

VIRTUAL PRIVATE CLOUD VPC INTERWORKING IMPLEMENTATION SYSTEM AND METHOD

TECHNICAL FIELD

[0001] One or more embodiments of this specification relate to the field of network
5 technologies, and in particular, to a virtual private cloud VPC interworking implementation system
and method.

BACKGROUND

[0002] In a current cloud computing environment, a virtual private cloud (VPC) has become a
common network architecture mode. Each VPC corresponds to one virtual network, can be
10 independently provided with network configurations such as an internet protocol (IP) address
range, a routing table, and a security group, and are mutually isolated from another VPC.

[0003] In a related technology, it is considered by default that different VPCs cannot be
accessed by each other. Therefore, in some cases, different VPCs may need to be interworked, to
implement across-VPC traffic forwarding and data transmission.

15 [0004] However, VPC interworking increases a security risk and management complexity.
Therefore, a virtual private cloud interworking solution is urgently needed, to improve security
and reliability of cross-VPC network communication when different VPCs are interworked.

SUMMARY

[0005] In view of this, one or more embodiments of this specification provide a virtual private
20 cloud VPC interworking implementation system and method.

[0006] To achieve the above-mentioned objectives, one or more embodiments of this
specification provide the following technical solutions.

[0007] According to a first aspect of one or more embodiments of this specification, a virtual
private cloud VPC interworking implementation system is provided, including a source VPC, a
25 relay VPC, and a target VPC.

- [0008] The source VPC is configured to send access traffic to the relay VPC.
- [0009] The relay VPC is configured to send, to the target VPC, the access traffic sent by the source VPC.
- [0010] The target VPC is configured to receive the access traffic sent by the relay VPC.
- 5 [0011] According to a second aspect of one or more embodiments of this specification, a virtual private cloud VPC interworking method is provided, including:
- [0012] A source VPC sends access traffic to a relay VPC.
- [0013] The relay VPC is configured to send, to the target VPC, the access traffic sent by the source VPC.
- 10 [0014] The target VPC is configured to receive the access traffic sent by the relay VPC.
- [0015] According to the solution provided in this specification, a relay VPC is introduced between a source VPC and a target VPC, the source VPC can send access traffic to the relay VPC, and the relay VPC forwards the access traffic to the target VPC, so that the target VPC can receive the access traffic sent by the source VPC, to implement communication between the source VPC
- 15 and the target VPC when network isolation is formed between the source VPC and the target VPC. In this way, networks of the source VPC and the target VPC are not exposed to each other, and security and reliability of network communication between the source VPC and the target VPC are improved.

BRIEF DESCRIPTION OF DRAWINGS

- 20 [0016] FIG. 1 shows a VPC interworking implementation system according to an example embodiment;
- [0017] FIG. 2 shows a VPC interworking implementation system according to an example embodiment;
- [0018] FIG. 3 shows a VPC interworking implementation system according to an example
- 25 embodiment; and
- [0019] FIG. 4 is a flowchart of a virtual private cloud VPC interworking method according to an example embodiment.

DESCRIPTION OF EMBODIMENTS

[0020] Example embodiments are described in detail here, and examples of the example embodiments are presented in the accompanying drawings. When the following description relates to the accompanying drawings, unless specified otherwise, same numbers in different
5 accompanying drawings represent same or similar elements. Implementations described in the following example embodiments do not represent all implementations consistent with one or more embodiments of this specification. On the contrary, the implementations are merely examples of apparatuses and methods that are described in the appended claims in detail and consistent with some aspects of one or more embodiments of this specification.

10 [0021] It is worthwhile to note that, in some other embodiments, the steps of the corresponding method are not necessarily performed in the order shown and described in this specification. In some other embodiments, the method can include more or fewer steps than those described in this specification. In addition, a single step described in this specification may be decomposed into a plurality of steps in some other embodiments for description; and a plurality of steps described in
15 this specification may be combined into a single step for description in some other embodiments.

[0022] User information (including but not limited to user device information, personal information of a user, etc.) and data (including but not limited to data used for analysis, stored data, displayed data, etc.) used in this specification are information and data that are authorized by the user or fully authorized by each party, related data needs to be collected, used, and processed by
20 abiding by related laws and regulations and standards of a related country and region, and a corresponding operation entry is provided, so that the user chooses to perform authorization or rejection.

