ALIBABA CLOUD

阿里云

VPN网关

IPsec-VPN入门

文档版本：20201102

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.教程概览

本教程为您介绍如何通过IPsec-VPN，建立VPC到本地数据中心的VPN连接。

前提条件

使用IPsec-VPN功能建立VPC到本地数据中心的VPN连接，确保满足以下条件：

- 本地数据中心的网关设备必须支持IKEv1和IKEv2协议。

  IPsec-VPN支持IKEv1和IKEv2协议。只要支持这两种协议的设备都可以和阿里云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。
- 本地数据中心的网关必须配置静态公网IP。
- 本地数据中心的网段和专有网络的网段不能重叠。

配置流程说明

建立VPC到本地数据中心的VPN连接的流程图如下：

1. 创建VPN网关

   VPN网关开启IPsec-VPN功能，一个VPN网关最多可以建立10个IPsec连接。
2. 创建用户网关

   通过创建用户网关，您可以将本地网关的信息注册到云上，然后将用户网关和VPN网关连接起来。一个用户网关可以连接多个VPN网关。
3. 创建IPsec连接

   IPsec连接是指VPN网关和用户网关建立连接后的VPN通道。只有IPsec连接建立后，用户侧企业数据中心才能使用VPN网关进行加密通信。
4. 配置本地网关

   您需要在本地VPN网关设备中加载阿里云VPN网关的配置。详细信息，请参见本地CPE配置。
5. 配置VPN网关路由

   您需要在VPN网关中配置路由，并发布到VPC路由表中。详细信息，请参见网关路由概述。
6. 测试访问

   登录到阿里云VPC内一台无公网IP的ECS实例，通过ping本地数据中心内一台服务器的私网IP地址，验证通信是否正常。

详细配置信息，请参见建立VPC到本地数据中心的连接。

2.建立VPC到本地数据中心的连接

本文介绍如何使用IPsec-VPN建立专有网络（VPC）到本地数据中心的VPN连接，从而实现本地数据中心与VPC的互通。

前提条件

开始前，请确保满足以下条件：

- 您已经注册了阿里云账号。如未注册，请先完成账号注册。
- 检查本地数据中心的网关设备。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等厂商的设备。
- 本地数据中心的网关已经配置了静态公网IP。
- 本地数据中心的网段和VPC的网段不能重叠。

背景信息

某公司在阿里云创建了VPC，网段为192.168.0.0/16。本地数据中心的网段为172.16.0.0/12，本地VPN设备的公网IP为211.xx.xx.68。因公司业务发展，需要本地数据中心与云上VPC互通。

如上图，您可以通过IPsec-VPN，建立本地数据中心与云上VPC的连接，实现云上和云下的互通。

步骤一：创建VPN网关

完成以下操作，创建VPN网关。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，单击**VPN > VPN网关**。
3. 在**VPN网关**页面，单击**创建VPN网关**。
4. 在购买页面，根据以下信息配置VPN网关，然后单击**立即购买**并完成支付。
   - **实例名称**：输入VPN网关的实例名称。
   - **地域和可用区**：选择VPN网关的地域和可用区。

     > **说明** 确保VPC的地域和VPN网关的地域相同。

   - **VPC**：选择要连接的VPC。
   - **带宽规格**：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
   - **IPsec-VPN**：选择开启IPsec-VPN功能。
   - **SSL-VPN**：选择是否开启SSL-VPN功能。SSL-VPN功能允许您从任何位置的单台计算机连接到专有网络。
   - **SSL连接数**： 选择您需要同时连接的客户端最大规格。

     > **说明** 本选项只有在选择开启了SSL-VPN功能后才可配置。

   - **计费周期**：选择购买时长。
5. 返回VPN网关页面，查看创建的VPN网关。刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态表明VPN网关完成了初始化，可以正常使用了。

> **说明** VPN网关的创建一般需要1~5分钟。

步骤二：创建用户网关

完成以下操作，创建用户网关。

1. 在左侧导航栏，单击**VPN > 用户网关**。
2. 选择用户网关的地域。
3. 在**用户网关**页面，单击**创建用户网关**。
4. 在**创建用户网关**对话框，根据以下信息配置用户网关，然后单击**确定**。
   - **名称**：输入用户网关的名称。
   - **IP地址**：输入VPC要连接的本地数据中心网关设备的公网IP。本示例输入**211.xx.xx.68**。
   - **描述**：输入用户网关的描述信息。

