**安全产品清单详细参数**

|  |  |  |
| --- | --- | --- |
|  | WEB防火墙 | ★1、标准1U机架式设备，配置4个千兆电口 ，整机吞吐量≥400Mbps，最大并发会话数≥25万，每秒新建会话数≥5万；  2、 支持包过滤，网络地址转换，状态检测，应用流量识别，应用层安全防护，用户控制，深度内容检测，支持IPSec VPN，支持统一安全运维管理；  3、为保障网络中应用的高效运行，应具备应用层流量的引流，支持针对应用的策略路由（提供基于应用的策略路由的配置页面截图证明）；  ★4、为保证整体网络安全，所投设备必须支持威胁的分析发现与防护并重，因此必须具备威胁发现功能：威胁情报预警与处置、业务系统实时漏洞分析功能，具备威胁防御功能：敏感信息泄漏防护、服务器保护、恶意链接防护(需提供以上威胁发现、威胁防护所有功能界面截图，并可提供实际测试）；  5、为保证能有效防护大规模攻击，所投设备必须具备web应用防护、入侵防御、僵尸网络的联动封锁功能，可智能生成临时规则封锁攻击源IP，临时封锁时间可自定义（需提供入侵防护、web应用防护、僵尸网络设置联动封锁配置功能截图证明、设置IP冻结时间，设置时间自动刷新封锁IP列表的截图证明，并可提供实际测试）；  6、为保证网络安全，必须具备PHP,JSP,ASPX等主流脚本语言编写的webshell后门脚本上传检测功能；  ★7、为保证网络安全，必须支持对重要业务系统提供重要URL或者其他应用服务的短信认证机制（提供至少包括web、rdp、pptp、nntp、rlogin等四种以上服务进行短信认证加强登录防护的配置截图证明，并可提供实际测试）；  ★8、为保证网络安全，应支持WEB行为进行过滤，提供Web攻击防护、Web远控木马防护等功能，web应用防护能力通过开源web应用安全项目组（OWASP）评测认证，并且在OWASP的25项评测要求中，获得满分（五星）评测项在19项（含）以上（提供OWASP认证证书以及对应的web攻击防护能力测评报告）；  9、为实现对业务系统的安全分析，支持Web漏洞扫描功能，可分析web网站各类漏洞，包括SQL盲注，LDAP注入，存储型跨站脚本，操作系统命令，文件包含等脚本漏洞（需提供以上五类详细的漏洞扫描截图证明）；  10、为保证网络流量安全纯净，必须支持对PC终端、服务器是否变成了僵尸肉鸡进行检测，识别特征总数在50万条以上（需提供木马远控、恶意链接、移动安全、异常流量的僵尸网络检测功能截图证明、僵尸网络识别库超过50万条的界面截图，并可提供实际测试）；  11、支持异常连接检测，对21，22，25，53，69，80/8080，110，143，443等常见端口的协议异常流量检测，并支持RDP和SSH端口反弹链接检测；  12、当前互联网威胁变化迅速，为保证网络安全能及时防护最新威胁，设备需具备终端请求恶意链接检测拦截功能，提供接入云端安全联动功能；  13、支持对内网主机外发的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为，支持外网对内网主动发起的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为；  ★14、为实现安全可视化，应支持对各类威胁行为进行深度分析，输出网络总存在的威胁问题，并对各类威胁行为输出有效攻击次数和攻击趋势；（提供具备有效攻击、攻击趋势的威胁报告证明，并可提供实际测试）  15、产品应具备计算机信息系统安全专用产品销售许可证；  16、产品经过国际知名实验室NSS Labs测试，并获得recommended推荐级别（提供NSS Labs相关测试报告）；  ★17、产品必须为防火墙市场的成熟产品，防火墙产品进入IDC多功能防火墙市场排名前三（提供2014年第三方IDC市场占有率报告）；  ★18、所投品牌厂商是第二代防火墙标准（GA／T 1177-2014）起草单位之一（提供相关证明复印件）； |