[0023] In a related technology, as a virtual network environment, a VPC can be configured to construct and manage a private network of a user in a public cloud platform, to provide a plurality
25 of functions such as secure isolation, network customization, cross-regional interconnection, flexibility, and scalability in the public cloud environment, and help the user construct a private, secure, flexible, and reliable cloud network environment, so as to satisfy various service requirements of the user.

[0024] A public cloud environment used to provide a database (DB) service is used as an
30 example. The database service can be deployed in a VPC maintained by a database public cloud

service provider. An application (APP) that is of a client and that uses the database service can be deployed in a VPC maintained by the client. If the app of the client needs to use a database service provided by the database public cloud service provider, the VPC maintained by the database public cloud service provider needs to be interworked with the VPC maintained by the client, to
5 implement cross-VPC use of the database.

[0025] However, if the two VPCs are directly interworked, networks of the two VPCs are exposed to each other, and a security risk is posed.

[0026] In view of this, this specification expects to provide a virtual private cloud VPC interworking implementation system and method, to implement communication between a source
10 VPC and a target VPC when network isolation is formed between the source VPC and the target VPC. In this way, networks of the source VPC and the target VPC are not exposed to each other, and security and reliability of network communication between the source VPC and the target VPC are improved.

[0027] Optionally, the solution provided in this specification can be applied not only to a
15 network environment used to provide a database service, but also to another network environment used to provide different service functions. A specific application scenario is not limited in this specification.

[0028] The following describes in detail the virtual private cloud VPC interworking implementation system and method provided in this specification.

[0029] FIG. 1 shows a VPC interworking implementation system according to an example
20 embodiment. As shown in FIG. 1, the VPC interworking implementation system can include a source VPC, a relay VPC, and a target VPC.

[0030] The source VPC is configured to send access traffic to the relay VPC. The relay VPC is configured to send, to the target VPC, the access traffic sent by the source VPC. The target VPC
25 is configured to receive the access traffic sent by the relay VPC.

[0031] Optionally, the source VPC and the relay VPC can be connected through a private connection, and the relay VPC and the target VPC can be connected through a private connection.

[0032] The private connection can be a virtual private cloud peering connection (VPC peering). VPC peering can be used to implement a network connection between two VPCs. Through this
30 connection, traffic can be routed between two VPCs by using a private internet protocol version 4 (IPv4) address or a private internet protocol version 6 (IPv6) address, so that instances of the two

VPCs can communicate with each other, as the instances are in the same network.

[0033] VPC peering is used to implement a connection between the source VPC and the relay VPC and a connection between the relay VPC and the target VPC, and a feature that a route between VPCs that is implemented through VPC peering has no transitivity can be fully used, to
5 implement mutual isolation between the source VPC and the target VPC.

[0034] After the source VPC and the relay VPC are connected through VPC peering, and the relay VPC and the target VPC are connected through VPC peering, the source VPC and the relay VPC can directly access each other through the VPC peering, and the relay VPC and the target VPC can directly access each other through VPC peering. However, the source VPC and the target
10 VPC cannot directly access each other through VPC peering. In other words, a virtual machine (VM) in the source VPC cannot directly implement internal access to a VM in the target VPC, to implement mutual isolation between the source VPC and the target VPC.

[0035] Optionally, network middleware can be introduced into the relay VPC, to provide a traffic forwarding function by using the network middleware.

[0036] In some embodiments, when the relay VPC sends, to the target VPC, the access traffic sent by the source VPC, the relay VPC can send, to the target VPC by using network middleware, the access traffic sent by the source VPC.
15

[0037] For example, an app in the source VPC can send access traffic to the network middleware in the relay VPC. The network middleware in the relay VPC can forward the access traffic to a corresponding service in the target VPC, so that the service in the target VPC can receive the access traffic.
20

[0038] The network middleware can be a proxy server (Proxy), or the network middleware can be a load balancer (LB).

