**台州市政府采购招标文件**

**TZCG-2018-GK060号**

采购项目：台州市妇幼保健院新院区（一期）医院数据中心建设项目

采购单位：台州市妇幼保健院

采购类别：货物类

集中采购机构：台州市政府采购中心

2018年9月30日

**招标文件目录**

1. **投标邀请**
2. **招标需求**
3. **投标人须知**
4. **评标方式、评标标准**
5. **台州市政府采购合同主要条款指引**
6. **应提交的有关格式范例**

**第一部分投标邀请**

根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》和财政部第87号《政府采购货物和服务招标投标管理办法》等有关规定, 受采购人委托，现就台州市妇幼保健院新院区（一期）医院数据中心建设项目进行公开招标采购 ，欢迎具备本项目投标人的资质要求且能够及时提供相关货物及服务的供应商前来投标。

**一、项目编号：**TZCG-2018-GK060号

**二、采购内容：**

1、货物名称及数量：台州市妇幼保健院 新院区（一期）医院数据中心建设项目 一批

2、本次采购不允许进口产品。

**三、交货期及地点：**

**交货期：**合同生效后30天内完成供货，50天内完成安装调试。

**交货地点**：业主指定。

**四、合格投标人的资格条件：**

（一）符合《中华人民共和国政府采购法》第二十二条规定的投标人资格条件:

1、具有独立承担民事责任的能力；

　　2、具有良好的商业信誉和健全的财务会计制度；

　　3、具有履行合同所必需的设备和专业技术能力；

　　4、有依法缴纳税收和社会保障资金的良好记录；

　　5、参加政府采购活动前三年内，在经营活动中没有重大违法记录；

　　6、法律、行政法规规定的其他条件。

（二）本项目供应商特定条件：

1、不接受联合体投标；

**五、招标文件获取的方式、时间：**

1、获取方式：网上免费下载，下载地址为http://www.zjzfcg.gov.cn或<http://www.tzztb.com/tzcms/zfcg.jhtml>

2、获取（公告）时间：2018年9月30日至2018年10月12日。

注：投标人如认为招标文件存在歧视性条款的，应在获取招标文件之日起7个工作日内提出。

**六、招标答疑会**

本项目不需要现场招标答疑会

**七、投标截止及开标时间、地点：**

本次招标将于：2018年10月30日星期二 上午9:30时整在台州市市府大道777号台州市公共资源交易中心(电信大楼南面)三楼306室开标，请在此时间前将投标文件送达开标地点，逾期或不符合规定的投标文件恕不接受。

**八、投标保证金：**

1、投标保证金为**人民币200000元**。投标人应于网上报名的同时根据网上自动生成的帐号（帐号随机产生，每个项目、每个供应商的帐号都会不一样）进行缴纳，未按上述要求报名缴纳的作无效处理， 财务联系电话：0576-88685133。

**九、办理供应商网上注册登记：**

所有参与政府采购项目的供应商，均需在浙江政府采购网上进行供应商注册登记(网址：http://www.zjzfcg.gov.cn)，并通过审核及公示合格后加入“浙江省政府采购供应商库”，成为注册供应商。

**十、网上投标报名：**

 凡是参与政府采购项目的注册供应商，均需登录**台州市公共资源交易网政府采购页面（<http://www.tzztb.com/tzcms/zfcg.jhtml>）**进行网上报名；尚未注册的供应商应当先在浙江政府采购网上申请注册，**注册终审通过后**再进行网上报名。

**十一、投标人信用信息查询渠道及截止时点、信用信息查询记录和证据留存的具体方式、信用信息的使用规则：**

1、查询渠道：中华人民共和国最高法院（网址：http://zhixing.court.gov.cn/search）、中国政府采购网（网址：http://www.ccgp.gov.cn）、信用中国（网址：<http://www.creditchina.gov.cn>。

2、截止时间为开标后评标前。

3、信用信息查询记录和证据留存的具体方式：将在规定查询时间内打印信用信息查询记录及相关证据，并将与其他采购文件一并保存。

4、使用规则：对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，将被拒绝其参与政府采购活动。

**十二、资格审查方式：**资格后审。

**十三、联系方式：**

**（一）采购人**（受理招标文件质疑及回复事项）

采购人名称：台州市妇幼保健院

联系人：李老师 联系电话：0576-88228865

**（二）集中采购机构**

项目联系人：陶先生

联系电话：0576-88685172 传真：0576-88685061

窗口联系人：阮女士

联系电话：0576－88685121（受理供应商注册及中标结果相关质疑）

地址：台州市市府大道777号

台州市政府采购中心

2018年9月30日

**第二部分 招标需求**

**一、招标项目一览表**

本次招标共 1 个标段，具体内容如下表：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **标段号** | **顶目名称** | **规格型号** | **数量** | **单位** | **预算（万元）** | **交货期**  **合同签订后几天内** | **交货地点** |
| 1 | 新院区（一期）医院数据中心建设项目 | 详见技术参数 | 1 | 批 | 1300 | 合同生效后30天内完成供货，50天内完成安装调试。 | 台州市妇幼保健院指定地点 |

1. **技术需求**

1 建设背景

1.1 项目整体概述

### 1.1.1 台州市妇女儿童医院整体需求概述

台州市妇女儿童医院（温州医科大学附属第二医院台州院区）的数字化医院建设，以满足区域医疗中心的建设目标、达到国内领先的智慧医院建设标准，因而核心网络及数据中心的规划与建设将要确保在未来**五年至十年**依然处于一个主流技术的管理运维水平，为建设区域运营管理中心、临床数据中心、影像智能中心、科研数据中心、患者随访数据中心，实现医院整体全面的移动化、无纸化、物联网化、互联网化、智能化，从而奠定一个坚实的成熟的基础架构平台。

### 1.1.2 网络及数据中心建设功能需求分析

* 满足多网融合的业务需要

为便于管理、减少浪费、提升安全等级，要求员工**内网、员工外网、医院设备网、数字电视网、病员外网wifi**实现**五网合一**、**逻辑隔离**。所有核心服务器、网络均需实现冗余备份建设，保证单个设备故障后，1分钟内恢复业务故障。

* 多业务的安全需求

避免非授权的人员使用终端（如收费系统、医生工作站）接入网络，防止信息泄露，如医院的关键资产**（统方数据）**及**病人隐私数据**。确保网络能避免来自网络的各种攻击，如黑客、病毒等。整体满足**等保三级**的安全防护技术要求，包括**网络结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码方法、网络设备防护、主机安全、数据库安全**等内容。

* 可管理、易维护的运维需求

医院的IT人员编制较少，常常是几个人就需要维持几千人的医院信息网络7×24小时正常运行，因此网络的**可管理、易维护**非常重要；不仅是减轻运维人员压力，更重要的是保障网络及各应用系统的稳定可靠、安全的运行。

同时，能实现所有网络设备节点的自动化上线，用户接入灵活管理，用户组/策略管理，业务配置管理，网络运维等一体化管理，并能摒弃传统的命令行维护方式，能通过直观的图形化界面完成。

1.2 台州市妇女儿童医院的建设内容

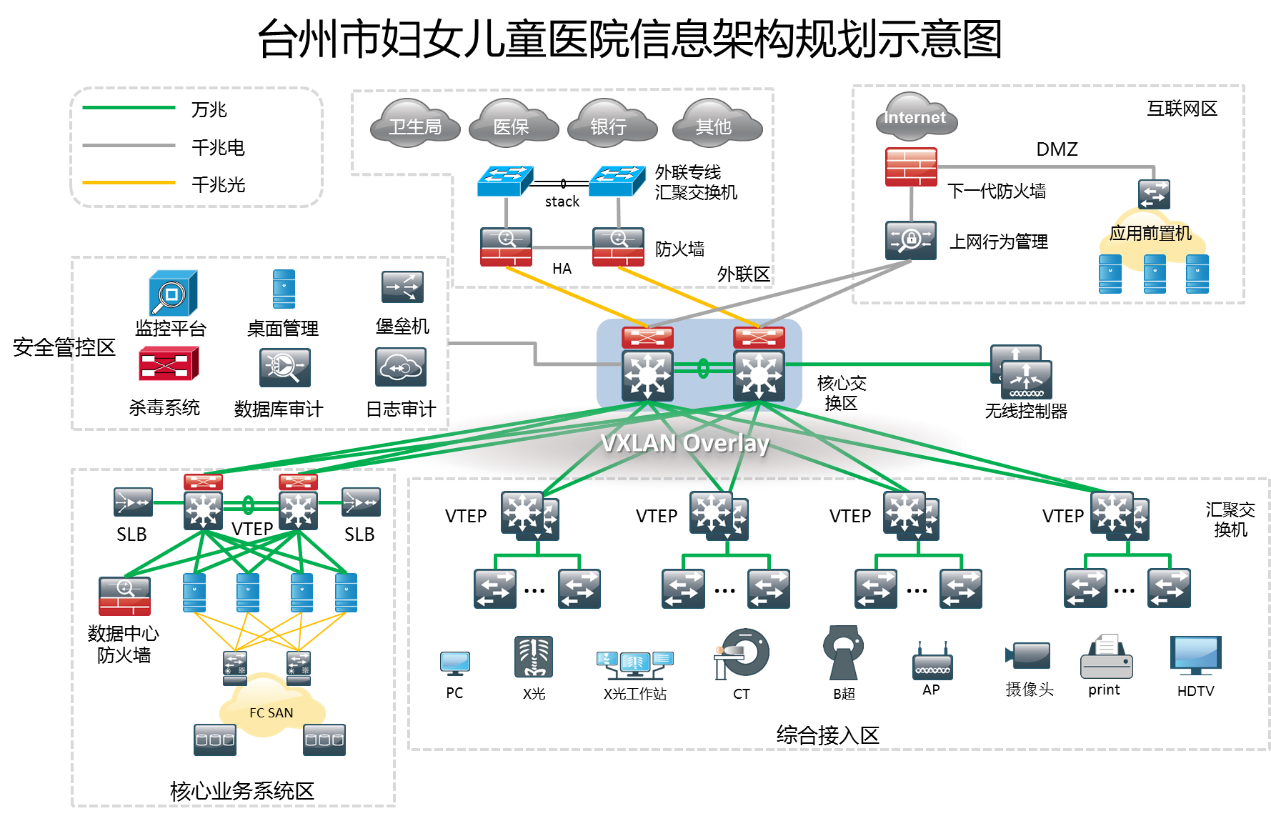
台州市妇女儿童医院（温州医科大学附属第二医院台州院区）数据中心建设包括网络及信息安全系统、数据中心服务器与存储等数字化信息系统建设，建设一个技术先进、经济实用、安全可靠的数据中心硬件支撑平台，满足医院业务信息系统的应用要求。

本次招标内容主要为：硬件及基础软件的采购、安装调试、系统集成、运行维护以及技术培训和售后现场技术服务等。投标人需按本招标文件的要求完成系统的设计、产品购买、运输、装卸、现场安装、调试及试运行，并完成系统集成、培训及售后服务等工作。本项目为交钥匙工程，项目涉及的软件系统安装实施、硬件设备系统集成以及其他相关项目实施工作均需在移交前完成。系统安全性须符合有关部门要求。

2 有线网络架构设计

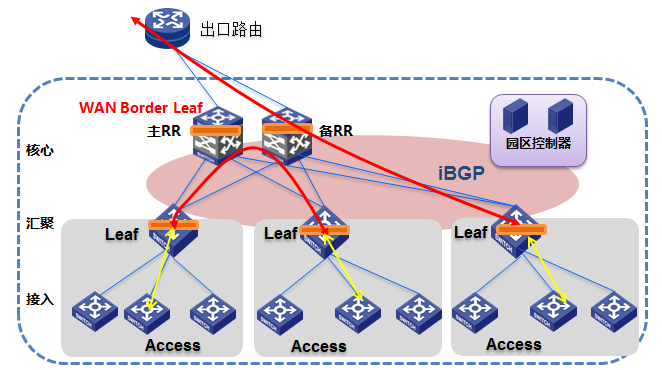
2.1 架构总体设计

整合吸纳当前较为成熟先进技术，建设稳定、高效、安全的综合性基础支撑平台。其物理架构如下：



首先，整个架构底层使用较目前成熟的网络架构和技术，包括设备横向虚拟化技术、高密万兆骨干设备等，实现一张高可用的医疗级网络。整个网络划分为物理上的三层架构（即核心层、汇聚层和接入层），内外网通过一套物理设备进行逻辑上的隔离，汇聚层和核心层分别通过横向虚拟化技术，使两台设备虚拟化为一台，提高汇聚层、核心层的可靠性以及安全性。

其次，在物理架构的基础上构建overlay网络，构建一个无状态的SDN网络架构，采用分布式L3网关并通过可靠的机制有效地抑制广播风暴，接入层设备采用动态VLAN接入，通过TRUNK的方式上行到汇聚层，汇聚层完成VLAN到VXLAN的映射。



采用SDN架构的最大优势主要体现在策略管理上，首先采用了面向用户的分组模式，将属性或者访问权限相近的用户分到一个用户组中，同时也将服务器侧的资源划分到相应的用户组进行统一管理。其次是，策略定义时，基于矩阵表格的方式简单直观。具体策略的定义可简单可复杂，以实现各种高级复杂的策略控制功能。

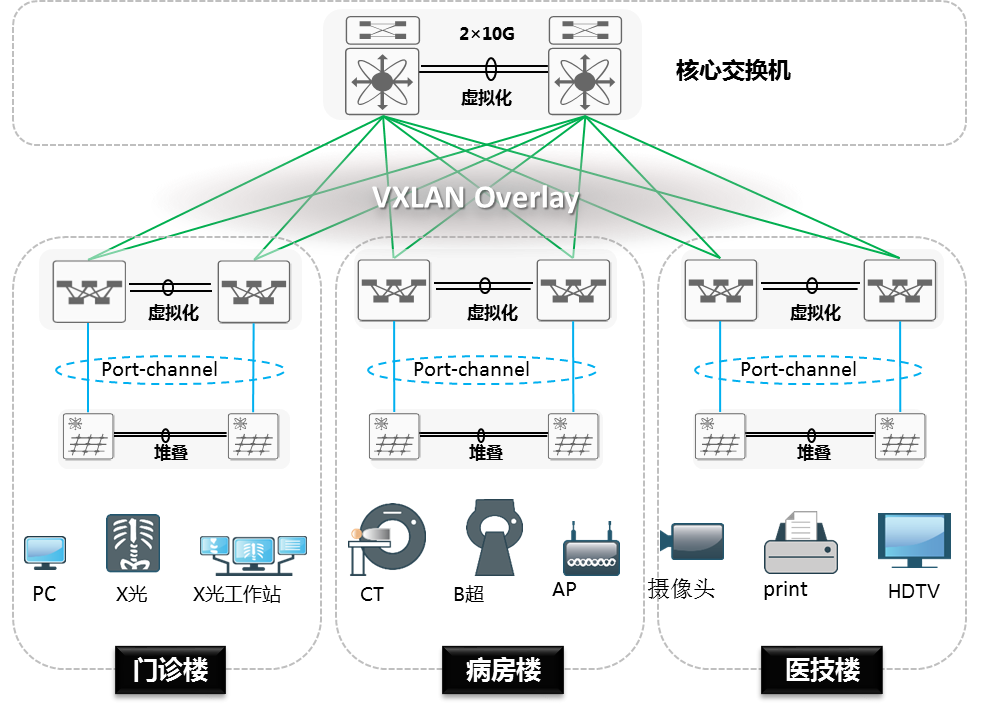
网络访问策略可以基于5W1H的灵活的用户认证接入机制，根据who（谁），whose（谁的设备），what（什么设备），when（什么时间），where（什么地点），how（什么方式）多个维度覆盖各种接入场景。用户可根据自己的需求，灵活定制场景，满足自己个性化的需求。

支持用户终端在整个生命周期中MAC和IP一对一的需求（如基于安全性需要可与端口进行绑定），终端不管移动到哪里，可以做到终端始终获取唯一固定的IP，简化后期的运维。

相比传统网络架构，SDN网络架构的核心为SDN控制器，其主要实现网络设备的自动化上线，用户接入管理，用户组/策略管理，业务配置管理，网络运维管理等功能，同时以上所有功能均能通过直观的图形化界面完成。SDN控制器将管理员的操作在后台转化为网络设备的具体命令进行下发给设备执行。

在整个网络架构设计中，以核心区为中心，其它区域模块化处理。这样设计是由应用的特点决定的，因为几乎所有的应用都需要与其他区域的应用进行通讯，所以需要在网络中设计一个核心交换区，这个区域作为其它区域的交换中心。为了保证更好的网络性能，核心交换区只提供实现高速转发功能，安全控制在各边缘区域中实现。

最后，结合建设需求，整体架构采用模块化的设计方法，清晰定义和区分不同的功能区域，将基础网络平台划分为不同的功能区域，部署不同的应用。能够有足够的稳定性和高性能承载医院医疗业务，并充分考虑网络的扩展性，为医院的语音业务、视频业务、移动医疗、物联网等应用留有足够的升级空间。网络采用万兆主干，千兆到桌面的设计原则。整个网络架构满足高扩展性、灵活性、高可用性和高安全性。



2.2 核心层设计

核心层是整个医院IT架构的运转大脑，因此重要性不言而喻。在核心机房内部署部署两台高性能核心交换机，两台核心交换机之间通过万兆捆绑实现虚拟化，从而实现两台核心设备逻辑上虚拟化为一台，以增强核心区域的可靠性，同时提升核心区域的性能和设备的利用率，核心交换机支持扩展IPS、LB、防火墙、流量分析等业务插卡增加整个网络的安全性。

核心层交换机虚拟化后通过四万兆单模与汇聚交换机互联，并利用链路聚合功能提升链路带宽和实现链路冗余。

2.3 汇聚层设计

在门诊楼、医技楼、住院楼内各部署两台高性能汇聚交换机，两台汇聚交换机之间通过40G捆绑实现虚拟化，从而实现两台汇聚交换机设备逻辑上虚拟化为一台设备，以增强核心区域的可靠性，同时提升区域的性能和设备的利用率，汇聚交换机支持扩展防火墙、流量分析等业务插卡便于后期提升整个网络的安全性控制能力。

汇聚交换机虚拟化后通过四万兆单模与核心交换机互联，并利用链路聚合功能提升链路带宽和实现链路冗余。通过万兆多模与接入交换机互联，并利用链路聚合功能提升链路带宽和实现链路冗余。

2.4 综合接入层设计

综合接入区主要为各类终端提供接入，例如pc、打印机、自助机、IP摄像头、IP电话、无线接入点等以IP网络传输数据的终端，因此接入交换机包含POE和非POE接入交换机。接入交换机以IDF为单位，IDF内的多台交换机通过虚拟化技术实现多虚一形成堆叠组，堆叠组通过万兆多模与汇聚交换机互联，并利用链路聚合功能提升链路带宽和实现链路冗余。

说明：其中由于POE和非POE交换机无法堆叠，因此POE交换机单独双上联汇聚交换机。

2.5 数据中心层设计

数据中心区域主要承载医院各个业务系统，例如HIS、PACS系统、EMR、LIS等，单独划分数据中心区域可保证各个业务系统的可靠性和安全性，在区域里设置两台万兆汇聚交换机，通过万兆连接各个业务系统服务器。同时通过四万兆多模连接核心交换机。

为优化各业务系统的响应效率以及提升业务端查询速度，在数据中心区域内部署应用负载均衡设备实现业务系统集群间的负载均衡，同时为保护应用系统的安全，配备高性能的下一代防火墙实现业务系统的安全防护。

2.6 外联层设计

外联层主要承担医院内网信息系统与医保、市民卡、银联、银行等机构互联互通，为满足等级保护的边界安全防护要求，在外联区域部署高性能的下一代防火墙设备实现安全互联，控制出口区域的流量，进一步增强安全的防护，对整个网络起到保驾护航的作用。

2.7 互联网层设计

互联网区主要是为了工作人员方便访问互联网以及提供掌上医院等业务，通过下一代防火墙实现与互联网的联通，在防火墙上设置DMZ区域，主要部署对外提供服务的前置机，例如在线挂号等，保证数据安全性，同时通过上网行为管理有效的记录每个访问网络的行为。

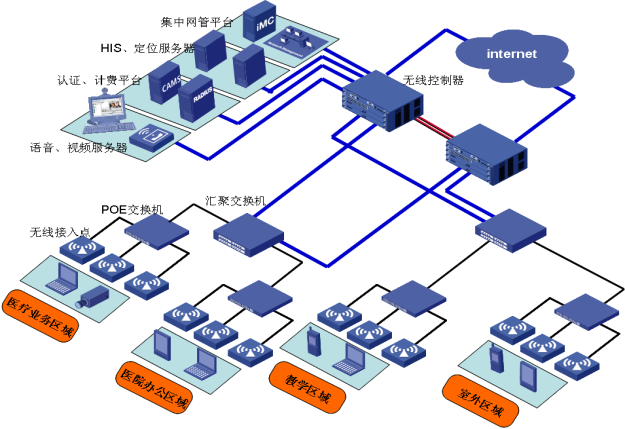
2.8 安全管控层设计

设立网络安全管控区并旁挂核心交换区域，在该区域内部署一系列安全设备，如内网入侵防御、数据库审计、堡垒机；入侵防御有效的对内外数据进行检测和清除有害数据，数据库审计则实时监控着谁操作了数据，堡垒机则实时检测谁对网络中的设备进行了相关的操作，通过这一系列的安全的设备的部署有效的对整个网络的进行防护。

3 无线网络架构设计

采用“瘦AP＋控制器”的集中式管理架构，该无线架构具有简单而强大的无线局域网集中式管理功能，AP本身并不存放任何的配置文件，AP的配置是从AC上获取的，通过AC就可以统一管理整个无线网络的AP。网管人员只需简单地配置无线交换机，即可实现开通、管理和维护所有AP设备以及移动终端，包括无线电波频谱、无线安全、接入认证、移动漫游以及接入用户。

具体的逻辑组网图如下图所示：



无线控制器+瘦无线AP的架构,在实现对医院进行无缝覆盖的同时,又能够实现对无线网络的灵活管理配置,提高网络维护效率。

3.1 无线控制器部署设计

本次方案采用在核心交换机上旁挂高性能无线控制器的方式。有以下几点优势：

* 统一配置

医院内所有无线控制器的配置需要进行统一，当为一台主无线控制器对无线网络系统进行配置后，其他所有从控制器都从主控制器进行同步配置，降低无线网络的维护管理成本，提高效率。

* Portal 热备

当多台无线控制器工作在双机模式时，可以实现Portal认证高可靠。用户通过其中一台AC完成Portal认证。双机将相互同步用户的认证状态等数据。任何一台AC down时，由于另台AC已经预同步了用户的认证数据，所以可以避免Portal重认证和用户业务中断，满足了电信级可靠性需求。

* DHCP Server热备

当2台无线控制器工作在双机模式时，用户通过其中一台AC获得DHCP地址分配后，AC间将同步地址池信息。一台AC down机后，当用户IP地址租约到期时，将发起DHCP请求续约。另一台AC用预备份的地址池数据回应续约，避免了为用户重新分配地址和用户业务中断。

3.2 无线AP部署设计

无线网络在医院的主要作用包括为移动查房提供网络、为医疗物理网应用提供接入、为患者以及内部职工提供网络访问等。按照医院内部区域以及结合区域上的应用需求，可以划分以下几种覆盖场景：

**3.2.1 高密度接入场景**

这类场景以覆盖行政楼、会议室、候诊区等人流量密集为主，这类场景主要以上网需求为主，对无线网络的接入能力要求高并发、高带宽、高稳定。

针对这类场景，采用接入性能高的AP放装部署方案，AP根据实际区域环境吸顶部署，实际数量根据覆盖面积和人数进行规划设计。

**3.2.2 病房场景**

以覆盖病区病房为主，这类场景主要为移动查房、移动护理等应用提供网络接入，对无线网络的接入能力要求无缝漫游、高稳定、抗干扰能力；

针对这类场景，采用分体式方案，即“母AP+子AP”，其中“母AP”部署在楼层弱电间内，通过网线连接“子AP”，“子AP”部署在每个病房内，同时“子AP”可以集成医疗物联网读卡器模块，采用WIFI+RFID模块方式，集成的RFID模块支持433M，还支持2路RFID模块扩展，RFID模块天线采用功分器+馈线方式。具体馈线数量根据实际楼层情况而定。在WiFi信号进入病房的同时，通过集成在AP内部的RFID读卡器，读卡器上的RFID馈线也进入病房和走廊，实现对房间内部和走廊的物联网业务的接入。同时，该款AP同时还支持Zigbee和蓝牙标准，可以实现扩展支持未来医院的物联网业务。

**3.2.3 公共区域**

以病房走廊过道等公共区域为主，这类场景主要实现为无线全覆盖，对无线网络的接入能力要求稳定、抗干扰能力。

针对这类场景，采用标准性能AP放装部署方案，AP根据实际区域环境吸顶部署，实际数量根据覆盖面积和人数进行规划设计。

3.3 无线物联网设计

物联网技术包括WLAN、RFID、蓝牙、zigbee等多种通信技术标准，其中WLAN和RFID技术最为成熟稳定，应用最广，也是本次项目物联网建设采用的主要技术。

本次项目医疗物联网硬件架构采用三层结构设计，分别是感知层、接入层和管理层；感知层实现对各类终端和标签的探知，接入层是AP和RFID阅读器层，实现对数据的接入，管理层是包括物联网AC、物联网中间件MC和网管系统，实现对全部终端和标签集中管理。

本次医疗物联网架构如下：

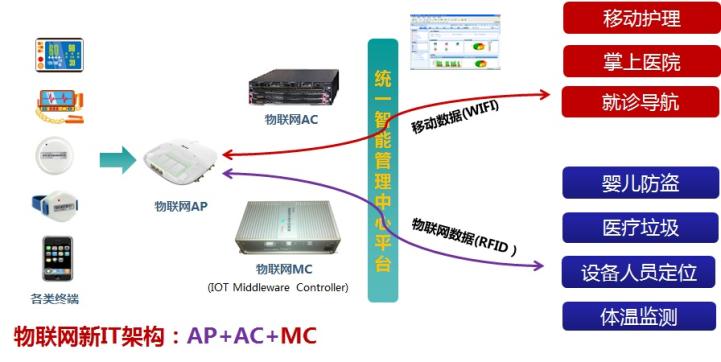


* 物联网AP：整合了WIFI和RFID、ZigBee、蓝牙阅读器功能，可以实现信息多频道的发送和接收，物联网AP既可以接收物联网标签的返回信息，也可以接收支持WIFI的移动终端返回信息，实现前段感知的融合。
* 物联网AC：能够对物联网AP进行统一的管理配置，达到安全、高效的目的。

本次在病房区域采用的AP是可以集成医疗物联网读卡器模块的AP，集成的RFID模块支持433M，支持现有物联网业务，RFID模块天线采用功分器+馈线方式， 医疗物联网AP要求做到如下所示：



需实现的数据处理如下：



3.4 无线AP供电设计

为方便统一管理，提高设备的安全性，本次无线供电设计采用POE供电的方式对无线AP进行远程供电。采用POE方式即通过网线对AP进行供电，POE供电方式具备以下几点优势：首先，安全性更高，通过网线进行供电可以避免本地电源的使用，有效减少强电部署，提高大楼的用电安全；另外，通过POE供电可以实现对AP供电的管理，实现AP的定时开关，一方面提高无线网络的安全性（不必要使用时可关闭无线网络），另一方面，还可以日常费用（不必要使用时，关闭AP节省用电）。

4 网络安全架构设计

4.1系统概述

在医疗行业的信息化建设过程中，信息安全的建设虽然只是一个很小的部分，但其重要性不容忽视。便捷、开放的网络环境，是医疗行业信息化建设的基础，在数据传递和共享的过程当中，数据的安全性要切实地得到保障，才能保障医疗信息化业务的正常运行。

国家公安部、保密局、国家密码管理局、国务院信息化领导小组办公室于2007年联合颁布了861号文件《关于开展全国重要信息系统安全等级保护定级工作的通知》和《信息安全等级保护管理办法》，要求涉及国计民生的信息系统应达到一定的安全等级，根据文件精神和等级划分的原则，医疗信息系统构筑至少应达到二级或以上防护要求。

针对《信息系统安全等级保护基本要求》，部署相应的网络安全防护设备，能够基本满足医院信息安全建设的需求以及通过等级保护测评。

4.2 安全防护设计原则

按照功能区域划分安全域，通过对不同的安全域设置安全防护级别，形成安全域之间互访的控制。

* **核心安全域：**

核心安全域需要对由外向内的数据进行严格控制，所有的流量必须在明确的策略允许下才可以进入，默认拒绝所有不确定的流量；核心安全域同时需要对由内向外的数据进行严格控制，原则上不允许任何主动发起的由内向外的数据流，以避免安全域的主机单点失效后，主动向外发送数据泄漏机密，有需要对外主动发起的通信，必须进行最严格的控制措施。同时，核心安全域需要完善的网络流量记录和审计能力，为网络流量监管提供足够的依据。

在本次方案中，数据中心区、安全管理中心区建议设定为核心安全域。

* **接入安全域：**

接入安全域需要对由外向内的数据进行严格控制，所有的流量必须在明确的策略允许下才可以进入，默认拒绝所有不确定的流量；接入安全域同时需要考虑对由内向外的数据进行精细的控制，根据应用模式的需求，明确的定制有内向外的数据流动策略，否则不允许任何主动发起的由内向外的数据流。同时，接入安全域需要考虑一定网络流量记录和审计能力，为网络流量监管提供足够的依据。

在本次方案中，各局域网区建议设定为接入安全域。

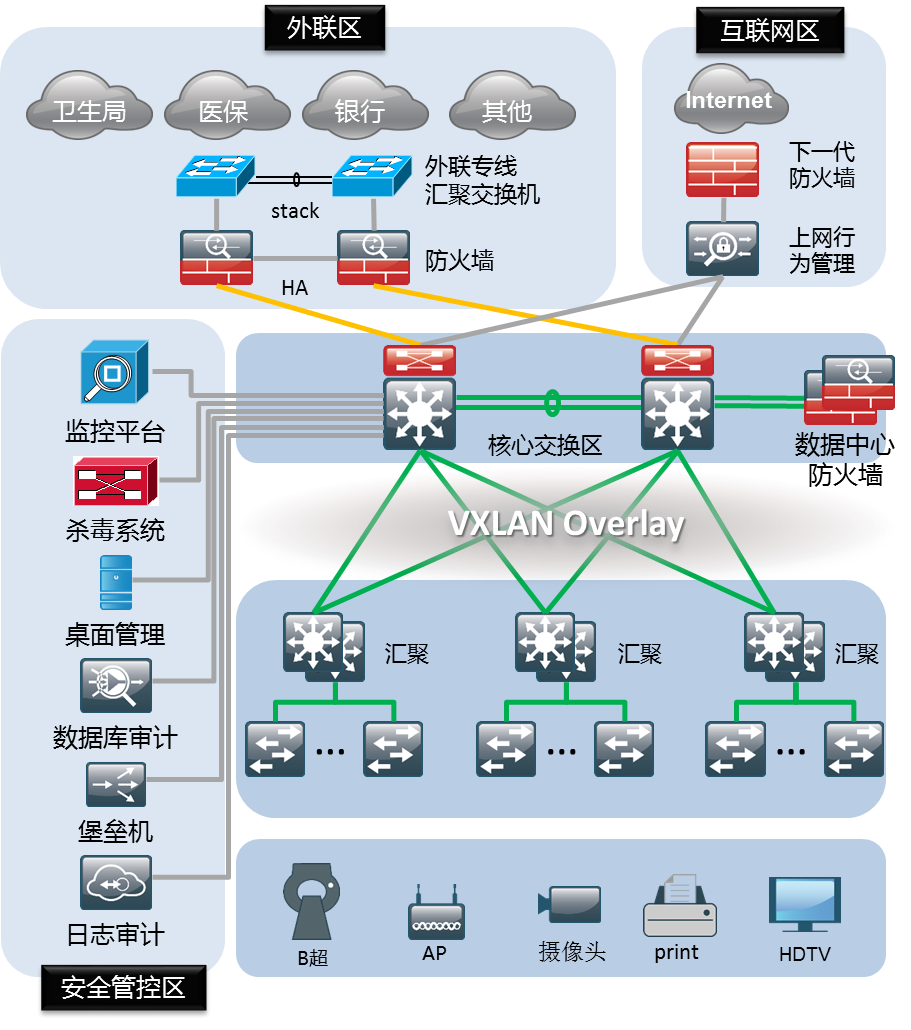
* **边界安全域：**

边界安全域需要对由外向内的数据进行严格控制，所有的流量必须在明确的策略允许下才可以进入，默认拒绝所有不确定的流量；接入安全域需要考虑对由内向外的数据进行精细的控制，根据应用模式的需求，明确的定制有内向外的数据流动策略，否则不允许任何主动发起的由内向外的数据流。

在本次方案中，内网外联区和互联网区建议设定为边界安全域。

4.3 网络安全防护设计

### 4.3.1 结构安全设计

由于SDN架构整网采用overlay的技术，所以架构天然具备网络逻辑隔离能力，相比MPLS的隔离方式，VXLAN的隔离只需要在端点（VTEP）做隔离，不需要全网隔离，端点之间只需要IP互通既可。一方面让整个运维节点大幅减少，另一方面端点之间支持多链路连接，负载均衡可以直接通过ECMP来实现，让整个组网清晰、运维更简单。

