**大数据安全防护体系（硬件）采购需求**

### 一、项目概况

根据党中央“以安全保发展、以发展促安全”的指导思想，落实浙江省“公安大脑”建设总体方案，依据公安大数据安全技术要求，在确保网络架构稳定、设备可靠、边界清晰，充分考虑现网运行情况下，合理规划网络安全架构、业务安全架构、数据安全架构、云平台安全架构，从而构建内生安全能力，推进公安大数据安全体系“一中心、两体系、两能力”的建设，有力支撑温州市公安大数据智能化建设应用。

### 二、建设目标

根据公安大数据智能化安全体系的指导思想、设计原则、建设思路，构建基于云计算、大数据、新一代公安网的安全、可信、合规的立体化纵深防御体系，形成科学实用的“体系化安全防护能力、规范化安全管理能力、综合化安全运维能力”，重点打造“一个中心（即安全管理中心）、两个体系（即零信任体系、安全防护体系）、两个能力（安全访问能力、数据交换能力），做到全网安全态势敏锐感知，安全威胁快速检测与处置，确保大数据全程可知、可控、可管、可查，变静态为动态，变被动为主动，为公安大数据智能化建设提供严密安全保障。

本项目建设目标如下：

网络接入控制系统建设

根据新一代公安信息网保护要求，应对入网设备进行安全管控，实现分类准入控制，防止外来设备随意接入新一代公安信息网带来安全风险；采用技术手段对终端主机、服务器、网络设备、安全设备等多样化资产进行有效准入控制，采用基于设备特征技术、网络流量镜像分析技术、虚拟网关技术等先进的准入手段，建立分类精确准入机制，实现对接入设备的准入控制管理；建立注册审核、安全检查等基线规则，对入网设备安全性进行评估，合规设备才允许入网。秉承“不改变网络、不依赖网络设备、部署简单”的特性，并兼容各种复杂的网络环境，支持分布式快速部署，解决非法设备随意新一代公安信息网的问题，达到“信任接入、接入可知、接入可管”的管理规范。

