虚拟专用网络

快速入门

文档版本 01

发布日期 2023-08-18

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 准备工作

在使用虚拟专用网络之前，您需要完成本文中的准备工作。

注册华为帐号并开通华为云

如果您已有一个华为帐号并已开通华为云，请跳到下一个任务。如果您还没有华为帐号，请参见以下步骤创建。

1. 进入**华为云**官网，单击页面右上角的“注册”。
2. 根据提示信息完成注册，详细操作请参见**注册华为帐号并开通华为云**。
   注册成功后，系统会自动跳转至您的个人信息界面。
3. 参见**实名认证**完成个人或企业帐号实名认证。

为账户充值

您需要确保账户有足够金额。

- 关于虚拟专用网络的价格，请参见**价格详情**。

创建用户并授权使用 VPN

您需要确保用户享有使用VPN服务的“VPN Administrator”权限。

- 关于VPN服务支持的系统权限，请参见**权限管理**。
- 如何创建用户并授权使用VPN，请参见**创建用户并授权使用VPN**。

2 通过企业版 VPN 实现数据中心和 VPC 互通

2.1 入门指引

功能支持区域

华东-青岛、亚太-曼谷、中国-香港、亚太-新加坡、亚太-雅加达、土耳其-伊斯坦布尔、拉美-墨西哥城一、拉美-墨西哥城二

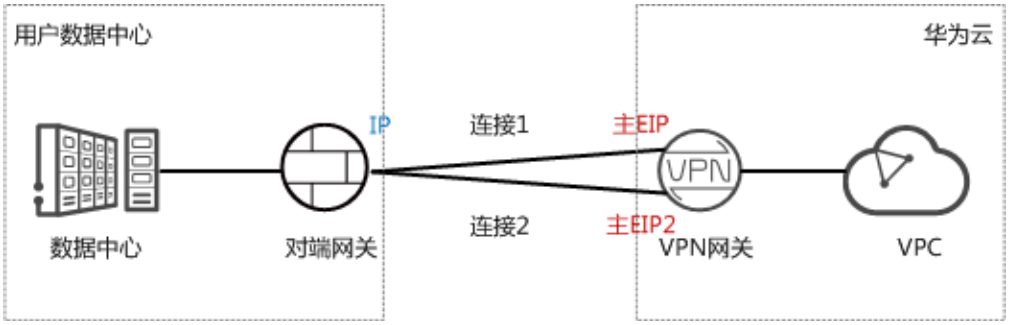
场景描述

由于业务发展，企业A需要将数据中心和VPC的数据进行互通。此时企业A可以通过VPN服务创建数据中心和VPC的连接，实现云上和云下数据互通。

- 如果用户数据中心仅有一个对端网关，且对端网关只能配置一个IP地址，推荐VPN网关使用双活模式，组网如图2-1所示。

  双活模式下，如果连接1链路故障，流量自动切换至连接2进行传输，企业业务不受影响；连接1恢复正常后，VPN仍使用连接2进行数据交互。

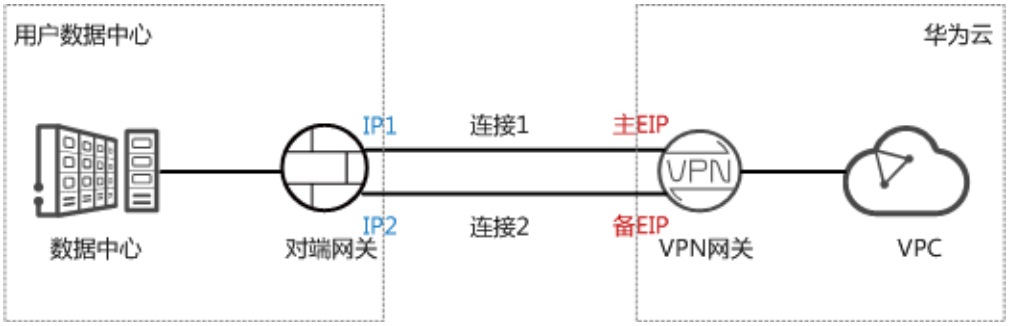
  图 2-1 双活模式

- 如果用户数据中心存在两个对端网关，或一个对端网关可以配置两个IP地址，推荐VPN网关使用主备模式，组网如图2-2所示。

  主备模式下，连接1和连接2互为主备，主链路为连接1，备链路为连接2。默认情况下流量仅通过主链路进行传输，如果主链路故障，流量自动切换至备链路进行传输，企业业务不受影响；主链路恢复正常后，VPN回切至主链路进行数据交互。

