**附件二：网闸详细技术参数**

|  |  |  |
| --- | --- | --- |
| **指标** | **指标项** | **详细要求** |
| **基本要求** | **系统架构** | ★2+1”系统结构，内外端机为TCP/IP网络协议的终点，阻断TCP/IP协议的直接贯通。内外端机之间采用专用硬件和专用协议进行连接，不可编程。为保障产品运行的安全及稳定性，要求产品设计、开发、生产及售后服务符合TL9000-H-S-V相关标准要求；提供第三方权威证明材料。 |
| **硬件架构** | 硬件架构由内端机、外端机、专有隔离硬件三部分组成。内端机和外端机各自具有独立主板、独立总线、独立的存储和运算单元；内端机和外端机之间非网线、USB线、SCSI线等线缆直连，基于光隔离技术专有硬件进行隔离和数据交换。 |
| **管理架构** | 管理控制层和业务数据层分离，管理系统部署于内端机上， 只能通过内端机上的管理口对网闸进行配置，不允许外端机存在任何形式的管理接口。可避免黑客从外部网络入侵，导致隔离网闸被黑客完全控制的现象。 |
| **产品要求** | **性能要求** | 2U,内外端机双侧液晶屏； 内端机6个10/100/1000Base-T接口，4个SPF插槽，2个SPF+插槽1个扩展槽位； 外端机6个10/100/1000Base-T接口，4个SPF插槽，2个SPF+插槽1个扩展槽位；,冗余电源,网络吞吐量：7Gbps； 并发连接数：40万；内外端机各1TB硬盘。可扩展WebFilter过滤模块，防病毒模块 |
| **功能要求** | **安全浏览功能** | 提供HTTP页面访问和WEB代理上网功能。 |
| 支持IP地址、端口、时间以及基于源用户身份的访问控制策略； |
| 支持访问控制日志记录和告警功能； |
| 支持http消息头、消息体，上下行方向，命令及关键字的管控，支持允许、阻断、告警三种处理方式。（提供截图） |
| 支持基于单一域名的黑白名单访问控制， |
| 支持50种以上文件类型特征识别，非扩展名过滤，包括可执行文件、文本文件、压缩文件、图片文件、多媒体文件等，支持上下行方向过滤单独控制，支持允许、阻断、告警三种处理方式。 |
| 支持JavaScript脚本、ActiveX插件、Applet插件过滤。 |
| 内置HTTP安全模块，支持URL过滤引擎、内容过滤引擎、文件过滤引擎、病毒过滤引擎、网页过滤引擎安全防护及单独启停控制。 |
| **文件传输功能** | 提供基于FTP协议和TFTP协议的文件传输功能。 |
| 支持代理、透明、路由三种接入方式； |
| 支持IP地址、端口、时间以及基于源用户身份的访问控制策略； |
| 支持访问控制日志记录和告警功能； |
| 支持FTP协议内部命令及数据层内容过滤，支持允许、阻断、告警三种处理方式。 |
| 支持50种以上文件类型特征识别，非扩展名过滤，包括可执行文件、文本文件、压缩文件、图片文件、多媒体文件等，支持上下行方向过滤单独控制，支持允许、阻断、告警三种处理方式。 |
| 内置FTP安全模块，支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制。（提供截图） |
| **数据库访问功能** | 提供对多种主流数据库,如：MYSQL、SQLSERVER、ORACLE、DB2、SYBASE等系统的安全访问。 |
| 支持代理、透明、路由三种接入方式； |
| 支持IP地址、端口、时间以及基于源用户身份的访问控制策略； |
| 支持访问控制日志记录和告警功能； |
| 内置数据库安全模块，支持内容过滤引擎，能够对数据库用户名、命令、关键字等内容进行管控，支持允许、阻断、告警三种处理方式。（提供截图） |
| **安全邮件功能** | 提供安全的邮件访问功能，支持POP3、SMTP协议。 |
| 支持代理、透明、路由三种接入方式； |
| 支持IP地址、端口、时间以及基于源用户身份的访问控制策略； |
