



云资源池集成虚拟防火墙方案及关键技术

黄志兰, 樊勇兵, 樊宁, 陈楠, 吴林泽, 林宝洪

(中国电信股份有限公司广州研究院, 广东 广州 510630)

摘要: 防火墙服务(FWaaS)是云资源池网络服务的关键组件之一, 要求具备自动开通、按需灵活调整的能力, 适合采用软件形态的虚拟防火墙(virtual firewall, vFW)承载。对于云资源池而言, 虚拟防火墙具有特殊性, 本身既是网络服务需要被业务系统编排, 又是网元组件需要被网络系统配置。云资源池环境下, 虚拟防火墙面临与云平台、SDN 等其他组件集成的问题。研究了现有云资源池集成虚拟防火墙的主要方案, 分析了云资源池集成虚拟防火墙的主要问题, 提出了基于可扩展的模型框架实现云资源池集成虚拟防火墙的方法。

关键词: 云计算; 异构; SDN; NFV; 虚拟防火墙

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019047

Solution and key technology of integrating vFW in cloud platform

HUANG Zhilan, FAN Yongbing, FAN Ning, CHEN Nan, WU Linze, LIN Baohong

Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

Abstract: FWaaS is one of the key cloud network services, which requires ability of auto provisioning and flexibility of on-demand adjustment. It is suitable for cloud platforms to provide FWaaS based on virtual firewalls (vFW) appliance. vFW has its own particularity comparing to other cloud components. It is not only a network service but also a network element, which should be orchestrated by business systems and should be automatically configured by network systems. In the environment of cloud resource pool, vFW faces the integration problem with other cloud components like SDN and cloud management platform. The main method of integrating vFW in cloud resource pool was studied, the existing integration problems were analyzed, and an integration method based on extensible model driven framework was proposed.

Key words: cloud computing, heterogeneous, SDN, NFV, vFW

1 引言

SDN (software defined networking, 软件定义网络) 是一种新型的网络设计理念, 通过分离网

络的控制平面和转发平面、开放网络的可编程能力等, 增加了网络的灵活性、开放性以及创新性, 已经成为云资源池网络构建的标准技术^[1]。通过引入 SDN, 云资源池可方便实现租户 L2~L3 层网

络的自动化配置,使云平台能够对计算、存储、网络资源进行统一的管理和调配^[2]。相较 L2~L3 层网络而言,以防火墙服务为代表的云资源池 L4~L7 层网络服务的自动化程度较低。传统防火墙以网络设备或者安全设备等硬件盒子的形式存在,需要逐个设备手工配置,在多租户支持、资源调配以及自动化配置等方面的能力较差,无法满足云资源池对 L2~L7 层网络服务虚拟化、动态化、透明化等方面的要求。为适应云计算特性,云计算环境下的防火墙技术呈现不同的发展态势,主要沿网络模式和虚拟化模式两个方向发展。网络模式防火墙基于现有成熟的网络或安全设备开发,将硬件产品软件化、虚拟化后通过网络技术将流量牵引到云计算防火墙进行检测与处置;虚拟化模式防火墙则与虚拟化软件深度结合,在虚拟化层实现安全防护功能^[3]。相较而言,网络模式对虚拟化技术的依赖更低,但要求网络层面配合引流;虚拟化模式则依赖于虚拟化层开放的 API,防护范围受限于物理主机。随着 NFV (network function virtualization, 网络功能虚拟化)技术的不断发展和应用,网络模式的虚拟防火墙(virtual firewall, vFW)成为云计算防火墙产品的主要形态,被越来越多的云资源池使用。NFV 形态的虚拟防火墙与 SDN 的解耦、集成,也成为云资源池网络构建的关键问题之一,亟待研究。

2 防火墙与云平台及 SDN 的关系概述

对于云资源池来说,虚拟防火墙是一个相对特殊的组件,本身既是云化资源池的网络服务,又是 NFV 形态的网元组件。

虚拟防火墙作为云化资源池的网络服务,由云平台以防火墙服务(FWaaS)的形式提供给租户,租户可以按需开通、付费使用。租户对防火墙服务的操作包括开通/关闭防火墙服务、配置防火墙策略、应用防火墙防护子网/端口等,云平台需要根据租户的操作相应完成对虚拟防火墙网元

