



(12) 发明专利申请

(10) 申请公布号 CN 114024782 A

(43) 申请公布日 2022. 02. 08

(21) 申请号 202210020064.2

(22) 申请日 2022.01.10

(71) 申请人 苏州博纳讯动软件有限公司

地址 215213 江苏省苏州市苏州工业园区
星湖街328号创意产业园7-9F

(72) 发明人 花磊 耿浩涛 张荣奇 崔骥

(74) 专利代理机构 苏州谨和知识产权代理事务
所(特殊普通合伙) 32295

代理人 叶栋

(51) Int.Cl.

H04L 9/40 (2022.01)

H04L 12/46 (2006.01)

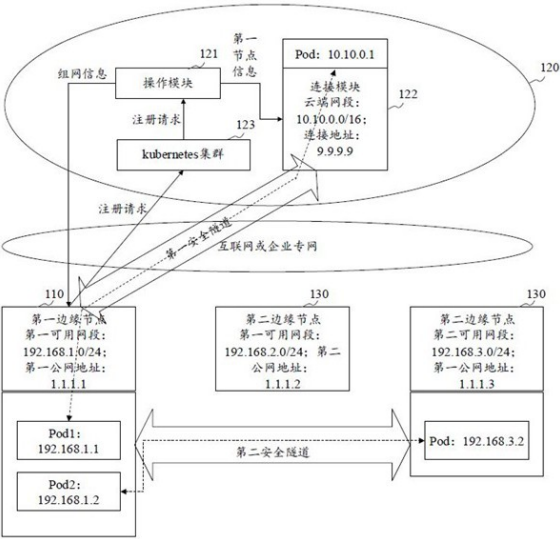
权利要求书1页 说明书6页 附图1页

(54) 发明名称

基于三层安全隧道技术的云与边缘、边缘与边缘组网系统

(57) 摘要

本申请涉及一种基于三层安全隧道技术的云与边缘、边缘与边缘组网系统,属于通信技术领域,其包括第一边缘节点发起注册请求;云端中的操作模块监控到注册请求的情况下,获取注册请求中的第一公网地址;基于第一公网地址为第一边缘节点分配第一可用网段;在连接模块的配置信息中加入第一边缘节点的第一节点信息;将组网信息发送至第一边缘节点;第一边缘节点使用三层安全隧道协议基于组网信息中的连接地址建立第一安全隧道,并基于组网信息中第二公网地址建立第二安全隧道;第一边缘应用使用私有IP地址基于第一安全隧道与云端应用通讯,并基于第二安全隧道与第二边缘应用通讯;可以解决IP地址管理复杂的问题;降低IP地址管理复杂度。



1. 一种基于三层安全隧道技术的云与边缘、边缘与边缘组网系统,其特征在于,所述系统包括:

第一边缘节点,用于向云端的kubernetes集群发起注册请求,所述注册请求携带有所述第一边缘节点的第一公网地址;

所述云端中的操作模块,用于监控所述kubernetes集群,并在监控到所述注册请求的情况下,获取所述注册请求中的第一公网地址;基于所述第一公网地址为所述第一边缘节点分配第一可用网段,所述第一可用网段用于供所述第一边缘节点中的边缘应用使用;在连接模块的配置信息中加入所述第一边缘节点的第一节点信息,所述第一节点信息包括所述第一公网地址和所述第一可用网段;将组网信息发送至所述第一边缘节点,所述组网信息包括所述第一可用网段、所述连接模块的连接地址、云端网段、以及所述配置信息中已加入的第二边缘节点的第二节点信息,所述第二节点信息包括所述第二边缘节点的第二公网地址和第二可用网段;所述第二边缘节点与所述第一边缘节点不同,所述云端网段用于供所述云端中的云端应用使用;

所述第一边缘节点,还用于接收所述组网信息;使用三层安全隧道协议基于所述组网信息中的连接地址与所述连接模块建立第一安全隧道;使用所述三层安全隧道协议基于所述组网信息中第二公网地址与所述第二边缘节点建立第二安全隧道;

所述第一边缘节点中的第一边缘应用,用于使用所述第一可用网段中的私有IP地址基于所述第一安全隧道与所述云端应用通讯;

