Hillstone
山石网科

山石网科K系列国产化下一代防火墙

SG-6000-K5280-A

K 系列防火墙是山石网科推出的满足自主可控要求的国产化网络安全产品。基于飞腾、兆芯、海光等国产处理器，搭载银河麒麟等国产操作系统，采用山石网科自主研发的软件系统，稳定安全高效。凭借全面立体的高级威胁防护、云网协同的纵深防御体系、业务可视的自动化运维，为政府、金融、能源等行业用户提供智能化、一体化、国产化边界安全解决方案。

产品特点

自主可控

智能防御

极简运维

自主可控

- 基于海光处理器，搭载银河麒麟操作系统，采用自主研发的软件系统，实现从硬件到软件自主研发，生产、升级、维护的全程安全可控
- 支持 SM 2/3/4 国密算法等技术标准，通过国家标准 GB/T 20281-2020 性能测试，满足等保合规要求
- 满足三权分立相关要求，管理角色可划分为系统管理员、安全操作员、安全审计员，三类管理权限相互制约，持续保障信息安全

智能防御

- 融合多种安全防护引擎，包含传统网络防火墙、入侵防御系统、上网行为管理、VPN、防病毒等功能于一体，简化网络部署与日常管理，满足安全合规需求
- 精细化多维防护，通过网络流量深度检测和解析技术，能够对应用、用户、内容、国家地理等进行多维度的精准识别，为用户提供丰富灵活的安全管控功能，快速感知网络业务环境
- 深度内容检测与识别，基于深度应用和协议检的入侵防御技术，有效检测过滤病毒、木马、蠕虫、间谍软件、漏洞 攻击等安全威胁，提供高级网络攻击威胁防护的能力
- 云网协同的纵深防御体系，与云端威胁情报、高级未知威胁 APT 防御(云沙箱/本地沙箱)实现智能化的协同联动。打破传统静态、被动、孤立的防护模式局限性，使安全有效性和防御实时性得到大幅提升

极简运维

- 集中管理，通过 HSM 实现“0”配置开局，统一的设备策略管理、设备健康状态监控、配置管理等。快速配置安全策略，定位安全故障，提升运维效率
- 策略优化，分析策略的命中情况，进行安全策略快速调优
- 根据业务流量，自适应的进行安全防御策略调整，实现人工运维到智能运维，降低安全运营成本
- 业务可视，为用户提供从网络到业务应用的可视化管理，丰富的可视化流量和威胁趋势、日志、自定义报表等功能，快速掌握全面真实的网络状况，更好地做出防护措施

功能规格

应用识别

- 全新一代基于应用特征、行为和关联信息的应用识别
- 支持 Windows/Android/iOS 平台 6000+应用识别及控制
- 支持应用类别、风险等级、应用技术等多维度的应用定义
- 支持自定义应用及应用组
- 应用特征库支持网络实时更新

用户认证

- 支持口令认证、短信认证、口令+短信的 Web 认证方式；支持 IPv6 web 认证；
- 支持外部服务器认证，包括 Raidus/Active Directory/LDAP/TACACS+/Oauth2
- 支持通过 SSO-monitor 协议标准进行认证用户同步
- 支持 WebAuth 认证页面定制
- 支持基于 MAC 的用户认证，支持基于接口的 web 认证
- WebAuth 支持防暴力破解
- 支持 IPv6 Radius 认证功能

安全策略

- 支持基于应用/角色/国家/省份及城市地理 IP/的安全策略
- 支持策略自学习，支持策略命中数分析
- 支持策略注释与审计，支持自定义策略属性字段
- 支持策略冗余、冲突规则检测
- 支持策略逻辑分组，支持分组一键启用/禁用
- 支持 mini policy，配置源目安全域/源目地址/协议类型

路由

- 支持静态/ISP/OSPF/BGP/RIP/ISIS/策略路由等
- 支持 IPv6 静态路由、BGP+、OSPFv3
- 支持组播 PIM-SSM 协议
- BGP、OSPF 支持平滑重启

攻击防护

- 支持多种攻击防护，包括不限 Flood 攻击、ARP 欺骗攻击、WinNuke 攻击、IP 地址欺骗攻击、DNS Query Flood 攻击等
- 支持目的 IP 地址白名单

入侵防御

- 支持实时攻击源阻断、IP 屏蔽、攻击事件记录
- 支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御
- 提供 16000 +攻击检测和防御特征，支持自定义特征
- 支持 Web 服务专项防护功能，至少支持 10 种 HTTP 请求方法检测
- 支持对常见应用协议的弱口令检查
- 支持逃逸检测能力，可有效抵御端口重映射

病毒过滤

- 支持基于流模式的病毒过滤，支持 AV 双引擎
- 支持手动导入病毒文件 MD5 检测
- 支持勒索软件、压缩病毒文件的扫描
- 支持针对 HTTP/SMTP/POP3/IMAP/FTP/SMB 等协议传输的文件进行病毒扫描

僵尸网络 C&C 防御

- 支持监控 C&C 连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏
- 支持 DGA 域名和 DNS tunneling 检测
- 支持 DNS sinkhole
- 支持动态 DNS 安全防护能力（需协同云端威胁情报平台）

威胁情报

- 支持与云端威胁情报中心联动

NAT

- 支持 NAT444/NAT64/DS-Lite/Full-Cone-NAT 等技术
- 支持双向 NAT/BNAT，支持 NAT 端口扩展
- 支持 SNAT/DNAT 命中数/冗余检测分析

