网络攻防实训室设备 **采购需求、评标标准等说明**

一、项目概况

     （一）项目名称：网络攻防实训室设备

（二）采购方式： 公开招标

（三）主要内容、数量及要求：网络攻防实训室设备1批

（四）预算金额：600000元 ；最高限价：600000元

（五）交付（服务、完工）时间：30天

（六）交付（服务、施工）地点：许昌职业技术学院

（七）进口产品：允许□不允许。

（八）分包：允许不允许□

二、需要落实的政府采购政策

本项目落实节能环保、中小微型企业扶持、支持监狱企业发展、残疾人福利性单位扶持等相关政府采购政策。

三、投标人资格要求

（一）具备《政府采购法》第二十二条第一款规定条件并提供相关材料。

（二）本次招标接受□不接受联合体投标。

四、采购需求

（一）采购清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 主要技术参数 | 单位 | 数量 | 核心产品 |
| 1 | 云计算虚拟化实训平台 | **一、基本功能**  1、系统采用B/S架构，学生做实验时不需加载客户端程序。  2、支持基于WEB的用户注册功能，用户自己可以修改个人信息，用户类型分为学生、教师、管理员和科研用户四种类型，管理员和科研用户能新建和管理虚拟机，科研用户新建的虚拟机必须由管理员审核。  3、云平台虚拟化集群管理功能，包括：  （1）分布式计算资源池管理：平台可动态增加、移除计算资源；新增计算资源后，平台可用的CPU数量和内存容量能够动态增加，并且由系统管理模块自动调度；配置能够满足本次招标产品所用的CPU授权许可。  （2）分布式存储资源管理：平台可动态增加、移除存储资源；新增存储资源后，平台可用的存储容量动态增加，在平台上新增课件及实验场景时，存储资源可即时同步，无需手动更新；  （3）分布式资源调度：平台可自动对资源按性能进行自动调度，实现负载均衡，不需要设置任何的阈值；  （4）系统资源监控：平台能对资源中所有节点进行监控，包括节点的CPU、RAM使用状态以及节点的可用性状态，对不可用节点可进行告警提醒；  4、云平台虚拟化管理功能，包括：  （1）支持在绘制拓扑界面直接点击设备打开设备的操作窗口，支持Windows、Linux、命令行管理模式；  （2）在Windows、Linux设备操作窗口支持文件上传，通过浏览器上传任意文件到虚拟机中，上传操作不使用USB接口，向虚拟机写入文件不依赖物理网络和虚拟网络；  （3）初始化设备时，可以将虚拟机映射为外部可以直接访问的地址及端口号，在外部环境中可以使用图形化和命令行远程工具连接拓扑环境中的虚拟机；  （4）支持拓扑映射到服务器的物理网口，将外部物理设备接入拓扑中，实现流量导出和回注操作，外部设备可直接访问拓扑中的设备；  5、设备内置DHCP服务器。  **二、课程管理**  6、支持必修课和选修课两种类型的课程。  7、提供实验报告的撰写、打印、导出功能。  8、支持用户课件的上传，提供用户上传课件内容后的在线浏览功能，同时可以在线下载课件。支持HTML、PPT、WORD、PDF、SWF、scom等格式。  9、上传课件支持HTTP和FTP方式。  10、支持串流大师4.0和Articulate Presenter‘09的课件导入。  11、支持对互联网或者设备外部课件资源的链接方式。  **三、实验管理**  12、支持实验分类管理、课程管理和实验调度管理。  13、实验拓扑设计，包括：  （1）支持图形化拖拽方式绘制拓扑、绘制拓扑能够保存；  （2）定制拓扑界面中，支持直接点击拓扑图中的相关设备（PC、服务器）能够进入参数配置界面，修改CPU、内存、网卡数量、启动方式、挂载ISO、映射端口；  （3）支持任意两个设备间绘制连线实现网络连通，点击设备时出现端口选择列表，选择任意端口与对端设备的任意端口连接；  （4）拓扑中的设备支持自由拖动，构建规整美观的网络拓扑图；  14、支持虚拟化设备和真实网络设备同时加入到同一个网络拓扑中。  