Alibaba Cloud vpn gateway

Best Practices

Issue: 20181129

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.	 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructio ns, 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]`*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *`{stand | slave}`*

Contents

1 Local gateway configurations

1.1 Configure H3C firewall

When using IPsec-VPN to create a site-to-site connection, you must configure the local gateway according to the IPsec connection configured for the Alibaba Cloud VPN Gateway. This document takes H3C firewall as an example to show how to configure the VPN settings.

Prerequisites

- Make sure you have configured IPsec connections. For more information, see *Configure a site-to-site connection*.
- After you create an IPsec connection, download the configurations of the created IPsec connection.

  In this tutorial, the configurations of the IPsec connection are as follows:

  — IPsec configuration

Configuration		Value
IKE	Authentication Algorithm	sha1
	Encryption Algorithm	aes
	DH Group	group2
	IKE Version	ikev1
	SA Life Cycle (seconds)	86400
	Negotiation Mode	main
	PSK	h3c
IPsec	Authentication Algorithm	sha1
	Encryption Algorithm	aes
	DH Group	group2
	IKE Version	ikev1
	SA Life Cycle (seconds)	86400
	Security Protocol	esp

  — Network configuration

Configuration		Value
VPC	Private CIDR block	192.168.10.0/24
	Public IP of VPN Gateway	101.xxx.xxx.127
IDC	Private CIDR block	192.168.66.0/24
	Public IP of local gateway	122.xxx.xxx.248
	Uplink public port	Reth 1
	Downlink private port	G 2/0/10

Procedure

1. Log on to the console of the H3C firewall, and then click**Network** > **VPN** > **IPsec** > **Policy** .
2. Configure the H3C firewall IPsec policy based on the IPsec configurations of the Alibaba Cloud VPN Gateway. Click **Add** in the **Protected Data Stream** list, set the IP address range of the IDC to the source IP and the IP address range of the VPC to the destination IP.
3. Click**IKE Proposal** > **Create**.

   Configure IKE proposal according to the IKE configurations of the Alibaba Cloud VPN Gateway.
4. Click**Network** > **VPN** > **IPsec** > **Policy**.
5. Select the new IPsec policy, click **Advanced Configuration** to configure the IPsec protocol.

   Configure the IPsec protocol according to the IPsec configurations of the Alibaba Cloud VPN Gateway.

   Create the downlink security policy and the uplink security policy.

   - The security policy configuration from the Alibaba Cloud VPC to the local IDC is shown in the following figure.
6. Click**Policy** > **Security Policy** > **Create**.

   The security policy configuration from the Alibaba Cloud VPC to the local IDC is shown in the following figure.

   The security policy configuration from the local IDC to the Alibaba Cloud VPC is shown in the following figure.

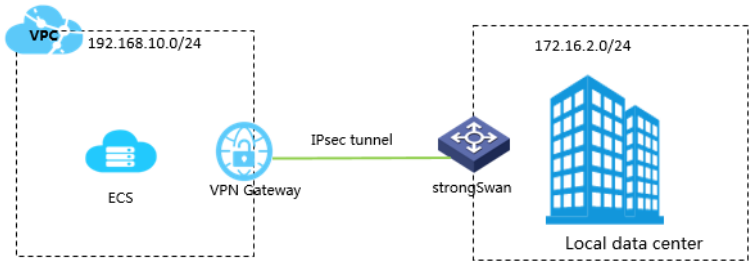
7. Click**Network** > **Route** > **Static Route**.
8. Add the default route, set the uplink interface as the next hop of the outbound traffic. In this tutorial, no configuration is required.

1.2 Configure strongSwan

When using IPsec-VPN to create a site-to-site connection, you must configure the local gateway according to the IPsec connection configured for the Alibaba Cloud VPN gateway. This article takes strongswan as an example to show you how to load a VPN configuration in a local site.

This document takes strongSwan as an example to show how to configure the VPN settings. The configurations used in this tutorial are as follows:

- The IP address range of the Alibaba Cloud VPC is 192.168.10.0/24.
- The IP address range of the local data center is 172.16.2.0/24.
- The public IP of strongSwan is 59.110.165.70.



Prerequisites

- Make sure you have configured IPsec connections. For more information, see *Configure a site-to-site connection*.
- After you create an IPsec connection, download the configurations of the created IPsec connection. For more information, see *Manage an IPsec connection*.

