**小木桥路268弄办公点网络安全服务项目**

**采购需求**

# 项目背景

小木桥路268弄为上海市司法局办公地点，现有机房及网络由于建设较早，架构较为繁琐且无法进行有效的统一管理，且性能已无法满足现有工作需要。

在对机房及网络进行升级改造建设工作的同时，贯彻落实《网络安全法》网络运行安全相关规定要求，采用技术措施提升网络安全防护能力，建立完善的运维管理措施，保障网络安全、稳定、可靠的持续运行，有效应对全新形势下的新威胁和新问题。

# 项目目标

根据小木桥路268弄上海市司法局办公点的配备要求，项目实施内容主要为：

网络安全系统：对现有网络安全能力进行评估，对现有能力的不足之处进行针对性的建设，提升网络安全防护能力。

网络系统：对现有交换机及网络线缆进行更换，满足办公终端的网络接入和管控需求。

机房改造：对机房机柜进行更新替换，减少精密空调及UPS的占用空间。

# 预算资金

预算金额：156.99万元。

# 建设内容

供应单位需要负责本次项目范围内各类设备的购置、运输、安装、调试、试运行、验收、培训、保修、售后服务等工作，具体包括以下内容：

* 负责本次采购范围内购置的各类设备的深化设计、采购、安装、调试等所有内容；
* 负责项目的实施和项目协调管理，包括不在本次采购范围内的各类信息设备的配合协调工作，保证设备的全部开通和使用；
* 负责本次采购范围内购置的各类设备的联动调试、试运行、竣工验收，并根据建设单位的要求完成本项目所需的整体联动调试等；
* 负责项目的验收资料的收集、编制和管理，提交各类设备与系统的安装部署和调试报告、用户手册等；
* 根据国家相关规定、技术规范等提供本次采购范围内各类设备的培训及后续维修保养服务；

# 详细技术要求

项目内容包括：网络安全设备、一体化机柜、接入交换机、综合布线。

## 网络安全设备

本次项目主要针小木桥路268弄上海市司法局办公点的政务外网网络，进行针对性补充和完善，提升整体网络安全防御能力，实施内容包括：

防火墙系统：在网络接入区域部署，进行网络访问权限控制，对网络攻击行为进行安全检测和阻断，保障网络的安全性。需能与已有终端安全管理系统实现联动，提高网络整体安全性。

入侵防御系统：在网络接入区域部署，使用多维动态特征异常检测，能够精准、有效的检测入侵行为，提高网络整体安全性。

网络安全审计系统：在网络核心交换区域部署，能够针对内部以及外部用户访问行为进行审计，及时发现各种不合规的访问流量和访问关系。

日志分析系统：在安全管理区域部署，通过对各种安全设备、网络设备等的日志、警报等信息，进行收集、存储、审计和分析，实现全网综合安全审计。

运维安全管理系统：在安全管理区域部署，通过对网络设备、安全设备等资源的运维与审计，进行集中化运维管控、运维过程实时监管、运维访问合规性控制、运维过程图形化审计等，构建一套完善的事前预防、事中监控、事后审计安全管理体系，满足运维审计规范要求。

威胁检测与分析系统：在网络核心交换区域部署，接入镜像流量，对网内设备进行身份分析、合规检查及流量控制等安全检查或控制。

## 一体化机柜

由于机房面积较小，本项目采用一体化机柜，可以减少精密空调及UPS的占用空间，提升设备的运行环境。

## 接入交换机

小木桥路268弄办公点自建成投入使用已经多年，随着信息化技术的快速发展，原有网络建设所使用的网络设备已无法满足现有终端的网络接入需求，其性能已无法满足现有工作负载，因此本项目通过对现有网络设备进行升级改造，更好的保障工作人员的网络使用环境。