15、虚拟化设备支持虚拟化防火墙、虚拟化路由器、虚拟化交换机，以上虚拟化设备运行时必须启用真实的网络操作系统IOS(非仿真系统)，可根据用户需求定制虚拟机，至少包括网络设备、基础服务器、web服务器、数据库、移动终端、PC终端等类型的母版和模板镜像系统（母版为基础镜像，模板集成测试环境），设备模板至少提供以下类型：  （1）网络设备：交换机、路由器、防火墙等；  （2）基础服务器：WinXP、Win2K、Win2K3、Win2K8、Win7、Win8、Ubuntu、Debain、RedHat、Centos、openSUSE、Fedora、中标麒麟；  （3）Web服务器：dedeCMS、Discuz!、DESTOON、phpwind、IIS、Apache、Nginx、Tomcat、Weblogic；  （4）数据库服务器：Oracle、MySQL、MSSQL；  （5）移动终端：Android Lollipop、Android Marshmallow、Android Nougat；  （6）PC终端：WinXP、Win7、Win8、Win10、Ubuntu；  16、提供对实验课件工具的启用，禁用设置，被禁用的实验工具无法使用。支持把实验工具和实验课件相关联，以便创建课程和开展实验。  17、老师可通过远程查看学生的实验过程，了解学生对课程的掌握情况。  18、系统提供用户项目式教学功能，实现用户自定义网络拓扑功能，组网设备包含虚拟主机系统、虚拟化防火墙、虚拟化路由器、虚拟化交换机等网络设备，虚拟化设备之间能够进行网络通讯，所组建的网络环境可以供多名学生同时使用进行项目训练，无需其他设备支持，完全虚拟化构建网络。  **四、考试管理**  19、支持题库管理、课程考试管理；支持查询统计、查看学生学习情况、查看学生考试结果、查看学生在线人数；  **五、硬件配置**  20、硬件配置：标准机架式，CPU：Intel 至强 E3，线程 数量：8（四核心八线程），主频：3300MHz ；内存：32GB；硬盘：1 块 7200 转 1T，1 块 SSD 120G；千兆网络接口≥2，支持云平台虚拟化集群管理。  21、支持至少20个独立的虚拟系统的同时加载并能够流畅的运行。  **六、实训内容**  22、平台至少满足以下类型的实训教学，实训教程数量不少于1200个，每个实验教程必须具有实验场景及配套电子实验教学文档，包含实验类型如下：  (1)密码学;(2)密码学应用;(3) PKI;(4)应用系统安全;(5) linux系统;(6)操作系统安全;(7)数据库安全;(8)计算机病毒分析实验;(9)安全审计;(10)容灾备份;(11) Web安全实验;(12)网络安全实验;(13) bt5;(14)安全风险评估;(15)防火墙;(16)入侵检测;(17) VPN;(18)漏洞扫描;(19)网络扫描与嗅探;(20)密码破解技术;(21)数据库攻击技术;(22)网络欺骗技术;(23)系统安全策略配置技术;(24)网络设备攻击技术;(25)安全攻防分析;(26)数据保密与安全;(27)隐写软件安装及使用;(28)信息隐藏;(29)数字水印;(30)缓冲区溢出技术与漏洞分析;(31)恶意代码分析;(32)逆向工程技术;(33)软件安全防护;(34)软件水印;(35)安全编程;(36)计算机取证和司法鉴定;(37)基础网络实训;（38）ACCESS实训;（39）SQLServer 实训;（40）MySQL 实训;（41）C语言 实训;（42）VC++实训 ;（43）C#实训 ;（44）JSP实训;（45）PHP 实训。 | 台 | 2 |  |
| 2 | 信息安全实战智能靶机平台 | 1、硬件配置：标准机架式，CPU：Intel 至强 E3，线程 数量：8（四核心八线程），主频：3300MHz ；内存：32GB；硬盘：1 块 7200 转 1T，1 块 SSD 120G；千兆网络接口≥2，支持至少20个独立的虚拟系统的同时加载并能够流畅的运行，支持云平台虚拟化集群管理。  2、支持靶机智能调度功能：系统根据不同的实战任务下发进行自动调度靶机虚拟化模板。  3、支持靶机通告管理:系统支持靶机模板将自己的被攻击状态自动通告给监控管理模块。  4、支持靶机任务下发管理:系统提供可以增加任务列表，下发任务给学生。  