**中 山 大 学 新 华 学 院**

广州校区防火墙设备采购项目

招

标

文

件

**二〇一八年三月二十九日**

目 录

[第一部分 投标邀请书 2](#_Toc373500451)

[一、招标项目 2](#_Toc373500452)

[二、投标截止时间及方式 2](#_Toc373500453)

[三、开标时间及地点 2](#_Toc373500454)

[四、联系方式 2](#_Toc373500455)

[第二部分 投标须知 3](#_Toc373500456)

[**一、概述** 3](#_Toc373500457)

[**二、招标文件** 4](#_Toc373500458)

[**三、投标文件** 5](#_Toc373500459)

[**四、开标及评标** 7](#_Toc373500460)

[第三部分 招标项目清单及技术参数要求 1](#_Toc373500461)0

[第四部分 合同主要条款 1](#_Toc373500462)5

[一、 产品要求 1](#_Toc373500463)5

[二、 供货及验收 1](#_Toc373500464)6

[三、 售后服务 1](#_Toc373500465)7

[四、 付款方式 1](#_Toc373500466)7

[第五部分 附件 1](#_Toc373500467)8

[**开标一览表**](#_Toc373500468) 18

[**投标函**](#_Toc373500469) 19

[**投标报价明细表** 2](#_Toc373500470)0

[**技术参数与商务条款偏离表**](#_Toc373500471) 21

# 第一部分 投标邀请书

根据中山大学新华学院2018年关于广州校区防火墙设备采购项目计划，我中心拟通过公开招标的方式选定投标单位，现邀请贵公司参加该项目的投标。

一、招标项目

（一）项目名称：广州校区防火墙设备采购项目

（二）项目内容：详见招标项目清单及技术参数要求。

二、投标截止时间及方式

（一）截止时间：**2018年4月16日16:00**时前递交投标文件。

（二）投标方式：快递或直接送达。

（三）投标文件密封递交至中山大学新华学院东莞校区行政楼A214。

三、开标时间及地点

（一）开标时间另行通知。

（二）地点：中山大学新华学院东莞校区行政楼会议室。

四、联系方式

联系人：王老师 邮箱：1248100835@qq.com

电 话：0769-82676032 18122888902

地 址：东莞市麻涌镇沿江西一路7号(523133)

第二部分 投标须知

**一、概述**

（一）投标人资格

1. 在国内工商管理部门注册，具有独立企业法人资格和良好的商业信誉，满足招标文件要求，具备完成该项目的能力；

2. 有健全的、有效的管理制度和质量保证体系，有履行合同所必须的设备及专业技术能力；

3. 有依法缴纳税收和社会保障资金的良好记录，投标人及投标产品在以往采购中无不良服务记录和表现；

4. 投标人须提供可证明其符合投标人资格和具有履行合同能力的合法有效文件；

5. 投标人应具有300万以上注册资金，须有能力在广州东莞提供长期的技术支持及售后服务。

（二）投标费用

投标人无论中标与否，应自行承担参加本招标活动所发生的所有费用。

（三）**投标保证金**

为保证此项目建设的顺利进行，保护我院免遭因投标人不当行为而蒙受损失，我院对该项目的建设收取**壹万元整**的投标保证金，作为投标书的一部分。投标方必需在开标前通过公司基本账户以存款或者转账的方式将投标保证金缴纳至中山大学新华学院基本账户2010027929200042277（工行东莞分行麻涌支行），**转账请附项目编号及名称信息。**

开标后，未中标单位的投标保证金在中标公示后的15个工作日内无息退还；中标单位签订合同后投标保证金自动转为履约保证金，履约保证金在项目验收通过后返还（**项目验收后请主动联系用户老师及招标中心办理保证金退还事宜**），如中标后不按招标文件履约并以不正当理由拒签合同，或者在签订合同时向我方提出附加条件，招标人有权不予返还其递交的投标保证金并有权追究其相关责任。

