山石网科云内部安全微隔离产品
——山石云·格

随着虚拟化技术的持续完善和发展，越来越多的用户正在逐步把业务迁移至公有云或私有云中。云计算在带来便捷、快速和灵活的同时，也带来了新的安全挑战。这些安全挑战已成为制约云计算发展的瓶颈，同时也阻碍关键业务向云中迁移。

- 云平台内部不可视，用户无法管控虚机上的流量和应用；
- 虚机之间缺乏威胁隔离机制，网络威胁一旦进入云平台内部，可以肆意蔓延；
- 云安全需要适应云平台的弹性扩展，能够动态部署和迁移。

山石网科在业界率先推出面向公有云及私有云的安全防护产品——山石云•格，帮助用户解决当前面临的云安全问题。山石云•格通过专利引流技术、虚机微隔离及可视化技术，能够为用户提供全方位的云安全服务，包括流量及应用可视化，虚机之间威胁检测与隔离，网络攻击审计与溯源等，帮助政府、金融、运营商、企业等搭建安全、合规的“绿色”云平台。

山石云•格是一款软件产品，以虚拟机的形式部署在云平台中，山石云•格产品的管理平面、控制平面、业务平面采用分离式设计，由 vSOM、vSCM、vSSM 三部分组成。vSOM 虚拟安全管理模块为管理平面，负责管理整个云•格产品安全服务生命周期。vSCM 虚拟安全控制模块为控制平面，负责安全配置管理，以及对业务平面进行调度。vSCM 通常采用冗余部署，可避免单点故障，提高云•格产品可靠性。vSSM 虚拟安全业务模块是业务平面，负责执行具体安全功能，如访问控制，攻击阻断等，在每一台需要保护的物理服务器部署一个 vSSM 即可实现对该物理服务器上所有虚拟机的安全保护。

产品亮点

实时流量深度可视

山石云•格能够收集并分析虚机之间的数据通信，帮助用户描绘出整个云平台上的流量模型，包括虚机之间以及不同端口组 (port group) 之间的的流量情况。同时，山石云•格还可为用户呈现云平台中的指定时间段内的新增流量及新增应用，帮助用户洞察云平台内部的细微变化。

借助山石网科深度可视技术，山石云•格可识别出虚机流量中的具体应用类型，并在此基础上提供了流量与应用控制功能，可对虚机间的业务访问进行细粒度的权限控制，以过滤非法访问，保护业务安全。

阻止攻击横向蔓延

现有云平台产品并没有为东西向流量提供威胁检测与隔离机制，因此一旦某台虚机被攻陷，整个云平台都岌岌可危。山石云•格提供的“虚机微隔离”技术为每个虚机提供了“贴身保镖”式的安全防护，通过专利引流技术，山石云•格可将每个业务虚机的流量牵引至虚拟安全业务模块 vSSM，进行 2-7 层的威胁检测，从而发现并阻断东西向流量的安全威胁，阻止攻击在云平台内横向蔓延。

产品亮点

云环境适应性

山石云•格支持 VMware 等当前主流的云平台技术，并与这些平台无缝融合。其全虚拟化的设计方式使山石云•格可随云平台的伸缩同步实现弹性扩展。在管理方式上，山石云•格支持统一集中管理，用户通过单一管理界面即可实现整个云平台的统一安全部署和管理。

山石云•格支持虚拟机迁移技术 (vMotion)，在虚机迁移至其他物理主机时，安全策略可随虚机同步迁移，无需人工干预，实现动态的实时安全防护。

降低部署及运维成本

山石云•格采用分离式设计，由 vSOM、vSCM、vSSM 三大虚拟模块组成，这些虚拟模块均以虚机的形式提供，基于云平台的模板分发机制，山石云•格可实现快速、高效部署。同时，山石云•格基于透明二层模式，用户无需更改虚机当前网络配置，即可实现山石云•格产品部署，不影响当前业务运行。山石云•格采用自主研发的专利引流技术，不依赖于云平台私有 API 接口，对 VMware 用户而言，无需购买 VMware NSX 产品即可实现山石云•格的所有安全功能。

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

可视化

- 支持虚拟机资产发现、支持对流量、应用、威胁的统计
- 支持对接入服务的虚拟机进行全方位的网络监控
- 支持会话日志、威胁日志、系统日志等
- 以逻辑拓扑图的方式展示可视化效果

防火墙

- 基于深度应用识别的访问控制
- 支持ALG
- 支持会话限制

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、NETBIOS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

部署模式

- 支持透明串接和旁路模式部署、无需改变现有的虚拟机配置和网络结构
- 通过vSSM提供安全服务、服务容量可随用户需求增长而扩展
- 用户的虚拟机可被随时加入或者移出安全服务
- 统一系统管理

高可用性 (HA)

- 支持双主控
- 管理平面 (vSOM)、控制平面 (vSCM)、安全业务平面 (vSSM) 完全分离，保障业务稳定运行
- 单块vSSM出现故障后对整机无影响、接入该vSSM的虚拟机业务自动脱离

自动化适应

- 支持虚拟机的vMotion
- 支持动态地址簿，实现基于虚拟机的访问策略

虚拟化平台

- 支持VMware

关键指标

山石云 · 格

指 标	山石云 · 格
防火墙吞吐量	1Tbps
最大并发连接数	3.4 亿
每秒新建连接数 (HTTP)	600 万
IPS 吞吐量	200Gbps
最大支持 vSSM 数量	200

vSSM (虚拟安全业务模块)

指 标	vSSM
防火墙吞吐量	5Gbps
最大并发连接数	170 万
每秒新建连接数 (HTTP)	3 万
IPS 吞吐量	1Gbps

除非另有说明，否则所列出的性能，容量和特性是基于运行StoneOS®5.5R1的系统，实际结果可能会因StoneOS®版本和部署情况而异。

注:

(1) 所有性能数据均是在VMware环境下测试得到的数据。

(2) 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。