Alibaba Cloud VPN Gateway

Best Practices

Issue: 20190918

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

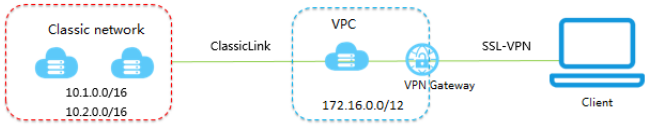
Contents

1 Use SSL-VPN in the classic network

1.1 Access cloud resources in a classic network from a Linux client

This topic describes how to use the SSL-VPN function of a VPN Gateway to access cloud resources deployed in a classic network from a Linux client.

Note that if you have configured the SSL-VPN, you only need to complete Step 5.



Prerequisites

Before you begin, the following conditions must be met:

- The Linux client can access the Internet.
- You have logged on to the new console.
- A VPC is created and the CIDR block of the VPC is set to 172.16.0.0/12. If you use an existing VPC, the VPC must meet the following conditions:

VPC CIDR block	Description
172.16.0.0/12	The VPC does not have a custom route entry whose destination CIDR block is 10.0.0.0/8. You can view the added route entries on the route table details page of the VPC console.
192.168.0.0/16	- The VPC does not have a custom route entry whose destination CIDR block is 10.0.0.0/8. - A route is added to an ECS instance of the classic network and the route is directed from 192.168.0.0/16 to the private NIC. You can download a script to add the route. Note: Read the readme file in the script carefully before you run the script.

Step 1: Create a VPN Gateway

If you use a classic network, the VPN Gateway purchased in the VPC can also be used in the VPC through the ClassicLink function.

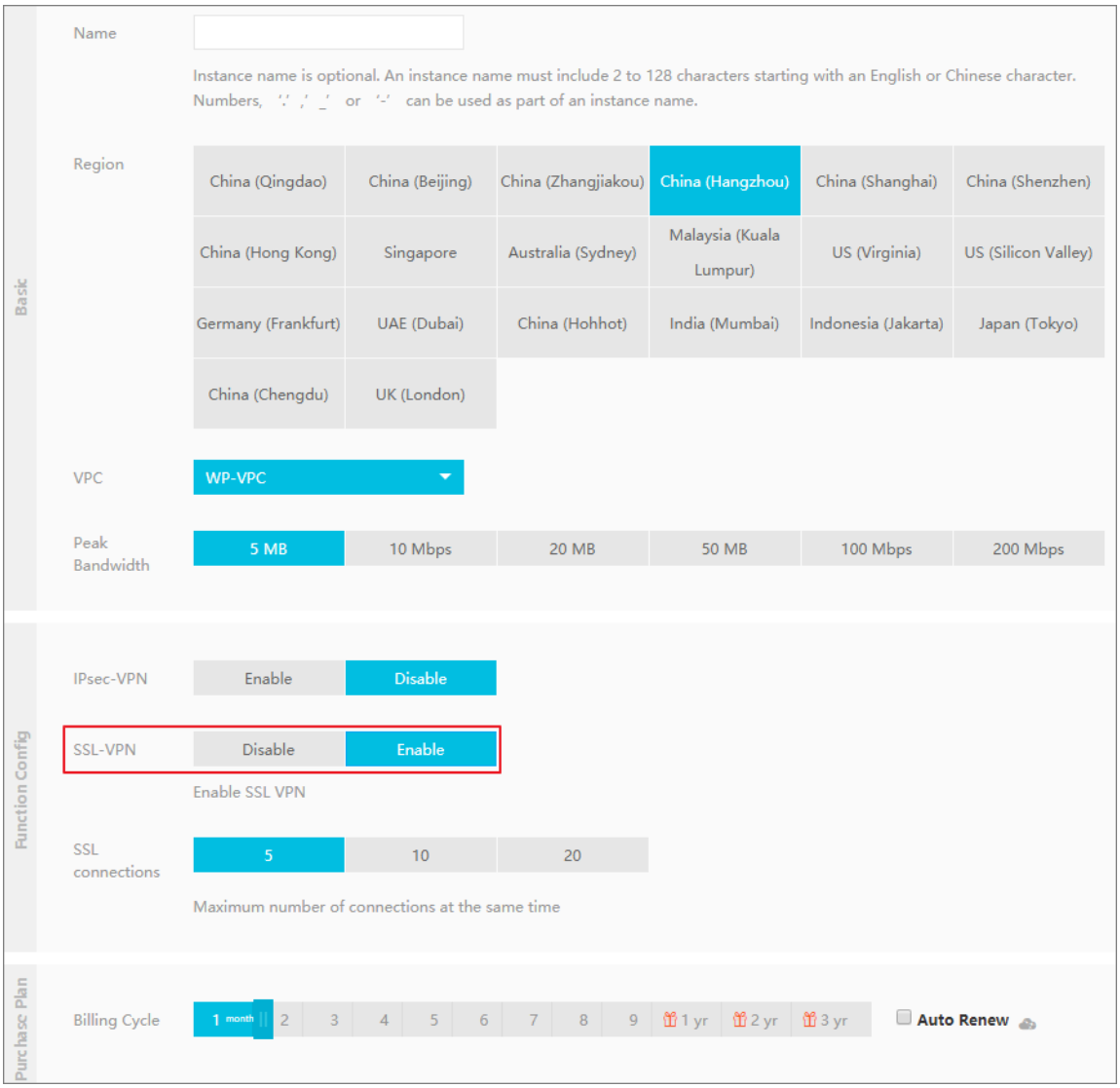
To create a VPN Gateway, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, choose VPN > VPN Gateways.
3. On the displayed page, click Create VPN Gateway.
4. On the purchase page, configure the VPN Gateway and complete the payment. In this example, the VPN Gateway is configured as follows:
   - Region: Select the region to which the VPN Gateway belongs. In this example, select China (Hangzhou).

Note:

The VPN Gateway must be in the same region as the VPC.

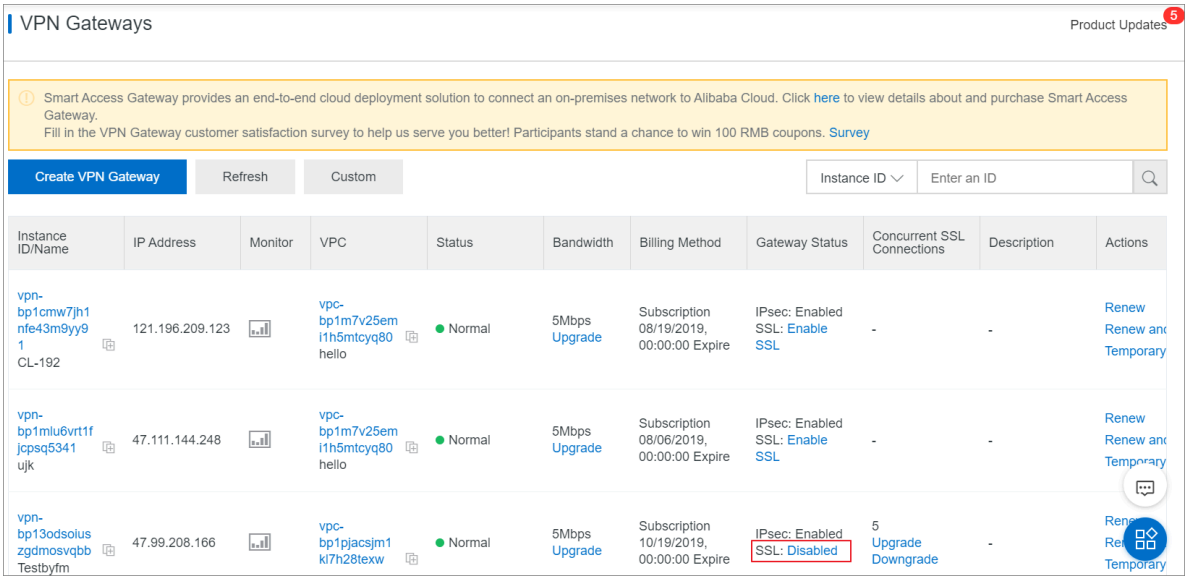
- **VPC: Select the target VPC.**
- **Peak Bandwidth: Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.**
- **IPsec-VPN: Select whether to enable the IPsec-VPN function, which applies to site-to-site connections.**
- **SSL-VPN: Select whether to enable the SSL-VPN function. In this example, select Enable.**
- **SSL Connections: Select the maximum number of clients to which you want to connect simultaneously.**



5. Go back to the VPN Gateways page to check the created VPN Gateway.

   The initial status of the VPN Gateway is Preparing. The status changes to Normal in about two minutes and then the VPN Gateway is ready to use.

