**2018年VPN设备采购项目报价清单**

2018年6月28日

公司全称：

联系人：

联系方式：

采购项目清单：（参考品牌型号：深信服VPN-1000-B440，配置不得低于以下参数）

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **分类** | **功能** | **详细指标** |
|  | 客户端需求量 | 本次采购要求并发SSL用户数（客户端授权数） | 配置300个安全桌面并发用户使用授权 |
|  | 对接 | 对接校内基于LDAP协议开发的数据中心，实现认证 | 支持LDAP协议，对接校内NETID认证系统进行认证。 |
|  | 性能参数 | SSL最大加密流量（Mbps） | ≥240 |
| 最大并发SSL用户数（个） | ≥**1100** |
| 每秒新用户数 | ≥90 |
| IPSec加密最大流量（Mbps） | 100 |
| IPSec理论并发会话数（Session） | 4000 |
| 设备大小 | 1U |
| 网络接口 | 4个千兆电口  4个千兆光口 |
| 内存 | 2G |
| 系统盘 | 32G SSD |
| 电源（标配） | 单电源 |
|  | 易用性 | 终端系统环境 | 支持终端使用包括Mac OS、Lunix的最新操作系统来登录SSLVPN系统； |
|  | ★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。（提供截图证明并加盖厂家公章） |
|  | 支持32位和64位的Windows 操作系统； |
|  | 部署方式 | 支持网关模式、单臂模式部署两种方式； |
|  | 易用功能 | 同时支持IPSec VPN和SSLVPN两种VPN协议， SSL和IPSec VPN并发授权数量可以由用户自由转化； |
|  | ★可支持虚拟门户功能，把一台设备虚拟成多台设备来访问，可以配置多个域名或者IP地址，配置不同的使用界面，提供给用户完全独立的访问使用体验，虚拟门户不受授权限制； |
|  | 产品支持单点登录功能（SSO）,可以实现B/S,C/S资源的单点登陆。 |
|  | 支持基于用户、用户组分配不同的虚拟IP |
|  | 支持多级用户组分级管理，下级组可继承上级组的角色，资源及认证方式等属性 |
|  | 支持基于用户用户组的流量控制和会话限制、超时时间设置 |
|  | 支持通过域服务器下发控件 |
|  | 支持文件访问代理功能，终端登录用户可以直接在SSL资源页面上以B/S的形式访问服务器上的文件资源，提高协同办公效率。 |
|  | ★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。（提供截图证明并加盖厂家公章） |
|  | 支持用户登录界面、服务界面的完全自定义，上传单独的Web页面作为用户登录界面、服务界面。 |
|  | 安全性 | 终端安全 | 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。 |
|  | 支持本地文件保护；指定终端硬盘中必须存在某文件，并以MD5值来检测文件是否完整，如不完整则禁止登陆。 |
|  | ★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。 |
|  | ★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。 |
|  | 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 |
|  | 服务器安全 | 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。 |
|  | 产品应具有角色授权机制，支持在用户组的基础上，根据角色的不同，组合关联不同的资源权限。 |
|  | ★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，V PN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 |
|  | 支持关键文件保护功能，可针对特定应用关键文件进行锁定，防止用户进行篡改进行越权 |
|  | 用户认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 |
|  | 支持三大运营商移动、联通、电信运营商的标准的外置短信设备或API接口；  支持GSM、CDMA制式短信猫；支持webservice方式短信认证，支持webservice嘉迅版； |
|  | 设备内部必须支持自建CA中心，便于数字证书认证平台搭建；  ★单台VPN设备可扩展同时支持5套以上CA根证书；（提供证明截图） |
|  | 防火墙 | 产品应具备基于状态监测技术的防火墙功能，能够抵抗常见的网络攻击，能够进行包过滤或WAN、LAN、DMZ口之间访问控制；为了避免人为配置错误，产品必须支持对防火墙的过滤规则能够进行在线虚拟测试。 |
|  | 高速性 | 数据传输加速 | 必须支持至少2条及以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能（提供自主知识产权证明） |
|  | 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。（提供自主知识产权证明） |
|  | 支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠IP地址库、不依赖于第三方动态IP寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称Webagent页面），通过Webagent页面自动寻找VPN设备IP(非DDNS）,该方法不必单独注册域名或占用IP地址，大大降低了系统部署难度。（提供自主知识产权证明） |
|  | 仅通过SSLVPN设备可实现资源负载均衡功能，用户接入同一资源根据权值可动态负载到多台承载服务器上；负载均衡可基于服务器性能指标、权值轮询、轮询等不同方式。 |
|  | ★支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度。(提供第三方评测报告及配置界面截图) |
|  | ★支持HTP快速传输协议，大幅优化无线环境（CDMA、GPRS、WIFI、3G）、高丢包、高延等恶劣网络环境下传输速度及效率；支持根据网络境自动选择并切换至最优的传输协议（提供配置界面截图并加盖厂家公章） |
