政府采购货物买卖合同

项目名称：河南财经政法大学网络安全加固项目

合同编号：

甲　　方：河南财经政法大学

乙　　方：紫光软件系统有限公司

签订时间：2024 年 12 月 18 日

第一节 政府采购合同协议书

甲方（全称）：河南财经政法大学（采购人、受采购人委托签订合同的单位或采购文件约定的合同甲方）

乙方：紫光软件系统有限公司（供应商或成交人）

依据《中华人民共和国民法典》、《中华人民共和国政府采购法》等有关的法律法规，以及本采购项目的招标/谈判文件等采购文件、乙方的《投标（响应）文件》及《中标（成交）通知书》，甲乙双方同意签订本合同。具体情况及要求如下：

1. 项目信息

（1）采购项目名称：河南财经政法大学网络安全加固项目

采购项目编号：豫财磋商采购-2024-1282

（2）采购计划编号：豫财磋商采购-2024-1282

（3）项目内容：

采购标的及数量（台/套/个/架/组等）：出口防火墙、1台

品牌：山石 规格型号：SG-6000-X8180-CN（软件：网科防火墙 SG-6000（万兆）V5.5）

采购标的及数量（台/套/个/架/组等）：数据中心防火墙、1台

品牌：山石 规格型号：SG-6000-A5800-CN （软件：网科防火墙 SG-6000-A（万兆）V5.5）

采购标的及数量（台/套/个/架/组等）：威胁检测探针、1台

品牌：山石 规格型号：BDS-I5835-ThreatSensor-AD-4T-CN（软件：网科 APT 监测平台(智能内网威胁感知系统)BDS/V5.5）

采购标的及数量（台/套/个/架/组等）：WEB 应用防火墙、1台

品牌：奇安信 规格型号：W9000-U045M （软件：网神 SecWAF3600Web 应用防火墙系统 SecWAF(万兆）V4.0）

采购标的及数量（台/套/个/架/组等）：一卡通防火墙、1台

品牌：奇安信 规格型号：NSG4000-TG45 （软件：网神 SecGate3600 安全网关 NSG（万兆）V3.6.6.0）

采购标的及数量（台/套/个/架/组等）：日志审计、1台

品牌：奇安信 规格型号：LAS-R33M （软件：网神 SecFox 日志收集与分析系统

LAS V5.0）

采购标的及数量（台/套/个/架/组等）：漏扫系统、1台

品牌：奇安信 规格型号：S5000-W020 （软件：网神SecVSS3600漏洞扫描系统SecVSS V3.0）

采购标的及数量（台/套/个/架/组等）：上网行为管理、1台

品牌：奇安信 规格型号：NBM7370 （软件：奇安信网神上网行为管理系统 NBM V7.0）

采购标的及数量（台/套/个/架/组等）：流量复制器、1台

品牌：盛邦 规格型号：下一代流量复制汇聚平台RayNGTAP-8000-Q0024E

采购标的及数量（台/套/个/架/组等）：智能IP统一管理平台系统、1台

品牌：木云 规格型号：MYIP-2200PLUS （软件：木云智能IP统一管理平台系统V3.2）

采购标的及数量（台/套/个/架/组等）：智能DNS系统、1台

品牌：木云 规格型号：MYD-3500 （软件：木云智能DNS系统V2.0）

采购标的及数量（台/套/个/架/组等）：服务器安全防护系统、1套

品牌：奇安信 规格型号：USS-AES-CPU-FL-STE-PS （软件：网神云锁服务器安全管理系统V8.0）

采购标的及数量（台/套/个/架/组等）：终端安全防护系统、1套

品牌：奇安信 规格型号：ESM-MGR （软件：天擎终端安全管理系统V10.0）

采购标的及数量（台/套/个/架/组等）：运维安全审计系统、1套

品牌：飞致云 规格型号：JumpServer运维安全审计系统 V3

采购标的及数量（台/套/个/架/组等）：综合布线、1项

品牌：紫光 规格型号：定制

采购标的的技术要求、商务要求具体见附件。

① 涉及信息类产品，请填写该产品关键部件的品牌、型号：

标的名称：/

关键部件：/ 品牌：/ 型号：/

关键部件：/ 品牌：/ 型号：/

关键部件：/ 品牌：/ 型号：/

（注：关键部件是指财政部会同有关部门发布的政府采购需求标准规定的需要通过国家有关部门指定的测评机构开展的安全可靠测评的软硬件，如CPU芯片、操作系统、数据库等。）

② 涉及车辆采购，请填写是否属于新能源汽车：

□是，《政府采购品目分类目录》底级品目名称：/ 数量：/ 金额：/

□否

（4）政府采购组织形式：■政府集中采购 □部门集中采购 □分散采购

（5）政府采购方式：□公开招标 □邀请招标 □竞争性谈判 ■竞争性磋商

□询价 □单一来源 □框架协议 □其他：/

（注：在框架协议采购的第二阶段，可选择使用该合同文本）

（6）中标（成交）采购标的制造商是否为中小企业：□是 ■否

本合同是否为专门面向中小企业的采购合同（中小企业预留合同）：□是 ■否

若本项目不专门面向中小企业采购，是否给予小微企业评审优惠：■是 □否

中标（成交）采购标的制造商是否为残疾人福利性单位：□是 ■否

中标（成交）采购标的制造商是否为监狱企业：□是 ■否

（7）合同是否分包：□是 ■否

分包主要内容：/

分包供应商/制造商名称（如供应商和制造商不同，请分别填写）：/

分包供应商/制造商类型（如果供应商和制造商不同，只填写制造商类型）：

□大型企业 □中型企业 □小微型企业

□残疾人福利性单位 □监狱企业 □其他

（8）中标（成交）供应商是否为外商投资企业：□是 ■否

外商投资企业类型：□全部由外国投资者投资 □部分由外国投资者投资

（9）是否涉及进口产品：

□是，《政府采购品目分类目录》底级品目名称：/ 金额：/

国别：/ 品牌：/ 规格型号：/

■否

（10）是否涉及节能产品：

□是，《节能产品政府采购品目清单》的底级品目名称：/

□强制采购　　□优先采购

■否

是否涉及环境标志产品：

□是，《环境标志产品政府采购品目清单》的底级品目名称：/

□强制采购　　□优先采购

■否

是否涉及绿色产品：

□是，绿色产品政府采购相关政策确定的底级品目名称：/

□强制采购　　□优先采购

■否

（11）涉及商品包装和快递包装的，是否参考《商品包装政府采购需求标准（试行）》、《快递包装政府采购需求标准（试行）》明确产品及相关快递服务的具体包装要求：

■是　　□否　　□不涉及

2. 合同金额

（1）合同金额小写：¥2538600

大写：贰佰伍拾叁万捌仟陆佰元整

分包金额（如有）小写：/

大写：/

（注：固定单价合同应填写单价和最高限价）

（2）合同定价方式（采用组合定价方式的，可以勾选多项）：

■固定总价 ■固定单价 □固定费率 □成本补偿 □绩效激励 □其他/

（3）付款方式（按项目实际勾选填写）：

☑ 全额付款：合同签订后（甲方在收到乙方开具相应金额的发票后 15 个工作日内），甲方向乙方支付合同金额的 70%作为预付款。项目验收合格后（15 个工作日内），甲方向乙方支付合同剩余金额的 30%，共计 100%。

□分期付款：/

□成本补偿：/

□绩效激励：/

3. 合同履行

（1）起始日期：2024年12月18日，完成日期：2024年12月26日。

（2）履约地点：河南财经政法大学郑东校区实验楼Λ座1楼

（3）履约担保：是否收取履约保证金：☑ 是　□否

收取履约保证金形式：转账

收取履约保证金金额：签订正式合同之前，乙方向甲方提供合同金额5%（小写：¥126930；大写：壹拾贰万陆仟玖佰叁拾元整）的履约保证金

履约担保期限：交货履约完成后 30 日内且乙方无违约行为向乙方退还履约保证金

（4）分期履行要求：无

（5）风险处置措施和替代方案：无

4. 合同验收

（1）验收组织方式：■自行组织 □委托第三方组织

验收主体：河南财经政法大学

是否邀请本项目的其他供应商参加验收：□是　■否

是否邀请专家参加验收：□是　■否

是否邀请服务对象参加验收：■是　□否

是否邀请第三方检测机构参加验收：□是　■否

是否进行抽查检测：□是，抽查比例：/　■否

是否存在破坏性检测：□是，（应明确对被破坏的检测产品的处理方式）

■否

验收组织的其他事项：无

（2）履约验收时间：（供应商提出验收申请之日起3日内组织验收）

（3）履约验收方式：■一次性验收

□分期/分项验收：（应明确分期/分项验收的工作安排）

（4）履约验收程序：确定验收标准-履约验收前的准备工作-履约验收的实施-履约验收的结果确认。

（5）履约验收的内容：乙方供货完成并且安装调试完成后，由甲方对货物的质量、规格和数量进行验收，如果发现规格、数量或两者有与合同附件2（货物技术性能参数）要求不一致的地方；或证实货物是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方应

