**网络安全与管理设备采购需求**

 一、项目概况

（一）项目名称：网络安全与管理设备

（二）采购方式：竞争性谈判

（三）主要内容、数量及要求：负载均衡1套、WEB应用防火墙1套、上网行为管理1套。

（四）预算金额：47.5万元 ；最高限价：47.5万元。

（五）交付（服务、完工）时间：合同签订后15个工作日内。

（六）交付（服务、施工）地点：河南省许昌电气职业学院网络管理中心机房。

（七）进口产品：不允许。

（八）分包：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√、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）本次招标不接受联合体投标。

四、采购需求

（一）本项目需实现的功能或者目标

1、有效管理校园网出口链路，提高各链路的利用率，保障网络出口稳定。

2、为学院网站、信息系统提供网络安全防护。

3、对校园网进行认证管理、应用管理、数据管理、溯源等。

（二）采购清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 货物  名称 | 技术规格及主要参数 | 单位 | 数量 | 是否为核心产品 |
| 1 | 链路负载均衡 | 1、 设备性能：  6个千兆电口，6个千兆光口（非光电复用），满配光模块；标准2U设备;四层吞吐量≥5.5G，并发连接数≥400W，四层新建连接数≥30W，七层新建连接数≥15W，SSL新建性能≥6000TPS，增加4条多链路授权；  2、 设备部署：  支持串接部署方式和旁路部署方式，支持三角传输模式；设备支持在IPV6环境下的部署并配置策略，其所有功能都支持IPv6，具有IPv6 Ready Phase-2认证。  3、电源：  标准机架式设备，冗余电源设计且满配。  4、多合一功能集成:  1）提供针对多条出口线路的链路负载均衡功能，实现inbound和outbound流量的均衡调度，以及链路之间的冗余互备。  2）提供针对L4/L7内容交换的服务器负载均衡功能，可在单一设备上支持多个应用和服务器集群，可以根据多种算法和要求分配用户的请求。  3）提供针对多站点业务发布的全局负载均衡功能，通过智能DNS等机制实现内外网用户对多个数据中心的最优接入路径选择  4）单一设备可同时支持包括链路负载均衡、全局负载均衡、服务器负载均衡的功能。以上功能同时处于激活可使用状态，无需额外购买相应授权。（提供设备操作界面截图)  5、负载均衡算法：  支持轮询、加权轮询、加权最小连接、动态反馈、最快响应、最小流量、带宽比例、哈希、主备、首个可用、优先级等算法。  6、可编程流量控制：  通过某种编程语言（如lua）实现自定义的流量编排，对TCP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。（提供设备操作界面)  7、链路负载均衡：  1）支持静态IP和PPPOE两种线路接入方式。（提供设备操作界面截图）  2）支持对不少于200条的线路进行流量负载均衡（提供设备操作界面截图）  3）支持基于五元组条件（源IP地址，源端口，目的IP地址，目的端口，传输层协议号）来进行出站访问的流量调度分发。  4）支持基于管理员自定义时间计划来进行出站访问的流量调度分发。（提供设备操作界面截图）  5）内置完备的IP地址库，无需手动导入并支持自动更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能（提供设备操作界面截图）  6）支持基于访问目标域名的链路负载，可根据访问的目标域名进行链路选择。（提供设备操作界面截图）  7）内置国外域名地址库，国外域名不少于10万条，支持自动更新。可将访问国外域名的请求分发至指定线路，实现对国外域名访问的优化，提升用户体验。（提供设备操作界面截图）  8）支持应用引流，可识别游戏、视频、网银等应用，并根据应用类型进行流量调度分发。（提供设备操作界面截图）  9）支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（提供设备操作界面截图）  10）支持DNS内网记录，包含A、AAAA、CNAME、MX和TXT等类型，可识别内网用户并对其DNS请求直接返回相应结果；支持智能DNS解析功能，实现外网用户访问内网业务系统的最优路径选择。  11）支持基于链路负荷情况的繁忙保护机制，能根据链路的上行/下行带宽占用率情况执行对出站/入站流量的高级调度策略。（提供设备操作界面截图证）  12）支持多种链路检测方法，能够通过PING、TCP、HTTP等方式监控链路的连通性，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅。  