**北仑区教育城域网IPV6改造及**

**核心设备冗余建设项目（2021年)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 名称 | 品牌型号 | 参数要求 | 数量 | 单价（万元） | 价格（万元） |
| 互联网应用交付网关 | 深信服AD-1000-B2400 | 详见下表相关内容 | 1 |  |  |
| 上网行为管理网关 | 深信服AC-1000-B2250 | 详见下表相关内容 | 1 |  |  |
| 网络安全防火墙 | 深信服AF-2000-B2450 | 详见下表相关内容 | 1 |  |  |
| IPv4/v6协议应用转化系统 | 微格VBC-NS2800iptra | 详见下表相关内容 | 1 |  |  |
| 项目服务费用 |  | 原防火墙和上网行为管理设备延保服务(各2年）、辅材、配件及项目调试安装等其它费用 | 1 |  |  |
| 合计 |  |  |  |  |  |

# 应用负载AD（AD-1000-B2400）

|  |  |
| --- | --- |
| **功能指标** | **参数要求** |
| 产品形态 | 需采用独立的专用硬件AD应用交付设备，而非通过添加功能模块的方式实现 |
| ▲产品配置 | 性能参数：4层吞吐量（默认网口）≥20Gbps，并发连接数≥20000000，4层新建连接数 CPS≥650000，7层新建连接数 RPS≥700000。 硬件参数：规格：2U，内存大小≥32G，硬盘容量≥480G SSD，电源：冗余电源，接口≥8千兆电口+8千兆光口SFP+2万兆光口SFP+。 |
| 设备部署 | 支持串接部署方式和旁路部署方式，支持三角传输模式 |
| 多合一功能集成 | ★单一设备可同时支持包括链路负载均衡、全局负载均衡和服务器负载均衡的功能。三种功能同时处于激活可使用状态，无需额外购买相应授权。（提供设备操作界面截图证明材料并加盖厂商公章) |
| 负载均衡算法 | 支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、最小流量、加权最小流量、按主机加权最小流量、带宽比例、哈希、主备、首个可用、优先级等算法 |
| 可编程流量控制 | 通过某种编程语言（如lua）实现自定义的流量编排，对IP、TCP、UDP、SSL、HTTP和HTTPS等类型的流量进行分发、修改和统计等操作。 |
| 链路负载均衡 | 支持静态IP和PPPOE两种线路接入方式。 |
| ★支持三明治架构，对防火墙、IPS、行为管理等网络设备进行流量负载均衡和故障切换，使以上网络设备获得Active-Active运行的能力。（提供实际的功能测试报告）支持跨设备健康状态监视（透明监视），同时支持IPv4和IPv6 |
| 支持基于五元组条件（源IP地址，源端口，目的IP地址，目的端口，传输层协议号）来进行出站访问的流量调度分发 |
| ★支持基于管理员自定义的时间计划来进行出站访问的流量调度分发。（提供设备操作界面截图证明材料） |
| 内置完备的IP地址库，无需手动导入并支持自动全网更新，可查看并编辑各国家、国内各省份的IP地址段和国内各大运营商IP地址段，并可灵活匹配IP地址库进行流量调度分发，实现链路负载功能 |
| ★支持基于URL的链路调度功能，内置不少于1000条的国外URL网址库，无需手动导入并支持自动更新，管理员可查看并进行编辑。可根据URL将访问国外网站的请求调度到指定线路。（提供设备操作界面截图证明材料） |
| 支持基于应用协议的智能选路，能对网银、游戏、视频等流量进行调度（提供设备操作界面截图证明材料） |
| 支持基于域名的流量调度，针对特定网站选择指定的链路转发。 |
| 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（提供设备操作界面截图证明材料） |
| SLB能够通过健康检查来获取后端服务器状态，同时将服务可用性、设备CPU、新建并发吞吐等数据上报GSLB，设备之间的联动使得GSLB能根据链路和服务器两者的综合状态实现智能切换，为用户选择最优的数据中心和服务器分配方式 |
| 支持跨数据中心集群和跨数据中心会话保持 |
| 支持多种链路检测方法，能够通过PING、TCP、HTTP等方式监控链路的连通性，当某一条链路故障时，可将访问流量切换到其它链路，保障用户业务的持久通畅 |
| ★支持链路负载投屏展示，能够分别基于链路监测、应用选路和ISP流量进行投屏展示分析。链路监测展示链路的健康状态、上下行带宽、总带宽、新建连接数、并发连接数和吞吐量；应用选路展示基于应用分类选择相应链路的示意图；ISP展示基于运营商分类选择链路的示意图。（提供设备操作界面截图证明材料并加盖厂商公章） |
| 支持cookie加密，提升cookie安全性。 |
| 支持优先级算法下最少可用节点保障，优先级高的节点故障时会自动进行选举，保证优先级高节点的可用性 |