5、靶机漏洞虚拟化模板数量不低于100个，支持用户自定义靶机模板，系统基本靶机漏洞模板至少提供如下漏洞场景：  (1)Apache服务器的banner获取与隐藏；(2)IIS服务器banner获取与隐藏；(3)apahce目录遍历漏洞及修复；(4)IIS目录遍历漏洞及修复；(5)IIS解析漏洞；(6)php cgi解析漏洞（nginx）；(7)apache解析漏洞；(8)tomcat部署war包木马并利用；(9)weblogic部署war包木马并利用；(10)JBoss部署war包木马并利用；(11)struts2漏洞；(12)jboss invoke接口未授权访问；(13)jboss反序列化漏洞利用；(14)weblogic反序列化漏洞利用；(15)IISPUT上传漏洞多种探测方式及利用；(16)sql注入整型报错注入；(17)sql注入单括号注入报错；(18)sql注入双引号报错注入；(19)sql注入字符型报错注入；(20)sql注入双注入；(21)sql注入写入读取文件；(22)sql注入bool注入；(23)sql注入sleep注入；(24)sql注入update注入；(25)sql注入POST注入；(26)sql注入cookie注入；(27)sql注入useragent注入；(28)pangolin使用；(29)sqlmap之acess注入；(30)sqlmap之mysql数据库注入；(31)sqlmap之Cookie注入；(32)sqlmap之post登陆框注入；(33)sqlmap之交互式写shell及命令执行；(34)sqlmap之常规伪静态注入；(35)sqlmap之伪静态中转注入；(36)sqlmap之请求延时注入；(37)sqlmap之绕过WAF防火墙；(38)sqlmap注入指定数据库；(39)sqlmap模板使用；(40)mysql手工注入(php)；(41)mssql手工注入(aspx)；(42)access手工注入(asp)；(43)wvs使用；(44)appscan使用； (45)burpsuit使用；(46)文件上传漏洞type绕过；(47)文件上传漏洞扩展名绕过；(48)文件上传漏洞JS绕过；(49)头文件上传绕过；(50)本地文件包含之读取敏感文件；(51)本地文件包含之包含日志获取webshell；(52)远程文件包含shell；(53)远程文件包含写shell；(54)本地包含配合文件上传；(55)文件包含PHP封装协议之读取文件；(56)文件包含PHP封装协议之读写文件；(57)文件包含PHP封装协议之命令执行；(58)文件包含file封装协议之读取文件；(59)利用数据库备份获取shell；(60)利用burpsuit暴力破解弱口令；(61)ASPX大马的使用；(62)JSP大马的使用；(63)php大马的使用；(64)udf木马提权；(65)简单提权；(66)Win2003溢出提权；(67)mysql弱口令提权；(68)SQL Server弱口令提权；(69)windows远程桌面协议RDP拒绝访问漏洞；(70)win2008溢出提权；(71)开启3389；(72)反射型xss；(73)存储型xss；(74)DOM型xss；绕过过滤；(75)xss会话劫持；(76)thinkphp命令执行；(77)eWebEditor；(78)命令执行漏洞；(79)php命令执行；(80)php代码执行；(81)php动态函数调用；(82)php函数代码执行漏洞；(83)CSRF GET型；(84)CSRF POST型；(85)AWVS基本操作；(86)AWVS http editor功能使用；(87)AWVS http fuzzer测试xss；(88)awvs http fuzz穷举密码；(89)awvs http fuzz寻找sql注入；(90)awvs http sniffer抓包；(91)awvs site crawer；(92)AWVS Target finder功能使用；(93)AWVS 扫描子域名；(94)AWVS定制化扫描；(95)awvs破解401认证；(96)wce抓取系统hash和明文密码；(97)Powershell 管道；(98)PowerShell (90)进行数学运算；(100)Powershell 执行外部命令. | 台 | 1 |  |
