**下一代防火墙参数**

| **指标项** | **参数要求** |
| --- | --- |
| 硬件架构 | 采用多核网络专用架构，使用64位MIPS多核处理器，非X86的多核架构或ASIC架构 |
| 产品规格 | 标准1U专用千兆硬件平台，内置交流单电源，硬盘≥500G |
| 网口数量 | 10\*GE电口，2\*Combo口；支持千兆接口总数≥12个 |
| 性能 | 设备最大吞吐量≥2Gbps，HTTP吞吐量≥1.5Gbps，IPS吞吐量≥620 Mbps，AV吞吐量≥600Mbps，IPSec VPN性能≥800Mbps，最大并发连接数≥100万，每秒新建连接数≥3.5万，IPSec VPN隧道数≥1024，SSL VPN接入数≥400 |
| 部署模式 | 支持路由、网桥、旁路、混合、虚拟线工作模式；工作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 |
| 接口 | ★接口支持配置从属IP地址，每个接口要求支持至少200个从属IP（提供截图证明并加盖公章） |
| 4G支持 | ★支持4G接入，并可实现4G连接与有线链路之间互为备份（提供截图证明并加盖公章）；  支持的4G网卡必须包括华为E3372；支持在4G接口上运行IPSec VPN |
| NAT | 支持支持源NAT、目的NAT、静态NAT、NAT44；支持FTP、H323、PPTP、RTSP、SIP、TFTP等应用协议ALG |
| 路由支持 | 支持静态路由、动态路由、ISP路由；支持基于入接口、源地址、目标地址、用户、服务、应用、时间、域名的策略路由；ISP路由支持内置联通、电信、教育网、移动等ISP服务商地址列表，并支持运营商地址自定义 |
| 链路负载均衡 | 支持基于7元组、域名的链路负载均衡策略，负载算法支持优先级和权重；支持过载保护、会话保持和健康检查，会话保持可实现用户的访问请求均分配至同一出口 |
| 服务器负载均衡 | 支持5元组的服务器负载均衡策略，负载算法支持权重、源地址散列+权重；支持服务器健康检查和会话保持 |
| DNS代理 | ★支持DNS透明代理功能，代理算法包括：优先级、权重和流量（提供截图证明并加盖公章） |
| 支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理，当一条链路出现故障时，流量自动切换到其他链路的同时将DNS服务器进行切换，避免出现跨运营商解析而导致访问变慢或中断 |
| 支持静态域名配置，支持特定域名由特定DNS服务器解析，支持DNS Proxy缓存控制 |
| DDNS | 支持DDNS功能，支持花生壳服务商的域名，将动态获取的IP地址映射为固定的域名 |
| IPv6支持 | 支持配置基于IPv6地址的安全策略，并在一条策略中可同时启用入侵防御、反病毒、URL过滤、应用识别等安全功能 |
| 支持6to4、ISATAP、IPv6手工等IPv6隧道技术 |
| VRF | 接口默认属于root，创建VRF后可把接口添加到VRF内，一个接口只能属于一个VRF；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 |
| 双机热备 | 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，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，链路探测 |
| 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（提供截图证明并加盖公章） |
| 应用识别与管控 | 支持应用识别，内置5000种以上应用特征库，并可识别iOS、安卓等移动互联网软件如微博、微信等特征，并可智能识别P2P和迅雷行为，并支持在线升级和手动升级 |
| 支持智能和快速两种应用识别模式，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（提供截图证明并加盖公章） |
| 支持自定义应用，可基于协议、端口、IP、域名等维度定义未知应用 |
| 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”、”登陆“等动作  提供邮件控制，支持针对邮件收发件人、邮件标题及内容关键字，邮件大小、邮件附件个数进行过滤  支持针对搜索引擎、HTTP上传、网页内容的WEB关键字过滤  支持针对虚拟账号过滤，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 |
| ★用户认证 | 支持IP准入、MAC准入、IP+MAC准入、本地WEB认证、Portal认证、短信认证、免认证、微信认证、混合认证、AD域单点登录和访客二维码认证（提供截图证明并加盖公章） |
| 微信认证功能支持使用微信连WiFi2.0接口，限制微信流量放通（移动端，认证通过放通），支持基于http获取access\_token，支持微信内部浏览器http弹portal，支持强制关注功能（定时检查用户是否关注公众号）（提供截图证明并加盖公章） |
