



网络安全管理控制系统技术规范书

深圳供电局有限公司

2026 年 01 月

目 录

1 总则	1
2 工作范围	2
2.1 项目概况	2
2.2 范围和界限	2
2.3 服务范围	2
3 应遵循的主要标准	3
4 使用环境要求	4
5 技术要求	5
5.1 设备技术要求	5
5.2 设备技术参数和性能要求响应表	5
5.3 设备及其附件主要元器件来源	15
6 试验	15
6.1 型式试验	15
6.2 出厂试验	15
6.3 现场交接试验和功能验收	16
7 产品对环境的影响	16
8 技术文件要求	16
9 监造、包装、运输、安装及质量保证	16
9.1 监造	16
9.2 包装	16
9.3 运输	17
9.4 质量保证	17
10 技术差异表	17
11 投标方需说明的其他问题	18

1 总则

1.1 本技术规范书适用于深圳供电局有限公司_____项目采购的网络安全管理控制系统，它提出了该设备本体及附属设备的功能设计、结构、性能、安装和试验等方面的技术要求。

1.2 本设备技术规范书提出的是最低限度的技术要求。凡本技术规范书中未规定，但在相关设备的行业标准、国家标准或 IEC 标准中有规定的规范条文，投标方应按相应标准的条文进行设备设计、制造、试验。对国家有关安全、环保等强制性标准，必须满足其要求。

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

1.4 本技术规范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 本技术规范书经招标、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的法律效力。若本技术规范书涉及有关商务方面内容，如与招标文件的商务部分矛盾时，以商务部分为准。

1.6 本技术规范书未尽事宜，由招标、投标双方协商确定。

1.7 投标方在应标技术规范书中应如实反映应标产品与本技术规范书的技术差异。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规范书的条文存在差异，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。

1.8 投标方应在应标技术部分按本技术规范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。

1.9 投标方应充分理解本技术规范书并按本技术规范书的具体条款、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、格式不符合本技术规范书的要求，则认为应标不严肃，在评标时将有不同程度的扣分。

1.10 标注“★”的条款为关键条款和技术参数，作为评标时的否决项。

2 工作范围

2.1 项目概况

本技术规范书采购的设备适用的工程概况见表 2.1：工程概况一览表。

表 2.1 工程概况一览表 （项目单位填写）

序号	名 称	内 容
1	采购设备或项目名称	
2	项目单位	深圳供电局有限公司
3	项目单位地址	深圳市福田区中心一路 39 号

2.2 范围和界限

1) 本技术规范书适用于所供设备的设计、制造、装配、工厂试验、交付和试验的指导、监督以及试运行工作。

2) 本技术规范书未说明，但又与设计、制造、装配、试验、运输、包装、保管和运行维护有关的技术要求，按条款 3 所规定的有关标准执行。

2.3 服务范围

1) 供货范围一览表

投标方提供的设备及其附件的具体规格、数量见表 2.2：设备供货范围响应表。投标方应如实填写“投标方保证”栏。

表 2.2 设备供货范围响应表（项目单位填写）

序号	名 称	单位	项目要求	
			型式、规格	数量
1	沙箱系统系统	套	按设备技术参数和性能要求响应表响应	3
2	VPN 安全网关	套	按设备技术参数和性能要求响应表响应	2
3	API 安全工具	套	按设备技术参数和性能要求响应表响应	1

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

3) 投标方应协助招标方解决设备运行中出现的问题。

4) 如果调试、性能试验、试运行及质保期内技术指标一项或多项不能满足合同技术部分要求，买卖双方共同分析原因，分清责任，如属制造方面的原因，或涉及索赔部分，按商务部分有关条款执行。

5) 设备正常使用后，投标方和招标方（业主）双方应根据相关法律、法规和公司管理制度签署合同设备的验收证明书。该证明书共两份，双方各执一份。

6) 投标方应按招标方要求免费提供必须的人员培训和技术指导，确保招标方正常使用和维护设备。

3 应遵循的主要标准

除本技术规范书特殊规定外，投标方所提供的设备均按规定的标准和规程的最新版本进行设计、制造、试验。如果这些标准内容有矛盾时，应按最高标准的条款执行或按双方商定的标准执行。如果投标方选用本技术规范书规定以外的标准时，则需提交这种替换标准供审查和分析。仅在投标方已证明替换标准相当或优于技术规范书规定的标准，并从招标方处获得书面的认可才能使用。提交供审查的标准应为中文或英文版本。标准如下：

