**海南师范大学网络安全加固产品参数**

|  |  |  |
| --- | --- | --- |
| **序号** | **资产名称** | **主要参数要求** |
| 1 | 互联网（边界）出口防火墙 | **硬件规格**1 、性能指标：网络层吞吐量≥80G，应用层吞吐量≥50G，并发连接≥1200万，每秒新建连接数≥90万。2、机箱与电源：标准2U机箱，冗余电源（双电源）。3、存储与内存：内存≥32G，≥256G固态+2T机械硬盘。4、接口配置：≥4个千兆电口，≥4个千兆光口，≥4个万兆光口（含相应光模块），≥4个40G光口（含4个40G光模块），≥2个扩展插槽，1个Console口，1个HA接口，1个MGT接口，2个USB接口。5、服务支持：6年硬件维保服务，6年病毒防护特征库升级服务。**功能参数** 1. 接口与链路聚合：支持通将多个物理口绑定为逻辑接口，实现接口级冗余。3. 高可靠性（HA）：支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式。4. 访问控制：支持基于源地址、目的地址、服务、应用、时间等多种方式进行访问控制。5. 病毒防护：支持对HTTP、FTP、POP3、SMTP、IMAP等协议进行病毒查杀（本地病毒库规模≥1200万）；含防病毒功能模块。6. 入侵防护：支持入侵防护功能模块，可检测远程扫描、暴力破解、缓存区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等攻击。7. 协议与网络支持：支持IPv4/v6双栈； |
| 2 | 数据库审计 | **硬件规格**1、存储与内存：内存≥32G，≥4TB SATA硬盘（默认支持RAID1）。2、 接口配置：≥1个RJ45串口，≥1个GE管理口，≥4个GE电口，≥4个千兆SFP接口插槽，≥2个接口扩展槽，2个USB接口。3、机箱与电源：标准2U机箱，冗余电源（双电源）。4、性能指标：网络层吞吐量≥5000Mbit/秒，SQL语句处理能力≥40000条/秒。5、 服务支持：6年原厂硬件维保服务，6年软件更新授权，6年病毒防护相关特征库升级服务。**功能参数**1、 数据库审计范围：支持对主流数据库进行审计，包括Oracle、SQL Server、MySQL、DB2、DM、PostgreSQL、Kingbase、Informix、Oscar、Sybase、Hbase、MongoDB、Spark、HDFS。2、数据资产发现与管理：支持数据资产的自动发现（包括基于网络流量发现数据库表和资源账号，如表名、数据库名、账号在线天数等）；支持用户数据库中敏感信息自动发现，定位敏感数据存储位置并形成审计规则。3、审计模式与内容：支持数据库访问行为与返回结果集的双向审计，支持全量审计与满足审计规则的审计模式。4、安全审计规则：可对SQL注入、CVE高危漏洞利用、缓冲区溢出等攻击行为进行审计。5、环境与部署支持：支持在IPv4、IPv6环境中部署，支持两种协议及混合流量的数据库审计；支持镜像旁路部署。 |
