附件1

2018年城域网改造项目设备清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **品目** | **配置** | **数量** |
| 1 | 核心交换机 | H3C S7510E-X   1. 采用正交架构、CLOS交换，支持独立的交换网板，业务线卡槽位与交换网板槽位互相垂直， 2. 2. 插槽数≥13，业务插槽数≥10，独立交换网模块≥1，交换容量≥256Tbps，包转发率≥72000Mpps； 3. 主控引擎模块≥2，满足1+1冗余，主控槽位与业务卡槽位宽度相同的全宽槽位，提供更好的扩展性和可靠性； 4.支持POE+，满足新一代园区网以太网供电需求，提供官网配置手册截图和链接； 5. 支持RPR接口； 6. 可靠性：双引擎快速倒换，主备切换时候板内转发无丢包 ，支持冗余模块化电源，支持独立的交换网板，支持NSF/GR for OSFP/BGP/IS-IS，支持热补丁功能，可在线进行补丁升级，支持BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。BFD收敛时间<50ms，支持IP FRR，满足网络收敛<50ms； 7. MAC表≥1M，学习速率≥130K/S，路由表：路由表≥256K，IPv4 FIB表项≥3M，IPv6 FIB表项≥1M，ARP： ARP表≥170K，ARP表≥180K，学习速率≥1.1K/S； 8. 虚拟化：多虚一技术(N:1)，支持4框虚拟化技术 ,一虚多技术（1:N）， 支持多虚一技术和一虚多技术的配合使用 ,支持远程端口扩展，作为控制设备 实现对端口扩展模块的集中控制； 9. VxLAN功能：支持VxLAN二层交换，支持VxLAN 路由，支持VxLAN 网关； 10. 支持Macsec技术（IEEE 802.1ae）介质访问控制安全技术；    11. 支持FCF模式转发，VSAN的创建及配置，支持FC地址的分配及WWN地址和FC地址的绑定等功能，提供官网配置手册截图和链接；支持FLOGI/PLOGI和DCBX功能； 12. 配置要求：单台配置≥1个主控模块，满配独立交换网板，≥3个电源模块，万兆光口≥48个，千兆以太网电接口≥48个（设备配置板卡必须能实现SDN部署），提供40G光口≥2个，提供40G QSFP+ 5m电缆1根。   13．为确保网络稳定运行，设备需与网络管理同一品 牌 | 2套 |
| 2 | 万兆光模块 | SFP+ 万兆模块（1550nm,40km,LC）  H3C SFP-XG-LH40-SM1550-D | 48块 |
| SFP+ 万兆模块（1310nm,10km,LC）  H3C SFP-XG-LX-SM1310-D | 16块 |
| SFP+ 万兆模块（1550nm,80km,LC）  H3C SFP-XG-LH80-SM1550-D | 6块 |
| SFP+ 万兆模块（850nm,300m,LC）  H3C SFP-XG-SX-MM850-D | 10块 |
| 1 | 核心交换机 (一、二、五、六中学) | H3C S7503E-M  1.交换容量≥48Tbps，包转发率≥16500Mpps，扩展槽位数≥3，支持主控冗余； 2.支持POE+，满足新一代园区网以太网供电需求，提供官网配置手册截图和链接； 3. 支持EPON OLT接口，提供官网配置手册截图和链接； 4. MAC表≥1M，学习速率≥130K/S，IPv4 FIB表项≥3M，IPv6 FIB表项≥1M，ARP表≥180K，学习速率≥1.1K/S； 5.虚拟化：多虚一技术(N:1)，支持4框虚拟化技术 ,一虚多技术（1:N）， 支持多虚一技术和一虚多技术的配合使用 ,支持远程端口扩展，作为控制设备 实现对端口扩展模块的集中控制； 6. VxLAN功能：支持VxLAN二层交换，支持VxLAN 路由，支持VxLAN 网关，提供官网配置手册截图和链接； 7. 支持Macsec技术（IEEE 802.1ae）介质访问控制安全技术；    8. 支持FCF模式转发，VSAN的创建及配置，支持FC地址的分配及WWN地址和FC地址的绑定等功能，提供官网配置手册截图和链接；支持FLOGI/PLOGI和DCBX功能；  10. 支持安全业务插卡FW、IPS、NSM、ACG、LB、SSL VPN；  11. 支持原生的无线AC功能，无需独立的AC板卡或带AC功能的接口板，即支持无线AP管理功能。只要保持无线AP的IP可达，拔出任意接口板，均不影响无线AC管理无线AP功能；  12.配置要求：单台配置单主控，双电源模块，配置8个无线AP管理授权，千兆电口≥48个，万兆光口≥24个，提供2端口40G/1端口100G以太网光接口，（设备配置板卡必须能实现SDN部署），提供≥1个SFP+ 万兆模块(1310nm,10km,LC)，≥5个光模块-SFP-GE-单模模块-(1310nm,10km,LC)。 | 4套 |
