

VIRTUAL PRIVATE CLOUD COMMUNICATION SYSTEM, SYSTEM CONFIGURATION METHOD AND CONTROLLER

The present application claims the priority to a Chinese patent application No. 201811463985.6, filed with the China National Intellectual Property Administration on November 30, 2018 and entitled "Virtual private cloud communication system, system configuration method and controller", which is incorporated herein by reference in its entirety.

Technical Field

The present application relates to the technical field of virtual private cloud, and in particular, to a virtual private cloud communication system, a method for configuring the system and a controller.

Background

Virtual private cloud (VPC) is a dynamic configuration pool of public cloud computing resources, which transmits data between private enterprises and cloud service providers by encryption protocols, tunneling protocols, and other security procedures.

The VPC system is implemented using tunnels or other similar network protocols, and gives a tenant granular control over which corresponding cloud resources can be allocated to tenants, thereby providing an on-demand distribution supply capacity for different tenants, while having strong flexibility, isolation, and security. In the current virtual private cloud, most of the computing resources provided by cloud computing providers are delivered to tenants in virtual machines (VM). The scheme abstracts and divides an original physical machine (host machine of VM) into more fine-grained individuals and places them in VPCs divided by tenants through virtualization technologies of CPU (Central Processing Unit), Memory, Disk and other resources.

When multiple VMs are created on one physical machine, the above-mentioned scheme may introduce a problem that the VMs compete for original resources of the physical machine (such as CPU scheduling, I/O reading and writing, and network bandwidth). If only one VM is created on a physical machine, performance aspects of the VM are improved. However, due to the introduction of virtualization technology, the original performance advantage of the physical machine cannot be still reached, and the overall resource performance cannot be maximized.

Furthermore, with the rise of artificial intelligence industry, the demand for GPU (Graphics Processing Unit) is very large, and the benefit of resource virtualization of GPU is much less appreciable.

In view of this, GPU-consuming tasks such as image, sound, and video processing can be distributed on the physical machine (PM), and some control processing programs can be distributed in the VM. The balanced distribution of resources is achieved by PM and VM.

At this time, intra-tenant communication and inter-tenant isolation are particularly important in an ultra large scale cloud environment. In the existing schemes, the communication and isolation is performed by VLAN (Virtual Local Area Network). However, due to a limited number of VLAN IDs (Virtual Local Area Network Identification), the number of VPCs that exceeds an upper limit of the number of VLAN IDs cannot be built. Therefore, in the field of cloud computing service, there are the large number of tenants, that is, the number of VPCs to be built is much greater than the upper limit of the number of VLAN IDs, thus for a cloud computing provider, the method of isolating tenants by VLAN IDs in the prior art is not adequate for the application environment of cloud computing.

Summary

In view of this, the objective of the present application is to provide a virtual private cloud communication system, a method for configuring the same, and a controller, which can establish a communication connection based on a gateway, without being limited to an upper limit of the number of VLAN IDs. Furthermore, the number of VMs and PMs allocating to tenants can increase with increase in tenants, thereby forming a large scale cloud environment and meeting current business development requirements.

In a first aspect, an embodiment of the present application provides a virtual private cloud communication system, including; at least one virtual machine (VM) and a system gateway communicatively connected to each of the VM;

at least one physical machine (PM), and a switch communicatively connected to each of the PM;

wherein the system gateway is communicatively connected to the switch;

the system gateway and the switch are configured for enabling communication between the VM and the PM belonging to a same virtual private cloud (VPC) based on preset configuration

information.

Optionally, the configuration information includes an isolation label corresponding to the VPC;

the configuration information further includes forwarding entries corresponding to the resources included in the VPC;

the resources include: a VM(s) and/or a PM(s).

Optionally, the system further includes a controller.

The controller is communicatively connected to the system gateway and the switch, respectively.

The controller is configured for performing information configuration on the system gateway and the switch, respectively, to generate configuration information, and sending the configuration information to the system gateway and the switch, respectively.

Optionally, the controller is further configured for:

generating an isolation label corresponding to each virtual private cloud (VPC) based on the VPC;

acquiring IP addresses of resources belonging to the same virtual private cloud (VPC), wherein the resources include a VM(s) and/or a PM(s);

establishing forwarding entries based on the IP addresses of the resources;

generating configuration information corresponding to the VPC based on the forwarding entries and the isolation label.

Optionally, the controller is further configured for:

establishing a forwarding entry(s) of the VM(s) based on the IP address of the VM(s), and/or

establishing a forwarding entry(s) of the PM(s) based on the IP address of the PM(s).

Optionally, the controller is further configured for:

managing the resources in the virtual private cloud (VPC) based on the configuration information, wherein the resources include the VM(s) and/or the PM(s), and the managing includes: adding resources and/or removing resources.

Optionally, the controller is further configured for:

receiving a management operation request for the resources in the VPC, wherein the management operation request includes an isolation label corresponding to a to-be-managed VPC; and

modifying configuration information corresponding to the to-be-managed VPC in the system gateway and the switch according to the isolation label.

Optionally, the controller is further configured for:

adding, based on a request for adding a resource, a forwarding entry corresponding to an IP address of the resource; and/or

removing, based on a request for removing part of the resources, forwarding entries corresponding to IP addresses of the part of the resources; and/or

removing the configuration information corresponding to the to-be-managed VPC based on a request for removing all of the resources.

