

虚拟私有云与云下数据中心通信、配置方法及相关装置

5 技术领域

本申请涉及云技术领域，特别涉及一种虚拟私有云与云下数据中心通信、配置方法及相关装置。

背景技术

- 10 随着云技术的发展，存在虚拟私有网络（Virtual Private Cloud，VPC）与云下数据中心通信的诉求，但由于私网地址规划等原因，若需要通信的 VPC 与云下数据中心之间存在私网地址重叠，即二者具有相同的私有网段，则会造成二者不能通信。

发明内容

- 15 为解决现有技术的问题，本申请提供一种虚拟私有云与云下数据中心通信、配置方法及相关装置，能够解决 VPC 与云下数据中心之间存在私网地址重叠而不能通信的技术问题。

- 20 第一方面，本申请提供一种虚拟私有云 VPC 与云下数据中心通信的配置方法，其中，具有相同私网地址段的第一虚拟私有云 VPC 和云下数据中心的子网通过第二 VPC 进行通信，该第二 VPC 的私网地址段与该第一 VPC、该子网的私网地址段均不相同，该方法包括：将该第一 VPC 内的私网地址与第一地址进行绑定，将该子网内的私网地址与第二地址进行绑定，其中，该第一地址和该第二地址为归属于该第二 VPC 的私网地址段的地址，该第一地址与该第二地址不相同；将该第一 VPC 发送至该子网的报文的源地址从该第一 VPC 内的私网地址配置为该第一地址，目的地址从该第二地址配置为该子网内的私网地址。

通过第二 VPC 的桥接，第一 VPC 通过第二 VPC 访问云下数据中心的子网，可以在第一 VPC 和第二 VPC 在私网地址段重叠的情况下实现第一 VPC 与第二 VPC 之间的通信。

- 30 根据第一方面的一种可能的实现方式，上述配置方法还包括以下步骤：在该第二 VPC 上配置远程连接网关，该远程连接网关与该子网远程连接；在该第二 VPC 上配置路由规则，该第二 VPC 上的路由规则包括：将目的地址为该第一地址的报文转发到该第一 VPC，将目的地址为该子网内的私网地址的报文转发到该远程连接网关。

通过配置路由规则，可使得第二 VPC 转发第一 VPC 与远程连接网关之间的报文，实现桥接。

- 35 根据第一方面的一种可能的实现方式，该配置方法还包括以下步骤：在该第一 VPC 中配置网络地址转换 NAT 网关，其中，将该 NAT 网关的私网地址配置为该第一地址，将该远程连接网关的私网地址配置为该第二地址；则，将该第一 VPC 内的私网地址与

第一地址进行绑定,将该子网内的私网地址与第二地址进行绑定包括:在该 NAT 网关上配置第一报文处理规则和第二报文处理规则,该第一报文处理规则包括:将出报文的源地址由该第一 VPC 内的私网地址转换为该第一地址,目的地址由该第二地址转换为该子网内的私网地址,并将修改后的出报文发送至该第二 VPC 的路由器;该第二报文处理规则包括:将入报文的源地址由该子网内的私网地址修改为该第二地址,目的地址由该第一地址转换为该第一 VPC 内的私网地址,并将修改后的入报文发送至该第一 VPC 的路由器。

通过配置报文规则, NAT 网关将第一 VPC 内的私网地址和第一地址绑定,并将云下数据中心的子网内的地址和第二地址绑定。

- 10 根据第一方面的一种可能的实现方式,该配置方法还包括配置路由规则的步骤,具体地,在该第一 VPC 的路由器上配置路由规则,该第一 VPC 的路由器上的路由规则包括:将目的地址为该第二地址的报文转发到该 NAT 网关,将目的地址为该第一 VPC 内的私网地址的报文转发到该第一 VPC 内的子网。

- 15 通过配置路由规则,可以使得第一 VPC 的路由器可以将报文在 NAT 网关和第一 VPC 的子网之间进行转发。

- 第二方面,本申请提供一种虚拟私有云 VPC 与云下数据中心通信的配置方法,具有相同私网地址段的第一虚拟私有云 VPC 和云下数据中心的子网通过第二 VPC 进行通信,该第二 VPC 的私网地址段与该第一 VPC、该第二 VPC 的私网地址段均不相同,该方法包括:在该第一 VPC 中配置网络地址转换 NAT 网关,以及在该第二 VPC 中配置与该子网连接的远程连接网关,其中,为该 NAT 网关配置第一地址,为该远程连接网关配置第二地址,该第一地址和该第二地址归属于该第二 VPC 的私网地址段,该第一地址以及该第二地址不相同;在该 NAT 网关上配置第一报文处理规则和第二报文处理规则,其中,该第一报文处理规则包括:将出报文的源地址由该第一 VPC 内的私网地址转换为该第一地址,目的地址由该第二地址转换为该子网内的私网地址,并将修改后的出报文发送至该第二 VPC 的路由器;该第二报文处理规则包括:将入报文的源地址由该子网内的私网地址修改为该第二地址,目的地址由该第一地址转换为该第一 VPC 内的私网地址,并将修改后的入报文发送至该第一 VPC 的路由器。