所述第一边缘节点中的第一边缘应用,还用于使用所述第一可用网段中的私有IP地址基于所述第二安全隧道与所述第二边缘节点中的第二边缘应用通讯。

2. 根据权利要求1所述的系统,其特征在于,所述第一边缘节点中的第一边缘应用,用于:

获取所述第一边缘应用对应的私有IP地址;

从所述组网信息中获取所述云端网段;

在所述第一安全隧道中,使用所述私有IP地址与所述云端网段中的IP地址进行通讯,以实现与所述云端应用通讯。

3. 根据权利要求1所述的系统,其特征在于,所述第一边缘节点中的第一边缘应用,用于:

从所述组网信息中获取所述第二可用网段;

在所述第二安全隧道中,使用所述私有IP地址与所述第二可用网段中的IP地址进行通讯,以实现与所述第二边缘应用通讯。

4. 根据权利要求1所述的系统,其特征在于,所述第一边缘节点与所述云端之间基于因特网或企业专网通信连接。

5. 根据权利要求1所述的系统,其特征在于,

所述操作模块,用于向所述连接模块发送通知消息,所述通知消息包括所述第一节点信息;

所述连接模块,用于基于所述通知消息,在所述配置信息中加入所述第一节点信息。

6. 根据权利要求1所述的系统,其特征在于,所述三层安全隧道协议包括网络协议安全性协议。

基于三层安全隧道技术的云与边缘、边缘与边缘组网系统

技术领域

[0001] 本申请涉及一种基于三层安全隧道技术的云与边缘、边缘与边缘组网系统,属于通信技术领域。

背景技术

[0002] 云计算(cloud computing)是分布式计算的一种,指的是通过网络“云”将巨大的数据计算处理程序分解成无数个小程序,然后,通过多部服务器组成的系统进行处理和分析这些小程序得到结果并返回给用户。

[0003] 然而,传统云计算能力已无法支撑起规模日趋庞大且异地分散的数据处理与计算需求。基于此,边缘计算应势而起。边缘计算是指在靠近物或数据源头的一侧,采用网络、计算、存储、应用核心能力为一体的开放平台,就近提供最近端服务。其应用程序在边缘侧发起,产生更快的网络服务响应,满足行业在实时业务、应用智能、安全与隐私保护等方面的基本需求。

[0004] 目前,如果边缘节点上的边缘应用需要访问云端的集群里的云端应用,需要将云端应用暴露成集群外的公网的IP地址。相应地,边缘应用使用边缘节点的公网身份访问暴露的IP地址。

[0005] 然而,现有的组网方式存在以下问题:1)如果应用很多,每个应用的IP地址都须要暴露到集群外,会导致IP地址管理复杂的问题;2)数据直接在公网上传输,会导致数据不安全的问题;3)当同一的边缘节点上的不同边缘应用访问云端中的云端应用的时候,所有边缘应用共用边缘节点的地址,会导致云端应用失去对边缘应用的源地址身份的可见性,导致审计、追踪困难的问题。

发明内容

[0006] 本申请提供了一种基于三层安全隧道技术的云与边缘、边缘与边缘组网系统,可以自动管理边缘节点的地址段分配,降低IP地址管理复杂度;另外,可以自动建立节点之间的安全隧道,保证数据安全;同时,还可以每个边缘应用对应的Pod在隧道建立后可以使用自己的私有IP地址与云端应用进行通讯,此时,云端应用可以追踪到边缘应用的源地址,实现对边缘应用的审计、追踪;同时,云端应用和边缘应用均通过私有IP地址进行通讯,避免IP地址在公网暴露端口,进一步提高通讯过程的安全性。具体地,本申请提供如下技术方案:

提供一种基于三层安全隧道技术的云与边缘、边缘与边缘组网系统,所述系统包括:

第一边缘节点,用于向云端的kubernetes集群发起注册请求,所述注册请求携带有所述第一边缘节点的第一公网地址;

