



专栏：云网智联，万物在线

公有云大规模资源池部署 SDN 的应用

月球, 刘芹, 杨小乐, 毕晓飞, 朱师萱

(中国移动通信集团设计院有限公司, 北京 100080)

摘要: 基于 SDN 的云计算数据中心网络方案是未来数据中心网络发展的趋势。对目前移动运营商网络中, 应用 SDN 组网技术并且已成功上线的优秀应用案例进行探讨, 此案例同时也是全球运营商最大的 SDN 商用案例之一。同时结合现网运行情况总结出云数据中心大规模部署 SDN 时需要考虑的关键问题及引入步骤, 可为后续 SDN 网络架构部署在其他云计算资源池及 NFV、5G 中提供一定的参考、借鉴。

关键词: 云计算; 公有云; SDN; 案例分析

中图分类号: TN915

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018197

Application of SDN deployment in large-scale public cloud across different resource pools

YUE Qiu, LIU Qin, YANG Xiaole, BI Xiaofei, ZHU Shixuan

China Mobile Group Design Institute Co.,Ltd, Beijing 100080, China

Abstract: The SDN-based network solution for cloud computing data center is the trend of future data center network development. For the current mobile operator network, the outstanding application case where SDN network technology has been applied and successfully launched was discussed. The case was also one of the largest SDN commercial cases among global operators. The key issues and introduction steps for the large-scale deployment of SDN in cloud data centers were summarized based on the current network operating conditions, which could provide the reference for SDN architectures deployment in other cloud computing resource pools such as the NFV and 5G network.

Key words: cloud computing, public cloud, SDN, case analysis

1 引言

云计算市场作为移动互联网时代信息化的重要战略市场, 已经成为互联网、IT 服务商与传统电信运营商的必争之地。

全球公有云服务市场在未来的几年内将保持高速发展, 国内运营商在云数据中心的建设步伐

也在加快推进, 如中国电信已把内蒙古自治区和贵州省的天翼云平台推向了 31 个省市, 中国联通已经布局大型的云数据中心 12 个、地市数据中心 335 个, 中国移动也宣称将从内环、中环、外环 3 个方向构建开放生态系统。

随着云计算数据中心的建设规模越来越大, 客户的个性化需求越来越强烈, 现有的网络技术

收稿日期: 2018-04-23; 修回日期: 2018-05-30



如何更好地满足业务需求，是亟待解决的重要问题。一个更加灵活、更加高效集中的网络成为网络发展的新方向。为解决新型网络下新市场的需求，在数据中心中应用 SDN 技术组网成为各国运营商普遍的解决方案^[1]。

SDN 是随着业务发展需求应运而生的新型创新网络技术，其原理主要在于将控制面的功能从原有的一体化架构中抽离出来，实现控制与数据转发解耦，最终分为三层彼此分离的网络模型：应用层、控制层和转发层。SDN 架构实现网络自动化和可编程性、缩短部署时间、支持安全与策略执行以及提高网络运维人员工作效率的能力，已在多个数据中心得到了验证。SDN 能降低人工错误的概率，同时减少运营开支^[2]。

SDN 还能减少未来 5G 新物联网项目中的棘手问题，如在部署智能设备、工业传感器等终端时，给企业网络带来无数新的端点。人工设置与配置耗时、容易出错，并且无法将物联网设备和应用程序集成到网络中。SDN 的自动化和可编程性应在保证安全的前提下实现物联网设备的自动配置和访问策略的自动执行，无需任何人工干预。最近出现的僵尸网络攻击表明，物联网安全策略的实施存在许多问题，一旦出现漏洞会造成严重的后果^[3]。

SDN 市场的年复合增长率为 53.9%，由于简化了数据中心网络管理流程，并加快了整个基础架构构建，SDN 在世界各地的数据中心取得成功。这种增长预计将持续到 2020 年，预计其市场价值近 125 亿美元。

本文对目前移动运营商网络中，云数据中心应用 SDN 组网技术并已成功上线的优秀应用案例之一进行探讨，并结合现网运行情况总结出云数据中心大规模部署 SDN 时需要考虑的关键问题。为后续 SDN 网络架构部署在其他云计算资源池及 NFV、5G 资源池部署提供一定的参考和借鉴。

