Hillstone NETWORKS

# 山石网科
# 虚拟云安全解决方案技术白皮书

山石云·格

www.hillstonenet.com.cn

## 面向虚拟化数据中心的软件定义安全

数据中心已经从物理架构演进到大规模虚拟和云的架构。服务器和存储被虚拟化成为很多数据中心的标准，新兴的网络功能虚拟化（NFV）和软件定义网络（SDN）技术有望通过虚拟化的网络和安全功能完成物理到虚拟的演进。

虚拟数据中心在效率、业务敏捷性，以及快速的产品上市时间上有明显的优势。然而，应用、服务和边界都是动态的，而不是固定和预定义的，因此实现高效的安全十分具有挑战性。传统安全解决方案和策略还没有足够的准备和定位来为新型虚拟化数据中心提供高效的安全层，这是有很多原因的。

## 从南北到东西

在传统数据中心里，防火墙、入侵防御，以及防病毒等安全解决方案主要聚焦在内外网之间边界上通过的流量，一般叫做南北向流量或客户端服务器流量。

在今天的虚拟化数据中心里，像南北向流量一样，交互式数据中心服务和分布式应用组件之间产生的东西向流量也对访问控制和深度报文检测有刚性的需求。多租户云环境也需要租户隔离和向不同的租户应用不同的安全策略，这些租户的虚拟机往往是装在同一台物理服务器里的。

不幸的是，传统安全解决方案是专为物理环境设计的，不能将自己有效地插入东西向流量的环境中，所以它们往往需要东西向流量被重定向到防火墙、深度报文检测、入侵防御，以及防病毒等服务链中去。这种流量重定向和静态安全服务链的方案对于保护东西向流量是效率很低的，因为它会增加网络的延迟和制造性能瓶颈，从而导致应用响应时间的缓慢和网络掉线。

## 负载移动性和可扩展性

静态安全解决方案在物理静态负载环境中是有效的。在虚拟化数据中心里，负载移动性和迁移是常态，那就意味着安全解决方案不仅也要具有移动性，还要能够感知负载的移动。而且它还得保持状态并对安全策略做出实时响应。要做到这一点，最好的办法就是通过与云管理平台（例如vCenter和OpenStack）紧密集成。

在虚拟化环境里，负载增大、减小和移动，以满足业务和应用的需求，安全解决方案的可扩展性和弹性显得尤为重要。固定静态的网关或服务器安全解决方案可以有效的工作在传统数据中心里，因为那里每台物理服务器的负载都是固定的。然而，移动弹性虚拟化数据中心需要能够跟被保护的环境一样弹性、可扩展，以及虚拟化的安全解决方案。这样能够确保它不会在一个地方成为瓶颈，过度的影响其它地方，而没有办法共享资源。理想情况下，安全服务应该一直工作在靠近负载的地方。

## 软件定义网络和网络功能虚拟化

任何虚拟化安全解决方案也必须融入以NFV和SDN为特点的新兴数据中心网络架构中。通过NFV，交换和路由功能由跑在X86服务器上的虚拟机来提供，而不再使用物理的路由器和交换机。SDN通过使网络平面和数据平面分离来提高网络的灵活性。

今天的大多数NFV实现的特点是分布式虚拟路由，这使每个租户拥有自己的虚拟路由器用于子网之间的通信。它将路由软件分布在网络中所有的虚拟交换机上，为高度移动负载环境提供可扩展的性能和策略执行。

## 用户急需解决的安全问题

在云环境中，某虚机由于某种原因中了病毒，从内部向其它虚机和外部网络发起端口扫描和DoS等攻击，缺少识控方案的情况下，只能将有问题的虚机从网络中移除，让问题虚机的管理员线下解决问题后，才允许连接回网络，这样的处理方案简单粗暴，虽然隔离了攻击，但也同时断掉了问题虚机的对外服务。

对于云环境，虽然外部可能部署入侵防御设施，但可能存在这样的情况，某虚机由于弱口令之类的漏洞被远程控制，然后黑客以此虚机为跳板，再对其它虚机进行漏洞扫描和利用入侵，DoS攻击会产生大量的会话，可能通过云管理平台发现，然而从内部发起的漏洞入侵的过程在网络层面上与正常访问无异，无法被发现，因此需要识控的方案。

## 当前虚拟化安全解决方案架构的局限

显然，传统的物理安全解决方案无法满足新兴虚拟化数据中心对安全性、性能、流量和移动性的需求。任何安全解决方案必须像它所要保护的数据中心一样，是虚拟、敏捷、弹性、移动和可扩展的。理想情况下，安全就应该作为另一个虚拟资源　池深度插入到数据中心的虚拟化环境中，随着计算、存储和网络资源池的增大、减小和迁移。就像虚拟路由器演进成分布式虚拟路由器一样，任何虚拟化网络服务必须能够以分布式的方式部署来满足虚拟化数据中心的需求。

