中国南方电网
CHINA SOUTHERN POWER GRID

防火墙技术规范书

贵州电网贵龙创新发展有限责任公司

目 录

1. 总则 4
2. 质量及安全保证 6
3. 项目综述 6
4. 技术要求 8
5. 保密要求 12
6. 验收 12
7. 技术文件要求 12
8. 监造、包装、运输、安装及质量保证 13
9. 现场服务及售后服务 14

1. 总则

本技术规范为防火墙技术规范。投标方必须仔细阅读本技术规范的所有条款，以中文逐条做出明确答复（点对点应答）并给出相关技术指标偏差，提供技术建议书，提交设备配置清单及相关产品详细说明文档，及具体实施计划等附件资料。

本技术规范描述了所需专用设备的技术参数，定义安装、测试和验收的细节和规范，明确对投标方在售后服务、培训服务、技术文档方面的要求，供投标方编写建议书和报价之用（建议书的内容格式应符合本规范书的要求）。投标方应针对自己的特点，根据本规范所描述的专用设备的具体要求，提供符合要求的产品。

本技术规范适用于防火墙项目**的物资采购、验收调试、交付、现场安装和试验的指导、监督以及试运行工作**。现场安装和试验在招标方的指导和监督下由投标方完成。

本技术规范所描述的各种功能、性能需求仅供投标方编制投标文件之用。投标方可以提出不同的建议方案，但是建议方案必须满足但不限于本标书所阐述的全部技术功能要求。

本标书仅描述基本的技术需求，不保证对一切技术细节做出规定，也不保证已充分引述有关标准和技术条文，投标方须根据需求目标提供进一步具体的可满足要求的功能和性能指标。

本招标技术文件经买、卖双方确认后作为订货合同的技术附件，与合同正文具有同等法律效力。

投标方应具备在贵阳当地服务提供能力。同时，软件原厂商应提供书面承诺，保证如中标方不能履行合同时，由原厂商无条件继续履行，且承担相应法律、商务及技术责任。

投标方所提供的组件或附件如需向第三方外购时，投标方应对质量向招标方负责，并提供相应出厂和验收证明。

招标方针对投标方所提供的技术服务质量将在中标后的产品供货、项目实施、验收、运行维护支持等阶段工作中进行考核评价，并将会把该考核评价结果计入下一年度的设备招标评价中，投标方应确保针对本次招标的服务承诺为真实可信的承诺标准，否则招标方保留进行追责和索赔的权利。

投标方提供的产品具有先进性、可靠性和可扩展性，并具有较高的性能价格比。

投标方提供的各项软件产品的特点、性能应完全符合招标方指明的标准，并满足或高于招标方提出的要求。

如果投标方提供的产品与本招标技术条件书的要求有差异，应在投标书中以“技术偏差”为标题的专门章节中加以详细描述。投标方如不能满足本招标技术条件书的要求部分，也应在技术建议书中提出说明。

招标采购单位在任何时候发现投标人提交的投标文件内容有下列情形之一时，将取消其投标或中标资格，并保留进一步依法追究投标人责任的权利：

1)提供虚假的资料（包括但不限于投标人在其投标文件中提供虚假的资格证明文件、业绩证明文件、剩余生产能力表、试验报告等）；

2)在实质性方面失实（包括但不限于投标人在其投标文件中提供的产品技术参数等与事实不符或虚假应答等）。

投标方建议的技术方案及软、硬件系统配置应符合有关标准(例如 ISO 标准、IEC 标准、ITU-T 建议、GB 标准和 IETF 建议等)，投标方若不作说明，则视为符合上述标准。若投标方的设备包含有自己专用标准，应在项目建议书中具体说明，并附上相应的详细的技术资料。