通过第二 VPC 的桥接,第一 VPC 内的设备可通过第二地址来访问远程连接网关。

- 30 根据第二方面的一种可能的实现方式,上述方法还包括以下步骤:配置该 NAT 网关与该第二 VPC 的连接,以及配置该远程连接网关与该云下数据中心的该子网远程连接。

由于 NAT 网关与该第二 VPC 连接,且远程连接网关与该云下数据中心的该子网远程连接,因此第一 VPC 可通过访问第二 VPC 的远程连接网关来访问该云下数据中心的该子网。

- 35 第三方面,本申请提供一种虚拟私有云 VPC 与云下数据中心的通信方法,具有相同私网地址段的第一虚拟私有云 VPC 和云下数据中心的子网通过第二 VPC 进行通信,该第二 VPC 的私网地址段与该第一 VPC、该子网的私网地址段均不相同,该方法包括:该第一 VPC 发送报文,该报文的源地址为第一地址,目的地址为该子网内的私网地址,该第一 VPC 内的私网地址与该第一地址绑定,该第一地址为归属于该第二 VPC 的私

网地址段的地址；该第二 VPC 接收该报文，根据预先设置的路由规则将该报文转发到该子网内的私网地址，其中该第二 VPC 的路由规则包括：将目的地址为该子网内的私网地址的报文转发到该子网，其中该第二 VPC 与该子网远程连接。

5 通过第二 VPC 的桥接，第一 VPC 通过访问与云下数据中心的子网绑定的第二地址来访问该子网，可以在第一 VPC 和第二 VPC 在私网地址段重叠的情况下实现第一 VPC 与第二 VPC 之间的通信。

根据第三方面的一种可能的实现方式，路由规则还包括：将目的地址为该第一地址的报文转发到该第一 VPC；该方法还包括：该子网发送响应报文至该第二 VPC，该响应报文的源地址为该子网内的私网地址，目的地址为该第一地址；该第二 VPC 接收
10 该响应报文，根据该路由规则将该响应报文转发到该第一 VPC。

通过设置路由规则，可使得云下数据中心的子网返回的应答报文通过第二 VPC 转发到第一 VPC，从而实现应答。

第四方面，本申请提供一种虚拟私有云 VPC 与云下数据中心通信的方法，具有相同私网地址段的第一虚拟私有云 VPC 和云下数据中心的子网通过第二 VPC 进行通信，
15 该第二 VPC 的私网地址段与该第一 VPC、该子网的私网地址段均不相同，该第一 VPC 设置有网络地址转换 NAT 网关，该第二 VPC 设置有远程连接网关，该 NAT 网关配置有第一地址，该远程连接网关配置有第二地址，该第一地址和该第二地址均归属于该第二 VPC 的私网地址段，该第一地址与该第二地址不相同，该远程连接网关远程连接该子网，该方法包括：该第一 VPC 的路由器接收第一 VPC 中的第一虚拟机发送的报文，其中，该报文的源地址为该第一设备的私网地址，目的地址为该第二地址；该第一 VPC 的路由器根据第一路由规则将该报文转发至该 NAT 网关；该 NAT 网关将该报文的源地址修改为该第一地址，目的地址修改为该子网中的第二设备的私网地址，将修改后的报文转发到该第二 VPC 的路由器，其中，该第二 VPC 的路由器设置有第二路由规则，该第一路由规则包括：目的地址属于该第二 VPC 的私网地址段的报文需要
20 转发至该 NAT 网关，该第二路由规则包括：目的地址属于该子网的私网地址段的报文需要转发至该第二 VPC 的远程连接网关。

通过第二 VPC 的桥接，第一虚拟机通过访问与云下数据中心的子网绑定的第二地址来访问连接云下数据中心的子网的远程连接网关，可以在第一 VPC 和第二 VPC 在私网地址段重叠的情况下实现第一 VPC 与云下数据中心的子网之间的通信。
30

在第四方面的一种可能的实现方式中，上述方法还包括以下步骤：第二 VPC 的路由器根据该第二路由规则将接收到的报文发送至该远程连接网关；该远程连接网关接收该报文，将该报文发送至该云下数据中心的子网。

由于远程连接网关与云下数据中心的子网远程连接，因此报文到达远程连接网关后，可经远程连接网关到达云下数据中心的子网。

35 第五方面，本申请提供虚拟私有云 VPC 与云下数据中心通信的配置装置，具有相同私网地址段的第一虚拟私有云 VPC 和云下数据中心的子网通过第二 VPC 进行通信，该第二 VPC 的私网地址段与该第一 VPC、该子网的私网地址段均不相同，该装置包括：地址绑定模块，用于将该第一 VPC 内的私网地址与第一地址进行绑定，将该子网内的私网地址与第二地址进行绑定，其中，该第一地址和该第二地址为归属于该第二 VPC

