# 海南政采招投标有限公司关于（项目编号：HNZC2022-080-001,万宁市公安局智能交通项目）的更正公告

## 一、项目基本情况

原公告的采购项目编号：HNZC2022-080-001

原公告的采购项目名称：万宁市公安局智能交通项目

首次公告日期：2022年7月20日

## 二、更正信息

更正事项：☑采购文件

更正内容：

**原文：**招标文件第三章采购需求A包采购需求--万宁市公安局智能交通项目硬件第二项服务要求（十）采购清单中

1.硬件设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **四** | **网络安全设备及网络设备** | | | |
| **4.1** | **网络安全设备** | | | |
| 1 | 防火墙 | 标准1U防火墙，双电源，默认支持2组bypass；标配6个千兆电口，千兆接口扩展卡：4个SFP插槽。；网络吞吐率：4Gbps，并发连接：200万；  防火墙标配功能模块包括用户识别、应用识别、访问控制、NAT转换、智能带宽管理、负载均衡、入侵防护、防病毒、URL过滤、内容过滤、VPN等，VPN模块默认提供5个IPSEC VPN客户端和5个SSL VPN客户端使用许可；防病毒库＋IPS攻击特征库3年升级服务许可。  功能要求：  1、根据防火墙转发策略，支持8元组（应用、用户等）进行流量镜像。  2、支持会话控制功能，要求能够基于源、连接数做会话数限制，支持按照用户、应用、时间、接口类型、地址、服务等方式对数据进行访问控制。  3、▲病毒防护模块预定义20种文件类型，支持自定义扫描文件类型，支持常见的压缩格式文件扫描。（要求提供功能截图并加盖厂商公章）  4、支持一对一、一对多，多对多的NAT转换，支持跨协议NAT转换，NAT64支持，NAT46支持，支持透明NAT。  5、具备对应用程序的识别和控制能力。应用程序特征库不少于2700种，并支持在线更新或手动更新，同时内置IPS特征库，特征库数量不少于3000条，支持检测库11000+，兼容CVE/CNCVE,支持事件集自定义自动和手动两种更新，支持应急事件及时更新（要求提供功能截图并加盖厂商公章）  6、▲产品内嵌自主研发的反病毒引擎，提供软件著作权证明。（提供反病毒引擎的计算机软件著作权登记证书复印件加盖公章）  7、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 3 |
| 2 | 光模块 | 千兆多模1.25G SFP 550m 850nm 光模块 | 个 | 6 |
| 3 | 防火墙 | 2U万兆防火墙，冗余电源，默认支持2组bypass，6个千兆电口，4个千兆SFP插槽，万兆接口扩展卡：2个SFPplus插槽，1个扩展槽位；网络吞吐率：16Gbps，并发连接：500万；  防火墙标配功能模块包括用户识别、应用识别、访问控制、NAT转换、智能带宽管理、负载均衡、入侵防护、防病毒、URL过滤、内容过滤、VPN等，VPN模块默认提供5个IPSEC VPN客户端和5个SSL VPN客户端使用许可；防病毒库＋IPS攻击特征库3年升级服务许可。  功能要求：  1、根据防火墙转发策略，支持8元组（应用、用户等）进行流量镜像。  2、支持会话控制功能，要求能够基于源、连接数做会话数限制，支持按照用户、应用、时间、接口类型、地址、服务等方式对数据进行访问控制。  3、▲病毒防护模块预定义20种文件类型，支持自定义扫描文件类型，支持常见的压缩格式文件扫描。（要求提供功能截图并加盖厂商公章）  4、支持一对一、一对多，多对多的NAT转换，支持跨协议NAT转换，NAT64支持，NAT46支持，支持透明NAT。  5、具备对应用程序的识别和控制能力。应用程序特征库不少于2700种，并支持在线更新或手动更新，同时内置IPS特征库，特征库数量不少于3000条，支持检测库11000+，兼容CVE/CNCVE,支持事件集自定义自动和手动两种更新，支持应急事件及时更新。（要求提供功能截图并加盖厂商公章）  6、▲产品内嵌自主研发的反病毒引擎，提供软件著作权证明。（提供反病毒引擎的计算机软件著作权登记证书复印件加盖公章）  7、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 1 |
| 4 | 光模块 | 万兆多模10G SFP+ 300m 850nm光模块 | 个 | 2 |
