(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107295008 A
(43)申请公布日 2017.10.24

(21)申请号 201710645203.X

(22)申请日 2017.08.01

(71)申请人 广东云下汇金科技有限公司
地址 510419 广东省广州市开发区科学城起云路3号自编三栋A1三楼301

(72)发明人 龚炎

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

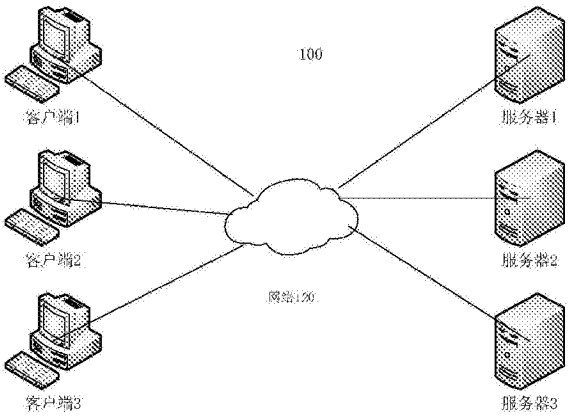
权利要求书2页 说明书10页 附图5页

(54)发明名称

一种企业混合云计算环境下的连接建立方法

(57)摘要

本发明提供了一种企业混合云计算环境下的连接建立方法。控制器集群连接到位于第一和第二网络域之间的VMS集群。在第一网络域中的第一端点处接收到请求以连接到第二网络域中的第二终点。如果连接应通过连接网络域的虚拟网络，则可以通过控制器集群的控制器所允许的方式建立虚拟网络连接。通过这种安全的虚拟网络平台，混合云环境中企业应用的部署和管理将会非常简单。



CN 107295008 A

1.一种企业混合云计算环境下的连接建立方法,其特征在于,包括:

建立一组虚拟网络交换机集群,所述虚拟网络交换机集群耦合在第一网络域和第二网络域之间,其中所述虚拟网络交换机集群与所述第一和第二网络域分开,并且所述第二网络域与第一个网域分开;

设置一控制器,所述控制器连接于第一网络域和第二网络域,所述控制器还连接于所述虚拟网络交换机集群;

在所述第一网络域中的第一端点接收与所述第二网络域中的第二端点建立连接的请求;确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接;

如果确定了第一网络域与第二网络域的虚拟网络来提供连接,则在第一端点和第二端点之间建立虚拟网络连接,以将数据从第一网络域传送到第二网络域,其中建立包括:

所述控制器发送建立连接至所述虚拟网络交换机集群的控制命令至所述第一端点,第一端点接收到所述控制命令后,建立与所述虚拟网络交换机集群的第一连接;

所述控制器发送建立连接至所述虚拟网络交换机集群的控制命令至所述第二端点,第二端点接收到所述控制命令后,建立与所述虚拟网络交换机集群的第二连接。

2.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法,其特征在于,所述第一端点和所述第二端点的其中一个或两个为隔离的虚拟环境。

3.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法,其特征在于,所述确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接具体包括:

确定所述发送数据的目的地址是否存储在所述第一端点的静态虚拟路由表中,所述静态虚拟路由表包括所述第二网络域的地址列表;如果目的地址存储在所述静态虚拟路由表中,则发送请求信息至控制器,以获得控制器的批准。

4.根据权利要求3所述的一种企业混合云计算环境下的连接建立方法,其特征在于,如果目的地址未存储在所述静态虚拟路由表中,则将请求转发到第一个网络域内的本地TCP / IP网络。

5.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法,其特征在于,在所述第一端点存储静态虚拟路由表,所述静态虚拟路由表包括通过虚拟网络允许第一端点连接到的第二网络域的目的地地址列表;当所述第一网络域和所述第二网络域的端点发生变化后,则更新所述静态虚拟路由表。

6.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法,其特征在于,所述确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接。

7.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法,其特征在于,

计算与在所述第一终点中运行的应用程序相关联的标识符;

将标识符与授权标识符的白名单进行比较;

如果标识符在白名单中,则确定允许通过虚拟网络提供连接。

8.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法,其特征在于,

计算与在所述第一终点中运行的应用程序相关联的标识符;

将标识符与标识符的黑名单进行比较;

如果标识符不在黑名单中,则确定允许通过虚拟网络提供连接。

9.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法,其特征在于,

所述第一或第二网络域中的一个包括专用网络域，并且所述第一或第二网络域中的另一个包括公共网络域。

10.根据权利要求1所述的一种企业混合云计算环境下的连接建立方法，其特征在于，所述方法还包括：

如果不能通过虚拟网络提供连接，则丢弃请求。

一种企业混合云计算环境下的连接建立方法

技术领域

[0001] 本发明涉及信息技术领域，更具体的，涉及组网的方法和技术。

背景技术

[0002] 企业云计算技术的利用正在变得越来越火。移动设备(如智能手机和触摸板)的进步进一步推动了云计算基础架构的部署，并且以支持各种应用在线业务。根据市场研究分析师的报告，截至2016年底，全球超过15％的IT支出将用于公共或混合云计算环境。

[0003] 虽然世界上大部分地区正在采用云计算，但云部署仍然需要进行大量的定制工作，并且对于企业来说，建立混合基础设施，随需应变，连接应用程序(例如客户端 - 服务器软件)和公共和私人计算环境中的计算资源仍然具有挑战性而不影响企业的安全性和合规性。

[0004] 传统的IT网络和基础设施安全技术并不直接应用于混合环境。企业IT正面临着巨大的经营风险和其必须通过更多努力来完成任务。因此，需要下一代的平台来满足目前的需求。

[0005] 世界顶级云服务提供商在单个数据中心部署平面云计算基础设施方面拥有丰富的经验。为了方便管理和按需服务，实施具有支持云的统一网络和基础设施安全。这种方法通过消除网络和基础架构安全性的复杂性，大大简化了在云中运行的应用程序的管理。虽然这种方法在单个数据中心的环境中可能是有益的，但是在混合云环境中难以应用，其中在于底层网络和基础架构的安全性分布特性。

[0006] 更具体地说，在现代企业中，网络和安全基础设施专门用于实施企业安全防护和合规治理。关键的业务数据和操作通常部署在网络域的内层后面的防火墙层。然而，另一方面，如果有任何新的业务计划需要从外部位置到达最内层的访问连接，则可能非常困难，或者可能需要大量的企业IT工作来重新提供环境。

[0007] 因此，需要提供用于两个或多个网络域之间的安全通信的系统和技术是目前亟不可待的。

[0008]

发明内容

[0009] 本发明旨在至少解决现有技术中存在的技术问题之一。

[0010] 安全的虚拟网络平台连接两个或多个不同的网络域时。当在一个网络域中的端点处接收到数据分组时，确定数据分组是否应该被转发到虚拟网络平台之外，或者经由虚拟网络发送到另一个网络域中的目的地。

