Hillstone
山 石 网 科

网络安全审计系统

山石网科网络安全审计系统以保障用户高效便捷、安全合规上网为目标，集上网行为管控、网络接入、基础安全防护、增值营销等功能于一体，为客户提供全面、完善的上网行为管理解决方案。

山石网科网络安全审计系统以透明、路由、或旁路模式部署在网络的关键节点上，对数据进行 2-7 层的全面检查和分析。实现深度审计和管控万余种 IM 聊天应用、P2P 下载应用、炒股应用、网络游戏应用、流媒体、在线视频应用等，结合智能流控、智能阻断、智能路由等技术提供强大的带宽管理机制，生成清晰易读的日志报表，帮助管理员构建安全合规的上网环境。

山石网科网络安全审计系统适用于政府、金融、教育、企业、分销等各个行业，广泛应用于上网认证、上网代理、权限管理、带宽保障、VPN、审计合规等场景。

产品价值

规范上网行为

- 规范企业管理，提升员工办公效率
- 结合业务内容和组织结构，细化访问权限
- 制定上网行为管理制度，阻断摸鱼行为
- 科学上网管理，阻断翻墙行为
- 基于关键业务进行带宽保障，提升效率
- 场景化报表，感知上网态势，为制定基线提供数据支撑

实名认证

- 用户实名上网，规避匿名用户非法风险
- 针对企业员工实现域控单点登录，简化准入流程
- 针对来宾访客提供普适易用的互联网认证机制，降低准入难度
- 广泛支持单点登录第三方 AAA 准入系统，用户身份可视化

一机多能

- 全面满足场景化建设需求，降低企业建设成本
- 互联网出口网关建设，支撑用户网络架构
- 多互联网出口智能化选路，保障业务稳定运行
- 为移动办公和异地分支等场景提供免费易用的 VPN 技术
- 助力 IPv6、代理、Portal 准入、WiFi 共享管控等场景

品牌营销

- 关联用户和应用内容，直观呈现异常上网行为

- 场景化用户画像，解决“网贷”、“办公效率”等场景化分析难题
- 构建用户上网画像，助力于大数据分析与品牌营销

功能规格

用户管理

- 支持批量导入导出用户或用户组，支持对用户和用户组新建、删除。查找和移动的操作，用户属性支持本地用户、Radius 用户、LDAP 用户、静态绑定地址用户，扩展了丰富的用户属性，支持自定义用户属性
- 在线用户状态显示（用户名、所属组、登录地址、认证方式、登录时间/冻结时间、状态、在线时长），支持用户注销、冻结、解冻操作
- 支持 Radius\数据库\POP3\LDAP 认证服务器和服务器组\邮件服务器\微信服务器\企业微信服务器\钉钉服务器\短信网关\移动 SIM\802.1X\IC 卡\酒店会员\小程序\CAS\OAUTH 联动实现准入
- 支持 Radius、Http 协议分析，认证服务器组支持主备和集群，支持 Portal chap 认证、混合认证
- 支持微信认证强制关注公众号
- 支持用户自注册自认证

上网行为管理

- 支持针对网络社区/P2P/文件传输/电子商务/IM/炒股/网络多媒体/网络游戏/远程控制/加密网站/加密邮件/HTTPS 加密搜索行为等进行审计和控制
- 支持基于用户、IP、账号、应用、行为动作、内容、终端系统及设备类型的审计
- 支持网站、邮件、论坛发贴、搜索关键字过滤和审计
- 支持对内置 URL 分类、恶意 URL 和自定义 URL 进行过滤和审计
- 支持万余种主流应用动作管理，应用特征库及 URL 库可在线或手动升级
- 支持真实文件类型、传输方向审计与管理
- 支持地址对象的限制
- 支持源 IP 的会话数、每秒新建的限制
- 支持当前 IP 地址的连接数统计，可监控当前连接的状态、协议、应用、会话时长等信息
- 全网资产识别，可通过主动&被动识别资产，深度管理内网资产

流量管控

- 支持虚拟线路和分级带宽管理，可支持 4 级通道嵌套
- 支持基于用户/应用/服务/IP/时间的带宽限制
- 具有动态流控功能，根据通道内的空闲情况，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
- 支持每 IP 限速、带宽保障和多优先级管理

终端准入管理

- 监控终端的操作系统、杀软、补丁、注册表是否符合要求，保障终端自身安全
- 监控终端的拨号行为、双网卡行为、连接非法 WIFI 等信息，确保终端联网过程中的安全
- 针对存储设备、网络设备、蓝牙、摄像头、打印机做相关管控，保障传输安全

