防火墙参数

|  |  |
| --- | --- |
| **指标项** | **技术参数** |
| 性能要求 | 设备最大吞吐量≥6Gbps，最大并发连接数≥995万，每秒新建连接数≥9.9万 |
| 硬件要求 | 标准1U机架式，1+1冗余电源，千兆电口≥10个，千兆光口≥4个，内存≥8GB，硬盘≥SSD 500G |
| 部署模式 | 支持网关模式、网桥模式、旁路模式、虚拟网线工作模式、混合模式；部署模式切换无需重启设备。 |
| 端口镜像 | 支持端口镜像功能；支持入流量、出流量和双向流量等维度镜像。以上参数提供相关证明截图。 |
| 接口 | 接口支持配置从属IP地址，每个接口支持至少200个从属IP。以上参数提供相关证明截图。 |
| DDNS | 支持DDNS功能，支持花生壳、阿里云等服务商的域名，将动态获取的IP地址映射为固定的域名。以上参数提供相关证明截图。 |
| NAT | ★支持IPv4/IPv6双栈协议的源地址转换、目的地址转换、双向NAT、NAT44、NAT66、NAT46、NAT64等地址转换。以上参数提供相关证明截图。 |
| DNS | ★支持DNS透明代理；支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载。以上参数提供相关证明截图。 |
| 支持针对特殊域名使用指定DNS进行解析；支持域名定向解析。 |
| 支持DNS解析动态缓存，缓存信息包括但不限于域名、IP、TTL和命中次数。 |
| IPv6 | 支持IPv6/IPv4双栈；支持IPv6安全策略、包括审计策略、NAT策略、流量控制策略、会话控制策略、黑名单、白名单、认证策略等。 |
| 支持IPv6策略路由、OSPFv3、静态路由、IPv6隧道，包括IPv6手工隧道、ISATAP、6to4等隧道模式；支持IPv6网络下的DHCPv6、DNSv6、SNMPv6、NTPv6、PPPoE等基础协议。 |
| 支持IPv6入侵防御、病毒防护、Web防护、风险扫描、安全分析、资产发现、弱密码防护等安全功能。 |
| VRF | 支持虚拟路由转发功能，使用VRF功能可以从系统层面隔离不同VRF组里的流量信息和路由信息，可作为MPLS组网环境中的MCE设备。以上参数提供相关证明截图。 |
| 不同VRF下的接口可以配置相同的IP地址。 |
| 支持VRF的静态路由。 |
| 访问控制 | 支持一体化安全策略：可基于设备接口/安全域、地址、服务、应用、用户、时间等属性，配置入侵防御、病毒防护、URL过滤、应用过滤、会话老化时间、终端过滤等高级访问控制功能。 |
| 入侵防御 | ★系统定义超过8700+条主流攻击规则，包含用户提权、任意代码执行、木马、后门、挖矿、Web序列化、Webshell等主流防护类型；以及对应IPS规则的攻击类型、严重程度、CVE编号、CNNVD编号、协议、操作系统、发布年份、漏洞厂商等详细信息。以上参数提供相关证明截图；并支持在线升级和手动升级。 |
| ★预置防护模板，可基于常见场景进行一键式的安全加固；支持基于常见协议进行异常检查，包括但不限于：HTTP、DNS、SMTP、POP3、FTP；检查内容支持自定义，包括但不限于：URL长度、请求长度、目录长度、Host字段、Version字段、字符检测、文本长度、文件名长度、命令参数长度，支持针对每协议设置处置动作和事件等级。以上参数提供相关证明截图。 |
| ★支持IPS高阶告警功能，可以配置多种告警条件，达到告警规则可通过邮件或者Syslog告警，不同告警规则可以发送给不同的用户。以上参数提供相关证明截图。 |
| 支持针对攻击进行本地报文存储，方便管理员事后回溯攻击事件；支持针对某一个和某一类攻击设置报文存储机制；支持针对某一个和某一类攻击的源地址进行隔离，隔离时间可自定义。 |
| 病毒防护 | 支持HTTP、FTP、POP3、SMTP、IMAP协议的病毒查杀；支持查杀邮件正文/附件、网页及下载文件中包含的病毒；支持400万余种病毒的查杀；并支持在线升级和手动升级病毒库。 |
