Hillstone
山 石 网 科

山石网科下一代防火墙

SG-6000-C1000

山石网科下一代防火墙以保障用户应用安全为目标，通过 L2-L7 层全面威胁防御及强大应用安全管控技术，为用户提供领先的网络安全解决方案。

山石网科下一代防火墙可精确识别数千种网络应用，并提供详尽的应用风险分析和灵活的策略管控。结合用户识别、内容识别、国家地理识别等多维度业务场景感知，山石网科下一代防火墙可为用户提供可视化及精细化的应用安全管理。同时，山石网科下一代防火墙内置了先进的威胁检测引擎及专业的 WEB 服务器防护功能，能够抵御包括病毒、木马、Botnet、SQL 注入、XSS 跨站脚本、CC 攻击在内的各种网络攻击，有效保护用户网络健康及 WEB 服务器安全。基于全并行软硬件架构实现的“一次解包、并行检测”，山石网科下一代防火墙在具备全面安全防护的同时，更为用户提供业界领先的安全防护性能。

山石网科下一代防火墙提供了全面的应用安全防护和灵活的扩展方式，可部署于政府、金融、企业、教育等各个行业，广泛适用于互联网出口、网络与服务器安全隔离、VPN 接入等多种网络应用场景。

产品亮点

精细化多维管控

安全防护的基础是对用户网络业务环境的全面感知，山石网科下一代防火墙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，为用户提供了前所未有的丰富而灵活的安全管控功能。

- 应用精准识别及灵活控制。山石网科下一代防火墙采用深度应用识别技术。能够准确识别数千种网络应用，其中包括600 余种移动应用、300 余种云应用。并为用户提供包括应用类别、应用风险等级、所用技术、应用特征分布等多维可视化信息，从而帮助用户及时发现应用安全隐患。同时，山石网科下一代防火墙支持灵活的应用安全控制功能，包括策略阻止、会话限制、流量管控、应用引流或时间限制等，使得应用管控十分得心应手。
- 用户认证及管控。山石网科下一代防火墙支持一套丰富的用户认证系统，支持本地认证以及 TACACS+、RADIUS、LDAP 等多种外部认证协议，支持口令认证、短信认证等多种认证方式。并可针对用户实施精细化的访问控制、应用限制、带宽保证等管控手段。
- 基于国家地理位置的访问控制。能够精确识别攻击源/ 目的IP 所处的国家地理位置，从而可以根据业务通信要求实施基于国家地理位置的访问控制，快速阻断攻击流量。
- 数据传输安全：基于数据深度检测技术，实现数据类型、大小、名称的文件传输控制，阻止关键性、敏感性、机密性数据及文件通过网络途径外发泄漏， 满足企业数据传输行为的合规性管理要求。
- SSL 加密流量全面威胁防护。可针对SSL 加密流量综合运用包括入侵防御、病毒防护、URL 过滤在内的多种管控手段，实现加密流量应用层威胁的全面防护。

全面威胁检测与防护

山石网科下一代防火墙提供了基于深度应用、协议检测和攻击原理分析的入侵防御技术，可有效过滤病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，为用户提供 L2-L7 层网络安全防护。

- 优化的攻击识别算法。能够有效抵御如SYN Flood、UDP Flood、HTTP Flood 等 DoS/DDoS 攻击，保障网络与应用系统的安全可用性。
- 专业Web 攻击防护功能。支持SQL 注入、跨站脚本、CC 攻击等检测与过滤，避免Web 服务器遭受攻击破坏；支持外链检查和目录访问控制，防止Web Shell 和敏感信息泄露，避免网页篡改与挂马，满足用户Web 服

务器深层次安全防护需求。

- 高性能的病毒过滤。领先的基于流扫描技术的检测引擎可实现低延时的高性能过滤。支持对 HTTP、FTP 及各种邮件传输协议流量和压缩文件（zip，gzip，rar 等） 中病毒的查杀。
- 支持千万级URL 特征库的URL 过滤功能。可帮助网络管理员轻松实现网页浏览访问控制，避免恶意 URL 带来的威胁渗入。
- SSL 加密流量全面的威胁防护。可针对SSL 加密流量综合运用包括入侵防御、病毒防护、URL 过滤在内的多种管控手段，实现加密流量应用层威胁的全面防护。
- 基于多核硬件架构及“一次解包，并行检测”技术，山石网科下一代防火墙在开 启多种威胁防护功能时，仍可为用户提供业界领先综合安全性能。

