**浙江省口腔医院华家池主院区网络二期设备清单及参数**

**简述:**本项目采购设备含部署和实施工作，主要包括设备上架、安装、调试、培训等。该工作为交钥匙工程，需要中标方满足招标参数基础上按需提供相关设备的辅助配件和材料。主要包括模块、尾纤跳线、网线、光纤及熔接、水晶头等。

**备注：**标注▲项为核心指标项，负偏离则为无效标。

# 设备清单列表

|  |  |  |
| --- | --- | --- |
| 序号 | 设备型号 | 数量 |
| 1 | 核心交换机:H3C S12508X-AF | 1套 |
| 2 | SDN内网汇聚交换机:H3C S10506 | 1套 |
| 3 | 服务器接入交换机: H3C S7506E-X | 2台 |
| 4 | TAP交换机:H3C S5560-30C-EI-G | 1台 |
| 5 | H3C SDN控制器 | 1套 |
| 6 | H3C 运维管理平台 | 1套 |

# 1.核心交换机（S12508X-AF 1套）

|  |  |
| --- | --- |
| **功能指标** | **技术要求** |
| 产品架构 | 采用正交CLOS架构，能够配置独立的交换网板，控制引擎和交换网板硬件相互独立。交换网板支持5+1冗余。 |
| ▲采用无中板技术，业务板与交换网板无中板交互，降低中板转接线路损耗，提供持续的带宽升级能力。提供官网链接及截图证明加盖原厂公章。 |
| 支持动态可变信元分片严格无阻塞交换，提高整体转发性能。 |
| 品牌要求 | 为便于管理和维护，要求国内主流交换机厂家，近2年曾入围中国企业市场交换机份额前三，提供IDC市场分析报告证明 |
| 兼容性 | ▲与原有设备实现虚拟双机,无缝兼容（需要经过实测，否则无法签订合同） |
| 空间要求 | ▲考虑医院现有机房空间的限制，高效率利用机房机柜空间资源，本次采购的核心交换机高度原则上不得高于13U。提供官网链接及截图证明加盖原厂公章。 |
| 交换容量  | ≥380Tbps，提供设备供应商官网链接及截图证明（若官网存在双指标，以较小为准）； |
| 包转发率 | ≥230000Mpps，提供设备供应商官网链接及截图证明（若官网存在双指标，以较小为准）； |
| ACL | 支持单板最大表项板卡HB系列板卡：Ingress:512K/每单板Egress:18K/每芯片（出入不共享）（最大值，实际与配置相关） |
| MAC | ▲支持单板最大MAC地址>=750K，提供第三方检测报告证明加盖原厂公章。  |
| ARP | 最大表项板卡单板1M。 |
| 路由转发表容量 | 单板卡支持不低于256K，最大单板容量4M。 |
| 槽位信息 | 主控板≥2，交换网槽位数≥6，业务槽位数≥8；提供官网截图证明；  |
| 槽位插卡特性 | 单槽位最多支持72口10G板卡，提供产品正视图照片。 |
| ▲单槽位支持48口100G单板线速，提供第三方检测报告。 |
| 可靠性 | 支持不间断转发技术NSR，双引擎快速倒换，实现50ms的引擎故障主备切换时间。 |
| 支持热补丁功能，可在线进行补丁升级。 |
| BFD及快速联动协议，提供工信部权威第三方测试报告。 |
| 横向虚拟化特性 | 支持四框虚拟化技术，多台核心交换机可以堆叠成一个堆叠组，大大提升堆叠组可靠性，提供工信部权威第三方测试报告加盖原厂公章。 |
| 纵向虚拟化特性 | 支持纵向虚拟化，支持纵向虚拟化+VXLAN |
| 支持多业务板卡 | 支持独立的硬件防火墙/IPS/ACG/LB；带宽100G； |
| 云主控板支持运行SDN控制器 | ▲X86云主控可以支持，本次实配X86云主控，用于安装本次采购的运维软件使用。提供支持云主控官网链接及截图；[提供X86架构主控板照片](#_X86云主控照片和参数)加盖原厂公章。 |
| 云主控板支持SSD硬盘 | X86云主控可以支持256G SSD硬盘。 |
| 电源冗余特性 | 支持扩展电源槽位≥8。 |
| VxLAN | 支持支持VxLAN二层网关，支持VxLAN三层网关，支持EVPN，支持基于IPv4/IPv6的VxLAN二三层互通。 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3，支持普通模式和Openflow 模式切换支持多控制器（EQUAL模式、主备模式）支持多表流水线支持Group table支持Meter |
| 网管功能一体化 | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级；  |
| FCoE | 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  |
| 通风散热 | 线卡与网板均采用前面板打孔/前后风道设计。 |
| 关键部件热插拔 | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔。风扇框冗余和单风扇框故障72小时内设备正常运行 |
| 路由特性 | 支持静态路由；支持RIPv1/v2，RIPng；支持OSPFv1/v2，OSPFv3；支持BGP4，BGP4+ for IPv6；支持IS-IS，IS-IS V6；支持等价路由，策略路由；支持VRRP/VRRPv3； |
| QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、SP+WRR三种队列调度算法  |
| 支持精细化的流量监管，粒度可达8K |
| 支持流量整形Shapping |
| 支持WRED拥塞避免 |
| 支持802.1p、TOS、DSCP、EXP优先级映射 |
| 管理维护 | 支持SNMP，支持RMON；支持通过命令行、Web、图形化配置软件等方式进行配置和管理； |
| 实配 | 实配云主控引擎≥2（安装本次采购的运维软件用）。交换网板≥4，万兆光口≥24,40G光口≥2，不少于2000W电源模块≥4,以太网交换机风扇模块≥2。网板假拉手条2块，7米40G AOC线缆一根。 |
| 服务要求 | ▲原厂5年质保，最终用户名为浙江大学医学院附属口腔医院 |

