合同编号：（郑大-竞谈-2021-0147）

**郑州大学政府采购货物合同**

**甲方：郑州大学**

**乙方：河南邦德仪器设备有限公司**

在甲方为获得（**郑州大学中原网络安全研究院工业互联网安全实验室项目**）货物和伴随服务实施公开招标，乙方参加了公开招标。通过公开招标，甲方接受了乙方以总金额（人民币：肆拾柒万玖仟捌佰圆整，小写：479800元）（以下简称“合同价”）的投标。双方以上述事实为基础，签订本合同。

**一、供货范围及分项价格表（详见附件1、附件2）**

1、本合同所指设备详见附件1、附件2 ，此附件是本合同不可分割的部分。

2、总价中包括设备金额、包装、运输、保险费、装卸费、安装及相关材料费、调试费、软件费、检验费及培训所需费用及税金，甲方不再另行支付任何费用。

**二、质量及技术规格要求**

乙方须按合同要求提供全新设备（包括零部件、附件、备品备件），设备的质量标准、规格型号、具体配置、数量须符合招标标书要求，其产品为原厂生产，且应达到乙方投标文件及澄清文件中明确的技术标准。

乙方应在本合同生效后 10 个日历日内向甲方提供安装计划及质量控制规范；并于 12 月 18 日前进驻安装现场；所有设备运送到甲方指定地点后，双方在 7 日内共同验收并签署验收意见。甲方无正当理由，不得拒绝接收；在安装调试过程中，甲方有权采取适当的方式对乙方产品的质量标准、规格型号、具体配置、数量以及安装质量和进度等进行检查。甲方如果发现乙方所供设备不符合合同约定，甲方有权单方解除合同，由此产生的一切费用乙方承担。

**三、包装与运输**

设备交付使用前发生的所有与设备相关的运输、安装及安全保障事项等均由乙方负责；设备包装应符合抗震、防潮、防冻、防锈以及长途运输等要求，由于包装不当或防护措施不力而导致的商品损坏、损失、腐蚀等损失均由乙方承担；设备交付使用前所发生的所有与设备相关的经济纠纷及法律责任均与甲方无关。

**四、质保期与售后服务（详见附件3）**

1、所有设备免费质保期为 1 年，自验收合格并交付给甲方之日起计算，且乙方应终身维护、维修。

2、在质保期内，因产品质量造成的问题，乙方应免费提供配件并现场维修，且所提供的任何零配件必须是其原设备厂家生产的或经其认可的。产品存在质量问题，甲方有权要求乙方换货。

3、乙方须提供一年 2 次全免费（配件+人力）对产品设备的维护保养。

4、乙方承诺凡设备出现故障，自接到甲方报修电话1小时响应，3小时内到达现场，24小时内解决故障问题。保修期外只收取甲方零配件成本费，其他免费。

5、乙方有责任对甲方相关人员实施免费的现场培训或集中培训措施，保证甲方相关人员能够独立操作、熟练使用、维护和管理有关设备。

6、其它应规定事项。

**五、技术服务**

1、乙方向甲方免费提供标准安装调试及 10 人次国内操作培训。

2、乙方向甲方提供设备详细技术、维修及使用资料。

3、软件免费升级和使用。

**六、专利权**

乙方应保证甲方在使用其所提供的产品时免受第三方提出侵犯其专利权、商标权或保护期的起诉。

1. **免税**

1、属于进口产品，用于教学和科研使用的，中标价为免税价格。

2、免税产品应由甲乙双方依据海关的要求签订委托进口代理协议，确认甲乙双方的责任与义务。委托进口代理协议作为本合同的不可分割部分。

3、免税产品通关时乙方必须进行商检，未商检的，造成的损失由乙方承担。

**八、交货时间、地点与方式**

1、乙方于 2021 年 12 月 23 日之前将货物按甲方要求在甲方指定地点交货、安装、调试完毕，并具备使用条件，未经甲方允许每推迟一天，按合同总额的千分之五扣除违约金。