图 2-2 主备模式



约束与限制

- 对端网关需要支持标准IKE和IPsec协议。
- 本地数据中心和VPC间互通的子网需要没有重叠，且数据中心待互通的子网中不能包含100.64.0.0/10和214.0.0.0/8。

  如果VPC使用DC/CC服务和其他VPC互通，则本地数据中心的子网也不能和其他VPC包含的子网存在重叠。

数据规划

表 2-1 规划数据

类别	规划项	规划值
VPC	待互通子网	192.168.0.0/16
VPN网关	互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。 192.168.2.0/24
	HA模式	双活
	EIP地址	EIP地址在购买EIP时由系统自动生成，VPN网关默认使用2个EIP。本示例假设EIP地址生成如下： ● 主EIP：11.xx.xx.11 ● 主EIP2：11.xx.xx.12
VPN连接	Tunnel接口地址	用于VPN网关和对端网关建立IPsec隧道，配置时两边需要互为镜像。 ● VPN连接1：169.254.70.1/30 ● VPN连接2：169.254.71.1/30
数据中心	待互通子网	172.16.0.0/16
对端网关	网关IP地址	网关IP地址由运营商统一分配。本示例假设网关IP地址如下： 22.xx.xx.22

类别	规划项	规划值
	Tunnel接口地址	• VPN连接1：169.254.70.2/30 • VPN连接2：169.254.71.2/30

操作流程

通过VPN实现数据中心和VPC互通的操作流程如图2-3所示。

图 2-3 操作流程

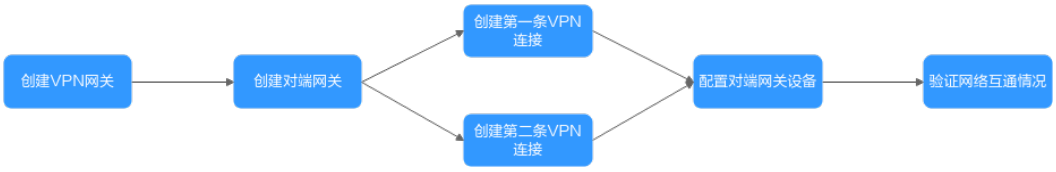


表 2-2 操作流程说明

序号	步骤	说明
1	**步骤一：创建VPN网关**	VPN网关需要绑定两个EIP作为出口公网IP。 如果您已经购买EIP，则此处可以直接绑定使用。
2	**步骤二：创建对端网关**	添加数据中心的VPN设备为对端网关。
3	**步骤三：创建第一条VPN连接**	VPN网关的主EIP和对端网关组建第一条VPN连接。
4	**步骤四：创建第二条VPN连接**	VPN网关的主EIP2和对端网关组建第二条VPN连接。 第二条VPN连接的路由模式、预共享密钥、IKE/IPsec策略建议和第一条VPN连接配置保持一致。
5	**步骤五：配置对端网关设备**	• 对端网关配置的本端隧道接口地址/对端隧道接口地址需要和华为云VPN连接配置互为镜像配置。 • 对端网关配置的路由模式、预共享密钥、IKE/IPsec策略需要和华为云VPN连接配置保持一致。
6	**步骤六：验证网络互通情况**	登录ECS，执行**ping**命令，验证网络互通情况。

