基于SDS的虚拟化数据中心安全探讨

Discussion on the Security of Virtualized Data Center Based on SDS

李姗姗，李　涛（中国联通网络技术研究院，北京 100048）
Li Shanshan，Li Tao（China Unicom Network Technology Research Institute，Beijing 100048，China）

摘　要：
传统的安全防护措施因其静态、僵化的防护策略，不能再应对虚拟化给数据中心带来的新的安全挑战。通过分析虚拟化安全风险类型，明确了虚拟化环境下安全防护需求，结合当前虚拟化安全防护技术发展现状，提出了一种基于SDS的虚拟化数据中心安全解决方案，实现了在多租户虚拟化环境下对虚拟资源的精细、高效、灵活和可扩展的安全防护目标。

关键词：
虚拟化；数据中心；软件定义安全
doi：10.12045/j.issn.1007-3043.2019.04.015
中图分类号：TN915.08
文献标识码：A
文章编号：1007-3043（2019）04-0067-04

Abstract：
Traditional security measures are no longer adapted to the new security challenges brought by virtualization to data centers due to their static，rigid protection strategies. By analyzing the types of virtualization security risks，the security protection requirements in the virtualized environment are clarified. Combined with the current development status of virtualization security protection technologies，the virtualized data center security solution based on SDS is proposed to realize a fine，efficient，flexible，and scalable security protection goal for virtual resources in the multi-tenant virtualization environment.

Keywords：
Virtualization；Data center；SDS

引用格式：李姗姗，李涛. 基于SDS的虚拟化数据中心安全探讨[J]. 邮电设计技术，2019(4)：67-70.

1 概述

近年来，随着IT技术的不断演化与发展，传统的数据中心正在逐步向虚拟化数据中心（VDC——Virtual Data Center）转型。虚拟化数据中心是一种利用云计算架构，将虚拟化技术运用于数据中心的一种新型的数据中心形态。VDC通过将物理资源抽象整合，动态地完成资源分配和调度，实现了数据中心的自动化部署，提高了资源的利用率和部署的灵活性，同时极大地降低了数据中心的建设成本。

虚拟化技术的引入，在改变传统数据中心架构的同时，也给安全防护带来了新的挑战，如资源共享引发的网络安全边界模糊、虚拟机之间流量不可见等问题，因此虚拟化安全风险防护是虚拟化数据中心安全的核心所在。近年来，软件定义安全（SDS ——Software Defined Security）不断发展，其利用软件编程的方式对安全资源进行灵活的业务编排、调度和管理，为虚拟化安全防护技术的发展注入新活力。

收稿日期：2019-03-01

2 虚拟化数据中心简介

2.1 虚拟化数据中心架构

虚拟化数据中心利用虚拟化技术将计算、存储和网络3种资源虚拟化为一个完整的、弹性化的基础设施资源池，从而实现底层物理设备与逻辑资源的解耦。在该资源池内，物理设备与网络链路不再单独地存在与使用，而是作为整个资源池内的一部分进行统一动态的管理与调度，实现数据中心的自动化部署，对用户实现按需分配与服务，提高了资源交付的灵活

性和资源的利用率,降低了数据中心的建设成本。

2.2 虚拟化数据中心面临安全挑战

由于虚拟化数据中心采用全新的服务计算模式、动态虚拟化管理方式和多租户共享运营模式,所以在传统安全风险基础上,面临更多安全挑战。

2.2.1 虚拟环境安全风险

a)逃逸风险:攻击者突破虚拟机管理器Hypervisor,获得物理机host的管理权限,并控制host上运行的其他虚拟机,这被称为VM Escape。攻击者在获得物理机管理权限后,既可以攻击同一host上的其他虚拟机,也可控制所有虚拟机对外发起攻击。VM Escape是虚拟化环境中最严重的安全威胁。

b)迁移攻击:将虚拟机从一台host迁移到另一台。在虚拟机迁移的过程中,虚拟磁盘会被重新创建。攻击者通过改变虚拟机磁盘的源配置文件和相关特性来打破其中的安全措施,如密码、重要认证等。

c)安全补丁风险:同一host上有多个VM时,每个VM需要对补丁进行定期的更新和维护。若个别VM不能及时补漏,则会成为严重的安全漏洞,被攻击者加以利用。

d)资源抢占风险:由于同一物理机下的虚拟机共享底层硬件资源,若某一台虚拟机因受到攻击或被非法利用对host的资源进行恶意抢占,从而使其他虚拟机资源严重不足而影响其正常运行。除此之外,资源抢占还会降低同一host下虚拟机的密度,导致成本的增加。

