ALIBABA CLOUD

阿里云

VPN网关

常见问题

文档版本：20201109

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.VPN网关常见问题

本文为您介绍VPN网关的常见问题及解答。

VPN网关是否支持经典网络？

不支持。VPN网关仅支持专有网络，如果您想在经典网络中使用VPN网关，需要在专有网络中开启ClassicLink功能。详细信息，请参见在经典网络中使用IPsec-VPN。

本地站点通过IPsec-VPN接入VPC的前提条件是什么？

本地站点需要一个静态公网IP和一个支持IKEv1和IKEv2协议的网关设备，并且VPC和本地站点之间需要互通的两个网段不冲突。详细信息，请参见建立VPC到本地数据中心的连接。

跨地域VPC是否可以通过VPN网关互通？

可以。详细信息，请参见建立VPC到VPC的连接。

哪些本地网关设备可以与阿里云VPN网关建立连接？

阿里云VPN网关支持标准的IKEv1和IKEv2协议。因此，只要支持这两种协议的设备都可以和云上VPN网关互连，例如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM和Ixia等。详细信息，请参见华三防火墙配置。

每个VPN网关可以建立多少个IPsec连接？

每个VPN网关默认支持创建10个IPsec连接。如需创建更多IPsec连接，请提升配额。详细信息，请参见管理配额。

是否可以通过VPN网关访问Internet？

不可以。VPN网关仅提供私网接入VPC功能，不提供Internet访问的功能。

VPC间互通流量是否经过Internet？

不经过。通过VPN网关实现跨地域VPC互连，流量只经过阿里云网络，不经过Internet。

是否支持在一个IPsec连接中配置多个对端网段？

支持。如果一个IPsec连接配置多个对端网段，建议IKE版本选择IKEv2。

是否可以降低VPN网关配置？

可以。如需降低VPN网关配置，请提交工单。

SSL-VPN发布前购买的VPN网关实例是否可以使用SSL-VPN功能？

SSL-VPN发布前购买的VPN网关实例无法使用SSL-VPN功能。如需使用，请提交工单。

如何充分利用VPN网关带宽？

一条IPsec连接支持的最大带宽峰值为200M，如果您的VPN网关的带宽峰值大于200M，您可以通过创建多条IPsec连接实现充分利用VPN网关带宽。

例如，您的VPN网关的带宽峰值为800M，云上私网网段为10.0.0.0/8，云下私网网段为192.168.0.0/24，您可以配置4条IPsec连接，每条IPsec连接的本端网段和对端网段的配置如下：

- IPsec连接1

  本端网段：10.0.0.0/10，对端网段：192.168.0.0/24

- IPsec连接2

  本端网段：10.64.0.0/10，对端网段：192.168.0.0/24

- IPsec连接3

  本端网段：10.128.0.0/10，对端网段：192.168.0.0/24

- IPsec连接4

  本端网段：10.192.0.0/10，对端网段：192.168.0.0/24

其他参数配置，请参见建立VPC到本地数据中心的连接。

VPN网关中如何为网络ACL配置规则？

- 如果您在VPN所在的子网中使用了网络ACL，需要在网络ACL的出方向和入方向分别配置规则允许放行：100.104.0.0/16。
- 如果在SSL-VPN中使用了网络ACL，网络ACL需配置规则允许放行1194端口。