2.2 步骤一：创建 VPN 网关

前提条件

- 虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。

- 虚拟私有云VPC中ECS的安全组规则已经配置，并确保安全组规则允许数据中心的对端网关可以访问VPC资源。如何配置安全组规则，请参见**安全组规则**。

操作步骤

步骤1 登录管理控制台。

步骤2 在系统首页，选择“网络 > 虚拟专用网络”。

步骤3 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN网关”。

步骤4 在“VPN网关”界面，单击“创建VPN网关”。

步骤5 根据界面提示配置参数，然后单击“立即购买”并完成支付。

本示例仅对关键参数进行说明，更全参数请参见**创建VPN网关**。

表 2-3 VPN 网关关键参数说明

参数	说明	参数取值
计费模式	支持“包年/包月”和“按需计费”两种模式。	包年/包月
区域	选择靠近您所在地域的区域。	亚太-新加坡
名称	输入VPN网关的名称。	vpngw-001
网络类型	• 公网：VPN网关通过Internet网络和用户数据中心的对端网关进行通信。 • 私网：VPN网关通过私有网络和用户数据中心的对端网关进行通信。	公网
关联模式	支持“虚拟私有云”和“企业路由器”两种方式。	虚拟私有云
虚拟私有云	选择需要和数据中心互通的VPC。	vpc-001(192.168.0.0/16)
互联子网	用于VPN网关和VPC通信，请确保选择的互联子网存在4个及以上可分配的IP地址。	192.168.2.0/24
本端子网	配置VPC待和数据中心互通的子网。 支持“输入网段”和“选择子网”两种方式。	192.168.0.0/24
规格	选择“专业型1”并去勾选“非固定IP接入”。	专业型1
HA模式	选择“双活”。	双活
主EIP	支持“现在创建”和“使用已有”两种方式。	11.xx.xx.11
主EIP2		11.xx.xx.12

----结束

结果验证

在“VPN网关”页面生成新创建的VPN网关信息，初始状态为“创建中”；当VPN网关状态变为“正常”，表示VPN网关创建完成。

2.3 步骤二：创建对端网关

操作步骤

步骤1 在左侧导航栏，单击“虚拟专用网络 > 企业版-对端网关”。

步骤2 在“对端网关”界面，单击“创建对端网关”。

步骤3 根据界面提示配置参数，然后单击“确定”。

本示例仅对关键参数进行说明，更全参数请参见**创建对端网关**。

表 2-4 对端网关参数说明

参数	说明	参数取值
名称	输入对端网关的名称。	cgw-001
标识	输入对端网关的IP。	IP Address，22.xx.xx.22。

----结束

结果验证

在“对端网关”页面生成新创建的对端网关信息。

2.4 步骤三：创建第一条 VPN 连接

操作步骤

步骤1 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN连接”。

步骤2 在“VPN连接”页面，单击“创建VPN连接”。

步骤3 根据界面提示配置第一条VPN连接参数，然后单击“提交”。

本示例仅对关键参数进行说明，详细参数说明请参见**创建VPN连接**。

表 2-5 第一条 VPN 连接参数说明

参数	说明	参数取值
名称	输入VPN连接的名称。	vpn-001
VPN网关	选择**步骤一：创建VPN网关**创建的VPN网关。	vpngw-001

参数	说明	参数取值
网关IP	选择VPN网关的**主EIP**。	11.xx.xx.11
对端网关	选择**步骤二：创建对端网关**创建的对端网关。	cgw-001
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	输入数据中心待和VPC互通的子网。	172.16.0.0/16
接口分配方式	支持“手动分配”和“自动分配”两种方式。	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。 **说明** 对端网关需要对此处的本端隧道接口地址/对端隧道接口地址做镜像配置。	169.254.70.2/30
对端隧道接口地址	配置在用户侧设备上的tunnel接口地址。	169.254.70.1/30
检测机制	用于多链路场景下路由可靠性检测。 **说明** 功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则会导致VPN流量不通。	勾选“使能NQA”
预共享密钥、确认密钥	VPN连接协商密钥。 VPN连接和对端网关配置的预共享密钥需要一致。	Test@123
策略配置	包含IKE策略和IPsec策略，用于指定VPN隧道加密算法。 VPN连接和对端网关配置的策略信息需要一致。	默认配置

