上海港湾学校虚拟化防病毒系统

技术要求

上海港湾学校于2014年搭建了桌面虚拟化和服务器虚拟化，目前学校近百教师具有虚拟桌面在进行移动办公和教学，学校业务系统服务器全部在服务器虚拟化池里面，桌面虚拟化和服务器虚拟化给学校信息化的发展带来非常重要的意义，学校业务系统的稳定运行乃重中之重，因此虚拟化平台的安全防护非常重要。

上海港湾学校2016年5月曾遭受大面积的网络及系统攻击，造成了一段时间内的网络瘫痪和部分业务系统崩溃。后经查实的主要原因是：僵尸病毒通过网络植入到学校内部系统，由于学校现有系统均已采用虚拟化系统，但尚未部署针对虚拟化系统的防病毒防护软件。僵尸病毒植入学校宿主机后向外猛烈的发送无意义报文造成学校出口拥塞，学校正常对外系统均无法访问网络，内网传输也造成了一定的拥堵。急需部署防病毒系统。

需要定制虚拟化防病毒系统软件，详细技术要求如下：

* 支持Vmware ESXi 5.0以上
* 支持Citrix Xenserver 6.2、Xenserver 6.5
* 支持Microsoft Hyper-V 2008R2、2012和2012 R2
* 虚拟机防御机制与扫描服务器以联动方式工作以降低虚拟机性能开销
* 客户端以轻代理方式部署在虚拟机操作系统层面
* 支持实时与按需恶意软件扫描防护功能
* 支持自动隔离机制(虚拟机失去保护，自动限制虚拟机访问控制)
* 支持主机桌面防火墙
* 支持基于主机的入侵防御
* 阻止恶意网站及钓鱼网站访问
* 支持网页访问控制
* 支持外设控制
* 多扫描服务器支持自动轮询工作机制保证性能负载均衡
* 扫描服务器支持HA模式
* 支持扫描服务器主备自动切换机制
* 支持扫描服务器压缩文件嵌套数量设定
* 提供虚拟桌面防病毒许可150点，具有引擎防病毒、钓鱼网站拦截、DNS智能解析保护、主动拦截防御技术、主机防火墙，动态网络隔离，下载扫描保护等功能，虚拟化环境感知
* 提供虚拟服务器防病毒许可100点，支持Citrix XenServer、Vmware ESXi、Microsoft Hyper-V，KVM和深信服HCI等虚拟化环境，提供集中扫描和共享缓存特性，避免扫描风暴