|  |  |
| --- | --- |
|  | **VPN设备技术及服务要求** |
| 用户数要求 | 本次招标的SSL VPN产品必须为知名产品，单台支持1000并发用户数以上，设备在不更换硬件条件下单台可以扩展到支持5000并发用户数。 |
| 性能要求 | 最大支持4000个并发SSL会话。 |
| SSL VPN网络吞吐量≥400M/秒。 |
| 每秒钟可以新建的用户数目>= 5000个/秒。 |
| 硬件要求 | 具有专业SSL硬件加速卡。 |
| 端口至少4个10/100/1000Base-TX。 |
| 提供冗余电源。 |
| 安全要求 | 系统必须为专用的硬件系统，通过专有操作系统进行所有功能实现，可以抵御针对系统本身的攻击，为了防止 SSL VPN产品在应用时由于产品自身的安全漏洞给生产应用带来巨大的损失和不方便。要求此次投标的SSL VPN产品必须具有极高的安全性，要求在产品本身具有防火墙访问控制功能；同时要求此次投标的SSL VPN产品不能具有任何已知安全漏洞，同时也不能有在近一年中某些产品版本存在重要安全漏洞，通过补丁或升级等方式解决的情况。 |
| 支持国际ICSA3.0认证 |
| 系统冗余要求 | 系统支持HA功能，并具有多台VPN设备间的负载均衡功能，具有多种均衡算法，支持的主/备模式和主/主模式。 |
| 功能要求 | 必须提供Windows系列的纯SSL通道的接入。支持密码保存、自动拨号等功能。必须提供linux 平台用户纯SSL通道的接入。必须提供Mac平台用户纯SSL通道的接入。 |
| 提供苹果IPAD、Iphone平台以及Android平台的纯SSLVPN通道的建立。IPAD、Iphone SSL VPN客户端软件必须支持在苹果公司APP store直接下载。支持移动设备硬件特征码的校验及用户绑定。可以通过增加许可的方式满足自建APP Store。支持手机安全浏览器功能。 |
| 投标的SSL VPN产品必须具有虚拟站点技术，既一台SSL VPN产品能够逻辑上当作多台SSL VPN产品应用和管理。为了在同一台SSL VPN设备上同时支持多种业务及应用（如同时支持OA应用、生产系统应用、远程维护）；要求单台设备最大支持256个虚拟站点，可通过不同的虚拟站点实现多种应用，每个虚拟站点可独立实现面向应用的全部SSL VPN功能。支持不同虚拟站点下内网主机属于相同IP地址段。并且可以基于站点对并发用户进行控制。 |
| 虚拟站点下提供对多种常用的认证服务器的支持，如RADIUS、LDAP、Active Directory认证，包括RSA SecurID®和X.509客户端数字证书, USB key登陆和身份验证等，同时也可在设备上建立本地用户数据库，本地数据库最大支持200，000个用户录入，用作身份认证。支持用户帐号和机器MAC地址、硬盘ID号进行绑定认证。同时支持多个AAA认证的同时使用，并且具有可选择性。 |
| 能够实现针对用户以及管理员的role-base的权限管理，能够实现不同用户访问通过不同角色的权限控制来访问相应角色下的资源，若一个用户包含多个角色，需要实现资源的叠加。能够实现不同管理员管理通过不同角色的权限控制来独立管理相应的虚拟站点。 |
| VPN的接入主机无需安装相应的客户端软件，利用系统已有的标准的WEB浏览器，同时系统必须对接入的主机提供跨平台的支持，如支持Windows、Linux、MacOS等； |
| 系统支持多种的网络应用程序，如基于WEB的B/S结构，C/S结构，以及文件共享(包括CIFS,NFS,DFS)及所有TCP、UDP、NetBOIS应用。且所有实现均必须仅通过SSL协议实现（而非通过除SSL协议以外的其它协议，如IPSec协议组）进行实现。特别是对3层VPN支持方面也必须基于SSL协议进行实现，而不能基于其它协议（例如ppp协议或IPSec协议）； |
| 系统必须全面解决由于WEB缓存所带来的安全隐患，例如清除缓存记录、超时检测等。具有客户端的安全检查机制，如可以检查客户端的个人防火墙、防病毒系统，检查客户端的文件、进程、注册表、操作系统及其版本等信息，并且可以根据检测的结果赋予不同的访问权限。支持安全桌面（虚拟桌面），支持安全桌面（虚拟桌面）资源互通； |
| 提供详细的用户访问信息日志：包括日期、时间、源IP地址尝试登陆、用户名、登陆成功后访问操作等等，从而能够通过分析日志将用户所有访问应用过程进行重现； |
| 要求提供Web资源映射，不用更换内部应用系统或暴露内部域名； |
| SSL 加密算法要求：密钥算法：AES (128-bit)，AES(256-bit)，DES (56-bit)，3DES (168-bit)，RC4 (128-bit)公钥算法：RSA (1024-bit)，RSA (2048-bit)消息认证：MD5 (128-bit)，SHA-1 (160-bit) |
| 要求支持SSL VPN与后台服务器之间明文或SSL加密； |
| SSL VPN访问权限应可授予单个用户、用户群或角色，将单个用户、用户群和角色的访问限制在具体的资源范围内； |
| 可以根据来源地址、来源端口，目的地址、目的端口，时间等进行数据包的过滤规则。可配置1000条访问控制列表； |
| 可进行内容检查，对远程进入流量进行深入的检查，扫描Web流量中不适当的内容，或者太长的数据包，当发现恶意的内容，阻止用户的访问； |
| 要求提供隧道分割(Split Tunneling)能力，只允许流向LAN的流量通过VPN连接器进行传输，与Internet的连接不会中断； |
| 管理员可以调整用户登陆VPN系统的标识与详细界面的外观，系统标识与外观界面可导入到VPN系统中直接进行替换实现，不需要借助第三方Web服务器； |
| L3VPN功能实现时，必须能够支持IPSec协议应用通信，既在基于SSL协议的L3VPN功能实现后，IPSec协议可以通过已建立的SSL L3VPN进行正常通信； |
| 提供Telent filter和ftp filter功能； |
| SSL VPN设备支持隧道模式，支持对客户端IP地址的动态分配、静态分配（特定用户分配特定IP）、DHCP分配IP等多种方式； |
| 支持单点登陆功能(SSO)； |
| 可选支持或禁止多用户使用相同用户名/口令认证登陆SSLVPN； |
| L3VPN功能模块要求通过微软WHQL认证体系，满足微软质量体系要求，能够和微软操作系统进行密切配合； |
| Portal支持多语言，包括中文简体，繁体，英文。 |
| 支持在HTTP的Header中传递客户端证书到服务器； |
| Inferface支持Mnet和Vlan功能； |
| 设备生产商必须具有高新技术企业证书须提供原厂商针对本项目的服务授权承诺函正本，且厂商服务规范须通过ISO 9001国际质量认证体系认证。提供全国400热线电话技术支持。 |
| 管理配置 | SSL VPN产品具有多种配置、管理界面方式，支持图形化配置、命令行配置。 |
| 售后支持 | 提供产品厂商在上海本地有产品技术支持工程师。 |
| 投标产品提供原厂项目授权书并提交两年原厂售后支持服务承诺函，提供包括7\*24\*4小时的电话、邮件及远程服务支持，提供下一工作日的备机到现场的服务（包含人工上门）。 |