[0011] 为此，本发明提供了一种企业混合云计算环境下的连接建立方法，包括：

建立一组虚拟网络交换机集群，所述虚拟网络交换机集群耦合在第一网络域和第二网络域之间，其中所述虚拟网络交换机集群与所述第一和第二网络域分开，并且所述第二网络域与第一个网域分开；

设置一控制器，所述控制器连接于第一网络域和第二网络域，所述控制器还连接于所述虚拟网络交换机集群；

在所述第一网络域中的第一端点接收与所述第二网络域中的第二端点建立连接的请求；

确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接；

如果确定了第一网络域与第二网络域的虚拟网络来提供连接，则在第一端点和第二端点之间建立虚拟网络连接，以将数据从第一网络域传送到第二网络域，其中建立包括：

所述控制器发送建立连接至所述虚拟网络交换机集群的控制命令至所述第一端点，第一端点接收到所述控制命令后，建立与所述虚拟网络交换机集群的第一连接；

所述控制器发送建立连接至所述虚拟网络交换机集群的控制命令至所述第二端点，第二端点接收到所述控制命令后，建立与所述虚拟网络交换机集群的第二连接。

[0012] 具体的，所述第一端点和所述第二端点的其中一个或两个为隔离的虚拟环境。

[0013]

具体的，所述确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接具体包括：

确定所述发送数据的目的地址是否存储在所述第一端点的静态虚拟路由表中，所述静态虚拟路由表包括所述第二网络域的地址列表；如果目的地址存储在所述静态虚拟路由表中，则发送请求信息至控制器，以获得控制器的批准。

[0014] 具体的，如果目的地址未存储在所述静态虚拟路由表中，则将请求转发到第一个网络域内的本地TCP / IP网络。

[0015] 具体的，在所述第一端点存储静态虚拟路由表，所述静态虚拟路由表包括通过虚拟网络允许第一端点连接到的第二网络域的目的地地址列表；当所述第一网络域和所述第二网络域的端点发生变化后，则更新所述静态虚拟路由表。

[0016] 具体的，所述确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接具体包括：

具体的，所述方法还包括，计算与在所述第一终点中运行的应用程序相关联的标识符；

将标识符与授权标识符的白名单进行比较；

如果标识符在白名单中，则确定允许通过虚拟网络提供连接。

[0017] 具体的，所述方法还包括，计算与在所述第一终点中运行的应用程序相关联的标识符；

将标识符与标识符的黑名单进行比较；

如果标识符不在黑名单中，则确定允许通过虚拟网络提供连接。

[0018] 更具体的，所述第一或第二网络域中的一个包括专用网络域，并且所述第一或第二网络域中的另一个包括公共网络域。

[0019] 更具体的，所述方法还包括：

如果不能通过虚拟网络提供连接，则丢弃请求。

[0020] 在本发明的具体实现中，提供了连接用于企业混合云计算环境的客户端-服务器应用程序的安全虚拟网络平台。该平台可以为运行在具有统一的虚拟网络和安全性的隔离网络域中。并且这种安全的虚拟网络平台与物理网络拓扑和安全性相互独立。通过这种安

全的虚拟网络平台，混合云环境中企业应用的部署和管理非常简单。

[0021] 本发明更多的优点将在下面的具体实施方式和附图中详细体现。

[0022]

附图说明

[0023] 图1示出了可以体现本发明的计算机网络系统框图；

图2示出了本发明的一种企业混合云计算环境下的连接建立方法的流程图；

图3示出了本发明计算机系统的系统框图；

图4示出了可以实现虚拟网络平台的分布式计算环境的简化框图；

图5示出了本发明虚拟网络平台的具体实现的总体流程的示意图；

图6示出了用于本发明另一实施例的方法流程图；

图7示出了本发明虚拟网络平台的技术的方法流程图；

图8示出了本发明另一实施例的方法流程图。

[0024]

具体实施方式

[0025] 为了能够更清楚地理解本发明的上述目的、特征和优点，下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

[0026] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的方式来实施，因此，本发明的保护范围并不受下面公开的具体实施例的限制。

[0027] 图1示出了可以体现本发明的计算机网络系统100框图。系统中可能有任意数量的服务器和客户端。例如，可能有数百，数千甚至数百万的服务器和客户端。在该系统中，有三台服务器，服务器1，服务器2和服务器3，客户端1，客户端2和客户端3都有三个客户端。客户端和服务器可以代表应用软件的载体。硬件机器可以但不限于服务器主机或任何类型的客户端硬件机器，例如台式PC，膝上型计算机和移动设备。服务器通过网络120交换分组来与客户端通信。计算机网络系统代表许多不同的环境，包括LAN(局域网)系统，广域网(WAN)系统，因特网系统，以太网，计算机网络，内联网，蜂窝电话网络等。

[0028] 另一个例子，可以有一个访问应用程序，其中一个用户的“客户端机器”正在访问“云”中的服务器。在这种情况下，使用GDB(GNU Debugger)作为示例，客户端软件然后在客户端用户机。该客户端GDB软件可能连接到云中“服务器”上运行的服务器GDB软件。可以通过本专利申请中所讨论的虚拟网络平台来进行连接。

[0029] 网络通常包括：(1)至少两台计算机，(2)每台计算机上的网络接口或网络接口卡(NIC)，(3)连接介质和(4)网络操作系统软件。NIC是一种让计算机与网络通信的设备。连接介质通常是电线或电缆，尽管网络计算机和外围设备之间的无线通信也可用。网络操作系统软件的一些示例包括Microsoft Windows 7或Windows Server 2012，Linux Red Hat 5，Ubuntu 13，Novell NetWare，AppleShare或Artisoft LANtastic。

[0030] 网络可以包括集线器，交换机或路由器。Hubs互连用户组。集线器可以将数据包

(包括电子邮件,文字处理文档,电子表格,图形,打印请求)转发到一个端口,从一个工作站到其余所有端口。

[0031] 交换机可以为用户或服务器组提供更多的专用带宽。交换机可以基于每个分组报头中的信息将数据分组转发到预期接收者的适当端口。为了隔离其他端口的传输,交换机建立源和目的地之间的临时连接,然后在对话完成时终止连接。

[0032] 路由器将本地网络连接到远程网络。在互联网上,路由器是一种设备,或者在某些情况下是计算机中的软件,用于确定要向其目的地转发数据包的下一个网络点。路由器连接到至少两个网络,并根据当前对其连接的网络的状态的理解,决定哪种方式发送每个信息包。路由器位于任何网关(其中一个网络与另一个网络相交),包括每个互联网的存在点。