| 5 | 运维审计 | 1U硬件设备，单电源，8G内存，6个千兆电口，1T硬盘，2个usb接口。最高支持字符并发100路或图形并发50路,无用户数限制;  运维安全管理系统以集中监控、SSO 单点登录和身份认证为基础，实现对以SSH，TELNET，FTP，SCP、SFTP、RDP、VNC、X11、HTTP、HTTPS等工具对服务器资源进行操作管理行为的统一入口、统一认证、统一授权、统一审计。  license授权包，默认自带50个主机授权。包含3年运维服务  功能要求：  1、支持双机热备，支持系统配置以及审计日志实时同步。支持第三方负载均衡，并支持集群自带的负载均衡模块；  2、支持在线批量设备帐号修改；支持设备帐号属性添加和修改，包括帐号密码、应用参数、帐号状态、改密脚本、特权帐号、应用端口、应用密码提示、帐号类型、帐号提示符、帐号同步。  3、图形终端协议：RDP、VNC、X11，字符终端协议：Telnet、SSH，文件传输协议：FTP、SFTP，数据库类型：Oracle：PLSQL、TOAD、SQLPLUS、SQLDEVELOPER；Informix：DBACCESS；Mysql：MYSQLFRONT、HIDESQL；SQL Server：SQLserver（2000-2012）；Sybase：SCVIEW4；DB2：DB2CMD、DB2QUEST，WEB应用：HTTP、HTTPS，KVM类:DSR、DSVIEW、RARITAN、RARITAN\_CC等，其它应用：AS400、REALVNC、PGADMIN、PCANYWHERE、RADMIN、DameWare、CiscoASDM、VMware vSphere Client等协议类型均可实现单点登录，图形化应用无需安装任何客户端和控件即可实现单点登录，即通过堡垒机实现图形化应用发布功能（要求提供功能截图并加盖厂商公章）。  4、系统支持IP自动禁止功能，对连续登陆账号密码错误的来源IP自动屏蔽，可通过管理员解除屏蔽（要求提供功能截图并加盖厂商公章）。  5、系统应具备审计到FTP/SFTP传输的原始文件，并可以在审计系统上进行备份并下载查看其具体内容。对大于一定大小的FTP/SFTP运维审计中的文件可进行异地转储，并可记录文件md5值，保障文件的完整性和有效性。支持人工开关自由选择是否备份原文件（要求提供功能截图并加盖厂商公章）。  6、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 1 |
| 6 | 日志审计 | 1U硬件设备，8G内存，6个千兆电口，1T硬盘，单电源，2个usb接口。  日志审计与分析系统是基于大数据技术的新一代日志收集和分析产品。能够集中收集、管理、分析各类日志信息的日志处理平台，能够对全网海量的日志数据进行集中收集，实现日志的集中管理、实时监控、告警分析、快速检索。  license授权包，默认自带50个主机授权。包含3年运维服务  功能要求:  1、系统需提供角色划分，至少有系统管理员、审计管理员、规则配置员、普通用户等多种角色。各角色功能定位明晰，不可越权；可根据不同权限，自行定义添加角色，赋予不同的功能与权限；  2、系统内置多种类报表模板；系统提供周期性报表的功能，可立即生成报表，也可按照报表设计式样生成日报、周报、月报等；报表支持html、Excel、PDF等格式，并可以在线或下载查看；报表要求支持，面积图、饼状图、柱形图、折线图等图标模式。  3、提供用户账号的有效期控制。对连续多次登录失败的账号进行锁定，可通过管理员解除锁定，或在登录失败一定时间后自动解锁。  4、需要在在系统页面中增加用于监控关键进程状态的功能，例如：SYSLOG接收服务、SNMP接收服务、系统守护进程状态、主动获取服务、编码处理服务、提取进程服务等系统中可能使用到的，用于获取日志的进程。  5、提供用户账号的有效期控制。对连续多次登录失败的账号进行锁定，可通过管理员解除锁定，或在登录失败一定时间后自动解锁（要求提供功能截图并加盖厂商公章）。  6、需要在在系统页面中增加用于监控关键进程状态的功能，例如：SYSLOG接收服务、SNMP接收服务、系统守护进程状态、主动获取服务、编码处理服务、提取进程服务等系统中可能使用到的，用于获取日志的进程（要求提供功能截图并加盖厂商公章）。  7、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 1 |