的配置管理,包括生命周期管理、策略配置和网络配置等。

虚拟防火墙作为 NFV 形态的网元组件,是云资源池网络的组成部分,与 SDN 的关系特殊,既可以归于 SDN 网络体系由 SDN 控制器统一管理和配置,也可以独立于 SDN 由上层云平台协同调度。主流 SDN 方案倾向于在其中集成虚拟防火墙,安全方案则倾向于提供独立的可集成于云平台的虚拟防火墙网元。云资源池集成虚拟防火墙和 SDN 时,需要解决虚拟防火墙网元的生命周期管理、策略配置以及虚拟防火墙与租户 L2~L3 层网络间的网络配置问题。

以基于 OpenStack 的云平台为例,租户操作防火墙服务时引发的 SDN 及虚拟防火墙配置关系如图 1 所示。

3 云资源池应用虚拟防火墙的行业现状

目前,云资源池对虚拟防火墙网元的集成主要有 3 种方式:在无 SDN 的情况下,由云平台管理和配置虚拟防火墙^[4];在有 SDN 的情况下,由 SDN 控制器管理和配置虚拟防火墙;在有 SDN 的情况下,由云平台协同管理 SDN 和虚拟防火墙。

3.1 无 SDN 情况下云资源池集成虚拟防火墙方案

在云资源池没有部署 SDN 的情况下,云平台直接管理和配置虚拟防火墙,完成虚拟防火墙生命周期、网络和策略相关的配置。OpenStack 已经成为云平台的行业事实标准,在其网络组件 Neutron 中提供安全组和 FWaaS 扩展来实现防火墙功能,两者均能实现对租户网络资源的 L3~L4 层防护,其中安全组功能提供主机级别的网络安全防护,FWaaS 功能则提供子网级别的网络安全防护。主流虚拟防火墙大多会提供插件来对接 OpenStack 的 FWaaS 服务。无 SDN 的情况下,云平台对接虚拟防火墙的典型架构如图 2 所示。

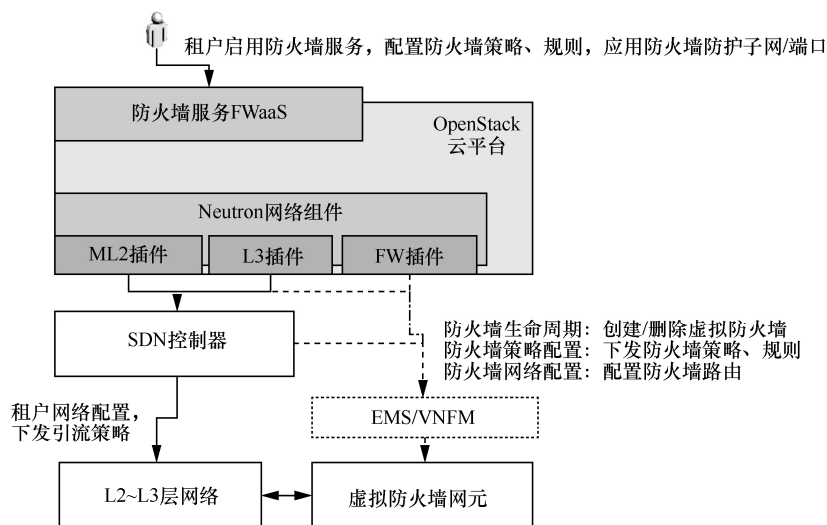


图1 基于 OpenStack 云平台的防火墙服务

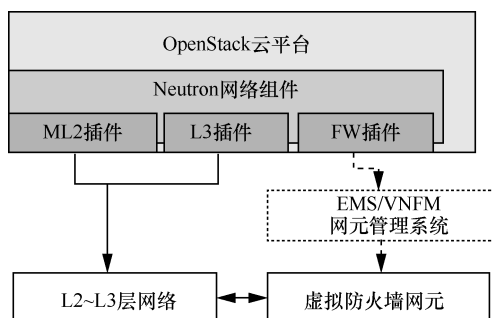


图2 无 SDN 情况下虚拟防火墙对接云平台架构

虚拟防火墙的 FWaaS 插件北向接收云平台的防火墙操作，南向发起对防火墙网元或者防火墙管理系统的调用，完成 OpenStack 防火墙操作指令到防火墙网元或者管理系统 API 间的逻辑转换。根据底层实现方案的不同，L2~L3 层网络插件如 ML2 插件、L3 插件和 FWaaS 插件的提供方可能不同，插件间需要引入额外的协同配置工作（手工配置），以实现租户网络与防火墙间的路由配置。