（四）禁止事项

1. 投标人不得相互串通投标损害国家利益，社会公共利益和其他当事人的合法权益，不得以任何手段排斥其他投标人参与竞争；

2. 投标人不得向采购人、招标小组成员行贿或者采取其他不正当手段谋取中标；

3. 《中华人民共和国政府采购法》及相关法律法规规定的其它禁止事项。

**二、招标文件**

（一）招标文件的组成

1. 招标文件用以阐明所需货物及服务、招标投标程序和要求等，招标文件的组成如下：

第一部分 投标邀请书

第二部分 投标须知

第三部分 招标项目清单及技术参数要求

第四部分 合同主要条款

第五部分 附件

1. 除上述文件外，还包括发出的书面澄清、修改和补充资料，作为招标文件的组成部分，具有同等法律效力。

（二）招标文件的澄清

1. 招标文件的各项组成文件应被认为是相互说明的，如出现矛盾或歧义，招标人有权发出其认为必要的指示、澄清来解决此矛盾或歧义。对于该指示或澄清，投标人均不得表示异议。

2.各投标人对招标文件如有疑点要求澄清，或认为有必要进行技术交流的，应以书面形式传真或发电子邮件给招标人。

（三）招标文件的修改

1. 在投标截止日期前，招标人可对招标文件以补充文件的方式进行修改，招标文件的修改将以书面形式通知所有投标人。

2. 补充文件为招标文件的补充，与其具有同等法律效力，若招标文件和补充文件冲突的，以补充文件为准。

3. 投标人需按照招标文件修改文件的要求参与投标，投标人没有作出实质性响应可能导致其投标被拒绝。

（四）招标文件的澄清、修改、补充等内容均以书面形式明确的内容为准，当招标文件、招标文件的澄清、修改、补充等在同一内容的表述上不一致时，以最后发出的书面文件为准。

**三、投标文件**

（一）投标文件的编制

1. 投标人应认真阅读招标文件中的所有事项包括投标文件的组成、格式、商务条款和技术要求等，在完全理解招标文件的前提下编制投标文件。

2. 投标人必须如实反映情况，对投标文件的真实性、准确性负责，投标人在投标中提供不真实的材料，无论其材料是否重要，都将直接导致投标文件无效，并承担由此产生的法律责任。

3. 如果投标人没有按照招标文件要求提交全部资料或者投标文件没有对招标文件在各方面都作出实质性响应，可能导致其投标被拒绝。

4. 投标文件为一式五份，正本一份，副本四份，标明“正本”和“副本”，封面及内容均需加盖公章。若正副本内容不一致，以正本为准。

5. 投标文件内容应无涂改和行间插字，如因招标人修改招标文件造成的投标文件涂（删）改，应在涂（删）改处加盖公章，投标代理人签名。

（二）投标文件文字和计量单位

1. 投标人提交的投标文件，包括技术文件、资料说明等，以及投标人与招标人就有关投标的所有来往函电均应使用中文。

2. 投标文件中所使用的计量单位除招标文件中有特殊规定外，一律使用国家法定计量单位。

（三）投标文件的递交

投标人应将投标文件密封，封面注明投标项目、投标单位、联系人、联系电话、投标日期，封口加盖公章，在投标截止日期前送达招标人指定地点。

（四）投标报价

1. 投标人须对所有项目内容作完整唯一的报价，每种货物只允许有一个报价，统一按人民币报价。
2. 投标报价应包含所有必要设备、随机零配件、标配工具、消耗品、包装、运输、保险、安装、调试、培训、验收、质保服务、各项税费及项目实施过程中不可预见的所有费用。
3. 投标有效期