8、服务器负载：  1）支持源IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session ID等多种会话保持机制。  2）支持常见的主动式健康检查功能，提供基于SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL数据库等多种类型的探测判断机制。  3）支持用户自定义方式的健康检查，支持多种编程语言（如Python、Java等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。（提供设备操作界面截图）  4）支持节点智能恢复，当节点出现故障时，负载均衡能自动重启服务器上的相关进程或重启服务器，使其恢复正常状态并继续提供服务；如无法使其恢复正常，则将其从节点池中移除，保证业务正常访问。（提供设备操作界面截图）  5）支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。（提供设备操作界面截图）  6）支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性。（提供设备操作界面截图）  7）可通过读写分离等技术手段实现数据库负载均衡，至少包括MySQL、Oracle、MSSQL等类型的数据库。以MySQL为例，通过对数据库操作请求做内容解析，将其中的写操作调度到指定服务器，读操作则调度到所有节点，提高数据库资源使用率，无需在服务器上安装任何插件。（提供设备操作界面截图）  8）对于非HTTP协议的长连接应用，可通过分析特征来识别消息的开始和截止，以消息为对象进行七层负载均衡，而非传统基于连接的四层负载均衡。 | 套 | 1 | 否 |
| 2 | WEB应用防火墙 | 1. 硬件规格：   1）专业WEB防火墙设备，非防火墙或NGAF、NGFW、UTM设备功能模块扩展；为自主研发且非OEM产品。  2）标准机架2U设备，冗余电源设计且满配，10个10/100/1000 Base-T接口，4个千兆SFP光接口插槽（非光电复用），实配4个光模块，2个USB3.0口，1个RJ45串口。  3）外置存储接口，配置全部接口开通使用授权。   1. 性能要求：   设备整机网络层吞吐量5G，应用层吞吐量2G，最大http并发连接数300万，每秒新建http连接数4万。  3、接入模式：  1）支持透明、代理模式、旁路部署、单臂部署、策略路由部署。  2）支持智能部署，上线WAF设备能够自动感知Web网站IP和端口(要求提供界面截图)。  3）支持安装向导式部署，按照该部署方式可直接部署完成。  4）支持静态路由、地址映射配置。  5）支持NAT环境下的用户识别能力。  6）支持IPv6，具有IPv6 Ready认证。  4、Web攻击防护：  1）具备SQL注入攻击的检测与防御能力。  2）具备XSS攻击的检测与防御能力。  3）具备Web恶意扫描防护的检测与防御能力。  4）具备虚拟补丁功能，支持扫描器扫描结果导入，支持根据扫描结果自动生成防护策略(要求提供界面截图)。  5）具备蜜罐检测功能，诱使攻击方对它实施攻击，从而可以对攻击行为进行捕获和阻断(要求提供界面截图)。  6）具备暴力扫描防护功能，防止暴力破解网站。  7）具备恶意文件检测功能，可对文件进行检测看是否恶意文件。  8）具备业务合规功能，可对业务进行恶意试探、恶意撞库、恶意登录等行为进行检测及拦截。  9）具备XML DoS检测与防御能力。  10）具备SYN Flood/UDP Flood/ICMP Flood攻击检测与防御能力。  11）具备网站锁功能，对网站进行锁定，可按日期、周期进行锁定时间设置(要求提供界面截图)。  12）具备源访问区域控制功能，可按照国家、省进行地址访问限制，防止区域性攻击对Web网站造成影响。  13）具备Web环境感知功能，自动识别被保护服务器操作系统、服务器类型、语言、中间件(要求提供界面截图)。  14）具备慢速攻击防护功能，有效防护Slow headers 方式、Slow body方式、Slow read方式等慢速攻击。  15）具备弱口令防护功能，可检测用户使用弱口令登录、检测用户注册密码强度等功能。  16）具备HTTP Flood（CC攻击）检测与防御能力。  17）Web非授权访问防护，具备CSRF攻击检测与防御能力，CSRF支持自学习功能。  18）支持Cookie信息防篡改功能，至少包括Cookie签名、Cookie自学习、Cookie加密等属性设置。  19）具备客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问。  20）支持网站盗链行为检测与防御。  5、Web恶意代码防护：  1）具备网页挂马检测与防御能力。  2）具备WebShell检测与防御能力  6、Web应用合规：  1）具备基于URL的应用层访问控制功能。  