   > **Note:**
   > It takes one to five minutes to create a VPN Gateway.



Step 2: Create an SSL server

To create an SSL server, follow these steps:

1. In the left-side navigation pane, chooseVPN > SSL Servers.
2. Click Create SSL Server. In this example, the SSL server is configured as follows:
   - Name: Enter a name for the SSL server.
   - VPN Gateway: Select the VPN Gateway created in Step 1.
   - Local Network: Enter the intranet CIDR block of the ECS instance in the target classic network. Click Add Local Network to add more intranet CIDR blocks.

     In this example, the intranet CIDR blocks are 10.1.0.0/16 and 10.2.0.0/16.

     > **Note:**

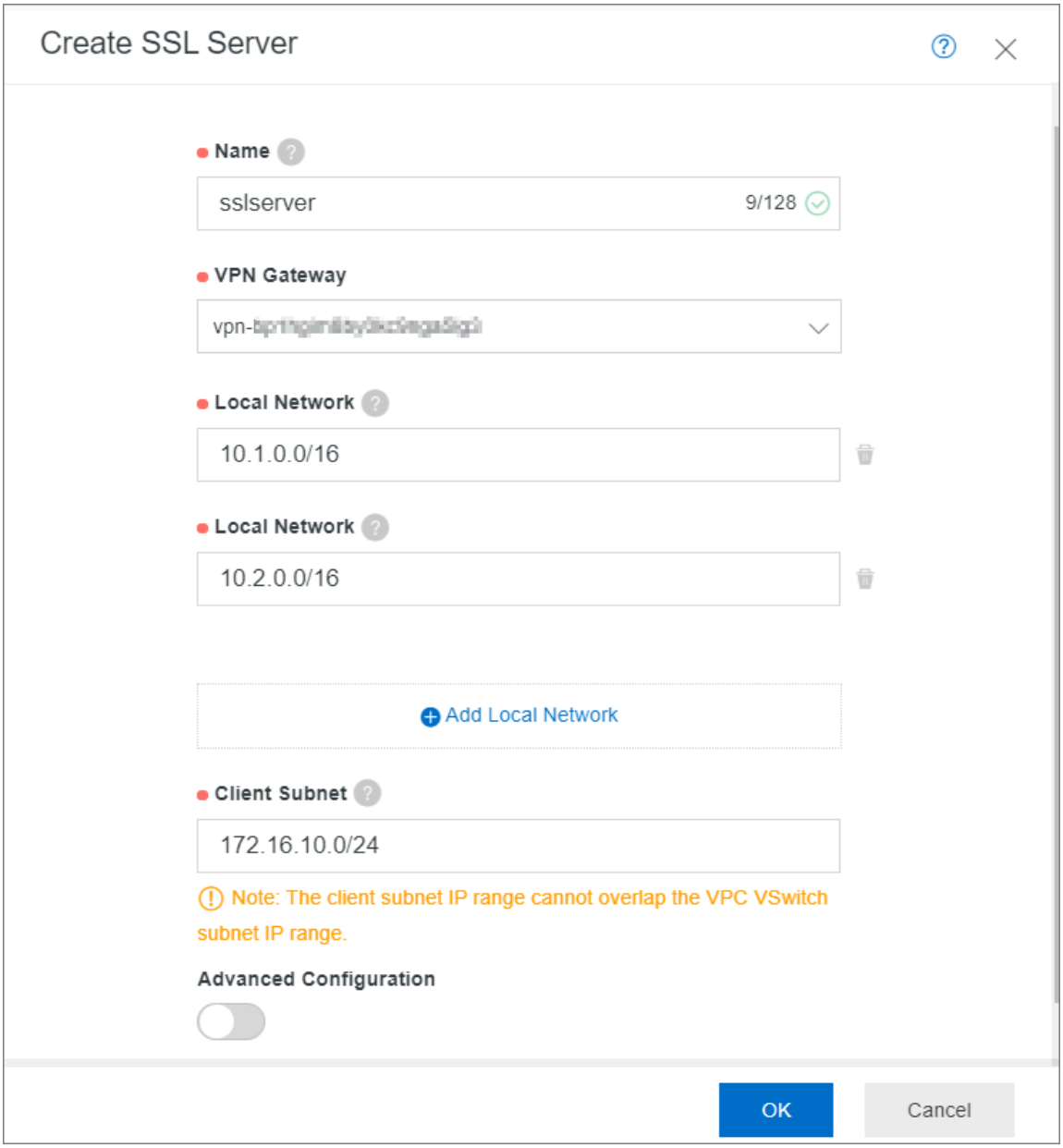
If the IP address of the newly created ECS instance is not in the intranet CIDR blocks, you must add the corresponding intranet CIDR block.

- Client Subnet: Enter the IP address used to interconnect the client and the server in the format of CIDR block. The client CIDR block must be a subnet of the CIDR block of the VPC to which the VPN Gateway belongs.

  In this example, the client CIDR block is 172.16.10.0/24.

  Note:
  The client CIDR block is not the existing IP address of your local client, but the IP address that is assigned to the client for access through SSL VPN.

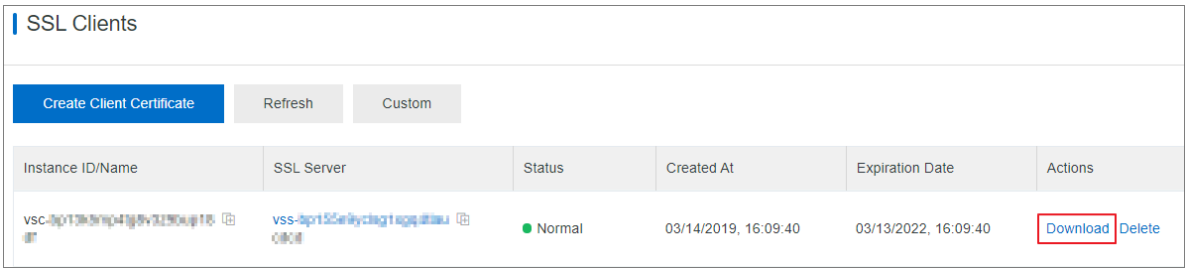
- Advanced Configuration: Use the default advanced configuration.



Step 3: Create a client certificate

To create a client certificate, follow these steps:

1. In the left-side navigation pane, chooseVPN > SSL Clients .
2. Click Create Client Certificate.
3. In the Create Client Certificate dialog box, enter a client certificate name, select the corresponding SSL server, and then click OK.
4. On the SSL Clients page, find the created client certificate, and then click Download to download the client certificate.