| Portal认证功能支持联动portal和radius服务器，支持portal逃生，支持针对HTTPS网页推送portal页面，支持伪portal推送抑制，可限制应用产生的HTTP伪推请求，有效缓解认证服务器压力（提供截图证明并加盖公章） |
| 用户全天行为分析 | ★支持用户全天行为分析，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息（提供截图证明并加盖公章） |
| SSL解密 | 支持对SSL协议进行解密，解密类型支持https和邮箱 |
| 流量管理 | 支持基于线路和多层通道嵌套的带宽管理和流量控制功能，提供至少四层管道嵌套；支持基于地址、用户、服务、应用、时间等匹配条件进行流量控制；并支持配置保障带宽、最大带宽、每IP带宽、每用户带宽、带宽优先级等QoS动作 |
| 支持带宽动态调整技术，带宽繁忙通道支持动态借用空闲通道的带宽，避免带宽浪费 |
| ★支持用户限额策略，可基于流量和时长两种限额类型、日限额和月限额两种统计维度，超过限额阈值，支持终端网页提醒，支持添加到惩罚流控通道或禁止上网的惩罚设置（提供截图证明并加盖公章） |
| 网络攻击防护 | 支持防ARP欺骗、ARP flood攻击防御 |
| 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 |
| 支持扫描攻击防御，可基于设定的阈值识别扫描，并自动对发起扫描的主机进行限制 |
| 支持基于目的IP和接口的SYN、UDP、ICMP、DNS等flood攻击防御 |
| 入侵防御 | 内置不少于8000条IPS规则库，包含安全漏洞、CGI攻击、缓存溢出、木马后门、网络数据库攻击、蠕虫病毒、间谍软件、欺骗劫持等安全类型  并支持在线升级和手动升级 |
| 支持自定义IPS特征，至少支持IP、UDP、TCP、ICMP、HTTP、FTP、POP3、SMTP等协议自定义入侵攻击特征；可拓展协议字段，设置数据包中的匹配内容，支持选择包含、等于、不等于、大于、正则匹配等匹配方式，可选择多种匹配条件，支持设置“与”和“或”的匹配顺序 |
| 至少支持telnet、ftp、imap、pop3、smtp、rlogin、http、oracle、mysql、postgres等常见协议的防暴力破解功能，针对每种协议可自定义检测时长、阈值和阻断时长 |
| 至少支持telnet、ssh、ftp、imap、pop3、smtp、mysql、postgresql、mssql、rlogim、vnc等常见协议的弱密码检测功能，支持弱口令、空密码、用户名和密码相同等检测方式，弱口令字典可自定义设置 |
| 支持DNS隧道传输检测，用于检测DNS隧道协议中的恶意流量 |
| ★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，也可通过流量自学习获得服务器合法的外联行为，学习时长可选择1小时、12小时、一天、一周等（提供截图证明并加盖公章） |
| 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 |
| 病毒防护 | 支持病毒检测引擎，内置病毒库不少于400万条，支持在线升级和手动升级 |
| 支持对HTTP，FTP，POP3，SMTP，IMAP等协议进行病毒查杀 |
| 支持对最多20级的压缩文件进行解压查杀 |
| Web防护 | 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，可替换服务器端出错页面(4xx)、替换服务器端出错页面(5xx)等 |
| 内置Web防护特征库，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，支持手动和自动特征库升级 |
| 支持网页防篡改，可手动清理缓存内容 |
| ★威胁情报 | 拥有自有数据来源，每日可获得不低于6亿次的互联网访问样本（提供访问量证明并加盖公章） |
| 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（提供截图证明并加盖公章） |
| 提供最新的威胁情报信息，能够对新爆发的0day、高危漏洞等进行预警，并提供配置向导协助管理员生成安全防护策略（提供截图证明并加盖公章） |
| 支持实时获取威胁情报，并应用威胁情报对本地资产进行威胁检测，并可对检测到的威胁情报支持单点登陆威胁情报云平台查看该情报详情（提供截图证明并加盖公章） |
| IPSec VPN | 支持与主流VPN厂商的IPSec VPN接入，支持的算法有DES、3DES、AES128、SM2、SM3、SM4等，支持预共享密钥、数字证书、国密证书方式建立隧道 |
| 支持IPSec快速配置，当跟自有设备对接时，自动生成加密算法等参数，仅需配置保护子网、共享密钥、IP地址 |
| 支持GRE隧道，支持GRE over IPSec VPN |
| SSL VPN | 支持自定义资源类型，可定义发布的协议和端口，资源支持导入导出，可快速完成配置；支持自定义门户页面中的标题、logo和公告内容 |
| 支持SSL VPN用户防暴力破解功能，可根据用户和IP设置防护阈值 |
