Hillstone
山石网科

山石网科K系列
国产化下一代防火墙

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。基于飞腾国产处理器，搭载中标麒麟、银河麒麟等国产操作系统，采用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、能源等行业用户客户提供智能化、一体化、国产化边界安全解决方案。

产品特点

自主可控：

- 基于飞腾国产处理器，搭载银河麒麟国产操作系统，采用自主研发的软件系统，实现从硬件到软件的自主研发，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的性能测试，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，基于用户的真实应用场景，预定义入侵防御策略。根据安全风险，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平台多达几千种的应用识别及控制
- 支持应用类别、风险等级、应用技术等多维度的应用定义

用户认证

- 支持外部服务器认证，包括RADIUS\Active Directory\LDAP\TACACS+
- 支持WebAuth认证页面定制
- 支持基于MAC的用户认

安全策略

- 基于应用/角色/国家地理IP的安全策略
- 支持自学习生成策略
- 支持聚合策略
- 支持安全策略重复与冗余规则检测

路由

- 支持静态路由、ISP路由，OSPF、BGP、RIP、ISIS、策略路由等
- 支持组播PIM-SSM

NAT

- 支持NAT444，NAT64，DS-Lite，Full-Cone-NAT等地址转换技术

攻击防护

- 支持SYN Flood、DNS Query Flood等多种DoS/DDoS攻击防护
- 支持ARP攻击防护
- 应用层安全功能支持一键Bypass

入侵防御

- 基于状态、精准的高性能攻击检测和防御
- 提供12000多种特征的攻击检测和防御，特征库支持网络实时更新
- 支持Web Server防护功能，含CC攻击防护和外链防护等

病毒过滤

- 支持基于流模式的病毒过滤
- 支持压缩病毒文件的扫描
- 支持针对SMB协议传输的文件进行病毒扫描

僵尸网络C&C防御

- 通过监控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IP和域名两种检测维度
- 支持DNS Tunneling检测

IP信誉库/IP Reputation

- 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
- 可对不同类别风险IP流量进行记录日志、丢弃数据包或阻断一定时间

数据安全

- 支持基于文件类型、文件大小、文件名称进行数据传输安全控制
- 支持对网页关键字、Web外发信息、邮件等内容进行过滤

网页访问控制

- 基于角色、时间、优先级、网页类别等条件的Web网页访问控制
- 支持千万级URL特征库

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、TrafficClass等信息设置管道匹配条件
- 支持两层八级管道嵌套功能

流量配额

- 支持用户/用户组限制指定时间段内的流量总额
- 支持限制每日总流量和每月总流量

链路负载均衡

- Outbound 相关功能 PBR 支持 ECMP、时间以及权重、支持内置 ISP 路由和动态探测
- Inbound 相关功能支持 SmartDNS（支持DNS A 记录解析）、支持动态探

功能规格

VPN

- 支持IPSec VPN及创新的PnPVPN
- 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
- 支持国密算法2/3/4

IPv6

- 隧道、DNS64/NAT64等多种过渡技术
- IPv6 路由（静态路由、策略路由、ISIS、RIPng、OSPFv3、BGP4+）
- 应用识别支持IPv6
- 访问控制功能支持IPv6
- URL过滤支持IPv6
- 防病毒支持IPv6
- iQoS支持IPv6
- IPS攻击防护支持IPv6

SSL解密

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

高可用性（HA)

- 支持主备模式（A/P）
- 支持peer mode模式
- 支持Twin-mode HA

虚拟系统(VSYS)

- 支持对每个VSYS分配系统资源
- 支持CPU虚拟化
- 支持防火墙、IPSec VPN、SSL VPN、IPS、URL过滤等功能

终端接入监控

- 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

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
- 全局威胁情报共享，全局阻断未知威胁

云景

- SaaS公有云服务方式，按需使用
- 对多设备的CPU、内存、流量趋势、应用、威胁等进行集中监控、可视化展现和告警

威胁情报

- 支持与云端威胁情报中心联动

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

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

报表

- 支持预定义和自定义报表模板
- 报表格式支持PDF、HTML、WORD
- 支持通过邮件或者FTP方式外发报表

硬件规格

指标	SG-6000-K5680
防火墙吞吐量	45Gbps
管理接口	1 个 Console 口、2 个 USB3.0 口、1个HA、1个MGT
扩展模块槽	8个通用扩展槽
扩展模块选项	IOC-K-8GE-B-FT-CN IOC-K-8SFP-FT-CN IOC-K-4SFP+-FT-CN IOC-K-2QSFP+-FT-CN
存储	4TB
安全策略数	60000
地址数	640000
NAT策略数	64000
电源规格	标配 冗余交流电源
外形尺寸	2U

Hillstone 山石网科

官方微信　　官方微博

文档编号：HS-NGFW-A-5.5R8P3.9-CH-202107-V1.0

中国·销售与服务热线： 400-828-6655