原采购信息内容：

第三章 采购内容及要求

第二部分（网络安全设计）

11.防火墙：

▲6、支持主流 ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD 攻击防护，采用专业高效攻击防护算法，非采用简单的阈值进行攻击防护。（提供 CMA、CNAS 标识的检测报告并加盖生产厂商公章）

▲10、支持 SMTP，POP 协议下的垃圾邮件检测，支持防邮件炸弹功能，即设置 POP3、SMTP 的连接频率；具备一种垃圾邮件过滤方法及装置。（提供权威机构颁发的证明文件并加盖生产厂商公章）

12.网络安全准入系统

▲6、支持对网络攻击行为，如 Smurf 入侵、LAND 攻击、WINNUK 攻击等，支持对攻击行为的发现和告警。（提供第三方检测报告并加盖生产厂商公章，报告中必须有此能力体现）

13.运维安全审计系统（堡垒机）

▲4、支持 WEB 界面上传改密脚本,通过自定义脚本模式实现新增改密类型，满足多种改密需求。(提供具有 CNAS 或 CMA 的检测报告复印件并加盖生产厂商公章）

6、支持在 Oracle 数据库运维，运维人员对变量进行绑定，执行 SQL 后，堡垒机系统可审计对应 SQL 中唯一标识符的具体值，协助审计员分析安全事件。

7、支持 FTP、SFTP、SSH、RDP、SCP 等协议运维时，对传输文件进行留存，为事后朔源留下证据。

8、审计查询关键字和结果显示支持多种编码(UTF-8,Big5,EUC-JP,EUC-KR,GB2312,GB18030,ISO-8859-2,KOI8-R,KS_C_5601_1987,Shift_JIS,Window-874)，由审计管理员自主选择。

9、支持调用运维人员终端电脑上的数据库工具,不改变运维人员使用习惯：SQLPlus、PLSQLDev、ToadforOracle、Db2cmd（DB2）、QuestCentralforDB2、

TeradataSQLAssistant、SqlDbxPersonal、SqlDbxProfessional、pgAdmin3、MysqlCommand、SSMS、Dbvisualizer、Navicat、Xshell7、OracleSQLDeveloperXFTP、SecureFX、GBaseDataStudio、Navicat4Redis、DBeaver、Sqldev。

10、支持H5应用发布运维，使用H5的方式去拉取应用发布服务器上的运维工具，通过应用发布服务器去运维目标协议。支持H5应用发布运维时，通过web界面进行文件上传、下载。

14.流量分析预警探针

▲3、支持基于不完整会话流的单包攻击检测能力。（提供具有 CNAS 或 CMA 的检测报告并加盖生产厂商公章）

▲11、为了能够快速、有效的检出流量中的威胁行为，所提供探针设备需具备一种加快旁路入侵检测的方法。（提供专业机构颁发的证明文件并加盖生产厂商公章）

15.日志审计

▲8、支持全智能范式化解析模式，支持解析字段的编辑和调整，如修改字段名称。（提供具有 CNAS 或 CMA 的检测报告并加盖生产厂商公章）

16.终端威胁检测与响应系统（EDR）

▲2、产品应具备多维度的态势大屏，至少包括资产态势大屏、运维态势大屏、威胁态势大屏。展示内容至少包括威胁告警统计、攻击阶段统计、威胁等级统计、漏洞信息Top5、终端威胁告警 Top5、最新告警事件、威胁态势评分等信息。（提供第三方测评报告证明并加盖生产厂商公章）

第四章 评审办法

七、综合评分法评分细则

2.技术部分（37分）-设备及技术指标（27分）

根据对技术指标的要求，全部满足或优于技术指标要求的得 27 分。加“▲”的技术部分如有一项出现负偏离的扣 3 分，扣完为止；不加“▲”的技术部分每出现一项负偏离的扣 1 分，扣完为止。

未按招标文件要求提供对应证明材料的，视为不符合对应的技术要求。

2.技术部分（37 分）-技术安全性（10 分）

1、为保障所投防火墙系统能高效、智能、安全、健壮的进行访问控制和威胁防御，要求防火墙系统采用 VSP 通用安全平台系统软件，提供权威机构出具的证明文件并加盖生产厂商公章得 4 分，不提供不得分。

2、为保证所投终端威胁检测与响应系统（EDR）具备有效的病毒检出率和误报率，所投产品需具备主机型入侵检测产品类别的网络安全专用产品安全检测证书，且具备第三方检测报告证明病毒检出率≥99%、检测误报率＜1%；提供证明材料等 3 分，不提供或材料不全不得分。

