ALIBABA CLOUD

阿里云

VPN网关

公告

文档版本：20201225

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网关支持BGP动态路由公告

VPN网关支持BGP（Border Gateway Protocol）动态路由功能，云上云下通过VPN网关建立连接，并通过BGP动态路由协议自动学习路由实现资源互通，降低网络维护成本和网络配置风险。

> **说明** 目前VPN网关BGP动态路由功能白名单开放。如需使用，请提交工单。

BGP动态路由简介

BGP是一种基于TCP协议的动态路由协议，主要应用于不同自治系统间交换路由信息和网络可达信息。

VPN网关的BGP动态路由功能是在IPsec连接的基础上增加的子功能。BGP动态路由集成CEN动态路由收发能力，帮助您更高效、灵活且可靠的建立VPN连接，实现云上和云下网络的互通。

BGP动态路由具有以下能力：

- 自动宣告云上和云下的动态路由，并具备自动处理路由冲突机制。
- 同时支持静态路由和动态路由，实现自定义指定流量出口。
- 同一VPN网关与同一本地数据中心创建多隧道连接，支持等值多路径路由协议ECMP（Equal-Cost Multipath Routing），实现高可用容灾。

> **注意** 使用BGP动态路由建立VPN连接前，您必须了解以下注意事项：
>
> - 如果您使用物理专线和VPN网关以主备的方式将云下本地数据中心接入云上VPC，为避免本地数据中心网络路由震荡，请确保边界路由器和VPN网关配置的本地数据中心的自治系统号（ASN）一致。
> - 如果您有多个VPC加载到同一云企业网，为避免云上网络路由震荡，请确保VPC关联的VPN网关未使用BGP路由协议建立连接。
> - 如果您使用同一云上VPN网关与不同本地数据中心建立VPN连接，禁止将不同VPN连接的路由互导。
> - 如果一个VPC创建了多个VPN网关，禁止将不同VPN网关的路由互导。

动态路由宣告原则

使用VPN网关建立VPN连接后，动态路由宣告原则如下：

- 云下到云上方向

  云下VPN网关通过BGP动态路由协议自动学习云下数据中心网段路由，并自动宣告给云上VPN网关。如果云上VPN网关开启了BGP路由自动传播功能，则云上VPN网关会将学习到的BGP路由自动传播到VPC的系统路由表中，而不会传播到VPC的自定义路由表中。

- 云上到云下方向

  云上VPN网关通过BGP路由协议自动学习VPC系统路由表中的路由，并自动宣告给云下数据中心侧VPN网关，而不会学习VPC自定义路由表中的路由。

路由优先级原则

如果VPN网关路由表或VPC路由表中存在路由冲突，各路由的优先级如下表所示。

> **说明** 路由优先级从高到底依次为：P0>P1>P2>P3。

路由类别	VPN网关内路由优先级	VPC内路由优先级
明细路由	P0	P0
系统路由	P1	P1
静态路由	P2	P2
动态路由	P3	P3

使用限制

单个VPN网关的BGP路由表支持的路由条目数为50条。如需提升配额，请提交工单。

使用教程

具体操作，请参见建立VPC到本地数据中心的连接（BGP动态路由）。

2.基于策略的IPsec-VPN变更为基于路由的IPsec-VPN

为了提供更灵活的流量路由方式，VPN网关由基于策略的IPsec-VPN变更为基于路由的IPsec-VPN。本次变更对SSL-VPN无影响。

VPN网关变更详情

基于路由的IPsec-VPN对当前VPN网关的产品形态有如下变化：

VPN网关详情页中存在两种路由表。

- 策略路由：基于源IP和目的IP进行更精确的路由转发。
- 目的路由：仅基于目的IP进行路由转发。

> **说明** 目前，VPN网关详情页中仅支持配置策略路由和目的路由，后续会支持配置动态路由。

变更存量VPN网关

存量VPN网关不支持基于路由的IPsec-VPN功能。如有需要，请提交工单。

您新建的VPN网关，默认支持基于路由的IPsec-VPN功能。您可以在VPN网关详情页中查看如下路由表：