# 2.SDN内网汇聚交换机（S10506 1套）

|  |  |
| --- | --- |
| **功能指标** | **技术要求** |
| 产品架构 | 支持正交CLOS架构，业务板卡与交换网板采用完全正交设计（槽位互相垂直），跨线卡业务流量通过正交连接器直接上交换网板，背板走线降低为零，极大规避信号衰减，具备平滑演进能力。**提供官网证明和实物正反面图片，指明槽位物理位置关系。** |
| 空间要求 | ▲采用紧凑型机框设计以达到更高的机房空间利用率，节约空间成本。机箱高度≤8RU。提供产品官网链接及截图证明加盖原厂公章。 |
| SDN园区网络特性 | 要求本次投标内网汇聚交换机产品适配SDN园区网解决方案，所有板卡均支持VXLAN，可组建成园区SDN网络并通过验收。 |
| 交换容量  | ≥31Tbps（若官网存在双指标，以较小为准）； |
| 包转发率 | ≥5700Mpps，提供设备供应商官网链接及截图证明（若官网存在双指标，以较小为准）； |
| 槽位信息 | 主控引擎模块≥2，满足1+1冗余，业务槽位数≥6，主控槽位与交换网板槽位宽度相同的全宽槽位，提供更好的扩展性和可靠性，其中支持独立交换网模块≥2。 |
| ACL | 支持双向ACL，ACL≥4K；支持端口ACL。 |
| MAC | MAC表≥1M，学习速率≥130K/S，提供工信部权威第三方测试报告证明 |
| 路由表项 | IPv4 FIB表项≥3M，IPv6 FIB表项≥1M，提供工信部权威第三方测试报告证明。 |
| ARP | ARP表项≥256K，提供工信部权威第三方测试报告证明 |
| IPv6 | 支持RIPng、OSPFv3、BGP4+、IS-ISv6协议支持IPv6策略路由；支持DHCPv6功能、IPv6 portal功能、IPv6管理功能；支持基于IPv6的VRRP功能 |
| 虚拟化特性 | ▲支持多虚一技术(N:1)，支持一虚多技术（1:N），支持多虚一技术和一虚多技术的配合使用，支持四框虚拟化技术，提供工信部权威第三方测试报告加盖原厂公章。 |
| 网络安全一体化 | 支持安全业务插卡FW、IPS、NSM、ACG、LB |
| 智能网管功能 | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级 |
| AD Campus特性 | 支持AD Campus 网络，与SDN 控制器联动，实现网随人动、位址分离、简易运维等SDN特性，方案与设备一体化部署  |
| 接口要求 | 插槽支持插拔千兆电口，千兆光口，万兆光口、万兆电口、40G端口、100G端口板卡  |
| 单槽位万兆电端口密度≥24 ，提供官网链接及截图证明 |
| ▲支持RPR接口，提供工信部权威第三方测试报告，提供官网配置手册截图和链接加盖原厂公章。 |
| ▲支持POE+，满足新一代园区网以太网供电需求，提供工信部权威第三方测试报告，提供官网配置手册截图和链接加盖原厂公章。 |
| VxLAN | 支持VxLAN二层网关，支持VxLAN三层网关，支持EVPN，支持基于IPv4/IPv6的VxLAN二三层互通。 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3，支持普通模式和Openflow 模式切换支持多控制器（EQUAL模式、主备模式）支持多表流水线支持Group table支持Meter |
| 可视化 | 支持Telemetry流量可视化功能 |
| 有线无线一体化 | 支持交换机内置AC功能  |
| 网管功能一体化 | 内置智能管理功能，支持通过图形化界面设备配置及命令一键下发和版本智能升级；  |
| FCoE | 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  |
| 安全特性 | 支持IEEE 802.1ae介质访问控制安全技术 |
| 通风散热 | 采用前后风道设计（包括业务模块、管理模块和电源模块），提供风扇正视图。 |
| 部件热插拔 | 主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔 |
| 路由特性 | 支持静态路由；支持RIPv1/v2，RIPng；支持OSPFv1/v2，OSPFv3；支持BGP4，BGP4+ for IPv6；支持IS-IS，IS-IS V6；支持等价路由，策略路由；支持VRRP/VRRPv3； |
| 高可靠性 | 支持主控板冗余，倒换时间为0ms，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。 |
| QOS | 每端口支持8个优先级队列，3个丢弃优先级，支持SP、WRR、SP+WRR三种队列调度算法 |
| 支持精细化的流量监管，粒度可达8K |
| 支持流量整形Shapping |
| 支持WRED拥塞避免 |
| 支持802.1p、TOS、DSCP、EXP优先级映射 |
| 管理维护 | 支持SNMP，支持RMON；支持通过命令行、Web、图形化配置软件等方式进行配置和管理； |
| 实配 | 实配双主控，满配交换网板，双电源， 5米QSFP+电缆1根，32端口万兆以太网光接口及4端口40G光接口板1块，48端口万兆以太网光接口2块， 24端口千兆以太网电接口及4端口万兆以太网光接口板2块。 |
| 服务要求 | ▲原厂5年质保，最终用户名为浙江大学医学院附属口腔医院 |