[0033] 图2示出了本发明的一种企业混合云计算环境下的连接建立方法的流程图。

[0034] 如图2所示,提供了一种企业混合云计算环境下的连接建立方法,包括:

建立一组虚拟网络交换机集群,所述虚拟网络交换机集群耦合在第一网络域和第二网络域之间,其中所述虚拟网络交换机集群与所述第一和第二网络域分开,并且所述第二网络域与第一个网域分开;

设置一控制器,所述控制器连接于第一网络域和第二网络域,所述控制器还连接于所述虚拟网络交换机集群;

其中控制器连接网络交换机和第一网络域和第二网络域,也可以连接至第一网络域和第二网络域中的每个端点。也就是说,控制器可以独立的控制网络交换机和第一网络域或第二网络域中的端点。

[0035] 在所述第一网络域中的第一端点接收与所述第二网络域中的第二端点建立连接的请求;

确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接;

如果确定了第一网络域与第二网络域的虚拟网络来提供连接,则在第一端点和第二端点之间建立虚拟网络连接,以将数据从第一网络域传送到第二网络域,其中建立包括:

所述控制器发送建立连接至所述虚拟网络交换机集群的控制命令至所述第一端点,第一端点接收到所述控制命令后,建立与所述虚拟网络交换机集群的第一连接;

所述控制器发送建立连接至所述虚拟网络交换机集群的控制命令至所述第二端点,第二端点接收到所述控制命令后,建立与所述虚拟网络交换机集群的第二连接。

[0036] 具体的,所述第一端点和所述第二端点的其中一个或两个为隔离的虚拟环境。

[0037] 具体的,所述确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接具体包括:

确定所述发送数据的目的地址是否存储在所述第一端点的静态虚拟路由表中,所述静态虚拟路由表包括所述第二网络域的地址列表;如果目的地址存储在所述静态虚拟路由表中,则发送请求信息至控制器,以获得控制器的批准。

[0038] 具体的,如果目的地址未存储在所述静态虚拟路由表中,则将请求转发到第一个网络域内的本地TCP / IP网络。

[0039] 具体的,在所述第一端点存储静态虚拟路由表,所述静态虚拟路由表包括通过虚拟网络允许第一端点连接到的第二网络域的目的地地址列表;当所述第一网络域和所述第二网络域的端点发生变化后,则更新所述静态虚拟路由表。

[0040] 具体的，所述确定是否通过连接第一网络域与第二网络域的虚拟网络来提供连接具体包括：

具体的，所述方法还包括，计算与在所述第一终点中运行的应用程序相关联的标识符；

将标识符与授权标识符的白名单进行比较；

如果标识符在白名单中，则确定允许通过虚拟网络提供连接。

[0041] 具体的，所述方法还包括，计算与在所述第一终点中运行的应用程序相关联的标识符；

将标识符与标识符的黑名单进行比较；

如果标识符不在黑名单中，则确定允许通过虚拟网络提供连接。

[0042] 更具体的，所述第一或第二网络域中的一个包括专用网络域，并且所述第一或第二网络域中的另一个包括公共网络域。

[0043] 更具体的，所述方法还包括：

如果不能通过虚拟网络提供连接，则丢弃请求。

[0044] 图3示出了本发明计算机系统的系统框图。例如，计算机系统包括监视器，键盘和大容量存储设备。计算机系统还包括子系统，例如中央处理器302，系统存储器304，输入/输出(I / O)控制器306，显示适配器308，串行或通用串行总线(USB)端口312，网络接口318和扬声器320.在一个实施例中，计算机系统包括附加或更少的子系统。

[0045] 计算机可以连接到网络并且可以使用该网络与其他计算机进行连接。网络可能是内联网，互联网或因特网等。网络可以是有线网络(例如铜缆)，电话网络，分组网络，光网络(例如，使用光纤)或无线网络，或这些的任何组合。例如，可以使用诸如Wi-Fi(IEEE标准802.11，802.11a，802.11b，802.11e，802.11g的协议)的无线网络在计算机和系统的组件(或步骤)之间传递数据和其他信息，802.11i和802.11n，仅举几个例子)。例如，来自计算机的信号可以至少部分地无线地传送到组件或其他计算机。

[0046] 在一个实施例中，通过在计算机工作站系统上的Web浏览器，用户通过诸如因特网的网络访问万维网(WWW)上的系统。Web浏览器用于下载各种格式的网页或其他内容，包括HTML，XML，文本，PDF等，并可用于将信息上传到系统的其他部分。Web浏览器可以使用统一的资源标识符(URL)来标识Web上的资源和在Web上传输文件的超文本传输协议(HTTP)。

[0047] 图4示出了可以实现虚拟网络平台的分布式计算环境405的简化框图。所述环境包括连接第一和第二网络域的第一网络域410，第二网络域415和网络420。第一网络域包括第一组终点425(例如，终点A1，终点A2，...，终点An)。第二网络域包括第二组终点430(例如，终点B1，终点B2，...，终点Bm)。网络域中的端点可以例如通过网络或本地网络互连。

[0048] 终点可以被称为节点或计算节点。在具体实施例中，第一和第二网络域是通过因特网分离和并且两者之间是互连的。第一或第二网络域中的一个可以包括私有云基础设施。第一或第二网络域中的另一个可以包括公共云基础设施。所以在图4的系统可以被称为混合云系统。

[0049] 混合云环境中的安全性是一个需要面临的问题，因为底层网络和基础设施是由多个权限进行分配的。即使变更请求是由经过验证和批准的业务案例驱动的，所有各方之间的安全重新配置协调可能是压倒性的和被禁止的。本发明的平台将部署在通过互联网互连的两个(或多个)分离的网络域中的客户端和服务器连接起来。

[0050] 网络域可以包括任何数量的端点。例如，可以有数百，数千甚至数百万的终点。终点可以包括物理设备，虚拟设备或两者都有。终点可以包括物理服务器(例如，刀片服务器)，虚拟机(VM)，虚拟网络边缘网关或其他物理或虚拟设备。

[0051] 更具体地，终点可以包括具有一个或多个组件的通用计算系统，例如图1所示的组件。例如，终点可以包括用户界面，一个或多个处理器，网络接口，大容量存储器和存储器。或者，一些实施例可以不包括用户界面，或者用户界面可能不直接连接到硬件平台。例如，用户交互可能会自动化或与数据中心管理有关的远程进行。第一个终点可以包括客户端。远离第一个终点的第二个终点可以是服务器。服务器可以为客户端承载应用服务。

[0052] 虚拟机(VM)是执行诸如物理机器的程序的机器(例如，计算机)的软件实现。换句话说，虚拟机是在“主机”硬件平台上作为“访客”安装的物理计算机系统的模拟软件。

