内蒙古自治区环境监测总站
ᠥᠪᠥᠭᠡᠨ ᠤᠯᠤᠰ ᠤᠨ ᠠᠷᠪᠢᠨ ᠤᠷᠴᠢᠨ ᠬᠣᠰᠢᠶᠠᠭᠤ ᠵᠠᠭᠰᠤᠭᠠᠯᠲᠠ ᠶᠡᠬᠡ ᠲᠥᠪ

内蒙古自治区环境监测总站
关于“专用设备采购项目”的变更说明

因“监测总站专用设备采购项目（项目编号：NMGZC-G-H-260247）”包5技术参数优化，依据《中华人民共和国政府采购法》及相关法律法规规定，经研究，我站决定对原招标文件变更如下：

一、原招标文件内容：

（一）一体化安全接入网关网络终端防火墙—功能和质量要求

1.基础要求：

1）设备需满足网络安全等级保护制度中安全区域边界范畴的边界防护、访问控制、入侵防范、流量控制等核心安全要求，同时兼容SD-WAN组网、上网身份认证、防火墙防护等场景化高危风险防护需求；需标配完整的特征库、威胁情报库及流量过滤、威胁检测相关功能模块。

2.规格与性能要求：

（1）采用1U标准机架式硬件形态，设备接口及性能指标满足以下要求：配置不少于8个GE电口、8个GE光口、6个10G光口；USB2.0接口数量≥2个，Console管理接口数量≥1个；

配备单交流供电模块，搭载 1TB SSD 固态硬盘；整机应用吞吐量≥12Gbps，最大接入用户数≥1500，并发连接数≥800 万。以上参数需提供证明材料，并加盖产品生产厂商公章。

3. 功能要求：

（1）支持双系统备份机制，支持主备系统自动无缝切换，系统切换时间小于 500 毫秒；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

★（2）具备网络 2 至 7 层全流量深度识别能力，重点强化 7 层应用层精准识别，可全面识别主流应用协议，并实现精细化分级分类，例如针对 HTTP 协议可逐级细分至 Web 视频-优酷、网络游戏-移动游戏等具体应用场景与客户端名称；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（3）支持识别国内常见应用协议数量≥1000 种，其中大型游戏类协议≥300 种，移动 APP 类应用协议≥30 种，现网实际协议识别准确率≥95%；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（4）支持 ChatGPT、DeepSeek 等主流 AI 类应用协议识别管控；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（5）支持网心云、亿点云等常见 PCDN 类应用协议识别管控；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（6）支持自由门、小火箭等主流代理类软件应用识别管控；

需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

3）线路负载：

（1）支持基于源 IP、目的 IP、源+目的 IP、四元组、上下行空闲带宽、最小连接数、主备模式的多维度负载均衡策略；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（2）支持基于域名、应用协议、对象库的精细化负载均衡调度；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（3）支持虚拟线路+LAN+WAN 组合模式，最大线路支持数量≥4000 条；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

4）流量控制：

（1）支持基于全局、链路、数据流向、共享用户、移动终端、应用协议/协议组、IP/IP 群组的多维度速率管控；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（2）支持单条策略总带宽限速功能，可自定义配置总控带宽阈值；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（3）支持单条策略单 IP 独立限速功能，可自定义配置单 IP 带宽阈值；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（4）带宽控制基础颗粒度为 50kbps，精细化限速颗粒度可

达到 1kbps，实现带宽精准管控；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（5）单个策略组支持多时段生效配置，满足不同场景差异化时段管控需求；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（6）支持“动态 IP 限速”功能（智能调控），可在启用此功能的链路中，针对单个 IP 设置“加速比”、“减速比”、“速度维持时间”等参数，百分比模式设置需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（7）支持策略嵌套功能，同一条策略内可实现特定对象总带宽管控、单 IP 限速、DSCP 标记等参数并行匹配，保障策略配置的灵活性与简洁性；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（8）支持带宽阈值管控功能，可针对指定链路设置带宽使用上限与下限，采用百分比模式配置；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