# 3.服务器接入交换机（ S7506E-X 2台）

|  |  |
| --- | --- |
| 功能指标 | 技术要求 |
| 产品架构 | 采用正交CLOS架构，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(需提供产品正反面照片，指明槽位关系，并提供官网截图及链接) |
| 业务插槽数 | 业务插槽数≥6 |
| 交换容量 | ≥30Tbps |
| 整机包转发能力 | ≥5700Mpps |
| 主控引擎 | 主控引擎模块≥2，满足1+1冗余，主控槽位与交换网板槽位宽度相同的全宽槽位，提供更好的扩展性和可靠性 |
| 关键部件热插拔 | 主控引擎、电源、接口模块、风扇、交换网板等关键部件可热插拔 |
| 链路聚合 | 聚合组数≥128组，每组成员≥8个 |
| 支持跨设备链路聚合 |
| 支持对广播、组播、单播报文的均匀分担 |
| 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IP FRR，满足网络收敛<50ms |
| 虚拟化 | 多虚一技术(N:1)  |
| 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（Controlling Bridge,CB）实现对端口扩展模块（Port Extender,PE）的集中控制 |
| VxLAN | 支持VxLAN 网关，提供官网截图和链接 |
| 网络安全一体化 | 支持安全业务插卡FW、IPS、NSM、ACG、LB  |
| 单台配置要求 | 实配双主控、双电源、满配交换网板，48端口万兆以太网光接口板 1块 |
| 服务 | 原厂5年质保，最终用户名为浙江大学医学院附属口腔医院 |