2、乙方负责所供货物的包装、运输、安装和调试，并承担所发生的费用；甲方为乙方现场安装提供水、电等便利条件。

3、安装过程中若发生安全事故由乙方承担。

4、乙方安装人员应服从甲方的管理，遵守国家法律法规和学校相关制度，否则一切后果均由乙方承担。

5、货物交付使用前，乙方负责对提供货物进行看管，并承担货物的丢失、损毁等风险。

**九、验收方式**

1、甲方按合同所列质量标准、规格型号、技术参数以及数量等在现场验收，并填写验收单（详见附件4）。验收时，甲方有权提出采用技术和破坏相结合的方法进行验收。

乙方应向甲方移交所供设备完整的使用说明书、合格证及相关资料。乙方在所有设备（工程）安装调试、软件安装完毕后，开展现场培训，使用户能够独立熟练操作使用仪器或设备，而后由供需双方共同初步验收；甲乙双方如产生异议，由第三方重新进行验收。如果乙方提供的货物与合同不符，甲方有权拒绝验收，由此所产生的一切费用由乙方承担。

**十、付款方式**

1、本合同总价款（大写）为肆拾柒万玖仟捌佰圆整（小写￥479800元）。

2、付款方式：货物验收合格后，经审计后，甲方向乙方支付全部货款的95％即人民币 肆拾伍万伍仟捌佰壹拾圆整（小写：￥455810元），质保期满后，甲方向乙方支付剩余的全部货款即人民币 贰万叁仟玖佰玖拾 元整（小写：￥23990元）。

**十一、履约担保**

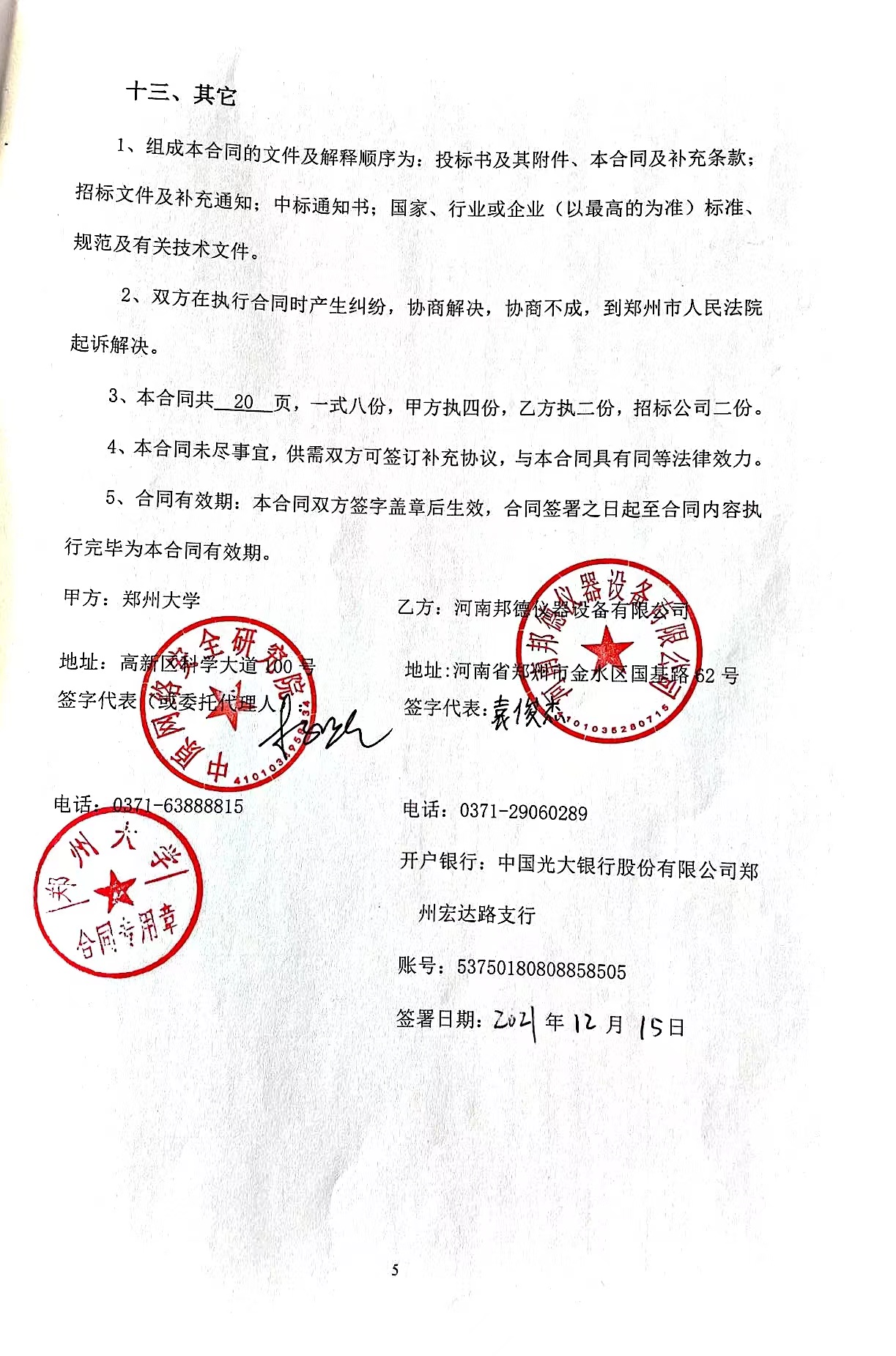
乙方向甲方以转帐的方式提供合同总额5%的履约保证金。履约担保金在签订合同前交学校财务处，货物验收合格，正式交付使用后予以退还。

