采购项目技术、服务、政府采购合同内容条款、质量及其他商务要求

本项目基本要求是指按采购人所提供的产品明细清单上所列出的全部要求，如果供应商能提供“技术参数、使用功能、安全性能、节能降耗减排、改善环境、使用寿命”等方面更优的产品的，允许优于基本要求的产品替代，但不得因此而要求采购人追加采购资金。

本次采购项目的所有产品的“技术参数和商务及服务要求及合同主要条款”详见产品明细清单。

注意：本章的要求不能作为资格性条件要求评审，如存在资格性条件要求，应当认定谈判文件编制存在重大缺陷，谈判小组应当停止评审。

**一、建设内容：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **单位** | **备注** |
| 1 | 综合运维管理平台 | 1 | 套 |  |
| 2 | 安全区交换机 | 1 | 台 |  |
| 3 | 业务区交换机 | 2 | 台 |  |
| 4 | 终端安全管理 | 1 | 套 |  |
| 5 | 动态防御系统 | 1 | 台 |  |

**二、技术参数要求：**

| **序号** | **产品名称** | **参数要求** | **数量** | **单位** |
| --- | --- | --- | --- | --- |
| 1 | 综合运维管理平台 | 1、采用B/S架构，支持分布式部署，具备资源权限管理，可按资源组、设备资源赋权； 2、具备对操作系统的监控，包含CPU、内存、进程、磁盘、网卡等信息，采用非代理方式监测。 3、可监控主流数据库。 4、具备对中间件和应用进行性能、状态和故障信息的监测。 5、具备对思科、华为、锐捷、H3C、中兴、迈普等品牌网络设备进行监控，包含但不限于设备性能、吞吐量，端口流量、端口丢包率、广播包速率，链路通断等。 6、能够自动生成拓扑图，并对拓扑图中的告警设备进行实时的动态播放，并可提供多个拓扑图轮流播放功能； 7、具备对思科、华为、华三、锐捷、摩托罗拉、中兴、Aruba等品牌无线设备进行监控；并能通过地理位置图呈现无线AP、无线用户的位置分布及运行状态；当无线AP出现故障，可在位置图中变成红色进行故障提醒和对故障AP的位置进行定位，并在同一个视图中实时统计无线AP及无线用户的连接情况、在线数、无线流量等信息。 8、具备告警分析，可分析告警产生时刻，与告警资源相关联的设备情况，包括设备状态、告警信息、指标信息均为告警产生时刻的快照，并提供性能指标知识库，分析性能指标含义、风险及处理建议。 9、提供业务系统与IT资源之间自定义建模的功能，可自定义业务所关联的关键IT资源，包括服务器、网络、数据库、应用服务等资源。 10、业务系统的可用情况、健康情况、忙碌情况等关键指标计算方式可进行自定义设置，并提供对外的API接口，可对接业务系统推送的自定义业务指标，主动获取用户所关心的业务数据。 11、内置多纬度多视角报表模版，如：资源报表模版、告警报表模版、趋势报表模版、TOPN报表等。 12、能够通过API接口实现对VMware 、Hyper-V、Citrix、H3C CAS、华为、KVM等主流虚拟化资源的监控；并提供虚拟化资源拓扑图、提供虚拟机漂移告警，告警包括漂移前所属主机、漂移后所属主机。 13、能够通过SNMP、SMI-S等多种方式支持对EMC、IBM、Netapp、HDS、博科光纤交换机等主流存储设备的监控；实现存储故障告警和统计分析，以列表形式展示FC交换机端口与存储设备端口、服务器主机HBA卡端口的连接关系； 14、在故障定位中，设备在线用户信息及设备流量信息是问题判断的依据之一，系统应具备以视图方式显示用户接入端到网络设备，再到应用端或网络出口的网络访问路径功能，并能通过视图显示所经过的交换机信息，包括设备接口信息，设备在线的用户、IP地址、MAC地址、上联设备、房间号、上行流量、下行流量等信息； 15、支持3D可视机房管理功能，界面风格与管理平台统一； 16、支持多维度、分领域对知识库进行管理，支持知识的创建、评审、发布等； 17、配置要求：配置网络设备、服务器、数据库、中间件、应用等≥50个节点授权，无线AP≥100个节点授权，日志监控授权≥30个，告警客户端授权≥5个。 | 1 | 套 |
| 2 | 安全区交换机 | 1、配置≥24个10/100/1000M自适应电口，≥8个1G/10G SFP+光口，支持在64Bytes-1518Bytes下线速转发； 2、配置MGMT端口≥1个、Console 端口≥1个、USB端口≥1个，模块化电源插槽≥2个，通用模块化插槽≥1个； 3、交换容量≥7.9Tbps，包转发率≥600Mpps 4、整机采用绿色环保设计，满负荷情况下功耗≤60W； 5、整机MAC地址≥196K，路由表项≥64K； 6、支持RIPv2，OSPFv2/v3，BGP4/4+，IS-ISv4/v6； 7、支持IGMP v1/v2/v3，PIM-SM等组播协议； 8、支持基于IPv4/IPv6五元组、基于源/目的MAC、基于VLAN、基于802.1P优先级的ACL； 9、支持特有的CPU保护策略，对发往CPU的数据流，进行流区分和优先级队列分级处理； 10、支持基础网络保护策略，限制用户向网络中发送ARP报文、ICMP请求报文、DHCP请求报文的数率； 11、支持基于流的采样功能，对所选数据流包头中的源IP地址、目的IP地址、协议号、源端口号、包长等信息进行采样； 12、支持虚拟化功能，可将多台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间达到毫秒级； 13、配置要求：主机≥1台，模块化电源≥2个。 | 1 | 台 |