2.2.2 虚拟机软件自身安全风险

构建虚拟化环境的软件是直接运行在裸机上的,提供创建、运行和销毁虚拟机的能力,但其本身也可能存在安全漏洞;攻击者利用这些安全漏洞进行攻击,将会造成不可估量的后果。目前市场上已经出现了多款针对虚拟化层的恶意攻击软件,如RedPill、BluePill、SubVirt等。

2.2.3 虚拟化网络安全风险

在虚拟化网络环境下,大二层扁平网络结构虽然解决了低效路径、带宽利用率低等问题,但若配置不当,可能会引起广播风暴、MAC表剧增等安全问题。同时,由于同一host内VM间的流量对外不可见,传统的安全防护措施难以监控东西向流量,这就导致VM间的攻击不易被发现和防范。

2.3 虚拟化数据中心安全防护需求

通过对虚拟化安全风险分析,虚拟化数据中心的安全防护需求应包括以下4个方面。

a)防范来自外部的威胁(如DDoS、SQL注入等)和非授权访问,即南北向流量安全防护。与传统南北向流量安全防护相比,在虚拟化环境下,用户需求更复杂,对设备的虚拟化程度要求更高,因此对南北向流量防护提出了新的技术要求。

b)防范VM之间的安全威胁和非授权访问,即在虚拟化环境下产生的东西向流量安全问题。

c)提供东西向、南北向流量的安全防护措施,相关安全策略可支撑资源的灵活加入、离开或迁移,提升安全管理能力。

d)提供保护虚拟化系统及管理平台的安全防护能力。

3 虚拟化安全防护技术

3.1 基于Hypervisor的安全防护技术

基于Hypervisor的安全解决方案以虚拟化厂商及传统防病毒厂商为代表。在虚拟化层Hypervisor引入安全虚拟机,安全虚拟机可以实现防火墙、防病毒等各种安全功能。安全虚拟机通过调用Hypervisor对外开放的API,对虚拟机的数据流量及资源使用情况进行监控,从而实现安全防护功能。

基于Hypervisor的安全防护技术不适合多租户应用场景,同时由于安全虚拟机和被监控虚拟机共享host,存在资源性能瓶颈。

3.2 基于网络虚拟化的安全防护技术

基于网络虚拟化的安全解决方案以网络设备/安全设备制造商为代表。将网络安全硬件设备虚拟化,具有一定软件可编程能力;同时与底层虚拟交换机进行耦合,通过二层网络或隧道方式,将被监控的虚拟机流量重定向到虚拟化的安全防护产品进行检测。

基于网络虚拟化的安全防护技术当前局限于网络层面的安全防护,4至7层的安全防护还有待提升。

3.3 基于SDS的安全防护技术

SDN和NFV技术的出现为虚拟化安全防护带来了新的发展机遇。SDN架构具备的控制与转发分离、开放可编程等优良特性,使SDN控制器具备了全局视野,可以为各个防护对象和数据流标记各种安全属性;NFV技术通过对软硬件解耦,能快速为虚拟化环境部署各种类型的安全资源。结合SDN和NFV 2种技术优势,业界提出软件定义安全即SDS的概念,其原理是利用虚拟化技术,将底层的物理资源抽象成安全

能力，形成安全资源池，并通过软件编程的方式根据业务需求进行安全服务能力编排和管理，完成定制化的安全功能，从而实现一种弹性、灵活的安全防护。

综上分析，基于Hypervisor和基于网络虚拟化的安全防护技术都是通过提升网络与虚拟化层的安全感知能力，并将安全防护延伸到虚拟化层面，实现更精细化的安全防护，仍属于传统安全防护解决方案；而SDS技术及理念的兴起，使虚拟化安全防护技术有了全新的突破。

4 基于SDS的虚拟化数据中心安全解决方案

4.1 基于SDS的虚拟化数据中心安全架构

基于SDS的虚拟化数据中心安全架构利用虚拟化技术，将安全资源抽象为安全资源池，依托安全控制管理模块，借助可编程能力，将安全功能模块化，并根据用户的个性化需求，抽象形成虚拟安全服务网关，进行灵活安全控制，最终实现了软件定义安全的思想，即控制和数据分离，逻辑和实现分离。具体架构如图1所示。