Optionally, the system gateway is configured for:

receiving a first message of the VM, wherein the first message includes an isolation label;

finding configuration information corresponding to the isolation label in the first message based on the isolation label, and forwarding the first message to a corresponding switch based on the found configuration information;

the system gateway is further configured for:

receiving a second message of the switch, wherein the second message includes an isolation label;

finding configuration information corresponding to the isolation label in the second message based on the isolation label, and forwarding the second message to a target VM based on the found configuration information.

Optionally, the switch is configured for:

receiving a third message of the PM, wherein the third message includes an isolation label;

finding configuration information corresponding to the isolation label in the third message based on the isolation label, and forwarding the third message to a corresponding system gateway based on the found configuration information;

the switch is further configured for:

receiving a fourth message of the system gateway, wherein the fourth message includes an isolation label;

finding configuration information corresponding to the isolation label in the fourth message based on the isolation label, and forwarding the fourth message to a target PM based on the found configuration information.

Optionally, the system gateway is implemented by running corresponding software in a server.

In a second aspect, an embodiment of the present application further provides a method for configuring a virtual private cloud communication system, which is applied to a controller in the virtual private cloud communication system described in the first aspect and any one of its possible implementations, wherein the controller is communicatively connected to the system gateway and the switch, respectively, and the method includes:

performing information configuration on the system gateway and the switch, respectively, to generate configuration information; and

sending the configuration information to the system gateway and the switch, respectively;

wherein the configuration information includes an isolation label corresponding to a VPC, and forwarding entries corresponding to resources included in the VPC, wherein the resources includes a VM(s) and/or a PM(s).

Optionally, the step of generating configuration information includes:

generating an isolation label corresponding to each virtual private cloud (VPC) based on the VPC;

acquiring IP addresses of resources belonging to a same virtual private cloud (VPC), wherein the resources includes a VM(s) and/or a PM(s);

establishing forwarding entries based on the IP addresses of the resources; and

generating configuration information corresponding to the VPC based on the forwarding entries and the isolation label.

Optionally, the step of establishing forwarding entries based on the IP addresses of the resources includes:

establishing a forwarding entry(s) of the VM(s) based on the IP address of the VM(s),

and/or

establishing a forwarding entry(s) of the PM(s) based on the IP address of the PM(s).

Optionally, the method further includes:

managing the resources in the virtual private cloud (VPC) based on the configuration information, wherein the resources include a VM(s) and/or a PM(s), and the managing includes: adding resources and/or removing resources.

Optionally, the method further includes:

receiving a management operation request for the resources in the VPC, wherein the management operation request includes an isolation label corresponding to a to-be-managed VPC; and

modifying configuration information corresponding to the to-be-managed VPC in the system gateway and the switch according to the isolation label.

Optionally, the management operation request includes one or more of a request for adding a resource, a request for removing part of the resources, and a request for removing all of the resources, and the method further includes:

adding, based on the request for adding a resource, a forwarding entry corresponding to an IP address of the resource; and/or

removing, based on the request for removing part of the resources, forwarding entries corresponding to IP addresses of the part of the resources; and/or

removing the configuration information corresponding to the to-be-managed VPC based on the request for removing all of the resources.

In a third aspect, an embodiment of the present application further provides a controller, including a memory and a processor. The memory stores a computer program that can be run on the processor, and the processor executes the computer program to implement the method described in the first aspect and any one possible implementation thereof.

In a fourth aspect, an embodiment of the present application provides a computer-readable storage medium having stored a computer program thereon, and the computer program is executed by a processor, so as to cause the processor to implement the method described above.

In a fifth aspect, an embodiment of the present application further provides an application

program which, when executed, implements the method for configuring the virtual private cloud communication system provided in the second aspect of the embodiment of the present application.

The embodiments of the present application bring the following beneficial effects:

In the embodiment of the present application, the virtual private cloud communication system includes at least one virtual machine VM and a system gateway communicatively connected to each of the VM; and at least one physical machine PM and a switch communicatively connected to each of the PM; wherein the system gateway is communicatively connected to the switch; the system gateway and the switch are configured to enable communication between the VM and the PM belonging to a same virtual private cloud VPC based on preset configuration information. In this scheme, a physical machine area formed by the PM accesses the network through the switch, and a virtual machine area formed by the VM is connected to the switch corresponding to the physical machine area through the system gateway, thereby establishing the connection between the PM of the physical machine area and the VM of the virtual machine area, and realizing the communication between the VM and the PM. Therefore, the communication connection established based on the gateway in the present application is not be limited to the upper limit of the number of VLAN IDs, and the number of VMs and PMs allocating to tenants can increase with increase in tenants, thereby forming a large scale cloud environment and meeting the current business development requirements.

Other features and advantages of the present application will be described in the following description, and a part of them will be obvious from the description, or understood by implementing the present application. The objective and other advantages of the present application are realized and obtained by the structures specifically pointed out in the description, claims and drawings.

In order to make the above-mentioned objectives, features and advantages of the present application more clear and understandable, the preferred embodiments and accompanying drawings are described in detail as follows.

Brief Description of the Drawings

In order to more clearly describe the technical solutions of the embodiments of the present application or of the prior art, drawings that need to be used in embodiments and the prior art

will be briefly described below. Obviously, the drawings provided below are for only some embodiments of the present application; those skilled in the art can also obtain other drawings based on these drawings without any creative efforts.

FIG. 1 is a structural diagram of a virtual private cloud communication system according to an embodiment of the present application;

FIG. 2 is a structural diagram of another virtual private cloud communication system according to an embodiment of the present application;

FIG. 3 is a diagram of communication connection of a virtual private cloud communication system according to an embodiment of the present application;

FIG. 4 is a flowchart of a method for configuring a system according to an embodiment of the present application;

FIG. 5 is a structural diagram of a controller according to an embodiment of the present application.

