

## 技术要求

采购包 1:

标的名称: 租赁城东派出所等 25 个单位网络链路服务

序号	符号标识	技术要求名称	技术参数与性能指标
1		公安专网链路服务	公安专网链路服务 25 条: ★1. 链路带宽 $\geq 1000\text{Mbps}$ , 上下行对等, 采取物理点对点专用透明传输电路, 禁止使用报文交报、共享网络等电路 (如各类 PON、VPN、PTN 等); 2. 单点网络延迟 $\leq 5\text{ms}$ ; 3. 链路过载丢包率 $\leq 0.01\%$ ; 4. 时延抖动上限值为 $50\text{ms}$ ; 5. 链路长期丢包率 $\leq 1 \times 10^{-7}$ ( $10$ 的负 7 次方); 6. 链路有效传输速率不低于带宽的 95%。
2		公安天网链路服务	公安天网链路服务 25 条: ★1. 链路带宽 $\geq 1000\text{Mbps}$ , 上下行对等, 采取物理点对点专用透明传输电路, 禁止报文交报、共享网络等电路 (如各类 PON、VPN、PTN 等); 2. 单点网络延迟 $\leq 5\text{ms}$ ; 3. 链路过载丢包率 $\leq 0.01\%$ ; 4. 时延抖动上限值为 $50\text{ms}$ ; 5. 链路长期丢包率 $\leq 1 \times 10^{-7}$ ( $10$ 的负 7 次方); 6. 链路有效传输速率不低于带宽的 95%。
3		网络防火墙	网络防火墙 1 台: ▲1、硬件架构: 采用非 X86 64 位多核高性能处理器和高速存储器架构 (多核架构需提供证明材料), 内存 $\geq 2\text{G}$ , 高度 $\geq 1\text{U}$ ; 2、支持扩展 $\geq 2$ 硬盘扩展槽位, 可扩展 480G M.2 硬盘 $\geq 2$ 个; ▲3、三层吞吐率 $\geq 5\text{Gbps}$ , 应用层吞吐 $\geq 800\text{Mbps}$ , 适用带宽 $\geq 550\text{Mbps}$ , 带机量 $\geq 1200$ 人, 自带 125 条 SSL VPN 用户数量授权, SSL VPN 并发用户数 $\geq 700$ 人 并发连接数 $\geq 150$ 万, 新建连接数 $\geq 3\text{W}$ , 默认自带单电源; ▲4、防火墙支持被 SDN 控制器纳管; 5、安全策略支持基于地理位置的防护策略; (提供功能截图, 并加盖投标人公章。) ▲6、支持至少 5700 种的 Web 特征的攻击检测和防御; (提供功能截图, 并加盖投标人公章。) ▲7、支持识别主流摄像头终端 (包含海量威视、大华、华智、宇视), 当终端流量流经设备时, 设备可以分析并提取出终端信息, 例如终端的厂商、型号等, 并支持在终端信息发生变更时 (比如将原厂商的摄像头换为其他厂商的摄像头) 向用户发送日志, 提示用户; (提供功能截图, 并加盖投标人公章。)

		<p>▲8、支持应用风险评级，并可包括但不限于安全策略分析、源安全域分析；（提供功能截图，并加盖投标人公章。）</p> <p>▲9、支持病毒库≥600 万，支持勒索病毒防护；（提供功能截图，并加盖投标人公章。）</p> <p>10、支持超过 22000 种特征的攻击检测和防御、支持“永恒之蓝”、“震网三代”、“暗云 3”、“Struts”、“Struts2”、“Xshell 后门代码”等攻击特征防护，支持自定义入侵防御规则；（提供功能截图，并加盖投标人公章。）</p> <p>11、支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证号、信用卡号、银行卡号、手机号等类型进行匹配；（提供功能截图，并加盖投标人公章。）</p> <p>12、支持基于 IP 地址、收件人和发件人设定邮件控制列表；支持基于邮件主题和内容的关键字过滤；（提供功能截图，并加盖投标人公章。）</p> <p>13、支持基于 IP 信誉的垃圾邮件过滤机制；（提供功能截图，并加盖投标人公章。）</p> <p>14、支持 HTTPS 加密流量的安全检测，支持 TCP 代理和 SSL 代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务；（提供功能截图，并加盖投标人公章。）</p> <p>15、支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发，避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率；（需提供设备功能界面截图证明，并加盖投标人公章。）</p> <p>16、能够防范 DOS/DDOS 攻击：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP 分片报文、ARP 欺骗、ARP 主动反向查询、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描、端口扫描等攻击防范；</p> <p>▲17、支持国密 SM1/2/3/4 算法；（提供功能截图，并加盖投标人公章。）；</p> <p>18、具备中国网络安全审查技术与认证中心颁发的 EAL4 增强级认证证书及信息产业信息安全测评中心出具的防火墙 EAL4+级型式试验报告；</p>
4	安全网关	<p>安全网关 25 台：</p> <p>▲1、设备支持 WAN 口≥2*GE，LAN 口≥3*GE，LAN/WAN≥2*GE，USB3.0≥1 个；</p> <p>▲2、带机量≥100；</p> <p>▲3、适用带宽≥1000Mbps；</p> <p>▲4、内存≥256MB；</p> <p>▲5、NAT 会话数≥4 万，（提供官网截图，并加盖投标人公章。）；</p> <p>▲6、内置无线控制器功能，支持管理 AP，最大支持管理 32 个 AP，（提供官网截图，并加盖投标人公章。）；</p> <p>▲7、支持 IPSec VPN，吞吐可达 100Mbps，支持隧道数≥100，（提供官网截图，并加盖投标人公章。）；</p>