的私网地址段的地址，该第一地址与该第二地址不相同；地址配置模块，用于将该第一 VPC 发送至该子网的报文的源地址从该第一 VPC 内的私网地址配置为该第一地址，目的地址从该第二地址配置为该子网内的私网地址。

5 第五方面或第五方面任意一种实现方式是第一方面或第一方面任意一种实现方式对应的装置实现，第一方面或第一方面任意一种实现方式中的描述适用于第五方面或第五方面任意一种实现方式，在此不再赘述。

第六方面，本申请提供一种虚拟私有云 VPC 与云下数据中心通信的配置装置，具有相同私网地址段的第一虚拟私有云 VPC 和云下数据中心的子网通过第二 VPC 进行通信，该第二 VPC 的私网地址段与该第一 VPC、该第二 VPC 的私网地址段均不相同，
10 该装置包括：网关配置模块，用于在该第一 VPC 中配置 NAT 网关，以及在该第二 VPC 中配置与远程连接网关；地址配置模块，用于为该 NAT 网关配置第一地址，为该远程连接网关配置第二地址，该第一地址和该第二地址归属于该第二 VPC 的私网地址段，该第一地址以及该第二地址不相同；地址绑定模块，用于在该 NAT 网关上配置第一报文处理规则和第二报文处理规则，其中，该第一报文处理规则包括：将出报文的源地址由该第一 VPC 内的私网地址转换为该第一地址，目的地址由该第二地址转换为该子网内的私网地址，并将修改后的出报文发送至该第二 VPC 的路由器；该第二报文处理规则包括：将入报文的源地址由该子网内的私网地址修改为该第二地址，目的地址由该第一地址转换为该第一 VPC 内的私网地址，并将修改后的入报文发送至该第一 VPC 的路由器。
15

20 第六方面或第六方面任意一种实现方式是第二方面或第二方面任意一种实现方式对应的装置实现，第二方面或第二方面任意一种实现方式中的描述适用于第六方面或第六方面任意一种实现方式，在此不再赘述。

第七方面，本申请提供一种虚拟私有云 VPC 与云下数据中心的通信系统，包括第一 VPC 和第二 VPC，具有相同私网地址段的该第一 VPC 和云下数据中心的子网通过
25 该第二 VPC 进行通信，该第二 VPC 的私网地址段与该第一 VPC、该子网的私网地址段均不相同，其中，该第一 VPC，发送报文，该报文的源地址为第一地址，目的地址为该子网内的私网地址，该第一 VPC 内的私网地址与该第一地址绑定，该第一地址为归属于该第二 VPC 的私网地址段的地址；该第二 VPC，接收该报文，根据预先设置的路由规则将该报文转发到该子网内的私网地址，其中该第二 VPC 的路由规则包括：将
30 目的地址为该子网内的私网地址的报文转发到该子网，其中该第二 VPC 与该子网远程连接。

第七方面或第七方面任意一种实现方式是第三方面或第三方面任意一种实现方式对应的系统实现，第三方面或第三方面任意一种实现方式中的描述适用于第七方面或第七方面任意一种实现方式，在此不再赘述。

35 第八方面，本申请提供一种虚拟私有云 VPC 与云下数据中心通信的系统，包括第一 VPC 和第二 VPC，具有相同私网地址段的第一 VPC 和云下数据中心的子网通过第二 VPC 进行通信，该第二 VPC 的私网地址段与该第一 VPC、该子网的私网地址段均不相同，该第一 VPC 设置有网络地址转换 NAT 网关，该第二 VPC 设置有远程连接网关，该 NAT 网关配置有第一地址，该远程连接网关配置有第二地址，该第一地址和该

第二地址均归属于该第二 VPC 的私网地址段, 该第一地址与该第二地址不相同, 该远程连接网关远程连接该子网, 其中, 该第一 VPC 的路由器, 接收该第一 VPC 内的第一虚拟机发送的报文, 其中, 该报文的源地址为该第一虚拟机的私网地址, 目的地址为该第二地址; 该第一 VPC 的路由器, 根据第一路由规则将该报文转发至该 NAT 网关; 该 NAT 网关, 将该报文的源地址修改为该第一地址, 目的地址修改为该子网中的第二设备的私网地址, 将修改后的报文转发到该第二 VPC 的路由器, 其中, 该第二 VPC 的路由器设置有第二路由规则, 该第一路由规则包括: 目的地址属于该第二 VPC 的私网地址段的报文需要转发至该 NAT 网关, 该第二路由规则包括: 目的地址属于该子网的私网地址段的报文需要转发至该第二 VPC 的远程连接网关。

10 第八方面或第八方面任意一种实现方式是第四方面或第四方面任意一种实现方式对应的系统实现, 第四方面或第四方面任意一种实现方式中的描述适用于第八方面或第八方面任意一种实现方式, 在此不再赘述。

15 第九方面, 本申请提供一种计算设备, 包括至少一个存储器和至少一个处理器, 该至少一个存储器用于存储程序指令, 该至少一个处理器执行该程序指令, 以执行实现第一方面及其任一种可能的实现方式的方法。

