VPN设备技术要求

|  |  |
| --- | --- |
| 项目 | 功能指标要求 |
| 硬件性能 | ★不少于6个千兆电口，SSL VPN加密速度不少于250Mps，SSL VPN最大并发数支持数不少于1200个，SSL VPN每秒新建用户数不少于180个，IPSecVPN加密速度不少于135Mps，IPSecVPN隧道数不少于5200个。★本次招标要求并发用户数授权1000个。 |
| 部署方式 | 支持网关模式、单臂模式、双机模式、集群模式的部署 |
| 基本特性 | 专业VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备。同时支持软件化交付 |
| 支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务； |
| 支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录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；支持Windows、IOS、Android、塞班、黑莓等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入，或通过PPTP、L2TP VPN方式接入； |
| ▲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。 |
| 产品应支持的密码算法包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1 |
| 在windows系统上，能同时安装并运行多个VPN客户端，满足有多套VPN的客户同时登录VPN |
| 易用性 | ▲可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果； |
| ▲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。 |
| ▲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） |
| 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问 |
| 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  |
| ▲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。 |
| 权限、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，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  |
| 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 |
| 针对服务器地址保护方面，可支持SSLVPN资源列表界面上的用户授权资源隐藏；针对B/S应用，可进行URL地址伪装，防止服务器真实IP地址泄露  |
| 身份认证 | 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  |
| 支持有驱USB KEY、无驱USB KEY认证，无驱KEY无需在客户端安装驱动，方便用户；支持配置第三方KEY，可与其他业务系统无缝结合；支持满足中国国家标准的《智能IC卡及智能密码钥匙密码应用接口规范》的智能TF/SD卡。 |
| ★支持结合口袋助理等移动APP，实现动态口令认证，增加认证的多样性。 |
| 支持随机验证码短信认证，可自定义所发送短信信息格式，支持用户端短信重发功能；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；支持与基于PKI体系的第三方CA进行结合认证 ，可根据CA某字段将通过CA认证的用户自动映射到指定用户组，方便进行权限授权配置；支持CRL证书撤销列表。 |
| 高速性 | ▲必须支持至少4条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 |
| 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） |
| 高管理要求 | 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  |
| ▲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。 |
| 远程应用 | 产品必须在Windows和MAC操作系统下支持远程应用发布功能（提供界面截图证明） |
| 登录客户端兼容全平台(windows、mac、linux主流系统)，并保持各平台易用性、用户使用习惯的一致性 |
| 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。 |
| 手机客户端必须经过苹果公司官方检测，并发布在苹果官方应用商店appstore，产品客户端必须通过google公司官方检测并发布在google应用商店PlayGoogle；产品客户端必须支持非“越狱”或非“Root”权限的手机/PAD安装。 |
| 远程应用发布必须支持本地资源，包括：本地磁盘资源映射、本地打印机、本地串行口、本地智能卡，本地输入法；支持剪切板，并能够实现剪贴板数据流双向控制，即可以分别控制是否允许用户将“客户端复制数据到远程应用”或将“远程应用数据复制到客户端” |

|  |  |
| --- | --- |
| 产品及企业资质 | 提供原厂商售后服务体系ISO9001认证证书 |
| 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》 |
| 提供产品IPV6 Ready认证证书，并在全球IPV6测试中心官网可查 |
| 产品售后服务 | 提供1年的硬件质保和软件升级售后维保服务。 |