**十二、违约责任**

乙方所交的货物产地、品牌、型号、规格、质量以及技术标准、数量等不符合

合同要求，甲方有权拒收，由此产生的一切费用由乙方负责；因货物更换而造成逾期交货，则按逾期交货处理，乙方应向甲方每天支付合同标总额日千分之五的违约金。甲方无正当理由拒收设备，应向供方偿付拒收设备款额百分之五的违约金。

甲方逾期付款，应向乙方支付本合同标的总额的日万分之四的违约金。



**附1：**

**供货范围及分项价格表 单位：元**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **品牌型号** | **制造厂（商）** | **原产地（国）** | **数量** | **单价** | **合价** | **备注** |
| 1 | 工控安全防护系统平台 | 天融信NGFW4000-UF/TG-A2614 | 北京天融信网络安全技术有限公司 | 中国 | 1套 | 35700 | 35700 | 免税 |
| 2 | 终端安全防护系统 | 天融信TopEDR/EDR-E-WINSER3/LINUX3-LIC1 | 北京天融信网络安全技术有限公司 | 中国 | 1套 | 41100 | 41100 | 免税 |
| 3 | 安全审计系统平台 | 天融信TopAudit/TA-L-SE-50 | 北京天融信网络安全技术有限公司 | 中国 | 1套 | 36500 | 36500 | 免税 |
| 4 | WEB安全应用平台 | 天融信TopWAF/TWF-A3106 | 北京天融信网络安全技术有限公司 | 中国 | 1套 | 34500 | 34500 | 免税 |
| 5 | 24口接入交换机 | 华三S5130S-28S-E1 | 新华三技术有限公司 | 中国 | 2台 | 39500 | 79000 | 免税 |
| 6 | 网络微分域安全平台 | 山石网科CloudHive-vSSM | 北京山石网科信息技术有限公司 | 中国 | 1套 | 253000 | 253000 | 免税 |
| 合计： 小写：￥479800元 大写：人民币肆拾柒万玖仟捌佰元整 | | | | | | | | |