[0039] That network middleware is used as a proxy server is taken as an example. FIG. 2 shows a VPC interworking implementation system according to an example embodiment. As shown in FIG. 2, an app in a source VPC can send access traffic to a proxy server (namely, a proxy) in a relay VPC, and the proxy in the relay VPC can forward the access traffic to a corresponding service in a target VPC, so that the service in the target VPC can receive the access traffic.
25

[0040] That network middleware is a load balancer is taken as an example. FIG. 3 shows a VPC interworking implementation system according to an example embodiment. As shown in FIG. 3, an app in a source VPC can send access traffic to a load balancer (namely, the LB) in a relay
30

VPC, and the LB in the relay VPC can forward the access traffic to a corresponding service in a target VPC, so that the service in the target VPC can receive the access traffic.

[0041] In some embodiments, the relay VPC can provide a traffic filtering capability in addition to a role of connecting the source VPC and the target VPC. For example, network
5 middleware in the relay VPC can filter the access traffic, to ensure that only access traffic encapsulated based on a target protocol (for example, a specific protocol) can pass.

[0042] Optionally, the access traffic can be network traffic encapsulated based on the target protocol, and the target protocol can be used to indicate a data transmission format of the access traffic. A VPC interworking implementation system in a public cloud environment used to provide
10 a database service is used as an example. The target protocol can be a structured query language (MySQL) access protocol, or the target protocol can be an Oracle access protocol, but is not limited thereto. A specific type of the target protocol is not limited in this specification.

[0043] In some embodiments, the relay VPC can forward the access traffic to a target port (for example, a specific protocol port) of the target VPC, so that the target VPC can receive, through
15 the target port, the access traffic sent by the relay VPC. The target port can be a network port dedicated to receiving access traffic.

[0044] Based on the above-mentioned system, a connection between the source VPC and the target VPC can be implemented in the following virtual private cloud VPC interworking method.

[0045] It is worthwhile to note that, the above-mentioned embodiment is described by using
20 an example in which the relay VPC is used to connect one source VPC and one target VPC. In more possible implementations, the relay VPC can connect more source VPCs and more target VPCs. In other words, one relay VPC can implement interworking between a plurality of source VPCs and a plurality of target VPCs.

[0046] For example, for a plurality of source VPCs and a plurality of target VPCs whose
25 network address segments do not overlap, one relay VPC can be used to implement interworking between the plurality of source VPCs and the plurality of target VPCs. However, if network address segments of the source VPC and the target VPC that need to be interworked overlap, interworking between the source VPC and the target VPC can be implemented by using different relay VPCs.

[0047] In other words, the relay VPC can be configured to connect a plurality of source VPCs
30 and a plurality of target VPCs whose network address segments do not overlap. For a VPC whose

network address segment overlaps with that of an existing VPC, a new relay VPC can be created separately to implement VPC interworking.

[0048] FIG. 4 is a flowchart of a virtual private cloud VPC interworking method according to an example embodiment. As shown in FIG. 4, the method includes steps 401 to 403.

5 **[0049]** Step 401: A source VPC sends access traffic to a relay VPC.

[0050] It is worthwhile to note that the source VPC and the relay VPC can be deployed in the same public cloud environment.

[0051] Optionally, the access traffic can be any type of network traffic. For example, the access traffic can be database service traffic, file transfer traffic, email traffic, video traffic, voice traffic,
10 real-time communication traffic, or network management traffic. A specific type of the access traffic is not limited in this specification.

[0052] The database service traffic can be traffic generated when an application interacts with a database service. The file transfer traffic can be traffic generated when a file is uploaded and/or downloaded based on a file transfer protocol (FTP) or in another file transfer manner. The email
15 traffic can be traffic generated when an email is sent and/or received based on an email protocol. The video traffic can be traffic generated when video content is transmitted based on a streaming media protocol. The voice traffic can be voice communication traffic generated based on a voice over internet protocol (VoIP) or by using a real-time voice communication application. The real-time communication traffic can be traffic generated by an instant messaging service (for example,
20 instant messaging, a voice call, or a video call). The network management traffic can be traffic used to manage a network running status in a network running process.

[0053] That the access traffic is database service traffic is taken as an example. The database service traffic can include but is not limited to database query traffic, database write traffic, database connection traffic, database backup traffic, database transaction traffic, database
25 management traffic, and database security traffic. The database service traffic is not limited thereto.