Detailed Description

In order to make the objectives, technical solutions, and advantages of the present application clearer and more understandable, the present application will be described in more detail below with reference to the appended drawings and embodiments. Obviously, the described embodiments are only some, and not all, of the embodiments of the present application. All other embodiments obtained based on the embodiments of the present application by those skilled in the art without any creative efforts fall into the scope of protection defined by the present application.

At present, in the existing solutions, the communication and isolation is performed by VLAN. However, due to being limited by the number of VLAN IDs and a hardware structure of a switch, VMs and PMs allocated to tenants cannot form a large scale cloud environment, which cannot meet current business development requirements for more and more tenants. In view of this, an embodiment of the present application provides a virtual private cloud communication system, a method for configuring the system, and a controller, which establishes a communication connection between VM and PM based on a gateway. Since VLAN is no longer used to isolate the local area network, it is not limited to the upper limit of the number of VLAN IDs. The number of VMs and PMs allocating to tenants can increase with increase in tenants,

thereby forming a large scale cloud environment and meeting the current business development requirements.

In order to facilitate the understanding of the present application, a virtual private cloud communication system according to an embodiment of the present application is first introduced in detail.

FIG. 1 shows a structural diagram of a virtual private cloud communication system according to an embodiment of the present application. As shown in FIG. 1, the virtual private cloud communication system includes at least one virtual machine VM 10 and a system gateway 12 communicatively connected to each of the VMs; and at least one physical machine PM 13 and a switch 14 communicatively connected to each of the PMs. The system gateway is communicatively connected to the switch. The system gateway and the switch are used to enable communication between the VM 10 and the PM 13 located in the same virtual private cloud VPC based on preset configuration information. The above-mentioned PM refers to a physical machine other than a host machine of VM .

The switch 14 is a three-layer switch and supports a tunnel protocol for subsequent data transmission through a tunnel. The VM is created on a physical machine as a host machine to realize resource virtualization, and may be used for, but is not limited to, the storage of control processing programs. The PM (which is not the host machine in which the VM is located) may be used for, but is not limited to, the storage of GPU-consuming task information such as image, sound, and video processing, etc. Data can be exchanged between a virtual machine area formed by a VM and a physical machine area formed by a PM, wherein the VM and the PM corresponds to the same tenant.

In a possible embodiment, the aforementioned system gateway is implemented by running corresponding software in a server (for example, an X86 server). Since the virtual private cloud communication system may have thousands of tenants, the system gateway is implemented by an X86 server cluster to form a system gateway cluster.

It should be noted that the number of VMs, the number of PMs, the number of system gateways, and the number of switches are determined according to actual situations, and FIG. 1 is only an example.

The physical machine area formed by a PM accesses the network through the switch, and

the virtual machine area formed by the VM is connected to the switch corresponding to the physical machine area through the system gateway, thereby establishing the communication between the PM of the physical machine area and the VM of the virtual machine area, and realizing the communication between the VM and the PM. Therefore, the communication connection established based on the gateway in the present application is not be limited to the upper limit of the number of VLAN IDs, and the number of VMs and PMs allocating to tenants can increase with increase in tenants, thereby forming a large scale cloud environment and meeting the current business development requirements.

Considering that IP addresses configured by different tenants for the resources (including VM and/or PM) in their VPC may overlap, configuration information is stored in the controller. The configuration information includes an isolation label for VPC isolation. One VPC corresponds to one isolation label.

Therefore, after receiving a resource creation request from a tenant, a logical operation is performed, and isolation labels are assigned based on different VPCs of different tenants to distinguish VMs and PMs in the different VPCs, so that the different VPCs are isolated from each other and do not interfere with each other. In view of this, the above configuration information includes an isolation label corresponding to the above VPC. In addition, the configuration information also includes a forwarding entry for a resource included in the corresponding VPC. Therefore, the system gateway and the switch can realize the communication between VMs and PMs in the same VPC based on the forwarding entry and the isolation label.

For example, the IP addresses of VM-A and PM-A of tenant A are 10.0.1.2/24 and 10.0.1.3/24, respectively, and the label is 100. The IP addresses of VM-B and PM-B of tenant B are also 10.0.1.2/ 24 and 10.0.1.3/24, respectively, and the label is 200. Assuming that the VMs of the two tenants are located in the same host machine in the virtual machine area, and the PMs of the two tenants are connected to the same switch correspondingly. The communication path between VM-A and PM-A and the communication path between VM-B and PM-B pass through the same host machine, through the system gateway, to the same switch. In the two communication paths, the system gateway and the switch are shared during the communication process. If an isolation technology is not adopted, a collision on the communication paths may occur during communication between the VM and PM of the tenant A and between the VM and

PM of the tenant B, which causes a communication abnormality.

Since tenants can set IP addresses for their own machines, there is a possibility that the tenant A and the tenant B set IP addresses of their VMs or PMs to be the same. In order to avoid confusing the machine of the tenant A with the machine of the tenant B, a service provider needs to distinguish the machines of the two tenants.

To solve the above problems, the controller may assign an isolation label to the VPC of each tenant, and then the controller simultaneously issues the isolation label and the forwarding entries for the PM and the VM to each system gateway and switch. When subsequent VMs of tenant A and tenant B communicate with their respective PMs at the same time, the controller may isolate the communication paths by encapsulating the isolation labels in the forwarding entries.