投标方应承诺所提供的设备本身不能有任何安全隐患，对此应承担终身责任。任何由产品安全引起的招标方的信息安全事件，投标方应承担连带责任。

本招标技术条件书应视为保证系统运行所需软件产品与服务的最低要求，如有遗漏，投标方应予以补充，否则一旦中标将认为投标方认同遗漏部分并免费提供。

对于有授权使用数量限制的软件，投标方应书面标出其基本配置可以合法使用的安装用户数量、使用级别和并发用户使用数量及单价，详细说明每个模块授权数量的价格计算方法，以后再增加用户数的价格计算方法，以及各种用户权限数之间的关系。若投标方没有明确表述告知或对招标方隐瞒，造成招标方少配、漏配、错配，导致授权数量、具体使用权限方面的版权纠纷，投标方应付全部责任。

投标方未经招标方同意，不得以任何形式向第三方公开本招标技术条件书。

本招标技术条件书未尽事宜，由招投标双方在合同履行阶段协商确定，或以其他招标文件（如合同模板，下同）规定为准；与其他招标文件冲突的，以本技术规范书为准；与其他招标文件同类要求标准不一致的，以标准较高为准。

本招标技术条件书解释权属招标方所有。

2. 质量及安全保证

投标方应保证制造过程中的所有工艺、材料等（包括投标方的外构件在内）均应符合协议书的规定。若招标方根据运行经验指定中标方提供某种外购零部件，中标方应积极配合。

中标方提供的任何固件和软件不得存在漏洞和后门。

中标方所提供固件和软件的原制造商应提供补丁支持。

中标方或中标方所提供固件和软件的原制造商发现缺陷，应在发布补丁程序后一周内向招标方提供补丁程序。

招标方发现中标方所提供固件和软件存在缺陷，原制造商应在接到招标方通知之日起 1 个月内提供相应的补丁程序。

中标方要确保供货范围完整，需满足本技术规范的供货要求及技术、功能、性能等要求，并以能满足用户安装、运行要求为原则。若签订合同后，在安装、调试、运行中发现缺项，则由中标方负责免费补充。

3. 项目综述

3.1 项目目标

本次项目建设目标：

满足网络安全边界合规要求：依据等级保护政策、标准、指南等文件要求以及业务安全需求，对不同的保护对象构建集检测、处置、响应能力于一体的安全区域边界，满足《南方电网电力监控系统网络安全全域防御与纵深防御体系建设工作方案》要求。

3.2 投标方应遵循的标准

项目建设应遵循国家标准、电力行业标准、工信部、南方电网公司颁布的标准（包括标准、制度、规范、管理办法）开展本项目工作，本项目所有成果应符合上述标准要求。所用的标准必须是最新版本，如果这些标准的内容有矛盾时，应按照最高标准的条款执行或按双方协商同意的标准或条款执行。