----结束

结果验证

在“VPN连接”页面生成新创建的VPN连接信息，初始状态为“创建中”；由于此时对端网关尚未配置，无法建立有效的连接，所以大约2分钟后，VPN连接状态会变成“未连接”。

2.5 步骤四：创建第二条 VPN 连接

操作步骤

步骤1 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN连接”。

步骤2 在“VPN连接”页面，单击“创建VPN连接”。

和第一条VPN连接相比，除了名称、网关IP、本端隧道接口地址和对端隧道接口地址不同，其他配置建议保持一致。

表 2-6 第二条 VPN 连接参数说明

参数	说明	参数取值
名称	输入VPN连接的名称。	vpn-002
VPN网关	选择**步骤一：创建VPN网关**创建的VPN网关。	vpngw-001
网关IP	选择VPN网关的**主EIP2**。	11.xx.xx.12
对端网关	选择**步骤二：创建对端网关**创建的对端网关。	cgw-001
连接模式	选择“静态路由模式”。	静态路由模式
对端子网	输入数据中心待和VPC互通的子网。	172.16.0.0/16
接口分配方式	支持“手动分配”和“自动分配”两种方式。	手动分配
本端隧道接口地址	配置在VPN网关上的tunnel接口地址。 **说明** 对端网关需要对此处的本端隧道接口地址/对端隧道接口地址做镜像配置。	169.254.71.2/30
对端隧道接口地址	配置在用户侧设备上的tunnel接口地址。	169.254.71.1/30
检测机制	用于多链路场景下路由可靠性检测。 **说明** 功能开启前，请确认对端网关支持ICMP功能，且对端接口地址已在对端网关上正确配置，否则会导致VPN流量不通。	勾选“使能NQA”
预共享密钥、确认密钥	VPN连接协商密钥。 VPN连接和对端网关配置的预共享密钥需要一致。	Test@123
策略配置	包含IKE策略和IPsec策略，用于指定VPN隧道加密算法。 VPN连接和对端网关配置的策略信息需要一致。	默认配置

----结束

结果验证

在“VPN连接”页面生成新创建的VPN连接信息，初始状态为“创建中”；由于此时对端网关尚未配置，无法建立有效的连接，所以大约2分钟后，VPN连接状态会变成“未连接”。

2.6 步骤五：配置对端网关设备

操作步骤

> **说明**
>
> 本示例对端网关以华为AR路由器为例。更多对端网关配置示例，请参见**管理员指南**。

步骤1 登录AR路由器配置界面。

步骤2 进入系统视图。

```
<AR651>system-view
```

步骤3 配置公网接口的IP地址。本示例假设AR路由器GigabitEthernet 0/0/8为公网接口。

```
[AR651]interface GigabitEthernet 0/0/8
[AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0
[AR651-GigabitEthernet0/0/8]quit
```

步骤4 配置默认路由。

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 22.xx.xx.1
```

其中，*22.xx.xx.1*为AR路由器公网IP的网关地址，请根据实际替换。

步骤5 开启SHA-2算法兼容RFC标准算法功能。

```
[AR651]IPsec authentication sha2 compatible enable
```

步骤6 配置IPsec安全提议。

```
[AR651]IPsec proposal hwproposal1
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

步骤7 配置IKE安全提议。

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh group14
[AR651-ike-proposal-2]authentication-algorithm sha2-256
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

步骤8 配置IKE对等体。

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer2]rsa signature-padding pss
```



```
[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer2]quit
```

相关命令说明如下：

- pre-shared-key cipher：预共享密钥，需要和VPN连接配置的预共享密钥保持一致。
- local-address：AR路由器的公网地址。
- remote-address：VPN网关的主EIP/主EIP2。

步骤9 配置IPsec安全框架。