| 3 | 信息安全实战渗透平台 | 1、硬件配置：标准机架式，CPU：Intel 至强 E3，线程 数量：8（四核心八线程），主频：3300MHz ；内存：32GB；硬盘：1 块 7200 转 1T，1 块 SSD 120G；千兆网络接口≥2，支持至少20个独立的虚拟系统的同时加载并能够流畅的运行，支持云平台虚拟化集群管理。  2、渗透虚拟化模板:渗透模板至少包括Kali、BT5、Web攻击机、移动端攻击机、逆向攻击机、NodeZero Linux、BackBox Linux、Blackbuntu、Samurai Web Testing Framework、Knoppix STD、Pentoo、WEAKERTH4N等渗透攻击主机模板，并支持用户自定义模板功能。  3、支持渗透模板智能调度功能:系统根据不同的实战任务下发进行自动调度渗透虚拟化模板功能。  4、支持渗透模板通告管理:系统提供渗透模板将用户实时的作战动作自动通告给监控管理模块。 | 台 | 1 |  |
| 4 | 信息安全竞赛平台 | 1、硬件配置：标准机架式，CPU：Intel 至强 E3，线程 数量：8（四核心八线程），主频：3300MHz ；内存：32GB；硬盘：1 块 7200 转 1T，1 块 SSD 120G；千兆网络接口≥2，支持至少20个独立的虚拟系统的同时加载并能够流畅的运行，支持云平台虚拟化集群管理。  2、系统支持利用信息安全理论知识，通过理论、个人对抗、分组对抗和夺旗四种竞赛相结合的方式进行信息安全对抗技能实战竞赛。  3、支持基于知识点均衡的智能组卷方案：系统提供近几年高校信息安全竞赛大赛赛题，通过考试题库管理功能，将题目按照科目类别分门别类的存储，通过考场管理、试卷管理的功能进行基于知识点均衡的智能组卷方法。可按课程分类搜索试题、可按知识点搜索试题，智能组卷中心支持自由组卷、智能试题分析与测评。  4、系统提供真实的攻防环境：包括目标主机、操作系统、漏洞均是真实存在的，入侵、防护过程完全真实  5、个人挑战赛：以典型的计算机信息网络为竞赛内容和考察重点：分为基础、脚本、破解、溢出、内核、综合六种题型。  6、关卡竞赛：考核内容涉及WEB知识、ASP/PHP脚本、缓冲区溢出、软件脱壳破解、系统漏洞利用、社会工程学等信息安全知识。  7、分组对抗：在封闭的真实对抗环境（包括DMZ区、数据区、开发测试区、内网服务区、终端区）中展开攻防角逐，考核各位选手的个人水平和小组的协同合作能力. | 台 | 1 |  |
| 5 | 三层交换机 | 1.10/100/1000M电口≥24，千兆光接口≥4；  2.交换容量≥250Gbps，包转发率≥90Mbps；  3.支持802.3ad，支持STP、RSTP、MSTP协议，支持端口镜像、远程端口镜像等；  4.支持静态、RIP/RIPng、OSPF/OSPFv3、IS-IS/IS-ISv6、BGP4/BGP4+等路由协议；  5.支持Super Vlan 、MAC Vlan、灵活QinQ、Voice Vlan、Protocol Vlan、subnet Vlan、Private Vlan等vlan特性；  6.支持PIM-SM/DM、DVMRP等IPv4/IPv6组播路由协议，支持信源受控组播、目的受控组播、策略组播等IPv4/IPv6受控组播功能；  7.每个端口提供≥6个优先级队列，可分别设定队列带宽，支持WRR/SP/SWRR/DWRR/SDWRR/WRED等调度方式；  8.内置 DHCPv4及DHCPv6 Server，可对客户端分配地址，节省地址分配服务器的投资；  9.支持防DOS攻击、CPU安全防护等技术，保障设备在攻击环境下正常转发数据；  10.支持基于源/目的IP、IP协议类型、IP优先级、TCP\UDP源和目的端口号，TCP\UDP端口范围，以及基于上述类型的组合的ACL，提供丰富的安全以及业务策略；  11.支持MPLS转发，MCE，LDP，访问公网；  12.支持MAC+端口捆绑、IP+MAC＋端口绑定(v4/v6)、IP+端口绑定(v4/v6)，支持端口MAC过滤，端口限速（带宽管理），广播风暴控制等；  13.支持防止ARP扫描 、ARP网关防护功能；  14.支持802.1X、Web Portal等认证方式；  15.支持基于温度传感实现温度监控、温度告警，可根据环境温度实时调节风扇转速，实现节能降噪；  16.支持SNMP、RMON、SSH、Telnet、Web等管理方式； | 台 | 1 |  |