An improvement is made on the virtual private cloud communication system shown in FIG. 1 according to the above-mentioned embodiments. As shown in FIG. 2, the present application also provides another virtual private cloud communication system, which includes a controller 20. The controller is communicatively connected to the system gateway and the switch, respectively, performs information configuration on the system gateway and the switch to generate configuration information, and sends the configuration information to the system gateway and the switch, respectively, thereby facilitating subsequent data transmission.

In a possible embodiment, the controller is connected to the host machine in which the VM is located and an out-of-band management system corresponding to the PM, and performs the resource configuration and information configuration through the host machine and the out-of-band management system according to tenant requirements, and obtains configuration information. The out-of-band management system is a management system for initializing the PM (such as reinstalling the operating system). The specific process is as follows:

(a1) Receiving a resource creation request from a tenant.

For example, the tenant may directly call a corresponding API (Application Programming Interface) through a tenant terminal (which may be a mobile terminal or a computer), or call the corresponding API by logging into a WEB (World Wide Web) console, and fill in information of actual requirements, such as required CPU type, memory size, network card, etc., to generate the resource creation request and send it to the controller.

(a2) Allocating resources to the tenant according to the resource creation request, wherein the resources constitute VPC of the tenant.

The resources of VPC include VM and/or PM, that is, the VM and/or PM constitutes the VPC of the tenant.

After receiving the resource creation request, the controller performs a logical operation to determine the required resources, and allocates available resources in a resource pool (host machines and PMs) through a management unit of the host machine and the out-of-band management system. If the controller determines that there are resources that meet the requirements, the controller performs the configuration operation, to allocate the corresponding number of VMs and/or PMs. The VMs and/or PMs constitute the VPC corresponding to the tenant. If there are no resources that meet the requirements, the controller returns information such as insufficient resources to the user.

For example, after receiving a resource creation request of the tenant, the controller may select, based on a CPU type, a memory size, and a transmission rate of a network card included in the resource creation request, a PM meeting the request from the resource pool as a target host machine. This is the logical calculation process mentioned above. Then, the controller may create a VM in the target host machine. In the embodiment of the present invention, the resource pool includes multiple types of PMs. Some PMs may be used as host machines, and some PMs may be used for image, sound, and video processing. These PMs may include GPUs, and thus when the tenant has a requirement to use a GPU, for example, the tenant has a requirement to perform image, sound and video processing, these GPUs may be directly allocated to the tenant as PMs. That is, these PMs which only contain GPUs may be taken as one type of PMs. The management unit in the host machine refers to a unit for managing configuration parameters of VMs in a PM as the host machine. The out-of-band management system refers to a management system for initializing the PMs (for example, reinstalling an operating system). The out-of-band management system may operate independently of the network shown in FIG. 2 and may interact with the controller. It can be understood that since the management unit manages the VMs in the host machine and the out-of-band management system manages the PMs, the controller can select a PM that meets the requirement of the tenant from the resource pool as a host machine through interaction with the management unit and the out-of-band management system.

(a3) Generating an isolation label corresponding to each virtual private cloud VPC based on

the VPC.

The isolation label may be composed of numbers, letters and/or special symbols, and so on.

(a4) Acquiring IP addresses of resources belonging to the same virtual private cloud VPC.

The resources include VMs and/or PMs. The IP addresses include the IP addresses of the VMs and the IP addresses of the PMs. That is, the acquired IP addresses are the IP addresses of the VMs and/or PMs belonging to the same VPC.

Specifically, during a configuration process of a tenant terminal, a network segment in which a PM and a VM are located can be customized. For example, IP configuration is performed on the VM and PM in the VPC by calling a corresponding API, and corresponding IP information is sent to the controller.

When a VM is communicatively connected to the system gateway, the VM may automatically acquire its corresponding IP address. When a PM communicates with the system gateway through the switch, the PM may also automatically acquire its corresponding IP address. Specifically, the above-mentioned IP configuration can be implemented by a DHCP (Dynamic Host Configuration Protocol) server in the system gateway. When the VM and PM are powered on, the VM and PM, as DHCP clients, interact with the DHCP server to acquire their corresponding IP addresses.

(a5) Establishing forwarding entries based on the IP addresses of the resources.

The process of establishing the forwarding entries includes: establishing a forwarding entry of the VM based on the IP address of the VM, and/or establishing a forwarding entry of the PM based on the IP address of the PM.

Therefore, the corresponding forwarding entries can be established through the process above-mentioned, and thus subsequent data transmission can be directly performed according to the forwarding entries.

The forwarding entry of the PM includes a source IP address of a source PM and a destination IP address of a destination PM, and the forwarding entry of the VM includes a source IP address of a source VM and a destination IP address of a destination VM.

(a6) Generating configuration information corresponding to the VPC based on the forwarding entries and the isolation label.

After acquiring the isolation label of the VPC of the tenant and the forwarding entry of the

VM and/or the forwarding entry of the PM in the VPC, the configuration information is generated (the configuration information includes the information of the forwarding entry of the VM and/or the forwarding entry of the PM, and the isolation label). After generating the configuration information, the controller sets the configuration information to the system gateway and the switch for use in data transmission (that is, data message forwarding).

In order to meet the diversified requirements of tenants, facilitate the tenants to control and manage the VPC, and improve the tenant's experience, in a possible embodiment, the controller is further configured to manage resources in the virtual private cloud VPC based on the configuration information. This management of resources includes the adding of resources and/or the removing of resources. That is, the tenants may add VMs or PMs into the VPC, or remove VMs and PMs in the VPC, through the controller.