Install strongSwan

1. Run the following command to install strongSwan.

```
# yum install strongSwan
```

2. Run the following to view the installed software version.

```
# strongswan version
```

Configure strongSwan

1. Run the following command to open the *ipsec.conf* file.

```
# vi /etc/strongswan/ipsec.conf
```

2. Refer to the following configurations to update the *ipsec.conf* file.

```
# ipsec.conf - strongSwan IPsec configuration file
 # basic configuration
 config setup
     uniqueids=never
 conn %default
     authby=psk
     type=tunnel
 conn tomyidc
     keyexchange=ikev1
     left=59.110.165.70
     leftsubnet=172.16.2.0/24
     leftid=59.110.165.70 (Public IP of the loca gateway)
     right=119.23.227.125
     rightsubnet=192.168.10.0/24
     rightid=119.23.227.125 (Public IP of the VPN Gateway)
     auto=route
     ike=aes-sha1-modp1024
     ikelifetime=86400s
     esp=aes-sha1-modp1024
     lifetime=86400s
     type=tunnel
```

3. Configure the *ipsec.secrets* file.

a. Run the following command to open the configuration file.

```
# vi /etc/strongswan/ipsec.secrets
```

b. Add the following configuration.

```
59.110.165.70 119.23.227.125 : PSK yourpassword
```

4. Enable system forwarding.

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

For more configuration examples for different scenarios, see *Configuration examples for different scenarios*.

5. Run the following command to start the strongSwan service.

```
# systemctl enable strongswan
# systemctl start strongswan
```

6. Configure two routings in strongSwan. One is used to route the requests destined for the IDC client to strongSwan. The other one is used to route the requests destined for strongSwan to your IDC client.

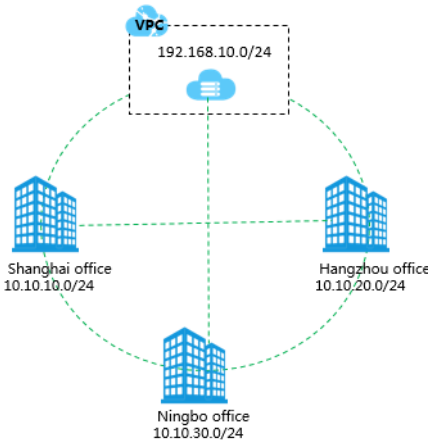
2 Configure multi-site connections

You can create IPsec connections between multiple sites and locations. With the VPN-Hub function, the connected sites can communicate with the connected VPC, and also communicate with each of the other sites. VPN-Hub meets the needs of large enterprises to establish intranet communications between different sites.

VPN-Hub overview

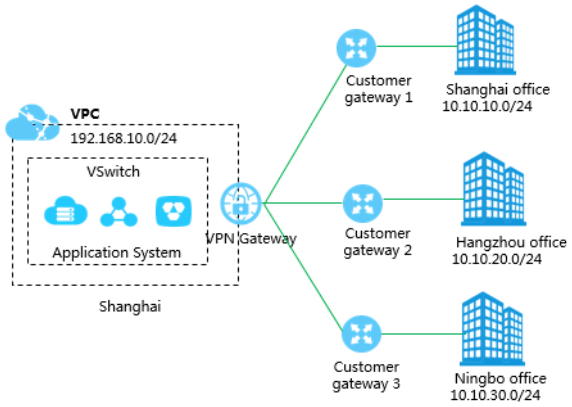
The VPN-Hub function is enabled by default. To achieve multi-site connections, you must create corresponding IPsec connections. A VPN Gateway can have up to ten IPsec connections. Therefore, you can connect up to ten office sites with one VPN Gateway.

The following scenario is used to illustrate connecting office sites in the cities of Shanghai, Hangzhou, and Ningbo. Before you begin, make sure that you have obtained the public IP address of the gateway device for each office site.



As shown in the following figure, to connect the three office sites (Shanghai, Hangzhou, and Ningbo), you only need to create a VPN Gateway and three customer gateways and establish three IPsec connections.

Note:
Make sure the IP address ranges of all the connected sites do not conflict with each other.



Step 1. Create a VPN Gateway

Create a customer gateway using the public IP address configured for the local gateway in the Shanghai office. For more information, see *Manage a VPN Gateway*.

Note:
Make sure the IPsec-VPN function is enabled.

Step 2: Create an IPsec connection to the Shanghai office

1. Create a customer gateway using the public IP address configured for the local gateway in the Shanghai office.

   For more information, see *Create a customer gateway*.
2. Create an IPsec connection.

   Create an IPsec connection to connect the VPN Gateway and the customer gateway. For more information, see *Create an IPsec connection*.

   - **Local network**: 0.0.0.0/0.

     Note:
     We recommend that you set local network to 0.0.0.0/0, which greatly simplifies the network. Only one IPsec connection is required per office and the current configurations do not need to be changed when new IPsec connections are created.
   - **Remote network**: the IP address range of the local data center. In this example, it is the IP address range of the Shanghai office: 10.10.10.0/24.
3. Configure the local gateway according to the configured IPsec connections.