| 支持常见的主动式健康检查功能，提供基于SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL数据库等多种类型的探测判断机制，支持对HTTPS服务进行内容健康检查 |
| 支持用户自定义方式的健康检查，支持多种编程语言（如Python、Java等），用户可根据节点运行的实际业务流程来编写代码，检查业务处理逻辑是否正常。 |
| 支持外部监视器探测方式通过编写脚本执行命令使得节点智能恢复，当节点出现故障时，负载均衡能自动重启服务器上的相关进程或重启服务器，使其恢复正常状态并继续提供服务；如无法使其恢复正常，则将其从节点池中移除，保证业务正常访问。 |
| ★支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规HTTP应用可配置基于反映URL失效的HTTP响应状态码的观测判断机制，对于复杂应用可配置基于RST关闭连接和零窗口等异常TCP传输行为的观测判断机制。（提供设备操作界面截图证明材料并加盖厂商公章）） |
| ★支持面向服务器健康度的弹性调控机制，可通过监控业务流中的TCP传输异常来衡量服务器节点的有效性，尝试对性能不足的服务器临时开启过载保护，动态调节服务器的负载。（提供设备操作界面截图证明材料） |
| ★支持主动探测方式与被动观测方式结合使用的服务器健康检查手段，以便适应各种复杂应用交互流程，保障业务系统的高可用性。（提供设备操作界面截图证明材料） |
| 支持命令行配置，支持Tab键补全操作，支持界面全部模块通过命令行的模式配置，支持命令批量操作，支持配置导入导出命令行操作 |
| 节点支持域名和IP两种形式，支持自定义DNS查询间隔。 |
| 支持后端服务不可用时主动关闭连接，保证客户端访问的连续性 |
| 支持Loose Initiation和Loose Close功能选项（支持非SYN建立会话的选择和任意FIN释放会话选择） |
| ★对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包（提供设备操作界面截图证明材料） |
| ★服务器负载状态支持投屏展示，能够显示设备的电源状态、风扇转速、磁盘温度、CPU温度、CPU和内存占用率、新建连接数、并发连接数、吞吐情况、SSL新建和SSL吞吐数据、压缩优化和缓存优化数据；业务的健康状态、新建连接数、并发连接数、上下行流量、每秒请求数；节点池的调度算法、健康状态、新建连接数、并发连接数、上下行流量；（提供设备操作界面截图证明材料并加盖厂商公章）） |
| 多分区功能 | 支持二个或四个以上的多重引导（根据硬盘的大小来判断，每100g可以虚拟出一个分区，比如240g就可以两个多重引导，480g就是4个多重引导），便于软件版本升级 |
| IPv6改造 | IPv6支持双栈模式，支持NAT46、NAT64、NAT66、FTP ALG、DNS64等协议转换 |
| IPv6改造方案能够解决天窗问题，支持一条策略匹配多个外链网站，同时外链和网站子链发生修改时支持自动识别并做主动修改，不允许通过人工解析配置的方式解决天窗问题 |
| 支持网站页面IP形式和域名形式外部链接的正常访问；支持静态和动态网站页面静态和动态引用站外内容的正常显示；支持静态和动态网站页面静态和动态外部链接的无限级正常跳转 |
| 支持通过syslog的方式实现IPv4/IPv6协议转换日志功能，累积存储和查询3个月内数据；提供IPv6/IPv4协议翻译和互通的日志信息，包括源/目的IP地址和端口，被访问的URL等信息，并在需要的情况下，回溯查询用户信息 |
| 业务交付优化（服务器负载） | 七层虚拟服务支持时间戳、TIME\_WAIT资源快速回收、节点失效关闭连接和重置无效连接功能（提供设备操作界面截图证明材料） |
| 支持SSL卸载功能，卸除服务器端的密集型运算任务，释放服务器计算资源，并提升SSL业务的处理速度 |
| ★支持非对称式部署的TCP协议优化技术，提升远端用户访问应用服务的速度。无需在用户终端或应用服务器上安装任何插件和软件，不受操作系统类型、浏览器版本等兼容性因素限制，并且用户首次访问应用服务即可产生加速效果。(提供第三方评测报告,证明所投产品厂商可提供此类技术) |
| ★支持图片优化技术，通过对图片格式的转换，减少传输流量，提升web页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的WebP或JPEG格式，优化加速效果。（提供设备操作界面截图证明材料并加盖厂商公章）） |
| 免费开通HTTP压缩、HTTP缓存、TCP连接复用、SSL卸载等功能，无需额外购买相应授权。 |
| 高可用性 | 支持双机热备部署方式，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换，支持基于链路流量进行有效性判断，能够在预设时间内进行主动探测。支持高可用集群N+M部署方式，单集群支持16台设备，可自动同步配置并提供连接会话的镜像功能，实现无缝故障切换； |
