中国华能集团有限公司

漫湾电厂生产网络安全防护优化建设标准询价采购文件

采购编号：MWDC2022/U32

采　　购　　人：华能澜沧江水电股份有限公司漫湾水电厂

日　　期：2022 年 9 月

目 录

第一章 采购公告（合格供应商公开）

漫湾电厂生产网络安全防护优化建设询价公告

一、项目介绍

1. 项目概况：漫湾电厂严格按照“安全分区、网络专用、横向隔离、纵向认证”方针建设电厂生产网络，安全Ⅰ区主要承载计算机监控系统业务；安全Ⅱ区承载继电保护信息系统业务、电能量计量业务、行波测距业务等业务；安全Ⅲ区主要分集控综合数据网、调度综合数据网及电厂生产管理信息大区，集控综合数据网主要承载工业电视系统、视频会商系统、调度 OMS 系统业务；调度综合数据网主要承载调度 OMS 系统，视频会商系统，辅助服务考核系统业务；电厂生产管理信息大区主要分全厂应用系统、厂房应用系统及工业互联网系统，其中全厂应用系统包括电能量发布系统、移动报警系统、综合信息报表系统及可靠性系统业务，厂房应用系统为独立系统，与其他系统没有物理连接，包括 SF6、避雷器、变压器等在线监测系统，环境监测系统，照明、风机辅助集中监控系统业务；工业互联网系统包括 KDM 服务器，且与安全Ⅱ区采用横向隔离装置进行物理隔离，与电厂办公信息系统区之间采用防火墙进行隔离。漫湾电厂调度数据网及 2M 专线于 2020 年 11 月改造完成，漫湾电厂新建调度综合数据网，相关调度综合业务不再由集控转接。安全Ⅰ区与安全Ⅱ区采用横向防火墙进行逻辑隔离，安全Ⅱ区与安全Ⅲ区内管理信息大区采用横向隔离装置进行物理隔离，安全Ⅲ区内集控综合数据网及调度综合数据网独立运行，与安全Ⅰ区、安全Ⅱ区及生产管理信息大区无物理链路连接。

根据《华能澜沧江水电股份有限公司电力监控系统网络规划优化建设方案》，漫湾电厂安全Ⅰ、Ⅱ、Ⅲ区不满足建设方案中的相关要求，需开展安全Ⅰ、Ⅱ、Ⅲ区合规性建设、提升性建设、功能性建设相关工作，以弥补网络安全防护存在的短板，提升电厂生产网络安全防护水平。

2. 交货/施工/服务地点： 云南省临沧市云县漫湾水电厂 。

3. 采购内容： 按照《华能澜沧江水电股份有限公司电力监控系统网络规划优化建设方案》开展以下工作：（1）合规性建设，在安全Ⅰ区部署入侵检测系统，在安全Ⅱ区、Ⅲ区部署入侵防御装置；安全Ⅰ、Ⅱ、Ⅲ区各主机部署防病毒系统（含 50 套防病毒软件及 3 套防病毒管理系统），防病毒网关。部署一台漏洞扫描装置，满足各系统日常定期漏洞扫描。（2）提升性建设，在安全Ⅰ区部署高级可持续威胁预警系统（APT）、

流量分析系统、“蜜罐”系统；在安全Ⅱ区部署高级可持续威胁预警系统（APT）、“蜜罐”系统、流量分析系统；安全Ⅲ区部署高级可持续威胁预警系统（APT）、流量分析系统、“蜜罐”系统。（3）功能性建设，在安全Ⅰ区监控系统部署符合国密要求的运维堡垒机；在安全Ⅱ区、Ⅲ区各部署运维堡垒机及日志审计；在安全Ⅰ区安全Ⅱ区、Ⅲ区各部署安防管理工作站。（4）主机加固，对安全Ⅰ区计算机监控系统工程师站、操作员站服务器进行加固，对安全Ⅱ、Ⅲ区相关业务服务器进行主机加固，加固台数30台。（5）对现有部署于安全Ⅰ区监控系统1台日志审计系统进行配置优化。

4. 施工期：自合同签订之日起至2022年10月15日。

5. 其他需要说明内容：/。

二、报价须知

1. 供应商通用资格要求：

（1）供应商须为华能集团供应商库内合格供应商，且未处于暂停参加采购活动的处罚期限内，满足供应商参与业务的权限。

（2）近三年没有严重违约，没有经鉴定部门认定的因其产品/服务/工程引起的重大及以上质量事故或重大及以上安全事故；

（3）未被市场监督管理部门在全国企业信用信息公示系统中列入经营异常名录或者严重违法企业名单；

（4）未被最高人民法院在“信用中国”网站（www.creditchina.gov.cn）或各级信用信息共享平台中列入失信被执行人名单；

（5）不存在不同供应商的响应文件的互联网协议地址（IP地址）信息检查一致的情况。

（6）与采购人存在利害关系可能影响采购公正性的法人、其他组织或者个人，不得参加询价；单位负责人为同一人或者存在控股、管理关系的不同单位，不得参加同一询价项目。

（7）不存在违反国家相关法规和华能集团相关制度的情况。

2. 供应商专用资格要求：

2.1 主要设备制造商资质等级要求：

（1）主要设备制造商需为国家信息安全漏洞库一级技术支撑单位成员；

（2）主要设备制造商需具备中国网络安全审查技术与认证中心信息颁发的信息安全风险评估服务资质认证证书（一级）；

（3）主要设备制造商需具备中国网络安全审查技术与认证中心信息颁发的信息安

全应急处理服务资质认证证书（一级）；

（4）主要设备制造商未受到上级监管单位（南方电网公司）市场禁入处罚。

2.2 报价人资质要求：

（1）报价人需具备国家信息安全测评信息安全服务资质证书（安全工程类一级及以上）；

（2）报价人需具备 ITSS 信息技术服务运行维护标准符合性证书（三级及以上）；

（3）报价人需具备 ISO27001 信息安全管理体系认证证书；

（4）报价人所投产品需为中国企业自主研发及自主知识产权的国产品牌。

（5）报价人所投的所有产品必须是原厂正品，所投的非主要系统/设备除交换机、工作站外需提供原厂服务承诺书。

2.3 业绩要求：

（1）主要设备制造商报价的，主要设备制造商必须具备类似项目工程经验，近三年内（2019 年 1 月 1 日至今，以合同签订之日为准）独立承担并完成合同金额 200 万以上网络安全项目工程实施业绩（非物资采购类项目）不少于 2 个（如报价人使用多个主要制造商产品，需按要求提供多个业绩，例：如报价人使用 3 个主要设备制造商则需提供不少于 6 个业绩）；提供业绩合同复印件（至少包含合同签订时间、项目规模、签署等关键页内容，如合同为集成商签订需体现制造商产品内容）或可查询的制造商安全设备的中标公示。

（2）集成商报价的，报价人必须具备类似项目工程经验，近三年内（2019 年 1 月 1 日至今，以合同签订之日为准）独立承担并完成合同金额 200 万以上的网络安全项目工程实施业绩（非物资采购类项目）不少于 2 个；主要设备制造商近三年内（2019 年 1 月 1 日至今，以合同签订之日为准）独立承担并完成合同金额 200 万以上网络安全项目工程实施业绩（非物资采购类项目）不少于 2 个（如报价人使用多个主要制造商产品，需按要求提供多个业绩，例：如报价人使用 3 个主要设备制造商则需提供不少于 6 个业绩），提供业绩合同复印件（至少包含合同签订时间、项目规模、签署等关键页内容，如合同为集成商签订需体现制造商产品内容）或可查询的制造商安全设备的中标公示。

2.4 其他要求：

（1）设备需使用同一制造商产品；

（2）本项目要求主要设备制造商负责工程实施，允许代理商（集成商）报价，代理商（集成商）报价的必须提供主要设备制造商针对此项目的唯一授权证明文件。

2.5 本工程不接受联合体报价。

三、基本信息

采购方案名称	漫湾电厂生产网络安全防护优化建设	采购单位	华能澜沧江水电股份有限公司漫湾水电厂
采购项目类型	工程	采购项目类别	信息化
工程项目编号		工程项目名称	漫湾电厂生产网络安全防护优化建设
寻源类型	询价	寻源方式	合格供应商公开
评价原则	经评审的最低价法	是否紧急采购	

四、报价要求

结算币种	人民币	报价截止前是否允许供应商修改报价	允许
是否缴纳保证金	/	保证金金额（元）	/
报价开始时间	以电商平台公布为准	报价截止时间	以电商平台公布为准
答疑 / 澄清时间	以电商平台公布为准		

五、采购需求信息

详见采购文件**第五章-采购需求**

六、联系人信息

联系人（采购人）	张先生	询价单位	华能澜沧江水电股份有限公司漫湾水电厂
联系电话	0883-3813446	传真	0883-3813446
邮编	675805	Email	mwdccgb@126.com
手机	18208759356	联系地址	云南省临沧市云县漫湾镇

七、附件

只接受供应商通过电子商务平台线上对需要澄清的内容提出问询。

第二章 供应商须知及前附表

供应商须知前附表

条款号	条款名称	编列内容
2.1	采购人及联系方式	采 购 人：华能澜沧江水电股份有限公司（漫湾水电厂） 地　　址：云南省临沧市云县漫湾镇 邮　　编：675805 电　　话：0883-3813446 电子邮箱：mwdccgb@126.com 联 系 人：张先生
2.4	采购代理机构及联系方式（如有）	
4.1	踏勘现场	■不组织 □组织，踏勘时间：_____ 踏勘集中地点：_____
6.1	采购文件的澄清、修改、补充	供应商需在华能电子商务平台显示的澄清截止时间24小时前在华能电子商务平台提出澄清问题。 对采购文件进行的澄清、修改、补充距报价截止时间不足24小时的，将相应延长报价截止时间。
9.6	最高限价	■无 □有，最高限价：_____
9.7	采购代理服务费	■无 □有，服务费收取标准： 取费按类型（工程、货物或服务）、分标段（包）参照《招标代理服务收费管理暂行办法》（计价格〔2002〕1980号）中规定的计费原则标准计取。
9.8	供应商报价的其他要求	采购人指定的增值税税种： ■提供增值税专用发票； □提供增值税普通发票； □不限制。
10	报价货币	■人民币 □其他：_____
11.1	响应保证金	■无 □有，按照以下方式：_____ 响应保证金的金额：_____ 响应保证金的形式：_____ 响应保证金的递交截止时间为：华能电子商务平台采购公告中显示的报价截止时间。 开户银行及账号如下： 账户名称：_____ 开户银行：_____ 账　　号：_____
12.1	采购有效期	自响应文件递交截止时间起 90 个日历日（注：原则上不少于90日