ISO	《国际标准化组织标准》
IEC	《国际电工委员会标准》
ITU—T G. 652、G. 655	《单模光纤标准》
IEEE	《美国电气电子工程师协会标准》

GA 1089-2013	《电力设施治安风险等级和安全防范要求》
DL	《中华人民共和国电力行业标准》
EIA	《电子工业协会标准》
	《中华人民共和国网络安全法》
GB 50348-2018	《中华人民共和国密码法》
GB17859-1999	《计算机信息系统 安全保护等级划分准则》
GB/T25058-2019	《信息安全技术 网络安全等级保护实施指南》
GB/T25070-2019	《信息安全技术 网络安全等级保护安全设计技术要求》
GB/T 22240-2020	《信息安全技术 网络安全等级保护定级指南》
GB/T22239-2019	《信息安全技术 网络安全等级保护基本要求》
GB/T28448-2019	《信息安全技术 网络安全等级保护测评要求》
DL/T 860	《变电站通信网络和系统》
	《电力二次系统安全防护规定》
Q/CSG 115001-2012	《南方电网调度自动化系统不间断电源配置规范》
	《南方电网公司反事故措施（2018 版）》
电监信息[2012]62 号	电力行业信息系统安全等级保护基本要求

4 使用环境要求

本设备招技术规范书技术文件需要采购的设备，其外部使用条件见下表。投标方应对所提供的设备性能参数在外部条件下进行校验、核对，使所供设备满足实际外部条件要求及全工况运行要求。

设备使用环境要求相应表（项目单位填写）

序号	名 称	项目要求值	投标方保证值	备注
1	长期工作环境温度	10℃～35℃		
2	存储温度	0℃～55℃		
3	长期工作环境相对湿度	35%～80%		
4	存储相对湿度	10%～95%		
5	长期工作海拔高度	0m～1000m		

6	存储海拔高度	0m~1000m		
---	--------	----------	--	--

5 技术要求

5.1 设备技术要求

5.1.1 设备基本要求

设备及全部配件必须为全新的、持久耐用的产品。即使在本技术规范书中没有明确地提出,也应满足作为一个完整产品一般所能满足的全部要求。同时,可根据系统、测试对象性能的要求并随着 IT 技术发展,可提供持续的软件开发和硬件的升级。

5.1.2 设备结构要求

无要求。

5.2 设备技术参数和性能要求响应表

投标方应认真逐项填写所供设备技术参数和性能要求响应表 5.2.1-5.2.3 中“投标方保证值”栏,不能空格,也不能以“响应”两字代替,不允许改动本表内“投标方保证值”栏之外的数值。如有差异,请填写表 10.1: 技术差异表。标注“★”的条款为关键条款,投标方应出具相应技术资料证明达到条款和技术参数的要求,作为评标时的否决项。

5.2.1 沙箱系统

指标	类别	技术要求说明
产品要求	硬件要求	★国产化 CPU \geq 8C, 内存 \geq 64G, 系统盘 \geq 256G SSD, 数据盘 \geq 4TB, 冗余电源, \geq 4 个万兆光口、 \geq 4 个千兆光口、 \geq 4 个千兆电口。
	★安全要求	产品集成部件的芯片基于自主可控芯片, 包括但不限于多核架构 CPU、DRAM 颗粒、PHY、FLASH、电源、交换转发、通信等芯片。
	性能要求	应用层吞吐量 \geq 4Gbps; 动态分析性能 \geq 40000 个/每天。
	高可靠性	产品系统盘和数据盘各自采用独立的物理存储介质, 提高抗故障及数据保护能力。
	分析对象提交	★支持多种方式获取分析对象, 包括但不限于通过协议还原、手工提交样本、手工提交 PCAP 数据包、手工提交 URL、API 接口提交等方式获取可疑文件。需提供制造商盖章的功能截图证明。
	系统部署	支持旁路模式部署, 对镜像或分光数据进行检测。