5）流量镜像：

（1）支持基于 IP 五元组、VLAN 的流量镜像。

（2）支持基于域名和 URL 的流量镜

（3）支持基于应用协议的流量镜像

（4）支持基于协议群组的流量镜像

（5）支持端口镜像只镜像会话前 N 个包功能

（6）支持基于时间的流量镜像调度像。

6）入侵防御：

（1）系统内置漏洞利用、木马病毒、Web 攻击等 15 大类常见网络威胁特征库，可快速检测并阻断网络异常攻击行为；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（2）支持按入侵事件发生时间、规则名称/分类、源目 IP 等维度展示入侵会话信息，以可视化图表呈现内网入侵事件趋势；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

7）威胁情报：

（1）内置威胁情报库条目数量≥百万条，保障威胁检测覆盖面；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

★（2）内置数字货币挖矿、C&C 控制节点、APT 攻击、网站后门、钓鱼网址、僵尸网络等 16 类细分威胁情报，实现网络异常行为深度检测分析；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（3）支持威胁情报命中监测，可查看情报命中趋势、类型分布，以及源 IP、目的 IP、源 MAC 等核心溯源信息；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

8）业务级质量测量

★（1）支持对每条网络会话的客户端时延、服务端时延、应用层时延指标实时监测。

（2）可精准统计客户端时延（设备至客户端网络时延）、

服务端时延（设备至服务器网络时延）、应用时延（会话上下行首包时间差）、会话上下行最大数据包长度等核心指标；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

9）日志审计

（1）支持全量记录会话日志，需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

（2）支持全量记录URL日志

（3）支持全量DNS会话日志

（4）支持按照应用协议、URL关键字、端口号、运营商等信息进行检索和查询。

质量要求：

1）提供具备合法资质机构出具的软件产品登记测试报告，保证产品符合相关技术规范。

2）设备到货后，依据招标文件规定及投标人投标响应内容进行逐项验收测试，各项技术指标与投标承诺一致且满足项目实际使用需求，方可通过验收；若技术参数与投标承诺不符或无法满足使用要求，则验收不合格，投标人须承担相应违约责任。

售后服务：

★1）包含设备安装及正常运行所需费用，提供三年原厂硬件质保服务，同时提供三年特征库、威胁情报库免费升级服务，确保安全检测能力持续有效。

★2）投标人须在投标时提供产品生产厂商出具的正式售后服务承诺函，承诺提供及时、高效的故障响应及技术支持服务。

服务要求：

1、日志分析：定期对安全设备及信息系统日志进行统一归集与分析，及时发现网络攻击、异常行为及安全隐患。

2、 远程巡检：提供常态化远程日常运维巡检服务，覆盖一体化安全接入网关、流量监测分析设备及其他配套网络安全设备，通过远程方式开展设备状态核查、参数校验、运行监测、隐患排查等工作，保障整套安全系统持续稳定、可靠运行。

3、应急处置：发现高危安全威胁时，及时通知采购方，并按规范开展预警、阻断、溯源等应急处置工作。

4、报告提交：巡检工作完成后，出具格式规范、内容完整的安全运维与巡检分析报告。

★5、人员要求：团队人员配置不得少于2人，所有成员均须取得网络安全领域CISP- PTE专业资质证书。

（二）全网流量安全威胁分析平台—功能和质量要求

1.基础要求：

1.通过分析网络流量、系统活动、应用程序日志及用户行为等数据，运用规则匹配、行为分析、机器学习与人工智能等方法，识别其中潜在的恶意活动与安全威胁的过程。其核心目的在于及时发现已知攻击模式和未知威胁，并发出警报，为后续的调查、溯源与响应处置提供关键依据。可满足等级保护-安全区域边界中恶意代码和垃圾邮件防范的要求，以及满足安全区域边界-入侵防范中“应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析”的高危风险要求。

2.规格与性能要求：

1）本项目所投网络安全设备采用标准机架式软硬一体化架构，配置不低于：4核CPU、32GB内存、4个千兆电口、2个扩展插槽、4TB硬盘；设备流量处理能力不低于15Gbps。以上参数需提供有效证明材料，并加盖产品生产厂商公章。

3.功能要求：

1）支持通过WEB图形化界面，将2个及以上管理网口绑定为聚合链路，实现管理口冗余与负载均衡，需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