| 3 | 业务区交换机 | 1、配置≥24个10/100/1000M自适应电口，≥8个1G/10G SFP+光口，支持在64Bytes-1518Bytes下线速转发； 2、配置MGMT端口≥1个、Console 端口≥1个、USB端口≥1个，模块化电源插槽≥2个，通用模块化插槽≥1个； 3、交换容量≥7.9Tbps，包转发率≥600Mpps 4、整机采用绿色环保设计，满负荷情况下功耗≤60W； 5、整机MAC地址≥196K，路由表项≥64K； 6、支持RIPv2，OSPFv2/v3，BGP4/4+，IS-ISv4/v6； 7、支持IGMP v1/v2/v3，PIM-SM等组播协议； 8、支持基于IPv4/IPv6五元组、基于源/目的MAC、基于VLAN、基于802.1P优先级的ACL； 9、支持特有的CPU保护策略，对发往CPU的数据流，进行流区分和优先级队列分级处理； 10、支持基础网络保护策略，限制用户向网络中发送ARP报文、ICMP请求报文、DHCP请求报文的数率； 11、支持基于流的采样功能，对所选数据流包头中的源IP地址、目的IP地址、协议号、源端口号、包长等信息进行采样； 12、支持虚拟化功能，可将多台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间达到毫秒级； 13、配置要求：主机≥1台，模块化电源≥2个，≥1根虚拟化专用线缆。  14、所投产品厂商在生产的过程进行静电防护管理，具备完善的静电防护管理体系，通过静电防护管理体系认证，提供证书复印件。 | 2 | 台 |
| 4 | 终端安全管理 | 1、支持文件特征云查询服务，能够连接厂家共有安全云系统自动进行文件特征查询同步，且能够支持隔离网环境。 2、采用稳定的C/S软件通讯架构，有良好的可扩展性和易用性，以支持大型网络跨地域跨网段等场景的部署； 3、管理控制台须支持谷歌、火狐、搜狗、opera、safari等非IE核心浏览器，满足网络管理人员管理的便利性。 4、可扩展的分级管理架构，通过对系统中心的分级，使用主系统中心来集中管理数据，以实现以单个系统中心对多个二级节点及其他特殊防毒节点的集中管理。具有良好的可扩展性和可伸缩性，对于网络规模扩大或新增节点都可以很容易地实现集中管理。 5、一键式部署功能，产品无论主节点所有组件还是二级节点所有组件均提供一键式安装功能。 6、支持云防御与云查杀功能，且无需借助其他软硬件平台。 7、提供实时和定时检测、清除病毒功能，实时检测和清除来自各种途径的各类恶意代码和特洛伊木马等黑客程序。对来自Internet、E-mail或是光盘、软盘、移动存储、网络等各种入口渠道的宏病毒、特洛伊木马、黑客程序和有害程序等全面进行实时监控。 8、发现病毒后，提供多种处理方法，例如清除、删除或隔离。 9、边界防御可识别、分析常见的PE类文件、文档类文件、压缩类文件、图片文件，并能生成相应的分析报告； 10、具有病毒自动隔离功能，对无法清除病毒的被感染文件，防病毒软件能够自动隔离感染文件。隔离系统不能将本地染毒文件隔离到其它计算机或服务器，以防止隔离的文件被未经授权的人员查看。 11、配置终端安全管理授权≥400个，配置服务器端安全管理授权≥15个。 | 1 | 套 |
| 5 | 动态安全防御系统 | 1、固化千兆电口做为管理口数量≥2个；≥4口业务口，内存≥8G，硬盘≥1T； 2、性能要求≥1万条/秒，并发连接≥30万，本次配置≥100个IP监控节点； 3、系统运行状态实时监控，包括CPU、内存、硬盘的实时运行状态，物理线路实时监控，对设备端口的实时监控； 4、要求接入主机实时监控，实时监控在线主机的上线时间、真实IP、虚拟IP、外网IP、VLAN\_ID等信息； 5、基于MAC地址、五元组的包过滤规则，支持同网段主机之间的访问控制； 6、要求内网主机通过虚拟地址进行相互通信，每台主机分别对应真实IP、虚拟IP、外网IP三类不同的地址； 7、要求虚拟响应节点属性可配置，可配置虚拟响应的节点属性，包括主机类型、MAC地址、提供的服务以及响应的概率等，支持多种网络协议虚拟响应； 8、支持流量重定向给第三方蜜罐主机； 9、要求提供包括攻击者IP、渗透类型、探测端口、探测次数、起始时间、截止时间等。  10、为保证绿色环保，所投产品厂商具备有害物质控制管理能力，提供QC080000:2017体系认证证书复印件；  11、所投产品厂商具有成熟的产品实施及售后服务能力，满足工信部制定的信息技术服务标准，成熟度达到二级，提供信息技术服务运行维护标准符合性证书复印件。 | 1 | 台 |