尽快以书面形式通知乙方。乙方在收到通知后最迟应于 48 小时内解决问题。如设备运行期间出现故障，乙方于接到甲方通知后 30 分钟内响应，2 小时到达现场维修维护设备。

（6）履约验收标准：符合行业管理部门规定的标准、方法和磋商文件、合同中内容

（7）是否以采购活动中供应商提供的样品作为参考：□是 ■否

（8）履约验收其他事项：无

5. 组成合同的文件

本协议书与下列文件一起构成合同文件，如下述文件之间有任何抵触、矛盾或歧义，应按以下顺序解释：

（1）政府采购合同协议书及其变更、补充协议

（2）政府采购合同专用条款

（3）政府采购合同通用条款

（4）中标（成交）通知书

（5）投标（响应）文件

（6）采购文件

（7）有关技术文件，图纸

（8）国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件

6. 合同生效

本合同自 2024 年 12 月 18 日签字盖章后生效。

7. 合同份数

本合同一式 8 份，甲方执 6 份，乙方执 2 份，均具有同等法律效力。

合同订立时间：2024 年 12 月 18 日

合同订立地点：河南财经政法大学

附件：具体标的及其技术要求和商务要求、联合协议、分包意向协议等。

甲方（采购人、受采购人委托签订合同的单位或采购文件约定的合同甲方）		乙方（供应商）	
单位名称（公章或合同章）	河南财经政法大学	单位名称（公章或合同章）	紫光软件系统有限公司
法定代表人或其委托代理人（签章）		法定代表人或其委托代理人（签章）	
		拥有者性别	男
住　所	郑州市金水东路 180 号	住　所	北京市海淀区中关村东路 1 号院 2 号楼 318 室
联 系 人	任剑锋	联 系 人	李超
联系电话	0371-86170001	联系电话	18611888108
通信地址	郑州市金水东路 180 号河南财经政法大学信息化管理中心	通信地址	北京市海淀区中关村东路 1 号院 2 号楼 318 室
邮政编码	450001	邮政编码	100084
电子邮箱	cyrjf@163.com	电子邮箱	lichao@unissoft.com
统一社会信用代码	12410000415803470E	统一社会信用代码	9111010880212382XF
		开户名称	紫光软件系统有限公司
		开户银行	招商银行股份有限公司北京清华园科技金融支行
		银行账号	866780433810001
注：涉及联合体或其他合同主体的信息应按上表格式加列。			

第二节 政府采购合同通用条款

1. 定义

1.1 合同当事人

（1）采购人（以下称甲方）是指使用财政性资金，通过政府采购方式向供应商购买货物及其相关服务的国家机关、事业单位、团体组织。

（2）供应商（以下称乙方）是指参加政府采购活动并且中标（成交），向采购人提供合同约定的货物及其相关服务的法人、非法人组织或者自然人。

（3）其他合同主体是指除采购人和供应商以外，依法参与合同缔结或履行，享有权利、承担义务的合同当事人。

1.2 本合同下列术语应解释为：

（1）“合同”系指合同当事人意思表示达成一致的任何协议，包括签署的政府采购合同协议书及其变更、补充协议，政府采购合同专用条款，政府采购合同通用条款，中标（成交）通知书，投标（响应）文件，采购文件，有关技术文件和图纸，以及国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件。

（2）“合同价款”系指根据本合同规定乙方在全面履行合同义务后甲方应支付给乙方的价款。

（3）“货物”系指乙方根据本合同规定须向甲方提供的各种形态和种类的物品，包括原材料、设备、产品（包括软件）及相关的其备品备件、工具、手册及其他技术资料和材料等。

（4）“相关服务”系指根据合同规定，乙方应提供的与货物有关的技术、管理和其他服务，包括但不限于：管理和质量保证、运输、保险、检验、现场准备、安装、集成、调试、培训、维修、废弃处置、技术支持等以及合同中规定乙方应承担的其他义务。

（5）“分包”系指中标（成交）供应商按采购文件、投标（响应）文件的规定，根据分包意向协议，将中标（成交）项目中的部分履约内容，分给具有相应资质条件的供应商履行合同的行为。

（6）“联合体”系指由两个以上的自然人、法人或者非法人组织组成，以一个供应商的身份共同参加政府采购的主体。联合体各方应在签订合同协议书前向甲方提交联合协议，且明确牵头人及各成员单位的工作分工、权利、义务、责任，联合体各方应共同与甲方签订合同，就合同约定的事项对甲方承担连带责任。联合体具体要求见**【政府采购合同专用条款】**。

（7）其他术语解释，见**【政府采购合同专用条款】**。

2. 合同标的及金额

2.1 合同标的及金额应与中标（成交）结果一致。乙方为履行本合同而发生的所有费用均应包含在合同价款中，甲方不再另行支付其他任何费用。

3. 履行合同的时间、地点和方式

3.1 乙方应当在约定的时间、地点，按照约定方式履行合同。

4. 甲方的权利和义务

4.1 签署合同后，甲方应确定项目负责人（或项目联系人），负责与本合同有关的事务。甲方有权对乙方的履约行为进行检查，并及时确认乙方提交的事项。甲方应当配合乙方完成相关项目实施工作。

4.2 甲方有权要求乙方按时提交各阶段有关安排计划，并有权定期核对乙方提供货物数量、规格、质量等内容。甲方有权督促乙方工作并要求乙方更换不符合要求的货物。

4.3 甲方有权要求乙方对缺陷部分予以修复，并按合同约定享有货物保修及其他合同约定的权利。

4.4 甲方应当按照合同约定及时对交付的货物进行验收，未在**【政府采购合同专用条款】**约定的期限内对乙方履约提出任何异议或者向乙方作出任何说明的，视为验收通过。

4.5 甲方应当根据合同约定及时向乙方支付合同价款，不得以内部人员变更、履行内部付款流程等为由，拒绝或迟延支付。

4.6 国家法律法规规定及**【政府采购合同专用条款】**约定应由甲方承担的其他义务和责任。

5. 乙方的权利和义务

5.1 签署合同后，乙方应确定项目负责人（或项目联系人），负责与本合同有关的事务。

5.2 乙方应按照合同要求履约，充分合理安排，确保提供的货物及相关服务符合合同有关要求。接受项目行业管理部门及政府有关部门的指导，配合甲方的履约检查及验收，并负责项目实施过程中的所有协调工作。

5.3 乙方有权根据合同约定向甲方收取合同价款。

5.4 国家法律法规规定及【政府采购合同专用条款】约定应由乙方承担的其他义务和责任。

6. 合同履行

6.1 甲乙双方应当按照**【政府采购合同专用条款】**约定顺序履行合同义务；如果没有先后顺序的，应当同时履行。

6.2 甲乙双方按照合同约定顺序履行合同义务时，应当先履行一方未履行的，后履行一方有权拒绝其履行请求。先履行一方履行不符合约定的，后履行一方有权拒绝其相应的履行请求。

7. 货物包装、运输、保险和交付要求

7.1 本合同涉及商品包装、快递包装的，除**【政府采购合同专用条款】**另有约定外，包装应适应远距离运输、防潮、防震、防锈和防野蛮装卸等要求，确保货物安全无损地运抵**【政府采购合同专用条款】**约定的指定现场。

7.2 除**【政府采购合同专用条款】**另有约定外，乙方负责办理将货物运抵本合同规定的交货地点，并装卸、交付至甲方的一切运输事项，相关费用应包含在合同价款中。

7.3 货物保险要求按**【政府采购合同专用条款】**规定执行。

7.4 除采购活动对商品包装、快递包装达成具体约定外，乙方提供产品及相关快递服务涉及到具体包装要求的，应不低于《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》标准，并作为履约验收的内容，必要时甲方可以要求乙方在履约验收环节出具检测报告。

