Hillstone
山石网科

在SDN环境下
如何更好实现微隔离和可视化

山石云•格结合VMware NSX实现零信任安全模型

摘要

本文以山石云•格与VMware公司的NSX产品的结合为主题，来深入探讨如何将基于SDN技术的网络产品和安全厂家的云安全产品相结合，从而为用户实现高性能、高效率的云中安全。

关键字：山石云•格,NSX,SDN,微隔离,可视化,零信任安全模型，云计算,VMware,山石网科

经常有人问：SDN网络产品，比如VMware的NSX功能非常强大，内置有分布式防火墙（DFW），是不是就不需要山石云•格这样安全厂家的微隔离产品了？在山石云•格全面支持VMware NSX产品之后，这一问题更多的被人问起。

答案是，只有两者SDN产品和专为云计算环境设计的微隔离和可视化安全产品紧密结合，才能打造一个安全的云计算环境！二者不冲突，是“1+1>2的关系”。

专业安全厂家的微隔离和可视化产品比如山石云•格，与优秀的SDN产品比如VMware的NSX结合，会给用户带来全面防护、高性能、高可用的云计算安全方案，真正在云计算环境下实现“零信任安全模型”！

本文就是以山石云•格和VMware NSX产品结合为例，讲述二者定位的差异，以及在实践中如何结合使用，从而达到性能和全面防护的完美结合！

溯本求源，先看看云计算内部面临的多样性的安全挑战。

第一章、云计算内部多样性的安全挑战

云计算和虚拟化技术出现后，在云内呈现了多样的安全挑战。

云计算环境内部，由于缺乏适应云计算需求的安全产品，在安全方面普遍呈现了以下问题：

- 云内部流量、应用、威胁不可视：虚机间通信流量部分通过虚拟交换机进行交换，传统技术手段无能为力。
- 被放大的安全域：体现为因为网络虚拟化和虚机的引入，传统上一个多台服务器组成安全域内，实际被防护的资产——虚机数量几十倍增长。
- 没有明确物理边界：因为虚网络和虚机迁移等技术的引入，传统的物理安全边界消失。
- 安全责任划分不确定：一些分工变得模糊，比如连接虚机的虚网络的 VLAN 维护工作，谁来负责？
- 巨大的工作量：被防护的数据资产——虚机几十倍增加，再加上云计算中虚机数量、网络的弹性扩展或收缩，带来了“数量、频度、复杂度”三维度的配置工作量提升。因为繁复，而疏于管理和配置。

今天面临的网络攻击动机已经从早期的以“好玩”转向为以明确牟利为目的的新时期。按照 Verizon 公司发布的《Data Breach Investigations Report》（数据泄漏调查报告）系列报告中，可以看到以牟利为目的的网络攻击行为 2017 年占到总攻击中的 93% ！这其中来自内部和合作伙伴的攻击持续上升。从攻击行为看，“网络间谍”（Cyber Espionage）、“权利滥用”（Privilege Misuse）和“杂项失误”（Miscellaneous）占据了攻击的前 2-4 位。

在山石网科撰写的《阻断云内数据泄露之路——零信任安全模型的云计算最佳实践之微隔离技术》的白皮书中，我们引用了国际知名的独立技术和市场调研公司Forrester Resarch公司在提出“Zero Trust Model”（零信任安全模型）中的观点。零信任安全模型被认为是一种有效应对今天以牟利为目的的网络攻击有效方法和安全模型。零信任安全模型认为，传统的以单一边界防护，遵从“通过认证即被信任”（Trust but Verify）原则的安全模型极易被突破，常见的例子如利用内部权限管理漏洞，黑客绕过外部边界防火墙，获取内部主机权限，“畅通无阻”的在内部进行攻击。

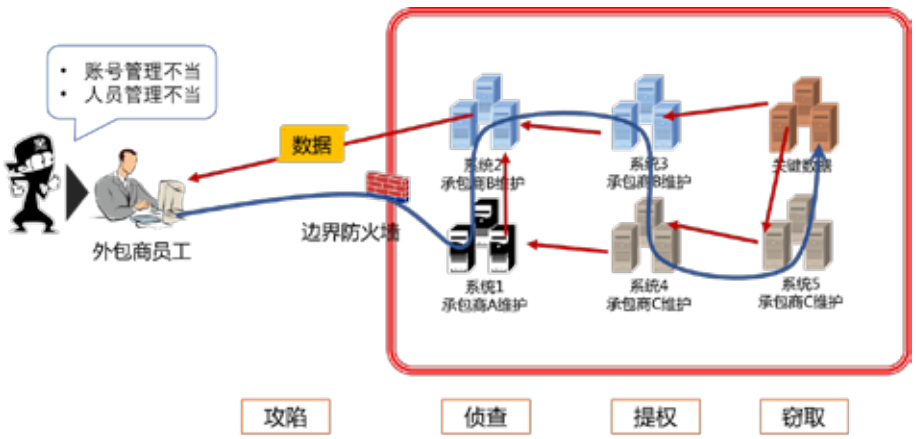


图1，在传统安全模型下，常见的承包商员工利用权限管理不当，绕过边界防火墙，实现系统内窃取数据的行为。

今天，很多的云计算内部，还停留在古老的“通过认证即被信任”的传统安全模型阶段，在云计算中心最外部边界部署安全设备，而内部对“黑客”则是畅通无阻。这也是为什么在山石网科推出山石云•格、山石云•界产品的近三年时间里，目睹了大量国内外客户云计算环境中，频繁发生网络安全事故。归纳起来，常见的导致安全事故的攻击行为如下：

内部攻击：

- 耗尽资源：耗尽宿主机计算资源，内部网络资源
- 恶意软件传播：传播病毒、木马、蠕虫等恶意程序
- 内部探索：内部网络探索、扫描宿主机、虚机、应用系统上可利用的漏洞
- 欺骗提权：利用网络欺骗、恶意软件等手段，提取关键应用系统使用权限
- 篡改：利用 Web、数据库等主机和应用程序漏洞，截获的系统权限，对关键应用系统、网站进行信息篡改
- 窃取数据：窃取数据，并将关键数据进行重新的封装和隐藏，伪装成普通应用协议向外传输
- 违规应用：擅自利用协作工具，发起远程协作带来安全风险。或者是违规安装如分享类软件，浪费宝贵计算资源和带宽

外部攻击：

- 主要体现为虚机被黑客利用，变成肉机，滥用云计算中心的带宽、计算资源，对其他网站或应用系统发起攻击。

零信任安全模型被业界认为可以有效的阻断新形势下以牟利为目的的攻击。如何在云计算内部打造零信任安全模型呢？

第二章、零信任安全模型与微隔离

微隔离和可视化（MicroSegmentation&Flow Visibility）类的产品和方案被认为是诸多云计算安全技术中最适合实现零信任安全模型。在山石网科推出的《阻断云内数据泄露之路——零信任安全模型的云计算最佳实践之微隔离技术》中，我们有非常详尽的阐述。为了更好的理解NSX的DFW的微隔离与山石云•格“深度”微隔离和可视化结合的意义，我们再简单复述一下其中观点。