所述云端中的操作模块,用于监控所述kubernetes集群,并在监控到所述注册请求的情况下,获取所述注册请求中的第一公网地址;基于所述第一公网地址为所述第一边

缘节点分配第一可用网段,所述第一可用网段用于供所述第一边缘节点中的边缘应用使用;在连接模块的配置信息中加入所述第一边缘节点的第一节点信息,所述第一节点信息包括所述第一公网地址和所述第一可用网段;将组网信息发送至所述第一边缘节点,所述组网信息包括所述第一可用网段、所述连接模块的连接地址、云端网段、以及所述配置信息中已加入的第二边缘节点的第二节点信息,所述第二节点信息包括所述第二边缘节点的第二公网地址和第二可用网段;所述第二边缘节点与所述第一边缘节点不同,所述云端网段用于供所述云端中的云端应用使用;

所述第一边缘节点,还用于接收所述组网信息;使用三层安全隧道协议基于所述组网信息中的连接地址与所述连接模块建立第一安全隧道;使用所述三层安全隧道协议基于所述组网信息中第二公网地址与所述第二边缘节点建立第二安全隧道;

所述第一边缘节点中的第一边缘应用,用于使用所述第一可用网段中的私有IP地址基于所述第一安全隧道与所述云端应用通讯;

所述第一边缘节点中的第一边缘应用,还用于使用所述第一可用网段中的私有IP地址基于所述第二安全隧道与所述第二边缘节点中的第二边缘应用通讯。

[0007] 可选地,所述第一边缘节点中的第一边缘应用,用于:

获取所述第一边缘应用对应的私有IP地址;

从所述组网信息中获取所述云端网段;

在所述第一安全隧道中,使用所述私有IP地址与所述云端网段中的IP地址进行通讯,以实现与所述云端应用通讯。

[0008] 可选地,所述第一边缘节点中的第一边缘应用,用于:

从所述组网信息中获取所述第二可用网段;

在所述第二安全隧道中,使用所述私有IP地址与所述第二可用网段中的IP地址进行通讯,以实现与所述第二边缘应用通讯。

[0009] 可选地,所述第一边缘节点与所述云端之间基于因特网或企业专网通信连接。

[0010] 可选地,所述操作模块,用于向所述连接模块发送通知消息,所述通知消息包括所述第一节点信息;

所述连接模块,用于基于所述通知消息,在所述配置信息中加入所述第一节点信息。

[0011] 可选地,所述三层安全隧道协议包括网络协议安全性协议。

[0012] 本申请的有益效果至少包括:通过第一边缘节点向云端的kubernetes集群发起注册请求,注册请求携带有第一边缘节点的第一公网地址;云端中的操作模块监控kubernetes集群,并在监控到注册请求的情况下,获取注册请求中的第一公网地址;基于第一公网地址为第一边缘节点分配第一可用网段,第一可用网段用于供第一边缘节点中的边缘应用使用;在连接模块的配置信息中加入第一边缘节点的第一节点信息,第一节点信息包括第一公网地址和第一可用网段;将组网信息发送至第一边缘节点,组网信息包括第一可用网段、连接模块的连接地址、云端网段、以及配置信息中已加入的第二边缘节点的第二节点信息,第二节点信息包括第二边缘节点的第二公网地址和第二可用网段;第二边缘节点与第一边缘节点不同,云端网段用于供云端中的云端应用使用;第一边缘节点接收组网信息;使用三层安全隧道协议基于组网信息中的连接地址与连接模块建立第一安全隧道;

使用三层安全隧道协议基于组网信息中第二公网地址与第二边缘节点建立第二安全隧道；第一边缘节点中的第一边缘应用使用第一可用网段中的私有IP地址基于第一安全隧道与云端应用通讯；第一边缘节点中的第一边缘应用使用第一可用网段中的私有IP地址基于第二安全隧道与第二边缘节点中的第二边缘应用通讯；可以解决应用很多，每个应用的IP地址都须要暴露到集群外，会导致IP地址管理复杂的问题；通过为每个第一边缘节点自动分配网段，不需要人工管理每个边缘应用的私有IP地址，可以降低IP地址管理复杂度，提高管理效率。

[0013] 另外，通过使用三层安全隧道协议建立第一安全隧道和第二安全隧道，可以保证边缘应用与云端应用之间、边缘应用和边缘应用之间的通讯安全性，可以解决数据直接在公网上传输，会导致数据不安全的问题，保证数据安全。