	离线扫描	★支持离线文件扫描模式，对指定的 FTP/SMB 文件目录进行读取检测。需提供制造商盖章的功能截图证明。
		支持手工批量上传可疑文件，指定检测类型进行检测。
		★支持管理扫描任务，包括但不限于新建、删除、查看进度等，支持生成任务详细报告并通过邮件发送扫描结果。需提供制造商盖章的功能截图证明。
	协议还原	系统自身具备流量采集和对 HTTP/FTP/SMTP/POP3/IMAP/NFS/SMB 协议的解析还原能力。
	动态检测	提供基于虚拟执行的动态检测技术，可以基于软件在虚拟环境的行为及通用漏洞利用特征（进程行为，逃逸行为），分类识别各种加壳病毒及未知恶意代码。
		支持对 office 文档、pdf、压缩文件、flash、pe 等常见 windows 平台文件进行动态检测。
		★支持 win xp、win7、win10、安卓等虚拟环境，支持四类环境同时启用，需提供制造商盖章的功能截图证明。
		支持模拟银河麒麟 V10-桌面版操作系统环境
		支持模拟 64 位 ubuntu 操作系统环境
		支持模拟 64 位 win7、win10 环境
		★系统至少内置 7 种不同类型的虚拟环境，支持用户自主配置，需提供制造商盖章的功能截图证明。
		支持基于样本的动态行为特征关联样本家族信息
		支持对样本的攻击类型特征占比进行分析，以图形化的方式展示样本行为特征的占比，输出样本最大概率攻击类型结论
		支持对样本的攻击行为映射至 att&ck 模型框架
		支持对样本的运行过程进行快照截图
	静态检测	支持自定义 YARA 检测规则。
		支持无签名静态检测技术，包括无差别的 shellcode 检测；
	联动协同	★需要承诺与现网电力网络安全防御系统联动，联动产品提交可疑文件，系统经过分析后，产生信誉下发到联动的设备进行阻断，实现检测和阻断闭环。需提供制造商盖章的承诺函。
	企业信誉	支持基于自身检测能力生成企业信誉库，信誉类型包括但不限于文件 MD5、URL、C&C 地址

产品要求		支持对生成的企业信誉进程查询和删除。
	IPv6 支持	支持 IPv6 环境下的部署与配置。
	产品资质	<p>★产品要求为国内开发，具备自主知识产权，具有软件著作权证书，提供产品软件著作权证书并加盖制造商公章</p> <p>★产品应具备《网络关键设备和网络安全专用产品认证证书》或《CNAS 认证的第三方检测单位出具的检测报告》相关资质证明材料，提供资质证明材料并加盖制造商公章。</p>

5.2.2VPN 安全网关

指标	类别	技术要求说明
产品要求	硬件要求	国产化 CPU ≥ 8 核，内存 $\geq 16G$ ，硬盘 $\geq 256G$ 固态硬盘，4T 机械硬盘，交流冗余电源， ≥ 6 个千兆电口， ≥ 4 个千兆光口（配置 4 个千兆多模光模块）， ≥ 4 个万兆光口（配置 4 个万兆多模光模块）， ≥ 1 个接口扩展槽位。具有硬件国密加密芯片，SSL VPN 并发用户数 ≥ 1000 个。
	★安全要求	产品集成部件的芯片基于自主可控芯片，包括但不限于多核架构 CPU、DRAM 颗粒、PHY、FLASH、电源、交换转发、通信等芯片。
	性能要求	IPSec 国密加密吞吐量 $\geq 3.2Gbps$ ；SSL VPN 国密加密吞吐量 $\geq 2.5G$ ，最大并发数 ≥ 240 万；每秒新增会话数 ≥ 7.5 万。
	部署方式	支持虚拟线，二层透明，三层，混合，旁路监听，单臂接入方式
	接口类型	支持三层接口、三层子接口、环回接口、VPN 接口
	交换	支持 VLAN 划分、VLAN Trunk/Access，支持 802.1Q，能进行封装和解封
	路由	支持基于源/目的地址、接口、基于服务、应用的策略路由 支持策略路由的多出口负载，根据链路情况自动实现负载分担
	链路探测	★支持通过 ICMP、TCP、UDP 协议，完成对目的 IP 地址可达性的探测，支持在策略路由、GRE 隧道、DNAT 策略、HA 中设置链路探测，请截图证明
	DHCP	支持创建多个 DHCP 服务器实例，为接入设备提供动态地址分配服务
		支持自定义地址池范围，支持不连续网段录入，保留部分地址不做分配
	IPSec VPN	支持网关-网关部署模式
		支持网关预共享密钥、x509 证书（RSA）、国密数字信封等认证方式
		★支持 3DES、AES-192、AES-128、AES-256、SM4、SM1 等加密算法，其中 SM1 为硬件加密算法，需要配备专用密码卡实现硬件加解密，密