[0053] 网络域可以是企业局域网(LAN)，服务器场环境，还有基础架构即服务(IaaS)云数据中心，可以由传统的外围防火墙来保护。两个网络域可以通过互联网或任何TCP / IP网络互连。

[0054] 在一个实施例中，第一网络域与第二网络域不同并且分离开来。例如，域可以在不同的物理或地理位置，具有不同的能力，具有不同的计算机体系结构，具有不同的网络环境，具有不同的物理设备，网络基础设施可以由不同的实体，公司，企业拥有，经营和管理，当局，各方或组织具有不同的管理政策，具有不同的存储策略，具有不同的安全策略或这些策略的组合。

[0055] 这两个网络域可以由同一企业拥有，但可能位于不同的地理位置。例如，一个网络域可能在北京。另一个域名可能在上海。作为另一个例子，一个域或网络基础设施可以是私有的。另一个域或网络基础架构可能由将计算资源租给企业的第三方拥有。域可以是云计算或多租户数据中心的一部分，可以有多个私有域，可以有多个公共域。

[0056] 在一具体实施例中，第一或第二域中的一个是私有云。第一个或第二个域中的另一个是公共云。私有云是指可以由单个企业操作，控制或拥有的计算基础设施(例如，硬件，软件或两者)，计算基础设施是企业内部的。公共云是指通过公开供公众使用的网络(例如因特网)呈现服务的计算基础设施。公共云可以提供对可配置计算资源(例如，网络，服务器，存储，应用和服务)的共享池的按需网络访问。

[0057] 在此具体实施例中，计算架构可以被称为混合云。混合云是两个或更多云(如私有云和公共云)的组合。混合云允许企业扩展其计算能力，而不必对物理空间和计算硬件等资产进行大量资本投资。企业也可以使用混合云来满足对计算资源需求的高峰，可以在需要时支付计算资源。可能会与计算资源的云服务提供商签订租赁，租赁或其他合同协议，可以利用多个云服务提供商的服务。

[0058] 图5示出了本发明虚拟网络平台的具体实现的总体流程605的示意图。

[0059] 在步骤510中，在第一网络域中的第一端点处接收要发送到目的地的数据分组(例如，请求数据)。数据包可以指示连接到目的地的请求地址。在具体实现中，请求来自应用程序的客户端应用程序组件，以与应用程序的服务器组件进行连接。

[0060] 然而，应当理解，请求或连接可以涉及连接到另一域中的任何类型的目的地的一个域中的任何类型的源，反之亦然。例如，在混合云环境中，存在实施“客户端软件”的服务器和实施“服务器软件”的其他服务器。虚拟网络平台便于服务器在云域之间相互通信。在

另一个具体实现中，有一个访问应用程序，其中一个用户的“客户端机器”正在访问“云”中的服务器。在这种情况下，以GNU Debugger(GDB)为例，客户端软件随即运行客户端用户机。该客户端GDB软件可以连接到在云端“服务器”上运行的服务器GDB软件。

[0061] 在步骤515中，确定是否应该通过将第一网络域与不同于或与第一网络域分开的第二网络域的虚拟网络来提供连接。

[0062] 在步骤520中，如果通过虚拟网络提供连接，则在第一网络域中的第一终点与目的地之间建立虚拟网络连接，目的地处于第二网络域中的第二终点。

[0063] 或者，在步骤525中，如果不应该通过虚拟网络提供连接，则数据分组被传递到虚拟网络之外。

[0064] 在具体实现中，关于虚拟网络是否应该被使用的决定可以在本地进行，也可以不经过虚拟网络。例如，可以在始发域(例如，第一域)内做出该决定。此功能有助于节省虚拟网络的计算资源，减少跨虚拟网络的网络流量，并防止瓶颈效应。虚拟网络平台为IT管理员提供了灵活性，可以决定何时使用(或不使用)虚拟网络在两个或多个网络域上传输数据的条件。例如，管理员可以使用系统来控制哪些应用程序将使用虚拟网络，哪些应用程序将不使用虚拟网络，或两者兼而有之。

[0065] 在具体实现中，系统存储被授权或允许使用虚拟网络的应用的列表。该列表可以被称为白名单。在各种其他具体实现中，系统存储未被授权或允许使用虚拟网络的应用的列表。该列表可以被称为黑名单。在具体实现中，允许未列在黑名单中的应用使用虚拟网络。

[0066] 图6示出了用于本发明另一实施例的方法流程图。在这个具体实现方式中，IT管理员将对中央控制器进行编程，以定义用户和用户组(因此，他们的计算机(例如笔记本电脑)在计算机上并自动成为端点并登录系统时)以及运行某些企业应用程序以在虚拟网络平台上访问的服务器或虚拟机。然后，管理员将定义访问规则(安全性)，谁可以访问什么，在什么情况下和运行什么应用程序(例如，哪些特定服务器已加载这些应用程序)。一旦定义了这些安全规则，用户(例如，作为终点的客户端计算机)将能够使用虚拟网络平台来安全地访问在分离的网络域中的其他端点上运行的所配置的应用程序。

[0067] 在步骤610中，IT管理员使用控制器的管理模块来定义用户，用户组，应用和终点。定义规则可以存储在配置文件或数据库中。管理模块可以包括图形用户界面(GUI)，使得管理员可以容易地管理系统。

[0068] IT管理者可根据实际需要设置对应的用户或者用户组的表格用以记录对应的规则。可以是设置一个白名单的表格，也可以设置一个黑名单的表格等等。

[0069] 在步骤615中，安全策略被定义并存储在策略数据库中。如上所述，策略可以包括谁可以访问什么，在什么情况下和运行什么应用程序(例如，哪些特定服务器已经加载了这些应用程序)的规则。策略可能包括要评估的程式化表达式，条件语句(例如，如果X然后执行Y else do Z)，嵌套条件，多条件，布尔运算符(例如，OR，AND或NOT)或这些组合。

[0070] 作为具体示例，例如，考虑用户A可以访问在第二网络域中在服务器A上运行的特定应用的情况。当用户A连接到服务器A并访问应用程序时，在这种情况下，允许另一个用户B同时访问服务器A并访问第二个应用程序。换句话说，可以存在这样的策略，使得用户B的访问权限仅在用户A进行到同一服务器的访问时被授予。这样的策略是有利于安全的，其

中，用户A是部署服务器A的域的员工。User-B是一个正在帮助正在开发应用程序的用户A的供应商。根据该策略，供应商，用户B不能单独访问服务器A。只有当用户A连接到服务器A时，才允许他的访问。