零信任安全模型，是一个构建网络的全新方法学，核心是把“通过认证即被信任”变为“通过认证，也不信任”，零信任安全模型的网络要做到以下几点：

- 围绕数据资产，由内到外设计网络，构筑安全防护。
- 确保对所有资源的访问行为都是安全的，不论是来自内部还是外部。
- 所有访问都不被信任，都被核查，采用最低特权，严格访问控制。
- 检查和记录所有流量，实现流量的可视化。

具体实现上，零信任安全模型给出了网络设计的思路原型：

1、围绕不同的数据资产划分安全域。根据组织内，不同的数据资产划分若干个MCAP（Micro-core and Perimeter，微型核心与边界MCAP），可以理解为一个聚焦的小型安全域。

2、平行对等互联的MCAP。这些MCAP会平行对等的连接到一个高度集成隔离网关上，每个MCAP对应一个网络接口，隔离网关会执行全局的控制策略。体现了“零信任安全模型”的精髓，即对所有访问的不信任，都要进行鉴别，限制最低的访问权限。

3、核心部署高度集成隔离网关。这种集成式安全网关应该类似现在市场上可以找到的UTM或NGFW，能够实现深度数据包的检查，做到细颗粒度的访问控制，能做到包括对恶意软件检查过滤的功能。集成隔离网关的性能要求很高，因为高度集成隔离网关部署在网络核心，和核心交换紧密结合。

4、集中管理。可以在网络核心的集成隔离网关上对MCAP们进行集中管理，设定全局的、无差别的安全控制策略，对MCAP之间的通信进行集中管理控制。

5、实现完整网络的流量和威胁可视。零信任安全模型的一个基础是必须检查和记录MCAP之间的来往数据

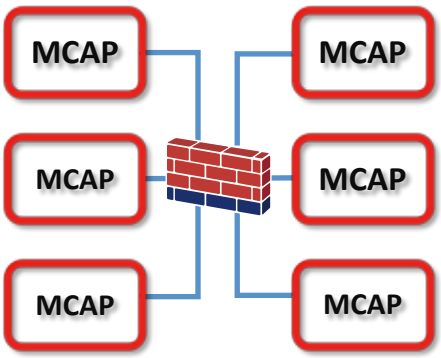


图2，零信任安全模型架构图

微隔离和可视化（MicroSegmentation&Flow Visibility）被认为是解决云计算内部安全问题的最佳技术方案之一，是连续两年上榜Gartner Group的信息安全十大技术，并且在Gartner Group的“技术成熟度曲线”（Hype Cycle）中即将达到曲线的顶点。从现已面市的微隔离产品看，主要有5大类产品。其中网络厂家的SDN产品、云计算厂商集成在虚机监视器（Hypervisor）内的NFV化的SDN产品、网络安全厂家如山石网科的山石云•格产品，以及一些靠在虚机上部署客户端软件的方案更契合云计算环境中，软件定义数据中心（SDDC）的发展方向。

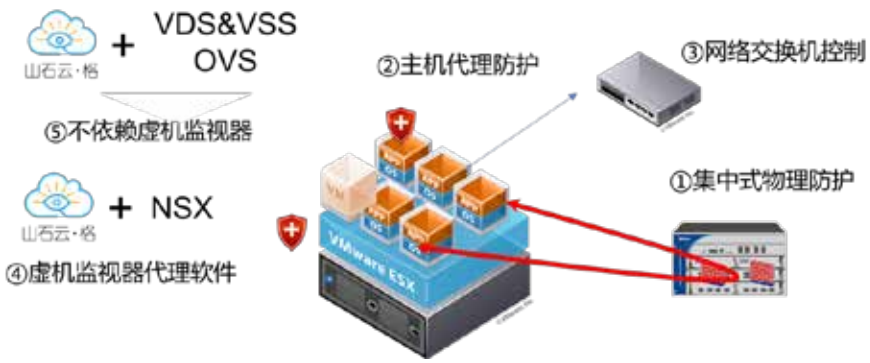


图3，常见的5类微隔离技术方案

不论是SDN产品如VMware NSX加分布式防火墙功能，还是山石云•格，它们都遵从了软件定义数据中心的思路，都可以按需、“随心”、合理的划分安全域。直至可为最小的数据资产每一个虚机划分一个独立安全域。就如同《阻断云内数据泄露之路——零信任安全模型的云计算最佳实践之微隔

离技术》提到的，遵从零信任安全模型，围绕着不同数据核心资产划分MCAP，将安全的DNA融入网络当中，从内到外设计网络。

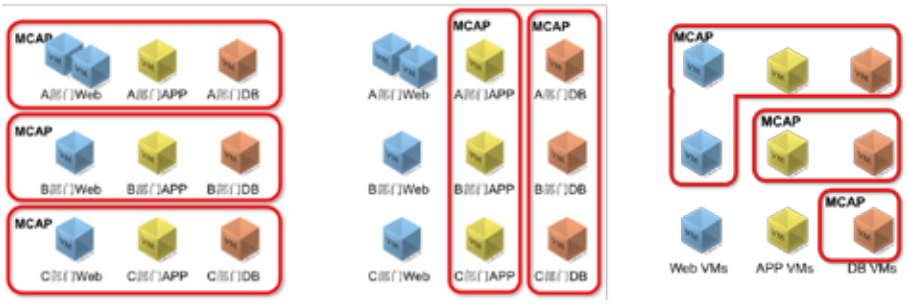


图4，NSX和山石云•格都可以做到可以随心所欲的划分安全域

NSX和山石云•格都采用了全分布式架构，分布在所有宿主机上的安全业务模块——山石云•格的vSSM和NSX的DFW就像一台设备，有统一的策略、转发表、会话表，而且集中管理，只是处理是分布式完成。

山石云•格，是一个全分布式架构的VNF（虚拟网络功能）产品，共由vSOM（云管理模块）、vSCM（云控制模块）、vSSM（云安全业务模块）和vDSM （虚拟数据服务模块）组成，这些软件模块都运行在普通虚拟机上。其中vSSM模块是为云计算中虚机提供全面网络安全防护的，它需要部署在云计算环境中每台宿主机上，利用云计算平台的引流接口，将受保护虚机进出网络的流量牵引到vSSM上，为每个虚机提供一个防火墙。由于采用分布式架构，所有的vSSM像一台设备在工作，由vSOM负责统一安装，由vSCM进行管理和控制，由vDSM统一输出日志。配置策略时，只需要围绕虚机进行配置即可，不必关心虚机在哪台宿主机上，系统会通过环境的资产发现，把安全策略在虚机所在宿主机的vSSM上执行，而迁移时，会话和策略也会在不同的vSSM模块间同步（山石云•格产品架构图见5）

