VPN网络平台设备采购项目采购需求表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **采购内容** | **参考品牌及型号** | **数量** | **技术参数及性能（配置）要求** |
| 1 | VPN安全网关系统 | 安达通  SJW74C-BH | 2台 | ★1、标准机架式设备，网络接口≥6个千兆电口；  ★2、VPN加密吞吐率(ESP/3DES+SHA) ≥300Mbps；VPN并发隧道数≥10000；防火墙吞吐率≥1.2Gbps；最大并发会话数≥100万；提供1000个并发用户许可授权；  ★3、VPN的设计完全遵守IPSec和IKE标准；可和第三方IPSEC厂商VPN对连；支持传输和隧道模式；  4、支持各种标准协议，包括IPv4, IPv6, VLAN标记，路由，NAT/NAPT，组播，OSPF, IGMP, Diff Serv，IPSec, IKE，VLAN Trunk，PPTP穿透，GRE，H.323，HTTP, SSL 3.0, TSL1.0, FTP, POP3, SMTP等多种应用层协议；  5、支持AES、DES、3DES、MD5、RC4、RSA 及SSP02，SSF33,SCB2等国密算法，支持扩展安全算法模块；  6、支持自有数字证书服务器和第三方CA，全面兼容标准X.509标准；  7、支持网到网的Intranet VPN，支持单机接入的Remote Access VPN，支持与合作伙伴和客户连接的Extra VPN；  8、支持VLAN Trunk，并能够在VLAN环境下构建VPN连接；  9、VPN内支持NAT 穿透（NAT-T）功能，并能够实现VPN互连的“双向NAT穿透”；  ★10、支持在网桥模式（透明模式）下VPN通信；  11、支持厂商专有地址服务器和DDNS两种方式的全动态IP组网；  12、提供基于角色权限的VPN内部控制；  13、定时检测和发起VPN通信，确保设备间加密通道的时时连通；  14、支持任意广播/组播包跨VPN复制 ；  15、支持在IP地址冲突情况下的VPN互连，而不需要IP地址冲突的一方大量更改局域网内PC的IP地址；  16、安全网关当作一台主机，单口接入网络，无需修改用户物理网络拓扑，支持动态IP和分支机构接入总部时无需修改总部内网路由器的路由；  ★17、采用“IPSec over Https/Http”技术替代传统的SSL技术，适应各种网络环境，可变换SSL访问端口,只允许80端口访问或者只运行443端口访问；  18、支持Html/Dhtml, Jsp, Asp,Java applet, Activx, Cookies及其其他所有WEB技术的访问；  19、支持TCP/IP等所有C/S应用服务；  20、移动用户终端无缓存和Cookie，避免了在公共环境（如：网吧）使用VPN，遗留的痕迹带来的安全隐患；  21、基于“角色”管理用户权限；  22、移动用户终端会自动检测隧道断开的情况，并和中心节点重建VPN隧道；  ★23、移动用户支持数字证书认证方式，并兼容第三方CA系统；  24、移动用户终端登陆有PIN码保护，该密码可以由移动用户自主修改；  25、访问资源信息每次VPN接入时自动下载，保证访问资源的灵活性和易管理性；  26、支持USB KEY，手机短信认证和动态口令卡认证，并可外挂Windows AD和LDAP；  27、支持USB KEY和用户的硬盘、CPU和网卡等计算机信息绑定，且该功能的开启是在VPN网关上集中进行控制；  28、通过网关控制该功能，启动后客户端用户PC将只能访问VPN资源而不能访问互联网的任何其他资源；  ★29、设备必须能够与采购单位原有VPN产品相互备份使用；  ★30、同时支持IPSec VPN和SSLVPN两种VPN协议；用户可以自行选择采用IPSec或SSL方式移动接入；设备必须支持单位原有的硬件USBkey接入，供应商负责开发或调试。 |