2 现网案例

2.1 公有云大规模部署 SDN 情况

以某移动运营商公有云建设为例，国内两大基地资源池分别部署 2 000 台计算服务器，以 OpenStack 云平台结合 SDN 实现业务的自动化发放为建设目标，完成业务上线时根据用户在云平台上的逻辑组网设计由 SDN 控制器自动化地打通端到端网络的各个环节所需下发的配置，为公众服务云提供弹性计算、弹性网络、弹性负载均衡、弹性安全等业务服务能力。为完成并增强各资源池提供云服务能力，能够快速对所属资源及能力进行自动化发放。

SDN 网络逻辑分为 4 层架构：应用层、协同层、控制器和转发层，如图 1 所示。应用层由业务和应用软件组成，通过软件来衡量网络资源，实现优化和全局调度。协同层即云操作系统，此处为 OpenStack，用于联动计算、存储、网络资源，与控制器以及网络增值设备（如负载均衡设备或防火墙设备）通过 VNFM 采用 plugin 对接。控制层包括控制器，由控制器接收上层业务请求，并转发为转发层的流表，配置到转发层网元。转发层指各种转发设备，SDN 转发设备接收控制器下发的流表，实现租户隔离、二三层业务转发、负载均衡、防火墙访问控制功能。

此场景下，网络分为底层（underlay）网络和 SDN 重叠（overlay）网络。underlay 网络不属于 SDN 集中控制范围，它包括非 SDN 接入交换机和核心交换机，将服务器、SDN 网关、增值业务网元 IP 地址连通。overlay 网络是 SDN 集中控制范围，包括虚拟交换机、SDN 网关、NAT、增值业务网元（包括防火墙、负载均衡器）等，为不同租户提供隔离的 VPC 网络服务。本案例中公有云资源池大规模 SDN 的部署基于 VxLAN 封装技术的 overlay 架构，即在 IP 网络上叠加虚拟的网络，实现网络松耦合、业务自动开通，网络具备规模