# 4.TAP交换机（S5560-30C-EI-G ：1台）

|  |  |
| --- | --- |
| **功能指标** | **技术要求** |
| 产品类型 | 1U盒式TAP交换机 |
| 产品架构 | 基于ASIC架构  |
| 交换容量  | ≥250 Gbps（若官网存在双指标，以较小为准）； |
| 包转发率 | ≥150 Mpps，提供设备供应商官网链接及截图证明（若官网存在双指标，以较小为准）； |
| 接口特性 | 自适应以太网端口≥24，万兆光口≥4，支持1个扩展插槽。 |
| 管理口 | 支持Micro USB Console端口管理。 |
| 扩展插槽 | 支持4口万兆光接口卡。  |
| MAC表项 | ≥64K。 |
| 虚拟化 | 用户可以将这多台设备看成一台单一设备进行管理和使用，简化管理、简化业务、提高系统可靠性，提升端口密度。 |
| 可信计算 | 产品可通过可信模块的RSA公共和私有密钥对加密算法方式，实现交互协议加密认证、安全密码控制保证数据存储及转发可控，网络内容防篡改等功能，保证网络安全。 |
| TAP分流功能 | ▲可实现流量的负载均衡、N:M的流量镜像、报文头识别及报文信息修改，可对流量进行识别及处理，匹配ACL策略等。提高官网链接及截图证明。 |
| 可靠性保护 | 产品支持可插拔交流双电源模块、以及可插拔双风扇可靠性设计，可以根据实际环境的需要灵活配置交流或直流电源模块，此外整机还支持电源和风扇的故障检测及告警，可以根据温度的变化自动调节风扇的转速，这些设计使设备具备了更高的可靠性。 |
| 流量识别 | 支持端口入方向ACL，匹配字段包括二层头部、内外层VLAN、IP/IPv6五元组、优先字段、分片报文。支持GRE识别，支持VXLAN和NVGRE的识别，支持封装报文内层五元组信息识别。 |
| 分片报文 | 支持 |
| IPv6复制 | 支持 |
| 单纤收发 | 支持 |
| 报文头部修改 | 支持用VLAN Tag来标记入端口，支持内外层VLAN Tag修改，支持剥除VLAN标记。 |
| 负载分担 | 根据配置的HASH类型负载分担到多个出口，同源同宿 |
| TAP-GrouP数量 | ≥512 |
| 服务要求 | 原厂5年质保 |