3、为保障日志存储能力，所投日志审计系统的后端存储平台需采用高性能海量数据存储管理系统，提供权威机构颁发的证明文件并加盖厂商公章得 3 分，不提供不得分。

3.商务部分（33 分）-生产厂商实力（11 分）

1、 投标人所投防火墙生产厂商具备国家信息安全测评信息安全服务资质(安全工程类二级)、国家信息安全测评信息安全服务资质证书(安全开发类一级)、国家信息安全测评信息安全服务资质证书(安全运营类一级)，每提供一项得 1 分，最高得 3 分。

2、 投标人所投防火墙生产厂商具备信息安全应急处理服务资质（一级）、信息安全风险评估服务资质（一级）、信息系统安全集成服务资质（一级）、信息系统安全运维服务资质（一级），每提供一项得 1.5 分，最高得 6 分。

3、投标人所投防火墙生产厂商具备信息系统建设和服务能力等级证书优秀级（CS4），提供的得 2 分，不提供不得分。

变更为：

第三章 采购内容及要求

第二部分（网络安全设计）

11.防火墙：

▲6、支持主流 ICMPFLOOD\SYNFLOOD\ACKFLOOD\SYNACKFLOOD\UDPFLOOD 攻击防护，采用专业高效攻击防护算法，非采用简单的闯值进行攻击防护。

▲10、支持 SMTP，POP 协议下的垃圾邮件检测，支持防邮件炸弹功能，即设置 POP3、SMTP 的连接频率；具备一种垃圾邮件过滤方法及装置。

12.网络安全准入系统

▲6、支持对网络攻击行为，如 Smurf 入侵、LAND 攻击、WINNUK 攻击等，支持对攻击行为的发现和告警。

13.运维安全审计系统（堡垒机）

▲4、支持 WEB 界面上传改密脚本,通过自定义脚本模式实现新增改密类型，满足多种改密需求。

删除运维安全审计系统（堡垒机）6、7、8、9、10 性能参数要求

14.流量分析预警探针

▲3、支持基于不完整会话流的单包攻击检测能力。

▲11、为了能够快速、有效的检出流量中的威胁行为，所提供探针设备需具备一种加快旁路入侵检测的方法。

15.日志审计

▲8、支持全智能范式化解析模式，支持解析字段的编辑和调整，如修改字段名称。

16.终端威胁检测与响应系统（EDR）

▲2、产品应具备多维度的态势大屏，至少包括资产态势大屏、运维态势大

屏、威胁态势大屏。展示内容至少包括威胁告警统计、攻击阶段统计、威胁等级统计、漏洞信息Top5、终端威胁告警 Top5、最新告警事件、威胁态势评分等信息。

第四章 评审办法

七、综合评分法评分细则

2.技术部分（29分）-设备及技术指标（15分）

根据对技术指标的要求，全部满足或优于技术指标要求的得 15分。

（1）指标序号中标注▲项为重要技术指标共9项，共 9分，每有一项不满足扣1分；

（2）其他无标注项为普通技术指标共100项，共6分，每有一项不满足扣0.06分。

2.技术部分（29分）-

删除“技术安全性（10分）”，增加“实施技术方案（14分）”

根据供应商提供的运维技术方案进行评比：

（1）实施技术方案对交通管理综合应用平台不限于系统现状了解程度、系统业务流程、系统界面、网络架构、数据分布、软硬件运行环境配置；提供实施过程的组织、质量把控和培训方案阐述，整体方案完善并优于项目需求，得 14分。

（2）实施技术方案对交通管理综合应用平台不限于系统现状了解程度、系统业务流程、系统界面、网络架构、数据分布、软硬件运行环境配置，提供实施过程的组织、质量把控和培训方案阐述，整体方案基本满足采购人要求，得 8分。

（3）实施技术方案对交通管理综合应用平台不限于系统现状了解程度、系统业务流程、系统界面、网络架构、数据分布、软硬件运行环境配置，提供实施过程的组织、质量把控和培训方案阐述，整体方案无法满足采购人要求，得 2分。

（4）供应商未提供技术方案，得 0 分。

3.商务部分（41 分）-

删除“生产厂商实力（11 分)”，增加“技术研发（19 分)”

（1)投标人具有有效期内的公安部交通安全产品质量监督检测中心(公安部交通管理科学研究所)颁发的交通管理综合应用平台社会化服务系统外挂系统（接入安全要求)-机动车安全技术检验业务信息系统相关软件测试报告的，得 4 分；

（2)投标人具有有效期内的公安部交通安全产品质量监督检测中心(公安部交通管理科学研究所)颁发的机动车安全技术检验业务信息系统相关软件测试报告，得 4 分；

（3）投标人参与起草正在施行的机动车安全技术检验业务、机动车查验检验相关的国家或行业标准的，每提供一类得 4 分，最多得 8 分；

（4）投标人具有机动车安全技术检验业务信息系统相关的计算机软件著作权登记证书及软件产品登记测试报告的，得 3 分，提供不全或未提供不得分；

注：相关证书或证明文件的取得日期在招标公示日期之前取得有效。