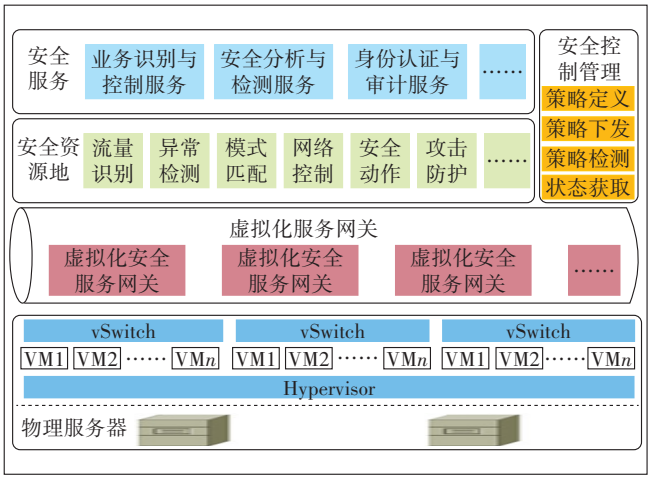

图1　基于SDS的虚拟化数据中心安全架构

a）安全控制管理模块：用于获取相关安全状态，根据用户的需求定义和维护安全策略，同时对安全策略进行检测和下发。

b）虚拟化安全服务网关：利用虚拟化技术，将安全资源池内的相关资源按需抽象为各种类型的安全服务网关，为用户提供所需的安全防护功能。安全服务网关通过不同的部署方式，对数据中心内外通信的南北向流量和内部通信的东西向流量进行防护。

c）安全资源池：安全资源池提供各种类型的安全资源，为虚拟化安全网关提供相应的物理资源基础。

d）安全服务：根据实际的资源，为用户提供多种不同类型的安全服务，使得用户可以根据自身需求，定制包括业务识别与控制、安全分析与检测、身份认证及审计等定制化安全服务。

4.2 基于SDS的虚拟化数据中心安全防护模型

基于SDS的虚拟化数据中心安全架构中，通过调整虚拟化安全服务网关的部署方式，能够提供可靠、灵活和全面的安全防护。下面针对虚拟化数据中心南北向流量和东西向流量不同的安全防护需求，分别介绍以下2类安全防护模型。

4.2.1 基于SDS的南北向流量防护模型

在南北向流量防护过程中，虚拟化安全服务网关部署在边界位置。根据租户需要，可为其创建并分配独享的虚拟化安全服务网关，也可以多个租户共享一个虚拟化安全服务网关。不同的虚拟化安全服务网关在逻辑上相互独立，互不影响。因此，当虚拟安全服务网关为租户独享模式时，可以由租户按需自行管理安全服务网关，自主配置安全策略，这种方式既减轻服务提供商的维护工作量，也满足了不同租户的独立管理需求；当安全服务网关为共享模式时，可以降低服务提供商的成本，从而实现资源的灵活配置和高效利用。南北向流量防护模型如图2所示。

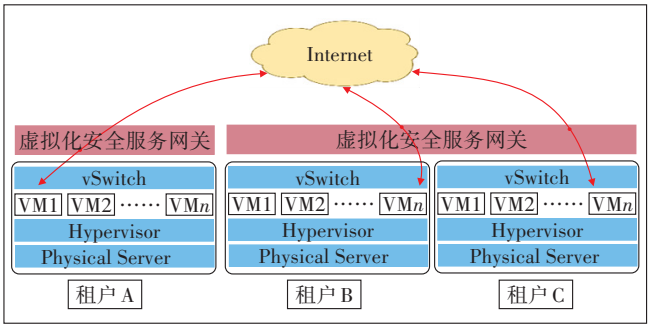

图2　基于SDS的南北向流量防护模型

4.2.2 基于SDS的东西向流量防护模型

随着SDN和NFV技术的发展，在虚拟化数据中心东西向流量防护过程中，各个虚机之间的流量不仅局限于同一台主机内部，更多的是不同主机上虚机之间的通信需求，因此为了提供更完善的东西向流量防护，部署如图3所示的防护模型。

对基于SDS的东西向流量防护模型进行详细解析，其防护流程如图4所示。

a）定义安全防护策略。用户根据自己的实际需

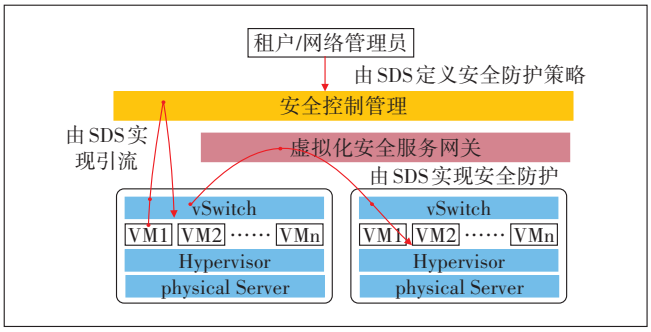

图3　基于SDS的东西向流量防护模型

求，对需要监控和检测的虚拟机之间的流量进行策略定义。可根据IP五元组、MAC地址信息或虚拟机上的属性（如名字、性能等）进行精细化定义，并根据防护策略，配置东西向流量在经过安全网关时的动作，如accept、drop或reject等。

b）实现引流。当vSwitch在接收到虚拟机生成的第1个数据包后，自动将该包上报至安全控制管理模块；根据预先定义的安全防护策略，安全控制管理模块将安全防护策略下发到vSwitch；vSwitch基于接收到