从提交投标文件截止日起计算90日内。

（六）投标文件的组成

投标人编写的投标文件应包括下列内容，需加盖公章：

1. 开标一览表（附件一，单独密封）；

2. 投标函（附件二）；

3. 投标报价明细表（附件三）；

4. 技术参数与商务条款偏离表（附件四）；

5. 法定代表人资格证明或授权委托书及身份证复印件；

6. 投标人需提供以下资格、资质文件：

（1）营业执照（副本）复印件；

（2）税务登记证（副本）复印件；

（3）组织机构代码（副本）复印件；

7. 开户银行资信证明、经审计的近一年的财务三大报表及近三年的成功案例；

8. 厂家/生产商授权书/产品合格证书及相关产品质检报告；

9. 详细的技术参数、彩色效果图文资料及重要材质样品；

10. 售后服务承诺书；

11. 投标方认为需要提交的其他文件。

**四、开标及评标**

1. 开评标由中山大学新华学院评标小组主持，可邀请所有投标人代表持本人身份证参加。
2. 投标人须携带招标文件在规定时间到达指定地点等候，有相关技术人员参加开评标的，须携带证明其身份的证件方可参加。
3. 允许投标代表人现场进行产品或产品材质的讲解与演示。
4. 评标是以招标文件和投标文件为依据，按照招标文件中规定的各项条件进行综合评审，采取少数服从多数原则，以评标总得分前两名的投标人作为中标候选供应商进行商务谈判及二次报价以确定中标者。
5. 评标标准
6. 提供最合理的方案及投标报价；
7. 投标人的信誉、业绩及质保体系；
8. 投标人的服务水平及承诺；
9. 投标人的供货期及供货能力；
10. 投标人对招标文件中合同条款的响应。
11. 投标文件出现下列任意情形之一的可认定为无效投标：
12. 不具备招标文件中规定资格要求的；
13. 未按招标文件规定要求密封、签署、盖章的；
14. 投标人以他人的名义投标、串通投标、以行贿手段谋取中标或以其他弄虚作假方式投标的；
15. 投标文件在投递过程中密封袋破损程度足以影响开评标公平、公正性的；
16. 投标文件粗制滥造，内容自相矛盾的；
17. 不符合法律、法规和招标文件中规定的其他实质性要求的。
18. 投标文件的澄清
19. 对投标文件中含义不明确的，评标小组可以要求投标人代表作出必要的澄清、说明。
20. 投标人的澄清、说明应当采用书面形式，由其授权代表签字。
21. 评标小组可以要求投标人代表进行二次报价，须密封提交。
22. 注意事项
23. 在开标、评标期间，投标人不得向评标小组询问评标情况，不得进行旨在影响评标结果的活动。
24. 评标小组无义务对评标结果作任何的解释，不退回投标文件。

第三部分 招标项目清单及技术参数要求

（如需了解更详细的情况及参数，可联系用户老师：谭老师，13802411438）

**一、 采购清单**（参考品牌：华为、天融信、山石网科）

1.主要参数:

|  |  |  |
| --- | --- | --- |
| **产品** | **配置说明** | **性能** |
| 防火墙 | <=2U；  ≥4个光口；  4个电口；  双冗余电源； | 防火墙吞吐量：≥10Gbps  最大并发连接数：≥300万  每秒新建连接：≥12万  防病毒吞吐量：≥3Gbps  IPS吞吐量：≥2.5Gbps  IPSEC加解密吞吐量：≥400Mbps |

