

# 山石云·界

## 山石网科云安全虚拟下一代防火墙

随着云计算、NFV、虚拟化技术的高速发展，越来越多的应用与用户业务运行在云计算环境中，但随之而来的安全防护问题却使传统的网络安全架构无法有效应对。山石云·界是专门为云计算环境设计的虚拟化网络安全产品，内嵌山石网科 StoneOS 网络防火墙专用操作系统，以虚拟机形态部署，适用于云计算环境，为用户提供不同安全等级应用之间的安全隔离和安全防护。产品支持精细化应用识别、VPN、入侵防御、病毒过滤、负载均衡等功能，具备快速部署能力，即可为公有云租户提供安全防护，又可为中小企业私有云用户提供高性价比的防护方案，能够降低客户初始采购和管理维护成本。

## 产品亮点

### 具有全面适应能力的软件防火墙

在云计算环境中，用户的计算、存储、数据资源都是运行在服务器的虚拟机上，在考虑安全防护的设计时，山石云·界可在虚拟机上实现快速灵活的部署，支持在 VMware、KVM、Hyper-V、XEN 等主流虚拟化监视器上运行，可串联或单臂连接到虚拟网络中（如：虚拟应用服务器前端的网关，或者是 VPC 网络的边界网关），为虚拟网络或应用提供专业的边界网络安全防护功能。

以虚拟机形式部署设备，能够克服物理防火墙的限制，在云计算环境中可部署于更加靠近 VM 的位置，对于 VM 主机内部流量进行过滤，实现同时对于南北向和东西向流量的安全防护。同时，用户可以根据网络搭建需求，弹性调配和管理网络资源等，并且能够按需进行灵活迁移，充分发挥云计算优势。

### 拥有专业 NGFW 安全防护功能

山石云·界云计算防火墙拥有与 NGFW 相同的操作系统，具有丰富的网络安全防护功能，对网络威胁进行防御，能够满足企业分支及公有云多租户环境中的网络安全需求。

- 具备精细化应用管控，可为用户提供多维的应用风险分析和筛选，以及灵活的安全控制，包括策略阻止、会话限制、应用引流和智能流量管理等。同时，还具备入侵防御、病毒过滤、攻击防护、链路与服务负载均衡、NAT 等功能，满足客户对安全访问，攻击防护以及应用识别和控制等需求。

- 具备 VPN 接入能力，包含 IPSec VPN、SSL VPN、L2TP VPN，可与物理防火墙或云计算防火墙建立安全加密隧道，确保数据的远程安全传输。可为网络管理员提供远程后台管理的安全访问通道，也可为混合云的组建提供安全、可靠，性价比高的安全互联通道。
- 具备 HA 组网能力，满足配置和会话同步的要求，从而实现高可靠的冗余部署，保障用户业务的不间断连续运营。

### 结合云计算特性的云原生特点

在云计算环境中，云平台自身提供了多种技术手段，来提高整体系统的稳定性，扩展性，并可以提高性能，这些技术手段与云计算环境密切相关，并且更具有云原生特点，领用这些技术特性解决特定的问题，会更加适应云环境。

山石云·界通过与云计算平台的紧密结合，云平台监控设备的运行状态，当性能不足时，可通过增加虚拟化设备或提高设备使用的虚拟机资源，实现设备的弹性伸缩，保障业务网络不遇到性能瓶颈。

一般虚拟机在云平台上，都会通过快照、迁移等方式，保障虚拟机的稳定性，并提高虚拟机故障的快速恢复能力。山石云·界通过对虚拟化环境的高度适配，可通过快照技术，快速的进行备份和故障恢复；通过迁移技术，保障设备运行的资源合理分配。

山石云·界通过对平台的增强感知，利用 DPDK, SR-IOV, CPU Pinnig, Huge Pages 等技术，可以在资源相同的情况下，提高整体的处理性能，更加充分而合理的利用云计算资源。

## 提供多种自动化部署方案

山石云·界适合在公有云和私有云中部署，可为公有云和私有云客户提供自动化的网络安全解决方案，抵御外部的网络攻击。借助云计算的优势特性，山石云·界可按需自动化部署和扩展安全服务资源，并可与现有的云计算管理平台进行紧密整合，将管理和安全防护能力直接深入到云计算架构中，可伴随着客户或虚拟业务资源的需求增长和缩减。

可为具有开发能力的客户提供完成初始化部署的方案，并提供二次开发对接接口；可为 OpenStack 的客户 提供替换原生 vRouter 以及 FWaaS 的整体交付方案；可为致力于方案解耦的客户 提供符合国际化标准的开源开放 NFV 集成方案。

更多方案相关详细内容，可登录山石网科 NFV 站点：[nfv.hillstonenet.com.cn](http://nfv.hillstonenet.com.cn)，下载《基于 NFV 构架的自动化部署与编排白皮书》或其他方案文档。

公有云 Public Cloud



私有云 Private Cloud  
社区云 Community Cloud  
区域公有云 Regional Public Cloud



虚拟机监视器 Hypervisor



## 产品功能

### 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、风险等级等多维度应用定义
- 支持多达几千种的应用特征库
- 应用特征库支持网络实时更新

### 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
- 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
- 支持通过netflow v9进行流量信息采集和转发
- 支持报表功能
- 支持日志本地存储

### 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、MSAD)
- 支持AD/LDAP用户/组织结构同步
- 支持Web认证
- 支持基于MAC的用户认证
- 支持MS AD用户组同步
- 支持Web认证后的SSO

### 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
- 全面的DNS策略
- 强大的NAT及ALG
- 策略自学习
- 垃圾策略检测与清理

### 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
- 支持缓冲区溢出、SQL注入和跨站脚本攻击的检测和防护
- 支持专业的Web Server防护功能，含CC攻击防护和外链防护等

