**附件：**

**采购需求**

1、采购需求一览表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品名称 | 说明 | 数量 |
| 1 | VPN联网设备（安全网关） | 硬件设备 | 1台 |
| 2 | 网关管理软件 | 适用于安全网关 | 1套 |
| 3 | 客户端授权软件 | 适用于2-500个客户端使用 | 70个 |

2、主要技术参数要求一览表

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 产品名称 | 技术参数 | 数量 |
| 1 | VPN联网设备（安全网关） | 1、理论加密流量（Mbps）≥100，理论并发用户数≥300，IPSec加密最大流量（Mbps）≥70，设备整机理论最大吞吐量≥150M，设备整机理论最大并发会话数≥35W。内存大小≥2G，SSD硬盘容量≥64G，接口≥4千兆电口；  2、支持IPv6/IPv4协议下的网关模式、单臂模式、主备模式、集群模式、分布式集群模式的部署；  3、支持国产化终端使用，包括中标麒麟、银河麒麟、深度OS等操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；**（需提供功能截图证明或提供至少2家国产系统厂商与VPN产品的兼容性认证报告）**  4、产品支持提供环境检测、自动修复工具，支持对Windows的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力，避免由于用户操作系统环境存在问题影响SSL VPN的使用，减轻运维工作**（需提供功能截图证明）**；  5、产品支持提供HTTPS驱动病毒查杀工具，支持对Windows环境下的针对HTTPS拦截监听的驱动病毒进行扫描查杀，避免因为HTTPS驱动病毒导致无法正常接入和使用SSL VPN；  6、支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统；  7、支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输；  8、设备应支持与全省所有血站机构的互联互通，并接受省血管中心安全策略的统一、可视化管理。 | 1台 |
| 2 | 网关管理软件 | 1、与硬件匹配；  2、网关管理软件需采用B/S管理维护方式，用户只需通过浏览器进入管理系统，通过用户名密码即可进行登陆管理，管理界面需进行可视化处理，无需使用命令行进行管理操作；  3、对VPN基本信息进行查看与设置，包括基本设置、与其他连接点的连接情况、DLAN运行状态、用户管理和连接管理、虚拟IP池管理、隧道间路由设置、与第三方对接情况管理和查看、内网服务设置和VPN端口设置；  4、对VPN设备进行SC设置，包含:SC基本设置和SC服务查看。SC设置用来设置SSL VPN设备加入某公司 SC 集中管理平台，可以实现SSL VPN 设备配置的集中管理；  5、对VPN设备的防火墙进行设置，包括过滤规则设置、NAT设置、访问监控、防DOS攻击、QOS级别设置及上传下载规则设置；  6、对DHCP服务进行设置。 | 1套 |
| 3 | 客户端  授权软件 | 适用于2-500个客户端的虚拟联网使用，本次采购人需求70个客户端的正常联网使用。 | 70个 |