山石网科下一代防火墙

SG-6000-E3965

山石网科下一代防火墙 E3965 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 E3965 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”，山石网科万兆高端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 E3965 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

精细化应用管控

山石网科下一代防火墙E3965支持深度应用识别技术，可根据协议特征、行为特征及关联分析等，准确识别数千种网络应用，其中包括400余种移动应用。并且，可支持SSL加密流量的应用识别。在此基础上，E3965为用户提供了精细而灵活的应用安全管控功能。

- 应用多维可视化及风险分析。除应用所在分类外，用户可了解到包括应用背景信息、应用风险级别、潜在风险描述、所用技术等详尽信息，如该应用是否大量消耗带宽、是否能够传输文件、是否存在已知漏洞等等。通过多维度的详尽应用分析，用户可制定针对性的安全策略以避免特定应用威胁网络安全。
- 精准应用筛选。E3965提供了精细化的应用筛选机制。用户可根据应用名称、应用类别、风险级别、所用技术、应用特征等6大条件，精确筛选出感兴趣的应用类型，如具备文件传输功能的通讯软件，或存在已知漏洞、基于浏览器的WEB视频应用等等，从而实现精细化的应用管控。
- 灵活应用控制。基于深度应用识别及精细化的应用筛选，E3965支持灵活的安全控制功能。包括策略阻止、会话限制、流量管控、应用引流或时间限制等。如山石网科下一代防火墙支持的iQoS技术，可在应用识别与用户识别基础上 ,进行两层八级细粒度流量管控 ,保证用户重要应用服务质量，提升网络带宽利用率。

全面威胁检测与防护

山石网科下一代防火墙E3965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。
- 高性能的病毒过滤功能。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。

强大的网络适应性

山石网科下一代防火墙E3965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。
- 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。
- 支持虚拟防火墙技术。可将一台物理防火墙在逻辑上划分成多个虚拟防火

墙，每个虚拟防火墙拥有独立系统资源和独立配置管理平台，可根据不同业务系统的安全需求为不同租户提供专属安全防护，还可对租户间互访的东西向流量进行安全隔离和策略防护。

全并行高性能安全

山石网科下一代防火墙E3965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性能，其高吞吐、低延时、高并发等高性能优势，可为用户带来更快速的安全体验。

- 一次解析，并行检测。山石网科下一代防火墙采用单次报文解析技术，报文经一次解包后，由各个安全模块并行检测。有效保障在开启多种威胁防护功能时的综合安全性能。
- 全并行软硬件架构。山石网科下一代防火墙基于多核硬件处理架构和拥有自主知识产权的64位操作系统StoneOS，实现软硬件全并行操作。专有算法可在每个CPU核上处理所有安全功能，并可将会话负载均分到所有内核，实现最优化的多核并行处理。

安全审计与集中管理

山石网科下一代防火墙E3965支持系统日志、配置日志、流量日志、攻击日志及会话日志等类型日志的海量信息记录，可配合高效的山石网科 HSA安全审计平台，为用户提供上网访问行为的监管和审计，满足公安部82号令及上级单位合规性监管要求。

山石网科下一代防火墙E3965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。

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
- 支持识别加密流量并阻断不可信流量
- 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 / 角色的安全策略
- 丰富的路由特性
- 强大的 NAT 及 ALG

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

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

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)、支持动态探测
- 可根据带宽占用及时延情况自动进行链路切换
- 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、加权轮询、加权最小会话数等算法
- 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 (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
- 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 日志、NAT 日志、会话日志、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

关键指标

指标	SG-6000-E3965
	

防火墙吞吐量（最大）	12Gbps
IPSec 吞吐量(1)	6Gbps
防病毒吞吐量(2)	3Gbps
IPS 吞吐量(3)	4Gbps
最大并发连接数	600 万
每秒新建连接数(TCP)	17 万
每秒新建连接数(HTTP)	12 万
IPSec 隧道数	10,000
SSL VPN 用户数（最大）	8,000
管理接口	1 个 CON 接口，1 HA 口，1 MGT 口，1 个 USB 口，1 个 AUX 口
网络接口	4 个千兆电口（含一对 Bypass 接口）、4 个 SFP 口、4个万兆 SFP+口
扩展模块槽	3 个通用扩展槽
扩展模块选项	IOC-4GE-B-M、IOC-8GE-M、IOC-8SFP-M、IOC-2XFP-Lite-M、IOC-4GE-POE、IOC-4SFP+、IOC-8SFP+
电源规格	双冗余热插拔电源，450W
电源输入范围	交流：100-240V 50/60Hz　直流：-40 ~ -60V
防雷击浪涌等级(4)	四级
产品形态	2U
外形尺寸(W×D×H, mm)	440.0mm × 530.0mm × 88.0mm
重量	11.8kg
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®5.5R1 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。

扩展模块

指标	IOC-4GE-B-M	IOC-4GE-POE	IOC-8GE-M
			
名称	4GE Bypass 千兆电口扩展模块	4GE POE 千兆电口扩展模块	8GE 千兆电口扩展模块
网络接口	4 端口千兆电接口 含 2 对 Bypass 接口	4 端口千兆电接口 支持 POE 供电功能	8 端口千兆电接口
外形尺寸	半 U 高，占 1 个通用扩展槽	1U 高，占 2 个通用扩展槽	半 U 高，占 1 个通用扩展槽
重量	0.8kg	0.4kg	0.8kg

指标	IOC-8SFP-M	IOC-2XFP-Lite-M	IOC-4SFP+	IOC-8SFP+
				
名称	8SFP 千兆光口扩展模块	2XFP 万兆光口扩展模块	4SFP+万兆光口扩展模块	8SFP+万兆光口扩展模块
网络接口	8 端口千兆 SFP 接口，不含 SFP 模块	2 端口万兆 XFP 接口，不含 XFP 模块	4 端口万兆 SFP+接口 ,不含 SFP+模块	8 端口万兆 SFP+接口 ,不含 SFP+模块
外形尺寸	半 U 高，占 1 个通用扩展槽	半 U 高，占 1 个通用扩展槽	1U 高，占 2 个通用扩展槽	1U 高，占 2 个通用扩展槽
重量	0.9kg	0.9kg	0.7kg	0.7kg