2）流量采集与识别：支持手动与FTP批量导入PCAP包离线分析，单文件≥500MB、总大小≥1GB，可记录导入与检测状态；支持基于IP、端口、协议、VLAN等结合BPF语法灵活过滤流量；可自定义记录TCP、UDP、HTTP协议流量负载，支持28种以上网络协议、7种以上数据库协议识别还原，可对9种以上文件传输协议行为进行还原并提取文件MD5；提供标准、精简、自定义三种日志外发模式，支持21类以上网络日志外发并可自定义字段。

3）隧道封装识别：支持多层VLAN、VXLAN、MPLS、GRE等隧道流量解析；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

4）流量威胁检测：系统可对13类Web攻击、各类网络攻击与远控、后门行为进行全面检测，Web攻击规则≥11000条，网络攻击规则≥7200条；支持WebShell上传、11种协议暴力破解、撞库爆破及自定义阈值，可识别DNS/ICMP隐秘信道、加密流量攻

击并支持 JA3 指纹；内置 130 条以上弱口令规则，覆盖 9 类协议弱口令机器学习检测，支持正则自定义与弱口令字典导入，全面满足攻击检测、暴力破解、弱口令及加密流量安全检测需求。

★5）高级威胁检测：系统支持 AI 驱动的智能检测引擎，可灵活加载机器学习模型，全面提升威胁识别精度与检出率。通过 ICMP 隧道、DNS 隧道、HTTP 隧道、远控 C&C 流量、挖矿流量、代理流量、暗网通信、弱口令行为、SSH 爆破成功、加密 WebShell 等深度学习检测模型，实现对隐蔽、加密、变种威胁的精准识别，有效弥补传统规则检测盲区；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

6）日志接入与处理：支持接入不同设备类型的第三方日志数据，对不同格式和结构的第三方数据进行解析、范化转换为统一的标准格式，接入分析平台进行分析；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

7）资产分析：支持对资产及资产分组间的互访行为进行专项可视化统计与智能分析，可全面呈现访问时间、源 IP/资产组、目的 IP/资产组、互访协议、目的端口、访问频次、访问拓扑、访问排行等关键信息，支持一键溯源定位原始访问日志；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

8）通过扩展可支持与公开的漏洞众测平台联动获取漏洞情报；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

9）病毒防护：静态病毒防护基本库检测率≥90%流行库检测

率≥95%误报库误报率为零;动态病毒防护可执行恶意软件样本库检测率≥90%恶意网页脚本样库检测率≥90%；需提供对应功能界面截图作为证明材料，并加盖产品生产厂商公章。

10）安全监测能力：支持对恶意扫描行为、钓鱼攻击、地址欺骗、漏洞攻击、恶意程序攻击、异常网络通信行为、未知威胁进行监测、并支持逃避监测防护，支持 IPV4/IPV6 网络场景的监测，支持以可视化方式提供指定时间段内，被监测网络中的特定主机与其他主机之间的相关联的已知、未知威胁事件与异常网络行为（需提供证明资料，如：白皮书或检测报告等并加盖产品生产厂商公章）。

11）挖矿检测：

（1）支持识别包括比特币、以太坊在内的币种通信。

（2）支持挖矿阶段识别，可识别挖各矿阶段，包括恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额。

（3）支持挖矿态势大屏展示，可查看矿机 TOP5、挖矿攻击源 TOP5、矿池 TOP5、币种 TOP5、挖矿阶段、挖矿告警趋势、挖矿币种活跃度情况等信息；（需提供证明资料，如：白皮书或检测报告等并加盖产品生产厂商公章）。

★12）全流程溯源

（1）DNS 行为分析：支持可疑 DNS 解析，可展示 DGA 域名与 DNS 隧道域名的统计信息，并可展示 DNS 解析详情，包含域名、异常类型、请求次数、访问时间等信息。

（2）非常规访问行为分析：支持可疑代理信息展示，可展示可疑代理类型分布、可疑代理访问趋势，以及 socks、http、reDuh、RegeoryTunnel、Tunna 等代理工具产生的流量详情信息。

