# 附件6：详细技术参数要求

**1、防火墙：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 指标要求 | 证明材料要求 |
| 1 |  | 产品规格 | 1U机箱，千兆电口≥10个，单电源。 | 否 |
| 2 |  | 产品性能 | 防火墙吞吐率≥5.5Gbp；  最大并发连接数≥180万；  每秒新建连接数≥6万；  IPSEC VPN吞吐率≥160Mbps。 | 否 |
| 3 |  | 产品功能 | 含3年攻击知识库升级许可；  含3年专业版病毒知识库升级许可。 | 否 |
| 4 |  | 系统结构 | 产品由专用的硬件平台、安全操作系统及功能软件构成。设备采用自主知识产权的专用安全操作系统，采用多核多平台并行处理机制。 | 否 |
| 5 | # | 路由交换 | 支持RIP、OSPF、BGP4、QinQ、PIM-SM、PIM-DM。 | 是 |
| 6 | # | 链路聚合 | 支持手动和LACP链路聚合，可根据源/目的MAC、源/目的IP、源/目的端口、五元组、端口轮询等条件提供不少于10种链路负载算法。 | 是 |
| 7 |  | IP/MAC绑定 | 支持IP/MAC绑定，支持跨三层绑定，支持IP/MAC绑定表导入导出，以便对IP/MAC绑定关系进行批量操作； | 否 |
| 8 | # | 地址转换 | 支持多种地址转换，支持源/目的NAT、双向NAT、NoNAT转换方式；支持源IP转换同一性；支持端口块地址转换和EIM地址转换。 | 是 |
| 9 |  | DNS Doctoring | 支持DNS Doctoring功能，能够将来自内部网络的域名解析请求定向到真实内网资源，提高访问效率，同时支持通过配置多条 DNS Doctoring，实现内网资源服务器的负载均衡； | 否 |
| 10 | # | 访问控制 | 支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、邮件安全、数据过滤、文件过滤、审计、防代理等功能配置,简化用户管理； | 是 |
| 11 | # | 访问控制策略执行动作支持允许、禁止及认证，对符合条件的流量进行Web认证，在策略中可设置用户 Web 认证的门户地址； | 是 |
| 12 |  | IPv6 | 支持RADVD、ND、RIPng、OSPFv3、BGP4+，支持IPv6静态、动态组播路由； | 否 |
| 13 |  | 支持IPv6域名控制，支持对多级域名进行控制，域名对象支持通配符； | 否 |
| 14 | # | 虚拟化 | 支持在一台物理设备上划分出多个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源，实配不少于24个虚拟防火墙授权； | 是 |
| 15 |  | 支持配置文件、系统服务、路由、链路聚合、安全策略、NAT策略、带宽管理、认证策略、IPV6功能、URL过滤、病毒过滤、WAF、僵木蠕、高级威胁防护、内容过滤、邮件安全、审计、报表、防代理等安全功能虚拟化； | 否 |
| 16 | # | 入侵防御 | 支持独立的入侵防护规则特征库，特征总数在5500条以上，能对常见漏洞进行安全防护，兼容国家信息安全漏洞库； | 是 |
| 17 | # | 厂商需具备强大的漏洞和攻防研究能力，为CNNVD一级支撑单位和CNVD技术组成员，能够确保每周至少更新1次攻击特征库； | 是 |
| 18 |  | DDOS防御 | 支持HTTP DDOS防护，采用阀值检查、源/目的限流、源认证、会话限制等方式综合进行HTTP FLOOD、HTTP URI CC攻击、HTTP连接耗尽等攻击防护； | 否 |
| 19 |  | 支持NTP DDOS防护，采用阀值检查、源/目的限流、源认证等方式综合进行NTP REQUEST FLOOD、NTP REPLY FLOOD攻击防护； | 否 |
| 20 |  | 邮件安全 | 内置邮件安全防护功能，支持邮件过滤、邮箱防暴力破解、邮件泛洪攻击防护、邮件黑、白名单检测； | 否 |
| 21 | # | 病毒过滤 | 支持对HTTP/SMTP/POP3/FTP/IM等协议进行病毒防御； | 是 |
| 22 | # | 支持至少2种专业反病毒厂商的病毒特征库（提供至少2家专业防病毒厂商的合作文件复印件），病毒特征库规模超过400万； | 是 |
| 23 | # | 配置维护 | 支持配置文件本地备份和回滚，支持＞3个配置文件备份，支持对整体配置进行加密备份和恢复，并对访问控制策略、NAT策略等关键配置进行单独备份和恢复；支持对配置命令及配置文件的操作行为进行审计； | 是 |
| 24 | # | 报表 | 内置≥16种预定义报表模板，支持应用流量、用户流量、上网行为、威胁统计等报表，支持报表自定义； | 是 |
| 25 | # | 威胁统计 | 支持对病毒防御、入侵防御、DDOS攻击等按照威胁类型/攻击主机/受攻击主机三种维度结合威胁等级和时间周期进行统计、排名。 | 是 |
| 26 | # | 产品资质 | 信息安全产品自主原创证明； | 是 |
| 27 | 防火墙密码检测证书； | 是 |
| 28 | 国家信息安全漏洞库兼容性资质； | 是 |

