

有限公司 11038

(51) Int.Cl.

H04L 9/40 (2006.01)

H04L 45/00 (2006.01)

G06F 9/455 (2006.01)

PCT/US2022/034753 2022.06.23

W02023/075869 EN 2023.05.04

地址 美国

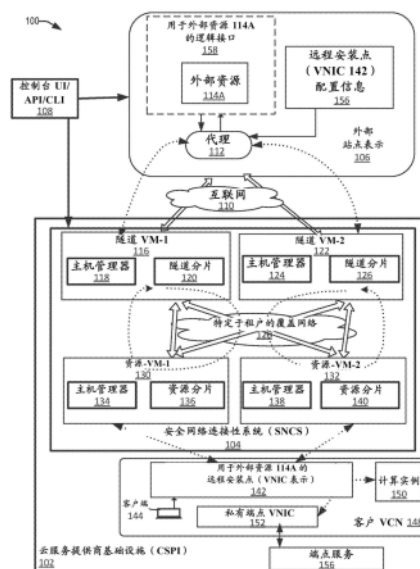
A · Y · 卡克 D · P · 沙阿 裴冠宏

C·M·马古克 P·I·凯恩卡尔

权利要求书4页 说明书45页 附图15页

私有网络之间的安全双向网络连接性系统

描述了云服务提供商基础设施 (CSPI) 内的安全私有网络连接性系统 (SNCS), 该系统在驻留在客户的本地部署环境中的外部资源与驻留在云中的客户的资源之间提供安全私有网络连接性。SNCS在驻留在客户的外部站点表示中的外部资源与驻留在云中的客户的VCN中的资源和服务之间提供安全私有双向网络连接性, 而无需企业的用户 (例如, 管理员) 必须显式配置外部资源、通告路由或设置站点到站点网络连接性。SNCS提供高性能、可伸缩且高度可用的站点到站点网络连接, 用于通过实现被用于提供安全的站点到站点网络连接性的网络元素和计算节点的稳健基础设施来处理客户的本地部署环境与CSPI之间的网络业务。



1. 一种方法, 包括:

由在云服务提供商中实现的安全网络连接性系统提供安全网络连接性服务, 用于在与云服务提供商的客户相关联的本地部署网络与由云服务提供商为客户托管的虚拟云网络 (VCN) 之间启用安全私有网络连接性, 该安全网络连接性系统包括虚拟覆盖网络, 该虚拟覆盖网络包括一个或多个计算节点的集合;

由安全网络连接性系统将驻留在本地部署网络中的外部资源注册为虚拟云网络中的外部端点, 该外部端点由虚拟云网络中的互联网协议 (IP) 地址识别;

由安全网络连接性系统中的一个或多个计算节点的集合中的第一计算节点为虚拟云网络中的外部端点创建外部资源表示, 创建外部资源表示包括:

由第一计算节点创建虚拟网络接口卡 (VNIC); 以及

由第一计算节点将与外部端点相关联的互联网协议 (IP) 地址指派给虚拟网络接口卡 (VNIC);

由第一计算节点将与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息传输到在与客户相关联的本地部署网络中配置的代理;

由安全网络连接性系统中的一个或多个计算节点的集合中的第二计算节点接收用于查询与驻留在与客户相关联的虚拟云网络 (VCN) 中的资源相关联的信息的请求, 该查询由驻留在本地部署网络中的外部资源传输, 并且外部资源被供应有逻辑接口;

由第二计算节点在为驻留在本地部署网络中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡 (VNIC) 之间建立连接;

由第二计算节点经由所建立的连接向驻留在虚拟云网络中的资源传输请求; 以及

由第二计算节点经由所建立的连接获得与所述请求对应的结果。

2. 如权利要求1所述的方法, 其中本地部署网络中的代理被配置为在驻留在本地部署网络中的外部资源与包括安全网络连接性系统的一个或多个计算节点的集合之间建立安全虚拟私有网络 (VPN) 连接。

3. 如权利要求1或2所述的方法, 其中代理被配置为至少部分地基于与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息来为驻留在本地部署网络中的外部资源供应逻辑接口。

4. 如权利要求3所述的方法, 其中为外部资源供应逻辑接口包括由代理将用于外部资源表示的虚拟网络接口卡 (VNIC) 的虚拟互联网协议 (IP) 地址指派给逻辑接口。

5. 如权利要求3或权利要求4所述的方法, 其中与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息包括虚拟网络接口卡 (VNIC) 的虚拟互联网协议 (IP) 地址、与和虚拟网络接口卡 (VNIC) 相关联的计算实例相关联的完全限定域名以及与客户相关联的虚拟云网络的云标识符。

6. 如权利要求1至5中的任一项所述的方法, 其中由第二计算节点在为驻留在本地部署网络中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡之间建立连接包括经由驻留在本地部署网络中的代理建立连接。

7. 如权利要求1-6中的任一项所述的方法, 其中由第二计算节点经由所建立的连接向驻留在虚拟云网络中的资源传输请求包括:

由第二计算节点将与外部资源相关联的物理IP地址转换成与用于与客户相关联的虚

拟云网络中的外部资源表示的虚拟网络接口卡相关联的虚拟IP地址;以及

由第二计算节点将请求传输到与虚拟网络接口卡相关联的虚拟IP地址。

8. 如权利要求1至7中的任一项所述的方法,还包括由安全网络连接性系统启用与客户相关联的本地部署网络的外部站点表示的创建,其中外部站点表示是本地部署网络的逻辑表示并且由外部站点标识符和客户标识符识别。

9. 如权利要求8所述的方法,其中外部资源被注册在外部站点表示中。

10. 如权利要求9所述的方法,还包括由第二计算节点在为驻留在外部站点表示中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡之间建立连接。

11. 如权利要求1至10中的任一项所述的方法,其中外部资源是驻留在本地部署网络中的数据库、应用或计算实例。

12. 一种在云服务提供商中实现的安全网络连接性系统,用于在与云服务提供商的客户相关联的本地部署网络与由云服务提供商为客户托管的虚拟云网络(VCN)之间启用安全私有网络连接性,该安全网络连接性系统包括虚拟覆盖网络,该虚拟覆盖网络包括一个或多个计算节点的集合,该计算节点的集合中的计算节点包括:

存储器;以及

一个或多个处理器,被配置为执行处理,该处理包括:

由安全网络连接性系统将驻留在本地部署网络中的外部资源注册为虚拟云网络中的外部端点,该外部端点由虚拟云网络中的互联网协议(IP)地址识别;

由安全网络连接性系统中的一个或多个计算节点的集合中的第一计算节点为虚拟云网络中的外部端点创建外部资源表示,创建外部资源表示包括:

由安全网络连接性系统中的一个或多个计算节点的集合中的第一计算节点创建虚拟网络接口卡(VNIC);以及

由安全网络连接性系统中的一个或多个计算节点的集合中的第一计算节点将与外部端点相关联的互联网协议(IP)地址指派给虚拟网络接口卡(VNIC);

由安全网络连接性系统中的第一计算节点将与用于外部资源表示的虚拟网络接口卡(VNIC)对应的配置信息传输到在与客户相关联的本地部署网络中配置的代理;

由安全网络连接性系统中的一个或多个计算节点的集合中的第二计算节点接收用于查询与驻留在与客户相关联的虚拟云网络(VCN)中的资源相关联的信息的请求,该查询由驻留在本地部署网络中的外部资源传输,并且外部资源被供应有逻辑接口;

由安全网络连接性系统中的第二计算节点在为驻留在本地部署网络中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡(VNIC)之间建立连接;

由安全网络连接性系统中的第二计算节点经由所建立的连接向驻留在虚拟云网络中的资源传输请求;以及

由安全网络连接性系统中的第二计算节点经由所建立的连接获得与所述请求对应的结果。

13. 如权利要求12所述的系统,其中本地部署网络中的代理被配置为在驻留在本地部署网络中的外部资源与包括安全网络连接性系统的一个或多个计算节点的集合之间建立

安全虚拟私有网络 (VPN) 连接。

14. 如权利要求12或13所述的系统,其中代理被配置为至少部分地基于与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息来为驻留在本地部署网络中的外部资源供应逻辑接口。

15. 如权利要求14所述的系统,其中为外部资源供应逻辑接口包括由代理将用于外部资源表示的虚拟网络接口卡 (VNIC) 的虚拟互联网协议 (IP) 地址指派给逻辑接口。

16. 如权利要求12至15中的任一项所述的系统,其中与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息包括虚拟网络接口卡 (VNIC) 的虚拟互联网协议 (IP) 地址、与和虚拟网络接口卡 (VNIC) 相关联的计算实例相关联的完全限定域名以及与客户相关联的虚拟云网络的云标识符。

17. 一种具有存储在其上的程序代码的非暂态计算机可读介质,该程序代码可由一个或多个处理设备执行以执行包括以下的操作:

将驻留在本地部署网络中的外部资源注册为虚拟云网络中的外部端点,该外部端点由虚拟云网络中的互联网协议 (IP) 地址识别;

为虚拟云网络中的外部端点创建外部资源表示,创建外部资源表示包括:

创建虚拟网络接口卡 (VNIC); 以及

将与外部端点相关联的互联网协议 (IP) 地址指派给虚拟网络接口卡 (VNIC);

将与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息传输到在与客户相关联的本地部署网络中配置的代理;

接收用于查询与驻留在与客户相关联的虚拟云网络 (VCN) 中的资源相关联的信息的请求,该查询由驻留在本地部署网络中的外部资源传输,并且外部资源被供应有逻辑接口;

在为驻留在本地部署网络中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡 (VNIC) 之间建立连接;

经由所建立的连接向驻留在虚拟云网络中的资源传输请求; 以及

经由所建立的连接获得与所述请求对应的结果。

18. 如权利要求17所述的非暂态计算机可读介质,其中代理被配置为至少部分地基于与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息来为驻留在本地部署网络中的外部资源供应逻辑接口。

19. 如权利要求18所述的非暂态计算机可读介质,其中为外部资源供应逻辑接口包括由代理将用于外部资源表示的虚拟网络接口卡 (VNIC) 的虚拟互联网协议 (IP) 地址指派给逻辑接口。

20. 如权利要求17至19中的任一项所述的非暂态计算机可读介质,其中与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息包括虚拟网络接口卡 (VNIC) 的虚拟互联网协议 (IP) 地址、与和虚拟网络接口卡 (VNIC) 相关联的计算实例相关联的完全限定域名以及与客户相关联的虚拟云网络的云标识符。

21. 一种计算机程序产品,包括计算机程序指令,该计算机程序指令在由处理器执行时使处理器:

将驻留在本地部署网络中的外部资源注册为虚拟云网络 (VCN) 中的外部端点,该外部端点由虚拟云网络 (VCN) 中的互联网协议 (IP) 地址识别;

为虚拟云网络 (VCN) 中的外部端点创建外部资源表示,创建外部资源表示的操作包括:
创建虚拟网络接口卡 (VNIC);以及
将与外部端点相关联的互联网协议 (IP) 地址指派给虚拟网络接口卡 (VNIC);
将与用于外部资源表示的虚拟网络接口卡 (VNIC) 对应的配置信息传输到在与客户相关联的本地部署网络中配置的代理;
接收用于查询与驻留在与客户相关联的虚拟云网络 (VCN) 中的资源相关联的信息的请求,该查询由驻留在本地部署网络中的外部资源传输,并且外部资源被供应有逻辑接口;
在为驻留在本地部署网络中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡 (VNIC) 之间建立连接;
经由所建立的连接向驻留在虚拟云网络 (VCN) 中的资源传输请求;以及
经由所建立的连接获得与所述请求对应的结果。

私有网络之间的安全双向网络连接性系统

[0001] 相关申请的交叉引用

[0002] 本申请是于2021年10月29日提交的、标题为“Secure Bi-Directional Network Connectivity System between Private Networks”的美国非临时申请17/515,093的PCT申请,并根据35U.S.C.119(e)要求其权益和优先权,其内容出于所有目的通过引用全文并入本文。

[0003] 本申请涉及于2021年10月29日提交的标题为“Transparent mounting of external endpoints between private networks”的序列号为17/515,087的申请,该申请的全部内容出于所有目的通过引用并入本文。

技术领域

[0004] 本公开一般而言涉及基于云的服务。更具体而言,但非限制性地,本公开描述了云基础设施内的安全私有网络连接性服务,该服务包括在驻留在客户的本地部署(on-premise)环境中的外部资源与驻留在云中的客户的资源之间建立安全私有双向网络连接性的改进的能力。

背景技术

[0005] 对基于云的服务的需求持续快速增长。术语“云服务”一般指使用云服务提供商提供的系统和基础设施(云基础设施)按需(例如,通过订阅模式)向用户或客户提供的服务。通常,构成云服务提供商的基础设施的服务器和系统与客户自己的本地部署服务器和系统是分开的。因此,客户可以自己利用由云服务提供商提供的云服务,而无需为服务购买单独的硬件和软件资源。云服务有多种不同类型,包括软件即服务(SaaS)、平台即服务(PaaS)、基础设施即服务(IaaS)等。

[0006] 为了利用由云服务提供的众多优势,企业常常需要将本地部署应用和数据从其本地数据中心迁移到公共云基础设施。这个过程通常要求企业建立站点到站点的网络连接,以在其本地部署数据中心与云基础设施之间建立安全连接性。对于企业来说,配置高性能、可伸缩且高度可用的站点到站点网络连接来处理不同网络之间的网络业务可以是复杂且耗时的任务,尤其是当企业的本地部署应用和数据跨多个不同网络伸缩时。

发明内容

[0007] 本公开一般而言涉及基于云的服务。更具体而言,但非限制性地,本公开描述了云基础设施内的安全私有网络连接性服务,该服务包括在驻留在客户的本地部署环境中的外部资源与驻留在云中的客户的资源之间建立安全私有双向网络连接性的改进的能力。

[0008] 在某些实施例中,公开了一种安全网络连接性系统。安全网络连接性服务启用与云服务提供商的客户相关联的本地部署网络与由云服务提供商为客户托管的虚拟云网络(VCN)之间的安全私有网络连接性。该安全网络连接性系统包括虚拟覆盖网络,该虚拟覆盖网络包括一个或多个计算节点的集合。系统将驻留在本地部署网络中的外部资源注册为虚

拟云网络中的外部端点。外部端点由虚拟云网络中的互联网协议 (IP) 地址识别。系统中的计算节点的集合中的第一计算节点为虚拟云网络中的外部端点创建外部资源表示。外部资源表示是通过创建虚拟网络接口卡 (VNIC) 并将与外部端点相关联的互联网协议 (IP) 地址指派给 VNIC 来创建的。然后, 第一计算节点将与用于外部资源表示的 VNIC 对应的配置信息传输到在与客户相关联的本地部署网络中配置的代理。

[0009] 在某些示例中, 系统中的计算节点的集合中的第二计算节点接收用于查询与驻留在与客户相关联的 VCN 中的资源相关联的信息的请求。该查询由驻留在本地部署网络中的外部资源传输。在某些实施方式中, 外部资源被供应有逻辑接口。第二计算节点在为驻留在本地部署网络中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的 VNIC 之间建立连接。第二计算节点经由所建立的连接向驻留在虚拟云网络中的资源传输请求并经由所建立的连接获得与该请求对应的结果。

[0010] 在某些实施例中, 本地部署网络中的代理被配置为在驻留在本地部署网络中的外部资源与包括安全网络连接性系统的一个或多个计算节点的集合之间建立安全虚拟私有网络 (VPN) 连接。在某些示例中, 代理被配置为至少部分地基于与用于外部资源表示的 VNIC 对应的配置信息来为驻留在本地部署网络中的外部资源供应逻辑接口。在某些示例中, 为外部资源供应逻辑接口包括由代理将用于外部资源表示的虚拟网络接口卡 (VNIC) 的虚拟互联网协议 (IP) 地址指派给逻辑接口。

[0011] 在某些示例中, 与用于外部资源表示的 VNIC 对应的配置信息包括 VNIC 的虚拟互联网协议 (IP) 地址、与和 VNIC 相关联的计算实例相关联的完全限定域名以及与客户相关联的虚拟云网络的云标识符。

[0012] 在某些示例中, 第二计算节点经由驻留在本地部署网络中的代理在为驻留在本地部署网络中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡之间建立连接。

[0013] 在某些示例中, 第二计算节点经由所建立的连接将请求传输到驻留在虚拟云网络中的资源。这个处理涉及由第二计算节点将与外部资源相关联的物理 IP 地址转换成与用于与客户相关联的虚拟云网络中的外部资源表示的 VNIC 相关联的虚拟 IP 地址, 并将请求传输到与 VNIC 相关联的虚拟 IP 地址。

[0014] 在某些示例中, 安全网络连接性系统使得能够创建与客户相关联的本地部署网络的外部站点表示。外部站点表示是本地部署网络的逻辑表示并由外部站点标识符和客户标识符识别。在某些示例中, 外部资源被注册在外部站点表示中。

[0015] 在某些示例中, 安全网络连接性系统中的第二计算节点在为驻留在外部站点表示中的外部资源供应的逻辑接口与为虚拟云网络中的外部资源表示创建的虚拟网络接口卡之间建立连接。在某些示例中, 外部资源是驻留在本地部署网络中的数据库、应用或计算实例。

[0016] 本文描述了各种实施例, 包括方法、系统、存储可由一个或多个处理器执行的程序、代码或指令的非暂态计算机可读存储介质等。提及这些说明性实施例并不是为了限制或定义本公开, 而是为了提供示例以帮助理解本公开。在具体实施方式中讨论附加实施例, 并且在那里提供进一步的描述。

附图说明

[0017] 图1描绘了根据某些实施例的包括云服务提供商基础设施 (CSPI) 内的安全私有网络连接性服务的分布式环境100。

[0018] 图2描绘了根据某些实施例的由图1中所示的系统 and 子系统执行的用于在驻留在客户的本地部署网络中的客户的外部资源与驻留在客户的VCN中的资源和服务之间提供安全私有网络连接性的操作的附加细节。

[0019] 图3描绘了根据某些实施例的由图1中所示的系统 and 子系统执行的用于提供安全私有网络连接性的处理的示例。

[0020] 图4是描绘根据某些实施例的驻留在客户的本地部署网络中的外部资源与客户的虚拟云网络中的外部资源的表示之间的网络分组流的流程图。

[0021] 图5是描绘根据某些实施例的在客户的虚拟云网络中的外部资源表示与驻留在客户的本地部署网络中的外部资源之间的网络分组流的流程图。

[0022] 图6是分布式环境的高级别图,示出了根据某些实施例的由云服务提供商基础设施托管的虚拟或覆盖云网络。

[0023] 图7描绘了根据某些实施例的CSPI内的物理网络中的物理组件的简化体系架构图。

[0024] 图8示出了根据某些实施例的CSPI内的示例布置,其中主机机器连接到多个网络虚拟化设备 (NVD)。

[0025] 图9描绘了根据某些实施例的主机机器和NVD之间的连接性,用于提供I/O虚拟化以支持多租赁。

[0026] 图10描绘了根据某些实施例的由CSPI提供的物理网络的简化框图。

[0027] 图11是图示根据至少一个实施例的用于实现云基础设施即服务系统的一种模式的框图。

[0028] 图12是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0029] 图13是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0030] 图14是图示根据至少一个实施例的用于实现云基础设施即服务系统的另一种模式的框图。

[0031] 图15是图示根据至少一个实施例的示例计算机系统的框图。

具体实施方式

[0032] 在以下描述中,出于解释的目的,阐述了具体细节以便提供对某些实施例的透彻理解。但是,显然可以在没有这些具体细节的情况下实践各种实施例。附图和描述并非旨在限制。词语“示例性”在本文用于表示“用作示例、实例或图示”。本文描述为“示例性”的任何实施例或设计不一定被解释为优选或优于其它实施例或设计。

[0033] 本公开一般而言涉及基于云的服务。更具体而言,但非限制性地,本公开描述了云基础设施内的安全私有网络连接性服务,其包括在驻留在客户的本地部署环境中的外部资源与驻留在云中的客户的资源之间建立安全私有双向网络连接性的改进的能力。

[0034] 云基础设施可以在灵活的覆盖虚拟网络中提供高性能计算、存储和网络能力,该覆盖虚拟网络在物理底层网络之上运行并且可以从企业的本地部署网络安全地访问。云基础设施允许企业以管理本地部署工作负载的方式管理其基于云的工作负载。因此,企业可以通过与其本地部署网络相同的控制、隔离、安全性和可预测的性能来获得云的所有益处。企业可以使用由云提供的计算、存储器和联网资源构建他们自己的网络。例如,客户可以使用由云提供的资源来构建一个或多个可定制的且私有的网络,称为虚拟云网络 (VCN)。客户可以在这些客户VCN上部署一个或多个客户资源,诸如计算实例。计算实例可以采用虚拟机、裸机实例等形式。因此,云提供了基础设施和互补云服务的集合,使得企业(客户)能够在高度可用的被托管环境中构建和运行各种应用和服务。

[0035] 为了利用由云基础设施提供的众多优势,许多企业执行将本地部署应用和数据从其本地数据中心到公共云基础设施的迁移。将工作负载从企业的本地(即,本地部署)数据中心迁移到云可以是复杂且具有挑战性的过程。云迁移期间遇到的常见挑战涉及由企业识别要执行的迁移的类型、需要被移动的资源以及资源之间的数据依赖性。在迁移工作负载时,一些资源(例如,数据库、应用等)可能需要在本地部署数据中心驻留特定时间段,直到它们能够被成功地迁移到云中为止。某些资源(例如,业务关键资源、具有数据可移植性限制的资源或具有严格地理要求的资源)可以被识别为由于安全原因未迁移到云并保留在本地部署数据中心的资源。为了使企业能够从其(在云中的)VCN安全地访问本地部署资源并且使得驻留在其本地部署数据中心中的资源能够安全地访问驻留在云中的资源,需要在客户的(企业的)本地部署数据中心与客户的VCN之间建立安全私有网络连接性。对于企业来说,设置安全的站点到站点网络连接可以是复杂且耗时的任务。这通常要求网络策略级别的管理,由企业的用户(例如,管理员)设置站点到站点的网络(例如,VPN)连接、设置多个配置参数、设置用于站点到站点网络连接性的VPN组件(例如,客户网关设备、目标网关设备)等。

[0036] 此外,为了使用站点到站点网络连接从其VCN访问驻留在其本地部署数据中心中的远程资产(例如,诸如数据库或应用之类的本地部署资源)或者为了使驻留在其本地部署数据中心中的远程资产能够安全地访问客户的VCN中的资源和服务,企业的用户必须执行附加任务,如手动配置网关设备以执行路由通告和网络地址转换,以便可以实现客户的外部环境中的远程资产与客户的VCN中的资源之间的安全连接性。用户还必须手动配置远程资产,以便业务(例如,网络分组)从客户的VCN到达远程资产并且反之亦然,配置路由表以包括站点到站点VPN连接所使用的路由,启用路由表的路由传播以自动传播站点到站点VPN路由、更新安全性规则等。

[0037] 在某些实施例中,描述了云服务提供商基础设施(CSPI)内的安全私有网络连接性服务,该服务包括在驻留在客户的本地部署环境中的外部资源与驻留在云中的客户的资源之间建立安全私有双向网络连接性的改进能力。安全私有网络连接性服务是使用云服务提供商基础设施(CSPI)内的安全网络连接性系统(SNCS)实现的。本公开中描述的SNCS提供了相对于常规基于云的网络连接性服务的若干技术进步和/或改进。使用所公开的由SNCS实现的新的和改进的体系架构,可以实现驻留在客户的外部站点表示中的外部资源与驻留在云中的客户的VCN中的资源和服务之间的安全私有双向网络连接性,而无需企业的用户(例如,管理员)必须显式配置外部资源、通告路由或设置站点到站点网络连接性。SNCS提供高

性能、可伸缩且高度可用的站点到站点网络连接,用于通过实现用于提供安全的站点到站点网络连接性的网络元素和计算节点的稳健基础设施来处理客户的本地部署环境与CSPI之间的网络业务。通过使用由SNCS实现的网络元素和计算节点的稳健基础设施,企业的用户可以安全地从云访问其外部资源,就好像他们连接到其VCN内的任何其它本机资源一样。此外,SNCS使驻留在客户的本地部署网络中的一个或多个外部资源能够安全地到达和访问驻留在客户的VCN(即,云)中的资源和服务。可以实现客户的外部站点表示中的外部资源与驻留在云中客户的VCN中的资源和服务之间的安全私有双向网络连接性,而无需企业的用户(例如,管理员)必须显式配置外部资源、通告路由或设置站点到站点网络连接性。

[0038] 现在参考附图,图1描绘了根据某些实施例的包括云服务提供商基础设施(CSPI)内的安全私有网络连接性服务的分布式环境100。分布式环境100包括经由一个或多个通信网络彼此通信耦合的多个系统。这些通信网络可以包括公共和私有网络。图1中描绘的分布式环境100仅仅是示例并且不旨在不适当地限制所要求保护的实施例的范围。许多变化、替代和修改都是可能的。例如,在一些实施方式中,图1中描绘的分布式环境可以具有比图1中所示的系统或组件更多或更少的系统或组件,可以组合两个或更多个系统,或者可以具有不同的系统配置或布置。

[0039] 如图1中描绘的示例中所示,分布式环境100包括提供客户可以订阅的服务和资源的CSPI 102。在某些实施例中,CSPI 102提供安全私有网络连接性服务,该服务包括在客户的本地部署网络与由CSPI 102托管的客户的VCN之间提供安全双向私有网络连接性的能力。在图1中所示的示例中,安全私有网络连接性服务可以由CSPI 102内的安全网络连接性系统(SNCS) 104实现。由SNCS104提供的安全私有网络连接性服务使得驻留在客户的本地部署网络中的一个或多个资源(本文中也称为外部资源或远程资产)能够安全地访问驻留在客户的VCN中的资源和服务。由SNCS104提供的安全私有网络连接性服务附加地使得客户的VCN中的资源和服务能够安全地访问驻留在客户的本地部署网络中的外部资源。客户可以从其VCN内部访问外部资源,就好像他们连接到驻留在客户的VCN中的任何其它本机资源一样。可以启用本地部署的外部资源与驻留在客户的VCN(即,云)中的资源之间的安全访问,而无需客户(例如,企业的用户)设置其本地部署网络与云之间的精心设计的站点到站点网络连接、无需客户必须对其外部资源进行任何改变或者无需客户必须配置要由站点到站点连接所使用的路由。下面详细描述由SNCS104执行的在驻留在客户的本地部署网络中的外部资源与云中客户的资源和服务之间启用安全双向连接性的处理的附加细节。

[0040] 在某些方法中,驻留在客户的本地部署网络中的外部资源与云(例如,客户的VCN)中客户的资源和服务之间的安全双向连接性由SNCS104使用多级(multi-stage)处理来实现。在第一级,与客户相关联的用户(例如,管理员)可以创建客户的本地部署网络的“外部站点表示”106。例如,用户可以经由由用户设备执行的应用的控制台用户接口(UI) 108、经由API或经由由用户的设备执行的命令行界面(CLI)与SNCS104交互以创建外部站点表示106。外部站点表示(例如,106)可以表示客户的外部站点(例如,本地部署网络/本地部署数据中心)的逻辑或虚拟表示,并且可以由外部站点标识符和租户(客户)标识符来识别。举例来说,外部站点表示106可以表示高级别容器资源,该高级别容器资源在逻辑上表示客户的本地部署网络的一部分以及驻留在本地部署网络中的一个或多个外部资源的子集。

[0041] 在第二级,用户下载代理112并在外部站点表示106中安装/配置代理112。在某些

实施例中,代理112可以是当用户订阅由SNCS104提供的安全私有连接性服务时由用户下载作为由SNCS 104提供的下载包的一部分的软件应用。代理112可以由用户经由控制台UI 108在外部站点表示106中安装和配置。

[0042] 在第三级,在外部站点表示106中成功安装代理112后,SNCS104认证代理112并为客户编排特定于租户的覆盖网络128的设置。特定于租户的覆盖网络128可以表示由SNCS104为订阅由该SNCS提供的服务的每个租户(客户)构建在物理网络之上的虚拟覆盖网络。特定于租户的覆盖网络128被用于在CSPI中的客户的VCN 148与客户的外部站点表示106之间建立安全私有网络连接性。如图1中所描绘的实施例中所示,特定于租户的覆盖网络128可以包括分布式且水平可伸缩的计算节点群(fleet),其包括一个或多个隧道主机(本文中也称为隧道虚拟机)的集合、隧道VM-1 116和隧道VM-2 122、以及一个或多个资源主机(本文中也称为资源虚拟机)的集合、资源VM-1 130和资源VM-2 132。主机(例如,隧道主机或资源主机)可以由在特定于租户的覆盖网络128中彼此互连的容器(本文中也称为分片(shard))的集合组成。隧道VM 116和122被用于运行每租户隧道分片。例如,如图1中所示,隧道VM-1 116被用于运行隧道分片120,并且隧道VM-2 122被用于运行针对CSPI的特定租户/客户的隧道分片126。每个隧道分片120或126负责提供到客户的外部站点表示106的安全连接性。资源VM 130和132的集合可以被用于运行每租户资源分片。例如,如图1中所示,资源VM-1 130被用于运行资源分片136并且资源VM-2 132被用于运行针对租户/客户的资源分片140。资源分片可以被用于接收来自客户的VCN的业务并将其转发到客户的外部站点表示。由图1中所示的隧道分片和资源分片执行的用于在客户的外部站点表示106与客户的VCN 148之间提供安全连接性的操作的附加细节在图1中详细描述。

