|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **技术要求** | **数量** | **单价** | **小计** |
| 1 | 多核防火墙 | 1. ★吞吐量≥10G,最大并发会话数≥20万,每秒新建连接数≥2万； 2. 最大IPSEC VPN隧道数≥512条,SSL VPN最大支持128个并发用户； 3. #要求提供9×GE，所有端口必须能够自定义局域网口和广域网口，USB接口≥1个,用于外接移动硬盘存储日志，系统升级； 4. 采用非X86多核架构，处理器为多核心以上并行处理CPU； 5. 要求具备自主研发的多核并行安全操作系统。 6. #支持将任意接口数据完全镜像到设备自身的其余接口，用于抓包分析。（要求提供产品界面截图）； 7. 支持透明、路由、混合、旁路四种工作模式；支持出站就近负载均衡技术，可动态探测链路响应速度并选择最优链路进行转发（要求提供产品界面截图）； 8. 基于多出口的DNS透明代理； 9. 支持SmartDNS，ISP动态探测； 10. #支持链路ping、应用端口等方式探测服务器状态（要求提供产品界面截图）。 11. 支持DNS透明代理；支持DNS代理黑白名单功能，用户可通过该功能过滤域名查询请求，保护DNS服务； 12. 支持支持GRE和GRE over IPSec、IPSEC VPN、SSL VPN、L2TP VPN，智能终端支持Android版APP，支持苹果和安卓系统的Xauth VPN； 13. 支持NAT full cone模式,求必须支持NAT的端口扩展技术, 要求必须支持多对多的NAT，且公网地址池可选择逐一使用和同时使用两种模式； 14. 支持免费 ARP广播，ARP客户端认证（基于PKI技术）防止ARP攻击和ARP病毒；支持常见的静态路由； 15. 支持OSPF、OSPFv3、BGP、BGP+、RIPv1/v2、RIPng（动态路由协议非透传）支持策略路由、支持ISP路由并内置多运营商路由表； 16. 支持BFD for Static/OSPF/BGP。 17. 支持基于会话的原路回包功能，可设置优先于路由策略而通过会话表中的入接口进行回包。必须支持基于角色、用户、用户组的策略路由。 18. 支持基于非固定端口的应用决定下一跳的策略路由（应用引流）；支持VRouter功能，同时系统支持2个VRouter（多VR）； 19. #支持ISP服务商路由（提供预定义和自定义的）；支持AP模式，AA模式，且透明模式下可支持AP模式 透明、路由模式下支持将多条链路带宽进行捆绑； 20. 支持虚拟线技术(Virtual wire)和Vlan标签转换技术；可抵御DNS Query Flood、Synflood、udpflood、icmpflood、ping of death、smurf、winnuke、等攻击，会话控制，基于安全区段和Profile的安全防护；支持H.323、SIP、FTP、TFTP、RSH、RTSP、SQL Net、HTTP、MS-RPC、PPTP/GRE、SUN-RPC等应用。 21. 可按照应用、时间、用户帐号、IP地址、服务端口、物理端口等方式对数据进行访问控制；支持会话控制功能，要求能够基于源、目的、应用协议三种条件做会话数限制； 22. 支持会话控制功能，要求能够限制会话新建速率；支持对防火墙策略命中次数的统计功能； 23. 支持Radius认证、LDAP认证和MS AD认证，并支持LDAP和AD用户的批量自动导入；支持双因素认证(用户名/口令＋USB-Key),支持客户端硬件特征码绑定认证,支持登陆SSLVPN后自动打开可客户化定制的网页； 24. 支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括指定文件、指定进程、系统补丁、浏览器版本、杀毒软件等方面。（要求提供产品界面截图） 25. 支持多种认证方式；支持基于角色的访问控制； 26. 支持短信口令认证功能；多出口链路下支持选择最快响应链路建立SSL连接；支持在Android移动终端上通过APP远程接入； 27. 支持本地用户修改密码功能；严格遵循RFC国际标准，支持DES、3DES、AES128、AES192、AES128、AES256，SHA-256、SHA-512等算法，支持NAT穿越；可于主流VPN设备互通； 28. 支持对VPN隧道中的应用进行控制；支持速连VPN部署技术，中心端自动下发配置到分支设备而无需手工配置； 29. 