| 2 | 核心交换机(28所（8所中学、4所九年制一贯制学校、12所小学、 幼儿园3所、特校）) | H3C S5560X-30F-EI  1.整机交换容量≥5.9Tbps，包转发能力≥222Mpps ；整机配置接口类型：24个SFP端口（其中有8个combo），4个万兆SFP+口，1个slot，最大支持12个万兆接口 2.设备内置图形化操作平台，实现对本校园内网络的统一运维及管理，提供官网截图和链接，  3. 支持软件定义网络SDN，符合OpenFlow 1.3协议标准，支持VxLAN功能：支持二层VxLAN，支持三层VxLAN，支持EVPN，提供官网配置手册截图和链接； 4. 支持可插拔双电源，支持可插拔双风扇，风扇模块化双风扇，前/后通风，风道可调；实配双电源双风扇； 5. 内置软无线控制器功能，交换平台实现有线无线一体化集成，配合县局无线控制实现分层模式，消除无线带宽瓶颈； 6. 支持防火墙插卡、及IPS、防病毒、应用识别、SSL VPN扩展，，提供官网配置手册截图和链接 ； 7. 支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权； 8. IPv4 特性：支持静态路由、RIP、OSPF、IS-IS、BGP4；IPv6 特性：支持静态路由、OSPFv3、BGP4+； 9. 支持基于云平台管理，支持设备蓝牙管理；  10、采用专业的内置防雷技术，支持业界领先的10KV业务端口防雷能力，使其在比较恶劣的工作环境中也能极大的降低雷击对设备的损坏率  11、提供双电源、模块双风扇冗余。 | 28套 |
| 3 | 核心交换机（3所远距离学校） | H3C S5560X-30F-EI  1.整机交换容量≥5.9Tbps，包转发能力≥222Mpps ；整机配置接口类型：24个SFP端口（其中有8个combo），12个万兆SFP+口，1个slot，最大支持12个万兆接口 2.设备内置图形化操作平台，实现对本校园内网络的统一运维及管理，提供官网截图和链接；    3. 支持软件定义网络SDN，符合OpenFlow 1.3协议标准，支持VxLAN功能：支持二层VxLAN，支持三层VxLAN，支持EVPN，提供官网配置手册截图和链接；方案必须实现SDN方案部署 4. 支持可插拔双电源，支持可插拔双风扇，风扇模块化双风扇，前/后通风，风道可调；实配双电源双风扇； 5. 内置软无线控制器功能，交换平台实现有线无线一体化集成，配合县局无线控制实现分层模式，消除无线带宽瓶颈； 6. 支持防火墙插卡、及IPS、防病毒、应用识别、SSL VPN扩展，，提供官网配置手册截图和链接 ； 7. 支持802.1ae Macsec安全加密，实现MAC层安全加密，包括用户数据加密、数据帧完整性检查及数据源真实性校验。无需软件授权； 8. IPv4 特性：支持静态路由、RIP、OSPF、IS-IS、BGP4；IPv6 特性：支持静态路由、OSPFv3、BGP4+； 9. 支持基于云平台管理，支持设备蓝牙管理；  10、采用专业的内置防雷技术，支持业界领先的10KV业务端口防雷能力，使其在比较恶劣的工作环境中也能极大的降低雷击对设备的损坏率  11、提供双电源、模块双风扇冗余 。 | 3套 |
| 4 | 接入交换机 | H3C S5130S-28P-EI  1、交换容量>=3.36Tbps，转发性能>=126Mpps  2、接口类型：24个GE端口，4个千兆SFP口  3、实现CPU保护功能，能限制非法报文对CPU的攻击，保护交换机在各种环境下稳定工作要求提供权威机构颁发的测试报告  4、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（万兆或千兆均支持），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，要求提供权威机构颁发的测试报告  5、支持基于端口的VLAN，支持基于协议的VLAN  6、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）  