		码卡支持自检功能，同时具备《商用密码型号证书》，请截图证明
		支持标准 MD5、SHA、SHA-256、SHA-384、SHA-512、SM3 摘要验证算法，SM2 非对称密钥算法
		支持星型、网状隧道连接
		支持隧道模式、传输模式
		支持主动模式、野蛮模式
		支持通过 PPPoE 接口建立 IPSec VPN 并自动适配动态 IP 地址变化
		支持对端地址为动态 IP 地址的场景
		支持 NAT 地址穿越
		支持 NAT 场景下配置本端映射 IP 地址与对端映射 IP 地址
		支持隧道心跳探测 DPD，如遇隧道异常自动断掉并尝试重新连接
		支持双机 HA 场景下的 IPSec VPN，总部两台设备做可靠性保护与多分支进行组网
	SSL VPN	支持网关-客户端/浏览器的业务部署方式
		支持 IE11、Firefox、Chrome、Safari 等常见厂商浏览器，支持 32/64 位系统浏览器
		支持七层 web 反向代理、三层隧道模式
		Web 反向代理支持 HTTP、HTTPS 等应用模式
		支持移动用户账号本地、Radius、证书认证（包括 RSA、SM2 国密数字证书格式）
		支持证书生成和导出
		支持基于用户、用户逻辑组的访问授权，包括七层 Web 和三层授权。授权粒度包括基于 URL、子网、IP、协议等的细粒度授权
		支持本地信息、告警、错误、调试等 vpn 日志
		支持双机热备，主设备出现故障，立即切换至从设备，VPN 自动连接正常运行
		支持 openvpn 客户端、自研客户端（支持 x86(32 位/64 位)win10、win11 相关操作系统）
		自研客户端，支持配置文件手动导入和自动拉取两种模式，自动拉取可以直接通过输入 VPN 网关的 IP 地址来实现
	GRE	支持建立 GRE 隧道，指定隧道源目的 IP
		支持 keepalive 探测，以及故障自动重连机制
		支持基于 GRE 逻辑接口的 SLA 探测能力，包括基于 TCP、UDP、ICMP 的探测，支持设置探测间隔与最大探测失败次数
		支持 GRE 隧道状态统计、隧道流量统计
一 体 化 策		提供基于源/目的 IP 地址、安全区、应用、应用组、协议/端口、时间、安全模板的精细粒度的安全访问控制，时间精确到秒级

略	★策略可按匹配顺序、策略分组、新建顺序、安全区分组等不同维度的查看方式，在按匹配顺序查看下，可以通过拖拽实现优先级的调整，也可以输入具体的策略序号、置顶或者置底等方式进行调整，请截图证明
	★为高效编辑策略，支持对多条策略的源/目的地址、协议/端口、应用、时间等进行批量修改，实现一次修改覆盖多条策略，请截图证明
策略模拟测算	★基于源安全区、目的安全区、源地址、目的地址、源端口、目的端口、协议等，模拟运行直接获得策略的命中信息，并可对命中的策略信息进行编辑，请截图证明
协议控制策略	★提供对二层协议（包含 BPDU、802.1Q、SLOW、MPLS 单播、MPLS 多播、pppoe 发现控制、pppoe 会话控制、QinQ）进行控制，请截图证明
	★支持非 IP 协议（包含 IPX 和 AppleTalk）的进行控制，请截图证明
NAT64	支持 NAT64，支持 TCP、UDP、ICMP 报文的 IPv6toIPv4 和 IPv4toIPv6 转换，同时支持有状态和无状态两种转换方式，支持调整策略优先级
路由	支持 IPv6 静态路由，IPv6 策略路由
一体化策略	支持基于源/目的 IPv6 地址、安全区、应用、应用组、协议/端口、时间的精细粒度的安全访问控制
全局黑名单	支持针对 IPv6 地址进行黑名单和白名单的配置，请截图证明
全局黑白名单	★支持针对源地址或者目的地址、网段、IP 地址池进行黑名单和白名单的配置，请截图证明
	★名单内容支持 IP 地址、协议 TCP/UDP/ICMP 和端口进行设置，请截图证明
	★黑名单支持配置生效时间，请截图证明
	★支持基于 IP 地理位置归属信息，进行黑白名单防护，请截图证明
双机聚合	当用户配置两台设备共同承载流量时，可以选择配置双机聚合模式，两台设备的上下行流量，将在两台设备之间进行动态分配（此模式只适用于虚拟线，上下接二层交换机的模式）
日志类型	支持基础系统日志、系统升级日志、网络故障日志、高可用日志、审计日志
证书对象	支持证书请求文件的生成与管理，包括 RSA 国际算法与 SM2 国密算法格式，来实现向第三方 CA 中心申请数字证书
	★支持内置 PKI，内置 CA 可根据请求文件离线签发证书，支持导入第三方 CA 证书，最大支持三级 CA 证书链认证
	支持数字证书的生成、上传与管理
	★支持 CRL 证书吊销列表的导入、管理与验证，支持手动上传与 HTTP