| 7 | 漏扫系统 | 标准1U 漏扫，单电源；标配6个千兆电口，1个扩展槽位。产品提供系统扫描、WEB扫描、弱口令扫描三大功能模块；可扩展数据库扫描、基线检查模块。漏洞特征库3年升级许可。  功能要求:  1、支持65000条以上系统漏洞库，并按照漏洞类别及漏洞威胁程度进行分类；  2、▲支持漏洞库涵盖标准包含CVE、CVSS、CNVID、CNNVD、CNCVE、Bugtraq编号6种；（要求提供功能截图并加盖厂商公章）  3、支持SSH、SMB、TELNET、POP、POP3、IMAP、FTP、RSH、REXEC、WSUS协议的登陆扫描；  4、支持Web漏洞扫描检测基于OWASP Top10标准进行规则定义；  5、支持对主机设备操作系统的安全配置核查，包括：Windows系列、Linux系列、HP-UX、AIX、Solaris；  6、▲弱口令扫描服务会对信息系统内的网络设备、操作系统、应用软件、中间件和服务等进行弱口令识别，同时可按照资产组和时间导出扫描报表，报表分为详细报告和统计报表，可支持导出常见格式报表的能力，包括HTML、WORD、PDF,EXCEL、XML，报表标题可自定义等。提供弱口令检查引擎，可以基于调度任务对目标进行自动扫描，支持目前主流协议和数据库弱口令检测，包括：TELNET、FTP、SSH、POP3、SMB、SNMP、RDP、SMTP、REDIS、Oracle、MySQL、PostgreSQL、MsSQL、DB2、MongoDB等服务的弱口令信息，包括用户名、密码。检查引擎支持通过用户名字典、密码字典、用户名密码组合字典进行检测，同时支持用户自定义用户名密码字典，可以进行标准模式破解以及组合模式破解两种扫描方式进行弱口令扫描（要求提供功能截图并加盖厂商公章）。  7、支持Web登陆扫描，支持Cookie认证、Form认证、Basic认证、NTLM认证、Session认证、Digest认证、SSL；  8、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 1 |
| 8 | 网络审计 | 1G应用吞吐，最大并发连接数为100万；最大新建连接数为28000个/秒； 1U硬件；标配6个千兆电接口（其中含1个管理接口和1个HA接口）；提供2个扩展插槽；1T硬盘；单交流电源。 含专用操作系统与网络审计标准软件。 3年软件升级、URL库、应用协议库定期更新服务和3年硬件质保服务。  功能要求：  1、可集中呈现上网行为风险等级和状态，行为风险等级包括安全等级、效率等级、合规等级和管控等级  2、支持远程登录在界面实现Bypass，并可进行切换；  3、应用协议库包含的应用数量不低于7100种，应用规则总数不低于30000种。  4、支持独立的网安应用行为审计策略；（要求提供功能证明截图并厂家盖章证明）  5、不同网页被阻塞后会跳转不同的阻塞页面；支持用户完全自定义；  6、▲通过SNMP、DNS、审计策略对SNMP、DNS通信内容进行审计和控制；（要求提供功能证明截图并厂家盖章证明）  7、支持策略管理、日志审计、权限分配相互独立的三权制衡管理机制，避免超级管理员权限过大的弊端。系统管理员和审计员的账号创建，权限变更需要审核员审批才能生效。管理员和审计员的操作会形成日志受审核员监督。  8、 所投产品具备国家信息安全测评信息技术产品安全测评证书》级别为 EAL3+。（要求提供资质有效复印件并加盖厂商公章）  9、 所投产品具备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证书》《中国国家信息安全产品认证》证书。  10、 设备制造厂商具有国测信息安全服务资质-云计算安全类（一级）资质。（要求提供资质有效复印件并加盖厂商公章）  11、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 1 |
| 9 | 数据库审计 | 事件处理10000条/秒，内置4TB磁盘存储空间。标准1U机箱，双电源；标配6个千兆自适应电口，1个Console口，支持两个扩展槽位，支持液晶屏，三年硬件维保服务。  功能要求：  1、 支持的数据库：Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用Gbase、Caché、REDIS。  2、 支持旁路阻断功能（非串联方式）。阻断两种模式，宽松模式：对单一会话危险操作阻断；严格模式：源IP操作的所有请求直接阻断。  3、 支持通过Agent审计回环地址的流量。  4、 支持全文检索数据库solr的审计，可审计到solr的查询、插入行为的操作信息。  5、▲支持C/S架构COM、COM+、DCOM组件的审计，可提取应用层工号（账号）的身份信息，精确定位到人。