| 支持SSL VPN账号与VPN资源唯一绑定，针对拨入用户设置拨入时间段和强制下线时间，精细管控用户访问权限 |
| 应用缓存 | 支持缓存安卓和iOS文件，文件形式不限于视频、APP、文本文件等，并支持自学习性缓存，设备可自动缓存特定服务器的所有终端应用 |
| 共享接入管理 | 支持识别和封堵私接主机，包括360随身wifi、猎豹wifi、无线路由器等软硬件网络共享方式，可制定策略分别设置私接终端类型个数为阀值进行封堵，同时支持基于IP配置白名单，支持自定义阻断时间，支持限速时长内添加到惩罚通道 |
| 支持私接用户的PPPoE账号展现，支持状态监控、解锁操作，支持基于用户、MAC、终端数量的监控和搜索 |
| 广告推送 | ★支持配置在用户上网时弹出广告页面，支持配置广告跳转链接和广告推送间隔，广告类型支持本地或第三方广告（提供截图证明并加盖公章） |
| PKI | 支持X.509 V3数字证书；支持CER/PEM/PKCS12多种证书编码；支持内置CA，为其他设备或移动用户签发证书；支持本地CA根证书、根私钥的更新；支持在线CRL列表 |
| 会话管理 | 支持基于IP的会话限制和每秒新建限制 |
| 实时显示当前会话数和历史1小时、1天、1周会话数；支持基于会话的源地址、目的地址、目的端口的排名统计 |
| 会话监控界面展示当前会话数信息，显示会话属性至少包含用户、用户组、源地址、源端口、目的地址、目的端口、协议、类型、应用、策略ID、发送包数、接收包数、总包数、发送流量、接收流量、总流量、会话状态、本地连接、策略动作、创建时间、超时时间、存在时间、入接口、出接口、源NAT地址、源NAT端口、目的NAT地址、目的NAT端口等25项，并且可根据任意条件进行查询和排序 |
| 策略分析 | 支持策略分组，每条策略添加到一个策略组，便于管理员区分化管理和运维 |
| 提供策略分析引擎，支持一键全局分析和单独策略的即时分析，至少支持检测出冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略，并提供问题策略的原因说明、优化建议，同时提供快捷的编辑修改方式，并以表格和柱状统计图形式展示全局问题策略 |
| 支持全局策略宽松度分析，以引用策略中的源地址、目的地址中的实际IP地址数目换算得到极宽松、较宽松、正常、准确这4种宽松度级别，并以表格和柱状统计图形式展示地址精确度分析结果 |
| ★安全分析 | 具备对检测到的攻击行为按照攻击源地址的地理位置进行威胁信息展示，并支持将攻击源地址一键加入到黑名单的操作（提供截图证明并加盖公章） |
| 支持基于资产的安全分析，支持展示网络中存在安全风险的资产以及对应的风险级别，至少可查看资产基本信息、攻击态势、攻击日志统计、攻击的具体事件类型、攻击时间等（提供截图证明并加盖公章） |
| 支持基于攻击不同阶段的方式来匹配并展示攻击者发起攻击的具体所处状态，资产遭受到攻击的具体所处状态，展示出具体的攻击链并可对威胁进行取证（提供截图证明并加盖公章） |
| 系统日志 | 支持本地日志记录和远程日志输出，SYSLOG日志支持同时发给多个日志服务器 |
| 业务告警 | 支持基于设备健康状态，业务信息等维度的邮件等方式告警 |
| 统计报表 | 支持每天、每周、每月生成报表，报表支持本地保存、下载、FTP服务器上传、邮件发送；支持自定义报表模板，模板下默认支持设备健康状态、数据统计、网络质量、网络安全等模块 |
| 系统维护 | 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 |
| 支持通过ICMP、TCP、DNS等协议实现对链路可用性的多重健康检查，并支持统计探测目标的成功率和延时 |
| 支持三权管理方式，包括账号管理员、权限管理员、审核员，各管理员权限制约；权限管理员支持分配权限，可细致分配界面中每一个模块的读写权限 |
| 支持管理员双因子认证 |
| 配置管理 | 支持中英文Web界面管理及命令行管理，支持基于SSL协议的远程安全管理 |
| 支持通过集中管理平台进行集中管理，包括统一状态检测、配置下发、配置自动备份，版本升级、特征库升级、日志收集 |
| 支持U盘零配置上线，设备端无需预配置，将U盘插入设备USB接口中，即可实现快速上线实施（提供截图证明） |
| 支持SNMPv1、v2、v3版本，支持跨三层自学习MAC地址 |
| 支持多配置切换，配置文件之间相对独立，灾备场景可快速恢复业务 |
| 产品资质 | 具备公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证（增强级）》  具备中国信息安全认证中心颁发的《中国国家信息安全产品认证证书（增强级）》  具备中国国家版权局颁布的《计算机软件著作权证书》  具备全球IPv6测试中颁布的《IPv6 Ready Phase 2证书》  具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》 |
| 售后服务 | 提供3年免费升级维护；  提供24小时支持热线；  原厂商在浙江省内有常驻机构能为用户提供快速及时的现场服务（须提供企业登记注册证明），提供本地应急响应时间<=4小时； |