2.IPsec连接常见问题

1. IPsec连接状态为“第一阶段协商失败”怎么办？

IPsec VPN第一阶段协商失败，可能与阿里云VPN网关同本地VPN网关的第一阶段配置参数不一致有关，可能的原因、解决方法及日志如下表：

原因	解决方法	日志
预共享密钥不一致。	设置一致的预共享密钥。	invalid HASH_V1 payload length, decryption failed? could not decrypt payloads message parsing failed
IKE协议版本不一致。	设置一致的IKE协议版本，如建立IPsec连接的两端网关都设置为IKEv1版本或IKEv2版本。	parsed IKE_SA_INIT response 0 [N(NO_PROP)] received NO_PROPOSAL_CHOSEN notify error received AUTHENTICATION_FAILED error notify
协商模式不一致。	设置一致的协商模式，如建立IPsec连接的两端网关都设置为main或aggressive。	received AUTHENTICATION_FAILED error notifyed
LocalId或RemoteId不一致。	设置一致的LocalId或RemoteId。	[IKE] IDir xxxx does not match to xxxx
加密、认证算法不一致。	确认两端网关的加密、认证算法，并设置一致。	无
DH分组不一致。	设置一致的DH组，如建立IPsec连接的两端网关都将DH组设置为group2。	无
对端网关不响应。	确认对端网关是否异常。	[IKE] sending retransmit 1 of request message ID 0, seq 1
创建用户网关时，设置错误的公网IP。	创建用户网关时，应设置本地网关的公网IP。	received UNSUPPORTED_CRITICAL_PAYLOAD error notify

部分极端情况下，参数完全一致也无法协商成功，此时建议将两端的协商模式改为野蛮模式（aggressive）。

2. IPsec连接状态为“第二阶段协商失败”怎么办？

IPsec连接第二阶段协商失败的可能原因、解决方法及日志如下表：

原因	解决方法	日志
感兴趣流不一致。	确认建立IPsec连接的两端网关的私网网段，并正确设置。	• 主模式 received INVALID_ID_INFORMATION error notify • 野蛮模式 received HASH payload does not match integrity check failed
加密算法或认证算法不一致。	确认两端网关的加密、认证算法，并设置一致。	parsed INFORMATIONAL_V1 request xxxx [HASH N(NO_PROP)] received NO_PROPOSAL_CHOSEN error notify
DH分组不一致。	设置一致的DH组。	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

3. 为什么IPsec连接状态为“第二阶段协商成功”，但VPC内的ECS实例无法访问本地IDC内的服务器？

如果本地IDC内存在将公网IP作为私有IP使用的情况且ECS实例可以访问公网，需要提交工单进行相关配置。否则请参考以下信息检查路由等相关配置：

- 检查VPC路由器上的路由配置。
- 检查本地IDC内的防火墙/iptables相关的设置，确认是否允许VPC的私网网段访问。

4. 为什么IPsec连接状态为“第二阶段协商成功”，但本地IDC内的服务器无法访问VPC内的ECS实例？

请参考以下信息检查配置：

- 检查本地IDC内的路由和ACL配置是否允许访问VPC的流量进入VPN隧道。
- 检查ECS实例的安全组规则是否允许本地IDC中的私网网段访问。

5. 为什么IPsec连接状态为“第二阶段协商成功”，但是多网段场景下部分网段通信正常，部分网段通信不正常？

多网段场景下，建议使用IKE V2协议。

如果已经使用了IKE V2协议但问题仍然存在，建议检查本地IDC的VPN网关的SA状态，正常情况下只有一个SA，例如172.30.96.0/19 === 10.0.0.0/8 172.30.128.0/17。

如果存在多个SA说明本地IDC的VPN网关使用非标准的IKE V2协议，此时只能使用多个IPsec连接将各个网段连接起来。例如可以将IPsec连接：172.30.96.0/19 <=> 10.0.0.0/8 172.30.128.0/17拆分为IPsec连接A：172.30.96.0/19 <=> 10.0.0.0/8和IPsec连接B：172.30.96.0/19 <=> 172.30.128.0/17。

> **说明** 拆分IPsec连接后由于两个IPsec连接需要共享第一阶段SA，所以两个IPsec连接的第一阶段协商参数需保持一致。

6. 为什么IPsec连接状态为“第二阶段协商成功”，但IPSec VPN单向不通？

原因：本地网关使用的是华为防火墙，且在出接口配置了nat enable，导致从该接口流出的所有数据包的源IP地址，都转换为该接口的IP地址。

解决方法：

1. 运行 `nat disable` 命令，关闭出接口的NAT功能。
2. 配置NAT策略。

```
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
```

其中：

192.168.0.0：本地网关的私网网段。

192.168.1.0：VPC侧VPN网关的私网网段。

Dialer0：本地网关的出接口。