| 6 | 防火墙 | 1、采用多核网络处理器或ASIC的纯硬件架构，非X86。配备能够独立使用的千兆口≥8个，1个console口，1个AUX口，1个USB口。  2、最大并发连接数≥250，000  3、支持nat、路由、透明等组网模式  4、支持IPv6/v4双栈  5、支持PPPOE客户端，支持单接口同时发起多个PPPOE拨号连接  6、支持扩展NAT地址转换，提升单个合法IP的转换的会话数数量，节约合法IP占用  7、802.1Q trunk封装、端口镜像、STP/RSTP等  8、可根据认证后的用户/用户组/用户角色分别设置其上、下行的最大带宽、预留带宽，并可定制带宽策略的生效时间。  9、可根据IP/应用/认证用户/自定义数据流/时间/DSCP/CoS/等多种元素制定高级复合带宽管理策略分别控制上下行的最大、最小带宽及保证带宽  10、可以实现基于源/目的IP地址，服务，、协议、端口、用户，组和时间的访问控制  11、支持 SSL VPN客户端安全完整性检查、SSL VPN用户帐号与主机绑定、SSL VPN用户帐号与IP绑定；SSL VPN用户数最大可扩128个，本次配置4个，支持USB Key  12、支持在线病毒防护，采用并行流扫描引擎，文件接收传送的同时进行病毒扫描，减少延迟；病毒库须能够本地手工升级和自动在线升级  13、可对HTTP\FTP\POP3\SMTP\IMAP等协议进行病毒检测，可对压缩文件进行病毒检测，可对多重压缩文件进行病毒检测，须支持RAR、ZIP、GZIP、BZIP2、TAR等压缩文件类型，扫描文件的大小无限制.  14、支持P2P应用识别和阻断；IM类识别和阻断；网络游戏类识别和阻断；在线视频类识别和阻断；炒股可识别和阻断等  15、支持URL分类过滤，控制用户对不良网站的访问，URL分类库包含的web站点数量≥2000万  16、可对Web页面内容可进行关键字过滤  17、可根据收件人/发件人/邮件正文关键字/附近名称对收发邮件行为进行阻断或审计  18、可设置关键字阻断或审计用户论坛发贴内容  19、支持对主流DoS和DDos攻击的防护  20、支持上网行为日志统计,支持对每接口上下行流量的监控统计，支持对每IP上下行流量的监控统计，支持对每IP会话数的监控统计，支持对主流应用占用带宽情况和会话数的监控统计，支持针对应用的带宽占用统计和会话数量统计 | 台 | 1 | 是 |
| 7 | 无线控制器 | 1、整体要求：学生通过该产品的实训，能够达到参加全国职业院校技能大赛高职组“信息安全管理与评估”赛项无线控制器竞赛的要求。  2、交换业务：交换容量≥480Gbps；Ipv4包转发速率≥200Mpps  3、CAPWAP：AP和AC之间支持L2/L3层网络拓扑；AP可以自动发现可接入的AC；AP可以自动从AC更新软件版本、自动从AC下载配置；AP可以自动从AC下载使用报告；支持CLI方式管理（支持Telnet、SSH、Console方式）；支持SNMP，支持SYSLOG协议；  4、管理特性：支持802.11 a/b/g/n协议；支持WDS；支持对所有AP(802.11a/b/g/n)进行统一管理，AP真正零配置上线；支持对AP的分组管理，不同的分组可以配置不同的认证方式、加密方式以及相关的所有WLAN特性；802.11吞吐量为单向64G，双向128G；  5、支持集中转发和本地转发两种转发方式；控制器可控制关闭所连AP的11b信号，从而优化目前主流11g，n终端的无线性能；支持信道自动控制，支持指定信道；支持功率自动控制，支持指定功率；支持带宽管理控制，最小精度8Kbps；  