3.2 SDN 内置虚拟防火墙方案

主流 SDN 方案大都内置网络防火墙功能，这些防火墙主要有两种形态，分别是：位于虚拟接入交换机的分布式防火墙，用于对租户东西向流量提供类似 ACL 的网络访问控制能力；位于网关节点或者以独立虚拟机形态部署的集中式防火墙，用于对租户南北向互访流量提供 L3~L4 层防

护。此类防火墙多由 SDN 控制器直接管理和配置，由 SDN 提供对接 OpenStack Neutron 的全套插件。SDN 方案内置虚拟防火墙时，对接云平台的典型架构如图 3 所示。

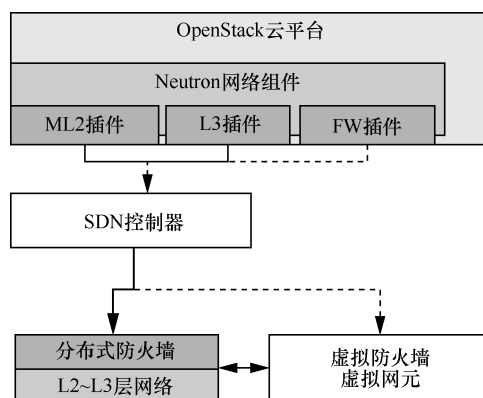


图3 SDN 自带虚拟防火墙对接云平台架构

SDN 提供对接 OpenStack L2~L3 层及防火墙的全套插件，包括 ML2 插件、L3 插件和 FW 插件。云平台对租户网络和防火墙的管理配置要求，通过 OpenStack 插件下发到 SDN 控制器，由 SDN 控制器完成对 L2~L3 层网元和虚拟防火墙网元的所有配置（包括路由配置、防火墙生命周期、策略、网络配置和状态监控）。

3.3 SDN 集成第三方虚拟防火墙方案

主流 SDN 也提供对第三方防火墙的集成，主

要有两种集成模式。第一种是紧耦合模式,由 SDN 控制器直接管理和配置第三方的虚拟防火墙网元,通常 SDN 会提供对接第三方网元的机制,如 VMware 提供 NetX API 供第三方集成 NSX;第二种是松耦合模式,SDN 控制器本身不直接管理和配置第三方虚拟防火墙,而是由云平台通过第三方的网元管理系统对虚拟防火墙进行管理和配置,SDN 和防火墙间通过某种机制进行协同,实现两者间的路由互通。目前,主要有两种协同 SDN 与防火墙的方式:在 SDN 控制器与防火墙网元管理系统之间互通 RPC 消息和在 OpenStack 层的 L3 插件和 FWaaS 插件间互通 RPC 消息。不管采用何种集成模式、何种协同方式,都需要在 SDN 和第三方虚拟防火墙间进行协同开发。因此,大多数 SDN 会限定支持的虚拟防火墙列表。

紧耦合模式下,SDN 集成第三方虚拟防火墙对接云平台的技术与 SDN 内置防火墙的情况类似。松耦合模式下,SDN 集成第三方虚拟防火墙对接云平台的典型架构如图 4 所示。

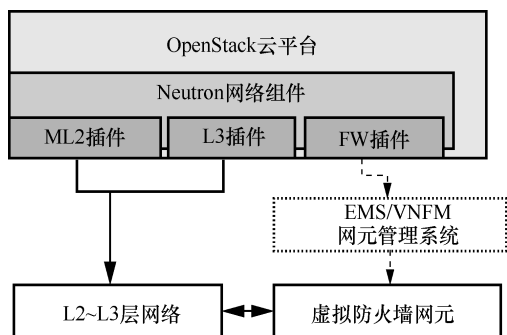


图 4 SDN 集成第三方虚拟防火墙对接云平台架构

对接 OpenStack 的 ML2 插件和 L3 插件由 SDN 提供,FWaaS 插件可由 SDN 或防火墙提供。松耦合模式下,FWaaS 插件大多由防火墙提供。图 4 标注了两种 SDN 与虚拟防火墙协同的方式:方式一,在 SDN 控制器和第三方的网元管理系统间通过 RPC 消息进行协同,由 SDN 控制器开放接口供第三方网元管理系统获取防火墙路由配置的相关信息;方式二,在 OpenStack 层面由 L3 插