| 支持访问控制日志记录和告警功能；支持最大活动会话数的控制和统计；支持IPV6扩展头的安全设置。（提供截图） |
| 支持发件人、收件人、邮件标题、邮件正文、邮件附件等数据内容过滤，支持允许、阻断、告警三种处理方式。 |
| 内置邮件安全模块，支持内容过滤引擎、文件过滤引擎、病毒过滤引擎安全防护及单独启停控制。（提供截图） |
| **安全VOIP功能** | 提供音视频通话访问功能，支持SIP和H323协议。 |
| 支持代理、透明、路由三种接入方式； |
| 支持IP地址、端口、时间以及基于源用户身份的访问控制策略； |
| 支持访问控制日志记录和告警功能； |
| ★内置VOIP安全模块，内置VOIP安全引擎，支持主被叫用户黑名单的控制。（提供截图） |
| **自定义访问功能** | 支持自定义的TCP、UDP协议的数据访问功能，用户自定义应用无需对自定义协议软件进行二次修改开发。 |
| 支持代理、透明、路由三种接入方式； |
| 支持IP地址、端口、时间以及基于源用户身份的访问控制策略； |
| 支持访问控制日志记录和告警功能； |
| **文件同步功能** | 提供有客户端和无客户端两种文件同步方式。 |
| 无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口；有客户端方式可提供专用文件同步客户端安装在用户服务器上，提供安全的文件同步服务。 |
| 支持NFS、FTP等多种文件服务器类型，支持实时同步和周期性同步。 |
| 支持文件同步重名策略处理，可选覆盖、不同步、重命名三种处理方式。 |
| 支持首次同步策略处理，可选合并和完全一致两种处理方式。 |
| 支持源文件处理策略，包括保留、删除、转存三种处理方式。支持同步删除、文件续传、子目录同步、日志记录开关控制；支持单一任务的线程数和缓冲时间设置，可手动设置同步任务的线程数； |
| ★支持基于文件大小和文件修改时间的同步策略，可手动指定上下限阈值。（提供截图） |
| 支持文件名和文件类型的黑白名单过滤，文件类型过滤基于文件特征识别，非扩展名识别，且支持不小于50种文件类型识别。支持文件同步信息统计，包括每个任务的开始时间、同步数据量、同步成功数、同步失败数，并能够以图表的方式进行实时可视化展现。（提供截图） |
| **数据库同步功能** | 提供有客户端和无客户端两种数据据库同步方式。 |
| 无客户端方式无需在用户服务器上安装任何插件，网闸不开放任何服务端口；有客户端方式可提供专用文件同步客户端安装在用户服务器上，提供安全的数据库同步服务。 |
| 提供多种主流数据库系统如：ORACLE、SQLSERVER、MYSQL、达梦数据库的同步。 |
| 支持一对一、一对多、多对一方式的数据库同步；支持同构、异构数据库之间的同步，同步可具体设置到字段级别。 |
| 支持网闸同侧数据库之间的数据同步，网闸可旁路部署实现数据库同步。 |
| 支持自动读取数据库表名和字段名，无需手动录入表名和字段名，降低配置复杂度。 |
| 快速配置支持全库表同步，可直接映射两个独立数据库进行同步，支持每策略映射表数量控制，支持每策略映射同步方向控制。（提供截图） |
| 支持首次同步策略处理，可选合并、完全一致、以源为准、以目的为准四种处理方式。 |
| 支持数据库同步冲突策略处理，包括覆盖、忽略、以源为准、以目的为准等处理方式。（提供截图） |
| 支持实时同步和周期性同步方式，可分别控制插入、删除、更新的同步操作。 |
| 支持数据库同步信息统计，包括每个任务的开始时间、同步成功数、同步失败数，同步忽略数，并能够以图表的方式进行实时可视化展现。（提供截图） |
| **病毒防御功能** | 支持企业版和专业版双病毒防御引擎，采用国内外知名厂商病毒库，支持病毒库升级，并提供后续升级服务。 |
| **URL过滤功能** | 支持基于URL分类知识库的web网站过滤功能，支持URL知识库的升级，并提供后续升级服务。（提供截图） |
| **入侵防御功能** | 支持入侵防御引擎，可基于攻击规则库对主流网络攻击行为进行拦截，支持告警和阻断两种处理方式。 |