网络基础功能

- 支持透明、路由、旁路、聚合、虚拟线、混合部署
- 支持 VLAN 子接口、桥接口、聚合接口
- 支持 DHCP 中继、DHCP 服务器、DHCP 客户端
- 支持源地址、目的地址 NAT，支持一对一、一对多、多对多地址转换，支持 NAT44
- 支持静态路由、动态路由(RIP\OSPF\BGP)、策略路由、应用路由、ISP 路由，支持 DDNS
- 支持 DES、3DES、AES 多种加密算法,支持 MD5 及 SHA-1 验证算法，支持数字证书认证
- 支持 IKE 主模式及野蛮模式, 支持 NAT 穿越和 DPD 检测
- 支持代理上网、二级代理服务器
- 支持网络引流，GRE 网络引流、IPSEC 网络引流

安全防护

- 支持 SYNflood、UDPflood、ICMPflood、DNSflood 攻击防护和异常包防护
- 支持与 IP 地址黑名单联动，禁用地址访问，支持 IP-MAC 绑定和唯一性检查
- 支持“防翻墙”配置，分析用户防翻墙行为，大屏展示跨境检测访问。
- 支持挖矿检测分析，展示挖矿类型分布、挖矿主机 TOP。

日志报表

- 基于用户、应用的流量趋势统计、分布统计和 TOP 排名
- 基于设备 CPU、内存、转发流量、会话数趋势统计
- 基于用户的网络行为、账号、流量统计分析，支持用户行为轨迹跟踪
- 支持 IM 聊天软件、网络社区、搜索引擎、邮件、文件传输、娱乐股票、网站访问、网络攻击、恶意 URL、系统操作等日志记录审计

系统管理

- 支持 Web、CLI 管理
- 配置文件支持导入导出，双备份配置
- 支持双机 HA、IPSec VPN HA，硬件 Bypass 和软件 Bypass
- 支持系统软件本地升级和远程升级
- 支持 SNMP 代理

- 支持发送 Syslog 服务器，支持日志级别过滤

故障监控

- 支持网络故障排查、解密策略故障排查、Web 访问质量检测、用户认证故障排查、上网故障检测

集中管理

- 可展示设备名称、设备分组、设备 IP、
- 设备版本、配置模板，状态等
- 可对设备进行新增、编辑、查询、复制、Web 管理及删除等操作
- 可展示设备 MAC、设备 SN、设备版本、设备型号、近 24 小时流量统计及近 24 小时 CPU、内存使用率趋势图
- 支持新增系统文件、URL 特征库、APP 特征库、AV 特征库以及 IPS 特征库
- 可展示版本名称、文件名称、文件类型、文件大小、升级次数
- 支持对所选的设备/设备组进行配置模板下发操作
- 可展示网管平台管理的设备总数，支持下钻显示设备详情
- 可展示异常设备数量，支持下钻显示异常设备的具体状态
- 可展示审计日志占比、用户流量排行、应用流量排行等

行为感知分析

- 用户行为画像，单个用户的行为画像建模分析及当前、历史分析搜索结果展示
- 工作效率分析，展示怠工人数/上网总人数，怠工比例，怠工人员平均每天怠工时长
- 非工作时间上网分析，包括员工非工作时间上网分析、部门非工作时间上网分析、非工作时间段上网使用应用分析、非工作时间段上网时长趋势统计
- 离职倾向分析，展示离职倾向人数/高危人数，离职行为最多部门的统计信息。
- 舆情分析，详细展示涉事人员信息，包括用户名、所属用户组、描述、涉事关键字搜索数量
- 不良网贷监控，包括涉及网贷人数、高风险人群、关注网贷人员的统计分析
- 沉溺网络分析，支持概览下钻详细展示，用户排行榜、用户信息，展示用户“关注内容明细”列表及用户上网时长趋

硬件规格

产品规格\国产型号	SG-6000-ICM1300-GC
推荐带宽	300M
产品形态	1U
固定业务接口	10*GE(电)+ 4*COMBO（光电复用）
扩展槽数量	2*扩展槽
BYPASS对	支持三对bypass
硬盘	1T
电源1+1备份	√
最大功率供给（W）	2*60W

集中管理平台软件

型号	SG-6000-ICM-NMS
描述	ICM集中管理平台软件系统，支持对多台ICM设备进行统一纳管。

行为分析平台软件

型号	SG-6000-ICM-BA
描述	ICM行为分析平台软件系统， 基于数台ICM设备产生的海量数据对上网用户的行为特征进行建模分析，根据不同的具体场景动态可视化呈现潜在上网风险，提高管理者对上网用户的管控能力。

注：性能数值仅供参考，实际结果可能会因不同版本和部署情况而异。

文档编号：SG-6000-ICM-V2.0P1-Y23M03-CH

www.hillstonenet.com.cn

官方微信　　视频号

中国 · 销售与服务热线： 400-828-6655

您优质可靠的伙伴　　为您的安全竭尽全力！