Hillstone
山石网科

基于OpenStack的一体化安全编排方案

一、概要

云计算是通过使计算分布在大量的分布式计算机上，而非本地计算机或远程服务器中，企业数据中心的运行将与互联网更相似。这使得企业能够将资源切换到需要的应用上，根据需求访问计算机和存储系统。

云计算目前已经成为当前计算，存储，网络技术的核心基础技术之一，云计算随着云计算的快速发展，更多的客户选择部署自己的私有云或专有云，同时，很多传统的IDC或运营商在向云服务商转型，为了部署云环境，客户目前有两种选择，使用商用产品，比如VMware或者CloudStack等，也可使用开源产品，比如，OpenStack。

过去，很多客户选择商业产品作为自身云计算的技术支撑，而今，更多的客户开始选择使用开源产品来做技术支撑，开源产品可以给客户提供更多定制化功能，满足客户的日新月异的需求变化。由于OpenStack在云计算领域发展的如日中天，因此，使用OpenStack作为客户云计算的技术支撑，已经成为客户的不二选择。

二、需求及挑战

OpenStack作为当今最炙手可热的开源项目，从各方面都已经接近商业产品，然而在OpenStack提供的一些网路和安全功能，依旧与客户实际需求有所差距。

2.1 面向租户的自服务

OpenStack作为一个云平台，本身就是以租户为基础，提供面向租户的各项服务，因此所有功能都需要是面向租户级的。

所谓面向租户级，就是要求某一个功能是为单独一个租户提供，而不是所有租

户共享，这里其实包含两个概念，一是让功能为每个租户提供独立的配置权限，二是要求租户具有独立的管理权限，即添加，修改，查询，删除功能或功能配置，对其他租户的同类功能不能产生任何影响。

同时，租户可以在自主意愿下进行自动化的开启或部署，而不需要云平台管理员进行管理或配发。

2.2 三层虚拟私有云

虚拟私有云（VPC，Virtual Private Cloud），也有称之为虚拟专有网络，为很多租户提供类似与传统网络的局域网一般的服务和组网，而存在多个类别的业务虚机时，租户往往需求将多个类别的业务虚机分布在不同的子网中，因此需要使用支持三层的VPC网络，需要使用OpenStack的vRouter来做三层VPC的网关路由，然而OpenStack的源生vRouter是逻辑路由，不论功能性，还是稳定性，都存在一些问题，因此，没有办法很好满足客户的需求，所以使用VNF方式的vRouter就是解决这个问题的一种方式。

2.3 安全防护

很多客户需要进行安全防护，而OpenStack源生的FWaaS（Firewall-as-a-Service）服务，可以为业务虚机设置安全控制策略，OpenStack毕竟不是专业的安全软件，所提供的安全功能也仅是基于五元组的访问控制，也就是如今常说的传统防火墙的功能，而如今网络上流行的攻击和入侵，大部分都是基于应用层，所以要完成对当今的攻击和入侵的防护，至少要实现应用层的安全控制。

除了基本的安全控制，租户的攻击防护，入侵防护以及病毒防护等更高级的安全防护功能，更需要通过其他产品的高级功能来实现防护。

2.4 统一管理风格

租户使用OpenStack进行业务虚机的管理和维护，对OpenStack的管理界面与管理风格已经形成了一种使用习惯，因此在增加新增功能时，如果可以和OpenStack的页面风格和配置方式兼容或接近，租户接受起来会更加容易。

所以将配置管理与OpenStack的页面进行对接和集成，对租户提供统一的管理风格，可以大大增加租户的接受程度和体验。

三、解决方案

在OpenStack环境中，通过山石网科的HillstoneNetworks-L3-agent或HillstoneNetworks-FWaaS-driver，可在OpenStack上创建vRouter或启用FWaaS时，调用对应的山石网科插件，来启动山石网科的虚拟化下一代防火墙（云•界）来作为功能承载，而不再是使用OpenStack自带的逻辑vRouter和基于iptables的FWaaS。

通过OpenStack的插件与VSOM进行通讯，租户在OpenStack的Horizon页面上启用三层VPC创建vRouter时，会自动创建山石网科的VNF，承载vRouter的功能，当在OpenStack界面上进行

vRouter的配置和管理时，会直接配置在山石云•界上；当通过OpenStack界面上的FWaaS进行安全策略配置时，会直接配置到云•界上，实现基于应用的安全访问控制。

Figure 1 OpenStack下插件安装替换效果图

这样，通过基于OpenStack插件方案，沿用了OpenStack的vRouter以及FWaaS的服务创建流程，并可通过OpenStack的Horizon页面进行管理和配置。在对OpenStack改动最小的情况下，实现最快最平滑的替代和集成，并实现自动化部署。

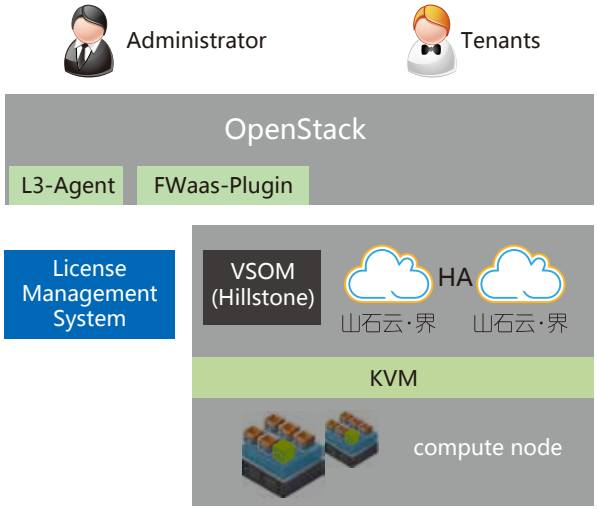

Figure 2 基于OpenStack插件的编排方案构架图

3.1 自动化部署及统一界面配置

进行云•界的部署，完全由OpenStack的页面进行触发，云•界的部署和启动完全实现自动化，同时在云•界启动后，可实现初始配置的注入以及自动化授权开通业务，后期的策略配置和子网添加完全通过OpenStack的Horizon页面，无需OpenStack的二次开发和对接。