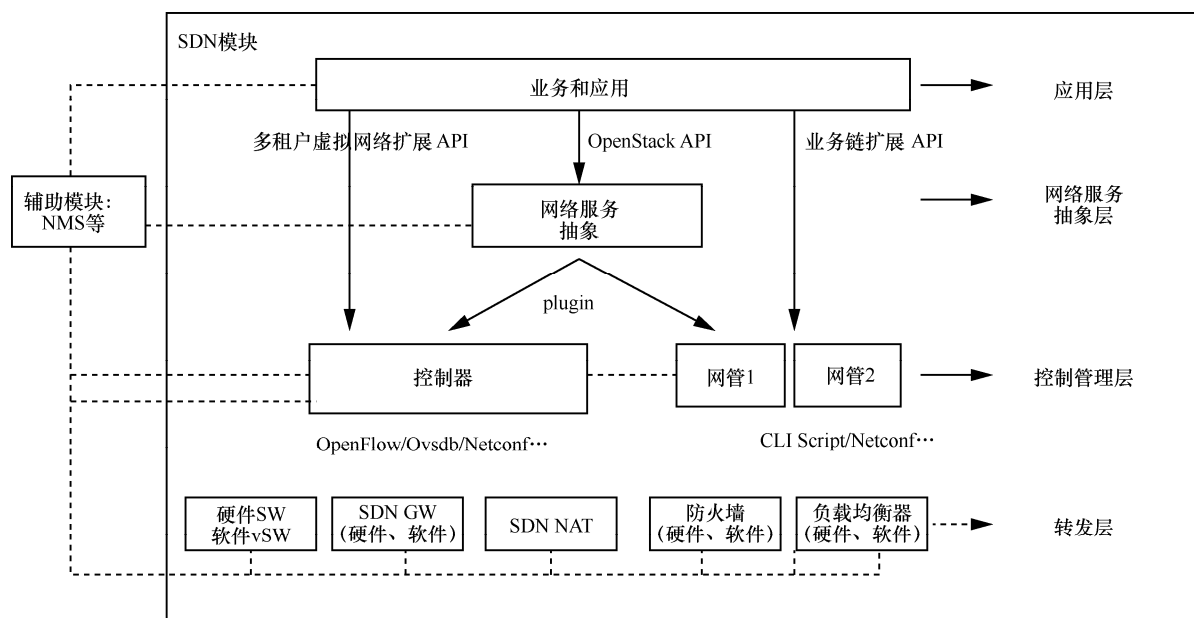


图1 SDN 软件架构

扩展的能力。具体架构主要包括以下两类。

- SDN 转发设备：虚拟交换机、SDN 硬件交换机、SDN 网关、分布式防火墙。
- SDN 控制设备：SDN 控制器，按需创建虚拟网络，完成业务实现和流量调度功能。

本案例中具体组网如图2所示。

目前两大基地公有云均已上线，运行稳定，并且由于SDN技术的引入，解决了许多原有的网

络问题。

2.2 解决的问题

(1) 解决了原有网络 VLAN 数量限制问题，实现跨越二层网络^[4]

基于 VxLAN overlay 的 SDN 支持 overlay 的灵活三层网络，实现云主机网络的可迁移性和隔离性，在 SDN 配置下，云主机能够自动迁移至新的宿主机维持原有 IP 地址，即基于三层方式的

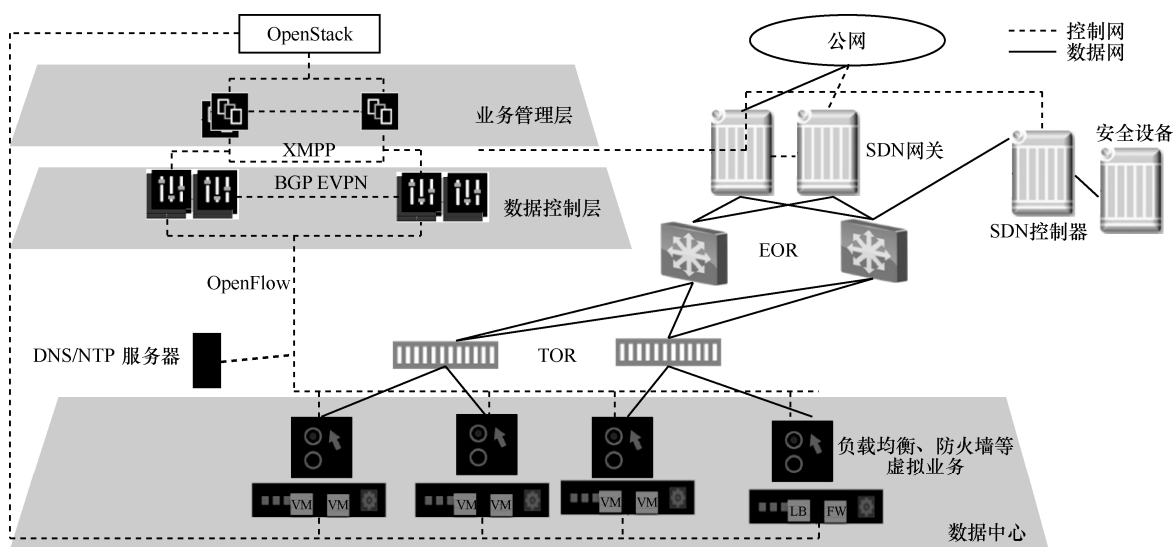


图2 公有云 SDN 组网示意



底层网络构建虚拟二层网络。同时，由于引入 VxLAN 技术扩展了新的标识符，未来可以提供超过 1 600 万个 VxLAN 网络，满足未来二层隔离的需求。

(2) 解决东西向流量迂回问题，简化流程^[5]

本案例中采用 overlay SDN 技术，提供东西向流量扁平化和东西向流量隔离功能。

东西向的流量不需要绕行三层交换机而直接通过三层分布式路由虚拟交换机（VRS）本地路由实现，可通过流表直接进行二三层转发，无论是东西向相同的主机还是东西向不同的主机，都减少了路由跳数，如图 3 所示。