## 综合布线

通过对原有设备拆除，强/弱电桥架建设，静电地板铺设，应急照明建设，防尘处理等的实施，使机房环境能更好的满足设备的运行需求。

# 采购清单

“▲”指标项为重要指标，投标人须按要求提供功能截图证明，未提供证明材料视为未响应或不满足。

## 网络安全设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 采购技术参数要求 | 单位 | 数量 |
|  | 防火墙 | 要求网络层吞吐量不小于23.6G；并发连接不小于1200万；每秒新建连接数不小于18万；  要求千兆电口不少于12个，千兆光口不少于12个；  支持信创CPU芯片和操作系统；  要求支持冗余电源，标准机架式安装；  支持MPLS流量透传；支持针对MPLS流量的安全审查；  支持基于策略的路由负载，支持ISP路由负载均衡；  支持全面的NAT44和NAT66转换配置；  支持基于安全域、用户、地址、服务、应用、VLAN等多种方式进行访问控制；  支持命中时间分析和安全策略推荐；(提供功能截图等证明材料)  支持对常用协议的文件传输行为进行上传、下载、双向的文件类型过滤；  ▲支持共享接入检测和管控，支持阻断或告警动作；(提供功能截图等证明材料)  支持基于安全区域的异常包攻击防御；  支持防御基于安全域的IP地址欺骗攻击；  ▲支持将其他硬件安全设备（包括但不限于IPS、流量探针等）加入网元组，并接受流量编排；(提供功能截图等证明材料)  支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为；  支持基于受害主机的一键式阻断链接、记录日志等处置动作； | 台 | 1 |
|  | 入侵防御系统 | 要求满检速率不小于3.94G；并发连接不小于400万；  要求千兆电口不少于8个，千兆光口不少于4个  要求支持冗余电源，标准机架式安装；  支持基于安全域、用户、地址服务、应用、VLAN等多种方式进行访问控制；  支持应用识别，为每种应用提供预定义的风险系数，并将应用进行特征分类；  ▲支持基于不同安全区域防御Flood攻击，并支持警告、丢弃、普通防护、增强防护、授权服务器防护等多种防护措施；(提供功能截图等证明材料)  支持漏洞防护功能，支持针对应用协议的漏洞防护；  支持间谍软件防护功能，支持自定义TCP、UDP、HTTP协议的漏洞特征；  ▲支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持将解密后流量镜像到其他设备进行分析统计；(提供功能截图等证明材料)  支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，统计网络中存在安全风险的主机数量以及对应的风险等级；(提供功能截图等证明材料)  支持单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能；  支持针对“应急响应消息”的手动或自动处置； | 台 | 1 |
|  | 网络安全审计系统 | 要求抓包速率不小于470Mbps，记录事件能力不小于5000条/秒；  要求千兆电口不少于8个、千兆光口不少于8个；  要求支持冗余电源，标准机架式安装；  支持国产化CPU芯片和操作系统；  支持应用审计、HTTP审计、文件审计、FTP审计、邮件审计，支持网络异常流量检测及报警；  ▲支持ICAP策略，支持解密流量外发；支持镜像流量外发的第三方联动；（提供产品功能截图）  支持记录应用行为，并对于阻断的应用可以触发告警；  支持根据应用协议库限制每个人的应用使用时长或应用流量；  ▲支持NETBIOS审计，对NETBIOS通信、登录名及文件、目录进行审计和控制；（提供产品功能截图）  支持用户网页访问被策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；（提供产品功能截图）  支持外发内容过滤，基于关键字、正则过滤；支持对身份证号码、银行号码、电话号码等敏感信息过滤；（提供产品功能截图）； | 台 | 1 |
|  | 日志分析统 | 要求产品具备35个目标授权许可；  要求千兆电口不少于6个、千兆光口不少于4个；  要求支持冗余电源，标准机架式安装；  支持国产化CPU芯片和操作系统；  支持审计各种网络设备、安全设备、主机操作系统、数据库、中间件、应用系统的配置日志、运行日志、告警日志等；  支持通过Syslog、Syslog-NG、SNMP Trap、Netflow V5、JDBC、Agent代理、WMI、(S)FTP、NetBIOS、文件\文件夹读取、Kafka等方式完成各种日志的收集；  支持资产按多种维度进行分组、分域管理；  支持页面可视化编辑归一化策略，对页面查看的日志编辑归一化策略；  ▲支持正则表达式、Key-Value、JSON日志解析，支持日志自动化辅助范化； (提供产品功能截图)  ▲支持自动识别收集的日志并自动选择范化策略，针对匹配的多条范化策略，系统支持设置策略匹配优先级； (提供产品功能截图)  系统具备全文检索的大数据处理能力，能够对事件进行非格式化的文本式处理；  支持采用机器学习对原始日志进行聚类分析，能够对原始日志结构模式进行自动识别； (提供产品功能截图)  支持单事件关联和多事件关联，能够针对多个不同类型不同来源的安全事件进行综合关联分析； | 台 | 1 |
|  | 运维安全管理系统 | 要求产品应具备50个目标授权许可；  要求千兆电口不少于6个、千兆光口不少于4个；  要求支持冗余电源，标准机架式安装；  支持国产化CPU芯片和操作系统；  ▲支持多因子认证，包括动态令牌、USBKey等多因子认证；支持不同用户配置不同多因子认证方式；（提供产品功能截图）  支持SSH、RDP、VNC、Telnet、FTP、SCP、SFTP、Rlogin等运维协议；  支持使用浏览器通过H5方式即可运维SSH、RDP、Telnet、VNC资源，无需安装任何插件；  ▲支持资源按标签管理，并可以对资源批量添加和删除标签；（提供产品功能截图）  支持针对核心设备可配置双人授权，需要管理员现场审批才能访问资源；（提供产品功能截图）  支持工单管理，通过工单申请需要访问的资源的权限；  支持对协同用户的操作审计，所有操作关联到实际的操作人员； | 台 | 1 |
|  | 威胁检测与分析系统 | 要求流量处理吞吐不小于1Gbps；；  要求千兆电口不少于6个、接口板卡扩展插槽不少于2个；  要求支持冗余电源，标准机架式安装；  支持常见协议识别并还原网络流量；  支持对流量中出现文件传输行为进行发现和还原；  ▲支持手动批量导入PCAP包对离线流量采集，支持通过配置FTP方式批量导入PCAP包对离线流量采集；（提供产品功能截图）  支持基于流量实时IOC匹配功能，设备具备主流的IOC；支持基于威胁情报的威胁检测；  支持检测针对WEB应用的攻击，支持跨站请求伪造CSRF攻击检测；支持其他类型的WEB攻击；  支持基于工具特征的WEBSHELL检测，支持基于webshell函数、加密webshell的攻击检测；  支持根据威胁情报、检测规则、用户配置数据，来检测失陷主机通信活动行为；  支持用于恶意软件检测的 SSL/TLS 客户端指纹识别；▲支持deimos，merlin，viper，silver等黑客工具的检测；（提供产品功能截图）  支持自定义弱口令字典、规则的弱口令检测；  支持基于网络请求的语义分析检测，详细展示请求内容，并能提升对未知威胁检测能力；  支持基于IP地址的旁路阻断，能够在实时镜像的流量中发现恶意IP并实现实时阻断；支持基于URL的旁路阻断，并能将URL请求进行重定向；（提供产品功能截图）  支持AES256、SM4数据传输加密；  支持将威胁告警外发集中管理平台，支持与集中管理平台进行联动，统一进行情报、规则的升级； | 台 | 1 |