（3）攻击源 IP 预警支持实时显示攻击源 IP 的画像信息，包括 IP 访问行为、IP 告警信息、网络测绘信息、处置建议、威胁级别、情报标签，关注热度、首次发现时间最近发现时间等。

需提供证明资料，如：白皮书或检测报告等并加盖产品生产厂商公章）。

13）可视化展示

支持不同维度的可视化大屏态势分析，包括：综合态势、挖矿态势、威胁事件态势、资产态势等，支持以客户端形式可视化效果呈现威胁态势。

14）质量要求：

1）产品具备 IT 产品信息安全认证证书，提供证书复印件；保证产品符合相关技术规范。

2）设备到货后，依据招标文件规定及投标人投标响应内容进行逐项验收测试，各项技术指标与投标承诺一致且满足项目实际使用需求，方可通过验收；若技术参数与投标承诺不符或无法满足使用要求，则验收不合格，投标人须承担相应违约责任。

15）售后服务：

★1）包含设备安装及正常运行所需费用，提供三年原厂硬件质保服务，同时提供三年特征库、威胁情报库免费升级服务，确保安全检测能力持续有效。

★2）投标人须在投标时提供产品生产厂商出具的正式售后服务承诺函，承诺提供及时、高效的故障响应及技术支持服务。

16）资质要求：

（1）设备厂商需具备商品售后服务认证证书

(2)设备厂商须具备 CCRC 信息安全应急处理服务一级证书；

（3）设备厂商需具备网络安全应急服务支撑单位证书

（4）设备厂商须具备国家信息安全测评信息安全服务资质风险评估二级，提供以上证书复印件。

服务要求：

1、通过全流量安全检测分析系统，构建集监测、响应、可视化于一体的全网流量安全综合防御体系。

2、核心功能：实现资产全面识别与规范化管理，具备安全风险提前感知与预警能力，支撑安全事件快速响应与精准处置。

3、运行机制：建立 “监测 — 分析 — 响应 — 研判 — 处置” 的全流程安全运营闭环，持续提升整体安全防护能力。

4、安全团队依托安全运营管理平台提供 7×24 小时安全威胁监测服务，对网络攻击、漏洞利用、恶意代码、内网安全风险等进行持续监测与分析。

5、现场服务：每月提供不少于 1 次现场技术支持服务，按月度提交服务分析报告。

★6、人员要求：团队人员配置不得少于 2 人，所有成员均须取得网络安全领域 CISP- PTE 专业资质证书。

打“★"号条款为实质性条款，若有任何一条负偏离或不满足

则导致响应无效。

二、变更后内容：

（一）一体化安全接入网关网络终端防火墙—功能和质量要求

1.基础要求：

设备需满足网络安全等级保护制度中安全区域边界范畴的边界防护、访问控制、入侵防范、流量控制等核心安全要求，同时兼容SD-WAN组网、上网身份认证、防火墙防护等场景化高危风险防护需求；需标配完整的特征库、威胁情报库及流量过滤、威胁检测相关功能模块。

★2.规格与性能要求：

采用1U标准机架式硬件形态，设备接口及性能指标满足以下要求：配置≥4个GE电口、≥4个GE光口、≥4个10G光口；≥2个USB2.0接口数量；配备双交流供电模块，搭载≥1TB SSD固态硬盘；整机应用吞吐量≥10Gbps，最大接入用户数≥1000，并发连接数≥500万。