**2、文档管理系统**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 重要性 | 指标项 | 指标要求 | 证明材料要求 |
| 1 | # | 文件上传 | 支持单个文件上传和文件的批量上传。 | 是 |
| 2 |  | 支持文件批量上传。 | 否 |
| 3 | # | 文件上传中可随时终止文件的上传任务。 | 是 |
| 4 |  | 文件上传时进行分片，多线程并行上传 | 否 |
| 5 | # | 文件下载 | 支持文件单个下载和批量下载。 | 是 |
| 6 | # | 文件安全存储 | 文件以碎片化的形式进行存储，且打乱顺序。不以整个文件的形式进行存储。 | 是 |
| 7 | # | 个人文档 | 个人文档只限个人可见、操作。 | 是 |
| 8 |  | 支持个人目录维护。 | 否 |
| 9 | # | 支持文件的上传、下载、删除、共享、检索、标签、内外网切换等操作。 | 是 |
| 10 |  | 部门文档 | 根据权限配置，可切换部门。 | 否 |
| 11 | # | 部门文档只限本部门的个人可见、操作。 | 是 |
| 12 |  | 支持部门的目录维护。 | 否 |
| 13 | # | 支持文件的上传、下载、删除、共享、检索、标签、评论、内外网切换等操作。 | 是 |
| 14 |  | 文件删除 | 支持文件的逻辑删除。 | 否 |
| 15 |  | 回收站 | 支持文件的还原。 | 否 |
| 16 |  | 支持文件的物理删除。 | 否 |
| 17 |  | 文件评论 | 支持在部门文档里，部门人员可对文档进行评论。 | 否 |
| 18 | # | 文件标签 | 支持对文件打单个标签个多个标签。 | 是 |
| 19 |  | 支持自定义标签 | 否 |
| 20 |  | 文件检索 | 我的文档：支持文件名、后缀名、标签码的文件检索。 | 否 |
| 21 |  | 部门文档：支持文件名、后缀名的文件检索。 | 否 |
| 22 |  | 回收站：支持时间范围的检索。 | 否 |
| 23 |  | 文件共享 | 支持文档共享的时间控制 | 否 |
| 24 |  | 支持查看我分享的文档。 | 否 |
| 25 |  | 支持查看分享给我的文档。 | 否 |
| 26 | # | 上传文件控制 | 可对文件上传的大小，后缀名进行限制。 | 是 |
| 27 | # | 内外网切换 | 支持文件内外网可见性的切换 | 是 |
| 28 | # | 日志管理 | 对所有用户操作记录日志 | 是 |
| 29 | # | 日志信息保留一年。 | 是 |
| 30 |  | 组织机构管理 | 对组织机构的单位进行维护，其中包括单位名称、单位地址、负责人、联系方式等信息，可进行新增、编辑删除等操作。 | 否 |
| 31 |  | 对组织机构的部门进行维护，其中包括部门名称、所属单位、上级部门、部门地址、部门负责人、联系方式等信息，可进行新增、编辑删除等操作。 | 否 |
| 32 |  | 对组织机构的人员进行维护，其中包括用户的登录账号、所属部门、姓名、联系方式等进行维护。 | 否 |
| 33 |  | 权限管理 | 对业务的功能进行精细划分。 | 否 |
| 34 | # | 系统支持将信息化的权限管理精细化到数据记录的度，做到数据针对不同的用户可见范围可控化。 | 是 |
| 35 |  | 对用户的权限进行分级授权，统一管理。对不同的业务操作划分不同级别的角色，对角色指定不同的功能权限和数据权限，再将角色统一授予给指定用户。 | 否 |
| 36 |  | 配置要求 | 上架式2U机箱，尺寸（W×D×H）：440\*560\*88mm。 | 否 |
| 37 |  | Intel® skylake H110；网口数：6电；BYPASS：1组（1-2网口） | 否 |
| 38 |  | I5-6400 CPU 四核四线程；每核主频2.7Ghz | 否 |
| 39 |  | DDR4 16GB | 否 |
| 40 |  | 4T监控级硬盘 | 否 |
| 41 |  | 250W电源 | 否 |
| 42 | # | 对组织机构的人员进行维护，其中包括用户的登录账号、所属部门、姓名、联系方式等进行维护。 | 是 |
| 43 | # | 厂商资质 | 具有信息系统建设和服务能力等级证书，提供证书复印件并加盖原厂公章 | 是 |
| 44 | # | 具有文档管理系统著作权，不会因使用该系统引起未知的知识产权纠纷（证书至少应包括“文档管理”字样）；（加盖原厂商公章） | 是 |
| 45 | # | 具有ISO20000信息技术服务管理体系认证证书（加盖原厂商公章） | 是 |
| 46 | # | 具有ISO27017云服务信息安全管理体系证书 | 是 |
| 47 | # | 具有ITSS信息技术服务运行维护标准符合性证书 | 是 |
| 48 | # | 具有国家信息安全测评中心颁发的风险评估资质证书 | 是 |
| 49 | # | 具备信息安全服务资质认证证书-信息系统安全运维资质证书 | 是 |
| 50 | # | 具备信息安全服务资质认证证书-信息安全应急处理资质证书 | 是 |
| 51 | # | 具备信息安全服务资质认证证书-信息系统安全集成资质证书 | 是 |