### 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等几十种协议和应用的攻击检测和防御
- 支持自定义入侵防御特征
- 提供预定义防御配置模板
- 提供几千种特征的攻击检测和防御，特征库支持网络实时更新

### 病毒过滤

- 基于流、低延时、高并发、高性能的病毒过滤
- 支持大病毒文件的扫描
- 实时病毒连接阻断，病毒事件记录
- 支持常见病毒传输协议 HTTP、FTP 及各种邮件协议扫描
- 超千万级的病毒特征库，病毒库可以在线更新、本地更新

### 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

### 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

### 云沙箱

- 支持SMTP、POP3、IMAP4、FTP等协议类型的检测。
- 支持APK、JAR、MS-OFFICE、PDF、SWF、RAR、ZIP等文件类型的检测
- 对PE文件在上传云沙箱前进行文件可信证书检测
- 在云沙箱配置中新增全局、profile、预定义及自定义等配置选项
- 独立出沙箱日志类型展示、支持行为报告PDF文件导出

### 终端接入管控

- 支持跨三层识别接入网络终端数
- 支持识别Window、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

### 页面访问控制

- 基于角色、时间、优先级、页面类型等条件的Web网页访问控制
- 支持自定义URL类别
- 支持千万级的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的带宽限制和保证
- 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
- 支持针对每IP或每用户进行延迟限速
- 基于时间和优先级的差分服务，支持带宽均分策略

### 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\L2TP VPN 及创新的 PnP VPN
- 支持 SSL VPN 及 TLSv1.2( 可选 USB-key)
- 支持IKEv1,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

### 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

### 高可用性 (HA)

- 主/备模式 (A/P)
- 支持配置、会话同步
- 支持128组HA数量
- 支持接口使用真实MAC
- 支持修改虚拟MAC地址
- 支持HA同步协商使用单播模式
- 支持HA协议号修改
- HA心跳接口设置MTU
- 阿里云支持HA
- 华为云支持HA
- 腾讯云支持HA
- AWS支持HA

### 支持山石云·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

### 授权管理

- 支持迁移，重装时，不更换授权文件
  - 支持公网授权验证方式
  - 支持内网授权验证方式
  - 支持授权自动分发
  - 支持授权回收、授权调度。
- 注：更多授权管理功能细节，可参考《许可证管理系统产品介绍文档》

### 配置注入插件

- 支持VMware Tools
- 支持Cloud-Init (Restful|Config Drive)
- 支持Qemu Guset Agent

### 增强平台感知

- 支持CPU Pinnig
- 支持Huge Pages
- 支持DPDK
- 支持SR-IOV (82599|X710|XL710)

### 虚拟化监视器

- 支持VMware Hypervisor
- 支持KVM Hypervisor
- 支持Xen Hypervisor
- 支持Hyper-V Hypervisor (Gen1)

### 公有云云市场

- 阿里云AliCloud
- 亚马逊AWS
- 微软云Azure
- 华为云Hwclouds
- 腾讯云Qcloud

### 云平台

- OpenStack L版本及以上
- VMware vCenter 5.5版本及以上
- EasyStack ESCloud
- FitTelecom Cloud
- Huawei FusionSphere
- Inspur InCloud Platform
- ZTE iROS
- 99Cloud Animbus

### REST API

- 登录/登出
- iCenter监控查询
- 应用/设备/用户/威胁监控、监控配置
- 日志配置/管理
- 对象配置
- 策略配置
- 网络配置
- 系统配置
- 特征库数量/升级

## 山石云·界——相关规格参数

产品名称	VM01	VM02	VM04
支持核数(最小)	2vCPU	2vCPU	4vCPU
内存(最小)	2G	4G	8G
硬盘(最小)	4GB	4GB	4GB
接口总数	10	10	10
最大并发会话数	100K	500K	5M
IPSec VPN 隧道数	100	500	10000
SSL VPN 用户数(标配/最大)	5/100	5/500	5/2000
防火墙吞吐量(虚拟网卡/SR-IOV)	2Gbps/10Gbps	4Gbps/20Gbps	8Gbps/30Gbps
IPS吞吐量(虚拟网卡/SR-IOV)	1Gbps/3Gbps	2Gbps/5Gbps	4Gbps/7Gbps
AV吞吐量(虚拟网卡/SR-IOV)	800Mbps/1Gbps	1.6Gbps/2Gbps	3.2Gbps/4Gbps
每秒新建连接数(虚拟网卡/SR-IOV)	20K/30K	40K/50K	80K/100K
IPSec VPN吞吐量(虚拟网卡/SR-IOV)	200Mbps/400Mbps	400Mbps/800Mbps	800Mbps/2Gbps

注：性能数据与实际使用的虚拟网络以及系统配置相关，最终性能数据以实际测试为准。本表内的性能数据是基于戴尔R720服务器(Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.70GHz, 64GB内存, 4x10 GE(82599ES)网卡)，并基于StoneOS 5.5R6版本测试。虚拟网卡是VMware环境下的VMXnet3, SR-IOV是KVM环境下的数据。

Copyright © 2019, 山石网科版权所有，保留所有权利。

Hillstone、Hillstone Networks 标识、山石网科、StoneOS、StoneManager、Hillstone PnPVPN、UTM Plus 均为山石网科所属商标。

所有其他商标和注册商标均为其各自公司的财产。

本文所包含信息可能会有所修改，恕不另行通知，如需最新信息请浏览山石网科网站 (www.hillstonenet.com.cn)

文档编号: EX-08.01-SG-VM-5.0-Y19M06-CH-08



官方微信



官方微博

中国·销售与服务热线: 400-828-6655