7、支持IGMP v1/v2/v3，MLD v1/v2，支持IGMP Snooping v1/v2/v3，MLD Snooping v1/v2，支11、持组播VLAN，支持MBGP，MBGP for Ipv6，支持IPv4静态路由、RIP V1/V2、OSPF，支持IPv4和IPv6环境下的策略路由要求提供权威机构颁发的测试报告  8、支持RRPP（快速环网保护协议），环网故障恢复时间不超过50ms，支持MSTP功能：收敛时间≤50ms支持PVST功能：收敛时间≤50ms要求提供权威机构颁发的测试报告  9、支持基于第二层、第三层和第四层的ACL，支持出方向ACL，以便于灵活实现数据包过滤，要求提供权威机构颁发的测试报告  10、 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换，需提供官网网站命令手册佐证支持多控制器  11、采用专业的内置防雷技术，使其在比较恶劣的工作环境中也能极大的降低雷击对设备的损坏，支持 ≥10KV业务端口防雷能力，  12、配置≥1个光模块-SFP-GE-单模模块(1310nm,10km,LC)。 | 175套 |
| 5 | 千兆光模块 | SFP-GE-LX-SM1310-D | 360块 |
| 1 | 防火墙+防病毒网关 | H3C SecPath F5030   1. 采用非X86多核架构，支持（双）交/直流电源。吞吐量≥30Gbps，最大并发连接数≥2000万，每秒新建连接数≥50万， 2. 提供配置千兆电口≥8，千兆光口≥4，万兆光口≥8（提供3个万兆模块(850nm,300m,LC)，1个SFP+ 万兆模块(1310nm,10km,LC)，4个光模块-SFP-GE-单模模块-(1310nm,10km,LC)；内置480G SSD存储硬盘； 3. 用户行为画像：提供基于用户名（或用户IP地址）实现对用户行为统一分析界面，采用饼状图对访问应用流量、网站访问集中分析展示，包含基于时间轴的访问行为轨迹(应用账号、行为内容等)，关联账号（微信、QQ）等相关用户行为审计内容； 4. 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。； 5. 诊断中心：支持报文示踪功能，可对原始报文进行回放。 支持丢包统计，提供详细分析丢包原因； 6. 国密算法：支持国密SM1/2/3/4算法； 7. 安全服务链：支持基于SDN网络的部署模式，支持对数据流进行服务链VXLAN封装转发。通过集中控制器对安全业务进行按需编排，实现安全能力的弹性扩展及多业务能力共享； 8. 所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。上述功能要求须提国家相关部委认可的第三方实验室测试报告证明， 2. 9. 所投设备支持高可靠性（包含主备/主主模式）部署； 10. 支持应用识别，URL过滤，行为审计，入侵防御，防病毒功能扩展； 11. 数据安全：持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配。   12. 特征库数量：攻击特征库数量≥7000+、病毒特征库数量≥37000+、支持的协议识别数量≥3000+。  13、NAT功能： 实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。  14．支持网络安全联动，实现信息安全深度防御，设备需与县局核心交换机同 一品 牌 | 2套 |
| 2 | 上网行为管理 | H3C SecPath ACG1000-EE  1. 网络吞吐量：≥32Gbps, 内存≥8G， 最大用户数≥20000； 2. 配置≥4千兆复用口，≥4万兆光口，扩展槽≥3，可扩展至≥16Combo接口或≥12SFP+接口（提供4个万兆模块(850nm,300m,LC)）； 3. 内置双电源；内置存储硬盘，内置存储硬盘，≥1T ； 4. 多核架构设计，CPU核数目≥8个，不允许采用X86架构，功能采用模块化结构设计；要求提供CPU型号、频率，最大功率≤300W；内置Bypass模块； 6. 支持静态路由、策略路由、RIP、OSPF、ISP路由，其中ISP路由支持自定义，并可提供基于应用的策略路由； 7. 支持3G扩展，支持电信、移动、联通等主流3G网卡。支持3G接口的常在线和按需上线模式，并支持在3G接口上运行IPSec VPN； 8. 支持基于带宽和优先级的多链路负载均衡，可支持链路过载保护； 9. 对目标地址提供基于ping、TCP、DNS等协议类型探测，可统计最近一周、一天、一小时的探测延时及成功率趋势，； 10. 支持即时通讯应用管控的精细化管理，可管控微信的“位置分享”、“朋友圈”、“附近的人”、“朋友圈”、“摇一摇”、“漂流瓶”、“收发文件”、“收发消息”、“视频语音”、“登陆注销”等行为，； 11. 支持微信认证和短信认证，微信认证通过DPI方式实现，；  12．提供网络安全联动实现信息安全深度防御，设备需与核心交换机同 一品 牌 | 2套 |