### 4.3.2 网络边界安全设计

**(1)外联区域边界安全防护**

外联区域主要包含与市民卡、医保专网、异地医保、银行等业务的互联，由于专网属于不同单位的核心网络，其安全级别和安全防护要求不一样，所以在外联区域出口部署高性能的防火墙进行流量的检测和隔离，通过将专网的专线接入到外联区域的边界防火墙上，通过防火墙的路由及NAT功能，实现内部系统与医保、市民卡等专网系统的互联互通。并通过在防火墙配置严格的访问控制措施，只允许授权用户及IP地址访问专网，同样只允许授权的用户及IP地址访问我院信息网络，其他未经授权的用户不得相互访问。

由于传统防火墙只能提供ISO三至四层的访问控制和过滤，无法做到应用层的安全防护。同时，由于医院内部网络部署了大量的应用服务器，有些服务器需要对互联网用户提供访问，为了保证应用服务器在被专网访问过程中的更高层次的安全防护，因此在外联区域部署入侵防御系统，对进出入侵防御系统的流量和会话进行过滤，通过入侵防御系统强大的特征库和入侵行为防御能力，有效的缓冲溢出攻击、WEB服务的注入、XSS跨站攻击、DDOS攻击、蠕虫、木马扫描等攻击行为进行有效的拦截，使得有效地过滤掉进出网络中的非法流量及入侵行为，确保我院内网服务器的安全。

通过入侵防御系统与防火墙协同配合，针对外联区域构建一道二至七层的安全防护体系，保证内网应用服务器和计算终端的安全，免遭黑客和非法访问者的攻击、蠕虫木马的危害，确保我院整体网络安全。

**(2)互联网出口边界防护设计**

通过在互联网出口部署防火墙设备，通过独立硬件式防火墙实现内网安全防护，并通过互联网边界的防火墙设备设立一个独立的DMZ区域，用来部署医院的WEB、网上挂号等对外提供访问的应用系统。

利用防火墙的NAT和路由功能，配置NAT地址转换策略，使用户能够通过防火墙访问互联网、浏览网页、邮件收发等。同时，通过在防火墙设备配置端口映射及IP地址映射策略，将DMZ区域的应用系统发布到互联网。如对外医院网站、办公系统、网上挂号、远程医疗协助等。

通过在防火墙配置严格的基于源IP、目的IP、源端口、目的端口、时间等五元组的访问控制策略，对内部上网用户进行严格控制，只有被允许的用户和IP地址才能访问互联网，未经授权的用户及IP严格控制其访问互联网。严格禁止互联网用户访问医院的内部网络，通过配置针对端口的访问策略只允许互联网用户访问DMZ区域应用服务器所允许访问的端口和服务，确保医院内网的安全。

利用防火墙的访问控制可以很好的过滤掉来自互联网威胁访问，但是由于防火墙只能提供ISO三至四层的访问控制和过滤，无法做到应用层的安全防护。同时，由于医院内部网络部署了大量的应用服务器，有些服务器需要对互联网用户提供访问，为了保证应用服务器在被外网用户访问过程中的安全，在互联网的出口部署入侵防御系统，对进出入侵防御系统的流量和会话进行过滤，通过入侵防御系统强大的特征库和入侵行为防御能力，实现缓冲溢出攻击、WEB服务的注入、XSS跨站攻击、DDOS攻击、蠕虫、木马扫描等攻击行为进行有效的拦截。入侵防御系统通过与防火墙协同配合，在互联网出口构建一道二至七层的安全防护体系，保证内网应用服务器和计算终端的安全，免遭黑客和非法访问者的攻击、蠕虫木马的危害。确保我院整体网络安全。

另外，通过部署上网行为管理设备，针对内部上网用户行为的管理和流量进行控制，能够有效对P2P下载、P2P视频、在线游戏、网络电视、视频网站、炒股软件、即时通讯攻击进行控制和过滤，同时可以实现用户上网行为的追溯，以满足公安部对互联网的82号令的政策要求。

### 4.3.3 内网网络安全设计

**(1) 入侵检测防护**

通过在安全管控区部署一台入侵检测系统，对核心数据区域及应用服务器区域的访问等内部全局流量进行检测，全局型入侵检测防护策略如下：

* 网络检测策略：在检测过程中入侵检测系统综合运用多种检测手段，在检测的各个部分使用合适的检测方式，综合采用误用检测技术和异常行为检测技术，能够有效发现网络中异常的访问行为和数据包；
* 协议检测策略：我院业务网底层协议为TCP/IP，入侵检测系统采用细粒度检测技术，协议分析技术，误用检测技术，协议异常检测，可有效防止各种攻击和欺骗。并且还能够通过策略编辑器中的用户自定义功能定制针对网络中各种TCP/IP协议的网络事件监控；
* 协议解码策略：部署的入侵检测系统通过对应用服务器区内、以及数据中心区域内采用基于TCP/IP的各种协议分析事件技术,如：HTTP、SMTP、FTP、TELNET等应用层协议连接、关闭，Pop3命令连接请求、应答，各种应用层协议的关键字解码等，保护服务的持续性；
* 智能IP碎片重组策略：对所监视网络中的IP碎片报文重组后进行分析，防止IP碎片欺骗，在业务网边界部署的防火墙进行访问控制基础上，进一步提高系统的抗攻击能力；
* 事件风暴处理策略：可将一定时间范围内的同种攻击类型事件合并成同一条在控制台进行显示并记录攻击次数，从而达到防止控制台被报警事件洪水淹没屏幕的目的；
* 安全联动策略：与防火墙安全联动策略类似，通过安全联动策略，使防火墙能够与入侵检测系统进行联动，当入侵检测系统发现攻击行为时，及时通知防火墙，防火墙在接收到信息后动态生成安全规则，将攻击来源进行阻断，从而形成动态的防护体系；
* 监控管理策略：入侵检测系统提供人性化的控制台，提供初次安装探测器向导、探测器高级配置向导、报表定制向导等，易于用户使用。一站式管理结构，简化了配置流程。强大的日志报表功能，用户可定制查询和报表。
* 异常报警策略：入侵检测系统通过报警类型的制定，明确哪类事件，通过什么样的方式，进行报警，可以选择的包括声音、电子邮件、消息以及与防火墙联动。

**(2)日志事件审计**

通过在安全管控区部署一台日志审计系统，对医院信息网络中有大量的访问和数据包进行安全审计并将审计日志存在本地磁盘，通过安全审计系统发现网络中存在的安全隐患，并可以对访问过程进行还原，在发生安全事故时，通过对访问过程的还原，即能有效发现系统中可能存在的安全隐患，还为安全事故的事后处理提供证据。

通过日志审计系统可以分析、判断特定行为或者事件是否为违反安全策略的异常行为，主要有如下四个步骤：

* 数据采集：网络安全审计系统需要采集必要的数据用于审计分析。
* 数据过滤/协议还原：根据预定义的设置，进行必要的数据过滤及缩略，从而提高检测、分析的效率。同时对数据进行协议还原，提取用户关心的内容数据。
* 数据存储：将内容数据按一定的策略进行本地或远程存储。
* 数据分析/审计/报警：根据定义的安全策略，进行审计/分析。一旦检测到违反安全策略的行为或者事件，进行报警。

**(3)访问控制设计**

在信息网络中全网实施VLAN与ACL访问控制列表，针对办公区域、业务办公等按照不同部门、不同科室等实施VLAN技术进行隔离，并采用ACL访问控制列表进行不同VLAN相互之间的访问控制。

VLAN技术是近年来在计算机网络领域使用广泛一种局域网技术。虚拟网在逻辑上等于OSI七层模型上第二层的广播域，它与具体的物理网及地理位置无关

在传统的网络技术中，同一物理网段中的用户在网络层上很难实施安全措施，而在虚拟网络环境中，不同的虚拟网络间用户之间的通信控制则可以做到。虚拟网间的安全与虚拟网间的通信方式有关，由于虚拟网间通信是通过第三层交换功能实现的，第三层交换功能使得通信双方不能直接连接，而第三层交换模块的ACL功能可被用来对不同虚拟网间用户的通信做逐项检查，通信可以按照网络管理人员的要求被允许或禁止，从而实现不同部门或不同应用系统间的访问控制，从而提高了网络的安全性。

**(4)准入控制防护**

通过准入控制实现网络入口的管控，将非信任的终端拒之门外，为网络安全把好第一道关。

传统解决方案，直接在接入交换机开启基于端口或基于MAC的802.1x协议实现准入认证。在本次方案中利用SDN架构自带的认证功能即能够实现不同终端的接入认证，比如摄像头等哑终端，通过MAC地址认证的方式接入，办公电脑通过域账户或者用户名和密码进行认证，无线终端可通过portal方式认证等

**(5)终端安全管理防护**

通过在安全管控区部署部署终端安全管理系统对终端主机实现桌面行为监管、外设和接口管理、非法外联监控和终端资产管理功能。通过它以强制执行统一安全策略为核心，实现从“自主安全”到“强制安全”。

通过终端安全管理系统可实现集中下发统一的安全策略，同时实现以下主要安全目标：

* 通过进程管理，采用黑白名单方式，约束终端只能运行经过允许的应用程序，禁止用户使用违规软件，防止病毒进程在系统中潜伏。
* 通过对终端的外设与接口管理，可以控制各种外设和接口的使用，防止通过这些接口进行文件拷贝、数据读取等操作行为带来各种潜在安全风险。
* 对接入办公网的计算机进行检查，必须符合相应的安全要求，如防病毒安装、运行情况，主机补丁安装情况。只有符合安全策略检查的终端，才可以接入网络。
* 对终端的非法外联行为进行监控，主要用于发现和管理内网非法建立通路连接互联网或其它网络的行为。通过对非法外联的监控管理，可以防止外联行为引入安全风险或导致信息泄密。
* 与边界安全设备进行联动，一旦发现终端上有不安全行为，立即通知边界安全设备，阻断相应终端的网络访问行为。

通过强化终端操作行为的管理，一方面，可以加强网络管理中心管理员对终端系统的控制；另一方面，减少终端引入各种攻击、木马、病毒、蠕虫等风险源，降低对办公网的安全威胁。

### 4.3.4 外网网络安全设计

**(1)WEB应用安全防护**

在互联网出口区域部署一台WEB安全防火墙，建议采用策略路由的方式连接。主要对进入内网服务器的Web流量进行检测，对由外部到内部核心应用发起的SQL注入、XXS跨站、网页篡改、CC等攻击进行有效的拦截。

以下WEB防火墙安主要功能：

* + Web应用安全防护

WAF需要防护基于HTTP/HTTPS/FTP协议的蠕虫攻击、木马后门、CGI扫描、间谍软件、灰色软件、网络钓鱼、漏洞扫描、SQL注入攻击及XSS攻击等常见的Web攻击；

* + 应用层DOS攻击防护

WAF需要防护带宽及资源耗尽型拒绝服务攻击。 XML DoS攻击防护是对HTTP请求中的XML数据流进行合规检查，防止非法用户通过构造异常的XML文档对Web服务器进行DoS攻击；

* + Web虚拟服务

通过部署WAF来管理多个独立的Web应用，各Web应用可采用不同的安全策略，可在不修改用户网络架构的情况下增加新的应用，为多元化的Web业务运营机构提供显著的运营优势与便利条件；

* + Web请求信息的安全过滤

针对HTTP请求，WAF能够针对请求信息中的请求头长度、Cookie个数、HTTP协议参数个数、协议参数值长度、协议参数名长度等进行限制。对于检测出的不合规请求，允许进行丢弃或返回错误页面处理；

* + Web敏感信息防泄露

WAF应内置敏感信息泄露防护策略，可以灵活定义HTTP错误时返回的默认页面，避免因为Web服务异常，而导致的敏感信息（如：Web服务器操作系统类型、Web服务器类型、Web错误页面信息、银行卡卡号等）的泄露；

* + Cookie防篡改

WAF产品能够针对Cookie进行签名保护，避免Cookie在明文传输过程中被篡改。用户可指定需要重点保护的Cookie，对于检测出的不符合签名的请求，允许进行丢弃或删除Cookie处理，同时记录相应日志；

* + 网页防篡改

WAF产品可按照网页篡改事件发生的时序，事中，实时过滤HTTP请求中混杂的网页篡改攻击流量（如SQL注入、XSS攻击等）；事后，自动监控网站所有需保护页面的完整性，检测到网页被篡改，第一时间对管理员进行告警，对外仍显示篡改前的正常页面，用户可正常访问网站；

* + Web业务的连续性

作为串行安全防护设备，WAF需要考虑了Web系统业务连续性保障措施，以有效避免单点故障；

### 4.3.5 应用安全防护

**(1)核心系统安全防护**

通过在数据中心区域内部署部署高性能的下一代防火墙，考虑防火墙对数据转发造成的影响以及未来的扩展，建议通过策略的方式连接核心交换机。

防火墙主要针对进出关键核心系统的流量进行检测，该防火墙在选型时必须考虑满足防火墙、入侵检测、WEB防护等能力。

**(2)虚拟化安全防护**

数据中心已经从物理架构演进到大规模虚拟和云的架构，服务器和存储被虚拟化成为很多数据中心的标准。虚拟数据中心在效率、业务敏捷性，以及快速的产品上市时间上有明显的优势。然而针对虚拟化系统的安全防护，传统安全解决方案和策略还没有足够的准备和定位来为新型虚拟化数据中心提供高效的安全层，这是有很多原因的。

这是因为传统安全解决方案是专为物理环境设计的，不能将各类产品有效地插入东西向流量的环境中，往往需要将东西向流量重定向到物理防火墙、深度报文检测、入侵防御，以及防病毒等服务链中去。这种流量重定向和静态安全服务链的方案对于保护东西向流量是效率很低的，因为它会增加网络的延迟和制造性能瓶颈，从而导致应用响应时间的缓慢和网络掉线。

例如在私有云环境中，某虚机由于某种原因中了病毒，从内部向其它虚机和外部网络发起端口扫描和DoS等攻击，缺少识控方案的情况下，只能将有问题的虚机从网络中移除，让问题虚机的管理员线下解决问题后，才允许连接回网络，这样的处理方案简单粗暴，虽然隔离了攻击，但也同时断掉了问题虚机的对外服务。所以一定程度上造成了虚拟化环境成为信息安全的一个黑洞。

对于云环境，虽然外部可能部署入侵防御设施，但可能存在这样的情况，某虚机由于弱口令之类的漏洞被远程控制，然后黑客以此虚机为跳板，再对其它虚机进行漏洞扫描和利用入侵，DoS攻击会产生大量的会话，可能通过云管理平台发现，然而从内部发起的漏洞入侵的过程在网络层面上与正常访问无异，无法被发现，因此需要识控的方案。

针对虚拟化环境的安全防护解决方案需要把防火墙等功能插入到虚拟机管理程序层中，从而实现每一个虚拟机跟外部网络或内部其它虚拟机之间通信的精细监控。这样的方案才能够完全解决解决虚拟化内部的安全风险，阻断从内部向其它虚机和外部网络发起的端口扫描和DoS等攻击，而仍然保持问题虚机的对外服务；监控到绕过外部防护、以被控制虚拟机为跳板的内部入侵，为每一台业务虚拟机都提供最贴身的安全防护力度。

**(3)系统运维防护**

通过在安全管控区部署一台堡垒机降低人为事故的发生，通过交换机的访问控制策略限定只能由堡垒主机内控管理平台直接访问服务器的远程维护端口。当维护人员对网络设备、安全设备和服务器系统进行远程维护时，首先以 WEB 方式登录堡垒主机，然后通过堡垒主机上展现的访问资源列表直接访问授权资源。

堡垒主机一般使用应用代理的方式旁路部署在网络上，用户通过本系统访问被管资源，用户的所有访问行为都在监视和控制之下，访问记录经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及关联分析功能，实现对信息系统整体安全状况的全面审计。

**(4)数据库审计防护**

在数据中心区域内部署数据库审计系统，实现三级系统的数据库库表的全面审计，未出现的数据库事件追溯提供证据。

实现功能：

* + 统一日志监控

将企业和组织的IT计算环境中部署的各类网络或安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警全部汇集起来，使得用户通过单一的管理控制台对IT计算环境的安全信息（日志）进行统一监控。

用户不必时常在多个控制台软件之间来回切换、浪费宝贵的时间。与此同时，由于企业和组织的所有安全信息都汇聚到一起，使得用户可以全面掌控IT计算环境的安全状况，对安全威胁做出更加准确的判断。

* + 日志归一化与实时关联分析

收集并归一化的所有安全日志和告警信息，然后通过智能事件关联分析引擎，帮助安全管理员实时进行日志分析，迅速识别安全事故，从而及时做出响应。

* + 集中日志存储

可以将采集来的所有日志、事件和告警信息统一存储起来，建立一个的集中日志存储系统，实现了国家标准和法律法规中对于日志存储的强制性要求，降低了日志分散存储的管理成本，提高了日志管理的可靠性，消除了本地日志存储情况下可能被抹掉的危险，也为日后出现安全事故的时候增加了一个追查取证的信息来源和依据。

* + 灵活的部署方式

部署方式十分灵活，对网络环境的适应性极强，既能够支持单一的中小型网络，也支持跨区域、分级分层、物理/逻辑隔离的大规模网络。产品分为软件形态和硬件形态两种，用户可以根据自身需要选择。系统采用旁路部署，对现有网络结构不做任何改动，支持多端口日志采集，支持通过硬件探针采集日志，支持级联部署。

* + 可视化日志分析

具备强大的事件可视化能力，方便用户日常安全管理的认知为感知。事件可视化不是简单的柱图、饼图、曲线图等统计趋势图表的展示，必须反映出大量事件之间的相互作用关系。可视化功能包括：

1)事件全球定位系统

2)主动事件图

3)事件行为分析

4)动态雷达图

* + 快速响应

识别出安全事故后，能够自动或者用户手工的对威胁进行响应，采取安全对策，从而形成安全审计的闭环。

可以综合分析来自防火墙、IDS、系统日志、网络等等一系列的信息，能够更为精确地定位安全威胁，使得实时自动阻止攻击变得更加可行。在发生告警后，可通过电子邮件、SNMP Trap等方式对外发出通告；能够执行预定义命令行程序，并将事件属性作为参数传递给该命令行程序。

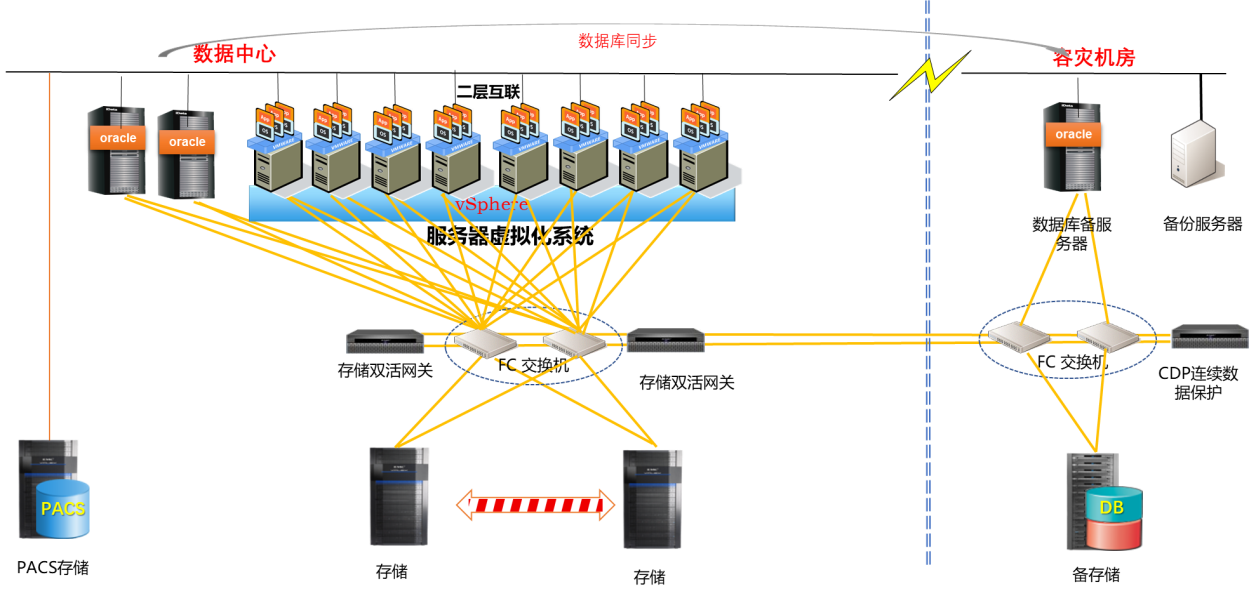
可通过与网络设备或安全设备共同协作来关闭威胁通信，以阻止正在进行的攻击。可以与众多第三方网络设备、安全设备进行联动。

* + 报表报告

可生成的报表图文并茂，报表可以按组管理，可以对报表生成进行日程规划，提供打印、导出以及邮件送达等服务，并根据计划归档报告，归档之后发送邮件通知。报告可用PDF、HTML、Excel、CSV或RTF等格式存档。用户可以自定义报表。

5 数据中心设计

5.1 设计目标

1. 
2. 数据中心拓扑图
3. 核心业务系统如HIS等主机平台的建设，并且满足核心系统平台性能及高可用要求；
4. 非核心业务系统主机平台的建设，以满足非核心业务系统平台性能及高可用要求，同时充分考虑设备的资源利用及未来的业务扩充；
5. 数据存储平台的建设，满足核心业务系统平台数据存储的性能及安全性要求，同时还需要考虑数据存储平台的横向及纵向扩展，满足双活数据中心的要求；
6. 数据备份系统的建设，以满足当业务系统故障时出现数据丢失时，能够快速的恢复数据，降低对业务的影响；
7. 数据中心运维与管理平台的建设，提升信息系统管理人员的工作效率，降低管理的难度。

5.2 应用双活设计

针对HIS等核心数据库应用系统采用2套4路服务器，通过Oracle RAC部署成数据集群，每台服务器配置双口万兆网卡，分别通过网卡绑定技术用于业务和RAC心跳。 主存储配置5块400G SSD硬盘作为数据缓存，配置20块1.8T 10K硬盘

针对PACS、LIS等系统采用服务器虚拟化技术，提升了X86服务器的可靠性、可用性，从基础架构层面获得了原先单机系统无法想象的功能，大大提高了业务连续性的级别，降低了故障率、减少了系统宕机的时间。虚拟化服务器采用了两路CPU服务器，分别部署在两台数据中心。每台配置2块16Gb单口HBA卡，通过光纤交换机，连接共享存储，组成HA高可用系统；

5.3 存储双活设计

此次数据中心双活存储虚拟系统解决方案，分别在两个机房部署两台存储网关，并分别将两台虚拟化存储部署在不同的机房，实现完全对等的双活数据中心，并实现容灾的效果。这样部署完成后，虚拟化存储之间数据的实时同步镜像，构建双活架构，项目建设完成后，两台存储同时工作，任何一台存储出现故障，业务访问不会中断，极大的提升了应用的高可用。

5.4 分布式海量存储

与分散的存储孤岛相比，可以更加高效地满足应用程序的文件请求。为使 IT 服务更加密切适应业务目标，我们需要做出很多的计划和努力，这其中的第一个步骤就是整合分散的资源，使整合后的系统数量更少但更具可扩展性。通过将数据集中至单一的命名空间/文件系统，并简化与保存、移动和访问文件相关的管理任务来支持整合。

目前的NAS 解决方案将会是一种复杂而又昂贵的方式。为了能容纳 IT 基础架构中的唯一名称逻辑分组，企业通常要使用多个命名空间。目前的 NAS 技术对于每个命名空间一个文件系统的各个文件管理器，因扩展能力有限带来了极高的复杂性和不必要的开支。

而分布式存储提供了一个全局命名空间，允许基础架构存储容量从 TB 级扩展至 PB 级，从而能够支持大容量的非结构化数据。该方案支持多种标准网络协议，包括通用互联网文件系统（CIFS）、网络文件系统（NFS）等。

分布式存储全局命名空间可使管理自动化。借助分布式存储所包含的基于策略的迁移工具进行分层和近线数据归档的存储池，可实现快速搜索、备份和还原。此外，该方案还具有安全性、智能负载平衡、动态精简配置、性能优化等数据管理功能。

本次针对PACS大容量存储存储采用横向扩展式（Scale-out）NAS，可组合多个节点，形成一个集群NAS系统。只需要向集群NAS架构中添加节点即可实现资源的扩展。本次配置3个节点，每个节点配置2T\*36=72T裸容量。整个系统实际可用容量会达到120T

5.5 数据安全保护设计

为了规避数据的逻辑性错误，同时部署CDP系统系统，可以为基于块、文件或应用数据，并且为数量无限的可变恢复点提供精细的可恢复对象。

另外，采用数据库复制技术将用户核心HIS、EMR系统数据库数据采用同步或异步方式复制到异地机房，此复制方式与硬件平台、系统平台无关，是基于数据库层面的一种备份方案。主数据库在遇到极端状况时，可以及时切换到备库，保证业务的连续性。

6 统一管理设计

采用统一的管理平台对全院所有有线、无线设备统一管理，轻松实现网络部署、流量监控、实时告警等管理功能。

要求管理平台能够实现如下要求：

(1)提供基于设备面板的设备、单板、端口配置功能，包括环境监控、设备基本信息、IGMP Snooping协议配置、VLAN接口管理、增加接口到VLAN、环回测试、硬件信息浏览、设备IPv6信息浏览、地址绑定、端口聚合管理、端口镜像管理、MSTP协议管理、设备监视、端口监视、OSPF信息浏览、BGP信息浏览、RIP信息浏览、L2/L3接口类型转换等功能。

(2)为了便于网络管理，需提供包含拓扑自动发现、拓扑编辑及自定义、拓扑操作等。系统可根据子网中的二层设备自动绘制的拓扑图，在二层拓扑中显示出了各个设备之间的链路层连接关系（包括聚合链路）、链路状态、设备状态等网络结构和状态信息。

(3)为了便于网络故障诊断，需要对设备性能管理，网络设备的性能综合监测和分析，应具有性能监测管理、性能数据管理、性能阈值门限管理、性能分析及展示等功能。可设置设备资源的CPU监视、内存监视、设备可用性、设备流量、接口流量指标是否监控；支持单个指标、具体实例的启动停止。

(4)提供基于拓扑的区域告警根源分析，提供告警关联分析，提供告警分组分析，有效屏蔽故障引起的海量表象告警，方便用户快速定位、查找故障根源，确认故障影响的范围。

(5)无线管理系统需要提供在拓扑图中对移动终端的信息进行查看，包括MAC地址、信号强度、发射速率集、RSSI、SSID、使用信道、所在AC设备、所在AP设备等，并能查看各移动终端的全部漫游记录，使用户随时了解最终接入用户的情况，并对其接入轨迹进行审计。

(6)提供评估无线网络质量的途径，方便用户了解某区域内的AP工作情况及用户体验情况，根据评估结果及数据记录，用户可采取有效措施进行网络优化，改善网络质量。通过AP设备及移动终端的相关数据进行采集并汇总，根据任务阈值设置的AP及用户的评价标准对AP及用户进行评价，完成评估后可查看网络评估报告了解评估期间AP的工作情况及用户网络使用情况。无线网络管理系统提供丰富的评估报告，显示各位置视图下AP设备的总评信息、评估期间AP及用户各项统计指标的历史及汇总记录、以及相应的评价结果，可通过总评信息了解某位置下AP的整体工作情况，通过各查询条件迅速找到关心的AP及用户。

(7)需要对网络流量进行分析，以便于对网络进行监控和管理。

(8)提供中心机房的3D视图管理、机房环境监控，支持与第三方环境监控系统对接，可以获取温度、湿度、UPS、空调、配电柜、泄漏检测设备、门禁、烟感、新风机等监控系统的数据，并统一显示在3D机房管理图中。提供机房的3D绘制和设计工具。

7 经费预算清单

## 7.1 硬件系统预算

温州医科大学附属第二医院台州院区医院数据中心建设硬件平台包含服务器、存储、网络、无线、信息安全等部分。同时为确保各硬件平台能够顺利实施及落地，本次项目将采用分标段方式进行采购。