2.具体技术要求：

|  |  |  |
| --- | --- | --- |
|  | 指标项 | 详细指标要求 |
| **基本要求** | 系统结构 | 产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统（提供相应资质证明）； |
| 系统软件 | 系统具有良好的扩展性，具有病毒防御、入侵防御、应用识别、网站分类库过滤、IPSEC VPN等功能；提供**5年**病毒防御、入侵防御、应用识别、网站分类库过滤库升级服务。 |
| **系统性能** | 防火墙吞吐 | 防火墙吞吐率：10Gbps |
| 应用层吞吐 | 防病毒吞吐率：3Gbps  IPS吞吐率：2.5Gbps  IPSEC加解密吞吐率（AES128+SHA1）：400Mbps |
| 最大并发连接数 | 并发连接数：≥300万 |
| 每秒新建连接数 | 每秒新建连接（FW&HTTP）：12万  每秒新建连接（FW+APP&HTTP）：8万 |
| **硬件配置** | 机箱 | 设备不得超过2U标准高度； |
| 电源 | 设备配置模块化双冗余电源； |
| 接口配置 | 要求至少配置4个1000BASE-T，4个SFP光口 |
| **网络**  **接入** | 工作模式 | 支持路由、交换工作模式； |
| 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，保证关键业务流量通过优质链路转发； |
| 接入功能 | 支持GRE与IPSEC VPN接入 |
| 链路聚合 | 为提高链路可靠性，需支持手工链路聚合及LACP链路聚合，提供不少于6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 |
| IP/MAC绑定 | 支持手动添加绑定，基于IP、接口的动态探测绑定，支持跨三层IP/MAC绑定，IP/MAC绑定表可导入导出； |
| 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，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡（提供截图） |
| **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（提供截图）； |
| 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（提供截图）； |
| **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；（提供截图） |
| 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；支持手动创建用户、批量导入导出用户，同时支持设备扫描方式创建用户；（提供截图） |
| 支持设置密码有效性，如首次登陆修改密码、密码定期修改、密码有效时间等设置，用户忘记密码时，支持密码找回；（提供截图） |
| 支持本地CA和第三方CA，支持作为CA认证中心为其他人签发证书，也可采用第三方CA为其他人签发证书（提供截图）；支持标准CRL列表，支持CRL手工更新，同时支持CRL自动下载，通过HTTP或者LDAP方式定时自动下载更新CRL文件（提供截图） |
| **应用管控** | 应用识别 | 内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如P2P（web应用、移动应用、云应用、加密应用等；内置独立应用识别特征库，总数2000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； |
| 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、应用、服务、时间、安全引擎（入侵防御、URL过滤、病毒过滤、数据防泄漏DLP、内容过滤、文件过滤、审计、APT）的识别与控制；（提供截图） |
| 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；（提供截图） |
| 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；（提供截图） |
| 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，实现对特定报文进行快速过滤；（提供截图） |
| **安全防护** | 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（提供截图），同时支持自定义特征库,且厂商具备强大的漏洞和攻防研究能力。 |
| DDOS防御 | 内置流量检测清洗引擎，支持基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等众多协议类型的防护策略；提供丰富的策略模板，且支持策略模板自定义；（提供截图） |
| 支持基于IP协议的检测清洗，包括但不限于：IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke等异常报文攻击； |
| 支持基于TCP协议的检测清洗，包括但不限于：TCP Flood、SYN Flood、SynACK Flood、ACK Flood、FIN Flood、RST Flood、新建SESSION Flood、SESSION Flood等；支持SYN源认证技术，认证模式可设置为基本模式或者高级模式，以防止虚假源攻击； |
| 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，认证方式可选基本源认证或者cname认证； |
| 支持基于HTTP协议的检测清洗，包括但不限于：HTTP Flood、HTTP新建连接Flood、HTTP并发连接Flood、HTTP URI CC等攻击检测，同时支持对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； |
| 支持基于NTP协议的检测清洗，包括NTP REQUEST FLOOD、NTP REPLY FLOOD等攻击检测，支持基于NTP请求限速、NTP响应限速、源认证、会话认证的防御策略； |
| 支持根据DOS/DDOS攻击行为自动添加动态黑/白名单功能，可自定义动态黑/白名单超时时间； |
| 病毒过滤 | 内置病毒检测引擎，支持HTTP/SMTP/POP3/FTP/IM等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载；（提供截图） |
| 内置专业反病毒厂商或研究机构的病毒特征库，符合等级保护相关标准对网关防病毒特征库和主机防病毒特征库异构的要求。 |
| 支持病毒白名单，用户可以根据实际业务需求将特定威胁进行排除（提供截图）； |
| URL过滤 | 内置互联网URL分类库，支持超过80大类、2000万的URL地址分类库，用户可根据上述网站类别，对自身网络的WEB应用实施全面化管控，杜绝非法、违规网站的访问行为，从而净化网络应用环境； |
| 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50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，可对微博、贴吧上传的内容及附件进行过滤，可对FTP上传/下载的文件名进行过滤，同时支持过滤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； |
| 配置维护 | 支持多个配置文件并存，配置文件数量不少于10个； |
| 系统诊断 | 支持分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、 TRACEROUTE、 TCP、 HTTP 和 DNS（提供截图）；  支持在WEB界面进入CLI模式，执行系统配置、网络诊断、过滤抓包等命令，提高管理员运维效率（提供截图）； |
| 管理员 | 支持系统管理员能够通过本地认证及外部认证方式进行登录管理，外部认证失败时可转本地认证  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（提供截图） |
| **数据中心** | 报表 | 内置15类预定义报表模板，支持根据通信流量、上网行为、威胁统计等来源数据库自定义报表模板；支持一次性报表及周期性报表，可自定义统计时间； |
| 支持报表按照PDF、WORD及EXCEL格式导出； |
| 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；（提供截图） |
| 支持网站访问审计：审计指定类别的 URL 地址、审计命中指定关键字的网页标题和网页内容； |
| 支持telnet审计：对telnet协议命令进行审计； |
| 日志 | 支持日志本地存储，可对不同类型日志设置存储空间；（提供截图）同时支持外发至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；（提供截图） |
| 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，具体包含用户、连接、流量、NAT、审计、HA、APT、未知威胁等20个日志类别； |
| **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；（提供截图） |
| 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，包括应用总流量排名和各个应用的协议名称、总流量、上行流量、下行流量、新建连接数、当前会话数以及流速；（提供截图） |
| 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，包括用户总流量排名和各个用户的用户名、认证类型、上行流量、下行流量、新建会话数、当前会话数以及流速；（提供截图） |
| 支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；（提供截图） |
| 支持指定监控时间周期，包括：实时、最近1小时、最近1天、最近1周、最近1月等；（提供截图） |
| 威胁统计 | 支持根据按照病毒防御、入侵防御、ADS攻击进行威胁统计，可按照威胁类型/攻击者/受害者三种方式进行威胁排名。（提供截图） |
| 资质要求 | 产品资质 | 公安部销售许可证 |
| 国家信息安全测评信息技术产品安全测评证书（至少达到EAL3） |
| **厂商资质** | 涉及国家秘密的信息系统集成甲级资质 |
| 信息安全管理体系ISO27001认证 |
| TL9000质量管理体系证书 |
| 中国通信企业协会通信网络安全服务能力评定—安全设计与集成二级资质 |

