



2025 年网络安全技术防护(网络安全软硬件 采购)项目(万兆级流量探针(日志分析与 管理系统采集节点))技术条件书

深圳供电局有限公司

2025 年 7 月

目 录

1 工作范围	3
1.1 供货范围	3
1.2 服务界限	4
1.3 服务期限	4
2 引用标准	4
3 技术要求	5
3.1 万兆级流量探针（日志分析与管理系统采集节点）（3 个）	5
4 资料管理	7
4.1 文档范围	7
4.2 投标方的责任	7
4.3 随机手册	7
4.4 文档种类	7
4.5 其它	7
5 售后服务及技术培训	8
6 质量保证	9
7 试验与调试	10
7.1 验收要求	10
7.2 测试报告	10
7.3 现场调试和现场试验（SAT）	11
7.3.1 现场调试	11
7.3.2 现场试验	11
8 技术性能偏差表	11
9 投标方需说明的其他问题	11

总则

1.1 本技术条件书适用于深圳供电局有限公司 2025 年网络安全技术防护（网络安全软硬件采购）项目采购，以及相关设备的功能、性能、安装等方面的技术要求。

1.2 本技术条件书提出的是最低限度的技术要求，并未对一切技术细节做出规定，也未充分引述有关标准和规范的条文，投标方应提供符合本技术条件书和工业标准的优质产品。

1.3 如果投标方没有以书面形式对本技术条件书的条文提出异议，则意味着投标方提供的设备(或系统)完全符合本技术条件书的要求。如有异议，不管是多么微小，都应在报价书中以“对招标技术文件的意见和同招标技术文件的差异”为标题的专门章节中加以详细描述。

1.4 本技术条件书所使用的标准如遇与投标方所执行的标准不一致时，按较高标准执行。

1.5 本技术条件书经招、投标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。

1.6 投标方在应标技术文件中应如实反映应标产品与本技术条件书的技术差异。如果投标方没有提出技术差异，而在执行合同的过程中，招标方发现投标方提供的产品与其应标技术文件的条文存在差异，招标方有权利要求退货，并将对下一年度的评标工作有不同程度的影响。

1.7 投标方应在应标技术部分按本技术条件书的要求如实详细的填写应标设备的标准配置表，并在应标商务部分按此标准配置进行报价，如发现二者有矛盾之处，将对评标工作有不同程度的影响。

1.8 投标方应充分理解本技术条件书并按本技术条件书的具体条款、格式要求填写应标的技术文件，如发现应标的技术文件条款、格式不符合本技术条件书的要求，则认为应标不严肃，在评标时将有不同程度的扣分。

1.9 本技术条件书未尽事宜，由招、投标双方协商确定。

1 工作范围

1.1 供货范围

本技术条件书要求采购的深圳供电局有限公司 2025 年网络安全技术防护（网络安全软硬件采购）项目采购供货范围包括：

设备名称	数量
万兆级流量探针（日志分析与管理 系统采集节点）	3 个

1.2 服务界限

从生产厂家至招标投标方应选派有经验的技术人员，对安装和运行人员免费培训方指定交货点的运输和装卸全部由投标方完成；

现场安装和试验在投标方的技术指导和监督下由招标方完成，投标方协助招标方按标准检查安装质量，处理调试投运过程中出现的问题。

1.3 服务期限

自合同生效之日起至 2026 年 6 月 30 日。

2 引用标准

除本招标书另有说明外，投标方提供的所有设备均应按照下列标准进行设计、制造、检验和安装。所用的标准必须是最新版本。如果这些标准的内容有不同之处时，应按照最高标准的条款执行或按双方协商同意的标准执行。如果投标方选用本条件书以外的标准时，需提交这种替换标准相当于或优于本条件书规定的标准的说明。标准如下：

- （1）ISO-----国际标准化组织标准
- （2）IEC-----国际电工委员会标准
- （3）ITU-T----国际电信联盟标准
- （4）IEEE-----美国电气电子工程师协会标准
- （5）EIA-----电子工业协会标准
- （6）GB-----中华人民共和国国家标准
- （7）DL-----中华人民共和国电力行业标准
- （8）《电力二次系统安全防护规定》
- （9）CCITT -----国际电报和电话咨询委员会
- （10）ITU-----国际电信联盟。
- （11）UL-----美国保险商试验室标准。
- （12）NFPA -----美国国家防火协会标准。
- （13）SI-----标准国际单位制。
- （14）NEMA-----美国国家电气制造协会标准。
- （15）ANSI
- （16）其它招标方指定的规约