|
|
| 一虚多 | 提供基于VM和容器两种方式的硬件一虚多。一台物理设备可从逻辑上划分为多台虚拟设备，各虚拟设备拥有独立的计算资源和网络资源，各虚拟设备可运行不同软件版本，虚拟设备重启或升级时不影响其他虚拟设备的正常运行，虚拟设备宕机可自动重启 |
| 运维管理 | 支持全中文管理界面和HTTPS方式登录、用户角色管理、多级授权管理。 |
| 支持设置管理地址白名单列表，远程维护支持设置是否允许WAN/LAN |
| 支持SNMP v1/v2c/v3，标准MIB库和自定义库，可接受第三方网管平台如zabbix的管理 |
| IPv6支持双栈模式，支持NAT46、NAT64、NAT66等协议转换 |
| ★内置智能告警系统, 支持E-mail、SNMP Trap两种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息。（提供设备操作界面截图证明材料） |
| 支持标准的RESTful形式的API接口，可实现与第三方应用平台的集成与二次开发。（提供设备操作界面截图证明材料） |
| 产品资质 | 所投产品具备《计算机软件著作权登记证书》所投产品具备《IPv6 Ready Phase-2金色认证证书》所投产品生产厂家通过CMMI5认证以保证产品代码质量与稳定性设备生产商的负载均衡类产品入选Gartner应用交付控制器（ADC）魔力象限报告，属于国际市场认可的知名品牌设备生产商的负载均衡类产品在2019年市场占有率达到前三名所投产品具备国家强制性产品认证（CCC认证）报告所投产品具备国家工业和信息化部颁发的《电信设备进网许可证》以上资质需提供资质复印件作为证明材料 |

# 全网行为管理AC（AC-1000-B2250）

|  |  |  |
| --- | --- | --- |
| **项目** | **功能指标** | **参数要求** |
| 性能参数 | ▲性能配置 | 网络层吞吐量（大包）≥18Gb，应用层吞吐量≥4.5Gb，带宽性能≥2.5G，IPSEC VPN加密性能（最高性能）≥800Mb，支持用户数≥25000，准入终端数（默认客户端授权数）≥14000，包转发率≥384Kpps，每秒新建连接数≥40000，最大并发连接数≥1800000。规格：2U，内存大小≥16G，硬盘容量≥64G SSD+960G SSD，电源：双电源，接口≥6千兆电口+4千兆光口SFP+2万兆光口SFP+。 |
| 部署方式 | 虚拟化模式 | 支持基于虚拟化平台的软件版本，支持的虚拟平台包括：VMware、深信服超融合等平台； |
| 全面支持IPv6 | 支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；（提供产品界面截图）； |
| 实时监控 | 首页可视化分析展示 | 支持首页分析显示接入用户人数、终端类型、认证方式；资产类型分布、新设备发现趋势、终端违规检查项排行、终端违规用户排行；带宽质量分析、实时流量排名；泄密风险、违规访问、共享上网等行为风险情况； |
| ★Web访问质量检测 | 1.针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级 2.支持以列表形式展示访问质量差的用户名单 3.支持对单用户进行定向web访问质量检测（提供产品界面截图） |
| 排障工具 | 图形化排障 | 提供图形化排障工具，便于管理员排查策略错误等故障，支持网络故障排查、权限策略排查、用户认证排查、SSL解密故障排查 |
| 认证方式 | 绑定短信和微信快捷认证 | 支持终端用户可以使用账号绑定的手机号码，接收短信验证码，然后使用手机号码和验证码完成密码认证；支持在终端用户的账号存在微信绑定关系的情况下，PC端的终端用户可以直接使用微信扫码二维码完成密码认证过程，移动端的终端用户，可以直接打开微信扫码完成密码认证过程。 |
| 自注册认证 | 密码登录支持用户自注册，通过Web页面申请注册新账号，管理员审批后新账号可用，自注册同时支持portal认证和802.1x认证；支持管理员关联了手机号码，可以通过手机号接受自注册、终端注册、终端绑定的审批通知（提供产品界面截图） |
| ★OA认证 | 支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；支持企业微信、MOA、钉钉 这三个平台支持同步组织结构，用户通过企业微信、MOA、钉钉认证上线，本地会创建与认证服务器上对应的用户组，用户会上线到对应创建的组；（提供产品界面截图并加盖厂商公章） |
| 会议扫码认证 | 支持提供二维码和会议号，用户扫码或输入会议号认证上网；支持通过验证手机号码实名认证 |
| 二维码审核认证 | 支持二维码认证，担保人扫描访客的二维码后对其网络访问授权；支持访客填写信息、担保人填写信息、免填写信息三种模式 |
| 终端资产管理 | ★IP管理 | 支持图形化查看当前内网IP使用情况，帮助管理员减少人工维护IP表的工作量；（提供截图证明文件） |
