第四章　采购需求

2.采购产品技术规格、要求和数量（包括附件、图纸等）

序号	商品名称	规格	数量及单位
1	●▲实训室台式机	CPU: Core i7 及以上 主板：≥Intel 及以上 内存： ≥8GB DDR4 2666MHz 内存 显卡：2G 独立显卡 声卡：集成 硬盘：≥1T SATA3 7200rpm 硬盘+120G 固态硬盘 网卡：集成 10/100/1000M 以太网卡；出厂可选内置无线网卡及蓝牙 扩展槽：≥2 个 M.2 接口，≥1 个 PCIex16，≥1 个 PCIex1，≥1 个 PCI 光驱：无光驱 键盘、鼠标：抗菌键盘，抗菌鼠标 接口：≥4 个 USB 3.1 端口，≥4 个 USB2.0 端口,1 个支持 CTIA 耳麦的通用音频插孔，1 个 VGA，1 个 HDMI；1 个串口， 电源：≤180 高效节能电源 安全性：具有 BIOS 保护芯片，可以自动恢复被恶意篡改的 BIOS，保证设备连续使用，可设置屏蔽 USB 接口和 SATA 接口，中文 BIOS 方便使用。 机箱：标准立式机箱，内置扬声器，体积≤17L，免工具开启机箱面板，静音设计，整机噪音低于 11 分贝； 显示器：21.5 英寸 LED 背光液晶显示器 服务：三年全保及上门，原厂 400/800 售后电话，第二工作日上门服务。 Windows10 专业版正版系统，每机独立序列号 标配耳机：	100 台

		设计：过耳式或头戴式； 扬声器直径(Diameter)：50mm； 电缆长度(cable length)：≥2m； 灵敏度(Sensitivity)：≥119DB/mW； 阻抗(Impedance)：≥32Ω； 频率范围(Frequency)：20-20.000HZ。 ★投标时提供耳机产品外包装参数照片或打印官方网站参数网页彩色截图并加盖供应商公章。	
2	网络防火墙	1、硬件规格及性能要求：标准 2U 设备，双电源；配置不少于 6 个 10/100M/1000M 自适应千兆电接口，不少于 4 个千兆 SFP 接口（不含光模块），不少于 4 个万兆 SFP+接口（不含光模块），不少于 5 个接口扩展槽。标配不少于 60G SSD 硬盘；配置入侵防御、网络防病毒、上网行为及 URL 分类管理三年特征库升级授权；提供 3 年硬件维保，最大吞吐量不小于 40Gbps，最大并发连接数不小于 1000 万，每秒新建连接数不小于 120 万。 2、虚拟化：支持基于硬件 Hypervisor 技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的 CPU、内存、接口等资源。提供虚拟防火墙 Hypervisor 层资源配置管理界面截图。每个虚拟防火墙均提供完整的安全功能，包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6 双栈等。提供一种专利级虚拟安全设备的部署配置方法及系统，需提供专利证明复印件。 3、访问控制： （1）支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略； （2）支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响。提供相关界面截图； （3）支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至 Syslog 服务器。 4、应用层防护： （1）支持并开通网络入侵检测及防御功能，入侵防御事件库事件数量不少于 4000 条，支持基于接口/安全域、地址、	1 台

		用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图； （2）★支持并开通对 HTTP、FTP、SMTP、POP3、IMAP 协议的病毒检测和过滤功能；支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于 1000 万，提供一种专利级结合病毒检测与入侵检测的方法及系统，需提供证明复印件； （3）★支持扩展 APT 检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和 ODAY 攻击的有效防护，要求提供一种专利级 APT 智能检测分析平台中的白数据过滤方法及系统，需提供证明复印件。 5、应用控制：支持并开通基于 DPI 和 DFI 技术的应用特征识别及行为控制，应用识别的种类不少于 1000 种；支持并开通 WEB 控制功能模块，包括 URL 访问分类管理、网页关键字过滤、http 文件下载类型管理等功能，URL 分类库规模不少于 2000 万条，支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套的流控界面截图；支持基于应用、用户、源地址、目标地址、服务、时间的通道匹配。 6、★威胁情报防护：支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护。提供防火墙配置界面及威胁情报云端界面截图。 7、网络参数：支持透明、路由、混合、旁路等部署模式；支持基于入接口、源地址、目标地址、服务端口、应用类型、域名的策略路由；支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT；支持并开通 SSL VPN、IPSec VPN 和 L2TP VPN，支持并开通链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法，支持链路负载均衡的目的会话保持功能；提供相关界面截图，支持 DNS 透明代理功能，可将指定范围内的 DNS 请求自动重定向至管理员指定的 DNS 服务器，且支持多台 DNS 服务器的负载均衡。★提供相关界面截图。 8、高可用性：支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能；支持 HA 设备之间的配置自动同步，确保用户只需在一台设备进行业务配置。 9、系统管理：支持基于 WEB 和命令行的设备管理模式，WEB 界面和命令行模式下均可实现对设备所有功能的管理配置；支持 SYSLOG 和 SNMP v3，SYSLOG 日志支持同时发给多个日	

		志服务器，支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的 TOP10 统计展示、基于具体威胁事件/威胁类型的 TOP10 统计展示等，统计展示的时间周期包括 1 小时/1 天/7 天/30 天。★提供相关界面截图。 10、集中管理：支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。支持扩展集中策略分析模块，通过集中策略分析模块，实现：集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置；集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息；集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的；集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的，★提供上述功能截图。 ★11、资质要求：（1）厂商资质：产品原厂商具备充分的网络安全研究能力，连续两年（2017 年~2018 年）每年的 CVE 漏洞发现数超过 300 个，请给出漏洞发现列表（CVE 编号，证明连接）。 产品生产厂商具备中国信息安全测评中心颁发的信息安全服务资质证书（安全工程类三级）。 产品生产厂商具备《通信网络安全服务能力评定证书（应急响应服务一级）》。 通信网络安全服务能力评定证书（安全设计与集成二级）。 厂商必须为微软 MAPP 计划成员。 （2）产品资质： 产品具有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》； 产品具有中国国家信息安全测评认证中心颁发的《信息技术产品安全测评证书-EAL4+》证书。	