## 一体化机柜

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 采购技术参数要求 | 单位 | 数量 |
|  | 一体化机柜 | ▲UPS、空调、配电、服务器机柜、监控主机、管理系统、监控采集器为同一品牌。  ▲UPS、配电、监控、空调一体化集成在一个综合柜，设备柜在综合柜两侧灵活扩展  机柜整体防护等级不小于IP20  IT机柜（宽×高）：600x2000（含通道）\*3台  机柜静态承载能力≥1500kg（提供第三方检测报告）  机柜所有面板可支持单独拆卸和拼装  机柜采用专用的机柜并柜连接件，应支持无需拆卸机柜门情况下实现机柜并柜功能。  机柜采用前后封闭设计，前后门单开，前门配置双层玻璃，以便内部设备可视，并降低设备运行声音。  机柜后门应采用密闭钣金门，并敷设保温层，防止内外温差导致的凝露  机柜的前门、后门及侧板均可锁定，用提供的专用钥匙打开。  前后门开启角度不小于120°。  机柜应配备自动弹门装置，方便紧急情况下自动弹开，提供消防联动和应急散热的功能。  各配电单元：UPS、配电盒、电源指示均模块化设计，机架安装便于维护  配电模块应配置C级防雷器，防雷器前端需具有防雷保护开关，同时具有防雷开关或防雷器故障指示的微动开关  UPS输入电压范围单相80~280V AC  UPS容量：10kVA  UPS输出功率因数：1.0  UPS最高效率不小于96%,在125%的额定负载时，可持续5min  每个机柜应配置两条国标配电排，单条配电排支持不少于20个10A和4个16A插孔  风冷空调，制冷量不小于12.5Kw  制冷量调节范围：20%~100%  空调风量不小于2600m³/h  空调应具备低载无凝露的设计，可以使低负载（最低10%）、高湿环境中冷通道的湿度下有效除湿  ▲需提供CE、CCC，第三方节能认证；CRAA认证、ROHS报告  模块应配备10英寸以上的统一监控显示屏，支持多点触控，可实现对模块所有动环进行监控；  显示屏支持面部识别，可通过面部识别方式登录系统/开启机柜门  前后门智能门锁，可检测门开关状态，支持本地钥匙打开，并支持通过密码、面部识别等方式打开机柜门。 | 套 | 1 |

