



(12)发明专利申请

(10)申请公布号 CN 109150737 A
(43)申请公布日 2019.01.04

(21)申请号 201710512124.1

(22)申请日 2017.06.28

(71)申请人 上海宽带技术及应用工程研究中心
地址 201201 上海市浦东新区卡园二路108号8幢302A室

(72)发明人 蒋暎青

(74)专利代理机构 上海光华专利事务所(普通合伙) 31219
代理人 徐秋平

(51)Int.Cl.

H04L 12/801(2013.01)

H04L 29/08(2006.01)

H04L 12/46(2006.01)

H04L 12/24(2006.01)

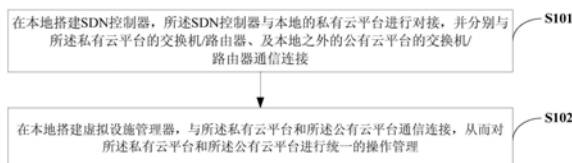
权利要求书2页 说明书5页 附图1页

(54)发明名称

基于SDN的混合云组网方法及混合云网络

(57)摘要

本发明提供基于SDN的混合云组网方法及混合云网络。组网方法包括：在本地搭建SDN控制器，所述SDN控制器与本地的私有云平台进行对接，并分别与所述私有云平台的交换机/路由器、及本地之外的公有云平台的虚拟交换机/路由器通信连接；在公有云的虚拟机中启动虚拟交换机，令公有云中的虚拟机的流量通过该虚拟交换机转发，该虚拟交换机对接安装在私有云中的SDN控制器。在本地搭建虚拟设施管理器，与所述私有云平台和所述公有云平台通信连接，从而对所述私有云平台和所述公有云平台进行统一的操作管理。本发明利用SDN技术，实现了公有云和私有云之间的互联互通和网络透明化。



1. 一种基于SDN的混合云组网方法,其特征在于,包括:

在本地搭建SDN控制器,所述SDN控制器与本地的私有云平台进行对接,并分别与所述私有云平台的交换机/路由器、及本地之外的公有云平台的虚拟交换机/路由器通信连接;所述公有云平台中的虚拟机的流量通过所述虚拟交换机转发;

在本地搭建虚拟设施管理器,与所述私有云平台 and 所述公有云平台通信连接,从而对所述私有云平台和所述公有云平台进行统一的操作管理。

2. 根据权利要求1所述的基于SDN的混合云组网方法,其特征在于,所述操作管理包括:通过所述虚拟设施管理器进行资源调度和管理、租户信息认证管理、及管理员权限管理中的一种或多种组合。

3. 根据权利要求1所述的基于SDN的混合云组网方法,其特征在于,所述虚拟设施管理器获取用户操作,并根据用户操作实现对所述私有云平台和所述公有云平台的网络资源和计算资源的控制。

4. 根据权利要求1所述的基于SDN的混合云组网方法,其特征在于,还包括:

所述虚拟设施管理器分别在所述私有云平台和所述公有云平台中创建虚拟网络和虚拟机;

所述公有云平台内部的流量通过所述公有云平台中的虚拟机中的虚拟交换机转发;

所述虚拟设备管理器通过所述公有云平台的API接口管理所述公有云平台的虚拟网络和虚拟机。

5. 根据权利要求4所述的基于SDN的混合云组网方法,其特征在于,所述SDN控制器对接所述虚拟设施管理器,从所述虚拟设施管理器中获取信息;通过所述SDN控制器控制所述私有云平台和所述公有云平台中的虚拟交换机。

6. 根据权利要求4所述的基于SDN的混合云组网方法,其特征在于,还包括:

在所述公有云平台上的虚拟机上启动软件实现的交换机;

所述公有云平台上的虚拟机的流量通过安装有软件实现的交换机的虚拟机;

所述部署在所述公有云平台上的软件实现的交换机被所述SDN控制器所控制;

所述SDN控制器下发流表到部署在所述公有云平台上的软件实现的交换机以实现对流量的转发。

7. 根据权利要求4所述的基于SDN的混合云组网方法,其特征在于,本地通过L2_Tunnel的方式连接所述私有云平台中的支持SDN的交换机和所述公有云平台中的支持SDN的虚拟交换机,以实现所述公有云平台的资源与数据中心网络的内网区的资源互联互通。