| 终端识别发现 | 自动发现网络里面的终端，并获取IP、Mac、厂商、操作系统、开放服务、开放端口等信息，设备必须支持PC、移动设备、哑终端、专用设备的发现和型号识别：至少支持Windows、Linux、MAC、瘦客户机等PC；至少支持手机、平板等移动设备；至少支持服务器、交换机、无线控制器等7类网络设备；至少支持打印机、投影仪、电视、摄像头、门禁系统等10类哑终端；（提供产品界面截图）  |
| ★终端分类可视 | 1.对网络接入的终端进行可视化管理，展示终端详细信息、异常状态等 2、支持查看终端类型，以及终端详细信息（厂商，系统，端口等）；3.支持查看终端类型分布（提供截图证明文件） |
| 共享接入管理 | 防共享接入 | 支持发现私接路由（或者共享软件等）共享网络的行为：1.支持自定义配置终端数量和冻结时间。2.支持“仅统计电脑”和“统计所有终端”两种模式。3.支持可选“冻结IP”还是“冻结用户名”。4.支持添加信任列表 5.支持显示以IP或用户名的维度统计一段时间内的趋势图。6.支持例外排除功能：如冻结条件是2. 指定例外条件1台PC，2个终端。当PC或终端数超过例外条件才会被判定为共享。7.支持在数据中心报表中可查询通过共享上网的IP、用户，并能导出报表；（提供产品界面截图） |
| 网页管理 | 静态URL库 | 设备内置海量预分类的URL地址库，能够针对：网上购物、成人内容、求职招聘、在线影音及下载等70个以上细分类型的URL做识别和分类，同时所有URL类型都支持区分“网站浏览”、“文件上传”、“其他上传”、“HTTPS”等细分行为并分别做权限控制。 |
| URL数量在3000万以上，包含分类数量150个以上，同时支持自定义URL；（提供第三方机构检测报告证明） |
| SSL加密网页识别过滤 | 1.识别并过滤SSL加密的钓鱼网站、非法网站等，支持将违规https访问重定向到告警页面，2.必须支持https网页全解密和按网站类别分类进行解密配置；3.必须支持旁路解密，支持非中间人代理的解密方式，终端用户上网无证书告警；（必须提供自主知识产权证明）；  |
| 应用管理 | 应用识别规则库 | 1.设备内置应用识别规则库，支持超过10000条应用规则数，支持超过6500种以上的应用，并保持每两个星期更新一次，保证应用识别的准确率；2.支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类；3.支持给每个应用自定义标签；4.支持根据标签选择一类应用做控制；5.支持对每一种应用的定义和解释，帮助客户快速定位应用的分类；6.支持给每一种应用列上图标，易于客户了解应用的特征。（提供产品界面截图） |
| ★SaaS应用规则 | 1. 对Saas应用有默认分类标签，帮助客户统一配置策略 2.必须支持超过200种主流网络会议/办公OA/教育学习应用（提供产品界面截图并加盖原厂商公章） |
| 桌面应用细分控制 | 1.能够对新浪微博、腾讯微博、网易微博等进行细分控制，如：登录、浏览、发微博、上传附件等。；2.能够对teamview、QQ远程桌面等远程控制应用做细分控制，如：接受对方远程控制；3.能够对Github、百度网盘、百度文库等网络应用的上传动作进行细分控制； |
| 移动应用的细分控制 | 支持对移动应用的细分权限控制，微信：微信网页版、微信传文件、微信朋友圈、微信游戏。移动QQ：QQ传文件、QQ视频语音等。 |
| 代理管理 | ★禁止使用代理 | 1. 不允许使用外部HTTP代理；2.不允许使用外部Sock4/5代理；3.不允许在HTTP,SSL一些的标准端口上使用其他协议；（比如在80端口上传输非HTTP协议数据，在443端口上传输非HTTPS协议数据等）（提供产品界面截图并加盖原厂商公章） |
| 多线路支持 | 多线路技术 | 网关必须能同时连接多条外网线路，且支持多条线路流量复用和智能选择流速最快线路的技术(必须提供自主知识产权证明)； |
| 流控策略 | 流控策略适用多种对象 | 支持基于用户组、位置、终端类型、URL类型配置流量管控策略 |
| 带宽分配 | 动态流控 | 支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；空闲值可自定义 |
| P2P智能流控 | 支持通过抑制P2P的上行流量，来减缓P2P的下行流量，从而解决网络出口在做流控后仍然压力较大的问题； |
| 单用户流控 | 流控黑名单 | 基于“流量”、“流速”、“时长”设置配额，当配额耗尽后，将用户加入到指定的流控黑名单惩罚通道中  |
| 流控可视化 | 流控通道实时可视化 | 能够实时看到各级流控通道的状态：包括所属线路、瞬时速率、通道占用比例、用户数、保证带宽、最大带宽、优先级，启用状态等。 |
| 审计策略 | 特权DKey | 支持针对特权用户配置免认证key、免审计key、免控制key |
| 网页审计 | 网页快照 | 支持网页内容审计后的网页快照功能； |
| 加密证书自定义 | 支持用户可以自定义产生根证书，导入包含秘钥的根证书； |