（要求提供功能证明截图并厂家盖章证明）  6、 支持重复操作的统计规则，一定时间内重复某项操作达到设定的统计次数，则触发审计告警。  7、▲支持全文检索数据库solr的审计，可审计到solr的查询、插入行为的操作信息；（要求提供功能证明截图并厂家盖章证明）  8、 所投产品具备国家信息安全测评信息技术产品安全测评证书》级别为 EAL3+。（要求提供资质有效复印件并加盖厂商公章）  9、 所投产品具备中国网络安全审查技术与认证中心颁发的《中国国家信息安全产品认证证书》。（要求提供资质有效复印件并加盖厂商公章）  10、 设备制造厂商具有国测信息安全服务资质-云计算安全类（一级）资质。（要求提供资质有效复印件并加盖厂商公章）  11、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 1 |
| 10 | 威胁检测系统 | 2U标准上架设备（含滑轨）一台；  1、产品采集恶意事件，功能说明包括流量采集、威胁检测、关联分析、威胁告警、策略配置、日志上传、威胁日志记录、日志管理等功能；  监听口：2个千兆电口；管理口：2个千兆电口，双电源；  缺省包含：3年授权，3年软硬件维保服务，1次现场部署安装服务。  功能要求:  1、产品采集恶意事件，功能说明包括流量采集、威胁检测、关联分析、威胁告警、策略配置、日志上传、威胁日志记录、日志管理等功能。  2、▲产品内嵌自主研发的反病毒引擎，提供软件著作权证明。（提供反病毒引擎的计算机软件著作权登记证书复印件加盖公章）  3、支持对不少于6万个恶意代码家族、1400万类恶意代码的精准判定，内置规则数不少于5000万条。  4、▲支持ATT&CK、NSA/CSS威胁框架展示及搜索。（要求提供功能截图并加盖厂商公章）  5、支持基于威胁画像的事件关联分析，生成关联分析报告，实现相关事件、攻击资源、攻击载荷、受害主机、漏洞利用情况的统一呈现。  6、▲支持基于IP、协议或端口进行全流量捕获和全包存储，可根据实际业务场景进行流量捕获策略的配置。（要求提供功能截图并加盖厂商公章）  7、支持提供每日威胁情报简讯，汇总研判的威胁情报信息、搜集研判的漏洞事件、安全事件、恶意代码信息、病毒事件等资讯内容，形成威胁简报。  8、支持超过370种文件格式的检测与还原，文件分类包括文档、可执行程序、脚本、压缩包、文本、图片、多媒体、软件数据、其他格式等。（要求提供功能截图并加盖厂商公章）  9、支持将 IP、域名、 URL、标签等信息进行组合，构建自定义检测场景并配置检测策略。可监控重点外网连接情况、 屏蔽低风险事件等。  10、支持自定义流量检测规则，可按照分类、信誉、协议、版本、动作、MITRE ATT&CK（对应的策略、对应的技术点）、NSA/CSS（对应的阶段、对应的目标、对应的行为）、流量方向等信息进行新建规则。  11、支持对信息泄露的相关属性，如泄露信息类型、泄露账号、泄露源IP、泄露源端口、访问IP、访问IP所在地域、请求内容、协议等进行分析，发现信息泄露事件。  12、▲提供与其他设备的数据联动接口，支持对NSQ、HTTP POST、SYSLOG、kafka服务进行设置。（要求提供功能截图并加盖厂商公章）  13、支持通过可视化界面统一呈现威胁态势，可通过攻击地图呈现感染源，感染目标；可展示威胁概况，包括威胁次数，恶意文件数，恶意代码传播源，受害主机，二次传播源，命令控制服务器访问等信息；可展示恶意代码家族规模排行；可展示威胁能力雷达图，包括传播移动，侦查探测，杀伤破坏，监控窃取，潜伏隐匿，权限获取，埋伏预置，对抗逃逸等信息。  14、制造厂商针对本项目的授权书及售后服务承诺函。（需提供加盖厂商公章的相应材料） | 台 | 1 |
| 11 | 安全管理域接入交换机 | 1、标准1U机架式盒式交换机；  2、设备提供不低于24个10/100/1000Base-T以太网端口，不低于4个万兆SFP+，不低于1个接口业务扩展插槽（可扩展支持8个SFP+端口，整机最大支持12个万兆SFP+端口），配置2个万兆多模光模块，冗余电源模块；  3、设备交换容量不低于1.2Tbps，包转发率不低于210Mpps（官网值是X/Y值时，取最小值为标准）（提供官网链接及截图证明并加盖厂商公章或投标专用章）；  4、支持IEEE 802.1d(STP), 802.w(RSTP), 802.1s(MSTP)等二层功能；  5、支持静态路由、RIP v1/v2、OSPF、BGP、ISIS、RIPng、OSPFv3、ISISv6、BGP4+等三层路由功能； | 台 | 1 |