**附2：**

**设备配置清单表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序 号 | 设备名称 | 具体技术规格参数、功能描述及配置清单描述 | 单 位 | 数 量 |
| 1 | 工控安全防护系统平台 | 1、采用系统结构：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，采用多核多平台并行处理机制。 | 套 | 1 |
| 2、采用性能指标：基于1U机箱设备,具有6个千兆电口，具有8个SFP插槽,防火墙吞吐4G，并发连接150万，每秒新建连接2万，含IPSEC VPN模块，IPSEC VPN吞吐80M，SSL VPN吞吐220M |
| 3、采用连接控制及模式：支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，可控制所有或单IP会话总数及单IP新建连接数。可支持路由、交换、虚拟线、Listening、混合工作模式。 |
| 4、采用用户管控及IP管控：支持防暴力破解、密码复杂度、密码有效性设置，如认证失败次数及锁定时间、密码格式、密码长度、密码找回、首次登陆修改密码、密码定期修改、密码有效时间等设置。 |
| 5、采用IPv4/v6双栈IP/MAC静态和动态探测绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出。 |
| 6、采用链路聚合：手动和LACP链路聚合，可根据源/目的mac、源/目的IP、源/目的端口、五元组、端口轮询等条件10种链路负载算法。 |
| 7、采用路由交换：支持根据入接口、源/目的IP地址/地址对象、源/目的端口、协议、用户、应用、选路算法、探测、度量值、权重等多种条件设置策略路由。 |
| 8、采用DNS Doctoring：支持DNS Doctoring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。 |
| 9、采用资源虚拟化：支持在一台物理设备上划分出128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。 |
| 2 | 终端安全防护系统 | 1、采用配置70个winserver和30个LINUX服务器授权，3年升级许可。系统支持中/英文界面，系统部署采用C/S架构，管理采用B/S架构，管理员只需通过浏览器登录控制中心，即可对系统进行管理 | 套 | 1 |
| 2、采用国产化支持：支持Linux、windows操作系统以及中标麒麟、银河麒麟、中科方德、深度、UOS等国产操作系统 |
| 3、采用虚拟化支持：支持虚拟机、主流虚拟化终端环境（VMware、华为、华三、阿里、腾讯等） |
| 4、采用客户端资源占用：客户端安装后至多占用50M硬盘资源，日常内存占用不到20M，有效节省PC/Server资源。 |
| 5、采用虚拟沙盒：支持基于虚拟沙盒的高效的本地反病毒引擎， 实现极高的本地查杀能力。 |
| 6、采用Webshell检测：支持对webshell后门进行扫描检测 , webshell后门库数量大于100000。 |
| 7、采用勒索病毒诱捕：设置诱饵文件并实时监控，当勒索病毒对该文件进行加密操作时进行拦截。 |
| 8、采用系统加固：对系统关键位置进行防护，阻止无文本攻击、流氓、广告程序对系统的恶意篡改等行为。从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。 |
| 9、采用文档检测：支持文档检测功能，针对终端存储的word、pdf、ppt、Excel、rtf、txt等文档的名称、内容进行包含关键字检查，对含有指定关键字的文档进行禁止发送、禁止拷贝等管控，消息提醒的同时将文档违规信息上报管理平台。 |
| 10、采用USB存储标签管理：支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读\_运行）和启用读写、启用（读写\_运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外USB设备。 |
| 11、采用设备联动：能够与同品牌的防火墙、态势感知和上网行为管理实现协同联动 |
| 3 | 安全审计系统平台 | 1、本采用性能：标准版，含日志收集、存储、查询、统计分析、告警响应等功能，日志采集处理均值20000EPS，峰值35000EPS，50个日志源授权。 | 套 | 1 |
| 2、采用系统部署：支持单级部署，支持代理分布式部署采集日志。 |
| 3、采用数据采集：支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等26类300种日志对象的日志数据采集；支持日志归一化处理。 |