| 3 | 入侵防御检测 | H3C SecPath T5010  1. 开启防护策略后整机吞吐量≥ 20G，并发连接数≥2000万，新建连接数≥30万，支持虚拟IPS，数量不少于64； 2.配置≥12个千兆电口，≥12个千兆光口，≥4个万兆光口（提供4个万兆模块(850nm,300m,LC)）；扩展槽位≥1 ； 配置双电源； 4. 基于专业多核硬件平台，非X86硬件平台，需提供多核CPU名称和型号，作为验收依据； 5. 必须实配病毒查杀能力、流量控制能力、URL过滤能力、攻击防护能力； 6. 产品支持≥14路防护授权，本次项目要求实配至14路防护授权； 7. 攻击特征库数量≥3000+、病毒特征库数量≥8000+、支持的协议识别数量≥800+； 8. 支持专业防病毒功能，集成第三方专业防病毒厂商的专业病毒库； 9. 采用全面深入的分析检测技术，结合模式特征匹配、协议异常检测、流量异常检测、事件关联等多种技术，能识别运行在非标准端口上的协议，准确检测入侵行为； 10. IPS可以针对不同的IP或IP网段应用不同的网络滥用带宽控制策略，针对不同网段应用不同的网络滥用带宽控制策略； 11.产品与国家信息安全漏洞共享平台及中国国家信息安全漏洞库建立信息互动机制。  12．提供网络安全联动实现信息安全深度防御，设备需与核心交换机同 一品 牌 | 2套 |
| 4 | WEB防火墙 | H3C SecPath W2010-G  1.性能要求： HTTP吞吐量不低于1Gbps，HTTP并发连接数不低于60万、HTTP每秒新建连接数不低于4万，保护网站站点数量无限制  2. 2U高机架式硬件架构，标配单电源（可支持双电源冗余），8G内存，1T硬盘，2个以太网千兆管理接口，支持至少6个以太网千兆电口及8个以太网千兆光口，支持至少2个接口扩展槽位，可支持至少22个以太网千兆接口及4个万兆接口的扩展能力  3. 支持透明、旁路监听、旁路阻断、反向代理、混合（反向代理及透明同时部署）多种工作模式  4. 支持对网站的URL、Cookie、文件类型进行自学习功能，学习结果可以直接引用到安全策略中  5. 支持白名单方式的服务器挂马监控过滤功能，具备独立的威胁地图展示大屏页面，包括攻击地图、设备性能监控、安全事件分类及趋势折线图  6. 具备WebShell侦测功能，不但能阻止入侵者访问调用WebShell文件，还阻止利用WebShelll发起的各种攻击或入侵行为  7. 支持按照服务器IP或域名的流量统计功能，包括访问数、攻击数、爬虫数量  8. 支持合规的逐级访问功能，支持一键快速加黑加白功能  9. 支持数据库错误信息屏蔽功能，支持周期自动保存配置功能，支持特征库回滚功能  10. 拥有单独防病毒扫描引擎，支持HTTP及FTP协议的上传行为恶意代码检测过滤功能  11．提供网络安全联动实现信息安全深度防御，设备需与核心交换机同 一品 牌 | 1套 |
| 5 | 堡垒机 | H3C SecPath A2020-G  1. 支持最大300个可管理设备，运维用户无限制，支持4个千兆以太网电口作为业务接口， 2个以太网电口作为管理接口（1个管理接口、1个HA接口），2个USB接口  2. 系统须安装在专用的CF卡中，审计数据存储在磁盘中，防止操作系统故障导致审计数据丢失。  3. 设备采用旁路部署，不得影响业务环境；须支持HA主备模式，管理口和心跳口须支持多链路端口绑定功能，防止单网卡或单线故障。  4. 支持手机APP动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定APP动态口令, 堡垒机须内嵌动态令牌和usbkey认证引擎，且支持2种认证方式同时使用  5. 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  6. 