

Alibaba Cloud

VPN Gateway FAQ

Document Version: 20220302

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.FAQ about IPsec-VPN connections	05
2.FAQ about VPN gateways	09

1. FAQ about IPsec-VPN connections

1. What can I do if the state of an IPsec-VPN connection indicates "Phase 1 negotiations failed"?

When the configuration of the VPN gateway on Alibaba Cloud is different from that of the on-premises VPN gateway, Phase 1 negotiations may fail. The following table describes the possible causes and solutions.

Cause	Solution	Log
The pre-shared keys are different.	Configure the same pre-shared key on both VPN gateways.	<pre>invalid HASH_V1 payload length, decryption failed? could not decrypt payloads message parsing failed</pre>
The IKE protocol versions are different.	Configure the same IKE version. For example, you can set the IKE protocol version to IKEv1 or IKEv2 on both VPN gateways of the IPsec-VPN connection.	<pre>parsed IKE_SA_INIT response 0 [N(NO_PROP)] received NO_PROPOSAL_CHOSEN notify error received AUTHENTICATION_FAILED error notify</pre>
The negotiation modes are different.	Configure the same negotiation mode. For example, you can set the negotiation mode to main or aggressive on both VPN gateways of the IPsec-VPN connection.	<pre>received AUTHENTICATION_FAILED error notified</pre>
The values of LocalId or RemoteId are different.	Set the same value for LocalId or RemoteId on both VPN gateways.	<pre>[IKE] IDir xxxx does not match to xxxx</pre>
The encryption or authentication algorithms are different.	Configure the same encryption and authentication algorithms on both VPN gateways.	N/A
The DH groups are different.	Configure the same DH group. For example, you can set the DH group to group 2 on both VPN gateways of the IPsec-VPN connection.	N/A

Cause	Solution	Log
The peering VPN gateway does not respond.	Make sure that the peering VPN gateway functions as expected.	<pre>[IKE] sending retransmit 1 of request message ID 0, seq 1</pre>
A wrong public IP address is specified when you create the customer VPN gateway.	You must specify the public IP address of the on-premises VPN gateway when you create the customer gateway.	<pre>received UNSUPPORTED_CRITICAL_PAYLOAD error notify</pre>

In some scenarios, the state of the IPsec-VPN connection indicates "Phase 1 negotiations failed" even if the preceding configurations on both VPN gateways are the same. To resolve this problem, we recommend that you change the negotiation mode to aggressive.

2. What can I do if the state of an IPsec-VPN connection indicates "Phase 2 negotiations failed" ?

The following table describes the possible causes and solutions.

Cause	Solution	Log
The interesting traffic flows are different.	Check the private CIDR blocks of both VPN gateways of the IPsec-VPN connection. Make sure that the private CIDR blocks are set correctly.	<ul style="list-style-type: none"> • Main mode <pre>received INVALID_ID_INFORMATION error notify</pre> • Aggressive mode <pre>received HASH payload does not match integrity check failed</pre>
The encryption or authentication algorithms are different.	Configure the same encryption and authentication algorithms on both VPN gateways of the IPsec-VPN connection.	<pre>parsed INFORMATIONAL_V1 request xxxx [HASH N(NO_PROP)] received NO_PROPOSAL_CHOSEN error notify</pre>

Cause	Solution	Log
The DH groups are different.	Configure the same DH group on both VPN gateways of the IPsec-VPN connection.	<pre> ESP:AES_CBC_256/HMAC_SHA1_96/MODP_1024/NO_EXT_SEQ ESP:AES_CBC_128/HMAC_SHA1_96/MODP_1024/NO_EXT_SEQ, ESP:AES_CBC_128/AES_CBC_192/AES_CBC_256/3DES_CBC/BLOWFISH_CBC_256/HMAC_SHA2_256_128/HMAC_SHA2_384_192/HMAC_SHA2_512_256/HMAC_SHA1_96/AES_XCBC_96/HMAC_MD5_96/NO_EXT_SEQ no matching proposal found, sending NO_PROPOSAL_CHOSEN </pre>

3. What can I do if the state of an IPsec-VPN connection indicates “Phase 2 negotiations succeeded” , but the Elastic Compute Service (ECS) instances in the virtual private cloud (VPC) cannot access the servers in the on-premises data center?

