

虚拟私有云 VPC 之间互通的实现系统及其方法

技术领域

[01]本说明书一个或多个实施例涉及网络技术领域，尤其涉及虚拟私有云 VPC 之间互通的实现系统及其方法。

背景技术

[02]在现代云计算环境中，虚拟私有云（Virtual Private Cloud，VPC）已经成为了一种常用的网络架构模式。每个 VPC 对应一个虚拟网络，可以独立设置网际协议（Internet Protocol，IP）地址范围、路由表、安全组等网络配置，并且与其他 VPC 相互隔离。

[03]相关技术中，不同的 VPC 之间默认是无法访问的，因此，在某些情况下，可能需要将不同的 VPC 打通，以实现跨 VPC 的流量转发和数据传输。

[04]但是，VPC 之间的打通会增加安全风险和管理复杂度，因此，亟需一种虚拟私有云之间的互通方案，以在打通不同的 VPC 时，提高跨 VPC 网络通信的安全性和可靠性。

发明内容

[05]有鉴于此，本说明书一个或多个实施例提供一种虚拟私有云 VPC 之间互通的实现系统及其方法。

[06]为实现上述目的，本说明书一个或多个实施例提供技术方案如下。

[07]根据本说明书一个或多个实施例的第一方面，提出了一种虚拟私有云 VPC 之间互通的实现系统，包括源 VPC、中继 VPC 和目标 VPC；其中，

源 VPC，用于将访问流量发送到中继 VPC；

中继 VPC，用于将源 VPC 发送的访问流量发送到目标 VPC；

目标 VPC，用于接收中继 VPC 发送的访问流量。

[08]根据本说明书一个或多个实施例的第二方面，提出了一种虚拟私有云 VPC 之间的互通方法，包括：

源 VPC 向中继 VPC 发送访问流量；

中继 VPC 将源 VPC 发送的访问流量发送到目标 VPC；

目标 VPC 接收中继 VPC 发送的访问流量。

[09]本说明书所提供的方案，通过在源 VPC 和目标 VPC 之间引入中继 VPC，源 VPC 可以将访问流量发送到中继 VPC，由中继 VPC 将访问流量转发给目标 VPC，以便目标 VPC 可以接收到源 VPC 发送的访问流量，以在源 VPC 和目标 VPC 之间形成网络隔离的前提下，实现源 VPC 与目标 VPC 之间的通信，从而使得源 VPC 和目标 VPC 之间的网络不会相互暴露，提高跨 VPC 网络通信的安全性和可靠性。

附图说明

[10]图 1 是一示例性实施例提供的一种 VPC 之间互通的实现系统。

[11]图 2 是一示例性实施例提供的一种 VPC 之间互通的实现系统。

[12]图 3 是一示例性实施例提供的一种 VPC 之间互通的实现系统。

[13]图 4 是一示例性实施例提供的一种虚拟私有云 VPC 之间的互通方法的流程图。

具体实施方式

[14]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[15]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[16]本说明书所涉及的用户信息（包括但不限于用户设备信息、用户个人信息等）和数据（包括但不限于用于分析的数据、存储的数据、展示的数据等），均为经用户授权或者经过各方充分授权的信息和数据，并且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准，并提供有相应的操作入口，供用户选择授权或者拒绝。

[17]相关技术中，VPC 作为一种虚拟的网络环境，可以用于在公共云平台中构建和管理

用户的私有网络，以在公共云环境中提供安全隔离、网络定制化、跨低于互联、弹性和可伸缩性等多种功能，帮助用户构建私有、安全、灵活和可靠的云网络环境，以满足用户多种多样的业务需求。

[18]以用于提供数据库（Database，DB）服务的公共云环境为例，数据库服务可以部署在数据库公有云云服务提供商所维护的 VPC 中，客户使用数据库服务的应用程序（Application，APP）可以部署在客户自己维护的 VPC 中，如果客户的 APP 要使用数据库公有云云服务提供商提供的数据库服务，则需要将数据库公有云云服务提供商所维护的 VPC 与客户所维护的 VPC 打通，以实现数据库服务的跨 VPC 使用。

[19]但是，如果将两个 VPC 之间直接打通，则会导致两个 VPC 之间的网络相互暴露，带来安全隐患风险。

[20]有鉴于此，本说明书期望提供一种虚拟私有云 VPC 之间互通的实现系统及其方法，以在源 VPC 和目标 VPC 之间形成网络隔离的前提下，实现源 VPC 与目标 VPC 之间的通信，从而使得源 VPC 和目标 VPC 之间的网络不会相互暴露，提高跨 VPC 网络通信的安全性和可靠性。