步骤三：创建IPsec连接

完成以下操作，创建IPsec连接。

1. 在左侧导航栏，单击**VPN > IPsec连接**。
2. 选择创建IPsec连接的地域。
3. 在**IPsec连接**页面，单击**创建IPsec连接**。
4. 在**创建IPsec连接**页面，根据以下信息配置IPsec连接，然后单击**确定**。
   - **名称**：输入IPsec连接的名称。
   - **VPN网关**：选择已创建的VPN网关。
   - **用户网关**：选择要连接的用户网关。
   - **本端网段**：输入已选VPN网关所属VPC的网段。本示例输入**192.168.0.0/16**。
   - **对端网段**：输入本地数据中心的网段。本示例输入**172.16.0.0/12**。
   - **立即生效**：选择是否立即生效。
     - **是**：配置完成后立即进行协商。
     - **否**：当有流量进入时进行协商。
   - **预共享密钥**：输入共享密钥，该值必须与本地网关设备的预共享密钥一致。

     其他选项使用默认配置。

步骤四：在本地网关设备中加载VPN配置

完成以下操作，在本地网关设备中加载VPN配置。

1. 在左侧导航栏，单击**VPN > IPsec连接**。
2. 选择IPsec连接的地域。
3. 在**IPsec连接**页面，找到目标IPsec连接，然后单击**操作**列下的**更多操作 > 下载对端配置**。
4. 根据本地网关设备的配置要求，将下载的配置添加到本地网关设备中。详细信息，请参见本地网关配置。下载配置中的RemotSubnet和LocalSubnet与创建IPsec连接时的本端网段和对端网段是相反的。因为从阿里云VPN网关的角度看，对端是用户IDC的网段，本端是VPC网段；而从本地网关设备的角度看，LocalSubnet就是指本地IDC的网段，RemotSubnet则是指阿里云VPC的网段。

步骤五：配置VPN网关路由

完成以下操作，配置VPN网关路由。

1. 在左侧导航栏，单击**VPN > VPN网关**。
2. 选择VPN网关的地域。
3. 在**VPN网关**页面，找到目标VPN网关，单击**实例ID/名称**列下的实例ID。
4. 在**目的路由表**页签，单击**添加路由条目**。
5. 在**添加路由条目**对话框，根据以下信息配置目的路由，然后单击**确定**。
   - **目标网段**：输入本地IDC侧的私网网段。本示例输入**172.16.0.0/12**。
   - **下一跳类型**：选择IPsec连接。
   - **下一跳**：选择IPsec连接实例。
   - **发布到VPC**：选择是否将新添加的路由发布到VPC路由表。本示例选择**是**。
   - **权重**：选择权重值。本示例选择**100**。

步骤六：测试访问

登录到阿里云VPC内一台无公网IP的ECS实例，并通过ping命令ping本地数据中心内一台服务器的私网IP地址，验证通信是否正常。

3.建立VPC到本地数据中心的连接（BGP动态路由）

本文介绍如何使用IPsec-VPN建立专有网络（VPC）到本地数据中心的VPN连接，并通过BGP动态路由协议自动学习路由实现VPC与本地数据中心间的资源互通，降低网络维护成本和网络配置风险。

前提条件

开始前，请确保满足以下条件：

- 您已经注册了阿里云账号。如还未注册，请先完成账号注册。详细信息，请参见账号注册。
- 您已经创建了需要与本地数据中心互通的VPC，且VPC的网段与本地数据中心的网段不重叠。详细信息，请参见创建专有网络。

背景信息

本教程以下图场景为例。某公司在德国（法兰克福）地域创建了一个VPC，私网网段为10.0.0.0/8，自治系统号（ASN）为10001。该公司在法兰克福拥有本地数据中心，公网IP为2.2.2.2，私网网段为172.17.0.0/16，ASN为10002。因业务发展，需要云上VPC与本地数据中心互通。

您可以通过IPsec-VPN建立VPC到本地数据中心的VPN连接，并配置BGP动态路由。配置成功后，VPC和本地数据中心通过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** 在互联网中，一个自治系统（AS）是一个有权自主决定在本系统中应采用何种路由协议的小型单位。这个网络单位可以是一个简单的网络也可以是一个或多个普通的网络管理员来控制的网络群体，它是一个单独的可管理的网络单元。一个自治系统将会分配一个全局的唯一的号码，这个号码叫做自治系统号（ASN）。

配置步骤

步骤一：创建VPN网关

VPN网关是一款基于Internet的网络连接服务，通过加密通道的方式实现网络互通。使用VPN网关建立VPC到本地数据中心的VPN连接前，您需要为要与本地数据中心互通的VPC创建VPN网关。

完成以下操作，为VPC创建VPN网关。

1. 登录VPN网关管理控制台。
2. 在**VPN网关**页面，单击**创建VPN网关**。
3. 在购买页面，根据以下信息为VPC创建VPN网关。
   - **实例名称**：输入VPN网关的实例名称。本示例输入**VPN**。
   - **地域和可用区**：选择VPN网关的地域。