7.5 乙方在运输到达之前应提前通知甲方，并提示货物运输装卸的注意事项，甲方配合乙方做好货物的接收工作。

7.6 如因包装、运输问题导致货物损毁、丢失或者品质下降，甲方有权要求降价、换货、拒收部分或整批货物，由此产生的费用和损失，均由乙方承担。

8. 质量标准和保证

8.1 质量标准

（1）本合同下提供的货物应符合合同约定的品牌、规格型号、技术性能、配置、质量、数量等要求。质量要求不明确的，按照强制性国家标准履行；没有强制性国家标准的，按照推荐性国家标准履行；没有推荐性国家标准的，按照行业标准履行；没有国家标准、行业标准的，按照通常标准或者符合合同目的的特定标准履行。

（2）采用中华人民共和国法定计量单位。

（3）乙方所提供的货物应符合国家有关安全、环保、卫生的规定。

（4）乙方应向甲方提交所提供货物的技术文件，包括相应的中文技术文件，如：产品目录、图纸、操作手册、使用说明、维护手册或服务指南等。上述文件应包装好随货物一同发运。

8.2 保证

（1）乙方应保证提供的货物完全符合合同规定的质量、规格和性能要求。乙方应保证货物在正确安装、正常使用和保养条件下，在其使用寿命期内具备合同约定的性能。存在质量保证期的，货物最终交付验收合格后在**【政府采购合同专用条款】**规定或乙方书面承诺（两者以较长的为准）的质量保证期内，本保证保持有效。

（2）在质量保证期内所发现的缺陷，甲方应尽快以书面形式通知乙方。

（3）乙方收到通知后，应在**【政府采购合同专用条款】**规定的响应时间内以合理的速度免费维修或更换有缺陷的货物或部件。

（4）在质量保证期内，如果货物的质量或规格与合同不符，或证实货物是有缺陷的，包括潜在的缺陷或使用不符合要求的材料等，甲方可以根据本合同第 15.1 条规定以书面形式追究乙方的违约责任。

（5）乙方在约定的时间内未能弥补缺陷，甲方可采取必要的补救措施，但其风险和费用将由乙方承担，甲方根据合同约定对乙方行使的其他权利不受影响。

9. 权利瑕疵担保

9.1 乙方保证对其出售的货物享有合法的权利。

9.2 乙方保证在交付的货物上不存在抵押权等担保物权。

9.3 如甲方使用上述货物构成对第三人侵权的，则由乙方承担全部责任。

10. 知识产权保护

10.1 乙方对其所销售的货物应当享有知识产权或经权利人合法授权，保证没有侵犯任何第三人的知识产权等权利。因违反前述约定对第三人构成侵权的，应当由乙方向第三人承担法律责任；甲方依法向第三人赔偿后，有权向乙方追偿。甲方有其他损失的，乙方应当赔偿。

11. 保密义务

11.1 甲、乙双方对采购和合同履行过程中所获悉的国家秘密、工作秘密、商业秘密或者其他应当保密的信息，均有保密义务且不受合同有效期所限，直至该信息成为公开信息。泄露、不正当地使用国家秘密、工作秘密、商业秘密或者其他应当保密的信息，应当承担相应责任。其他应当保密的信息由双方在**【政府采购合同专用条款】**中约定。

12. 合同价款支付

12.1 合同价款支付按照国库集中支付制度及财政管理相关规定执行。

12.2 对于满足合同约定支付条件的，甲方原则上应当自收到发票后 15 个工作日内将

资金支付到合同约定的乙方账户，不得以机构变动、人员更替、政策调整等为由迟延付款，不得将采购文件和合同中未规定的义务作为向乙方付款的条件。具体合同价款支付时间在**【政府采购合同专用条款】**中约定。

13. 履约保证金

13.1 乙方应当以支票、汇票、本票或者金融机构、担保机构出具的保函等非现金形式提交。

13.2 如果乙方出现**【政府采购合同专用条款】**约定情形的，履约保证金不予退还；如果乙方未能按合同约定全面履行义务，甲方有权从履约保证金中取得补偿或赔偿，且不影响甲方要求乙方承担合同约定的超过履约保证金的违约责任的权利。

13.3 甲方在项目通过验收后按照**【政府采购合同专用条款】**规定的时间内将履约保证金退还乙方；逾期退还的，乙方可要求甲方支付违约金，违约金按照**【政府采购合同专用条款】**规定支付。

14. 售后服务

14.1 除项目不涉及或采购活动中明确约定无须承担外，乙方还应提供下列服务：

（1）货物的现场移动、安装、调试、启动监督及技术支持；

（2）提供货物组装和维修所需的专用工具和辅助材料；

（3）在**【政府采购合同专用条款】**约定的期限内对所有的货物实施运行监督、维修，但前提条件是该服务并不能免除乙方在质量保证期内所承担的义务；

（4）在制造商所在地或指定现场就货物的安装、启动、运营、维护、废弃处置等对甲方操作人员进行培训；

（5）依照法律、行政法规的规定或者按照**【政府采购合同专用条款】**约定，货物在有效使用年限届满后应予回收的，乙方负有自行或者委托第三人对货物予以回收的义务；

（6）**【政府采购合同专用条款】**规定由乙方提供的其他服务。

14.2 乙方提供的售后服务的费用已包含在合同价款中，甲方不再另行支付。

15. 违约责任

15.1 质量瑕疵的违约责任

乙方提供的产品不符合合同约定的质量标准或存在产品质量缺陷，甲方有权要求乙方根据**【政府采购合同专用条款】**要求及时修理、重作、更换，并承担由此给甲方造成的损失。

15.2 迟延交货的违约责任

（1）乙方应按照本合同规定的时间、地点交货和提供相关服务。在履行合同过程中，如果乙方遇到可能影响按时交货和提供服务的情形时，应及时以书面形式将迟延的事实、可能迟延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延长交货时间或延期提供服务。

（2）如果乙方没有按照合同规定的时间交货和提供相关服务，甲方有权从货款中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按**【政府采购合同专用条款】**规定执行。如果涉及公共利益，且赔偿金额无法弥补公共利益损失，甲方可要求继续履行或者采取其他补救措施。

15.3 迟延支付的违约责任

甲方存在迟延支付乙方合同款项的，应当承担**【政府采购合同专用条款】**规定的逾期付款利息。

15.4 其他违约责任根据项目实际需要按**【政府采购合同专用条款】**规定执行。

16. 合同变更、中止与终止

16.1 合同的变更

政府采购合同履行中，在不改变合同其他条款的前提下，甲方可以在合同价款10%的范围内追加与合同标的相同的货物，并就此与乙方协商一致后签订补充协议。

16.2 合同的中止

（1）合同履行过程中因供应商就采购文件、采购过程或结果提起投诉的，甲方认为有必要的，可以中止合同的履行。

（2）合同履行过程中，如果乙方出现以下情形之一的：1．经营状况严重恶化；2．转移财产、抽逃资金，以逃避债务；3．丧失商业信誉；4．有丧失或者可能丧失履约能力的其他情形，乙方有义务及时告知甲方。甲方有权以书面形式通知乙方中止合同并要求乙方在合理期限内消除相关情形或者提供适当担保。乙方提供适当担保的，合同继续履行；乙方在合理期限内未恢复履约能力且未提供适当担保的，视为拒绝继续履约，甲方有权解除合同并要求乙方承担由此给甲方造成的损失。

（3）乙方分立、合并或者变更住所的，应当及时以书面形式告知甲方。乙方没有及时告知甲方，致使合同履行发生困难的，甲方可以中止合同履行并要求乙方承担由此给甲方造成的损失。

（4）甲方不得以行政区划调整、政府换届、机构或者职能调整以及相关责任人更替为由

中止合同。

16.3 合同的终止

（1）合同因有效期限届满而终止；

（2）乙方未按合同约定履行，构成根本性违约的，甲方有权终止合同，并追究乙方的违约责任。

16.4 涉及国家利益、社会公共利益的情形

政府采购合同继续履行将损害国家利益和社会公共利益的，双方当事人应当变更、中止或者终止合同。有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。