3 技术要求

其中★项目为关键参数。▲项目为重点评分项，如优于指标要求需提供证明材料并加盖公章。

1、★本项目采购的设备须满足自主可控要求，满足 IPv4/IPv6 协议双栈要求，提供承诺函。

2、★产品到货后按照国家及南网的要求，如需开展系统入网安评、商用密码应用安全性评估、信息系统安全等级测评及备案等合规性审查工作，以及如需开展数认平台、统一密码平台等安全管控系统接入集成工作，涉及相关系统集成及网络安全测评费用且无其他相关项目支撑的，由投标方承担所投产品的集成与测评费用，提供承诺函。

3、★采购设备在并网投运时应确保不存在弱口令风险，在维保期内发现弱口令风险应按合同和技术协议要求整改，提供承诺函。

4、参数指标

3.1 万兆级流量探针（日志分析与管理系统采集节点）（3个）

指标项	指标子项	指标要求
硬件规格	硬件要求	▲CPU≥（16 核心 32 线程,主频 2.5GHz）、内存≥64G（总容量）DDR4；硬盘≥4TB 企业级 SATA3.5 寸硬盘；电源：冗余双电源；千兆电口≥2 个，万兆光口≥2 个（含两个 SFP+ 多模光模块）
系统兼容性	安全事件信息发送	▲支持与 SOC 平台无缝融合，能够按照固定格式将安全事件、预警信息通过 API 传递给 SOC 平台
功能要求	旁路部署	支持通过流量镜像的方式旁路部署在虚拟化网络中，实现网络流量数据采集、威胁检测和日志外发，支持通过重置会话的方式阻断 TCP 威胁会话连接，支持通过流量被动识别资产。
	流量采集	采集过滤条件支持但不限于源地址、目的地址、服务、流量采样比、时间等；
		需支持空载荷过滤，支持对采集的流量的上下行载荷长度设置；（提供功能截图证明）
		支持离线采集，可通过手动 PCAP 导入或 FTP 等协议批量上传导入等方式对离线流量进行采集（提供功能截图证明）
	流量识别与解析	支持精准识别通讯类、语音类、视频类、更新类、下载类、邮件类、金融类、理财类等多类别的应用识别，应用识别库 3000+。
		支持 Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2 等数据库行为的解析；
		支持 WebMail、SMTP、POP3、IMAP 邮件行为解析；
		支持如 ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp 的登录动作解析
	文件还原	支持还原多种文件传输协议，包括：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB、TFTP、QQ；
		支持多种文件类型的筛选，可执行文件还原格式包含：bin、

		exe、bat、dll、sys、com、ax、acm、drv 等；压缩文件还原格式包含：rar、zip、gz、7z、tar 等；文档类型的还原格式包含：doc、docx、xls、txt、pptx、pdf、rtf、ppt 等。
	威胁检测	系统具备全面的间谍软件检测能力，可检测常见的病毒蠕虫、僵尸网络、黑市工具、勒索软件、挖矿木马、隧道、代理通道、后门程序、远控木马等
		系统具备全面的漏洞检测能力，可检测常见的溢出攻击、跨站脚本、SQL 注入、拒绝服务、跨站请求伪造、目录遍历、webshell 上传等
		系统支持 Flood 攻击检测，包括 SYNflood、ICMPflood、UDPFlood 和 IPFlood；支持应用层 Flood 攻击检测，包括 DNSFlood 和 HTTPFlood。
		系统需支持按照协议类型对攻击事件规则的设置检测有效性，协议类型包括 HTTP、DNS、FTP、ICMP、IMAP、IRC、Mongodb、NNTP、POP3、RIP、RLOGIN、SMTP、SNMP、TDS、TELNET、TFTP、TNS 等
		系统提供的攻击特征不应少于 10000 条有效最新攻击规则，特征库需支持自动及手动升级
		系统需具备专业的查毒引擎，独立的病毒库，支持通过对 HTTP、FTP、SMTP、POP3、IMAP、SMB、TFTP、NFS 协议进行恶意文件检测。
		支持恶意文件例外，对指定特征的恶意文件及文件类型不进行查杀。
		具有云端检测能力，并支持云端沙箱检测
		漏洞与间谍软件需支持 HTTP 协议攻击特征自定义，提供 rsp_headers、req_headers、rsp_body、req_body、req_first_line 等协议变量特征的自定义，支持设置协议变量的操作符，操作符包括等于、包含或通过正则表达式设置；
	SSL 旁路解密	支持灵活配置外发策略，日志类别可配置
		▲传输模式支持加密、压缩、以及认证，认证包括但不限于 kerberos 认证、LDAP 认证。（提供功能截图证明）
		外发类别支持但不限于流量日志、威胁日志、资产日志、样本文件、威胁相关 pcap 等
		▲持基于 SSL 协议的 SMTPS、POP3S、IMAPS、HTTPS 流量进行解密，可添加基于源目的地址及端口的过滤条件。（提供功能截图证明）
		支持解密后的明文流量镜像至下游设备。（提供功能截图证明）
	资产识别	系统具有资产识别能力，能够根据流量识别资产的操作系统、服务、开放端口、banner 信息等；
		支持资产识别范围配置、支持资产识别展示及导出
	网络配置	支持 ipv4/ipv6 双协议栈，接口支持 IPv4、IPv6 配置，支持 IPv4、IPv6 流量接入，支持对 IPv4 路由监控和对 IPv6 路由监控。
	业务统计和状态监控	支持失陷主机、恶意文件检测、漏洞攻击检测的数量统计。
		基于应用维度的 TOP5、TOP10 的 24 小时/7 天的实时流量统计和可视化展示。
		基于接口维度的发送、接收和总数的实时流量统计和可视化展示
		支持监控系统 CPU 状态（使用率、温度）。