If public IP addresses are used as private IP addresses within the on-premises data center and the ECS instances can access the Internet, submit a ticket to modify the configuration. Otherwise, check the routes and other relevant configurations based on the following information:

- Check the routes on the router of the VPC.
- Check the configuration of the firewall or iptables in the on-premises data center. Make sure that requests sent from the private CIDR block of the VPC are allowed to reach the on-premises data center.

4. What can I do if the state of an IPsec-VPN connection indicates “Phase 2 negotiations succeeded” , but servers in the on-premises data center cannot access the ECS instances in the VPC?

Check the configurations based on the following information:


- Check the routes and ACLs in the on-premises data center. Make sure that data is allowed to be transmitted to the VPC through the IPsec-VPN connection.
- Check the rules in the security group of the ECS instances. Make sure that requests from the private CIDR block of the on-premises data center are allowed to reach the ECS instances.

5. What can I do if the state of the IPsec-VPN connection indicates “Phase 2 negotiations succeeded” , but communication is successful only in some of the CIDR blocks?

Check whether the IKEv2 protocol is used. If you want to establish an IPsec-VPN connection to connect multiple CIDR blocks, we recommend that you use the IKEv2 protocol.

If the IKEv2 protocol is used, check the Security Association (SA) on the on-premises VPN gateway. In most cases, only one SA is created for each IPsec-VPN connection, for example, 172.30.96.0/19 ==> 10.0.0.0/8 172.30.128.0/17.

If more than one SA exists, it indicates that the IKEv2 protocol that the on-premises VPN gateway uses is not a standard protocol. To resolve this problem, you must create multiple IPsec-VPN connections to connect the CIDR blocks. For example, you can split the IPsec-VPN connection 172.30.96.0/19 <=> 10.0.0.0/8 172.30.128.0/17 into IPsec-VPN connection A 172.30.96.0/19 <=> 10.0.0.0/8 and IPsec-VPN connection B 172.30.96.0/19 <=> 172.30.128.0/17.

 **Note** The two IPsec-VPN connections must share the Phase 1 SA. Make sure that the same Phase 1 negotiation settings are configured for the IPsec-VPN connections.

2.FAQ about VPN gateways

This topic provides answers to some frequently asked questions about VPN gateways.

- [Can I deploy a VPN gateway in a classic network?](#)
- [What are the prerequisites for connecting a data center to a VPC through IPsec-VPN?](#)
- [Can I use VPN gateways to connect VPCs across regions?](#)
- [What types of gateway devices can connect to VPN gateways?](#)
- [How many IPsec-VPN connections can be established to a VPN gateway?](#)
- [Can I use VPN gateways to access the Internet?](#)
- [Does network traffic between VPCs traverse the Internet?](#)
- [Can I specify more than one client CIDR block for an IPsec-VPN connection?](#)
- [Can I downgrade a VPN gateway?](#)
- [Can I enable SSL-VPN for VPN gateways that are created before the release date of SSL-VPN?](#)
- [How can I configure network access control list \(ACL\) rules on a VPN gateway?](#)
- [Why am I unable to connect to an AWS VPN gateway through IPsec-VPN?](#)

Can I deploy a VPN gateway in a classic network?

No, you cannot deploy a VPN gateway in a classic network.

VPN gateways support only virtual private clouds (VPCs). If you want the resources in a classic network to use the VPN gateway of a VPC, you must enable ClassicLink for the VPC. For more information, see [Connect a data center to a classic network by using IPsec-VPN](#).

What are the prerequisites for connecting a data center to a VPC through IPsec-VPN?