# 5.SDN控制器

|  |  |
| --- | --- |
| **功能指标** | **技术要求** |
| 支持容器化部署 | 方案相关组件支持容器化部署，提供易部署、易扩展、轻量化、故障快速恢复能力。 |
| 支持VxLan | 网络层面支持VxLan，通过VxLan实现业务解耦及业务隔离 |
| 要求实现基于角色的IP分配 | ▲要求实现基于角色的IP地址分配，能够针对某一类用户或者终端进行分组并分配对应网段，从而方便通过一条ACL在任意设备上实现对用户组权限的控制。要求提供第三方测试报告。 |
| 用户名和IP地址绑定 | 要求每用户在认证之后，系统实现用户名和IP地址的绑定或者自动锁定；且要求全网支持用户在任意位置（包括有线和无线）都可以正确接入并且获取的IP地址不变，并且无广播风暴隐患。从而实现园区内用户行为的精准溯源。要求提供第三方测试报告。 |
| 自动化上线 | 基于角色自动化，至多3份配置模板实现全网设备配置自动上线，上线过程不需要U盘等任何介质。 |
| 设备网哑终端接入自动化上线 | ▲根据事先导入系统的设备网各类哑终端MAC地址列表，实现哑终端的自动化上线，自动完成对接入层设备、汇聚层设备的配置下发，实现专网隔离、即插即用效果。对于同型号哑终端，根据终端的OUI进行匹配，实现自动化批量上线。要求提供第三方测试报告。要求提供界面截图。 |
| 故障设备替换即插即用 | 支持将园区设备按核心、汇聚、接入进行分组，对于同种角色的设备更换，可通过新设备自动化上线纳管后，执行一键替换功能快速完成设备的更换，尽快恢复业务。同时可以支持不同型号的设备替换能力。要求提供第三方测试报告。要求提供界面截图。 |
| 宽带物联终端自动识别，快速上线 | 支持园区宽带物联终端的识别方法进行配置，基于预定义规则，宽带物联终端可以自动识别归类，自动进入隔离通道并快速上线，无需收集MAC地址实现终端的轻量化快速入网。要求提供第三方测试报告。 |
| 多园区统一管理 | 通过一套控制器统一管理多园区，各园区之间支持用户策略随行。 |
| 多园区设备自动化上线 | 支持一套控制器实现多园区设备同时自动化上线。 |
| 接入交换机支持第三方品牌 | 接入交换机支持第三方品牌，保护用户前期投资。 |
| 场景融合 | 支持数据中心、广域网、园区及分支融合管理与控制,实现跨场景的业务编排，实现用户多场景业务的联动 |
| 安全合规 | 通过融合应用系统，实现对园区各类终端的实时扫描、防篡改及非法终端强制下线等合规检查 |
| 服务链 | 支持东西向、南北向服务链，东西向服务节点任意部署。 |
| 网络通道隔离与位置无关 | 针对不同用户组进行网络通道隔离，可以采用MPLS或者VXLAN等，要求对于终端或用户的隔离可以做到与位置无关，即用户在任意位置认证后，不需要人工干预都可以进入到正确的隔离通道内，方便整网权限管理。要求提供第三方测试报告。 |
| ACL与用户位置无关 | ▲针对不同用户组进行网络权限ACL隔离，要求对于终端或用户的任意访问权限的设置都可以做到与位置无关，方便整网权限管理。要求提供第三方测试报告。 |
| 无客户端下防MAC地址仿冒 | 网络中可以在无客户端下实现防止PC终端通过MAC地址仿冒哑终端、智能终端接入的情况，保持网络终端接入的安全性。要求提供第三方测试报告。 |
| 无线资源与用户的统一管理 | ▲要求在一个软件系统中实现有线网络、无线网络一体化管理，不仅可以对有线资源和用户进行管理，还可以对无线资源及用户进行统一管理，不需要再额外部署一套系统对无线业务进行单独管理。要求提供第三方测试报告和功能截图。 |
| 设备支持SDN Overlay的能力 | 要求整体方案基于SDN Overlay技术构建，要求核心或汇聚设备支持VXLAN网关，提供官网配置手册截图或链接。 |
| 解决方案和设备的兼容性能力 | 园区SDN建设方案和提供的配套设备要有工信部下属第三方检测机构的权威认证，并提供测试报告。 |
| 支持Hub下用户权限精细控制 | Hub场景下，不同角色用户权限可以实现精细化控制 |
| 多种802.1X接入认证 | 支持PAP认证、CHAP认证、EAP-MD5认证、EAP-PAP认证、EAP-TLS认证、EAP-PEAP-MSCHAPV2认证、EAP-PEAP-MD5、EAP-GTC、EAP-TTLS认证，防客户端破解。 |
| RADIUS认证 | 无需终端用户输入用户名和密码；支持证书、多级证书认证和无线的WAPI认证方式。 |
| LDAP认证 | 支持从LDAP服务器上同步账户信息，支持的LDAP服务器包括：Microsoft Active Directory、Novell Directory Server、Netscape iPlanet、SUN ONE Directory、OpenLDAP等；支持LDAP服务器主备模式；支持实时与本地LDAP认证；支持自动、手工和按需同步账户信息；支持AD域控组用户，支持AD域控密码控制。 |