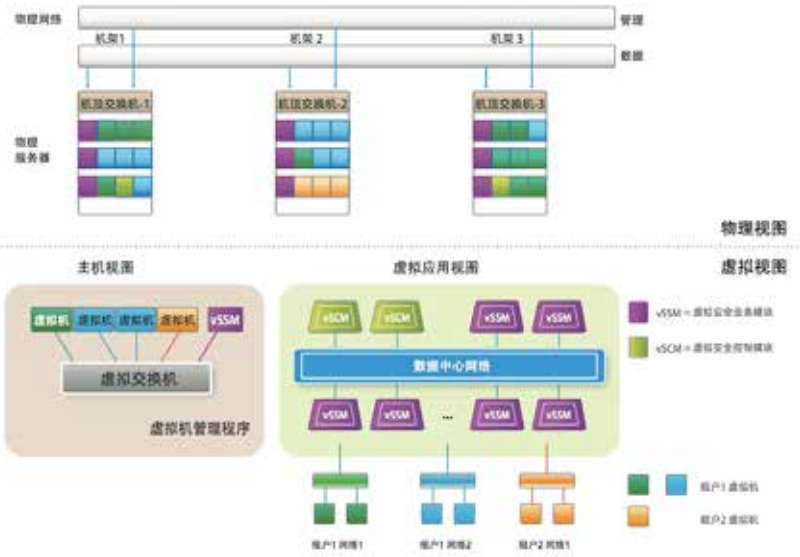


图5，山石云•格产品架构图

作为SDDC（软件定义数据中心）的代表，VMware公司的NSX是业界领先的SDN产品。NSX可以达到服务器虚拟化相同的效果，可以独立于不同品牌的物理网络设备，按需（按使用量和用途）进行自动服务，只要物理交换机提供了基本联通性，VLAN、路由的调整都在NSX上完成。NSX集成了交换机、DFW、防火墙等网络功能。其中交换机、DFW是在Hypervisor主机内核空间中安装内核模块来实现的，通过统一的管理模块进行管理。使用NSX的数据中心最终达到的效果是：无论系统规模多大，无论物理服务器、虚拟机有多少台，无论底层网络多么复杂，无论多站点数据中心跨越多少地域，在NSX网络虚拟化解决方案的帮助下，成千上万的虚拟机就如同链接在一个物理交换机和防火墙上。（NSX产品架构图见图6）

图6，NSX产品的架构示意图。

不论是山石云•格还是VMware的NSX，这样的分布式VNF产品，都可以做到按需的扩展，随着宿主机数量的增加，处理性能随之增加。不论两个通信的虚机，身处哪台宿主机，他们之间通信，都像只经过了一台设备，这就很好的诠释了零信任安全模型，MCAP对等互联、集中管理的要求。

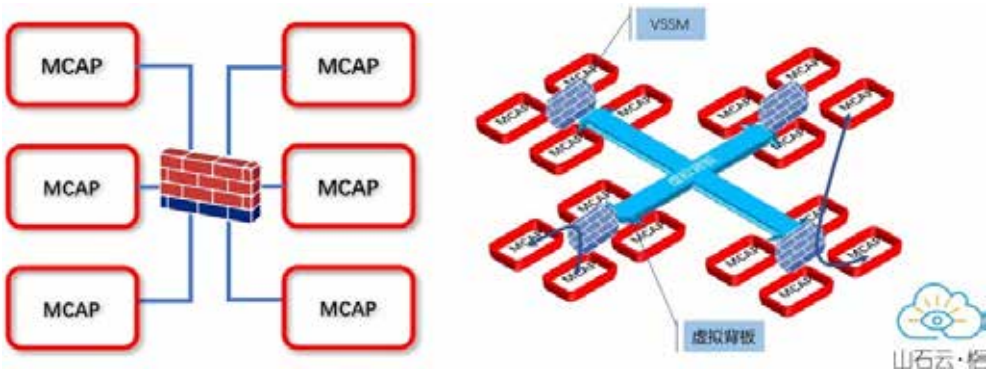


图7，采用全分布式架构的微隔离产品。

在功能上，NSX首先是一个软件的SDN产品，实现了交换机、DFW、分布式路由器、边界网关，其DFW是一个2-4层的防火墙，主要实现2-4层的访问控制。而山石云•格则是一个纯安全产品，使用了NGFW——实现2-7层的访问控制与攻击防护，应用识别、IPS、轻量级WAF、网络防病毒。

从微隔离角度看，NSX及其DFW实现了微隔离，相比较而言山石云•格则是深度微隔离和可视化产品，“深度”体现的是2-7层的应用识别、访问控制、威胁发现与防护。

那么在云计算内部仅仅是2-4层的隔离、访问控制，够吗？是不是就实现了零信任安全模型呢？

第三章、零信任模型还需最低授权和深度可视

答案是仅仅是2-4层的访问控制，不够！需要VMware这个SDN界的微隔离产品与山石云•格这样的深度微隔离和可视化产品深度整合，因为零信任模型还要最低授权，并且深度可视。

我们结合行业和国家标准，以及几个现网中常会遇到的例子，看看缺失了最低授权和深度可视会怎样。

1、发现阻断租户对外攻击

在已经成为中国行业标准的《GA:T1390.2-2017云计算扩展要求》要求“应能检测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等”（《GA:T1390.2-2017云计算扩展要求》第6页，6.1.2.3），这体现了两种攻击，其中之一是第二章提到的对外部的攻击，“由北向南”的攻击。

对于很多云计算服务商和云租户来说，这都是非常令人苦恼的事情。我们遇到过多个公有云、私有云运营商备受由内向外攻击的困扰。困扰他们的问题集中在：

- 难以发现：不论是最基础的 Flood 类 DoS 攻击，还是高级的 CC 攻击，服务商都难以发现，通常都是在网监部门、或其他服务商定位攻击源头是自己之后，才发现这些对外攻击。而从安全管理员的视角来说，通常使用防火墙等安全设备，关注的是由外向内的攻击。
- 难以定位：难以定位内部的攻击源。可以试想一个拥有几个吉比特每秒乃至几十吉比特每秒的数据中心出口，在几个月的防火墙日志中，想找到某一段时间的攻击，同时再考虑到 NAT，地址伪造等等因素，定位一个攻击源头，如同大海捞针。
- 难以阻断：大多数防火墙上的策略是由外向内阻断，由内向外通过。对于公有云服务商，即使定位了某一租户的虚机被植入恶意软件在对外进行攻击，也很难阻断这一由内向外的攻击。而对于私有云服务商来说，则要在业务持续性以及安全“义务”上做艰难的决定。虽然可以通过让虚机下线的方式进行攻击阻断，但是云计算中心的虚机大多都是运行某种应用的服务器，对业务持续性要求很高。这种高要求，甚至会使管理员让运行着存在大量已知高风险漏洞的老操作系统和软件的虚拟机，在不打补丁、不安装杀毒软件情况下继续运行。

仅仅是具备访问控制功能的SDN和2-4层DFW产品，在这种情况下无法做到可视——发现威胁、定位威胁；无法做到阻断和最低授权，仅允许正常访问通过。单凭2-4层防护且不要说零信任安全模型，即使是等保二级的要求也无法满足。需要具备2-7层全面防护可视的产品来帮助。

2、阻断东西向攻击

《GA:T1390.2-2017云计算扩展要求》要求“应能检测到云租户的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等”的另一种体现云内的东西向攻击，既可能出现在租户之间也可能出现在虚机之间。

通常来说以窃取数据为目的的攻击，特别是近年来出现的高级可持续性攻击，通常都是以首先获得信息系统中低价值服务器的控制权，而后向高价值服务器渗透，最终完成攻击的。在整个攻击过程中，攻击者会在不同的服务器之间不断的重复以下步骤，最终达到对核心数据的窃取或破坏。