相关标准包括但不限于以下：

(1)《中华人民共和国网络安全法》

(2)《中华人民共和国密码法》

(3)《中华人民共和国数据安全法》

(4)《关键信息基础设施安全保护条例》

(5)《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令147 号）

(6)《电力监控系统安全防护规定》（国家发展和改革委员会令 2014 年第 14 号）

(7)《电力监控系统安全防护总体方案》（国能安全〔2015〕36 号）

(8)《电力监控系统安全防护评估规范》（国能安全〔2015〕36 号）

(9)《电力行业信息安全等级保护管理办法》（国能安全〔2014〕318 号）

(10)《电力行业网络安全管理办法》（国能发安全规〔2022〕100 号）

(11)《电力行业网络安全等级保护管理办法》（国能发安全规〔2022〕101 号）

(12)《信息安全等级保护管理办法》（公通字〔2007〕43 号）

(13)《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）

(14)《信息安全技术网络安全等级保护定级指南》（GB/T 22240-2020）

(15)《信息安全技术网络安全等级保护实施指南》（GB/T 25058-2019）

(16)《信息安全技术网络安全等级保护测评过程指南》（GB/T 28449-2018）

(17)《信息安全技术网络安全等级保护测评技术要求》（GB/T 28448-2019）

(18)《信息安全技术信息安全风险评估规范》（GB/T 20984-2016）

(19)《关于加强工业控制系统信息安全管理的通知》（工信部协〔2011〕451 号）

(20)《中国南方电网电力调度管理规程》（Q/CS212045-2011）

(21)《中国南方电网电力监控系统网络安全技术规范》

(22)《中国南方电网电力监控系统网络安全管理办法》（Q_CSG2072003-2021）

这些标准提出了最基本要求，如果根据投标方的意见并经招标方接受，使用优于或更为经济的材料和服务，并能使投标方良好地、连续地在本规范所规定的条件下运行时，则这些标准也可以由投标方超越。

当标准、规范之间出现矛盾时，以较高标准执行，同时投标方应将矛盾情况提交招标方。

4. 技术要求

标★为确保本次中标方所投标的产品满足标书的相关技术要求，招标方有权将中标方的产品送交第三方检测机构进行检测，所投标产品需提供所投产品原厂商加盖公章的承诺函。

4.1 使用条件

(1)正常工作大气条件

1. 环境温度：-10℃～+55℃；

2. 相对湿度：5%~95%（产品内部既不应凝露，也不应结冰）；

3. 大气压力：80kPa～106kPa。

(2)贮存、运输环境条件

1. 装置在运输中允许的环境温度-40℃～＋70℃，相对湿度不大于85%；

2. 在贮存中允许的环境温度-25℃～＋55℃，相对湿度不大于85%，在不施加任何激励量的条件下，装置不出现不可逆变化。

4.2 性能要求

以下性能要求中，标注“★”的条款为重要性能参数，须提供原厂商加盖公章的承诺函（招标方保留功能测试查验权利），评标过程中将重点关注。

产品类型	指标项	参数要求
防火墙	规格配置	★1. 自主可控要求：采用国产化操作系统及CPU 2. 标准机架式设备，内存≥8G，硬盘容量≥480G SSD，接口接口≥6千兆电口+2千兆光口SFP，USB接口≥2个冗余风扇设计；
	性能要求	★网络层吞吐量≥10G，应用层吞吐量≥4G，防病毒吞吐量≥1G，IPS吞吐量≥2G，并发连接数≥400万，HTTP新建连接数≥10万； 3、实配：双交流电源，5年IPS、AV、URL特征库升级授权，内存8G\256G固态硬盘。

4.3 功能要求

以下功能要求中，标注“★”的条款为重要功能参数，须提供原厂商加盖公章的承诺函（招标方保留功能测试查验权利），评标过程中将重点关注。

产品类型	指标项	参数要求
防火墙	功能要求	1.支持自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能 2.支持协议类型、网络对象、国家地区等条件进行自动选路的策略路由 ★3.具备基于国家/地区的流量管理功能（需提供产品功能截图和具备CMA/CNAS标识的第三方检测报告关键页证明） 4.支持基于网络区域、网络对象、MAC地址、服务、应用、域名等维度进行访问控制策略设置 ★5.产品支持CC攻击防护功能，保障针对CC攻击的检测效果（需提供产品功能截图和具备CMA/CNAS标识的第三方检测报告关键页证明） 6.支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御 ★7.产品内置超过4000种WEB应用攻击特征，支持对跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等攻击类型进行防护。（需提供产品功能截图和具备CMA/CNAS标识的第三方检测报告关键页证明） ★8.产品内置不低于16000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则（需提供产品功能截图和具备CMA/CNAS标识的第三方检测报告关键页证明） ★9.产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁（需提供产品功能截图和具备