- The gateway device of the data center must support the IKEv1 and IKEv2 protocols.
IPsec-VPN supports both IKEv1 and IKEv2. All gateway devices that support the IKEv1 and IKEv2 protocols can connect to VPN gateways on Alibaba Cloud.
- A static public IP address is assigned to the gateway device in the data center.
- The client CIDR block and the VPC CIDR block do not overlap with each other.

For more information about how to connect a data center to a VPC through IPsec-VPN, see [Connect a data center to a VPC](#).

Can I use VPN gateways to connect VPCs across regions?

Yes, you can use VPN gateways to connect VPCs across regions. For more information, see [Establish IPsec-VPN connections between two VPCs](#).

What types of gateway devices can connect to VPN gateways?

Alibaba Cloud VPN gateways support the standard IKEv1 and IKEv2 protocols. All gateway devices that support the IKEv1 and IKEv2 protocols can connect to VPN gateways on Alibaba Cloud. For example, gateway devices manufactured by H3C, Hillstone, Sangfor, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia can connect to VPN gateways on Alibaba Cloud. For more information, see [Configure a gateway device in a data center](#).

How many IPsec-VPN connections can be established to a VPN gateway?

By default, you can establish at most 10 IPsec-VPN connections to a VPN gateway. To create more IPsec-VPN connections, request a quota increase. For more information, see [Manage quotas](#).

Can I use VPN gateways to access the Internet?

No, you cannot use VPN gateways to access the Internet.

You can use VPN gateways to access only VPCs through private connections.

Does network traffic between VPCs traverse the Internet?

No, network traffic between VPCs does not traverse the Internet.

When you use VPN gateways to connect VPCs across regions, network traffic is transmitted only within Alibaba Cloud.

Can I specify more than one client CIDR block for an IPsec-VPN connection?

Yes, you can specify more than one client CIDR block for an IPsec-VPN connection.

We recommend that you specify IKEv2 when you create the connection.

Can I downgrade a VPN gateway?

Yes, you can downgrade a VPN gateway.

To downgrade a VPN gateway, [submit a ticket](#).

Can I enable SSL-VPN for VPN gateways that are created before the release date of SSL-VPN?

No, you cannot enable SSL-VPN for VPN gateways that are created before the release date of SSL-VPN.

If you want to enable SSL-VPN for VPN gateways that are created before the release date, [submit a ticket](#).

How can I configure network access control list (ACL) rules on a VPN gateway?

Type of VPN gateway	Rule Configuration
IPsec-VPN	<p>Configure outbound and inbound rules to allow the following CIDR block and IP addresses. This way the VPN gateway can establish IPsec-VPN connections.</p> <ul style="list-style-type: none">• 100.104.0.0/16• The IP address of the customer gateway• The IP address of the VPN gateway

Type of VPN gateway	Rule Configuration
SSL-VPN	<p>Configure inbound and outbound rules to allow the following IP addresses and CIDR block and open the following port. This way, the VPN gateway can establish SSL-VPN connections.</p> <ul style="list-style-type: none">• 100.104.0.0/16• The public IP address of the client• The IP address of the VPN gateway• The port that can be used by SSL-VPN connections. <p>For example, you can specify port 1194.</p>

Why am I unable to connect to an AWS VPN gateway through IPsec-VPN?

- Cause

When you use an AWS VPN gateway to create an IPsec-VPN connection, each tunnel of the IPsec-VPN connection supports only one security association (SA). If the routing mode of the IPsec-VPN connection on the Alibaba Cloud side is set to Protected Data Flows and multiple VPC CIDR blocks or client CIDR blocks are specified for the IPsec-VPN connection, the AWS VPN gateway cannot forward traffic.

- Solution

- If the routing mode of the IPsec-VPN connection on Alibaba Cloud is set to Protected Data Flows, you must specify only one VPC CIDR block and one client CIDR block.
- Change the routing mode of the IPsec-VPN connection on Alibaba Cloud to Destination Routing Mode.