| 接入认证 | 支持微信认证、二维码的认证方式。 |
| 帐号管理 | 支持帐号的增改查，账号可批量开户、导入导出和注销；支持将用户的分组管理，不同的用户分组可以由不同的管理员管理；支持终端账号的密码强度检测；可查询账号的接入明细日志和认证失败日志；支持账户失效提醒，过期账号自动销户。要求提供界面截图。 |
| 帐号接入控制 | 支持用户同时在线数限制、最大闲置时长限制，支持黑名单限制接入、支持自动加入黑名单、限制接入客户端的类型和版本，支持限制用户修改终端MAC地址和使用代理等策略。 |
| 在线用户管理 | 可以在线查看用户状态及其所连接的网络设备信息，如此用户接入的登录名称、登录设备IP、设备端口、终端信息、在线session信息、接入开始时长、接入持续时长、安全状态等，对非法用户可以执行发送消息、在线检查、强制下线、关闭端口等操作。 |
| 设备网哑终端接入自动化上线 | 根据事先导入系统的设备网各类哑终端MAC地址列表，实现哑终端的自动化上线，自动完成对接入层设备、汇聚层设备的配置下发，实现专网隔离、即插即用效果。要求提供第三方测试报告。要求提供界面截图。 |
| 智能终端认证页面定制 | 定制页面包括认证（或者注册）页面和处理结果页面，根据显示屏幕分为PC、PAD和手机多种页面类型。预置多套模板方便管理员通过可视化手段绘制页面，也可导入第三方定制的页面。要求提供界面截图。 |
| 智能终端注册页面的属性定制 | 定制注册页面的属性，包括是否显示、是否作为必填项、配置缺省值（用户姓名、证件号码和密码支持随机生成，密码是6位数字，其它是32位大小写字母和数字组成的随机数）、调整显示顺序、修改属性的显示名称。 |
| 用户自助管理 | 可通过自助平台进行预注册申请，管理员审核后即可开通用户帐号，用户可以通过自助平台对自己的用户信息进行管理，如查询、修改、密码设置、密码重新获取等；用户自助页面支持自定义。要求提供界面截图。 |
| 支持不同的访客账号创建方式 | 支持公共领域访客短信认证模式、访客接待员手工开户模式、访客自助开户模式，其中短信认证可支持定制逆向收费方案，节省学校的短信费用开支。 |
| 访客无感知认证 | ▲提供访客一次接入，多次使用的无感知认证，访客只需要输入一次用户名/密码，后续接入无需再输入用户名/密码。要求提供第三方测试报告。 |
| 访客接入权限控制 | 支持访客账号与设备IP地址、接入端口、VLAN、用户IP地址、MAC地址、等信息绑定认证，增强访客认证的安全性，防止帐号盗用和非法接入；可以控制访客账号有效上网时长，有效防止个别访客对网络资源的过度占用；可以实现对访客ACL、VLAN的控制，限制访客对内部敏感服务器和外部非法网站的访问；可以限制访客的接入时段和接入区域，访客只能在允许的时间和地点上网；支持访客使用一次一密方式，访客密码可设置有效时长。 |
| 访客行为审计 | 提供强大的“黑名单”管理，可以将恶意猜测密码的访客加入黑名单，并可按MAC、IP地址跟踪非法行为的来源。支持管理员可以实时监控在线访客，强制非法访客下线。提供接入明细日志，便于审计访客的接入网络记录。通过与UBA用户行为审计系统联动，实现按照访客账号审计上网URL、FTP等访问日志。（需要和ADUBA联动） |
| 多元素绑定 | 支持用户名、密码与用户IP、MAC、VLAN、设备IP、设备端口、主机名等多种元素的绑定认证；支持第一次认证成功时的自学习绑定属性功能。要求提供第三方测试报告。 |
| 用户组管理 | 关联接入策略和接入场景，用户组中的用户在不同的场景下应用不同的接入策略。要求提供第三方测试报告。 |
| 接入策略管理 | 接入策略关联安全组，可以控制用户是否绑定IP。要求提供第三方测试报告。 |
| 多种终端识别技术 | 支持通过客户端、DHCP、HTTP、MAC地址等技术准确识别接入网络的终端厂商、终端类型和操作系统信息。要求提供界面截图。 |
| 基于场景的终端网络接入授权 | 支持根据终端接入区域、接入时间段、终端IP地址、终端MAC地址、终端厂商、终端操作系统和终端类型等对网络接入终端授予不同的访问权限。要求提供第三方测试报告。要求提供界面截图。 |
| 帐号防暴力破解 | 具备帐号自动锁定功能，一定时间内多次恶意尝试登录的用户，可以自动锁定并且加入黑名单，由管理员解锁后才能恢复使用。因暴力破解进入黑名单的情况，不会影响实际用户的正常使用。支持自动解除黑名单。 |
| 认证后其他系统对接 | ▲当接入用户认证通过后会自动弹出设置的提示信息，支持自动打开浏览器访问内部系统并自动完成登录，支持自动在上线之后开启本地应用程序。要求提供界面截图。 |
| **实配授权** | 实配SDN控制器软件1套，开放性先知网络中心软件1套，管理1个园区控制器集群授权。配置20个leaves节点，3台控制器服务器节点授权，50台物理交换机管理授权，不少于500个终端准入认证授权。不少于5年7\*24小时技术支持服务。实配1套vDHCP实现DHCP sever功能。 |