Step 4: Configure the client

To configure the client, follow these steps:

1. Run the following command to install the OpenVPN client:

```
yum  install  - y  openvpn
```

2. Decompress the certificate downloaded in Step 3 and copy it to the */ etc / openvpn / conf /* directory.
3. Run the following command to start the OpenVPN client:

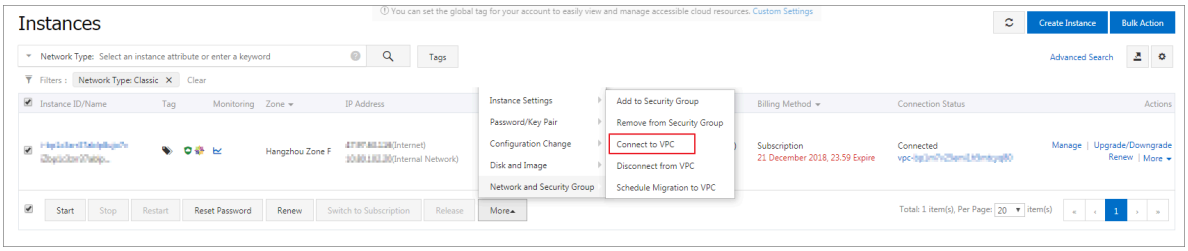
```
openvpn  -- config  / etc / openvpn / conf / config . ovpn  -
daemon
```

Step 5: Establish a ClassicLink connection

To establish a ClassicLink connection, follow these steps:

1. Log on to the VPC console.
2. Select the region to which the target VPC belongs, and then click the ID of the target VPC.
3. On the VPC Details page, click Enable ClassicLink.
4. In the displayed dialog box, click OK.
5. Log on to the ECS console.
6. In the left-side navigation pane, click Instances.

7. Select one or more ECS instances in the target classic network, and chooseMore > Connect to VPC .



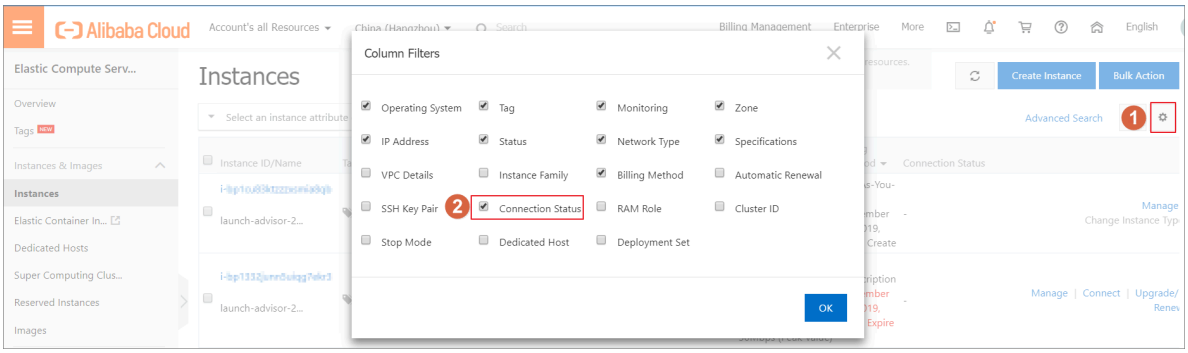
8. In the displayed dialog box, select the target VPC, and then click OK.
9. In the left-side navigation pane, chooseNetwork & Security > Security Groups .
10. On the Security Groups page, click the Internal Network Ingress tab, and then click Add Security Group Rule. Configure the security group rule as follows:

   - Rule Direction: Select Inbound.
   - Action: Select Allow.
   - Protocol Type: Select All.
   - Authorization Type: Select IPv4 CIDR Block.
   - Authorization Objects: Enter the private IP address (for example, 172.16.3.44/32) that needs to access the ECS instance through the VPN Gateway.

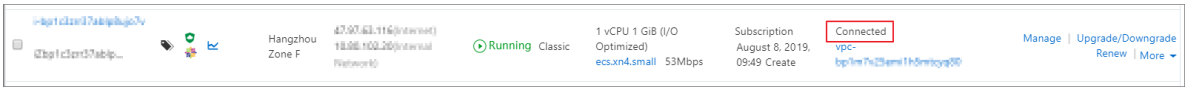
     Run the `ifconfig` command on the Linux client, and then find the message that is similar to `inet 172.16.10.6 --> 172.16.10.5 netmask 0xffffffff`, where `172.16.10.6` is the IP address of the client (the authorization object configured for the security group).

     Note:
     If you cannot access the ECS instance through the VPN Gateway, the client IP address has changed and you must add a new security group rule.

11. Go back to the ECS console, click the Column Filters icon on the right, select Connection Status in the displayed dialog box, and then click OK.



12. Check the connection status of the ECS instance.



After the configuration, you can access the applications deployed in the connected classic network ECS instance from the Linux client.

2 Use IPsec-VPN in the classic network

In the VPC network, you can create a site-to-site connection directly by using the IPsec-VPN function of VPN Gateway. However, to use VPN Gateway in the classic network, you must first configure the ClassicLink.

Prerequisites

Before you begin, plan your network:

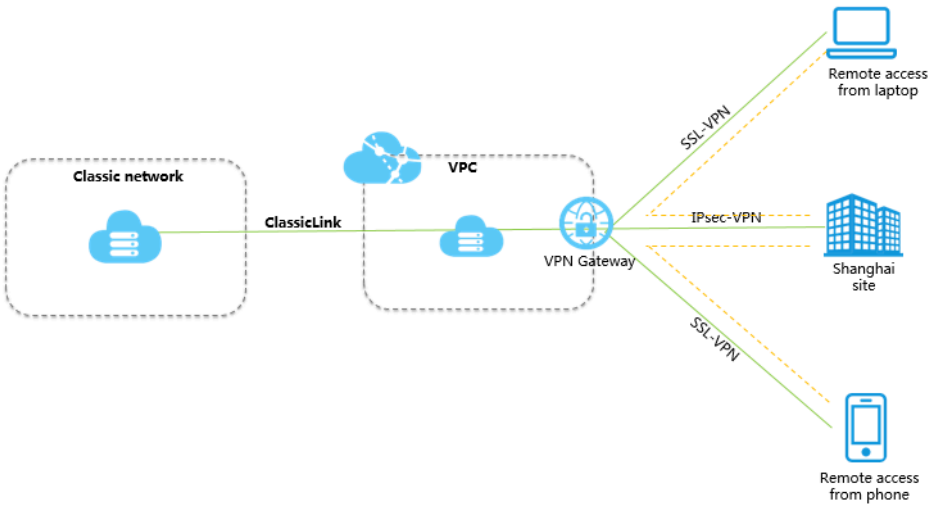
- The IP address range of the local client or office must belong to the IP address range of the VPC, but cannot conflict with the IP address ranges of VSwitches in the VPC.
- Plan the VPC for which a VPN gateway is created. If the ECS instances in the classic network do not need to communicate with ECS instances in the existing VPC, we recommend creating a new VPC.
- You have created a VPC. The VPC must use the following IP address range or its subnet, and meet the corresponding requirements:

VPC CIDR Block	Limitations
172.16.0.0/12	There is no route entry destined for 10.0.0.0/8 in this VPC.
192.168.0.0/16	- There is no route entry destined for 10.0.0.0/8 in this VPC. - A route, of which the destination CIDR block is 192.168.0.0/16 and the next hop is the private NIC, is added to the ECS instance of the classic network. You can use the provided script to add the route. Click Here to download the route script. Note: Before running the script, read the readme file in the script carefully.

Context

If you want to use VPN Gateway in the classic network, purchase a VPN Gateway for the VPC, and configure the IPsec-VPN function. After the configuration, the local data center or office site can access the VPC. Then, connect the VPC and the ECS instances

in the classic network using the ClassicLink function. Once the private connection is established, the local office site can access the ECS instances in the classic network.



Procedure

1. Create an IPsec-VPN connection.

   For more information, see Establish a connection between a VPC and an on-premises data center.

2. Create an SSL-VPN connection.

   For more information, see #unique_7.

3. Create a ClassicLink connection.

   For more information, see #unique_8.