| IM审计 | IM客户端审计 | 支持根据QQ、微信账号查询IM聊天行为和内容，以会话回放的方式查询IM审计日志 |
| 运维工具审计 | 运维工具审计 | 支持telnet协议，可对登陆的账号、执行的命令进行审计；支持SSH/RDP协议，可对连接开始时间，连接结束时间，传输的流量大小进行审计；支持运维类应用的外发附件审计，包括Xshell，Pshell，MobaXterm，SecureCRT；（提供产品界面截图） |
| 远程应用审计 | ★远程应用审计 | 支持Teamviewer、向日葵、Anydesk、RDP的远程应用的外发文件审计； |
| 业务行为审计 | 业务系统自定义 | 支持自定义业务系统名称、描述，绑定到相应的IP地址和端口或域名，以每个业务系统作为单独审计对象；  |
| ★业务访问审计 | 支持HTTP/HTTPS/FTP/SMB类型业务的行为和内容审计，对上传/下载文件可选择只审计文件名或同时审计文件内容；（需提供产品界面截图并加盖原厂商公章） |
| 离线上网管理 | ★离线上网审计 | 在非内网环境下通过客户端引流实现网页审计、邮件审计、应用审计、流量和时长审计，引流实现上网权限策略控制、上网时长控制、上网流量控制，支持windows终端，支持windows终端。 |
| 上网安全 | ★僵尸主机检测 | 具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证；（需提供产品界面截图并加盖原厂商公章） |
| 支持识别、阻断、冻结（指定时长）僵尸主机，并推送同品牌端点安全软件进行查杀， |
| 场景应用分析 | 数据分析应用 | 数据中心可以对上网日志进行大数据分析，并支持多个大数据分析模型，包括泄密分析、离职倾向分析、上网态势分析、带宽分析、工作效率分析，可导出报表。 |
| 查询和订阅 | ★支持与多种网安日志平台对接 | 内置多套日志模板与各省市网安日志平台对接，至少支持以下平台：派博、任子行、网博、云辰、烽火、中新软件、兆物、新网程、美亚柏科、爱思等。（提供产品界面截图） |
| 等保合规自检 | 等级保护评估合规自检 | 可以对接等保合规自检平台，设备自检后将结果发送给平台，快速输出等级保护合规自检报告； |
| 产品成熟度 | 《计算机信息系统安全专用产品销售许可证》中国信息安全认证中心ISCCC《IT产品信息安全产品认证证书》具有工信部颁发的《电信设备进网许可证》应为市场成熟产品，最近两年在国内IDC内容安全市场占有率排名都在前3产品应具备相当的技术认可度，最近两年产品曾入围Gartner SWG魔力象限国家标准《信息安全技术信息系统安全审计产品 技术要求和测试评价方法》的主要起草单位公司研发体系通过国际认证CMMI5国家应急中心应急支撑单位CNCERT证书（国家级）以上资质需提供资质证书复印件 |
| 其他 | 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。 |

# 下一代防火墙AF（AF-2000-B2450)

|  |  |  |
| --- | --- | --- |
| **项目** | **功能指标** | **参数要求** |
| 硬件要求 | 产品架构要求 | ★产品采用自主知识产权的专用操作系统，应用多核并行处理技术保障产品处理性能，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“多核并行安全操作系统”的证书或检测报告。 |
| 性能要求 | ▲配置要求 | 网络层吞吐量≥60G，应用层吞吐量≥17G，IPS吞吐量≥5.3G，防病毒吞吐量≥7.5G，全威胁吞吐量≥4G，并发连接数≥900万，HTTP新建连接数≥35万。规格：2U，内存大小≥24G，硬盘容量≥64GB SSD+1TB SATA，电源：冗余电源，接口≥4千兆电口+8千兆光口SFP+4万兆光口SFP+。 |
| 网络适应性 | 链路状态检测 | 产品支持链路健康检查功能，支持基于多种协议对链路可用性进行探测，探测协议至少包括DNS解析、ARP探测和PING方式。 |
| 链路聚合 | 产品支持链路聚合功能，可以将多个物理链路组合成一个性能更高的逻辑链路接口，提高链路带宽和链路可靠性。 |
| IPv6功能 | 产品支持IPv4/IPv6双栈工作模式，以适应IPv6发展趋势。 |
| 产品支持IPv6访问控制策略设置，基于IPv6的IP地址、服务、域名、应用、时间等条件设置访问控制策略。 |
| VPN功能 | 产品支持IPsec VPN和SSL VPN功能。 |
| 产品支持IPSec VPN智能选路功能，根据线路质量实现自动链路切换。 |
| 产品支持多种SSL VPN用户认证方式，至少包括本地密码认证、LADP认证和硬件特征码认证。 |
| 应用控制 | 应用识别 | 产品支持对不少于9880种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（需提供产品功能截图证明） |
