**技术文档**

**网络审计系统技术参数**

|  |  |  |
| --- | --- | --- |
| **性能参数** | | |
| 性能参数 | 适用带宽 | 2G |
| 适用用户数 | 35000人 |
| 最大并发连接数 | 300万 |
| 最大新建连接数 | 90,000个/S |
| **硬件参数** | | |
| **接口** | 默认网络接口 | 1管理网口、1HA网口  加配4口万兆光口板卡 |
| USB接口数 | 2 |
| RS232串口(RJ45) | √ |
| **旁路模块** | 面板硬件bypass按钮 | √ |
| 内置电口bypass模块 | 板载无Bypass接口 扩展电口均支持 |
| 内置光口bypass模块 | √ （仅配置光口内置BYPASS扩展网卡时支持） |
| 支持外置光口bypass模块 | √ （仅配置光口扩展网卡时支持） |
| **存储** | 硬盘 | 1T |
| **电源** | 交流电压 | 110～240V |
| 直流电压（直流主机参数） | -48±5V |
| 最大功率 | 300W |
| 冗余电源 | √ |
| **硬件规格** | 尺寸(WxDxH mm) | 440x540x88 |
| 机箱高度 | 2U |
| **环境要求** | 工作温度 | 0°C - 40°C |
| 存储温度 | 0°C- 70°C |
| 工作湿度 | 20%~85%RH |

**网络审计系统应答**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **产品指标项** | **产品性能参数和要求** | **应答** |
| 基本要求 | 性能 | 网络层吞吐率：≥10Gbps，审计事件入库速度不小于3万条/秒； | 产品满足此要求 |
| 规格 | 机架式2U设备，含1个RJ45串口，1个GE管理口，1个HA接口，双冗余电源；  设备提供不少于4个万兆光口业务口，并提供对应多模光模块和线缆；支持千兆光口和千兆电口的扩容；  系统自带内部存储，存储空间不低于2TB，最大支持4TB存储；支持外部存储设备。  提供三年服务和license； | 满足 |
| 满足 |
| 满足 |
| 满足 |
| 产品资质 | 《计算机信息系统安全专用产品销售许可证》；  信息安全产品强制性认证证书(ISCCC)； |  |
| 满足 |
| 满足 |
| 网络功能 | 工作模式 | 监听模式接入 | 满足 |
| 网络适应性 | 多端口链路聚合、支持MPLS网络； | 满足 |
| 监控功能 | 系统状态监控 | 提供设备实时CPU、内存、磁盘占有率、会话数、在线用户数、系统时间、网络接口、当天网络质量、最近发现移动终端等信息； | 满足 |
| 安全状态监控 | 实时显示当天的安全状况，最后发生安全事件的时间、类型、总次数、源对象，帮助管理员管理内网安全； | 满足 |
| 审计功能 | 网络审计 | 支持电子邮件审计：支持SMTP、POP3、WEBMAIL等协议，支持基于邮箱地址、邮件主题、邮件内容、附件名的关键字审计功能；可记录源IP地址、目的IP地址、时间、邮箱地址、邮件主题、邮件内容、邮件附件等信息；邮件附件格式支持DOC、PDF、ZIP、RAR、TXT等；也可以无条件完全记录所有邮件内容和附件； | 满足 |
| 支持HTTP网页浏览及关键字搜索审计：记录用户网站访问行为包括源IP地址、目的IP地址、访问时间、URL、网页浏览时间等，并提供网页还原功能。 | 满足 |
| 支持审计NFS协议的用户名、文件名等 | 满足 |
| 支持Telnet协议的审计，能够审计用户名、操作命令、命令响应时间、返回码等； | 满足 |
| 支持对FTP协议的审计，能够审计用户名、命令、文件、命令响应时间、返回码等； | 满足 |
| 支持移动应用审计，能够识别通过移动热点所访问的移动类应用，例如IM类、社交类、网购类、影音类、资讯类等应用，并记录IP地址、应用名称、访问时间等信息；能够对主流的移动应用进行内容层面的详细审计，主要是对微博、网页言论、网页访问详细记录IP地址、URL地址、访问时间、访问或发布的具体内容等信息。 | 满足 |
| 支持流量审计：支持基于时间、协议、IP地址等组合流量审计策略。支持统计各种应用协议的总流量、上下行流量及TOP10排名；针对协议TOP10排名， 可查看使用当前协议的IP及其流量。支持统计各IP的总流量、上下行流量及TOP10排名；针对IP TOP10排名，可查看当前IP使用的协议及其流量。 | 满足 |
| 支持基于论坛主题、发帖内容的关键字审计功能；支持基于用户/用户组、时间、关键字等多种组合审计策略，可记录源IP地址、目的IP地址、发帖论坛、发帖人、主题、发帖时间、发帖内容等，并提供内容还原功能。 | 满足 |
| 支持文件传输审计：支持HTTP、FTP协议，支持基于用户/用户组、时间、关键字等多种组合审计策略，用户可自定义下载文件类型，对文件上传、下载类型进行审计，可记录日志包括源IP地址、目的IP地址、时间、传输文件名等。 | 满足 |
| 系统功能 | 日志查询功能 | 支持以时间、源IP、客户端程序、业务系统、数据库用户、数据库名、操作类型、表名、返回行数、影响行数、响应时长、响应码、策略、规则、风险级别、SQL模版为条件的数据库风险查询。 | 满足 |
| 告警功能 | 支持邮件告警功能，支持短信告警功能； | 满足 |
| 报表功能 | 应提供完善的日志管理功能，支持自动报表功能，用户可自行定义生成报表的周期、设备、日志类型、日志等级等；  生成的报表可自动发送至用户指定邮箱。 | 满足 |
| 备份与恢复 | 支持系统配置文件的备份和恢复； | 满足 |
| 第三方扩展接口与联动功能 | 支持SNMP和syslog，支持开放API接口或者其他接口与其他平台进行对接； | 满足 |
| 其他功能 | 支持NTP服务器 | 满足 |