支持oracle、mysql、sqlserver数据库协议代理运维，可直接调用本地windows系统的数据库客户端工具，支持自动登录、无需应用发布前置机  7. 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，甚至可自动完成授权  8. 支持使用本地的winscp/flashFXP/SecureFX等客户端工具登录堡垒机访问SFTP/FTP设备  9. 支持批量登录字符设备功能：能自动生成SecurCRT/Xshell工具的批量登录文件，实现在工具中批量登录多台设备  10. 支持保存SSH的sz/rz命令（zmodem）传输的原始文件, 支持保存RDP磁盘映射传输的原始文件  11．提供网络安全联动实现信息安全深度防御，设备需与核心交换机同 一品 牌 | 1套 |
| 6 | 网络管理 | H3C DR2000   1. 支持纯Web认证和客户端Portal认证，客户端方式支持可溶解方式，无需安装；支持二次地址分配；Portal页面支持定制；支持IPV6纯Portal认证以及NAT环境下的Portal认证；基于不同的端口组、WLAN SSID、终端操作系统推出不同的认证页面；支持Web Portal页面可视化定制；支持无感知认证，可在多台认证设备间漫游；支持微信认证；支持短信认证，与短信平台、短信猫对接，具备面开发即可支持的短信网关平台； 2. 提供向导式配置界面，点击开始后即可逐步进行业务配置，帮助用户快速完成业务部署。 3. 支持通过图形界面方式规划网络拓扑，并展示设备自动上线过程。 4. 支持基于用户以及用户组进行网络资源编排，实现用户以及用户组和网络属性VLAN、VXLAN、IP网段、IP地址的绑定。简化底层网络规划； 5. 业务联动控制：根据预定义的联动策略对匹配的事件（Trap）执行联动控制；支持各类安全威胁的分析和联动（支持防火墙、IPS、交换机、终端软件等上报信息的分析）；并支持在拓扑中显示攻击路径、攻击源等节点信息，； 6. IP地址自动扫描：实现网络IP地址自动扫描、统计、分配和管理，同时允许用户手工分配和管理IP地址，以达到更加灵活的分配管理。结合IP地址段的管理功能，将整个网络的IP，划入各个不同的IP地址段，分别进行管理，并给出详细直观的IP分配情况统计图表，使管理员能清楚的了解和掌握整个网络的IP使用情况， 7. 提供集中化的界面配置组间策略矩阵，支持拖拽方式实现策略部署，并自动统一下发到所有的策略执行点。用户移动时无需修改配置，策略保持不变，实现策略随行； 8. 基于接入场景的权限控制: 可基于用户角色、接入位置、接入终端类型等情境，向联动设备下发事先配置的接入控制策略，按用户不同的情境场景控制用户的网络使用行为；支持一用户多策略授权，从同一地点可获取不同的接入权限，实现内外网隔离场景； 9. 通过统一的用户编排实现用户及用户组接入时自动识别用户所属组，并将接入终端自动划入到相应的VRF隔离域。 2. 10. 通过统一的用户编排界面实现物联网终端接入时自动识别终端，并将接入终端按照业务应用自动划入到相应的VRF隔离域。 3. 11. 配置≥500网络设备管理，≥5000个并发终端认证授权。   12．提供网络安全联动实现信息安全深度防御，设备需与核心交换机同 一品 牌 | 1套 |
| 1 | 机柜 | 1.规格：600\*600\*2000mm，内高42U； 2.外观：外观高雅，工艺精湛，具有细沙质感，同时具备金属光泽； 3.材质：机柜使用优质钢板，整体框架采用可拆卸六折钢架结构，整体门包框外观，冷加工工艺。机柜主体角规2.0mm加工，其它1.5mm以上； 4.通风：机柜采用钢化玻璃前门，快速拆卸式钢制后门，柜门均制有发泡缓冲胶条，提供较好防护； 5.载重：机柜加载重量不低于820KG，机柜结构无松动变形； 6.抗震：机柜需通过对地固定安装后抗震等级达到UBC-Zone4(等同国标8级地震)； 7.走线槽：自带二条钢质垂直走线槽，方便网络设备及服务品的强电线与弱电线分开上下走线，保证机柜内线缆的整齐美观； 8.结构：19in和ETSI标准，EIA标准立柱，灵活调整，主体角规采用加大型，宽度为484mm，可根据安装要求前后调节≧170毫米； 9.表面处理：应符合防静电及BS6497国际标准，达到国家无毒无害的喷涂标准； 10.产品静电喷塑表面附着力：符合GB/T9286-1998规定的二级或二级以上标准，产品静电喷塑表面硬度：符合GB/T6739-1996规定的2H或2H以上标准；产品静电喷塑表面耐冲击性：按照GB/T1732-1993进行测试，机柜涂层的耐冲击指标应≥50Kg.cm ；产品静电喷塑表面涂层厚度：按照GB/T4957-2003进行测试，机柜涂层厚度应在50μm~100μm之间。 | 36套 |