17. 合同分包

17.1 乙方不得将合同转包给其他供应商。涉及合同分包的，乙方应根据采购文件和投标（响应）文件规定进行合同分包。

17.2 乙方执行政府采购政策向中小企业依法分包的，乙方应当按采购文件和投标（响应）文件签订分包意向协议，分包意向协议属于本合同组成部分。

18. 不可抗力

18.1 不可抗力是指合同双方不能预见、不能避免且不能克服的客观情况。

18.2 任何一方对由于不可抗力造成的部分或全部不能履行合同不承担违约责任。但迟延履行后发生不可抗力的，不能免除责任。

18.3 遇有不可抗力的一方，应及时将事件情况以书面形式告知另一方，并在事件发生后及时向另一方提交合同不能履行或部分不能履行或需要延期履行的详细报告，以及证明不可抗力发生及其持续时间的证据。

19. 解决争议的方法

19.1 因本合同及合同有关事项发生的争议，由甲乙双方友好协商解决。协商不成时，可以向甲方所在地人民调解委员会申请调解。合同一方或双方不愿调解或调解不成的，可以通过仲裁或诉讼的方式解决争议。

19.2 选择仲裁的，应在**【政府采购合同专用条款】**中明确仲裁机构及仲裁地；通过诉讼方式解决的，可以在**【政府采购合同专用条款】**中进一步约定选择与争议有实际联系的地点的人民法院管辖，但管辖法院的约定不得违反级别管辖和专属管辖的规定。

19.3 如甲乙双方有争议的事项不影响合同其他部分的履行，在争议解决期间，合同其他部分应当继续履行。

20. 政府采购政策

20.1 本合同应当按照规定执行政府采购政策。

20.2 本合同依法执行政府采购政策的方式和内容，属于合同履约验收的范围。甲乙双方未按规定要求执行政府采购政策造成损失的，有过错的一方应当承担赔偿责任，双方都有过错的，各自承担相应的责任。

20.3 对于为落实中小企业支持政策，通过采购项目整体预留、设置采购包专门预留、要求以联合体形式参加或者合同分包等措施签订的采购合同，应当明确标注本合同为中小企业预留合同。其中，要求以联合体形式参加采购活动或者合同分包的，须将联合协议或者分包意向协议作为采购合同的组成部分。

21. 法律适用

21.1 本合同的订立、生效、解释、履行及与本合同有关的争议解决，均适用法律、行政法规。

21.2 本合同条款与法律、行政法规的强制性规定不一致的，双方当事人应按照法律、行政法规的强制性规定修改本合同的相关条款。

22. 通知

22.1 本合同任何一方向对方发出的通知、信件、数据电文等，应当发送至本合同第一部分《政府采购合同协议书》所约定的通讯地址、联系人、联系电话或电子邮箱。

22.2 一方当事人变更名称、住所、联系人、联系电话或电子邮箱等信息的，应当在变更后3日内及时书面通知对方，对方实际收到变更通知前的送达仍为有效送达。

22.3 本合同一方给另一方的通知均应采用书面形式，传真或快递。

第三节 政府采购合同专用条款

第二节 第 1.2（6）项	联合体具体要求	不接受联合体
第二节 第 1.2（7）项	其他术语解释	无
第二节 第 4.4 款	履约验收中甲方提出异议或作出说明的期限	10 个工作日
第二节 第 4.6 款	约定甲方承担的其他义务和责任	无
第二节 第 5.4 款	约定乙方承担的其他义务和责任	无
第二节 第 6.1 款	履行合同义务的顺序	无
第二节 第 7.1 款	包装特殊要求	包装方式（防潮、缓冲设计）应满足国标要求，并防潮防震防倾倒标识。由于运输包装、贮存不当导致的设备损坏由供应商负责。
	指定现场	河南财经政法大学
第二节 第 7.2 款	运输特殊要求	无
第二节 第 7.3 款	保险要求	无
第二节 第 8.2（1）项	质量保证期	自验收合格之日起 3 年
第二节 第 8.2（3）项	货物质量缺陷 响应时间	同采购需求内要求
第二节 第11.1款	其他应当保密的信息	无

第二节 第 12.2 款	合同价款支付时间	付款方法和条件：合同签订后（甲方在收到乙方开具相应金额的发票后 15 个工作日内 ），甲方向乙方支付合同金额的 70%作为预付款。项目验收合格后（15 个工作日内），甲方向乙方支付合同剩余金额的 30%，共计 100%。
第二节 第 13.2 款	履约保证金不予退还的情形	如果乙方有违约行为，履约保证金不予退还。
第二节 第 13.3 款	履约保证金退还时间及逾期退还的违约金	采购人应于交货履约完成后 30 日内向成交人退还履约保证金。
第二节 第 14.1（3）项	运行监督、维修期限	3 年
第二节 第 14.1（5）项	货物回收的约定	无
第二节 第 14.1（6）项	乙方提供的其他服务	无
第二节 第 15.1 款	修理、重作、更换相关具体规定	无
第二节 第 15.2（2）项	迟延交货赔偿费	1 乙方未按合同规定时间完成供货、设备安装调试、系统集成环境改造达到验收条件，乙方每逾期一天，须按照合同总额 5‰的标准向甲方交纳违约金，累计不超过合同总额的 5%。 2. 未能按期完成，经乙方提出逾期情况说明，甲方同意 延期，不视为乙方违约。

第二节 第 15.3 款	逾期付款利息	无
第二节 第 15.4 款	其他违约责任	无
第二节 第 19.2 款	解决争议的方法	因本合同及合同有关事项发生的争议，按下列第 2 种方式解决： （1）向郑州市郑东新区仲裁委员会申请仲裁，仲裁地点为甲方所在地； （2）向甲方所在地人民法院起诉。
第二节 第 23.1 款	其他专用条款	无

附件 1

报价明细表

单位：人民币元

序号	货物名称	品牌	产地	规格型号	单位	数量	单价（元）（不含税）	单价（元）（含税）	合计（元）
1	出口防火墙	山石	北京	SG-6000-X8180-CN（软件：网科防火墙 SG-6000（万兆）V5.5）	台	1	362831.86	410000.00	410000.00
2	数据中心防火墙	山石	北京	SG-6000-A5800-CN（软件：网科防火墙 SG-6000-A（万兆）V5.5）	台	1	221238.94	250000.00	250000.00
3	威胁检测探针	山石	北京	BDS-I5835-ThreatSensor-AD-4T-CN（软件：网科 APT 监测平台(智能内网威胁感知系统) BDS/V5.5）	台	1	203539.82	230000.00	230000.00
4	WEB 应用防火墙	奇安信	北京	W9000-U045M（软件：网神 SecWAF3600Web 应用防火墙系统 SecWAF(万兆）V4.0）	台	1	146017.70	165000.00	165000.00
5	一卡通防火墙	奇安信	北京	NSG4000-TG45（软件：网神 SecGate3600 安全网关 NSG（万兆）V3.6.6.0）	台	1	115044.25	130000.00	130000.00
6	日志审计	奇安信	北京	LAS-R33M（软件：网神 SecFox 日志收集与分析系统 LAS V5.0）	台	1	123893.81	140000.00	140000.00
7	漏扫系统	奇安信	北京	S5000-W020（软件：网神 SecVSS3600 漏洞扫描系统 SecVSS V3.0）	台	1	97345.13	110000.00	110000.00

8	上网行为管理	奇安信	北京	NBM7370 （软件：奇安信网神上网行为管理系统 NBM V7.0）	台	1	228849.56	258600.00	258600.00
9	流量复制器	盛邦	北京	下一代流量复制汇聚平台 RayNGTAP-8000-Q0024E	台	1	97345.13	110000.00	110000.00
10	智能 IP 统一管理平台系统	木云	郑州	MYIP-2200PLUS （软件：木云智能 IP 统一管理平台系统 V3.2）	台	1	176991.15	200000.00	200000.00
11	智能 DNS 系统	木云	郑州	MYD-3500 （软件：木云智能 DNS 系统 V2.0）	台	1	194690.27	220000.00	220000.00
12	服务器安全防护系统	奇安信	北京	USS-AES-CPU-FL-STE-PS （软件：网神云锁服务器安全管理系统 V8.0）	套	1	97345.13	110000.00	110000.00
13	终端安全防护系统	奇安信	北京	ESM-MGR （软件：天擎终端安全管理系统 V10.0）	套	1	57522.12	65000.00	65000.00
14	运维安全审计系统	飞致云	杭州	JumpServer 运维安全审计系统 V3	套	1	79646.02	90000.00	90000.00
15	综合布线	紫光	北京	定制	项	1	44247.79	50000.00	50000.00
总计　大写：贰佰伍拾叁万捌仟陆佰元整									2538600