6、支持二三层快速漫游，跨AC、AP漫游，漫游中断时间≤30ms；对非法未授权无线AP的侦测并拒绝接入无线网络；检测未知AP假冒合法的SSID，非法AP抑制与攻击支持二三层用户隔离，登录到无线的用户之间不能互相访问；支持基于MAC地址过滤的二层ACL；  7、IPV6特征：支持IPV4/V6双栈、6to4隧道、IPv4 over IPv6 隧道；DHCPv6、DNSv6、SNMP v6、Ping v6、Telnet/SSH v6、IPv6 QoS；  8、SSID特征：支持IEEE 802.1Q标准的VLAN标记，并且可以根据SSID来划分VLAN，单一SSID映射到多个VLAN的功能；支持为用户提供不同的带宽限制，支持对整个SSID进行带宽控制；支持不少于32组SSID，实现基于不同SSID下的用户身份验证，无线加密，访问控制，上下行链路速率限制、VLAN等的安全功能；不同SSID能够弹出不同的Portal页面，并能使用不同的认证方式，Portal页面能够定制；  9、QoS：支持不同SSID映射不同QoS策略；支持802.11e(WMM)；支持基于用户数量的负载均衡；支持AP负载能力的负载均衡；支持对语音、视频、数据等不同流量设置优先级；支持对每个SSID上下行流量限速；  10、安全/认证：MAC地址认证；支持802.1x认证(EAP-TLS， EAP-TTLS， EAP-PEAP， EAP-MD5)；支持EAP透传功能；支持Captive Portal认证，且支持Captive Portal界面客户自定义；支持入侵防护以防止无线网络收到过多的无效无线请求；支持 PSK；支持Radius Client/Server，支持Radius通讯接口，支持标准Radius RFC协议，可以与第三方Radius互通；支持LDAP，可实现与LDAP服务器直接认证，不需要经第三方Radius服务器跳转；能够完成计费信息的采集，如用户信息，连接时长，数据流量；能够侦测用户下线，并在控制器端实现强制用户下线；  11、可靠性：AC支持1+1、N+1、N+N冗余备份方式；电源冗余；  12、网络管理：支持WEB 管理，支持Console口配置，SNMP v1/v2c/v3， SYSLOG。  13、物理参数：千兆POE接口≥24，千兆SFP光口≥4，万兆SFP+光口≥4，支持双热插拔AC & DC电源，标配标配1个交流电源模块；配置8台AP管理许可。 | 台 | 1 |  |
| 8 | 无线接入点 | 1.整体要求：学生通过该产品的实训，能够达到参加全国职业院校技能大赛高职组“信息安全管理与评估”赛项无线接入点竞赛的要求。  2.通过802.3af供电,绿色环保；  3.支持电源适配器供电，为保障实施安全，供电电压<24V；  4. 空间流数≥2,无线数据传输速率≥1.167Gbps；  5.支持IEEE802.11a/b/g/n/ac标准，可同时工作在802.11a/n/ac、802.11b/g/n模式；  6.支持IPV6接入和转发功能：支持在IPv4网络中构建IPv6的WLAN接入服务，支持在IPv6网络中提供IPv4的WLAN接入服务，支持在IPv6网络中构建私有的IPv6的WLAN网络服务；  7.支持无线SAVI功能，防ARP欺骗与防私设IP地址  8.支持不少于32个SSID，每个SSID可单独配置安全策略，认证方法，RADIUS服务器和VLAN ID；  9.AP能存储两份image，当前启动失败后切到备份image启动 ；  10.USB接口≥1，提供灵活扩展；  11.支持瘦AP模式/胖AP模式切换；  12.支持WPA/WPA2,TKIP 和 PSK，802.11i AES，以实现增强型无线安全功能；  13.支持802.1x认证，支持AP、AC双向数字证书的认证；  14.硬件配置：≥1个10/100/1000Base-T端口，≥1个10/100Base-T端口，≥1个RJ45的Console口； | 台 | 1 |  |
| 9 | 冷暖空调 | 定频,2P柜机冷暖空调，柜机，节能环保 | 台 | 2 |  |
| 10 | 综合布线 | 根据现场实际需求进行布线 | 批 | 1 |  |