**漏洞扫描系统产品参数**

|  |  |
| --- | --- |
| **产品名称** | 网神SecVSS 3600 漏洞扫描系统 |
| **产品型号** | S9000-W030M |
| **系统扫描** | 支持扫描A类、B类、C类地址（可添加1024个IP） |
| **系统扫描并发IP数** | 150 |
| **Web扫描** | Web扫描域名无限制（可添加300个域名） |
| **Web扫描并发域名数** | 25 |
| **MTBF（小时）** | 100000 |

硬件规格

|  |  |
| --- | --- |
| **产品名称** | 网神SecVSS 3600 漏洞扫描系统 |
| **产品型号** | S9000-W030M |
| **串行配置管理接口（个）** | 1 |
| **千兆电口** | 6 |
| **千兆光口（SFP插槽）** | 2 |
| **扩展插槽** | 2 |
| **扩展板卡** | 2电、4电、8电、2光、4光、8光、2万兆光、4万兆光 |
| **机箱** | 2U |
| **内存** | 16G |
| **硬盘** | 1TB |
| **电源** | 冗余电源 |
| **尺寸** | （深）560mm\*（宽）440mm\*（高）88mm |

**漏洞扫描系统应答**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **产品指标项** | **产品性能参数和要求** | **应答** |
| 基本要求 | 性能 | 系统扫描IP地址无限制，支持扫描A类、B类、C类地址，系统扫描支持至少100个IP地址并行扫描； | 满足 |
| 规格 | 机架式设备，含1个RJ45串口，1个GE管理口，1个HA接口，双冗余电源； | 满足 |
| 设备提供不少于2个千兆光口业务口，并提供对应多模光模块和线缆；支持千兆光口和千兆电口的扩容； | 满足 |
| 提供三年服务和license； | 满足 |
| 产品资质 | 《计算机信息系统安全专用产品销售许可证》； | 满足 |
| 信息安全产品强制性认证证书(ISCCC) | 满足 |
| 网络功能 | 工作模式 | 旁路接入网络； | 满足 |
| 监控 | 系统状态监控 | 提供设备实时CPU使用率、内存使用率、磁盘使用率、网络接口状态、设备系统状态、设备版本信息、设备规则库状态等设备资源信息； | 满足 |
| 防护业务安全 | 支持系统漏洞、网站安全漏洞整体态势的图表统计展示模式；支持漏洞整体态势分布的地图展示模式；可以通过参数配置切换展示模式； | 满足 |
| 支持总体漏洞分布态势展示，支持风险等级、风险评分、发现漏洞数量最多的系统和应用类型TOP10、周和月度漏洞数量趋势、漏洞处置情况统计等 | 满足 |
| 资产管理功能 | 资产发现 | 支持资产自动发现功能，支持利用历史扫描过程中所发现的在线主机信息，来添加资产； | 满足 |
| 资产信息包括操作系统类型、版本；设备类型、厂商及型号，开放的端口、服务、协议及版本信息； | 满足 |
| 资产管理 | 支持通过文件导入或手工录入的方式，录入资产信息； | 满足 |
| 支持手工添加、删除、修改资产信息； | 满足 |
| 支持资产列表的导入和导出； | 满足 |
| 扫描功能 | 系统扫描 | 产品扫描信息包括主机信息、用户信息、服务信息、漏洞信息等内容。需给出各类扫描信息的详细列表，支持40000种以上漏洞，其中数据库漏洞库为2000种以上； | 满足 |
| 支持Windows系列、苹果操作系统、Linux、AIX、HPUX、IRIX、BSD、Solaris等目标主机的系统进行扫描； | 满足 |
| 支持对Cisco、Juniper、华为、F5、Checkpoint等网络设备扫描； | 满足 |
| 支持对VMware、KVM等虚拟化设备检测； | 满足 |
| 支持主流数据库的检测，应包括但不限于：Oralce、Sybase、SQLServer、DB2、Postgres、MySql、MsSql、mongodb等； | 满足 |