2）支持针对HTTP的请求头信息进行合规性检查。  3）支持针对指定的URL页面，对HTTP请求信息中的方法以及参数长度等信息进行检测。  4）支持Web服务器操作系统指纹信息返回保护。  5）支持Web服务器信息返回保护。  6）支持HTTP错误页面信息返回保护。  7）支持银行卡信息返回保护  8）支持身份证信息返回保护  9）支持文件上传下载控制功能。  10）支持真实文件识别功能。  11）支持Web表单关键字过滤功能。  7、Web应用交付：  1）支持针对重点URL的网页防篡改功能，同时不会对Web服务器及Web应用系统造成额外影响。  2）支持基于URL的流量控制功能(要求提供界面截图)。  3）支持多服务器负载均衡功能，应至少支持3种负载均衡算法。  8、实时监控：  1）支持针对Web安全事件的实时监控。  2）支持针对Web应用连接状况和流量信息的实时监控(要求提供界面截图)。  3）支持针对Web服务器服务质量的实时监控。  4）支持指定Web页面访问状况的实时监控。  5）支持设备资源使用情况的实时监控。  6）支持Web安全事件的分级上报、监控、统计功能  9、系统管理：  1）应具备设备集中管理功能，可实现设备分布式部署、集中式监控管理，适合大规模部署环境。  2）具备多设备拓扑显示功能，可以在界面上以图形化的方式显示当前的部署拓扑。  10、升级管理：  应保证Web应用防护事件库的定期与应急升级，保证重大、突发Web安全事件的及时响应。  11、安全联动：  支持和业务审计系统联动，满足用户对Web应用安全防护和审计需求。  12、产品资质：  设备厂商须具有《计算机信息系统安全专用产品销售许可证》，提供复印件。 | 套 | 1 | 是 |
| 3 | 上网行为管理 | 1、产品性能：硬盘≥500G；吞吐量≥5Gbps；并发会话数≥2,000,000；用户规模≥20,000。  2、电源：标准机架式设备，冗余电源设计且满配。  3、端口：≥8个千兆电口，≥4个千兆光口（非光电复用），满配光模块；2个高速USB2.0接口，1个RJ45口，并带有富余的扩展接口。  4、部署方式：支持网桥模式部署、旁路模式部署，支持多机模式部署，具备故障BYPASS功能；在各种合理控制策略开启的情况下，至少具备5G以上的实际流量处理能力。  5、IPv6：支持部署在IPv6环境中，其所有功能（认证、应用控制、内容审计、报表等）都支持IPv6；（提供产品界面截图）支持IPV6用户身份认证，支持与IPV4同时做用户管理；支持IPV6网络的应用识别、网页过滤、应用控制和行为审计（提供产品界面截图）；支持IPV6网络配置两台或者多台设备多机配置（提供产品界面截图），具有IPv6 Ready Phase-2认证。  6、设备管理：支持通过IE、firefox等浏览器通过SSL加密WEB方式、SSH命令行方式管理设备；支持从CF卡启动，支持CF系统备份；硬件上支持国产和silicom受控式bypass，支持千兆和万兆，多模和单模的任意搭配；支持v1、v2、v3方式连接设备SNMP服务；支持设备配置备份与恢复，能够识别终端操作系统版本、系统补丁安装情况，能够识别终端系统后台运行的进程信息，防止间谍软件的运行。  7、网络配置：支持在IPV4/IPv6环境下做静态路由（提供产品界面截图）。支持对IPV4/IPv6的L2TP、MPLS、PPPoE、Q-in-Q的协议剥离，即支持在以上环境中做行为管理（提供产品界面截图）。  8、用户管理：支持触发式WEB认证，静态用户名密码认证、以USB-Key方式实现双因素身份认证、短信认证、微信认证、访客二维码认证；支持LDAP、Radius、POP3、Proxy等第三方认证；支持ISA\lotus ldap\novel ldap\oracle、sql server、db2、mysql等数据库等第三方认证。  9、网络实时监控：提供设备实时CPU、内存、磁盘占有率、会话数、在线用户数、系统时间、网络接口等信息；实时提供用户流量排名、应用流量排名、所有线路应用流速趋势、流量管理状态、连接监控信息：实时显示设置过滤条件的用户上网行为监控，支持手动设置刷新时间。  10、网页过滤：设备内置千万级URL，具有完整URL分类，保持每两周更新一次，同时支持URL智能识别，保障网页识别率；支持根据网页类型过滤访问的http、https网站；支持根据网页搜索关键字过滤访问的网站，并发送告警邮件；支持根据关键字过滤http上传内容，并发送告警邮件。  11、应用控制：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；（提供产品界面截图）支持应用标签化，每个应用支持列上图标；支持应用细分控制，如针对网易网盘、金山快盘、华为网盘等区分登录、上传、下载等动作进行分别控制。  