# **竞争性谈判内容及服务要求**

|  |  |  |
| --- | --- | --- |
| 序号 | 设备名称 | 技术参数 |
| 1 | 防火墙系统 | 硬件要求：1U机箱，单电源，默认配置≥6个千兆电口，≥8个SFP插槽 软件要求：默认含IPSEC VPN模块，采用专用操作系统并支持多核特性； 性能要求：防火墙吞吐≥4G，并发连接≥150万，每秒新建连接≥2万，IPSec吞吐≥80M，SSL VPN吞吐≥220M 功能要求： 1、支持静态路由、PBR与多播路由，支持RIPv1/2、OSPF、BGP等多种动态路由协议；并支持ECMP、WCMP等路由均衡方式，能够根据预设探测条件实现动态的链路切换。 2、支持链路聚合，支持至少10种以上的聚合负载算法。 3、至少内置6个ISP服务商路由，提高多链路接入时的出站访问效率。 4、支持入站智能DNS功能，并至少具有10种以上服务器负载均衡算法。 5、能够基于访问控制策略进行最大并发连接数限制，支持策略冲突检查功能。 6、支持网络应用自学习并且能够根据自学习结果生成相关安全策略，   1. ★具有防止共享上网功能；   8、★支持加密流量识别，如HTTPS流量、BT加密流量、迅雷加密流量、网络视频加密流量等等；  9、★支持采用基于访问控制策略的一体化带宽管理模式，能够针对用户、用户组、IP、MAC、时间、应用等进行带宽管理，并且支持共享策略、独享策略、访问控制独享策略等多种带宽策略类型；  10★为保证设备生产来源正规，所投产品需销售许可证证明。 |
| 2 | 上网行为管理系统 | 硬件要求：  1U, ≥6个千兆电口，支持1对bypass, ≥2个千兆光口,单电源, 日志存储空间≥1TB硬盘。包含3年系统软件及特征库升级许可。  ★系统CF卡≥4G，设备本身的操作系统单独存放在CF中，要与日志存储分开。  性能要求:  适配带宽：≥100M，用户数≥600人。  功能要求:   1. 支持路由模式，旁路模式、网桥模式、混合模式部署；切换部署模式无需重启，不影响设备正常使用。 2. 支持即插即用功能。不管电脑的IP如何配置，开启即插即用功能后，只要插上网线，即可上网。 3. ★支持与同品牌的安全检测与响应系统联动，实现安装了安全检测与响应系统的终端才能入网，没有安装的不允许入网。 4. 支持基于应用层服务和SAAS的策略路由，可基于IP、国家列表、ISP自动地址表和域名来控制目的地址；支持ISP自动地址表（电信、移动、网通、铁通等）的策略路由的选路方式； 5. 支持DNS链路健康检查算法；支持ICMP链路健康检查算法；支持TCP链路健康检查算法；支持自定义的链路健康检查算法； 6. 支持https网站识别，支持加密网站搜索，支持ssl论坛加密发帖内容识别，支持基于关键字的控制。 7. 支持基于授权签名的方式实现https审计免除告警的行为。 8. 支持url白名单，添加到白名单的url不受策略控制和审计。 9. ★支持将多个以太网物理端口捆绑成一条逻辑端口（即将多个端口捆绑成一个逻辑的端口以增加带宽，同时增加链路备份）支持基于轮循、主备、哈希、广播、802.3ad、发送自适应、双向自适应等多种负载方式。   10、具有良好的网络适应性并满足《网络安全法》、公安部151号令、等保2.0关于用户行为审计和日志留存的要求。  11、为保证设备生产来源正规，所投产品需销售许可证证明； |