## 7.2 详细设备清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **产品配置描述** | **功能要求** | **数量** |
| 1 | 网络控制器 | 软件定义网络控制器，实现网络设备自部署上线，控制用户灵活接入等功能。支持Windows、Linux平台及MS SQL、Oracle数据库，支持B/S架构。本次配置3个集群节点服务器，配置250个有线设备管理授权，配置400个普通无线AP管理授权，配置160个分体AP管理授权，配置2000个终端准入认证授权，配置2000个终端识别授权；三年原厂保修服务； | 详见技术要求章节 | 1套 |
| 2 | 核心交换机 | 采用Clos架构，整机≥8个扩展插槽；支持SDN网络协议并配置功能许可；整机交换容量(以官网标注 的最小值为准)≥30Tbps，包转发率≥36000Mpps；本次单台配置双引擎、冗余电源和风扇、满配交换矩阵、56个万兆光口、40个千兆光口、48个千兆电口，配置1条万兆堆叠线缆；三年原厂保修服务； | 详见技术要求章节 | 2台 |
| 3 | 汇聚交换机 | 支持SDN网络协议并配置功能许可；整机≥4个扩展插槽；整机交换容量≥48Tbps，包转发率≥12000Mpps；本次单台配置冗余电源和风扇；配置48个万兆光口、4个40G光口；配置1条40堆叠线缆；三年原厂保修服务； | 详见技术要求章节 | 12台 |
| 4 | 48口接入交换机 | 支持SDN网络协议并配置功能许可；整机交换容量≥336Gbps，包转发率≥132Mpps；支持48个千兆电口和4个万兆光口，本次单台配置1条万兆堆叠线缆；三年原厂保修服务； | 详见技术要求章节 | 93台 |
| 5 | 24口接入交换机 | 支持SDN网络协议并配置功能许可；整机交换容量≥336GTbps，包转发率≥96Mpps；支持24个千兆电口和4个万兆光口，本次单台配置1条万兆堆叠线缆；三年原厂保修服务； | 详见技术要求章节 | 32台 |
| 6 | 48口POE交换机 | 支持SDN网络协议并配置功能许可；整机交换容量≥336Gbps，包转发率≥166Mpps；支持48个千兆电口和4个万兆光口，本次单台配置1条万兆堆叠线缆；支持POE和POE+，整机输出功率≥800w；三年原厂保修服务； | 详见技术要求章节 | 5台 |
| 7 | 24口POE交换机 | 支持SDN网络协议并配置功能许可；整机交换容量≥336GTbps，包转发率≥96Mpps；支持24个千兆电口和4个万兆光口，本次单台配置1条万兆堆叠线缆；支持POE和POE+，整机输出功率≥370w；三年原厂保修服务； | 详见技术要求章节 | 20台 |
| 8 | 万兆单模光模块 | 汇聚和核心互联使用，LC接口，传输距离10KM； | 详见技术要求章节 | 40个 |
| 9 | 万兆多模光模块 | 汇聚与接入、服务器互联使用，LC接口，传输距离300m； | 详见技术要求章节 | 400个 |
| 10 | 千兆单模光模块 | 汇聚与室外交换机互联使用，LC接口，传输距离10km； | 详见技术要求章节 | 10个 |
| 11 | 千兆多模光模块 | LC接口，传输距离500m； | 详见技术要求章节 | 50个 |
| 12 | 无线控制器 | 支持6个千兆光电复用端口和2个万兆光口；最大可管理1024个AP；本次配置512个AP授权函，配置冗余电源，配置堆叠模块和线缆；三年原厂保修服务； | 详见技术要求章节 | 2台 |
| 13 | 放装AP | 支持 802.11ac wave2协议，同时支持2.4和5G双频；内置天线，支持2个千兆电口；三年原厂保修服务； | 详见技术要求章节 | 360台 |
| 14 | 高密AP | 支持 802.11ac wave2 协议，支持3射频组网，同时支持2.4和5G双频；内置天线，支持2个千兆电口；三年原厂保修服务； | 详见技术要求章节 | 10台 |
| 15 | 本体AP | 吞吐量24Gbps；24个10/100/1000M电口和4个万兆千兆自适应光口；整机最大输出功耗240W，每端口最大功率输出14W；最多支持接入24个分体AP；原厂三年质保服务； | 详见技术要求章节 | 10台 |
| 16 | 分体AP | 配置4个千兆电口，提供1个IOT端口，1个RJ45 透传接口，1个上行口；支持802.3af/802.3at兼容供电；支持2.4和5G双频，最大发射功率23dBm；内置低辐射全向天线(基础增益2dBi)；2条空间流数(Streams)，支持802.11ac Wave2；原厂三年质保服务； | 详见技术要求章节 | 160台 |
| 17 | 室外AP | 支持 802.11ac wave2 协议，支持IP68防护等级，同时支持2.4和5G双频；内置天线，支持2个千兆电口；配置室外安装套件；三年原厂保修服务； | 详见技术要求章节 | 10台 |
| 18 | 网络管理系统 | 支持无线设备管理，兼容主流第三方AP，配置≥1000个无线设备管理授权，支持≥2000个终端在线认证；三年原厂保修服务； | 详见技术要求章节 | 1套 |
| 19 | 互联网出口下一代防火墙 | 1U机架式机型，标配6个10/100/1000MBase-T端口，4个SFP扩展插槽，4个SFP光模块；模块化冗余电源；链路聚合、智能DNS、防火墙安全防护、虚拟系统、用户认证与管控、应用识别与管控、带宽管控、连接数控制、访问控制策略、DDOS攻击防御、文件过滤、内容过滤、审计报表、监控统计等；整机吞吐率：>12Gbps；应用层吞吐率：4Gbps；最大并发连接数：>400W，配置IDP攻击规则特征库三年许可，三年原厂保修 | 详见技术要求章节 | 1台 |
| 20 | 互联网上网行为管理 | 吞吐量1G；IPSEC VPN性能100Mb；支持用户数4000；支持超过4700条应用规则数，支持超过2100种以上的应用，660种以上移动应用，并保持每两个星期更新一次；支持URL智能识别；支持审计功能；支持流控功能；2U尺寸，4G内存，1TB硬盘， 单电源，2对ByPass口，4电4光接口 ，1个串口(RJ45) ，2个USB2.0；含三年特征库升级及三年保修服务； | 详见技术要求章节 | 1台 |
| 21 | 外联区域安全防火墙 | 1U机架式机型，标配6个10/100/1000MBase-T端口，4个SFP扩展插槽，4个SFP光模块；模块化冗余电源；链路聚合、智能DNS、防火墙安全防护、虚拟系统、用户认证与管控、应用识别与管控、带宽管控、连接数控制、访问控制策略、DDOS攻击防御、文件过滤、内容过滤、审计报表、监控统计等；整机吞吐率：>12Gbps；应用层吞吐率：4Gbps；最大并发连接数：>400W，配置IDP攻击规则特征库三年许可，三年原厂保修 | 详见技术要求章节 | 2台 |
| 22 | 防病毒软件 | 支持Windows Embedded POSReady 2009、Windows Embedded Enterprise（Windows 7、Vista 和 XP 版本）、Windows Server Core 2008等主流操作系统，本次配置1000个客户端授权，50个服务器端；三年升级服务； | 详见技术要求章节 | 1套 |
| 23 | 日志审计系统 | 2U机架式设备，交流供电，4个工作口，2个管理口；支持审计100个日志源；平均处理能力（每秒日志解析能力EPS）：4000EPS；峰值处理能力（每秒日志解析能力EPS）：5000EPS。三年升级服务； | 详见技术要求章节 | 1台 |
| 24 | 桌面管理系统 | 支持并配置移动介质管理、非法外联控制、资产管理、补丁管理、应用管理、远程协助等功能许可；提供1000个终端管理许可；三年保修服务； | 详见技术要求章节 | 1台 |
| 25 | 内网核心防火墙 | 1U机架式机型，标配6个10/100/1000MBase-T端口，2个SFP扩展插槽，4个万兆光口，4个光模块；链路聚合、智能DNS、防火墙安全防护、虚拟系统、用户认证与管控、应用识别与管控、带宽管控、连接数控制、访问控制策略、DDOS攻击防御、文件过滤、内容过滤、审计报表、监控统计等；整机吞吐率：>16Gbps；应用层吞吐率：8Gbps；最大并发连接数：>800W，配置IDP攻击规则特征库三年许可，三年原厂保修 | 详见技术要求章节 | 2台 |
| 26 | 运维堡垒机 | 1U机架式结构，可用存储容量2TB，4个千兆电口，系统图形并发80，字符并发180。本次配置100个设备授权，三年保修服务； | 详见技术要求章节 | 1台 |
| 27 | 数据库审计 | 1U机架式设备，硬盘可用容量1TB, 支持RAID0、RAID1；提供4个千兆电口；整机吞吐量1Gbps，日处理业务操作数2亿条，数据采集1万条/秒，审计日志检索1500万条/秒；三年保修服务； | 详见技术要求章节 | 1台 |
| 28 | 应用负载均衡 | 吞吐量最大可扩展至26Gbps，提供2个万兆光口和8个千兆电口；四层并发会话数12M，每秒新建778000，每秒七层请求1100000；配置动态就近性选路功能、2个VDC许可、web应用加速功能、全局负载均衡功能、服务器负载功能；支持流量透明转发，7层应用分发功能；三年保修服务； | 详见技术要求章节 | 2台 |
| 29 | 数据库服务器 | 4\*E7-4830 v4，256G DDR4 2400内存，2块600G 15K SAS,2块双口万兆SFP+网卡，2块单口16G FC HBA卡，冗余电源风扇。三年保修服务； | 详见技术要求章节 | 2台 |
| 30 | 数据库存储 | 同时支持并提供NAS、IP SAN和FC SAN模式，控制器数量≥2；配置控制器缓存≥96GB；本次配置5块400G SSD硬盘作为数据缓存，配置20块1.8T 10K硬盘；三年保修服务； | 详见技术要求章节 | 3台 |
| 31 | 双活存储虚拟化系统 | 配置2个控制器，8个16Gb/s FC 主机接口，8个16Gb/s FC后端阵列接口。引擎互联采用IB互联，提高交换机速度，配置256GB 高速缓存，配置1TB容量许可和双活许可，三年保修服务； | 详见技术要求章节 | 2套 |
| 32 | 存储光纤交换机一 | 本次配置48个线速端口,激活48个许可；配置46个16G FC模块和2个16G FC 10KM单模模块；三年保修服务； | 详见技术要求章节 | 2台 |
| 33 | 存储光纤交换机二 | 本次配置48个线速端口,激活24个许可；配置22个16G FC模块和2个16G FC 10KM单模模块；三年保修服务； | 详见技术要求章节 | 2台 |
| 34 | 虚拟化服务器 | 2颗Intel E5-2630v4 CPU; 256GB ECC DDR4-2400内存； 2块600GB 10K SAS 2.5寸硬盘；集成双口万兆含SPF模块；2块单端口16GB光纤HBA卡；热插拔冗余电源和系统风扇；2U机架式;三年保修服务； | 详见技术要求章节 | 8台 |
| 35 | 备份服务器 | 2颗Intel E5-2630v4 CPU; 64GB ECC DDR4-2400内存； 8\*6TB硬盘；集成双口万兆含SPF模块；热插拔冗余电源和系统风扇；2U机架式;三年保修服务； | 详见技术要求章节 | 1台 |
| 36 | 分布式存储 | 3个分布式节点，采用QDR InfiniBand交换机互连，每个节点配置2个InfiniBand接口。每节点配置每节点配置36块2TB 7200RPM SATA硬盘。配置SmartConnect许可，配置SmartQuotas许可；三年保修服务； | 详见技术要求章节 | 1套 |
| 37 | 服务器虚拟化软件 | 配置16个CPU授权合法许可，含虚机备份。配置云管理平台，包含100台虚拟机许可。可与虚拟化系统无缝配合，实现虚拟化环境的管理和运维。三年技术支持服务； | 详见技术要求章节 | 1套 |
| 38 | 操作系统 | windows 2012 Datacenter版，三年技术支持服务； | 详见技术要求章节 | 8套 |
| 39 | Oracle数据库 | Oracle 12C 4C+4RAC，三年技术支持服务； | 详见技术要求章节 | 1套 |
| 40 | SQL数据库 | Sqlserver 2016企业版，三年技术支持服务； | 详见技术要求章节 | 1套 |
| 41 | 数据库容灾软件 | 实现主备中心之间的文件、数据实时复制，当生产系统发生故障或灾难时，可以及时启用灾备系统，减少业务系统下线时间。并要求灾备中心数据库始终处于Open状态，用于提供数据查询和统计报表功能。三年技术支持服务； | 详见技术要求章节 | 1套 |
| 42 | 备份软件 | 同时支持备份、还原、复制和容灾解决方案。无代理方式备份、复制和还原数据库应用（Oracle, SQL, Exchange,SharePoint,AD或者其它应用系统），配置广域网加速器，提升广域网容灾的性能。配置8台服务器或16CPU许可。三年保修服务； | 详见技术要求章节 | 1套 |
| 43 | CDP连续数据保护 | 配置1套连续数据保护集群，2个控制器，配置Local 10TB本地复制许可，用户提供机架，国标电源线; 三年保修服务； | 详见技术要求章节 | 1套 |
| 44 | 灾备主机 | 4\*E7-4830 v4，256G DDR4 2400内存，2块600G 15K SAS,2块双口万兆SFP+网卡，2块单口16G FC HBA卡，冗余电源风扇。三年保修服务； | 详见技术要求章节 | 1台 |
| 45 | KVM切换器 | 16口切换器及LCD套件；三年保修服务 | 详见技术要求章节 | 1台 |

7.3 具体技术参数

### 7.3.1 网络控制器

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| 系统兼容性 | 可以支持Windows、Linux平台及MS SQL、Oracle数据库，支持B/S架构。 |
| 控制器部署方式 | 可以支持多服务器分布式虚拟化部署，可实现负载分担；支持双机热备、冷备模式，实现高可用性。 |
| 系统权限划分 | 操作员权限基于资源、角色等多维度划分；支持RADIUS、LDAP等多种认证方式，实现更安全更细致的登录控制；操作员支持ACL访问控制列表。 |
| ▲开放性 | 支持Restful API标准接口，便于向第三方系统对接。要求接口免费开放并且提供接口说明文档。 |
| 界面友好体验 | 基于操作员视图，提供拖拽方式布局和增加自定义首页监控对象和内容。 |
| 基于角色的网络设备自动化 | 支持网络设备（院区核心、汇聚、接入等）自动化部署上线，通过DHCP实现设备配置一次性完全下发，而不是借助任何介质（比如U盘或者4G等方式）进行的设备自动化上线。对于已有网络，新增设备，可以自动纳管并且进行设备配置的下发。 |
| 设备可视化自动上线 | 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。 |
| 全网资源统一管理 | 支持路由器、交换机、无线、安全、语音、存储、监控、服务器、打印机、UPS等设备进行管理，实现设备资源的集中化管理。管理员可以通过该功能根据业务需求创建设备组视图，并将所需设备加入该视图中，以便进行管理。 |
| 拓扑管理与融合拓扑 | 提供多种拓扑视图，方便管理员以不同视角查看网络拓扑信息。能够提供接入用户网络拓扑，在拓扑上实现在线用户管理的功能。 |
| IP管理 | 提供IP地址统计、查找功能，IP地址分配完成后，管理员能够通过IP地址分配情况统计图表和各类查询条件，直观的了解和掌握整个网络的IP地址资源使用情况。 |
| 基于用户网络资源编排 | 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(不限于VLAN、VXLAN、IP网段、IP地址）的绑定。简化底层网络规划。 |
| 图形化策略定义 | 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。 |
| 隔离域编排 | 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。 |
| 物联终端的接入 | 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。 |
| 按角色进行IP地址分配 | 支持基于角色的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，方便通过一条ACL在任意设备上实现对用户组权限的控制。 |
| 用户IP绑定 | 可以实现对DHCP服务器进行控制，配合基础网络实现接入用户名绑定IP地址，可以实现提前规划，DHCP按照用户规划进行终端的IP分配。 |
| 用户IP锁定 | 可以实现对DHCP服务器进行控制，配合基础网络实现接入用户名锁定IP地址，即某用户首次入网获取某一IP地址，再次入网，即使在更换终端，更换接入方式，更换位置的情况下，仍旧获取原有的IP地址。 |
| 多场景的名址绑定能力 | 用户名和IP绑定、锁定支持单用户多终端场景使用、也可以支持单终端多用户的场景，实现公共终端的使用。 |
| 单账号多终端 | 所有账号，默认最大绑定一个IP，绑定多终端，其实是指最大允许多个绑定的IP同时在线；如果账号最大在线IP未达到绑定上限个数，允许新终端接入和绑定，并挤占非在线用户的绑定IP；如果账号对应的在线用户数已经达到上限，使用该账号的新用户不允许接入；实时刷新DHCP server上的绑定关系，确保正确绑定。 |
| 单终端多账号（公共机） | 用户即使在公共机上，也能获得自己所属角色的绑定IP，和在专属机器上的体验一致；对于公共机来说，不同用户切换，公共机的所属安全组不停切换，绑定IP不停切换；通过EIA和后台dhcp server的交互，完成对绑定表项的刷新。 |
| 业务虚拟网络（Overlay网络）管理 | 提供针对业务的虚拟Overlay网络的管理，可以自动识别并导入端点设备，自动识别网络中的虚拟专用网络和隧道，并实现对虚拟网络的加入监控、移除监控、查看分层拓扑、查看业务拓扑、查看全网拓扑、查看详细信息和查看流量信息等功能。 |
| 告警管理 | 提供对全网设备告警的实时监控和统一浏览；提供多种提醒方式，如界面上的告警实时提醒、告警音响提示；支持多种转发方式，比如转E-mail，转短信等。提供告警分析，可以屏蔽重复告警、闪断告警，提供告警自动确认功能。 |
| Syslog | 可以接收Syslog，完成基本格式的解析，并入库。提供Syslog特征分析及策略注册能力，支持基于统计规则进行聚合生成告警（Trap）。 |
| 性能 | 提供基于任务的性能监控，可定制监控任务，长期监控网络性能，可以形成日报、周报、月报等报表。支持定制性能阈值，可以为监控的性能指标设置两级阈值，当性能指标超过阈值时根据不同的阈值发送不同级别的告警。 |
| 合规 | 提供合规检查，通过此功能可以简单方便的检查园区网络是否满足园区定制的法规，并提供修复功能，可以及时解决在网络环境中出现的配置、安全问题，使网络长期处于一个安全、稳定的环境。 |
| 故障诊断 | 提供单设备故障诊断和设备间连通性诊断功能，管理员通过诊断的设备IP地址，即可以在整个控制器平台搜索出告警信息、性能信息、网络配置等一系列相关信息，协助管理员快速进行故障定位，并且管理员可以通过诊断结果进行相应操作。 |
| 承载服务器 | 为保证SDN控制器可靠性，要求部署三台承载服务器。CPU：E5 2609 V4\*2,32G内存，2块900G 10K SAS硬盘，4个千兆电口，2个万兆光口,500W电源 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 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。 |
| 配置要求 | 配置≥1套网络控制器平台软件，配置高可靠HA授权，配置业务编排功能授权，配置≥250个有线设备管理授权，配置≥400个普通无线AP管理授权，配置≥160个分体AP管理授权，配置≥2000个终端准入认证授权，配置≥2000个终端识别授权，配置相应的部署服务 |
| 服务要求 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.2 核心交换机

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| ▲架构 | 能够配置独立的交换网板与独立的主控板，交换网板与主控板硬件槽位分离；业务板卡与交换网板采用CLOS架构。 |
| 设备性能要求 | 交换容量（以官网标注的最小值为准）≥30Tbps；包转发率≥36000Mpps |
| 主控槽位≥2 个，业务槽位≤8 个，独立交换网板≥4 个 |
| 接口要求 | 要求设备支持千兆电口，千兆光口，万兆光口、万兆电口、40G端口、100G端口，单槽位万兆电端口密度≥24，单槽位100G端口密度≥16 |
| MPLS | 实配MPLS功能，支持L3 VPN、支持VLL、支持VLPS、支持MCE |
| 虚拟化 | 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 |
| 支持全面网络虚拟化技术，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Overlay网络虚拟化能力，支持二层、三层VxLAN网关功能 |
| 路由表 | 整机IPv4 FIB表项≥3M，IPv6 FIB表项≥1M |
| ARP | 整机ARP表项≥170K，学习速率≥1.1K/S， |
| 多业务扩展 | 支持独立硬件应用控制网关业务板、独立硬件负载均衡业务板、独立硬件流量分析业务板 |
| 安全特性 | 支持硬件级加密技术（IEEE802.1ae）介质访问控制安全功能 |
| 设备支持CPU防攻击功能，支持对协议攻击报文的识别和拦截，保证CPU的正常工作 |
| ▲单台配置要求 | 配置双主控引擎、配置此设备最高规格的独立交换网板（≥4块）、配置≥3块1200W节能交流电源、配置双机虚拟化；配置≥56个万兆光口，配置≥40个千兆光口，配置≥48个千兆电口，所配插卡需要配置三层VxLAN功能 |
| 服务要求 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.3 汇聚交换机

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| 交换架构 | 支持40GE和100GE以太网标准 |
| ▲设备性能要求 | 整机交换容量≥48T，包转发≥12000Mpps |
| 业务插槽数≥4； |
| 接口要求 | 以太网支持千兆电口，千兆光口，万兆光口、万兆电口、40G接口、100G接口 |
| 整机万兆电口密度≥48，提供官网链接证明 |
| 单槽位能够同时提供万兆电口+40G接口/万兆光口+40G接口，提高槽位利用率 |
| 关键部件热插拔 | 电源（N+M冗余）、接口模块、风扇等关键部件可热插拔 |
| 虚拟化 | 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 |
| 支持全面网络虚拟化技术，支持多虚一技术(N:1) |
| 支持Overlay网络虚拟化能力，支持二层、三层VxLAN网关功能 |
| 安全特性 | 支持硬件级加密技术（IEEE802.1ae）介质访问控制安全功能 |
| 设备支持CPU防攻击功能，支持对协议攻击报文的识别和拦截，保证CPU的正常工作 |
| 单台配置要求 | 交流电源：配置≥4块650W节能交流电源 |
| 风扇：配置≥2个 |
| 虚拟化：配置双机虚拟化，单台设备虚拟化接口≥4个40G接口（配置40G虚拟化线缆套件），支持虚拟化接口分布在不同的≥4块物理业务插卡。 |
| 业务接口：配置≥48个万兆光口，配置≥4个40G光口，所配插卡需要配置三层VxLAN功能 |
| 服务要求 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.4 48口接入交换机

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| ▲性能要求 | 交换容量≥336Gbps，包转发率≥132Mpps |
| ▲配置要求 | 提供≥48个千兆电口，≥1个Mircro USB接口，≥4个万兆光口 |
| CPU防护 | 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 |
| 堆叠 | 支持横向，纵向虚拟化 |
| 支持跨设备链路聚合，可将多台设备虚拟化为一台，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） |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF |
| 支持IPv6静态路由、RIPng |
| 支持IPv4和IPv6环境下的策略路由 |
| 防雷 | 为保证设备的可靠性，要求业务端口内置10KV防雷能力 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换 |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| 资质认证 | 提供信产部入网证 |
| 服务要求 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.5 24口接入交换机

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| ▲性能要求 | 交换容量≥336Gbps，包转发率≥96Mpps |
| ▲配置要求 | 提供≥24个千兆电口，≥1个Mircro USB接口，≥4个万兆光口 |
| CPU防护 | 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 |
| 堆叠 | 支持横向，纵向虚拟化 |
| 支持跨设备链路聚合，可将多台设备虚拟化为一台，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） |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF |
| 支持IPv6静态路由、RIPng |
| 支持IPv4和IPv6环境下的策略路由 |
| 防雷 | 为保证设备的可靠性，要求业务端口内置10KV防雷能力 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换 |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| 资质认证 | 提供信产部入网证 |
| 服务要求 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.6 48口POE交换机

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| ▲性能要求 | 交换容量≥336Gbps，包转发率≥166Mpps |
| ▲配置要求 | 提供≥48个千兆电口，≥1个Mircro USB接口，≥4个万兆光口 |
| ▲PoE供电 | 所有电接口均支持PoE及PoE+供电，整机PoE供电功率≥740W |
| CPU防护 | 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 |
| 堆叠 | 支持横向，纵向虚拟化 |
| 支持跨设备链路聚合，可将多台设备虚拟化为一台，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） |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF |
| 支持IPv6静态路由、RIPng |
| 支持IPv4和IPv6环境下的策略路由 |
| 防雷 | 为保证设备的可靠性，要求业务端口内置8KV防雷能力 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换 |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| 资质认证 | 提供信产部入网证 |
| 服务要求 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.7 24口POE交换机

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| ▲性能要求 | 交换容量≥336Gbps，包转发率≥96Mpps |
| ▲配置要求 | 提供≥24个千兆电口，≥1个Mircro USB接口，≥4个万兆光口 |
| ▲PoE供电 | 所有电接口均支持PoE及PoE+供电，整机PoE供电功率≥370W |
| CPU防护 | 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 |
| 堆叠 | 支持横向，纵向虚拟化 |
| 支持跨设备链路聚合，可将多台设备虚拟化为一台，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） |
| VLAN特性 | 支持基于端口的VLAN，支持基于协议的VLAN； |
| 支持基于MAC的VLAN； |
| 路由协议 | 支持IPv4静态路由、RIP V1/V2、OSPF |
| 支持IPv6静态路由、RIPng |
| 支持IPv4和IPv6环境下的策略路由 |
| 防雷 | 为保证设备的可靠性，要求业务端口内置8KV防雷能力 |
| SDN/OPENFLOW | 支持OPENFLOW 1.3标准支持普通模式和Openflow 模式切换 |
| 支持多表流水线 |
| 支持Group table |
| 支持Meter |
| 资质认证 | 提供信产部入网证 |
| 服务要求 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.8 光模块

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| 万兆单模光模块 | 与交换机同一品牌，汇聚和核心互联使用，LC接口，传输距离10KM； |
| 万兆多模光模块 | 与交换机同一品牌，汇聚与接入、服务器互联使用，LC接口，传输距离300m； |
| 千兆单模光模块 | 与交换机同一品牌，汇聚与室外交换机互联使用，LC接口，传输距离10km； |
| 千兆多模光模块 | 与交换机同一品牌，LC接口，传输距离500m； |

### 7.3.9无线控制器

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 可管理的AP数 | 最大管理AP数≥1024，可配置最大AP数≥4096，同时支持802.11a/b/g/n/ac AP的管理 |
| 接口类型 | 千兆光电接口≥8,万兆光接口≥2，管理端口≥1 |
| 配置要求 | 本次配置AP管理数≥512，5m万兆堆叠电缆≥1 |
| 吞吐量≥20Gbps |
| CAPWAP协议 | 支持自动输入AP序列号，支持AC发现（DHCP option43、DNS方式），支持IPv6隧道、时钟同步、jumbo帧发送，AC与AP间支持穿越NAT。 |
| VLAN特性 | 支持4K 可用VLAN，支持基于端口的VLAN，支持基于SSID的VLAN，支持基于用户的VLAN |
| 流量控制功能 | 可以实现流量限制，且限制流量的速率误差小于10%；实现基于源MAC地址进行流分类；实现基于目的MAC地址进行流分类；实现流量整形功能，且速率误差小于10%； |
| IPv6 | 支持IPv4/IPv6双协议栈 |
| 高可用性 | 支持虚拟化或热备，必须配置足够数量的License（含备份）。 |
| 射频管理 | 自动调整功率和信道，故障AP覆盖黑洞补偿，支持基于流量和基于用户数的AP负载分担，支持无线射频干扰监测和规避 |
| 用户访问控制 | 可为远程连接用户提供访问控制，拒绝未通过验证的连接，可以为用户分配不同权限，每个用户只能进行其权限所允许的操作； |
| ACL及QOS | 支持基本ACL、扩展ACL、时间段ACL、基于VLAN的ACL，支持IPv6 ACL，支持速率限制，粒度≤8Kbit/s |
| 安全审计 | 支持安全日志功能，日志内容包括安全事件来源、发生时间、事件描述等；对本地操作日志中对用户登录IP地址、登陆时间、所进行的操作、退出时间进行记录，可以将操作日志输出至日志服务期； |
| 分层AC | 支持一个核心AC下挂多个接入AC，接入AC实现AP接入和数据转发；核心层AC作为接入集中认证点和管理点； |
| 核心层AC对接入层AC以及下属AP统一进行版本管理和配置管理； |
| 垂直备份：接入层AC故障时，核心层AC可起到备份作用； |
| 高可靠：核心层AC和接入层AC之间链路故障时，接入层AC和AP可独立工作； |
| License共享：License安装在核心层AC上，接入层AC无需License； |
| 分级分权管理：核心层AC可进行全局管理工作，接入层AC可进行本地差异化管理工作； |
| 认证点自由选择：可支持核心层AC和接入层AC同时做认证点； |
| 无线漫游 | 支持AC内漫游，支持跨AC间漫游，单AC内漫游时间不超过50ms |
| 备份机制 | AC支持1+1备份、N+1备份、N+N备份三种机制，支持Portal双机热备，1+1备份时，支持100毫秒业务备份 |
| 管理特性 | 支持CLI、SNMP V1/V2/V3，支持WEB管理、SSH管理，有线无线一体化管理，在同一网管视图下可以看到有线、无线设备统一网络拓扑。 |
| 基本功能 | 可以通过管理平台自行开户，实现设备自动上线 |
| 支持分级分权多租户精细化运维管理 |
| 备份认证支持：认证方式支持固定账号认证、portal认证、短信认证 |
| 可实现对无线控制器、无线AP的统一管理，实现网络配置、网络规划、增加设备的操作 |
| 支持终端用户认证类型人数统计，支持终端操作系统识别，支持显示在网终端系统类型统计；支持终端驻留时间统计 |
| 支持第三方应用扩展（数据调用不受被调用端数目限制，也不受被调用端下联设备数目限制），并免费开放对接接口，对第三方平台数据调用响应至少应包含：AC身份信息及工作状态、带宽状况、系统综合健康度、AP在线率、AP关联终端数、区域内无线用户分布情况、AP告警指标信息等 |
| 支持 AP下线，软件升级失败等告警，并支持短信通知或微信通知 |
| 运维功能 | 实配无线运营管理平台一套，平台支持自行开户功能，可实现设备自动上线， |
| 支持分级分权多租户精细化运维管理功能，可实现对无线控制器、无线AP的统一管理，可实现网络配置、网络规划、增加设备的操作， |
| 支持固定账号认证、portal认证、短信认证功能，支持终端用户认证类型人数统计功能，支持终端操作系统识别功能，支持显示在网终端系统类型统计功能；支持终端驻留时间统计功能， |
| 实配 AP下线，软件升级失败等告警功能，支持短信通知或微信通知功能，实配空口资源、负载测量功能，提供无线优化参考数据，对关键链路的实时状态具备智能检测功能，能够智能快速的定位故障点，并支持以多种告警形式通知管理员，以便使网络尽快恢复正常， |
| 服务 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.10 放装AP

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 品牌 | 与无线控制器为同一品牌 |
| 工作模式 | 支持802.11ac Wave2协议，支持MU-MIMO。 |
| 协议支持 | 同时支持802.11a/n/ac/ac Wave2和802.11b/g/n工作 |
| 接口 | ≥2个10/100/1000Mbps(RJ45)，双网口PoE供电，单网口出现故障后，另一网口能保证业务的正常运行。 |
| 天线 | 内置天线 |
| 准入控制 | 从控制用户终端安全接入网络的角度入手，整合网络接入控制与终端安全产品，对接入网络的用户终端强制实施企业安全策略，通过与安全策略服务器的联动，可以对感染病毒或存在系统漏洞等不合格的无线客户端进行下线、隔离、提醒或监控等多种方式的处理，只有无线客户端符合相应的安全策略之后才允许正常访问网络，从而提高了无线网络的整体安全性。 |
| 核准频段 | 802.11a/n/ac : 5.725GHz-5.850GHz (中国) |
| 802.11b/g/n : 2.4GHz-2.483GHz (中国) |
| 负载均衡 | 支持智能负载均衡技术，实现接入用户科学调配，提高资源有效利用和配比。 |
| 供电 | RJ45网线供电或本地电源适配器 |
| 加密 | 支持64、128位WEP加密，WPA，802.11i和WAPI。 |
| 认证 | 配合AC支持： |
| PORTAL认证(远程,外挂服务器)、基于SSID的Portal页面推送、基于AP的Portal页面推送、Portal支持代理功能、Portal双机热备、[EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-MD5、EAP-SIM、LEAP、EAP-FAST、EAP offload (仅支持TLS, PEAP)]、SSID防假冒(用户名与SSID绑定)、LDAP |
| (1. 支持802.1X与Portal接入 |
| 2. 802.1X接入时,支持EAP-GTC和EAP-TLS两种) |
| QoS策略映射 | 支持不同SSID/VLAN映射不同的QoS策略 |
| 智能带宽限速 | 1、基于带宽均分算法 |
| 2、基于每用户指定带宽的算法 |
| 3、在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 服务 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.11 高密AP

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 品牌 | 与无线控制器为同一品牌 |
| 工作模式 | 可支持胖/瘦AP两种工作模式，支持802.11ac Wave2协议，支持MU-MIMO。 |
| 接入能力 | 单个AP同时具备三个射频，一个射频支持2.4GHz频段，一个射频支持5GHz频段，第三个射频可根据终端情况在2.4GHz和5GHz之间可调； |
| 整机能够支持768个用户同时上线， |
| 协议支持 | 同时支持802.11a/n/ac和802.11b/g/n工作 |
| 802.11ac/n/a : 5.725GHz-5.850GHz ; 5.15~5.35GHz (中国) |
| 802.11b/g/n : 2.4GHz-2.483GHz (中国), 2.4GHz/5GHz |
| 协商速率 | 整机协商速率不低于2950Mbps，用于高密度接入场景使用， |
| 接口 | ≥2个10/100/1000Mbps(RJ45) |
| 天线 | 由于AP部署环境复杂，要求为内置天线，提高三防能力 |
| 供电 | PoE+或本地电源适配器，要求双网口可同时进行POE供电， |
| IPv6支持 | 支持IPv4/IPv6双协议栈、Native原生，特别支持IPv6 Portal、IPv6 SAVI |
| 灵活转发 | 支持 |
| 远程探针分析 | 支持作为远程探针分析的Sensor设备，可以对覆盖区内的Wi-Fi报文进行侦听捕获并实时镜像到本地分析设备供网络管理员进行故障排查、优化分析。远程探针分析功能既可以针对工作信道进行无收敛镜像，也可以对所有信道轮询采样，灵活满足无线网络监控运维要求， |
| 负载均衡 | 支持智能负载均衡技术，实现接入用户科学调配，提高资源有效利用和配比。 |
| 性能测试 | 整机接入200用户，同时播放1M码流的视频文件时，视频点播流畅无卡顿， |
| 认证 | 配合AC支持： |
| PORTAL认证(远程,外挂服务器)、基于SSID的Portal页面推送、基于AP的Portal页面推送、Portal支持代理功能、Portal双机热备、[EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-MD5、EAP-SIM、LEAP、EAP-FAST、EAP offload (仅支持TLS, PEAP)]、SSID防假冒(用户名与SSID绑定)、LDAP |
| (1. 支持802.1X与Portal接入 |
| 2. 802.1X接入时,支持EAP-GTC和EAP-TLS两种) |
| QoS策略映射 | 支持不同SSID/VLAN映射不同的QoS策略 |
| 智能带宽限速 | 1、基于带宽均分算法 |
| 2、基于每用户指定带宽的算法 |
| 3、在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 服务 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.12 本体AP

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 品牌 | 与无线控制器为同一品牌 |
| 可管理AP数 | 集中转发模式下单台支持管理下属AP的能力不小于24台 |
| 网络接口 | 千兆电接口不小于24个，万兆光接口不少于4个。 |
| ACL数量 | 不小于2K。 |
| POE供电 | 网络接口支持POE供电，供电端口不少于24个。 |
| SSID | 支持中文SSID |
| 加密方式 | 支持64、128位WEP加密，WPA，802.11i和WAPI。 |
| 服务质量 | 支持用户数负载均衡 |
| 在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 支持不同SSID/VLAN映射不同的QoS策略 |
| 二层支持 | 支持vlan数量不少于4094个 |
| 支持多SSID之间的隔离 |
| 远程探针分析 | 支持作为远程探针分析的Sensor设备，可以对覆盖区内的Wi-Fi报文进行侦听捕获并实时镜像到本地分析设备供网络管理员进行故障排查、优化分析。远程探针分析功能既可以针对工作信道进行无收敛镜像，也可以对所有信道轮询采样，灵活满足无线网络监控运维要求。 |
| 路由支持 | 支持IPv4/IPv6双协议栈、Native原生，特别支持IPv6 Portal、IPv6 SAVI |
| 负载均衡 | 支持智能负载均衡技术，实现接入用户科学调配，提高资源有效利用和配比。 |
| 统一性 | 本次配置的无线物联网系统（无线转发及供电设备+物联网 AP）支持物联网扩展能力，为保证医院部署的灵活性，要求无线转发及供电设备及物联网AP 均可扩展物联网功能，同时必须保证医院病房与病房之间现实无漫游查房 |
| 服务 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.13 分体AP