|  | 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。（提供界面配置截图，并提供自主知识产权证明） |
|  | 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；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果（提供界面配置截图，并提供自主知识产权证明） |
|  | 高管理 | 系统管理 | 支持15级以上的管理员分级分权限管理，从Admin派生树形结构下级管理员；上级管理员可分配下级管理员享有设备配置模块权限，可管理的用户、资源、角色权限，并可限制下级管理员是否允许创建下级管理员、创建资源、创建角色；上级管理员可限制下级管理员对权限内配置享有查看或配置权限 |
|  | 支持设置对控制台管理员密码复杂度的要求，提升设备的安全性； |
|  | 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 |
|  | 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。 |
|  | 支持整体网关配置的本地及远程备份、恢复功能；支持SSLVPN配置的单独备份、恢复功能，并支持历史配置的回滚 |
|  | 稳定性、可扩展性 | 系统可扩展功能 | 支持基于自组域简化部署VPN网络的方法，即当有多台设备处于VPN网络中时，通过连接任意节点的VPN设备，即相当于连入整个VPN网络,该方法解决了传统VPN部署是，需要部署多台; （提供自主知识产权证明） |
|  | 支持253台不同型号设备间进行集群（A/A），支持路由模式、单臂模式下多线路部署的集群；支持集群设备间Session同步，一台设备宕机后其上用户无需重新登录SSLVPN可继续使用；可扩展分布式集群功能，无需专门的全局负载设备即可实现异地SSLVPN设备间的接入用户负载分担、速度优选接入，异地设备间互为备份，分布式集群中用户可通过唯一的一个地址访问到所有加入到分布式集群的SSLVPN设备 |
|  | 在负载均衡集群部署模式下，支持授权漂移，即当集群中一台设备宕机，该宕机设备中的并发授权自动迁移到其他正常的设备中，而无需额外购买授权。 |
|  | 产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）代码量不超过20行。 |
|  | ★支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固（提供界面截图证明） |
|  | 移动智能终端支持 | 移动智能终端支持 | 产品必须支持远程应用发布功能，可以无需二次开发，即把Windows应用发布到移动智能终端中，也可以支持无需开发，将C/S资源Web化。 |
|  | 产品必须支持会话复用功能，即当存在多台终端发布服务器且未设置集中存储时时，同一用户的同一会话必须始终发布到同一终端服务器。 |
|  | 远程应用发布必须支持负载均衡策略，即当存在多台终端发布服务器时，可以根据服务器可用会话数、CPU、内存、I/O、综合性能等指标，智能的将用户分配到不同的终端服务器。 |
|  | 产品应该支持企业级“云盘”（又名“网盘”、“文件共享”）功能，即可以通过手机、PC、IPAD的客户端，将数据、文件同步到云端或和分享到终端。  也能够能够支持分享给他人。 |
|  | 远程应用发布数据传输过程中使用SSLVPN协议加密，加密算法支持中国家标准的商用密码算法（简称国密），保证了数据传输的合法性和安全性； |
|  | ★支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置。（必须提供配置界面截图并加盖厂家公章） |
|  | 资质要求 | 设备厂商资质要求 | 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》 |
|  | 提供公安部信息安全产品检测中心颁发的《GA/T 686-2007信息安全技术 虚拟专用网安全技术要求》三级或三级以上检测报告（三级以上为四级、五级） |
|  | 提供产品IPV6 Ready认证证书，（提供证书复印件并加盖厂家公章） |
|  | 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 |
|  | 为保障软件开发质量，要求厂商具有CMMI5级认证。（提供证书复印件并加盖厂家公章） |
|  | 提供在2014年中国国内SSL VPN市场占有率为前三名，（提供权威的第三方机构数据证明并加盖厂家公章） |
|  | 售后服务 | 服务响应 | 要求原厂商在广东区域设有直属办事处等服务机构，以便于为客户提供完善、及时的售后服务。  招标人将参照预中标结果对预中标人的投标产品进行测试，必须完全满足招标方需求方可确定为最终中标人，对于提供虚假参数强行中标的供应商，经测试查实后将以废标处理并录入我单位采购黑名单。 |
|  | 设备软硬件维保和服务 | ★提供5年质保，包括产品硬件质保，软件质保和升级，400电话服务。 |
|  | 原厂授权 |  | ★针对该项目投标产品，需要提供原厂对供应商授权证明并加盖公章。 |
|  | 培训要求 |  | 提供一次为期1天的现场培训. |

注：

1. 报价含税，可普票，要求密封送达，报价文件材料需加盖公章。报价清单一式五份。
2. 报价应包括设计、印制、材料、人工、规费、质保服务、各项税费及合同实施过程中不可预见的所有费用。
3. 中标单位需提供中标型号设备给用户方测试两个月，测试通过后于2018年9月15日后签订正式合同。
4. 截止时间及方式

截止时间：2018年7月4日16:00时前递交投标文件。

送达方式：直接送达，密封袋需注明公司名称、联系人及联系方式。

送达地址：东莞市麻涌镇沿江西一路7号中山大学新华学院行政楼A214。

联系人：王老师，0769-82676032,18122888902。

1. 免费送货上门，上门服务，验收合格后付款。
2. 付款方式：转账或支票，付款前提供正规发票。
3. 报价文件应注明供货期、质保期及售后服务承诺。
4. 需提供授权委托书及身份证复印件。
5. 应提交营业执照三证合一副本复印件。
6. 公司详细介绍（资质、业绩，同类产品案例合同等）、产品详细介绍。

11.如有技术疑问或需要看现场，可联系信网处陈老师：18002798337。