3 High availability architecture using IPsec-VPN connections

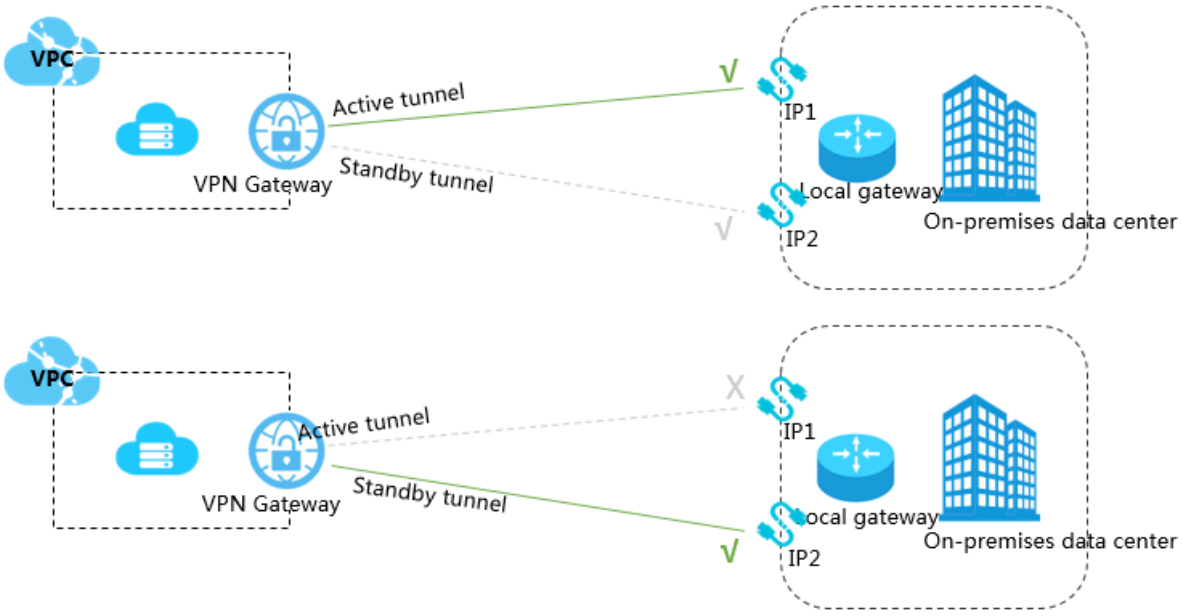
3.1 Dual IPsec-VPN tunnel configuration

This topic describes how to establish two IPsec-VPN tunnels with a VPN Gateway to implement active and standby tunnels. This configuration is suitable for a local gateway with two public IP addresses.

Overview

You can connect a VPN Gateway with two public IP addresses (in this example, they are labeled as IP1 and IP2) to establish two IPsec-VPN connections, and enable health checks. Afterwards, you can set the weights of the corresponding two routes to set one route as the active route and the other route as the standby route. The IPsec-VPN tunnel associated with the active route is the active tunnel, and the IPsec-VPN tunnel associated with the standby route is the standby tunnel.

- In this way, when the IP1-based Internet link is normal, all traffic between the on-premises data center and the VPC is forwarded only through this connection because it is the active tunnel.
- When the IP1-based Internet link is abnormal, all traffic between the on-premises data center and the VPC is directed to the standby tunnel.



Prerequisites

Before you begin, make sure that the following conditions are met:

- The gateway device of the on-premises data center operates properly. Alibaba Cloud VPN Gateways support standard IKEv1 and IKEv2 protocols. Devices that support these two protocols can connect to Alibaba Cloud VPN Gateways, including devices from Huawei, H3C, Hillstone, SANGFOR, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
- A static public IP address is configured for the gateway device of the on-premises data center.
- The CIDR block of the on-premises data center does not overlap the CIDR block of the VPC.

Step 1: Create a VPN Gateway

To create a VPN Gateway, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, choose VPN > VPN Gateways.
3. On the VPN Gateways page, click Create VPN Gateway.
4. On the purchase page, set the parameters, and then click Buy Now to complete the payment.
   - Name: Enter a name for the VPN Gateway.
   - Region: Select a region for the VPN Gateway.

     Note:
     The VPN Gateway must be in the same region as the VPC.
   - VPC: Select the VPC to be connected.
   - Peak Bandwidth: Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.
   - IPsec-VPN: Enable the IPsec-VPN function.
   - SSL-VPN: Select whether to enable the SSL-VPN function. The SSL-VPN function allows access to the VPC from a computer anywhere.
   - SSL connections: Select the maximum number of clients to which you want to connect simultaneously.

     Note:

This parameter is valid only after the SSL-VPN function is enabled.

- Billing Cycle: Select a billing cycle.

5. Go back to the VPN Gateways page to check the created VPN Gateway.

   The initial status of the VPN Gateway is Preparing. The status changes to Normal in about two minutes and then the VPN Gateway is ready to use.

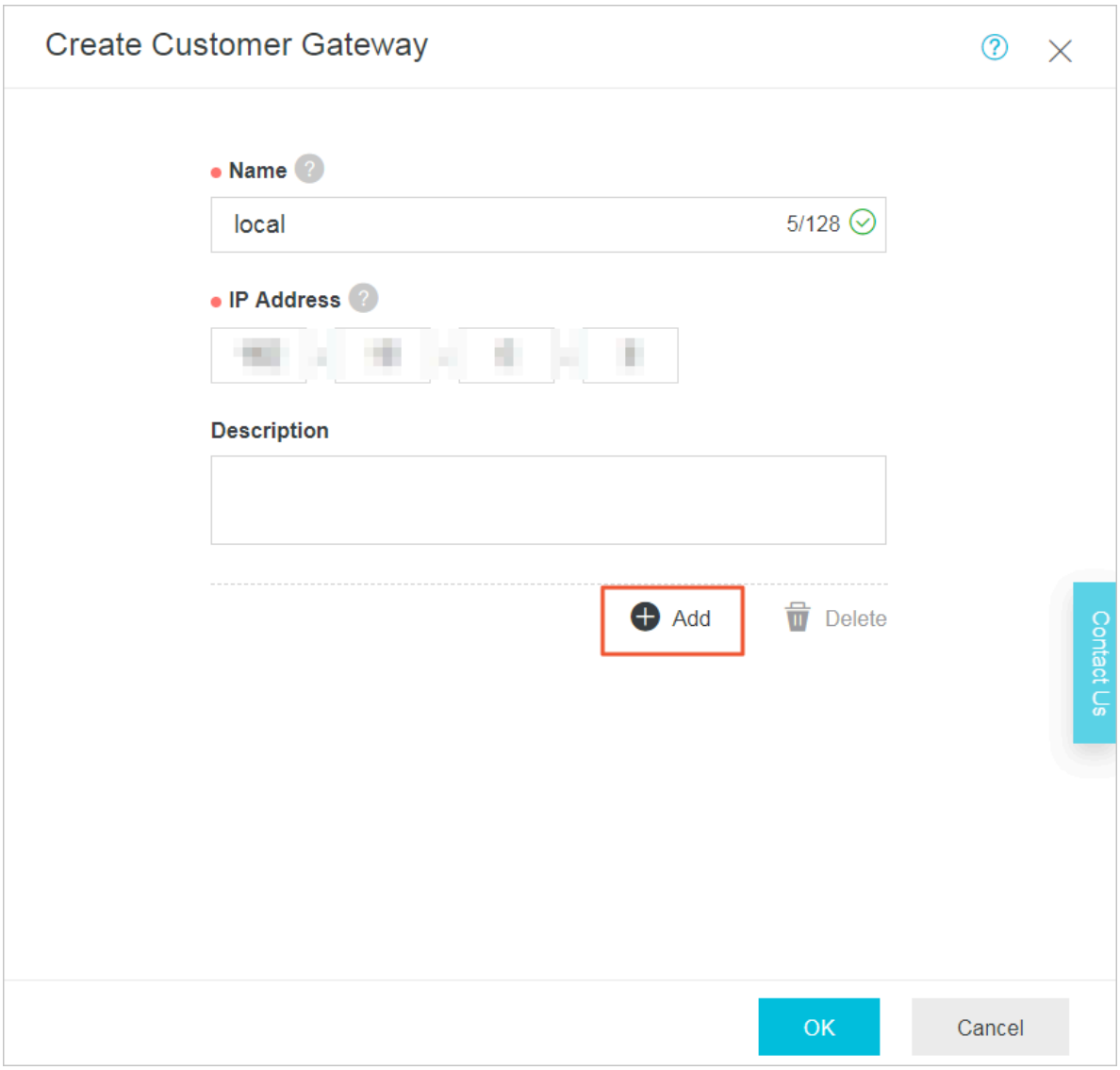
   Note:
   It takes one to five minutes to create a VPN Gateway.