[0014] 另外，通过在第一安全隧道建立完成后，边缘应用和云端应用之间通过私有IP地址进行通讯；在第二安全隧道建立完成后，边缘应用和边缘应用之间也通过私有IP地址进行通讯，可以实现应用的源地址追踪，实现应用的审计和追踪。同时，云端应用和边缘应用均通过私有IP地址进行通讯，避免IP地址在公网暴露端口，进一步提高通讯过程的安全性。

[0015] 上述说明仅是本申请技术方案的概述，为了能够更清楚了解本申请的技术手段，并可依照说明书的内容予以实施，以下以本申请的较佳实施例并配合附图详细说明如后。

附图说明

[0016] 图1是本申请一个实施例提供的基于三层安全隧道技术的云与边缘、边缘与边缘组网系统的结构示意图。

具体实施方式

[0017] 下面结合附图和实施例，对本申请的具体实施方式做进一步详细描述。以下实施例用于说明本申请，但不用来限制本申请的范围。

[0018] 首先，对于本申请涉及的若干名词进行介绍。

[0019] 云节点是指云计算里使用的主机/服务器。

[0020] 边缘节点是指边缘计算里使用的主机/服务器。

[0021] 网际协议(Internet Protocol, IP)地址：提供的一种统一的地址格式，它为互联网上的每一个网络和每一台主机分配一个逻辑地址，以此来屏蔽物理地址的差异。它可以分为公网地址和私有地址。公网地址由因特网信息中心(Internet Network Information Center, Internet NIC)负责。这些IP地址分配给注册并向Internet NIC提出申请的组织机构，通过它直接访问因特网。私有地址(Private address)属于非注册地址，专门为组织机构内部使用。

[0022] 网络转换技术(Network Address Translate, NAT)是当在专用网内部的一些主机仅有在本专用网内使用的私有地址，但又想和互联网上的其它主机通信时使用的方法。这种方法需要在专用网连接到因特网的路由器上安装NAT软件，它至少有一个公网IP地址。这样，所有使用私有IP地址的主机在和外界通信时，都要在NAT路由器上将其本地地址转换成公网IP地址，才能和Internet因特网连接。

[0023] 虚拟专用网络(Virtual Private Network, VPN)：是在公用网络上建立专用网络，

进行加密通讯的技术。VPN网关通过对数据包的加密和数据包目标地址的转换实现远程访问。

[0024] 隧道：是指VPN中一个节点到另外一个节点通讯使用的路径。

[0025] Kubernetes：简称K8s，是用8代替名字中间的8个字符“ubernete”而成的缩写。Kubernetes是一个开源的容器编排引擎，它支持自动化部署、大规模可伸缩、应用容器化管理。在生产环境中部署一个应用程序时，通常要部署该应用的多个实例以便对应用请求进行负载均衡。在Kubernetes中，可以创建多个容器(Pod)，每个容器里面运行一个应用实例，然后通过内置的负载均衡策略，实现对这一组应用实例的管理、发现、访问。

[0026] Pod：是Kubernets管理的资源的最小单位，有一个或多个容器组成，共享同一个网络的命名空间，即有同一个IP地址。

[0027] 三层隧道协议：是用公用网来封装和传输三层(网路层)协议(如IP、IPX、AppleTalk等)，此时在隧道内传输的是网路层的分组。IETF制定的IP层加密标准协议网络协议安全性(Internet Protocol Security, IPsec)也是一个三层隧道协议，利用IPSec(ESP/AN)的隧道模式可以构成VPN隧道。

[0028] 图1是本申请一个实施例提供的基于三层安全隧道技术的云与边缘、边缘与边缘组网系统的结构示意图，该系统包括：第一边缘节点110、云端120和第二边缘节点130。

[0029] 第一边缘节点110是待向云端120注册的边缘节点。第一边缘节点110的数量可以是一个或至少两个，本实施例不对第一边缘节点110的数量作限定。

[0030] 第一边缘节点110与云端120之间通过传输网络通信相连。其中，传输网络基于因特网或企业专网实现。

[0031] 本实施例中，第一边缘节点110，用于向云端120的kubernetes集群发起注册请求，以将第一边缘节点110注册至云端120。其中，注册请求携带有第一边缘节点110的第一公网地址。