[0043] 每个隧道VM(116、122)和资源VM(130、132)还分别配置有主机管理器(118、134)。主机管理器(118、134)表示在隧道VM和资源VM上执行的处理。主机管理器(118或134)可以实现用于创建隧道和资源分片的API。在某些实施方式中,主机管理器(118、134)可以是无状态的并且通过从用户(经由API108)接收关于要创建的分片的类型(隧道或资源分片)和分片的具体配置的指令来以命令模式(即,作为主机管理器执行的命令的序列)进行操作。主机管理器还可以负责收集和监视隧道分片和资源分片的状态。

[0044] 在SNCS104如上所述为客户设置特定于租户的覆盖网络128之后,在第四级,用户在外部站点表示106中注册本地部署资产(例如,外部资源114A)作为其VCN中的外部端点。外部资源114A可以表示驻留在客户的本地部署网络中的客户打算与驻留在客户的VCN中的资源和服务建立安全双向连接性的本地部署资源或资产(诸如数据库、计算实例、应用等)。为了注册外部资源114A,用户(经由控制台UI 108)识别要从其VCN 148启用安全私有网络连接性的外部资源(例如,114A),并使用控制台UI 108(或经由API)注册外部资源作为其VCN中的外部端点。作为注册外部资源的一部分,用户经由SNCS所提供的控制台UI或API来提供与外部资源相关的配置信息,诸如与外部资源相关联的本地部署物理IP地址、可访问外部资源的端口号以及外部资源的主机名(或完全限定域名(FQDN))。用户还可以在客户的VCN中选择在其中创建用于外部资源的外部端点的子网。SNCS接收配置信息,并且在客户的VCN中为外部资源创建外部端点。外部端点由客户的VCN中的IP地址、端口号和FQDN(主机名)识别。

[0045] 在第五级,SNCS104(经由控制平面API)然后为客户的VCN中的外部端点创建外部

资源表示。在特定实施方式中,外部资源表示的创建包括创建远程安装点VNIC并将与外部端点相关联的IP地址分配给VNIC。然后,SNCS(经由控制平面API)在资源VM上创建资源分片,这些资源VM能够在逻辑上将VNIC(经由工作者接口)附接到资源分片。

[0046] 在第六级,代理112下载并读取与为客户的VCN 148中的外部资源表示114A创建的VNIC 142相关联的配置信息156,并将配置信息156复制到注册的外部资源114A上。配置信息可以包括例如VNIC的虚拟IP地址、与和VNIC相关联的计算实例相关联的完全限定域名以及与客户相关联的虚拟云网络的云标识符。使用配置信息156,代理112创建/供应用于外部资源114A的逻辑接口158。逻辑接口158可以表示由IP地址组成的软件实体。在某些实施方式中,由代理112创建或供应逻辑接口158包括由代理将指派给为外部资源表示创建的VNIC 142的虚拟IP地址指派给逻辑接口158。

[0047] 由于外部资源114A被供应有逻辑接口158,该逻辑接口158被指派有与驻留在客户的VCN中的用于外部资源表示的VNIC 142对应的虚拟IP地址,因此外部资源现在变成客户的VCN的一部分,并且通过使用由SNCS104提供的安全私有网络连接性服务,能够安全地访问云中(例如,客户的VCN 148中)的资源和服务。例如,外部资源114A经由其逻辑接口158可以通过经由代理112建立到SNCS104中的隧道主机的连接而安全地到达/访问客户的VCN 148中的计算实例150或客户的VCN中的服务152(例如,流传输服务或对象存储服务)。类似地,客户的VCN 148中的客户端应用可以使用由SNCS104提供的服务以使用外部资源的VNIC表示142来安全地访问客户的本地部署网络中的外部资源114A,就好像他们连接到客户的VCN 148中的任何其它本机资源一样。以这种方式,由SNCS104实现驻留在客户的本地部署网络中的外部资源与云(例如,客户的VCN)中客户的资源和服务之间的安全双向连接性。

[0048] 图2描绘了根据某些实施例的由图1中所示的系统 and 子系统执行的用于在驻留在客户的本地部署网络中的客户的外部资源与驻留在客户的VCN中的资源和服务之间提供安全私有网络连接性的操作的附加细节。图2中描绘的系统 and 子系统可以使用由计算系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)、硬件或其组合来实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。图2中描绘的分布式环境200仅仅是示例并且不旨在不适当地限制所要求保护的实施例的范围。许多变化、替代和修改都是可能的。例如,在一些实施方式中,图2中描绘的分布式环境可以具有比图2中所示的系统或组件更多或更少的系统或组件,可以组合两个或更多个系统,或者可以具有不同的系统配置或布置。作为发明人,我们主要基于发明1(IaaS272.1)中描述的系统体系架构(SNCS)描述了图2中的系统。请查看下面关于图2的描述并根据需要添加/编辑它以使其更加清晰。

[0049] 如先前在图1中所描述的,作为由SNCS104实现的在客户的本地部署网络与由CSPI 102托管的客户的VCN之间提供安全的私有网络连接性的连接处理的一部分,与客户相关联的用户(例如,管理员)创建客户的本地部署网络的“外部站点表示”(例如,106),在外部站点表示中配置代理(例如,112),在外部站点表示中注册本地部署资产并且在客户的VCN中为注册的外部资源创建远程安装点(本文中也称为端点)。在外部站点表示中成功安装代理(例如,112)后,代理112经由公共网络(例如,互联网110)建立到SNCS104的虚拟私有网络(VPN)连接(在本文中也称为VPN隧道)。VPN连接是客户的外部站点表示106与客户的VCN 148之间的加密连接。在某个实施方式中,VPN连接利用安全隧穿协议(例如,层2隧穿协议

(L2TP)) 协议) 以经由互联网110建立到SNCS104的安全私有网络连接性。当代理112被安装在外部站点表示106中时,它开始引导处理以通过将诸如配置文件中与代理112相关联的隔间标识符及外部站点表示标识符之类的信息传递给SNCS104来激活其自身。当代理112引导其自身时,它与SNCS的开始注册和激活处理的控制平面进行通信。在激活处理期间,控制平面发回网关器件建立与VPN服务器的安全隧道连接所需的所有信息(例如,证书、公共IP等)。然后,代理112通过执行VPN客户端程序来建立到SNCS104的安全VPN连接性,该VPN客户端程序打开到安装在SNCS处的VPN服务器的安全VPN隧道连接。安全隧道终止于隧道分片(例如,120),该隧道分片位于SNCS104中的隧道VM(例如,116)上。

[0050] 在图1中所描绘的具体实施方式中,代理112被配置有两个VPN客户端:VPN客户端-1 206和VPN客户端-2 208,它们各自被配置为建立终止于两个不同VPN服务器(分别在隧道分片(隧道分片-1 120和隧道分片-2 126)上执行的VPN服务器-1 224和VPN服务器-2 226)上的隧道。在图2中所描绘的实施方式中,代理112的每次物理安装都导致两个隧道的建立,因此如果一个隧道宕机,那么业务(即,网络分组)可以自动地跨第二个隧道进行路由。虽然图2中所示的具体实施方式描绘了两个隧道,但在其它实施方式中,SNCS104可以被配置为对于代理112的每次物理安装实现多于两个的冗余隧道,或者可以在安装代理112时仅实现单个隧道。

[0051] 在某些实施例中,代理112使用诸如边界网关协议(BGP)之类的标准外部网关协议来建立与隧道分片120和126的BGP对等会话。使用BGP,代理112经由在代理112内实现的公共接口220与隧道分片交换路由和可达性信息。作为BGP对等会话所需的配置信息的一部分,代理112将其本地部署IP地址注入其本地路由表212(本文中也称为路由信息库(RIB)),该本地路由表212由隧道分片接收。在应用适当的路由过滤策略之后,隧道分片将路由信息导入其本地路由表(228和236)中。路由过滤是优选的以确保受损的代理112不将任意路由注入隧道分片。在某些示例中,代理112附加地包括路由管理器214。可以使用作为路由套件(例如,Quagga)的一部分的开源路由管理器(例如,Zebra)来实现路由管理器214。当BGP对等会话学习路由并将它们导入其路由表212中时,BGP对等会话执行最佳路径计算并使用路由管理器214将最佳路由添加到本地内核。

[0052] 隧道分片(例如,120、126)可以由一个或多个容器的集合组成。在某些实施方式中,隧道分片(120或126)可以包括外壳容器,该外壳容器可以被用于设置使得隧道分片能够与代理112和作为特定于租户的覆盖网络128的一部分的其它分片(例如,资源分片136和140)两者进行通信的各种网络接口。在图2中所描绘的实施例中,在隧道分片中的外壳容器内实现的网络接口可以包括外部站点接口(esi)、隧道接口和分片后端接口。例如,在隧道分片-1 120中实现的网络接口包括隧道接口216、外部站点接口222和分片后端接口234。类似地,在隧道分片-2 126中实现的网络接口包括隧道接口218、外部站点接口223和分片后端接口235。隧道分片(例如,120或126)附加地包括VPN服务器(224、226),VPN服务器(224、226)被用于建立到在外部网关器具(appliance)112中执行的VPN客户端(206、208)的VPN隧道。外部站点接口(222、223)可以由VPN客户端在其上运行的代理112已知的公共IP来识别,并且被用于建立到隧道分片的隧道。当VPN客户端(例如,206、208)连接到VPN服务器(224、226)时,创建隧道接口(216、218)并将其放置在隧道分片的预配置的VPN子网中。

[0053] 在某些实施方式中,每个隧道分片(例如,120、126)可以利用边界网关协议(BGP)

来建立外部网关器具与隧道分片之间的BGP对等会话以及隧道分片与资源分片之间的BGP对等会话。BGP对等会话被用于经由分片后端接口(234、235)与资源分片交换路由和可达性信息,以及经由外部站点接口(222、223)与外部站点表示106交换路由和可达性信息。作为BGP对等会话所需的配置信息的一部分,识别特定于租户的覆盖网络128的IP地址被添加到分别在隧道分片120、126中实现的路由表228、236(即,路由信息库(RIB))。在某些实施方式中,无类别域间路由(CIDR)技术可以被用于将IP地址分配给特定于租户的覆盖网络。路由表(228、236)列出到特定网络目的地(诸如到资源分片(136、140)和到外部站点表示106)的路由。在一些情况下,路由表(228、236)还列出与这些路由相关联的度量(距离)。当建立与资源分片的BGP对等会话时,路由表中的路由被传播到资源分片。如图2中所示,每个隧道分片(120、126)附加地包括路由管理器(228、240)。路由管理器(228或240)可以以与在外部网关器具112中实现的路由管理器(214)类似的方式来实现。当BGP学习路由并将它们导入隧道分片中的路由表时,它执行最佳路径计算并使用路由管理器将最佳路由推送到外部站点表示106和资源分片136、140。

[0054] 资源分片(136、140)可以由容器的集合组成。在某些实施方式中,资源分片(136、140)可以包括外壳容器,该外壳容器可以被用于与隧道分片(116、126)设置虚拟隧道端点VTEP(242、243)。每个资源分片(136、140)可以使用BGP来建立与隧道分片的对等会话并且经由虚拟隧道端点(242、243)与隧道分片交换路由和可达性信息。资源分片(136、140)附加地包括路由管理器(250、260),其被配置为执行与在隧道分片中实现的路由管理器(232或240)相同的功能。每个资源分片(136、140)附加地包括代理服务器(244、254)。代理服务器(244或254)可以被配置为接受来自客户的VCN 148中的客户端应用144的连接,并且发起到外部站点表示中的外部资源的新连接。

[0055] 在某些实施方式中,对于每个注册的外部端点(即,与外部站点表示中的外部资源对应),启动唯一的代理服务器容器并将其附接到资源分片。当注册外部资源并为客户的VCN中注册的外部端点创建远程安装点VNIC时,用户可以向SNCS104提供配置信息,诸如外部资源的IP地址、外部资源的端口号以及外部资源的名称。这个配置信息在代理服务器中供应并由客户的VCN中的客户端应用用来连接到外部资源。当外部资源被SNCS成功注册为客户的VCN中的外部端点时,SNCS104(经由控制平面API)创建VNIC并将与外部端点相关联的IP地址指派给VNIC。

[0056] 在图2中所描绘的示例中,注册的外部端点(即,外部站点表示中的外部资源)表示驻留在外部站点表示106中的数据库202。代理服务器(244、254)侦听指派给为注册的外部端点202创建的VNIC 206的虚拟IP地址。这确保同一VNIC IP无法用于访问外部站点表示中的其它已注册外部资源。当在客户的VCN中运行的客户端应用144接收到获得存储在外部数据库202中的信息的查询时,它将网络分组传输到客户的VCN中的VNIC IP。网络分组由附接到资源分片(136、140)的工作者VNIC(251、252)接收。工作者VNIC被配置有VNIC的虚拟IP地址,并且进而经由代理服务器(244、254)发起到外部站点表示中的注册的外部资源的连接。代理服务器(244、254)执行网络地址转换(NAT)以将指派给VNIC 206的虚拟IP地址转换成外部站点表示106中的外部资源114A的真实/物理IP地址。使用代理服务器(244、254)的资源分片(136、140)发起经由隧道分片(120、126)到代理112的连接。代理112从隧道分片(120、126)接收网络分组,并且进而将分组路由到外部站点表示106中的注册的外部资源

(即,数据库202)。代理服务器(244、254)附加地包括跨隧道分片将网络业务负载平衡到外部资源的能力。在某些实施例中,代理服务器(244、254)可以被配置为将来自多个客户端应用的连接多路复用到去往外部站点表示的单个连接上。

[0057] 以类似的方式,驻留在外部站点表示106中的注册的外部资源(即,数据库202)可以到达并安全地访问驻留在客户的VCN中的资源(例如,计算实例150)或服务(例如,私有端点VNIC 152)。如先前在图1中所描述的,代理112创建/供应用于外部资源202的逻辑接口204。通过为外部资源114A创建逻辑接口158并将数据库202的VNIC表示206的虚拟IP地址指派给逻辑接口,数据库202(其驻留在客户的本地部署网络中)能够使用由SNCS 104提供的安全私有网络连接性服务经由客户的VCN 148中的私有端点VNIC 142安全地访问客户的VCN 148中的计算实例150或服务156(例如,CSPI中的流传输服务或对象存储服务)。例如,在图2中所描绘的实施例中,代理112可以从数据库202接收请求与客户的VCN中的资源(例如,150)相关联的信息的查询。代理112然后将与查询对应的网络分组传输到隧道分片(120、126)。隧道分片进而发起到资源分片(136、140)的连接。资源分片(136、140)中的代理服务器(244、254)执行网络地址转换(NAT)以将外部站点表示106中的外部资源的真实IP地址转换成客户的VCN中的外部资源(例如,数据库202)的VNIC表示206的虚拟IP地址。附接到资源分片(136、140)的工作者VNIC(251、252)进而发起到客户的VCN中的数据库202的VNIC表示206的连接,该连接将与查询对应的网络分组传输到客户的VCN中的发出请求的资源(例如,150)。以这种方式,SNCS 104确保在驻留在客户的本地部署网络中的外部资源(例如,数据库202)与客户的VCN(即,云)中的资源(例如,150)和服务(例如,152)之间建立安全私有双向网络连接性。

[0058] 在某些实施方式中,要求来自客户的VCN 148的私有连接性的注册的外部端点可以被实现为服务VNIC,在本文中也称为客户的VCN 148中的“SVNIC”。SVNIC可以由CSPI 102使用VNIC即服务(VNICaaS)系统(图2中未示出)来实现,该VNICaaS系统可以表示由能够托管多个VNIC(例如,服务VNIC 254)以处理和传输虚拟云网络之间的业务的CSPI 102实现的水平可伸缩的服务。具体而言,VNICaaS是虚拟联网特征,其使得VNIC能够被表示为或用作服务(即,SVNIC)。VNICaaS提供VNIC的功能性,而不要求虚拟网络内的特定SmartNIC或计算实例的主机来托管VNIC。用于将注册的端点表示为SVNIC的技术已在标题为“Techniques for high performance virtual routing capability”的编号为17/175,573的美国专利申请中进行了详细描述。编号为17/175,573的美国专利申请中描述的技术仅意味着作为示例并且不旨在进行限制。在替代实施例中,还可以使用各种其它技术来表示注册的端点并处理和传输虚拟云网络之间的业务。由于为每个注册的外部端点(例如,数据库202)创建SVNIC,因此可以为每个SVNIC配置灵活数量的工作者。在具体实施方式中,每个SVNIC可以与附接到不同资源分片(例如,136、140)的两个工作者VNIC(例如,251、252)相关联。工作者VNIC被传递到资源分片并配置有SVNIC IP。

[0059] 在图2中所描绘的具体实施方式中,单个代理112安装在外部站点表示106中并且被配置为建立两个隧道,从而导致需要放置在由SNCS104实现的隧道群上的总共两个隧道分片。对于这个实施方式中描述的固定数量的隧道分片,每个资源分片可以预配置有BGP对等体的固定集合以及用于这些对等体的静态地址解析协议(ARP)条目。在某些方法中,隧道分片上的BGP容器可以配置有“动态BGP对等体”,其中可以指定IP地址的CIDR块,其中BGP可

以接受传入的连接。这个CIDR块可以被设置为特定于租户的覆盖网络的CIDR,因此随着资源分片的增长/收缩,隧道分片上的BGP对等点也适当地改变。从资源分片的角度来看,每个资源分片现在都有两个BGP对等连接,并且由于每个BGP对等体都将相同的CIDR路由传播到它从外部站点表示中学习到的本地部署网络,因此每个资源分片都具有去往本地部署网络的两条相等成本的路径。类似地,从外部网关的角度来看,代理112建立去往SNCS104的两个隧道并且隧道分片将特定于租户的覆盖网络路由通告给代理112,代理112然后将适当的路由安装到特定于租户的覆盖网络。

[0060] 使用由SNCS104实现的所公开的新的和改进的体系架构,可以实现客户的外部站点表示中的外部资源与驻留在云中的客户的VCN中的资源和服务之间的安全私有双向网络连接性,而无需企业的用户(例如,管理员)必须显式配置外部资源、通告路由或设置站点到站点网络连接性。如所描述的,安全私有双向网络连接性是由SNCS使用客户的外部站点表示与客户的VCN之间的加密连接并通过在为客户设置特定于租户的覆盖网络之前认证代理来建立的。SNCS104通过为使用由SNCS104提供的服务的每个租户/客户实现网络元素和计算节点的稳健基础设施(即,特定于租户的覆盖网络128)来提供高性能、可伸缩且高度可用的站点到站点网络连接以处理客户的本地部署环境与CSPI之间的网络业务。特定于租户的覆盖网络128中的隧道主机被用于提供到客户的外部站点表示106的安全连接性,并且资源主机被用于从客户的VCN接收业务并将其转发到客户的外部站点表示。资源主机附加地能够从外部站点表示中的外部资源接收业务并将其转发到驻留在客户的VCN中的资源或服务。通过使用由特定于租户的覆盖网络实现的网络元素和计算节点的稳健基础设施,企业可以安全地从云端访问其外部资源,就好像它们连接到其VCN内的任何其它本机资源一样。企业的用户可以访问其外部资源而无需在其本地部署网络与云之间设置精心设计的站点到站点网络、无需对其外部资源进行任何改变并且无需配置要由站点到站点连接使用的路由。类似地,通过为外部资源创建逻辑接口并将该逻辑接口与外部资源的VNIC表示的虚拟IP地址相关联,外部资源(其驻留在客户的本地部署网络中)能够使用由SNCS104提供的安全私有网络连接性服务来安全地访问在云中(例如,在客户的VCN 148中)的资源和服务。

[0061] 图3描绘了根据某些实施例的由图1中所示的系统和子系统执行的用于提供安全私有网络连接性的处理的示例。图3中描绘的处理可以以在由相应系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)、硬件或其组合来实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。图3中呈现并在下面描述的过程300旨在是说明性和非限制性的。虽然图3描绘了以特定顺序或次序发生的各种处理步骤,但这并不旨在进行限制。在某些替代实施例中,这些步骤可以以某种不同的次序执行,或者一些步骤也可以并行执行。在某些实施例中(诸如在图1中描绘的实施例中),图3中描绘的处理可以由包括特定于租户的覆盖网络128的计算节点(例如,116、122、130和132)执行。

[0062] 图3中描述的处理假设与客户相关联的用户(例如,管理员)已创建客户的本地部署网络的外部站点表示(例如,106)并配置了外部网站表示106中的代理(例如,112)。图4中描绘的处理还假设SNCS104已经认证了代理112并且已经配置/建立了包括用于客户的分布式且水平可伸缩的计算节点群的特定于租户的覆盖网络(例如,128)。如图1中所描述的,一个或多个计算节点的集合包括资源主机(即,资源虚拟机130、132)和隧道主机(即,隧道虚拟机116、122)。

[0063] 当SNCS104执行包括分布式且水平可伸缩的计算节点群的特定于租户的覆盖网络(例如,128)时,可以在方框302处发起图3中描绘的处理。特定于租户的覆盖网络被用于在CSPI中的客户的VCN(例如,148)与客户的外部站点表示之间建立安全私有网络连接性。

[0064] 在方框304处,SNCS(经由控制平面API)将驻留在客户的本地部署网络中的外部资源注册为客户的VCN中的外部端点。外部端点由客户的VCN中的IP地址识别。如前所述,外部资源可以表示外部站点表示106中客户意图从其VCN内启用安全双向私有网络连接性的数据库、计算实例或应用。作为注册外部资源的一部分,SNCS的用户经由控制台UI或API提供与外部资源相关的配置信息,诸如与外部资源相关联的本地部署物理IP地址、可访问外部资源的端口号以及外部资源的主机名(或完全限定域名(FQDN))。用户还在客户的VCN中选择要在其中创建用于外部资源的外部端点的子网。基于配置信息,SNCS为客户的VCN中的外部资源创建外部端点。外部端点由客户的VCN中的IP地址、端口号和FQDN(主机名)识别。

[0065] 在方框306处,SNCS中的第一计算节点(例如,资源VM 130或资源VM 132)为客户的VCN中的外部端点创建外部资源表示。在某些实施方式中,外部资源表示的创建涉及由第一计算节点创建VNIC以及将外部端点的IP地址指派给VNIC。

[0066] 在方框308处,第一计算节点将与为客户的VCN中的外部资源表示创建的VNIC对应的配置信息传输到在本地部署网络中配置的代理112。作为在方框308中执行的处理的一部分,代理112下载配置信息并将其复制到驻留在本地部署网络中的注册的外部资源上。如前所述,配置信息可以包括例如VNIC的虚拟IP地址、与和VNIC相关联的计算实例相关联的完全限定域名以及与客户相关联的虚拟云网络的云标识符。使用配置信息,代理112创建/供应用于外部资源(例如,114A)的逻辑接口(例如,158)。在某些实施方式中,由代理112创建或供应逻辑接口包括由代理将指派给为外部资源表示创建的VNIC 142的虚拟IP地址指派给为外部资源114A供应的逻辑接口158。

[0067] 在方框310处,第二计算节点(例如,隧道VM 116或隧道VM 122)接收用于查询与驻留在客户的VCN中的资源(例如,计算实例150)相关联的信息的请求。在某些示例中,请求可以由驻留在本地部署网络中的外部资源(例如,114A)经其逻辑接口158被传输。例如,与客户相关联的用户可以(例如,经由UI 108)将用于查询与驻留在客户的VCN中的计算实例150相关联的信息的请求传输到驻留在客户的本地部署网络中的外部资源。外部资源可以进而将查询传输到驻留在本地部署网络中的代理112。代理112接收查询请求并将与查询请求对应的网络分组传输到在隧道VM中运行的隧道分片(120或126)。

[0068] 在方框312处,第二计算节点(例如,隧道VM 116或隧道VM 122)经由资源分片(例如,136或140)在为外部资源供应的逻辑接口与为客户的VCN中的外部资源表示创建的VNIC之间建立连接。在具体实施方式中,隧道分片(例如,120或126)可以包括将指派给外部资源的真实/物理IP地址转换成VNIC 142的虚拟IP地址并经由资源分片(136或140)发起到VNIC 142的连接的能力。资源分片进而发起与客户的VCN中的资源(例如,150)的连接。

[0069] 在方框314处,第二计算节点(例如,隧道VM 116或隧道VM 122)经由在方框410中建立的连接将请求传输到驻留在客户的VCN中的资源。在方框412处,第二计算节点经由建立的连接获得与请求对应的结果。然后将结果经由代理112传输到驻留在外部站点表示中的外部资源。例如,如果资源是在客户的VCN中执行的数据库,那么结果可以包括存储在数据库中的一个或多个表中的信息。

[0070] 图4是描绘根据某些实施例的驻留在客户的本地部署网络中的外部资源与客户的虚拟云网络中的外部资源的表示之间的网络分组流的流程图。图4中描绘的处理可以以在由相应系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)、硬件或其组合来实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。图4中呈现并在下面描述的过程400旨在是说明性和非限制性的。虽然图4描绘了以特定顺序或次序发生的各种处理步骤,但这并不旨在进行限制。在某些替代实施例中,这些步骤可以以某种不同的次序执行,或者一些步骤也可以并行执行。在某些实施例中(诸如在图2中描绘的实施例中),图4中描绘的处理可以由包括特定于租户的覆盖网络128的计算节点(例如,116、122、130和132)执行。

[0071] 当驻留在客户的本地部署网络(即,客户的外部站点表示106)中的外部资源(例如,数据库202)接收到对与驻留在客户的VCN(例如,148)中的资源(例如,150)相关联的信息的查询时,可以在方框402处发起图4中描绘的处理。如先前所描述的,与客户相关联的用户可以(例如,经由UI 108)将用于查询与驻留在客户的VCN中的计算实例150相关联的信息的请求传输到驻留在客户的本地部署网络中的外部资源。外部资源进而可以将查询传输到驻留在本地部署网络中的代理112。

[0072] 在方框404处,代理112接收查询并将与该查询对应的网络分组传输到在隧道VM中运行的隧道分片(120或126)。在某些示例中,作为在方框404中执行的处理的一部分,代理112可以在将网络分组传输到隧道分片之前对网络分组进行加密。

[0073] 在方框406处,隧道分片接收加密的网络分组并将加密的网络分组传输到在资源VM中运行的资源分片(136、140)。具体而言,并且如图2中所示,加密的网络分组可以由附接到资源分片(136、140)的工作者VNIC(251、252)接收。

[0074] 在方框408处,资源分片(136、140)对网络分组进行解密并执行网络地址转换(NAT)以将指派给外部资源的物理IP地址转换成与客户的VCN中的外部资源表示相关联的VNIC(例如,206)的虚拟IP地址。

[0075] 在方框410处,资源分片(136、140)将网络分组传输到为客户的VCN中的外部资源表示创建的VNIC。

[0076] 在方框412处,VNIC将与查询对应的网络分组传输到驻留在客户的VCN中的资源(例如,150)。

[0077] 图5是描绘根据某些实施例的在客户的虚拟云网络中的外部资源表示与驻留在客户的本地部署网络中的外部资源之间的网络分组流的流程图。图5中描绘的处理可以以在由相应系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)、硬件或其组合来实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。图5中呈现并在下面描述的过程500旨在是说明性和非限制性的。虽然图5描绘了以特定顺序或次序发生的各种处理步骤,但这并不旨在进行限制。在某些替代实施例中,这些步骤可以以某种不同的次序执行,或者一些步骤也可以并行执行。在某些实施例中(诸如在图2中描绘的实施例中),图5中描绘的处理可以由包括特定于租户的覆盖网络128的计算节点(例如,116、122、130和132)执行。

[0078] 当客户的VCN中的客户端应用(例如,144)接收到对与驻留在客户的本地部署网络(即,客户的外部站点表示106)中的外部资源(例如,202)相关联的信息的查询时,可以在方

框502处发起图5中描绘的处理。例如,可以经由客户端应用从与客户相关联的用户接收查询。作为在方框502中执行的处理的一部分,客户端应用144通过将与查询对应的网络分组传输到指派给客户的VCN中的VNIC的虚拟IP地址来发起到与外部资源表示相关联的VNIC (例如,206)的连接。

[0079] 在方框504处,客户端应用将与查询对应的网络分组传输到在SNCS中的资源VM中运行的资源分片(136或140)。具体而言,并且如图2中所示,网络分组可以由附接到资源分片(136、140)的工作者VNIC(251、252)接收。资源分片(136、140)中的代理服务器(244、254)执行网络地址转换(NAT)以将指派给VNIC的虚拟IP地址转换成外部站点表示106中的外部资源的物理IP地址并经由隧道分片(120、126)发起到代理112的连接。

