ALIBABA CLOUD

Alibaba Cloud

VPN Gateway

Product Overview

Document Version: 20200930

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

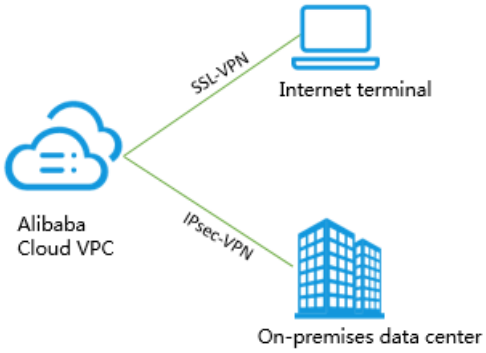
Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is VPN Gateway?

VPN Gateway is an Internet-based service that securely and reliably connects enterprise data centers, office networks, or Internet-facing terminals to Alibaba Cloud Virtual Private Cloud (VPC) networks through encrypted connections. VPN Gateway supports both IPsec-VPN connection and SSL-VPN connection.

> **Note** Alibaba Cloud VPN Gateway provides services complied with the local regulations and policies. VPN Gateway does not provide Internet access services.



Features

VPN Gateway has the following features:

- IPsec-VPN

  The route-based IPsec-VPN facilitates the configuration and maintenance of VPN policies, and provides flexible traffic routing methods.

  You can use IPsec-VPN to connect an on-premises data center to a VPC network or connect two VPC networks. IPsec-VPN supports IKEv1 and IKEv2 protocols. Any devices that support these two protocols can connect to Alibaba Cloud VPN Gateway, such as devices manufactured by Huawei, H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.

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

- SSL-VPN

  SSL-VPN is implemented based on the OpenVPN framework. You can create an SSL-VPN connection to connect a remote client to applications and services deployed in a VPC network. After the deployment is complete, you only need to import the certificate to the client to initiate the connection.

  For more information, see Remote access from a Linux client, Remote access from a Window client, and Remote access from a Mac client.

Benefits

VPN Gateway offers the following benefits:

- High security: You can use the IKE and IPsec protocols to encrypt data to ensure secure and

reliable data transmission.

- High availability: VPN Gateway adopts the hot-standby architecture to achieve failover of less than several seconds, session persistence, and zero service downtime.
- Low cost: The encrypted Internet-based channel of VPN Gateway is more cost-effective than a leased line.
- Ease of use: VPN Gateway is a ready-to-use service that requires no additional configuration.

2.Scenarios

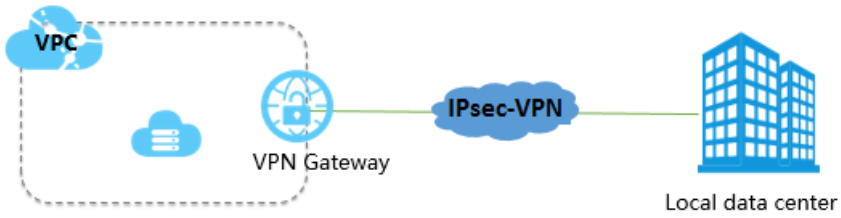
VPN Gateway is an Internet-based service that allows you to connect enterprise data centers, office networks, or Internet-facing terminals to Alibaba Cloud Virtual Private Cloud (VPC) networks through encrypted connections. VPN Gateway can be configured based on your requirements and applied in multiple scenarios.

Connect a VPC network to an on-premises data center

You can use IPsec-VPN to connect an on-premises data center to a VPC network and build a hybrid cloud.

Route-based IPsec-VPN allows you to route network traffic in multiple ways, and also facilitates the configuration and maintenance of VPN policies. For more information, see Establish a connection between a VPC and an on-premises data center.

> **Note** Before you create an IPsec-VPN connection between an on-premises data center and a VPC network, make sure that the IP address of the on-premises data center is different from that of the VPC network. In addition, you must set a static public IP address for your VPN gateway.