     确保VPC的地域和VPN网关的地域相同。本示例选择**德国（法兰克福）**。
   - **VPC**：选择要连接的VPC。本示例选择德国（法兰克福）地域创建的VPC。
   - **指定交换机**：选择是否为VPN网关指定所属的交换机。本示例选择**否**。
   - **虚拟交换机**：选择VPN网关所属的交换机。

> **说明** 仅**指定交换机**选择**是**时，才会显示该选项。

- **带宽规格**：选择带宽规格。

  带宽规格是VPN网关所具备的公网带宽。本示例选择**5Mbps**。

- **IPsec-VPN**：选择开启或关闭IPsec-VPN功能。

  IPsec-VPN功能可以实现本地数据中心与VPC或不同VPC之间进行连接。本示例选择**开启**。

- **SSL-VPN**：选择开启或关闭SSL-VPN功能。

  SSL-VPN功能可以实现任何位置的单台计算机连接到VPC。本示例选择**关闭**。

- **SSL连接数**：选择您需要同时连接的客户端最大规格。

  > **说明** 本选项只有在选择开启了SSL-VPN功能后才可配置。

- **计费周期**：选择购买时长。

4. 单击**立即购买**并完成支付。

VPN网关的创建一般需要1~5分钟。刚创建好的VPN网关的状态是准备中，约两分钟左右会变更为正常。正常状态表明VPN网关已经完成了初始化，可以正常使用。VPN网关创建后，系统会为VPN网关自动分配一个公网IP用于建立VPN连接。

步骤二：开启BGP

BGP用于在不同的自治系统（AS）之间交换路由信息。使用BGP动态路由功能前，您需要为VPN网关开启BGP功能。

> **说明** VPN网关开启BGP功能后，不支持关闭。

完成以下操作，为VPN网关开启BGP功能。

1. 在左侧导航栏，单击**VPN > VPN网关**。
2. 在**VPN网关**页面，找到步骤一创建的VPN网关，单击**操作**列下的**开启BGP**。
3. 在**开启BGP**对话框，选择BGP路由是否传播到VPC。
   - **是**：VPN网关会将BGP路由自动传播到VPC。
   - **否**：VPN网关不会将BGP路由传播到VPC。如需传播，您需要手动将BGP路由发布到VPC。

     本示例选择**是**。
4. 单击**确定**。

为VPN网关开启BGP功能后，VPN网关的BGP状态变更为**已开启BGP**。

步骤三：创建用户网关

您可以通过创建用户网关，将本地数据中心的网络信息注册到云上，然后将用户网关和VPN网关连接起来。

完成以下操作，创建用户网关。

1. 在左侧导航栏，单击**VPN > 用户网关**。
2. 在**用户网关**页面，单击**创建用户网关**。
3. 在**创建用户网关**对话框，根据以下信息配置用户网关。
   - **名称**：输入用户网关的名称。本示例输入**CGW**。
   - **IP地址**：输入本地数据中心网关设备的公网IP。本示例输入**2.2.2.2**。
   - **自治系统号**：输入本地数据中心网络的自治系统号。本示例输入**10002**。
   - **描述**：输入用户网关的描述信息。
4. 单击**确定**。

步骤四：创建IPsec连接

IPsec-VPN基于路由，不仅可以更方便的配置和维护VPN策略，而且还提供了灵活的流量路由方式。

完成以下操作，创建VPC到本地数据中心间的IPsec连接。

1. 在左侧导航栏，单击**VPN > IPsec连接**。
2. 在**IPsec连接**页面，单击**创建IPsec连接**。
3. 在**创建IPsec连接**对话框，根据以下信息创建VPC到本地数据中心间的IPsec连接。
   - **名称**：输入IPsec连接的名称。本示例输入**VPC TO IDC**。
   - **VPN网关**：选择要连接的VPN网关。

     本示例选择步骤一中创建的VPN网关。详细信息，请参见步骤一：创建VPN网关。
   - **用户网关**：选择要连接的用户网关。

     本示例选择步骤三中创建的用户网关。详细信息，请参见步骤三：创建用户网关。
   - **本端网段**：输入VPC的网段。本示例输入**10.0.0.0/8**。
   - **对端网段**：输入本地数据中心的网段。本示例输入**172.17.0.0/16**。
   - **立即生效**：选择是否立即生效。
     - 是：配置完成后立即进行协商。
     - 否：当有流量进入时进行协商。

     本示例选择**是**。
   - **预共享密钥**：输入预共享密钥。

     请确保要建立的IPsec连接的预共享密钥一致。本示例输入**123456**。
   - **版本**：选择ike的版本。本示例选择**ikev2**。
   - **加密算法**：选择加密算法。本示例选择**aes**。
   - **认证算法**：选择认证算法。本示例选择**sha1**。
   - **DH分组**：选择DH分组。本示例选择**group2**。
   - **隧道网段**：输入IPsec隧道的网段，该网段在169.254.0.0/16内的掩码长度为30的网段。本示例输入**169.254.10.0/30**。
   - **本端BGP地址**：输入本端BGP地址，该地址为隧道网段内的一个IP地址。本示例输入**169.254.10.1**

