造商公章）； 3、登陆方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD 域认证、Radius 认证等认证方式，同时支持各种认证方式和静态口令组合认证； 4、★支持内置三员角色的同时支持角色灵活自定义，可根据实际管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴（提供截图证明并加盖制造商公章）； 5、支持 IPV6 功能，设备自身可以配置 IPV6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登陆和审计； 6、支持对常见设备运维操作进行记录（至少包括 windows 主机、linux/unix 主机、网络设备等），审计信息至少包括以下内容：用户账户、起止时间、登陆 IP、设备 IP、设备名称、设备类型、访问账号、访问协议等信息；	1	套	
3.6	虚拟日志审计 NFV 组件	1、软件版，组件性能要求：至少支持 100 个主机审计证书授权。 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 LogBase 专用协议等协议事件日志，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； 3、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] 4、支持数据策略，可设定采集多种 WEB 访问数据，包括：脚本访问、样式访问、图片访问及地理数据访问；（需提供产品截图证明并加盖制造商公章）； 5、审计员只限于操作权限设置范围内的日志数据，无权限日志数据透明； 6、支持完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，从而减少对网络带宽和数据库存储空间的占用 7、★支持定义部门和人员的对应关系，支持定义人员与账号的对应关系。（需提供产品截图证明并加盖制造商公章）	1	套	
3.7	全流量威胁分析系统	1、软、硬件一体化，提供流量监测与分析。内存不低于 16G，存储不低于 2TB，吞吐性能不低于 600Mbps，接口配置 6 个千兆电口、2 个 SFP 光口、1 个串口（RJ45）、2 个 USB 2.0 接口。 2、★具备失陷(业务和终端)主机详细分析，包含攻击阶段分布、风险等级趋势、安全事件举证、开放端口等信息。攻击阶段包含存在漏洞、遭受攻击、C&C 通信、黑产牟利、内网扫描、内网扩散、盗取数据；	1	套	

		支持对每个安全事件详细举证分析，包含风险危害、处置建议、专杀工具等（需提供截图证明并加盖原厂商公章）； 3、支持感知业务/服务器资产，可定义 IP 地址、主机名、责任人、所属业务、操作系统、服务与端口等信息。（需提供截图证明并加盖原厂商公章）； 4、支持展示需要处理的风险主机与风险状况报告，报告内容包括业务与终端风险、业务风险与终端详情分析，提供危害解释和参考解决方案；适用于日常处理安全问题的运维人员。 5、★具备漏洞特征识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、白名单库，其中漏洞特征识别库 9000+以上规则，僵尸网络识别库 35 万以上规则，支持定期自动升级或离线手动升级（需提供截图证明并加盖原厂商公章）。 6、★支持与同品牌防火墙进行联动响应，支持系统下发安全策略到防火墙上，阻断攻击流量。（需提供功能截图证明并加盖原厂商公章） 7、提供安全分析大屏，能够展示资产分布，看清内网风险终端和风险资产概况，能够提示终端和服务器资产数据，能够展示风险终端和服务器数量。能够基于资产展示 web 明文、弱密码等脆弱性概况。能够展示风险终端和服务器 top5 安全事件。（需提供功能截图证明并加盖原厂商公章）			
3.8	边界下一代防火墙	具备传统墙、入侵防御 IPS、防病毒、DDOS 防护、WEB 应用防御 WAF、SSL VPN 等融合安全功能的万兆下一代防火墙或同等配置。 1、网络层吞吐量≥25G，应用层吞吐量≥9G，并发连接数≥220W，新建连接数≥20W，冗余电源，至少配备 6 个千兆电口，2 个万兆光口； 2、支持 IPV6 环境部署，包括接口/区域配置、路由配置等网络适应性功能，支持核心常用安全功能，包括僵尸网络，IPS 漏洞防御，WEB 应用防护等支持 IPV6 技术环境。 3、支持多链路出站负载，支持基于源/目的 IP、源/目的端口、协议、ISP、应用类型以及国家/地域来进行选路的策略。 4、支持模拟策略匹配的访问控制规则，即输入源目的 IP、端口、协议五元组信息，给出最可能的匹配结果，方便排查故障，或环境部署前的调试； 5、支持对网络总业务服务器的自动发现以及业务服务器脆弱性和服务器开放端口的自动识别，支持包含敏感数据业务的识别； 6、★支持采用安全智能检测技术对恶意勒索病毒及挖矿病毒等热点病毒进行检测（需提供产品截图证明并加盖制造商公章） 7、支持网络访问控制，配置特定网络区域只允许指定的 IP 地址或 IP 范围对外进行访问，防止内部伪造源 IP 对外 DoS 攻击的情况； 8、产品具备独立的入侵防护漏洞规则特征库，特征总数在 7400 条以上，具备独立的 WEB 应用防护识别库，特征总数在 3500 条以上； 9、★支持安全运营中心功能，可以对全网所有的服务器和主机的威胁进行全面评估，管理员通过一键便可完成对服务器和主机的资产更新识别、脆弱性评估、策略动作的合理化监测、当前服务器和用户的保护状态、当前的服务器和主机的风险状态及需要管理员待办的紧急事项等，可以自动化直观的展示最终的风险；（需提供产品截图证明并加	2	套	

		盖制造商公章）			
3.9	核心交换机	采用高可靠的模块化设计方式，要求所有接口板必须是分布式转发工作模式，插槽数≥10 个；交换容量≥28Tbps，包转发率≥4300Mpps；支持多虚一技术，将四台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项，统一的管理，跨物理设备的链路聚合；每台配置单主控引擎、冗余电源； 每台配置 2 块 48 端口千兆光接口板卡，含 36 块 SFP 多模模块，12 块 SFP 单模模块；2 块 48 端口千兆电接口板卡；1 块 8 端口万兆板卡，含 8 块万兆多模模块。	2	台	
4	业务迁移及容灾实施服务				
4.1	业务迁移及容灾实施服务	Oracle RAC 在超融合虚拟化环境安装一次。	1	次	