In a specific implementation process, the controller is further configured for: (1) receiving a management operation request for resources in a VPC; wherein the management operation request contains an isolation label corresponding to the to-be-managed VPC; (2) modifying, according to the isolation label, configuration information corresponding to the to-be-managed VPC in the system gateway and the switch.

The resources in the VPC can be managed by modifying the configuration information. For example, in order to expand the VPC resources, configuration information corresponding to the expanded resources may be added in the system gateway and the switch, so as to realize the communication between the expanded VMs and PMs.

In a possible embodiment, the management operation request may include, but is not limited to, a request for adding a resource, a request for removing a part of resources, and a request for removing all of resources. Based on this, the controller is further configured for adding a forwarding entry corresponding to an IP address of a resource based on the request for adding a resource; and/or removing forwarding entries corresponding to IP addresses of the part of resources based on the request for removing the part of resources; and/or removing configuration information corresponding to the to-be-managed VPC based on the request for removing all of resources.

For example, the process of the controller processing the request for adding a resource includes:

(b1) Receiving a request for adding a resource, sent by a tenant, for resources in the VPC.

The request for adding a resource includes an isolation label corresponding to the to-be-added VPC.

For example, the tenant may, through a tenant terminal (which may be a mobile terminal or a computer), directly call a corresponding API or call a corresponding API by logging into a WEB console, to select and add a VM or PM into the VPC.

(b2) Adding a forwarding entry corresponding to an IP address of a resource based on a request for adding a resource.

That is, after adding resources (VM and/or PM) into the to-be-added VPC, forwarding entries are created for the corresponding VM and/or PM, and the forwarding entries are added into the configuration information of the to-be-added VPC.

(b3) Sending the updated configuration information to the system gateway and the switch.

Specifically, the configuration information can be generated according to the above-mentioned steps (a1) to (a6).

The process of the controller processing the request for removing a part of resources includes:

referring to the above steps (b1) and (b3), removing forwarding entries corresponding to to-be-removed resources in the VPC from the existing configuration information, and then sending the updated configuration information to the system gateway and the switch.

For the request for removing all of resources, the controller may directly control the system gateway and the switch to remove the configuration information of the to-be-managed VPC therein based on the isolation label in the request for removing all of resources.

In a possible embodiment, after receiving the request for removing all of resources or request for removing part of resources, the controller changes a VM and PM from a configured state to an unconfigured state through a host machine corresponding to the VM and an out-of-band management system corresponding to the PM, so as to facilitate subsequent reuse.

Therefore, by means of the isolation label, different VPCs of different tenants can be isolated without interfering with each other, which provides security policy protection capability for each VPC; at the same time, during removal and addition operations, it is possible to only update the configuration information of the VPC corresponding to the tenant without affecting

the configuration information of other tenants, which increases the flexibility of adding and removing VMs and PMs in the VPC by the tenants.

In summary, in specific applications, in data transmission between VM and PM, the function of the system gateway is as follows.

During transmission in a direction from the VM to the PM, the system gateway is configured for: receiving a first message of the VM, which includes an isolation label; finding configuration information corresponding to the isolation label based on the isolation label in the first message; and forwarding the first message to a corresponding switch based on the found configuration information.

During transmission in a direction from the PM to the VM, the system gateway is further configured for: receiving a second message of the switch, which includes an isolation label; finding configuration information corresponding to the isolation label based on the isolation label in the second message; and forwarding the second message to a target VM based on the found configuration information.

The function of the switch is as follows.

During transmission in the direction from the PM to the VM, the switch is configured for: receiving a third message of the PM, which includes an isolation label; finding configuration information corresponding to the isolation label based on the isolation label in the third message; and forwarding the third message to a corresponding system gateway based on the found configuration information.

During transmission in the direction from the VM to the PM, the switch is further configured for: receiving a fourth message of the system gateway, which includes an isolation label; finding configuration information corresponding to the isolation label based on the isolation label in the fourth message; and forwarding the fourth message to a target PM based on the found configuration information.

In order to facilitate the acquisition of corresponding data from a public network, in another embodiment, the virtual private cloud communication system may also be connected to the public network such as Internet. In a possible embodiment, as shown in FIG. 3, VMs in the virtual private cloud system are connected to the public network through a network gateway 30. PMs in the virtual private cloud system are connected to the public network through a

corresponding switch, system gateway, and network gateway 30 in turn.

In the above description of the system, two parts are mainly involved: implementation, configuration and management of the system gateway, and configuration management of the switch of the PM. However, in the virtual private cloud communication system in the present application, the communication between PMs and the communication between PM and other network elements (including VM and Internet) also play an important role in the network forwarding process. As the scale of the cloud environment increases, the load between communication devices will increase linearly. The switch is a wire speed forwarding device, and its load is mainly reflected in configuration and management under the large scale cloud environment. The system gateway is a gateway implemented by running software on X86, and its performance is not as good as that of the switch. The load of the system gateway is mainly reflected in network forwarding.

In an aspect of management and configuration of the switch, when the physical machine area formed by PMs is in an ultra-large-scale environment, the forwarding entries on the switch will be multiply. Furthermore, based on flooding prevention learning between devices, the broadcast storm will occur in the physical machine area and the corresponding bandwidth is consumed. At this time, if the switch only supports a two-layer forwarding device, that is, it is a two-layer forwarding device, in order to support communication across three layers between PMs, gateways required by all PMs will be implemented by the system gateway, that is, the communication must pass through the system gateway, which brings a heavy load to system gateway. Based on this, in the virtual private cloud communication system, the switches are three-layer switches that support a tunnel protocol and support three-layer forwarding, and synchronize forwarding entries between switches in cooperation with EVPN (Ethernet Virtual Private Network) technology, so as to transfer the gateways required by the PMs from the system gateway to the switches. Then the communication between PMs can be directly forwarded through the switch.