| 流量控制 | 产品支持多维度流量控制功能，支持基于IP地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。 |
| ★产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。所投产品必须提供具备CMA（中国国家认证认可监督管理委员会）认证的第三方权威机构关于“国家/地区的流量管理”功能项的产品检测报告并加盖原厂商公章。 |
| 会话控制 | 产品支持基于IP对象的会话控制策略，实现并发连接数的合理限制。 |
| 访问控制 | 访问控制策略 | 产品支持多维度安全策略设置，可基于时间、用户、应用、IP、域名等内容进行安全策略设置。 |
| 地域访问控制 | 产品支持与国家位置信息结合设置安全策略，识别流量发起的国家或地区的位置信息，根据流量发起的国家或地区的访问位置信息实现对不同区域访问的差异化控制。 |
| 安全防护 | DDoS防护 | 产品支持异常包攻击防御，异常包攻击类型至少包括Ping of Death、Teardrop、Smurf、Land、WinNuke等攻击类型。 |
| 加密流量安全防护 | 产品支持对HTTPS协议加密流量进行解密，支持配置基于区域、对象、业务类型、服务器IP/端口的解密策略。 |
| 防病毒 | 产品支持对SMTP、HTTP、FTP、SMB、POP3、HTTPS、IMAP等协议进行病毒防御。 |
| 产品支持对多重压缩文件的病毒检测能力，支持不小于12层压缩文件病毒检测与处置。（需提供产品功能截图证明） |
| 产品支持病毒例外特征设置，根据文件MD5值和文件URL设置病毒白名单，不对白名单进行病毒查杀。 |
| ★产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，所投产品必须提供具备CMA（中国国家认证认可监督管理委员会）认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告并加盖原厂商公章 |
| 入侵防御 | ★产品预定义漏洞特征数量超过7650种，支持在产品漏洞特征库中以漏洞名称、漏洞ID、漏洞CVE标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明） |
| 产品支持基于IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL等应用协议进行深度检测与防护。 |
| ★产品支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。（需提供产品功能截图证明） |
| Web安全防护 | ★产品支持对常见Web应用攻击防御，攻击类型至少支持跨站脚本（XSS）攻击、SQL注入、文件包含攻击、信息泄露攻击、WEBSHELL、网站扫描、网页木马等类型，产品预定义Web应用漏洞特征库超过3320种。（需提供产品功能截图证明并加盖原厂商公章） |
| ★产品支持对请求报文头的X-Forward-For字段检测，并对非法源IP进行日志记录和联动封锁。（需提供产品功能截图证明） |
| 产品支持CC攻击防护功能，为保障勒CC攻击的检测效果，所投产品必须提供具备CMA（中国国家认证认可监督管理委员会）认证的第三方权威机构关于“CC攻击防护”功能项的产品检测报告。 |
| ★产品支持未知威胁检测能力，需提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局、公安部信息安全产品检测中心之中任意一家检测机构出具关于“未知威胁检测”的证书或检测报告并加盖原厂商公章。 |
| 支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用。（需提供产品功能截图证明） |
| 账号安全 | ★产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生。（需提供产品功能截图证明并加盖原厂商公章） |
| 产品支持文件目录防护功能，通过对用户账号进行认证，对网站内容的修改行为进行合法性控制。 |
| 产品联动 | 蜜罐联动 | 产品支持与本地蜜罐联动，实现对APT攻击的防御功能。 |
| ★产品支持主动诱捕功能，通过伪装业务诱捕内外网的攻击行为，并联合云蜜罐获取黑客指纹信息，并自动封锁高危IP。（需提供产品功能截图证明） |
| 终端安全软件联动 | ★产品支持与终端安全软件联动管理，在防火墙产品完成终端安全策略设置和内网终端安全软件的统一管理。（需提供产品功能截图证明） |
| 态势感知平台联动 | 产品支持与态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行威胁展示。 |
| 安全策略管理 | 策略有效性分析 | 产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 |