		历日，最长不超过 180 日历日）
13	响应文件递交截止时间及地点	响应文件递交截止时间：以华能电子商务平台显示的递交截止时间为准 响应文件递交地址：华能电子商务平台（http://ec.chng.com.cn/）
16	开启响应文件	开启响应文件时间：同响应文件递交截止时间
18	成交供应商的推荐原则	■一个采购项目，只能推荐一个成交供应商。 □一个采购项目，按照物料行，可以推荐多个成交供应商。
21.3	履约担保	■不提供 □提供，履约担保金额：_____ 履约担保形式：_____
22	其他需要补充的内容	不接受联合体报价

备注：供应商须知前附表是对供应商须知的具体补充和修改，如有矛盾，应以本表为准。

1. 适用范围

本采购文件仅适用于本项目公告/邀请函中所述项目。

2. 定义

2.1 采购人：指依法提出采购项目进行采购的法人或其他组织，采购人及联系方式见前附表。

2.2 供应商：指响应询价采购，参与询价竞争的法人或其他组织。

2.3 成交供应商：指最终被授予合同的供应商。

2.4 采购代理机构：依法设立并提供采购代理服务的专业组织，采购代理机构及联系方式见前附表。

3. 询价费用

供应商应承担与其参加询价有关的所有费用。不论询价过程和结果如何，供应商应自行承担所有与参加询价有关的费用，采购人在任何情况下均无义务和责任承担这些费用。

4. 现场踏勘

4.1 供应商须知前附表规定组织踏勘现场的，采购人按供应商须知前附表规定的时间、地点组织供应商踏勘项目现场。

4.2 供应商自行负责在踏勘现场中所发生的人员伤亡和财产损失。

4.3 采购人在踏勘现场中介绍的项目场地和相关的周边环境情况，仅供应商在编制响应文件时参考，采购人不对供应商据此作出的判断和决策负责。

5. 采购文件的构成

5.1 采购文件由下列文件以及在询价过程中发出的修正和补充文件组成：

第一章 采购公告/采购邀请函

第二章 供应商须知及前附表

第三章 评审办法

第四章 合同条款及格式

第五章 采购需求

第六章 响应文件格式

5.2 供应商下载采购文件过程中，如发现下载不成功或下载的文件格式有误等问题请务必于采购文件发售期内联系电子商务平台客服热线。如果供应商不按上述要求提出而造成不良后果，电子商务平台不承担责任。

5.3 供应商应认真阅读采购文件中所有的事项、格式、条款和要求等。供应商没有按照采购文件要求提交全部资料，或者响应文件没有对采购文件在各方面都做出实质性响应，可能导致其报价被拒绝。

5.4 响应文件一经递交成功即表示供应商确认采购文件的法律效力，并对此采购文件提出的要求做出相应的响应，承担与采购文件要求相适应的民事、经济和法律责任。

5.5 由于供应商对采购文件的误解与疏忽或报价误差，而导致询价失败或成交后的任何风险，其责任均由供应商自负。

6. 采购文件的澄清、修改、补充

6.1 任何要求对采购文件进行澄清的供应商，均应在供应商须知前附表规定的时间提出澄清问题。

6.2 在询价报价截止时间前的任何时候，无论出于何种原因，采购人/采购代理机构可主动地对采购文件进行修改、补充，原则上采购人应在收到澄清请求 24 小时内，在电子商务平台上给予书面答复。采购文件的澄清、修改、补充均作为采购文件的组成部分，对供应商具有约束力。采购文件的澄清、修改、补充将**以书面形式**通知供应商。供应商应在收到通知后进行确认。如果供应商不予确认，引起的后果由供应商自行承担。

6.3 为使供应商有充分时间对采购文件的修改部分进行研究。采购人/采购代理机构对采购文件进行澄清、修改、补充距报价截止时间不足 24 小时的，应将报价截止时间延长至本次澄清答复、修改、补充时间点后的 24 小时，并**以书面形式**通知所有购买采购文件的供应商。

7. 编制基本要求

7.1 供应商应在认真阅读，充分理解本采购文件所有内容（包括所有的澄清、修改、补充内容）的基础上，按照“第六章响应文件格式”的要求编制完整的响应文件。

7.2 供应商必须保证响应文件所提供的全部资料真实可信，并接受采购人对其中任何资料在合同最终授予前进一步审查的要求，如若存在供应商利用弄虚作假等不当手段谋取成交的，一经查实，采购人有权予以否决，并保留进一步追究其责任的权利。

7.3 如果响应文件填报的内容不详，或没有提供采购文件中所要求的全部资料及数据，给评审造成困难，责任由供应商自行承担。

7.4 如供应商没有对本采购文件的要求提出偏离，采购人可认为供应商完全接受和同意本采购文件的要求。响应文件对采购文件未提出偏离条款的，均被视为接受和同意。响应文件与采购文件有偏离之处，无论多么微小，均应按采购文件格式要求统一汇总说明。

8. 语言和计量单位

8.1 响应文件及供应商与采购人之间的凡与采购有关的来往信函和文件均使用中文，若其中有其它语言的书面材料，则应附有中文译文，并以中文译文为准。

8.2 除非采购文件中另有规定，计量单位均采用中华人民共和国法定的计量单位。

9. 报价

9.1 供应商应按照采购文件规定的内容、责任范围以及技术要求条件进行报价。并按报价部分规定的格式报出分项价格和总价。

9.2 供应商报价应包括供应商成交后为完成采购文件约定的全部工作需支付的一切费用和拟获得的利润，并考虑了应承担的风险。

9.3 供应商必须根据采购文件报价格式进行报价，若供应商提供免费服务，应在响应文件中说明或在报价表中填“免费”，否则视为已包含在总报价中。

9.4 供应商不得以低于成本报价。

9.5 响应文件中标明的最终报价在合同执行过程中是固定不变的，不得以任何理由予以变更。

9.6 采购人设有最高限价的，供应商的报价不得超过最高限价，如超过最高限价，将予以否决，最高限价在供应商须知前附表中载明。

9.7 采购代理服务费按照供应商须知前附表规定收取的，采购代理服务费由供应商计入报价，但不单独列项，成交供应商须一次性向采购代理机构支付采购代理服务费。

9.8 供应商报价的其他要求见供应商须知前附表。

10. 报价货币

采用人民币报价，供应商须知前附表有明确规定的除外。

11. 响应保证金

11.1 应提交供应商须知前附表中规定数额和形式的响应保证金，作为其响应文件的一部分，响应保证金的有效期应满足采购有效期的要求。

11.2 任何未按第 11.1 款规定提交响应保证金的，将被视为非实质性响应采购文件

而予以拒绝。

11.3 发生下列情况之一，响应保证金可不予退还：

（1）供应商在采购有效期内撤回其响应文件；

（2）供应商被通知成交后，拒绝签订合同（即不按成交时规定的技术服务方案、价格等签订合同）或没有按照要求提交履约担保。

11.4 响应保证金的退还

成交供应商与采购人签订合同后 5 日内，采购人/采购代理单位向成交供应商退还扣除代理服务费后的剩余保证金，同时退还未成交供应商响应保证金。

12. 采购有效期

12.1 采购有效期自本采购文件规定的响应文件递交截止时间起生效，并在供应商须知前附表中规定采购有效期内保持有效。采购有效期短于这个规定期限的响应文件将被视为非实质性响应而予以拒绝。

12.2 采购人可于采购有效期截止之前要求供应商同意延长有效期。供应商应在规定的时间内以书面答复表示同意，并相应延长响应保证金有效期，此时供应商不能对响应文件进行任何修改；供应商若不同意延长采购有效期，则应在规定的时间内以书面形式给予明确答复，此时供应商被视为自动退出本次采购活动，响应保证金予以全额退还。在这种情况下，本须知中有关退还和不予退还响应保证金的规定将在延长后的采购有效期内继续有效。

13. 响应文件递交截止时间及地点

13.1 供应商应在供应商须知前附表中规定的响应文件递交截止时间前将响应文件成功上传至电子商务平台，则视为响应文件已递交。

13.2 采购人将拒绝接受供应商须知前附表规定的响应文件递交截止时间后上传响应文件至电子商务平台。

14. 响应文件的修改和撤销

14.1 供应商在递交响应文件后，可以在规定的响应文件递交截止时间之前修改或撤回其响应文件。

14.2 供应商不得在采购有效期内撤销响应文件。

15. 询价小组

15.1 采购人将按照《中国华能集团有限公司非招标采购管理办法》及有关法律、

法规的规定组建询价小组。

15.2 询价小组负责评审工作，根据采购文件的要求对响应文件进行审查、质疑、评估和比较，出具评审报告，推荐成交候选供应商。

16. 开启响应文件

在供应商须知前附表规定的时间开启响应文件。

17. 评审方法

评审将严格按照采购文件第三章规定的评审标准和办法及国家有关法律、法规的要求进行。

18. 确定成交供应商

采购人按询价小组推荐的成交候选供应商名单确定成交供应商。成交候选供应商的推荐原则，见供应商须知前附表。

19. 采购结果公告

采购人确定成交供应商，询价采购结果在电子商务平台进行公告，采购结果公告应列出询价文件规定的成交供应商资质、业绩、交货期（工期或服务期）、承诺的项目负责人姓名及其相关证书名称和编号等情况。

20. 成交通知

20.1 采购人向成交供应商发出《成交通知书》，同时通知所有未成交的供应商。

20.2 《成交通知书》将构成合同的组成部分。

21. 签订合同

21.1 成交供应商在接到《成交通知书》后，必须在规定的时间内派法定代表人或其授权人到指定地点按采购活动双方最终确认的合同条款与采购人签订合同。

21.2 采购文件、成交供应商的响应文件及评审过程中的有关澄清文件均为签订合同的依据。

21.3 采购文件中要求成交供应商提交履约担保的，成交供应商应在合同规定的时间前根据供应商须知前附表的要求向采购人提交履约担保。

22. 其他需要补充的内容

第三章 评审办法

一、总则

1.评审依据

1.1《中国华能集团有限公司非招标采购管理办法》及相关法律法规；

1.2 采购文件及其有效的补充文件。

2.评审原则

评审活动遵循“公平、公正、科学、择优”的原则。

二、评审方法

本项目采用经评审的最低价法。

三、评审程序

询价小组评审包括初步评审和详细评审两部分。

1. 初步评审

询价小组对响应文件进行初步评审，评审内容如下：

1.1 供应商资格条件是否满足采购文件要求；

1.2 供应商是否按采购文件要求提交响应保证金或金额不足（如有）；

1.3 响应文件是否附有采购人不能接受的条件；

1.4 供应商报价是否超出最高限价（如有）；

1.5 有下列情形之一的，视为供应商相互串通：

(1) 不同供应商的响应文件由同一单位或者个人编制；

(2) 不同供应商委托同一单位或者个人办理询价事宜；

(3) 不同供应商的响应文件载明的项目管理成员为同一人；

(4) 不同供应商的响应文件异常一致或者报价呈规律性差异；

(5) 不同供应商的响应文件相互混装；

(6) 不同供应商的响应保证金从同一单位或者个人的账户转出。

(7) 不同供应商的响应文件的互联网协议地址（IP 地址）信息检查一致；

1.6 国家相关法规规定的其它否决条款。

如发生上述条款中的任何一项，初步审查将视为不合格，供应商只有通过初步评审，

才能进入详细评审。

2.详细评审

详细评审包括商务、技术和价格评审。如详细评审阶段，商务、技术、价格评审中有一项不通过，将视为否决供应商。

2.1 商务评审，是否实质上响应了采购文件的要求，主要包括交货期/工期/服务期、付款条件、商务偏离等。

2.2 技术评审，是否实质上响应了采购文件的要求；主要包括采购需求是否符合要求等。

2.3 报价评审，以供应商在电子商务平台线上填报的总报价为准作为最终报价，如果平台报价异常的，询价小组可向供应商进行书面澄清，如供应商确认平台报价错误时，应当将其否决。询价小组对供应商的报价文件进行比较。询价小组不得同某一供应商就其报价进行谈判。