		<p>8、支持固定 IP 地址、DHCP 自动获取地址、PPPoE 拨号等多种方式，支持链路状态检测功能，支持 ICMP、DNS、NTP 等检测方式，支持静态路由和策略路由；</p> <p>9、支持端口划分 VLAN，中小场景节省交换机成本；</p> <p>10、支持 MAC 地址学习、广播风暴抑制、流量镜像功能；</p> <p>▲11、支持精细化流控，支持每 IP 限制流量、支持基于用户组限制流量、支持绿色通道功能，（提供官网截图，并加盖投标人公章。）；</p> <p>12、支持 MAC 地址过滤功能，支持 MAC 地址黑白名单；</p> <p>▲13、支持多种负载均衡，支持基于运营商目的地址负载分担、支持基于链路带宽负载分担、支持基于用户（IP 地址）负载分担、支持策略路由指定线路转发、支持端到端链路检测与备份功能，提供官网截图；</p> <p>14、支持基于源目的地址、端口定义防火墙过滤策略、URL 过滤，网站黑白名单，关键字模糊匹配、支持 HTTP 下载文件过滤功能、支持 ARP 扫描、ARP 检测、ARP 防护等功能、支持互联网常见应用识别和控制、支持 IP 地址流量统计和排名、支持异常主机流量防护功能；</p> <p>▲15、支持短信、微信公众号、账号等多种接入认证方式（需要配合云简网络管理平台）；（提供官网截图，并加盖投标人公章。）</p> <p>▲16、支持多种防攻击功能，支持 DDoS 攻击防范和统计、防止 WAN 口的 Ping、防止 TCP syn 扫描、防止 TCP Stealth FIN 扫描、防止 TCP Xmas Tree 扫描、防止 TCP Null 扫描、防止 UDP 扫描功能、防止 Land 攻击功能、防止 Smurf 攻击功能、防止 WinNuke 攻击功能、防止 Ping of Death 攻击、防止 SYN Flood 攻击功能、防止 UDP Flood 攻击功能、防止 ICMP Flood 攻击功能、防止 IP Spoofing 功能、防止碎片包攻击、防止 TearDrop 攻击、防止 Fraggle 攻击功能；</p> <p>17、支持 DHCP Server、支持 NTP Client、支持 DDNS（花生壳和 3322.org）、支持 UPnP 等网络特性。</p> <p>18、支持 WEB 管理页面、支持云管理平台远程管理、支持 APP 管理；</p> <p>▲19、提供工信部电信设备进网许可证证书复印件；</p>
5	威胁检测	<p>威胁检测 2 个：</p> <p>1、产品采用 B/S 架构，支持通过 HTTPS 方式登录管理控制台，管理控制台访问需进行加密访问；</p> <p>▲2、支持一个管理控制台同时管理 Windows,Linux,信创操作系统，同时支持这些操作系统的服务器版和客户端版；</p> <p>3、一体化管理，统一客户端，统一服务端提供病毒防护、检测响应、运维管控、基线核查、漏洞管理、虚拟补丁等多重防护能力；</p> <p>4、支持上传多种格式文件，并将文件下发给多个终端，可设置分发的时间、存储位置、执行方式等，查看分发结果；</p> <p>▲5、客户端支持多级分组管理，支持多级分组的创建、删除、</p>