件和 FWaaS 插件间通过 RPC 消息协同,引导 SDN 控制器正确配置 L2~L3 层网络和第三方网元管理系统正确配置防火墙路由。

此外,云平台也可以通过业务功能链(service function chain, SFC)技术^[5],实现租户网络流量按需经过各个虚拟 L4~L7 层网络服务。受业务链相关技术多样化以及标准尚未成熟等多方面因素影响,该方案尚未成为主流。

3.4 云资源池应用虚拟防火墙的方案对比

上述 3 种不同的虚拟防火墙集成方案适用于不同的应用场景,有着不同的优缺点。表 1 从配置界面、部署复杂度、异构多方案接入能力、兼容性、自动化水平等方面对各方案进行了对比。

方案一适用于云资源池没有引入 SDN 的场景,通常为早期建设的云资源池,部分小规模云资源池出于成本考虑,也可能采用此部署方案。

方案二为 SDN 提供的一体化解决方案,架构简单、自动化程度最高,存在锁定风险,适用于小规模云资源池或者大规模云资源池划小建设且对租户防火墙能力要求较低的场景。

方案三(1)和方案三(2)为 SDN 集成第三方虚拟防火墙的两种主流方案,对第三方防火墙的兼容性有限,支持的第三方列表受限于 SDN,自动化水平较高,适用于自身集成能力有限又对租户防火墙有较高要求的云平台。

可见,云资源池引入虚拟防火墙时,需要综合考虑云平台、SDN 及虚拟防火墙三者之间的兼容性和配合度。要实现防火墙服务端到端的自动化开通,要求 SDN 及虚拟防火墙能够被云平台统一纳管,并且 SDN 与虚拟防火墙间的网络能够协同配置。

在云平台统一纳管方面,OpenStack 已经成为云平台的事实标准,大多数 SDN 及虚拟防火墙均已实现对 OpenStack 的支持,但受 OpenStack 自身架构的限制,不支持异构、多 SDN 以及虚拟防火墙方案的接入。



表 1 云资源池集成虚拟防火墙方案对比分析

编号	方案	配置界面	复杂度	异构多方案接入	兼容性	自动化水平
一	无 SDN 情况下集成虚拟防火墙	OpenStack 作为统一配置界面	低, 架构简单	不支持	好, 支持主流虚拟防火墙	较低, L2~L3 层与防火墙间的网络需要手工配置或者额外协同
二	SDN 内置虚拟防火墙	OpenStack 和 SDN 控制器	低, 架构简单	不支持	差, 仅支持 SDN 内置虚拟防火墙	高, SDN 控制器完成端到端网络配置
三(1)	紧耦合模式下 SDN 集成第三方防火墙	OpenStack、SDN 控制器、第三方网元管理系统	低, 架构相对简单	不支持	一般, 仅支持兼容列表里的虚拟防火墙	较高, SDN 控制器完成端到端网络配置
三(2)	松耦合模式下 SDN 集成第三方防火墙	OpenStack、SDN 控制器、第三方网元管理系统	高, 架构复杂	不支持	一般, 仅支持兼容列表里的虚拟防火墙	较高, SDN 控制器及网元管理系统配合完成端到端网络配置

在 SDN 与虚拟防火墙的网络协同配置方面, 由于缺乏统一的标准机制, 手工协同或者 SDN 主导成为目前主流的方式, 导致多数情况下, 虚拟防火墙与 SDN 存在一定的耦合, 限定了防火墙的可选择范围, 无法发挥防火墙产业竞争的优势。