(3) 产品快速上线，解决维护问题

SDN 的主要组成部分是使用应用编程接口（API）实现网络与安全设备、基础架构和应用程序之间的通信和集成。API 还能实现针对业务目标的网络应用程序的本机开发，从而避免网络团队与软件开发团队“各自为政”的问题。API 最终可以通过缩短维修时间加快创新速度，并且不影响安全性。

公有云未部署 SDN 之前，新增业务需求需要经过新业务需求→网络能力评估→网络配置实施→网络配置验证→业务部署→业务上线等流程，即使中间过程绝对顺利，不存在任何人工交接时延，全部过程也需要至少 15 天；而应用了 SDN 后，

所有操作自动化实现，避免了人工操作可能存在失误的情况，实现业务开通端到端的网络自动化打通，业务上线可在一天内实现。

(4) 云网互联，使得公有云具备未来扩展为混合云的能力

通过 SDN 技术，未来可通过专线及多种 VPN 技术，打通与私有云、传统数据中心的互联及组网，形成混合云网络解决方案，如图 4 所示。

3 公有云资源池中大规模部署 SDN 时需要考虑的关键问题

3.1 SDN 的应用场景

对于网络中是否需要引入 SDN 技术，需要分别分析。本案例中，除了在全虚拟化的云数据中心部署 SDN 外，其他适合 SDN 引入的场景主要有如下几种。

(1) 半虚拟化数据中心的 SDN 部署

此场景下，可通过在未虚拟化环境边缘部署 SDN 虚拟业务网关，完成非虚拟化环境的 SDN 扩展，以突破人工网络配置瓶颈、提升 IT 人员网络配置效率；实现网络的多租户化；解决 IP 地址复杂性及东西向流量问题；并提供基于运营商模式的统一运维管理功能。半虚拟化数据中心的 SDN 部署如图 5 所示。