| 4、采用日志归一化处理：支持日志归一化处理，将不同设备所产生的不同格式的难以理解的日志数据进行统一格式化处理，提炼出有用信息清晰、明确的展示给管理者。 |
| 5、本次所投标产品采用数据采集方式：支持主动、被动相结合的数据采集方式。 |
| 6、采用独立展示：支持独立展示每个被采集源最近24小时的日志数量趋势，便于掌握设备的安全事件情况，支持独立展示每个设备日志的最新采集时间，便于了解设备日志的采集状态。 |
| 7、采用日志保存：支持根据设备重要程度设置独立设置每个被采集源的日志、报表数据存储时间为1个月、3个月、6个月和永久保存等参数。 |
| 8、采用地图展示：支持首页以全国地图、全球地图展示最近24小时日志访问源和访问目的的分布，能根据颜色区分访问来源和访问目的数据量大小，能够通过首页地图快速下钻查询指定区域的日志详细信息。 |
| 9、采用日志查询：支持在日志查询结果上针对源IP、目的IP、操作、源端口、目的端口等字段一键快速统计，以饼图方式展示，对于源IP和目的IP（公网地址）还支持以中国地图、世界地图方式展示，在统计图上能够进行点击下钻查询对应条件的日志结果。 |
| 10、采用拓扑图显示：基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据。 |
| 4 | WEB安全应用平台 | 1、采用性能：基于1U机箱设备,具有6个千兆电口,应用层吞吐200Mbps、网络层吞吐2.5G、并发连接50W,含1年应用特征库升级许可 | 套 | 1 |
| 2、采用默认含SQL注入、XSS、CSRF等WEB攻击防护功能、URL访问控制功能、防盗链功能、WEB漏洞扫描功能、DDoS攻击防护功能、网页防篡改功能、服务器负载均衡功能、报表分析及告警功能 |
| 3、**系统架构：**采用专用硬件架构与安全操作系统，基于操作系统内核的完全检测技术；产品为专业性 Web 应用安全防护系统硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能模块。 |
| 4、**部署方式：**无IP纯透明模式串联部署、负载均衡模式部署、反向代理模式部署、旁路监测模式部署。 |
| 5、**网络适应性：**支持虚拟线接入，无论任何网络环境可强制数据从一个接口转发到另一个接口。 |
| **Web攻击防护** |
| 1. 支持2600+的应用层安全防护规则。 |
| 应能识别和阻断SQL注入攻击,Cookie 注入攻击，命令注入攻击。 |
| 1. 产品能识别和阻断跨站脚本(XSS)攻击。 |
| 1. 采用能识别和阻断跨站请求伪造(CSRF)攻击，支持HTTP token防护和referer匹配防护等多种防护方式。 |
| 10、**恶意扫描防护：**通过人机识别方式，进行恶意扫描智能检测；支持扫描防护阈值设置和扫描IP的阻断周期设置。 |
| 11、**爬虫攻击防护：**包括但不限于内置爬虫对象库，自定义爬虫对象，导入或者下载后端服务器robots.txt 等方式提供爬虫攻击防护。 |
| 12、**访问控制：**支持网络层访问控制，支持基于源IP 、目的IP 及源目的区域、服务类型、地理位置区域等条件的访问控制。 |
| **网页防篡改** |
| 13、支持网关型网页防篡改，无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容。 |
| 14、支持缓存型网页篡改防护；WAF通过将缓存的网站页面返回给客户端，从而保证客户端无法看到被非法篡改的页面，来做到网页篡改防护。 |
| 5 | 24口接入交换机 | 1、支持交换容量430Gbps，包转发率140Mpps（如官网中同项指标有多个数值，以最小值为准） | 台 | 2 |
| 2、支持10/100/1000Base-T电接口24个； |
| 3、本支持本地堆叠和远程堆叠，支持跨设备链路聚合，单一IP管理，分布式弹性路由；要求支持完善的堆叠裂检测机制，堆叠分裂后能自动完成MAC和IP地址的重配置，无需手动干预； |
| 4、支持最大堆叠台数9台 |
| 5、支持基于端口的VLAN，支持基于协议的VLAN；支持基于MAC的VLAN；最大VLAN数(不是VLAN ID) 4094； |
| 6、产品支持8个端口聚合；支持128个聚合组；支持LACP；支持本地端口镜像和远程端口镜像RSPAN、支持流镜像； |
| 7、支持IGMP Snooping /MLD Proxy，支持组播VLAN；要求支持IPv4 静态路由、RIPv1/v2、OSPF，支持IPv6 静态路由、RIPng，支持IPv4和IPv6环境下的策略路由； |
| 8、支持RRPP（快速环网保护协议），环网故障恢复时间不超过50ms；支持Smartlink、支持RSTP功能、支持MSTP功能、支持PVST功能； |