[0071] 在步骤620中，将虚拟网络代理(例如，控制守护程序和虚拟网络代理)以及虚拟路由表提供给端点和虚拟网络交换机。

[0072] 图7示出了本发明虚拟网络平台的技术的方法流程图。

[0073] 在步骤710中，分配IP地址。

[0074] 在步骤715中，应用程序被配置为使用虚拟网络。在该示例中，应用客户端软件被配置为使得它理解第二虚拟IP地址(“vIPb”)是到达应用服务器软件的IP地址。

[0075] 在步骤720中，为虚拟网络代理创建静态虚拟路由表。这些表帮助虚拟网络代理(例如，VNPA或VNPB)进行过滤业务，并决定是否经由虚拟网络或本地TCP / IP网络转发数据包。

[0076] 在步骤725中，根据静态虚拟路由表接收和过滤业务或数据分组。没有静态路由表中列出的路由地址的数据包转发到本地TCP / IP网络(步骤730)。

[0077] 接着，客户端管理器随后根据需要检查控制器的安全许可(步骤735)。虚拟网络交换机(VNS1)创建连接会话(步骤745)。如果安全检查失败(步骤740)，则阻止应用程序客户端连接到应用程序服务器。

[0078] 在步骤750中，创建动态路由表。在步骤750中，为虚拟网络代理和虚拟网络交换机创建动态虚拟网络路由表。然后根据动态路由表路由第一和第二网络域之间的业务(步骤755)。

[0079] 在没有静态路由表中列出的路由地址的数据包转发到本地TCP / IP网络(步骤730)。

[0080] 图8示出了本发明另一实施例的方法流程图。

[0081] 如图8，在步骤810中，系统存储与被授权或允许使用虚拟网络的特定应用程序相关联的标识符或预定标识符。标识符可以由系统计算，或者可以使用系统外部的算法来计算标识符。标识符可以是有助于唯一标识应用程序的特定版本的任何数据单元。在具体实现中，标识符包括与应用程序的特定版本相关联的校验和。应用程序的标识符可以包括签名，散列值，指纹或这些的组合。在具体实现中，可以将标识符提供给网络域中的一个或多个端点并将其存储在网络域中的一个或多个端点。

[0082] 在步骤815中，从应用程序的客户端组件接收请求以连接到应用程序的服务器组件。例如，可以在端点处的终端模块(例如，客户端管理器)处接收该请求。

[0083] 在步骤820中，相应的客户端或服务器管理器确定与应用程序相关联的标识符是否与存储的与特定应用程序相关联的标识符相匹配。如果存在匹配，则在步骤825中，可允许客户端组件通过虚拟网络连接到服务器组件。在具体实现中，使用虚拟网络需要得到控制器的进一步批准。在另一具体实现方式中，允许使用虚拟网络，而无需得到控制器的许可。在安全性比例如响应时间和网络性能更少的情况下，这种具体实现是可取的。

[0084] 或者如果不匹配，则在步骤830中，客户端组件不允许通过虚拟网络连接到服务器组件。换句话说，在具体实现中，标识符与被授权使用虚拟网络的每个应用程序相关联。在具体实现中，当第一网络域中的第一端点处的客户端应用程序经由虚拟网络尝试连接到第

二网络域中的第二终端处的服务器应用时，执行检查以确定应用被授权使用虚拟网络。检查包括将与应用相关联的标识符与与授权应用相关联的标识符列表进行比较(步骤820)。如果存在匹配，则可以在两个端点之间允许虚拟网络连接(步骤825)。如果没有匹配，则不允许虚拟网络连接(步骤830)。

[0085] 在另一具体实现方式中，系统存储被禁止的应用程序或不允许用户使用虚拟网络的应用程序相关联的标识符列表。在该具体实现方式中，检查包括将与应用相关联的标识符与与禁用或未经授权的应用相关联的标识符列表进行比较。如果有匹配，两个端点之间不允许虚拟网络连接。如果没有匹配，两个端点之间允许虚拟网络连接。

[0086] 应理解，说明书通篇中提到的“一个实施例”或“一实施例”意味着与实施例有关的特定特征、结构或特性包括在本发明的至少一个实施例中。因此，在整个说明书各处出现的“在一个实施例中”或“在一实施例中”未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。应理解，在本发明的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本发明实施例的实施过程构成任何限定。上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0087] 需要说明的是，在本文中，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、物品或者装置不仅包括那些要素，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、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

[0088] 在本申请所提供的几个实施例中，应该理解到，所揭露的设备和方法，可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，如：多个单元或组件可以结合，或可以集成到另一个系统，或一些特征可以忽略，或不执行。另外，所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口，设备或单元的间接耦合或通信连接，可以是电性的、机械的或其它形式的。

[0089] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的，作为单元显示的部件可以是、或也可以不是物理单元；既可以位于一个地方，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全部单元来实现本实施例方案的目的。

[0090] 另外，在本发明各实施例中的各功能单元可以全部集成在一个处理单元中，也可以是各单元分别单独作为一个单元，也可以两个或两个以上单元集成在一个单元中；上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

[0091] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：移动存储设备、只读存储器(Read Only Memory，ROM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0092] 或者，本发明上述集成的单元如果以软件功能模块的形式实现并作为独立的产品销售或使用时，也可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明实施例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一个存储介质中，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、服务器、或者网络设备等)执行本发明各个实施例所述方法的全部或部分。而前述的存储介质包括：移动存储设备、ROM、磁碟或者光盘等各种可以存储程序代码的介质。

[0093] 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，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。