强大的网络适应性

山石网科下一代防火墙具备强大的网络适应能力，具备复杂环境下的安全部署能力，满足用户多样化的网络功能需求。

- 智能链路负载均衡功能。其出站动态探测和入站SmartDNS 等功能允许网络访问流量在多条链路上实现智能分担，极大提升链路利用效率和用户网络访问体验。
- 支持RIP、OSPF 和BGP 等动态路由协议。可根据网络系统的运行情况自动调整动态路由表，满足运营商、高校等复杂网络环境部署。
- 内置VPN 加速芯片。可显著提升IPSec/SSL VPN 性能，支持大规模网络环境中VPN 部署。结合iOS 及Android 平台下的VPN 客户端，可为用户提供移动终端远程接入解决方案。

统一集中管理

山石网科下一代防火墙支持集中管理，借助HSM 安全管理平台，可对多设备进行统一策略管理、设备配置管理及实时安全监控，从而实现网络的快速部署以及发生安全事件的及时响应，提高管理效率，降低运维成本。

山石网科下一代防火墙支持集中管理，借助HSM 安全管理平台，可对多设备进行统一策略管理、设备配置管理及实时安全监控，从而实现网络的快速部署以及发生安全事件的及时响应，提高管理效率，降低运维成本。

山石网科下一代防火墙支持山石“云•景”云运维功能，支持通过 web 和手机APP 实时监控多设备的 CPU、内存、流量趋势，以及应用、用户排名、威胁信息， 云景还为用户提供7×24 小时告警监控，便于用户能够及时获知网络中的动态变化及安全风险。

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
- 支持自定义应用及应用组
- 应用特征库支持远程或者本地升级，支持手动和自动升级两种方式

用户认证

- 支持本地用户的 Web 认证和短信认证
- 支持外部服务器认证（Raidus\Active Directory\LDAP\ TACACS+）
- 支持 AD 和 LDAP 的用户组及 OU 同步
- 支持 802.1X、SSO 代理
- 支持 WebAuth 认证页面定制
- 支持基于接口的主动认证
- 支持无 Agent 方式的 AD SSO 功能（AD Polling）
- 支持通过 SSO-monitor 协议标准进行认证用户同步
- 支持基于 MAC 的用户认证

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
- 支持加密流量白名单设置
- 支持 SSL 代理 offload 模式
- 支持资源列表

防火墙

- 基于深度应用识别的访问控制
- 基于应用/角色/国家地理 IP 的安全策略
- 丰富的路由特性
- 支持策略自学习
- 支持垃圾策略清理
- 具备强大的 NAT 及 ALG
- 支持防火墙策略重复与冗余规则检测

攻击防护

- 支持多种畸形报文攻击防护
- 支持 SYN Flood、DNS Query Flood 等多种 DoS/DDoS 攻击防护
- 支持 ARP 攻击防护

入侵防御

- 基于状态、精准的高性能攻击检测和防御
- 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、NETBIOSP 等 20 余种协议和应用的攻击检测和防御
- 支持缓冲区溢出、SQL 注入和跨站脚本攻击的检测和防护
- 支持自定义入侵防御特征
- 提供预定义防御配置模板
- 提供 8000 多种特征的攻击检测和防御，特征库支持网络实时更新
- 支持专业的 Web Server 防护功能，含 CC 攻击防护和外链防护等

病毒过滤

- 基于流的病毒过滤
- 支持压缩病毒文件的扫描
- 超过 200 万的病毒特征库，病毒库支持网络实时更新

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
- 基于日志、报表、监控信息、文件行为报告等， 提供未知威胁可视化能力
- 对于判断为恶意的文件，提供完整的文件行为分析报告
- 支持 HTTP、HTTPS 协议
- 支持 PE 文件类型的检测
- 支持 HTTP、HTTPS、SMTP、POP3、IMAP4、FTP 协议
- 支持 PE、APK、JAR、MS-OFFICE、PDF、SWF、RAR、ZIP 文件类型的检测
- 云沙箱检测结果阻断能力，快速阻断未知威胁
- 全局威胁情报共享，全局阻断未知威胁

僵尸网络 C2 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
- 定期僵尸网络服务器地址升级更新
- 支持 C&C IP 和域名两种方式检测
- 支持 TCP 和 HTTP、DNS 协议检测
- 支持 C&C IP 和域名白名单

IP 信誉库

- 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。
- 定期 IP 信誉特征库升级更新

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 HTTP、FTP、SMTP、POP3 协议文件传输的识别
- 支持配合 SSL Proxy，对 HTTPS 传输的文件进行过滤
- 支持近百种主流文件类型的特征码及后缀名双重识别
- 支持对网页关键字、Web 外发信息、邮件等内容进行过 滤
- 支持新浪微博、微信 UID 和 QQ 虚拟身份的识别及相关上 网行为的审计记录

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，支持自定义 URL 类别
- URL 特征库支持远程或者本地升级，支持手动和自动升级两种方式