附件 2　　货物技术性能参数

一、出口防火墙　数量：1 台

品牌型号：山石 SG-6000-X8180-CN（软件：网科防火墙 SG-6000（万兆）V5.5）

1、具备可插拔冗余电源模块、冗余风扇模块，采用控制、数据、业务相分离的分布式架构，主控引擎、业务引擎、接口单元均硬件槽位分离；设备高度 3U，用于流量分析和安全防护的内核数 24 个，所有功能完全支持 IPv4 和 IPv6；

2、配置独立主控卡 2 块，接口业务处理卡 1 块，电源 2 块，风扇 4 块；配置后满足具备独立的 CON 口 2 个，USB 口 1 个，MGT 口 2 个，HA 光接口 4 个，万兆接口 16 个，100G 接口 2 个；吞吐量：200Gbps，最大并发连接数 4500 万，每秒新建连接数 90 万；满配整机最大吞吐量 600Gbps，最大并发连接数 1.8 亿，每秒新建连接数 400 万；提供三年升级许可服务，服务内容包含但不限于用识别特征库、僵尸网络防御、入侵防御、防病毒、威胁情报等；

3、具备本地日志存储功能，每个主控板卡实配 2T SSD 硬盘，日志可从指定接口输出到多个 syslog 设备；

4、支持策略规则数 100 万条；

5、支持基于应用/角色/国家地理 IP 的安全策略，支持基于国家/地区维度进行流量控制等安全策略，支持自学习生成策略，支持垃圾策略清理，支持聚合策略以及策略导出；

6、支持策略优化功能，提取策略 ID 的流量进行分析，根据管理员设置的替换规则、聚合规则自动生成安全策略规则；

7、支持针对特定域名进行链路质量探测选择最优线路；支持基于应用特征的策略路由，包含但不限于 P2P 流量、网络视频流量指定从某条或多条运营商链路转发；

8、具备 ssl vpn 功能，实配并发用户数 128 个，最大可支持 20000 个。实配 l2tp 功能，可创建 lns 数量 50 个，每个 lns 可归属到一个安全域，lns 地址与拨入后地址池可自由组合 ipv4/ipv6 地址及仅使用单一协议栈使用 l2tp 完整功能，并发连入用户数 20000 个；

9、针对设备检测到的威胁可跳转至威胁情报平台查询与溯源，云端提供多维度的威胁溯源分析；

10、具备抵御各类攻击，包括但不限于 DNS Flood、SYS Flood、UDP Flood、ICMP Flood、Ping of Death、Winnuke 等网络攻击，支持 Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法超大 ICMP 报文、地址扫描、支端口扫描等攻击行为；

11、具备独立的僵尸网络防御模块，特征库基于网络实时更新，支持对虚拟货币“挖矿”活动进行协议检测及封堵，支持对僵尸、肉鸡、垃圾邮件发送者、Tor 节点、失陷主机、暴力破解等风险 IP 的流量进行识别和过滤，支持 C&C IP 和域名两种方式检测，支持 TCP 和 HTTP、DNS 协议、DGA 域名检测；

12、具备独立的入侵防御模块，特征库基于网络实时更新，IPS 特征库在自动升级条件下有 12000 种，支持 Web Server 防护功能，含 CC 攻击防护和外链防护等；

13、具备独立的防病毒模块，病毒特征库 300 万，特征库网络实时更新，支持基于流的病毒过滤，支持压缩病毒文件的扫描，支持压缩文件的解压查杀 5 层；

14、具备流量管理功能，支持两层八级管道嵌套，流量控制维度 2，识别应用数量 5800 个，应用识别库更新频率 4 次/年，可实现流量整形；

15、提供 SaaS 模式的安全运维 APP：通过移动终端可实时获取设备的 CPU、内存、流量等信息，以及应用、用户排名、威胁信息等安全状态，安全可视化实时呈现。APP 不限制使用用户数，

16、免费开放标准 API 接口支持和其它安全设备对接联动。

二、数据中心防火墙　数量：1 台

品牌型号：山石 SG-6000-A5800-CN（软件：网科防火墙 SG-6000-A（万兆）V5.5）

1、功能具备防火墙、应用识别、链路负载均衡、IPV6、VPN 等功能，支持扩展 URL 过滤、垃圾邮件过滤、IPS、AV、僵尸网络防护、云沙箱、威胁情报等功能；

2、硬件参数：1U 标准机架式设备，配备独立的 CON 口 1 个， USB3.0 口 2 个，千兆管理口 1 个，千兆 HA 口 1 个，QSFP+光口 2 个，万兆 SFP+光口 16 个，千兆电口 8 个（bypass 有 2 个），SSD 硬盘 4T；

3、性能参数：吞吐量 80Gbps，最大并发连接数 3000 万，新建会话 100 万；IPsec VPN 吞吐率 45Gbps，配备 IPsec VPN 隧道数 20000；配备 SSL VPN 并发用户数 8 个，支持扩展 10000 个；含三年入侵防御、僵尸网络防御、应用识别特征库、威胁情报升级许可等服务；

4、支持透明网桥旁挂部署模式下的基于 VLAN 标签改写替换功能；

5、支持通过 Ping、TCP、DNS 等方式进行 NAT 探测，支持基于指定源 IP 进行探测，支持对 NAT 转换后的地址是否有效进行探测；

6、支持多虚拟路由器路由划分功能，每个虚拟路由中拥有独立的路由表，支持自定义虚拟系统资源，包括会话数、策略数和 NAT 规则数的设置；

7、支持系统的日志功能记录，并可输出安全网关的各种日志信息，包括事件日志、配置日志、操作日志、网络日志、威胁日志、文件过滤日志、内容过滤日志、上网行为审计日志、流量日志、云沙箱日志和调试信息日志；

8、设备支持手机 APP 巡检，功能包含多设备集中监控 CPU、内存、IP、软件版本；监控整机流量趋势、会话趋势、接口流量趋势；支持应用及用户排名可视化展示；支持实时告警消息推送；支持许可证信息及到期提醒等；

9、支持设备检测到的威胁行为，跳转至威胁情报平台查询与溯源，云端服务提供对 IoC 威胁类型、多源情报等多维度的溯源分析；

10、支持策略助手功能生成细粒度安全策略，可精细到服务端口；

11、通过监控 C&C 连接可发现内网肉鸡，支持阻断僵尸网络、勒索软件等威胁，支持 C&C IP 和域名两种方式检测，支持 TCP、HTTP、DNS 协议检测和 DGA 域名检测；

12、支持攻击检测和防御特征数量 17000 种，支持特征库网络实时更新，支持 Web Server 防护功能，含 CC 攻击防护和外链防护等；

13、免费开放标准 API 接口支持和其它安全设备对接联动。

三、威胁检测探针　数量：1 台

品牌型号：山石 BDS-I5835-ThreatSensor-AD-4T-CN（软件：网科 APT 监测平台(智能内网威胁感知系统)BDS/V5.5）

1、标准机架式设备，内存 64G，千兆电口 8 个，万兆光口 16 个，40GE 光口 2 个，独立 CON 口 1 个，USB3.0 口 2 个，千兆管理口 2 个，SSD 容量 4T，双冗余电源和双冗余风扇；

2、应用层数据处理性能 10Gbps，流量会话数处理量 800 万，每秒流量会话处理量 90 万。含三年威胁检测特征库升级服务(包括入侵检测、防病毒、僵尸网络防御、威胁情报等)；

3、支持旁路部署，支持对网络镜像流量的采集和分析，能够发送威胁和全网流量日志信息至主流态势感知平台，免费提供系统对接服务；

4、支持看板实时展示，呈现网络威胁攻击路径，通过不同标识区分服务器/终端的风险程度，支持条件过滤，可通过可视化手段分析并呈现高风险 APT 的攻击过程；

5、支持根据资产类型、威胁行为等条件自定义威胁范围，对范围内的威胁自动进行相

关威胁响应操作，包括防火墙联动处理、界面告警、邮件告警等；

6、提供特征攻击检测 35000 种，特征库支持网络实时更新，支持基于流的病毒检测；支持压缩病毒文件的扫描；病毒特征库 1500 万种，病毒库支持网络实时更新；

7、支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等协议和应用的攻击检测；支持缓冲区溢出、SQL 注入、CC 攻击、外链攻击和跨站脚本攻击的检测；支持自定义应用层攻击特征，提供预定义检测配置模板；

