

Alibaba Cloud vpn gateway

Product Overview

Issue: 20190417

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 .
<code>Courier font</code>	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

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

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 What is VPN Gateway?.....	1
2 Scenarios.....	3
3 Limits.....	7

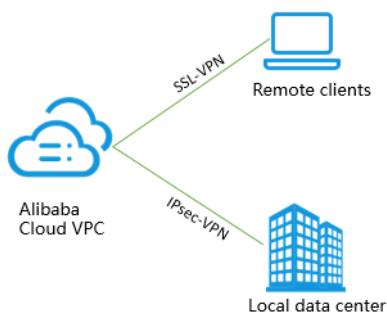
1 What is VPN Gateway?

VPN Gateway is an Internet-based service that securely and reliably connects enterprise data centers, office networks, and Internet terminals to Alibaba Cloud VPCs through encrypted channels. VPN Gateway provides both IPsec-VPN connection and SSL-VPN connection.



Note:

Alibaba Cloud VPN Gateway does not support access to the Internet. The use of VPN Gateway is subject to local laws and policies.



Features

VPN Gateway provides the following features:

- IPsec-VPN

IPsec-VPN provides site-to-site VPN connection. You can use IPsec-VPN to connect a VPC to an on-premises data center or interconnect two VPCs. IPsec-VPN supports the IKEv1 protocol and IKEv2 protocol. Therefore, any devices that support these two protocols can connect to Alibaba Cloud VPN Gateway, including devices from Huawei, H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.

For more information, see [Create a site-to-site connection through IPsec-VPN](#) and [Configure a VPC-to-VPC connection](#).

- **SSL-VPN**

You can create an SSL-VPN connection to connect a remote client to applications deployed in a VPC. When the deployment is complete, you only need to load a certificate in the client to initiate the connection.

For more information, see [Linux client remote access](#), [Window client remote access](#), and [Mac client remote access](#).

Benefits

VPN Gateway offers the following benefits:

- **High security:** You can use the IKE and IPsec protocols to encrypt data to ensure data security and reliability.
- **High availability:** With active/standby hot backup, VPN Gateway automatically switches over to failover mode within seconds to ensure session continuity and service availability.
- **Low cost:** The encrypted Internet-based channel of VPN Gateway is more cost-effective than a leased line.
- **Easy to use:** VPN Gateway is ready for use after you purchase it, with no additional configurations required.

2 Scenarios

This topic describes scenarios that implement Alibaba Cloud VPN Gateway. VPN Gateway is an Internet-based service that securely and reliably connects enterprise data centers, office networks, and Internet terminals to Alibaba Cloud VPCs through encrypted channels. VPN Gateways provides flexible configurations to meet the demands of different scenarios.

IPsec-VPN scenarios

Scenario one: Connect a VPC to an on-premises data center

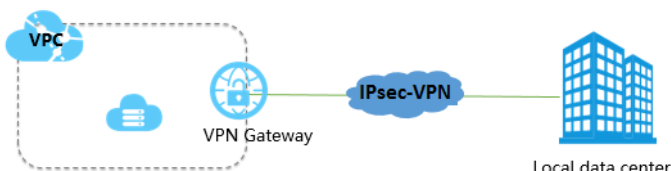
You can build a hybrid cloud environment by creating an IPsec-VPN tunnel to connect a VPC to your on-premises data center.

For more information, see [Configure an IPsec-VPN connection to connect a VPC to an on-premises data center](#).



Note:

The IP address range of the on-premises data center cannot conflict with that of the VPC, and a static public IP address must be configured for the VPN Gateway of the on-premises data center.



Scenario two: Interconnect two VPCs

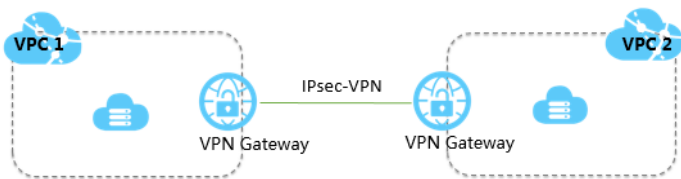
You can use a VPN Gateway to create an IPsec-VPN tunnel to interconnect two VPCs.

For more information, see [Create an IPsec connection to interconnect two VPCs](#).