3.2 解决三层VPC可用性

山石云•界提供多种路由功能，包括多种静态路由，动态路由以及策略路由，其功能性远超OpenStack源生的逻辑路由；同时，云•界已独立虚机运行，性能和稳定性相对OpenStack源生的逻辑路由得到了大大的提升，并且成本和部署难度远低于分布式路由。

从而即解决了OpenStack源生逻辑路由的功能性、稳定性和性能，同时，又比分布式路由的部署成本和部署要求更低。

3.3 提高网络安全防护等级

山石云•界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、链路与服务器负载均衡等功能，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，为租户提供更多更高级的安全防护功能。

3.4 授权分发

授权服务器是山石网科为配合云•界自动化部署而研发的独立产品，通过授权服务器，当云•界启动同时需要开通业务时，会连接授权服务器，授权服务器通过配置好的策略，为连接上来的云•界分配授权；当云•界需要响应业务需求而进行调整或关闭时，授权服务器可将此云•界的授权进行回收，并在其他云•界需要时进行重新分配。

这样通过授权服务器，在云•界进行业务开通、调整和关闭时，云•界的授权也可以进行分发和回收，实现真正的随业务调整。

3.5 REST API

REST是目前非常流行，使用非常便捷的一种接口风格，主流的云平台厂家（比如，AWS，Azure，OpenStack等）都支持使用REST风格的接口为用户提供对接和开发。

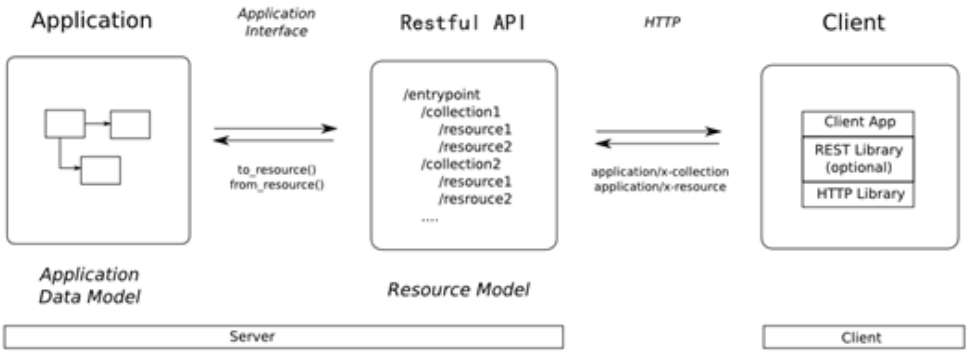

Figure 3 REST API逻辑原理（图片来自网络）

山石云•界为了与云管理平台或其他管理软件进行集成或协同，已支持通过RESTAPI对云•界进行管理和配置。通过RESTAPI，云平台厂家可以将一些高级配置下发到云•界上，同时，也可以通过统一风格的portal页面为用户/租户提供自管理服务。

目前山石网科已支持系统设置，策略下发，接口及网络等基本功能配置已提供标准REST API。

Figure 4 山石网科REST API手册部分截图

四、方案优势

4.1 易交付

方案可在OpenStack环境整体交付，无需第三方开发或对接，即可实现自动化部署以及基于租户的自服务，不依赖任何第三方中间件，支持开源社区版本的OpenStack，并将山石插件开源，可供有需求的客户进行二次开发，实现高级功能。

4.2 稳定性

使用山石云•界做VPC的vRouter，大大提高了vRouter的功能性及稳定性。

每个租户的vRouter都为一个或一组HA的山石云•界，每个租户的设备独立，所有租户可根据自身需求进行创建和修改，单个租户的山石云•界出现问题可进行HA切换，即便HA出现问题，受影响面也为单个租户，不会对其他租户造成不良影响。

4.3 统一界面&逻辑

所有设备的创建和配置，完全依靠OpenStack的源生逻辑及配置界面，无需二次开发，与源生流程及配置界面完全兼容，符合租户的原始使用流程和配置方式，无需租户的二次学习和培训，即可了解创建和配置方法，大大降低了运维培训成本。

五、总结

在OpenStack环境中，当存在安全需求时，为了满足租户的自服务以及配置管理方便性时，很多方案都需要对OpenStack做二次开发或者对接开发，而通过山石网科基于OpenStack的一体化编排方案，在不需要云平台做任何二次开发的情况下，就可以实现租户的自服务，并且可以通过OpenStack源生页面进行配置管理，即使之前有做过界面的二次包装，也可以直接调用OpenStack的接口依然对接有效。

因此，在OpenStack环境中，山石网科的解决方案可以在最少开发，最快时间完成部署，同时满足自服务及界面集成需求，是云平台提供安全服务时的最佳选择。

文档编号：EX-08-CLOUD-5.5R2-0717-Ch-01