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 品牌 | 与无线控制器为同一品牌 |
| 工作模式 | 支持802.11ac Wave2协议 |
| 协议支持 | 同时支持802.11a/n/ac和802.11b/g/n工作 |
| 802.11ac/n/a : 5.725GHz-5.850GHz ; 5.15~5.35GHz (中国) |
| 802.11b/g/n : 2.4GHz-2.483GHz (中国), 2.4GHz/5GHz双频段同时工作 |
| 协商速率 | 要求整机最大协商速率≥1167Mbps |
| LAN接口 | ≥4个10/100/1000Mbps(RJ45)下行口（包含1个IOT端口） |
| 1个下行口可做IOT口，外接物联网模块，提供完整的物联网解决方案 |
|  |
| 在设备断电状态下，可传输数据接口≥1个 |
| ≥1个10/100/1000Mbps(RJ45)透传口 |
| WAN接口 | ≥1个10/100/1000Mbps(RJ45) |
| 协商速率 | 5GHz: 866Mbps 2.4GHz: 300Mbps |
| 天线 | 内置低辐射全向天线 |
| 实时频谱防护 | 支持内置射频采集模块，实现深度融合的射频监控和实时频谱防护， |
| IPv6支持 | 支持IPv4/IPv6双协议栈、Native原生，特别支持IPv6 Portal、IPv6 SAVI |
| 远程探针分析 | 支持作为远程探针分析的Sensor设备，可以对覆盖区内的Wi-Fi报文进行侦听捕获并实时镜像到本地分析设备供网络管理员进行故障排查、优化分析。远程探针分析功能既可以针对工作信道进行无收敛镜像，也可以对所有信道轮询采样，灵活满足无线网络监控运维要求。 |
| 灵活转发 | 支持 |
| TR-069动态分支管理 | 支持 |
| 加密 | 支持64、128位WEP加密，WPA，802.11i和WAPI。 |
| 负载均衡 | 支持智能负载均衡技术，实现接入用户科学调配，提高资源有效利用和配比。 |
| 用户隔离 | 支持AP上二层转发抑制 |
| 支持虚拟AP(多SSID)之间的隔离 |
| 报文过滤 | 支持 |
| IPv6 SAVI | 支持 |
| 终端感知准入 | 支持 |
| 实时频谱防护 | 支持 |
| wIPS 探针 | 支持 |
| 广播抑制 | 支持 |
| SSID隐藏 | 支持 |
| 认证 | 配合AC支持： |
| PORTAL认证(远程,外挂服务器)、基于SSID的Portal页面推送、基于AP的Portal页面推送、Portal支持代理功能、Portal双机热备、[EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-MD5、EAP-SIM、LEAP、EAP-FAST、EAP offload (仅支持TLS, PEAP)]、SSID防假冒(用户名与SSID绑定)、LDAP |
| 1. 支持802.1X与Portal接入 |
| 2. 802.1X接入时,支持EAP-GTC和EAP-TLS两种) |
| 智能带宽限速 | 1、基于带宽均分算法 |
| 2、基于每用户指定带宽的算法 |
| 3、在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 型号核准证 | 要求投标产品提供无线管理委员会型号核准证书 |
| 服务 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.14 室外AP

|  |  |
| --- | --- |
| 指标项 | 指标要求 |
| 品牌 | 与无线控制器为同一品牌 |
| 工作模式 | 支持802.11ac Wave2协议，支持MU-MIMO。 |
| 协议支持 | 同时支持802.11a/n/ac/ac Wave2和802.11b/g/n工作 |
| 协商速率 | 5GHz频段867Mbps，2.4GHz频段400Mbps |
| 以太端口 | ≥2个 |
| 物联网扩展 | 要求支持物理网扩展能力，物联网端口个数≥1； |
| 支持对Zigbee、RFID等全制式物联网协议的扩展，根据用户需求定制化相应的业务 |
| 天线 | 内置硬件智能天线 |
| 发射功率(最大) | 27dBm |
| 核准频段 | 802.11a/n/ac : 5.725GHz-5.850GHz (中国) |
| 802.11b/g/n : 2.4GHz-2.483GHz (中国) |
| 防护等级 | IP68 |
| 远程探针分析 | 支持作为远程探针分析的Sensor设备，可以对覆盖区内的Wi-Fi报文进行侦听捕获并实时镜像到本地分析设备供网络管理员进行故障排查、优化分析。远程探针分析功能既可以针对工作信道进行无收敛镜像，也可以对所有信道轮询采样，灵活满足无线网络监控运维要求。 |
| 安全规范 | GB4943、EN60601-1-2(医疗)、UL/CSA 60950-1、EN/IEC 60950-1、EN/IEC 60950-22 |
| MTBF | >250000H |
| IPv6支持 | 支持IPv4/IPv6双协议栈、Native原生，特别支持IPv6 Portal、IPv6 SAVI |
| 认证 | 配合AC支持： |
| PORTAL认证(远程,外挂服务器)、基于SSID的Portal页面推送、基于AP的Portal页面推送、Portal支持代理功能、Portal双机热备、[EAP-TLS、EAP-TTLS、EAP-PEAP、EAP-MD5、EAP-SIM、LEAP、EAP-FAST、EAP offload (仅支持TLS, PEAP)]、SSID防假冒(用户名与SSID绑定)、LDAP |
| (1. 支持802.1X与Portal接入 |
| 2. 802.1X接入时,支持EAP-GTC和EAP-TLS两种) |
| 智能带宽限速 | 1、基于带宽均分算法 |
| 2、基于每用户指定带宽的算法 |
| 3、在流量未拥塞时，确保不同优先级SSID下的报文都可以自由通过；在流量拥塞时，确保每个SSID可以保持各自约定的最小带宽 |
| 服务 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.15 网络管理系统

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| 支持有线无线一体化管理 | 可统一管理AC、Fat/Fit AP、无线终端、PoE交换机等设备，支持在拓扑上支持展示设备告警、状态，可以十分逼真的展示全网的网络结构 |
| 无线位置视图拓扑 | 按照设备所在区域，能够在位置视图中查看AP设备的物理位置 |
| 支持自定义视图并且在视图上显示设备告警和实时状态 | 可以导入背景图，方便管理员按需进行重点设备的重点管理；在拓扑上支持查看AP当前在线Station及详细信息，可以实现设备和用户的统一管理，支持进行Station上线历史记录浏览 |
| 显示AP的RF覆盖范围 | 支持按信号强度、速率和信道显示RF覆盖范围，支持频段及类型（11a/11b/11g/11an/11gn）的显示 |
| 支持带障碍物的RF覆盖显示 | 位置视图中可以添加障碍物，通过不同障碍物的衰减情况，绘制不规则的RF覆盖图形 |
| 支持对移动终端的信息进行查看 | 包括MAC地址、信号强度、发射速率集、RSSI、SSID、使用信道、所在AC设备、所在AP设备等、所在Radio等等。同时可以查看终端的漫游轨迹动画，漫游记录报表。使管理员随时了解最终接入用户的情况，并对其接入轨迹进行审计 |
| 无线网络安全检测 | 支持检测Ad hoc网络、AP MAC地址仿冒、无线客户端MAC地址仿冒、非法信道等威胁，并与消除措施相关联，根据安全事件的严重程度，人工或自动采取反制、忽略、禁用、信任等消除措施 |
| 提供实时安全状态查看 | 按事件类型统计，按检测AP统计，按虚拟安全域统计；实时安全事件查看，历史安全事件回放，事件关联分析；支持对非法设备与终端的定位 |
| 支持蓝牙、微波炉等干扰源的实时检测 | 支持丰富的频谱分析图表，包括实时FFT图，duty cycle图，信道利用率图以及信道质量图等,支持历史频谱数据的保存和回放,支持干扰源位置定位 |
| 支持AP接入端口管理 | 支持PoE功能的设备，可以通过禁止、使能PoE供电功能使AP重启 |
| 绿色节能管理 | 按指定时间控制无线射频的开闭，节约能源，降低辐射；按指定时间控制AP、SSID、PoE的开闭，从而达到控制无线用户上网时间效果 |
| 能耗分析 | 定期采集功耗指标形成报表，分析能耗趋势及节能效果 |
| 无线网络质量评估 | 通过人性化的优化向导设置，建立网络评估任务对无线网络运行状况进行评估，了解WLAN网络运行状况；生成基于拓扑，AP，终端三个维度的网络优化报告，发现薄弱区域，确认需要补点的位置，通过专业报表给未来网络优化提供建议 |
| 智能分析功能 | 无线数据解析功能具备快速非结构化转换结构化的能力，能将无线日志数据及时分词、建立索引、结构化存储。 |
| 用户终端类别识别、统计功能。 |
| 轨迹分析功能。包括历史轨迹查询，实时轨迹呈现、区域主流时间可视化等功能，可以根据电话号码、手机Mac查找特定人物的轨迹， |
| 无线人群统计分析功能。能够识别无线人群，并能统计分析，查询人群轨迹。 |
| 定位引擎及数据分析:数据分析平台后台系统，支持TB数据级别的定位数据分析。 |
| 支持监控并记录各区域接入网络的终端数量 |
| 根据用户提供的规则，建立人流密度预警机制 |
| 基于位置数据分析公共资源使用情况。 |
| 提供无线实时统计功能。 |
| 提供外部消息分发接口以支持用户通过外部APP查询公共区域实时人员密度 |
| 基于用户提供的规则（如：7日未连接WIFI等）过滤出特征用户 |
| 授权配置 | 配置≥1000个无线设备管理授权，支持≥2000个终端在线认证 |
| 服务 | 电源、相关缆线及上机柜的配套设备必须齐全并满足机房实际布局连接要求，在售后服务期内，电话响应、现场支持、故障备件更换都不予另行收费。 |

### 7.3.16 互联网出口下一代防火墙

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| **基本要求** | 操作系统 | 要求采用先进的多核网络专用架构多核硬件平台，x86多核处理器，非MIPS的多核架构或ASIC架构；安全操作系统采用冗余设计，系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合IOS9001标准，提供相关证明； |
| **系统性能** | 系统配置 | 1U机架式机型，标配6个10/100/1000MBase-T端口，4个SFP扩展插槽，4个SFP光模块；1TB硬盘。模块化冗余电源；整机吞吐率：>12Gbps；应用层吞吐率：4Gbps；最大并发连接数：>400W，配置IPS攻击规则特征库三年许可； |
| **网络**  **接入** | 工作模式 | 支持路由、交换、混合、工作模式； |
| 路由交换 | 支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式； |
| 支持基于源/目的地址、源/目的端口、用户、应用的策略路由； |
| 接入功能 | 支持GRE与IPSEC VPN接入；IPSEC VPN可提供国密算法；（提供软件截图） |
| 链路聚合 | 提供不少于11种的负载分担算法，灵活实现对聚合组内业务流量的负载分担（提供软件截图） |
| 地址转换 | 支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式；支持Sticky NAT开关，使相同源IP的数据包经过地址转换后为其转换的源 IP 地址相同； |
| 智能DNS | 支持智能DNS及DNS Docting功能 |
| **IPv6** | 双栈模式 | 支持IPv4/IPv6双栈工作模式； |
| 访问控制 | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； |
| 安全防护 | 支持基于IPv6的应用层检测（FTP\TFTP）、病毒过滤、URL过滤、ADS、IPS检测； |
| **虚拟系统** | 资源虚拟化 | 支持在一台物理设备上划分出最大4000个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源； |
| 功能虚拟化 | 支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、异常行为分析、病毒过滤、内容过滤、审计、报表等安全功能虚拟化； |
| **用户管控** | 认证方式 | 内置强大的用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持RADIUS、LDAP、TACACS等多种第三方外部认证设置； |
| 用户管控 | 综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控； |
| **应用管控** | 应用识别 | 内置独立应用识别特征库，总数2100种以上，支持应用特征库在线或本地更新，支持应用特征自定义； |
| 带宽管理 | 支持基于IP/IP组、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略； |
| 连接控制 | 支持对单条访问控制策略进行最大并发连接数限制； |
| 为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的IP地址、MAC地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个IP每秒新建连接限制、单个IP连接数限制及连接总数限制； |
| 支持监控功能，显示最近被拦截的IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制； |
| **访问控制** | 一体化访问控制 | 内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名等的识别与控制； |
| 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址； |
| 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在WEB界面显示检测结果； |
| 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等； |
| **安全防护** | 未知威胁防御 | 支持APT防御扩展，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day漏洞）、木马、病毒具有检测能力；可根据用户环境，将APT工作模式设置为深度模式或者智能模式； |
| 支持异常行为检测，如存在异常则报警。 |
| 入侵防御 | 内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持web攻击识别和防护，如跨站脚本攻击、SQL注入攻击；支持攻击特征库，同时支持自定义特征库。 |
| DDOS防御 | 支持基于IP协议的检测清洗； |
| 支持基于TCP协议的检测清洗； |
| 支持基于UDP协议的检测清洗，包括对源、目的限速，对UDP最大及最小报文限制；同时支持UDP关联认证，要求所有去往服务器的UDP报文，必须首先与该服务器的TCP端口建立TCP连接，对源地址进行合法性认证； |
| 支持基于DNS协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒攻击、DNS格式检查、DNS NX异常比率检测等；支持DNS QUERY源认证、DNS REPLY源认证； |
| 支持基于HTTP协议的检测清洗，支持对HTTP slow-header和HTTP slow-post设置最大传输时间以及异常会话数阈值，有效防御慢速攻击； |
| 支持根据DOS/DDOS攻击行为自动添加动态黑/白名单功能； |
| 文件过滤 | 内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM文件传输等应用类型以及HTTP/FTP/SMTP/POP3等标准协议进行检测，识别可执行文件、office文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过40种文档类型的文件过滤； |
| 内容过滤 | 支持基于http、ftp、telnet、smtp、pop3等协议的内容过滤策略，支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤； |
| 敏感数据泄漏防护 | 内置DLP数据防泄漏引擎，对数据进行监控识别，达到敏感数据防护目的。支持识别的文件类型数量不少于1000种；文件内容识格式不少于300种。  支持多种加密和压缩文件格式，如RAR、ZIP、GZ、TAR等；支持识别Linux，Unix等非Winodws的文件类型；支持识别异常文件格式类型；支持识别自定义文件类型； |
| 配置维护 | 支持多个配置文件并存，配置文件数量不少于20个； |
| 升级维护 | 支持多个系统升级包并存，系统升级包文件数量不少于5个 |
| 管理员 | 支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置（提供软件截图） |
| **数据中心** | 审计 | 支持独立配置审计策略，同时也可将指定的 IP 地址、 URL、应用加入白名单，不进行数据审计； |
| 日志 | 支持日志本地存储，可对不同类型日志设置存储空间；  支持外发至SYSLOG服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密，设定8位的加密密钥； |
| 日志查看可划分为管理日志、系统日志、策略日志、应用行为日志等四大模块，可将日志按照CSV或XML格式导出； |
| **显示监控** | 资源监控 | 在WEB界面提供资源监控开关，可对cpu占用率、内存占用率、磁盘占用率设置阈值； |
| 流量统计 | 支持根据应用对通过设备的数据报文流量进行统计； |
| 支持根据用户/用户组对通过设备的数据报文流量进行统计； |
| 支持根据服务器对通过设备的数据报文流量进行统计； |
| 威胁统计 | 支持根据按照病毒防御、入侵防御、APT防御、ADS攻击进行威胁统计，可按照威胁类型/攻击者/受害者等类似威胁排名， |
| **其他** | 服务要求 | （1）提供专业工程师进行施工、安装，其中施工安装费已包括在本次采购项目中；  （2）提供用户现场培训服务，保证用户运维人员能够日常维护和故障处理，同时提供完整的实施和维护文档； |

### 7.3.17 互联网上网行为管理

|  |  |
| --- | --- |
| 指标项 | 技术指标要求 |
| 吞吐量 | ≥1Gbps |
| 并发会话数 | ≥300000 |
| 用户规模 | ≥4000人 |
| 设备接口 | 4个千兆电口 4个千兆光口 |
| 硬盘 | ≥1TB |
| 尺寸要求 | 标准机架架构 |
| BYPASS | 支持 |
| 设备架构 | 设备必须为多核X86架构，以保证软件库的灵活更新与升级。 |
| 部署方式 | 要求设备支持网关模式，支持NAT、路由转发、DHCP、GRE、OSPF等功能；支持网桥模式，以透明方式串接在网络中；支持两台及两台以上设备同时做主机的部署模式，支持基于虚拟化平台的软件版本，支持的虚拟平台包括：VMware、深信服虚拟化等。 |
| IPv6支持 | 支持IPv6 |
| IPSEC VPN功能 | 要求设备支持IPSEC VPN远程安全接入维护，能提供IPsec VPN客户端授权远程接入访问； |
| 链路负载 | 要求支持多种方式进行多链路负载，支持使用VPN专线备份。 |
| 业务需要 | 为减少短信费用投入，要求设备支持微信身份验证，用户可以通过微信“扫一扫”、关注公众号等操作获取上网权限，后台能够记录下用户微信的ID，支持与第三方微信平台对接，无需修改第三方平台代码。 |
| 为满足访客PC的简易接入授权，访客终端接入无线网络后，终端自动弹出二维码页面，审核人通过手机扫描访客终端二维码，添加备注信息，访客即可完成上网，同时设备记录访客备注信息、接入终端MAC以及审核人帐号。（提供产品配置界面截图） |
| 支持认证页面分权分域管理。启用后，普通管理员只能看到自己有权限的页面，其他管理员页面不可见。系统管理员可以将某个页面授权给指定的普通管理员管理。 |
| ▲为加强对我单位员工私接无线上网的行为管理，要求设备能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，匹配管理员配置的热点信任列表，对信任列表外非法接入的热点和终端能够进行阻止上网，支持冻结用户IP，并通过邮件形式告警通知管理员，支持显示以IP或用户名的维度统计一段时间内的趋势图。 |
| 要求设备必须能够识别并过滤SSL加密的钓鱼网站、金融购物网站；识别和审计加密的邮箱等。 |
| 应用识别规则库 | 目前互联网应用种类较多，为了降低管理员配置应用管理策略的难度，要求设备能够按照管控需求对应用进行标签化管理，应用标签至少默认包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类，此外可根据我单位需求自定义标签，根据标签做应用控制。 |
| 应用控制 | 1. 设备内置应用识别规则库，支持超过4700条应用规则数，支持超过2100种以上的应用，660种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率； 2. 支持根据应用的特征智能识别新更新的应用； 3. 支持根据IP、端口、协议等自定义应用规则；   支持根据不同的应用类型或具体的某种应用设置允许或拒绝； |
| 移动应用的细分控制 | 支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏。移动QQ：QQ传文件、QQ视频语音等。 |
| URL访问及关键字控制 | 要求设备内置海量的URL地址库，可根据访问URL的网页关键字进行过滤控制，特别对于SSL加密的网页、论坛、BBS上的发帖行为也需要支持关键字过滤控制 |
| 流控黑名单 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中。 |
| 上网流速提醒 | 用户指定应用上网流速超过预设阈值后，网关自动提醒该用户； |
| 动态流控 | 要求设备可以针对整体线路或者某流量通道内流量情况进行实时监控，根据设定的流量空闲值自动的调整流控控制策略，提升我单位带宽使用率（提供产品配置界面证明） |
| P2P智能流控 | 要求设备有效抑制如迅雷、ppstream等P2P应用带宽，通过抑制可看到出口上下行带宽的明显改善。 |
| 多维度权限控制 | 要求设备可以根据员工的所在位置以及所使用终端配置不同的上网策略和流控策略，做到更精细化权限管理。 |
| 移动APP审计 | 支持常见论坛（天涯社区、猫扑社区、百度贴吧、新浪论坛、搜狐社区等  ）、微博（新浪）、新闻评论类（腾讯新闻、网易新闻、搜狐新闻、新浪新闻）的移动APP内容审计 |
| IM审计 | 支持对QQ（客户端版本）、阿里旺旺、万德（Wind）、路透等应用的聊天，群聊天等内容的审计。 |
| 邮件审计 | 支持对加密HTTPS、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电邮客户端的邮件进行关键字过滤 |
| 加密证书自动分发 | 审计SSL网页时，支持加密证书自动分发功能，用户点击网页上的工具即可一次性安装完成。解决管理员给每台PC单独安装证书的问题 |
| 关键字订阅 | 支持预置几组关键字，当审计日志中出现这些关键字时，将定期以邮件的方式发送报告给指定邮箱 |
| 网络整体状况报表 | 从带宽健康分析、工作效率分析、离职风险分析、合规性分析四个大块对网络整体状况进行说明 |
| 下钻查询 | 在流量时长分析、用户行为分析、终端接入分析等纬度相关页面支持对统计结果的向下钻取查询 |
| 特权用户 | 支持针对特权用户配置免认证key、免控制key |
| 数据中心 | 要求设备必须支持将审计数据备份到外置数据中心，实现海量存储；必须支持通过USBKEY方式对数据中心管理员进行身份验证，确保我单位核心数据不会外泄 |
| 投标产品资质要求 | 中国信息安全测评中心《信息技术产品安全测评证书EAL3级》 |
| 具有工信部颁发的《电信设备进网许可证》 |
| 服务要求 | 支持系统、应用协议库、URL地址库的在线自动升级；提供三年免费URL及应用识别规则库升级；协议库每二周至少能升级一次，客户发现有不能封堵的应用，厂商应在一周内完成协议库更新并解决问题。 |
| 应提供7×24小时现场技术支持及产品备机，1小时内响应，4小时内到达现场，24小时内不能解决问题应提供备机。 |

### 7.3.18 外联区域安全防火墙

|  |  |  |
| --- | --- | --- |
| 指标项 | | 指标要求 |
| **基本要求** | 操作系统 | 要求采用先进的多核网络专用架构多核硬件平台，x86多核处理器，非MIPS的多核架构或ASIC架构；安全操作系统采用冗余设计，系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合ios9001标准，提供相关证明； |
| **系统性能** | 系统配置 | 机架式机型，标配6个10/100/1000MBase-T端口，4个SFP扩展插槽，4个SFP光模块；1TB硬盘。模块化冗余电源；整机吞吐率：>12Gbps；应用层吞吐率：4Gbps；最大并发连接数：>400W，配置IPS攻击规则特征库三年许可； |
| **网络**  **接入** | 工作模式 | 支持路由、交换、混合、工作模式； |
| 路由交换 | 支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式； |
| 支持基于源/目的地址、源/目的端口、用户、应用的策略路由； |
| 接入功能 | 支持GRE与IPSEC VPN接入；IPSEC VPN可提供国密算法； |
| 链路聚合 | 提供不少于11种的负载分担算法，灵活实现对聚合组内业务流量的负载分担 |
| 地址转换 | 支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式；支持Sticky NAT开关，使相同源IP的数据包经过地址转换后为其转换的源 IP 地址相同； |
| 智能DNS | 支持智能DNS及DNS Docting功能 |
| **IPv6** | 双栈模式 | 支持IPv4/IPv6双栈工作模式； |
| 访问控制 | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； |
| 安全防护 | 支持基于IPv6的应用层检测（FTP\TFTP）、病毒过滤、URL过滤、ADS、IPS检测； |
| **虚拟系统** | 资源虚拟化 | 支持在一台物理设备上划分出最大4000个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源； |
| 功能虚拟化 | 支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、异常行为分析、病毒过滤、内容过滤、审计、报表等安全功能虚拟化； |
| **用户管控** | 认证方式 | 内置强大的用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持RADIUS、LDAP、TACACS等多种第三方外部认证设置； |
| 用户管控 | 综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控；支持创建用户； |
| **应用管控** | 应用识别 | 内置独立应用识别特征库，总数2100种以上，支持应用特征库在线或本地更新，支持应用特征自定义； |
| 带宽管理 | 支持基于IP/IP组、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略； |
| 连接控制 | 支持对单条访问控制策略进行最大并发连接数限制； |
| 为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的IP地址、MAC地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个IP每秒新建连接限制、单个IP连接数限制及连接总数限制； |
| 支持监控功能，显示最近被拦截的IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制； |
| **访问控制** | 一体化访问控制 | 内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户、域名等的识别与控制； |
| 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址； |
| 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在WEB界面显示检测结果； |
| 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等； |
| **安全防护** | 未知威胁防御 | 支持APT防御扩展，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day漏洞）、木马、病毒具有检测能力；可根据用户环境，将APT工作模式设置为深度模式或者智能模式； |
| 支持异常行为检测，如存在异常则报警。 |
| 入侵防御 | 内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持web攻击识别和防护，如跨站脚本攻击、SQL注入攻击；支持攻击特征库，同时支持自定义特征库。 |
| DDOS防御 | 支持基于IP协议的检测清洗； |
| 支持基于TCP协议的检测清洗； |
| 支持基于UDP协议的检测清洗，包括对源、目的限速，对UDP最大及最小报文限制；同时支持UDP关联认证，要求所有去往服务器的UDP报文，必须首先与该服务器的TCP端口建立TCP连接，对源地址进行合法性认证； |
| 支持基于DNS协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒攻击、DNS格式检查、DNS NX异常比率检测等；支持DNS QUERY源认证、DNS REPLY源认证； |
| 支持基于HTTP协议的检测清洗，支持对HTTP slow-header和HTTP slow-post设置最大传输时间以及异常会话数阈值，有效防御慢速攻击； |
| 支持根据DOS/DDOS攻击行为自动添加动态黑/白名单功能， |
| 文件过滤 | 内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM文件传输等应用类型以及HTTP/FTP/SMTP/POP3等标准协议进行检测，识别可执行文件、office文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过40种文档类型的文件过滤； |
| 内容过滤 | 支持基于http、ftp、telnet、smtp、pop3等协议的内容过滤策略，支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤； |
| 敏感数据泄漏防护 | 内置DLP数据防泄漏引擎，对数据进行监控识别，达到敏感数据防护目的。支持识别的文件类型数量不少于1000种；文件内容识格式不少于300种。  支持多种加密和压缩文件格式，如RAR、ZIP、GZ、TAR等；支持识别Linux，Unix等非Winodws的文件类型；支持识别异常文件格式类型；支持识别自定义文件类型； |
| 配置维护 | 支持多个配置文件并存，配置文件数量不少于20个； |
| 升级维护 | 支持多个系统升级包并存，系统升级包文件数量不少于5个； |
| 管理员 | 支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置 |
| **数据中心** | 审计 | 支持独立配置审计策略，同时也可将指定的 IP 地址、 URL、应用加入白名单，不进行数据审计； |
| 日志 | 支持日志本地存储，可对不同类型日志设置存储空间；  支持外发至SYSLOG服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密，设定8位的加密密钥； |
| 日志查看可划分为管理日志、系统日志、策略日志、应用行为日志等四大模块，可将日志按照CSV或XML格式导出； |
| **显示监控** | 资源监控 | 在WEB界面提供资源监控开关，可对cpu占用率、内存占用率、磁盘占用率设置阈值； |
| 流量统计 | 支持根据应用对通过设备的数据报文流量进行统计； |
| 支持根据用户/用户组对通过设备的数据报文流量进行统计； |
| 支持根据服务器对通过设备的数据报文流量进行统计； |
| 威胁统计 | 支持根据按照病毒防御、入侵防御、APT防御、ADS攻击进行威胁统计，可按照威胁类型/攻击者/受害者等类似威胁排名， |
| **其他** | ▲服务要求 | （1）提供专业工程师进行施工、安装，其中施工安装费已包括在本次采购项目中；  （2）提供用户现场培训服务，保证用户运维人员能够日常维护和故障处理，同时提供完整的实施和维护文档； |

### 7.3.19 防病毒软件

|  |  |  |
| --- | --- | --- |
| **指标项** | | **技术参数要求** |
| 软件效能 | 最少支持客户端数 | 1000个客户端授权，50服务器端 |
| 功能 | 具备Web信誉评估功能 | 包含HTTPS通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新。 |
| 支持两种扫描运行方式 | 支持云安全扫描和传统病毒码扫描两种运行方式。 |
| 支持与微软AD的集成 | 可套用AD的分组方式，方便管理 |
| 支持对各种外设使用权限进行控制 | 支持对USB、软驱、光驱、网络共享的使用权限进行控制 |
| 支持对COM／LPT端口、IEEE 1394 接口、图像处理设备、红外设备、调制解调器、PCMCIA 卡、打印影屏幕键的使用权限进行控制 |
| 自动识别客户端类型 | 自动识别客户端运行环境于物理终端或虚拟终端，从而提供更好的防护目标 |
| 客户端支持多种操作系统类型 | 客户端要能够支持Windows Embedded POSReady 2009、Windows Embedded Enterprise（Windows 7、Vista 和 XP 版本）、Windows Server Core 2008。支持扩展对主流的智能终端设备的安全防护和管理，支持的智能终端类型包括但不限于：iOS 4.0＋、Android 2.1＋、Windows Mobile 5.0, 6.0~6.5、Symbian 和 RIM Blackberry；需要提供软件功能设置界面截图证明 |
| 具备个人防火墙功能 | 可对多种协议数据包进行阻挡，可对网络中异常浏览进行监控 |
| 客户端集成“病毒专杀”工具 | 不需要人工辅助，“病毒专杀”工具必须支持目前最流行的新型态病毒。管理控制台可以直接控制实现客户端恢复动作 |
| 客户端对“预设扫描”的控制权限 | 比如延迟扫描、跳过扫描、停止扫描等 |
| 具备远程病毒集中清除功能 | 可对网络中感染病毒的计算机进行远程自动清除，无需知道计算机的物理位置，无需到客户端逐一清除病毒 |
| 智能型扫描机制 | 能够以文件真正格式作扫描，通过文件头的真实信息而不是简单的通过文件扩展名来识别文件的类型，以提高扫描效率 |
| 支持智能式的处理方式 | 根据不同的病毒类型，采取不同的处理策略 |
| 支持网络病毒识别码 | 网络病毒识别码与传统的病毒代码不同，网络病毒识别码能够识别网络病毒攻击行为。在客户端实现网络病毒的封包过滤 |
| 具备病毒源准确定位功能 | 具备病毒源准确定位功能，快速查获病毒 |
| 多种方式部署客户端 | 必须支持WEB安装方式、SMS安装方式、MSI程序打包安装方式、共享安装等 |
| 提供密码保护功能 | 客户端产品防毒服务关闭和产品卸载均需提供密码保护功能，预防防毒系统漏洞的出现 |
| 支持对客户端进行逻辑分组 | 对不同的客户端实行不同的防毒管理策略 |
| 具备数据资产控制 | 定义要保护的数据资产（正规表达式、关键字、文档属性） |
|  | 创建用于限制或机密阻止通过网络通道（Email、FTP、HTTP、HTTPS、IM、SMB、Webmail）以及系统通道（数据记录器、对等应用程序、PGP加密、打印机、可移动储存、同步软件、剪贴板）传输数据资产的策略 |
|  | 按照以建立的标准强制执行合规 |
| 支持制定化仪表盘 | 管理控制台具备集于小组件平台架构（Widget Framework）的定制化仪表盘，可让管理员弹性定制专属的管理介面，体现高效管控及提高可视性。 |
| APT防护 | 以云扫描服务企集成 C&C 黑名单的通讯侦测与阻挡. 双名单源从智能防护云与本地沙箱 (TDA) 分析产生的黑名单. |
| 以数据统计技术计算威胁普遍率, 侦测独一应用时 (高可能性是针对性攻击)实时通知用户. |
| 管理架构可与中央控制台  集成 | 统一管理软件即服务的终端安全 |
| 部署与管理 | 硬件性能标示 | 硬件性能CPU,内存使用情况 |
| 部署 | 支持虚拟机和物理机部署 |
| 管理 | 基于B/S的管理架构， Web界面支持 MS IE、Netscape、Firefox、Opera四大浏览器 |
| 提供CLI（命令行）配置模式 |
| 提供SSH远程调试模式 |
| 语言支持 | 支持中文与英文管理画面 |
| 升级 | 升级方式 | 支持实时在线升级、自动在线升级、手工升级多种升级方式 |
| 更新源 | 全球升级架构以及本地升级源的设计降低升级带宽使用 |
| 设备本身安全 | 安全性 | 通过强加密的SSL安全通道进行通讯 |
| 日志管理 | 日志类型 | 支持SYSlog/SNMP 协议 |
| 系统日志 |
| 网络病毒日志 |
| 备份复原 | 备份 | 系统提供备份功能与备份配置 |
| 复原 | 产品包装包含救援U盘,快速回复系统 |
| 厂商增强资质 | 产品获国家公安部销售许可证。(提供证明材料) | |
| 所有产品必须是自主开发，拥有自主知识产权。(提供证明材料) | |