异构、多种 SDN 及虚拟防火墙间的解耦、协同, 成为云资源池引入 SDN 及虚拟防火墙面临的重要问题。

4 云资源池集成 SDN 与虚拟防火墙的关键问题

云资源池在集成 SDN 和虚拟防火墙时, 应能充分解耦两者, 使得云提供商能够按需选择不同的 SDN 产品和防火墙产品, 从而充分释放 SDN 产业及防火墙产业各自竞争带来的价格红利。而防火墙作为云平台面向租户提供的一种增值服务, 应具有多样性, 要求云平台能够提供多种方案、多种功能、多种型号、多种规格的防火墙供租户按需选用, 云平台需要具备同时部署异构虚拟防火墙的能力。云平台在纳管异构 SDN 及虚拟防火墙时, 需要满足异构多方案接入、异构兼容、异构协同等要求。

- 异构多方案接入: 要求云平台能够同时支持多种不同的 SDN 和虚拟防火墙方案, 并能按需热插拔不同的 SDN 及虚拟防火墙,

且不引发系统性的重构。

- 异构兼容: 要求云平台能实现异构 SDN 以及异构虚拟防火墙之间的兼容, 使得不同 SDN 与不同虚拟防火墙间可以灵活组合, 即实现 SDN 及虚拟防火墙解耦。
- 异构协同: 要求解决异构 SDN 与异构虚拟防火墙间的网络协同配置问题, 而不需要逐 SDN 和虚拟防火墙进行双向适配和开发。

受 OpenStack 自身架构限制以及标准缺失、私有化实现等多方面因素的影响, 现有云平台在纳管异构 SDN 及异构虚拟防火墙时, 均无法有效地解决这些问题。

OpenStack 以插件的方式对接不同的解决方案, 仅能同时启用单个插件, 意味着基于 OpenStack 构建的云平台在对接 SDN 或虚拟防火墙时, 仅能支持单个解决方案。异构兼容和异构协同问题本质上是由 SDN 及虚拟防火墙的私有化实现引起的, OpenStack 定义了云资源池租户的 L2~L7 层网络及服务模型, 在一定程度实现了接口的标准和统一^[6]。主流 SDN 方案大都支持 OpenStack 的网络模型, 主流虚拟防火墙也基本兼容 OpenStack 定义的 FWaaS 服务模型。但是, OpenStack 定义的网络和服务模型无法覆盖多数 SDN 和虚拟防火墙的高级特性, 只能满足租户最基本的虚拟网络需求。市场竞争的激烈性以及来

自用户的差异化服务需求,使得SDN及虚拟防火墙在实现时并未完全遵循OpenStack标准,而采用了私有实现。SDN及虚拟防火墙间对外提供的接口各不相同,从而缺乏互操作的能力^[7]。兼容性不足使得云平台在使用不同方案时,需要逐方案开发适配插件,效率低下。此外,SDN和虚拟防火墙之间的路由配置也因接口和实现方式的不同,无法从机制上进行统一。

因此,云资源池在部署SDN和虚拟防火墙时,需引入额外的机制解决异构多方案接入、异构兼容及异构协同问题。

5 云资源池集成异构SDN与虚拟防火墙的关键技术

基于OpenStack的云平台受架构、模型等方面的限制,在纳管SDN及虚拟防火墙时,无法支持异构多方案接入、解耦协同等需求,需要引入额外的机制对OpenStack进行扩展。

5.1 可扩展的模型驱动框架

在OpenStack外引入一层可扩展的模型驱动框架(extensible model driven framework,以下简称模型驱动框架),可以有效地解决上述问题。

模型驱动框架作为底层各类L2~L7层网络解决方案的统一代理,通过相同的插件对接OpenStack Neutron组件,各个SDN、虚拟防火墙方案等通过编写驱动插件的方式接入模型驱动框架,由模型驱动框架负责将OpenStack Neutron的相关调用转发到底层相应的SDN控制器或者防火墙上。基于可扩展的模型驱动框架,引入标准化的模型语言、驱动插件协同机制、驱动插件动态接入机制等,可以解决云资源池集成异构SDN及虚拟防火墙时面临的异构多方案接入、异构兼容和异构协同问题。