   Download the configurations of the IPsec connection, then configure the local gateway. For more information, see *Local gateway configurations*.

Step 3: Create additional IPsec connections for the other two sites

Follow the same procedures in the Step 2 to create two IPsec connections for the Hangzhou office and the Ningbo office.

Step 4: Configure the route in VPC

1. Log on to the VPC console.
2. In the left-side navigation bar, click **Route Tables**. Find the route table of the target VPC and click **Manage**.
3. On the **Route Tables** page, click **Add Route Entry** to add the following routes.

Destination CIDR block	Next hop type	Next hop
10.10.10.0/24	VPN Gateway	The VPN Gateway created in the Step 1
10.10.20.0/24	VPN Gateway	The VPN Gateway created in the Step 1
10.10.30.0/24	VPN Gateway	The VPN Gateway created in the Step 1

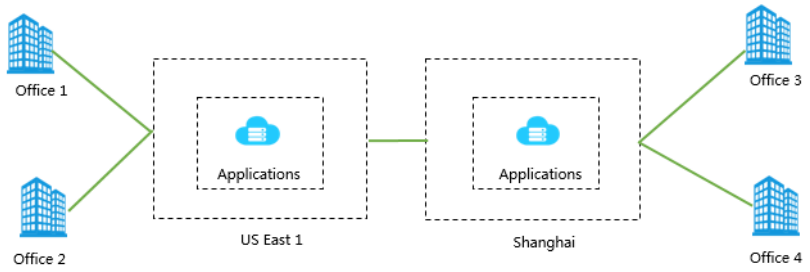
The IPsec connections to the three office sites have now been established. Each office site can now communicate with the VPC and can communicate with the other office sites over their intranet .

3 Use VPN Gateway and Express Connect together

Multinational corporations can use Express Connect to connect two VPCs from different regions and use VPN Gateway to connect local sites within regions with low latency at a low cost.

Example scenario

Multinational corporations often have the need to deploy applications in multiple countries and interconnect Operation and Maintenance systems around the world. For example, an enterprise deploys two sets of applications in the eastern United States and Shanghai, and needs to connect offices worldwide as shown in the following figure:



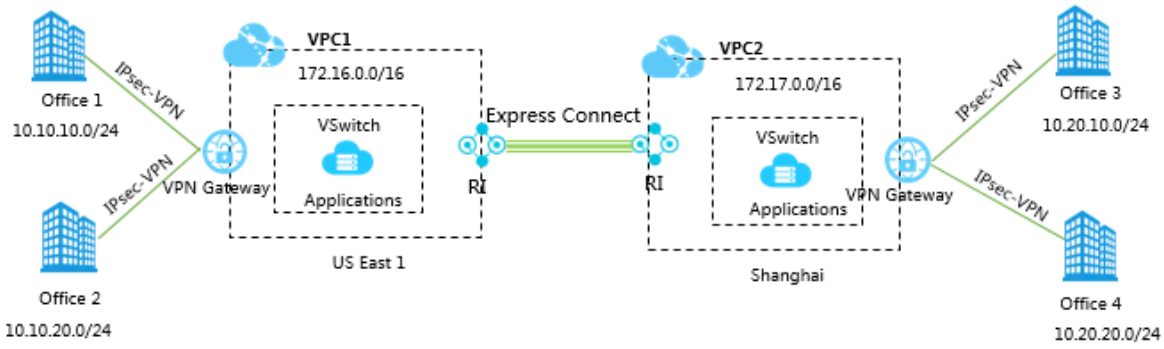
Solution overview

Typical worldwide communication and data transfer solutions, and risks include the following:

Typical solutions	Risks
Direct connections over the Internet	Sensitive, proprietary data is disclosed over the Internet and the network quality is unstable.
IPsec VPN	Provides high security, but is still dependent on the public Internet. The multinational network quality is limited by the Internet network infrastructure.
Dedicated leased line	High security and high network quality, but with relatively high costs.

Alibaba Cloud provides secure, high-quality, and relatively low-cost solution for connecting office networks around the world by combining VPN Gateway and Express Connect.

You can use Express Connect to connect two VPCs and use VPN Gateway to connect the office sites to VPCs as shown in the following figure:



Prerequisites

- Create a VPC and a VSwitch.
- Configure a local gateway in each office and make sure a static public IP address is available.
- The IP address ranges of the sites to be connected cannot be in conflict with one another.

Step 1: Create IPsec connections to the US East offices

You can create two IPsec connections to connect the offices in the East US region to the VPC. With VPN-Hub, the connected offices can communicate with each other. For more information, see *Configure multi-site connections*.

1. Create a VPN gateway for the VPC in the East US region. For more information, see *Create a VPN gateway*.
2. Create two customer gateways using the public IP addresses of the two offices.