### 7.3.20 日志审计系统

|  |  |
| --- | --- |
| **技术指标** | **技术指标要求** |
| 产品资质 | 通过公安部检测并获得公安部计算机信息系统安全专用产品销售许可证 |
| 工作模式 | 独立完成审计日志采集，不依赖于设备或系统自身的日志系统； |
| 审计工作不影响被审计对象的性能、稳定性或日常管理流程； |
| 审计结果存储于独立存储空间； |
| 自身用户管理与设备或主机的管理、使用、权限无关联； |
| 提供全中文WEB管理界面，无需安装任意客户端软件或插件 |
| 硬件规格 | 机架式设备，交流供电 |
| 4个工作口，2个管理口 |
| 处理性能 | 支持审计100个日志源； |
| 平均处理能力（每秒日志解析能力EPS）：4000EPS； |
| 峰值处理能力（每秒日志解析能力EPS）：5000EPS。 |
| 功能扩展 | 采用解决方案包上传对产品进行功能扩展，无需要代码开发。 |
| 日志收集 | 支持Syslog、SNMP Trap、OPSec、FTP协议日志收集 |
| 支持使用代理(Agent)方式提取日志并收集； |
| 支持目前主流的网络安全设备、交换设备、路由设备、操作系统、应用系统等； |
| 设备厂家包括但不限于本次投标产品厂家。 |
| 支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等 |
| 日志分析 | 可以以日志等级进行过滤； |
| 应该可以通过自定义配置将用户不关心的日志过滤掉； |
| 支持对收集到的重复的日志进行自动的聚合归并，减少日志量； |
| 支持可由用户定义和修改的日志的聚合归并逻辑规则; |
| 支持将收集到的日志转发，当原始日志设备无法设置多个日志服务器时，可以通过本系统的日志转发功能将日志转发到其他日志存储设备； |
| 支持对收集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展。 |
| 可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息（公网情况） |
| 支持基于内存的实时关联分析，跨设备的多事件关联分析； |
| 支持自定义条件都事件进行聚合； |
| 进行关联分析的规则可定制； |
| 关联分析功能:系统须具备一个安全知识库和包含资产信息的弱点库，当接收到指定资产并且匹配到弱点库中指定漏洞的攻击时，须触发与安全知识库、弱点库的关联，新增新的事件，并且提高威胁等级。需提供第三方权威测评机构。 |
| 日志备份 | 可设置日志存储备份策略。包括系统日志保存期（天）、磁盘使用率百分比； |
| 支持日志备份自动传送到远程服务器； |
| 日志查询 | 支持B/S模式管理，支持SSL加密模式访问； |
| 支持按日期、时间、设备类型、日志类型、日志来源、威胁值、源地址、目的地址、事件类型、时间范围、操作对象、技术方式、技术动作、技术效果、攻击类型、地理城市等参数进行过滤查询； |
| 支持用任意关键字对所有事件进行高性能全文检索 |
| 支持可指定多个查询条件进行组合查询 |
| 支持将查询的条件存储为查询模版，方便再次使用 |
| 极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件，在秒级里返回查询结果。 |
| 应用性能监控 | 性能监控：通过在目标主机上安装agent程序，支持监控目标主机的CPU利用率、内存使用率、磁盘使用情况、流量等信息，并支持设置报警阈值。 |
| （APM） | 支持如下应用的性能监控（Windows、Linux、Aix、FeeBSD、HP-UX/Tru64、Max OS、Sun Solaris）、数据库（mysql、oracle）、应用服务器（weblogic、tomcat）、web服务器（apache）。 |
| 支持应用性能历史详情回溯查看 |
| 支持如下性能监控参数 |
| 支持监控Windows操作系统如下参数：cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数； |
| 支持监控Linux操作系统如下参数：一分钟系统负载、5分钟系统负载、15分钟系统负载、cpu使用率、内存使用率、磁盘使用率、网络发送流量、网络接收流量、网络发送接收总流量、交换区使用率、磁盘总使用率、进程数、线程数 |
| 支持监控Mysql如下参数：查询缓存命中率、键缓存命中率、立即获得锁数、连接数、线程数、每秒SQL查询数、每秒发送字节、每秒接收字节； |
| 支持监控Oracle如下参数：库缓存命中率、内存排序比率、词典缓存命中率、SGA数据缓存命中率、重做日志缓存命中率； |
| 支持监控Apache如下参数：总访问数、写日志次数、每秒发送字节数、长连接数、关闭连接数、空闲活动数、查询DNS数、正在发送数、请求完成数、负载、等待连接数、总数据量、读操作数、工作线程数、空闲线程数、CPU占用率 |
| 支持监控应用服务器（tomcat、weblogic）如下参数：活动线程数、堆内存（已用）、守护线程数； |
| 脆弱性管理 | 弱点管理：支持导入主流扫描器的扫描报告，可进行统一检索，并支持计算威胁等级。 |
| 内置73000+条CVE漏洞数据知识库 |
| 内置数十项符合OWASP的Web漏洞数据知识库 |
| 地理安全系统 | 内置GeoSec地理安全子系统，内置世界以及中国安全GIS地图 |
| 支持用地理地图展示来源威胁的趋势 |
| 支持用地理地图展示目的威胁的趋势 |
| 支持在地理地图上标注威胁事件的发生分布 |
| 内置IP地址到经纬度的转换库 |
| 支持以地理信息类进行统计的数据报表 |
| 支持切换Google地图（需要连通互联网） |
| 告警功能 | 可预设置安全告警策略； |
| 支持数据阀值设置，超过阀值将产生告警; |
| 可以通过邮件、短信和屏幕显示进行告警； |
| 支持自动防止报警信息在短时间内大量发送(告警抑制)； |
| 具备报警合并和在一个时间段内抑制报警次数的能力。 |
| 综合查询及报表管理 | 内置合规性报表1000+种； |
| 内置SOX、ISO27001、WEB安全等解决方案包 |
| 内置完善的等级保护合规报表 |
| 内置综合性自动化审计报告 |
| 支持用户自定义报表； |
| 自定义的报表支持多个统计维度的数据集合。 |
| 数据报表支持数据趋势预测功能，根据历史规律数据对未来数据的发展趋势进行预测 |
| 报表支持详单数据钻取 |
| 支持报表导出为PDF和Word格式文件。 |
| 用户管理 | 根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，审计员只负责查看相关的审计结果及告警内容；日志员只负责完成对系统本身的用户操作日志管理。 |
| 系统自带自身管理日志 |
| 注册用户资产时，提供自动发现识别能力。 |
| 提供一键式故障排除功能。 |
| 提供自助式的升级接口，支持对产品升级、规则升级。 |
| 部署方式 | 支持分布式部署； |
| 支持集中式管理和升级模式； |
| 支持分级管理模式； |
| 采用B/S架构操作方式，无需客户端安装。 |
| 支持监控设备自身CPU、内存、磁盘等工作运行状况 |

### 7.3.21 桌面管理系统

|  |  |  |
| --- | --- | --- |
| **指标项** | | **功能描述** |
| 系统性能及要求 | 基础要求 | 具有独立的自主知识产权的一体式机架结构硬件产品，不接受PC SERVER系统架构。 |
| 支持多级级联架构，满足分级管理要求。 |
| 硬件指标 | 1U机架结构；单电源；标准配置6个1000MBASE-T接口；每秒事务数（TPS）：≥1000（次/秒），最大吞吐量：≥1Gbps，最大并发连接数：2000（条）； |
| 高可用性 | 必须具备HA模式，HA须支持主备机心跳IP检测及虚地址管理模式。 |
| 提供第三方监控平台，在出现重大异常情况时能及时通知网络设备放开网络。 |
| 网络准入 | 强制技术 | 支持基于策略路由技术的准入控制模式，入网设备在访问网内关键资源时，将被强制隔离、引导至认证管理页面。 |
| 可支持端口镜像准入技术，通过对交换机镜像数据的实时分析，能够及时发现并阻断非授权终端的接入。 |
| 单台准入设备可支持至少2个核心交换机进行策略路由准入控制。 |
| 定向引导 | 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导。 |
| 可根据用户的实际环境自定义非80端口的Web服务端口号及用户重定向引导。 |
| 能通过浏览器完成身份认证、客户端安装、设备注册、安全检查、检查结果展现等全流程引导管理。 |
| 资产管理 | 设备发现 | 自动发现接入网络的所有网络设备、PC和其他IP设备。 |
| 发现内网私接的Hub、傻瓜交换机等非网管设备，当多台计算机通过Hub接入网络时，能够及时产生告警通知管理员。 |
| 支持混合厂商大规模网络环境，支持跨越路由器、防火墙等复杂环境。 |
| 资产采集 | 自动采集各计算机的IP地址、计算机名、MAC地址、网卡型号和生产厂商、计算机所在域、操作系统、主要硬件、软件信息。 |
| 提供计算机信息综合查询报表。 |
| 硬件资产 | 能够对终端硬件初始记录、最新记录和变动记录形成报表，支持对硬件变动进行报警，并且能够查询变动的历史。 |
| 软件资产 | 支持对软件资产进行实时统计，能够灵活指定必须使用的软件资产和禁止安装的软件资产，支持对软件变动进行报警，并且能够查询变动的历史。 |
| IP地址资产 | 可通过矩阵图的方式自动进行网内IP地址池的展示。 |
| 可通过颜色不同标识出该IP的状态：未分配、开机、关机。 |
| IP使用历史记录：设备名称、设备IP、上线时间、离线时间、运行时长。 |
| 软件使用管理 | 支持以软件为单位，审计使用的时间和次数。 |
| 支持以软件为单位，限制软件的打开和使用。 |
| 系统安全 | Windows安全登录 | 可以与用户已有认证系统（UKey、LDAP等）相结合实现Windows系统安全登录与身份认证（替代Windows本地用户/密码认证模式）。 |
| 杀毒软件 | 支持至少18种杀毒软件的检查。 |
| 区分版本不合规、病毒库不合规，提供自动下载程序修复和网址引导修复。 |
| 系统配置安全 | 建立终端设备的安全性评估任务，支持对帐户密码安全性、屏保设置、共享安全、系统服务、进程及服务等项目进行检查、评定，对存在安全风险的终端支持实时自动修复。 |
| 支持终端安全状况图形化展示，能够显示每台终端的详细风险信息并提供评估得分的统计报表。 |
| 应用安全 | 重要进程管理 | 能够统计网内运行的所有进程，支持设置黑白名单指定禁止或允许的进程，支持进程MD5值识别方式，防止更改或伪造进程。 |
| 异常进程监控 | 能够设定进程运行的环境阀值，包括cpu占用率、内存占用率、tcp连接数、tcp监听端口数、I/O读写字节数、进程名长度和特殊字符、进程运行次数等，对超过阀值的异常进程进行报警等处理。 |
| 私设网站检查 | 可设置终端主动进行网段内私设WEB站点的扫描。 |
| 可扫描浏览器是否有上网的历史记录。 |
| 私设代理控制 | 管理员可设置策略禁止终端设置代理。 |
| 管理员可为被管控终端在管理系统后台设置指定代理、端口号，终端用户无感知。 |
| 流量控制检查 | 可对上传、下载流量、总流量、发包频率、TCP连接数、UDP监听端口数进行控制。 |
| 软件黑白名单 | 支持对终端应用进行控制管理，支持建立软件黑名单和白名单，强制终端只能在管理策略允许的范围内安装应用。 |
| 软件分发 | 支持可执行程序、MSI安装包或者文档数据文件自动下发与安装。 |
| 支持指定组范围、指定时间进行安装并提供程序打包工具。 |
| 自动统计分发成功率及软件安装成功率，支持进程、注册表、安装路径等多种参数判断方式。 |
| 远程维护 | 远程协助方式 | 管理员计算机与被管理计算机采用专用tcp端口进行直接连接，远程协助时不占用服务器端口资源。 |
| 远程协助功能 | 支持实时查看远端计算机的操作进程、服务、系统日志等信息。 |
| 支持对远端计算机进行关机、重启、断网等管理。 |
| 对远端计算机远程查看和远程控制，可根据管理需要灵活配置是否强制管理还是授权管理。 |
| 支持对远端计算机进行文件级远程管理，可在用户无感知的情况下远程创建、重命名、拷贝、删除文件。 |
| 远程查看、远程控制可以根据管理需要和网络状况，选择、配置适合管理员的窗口分辨率、显示比例、色彩、鼠标按键、光标等。 |
| 权限管理员支持限制操作管理员远程控制的权限，是否允许强制查看、控制和文件传输，允许指定必须申请管理的终端列表。 |
| 网络适应性 | 支持各种网络环境的终端管理，包括同一网段、单方处于NAT子网中、双方各自处于不同的NAT子网中、处于VPN环境中。 |
| 支持自动穿透管理计算机的防火墙设置。 |
| 多方管理 | 支持一台计算机接受多台计算机同时维护管理。 |
| 支持一台计算机同时管理控制多台计算机。 |
| 违规外联 | 外联行为控制 | 能够检测出通过代理等方式产生的外联行为并进行报警阻断，在内网设备带出外网的情况下同样能够检测出上述外联行为并进行违规行为上报和阻断。 |
| 违规访问控制 | 控制终端只能访问外网或只能访问内网，能够以策略方式按照区域、部门、组、ip段或单台设备设定内网访问范围。 |
| 对违规网络访问行为进行报警和阻断。 |
| 支持内网设备带出后在访问外网时自动进行阻断和违规行为上报。 |
| 网络代理使用管控 | 从网络协议层面检测网络代理的行为，支持基于网卡数据包的代理数据阻断功能，并支持报警、断网、锁屏等强制控制措施。 |
| 支持检测Windows的代理配置选项，检测不符合要求的代理配置情况，并支持自动清除、报警、断网、锁屏等强制控制措施。 |
| 代理行为的管制支持例外合法的代理地址。 |
| 网络安全管理 | 网络配置绑定 | 能够实时监测终端IP地址、MAC地址、DNS配置等相关网络信息，支持对应信息的实时绑定，当IP或MAC发生改变时能够强制恢复至修改前。 |
| 外设管理 | 禁用终端设备的USB接口、光驱、软驱、打印机、调制解调器、串并口、1394、 红外、蓝牙及PCMCIA卡等外设接口。 |
| 单独禁用USB移动存储设备而不影响其他USB设备。 |
| 反ARP欺骗 | 支持网关、关键服务器等IP、MAC的静态绑定，从而免受ARP的欺骗攻击。能够实时检测ARP欺骗的病毒源，能够对有ARP攻击的终端设备进行隔离。 |
| 主机防火墙 | 提供基于协议、基于IP和端口、Ping共3种拦截方式。 |
| 设定允许或禁止主机访问的IP段、端口和协议。 |
| 设定允许或禁止某个IP段访问本地主机的端口和协议。 |
| 上网访问控制 | 能够基于URL关键字设定允许或禁止终端设备访问的网站，能够对违规访问设备进行报警或阻断。 |
| 可信主机访问 | 能够设置为例外可信设备，与其他安装客户端的设备通信。 |
| 移动存储介质管理 | 移动介质授信管理 | 禁止未注册USB移动存储设备的随意接入。 |
| 必须支持新USB移动存储设备用户在线申请、注册，管理员在线审核，无需上交信息中心注册。 |
| 能够对指定的USB移动存储设备进行注册，设定所属部门和使用人，并进行加密、只读和可写的控制。 |
| 控制指定USB移动存储设备在外网无法使用。 |
| 能够针对区域、部门、组、IP段或单台设备控制指定USB移动存储设备的读写权限，能够对终端和USB移动存储设备进行一对一绑定。 |
| 移动介质安全管理 | 能够对USB移动存储设备中指定名称的文件进行允许或禁止访问的控制。 |
| 能够禁止访问USB移动存储设备中的可执行文件。 |
| 能够禁止USB移动存储设备的自动运行。 |
| 移动介质审计 | 能够对USB移动存储介质的插入和拔出行为进行审计。 |
| 能够指定审计的设备范围，能够指定审计的USB设备，能够指定审计的文件名称和操作类型，能够对通过USB设备进行的文件拷入、拷出行为进行审计，支持按照使用设备、文件路径、操作名称、操作时间进行报表的查询。 |
| 行为控制 | 组策略管理 | 支持基于组策略的操作系统组件功能，如：禁用控制面板、禁止添加打印机、禁用任务管理器、阻止更改桌面背景、禁用注册表编辑器、阻止访问命令提示符等。 |
| 支持基于自定义工具定制组策略模板配置，可自动录制计算机的组策略配置信息，并可批量下发和批量执行。组策略模板执行的内容，在策略取消或停止后能自动回滚到执行前的配置状态。 |
| 行为审计 | 文档审计 | 能够记录终端用户日常的文档的操作行为，可以详细审计用户新建、拷贝、修改、移动、删除等操作行为。 |
| 邮件审计 | 能够对用户日常邮件的收发做有效审计，审计内容包括邮件地址、邮件标题、邮件内容以及附件等，方便事后追查。 |
| 网站审计 | 实时记录终端计算机访问过那些网站，并以饼状、表单等图表方式形象的展现统计结果、访问量排行。 |
| 刻录审计 | 可以通过黑白名单方式进行审计或不审计指定光盘刻录机，同时可以对指定审计某种文件格式以及所在路径的文件。 |
| 屏幕录像审计 | 支持以截图的形式录制计算机的操作录像。 |
| 支持以视频的形式播放，支持快进、快退、暂停、播放速度调节。 |
| 支持自定义选择录制的帧率、图像质量。 |
| 支持上传和存储到第三方的文件服务器。 |
| 支持录像记录文件的定期自动清理功能。 |
| 支持基于桌面程序窗口的筛选录制，可实现只录制指定窗口的屏幕记录。 |
| 测试 | | 签合同前要求进行上述产品功能测试。 |
| 资质要求 | | 公安部《信息安全产品检测报告》 |
| 公安部《计算机信息系统安全专用产品销售许可证》 |

### 7.3.22 内网核心防火墙

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| **基本要求** | 操作系统 | 要求采用先进的多核网络专用架构多核硬件平台，x86多核处理器，非MIPS的多核架构或ASIC架构；安全操作系统采用冗余设计，系统运行的可靠性与稳定性，要求信息安全设备、系统软件的开发、生产符合ios9001标准，提供相关证明； |
| **系统性能** | 系统配置 | 1U机架式机型，标配6个10/100/1000MBase-T端口，2个SFP扩展插槽，4个万兆光口，4个光模块；1T硬盘；整机吞吐率：>16Gbps；应用层吞吐率：8Gbps；最大并发连接数：>800W，配置IPS攻击规则特征库三年许可； |
| **网络**  **接入** | 工作模式 | 支持路由、交换、混合、工作模式； |
| 路由交换 | 支持静态路由、ISP路由及动态路由协议，支持802.1q、QinQ模式； |
| 支持基于源/目的地址、源/目的端口、用户、应用的策略路由； |
| 接入功能 | 支持GRE与IPSEC VPN接入；IPSEC VPN可提供国密算法； |
| 链路聚合 | 提供不少于11种的负载分担算法，灵活实现对聚合组内业务流量的负载分担 |
| 地址转换 | 支持一对一SNAT、多对一SNAT、一对一DNAT、双向NAT、NoNAT等多种转换方式；支持Sticky NAT开关，使相同源IP的数据包经过地址转换后为其转换的源 IP 地址相同； |
| 智能DNS | 支持智能DNS及DNS Docting功能 |
| **IPv6** | 双栈模式 | 支持IPv4/IPv6双栈工作模式； |
| 访问控制 | 支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置； |
| 安全防护 | 支持基于IPv6的应用层检测（FTP\TFTP）、病毒过滤、URL过滤、ADS、IPS检测； |
| **虚拟系统** | 资源虚拟化 | 支持在一台物理设备上划分出最大4000个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源； |
| 功能虚拟化 | 支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、异常行为分析、病毒过滤、内容过滤、审计、报表等安全功能虚拟化； |
| **用户管控** | 认证方式 | 内置强大的用户身份管理系统，支持本地认证、证书认证及免认证等方式，同时支持RADIUS、LDAP、TACACS等多种第三方外部认证设置； |
| 用户管控 | 综合运用身份认证与访问控制技术，通过内置智能过滤引擎实现基于用户身份的安全防护策略部署与可视化监控；支持创建用户； |
| **应用管控** | 应用识别 | 内置独立应用识别特征库，总数2100种以上，支持应用特征库在线或本地更新，支持应用特征自定义； |
| 带宽管理 | 支持基于IP/IP组、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略； |
| 连接控制 | 支持对单条访问控制策略进行最大并发连接数限制； |
| 为保护内部网络资源以及合理分配设备系统资源，需支持对指定的源/目的IP地址、MAC地址、应用制定相应的连接限制策略，策略包含三种限制类型：单个IP每秒新建连接限制、单个IP连接数限制及连接总数限制； |
| 支持监控功能，显示最近被拦截的IP、地址对象及应用的节点信息；同时支持对连接数限制策略匹配信息进行分类统计，方便管理员根据统计分析结果进行相应的防护控制； |
| **访问控制** | 一体化访问控制 | 内置高度集成的一体化智能过滤引擎技术，实现在同一条访问控制策略中配置传统的五元组信息、用户等的识别与控制。 |
| 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址； |
| 提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在WEB界面显示检测结果； |
| 支持黑名单功能，可设置多个对象条件，如：五元组信息、地址范围、应用、用户等； |
| **安全防护** | 未知威胁防御 | 支持APT防御扩展，不依赖于攻击、恶意代码等特征库进行检测，通过沙箱技术对于未知漏洞攻击（0day/1day漏洞）、木马、病毒具有检测能力；可根据用户环境，将APT工作模式设置为深度模式或者智能模式； |
| 入侵防御 | 内置攻击检测引擎，采用协议分析、模式识别、统计阀值和流量异常监视等综合技术手段来判断入侵行为；支持web攻击识别和防护，如跨站脚本攻击、SQL注入攻击；支持超过4000攻击特征库，同时支持自定义特征库。 |
| DDOS防御 | 支持基于IP协议的检测清洗； |
| 支持基于TCP协议的检测清洗； |
| 支持基于UDP协议的检测清洗，包括对源、目的限速，对UDP最大及最小报文限制；同时支持UDP关联认证，要求所有去往服务器的UDP报文，必须首先与该服务器的TCP端口建立TCP连接，对源地址进行合法性认证； |
| 支持基于DNS协议的检测清洗，包括但不限于：DNS QUERY FLOOD、DNS REPLY FLOOD、DNS投毒攻击、DNS格式检查、DNS NX异常比率检测等；支持DNS QUERY源认证、DNS REPLY源认证； |
| 支持基于HTTP协议的检测清洗，支持对HTTP slow-header和HTTP slow-post设置最大传输时间以及异常会话数阈值，有效防御慢速攻击； |
| 支持根据DOS/DDOS攻击行为自动添加动态黑/白名单功能； |
| 文件过滤 | 内置文件过滤引擎，支持对即时通讯、社交网络、网络硬盘、网页邮箱、IM文件传输等应用类型以及HTTP/FTP/SMTP/POP3等标准协议进行检测，识别可执行文件、office文件、视频文件、图片文件、帮助文件、压缩文件、数据文件等超过40种文档类型的文件过滤 |
| 内容过滤 | 支持基于http、ftp、telnet、smtp、pop3等协议的内容过滤策略，支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤； |
| 敏感数据泄漏防护 | 内置DLP数据防泄漏引擎，对数据进行监控识别，达到敏感数据防护目的。支持识别的文件类型数量不少于1000种；文件内容识格式不少于300种。  支持多种加密和压缩文件格式，如RAR、ZIP、GZ、TAR等；支持识别Linux，Unix等非Winodws的文件类型；支持识别异常文件格式类型；支持识别自定义文件类型。 |
| 配置维护 | 支持多个配置文件并存，配置文件数量不少于20个； |
| 升级维护 | 支持多个系统升级包并存，系统升级包文件数量不少于5个（提供截图） |
| 管理员 | 支持管理员分权管理，可自定义管理员权限模板，所有功能模块组合可由管理员自由组合配置 |
| **数据中心** | 审计 | 支持独立配置审计策略，同时也可将指定的 IP 地址、 URL、应用加入白名单，不进行数据审计； |
| 日志 | 支持日志本地存储，可对不同类型日志设置存储空间；  支持外发至SYSLOG服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密，设定8位的加密密钥； |
| 日志查看可划分为管理日志、系统日志、策略日志、应用行为日志等四大模块，可将日志按照CSV或XML格式导出； |
| **显示监控** | 资源监控 | 在WEB界面提供资源监控开关，可对cpu占用率、内存占用率、磁盘占用率设置阈值； |
| 流量统计 | 支持根据应用对通过设备的数据报文流量进行统计； |
| 支持根据用户/用户组对通过设备的数据报文流量进行统计； |
| 支持根据服务器对通过设备的数据报文流量进行统计； |
| 威胁统计 | 支持根据按照病毒防御、入侵防御、APT防御、ADS攻击进行威胁统计，可按照威胁类型/攻击者/受害者等类似威胁排名， |

### 7.3.23 运维堡垒机

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| 配置要求 | 授权管理数 | 授权管理100台，含三年服务 |
| 部署方式 | 采用物理旁路模式部署，不影响网络结构。 |
| 管理结构 | B/S架构，采用HTTPS方式远程安全管理，无需安装客户端。 |
| 网络接口 | 1U，含单交流电源 |
| 2\*USB接口，1\*RJ45串口，1\*GE管理口，4\*GE电口 |
| 数据存储 | 系统自带内部存储，存储空间不低于2T； |
| 并发访问 | 图形并发≥80 |
| 字符并发≥180 |
| 权限管理 | 用户角色 | 堡垒机具有用户多角色划分功能，如堡垒机系统管理员、运维主管、设备管理员、普通用户、审计管理员、审计员等，对各类角色需要进行细粒度的权限管理。 |
| 设备访问授权 | 设备访授权：身份认证之外，需要更高级管理员授权才能对设备进行运维操作； |
| 命令执行授权 | 命令执行授权：对特定命令的执行需要更高级管理员授权才能执行 |
| 工单系统 | 支持工单授权功能，通过运维人员申请或管理员下发工单的方式来赋予运维人员访问目标服务器的权限，且有工单生效时间限制， |
| 身份认证 | 身份认证 | 主帐号登录堡垒机应支持本地静态密码认证、LDAP认证、RADIUS认证、证书认证等身份认证方式； |
| 用户登陆堡垒机支持MAC绑定，非法地址无法登陆堡垒机； |
| 堡垒机访问自身的ACL限制，支持配置可访问的IP范围； |
| 设备资产管理 | 支持的协议 | 字符型远程操作协议：SSH(V1、V2)、TELNET； |
| 图形化远程操作协议：RDP、VNC、X11，其支持文件共享；可支持RDP、VNC的客户端直接访问堡垒机； |
| 文件传输协议：FTP、SFTP、SCP；可支持FTP客户端Winscp直接访问堡垒机 |
| 支持Oracle、MS SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、PostgreSQL等数据库 |
| 支持HTTP、HTTPS操作审计，HTTP/HTTPS协议可以直接代理； |
| 数据库运维支持能力 | 要求支持数据库审计功能，能够将网络中的流量通过镜像的方式传到堡垒机，堡垒机以录屏加数据库日志的形式审计运维人员的操作，支持将操作语句与录屏进行实时绑定，能够准确快速的定位数据库语句执行时，整个屏幕的状态。提供产品功能截图。 |
| 目标设备登录方式 | 自动登录目标设备：运维人员不必知道目标设备帐号及密码，无需进行二次登录认证，实现单点登录； |
| 手工登录目标设备：运维人员每次通过堡垒机登录目标设备都需要手工输入目标设备用户名密码； |
| 半自动登录目标设备：即第一次登录目标设备时运维人员需手工输入目标设备帐号和密码并允许堡垒机保存该帐号密码，运维人员在后期登录时即可实现自动登录目标设备。 |
| 密钥登录方式：在登录目标服务器时，使用的是秘钥登录，而非密码。在既可以使用密码，又可以使用秘钥的环境，可以自由选择登录认证方式。 |
| 设备维护 | 支持批量导入/导出/修改目标设备信息； |
| 支持智能扫描方式自动发现网络中的设备，通过IP地址扫描，快速发现指定IP地址范围内的主机、服务器和网络设备，并自动识别启用服务和端口，方便管理员快速添加设备。 |
| 密码对象管理 | 支持改密审批，改密前可选择是否需要提交领导审批，进一步确保改密安全。 |
| 改密结果详情中显示旧密码和新密码列，提供链接来测试登录。 |
| 由于密码的重要性，备份的密码文件必须采用加密的方式，支持通过配置界面将需要备份的密码打包成压缩文件并设置加密口令；请提供截图证明 |
| 设置账号可设置自动定期改密，自动改密后支持邮件通知，将改密后的密码文件发送到指定邮箱，须支持设置附件密码；请提供截图证明 |
| 系统管理 | 配置向导 | 提供对部分配置操作进行向导式配置界面，尤其是操作步骤比较多，前后有关联的数据库审计配置。请提供截图证明并加盖公章。 |
| 实时监控 | 支持实时监控通过SSH、SFTP、RDP、VNC 、Telnet、FTP、X11等协议的操作行为；对监控到的非法操作，可实时手工切断。 |
| 静态路由 | 可添加静态路由信息，部署于复杂的网络环境。提供截图证明并加盖公章。 |
| 自动生成报表 | 提供周期生成报表，用于审计或者上报，提供给用户按照自定义规则自动周期生成报表的功能。 |
| 增强功能 | 应用发布 | 可通过应用发布的方式进行协议扩展，无需定制即可支持其他通用及专有的运维客户端程序。 |
| 支持的设备访问方式 | Web访问方式:支持通过审计系统的Web页面直接访问设备； |
| 客户端访问方式：支持通过SecurCRT等常用的命令行客户端工具登录堡垒机并访问目标设备，并支持会话克隆； |
| 支持web服务器访问用户名密码代填，支持vSphere Web Client 用户名密码代填。 |
| 访问控制及异常告警 | 支持通过基于时间、IP/IP段、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字正则表达式、内置命令集、危险级别（按危险程度分为高、中、低）等组合访问控制策略，授权用户可访问的目标设备。内置命令集请提供截图证明。 |
|
| 入侵审计 | 要求支持主动对配置的子账号进行关联分析，当发现攻击者植入的异常账号时，对相关管理员采取告警、记录及通知等操作。 |
| 远程运维安全 | 支持通过VPN联动 |
| 资质要求 | 产品资质 | 获得由国家信息安全测评中心颁发的《信息技术产品安全测评证书（EAL3+）》，并提供证书复印件 |

**7.3.24 数据库审计**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 产品资质 | 所有资质必须为数据库审计产品专有的资质，不能是网络审计产品或者综合审计的产品资质。 |
| 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》,提供证书复印件； |
| 产品通过国家信息安全认证中心3C认证检测，提供证书复印件； |
| 提供产品第三方权威检测报告，根据关联程度和完整程度评定。 |
| 硬件指标 | 产品须采用专用工控机硬件架构，非普通PC服务器， MTBF(平均故障间隔时间)≥65000小时； |
| 系统须启动采用CF卡加硬盘方式，保证稳定可靠不可篡改。 |
| 规格：1U机架式设备， |
| 硬盘可用容量：≥1TB, 支持RAID0、RAID1 |
| 网络端口：千兆电口\*4 |
| 处理能力 | 吞吐能力：≥1000M，日处理业务操作数：≥2亿条 |
| 数据采集性能：≥1万条/秒 |
| 审计日志检索能力：≥1500万条/秒； |
| 部署方式 | 旁路部署模式下无须在被审计数据库系统上安装任何代理即可实现审计 |
| 软件代理模式：支持在目标数据库安装软件代理（agent）解决云环境、虚拟化环境内部流量无法镜像场景下数据库的审计。 |
| 支持分布式部署，管理中心可实现统一配置、统一报表生成、统一查询； |
| 管理中心和探测器都可存储审计数据，实现大数据环境下磁盘空间的有效利用和扩展； |
| 管理中心和探测器之间的数据传输速率、时间、端口都可自定义； |
| 协议支持 | 支持Oracle、SQL-Server、DB2、Informix、Sybase、MySQL等六种主流数据库审计； |
| 支持对SQLserver 2005以上版本加密用户名的审计 |
| 支持PostgreSQL、Teradata、Cache、人大金仓、达梦、南大通用等数据库审计； |
| 支持主流业务协议 HTTP、Telnet、FTP、SMTP、POP3、DCOM； |
| 支持对各种协议自动识别编码及在web界面手工配置特定编码 |
| 审计功能 | 支持数据库操作类、表、视图、索引、存储过程等各种对象的所有SQL操作审计； |
| 支持对操作时间、SQL语句、执行结果、返回结果集、影响行数、执行时长、数据库用户名、实例名、源/目的IP、源/目的端口、源/目的MAC、客户端主机名、客户端程序名称、客户端操作系统用户名、业务主机群、SQL模板、会话ID、事件唯一ID等至少21个条件进行审计； |
| 数据库请求和返回的双向审计：支持审计返回时长、SQL错误代码、返回行数、返回结果集的审计，以及客户端发送的数据库操作指令。 |
| 支持跨语句、跨多包的绑定变量名及绑定变量值的审计 |
| 支持对超长SQL操作语句审计，可以正常记录单条长度<=64K个字节的SQL语句内容； |
| 支持在IPV6环境中部署，且支持所有数据库IPV6协议的审计 |
| 支持数据库防火墙功能，支持对根据IP、账号、客户端工具名、时间等定制规则进行阻断 |
| 支持导入审计关联的账号信息，支持通过IP和账号关联到具体SQL是哪个自然人操作。 |
| 智能发现 | 自动识别流量中存在的数据库，也可通过扫描发现网络中的数据库 |
| 数据库风险评估：支持对主流数据库的安全漏洞扫描。 |
| 应用关联 (三层关联) | 支持B/S业务系统三层关联审计，客户端访问WEB服务器执行SQL操作，系统需支持将URL和SQL语句关联，记录客户端地址等信息。 |
| 支持C/S、B/S三层架构下的真实用户名关联配置 |
| 支持通过部署agent实现java web环境100%准确关联 |
| 支持旁路自动学习三层审计关联功能 |
| 运维审计 | 支持网络TCP会话审计； |
| 支持数据库协议解析成会话形式，并支持一键关联到具体的SQL操作会话。 |
| 支持与堡垒主机自动关联审计通过ssh、rdp等加密协议操作数据库行为 |
| 安全审计 | 支持审计记录中敏感数据的模糊化处理，内置常见敏感数据掩码规则，支持自定义敏感数据掩码规则 |
| 内置安全特征库规则不少于300条，支持对数据库安全进行检查，如SQL注入，缓冲区溢出，数据库漏洞、弱口令等； |
| 审计策略 | 内置审计规则库不少于200条。支持事件类型和策略分组，同时支持黑白名单方式策略 |
| 可自定义审计策略。审计策略至少支持18个条件； |
| 规则各条件之间支持与或非逻辑关系 |
| 告警数量需支持最大告警数量限制，超过告警阈值之后便不告警 |
| 告警分析应支持根据SQL模板排行分析，便于告警处理。 |
| 告警查询应支持根据登陆用户、客户端工具名、客户端IP、规则进行归并分析，能详细展示每类告警占总告警数量百分比，便于告警分析处理 |
| 审计查询 | 具有高效的查询性能，后台采用SPHINX全文检索引擎检索 |
| 查询条件易于使用，审计查询条件均为非正则表达式形式进行 |
| 支持采用部分匹配模糊查询方式检索审计日志 |
| 支持基于数据库访问日期、时间、源/目的IP、来源、数据库名、数据库表名、字段值、数据库登陆账号、SQL关键词、数据库返回码、SQL响应时间、数据库操作类型、影响行数等条件的审计查询； |
| 统计报表 | 系统提供内置多种报表模板库，内置的报表不少于35种, |
| 支持根据单个数据库或逻辑数据库组生成报表 |
| 报表支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告； |
| 支持按照源IP地址、客户端工具、帐号、告警数等源信息生成报表； |
| 支持按照数据库访问行为生成报表，智能识别帐号的增删、权限变更、密码修改、特权操作等行为； |
| 支持按照时间曲线统计流量、在线用户数、并发会话、DDL操作数、DML操作数、执行量最多的SQL语句等报表； |
| 支持性能分析，准确提炼出SQL语句执行频率和执行时间异常的报表； |
| 支持Word、PDF、ppt等格式的报表导出； |
| 支持定期自动生成审计报表且以电子邮件方式自动进行发送； |
| 支持报表自定义，自定义的条件不少于20个 |
| 模型分析 | 支持对数据库自动建模及智能对异常行为告警功能；模型包括但不限于：新增行为、帐号视图、源IP视图等，并自动对模型以外的行为进行告警。 |
| 可通过行为轨迹图方式展示数据库访问行为 |
| 可基于账号、IP地址、访问权限、客户端工具等维度对行为模型做钻取分析、变更分析，对学习的安全基线以外的行为自动智能的进行告警 |
| 可以自动对比不同时期的行为模型，以区分其审计日志数趋势、用户、IP地址、工具、访问权限的差异情况； |
| 数据管理 | 支持根据保留天数和占用百分比自动清理最早的数据 |
| 备份文件需要加密，支持审计数据自动备份审计日志，并外送到独立FTP服务器； |
| 提供审计策略和系统配置信息的单独导入、导出功能； |
| 数据库弱点扫描模块 | 模块类型为软件形式，须提供光盘介质一套； |
| 支持对Oracle、MS SQLserver、Mysql、Infomix、DB2、Sybase、达梦、人大金仓等数据库进行弱点扫描并提供检测报告。 |
| 模块拥有独立国内自主知识产权；通过公安部信息安全产品检测中心检测并获得销售许可证书。 |
| 实时监视 | 提供用户界面告警、Syslog告警、SNMP告警、邮件告警、短信告警、ftp告警等六种方式 |
| 支持本地和数据中心查看CPU、内存、磁盘、网口、运行状态等信息 |
| 系统管理 | 采用B/S架构管理，支持中英文两种管理界面 |
| 支持系统安全配置（会话锁定、超时退出、IP地址访问控制、密码复杂性管理、验证码登陆等安全措施） |
| 支持NTP时间同步、SNMP(v1、V2、V3)网络管理协议 |
| 支持离线手工自动升级，升级数据和配置均需保留 |
| 支持三权分立，系统默认设定系统管理员、规则配置员、审计查看员、操作日志查看员等角色 |
| 具有自身安全审计功能，可以对审计系统的所有用户操作进行审计记录 |
| 故障排错 | 系统内置独立的故障排错系统，可以支持一键导出加密的系统调试日志，支持一键检测服务、许可证、流量等大部分常见常见故障的检测 |
| 支持流量分析功能，包括抓包、包内容查看、自动探测sql语句等； |
| 售后服务 | 本地应急响应时间<=4小时； |