1. 其他

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 二 | **网络安全服务** | | | |
| 1 | 应急演练服务 | 协助用户单位制定各业务系统应急演练预案，并协助各级单位开展预案演练，提高应对网络与信息安全事件的处置能力，预防和减少网络与信息安全事件造成的危害和损失。应急演练服务主要分为三个阶段，包括应急演练准备阶段、应急演练实施阶段和应急演练收尾阶段，我们在应急演练准备阶段提供演练计划咨询、演练方案设计撰写与修订、演练前培训等工作，并在应急演练实施和收尾阶段提供全程化的指导与咨询。 | 次 | 1 |
| 2 | 安全意识培训 | 提供培训服务。培训内容涵盖网络安全意识、安全管理、安全技术、网络安全政策法规培训等四方面内容，目标群体为面向政府、企事业单位等，旨在培养具有实战攻防能力的管理和技术专业人员，提升网络安全意识、以及发现脆弱性与处置安全威胁的能力，将网络安全防御常态化。此外可以根据客户需求定制培训课程。  ·全员提供的网络安全意识培训，包括典型案例解析、日常办公中常见的网络安全问题、安全操作习惯及防范建议等；  ·提供网络安全监测、研判、应急处置、溯源分析等技术的培训；  ·提供网络安全管理体系和应急体系知识培训，帮助用户理解ISO 27001、等保、应急等相关标准要求，并学习网络安全管理体系规划的一般原则和方法；  ·提供网络安全法、等级保护制度、关键信息基础设施保护、数据安全、个人信息保护等相关政策的培训。时间≦3小时，提供培训课件，不包括学员培训场地、食宿、差旅等费用。 | 次 | 1 |
| 3 | 漏洞扫描 | 开展对指定的网络设备和服务器的漏洞扫描工作，使用合规性的漏洞扫描工具，对指定的网络设备和服务器进行漏洞扫描工作，以评估网络设备和服务器的风险等级信息、包含设备漏洞的高中低风险分布、漏洞风险类型、漏洞情况列表等安全风险等级情况，提供网络设备和服务器的安全检测和扫描评估报告，并协助做好整改处置工作； | 次 | 4 |
| 4 | 代码审计服务 | 通过开展应用系统的源代码安全审计工作，发现应用系统的安全漏洞和缺陷隐患，针对安全风险提供加固处置建议，有效降低应用系统的安全风险，保障应用系统安全稳定运行。 | 次 | 1 |

**现变更为：**删除招标文件第三章采购需求A包采购需求--万宁市公安局智能交通项目硬件第二项服务要求（十）采购清单中列出的以上内容，并将该部分内容增加至招标文件第三章采购需求B包采购需求--万宁市公安局智能交通项目软件第二项服务要求(六）采购清单表中。

更正日期：2022年7月22日

## 三、其他补充事宜

1、请各投标人登陆全国公共资源交易平台（海南省）（http://zw.hainan.gov.cn/ggzy/）下载最新招标文件。

## 四、凡对本次公告内容提出询问，请按以下方式联系。

## 1.采购人信息

名 称：万宁市公安局

地 址：海南省万宁市万城镇望海大道北侧

联系方式：0898-62230606

## 2.采购代理机构信息

名 称：海南政采招投标有限公司

地 址：海口市国贸路49号中衡大厦13楼A座

联系方式：贾玲/0898-68501635/13976096820

## 3.项目联系方式

项目联系人：贾玲

电　　 话：0898-68501635/13976096820