   For more information, see *Create a customer gateway*.
3. Create two IPsec connections to connect the VPN gateway and the customer gateways. For more information, see *Create an IPsec connection*.
   - **Local network**: Enter 0.0.0.0/0.

     Note:
     We recommend that you set local network to 0.0.0.0/0, which greatly simplifies the network. Only one IPsec connection is required per office and the current configurations do not need to be changed when new IPsec connections are created.
   - **Remote network**: 10.10.10.0/24 and 10.10.20.0/24
4. Configure the local gateway according to the configured IPsec connections.

Load the VPN configurations according to the requirements of the local office on gateway device. For more information, see *Local gateway configurations*.

Step 2: Create IPsec connections to the Shanghai offices

Follow procedures in Step 1 to create two IPsec connections to connect the offices in the Shanghai to the Shanghai VPC.

Step 3: Connect the two VPCs

You can connect the two VPCs by creating a pair of Express Connect router interfaces. For more information, see *VPC interconnection*.

The router interface configuration in this tutorial is shown in the following figure.

Step 4: Configure the route

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**. Find the route table of the target VPC and click **Manage**.
3. On the **Route Tables** page, click **Add Route Entry** to add the following routes.

   Add the following route entries for VPC 1 (172.16.0.0/16):

Destination CIDR block	Next hop type	Next hop	Description
10.10.10.0/24 (US office 1)	VPN Gateway	VPN Gateway for VPC 1	Route the traffic destined for 10.10.10.0/24 or 10.10.20.0/24 to the VPN gateway in the US.
10.10.20.0/24 (US office 2)	VPN Gateway	VPN Gateway for VPC 1	
172.17.0.0/16 (Shanghai VPC)	VPC	VPC2	Route the traffic destined for the destination CIDR block to VPC 2.
10.20.10.0/24 (Shanghai office 3)	VPC	VPC2	
10.20.20.0/24 (Shanghai office 4)	VPC	VPC2	

4. Add the following route entries to VPC2 (172.17.0.0/16):

Destination CIDR block	Next hop type	Next hop	Description
10.20.10.0/24 (Shanghai office 3)	VPN Gateway	VPN Gateway for VPC 2	Route the traffic destined for 10.20.10.0/24 or 10.20.20.0/24 to the VPN gateway in Shanghai.
10.20.20.0/24 (Shanghai office 4)	VPN Gateway	VPN Gateway for VPC 2	
172.16.0.0/16 (US VPC)	VPC	VPC1	Route the traffic destined for the destination CIDR block to VPC 1.
10.10.10.0/24 (US office 1)	VPC	VPC1	
10.10.20.0/24 (US office 2)	VPC	VPC1	

Step 5: Configure security rules

Configure security rules for the ECS instances in the VPC networks

according to your individual business requirements.

4 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

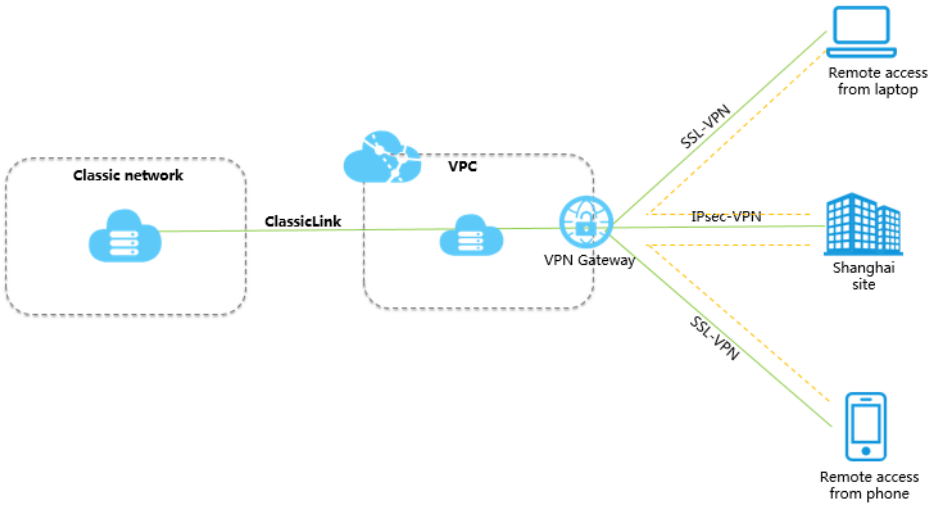
Before you begin, plan your network:

- 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 *Configure a site-to-site connection*.

2. Create an SSL-VPN connection.

   For more information, see *Linux client remote access*.

3. Create a ClassicLink connection.

   For more information, see *Build a ClassicLink connection*.