Step 2: Create two customer gateways

Create two customer gateways and register the two public IP addresses of the local gateways to the customer gateways to create IPsec-VPN connections. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > Customer Gateways.
2. Select a region.
3. On the Customer Gateways page, click Create Customer Gateway.
4. Configure the customer gateway according to the following information:
   - Name: Enter the name of the customer gateway.
   - IP Address: Enter the public IP address of the local gateway.
   - Description: Enter a description of the customer gateway.

5. On the Create Customer Gateway page, click + Add to add multiple customer gateways.



Step 3: Create two IPsec-VPN connections

Create two IPsec-VPN connections to connect the VPN Gateway with the two customer gateways. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select a region.
3. On the IPsec Connections page, click Create IPsec Connection.

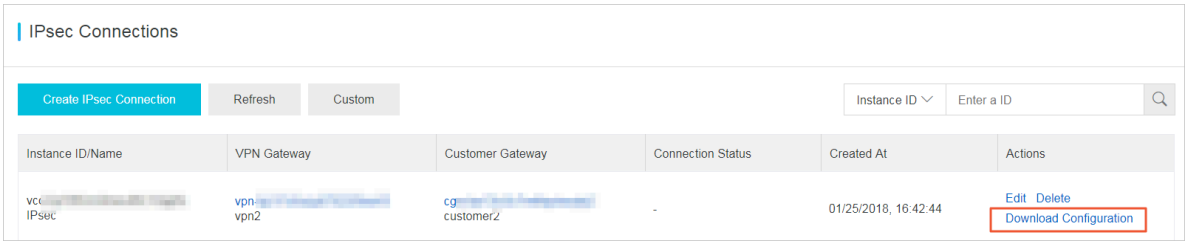
4. Configure the IPsec-VPN connection according to the following information and click OK.
   - Name: Enter the name of the IPsec-VPN connection.
   - VPN Gateway: Select the created VPN Gateway.
   - Customer Gateway: Select the created customer gateway.
   - Local Network: Enter the IP address range of the VPC to which the selected VPN Gateway belongs.
   - Destination CIDR Block: Enter the CIDR block of the local data center.
   - Effective Immediately: Select whether to start the negotiation immediately.
     - Yes: Start the negotiation immediately once the configuration is complete.
     - No: Start the negotiation only when traffic is detected in the tunnel.
   - Pre-Shared Key: Enter a pre-shared key. This value must be the same as the one configured in the local gateway.
   - Health Check: Enable health checks and enter the destination IP address, source IP address, retry interval, and number of retries.

   Use the default configurations for other parameters.
5. Repeat the preceding steps to create an IPsec-VPN connection for the other customer gateway.

Step 4: Configure the local gateway

To configure the local gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select the target region.
3. Find the target IPsec-VPN connection and click Download Configuration.



4. Configure the local gateways by loading the downloaded IPsec-VPN connection configurations to the local gateway device. For more information, see Local gateway configuration.

   The RemoteSubnet and LocalSubnet in the downloaded configurations are the converse in the actual operations of the local network and the remote network you configured when you create the IPsec-VPN connection. From the perspective of VPN Gateway, the remote network is the local IDC and the local network is the VPC. However, from the perspective of the local gateway, LocalSubnet is the CIDR block of the on-premises data center and RemoteSubnet is the CIDR block of the VPC.

Step 5: Configure the VPN Gateway route

To configure a route for the VPN Gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > VPN Gateways.
2. On the VPN Gateways page, select the region of the VPN Gateway.
3. Find the target VPN Gateway, and click the instance ID in the Instance ID/Name column.
4. On the Destination-based Routing tab page, click Add Route Entry.

5. Configure the route entry according to the following information and then click OK.
   - Destination CIDR Block: Enter the private CIDR block of the local gateway.
   - Next Hop: Select the target IPsec-VPN connection instance.
   - Publish to VPC: Select whether to publish the new route to the VPC route table.
   - Weight: Select a weight.

   The routes used in this example are as follows:

CIDR Block	Next Hop	Publish to VPC	Weight
The private CIDR block of the local gateway	IPsec-VPN connection instance 1	Yes	100
The private CIDR block of the local gateway	IPsec-VPN connection instance 2	Yes	0

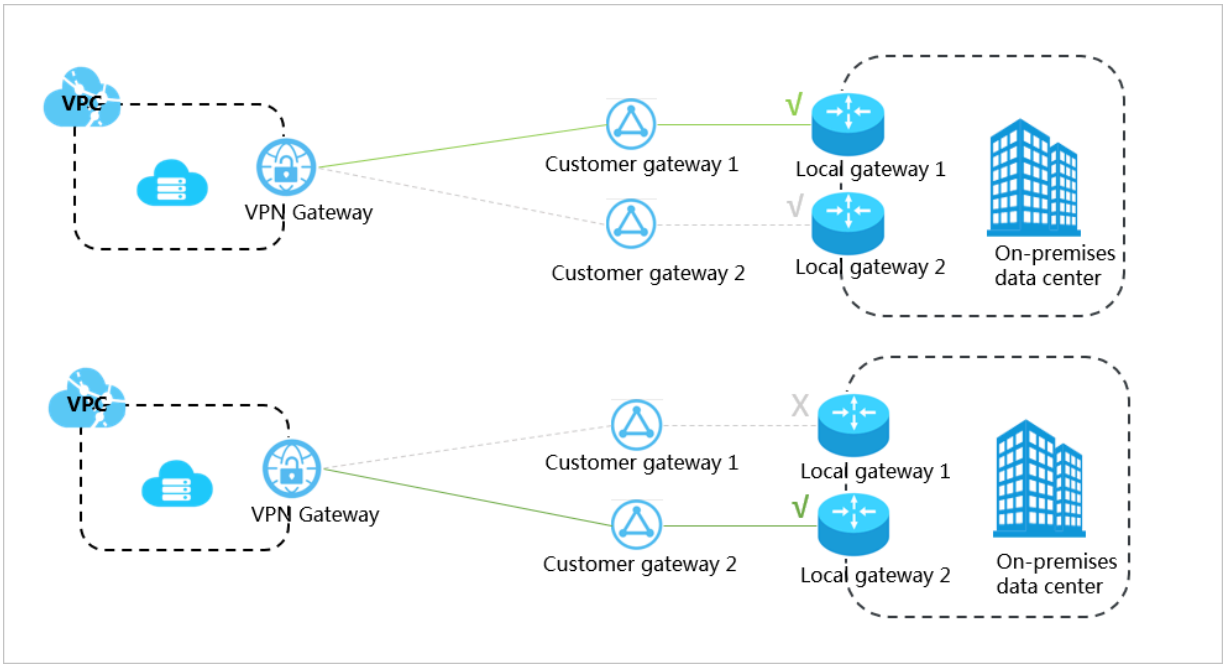
3.2 Dual customer gateway configuration

You can deploy two local gateways and connect the two local gateways to a VPN Gateway to create two IPsec-VPN connections. In this way, you can implement an IPsec-VPN connection redundancy.

Solution

As shown in the following figure, you can connect each of the two customer gateways to the VPN Gateway to create two IPsec-VPN tunnels.

Then, you can enable health checks for the two IPsec-VPN tunnels and make sure that the two IPsec-VPN tunnels are negotiated successfully. After that, if a health check detects that one customer gateway is abnormal, the traffic switches to the other customer gateway automatically.



Prerequisites

Before you begin, make sure that the following conditions are met:

- The gateway device of the on-premises data center operates properly. Alibaba Cloud VPN Gateways support standard IKEv1 and IKEv2 protocols. Devices that support these two protocols can connect to Alibaba Cloud VPN Gateways, including devices from Huawei, H3C, Hillstone, SANGFOR, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
- A static public IP address is configured for the gateway device of the on-premises data center.
- The CIDR block of the on-premises data center does not overlap the CIDR block of the VPC.