# 6.运维管理平台

|  |  |
| --- | --- |
| **功能指标** | **技术要求** |
| 基本需求 | 1）能够对网络、系统、主机、存储、应用、虚拟化等的统一监控管理（包括展现与操作）、统一告警管理、统一报表管理； |
| 2）为保障架构稳定型与数据互通性，软件产品及组件为自主研发统一产品，不得采用OEM第三方产品或组件； |
| 3）系统支持部署到windows、linux平台，支持使用MS SQL、Oracle数据库，采用B/S架构。必须支持系统安装，卸载，数据同步备份、数据恢复的可视化界面。 |
| 4） 系统支持8000以上节点的数据采集要求，支持同时在线50以上运维操作员并发访问。须提供同等规模项目的证明文件。  |
| 网络 | 1）支持多厂商设备管理，包含了设备的基本信息、接口信息、性能数据、面板信息、存储空间，离线自动删除和告警信息等。 |
| 2） 可接收分析各类SNMP trap告警，完成基本格式的解析，并入库，系统预定义解析各类trap类型不小于8000条。 |
| 3）支持对网络设备指标支持最小5秒采集周期的实时性能监控 |
| 网络拓补管理 | 1)自动发现拓扑：自动发现网络中的所有网络设备，并在拓扑中显示出来，支持拓扑图自定义修改，包括设备、链路等。 |
| 2）支持IP拓扑、自定义拓扑视图（支持网络区域的任意划分、命名、拖拽、折叠和展开）、全景拓扑等多种拓扑类型；拓扑支持多协议，包括Bridge、NDP、CDP、MSTP、STP、LLDP、DISMAN-PING等二层协议，支持聚合链路，支持第三方的设备；拓扑可融合链路状态、设备告警等多种信息。 |
| 服务器硬件管理 | 1） 平台需具备全面性，必须支持通过IPMI、SNMP和RESTful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以及服务器远程控制。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。必须提供截图 |
| 自定义应用 | 1） 平台需具备扩展性，必须支持自定义应用监控，不用修改原系统的任何代码，按照规则增加配置文件及脚本即可生成一种新的监控应用类型。指标的采集方式、展现形式及页面布局均可通过配置文件指定。支持手动输入shell脚本的方式进行自定义数据的采集并展现，必须提供截图 |
| 操作系统 | 1）操作系统管理：提供对常见操作系统的监控管理,必须包括Windows、AIX、IBM AS400 / iSeries、FreeBSD/OpenBSD、HP-UX/Tru64、Linux、Mac OS、Sun Solaris、中标麒麟、凝思磐石等，支持对疑似存在内存泄露的操作系统进行自动检测并发送告警信息 |
| 2） 支持通过智能算法模型对操作系统内疑似内存泄露的进程进行检测、分析并告警。同时支持从不同维度检测占用内存高的进程并发送告警，包括TopN CPU利用率进程、TopN 内存利用率进程等，并显示其变化趋势。支持对僵尸进程的数量统计以及每个僵尸进程详细信息的监控。必须提供截图 |
| 3） 支持对监控的操作系统和上层应用的流量进行采集和统计，包括总速率/流入速率/流出速率、最近一小时流量/入流量/出流量、最近一天流量/入流量/出流量等指标项；必须提供截图。 |
| 4) 支持通过HMC对小机进行管理，包括小机逻辑分区、虚拟处理器、镜像内存等信息的监控，必须提供截图。 |
| 业务服务管理 | 1)    具备可配置的业务服务管理仪表板，从健康度、繁忙度、可用性维度呈现业务系统当前状态，并且用图形化的方式按业务系统、设备类型（主机、网络、应用）、软硬件设备的层次展示健康度、繁忙度、可用度计算过程。 |
| 2)    提供基于时间轴同步的业务投资分析，按业务系统、服务主机、业务应用、网络设备的层次分析同一时间范围内繁忙度、健康度变化趋势，提供灵活的天、周、月、年、自定义时间范围切换方式。分析的指标至少包含：流量、CPU利用率、物理内存使用率、I/O延时。 |
| 3)    提供基于业务系统的容量分析报告, 提供业务系统总容量效率；展示CPU、内存、磁盘总容量和实际利用比例；可以按CPU、内存、磁盘分别统计平均利用率、利用率峰值、利用率波动；能够预测未来15天是否存在容量瓶颈。 |
| 4)  提供整个数据中心运行状态视图，包括数据中心、集群、主机、虚拟机，并能分别查看详细运行报告。数据中心报告应包括：集群、宿主机、应用系统和虚拟机数量、CPU利用率、内容利用率、磁盘利用率指标。 |
| 5) 能够通过业务状态分布图呈现所有业务系统健康度、繁忙度分布，方便运维人员快速定位存在异常的业务系统；在业务图标上可以显示该业务详细信息，并对该业务健康度、可用度、繁忙度进行趋势分析。 |
| 6) 具备业务组织树，按树形层次关系展示部门、子部门、业务系统的关系和状态，业务组织树可以放大缩小、可以按部门收缩或展开。 |
| 7) 可以用包含IT基础架构层、业务逻辑层、用户体验层三位一体业务卡片显示业务运行状态；当某个业务系统没有全部三层监控的时候，业务卡片可以自适应只显示IT基础架构层或IT基础架构层加用户体验层状态。 |
| 数据采集 | 1） 支持代理和免代理两种模式，可根据不同的场景选择不同的监控模式，必须支持两种模式同时使用。必须提供截图 |
| 2） 支持agent程序远程推送安装升级、安装环境自检等；必须提供截图 |
| 3）支持对采集指标按照重要程度分别设置采集周期或者设置不采集，既可全局配置生效，也可以针对某一实例单独配置以满足特殊的采集需求。 |
| 4） 支持对应用监控采集、服务器硬件监控采集分布式部署多个采集节点，可根据实际情况弹性扩展。必须具备动态冗余采集方式，当单个采集节点出现故障时，可通过执行脚本的方法将该采集节点上的管理对象分配到其他采集节点上，以保证数据的完整性。必须提供截图 |
| 提供图形化的IP地址分配界面 | 支持图形化IP地址分配；支持基于IP地址的网络视图，能够轻松查找子网；从子网中标记IP地址的使用情况，保留、已分配等。同时可标记IP地址类型如互联IP、网关IP、管理IP、用户IP。支持现场操作。 |
| IP地址规划 | 支持，可以自定义分区域分组进行IP地址规划 |
| 支持按需的子网划分 | 支持任意子网划分，非常灵活，在地址分配时判断子网网段的可用性，如创建的子网下有在用的IP，会有提示信息。 |
| 告警管理 | 支持IP地址冲突检测，冲突IP地址信息可查询，历史告警信息汇总、首页进行趋势展示 |
| MAC与IP对应关系联动 | 支持导入MAC与IP对应关系表，发现现网中所有与对应关系不一致的情况； |
| 部署方式 | 1）支持双机热备：主备服务器共享存储，公用一个虚拟IP，实时备份，保障系统切换时无数据丢失。 |
| 2）支持数据库及软件重要文件的备份及还原：支持手动或定时备份指定数据库数据及软件重要文件，并可通过FTP等方式将备份文件上传；支持在指定数据库上使用备份的数据库文件进行还原操作。必须提供界面方式的可视化管理。 |
| 3) 分级管理：整个运维管理系统分为上、下级两层，同一分级的多个物理区域，其管理区域之间是独立的，各下级运维管理系统也是相互独立的，上级运维平台与下级运维平台采用rest API进行通信。管理员可通过上级运维平台直接对下级运维平台进行访问，下级告警可上报到上级网管展示，必须提供分级管理界面视图。 |
| 云环境 | 1) 支持云环境下的运维监控管理，支持租户VPC内云业务的监控，支持不同VPC下IP地址重复的业务监控。提供双视角监控模式，管理员视角可对云环境的基础资源的统一管理；租户视角提供多租户监控模式，不同的租户VPC资源隔离，租户可管理自己VPC内业务应用资源，添加、修改、监控租户应用，查看本租户内的业务状态。  |
| 开放性 | 1） 开放接口：提供丰富REST API的接口，官网网站可查，可供第三方系统调用。 |
| 实配授权 | 实配225个网络管理授权，75个服务器应用管理授权，10个服务器硬件管理授权，200IP地址管理节点授权。带服务器部署服务20个节点，网络设备监控部署服务75节点。 |