| 3 | 安全检测与响应系统 | 集成病毒查杀、漏洞修复、系统加固、网络防御、终端管控、资产管理、风险态势展示等功能；采用领先的虚拟沙盒技术对威胁行为深度分析，结合勒索诱捕、虚拟补丁、微隔离等主动防御技术，有效解决勒索、挖矿、免杀逃逸等威胁，多维度防御病毒传播和横向感染，全面提升用户的终端安全管理能力。 配置要求：  35个Windows PC客户端防病毒功能授权,含3年升级许可。防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS病毒等进行查杀，提供主动防御系统防护等功能。客户端系统默认支持Windows XP/VISTA/WIN7/WIN8/WIN10。  默认包含3年病毒库升级服务  软件功能要求：   1. 系统部署采用C/S架构，管理采用B/S架构，管理员只需通过浏览器登录控制中心，即可对系统进行管理。 2. 客户端至少支持WindowsXP、Windows 7、Windows 8、Windows 10等32位/64位终端操作系统，支持Windows server 2003、Windows server2008、Windows server 2012、Windows server 2016、Windows server 2019等32位/64位服务器操作系统。 3. 支持中标麒麟、银河麒麟、中科方德、深度、UOS等国产操作系统。 4. ★客户端安装后至多占用50M硬盘资源，日常内存占用不到20M，有效节省PC/Server资源（要求截图证明）。 5. 支持定制安全防护策略：包括病毒防御（病毒查杀、文件实时监控、恶意行为监控、U盘保护、下载保护、邮件监控）；系统防御（浏览器保护、软件安装拦截、系统加固）；网络防御（黑客入侵拦截、IP协议控制、恶意网站拦截、IP黑名单）；文档安全（文档检测、文档跟踪、USB存储）；系统监控（设备监控、进程监控、软件监控、服务监控、账号监控、外联监控）；其他设置（心跳配置、管理员配置、升级配置、白名单、补丁配置、弹窗配置） 6. ★支持远程控制，通过管理中心实现对客户端的远程运维。。 7. ★对系统关键位置进行防护，阻止无文本攻击、流氓、广告程序对系统的恶意篡改等行为。从系统文件保护、病毒免疫、进程保护、注册表保护、危险动作拦截、执行防护等多个维度对系统进行防护。 8. ★支持对移动存储设备采用标签式注册管理，可以区分内外部介质使用，定义禁用、启用只读、启用（只读\_运行）和启用读写、启用（读写\_运行）五种操作，按照文件类型审计在移动存储介质上文件操作记录，并可设置例外USB设备. 9. ★能与同品牌的防火墙、上网行为管理系统设备联动；   10、★为保证设备生产来源正规，所投产品需销售许可证证明； |
| 4 | 网络路由系统 | 1、★采用无阻塞交换架构、支持多核CPU，要求提供官网货截图证明  2、整机最大支持2个扩展插槽，内置电源，所有业务板卡支持直接热插拔，不需要配置命令  3、★转发性能≥9MppsMpps，交换容量≥20Gbps、提供官网截图和产品彩页证明；  4、固化接口≥8\*GE电，≥1\*GE光 ≥3\*GE Combo口（支持LAN可切换为WAN口），1\*USB接口  5、支持DHCP server/client/relay，PPPoE server/client，NAT，子接口管理等  6、支持IEEE 802.1P，IEEE 802.1Q，IEEE 802.3 ，VLAN管理，VLAN聚合，MAC管理，STP/RSTP/ MSTP，SEP等  7、支持静态路由，策略路由，动态路由协议：RIP、OSPF、BGP、IS-IS、RIPng，OSPFv3，IS-ISv6，BGP4+  8、支持IPsec VPN，GRE VPN，DSVPN，A2A VPN，L2TP VPN，L2TPv3 VPN, VxLAN  9、支持ACLv4/v6，基于域的状态防火墙，802.1x认证，MAC认证，Portal认证，AAA，RADIUS，HWTACACS，PKI，广播风暴抑制，ARP安全，ICMP防攻击，URPF，CPCAR，黑名单，攻击源追踪，国密算法，上网行为管理，IPS，URL过滤  10、提供入网证明 |