**三、商务及售后服务要求**

**（一）商务要求**

1.交货地点：采购人指定地点。

★2.合同签订：成交供应商在成交通知书发出之日起5日内与采购人签订采购合同。

★3.货物（产品）交付时间：合同签订之后 10 日内完成货物（产品）交付。

4.付款方式和条件：

（1）付款方式

设备安装调试完成，经初验合格后，中标方提出付款申请且满足付款条件的情况下支付合同金额的40%。稳定运行2个月后终验合格，支付合同金额的55%。

（2）三年免费维保期结束后，中标方提出付款申请且满足付款条件的情况下支付合同金额的5%。

5.建设工期要求

按照《广元市医保骨干网横向接入区设计方案》，合同签订20日内，配合其他设备供应商及原厂技术人员完成横向接入区项目系统集成建设工作。

**（二）售后服务要求**

★（1）供应商提供所投产品三年(从终验合格后开始计算)原厂免费保修服务和相应的软件三年(从终验合格后开始计算)原厂免费更新升级服务（提供证明材料并加盖供应商公章）。

（2）供应商或原厂服务人员接电话报修后1小时内响应、4小时内上门服务、6小时内排除故障。用户报修后，原厂工程师和需要更换的备件4小时到达现场，保证到达现场后4小时内解决故障。若无法排除，免费提供备用方案和设备，帮助用户恢复关键业务。

★（3）供应商需保证在质保期内，每季度提供不少于1次巡检服务，服务范围包括但不限于市级横向接入区设备健康检查、性能调优和配置调整等，并提供相关报告；提供专业团队在重要时期内保障网络稳定安全。供应商书面承诺安排原厂代表对实施方案进行技术把关，参与到货上架、安装、调试等服务全过程（提供证明材料并加盖供应商公章）。

（4）供应商配合采购人完成与本项目相关系统的系统集成和建设工作，过程中产生的费用，均须由中标方自行提供，采购方不另外支付任何费用。供应商提供设备连接所需的各种模块、线缆（电源线、网线、光纤等），完成设备上架、安装、设备与线缆标签制作粘贴、理线等工作。

★（5）供应商需保证建设期内每个厂商安排原厂驻场工程师1名（提供证明材料并加盖供应商公章）。

（6）协助其他供应商开展横向接入区安全网络建设工作。

★（7）供应商在成交后签订合同前提供所投产品厂商针对本项目的售后服务承诺函（提供承诺函并加盖厂商公章）。

（8）响应产品必须为全新未使用过的设备（包括配套设备及零部件），并且符合国家、行业规定的质量、规格和性能等要求。

（9）合同总价已包括货物设计、材料、制造、包装、运输、安装及调试、人员培训、配套辅材等验收检测合格交付使用之前及保修期内保修服务与备用物件等所有其他有关各项等含税费用。采购人无须另向供应商支付其他任何费用。

（10）供应商提供售后服务方案。

（11）供应商须指派专人负责与采购人联系售后服务事宜。

**（三）验收标准**

（1）成交人与采购人应严格按照政府采购相关法律法规以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205 号）的要求进行验收。

（2）货物（设备）在安装运行后无质量问题，采购人与供应商应签署《安装运行验收报告》

**注：以上“★”代表实质性要求，供应商必须满足，不满足将作无效响应处理。**