[0032] 每个边缘节点(包括第一边缘节点110和下文中的第二边缘节点130)均具有对应的公网地址，该公网地址预先存储在边缘节点中。

[0033] 本实施例中，云端120包括一个标准的kubernetes集群123。另外，本实施例中，云端120还包括操作模块121和与操作模块121通信相连的连接模块122。其中，操作模块121和连接模块122可以实现在同一服务器中，或者实现在不同服务器中，本实施例不对操作模块121和连接模块122的实现方式作限定。

[0034] 其中，操作模块121用于对kubernetes集群123进行监控，并可以拦截到发送至kubernetes集群的注册请求。

[0035] 具体地，操作模块121用于监控kubernetes集群，并在监控到注册请求的情况下，获取注册请求中的第一公网地址(比如：获取到第一边缘节点110的公网IP地址为1.1.1.1)；基于第一公网地址为第一边缘节点110分配第一可用网段(比如：第一可用网段为192.168.1.0/24)；在连接模块122的配置信息中加入第一边缘节点110的第一节点信息，第一节点信息包括第一公网地址和第一可用网段；将组网信息发送至第一边缘节点110。

[0036] 其中，组网信息包括第一可用网段、连接模块122的连接地址(比如：连接地址为9.9.9.9)、云端120网段(比如：云端120网段为10.10.0.0/16)、以及配置信息中已加入的第二边缘节点130的第二节点信息，第二节点信息包括第二边缘节点130的第二公网地址(比

如：一个第二边缘节点130的公网IP地址为1.1.1.2、另一个第二边缘节点130的公网IP地址为1.1.1.3)和第二可用网段(比如：公网IP地址为1.1.1.2对应的第二可用网段为192.168.2.0/24、公网IP地址为1.1.1.3对应的第二可用网段为192.168.3.0/24)。

[0037] 其中，第二边缘节点130与第一边缘节点110不同。第二边缘节点130是指已在云端120中完成注册的边缘节点。由于每个第二边缘节点130的注册流程与第一边缘节点110的注册流程相同，因此，连接模块122的配置信息中会存储有第二边缘节点130的第二节点信息。图1中以第二边缘节点130的数量为两个为例进行说明，在实际实现时，第二边缘节点130的数量可以为1个或多个，本实施例不对第二边缘节点130的数量作限定。

[0038] 第一可用网段用于供第一边缘节点110中的边缘应用使用，比如：第一边缘节点110中Pod1对应的边缘应用使用第一可用网段192.168.1.0/24中的192.168.1.1作为私有IP地址、第一边缘节点110中Pod2对应的边缘应用使用第一可用网段192.168.1.0/24中的192.168.1.2作为私有IP地址。

[0039] 云端120网段用于供云端120中的云端120应用使用，比如：云端120中的Pod对应的云端120应用使用云端120网段10.10.0.0/16中的10.10.0.1作为私有IP地址。

[0040] 在连接模块122的配置信息中加入第一边缘节点110的第一节点信息时，操作模块121用于向连接模块122发送通知消息，该通知消息包括第一节点信息。相应地，连接模块122用于基于通知消息，在配置信息中加入第一节点信息。

[0041] 在实际实现时，通知消息中还可以包括其它信息，本实施例不对通知消息中携带的信息内容作限定。

[0042] 相应地，第一边缘节点110还用于接收组网信息；使用三层安全隧道协议基于组网信息中的连接地址与连接模块122建立第一安全隧道；使用三层安全隧道协议基于组网信息中第二公网地址与第二边缘节点130建立第二安全隧道。

[0043] 可选地，三层安全隧道协议包括IPSec协议。

[0044] 使用三层安全隧道协议基于组网信息中的连接地址与连接模块122建立第一安全隧道，包括：第一边缘节点110使用第一公网地址使用三层安全隧道协议与连接地址建立第一安全隧道。