3.详细功能需求：

**3.1网络接入**

（1）支持路由、透明、直连部署模式；

（2）支持静态路由、动态路由、策略路由及ISP路由；

（3）链路聚合、虚拟线及子接口等多种网络接入方式；

（4）支持IPv6（接口配置、路由、ICMPv6、ND、DHCPv6、SNMP等）；

**3.2安全防护**

（1）基于传统五元组、用户、应用、内容、时间等多元组一体化访问控制；

（2）源地址转换、目的地址转换、双向地址转换及端口转换多种NAT策略；

（3）支持FTP、TFTP、PPTP、SQLNET、H.323、SIP、RTSP等动态端口协议；

**3.3身份认证**

（1）采用内网终端统一管理的集中式认证系统；

（2）支持本地认证与第三方外部认证（如RADIUS、TACACS、LDAP等）；

（3）集成PKI服务，内置CA并支持第三方CA；

**3.4系统服务**

（1）提供DHCP服务器/客户端/中继、NTP等网络服务；

（2）支持跨越三层设备进行IP/MAC绑定；

（3）支持网关虚拟化技术；

**3.5系统管理**

（1）基于SSH、HTTPS安全协议的配置交互界面；

（2）管理员分级、权限自定义、密码强度分级、管理端口自定义等扩展安全配置；

（3）支持管理员外部认证；

（4）系统资源、硬件状态、网络流量、安全事件的可视化监控；

（5）邮件、声音、SNMP、控制台等多种组合报警方式；

（6）采用Syslog日志格式，支持分级和按类型输出以及日志加密传输；

（7）图形界面与命令行方式进行系统升级；

（8）提供报文调试功能及系统健康记录，支持端口镜像；

**3.6负载均衡**

（1）**多运营商接入（内置ISP路由），支持多种路由均衡算法及路由备份功能**；

（2）采用链路有效性探测实现智能链路切换；

（3）支持入站智能DNS；

（4）支持多线路接入下报文的源路径返回；

（5）支持服务器负载均衡，提供多种负载均衡算法并支持服务器的应用有效性探测；

**3.7连接限制**

（1）基于源地址、目的地址、应用的连接限制；

（2）支持每IP连接总数限制、所有IP连接总数限制、每IP新建连接数限制；

（3）支持连接限制策略命中统计查看，显示最近被拒的10条地址对象节点信息；

**3.8攻击防护**

（1）DDoS攻击防护，包括非法报文攻击及统计型报文攻击；

（2）基于IP、ICMP、TCP、UDP、DNS、HTTP、NTP等协议的DDOS攻击防护；

（3）支持根据威胁事件、攻击来源、受威胁主机查询攻击；

**3.9病毒防御**

（1）支持HTTP、FTP、SMTP、POP3、IM等协议进行病毒检测；

（2）支持木马病毒、蠕虫病毒、宏病毒、后门病毒查杀；

（3）支持7z，rar，gzip，zip等多级压缩文件查杀；

（4）支持根据病毒ID的防病毒例外功能，支持病毒过滤阻断生成基于五元组的动态黑名单功能；

（5）提供多种国内外知名防病毒厂商病毒库可供选择，病毒库可定期更新或实时更新；

**3.10异常行为分析**

（1）内置统计智能学习算法，对新建连接数、并发连接数、流量等数据智能学习；

（2）监控对象包括：源IP、目的IP，地址对象支持主机地址、子网地址、范围地址；

（3）定时器定时比较实时数据，触发报警；

**3.11上网行为管理**

（1）支持包括P2P、IM、炒股、网游、流媒体等类别的应用识别与过滤；

（2）P2P应用行为的识别控制；

**3.12网站分类过滤**

（1）支持网站分类过滤功能；

（2）HTTP、FTP、SMTP、POP3、Telnet等协议的深度内容过滤；

（3）基于HTTP、FTP、SMTP、POP3等标准协议等应用的文件类型过滤；

**3.13远程接入**

（1）支持IPSEC VPN 、SSL VPN多种隧道接入技术；

（2）支持DES/3DES/AES等标准加密算法及MD5/SHA1等标准HASH算法；

**3.1****4报表功能**

（1）支持根据通信流量、威胁统计、DDOS等来源数据库自定义报表模板；

