

Alibaba Cloud vpn gateway

FAQ

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.
Courier font	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 VPN Gateway.....	1
2 IPsec-VPN connections FAQ.....	3

1 VPN Gateway

1. Does VPN Gateway support the classic network?

Not supported. VPN Gateway supports only the VPC network. If you want to use VPN Gateway in the classic network, you must enable the ClassicLink function in VPC. For more information, see [Use IPsec-VPN in the classic network](#).

2. What are the prerequisites for a local site to access VPC through the IPsec-VPN function?

A static public IP and a gateway device supporting IKEv1 and IKEv2 are required. The CIDR block of the VPC and the CIDR block of the local site do not conflict with each other. For more information, see [Create a site-to-site connection through IPsec-VPN](#).

3. Can VPCs in different regions use VPN Gateway to achieve intercommunication?

Yes. For more information, see [Configure a VPC-to-VPC connection](#).

4. Which local gateways does VPN Gateway support?

IPsec connections support IKEv1 and IKEv2 protocols. Therefore, any device that supports these two protocols can connect to Alibaba Cloud VPN Gateway. These devices include those from Huawei, H3C, Cisco, ASN, Juniper, SonicWall, Nokia, IBM, and Ixia. For more information, see [#unique_7](#).

5. Does VPN Gateway support SSL-VPN?

Yes. For more information, see [Tutorial overview](#).

6. How many IPsec connections can be created for each VPN Gateway?

Each VPN Gateway can support up to 10 IPsec connections. If you want more IPsec connections, create more VPN Gateways.

7. Can I use VPN Gateway to access the Internet?

No, it cannot. VPN Gateway only provides intranet access to VPCs. It does not provide access to the Internet.

8. Does the traffic between two VPCs connected by VPN Gateway go through the Internet?

No. Cross-region VPC intercommunication is achieved through VPN, and the traffic passes through Alibaba Cloud network instead of the Internet.

9. Can I configure multiple remote networks in one IPsec connection?

Yes. You can separate the networks by commas. We recommend that you use the IKEv2 protocol.

10. Can I downgrade the VPN Gateway configuration?

Yes. You can submit a ticket to downgrade the configuration.

11. Can a VPN Gateway instance purchased before the launching of the SSL-VPN function use this function?

You cannot directly enable the SSL-VPN function on a VPN Gateway instance purchased before the launching of this function. You must open a ticket if you want to enable the SSL-VPN function in this situation.

2 IPsec-VPN connections FAQ

1. What do I do if the IPsec-VPN connection status is “Phase 1 of IKE Tunnel Negotiation Failed” ?

A negotiation failure during IKE phase one negotiation may be caused by inconsistent parameters between the phase one configuration of the Alibaba Cloud VPN Gateway

and that of the local gateway. Possible causes and corresponding solutions are provided in the following table.

Cause	Solution	Log
The pre-shared keys are inconsistent.	Use the same pre-shared key when you create the IPsec-VPN connection and configure the local gateway.	invalid HASH_V1 payload length , decryption failed ? could not decrypt payloads message parsing failed
The IKE protocol versions are inconsistent.	Use the same IKE version. For example , you can set the IKE version to IKEv1 or IKEv2 for both ends of the IPsec-VPN connection.	parsed IKE_SA_INI T response 0 [N (NO_PROP)] received NO_PROPOSA L_CHOSEN notify error received AUTHENTICA TION_FAILE D error notify
The negotiation modes are inconsistent.	Use the same negotiation mode. For example, you can set the negotiation mode to main or aggressive for both ends of the IPsec-VPN connection.	received AUTHENTICA TION_FAILE D error notified
The LocalIds or RemoteIds are inconsistent.	Use the same LocalId and RemoteId.	[IKE] IDir xxxx does not match to xxxx
The encryption or authentication	Use the same encryption and	None

Cause	Solution	Log	
The DH groups are inconsistent.	Use the same DH group. For example, you can set the DH group to group2 for both ends of the IPsec-VPN connection.	None	
The peer-end gateway does not respond.	Make sure that the peer-end gateway is normal.	[IKE] sending retransmit 1 of request message ID 0 , seq 1	
An invalid public IP address is set when you create the customer gateway.	Set a valid public IP address of the local gateway when you create the customer gateway.	received UNSUPPORTED_CRITICAL_PAYLOAD error notify	

In some extreme cases, the negotiation fails even when the parameters are completely consistent. In this situation, we recommend that you change the negotiation mode to the aggressive mode.

2. What do I do if the IPsec-VPN connection status is “Phase 2 of IKE Tunnel Negotiation Failed” ?

Possible causes for an IKE phase two negotiation failure, and corresponding solutions, are provided in the following table.