### 三、建设内容

网络接入控制设备1台（意向品牌：远望）

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 运行环境 | 采用国产化标准机架式的硬件设备，专用安全加固操作系统，系统支持采用B/S架构进行配置管理维护。 |
| 硬件参数 | CPU支持海光，基于X86架构，主频≥2.0Ghz，硬盘：≥1TB硬盘；网络接口：≥6个千兆电口，2个万兆光口；其他接口：≥1个VGA接口，≥2个USB接口 |
| 性能指标 | 最大镜像流量：20Gbps；设备入网控制IP点数：≥3000点 |
| 资产发现 | 支持以主动扫描和交换机信息采集等技术手段发现网络内部的存活资产。 |
| ★资产识别 | 支持计算机设备、网络设备、安全设备、安防设备、办公设备等网络内存活资产设备的发现和资产类型识别。支持网络内资产异常在网状态监测，包括：资产IP和MAC变化、MAC和交换机端口变化等。（需提供公安部信息安全产品检测中心等权威测评机构对该项功能的检测结果作为证明） |
| IP资源管理 | 支持从C类段的维度查看管控范围内IP使用情况，当前未存在设备的C类段不做展示； |
| 支持从组织结构的维度查看某个部门IP范围内IP使用情况，并以C类段分段展示。可选择的C类段包含当前未存在设备的C类段，但不包含已分配给下级部门的C类段。 |
| 注册管理 | 1）支持注册IP审核,需展示信息包含：IP地址、MAC地址、责任人、联系电话、所属部门、设备所在地、审核状态、申请时间，其中待审核数据支持操作审核通过、审核不通过。 |
| 2）支持注册审核开关配置，开启注册审核后，新安装终端代理程序的设备需管理员审核通过后允许入网。 |
| 3）支持注册密码启用/禁用状态切换，启用后支持设置生效方式（永久生效、生效天数、生效次数）、禁止注册时间段。 |
| 卸载管理 | 1）支持根据终端代理程序卸载时的序列号生成卸载密码； |
| 卸载密码审核列表展示信息包含：设备IP地址、申请人姓名、卸载区域标记、卸载序号、申请理由、申请时间、审核状态，其中待审核数据支持操作审核通过、审核不通过； |
| 2）提供对监测代理程序卸载日志信息查询，展示信息包含：IP地址、MAC地址、责任人、联系电话、所属部门、卸载时间、设备当前状态。 |
| 设备统计 | 每日统计设备注册状态，并支持按区域、按部门进行统计查询，包含：IP设备总数、应注册数、已注册数、保护数、非应注册数、应注册未注册数、应注册未注册已保护数、注册率； |
| 定时对设备类型进行统计，并支持按区域、按部门进行统计查询； |
| 每日统计杀毒软件安装情况，包括：未安装杀毒软件设备数、杀毒软件覆盖率，并支持按区域、按部门进行统计查询。 |
| 入网申请和审核 | 申请者通过引导页发起设备入网申请，管理员在后台审核，通过审核的设备会置成保护状态，申请者可在引导界面查询审核状态。 |
| 批量入网申请和审核 | 申请者通过引导页发起设备批量入网申请，管理员在后台审核，审核后可在引导界面查询状态。 |
| 接入控制日志 | 查询接入控制日志，包括源IP、目的IP、执行动作、上报时间等信息。 |
| 准入名单管理 | 支持合规（白名单）和不合规（黑名单）两种模式实现设备入网控制； |
| 支持多种入网规则配置，包括：设备信息完整性、第三方设备入网名单等。 |
| 审核配置 | 配置入网申请的审核方式及审核过程中是否开启短信通知。 |
| 准入控制配置 | 支持策略路由、透明网桥、802.1x、旁路镜像（SPAN）等多种准入控制技术； |
| 支持为不同网络区域配置差异化入网认证和访问控制规则。 |
| ★基于客户端通信的设备网络通信控制 | 终端双方要实现通信必须进行终端代理相互连接，若连接不通过，则其通信请求会被认为是非法且被客户端阻断，反之，连接通过则可以进行通信。（需提供公安部信息安全产品检测中心等权威测评机构对该项功能的检测结果作为证明） |
| ★设备替换阻断 | 能自动识别网络摄像机的接入，在开启接入控制时，能对网络摄像机自动放行，当网络摄像机的IP地址被替换为其他设备时能自动对替换设备进行接入控制。（需提供公安部信息安全产品检测中心等权威测评机构对该项功能的检测结果作为证明） |
| 入网安检 | 提供已安装客户端的终端设备在接入网络前进行安全检查，检查项包括：杀毒软件、补丁检查、不可信进程、不可信软件、账户弱口令、来宾账户、必要服务、必要软件，其中对于杀毒软件和必要软件可配置软件推送安装。对不符合安全要求的终端设备进行断网隔离，修复完成后才能入网。 |
| 安检日志 | 提供入网安检设备的安检日志查询功能，包括设备IP地址、MAC地址、责任人、部门、规范名称、安检时间、安检状态、安检描述等信息。 |
| 保护管理 | 提供自动保护、自动取消保护、第三方保护、手动批量保护和手动批量取消保护的规则配置，并可查询自动保护设备和自动取消保护设备的列表。 |
| 认证服务管理 | 支持多种认证服务配置，包括：系统内置Radius服务认证、外部Radius服务认证、第三方web登录认证等。 |
| 成效报告 | 成效报告按月生成，内容包含：当月的注册率变化趋势、非法设备访问拦截情况、安检通过率变化趋势和安检通过设备情况统计。 |
| 入网安全配置 | 支持各类入网安全模板配置，包含：入网安全须知、终端代理安装说明、结束进程方法说明、卸载软件方法说明、弱口令修改方法、禁用来宾用户说明、杀毒软件下载地址、必须安装的补丁、必要软件下载、必须开启的服务。 |
| 短信配置管理 | 短信配置：包含短信网关地址、短信签名、唯一认证码； |
| 手动发送短信：给指定手机号发送自定义短信内容； |
| 自动发送短信规则支持的业务种类：入网申请短信、卸载密码短信、批量入网短信，支持规则的新增、编辑、删除； |
| 短信池：根据业务种类查看未发送及已发送短信列表，展示内容包含业务种类、接收人、短信内容、短信来源、状态、录入时间、执行时间，支持情况未发送短信的操作。 |
| 假期管理 | 支持假期的新增、编辑、删除，假期配置包含：开始时间、结束时间、描述。 |

服务要求

1、免费维护期为5年，自设备通过验收之日起计算。

2、设备供应方应根据采购方的需求，对所提供的系统保证全面、有效、及时的技术支持和售后服务。

3、在免费维护期内，设备供应方应向采购方提供7\*24 小时的服务响应，保证招标方可以随时找到相应的技术人员，如有必要，要在24 小时之内赶到现场予以技术支持。