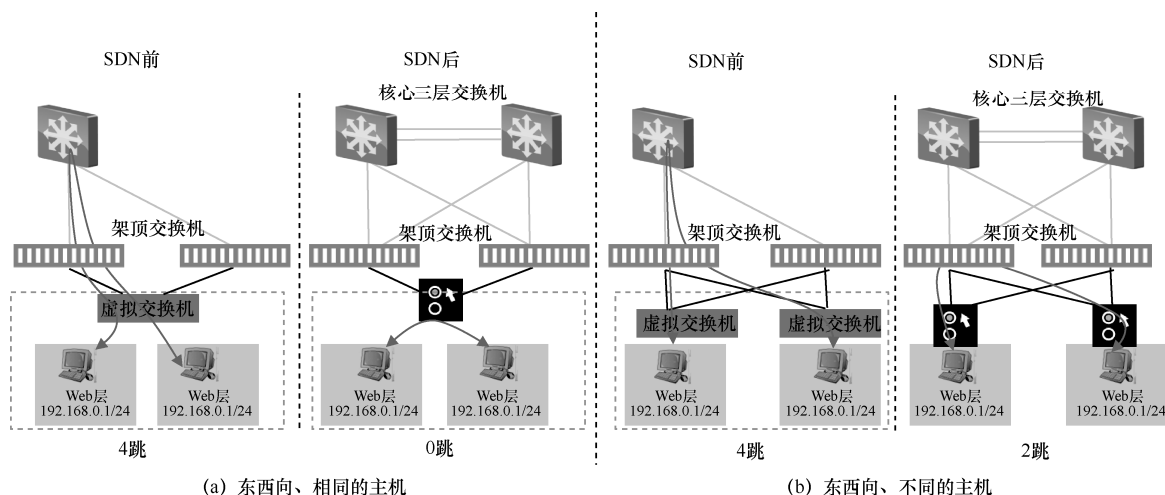


图3 引入SDN组网前后的流量变化

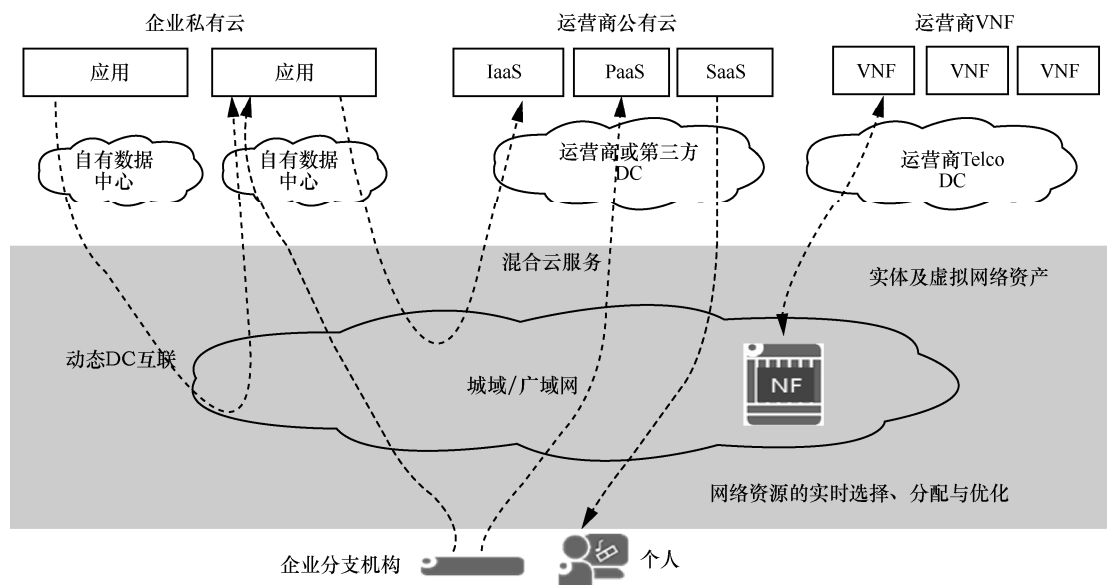
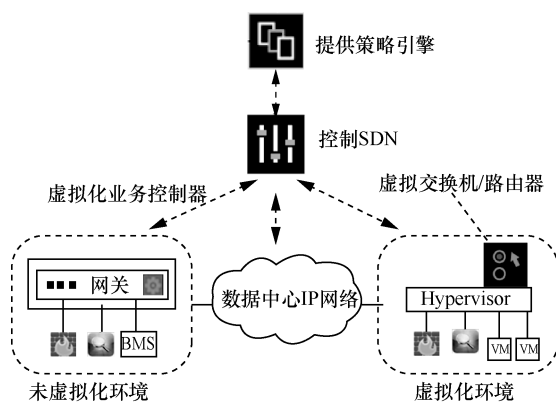
图4 SDN 可实现未来混合组网^[6]

图5 半虚拟化数据中心的SDN部署

(2) 跨数据中心的SDN部署：可连接不同虚拟化平台的异构网络

SDN技术可实现大二层数据迁移，因此可应用在需要数据中心互联的场景下。适用于不同平台数据中心的SDN整合，可屏蔽底层网络，不对现网组网模式、现有设备进行大量调整，并充分保护现有设备资源投资，同时在虚拟机迁移时自动实现网络的适配。跨数据中心的SDN部署如图6所示。

(3) 非云化数据中心中的部署^[7]

非云化数据中心存在机架碎片问题，即机架

利用率在70%，机架出租利用率低。此时可通过SDN架构对系统进行改造，实现多数据中心互联，盘活数据中心的机架“碎片”。多数据中心采用统一的出口网关进行流量计费和QoS控制。对于租户的调整（退场、进场、IP地址规划、网络规划的调整），简化原来逐个配置交换机的形式，改为通过统一界面下发策略来实现，避免大量的IDC内部交换机、路由器的数据调整。SDN解决非云化数据中心的碎片问题示意如图7所示。