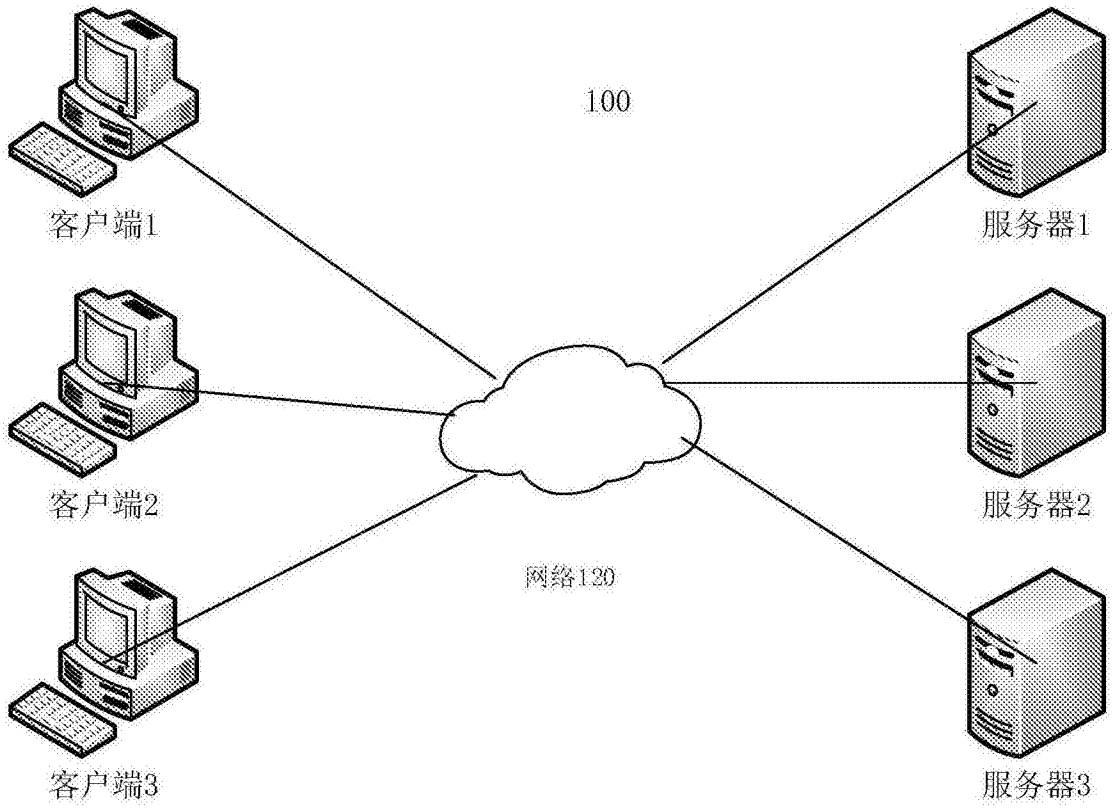

100
客户端1
客户端2
客户端3
网络120
服务器1
服务器2
服务器3

图1

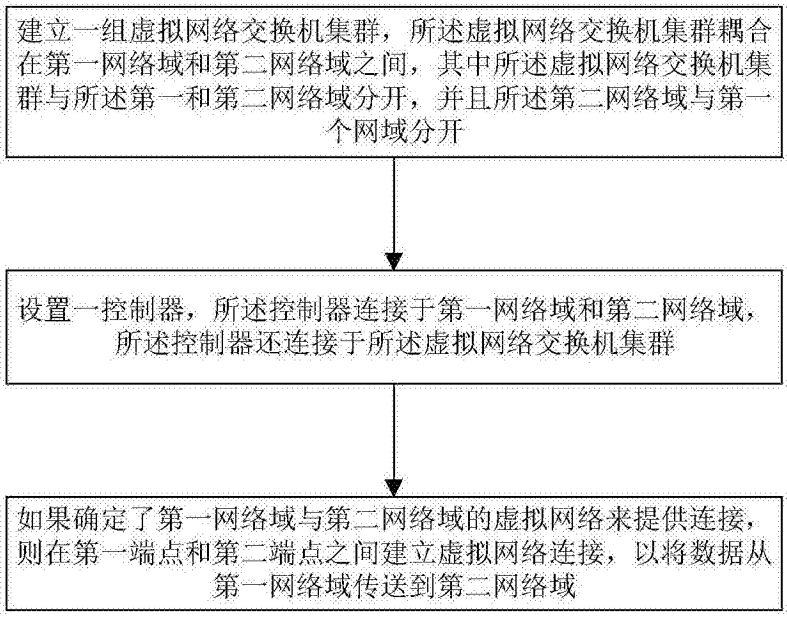

建立一组虚拟网络交换机集群，所述虚拟网络交换机集群耦合在第一网络域和第二网络域之间，其中所述虚拟网络交换机集群与所述第一和第二网络域分开，并且所述第二网络域与第一个网域分开
设置一控制器，所述控制器连接于第一网络域和第二网络域，所述控制器还连接于所述虚拟网络交换机集群
如果确定了第一网络域与第二网络域的虚拟网络来提供连接，则在第一端点和第二端点之间建立虚拟网络连接，以将数据从第一网络域传送到第二网络域

图2

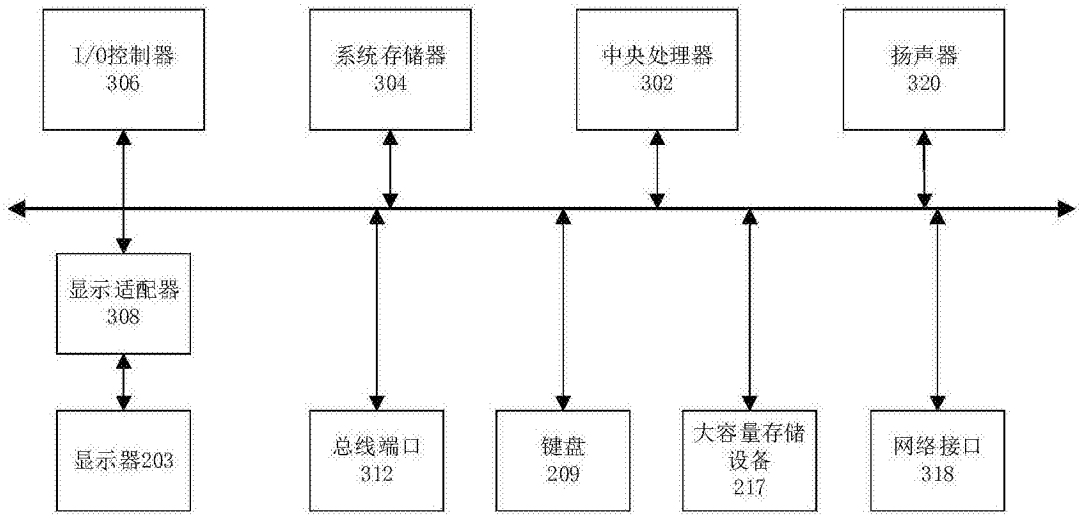

I/O控制器
306
系统存储器
304
中央处理器
302
扬声器
320
显示适配器
308
显示器203
总线端口
312
键盘
209
大容量存储
设备
217
网络接口
318