| ★支持对20级的压缩文件进行解压查杀。以上参数提供相关证明截图。 |
| Web防护 | 支持独立的Web防护模块，提供SQL注入攻击、XSS攻击、恶意扫描与爬虫、服务器防护、CMS漏洞防护等不少于10种的防护类型。 |
| 支持HTTP协议的精确访问控制，可针对IP、URL、Method、Referer、User-Agent、Cookie、URL-args等字段设置内容，匹配内容包括但不少于：包括、不包含、等于、不等于、属于、不属于、长度小于、长度等于、长度大于、正则匹配等。 |
| 支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护；应用隐藏可隐藏Server信息、X-Powered-By信息、替换客户端出错页面(4xx)、替换服务器端出错页面(5xx)等。 |
| 支持缓存防篡改网页，可手动清理缓存内容。 |
| 端口扫描 | ★支持针对IP、端口进行端口扫描，可选择立即执行或定期执行；支持呈现扫描结果，包括端口、端口状态、端口服务、程序版本、操作系统、风险状态、设备类型和时间等信息，支持导出功能。以上参数提供相关证明截图。 |
| 弱密码扫描 | 支持弱密码扫描能力，可针对IP、端口等对象，扫描监控空密码、用户名密码相同、预置弱口令、自定义弱口令等规则，可设置立即扫描或定期扫描，弱口令字典可自定义设置。以上参数提供相关证明截图。 |
| 其他防护 | 支持IPv4、IPv6双协议栈异常包攻击防御，攻击类型至少包含：Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP选项、IP Spoof、Jolt2等。 |
| 支持非法外联学习和防护特性，可有效保障服务器安全，可定义外联白名单地址和端口；支持通过流量自学习获得服务器合法的外联行为，检测流量中的异常访问流量，实现自动拦截；学习时长可选择1小时、12小时、一天、一周等。 |
| 失陷主机 | ★支持通过木马、数据外传、间谍软件、病毒、挖矿等行为判断主机是否失陷；支持手动或者自动的方式将失陷主机加入到黑名单中，避免威胁在内网进一步扩散。以上参数提供相关证明截图。 |
| 威胁情报 | ★支持与多个威胁情报中心订阅，帮助产品实现检测、预警和防御。以上参数提供相关证明截图，并要求产品的威胁情报功能出具关于产品的“威胁情报软件”的计算机软件著作权登记证明。 |
| ★提供在设备端上的全网威胁情报的搜索查询，包括IP、域名、文件（MD5/SHA1等）情报的查询。以上参数提供相关证明截图。 |
| 应用识别 | ★应用特征不少于7300个，移动应用不少于2400个。以上参数提供相关证明截图。 |
| 支持根据标签选择应用，预置标签分类至少包含安全风险、高带宽消耗、降低工作效率等10大类；支持给每个应用自定义标签；支持根据标签选择一类应用做控制。 |
| 支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式；支持DNS域名学习模式，可引用数据包特征中的目标域名或指定域名。 |
| ★支持应用智能识别，有效识别迅雷和P2P行为，识别模式可选择严格、适中、宽松，支持排除扫描端口。以上参数提供相关证明截图。 |
| 支持智能识别模式和快速识别模式，在智能识别模式下应用引擎尽可能地用各种方式识别网络流量，在快速识别模式下应用引擎将关闭部分智能分析功能以提高性能。 |
| 应用过滤 | 提供应用控制，支持针对应用动作的细粒度控制，比如针对社区类型，支持管控”上传“、“发表”、“浏览”、“登录”等动作。 |
| ★支持邮件控制；支持基于发件人黑白名单、收件人黑白名单、标题及内容关键字、邮件大小、附件个数进行行为过滤。以上参数提供相关证明截图。 |
| 支持针对搜索引擎、HTTP、网页内容进行关键字过滤并实时生成日志记录。 |
| 支持针对虚拟账号进行黑白名单管理，设定允许登录的QQ账号白名单或禁止登录的QQ账号黑名单。 |