```
[AR651]IPsec profile hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
[AR651-IPsec-profile-hwpro1]proposal hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-group14
[AR651-IPsec-profile-hwpro1]quit
[AR651]IPsec profile hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]proposal hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-group14
[AR651-IPsec-profile-hwpro2]quit
```

步骤10 配置虚拟隧道接口。

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

相关命令说明如下：

- interface Tunnel0/0/1、interface Tunnel0/0/2：两条VPN连接对应的Tunnel隧道。

  本示例中，Tunnel0/0/1对应VPN网关主EIP所在的VPN连接；Tunnel0/0/2对应VPN网关主EIP2所在的VPN连接。
- ip address：AR路由器的Tunnel接口地址。
- source：AR路由器的公网地址。
- destination：VPN网关的主EIP/主EIP2。

步骤11 配置NQA。

```
[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
```



```
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

相关命令说明如下：

- nqa test-instance IPsec_nqa1 IPsec_nqa1、nqa test-instance IPsec_nqa2 IPsec_nqa2：NQA名称。

  本示例中，IPsec_nqa1对应VPN网关主EIP所在的VPN连接；IPsec_nqa2对应VPN网关主EIP2所在的VPN连接。
- destination-address：VPN网关的Tunnel接口地址。
- source-address：AR路由器的Tunnel接口地址。

步骤12 配置静态路由联动NQA功能。

```
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nqa IPsec_nqa2 IPsec_nqa2
```

相关参数说明如下：

- 192.168.0.0：VPC的本端子网。
- 同一条命令中，Tunnel*x*和IPsec_nqa*x*需要同属于一条VPN连接。

----结束

结果验证

步骤1 登录管理控制台。

步骤2 在系统首页，选择“网络 > 虚拟专用网络”。

步骤3 在左侧导航栏，单击“虚拟专用网络 > 企业版-VPN连接”。

此时可以看到两条VPN连接状态均变为“正常”。

----结束

2.7 步骤六：验证网络互通情况

操作步骤

步骤1 登录管理控制台。

步骤2 在管理控制台左上角单击 图标，选择区域和项目。

步骤3 单击“服务列表”，选择“计算 > 弹性云服务器”。

步骤4 登录弹性云服务器。

弹性云服务器有多种登录方法，具体请参见**登录弹性云服务器**。

本示例是通过管理控制台远程登录（VNC方式）。

步骤5 在弹性云服务器的远程登录窗口，执行以下命令，验证网络互通情况。

ping 172.16.0.100

其中，172.16.0.100为数据中心服务器的IP地址，请根据实际替换。

回显如下信息，表示网络已通。

```
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=28ms TTL=245
来自 xx.xx.xx.xx 的回复: 字节=32 时间=27ms TTL=245
```

----结束

3 经典版 VPN 购买流程

3.1 入门指引

不同区域的经典版VPN操作流程有所区别，详细请参见**表3-1**。

表 3-1 入门指引

上线区域	华北-北京四、华东-上海一、华南-广州、西南-贵阳一、中国-香港、亚太-曼谷、亚太-新加坡、非洲-约翰内斯堡、拉美-圣地亚哥	拉美-墨西哥城一、拉美-圣保罗一
页面操作	创建步骤及顺序如下： 1. **创建VPN网关** 2. **创建VPN连接** 3. **配置对端设备**	创建步骤及顺序如下： 1. **申请创建购买VPN（墨西哥城一/圣保罗一）** 2. **配置对端设备**