模型驱动框架包含模型定义、模型解析、接口生成、驱动注册、驱动管理和路由等方面,并提供基于消息或者RPC的通信机制供

SDN和虚拟防火墙协同。模型驱动框架的基本结构如图5所示。

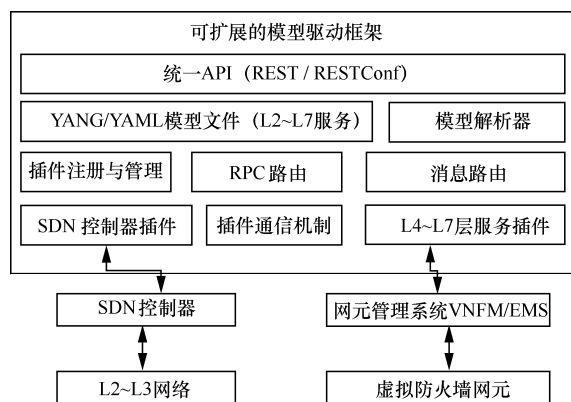


图5 可扩展的模型驱动框架

参考业界主流实现,模型驱动框架可采用YANG或者YAML等在云计算领域应用广泛的模型定义语言。这两种模型语言适用的场景不同,YANG适用于网络配置定义,YAML适用于服务层面的数据模型定义。OpenDaylight等SDN控制器采用YANG语言来定义网络及服务模型,OpenStack、ONAP等管理及编排系统则采用可读性更高的YAML语言来定义数据模型。基于框架开放的接口,用户可按照模型语言规范、根据实际业务需求来定义具体的网络及服务模型,可以基于OpenStack网络和服务模型扩展,也可以引入新的网络及服务模型用于描述云网络及防火墙的高级特性。模型驱动框架提供持久化机制,用于存储用户定义的模型文件。

框架集成YANG或者YAML解析器,能够基于用户定义的模型文件,自动生成REST或者RESTConf类型的API,供OpenStack等上层管理平台 and 业务系统调用。

SDN和虚拟防火墙基于框架定义的网络和服务模型,编写驱动插件进行适配,完成标准模型和API到自家模型和API的转换。框架引入OSGI技术实现驱动插件的动态加载,并提供驱动插件的注册、管理和路由功能。SDN和虚拟防火墙以OSGI Bundle的方式撰写驱动插件,向驱动



框架注册插件，提供插件所支持的产品名称、型号、功能列表、配置数据和插件 ID 等关键信息，驱动框架根据这些信息完成上层服务调用到驱动插件的路由。根据需求场景的不同，框架支持点对点（RPC 路由）、点对多点（消息路由）等多种形式的服务路由。

框架内置基于 RPC 或者消息的通信机制，供 SDN 和虚拟防火墙插件间协同。通过定义两者间的标准通信接口，不同 SDN 和虚拟防火墙间可以按需配置互通路由，实现云资源池 L2~L7 层网络服务的自动化配置。

引入模型驱动框架之后，OpenStack 平台网络侧的技术架构如图 6 所示。

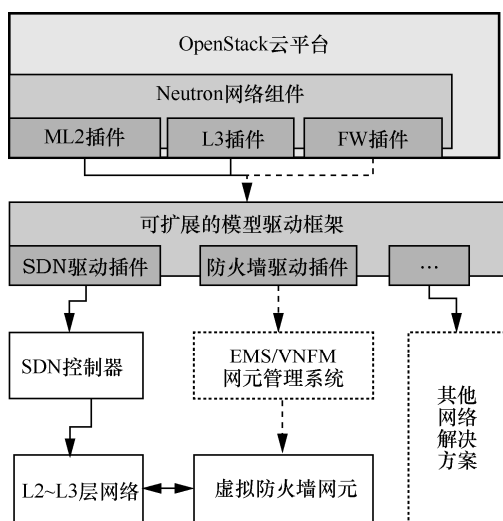


图 6 基于可扩展模型驱动框架的 OpenStack 云平台网络架构

5.2 基于模型驱动框架集成异构 SDN 和虚拟防火墙

模型驱动框架从代码级别实现了云资源池 L2~L7 层网络及服务的标准化。框架为上层管理及业务系统提供标准、统一的北向 API，南向则通过插件兼容不同 SDN 及虚拟防火墙，实现了 SDN 和虚拟防火墙间的彻底解耦。框架支持同时接入多种不同的 SDN 和虚拟防火墙，能够有效扩展云资源池对多方案的接入能力。基于模型驱动框架的能力，云提供商可进一步引入编排软件，