第十方面, 本申请提供一种计算设备, 包括至少一个存储器和至少一个处理器, 该至少一个存储器用于程序指令, 该至少一个处理器执行该程序指令, 以执行实现第二方面及其任一种可能的实现方式的方法。

20 第十一方面, 本申请提供了一种非瞬态的可读存储介质, 该非瞬态的可读存储介质被计算设备执行时, 该计算设备执行前述第一方面或第一方面的任意可能的实现方式中提供的方法。该存储介质中存储了程序。该存储介质包括但不限于易失性存储器, 例如随机访问存储器, 非易失性存储器, 例如快闪存储器、硬盘(英文: hard disk drive, 缩写: HDD)、固态硬盘(英文: solid state drive, 缩写: SSD)。

25 第十二方面, 本申请还提供了一种非瞬态的可读存储介质, 该非瞬态的可读存储介质被计算设备执行时, 该计算设备执行前述第二方面或第二方面的任意可能的实现方式中提供的方法。该存储介质中存储了程序。该存储介质包括但不限于易失性存储器, 例如随机访问存储器, 非易失性存储器, 例如快闪存储器、硬盘(英文: hard disk drive, 缩写: HDD)、固态硬盘(英文: solid state drive, 缩写: SSD)。

30 第十三方面, 本申请提供了一种计算设备程序产品, 该计算设备程序产品包括计算机指令, 在被计算设备执行时, 该计算设备执行前述第一方面或第一方面的任意可能的实现方式中提供的方法。该计算机程序产品可以为一个软件安装包, 在需要使用前述第一方面或第一方面的任意可能的实现方式中提供的方法的情况下, 可以下载该计算机程序产品并在计算设备上执行该计算机程序产品。

35 第十四方面, 本申请还提供了另一种计算设备程序产品, 该计算设备程序产品包括计算机指令, 在被计算设备执行时, 该计算设备执行前述第二方面或第二方面的任意可能的实现方式中提供的方法。该计算机程序产品可以为一个软件安装包, 在需要使用前述第二方面或第二方面的任意可能的实现方式中提供的方法的情况下, 可以下载该计算机程序产品并在计算设备上执行该计算机程序产品。

附图说明

- 图 1 是一种 VPC 通信系统的系统结构示意图；
图 2 是 VPC 通信系统的另一系统结构示意图；
图 3 是根据本发明实施例的 VPC 与云下数据中心通信的配置方法的流程图；
5 图 4 是根据本发明实施例的 VPC 通信系统的系统结构示意图；
图 5 是本发明实施例的 VPC 与云下数据中心的通信方法的数据交互图；
图 6 是根据本发明实施例的配置装置的装置结构示意图；
图 7 是根据本发明实施例的计算设备的装置结构示意图。

10 具体实施方式

- 首先，本发明实施例涉及的名词解释如下：
云上数据中心：提供公有云业务的数据中心。
云下数据中心：提供非公有云业务的数据中心，云下数据中心提供本地部署业务的情况下，云下数据中心包括多个物理机（physical machine），云下数据中心提供私有云业务的情况下，云下数据中心包括多个虚拟机。
15 公有云业务：即基础设施即服务（Infrastructure as a Service, IaaS）是指把公有云业务提供方提供的基础设施作为一种服务通过互联网对外提供。在这种服务模型中，用户不用自己构建一个数据中心，而是通过租用的方式来使用服务器、存储和网络等基础设施。公有云业务通过提供虚拟环境（例如虚拟机）实现，公有云的核心属性是多用户共享云基础设施且用户之间隔离。
20 非公有云业务：单个用户专属的基础设施，例如为私有云业务和本地部署业务。
私有云(Private Clouds)业务：单个用户拥有服务器、存储和网络等基础设施，并可以完全控制此基础设施，私有云业务通过提供虚拟环境（例如虚拟机）实现，私有云业务的核心属性是单用户独享基础设施。
25 本地部署（On-premises）业务：单个用户在本地自建服务器、存储和网络等基础设施，该用户独享该自建的基础设施，本地部署业务通过物理机（physical machine）实现。
私网地址：不能在互联网寻址，只能在局域网中寻址的 IP 地址，私网地址被禁止出现在互联网中。

- 30 私网地址是一段保留的 IP 地址，私网地址的分类、网段以及数量如下表所示：

私网地址分类	网段	可用私网地址数量
A 类私网地址	192.168.0.0/16	65,532
B 类私网地址	172.16.0.0/12	1,048,572
C 类私网地址	10.0.0.0/8	16,777,212

- 虚拟私有网络（Virtual Private Cloud, VPC）： VPC 设置于公有云中，VPC 是公有云业务的用户在云上数据中心的的局域网。
具体而言，VPC 隔离了虚拟网络，每个 VPC 都有一个独立的隧道号，一个隧道号对应着一个虚拟化网络。一个 VPC 内的虚拟机之间的报文对应有相同的隧道标识，然后送到物理网络上进行传输。不同 VPC 内的虚拟机因为所在的隧道标识不同，本身处
35