3.2 购买 VPN（墨西哥城一/圣保罗一）

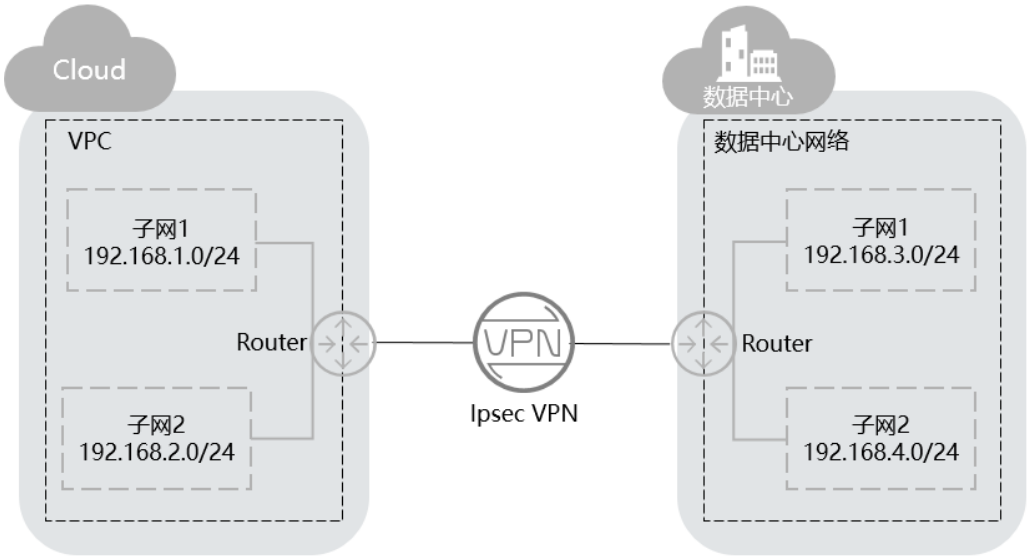
简介

默认情况下，在Virtual Private Cloud (VPC) 中的弹性云服务器无法与您自己的数据中心或私有网络进行通信。如果您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，可以启用虚拟专用网络功能。此操作您需要在VPC中创建VPN并更新安全组规则。

简单的 IPsec VPN 内网对连拓扑说明

如**图3-1**所示，假设您在云中已经申请了VPC，并申请了2个子网（192.168.1.0/24，192.168.2.0/24），您在自己的数据中心Router下也有2个子网（192.168.3.0/24，192.168.4.0/24）。您可以通过VPN使VPC内的子网与数据中心的子网互相通信。

图 3-1 IPsec VPN



华为云支持点到点VPN（Site-to-Site VPN），可实现VPC子网和用户数据中心局域网互访。在建立IPsec VPN前，请确认拟开通VPN的用户数据中心满足以下3个条件：

1. 用户数据中心有支持标准IPsec协议的设备。
2. 上述设备可以分配独立的公网IP（NAT IP也支持）。
3. VPC子网和用户数据中心子网不冲突，用户数据中心子网到上述设备可达。

满足以上条件后，配置IPsec VPN时，需要保证两端IKE策略以及IPsec策略配置一致，两端子网互为镜像。

配置完成后，需要通过私网数据流触发VPN协商。

操作场景

通过执行该任务，您可以创建VPN，以便在您的数据中心与云服务之间建立一条保密而安全的通信隧道。

前置条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在“虚拟专用网络”界面，单击“购买VPN”。
5. 根据界面提示配置参数，并单击“立即购买”。
   参数说明如**表3-2**、**表3-3**、**表3-4**所示。

表 3-2 基本参数

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	亚太-新加坡
计费模式	VPN支持按需计费。	按需计费
名称	VPN名称。	VPN-001
VPC	VPC的名称。	VPC-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段重合。	192.168.3.0/24， 192.168.4.0/24
预共享密钥	配置在云上VPN连接的密钥，需要与本地网络VPN设备配置的密钥一致。此密钥用于VPN连接协商。 取值范围：6~128位。	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	• 默认配置 • 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见**表3-3**和**表3-4**。	自定义配置

表 3-3 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● MD5（此算法安全性较低，请慎用） ● SHA1（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
DH算法	Diffie-Hellman密钥交换算法，支持的算法： ● Group 5（此算法安全性较低，请慎用） ● Group 2（此算法安全性较低，请慎用） ● Group 14 默认配置为：Group 14。	Group 14
版本	IKE密钥交换协议版本，支持的版本： ● v1（有安全风险不推荐） ● v2 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400

参数	说明	取值样例
协商模式	选择IKE策略版本为“v1”时，可以配置协商模式，取值支持Main、Aggressive。 默认配置为：Main	Main

表 3-4 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用） ● MD5（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法： ● DH group 2（此算法安全性较低，请慎用） ● DH group 5（此算法安全性较低，请慎用） ● DH group 14 默认配置为：DH group 14。	DH group 14
传输协议	IPsec传输和封装用户数据时使用的安全协议，目前支持的协议： ● AH ● AH-ESP 默认配置为：ESP。	ESP