- 侦查：网络和资产发现，可用端口、可用漏洞发现。
- 恶意软件组装 & 传输：病毒、蠕虫、木马文件的传输。
- 执行攻陷：通过恶意软件、网络欺骗等多种手段提取系统权限。
- C&C：远程遥控，进行攻击。
- 窃取或破坏：最终窃取或破坏数据。

每一个步骤的攻击行为，SDN和2-4层的DFW也无法做到可视和最低授权。东西向的网络发现和可用端口的扫描，安全厂家的产品都有多年积累的经验和算法，会及时告警，做到可视。而东西向漏洞扫描、恶意文件传输、SQL注入攻击等高层的攻击行为，不依赖具备2-7层防护的专业安全产品是无法发现攻击行为，及时告警，并阻断攻击行为的。

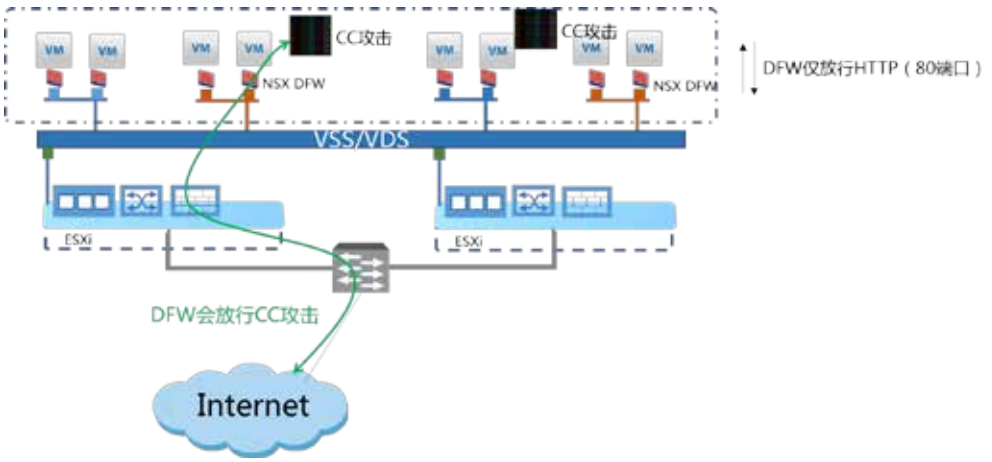


图8，黑客对内部外部系统进行CC攻击。CC攻击常常利用开放的80端口进行攻击，仅仅依赖DFW难以发现和控制租户间以及内部的攻击。

3、发现违规应用

在国家标准《GB/T 31168-2014信息安全技术 云计算服务安全能力要求》中提到，“云服务商应实时监视非授权的云服务远程连接，并在发现非授权连接时，采取恰当的应对措施”（见《GB/T 31168-2014信息安全技术 云计算服务安全能力要求》，7.19.2）。

除互联网和部分金融客户，很多政府、企业使用的应用系统都由外包供应商完成开发。在进行系统升级、维护过程中，最担心外部黑客利用远程协助工具，实现对内部的攻击。而摆在大多数云服务商面前的难题是：

- 难以发现：大量新型远程协助软件都使用 HTTP 协议，使用 80 端口进行通信，如果不具备深度包检测的能力（DPI）难以发现。
- 难以定位：同上，在一个大出口防火墙，几个月的日志中，筛查哪个 IP，在什么时间启用了远程协助……
- 难以阻断：由于这类应用大量使用 HTTP 的 80 端口，这一端口在大多数防火墙的配置中都是打开的，简单通过阻断 80 端口的访问，即使明确源 IP 地址，也是让网络安全管理员难以下决心阻断的。

仅仅只是2-4层的DFW，更是无法发现并有效控制这类违规的远程协助应用的。

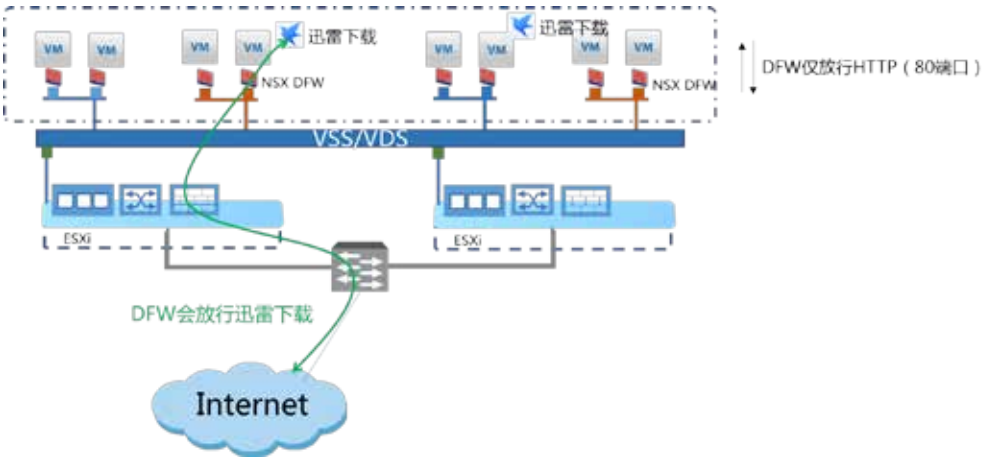


图9，迅雷是国内常见的P2P违规应用，类似的还有很多利用80端口实现的远程协助应用。这类应用不仅仅带来云计算资源的消耗，也是安全风险。

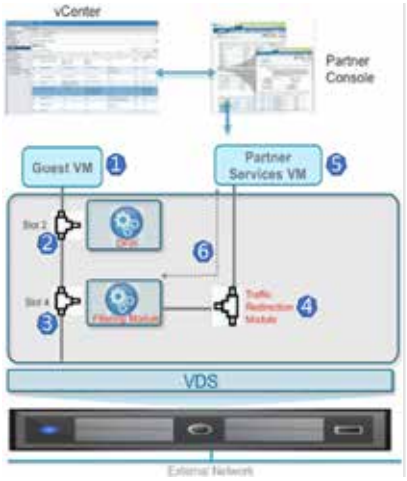
在零信任安全模型中有两点非常重要，就是对MCAP最低授权访问和要求记录所有流量，实现全面的流量和威胁可视。这也是为什么零信任安全模型提到，在进行MCAP平行对等互联时，需要一个像NGFW或UTM这样可以做到深度流量可视的高度集成的安全网关。

在今天的云计算中心，少则数十台高性能服务器，多则几百上千台服务器，实现更深度的网络可视、更细粒度的授权控制，依赖传统硬件的高度集成网关来处理各个微型安全域之间的东西向流量，不论从性能、弹性、效率上都难以满足需要。《阻断云内数据泄露之路——零信任安全模型的云计算最佳实践之微隔离技术》中认为，只有采用NFV技术，充分利用通用处理器的计算能力，采用全分布式架构才能满足需求。充分发挥NSX这样的微隔离产品与山石云•格这样的深度微隔离可视化产品优势，紧密结合、分工协作，会是更好的方案。

第四章、SDN 与微隔离可视化产品结合

在VMware NSX产品上市之初，就一直在营造安全领域生态环境，NSX面向第三方安全厂家提供了丰富的接口，与像山石网科这样的专业安全公司一起，打造一个高性能、高度弹性、自动化和全面防护的方案。我们就以VMware　NSX为例，来看看SDN类的微隔离产品和山石云•格这样的深度微隔离和可视化产品，如何有机结合，发挥价值。

