**型号：安恒 DAS-IPS**

 **简要参数：**整机吞吐量≥4Gbps，并发连接数≥1,500,000，每秒新建连接数≥40,000,开通IPS功能模块；AV防病毒模块；负载均衡模块；7\*24小时上门服务；三年保。

**详细参数**

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 硬件要求 | 1U标准机架设备，设备配置≥10个千兆电口，2个高速USB2.0接口，硬盘≥500G |
| 性能要求 | 整机吞吐量≥4Gbps，并发连接数≥1,500,000，每秒新建连接数≥40,000,； |
| 部署方式 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式； |
| 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。以上参数提供Web配置界面截图★支持基于负载链路的出接口的DNS请求主动完成DNS服务器替换，解决用户主机配置DNS解析结果，与实际转发运营商链路解析结果有冲突，从而导致跨运营商访问慢的问题；支持进行DNS探测，针对探测失败情况，支持选择禁用dns-dnat功能或禁用负载链路出接口。以上参数提供Web配置界面截图 |
| 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。以上参数提供Web配置界面截图 |
| IPS功能 | 支持系统定义超过8000+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。以上参数提供Web配置界面截图；并支持在线升级和手动升级★支持预置防护模板，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、HTTPS\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Web配置界面截图支持基于攻击类型、严重程度、操作系统、发布时间、CVE编号、CNNVD编号、规则关键词等条件搜索过滤防护规则，帮助管理员快速检索和配置防护策略★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；支持设置检测方向，包括双向、客户端方向和服务端方向；支持自定义选择重要等级。以上参数提供Web配置界面截图★支持日志聚合，可按照源IP、目的IP、防护规则和源目IP等维度进行聚合，方便管理员快速进行攻击事件统计和回溯。以上参数提供Web配置界面截图★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Web配置界面截图 |
| 防病毒功能 | 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★支持对最多20级的压缩文件进行解压查杀。以上参数提供Web配置界面截图 |
| 自动发现 | ★支持内网资产自动发现功能，开启后自动评估内网资产安全，无需人工干预。支持展示内网资产的风险级别、IP、用户、部门、操作系统、重要程度、受攻击总数、来源等内容。以上参数提供web配置界面截图 |
| 认证 | ★系统管理员登陆认证支持USBkey双因子认证。以上参数提供Web配置界面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。以上参数提供Web配置界面截图 |
| 可视化 | ★支持数据下钻至单资产风险详情，可自动关联该资产所有安全信息，安全信息包括但不少于：入侵防御、威胁情报、防暴力破解、非法外联防护、弱密码防护、扫描攻击防御和行为模型等，支持以趋势图方式按时间展示各类安全事件的趋势，方便管理员快速了解资产安全状况，以便进行准确的安全防护。以上参数提供web配置界面截图支持关联所有安全事件，基于全球地图进行攻击源地域分析统计，支持以发起的网络攻击次数展现全球攻击源热度，统计攻击源 TOP国家，统计时间包括但不限于：一天、一周、一月和自定义时间。以上参数提供web配置界面截图支持展示攻击源的相关信息，包括但不少于：归属地、级别、攻击次数、开始时间、结束时间等，支持针对攻击源进行“一键处置”，将攻击源加入至黑名单。以上参数提供web配置界面截图 |
| 系统服务 | 支持PING、TCP、DNS方式进行接口、域名、IP地址连通性和时延探测，对整体网络提供清晰的整体网络质量评级，支持以列表形式展示的名单。以上参数提供Web配置界面截图 |
| 安全分析 | ★支持安全事件攻击链分析，以资产和攻击者两种角度关联所有安全事件，将攻击过程阶段化，分析和统计每个攻击阶段的攻击内容和攻击次数，支持针对每个攻击阶段进行数据下钻，支持分析攻击时间、攻击源、攻击目的、攻击事件、检测模块、攻击级别等信息，帮助管理员清晰了解APT攻击的攻击进度，及时在数据泄露前加固网络，针对已经数据泄露的情况，进行事件回溯，为后续网络加固提供数据支撑。以上参数提供web配置界面截图 |
| 应用缓存 | ★支持文件缓存，缓存文件形式不限于视频、安卓和IOS形式的APP等；设备智能解析用户流量，针对域名或者文件请求，设备推送文件至终端，帮助用户缓解互联网出口压力，实现文件下载加速的效果。以上参数提供Web配置界面截图 |
| 产品资质 | 产品具有计算机软件著作权证书产品具有计算机信息系统安全专用产品销售许可证产品具有IT产品信息安全认证证书三级 |