| 策略生命周期管理 | ★产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明） |
| 高可用性 | 双机部署 | 产品支持主主、主备两种双机模式部署。 |
| 产品运维管理 | 管理方式 | 产品支持Web管理、串口管理、SSH管理等多种不同方式。 |
| 资产识别 | ★支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。（需提供产品功能截图证明） |
| 安全日志设置 | 产品安全日志支持本机、Syslog服务器和第三方管理平台等不同形式存储方式。 |
| 双因素认证 | ★产品支持管理员双因素认证功能，用户通过用户名/密码和Key等不同方式登陆产品管理界面。（需提供产品功能截图证明） |
| 网管协议 | 产品支持标准网管协议SNMP V1、SNMP V2、SNMP V3、SNMP Trap。 |
| 资质要求 | 产品资质 | 要求所投产品具备计算机信息系统安全专用产品销售许可证要求所投产品具备中国国家信息安全产品认证证书要求所投产品连续5年入围Gartner企业级防火墙魔力象限。要求所投产品在IDC在2020年 UTM品类市场占有率排名前三要求所投产品通过ICSA Labs 防火墙品类产品认证，提供有效证明材料。要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书复印件。要求所投产品具备IPv6 Ready Phase-2认证以上资质需提供资质复印件 |
| 厂商资质 | 所投产品的生产厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位所投产品的生产厂商的软件研发实力具备CMMI L5认证。所投产品的生产厂商具备云安全成熟度成熟度模型CS-CMMI 5认证。要求所投产品的生产厂商参与制定《信息安全技术 第二代防火墙安全技术 要求》要求所投产品的生产厂商为国家信息安全漏洞共享平台(CNVD)技术组成员。要求所投产品的生产厂商为中国反网络病毒联盟ANVA成员单位。要求所投产品的生产厂商为国家信息安全漏洞库CNNVD技术支撑单位。要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全软件开发服务资质以上资质需提供资质复印件 |

# IPv4/v6协议应用转化系统 (微格VBC-NS2800iptra)

|  |  |
| --- | --- |
| 功能要求 | 设备支持IPv4/IPv6用户访问IPv4信息源，支持IPv4/IPv6用户访问IPv6信息源；支持IPv4/IPv6协议转换日志的溯源审计功能；支持对于Web应用中外部链接的正常访问；支持页面缓存加速功能；支持DNS域名解析，支持权威解析和递归解析；全面支持IPv6 |
| 硬件规格 | ▲采用1U机架式专用硬件平台；固定业务接口，不低于6个千兆电口；存储介质，企业级存储介质、容量1TB；采用专用的、经过加固的操作系统 |
| 性能要求 | 单项吞吐量不低于1.2Gbps，双向吞吐量不低于2.4Gbps；最大并发连接数不低于300万，最大新建会话数不低于3万/秒 |
| 高可用性 | ▲部署方式：旁路模式部署，设备在客户实际网络中进行设备测试和验证过，以确保设备具备实际网络适用性 |
| 设备必须支持高可靠，高可用，支持HA（high-availability）自动切换功能和active-standby模式 |
| 管理功能 | 用户界面支持中文，并具有纠错功能 |
| 支持双因子登录鉴别，支持动态令牌种子文件的导入，支持动态令牌+用户名/密码方式，防止密码重放性攻击 |
| 支持设定系统的管理IP，只允许通过管理IP访问管理系统界面，对系统进行管理 |
| 支持操作日志的完整记录与查询，包括登录日志、配置变更日志等 |
| 支持系统的软件升级功能 |
| 支持将数据库内容实时备份和定时备份 |
| 支持将设备的日志文件方便的导出 |
| 支持简单网络管理协议，支持SNMPv1、v2c、v3 |
| 支持WEB远程管理，支持HTPS访问，支持Telnet或ssh |
| 支持IPv4和IPv6独立防火墙功能，支持自定义防火墙规则 |
| 支持设备实时运行状态拓扑监测，实现故障告警展现，支持自动布局和圆形布局两种拓扑展现 |
| 渗透防护 | ▲支持登录认证页面产生加密随机数，可以和Session会话进行对比分析，预防CSRF攻击（提供产品运行时操作界面截图，加盖原厂公章） |
| ▲支持HTTPS访问禁用TLSv1协议，支持TLSv1.2或更高版本（提供产品运行时操作界面截图，加盖原厂公章） |
| IPv6翻译 | ▲保持现有IPv4网络架构和主要设备不变，在Web应用系统无需改动的前提下，进行设备的部署，实现翻译功能 |
| 支持IPv4用户、IPv6用户访问IPv4信息源 |
| 支持IPv4用户、IPv6用户访问IPv6信息源 |