| 3 | 智慧教育云平台防火墙 | **硬件规格**1、存储与内存：内存≥16G，固态硬盘存储≥256G，机械硬盘≥4T。2、机箱与电源：标准2U设备，双电源。3接口配置：≥1个RJ45串口，≥2个RJ45管理口，≥6个千兆电口，≥4个千兆SFP接口，≥4个万兆光口（含相应光模块），≥2个接口扩展槽，2个USB接口。4、性能指标：整机吞吐量≥40G，应用层吞吐量≥28G。5、服务支持：6年原厂硬件维保服务，6年软件升级服务，6年特征库升级服务（含病毒防护、入侵防御等特征库）。 **功能参数**1.、功能模块：含防火墙模块、入侵防御模块、防病毒模块等。2、病毒防护：支持对FTP、HTTP、SMTP、POP3、IMAP等协议进行病毒检测与阻断（包括邮件正文/附件、网页及下载文件中的病毒）；病毒特征库规模≥1200万；支持恶意文件防护功能。3、入侵防护：支持远程扫描、暴力破解、缓冲区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等攻击的检测和防护。4、访问控制：支持针对源地址、域名、网段进行黑名单和白名单配置。5、协议与网络支持：支持IPv4/v6双栈。6、策略管理：提供策略分析功能7、联动与响应：支持与态势感知平台联动，由态势感知平台统一调用并下发安全策略进行响应封堵。 |
| 4 | 5G专网防火墙 | **硬件规格**1、存储与内存：内存≥16G，固态硬盘存储≥256G，机械硬盘≥4T。2、机箱与电源：标准2U设备，双电源。3、接口配置：≥1个RJ45串口，≥2个RJ45管理口，≥8个千兆电口，≥4个千兆SFP接口，≥4个万兆光口（含相应光模块），≥2个接口扩展槽，2个USB接口。4、性能指标：整机吞吐量≥40G，应用层吞吐量≥28G，最大并发连接数≥450万，新建连接数≥35万。5、服务支持：6年原厂硬件维保服务，6年软件升级服务，6年特征库升级服务（含病毒防护、入侵防御等特征库）。 **功能参数** 1、功能模块：含防火墙模块、入侵防御模块、防病毒模块等。2、病毒防护：支持对FTP、HTTP、SMTP、POP3、IMAP、等协议进行病毒检测与阻断（包括邮件正文/附件、网页及下载文件中的病毒）；病毒特征库规模≥1200万；支持恶意文件防护功能。3、入侵防护：支持远程扫描、暴力破解、缓冲区溢出、蠕虫病毒、木马后门、SQL注入、跨站脚本等攻击的检测和防护。4、访问控制：支持针对源地址、域名、网段、进行黑名单、白名单配置。5、协议与网络支持：支持IPv4/v6双栈。7、联动与响应：支持与态势感知平台联动，由态势感知平台统一调用并下发安全策略进行响应封堵。 |
| 5 | 堡垒机 | **硬件配置**：1、内存≥8G， 硬盘≥4T2、机箱与电源：标准2U设备，双电源。3、接口配置：≥6个千兆电口，≥2USB接口，≥1串口，≥1\*GE管理口，1个扩展插槽4、维保服务：原厂维保六年**功能参数**1、资产授权：提供200个资产授权2、用户权限管理：具有用户角色权限自定义功能，可对用户进行细粒度权限划分，可细分用户管理、用户角色管理、资产管理、密码管理、策略管理、审计管理，支持不同角色相互组合。3、协议与运维支持：支持RDP、VNC、SSH、TELNET、SFTP、FTP、协议的HTML5运维，无需本地运维客户端，支持通过H5文件运维的方式上传和下载文件4、授权管理：支持基于组织机构和账户的静态授权，通过不同授权模型满足运维管控要求。5、操作审计：支持HTTP、HTTPS操作审计，审计内容包括用户名、用户IP地址、目标设备IP、设备名称、协议/应用类型、操作内容等;支持操作内容录像回放。6、SQL审计：支持SQL语句级别审计，审计内容包括时间、用户、类型、用户IP、设备IP、数据库账号和SQL关键字等信息;可通过SQL语句审计结果定位数据库运维操作录像回放 |