（2）支持报表的生成，能按照PDF、WORD及EXCEL格式导出。

**注：**

**1. 质保要求至少五年，含硬件和软件的升级（含病毒库、应用识别特征库等升级）。**

**2.中标单位需提供中标型号设备给用户方测试一个月，测试通过后再签订正式合同。**

第四部分 合同主要条款

1. 产品要求

（一）产品必须是全新，且符合国家标准、行业标准及招标文件要求，等于或优于招标文件技术要求，严格按中标价按时按量按质供货。卖方应提供软件的安装、使用和维护的技术文件，如质量合格检定证明文件、保修服务卡、使用说明（原版正本）和维护手册，使用操作及维护等重要资料应附有中文说明（教学软件必须配有实训指导书）。

（二）卖方必须为用户（免费）培训软件使用操作人员，请投标方说明针对买方专业技术人员的培训计划。

（三）卖方保证买方在使用该产品或产品的任何一部分时，免受第三方提出的侵犯其专利权、商标权、工业设计权或其他知识产权的起诉，因产品存在知识产权瑕疵或纠纷的，卖方须承担可能发生的一切法律责任和费用。

1. 因产品存在知识产权瑕疵或纠纷的，卖方须承担可能发生的一切法律责任和费用。产品或产品的任何部分因最终裁决构成侵权，卖方应自担费用并主动做出相应的安排：或为买方获取继续使用受指控侵权的产品或产品的某一部分的权利，或用不会造成侵权的同等技术水平的产品免费更换。
2. 中标人须到现场勘察、量取尺寸，并按所附清单提供设备及材料，负责所有线管及强、弱电线的铺设，并完成所有网络信息点和强电插座的安装、调试，要求做到布局合理，布线规范，便于使用及维护方便。
3. 在项目实施过程中，乙方须对本项目实施管理、协调和进度控制，应及时向甲方报告项目进度，在保证质量和施工进度的前提下安全文明施工且按时完工，现场达到工完料净场地清的要求。
4. 项目实施期间出现工伤事故，由乙方自行负责。
5. 乙方在搬迁、移动甲方设备时，不得对甲方设备、财产等造成任何破坏及损失。
6. 供货及验收
7. **中标单位需提供中标型号设备给用户方测试一个月，测试通过后再签订正式合同。**
8. 在安装、调试过程中对产品或买方原有设备造成任何损坏的由卖方负责。由于产品缺陷，卖方技术人员的指导错误或提供的技术资料、说明书的错误造成产品损坏的，卖方应及时采取必要的补救措施，由此造成的损失由卖方承担。
9. 卖方派专业技术人员对买方技术人员进行培训（培训学时>48小时），直至其全面掌握所有设备系统的应用及维护并认可为止。
10. 软件试运行两个月后组织验收，验收过程中如发现产品技术指标或功能上不符合招标要求或产品介绍资料时，卖方应提出解决方案，协商不行的买方有权要求退货，造成的一切损失由卖方承担。
11. 乙方按所附清单提供设备及材料，负责所有线管及强、弱电线的铺设，并完成所有信息点的安装、调试，要求做到布局合理，布线规范，便于使用及维护方便，项目完工后提供所有网络信息点的测试数据报告。
12. 在项目实施过程中，乙方须对本项目实施管理、协调和进度控制，应及时向甲方报告项目进度，在保证质量和施工进度的前提下安全文明施工且按时完工，现场达到工完料净场地清的要求。
13. 售后服务
14. 保修期自买、卖双方签订验收合格报告之日起算，整体免费保修期**伍**年，包括技术支持、版本升级及维护服务（包括上门服务），卖方承担因产品问题所发生的一切费用。质保期内，买方硬件、网络设备故障导致要重新安装软件的，卖方应无条件免费安装、调试。
15. 在每学期开学前提供一次维护服务，对产品进行一次检查及维护，因服务产生的费用由卖方承担。
16. 软件故障响应时间及方式：4小时内远程维护，24小时内到达现场，48小时内解决问题。
17. 卖方未及时响应并维护的，买方有权自行组织维护，因此而产生的一切费用由卖方承担。
18. 质保期满后，根据甲方的需要，继续提供免费版本升级服务。
19. 付款方式
20. 合同签定之日起7个工作日内，买方预付合同总价20%作为定金；验收合格后，15个工作日内支付合同总价75%；合同总价5%作为质保金,1年内无质量及服务问题的，7个工作日内支付余款。
21. 支付以上款项前，卖方必须按付款金额向买方提供等额正规发票，否则甲方有权拒绝付款。