**商务条款**

1、供应商应提供3年的原厂质保服务并出具原厂质保函，7\*24小时技术服务及设备维保服务。

2、中标方提供一年两次网络安全运维服务包含漏洞扫描服务、系统渗透服务、系统加固服务并出相关运维报告。

3、中标后签订合同前，中标方必须提供中国信息安全认证中心的信息系统安全集成证书和信息系统安全运维证书、政府部门认可的内网流量监控系统著作权证书、网站漏洞扫描系统著作权证书、服务器漏洞扫描系统著作权证书。

4、自合同签订之日起，中标方必须在20个工作日内完成交货。自交货之日起，中标方必须在15个工作日内按照采购方需求完成设备安装调试，并能上线正常运行使用且各项功能均能满足采购方需求，按照采购方需求提供服务。

5、中标方所提供的货物必须是合同约定的厂家生产、全新未使用过的（包括零部件、备件等），并完全符合原厂质量检测标准（以说明书、合格证为准）和国家质量检测标准以及合同规定的性能和功能要求。

6、附件参数里面★的部分不允许负偏离。

7、若验收不合格，则采购方有权解除合同，中标方必须支付合同价款的10%用以赔偿采购方的损失。

8、为避免虚假应标，中标单位在签订合同前需提供上述参数要求的所有证书及附件参数里面★的截图材料，若无法提供或提供材料不完整，则中标单位的本次投标将被视为无效投标。

以上商务条款中标供应商必须全部满足，否则报价无效。供应商如果不按要求报价、中标后无故放弃、不按合同履行等违约行为的，采购人将依法向政府采购管理部门举报，并根据政府云在线询价规则上报政府云监管部门处理。