[0045] 使用三层安全隧道协议基于组网信息中第二公网地址与第二边缘节点130建立第二安全隧道，包括：

第一边缘节点110使用第一公网地址使用三层安全隧道协议与第二公网地址建立第二安全隧道。

[0046] 在第一安全隧道建立之后，第一边缘节点110中的第一边缘应用用于使用第一可用网段中的私有IP地址基于第一安全隧道与云端120应用通讯。

[0047] 具体地，第一边缘应用用于：获取第一边缘应用对应的私有IP地址；从组网信息中获取云端120网段；在第一安全隧道中，使用私有IP地址与云端120网段中的IP地址进行通讯，以实现与云端120应用通讯。

[0048] 比如：第一边缘节点110中Pod1对应的第一边缘应用使用私有IP地址192.168.1.1与私有IP地址为10.10.0.1的云端120的Pod通讯。此时，由于第一边缘应用使用私有IP地址与云端120应用进行通讯，因此，云端120应用可以追踪到源地址，方便应用审计和追踪。

[0049] 在第二安全隧道建立之后，第一边缘应用还用于使用第一可用网段中的私有IP地

址基于第二安全隧道与第二边缘节点130中的第二边缘应用通讯。

[0050] 具体地,第一边缘节点110中的第一边缘应用,用于:从组网信息中获取第二可用网段;在第二安全隧道中,使用私有IP地址与第二可用网段中的IP地址进行通讯,以实现与第二边缘应用通讯。

[0051] 比如:第一边缘节点110中Pod2对应的第一边缘应用使用私有IP地址192.168.1.2与第二边缘节点130中私有IP地址为192.168.3.2的Pod通讯。此时,由于第一边缘应用使用私有IP地址与第二边缘应用进行通讯,因此,第二边缘应用可以追踪到源地址,方便应用审计和追踪。

[0052] 综上所述,本实施例提供的基于三层安全隧道技术的云与边缘、边缘与边缘组网系统,通过第一边缘节点向云端的kubernetes集群发起注册请求,注册请求携带有第一边缘节点的第一公网地址;云端中的操作模块监控kubernetes集群,并在监控到注册请求的情况下,获取注册请求中的第一公网地址;基于第一公网地址为第一边缘节点分配第一可用网段,第一可用网段用于供第一边缘节点中的边缘应用使用;在连接模块的配置信息中加入第一边缘节点的第一节点信息,第一节点信息包括第一公网地址和第一可用网段;将组网信息发送至第一边缘节点,组网信息包括第一可用网段、连接模块的连接地址、云端网段、以及配置信息中已加入的第二边缘节点的第二节点信息,第二节点信息包括第二边缘节点的第二公网地址和第二可用网段;第二边缘节点与第一边缘节点不同,云端网段用于供云端中的云端应用使用;第一边缘节点接收组网信息;使用三层安全隧道协议基于组网信息中的连接地址与连接模块建立第一安全隧道;使用三层安全隧道协议基于组网信息中第二公网地址与第二边缘节点建立第二安全隧道;第一边缘节点中的第一边缘应用使用第一可用网段中的私有IP地址基于第一安全隧道与云端应用通讯;第一边缘节点中的第一边缘应用使用第一可用网段中的私有IP地址基于第二安全隧道与第二边缘节点中的第二边缘应用通讯;可以解决应用很多,每个应用的IP地址都须要暴露到集群外,会导致IP地址管理复杂的问题;通过为每个第一边缘节点自动分配网段,不需要人工管理每个边缘应用的私有IP地址,可以降低IP地址管理复杂度,提高管理效率。

[0053] 另外,通过使用三层安全隧道协议建立第一安全隧道和第二安全隧道,可以保证边缘应用与云端应用之间、和边缘应用和边缘应用之间的通讯安全性,可以解决数据直接在公网上传输,会导致数据不安全的问题,保证数据安全。

[0054] 另外,通过在第一安全隧道建立完成后,边缘应用和云端应用之间通过私有IP地址进行通讯;在第二安全隧道建立完成后,边缘应用和边缘应用之间也通过私有IP地址进行通讯,可以实现应用的源地址追踪,实现应用的审计和追踪。同时,云端应用和边缘应用均通过私有IP地址进行通讯,避免IP地址在公网暴露端口,进一步提高通讯过程的安全性。