| 9、支持基于第二层、第三层和第四层的ACL；整机提供ACl条目数1K条；支持基于端口和VLAN的 ACL；支持IPv6 ACL；支持出方向ACL，以便于灵活实现数据包过滤；支持802.1x认证，支持集中式MAC地址认证。 |
| 10本次所投标产品支持OPENFLOW 1.3标准、支持普通模式和Openflow 模式切换。 |
| 6 | 网络微分域安全平台 | 1. 1、采用虚拟机形态本地化、分布式网络安全服务，使得业务虚拟机流量不用外出宿主机，即可高效的实现网络安全管控。 | 套 | 1 |
| 1. 2、的安全服务能力，无需要求在业务虚机中额外安装第三方插件或Agent软件。为保障云基础平台的可靠性，要求不能在云基础平台中安装任何第三方插件和Agent软件。部署方式为二层透明部署。 |
| 1. 3、采用吞吐量100Gbps，可支持扩展至1Tbps；ips防护吞吐量30Gbps，可支持扩展至200Gbps；AV防护吞吐量30Gbps，可支持扩展至200Gbps；最大并发连接数3400万，可支持扩展至3.4亿，本次配置每秒新建HTTP连接数60万，可支持扩展600万，支持物理CPU数量40个；本次配置要求可防护虚拟机数量400台，配备IPS、AV模块。 |
| 1. 4、采用部署vmware标准环境5.5-7.0版本和NSX组件云环境；支持FusionSphere OpenStack、FusionCompute环境； |
| 1. 5、采用在VMware标准环境，不依赖NSX组件或依赖第三方SDN产品方案配合 |
| 1. 6、采用在VMware标准环境 + NSX组件的云环境中，不依赖第三方SDN产品方案配合，已提供云内虚机间网络微分域解决方案。支持IPv6网络环境。 |
| 1. 7、为同一宿主机，相同VLAN内的虚拟机之间，已提供网络微分域的安全管控服务。 |
| 1. 8、本次所投标产品满足网络安全监测和防护需求，须在非NSX环境下，以及不改变业务原有三层网络结构的前提下，支持2层串行部署模式。 |
| 1. 9、具备L2-L7层安全防护服务能力，包括基础5元组控制能力，应用识别控制能力，以及网络攻击防御、IPS和AV功能。 |
| 1. 10、采用为确保安全服务的有效性，需实时掌握云环境中的资产信息和变更状况，支持对云虚机名称，IP，MAC，网络，宿主机等信息的同步和更新。 |
| 1. 11、支持会话同步能力，安全防护可随虚机迁移而自动跟随，最大限度的确保安全防护的持续性和业务连续性。 |
| 1. 12、采用虚拟资产分布可视化，可基于虚拟网络-虚拟机分组方式管理，并呈现各分组之间和分组内部的流量交换关系。 |
| 1. 13、可基于IP地址，流量，防护状态，虚机和网络名称，应用类型，威胁名称/类型/安全级别等条件不同组合关系控制视图呈现效果 |
| 1. 14、采用分布式处理，基于状态、精准的高性能攻击检测和防御能力。 |
| 1. 15、采用具备7000种以上攻击特征库规则列表，支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征ID等方式的查询；。 |
| 1. 16、采用4000种以上HTTP特征库规则列表。 |
| 1. 17、采用缓冲区溢出、SQL注入、XSS防护，支持HTTP头域中的URL、Cookie、Referer、POST检查点配置防护策略；。 |
| 1. 18、支持针对bzip、gzip、rar、tar、zip、html、jpeg、mail、riff、PE等文件类型的病毒扫描，支持针对POP3\HTTP\SMTP\IMAP4以及FTP协议病毒扫描。 |
| 1. 19、支持多层嵌套式压缩文件的病毒扫描，支持恶意网站过滤功能。具备320万条主流病毒特征库，支持手工导入或网络实时、定时更新。 |
| 1. 20、提供内网安全平台性能监控正式授权一套，实现内网网络监控状态、网络质量状态在线监控 |
| 1. 21、支持虚拟化平台网络、业务状态监控，包括丢包、延时、抖动等参数 |
| 1. 22、支持设置关键参数阈值，如：CPU、内存、丢包、延时、抖动等，对关键业务提供监测告警功能。 |
| 1. 1.为方便管理员制定安全策略，需支持流量学习和安全策略配置的策略助手功能，提高工作效率。 |
| 1. 2.为了能与云管平台协同、自动化工作，RestAPI接口能力，实现产品主要功能特性的对接调用。 |
| 1. 3.为改善安全策略的管理有效率，提升安全服务运行效率，支持对安全策略冗余检测，以及重叠性检查能力。 |
| 1. 23、本次所投标产品采用支持与FireMon和Algosec统一安全策略管理平台联动，实现大规模配置的自动整理收敛。 |
| 1. 24、具有虚拟化微隔离系统著作权，以及相关测试报告； |
| 1. 25、具备公安部颁发的“虚拟化云安全防火墙销售许可证”增强级； |
| 26、提供三年IPS、AV、应用特征库升级及硬件保修、软件升级服务。 |