		在线获取。支持自动更新功能，可以自定义更新周期。
管 理 方式		支持 Web 管理、串口管理、SSH 管理，支持配置最大同时登录用户数
		支持基于物理接口进行接口的客户管理属性配置（是否可以通过 HTTPS/SSH/ICMP 方式登录设备）
升 级 管理		支持离线升级
帐 号 管理		支持角色定义，为角色定义不同的功能权限
		支持三权分立
维 护 工具		网络诊断、抓包与回放、转发信息、会话表、网络连接状态、网卡状态、报文示踪等维护手段
		支持智能巡一键检信息采集，包括系统运行异常信息、关键进程异常信息等
备 份 恢复		可对全部配置配置文件进行备份与恢复
SNMP		支持 SNMP V1、V2、V3 版本，支持 agent 及 trap 警告发送
系 统 设置		支持设置设备名称和位置
		支持系统重启、系统关机、应用层防护控制、web 服务重启、引擎重启等操作
产 品 资质		★产品具备《网络安全专用产品安全检测证书》，提供有效证书复印件
		★产品具备《商用密码产品认证证书》，要求证书型号与所投标产品完全一致，提供有效证书复印件
		产品符合 GM/T 0023《IPSec VPI 网关产品规范》、GM/T 0025《SSLVPN 网关产品规范》、GM/T 0026《安全认证网关产品规范》、GM/T0028《密码模块安全技术要求》

5.2.3 API 安全工具

指标	类别	技术要求说明
产 品 要求	硬 件 要求	2U 机架式（专用硬件平台），冗余交流电源，2GE 板载管理口，4GE 板载接口+4GE(SFP)板载接口，2 个万兆光接口，1×接口板卡插槽。64GB 内存，1×6TB 硬盘，
	★安 全要 求	产品集成部件的芯片基于自主可控芯片，包括但不限于多核架构 CPU、DRAM 颗粒、PHY、FLASH、电源、交换转发、通信等芯片。
	性 能 要求	Agent 授权≥40，流量≥1Gbps
	部署	支持镜像和探针获取流量以及混合部署。

网 络 协 议	★支持 HTTP、HTTP2、DUBBO、FTP、WebSocket，IPV4，IPV6 的常用网络协议解析能力。 支持接口协议类型包括但不限于 SOAP、gRPC、GraphQL、Jsonp、Json-RPC、OAuth、Restful API、Swagger 等。
	★支持 TLS 协议流量的基础信息统计分析，包括：服务器 IP、服务器端口、SNI、请求包数、响应包数、请求字节数、响应字节数、总访问量、TLS 版本、加密套件。
	★支持 WebSocket 的基础信息审计：服务端 IP、服务端端口、客户端 IP、客户端端口、地域、Direction、敏感标签、时间
	★支持 FTP 协议的基础信息审计：服务端 IP、服务端端口、客户端 IP、客户端端口、地域、敏感标签、请求命令、请求内容、返回码、返回内容、时间
大 数 据 云 存 储 协 议	★支持大数据协议及云存储协议识别，包含： MaxCompute、Clickhouse、Hadoop、ElasticSearch、腾讯云存储(COS)、阿里云存储(OSS)、华为云存储(OBS)、京东云存储、百度云。
文 件 识 别	支 持 资 源 文 件 识 别 ， 包 含 ： HTML, JSON, XML, TXT, PDF, DOC, DOCX, XLS, XLSX, CSV, PPT, PPTX, ZIP, RAR, 7z, TAR, GZ, WPS, ET, DPS, RTF, OFD。 支持对删除文件后缀等逃逸方式进行识别。 支持对加密文件的发现 支持对于图片文件的识别：BMP、GIF、JPG、PNG
源 码 类 型 识 别	★支持源码文件识别，包含：Python, JSP, Lua, SQL, ASP, ASP.net, Perl, C, Java, PHP, C#, C++, Javascript。
应 用 清 单	可通过列表形式展现应用列表清单，并通过应用标签、部署域、请求敏感标签、响应敏感标签维度进行分组统计； 可通过树形展示应用结构；
	应用画像展示，内容包含：应用常用账号、常用 IP、常用接口、敏感数据分布、弱点分布以及部署 IP 分布、风险事件、数据访问趋势
接 口 清 单	支持通过内部识别规则自动发现 API 接口，同时支持手工方式添加 API 接口；
	可通过列表形式展现应用接口清单，并通过通过多维度进行分组统计，分组维度至少包括：应用、接口标签、接口等级、请求敏感标签、响应敏感标签、访问域。
	支持按业务属性自动为接口打标，识别接口标签，如：敏感数据外发接口、人机交互接口、数据采集接口、互联网登录接口等