3.功能要求：

1）支持双系统备份机制，支持主备系统自动无缝切换，系统切换时间小于500毫秒。

2）具备网络2至7层全流量深度识别能力，可全面识别主流应用协议，并实现精细化分级分类。

3）支持识别国内常见应用协议。

4）线路负载：

（1）支持基于源 IP、目的 IP、源+目的 IP、四元组、上下行空闲带宽、最小连接数、主备模式的多维度负载均衡策略。

（2）支持基于域名、应用协议、对象库的精细化负载均衡调度。

（3）支持虚拟线路+LAN+WAN 组合模式。

5）流量控制：

（1）支持基于全局、链路、数据流向、共享用户、移动终端、应用协议/协议组、IP/IP 群组的多维度速率管控。

（2）支持单条策略总带宽限速功能，可自定义配置总控带宽阈值。

（3）支持单条策略单 IP 独立限速功能，可自定义配置单 IP 带宽阈值。

（4）单个策略组支持多时段生效配置，满足不同场景差异化时段管控需求。

（5）支持“动态 IP 限速”功能（智能调控），可在启用此功能的链路中，针对单个 IP 设置“加速比”、“减速比”、“速度维持时间”等参数，百分比模式设置。

（6）支持策略嵌套功能，同一条策略内可实现特定对象总带宽管控、单 IP 限速、DSCP 标记等参数并行匹配，保障策略配置的灵活性与简洁性。

（7）支持带宽阈值管控功能，可针对指定链路设置带宽使用上限与下限，采用百分比模式配置。

6）流量镜像：

（1）支持基于 IP 五元组、VLAN 的流量镜像。

（2）支持基于域名和 URL 的流量镜

（3）支持基于应用协议的流量镜像

（4）支持基于协议群组的流量镜像

（5）支持端口镜像只镜像会话前 N 个包功能

（6）支持基于时间的流量镜像调度像。

7）入侵防御：

（1）系统内置漏洞利用、木马病毒、Web 攻击等常见网络威胁特征库，可快速检测并阻断网络异常攻击行为。

（2）支持按入侵事件发生时间、规则名称/分类、源目 IP 等维度展示入侵会话信息，以可视化图表呈现内网入侵事件趋势。

8）威胁情报：

（1）内置已知威胁情报库，保障威胁检测覆盖面。

（2）内置数字货币挖矿、C&C 控制节点、APT 攻击、网站后门、钓鱼网址、僵尸网络等威胁情报，实现网络异常行为深度检测分析。

（3）支持威胁情报命中监测，可查看情报命中趋势、类型分布，以及源 IP、目的 IP、源 MAC 等核心溯源信息。

9）业务级质量测量

（1）支持对每条网络会话的客户端时延、服务端时延、应用层时延指标实时监测。

（2）可精准统计客户端时延（设备至客户端网络时延）、服务端时延（设备至服务器网络时延）、应用时延（会话上下行首

包时间差）、会话上下行最大数据包长度等核心指标。

10）日志审计

（1）支持全量记录会话日志。

（2）支持全量记录URL日志

（3）支持全量DNS会话日志

（4）支持按照应用协议、URL关键字、端口号、运营商等信息进行检索和查询。

★11）产品要求

产品需符合《网络关键设备和网络安全专用产品目录》的要求。

★12）质量要求：

设备到达3个盟市分站后，依据招标文件规定及投标人投标响应内容进行逐项验收测试，各项技术指标与投标承诺一致且满足项目实际使用需求，方可通过验收；若技术参数与投标承诺不符或无法满足使用要求，则验收不合格，投标人须承担相应违约责任。

★13）售后服务：

提供不少于三年硬件质保服务，同时提供不少于三年特征库、威胁情报库免费升级服务，确保安全检测能力持续有效。

★14）服务要求：

在质保期内每月出具格式规范、内容完整的安全运维与巡检分析报告。

（二）全网流量安全威胁分析平台—功能和质量要求

1.基础要求：

通过分析网络流量、系统活动、应用程序日志及用户行为等数据，运用规则匹配、行为分析、机器学习与人工智能等方法，识别其中潜在的恶意活动与安全威胁的过程。其核心目的在于及时发现已知攻击模式和未知威胁，并发出警报，为后续的调查、溯源与响应处置提供关键依据。可满足等级保护-安全区域边界中恶意代码和垃圾邮件防范的要求，以及满足安全区域边界-入侵防范中“应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析”的高危风险要求。

★2.规格与性能要求：

本项目所投网络安全设备采用标准机架式软硬一体化架构，配置不低于：4核CPU、32GB内存、2个千兆口、2个扩展插槽、4TB硬盘；设备流量处理能力不低于10Gbps。

3.功能要求：

1）支持通过WEB图形化界面，将2个及以上管理网口绑定为聚合链路，实现管理口冗余与负载均衡。

2）流量采集与识别：支持手动与FTP批量导入PCAP包离线分析，可记录导入与检测状态；支持基于IP、端口、协议、VLAN等过滤流量；可自定义记录TCP、UDP、HTTP协议流量负载。