[21]可选地，本说明书所提供的方案，不仅可以应用到用于提供数据库服务的网络环境中，还可以应用到其他用于提供不同服务功能的网络环境中，本说明书对具体的应用场景不加以限定。

[22]下面对本说明书所提供的虚拟私有云 VPC 之间互通的实现系统及其方法进行详细介绍。

[23]参见图 1，图 1 是一示例性实施例提供的一种 VPC 之间互通的实现系统。如图 1 所示，上述 VPC 之间互通的实现系统可以包括源 VPC、中继 VPC 和目标 VPC。

[24]其中，源 VPC，用于将访问流量发送到中继 VPC；中继 VPC，用于将源 VPC 发送的访问流量发送到目标 VPC；目标 VPC，用于接收中继 VPC 发送的访问流量。

[25]可选地，源 VPC 与中继 VPC 之间可以通过私有连接相连，中继 VPC 与目标 VPC 之间可以通过私有连接相连。

[26]其中，私有连接可以为虚拟私有云对等连接（VPC Peering）。VPC Peering 可以用于实现两个 VPC 之间的网络连接，通过此连接，可以使用私有的互联网协议第四版（Internet Protocol Version 4，IPv4）地址或互联网协议第六版（Internet Protocol Version 6，IPv6）地址在两个 VPC 之间路由流量，以便这两个 VPC 中的实例可以彼此通信，

就像它们在同一个网络中一样。

[27]通过使用 VPC Peering 实现源 VPC 与中继 VPC 之间、以及中继 VPC 与目标 VPC 之间的连接，可以充分利用通过 VPC Peering 实现 VPC 之间的路由不具有传递性的特性，以实现源 VPC 和目标 VPC 之间的相互隔离。

[28]源 VPC 和中继 VPC 通过 VPC Peering 连接、中继 VPC 和目标 VPC 通过 VPC Peering 连接后，源 VPC 和中继 VPC 之间可以直接相互访问，中继 VPC 和目标 VPC 之间可以直接相互访问，但源 VPC 和目标 VPC 之间无法直接相互访问，也即是，源 VPC 中的虚拟机（Virtual Machine，VM）不能直接与目标 VPC 中的 VM 实现内部访问，以实现源 VPC 和目标 VPC 的相互隔离。

[29]可选地，可以在中继 VPC 中引入一个网络中间件，以通过该网络中间件提供流量转发的功能。

[30]在一些实施例中，中继 VPC 在将源 VPC 发送的访问流量发送到目标 VPC 时，可以通过网络中间件，将源 VPC 发送的访问流量发送到目标 VPC。

[31]例如，可以由源 VPC 中的 APP 向中继 VPC 中的网络中间件发送访问流量，中继 VPC 中的网络中间件可以将访问流量转发给目标 VPC 中的相应服务，以便目标 VPC 中的服务可以接收到访问流量。

[32]其中，网络中间件可以为代理服务器（Proxy），或者，网络中间件可以为负载均衡器（Load Balancer，LB）。

[33]以网络中间件为代理服务器为例，参见图 2，图 2 是一示例性实施例提供的一种 VPC 之间互通的实现系统，如图 2 所示，可以由源 VPC 中的 APP 向中继 VPC 中的代理服务器（也即是 Proxy）发送访问流量，中继 VPC 中的 Proxy 可以将访问流量转发给目标 VPC 中的相应服务，以便目标 VPC 中的服务可以接收到访问流量。

[34]以网络中间件为负载均衡器为例，参见图 3，图 3 是一示例性实施例提供的一种 VPC 之间互通的实现系统，如图 3 所示，可以由源 VPC 中的 APP 向中继 VPC 中的负载均衡器（也即是 LB）发送访问流量，中继 VPC 中的 LB 可以将访问流量转发给目标 VPC 中的相应服务，以便目标 VPC 中的服务可以接收到访问流量。

[35]在一些实施例中，中继 VPC 除可以起到连通源 VPC 和目标 VPC 的作用之外，还可以提供过滤流量的能力。例如，可以通过中继 VPC 中的网络中间件来对访问流量进行过滤，以保证仅有按照目标协议（如某种特定协议）封装得到的访问流量可以通过。

[36]可选地，访问流量可以为按照目标协议封装得到的网络流量，目标协议可以用于指示访问流量的数据传输格式。以用于提供数据库服务的公共云环境中的 VPC 互通实现系统为例，目标协议可以为结构化查询语言（My Structured Query Language, MySQL）访问协议，或者，目标协议可以为甲骨文（Oracle）访问协议，但不限于此，本说明书对目标协议的具体类型不加以限定。