8、对于存在威胁情报信息的 IP、MD5、URL 和 domain 可跳转到威胁情报中心进行详细信息查看；

9、云端威胁情报库实时推送威胁信息至设备，可以弹窗形式显示；

10、支持对勒索、挖矿、木马、永恒之蓝、WannaCry 和 MIRAI 等关键威胁事件进行标签标记，对发生次数进行统计分析；支持将分析到的 WEBSHELL 攻击、木马回连和恶意攻击行为同步到防火墙，实现深度威胁分析与防火墙联动阻断；

11、支持基于高级威胁行为集的未知威胁检测，高级恶意软件家族的检测 2000 种，包含 Virus、Worm、Trojan、Over ow 等类型；Advance Malware Family 特征库支持网络实时更新；支持 HTTP 扫描、Spider、SPAM、SSH/FTP 弱口令等异常行为检测；

12、PC 及移动端应用程序识别种类 3000 种，可识别 IM、P2P 下载、文件传输、邮件、在线游戏、股票软件、流媒体、非法信道等应用；

13、兼容性：提供所投标产品与主流态势感知平台的兼容性证明材料，免费开放标准 API 接口和定制开发功能，并承诺免费对接服务；

14、产品已经过国家计算机病毒应急处理中心检验。

四、WEB 应用防火墙　数量：1 台

品牌型号：奇安信 W9000-U045M（软件：网神 SecWAF3600Web 应用防火墙系统 SecWAF（万兆）V4.0）

1、标准 2U 机箱，有液晶面板，硬盘 1TB，扩展插槽 2 个，冗余电源，千兆自适应电口 8 个，千兆 SFP 插槽 8 个，bypass4 组，Console 口 1 个，USB 口 2 个，Web 安全保护站点 256 个，含 3 年硬件维保和特征库升级服务；

2、网络吞吐量 8Gbps，应用层处理能力 3Gbps，网络并发连接数 300 万，HTTP 并发 150 万，HTTP 每秒新建连接数 30000 个；

3、在旁路镜像阻断模式下，可配置多组阻断以及镜像口，对检测到的攻击进行旁路阻断，并可指定对端设备 MAC 地址；

4、支持路由牵引部署模式，通过路由牵引、SNT 回注方式对流量进行过滤，支持 IPv4 和 IPv6 双栈流量过滤防护；

5、支持页面一键断网（禁止访问）功能，可实现对网站的快速下线；

6、支持攻击态势实时展示，支持攻击态势 GIS 展示，包含源地址、源地域、目标资产、安全防护攻击类型、攻击趋势、HTTP 并发请求及实时事件的动画统计；

7、具备 SQL 注入、XSS 跨站攻击防御策略，支持特征检测与语义分析算法检测，支持入侵防护功能，并提供入侵防护特征库，入侵检测特征库数量 13000 条；

8、支持检测/清洗 DDOS 攻击，包括 IP 攻击、TCP 攻击、UDP 攻击、ICMP 攻击、DNS 攻击和 HTTP 攻击等，类型数量 20 个；

9、支持防暴力破解功能，可支持频率阈值、动态令牌以及频率阈值+动态令牌等三种暴力破解防护方式；

10、支持虚拟补丁功能，可根据 Appscan 或 SecVSS 扫描器的扫描结果生成 WAF 防护规则，并对漏洞直接防护；

11、支持轻量级蜜罐防御，提供伪后台管理系统页面，记录黑客攻击行为，具有资产探测功能，自动识别资产的系统类型和端口开放信息；

12、支持智能封禁，通过对网站发起的攻击次数、危害级别等维度进行算法分析与识别，对攻击源进行封禁，可自定义封禁时间；

13、支持非法外链检测，针对特定外链进行监控或阻断，支持自定义外链地址；

14、支持日志快速响应功能，具备黑白名单设置功能，支持网页防篡改功能；

15、支持移动终端管理，通过浏览器可查看设备 CPU、内存使用情况，可在移动终端实现对网站资产的断网、下线以及批量下线等应急措施；

五、一卡通防火墙　数量：1 台

品牌型号：奇安信 NSG4000-TG45（软件：网神 SecGate3600 安全网关 NSG（万兆）V3.6.6.0）

1、网络处理能力 20Gbps，并发连接 1000 万，每秒新建连接 13 万，2U 机箱，冗余电源，千兆电口 14 个，千兆光口 10 个，万兆光口 6 个，扩展插槽 2 个，具有液晶屏，提供包含访问控制、地址转换、静态路由、动态路由、策略路由、流量控制、VPN 等功能；

2、产品具备语境关联分析功能；

3、支持 MPLS 流量透传；支持针对 MPLS 流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL 过滤、基于终端状态访问控制等安全防护功能；

4、支持 MTU≥9000byte 的巨型帧处理；

5、支持在源地址转换过程中，对 SNAT 地址池利用率进行监控，利用率超过阈值时，可通过 SNMP Trap、邮件等方式告警；

6、支持 IPv4 和 IPv6 流量的 HTTPS、POP3S、SMTPS、IMAPS 协议进行解密，支持镜像端口偏移，可对解密后的明文流量做镜像时修改端口；

7、支持将其他硬件安全设备作为网元组并进行流量编排；支持将同类型安全设备划归同一网元组，组成硬件安全资源池，并将流量通过负载均衡编排给组内所有网元；

8、支持服务链编排功能，支持串接链和旁路链，支持网元组的方向和位置设置；

9、支持细粒度引流策略，可基于源安全域、目的安全域、源用户、源地址、目的地址、服务、VLAN、服务链、内网到外网/外网到内网的流量方向引流策略，并详细记录日志；

10、具备 IPv6 Enabled Logo 认证；

11、具备中国信息安全测评中心颁发的自主原创产品检测证书。

六、日志审计　数量：1 台

品牌型号：奇安信 LAS-R33M（软件：网神 SecFox 日志收集与分析系统 LAS V5.0）

1、标准 2U 机箱，千兆电口 6 个，扩展插槽 2 个，　Console 接口 1 个，冗余电源，硬盘 8TB，日志源授权 200 个；

2、综合日志处理性能 6000EPS，日志采集处理均值 12000EPS；

3、支持等保大屏展示，展示包含：设备运行天数、日志源数量、原始日志数、关联事件数、告警总数、本地最早日志产生时间、已保存日志天数、平均每天日志存储量、存储空间情况等；

4、能够对各类资源：网络设备、安全设备、安全系统、主机操作系统、虚拟化、云计算、数据库、中间件以及各种应用系统的日志、事件、告警等安全信息进行全面的审计；

5、支持通过 Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent 代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka 等多种方式完成日志的收集，支持日志合并；

6、支持对资产 IP 地址（含内网 IP）的地理信息进行管理，设置单 IP 及 IP 段行政区及经纬度，支持地图显示；

7、支持对资产日志进行过滤，可设置允许和拒绝接收日志，可以日志采集的异常情况进行告警；

8、支持正则表达式、JSON、Key-Value、分隔符等解析方案，支持日志自动化辅助范化；

9、日志解析字段内置字段 150 个，属性字段可扩展，可自定义创建字段，支持关联函数字段类型，所有字段均可参与事件查询、关联分析和报表数据源统计；

10、对匹配的多条范化策略，支持策略优先级的自定义匹配；

11、以图形化的方式展示日志属性之间的聚合关系，并支持手动选择日志属性，显示多维事件分析图；属性可增加或减少，支持分析图大小调整；

12、能够在世界地图上实时定位事件源/目的 IP 地址（内网 IP）的地理位置；

13、支持仪表板导入导出，支持仪表板共享、复制，可将仪表板共享给其他用户，支持对关联规则进行监控，了解该规则命中历史情况；

14、具有国家信息安全测评中心《信息技术产品安全测试证书》EAL3+ 。

七、漏扫系统　数量：1 台

品牌型号：奇安信 S5000-W020(软件：网神 SecVSS3600 漏洞扫描系统 SecVSS V3.0)

1、Web 扫描域名无限制，Web 扫描任务并发数 10 个，系统 IP 地址扫描上限 1024 个，支持扫描 A 类、B 类、C 类地址， IP 地址并行扫描 100 个，1U 机架式，硬盘 4T，千兆自适应电口 6 个，扩展插槽 2 个，配置液晶面板， USB 口 2 个， Console 口 1 个；