	安全管理	支持 HTTP、HTTPS、Telnet、远程 SSH 等多种管理方式，用户可自定义修改管理端口
		支持可信主机和可信 MAC 功能，仅可信地址可访问该设备
		支持用户自定义系统管理的安全级别，包括登录超时时间、密码有效期、密码长度、密码复杂度、登录安全策略、登录失败次数锁定、登录失败间隔、账号锁定时间，锁定方式等。
	配置文件管理	支持配置文件的导入、导出。支持基于本地、FTP 和 TFTP 的配置文件导出，导出的配置支持加密。
	证书管理	支持导入可信 CA 和证书；支持生成证书请求文件
		支持本地生成自签发 CA 或导入第三方 CA，支持生成一般证书与证书审批
	二次开发接口	▲系统提供二次开发接口，接口形式为 RestfulAPI，提供功能配置、统计等接口；（提供功能截图证明）

4 资料管理

4.1 文档范围

- 1) 投标方提供的文档包括系统技术资料、维护手册、培训资料、和用户手册等。
- 2) 提供的文档还应包括由投标方采购供货的第三方设备的软件的技术手册及相关资料。

4.2 投标方的责任

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。

4.3 随机手册

对每一设备都应有完整的、装订好的安装图和说明手册，随设备装箱一起运至现场。

4.4 文档种类

投标方必须至少提供以下文档（所有文档提供电子文档一份）：

项目	说明	数量
1	用户使用手册	1
2	系统维护手册	1
3	系统功能说明手册	1
4	系统安装和配置手册	1
5	系统测试手册	1

4.5 其它

在投标方定购设备到货后，投标方应立即准备以下文档各 1 份交给招标方：

- 1) 全部订购系统的型号、技术特点和性能参数清单。
- 2) 所有主要部件和连接线缆的材料规格。

5 售后服务及技术培训

5.1 软件类系统技术服务要求

- 1) 提供 3 年的原厂安全和性能补丁服务；
- 2) 提供 1 年原厂标准服务，包含：
 - 提供 7×24 小时技术支持服务，指定相对固定的技术负责人及联络电话、传真、e-mail 等。
 - 在用户发现软件缺陷时，投标方必须在用户提出维护要求的 2 小时内作出响应，24 小时内提交故障分析报告和解决方案，48 小时内故障得以解决。
 - 重大软件故障时，投标方应在接到故障电话后 4 小时到达现场，24 小时内修复故障。
 - 在有新的系统补丁或升级版本时，在征得用户同意的情况下可进行升级或打补丁。由于未提供给用户补丁或升级而引起的运行故障由投标方负责一切后果。

5.2 硬件类系统技术服务要求

- 1) 提供 3 年的设备保修服务；
- 2) 提供 1 年原厂标准服务，包含：
 - 提供 7×24 小时技术支持服务，指定相对固定的技术负责人及联络电话、传真、e-mail 等。
 - 在用户发现系统缺陷时，投标方必须在用户提出维护要求的 2 小时内作出响应，24 小时内提交故障分析报告和解决方案，48 小时内故障得以解决。
 - 重大系统故障时，投标方应在接到故障电话后 4 小时到达现场，24 小时内修复故障。
 - 在有新的系统补丁或升级版本时，在征得用户同意的情况下可进行升级或打补丁。由于未提供给用户补丁或升级而引起的运行故障由投标方负责一切后果。

5.3 技术培训

- 1) 投标方应由资深系统研发专家为招标方的技术人员开设现场培训课程。招标方的技术人员应在安全防护设备的部署、运行维护等各方面得到培训，熟悉和掌握运行、检查、修理和维护相关安全防护设备并掌握软件开发工具。

- 2) 投标方应向受训人员提供技术资料、图纸、参考材料、培训手册等；还应提供测试设备、工具和安全设备，以及其它必需品和工作场地。
- 3) 投标方应提出对受训者最为有利的培训计划(包括培训时间、地点、内容)。
- 4) 投标方应向招标方提交培训时间表和课程表，投标方应定出培训大纲，培训大纲和计划应提交招标方确认，根据招标方实际运行需求进行修改。
- 5) 免费提供培训，甲方选派人员参加；培训内容为相关系统的现场安装、调试、维护、使用、故障诊断等；