**附3：**

**售后服务计划及保障措施**

售后服务及培训计划

针对郑州大学中原网络安全研究院工业互联网安全实验室项目（招标编号： 郑大-竞谈-2021-0147 ），我公司承诺投标产品的质量保证期（即保修期）为 1年，提供 1年免费原厂技术支持与上门售后服务，质保期内提供免费升级服务。服务时间从自验收合格之日起计算。

 维修响应时间

我公司承诺就所提供的设备发生故障造成较大影响时，在接到用户保修之后在保修期内对影响生产的软件故障提供 7\*24 服务，1 小时内响应，2 小时内提供补救方案，4 小时内恢复；提供 7×24 小时售后服务响应机制。

 巡检巡修方案

在质保期内，我公司提供一月 1 次的电话巡检和每季度 1 次的现场巡检。

每次巡检时，我公司将对设备的以下情况进行检查：

 设备资源状态

 系统性能

 运行状况调查

 设备安装情况

 物理状态检查

 设备资源状态

 系统性能

 日常情况搜集

 策略配置情况

每次巡检结束之后，我公司将向用户提交巡检报告，报告内容包括： 系统性 能、运行状况、稳定程度等，并对系统的优化和今后运行维护给出建议。

另外，每年度我公司将向用户提交《年度产品运行报告》 巡检方式

我公司提供两者巡检方式：

1.电话巡检

2.现场巡检

 巡检频率

|  |  |
| --- | --- |
| 巡检方式 | 巡检频率 |
| 电话巡检 | 一月 1 次 |
| 现场巡检 | 每季度 1 次 |

 培训计划

我方承诺，经过培训后，确保最终用户的网络安全维护人员及普通用户能够 对网络攻防基础知识、内置安全产品操作有所了解。熟悉目前系统中产品的原理、 部署，充分掌握维护系统、产品正常运行的技术知识，从而快捷的维护本次采购 的设备的日常运行，能够独立地对设备进行管理、维护，而不需厂商技术人员实 时在场指导，能够独立解决系统、产品使用中的一般故障，能根据需求的变化， 对产品配置进行调整，保证系统、产品长期的运行。

基于对本项目极为重视，根据本项目的情况制定了详细的技术培训方案，在 该方案中，我公司将安排原厂商专业的培训讲师，使最终用户相关人员在培训后 能够独立地对安全系统进行管理和维护。我公司的培训内容将包括所提供系统的 结构、性能、维护、定制和升级等各个方面，并提供全套培训课程计划表。

 培训目的

为用户解决技术疑问、排除设备故障、确保设备正常运行，使用户方工作人 员在培训后能熟练地掌握设备的使用和日常维护工作，并能及时排除大部分的设 备障碍。同时使使用老师充分的掌握和了解实训室的具体功能。让老师充分的对 专业技能训练，提高老师的专业综合实践能力，增强专业素养。帮助校方在日常实践过程中充分利用好这项资源，提升整体实力基础。

 培训对象

使用教师:在用户系统的使用中，最多接触系统的人员是各级的使用教师， 为他们提供良好的培训可以提高整个系统的实际使用效率，减少运行维护人员的 工作量，降低系统的运行维护成本。

运行维护、管理人员： 对于本项目这样规模的应用系统的管理、维护会非常 复杂，培养具有一定技术和管理思想的运行维护员和管理人员，对于今后系统的 运行也是非常有益的，所以，我们开设了相关的培训课程，为运行维护员和管理 人员提供培训。

 培训内容

培训内容包括对使用教师、运行维护、管理人员进行详尽的工作原理、操作

使用、一般维护、常见故障排除等一系列的专业培训，使之能够正确操作与使用

全部设备并能进行常见故障排除，提供各个层次的操作培训。

（一） 工作原理培训

设备和系统的基础知识

设备硬件和软件的功能描述

设备硬件的正确使用

设备硬件和软件的调试

（二） 实际操作培训

设备使用注意事项

各种功能的操作方法

系统设备功能的参数设置

各种自动操作预案的设定和使用

各种操作模式的设定和使用

备件的更换

（三） 常见故障的判断及排除培训

设备相互间的连接线路问题

设备网络故障问题

系统（软件） 的升级安装以及维护

 培训地点、对象人数、授课人、费用

（1） 用户场地培训

利用实际系统设备，主要针对技术人员、调度人员进行系统功能、系统原 理、操作使用、故障诊断与排除的培训。在实训室整体环创完成后，我们单位组 织培训讲师向校方专业教师进行教学示范指导 5 天。3 年内，每年 1 次（每次 2 天） 。

整个培训过程采用现场授课、实际操作以及现场演示最后进行考核相结合 的方式进行。使用户既有感官上的认识，又有现场亲自动手操作的切身体会，让 用户充分了解产品的同时，掌握产品的基本构成、工作原理、功能、特性，硬件

的操作与使用及设备的日常维护与保养等基本知识。以此为桥梁为契机，加深用

户与我方之间的相互了解、相互信任，为以后开展工作做好铺垫，打下一个良好

的基础。

（2） 公司培训授课人、对象人数、费用

我公司将组织由设备厂家认证的工程师负责对所售仪器的安装、调试、培训； 为减少用户的操作错误概率，为用户免费培训 1-2 名技术人员，使培训人员达到熟练掌握、灵活应用的程度； 同时安排专业培训讲师进行现场教学示范指导。

所有的培训教员用中文授课并为所有被培训人员提供培训用计算机、网络 环境、文字资料和讲义；所有的培训资料用中文书写；

培训形式：采用线下现场 培训，根据用户需求采用集中培训和分组培训两种方式进行，培训次数 4 次(具 体培训形式按学校要求） ；在设备安装调试、故障处理过程中进行培训。现场培 训包括对运维人员、使用人员的培训。讲授各种设备的安装、运维和使用时注意的事项及相关知识。