NSX本身具备防火墙功能，但仅提供了2-4层的状态检测防火墙，可以实现隔离和访问控制（Isolation、Segmentation），前者是干脆的不能通信，就像现在很多公有云或社区云中不同租户之间的网络是完全不能互相通信，完全是隔离开的。后者则是说，在一个可以通信的网络，按照安全策略来控制A虚机是否能和B虚机通信。比如A不能和B通信，但是B可以发起和A通信。5-7层的安全防护，NSX则必须通过和专业的安全合作伙伴合作实现，比如山石云•格。



1、被保护虚机向外发数据包

2、分布式防火墙模块根据策略是否放过，放过的进入流量重定向模块

3、流量重定向模块根据策略是否转向

4、转向的转给第三方安全服务虚机（共享内存拷贝方式）

5、第三方安全服务虚机根据策略是否放过

6、放过的再回到流量重定向模块

图10，NSX引流原理

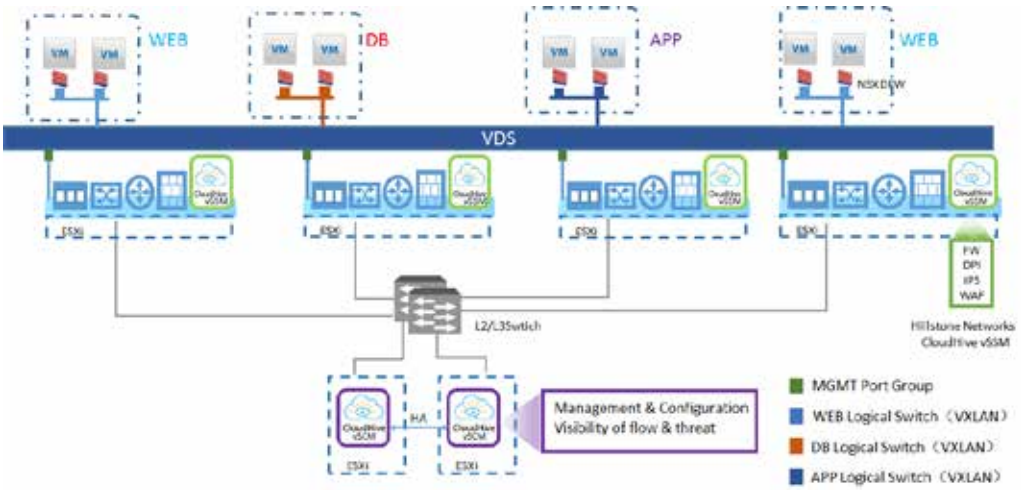


图11，NSX与云格结合方案

图10中显示了NSX与山石•云格等第三方安全产品的结合技术原理：每台虚机的虚拟网卡（vNIC）会接在NSX DFW上，而NSX DFW再接入虚拟交换机，也就是相当于为每个虚机的网卡，DFW都准备了一个防火墙。根据管理员的设置，DFW会对选择了深度防护的数据包，重定向给部署在每台ESXi的山石云•格的vSSM卡。山石云•格会把通过安全审核的数据包送到虚拟交换机上。图11显示了山石云格在NSX环境下部署的方式。

NSX和山石云•格一个经典的配合例子是， NSX DFW只允许一组Web服务虚机与内部、外部虚机利用TCP80端口进行通信，其他端口的访问、与数据库虚机的访问等等均被NSX的2-4层访问控制禁止掉。NSX会把80端口的流量重定向给山石云•格，由山石云•格来进行更细粒度的安全防护。在这种情况下，山石云•格可以实现应用识别、访问控制、攻击防护、IPS、网络传输文件的病毒识别、恶意代码查杀等等安全功能。这样的配合就会解决第三章中举的三个例子，实现深度的应用、威胁可视，以及最低授权，阻止80端口内的攻击行为、非法应用。同时山石云•格特有的可视化能力，也可以描绘出虚机间交互的关系，哪些虚机间发生过通信，实际是什么应用，应用的流向，耗费带宽等等。

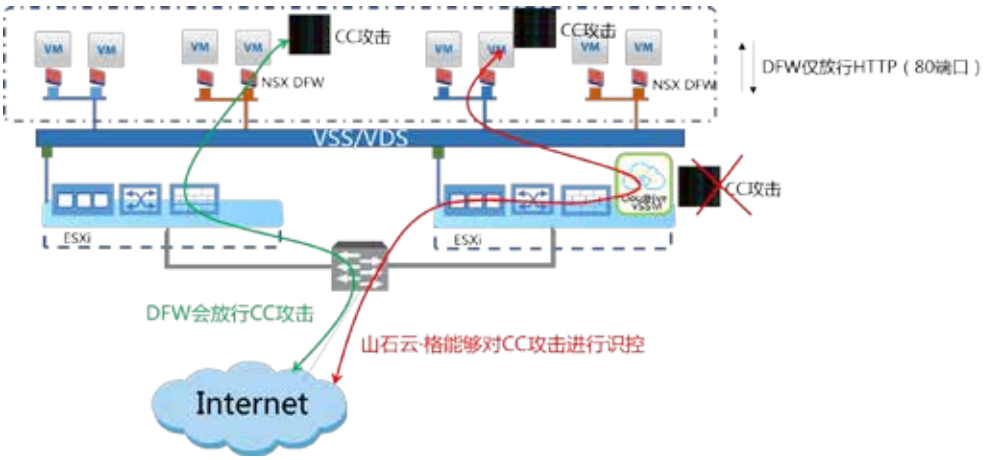


图12，NSX结合山石云•格，阻断云内的CC攻击

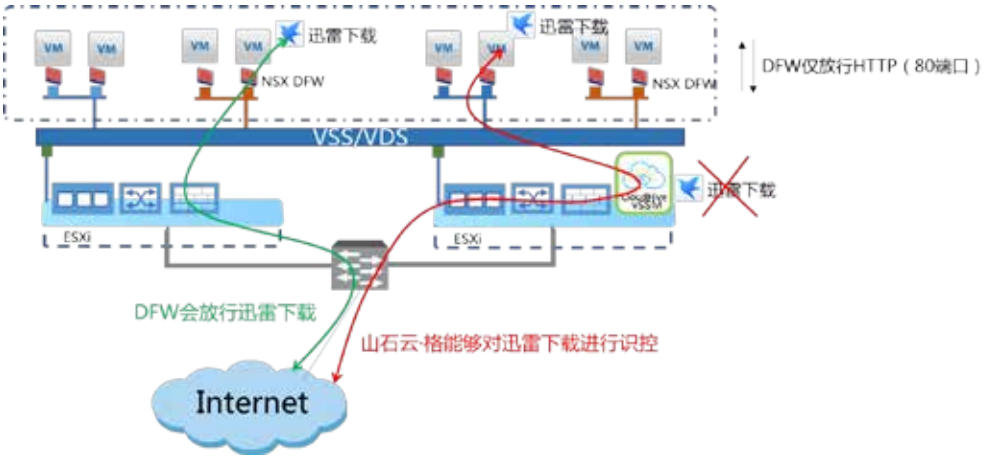


图13，NSX结合山石云•格，阻断云内的违规应用

图14，山石云•格的透视镜效果

流量重定向之外，NSX会与山石云•格实现管理控制信息的同步，比如IP地址、MAC地址、虚机名称、所在安全组、位置，山石云•格对恶意数据包的处理情况。控制层面的结合，结合山石云•格动态地址簿、资产发现等方面的优势功能，会给网络安全管理员提供极大的易用性，使他们的生产效率得到极大的提升。（要了解更多关于微隔离产品提升安全运维生产效率内容，可以阅读《阻断云内数据泄露之路——零信任安全模型的云计算最佳实践之微隔离技术》“安全生产力”部分内容）。