5.4 中标人须为合同产品提供硬件 3 年、软件 1 年原厂技术支持和服务和软件 3 年安全及性能补丁更新服务，投标时须提供原厂服务承诺函。

5.5 在系统频繁出现故障、或遇重大节假日等特殊情况下，需要提高系统维护等级的情况下，应招标人要求，应提供技术人员提供现场技术支持，及时处理各类故障。

5.6 一旦发现系统运行不稳定，而与合同产品有关，须免费提供合乎原厂商规定的合同产品的更新或版本升级，或对系统进行维修、维护，直至问题得到解决。

5.7 免费进行必要的软件更新和版本升级。当招标人准备对合同产品进行升级或扩容时，须提供咨询服务，并提交相关方案。

5.8 向招标人提供合同产品相关的新技术的日常技术咨询服务。

5.9 系统发生搬迁时，中标人须派遣专业技术人员现场支持，免费提供合理、可行的搬迁技术方案给招标人并保证搬迁后系统的正常运行。

5.10 提供免费实施，投标方所投标价格中需要包含系统的安装部署。

5.11 提供免费开发，投标方提供与招标方的自动化运维平台、态势感知系统的接口开发与对接，不在单独收取任何费用。

6 质量保证

6.1 订购的新型产品除应满足本规范书外，投标方还应提供产品的鉴定证书。

6.2 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）均应符合本规范书的规定。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。

6.3 投标方应遵守本规范书中各条款和工作项目的 ISO9000、GB/T1900 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。

6.4 质保期间，因制造质量问题而发生损坏，或不能正常工作时，投标方应免费为招标方修理或更换零部件（质保期按设备投运日算起一年或投标方的最后一种设备到货之日算起一年半，两者以先到日期为准）

7 试验与调试

7.1 验收要求

1) 本项目仅进行现场验收（SAT）。且为针对整个项目的验收，不单独对本设备进行验收测试，但投标方应配合系统集成商进行整个项目的验收测试，并负责设备的验收测试相关资料的编制及其它配合性工作。

2) SAT 验收测试大纲根据项目招标技术文件、投标技术应答书、合同技术协议书等技术文件的内容编写，由投标方编制，招标方审核批准。

3) 投标方应在验收测试前 2 周提供详细的 SAT 验收测试大纲，大纲应提供所有现场验收的细则，细则指定的实验项目以及达到的性能指标不得小于本招标文件要求。招标方有权提出一些合理的特殊测试，并保留对大纲的修改权力。大纲经双方确认生效后，招标方人员对验收的认可签字并不解除投标方对合同的保证责任。

4) 投标方将负责对现场安装和测试进行指导，投标方的工程师将协助进行现场试验验收。

5) 在现场验收完成后 20 天内，双方的代表将签署验收报告。

6) 验收计划由投标方准备，交给招标方审查同意。

7) 为有利于系统的安装、投运和测试，投标方应派出有经验的专家提供技术服务。

8) 在现场安装、投运及验收过程中，投标方应对损坏的设备负责。

9) 备品备件、文档资料均作为验收的一部分。

7.2 测试报告

在 SAT 测试完成后的二十天内，投标方应提供四份测试报告的副本，每份报告至少包括以下内容：

1) 设备说明。

2) 报告编号、日期。

3) 设备的项目编号、数量及顺序号。

4) 测试的时间、地点及方法。

5) 测试环境。

6) 试验数据包括表计型号、读数、测试点的位置、数据打印出的结果及有关图形等。

7) 测试合格的标准。

8) 测试人员名单。

9) 负责人签字。

7.3 现场调试和现场试验（SAT）

7.3.1 现场调试

- 1) 设备运到现场安装完毕, 招标方应通知投标方人员到场参加设备调试。
- 2) 在调试过程中, 若发现设备存在元器件损坏或不正常工作情况, 投标方应负责更换。

7.3.2 现场试验

- 1) 现场验收应在所有设备安装调试完毕, 且设备准备投入试运行进行, 并出具书面测试报告。
- 2) 现场验收应在工厂系统试验完全完成的基础上进行。
- 3) 在验收开始前二周相应的安装调试单位应提出 SAT 验收大纲供招标方认可, 投标方予以配合。

8 技术性能偏差表

投标方应将所供设备与本招标书技术文件有差异之处, 无论优于或劣于本招标书技术文件要求, 均汇集至以下表中。

技术差异表

序号	采购技术条件书		投标文件	
	条目	简要内容	条目	简要内容

9 投标方需说明的其他问题

如有需说明的其他问题, 投标方应通过书面形式提交, 并加盖公章。