		<p>移动至新分组；</p> <p>6、支持设置统一管理平台登录密码的安全策略，包括不限于密码有效期、密码最小长度、密码复杂度等</p> <p>7、提供灵活的策略管理能力，支持下发全局策略以及分组策略；</p> <p>8、平台保留扩展能力，可基于数据和日志接口，可根据需求开放能力接口与第三方平台系统联动对接，如终端软件安装资产数据信息的对接，安全日志、告警信息的对接；</p> <p>9、支持按小时级的周期性安全评估，同时支持手动触发的立即评估；</p> <p>10、支持统计并折线图展示最近 24 小时、7 天、30 天的安全评分趋势；</p> <p>▲11、支持统计并呈现最近 24 小时、7 天、30 天的不同来源的病毒入侵风险趋势折线图。病毒来源分为：本地或网络驱动器、Web、电子邮件、移动设备、其他来源；</p> <p>▲12、推荐措施支持一键处置、手动标记处置、忽略、单个策略处置等多种处置方式；</p> <p>▲13、对于恶意文件处理措施至少支持三种以上，包括厂家推荐措施、统一处理措施、以及针对不同类型病毒/恶意软件提供不同处理措施，同时不同病毒/恶意软件类型不少于 5 种分类；</p> <p>14、具备爆发阻止功能，管理端可配置爆发阻止策略，封堵共享目录；</p> <p>15、支持管理员自定义 SHA1、MD5 黑名单，并可指定其动作包括：（阻止，隔离，记录）</p> <p>▲16、终端行为日志记录的时候，可指定忽略记录指定的 IP，网络协议，进程的事件；</p> <p>▲17、支持自定义可疑操作检测规则：自定义规则的规则条件为 shell 命令内容匹配的正则表达式等。自定义规则支持设置风险等级、应用主机范围；</p> <p>18、提供压缩文件扫描功能，可以对超过固定大小文件不予扫描，以减少扫描时间；</p> <p>▲19、支持进程阻断自动化响应动作：针对自定义进程规则，支持配置进程阻断的自动化响应动作；</p> <p>20、支持 USB 外设进行管理，提供允许、禁用的控制能力，包括光驱、打印机、扫描仪、手机/平板、红外等设备；</p> <p>21、支持对 USB 存储设备进行只读、读写、读写执行、禁用的权限控制；</p> <p>▲22、支持基于外设 ID，VID/PID 的白名单配置；</p>
6	信创终端准入管理	<p>一、系统要求：</p> <p>1、识别、扫描识别准确的发现接入网络环境中信创终端的 MAC 厂商、状态、IP 地址、MAC 地址、设备类型、系统类型，所连接的交换机端口。</p> <p>2、支持对信创入网终端进行安全检查，并对安检进度提供进度条提示，未通过安检的终端给出未通过项提示并阻断入网，支持用户在管理界面编辑安检结果显示内容。支持安检未通过终端一</p>

		<p>键修复功能。</p> <p>3、支持对信创终端进行基于“一机两用”程序的认证，对未安装“一机两用”客户端程序计算机给予隔离及重定向。</p> <p>▲4、支持对已经安装“一机两用”客户端，但是版本号不合规设备进行强制认证，给予隔离及重定向，并支持对将来的版本进行更新检测。（提供功能截图，并加盖投标人公章。）</p> <p>5、入网审核，设备完成注册后，支持安全管理员人工或自动审核，只允许通过使用申请通过的账号认证接入网络。</p> <p>6、要求支持准入流程差异化控制，可根据准入策略控制终端仅注册、仅认证、注册及认证、注册认证并安检等差异化准入。</p> <p>7、信创终端安全检查，支持对信创终端用户弱口令、用户密码安全策略、高危端口等安全项目进行检查，禁止安全检测未通过的终端访问网络。</p> <p>▲8、支持在现有公安信息网网络准入控制系统进行功能升级和增加授权点数的方式实现对信创终端的准入管理，本次项目要求提供不少于 200 点信创终端管理授权。（提供技术实现承诺函，并加盖投标人公章）</p> <p>▲9、信创准入客户端至少兼容中标麒麟、银河麒麟、统信 UOS 等终端信创操作系统，可对终端进行安全管控。（提供功能截图，并加盖投标人公章。）</p> <p>10、支持对信创终端的杀软软件安装情况进行安全检查，对未安装杀毒软件的终端进行网络隔离。</p> <p>11、支持对信终端的 IP 和 MAC 绑定认证，仅允许已经绑定的 IP/MAC 终端在指定认证时间内接入到网络中，防止终端随意更改 IP 地址冒用其他用户进行非授权网络访问。</p> <p>12、支持对信创终端的系统进程、软件安装、系统服务等系统环境进行安全检查，对不符合安检项的终端进行网络隔离。</p>
7	准入功能升级	<p>1、数据同步服务支持与公安专用数据处理服务对接联网设备保护、一机两用注册/卸载和无效阻断等信息。（提供功能截图，并加盖投标人公章。）</p> <p>2、支持通过 Kafka 和 ActiveMQ 两种技术方式进行数据传输，为确保数据安全数据传输中间件须具备密码验证功能。</p> <p>▲3、通过对现有准入网关系统进行功能升级的方式，实现与“一机两用”监控系统的联动管理。</p> <p>4、同步的保护信息至少包含 IP、服务器 IP、引用次数、同步时间等信息；无效阻断列表至少包含设备 IP、设备 MAC、类型、服务器 IP、原因编号、同步时间等字段。</p> <p>5、同时支持准确查询和模糊查询两种方式对注册信息、保护信息和无效阻断信息进行查询。</p> <p>6、支持通过配置，当出现同步的黑白名单与本地黑白名单的默认网络处置方式时是放行或阻断。</p> <p>▲7、要求对现有准入网关客户端软件进行升级，实现与公安信息网“一机两用”监控系统客户端一体化融合部署。</p>