3.响应文件的澄清、说明和补正

3.1 在评审过程中，询价小组可以书面形式要求供应商对所提交的响应文件中不明确的内容进行书面澄清或说明，或者对细微偏差进行补正，供应商的书面澄清、说明和补正属于响应文件的组成部分，询价小组不接受供应商主动提出的澄清、说明或补正。

3.2 澄清、说明和补正不得改变响应文件的实质性内容(算术性错误修正的除外)。

3.3 询价小组对供应商提交的澄清、说明或补正有疑问的，可以要求供应商进一步澄清、说明或补正，直至满足询价小组的要求。如不按询价小组要求进行澄清、说明或补正的，可以否决其响应文件。

4. 评审报告

4.1 在评审各阶段的结论，如评审人员有不同意见，按少数服从多数的原则得出最终评审结论。

4.2 询价小组完成评审工作后，向采购人提出书面评审报告。如果询价小组成员对评审报告有异议，可以书面方式阐述其不同意见和理由。询价小组成员拒绝在评审报告上签字且不陈述其不同意见和理由的，视为同意评审报告，询价小组应当对此做出书面说明，并记录在案。

四、推荐成交候选供应商

本次评审采用经评审的最低价法。询价小组对满足采购文件实质要求的响应文件，按照经评审的价格（算术性修正后的价格）由低到高的顺序依次推荐 1～3 名成交候选供应商。若经评审的价格相同，按满足资格条件业绩要求的业绩数量多者优先；如业绩

数量也相等时，由询价小组投票确定。

第四章 合同条款及格式

漫湾电厂生产网络安全防护优化建设合同

合同编号：MWDC2021/U32

甲方：华能澜沧江水电股份有限公司

乙方：**********公司

签订地点：云县漫湾镇

签定时间：　　年　月　日

漫湾电厂生产网络安全防护优化建设合同

甲方：华能澜沧江水电股份有限公司

乙方：********公司**

根据《中华人民共和国民法典》及相关法律、法规，甲、乙双方本着公平公正、平等互利、诚实信用的原则，经友好协商，甲方委托乙方实施漫湾电厂生产网络安全防护优化建设事项，双方协商一致，订立本合同。

第一条 工程内容

漫湾电厂生产网络安全防护优化建设，主要内容为根据公司《电力监控系统网络安全防护优化建设方案》开展以下工作：

（1）合规性建设，在安全Ⅰ区部署入侵检测系统，在安全Ⅱ区、Ⅲ区部署入侵防御装置；安全Ⅰ、Ⅱ、Ⅲ区各主机部署防病毒系统（含50套防病毒软件及3套防病毒管理系统），防病毒网关。部署一台漏洞扫描装置，满足各系统日常定期漏洞扫描。

（2）提升性建设，在安全Ⅰ区部署高级可持续威胁预警系统（APT）、流量分析系统、“蜜罐”系统；在安全Ⅱ区部署高级可持续威胁预警系统（APT）、“蜜罐”系统、流量分析系统；安全Ⅲ区部署高级可持续威胁预警系统（APT）、流量分析系统、“蜜罐”系统。

（3）功能性建设，在安全Ⅰ区监控系统部署符合国密要求的运维堡垒机；在安全Ⅱ区、Ⅲ区各部署运维堡垒机及日志审计；在安全Ⅰ区安全Ⅱ区、Ⅲ区各部署安防管理工作站。

（4）主机加固，对安全Ⅰ区计算机监控系统工程师站、操作员站服务器进行加固，对安全Ⅱ、Ⅲ区相关业务服务器进行主机加固，加固台数30台。

（5）对现有部署于安全Ⅰ区监控系统1台日志审计系统进行配置优化。

第二条 履行期限、地点

一、计划工期：自合同签订之日起至2022年10月15日，具体时间以电厂通知为

准。发生国家相关规定的不可抗力因素或因实际工作需要另行安排调整相关工作，工期可进行延长或调整。

二、履行地点：漫湾电厂。

第三条 合同价款及支付方式

一、 **合同总价：**合同含税总价为人民币***（¥***），合同税率为13%，合同不含税总价为人民币********（¥***** ），合同税额为人民币********（¥******）。合同执行期间如因国家政策、法律及法规变化等原因需进行税率调整，应以“维持合同不含税总价不变”原则调整合同税率及合同含税总价。

合同总价中包括了乙方为实施和完成承包项目的工作内容和施工工序所需的生活设施、人员和工器具、机械设备进退场、施工准备、劳务、材料、缺陷修复、管理、保险、质量保证、税费，及承担质量、安全等费用。其中安全措施费为人民币******（¥******）。

二、 结算方式

总价包干。

三、 支付方式（具体合同支付方式以合同谈判为准）

1. 合同签订后，完成主设备到货验收，由甲方通知乙方开具10%合同金额的增值税专用发票（税率为13%），乙方提交以下单据，经审核无误后，甲方收到乙方合格票据后次月内，支付乙方进度款：

(1)金额等于合同金额10%的增值税专用发票（税率为13%）；

(2)按合同规定的由双方共同签署的到货验收单、进度款支付证明及其他相关资料。

2. 完成合同规定所有内容，试运行3个月无异常，工程竣工验收合格，由甲方通知乙方开具90%合同金额的增值税专用发票（税率为13%），乙方提交以下单据，经审核无误后，甲方收到乙方合格票据后次月内，扣留违约考核款及合同金额3%的质保金后支付乙方结算款：

(3)金额等于合同金额90%的增值税专用发票（税率为13%）；

(4)合同规定的全部技术资料及竣工资料；

(5)按合同规定的由双方共同签署的竣工验收单、结算书及其他竣工资料。

3. 质保金：本工程的质量保证金金额为合同总金额的3%结算时扣留，质保期满无质量问题，甲方收到乙方质保金收据后次月内支付合同总金额3%的质保金。质保期内若存在因质量问题而发生的非乙方处理的费用，将按实扣除质保金，质保期满后退回剩余质保金，质保金不计利息。

四、 开票信息

单位名称：华能澜沧江水电股份有限公司漫湾水电厂

纳税人识别号：915300007194494905

地址、电话：云南省临沧市云县漫湾镇、0883-3813030

开户银行及帐号：建行云县支行 53001776140050014003

第四条 工程质量、技术要求

1. 本工程质量经双方协商要求达到：技术方案及图纸中的技术要求；无明确技术要求的，要求达到国家相关质量标准。

2. 乙方必须严格按照设计图纸、说明文件和国家颁发的规程、规范、标准和有关实施细则进行施工，并接受甲方代表的监督。

3. 本项目不得转包，主体工程和关键性工作不得分包。

4. 乙方在施工过程中必须遵守下列规定：

（1）乙方采购的材料、设备，必须附有产品合格证书，甲方认为提供的材料需要复验的，应允许复验。经复验符合质量要求的，方可用于工程，其复验费由甲方承担；不符合质量要求的，不允许用于工程，其复验费由乙方承担。

（2）项目实施方案或技术协议中对材料的品牌、型号有明确要求的，对材料改变或代用必须经甲方同意后，方可用于工程。

（3）隐蔽工程必须经甲方代表检查、验收签字确认后，方可进行下一道工序。

第五条 施工与设计变更

1. 甲方交付乙方的设计图纸、说明和有关技术资料，作为施工有效依据。施工中如发现设计有错误或严重不合理的地方，乙方应及时以书面形式通知甲方，由甲方、乙方及时会同有关单位研究确定修改意见或变更设计文件，乙方按修改或变更的设计文件进行施工，由此引起设计变更所增加的工程费用，由甲方负责。

2. 由乙方原因造成的工程费用增加，由乙方自行承担。

第六条 工程验收及质量保修

1．验收标准：

漫湾电厂生产网络安全防护优化建设应遵照下列标准，在合同签定时最新版或经甲方同意的与之相当的标准。若在项目实施阶段又出现了标准或规程的最新修改版，乙方应尽量采用，对实施中出现的问题由双方协商解决。如所采用的各种标准之间存在矛盾时，应按高标准的要求执行并经甲方批准。

发改委 14 号令　　《电力监控系统安全防护规定》

GB/T 22239-2008　　《信息安全技术信息系统安全等级保护基本要求》

DL／Z 981-2005　　《电力系统控制及其通信数据和通信安全》

国能安全〔2015〕36 号《电力监控系统安全防护总体方案等安全防护方案和评估规范》

公通字[2007]43 号　　《信息安全等级保护管理办法》

GB/T 22080-2008　　《信息安全管理体系要求》

《华能澜沧江水电股份有限公司电力监控系统网络规划优化建设方案》

2．本工程的质保期为 壹 年，质保期自工程竣工验收合格之日起计算。如果在质保期间出现由于乙方的责任引起的任何质量问题，则应由乙方进行免费修复，并承担由此带来的一切损失及法律责任，质保期自修复完成验收合格之日起重新计算。

第七条 权利与义务

一、 甲方的权利与义务：

1. 协助乙方处理在施工过程中与各相关单位的关系。

2. 检查监督乙方的工程实施进度、工程质量和施工安全。

3. 明确一名甲方 代表，参与对本工程实施的监督管理。

4. 按合同条款支付相应合同款。

5. 按时参加工程的竣工验收。

6. 因故未能按计划开工的项目提前通知乙方。

二、 乙方的权利与义务：

1. 乙方根据现场踏勘情况编制施工方案及图纸，按照甲方审定后的施工方案及图纸，组织实施项目工程。

2. 严格按照国家有关规范标准按质、按量、按时完成甲方委托的全部工作内容。

3. 制定和采取有效的技术保障措施，做好施工现场的环境保护工作。

4. 承担因安全管理不到位或安全技术措施不力导致的安全责任事故。

5. 乙方应成立专门的项目组织机构，提供执行本项目质量控制、质量保证的人员及现场安装的主要技术指导人员。本项目的总人数不得少于 2 人，其中项目负责人 1 人、技术人员 1 人；其中项目负责人具有 Microsoft SQL SERVER 数据库构建、软件开发等相关技能，具有 3 年以上的专业工作经验，并担任过类似项目负责人，技术人员具备 Microsoft SQL SERVER 数据库使用、软件编译等相关技能，具有 3 年以上的专业工作经验。