2、可检测漏洞数 350000 条，漏洞标准包含 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq 等；

3、支持同时下发系统扫描、Web 扫描、弱口令扫描任务，扫描目标包括 IP、域名、URL 等格式；

4、支持同时导出包含系统扫描、Web 扫描、弱口令扫描等结果的报表，可统一分析网站漏洞、网站所在主机漏洞以及主机弱口令漏洞；

5、支持自动探测指定网段中的 Web 站点，可转为 Web 资产并下发 Web 扫描任务，支持自适应网络扫描，根据网络状况自动控制发包速率；

6、支持三种漏洞验证方式，包含浏览器验证、注入验证、通用验证等验证方式，支持国产操作系统和数据库扫描，支持主流数据库的弱口令检测；

7、支持通过 SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP、WMI、RSH、REXEC、WINRM、SNMP 等协议对目标主机进行登录扫描；

8、支持以树形结构展示网站目录结构，并在网站目录上关联显示相应漏洞，支持已有任务复制，可对复制任务进行再编辑，包括基本信息、策略、目标范围、调度、扫描参数等；

9、支持自定义立即执行、定时扫描、周期性扫描等多种扫描任务执行方式，可针对指定时间、执行对象自动执行扫描任务，并自动生成报告，时间可具体到某月、某天、某时、某分；

10、支持目前主流协议的弱口令检测，包括且不限于 TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、Tomcat 等；

11、可对资产历史扫描结果变化趋势进行分析与展示，支持两次扫描结果的对比查看；

12、支持自动导出报表或扫描任务结束后自动发送报表到指定邮箱，报表格式包括但不限于 HTML、PDF、XML、Excel 和 Word 等；

13、支持扫描任务完成后发送告警，告警方式包含邮件告警、短信告警、SNMPtrap 告警、SYSLOG 告警、FTP 告警等；

八、上网行为管理　数量：1台

品牌型号：奇安信 NBM7370(软件：网神上网行为管理系统 NBM V7.0)

1、满配网络带宽支撑 10G，标准机架式 2U 设备，交流冗余电源，最大并发连接数 500 万，最大新建连接数 25 万/秒，千兆电口 4 个，千兆光口 4 个，SFP+万兆接口 4 个，管理网口 1 个，HA 口 1 个，硬盘容量 2T，支持外置日志存储，扩展槽 5 个；

2、设备具备硬件 bypass 按钮；

3、可实现对主流认证计费系统的单点登录联动；

4、内置有效 URL 数据 3000 万条，支持根据 URL 库及 URL 关键字进行网址访问管理，具备阻断、记录、告警等功能；支持阻塞页面的自定义跳转，阻塞页面内容可自定义；

5、支持用户异常行为分析识别分类，提供包含但不限于校园网内部暴力/色情异常兴趣分析识别、网络舆情分析识别、异常网贷风险分析识别、游戏沉迷分析识别、校园一卡通消费异常分析识别、各类视频沉迷分析识别、图书馆资源下载异常分析识别等功能，并提供可视化展示；

6、应用协议库 10000 种，应用规则 70000 种，设备可展示特征库规模详情；

7、支持拦截违规 VPN 行为和违规代理软件，识别种类 100 种，

8、提供 DNS 审计策略，可对 DNS 通信内容进行审计和控制；

9、可识别网络中的私接路由和共享 wifi 的网络行为，并能配置阻塞策略，可配置禁用 PC 热点开启功能；

10、可配置多条共享接入策略，策略基于源 IP、用户、位置、终端台数、PC 台数、移动台数、阻塞时间和动作等多种条件；

11、基于对接云端大数据安全平台，提供云安全防护和业务安全防护功能，包含但不限于杀毒、恶意 URL、失陷主机检测、云沙箱、入侵检测服务等；

12、可识别内网爬虫行为，并可监控爬虫用户数趋势和爬虫请求数趋势；可查询爬虫行为详情，支持配置源/目的 IP 和域名白名单；

13、支持对接威胁情报大数据平台，可识别、封堵失陷主机并记录日志；

14、支持拦截内网对外部威胁 IP 的访问请求，支持阻塞失陷主机 IP，阻塞后可向用户推送威胁情报阻塞提示页面；

15、可实现 SSL/SSH 协议的流量解密，能指定的源/目的 IP 或 IP 段；

九、流量复制器　数量：1台

品牌型号：盛邦下一代流量复制汇聚平台 RayNGTAP-8000-Q0024E

1、万兆/千兆自适应光口 20 个；管理电口 1 个；Console 口 1 个；冗余电源；满配整机吞吐量 240Gbps；

2、支持基于端口输入\输出双向的流量复制；

3、支持基于流量分类规则的复制，支持 1 路到多路复制，支持多路到 1 路汇聚；

4、支持基于指定输出接口转发；

5、支持基于流分类结果转发；

6、支持大负载的环境下输出的报文流保序；

7、支持对 INGRESS 端口流量基于五元组的规则进行过滤，可根据规则过滤出的流量进行复制；

8、支持 IP 网段进行过滤，并将过滤后的流量进行复制；

9、透明支持 802.1Q/Q-IN-Q、IPX/SPX、MPLS、PPPOE、ISL、GRE、PPTP 等各类协议封装；

10、支持用户通过配置对带有 VLAN 标签的报文进行丢弃；

11、支持 CLI、SNMP、WEB 管理，提供配置界面，可完成所有配置管理；

十、智能 IP 统一管理平台系统　数量：1 台

品牌型号：木云 MYIP-2200PLUS(软件：木云智能 IP 统一管理平台系统 V3.2)

1、软硬件一体化设计，2U 机架，千兆电接口 6 个，千兆光口 4 个，LPS 为 1500 个，内置存储空间 2T，冗余电源，系统具备功能模块包括但不限于 DHCP、IPAM、告警通知、端口聚合、网络工具、用户角色管理、服务集群管理、操作日志等；

2、可对 IPv4 和 IPv6 地址进行集中分配管理，IPv6 支持 MAC 和 DUID 的地址绑定，IPv6 地址分配方式包括但不限于基于起始地址、前缀、以及地址段和前缀结合等方式；

3、支持地址池、固定地址和保留地址设置，支持设置某个 IP、IP 地址段为保留或分配状态，支持二次地址分配；

4、支持基于 MAC、数字指纹以及 Option 数据的接入控制，支持发现网络终端设备指纹标识、终端厂家标识等，可禁止非法路由器接入；

5、支持 DHCP DECLINE 报文的地址冲突处理，包括但不限于 IP 地址冲突检测、冲突地址隔离、隔离冲突地址定期回收功能和拒绝分配 IP 记录以及原因描述查询；

6、以当前流程镜像数据作为基线，支持 IP 基线数据对比分析及告警；

7、支持终端远程管理，管理方式包括但不限于 SSH、Telnet、RDP、VNC 等；

8、免费开放标准 API 接口支持与主流虚拟化或超融合平台对接，为计算资源池自动分配 IP 资源；

9、支持 DHCP Failover 双备，可指定 DHCPv4 与 DHCPv6 服务的故障切换，支持负载均衡和热备两种模式；

10、提供超级管理员管理权限，对设备进行“写”操作时需特权模式完成，支持回收站功能包括但不限于恢复被删除的 IP 地址管理、地址池管理、控制策略、固定地址管理、IPv6 前缀委派、动态租约和 DHCP 集群等；

11、支持远程协助功能，远程技术无需在出口网关上对互联网开放管理端口；

12、支持 IAM 基础服务控制台集中管理，支持与资源统一管理平台、智能 DNS 系统进行集中用户与权限管理和操作，支持 OIDC 授权服务器，使用 ID Token 数据结构进行用户身份校验；

13、实时展现设备访问的并发数据，展示方式包括但不限于饼图、柱状图等，展示内容包括但不限于 QPS、Top 域名、Top IP 、解析记录统计等，分析数据支持在系统首页集中展示，支持全面详尽的 DHCP 日志包括但不限于 DHCP 日志、DHCP 运行日志等，展示的字段包括但不限于 IP 地址、MAC 地址、类型、Request 源地址等；