[37]在一些实施例中，中继 VPC 可以将访问流量转发到目标 VPC 的目标端口（如特定协议端口），以便目标 VPC 可以通过目标端口接收中继 VPC 发送的访问流量。其中，目标端口可以为专门用于接收访问流量的网络端口。

[38]基于如上所述的系统，可以通过如下的虚拟私有云 VPC 之间的互通方法，实现源 VPC 和目标 VPC 的连通。

[39]需要说明的是，上述实施例是以中继 VPC 用于连通一个源 VPC 和一个目标 VPC 为例来进行说明的，在更多可能的实现方式中，中继 VPC 所连通是源 VPC 和目标 VPC 的数量可以更多，也即是，一个中继 VPC 可以实现多个源 VPC 和多个目标 VPC 之间的打通。

[40]例如，对于网络地址段之间没有重叠的多个源 VPC 和多个目标 VPC，可以通过一个中继 VPC 实现这多个源 VPC 和多个目标 VPC 之间的打通，但是，如果需要打通的源 VPC 和目标 VPC 的网络地址段之间有重叠交集，则可以通过不同的中继 VPC 来实现源 VPC 和目标 VPC 之间的打通。

[41]也即是，中继 VPC 可以用于连通网络地址段之间没有重叠的多个源 VPC 和多个目标 VPC，对于与既有 VPC 有网络地址段重叠的 VPC，可以单独新建一个中继 VPC 来负责实现 VPC 打通。

[42]参见图 4，图 4 是一示例性实施例提供的一种虚拟私有云 VPC 之间的互通方法的流程图，如图 4 所示，该方法包括步骤 401 至 403。

[43]步骤 401、源 VPC 向中继 VPC 发送访问流量。

[44]需要说明的是，源 VPC 和中继 VPC 可以部署在同一个公共云环境中。

[45]可选地，访问流量可以为任意类型的网络流量，例如，访问流量可以为数据库服务流量、文件传输流量、邮件流量、视频流量、语音流量、实时通信流量、网络管理流量等，本说明书对访问流量的具体类型不加以限定。

[46]其中，数据库服务流量可以为应用程序与数据库服务进行交互时产生的流量。文件传输流量可以为通过文件传输协议（File Transfer Protocol, FTP）或其他文件传输方式进行文件上传和/或下载时所产生的流量。邮件流量可以为通过电子邮件协议发送和/或接收电子邮件时产生的流量。视频流量可以为通过流媒体协议传输视频内容时所产生的流量。语音流量可以为通过因特网语音协议（Voice over Internet Protocol, VoIP）或实时语音通信应用产生的语音通信流量。实时通信流量可以为通过即时通信服务（如即时消息、语音通话、视频通话）产生的流量。网络管理流量可以为网络运行过程中用于管理网络运行状态的流量。

[47]以访问流量为数据库服务流量为例，数据库服务流量可以包括数据库查询流量、数据库写入流量、数据库连接流量、数据库备份流量、数据库事务流量、数据库管理流量、数据库安全流量等，但不限于此。

[48]其中，数据库查询流量可以为应用程序向数据库发送查询请求时产生的流量。数据库写入流量可以为应用程序向数据库执行插入、更新或删除操作时产生的流量。数据库连接流量可以为应用程序与数据库建立连接时所产生的流量。数据库备份流量可以为数据库执行备份操作时所产生的流量。数据库事务流量可以为应用程序执行事务操作时产生的流量。数据库管理流量可以为用于监测和管理数据库性能和状态的流量。数据库安全流量可以为数据库安全相关的通信流量，包括但不限于身份验证和授权过程中进行数据传输时产生的流量、以及加密和解密操作时所产生的流量。

[49]步骤 402、中继 VPC 将源 VPC 发送的访问流量发送到目标 VPC。

[50]需要说明的是，中继 VPC 可以作为源 VPC 和目标 VPC 之间的中转站，以将源 VPC 发送的流量中转桥接到目标 VPC，以在实现源 VPC 和目标 VPC 之间的通信的前提下，避免源 VPC 和目标 VPC 直接互通，以在源 VPC 和目标 VPC 之间形成网络隔离，以有效应对网络攻击。

