山石云·格 & VMware NSX 集成解决方案

IT 人都知道 SDN 会改变世界，VMware 和 VMware 的 NSX SDN 解决方案使软件定义数据中心变成了现实。

毫无疑问，当你进入软件定义数据中心的世界，你会遇到一系列的挑战：

1、对东西向（虚机之间）的流量不可视。

2、在虚拟化环境内部署安全方案需要人工做大量的网络配置工作。

3、安全业务跟不上虚拟机生命周期的脚步。

4、很多传统的安全功能对虚拟化网络环境都不适用。

很多安全厂商已经提供了一些方案来跟进这些 SDN 的挑战。作为云安全的领导厂商，山石网科也提供了山石云 · 格产品跟 VMware NSX 紧密集成的方案。在 NSX 的基础上为用户提供微隔离、可视化，以及下一代防火墙的安全能力：

1、 通过 VMware NSX 平台提供的扩展服务插入和服务链接口，将安全业务虚拟机透明的部署在每台 ESXi 主机上。

2、 山石云 · 格的 vSOM 组件能够从 VMware NSX 平台同步配置信息，使得安全运维人员能够根据虚拟应用的创建和变更快速的制定安全策略。

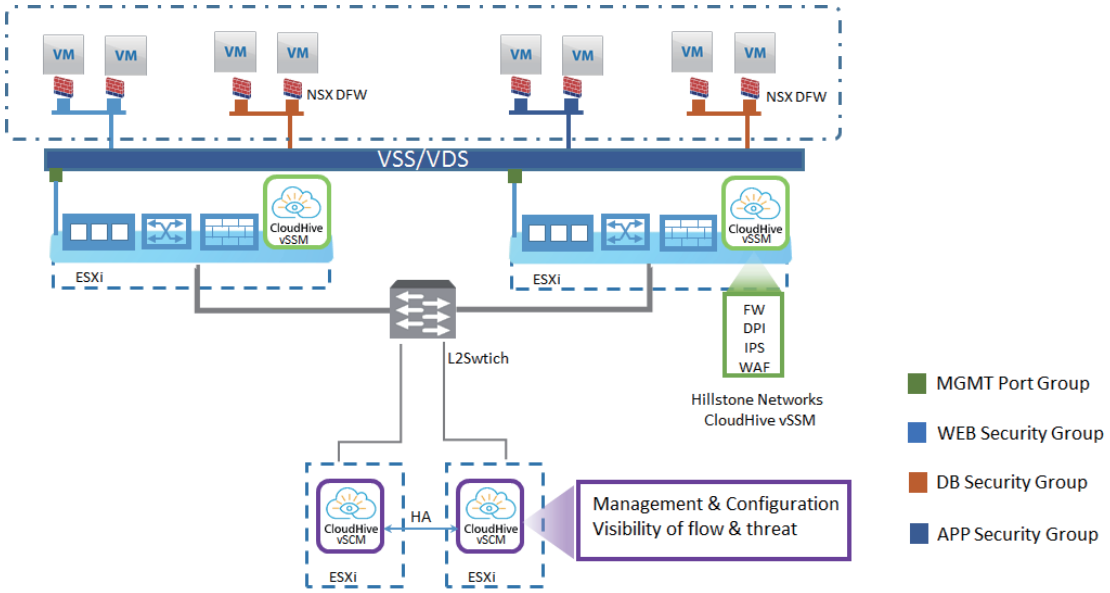
3、 安全策略能够跟随虚拟应用的变更而动态的变化。

4、 企业能够更快的运维安全服务，并高效的利用云基础设施的能力，不必担心安全问题。

那么，VMware NSX 和山石云 · 格都能提供哪些解决方案呢，下面我们来看几个：

解决方案 1：不用 VXLAN 的 NSX 场景

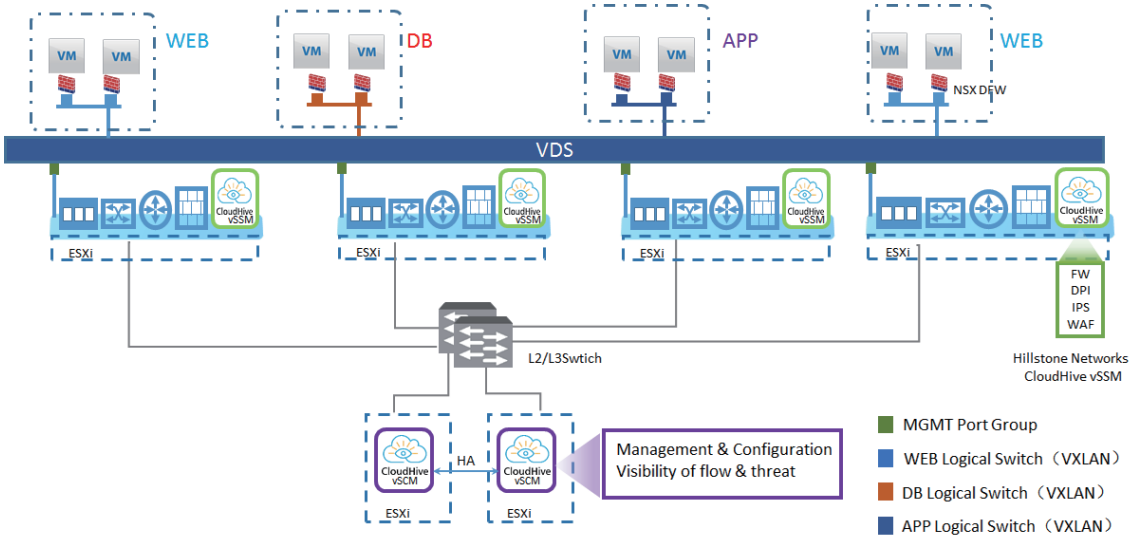
在 VMware 的云环境中，ESXi 和 vCenter 的搭配是最常见的。在 VMware ESXi5.5，6.0，甚至 6.5 的环境中，大量的用户还在用 VSS（标准交换机）。对于这些用户，过渡到 VXLAN 需要花费大量的人力物力，仅使用 NSX 的 Introspection 特性来满足网络安全需求是一个性价比很高的解决方案。由于 ESXi 和 vCenter 搭配的场景通常都是大二层部署，微隔离的需求就变得十分重要。山石云 · 格则在 NSX 的流量重定向能力的配合下，能够为用户提供一整套微隔离、可视化，以及下一代防火墙安全能力的完美微隔离解决方案。