### 7.3.25 应用负载均衡

|  |  |  |
| --- | --- | --- |
| **指标项** | | **指标要求** |
| 总体要求▲ | 产品要求 | 要求产品为独立的硬件负载均衡设备，不接受交换机插板式负载均衡解决方案 |
| 硬件和系统 | 硬件架构 | 采用基于每个端口的ASIC芯片 |
| 系统内核 | 采用封闭式的专有操作系统，无已知安全漏洞 |
| 处理模式 | 多核CPU并行处理，充分利用交换机多CPU资源 |
| CPU | CPU核数量≥ 4 |
| 内存 | 8G，可扩展至32G |
| 接口 | ≥2个万兆光口和≥8个千兆电口 |
| 硬盘 | ≥500G |
| 性能要求 | 平台4/7层最大吞吐能力 | ≥26G |
| 投标吞吐能力 | ≥6G，可通过License升级到26G |
| 并发连接数 | ≥12M |
| L4每秒新建连接（CPS） | ≥600K |
| L7每秒请求处理（RPS） | ≥850K |
| SSL CPS(2k) | ≥2000/7000/13000（Std/XL/Extreme） |
| SSL吞吐量 | ≥6.7/7.7G（Std/XL/Extreme） |
| 平台HTTP压缩 | ≥2/3.5/6.8G（Std/XL/Extreme） |
| 虚拟化要求 | 虚拟化管理程序▲ | 采用专用虚拟化管理程序，非第三方的服务器虚拟化架构 |
| 虚拟化方式 | CPU、内存、SSL加速、网络等计算资源虚拟化。不接受网络标签模式 |
| 平台vADC数量 | ≥24，本次配置2个VADC授权 |
| vADC性能隔离 | 每个vADC可以按需扩展性能，并能保证每个vADC达到原先设定的性能指标； |
| vADC网络隔离 | 每个vADC有独立的二层和三层的数据处理，包括ARP表、转发表、VLAN、路由表, 可以实现IP地址域的重用； |
| vADC版本隔离 | 每个vADC单元都具有独立版本的负载均衡操作系统，可以单独升级软件； |
| vADC功能隔离 | 每个vADC有完整的应用交付功能，包括本地和全局的服务器负载均衡，链路负载均衡，SSL加密、缓存、压缩等； |
| vADC管理隔离 | 每个vADC有单独的配置权限和文件，对于一个vADC的配置修改不影响其它的vADC |
| vADC故障隔离 | 每个vADC可单独重启和冗余切换，不影响其他vADC和主机 |
| P2V/V2V工具 | 提供vADC封装后在不同平台和资源上迁移能力 |
| 服务器虚拟化环境支持 | 支持主流的Orchestration管理软件，提供主流Orchestration系统的插件，包括VMWare、Redhat、HP和IBM等； |
| 网络功能要求 | VLAN功能 | 支持IEEE 802.1Q 标准，可设定至少2048 (含)以上VLAN |
| 链路聚合 | 支持802.3ad Link Aggregation 功能 |
| 其它L2功能 | 支持 IEEE 802.1d Spanning-Tree、802.1Q、802.3x Flow Control、802.3 Auto-Negotiation功能 |
| 路由 | 支持RIP、RIP2、OSPF/OSPFv3，BGP等路由协议 |
| IPV6网络支持 | 完全支持IPV6环境，包括：Address、Neighbor Discovery router advertisements、Static Route、Gateway、VRRP等IPv6 功能，并已获取IPV6 Ready Logo认证 |
| 负载均衡功能要求 | 负载均衡算法 | 支持负均衡算法：轮询、加权轮询、最少用户数、HASH、最少流量 |
| 对话保持 | 支持会话保持方式：cookie，session ID，URL，Http Header等模式 |
| 健康检查 | 支持基于ICMP、UDP端口、TCP端口和HTTP, Radius, DNS, SMTP, POP3, LDAP, IMAP4,FIX,FTP,RTSP,SSL等应用的健康检查方式，并可自主编写脚本检查应用复杂的服务器 |
| 应用层负载均衡 | 支持L7内容智能检查及应用重定向 |
| 全局负载均衡 | 支持全局负载均衡 |
| Internet链路负载均衡 | 支持Internet链路负载均衡 |
| 透明重定向 | 支持透明重定向，实现NAT，代理功能； |
| 应用支持 | 支持防火墙、VPN、IDS 设备负载均衡 |
| 应用加速功能 | 包括SSL卸载、TCP优化、Http压缩和Caching |
| 可编程负载均衡 | 基于TcL语言的脚本，灵活控制应用交付 |
| 攻击防范 | 可防范下列类型的DOS (Denial Of Service)攻击，TCP、IP、UDP、ICMP、ARP |
| 带宽管理 | 可提供带宽管理功能， |
| Web应用加速 | 支持浏览器 | 支持所有浏览器类型 |
| 减少HTTP请求数量 | CSS/JS代码对象合并和植入，减少内容和HTTP请求数量 |
| 动态缓存技术 | 支持动态修改页面内容标签，同时支持把缓存内容推送到浏览器 |
| 图像优化 | 支持图像优化和压缩，提高页面加载客户QoE |
| HTML 5支持 | 可识别移动用户类型，实现Web性能加速 |
| TCP 协议优化 | 支持TCP协议优化和拥塞防止，可优化传输层性能，实现压缩 |
| 应用性能监控 | 监控方式 | 真实用户性能，且用户端无需安装插件或程序，即可实现用户监控端到端的 Web应用响应时间 |
| 监控数据 | 提供数据中心、网络和客户端性能数据 |
| 性能报告类型 | 可基于应用、页面、地理位置提供性能报告 |
| 可靠性部署 | 冗余协议 | 支持VRRP冗余 |
| Hot-Standby | 主备模式 |
| Active-Backup | 互为主备 |
| Active-Active | 集群方式提供同一VIP地址服务 |
| 管理功能 | 应用配置模板 | 包括MS Exchange，Web Application，Oracle E-Business等 |
| 设备性能监控 | 设备CPU等资源利用等 |
| 专用网管接口 | 支持专用网管接口实现带外管理 |
| 管理方式 | 支持下列管理方式：CLI，WEB（HTTP/HTTPS），Telnet，SSH，GUI界面管理； |
| API接口 | 支持API接口和标准XML接口 |
| 集中管理 | 支持图形化集中管理，可在管理平台上集中管理多台设备。 |

### 7.3.26 数据库服务器

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 服务器外型 | 机架式 |
| 服务器高度 | ≤4U，标配原厂滑动导轨 |
| CPU型号 | Intel Xeon E7-4830v4 处理器 |
| CPU实配数量 | ≥4颗 |
| 内存功能 | 高级ECC、在线备用内存、内存镜像、故障内存隔离、DDDC/SDDC等 |
| 内存实配规格 | ≥32GB\*8 DDR4 2400MHz |
| 插槽数量 | 可扩展≥96个内存插槽 |
| 内存可扩展数量 | 最大容量支持≥6T容量 |
| 实配硬盘及托架 | ≥2\*600GB SAS 15k 2.5寸硬盘， |
| 硬盘扩展能力 | ≥最大支持10个2.5寸硬盘槽位 |
| 阵列控制器 | ≥1个阵列卡专用插槽（不占用PCIE扩展槽），配置12Gbps SAS磁盘阵列控制器，支持Raid0/1/10/5/6盘镜像，调整缓存读写比例等功能。 |
| 实配≥4GB缓存，支持缓存数据保护，且后备保护不受时间限制； |
| 支持raid 1/10 |
| PCI I/O插槽 | ≥9个PCI-e 3.0全高/全长插槽 |
| 网卡 | 标配1个网卡专用插槽（不占用PCIE扩展槽），可选配千兆或万兆网卡。本次配置≥4个10/100/1000M-BaseT 多功能以太网接口，2个双口万兆光口网卡（含4个SFP+光模块），2块单口16G FC HBA卡(含2个SFP模块) |
| 冗余电源 | 4个≥1200W铂金版热插拔冗余电源（2+2冗余） |
| 冗余风扇 | 热插拔冗余风扇 |
| 远程管理卡 | 配置≥1Gb独立的远程管理控制端口，配置虚拟KVM功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶，提供国家强制性产品认证证书，并配置支持上述功能的授权。 |

### 7.3.27 数据库存储

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 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；统一存储池架构支持LUN、VVOLs及NAS 服务器，分别提供数据块和文件访问服务；以上均需提供官网链接证明； |
| 控制器 | 控制器部件全冗余，支持NAS、FC、iSCSI数据访问服务；  控制器对称双活，双控制器能同时访问同一个份数据单元（LUN）；  控制器数量≥2；配置控制器总缓存≥96GB；  每控制器CPU≥8核，主频≥2.4G Hz； |
| 磁盘存储容量 | 本次磁盘配置：本次配置5块400G SSD硬盘作为数据缓存，配置20块1.8T 10K硬盘； |
| 支持磁盘类型 | 所投存储系统可同时支持服务器 SSD；硬盘数量≥250块（非Cluster模式）；SSD单盘最大可支持3.2TB。 |
| 前端主机端口 | 支持接口类型：  最大支持的FC端口≥20；  最大支持的10GbiSCSI端口≥24；  本次配置4个16Gb/s的前端FC光纤通道端口+4个万兆电口IP接口；  以上均需提供官网链接证明； |
| 后端端口带宽 | 配置磁盘阵列连接磁盘的后端端口带宽≥96Gb/s； |
| 扩展能力 | 单台阵列最大支持的磁盘数≥250；  具有完全在线、无需停机的扩充能力，包括系统微码升级、系统处理能力的扩充、存储容量的扩充等； |
| 高可靠性 | 完全的硬件冗余：处理器、缓存、电源、风扇、适配卡、总线等都提供冗余，并保证在某硬件出问题时，能够进行自动切换，不出现单点故障，磁盘阵列系统具有高可靠性，达到99.999%可用性； |
| RAID保护方式 | 支持多种RAID保护方式，包括0/1,5,6； |
| 双控制器最大支持SAN主机数 | ≥1024，本次配置双控制器（一个HA对）1024个主机支持，必须提供官方网站链接和截图。 |
| 存储管理软件 | 需提供图形化存储管理软件，支持带外管理；  支持基于角色的管理；为不同的管理人员分配对应的管理权限； |
| 存储控制器软件 | 配置主存储控制器软件的独立运行版本，支持Windows、Linux、Unix操作系统，配置SAN、NFS、CIFS、iSCSI与VVOLs协议，配置自动存储分层功能，配置存储复制功能，能够与此次所投存储实现复制，配置服务质量管理QoS功能；配置不小于4TB的容量许可；以上均需提供官网链接证明； |
| 集中化管理 | 提供管理软件，可管理的阵列数量多台； |
| 性能分析软件 | 配置阵列的性能分析软件，能够获取实时的性能数据和历史性能数据；产生性能报表； |
| 虚拟资源调配 | 支持并配置虚拟资源调配功能，按照实际使用的存储容量分配存储空间，提高存储利用率； |
| 磁盘降速 | 在磁盘没有IO访问的情况下，能够智能的将磁盘处于停止状态，从而降低系统对能源的消耗； |
| 服务质量管理(QoS) | 通过优化磁盘阵列中的应用程序IO队列，实现对应用程序的IOPS、带宽和响应时间的控制优化； |
| 本地数据复制保护功能 | 配置防病毒，加密，存储系统配置本地快照及本地克隆技术；每系统的快照数量≥4000个； |
| Vvol配置 | 配置vvol支持，支持数量≥8000； |
| 生态系统集成 | 配置VMware、Microsoft、OpenStack集成功能，包括 VSI、VASA、ESI、SRM、ODX等的集成功能，需提供供官网链接及截图证明。 |
| 数据本地迁移 | 要求存储系统配置具有内部数据迁移功能的软件；基于存储系统本身的控制器实现数据在不同逻辑卷之间、不同RAID类型的卷之间数据迁移，且无需中断应用访问； |
| 基于异构阵列的数据迁移 | 提供迁移工具，将存储系统中的数据在不同厂商的磁盘阵列中进行数据迁移； |
| 数据通道安全(负载均衡/链路切换) | 配置通道管理软件，实现对主机的多通道路径访问以及对应用透明的自动故障通道切换及负载均衡，具备在SAN环境中的负载均衡功能； |
| 灾难恢复 | 需支持基于数据块级远程复制功能，以实现基于存储设备的灾备数据复制及恢复；配置同步/异步复制软件许可； |
| 支持操作系统 | 磁盘阵列能提供对主流操作系统的支持：能够同时支持SUN Solaris、HP-UX， IBM AIX， Linux， windows操作系统，支持服务器集群功能； |

### 7.3.28双活存储虚拟化系统

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 虚拟化设备类型 | 主流最新的独立硬件产品，虚拟化时必须使用非阵列计算资源，必须为原厂生产非OEM产品。体系结构为灵活可扩展。 |
| 虚拟化设备控制器 | 本次配置2个控制器，总共含有4个6核处理器，最大可以扩展到8个控制器。 |
| 端口数≥8个16Gb/s FC 主机接口，≥8个16Gb/s FC后端阵列接口 |
| 引擎支持IB互联，提高交换机速度 |
| 当前配置≥256GB 高速缓存，最大可以扩展到1024GB cache. |
| 虚拟化支持 | 通过硬件的方式将已有的阵列虚拟化管理，实现在本台存储设备上实现和EMC，Netapp,IBM,HP，HDS阵列的卷镜像保护。这样，当任何原有阵列中数据卷损坏时，都可以在当前阵列有完全同步的镜像保护数据。虚拟化必须以数据块为单位，而不是文件。最大虚拟化容量无限制。 |
| Vmware系列认证 | 要求提供对Vmware HA/Vmotion/Vmsc的支持。 |
| 功能实现 | 在单个群集内引擎之间实现存储域的自动共享、平衡和故障切换；能够在异构阵列之间移动生产卷并无主机中断或宕机；能够创建分条卷、联合卷和切片卷，并能够实现异构阵列镜像数据，可以在网络中创建一个异构存储池。可升级为跨多数据中心的实现高可用性和工作负载，支持同步或异步模式。 |
| 集群间通信 | 多控制器构成集群时，控制器间通讯通过额外的FC端口进行，不占用用于连接主机和存储阵列的FC端口 |
| 内置远程支持能力 | 所提供产品必须具备高级预警机制，免费配置功能软件。在系统发生故障前能将系统存在的潜在问题自动反馈到设备厂商技术响应中心。 |
| 连接数 | 通过FC端口连接主机，最大支持主机数量≥1600 |
| 最大卷支持数量≥12000个 |

### 7.3.29 存储光纤交换机

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 交换端口 | 本次配置48个线速端口,激活48个许可 |
| 供电和散热模块 | 冗余电源和冗余风扇 |
| 本次配置功能 | 配置Zoning功能模块，  配置远程长距离连接功能模块  配置Enterprise package license  配置VSAN技术和VoQ技术功能（相类似）  配置DCNM for SAN Licens（相类似）  配置Trunking链路捆绑功能模块  支持SNMPv3，SMI-S，TACACS+，AAA，SFTP |
| 模块和线缆 | 本次配置46个16G FC多模光模块和2个10KM以上单模16G光模块，满配相关线缆 |

### 7.3.30 存储光纤交换机

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 交换端口 | 本次配置48个线速端口,激活24个许可 |
| 供电和散热模块 | 冗余电源和冗余风扇 |
| 本次配置功能 | 配置Zoning功能模块，  配置远程长距离连接功能模块  配置Enterprise package license  配置VSAN技术和VoQ技术功能（相类似）  配置DCNM for SAN Licens（相类似）  配置Trunking链路捆绑功能模块  支持SNMPv3, SMI-S，TACACS+,AAA, SFTP |
| 模块和线缆 | 本次配置22个16G FC多模光模块和2个10KM以上单模16G光模块，满配相关线缆 |

### 7.3.31 虚拟化服务器

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 服务器外型 | 机架式 |
| 服务器高度 | ≥2U，标配原厂导轨 |
| CPU型号 | Intel Xeon E5-2630 V4，可支持≥135w处理器 |
| CPU实配数量 | ≥2颗 |
| 内存功能 | Advanced ECC、内存在线热备 |
| 内存实配规格 | ≥32GB\*8 2400 DDR4 |
| 内存可扩展数量 | 可扩展≥24个内存插槽，官方支持最大容量3T。 |
| 实配硬盘及托架 | ≥2\*600GB SAS 10k 硬盘，硬盘托架具备Raid重建时不可拔出硬盘提示指示灯。 |
| 硬盘槽位 | 配置≥8个2.5寸热插拔硬盘槽位，可扩展至≥26个2.5寸热插拔硬盘槽位 |
| 阵列控制器 | ≥1个标配SAS Raid阵列卡（不占用PCIE扩展槽），支持Raid0/1/10/5/6。 |
| 实配≥2GB缓存，支持缓存数据保护，且后备保护时间不受限制； |
| PCI I/O插槽 | 最多提供≥6个全高PCIE3.0插槽  当配15个3.5寸热插拔硬盘时须提供≥3个标准全高PCIE 3.0插槽。 |
| 网卡 | 本次配置≥4个10/100/1000M-BaseT 多功能以太网接口  要求额外提供≥1个网卡专用插槽（不占用PCIE扩展槽）  提供2个SFP+网口（含光模块），2块16G单口FC HBA卡（含模块） |
| GPU | ≥12个3.5寸热插拔硬盘时，可配置≥1块K2级别显卡 |
| 接口 | ≥5个USB3.0接口 |
| 冗余电源 | 2个≥500w铂金版热插拔冗余电源，可选服务器内部后备电池，断电情况下，支撑服务器运行≥60秒。 |
| 冗余风扇 | 热插拔冗余风扇 |
| 远程管理卡 | 配置≥1Gb独立的远程管理控制端口，配置虚拟KVM功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，支持3D图形化的机箱内部温度拓扑图显示，可支持动态功率封顶。  嵌入式管理工具支持联合管理功能，无需软件即可实现多台服务器统一管理功能，如监控硬件健康状况，固件升级等。  免费提供升级工具，无需安装代理即可可统一升级同一网络中服务器的固件及驱动程序。 |
| 多平台支持 | 支持Windows、Linux平台及MS SQL、Oracle数据库，支持B/S架构 |

### 7.3.32 备份服务器

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 服务器外型 | 机架式 |
| 服务器高度 | ≥2U，标配原厂导轨 |
| ▲CPU型号 | Intel Xeon E5-2630 V4及以上，可支持≥135w处理器 |
| CPU实配数量 | ≥2颗 |
| 内存功能 | Advanced ECC、内存在线热备 |
| 内存实配规格 | ≥64GB |
| 内存可扩展数量 | 可扩展≥24个内存插槽，官方支持最大容量3T。 |
| 实配硬盘及托架 | ≥8\*6TB硬盘，硬盘托架具备Raid重建时不可拔出硬盘提示指示灯。 |
| 阵列控制器 | ≥1个标配SAS Raid阵列卡（不占用PCIE扩展槽），支持Raid0/1/10/5/6。 |
| 实配≥2GB缓存，支持缓存数据保护，且后备保护时间不受限制； |
| PCI I/O插槽 | 最多提供≥6个全高PCIE3.0插槽  当配15个3.5寸热插拔硬盘时须提供≥3个标准全高PCIE 3.0插槽。 |
| 网卡 | 本次配置≥2块双口万兆以太网光纤网卡，含SFP模块。  要求额外提供≥1个网卡专用插槽（不占用PCIE扩展槽） |
| GPU | ≥12个3.5寸热插拔硬盘时，可配置≥1块K2级别显卡 |
| 接口 | ≥5个USB3.0接口 |
| 冗余电源 | 2个≥500w铂金版热插拔冗余电源，可选服务器内部后备电池，断电情况下，支撑服务器运行≥60秒。 |
| 冗余风扇 | 热插拔冗余风扇 |
| 远程管理卡 | 配置≥1Gb独立的远程管理控制端口，配置虚拟KVM功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，支持3D图形化的机箱内部温度拓扑图显示，可支持动态功率封顶。  嵌入式管理工具支持联合管理功能，无需软件即可实现多台服务器统一管理功能，如监控硬件健康状况，固件升级等。  免费提供升级工具，无需安装代理即可可统一升级同一网络中服务器的固件及驱动程序。 |
| 多平台支持 | 支持Windows、Linux平台及MS SQL、Oracle数据库，支持B/S架构 |

### 7.3.33 分布式存储

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 体系架构 | 要求采用全对称集群存储体系架构，无需增加专门的管理节点或管理服务器。无管理节点或元数据服务器；不接受服务器硬件加文件管理软件拼凑方式； |
| 文件系统 | 要求单一文件系统和单一卷≥15PB |
| 存储节点数量 | 不少于三个节点。 |
| 存储节点内部互连 | 采用QDR InfiniBand交换机互连，每个节点配置2个InfiniBand接口。 |
| Infiniband交换机 | 配置两个8端口的QDR Infiniband交换机及其相应配件，每个端口单向40Gb/s。 |
| 最大NAS头数量 | 支持最大NAS头数量>100 |
| 存储节点CPU数 | 每节点≥2个Intel Xeon四核处理器 |
| 存储节点Cache | 每节点≥12GB Cache,集群各存储节点全局缓存，总Cache≥36GB |
| 存储节点接口 | 每节点配置2个万兆带光模块前端NAS服务网络接口；管理网络端口除外。 |
| 存储节点容量 | 要求每节点配置36块2TB 7200RPM SATA硬盘 |
| 安装方便性 | 安装过程中，存储系统自动执行卷和文件系统初始化，不需要人工操作RAID配置、卷划分和文件系统配置。 |
| 零操作在线扩容 | 要求在存储集群扩展时，新节点连接到IB网络后，存储系统能够自动识别所加入的节点的容量，并自动合并所加入的空间。无需人工操作RAID配置、卷划分和文件系统配置。 |
| 可用性 | 要求存储系统任何一个节点发生故障，或两块在两个不同的节点上的磁盘同时发生故障时，存储系统不会停机，数据仍然保持完整。 |
| NDMP备份 | 支持备份功能。 |
| WORM功能 | 支持WORM功能，防止文件意外删除 |
| 数据自动条带化 | 存储系统能跨所有节点自动均衡条带化数据，每个节点上数据相差少于5%。 |
| 数据保护级别在线更改 | 文件系统中的文件可以根据需要分别设置不同的保护级别，并且能在线修改数据安全保护级别。 |
| 图形化存储管理软件 | 支持Telnet/SSH管理，提供基于Web浏览器的管理界面，管理界面简单易用。 |
| 文件和文件系统快照 | 要求支持整个文件系统、目录和子目录的快照。 |
| 配额管理 | 要求支持针对目录、子目录和用户、用户组的配额管理 |
| 连接管理 | 配置客户端连接管理软件，要求支持针对节点的轮询、CPU利用率、连接数和流量的均衡策略。 |
| 网络协议支持 | 同时支持NFS，CIFS，FTP，iSCSI，HDFS。 |
| 软件许可 | 配置负载均衡许可和配额管理许可。 |

### 7.3.34 服务器虚拟化软件

| **指标项** | | **指标要求** |
| --- | --- | --- |
| 服务器管理功能 | 基本管理要求 | 提供统一的图形界面管理软件，可以在一个界面完成服务器的日常功能和运维操作； |
| 提供强大的命令行工具，支持编制脚本实现虚拟化管理的自动化； |
| 提供开放的开发接口，支持其它应用的调用； |
| 高级集中管理 | 可以将多台服务器组合为服务器组，通过一个界面完成多台服务器的统一运维操作； |
| 服务器虚拟化功能 | 虚拟机独立性 | 利用Intel VT和AMD-V的硬件虚拟化技术，提供对硬件驱动的高性能访问； |
| 虚拟机之间可以做到隔离保护，每个虚拟机上的用户权限只限于本虚拟机之内，保障系统平台的安全性； |
| 虚拟机具有自己的资源（内存、CPU、网卡、存储），可以指定单独的IP地址、MAC地址等； |
| 虚拟机安全 | 支持受保护的虚拟机（Shielded Virtual Machines） |
| 异构支持 | 支持在Intel和AMD两个品牌或同一品牌不同CPU类型之间的服务器建立支持异构CPU的虚拟化资源池；  支持市面上主流的x86服务器，包括HP、Dell、联想等厂商的机架或刀片服务器； |
| 虚拟化资源池内的每个服务器都可以安装虚拟机，并且虚拟机操作系统可以异构。 |
| 兼容现有市场上X86服务器上能够运行的主流操作系统，具有双方认可的官方客户操作系统兼容性列表，包括不限于以下操作系统：WINDOWS 2003、WINDOWS 2008、WINDOWS 2012、WINDOWS 2016、REDHATLINUX、CENTOSLINUX、ORACLELINUX、SUSELINUX、FREEBSD、UBUNTU、DEBIAN等。 |
| ORACLE、IBM等主流应用厂商支持其应用运行于虚拟化技术之上的虚拟机中。 |
| 兼容现有市场上主流的存储阵列产品，如IP-SAN、FC-SAN、SAS和iSCSI，品牌包括EMC、IBM、HP、HDS、Netapp、Sun、Dell等，兼容现有市场上主流的网卡和HBA卡产品，包括Qlogic，Emulex，Brocade的HBA卡。 |
| 功能性要求 | 支持虚拟机实时迁移动能，可以在不停机的状态下，手工或自动地实现虚拟机在群集之内的不同物理主机之间迁移，保障业务连续性；  实时迁移无需依赖高可用群集和共享存储，支持位于本地存储的虚拟机在不同的物理主机进行迁移，迁移过程中不停机；  支持位于共享文件夹中的虚拟机实时迁移；  支持在群集内的不限数量的并发实时迁移，并可以查看实时迁移状态和队列； |
| 支持存储实时迁移，可以在不同的LUN之间迁移虚拟机存储，迁移过程中虚拟机不会停机； |
| 支持跨越软件和硬件交换机、跨越数据中心进行虚拟机在线复制、迁移，可实现远距离无中断实时迁移工作负载。 |
| 支持故障转移功能，当一台物理主机发生故障时，之上的虚拟机可以实现在虚拟化群集之内的其它物理主机上重新启动，保障业务连续性； |
| 支持资源动态优化，在物理主机的负载达到一定程度后，自动将高负载物理服务器上运行的虚拟机迁移到其它比较空闲的物理服务器上。支持按照CPU、内存、网络和磁盘设定相关阀值和策略实现负载均衡。 |
| 支持自动化的电源管理功能，在满足业务性能需求的前提下，根据各种业务工作负载情况整合物理服务器，使服务器数量最少；同时关闭不需要的服务器以降低整个系统的资源能耗。当业务需要更多的物理资源时自动开启服务器。整个过程系统自动完成； |
| 支持在线快照功能：在线为虚拟机打快照，可包括内存数据。在线删除快照时可立即合并增量数据，无需等待关机后再执行； |
| 支持虚拟机快照的创建、恢复及删除，并支持按照时间顺序以树状结构显示 |
| 支持存储空间功能，群集共享卷内可以包括多个LUN，支持在线增加LUN以扩展存储空间； |
| 支持最多将64台物理主机配置为单一群集，虚拟机可以在群集内实现实时迁移、故障转移，同时支持动态资源调节和电源优化功能，可以根据配置的策略自动调整虚拟机在物理主机上的分布；  单一群集至少支持8000台虚拟机的负载； |
| 支持虚拟机复制功能，可以在不同站点，不同物理主机和存储系统上进行虚拟机的复制，复制的副本虚拟机和原始虚拟机保持数据一致；  可制定复制的频率、次数，可随时检查复制状态，对复制进行检查；  支持对复制的虚拟机进行计划或非计划的故障转移，进行计划故障转移时保证数据的完整性，支持对故障转移进行测试； |
| 虚拟机可以配置CPU资源分配权重，并支持在线调整分配权重；  支持对内存的动态控制，可指定虚拟机的最小内存、启动内存和最大内存，并在指定范围内自动的根据虚拟机的业务运行自动的调整和调度内存的使用，在线动态增加和减少内存；  支持为虚拟机添加和删除网卡，在线的添加和删除SCSI虚拟磁盘； |
| 虚拟机支持直通磁盘访问，可以直接访问物理存储；  可以为虚拟机配置虚拟光纤通道卡，实现虚拟机对FC-SAN的访问，在实时迁移过程中，不会中断虚拟机对FC存储的连接； |
| 虚拟机支持动态、固定和差异三种类型的磁盘，支持对磁盘进行在线扩展和压缩； |
| 支持虚拟机导入、导出，同时支持在不导出虚拟机的情况下直接导入虚拟机； |
| 存储功能 | 存储虚拟化 | 支持直接将服务器本地磁盘或直连的JBOD盘柜中的磁盘配置为存储池，并从存储池中创建逻辑单元； |
| 支持分离式设计，虚拟化服务器可以通过常用的网络协议访问存储池中的逻辑单元，而无需直连存储设备， |
| 支持SMB3.0、iSCSI和NFS； |
| 支持在逻辑单元中进行数据去重和数据分层； |
| 支持在创建逻辑单元时设置可用性模式，支持包括Simple、双层和三层Mirror、Parity模式； |
| 支持存储服务器、磁盘和Enclosure多层级容灾功能，可以防止单个或多个存储服务器、磁盘和Enclosure损坏，且可有效恢复数据； |
| 分布式服务器存储，支持多个独立的服务器本地SSD或磁盘组成一个分布式的存储资源池，提供给虚拟化或其他应用使用。易于管理，并支持横向扩展 |
| 对存储的管理简单易行，可对存储容量进行扩展和容量性能平衡，制定存储QOS策略  提供基于存储策略的管理机制，可根据业务应用的需求，事先创建好相应的存储策略。之后，创建同一类业务应用的虚机时，无需进入存储管理界面，即可按分配存储资源，并支持通过变更存储策略进行在线的动态调整业务应用正在使用的存储资源  支持SSD作为高速读/写缓存，并且提供可以动态调整的虚拟机级别的读写缓存预留，确保重要应用的读写性能  可支持16节点数量组成高可用级  支持SSD和SAS/SATAHDD磁盘混合存储  支持NVME类型SSD作为读写缓存  支持使用JBOD存储，本地硬盘等形式  提供对存储资源的集中化管理界面，具备针对存储资源的硬件监控、合规性运行状况检查、容量规划和根本原因分析功能。 |
| 软件定义存储 | 支持直接存储空间技术以及存储复制技术（Storage features including Storage Spaces Direct and Storage Replica） |
| 可扩展文件服务器 | 提供基于SMB 3.0的文件共享访问。服务器消息块（SMB）客户端连接以每个文件共享（而非每台服务器）为单位进行跟踪，客户端接着被重定向至文件共享使用的对卷有最佳访问能力的集群节点。通过降低文件服务器节点间的重定向数据传输，提高运行效率；  客户端会根据初始连接，以及当集群存储被重新配置时被重定向；  客户端会根据本地和共享服务器的网卡数量，自动配置使用多块网卡同时访问文件共享，提供网络性能； |
| 如果服务器网卡支持RDMA功能，SMB3.0会自动使用RDMA功能，减少网络访问延迟； |
| 网络功能 | 虚拟化网络功能 | 支持外部网络、内部网络和私有网络三种类型虚拟网络，虚拟机可以通过外部网络和物理网络联通； |
| 支持虚拟机之间的通信可以配置为通过同一主机的内部虚拟交换网络； |
| 支持对虚拟机交换机及端口进行VLAN设置，支持同一物理主机上虚拟机之间的网络隔离； |
| 支持网络虚拟化技术，提供同一物理网络上多个虚拟网络隔离的能力；提供基于软件定义的虚拟网络网关、负载均衡器，虚拟网关需能支持站点到站点和点到站点的VPN； |
| 支持在操作系统中配置可扩展交换机，可将第三方开发的虚拟交换机软件添加到操作系统中，扩展操作系统网络管理功能； |
| 支持宿主机至少32块网卡绑定，支持虚拟机内多网卡绑定，虚拟机网卡绑定不依赖与网卡驱动，不同型号和厂家的网卡可以进行绑定； |
| 支持对虚拟机网络流量进行带宽控制； |
| 支持对通过虚拟交换机的流量进行计量； |
| 支持SR-IOV技术，虚拟机可以直接使用物理网卡虚拟功能模块，提高虚拟机网络性能； |
| 软件定义网络 | 软件定义网络方案，可从底层硬件分离网络并对网络基础架构应用虚拟化策略，能够在软件中重现整个网络连接环境，包括每个虚拟网络中的L2、L3 和L4–L7 网络服务。  支持虚拟化平台软件(HYPERVISOR)的软件网络及安全构件，包含控制节点、软件交换机、软件路由器、软件防火墙、软件网关等虚拟网络能力。  各软件交换机、软件路由器、软件防火墙应具备同高带宽、高并发能力。  控制节点应作为统一的虚拟网络服务管理点，提供基于图形和脚本模式下的配置管理界面。  控制节点支持高可用模式，至少支持3台控制节点实现的高可用架构。  控制节点与其他软件虚拟网络组件之间应基于X.509证书模式的加密通讯。  控制节点应提供RESTFULAPI接口进行调用。  可创建多个基于租户概念的逻辑网络，并且各逻辑网络是相互隔离。  在各逻辑网络中，网络子网是可以重复的，在各自逻辑网络中的资源对其他逻辑网络中的资源没有感知。  逻辑网络内可支持多个自定义的网络子网。  逻辑网络的入站和出站通讯均支持ACL控制。  同一逻辑网络可以分布在不同的虚拟化主机上，虚拟机可以在不同的虚拟化主机上访问到相同的逻辑网络。  支持快速部署逻辑网络，支持脚本化、配置文件等模式下的部署。  分布式防火墙可以分布在边缘和核心网络区域进行防护。支持基于资源组或者标签的方式，对资源对象集合进行ACL控制。  ACL访问控制策略可以跟随虚拟机进行应用，即使虚拟机被迁移到其他虚拟主机上运行。  软件负载均衡组件应支持网络4层级别负载均衡模式，支持对内NAT和对外NAT转换。  在虚拟机启动时自动应用安全策略，在迁移虚拟机时移动安全策略，在取消调配虚拟机时删除安全策略  可按需提供基于虚拟机的网络边界网关的网络边界网关，为虚拟机提供路由器、防火墙、负载均衡器等网络服务。  提供与网络封装覆盖(OVERLAY)的交换机制(VXLAN/NVGRE)，可支持在不限定网络设备品牌的基础上创建软件交换机，且修改软件交换机时不需要对底层的实体网络进行设定的更改。  提供网络流量监控功能(FLOWMONITORING)，可针对方案内防护的虚拟机的进出流量。  方案内软件负载均衡器可支持以下功能：  • TCP / UDP / HTTP / HTTPS等协议的负载均衡机制  • 负载均衡机制支持ROUND-ROBIN / IPHASH / LEASTCONNECTION等方式进行  • 可以后端应用服务器进行健康检查(HEALTHCHECK)  支持虚拟交换机，并且支持VXLAN/NVGRE封装协议。  VXLAN/NVGREVTEP支持多网卡的负载均衡机制，可基于LACP、MAC或IP作为分配条件。  软件路由器需支持分布式的功能，由虚拟化平台软件（HYPERVISOR）直接判断虚拟网络内三层东西向的端到端通信  支持分布式防火墙的功能，由虚拟化平台软件（HYPERVISOR）直接判断虚拟网络的在线访问能力。  支持网络边界的软件功能，包含负载均衡、NAT等功能。  支持软件负载均衡器，并且支持ROUND-ROBIN,IPHASH, LEASTCONNECTION等负载均衡机制。  支持网络堆栈（Software Defined Networking (SDN) Stack） |
| 通用网络服务支持 | 提供用户、用户组管理功能  提供统一用户授权功能  提供DNS服务  提供DHCP服务  提供传真服务器  提供文件及存储服务  提供终端计算机统一管理  支持通过策略对终端计算机进行统一管理（包括配置修改、行为限定等）  支持通过LDAP进行帐户和网络资源管理，并支持通过策略统一管理帐户权限，目录服务对象包含但不限于用户帐户、计算机帐户和打印机等。 |
| 高可用功能 | 故障转移群集功能 | 支持配置为主备或多活模式群集；  支持自动配置仲裁，支持基于共享磁盘、共享文件夹、节点多数三种仲裁模式；  支持在故障转移群集中配置虚拟化、DNS、DHCP、文件共享、分布式文件系统、数据库等多种资源高可用；  支持资源反关联和关联性配置； |
| 故障转移群集指标 | 每个虚拟机高可用性群集至少支持8000个虚拟机；  每个高可用性群集至少支持64个节点； |
| 网络负载均衡 | 支持配置网络负载均衡； |
| 数据要求 | 每个宿主机至少支持512个逻辑CPU；  每个宿主机至少支持24TB物理内存；  每个虚拟机至少支持240个虚拟CPU；  每个虚拟机至少支持16TB内存； |