于两个不同的路由平面，所以不同 VPC 内的虚拟机无法进行通信，天然地实现了逻辑隔离。

隧道标识可例如为虚拟局域网标识（Virtual Local Area Network Identification, VLAN ID）或虚拟网络标识（Virtual Network ID, VNI）。

5

首先请参见图 1，图 1 是一种 VPC 通信系统的系统结构示意图，如图 1 所示，VPC 通信系统包括云上数据中心 10、客户端 7 以及云下数据中心 20，云上数据中心 10、客户端 7 以及云下数据中心 20 均接入互联网 8，客户端 7 通过互联网 6 访问云上数据中心 10。

10 如图 1 所示，云上数据中心 10 为公有云用户提供 VPC1，VPC1 包括子网 1 和子网 2，子网 1 和子网 2 与路由器 1 连接，子网 1 包括虚拟机（virtual machine, VM）1、VM2 以及交换机 1，子网 2 包括 VM3、VM4 以及交换机 2，VM1 和 VM2 与交换机 1 连接，VM3 和 VM4 与交换机 2 连接。

路由器 1 用于转发子网 1 和子网 2 之间通信的报文。

15 云下数据中心 20 包括子网 3 和远程连接网关 2，子网 3 包括交换机 3、物理机（Physical machine, PM）1 和 PM2，PM1 和 PM2 与交换机 3 连接，交换机 3 与远程连接网关 2 连接。

如图 1 所示，子网 1 和子网 3 具有相同的私网网段，因此子网 1 和子网 2 私网地址重叠。

20 客户端 7 通过互联网 8 访问控制平台 6，在控制平台 6 中输入配置信息，控制平台 6 根据配置信息在云上数据中心 10 配置 VPC1，具体地，可配置 VPC1 中的各功能模块，例如可创建或删除 VPC1，在 VPC1 中创建或删除虚拟机，配置 VPC1 中的路由器的路由规则等，控制平台 6 可根据用户输入的配置信息对 VPC 进行管理。

控制平台 6 配置好 VPC1 后，客户端 7 可通过远程桌面登陆 VPC1 的 VM1-4。

25 客户端 7 例如为具有上网功能手机、个人电脑、个人数字助理等终端设备，公有云用户通过操作客户端 7 访问云数据中心 10 提供的 VM1-4。

云下数据中心 20 归属于公有云用户，云上数据中心 10 归属于公有云服务提供商，公有云用户通过向公有云服务提供方付费获得云上数据中心 10 的 VPC1 的控制和管理权限，在一些业务需求中，公有云用户需将子网 3 和子网 1 连通，因此需在 VPC1 中配置远程连接网关 1，来与云下数据中心 20 的远程连接网关 2 连接，具体可参见图 2。

30 图 2 是 VPC 通信系统的另一系统结构示意图，与图 1 相比，图 2 增设远程连接网关 1，且远程连接网关 1 与远程连接网关 2 之间建立有远程通信隧道，IP 报文可通过远程通信隧道在 VPC1 与子网 3 之间传输。

当 VM1 需和 PM1 通信，假设子网 1 和子网 3 具有不同的私网地址段，则子网 1 中的 VM1 可构造 IP 报文，该 IP 报文的源 IP 地址是 VM1 在子网 1 的私网地址，目的 IP 地址是 PM1 在子网 3 的私网地址，该 IP 报文经由交换机 1、路由器 1、远程连接网关 1、远程连接网关 2、交换机 6 到达 PM1。

但是，图 2 所示的网络环境中，子网 1 和子网 3 具有相同的私网地址段，因此 VM1 构造的 IP 报文的源 IP 地址是 VM1 在子网 1 的私网地址 192.168.0.2，目的 IP 地址是

PM1 在子网 3 的私网地址 192.168.0.2, 该 IP 报文的源 IP 地址和目的 IP 地址相同, 该 IP 报文会被 VM1 的操作系统拦截, 或者会被交换机 1 返回到 VM1。

同理, PM1 发送至 VM1 的 IP 报文的源 IP 地址和目的 IP 地址也相同, 也会产生相同的技术问题。

5

为解决以上技术问题, 本发明实施例提供一种 VPC 与云下数据中心通信的配置方法, 该方法在图 1 所示的 VPC 系统的基础上进行配置, 具体请参见图 3, 图 3 是根据本发明实施例的 VPC 与云下数据中心通信的配置方法的流程图, 该方法具体包括以下步骤:

10 步骤 S101: 在云上数据中心 10 创建 VPC2。

步骤 S102: 在 VPC1 创建网络地址转换 (Network address translation, NAT) 网关 10, 并设置 NAT 网关 10 与 VPC2 连接。

其中 NAT 网关 10 设置有 VPC2 的私网地址段中的私网地址 10.0.0.9。

值得注意的是, NAT 网关 10 也设置有 VPC1 的私网地址段中私网地址, 本发明
15 实施例如无特别说明, 所提及的 NAT 网关 10 的私网地址均是指 NAT 网关 10 在 VPC2 中的私网地址 10.0.0.9。