Note:

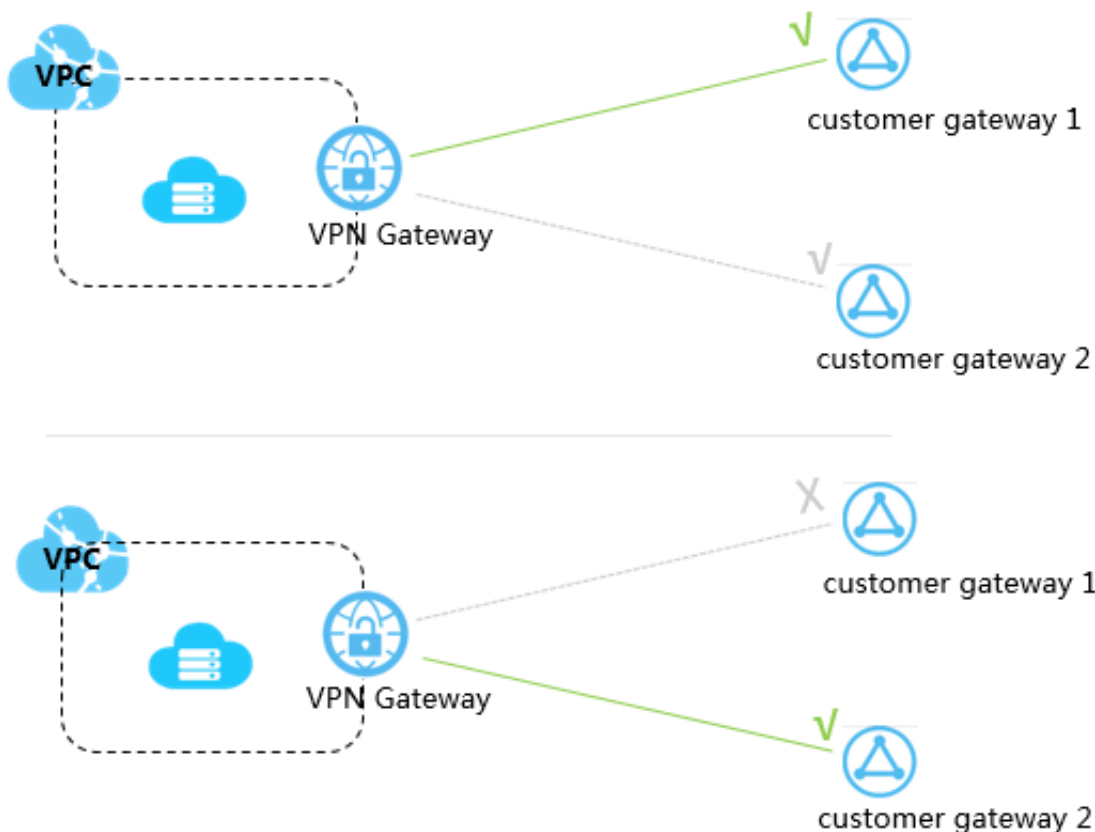
The VSwitch IP address ranges of the VPCs cannot conflict with each other.



Scenario three: Achieve redundancy with multiple VPN connections

One VPN Gateway is deployed at the Alibaba Cloud side and two customer gateways are deployed at the customer side.

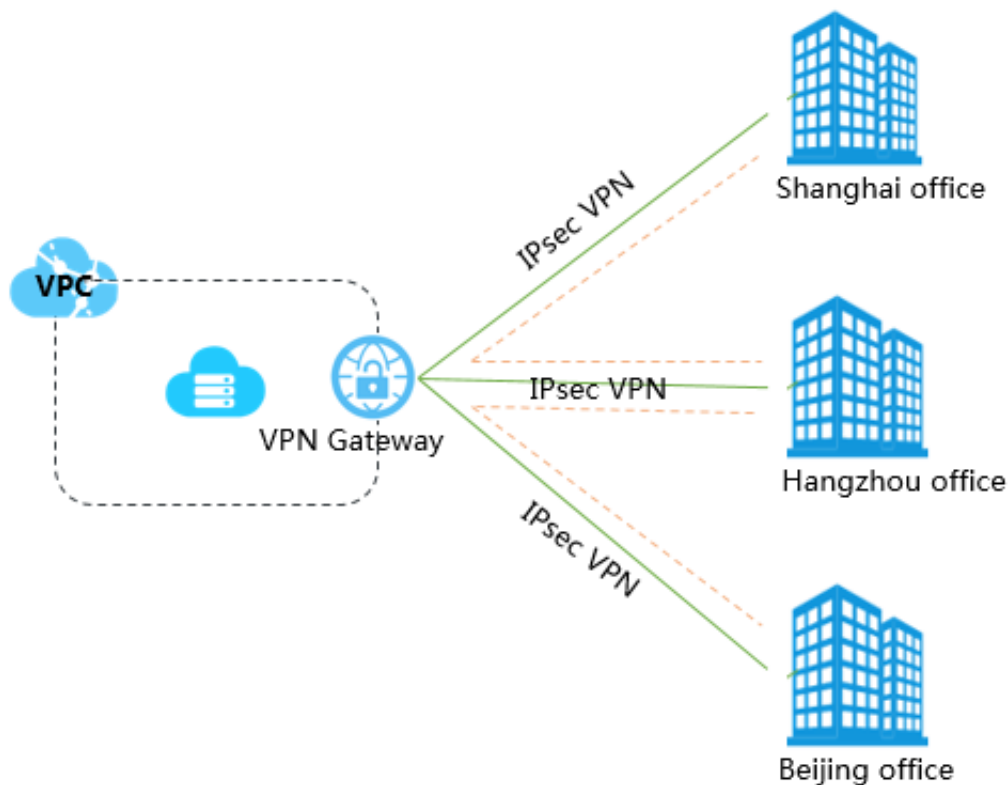
The two customer gateways are connected to the VPN Gateway and an IPsec connection is established between each customer gateway and the VPN Gateway. The two IPsec connections are configured with health checks and have succeeded in negotiation. When a customer gateway is declared as unhealthy, traffic is automatically directed to the other customer gateway.