[0080] 在方框506处,资源分片将网络分组传输到隧道分片(120、126)。作为在方框506中执行的处理的一部分,隧道分片可以在将分组传输到外部站点表示106中的代理112之前对从资源分片接收到的网络分组进行加密。

[0081] 在方框508处,隧道分片将网络分组传输到驻留在客户的外部站点表示中的代理112。作为在方框508中执行的处理的一部分,代理112在将网络分组传输到外部站点表示(例如,106)中的外部资源(例如,202)之前对网络分组进行解密。

[0082] 在方框510处,代理112将网络分组传输到驻留在客户的外部站点表示中的外部资源(例如,202)。外部资源接收与查询对应的网络分组并生成与查询对应的响应网络分组。然后,响应网络分组可以由外部资源传输回客户端应用。例如,作为响应网络分组流的一部分,与对查询的响应对应的网络分组从外部资源传输到代理。代理对网络分组进行加密并将加密的网络分组传输到隧道分片。隧道分片接收加密的分组并将分组传输到资源分片。资源分片对网络分组进行解密并执行反向网络地址转换(NAT)以将指派给外部资源的物理/真实IP地址转换成与客户的VCN中的外部资源表示相关联的VNIC的虚拟IP地址。然后,资源分片将响应网络分组传输到VNIC,该VNIC进而将响应分组传输到客户的VCN 148中的发出请求的客户端应用144。

[0083] 示例虚拟联网体系架构

[0084] 术语“云服务”一般用于指由云服务提供商(CSP)使用由CSP提供的系统和基础设施(云基础设施)按需(例如,经由订阅模型)向用户或客户提供的服务。通常,构成CSP的基础设施的服务器和系统与客户自己的本地部署的服务器和系统是分开的。因此,客户可以自身利用由CSP提供的云服务,而无需为服务购买单独的硬件和软件资源。云服务被设计为向订阅客户提供对应用和计算资源的简单、可伸缩的访问,而无需客户投资获得用于提供服务的基础设施。

[0085] 存在若干云服务提供商供应各种类型的云服务。存在各种不同类型或模型的云服务,包括软件即服务(SaaS)、平台即服务(PaaS)、基础设施即服务(IaaS)等。

[0086] 客户可以订阅由CSP提供的一个或多个云服务。客户可以是任何实体,诸如个人、组织、企业等。当客户订阅或注册由CSP提供的服务时,将为客户创建租赁或账户。然后,客户可以经由这个账户访问与该账户相关联的订阅的一个或多个云资源。

[0087] 如上所述,基础设施即服务(IaaS)是一种特定类型的云计算服务。在IaaS模型中,CSP提供基础设施(称为云服务提供商基础设施或CSPI),这些基础设施可以被客户使用来构建他们自己的可定制网络并部署客户资源。因此,客户的资源和网络由CSP提供的基础设

施托管在分布式环境中。这与传统计算不同,在传统计算中,在传统计算中,客户的资源和网络由客户提供的基础设施托管。

[0088] CSPI可以包括形成物理网络的互连的高性能计算资源,包括各种主机机器、存储器资源和网络资源,该物理网络也被称为基板网络或底层网络。CSPI中的资源可以散布在一个或多个数据中心上,这些数据中心可以在地理上散布在一个或多个地理地区上。虚拟化软件可以由这些物理资源执行以提供虚拟化的分布式环境。虚拟化在物理网络上创建覆盖网络(也称为基于软件的网络、软件定义的网络或虚拟网络)。CSPI物理网络为在物理网络之上创建一个或多个覆盖或虚拟网络提供了底层基础。物理网络(或基板网络(substrate network)或底层网络)包括物理网络设备,诸如物理交换机、路由器、计算机和主机机器等。覆盖网络是运行在物理基板网络之上的逻辑(或虚拟)网络。给定的物理网络可以支持一个或多个覆盖网络。覆盖网络通常使用封装技术来区分属于不同覆盖网络的业务。虚拟或覆盖网络也称为虚拟云网络(VCN)。虚拟网络是使用软件虚拟化技术实现的(例如,管理程序、由网络虚拟化设备(NVD)(例如,智能网卡(smartNIC))实现的虚拟功能、架顶式(TOR)交换机、实现由NVD执行的一个或多个功能的智能TOR,以及其它机制)以创建可以在物理网络之上运行的网络抽象的层。虚拟网络可以采用多种形式,包括对等网络、IP网络等。虚拟网络通常是或者层3IP网络或者层2VLAN。这种虚拟或覆盖联网的方法常常被称为虚拟或覆盖层3网络。为虚拟网络开发的协议的示例包括IP-in-IP(或通用路由封装(GRE))、虚拟可扩展局域网(VXLAN—IETF RFC7348)、虚拟私有网络(VPN)(例如,MPLS层3虚拟私有网络(RFC4364))、VMware的NSX、GENEVE(通用网络虚拟化封装)等。

[0089] 对于IaaS,由CSP提供的基础设施(CSPI)可以被配置为通过公共网络(例如,互联网)提供虚拟化计算资源。在IaaS模型中,云计算服务提供商可以托管基础设施组件(例如,服务器、存储设备、网络节点(例如,硬件)、部署软件、平台虚拟化(例如,管理程序层)等)。在一些情况下,IaaS提供商还可以供应各种服务来伴随这些基础设施组件(例如,计费、监视、日志记录、安全性、负载均衡和聚类等)。因此,由于这些服务可以是策略驱动的,因此IaaS用户可以能够实现策略来驱动负载均衡以维持应用可用性和性能。CSPI提供基础设施和互补云服务的集合,这使得客户能够在高度可用的被托管的分布式环境中构建和运行广泛的应用和服务。CSPI在可从各种联网位置(诸如从客户的本地部署网络)安全访问的灵活的虚拟网络中供应高性能计算资源和能力以及存储容量。当客户订阅或注册由CSP提供的IaaS服务时,为该客户创建的租赁是CSPI内的安全且隔离的分区,客户可以在其中创建、组织和管理他们的云资源。

[0090] 客户可以使用由CSPI提供的计算、存储器和联网资源来构建他们自己的虚拟网络。可以在这些虚拟网络上部署一个或多个客户资源或工作负载,诸如计算实例。例如,客户可以使用由CSPI提供的资源来构建一个或多个可定制且私有的虚拟网络,称为虚拟云网络(VCN)。客户可以在客户VCN上部署一个或多个客户资源,诸如计算实例。计算实例可以采用虚拟机、裸机实例等形式。因此,CSPI提供基础设施和互补云服务的集合,这使得客户能够在高度可用的虚拟托管环境中构建和运行广泛的应用和服务。客户不管理或控制由CSPI提供的底层物理资源,但可以控制操作系统、存储装置和已部署的应用;并且可能对所选择的联网组件(例如,防火墙)进行有限的控制。

[0091] CSP可以提供控制台,该控制台使得客户和网络管理员能够使用CSPI资源来配置、

访问和管理部署在云中的资源。在某些实施例中,控制台提供可以被用于访问和管理CSPI的基于web的用户界面。在某些实施方式中,控制台是由CSP提供的基于web的应用。

[0092] CSPI可以支持单租赁或多租赁体系架构。在单租赁体系架构中,软件(例如,应用、数据库)或硬件组件(例如,主机机器或服务器)服务于单个客户或租户。在多租赁体系架构中,软件或硬件组件服务于多个客户或租户。因此,在多租赁体系架构中,CSPI资源在多个客户或租户之间共享。在多租赁情况下,在CSPI内采取预防措施并实施保护措施,以确保每个租户的数据都是隔离的并且对其他租户保持不可见。

[0093] 在物理网络中,网络端点(“端点”)是指连接到物理网络并与其所连接的网络来回通信的计算设备或系统。物理网络中的网络端点可以连接到局域网(LAN)、广域网(WAN)或其它类型的物理网络。物理网络中传统端点的示例包括调制解调器、集线器、桥接器、交换机、路由器和其它联网设备、物理计算机(或主机机器)等。物理网络中的每个物理设备都有可以被用于与设备通信的固定网络地址。这个固定网络地址可以是层2地址(例如,MAC地址)、固定的层3地址(例如,IP地址)等。在虚拟化环境或虚拟网络中,端点可以包括各种虚拟端点,诸如由物理网络的组件托管(例如,由物理主机机器托管)的虚拟机。虚拟网络中的这些端点由覆盖地址寻址,其中覆盖地址诸如覆盖层2地址(例如,覆盖MAC地址)和覆盖层3地址(例如,覆盖IP地址)。网络覆盖通过允许网络管理者使用软件管理(例如,经由实现用于虚拟网络的控制平面的软件)在与网络端点相关联的覆盖地址周围移动来实现灵活性。因而,与物理网络不同,在虚拟网络中,可以使用网络管理软件将覆盖地址(例如,覆盖IP地址)从一个端点移动到另一个端点。由于虚拟网络构建在物理网络之上,因此虚拟网络中组件之间的通信涉及虚拟网络和底层物理网络两者。为了促进此类通信,CSPI的组件被配置为学习和存储将虚拟网络中的覆盖地址映射到基板网络中的实际物理地址的映射,反之亦然。然后使用这些映射来促进通信。客户业务被封装以促进在虚拟网络中的路由。

[0094] 因而,物理地址(例如,物理IP地址)与物理网络中的组件相关联,并且覆盖地址(例如,覆盖IP地址)与虚拟或覆盖网络中的实体相关联。物理IP地址是与基础或物理网络中的物理设备(例如,网络设备)相关联的IP地址。例如,每个NVD都具有相关联的物理IP地址。覆盖IP地址是与覆盖网络中的实体相关联的覆盖地址,诸如与客户的虚拟云网络(VCN)中的计算实例相关联的覆盖地址。两个不同的客户或租户(每个客户或租户都具有其自己的私有VCN)可以潜在地在其VCN中使用相同的覆盖IP地址而无需彼此了解。物理IP地址和覆盖IP地址两者都是真实IP地址的类型。这些地址与虚拟IP地址是分开的。虚拟IP地址通常是表示或映射到多个真实IP地址的单个IP地址。虚拟IP地址提供了虚拟IP地址与多个真实IP地址之间的一对多映射。例如,负载均衡器可以使用VIP来映射或表示多个服务器,每个服务器都具有其自己的真实IP地址。

[0095] 云基础设施或CSPI在物理上托管在世界上一个或多个地区的一个或多个数据中心中。CSPI可以包括物理或基板网络中的组件和位于构建在物理网络组件之上的虚拟网络中的虚拟化组件(例如,虚拟网络、计算实例、虚拟机等)。在某些实施例中,CSPI在领域(realm)、地区(region)和可用性域(availability domain)中被组织和托管。地区通常是包含一个或多个数据中心的局部化的地理区域。地区一般彼此独立并且可以相隔很远,例如,跨越国家甚至大陆。例如,第一个地区可以在澳大利亚,另一个在日本,又一个在印度,等等。CSPI资源在地区之间划分,使得每个地区都有自己独立的CSPI资源子集。每个地区可

以提供核心基础设施服务和资源的集合,诸如计算资源(例如,裸机服务器、虚拟机、容器和相关基础设施等);存储资源(例如,块卷存储装置、文件存储装置、对象存储装置、归档存储装置);联网资源(例如,虚拟云网络(VCN)、负载平衡资源、与本地部署网络的连接)、数据库资源;边缘联网资源(例如,DNS);以及访问管理和监视资源等。每个地区一般具有多条路径将其连接到领域中的其它地区。

[0096] 一般而言,应用被部署在它被最频繁使用的地区中(即,部署在与该地区相关联的基础设施上),因为使用附近的资源比使用远处的资源更快。应用也可以出于各种原因而部署在不同的地区,诸如冗余以减轻地区范围内事件(诸如大型天气系统或地震)的风险,以满足法律管辖区、税域和其它商业或社会标准等的不同要求。

[0097] 地区内的数据中心可以被进一步组织和细分为可用性域(AD)。可用性域可以与位于地区内的一个或多个数据中心对应。地区可以由一个或多个可用性域组成。在这种分布式环境中,CSPI资源是特定于地区的(诸如虚拟云网络(VCN)),或者是特定于可用性域的(诸如计算实例)。

[0098] 地区内的AD彼此隔离,具有容错能力,并且被配置为使得它们极不可能同时发生故障。这是通过AD不共享关键基础设施资源(诸如联网、物理线缆、线缆路径、线缆入口点等)来实现的,使得地区内的一个AD处的故障不太可能影响同一地区内其它AD的可用性。同一地区内的AD可以通过低时延、高带宽网络彼此连接,这使得为其它网络(例如,互联网、客户的本地部署网络等)提供高可用性连接并且在多个AD中构建复制系统以实现高可用性和灾难恢复成为可能。云服务使用多个AD来确保高可用性并防止资源故障。随着IaaS提供商提供的基础设施的增长,可以添加更多地区和AD以及附加的容量。可用性域之间的业务通常是加密的。

[0099] 在某些实施例中,地区被分组为领域。领域是地区的逻辑集合。领域彼此隔离并且不共享任何数据。同一领域中的地区可以彼此通信,但不同领域中的地区不能通信。客户与CSP的租赁或账户存在于单个领域中,并且可以散布在属于该领域的一个或多个地区中。通常,当客户订阅IaaS服务时,会在领域内客户指定的地区(称为“主(home)”地区)中为该客户创建租赁或账户。客户可以将客户的租赁扩展到领域内的一个或多个其它地区。客户无法访问不在客户的租赁所在领域中的地区。

[0100] IaaS提供商可以提供多个领域,每个领域迎合客户或用户的特定集合。例如,可以为商业客户提供商业领域。作为另一个示例,可以为特定国家为该国家内的客户提供领域。作为又一个示例,可以为政府等提供政府领域。例如,政府领域可以迎合特定政府并且可以具有比商业领域更高的安全性级别。例如,Oracle云基础设施(Oracle Cloud Infrastructure,OCI)目前为商业地区提供领域,并且为政府云地区提供两个领域(例如,FedRAMP授权的和IL5授权的)。

[0101] 在某些实施例中,AD可以被细分成一个或多个故障域。故障域是AD内的基础设施资源的分组,以提供反亲和性。故障域允许计算实例的分布,使得这些实例不位于单个AD内的相同物理硬件上。这被称为反亲和性。故障域是指共享单点故障的硬件组件(计算机、交换机等)的集合。计算池在逻辑上被划分为故障域。因此,影响一个故障域的硬件故障或计算硬件维护事件不影响其它故障域中的实例。用于每个AD的故障域的数量可以因实施例而异。例如,在某些实施例中,每个AD包含三个故障域。故障域充当AD内的逻辑数据中心。

[0102] 当客户订阅IaaS服务时,来自CSPI的资源被供应给客户并与客户的租赁相关联。客户可以使用这些供应的资源来构建私有网络并在这些网络上部署资源。由CSPI在云中托管的客户网络被称为虚拟云网络(VCN)。客户可以使用为客户分配的CSPI资源来设置一个或多个虚拟云网络(VCN)。VCN是虚拟或软件定义的私有网络。部署在客户的VCN中的客户资源可以包括计算实例(例如,虚拟机、裸机实例)和其它资源。这些计算实例可以表示各种客户工作负载,诸如应用、负载均衡器、数据库等。部署在VCN上的计算实例可以通过公共网络(诸如互联网)与公共可访问端点(“公共端点”)、与同一VCN或其它VCN(例如,客户的其它VCN或不属于该客户的VCN)中的其它实例、与客户的本地部署数据中心或网络、以及与服务端点和其它类型的端点进行通信。

[0103] CSP可以使用CSPI来提供各种服务。在一些情况下,CSPI的客户本身可以像服务提供商一样起作用并使用CSPI资源来提供服务。服务提供商可以暴露服务端点,该服务端点由标识信息(例如,IP地址、DNS名称和端口)表征。客户的资源(例如,计算实例)可以通过访问由服务针对特定服务暴露的服务端点来消耗该特定服务。这些服务端点一般是用户经由公共通信网络(诸如互联网)使用与端点相关联的公共IP地址可公共访问的端点。可公共访问的网络端点有时也称为公共端点。

[0104] 在某些实施例中,服务提供商可以经由用于服务的端点(有时称为服务端点)来暴露服务。服务的客户然后可以使用这个服务端点来访问服务。在某些实施方式中,为服务提供的服务端点可以由打算消耗该服务的多个客户访问。在其它实施方式中,可以为客户提供专用服务端点,使得只有该客户可以使用该专用服务端点来访问服务。

[0105] 在某些实施例中,当创建VCN时,它与私有覆盖无类域间路由(CIDR)地址空间相关联,该地址空间是指派给VCN的一系列私有覆盖IP地址(例如,10.0/16)。VCN包括相关联的子网、路由表和网关。VCN驻留在单个地区内,但可以跨越该区域的可用性域中的一个或多个或全部。网关是为VCN配置的虚拟接口并且启用去往VCN或从VCN到VCN外部的一个或多个端点的业务的通信。可以为VCN配置一种或多种不同类型的网关,以启用去往和来自不同类型端点的通信。

[0106] VCN可以被细分为一个或多个子网络,诸如一个或多个子网。因此,子网是可以在VCN内创建的配置的单元或细分。VCN可以具有一个或多个子网。VCN内的每个子网都与连续范围的覆盖IP地址(例如,10.0.0.0/24和10.0.1.0/24)相关联,这些IP地址不与该VCN中的其它子网重叠并且表示VCN的地址空间内的地址空间子集。

[0107] 每个计算实例都与虚拟网络接口卡(VNIC)相关联,这使得计算实例能够参与VCN的子网。VNIC是物理网络接口卡(NIC)的逻辑表示。一般而言,VNIC是实体(例如,计算实例、服务)与虚拟网络之间的接口。VNIC存在于子网中,具有一个或多个相关联的IP地址,以及相关联的安全性规则或策略。VNIC相当于交换机上的层2端口。VNIC附接到计算实例和VCN内的子网。与计算实例相关联的VNIC使得计算实例能够成为VCN的子网的一部分,并且使得计算实例能够与和计算实例位于同一子网上的端点、与VCN中的不同子网中的端点、或者与VCN外部的端点进行通信(例如,发送和接收分组)。因此,与计算实例相关联的VNIC确定计算实例如何与VCN内部和外部的端点连接。当创建计算实例并将其添加到VCN内的子网时,创建用于计算实例的VNIC并将其与该计算实例相关联。对于包括计算实例的集合的子网,该子网包含与计算实例的该集合对应的VNIC,每个VNIC附接到计算机实例的该集合内的计

算实例。

[0108] 经由与计算实例相关联的VNIC为每个计算实例指派私有覆盖IP地址。这个私有覆盖IP地址在创建计算实例时指派给与计算实例相关联的VNIC并被用于路由去往和来自计算实例的业务。给定子网中的所有VNIC都使用相同的路由表、安全性列表和DHCP选项。如上所述,VCN内的每个子网都与连续范围的覆盖IP地址(例如,10.0.0.0/24和10.0.1.0/24)相关联,这些IP地址不与该VCN中的其它子网重叠并且表示VCN的地址空间内的地址空间子集。对于VCN的特定子网上的VNIC,指派给该VNIC的私有覆盖IP地址是来自为子网分配的连续范围的覆盖IP地址的地址。

[0109] 在某些实施例中,除了私有覆盖IP地址之外,计算实例还可以可选地被指派附加的覆盖IP地址,诸如例如在公共子网中的情况下的一个或多个公共IP地址。这些多个地址在同一个VNIC上或者在与计算实例相关联的多个VNIC上被指派。但是,每个实例具有主VNIC,该主VNIC是在实例启动期间创建的并且与指派给该实例的覆盖私有IP地址相关联—这个主VNIC无法被移除。称为辅VNIC的附加VNIC可以添加到与主VNIC相同的可用性域中的现有实例。所有VNIC都在与该实例相同的可用性域中。辅VNIC可以位于与主VNIC相同的VCN中的子网中,或者位于同一VCN或不同VCN中的不同子网中。

[0110] 如果计算实例在公共子网中,那么可以可选地为其指派公共IP地址。在创建子网时,可以将子网指定为公共子网或者私有子网。私有子网意味着子网中的资源(例如,计算实例)和相关联的VNIC不能具有公共覆盖IP地址。公共子网意味着子网中的资源和相关联的VNIC可以具有公共IP地址。客户可以指定子网存在于单个可用性域中,或者跨地区或领域中的多个可用性域存在。

[0111] 如上所述,VCN可以被细分成一个或多个子网。在某些实施例中,为VCN配置的虚拟路由器(VR)(称为VCN VR或简称为VR)使得VCN的子网之间能够通信。对于VCN内的子网,VR表示用于该子网的逻辑网关,它使得该子网(即,该子网上的计算实例)能够与VCN内其它子网上的端点以及VCN外的其它端点进行通信。VCN VR是逻辑实体,其被配置为在VCN中的VNIC和与VCN相关联的虚拟网关(“网关”)之间路由业务。下文关于图6来进一步描述网关。VCN VR是层3/IP层概念。在一个实施例中,对于VCN存在一个VCN VR,其中VCN VR具有潜在不受限制数量的由IP地址寻址的端口,VCN的每个子网有一个端口。以这种方式,VCN VR对于VCN VR所附接到的VCN中的每个子网具有不同的IP地址。VR还连接到为VCN配置的各种网关。在某些实施例中,用于子网的覆盖IP地址范围中的特定覆盖IP地址被保留用于该子网的VCN VR的端口。例如,考虑VCN具有两个子网,相关联的地址范围分别是10.0/16和10.1/16。对于地址范围为10.0/16的VCN内的第一个子网,这个范围内的地址被保留用于该子网的VCN VR的端口。在一些情况下,范围内的第一个IP地址可以被保留用于VCN VR。例如,对于覆盖IP地址范围为10.0/16的子网,可以为该子网的VCN VR的端口保留IP地址10.0.0.1。对于地址范围为10.1/16的同一VCN内的第二个子网,VCN VR可以具有用于IP地址为10.1.0.1的第二个子网的端口。VCN VR对于VCN中的每个子网具有不同的IP地址。

[0112] 在一些其它实施例中,VCN内的每个子网可以具有其自己的相关联的VR,该VR可由子网使用与VR相关联的保留或默认IP地址进行寻址。例如,保留或默认的IP地址可以是与该子网相关联的IP地址范围中的第一个IP地址。子网中的VNIC可以使用这个默认或保留的IP地址与和子网相关联的VR进行通信(例如,发送和接收分组)。在这种实施例中,VR是该子

网的入口/出口点。与VCN内的子网相关联的VR可以与和VCN内的其它子网相关联的其它VR进行通信。VR还可以与和VCN相关联的网关进行通信。子网的VR功能在为子网中的VNIC执行VNIC功能的一个或多个NVD上运行或由该一个或多个NVD执行。

[0113] 可以为VCN配置路由表、安全性规则和DHCP选项。路由表是用于VCN的虚拟路由表并且包括通过网关或特殊配置的实例将业务从VCN内的子网路由到VCN外的目的地的规则。可以定制VCN的路由表以控制分组如何转发/路由到VCN和从VCN转发/路由。DHCP选项是指在实例启动时自动提供给实例的配置信息。

[0114] 为VCN配置的安全性规则表示用于VCN的覆盖防火墙规则。安全性规则可以包括入口和出口规则,并指定允许进出VCN实例内的业务的类型(例如,基于协议和端口)。客户可以选择给定规则是有状态的还是无状态的。例如,客户可以通过用源CIDR0.0.0.0/0和目的地TCP端口22设置有状态入口规则来允许来自任何地方的传入SSH业务到达实例的集合。安全性规则可以使用网络安全组或安全性列表来实现。网络安全组由仅适用于该组中的资源的安全性规则的集合组成。另一方面,安全性列表包括适用于使用该安全性列表的任何子网中的所有资源的规则。VCN可以设置有带有默认安全性规则的默认安全性列表。为VCN配置的DHCP选项提供配置信息,该配置信息在实例启动时自动被提供给VCN中的实例。

[0115] 在某些实施例中,用于VCN的配置信息由VCN控制平面确定和存储。例如,用于VCN的配置信息可以包括关于以下的信息:与VCN相关联的地址范围、VCN内的子网和相关联的信息、与VCN相关联的一个或多个VR、VCN中的计算实例和相关联的VNIC、执行与VCN相关联的各种虚拟化网络功能(例如,VNIC、VR、网关)的NVD、用于VCN的状态信息以及其它VCN相关信息。在某些实施例中,VCN分发服务向NVD发布由VCN控制平面或其部分存储的配置信息。分发的信息可以被用于更新由NVD存储和使用的信息(例如,转发表、路由表等),以将分组转发到VCN中的计算实例或从计算实例转发分组。

[0116] 在某些实施例中,VCN和子网的创建由VCN控制平面(CP)处置并且计算实例的启动由计算控制平面处置。计算控制平面负责为计算实例分配物理资源,然后调用VCN控制平面来创建VNIC并将其附接到计算实例。VCN CP还将VCN数据映射发送到被配置为执行分组转发和路由功能的VCN数据平面。在某些实施例中,VCN CP提供负责向VCN数据平面提供更新的分发服务。VCN控制平面的示例也在图11、图12、图13和图14中描绘(参见附图标记1116、1216、1316和1416)并在下面进行描述。

[0117] 客户可以使用由CSPI托管的资源创建一个或多个VCN。部署在客户VCN上的计算实例可以与不同的端点进行通信。这些端点可以包括由CSPI托管的端点和CSPI外部的端点。

[0118] 用于使用CSPI实现基于云的服务的各种不同体系架构在图6、图7、图8、图9、图10、图11、图12、图13和图15中描绘,并且在下文中进行描述。图6是分布式环境600的高级别图,示出了根据某些实施例的由CSPI托管的覆盖或客户VCN。图6中描绘的分布式环境包括覆盖网络中的多个组件。图6中描绘的分布式环境600仅仅是个示例,并且不旨在不适当地限制要求保护的实施例的范围。许多变化、替代和修改是可能的。例如,在一些实施方式中,图6中描绘的分布式环境可以具有比图1中所示的系统或组件更多或更少的系统或组件,可以组合两个或更多个系统,或者可以具有不同的系统配置或布置。

[0119] 如图6中描绘的示例中所示,分布式环境600包括提供服务和资源的CSPI 601,客户可以订阅并使用这些服务和资源来构建他们的虚拟云网络(VCN)。在某些实施例中,CSPI

601向订阅客户供应IaaS服务。CSPI 601内的数据中心可以被组织到一个或多个地区。图6中示出了一个示例地区“地区US”602。客户已经为地区602配置了客户VCN 604。客户可以在VCN 604上部署各种计算实例,其中计算实例可以包括虚拟机或裸机实例。实例的示例包括应用、数据库、负载均衡器等。

[0120] 在图6中描绘的实施例中,客户VCN 604包括两个子网,即,“子网-1”和“子网-2”,每个子网具有其自己的CIDR IP地址范围。在图6中,子网-1的覆盖IP地址范围是10.0/16,并且子网-2的地址范围是10.1/16。VCN虚拟路由器605表示用于VCN的逻辑网关,它启用VCN 604的子网之间以及与VCN外部的其它端点的通信。VCN VR 605被配置为在VCN 604中的VNIC与和VCN 604相关联的网关之间路由业务。VCN VR 605为VCN 604的每个子网提供端口。例如,VR 605可以为子网-1提供具有IP地址10.0.0.1的端口并为子网-2提供具有IP地址10.1.0.1的端口。

[0121] 可以在每个子网上部署多个计算实例,其中计算实例可以是虚拟机实例和/或裸机实例。子网中的计算实例可以由CSPI 601内的一个或多个主机机器托管。计算实例经由与计算实例相关联的VNIC参与子网。例如,如图6中所示,计算实例C1经由与计算实例相关联的VNIC成为子网-1的一部分。同样,计算实例C2经由与C2相关联的VNIC成为子网-1的一部分。以类似的方式,多个计算实例(可以是虚拟机实例或裸机实例)可以是子网-1的一部分。经由其相关联的VNIC,每个计算实例都被指派私有覆盖IP地址和MAC地址。例如,在图6中,计算实例C1的覆盖IP地址为10.0.0.2,MAC地址为M1,而计算实例C2的私有覆盖IP地址为10.0.0.3,MAC地址为M2。子网-1中的每个计算实例(包括计算实例C1和C2)都具有去往使用IP地址10.0.0.1的VCN VR 605的默认路由,该IP地址是用于子网-1的VCN VR 605的端口的IP地址。

[0122] 子网-2上可以部署有多个计算实例,包括虚拟机实例和/或裸机实例。例如,如图6中所示,计算实例D1和D2经由与相应计算实例相关联的VNIC成为子网-2的部分。在图6中所描绘的实施例中,计算实例D1的覆盖IP地址为10.1.0.2,MAC地址为MM1,而计算实例D2的私有覆盖IP地址为10.1.0.3,MAC地址为MM2。子网-2中的每个计算实例(包括计算实例D1和D2)都具有去往使用IP地址10.1.0.1的VCN VR 605的默认路由,该IP地址是用于子网-2的VCN VR 605的端口的IP地址。