6. 及时组织开展工程的竣工验收。

7. 做好工程技术档案的管理工作，做到工程技术资料真实、完整、及时、规范。

8. 工程竣工验收后 30 天内提交完整竣工资料。

第八条 违约责任

一、 乙方违约

1. 因施工造成工程质量不符合合同规定的，负责无偿修理或返工；由于修理返工造成逾期交付的，偿付逾期违约金，还需承担由于违约给甲方造成的损失及法律责任。

2. 因乙方原因（设备、材料未按时到货或到货后验收不合格）导致项目实施后设备设施不能按期投入运行，每拖延一天扣罚乙方总价的1‰（最低不少于500元），最高扣罚不超过合同总价的20%。

3. 不可抗力原因造成延误，乙方应及时将情况以书面形式通知甲方，得到甲方签字认可后可免除违约责任。

4. 现场施工工程中违反漫湾电厂《外包工程安全管理标准》相关要求的，执行《外包工程安全管理标准》考核条款。

5. 因乙方原因造成工期与合同工期不符的，每超过一天扣罚乙方总价的1‰（最低不少于500元），最高扣罚不超过合同总价的20%。

6. 乙方未按时提交全部的竣工资料或提交的竣工资料存在明显与合同工期、施工内容、遗留的问题等实际情况不符的，扣罚乙方总价的1‰（最低不少于500元）。

7. 乙方违反合同任何一条义务的，均属违约，对于违约责任，合同有约定的从其约定，没有约定的，乙方应按照合同总价的20%向甲方支付违约金，给甲方造成损失的，还需承担赔偿责任。

二、 甲方违约

1. 在完全满足支付条件的前提下，若甲方不按合同条款规定向乙方支付费用时，以30天为宽限期,乙方可要求甲方支付违约金,每迟付15天违约金为合同总价的0.5%，累计不超过合同总价的20%。

2. 其它违约责任按民法典执行。

第九条 合同生效和终止

一、 合同生效

甲方和乙方的法定代表人或其授权代表在协议书上签名并加盖本单位行政公章或合同专用章后，合同生效。

二、 合同终止

本合同质量保证期结束，运行正常，合同双方均按合同规定履行完毕义务时，合同自然终止。

发生以下情形，甲乙双方可依法终止合同：

1. 甲乙双方公司被依法宣告破产的；

2. 甲乙双方公司被吊销营业执照、责令关闭、撤销或者公司决定提前解散的；

3. 甲乙双方公司经营期限届满，不再继续经营的；

4. 因法律法规、方针政策变化，发布方应上级单位要求、经营方式改变或其它原因，导致合同执行方式、合同内容不再适宜的；

5. 因甲乙双方单位在经营过程中存在问题，被国家相关监管部门提出整改要求，导致合同不能继续履行的；

6. 法律、法规规定的其它情形。

除上述终止合同条款以外，发生以下情形，甲、乙双方可依法解除合同，并保有依法追究相关法律责任的权利：

1. 甲、乙双方擅自变更合同内容、或不按合同内容执行，并造成对方重大损失的；

2. 乙方不服从甲方规章制度，或不按电力安全规范要求，导致施工过程存在较大安全风险，或发生电力安全生产事故的；

3. 法律、法规规定的其它情形。

三、 合同解除

在合同执行中，乙方不按合同约定履行合同，出现下列情况时，甲方有权解除合同，要求乙方全额退还已支付的合同款，并有权追索经济损失。

1. 实施期间乙方投入的资源不能满足项目实施需要，严重影响项目工作，甲方要

求乙方限期整改后，乙方仍未按要求整改的。

2. 乙方私自将合同或合同的任何部分或任何权利转让给其他人，或私自将工程或工程的一部分违规分包出去的；

3. 在合同执行过程中，乙方未按合同要求完成工程内容或工程质量未达到技术要求的；

4. 在合同执行过程中，出现重大安全、质量事故、协调纠纷的，甲方发出停工整改通知 3 天后，乙方继续无视甲方的指示，不采取整改措施的。同时乙方支付甲方当年合同总价 20%的违约金，并赔偿甲方经济损失。

在履行合同过程中，甲方发生下述行为，且乙方向已向甲方发出通知，并采取了暂停的行动后，甲方仍不采取有效措施纠正违约行为，乙方有权向甲方提出解除合同的要求。

1. 甲方未能按合同规定支付乙方合同价款。

2. 由于法律、财务等原因导致甲方已无法继续履行或实质上已停止履行本合同的义务。

第十条 合同争议的解决方式

1. 所有在履行合同过程中以及与合同有关的争议，双方应通过友好协商解决，并签订协议书。如不能达成协议，任何一方均可向工程所在地云南省临沧市云县人民法院起诉。

2. 诉讼费用由败诉方负担。

3. 在诉讼期间，除提交诉讼的事项外，合同仍应继续履行。

第十一条　通讯与联络

1. 为方便开展工作，提高双方的工作效率，甲方安排_____负责与乙方保持日常联系，乙方项目负责人_____，负责合同责任范围内的全部管理和协调工作。如双方确有必要更换联系人员时，应以书面形式提前通知另一方。甲方工作人员的联系方

式是_____；乙方工作人员的联系方式是_____。

2. 双方履行合同的有关事项，按照上述约定通知到对方联系人的，视为完成通知送达。

3. 双方的通讯地址或者联系方式如发生变动，应书面通知对方，因未及时通知而造成的损失由其自行承担。

第十二条　移交竣工资料

1. 总结、报告及各阶段验收材料。

2. 其他应提交的重要文件资料（如有）。

第十三条　附则

1. 本合同经双方授权代表签字盖章后生效。

2. 本合同未尽事宜，双方协商一致可签订补充条款，补充条款与本合同具有同等法律效力。

3. 本合同一式六份，正本二份，副本四份，甲方执一正三副，乙方执一正一副。

第十四条　附件

本合同具有以下附件，是合同不可分割的组成部分，与合同具有同等法律效力。

1. 漫湾电厂生产网络安全防护优化建设费用组成表

2. 漫湾电厂生产网络安全防护优化建设项目保密协议

3. 漫湾电厂生产网络安全防护优化建设项目组织机构及对应的岗位人员数量统计表

此页无正文。

甲方：华能澜沧江水电股份有限公　司

（公章）

法定代表人或

委托代理人：

经 办 人：

地址：云南省临沧市云县漫湾镇

电话：0883-3813720

传真：0883-3814022

邮政编码：675805

开户银行：　建行云县支行

银行账号：53001776140050014003

纳税人识别号：915300007194494905

乙方：**********公司

（公章）

法定代表人或

委托代理人：

经　办　人：

地址：昆明市一二一大街 71 号 1 幢 5-27、29、31 号

电话：0871--65166681

传真：0871--65166681

邮政编码：650010

开户银行：华夏银行昆明分行翠湖支行

银行账号：4842000001801900007446

纳税人识别号：915301027846355721

第五章 采购需求

漫湾电厂电力监控系统网络安全防护优化项目技术方案

一、 技术规范要求

本标准和规程提出的是最低限度的技术要求，并未对一切技术细节作出规定，也未引述有关标准和有关规范的条文。项目承建方应保证所提供的设备及有关产品是安全、可靠的，按国家有关标准通过检测。既必须是为本项目生产的全新产品，并符合国家有关安全环保等强制性标准及规定。本项目实施应符合：

发改委14号令　　《电力监控系统安全防护规定》

GB/T 22239-2008　　《信息安全技术信息系统安全等级保护基本要求》

DL／Z 981-2005　　《电力系统控制及其通信数据和通信安全》

国能安全〔2015〕36号《电力监控系统安全防护总体方案等安全防护方案和评估规范》

公通字[2007]43号　　《信息安全等级保护管理办法》

GB/T 22080-2008　　《信息安全管理体系要求》

《华能澜沧江水电股份有限公司电力监控系统网络规划优化建设方案》

二、 方案设计

（一）优化方案

1. 安防系统建设方案

1.1 合规性建设

按照《华能澜沧江水电股份有限公司电力监控系统网络规划优化建设方案》，结合漫湾电厂存在的问题，合规性建设需要在安全Ⅰ区部署入侵检测系统，在安全Ⅱ区、Ⅲ区部署入侵防御装置；安全Ⅰ、Ⅱ、Ⅲ区各主机部署防病毒系统（含50套防病毒软件及3套防病毒管理系统），防病毒网关。部署一台漏洞扫描装置，满足各系统日常定期漏洞扫描。

1.2 提升性建设

按照《华能澜沧江水电股份有限公司电力监控系统网络规划优化建设方案》，结合漫湾电厂存在的问题，提升性建设需要在安全Ⅰ区部署高级可持续威胁预警系统（APT）、流量分析系统、“蜜罐”系统；需要在安全Ⅱ区部署高级可持续威胁预警系

统（APT）、“蜜罐”系统、流量分析系统；安全III区部署高级可持续威胁预警系统（APT）、流量分析系统、“蜜罐”系统。

1.3 功能性建设

按照《华能澜沧江水电股份有限公司电力监控系统网络规划优化建设方案》，结合漫湾电厂存在的问题，功能性建设需要在安全Ⅰ区监控系统部署符合国密要求的运维堡垒机；需要在安全Ⅱ区、Ⅲ区各部署运维堡垒机及日志审计；需在安全Ⅰ区安全Ⅱ区、Ⅲ区各部署安防管理工作站。

2. 主机加固

对安全Ⅰ区计算机监控系统工程师站、操作员站服务器进行加固，对安全Ⅱ、Ⅲ区相关业务服务器进行主机加固，加固台数30台。

3. 现有安防设备配置优化

对现有部署于安全Ⅰ区监控系统1台日志审计系统进行配置优化，并接入安全管理平台。

（二）设备技术参数和性能要求

1、设备必须满足标有“★”项技术要求；

2、主要设备需使用同一制造商；

3、设备必须是标准的，元器件、材料是崭新的，软件版本需要是最新的。

注：主要设备为（入侵监测、入侵防御、高级可持续威胁检测系统（APT）、漏洞扫描、堡垒机、日志审计、防火墙）

2.1 入侵检测要求

★系统性能：整机吞吐率≥9.5Gbps,最大并发连接数≥220 万,IDS 吞吐率≥3.8Gbps。

★硬件配置：机架式设备，冗余电源；≥5 个千兆电口，≥4 个千兆光口；≥1T 硬盘；配置应用识别功能，含 3 年应用识别规则库升级许可；配置攻击规则特征库 3 年升级许可；提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

系统可靠性：系统软件属国产自主研发软件，并具有软件著作权。支持多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择（提供产品功能界面截图