| ★可识别多种文件类型，包括电影、音频、文本、图片、压缩文件（ZIP、RAR、GZ、BZ2、Z、TGZ、TBZ、7Z、CAB、BZ等）、应用程序、Office系列等；并支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤。以上参数提供Web配置界面。 |
| ★支持对FTP、Telnet、DNS等协议的相关操作命令进行过滤控制。以上参数提供Web配置界面。 |
| URL识别与控制 | 内置URL分类库，支持≥56个URL分类，URL库可在线升级；支持自定义URL过滤，包括恶意URL白名单、恶意URL黑名单、URL白名单等；并支持URL的模糊匹配。 |
| 支持基于DNS前置技术实现在DNS解析阶段针对HTTP和HTTPS域名进行过滤，防止HTTPS域名过滤逃逸情况。 |
| 旁路阻断 | 支持在设备旁路部署时针对违规上网行为进行阻断过滤。以上参数提供相关证明截图。 |
| 用户认证 | ★本地认证、Portal认证、Radius认证、LDAP认证、POP3认证、AD域单点登录、短信认证、微信认证、APP认证、二维码认证、互联网钉钉认证、混合认证和免认证，其中微信认证支持通过小程序获取手机号。以上参数提供相关证明截图。 |
| ★短信认证需支持短信平台方式，短信平台包括但不限于亿美软通、凌凯、一信通、佳诺、阿里云、梦网科技、移动云MAS、诺尔等，针对亿美软通平台支持拓展号段，拓展号段类比“电话分机号”，企业分部之间可以分别设置“拓展号段”，短信认证时设备携带“拓展号段”将手机号和验证码提交至亿美平台，亿美平台根据每一个分部的“拓展号段”通道进行短信发送，从而避免多个分部使用一个亿美账号发送短信时产生拥堵的情况。以上参数提供相关证明截图。 |
| VPN | 支持标准IPSec VPN和快速IPSec VPN，标准IPSec VPN认证方式包括但不限于数字证书和预共享密钥；同品牌设备快速IPSec VPN对接时加密算法等参数无需配置，自动生成，仅需配置保护子网、共享密钥、IP地址。 |
| 支持IPSec VPN、SSL VPN、GRE VPN；支持手机、平板电脑等移动终端VPN接入，功能标配，无需增加功能授权即可使用。 |
| API管理 | 支持被第三方管理平台通过RESTFUL接口进行调动管理，结合业务需求，实现业务快速变更和威胁动态处置。防火墙主要功能应具备RESTFUL接口，包括但不限于：接口管理、路由、NAT、DNS、控制策略、QoS、系统管理等。 |
| 管理员认证 | 系统管理员登录认证支持USBKey双因子认证。以上参数提供相关证明截图。 |
| 系统管理员支持与第三方服务器联动认证，第三方服务器包括但不限于Radius服务器、LDAP服务器；支持第三方服务器状态探测，根据服务器状态自动切换认证方式，服务器异常时，切换为本地认证，服务器恢复后使用外部认证。 |
| 系统维护 | ★提供智能策略分析功能，支持策略命中分析、隐藏策略分析、冗余策略分析、冲突策略分析、可合并策略分析、过期策略发现、空策略发现、策略宽松度分析，并在Web页面显示分析结果。以上参数提供相关证明截图。 |
| 支持SNMPv1、v2、v3版本，支持跨三层自学习MAC地址。 |
| Web管理界面支持Ping、Traceroute、TCP SYN诊断工具，可支持基于接口、协议、IP地址、端口、应用进行网络抓包，并可下载导出分析。 |
| 其他 | ★至少三年质保期 |

特别说明：投标人需具备本项目的实施技术能力， 投标人需要提供切实可行的安装方案、售后应急方案及设立专门的售后维护队伍，包括对现场的故障诊断、应急的解决方案、故障排除的时间等。为保证设备在更换过程中不影响采购人的业务正常运行，要求设备原厂工程师到现场安装调试，如投标产品不能满足功能及性能要求，将不能通过采购人验收。每年至少一次来现场进行巡检。中标后七个工作日内，有权要求提供样机进行上述功能要求的逐一测试验证，全部通过后才能执行合同流程，测试中发现虚假应标的行为将予以废标处理并保留对该厂商追究相关责任的权利。文中标有“★”的技术指标不容许发生偏离，如发生偏离视为无效投标。质保期满后，必须配合采购单位做好后续衔接工作。