[0123] VCN A 604还可以包括一个或多个负载均衡器。例如,可以为子网提供负载均衡器,并且可以将负载均衡器配置为跨子网上的多个计算实例对业务进行负载平衡。还可以提供负载均衡器以在VCN中跨子网对业务进行负载平衡。

[0124] 部署在VCN 604上的特定计算实例可以与各种不同的端点通信。这些端点可以包括由CSPI 700托管的端点和CSPI 700外部的端点。由CSPI 601托管的端点可以包括:与特定计算实例位于同一子网上的端点(例如,子网-1中两个计算实例之间的通信);位于不同子网上但位于同一VCN内的端点(例如,子网-1中的计算实例与子网-2中的计算实例之间的通信);同一地区中不同VCN中的端点(例如,子网-1中的计算实例与同一地区中的VCN 606或610中的端点之间的通信,子网-1中的计算实例与同一地区中服务网络610中的端点之间的通信);或不同地区中的VCN中的端点(例如,子网-1中的计算实例与不同地区中的VCN 608中的端点之间的通信)。由CSPI 601托管的子网中的计算实例也可以与不由CSPI 601托管(即,在CSPI 601外部)的端点进行通信。这些外部端点包括客户的本地部署网络616中的

端点、其它远程云托管网络618内的端点、经由公共网络(诸如互联网)可访问的公共端点614及其它端点。

[0125] 使用与源计算实例和目的地计算实例相关联的VNIC促进同一子网上的计算实例之间的通信。例如,子网-1中的计算实例C1可能想要将分组发送到子网-1中的计算实例C2。对于源自源计算实例且其目的地是同一子网中的另一个计算实例的分组,该分组首先由与源计算实例相关联的VNIC处理。由与源计算实例相关联的VNIC执行的处理可以包括根据分组报头确定分组的目的地信息、识别为与源计算实例相关联的VNIC配置的任何策略(例如,安全性列表)、确定用于分组的下一跳、根据需要执行任何分组封装/解封装功能,然后将分组转发/路由到下一跳,目的是促进分组到其预期目的地的通信。当目的地计算实例与源计算实例位于同一子网中时,与源计算实例相关联的VNIC被配置为识别与目的地计算实例相关联的VNIC并将分组转发到该VNIC进行处理。然后执行与目的地计算实例相关联的VNIC并将分组转发到目的地计算实例。

[0126] 对于要从子网中的计算实例传送到同一VCN中不同子网中的端点的分组,通过与源和目的地计算实例相关联的VNIC以及VCN VR来促进通信。例如,如果图6中子网-1中的计算实例C1想要将分组发送到子网-2中的计算实例D1,那么该分组首先由与计算实例C1相关联的VNIC处理。与计算实例C1相关联的VNIC被配置为使用默认路由或VCN VR的端口10.0.0.1将分组路由到VCN VR 605。VCN VR 605被配置为使用端口10.1.0.1将分组路由到子网-2。然后,与D1相关联的VNIC接收并处理分组并且VNIC将分组转发到计算实例D1。

[0127] 对于要从VCN 604中的计算实例传送到VCN 604外部的端点的分组,通信由与源计算实例相关联的VNIC、VCN VR 605和与VCN 604相关联的网关促进。一种或多种类型的网关可以与VCN604相关联。网关是VCN和另一个端点之间的接口,其中该另一个端点在VCN外部。网关是层3/IP层概念并且使得VCN能够与VCN外部的端点进行通信。因此,网关促进VCN与其它VCN或网络之间的业务流动。可以为VCN配置各种不同类型的网关以促进与不同类型的端点的不同类型的通信。取决于网关,通信可以通过公共网络(例如,互联网)或通过私有网络进行。各种通信协议可以用于这些通信。

[0128] 例如,计算实例C1可能想要与VCN 604外部的端点通信。分组可以首先由与源计算实例C1相关联的VNIC处理。VNIC处理确定分组的目的地在C1的子网-1外部。与C1相关联的VNIC可以将分组转发到用于VCN 604的VCN VR 605。VCN VR 605然后处理分组,并且作为处理的一部分,基于分组的目的地来确定与VCN 604相关联的特定网关作为分组的下一跳。然后,VCN VR 605可以将分组转发到特定的识别出的网关。例如,如果目的地是客户的本地部署网络内的端点,那么分组可以由VCN VR 605转发到为VCN 604配置的动态路由网关(DRG)网关622。分组然后可以从网关转发到下一跳,以促进分组到其最终预期目的地的传送。

[0129] 可以为VCN配置各种不同类型的网关。可以为VCN配置的网关的示例在图6中描绘并且在下文进行描述。与VCN相关联的网关的示例也在图11、图12、图13和图14中描绘(例如,通过附图标记1134、1136、1138、1234、1236、1238、1334、1336、1338、1434、1436和1438引用的网关)并且在下文进行描述。如图6中描绘的实施例中所示,动态路由网关(DRG) 622可以添加到客户VCN 604或与客户VCN 604相关联,并为客户VCN 604与另一个端点之间的私有网络业务通信提供路径,其中该另一个端点可以是客户的本地部署网络616、CSPI 601的不同地区中的VCN 608、或者不由CSPI 601托管的其它远程云网络618。客户本地部署网络

616可以是使用客户的资源构建的客户网络或客户数据中心。对客户本地部署网络616的访问一般是非常受限的。对于同时具有客户本地部署网络616和由CSPI 601在云中部署或托管的一个或多个VCN 604的客户,客户可能想要他们的本地部署网络616和他们的基于云的VCN 604能够彼此通信。这使客户能够构建扩展的混合环境,包括由CSPI 601托管的客户的VCN 604和他们的本地部署网络616。DRG 622实现这种通信。为了实现此类通信,设置通信信道624,其中信道的一个端点位于客户本地部署网络616中,而另一个端点位于CSPI 601中并连接到客户VCN 604。通信信道624可以通过公共通信网络(诸如互联网)或私有通信网络。可以使用各种不同的通信协议,诸如公共通信网络(诸如互联网)上的IPsec VPN技术、使用私有网络而非公共网络的Oracle的FastConnect技术等。客户本地部署网络616中形成通信信道624的一个端点的设备或装备被称为客户本地装备(CPE),诸如图6中描绘的CPE 626。在CSPI 601侧,端点可以是执行DRG 622的主机机器。

[0130] 在某些实施例中,可以将远程对等连接(RPC)添加到DRG,这允许客户将一个VCN与不同地区中的另一个VCN对等。使用这种RPC,客户VCN 604可以使用DRG 622与另一个地区中的VCN 608连接。DRG 622还可以被用于与不由CSPI 601托管的其它远程云网络618(诸如Microsoft Azure云、亚马逊AWS云等)进行通信。

[0131] 如图6中所示,可以为客户VCN 604配置互联网网关(IGW)620,其使VCN 604上的计算实例能够与通过公共网络(诸如互联网)可访问的公共端点614通信。IGW 620是将VCN连接到诸如互联网之类的公共网络的网关。IGW 620使VCN(诸如VCN 604)内的公共子网(其中公共子网中的资源具有公共覆盖IP地址)能够直接访问公共网络614(诸如互联网)上的公共端点612。使用IGW 620,可以从VCN 604内的子网或从互联网发起连接。

[0132] 可以为客户的VCN 604配置网络地址转换(NAT)网关628,并使客户的VCN中不具有专用公共覆盖IP地址的云资源能够访问互联网,并且在不暴露这些资源的情况下这样做以指引传入的互联网连接(例如,L4-L7连接)。这使VCN内的私有子网(诸如VCN 604中的私有子网-1)能够私有访问互联网上的公共端点。在NAT网关中,只能从私有子网发起到公共互联网的连接,而不能从互联网发起到私有子网的连接。

[0133] 在某些实施例中,可以为客户VCN 604配置服务网关(SGW)626,并为VCN 604和服务网络610中支持的服务端点之间的私有网络业务提供路径。在某些实施例中,服务网络610可以由CSP提供并且可以提供各种服务。这种服务网络的示例是Oracle的服务网络,它提供可供客户使用的各种服务。例如,客户VCN 604的私有子网中的计算实例(例如,数据库系统)可以将数据备份到服务端点(例如,对象存储装置(Object Storage)),而无需公共IP地址或访问互联网。在某些实施例中,VCN可以仅具有一个SGW,并且连接只能从VCN内的子网发起,而不能从服务网络610发起。如果VCN与另一个VCN对等,那么另一个VCN中的资源通常不能访问SGW。用FastConnect或VPN Connect连接到VCN的本地部署网络中的资源也可以使用为该VCN配置的服务网关。

[0134] 在某些实施方式中,SGW 626使用服务无类域间路由(CIDR)标签的概念,该标签是表示用于感兴趣的服务或服务组的所有地区性公共IP地址范围的字符串。客户在他们配置SGW和相关路由规则以控制去往服务的业务时使用服务CIDR标签。如果服务的公共IP地址在未来发生改变,那么客户可以在配置安全性规则时可选地使用服务CIDR标签,而无需调整安全性规则。

[0135] 本地对等网关 (LPG) 632是可以添加到客户VCN 604并使VCN 604能够与同一地区中的另一个VCN对等的网关。对等是指VCN使用私有IP地址进行通信,业务无需穿过公共网络 (诸如互联网) 或无需通过客户的本地部署网络616路由业务。在优选实施例中,VCN对于它建立的每个对等体具有单独的LPG。本地对等或VCN对等是用于在不同应用或基础设施管理功能之间建立网络连接性的常见做法。

[0136] 服务提供商 (诸如服务网络610中的服务的提供商) 可以使用不同的访问模型提供对服务的访问。根据公共访问模型,服务可以作为可由客户VCN中的计算实例经由公共网络 (诸如互联网) 可公共访问的公共端点暴露,和/或可以经由SGW 626来私有访问。根据特定的私有访问模型,服务可作为客户的VCN中的私有子网中的私有IP端点进行访问。这被称为私有端点 (PE) 访问并且使服务提供商能够将其服务作为客户的私有网络中的实例暴露。私有端点资源表示客户的VCN内的服务。每个PE在客户的VCN中由客户选择的子网中表现为VNIC (称为PE-VNIC,具有一个或多个私有IP)。因此,PE提供了使用VNIC在私有客户VCN子网中呈现服务的方式。由于端点作为VNIC暴露,因此与VNIC相关联的所有特征 (诸如路由规则、安全性列表等) 现在都可用于PE VNIC。

[0137] 服务提供商可以注册他们的服务以启用通过PE的访问。提供商可以将策略与服务相关联,这限制了服务对客户租赁的可见性。提供商可以在单个虚拟IP地址 (VIP) 下注册多个服务,尤其是对于多租户服务。可以存在表示相同服务的多个这样的私有端点 (在多个VCN中)。

[0138] 私有子网中的计算实例然后可以使用PE VNIC的私有IP地址或服务DNS名称来访问服务。客户VCN中的计算实例可以通过将业务发送到客户VCN中的PE的私有IP地址来访问该服务。私有访问网关 (PAGW) 630是可以附接到服务提供商VCN (例如,服务网络610中的VCN) 的网关资源,该服务提供商VCN充当来自/去往客户子网私有端点的所有业务的入口/出口点。PAGW 630使提供商能够在不利用其内部IP地址资源的情况下扩展PE连接的数量。提供商只需要为在单个VCN中注册的任何数量的服务配置一个PAGW。提供商可以将服务表示为一个或多个客户的多个VCN中的私有端点。从客户的角度来看,代替附接到客户的实例,PE VNIC看起来附接到客户希望与之交互的服务。去往私有端点的业务经由PAGW 630路由到服务。这些被称为客户到服务私有连接 (C2S连接)。

[0139] 通过允许业务流经FastConnect/IPsec链路和客户VCN中的私有端点,PE概念还可以被用于将对于服务的私有访问扩展到客户的本地部署网络和数据中心。通过允许业务在LPG 632和客户的VCN中的PE之间流动,还可以将对于服务的私有访问扩展到客户的对等VCN。

[0140] 客户可以在子网级别控制VCN中的路由,因此客户可以指定客户的VCN (诸如VCN 604) 中的哪些子网使用每个网关。VCN的路由表被用于决定是否允许业务通过特定网关离开VCN。例如,在特定实例中,用于客户VCN 604内的公共子网的路由表可以通过IGW 620发送非本地业务。用于同一客户VCN 604内的私有子网的路由表可以通过SGW 626发送以CSP服务为目的地的业务。所有剩余业务可以经由NAT网关628发送。路由表仅控制离开VCN的业务。

[0141] 与VCN相关联的安全性列表被用于控制经由入站连接经由网关进入VCN的业务。子网中的所有资源都使用相同的路由表和安全性列表。安全性列表可以被用于控制允许进出

VCN的子网中的实例的特定类型的业务。安全性列表规则可以包括入口(入站)和出口(出站)规则。例如,入口规则可以指定允许的源地址范围,而出口规则可以指定允许的目的地地址范围。安全性规则可以指定特定的协议(例如,TCP、ICMP)、特定的端口(例如,用于SSH的22、用于Windows RDP的3389)等。在某些实施方式中,实例的操作系统可以强制执行其自己的符合安全性列表规则的防火墙规则。规则可以是有状态的(例如,跟踪连接并自动允许响应,而无需针对响应业务的明确安全性列表规则)或无状态的。

[0142] 来自客户VCN的访问(即,通过部署在VCN 604上的资源或计算实例)可以被分类为公共访问、私有访问或专用访问。公共访问是指使用公共IP地址或NAT来访问公共端点的访问模型。私有访问使VCN 604中具有私有IP地址的客户工作负载(例如,私有子网中的资源)能够访问服务,而无需穿过诸如互联网之类的公共网络。在某些实施例中,CSPI 601使具有私有IP地址的客户VCN工作负载能够使用服务网关访问服务(的公共服务端点)。因此,服务网关通过在客户的VCN和驻留在客户的私有网络外部的服务的公共端点之间建立虚拟链路来供应私有访问模型。

[0143] 此外,CSPI可以使用诸如FastConnect公开对等之类的技术供应专用公共访问,其中客户本地部署实例可以使用FastConnect连接来访问客户VCN中的一个或多个服务,而无需穿过公共网络(诸如互联网)。CSPI还可以使用FastConnect私有对等来供应专用私有访问,其中具有私有IP地址的客户本地部署实例可以使用FastConnect连接访问客户的VCN工作负载。FastConnect是对使用公共互联网将客户的本地部署网络连接到CSPI及其服务的网络连接性替代方案。与基于互联网的连接相比,FastConnect提供了简单、灵活且经济的方式来创建具有更高带宽选项的专用和私有连接以及更可靠和一致的联网体验。

[0144] 图6和上面的伴随描述描述了示例虚拟网络中的各种虚拟化组件。如上所述,虚拟网络构建在底层物理或基板网络上。图7描绘了根据某些实施例的为虚拟网络提供底层的CSPI 700内的物理网络中的物理组件的简化体系架构图。如图所示,CSPI 700提供分布式环境,包括由云服务提供商(CSP)提供的组件和资源(例如,计算、存储器和联网资源)。这些组件和资源被用于向订阅客户(即,已订阅由CSP提供的一个或多个服务的客户)提供云服务(例如,IaaS服务)。基于客户订阅的服务,为客户供应CSPI 700的资源(例如,计算、存储器和联网资源)的子集。然后,客户可以使用由CSPI 700提供的物理计算、存储器和联网资源构建其自己的基于云的(即,CSPI托管的)可定制且私有的虚拟网络。如前面所指示的,这些客户网络被称为虚拟云网络(VCN)。客户可以在这些客户VCN上部署一个或多个客户资源,诸如计算实例。计算实例可以是虚拟机、裸机实例等形式。CSPI 700提供基础设施和互补云服务的集合,这使客户能够在高度可用的托管环境中构建和运行广泛的应用和服务。

[0145] 在图7中描绘的示例实施例中,CSPI 700的物理组件包括一个或多个物理主机机器或物理服务器(例如,702、706、708)、网络虚拟化设备(NVD)(例如,710、712)、架顶式(TOR)交换机(例如,714、716)和物理网络(例如,718)、以及物理网络718中的交换机。物理主机机器或服务器可以托管和执行参与VCN的一个或多个子网的各种计算实例。计算实例可以包括虚拟机实例和裸机实例。例如,图6中描绘的各种计算实例可以由图7中描绘的物理主机机器托管。VCN中的虚拟机计算实例可以由一个主机机器或多个不同的主机机器执行。物理主机机器也可以托管虚拟主机机器、基于容器的主机或功能等。图6中描绘的VNIC和VCN VR可以由图7中描绘的NVD执行。图6中描绘的网关可以由图7中描绘的主机机器和/

或由NVD执行。

[0146] 主机机器或服务器可以执行在主机机器上创建和启用虚拟化环境的管理程序(也称为虚拟机监视器或VMM)。虚拟化或虚拟化环境促进了基于云的计算。一个或多个计算实例可以由主机机器上的管理程序在该主机机器上创建、执行和管理。主机机器上的管理程序使主机机器的物理计算资源(例如,计算、存储器和联网资源)能够在由主机机器执行的各种计算实例之间共享。

[0147] 例如,如图7中所描绘的,主机机器702和708分别执行管理程序760和766。这些管理程序可以使用软件、固件或硬件或其组合来实现。通常,管理程序是位于主机机器的操作系统(OS)之上的进程或软件层,OS进而在主机机器的硬件处理器上执行。管理程序通过使主机机器的物理计算资源(例如,诸如处理器/核之类的处理资源、存储器资源、联网资源)能够在由主机机器执行的各种虚拟机计算实例之间共享来提供虚拟化环境。例如,在图7中,管理程序760可以位于主机机器702的OS之上并使主机机器702的计算资源(例如,处理、存储器和联网资源)能够在由主机机器702执行的计算实例(例如,虚拟机)之间共享。虚拟机可以具有其自己的操作系统(称为访客操作系统),其可以与主机机器的OS相同或不同。由主机机器执行的虚拟机的操作系统可以与由同一主机机器执行的另一个虚拟机的操作系统相同或不同。因此,管理程序使多个操作系统能够彼此一起执行,同时共享主机机器的相同计算资源。图7中描绘的主机机器可以具有相同或不同类型的管理程序。

[0148] 计算实例可以是虚拟机实例或裸机实例。在图7中,主机机器702上的计算实例768和主机机器708上的计算实例774是虚拟机实例的示例。主机机器706是提供给客户的裸机实例的示例。

[0149] 在某些情况下,可以向单个客户供应整个主机机器,并且由该主机机器托管的全部一个或多个计算实例(或者虚拟机或者裸机实例)都属于该同一客户。在其它情况下,主机机器可以在多个客户(即,多个租户)之间共享。在这种多租赁场景中,主机机器可以托管属于不同客户的虚拟机计算实例。这些计算实例可以是不同客户的不同VCN的成员。在某些实施例中,裸机计算实例由没有管理程序的裸机服务器托管。当供应裸机计算实例时,单个客户或租户维护对托管该裸机实例的主机箱器的物理CPU、存储器和网络接口的控制,并且主机机器不与其他客户或租户共享。

[0150] 如前所述,作为VCN的一部分的每个计算实例都与使该计算实例能够成为VCN的子网的成员的VNIC相关联。与计算实例相关联的VNIC促进去往和来自计算实例的分组或帧的通信。VNIC在创建计算实例时与该计算实例相关联。在某些实施例中,对于由主机机器执行的计算实例,与该计算实例相关联的VNIC由连接到主机机器的NVD执行。例如,在图7中,主机机器702执行与VNIC 776相关联的虚拟机计算实例768,并且VNIC 776由连接到主机机器702的NVD 710执行。作为另一个示例,由主机机器706托管的裸机实例772与由连接到主机机器706的NVD 712执行的VNIC 780相关联。作为又一个示例,VNIC 784与由主机机器708执行的计算实例774相关联,并且VNIC 784由连接到主机机器708的NVD 712执行。

[0151] 对于由主机机器托管的计算实例,连接到该主机机器的NVD还执行与计算实例是其成员的VCN对应的VCN VR。例如,在图7中描绘的实施例中,NVD 710执行与计算实例768是其成员的VCN对应的VCN VR 777。NVD 712还可以执行与VCN对应的一个或多个VCN VR 783,该VCN与由主机机器706和708托管的计算实例对应。

[0152] 主机机器可以包括使主机机器能够连接到其它设备的一个或多个网络接口卡(NIC)。主机机器上的NIC可以提供使主机机器能够通信地连接到另一个设备的一个或多个端口(或接口)。例如,主机机器可以使用在主机机器上和NVD上提供的一个或多个端口(或接口)连接到NVD。主机机器也可以连接到其它设备(诸如另一个主机机器)。

[0153] 例如,在图7中,主机机器702使用链路720连接到NVD 710,链路720在由主机机器702的NIC 732提供的端口734与NVD 710的端口736之间延伸。主机机器706使用链路724连接到NVD 712,链路724在由主机机器706的NIC 744提供的端口746与NVD 712的端口748之间延伸。主机机器708使用链路726连接到NVD 712,链路726在由主机机器708的NIC 750提供的端口752与NVD 712的端口754之间延伸。

[0154] NVD进而经由通信链路连接到架顶式(TOR)交换机,这些交换机连接到物理网络718(也称为交换机架构)。在某些实施例中,主机机器和NVD之间以及NVD和TOR交换机之间的链路是以太网链路。例如,在图7中,NVD 710和712分别使用链路728和730连接到1126TOR交换机714和716。在某些实施例中,链路720、724、726、728和730是以太网链路。连接到TOR的主机机器和NVD的集合有时称为机架(rack)。

[0155] 物理网络718提供使TOR交换机能够彼此通信的通信架构。物理网络718可以是多层网络。在某些实施方式中,物理网络718是交换机的多层Clos网络,其中TOR交换机714和716表示多层和多节点物理交换网络718的叶级节点。不同的Clos网络配置是可能的,包括但不限于2层网络、3层网络、4层网络、5层网络和一般的“n”层网络。Clos网络的示例在图10中描绘并在下面进行描述。

[0156] 主机机器和NVD之间可能存在各种不同的连接配置,诸如一对一配置、多对一配置、一对多配置等。在一对一配置实施方式中,每个主机机器连接到自己单独的NVD。例如,在图7中,主机机器702经由主机机器702的NIC 732连接到NVD 710。在多对一配置中,多个主机机器连接到一个NVD。例如,在图7中,主机机器706和708分别经由NIC 744和750连接到同一个NVD 712。

[0157] 在一对多配置中,一个主机机器连接到多个NVD。图8示出了CSPI 800内的示例,其中主机机器连接到多个NVD。如图8中所示,主机机器802包括网络接口卡(NIC)804,其包括多个端口806和808。主机机器800经由端口806和链路820连接到第一NVD 810,并经由端口808和链路822连接到第二NVD 812。端口806和808可以是以太网端口并且主机机器802与NVD 810之间的链路820和与NVD 812之间的链路822可以是以太网链路。NVD 810进而连接到第一TOR交换机814并且NVD 812连接到第二TOR交换机816。NVD 810和812之间以及TOR交换机814和816之间的链路可以是以太网链路。TOR交换机814和816表示多层物理网络818中的层0交换设备。

[0158] 图8中描绘的布置提供了物理交换机网络818与主机机器802之间的两条单独的物理网络路径:第一条路径穿过TOR交换机814到NVD 810再到主机机器802,并且第二条路径穿过TOR交换机816到NVD 812再到主机机器802。单独的路径提供了主机机器802的增强的可用性(称为高可用性)。如果以下中的一者出现问题:路径(例如,路径之一中的链路断开)或设备(例如,特定NVD未运行),那么另一条路径可以被用于去往/来自主机机器802的通信。

[0159] 在图8中描绘的配置中,主机机器使用由主机机器的NIC提供的两个不同端口连接

到两个不同的NVD。在其它实施例中,主机机器可以包括使主机机器能够连接到多个NVD的多个NIC。

[0160] 返回参考图7,NVD是执行一个或多个网络和/或存储虚拟化功能的物理设备或组件。NVD可以是具有一个或多个处理单元(例如,CPU、网络处理单元(NPU)、FPGA、分组处理流水线等)、存储器(包括高速缓存)和端口的任何设备。各种虚拟化功能可以由NVD的一个或多个处理单元执行的软件/固件来执行。

[0161] NVD可以以各种不同的形式实现。例如,在某些实施例中,NVD被实现为称为smartNIC的接口卡或具有板载嵌入式处理器的智能NIC.smartNIC是独立于主机机器上的NIC的设备。在图7中,NVD 710和712可以被实现为分别连接到主机机器702以及主机机器706和708的smartNIC。

[0162] 但是,smartNIC只是NVD实施方式的一个示例。各种其它实施方式是可能的。例如,在一些其它实施方式中,NVD或由NVD执行的一个或多个功能可以结合到一个或多个主机机器、一个或多个TOR交换机以及CSPI 700的其它组件中或由其执行。例如,NVD可以在主机机器中实施,其中由NVD执行的功能由主机机器执行。作为另一个示例,NVD可以是TOR交换机的一部分,或者TOR交换机可以被配置为执行由NVD执行的功能,这使TOR交换机能够执行用于公共云的各种复杂分组转换。执行NVD的功能的TOR有时被称为智能TOR。在向客户供应虚拟机(VM)实例而非裸机(BM)实例的另外其它实施方式中,由NVD执行的功能可以在主机机器的管理程序内部实现。在一些其它实施方式中,NVD的功能中的一些功能可以被卸载到运行在主机机器群上的集中式服务。

[0163] 在某些实施例中,诸如当实现为如图7中所示的smartNIC时,NVD可以包括使其能够连接到一个或多个主机机器以及一个或多个TOR交换机的多个物理端口。NVD上的端口可以被分类为面向主机的端口(也称为“南端口”),或者面向网络或面向TOR的端口(也称为“北端口”)。NVD的面向主机的端口是用于将NVD连接到主机机器的端口。图7中面向主机的端口的示例包括NVD 710上的端口736以及NVD 712上的端口748和754。NVD的面向网络的端口是用于将NVD连接到TOR交换机的端口。图7中面向网络的端口的示例包括NVD 710上的端口756和NVD 712上的端口758。如图7中所示,NVD 710使用从NVD 710的端口756延伸到TOR交换机714的链路728连接到TOR交换机714。类似地,NVD 712使用从NVD 712的端口758延伸到TOR交换机716的链路730连接到TOR交换机716。

[0164] NVD经由面向主机的端口从主机机器接收分组和帧(例如,由主机机器托管的计算实例生成的分组和帧),并且在执行必要的分组处理之后,可以经由NVD的面向网络的端口将分组和帧转发到TOR交换机。NVD可以经由NVD的面向网络的端口从TOR交换机接收分组和帧,并且在执行必要的分组处理之后,可以经由NVD的面向主机的端口将分组和帧转发到主机机器。

[0165] 在某些实施例中,在NVD和TOR交换机之间可以存在多个端口和相关联的链路。可以聚合这些端口和链路以形成多个端口或链路的链路聚合体组(称为LAG)。链路聚合允许将两个端点之间(例如,NVD和TOR交换机之间)的多条物理链路视为单条逻辑链路。给定LAG中的所有物理链路都可以以相同的速度在全双工模式下操作。LAG有助于增加两个端点之间的连接的带宽和可靠性。如果LAG中的物理链路中的一条物理链路发生故障,那么业务将动态且透明地重新指派到LAG中的其它物理链路中的一条物理链路。聚合的物理链路比每

条单独的链路递送更高的带宽。与LAG相关联的多个端口被视为单个逻辑端口。业务可以在LAG的多条物理链路之间进行负载平衡。可以在两个端点之间配置一个或多个LAG。这两个端点可以位于NVD和TOR交换机之间、主机机器和NVD之间,等等。

[0166] NVD实现或执行网络虚拟化功能。这些功能由NVD执行的软件/固件执行。网络虚拟化功能的示例包括但不限于:分组封装和解封装功能;用于创建VCN网络的功能;用于实现网络策略的功能,诸如VCN安全性列表(防火墙)功能;促进分组去往VCN中的计算实例和来自该计算实例的路由和转发的功能等。在某些实施例中,在接收到分组后,NVD被配置为执行分组处理流水线用于处理分组并确定如何转发或路由分组。作为这个分组处理流水线的一部分,NVD可以执行与覆盖网络相关联的一个或多个虚拟功能,诸如执行与VCN中的计算实例相关联的VNIC、执行与VCN相关联的虚拟路由器(VR)、分组的封装和解封装以促进虚拟网络中的转发或路由、某些网关(例如,本地对等网关)的执行、安全性列表的实施、网络安全组、网络地址转换(NAT)功能(例如,逐个主机地将公共IP转换为私有IP)、节流功能和其它功能。