Scenario four: Hub Spoke connection

You can establish secure communications among multiple sites by using the Hub Spoke function to interconnect the sites through the VPN Gateway of the VPC.

For more information, see [Hub Spoke connection](#).



SSL-VPN scenarios

You can connect a client to a VPC through an SSL-VPN tunnel to meet the needs of remote working. With SSL-VPN connections, you can securely access a VPC through the Internet at anytime, anywhere.

SSL-VPN connections support remote access from clients running various operating systems, including Windows, Linux, Mac, IOS, and Android.

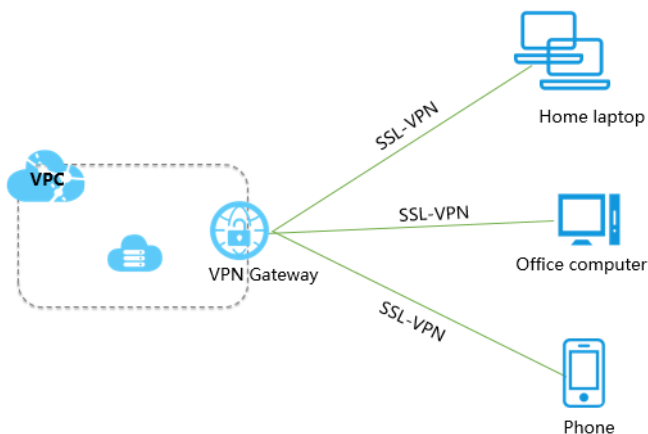
a

For more information, see [Linux client remote access](#), [Windows client remote access](#) and [Mac client remote access](#).



Note:

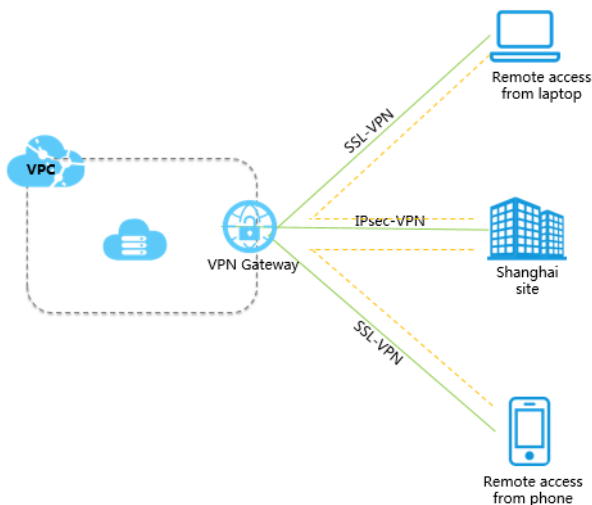
The IP address ranges of clients cannot conflict with the VSwitch IP address range of the VPC.



Use IPsec-VPN and SSL-VPN together

You can establish both IPsec-VPN and SSL-VPN connections to expand your network topology. After the connections are established, clients can access both the VPC and the connected office networks.

 **Note:**
All private IP address ranges to be connected cannot conflict with each other.



3 Limits

The following table describes the maximum limits of different functions of VPN Gateway.

Item	Limit	Can I adjust the limit?
The number of VPN Gateways per account	30	Yes (open a ticket)
The number of customer gateways in a region	100	No
The number of IPsec connections per VPN Gateway	10	No
The number of policy routes per VPN Gateway	20	Yes (open a ticket)
The number of destination routes per VPN Gateway	20	Yes (open a ticket)
The number of SSL servers that can be associated with a VPN Gateway	1	No
The number of clients that can be created by an SSL server	50	No
The number of SSL client creations	100 times	No
The validity period of an SSL client certificate	3 years	No

Furthermore, the following SSL server ports are not allowed: 22, 2222, 22222, 9000, 9001, 9002, 7505, 80, 443, 53, 68, 123, 4510, 4560, 500, and 4500.