## 接入交换机

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 采购技术参数要求 | 单位 | 数量 |
|  | 接入交换机 | 交换容量≥1.28Tbps，转发性能≥426Mpps ，需提供彩页及检测报告。  支持可插拔的双电源，支持模块化可插拔双风扇和前后风道。  设备高度：≤1U。  端口要求：24个千兆电口 ，4个万兆SFP+，1个扩展插槽。  支持双 10G 上传链路连接相应汇聚交换机。  支持在线式软件升级而不影响网络的使用以及表现。  支持 IPv6 以便后期 IPv6 的部署升级。  支持端口镜像、链路聚合等基础功能。 | 台 | 2 |

## 综合布线

包含原有设备拆除，强/弱电桥架，原有设备上架，新建网络安全设备安装调试，静电地板，应急照明，机房接地，防尘处理，辅料辅材等。

# 项目集成

## 总体要求

1. 供应单位负责本次项目现场环境调研，包含网络环境、安全体系架构、业务系统现状等多方面，为本次项目顺利实施做好前期准备工作。
2. 供应单位提供的产品应满足采购需求技术指标，应是市场主流设备（不接受已停产或即将停产的设备），具有在中国境内的合法使用权，且产品均为中国境内生产的产品。
3. 供应单位提供的防火墙设备，对原有网络具有良好的兼容性，能够与已有的终端安全管理系统进行联动；供应单位提供的日志分析系统、威胁检测与分析系统，能够与上海市司法局实现级联管理。（需提供证明文件）
4. 供应单位应本着认真负责态度，组织技术队伍，认真做好本次数据安全系统建设的实施工作。
5. 供应单位应参照涉密系统建设项目加强安全保密管理，对参与建设的单位和人员开展安全保密教育，严禁对外泄露上海市司法局信息及相关文档资料。

## 产品要求

供应单位需提供合法获得网络安全设备系统（含防火墙、入侵防御系统、网络安全审计系统、日志分析系统、运维安全管理系统、威胁检测与分析系统等6个）、一体化机柜、接入交换机产品的原厂授权服务承诺函或原厂商授权书。

## 系统测试

系统经过完整测试后，才能正常进入验收环节。测试包含系统整体性能和压力测试、与原有系统对接的测试、安全策略联调测试。

# 培训服务

1. 供应单位应提供完善的项目培训方案，包括培训内容、方式等。
2. 供应单位应对本系统的相关使用者提供产品的安装、日常操作和管理维护，以及基本的故障诊断与排错等培训。

# 售后服务

1. 本项目提供3年免费的保修服务，保修日期从系统验收之日起开始计算。
2. 供应单位需承诺在接到故障报修后1小时内到现场、4小时内修复故障。如遇系统硬件故障无法在故障恢复时间（24小时）内及时解决的，需提供同等性能的备用设备供临时使用。
3. 供应单位应有完善的技术支持与售后服务体系，提供技术支持和保障服务。当发生网络安全事件时，技术服务团队在接到客户通知后，需赶赴现场进行溯源分析和应急处理，提出解决方案并工作直至故障修妥完全恢复正常服务为止。
4. 在保修期内由于设备本身质量原因造成的任何损伤或损坏，供应单位须免费负责修理或更换。

# 项目人员

本次项目实施过程中需根据对项目的理解，提供人员配置管理计划，采购人有权根据实施情况要求更换项目经理和实施人员。

项目经理具有项目集成项目管理工程师证书的为优。

为保证项目顺利实施，供应单位在项目实施期间需提供现场不少于3人的项目实施团队，提供项目组成员姓名、在本项目中的职责及以前参与过的项目情况说明等，并提供对应的社保证明。

为保证项目的服务质量，供应单位在本市需能提供良好的专业技术支持和售后服务。

# 供应商资质要求

（一）符合《中华人民共和国政府采购法》第二十二条规定的供应商。

（二）根据《上海市政府采购供应商登记及诚信管理办法》已登记入库的供应商。

（三）未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单。