### 今天的大多数虚拟数据中心安全解决方案使用以下两种架构之一：

第一个是给每个租户分配一个单防火墙虚机，同时解决南北向和东西向流量问题，允许每个租户有一套自己独立的防火墙策略应用。要无瓶颈或无计算资源浪费的满足平均和突发负载的需要，扩展单防火墙虚机的性能是一个挑战。管理大量有自己独立策略的不同租户的防火墙虚机也是一个很大的困难。

第二个是把防火墙功能插入到虚拟机管理程序层中。由于它是虚拟机管理程序的一部分，它就能更有效地处理负载在虚拟化环境中的移动和弹性。然而，重要的是要记住，虚拟机管理程序是整个虚拟计算资源的基础操作系统，虚拟机管理程序中任何服务的问题都将对整个虚拟化环境产生影响。这个问题限制了可以应用到管理程序的安全服务的功能和复杂性。因此开发一个不会影响虚拟化环境和应用性能而又健壮的虚拟机管理程序防火墙解决方案，是一个显著的挑战。

## 用户对虚拟化安全方案的顾虑

云环境先有网络，后有安全，虚拟安全方案如何插入不对既有网络产生影响？

传统物理网络中，通常仅需做不同网段间的安全隔离，而虚拟化网络中需要细粒度到虚拟机之间的隔离，怎么做？

几十台甚至上百台的分布式安全防护业务虚机如何管理，会不会给管理员带来巨大的工作量？

云环境中虚拟机的动态迁移是常态，安全防护如何跟随？

## 山石网科视角

山石网科的云内部安全防护产品（山石云•格）基于第三方视角，利用NFV和SDN的优势，将自己深度插入到虚拟化环境中，按需部署和扩展防火墙资源。与现有的云计算管理平台（如vCenter和OpenStack）紧密集成，将可视化能力一直深入到虚拟化架构中，使防火墙资源随其要保护的的虚拟资源增长和缩减。

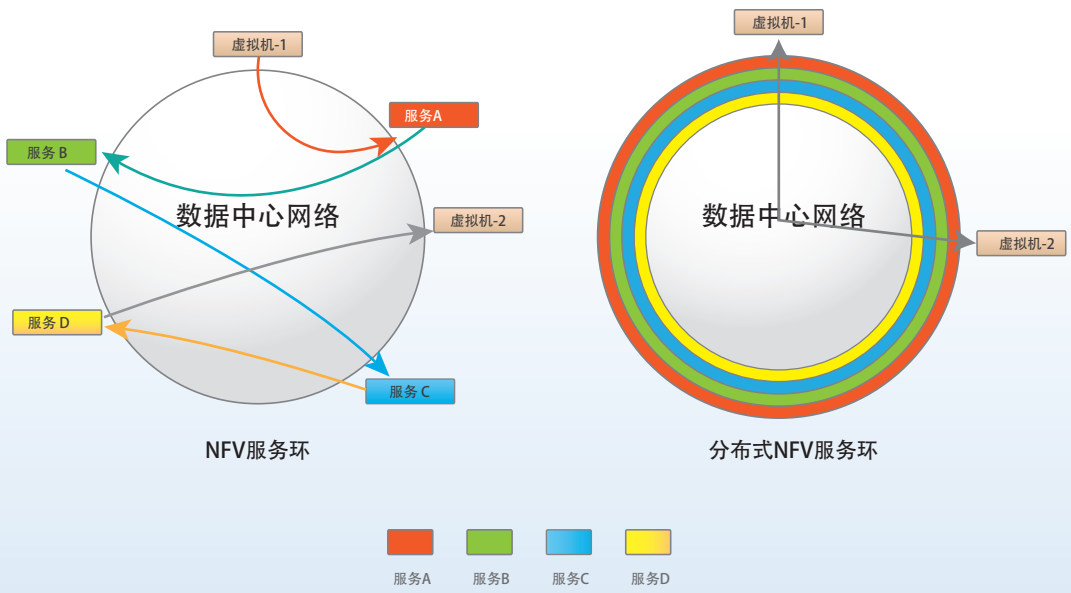


图1：山石网科的分布式NFV业务环保证安全服务始终贴近被保护的虚拟资源

不走安全服务链的流量重定向绕路，也不产生性能瓶颈，山石云•格的分布式架构将防火墙业务虚机部署在靠近租户负载的位置上，创建了一个一直靠近数据中心资源的虚拟安全业务环（如图1所示），弹性的处理东西向流量和南北向流量。由于安全业务环一直靠近被保护的虚拟资源，不会产生不必要的延迟。