| 支持Windows域环境扫描，可针对目标主机的系统配置缺陷及漏洞进行扫描； | 满足 |
| 产品支持对扫描对象安全脆弱性的全面检查，如安全补丁、服务配置等。 | 满足 |
| 支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL认证，SID、数据库名称、实例名称及实例号等登录选项的设置； | 满足 |
| 支持SNMP等协议的漏洞检测； | 满足 |
| 口令扫描 | 产品具备专用的口令破解字典，包括密码字典、用户名字典、组合字典等多种口令破解字典； | 满足 |
| 产品具备SMB、TELNET、FTP、SSH、POP3、TOMCAT、SQL SERVER、MYSQL、ORACLE、SYBASE、DB2、SNMP等协议进行口令猜测 | 满足 |
| 扫描策略 | 产品要求提供多种缺省扫描策略，并可按照特定的需求，灵活制定目标对象或目标群组，可以同时应用不同扫描策略，并允许自定义扫描策略和扫描参数； | 满足 |
| 支持自动定时扫描和多种计划扫描任务管理功能，可按照指定的时间、对象自动扫描，并自动生成报告； | 满足 |
| 可以并行地检查多个被评估的系统，能够提供扫描策略定制，可以保证扫描的安全性，不影响应用系统和网络业务的正常运行； | 满足 |
| 扫描报告 | 报告应具有易懂的漏洞描述和详尽的安全修补方案建议，并提供相关的技术站点以供管理员参考； | 满足 |
| 应可根据角色需求产生灵活的报告格式，支持用户自定义报表和预定义报表；产品应可灵活定制产生各类报表数据的饼图、柱图等图表信息； | 满足 |
| 扫描报告应可对安全的威胁程度分级，并能够形成风险趋势分析报表和主机间风险对比分析报告； | 满足 |
| 系统功能 | 第三方扩展接口与联动功能 | 支持SNMP和syslog，支持开放API接口或者其他接口与其他平台进行对接 | 满足 |
| 其他功能 | 支持NTP服务器 | 满足 |

主机防病毒技术参数

360网神虚拟化安全管理系统支持的虚拟化平台列表如下：

|  |  |
| --- | --- |
| 支持的虚拟化平台 | VMware vCenter |
| Citrix XenServer |
| H3C CAS |
| Hyper-V |
| Huawei FusionSphere |
| 东方通虚拟化 |

各组件建议配置要求：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 组件 | 支持操作系统 | CPU | 内存 | 磁盘 |
| 管理控制中心 | CentOS 6.8 64bit | 4CORE | 16G | >500G |
| 轻代理 | Windows Server 2003 32bit  Windows Server 2003 64bit  Windows Server 2008 32bit  Windows Server 2008 64bit  Windows Server 2008 r2 64bit  Windows Server 2012 64bit  Windows Server 2012 R2 64bit  CentOS 5 64bit  CentOS 6 64bit  CentOS 7 64bit  Redhat 5 64bit  Redhat 6 64bit  Redhat 7 64bit  Ubuntu 10 64bit  Ubuntu 12 64bit  Ubuntu 14 64bit  SuSE 9 64bit  SuSE 10 64bit  SuSE 11 64bit  Debian 9 64bit  Oracle Linux 6 64bit  Asianux 3 64bit  Asianux 4 64bit  Deepin 15.1 64bit  NeoKylin 6.7 64bit  NeoKylin 7.0 64bit | 1CORE | 1G | >20G |