|  | 上网行为管理 | 1. 标准1U机架设备,标配4个千兆电口，整机吞吐量≥200 Mbps，并发会话数≥150000，支持用户规模≥400人 2. ★支持网桥、路由、旁路等设备部署模式；支持多机部署模式，两台以上设备同时以主机模式运行，完美支持组织的VRRP环境，起到设备冗余与负载均衡的作用；支持双机部署模式，两台设备以双机模式运行。两台设备通过串口线相连，一主一备，当主设备发生故障时自动切换到备用设备，提高网络的稳定可靠性。（提供以上3种设备部署模式以及多机、双机部署模式配置界面截图） 3. 支持多种认证方式，提供短信认证：以手机号码为用户名，登录密码以短信方式发送、与微信结合认证：用户关注微信公众号后即通过身份认证，后台记录用户ID，二维码认证：管理员扫描访客的二维码后对其网络访问进行授权。（提供短信、微信认证、二维码认证功能截图） 4. 设备内置全面大量的应用识别规则库，支持超过4600条应用规则数，支持超过2100种以上的应用，650种以上移动应用，保证应用识别的准确率（提供产品应用识别库总应用数量及移动应用数量界面截图） 5. 支持审计用户使用邮件客户端外发SSL加密邮件的邮件内容，支持审计用户通过SSL加密Webmail网站外发邮件的内容（提供设备支持加密邮件内容识别的界面截图） 6. ★设备可统计访问互联网应用的情况，对互联网应用进行自定义标签化管理，可自行配置：高带宽消耗、不良应用、色情暴力、邪教宗教等；能对每一种应用进行解释，帮助管理员快速定位应用的分类并关联到日常互联网访问管理策略（提供产品自定义标签，如定制以上4种标签的策略配置界面截图） 7. ★设备能对终端发生的危险行为(木马控制、端口扫描、异常邮件外发、代理工具)进行统计和报表输出（提供以上4种风险行为智能分析报表界面截图） 8. ★支持在默认桌面上虚拟出一个新的桌面，在虚拟桌面中上网，在推出安全桌面后，一切还原到干净的默认桌面，防止PC和内网中毒；支持通过设置安全桌面和默认桌面网络访问权限，实现互联网和内网的内外网隔离；支持通过设置安全桌面访问默认桌面目录文件访问权限，防止被动泄密（提供设置安全桌面访问默认桌面的网络和目录文件访问及文件导出权限的配置功能截图） 9. ★设备能适应无线网络建设，内置无线控制器模块功能，对接入点AP配置工作模式、射频参数、负载均衡（提供产品上述配置项目功能界面截图） 10. ★设备必须支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型，同时支持例外排除功能：如冻结条件是指定例外条件1台PC，2个终端。当PC或终端数超过例外条件才会被判定为共享。（提供共享接入检测和移动终端管理配置功能截图及例外条件配置截图） 11. 为防止P2P流量造成网络堵塞，需支持通过抑制P2P的上行流量，来抑制P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题（提供抑制P2P下行丢包的配置界面截图） 12. 为更合理利用带宽资源，需支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义（提供线路空闲阀值设置、线路繁忙保护阀值设置截图） 13. ★为及时了解用户访问网络速度缓慢的原因，需支持对内网用户的web访问质量进行检测， 对整体网络提供清晰的整体网络质量评级,支持以列表形式展示访问质量差的用户名单,支持对单用户进行定向web访问质量监测（提供质量检测功能截图） 14. 支持对加密HTTPS、SMTP-SSL、SMTP-TLS、SMTP、客户端的邮件进行关键字过滤，防止主动泄密风险。（提供实际测试效果图） 15. 支持对加密HTTPS、POP3-SSL 、POP3、IMAP 、IMAP-TLS 、IMAP-SSL、SMTP-SSL、SMTP-TLS、SMTP、Gmail、闪电客户端邮件内容的记录，提供主动泄密风险行为依据。（提供实际测试效果图） 16. ★根据管理者自定义的风险行为特征自动挖掘并输出泄密风险、安全风险、法律风险智能报表（提供泄密风险、安全风险、法律风险报表截图） 17. ★具备管理员能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等（提供上述所有流量实时状态的截图） 18. 产品具备公安部颁发的《销售许可证（网络通讯安全审计）》（提供网络通讯安全审计类的销售许可证） 19. 产品具备中国信息安全测评中心颁发的《信息技术产品安全测评证书EAL3级》（提供安全测评证书） 20. ★产品应具有中国信息安全产品认证中心颁发的《中国国家信息安全产品认证证书》（提供证书复印件） |