实现在多种 SDN 及虚拟防火墙方案共存的情况下，按需将租户 L2~L7 层网络服务编排至不同的 SDN 控制器及虚拟防火墙上。

云资源池基于模型驱动框架集成异构 SDN 和虚拟防火墙的整体架构如图 7 所示。

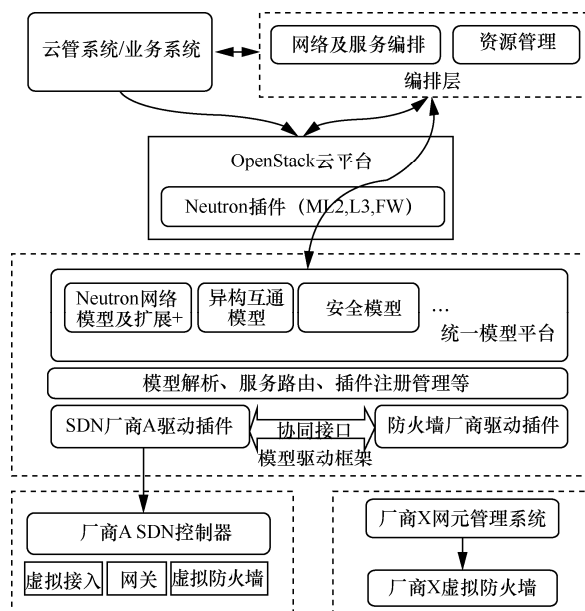


图 7 云资源池基于模型驱动框架集成异构 SDN 和虚拟防火墙的架构

引入模型驱动框架之后，云资源池的管理和控制平面由云管系统/业务系统、编排层、OpenStack 云平台、模型驱动框架、SDN 控制器、虚拟网元管理系统等几大组件构成。

- 云管系统/业务系统作为云资源池的上层系统，负责维护整个云资源池的物理和虚拟资源，拥有资源的全局视图，按需为租户开通各类云服务。
- 编排层用于在多资源池、多种异构 SDN 和虚拟防火墙共存的情况下，为云管系统/业务系统提供跨域、跨 SDN 控制器、跨虚拟防火墙的租户网络资源编排服务^[8]。
- OpenStack 云平台负责统一管理云资源池各类虚拟资源，包括计算、存储、网络等资源，对接底层各类虚拟化产品、SDN 方案等，包括计算虚拟化平台（如 VMware

ESXi、KVM、XEN 等)以及网络虚拟化平台(如 ODL、ONOS 等)。

- 模型驱动框架通过 Neutron 插件对接 OpenStack, 作为 OpenStack 云平台的网络组件, 负责将云平台对 L2~L7 层网络及服务的调用转发到底层合适的 SDN 及虚拟防火墙产品。
- SDN 控制器作为云资源池逻辑网络的管理和控制平面, 按需配置租户的 L2~L3 层网络。
- VNF 管理系统则负责对虚拟防火墙等 L4~L7 层虚拟网元进行配置管理。

5.3 基于模型驱动框架的方案与现有方案的对比分析

与现有的云资源池集成虚拟防火墙方案相比(参考第 3.4 节), 基于模型驱动框架集成异构 SDN 和虚拟防火墙的方案具有如下优点:

- 模型驱动框架作为 L2~L7 层网络解决方案的代理, 统一对接 OpenStack Neutron, 架构更为简单;
- SDN 及虚拟防火墙以驱动插件的方式动态接入模型驱动框架, 可在不修改 OpenStack 架构的基础上, 实现云平台支持异构多方案接入;
- 解耦 SDN 及虚拟防火墙, 使得虚拟防火墙的选型不受 SDN 限制, 兼容性更好;
- 提供 SDN 及虚拟防火墙间协同的标准机制, 能够实现 L2~L3 层网络及虚拟防火墙网元的端到端配置, 自动化程度高;
- 模型驱动框架支持灵活的网络及服务模型定义, 云资源池可以突破 OpenStack 网络模型的限制, 按需引入更多 L2~L7 层网络服务如 VPN、NAT、DPI、IPS 等, 扩展性更好。