In an aspect of the forwarding performance of the system gateway, the forwarding performance of the system gateway is completely dependent on the implementation of the software architecture. Due to the huge and cumbersome network protocol stack of Linux, the Linux kernel forwarding is unsatisfactory in terms of the processing of network forwarding. A DPDK (Data Plane Development Kit) technology allows network forwarding logics to be

implemented in a tenant space of the Linux system, and allows a forwarding program of the system gateway to directly operate a network card by bypassing the Linux network protocol stack to obtain and send data messages, which can greatly improve data processing performance and throughput. Therefore, in the subsequent message forwarding process, the DPDK technology can be used.

The virtual private cloud system in the present application establishes a communication bridge among the physical machine area, the virtual machine area and the public network (such as Internet), so that the resources in the virtual machine area and the physical machine area can form a large scale of VPC without being limited to the upper limit of the number of VLAN IDs. At the same time, it can provide the security policy protection capability for the VPC, so that a tenant can flexibly allocate virtual machine and physical machine resources according to business requirements.

On the basis of the above-mentioned system embodiments, an embodiment of the present application also provides a method for configuring the virtual private cloud communication system. The method is applied to the controller in the above-mentioned system embodiments. As shown in FIG. 4, the method of configuring the virtual private cloud communication system includes:

S401, performing information configuration on a system gateway and a switch, respectively to generate configuration information; and

S402, sending the configuration information to the system gateway and the switch respectively,

wherein the configuration information includes an isolation label corresponding to the VPC, and forwarding entries corresponding to resources included in the VPC; the resources include: a VM and/or a PM.

The step 402 of generating configuration information includes: generating an isolation label corresponding to each virtual private cloud VPC based on the VPC; acquiring IP addresses of resources belonging to the same virtual private cloud VPC; establishing forwarding entries based on the IP addresses of the resources; and generating configuration information corresponding to the VPC according to the forwarding entries and the isolation label.

The step of establishing the forwarding entries based on the IP addresses of the resources includes: establishing the forwarding entry of the VM based on the IP address of the VM, and/or establishing the forwarding entry of the PM based on the IP address of the PM.

Furthermore, the above method further includes: managing the resources in the virtual private cloud VPC based on the configuration information; the managing of the resources includes: adding resources and/or removing resources.

Furthermore, the above method further includes: receiving a management operation request for the resources in the VPC, wherein the management operation request includes an isolation label corresponding to the to-be-managed VPC; and modifying, according to the isolation label, configuration information corresponding to the to-be-managed VPC in the system gateway and the switch.

Furthermore, the management operation request includes one or more of a request for adding a resource, a request for removing part of resources, and a request for removing all of resources. The above method further includes: adding a forwarding entry corresponding to an IP address of a resource based on the request for adding a resource; and/or removing, based on the request for removing part of resources, forwarding entries corresponding to IP addresses of the part of resources; and/or removing the configuration information corresponding to the to-be-managed VPC based on the request for removing all of resources.

Furthermore, based on the description of the management and configuration of the switch in the embodiment above-mentioned, the switch of the virtual private cloud communication system is a three-layer switch and supports the tunnel protocol. The method further includes: synchronizing forwarding entries between switches for the PM by an EVPN technology, to transfer a gateway required by the PM from the system gateway to the switch. After that, the communication between PMs can be directly forwarded through the switch, which effectively reduces the forwarding pressure of the system gateway.

Referring to FIG. 5, an embodiment of the present application further provides a controller 100, including: a processor 40, a memory 41, a bus 42 and a communication interface 43. The processor 40, the communication interface 43 and the memory 41 are connected through the bus 42. The processor 40 is configured to execute executable modules stored in the memory 41, such

as a computer program.

The memory 41 may include a random access memory (RAM), or may also include a non-volatile memory (NVM), for example at least one disk memory. The communication connection between the network elements of the system and at least one of other network elements is implemented through at least one communication interface 43 (which may be wired or wireless), such as Internet, wide area network, local network, metropolitan area network, and the like.

The bus 42 may be an ISA bus, a PCI bus, an EISA bus, or the like. The bus may include an address bus, a data bus, a control bus, or the like. For representation, the bus is represented by only one bidirectional arrow in FIG. 5, which does not mean there is only one bus or one type of bus.

The memory 41 is used to store a program. The processor 40 executes the program after receiving an execution instruction. The method executed by an apparatus defined in a flow disclosed in any of the foregoing embodiments of the present application can be applied in the processor 40, or implemented by the processor 40.

The processor 40 may be an integrated circuit chip with a signal processing function. In the implementation process, each step of the above method may be completed by an integrated logic circuit in the form of hardware or instructions in the form of software in the processor 40. The processor 40 may be a general-purpose processor, including a central processing unit (CPU), a network processor (NP), or the like. It may also be a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field-programmable gate array (FPGA) or other programmable logic devices, discrete gates or transistor logic devices, discrete hardware components. The methods, steps, and logical blocks disclosed in the embodiments of the present application can be implemented or executed. The general-purpose processor may be a microprocessor or any conventional processor or the like. The steps of the method disclosed in the embodiments of the present application may be directly executed by a hardware coding processor, or executed by a combination of hardware and software modules in the coding processor. The software module may be located in a storage medium known in the prior art, such as a random access memory, flash memory, read-only memory, programmable read-only memory, electrically erasable programmable memory, register, and the like. The storage medium is located in the memory 41, and the processor 40 reads the information in the memory 41, and

performs the steps of the above method in combination with its hardware.