8. 根据权利要求4所述的基于SDN的混合云组网方法,其特征在于,在所述公有云平台上利用部署在所述私有云平台中的所述SDN控制器的Plugin对接所述公有云平台中的虚拟机里面启动的虚拟网络设备和所述私有云平台中的支持SDN的交换机,从而根据所述SDN控制器对所述公有云平台和私有云平台的虚拟网络设备进行统一的网络策略的下发。

9. 根据权利要求4所述的基于SDN的混合云组网方法,其特征在于,所述私有云平台与所述公有云平台的内部分别通过南向接口的方式与对应的虚拟网络设备连接。

10. 根据权利要求9所述的基于SDN的混合云组网方法,其特征在于,所述SDN控制器将网络配置策略下发到所述公有云平台和所述私有云平台的虚拟网络设备,并根据南向协议对所述私有云平台和所述公有云平台上的交换机/路由器进行通信策略以及安全策略的下

发。

11. 一种混合云网络,其特征在于,所述混合云网络由权利要求1至10中任一所述的基于SDN的混合云组网方法构建而成。

基于SDN的混合云组网方法及混合云网络

技术领域

[0001] 本发明涉及云间的混合组网技术,特别是涉及基于SDN的混合云组网方法及应用该方法构建的混合云网络。

背景技术

[0002] 混合云是一种组合的云,它是一种公有云和私有云的组合,是组织提供和管理一些内部资源,以及其他组织提供外部资源的云计算环境。混合云是一种为企业节省空间和成本的好方法,既利用了公有云更便宜的优势,又确保了对高度敏感信息的保护。如今的企业大多不愿意为公有云的安全问题承担风险,所以将大部分的信息存储在自己的服务器上。混合云不但能为他们内部网络的存储提供机会,还在通过网络访问时又可以从任何地点访问一个公有云,从而达到保护数据的效果。

[0003] 一种典型的混合云是企业内部的服务器中构建了私有云,连同在公有云上租赁的部分公有云资源从而组成了混合云。在混合云场景中,公有云的虚拟机需要和私有云之间的虚拟机进行连通,鉴于此,如何找到一种快速、高效的混合云组网方案就成了本领域技术人员亟待解决的问题。

发明内容

[0004] 鉴于以上所述现有技术的缺点,本发明的目的在于提供基于SDN的混合云组网方法及混合云网络,用于解决现有技术中的上述问题。

[0005] 为实现上述目的及其他相关目的,本发明提供一种基于SDN的混合云组网方法,在本地搭建SDN控制器,所述SDN控制器与本地的私有云平台进行对接,并分别与所述私有云平台的交换机/路由器、及本地之外的公有云平台的虚拟交换机/路由器通信连接;在所述公有云平台中的虚拟机中启动虚拟交换机,令所述公有云平台中的虚拟机的流量通过该虚拟交换机转发,该虚拟交换机对接安装在私有云中的SDN控制器。在本地搭建虚拟设施管理器,与所述私有云平台 and 所述公有云平台通信连接,从而对所述私有云平台 and 所述公有云平台进行统一的操作管理。

[0006] 于本发明一实施例中,所述操作管理包括:通过所述虚拟设施管理器进行资源调度和管理、租户信息认证管理、及管理员权限管理中的一种或多种组合。

[0007] 于本发明一实施例中,所述虚拟设施管理器获取用户操作,并根据用户操作实现对所述私有云平台 and 所述公有云平台的网络资源和计算资源的控制。

[0008] 于本发明一实施例中,还包括:所述虚拟设施管理器分别在所述私有云平台 and 所述公有云平台中创建虚拟网络和虚拟机;所述公有云平台内部的流量通过所述公有云平台中的虚拟机中的虚拟交换机转发;所述虚拟设备管理器通过所述公有云平台的API接口管理所述公有云平台的虚拟网络和虚拟机。

[0009] 于本发明一实施例中,所述SDN控制器对接所述虚拟设施管理器,从所述虚拟设施管理器中获取信息;通过所述SDN控制器控制所述私有云平台 and 所述公有云平台中的虚拟

交换机。

[0010] 于本发明一实施例中,其特征在于,还包括:在所述公有云平台上的虚拟机上启动软件实现的交换机;所述公有云平台上的虚拟机的流量通过安装有软件实现的交换机的虚拟机;所述部署在所述公有云平台上的软件实现的交换机被所述SDN控制器所控制;所述SDN控制器下发流表到部署在所述公有云平台上的软件实现的交换机以实现对流量的转发。

[0011] 于本发明一实施例中,本地通过L2_Tunnel的方式连接所述私有云平台中的支持SDN的交换机和所述公有云平台中的支持SDN的虚拟交换机,以实现所述公有云平台的资源与数据中心网络的内网区的资源互联互通。