并加盖制造商公章），不得在 WEB 维护界面中设置系统切换选项。

攻击取证：支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据。

自定义规则：支持自定义规则，并且自定义规则库可以导入导出。（提供产品功能界面截图并加盖制造商公章）

DDOS 检测：支持 DHCP 异常包及 DHCPFlood 攻击检测。（提供产品功能界面截图并加盖制造商公章）

流量异常检测及报警：支持对协议组的流量阀值和连接数进行设置及报警，协议组类型包括 P2P 类、即时通讯类、标准协议类、移动应用类、http 应用类、工控互联网类等。（提供产品功能界面截图并加盖制造商公章）

流量采集：支持流量采集策略设置，对流量采集的方向、时间、源 IP 地址、目的 IP 地址、源端口、目的端口进行设置。（提供产品功能界面截图并加盖制造商公章）

日志存储：支持多种形式的日志存储,本地存储、发送至日志服务器、本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式。

日志展示：支持攻击检测日志中可以直观的展示攻击事件中的攻击特征编码。

设备监控：支持设备运行状态各指标的监视以及报警。（提供产品功能界面截图并加盖产商公章）

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》网络入侵检测系统（第三级）（产品专属证书，非复用其他产品证书）；提供中国网络安全审查技术与认证中心颁发的产品《IT 产品信息安全认证证书》（EAL3 增强级）（产品专属证书，非复用其他产品证书）；提供产品的《IPv6 Ready Logo 认证证书》（产品专属证书，非复用其他产品证书）。

2.2 入侵防御要求

★性能参数：整机吞吐率≥5.7Gbps,最大并发连接数≥115 万,IPS 吞吐率≥1.9Gbps。

★硬件配置：机架式设备，冗余电源；≥5 个千兆电口，≥4 个千兆光口；≥1T 硬盘；配置应用识别功能，含 3 年应用识别规则库升级许可；配置攻击规则特征库 3 年升

级许可;提供3年原厂硬件维保和3年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

系统可靠性：系统软件属国产自主研发软件，并具有软件著作权。支持多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择（提供产品功能界面截图并加盖制造商公章），不得在WEB维护界面中设置系统切换选项。

流量采集：支持流量采集功能，支持在设备界面对服务器地址、端口、以及采样百分比进行设置。（提供产品功能界面截图并加盖制造商公章）

攻击取证：支持攻击报文取证功能，检测到攻击事件后将原始报文完整记录下来，作为电子证据。

自定义规则：支持自定义规则，并且自定义规则库可以导入导出。（提供产品功能界面截图并加盖制造商公章）

流量异常检测及报警：支持对网络内的TCP、UDP、其他流量协议占比进行设置及报警。（提供产品功能界面截图并加盖制造商公章）

DDOS防御：支持对主机并发连接数和半连接数进行限制。（提供产品功能界面截图并加盖制造商公章）

日志存储：支持多种形式的日志存储,本地存储、发送至日志服务器、本地日志服务器双存储、自动方式判断日志服务器状态自动决定日志的记录方式。

设备监控：支持设备运行状态各指标的监视以及报警。（提供产品功能界面截图并加盖产商公章）

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》NIPS（三级）（产品专属证书，非复用其他产品证书）；提供中国信息安全测评中心颁发的产品《国家信息安全测评信息技术产品安全测评证书》（EAL3+级）（产品专属证书，非复用其他产品证书）；提供产品的《IPv6 Ready Logo认证证书》（产品专属证书，非复用其他产品证书）。

2.3 主机防病毒软件要求

★产品形态：系统支持中/英文界面，系统部署采用C/S架构。本次采购主机防病毒软件管理中心含3年升级许可，linux主机防病毒软件含3年升级许可。

★客户端资源占用：客户端安装后占用≤51M 硬盘资源，日常内存占用≤21M，能有效节省 PC/Server 资源。（提供证明并加盖制造商公章）

远程控制：支持远程控制，通过管理中心实现对客户端的远程运维。

Webshell 检测：支持对 webshell 后门进行扫描检测,webshell 后门库数量≥100000。

勒索病毒诱捕：支持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。（提供产品功能界面截图并加盖制造商公章）

★系统加固：支持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。（提供产品功能界面截图并加盖制造商公章）

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。（提供产品功能界面截图并加盖制造商公章）

文档跟踪：支持文档跟踪策略，可按照不同文件、压缩包类型跟踪文档内到外、外到内、外到外、内到内等流转方向，并可跟踪文档包括拷贝、压缩、解压缩、修改、删除、重命名、移动等操作。（提供产品功能界面截图并加盖制造商公章）

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。（提供产品功能界面截图并加盖制造商公章）

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》网络版防病毒产品（一级品）（产品专属证书，非复用其他产品证书）；提供中国信息安全测评中心颁发的产品《国家信息安全测评信息技术产品安全测评证书》EAL3+（产品专属证书，非复用其他产品证书）；提供产品的《IPv6 Ready Logo 认证证书》（产品专属证书，非复用其他产品证书）。

2.4 防病毒网关要求

★性能参数：整机吞吐率≥2.8Gbps，最大并发连接数≥240 万，病毒检测吞吐率≥750Mbps。

★硬件配置：机架式设备，冗余电源；≥5 个千兆电口（支持≥1 组 Bypass 接口），≥2 个千兆光口；硬盘≥1T。配置快速扫描防病毒查杀和深度扫描防病毒查杀功能，含 3 年病毒库升级许可；提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

专业设备：设备必须为专业的防病毒网关产品，非防火墙/下一代防火墙、UTM、IPS 等具有防病毒功能模块的产品。（提供产品登录界面截图并加盖制造商公章）

系统可靠性：支持多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择（提供产品功能界面截图并加盖制造商公章），不得在 WEB 维护界面中设置系统切换选项。

★病毒引擎：支持双库双引擎，可选择使用不同的病毒库，可选择使用不同的扫描引擎（快速扫描引擎或深度扫描引擎）。（提供产品功能界面截图并加盖制造商公章）

病毒检测与过滤：支持对 HTTP、FTP、POP3、SMTP、IMAP 等常用应用协议进行病毒检测与过滤。（提供产品功能界面截图并加盖制造商公章）

病毒库：具有独立的蠕虫防护规则库，并可通过手动或自动方式进行升级。（提供产品功能界面截图并加盖制造商公章）

网络适用性：支持多接口可旁路的病毒监听检测模式，可并行监听检测多条链路、多个网段内的病毒传输行为。（提供产品功能界面截图并加盖制造商公章）

日志检测：具有针对 FTP 流量的病毒检测过滤日志，且过滤日志能定位到具体的文件名，方便管理处理携带病毒的文件。

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》网关防病毒产品（增强级）（设备专属证书，非复用其他产品证书）；提供国家版权局颁发的产品《计算机软件著作权登记证书》；提供产品的《Pv6 Ready Logo 认证证书》（设备专属证书，非复用其他产品证书）。

2.5 流量分析系统要求

★系统性能：整机吞吐量≥1.9Gbps，最大并发连接数：≥580 万。

★硬件配置：机架式设备，冗余电源；≥6 个千兆电口，≥4 个千兆光口；系统盘≥240GSSD，数据盘≥16THDD；内存≥96G；包含 3 年系统版本升级及应用特征库升级许可；提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

高性能检测分析感知引擎：拥有独立的安全分析引擎：覆盖 32 个大类 41000 余种攻击行为；病毒库规模 900 万以上，支持文件还原和病毒检测；拥有漏洞扫描知识库包含 6 万条以上的漏洞规则，覆盖十万条以上 CVE 漏洞记录。（提供产品功能界面截图并加盖制造商公章）

全局可视化态势分析系统：支持以全局形式展示整体态势，包括网络性能态势、安全态势、资产态势、外联风险态势、横向威胁态势等，支持按不同时段、不同链路查看。（提供产品功能界面截图并加盖制造商公章）

★流量监控分析：支持按链路层、网络层、传输层所支持的协议，包括 TCP/UDP/IPv4/IPv6/ICMPv4/ICMPv6/Unicast/Broadcast/Multicast/ARP/RARP 协议，按协议统计网络流量的平均速率、最大值、最小值、中值、标准差等，及各层流量的平均速率趋势图，并且可以按 5 分钟、30 分钟、3 小时、天、周、月、季、年等粒度查询相关流量。支持按各层支持协议展示或比特、字节、数据包展示。在各层流量的趋势图分析中支持对任意时刻的流量进行 TOPN 的数据关联，确定网络流量来源、识别其所对应的应用类型、追踪其传输的目的地。（提供产品功能界面截图并加盖制造商公章）

★业务性能分析：支持 http/https、DNS、Oracle、mysql、pop3、smtp、telnet、RTSP、RTP、MMS、SIP、RTMP、FTP 等核心业务的性能监控，包括 2-7 层数据的 20 余种各类指标分析，如登录状态、登陆时间、三次握手时间、登陆交互流程等信息呈现。（提供产品功能界面截图并加盖制造商公章）

业务监控：支持 http 业务的监控，能提炼出每次访问的行为的源目的地址、DNS 查询次数、持续时间、资源类型、响应状态、页面元素加载瀑布图等，支持非加密页面访问行为页面还原。支持 URL 访问过程解析，可以从 DNS 解析过程、网络端和服务器端响应时延等关键指标分析异常问题。支持对 HTTP/HTTPS 网页访问服务的综合评分机制，包括页面载入时间、首字节加载时间、dns 解析时间、建立连接时间、网页元素加载状

态等，支持网页中每个元素的获取周期不同阶段监控，如域名解析、建立连接、发送请求、等待响应、接收数据 5 个阶段，响应头信息包含 Cache-Control、Connection、Content-Encoding、Content-Length、Content-Type、Date、Expires、Last-Modified、Server，请求头信息包含 Accept、Accept-Encoding、Accept-Language、Cookie、Host、User-Agent 支持对业务的综合对比分析，按地区、按服务器角度对比分析。支持 http 访问信息还原分析，包括 Image、Application、Text、Multipart、Video、Message、Audio 等方式还原访问场景。

网络性能分析：支持端到端的网络性能监控分析，可以从 C2S 和 S2C 的监督溯源 TCP 会话指标，指标包括：该 TCP 会话的源目的 IP、源目的端口、平均 rtt、重传报文大小、重传包大小占比、乱序包数量、包传输速率、流传输速率、拥塞率、吞吐量、滑动窗口最大值、滑动窗口最小值、零窗口数、tcp 值、ack 值、rst 值、syn 值、fin 值等。

全流量溯源分析：支持通讯数据的回溯分析。会话记录数据包含记录时间/源地址/源端口/目的地址/目的端口/源MAC地址/目的MAC地址/应用/开始时间/持续时间/总字节数/总包个数/包速率等 25 个以上关键字段；支持流记录的自定义检索，如特定源目的 IP、应用协议、源目的端口等；流记录分析支持按表格、逻辑连接 TOPO 图、访问矩阵图多种形式查看；支持网络连接关系自动发现，形成网络逻辑连接关系图展示网络流量、端口、协议等信息。

资产分析：支持系统主动扫描探测内网资产，资产类型包括：终端、服务器、交换机、虚拟机、路由器、打印机、防火墙、存储设备、游戏机、网桥设备、动力装置、负载均衡设备等。（提供产品功能界面截图并加盖制造商公章）