Step 1: Create a VPN Gateway

To create a VPN Gateway, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, choose VPN > VPN Gateways.
3. On the VPN Gateways page, click Create VPN Gateway.

4. On the purchase page, set the parameters, and then click Buy Now to complete the payment.
   - Name: Enter a name for the VPN Gateway.
   - Region: Select a region for the VPN Gateway.

     Note:
     The VPN Gateway must be in the same region as the VPC.
   - VPC: Select the VPC to be connected.
   - Peak Bandwidth: Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.
   - IPsec-VPN: Enable the IPsec-VPN function.
   - SSL-VPN: Select whether to enable the SSL-VPN function. The SSL-VPN function allows access to the VPC from a computer anywhere.
   - SSL connections: Select the maximum number of clients to which you want to connect simultaneously.

     Note:
     This parameter is valid only after the SSL-VPN function is enabled.
   - Billing Cycle: Select a billing cycle.
5. Go back to the VPN Gateways page to check the created VPN Gateway.

   The initial status of the VPN Gateway is Preparing. The status changes to Normal in about two minutes and then the VPN Gateway is ready to use.

   Note:
   It takes one to five minutes to create a VPN Gateway.

Step 2: Create two customer gateways

Create two customer gateways and register the public IP addresses of the local gateway devices to the customer gateways. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > Customer Gateways.
2. Select a region.
3. On the Customer Gateways page, click Create Customer Gateway.

4. On the Create Customer Gateway page, configure the customer gateway according to the following information, and click OK.
   - Name: Enter a customer gateway name.
   - IP Address: Enter the public IP address of the local gateway.
   - Description: Enter a description of the customer gateway.
   - + Add: Add another customer gateway.

Step 3: Create two IPsec-VPN connections

Create two IPsec-VPN connections to connect the VPN Gateway with the two customer gateways. To do so, follow these steps:

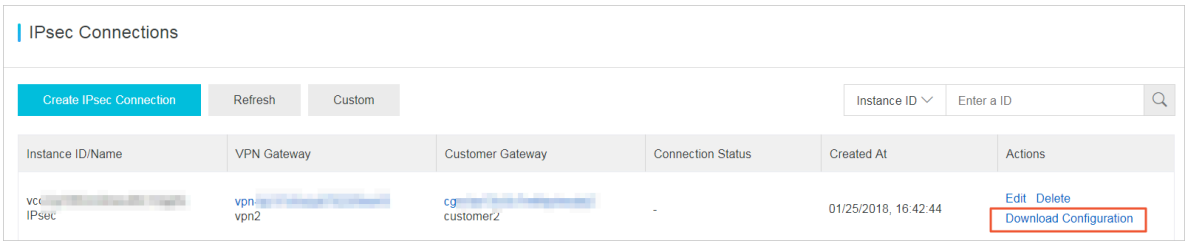
1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select a region.
3. On the IPsec Connections page, click Create IPsec Connection.
4. Configure the IPsec-VPN connection according to the following information and click OK.
   - Name: Enter a name for the IPsec-VPN connection.
   - VPN Gateway: Select the created VPN Gateway.
   - Customer Gateway: Select the created customer gateway.
   - Local Network: Enter the IP address range of the VPC to which the selected VPN Gateway belongs.
   - Destination CIDR Block: Enter the CIDR block of the local data center.
   - Effective Immediately: Select whether to start the negotiation immediately.
     - Yes: Start the negotiation immediately once the configuration is complete.
     - No: Start the negotiation only when traffic is detected in the tunnel.
   - Pre-Shared Key: Enter a pre-shared key. This value must be the same as the one configured in the local gateway.
   - Health Check: Enable health checks and enter the destination IP address, source IP address, retry interval, and number of retries.

     Use the default configurations for other options.
5. Repeat the preceding steps to create an IPsec-VPN connection for the other customer gateway.

Step 4: Configure the local gateway

To configure the local gateway, follow these steps:

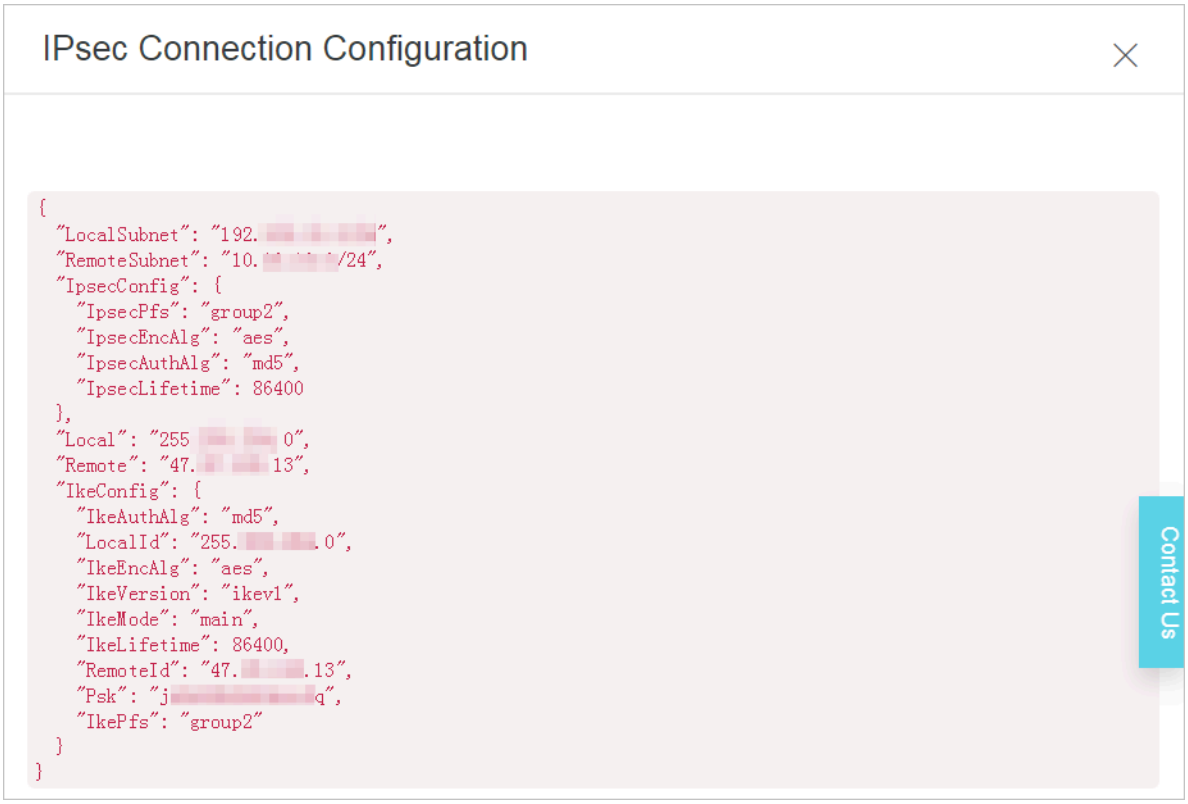
1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select a region.
3. Find the target IPsec-VPN connection and click Download Configuration.



4. Configure the local gateways by loading the downloaded IPsec-VPN connection configurations to the local gateway device. For more information, see Local gateway configuration.

   The RemoteSubnet and LocalSubnet in the downloaded configurations are converse in operation of the local network and the remote network you configured when you create the IPsec-VPN connection. From the perspective of VPN Gateway, the remote network is the local IDC and the local network is the VPC. However,

from the perspective of the local gateway, LocalSubnet is the CIDR block of the on-premises data center and RemoteSubnet is the CIDR block of the VPC.



Step 5: Configure a route for the VPN Gateway

To configure a route for the VPN Gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > VPN Gateways.
2. On the VPN Gateways page, select the region of the VPN Gateway.
3. Find the target VPN Gateway, and click the instance ID in the Instance ID/Name column.
4. On the Destination-based Routing tab page, click Add Route Entry.