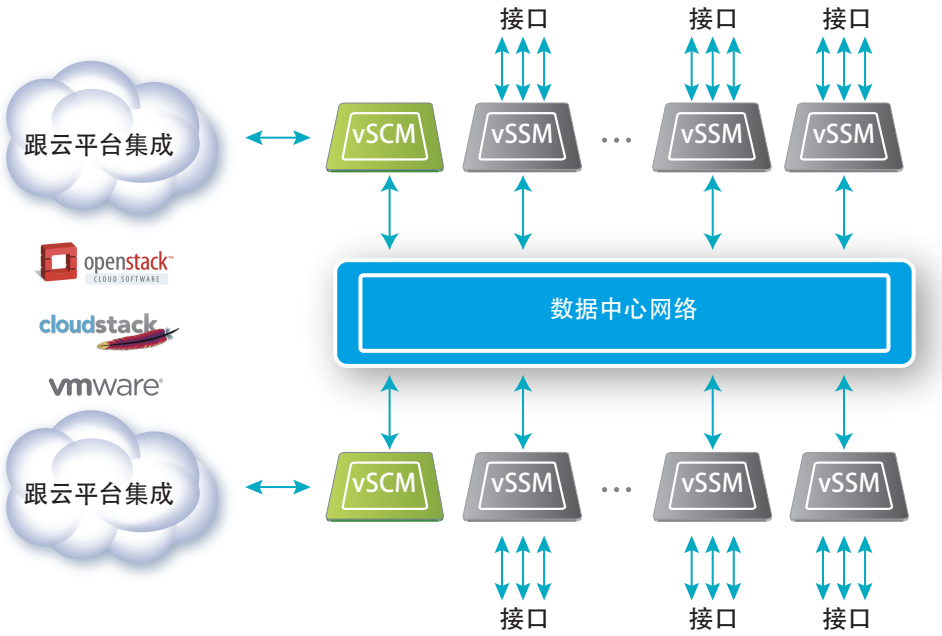


图2：云内部安全防护产品（山石云•格）架构

类似NFV，山石云•格是基于虚拟机和软件的。为了分发和扩展安全服务，山石云•格将控制平面和业务平面进行了分离。

**控制平面**，就是山石云•格的虚拟安全控制模块（vSCM），作为中央安全配置管理器，主备模式设计，通过驱动程序和RESTful API与数据中心的云计算管理平台紧密集成，并提供了管理界面来配置和监控虚拟安全服务。

**业务平面**，就是山石云•格的虚拟安全业务模块（vSSM），处理安全策略查找和高级安全服务，转发南北和东西向的数据流量，随流量的增加和减少弹性扩展，以确保没有性能瓶颈。

图2展示了山石云•格如何在数据中心租户网络中互联，以形成一个安全服务平台，以及如何通过按需增加vSSM虚机来简单的完成扩展。

由于所有这些服务都是弹性和分布于整个虚拟化环境中的，它们总是靠近需要被保护的虚拟资源。这使它们能够不需要流量重定向绕路和无性能瓶颈的使能安全策略。

安全管理员可以管理整个防火墙架构就好像它是一台单一的设备，同时在管理界面中允许每个租户有自己的防火墙管理接口和个人的安全策略集。

面对新的恶意软件不断挑战的安全环境，防火墙的升级绝对是至关重要的。不幸的是，升级可能破坏防火墙、网络和应用性能。山石网科在山石云•格中另外做了一个重要组件，在线软件升级（ISSU），使部署的更新和升级不会产生任何服务中断。

## 面向虚拟机的微隔离

山石云•格将自己深度插入到虚拟化环境中，能够做到每一个虚拟机跟外部网络或内部其它虚拟机之间通信的精细监控，我们称之为微隔离。这样的方案才能够完全解决用户急需解决的安全问题，阻断从内部向其它虚机和外部网络发起的端口扫描和DoS等攻击，而仍然保持问题虚机的对外服务；监控到绕过外部防护、以被控制虚拟机为跳板的内部入侵，为每一台业务虚拟机都提供最贴身的安全防护力度。