### 7.3.35 操作系统

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 操作系统 | windows 2012Datacenter版 |

### 7.3.36 Oracle数据库

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 数据库企业版 | Oracle Database Enterprise Edition 4 Processor Fulluse License (Oracle数据库企业版完全许可4 CPU ) 含原厂一年标准服务，允许迁移和升级, 合法授权类型： Full Use。 |
| 真正应用集群 | Real Application Clusters 4 Processor Fulluse License  (RAC完全许可4 CPU )  RAC允许多个数据库实例以集群方式运行在多个服务器上，并且共享一份数据文件（数据库）。RAC消除了单点故障，也提供了更好的性能扩展，含原厂一年标准服务。 |
| 数据库企业版要求 | 支持当前最流行的数据库技术标准；完全支持中文国家标准中文字符的存储处理。  支持数据库多版本读写一致性及自动的死锁处理能力；支持范围、列表、哈希、组合、引用、间隔等多种表分区方式。  支持多级增量备份；支持不依赖于第三方软件的异地容灾方案，且容灾数据库可打开用于查询等操作；必须支持数据库闪回技术，能保障数据准确恢复到以前某个时间点。  支持C2级安全标准，多级安全控制；支持透明数据加密、标签安全等数据库安全特性。  支持主流硬件平台及操作系统（Windows/Linux/Unix等)；支持主流的网络通信协议；支持具有广泛适应性的开发语言和工具(VC/JAVA/XML等)。  支持多个数据库共享一套硬件资源和后台进程的能力，具有将多个数据库作为一个进行管理，并且保留独立数据库的数据隔离和资源优先级。  支持单一的B/S模式管理控制台，要求数据库提供自我诊断、自我调优功能。 |
| 真正应用集群要求 | 要求与数据库产品同一厂商；要求是基于共享存储的真正应用集群系统，可同时应用与OLAP和OLTP环境，支持负载均衡和秒级自动故障切换功能，集群可水平扩展至上百节点，增加节点无需停机；要求集群产品在国内具有多个成功案例。 |
| 服务 | 提供一年标准服务。 |

### 7.3.37 SQL数据库

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| SQL数据库 | Sqlserver 2016企业版 |

### 7.3.38 数据库容灾软件

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 灾备架构总体要求 | 要求采用灾备复制软件实现主备中心之间的文件、数据实时复制，当生产系统发生故障或灾难时，可以及时启用灾备系统，减少业务系统下线时间。并要求灾备中心数据库始终处于Open状态，用于提供数据查询和统计报表功能。通过独立开发实现数据库日志分析、交易排序、数据格式化、传输压缩、高速装载等数据同步全部过程，不接受使用操作系统或者数据库自带工具参与投标。 |
| 基本功能要求 | 支持对文件数据的同步，包括应用程序、图像数据、音视频数据、网站文件等；支持Oracle、MYSQL、SQLSever等异构数据库的交易复制，且灾备数据库始终处于Open状态； |
| 容灾软件License满足Unix(X86平台，RAC或HA模式）到X86平台的oracle数据库复制需求 |
| 要求支持任意数据库版本，硬件平台异构实时灾备 |
| 要求具有备份模块 |
| 资质 | 产品需具有国家版权局颁发的《软件著作权登记证书》，具有自主知识产权，独立研发能力。 |
| 产品需具有国家信息中心软件测试报告； |
| 兼容性要求 | 容灾及备份软件支持主流操作系统：Linux、HP-UNIX、Sun Solaris、IBM AIX、Windows； |
| 支持HA和RAC模式； |
| 支持Oracle、Sql、Mysql、Hadoop、Db2、人大金仓、神州通用等数据库跨数据库种类的数据交易复制；且灾备库始终处于Open状态，实现业务系统读写分离，灾备系统查询分析等服务； |
| 在数据迁移初始化同步过程中，业务不能停止；异构平台或跨数据库版本之间的数据初始化过程中不需要人工干预； |
| 技术指标要求 | 系统资源占用少，保证主机的正常运行； |
| 源端CPU占用小于3％；内存占用小于200M； |
| 目标端CPU占用小于3％；内存占用小于200M； |
| 一体化同步要求 | 启动同步后，软件自动实现全同步和增量同步操作，‘一键式’执行，无需人工干预。支持异构平台下的首次数据初始化同步。支持跨数据库版本之间数据库的初始化同步操作。 |
| 应用系统等文件数据的容灾功能要求 | 针对用户的应用系统，需要具有提供实时容灾的功能，当主机上的应用软件出现配置调整或者其他变化的时候，由软件实现同步复制功能。 |
| 文件同步功能可支持基于用户管理策略规则，用户可对指定文件进行同步； |
| 文件发生变化后，可以识别变化的部分，只需要传输变化的部分，而不需要重新传输整个文件； |
| 支持镜像保存整个目录树和文件系统； |
| 可保持原来文件的权限、时间、软硬链接； |
| 优化的流程，文件传输效率高；无须特殊权限即可安装； |
| 可以使用rcp、ssh、socket等方式来传输文件 |
| 文件传输可设定压缩选项，来降低网络带宽需求； |
| 数据库在非归档模式下，也可以增量备份。 |
| DDL支持要求 | 支持从数据库日志中分析所有DDL操作，不影响整个同步过程。 |
| 智能化要求 | 在源端数据库数据结构发生变化(如修改表结构，增加表等)后，复制软件可自动将新增结构变化同步到目标端。 |
| 数据库的容灾功能要求 | 支持一对一，双向，一对多，多对一，和级联复制； |
| 支持数据转换、数据拆分及分发； |
| 支持从多个数据库中同一类型表的记录整合到一个表中去； |
| 支持对列的数据进行转换，包括列映射、增/删除列、列转换 |
| 支持DML操作复制、支持SEQUENCE、函数、存储过程、视图、同义词、索引、应用包、用户等数据库对象进行复制； |
| 支持没有PK/UK字段的表的复制、并无需打开或修改数据库参数，可定义并过滤不需要复制的事务； |
| 支持按照schema方式设置复制关系，无需单表设置复制关系，支持不同源和目标端在不同的schema名情况下的复制； |
| 支持中文汉字内码，符合双字节编码；支持自定义数据格式的装载；支持数据详细地址的方式实现数据快速定位； |
| 文件复制系统 | 实现应用系统实时同步灾备要求，要求软件各种操作系统的文 件复制，且灾备服务器始终处于可用状态；具有软件著作权证书；(提供复印件) |
| 灾备切换导航监控 | 可以监控并管理数据库灾备软件和文件复制灾备软件，中文操作界面，灾备导航和主备一键切换图形化操作，实现对灾备软件的运行状态、运行日志、系统配置等方面进行统一的管理及监控；识别异常并发出以短信/邮件等形式的告警信息； |
| 故障应对能力 | 1、  在遇到系统错误引起的复制中断时，例如硬件故障、数据库故障、网络中断或延迟，分级存储机制能完好的保存已经合成的交易信息，避免数据丢失，直到系统故障解决，恢复从队列传输的中断点开始；（提供软件截图） |
| 2、  系统需提供数据比对功能，如果发现不一致情况后能够提供便利的单表以及单用户的数据修复工作，要求操作简单，修复速度快，且修复过程中不影响业务正常运行；（提供软件截图） |
| 3、  生产灾备切换后，支持快速的增量回切、全量回切功能； |
| 管理监控功能 | 1、要求提供中文操作界面； |
| 2、复制软件需提供统一的管理监控功能，能实现对复制软件的运行状态、运行日志、系统配置等方面进行统一的管理及监控（提供软件截图）； |
| 3、系统软件应具有故障的监视和诊断能力，出现不正常情况时，应能及时识别并发出告警信息； |
| 审计功能 | 通过分析Oracle数据库的日志对数据库操作进行监控，具有记录，留痕，报表回溯等功能。（提供软件截图） |
| 归档功能 | 按照客户要求将使用频度低的数据一次性(从数据库文件读取)或者连续归档(分析数据库日志)到目标数据库中，并在源端进行数据清理，从而减少源库数据量，提升系统效率，分担系统压力。（提供软件截图） |
|
|
| ▲服务要求 | 1、原厂负责首次安装调试、现场培训及售后服务，并出具2年现场7X24响应、4小时到现场、原厂10个现场人/天，软件免费升级，无节假日限制的服务承诺；（中标后提供） |
| 2、投标方在标书中详细描述初始化数据同步解决方案。 |
| 3、投标方在标书中详细描述数据迁移方案。 |

### 7.3.39备份软件

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 1 | 单一产品同时支持备份、还原、复制和容灾解决方案 |
| 2 | 全面支持VMware vSphere平台和Microsoft Hyper-V平台 |
| 3 | 无须在每一台虚拟机上安装代理程序 |
| 4 | 无代理方式备份、还原关键应用（Oracle, SQL, Exchange, SharePoint, AD活动目录以及其它应用系统） |
| 5 | 支持应用程序一致性的映像级虚拟机备份和复制 |
| 6 | 能够通过vCenter或者单个ESX /ESXi主机, 充分利用VSphere API进行数据保护 |
| 7 | 支持VMware vSphere的块改变跟踪（CBT）技术, 或Microsoft Hyper-V虚拟机的 弹性变化跟踪（RCT）技术进行备份 |
| 8 | 能够在备份作业运行期间动态的增加新虚拟机 |
| 9 | 支持LAN-free方式备份 |
| 10 | 支持连续的作业计划，当一个备份完成立即开始新备份，以达到接近CDP的数据保护 |
| 11 | 支持thin模式和thick模式磁盘分配的虚拟机 |
| 12 | 支持设置不同的用户权限，设置特定的用户只能查看备份状态或者进行恢复操作 |
| 13 | 在设定的时间段内，过期的虚拟机备份镜像文件可以自动删除以节省存储空间 |
| 14 | 支持备份到磁盘、LTO规格的磁带（备份和归档文件到磁带,归档备份文件到磁带）、以及具有去重功能的专业备份设备，例如：EMC DataDomain、HPEStoreOnce或某些公有云 |
| 15 | 提供基于网络访问的企业控制台用于监控、管理、备份、恢复和统计等管理操作 |
| 16 | 能够支持整个虚拟机恢复、虚拟机文件、虚拟磁盘恢复，支持直接从备份文件中启动虚拟机和业务系统，同时支持将备份虚拟机直接恢复到公有云中 |
| 17 | 能够提供Guest OS层面的文件级即时恢复 |
| 18 | 能够从EMC、HPE、NetApp、Nimble等企业存储级快照中恢复单个虚拟机、客户机操作系统文件或应用程序及程序中的子项目 |
| 19 | 能够备份并恢复虚拟机的配置文件，比如vSphere虚拟机的vmx文件 |
| 20 | 能够支持无代理应用-条目级恢复（用于MS SQL 、Exchange、AD 、SharePoint、Oracle以及其它应用） |
| 21 | 能够搜索和还原所有AD对象类型，包括用户、组、计算机账号、联系人以及计算机密码的恢复，多选还原、容器恢复、组策略对象还原等 |
| 22 | 能够实现对单个Exchange项目（电子邮件、备份、联系人）、硬删除项目的项目恢复，支持还原回原始邮箱 |
| 23 | 还原单个 SQL 数据库，支持本地时间点导出 SQL 数据库文件，无代理事务日志备份和重播，支持将数据库和 SQL 对象（表、存储的程序、视图等）事务级还原至原始或新 SQL 服务器的功能 |
| 24 | 支持 SharePoint 细粒度还原并可对还原的项目执行保存、发送和导出操作。还支持还原至原始位置的功能 |
| 25 | 还原单个 Oracle 数据库，包括无代理事务日志备份、存档日志管理以及将数据库事务级还原至原始或新Oracle 服务器的功能 |
| 26 | 可通过 Web 用户界面进行一键式的自助式恢复，包括文件、应用程序和虚拟机等 |
| 27 | 通过Web页访问的方式，可将恢复任务委派给特定用户或用户组，从而能够实现所有 Web UI 自助恢复功能 |
| 28 | 支持对备份I/O进行设置，以确保备份和复制活动不会影响用于满足生产负荷的存储可用性 |
| 29 | 支持通过利用存储快照技术（EMC、NetApp、HPE、Nimble、Cisco HyperFlex等）来备份和复制虚拟机，减低物理服务器负载，实现更快速的虚拟机和应用程序保护 |
| 30 | 支持NFS直接访问，可通过基于文件的 (NFS) 主存储中直接备份，能够更快地执行 VSphere 备份、复制和还原，并降低对虚拟化环境的影响 |
| 31 | 支持正向增量/反转增量/合成全备份等备份方法 |
| 32 | 能够从备份作业中排除虚拟机特殊类型的虚拟磁盘、单个文件或者文件夹，支持排除临时文件块以及交换空间、被删除文件块等无效数据块 |
| 33 | 加密、重复数据删除和压缩功能已内嵌在软件中无须额外购买 |
| 34 | 支持重复数据删除,可根据不同的网络环境来自定义数据去重的块大小 |
| 35 | 可以并行和顺序处理备份作业 |
| 36 | 支持广域网加速器，提升广域网容灾的性能 |
| 37 | 支持横向扩展式备份存储库，通过由软件定义的单一备份存储库来管理多个异构存储设备，可提升备份性能，降低存储硬件开支，降低维护风险 |
| 38 | 提供CDP级别的复制容灾功能，内置在产品中无须额外购买 |
| 39 | 能够从生产中心和容灾中心的备份文件快速启动虚拟机接替生产，而无需将备份文件先恢复到生产存储 |
| 40 | 提供一键故障切换协调机制，通过流程式的故障切换机制减低故障切换风险 |
| 41 | 自动验证备份映像和复制副本以确保虚拟机和应用程序可正常恢复,无需人工干预。自动检查相应虚拟机，操作系统和应用程序来确保可恢复性。验证报告邮件可配置为自动向管理员发送 |
| 42 | 支持在隔离环境内直接从备份或者复制副本运行一个或多个虚拟机，能够在不影响业务运营的情况下进行故障排除、测试 |
| 43 | 支持使用存储快照创建完全隔离的生产环境副本，以便快速轻松地进行测试和故障排除 |
| 44 | 任务自动化支持RESTful API 和 PowerShell命令 |
| 45 | 支持 VMware vSAN深度集成，且获得VMware ready官方认证. |
| 46 | 支持从vSAN智能读取数据，选择最佳备份路径；并支持VMware SPBM策略的自动备份和还原 |

### 7.3.40 CDP连续数据保护

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 总体要求 | 要求:能够在核心存储内部保存应用程序故障时间点之前任意时刻内应用数据的持续恢复点，或者采用虚拟化存储的方式实现并采用持续快照方式记录所有持续恢复点，要求数据复制完全基于存储,IP或SAN网络,而无需在服务器上附加其它软件模块或者改变当前服务器上卷组的配置，当生产数据故障时，可以通过持续恢复点把生产数据恢复到生产数据故障前的任意时间点。配置数据保护装置，该装置配置2个独立的Active的控制器，每个控制器配置>=2 颗4核Intel Sandy Bridge 处理器，配置>=16GB高速缓存，配置>=2块300GB SAS硬盘，配置4端口8GB HBA卡,6个千兆IP端口，可以通过添加更多控制器，实现性能的线性扩展，当前系统内控制器数量可扩展至八个以上，可以捕获并记录每一个写I/O操作，当数据需要恢复时，用户可从时间点中选择，使应用程序能够基于以前的事务快速地从任一时间点恢复，或者提供尽可能多的恢复时间点。采用“带外”基于SAN网络的应用装置，不在主机I/O 路径中进行监控和数据保护，不影响主机性能。 |
| 保证应用数据的一致性 | 提供一致性组功能，可以将某个特定应用程序的所有LUN绑定到一个一致性组中，以确保事务向以前时间点的回滚同时进行，从而确保应用程序的一致恢复 |
| 数据保护方式 | 对于捕获的写I/O，既支持复制到本地站点，也支持复制到远程容灾站点，提供对同一数据卷的并行本地和远程保护，为未来做远程数据保护奠定基础，本次配置本地站点复制方式。 |
| 目标端处理功能 | 支持在执行故障切换之前装载复制的映像以处理和检查一致性的能力 |
| 支持操作系统 | 支持各种主流操作系统，包括AIX，HP-UX，Solaris，RedHat Linux，SuSE Linux，Windows，VMWare ESX等。 |
| 支持存储类别 | 支持EMC，HDS，HP ，IBM，LSI，SUN，NetApp等多家存储 |
| 集群软件支持 | 支持HACMP、HP Service Guard、MSCS、Oracle RAC、VCS等多种集群软件 |
| 多路径软件支持 | 支持DMP、ESX Native、HDLM、HP-MPIO、MPIO、PowerPath、RDAC、SDD-DSM等多路径软件 |
| 管理界面 | 提供可在多种主机系统上运行的基于 Java 的管理界面，使管理员能够集中管理所有的操作，包括设置复制关系和参数、查看复制状态、恢复到某一时间点，和启动生产故障切换等。 |

### 7.3.41 灾备主机

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 服务器外型 | 机架式 |
| 服务器高度 | ≤4U，标配原厂滑动导轨 |
| CPU型号 | Intel Xeon E7-4830v4 处理器 |
| CPU实配数量 | ≥4颗 |
| 内存功能 | 高级ECC、在线备用内存、内存镜像、故障内存隔离、DDDC/SDDC等 |
| 内存实配规格 | ≥32GB\*8 DDR4 2400MHz |
| 插槽数量 | 可扩展≥96个内存插槽 |
| 内存可扩展数量 | 最大容量支持≥6T容量 |
| 实配硬盘及托架 | ≥2\*600GB SAS 15k 2.5寸硬盘， |
| 硬盘扩展能力 | ≥最大支持10个2.5寸硬盘槽位 |
| 阵列控制器 | ≥1个阵列卡专用插槽（不占用PCIE扩展槽），配置12Gbps SAS磁盘阵列控制器，支持Raid0/1/10/5/6，调整缓存读写比例等功能。 |
| 实配≥2GB缓存，支持缓存数据保护，且后备保护不受时间限制； |
| 支持Raid 1/10 |
| PCI I/O插槽 | ≥9个PCI-e 3.0全高/全长插槽 |
| 网卡 | 标配1个网卡专用插槽（不占用PCIE扩展槽），可选配千兆或万兆网卡。本次配置≥4个10/100/1000M-BaseT 多功能以太网接口，2个双口万兆光口网卡（含4个SFP+光模块），2块单口16G FC HBA卡(含2个SFP模块) |
| 冗余电源 | 4个≥1200W铂金版热插拔冗余电源（2+2冗余） |
| 冗余风扇 | 热插拔冗余风扇 |
| 远程管理卡 | 配置≥1Gb独立的远程管理控制端口，配置虚拟KVM功能, 可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、更新Firmware、虚拟软驱、虚拟光驱、虚拟文件夹等操作，提供服务器健康日记、服务器控制台录屏/回放功能，能够提供电源监控，可支持动态功率封顶，提供国家强制性产品认证证书，，并配置支持上述功能的授权。 |
| 售后服务 | 提供原厂商3年7x24技术支持服务 |

### 7.3.42 Kvm切换器

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| KVM | 16端口Cat 5高密度KVM多电脑切换器，配置16个转换模块 |
| Lcd套件 | 整合17寸LCD、超薄键盘，Touch Pad鼠标触摸板，集成在1U高度单元内 |

8 项目建设要求

## 8.1 项目实施进度要求

合同签订后，总工期不得超过2个月。

## 8.2 项目培训要求

对系统使用人员、系统运行维护管理人员等不同对象的培训计划；

培训课程安排、培训方式及时间；地点场所由采购人提供；

提供系统日常维护系统培训：主要面向医院信息管理技术人员（至少2名）进行现场培训，使其具备独立进行系统日常维护、故障的诊断与处理等方面的培训。

## 8.3 项目验收要求

项目的工作内容及成果文档的提交应覆盖以下内容，电子文档是成果不可分割的部分

1. 系统的体系架构及描述；
2. 提供所有本项目软件系统相关的源码，以便后续的自行更新维护；
3. 提供的其它技术手册，包括：

需求分析报告（含软件功能需求与数据要求）；

系统实施确认书；

软件培训资料；

程序安装维护手册；

软件使用操作手册；

项目验收报告。

## 8.4 项目售后服务要求

1. 投标人必须根据本次招标文件所制定的目标和范围，提出相应的售后服务方案。
2. 中标后签订合同前，投标人必须提供原厂商针对本项目的3年原厂服务承诺函原件，产品厂商要求在台州或温州地区设有产品备件库。（招标文件里单独标明的除外）
3. 为了保证本次项目顺利成功，要求投标人承诺项目验收后提供三年供应商及原厂的质保，7\*24小时售后技术服务，包括免费升级、功能完善、故障排除、性能调优、技术咨询等。（招标文件里单独标明的除外）
4. 投标人须保证所提供产品具有合法的版权或使用权，本项目采购的产品，如在本项目范围内使用过程中出现版权或使用权纠纷，应由中标人负责，采购人和采购机构不承担任何责任。
5. 投标人应为用户提供系统培训，使其能对系统熟练的操作和日常的维护以及能对一般系统故障进行处置。
6. **商务需求**

**1、质保期：**货物通过最终验收之日起三年（36个月）（招标文件第二部分技术参数另有规定的除外），货物上标明的质量保证期超过以上规定期限的，以标明的质量保证期为准。在质量保证期内，供应商对由于产品设计、工艺、材料、配套件的缺陷而造成的任何产品质量问题或故障负责。

**2、交货时间及地点：**同前面“招标项目一览表”内所填的相关内容。

**3、付款条件：**在合同签订前卖方提供合同总金额5%的履约保证金，如卖方在签约前未在规定的时间内提交履约保证金则买方有权拒签合同；设备安装调试验收合格后，买方向乙方支付100%的合同价款，履约保证金转为质量保证金，质量保证金待质量保证期满后无质量问题无息一次性退还；卖方开具可抵扣专用增值税发票。

**四、相关说明**

**1、投标文件份数：**资格资信证明文件、技术文件各需正本1份，副本7份；报价文件1份。报价文件、资格资信证明文件、技术文件各自密封（正本分别单独密封于一袋，所需副本可统一密封于一袋或多袋）。除报价文件外其余一律不准出现数字报价。如有不同标段，请按标段号分别装订，密封要求同上。

2、电子文件与纸质文件有出入的，以纸质文件为准。

**第三部分 投标人须知**

**一 、总 则**

**（一） 适用范围**

本招标文件适用于本次项目的招标、投标、评标、定标、验收、合同履约、付款等行为（法律、法规另有规定的，从其规定）。

**（二）定义**

### 1、招标人：是指组织本次招标的台州市政府采购中心。

2、采购人：是指委托招标人采购本次项目的国家机关、事业单位和团体组织。

3、投标人：是指向招标人提交投标文件的单位或个人。

4、货物：是指各种形态和种类的物品，包括原材料、燃料、设备、产品等。

5、产品：是指供方按招标文件规定，须向采购人提供的一切设备、保险、税金、备品备件、工具、手册及其它有关技术资料和材料。

6、服务：是指除货物和工程以外的政府采购对象，包括各类专业服务、信息网络开发服务、金融保险服务、运输服务，以及维修与维护服务等。

7、项目：是指投标人按招标文件规定向采购人提供的产品和服务。

8、“书面形式”包括信函、传真等。

9、“▲”系指实质性要求条款。

**（三）投标费用**

不论投标结果如何，投标人均应自行承担所有与投标有关的全部费用（招标文件有相反规定除外）。

**（四）特别说明**

1、投标人投标所使用的资格、信誉、荣誉、业绩与企业认证必须为本法人所拥有。投标人投标所使用的采购项目实施人员必须为本法人员工（或必须为本法人或控股公司正式员工）。

2、投标人应仔细阅读招标文件的所有内容，按照招标文件的要求提交投标文件，并对所提供的全部资料的真实性承担法律责任。

3、投标供应商所标产品除招标文件中明确规定要求“提供官网截图或相应检测报告的证明材料”以外，所有技术参数描述均以投标文件为准。**投标供应商对所投产品技术参数的真实性承担法律责任。**项目招标结束后、质疑期限内，如有质疑供应商认为中标供应商所投产品、投标文件技术参数与招标需求存在重大偏离、错误、甚至造假的情况，应提供具体有效的证明材料。

4、投标人在投标活动中提供任何虚假材料,其投标无效，并报监管部门查处；中标后发现的,中标人须依照根据《中华人民共和国政府采购法》第七十七条第一款第一项之规定，处以采购金额千分之五以上千分之十以下的罚款，列入不良行为记录名单，在一至三年内禁止参加政府采购活动，有违法所得的，并处没收违法所得，情节严重的，由工商行政管理机关吊销营业执照；构成犯罪的，依法追究刑事责任。

### 5、投标人不得相互串通投标报价，不得妨碍其他投标人的公平竞争，不得损害采购人或其他投标人的合法权益，投标人不得以向采购人、评标委员会成员行贿或者采取其他不正当手段谋取中标。

### 6、为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

7、关于小微企业投标

小微企业投标是指符合《中小企业划型标准规定》的投标人，通过投标提供本企业制造的货物、承担的工程或者服务，或者提供其他小微企业制造的货物。本项所指货物不包括使用大、中型企业注册商标的货物。小微企业投标应提供《小微企业声明函》；提供其他小微企业制造的货物的，应同时提供制造商的《小微企业声明函（制造商）》。

**二、招标文件**

（一）招标文件：招标文件由招标文件总目录所列内容组成。

（二）招标文件的澄清或修改

1、在提交投标文件截止时间十五日前，招标人可视采购具体情况对已发出的招标文件进行必要的澄清或修改，并以书面形式通知所有招标文件的收受人，投标人在收到该通知后应立即以传真的形式予以确认。招标文件的修改书将构成招标文件的一部分，对投标人有约束力。

2、招标人可视采购具体情况，酌情延长投标截止时间和开标时间，招标人会在提交投标文件截止时间三日前，将变更时间书面通知所有招标文件收受人。如有误期，其投标将被拒绝。

3、投标人在规定的时间内未对招标文件提出疑问、质疑或要求澄清的，将视其为无异议。对招标文件中描述有歧义或前后不一致的地方，评标委员会有权进行评判，但对同一条款的评判应适用于每个投标人。