5. Configure the route entry according to the following information and then click OK.
   - Destination CIDR Block: Enter the private CIDR block of the local gateway.
   - Next Hop: Select the target IPsec-VPN connection instance.
   - Publish to VPC: Select whether to publish the new route to the VPC route table.
   - Weight: Select a weight.

   The routes used in this example are as follows:

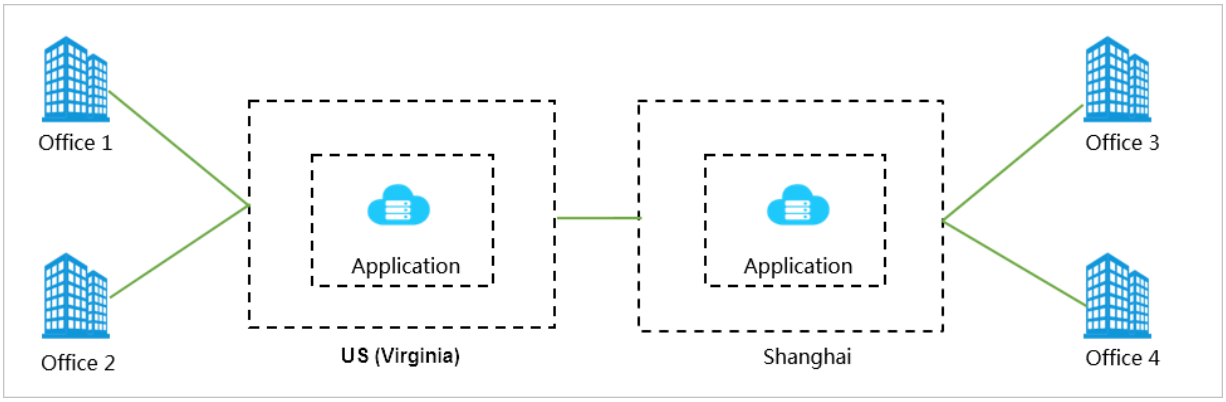
CIDR Block	Next Hop	Publish to VPC	Weight
The private CIDR block of the local gateway	IPsec-VPN connection instance 1	Yes	100
The private CIDR block of the local gateway	IPsec-VPN connection instance 2	Yes	0

4 Establish a global network through IPsec-VPN and CEN

This topic describes how to establish a global network by using VPN Gateway and Cloud Enterprise Network (CEN). International enterprises can establish a global network by using VPN Gateway and CEN. CEN can reduce cross-border network latency and VPN Gateway can help lower the cost of last-mile connections and client connections.

Scenario

An international company wants to deploy different applications in multiple countries, but the applications need to be accessible by multiple offices in each country. In this example, the company has one VPC in the US (Virginia) region, and one in the China (Shanghai) region, and each VPC has a separate application deployed . The company also has two offices in Virginia and two in Shanghai.



Solution

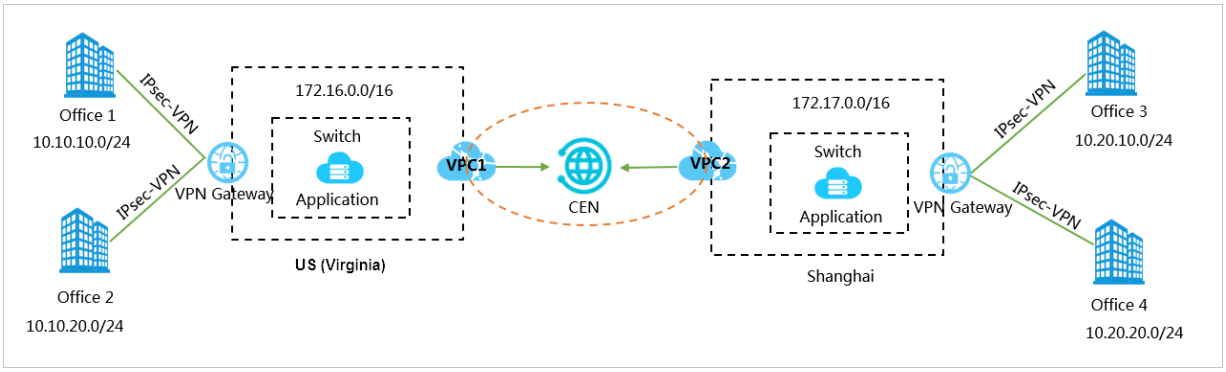
The following table details traditional connectivity solutions for offices across the globe to communicate with each other, and the problems inherent in these traditional solutions.

Traditional solution	Problem
Communication through the Internet	Data stored locally is exposed over the Internet and the network quality of the Internet connection is not guaranteed.

Traditional solution	Problem
Communication through IPsec-VPN	Cross-border communication is affected by the network quality of the Internet connection.
Communication through leased lines	The installation of leased lines and subsequent maintenance incur high costs.

To resolve the preceding problems of traditional connection solutions, Alibaba Cloud allows you to use VPN Gateway and CEN to connect applications and offices located around the world.

In the Alibaba Cloud solution, an application is deployed to each VPC located in US (Virginia) and China (Shanghai) respectively (in this example, the VPCs for Virginia and Shanghai are VPC1 and VPC2 respectively). Then, VPC1 and VPC2 are connected by using CEN. After that, Office 1 and Office 2 in Virginia are connected to the VPN Gateway of VPC1, and Office 3 and Office 4 in Shanghai are connected to the VPN Gateway of VPC2 through IPsec-VPN connections. In this way, the applications and offices connected to the VPCs in the US (Virginia) region and the China (Shanghai) region can communicate with each other.



Prerequisites

- The Alibaba Cloud environment is prepared. Specifically, VPCs and VSwitches are created and applications are deployed.
- Local gateways are configured in the offices and a static public IP address is configured for each local gateway.
- The CIDR blocks to be connected do not conflict with each other.

Step 1: Create IPsec-VPN connections for the offices in Virginia

1. Create a VPN Gateway for the VPC in the US (Virginia) region. For more information, see #unique_14/unique_14_Connect_42_section_zv3_nyf_xdb.
2. Create two customer gateways and register the public IP addresses of the two local gateways in the two Virginia offices to the customer gateways.

   The IP addresses of customer gateways are the public IP addresses of local gateways in the offices. For more information, see #unique_15/unique_15_Connect_42_section_mwf_lxc_xdb.
3. Create two IPsec-VPN connections to connect the VPN Gateway with the two customer gateways. For more information, see #unique_16/unique_16_Connect_42_section_mxd_fyc_xdb.
4. Load VPN configurations to the gateway devices of local office sites.

   Load the VPN configurations according to the requirements on the local gateway devices. For more information, see Local gateway configuration.
5. Configure the VPN Gateway route. For more information, see #unique_17.

Step 2: Create IPsec-VPN connections to the Shanghai offices

Create IPsec-VPN connections for the offices in Shanghai. To do so, refer to the instructions detailed in Step 1.

Step 3: Connect the two VPCs

Connect the VPCs by using CEN. For more information, see #unique_18.

Step 4: Add routes in CEN

Publish the routes in the VPCs that are directed to the VPN Gateways to CEN so that other networks in CEN can learn the routes.

For more information, see #unique_19/unique_19_Connect_42_section_qts_1ct_q2b.

Step 5: Configure security groups

Configure security groups for the ECS instances where you applications are deployed.