解决方案2：使用VXLAN的NSX场景

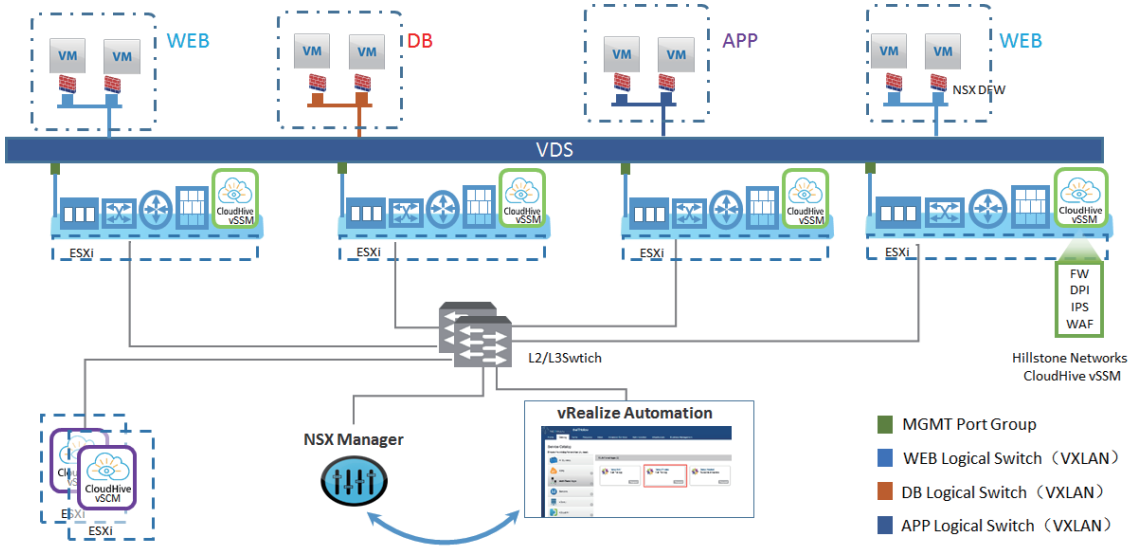
一些新建的 VMware 的云环境在 NSX 的配合下可以直接进行 VXLAN 网络部署。在这种场景下，客户虚拟机直接被划分到了不同的二层域下，使用传统的网段隔离方式进行隔离：虚拟机根据角色的不同被连到不同特定的 VXLAN 逻辑交换机

上。例如，在三层应用模型中，所有 Web 服务器虚拟机被连到 Web 逻辑交换机上，所有应用虚拟机被连到应用逻辑交换机上，所有数据库虚拟机被连到数据库逻辑交换机上。山石云 · 格的安全服务则可以部署在每个逻辑交换机旁边，为层与层之间的通信提供安全防护。



解决方案3：使用VXLAN的NSX跟vRA（vRealize Automation）配合的场景

对于在 NSX 基础上又部署了 vRA 的用户，他们可以在软件定义 IT 的基础上使用安全即是服务。在解决方案 2 的基础上，NSX 上定义的安全策略和安全组能够以模板的形式被 vRA 的业务直接关联调用，使得 vRA 能够在一键部署 IT 业务的过程中同时为租户自动部署网络安全服务，山石云 · 格则在后台提供了安全能力的支持



在每个解决方案中，引流策略都是在 NSX 的服务编排和安全策略中进行配置，使得安全组之间的流量被重定向到山石云 · 格的安全服务虚拟机上。通过山石云 · 格的动态地址簿功能，安全策略就可以基于虚拟机或者虚拟机组来规划。

山石云 · 格跟 VMware NSX 的配合过程中，如果有新的 ESXi 主机加入，山石云 · 格的安全业务虚拟机会自动在新的 ESXi 主机上部署出来。而且，已经存在的安全策略会自动施加在新的虚拟机上。这绝对是不需要人工干预的扩容场景。应用数量不断的增长，在山石云 · 格跟 VMware NSX 的配合下，新建虚拟机的流量不断被引流到山石云 · 格的安全业务虚拟机上得到安全防护。