[0012] 于本发明一实施例中,在所述公有云平台上利用部署在所述私有云平台中的所述SDN控制器的Plugin对接所述公有云平台中的虚拟机里面启动的虚拟网络设备和所述私有云平台中的支持SDN的交换机,从而根据所述SDN控制器对所述公有云平台 and 私有云平台的虚拟网络设备进行统一的网络策略的下发。

[0013] 于本发明一实施例中,所述私有云平台与所述公有云平台的内部分别通过南向接口的方式与对应的虚拟网络设备连接。

[0014] 于本发明一实施例中,所述SDN控制器将网络配置策略下发到所述公有云平台和所述私有云平台的虚拟网络设备,并根据南向协议对所述私有云平台和所述公有云平台上的交换机/路由器进行通信策略以及安全策略的下发。

[0015] 为实现上述目的及其他相关目的,本发明提供一种混合云网络,所述混合云网络由上述任一种基于SDN的混合云组网方法构建生成。

[0016] 如上所述,本发明的基于SDN的混合云组网方法及混合云网络,提供了一种高效灵活的混合云之间的组网方式,利用SDN控制器进行对网络的OpenFlow交换机进行策略的下发,对公有云和私有云之间的网络的流量进行控制,从而达到高效灵活的组网目的。虚拟网络设施管理器OpenStack/CloudStack通过公有云的API对公有云进行虚拟的创建和删除以及网络的创建和删除等操作。SDN控制器同时对私有云和公有云的物理或虚拟的支持SDN的交换机进行策略下发,私有云和公有云的OpenFlow交换机之间通过L2Tunnel进行连接,达到实现公有云和私有云网络之间的互联互通和使网络透明化的目的。

附图说明

[0017] 图1显示为本发明一实施例中的基于SDN的混合云组网方法的流程示意图。

[0018] 图2显示为本发明一实施例中的基于SDN的混合云组网方法所构建的网络架构的示意图。

具体实施方式

[0019] 以下通过特定的具体实例说明本发明的实施方式,本领域技术人员可由本说明书所揭露的内容轻易地了解本发明的其他优点与功效。本发明还可以通过另外不同的具体实施方式加以实施或应用,本说明书中的各项细节也可以基于不同观点与应用,在没有背离本发明的精神下进行各种修饰或改变。需说明的是,在不冲突的情况下,以下实施例及实施例中的特征可以相互组合。

[0020] 需要说明的是,以下实施例中所提供的图示仅以示意方式说明本发明的基本构想,遂图式中仅显示与本发明中有关的组件而非按照实际实施时的组件数目、形状及尺寸绘制,其实际实施时各组件的型态、数量及比例可为一种随意的改变,且其组件布局型态也可能更为复杂。

[0021] 本发明提供一种高效灵活的混合云之间的组网方式,利用SDN控制器的集中控制和基于策略的流表下发等特点,对混合云之间的网络进行策略的优化配置,达到高效灵活的组网目的,利用二层的组网技术,实现私有云与公有云之间网络的互联互通。

[0022] 请参阅图1,本发明提供的基于SDN软件定义网络技术的混合云组网方法,主要包括如下步骤:

[0023] 步骤S101:在本地搭建SDN控制器,并令所述SDN控制器与本地的私有云进行对接,包括:对接私有云网络功能组件,从私有云网络功能组件中获取信息,并由所述SDN控制器的Plugin进行相关的配置操作等,以及,令所述SDN控制器分别与所述私有云平台的交换机/路由器、本地之外的公有云平台的虚拟交换机/路由器建立连接。

[0024] 步骤S102:建立本地虚拟设施管理器,并分别与所述私有云平台 and 所述公有云平台建立连接,用于对本地的私有云和外部的公有云进行统一的资源调度和管理,以及统一的租户信息认证管理、统一的管理员权限管理等。

[0025] 公有云中包含的API可以允许外界进行对路由器/交换机的配置。在本地搭建SDN控制器,在公有云的虚拟机中安装虚拟交换机,通过SDN控制器控制公有云上的虚拟交换机/路由器,并对其下发流表,控制流量的转发。通过L2Tunnel与私有云中的交换机/路由器进行连接,从而打通私有云与公有云的网络。如图2显示了构建的混合云网络的架构模型。

[0026] 在一种具体的实施方式中:

[0027] 所述虚拟设施管理器在本地和通过公有云API在公有平台上分别创建虚拟网络和虚拟主机。在上层的虚拟基础设施管理器中通过公有云的API接口,实现了对公有云的资源的操作,因此,虚拟基础设施管理器可以管理公有云平台上的虚拟机资源以及网络资源。同时,虚拟基础设施管理根据用户的操作来控制SDN控制器对网络设备进行策略的下发。

[0028] 在公有云平台中,公有云通过对虚拟机中的虚拟交换机进行转发策略的下发;在私有云中通过对物理或虚拟的支持SDN的交换机进行转发策略的下发。在云平台中,私有云与公有云内部则可以通过物理或虚拟交换机(如:通过南向接口的方式)进行与虚拟机之间的连接,从而实现云内的网络连通性。

[0029] 进一步地,利用公有云的基础设施把私有云的数据中心网络扩展到公有云,并划分互联网区和内网区。通过L2_TUNNEL连接到企业私有云,以实现公有云的资源 and 自有数据中心的资源内网互联互通。

[0030] 承接上述,专有网络(Virtual Private Cloud)是基于公有云构建出一个隔离的网络环境,可以自定义IP地址范围、网段、路由表和网关等,通过交换机的L2_TUNNEL的连接方式实现VPC与传统数据中心互联,构建混合云业务。在本发明的混合云组网方法中,利用在公有云中购买的网络资源,使用VPC在公有云上创建安全、隔离的虚拟私有网络;还可以根据私有云的网络环境,定义公有云VPC内部虚拟私有网络,包括选择自有IP地址范围、划分网段、配置路由表和网关等。通过L2Tunnel将私有云与公有云VPC打通、实现安全互访。

[0031] 私有云的交换机或虚拟路由器通过二层通道连接到公有云的交换机或路由器,组

建二层的网络。SDN控制器连接私有云和公有云的网络,对接虚拟设施管理器的网络功能组件,管理私有云的网络,实现和公有云虚拟网络的互联互通,包括子网网段和子网间访问控制策略的统一管理,二层和三层网络间的互通。在公有云和私有云的虚拟机进行热迁移的情况下,公有云和私有云的虚拟机IP和MAC需要进行无缝迁移,而计算资源和存储资源也通过混合云的网络进行传输,实现用户无感知地无缝迁移。

[0032] 公有云平台上的虚拟机上需要启动软件实现的交换机,公有云上软件实现的交换机需要被SDN控制器所控制,SDN控制器下发流表到部署在公有云上软件实现的交换机实现对流量的转发,公有云上的虚拟机的流量需要通过安装有软件实现的交换机的虚拟机。VPC租户网络到公有云的延伸和统一管理,在大二层的情况下,公有云和私有云中的虚拟机可以在视为在同一个外网出口之内,由虚拟设施管理器进行统一的管理。实现混合云的灵活部署,实现公有云与私有云之间的高速互连互通。

[0033] 在上述实施方式下,SDN控制器根据公有云API接口对公有云中的交换机和路由器设备进行配置,SDN控制器通过虚拟设施管理器接口把子网隔离等网络配置策略下发到公有云和私有云的虚拟网络设备。SDN控制器根据OpenFlow协议(南向协议)对私有云和公有云中的交换机和路由器进行网络通信策略以及安全策略的下发,使得私有云和公有云中需要相互访问的流量在云的边缘处可以顺利转发,使得私有云中的虚拟机与公有云中的虚拟机可以进行基于安全策略的网络通信。

[0034] 在一实施例中,在公有云上利用部署在私有云中SDN控制器的Plugin对接公有云中的虚拟网络设备,根据SDN控制器对公有云中的虚拟网络设备进行统一的网络策略的下发,主要包括网络的连通性,统一的Floating IP,NAT的出外网等情况的统一管理,安全组的统一下发,以及负载均衡的统一分配等。创建、删除、更新网络信息由本地的虚拟基础设施管理进行统一的管理,SDN控制器通过Restful API感知到公有云中创建、删除、更新网络等用户操作,而具体的实现细节则由SDN控制器通过Plugin来对公有云中的虚拟网络设备进行管理和策略的下发,使得公有云中的虚拟机的流量按照流表规则进行转发,使得用户的操作可以得到及时的响应和完成。

[0035] 在利用SDN技术构建混合云网络的条件下,可以利用SDN的高效、灵活、透明的特点,针对混合云中原先不可见的网络流量,在SDN控制器的感知下,可以对混合云中的网络流量进行感知和控制转发。而且,相比较需要人工配置或者脚本配置的网络设备,SDN的组网方式可以实现比Site-To-Site VPN更加智能和灵活,满足了混合云对组网的要求。