12、标签：支持根据标签选择应用，标签分类至少包含安全风险、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；支持给每个应用自定义标签；支持根据标签选择一类应用做控制；支持对每一种应用的定义和解释，帮助客户快速定位应用的分类。  13、流量控制：支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义（提供产品界面截图）；能够对IPv6流量进行控制；具备在链路聚合环境下使用流控的功能；具备线路繁忙保护功能；具备P2P智能流控功能，能够通过抑制P2P的下行流量，来减缓P2P的上行流量，从而解决流控功能开启时设备负载较大的问题; 支持灵活配置流控单位是IP还是用户名（适用于公共账号：多个IP公用一个账号时，可以对每个IP进行限速，更加灵活准确）；支持基于“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；（提供产品界面截图）。  14、应用审计：支持记录QQ、MSN等IM聊天行为和传文件的内容；支持移动APP（IOS和android）审计（如论坛类、微博类、新闻评论类等）；支持金融类应用内容审计如：阿里旺旺、万德（Wind）、路透等应用的聊天内容。（提供产品界面截图）  15、加密审计和过滤：针对SSL加密的网站、论坛发帖、web邮箱以及客户端邮箱（如闪电邮）的内容进行关键字过滤和审计。（提供产品界面截图）  16、上网安全：支持防火墙功能；支持防DOS攻击，识别并封堵来自于内网或外网的DOS攻击；支持防ARP欺骗，防范三层网络环境中的ARP欺骗问题；支持病毒查杀功能，必须能够针对各种下载文件进行病毒查杀。  17、数据分析：学生上网行为感知支持以应用商店的形式发布各种数据分析应用，包括但不限于网贷行为分析、沉迷网络游戏分析、家庭困难学生资助分析等。（提供分析平台界面截图）。  18、应用支持：支持直接展示已安装和未安装的应用，支持选择安装或卸载应用；支持直接展示应用更新列表，可选择是否更新当前已安装应用。  19、管理功能：内置各类网贷网站和关键字，支持用户自定义网贷网站和关键字；提供三种人群划分：涉及网贷人群、高危人群、关注人群；对每类人群进行用户排行，支持直观显示每个用户访问网贷网站的种类和访问次数；对每个用户访问关键字进行排行，针对每个关键字提供访问URL地址、访问时间、访问快照和访问次数。  20、应用设置：自定义不同的应用成为沉迷网络的影响因素；支持自定义过滤条件：时间、对象、用户组、设备、以及沉迷时长；支持统计整体沉迷人数，以及各应用大类下的沉迷人数；支持对沉迷人员进行排行，支持直接显示该人员沉迷时长、关注内容明细、每日关注内容、以及最近上网时长趋势。  21、检索功能：支持基于时间、用户/组、终端类型、位置、日志类型等条件下的关键字检索定位功能；必须支持对日志中OFFICE等附件正文内容关键字的检索。  22、预置关键字：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。（提供产品界面截图）  23、图形显示：支持在地图上显示用户访问的地理位置，直观展示境外访问次数和在线用户数；支持图形形式，动态显示整体上网态势，包括：总体应用流速趋势、单位流量分布、应用流量分布、热门应用排行等。（提供产品界面截图）  24、支持用户自定义：支持轮播形式显示各部门应用流量分布；提供三种页面布局选择，用户可根据需要灵活配置；提供自定义配置显示模块，对需要显示的模块内容勾选即可；支持自定义配置不良内容，包括不良应用和不良网站。  25、资质证书：  提供上网行为感知系统软件著作权证书，证明产品具备日志数据分析的能力。 | 套 | 1 | 是 |
| 4 | 服务 | 提供原厂三年特征库升级、软件升级和硬件质保服务；三年后，若特征库和软件停止更新和升级，需保证设备仍可使用；三年后，若特征库和软件继续更新升级，每年费用不超过设备购置价格的10%。 | 1 | 项 | 否 |

（三）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。

1、按照国家相关标准、行业标准规范验收。

2、按照招标文件要求、投标文件响应和承诺验收。

（四）采购标的的其他技术、服务等要求

1、中标人负责与采购人现有网络设备对接，并满足采购人对采购设备的安装和对接要求，在对接过程中，不能对校内网络用户产生大的影响，实现平稳过度。

2、中标人在与采购人签订合同时，须提供采购清单第4项“服务”要求的生产厂家承诺书，加盖生产厂家公章。

五、评标方法和评标标准

（一）评标方法：最低评标价法

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：杨应坡    联系电话：13903996928

单位地址：许昌市魏文路与永昌大道交叉口。

许昌电气职业学院（公章）

年    月   日