山石网科下一代防火墙

SG-6000-C1300

山石网科下一代防火墙 C1300 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 C1300 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，山石网科下一代防火墙 C1300 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 C1300 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 C1300 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支持深度应用识别技术.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丰富的用户认证方式，包括TACACS+、RADIUS、LDAP 等外部服务器用户认证，以及本地认证、web 认证等。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。
- 文件传输管控。结合文件深度检测技术，实现基于文件类型、文件大小、文件名称的文件传输控制，满足企业文件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C1300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。
- 专业的Botnet过滤功能。通过专业的僵尸主机地址以及Botnet外网恶意伺服器IP地址的过滤，从根本上阻断僵尸网络向机构内网的渗透，有效抵御僵尸网络的威胁。
- 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C1300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C1300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
- 支持应用类别、风险等级等多维度的应用定义
- 多达几千种的应用特征库
- 应用特征库支持网络实时更新

用户认证

- 支持本地用户认证
- 支持外部服务器用户认证(RADIUS、LDAP、MS AD)
- Web 认证
- 802.1X
- 支持 MS AD 用户组同步
- 支持 Web 认证后的 SSO

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

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
- 强大的 NAT 及 ALG
- 防火墙策略重复与冗余规则检测

攻击防护

- 多种畸形报文攻击防护
- 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 7000 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 130 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
- 支持 HTTP、HTTPS、SMTP、POP3、IMAP4、FTP 等协议
- 支持 APK、JAR、MS-OFFICE、PDF、SWF、RAR、ZIP 等文件类型的检测
- 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
- 对判定为恶意的文件提供完整的文件行为分析报告
- 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

Botnet Filter

- 支持专业的僵尸主机地址、Botnet 外网恶意伺服器 IP 地址的过滤

文件传输管控

- 支持基于文件类型、文件大小、文件名称进行文件传输安全控制

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
- 支持自定义 URL 类别
- 支持千万级 URL 特征库，URL 库支持网络实时更新

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

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

IPv6

- 访问控制
- IPsec VPN
- ND 攻击防护
- 隧道、DNS64/NAT64 等多种过渡技术
- IPv6 路由（静态路由、RIPng、OSPFv3、BGP4+）

高可用性（HA）

- 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）

- 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

监控统计

- 支持 URL、NAT、会话、威胁日志等
- 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；支持云应用的多维统计监控

云·景

- 支持将设备注册到山石云·景云服务平台
- 通过手机 APP、Web 方式实时集中监控多台设备状态、网络流量、网络攻击等，及时获知告警信息
- 报表生成及云端保存
- 日志云端托管

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 9 种操作系统
- 支持 IP 及终端接入数的条件过滤

关键指标

指标	SG-6000-C1300
	
防火墙吞吐量（最大）	1Gbps
IPSec 吞吐量(1)	600Mbps
防病毒吞吐量(2)	300Mbps
IPS 吞吐量(3)	400Mbps
最大并发连接数	36 万
每秒新建连接数(TCP)	12,000
每秒新建连接数(HTTP)	10,000
IPSec 隧道数	1,000
终端安全管理用户数（最大）	500
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
SSD 存储	无
电源规格	单 45W，可选双冗余
电源输入范围	交流 100-240V 50/60Hz，直流-40V~-60V
防雷击浪涌等级(4)	四级
产品形态	1U
外形尺寸(W×D×H, mm)	442.0mm×241.0mm×44.0mm
重量	2.5kg
工作环境温度	0-40℃
工作环境湿度	10-95%(不结露)

注：除非另有说明，否则所列出的性能，容量和特性是基于 StoneOS®5.5R4 的系统，实际结果可能会因 StoneOS®版本和部署情况而异。

(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。