## 山石云·格的优势

**山石云•格的优势是十分明显的。**

**敏捷** 山石云•格的易于扩展、移动和弹性保证了数据中心安全像被保护的虚拟架构一样敏捷、弹性和灵活，提高业务灵活性并为新的IT创新产品缩短上市时间。山石云•格既保护了南北向的流量，也保护了东西向的流量。

**高效** 很多静态模型不是在平均负载时提供过多的资源，就是在峰值负载时提供不足的资源，山石云•格能够为所需之处申请确切数量的资源，非常的高效。

**应用和负载性能** 山石云•格不需要流量重定向而弹性申请安全资源的能力，保证了应用程序性能不会对负载产生不利影响。这对于关键应用特别的重要，因为性能下降、停机或安全漏洞可能导致收入的损失或客户的丢失。

**高可靠性** 山石云•格架构的冗余和ISSU方面的考虑确保防火墙的保护始终正常运行不会中断。

**管理简单** 集中式的管理界面以及跟云计算管理平台的紧密集成，简化了虚拟化环境中的安全管理，允许更多的IT资源被分配给项目和功能，以增强业务能力。

**保护能力强大** 山石云•格提供了强大的深度包检测、防火墙、入侵防御以及分布式拒绝服务攻击（DDoS）防护，以抵御当今最复杂的威胁。实时升级确保新的防御技术可以被立即应用，没有任何业务会因为新的威胁出现而中断。

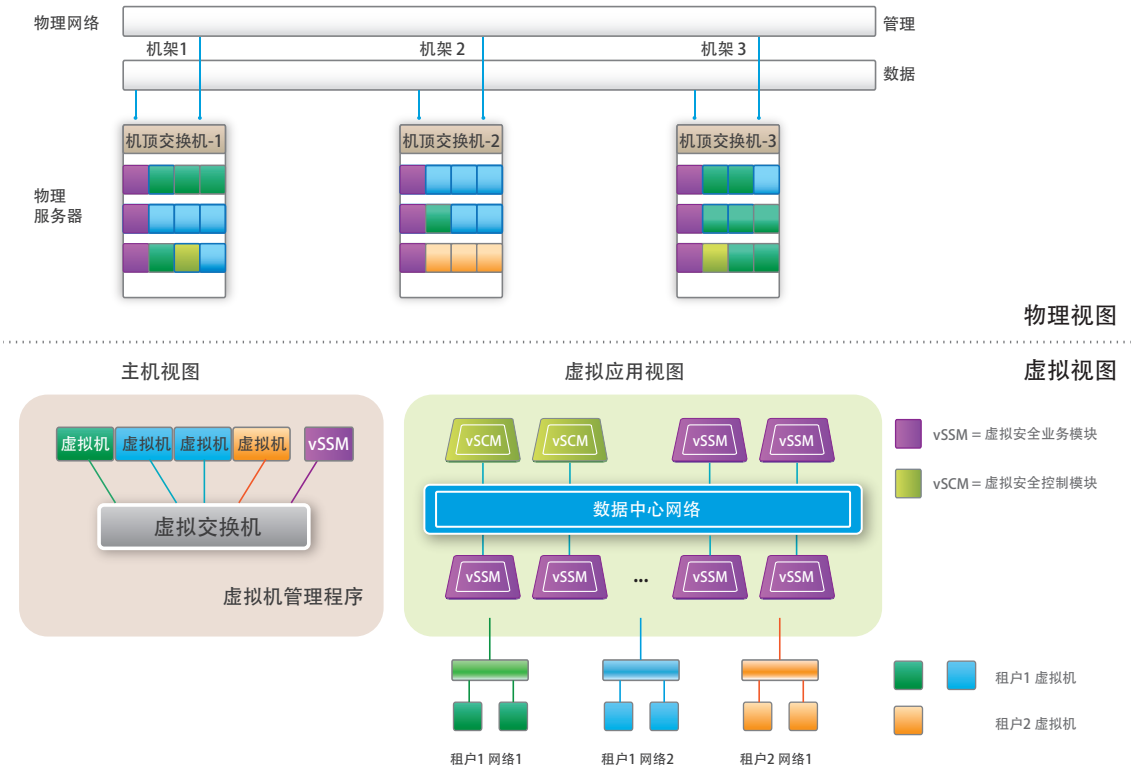


图3：云内部安全防护产品（山石云•格）二层部署

为了能够看到和控制同一VLAN内虚拟机之间的流量，图3展示了山石云•格被应用在二层网络环境中的用例。在这个用例中，不同数量的vSCM，vSSM被按需部署，来保护一个个的租户和负载。

虚拟和基于云的技术给数据中心带来了许多新的安全挑战，这些在物理数据中心环境中是不存在的。只有分布式的虚拟防火墙弹性架构能够提供敏捷性、灵活性、弹性，以及南北和东西流量的高效通路，这是虚拟和基于云的数据中心所要需要的。山石云•格采用了最前沿的新兴NFV和SDN技术，将自己深度插入和集成到虚拟化环境中，为虚拟化数据中心提供最强大、高效和最少侵扰的安全解决方案。

官方微信

Hillstone NETWORKS