基于策略的VPN和基于路由的VPN； 30. 具有自主知识产权的检测引擎，具备基于协议异常、会话状态和七层应用行为等的攻击识别功能；内置IPS特征库，特征规则数量超过3000条；支持对HTTP、SMTP、POP3、FTP、Telnet、VLAN、MPLS、ARP、TCP、UDP、RPC、GRE等多种协议的分析。 31. 在保障合法应用正常运转的前提下，提供对网络病毒、蠕虫、间谍软件、木马后门、刺探扫描、暴力破2解等恶意流量的检测和阻断； 32. 有效抵御SQL注入、XSS注入，外链检查、CC防护等；内置病毒（AV）特征库，病毒库可以在线更新、本地更新； 33. 支持路由、透明、混合等各种工作模式下的网络病毒检测，支持无IP地址的透明桥下的网络病毒检测模式，支持VPN 模式下的病毒扫描；可对HTTP、FTP、SMTP、POP3、IMAP等协议的应用进行文件的病毒扫描和过滤； 34. 可按照应用分类进行流量监控并提供实时的图形化监控报表；必须支持基于安全域、用户、ip地址以及7层应用进行保证带宽，最大带宽的控制，支持针对7层应用的优先级转发控制。多层QoS功能要求包含应用QoS 和IP QoS 是两个独立的数据流控制功能，应用QoS下可以嵌套IP Qos策略；IP QoS可以嵌套应用QoS必须支持弹性带宽功能，可自定义阀值来上弹或回收带宽，充分利用网络带宽资源； 35. 内置应用特征库，要求可升级。应用程序特征库不少于1300种，智能终端应用不少于200种。（提供应用程序数量证明的界面截图）；支持2000万以上分类web页面库，且支持自定义URL分类过滤；支持包含关键字的邮件标题、邮件正文进行过滤，可审计用户、关键字、邮件发件人、收件人、发件时间等信息；支持根据邮件附件的文件类型进行过滤，可审计用户、关键字、邮件发件人、收件人、发件时间等信息；支持对QQ的上下线进行审计，可审计QQ账号；支持包含关键字的论坛发帖或者微博内容进行过滤，可审计用户、关键字、论坛发帖或发微博时间；可设置白名单，白名单内的用户免于过滤和审计。 36. 可实现与外置第三方认证计费系统对接，至少支持深澜和城市热点对接成功；支持http和https两种方式web管理，console、telnet、SSH管理，支持针对电信的TR069管理口；支持10个配置文件并存，并支持配置回滚（要求提供产品界面截图）；IPv6邻居发现协议、IPv6 SNMP管理、?IPv6路由配置、IPv6 DNS配置、IPv6策略配置、IPv6 ALG配置、IPv6 6to4隧道配置、IPv6 4to6隧道配置、NAT-PT配置、NAT64和DNS64配置； 37. ★要求提供产品的合法来源渠道证明、及原厂商针对本项目的三年服务承诺函。 38.★为保证实验实训设备的兼容性及有效的后续教学支撑，要求同一品牌。 （#井号项技术指标需提供产品彩页和功能截图，盖设备生产企业公章或投标专用章，否则视为未响应招标文件要求） | 5台 | 33000 | 165000 |
| 2 | 串口控制服务器 | 1U机架式 ★RJ45串行通信口≥16个  Console口≥1个 ★10/100M以太网口，并且支持MDI,MDI-X自适应功能≥2个 设备支持Console（串口/TELNET），Web，SNMP方式配置。 支持串口独立配置：不同的串行接口可以被配置成不同的模式，如将端口1设为SOKET模式，端口2设为COM模式，端口3设为PPP模式等。 ★支持实串口模式：支持WindowsNT/2000/XP下可最多管理1024个串口。在这种模式下，每个串口均支持多达6台PC机控制，1人操作其它人可观看同步操作。 支持PPP模式：各串口都可支持PPP。每个串口可以作为PPP服务端或PPP客户端使用。 支持Real Com/TTY驱动，完全兼容原有应用软件 具有TCP Server、TCP Client和UDP等通用透明传输模式 附带Windows平台下的管理软件，提供强大管理功能，可批量搜索实训室中的所有串口调试控制器，进行批量配置  可通过网页浏览器或Telnet终端进行配置管理 单个串口配置可应用到所有串口上，无需逐一设置，数据端口号自动累加 每个串口带有15KV ESD浪涌保护 串口通信速率最高可达460.8Kbps 可配置登录用户和密码 ★可配置基于IP或Mac地址的访问限制 ★要求和其它网络设备同一品牌。 ★可和同一品牌的管理中心联动，实现所有设备的集中管理，批量配置。 | 5台 | 7000 | 35000 |
| 总计： | | | |  | 200000 |