告警：系统支持异常流量告警、网络性能异常告警、安全事件告警、系统状态告警等，支持短信、邮件、弹窗等方式呈现、推送，支持告警详情查看，系统支持手动创建异常流量告警策略，可根据网络链路层、网络层、传输层、应用层所支持的不同协议以及作用的链路创建告警规则，判别方式支持静态阈值和基准线两种。（提供产品功能界面截图并加盖制造商公章）

产品资质：产品拥有自主知识产权，并且为国内研发和生产，提供产品《计算机软件著作权登记证书》（产品专属证书，非复用其他产品证书）；提供产品《计算机信息

系统安全专用产品销售许可证》（产品专属证书，非复用其他产品证书）。

2.6 高级可持续威胁检测系统（APT）要求

★性能参数：综合监测吞吐≥1.8Gbps。

★硬件配置：机架式设备，冗余电源；日志存储空间≥8TBHDD，系统存储空间≥250GSSD；≥6 个千兆电口，≥4 个千兆光口，≥2 个万兆光口。提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

基础功能：系统应具备流量采集、文件还原、文件静态和动态沙箱检测、web 攻击检测、异常行为分析、数据分析与风险预警等功能，能够检测已知/未知恶意文件，0Day/nday 漏洞利用，Web 攻击，恶意扫描攻击等；还支持对失陷主机、DGA 域名、动态域名、隐蔽信道、异常协议等异常通信行为进行分析告警。

文件还原：支持解析还原包括邮件文件（EML）、Office（Word、Excel、PPT、RTF）、WPS、PDF、HTML、JS、PE（EXE、DLL 等）、压缩包（ZIP、7Z、RAR 等）、脚本文件（BAT、VBS、CMD、Powershell）、图片文件（PNG、JPG 等）、APK 等 70 余种默认文件格式。（提供产品功能界面截图并加盖制造商公章）

检测引擎：具备动态行为检测引擎、机器学习检测引擎、威胁情报检测引擎、AV 检测引擎、CVE 检测引擎、YARA 规则检测引擎等文件检测引擎，且每种检测引擎均可输出各自检测结果。（提供产品功能界面截图并加盖制造商公章）

机器学习：支持 3 种以上机器学习算法模型（静态检测模型、动态检测模型、静态和动态混合检测模型）对文件进行威胁判定，且每种机器学习模型会对所支持的样本文件进行检测，输出不同的机器学习算法对样本恶意与非恶意的判定结果。（提供产品功能界面截图并加盖制造商公章）

沙箱行为监测：沙箱支持安装包程序释放物检测，沙箱能够自动完成安装包类型样本的安装，检测安装包中隐藏的恶意释放物，同时支持 shellcode 提取，能将 shellcode 反汇编成汇编代码。（提供产品功能界面截图并加盖制造商公章）

Web 攻击检测：支持对 Web 应用攻击行为进行检测，包括恶意扫描攻击、漏洞利用行为、注入攻击，XSS，CSRF、文件包含、目录遍历等常见 web 攻击类型。（提供产品功能界面截图并加盖制造商公章）

隐蔽信道检测：支持隐蔽信道通信检测功能，能够在看似正常的流量中识别木马的隐藏传输行为，并具备对通信会话的 PCAP 文件记录、存储以及在线查看功能。

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》（产品专属证书，非复用其他产品证书）；提供产品的《IT 产品信息安全认证证书》测试标准符合 ISCCC-TR-083-2018《APT 安全监测产品安全技术要求》（产品专属证书，非复用其他产品证书）；提供产品的《IPv6 Ready Logo 认证证书》（产品专属证书，非复用其他产品证书）。

2.7 蜜罐系统要求

★系统性能：提供≥9 个仿真主机 IP 授权，多合一形态产品，单台即可满足功能需求。

★硬件配置：标准机架设备，冗余电源；≥5 个千兆电口，≥4 个千兆光口；内存≥16G；包含 3 年系统升级服务；提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

服务模拟及攻击检测能力：支持使用非默认端口号提供蜜罐交互服务（提供产品功能界面截图并加盖制造商公章）

★诱捕场景：支持自定义诱捕场景名称；支持 Linux、Windows 系统诱捕场景；诱捕场景可选服务类型包括但不限于网络工具、云计算服务、文件传输服务、WEB 服务、邮件服务、远程控制服务、数据库服务、虚拟网络服务（提供产品功能界面截图并加盖制造商公章）

诱捕主机：支持批量创建仿真诱捕主机（提供产品功能界面截图并加盖制造商公章）

告警筛选：支持对告警日志进行筛选，至少基于起始日期、结束日期、源 IP、目标 IP、目标端口、服务、协议、攻击类别、告警级别、日志状态等进行导出操作（提供产品功能界面截图并加盖制造商公章）

安全登陆：为确保安全，设备支持登陆次数限制，支持设置登陆异常次数、锁定时间，超过次数限制的 IP 将被加入黑名单一段时间，防止暴力破解。（提供产品功能界面截图并加盖制造商公章）

接入方式：支持配置物理接口为 Trunk 模式，以便于在一个接口传输不同 VLAN 数

据。

网络拓扑：具备直观展示仿真诱捕主机的部署情况，以及仿真诱捕主机与真实主机的对应网络拓扑。

SNMP：支持 SNMP 的 V1、V2C、V3 版本、支持 SNMPTRAP 功能。

被锁定 IP：登陆 IP 锁定可可在界面进行解锁。

产品资质：提供产品的《计算机信息系统安全专用产品销售许可证》（产品专属证书，非复用其他产品证书）；提供产品的《计算机软件著作权登记证书》（产品专属证书，非复用其他产品证书）。

2.8 漏洞扫描要求

★系统性能：任务不限制 IP 数量，并发扫描≥95 个 IP 地址，并发扫描≥13 个扫描任务。

★硬件配置：机架式设备；≥5 个千兆电口，≥2 个千兆光口，≥2 个扩展槽位，硬盘≥1T；配置规则库 3 年升级许可。提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

资产管理：支持资产自动发现功能，支持利用历史扫描过程中所发现的在线主机信息，来添加资产。

漏洞管理：产品漏洞库涵盖目前的安全漏洞和攻击特征，漏洞库具备 CVE、CNNVD、CNCVE、CNVD、BUGTRAQ 编号等信息。（提供产品功能界面截图并加盖制造商公章）

系统检测：支持传统 IT 设备/系统/数据库漏洞检测。（提供产品功能界面截图并加盖制造商公章）

工业控制系统检测：支持扫描西门子、施耐德、Samsung、研华、罗克韦尔、松下、罗杰康、霍尼韦尔等 20 多种制造商的各类工控系统。（提供产品功能界面截图并加盖制造商公章）

扫描策略配置：产品具有无限 IP 漏洞扫描能力。（提供产品功能界面截图并加盖产商公章）

主机存活探测：支持主机存活探测，支持 ARP、ICMPping、TCPping 及 UDPping 四种类型。

扫描功能：支持系统登录验证功能，对提供的帐号密码进行登陆验证以保证扫描器能正常登陆系统。

报表功能：支持最大限度报告漏洞。

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》网络脆弱性扫描类（增强级）（设备专属证书，非复用其他产品证书）；提供产品的《计算机软件著作权登记证书》（设备专属证书，非复用其他产品证书）。

2.9 基线核查系统要求

★性能参数：并发扫描任务数≥14；被检查设备性能影响≤6%，检查结果的误报率≤11%；扫描速率≥24IP/分钟，≥195 个扫描对象 license 授权。

★硬件配置：机架式设备，冗余电源；≥5 个千兆电口，≥2 个千兆光口；≥1T 存储空间。提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

支持检查类型：支持西门子、施耐德等制造商上位机的配置检查；支持工控交换机配置检查。（提供产品功能界面截图并加盖制造商公章）

扫描方式：支持跳板机方式，在线扫描网络不可直达的设备。（提供产品功能界面截图并加盖制造商公章）

扫描方式：支持无资产扫描方式：系统提供密码文件模版下载功能，在建立核查任务时提供导入功能，系统读取设备信息后保存在内存中，在任务执行完毕后销毁，系统自身不存储用户资产信息，保证用户机密数据安全。（提供产品功能界面截图并加盖制造商公章）

配置管理：支持对扫描对象的下列内容进行核查：设备负载、设备配置、设备硬件状态、设备安全性检查、协议运行状态、设备资源情况、软件运行状态。

配置备份：支持对全网设备（如操作系统、网络设备、安全设备、中间件、数据库、大数据组件、虚拟设备等）的 IT 资源相关配置进行自定义周期配置备份。

配置审计：支持在发现异常配置变更后，自动通过邮件、syslog 等多种方式向用户及时预警。

合规审计联动：支持在多任务、多标准情况下，对同一目标设备仅做一次配置采集，

减少对其相应 IT 资源及网络的负载。

自定义检查项：支持对资产的检查项进行自定义添加，包括对于检查类型、检查项权重、脚本命令行、匹配规则、正则表达等项进行自定义。（提供产品功能界面截图并加盖制造商公章）

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》主机安全检查（行标-增强级）（产品专属证书，非复用其他产品证书）；提供产品的《IPv6 Ready Logo 认证证书》（产品专属证书，非复用其他产品证书）；提供产品的《计算机软件著作权登记证书》（产品专属证书，非复用其他产品证书）。

2.10 堡垒机要求

★性能参数：≥95 个主机/设备许可，用户数不限制。

★硬件配置：机架式设备；≥5 个千兆电口，≥2 个千兆光口；≥16G 内存，≥2T 存储空间。提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

认证管理：支持本地认证和三方认证服务器接入认证，如 AD、LDAP、Radius 服务器；支持密码认证、证书认证、USBKEY 认证等双因素认证方式。（提供产品功能界面截图并加盖制造商公章）

资源管理：支持主机、服务器、网络设备、安全设备、数据库等的资产管理。（提供产品功能界面截图并加盖制造商公章）

动态展示：支持首页动态展现资源总量、活动用户、实时会话、待审批工单、当日运维记录、资产运行状态、今日运维总数、今日运维时长 TOP10、今日告警总数、今日运维指令 TOP10 等信息,方便管理员实时查看系统运行情况掌握资产会话连接情况。(提供产品功能界面截图并加盖制造商公章）

设备自动发现：对于设备支持一键更新发现功能。（提供产品功能界面截图并加盖制造商公章）

账号改密：支持改密结果自动发送到制定改密计划的管理员邮箱；密码采用密码信封加密保存，以保证安全性。

会话分享：支持会话请求远程协助，且协同会话保持实时同步。（提供产品功能界

面截图并加盖制造商公章）

图形协议审计：图像审计采用 OCR 图像识别技术，通过加载训练过的运维图片集合，可以识别图形操作中的程序标题、快捷方式标题、窗口内容中的文本信息；

全文检索：支持全文审计检索。可以对操作行为中的用户信息、资产信息、管理地址信息、管理方式信息、操作命令信息、操作结果信息进行全文检索、过滤，极大提高查询效率，更方便的进行用户关联追溯。