The method for configuring the virtual private cloud communication system and the controller according to the embodiments of the present application have the same technical features as the virtual private cloud communication system provided in the above embodiments, thereby solving the same technical problems and producing the same technical effects.

An embodiment of the present application also provides a computer-readable storage medium having stored a computer program therein, which is executed to implement the method for configuring the virtual private cloud communication system described in the foregoing method embodiments.

A computer program product for performing the method provided by an embodiment of the present application includes a non-volatile computer-readable storage medium storing executable program codes by a processor. Instructions included in the program codes can be executed to implement the method for configuring the virtual private cloud communication system described in the method embodiments. For specific implementation, please refer to the method embodiments, which will not be repeated here.

Those skilled in the art can clearly understand that, for convenience and conciseness of the description, the specific operation process of the method and the controller described above can refer to the corresponding process in the foregoing system embodiments, which will not be repeated here.

The flowchart and block diagram in the accompanying drawings show possible implementation of the method and a system architecture, functions, and operations of the computer program product according to multiple embodiments of the present application. In this regard, each block in the flowchart and the block diagram represents one module, part of code or program segment, which contains one or more executable instructions for implementing specified logical functions. It should also be noted that in some alternative implementations, the functions shown in the blocks may also implemented in a different order from that shown in the drawings. For example, two continuous blocks may actually be executed substantially in parallel, and they may sometimes be executed in a reverse order, depending on the functions involved. It should also be noted that, each block in the flowchart and the block diagram, and a combination of blocks in the flowchart and the block diagram may be implemented in a dedicated hardware-based system that performs specified functions or actions, or may be implemented by a

combination of dedicated hardware and computer instructions.

In the description of this application, it should be noted that the orientation or position relationship indicated by the terms "center", "upper", "lower", "left", "right", "vertical", "horizontal", "inner", "outer", etc. is based on the orientation or position relationship shown in the drawings, and is only for the convenience of describing the present application and simplifying the description, and does not indicate or imply that apparatuses or elements must have a specific orientation and be constructed and operated in a specific orientation, so it cannot be understood as a limitation on the present application. In addition, the terms "first", "second", and "third" are only used for description, and are not intended to indicate or imply relative importance. Unless otherwise specified, the relative steps, numerical expressions and numerical values of the steps and the components set forth in these embodiments do not limit the scope of the present application.

It should be understood that in the embodiments herein, the disclosed system and method can be implemented in other ways. The apparatus embodiments described above are merely illustrative. For example, the units are differentiated in logical functions. In practice, the units are differentiated in other ways. For example, a plurality of units or components can be combined or integrated into another system, or some features can be ignored or not executed. Further, the coupling, direct coupling or communication connection shown or described above may be indirect coupling or communication connection between the communication interfaces, apparatus or units, and may be electrical connections, mechanical connections or other forms of connections.

The units illustrated as separate components may or may not be physically separated. The components shown as units may or may not be physical units, and may be located on one unit or may be distributed on a plurality of units. Some or all of the units can be selected from the units above according to actual needs to achieve the objective of the solution of the embodiments.

In addition, all the functional units in the embodiments of the present application may be integrated in one processing unit, or each of the units may be an individual unit, or two or more units may be integrated in one unit.

When the function is implemented as a software function unit and is sold or used as an independent product, the integrated unit can be stored in a non-volatile computer readable storage medium executable by processor. In view of this, the technical solution of the present

disclosure or a part contributing to the prior art or the part of the technical solution can be embodied essentially in the form of a software product. The computer software product is stored in one storage medium, including several instructions to cause one computer device (which may be a personal computer, a server, a network device, or the like) to perform all or part of steps of the method of the embodiment of the present disclosure. The storage medium includes a medium capable of storing program code, such as a USB flash disk, a mobile hard disk, a Read Only Memory (ROM), a Random Access Memory (RAM), a magnetic disk, or an optical disk.

Finally, it should be noted that the above-mentioned embodiments are only preferred implementations of the present application, which are used to illustrate the technical solution of the present application, and are not intended to limit the present application. The scope of protection of this application is not limited thereto. Although the application is described in detail with reference to the above-mentioned embodiments, it should be understood that a person of ordinary skill in the art can modify the technical solutions described in the foregoing embodiments within the technical scope disclosed in the present application, or can be easily conceived of changes, or equivalent replacements of some of the technical features. These modifications, changes or replacements do not make the corresponding technical solutions depart from the spirit and scope of the technical solutions of the embodiments of this application, and should be fall into the scope of protection in the present application. Therefore, the protection scope of the present application shall be embodied by the protection scope of the claims.

The embodiments described above are simply preferable embodiments of the present application, and are not intended to limit the scope of protection of the present application. Any modifications, alternatives, improvements, or the like within the spirit and principle of the present application shall be included within the scope of protection of the present application.