6 结束语

SDN/NFV 已经成为云资源池 L2~L7 层网络

自动化的关键技术, SDN 实现了 L2~L3 层网络的自动化, NFV 则是实现防火墙、负载均衡、VPN 等 L4~L7 网络服务自动化的基础。在云计算领域, SDN 与 L4~L7 层 NFV 的融合尚未成熟, 没有形成标准、完整的解决方案, 大都依赖彼此间相互合作、适配开发完成, 效率低下, 并存在一定程度的锁定, 对产业发展不利。引入可扩展的模型驱动框架实现代码级别的标准, 能够有效解耦 SDN 和 NFV, 实现异构 SDN 及虚拟防火墙的兼容、协同, 从而提升云资源池网络构建的灵活性。

参考文献:

- [1] 樊勇兵, 陈楠, 黄志兰, 等. 解惑 SDN[M]. 北京: 人民邮电出版社, 2015.
FAN Y B, CHEN N, HUANG Z L, et al. Disabuse SDN[M]. Beijing: Posts and Telecom Press, 2015.
- [2] 陈楠, 樊勇兵, 何晓武, 等. 面向应用的云数据中心网络技术研究[J]. 电信科学, 2014, 30(9): 128-132.
CHEN N, FAN Y B, HE X W, et al. Research on the technology of application-oriented cloud data center network[J]. Telecommunications Science, 2014, 30(9): 128-132.
- [3] 樊宁, 沈军, 金华敏. 云计算环境下防火墙技术发展现状及趋势[M]//2013-2014 中国通信行业发展分析报告. 北京: 人民邮电出版社, 2014: 250-253.
FAN N, SHEN J, JIN H M. Development and trend of firewall technology in cloud computing environment[M]//2013-2014 China Communications Industry Development Analysis Report. Beijing: Posts and Telecom Press, 2014: 250-253.
- [4] 李洪, 伍思源, 渠凯, 等. 大规模云资源池中虚拟防火墙部署问题研究[J]. 电信科学, 2014, 30(Z1): 164-167.
LI H, WU S Y, QU K, et al. Research on deployment of virtual firewall in large scale cloud resource pool [J]. Telecommunications Science, 2014, 30(Z1): 164-167.
- [5] Service function chaining (SFC) architecture: RFC 7665 [S]. 2015.
- [6] 李晨, 陈俏钢, 李凤凯, 等. SDN 的网络模型及北向接口[J]. 中兴通讯技术, 2016, 22(6): 17-21.
LI C, CHEN Q G, LI F K, et al. Network model and northbound interface of SDN[J]. ZTE Technology Journal, 2016, 22(6): 17-21.
- [7] 黄志兰, 樊勇兵, 陈楠, 等. Overlay SDN 实现异构兼容的关



键技术[J]. 电信科学, 2016, 32(11): 112-118.

HUANG Z L, FAN Y B, CHEN N, et al. Key technologies of heterogeneous compatibility in overlay SDN[J]. Telecommunications Science, 2016, 32(11): 112-118.

- [8] 赵鹏, 段晓东. SDN/NFV 发展中的关键: 编排器的发展与挑战[J]. 电信科学, 2017, 33(4): 18-25.

ZHAO P, DUAN X D. Key of SDN/NFV development: development and challenge of orchestrator[J]. Telecommunications Science, 2017, 33(4): 18-25.

[作者简介]



黄志兰 (1982-), 女, 现就职于中国电信股份有限公司广州研究院, 主要研究方向为 SDN、云计算、IPv6。



樊勇兵 (1970-), 男, 博士, 现就职于中国电信股份有限公司广州研究院, 中国数据中心产业发展联盟云计算服务专家委员会第一批专家委员, 主要从事中国电信云计算、IDC 等方面的工作。



樊宁 (1983-), 女, 现就职于中国电信股份有限公司广州研究院, 主要研究方向为云安全、SDN 安全及 NFV 安全解决方案。



陈楠 (1981-), 男, 博士, 现就职于中国电信股份有限公司广州研究院, ITU-T Q14/SG11 联合报告人, Q18/SG13 编辑人, 主要研究方向为 SDN、NFV、服务器虚拟化、数据中心网络、管理平台技术等。



吴林泽 (1992-), 女, 现就职于中国电信股份有限公司广州研究院, 主要研究方向为 SDN、云计算。

林宝洪 (1987-), 男, 现就职于中国电信股份有限公司广州研究院, 主要研究方向为云计算、SDN/NFV。