基本转发

- 支持开启巨帧报文（Jumbo Frame）转发功能
- 支持 IP 分片管理
- 支持 TCP 状态检测
- 支持会话管理
- 支持 ALG

链路负载均衡

- 支持出站/入站负载均衡
- 支持智能选路功能（包括 SLA 链路探测与选择）
- 支持链路状态监测
- 入站负载均衡支持 SmartDNS

高可用性（HA）

- 支持主备模式，同步配置/会话
- 主备模式支持防脑裂功能
- 支持主备配置差异对比
- 支持 IPv4/IPv6 Twin mode

带宽管理

- 支持根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、Vlan 等信息划分管道。
- 支持两层八级管道嵌套功能
- 支持对多层级管道进行最大带宽限制、最小带宽保证

VSYS

- 支持虚拟化成多个虚拟防火墙并查看各虚拟防火墙信息
- 支持统一备份所有 VSYS 的配置

共享接入

- 支持跨三层识别接入网络终端数
- 支持识别 Windows、iOS、Android 等主流操作系统和终端类型
- IPv6 支持共享接入

数据安全

- 支持基于文件类型/文件大小/文件名称过滤
- 支持上网行为审计
- 支持内网过滤

IP 信誉库/IP Reputation

- 支持对僵尸肉鸡、垃圾邮件发送者、Tor 节点、失陷主机、暴力破解等风险 IP 的流量进行识别和过滤
- 支持对不同类别风险 IP 流量进行记录日志、丢弃数据包或阻断一定时间
- 支持通过 PTF 方式获取 IP 外部动态列表

黑白名单

- 支持基于 IPv4/v6 地址类型、服务类型、MAC 地址的黑名单
- 支持静态黑名单功能
- 支持全局白名单功能，实现 bypass 所有安全功能
- 支持周期性通过 FTP/TFTP/HTTP/HTTPS 等获取 IP 黑名单

IoT 安全

- 支持 IoT 资产管理，包括识别 IoT 终端，展示设备信息
- 支持按设备对象放行 iot 终端流量，对非指定设备阻断其流量
- 支持云端资产识别智能引擎精确识别终端厂商/类型/型号

云沙箱

- 基于云端架构的恶意软件虚拟运行环境，发现未知威胁
- 多重静态检测引擎快速过滤正常文件及已知威胁，提升沙箱检测效率
- 全局威胁情报共享，全局阻断未知威胁

网页访问控制

- 支持基于角色、时间、优先级、网页类别等条件的 Web 网页访问控制
- 支持自定义 URL 类型，配置 URL 黑白名单
- 支持实时更新 URL 库

SSL 解密

- 支持对 https 加密流量进行 URL 过滤、应用识别
- 支持 SSL 加密流量开启入侵防御功能、病毒过滤功能

零信任

- 默认提供 8 个 ZTNA 端点数
- 支持配置应用资源和应用资源组，自定义名称、描述、IP、端口、协议或者域名
- 支持应用发布，推送客户端被授权的应用清单
- 支持独立于安全 policy 之外的 ZTNA Policy
- 支持 ZTNA 客户端周期收集和上报终端信息

VPN

- 支持 IPSec VPN /PnP VPN/SSL VPN
- 支持国密算法 SM 2/3/4，，国密型号支持 SM1
- IPSEC VPN 配置多条感兴趣流支持 DNAT 场景
- IPSEC VPN 支持 IKEV2 模式下的多条感兴趣流
- SSLVPN 客户端接入认证支持双因子认证，支持短信口令认证、令牌口令认证、邮件口令认证、证书口令认证等方式

监控统计

- 支持用户应用流量、URL 访问等统计分析
- 支持应用的多维度统计监控，包括应用风险、类别、特征、所用技术等
- 支持 URL 访问和 URL 类别统计分析
- 支持实时流量统计和分析功能
- 支持安全事件统计功能

报表

- 支持安全威胁、网络流量、URL 访问等报表项
- 支持 PDF 格式报表
- 支持通过邮件或者 FTP 方式外发报表

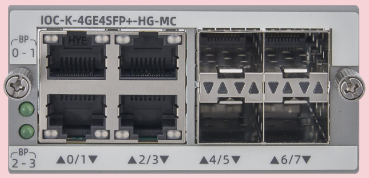
日志

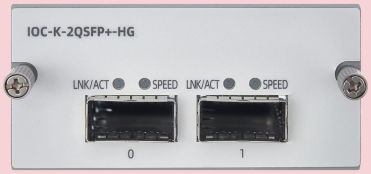
- 支持 NAT 日志、会话日志、策略路由日志、威胁日志、URL 日志、IM 上线日志等
- 支持通过二进制、文本格式外发日志

硬件规格

指标	SG-6000-K5280-A
产品图片	
防火墙吞吐量	30Gbps
管理接口	1 个 Console 口、2 个 USB口、1个HA、1个MGT
网络接口	NA，无标配网络接口
扩展模块槽	4个通用扩展槽
扩展模块选项	IOC-K-4GE4SFP+-HG-MC、IOC-K-8SFP-HG-WX IOC-K-2QSFP+-HG
存储	系统盘+SSD数据盘
电源规格	交流热插拔双电源
外形尺寸	2U（W440mm×D550mm×H89mm）

扩展模块

模块名称	IOC-K-4GE4SFP+-HG-MC	IOC-K-8SFP-HG-WX
模块图片		
描述	4 个千兆电口+4个万兆光口	8 个千兆光口
槽位占用	占用 1 个通用扩展槽	占用 1 个通用扩展槽

模块名称	IOC-K-2QSFP+-HG	
模块图片		
描述	2 个40GE光口	
槽位占用	占用 1 个通用扩展槽	

文档编号：HS-NGFW-K-5.5R11P3-CH-202503-V1.0

官方微信　视频号

中国·销售与服务热线： 400-828-6655