3.2 SDN引入时关注的问题

当根据不同数据中心场景决定引入SDN后，部署SDN需要首先考虑的是，选择overlay还是underlay架构。

underlay架构需要沿途每一跳支持硬件SDN架构，即用SDN交换机替换现有的所有交换机和路由器，适合规模较小（仅支持几百台设备）数据中心，由硬件交换机需要负责所有虚拟机的通信。目前支持的厂商有Cisco（思科）、华为和新华三等硬件交换机厂商。

overlay架构即软件叠加架构需两端的交换机

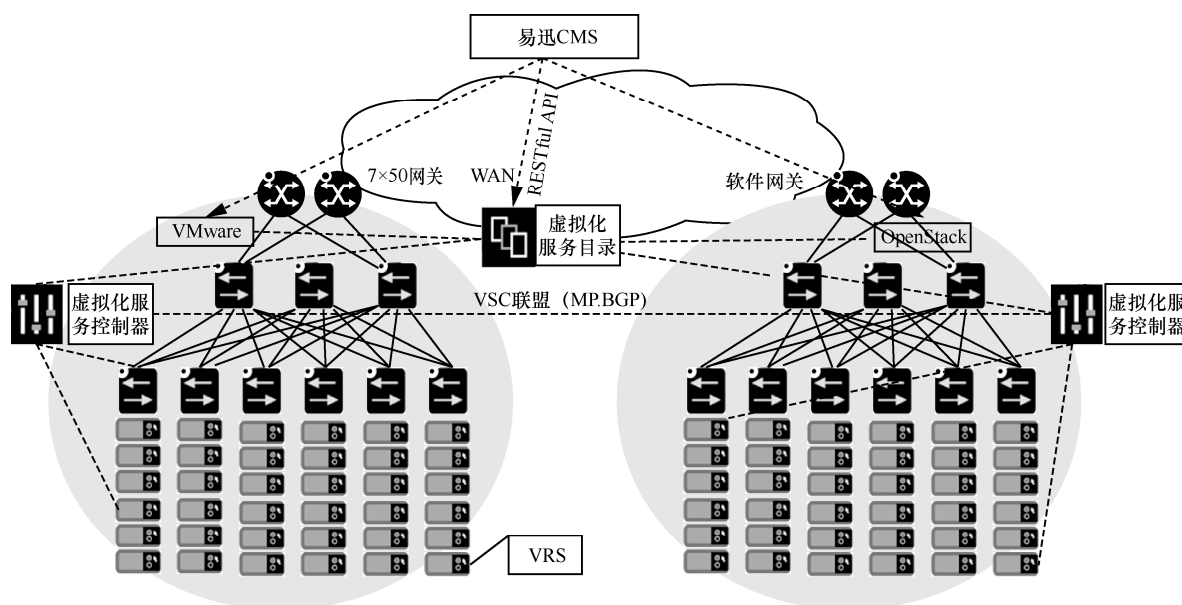


图6 跨数据中心的SDN部署

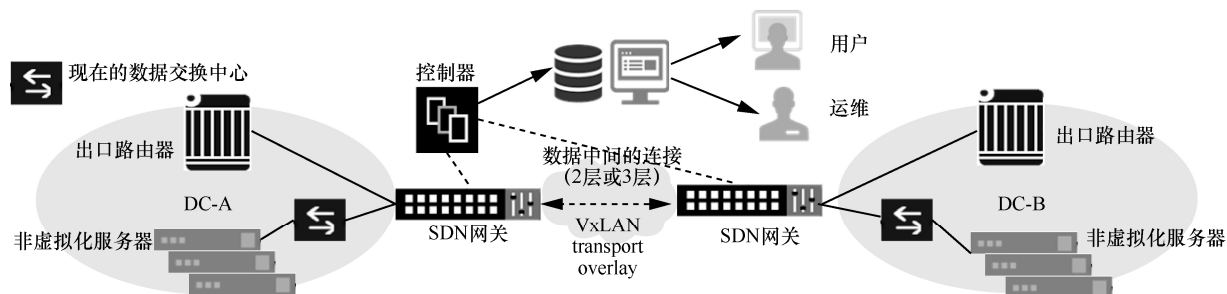


图7 SDN解决非云化数据中心的碎片问题示意

软件支持虚拟化，新增实现东西向三层互通的分布式路由器/交换机，通过隧道透传中间流量。可保留现网已有的交换机、路由器，支持规模较大的数据中心。目前支持的厂商有上海贝尔、VMware等。