（二）验收标准

由采购人成立验收小组,按照采购合同的约定对中标人履约情况进行验收。验收时,按照采购合同的约定对每一项技术、服务、安全标准的履约情况进行确认。验收结束后,出具验收书,列明各项标准的验收情况及项目总体评价,由验收双方共同签署。

五、评标方法和评标标准

（一）评标方法：最低评标价法□ 综合评分法

（二）综合评分法评标标准：

|  |  |  |
| --- | --- | --- |
| 分值构成  (总分100分) | 价格分值： 50 分  商务部分： 15 分  技术部分： 35 分 | |
| **一、价格部分（满分50分）** | | |
| **评分因素** | **评分标准** | **分值** |
| 投标报价  评分标准 | 评标基准价：满足招标文件要求的有效投标报价中，最低的投标报价为评标基准价。  投标报价得分=（评标基准价/投标报价）×50 | 50 分 |
| **二、商务部分（满分16分）** | | |
| **评分因素** | **评分标准** | **分值** |
| 信誉 | *1*、投标人须提供工商企业信用信息公示报告【国家企业信用信息公示系统http//www.gsxt.gov.cn包括基础信息、行政许可信息、行政处罚信息、列入经营异常名录信息、列入严重违法失信企业名单（黑名单）信息】、企业所在地税务主管部门出具的纳税情况证明等信用情况，无不良信息者每项1分，未提供或有不良信息者不得分，满分2分。  2、根据投标人在本项目以前社会对其认可度以及行政主管部门、工商、银行、行业部门颁发的荣誉证书等情况评定，基本分1分，每提供一份荣誉证书加1分，满分3分。 | 5分 |
| 业绩 | 2012年以来具有类似项目业绩，合同及验收报告齐全的，每个2分，满分8分（以合同日期为准）。（以原件为准） | 8分 |
| 投标文件规范程度 | 1、装订规范、文字清晰、无差错1分，  2、所提供资料准确完整1分。 | 2分 |
| **技术部分（满分35分）** | | |
| **评分因素** | **评分标准** | **分值** |
| 对招标文件  响应程度 | 1、不满足招标文件技术指标要求和商务条款规定的为无效投标。  2、满足招标文件技术要求的基本分28分。 | 28分 |
| 技术实力 | 投标人拟派技术人员（两名及以上）具有所投产品厂商认证的高级网络工程师证书，得4分（须提供证书原件）。 | 4分 |
| 售后服务 | 1、解决问题时间：以小时为单位（四舍五入法，30分钟及以上按1小时计算），以24小时为起点，基本分0.5分，每减少1小时，加0.5分，满分1分。  2、免费保修时间：以年为单位（四舍五入法，6个月及以上按1年计算），以1年为起点，基本分1分，每增加1年加1分，满分2分。1年以下的不得分。 | 3分 |

六、采购资金支付

（一）支付方式：银行转账

（二）支付时间及条件：经验收合格付合同总价款的90%，剩余10%满一年无质量问题一次付清。

七、联系方式

联系人姓名： 王甫      联系电话：18503749668

单位地址：新兴东路4336号 许昌职业技术学院