		CMA/CNAS 标识的第三方检测报告关键页证明） 10.支持 https 解密功能，支持 TCP 代理和 SSL 代理 ★11.产品支持 Cookie 攻击防护功能，并通过日志记录 Cookie 被篡改。（需提供产品功能截图和具备 CMA/CNAS 标识的第三方检测报告关键页证明） 12.产品应具备独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略，支持在设备首页独立展示勒索风险板块。（需提供产品功能截图证明） ★13.产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过 120 万种，可识别主机的异常外联行为（需提供产品功能截图和具备 CMA/CNAS 标识的第三方检测报告关键页证明） ★14.产品支持 X-Forworded-For 字段检测，并对非法源 IP 进行日志记录和联动封锁（需提供产品功能截图和具备 CMA/CNAS 标识的第三方检测报告关键页证明） 15.产品内置蜜罐诱捕服务，在防火墙上部署一些作为诱饵的伪装业务，诱捕内外网的攻击行为，并联合分析技术溯源和反制，在设备界面可以看到攻击者列表，包含攻击者 IP、危险等级、攻击源、地理位置、社交指纹、影响真实业务、攻击次数、最高攻击时间、最近攻击时间（需提供产品功能截图证明） ★16.产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理（需提供产品功能截图和具备 CMA/CNAS 标识的第三方检测报告关键页证明） ★17.主机故障时，双机切换时不丢包，并可实现双机部署下升级不断网（需提供产品功能截图和具备 CMA/CNAS

		标识的第三方检测报告关键页证明） 18.产品支持三权分立功能，根据管理员权限分为安全管理员、审计员、系统管理员三种角色。 19.★产品支持管控非法、违规网站的访问行为，具备海量的URL分类库。（需提供产品功能截图证明） 20.支持记录全量访问日志、安全防护日志、设备运行日志、安全审计日志等记录，详细记录日志详情，包括五元组信息、告警信息等。

4.4 安全要求

产品类型	指标项	参数要求
防火墙	安全性要求	★1、投标设备具有中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》。 ★2、投标设备具有中国信息安全测评中心颁发的《国家信息安全测评信息技术产品安全测评证书 EAL4 增强级》及以上标准的证书。 ★3、投标设备厂家为CNVD用户组和工作组成员，提供相关证明材料。

中标方提供的任何固件和软件不得存在漏洞和后门。

中标方所提供固件和软件的原制造商应提供补丁支持。

中标方或中标方所提供固件和软件的原制造商发现缺陷，应在发布补丁程序后一周内向招标方提供补丁程序。

招标方发现中标方所提供固件和软件存在缺陷，原制造商应在接到招标方通知之日起1个月内提供相应的补丁程序。

投标方及其产品和服务的提供者须承诺不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备。无正当理由不中断产品供应或必要的技术支持服

务等。

5. 保密要求

供需双方均应承担保密责任，在项目实施过程前双方应签订保密协议，明确双方责任义务。在项目实施过程中，双方需要复制对方提供的相关资料时，应提交书面申请，在得到对方书面同意后方可复制，并将数据内容记录成表，签字确认。未经双方书面同意，不得向第三方透露项目和涉及双方企业信息安全、技术成果的任何内容。项目结束后，双方必须互相确认测评过程中提供的相关资料，相互承担保密责任。