[0167] 在某些实施例中,NVD中的分组处理数据路径可以包括多个分组流水线,每个分组流水线由一系列分组变换级(stage)组成。在某些实施方式中,在接收到分组后,分组被解析并分类到单个流水线。然后以线性方式处理分组,一个级接一个级,直到分组被丢弃或者通过NVD的接口被发送出去为止。这些级提供基本的功能性分组处理构建块(例如,验证报头、强制执行节流、插入新的层2报头、强制执行L4防火墙、VCN封装/解封装等),以便可以通过组合现有级来构建新的流水线,并且可以通过创建新级并将它们插入现有流水线来添加新的功能。

[0168] NVD可以执行与VCN的控制平面和数据平面对应的控制平面功能和数据平面功能两者。VCN控制平面的示例也在图11、图12、图13和图14中描绘(参见附图标记1116、1216、1316和1416)并在下文中进行描述。VCN数据平面的示例在图11、图12、图13和图14中描绘(参见附图标记1118、1218、1318和1418)并在下文中进行描述。控制平面功能包括用于配置控制数据如何转发的网络的功能(例如,设置路由和路由表、配置VNIC等)。在某些实施例中,提供了VCN控制平面,它集中计算所有覆盖到基板映射并将它们发布到NVD和虚拟网络边缘设备(诸如各种网关,诸如DRG、SGW、IGW等)。防火墙规则也可以使用相同的机制发布。在某些实施例中,NVD仅获得与该NVD相关的映射。数据平面功能包括基于使用控制平面设置的配置来实际路由/转发分组的功能。VCN数据平面是通过在客户的网络分组穿过基板网络之前对其进行封装来实现的。封装/解封装功能在NVD上实现。在某些实施例中,NVD被配置为拦截进出主机机器的所有网络分组并执行网络虚拟化功能。

[0169] 如上面所指示的,NVD执行各种虚拟化功能,包括VNIC和VCN VR。NVD可以执行与连接到VNIC的一个或多个主机机器托管的计算实例相关联的VNIC。例如,如图7中所描绘的,NVD 710执行与由连接到NVD 710的主机机器702托管的计算实例768相关联的VNIC 776的功能。作为另一个示例,NVD 712执行与由主机机器706托管的裸机计算实例772相关联的VNIC 780,并执行与由主机机器708托管的计算实例774相关联的VNIC 784。主机机器可以托管属于不同VCN(属于不同客户)的计算实例,并且连接到主机机器的NVD可以执行与计算实例对应的VNIC(即,执行VNIC相关功能)。

[0170] NVD还执行与计算实例的VCN对应的VCN虚拟路由器。例如,在图7中描绘的实施例

中,NVD 710执行与计算实例768所属的VCN对应的VCN VR 777。NVD 712执行与由主机机器706和708托管的计算实例所属的一个或多个VCN对应的一个或多个VCN VR 783。在某些实施例中,与该VCN对应的VCN VR由连接到托管属于该VCN的至少一个计算实例的主机机器的所有NVD执行。如果主机机器托管属于不同VCN的计算实例,那么连接到该主机机器的NVD可以执行与这些不同VCN对应的VCN VR。

[0171] 除了VNIC和VCN VR之外,NVD还可以执行各种软件(例如,守护进程)并且包括一个或多个硬件组件,这些组件促进由NVD执行的各种网络虚拟化功能。为了简单起见,这些各种组件被分组在一起作为图7中所示的“分组处理组件”。例如,NVD 710包括分组处理组件786并且NVD 712包括分组处理组件788。例如,用于NVD的分组处理组件可以包括分组处理器,该分组处理器被配置为与NVD的端口和硬件接口进行交互以监视由NVD接收和使用NVD传送的所有分组并存储网络信息。网络信息例如可以包括识别由NVD处置的不同网络流的网络流信息和每个流信息(例如,每个流统计信息)。在某些实施例中,网络流信息可以以每个VNIC为基础进行存储。分组处理器可以执行逐分组的操纵以及实现有状态的NAT和L4防火墙(FW)。作为另一个示例,分组处理组件可以包括被配置为将由NVD存储的信息复制到一个或多个不同的复制目标存储库的复制代理。作为又一个示例,分组处理组件可以包括被配置为执行NVD的日志记录功能的日志记录代理。分组处理组件还可以包括用于监视NVD的性能和健康状况并且还可能监视连接到NVD的其它组件的状态和健康状况的软件。

[0172] 图6示出了示例虚拟或覆盖网络的组件,包括VCN、VCN内的子网、部署在子网上的计算实例、与计算实例相关联的VNIC、用于VCN的VR、以及为VCN配置的网关的集合。图6中描绘的覆盖组件可以由图7中描绘的物理组件中的一个或多个组件执行或托管。例如,VCN中的计算实例可以由图7中描绘的一个或多个主机机器执行或托管。对于由主机机器托管的计算实例,与该计算实例相关联的VNIC通常由连接到该主机机器的NVD执行(即,VNIC功能由连接到该主机机器的NVD提供)。用于VCN的VCN VR功能由连接到托管或执行作为该VCN的一部分的计算实例的主机机器的所有NVD执行。与VCN相关联的网关可以由一种或多种不同类型的NVD执行。例如,某些网关可以由smartNIC执行,而其它网关可以由一个或多个主机机器或NVD的其它实施方式执行。

[0173] 如上所述,客户VCN中的计算实例可以与各种不同的端点进行通信,其中端点可以与源计算实例在同一子网内、与源计算实例在不同子网中但在同一VCN内,或者与位于源计算实例的VCN外部的端点进行通信。使用与计算实例相关联的VNIC、VCN VR以及与VCN相关联的网关来促进这些通信。

[0174] 对于VCN中同一子网上的两个计算实例之间的通信,使用与源和目的地计算实例相关联的VNIC促进通信。源和目的地计算实例可以由同一主机机器或不同主机机器托管。源自源计算实例的分组可以从托管源计算实例的主机机器转发到连接到该主机机器的NVD。在NVD上,使用分组处理流水线处理分组,这可以包括与源计算实例相关联的VNIC的执行。由于用于分组的目的地端点位于同一子网内,因此与源计算实例相关联的VNIC的执行导致分组被转发到执行与目的地计算实例相关联的VNIC的NVD,然后NVD处理分组并将其转发到目的地计算实例。与源和目的地计算实例相关联的VNIC可以在同一NVD上执行(例如,在源和目的地计算实例两者由同一个主机机器托管的情况下)或在不同NVD上执行(例如,在源和目的地计算实例由连接到不同NVD的不同主机机器托管的情况下)。VNIC可以使用由

NVD存储的路由/转发表来确定分组的下一跳。

[0175] 对于要从子网中的计算实例传送到同一VCN中不同子网中的端点的分组,源自源计算实例的分组从托管源计算实例的主机机器传送到连接到该主机机器的NVD。在NVD上,使用分组处理流水线处理分组,这可以包括一个或多个VNIC以及与VCN相关联的VR的执行。例如,作为分组处理流水线的一部分,NVD执行或调用与和源计算实例相关联的VNIC对应的功能(也称为执行VNIC)。由VNIC执行的功能可以包括查看分组上的VLAN标记。由于分组的目的地在子网外部,因此接下来由NVD调用和执行VCN VR功能。然后,VCN VR将分组路由到执行与目的地计算实例相关联的VNIC的NVD。与目的地计算实例相关联的VNIC然后处理分组并将分组转发到目的地计算实例。与源和目的地计算实例相关联的VNIC可以在同一NVD上执行(例如,在源和目的地计算实例两者由同一主机机器托管的情况下)或在不同NVD上执行(例如,在源和目的地计算实例由连接到不同NVD的不同主机机器托管的情况下)。

[0176] 如果用于分组的目的地在源计算实例的VCN外部,那么源自源计算实例的分组从托管源计算实例的主机机器传送到连接到该主机机器的NVD。NVD执行与源计算实例相关联的VNIC。由于分组的目的地端点在VCN外部,因此分组随后由该VCN的VCN VR处理。NVD调用VCN VR功能,这可能导致分组被转发到执行与VCN相关联的适当网关的NVD。例如,如果目的地是客户的本地部署网络内的端点,那么分组可以由VCN VR转发到执行为VCN配置的DRG网关的NVD。VCN VR可以在与执行与源计算实例相关联的VNIC的NVD相同的NVD上执行,或者由不同的NVD执行。网关可以由NVD执行,NVD可以是smartNIC、主机机器或其它NVD实施方式。然后,分组由网关处理并转发到下一跳,这促进将分组传送到其预期的目的地端点。例如,在图7中描绘的实施例中,源自计算实例768的分组可以通过链路720(使用NIC 732)从主机机器702传送到NVD 710。在NVD 710上,调用VNIC 776,因为它是与源计算实例768相关联的VNIC。VNIC 776被配置为检查分组中封装的信息,并确定用于转发分组的下一跳,目的是促进将分组传送到其预期的目的地端点,然后将分组转发到所确定的下一跳。

[0177] 部署在VCN上的计算实例可以与各种不同端点进行通信。这些端点可以包括由CSPI 700托管的端点和CSPI 700外部的端点。由CSPI 700托管的端点可以包括同一VCN或其它VCN中的实例,这些VCN可以是客户的VCN,或者是不属于客户的VCN。由CSPI 700托管的端点之间的通信可以通过物理网络718执行。计算实例还可以与不由CSPI 700托管的端点或在CSPI 700外部的端点进行通信。这些端点的示例包括客户的本地部署网络或数据中心内的端点,或者通过公共网络(诸如互联网)可访问的公共端点。与CSPI 700外部的端点的通信可以使用各种通信协议通过公共网络(例如,互联网)(图7中未示出)或私有网络(图7中未示出)来执行。

[0178] 图7中描绘的CSPI 700的体系架构仅仅是示例并且不旨在限制。在替代实施例中,变化、替代方案和修改是可能的。例如,在一些实施方式中,CSPI 700可以具有比图7中所示的系统或组件更多或更少的系统或组件,可以组合两个或更多个系统,或者可以具有不同的系统配置或布置。图7中描绘的系统、子系统和其它组件可以在由相应系统的一个或多个处理单元(例如,处理器、核)执行的软件(例如,代码、指令、程序)中实现、使用硬件实现、或根据其组合实现。软件可以存储在非暂态存储介质上(例如,存储器设备上)。

[0179] 图9描绘了根据某些实施例的主机机器和NVD之间的连接,用于提供I/O虚拟化以支持多租赁。如图9中所描绘的,主机机器902执行提供虚拟化环境的管理程序904。主机机

器902执行两个虚拟机实例：属于客户/租户#1的VM1 906和属于客户/租户#2的VM2 908。主机机器902包括经由链路914连接到NVD 912的物理NIC 910。每个计算实例都附接到由NVD 912执行的VNIC。在图9中的实施例中，VM1 906附接到VNIC-VM1 920并且VM2908附接到VNIC-VM2 922。

[0180] 如图9中所示，NIC 910包括两个逻辑NIC：逻辑NIC A 916和逻辑NIC B 918。每个虚拟机附接到其自己的逻辑NIC并被配置为与其自己的逻辑NIC一起工作。例如，VM1 906附接到逻辑NIC A 916并且VM2 908附接到逻辑NIC B 918。虽然主机机器902仅包括由多个租户共享的一个物理NIC 910，但由于逻辑NIC，每个租户的虚拟机都相信他们具有自己的主机机器和NIC。

[0181] 在某些实施例中，每个逻辑NIC被指派有其自己的VLAN ID。因此，特定的VLAN ID被指派给用于租户#1的逻辑NIC A 916，并且分离的VLAN ID被指派给用于租户#2的逻辑NIC B 918。当分组从VM1 906传送时，由管理程序将指派给租户#1的标记(tag)附接到分组，然后分组通过链路914从主机机器902传送到NVD 912。以类似的方式，当分组从VM2 908被传送时，指派给租户#2的标记由管理程序附接到分组，然后分组通过链路914从主机机器902传送到NVD 912。因而，从主机机器902传送到NVD 912的分组924具有识别特定租户和相关联的VM的相关联的标记926。在NVD上，对于从主机机器902接收到的分组924，与该分组相关联的标记926被用于确定分组是由VNIC-VM1 920还是由VNIC-VM2 922处理。分组随后由对应的VNIC处理。图9中描述的配置使每个租户的计算实例能够相信他们拥有其自己的主机机器和NIC。图9中描绘的设置提供了用于支持多租赁的I/O虚拟化。

[0182] 图10描绘了根据某些实施例的物理网络1000的简化框图。图10中描绘的实施例被结构化为Clos网络。Clos网络是特定类型的网络拓扑，其被设计为提供连接冗余性，同时维持高对分带宽和最大资源利用率。Clos网络是无阻塞、多级或多层交换网络的类型，其中级数或层数可以是二、三、四、五等。图10中描绘的实施例是3层网络，包括层1、层2和层3。TOR交换机1004表示Clos网络中的层0交换机。一个或多个NVD连接到TOR交换机。层0交换机也被称为物理网络的边缘设备。层0交换机连接到也称为叶交换机的层1交换机。在图10中描绘的实施例中，“n”个层0TOR交换机的集合连接到“n”个层1交换机的集合并且一起形成群聚(pod)。群聚中的每个层0交换机都互连到该群聚中的所有层1交换机，但群聚之间没有交换机的连接。在某些实施方式中，两个群聚被称为块(block)。每个块由“n”个层2交换机(有时称为主干交换机)的集合提供服务或连接到该交换机的集合。物理网络拓扑中可以存在若干个块。层2交换机进而连接到“n”个层3交换机(有时称为超级主干交换机)。物理网络1000之上的分组的通信通常使用一种或多种层3通信协议来执行。通常，物理网络的所有层(TOR层除外)都是n向冗余的，因此允许高可用性。可以为群聚和块指定策略，以控制交换机在物理网络中彼此的可见性，从而启用物理网络的伸缩(scaling)。

[0183] Clos网络的特征是从一个层0交换机到达另一个层0交换机(或从连接到层0交换机的NVD到达连接到层0交换机的另一个NVD)的最大跳数是固定的。例如，在3层Clos网络中，分组从一个NVD到达另一个NVD最多需要七跳，其中源和目标NVD连接到Clos网络的叶层。同样，在4层Clos网络中，分组从一个NVD到达另一个NVD最多需要九跳，其中源和目标NVD连接到Clos网络的叶层。因此，Clos网络体系架构在整个网络中维持一致的时延，这对于数据中心内部和数据中心之间的通信是重要的。Clos拓扑在水平上伸缩并且具有成本效

益。通过在各个层添加更多交换机(例如,更多叶交换机和骨干交换机)以及通过增加相邻层的交换机之间的链路数量,可以轻松增加网络的带宽/吞吐量容量。

[0184] 在某些实施例中,CSPI内的每个资源都被指派唯一标识符(称为云标识符(CID))。这个标识符作为资源的信息的一部分包括在内并且可以用于(例如经由控制台或通过API)管理资源。

[0185] 用于CID的示例语法是:

[0186] `ocid1.<RESOURCE TYPE><REALM>.[REGION][.FUTURE USE].<UNIQUE ID>`

[0187] 其中,

[0188] `ocid1`:指示CID的版本的文字串;

[0189] `resource type`:资源的类型(例如,实例、卷、VCN、子网、用户、组等);

[0190] `realm`:资源所在的领域。示例值为用于商业领域的“c1”、用于政府云领域的“c2”、或者用于联邦政府云领域的“c3”等。每个领域可以有其自己的域名;

[0191] `region`:资源所在的地区。如果该地区不适用于该资源,那么这个部分可能为空;

[0192] `future use`:保留以备将来使用。

[0193] `unique ID`:ID的唯一部分。格式可以因资源或服务的类型而异。

[0194] 图11是图示根据至少一个实施例的IaaS体系架构的示例模式的框图1100。服务运营商1102可以通信地耦合到可以包括虚拟云网络(VCN)1106和安全主机子网1108的安全主机租赁1104。在一些示例中,服务运营商1102可以使用一个或多个客户端计算设备(客户端计算设备可以是便携式手持设备(例如,**iPhone®**、蜂窝电话、**iPad®**、计算平板、个人数字助理(PDA))或可穿戴设备(例如,Google **Glass®** 头戴式显示器),运行软件(诸如Microsoft Windows **Mobile®**)和/或各种移动操作系统(诸如iOS、Windows Phone、Android、BlackBerry 8、Palm OS等),并且支持互联网、电子邮件、短消息服务(SMS)、**Blackberry®**或其它通信协议。可替代地,客户端计算设备可以是通用个人计算机,包括例如运行各种版本的Microsoft **Windows®**、Apple

[0195] **Macintosh®**和/或Linux操作系统的个人计算机和/或膝上型计算机。客户端计算设备可以是运行各种商业上可获得的**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统(诸如例如Google Chrome OS))中的任何操作系统的工作站计算机。替代地或附加地,客户端计算设备可以是任何其它电子设备,诸如瘦客户端计算机、支持互联网的游戏系统(例如,具有或不具有**Kinect®**手势输入设备的Microsoft Xbox游戏控制台)、和/或能够通过可以访问VCN 1106和/或互联网的网络进行通信的个人消息传递设备。

[0196] VCN 1106可以包括本地对等网关(LPG)1110,该VCN 1106可以经由包含在安全壳(SSH)VCN 1112中的LPG 1110通信地耦合到SSH VCN 1112。SSH VCN 1112可以包括SSH子网1114,并且SSH VCN 1112可以经由包含在控制平面VCN 1116中的LPG 1110通信地耦合到控制平面VCN 1116。此外,SSH VCN 1112可以经由LPG 1110通信地耦合到数据平面VCN 1118。控制平面VCN 1116和数据平面VCN 1118可以包含在可以由IaaS提供商拥有和/或操作的服务租赁1119中。

[0197] 控制平面VCN 1116可以包括充当外围网络(例如,公司内部网络和外部网络之间的公司网络的部分)的控制平面非军事区(DMZ)层1120。基于DMZ的服务器可以承担有限责任并有助于控制安全性违规。此外,DMZ层1120可以包括一个或多个负载平衡器(LB)子网1122、可以包括(一个或多个)应用(app)子网1126的控制平面应用层1124、可以包括(一个或多个)数据库(DB)子网1130(例如,(一个或多个)前端DB子网和/或(一个或多个)后端DB子网)的控制平面数据层1128。包含在控制平面DMZ层1120中的(一个或多个)LB子网1122可以通信地耦合到包含在控制平面应用层1124中的(一个或多个)应用子网1126和可以包含在控制平面VCN 1116中的互联网网关1134,并且(一个或多个)应用子网1126可以通信地耦合到包含在控制平面数据层1128中的(一个或多个)DB子网1130以及服务网关1136和网络地址转换(NAT)网关1138。控制平面VCN 1116可以包括服务网关1136和NAT网关1138。

[0198] 控制平面VCN 1116可以包括数据平面镜像应用层1140,其可以包括(一个或多个)应用子网1126。包含在数据平面镜像应用层1140中的(一个或多个)应用子网1126可以包括可以执行计算实例1144的虚拟网络接口控制器(VNIC) 1142。计算实例1144可以将数据平面镜像应用层1140的(一个或多个)应用子网1126通信地耦合到可以包含在数据平面应用层1146中的(一个或多个)应用子网1126。

[0199] 数据平面VCN 1118可以包括数据平面应用层1146、数据平面DMZ层1148和数据平面数据层1150。数据平面DMZ层1148可以包括(一个或多个)LB子网1122,其可以通信地耦合到数据平面应用层1146的(一个或多个)应用子网1126和数据平面VCN 1118的互联网网关1134。(一个或多个)应用子网1126可以通信地耦合到数据平面VCN 1118的服务网关1136和数据平面VCN 1118的NAT网关1138。数据平面数据层1150还可以包括可以通信地耦合到数据平面应用层1146的(一个或多个)应用子网1126的(一个或多个)DB子网1130。

[0200] 控制平面VCN 1116和数据平面VCN 1118的互联网网关1134可以通信地耦合到元数据管理服务1152,该元数据管理服务1152可以通信地耦合到公共互联网1154。公共互联网1154可以通信地耦合到控制平面VCN 1116和数据平面VCN 1118的NAT网关1138。控制平面VCN 1116和数据平面VCN 1118的服务网关1136可以通信地耦合到云服务1156。

[0201] 在一些示例中,控制平面VCN 1116或数据平面VCN 1118的服务网关1136可以对云服务1156进行应用编程接口(API)调用,而无需通过公共互联网1154。从服务网关1136到云服务1156的API调用可以是单向的:服务网关1136可以对云服务1156进行API调用,并且云服务1156可以将请求的数据发送到服务网关1136。但是,云服务1156可以不发起对服务网关1136的API调用。

[0202] 在一些示例中,安全主机租赁1104可以直接连接到服务租赁1119,服务租赁1119否则可以被隔离。安全主机子网1108可以通过LPG 1110与SSH子网1114通信,LPG 1110可以使得能够在否则隔离的系统上进行双向通信。将安全主机子网1108连接到SSH子网1114可以使安全主机子网1108访问服务租赁1119内的其它实体。

[0203] 控制平面VCN 1116可以允许服务租赁1119的用户设置或以其它方式供给期望资源。在控制平面VCN 1116中供给的期望资源可以在数据平面VCN 1118中部署或以其它方式使用。在一些示例中,控制平面VCN 1116可以与数据平面VCN 1118隔离,并且控制平面VCN 1116的数据平面镜像应用层1140可以经由VNIC 1142与数据平面VCN 1118的数据平面应用层1146通信,VNIC 1142可以包含在数据平面镜像应用层1140和数据平面应用层1146中。

[0204] 在一些示例中,系统的用户或客户可以通过可以将请求传送到元数据管理服务1152的公共互联网1154来做出请求,例如创建、读取、更新或删除(CRUD)操作。元数据管理服务1152可以通过互联网网关1134将请求传送到控制平面VCN 1116。请求可以由包含在控制平面DMZ层1120中的(一个或多个)LB子网1122接收。(一个或多个)LB子网1122可以确定请求是有效的,并且响应于该确定,(一个或多个)LB子网1122可以将请求传输到包含在控制平面应用层1124中的(一个或多个)应用子网1126。如果请求被验证并且需要对公共互联网1154的调用,那么对公共互联网1154的调用可以被传输到可以对公共互联网1154进行调用的NAT网关1138。请求可能期望存储的存储器可以存储在(一个或多个)DB子网1130中。

[0205] 在一些示例中,数据平面镜像应用层1140可以促进控制平面VCN 1116和数据平面VCN 1118之间的直接通信。例如,可能期望对包含在数据平面VCN 1118中的资源应用对配置的更改、更新或其它适当的修改。经由VNIC 1142,控制平面VCN 1116可以直接与包含在数据平面VCN 1118中的资源通信,并且从而可以执行对这些资源的配置的更改、更新或其它适当的修改。

[0206] 在一些实施例中,控制平面VCN 1116和数据平面VCN 1118可以包含在服务租赁1119中。在这种情况下,系统的用户或客户可能不拥有或操作控制平面VCN 1116或数据平面VCN 1118。替代地,IaaS提供商可以拥有或操作控制平面VCN 1116和数据平面VCN 1118,这两种平面都可以包含在服务租赁1119中。该实施例可以使得能够隔离可能阻止用户或客户与其它用户或其它客户的资源进行交互的网络。此外,该实施例可以允许系统的用户或客户私自存储数据库,而无需依赖可能不具有期望威胁防范级别的公共互联网1154以进行存储。

[0207] 在其它实施例中,包含在控制平面VCN 1116中的(一个或多个)LB子网1122可以被配置为从服务网关1136接收信号。在这个实施例中,控制平面VCN 1116和数据平面VCN 1118可以被配置为由IaaS提供商的客户调用而无需调用公共互联网1154。IaaS提供商的客户可能期望这个实施例,因为客户使用的(一个或多个)数据库可以由IaaS提供商控制并且可以存储在服务租赁1119上,服务租赁1119可能与公共互联网1154隔离。

[0208] 图12是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1200。服务运营商1202(例如,图11的服务运营商1102)可以通信地耦合到安全主机租赁1204(例如,图11的安全主机租赁1104),该安全主机租赁1204可以包括虚拟云网络(VCN) 1206(例如,图11的VCN 1106)和安全主机子网1208(例如,图11的安全主机子网1108)。VCN 1206可以包括本地对等网关(LPG) 1210(例如,图11的LPG 1110),该VCN 1206可以经由包含在安全壳(SSH)VCN 1212(例如,图11的SSH VCN 1112)中的LPG 1110通信地耦合到SSH VCN 1212。SSH VCN 1212可以包括SSH子网1214(例如,图11的SSH子网1114),并且SSH VCN 1212可以经由包含在控制平面VCN 1216(例如,图11的控制平面VCN 1116)中的LPG 1210通信地耦合到控制平面VCN 1216。控制平面VCN 1216可以包含在服务租赁1219(例如,图11的服务租赁1119)中,并且数据平面VCN 1218(例如,图11的数据平面VCN 1118)可以包含在可能由系统的用户或客户拥有或操作的客户租赁1221中。

[0209] 控制平面VCN 1216可以包括控制平面DMZ层1220(例如,图11的控制平面DMZ层1120),其可以包括(一个或多个)LB子网1222(例如,图11的(一个或多个)LB子网1122)、可以包括(一个或多个)应用子网1226(例如,图11的(一个或多个)应用子网1126)的控制平面

应用层1224(例如,图11的控制平面应用层1124)、可以包括(一个或多个)数据库(DB)子网1230(例如,类似于图11的(一个或多个)DB子网1130)的控制平面数据层1228(例如,图11的控制平面数据层1128)。包含在控制平面DMZ层1220中的(一个或多个)LB子网1222可以通信地耦合到包含在控制平面应用层1224中的(一个或多个)应用子网1226和可以包含在控制平面VCN 1216中的互联网网关1234(例如,图11的互联网网关1134),并且(一个或多个)应用子网1226可以通信地耦合到包含在控制平面数据层1228中的(一个或多个)DB子网1230以及服务网关1236(例如,图11的服务网关)和网络地址转换(NAT)网关1238(例如,图11的NAT网关1138)。控制平面VCN 1216可以包括服务网关1236和NAT网关1238。

[0210] 控制平面VCN 1216可以包括可以包括(一个或多个)应用子网1226的数据平面镜像应用层1240(例如,图11的数据平面镜像应用层1140)。包含在数据平面镜像应用层1240中的(一个或多个)应用子网1226可以包括可以执行计算实例1244(例如,类似于图11的计算实例1144)的虚拟网络接口控制器(VNIC) 1242(例如,1142的VNIC)。计算实例1244可以促进数据平面镜像应用层1240的(一个或多个)应用子网1226和可以包含在数据平面应用层1246(例如,图11的数据平面应用层1146)中的(一个或多个)应用子网1226之间的经由包含在数据平面镜像应用层1240中的VNIC 1242以及包含在数据平面应用层1246中的VNIC 1242的通信。

[0211] 包含在控制平面VCN 1216中的互联网网关1234可以通信地耦合到元数据管理服务1252(例如,图11的元数据管理服务1152),该元数据管理服务1252可以通信地耦合到公共互联网1254(例如,图11的公共互联网1154)。公共互联网1254可以通信地耦合到包含在控制平面VCN 1216中的NAT网关1238。包含在控制平面VCN 1216中的服务网关1236可以通信地耦合到云服务1256(例如,图11的云服务1156)。

[0212] 在一些示例中,数据平面VCN 1218可以包含在客户租赁1221中。在这种情况下,IaaS提供商可以为每个客户提供控制平面VCN 1216,并且IaaS提供商可以为每个客户设置包含在服务租赁1219中的唯一计算实例1244。每个计算实例1244可以允许包含在服务租赁1219中的控制平面VCN 1216和包含在客户租赁1221中的数据平面VCN 1218之间的通信。计算实例1244可以允许在包含在服务租赁1219中的控制平面VCN 1216中供给的资源被部署或以其它方式用于包含在客户租赁1221中的数据平面VCN 1218中。

[0213] 在其它示例中,IaaS提供商的客户可以具有存在于客户租赁1221中的数据库。在这个示例中,控制平面VCN 1216可以包括数据平面镜像应用层1240,该数据平面镜像应用层1240可以包括(一个或多个)应用子网1226。数据平面镜像应用层1240可以驻留在数据平面VCN 1218中,但数据平面镜像应用层1240可能不存在于数据平面VCN 1218中。换句话说,数据平面镜像应用层1240可以访问客户租赁1221,但是数据平面镜像应用层1240可能不存在于数据平面VCN 1218中或者由IaaS提供商的客户拥有或操作。数据平面镜像应用层1240可以被配置为对数据平面VCN 1218进行调用,但可以被配置为对包含在控制平面VCN 1216中的任何实体进行调用。客户可能期望在数据平面VCN 1218中部署或以其它方式使用在控制平面VCN 1216中供给的资源,并且数据平面镜像应用层1240可以促进客户的期望部署或资源的其它使用。

[0214] 在一些实施例中,IaaS提供商的客户可以将过滤器应用到数据平面VCN 1218。在这个实施例中,客户可以确定数据平面VCN 1218可以访问什么,并且客户可以限制从数据