NSX与山石云•格的结合，会给对方，乃至云数据中心的网络安全管理员带来哪些好处呢？

1、高可用性：NSX的软件定义网络特性为用户带来了高可用性，一方面是网络的高可用性，高度自愈，在安全防护方面也带来了系统级的高可用性。比如虚机迁移这样的事件，NSX会主动向山石云•格提供相关信息，便于山石云•格给予及时的防护。

2、高效率与自动化：NSX的软件定义网络会给用户带来更高的维护效率，降低了安全策略部署调整的难度。

a) 不论是租户间的彻底隔离，还是调整 VLAN，或系统内的安全域，都只要在 NSX 上即可完成相关配置。
b) 引流到山石云•格，只要在 NSX Manager 上即可完成操作。
c) 降低第三方产品部署难度。比如山石云•格设计时出于自身安全性考虑，进行了控制与数据平面分离并采用私有协议传输控制信令，在 NSX 环境下，为山石云•格开通一条隔离的控制通道非常便捷，不必去物理交换机上做任何配置。
d) 自动化，可编程化。NSX 和山石云•格在这方面都做了大量工作。比如提供标准 API 方便维护者合作伙伴进行外部编程。再比如 NSX 的安全组，山石云•格的动态地址簿，都可以根据预先定义的策略模版，为同类虚机批量增加策略，见图 15。

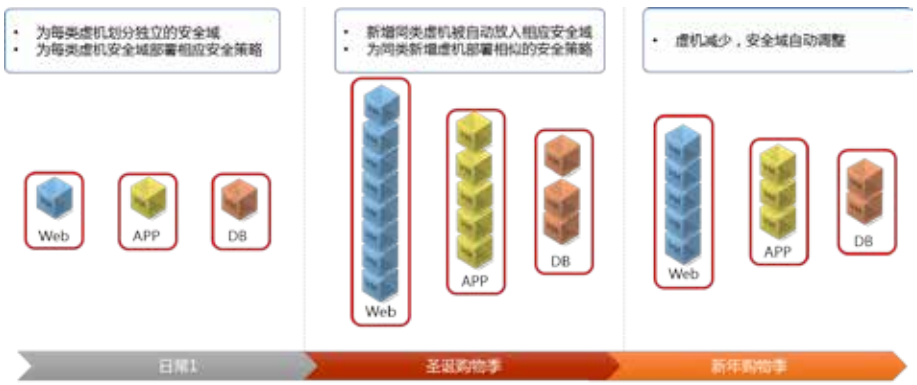


图15，NSX的安全组、山石云•格的动态地址簿可以适应云计算动态调整的需求，根据业务变化，动态调整安全域，为新增同类虚机增加相同安全策略，提高管理工作效率，减少安全防护漏洞。

3、 更高、更合理的安全处理性能。NSX与山石云•格结合，通过合理配置，策略优化，可以实现最优的安全处理性能。

a) NSX 的逻辑交换机和 DFW 做线速的 2 层隔离和 2-4 层的访问控制。
b) 山石云•格处理余下的部分流量，专注于 5-7 层的应用识别、访问控制，以及恶意代码阻断、攻击防护等。
c) 利用山石云•格的可视化能力，通过观察、分析，可以将更多的防护简化为“2-4 层访问控制”。这样 NSX 承担更多的 2-4 层访问控制，实现线速处理转发。山石云•格则更聚焦于深层防护、可视，集中到需要更低授权的关键资产上，实现云内部更高也更合理的安全处理性能。

图16，山石云•格与NSX结合，合理分工实现安全处理性能的优化

4、 最低授权：山石云•格给NSX和云内网络带来的帮助是更严格的最低授权，到应用级别的访问控制和安全防护。利用软件定义数据中心的新技术，山石云•格和NSX可以在云内实现多维度、立体的安全域划分，而且安全域的划分调整、安全策略的添加调整效率会非常高。在云中，一台虚机可能属于多个互相配合的安全域（见图17）：

a) 租户级别
b) 传统的基于网段的安全域
c) 虚机级别的安全域
d) 应用级别的
e) 其他

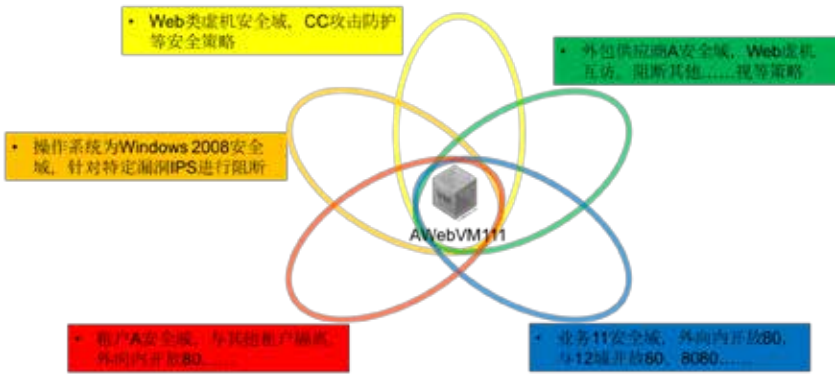


图17，多维度立体的安全域划分，实现最低授权访问

5、 深度可视：山石云•格给NSX和云计算中心带来的另一大帮助是深度可视。这种多维度、直观的云内可视，有助于发现隐蔽威胁，并便于实现策略的优化。

a) 多维度可视：山石云•格可以在统一时间轴上，呈现云内资产变化、网络内东西、南北向流量，以及其中应用和威胁情况，可以识别 6000 多种常见应用，7000 多种威胁、320 万种网络病毒。
b) 直观可视：
   - ◇ 定位到虚机：通过调用 vCenter 和 NSX 的 API，山石云•格将应用、威胁的源和目的定位到具体虚机上，直接显示虚机名称 /IP 地址。
   - ◇ 威胁流向：山石云•格会正确反映威胁和应用流向，方便锁定云内东西向或由北向南的攻击和应用。
   - ◇ 多维度搜索：可以分别按照时间、虚机名称、威胁名称、应用名称进行多维度搜索，定位问题
c) 虚机网络画像发现未知威胁：在云计算环境中，虚机承载的应用日益单一，其通信行为相对

简单。利用山石云•格长期监测虚机应用行为，实际上为虚机画下了正常通信的“画像”。今天很多高级威胁都隐藏在正常应用中，通过通常的特征识别较难发现，通过对比过往正常通信情况，则是发现未知威胁的有益尝试。图 17，如何通过观察虚机网络行为画像发现威胁。