		支持按开发属性自动识别接口类型,包括但不限于普通接口、登录接口、敏感接口、脱敏接口、伪脱敏接口、上传接口、下载接口等;
		支持接口的生命周期自动管理,生命周期新增接口、活跃接口、失活接口; 识别涉敏接口、风险接口以及弱点接口
		支持对涉敏数据的接口自动打上敏感数据标签,例如身份证、姓名、手机号等
		支持查看和导出接口记录日志, 并支持在线模拟接口访问测试
		接口画像展示, 内容包含: 常用账号、常用 IP、数据访问趋势、访问集中度, 弱点分析、敏感数据分布、风险事件等;
行 数 解 析		支持通过内置规则识别出接口返回的数据行数, 识别的数据类型包含 json、xml、soap 三种类型; 可基于解析的数据行数作为业务风险的输入,对于超过行数的数据的访问行为进行预警。
		支持手工配置接口行数解析规则, 并可根据实际运行性能设置是否启用。
接 口 的 合 并 拆 分		★支持自动或者手动方式对接口合并和拆分; 支持智能分析出推荐合并的接口; 数据台账、统计分析、报表等内容按接口合并后的结果呈现; 支持 SOAP 和 RESTful 接口自动拆分;
敏 感 数 据 识 别		支持 150 以上内置敏感数据类型标签包括但不限于:手机号、个人姓名、住址、电子邮箱、生日、民族、性别、家庭关系、脱敏手机号、脱敏身份证号;
		支持自定义敏感数据识别策略,可通过自定义正则表达式或配置数据字典方式, 从请求 (request-header、request-body、request-param、response-header、response-body) 中识别到敏感数据。
数 据 资 产 清 单		★支持敏感数据列表展示, 查看识别到的敏感数据内容, 敏感标签、敏感级别、出现位置等
		支持敏感数据脱敏处理, 对事件中包含的敏感数据进行脱敏处理, 防止运维过程中的数据泄漏。 支持通过取消脱敏对包含的原始敏感数据进行查看。
数 据 访 问 流 向		★支持针对具体的敏感数据绘制出具体数据->应用->接口->访问 IP->应用账号的完整访问流向图;
账 号 识 别		支持账号资产识别管理, 支持从流量中解析还原应用系统登录账号, 支持账号解析的位置, 至少包含: Request-Body、Request-Header、Response-Body、Response-Header;

		支持单点登录 SSO 场景的解析配置,能够清晰显示单点登录系统间的关联关系;
用户信息		支持对账号对应的用户信息(如:员工 ID、部门、个人姓名、网络昵称、登录用户名、手机号、身份证号、银行卡号)进行自动解析
用户和账号关联		★支持手动/自动将账号与用户信息进行关联,在后续溯源中,直接通过账号下的用户信息快速找到对应人员
信息识别		自动识别文件中携带的敏感数据内容,包括:敏感数据标签,敏感数据标签去重数据量。 自动识别文件的信息,包括:文件名称,文件格式,文件大小,MD5 值。
访问统计		统计文件访问情况,包括但不限于文件下载次数,文件上传次数、下载账号个数、上传账号个数、下载 IP 数、上传 IP 数等
弱点策略		内置脆弱性问题发现规则包括但不限于明文密码传输、弱口令、弱加密、数据伪脱敏、接口执行命令、接口可执行 SQL、接口未鉴权、接口缺乏速率限制、单次返回大量或多种敏感数据、URL 中包含敏感信息、文件目录暴露、SQL 注入、水平越权、登录错误提示不合理等。 支持自定义弱点规则,多条识别规则可以逻辑组合,规则识别的内容不仅限于:URL 参数、请求头、请求体、Cookie、SET-COOKIE、响应头、响应体、敏感标签类型、IP 数量、账号数量;
弱点清单		支持弱点信息分类展示和导出,分类包含:OWASP API Security T010、弱点级别、弱点核实状态,展示弱点内容包含:每个弱点的统计数、弱点名称,产生弱点的应用和接口信息、应用部署位置;
弱点关联风险		★可关联到风险:关联风险显示证据样例标识、关联风险规则、客户端 IP、账号、代理 IP、服务器 IP、应用名称、发生时间;
弱点取证		支持对识别的弱点提供判断线索,并对线索信息高亮展示,同时并自动关联访问日志和涉敏数据信息; 支持提供弱点的原理描述和修复建议; 支持对弱点详情导出;
		内置数据泄漏风险规则包括但不限于超量爬取、高频爬取、账号访问数据类型和数据量异常、单 IP 访问量异常、路径探测、账号共用、撞库、短信轰炸等;
风险策略		支持自定义配置告警策略,包括风险对象:指定账号,指定网段,指定时间段,指定应用系统,指定接口,指定风险周期:秒、分钟、天,设定多种风险指标; 支持配置多个敏感数据标签的“逻辑与”和“逻辑或”复合条件; 支持配置多种统计指标的“逻辑与”和“逻辑或”复合条件,统计指标