平面VCN 1218对公共互联网1254的访问。IaaS提供商可能无法应用过滤器或以其它方式控制数据平面VCN 1218对任何外部网络或数据库的访问。客户将过滤器和控制应用到包含在客户租赁1221中的数据平面VCN 1218上可以帮助将数据平面VCN 1218与其它客户和公共互联网1254隔离开。

[0215] 在一些实施例中,云服务1256可以由服务网关1236调用以访问公共互联网1254、控制平面VCN 1216或数据平面VCN 1218上可能不存在的服务。云服务1256与控制平面VCN 1216或数据平面VCN 1218之间的连接可以不是实时的或连续的。云服务1256可以存在于由IaaS提供商拥有或操作的不同网络上。云服务1256可以被配置为接收来自服务网关1236的调用并且可以被配置为不接收来自公共互联网1254的调用。一些云服务1256可以与其它云服务1256隔离,并且控制平面VCN 1216可以与可能与控制平面VCN 1216不在同一区域的云服务1256隔离。例如,控制平面VCN 1216可能位于“区域1”,并且云服务“部署11”可能位于区域1和“区域2”。如果包含在位于区域1中的控制平面VCN 1216中的服务网关1236对部署11进行调用,那么该调用可以被传输到区域1中的部署11。在这个示例中,控制平面VCN 1216或区域1中的部署11可能不与区域2中的部署11通信地耦合或以其它方式通信。

[0216] 图13是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1300。服务运营商1302(例如,图11的服务运营商1102)可以通信地耦合到安全主机租赁1304(例如,图11的安全主机租赁1104),该安全主机租赁1304可以包括虚拟云网络(VCN) 1306(例如,图11的VCN 1106)和安全主机子网1308(例如,图11的安全主机子网1108)。VCN 1306可以包括LPG 1310(例如,图11的LPG 1110),该VCN 1306可以经由包含在SSH VCN 1312(例如,图11的SSH VCN 1112)中的LPG 1310通信地耦合到SSH VCN 1312。SSH VCN 1312可以包括SSH子网1314(例如,图11的SSH子网1114),并且SSH VCN 1312可以经由包含在控制平面VCN 1316(例如,图11的控制平面VCN 1116)中的LPG 1310通信地耦合到控制平面VCN 1316并且经由包含在数据平面VCN 1318(例如,图11的数据平面1118)中的LPG 1310通信地耦合到数据平面VCN 1318。控制平面VCN 1316和数据平面VCN 1318可以包含在服务租赁1319(例如,图11的服务租赁1119)中。

[0217] 控制平面VCN 1316可以包括可以包括(一个或多个)负载平衡器(LB)子网1322(例如,图11的(一个或多个)LB子网1122)的控制平面DMZ层1320(例如,图11的控制平面DMZ层1120)、可以包括(一个或多个)应用子网1326(例如,类似于图11的(一个或多个)应用子网1126)的控制平面应用层1324(例如,图11的控制平面应用层1124)、可以包括(一个或多个)DB子网1330的控制平面数据层1328(例如,图11的控制平面数据层1128)。包含在控制平面DMZ层1320中的(一个或多个)LB子网1322可以通信地耦合到包含在控制平面应用层1324中的(一个或多个)应用子网1326和可以包含在控制平面VCN 1316中的互联网网关1334(例如,图11的互联网网关1134),并且(一个或多个)应用子网1326可以通信地耦合到包含在控制平面数据层1328中的(一个或多个)DB子网1330以及服务网关1336(例如,图11的服务网关)和网络地址转换(NAT)网关1338(例如,图11的NAT网关1138)。控制平面VCN 1316可以包括服务网关1336和NAT网关1338。

[0218] 数据平面VCN 1318可以包括数据平面应用层1346(例如,图11的数据平面应用层1146)、数据平面DMZ层1348(例如,图11的数据平面DMZ层1148)、以及数据平面数据层1350(例如,图11的数据平面数据层1150)。数据平面DMZ层1348可以包括可以通信地耦合到数据

平面应用层1346的(一个或多个)可信应用子网1360和(一个或多个)不可信应用子网1362以及包含在数据平面VCN 1318中的互联网网关1334的(一个或多个)LB子网1322。(一个或多个)可信应用子网1360可以通信地耦合到包含在数据平面VCN 1318中的服务网关1336、包含在数据平面VCN 1318中的NAT网关1338、以及包含在数据平面数据层1350中的(一个或多个)DB子网1330。(一个或多个)不可信应用子网1362可以通信地耦合到包含在数据平面VCN 1318中的服务网关1336和包含在数据平面数据层1350中的(一个或多个)DB子网1330。数据平面数据层1350可以包括可以通信地耦合到包含在数据平面VCN 1318中的服务网关1336的(一个或多个)DB子网1330。

[0219] (一个或多个)不可信应用子网1362可以包括可以通信地耦合到租户虚拟机 (VM) 1366(1) - (N) 的一个或多个主VNIC 1364(1) - (N)。每个租户VM 1366(1) - (N) 可以通信地耦合到可以包含在相应容器出口VCN 1368(1) - (N) 中的相应应用子网1367(1) - (N), 该相应容器出口VCN 1368(1) - (N) 可以包含在相应客户租赁1370(1) - (N) 中。相应辅VNIC 1372(1) - (N) 可以促进包含在数据平面VCN 1318中的(一个或多个)不可信应用子网1362与包含在容器出口VCN 1368(1) - (N) 中的应用子网之间的通信。每个容器出口VCN 1368(1) - (N) 可以包括NAT网关1338, 该NAT网关1338可以通信地耦合到公共互联网1354(例如, 图11的公共互联网1154)。

[0220] 包含在控制平面VCN 1316中以及包含在数据平面VCN 1318中的互联网网关1334可以通信地耦合到元数据管理服务1352(例如, 图11的元数据管理系统1152), 该元数据管理服务1352可以通信地耦合到公共互联网1354。公共互联网1354可以通信地耦合到包含在控制平面VCN 1316中以及包含在数据平面VCN 1318中的NAT网关1338。包含在控制平面VCN 1316中以及包含在数据平面VCN 1318中的服务网关1336可以通信地耦合到云服务1356。

[0221] 在一些实施例中, 数据平面VCN 1318可以与客户租赁1370集成。在一些情况下, 诸如在执行代码时可能期望支持的情况下, 这种集成对于IaaS提供商的客户可能是有用的或期望的。客户可能提供可能具有破坏性、可能与其它客户资源通信或可能以其它方式导致非期望效果的代码来运行。作为对此的响应, IaaS提供商可以确定是否运行由客户给予IaaS提供商的代码。

[0222] 在一些示例中, IaaS提供商的客户可以向IaaS提供商授予临时网络访问, 并请求附加到数据平面应用1346的功能。运行该功能的代码可以在VM 1366(1) - (N) 中执行, 并且该代码可以不被配置为在数据平面VCN 1318上的其它任何地方运行。每个VM 1366(1) - (N) 可以连接到一个客户租赁1370。包含在VM 1366(1) - (N) 中的相应容器1371(1) - (N) 可以被配置为运行代码。在这种情况下, 可以存在双重隔离(例如, 容器1371(1) - (N) 运行代码, 其中容器1371(1) - (N) 可能至少包含在(一个或多个)不可信应用子网1362中所包含的VM 1366(1) - (N) 中), 这可以帮助防止不正确的或以其它方式非期望的代码损坏IaaS提供商的网络或损坏不同客户的网络。容器1371(1) - (N) 可以通信地耦合到客户租赁1370并且可以被配置为传输或接收来自客户租赁1370的数据。容器1371(1) - (N) 可以不被配置为从数据平面VCN 1318中的任何其它实体传输或接收数据。在运行代码完成后, IaaS提供商可以终止或以其它方式处置容器1371(1) - (N)。

[0223] 在一些实施例中, (一个或多个)可信应用子网1360可以运行可以由IaaS提供商拥有或操作的代码。在这个实施例中, (一个或多个)可信应用子网1360可以通信地耦合到(一

个或多个)DB子网1330并且被配置为在(一个或多个)DB子网1330中执行CRUD操作。(一个或多个)不可信应用子网1362可以通信地耦合到(一个或多个)DB子网1330,但是在这个实施例中,(一个或多个)不可信应用子网可以被配置为在(一个或多个)DB子网1330中执行读取操作。可以包含在每个客户的VM 1366(1)-(N)中并且可以运行来自客户的代码的容器1371(1)-(N)可以不与(一个或多个)DB子网1330通信地耦合。

[0224] 在其它实施例中,控制平面VCN 1316和数据平面VCN 1318可以不直接通信地耦合。在这个实施例中,控制平面VCN 1316和数据平面VCN 1318之间可能不存在直接通信。但是,通信可以通过至少一个方法而间接地发生。LPG 1310可以由IaaS提供商建立,其可以促进控制平面VCN 1316和数据平面VCN 1318之间的通信。在另一个示例中,控制平面VCN 1316或数据平面VCN 1318可以经由服务网关1336对云服务1356进行调用。例如,从控制平面VCN 1316对云服务1356的调用可以包括对可以与数据平面VCN 1318通信的服务的请求。

[0225] 图14是图示根据至少一个实施例的IaaS体系架构的另一个示例模式的框图1400。服务运营商1402(例如,图11的服务运营商1102)可以通信地耦合到安全主机租赁1404(例如,图11的安全主机租赁1104),该安全主机租赁1404可以包括虚拟云网络(VCN)1406(例如,图11的VCN 1106)和安全主机子网1408(例如,图11的安全主机子网1108)。VCN 1406可以包括LPG 1410(例如,图11的LPG 1110),该VCN 1406可以经由包含在SSH VCN 1412(例如,图11的SSH VCN 1112)中的LPG 1410通信地耦合到SSH VCN 1412。SSH VCN 1412可以包括SSH子网1414(例如,图11的SSH子网1114),并且SSH VCN 1412可以经由包含在控制平面VCN 1416(例如,图11的控制平面VCN 1116)中的LPG 1410通信地耦合到控制平面VCN 1416并且经由包含在数据平面VCN 1418(例如,图11的数据平面1118)中的LPG 1410通信地耦合到数据平面VCN 1418。控制平面VCN 1416和数据平面VCN 1418可以包含在服务租赁1419(例如,图11的服务租赁1119)中。

[0226] 控制平面VCN 1416可以包括可以包括(一个或多个)LB子网1422(例如,图11的(一个或多个)LB子网1122)的控制平面DMZ层1420(例如,图11的控制平面DMZ层1120)、可以包括(一个或多个)应用子网1426(例如,图11的(一个或多个)应用子网1126)的控制平面应用层1424(例如,图11的控制平面应用层1124)、可以包括(一个或多个)DB子网1430(例如,图13的(一个或多个)DB子网1330)的控制平面数据层1428(例如,图11的控制平面数据层1128)。包含在控制平面DMZ层1420中的(一个或多个)LB子网1422可以通信地耦合到包含在控制平面应用层1424中的(一个或多个)应用子网1426和可以包含在控制平面VCN 1416中的互联网网关1434(例如,图11的互联网网关1134),并且(一个或多个)应用子网1426可以通信地耦合到包含在控制平面数据层1428中的(一个或多个)DB子网1430以及服务网关1436(例如,图11的服务网关)和网络地址转换(NAT)网关1438(例如,图11的NAT网关1138)。控制平面VCN 1416可以包括服务网关1436和NAT网关1438。

[0227] 数据平面VCN 1418可以包括数据平面应用层1446(例如,图11的数据平面应用层1146)、数据平面DMZ层1448(例如,图11的数据平面DMZ层1148)、以及数据平面数据层1450(例如,图11的数据平面数据层1150)。数据平面DMZ层1448可以包括可以通信地耦合到数据平面应用层1446的(一个或多个)可信应用子网1460(例如,图13的(一个或多个)可信应用子网1360)和(一个或多个)不可信应用子网1462(例如,图13的(一个或多个)不可信应用子网1362)以及包含在数据平面VCN 1418中的互联网网关1434的(一个或多个)LB子网1422。

(一个或多个)可信应用子网1460可以通信地耦合到包含在数据平面VCN 1418中的服务网关1436、包含在数据平面VCN 1418中的NAT网关1438以及包含在数据平面数据层1450中的(一个或多个)DB子网1430。(一个或多个)不可信应用子网1462可以通信地耦合到包含在数据平面VCN 1418中的服务网关1436和包含在数据平面数据层1450中的(一个或多个)DB子网1430。数据平面数据层1450可以包括可以通信地耦合到包含在数据平面VCN 1418中的服务网关1436的(一个或多个)DB子网1430。

[0228] (一个或多个)不可信应用子网1462可以包括可以通信地耦合到驻留在(一个或多个)不可信应用子网1462内的租户虚拟机 (VM) 1466 (1) - (N) 的主VNIC 1464 (1) - (N)。每个租户VM 1466 (1) - (N) 可以运行相应容器1467 (1) - (N) 中的代码,并且通信地耦合到可以包含在数据平面应用层1446中的应用子网1426,该数据平面应用层1446可以包含在容器出口VCN 1468中。相应辅VNIC 1472 (1) - (N) 可以促进包含在数据平面VCN 1418中的(一个或多个)不可信应用子网1462和包含在容器出口VCN 1468中的应用子网之间的通信。容器出口VCN可以包括可以通信地耦合到公共互联网1454 (例如,图11的公共互联网1154) 的NAT网关1438。

[0229] 包含在控制平面VCN 1416中以及包含在数据平面VCN 1418中的互联网网关1434可以通信地耦合到元数据管理服务1452 (例如,图11的元数据管理系统1152),该元数据管理服务1452可以通信地耦合到公共互联网1454。公共互联网1454可以通信地耦合到包含在控制平面VCN 1416中以及包含在数据平面VCN 1418中的NAT网关1438。包含在控制平面VCN 1416中以及包含在数据平面VCN 1418中的服务网关1436可以通信地耦合到云服务1456。

[0230] 在一些示例中,图14的框图1400的体系架构所示的模式可以被认为是图13的框图1300的体系架构所示的模式例外,并且在IaaS提供商不能直接与客户通信 (例如,断开连接的区域) 的情况下,这可能是IaaS提供商的客户所期望的。客户可以实时访问每个客户的包含在VM 1466 (1) - (N) 中的相应容器1467 (1) - (N)。容器1467 (1) - (N) 可以被配置为对包含在数据平面应用层1446的(一个或多个)应用子网1426中的相应辅VNIC 1472 (1) - (N) 进行调用,该数据平面应用层1446可以包含在容器出口VCN 1468中。辅VNIC 1472 (1) - (N) 可以将调用传输到NAT网关1438,该NAT网关1438可以将调用传输到公共互联网1454。在这个示例中,可以由客户实时访问的容器1467 (1) - (N) 可以与控制平面VCN 1416隔离,并且可以与包含在数据平面VCN 1418中的其它实体隔离。容器1467 (1) - (N) 也可以与来自其它客户的资源隔离。

[0231] 在其它示例中,客户可以使用容器1467 (1) - (N) 来调用云服务1456。在这个示例中,客户可以运行容器1467 (1) - (N) 中的从云服务1456请求服务的代码。容器1467 (1) - (N) 可以将该请求传输到辅VNIC 1472 (1) - (N),该辅VNIC 1472 (1) - (N) 可以将请求传输到NAT网关,该NAT网关可以将请求传输到公共互联网1454。公共互联网1454可以经由互联网网关1434将请求传输到包含在控制平面VCN 1416中的(一个或多个)LB子网1422。响应于确定请求有效,(一个或多个)LB子网可以将请求传输到(一个或多个)应用子网1426,该(一个或多个)应用子网1426可以经由服务网关1436将请求传输到云服务1456。

[0232] 应当认识到的是,各图中描绘的IaaS体系架构1100、1200、1300、1400可以具有除所描绘的组件之外的其它组件。另外,各图中所示的实施例仅仅是可以结合本公开的实施例的云基础设施系统的一些示例。在一些其它实施例中,IaaS系统可以具有比各图中所示

更多或更少的组件、可以组合两个或更多个组件、或者可以具有不同的组件布置或配置。

[0233] 在某些实施例中,本文描述的IaaS系统可以包括以自助服务、基于订阅、弹性可伸缩、可靠、高度可用和安全的方式交付给客户的应用套件、中间件和数据库服务产品。此类IaaS系统的示例是本受让方提供的Oracle云基础设施(OCI)。

[0234] 图15图示了其中可以实现各种实施例的示例计算机系统1500。系统1500可以用于实现上述任何计算机系统。如图所示,计算机系统1500包括经由总线子系统1502与多个外围子系统通信的处理单元1504。这些外围子系统可以包括处理加速单元1506、I/O子系统1508、存储子系统1518和通信子系统1524。存储子系统1518包括有形计算机可读存储介质1522和系统存储器1510。

[0235] 总线子系统1502提供用于让计算机系统1500的各种组件和子系统按意图彼此通信的机制。虽然总线子系统1502被示意性地示出为单条总线,但是总线子系统的替代实施例可以利用多条总线。总线子系统1502可以是若干种类型的总线结构中的任何一种,包括存储器总线或存储器控制器、外围总线、以及使用任何各种总线体系架构的局部总线。例如,这种体系架构可以包括工业标准体系架构(ISA)总线、微通道体系架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围组件互连(PCI)总线,其可以被实现为按IEEE P1386.1标准制造的Mezzanine总线。

[0236] 可以被实现为一个或多个集成电路(例如,常规微处理器或微控制器)的处理单元1504控制计算机系统1500的操作。一个或多个处理器可以被包括在处理单元1504中。这些处理器可以包括单核或多核处理器。在某些实施例中,处理单元1504可以被实现为一个或多个独立的处理单元1532和/或1534,其中在每个处理单元中包括单核或多核处理器。在其它实施例中,处理单元1504也可以被实现为通过将两个双核处理器集成到单个芯片中形成的四核处理单元。

[0237] 在各种实施例中,处理单元1504可以响应于程序代码执行各种程序并且可以维护多个并发执行的程序或进程。在任何给定的时间,要执行的程序代码中的一些或全部代码可以驻留在(一个或多个)处理器1504中和/或存储子系统1518中。通过适当的编程,(一个或多个)处理器1504可以提供上述各种功能。计算机系统1500可以附加地包括处理加速单元1506,其可以包括数字信号处理器(DSP)、专用处理器,等等。

[0238] I/O子系统1508可以包括用户接口输入设备和用户接口输出设备。用户接口输入设备可以包括键盘、诸如鼠标或轨迹球的定点设备、结合到显示器中的触摸板或触摸屏、滚动轮、点击轮、拨盘、按钮、开关、键盘、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备可以包括例如运动感测和/或手势识别设备,诸如Microsoft **Kinect®**运动传感器,其使得用户能够使用手势和语音命令通过自然用户接口来控制诸如Microsoft **Xbox®**360游戏控制器的输入设备并与之交互。用户接口输入设备也可以包括眼睛姿势识别设备,诸如从用户检测眼睛活动(例如,当拍摄照片和/或做出菜单选择时的“眨眼”)并且将眼睛姿势转换为去往输入设备(例如,Google **Glass®**)的输入的Google **Glass®**眨眼检测器。此外,用户接口输入设备可以包括使用户能够通过语音命令与语音识别系统(例如,**Siri®**导航器)交互的语音识别感测设备。

[0239] 用户接口输入设备也可以包括但不限于三维(3D)鼠标、操纵杆或指向棒、游戏面

板和绘图板、以及音频/视频设备,诸如扬声器、数码相机、数码摄录机、便携式媒体播放器、网络摄像头、图像扫描仪、指纹扫描仪、条形码阅读器3D扫描仪、3D打印机、激光测距仪和视线跟踪设备。此外,用户接口输入设备可以包括例如医学成像输入设备,诸如计算机断层扫描、磁共振成像、正电子发射断层摄影术、医疗超声设备。用户接口输入设备也可以包括例如音频输入设备,诸如MIDI键盘、数字乐器等。

[0240] 用户接口输出设备可以包括显示子系统、指示灯,或者诸如音频输出设备的非可视显示器等。显示子系统可以是阴极射线管(CRT)、诸如使用液晶显示器(LCD)或等离子显示器的平板设备、投影设备、触摸屏等。一般而言,术语“输出设备”的使用意在包括用于从计算机系统1500向用户或其它计算机输出信息的所有可能类型的设备和机制。例如,用户接口输出设备可以包括但不限于可视地传达文本、图形和音频/视频信息的各种显示设备,诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备、以及调制解调器。

[0241] 计算机系统1500可以包括包含软件元件、被示为当前位于系统存储器1510内的存储子系统1518。系统存储器1510可以存储在处理单元1504上可执行且可加载的程序指令,以及在这些程序的执行期间所产生的数据。

[0242] 取决于计算机系统1500的配置和类型,系统存储器1510可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存存储器等)。RAM通常包含可被处理单元1504立即访问和/或目前正被处理单元1504操作和执行的数据和/或程序模块。在一些实施方案中,系统存储器1510可以包括多种不同类型的存储器,诸如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。在一些实施方案中,包含有助于在诸如启动期间在计算机系统1500内的元件之间传送信息的基本例程的基本输入/输出系统(BIOS)通常可以被存储在ROM中。作为示例而非限制,系统存储器1510也示出了可以包括客户端应用、Web浏览器、中间层应用、关系数据库管理系统(RDBMS)等的应用程序1512、程序数据1514、以及操作系统1516。作为示例,操作系统1516可以包括各种版本的Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种可商业获得的 **UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux操作系统、Google **Chrome®** OS等)和/或诸如iOS、**Windows®** Phone、**Android®** OS、**BlackBerry®** 10S和**Palm®** OS操作系统的移动操作系统。

[0243] 存储子系统1518也可以提供用于存储提供一些实施例的功能的基本编程和数据构造的有形计算机可读存储介质。当被处理器执行时提供上述功能的软件(程序、代码模块、指令)可以被存储在存储子系统1518中。这些软件模块或指令可以被处理单元1504执行。存储子系统1518也可以提供用于存储根据本公开使用的数据的储存库。

[0244] 存储子系统1500也可以包括可被进一步连接到计算机可读存储介质1522的计算机可读存储介质读取器1520。与系统存储器1510一起,并且可选地与其相结合,计算机可读存储介质1522可以全面地表示用于临时和/或更持久地包含、存储、传输和检索计算机可读信息的远程、本地、固定和/或可移除的存储设备加存储介质。

[0245] 包含代码或代码的部分的计算机可读存储介质1522也可以包括本领域已知或使用的任何适当的介质,包括存储介质和通信介质,诸如但不限于:以用于信息的存储和/或

传输的任何方法或技术实现的易失性和非易失性、可移除和不可移除的介质。这可以包括有形的计算机可读存储介质,诸如RAM、ROM、电可擦除可编程ROM(EEPROM)、闪存存储器或其它存储器技术、CD-ROM、数字多功能盘(DVD)或其它光学存储装置、磁带盒、磁带、磁盘存储装置或其它磁存储设备、或者其它有形的计算机可读介质。这也可以包括非有形的计算机可读介质,诸如数据信号、数据传输、或者可以用于传输期望信息并且可以被计算机系统1500访问的任何其它介质。

[0246] 举例来说,计算机可读存储介质1522可以包括从不可移除的非易失性磁介质读取或写到其的硬盘驱动器、从可移除的非易失性磁盘读取或写到其的磁盘驱动器、以及从可移除的非易失性光盘(诸如CD ROM、DVD和 **Blu-Ray®**盘或其它光学介质)读取或写到其的光盘驱动器。计算机可读存储介质1522可以包括但不限于:**Zip®**驱动器、闪存卡、通用串行总线(USB)闪存驱动器、安全数字(SD)卡、DVD盘、数字视频带等。计算机可读存储介质1522也可以包括基于非易失性存储器的固态驱动器(SSD)(诸如基于闪存存储器的SSD、企业闪存驱动器、固态ROM等)、基于易失性存储器的SSD(诸如基于固态RAM、动态RAM、静态RAM、DRAM的SSD)、磁阻RAM(MRAM) SSD、以及使用基于DRAM的SSD和基于闪存存储器的SSD的组合的混合SSD。盘驱动器及其关联的计算机可读介质可以为计算机系统1500提供计算机可读指令、数据结构、程序模块及其它数据的非易失性存储。

[0247] 通信子系统1524提供到其它计算机系统和网络的接口。通信子系统1524用作用于从其它系统接收数据和从计算机系统1500向其它系统传输数据的接口。例如,通信子系统1524可以使计算机系统1500能够经由互联网连接到一个或多个设备。在一些实施例中,通信子系统1524可以包括用于访问无线语音和/或数据网络的射频(RF)收发器组件(例如,使用蜂窝电话技术、诸如3G、4G或EDGE(用于全球演进的增强型数据速率)的先进数据网络技术、WiFi(IEEE 802.11系列标准)、或其它移动通信技术、或其任何组合)、全球定位系统(GPS)接收器组件和/或其它组件。在一些实施例中,通信子系统1524可以提供有线网络连接(例如,以太网),作为无线接口的附加或者替代。

[0248] 在一些实施例中,通信子系统1524也可以代表可以使用计算机系统1500的一个或多个用户接收结构化和/或非结构化的数据馈送1526、事件流1528、事件更新1530等形式的输入通信。

[0249] 举例来说,通信子系统1524可以被配置为实时地从社交网络和/或其它通信服务的用户接收数据馈送1526,诸如**Twitter®**馈送、**Facebook®**更新、诸如丰富站点摘要(RSS)馈送的web馈送和/或来自一个或多个第三方信息源的实时更新。

[0250] 此外,通信子系统1524也可以被配置为接收连续数据流形式的数据,这可以包括本质上可以是连续的或无界的没有明确终止的实时事件的事件流1528和/或事件更新1530。生成连续数据的应用的示例可以包括例如传感器数据应用、金融报价机、网络性能测量工具(例如,网络监视和流量管理应用)、点击流分析工具、汽车流量监视等。

[0251] 通信子系统1524也可以被配置为向一个或多个数据库输出结构化和/或非结构化的数据馈送1526、事件流1528、事件更新1530等,该一个或多个数据库可以与耦合到计算机系统1500的一个或多个流式传输数据源计算机进行通信。

[0252] 计算机系统1500可以是各种类型之一,包括手持便携式设备(例如, **iPhone®**蜂

窝电话、iPad®计算平板电脑、PDA)、可穿戴设备(例如,Google Glass®头戴式显示器)、PC、工作站、大型机、信息站、服务器机架、或任何其它数据处理系统。

[0253] 由于计算机和网络的不断变化的性质,图中描绘的计算机系统1500的描述仅旨在作为具体示例。具有比图中描绘的系统更多或更少组件的许多其它配置是可能的。例如,也可以使用定制的硬件和/或可以在硬件、固件、软件(包括小应用程序)或组合中实现特定元素。另外,可以采用与其它计算设备(诸如网络输入/输出设备)的连接。基于本文提供的公开和教导,本领域普通技术人员将认识到实现各种实施例的其它方式和/或方法。

[0254] 实施例可以通过使用计算机程序产品来实现,该计算机程序产品包括计算机程序指令,计算机程序指令在由处理器执行时,使得处理器执行本公开中描述的任何方法。

[0255] 虽然已经描述了具体实施例,但是各种修改、变更、替代构造和等效形式也包含在本公开的范围。实施例不限于在某些特定数据处理环境内操作,而是可以在多个数据处理环境内自由操作。此外,虽然已经使用特定系列的事务和步骤描述了实施例,但是本领域技术人员应该清楚本公开的范围不限于所描述系列的事务和步骤。上述实施例的各种特征和方面可以单独或联合使用。

[0256] 另外,虽然已经使用硬件和软件的特定组合描述了实施例,但是应当认识到硬件和软件的其它组合也在本公开的范围。实施例可以仅用硬件、或仅用软件、或使用它们的组合来实现。本文描述的各种处理可以以任何组合在相同的处理器或在不同的处理器上实现。因而,在组件或模块被描述为被配置为执行某些操作的情况下,可以通过例如设计电子电路来执行操作、通过对可编程电子电路(诸如微处理器)进行编程来执行操作、或通过其任何组合来完成这样的配置。处理可以使用多种技术进行通信,包括但不限于用于进程间通信的常规技术,并且不同的进程对可以使用不同的技术,或者同一进程对可以在不同时间使用不同的技术。

[0257] 因而,说明书和附图被认为是说明性的而不是限制性的意义。但是,在不脱离权利要求中阐述的更广泛的精神和范围的情况下,显然可以对其进行添加、减少、删除和其它修改和改变。因此,虽然已经描述了具体的公开实施例,但这些并不旨在进行限制。各种修改和等效形式都在以下权利要求的范围内。