| 2 | 精密空调 | 1.国际知名一线品牌、原厂制造的全新合格产品；  2. 电气性能:输入电压允许波动范围：220/380V +10%-15%;频率：50HZ2HZ  3. 适应环境: 室内温度:-10℃+30℃;室外温度：-15℃+40℃; 湿度:≤95%RH  4. 应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  5. 采用智能控制器，具有分组联动功能，支持备份、轮询、避免竞争运行  6. 采用智能控制器，具有分组联动功能，支持备份、轮询、避免竞争运行  7. 按照机房设计方案中设计的路由，计算管线长度和高差，对于超过室内、外机  组的安装正、负高差或水平距离要求的采取补偿措施 | 1 |
| 3 | 辅助材料 | 跳线，扎带、标签，排插、全部按超六类网线布线 。 | 36套 |
| 1 | 应用服务器 | H3C UIS-Cell 3010  1、国内外知名厂商，机架式，≥2U，标配原厂导轨。  2、每服务器配置2颗处理器，要求：采用Intel 至强可扩展系列处理器：6150(2.7GHz/18核/24.75MB/165W) CPU模块。  3、每服务器配置256 GB内存。要求：可扩展≥24个内存插槽，官方支持最大内存容量不小于1.5TB。  4、提供≥8个标准PCIE3.0插槽，可配置≥3块双宽企业级GPU，配置2端口万兆网卡（包含模块），2端口16GB  5、每台刀片服务器配置2块600GB 6G SAS 转速10K rpm SFF (2.5-inch) 硬盘；配置≥8个2.5寸热插拔硬盘槽位，可扩展至≥37个2.5寸热插拔硬盘槽位，同时可扩展3个3.5寸硬盘。  6、配置单独的远程管理控制端口，可实现与操作系统无关的远程对服务器的完全控制，包括:虚拟电源可远程开机、重启、关机；更新Firmware;支持远程故障现象重现；虚拟控制台可远程监控图形界面，可远程从本地软盘和光盘或其影像启动安装、操作Windows,Linux等软件（虚拟软驱、虚拟光驱、虚拟目录和虚拟U盘）；远程虚拟KVM，虚拟光驱和虚拟电源整合进单一界面；内嵌电源优化管理；和管理软件集成；传输用SSL加密，出厂采用私有密码。  7．支持RAID0/1/10/5/6/50/60/1E/Simple Volume；  ≥2GB缓存，支持缓存数据保护，且后备保护时间不受限制  8．2个≥500w铂金版热插拔冗余电源，支持96%能效比的钛金版电源选件 | 3台 |
| 2 | 存储 | H3C CF8840  1、投标品牌必须是国产品牌，设备原厂商在中国有生产厂  2、体系结构：一体化统一存储架构，同时支持并提供NAS、IP SAN和FC SAN模式；全冗余模块化体系结构；控制器上采用专用ASIC芯片负责数据I/O处理，该芯片具备RAID运算、在线去零和在线去重的功能，  3、多控架构：存储阵列采用全网状存储架构，最大可以扩展到4个（含）以上完全物理独立的控制器引擎，控制器引擎之间采用高速总线连接：PCIe；控制指令和数据的传输通道物理分离，主控芯片也同样物理分离，  4、底层虚拟化：存储内部底层虚拟化技术：发挥每一块盘的性能，保证了存储系统的高IO性能，不会出现热点硬盘，无需配置专用热备盘，使用全局热备空间技术，在硬盘故障的情况下能够多对多高速重建，同一块硬盘上可以同时存在RAID1/5/6等不同的RAID类型，  5、配置20块1.8TB 10K SAS磁盘， 全局宽条带化必须能够遍历至少60块磁盘，配置跨盘柜RAID保护，并且在安装时自动实现，必须同时支持SSD、15K SAS、10K SAS和7.2K NL-SAS硬盘，最大支持576块硬盘，单盘上至少支持RAID 1/5/6三种类型并存  6、配置高速缓存（非Flash）≥64GiB，支持扩展≥128GiB，数据缓存和控制缓存分离，仅写缓存采用镜像保护，缓存刷新频率不固定在线动态自适应调节，  7、配置Flash Cache功能许可，支持将SSD空间作为二级缓存使用，同一块SSD盘空间可以被数据卷和Flash高速缓存共享  8、配置FC主机接口≥4\*16Gbps，配置2个1GbE 以太口，可用于远程容灾复制或者NAS功能  9、配置精简功能，精简回收颗粒度≤16KB，配置在线重删和压缩，每个LUN可以单独开启重删或压缩功能，配置(或者支持)快照功能，快照无需预留空间，同时支持CoW和RoW两种快照机制，配置性能监控和分析软件，配置高级图形化报表软件，可以定制历史运行数据的图形化报表，配置子卷级自动分层功能，层次数量≥3  10、支持与同厂商中、高端型号阵列间实现存储底层的同步复制或异步复制，不同型号的同系列设备之间可以组成存储联邦，要求在同城实现阵列HA集群功能的情况下，同时可以支持3DC容灾  11、 高可用性：设备拥有高达99.9999%的可用性，提供从主机HBA 端口到存储阵列硬盘的T10-PI一致性数据检测保护，保障数据的完整性  12．