		包括但不限于 IP 数量、账号数量、访问次数、敏感数据量、去重敏感数据量、数据行数、数据去重行数、去重的账号密码组合数，统计周期包括但不限于单词、分钟、日、周、月；
	风 险 关 联 弱 点	★根据风险可关联到弱点:关联弱点显示证据样例标识、关联弱点规则、客户端 IP、账号、服务器 IP、应用名称、发生时间；
	基 线 风 险	★基于应用、接口、账号、IP 等维度建立多维度行为基线，设置异常行为检测规则，识别传统风险模型无法识别的未知威胁； 支持不同策略、学习周期的基线任务，包括行为基线、自然周基线； 支持自定义基线的学习周期，不同周期的基线支持自定义合并策略和机器学习智能合并；
	数 据 泄 露 追 溯	支持以泄露的一条和多条敏感数据作为线索对数据访问事件记录进行检索分析，按应用、接口、客户端 IP、账号、时间维度统计涉及的线索条数，协助分析出数据泄露的应用、接口、客户端 IP、账号、时间信息。 多条线索匹配逻辑可支持匹配任意一条或者全匹配；
	风 险 关 联 行 为 轨 迹	支持调阅特定风险事件所固定的原始访问数据及其上下文请求响应数据，可还原风险事件现场，可还原账号或 IP 历史访问轨迹。
	记 录 真 实 用 户 IP、 真 实 域 名	支持在 NAT 和代理环境下自动识别出 HTTP 数据包转发前的真实 IP 地址（X-Forwarded-For 地址）和正式域名信息（X-Forwarded-Host），为威胁溯源提供依据。
	敏 感 数 据	★支持以桑基图形式查看数据、类型及敏感级别的占比情况； 支持以应用和接口视角查看指定应用和接口的资产信息，包括但不限于敏感数据分布、访问趋势变化、风险情况等。
	账 号 画 像	★账号过程化数据展示，包含账号（支持一键复制按钮、账号设置-跳转到账号解析页面，数据对比分析）、总访问量、涉敏访问量、总行数、总接口、涉敏接口、访问 IP、登录次数、上传次数、下载次数、账号名称、所属应用、账号类型、是否涉敏、姓名、职位、组织机构、手机号、发现时间、请求敏感标签、响应敏感标签； 统计数据包含常用 IP、常用终端、棉感数据分布、敏感数据访问统计、常用接口、风险事件、时间集中度；点击详情按钮会显示对应的详情页面； 支持账号周期对比：支持按周、月、日、行为基线的周期对比；行为基

		线对比支持选择基线的自然周对比
产 品 要求	访 问 耗时 产 品 资质	<p>★可列表展示详细信息，包含最大耗时、总耗时、平均耗时、接口地址、所属应用、请求方法、响应类型等信息，并且可以支持按照最大耗时、最大耗时发生时间、总耗时、总访问量、平均耗时、涉敏访问量进行排序。</p> <p>★产品要求为国内开发，具备自主知识产权，具有软件著作权证书，提供产品软件著作权证书并加盖制造商公章</p> <p>★产品应具备《网络关键设备和网络安全专用产品认证证书》或《CNAS认证的第三方检测单位出具的检测报告》相关资质证明材料，提供资质证明材料并加盖制造商公章。</p>

5.3 设备及其附件主要元器件来源

投标方应按下表如实填写主要元器件来源。

设备及附件主要元器件来源一览表 （投标方填写）

序号	元器件名称	型号	厂家或供应商名称	产地	备注

6 试验

根据相关国标和行标等有关标准及其补充说明进行各项试验,有关条款的特殊要求和补充应在试验期间遵守并执行。

6.1 型式试验

型式试验是为了验证所设计和制造的设备的性能是否能够达到相应产品标准的要求,投标方应提供有相应资质的第三方检测机构出具的产品型式试验报告,型式试验的项目内容如下:

无

6.2 出厂试验

出厂试验是为了发现产品所用材料和制造中的缺陷,它不应损伤产品的性能和可靠性。出厂试验应在整体组装后进行,应该对每台成品进行检验,以确保每台产品与已经通过型式试验的产品相一致。出厂试验的项目内容如下:

无

6.3 现场交接试验和功能验收

本技术规范书采购设备应进行现场交接试验和功能验收,投标厂家应安排专人进行现场设备交付和验收工作。交接试验和功能验收是为了确认设备经过运输、储存和/或调整等过程后是否存在损坏、各个单元的兼容性、装配是否正确。

7 产品对环境的影响

投标方应该提供有关设备对环境影响所需要的材料。任何已知的化学危险和环境危害应在手册或使用说明中明确。

投标方应该对有关设备的不同材料的使用寿命和拆除的程序给予必要的指导,对再循环使用的可能性给予简要说明。

8 技术文件要求

在设备到货时,投标方应按招标方要求提供满足本次采购设备、调试、使用、维护所需要的相关技术文件纸质版至少 2 套,电子版资料 1 套。投标方提供的所有资料均应为中文版或中英文对照版。投标方提供本次采购设备所需的软件应为原装正版软件。具体要求提供资料如下:

- a. 出厂试验报告;
- b. 产品合格证;
- c. 产品安装说明书和产品使用手册(包括:软件和硬件安装使用说明、系统功能说明、调试方法、维护项目、培训教程等等)。
- d. 其它相关图纸资料、测试数据、软件密钥等等;

9 监造、包装、运输、安装及质量保证

9.1 监造

本技术规范书采购设备无监造要求。

9.2 包装

1) 要严格按照制造厂给出的说明书对设备进行包装、运输和储存。制造厂应在交货前的适当时间提供设备的运输和储存说明书。

2) 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。其包装也应符合铁路、公路和海运部门的有关规定。

3) 包装箱上应有明显的包装储运图示标志, 并应标明招标方的订货号和发货号。

4) 设备的包装应能保证设备各零部件在运输过程中不致遭到脏污、损坏、变形、丢失及受潮。对于其中的绝缘部件及由有机绝缘材料制成的绝缘件应特别加以保护,以免损坏和受潮。对于外露的接触表面,应有预防腐蚀的措施。所有运输措施均应经过验证。凡有运输损坏,应由制造厂负责赔偿。

9.3 运输

- 1) 设备单独运输的零部件应有标志,便于用户安装装配。
- 2) 整体产品或分别运输的部件,都要适合于运输及装卸的要求。
- 3) 制造厂应提供按全部解体检修用的备品备件和装用机具,随同产品发运。
- 4) 随同运输的产品应附有装箱清单,产品所需提供的技术资料应完整无缺。

9.4 质量保证

1) 全部设备必须是全新的,持久耐用的,应满足作为一个完整产品所能满足的全部要求。投标方应保证设备在规定的使用条件下运行、预期使用寿命应不少于 12 年。

2) 投标方应对其整组设备在到货后提供不少于 3 年的“三包”质量保证。之后如发生产品损坏,投标方应及时为本组装置提供维修部件,并按最近的投标价提供。

3) 订购的新型产品除应满足本标准外,投标方还应提供该产品的鉴定证书。

4) 投标方应保证制造过程中的所有工艺、材料试验等(包括投标方的外购件在内)均应符合本标准的规定。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。

5) 附属及配套设备必须满足有关行业标准的要求,并提供试验报告和产品合格证。

6) 投标方应有遵守本标准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通过国家认证并在正常运转。

7) 对仪器设备在质保期内出现的故障,投标方人员在接到通知后应在 2 个工作日内派技术人员到现场检查处理,并立刻提出处理意见,免费进行维修。

8) 对于质保期已过的仪器设备,厂家将负责终身维修。对于一般的故障,处理时间 15 个工作日内。对于严重的故障,将根据情况安排维修时间的长短。

10 技术差异表

投标方应将所供设备与本招技术规范书技术文件有差异之处,无论优于或劣于本招技术规范书技术文件要求,均汇集至表 10.1。

表 10.1 技术差异表 (投标方填写)

序 号	招 标 文 件		投 标 文 件	
	条 目	简 要 内 容	条 目	简 要 内 容

11 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。