| 支持HTTP攻击类，RPC攻击类，WEBCGI攻击类，拒绝服务类、木马类、蠕虫类等11大类不少于4000条的攻击规则知识库。 |
| **DDOS防护功能** | 支持DOS攻击防御，支持端口扫描防御、IP扫描防御、支持IP\TCP\UDP源限速和目的限速，可手动设置相关阈值。 |
| **安全防护功能** | 提供连接保护功能，支持基于源和目的IP地址的并发连接数和新建连接数控制，并可以手动设置相关阈值，超过阈值后可选限制和警告两种处理方式。（提供截图） |
| 提供IPV4\IPV6双栈IP+MAC绑定功能，支持基于物理接口和IP网段的IP+MAC主动探测，支持IP、MAC信息查询功能。（提供截图） |
| **用户认证功能** | 提供本地认证功能和外部认证功能，外部认证支持Radius、Ldap、Tacacs等类型的认证服务器。 |
| 支持认证页面的门户配置，支持认证用户的界面保活，可手动设置保活时间。（提供截图） |
| **负载均衡**（**网络管理功能）** | 网络接口支持IPV4\IPV6双栈IP地址配置，支持MTU、双工模式、接口速度的手动设置。 |
| 支持接口聚合，可手动设置聚合接口的负载均衡算法。 |
| 支持IPV4/IPV6双栈基础路由配置和邻居学习。 |
| 提供服务器负载均衡功能，支持轮询、加权轮询、最少连接、加权最少连接等负载均衡算法。（提供截图） |
| **设备监控功能** | 提供状态信息监控，以图表形式实时展现内外端机的CPU、内存、硬盘利用率，流量和会话数。 |
| 提供接口流量监控，以图表形式实时展现内外端机每个物理接口的当前状态和流量信息。 |
| 提供应用流量监控，以图表形式实时展现内外端机TOP10应用流量排名，包括上下行流量、总流量和流速信息。 |
| 提供用户流量监控，以图表形式实时展现内外端机TOP10用户流量排名，包括上下行流量、总流量和流速信息。 |
| 提供威胁统计监控，以图表形式实时展现内外端机TOP20的病毒防御威胁事件统计排名。 |
| 提供在线用户监控，可实时展现内外端机在线用户名称、IP地址、认证服务器名称、客户端类型和在线时间信息，并可根据管理需要手动强制指定用户下线。 |
| **系统管理功能** | 管理端通过独立的管理口与网闸内端机相连，策略统一从内端机下发，不允许采用外端机上的任何网络接口进行管理。 |
| 提供统一的https管理界面，支持ssh和telnet远程管理，支持配置文件的加密导入导出。 |
| 提供固件维护和license升级功能，支持本地、FTP、TFTP三种导入方式。 |
| 提供ping、traceroute、tcp、http、dns等诊断诊断测试工具，支持设备健康记录和调试信息的导出。（提供截图） |
| 提供告警功能，支持邮件、声音、控制台、SNMP等多种告警方式。（提供截图） |
| **日志审计功能** | 支持日志审计功能，包括管理日志、系统日志、策略日志、同步日志和应用行为日志。支持日志记录查询、删除、导出，日志记录可导出文本文件和数据库文件两种格式。 |
| 支持日志记录本地数据库存储，也可以将日志传输到独立的日志服务器上，传输日志格式支持syslog和welf，支持日志加密传输。 |
| **资质要求** | **销售许可证** | 公安部计算机信息系统安全专用产品销售许可证书（增强级） |
| **涉密证书** | 保密局涉密信息系统产品检测证书 |
| **软著** | 计算机系统软件著作权登记证书 |
| **CCRC** | 网络关键设备和网络安全专用产品安全认证证书  中国国家信息安全产品认证证书(增强级) |
| **IPV6证书** | 具有IPv6 Ready Logo 认证证书 |
| **GB/T28181** | 公安部GB/T28181-2016《公共安全视频监控联网系统信息传输、交换、控制技术要求》检测报告 |
| **CMMI5** | 所投厂商具备云安全成熟度模型CS-CMMI 5认证，提供证书复印件 |