第五部分 附件

附件一：

**开标一览表**

项目名称：

投标人名称：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 产品名称 | 生产商/型号 | 数量 | 投标报价 | 供货期 | 备注 |
|  |  |  |  |  |  |

注：1.此表请单独密封，信封封面请注明招标项目名称、投标人名称及"开标一览表"字样。

2.投标报价应包含必要设备、配备件、标配工具、运输、安装、调试、技术指导、验收、维保、税金及项目实施过程中不可预见的一切费用。

3.“开标一览表”的内容应与“投标报价明细表”以及投标文件的其他相关内容一致。如果“开标一览表”的内容与“投标报价明细表”以及投标文件的其他相关内容不一致，则以“开标一览表”的内容为准。

法人代表或委托代理人签名：

投标人盖章：

日 期：

附件二：

**投标函**

中山大学新华学院 ：

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(投标人全称)授权\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (委托代理人姓名)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(职务、职称)为全权代表，参加贵方组织的\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (招标项目名称)招标的有关活动，并对此项目进行投标。为此：我方同意遵守本投标书中的承诺且具有约束力。

1. 提供投标须知规定的全部投标文件：

一式五份，其中正本一份，副本四份；具体要求按照招标文件规定。

1. 总投标价为（大写）： 元人民币；
2. 保证忠实地执行双方所签订的合同，并承担合同规定的责任和义务。
3. 保证遵守招标文件中的其他有关条款。
4. 我方愿意向贵方提供真实完整的任何与该项投标有关的数据、情况和技术资料，若贵方需要，我方愿意提供我方作出的一切承诺的证明材料。
5. 我方已详细审核全部招标文件，包括招标文件的澄清或修改文件、参考资料及

有关附件，确认无误。

1. 我方的投标文件在开标后90天内有效。

与本投标有关的一切往来通讯请寄：

地址：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 邮编：\_\_\_\_\_\_\_\_\_\_\_\_

电话：\_\_\_\_\_\_\_\_\_\_\_\_　 传真：\_\_\_\_\_\_\_\_\_\_\_\_

法人代表或委托代理人签名：

投标人盖章：

日 期：

附件三：

**投标报价明细表**

项目名称：

投标人名称：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 产品名称 | 规格型号 | 品牌 | 技术参数 | 单位 | 数量 | 单价 | 金额 | 备注 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

注：1、投标人必须按“分项报价明细表”的格式详细报出投标总价的各个组成部分的

报价，否则作无效投标处理。

2、“投标报价明细表”各分项报价合计应当与“开标一览表”报价合计相等。

法人代表或委托代理人签名：

投标人盖章：

日 期：

附件四：

**技术参数与商务条款偏离表**

项目名称：

投标人名称：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 招标文件要求 | 响应情况 | 偏离 | 说明 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

法人代表或委托代理人签名：

投标人盖章：

日 期：