图3

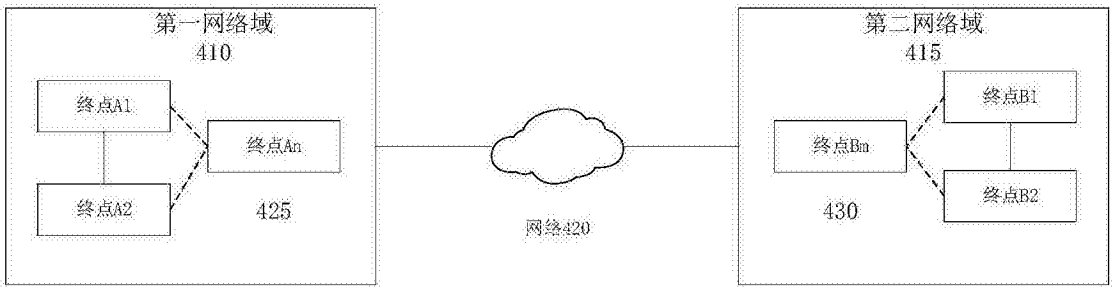

第一网络域
410
终点A1
终点An
终点A2
425
网络420
第二网络域
415
终点B1
终点Bm
终点B2
430

图4

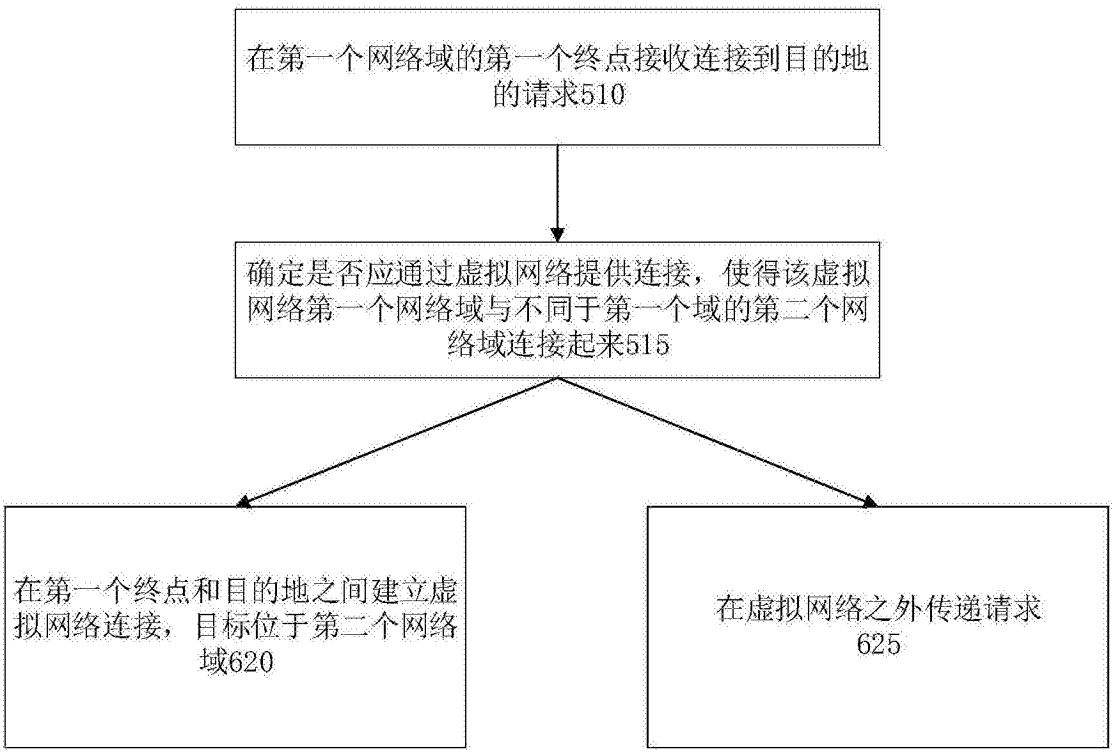

在第一个网络域的第一个终点接收连接到目的地的请求510
确定是否应通过虚拟网络提供连接，使得该虚拟网络第一个网络域与不同于第一个域的第二个网络域连接起来515
在第一个终点和目的地之间建立虚拟网络连接，目标位于第二个网络域620
在虚拟网络之外传递请求625