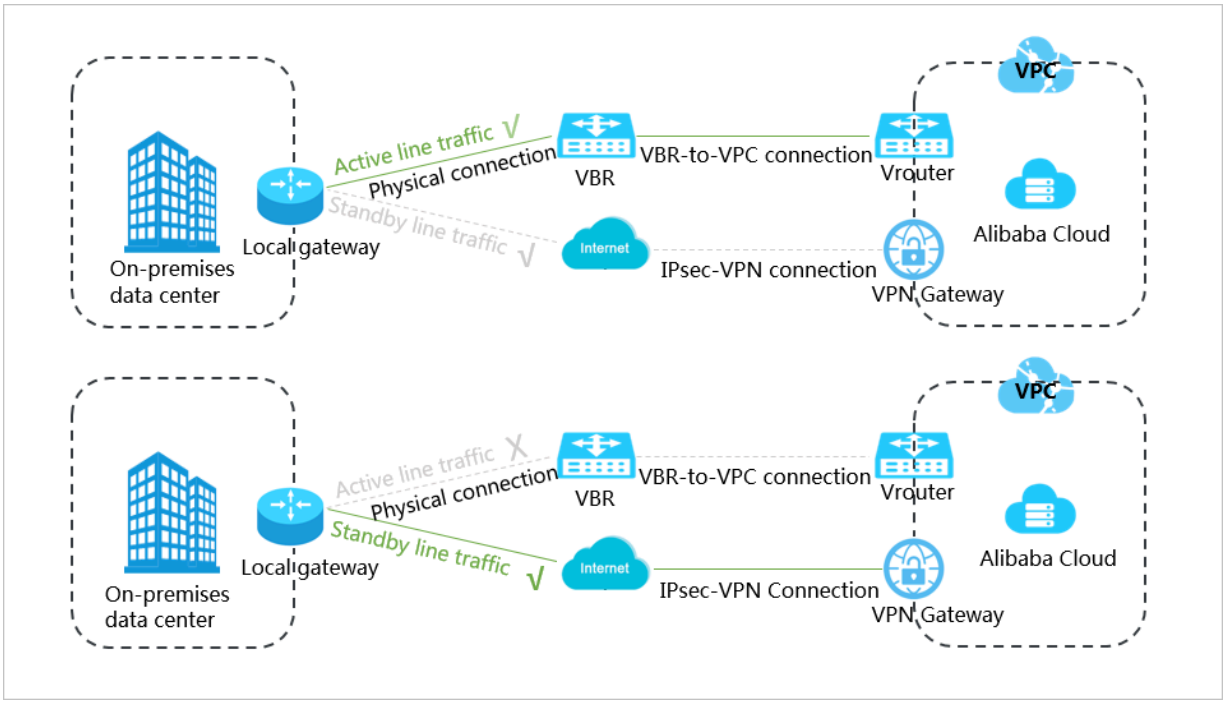
After you have completed the preceding steps, you can connect your applications with offices in different regions, and the offices and applications can communicate with each other over the intranet.

5 Implement an active/standby configuration by using VPN Gateway and Express Connect

This topic describes how to implement an active/standby configuration by using a VPN Gateway and a physical connection of Express Connect to improve the availability of your applications.

You can connect your on-premises data center to an Alibaba Cloud VPC through both a physical connection and an IPsec-VPN connection.

- When the physical connection works normally, the traffic between the on-premises data center and the VPC is forwarded through the physical connection.
- When the physical connection is abnormal, the traffic between the on-premises data center and the VPC is directed to the IPsec-VPN tunnel.



Prerequisites

A physical connection is created to allow intercommunication between your on-premises data center and the VPC.

For more information, see #unique_21.

Step 1: Create a VPN Gateway

To create a VPN Gateway, follow these steps:

1. Log on to the VPC console.
2. In the left-side navigation pane, choose VPN > VPN Gateways.
3. On the VPN Gateways page, click Create VPN Gateway.
4. On the purchase page, set the parameters, and then click Buy Now to complete the payment.
   - Name: Enter a name for the VPN Gateway.
   - Region: Select a region for the VPN Gateway.

     Note:
     The VPN Gateway must be in the same region as the VPC.
   - VPC: Select the VPC to be connected.
   - Peak Bandwidth: Select a peak bandwidth. The bandwidth is the Internet bandwidth of the VPN Gateway.
   - IPsec-VPN: Enable the IPsec-VPN function.
   - SSL-VPN: Select whether to enable the SSL-VPN function. The SSL-VPN function allows access to the VPC from a computer anywhere.
   - SSL connections: Select the maximum number of clients to which you want to connect simultaneously.

     Note:
     This parameter is valid only after the SSL-VPN function is enabled.
   - Billing Cycle: Select a billing cycle.
5. Go back to the VPN Gateways page to check the created VPN Gateway.

   The initial status of the VPN Gateway is Preparing. The status changes to Normal in about two minutes and then the VPN Gateway is ready to use.

   Note:
   It takes one to five minutes to create a VPN Gateway.

Step 2: Create a customer gateway

Create a customer gateway and register the public IP address of the local gateway to the customer gateway. To do so, follow these steps:

1. In the left-side navigation pane, choose VPN > Cusomer Gateways.
2. Select the region in which you want to create a customer gateway.

3. On the Customer Gateways page, click Create Customer Gateway.
4. On the Create Customer Gateway page, set the parameters, and then click OK.
   - Name: Enter a name for the customer gateway.
   - IP Address: Enter the private IP address of the gateway device in the on-premises data center.
   - Description: Enter a description of the customer gateway.

Step 3: Create an IPsec-VPN connection

To create an IPsec-VPN connection, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select a region.
3. On the IPsec Connections page, click Create IPsec Connection.
4. Configure the IPsec-VPN connection according to the following information and click OK.
   - Name: Enter the name of the IPsec-VPN connection.
   - VPN Gateway: Select the created VPN Gateway.
   - Customer Gateway: Select the created customer gateway.
   - Local Network: Enter the IP address range of the VPC to which the selected VPN Gateway belongs.
   - Destination CIDR Block: Enter the CIDR block of the local data center.
   - Effective Immediately: Select whether to start the negotiation immediately.
     - Yes: Start the negotiation immediately once the configuration is complete.
     - No: Start the negotiation only when traffic is detected in the tunnel.
   - Pre-Shared Key: Enter a pre-shared key. This value must be the same as the one configured in the local gateway.
   - Health Check: Enable health checks and enter the destination IP address, source IP address, retry interval, and number of retries.

     Use the default configurations for other parameters.

Step 4: Load the VPN configuration to the local gateway

To load the VPN configuration to the local gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > IPsec Connections.
2. Select the region to which the target IPsec connection belongs.

3. On the IPsec Connections page, find the target IPsec connection, and then click Download Configuration in the Actions column.
4. Add the downloaded configuration to the local gateway device. For more information, see Local gateway configuration.

   RemotSubnet and LocalSubnet are opposite to the Local Network and Remote Network that you set when you create an IPsec connection in Step 3. Specifically, for the VPN Gateway, its remote network is the CIDR block of the on-premises data center and its local network is the CIDR block of the VPC. For the local gateway, LocalSubnet is the CIDR block of the on-premises data center and RemoteSubnet is the CIDR block of the VPC.

Step 5: Configure a route for the VPN Gateway

To configure a route for the VPN Gateway, follow these steps:

1. In the left-side navigation pane, choose VPN > VPN Gateways.
2. Select the region to which the target VPN gateway belongs.
3. On the VPN Gateways page, find the target VPN Gateway, and then click the instance ID in the Instance ID/Name column.
4. On the Destination-based Routing tab, click Add Route Entry.
5. On the Add Route Entry page, set the parameters, and then click OK.
   - Destination CIDR Block: Enter the private CIDR block of the on-premises data center.
   - Next Hop: Select the IPsec connection instance.
   - Publish to VPC: Select whether to publish the new route to the VPC route table. In this example, select Yes.
   - Weight: Select a weight. In this example, select 100.

Step 6: Configure health checks for the VBR of the physical connection

Configure health checks for the Virtual Border Router (VBR) of the physical connection to make sure that the status of the physical connection can be checked by the VPC and traffic can be directed to the IPsec-VPN connection when the physical connection fails.

For more information, see #unique_22.

Step 7: Configure the local gateway

Configure an active route and a standby route that point to the VPC on the local gateway device, and enable the health check function for the physical connection. In this way, when the physical connection fails, traffic is forwarded to the IPsec-VPN connection.