由于overlay架构基于软件叠加可保护现有投资、性能也可满足目前及后续发展需要，是业界主流SDN架构。

此外，在引入SDN时，需根据不同需求考虑SDN控制器的工作方式及设备管理能力，并充分验证SDN解决方案与虚拟化平台、负载均衡、防火墙等的兼容性，统筹考虑引入合适的SDN解决方案。主流SDN厂商SDN控制器见表1，主流

SDN厂商SDN解决方案见表2。

目前SDN软件方案需部署vSwitch在计算节点服务器内，故SDN需要与虚拟化平台兼容。

SDN对不同虚拟化平台支持的成熟度不同，其中KVM和VMware平台具备商用条件，XEN平台成熟度低。SDN与虚拟化平台兼容性见表3，其中阿尔卡特朗讯简称阿朗。

在部署SDN方案时，还需要考虑SDN控制器和防火墙/负载均衡器的兼容性。

公有云中租户多，且每个租户对LB/FW的性能要求不高，可以考虑部署vLB/vFW，有利于不同租户的业务隔离。SDN与防火墙负载均衡的兼容性见表4。

表1 主流SDN厂商SDN控制器

	VMware	上海贝尔	华为	新华三	
控制器工作模式	集群	集群	集群	集群	
工作方式	节点规模	3/5	单集群 2 个，可扩展 250 个集群	2	32
设备纳管能力	单个控制器可纳管设备数量	N/A	1 000（虚拟交换机）	1 000（虚拟交换机）	1 000（虚拟交换机）
	控制器纳管网元类型	Open vSwitch, NSX vSwitch	虚拟交换机、软件网关、硬件网关 VSG、白盒设备	OVS、EVS、华为 CE 交换机	华三 vSwitch、华三软硬件网关、华三交换机
负载分担		支持	支持	支持	支持
高可用		支持	支持	支持	支持

表2 主流SDN厂商SDN解决方案

供应商	解决方案类型	支持云平台类型	虚拟化平台
上海贝尔	软件 overlay	OpenStack, CloudStack, VMware	XEN, Hyper-V, KVM, EXSI
华为	硬件 underlay	OpenStack, CloudStack	屏蔽虚拟化平台
新华三	软件 overlay & 硬件 underlay	OpenStack, VMware	KVM、EXSI
VMware	软件 overlay	VMware	EXSI

表3 SDN与虚拟化平台兼容性

	KVM 平台	VMware 平台	XEN 平台
厂商支持情况	阿朗、新华三、华为、赛特斯、中兴、Juniper、VMware	新华三、阿朗、华为、赛特斯、VMware	Citrix: 阿朗 Suse: 新华三 华为: 华为
SDN 业界商用情况	腾讯云: 新华三 阿里云: 新华三、华为 联通公有云: 华为	电信公有云: 阿朗	

表4 SDN与防火墙负载均衡的兼容性

SDN 厂商	负载均衡器	防火墙
阿朗	开源、Brocade, 软件 (vLB) 形式	Brocade, 软件 (vLB) 形式
新华三	新华三, 软件 (vLB)、硬件 (LB) 都有	新华三, 软件 (vLB)、硬件 (LB) 都有
华为	F5, 硬件 (LB) 形式	华为, 硬件 (LB) 形式
中兴	A10, 硬件 (LB)	山石, 软件 (vLB)、硬件 (LB) 都有
其他厂商	开源, 软件 (vLB) 形式	开源, 软件 (vLB) 形式

3.3 部署SDN时的云安全问题

在构建云时,除了计算、网络和存储,安全也是极其重要的问题。

如果云资源池被外网攻击通常不会成为严重

问题,因为完全可以通过加防护来应对;而对于内网存在共攻击计算服务器中了病毒,则病毒可当作跳板攻击别的机器,这个问题就比较严重了。因此内网安全事件的严重性远高于外网安全事件。



现在安全产品部署的模式为：大量的安全产品都部署在南北向，即在数据中心或者云的出口及入口处，这样的部署模式相对简单，串联就好了。而东西向大流量数据中遭遇的小攻击是极难防护的。东西向流量很大，一般很难发现，也很难把内网流量引出去，这样就会把一些非常严重的安全事件忽略掉；云资源池中不同租户业务的重要性不同，然而资源池里虚拟化层面的许多资源是共享的，因此网络攻击有可能相互影响。