[0055] 以上所述实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0056] 以上所述实施例仅表达了本申请的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本申请构思的前提下,还可以做出若干变形和改进,这些都属于本申请的保护范围。因此,本申请专利的保护范围应以所附权利要求为准。

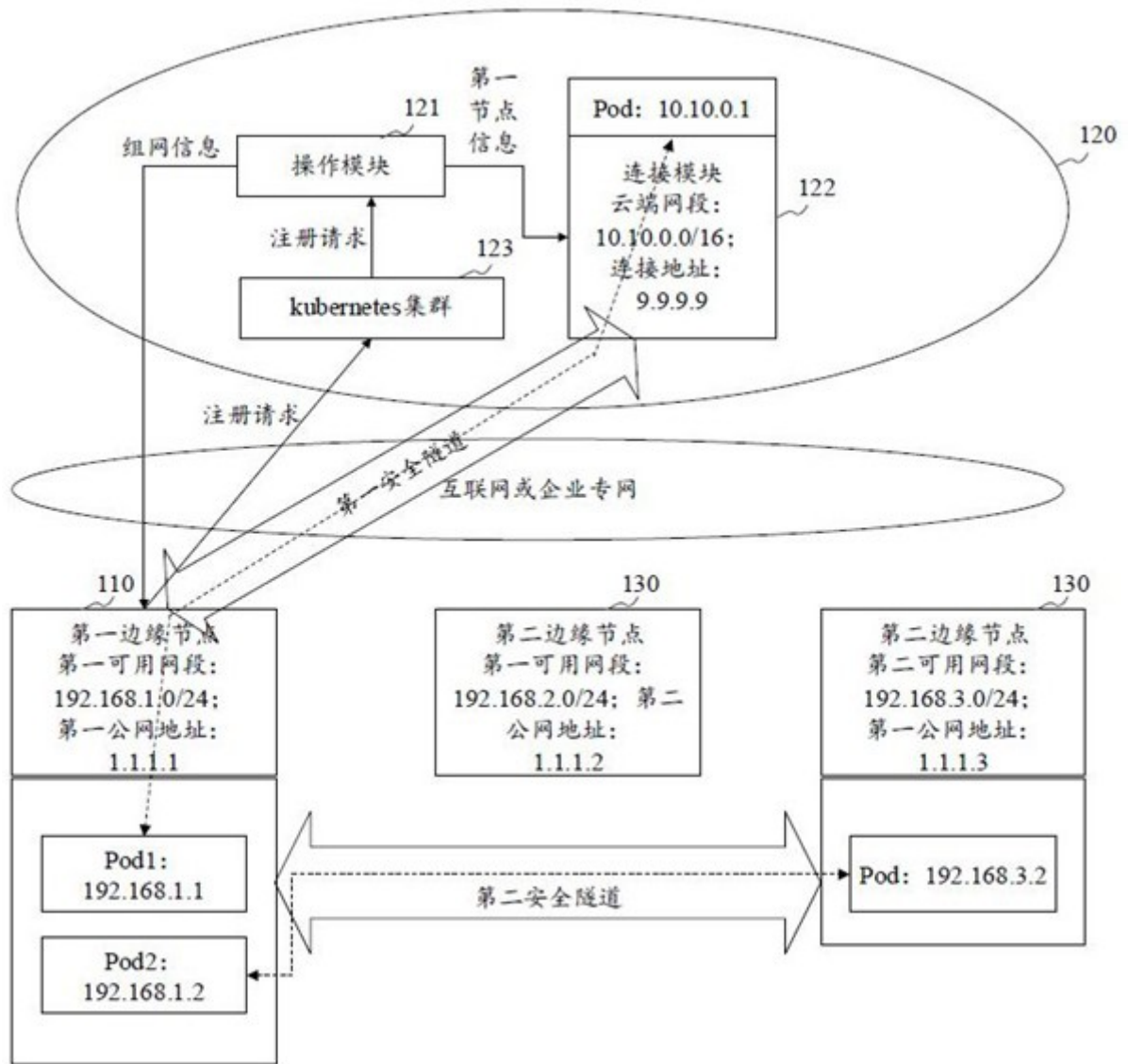


图1