| 6 | 漏洞扫描 | **硬件配置**：1、内存≥8G，硬盘≥4T，2、机箱与电源：标准2U设备，双电源。3、接口配置：≥4个千兆电口，≥4个千兆光口（或千兆SFP接口），≥1个扩展槽位，≥2个USB口，≥1个串口**功能参数**1、IP/域名支持：主机扫描支持无限个IP地址或域名， Web扫描支持≥320个子域名或IP.2、并发能力：- 最大并发主机数60、最大并发任务数10。3、接口与联动：提供数据接口模块，支持API接口与第三方产品联动。4、扫描模块：提供Web应用扫描模块，支持对Web应用的漏洞、挂马检测和分析包含主机漏洞扫描模块。5、漏洞扫描范围：持扫描国产操作系统、应用及软件的安全漏洞，支持扫描大数据组件框架的漏洞。6、漏洞验证与报告：支持对扫描出的漏洞提供取证性质的验证并输出报告，直观展示漏洞利用过程和危害性;支持漏洞验证扫描，包括系统漏洞验证、Web漏洞验证.7、风险展示：支持通过仪表盘直观展示主机风险等级分布、资产风险趋势、资产风险分布趋势等内容，并可查看详情.8、维保与升级：原厂维保六年、提供六年漏洞库升级授权。 |
| 7 | 威胁检测探针 | **硬件配置**：1、内存≥32G，机械硬盘≥4T。2、机箱与电源：标准2U设备，双电源3、接口配置：≥4个千兆电口，≥2个万兆接口（含2个万兆多模模块），≥2个USB口，≥1个串口（或管理口）。**功能参数**1、吞吐与基础功能：支持20G吞吐（应用层），包含流量采集、元数据提取、存储等功能。2、检测模块与升级：提供入侵行为检测模块（含WEB应用攻击检测），提供恶意文件检测模块-，含六年的规则特征库升级，含六年的病毒特征库升级3、阻断与处置：支持旁路阻断策略，可针对IP进行旁路封堵;支持与态势感知平台进行一键封堵策略，对攻击者进行一键处置，快速封堵攻击行为.4、加密流量处理：支持导入证书对HTTPS协议流量进行解密。6、流量存储与取证：支持对威胁相关的数据包进行存储，供关联分析和取证使用7\恶意流量检测范围：可针对网络病毒、蠕虫、间谍软件、木马后门、扫描探测、暴力破解等恶意流量进行检测.8资产识别与评估：支持从流量中自动识别资产信息和归类，识别的信息至少包括资产IP、资产MAC、资产类型、操作系统名称、操作系统版本、端口、服务、协议;支持对资产进行风险评估，结合威胁事件对资产判定为是否失陷.9、维保与升级：原厂维保六年、提供六年漏洞库升级授权。 |
| 8 | 态势感知平台 | **硬件配置**：1、内存≥128G，硬盘≥256G SSD， 数据硬盘≥16T SATA- ≥2个千兆电口，≥2个万兆光口（含2个万兆多模光模块）或≥2个千兆光口，具备管理口、扩展插槽等基础接口2、机箱与电源：≥标准2U设备，双电源3、接口配置：≥2个USB口，≥1个串口（或管理口）。**功能参数**1、数据处理与存储能力：基于大数据基础构架，具备海量数据接入、存储、访问、计算能力。支持多源异构安全设备、网络设备、全流量设备、终端设备、APT威胁检测设备、漏洞扫描设备等数据接入与威胁分析，输出可疑威胁事件。2、核心功能：综合各类网络安全分析日志，完成关联分析、视图展示、策略下发等能力，形成综合安全管理能力，支持对存储的流量日志进行回溯查询（包括TCP/UDP会话日志、DNS解析日志、Web访问日志等多种类型），回溯时间可自定义;支持对日志基于安全分析引擎进行关联、归并和过滤，转化为少量安全事件，提供统一监测界面.3、威胁事件管理：提供威胁事件统一运维入口。支持展示安全事件涉及的攻击路径，可详细查看攻击源和目的.4、可视化展示：提供可视化大屏，支持以地图、指数、柱状图、趋势图等形式展示整体安全态势;5、联动能力：支持与防火墙、WAF设备等协同联动，平台可下发指令执行网络阻断（需对端厂商配合提供接口规范）;支持对接主流厂家设备，内置多种日志解析规则.6、维保服务：原厂维保六年，含特征库升级（硬件维保六年）。 |