# 商务条款要求

**实施验收**

1、投标人须完成现有设备清单的所有设备的供货与实施工作，同时考虑到原有设备的网络结构，进行统一规划和部署；提供完整的实施计划方案（包括网络拓扑现状图、实施文档，需求分析等等）及相应的应急预案。免费配合用户后续系统架构调整、应急演练，不限次数。

2、由中标人工程师按用户要求定期进行巡检，每季度一次对系统的运行状况分析，提供用户设备运行状态和性能的分析、评估服务，每半年向用户提交一份详细的系统可用行、安全性、运行状况分析报告。

3、采购文件中标有“▲”为关键技术指标是不容许发生偏离的，关键技术指标发生偏离或其他技术指标如有明显不符合采购文件参数标明的，采购单位有权取消其中标资格；中标三个工作日内，如采购人要求，需提供所有投标产品样品给采购人进行功能测试验证，测试中发现虚假应标的行为将予以无效标处理（因中标人未按规定时间及时提供测试产品，导致采购人损失的，取消其中标资格）；验收时发现产品不符合采购文件参数要求的不予验收通过；如有投标方虚假投标，采购方有权将此供应商上报给政府采购相关单位处理。

7、验收：采购人参照设备清单，进行产品品牌、型号、数量到货初验（所有货物一次性到安装场地），安装调试完成后根据招标文件里技术功能进行项目终验，发现产品达不到验收标准或合同规定的性能指标，供方必须立即调整或更换产品。并且赔偿由此给用户造成的损失。

**售后服务**

1、要求原厂商认证工程师和原厂工程师提供7\*24小时不间断技术支持服务；

2、提供远程服务与现场服务相结合的方式，根据不同的故障级别采用不同的响应方案：电话及远程服务接到通报故障的电话或传真后的20分钟之内响应；对电话或远程无法排除的故障，在2小时之内到达现场，进行故障排除工作。一般非重大的故障保证系统在4小时之内修复，重大故障保证系统在8小时之内修复。对于无法修复的故障，提供相应的代用设备供用户应急使用，以确保系统的正常运行；

**培训要求**

1、由原厂商工程师提供现场技术培训服务一次

2、培训服务具体要求如下：

•基于现有设备的基础技术培训讲解

•基于新架构网络（SDN）的技术培训讲解及实施。