[0036] 此外,私有云中的网段和公有云中的网段利用二层技术在同一个网络中,由SDN控制器对流量进行策略下发,私有云与公有云网络对于虚拟机是透明的,创建的虚拟机可以在安全策略的允许下与私有云和公有云的虚拟机进行通信,而在本地的虚拟基础设施管理中进行统一的资源分配和调度。利用SDN的混合云组网技术,可以实现兼容私有云环境中的物理服务器与虚拟服务器资源,减少对私有云架构的改动,构建多技术平台。

[0037] 最后,本发明提供一种由前述的基于SDN的混合云组网方法所构建的混合云网络,由于前述实施例中的已经对各个技术特征做了详细说明,在此不重复赘述。

[0038] 综上所述,本发明的混合云组网技术提供了一种新型网络架构,是网络虚拟化的一种实现方式,通过SDN的核心技术OpenFlow将网络设备的控制面与数据面分离开来,在公有云和私有云的网络设备中下发策略,从而实现对网络流量的灵活控制,使网络作为管道

变得更加智能,有效克服了现有技术中的种种缺点而具高度产业利用价值。

[0039] 上述实施例仅例示性说明本发明的原理及其功效,而非用于限制本发明。任何熟悉此技术的人士皆可在不违背本发明的精神及范畴下,对上述实施例进行修饰或改变。因此,举凡所属技术领域中具有通常知识者在未脱离本发明所揭示的精神与技术思想下所完成的一切等效修饰或改变,仍应由本发明的权利要求所涵盖。

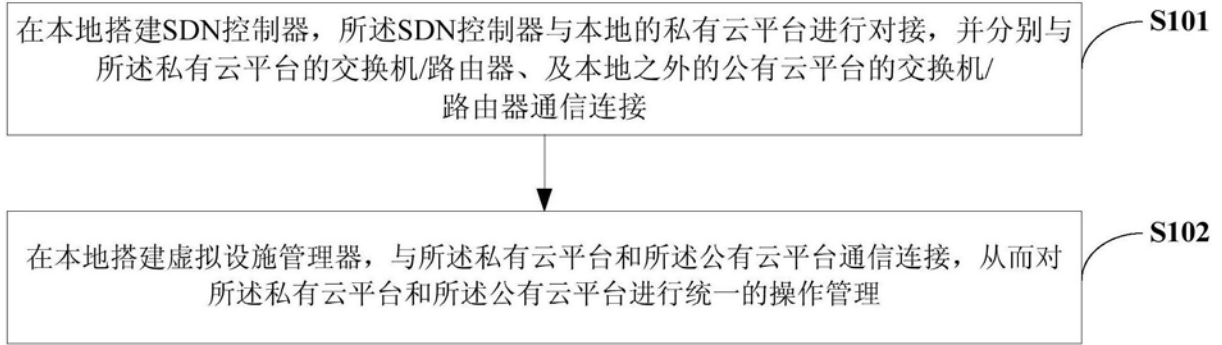


图1

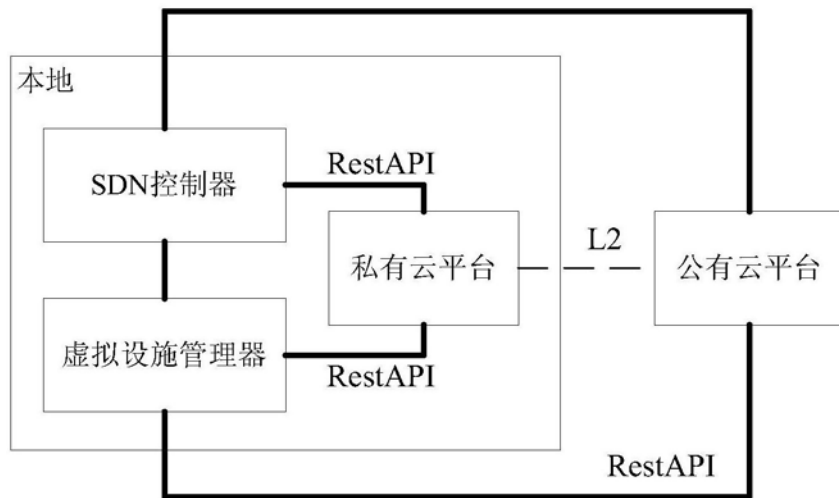


图2