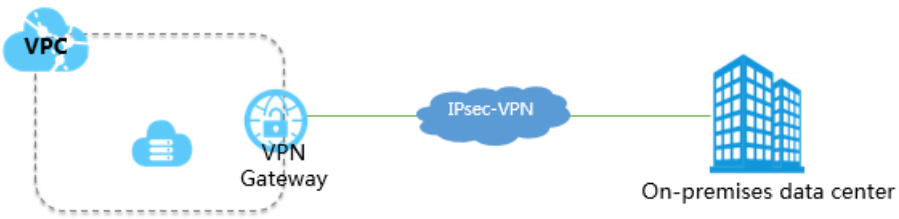


Connect two VPC networks

You can use IPsec-VPN to connect two VPC networks. This way, cloud resources can be shared across these VPC networks.

Route-based IPsec-VPN allows you to route network traffic in multiple ways, and also facilitates the configuration and maintenance of VPN policies. For more information, see Establish a connection between two VPCs.

> **Note** The CIDR blocks of the two VPC networks must not overlap with each other.



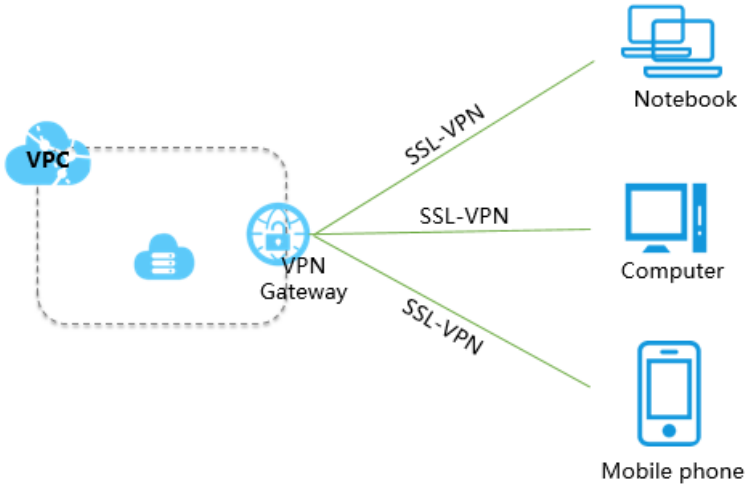
Connect a VPC network to a mobile client

If you require office automation, you can use SSL-VPN to connect a mobile client to a VPC network. This way, the mobile client can access cloud resources deployed in the VPC network anytime and anywhere.

You can initiate an SSL-VPN connection from clients that run Windows, Linux, macOS, iOS, and Android.

For more information, see Create a remote connection from a Linux client, Create a remote connection from a Windows client and Create a remote connection from a macOS client.

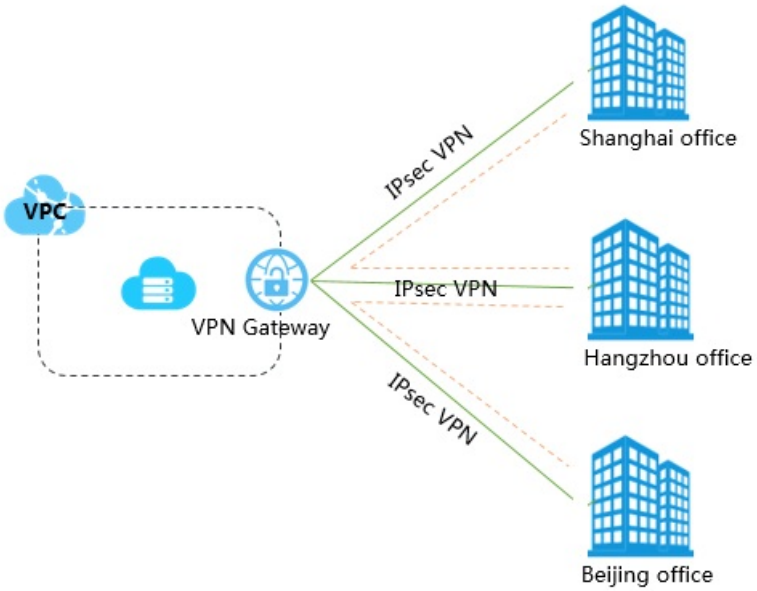
> **Note** The CIDR block assigned to the client must not overlap with that of the VSwitch in the VPC network.



Hub-and-Spoke VPN

You can use Hub-and-Spoke VPN to connect multiple sites. These sites can communicate with each other through VPC networks, which ensures the security of data transmission. Hub-and-Spoke VPN enables branches of large enterprises to communicate with each other through the intranet.