主机防病毒应答

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **产品指标项** | **产品性能参数和要求** | **应答** |
| 基本  要求 | 性能 | 不少于350个终端（物理机、宿主机、虚拟机）的安全防护 | 满足 |
| 规格 | 支持常见的操作系统平台：Windows9x/Me/NT/2000/XP/2003/Vista，支持Linux、AIX、Free BSD、Solaris、HP-UX等操作系统；；  提供三年服务和license； | 满足 |
| 产品要求 | 具有自主知识产权的国产产品；  《计算机信息系统安全专用产品销售许可证》； | 满足 |
| 安装部署 | 安装部署方式 | 支持多种安装方式，包括下载安装、远程安装、脚本安装、web发布安装、域策略；  可通过单一的部署工具来进行安装，即该部署工具包括安装所需的全部组件； | 满足 |
| 病毒防范  和查杀能力 | 病毒防范功能 | 具有主动防御功能；开启实时监控后能完全预防已知病毒的危害； | 满足 |
| 可防范、检测并清除隐藏于电子邮件、公共文件夹及数据库中的计算机病毒、恶性程序、病毒邮件。 | 满足 |
| 具备病毒爆发监控功能，一旦客户机连接异常，可以迅速发出报警，激活相应的反病毒策略和任务； | 满足 |
| 具备个人防火墙、IDS/IPS功能，保护用户重要数据，阻止恶意入侵对本地计算机造成危害； | 满足 |
| 病毒查杀功能 | 能有效预防、查杀映像劫持类型的病毒；可以防范网页中的恶意代码；  压缩文件、打包文件查杀毒； | 满足 |
| 内存查杀毒；引导区查杀毒；运行文件查杀毒；支持图片、视频等多媒体文件的查杀毒；能够有效查杀各类Office文档中的宏病毒；支持共享文件的病毒查杀；  具有未知病毒检测、清除能力； | 满足 |
| 发现病毒后有多种处理方法，例如清除、删除或隔离（隔离区可进行自定义），所有方法可在控制台统一设置和在客户端单独设置； | 满足 |
| 能够实时监控和清除来自各种途径的病毒、木马、广告软件、恶意插件、隐蔽软件、黑客工具、风险程序等，在程序界面显著位位置以不同颜色区分系统的不同安全状态； | 满足 |
| 管理功能 | 手动自动升级 | 依据策略，全网统一自动升级，不需要人为干涉；在与Internet隔离的内部网络中，提供多种升级方式，包括：自动在线升级、手动升级、下载离线升级包升级等； | 满足 |
| 增量升级 | 增量升级，以减少升级时带来的网络流量；  可设置升级周期和升级时间范围，保证及时升级并避免升级时占用网络带宽影响用户正常业务的通讯； | 满足 |
| 漏洞扫描管理 | 具有全网漏洞扫描和管理功能，可以通过扫描系统中存在的漏洞和不安全的设置，提供相应的解决方案，同时，支持下级中心从上级中心下载补丁的功能。 | 满足 |
| 控制台管理 | 控制台可以实时显示客户端的状态，远程开启/关闭实时监控，远程查杀病毒；管理中心实时监控客户端防毒状况；控制台可跨网段管理，管理不依赖网络拓扑结构； | 满足 |
| 报警功能 | 支持多种病毒报警方式，包括发送到管理控制台、声音报警、发送邮件(SMTP)、发送SNMP陷阱(SNMP Trap)、显示消息框(Message)、保存NT事件日志(NT Log)、报告给上级中心等，用户可自订制报警方式； | 满足 |
| 日志统计 | 具有病毒日志查询与统计，可以随时对网络中病毒发生的情况进行查询统计；可进行病毒事件和攻击事件趋势分析；提供自动生成报表并导出的功能。 | 满足 |
| 服务 | 售后应急服务 | 提供病毒事件应急响应预案；  在服务期内，为用户提供免费的病毒库更新和产品升级信息服务；  对于新发现的病毒，厂商能够于24小时内作出响应，及时通知用户，并提供专杀工具。 | 满足 |