审计报表：系统内置丰富报表统计模板：协议运维排名、资产运维次数 top10、资产运维趋势 top10、用户运维趋势 top10、协议运维趋势、用户运维次数 top10、指令分布 top10、top10 指令资产分布、指令用户分布 top10、指令资产账号分布、指令排名、指令趋势、风险指令次数、风险指令 top10 等多种类型报表模板。

虚拟化：支持对堡垒机虚拟为多台逻辑堡垒机，虚拟堡垒机之间实现独立配置、独立数据。实现 IT 资源的动态分配、灵活调度、跨域共享，提高 IT 资源利用率。（提供产品功能界面截图并加盖制造商公章）

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》（产品专属证书，非复用其他产品证书）；提供产品的《IT 产品信息安全认证证书》（产品专属证书，非复用其他产品证书）；提供产品的《计算机软件著作权登记证书》（产品专属证书，非复用其他产品证书）；提供产品的《信息技术产品安全测评证书》EAL3+（产品专属证书，非复用其他产品证书）。

2.11 日志审计系统要求

★性能参数：日志综合采集处理峰值≥3000EPS，日志源授权≥45。

★硬件配置：机架式设备，冗余电源；内存≥16G；硬盘≥4T；≥5 千兆电口,≥4 千兆光口;提供 3 年原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

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、业务系统等不少于 26 类 300 种日志对象的日志数据采集；支持日志归一化处理；

★数据查询：支持基于时间轴展示数据分布，能够通过时间轴进行查询分析。（提供产品功能界面截图并加盖制造商公章）

报表：系统内置上百种报表模版，支持自动实现智能报表创建，每添加一个日志源，系统自动分析日志源类型进行相应报表创建，无需人工干预，报表和资产一一对应。（提供产品功能界面截图并加盖制造商公章）

★限速采集：支持对日志流量非常大但是日志重要程度低的 syslog 类型日志源进行限制接收速率，降低对系统资源的占用，保障重要日志的收集。（提供产品功能界面截图并加盖制造商公章）

数据存储：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。

数据展示：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。（提供产品功能界面截图并加盖制造商公章）

日志查询：支持为不同类型日志设置不同的查询条件和显示条件。（提供产品功能界面截图并加盖制造商公章）

日志源管理：支持对重点日志源的关注设置，并可通过关注列表快速查看重点日志源的状态、当日日志量、采集日志总量、最近接收时间、业务组等基础信息。（提供产品功能界面截图并加盖制造商公章）

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》日志分析（三级）（设备专属证书，非复用其他产品证书）；提供产品的《IPv6 Ready Logo 认证》（设备专属证书，非复用其他产品证书）。

2.12 安防管理工作站要求

★国产品牌。

★处理器：配置 1 颗至强 Xeon-银牌系列以上处理器，不低于 W-2223 四核 3.6G。

内存：配置≥8 个内存插槽，不低于 32G DDR4 2666MHz（2x16GB）。

光驱：≥1 个光盘驱动器。

端口：USB3.0≥6，USB2.0≥2；千兆网卡接口≥1。

★显卡：配置 NVIDIA Quadro 专业图形显卡，不低于 P2000 4G 显存。

硬盘：≥512GB SSD，2TB HDD。

电源：≤500W。

★显示器:不低于 10Bit IPS 面板,尺寸≥27 英寸,分辨率≥3840x2160,≥99%sRGB。

系统：预装 windows 10 正版系统。

提供 3 年质保服务。

2.13 交换机要求

★国产品牌。

★系统性能：整机最大交换容量≥1.28Tbps/11.52Tbps，整机最大包转发率≥252Mpps。

★硬件配置：千兆电口≥48 个，万兆光口≥4，40G 端口≥2 个，冗余电源；提供 3 年原厂硬件维保的售后服务承诺书原件及原厂授权书原件。

安全特性：支持用户分级管理和口令保护；支持 802.1x、AAA、Radius、HWTACACS 等多种认证；支持 IP、MAC、端口、VLAN 的组合绑定；支持防止 DOS、ARP、ICMP 等攻击；支持 IP Source Guard、端口隔离；支持 HTTPs、SSL。

管理和维护：支持 Telemetry 可视化功能；支持零配置 Auto-config 和配置回滚；支持命令行接口（CLI）配置；支持通过 Console、Telnet、SSH 等配置方式；支持 RMON（RemoteMonitoring）；支持 SNMPv1/v2c/v3；支持网管系统；支持 Netconf 和 Python；支持系统日志和用户操作日志；支持分级告警；支持电源、风扇、温度告警功能；支持 NTP 网络时间协议；支持 JumboFrame；支持 Ping、Tracert 等调试信息输出；支持 FTP、TFTP、USB 等方式上传和下载文件；支持 XModem 协议加载升级。

镜像：支持流量镜像；支持 N:4 端口镜像；支持本地镜像和远程端口镜像 ERSPAN。

设备虚拟化：支持 IRF2 横向虚拟化，支持本地和远程堆叠；支持分布式设备管理，分布式链路聚合；支持跨设备链路聚合 DRNI。

网络虚拟化：支持 BGP-EVPN；支持 GRETunnel。

IP 路由：支持静态路由和默认路由；支持 RIP、OSPF、BGP、ISIS 等 IPv4 动态路由协议；支持 RIPng、OSPFv3、BGP4+、ISISv6 等 IPv6 动态路由协议；支持等价路由、策略路由。

2.14 主机加固软件要求

★客户端部署环境：支持 32bit/64bit 的 windows2000/XP/7/8/10 和 windowsserver2003/2008/2012/2016/2019 等操作系统，支持主流 linux 操作系统 Centos、Redhat，支持国产操作系统麒麟、统信和凝思等，安装包应为 msi 格式，无需配置服务器 IP 等参数，一键自动安装。（提供国产操作系统互认证证书，至少包含中标麒麟、银河麒麟互认证证书）

★文件类型：白名单支持的可执行文件和脚本文件类型至少 12 种包括.exe；dll;.ocx;.scr;.sys;.cpl;.ime;.efi;.mui;.tsp;.drv;.bat;.cmd;.js;.vbs;.vbe;.wsf;.wsc;.hta;.pl;.psl;.py。（提供产品功能界面截图并加盖制造商公章）

设备类策略：支持对各类外设进行启用/禁用管理，防止非法/无关外设接入。支持的外设类型应包括：光驱、打印机、调制解调器、网络适配器、图形图像设备、通讯端口、红外设备、蓝牙设备、1394 控制器、PCMCIA 卡、便携设备。（提供产品功能界面截图并加盖制造商公章）

脱壳进程白名单：支持脱壳进程白名单，可自动将脱壳进程释放的可执行文件加入白名单，确保程序正常运行。（提供产品功能界面截图并加盖制造商公章）

安全基线加固：1、支持对工业主机账户策略加固，包括但不限于密码复杂性配置、账号状态配置、账户锁定配置等；2、支持对工业主机审核策略加固，包括但不限于登录事件、对象访问、策略更改、特权使用等；3、支持对工业主机安全选项加固，包括但不限于清除虚拟内存、密码到期提示设置、网络会话保持设备等。（提供产品功能界面截图并加盖制造商公章）″

日志审计：支持安全日志（白名单、外设监控、应用防护、自保护等）审计展示、查询、导出；支持终端操作日志（登录账号、修改密码、创建账号、配置策略等）审计展示、查询、导出；支持实时报警功能，告警方式包括桌面提示框、任务栏气泡等方式。

业务数据保护策略：支持应用程序及文件完整性保护，防止文件或数据被篡改；支持对关键注册表项以及关键配置文件保护，防止被篡改；支持对操作系统完整性保护。（提供产品功能界面截图并加盖制造商公章）

USB 管理策略：支持 USB 移动存储设备的注册和只读、读写、只读执行、读写执行、禁用的细粒度策略管理。

产品资质：提供公安部网络安全保卫局颁发的产品《计算机信息系统安全专用产品销售许可证》文件加载执行控制（产品专属证书，非复用其他产品证书）；提供产品的《IT 产品信息安全认证证书》（产品专属证书，非复用其他产品证书）；提供产品的《计算机软件著作权登记证书》（产品专属证书，非复用其他产品证书）。

2.15 防火墙要求

★系统性能：防火墙吞吐≥11.5Gbps，应用层吞吐量≥9.5Gbps，全威胁吞吐量≥1.2Gbps，最大并发连接数：≥290 万，每秒 HTTP 新建连接速率：≥5.5 万。

★硬件配置：机架式设备，冗余电源；≥5 个千兆电口，≥2 个千兆光口；硬盘≥1T；配置入侵防御功能模块，含 3 年攻击规则库升级许可；配置应用识别功能，含 1 年应用识别特征库升级许可；提供 3 年质保服务。

★访问控制：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认证。（提供产品功能界面截图并加盖制造商公章）

原厂硬件维保和 3 年软件版本升级服务的售后服务承诺书原件及原厂授权书原件。

多系统：支持多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择（提供产品功能界面截图并加盖制造商公章），不得在 WEB 维护界面中设置系统切换选项。

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 StickyNAT 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。（提供产品功能界面截图并加盖制造商公章）

IPV6：支持基于 IPv6 的病毒防御、入侵防御、URL 过滤、ADS、WAF、流量控制、连接限制、文件过滤、数据过滤、邮件安全等。（提供产品功能界面截图并加盖制造商公章）

功能虚拟化：支持配置文件、系统服务、路由、链路聚合、安全策略、NAT 策略、带宽管理、认证策略、IPV6 功能、URL 过滤、病毒过滤、WAF、内容过滤、审计、报表、防代理等安全功能虚拟化。（提供产品功能界面截图并加盖制造商公章）

认证方式：内置强大的用户身份管理系统，支持本地认证、外部认证及免认证等方式，支持 RADIUS、LDAP、TACACS 等第三方外部认证。

DDOS 防御：支持基于 HTTP 协议的检测清洗，包括但不限于：HTTPFlood、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 HTTPslow-header 和 HTTPslow-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。（提供产品功能界面截图并加盖制造商公章）

审计：提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、论坛微博、FTP、TELNET 等；同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等。

系统诊断：支持在 WEB 界面进行网络诊断，支持 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式。

产品资质：提供产品的《计算机信息系统安全专用产品销售许可证》防火墙（增强级）（产品专属证书，非复用其他产品证书）；提供产品的《国家信息安全测评信息技术产品安全测评证书》(EAL4+)（产品专属证书，非复用其他产品证书）；提供产品的《中国国家信息安全产品认证》证书（产品专属证书，非复用其他产品证书）。