| 2 | 防火墙系统 | 天融信防火墙系统V3  NGFW4000-UF | 2台 | ★1、1U机箱，X86架构，千兆电口≥6个, 1个扩展槽；默认含IPSEC VPN模块，可扩展SSL VPN模块，支持AI应用识别、入侵防御和防病毒功能；防火墙吞吐率≥5.5Gbps,IPSec VPN吞吐率≥40Mbps，SSL VPN吞吐率≥100Mbps；并发连接≥220万，每秒新建连接≥4万；  ★2、产品由专用的硬件平台、安全操作系统及功能软件构成，采用自主知识产权的专用安全操作系统，采用多核多平台并行处理特性。  3、支持路由、交换、混合、虚拟线工作模式；支持静态路由及动态路由协议，支持802.1q、QinQ模式；  4、支持基于源/目的地址、源/目的端口、用户、应用的策略路由，保证关键业务流量通过优质链路转发；  ★5、产品的安全操作系统采用冗余设计，配置多操作系统引导，出于安全性考虑，多系统需在设备启动过程中进行选择，不得在WEB维护界面中设置系统切换选项；  ★6、为提高链路可靠性，产品应支持手工链路聚合及LACP链路聚合，提供不少于8种的负载分担算法，灵活实现对聚合组内业务流量的负载分担；  7、产品应支持Internet Protocol Version 6(即下一代互联网协议IPv6),支持IPv4/IPv6双栈工作模式；支持IPv6安全控制策略设置，能针对IPv6的目的/源地址、目的/源服务端口、区域、服务、时间、扩展头属性等条件进行安全访问规则的设置；  ★8、产品应支持在一台物理设备上划分出最大128个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源；  9、产品应支持基于http、ftp、telnet、smtp、pop3等协议的内容过滤策略，可对微博、贴吧上传的内容及附件进行过滤，可对FTP上传/下载的文件名进行过滤，同时支持过滤FTP信令：上传文件、下载文件、删除文件、重命名文件、创建目录、删除目录、列出目录等，邮件过滤支持对发件人、收件人、主题、内容、附件等进行过滤；  ★10、产品应支持配置文件、系统服务等系统功能虚拟化，支持路由、链路聚合等网络功能虚拟化，支持安全策略、NAT策略、流量管理、用户管理、IPV6功能、URL过滤、病毒过滤、内容过滤、审计、报表等安全功能虚拟化；  11、产品应支持异常行为检测，内置统计智能学习算法，对特定地址对象建立监控策略，基于新建、并发、流量等数据与上一周期记录值进行比较判定是否异常，如果存在异常则报警；  12、产品应支持对单条访问控制策略进行最大并发连接数限制；产品应支持监控功能，显示最近被拦截的IP、地址对象及应用的节点信息；  13、产品应支持攻击检测引擎，采用协议分析、模式识别、统计阈值和流量异常监视等综合技术手段来判断入侵行为；支持web攻击识别和防护，如跨站脚本攻击、SQL注入攻击；支持超过4100+攻击特征库,产品生产厂商应具备强大的漏洞和功放研究能力，能够确保每周至少更新1次攻击特征库；  14、内置病毒检测引擎，支持HTTP/SMTP/POP3/FTP/IM等协议的病毒防御，对每种协议数据流的检测方向可选双向、上传、下载；  15、支持病毒白名单，用户可以根据实际业务需求将特定威胁进行排除；  16、产品应支持日志本地存储，可对不同类型日志设置存储空间；同时支持外发至SYSLOG服务器，可将多条日志合并成一条日志传送到日志服务器中，可选择对日志传输是否加密，设定8位的加密密钥；  ★17、产品应支持提供智能策略分析功能，支持策略命中分析、策略冗余分析、策略冲突检查，并且可在WEB界面显示检测结果；  18、产品应支持根据服务器对通过设备的数据报文流量进行统计，包括各个服务器的服务器 IP、上行流量、下行流量、总流量以及新建会话数；支持根据按照病毒防御、入侵防御、ADS攻击进行威胁统计，可按照威胁类型/攻击者/受害者三种方式进行威胁排名；  19、内置强大应用识别引擎，综合运用端口识别、行为识别、特征识别、关联识别等技术手段，准确识别传统应用如P2P、web应用、移动应用、云应用、加密应用等；  20、支持多个系统升级包并存，系统升级包文件数量不少于5个；  ★21、中标后签订合同时提供原厂针对本项目的授权及售后服务承诺书。 |
| 3 | VPN客户端 | USB KEY | 500套 | 1、安达通的VPN安全客户端软件（包括安全密钥）。  ★2、USB KEY，USB接口的密码运算和安全存储设备，与安达通“安全客户端”和SureCA配套使用；  3、能与安达通VPN安全网关配套使用。 |