| 5 | 网络安全监管系统 | 硬件要求：  1、1U,≥6个千兆电口,单电源,应用层吞吐≥200Mbps、网络层吞吐≥2.5G、并发连接≥50W。含3年产品特征库升级许可  2、含SQL注入、XSS、CSRF等WEB攻击防护功能、URL访问控制功能、防盗链功能、WEB漏洞扫描功能、DDoS攻击防护功能、网页防篡改功能、服务器负载均衡功能、报表分析及告警功能。  功能要求：  3、采用专用硬件架构与安全操作系统，基于操作系统内核的完全检测技术；产品为专业性 Web 应用安全防护系统硬件设备，而非下一代防火墙\UTM 类设备集成的 WEB 防护功能模块。  4、硬件模块化设计 硬件采用模块化设计，可以通过扩展卡来增减业务接口，而非软件WAF。  5、★支持虚拟线接入，无论任何网络环境可强制数据从一个接口转发到另一个接口  6、支持链路聚合(Channel)部署，提高链路带宽。支持静态路由，策略路由，ISP路由配置。  7、支持网络层访问控制，支持基于源IP 地址、目的IP 地址、源端口、目的端口、协议类型及目的区域等条8、支持应用层访问控制功能，针对 HTTP请求字段进行过滤，包括HTTP协议版本，请求方法，Cookie信息等。  9、具备WebShell攻击，文件包含漏洞利用、目录遍历等攻击的防护功能支持对网站登录页面提供暴力破解防护功能。具备盗链防护功能，防止服务器资源被滥用。支持Cookie安全防护，通过对cookie进行加密签名，保障cookie信息安全可信。  10、 ★支持恶意扫描防护：通过人机识别方式，进行恶意扫描智能检测；支持扫描防护阈值设置和扫描IP的阻断周期设置。  11、★支持多种爬虫攻击防护：包括但不限于内置爬虫对象库，自定义爬虫对象，导入或者下载后端服务器robots.txt 等方式提供爬虫攻击防护。  12、 ★网关型网页防篡改，无需在服务器中安装任何插件，即可对网站文件内容进行篡改防护，当检测到篡改后可以实时恢复篡改内容。  13、★为保证设备生产来源正规，所投产品需销售许可证证明。 |
| 6 | 安全保障管理服务 | 1、上报服务：安全设备系统更新情况查询上报服务；更新服务：安全设备补丁升级更新服务；  2、远程实验室技术支持服务：为了尽快发现故障原因、及时解决问题，技术人员可在得到用户授权的情况下，通过远程连接进入用户系统查找故障、分析解决问题。并通过网站、邮件、视频会议等远程支持方式获得远程免费技术支持。  3、硬件故障上门维修服务：当出现需要更换安全防护产品硬件模块的技术故障时，提供备品备件，完成硬件设备的返修过程，并完成硬件模块的更换。  4、重大保障支持：在用户单位重要时刻（例如重大会议、重大事件等）或客户重大系统投产、重大网络割接的情况下，免费安排工程师到现场进行技术保障的服务。并提供必要的技术协助主要包括：现场网络运行监控、协助监控网络设备的运行状况、实时故障处理、协助进行现场故障诊断及紧急恢复。  5、安全通告服务：及时提供符合客户实际的安全信息，包括最新的安全事件和相应的处理意见 ；及时告知客户最新的安全事件（0day系统漏洞、网络攻击）的解决办法。  6、调优服务：质保期内，提供产品软件升级服务、调优、故障排除和故障排除所需的备件更换（含备件本身）等。  7、巡检服务：在保修期内至少每季度提供一次巡检服务。巡检服务内容包括：系统运行环境检查；系统硬件运行情况检查；系统ERROR　LOG分析；系统运行性能、状态检查和安全策略优化等。  8、培训服务：至少提供2名系统运维人员的现场技术培训服务。 |