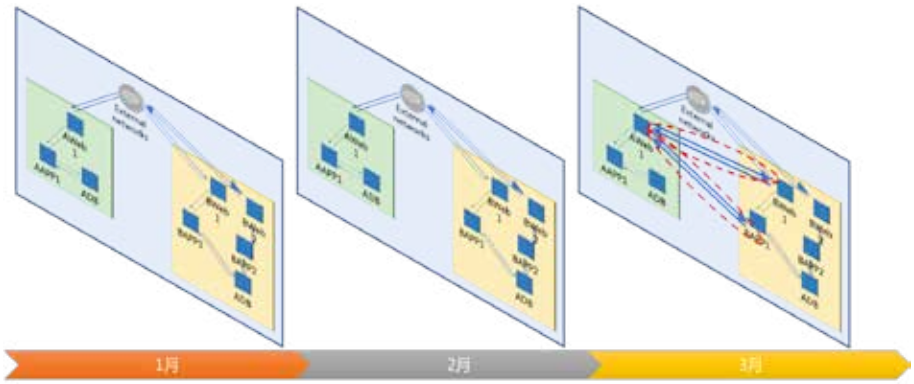


图18，通过长期监测，基于虚机网络行为画像，发现异常通信，挖掘未知威胁和高级持续攻击。

6、策略优化：图16中描述的策略优化，是山石云•格深度可视化能力给予云计算环境的另一贡献，通过可视、分析，而后不断优化NSX和山石云•格的安全策略，实现最优，这是我们将在下一章节中重点阐述的内容。

第五章、NSX 与山石云•格结合使用的方法论

“微隔离、零信任的想法很好，但是我们不知道该如何划分安全域，配置访问控制策略！” 在山石云•格上市的头一年中，我们遇到很多客户询问类似问题。接下来我们将就如何在云中部署微隔离与可视化产品，如何让NSX和山石云•格更优化结合，谈谈实践的方法学问题。

ISO 27001 标准中 PDCA 循环，即计划（Plan）、实施（Do）、检查（Check）、处理（Action）的方法对利用 NSX 和山石云•格实现云计算中心的零信任安全模型是有非常重要的借鉴意义。在 PDCA 循环的基础上，我们将“计划”这一步又拆分为四步，强调了“明确核心资产”、“学习和可视”、“确定最低授权策略” 这三步。我们来看看如何通过 7 步实现零信任安全模型见图 19。在整个过程中，我们需要不断从 NSX 和山石云•格之间调整配置，调整 NSX 和山石云•格的工作“负载”，优化各自策略配置。

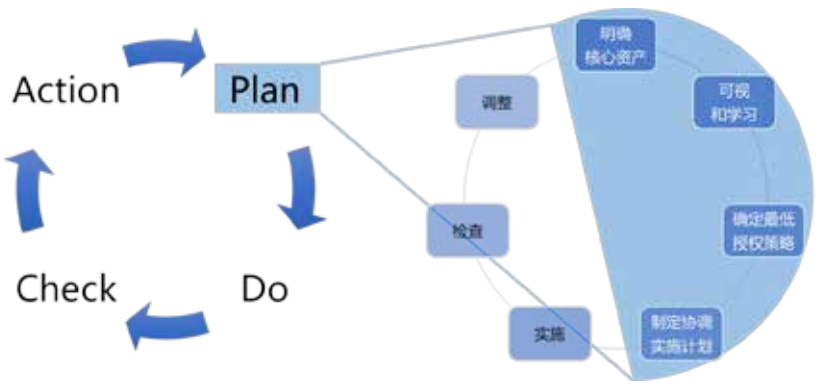


图19，零信任模型如何在云及微隔离产品上实践

第一步，明确云内核心数据资产，是实现零信任安全模型，从内向外设计网络，划分安全域的第一步。在PDCA的循环中，这是一个动态的过程，不要奢望一劳永逸。

最初明确核心资产，可以根据租户、应用系统类型进行初步的划分。

而在其后的PDCA循环过程中，核心数据资产还可以不断细化。如上一章图17阐述的，微隔离和可视化产品，可以围绕核心数据资产划分多维度、细粒度的安全域。所以明确核心数据资产，要考虑更多，不是一蹴而就的过程，需要在多个PDCA的大循环中，不断调整细化。

第二，云计算的优势是快，部署快、调整灵活、弹性好，这意味着云计算中心会面临不断增加新业务系统，业务系统自身内部也在做快速调整。需要不断明确核心数据资产及其安全域边界。

第三，明确核心数据资产，不断通过第二步学习和可视，方面明确安全策略执行，究竟在山石云•格还是NSX上完成，如图16阐述，“好钢用在刀刃”。

第二步，可视和学习，确定MCAP之间的最低授权策略，是实现零信任安全模型中“起承转折”的关键一环。另外，“学习和可视”，也在为在后续PDCA循环中，不断明确核心资产，调整细化安全域边界，做准备。

首先是可视，做到云中的资产可视，资产之间交互关系可视、网络流量可视，网络中的应用可视、威胁可视。

而后是学习，即基于可视化效果，通过学习确定未来要在山石云•格和NSX上部署的最低授权的策略。学习同时也是分析，看到了核心资产之间的通信情况，通过分析，以及求助系统、应用部门，确定哪些是合理的，哪些是问题，哪些是威胁，最终确定白名单的控制策略。

这一步也是一个动态的过程，在多个PDCA循环过程中不断调整可视和学习的焦点，不断细化。

在“可视和学习”阶段，是山石云•格最能体现价值的阶段。对于云数据中心和NSX，山石云•格的作用如同“眼睛”一般。云•格可以做的的工作有：

1、利用山石云格的透视镜功能（DC Visibility）发现核心资产（虚机、网络）之间通信情况，如交互关系、流向、流量、会话数量、时间、应用、威胁。在相关部门的协助下，学习确定围绕核心资产的安全域之间的最低授权策略。
2、利用山石云•格的策略助手，发现已知应用的适配的配置策略，流向、地址、端口、应用控制策略。对于一些定制化应用，还可以通过导出山石云•格的会话日志，确定应用使用的自定义端口号，哪些虚机之间进行通信，以及流向，从而确定在山石云•格上配置适配应用需求的白名单策略。
3、定期输出山石云•格的云内安全报告，或通过日志分析软件，通过长期监控和学习，确定未来安全域调整的思路或最低授权策略。

在多个PDCA循环过程中，山石云•格策略助手产生的策略还是通过日志分析获得的策略，其中可以由2-4层访问控制实现的，都可以逐步部署到NSX上，就如同图16中阐述的思路一样。

在多个PDCA循环中，NSX可以像个显微镜，让山石云•格不断聚焦。比如在最初的PDCA循环中，山石云•格可以聚焦各个应用间交互关系（比如多个端口组（Port Group）间）。而后在下一轮的PDCA循环中，NSX可以在新定义安全组，将一个应用内部虚机（Port Group内）的流量引给山石云•格。第三轮的PDCA循环中，则可把Web与APP虚机特定端口的流量，引给山石云•格，做更深度的可视和学习，如图20所示。

