**安全和应用性能测试平台详细参数指标**

| **产品名称** | **基本参数描述** | **预算金额 （万元）** | **备注** |
| --- | --- | --- | --- |
| **安全和应用性能测试平台** | **\*（1）整机支持不少于8个可用的1G/10G物理接口，单接口支持1G/10G两种网络带宽速率；**  **（2）测试平台应能够支持多个同种类型接口的捆绑使用，能够将多个接口的测试能力汇聚到1个或者多个接口上；**  **（3）应能够模拟数据通信网络环境中的各类设备，至少包括终端设备、网元设备和应用服务器；**  **\*（4）支持不少于30000种恶意代码样本和僵尸网络样本库，且该样本库应能够做到实时或者定期的更新；**  **（5）支持常见的僵尸网络仿真功能，包括但不限于：TDL4，Duqu，ZeroAccess，Evil，PushDO，TDW，Zeus等；** | **190** |  |
| **安全和应用性能测试平台** | **（6）支持用户自定义病毒或者恶意代码样本的导入功能；支持在HTTP、HTTPS、SMTP、POP3、FTP协议或加密连接等应用场景中嵌入恶意软件和病毒样本；**  **\*（7）支持仿真不少于7000种的网络攻击方法，且能够做到实时或者定期的更新；**  **（8）支持常见的攻击行为和场景，包括模拟口令破解等解码攻击行为、模拟恶意代码和后门程序的攻击行为、模拟操作系统漏洞渗透攻击行为、模拟缓冲区溢出类攻击行为、模拟蠕虫攻击行为、模拟数据库攻击（如SQL注入等）行为等；支持Shellcode攻击和0-day攻击；支持常用的2-4层DDoS攻击和应用层DDoS攻击；支持常见的2-7层攻击逃避技术，用例不少于180种；支持针对IPv6的攻击；**  **（9）支持针对SCADA／ICS等工控网络环境的攻击行为，种类不少于70种；**  **（10）攻击用例库支持基于攻击威胁等级CVSS评分体系进行威胁等级区分；**  **（11）具备多点测试能力，能够支持至少4个测试点同时开展测试工作。**  **（12）在单一物理端口上同时支持不少于30种非回放应用协议的流量仿真发送和多种攻击流量、病毒流量的混合发送；** |  |
| **安全和应用性能测试平台** | **（13）支持正常应用和DDoS攻击流量、应用攻击流量、恶意流量的混合发送；**  **（14）应用层背景流量仿真支持添加30种以上的明文可编辑非回放应用协议，且可灵活调整协议种类和带宽配比；**  **（15）能够提供不少于10Gbps（双向）的L7层实际网络流量发送能力；**  **（16）能够提供不少于10Gbps（双向）L2/3层实际网络流量发送能力；**  **\*（17）支持RFC2544等常用的标准化性能测试方法，且提供集成测试环境；**  **\*（18）支持不少于5000万并发连接能力；**  **\*（19）支持不小于200万/秒新建连接能力；**  **（20）支持不少于300种应用层协议全状态仿真（非回放、明文可编辑）能力；**  **（21）网络攻击方法用例模板应不少于5000个；**  **（22）病毒样本和恶意代码样本库应不少于20000个；**  **（23）逃逸攻击方法用例模板应不少于150个；**  **\*（24）支持2年以上升级和维护服务。** |