| ▲支持HTTP、HTTPS、POP3、SMTP、IMAP、RTCP、RTSP等协议（提供产品运行时操作界面截图，加盖原厂公章） |
| 支持网站页面IP形式和域名形式外部链接的正常访问 |
| 支持多网站并行升级转换 |
| 支持静态和动态网站页面静态和动态引用站外内容的正常显示 |
| 支持静态和动态网站页面静态和动态外部链接的正常跳转 |
| ▲支持外链过滤器添加/删除/修改，支持网站页面静态和动态外部链接的识别和处理（提供产品运行时操作界面截图，加盖原厂公章） |
| 支持IPv4/IPv6静态路由协议的配置 |
| 支持可视化状态监控，支持实施监控设计及服务的运行状况 |
| 内容缓存 | ▲支持JPEG、GIF、MP3、MP4、WMA、ZIP、RAR、FLV、LETV、F4V、EXE、ISO、APK、XML、CSS、JS等资源的缓存（提供产品运行时操作界面截图，加盖原厂公章） |
| 支持启动和禁用内容缓存 |
| 支持清理内容缓存的机制 |
| 协议转换审计 | ▲支持IPv4/IPv6协议转换日志溯源审计功能，包括用户访问时刻、用户使用的IP、访问的URL等信息，必须支持XFF协议（提供产品运行时操作界面截图，加盖原厂公章） |
| 支持将协议转换日志重定向到Syslog日志服务器 |
| 支持实时存储和查询协议转换日志功能 |
| DNS域名解析 | 支持在IPv6环境下的DNS权威解析和递归解析，支持IPv4环境或纯IPv6环境下的A/AAAA记录解析 |
| 当域名解析结果同时包含A和AAAA记录时，能够选择性过滤掉A或AAAA的结果 |
| 支持IPv6，DNS解析服务支持IPv6 |
| 支持对NS、SOA、A、AAAA、MX、CNAME、DNAME、TXT、PTR、SRV、NAPTR等记录的解析 |
| 支持标准 DNS 服务、反向DNS解析、DNS委派授权、DNS主从实时备份机制、支持DNS全局和区域转发 |
| 支持DNS参数定义（如allow-transfer、allow-recursion、allow-query、allow-notify、acl、Minimal Responses、check-names、RRSet-Order、Server TSIG key等参数） |
| 中文域名支持：支持中文域名，为企业定制中文的内部域名体系 |
| DNS智能解析，支持设定网通、电信、移动、教育、科技网等IP地址段，针对不同的地址段解析不同的IP，便于外部访问主页提高访问速度 |
| ▲支持EDNS0，支持DNS的扩展方案ECS，可通过在DNS请求报文里加入原始请求的IP（即客户端的IP），使得权威能根据该信息返回正确的结果，精准DNS调度能力（提供产品运行时操作界面截图，加盖原厂公章） |
| 支持泛域名解析：支持泛域名解析，可有效防止用户输入错误而导致网页无法打开的问题 |
| 默认TTL设置，更改资源记录的TTL值和资源记录在缓存中的TTL值。以便DNS服务器提供更好的解析响应能力 |
| ▲支持与钉钉办公系统联动，读取钉钉部门信息（提供产品运行时操作界面截图，加盖原厂公章） |
| ▲支持DNS防火墙响应策略，支持恶意域名的识别和过滤，针对域名进行阻断，支持域名不存在/存在无响应/不启用策略/强制TCP/丢弃/域名劫持等操作（提供产品运行时操作界面截图，加盖原厂公章） |
| 一键断网 | ▲特殊时期或者网站出现问题的时候，通过该功能随时随地实现“一键断网”管理，中止服务器对外提供服务。支并持自定义设置资源关闭或开启的时间（提供产品运行时操作界面截图，加盖原厂公章） |
| 质保期 | 原厂3年质保期 |
| 服务效率 | ▲1、投标厂商必须是浙江省内企业或在浙江省内有分公司（投标时需提供工商备案信息材料复印件加盖厂商公章），并具有完整的备品备件库，具备2小时内提供备件支持的能力，用户有权要求在合同签订前核实，若有虚假应标的将报告相关部门进行处理。2、提供应急响应服务：服务2小时响应，8小时解决，重大故障24小时内解决，提供7\*24小时的应急支持，针对目标信息系统出现安全风险、恶意攻击、入侵等威胁时，能2小时之内到达现场及时提供安全应急响应服务，确定故障原因并排除设备故障，确保系统运行的安全和稳定。 |
| 其他说明 | ▲1、投标人必须承诺：采购人在签订合同前随时有权利要求投标人提供此次投标设备参加复查性测试，如投标人3日内无法提供设备配合测试或测试内容与投标文件应答内容不一致，则判定为虚假应标，取消中标资格并承担相应的法律责任。2、投标人必须承诺：合同签订后5个工作日内货物须以送货上门的方式交付到招标方用户网络机房。3、投标人必须承诺：货物全部到货以后，中标方应提出合理的硬件配置和软硬件部署方案，并提供详细的系统对接方案和实施方案，经用户确认后，作为后期该设备验收的标准，中标方应安排中标设备原厂商技术工程师按上述方案在1个自然日内完成设备测试、安装、调试和有关配置工作。按照用户要求完成系统的设计对接工作。在调试完成后该原厂技术工程师需在现场驻留30个工作日，保证系统稳定运行。 |