[51]步骤 403、目标 VPC 接收中继 VPC 发送的访问流量。

[52]通过本说明书所提供的虚拟私有云 VPC 之间的互通方法，源 VPC 可以将访问流量发送到中继 VPC，由中继 VPC 将访问流量转发给目标 VPC，以便目标 VPC 可以接收到源 VPC 发送的访问流量，以在源 VPC 和目标 VPC 之间形成网络隔离的前提下，实现源 VPC 与目标 VPC 之间的通信，从而使得源 VPC 和目标 VPC 之间的网络不会相互暴露，提高跨 VPC 网络通信的安全性和可靠性。

[53]在介绍了本说明书所提供的虚拟私有云 VPC 之间的互通方法的基本实现流程之后，下面对本说明书的各个可选实现方式进行详细介绍。

[54]在一些实施例中，源 VPC 与中继 VPC 之间可以通过私有连接相连，中继 VPC 与目标 VPC 之间可以通过私有连接相连。则源 VPC 可以通过私有连接向中继 VPC 发送访问流量，中继 VPC 可以通过私有连接将源 VPC 发送的访问流量发送到目标 VPC，目标 VPC 可以通过私有连接接收中继 VPC 发送的访问流量。

[55]其中，私有连接可以为 VPC Peering。VPC Peering 可以用于实现两个 VPC 之间的网络连接，通过此连接，可以使用私有的 IPv4 地址或 IPv6 地址在两个 VPC 之间路由流量，以便这两个 VPC 中的实例可以彼此通信，就像它们在同一个网络中一样。

[56]通过使用 VPC Peering 实现源 VPC 与中继 VPC 之间、以及中继 VPC 与目标 VPC 之间的连接，可以充分利用通过 VPC Peering 实现 VPC 之间的路由不具有传递性的特性，以实现源 VPC 和目标 VPC 之间的相互隔离。

[57]源 VPC 和中继 VPC 通过 VPC Peering 连接、中继 VPC 和目标 VPC 通过 VPC Peering 连接后，源 VPC 和中继 VPC 之间可以直接相互访问，中继 VPC 和目标 VPC 之间可以直接相互访问，但源 VPC 和目标 VPC 之间无法直接相互访问，也即是，源 VPC 中的虚拟机（Virtual Machine，VM）不能直接与目标 VPC 中的 VM 实现内部访问，以实现源 VPC 和目标 VPC 的相互隔离。

[58]可选地，中继 VPC 可以包括网络中间件，以通过该网络中间件提供流量转发的功能。

[59]在一些实施例中，中继 VPC 在将源 VPC 发送的访问流量发送到目标 VPC 时，可以通过网络中间件，将源 VPC 发送的访问流量发送到目标 VPC。

[60]例如，源 VPC 中的 APP 可以向中继 VPC 中的网络中间件发送访问流量，中继 VPC 中的网络中间件可以将访问流量转发给目标 VPC 中的相应服务，以便目标 VPC 中的服务可以接收到访问流量。

[61]其中，网络中间件可以为代理服务器或负载均衡器。

[62]以网络中间件为代理服务器为例，源 VPC 中的 APP 可以向中继 VPC 中的代理服务器（也即是 Proxy）发送访问流量，中继 VPC 中的 Proxy 可以将访问流量转发给目标 VPC 中的相应服务，以便目标 VPC 中的服务可以接收到访问流量。

[63]以网络中间件为负载均衡器为例，源 VPC 中的 APP 可以向中继 VPC 中的负载均衡

器（也即是 LB）发送访问流量，中继 VPC 中的 LB 可以将访问流量转发给目标 VPC 中的相应服务，以便目标 VPC 中的服务可以接收到访问流量。

[64]在一些实施例中，中继 VPC 还可以对接收到的访问流量进行过滤，以保证仅有按照目标协议（如某种特定协议）封装得到的访问流量可以通过。

[65]可选地，访问流量可以为按照目标协议封装得到的网络流量，目标协议可以用于指示访问流量的数据传输格式。以用于提供数据库服务的公共云环境中的 VPC 互通实现系统为例，目标协议可以为 MySQL 访问协议，或者，目标协议可以为 Oracle 访问协议，但不限于此，本说明书对目标协议的具体类型不加以限定。

[66]在一些实施例中，中继 VPC 可以将访问流量转发到目标 VPC 的目标端口（如特定协议端口），以便目标 VPC 可以通过目标端口接收中继 VPC 发送的访问流量。其中，目标端口可以为专门用于接收访问流量的网络端口。

[67]通过本说明书所提供的方案，可以通过中继 VPC 实现源 VPC 和中继 VPC 之间的相互访问、以及中继 VPC 和目标 VPC 之间的相互访问，但源 VPC 和目标 VPC 之间不能直接互通，以形成源 VPC 和目标 VPC 的网络隔离，避免源 VPC 和目标 VPC 之间的网络相互暴露，提高网络安全性。