CLAIMS

What is claimed is:

1. A virtual private cloud communication system, comprising: at least one virtual machine (VM) and a system gateway communicatively connected to each of the VM;
at least one physical machine (PM), and a switch communicatively connected to each of the PM;
wherein the system gateway is communicatively connected to the switch;
the system gateway and the switch are configured for enabling communication between the VM and the PM belonging to a same virtual private cloud (VPC) based on preset configuration information.
2. The system of claim 1, wherein,
the configuration information comprises an isolation label corresponding to the VPC, and forwarding entries corresponding to resources comprised in the VPC;
the resources comprise: a VM(s) and/or a PM(s).
3. The system of claim 1, further comprising a controller;
wherein the controller is communicatively connected to the system gateway and the switch, respectively;
the controller is configured for performing information configuration on the system gateway and the switch, respectively, to generate configuration information, and sending the configuration information to the system gateway and the switch, respectively.
4. The system of claim 3, wherein the controller is further configured for:
generating an isolation label corresponding to each virtual private cloud (VPC) based on the VPC;
acquiring IP addresses of resources belonging to the same virtual private cloud (VPC), wherein the resources comprise a VM(s) and/or a PM(s);
establishing forwarding entries based on the IP addresses of the resources;
generating configuration information corresponding to the VPC based on the forwarding entries and the isolation label.
5. The system of claim 4, wherein the controller is further configured for:

establishing a forwarding entry(s) of the VM(s) based on the IP address of the VM(s),
and/or

establishing a forwarding entry(s) of the PM(s) based on the IP address of the PM(s).

6. The system of claim 3, wherein the controller is further configured for:

managing the resources in the virtual private cloud (VPC) based on the configuration information, wherein the resources include the VM(s) and/or the PM(s), and the managing comprises: adding resources and/or removing resources.

7. The system of claim 6, wherein the controller is further configured for:

receiving a management operation request for the resources in the VPC, wherein the management operation request comprises an isolation label corresponding to a to-be-managed VPC; and

modifying configuration information corresponding to the to-be-managed VPC in the system gateway and the switch according to the isolation label.

8. The system of claim 7, wherein the controller is further configured for:

adding, based on a request for adding a resource, a forwarding entry corresponding to an IP address of the resource; and/or

removing, based on a request for removing part of the resources, forwarding entries corresponding to IP addresses of the part of the resources; and/or

removing the configuration information corresponding to the to-be-managed VPC based on a request for removing all of the resources.

9. The system of claim 2, wherein the system gateway is configured for:

receiving a first message of the VM, wherein the first message comprises an isolation label;

finding configuration information corresponding to the isolation label in the first message based on the isolation label, and forwarding the first message to a corresponding switch based on the found configuration information;

the system gateway is further configured for:

receiving a second message of the switch, wherein the second message comprises an isolation label;

finding configuration information corresponding to the isolation label in the second

message based on the isolation label, and forwarding the second message to a target VM based on the found configuration information.

10. The system of claim 2, wherein the switch is configured for:

receiving a third message of the PM, wherein the third message comprises an isolation label;

finding configuration information corresponding to the isolation label in the third message based on the isolation label, and forwarding the third message to a corresponding system gateway based on the found configuration information;

the switch is further configured for:

receiving a fourth message of the system gateway, wherein the fourth message comprises an isolation label;

finding configuration information corresponding to the isolation label in the fourth message based on the isolation label, and forwarding the fourth message to a target PM based on the found configuration information.

11. The system of any one of claims 1-10, wherein the system gateway is implemented by running corresponding software in a server.

12. A method for configuring a virtual private cloud communication system, which is applied to the controller in the system of any one of claims 1-11, wherein the controller is communicatively connected to the system gateway and the switch, respectively; the method comprises:

performing information configuration on the system gateway and the switch, respectively, to generate configuration information; and

sending the configuration information to the system gateway and the switch, respectively;

wherein the configuration information comprises an isolation label corresponding to a VPC, and forwarding entries corresponding to resources comprised in the VPC, wherein the resources comprises a VM(s) and/or a PM(s).

13. The method of claim 12, wherein generating the configuration information comprises:

generating an isolation label corresponding to each virtual private cloud (VPC) based on the VPC;

acquiring IP addresses of resources belonging to a same virtual private cloud (VPC), wherein the resources comprises a VM(s) and/or a PM(s);

establishing forwarding entries based on the IP addresses of the resources; and

generating configuration information corresponding to the VPC based on the forwarding entries and the isolation label.

14. The method of claim 13, wherein establishing the forwarding entries based on the IP addresses of the resources comprises:

establishing a forwarding entry(s) of the VM(s) based on the IP address of the VM(s), and/or

establishing a forwarding entry(s) of the PM(s) based on the IP address of the PM(s).

15. The method of claim 12, further comprising:

managing the resources in the virtual private cloud (VPC) based on the configuration information, wherein the resources comprise a VM(s) and/or a PM(s), and the managing comprises: adding resources and/or removing resources.

16. The method of claim 15, further comprising:

receiving a management operation request for the resources in the VPC, wherein the management operation request comprises an isolation label corresponding to a to-be-managed VPC; and

modifying configuration information corresponding to the to-be-managed VPC in the system gateway and the switch according to the isolation label.

17. The method of claim 16, wherein the management operation request comprises one or more of a request for adding a resource, a request for removing part of the resources, and a request for removing all of the resources, and the method further comprises:

adding, based on the request for adding a resource, a forwarding entry corresponding to an IP address of the resource; and/or

removing, based on the request for removing part of the resources, forwarding entries corresponding to IP addresses of the part of the resources; and/or

removing the configuration information corresponding to the to-be-managed VPC based on the request for removing all of the resources.

18. A controller, comprising a memory and a processor, wherein the memory stores a computer program that can be run on the processor, and the processor executes the computer program to implement the method of any one of claims 12-17.

19. A computer-readable storage medium having stored a computer program thereon, wherein, the computer program is executed by a processor, so as to cause the processor to implement the method of any one of claims 12-17.

20. An application which, when executed, implements the method of any one of claims 12-17.