为确保设备稳定运行，需与网络管理同一品牌 | 1台 |
| 3 | 光纤交换机 | H3C CN3300B  1.≥24个光纤自感应端口，≥24口激活，配置≥8个16G多模光纤模块；2. 全双工1Gbit/sec、2Gbit/sec、4Gbit/sec和8bit/sec自适应。 | 2台 |
| 4 | 管理矩阵 | H3C UIS Manager-UIS Manager  1、提供≥48\*GE电口+4\*10GE光口，云矩阵融合了对云计算基础设施的管理，包括服务器、交换机、存储以及机柜等；对云计算产品的管理，比如虚拟机、零存储、虚拟交换机等，同时还包括了资质管理，应用管理等机房常见功能。  2、支持VLAN划分、支持Super VLAN、QoS  3、支持IPv4/v6静态路由、RIP、RIPng功能，支持多台设备虚拟化为单台逻辑设备，主机堆叠数不小于9台  实配管理100台服务器授权  4、支持对服务器的远程KVM、批量装OS，并且可以把服务器现有配置生成模板保存。实时显示服务器CPU、内存利用率、温度示意图，并可对服务器做重启、短按、关机、开机等操作。监控服务器的运行状态，对运行过程中出现的异常进行告警，并且支持历史的告警记录查询  5、可创建、删除、关闭、迁移、备份虚拟机，显示虚拟机CPU、内存。支持虚拟化集群的建立，支持虚拟化集群的主机的管理。支持虚拟机的克隆，支持影子虚拟机，支持虚拟机的批量部署。支持为虚拟机自动分配共享存储。支持vSwitch的管理。支持对主机和虚拟机的工作状态的监控，CPU，内存，IO等性能数据的监控，对于异常的情况进行告警，支持对历史的告警记录进行查询。  6、支持对交换机的管理。自动获取交换机的拓扑，支持网络拓扑的显示。支持交换机的集中配置，支持自动配置（通过拓扑下发配置），支持手动配置（通过命令行或者页面操作下发配置）。支持网络的监控，对交换机，端口，链路，等性能进行监控，对于出现的异常能够进行报警，并且支持历史的告警记录的查询，可以查询出现告警的历史的网络拓扑。  7、支持创建、删除存储卷，显示卷的空间使用率、实时IOPS、卷属性，支持将卷挂载在某个主机上。支持对软件定义存储，以及独立FC存储等存储的管理。支持创建，删除存储卷，支持创建，删除主机，主机集，支持将存储卷和主机的关联支持虚拟机创建自动创建存储卷，支持虚拟机自动关联存储卷。支持对存储的监控，查看存储的使用情况，以及IO。  8、可以自定义机柜视图，并输出机柜设备列表、总体功率、电源使用情况。可以支持对机柜的监控，监控机柜的状态（包括机柜中设备的状态），功率使用情况，端口使用情况等。支持对机柜（包括机柜的设备）的历史数据的查询。  9、支持应用自动部署，根据应用规划生成虚拟机，vswitch，存储卷，配置网络设备（包括LB）。支持应用的手动部署，将应用和对应的设备进行关联。支持对应用的监控，支持应用的实时状态的监控，包括虚拟机的工作情况，网络设备的工作情况，存储的工作情况等。支持对应用的历史状态的查询，支持对任意时刻的历史记录的查询，包括应用的虚拟机，存储，网络等。  10．为确保设备稳定运行，需与云统 一架构同一品 牌 | 1台 |
| 5 | 虚拟化 | H3C CAS  1.平台技术架构：采用裸金属架构，无需绑定操作系统即可搭建虚拟化平台； 2. 支持现有市场上主要国内外操作系统，包括Windows、CentOS、Fedora、RedHat、SUSE、Ubuntu、FreeBSD、MacOS、中标红旗、中标麒麟、中标普华、深度、一铭、凝思等  3. 支持分布式存储功能，以x86服务器本地硬盘为基础构建单位组成存储集群。集群对各节点的本地硬盘进行统一管理，将其组成虚拟存储池； 4. 支持批量修改虚拟机的配置参数，包括：I/O优先级、启动优先级、是否自动迁移、CPU调度优先级、CPU个数、内存大小、自动启动、启用VNC代理、tools自动升级等； 5. 