VPN设备询价采购公告

　 我局计划购置一台VPN设备，拟采用网上商城采购方式进行询价采购，邀请符合要求的供应商报名参加。

一、采购项目及内容

项目名称： VPN设备采购项目

内容：见采购需求表。

二、须知

（一）供应商资格要求

1.属于在中华人民共和国注册的法人；

2.具备拟采购产品海南省政府采购网上商城供应商资质；

3.近三年内在经营活动中没有重大违法记录；

4.未被列入“信用中国”网站www.creditchina.gov.cn）失信被执行人名单和没有列入中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单。

（二）报价及相关要求

1.金额应以人民币报价，报价总价不得超过30万元，超过则视为无效。

2．报价产品须为海南省政府采购网上商城所列型号。

3.交货时间：2020年11月30日前。

4.交货地点：海口市

5.付款方式：验收合格后，10个工作日内一次性支付。

（三）材料装订和份数要求

复印件盖单位章，且所有的材料按以下顺序装订成册，一式三份，盖章密封：

1.  单位的营业执照副本复印件；

2.  组织机构代码证复印件；

3. 具备拟采购产品网上商城的供应商资质证明；

4. 近三年内在经营活动中没有重大违法记录（提供承诺函）；

5.未被列入“信用中国”网站（www.creditchina.gov.cn）失信被执行人名单和没有列入中国政府采购网（www.ccgp.gov.cn）政府采购严重违法失信行为记录名单（提供信息查询结果界面截图，加盖供应商公章）；

6.应急响应服务承诺书；

7.报价单；

报价单应加盖供应商法人公章。

（四）报名及获取采购需求文件要求

（1）方式：现场报名并领取采购文件，不收取费用；

（2）报名领取采购文件时，须携带以下资料（均须加盖公章）；

A.营业执照副本、组织机构代码证副本、税务登记证副本等复印件（如三证合一只需提供营业执照副本复印件）；

B.法人代表授权书，法人代表身份证复印件，被授权人身份证复印件；

（五）公告发布媒体：海南省考试局网。

（六）文件获取及响应文件报送时间、地点：

1．报名截止时间：2020年10月15日 17:00。

2. 报名地点：海南省考试局办公楼四楼信息管理处。

3．报名联系人：陈老师；联系电话：65390322。

4. 投标文件递交截止时间：2020年10月19日 17:00。

5. 投标文件递交地点：海南省考试局办公楼二楼207房。

6. 投标文件递交联系人：周老师；联系电话：65851969。

海南省考试局

2020年10月13日

采购需求表（报价单）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 采购项目名称  | 标准配置技术参数  | 数量（台） | 投标货物型号及参数 | 单价 |
| VPN设备设备 | 1、性能参数：最大理论加密流量（Mbps）≥350，最大理论并发用户数≥4000，IPSec加密最大流量（Mbps）≥180，设备整机理论最大吞吐量≥1.2Gbps，设备整机理论最大并发会话数≥130w。 硬件参数：1U，内存大小≥8G，硬盘容量≥64G SSD，单电源，千兆电口≥6个，千兆光口SFP≥2个。2、提供300个SSL VPN接入授权。3、支持IPv6/IPv4协议下的网关模式、单臂模式、双机模式、集群模式的部署 4、支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用。（提供产品功能截图并加盖厂商公章）5、支持断线重连自动技术，防止用户误操作关闭浏览器导致VPN隧道断开；防止用户在无线网络环境下网络正常切换时VPN隧道断开。支持客户端永久在线功能，对于无人值守的设备可以设定永久在线，如果网络断开，可提供无限次重连。（提供产品功能截图并加盖厂商公章）6、支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持Web参数修正，可针对Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题（提供产品功能截图并加盖厂商公章）7、产品应提供环境检测、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。（提供产品功能截图并加盖厂商公章）8、产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象。（提供产品功能截图并加盖厂商公章）9、支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接10、产品应提供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。（提供产品功能截图并加盖厂商公章）11、支持15级以上用户组树形结构分级管理，下级组可继承上级组的角色，资源及认证方式等属性12、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。（提供产品功能截图并加盖厂商公章）13、支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式。（提供产品功能截图并加盖厂商公章）14、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。（提供产品功能截图并加盖厂商公章）15、针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度。（提供产品功能截图并加盖厂商公章）16、产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权。17、支持Syslog（系统日志）服务器，可将管理员日志，系统日志、用户日志输出到syslog服务器中。支持对接多个Syslog服务器，实现日志备份（最多3个），并且支持TCP和UDP传输协议；Syslog服务器支持白名单配置，只允许白名单的IP地址输入日志。18、支持独立日志中心进行SSLVPN实时日志记录，可详细记录用户访问资源记录（用户、主机IP、资源、时间）、管理员日志（管理员、主机IP、时间、管理行为、对象）、系统日志、告警日志；可根据用户名、主机IP等信息进行用户行为查询；可提供用户组/用户流量排行及查询、资源流量排行及查询、资源活跃程度、用户活跃程度等记录；提供暴破登录记录；可提供用户登陆SSLVPN采用非绑定账号访问应用系统的记录。19、支持配置迁移，实现将原有vpn设备配置同步到新设备上，保障老设备配置保存以及新设备快速同步上线。20、提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证明截图并加盖厂商公章）21、设备生产厂商需为国家密码管理局发布的《SSL VPN技术规范》起草单位之一（提供证明截图并加盖厂商公章）22、设备生产厂商需为国家密码管理局发布的《IPSec VPN技术规范》起草单位之一（提供证明截图并加盖厂商公章）23、为保障软件开发质量，要求厂商具有CMMI5级认证。（提供证书复印件）（提供证明截图并加盖厂商公章） | 1 |  |  |

总价： 元；人民币大写：

单位名称：

联系人：

联系电话： 　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　单位盖公章

2020年　月　 日