3）隧道封装识别：支持多层VLAN、VXLAN、MPLS、GRE等隧道流量解析。

4）流量威胁检测：系统可对Web攻击、各类网络攻击与远控、后门行为进行全面检测，支持WebShell上传、暴力破解、撞

库爆破及自定义阈值，可识别 DNS/ICMP 隐秘信道、加密流量攻击并支持 JA3 指纹；内置弱口令规则。

5）高级威胁检测：系统支持 ICMP 隧道、DNS 隧道、HTTP 隧道、远控 C&C 流量、挖矿流量、代理流量、暗网通信、弱口令行为、SSH 爆破成功、加密 WebShell 等检测。

6）日志接入与处理：支持接入不同设备类型的第三方日志数据，对不同格式和结构的第三方数据进行解析、范化转换为统一的标准格式，接入分析平台进行分析。

7）资产分析：支持对资产及资产分组间的互访行为进行专项可视化统计与智能分析，可全面呈现访问时间、源 IP/资产组、目的 IP/资产组、互访协议、目的端口、访问频次、访问拓扑、访问排行等关键信息，支持一键溯源定位原始访问日志。

8）病毒防护：静态病毒防护基本库检测率≥90%，流行库检测率≥95%，误报库误报率为零；动态病毒防护可执行恶意软件样本库检测率≥90%，恶意网页脚本样库检测率≥90%。

9）安全监测能力：支持对恶意扫描行为、钓鱼攻击、地址欺骗、漏洞攻击、恶意程序攻击、异常网络通信行为、未知威胁进行监测、并支持逃避监测防护，支持 IPV4/IPV6 网络场景的监测，支持以可视化方式提供指定时间段内，被监测网络中的特定主机与其他主机之间的相关联的已知、未知威胁事件与异常网络行为。

10）挖矿检测：

（1）支持识别包括比特币、以太坊在内的币种通信。

（2）支持挖矿阶段识别，可识别挖各矿阶段，包括恶意代码传输、远控通信、连接矿池、登录矿池、获取挖矿任务、提交挖矿份额。

（3）支持挖矿态势大屏展示，可查看矿机、挖矿攻击源、矿池、币种、挖矿阶段、挖矿告警趋势、挖矿币种活跃度情况等信息。

11）全流程溯源

（1）DNS 行为分析：支持可疑 DNS 解析，可展示 DGA 域名与 DNS 隧道域名的统计信息，并可展示 DNS 解析详情，包含域名、异常类型、请求次数、访问时间等信息。

（2）非常规访问行为分析：支持可疑代理信息展示，可展示可疑代理类型分布、可疑代理访问趋势，以及 socks、http、reDuh、RegeoryTunnel、Tunna 等代理工具产生的流量详情信息。

（3）攻击源 IP 预警支持实时显示攻击源 IP 的画像信息，包括 IP 访问行为、IP 告警信息、网络测绘信息、处置建议、威胁级别、情报标签，关注热度、首次发现时间最近发现时间等。

12）可视化展示

实现可视化大屏态势分析，包括但不限于:综合态势、挖矿态势、威胁事件态势、资产态势，实现可视化效果呈现威胁态势。

★13）质量要求：

设备到达 12 个盟市分站后，依据招标文件规定及投标人投标响应内容进行逐项验收测试，各项技术指标与投标承诺一致且满足项目实际使用需求，方可通过验收；若技术参数与投标承诺

不符或无法满足使用要求，则验收不合格，投标人须承担相应违约责任。

★14）售后服务：

提供不少于三年硬件质保服务，同时提供不少于三年特征库、威胁情报库免费升级服务，确保安全检测能力持续有效。

★15）服务要求：

建立“监测—分析—响应—研判—处置”的全流程安全运营闭环，持续提升整体安全防护能力，质保期内每月提供不少于1次现场技术支持服务，按月度提交服务分析报告。

打“★"号条款为实质性条款，若有任何一条负偏离或不满足则导致响应无效。

特此说明。

内蒙古自治区环境监测总站

2026年5月25日