图5

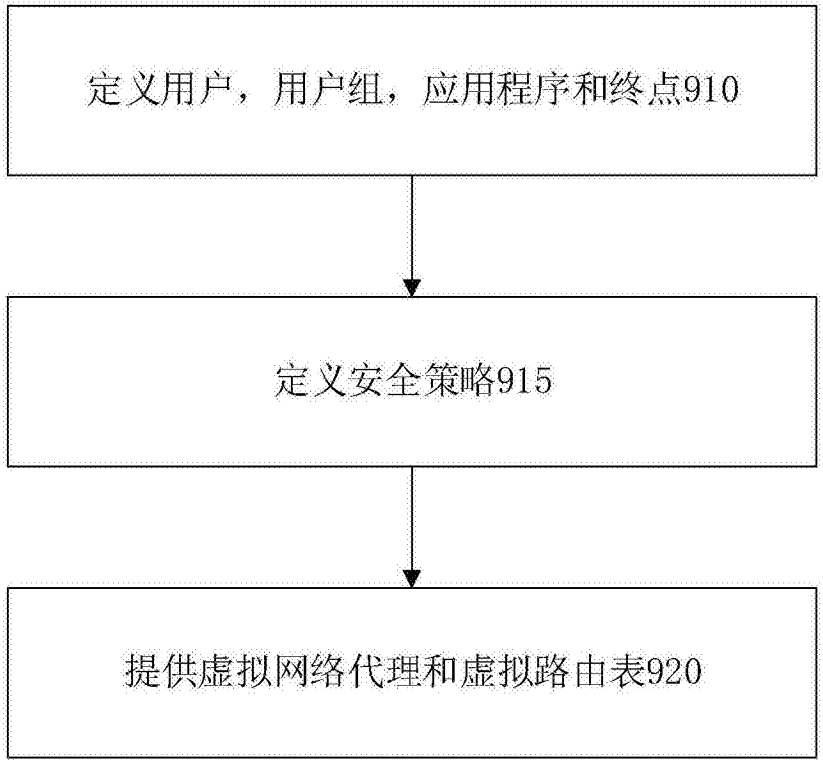

定义用户，用户组，应用程序和终点910
定义安全策略915
提供虚拟网络代理和虚拟路由表920

图6

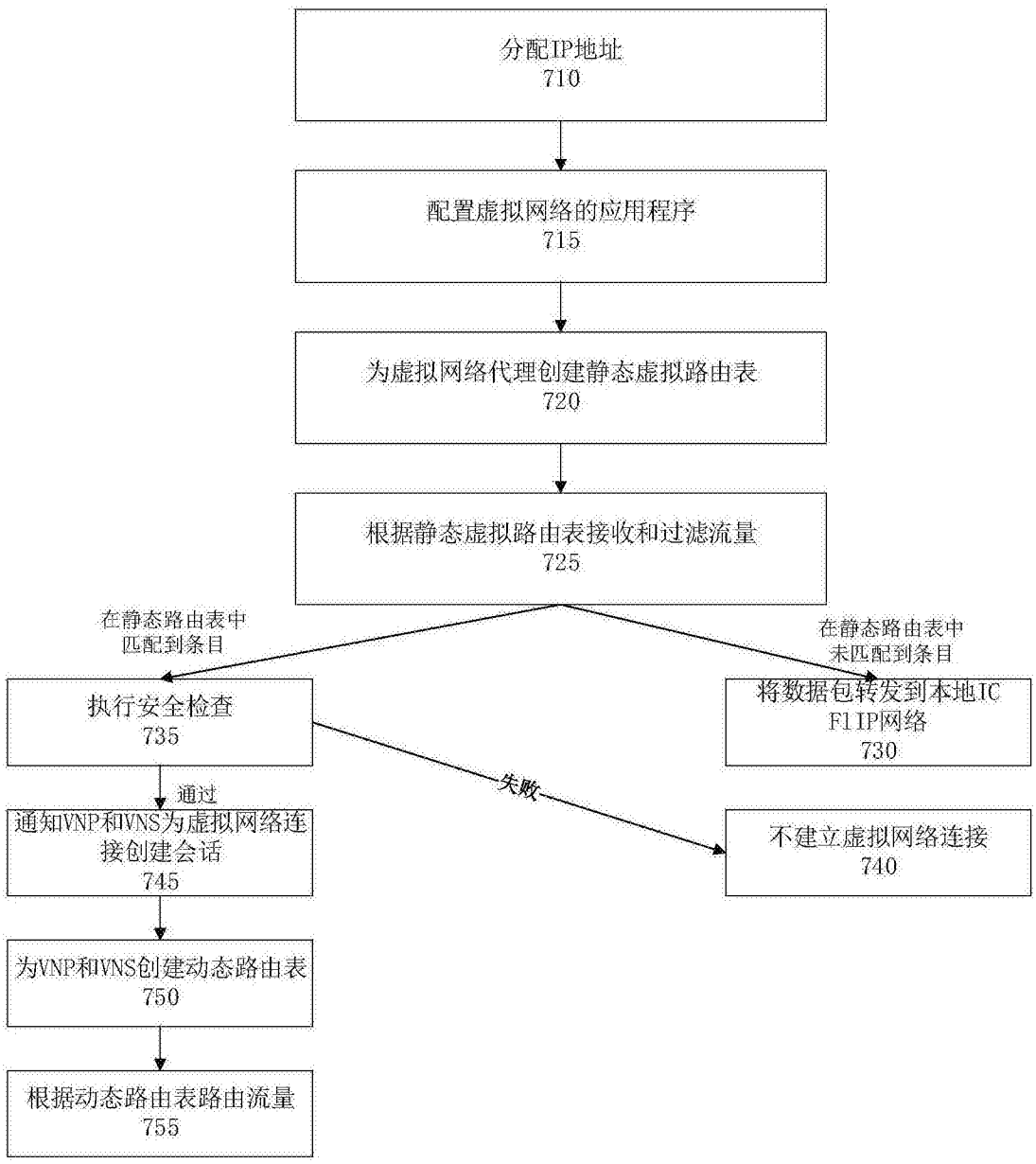

分配IP地址
710
配置虚拟网络的应用程序
715
为虚拟网络代理创建静态虚拟路由表
720
根据静态虚拟路由表接收和过滤流量
725
在静态路由表中匹配到条目
在静态路由表中未匹配到条目
执行安全检查
735
将数据包转发到本地ICF1IP网络
730
失败
通过
通知VNP和VNS为虚拟网络连接创建会话
745
不建立虚拟网络连接
740
为VNP和VNS创建动态路由表
750
根据动态路由表路由流量
755

图7

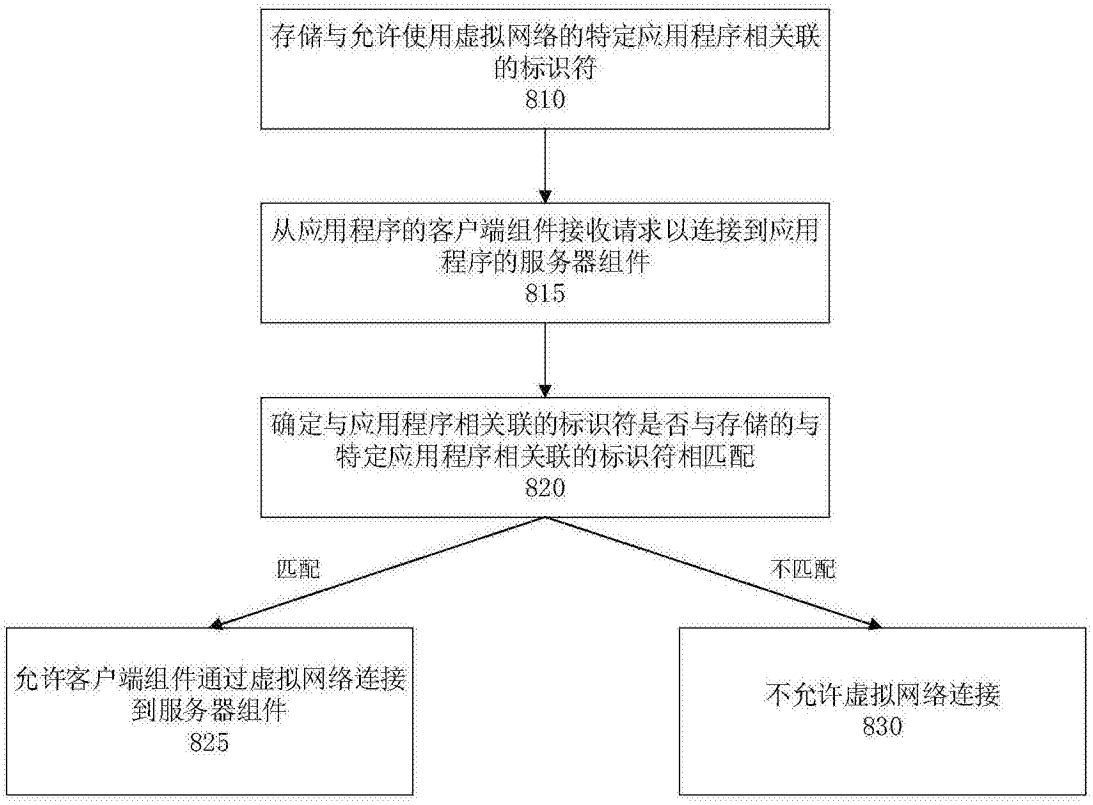

存储与允许使用虚拟网络的特定应用程序相关联的标识符
810
从应用程序的客户端组件接收请求以连接到应用程序的服务器组件
815
确定与应用程序相关联的标识符是否与存储的与特定应用程序相关联的标识符相匹配
820
匹配
不匹配
允许客户端组件通过虚拟网络连接到服务器组件
825
不允许虚拟网络连接
830

图8