因此云数据中心若要高级别地提高安全性，需对流量进行处理：一是对南北向流量监控；二是对接近租户的业务和虚拟机的东西向流量进行监控；三是在虚拟化层面把流量引入监控网络。

可见，在部署 SDN 时，要充分利用 SDN 的灵活性，实现更灵活的引流，就要实现软件定义探针。它最终解决的问题就是用 SDN 的手段对流量监控以及 OpenFlow 中流量的采集、过滤和流量的控制，再把云平台的信息关联起来，实现安全分析监控。

4 结束语

根据 IDC 的数据显示，预计到 2020 年，全球数据中心网络规模将增长 10 倍，基于 SDN 及虚拟化的智能数据中心将会解决未来大部分智能业务的部署问题。在公有云中部署 SDN 架构能很好地契合数据中心网络的集中网络管理、灵活组网多路径转发、虚拟机部署和智能迁移、虚拟多租户、IaaS 等方面的需求，非常适合在数据中心网络中应用。

本文跟踪的公有云大规模部署 SDN 案例，为目前全球运营商最大的 SDN、NFV 商用案例之一。根据公有云 SDN 引入后网络性能的优化，深入分析总结出 SDN 部署时需要注意的问题，为后续 NFV、5G 时代，SDN 架构如何部署在其他云计算资源池中提供详细的应用参考。

参考文献：

- [1] SIMEONIDOU D E, NEJABATI R, CHANNEGOWDA M. Software-defined optical networks technology and infrastruc-

ture: enabling software-defined optical network operations[J]. IEEE/OSA Journal of Optical Communications & Networking, 2013, 5(10).

- [2] JARSCHER M, ZINNER T, HOSSFELD T, et al. Interfaces, attributes, and use cases: a compass for SDN[J]. IEEE Communications Magazine, 2014, 52(6): 210-217.
- [3] BOURAS C, KOLLIA A, PAPAZOIS A. SDN & NFV in 5G: advancements and challenges[C]//2017 20th Conference on Innovations in Clouds, Internet & Networks, March 7-9, 2017, Paris, France. Piscataway: IEEE Press, 2017.
- [4] 肖子玉. SDN 技术优化的最新研究综述[J]. 电信科学, 2015, 31(Z1): 132-139.
- XIAO Z Y. A review of the latest research on SDN technology optimization[J]. Telecommunications Science, 2015, 31(Z1): 132-139.
- [5] KARAKUS M, DURRESI A. A survey: control plane scalability issues and approaches in software-defined networking (SDN)[J]. Computer Networks, 2017(112): 279-293.
- [6] 赵慧玲, 史凡. SDN/NFV 的发展与挑战[J]. 电信科学, 2014, 30(8): 13-18.
- ZHAO H L, SHI F. Development and challenge of SDN/NFV[J]. Telecommunications Science, 2014, 30(8): 13-18.
- [7] SADASIVARAO A, SYED S, PAN P, et al. Bursting data between data centers: case for transport SDN[C]//2013 IEEE 21st Annual Symposium on High-Performance Interconnects, August 21-23, 2013, San Jose, CA, USA. Piscataway: IEEE Press, 2013: 87-90.

作者简介



月球（1985-），女，中国移动通信集团设计院有限公司咨询设计专家，主要研究方向为移动通信核心网、5G、云计算、NFV。

刘芹（1977-），女，中国移动通信集团设计院有限公司咨询设计总监，主要研究方向为数据业务平台、IT 支撑系统、云计算等。

杨小乐（1986-），男，中国移动通信集团设计院有限公司咨询设计专家，主要研究方向为 3G/4G/5G 核心网技术、数据业务平台等。

毕晓飞（1985-），男，中国移动通信集团设计院有限公司咨询设计师，主要研究方向为云计算资源池系统方案与建设。

朱师萱（1987-），女，中国移动通信集团设计院有限公司咨询设计师，主要研究方向为云计算、NFV、SDN。