[0258] 在描述所公开的实施例的上下文中(尤其在以下权利要求的上下文中)使用术语“一”和“一个”和“该”以及类似的指称应被解释为涵盖单数和复数两者,除非本文另有指示或与上下文明显矛盾。除非另有说明,否则术语“包括”、“具有”、“包含”和“含有”应被解释为开放式术语(即,意思是“包括但不限于”)。术语“连接”应被解释为部分或全部包含在内、附接到或连接在一起,即使中间存在一些东西。除非本文另有指示,否则本文中的值范围的描述仅旨在用作单独引用落入该范围内的每个单独值的简略方法,并且每个单独值被并入说明书中,就好像它在本文中单独描述一样。除非本文另有指示或与上下文明显矛盾,否则本文描述的所有方法都可以以任何合适的顺序执行。除非另有声明,否则本文提供的任何和全部示例或示例性语言(例如,“诸如”)的使用仅旨在更好地阐明实施例并且不对本公开的范围构成限制。说明书中的任何语言都不应被解释为指示任何未要求保护的元素对于本公开的实践是必不可少的。

[0259] 除非另有明确说明,否则析取(disjunctive)语言(诸如短语“X、Y或Z中的至少一个”)旨在在上下文中被理解为用作一般地表示项目、术语等可以是X、Y或Z中的一者或者是

它们的任何组合(例如,X、Y和/或Z)。因此,这种析取语言通常不旨在也不应暗示某些实施例需要X中的至少一个、Y中的至少一个或Z中的至少一个各自存在。

[0260] 本文描述了本公开的优选实施例,包括已知用于实施本公开的最佳模式。这些优选实施例的变型对于本领域普通技术人员在阅读前述描述后会变得显而易见。普通技术人员应该能够适当地采用这样的变型并且可以以不同于本文具体描述的方式来实践本公开。因而,本公开包括在适用法律允许的情况下对所附权利要求中记载的主题的所有修改和等效形式。此外,除非在本文中另有指示,否则本公开包括上述元素在其所有可能的变型中的任何组合。

[0261] 本文引用的所有参考文献(包括出版物、专利申请和专利)均以相同的程度通过引用并入本文,就好像指示每个参考文献单独且具体地通过引用并入并且在本文中全文阐述一样。

[0262] 在前述的说明书中,本公开的各方面参考其具体实施例进行了描述,但本领域技术人员将认识到的是,本公开不限于此。上述公开的各个特征和方面可以被单独或联合使用。此外,在不脱离本说明书的更广泛精神和范围的情况下,实施例可以在除本文所述的环境和应用之外的任何数量的环境和应用中被使用。因而,本说明书和附图应当被认为是说明性而不是限制性的。