步骤 S103: 在 VPC2 创建并配置远程连接网关 3, 并设置远程连接网关 3 与远程连接网关 2 远程连接。

其中远程连接网关 3 设置有 VPC2 的私网地址段中的私网地址 10.0.0.10。

20 远程连接网关例如为专线网关, 或虚拟私有网络 (Virtual private network) VPN 网关。

步骤 S104: 配置 NAT 网关 10 的报文处理规则:

报文处理规则 1:

源 IP 地址是 192.168.0.2, 目的 IP 地址是 10.0.0.10 的出报文, 源 IP 地址修改为
25 10.0.0.9, 目的 IP 地址修改为 192.168.0.2, 并将修改后的出报文发送至路由器 3。

报文处理规则 2:

源 IP 地址是 192.168.0.2, 目的 IP 地址是 10.0.0.9 的入报文, 源 IP 地址修改为
10.0.0.10, 目的 IP 地址修改为 192.168.0.2, 并将修改后的入报文发送至路由器 1。

其中, 出报文是指 NAT 网关 10 从路由器 1 接收到的报文, 入报文是指 NAT 网关
30 10 从路由器 2 接收到的报文。

步骤 S105: 配置 VPC1 的路由规则:

路由规则 1: 将目的 IP 地址属于 10.0.0.0/24 的报文转发至 NAT 网关 10;

路由规则 2: 将目的 IP 地址属于 192.168.0.0/24 的报文转发至子网 1。

该路由规则应用于 VPC1 的路由器 1。

35 步骤 S106: 配置 VPC2 的路由规则:

路由规则 3: 将目的 IP 地址是 10.0.0.9 的报文转发至 NAT 网关 10;

路由规则 4: 将目的 IP 地址是 192.168.0.2 转发至远程连接网关 3。

该路由规则应用于 VPC2 的路由器 2。

上述配置方法由控制平台 6 执行, 并请结合图 4, 图 4 是经图 3 所示的配置方法

对图 1 所示的 VPC 进行配置之后的 VPC 通信系统结构示意图。如图 4 所示，通过上述配置，使得子网 1 与 NAT 网关 10 绑定，子网 2 与远程连接网关 3 绑定，通过 VPC2 实现桥接，打通子网 1 和子网 3，VM1 通过构造目的 IP 地址是远程连接网关 3 的私网地址的 IP 报文，即可访问 PM1，而 PM1 通过构造目的 IP 地址是 NAT 网关 2 的私网地址的 IP 报文，即可访问 VM1。

以下请参见图 5，图 5 是本发明实施例基于图 4 所示的 VPC 通信系统的 VPC 与云下数据中心的通信方法的数据交互图，该通信方法用于揭示 VM1 与 PM1 进行通信的过程，如图 5 所示，该方法包括以下步骤：

步骤 1：VM1 构造 IP 报文 1 并将 IP 报文 1 发送至交换机 1。

10 IP 报文 1 的 IP 头的源 IP 地址是 VM1 在子网 1 的私网地址 192.168.0.2，目的 IP 地址是远程连接网关 2 的私网地址 10.0.0.10，IP 报文 1 的数据部分携带有请求信息。

值得注意的是，VM1 根据业务需要，可以提前查询获取 10.0.0.10 与 PM1 的对应关系，例如可以向第二 VPC 查询 10.0.0.10 与 PM1 的对应关系，也可以向控制平台 6 查询 10.0.0.10 与 PM1 的对应关系。

15 步骤 2：交换机 1 转发 IP 报文 1 至路由器 1。

交换机 1 接收 IP 报文 1 后，确认 IP 报文 1 的目的 IP 地址不属于子网 1，将 IP 报文 1 发送至路由器 1 进行跨网段报文传输。

步骤 3：路由器 1 根据路由规则 1 转发 IP 报文 1。

20 路由器 1 接收 IP 报文 1 后，根据 IP 报文 1 的目的 IP 地址（10.0.0.10）匹配路由规则 1，根据路由规则 1 将 IP 报文 1 发送至 NAT 网关 10。

步骤 4：NAT 网关 10 根据报文处理规则 1 修改 IP 报文 1 的源 IP 地址并发送修改后的 IP 报文 1 至路由器 3。

25 NAT 网关 10 从路由器 1 接收 IP 报文 1 后，由于 IP 报文 1 来自路由器 1，因此确认 IP 报文 1 为出报文，匹配报文处理规则 1，将 IP 报文 1 的源 IP 地址从 192.168.0.2 修改为 10.0.0.9，目的 IP 地址从 10.0.0.10 修改为 192.168.0.2，并将修改后的 IP 报文 1 发送至路由器 3。

步骤 5：路由器 3 根据路由规则 4 转发 IP 报文 1 至远程连接网关 3。

路由器 3 接收 IP 报文 1 后，根据 IP 报文 1 的目的 IP 地址（192.168.0.2）匹配路由规则 4，将 IP 报文 1 转发至远程连接网关 3。