**三、投标文件**

（一） 投标文件的要求

1、投标人应仔细阅读招标文件的所有内容，按照要求详细编制投标文件，并保证投标文件的正确性和真实性。

2、不按招标文件的要求提供的投标文件将被拒绝。

（二）投标文件的组成

投标人接到招标文件后，按照招标人的要求提供：资格资信证明文件、技术文件和报价文件。

**1、资格、资信证明文件**（附件1）

（1）声明书 (须包含参加政府采购活动前3年内在经营活动中没有重大违法记录的内容，见附件2)；

（2）法定代表人授权书（法定代表人亲自办理投标事宜的，则无需提交本证明书，见附件3)；

（3）营业执照、税务登记、组织机构代码证、社会保险登记证；

（4）上年度企业资产负债表及损益表；

（5）本项目要求的特定资质证书（对应第一部分第四条第（二）款）（见附件5）；

（6）投标人情况介绍（如主要产品、技术力量、生产规模等等所有有必要介绍的情况，见附件4）；

（7）投标人通过的质量管理和质量保证体系、环保体系、自主创新或其他体系等的认证证书或文件；（见附件5）；

（8）资信及商务需求响应表（见附件6）；

（9）近三年来类似项目的成功案例（投标人类似项目实施情况一览表、合同复印件及其相应的发票、用户验收报告等；见附件7）；

（10）产品代理资格证明和制造商授权证（一般不需，视情选用）；

（11）投标人认为可以证明其能力或业绩的其他材料；

说明：所有按上述要求提供的资格、资信证明文件应均为有效期内的，若提供的文件是扫描件或是复印件的必须加盖单位公章，方能做入投标文件。

**2、技术文件**（附件8）

（1）对本项目的具体响应方案（对应第二部分）：

①功能说明、性能指标及设备选型说明（质量、性能、价格、外观、体积等方面进行比较和选择的理由及过程）；

②提供产品出厂标准、质量检测报告。

（2）设备配置清单（均不含报价）（附件9）；

（3）主要货物用材响应表(类似家具类货物采用) （附件10）；

（4）技术需求响应表（填制时对应第二部分）（附件11）；

（5）保证工程质量的技术力量及技术措施；

（6）保证工期的施工组织方案及人力资源安排；

（7）项目实施人员一览表（根据项目实施的内容、标准和实际情况拟配置各人员的具体情况见附件12 ）；

（8）项目负责人资格情况表（附件13）；

（9）技术服务（含服务方式、服务网点等）、技术培训、售后服务的内容和措施（附件14）；

（10安装、调试及验收方案（包括项目验收标准和验收方法等）和措施；

（11）投标人需要说明的其他内容（格式自拟）。

**3、报价文件**（附件15）

此报价为投标人一次性报出唯一的最终价格，包含其它一切所要涉及到的费用，有选择的报价将被拒绝。

（1）开标一览表（附件16）；

（2）报价明细表（附件17)；

（3）针对报价投标人认为其他需要说明的；（格式自拟）；

（4）微小企业声明函（非微小企业无需提供，见附件18）；

（5）产品适用政府采购政策情况表（附件19）。

**投标文件制作说明：**

1、请投标人严格按照上述内容及项目招标需求制作投标文件，所有证书类文件提供的复印件必须全部加盖单位公章且必须在有效期内的。

2、与本次投标无关的内容请不要制作在内，确保投标文件有针对性、简洁明了，同时节约纸张；投标文件统一以A4纸大小双面打印并装订。

3、不按招标文件要求制作投标文件的将视情扣分。

4、开标前集中采购机构不安排资格预审，投标人的资格审查在开标后由采购人或采购代理机构负责，若投标人不按采购文件的要求提供资格审查材料，其风险由投标人自行承担。

**（三）投标文件的语言及计量**

1、投标文件以及投标人与招标人就有关投标事宜的所有来往函电，均应以中文汉语书写。除签名、盖章、专用名称等特殊情形外，以中文汉语以外的文字表述的投标文件视同未提供。

2、投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，应采用中华人民共和国法定计量单位（货币单位：人民币元），否则视同未响应。

**（四）投标报价**

1、投标报价应按招标文件中相关附表格式填写。

2、相关报价单需打印或用不退色的墨水填写， 投标报价单不得涂改和增删，如有错漏必须修改，修改处须由同一签署人签字或盖章。由于字迹模糊或表达不清引起的后果由投标人负责。

**（五）投标保证金**

1、中标供应商的投标保证金在合同签订后五个工作日内凭合同退还，或转为中标人的履约保证金。

2、未中标供应商的投标保证金将在中标通知书发出后五个工作日内由项目负责人负责通知财务退还（财务联系电话：0576-88685133、传真：0576-88685133）。

**3、投标人有下列情形之一的，投标保证金将不予退还：**

（1）投标人在投标有效期内撤回投标文件的；

（2）投标人在投标过程中弄虚作假，提供虚假材料的；

（3）中标人无正当理由不与采购人签订合同的；

（4）将中标项目转让给他人或者在投标文件中未说明且未经招标人同意，将中标项目分包给他人的；

（5）其他严重扰乱招投标程序的。

**（六）投标文件的有效期**

1.自投标截止日起90天投标文件应保持有效。有效期不足的投标文件将被拒绝。

2.在特殊情况下，招标人可与投标人协商延长投标书的有效期，这种要求和答复均以书面形式进行。

3.投标人可拒绝接受延期要求而不会导致投标保证金被没收。同意延长有效期的投标人需要相应延长投标保证金的有效期，但不能修改投标文件。

4.中标人的投标文件自开标之日起至合同履行完毕均应保持有效。

**四、投标文件的递交**

（一）投标文件的密封及标记

1、所有投标资料按投标文件的组成所列内容及顺序装订成册。资格资信证明文件、技术文件和报价文件各自密封（份数及装订要求详见第二部分第四条）；

2、请在密封袋封面上加盖“正本”或“副本”字样，封口处应有投标单位公章或投标全权代表签字。封皮上写明项目编号、标项、招标项目名称、投标人名称，并注明“投标文件名称（资格资信证明文件、技术文件和报价文件）”、“开标时启封”字样；

3、如果投标人未按上述要求密封及加写标记，招标人对投标文件的误投和提前启封不负责任。

（二）投标截止时间

1、投标文件必须在规定的投标截止时间前派人送达指定的投标地点。

2、如有特殊情况，招标人延长截止时间和开标时间，招标人和投标人的权利和义务将受到新的截止时间和开标时间的约束。

（三）投标文件的补充、修改和撤回。

1、投标人如需对上交的投标文件进行补充、修改或撤回的，必须在投标

截止时间以前书面通知招标人（邮寄或送达）。

2、投标修改文件必须密封，在密封袋上写明项目编号、标项、招标项目名称、投标人名称、并注明“修改文件”、“开标时启封”字样，其作为投标文件的组成部份。

3、投标人在投标截止时间前撤回已提交的投标文件的，项目负责人应当通知财务自收到投标人书面撤回通知之日起5个工作日内，退还已收取的投标保证金，但因投标人自身原因导致无法及时退还的除外。

**五、开标**

（一）开标

1、招标人在“招标公告”规定的时间和地点公开开标，投标人的法定代表

人或其授权代表应参加开标会并签到。投标人的法定代表人或其授权代表未按时签到的，视同放弃开标监督权利、认可开标结果。评标委员会成员不得参加开标活动。（本次招标采用先评审商务资格和技术服务方案，后公开并评审商务报价的办法实施）。

**（二） 开标、评标及定标程序：（综合评分法使用）**

1、开标会由招标项目负责人主持，主持人宣布开标会议开始；

2、主持人介绍参加开标会的人员名单；

3、主持人宣布评标期间的有关事项，告知应当回避的情形,提请有关人员回避；

4、投标人或其当场推荐的代表，检查投标文件密封的完整性；

5、按投标人签到的先后顺序当场拆封资格资信证明文件、技术文件后，评标委员会先对资格资信证明文件、技术文件进行评审及必要的询标，结束后公布无效投标的投标人名单、投标无效的原因；

6、由主持人按投标人签到顺序当场拆封报价文件，并现场宣读《开标一览表》中的投标报价、报价内容（投标设备名称、规格型号或者服务项目名称），以及招标人认为有必要宣读的其他内容；

7、招标人做开标记录, 投标人代表对开标记录进行当场校核及勘误，并签字确认。同时由记录人、监督人当场签字确认。投标人代表未到场签字确认或者拒绝签字确认的，不影响评标过程；

8、采购人或采购代理机构进行资质后审；

9、评标委员会对资格资信证明文件进行评审及必要的询标，计算价格分及总得分；

9、评标委员会完成评标后,按评标原则确定中标候选人，以及根据采购人委托直接确定中标人；同时编写评审报告；

10、宣布评标结果，开标会议结束。

**六、评标**

**（一）组建评标委员会**

本项目评标委员会由政府采购评审专家和采购单位评审代表组成。

**（二）评标程序**

**1、资格审查**

公开招标采购项目开标结束后，采购人或者采购代理机构应当依法对投标人的资格进行审查。

**2、实质审查与比较**

（1）评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。

（2）对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者补正。

（3）评标委员会应当按照招标文件中规定的评标方法和标准，对符合性审查合格的投标文件进行商务和技术评估，综合比较与评价。

（4）评标时，评标委员会各成员应当独立对每个投标人的投标文件进行评价，并汇总每个投标人的得分。

（5）评标委员会完成评标后,按评标原则确定中标候选人，以及根据采购人委托直接确定中标人。同时编写评标报告。

**3、评价**

（1）采购人对项目采购情况进行评价；

（2）招标人对评标委员会评审专家进行评价。

**（三）澄清问题的形式**

投标人的澄清、说明或者补正应当采用书面形式，并加盖公章，或者由法定代理人或其授权的代表签字，并不得超出投标文件的范围或者改变投标文件的实质性内容。

**（四）错误修正**

投标文件报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

　　1、投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；

　　2、大写金额和小写金额不一致的，以大写金额为准；

　　3、单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价；

　　4、总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

　　同时出现两种以上不一致的，按照前款规定的顺序修正。修正应当采用书面形式，并加盖公章，或者由法定代表人或其授权的代表签字。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

**（五）投标人存在下列情况之一的，投标无效:**

1、未按照招标文件的规定提交投标保证金的。

2、投标文件未按招标文件要求密封、签署、盖章的（所有盖章均加盖投标单位公章，其它印章均作无效）。

　　3、不具备招标文件中规定的资格要求的。

　 4、报价超过招标文件中规定的预算金额或者最高限价的。

　　5、投标文件含有采购人不能接受的附加条件的。

6、投标代表人未能出具身份证明或与法定代表人授权委托人身份不符的；

7、资格资信证明文件或技术文件里出现数字报价的。

8、评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

9、投标报价高于市场平均价格，评标委员会认为有背《中华人民共和国政府采购法》第十七条的。

10、商务需求不响应的。

11、主要性能参数指标负偏离 15 项（含）以上的。

12、投标文件提供虚假材料的。

13、不符合中华人民共和国财政部令第87号《政府采购货物和服务招标投标管理办法》第三十七条情形之一的，视为投标人串通投标，其投标无效，并移送采购监管部门：

　 （1）不同投标人的投标文件由同一单位或者个人编制；

　 （2）不同投标人委托同一单位或者个人办理投标事宜；

　 （3）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

　 （4）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

　 （5）不同投标人的投标文件相互混装；

　 （6）不同投标人的投标保证金从同一单位或者个人的账户转出。

14、不符合法律、法规和招标文件中规定的其他实质性要求的（招标文件

中打“▲”内容及被拒绝的条款）。

**（六）有下列情况之一的，本次招标作为废标处理：**

1、出现影响采购公正的违法、违规行为的；

2、评标委员会发现招标文件存在歧义、重大缺陷导致评标工作无法进行，或者招标文件内容违反国家有关强制性规定的；

3、投标人技术性能得分均低于技术性能分值60%，被评标委员会认定为不具有履行合同所必需的设备和专业技术能力的；

4、因重大变故，采购任务取消的；

5、法律、法规和招标文件规定的其他导致评标结果无效的。

**（七）评标原则和评标办法**

1、评标原则。评标委员会必须公平、公正、客观，不带任何倾向性和启发性；不得向外界透露任何与评标有关的内容；任何单位和个人不得干扰、影响评标的正常进行；评标委员会及有关工作人员不得私下与投标人接触。

2、评标办法。具体评标内容及评分标准等详见《第四部分：评标方法及评分标准》。

**（八）评标过程的监控**

本项目评标过程实行全程录音、录像监控（或请政府采购监管部门将同时进行现场监督），投标人在评标过程中所进行的试图影响评标结果的不公正活动，可能导致其投标被拒绝。

**七、定标**

评标委员会根据采购单位的委托协议，推荐或确定中标供应商。

**八、合同授予**

1、中标结果将自中标人确定之日起2个工作日内在省级以上财政部门指定的媒体及相关网站公告。

2、采购人应当在《中标通知书》中要求的时间内，按照招标文件和中标人投标文件的规定，与中标人签订书面合同。所签订的合同不得对招标文件确定的事项和中标人投标文件作实质性修改。

采购人不得向中标人提出任何不合理的要求作为签订合同的条件。

3、中标供应商拖延、拒签合同的,投标保证金将不予退还并取消中标资格。

4、如需合同履约保证金的请合同双方在签定合同时商定，但履约保证金的数额不得超过政府采购合同金额的10%。

**第四部分　评标方法、评标标准**

一、招标人将组织评标委员会，对投标人提供的投标文件进行综合评审。

二、评标委员会按抽签序号听取投标单位的情况介绍，对有关问题进行询标。

三、本次招标项目的评标方法为**综合评分法**，总计100分。评标标准按以下5项内容及分值进行评审。

|  |  |
| --- | --- |
|  | **第1标段** |
| **技术性能** | 41 |
| **实力信誉及业绩** | 14 |
| **售后服务** | 8 |
| **对招标文件的响应程度等** | 2 |
| **信用评价** | 5 |
| **产品价格** | 30 |

四、在最大限度地满足招标文件实质性要求前提下，评标委员会按照招标文件中规定的各项因素进行综合评审后，以评标总得分最高的投标人为中标候选人。

五、如得分相同，投标报价低者为中标候选人；如得分且投标报价相同的，投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

六、提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，按技术指标优者为中标候选人。

七、如果中标供应商自动放弃中标资格或因质疑或是投诉被取消中标资格的，可视情报经财政部门同意后根据评审结果按顺序由排在后面的候选供应商递补，以此类推。

七、本次评分具体分值细化条款如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **评标内容** | **细则内容** | | **分值** |
| **技术性能41分** | 技术方案：投标人对项目方案设计的合理性、可行性、兼容性和扩展性等，包含现状与需求分析、建设必要性分析、建设可行性分析、总体建设框架、详细建设内容等，横向比较，一档得5分，二档得4-3分，三档得2-1分。 | | 5 |
| 实施方案：投标人提供的进度计划与实施是否清晰、准确、完整，关键节点的控制措施是否有力、合理、可行；质量管理机构是否健全，制度完善，质量规格能否符合技术要求规定，是否有完善项目开发质量保证体系和措施，横向比较，一档得5分，二档得4-3分，三档得2-1分。 | | 5 |
| 所投主要产品品牌知名度、市场认可度、占有率等方面综合评分（好7-8分，较好4-6分，一般0-3分）。 | | 8 |
| 根据投标产品的基本性能配置是否符合招标文件的要求及符合程度进行评价：1、基本性能满足或高于要求的得满分，每项负偏离-0.5分，满分7分，扣完为止。2、横向比较，根据投标产品性能优异程度打分：好13-10分，较好9-6分，一般5-0分。 | | 20 |
| 为保证产品稳定性，所投主要产品具备CMMI认证，提供CMMI L5级证书得3分，提供CMMI L4级证书的得2分，提供CMMI L3级证书的得1分，其他不得分，需提供加查询链接地址。 | | 3 |
| **企业实力及信誉14分** | 投标方企业实力，提供近三年财务报表、荣誉证书、信用等级证书等，酌情给分。 | | 3 |
| 投标人具有ITSS信息技术服务运行维护标准证书，得1分 ；投标人具有ISO27001信息安全管理体系认证证书，得1分；ISO20000 IT服务管理体系认证证书，得1分；具有国家信息安全服务资质证书，得1分。(证书复印件加盖公章） | | 4 |
| 项目实施人员安排：项目经理及施工人员配备数量及相关资质证书情况，酌情打分。 | | 2 |
| 投标人2015年7月以来，类似成功案例（500万以上每个2分；100万以上，每个得1分，以提供清晰的合同及相应发票复印件为准，缺一不得分）。 | | 5 |
| **售后服务8分** | 根据提供的免费质保期限，横向比较，酌情评分。 | | 2 |
| 售后服务方案（包括定期巡检，保修范围，服务标准，服务力量，人员配备，故障响应修复时间方式及保障措施等），酌情评分。 | | 2 |
| 根据本地化服务能力酌情评分，0-4分。（提供的相关证明材料） | | 4 |
| **对招标文件的响应程度等2分** | 1、根据投标文件的制作及装订情况由评委酌情打分0-1.5 分  2、电子文档是否按招标文件要求提供，有得0.5分，无不得分 | | 2 |
| **信用评价5分** | **基准分** | 网上注册情况：已在浙江政府采购网上正式注册入库的供应商得基准分0.5分 | 0.5 |
| **市场行为** | 1.重约守信：连续3年以上（包括3年）被评为守合同重信用单位的，加0.5分； | 0.5 |
| 2.投标行为：根据供应商2015以来参加台州市本级政府采购活动行为记录进行打分。若无存在提供虚假资料、保证金不予退还、不遵守开、评标现场纪律等不良记录及监管部门的处理处罚决定的，得1分； | 1 |
| **履约行为** | 履约信用：根据采购人反馈的《供应商履约情况评价表》进行打分。  采购人评价等级为优秀的得3分，良好的得2分，合格的得1分，基本合格的得0.5分，不合格的不得分。  注：1.在本市至今尚无得到过评价的（指首次参加或以往有参加但因未中标而没有被评价的）投标供应商视为合格供应商，按合格档次进行打分；  2.本项最终得分按评价等级加权计算。 | 3 |
| **价格**  **30分** | 取投标合格供应商的投标最终报价最低价为基准价。基准价为30分。投标报价得分＝（评标基准价/最终投标报价）×30%×100（小数点后保留2位小数）。（注：对于小型和微型企业产品的价格给予6%的扣除，用扣除后的价格参与评审。小型和微型企业需提供《小微企业声明函》，并提供当地小型和微型企业行政主管部门的确认意见及相关依据；确认意见如无明确有效期，则须在投标截止1年内。） | | 30 |

**第五部分　台州市政府采购合同文本**

**-通用条款**

以下为成交后签定本项目合同的通用条款，成交供应商不得提出实质性的修改，关于专用条款将由采购人与成交供应商结合本项目具体情况协商后签订。

项目名称： 项目编号：

甲方：（采购单位） 所在地：

乙方：（中标供应商） 所在地：

甲、乙双方根据中心关于××单位××项目公开招标的结果，签署本合同。

**一、货物内容**

1. 货物名称：

2. 型号规格：

3. 技术参数：

4. 数量（单位）：

**二、合同金额**

本合同金额为（大写）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元（￥\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_元）人民币。

**三、技术资料**

1.乙方应按招标文件规定的时间向甲方提供使用货物的有关技术资料。

2. 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

**四、知识产权**

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

**五、产权担保**

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

**六、履约保证金**

本项目履约保证金为合同金额的\_\_\_\_%。

**七、转包或分包**

1.本合同范围的货物，应由乙方直接供应，不得转让他人供应；

2.除非得到甲方的书面同意，乙方不得将本合同范围的货物全部或部分分包给他人供应；

3.如有转让和未经甲方同意的分包行为，甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

**八、质保期**

1. 质保期年。（自交货验收合格之日起计）

**九、交货期、交货方式及交货地点**

1. 交货期：

2. 交货方式：

3. 交货地点：

**十、货款支付**

1. 付款方式：

**十一、税费**

本合同执行中相关的一切税费均由乙方负担。

**十二、质量保证及售后服务**

1. 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

2. 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

3. 如在使用过程中发生质量问题，乙方在接到甲方通知后在小时内到达甲方

现场。

4. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切

费用。

5.上述的货物免费保修期为年，因人为因素出现的故障不在免费保修范围

内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

**十三、调试和验收**

1. 甲方对乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准

进行现场初步验收，外观、说明书符合招标文件技术要求的，给予签收，初

步验收不合格的不予签收。货到后，甲方需在五个工作日内验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作

为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的

使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验

收。

4.对技术复杂的货物，甲方应请国家认可的专业检测机构参与初步验收及最终

验收，并由其出具质量检测报告。

5.验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由乙方负

责。

**十四、货物包装、发运及运输**

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

3. 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备接货。

4. 货物在交付甲方前发生的风险均由乙方负责。

5. 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需

通知甲方货物已送达。

**十五、违约责任**

1. 甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2. 甲方无故逾期验收和办理货款支付手续的,甲方应按逾期付款总额每日万分之五向乙方支付违约金。

3. 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期10个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4. 乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

**十六、不可抗力事件处理**

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行

期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续120天以上，双方应通过友好协商，确定是否继续履行合

同。

**十七、解决争议的方法**

1.当事人可以通过和解或者调解解决合同争议。当事人不愿和解、调解或者和解、调解不成的，按下述（1）、（2）种方式解决；

1. 提交\_台州\_仲裁委员会仲裁。
2. 依法向人民法院提起诉讼。

2.当事人可以向办理采购事宜的采购代理机构申请调解。

3.当事人可以向同级财政部门申请调解。

**十八、合同生效及其它**

1. 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2. 本合同未尽事宜，遵照《合同法》有关条文执行。

3. 本**合同一式四份。甲、乙双方各执一份，台州市政府采购中心及台州市政府采购监管处各执一份。本项目未尽事宜以招标文件、投标文件及澄清文件等为准。**

**4、**合同必须经台州市政府采购中心监证。

甲方（公章） 乙方（公章）

法定代表人： 法定代表人：

委托代理人： 委托代理人：

联系电话： 联系电话：

开户银行： 开户银行：

帐号： 帐号：

地址及邮编： 地址及邮编：

签订时间： 年 月 日

合同鉴证方（盖章）:

项目负责人:

鉴证日期: 年 月 日

**第六部分： 应提交的有关格式范例**

**附件1：**本

项目名称

项目编号：（标项）

投

标

文

件

（**资格资信证明文件）**

投标人全称（公章）：

地 址：

时 间：

**资格资信证明文件目录**

1、声明书；

2、法定代表人授权书；

3、营业执照、税务登记、组织机构代码证**、**社会保险登记证；

4、上年度企业资产负债表及损益表；

5、本项目要求的特定资质证书

6、投标人情况介绍；

7、投标人通过的质量管理和质量保证体系、环保体系、自主创新或其他体系等的认证证书或文件；；

8、资信及商务需求响应表；

9、近三年来类似项目的成功案例；

10、投标人认为可以证明其能力或业绩的其他材料；

**附件2**

**声明书**

台州市政府采购中心：

（投标人名称）系中华人民共和国合法企业，经营地址。

我（ 姓名 ）系（ 投标人名称 ）的法定代表人，我公司自愿参加贵方组织的（招标项目名称）（编号为）的投标，为此，我公司就本次投标有关事项郑重声明如下：

1**、我公司声明截止投标时间近三年以来，在政府采购领域中的项目招标、投标和合同履约期间无任何不良行为记录和违法、违规行为。**

2、我公司在参与投标前已详细审查了招标文件和所有相关资料，我方完全明白并认为此招标文件没有倾向性，也没有存在排斥潜在投标人的内容，我方同意招标文件的相关条款，放弃对招标文件提出误解和质疑的一切权利。

3、我公司不是采购人的附属机构；在获知本项目采购信息后，与采购人聘请的为此项目提供咨询服务的公司及其附属机构没有任何联系。

4、我公司向贵方提交的所有投标文件、资料都是准确、真实、合法的。

5、若中标，我公司将按招标文件规定履行合同责任和义务。

6、我公司保证，采购人在中华人民共和国境内使用我公司投标货物、资料、技术、服务或其任何一部分时，享有不受限制的无偿使用权，如有第三方向采购人提出侵犯其专利权、商标权或其它知识产权的主张，该责任由我方承担。我方的投标报价已包含所有应向所有权人支付的专利权、商标权或其它知识产权的一切相关费用。

7、以上事项如有虚假或隐瞒，我公司愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

投标人名称(公章)：

法定代表人或授权委托人(签字)：

日期：2015年 月 日

**附件3**

**法定代表人授权书**

台州市政府采购中心：

本人（姓名）系（投标人全称）法定代表人，现授权委托（ 投标人代表名称）为全权代表，参加贵处组织的项目（括号内填写项目编号及项目名称）投标活动，并代表我公司全权办理针对上述项目的**投标全程各事项、投标文件签署、合同签订及项目实施**等涉及的一切事宜，我公司对被授权人的签名等行为均予以承认，由此所产生的一切法律后果和法律责任，均由我公司承担。同时宣布承诺如下：

1. 我公司已详细阅读全部招标文件（含补充修改文件），并理解其实质

性内容，同意承担招标文件规定的全部义务和相关责任。

1. 我公司同意提供招标人可能要求的与其投标有关的一切数据或资料。
2. 我公司所提交的一切投标资料均为合法且真实有效。

法定代表人签字：

投标人全称（公章）： 日期：

**附：**

|  |
| --- |
| **全权代表身份证复印件粘帖处** |

全权代表姓名： 职务：

传真：

电话：

详细通讯地址：

邮政编码：

**附件4**

**投标人基本情况表**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 企业名称 |  | | | | | | 法人代表 | | |  | |
| 地址 |  | | | | | | 企业性质 | | |  | |
| 股东姓名 |  | 股权结构（%） | |  | | | 股东关系 | | |  | |
| 联系人姓名 |  | 固定电话 | |  | | | 传真 | | |  | |
| 手机 | |  | | |
| 1.  企  业  概  况 | 职工人数 |  | | 具备大专以上学历人数 |  | | 国家授予技术职称人数 | | |  | |
| 占地面积 |  | | 建筑面积 | 平方米  □自有□租賃 | | 生产经营场所及场所的设施与设备 | | |  | |
| 注册资金 |  | | 注册发证机关 |  | | | | | 公司成立时间 |  |
| 核准经营范围 |  | | | | | | | | | |
| 发展历程及主要荣誉： | | | | | | | | | | |
| 2．  企业有关资质获证情况 | 产品生产许可证情况（对需获得生产许可证的产品要填写此栏） | | 产品名称 | | | 发证机关 | | 编号 | 发证时间 | | 期限 |
|  | | |  | |  |  | | |
| 企业通过质量体系、环保体系、计量等认证情况 | |  | | | | | | | | |
| 企业获得专利情况 | |  | | | | | | | | |

**要求：**

1.姓名栏必须将所有股东都统计在内，若非股份公司此行（第三行）无需填写；

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：：

**附件5**

**证书一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **证书名称** | **发证单位** | **证书等级** | **证书有效期** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**要求：**

1.填写投标人获得资质、认证或企业信誉证书。

2.请提供本表所列的证书资料。

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：：

**附件6**

**资信及商务需求响应表(第 标)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **内容** | **招标需求** | **是否响应** | **投标人的承诺或说明** |
|  | 售后服务保障要求 |  |  |  |
|  | 备品备件及耗材等要求 |  |  |  |
|  | 质保期 |  |  |  |
|  | 交货和服务  时间及地点 |  |  |  |
|  | 付款条件 |  |  |  |
|  | …… |  |  |  |
|  | 政策性加分条件 |  |  |  |
|  | 质量管理、企业信用要求 |  |  |  |
|  | 能力或业绩要求 |  |  |  |
|  | …… |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件7**

**投标人类似项目实施情况一览表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **项目地址** | **合同总价** | **实施时间** | **项目质量** | **项目单位名称及其联系人电话** |
| 1 |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| … |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**要求：**

1.业绩证明应提供证明材料（合同复印件可只提供首页、含金额页、盖章页并加盖投标人公章，不按照要求提供不得分，报价时携带完整的合同原件备查）；

2.报价供应商可按此表格式复制。

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件8** 本

项目名称

项目编号：（标项）

投

标

文

件

（**技术文件）**

投标人全称（公章）：

地 址：

时 间：

**技术文件目录**

1、对本项目的具体响应方案；

2、设备配置清单；

3、主要货物用材响应表

4、技术需求响应表；

5、保证工程质量的技术力量及技术措施；

6、保证工期的施工组织方案及人力资源安排（附件6）；

7、项目实施人员一览表；

8、项目负责人资格情况表；

9、技术服务、技术培训、售后服务的内容和措施；

10、安装、调试及验收方案和措施；

11、投标人需要说明的其他内容。

**附件9**

**设备配置清单 (第 标)**

项目编号：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **品牌** | **规格型号** | **产地** | **数量** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**要求：**

**1.**本表中的名称、数量应与报价明细表中相对应的报价名称、数量一致

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件10**

**主要货物用材响应表(类似家具类货物采用)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 产品配置 | 产品主要用材 | | | | | |
| 材料规格及参数 | 品牌  商标 | 生产厂家 | 符合标准 | 性能说明 | 备注 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**要求：**

1.请列出以上产品的各项主要用材、辅料、油漆、五金件等。

2.本表所列产品主要用材均为采购人抽样送检的范围。

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件11**

技术需求响应表**(第 标)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **规格型号** | **招标参数** | **投标参数** | **偏离说明** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**要求：**

1. 本表的名称须与《报价明细表》一致。

2.本表参照本招标文件第二部分“招标需求”内第二条“具体技术需求”填制，投标人应根据投标设备的性能指标、服务指标，对照招标文件要求在“偏离情况”栏注明“正偏离”、“负偏离”或“无偏离”。

3.对于投标产品的技术偏离情况需严格按照招标文件的技术要求一一比对给出，未达到技术要求中规定的数值应以负偏离标注。若因技术实现方式等其他问题而导致的理解不同未标注负偏离的，需在备注中具体说明；若未按要求标注负偏离又未予以说明的，评审小组将视偏离程度给予扣分或认定为虚假应标。

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件12**

**项目实施人员一览表（第 标）**

（主要从业人员及其技术资格）

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **姓名** | **职务** | **职责** | **专业技术资格** | **证书编号** | **参加本单位工作时间** | **劳动合同编号** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**要求：**

**1.**在填写时，如本表格不适合投标单位的实际情况，可根据本表格式自行划表填写。

2.附人员证书复印件；

　　3.出具上述人员在本单位服务的外部证明，如：投标截止日之前六个月以内的代缴个税税单、参加社会保险的《投保单》或《社会保险参保人员证明》等。

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件13**

**项目负责人资格情况表**

采购项目： 采购编号：

|  |  |  |
| --- | --- | --- |
| **姓名** |  | **近年来主要工作业绩** |
| **性别** |  | 注：业绩证明应提供旁证材料  （供货合同或中标通知书）。 |
| **年龄** |  |
| **职称** |  |
| **毕业时间** |  |
| **学校专业** |  |
| **联系电话** |  |
| **最近一年工作状况** |  |
| **拟在本项目中担任主要工作** |  | |

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件14**

**售后服务情况表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **投标人承诺** | **备注** |
| 1 | 保修期内售后服务情况(服务方式、服务网点、售后服务的内容和措施等等，可用附页和宣传材料) | 生产厂商售后服务情况： |  |
| 投标人售后服务情况： |  |
| 2 | 保修期后售后服务 |  |  |
| 3 | 培训方案（可用附页） |  |  |
| …… | …… |  |  |

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件15**

项目名称

项目编号：（标项）

**报**

**价**

**文**

**件**

供应商全称（公章）：

地 址：

时 间：

**报价文件目录**

1、开标一览表；

2、报价明细表；

3、针对报价投标人认为其他需要说明的；

4、小微企业声明函；

5、产品适用政府采购政策情况表。

**附件16**

**开标一览表 (第 标)**

项目编号： [货币单位：人民币元]

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **项目名称** | **规格型号** | **产**  **地** | **单位** | **数量** | **单价**  **（元）** | **交货期**  **合同签订后几天内** | **交货地点** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **合计人民币**：**大写： 小写：** | | | | | | | | |

**填报要求：**

1.报价一经涂改，应在涂改处加盖单位公章或者由法定代表人或授权委托人签字或盖章，否则其投标作无效标处理；

2.以上报价应与“报价明细表”中的“合计人民币”数相一致；

3.项目费用包括项目实施所需的工程费、工时费、服务费、运输费、安装调试费、购买及制作标书费、税费及其他一切费用。

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件17**

**报价明细表 (第 标)**

项目编号：

[货币单位：人民币元]

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **报价项目** | **品牌、产地** | **型号规格** | **数量** | **单价** | **小计** | **备注** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **合计人民币：大写 小写** | | | | | | | |

**要求：**

1. 本表为《开标一览表》的报价明细表，如有缺项、漏项，视为投标报价中已包含相关费用，采购人无需另外支付任何费用。

2.本表同《开标一览表》的合计人民币数相等。

▲3. 本表中的型号规格必须明确，招标文件中明确要求定制的除外。

▲4.供应商在投标时需提供本表的电子文档（单独封装，建议使用光盘），提供的电子文档内容必须与此表一致，若所投产品品牌、型号等重要内容缺失的将视作无效标；电子文档将不予退还。

投标人名称（盖章）：

投标人代表签字：

职 务：

日 期：

**附件18**

**小微企业声明函**

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）的规定，本公司为\_\_\_\_\_\_（请填写：小型、微型）企业。即，本公司同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定的划分标准：第四条第\_\_\_\_\_\_项\_\_\_\_\_\_行业，本公司*（此处填写从业人员和营业收入的具体数据）*，为\_\_\_\_\_\_（请填写：小型、微型）企业。

2.本公司参加台州市政府采购中心组织的采购项目（项目编号： ）采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他\_\_\_\_\_\_（请填写：小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

投 标 人（单位公章）：

日期：20 年 月 日

**小微企业声明函（制造商）**

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181号）的规定和《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300号）规定的划分标准：第四条第\_\_\_\_\_\_项\_\_\_\_\_\_行业，本公司（此处填写营业收入和从业人员的具体数据），为\_\_\_\_\_\_（请填写：小型、微型）企业。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（单位公章）：

日期：20 年 月 日

**附件19**

**产品适用政府采购政策情况表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 小企业扶持政策 | 如属所列情形的，请在括号内打“√”：  （ ）小型、微型企业投标且提供本企业制造的产品。  （ ）小微企业投标且提供其它小型、微型企业产品的，请填写下表内容： | | | |
| 产品名称（品牌、型号） | 制造商 | 制造商  企业类型 | 金额 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 小型、微型企业产品金额合计 | | |  |

填报要求：

1. 本表的产品名称、规格型号和注册商标、金额要与《报价明细表》一致。
2. 制造商为小型或微型企业时才需要填“制造商企业类型”栏，填写内容为“小型”或“微型”。
3. 请投标人正确填写本表，所填内容将作为评分的依据。其内容或数据应与对应的证明资料相符，如果不一致，可能导致该项的得分为0分。