[0054] The database query traffic can be traffic generated when an application sends a query request to a database. The database write traffic can be traffic generated when an application performs an insert, update, or delete operation on the database. The database connection traffic can be traffic generated when an application establishes a connection with the database. The database
30 backup traffic can be traffic generated when the database performs a backup operation. The database transaction traffic can be traffic generated when an application performs a transaction

operation. The database management traffic can be traffic used to monitor and manage performance and a status of the database. The database security traffic can be communication traffic related to database security, including but not limited to traffic generated when performing data transmission during authentication and authorization, and traffic generated during encryption and decryption operations.

[0055] Step 402: The relay VPC sends, to a target VPC, the access traffic sent by the source VPC.

[0056] It is worthwhile to note that the relay VPC can serve as a relay station between the source VPC and the target VPC, so that the traffic sent by the source VPC is bridged to the target VPC, to avoid direct interworking between the source VPC and the target VPC when communication between the source VPC and the target VPC is implemented. In this way, network isolation is formed between the source VPC and the target VPC, to effectively cope with a network attack.

[0057] Step 403: The target VPC receives the access traffic sent by the relay VPC.

[0058] According to the virtual private cloud VPC interworking method provided in this specification, the source VPC can send access traffic to the relay VPC, and the relay VPC forwards the access traffic to the target VPC, so that the target VPC can receive the access traffic sent by the source VPC, to implement communication between the source VPC and the target VPC when network isolation is formed between the source VPC and the target VPC. In this way, networks of the source VPC and the target VPC are not exposed to each other, and security and reliability of network communication between the source VPC and the target VPC are improved.

[0059] After a basic implementation procedure of the virtual private cloud VPC interworking method provided in this specification is described, the following describes in detail each optional implementation of this specification.

[0060] In some embodiments, a source VPC and a relay VPC can be connected through a private connection, and the relay VPC and a target VPC can be connected through a private connection. The source VPC can send access traffic to the relay VPC through the private connection. The relay VPC can send, to the target VPC through the private connection, the access traffic sent by the source VPC. The target VPC can receive, through the private connection, the access traffic sent by the relay VPC.

[0061] The private connection can be VPC peering. VPC peering can be used to implement a

network connection between two VPCs. Through this connection, traffic can be routed between two VPCs by using a private IPv4 address or a private IPv6 address, so that instances of the two VPCs can communicate with each other, as the instances are in the same network.

[0062] VPC peering is used to implement a connection between the source VPC and the relay VPC and a connection between the relay VPC and the target VPC, and a feature that a route between VPCs that is implemented through VPC peering has no transitivity can be fully used, to implement mutual isolation between the source VPC and the target VPC.

[0063] After the source VPC and the relay VPC are connected through VPC peering, and the relay VPC and the target VPC are connected through VPC peering, the source VPC and the relay VPC can directly access each other through the VPC peering, and the relay VPC and the target VPC can directly access each other through VPC peering. However, the source VPC and the target VPC cannot directly access each other through VPC peering. In other words, a virtual machine (VM) in the source VPC cannot directly implement internal access to a VM in the target VPC, to implement mutual isolation between the source VPC and the target VPC.

[0064] Optionally, the relay VPC can include network middleware, to provide a traffic forwarding function by using the network middleware.

[0065] In some embodiments, when the relay VPC sends, to the target VPC, the access traffic sent by the source VPC, the relay VPC can send, to the target VPC by using network middleware, the access traffic sent by the source VPC.

[0066] For example, an app in the source VPC can send access traffic to the network middleware in the relay VPC. The network middleware in the relay VPC can forward the access traffic to a corresponding service in the target VPC, so that the service in the target VPC can receive the access traffic.

[0067] The network middleware can be a proxy server or a load balancer.

[0068] That network middleware is used as a proxy server is taken as an example. An app in a source VPC can send access traffic to a proxy server (namely, a proxy) in a relay VPC, and the proxy in the relay VPC can forward the access traffic to a corresponding service in a target VPC, so that the service in the target VPC can receive the access traffic.