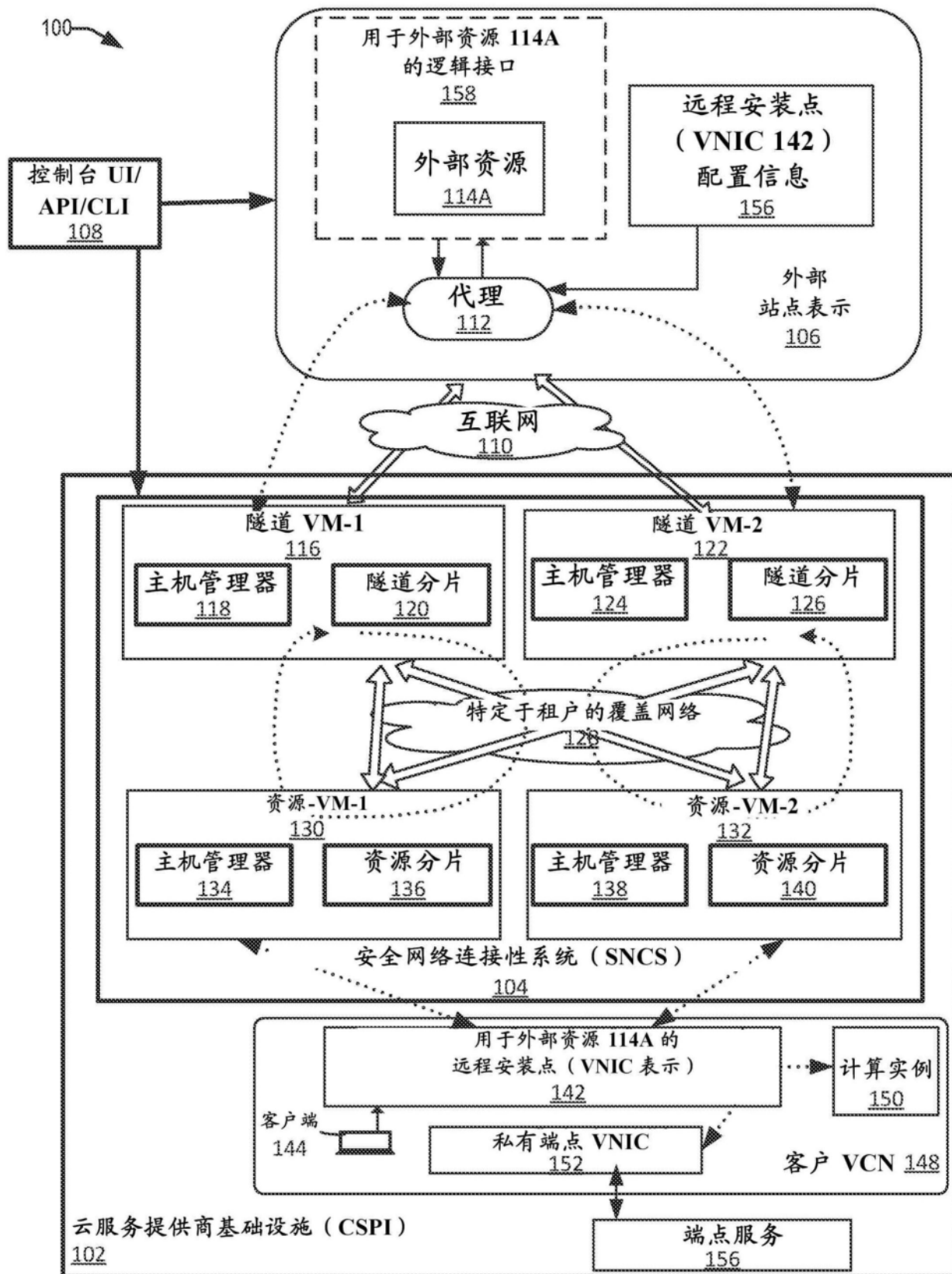


图1

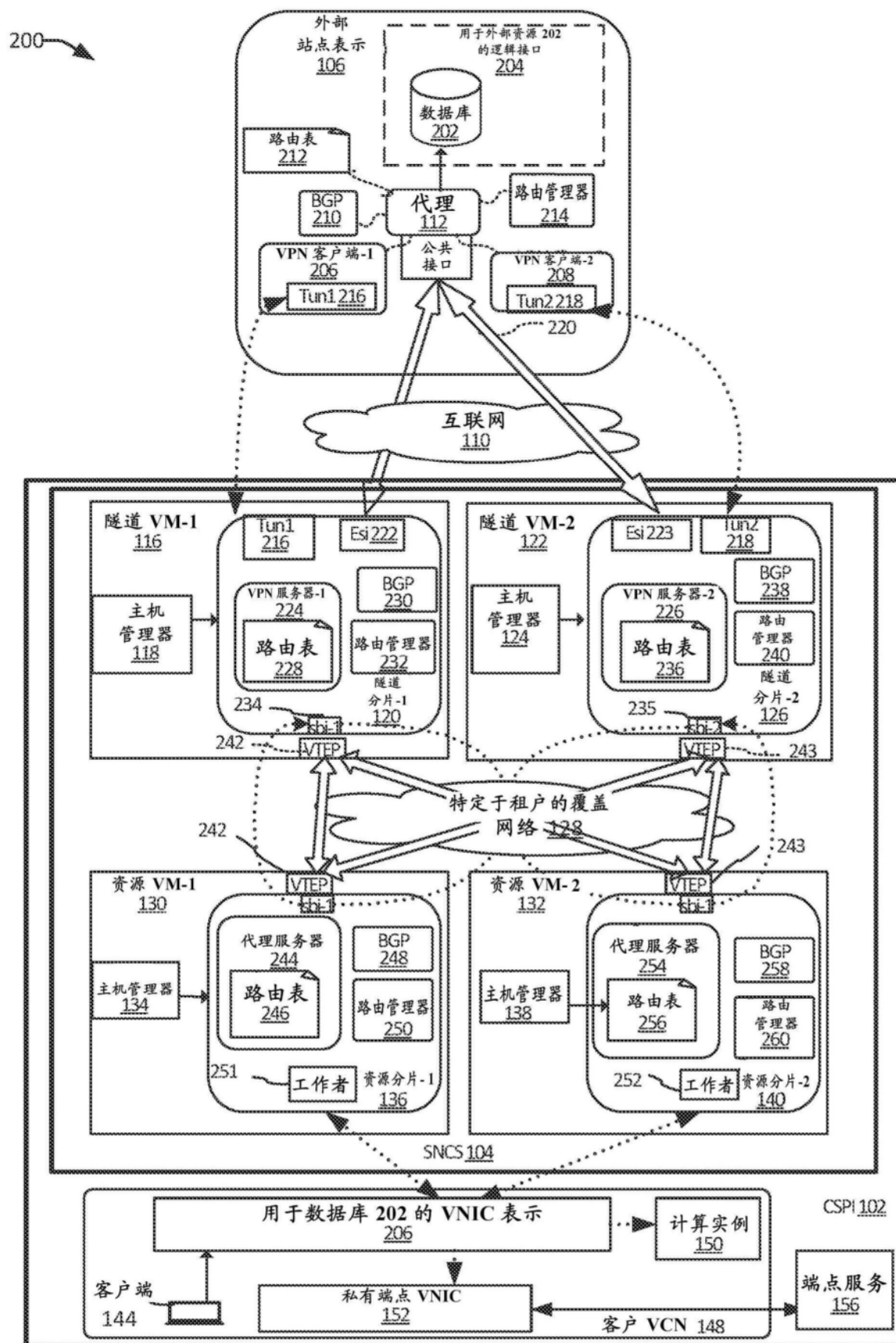


图2

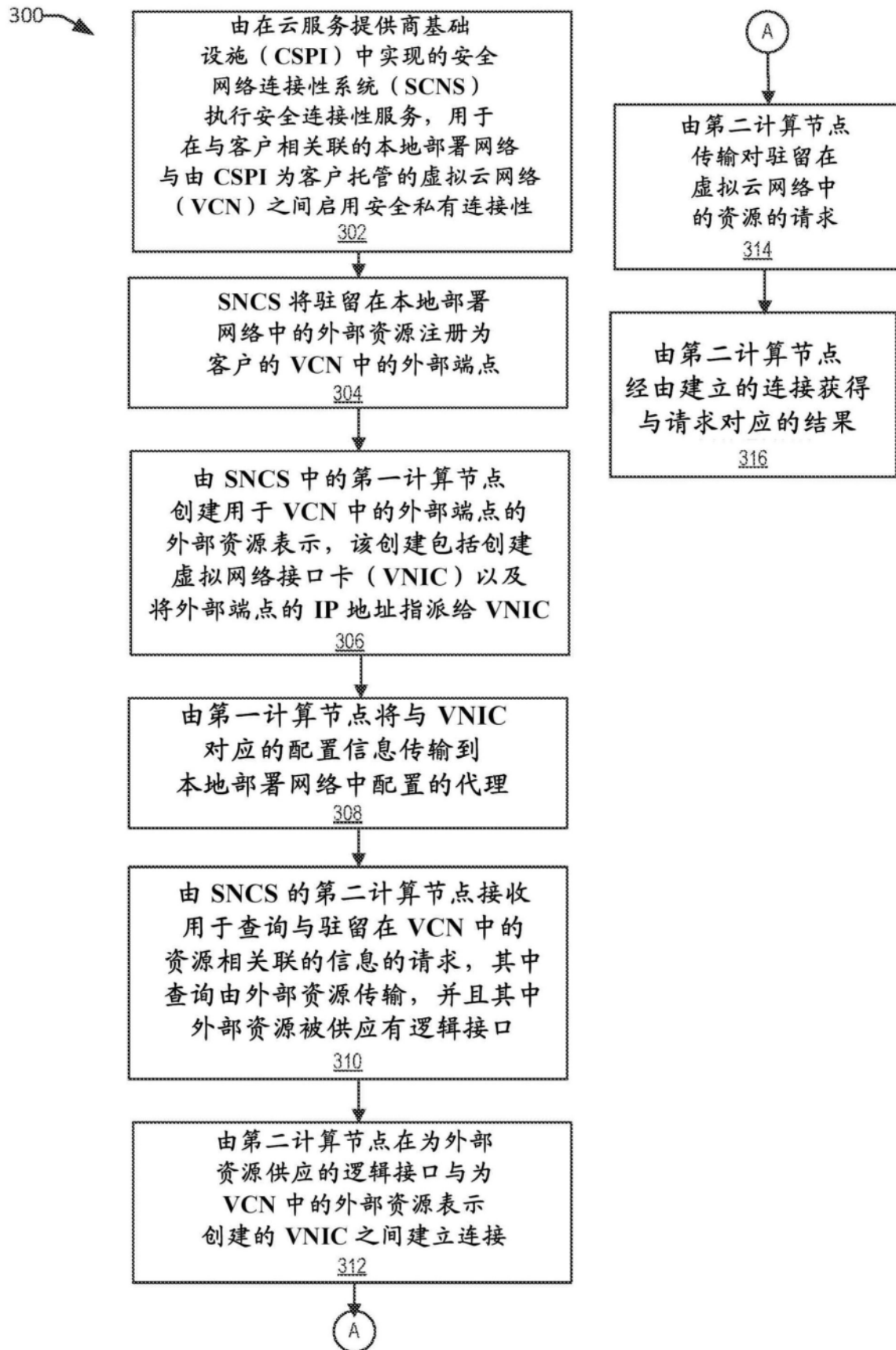


图3

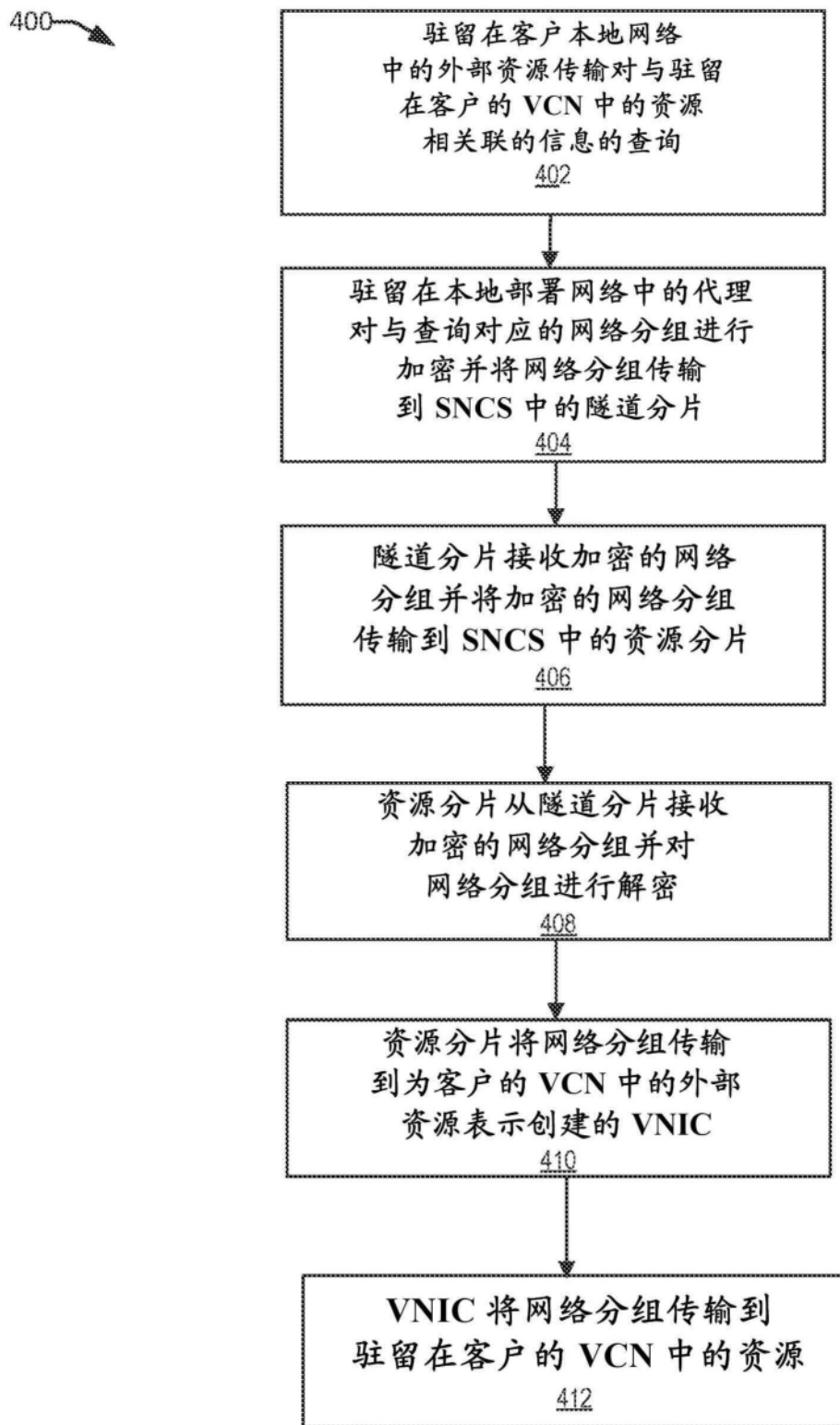


图4

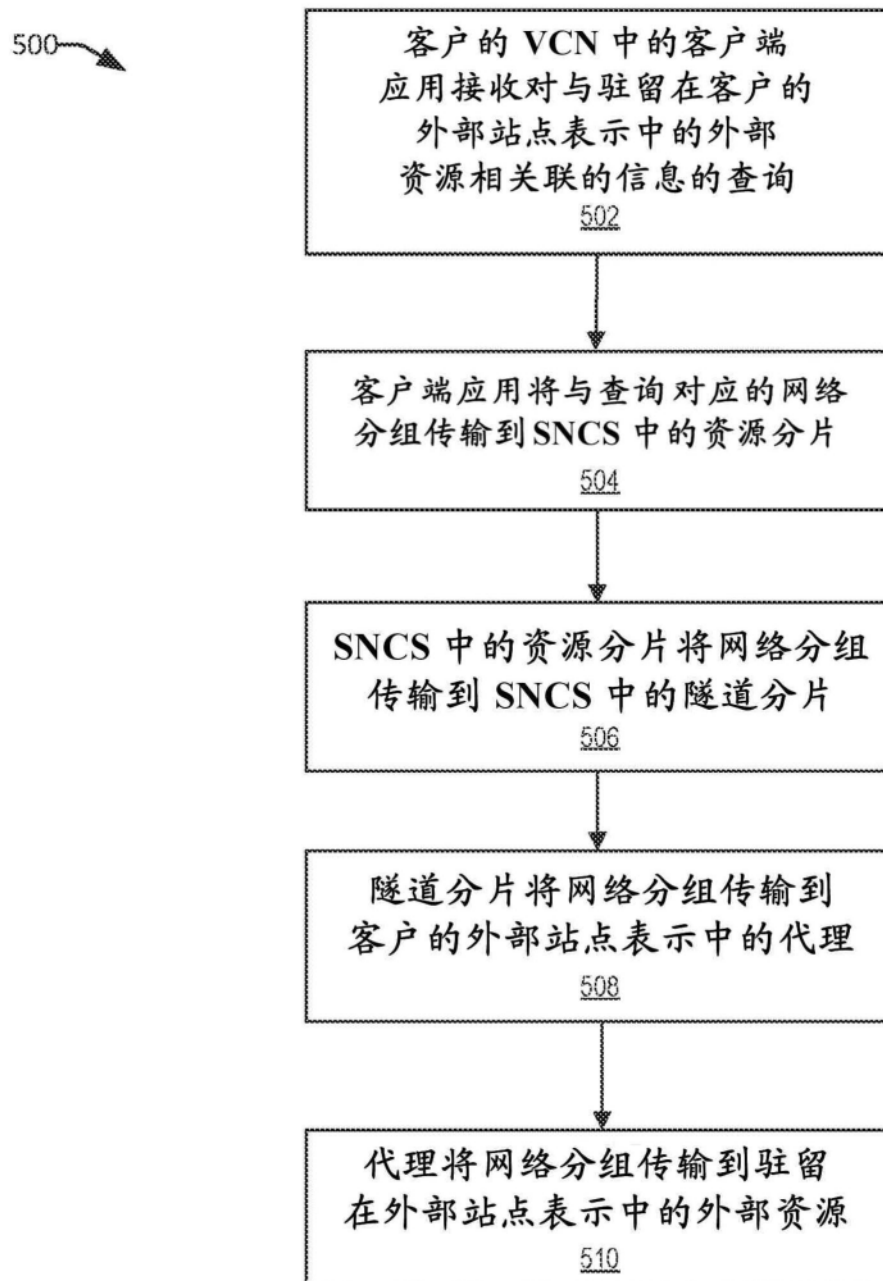


图5

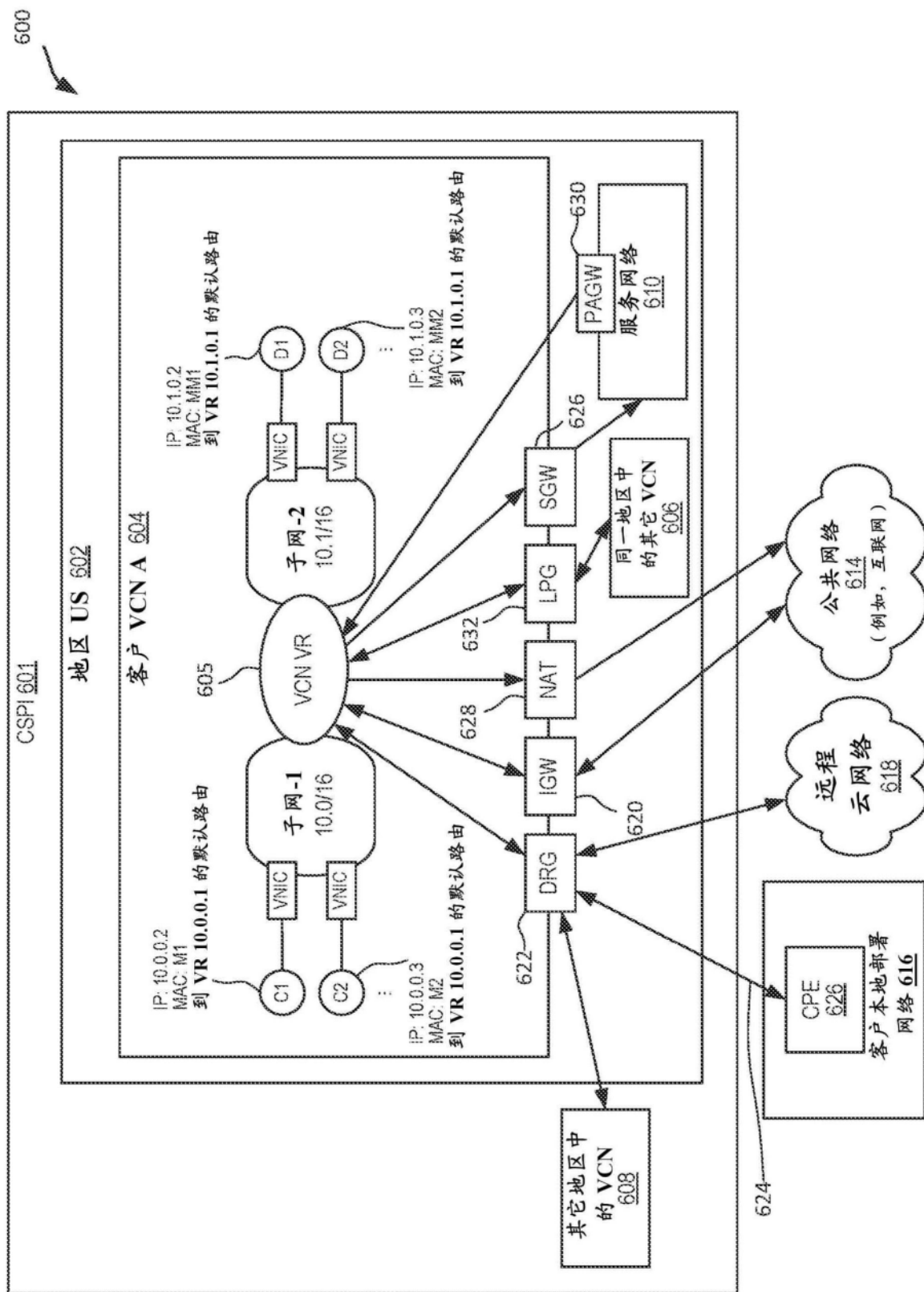


图6

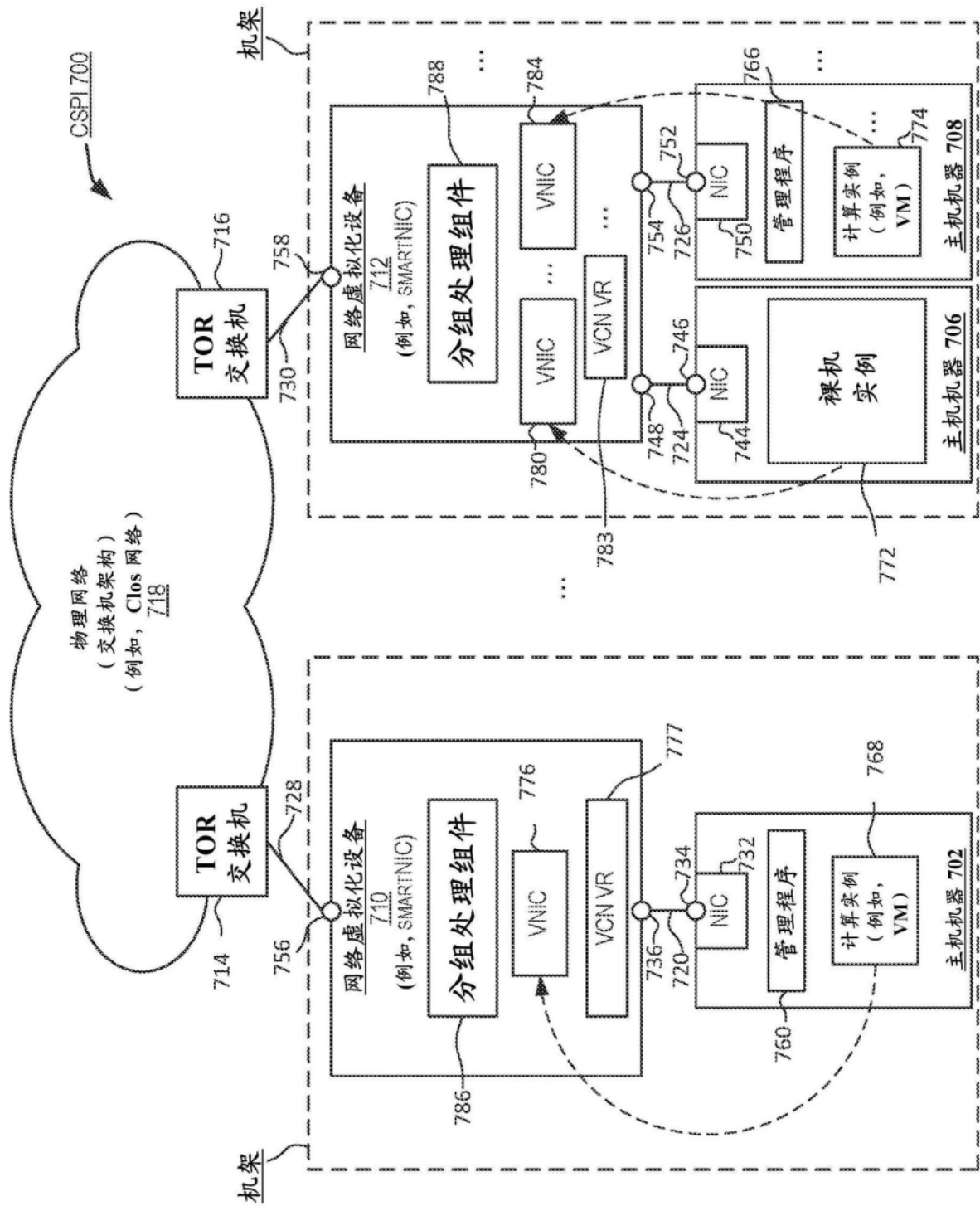


图7

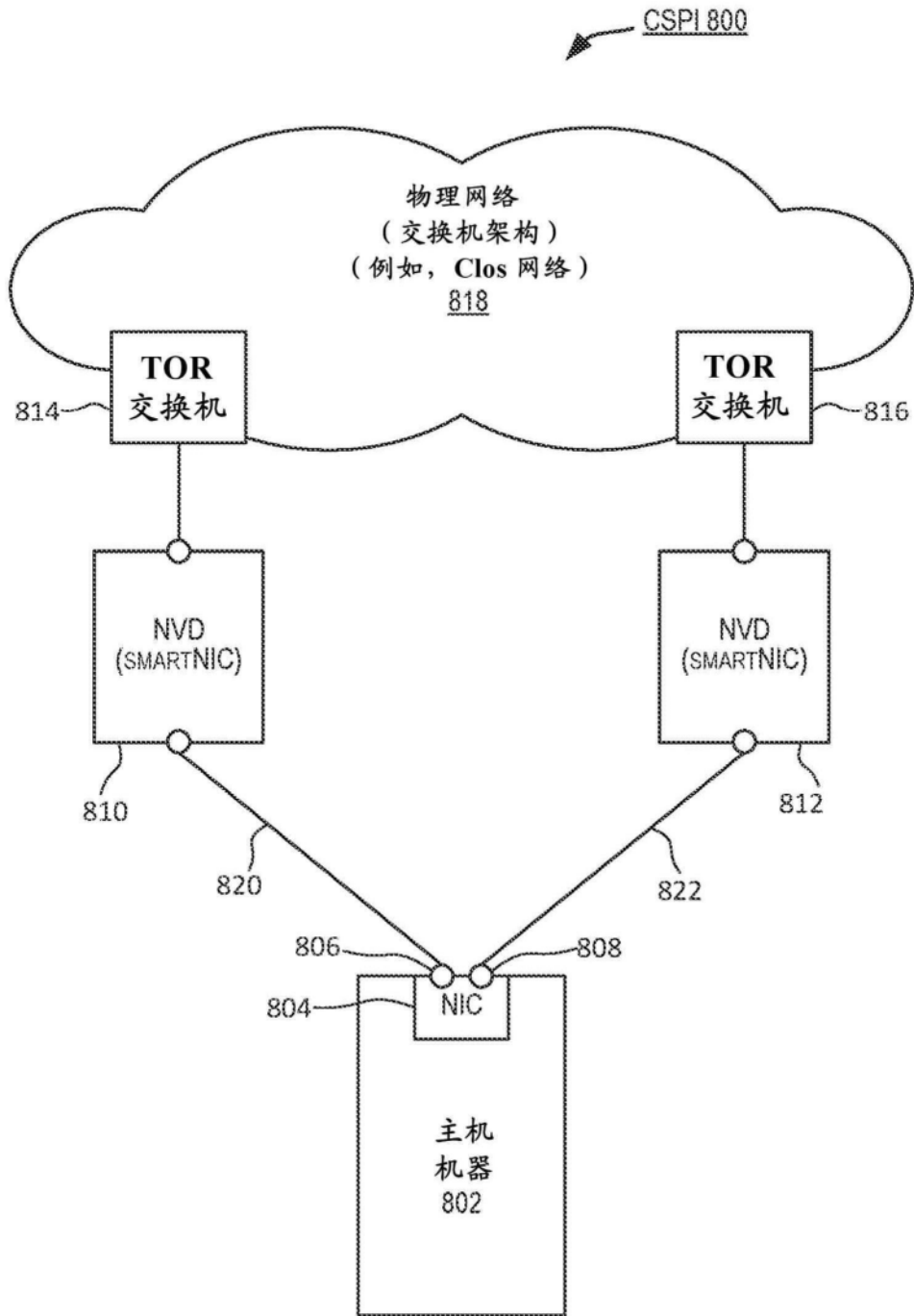


图8

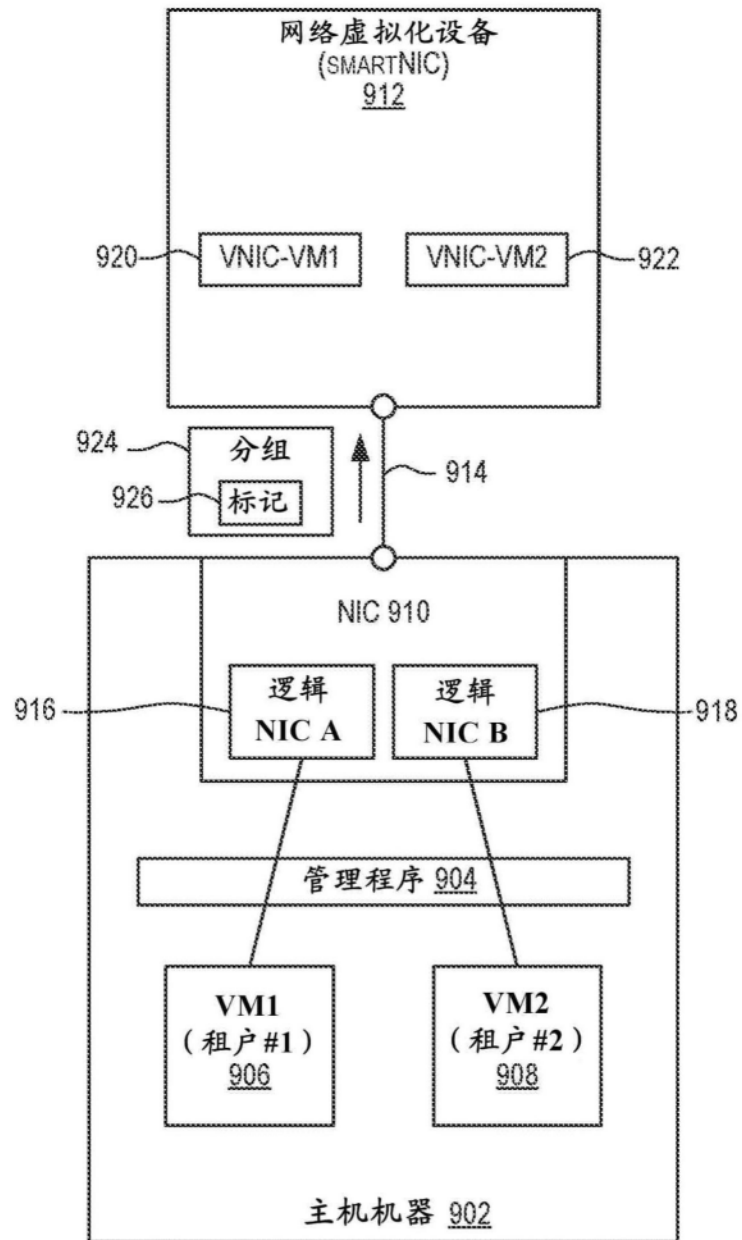


图9

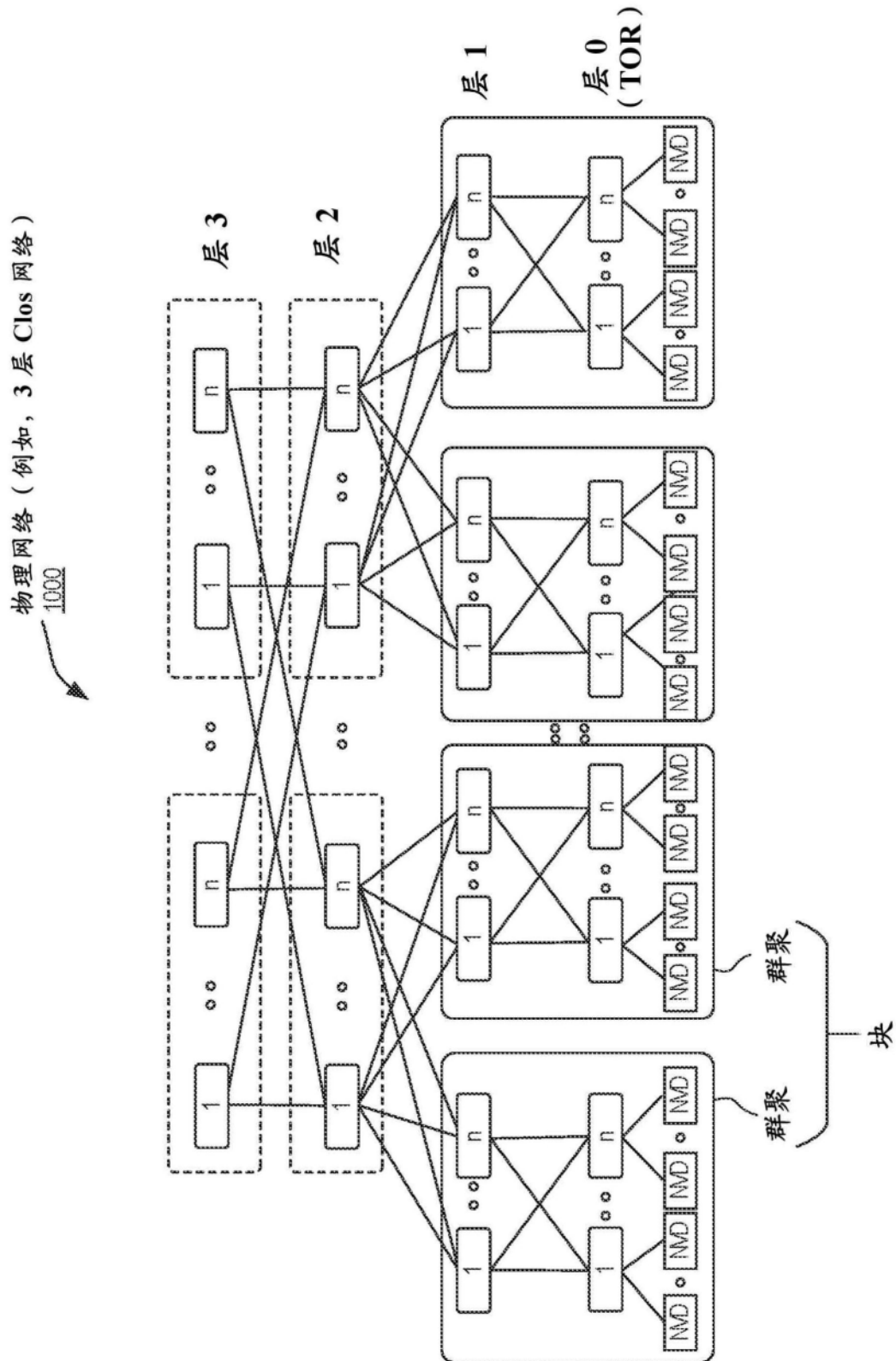


图10

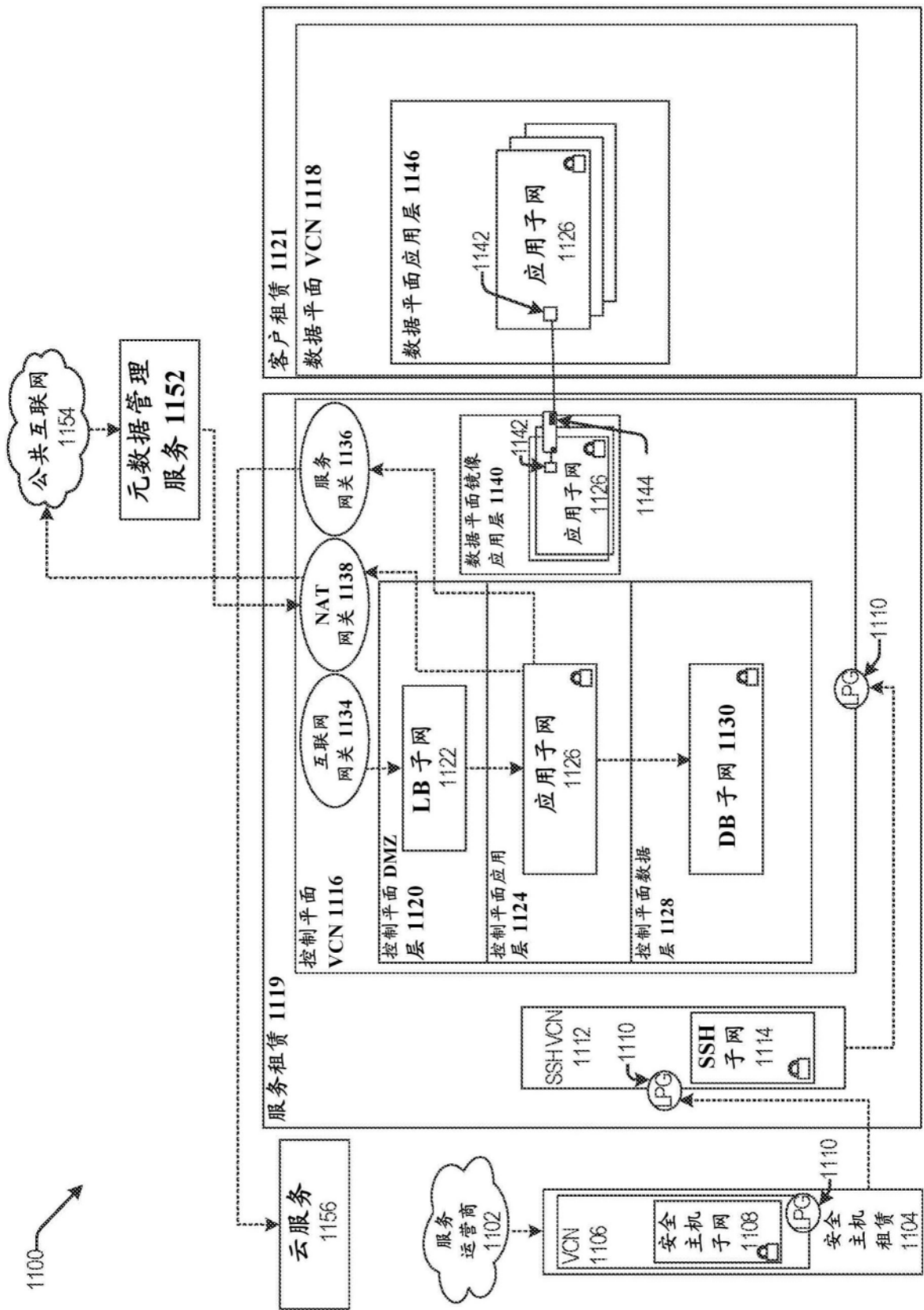


图11

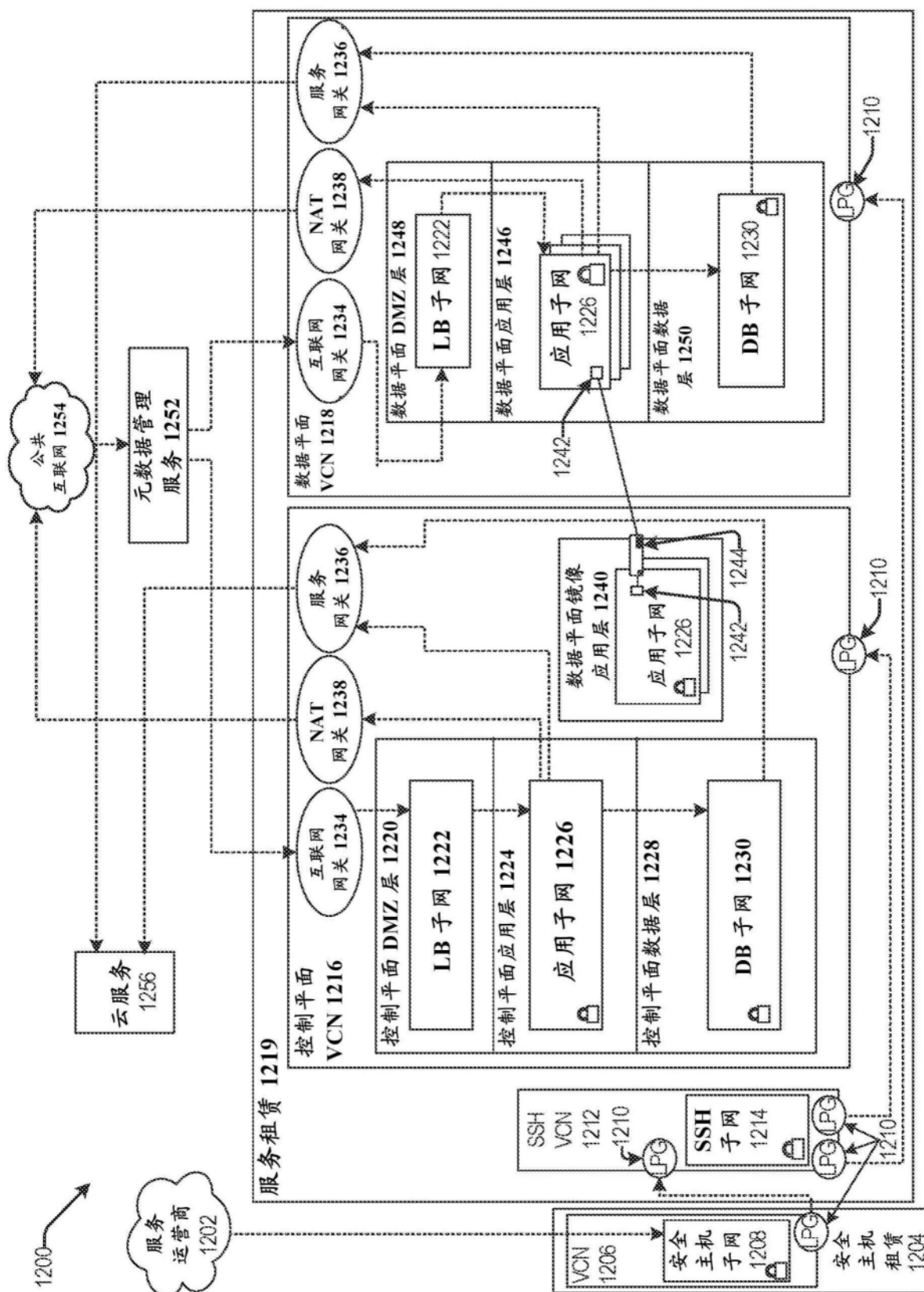


图12

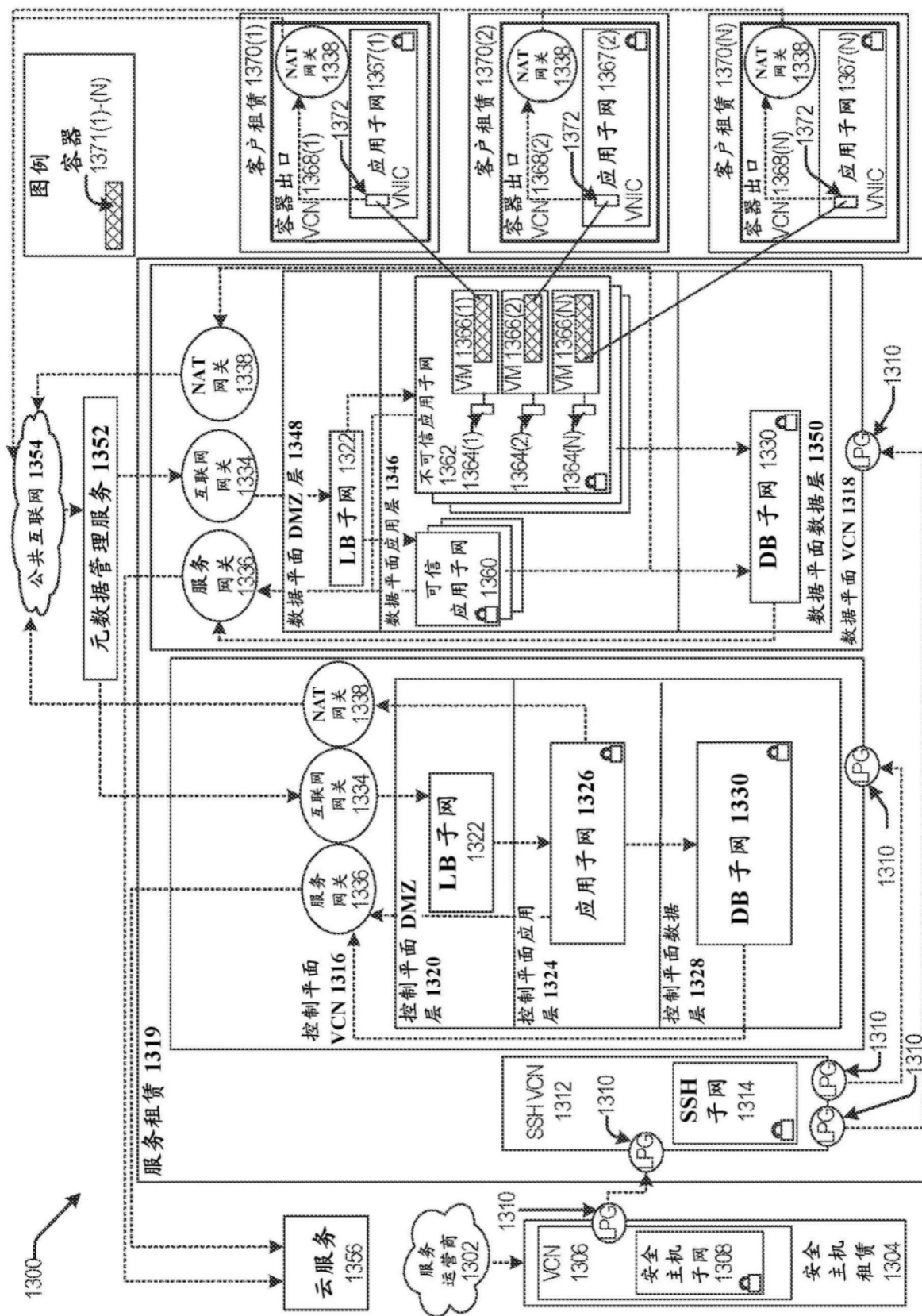


图13

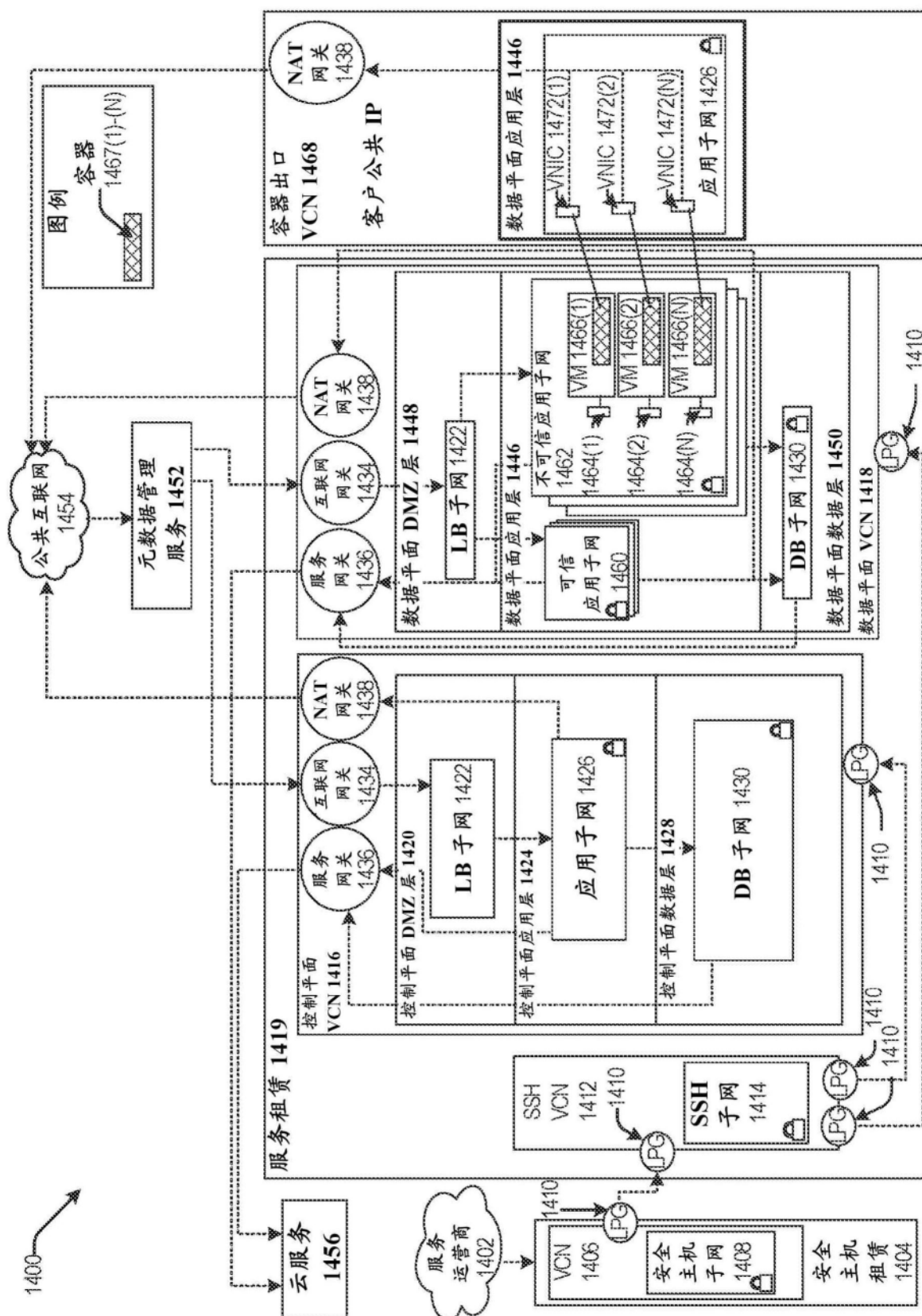


图14

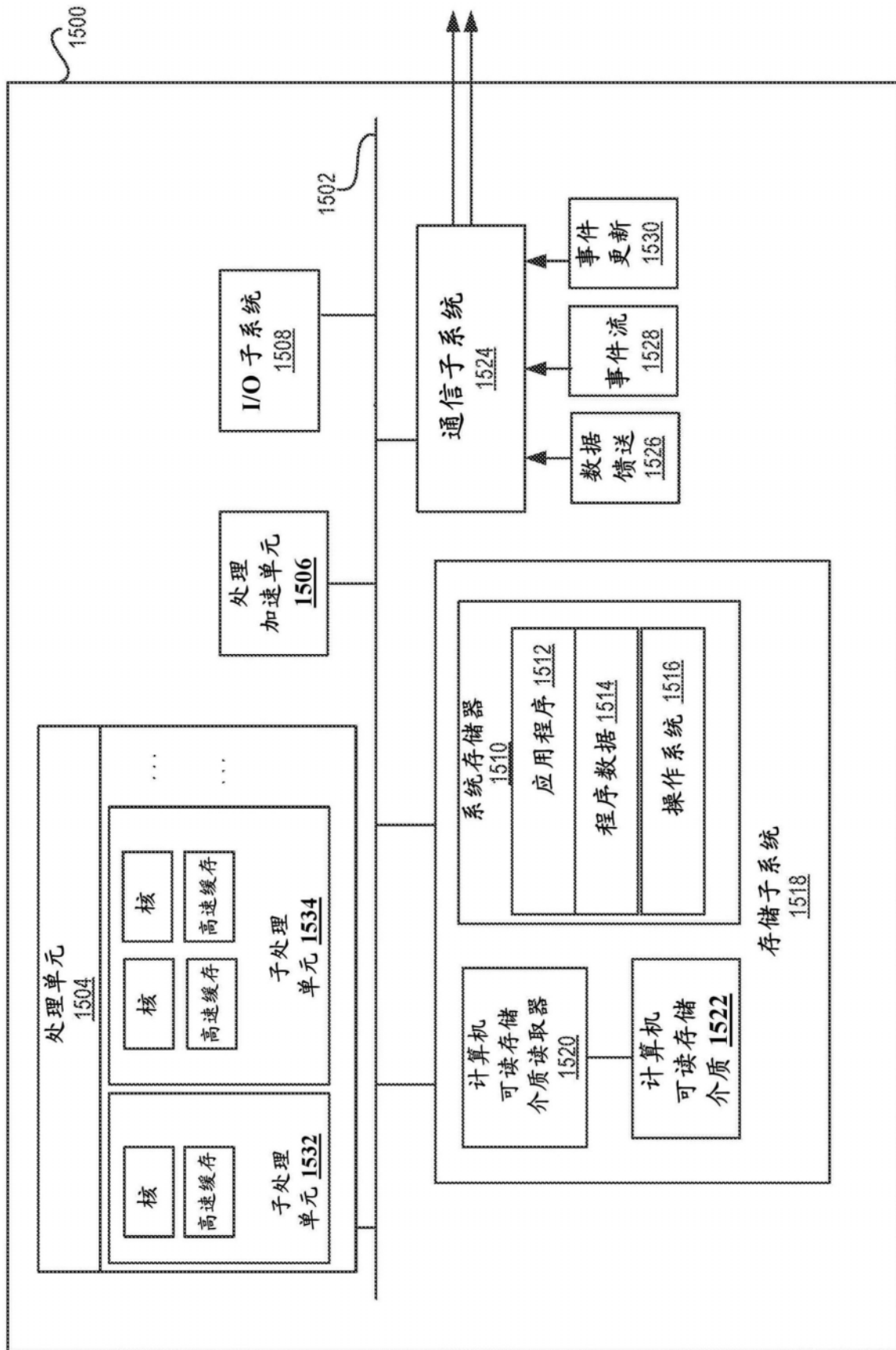


图15