Cause	Solution	Log
The local network and remote network parameters configured in the Alibaba Cloud VPN Gateway are inconsistent with those configured in the local gateway.	Check the CIDR blocks that are configured for both ends of the IPsec-VPN connection and make sure that they are set correctly.	<ul style="list-style-type: none"> main mode <pre>received INVALID_ID _INFORMATI ON error notify</pre> aggressive mode <pre>received HASH payload does not match integrity check failed</pre>
The encryption or authentication algorithms are inconsistent.	Check the encryption and authentication algorithms that are configured for both ends of the IPsec-VPN connection and make sure that you use the same encryption and authentication algorithms.	<pre>parsed INFORMATIO NAL_V1 request xxxx [HASH N (NO_PROP)] received NO_PROPOSA L_CHOSEN error notify</pre>
The DH groups are inconsistent.	Set the same DH groups for both ends of the IPsec-VPN connection.	<pre>ESP : AES_CBC_25 6 / HMAC_SHA1_ 96 / MODP_1024 / NO_EXT_SEQ ESP : AES_CBC_12 8 / HMAC_SHA1_ 96 / MODP_1024 / NO_EXT_SEQ , ESP : AES_CBC_12 8 / AES_CBC_19 2 / AES_CBC_25 6 / 3DES_CBC / BLOWFISH_C BC_256 / HMAC_SHA2_ 256_128 / HMAC_SHA2_ 384_192 / HMAC_SHA2_ 512_256 / HMAC_SHA1_ 96 / AES_XCBC_9 6 / HMAC_MD5_9 6 / NO_EXT_SEQ no matching proposal found , sending NO_PROPOSA L_CHOSEN</pre>

3. What do I do if the IPsec-VPN connection status is “Phase 2 of IKE Tunnel Negotiation Succeeded” , but ECS instances in the VPC cannot access servers in the on-premises data center?

If the on-premises data center uses a public IP address as a private IP address and ECS instances can access the Internet, you need to open a ticket to adjust the configurations. Additionally, you can check the route configurations as follows:

- Check route configurations on the VRouter.
- Check firewall/iptables configurations of the on-premises data center and make sure that access from the private networks of the VPC are allowed.

4. What do I do if the IPsec-VPN connection status is “Phase 2 of IKE Tunnel Negotiation Succeeded” , but servers in the on-premises data center cannot access ECS instances in the VPC?

Check the configurations by referring to the following information:

1. Check if the routing and ACL configurations in the on-premises data center allow traffic destined for the VPC to enter the VPN tunnel.
2. Check if security group rules of the ECS instances allow access from the private networks of the on-premises data center.

5. Why the IPsec-VPN connection status is “Phase 2 of IKE Tunnel Negotiation Succeeded” , but in my multi-network scenario some networks can communicate normally while some networks cannot?

Usually, the IKE V2 protocol is not being used. In multi-network scenarios, we recommend that you use the IKE V2 protocol.

If you have used the IKE V2 protocol but the problem persists, we recommend that you check the SA (Security Association) status of the gateway of the on-premises data center. Normally only one SA exists. For example, 172.30.96.0/19 == 10.0.0.0/8 172.30.128.0/17.

If multiple SAs exist, the gateway of the on-premises data center is using a non-standard IKE V2 protocol. As a result, you can only use multiple IPsec-VPN connections to connect the networks. For example, you can split the IPsec-VPN connection 172.30.96.0/19 <=> 10.0.0.0/8 172.30.128.0/17 to 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:

Because two separated IPsec-VPN connections must share the first-phase SA, the first-phase negotiation parameters of the two IPsec-VPN connections must be consistent.

6. Why is my IPsec-VPN connection through my USGX series NGFW device from Huawei abnormal even though its status is “Phase 2 of IKE Tunnel Negotiation Succeeded” ?

Cause: The Huawei firewall device has NAT enabled at the outbound interface, which means the IP addresses of all packets sent from the outbound interface are converted to the IP address of this interface.

Solution:

1. Run the `nat disable` command to disable the NAT function.
2. Configure NAT policies.

```
nat - policy    interzone    trust    untrust    outbound
policy    0
action    no - nat
policy    source    192 . 168 . 0 . 0    mask    24
policy    destination    192 . 168 . 1 . 0    mask    24
policy    1
action    source - nat
policy    source    192 . 168 . 0 . 0    mask    24
easy - ip    Dialer0
```

Where:

192.168.0.0 is the intranet CIDR block of the local gateway.

192.168.1.0 is the intranet CIDR block of the VPN Gateway.

Dialer0 is the outbound interface of the local gateway.