30 步骤 6：远程连接网关 3 通过远程通信隧道发送 IP 报文 1 至远程连接网关 2。

步骤 7：远程连接网关 2 转发 IP 报文 1 至交换机 6。

步骤 8：交换机 6 将 IP 报文 1 发送至 PM1。

交换机 6 根据 IP 报文 1 的目的 IP 地址 192.168.0.2 将 IP 报文 1 发送至 PM1。

步骤 9：PM1 构造并发送 IP 报文 2 至交换机 6。

35 IP 报文 2 是 IP 报文 1 的应答报文。

PM1 接收 IP 报文 1 之后，从 IP 报文 1 的数据部分获取请求信息，根据请求信息产生应答信息，并构造 IP 报文 2，具体地，PM1 将 IP 报文 1 的源 IP 地址 10.0.0.9 设置为 IP 报文 2 的目的 IP 地址，将 IP 报文 1 的目的 IP 地址 192.168.0.2 设置为 IP 报文 2 的源 IP 地址，将应答信息设置于 IP 报文 2 的数据部分，将 IP 报文 2 发送至交换机

6。

步骤 10: 交换机 6 转发 IP 报文 2 至远程连接网关 2。

交换机 6 接收 IP 报文 2 后, 确认 IP 报文 2 的目的 IP 地址 10.0.0.9 不属于子网 3 (192.168.0.0/24), 将 IP 报文 2 发送至远程连接网关 2 进行远程报文传输。

5 步骤 11: 远程连接网关 2 通过远程通信隧道发送 IP 报文 2 至远程连接网关 3。

步骤 12: 远程连接网关 3 发送 IP 报文 2 至路由器 3。

步骤 13: 路由器 3 根据路由规则 3 转发 IP 报文 2 至 NAT 网关 10。

路由器 3 接收 IP 报文 2 后, 根据 IP 报文 2 的目的 IP 地址 (10.0.0.9) 匹配路由规则 3, 将 IP 报文 2 转发至 NAT 网关 10。

10 步骤 14: NAT 网关 10 根据报文处理规则 2 修改 IP 报文 2 并发送修改后的 IP 报文 2 至路由器 1。

NAT 网关 10 从路由器 3 接收 IP 报文 2 后, 由于 IP 报文 2 来自路由器 3, 因此确认 IP 报文 2 是入报文, 匹配报文处理规则 2, 将 IP 报文 2 的目的 IP 地址从 10.0.0.9 修改为 192.168.0.2, 源地址从 192.168.0.2 修改为 10.0.0.10, 并将修改后的 IP 报文 2

15 发送至路由器 1。

步骤 15: 路由器 1 根据路由规则 2 转发修改后的 IP 报文 2 至交换机 1。

路由器 1 根据 IP 报文 2 的目的 IP 地址 192.168.0.2 匹配路由规则 2, 将 IP 报文 2 发送至子网 1, 具体地, 是将 IP 报文 2 发送至子网 1 的交换机 1。

步骤 16: 交换机 1 将 IP 报文 2 发送至 VM1。

20 交换机 1 根据 IP 报文 2 的目的 IP 地址 192.168.0.2 将 IP 报文 2 发送至 VM1。

VM1 接收到 IP 报文 2 后, 根据 IP 报文 2 的源 IP 地址 10.0.0.10 和目的 IP 地址 192.168.0.2 确认 IP 报文 2 是 IP 报文 1 的应答报文(由于 IP 报文 2 的源 IP 地址和目的 IP 地址与 IP 报文 1 相比是倒置的), VM1 从 IP 报文 2 的数据部分获取应答信息, 从而完成 VM1 与 VM2 之间的通信过程。

25 综上, 通过在云上数据中心 10 配置 NAT 网关 1 和 VPC2, 并进行规则配置, 可使得云上的 VM1 和云下的 PM1 在私网地址相同的情况下也能够实现通信。

举例而言, 本发明实施例适用于以下场景, 即 VPC2 作为企业内部的大网, 而 VPC1 作为企业内部小网, VPC1 例如为财务部的虚拟网络, 子网 3 例如为研发部的本地部署网络, VPC2 例如为企业的 IT 管理部的虚拟网络, 当 VPC1 与子网 3 私网地址重叠时, 可向控制平台申请 VPC2 的私网地址, 例如 VPC1 申请到 VPC2 的私网地址 1, 子网 3 申请到 VPC2 的私网地址 2, 控制平台通过在 NAT 网关 10 设置报文处理规则将 VPC1 中的虚拟机与私网地址 1 绑定, 将子网 3 中的物理机与私网地址 2 绑定, VPC1 的虚拟机可通过访问私网地址 2 来访问子网 3 中的物理机, 子网 3 中的物理机可通过访问私网地址 1 来访问 VPC1 的虚拟机, 从而解决企业内部云上和云下私网地址重叠而造成不能相互通信的技术问题。

35 值得注意的是, 在本发明实施例中, 云下数据中心也可以设置虚拟机, 即 PM 可以替换为 VM, 本发明实施例对此不作限定。

并且, 在本发明其他实施例中, 可进一步对 NAT 网关 10 设置报文处理规则 3 和

4, 以替代报文处理规则 1 和 2。

报文处理规则 3:

源 IP 地址是 192.168.0.2, 目的 IP 地址是 10.0.0.10 的出报文, 源 IP 地址修改为 9.9.9.9, 目的 IP 地址修改为 192.168.0.2, 并将修改后的出报文发送至路由器 3;

5 报文处理规则 4:

源 IP 地址是 192.168.0.2, 目的 IP 地址是 9.9.9.9 的入报文, 源 IP 地址修改为 10.0.0.10, 目的 IP 地址修改为 192.168.0.2, 并将修改后的入报文发送至路由器 1。

在该实施例中, 假设 PM1 只信任源 IP 地址是 9.9.9.9 的 IP 报文, 且在接收到源 IP 地址非 9.9.9.9 的 IP 报文时, 会丢弃该 IP 报文, 此时, 通过配置报文处理规则 3 和 4
10 到 NAT 网关 10, 使得 PM1 接收到的 IP 报文的源 IP 地址是 9.9.9.9, 从而确保 PM1 不会丢弃该 IP 报文, 而是对该 IP 报文应答。

本实施例适用于 PM1 设置有重要的数据库的情况, 例如 PM1 为银行的数据库, VPC 需通过 NAT 网关 10 进行源地址转换, 将 VPC1 内虚拟机发出的 IP 报文的源地址修改为 PM1 的信任地址, 才能保证 PM1 对该 IP 报文进行正常处理。

15

进一步, 请参见图 6, 图 6 示出根据本发明实施例的配置装置的装置结构示意图, 如图 6 所示, 配置装置 60 包括地址绑定模块 601、网关配置模块 602、地址配置模块 603, 路由规则配置模块 604, 其中, 网关配置模块 602 用于执行上述实施例揭示的配置方法中创建 NAT 网关和远程连接网关的动作, 地址配置模块 603 用于执行上述实施例揭示的配置方法中为 NAT 网关和远程连接网关配置私网地址的动作, 地址绑定模块
20 601 用于执行上述实施例揭示的配置方法中为 NAT 网关配置报文处理规则的动作, 路由规则配置模块 604 用于执行上述实施例揭示的配置方法中为路由器配置路由规则的动作。

其中, 配置装置 60 可设置在以上实施例所揭示的控制平台 6 中。

25

以下请参见图 7, 图 7 示出根据本发明实施例的计算设备的装置结构示意图, 如图 7 所示, 计算设备可以包括处理单元 421 和通信接口 422, 处理单元 421 用于执行物理服务器上运行的操作系统以及各种软件程序所定义的功能, 例如, 用于实现图 2 所示的控制平台 6 的功能。通信接口 422 用于与其他计算节点进行通信交互, 其他设备可以是其它物理服务器, 具体地, 通信接口 422 可以是网络适配卡。可选地, 该物理服务器还可以包括输入/输出接口 423, 输入/输出接口 423 连接有输入/输出设备, 用于接收输入的信息, 输出操作结果。输入/输出接口 423 可以为鼠标、键盘、显示器、或者光驱等。可选地, 该物理服务器还可以包括辅助存储器 424, 一般也称为外存, 辅助存储器 424 的存储介质可以是磁性介质(例如, 软盘、硬盘、磁带)、光介质(例如光盘)、或者半导体介质(例如固态硬盘)等。处理单元 421 可以有多种具体实现形式,
30 例如处理单元 421 可以包括处理器 4212 和存储器 4211, 处理器 4212 根据存储器 4211 中存储的程序指令执行上述实施例中控制平台 6 的相关操作, 处理器 4212 可以为中央处理器(CPU)或图像处理器(英文: graphics processing unit, GPU), 处理器 4212 可以是单核处理器或多核处理器。处理单元 421 也可以单独采用内置处理逻辑的逻辑器件来实现, 例如现场可编程门阵列(英文全称: Field Programmable Gate Array, 缩
35

写：FPGA）或数字信号处理器（英文：digital signal processor，DSP）等。

所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。上述各个附图对应的流程的描述各有侧重，某个流程中没有详述的部分，可以参见其他

5 其他流程的相关描述。

进一步地，在本发明其他实施例中，也可以使用容器来替换虚拟机，本发明实施例对此不作限定。

需说明的是，以上描述的任意装置实施例都仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部进程来实现本实施例方案的目的。另外，本发明提供的装置实施例附图中，进程之间的连接关系表示它们之间具有通信连接，具体可以实现为一条或多条通信总线或信号线。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

15 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件的方式来实现，当然也可以通过专用硬件包括专用集成电路、专用CPU、专用存储器、专用元器件等来实现。一般情况下，凡由计算机程序完成的功能都可以很容易地用相应的硬件来实现，而且，用来实现同一功能的具体硬件结构也可以是多种多样的，例如模拟电路、数字电路或专用电路等。但是，对本发明而言更多情况下软件程序实现是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在可读取的存储介质中，如计算机的软盘，U盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，主机，20 或者网络设备等）执行本发明各个实施例所述的方法。

所属领域的技术人员可以清楚地了解到，上述描述的系统、装置或单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，30 都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。