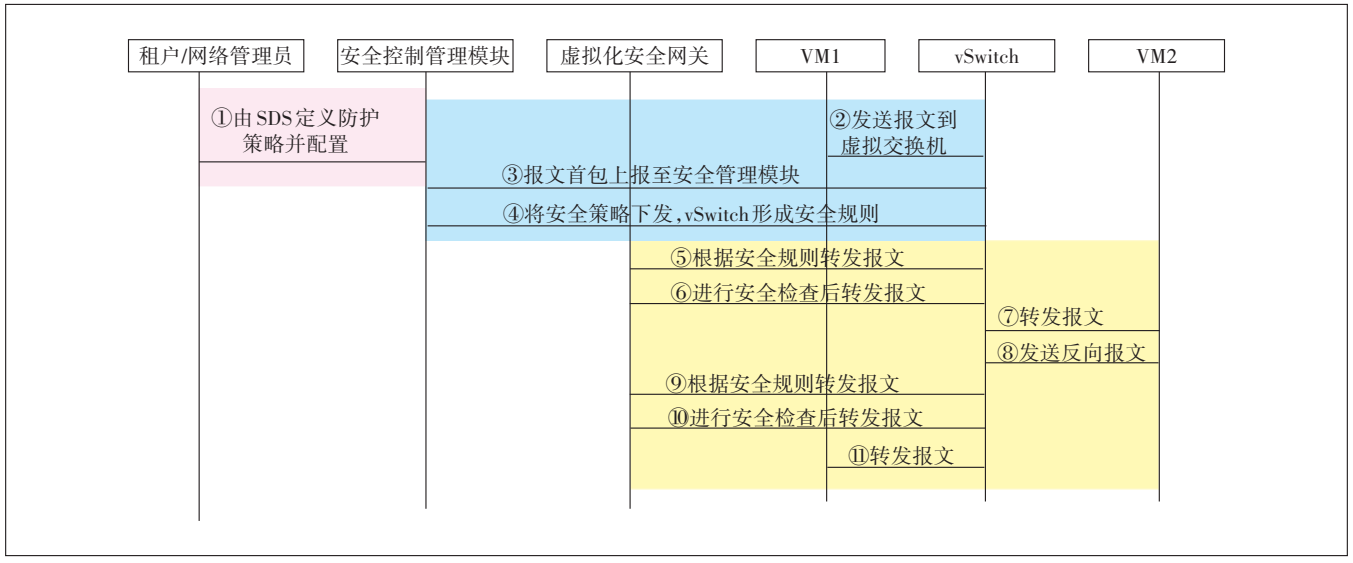

图4　基于SDS的东西向流量防护流程

的安全策略，形成相应的安全转发规则；后续报文将根据安全转发规则决定是否对数据包进行安全检查。

c）实现安全防护。利用NFV技术将安全资源抽象成各种安全能力，用户根据实际需求，对安全能力灵活编排，形成提供不同安全能力的虚拟化安全网关。当流量经过虚拟化安全网关时，根据安全策略，自动完成各项安全检查，执行相关安全动作；通过安全检查的流量将被转发至目的虚拟机。

d）实现策略迁移。当安全管理模块检测到虚拟机迁移后，会自动将以该虚拟机为源或目的节点的流转发策略转移至新的接入或上行端口，同时自动更新相关安全策略，保证安全防护规则随虚机的迁移进行动态自适应。

5　结束语

随着云计算的不断发展，虚拟化在数据中心中的应用越来越普遍，与之相关的安全防护能力也不断演进。本文基于SDS理念，提出了一种基于SDS的虚拟化数据中心安全解决方案，给出了基于SDS的虚拟化数据中心安全架构及安全防护模型。该方案基于SDN和NFV技术，形成可定制的安全服务网关，灵活地满足不同用户的安全防护需求，具有较好的可扩展性，同时为后续数据中心安全防护建设提供参考。

参考文献：

[1]　李知杰，赵健飞. 云计算数据中心网络安全的实现原理[J]. 软件导刊，2011，10(12)：135-136.

作者简介：

李姗姗，工程师，硕士，主要从事IT规划、大数据挖掘等研究工作；李涛，教授级高工，硕士，中国人工智能学会高级会员，主要从事人工智能、能力开放、IT规划等方面的研究。