     > **说明** 请确保IPsec隧道两端的BGP地址不冲突。

- **本端自治系统号**：输入VPC侧的自治系统号。本示例输入**10001**。

其他选项使用默认配置。

4. 单击**确定**。

步骤五：在本地网关设备中加载VPN配置

云上创建IPsec连接后，您还需要在本地网关设备中加载VPN配置，才能建立VPC到本地数据中心的VPN连接。

本示例以思科IOSXE系统为例，介绍如何在本地网关设备中加载VPN配置。

1. 登录思科防火墙设备的命令行配置界面。
2. 执行以下命令，配置ikev2 proposal和policy 。

```
crypto ikev2 proposal alicloud
encryption aes-cbc-128  //配置加密算法，本示例配置为aes-cbc-128。
integrity sha1  //配置认证算法，本示例配置为sha1。
group 2 //配置DH分组，本示例配置为group2。
exit
!
crypto ikev2 policy Pureport_Pol_ikev2
proposal Pureport_prop
exit
!
```

3. 执行以下命令，配置ikev2 keyring。

```
crypto ikev2 keyring alicloud
peer alicloud
address 1.1.1.1  //配置VPC侧VPN网关的公网IP地址，本示例配置为1.1.1.1。
pre-shared-key 123456 //配置钥匙串，本示例配置为123456。
exit
!
```

4. 执行以下命令，配置ikev2 profile。

```
crypto ikev2 profile alicloud
match identity remote address 1.1.1.1 255.255.255.255  //匹配VPC侧VPN网关的公网IP，本示例匹配的地址为1.1.1.1。
identity local address 2.2.2.2  //本地数据中心的公网IP，本示例配置为2.2.2.2。
authentication remote pre-share  //认证对端的方式为PSK。
authentication local pre-share  //认证本端的方式为PSK。
keyring local alicloud  //调用密钥串。
exit
!
```

5. 执行以下命令，配置transform。

```
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
mode tunnel
exit
!
```

6. 执行以下命令，配置IPsec Profile，并调用transoform、pfs和ikev2 profile。

```
crypto ipsec profile alicloud
set transform-set TSET
set pfs group2
set ikev2-profile alicloud
exit
!
```

7. 执行以下命令，配置IPsec隧道。

```
interface Tunnel100
ip address 169.254.10.2 255.255.255.252  //配置本端（本地数据中心）隧道地址，本示例配置为169.254.10.2
。
tunnel source GigabitEthernet1
tunnel mode ipsec ipv4
tunnel destination 1.1.1.1  //隧道对端（云上VPN网关）公网IP地址，本示例配置为1.1.1.1。
tunnel protection ipsec profile alicloud
no shutdown
exit
!
interface GigabitEthernet1
ip address 2.2.2.2 255.255.255.0
negotiation auto
!
```

8. 执行以下命令，配置BGP路由协议。

```
router bgp 10002  //开启bgp路由协议，并配置本端（本地数据中心）ASN。本示例配置ASN为10002。
bgp router-id 169.254.10.2  //bgp路由器id，本示例设置为169.254.10.2。
bgp log-neighbor-changes
neighbor 169.254.10.1 remote-as 10001  //配置bgp邻居的ASN。
neighbor 169.254.10.2 ebgp-multihop 10  //配置ebgp跳数为10。
!
address-family ipv4
network 172.17.0.0 mask 255.255.0.0  //宣告本端（本地数据中心）网段，本示例配置为172.17.0.0/16。
neighbor 169.254.10.1 activate  //激活bgp邻居。
exit-address-family
!
```

IPsec连接建立成功后，云上云下VPN网关会进行如下路由宣告：

- 本地数据中心VPN网关通过BGP动态路由协议自动学习本地数据中心网段路由，并自动宣告给云上VPN网关。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。
- 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，并自动宣告给本地数据中心侧VPN网关设备。

步骤六：测试网络连通性

IPsec连接建立成功后，您可以测试VPC与本地数据中心间的网络连通性。

> **说明** 请确保要访问的本地数据中心终端的防火墙规则允许远程连接。

1. 登录VPC下的ECS实例。
2. 通过 ping 命令 ping 本地数据中心的终端的IP地址，验证通信是否正常。 经验证，VPC ECS实例可以访问本地数据中心终端。
3. 登录本地数据中心终端。
4. 通过 ping 命令 ping VPC下的ECS实例的IP地址，验证通信是否正常。 经验证，本地数据中心终端可以访问VPC ECS实例。