## 一、 项目概述

青羊区人民法院已经建设了防火墙、态势感知堡垒机、漏洞扫描等安全设备，满足了青羊区人民法院内网基本的安全建设要求，但随着安全形式的发展和法院业务发展需求的增加，在终端准入、日志审计以及互联网上网行为管理方面还存在明显的不足。因此，在此次建设中要加强终端准入、日志审计以及互联网上网行为管理的建设。

实现目标：此次建设希望达到三个效果：1、在法院内网所有的终端都需要经过认证才能接入到法院专网，避免任意人员用法院专网的线路直接接入到法院专网中；2、实现日志统一管理；3、在互联网中实现行为管理，同时达到带宽的有效控制，保障重要业务优先使用。

具体内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 品目号 | 标的名称 | \*数量 | 所属行业 |
| 1-1 | 内网安全准入系统 | 1套 | 软件和信息技术服务业 |
| 1-2 | 上网行为管理系统 | 1套 |
| 1-3 | 日志审计系统 | 1套 |

## 二、商务要求

\*1、交货时间及要求：成交供应商应于合同签订之日起30日内完成设备安装调试、应用培训、部署上线等工作。

\*2、交货地点：成都市青羊区人民法院。

\*3、付款条件（进度和方式）：合同签订之日，采购人收到发票后10个工作日内，向成交供应商支付合同总额的40 %作为预付款；货物安装调试、操作培训完成后，采购人组织验收，在验收合格后并收到成交供应商发票后10个工作日内支付合同总额的60 %。

\*4、包装与运输：

1）包装：设备包装应坚固完好，能抗御运输、储存和装卸过程中正常冲击、振动和挤压，并便于装卸和搬运。设备包装前检查包装材料的材质、规格和包装结构与所装产品的规格和重量相适应。组件包装时安全，防止撞击，包装表面应清洁。组件排放整齐，不可有高低不平。外包装箱表面不应该有突出的锁扣等装置，以避免箱体移位时发生拉挂等现象，影响箱体安全。

2）运输：装运设备的运输工具应清洁、干燥、无污染物。敞车运输时，必须用防雨布盖好，以保证设备不被雨(雪)浸入。设备中转时，应堆放在库房内。短暂露天堆放时，必须用防雨布盖好，产品在装卸时，应采用合适的装卸方式，严防将包装箱(件)损坏，包装箱应注意谨慎堆放，防止产品碰伤。装载时，运输车辆与包装箱之间、包装箱之间应用防震减压的填充物填实，不得留有空隙，防止在运输途中造成货物之间互相碰撞、摩擦，避免发生箱体移位。避免货物在运载工具上的堆码不当，使底层货物承载过重，造成包装破损，甚至商品在运输过程中变形、损坏。在运输过程中避免接触腐蚀性物质。

\*5、验收、交付标准和方法：本项目采购人将严格按照政府采购相关法律法规、《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）以及《政府采购需求管理办法》（财库〔2021〕22号）的要求进行验收。

6、售后服务要求

▲1）为保证服务质量，本项目要求产品制造商提供售后服务。（提供承诺函原件）

2）提供 7×24 小时的电话、网络、现场等方式的技术支持服务。

3）须配备不少于一名维修工程师，提供工程师名单、电话。

4）质保期内出现质量问题，应及时做出响应。在故障问题解决后12小时内，向采购人提出问题处理报告，说明问题种类、问题原因、问题解决中使用的方法等情况。如经过维修3次仍不能达到合同约定的质量标准的，采购人有权要求供应商更换同品牌同型号的全新设备并可正常使用，保留追究供应商的违约责任。

5）货到现场经采购人签收后由于采购人保管不当造成的问题，供应商或产品制造商亦应负责修复，费用由采购人负担。

6）供应商提供的全部设备各种部件均保证齐备、充足供应，若因设备升级更新等原因不能保障供应造成采购人损失的，供应商承担全部赔偿责任，在交货时需向采购人提供设备常规备品备件目录或清单。

7）供应商需指派专人负责与采购人联系或协调售后服务事宜。

\*8) 质保期：验收合格后不低于三年。

\*9）质保范围：提供产品硬件质保、软件升级和规则库更新

## 三、技术、服务要求

**1-1 内网安全准入系统**

1.\*性能参数：网络层吞吐量≥3.5Gbps，准入终端数量≥800个，最大并发连接数≥150000；接口：个千兆电口≥6个，个千兆光口≥2个，电源：单电源，为防止设备关键信息泄露，设备禁止配置显示器等显示设备。

2.支持网关、网桥、旁路、多主模式模式部署；网关模式支持NAT、路由转发、DHCP、GRE、OSPF等功能；多主模式支持两台及两台以上设备同时做主机的部署模式；

3. 支持统一平台设备下发升级包，一次下发，2 台设备连续同时升级成功。升级过程中会进行双机切换来保证业务不中断；

4.▲支持802.1x认证，支持二维码认证（提供截图证明，并加盖供应商公章）

5.多种认证方式，支持触发式WEB认证，支持用户名密码认证、短信认证、微信认证、单点登录认证、USB-KEY认证等多种认证方式；

6.▲设备配置web界面提供分析显示接入用户人数、终端类型、认证方式、带宽质量分析、实时流量排名、泄密风险、违规访问、共享上网等行为风险情况；（需提供产品功能截图证明并加盖供应商公章）