图20，在多个PDCA循环中，NSX将更细致需要可视和学习的流量引给山石云•格

学习和可视也是发现未知威胁和高级可持续攻击的重要手段，正如上一章图17所阐述的。

第三步，确定最低授权策略。

根据学习可视阶段的成果，可以制定接下来的MCAP划分思路、访问控制和防护的策略。把这些策略根据防护的不同要求，划分策略的执行点，是NSX还是山石云•格。

第四步，制定实施的计划，确定最终的实施计划，协调不同部门，实施最终的授权策略。

第五步，实施。

依照前面四步明确的核心资产及其安全域，最低的授权策略，可以分别在NSX和山石云•格上进行实施。整个实施的思路基本上可以参照图16来进行操作。即：

1. 租户间的隔离在NSX上进行配置，利用VXLAN或者VLAN进行隔离。
2. 应用系统间的隔离和2-4层访问控制，可以在NSX或山石云•格上实现
3. 虚机间的隔离和2-4层访问控制，可以在NSX或山石云•格上实现
4. 5-7层的访问控制、攻击防护、恶意文件、代码阻断在山石云•格上配置实现

需要NSX和山石云•格配合实现，即由NSX引流给山石云•格的，主要可以在NSX上设定安全组，引流给山石云•格进行进一步防护（相见山石云•格和NSX的操作配置手册）。

2-4层的访问控制，最终建议还是在NSX上实现，而让山石云•格聚焦在5-7层防护和深度可视上。前期，利用山石云•格上的策略命中统计功能，可以检验前期规划的安全策略是否合理。

第六步，检查

主要是检查隔离、访问控制策略是否起作用，一些安全策略生效之后是否对业务造成了影响。如上面提到的山石云•格的可视化能力，包括策略命中统计功能都可以帮助网络安全管理员进行检查。

第七步，调整

根据检查的结果，对安全策略进行微调，确保防护效果和对业务通信最小的影响。

实施之后，将会回到第一和第二步，一方面检查策略是否实施有效，另一方面是重新审视内部情况，制定下一步的行动计划。我们建议采用一个循序渐进的思路，在云内实现零信任安全模型。

山石云•格提供了云内安全报告的功能，可以按照既定的时间周期，导出云内的安全报告，可以通过安全域划分情况、云内的威胁情况、应用情况、高风险应用的情况，定期对云内部的安全状况进行分析，有针对性的进入到新的PDCA循环中，从而结合NSX和山石云•格调整防护策略。

NSX 和山石云•格结合应用举例

接下来我们结合一个例子来更直观的理解NSX和山石云•格如何配合在云中实现零信任安全模型，如何通过多个PDCA循环实现最优化配置的。

某客户的云计算数据中心中，每个虚机会有两个虚拟网卡，一个连接到业务网络，一个连接到NAS，业务网络有一些初步的网络划分，而在存储侧所有业务虚机都连到同一网段。客户计划部署NSX和山石云•格，对云内安全资产进行全面防护。

通过明确核心资产发现，各种业务网络是多个核心数据资产，情况不清晰，且还有细化的空间。而在存储网络这边情况简单，每个虚机与NAS进行通信，虚机之间没有互访的需求。

在存储网络侧，仅需要虚机间互访隔离，同时存储对网络性能要求高，直接使用NSX执行虚机间微隔离，满足安全隔离需求，同时性能最优。

在业务网络这一侧比较复杂。一些已经运营多年的云计算中心面临的最大挑战是内部不可视，特别是虚机间、应用系统间交互关系不清楚；这些系统间跑哪些应用，使用哪些已知端口或自定义端口不清楚；网络通信中是否有攻击有违规应用，也不清楚。不可视带来的难题是，想实现微隔离，核心资产及其安全域的边界不明晰；不清楚跑哪些应用，调用哪些端口号，无法确定最低授权策略……很多用户既想在内部实现安全，却因不清晰担心安全设备上线后，错误的配置会影响业务的正常使用。

在业务网络这一侧需要经历多个PDCA循环，完成NSX和山石云•格的部署，安全域的划分和调整，最低授权策略的部署和调整优化。在多个PDCA循环过程中，建议分两个大的阶段实施：

第一阶段目标是“明确”。利用山石云•格的可视和学习，明确资产、最低授权策略。可以充分利用山石云•格的“透视镜”、“策略助手”等功能。NSX向山石云•格的引流策略可以较粗，或者选择分区域抽样引流。山石云•格具备云内资产发现功能，配合山石云•格的多维度过滤功能，网络管理员可以区分哪些流量来自云数据中心之外，哪些是内部但未防护的区域。在这一阶段中，既可以勾勒出云内不同业务系统、租户间网络交互的情况，也能及时发现并阻断威胁。

第二阶段目标是优化。逐步将一些经过验证，可以由NSX完成的2-4层访问控制策略从山石云•格上转移到NSX上实施，山石云•格则集中在一些5-7层的安全防护上，实现性能、全面防护的有效结合。

第六章、结束语

山石云•格与VMware NSX产品的结合，给出了SDN类的微隔离产品和深度微隔离和可视化产品结合使用的最佳范例。

SDN产品提供了维护管理的高效率、网络的健壮性可用性、以及内核级的高性能处理。而山石云•格则是整个系统的眼睛，充分发挥深度可视的作用，协助网络安全管理员明确核心资产，明确交互关系、应用情况和网络中的威胁。在可视的基础上，网络管理员可以明确最低授权的策略，并确定哪些隔离防护工作由SDN微隔离产品承担，哪些由山石云•格承担更合理。或者说，在哪个时间段里由山石云•格先承担，随着时间的推移，可以逐步转移由SDN微隔离产品承担，山石云•格最终聚焦在5-7层防护和可视上。

希望本篇白皮书能够起到抛砖引玉的效果，广大云数据中心网络安全管理人员能在日常运营管理中充分发挥SDN微隔离产品和山石云•格的优势。也希望广大网络安全管理人员分享给我们您使用中的心德、建议，我们不断完善产品，与大家一起共建安全的云计算空间。

术语简写

API	Application Programming Interface
APP	Application
APT	Advanced Persistent Threat
CRM	Customer Relationship Management
DDOS	Distributed Denial of Service
DOS	Denial of Service
DFW	Distributed Firewall
DPDK	Data Plane Development Kit
HA	High Availability
HDDC	Hardware Defined Data Center
IP	Internet Protocol
IAAS	Infrastructure as a Service
KVM	Kernel Virtual Machine
MCAP	Microcore and Perimeter
NAV	Network Analysis and Visibility
NFV	Network Functions Virtualisation
NGFW	Next Generation Fire Wall
NTA	Networktraffic analysis
OVS	Open vSwitch
PDCA	Plan Do Check Action
RestAPI	Representational State Transfer API
SDDC	Software-Defined Data Center
SDN	Software-Defined Networking
SDS	Software Defined Security
SFC	Service Function Chain
SIEM	Security Information and event Management
SOA	Service-Oriented Architecture
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
UEBA	User and Entity Behavioral Analytics
UTM	Unified Threat Management
VDC	Virtual Data Center
vDSM	Virtual Data Service Module
VIM	Virtualised Infrastructure Manager
VM	Virtual Machine
VNF	Virtualised Network Function
vSCM	Virtual Security Control Module
vSOM	Virtual Security Orchestration Module
vSSM	Virtual Security Service Module
VXLAN	Virtual eXtensible LAN

文档编号：EX-08-CLOUD-5.5R2-1017-Ch-01