根据本项目的实际情况，为了尽快提高本项目设备的操作技能，特制定以 下方案,具体实施培训计划时和招标人协商确定，由招标人统一安排：

一、培训对象： 使用教师、运行维护、管理人员：

二、培训地点： 用户指定地点

三、培训时间： 双方协定

四、培训方式： 采用线下现场培训，根据用户需求采用集中培训和分组培训两种方式进行五、授课人员： 设备厂家认证的工程师和专业培训讲师

六、组织形式： 组织形式分为两种，对学校全体教师着重进行产品操作使用方面 系统培训，对设备管理人员着重进行设备管理系统操作、管理、维护等专项培训。

 项目培训实施流程

1.介绍本次项目的所有设备。

2.了解所有设备的工作原理、组成部分、功能及操作注意事项。

3.现场操作设备。

4.使学员自己动手操作整套教具，针对有疑问的地方进行重点讲解。

5.讲授设备平时使用中易出现的问题，提供解决方案和对策以及日常如何维护。

6.对学校全体教师着重进行产品操作使用方面系统培训，对设备管理人员着重进 行设备管理系统操作、管理、维护等专项培训。

7.由供需双方针对培训进行考核，对于考核不通过的学员再进行针对性的培训， 保证所有受训人员都能操作整套设备； 培训合格的标准为： 被培训者要能依据基 本规则对产品进行正常使用。对于有可能遇到的特殊工作使用条件和任务能合理的应对措施。

附4：

**郑州大学仪器设备初步验收单**

**No. 年 月 日**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 使用单位 | | 郑州大学中原网络安全研究院 | | | 使用人 | 杨晨光 | | 合同编号 | | | | 郑大-竞谈-2021-0147 | |
| 供货商 | | 河南邦德仪器设备有限公司 | | | | | | 合同总金额 | | | | 479800元 | |
| 设备明细（品名、型号、规格、生产厂家、数量、金额等，不够可另附表） | | | | | | | | | | | | | |
| **序号** | **品名** | | | **技术参数**  **（规格型号）** | | | **生产厂家（产地）** | | **数量** | | **单位** | | **金额（元）** |
| 1 | 工控安全防护系统平台 | | | 天融信NGFW4000-UF/TG-A2614 | | | 北京天融信网络安全技术有限公司 | | 1 | | 套 | | 35700 |
| 2 | 终端安全防护系统 | | | 天融信TopEDR/EDR-E-WINSER3/LINUX3-LIC1 | | | 北京天融信网络安全技术有限公司 | | 1 | | 套 | | 41100 |
| 3 | 安全审计系统平台 | | | 天融信TopAudit/TA-L-SE-50 | | | 北京天融信网络安全技术有限公司 | | 1 | | 套 | | 36500 |
| 4 | WEB安全应用平台 | | | 天融信TopWAF/TWF-A3106 | | | 北京天融信网络安全技术有限公司 | | 1 | | 套 | | 34500 |
| 5 | 24口接入交换机 | | | 华三S5130S-28S-E1 | | | 新华三技术有限公司 | | 2 | | 台 | | 39500 |
| 6 | 网络微分域安全平台 | | | 山石网科CloudHive-vSSM | | | 北京山石网科信息技术有限公司 | | 1 | | 套 | | 253000 |
| 实 物 验 收 情 况 | 外观质量（有无残损，程度如何）。 | | | | | | | | | | | | |
| 清点数量（主机、配件、型号、规格、产地是否与招投标文件、合同、发票、装箱单的数量相同，若有出入，说明缺件名称、规格、数量、金额）。 | | | | | | | | | | | | |
| 仪器设备安装调试及使用人员培训情况（是否完成整套设备安装、有无安装缺陷，使用人员是否经过培训）。 | | | | | | | | | | | | |
| 技术验收情况 | 依据合同约定技术条款逐一测定设备的性能和各项技术指标，所测结果是否与合同约定技术条款规定的一样，性能是否稳定，配件是否齐全，是否有安全隐患，具体说明。 | | | | | | | | | | | | |
| 初步验收情况 | □通过验收 □整改后再组织验收  □不通过验收 索赔要求 □其他结论 | | | | | | | | | | | | |
| 验收小组  成员签字 | | |  | | | | 供货商  授权代表签字 | | |  | | | |

**附5：**

**中标通知书**