2.16 流量镜像交换机要求

★国产品牌。

★系统性能：整机最大交换容量≥205 Gbps。

★硬件配置：千兆电口≥24 个，万兆光口≥8；提供 3 年质保服务。

流量复制：支持 M:N 的复制（M 个源复制到 N 个目的）；支持 Ingress 和 Egress ACL，支持匹配 L2、L3、L4 和 IP 五元组，进行复制、转发、丢弃；支持 VxLAN 和 GRE/NvGRE, 支持匹配内层 L2,L3,L4 和 IP 五元组,进行复制、转发、丢弃；支持匹配 erSpan id，进行复制、转发、丢弃；支持匹配 PBB 报文；支持匹配 UDF（用户自定义字段），进行复制、转发、丢弃；支持匹配 IPv6SA 和 IPv6DA，flow-label 字段，进行复制转发；支持匹配内层 IPv6SA 和 IPv6DA，flow-label 字段，进行复制、转发、丢弃。（提供产品功能界面截图并加盖制造商公章）

报文：支持使用 VLAN Tag 标记入端口；支持 LAG 作为 Ingress 和 Egress 端口；支持时间戳，可根据本地时间作为时间源；支持剥除或者编辑 VLAN Tag；支持报文编辑 MACDA, MACSA 和 IPDA；支持报文编辑 IPSA；支持报文编辑 IPv6SA 和 IPv6DA；支持报文截断；支持基于流的复制。（提供产品功能界面截图并加盖制造商公章）

解封装：支持 GRE 解封装/加封装；支持 NvGRE 封装；支持 ip 解封装；支持 VxLAN 解封装/加

封装；支持 ERSPAN 解封装；支持 ERSPAN 加封装；支持 MPLS 解封装；支持 PPPOE 解封装；支持自定义报文头剥除；支持 web 上配置 udf。（提供产品功能界面截图并加盖制造商公章）

负载均衡：支持基于 Session 的 HASH，同源同宿；支持基于五元组的 HASH；支持基于 VxLAN 和 GRE/NvGRE 内层 MAC/IP 的 HASH；支持基于 MAC 地址的 HASH；支持轮询的负载均衡。（提供产品功能界面截图并加盖制造商公章）

管理：支持四级 CLI 权限控制；支持串口管理；支持 Telnet 管理；支持 SSH 管理；支持 WebUI 管理；支持 SNMP Get；支持 SNMP Trap；支持 OpenAPI。（提供产品功能界面截图并加盖制造商公章）

安全控制：支持 TACAS+；支持 RADIUS；支持本地用户名密码；支持异常用户锁定；支持 ACL 过滤 Telnet/SSH 的登录接入。（提供产品功能界面截图并加盖制造商公章）

三、 设备及服务清单

序号	设备名称	部署位置	单位	数量
1	IDS 入侵检测系统	安全Ⅰ区	台	1
2	IPS 入侵防御系统	安全Ⅱ、Ⅲ区	台	2
3	漏洞扫描系统	安全Ⅰ、Ⅱ、Ⅲ区	套	1
4	防病毒管理系统（含防病毒软件及 3 套管理系统）	安全Ⅰ、Ⅱ、Ⅲ区内主机	套	50
5	防病毒网关	安全Ⅰ、Ⅱ、Ⅲ区	台	3
6	高级可持续威胁安全监测系统	安全Ⅰ、Ⅱ、Ⅲ区	台	3
7	流量分析系统	安全Ⅰ、Ⅱ、Ⅲ区	台	3
8	蜜罐系统	安全Ⅰ、Ⅱ、Ⅲ区	台	3
9	基线检查系统	安全Ⅰ、Ⅱ、Ⅲ区	台	1
10	堡垒机	安全Ⅰ、Ⅱ、Ⅲ区	台	3
11	日志审计	安全Ⅱ、Ⅲ区	台	2
12	主机加固	安全Ⅰ、Ⅱ、Ⅲ区	台	30
13	流量镜像交换机	安全Ⅰ、Ⅱ、Ⅲ区	台	3
14	交换机	安全Ⅱ、Ⅲ区	台	2
15	防火墙	安全Ⅱ、Ⅲ区	台	2
16	安防管理工作站	安全Ⅰ、Ⅱ、Ⅲ区	台	3

17	施工调试及服务	含现有网安设备配置优化，现有网安设备为：1 台日志审计	项	1

第六章 响应文件格式

_____项目采购

响 应 文 件

采购编号：_____

供应商：_____（盖章）

日　期：____年___月___日

目　录

一、授权委托书

本人（姓名）系（供应商名称）的法定代表人（单位负责人），现委托（姓名）为我方代理人。代理人根据授权，以我方名义签署、澄清确认、递交、撤回、修改（项目名称）采购项目响应文件、签订合同和处理有关事宜，其法律后果由我方承担。

委托期限：_____。

代理人无转委托权。

附：法定代表人（单位负责人）身份证复印件及委托代理人身份证复印件

注：本授权委托书需由供应商加盖单位公章并由其法定代表人（单位负责人）签字。

供应商：（单位公章）_____

法定代表人（单位负责人）：（签字）_____

委托代理人：（签字）_____

_____年_____月_____日

注：如供应商法定代表人参加采购行为，只需附其身份证复印件。

二、报价部分

1.报价说明

1.1 本说明应与供应商须知、合同条款等文件一起参照阅读。

1.2 除合同另有规定外，**报价应包括供应商为完成本采购文件采购需求及合同规定的工作所承担的全部费用，包括成本、税金、利润等，并考虑了应由供应商承担的义务、责任和风险所发生的费用**。

1.3 上传 PDF 版响应文件及 Excel 2003 及以上版本电子文档（可编辑版）报价部分文件.

1.4 本采购实行电子商城采购，须上传响应文件和系统填报报价，**请报价人确保系统报价与响应文件报价一致**。如遇系统报价与响应文件报价不一致的情况，最终报价确认原则为两者中最低报价为最终报价；如报价人无法确认最终报价，则视为无效报价。

1.5 响应文件命名格式为：**响应文件-****公司**。

1.6 本项目合同结算方式为**总价包干**，报价须为**全费用综合报价**，分项报价表所列子项为本项目实施主要内容，参与报价供应商报价须根据《第五章-采购需求》具体要求进行综合报价。

2.响应报价表

2.1 报价汇总表（格式）

报价表

单位：人民币元

序号	项目	含税总价	增值税发票类型
1			□提供增值税普通发票； ■提供增值税专用发票。不含税价为：元，税率：13%。
备注：			

供应商名称：____（盖章）____

_____年_____月_____日

2.2 分项报价表

序号	设备名称	单位	数量	单价	总价	备注
1	IPS 入侵防御系统	台	1			安全Ⅱ、Ⅲ区。
2	漏洞扫描系统	台	2			安全Ⅰ、Ⅱ、Ⅲ区
3	防病毒管理系统（含防病毒软件及 3 套管理系统）	套	1			安全Ⅰ、Ⅱ、Ⅲ区内主机
4	防病毒网关	套	50			安全Ⅰ、Ⅱ、Ⅲ区
5	高级可持续威胁安全监测系统	台	3			安全Ⅰ、Ⅱ、Ⅲ区
6	流量分析系统	台	3			安全Ⅰ、Ⅱ、Ⅲ区
7	蜜罐系统	台	3			安全Ⅰ、Ⅱ、Ⅲ区
8	基线检查系统	台	3			安全Ⅰ、Ⅱ、Ⅲ区
9	堡垒机	台	1			安全Ⅰ、Ⅱ、Ⅲ区
10	日志审计	台	3			安全Ⅱ、Ⅲ区。
11	主机加固	台	2			安全Ⅰ、Ⅱ、Ⅲ区
12	流量镜像交换机	台	30			安全Ⅰ、Ⅱ、Ⅲ区
13	交换机	台	3			安全Ⅰ、Ⅱ、Ⅲ区
14	防火墙	台	2			安全Ⅱ、Ⅲ区。
15	安防管理工作站	台	2			安全Ⅰ、Ⅱ、Ⅲ区
16	施工调试及服务	台	3			为完成本采购文件采购需求所涵盖的所有施工调试及服务，包含现有网安设备配置优化。（现有网安设备为：1 台入侵检测，1 台日志审计）
17	**措施费**					按照**第 16 项**费用的 2%计列
17.1	安全防护用具费	项	1			
17.2	安全防护设施费	项	1			
17.3	安全教育培训费	项	1			
17.4	安全标识费	项	1			
	总计					税率 13%

三、商务部分

1. 商务部分摘要表

商务部分摘要表

<table>
<tr><td>供应商名称</td><td colspan="7"></td></tr>
<tr><td>注册地址</td><td colspan="3"></td><td>邮政编码</td><td colspan="3"></td></tr>
<tr><td rowspan="2">联系方式</td><td>联系人</td><td colspan="2"></td><td>电话</td><td colspan="3"></td></tr>
<tr><td>传真</td><td colspan="2"></td><td>网址</td><td colspan="3"></td></tr>
<tr><td>股权结构</td><td colspan="7">XX：A%；
YY：B%；</td></tr>
<tr><td>法定代表人</td><td>姓名</td><td></td><td>技术职称</td><td></td><td>电话</td><td colspan="2"></td></tr>
<tr><td>技术负责人</td><td>姓名</td><td></td><td>技术职称</td><td></td><td>电话</td><td colspan="2"></td></tr>
<tr><td>成立时间</td><td colspan="2"></td><td colspan="5">员工总人数：</td></tr>
<tr><td>企业资质等级</td><td colspan="2"></td><td rowspan="6">其中</td><td>项目经理</td><td colspan="3"></td></tr>
<tr><td>营业执照号</td><td colspan="2"></td><td>高级职称人员</td><td colspan="3"></td></tr>
<tr><td>注册资本金</td><td colspan="2"></td><td>中级职称人员</td><td colspan="3"></td></tr>
<tr><td>开户银行</td><td colspan="2"></td><td>初级职称人员</td><td colspan="3"></td></tr>
<tr><td>账号</td><td colspan="2"></td><td>技工</td><td colspan="3"></td></tr>
<tr><td>经营范围</td><td colspan="7"></td></tr>
<tr><td>类似业绩列表</td><td colspan="7"></td></tr>
<tr><td>备注</td><td colspan="7"></td></tr>
</table>

按照采购文件要求后附企业法人营业执照副本、资质证书（如要求）、安全生产许可证（如要求）、类似业绩（如要求）合同扫描件等资料影印件。

供应商全称：_____（盖章）_____

日　　期：_____

2.法人营业执照

3.近 3 年内财务状况

4.付款条件

5.类似项目业绩合同（如要求）

6.商务偏离表及配套性说明

7.资质证书及其他证明材料（**请按照采购文件供应商专用资格要求及采购需求部分内容要求进行提供**）

四、技术部分

（根据采购需求编制，格式自拟，需包含**技术方案、方案设计、设备设施及相关软硬件参数/授权书、主要人员组成表等相关材料**）。

五、偏差表

序号	采购文件（条目及简要内容）	响应文件（条目及简要内容）	备注
1			如无偏差，需写：“无”；有偏差，须如实填写。
2			
3			
4			