以图形化的方式直观展示集群、主机、虚拟机、网络和存储之间的关系，包括以计算资源为中心的虚拟计算拓扑、以虚拟交换机为中心的虚拟网络拓扑和以存储LUN为中心的虚拟存储拓扑； 6. 提供虚拟机快照功能，支持设置手工和定时快照将虚拟机磁盘文件和内存状态信息保存到镜像文件中； 7. 虚拟机支持跨虚拟化管理平台在线迁移，迁移过程中对业务运行无影响； 8. 虚拟机支持跨虚拟化管理平台在线迁移，迁移过程中对业务运行无影响； 9. 持对资源扩展和收缩策略的灵活配置，能够根据虚拟机CPU、内存、连接数、存储容量、磁盘IO等参数动态的克隆虚拟机或删除虚拟机以满足“业务量大时使用多个虚拟机提供服务、业务量少时使用少量虚拟机提供服务”的业务需求，整个过程不需要人工干预，同时支持对业务虚拟机组的统一负载监控和负载状态展示； 10. 支持当虚拟机的CPU、内存利用率超过设置的阈值时，系统将自动为该虚拟机增加相应的CPU和内存资源，无需人工干预； 11. 支持GPU资源池功能，根据设置的业务模板及资源抢占策略，实现对GPU资源的自动分配和回收； 12. 虚拟化平台内置健康巡检功能，从系统、集群、主机、存储、网络、告警分析等维度对系统运行情况进行巡检，针对巡检问题平台可自动给出优化建议，巡检报告支持以pdf方式导出； 13. 虚拟化软件内置备份模块，无需单独安装备份软件即可实现虚拟机全量、增量、差异备份功能，备份时对业务运行无影响，支持按时间（按天、按周、按月）设置自动化备份策略，备份策略可细化到分钟级； 14. 提供应用级别的HA功能，无需在虚拟机内部安装代理即可自动检测并可自动修复虚拟机内运行的应用故障，包括但不限于Apache Tomcat、JDK、Apache HTTP Server、MySQL、SQL Server、SharePoint等应用，并支持用户自定义脚本进行应用状态的监控； 15. 支持一键切换展示大屏功能，直观展示虚拟化资源池的健康度、告警、资源使用情况等，同时展示内容支持用户自定义，可定制的指标包括但不限于主机性能、虚拟机性能、共享存储性能、系统总体健康度、主机健康度、CPU分配比、内存分配比、存储分配比、系统告警、Top 5主机CPU和内存利用率、Top 5虚拟机CPU和内存利用率、主机和虚拟机状态统计等； 16. 支持虚拟机桌面预览功能，无需登录虚拟机即可在虚拟化管理平台上看到虚拟机当前桌面的状态； 17. 用户可登录自助服务平台提交电子流进行云主机、云硬盘等资源的申请，管理员可查看用户提交的资源申请电子流，对电子流进行审批（拒绝、同意）； 18. 平台提供备份服务，用户可通过自助服务平台申请备份策略对重要虚拟机进行数据备份； 19. 支持业务流程定制功能，可以根据自身业务审批机制定义业务流程，管理员审核完用户申请后，以邮件或短信等方式及时通知用户； 20. 支持工单流程，用户可通过工单向管理员提交IT需求，支持租户账号的预注册与密码找回； 21. 虚拟化软件（含管理平台）一套，含6颗CPU授权许可；软件要求实配DRS动态资源调度功能、DPM智能电源管理功能、分布式虚拟交换机功能、网络IO控制、用户自助服务门户、资源自助交付功能。 | 1套 |
| 6 | 虚拟化杀毒软件 | H3C 企业版&亚信安全DeepSecurity(AV+DPI模块)  1. 必须具有集中控管的功能，能够统一的管理和配置，并且日志能够统一的在集中控管平台上呈现，支持对虚拟化内核层Hypervisor和虚拟机的安全防护，由虚拟化安全防护系统管理中心统一下发安全策略。 2. 产品控制台上以虚拟机为单位，进行策略配置、部署和管理，为虚拟机提供防护，其中虚拟机皆无需安全任何客户端代理便能由主机继承安全策略、防护，物理主机整体资源与搭载虚拟机数量无直接关系，虚拟资源消耗不会随虚拟机数量成长。； 3. 支持虚拟补丁功能，在服务器尚无安装补丁前，提供针对此补丁攻击的防护能力； 4. 支持防火墙功能，并且可集中控管防火墙策略，策略定制可以针对IP、MAC地址或通讯端口，可保护所有基于IP通讯协议（TCP、 UDP、 ICMP 等）和所有框架类型（IP、ARP 等）； 5. 支持防御应用层攻击、SQL Injection 及Cross-site跨网站程序代码改写的攻击； 6. 支持提供包含攻击来源、攻击时间及试图利用什么方式进行攻击等必要信息，并在事件发生时，立即自动通知管理员。  7、本次配置相应6颗物理CPU的防护授权，需要实际配置客户需要的防火墙、数据包过滤、底层防病毒授权数。 | 1套 |