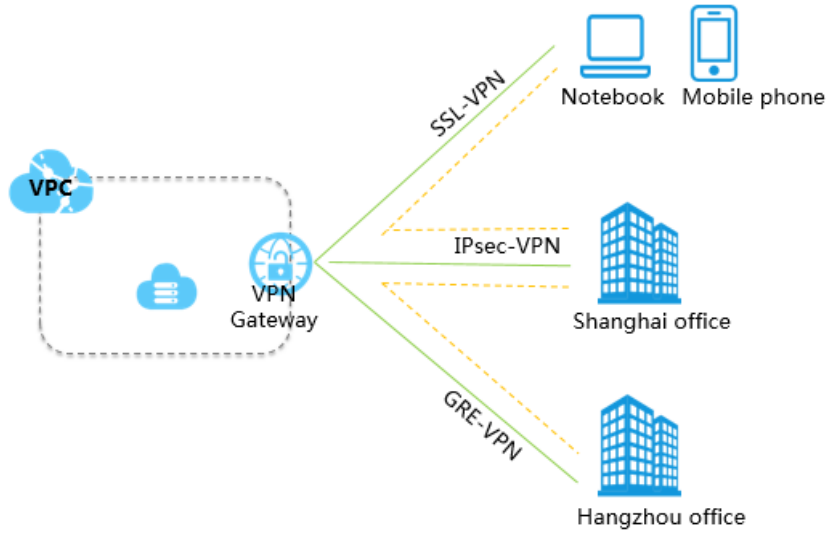
For more information, see Configure Hub-and-Spoke VPN connections.



Use IPsec-VPN and SSL-VPN together

You can use IPsec-VPN and SSL-VPN connections together to expand your network topology. After the connections are established, the client can access the applications deployed in the connected VPC network, and can also access the applications deployed in the connected office networks.

> **Note** The private CIDR blocks to be interfaced must not overlap with each other.



3.Limits

This topic describes the limits on using VPN gateways. Before you use a VPN gateway, note the following limits.

Instance limits

Item	Limit	Adjustable
Number of VPN gateways that can be created for each account	30 Note The maximum number of VPN gateways that can be created is determined by the account, regardless of the region where the VPN gateways are deployed or the VPC networks to which the VPN gateways belong. For example, for each account: • You can create up to 30 VPN gateways that are deployed in a Virtual Private Cloud (VPC) network within a region. • You can create up to 30 VPN gateways that are deployed in multiple VPC networks across multiple regions.	Go to the Quota Management page and request a quota increase. For more information, see Manage quotas.
Number of policy-based routes that can be created for each VPN gateway	20	
Number of destination-based routes that can be created for each VPN gateway	20	

Customer gateways

Item	Limit	Adjustable
Number of customer gateways that can be created in a region	100	N/A

IPsec-VPN connections

Item	Limit	Adjustable
Number of IPsec-VPN connections that can be created for each VPN gateway	10	Go to the Quota Management page and request a quota increase. For more information, see Manage quotas.
Maximum bandwidth that each IPsec-VPN connection supports	200M Note If the maximum bandwidth of a VPN gateway is higher than 200 Mbit/s, you can create multiple IPsec-VPN connections to make full use of the bandwidth of the VPN gateway. For more information, see How to make full use of VPN Gateway bandwidth.	N/A
Number of source CIDR blocks that can be added to each IPsec-VPN connection	5	
Number of destination CIDR blocks that can be added to each IPsec-VPN connection	5	

SSL-VPN connections

Item	Limit	Adjustable
Number of SSL client certificates that each account can reserve	50	Go to the Quota Management page and request a quota increase. For more information, see Manage quotas.

Item	Limit	Adjustable
Number of SSL servers that can be associated with each VPN gateway	1	N/A
Number of source CIDR blocks that can be added to each SSL server	5	
Number of destination CIDR blocks that can be added to each SSL server	1	
Ports that are not supported by SSL servers	22, 2222, 22222, 9000, 9001, 9002, 7505, 80, 443, 53, 68, 123, 4510, 4560, 500, and 4500	
Validity period of an SSL client certificate	Three years	