7.支持检测windows重要补丁的安装情况，并反馈检测结果，支持IP管理功能，管理员可以查看每个IP的详细使用情况；

8.对网络接入的终端进行可视化和管理，展示终端详细信息、异常状态等；

9. ▲支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，支持移动终端型号识别；（提供产品界面截图）

10.▲支持拨号行为、双网卡行为、有4G网卡、有无线网卡行为、连接非法wifi行为、使用非法网关行为、连接外网行为、自定义外联行为，8种外联方式的检查（提供截图证明，并加盖供应商公章）；

11.检查到非法外联行为后，支持发送告警邮件、断网的违规处理配置；

12. ▲支持针对用户认证的故障进行分析，给出错误详情以及处置建议；（提供产品界面截图）

13.支持自动删除长期不登录账号信息；（提供产品界面截图）

14. ▲支持自动注销指定时间内无流量的已认证用户；（提供产品界面截图）

15. ▲支持多终端账号绑定，同一个账号能与指定数量的多个终端进行自动绑定；（提供产品界面截图）

**1-2 上网行为管理系统**

1.\*性能参数：网络层吞吐量≥4.8Gbps，带宽性能≥600M，最大并发连接数≥40000，新建连接数≥8000，接口：千兆电口≥4个，千兆光口≥4个，电源：单电源，为防止设备关键信息泄露，设备禁止配置显示器等显示设备。

2.支持网关、网桥、旁路、多主模式模式部署；网关模式支持NAT、路由转发、DHCP、GRE、OSPF等功能；多主模式支持两台及两台以上设备同时做主机的部署模式；

3. ▲支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；（提供产品界面截图）；

4.支持DNS透明代理，能够基于用户、域名、目标DNS，指定代理策略生效，代理策略可以设置为：重定向至DNS服务器、解析为IP、丢弃、重定向至指定线路；

5.支持统一平台设备下发升级包，一次下发，2 台设备连续同时升级成功。升级过程中会进行双机切换来保证业务不中断；

6. 支持管理员账号安全保障机制，可配置管理员账号登录允许尝试次数，并支持管理员用户登录进行双因素认证，密码认证加邮件验证；

7. 支持查看当前设备的线路状态，线路带宽利用率以及当前策略的引流流量分布和实时的引流策略，支持设置线路流控策略;

8. ▲支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况；（提供产品界面截图）

9. ▲支持针对上网权限策略进行检测分析，查看各个应用是否匹配相关策略；（提供产品界面截图）

10. 支持为用户添加自定义属性（职位、临时项目组、邮件组等），能够根据用户属性自动归类并可以针对用户属性配置上网权限策略、流控策略，审计策略等;（提供产品界面截图）

11. 支持发现私接路由（或者共享软件等）共享网络的行为，包括1）.支持自定义配置终端数量和冻结时间; 2）.支持“仅统计电脑”和“统计所有终端”两种模式; 3）.支持可选“冻结IP”还是“冻结用户名”。4）.支持添加信任列表; 5）.支持显示以IP或用户名的维度统计一段时间内的趋势图; 6）.支持例外排除功能：如冻结条件是指定例外条件1台PC，2个终端。当PC或终端数超过例外条件才会被判定为共享; 7）.支持在数据中心报表中可查询通过共享上网的IP、用户，并能导出报表；

12. ▲支持https网页全解密和按网站类别分类进行解密配置；（提供产品界面截图）

13. 支持根据源地址和目的地址过滤外发邮件；包括https网页全解密和按网站类别分类进行解密配置；

14. ▲支持对加密HTTPS、SMTP-SSL、SMTP的邮件进行关键字过滤；（提供产品界面截图）

15. 支持HTTP上传/FTP/邮件附件等形式的外发文件行为，支持基于扩展名识别并拦截外发文件；（提供产品配置界面）

16. ▲支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义;（提供产品界面截图）

17.终端分类可视：对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等，支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；

18.▲设备配置web界面提供分析显示接入用户人数、终端类型、认证方式、带宽质量分析、实时流量排名、泄密风险、违规访问、共享上网等行为风险情况；（需提供产品功能截图证明并加盖供应商公章）

19.支持基于用户组、位置、终端类型、URL类型配置流量管控策略；

20.▲支持终端调用管理员指定脚本/程序以满足个性化检查要求，包含：检测系统更新是否开启、开放端口、已安装程序列表、终端发通知等对不满足检查要求的终端可弹窗提示、禁止上网；（需提供产品功能截图证明并加盖供应商公章）

21.支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题；（提供产品界面截图）

22.▲支持二维码认证，管理员扫描访客的二维码后对其网络访问授权；（需提供产品功能截图证明并加盖供应商公章）

23.针对SSL加密的网站、论坛发帖、web邮箱的内容进行关键字过滤和内容审计；

**1-3 日志审计系统**

1.\*主机审计许可证书≥50个，≥6个千兆电口，内存≥8G，硬盘≥2T，电源：单电源，为防止设备关键信息泄露，设备禁止配置显示器等显示设备。；

2.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等不少于700种日志对象的日志数据采集；

3.支持将检索查询的条件收藏为查询模版，支持查询模版创建、导入导出、删除功能，支持历史搜索记录功能；

4.▲支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射；（需提供截图证明并加盖供应商公章）

5.支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP地址、特征ID、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；

6.支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析；

7.支持对单个/多个日志源批量转发，支持定时转发，可通过syslog和kafka方式转发到第三方平台，并且支持转发原始日志和已解析日志的两种日志；

8.▲支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。（需提供截图证明并加盖供应商公章）