[0069] That network middleware is a load balancer is taken as an example. An app in a source VPC can send access traffic to a load balancer (namely, the LB) in a relay VPC, and the LB in the relay VPC can forward the access traffic to a corresponding service in a target VPC, so that the

service in the target VPC can receive the access traffic.

[0070] In some embodiments, the relay VPC can further filter the received access traffic, to ensure that only access traffic encapsulated based on a target protocol (for example, a specific protocol) can pass.

5 **[0071]** Optionally, the access traffic can be network traffic encapsulated based on the target protocol, and the target protocol can be used to indicate a data transmission format of the access traffic. A VPC interworking implementation system in a public cloud environment used to provide a database service is used as an example. The target protocol can be a MySQL access protocol, or the target protocol can be an Oracle access protocol, but is not limited thereto. A specific type of
10 the target protocol is not limited in this specification.

[0072] In some embodiments, the relay VPC can forward the access traffic to a target port (for example, a specific protocol port) of the target VPC, so that the target VPC can receive, through the target port, the access traffic sent by the relay VPC. The target port can be a network port dedicated to receiving access traffic.

15 **[0073]** According to the solution provided in this specification, the relay VPC can be used to implement mutual access between the source VPC and the relay VPC and mutual access between the relay VPC and the target VPC. However, the source VPC and the target VPC cannot be interworked directly, to form network isolation between the source VPC and the target VPC, avoid mutual exposure of networks of the source VPC and the target VPC, and improve network security.

20 **[0074]** In addition, the network middleware is introduced into the relay VPC, to implement forwarding bridging of the access traffic. When a connection between VPCs is implemented, the access traffic can be filtered, to ensure that only traffic encapsulated based on a specific protocol can pass and be forwarded to a specific protocol port in the target VPC. The target VPC needs to expose only the specific protocol port, to effectively cope with over-exposure of a virtual machine
25 and a service in the target VPC, and further improve network security.

[0075] In addition, the relay VPC and the network middleware are introduced, to form a network interworking solution with a security isolation capability. A client only needs to operate the source VPC and the target VPC for interworking, and does not need to sense presence of the relay VPC, so that network isolation between the source VPC and the target VPC is implemented
30 without sensing by the client.

[0076] The system illustrated in the embodiments may be specifically implemented by a

computer chip or an entity, or may be implemented by a product having a specific function. A typical implementation device is a computer, and a specific form of the computer may be a personal computer, a laptop computer, a cellular phone, a camera phone, a smartphone, a personal digital assistant, a media player, a navigation device, an e-mail transceiver device, a game console, a tablet
5 computer, a wearable device, or any combination of several devices in these devices.

[0077] In a typical configuration, the computer includes one or more processors (central processing unit, CPU), one or more input/output interfaces, one or more network interfaces, and one or more memories.

[0078] The memory may include a non-persistent memory, a random access memory (RAM),
10 a nonvolatile memory, and/or another form in a computer-readable medium, for example, a read-only memory (ROM) or a flash memory (flash RAM). The memory is an example of the computer-readable medium.

[0079] The computer-readable medium includes a persistent and a non-persistent, removable and non-removable media, which implement information storage by using any method or
15 technology. The information may be a computer-readable instruction, a data structure, a program module, or other data. Examples of a computer storage medium include but are not limited to: a phase change random access memory (PRAM), a static random access memory (SRAM), a dynamic random access memory (DRAM), another type of random access memory (RAM), a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a
20 flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital video disc (DVD) or another optical storage, a magnetic cassette, a magnetic storage, a quantum memory, a graphene-based storage medium or another magnetic storage device, or any other non-transmission medium. The computer storage medium can be configured to store information that can be accessed by a computing device. Based on the definition in this
25 specification, the computer-readable medium does not include transitory computer-readable media (Transitory Media) such as a modulated data signal and carrier.

[0080] It is worthwhile to further note that, the terms "include", "comprise", or any other variant thereof are intended to cover a non-exclusive inclusion, so that a process, a method, a product, or a device that includes a list of elements not only includes those elements but also
30 includes other elements which are not expressly listed, or further includes elements inherent to such process, method, product or device. Without more constraints, an element preceded by

"includes a ..." does not preclude the existence of additional identical elements in the process, method, product or device that includes the element.

