入侵防御系统一套

保修期：原厂保修3年

注：★为废标项，#为重要指标项

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **重要性** | **指标项** | **指标要求** |
|  | # | 硬件规格 | 1U独立IPS机架式设备，全内置封闭式结构，具有完全自主知识产权的专用安全操作系统，含交流双电源模块， 1个RJ45串口，2个GE管理口，≥4个10/100/1000M电口（2路Bypass），≥1T SATA硬盘 |
|  | **★** | 性能指标 | 网络层吞吐≥12G，应用层吞吐≥3Gbps |
|  |  | 入侵检测能力 | 系统需提供入侵规则分类，帮助更便捷的制定检测策略。如勒索、挖矿、SQL注入、XSS注入、webshell、命令代码执行、内存破坏、类型混淆、反序列化、信息泄露、目录遍历、文件操作漏洞、注入攻击、重定向漏洞、CSRF、僵木蠕、拒绝服务、弱口令、欺骗劫持、扫描类攻击等。 |
|  |  | 系统应提供入侵行为特征的自定义接口，可根据用户需求定制相应的检测规则。支持以下自定义：名称、级别、协议类型、协议类型、包长度、正则表达式定义关键字。至少支持IP\TCP\UDP\ICMP\HTTP\POP3\SMTP\MSN\QQTCP\\QQUDP\FTP协议的规则自定义 |
|  | # | 支持基于SCADA、IEC 61850、IEC 60870-104等工控协议的相关漏洞攻击检测。 |
|  | # | 入侵规则管理能力 | 系统攻击特征库数量至少为9000种以上。 |
|  |  | 入侵检测规则须支持按CVE、CNNVD、CWE关联、查询和筛选，  |
|  |  | 系统须提供规则升级更新内容，如更新规则列表、修改规则的规则ID、名称、缺省动作，以帮助客户了解更新规则的内容 |
|  |  | 数据泄露检测 | 系统应提供敏感数据泄露检测功能，能够识别超过阈值的敏感数据信息（身份证号、银行卡、手机号等）。 |
|  |  | 系统应提供关键文件泄露检测功能，能够识别通过网络传输的关键文件，并记录文件的文件名和MD5值，以检测非法外传行为。 |
|  | # | 黑白名单功能 | 系统需提供厂商专业积累的黑IP库，允许客户选择加载。 |
|  |  | 系统具有手动添加白名单IP、域名的能力，对白名单中的条目不进行安全检测 |
|  | # | 系统需提供厂商专业积累的预置白名单库，可在流量较大时启用白名单，提高系统实际检测性能。 |
|  |  | 应用识别 | 系统应能识别主流的应用程序，识别不少于6000个应用。支持至少5G应用，支持PFCP、NAS、HTTP2、SIGTRAN、S1AP、MML等协议；至少20种工控协议，如IEC 60870 104、DNP3、CIP、Modbus、LonWorks 等协议，。 |
|  |  | 防病毒 | 支持流式防病毒，且病毒库在10万以上。 |
|  | # | 具有防病毒能力，支持HTTP、FTP、SMTP、POP3、IMAP、NFS、SMB2、工控（IEC-61850、IEC 60870）等协议。 |
|  |  | 用户认证 | 系统应具备用户身份识别能力，支持基于用户身份进行策略配置、日志记录与查询；支持自动与手动获取用户信息列表并生成组织结构图。 |
|  | # | 威胁/系统状态监控 | 系统需提供系统资源的告警规则设置，可CPU利用率、内存利用率、CF卡利用率、硬盘利用率等阈值。并能推送到消息中心。 |
|  |  | 可通过各种统计分析呈现当前整体威胁状态：如日志类别整体占比、IPS攻击手段分布、事件发生趋势、危险程度分布、事件发生次数排名、被阻断事件发生次数排名、源/目的 地址按事件发生次数排名等 |