十一、智能 DNS 系统　数量：1 台

品牌型号：木云 MYD-3500（软件：木云智能 DNS 系统 V2.0）

1、采用软硬件一体式设计，2U 机架，千兆电口 6 个，千兆光口 4 个，万兆接口 2 个，QPS220000 个，内置存储空间 2T，冗余电源，功能模块包括但不限于权威域管理、递归域管理、DNS 防火墙、告警通知、网络工具、用户角色管理、服务集群管理、操作日志、DNS 日志等；

2、内置 ISP 运营商以及各省市精确 IP 地址库，IP 地址库维护支持手动维护和自动更新；

3、支持 DNS 转发，转发功能包括但不限于全局转发、基于线路的转发、基于域名的转发等，可设置多个转发服务器，支持定时转发策略的关停与开启；支持纯 IPv6、纯 IPv4 及 IPv6/IPv4 双栈解析；

4、支持双栈模式下 IPv4 记录和 IPv6 记录过滤功能，支持指定递归域名的 AAAA 解析内容过滤；

5、支持与主流安全设备联动实现对“挖矿”域名进行实时拦截，提供威胁域名数据库的 API 接口文档；

6、支持与资源访问控制系统联动，访问控制系统与 DNS 系统的域名资源同步；提供联动 API 接口说明文档及免费接口对接，并承诺免费对接服务；

7、配置 DNS 防火墙模块，内置病毒、木马、挖矿、网络钓鱼以及广告等恶意域名数据库，域名库数量 50 万条，可对恶意域名进行批量拦截；

8、支持与上级监管平台提供的域名数据库联动，实现自动更新和拦截；

9、支持特权模式设定，可对写权限操作进行管理，支持回收站功能，可恢复被删除的集群、域、线路、记录等信息。

10、支持远程协助功能，远程技术无需在出口网关上对互联网开放管理端口；

11、支持 IAM 基础服务控制台集中管理，支持与资源访问控制系统、智能 IP 统一管理平台系统进行集中用户与权限管理和操作，无需在管理使用时登录单个产品管理端。支持 OIDC 授权服务器，使用 ID Token 数据结构进行用户身份校验；

12、支持 DNS 防火墙安全日志分析，支持非法域名类型的安全事件报表分析、支持根据时间段、请求方、威胁类型查询统计，支持 DNS 查询趋势、威胁分类及 TOP 威胁域名排行及导出功能。

13、为保障产品质量，通过高新技术企业认证；

十二、服务器安全防护系统　数量：1 套

品牌型号：奇安信 USS-AES-CPU-FL-STE-PS（软件：网神云锁服务器安全管理系统 V8.0）

1、支持 windows/linux 主流操作系统，包括但不限于 Windows Server、CentOS、RHEL、Ubuntu、麒麟、统信、欧拉等；

2、具有自身安全保护措施，防止被非授权用户强行卸载、删除或修改，支持各功能组件间通过网络传输的数据进行保护，防止被非法授权获取；

3、支持服务器资产的自定义采集，支持自动采集和任务采集等采集方式，支持设置不同类型资产不同频率和不同服务器范围的采集；

4、产品杀毒引擎数量 4 种，其中自研杀毒引擎 1 种；

5、支持对多层压缩包文件的查杀，最大查杀压缩包文件 100MB，可自定义配置压缩包的层数 10 层，压缩包提取文件数量 9000 个；

6、支持通过扫描任务方式检测服务器存在的漏洞，支持检测的漏洞数量 4000 个，支持设置扫描任务的定时计划，支持按照每天、每周、每月来计划扫描任务；

7、支持对 Windows 服务器漏洞进行补丁修复安装，支持对漏洞的快速验证，以检验漏洞是否成功修复；

8、支持基线检查能力，可自定义基线规则，支持从服务器维度和检查项维度查看两次基线检查结果的对比分析；

9、支持通过扫描任务的方式检测目录中存在的恶意 Webshell；

10、支持入侵检测功能，包括恶意扫描防护、异常登录防护、反弹 Shell 监测、无文件攻击检测、RCE 利用检测和本地提权检测等功能；

11、提供 300 点服务器安全防护使用授权，提供一年软件更新和全库更新服务。

十三、终端安全防护系统　数量：1 套

品牌型号：奇安信 ESM-MGR（软件：天擎终端安全管理系统 V10.0）

1、支持单机部署和集群部署，管理中心操作系统支持 Windows Server；

2、支持管理员预先设置好灰度发布批次和漏洞修复策略，支持自动分组，按 IP 地址、CPU 数量、内存容量、主机名、计算机工作组等参数动态调整分组；

3、支持对客户端主程序、病毒库版本按分组和多批次进行更新，支持设置不同终端类型设置和每批次观察时长；

4、支持不同分组的客户端切换功能模式，支持按照病毒类型设置告警规则，支持三个杀毒引擎混合使用，提高病毒检出率；

5、支持手动扫描和清理软件安装残留文件以及系统历史记录文件，支持检测系统启动项、服务项、计划任务和启动项的优化；

6、支持查杀未处理，一键处理指定终端上存在的被用户忽略的病毒，且不需要再次扫描，支持添加扫描文件类型，可自定义时间段完成全盘扫描；

7、支持主动防御分析，可提供主动防御细分类型的防御趋势分析，支持对压缩包内的病毒扫描，支持多层压缩包的扫描；

8、支持进程防护、注册表防护、驱动防护、U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护、勒索软件防护等防护；

9、支持按照补丁的维度统计补丁安装情况，包括补丁号、系统类型、补丁类型、补丁级别、补丁名称、补丁描述等信息；

10、支持主机防火墙功能，支持添加 IP、域名规则，支持允许/拒绝规则，支持任意流向拦截和允许；

11、提供一年场地授权。

十四、运维安全审计系统　数量：1 套

品牌型号：飞致云 JumpServer 运维安全审计系统 V3

1、被管资源数 500 个，无用户数、并发数限制；

2、采用 B/S 架构部署，通过 HTTPS 方式远程安全管理，支持的主流浏览器包括但不限于 IE（IE11 以上）、Edge、Chrome、Firefox、Safari 等，可通过浏览器访问托管资源，访问方式包括但不限于 SSH、RDP、Telnet、VNC 等；

3、支持主流数据库访问，数据库类型包括但不限于 SQL Server、MariaDB、MySQL、Oracle、PostgresSQL 等，支持本地客户端访问，支持通过 WEB GUI 的方式对数据库进行可视化操作，支持导入 SQL 文件和导出查询数据集（含 CSV、XLSX 等格式），支持对数据库命令进行复核，通过 CLI 和 Web CLI 方式连接数据库；

4、支持基于角色的细粒度权限访问控制，包括但不限于查看、创建、更新、删除资产等权限；

5、支持 RDP 客户端连接，支持 RDP 复制粘贴功能，对 Windows 资产可以实现文件或文件内容的复制粘贴，支持通过 XRDP 连接远程应用时的复制粘贴、上传下载、磁盘挂载等权限控制，支持禁止 RDP 会话使用系统剪切板功能；

6、支持对接混合云场景下的主流平台，包括但不限于 vmware 虚拟化、Fusion Compute、华为私有云、深信服、阿里云等，实现资产定时同步；

7、支持以 Excel 等文件方式批量导入、导出用户信息、关联角色和组织架构，支持从 LDAP 域导入用户、用户组并能自动同步；

8、支持 Windows Server、国产等操作系统作为远程应用发布机，支持管理远程应用和一键部署远程应用发布机，提供应用安全下载源，可下载的应用包括但不限于达梦、SSMS、PL\SQL Developer、Studio 3T、IBM DB2、Hive、Spark 等客户端；

9、支持对 Windows、Linux/Unix 及数据库的运维操作进行审计录像；支持 Windows 键盘操作记录、Linux/Unix 命令、数据库 SQL 语句进行命令记录，支持开启会话背景水印；

10、支持按部门或项目等架构进行组织管理，支持多组织管理，每个组织间用户、资产、授权逻辑隔离；

11、考虑网络安全、系统后续扩展和未来系统集成，免费开放系统接口源码和 API 操作文档；

12、产品已通过网络安全专用产品安全检测及 IT 产品信息安全认证。

十五、综合布线　数量：1 项

品牌型号：紫光定制

1、辅材包含所需 RJ45 水晶头、RJ45 压线钳、PVC 线材、线槽、电源线、插座、接头、线架等配件及机房内综合布线所需的网线、电源线、线槽等所需材料、配件等，所有辅材均符合国标；

2、免费提供 90 天的驻场服务，驻场事宜由双方协商决定。