6. 验收

验收分为到货验收、功能验收。所有验收工作由甲方组织进行。

6.1 到货验收

1)设备和技术文件到达交货地点后，甲、乙双方共同对其进行检查，并认真做好交接记录，各方签字。确保软件产品和技术文件的数量、名称与合同要求的清单核实无误。

2)甲方如发现乙方所提供产品的规格、数量等与合同规定不符，乙方须按合同要求更换或是补足与合同不符的或是短缺的产品，并承担由此而产生的一切费用。

3)所进行检查的结果符合合同中的规定时，由甲、乙双方共同签署到货验收报告。

6.2 功能验收

1)到货验收完成后，乙方须完成合同产品的安装、调试等工作。确保乙方提供的软件产品功能与合同要求内容一致，且能稳定、可靠的运行使用。

2)若验收内容均达到验收标准，则功能验收通过，乙方须撰写并提交功能验收报告，并将所有系统配置的有关资料整理移交甲方，甲、乙双方共同签署功能验收报告。

7. 技术文件要求

投标方提供的技术文件包括：

1)实施安装、调试、测试、验收、培训阶段的文件、图纸，及设备操作维护手册等。

2)每次维护（包括硬件及软件）的维护报告及技术文档。

3)投标方采购供货的第三方设备的技术手册及相关资料。

4)投标方应对其所提供的全部文档的准确性和完整性负责。所有由投标方采购供货的第三方设备的技术手册的准确性由投标方负责。

5)设备应附有完整的、装订好的安装图和说明手册，随设备装箱一起运至现场。

6)投标方至少提供技术文件资料电子版1份，纸质形式打印稿2份。文字部分采用Microsoft Office 2003格式（包括Word,Execel,PowerPoint等文件格式），图纸部分采用AUTOCAD R14/2000或 Visio 2003格式。

8.监造、包装、运输、安装及质量保证

1)设备制造完成并通过试验后应及时包装，否则应得到切实的保护，确保其不受污损。

2)所有部件经妥善包装或装箱后,在运输过程中尚应采取其它防护措施,以免散失损坏或被盗。

3)在包装箱外应标明需方的订货号、发货号。

4)各种包装应能确保各零部件在运输过程中不致遭到损坏、丢失、变形、受潮和腐蚀。

5)包装箱上应有明显的包装储运图示标志(按GB/T 191-2008)。

6)整体产品或分别运输的部件都要适合运输和装载的要求。

7)随产品提供的技术资料应完整无缺。

8)订购的新型产品除应满足本招标技术文件外， 投标方还应提供产品的鉴定证书。

9)投标方应保证制造过程中的所有工艺、材料等（包括投标方的外购件在内）均应符合本招标技术文件的规定。若招标方根据运行经验指定投标方提供某种外购零部件，投标方应积极配合。

10)投标方应遵守本招标技术文件中各条款和工作项目的ISO9000、GB/T19000质量保证体系，该质量保证体系已经过国家认证和正常运转。

11)投标方并应做出承诺保证。在质保期内，免费进行维修、更换损坏设备以及对设备和软件的维护等。在质保期内，应提供7×24小时的服务；如发生设备或部件硬

件故障，应该承诺在3个工作日内完成备件的更换，本项要求的满足情况将作为评标的重要依据之一。

12)柜内的各种元件,应选择具有生产许可证的专业制造厂家的产品。

13)交货期：合同签订后30个工作日。

14)交货地点：项目建设单位所在地。

9.现场服务及售后服务

9.1现场服务要求

1)投标方应派出足够的技术人员到现场负责安装、调试、测试、验收、试运行，并负责解决合同设备制造及性能等方面的有关问题，详细解答合同范围内招标方提出的问题。

2)在产品质保期内有制造质量的设备，由投标方负责修理或更换。对非投标方责任造成的设备损坏，投标方有优先提供配件和修理的义务。

3)对招标方选购的与本合同设备有关的配套设备，投标方有提供技术配合的义务，并不由此而增加任何费用。

4)投标方到招标方现场进行设备安装及维修人员必须为其正式员工。

5)现场工作过程中，现场服务人员应保持固定，除非获得项目单位允许，否则供应商不可对人员进行调整。

9.2售后服务要求

1)在承诺的质量保证期内，投标方应提供7×24小时的技术支持服务，提供固定的技术负责人及联络电话。

2)质保期内硬件故障时，投标方必须在用户提出维护要求的4小时内作出响应，所提供的替代硬件设备的性能应等于和高于原产品的性能，24小时内故障应得以解决。

3)在承诺的质量保证期内，投标方应免费提供系统软件升级、培训、设计联络、技术服务。

4)在用户发现软件故障时，投标方必须在用户提出维护要求的2小时内作出响应，12小时内提交故障分析报告和解决方案，24小时内故障得以解决。