[68]此外，在中继 VPC 中引入网络中间件，以实现访问流量的中转桥接，在实现 VPC 连通的同时，还可以过滤访问流量，保证仅有按照特定协议封装得到的流量可以通过，并转发到目标 VPC 中的特定协议端口处，目标 VPC 仅需将特定协议端口暴露出来即可，以有效应对目标 VPC 内的虚拟机和服务过度暴露，进一步提高网络安全性。

[69]另外，通过引入中继 VPC 和网络中间件以形成一种具备安全隔离能力的网络打通方案。对于客户而言，仅需操作源 VPC 和目标 VPC 的打通即可，无需感知到中继 VPC 的存在，以在客户无感知的前提下实现源 VPC 和目标 VPC 之间的网络隔离。

[70]上述实施例阐明的系统，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[71]在一个典型的配置中，计算机包括一个或多个处理器（Central Processing Unit, CPU）、输入/输出接口、网络接口和内存。

[72]内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器（Random Access Memory, RAM）和/或非易失性内存等形式，如只读存储器（Read-Only Memory, ROM）或闪存（flash RAM）。内存是计算机可读介质的示例。

[73]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（Phase Change Random Access Memory, PRAM）、静态随机存取存储器（Static Random Access Memory, SRAM）、动态随机存取存储器（Dynamic Random Access Memory, DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（Electrically Erasable Programmable Read-Only Memory, EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（Compact Disc Read-Only Memory, CD-ROM）、数字多功能光盘（Digital Video Disc, DVD）或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体（Transitory Media），如调制的数据信号和载波。

[74]还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[75]上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[76]在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[77]应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[78]以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种虚拟私有云 VPC 之间互通的实现系统,包括源 VPC、中继 VPC 和目标 VPC;
其中,
源 VPC, 用于将访问流量发送到所述中继 VPC;
所述中继 VPC, 用于将所述源 VPC 发送的访问流量发送到所述目标 VPC;
所述目标 VPC, 用于接收所述中继 VPC 发送的访问流量。
2. 根据权利要求 1 所述的系统, 所述中继 VPC 包括网络中间件; 其中,
所述中继 VPC, 用于通过所述网络中间件, 将所述源 VPC 发送的访问流量发送到
所述目标 VPC; 所述网络中间件为代理服务器或负载均衡器。
3. 根据权利要求 1 所述的系统, 所述目标 VPC, 用于通过目标端口接收所述中继
VPC 发送的访问流量;
其中, 所述目标端口为专门用于接收访问流量的网络端口。
4. 根据权利要求 1 所述的系统, 所述访问流量为按照目标协议封装得到的网络流
量, 所述目标协议用于指示所述访问流量的数据传输格式。
5. 根据权利要求 1 所述的系统, 所述源 VPC 与所述中继 VPC 之间通过私有连接
相连, 所述中继 VPC 与所述目标 VPC 之间通过私有连接相连。
6. 一种虚拟私有云 VPC 之间的互通方法, 包括:
源 VPC 向中继 VPC 发送访问流量;
所述中继 VPC 将所述源 VPC 发送的访问流量发送到目标 VPC;
所述目标 VPC 接收所述中继 VPC 发送的访问流量。
7. 根据权利要求 6 所述的方法, 所述中继 VPC 包括网络中间件;
所述中继 VPC 将所述源 VPC 发送的访问流量发送到目标 VPC, 包括:
所述中继 VPC 通过所述网络中间件, 将所述源 VPC 发送的访问流量发送到所述目
标 VPC; 所述网络中间件为代理服务器或负载均衡器。
8. 根据权利要求 6 所述的方法, 所述目标 VPC 接收所述中继 VPC 发送的访问流
量, 包括:
所述目标 VPC 通过目标端口接收所述中继 VPC 发送的访问流量;
其中, 所述目标端口为专门用于接收访问流量的网络端口。
9. 根据权利要求 6 所述的方法, 所述访问流量为按照目标协议封装得到的网络流
量, 所述目标协议用于指示所述访问流量的数据传输格式。
10. 根据权利要求 6 所述的方法, 所述源 VPC 与所述中继 VPC 之间通过私有连接

相连，所述中继 VPC 与所述目标 VPC 之间通过私有连接相连；

所述方法包括：

所述源 VPC 通过私有连接向中继 VPC 发送访问流量；

所述中继 VPC 通过私有连接将所述源 VPC 发送的访问流量发送到所述目标 VPC；

所述目标 VPC 通过私有连接接收所述中继 VPC 发送的访问流量。