带宽管理

- 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
- 对多层级管道进行最大带宽限制、最小带宽保证、每 IP 或每用户的最大带宽限制和最小带宽保证
- 基于时间和优先级的差分服务，支持带宽均分策略
- 对剩余带宽根据优先级进行弹性分配
- 主动抑制服务器端传送流量
- 支持 URL 分类的流控控制策略
- 支持针对每 IP 或每用户进行延迟限速

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，可针对目的地址或子网实时探测链路质量状况
- Inbound 相关功能支持 SmartDNS（支持 DNS A 记录解析）、支持动态探测
- 可根据带宽占用及时延自动进行链路切换
- 支持通过 ARP、PING、DNS 等方法来检测链路状态

服务器负载均衡

- 支持服务器健康检查和服务器会话保护、支持会话保持
- 支持加权哈希、轮询、最小会话数等算法
- 支持服务器会话状态的监控

VPN

- 支持 IPSec VPN 及创新的 PnPVPN
- 支持 SSL VPN 及 TLS1.2(可选 USB-key)
- 支持 L2TP、GRE 协议
- 支持 IKEv2 协议
- 支持 Xauth 协议
- 支持 OCSP 和 SCEP 协议
- 支持 Android、iOS 等移动设备的安全接入
- 支持国家商用密码算法 SM1/SM2/SM3/SM4

IPv6

- 访问控制
- ND 攻击防护
- 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
- URL 过滤
- 防病毒
- iQoS
- 支持 DNS、DNS64
- Track 地址探测
- IPS 攻击防护

高可用性 (HA)①

- 主/主模式 (A/A) 和主/备模式 (A/P)
- 支持配置、会话同步
-

虚拟系统 (VSYS)②

- 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 功能
- 支持监控统计
- vsys 支持描述文件

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
- 支持自定义监控
- 支持设备并发连接
- 支持设备 CPU、内存、温度等状态监控
- 支持 QoS 两层策略管道实际流量处理情况监控，支持多个时间粒度，Top50~Top300 的不同方向、不同策略的管道流量查看
- 支持 iQoS 管道策略实际流量情况监控，支持子管道叠加情况监控
- 支持链路状态监控，可查看指定应用/应用组详情，支持选择多条链路进行对比分析
- 支持通过 netflow v9 进行流量信息采集和外发

山石云•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
- 支持报表功能和云端存储，可自定义报表模板及生成计划
- 支持将设备日志上传云端进行存储，可按条件查询
- 支持手机 APP、WEB 访问方式

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
- 支持 IP、管控规则、接入终端数、状态等条件过滤查询监控结果
- 支持对超限 IP 进行日志记录、干扰操作
- 支持自定义干扰操作后重定向页面显示内容
- 支持对超限 IP 进行阻断操作

流量配额

- 支持对用户/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
- 用户已使用流量支持手动清理和到期自动清理

视频管控③

- 支持识别 IP 摄像头、网络视频录像机等各类网络终端
- 支持终端类型、IP、终端状态等条件过滤查询终端监控结果
- 支持自定义准入名单，对接入的终端进行管理

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
- 支持通过 UDP、TCP、Secure-TCP 协议进行日志传输

注：①C1200W 不支持②C1000、C1200W、C1300 型号不支持③仅 C1000、C2000、C4100、C5450 支持

关键指标

指 标	SG-6000-C1000
	
防火墙吞吐量（最大）	300Mbps
IPSec吞吐量(1)	100Mbps
防病毒吞吐量(2)	50Mbps
IPS吞吐量(3)	150Mbps
最大并发连接数	10万
每秒新建连接数	10,000
IPSec隧道数	512
SSL VPN用户数（最大）	标配100个（128）
管理接口	1个CON口，1个USB2.0口
网络接口	9个千兆电口
扩展模块槽	NA
扩展模块选项	NA
电源规格	整机功率30W，单交流电源
电源输入范围	交流：100-240V 50/60Hz
防雷击浪涌等级(4)	四级
产品形态	桌面型
外形尺寸（WxDxH,mm）	320.0mm x150.0mm x44.0mm
重量	1.5KG
工作环境温度	0-40°C
工作环境湿度	10-95%(不结露)

除非另有说明，否则所列出的性能，容量和特性是基于 StoneOS®5.5R7 的系统，实际结果可能会因 StoneOS®版本和部署情况而异。

注：(1) IPSec 吞吐量是用 Pre-shared key+AES256+SHA-1，用 1,400 字节数据流测试所得;

(2) 防病毒吞吐量根据带附件的 HTTP 流量测试所得；

(3) IPS 吞吐量是使用 HTTP 流量，在启用所有 IPS 规则，并打开双向检测的条件下测试所得；

(4)测试标准国家标准 GB/T17626.5-2008 及国际标准 IEC61000-4-5。

文档编号：HS-NGFW-C -5.5R7-CH-202001-V1.0

官方微信　　官方微博

中国·销售与服务热线： 400-828-6655