5 [0081] Specific embodiments of this specification are described above. Other embodiments fall within the scope of the appended claims. In some cases, the actions or steps described in the claims can be performed in an order different from that in the embodiments, and the desired results can still be achieved. In addition, the process depicted in the accompanying drawings does not necessarily need a particular order or consecutive order to achieve the desired results. In some implementations, multi-tasking and parallel processing are feasible or may be advantageous.

10 [0082] Terms used in one or more embodiments of this specification are merely used to describe specific embodiments, and are not intended to limit the one or more embodiments of this specification. The terms "a" and "the" of singular forms used in one or more embodiments of this specification and the appended claims are also intended to include plural forms, unless otherwise specified in the context clearly. It should be further understood that the term "and/or" used in this specification indicates and includes any or all possible combinations of one or more associated
15 listed items.

[0083] It should be understood that although terms "first", "second", "third", etc. may be used in one or more embodiments of this specification to describe various types of information, the information should not be limited to these terms. These terms are used merely to differentiate information of the same type. For example, without departing from the scope of one or more
20 embodiments of this specification, first information can also be referred to as second information, and similarly, the second information can also be referred to as the first information. Depending on the context, for example, the word "if" used here can be explained as "while", "when", or "in response to determining".

[0084] The above-mentioned descriptions are merely example embodiments of one or more
25 embodiments of this specification, but are not intended to limit the one or more embodiments of this specification. Any modification, equivalent replacement, improvement, etc. made without departing from the spirit and principle of the one or more embodiments of this specification shall fall within the protection scope of the one or more embodiments of this specification.

CLAIMS

What is claimed is:

1. A virtual private cloud VPC interworking implementation system, comprising a source VPC, a relay VPC, and a target VPC, wherein
 - 5 the source VPC is configured to send access traffic to the relay VPC;
 - the relay VPC is configured to send, to the target VPC, the access traffic sent by the source VPC; and
 - the target VPC is configured to receive the access traffic sent by the relay VPC.
2. The system according to claim 1, wherein the relay VPC comprises network middleware;
 - 10 and
 - the relay VPC is configured to send, to the target VPC through the network middleware, the access traffic sent by the source VPC, wherein the network middleware is a proxy server or a load balancer.
3. The system according to claim 1, wherein the target VPC is configured to receive, through
 - 15 a target port, the access traffic sent by the relay VPC, wherein
 - the target port is a network port dedicated to receiving access traffic.
4. The system according to claim 1, wherein the access traffic is network traffic encapsulated based on a target protocol, and the target protocol is used to indicate a data transmission format of the access traffic.
- 20 5. The system according to claim 1, wherein the source VPC and the relay VPC are connected through a private connection, and the relay VPC and the target VPC are connected through a private connection.
6. A virtual private cloud VPC interworking method, comprising:
 - sending, by a source VPC, access traffic to a relay VPC;
 - 25 sending, by the relay VPC to a target VPC, the access traffic sent by the source VPC; and
 - receiving, by the target VPC, the access traffic sent by the relay VPC.
7. The method according to claim 6, wherein the relay VPC comprises network middleware;
 - and
 - the sending, by the relay VPC to a target VPC, the access traffic sent by the source VPC
 - 30 comprises:

sending, by the relay VPC to the target VPC through the network middleware, the access traffic sent by the source VPC, wherein the network middleware is a proxy server or a load balancer.

8. The method according to claim 6, wherein the receiving, by the target VPC, the access traffic sent by the relay VPC comprises:

5 receiving, by the target VPC through a target port, the access traffic sent by the relay VPC, wherein

the target port is a network port dedicated to receiving access traffic.

9. The method according to claim 6, wherein the access traffic is network traffic encapsulated based on a target protocol, and the target protocol is used to indicate a data transmission format of
10 the access traffic.

10. The method according to claim 6, wherein the source VPC and the relay VPC are connected through a private connection, and the relay VPC and the target VPC are connected through a private connection; and

the method comprises:

15 sending, by the source VPC, the access traffic to the relay VPC through the private connection;
 sending, by the relay VPC through the private connection to the target VPC, the access traffic sent by the source VPC; and

 receiving, by the target VPC through the private connection, the access traffic sent by the relay VPC.

20