参数	说明	取值样例
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

说明

IKE策略指定了IPsec 隧道在协商阶段的加密和认证算法，IPsec策略指定了IPsec在数据传输阶段所使用的协议，加密以及认证算法；这些参数在VPC上的VPN和您数据中心的VPN中需要进行相同的配置，否则会导致VPN无法建立连接。

以下算法安全性较低，请慎用：

- **认证算法：**SHA1、MD5。
- **加密算法：**3DES。
- **DH算法：**Group 1、Group 2、Group 5。

6. 提交申请。

   创建成功后云为该IPsec VPN分配一个公网出口IP地址。该地址为VPN页面中，已创建的VPN的本端网关地址。在您自己数据中心配置对端隧道时，远端网关需要配置为该IP地址。

7. 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行IPsec VPN隧道配置。

3.3 创建 VPN 网关

操作场景

您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，需要先创建VPN网关。按需计费购买VPN网关时，可以同时购买一条与其关联的VPN连接。

前置条件

- 请确认虚拟私有云VPC已经创建完成。如何创建虚拟私有云VPC，请参见**创建虚拟私有云和子网**。
- 请确认虚拟私有云VPC的安全组规则已经配置，ECS通信正常。如何配置安全组规则，请参见**安全组规则**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版-VPN网关”。

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。

5. 在“VPN网关”界面，单击“创建VPN网关”。
6. 根据界面提示配置参数，并单击“立即购买”。VPN网关参数请参见表3-5

表 3-5 VPN 网关参数说明

参数	说明	取值样例
计费模式	VPN网关支持按需计费计费模式。 按需计费：购买VPN网关时，可以同时购买一条与其相关联的VPN连接。	按需计费
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	亚太-新加坡
名称	VPN网关名称。	vpngw-001
虚拟私有云	VPN接入的VPC名称。	vpc-001
类型	VPN类型。默认为选择“IPsec”。	IPsec
计费方式	按需计费支持两种计费方式：按带宽计费/按流量计费。 • 按带宽计费：指定带宽上限，按使用时间计费，与使用的流量无关。 • 按流量计费：指定带宽上限，按实际使用的上行流量计费，与使用时间无关。	按流量计费
带宽大小	本地VPN网关的带宽大小（单位Mbit/s），为所有基于该网关创建的VPN连接共享的带宽，VPN连接带宽总和不超过VPN网关的带宽。 在VPN使用过程中，当网络流量超过VPN带宽时有可能造成网络拥塞导致VPN连接中断，请用户提前做好带宽规划。 可以在CES监控中配置告警规则对带宽进行监控。	10

说明

当用户创建的VPN网关为按需计费时，默认创建一个VPN连接（深圳Region除外），所以需要同时配置与VPN网关关联的VPN连接参数，详细请参见表3-6。

表 3-6 VPN 连接参数说明

参数	说明	取值样例
名称	VPN连接名称	vpn-001

参数	说明	取值样例
VPN网关	VPN连接挂载的VPN网关名称	vpcgw-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。支持以下方式设置本端子网： ● 选择子网，表示用户数据中心或者私有网络与您选择的子网进行互通。 ● 手动输入网段，表示用户数据中心或者私有网络与您配置的网段之间进行互通。 **说明** 多个本端子网不支持子网网段重叠。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段、专线/云连接的远端子网网段重复。 **说明** 多个远端子网不支持子网网段重叠。	192.168.3.0/24， 192.168.4.0/24
预共享密钥	配置在VPC的VPN和您的数据中心的VPN中，配置需要一致。 取值范围： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 数字 – 大小写字母 – 特殊符号：包括“~”、“`”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“[”、“]”、“{”、“}”、“|”、"\"、","、"."、"/"、“:”和“;”	Test@123
确认密钥	再次输入预共享密钥。	Test@123
高级配置	● 默认配置 ● 自定义配置：自定义配置IKE策略和IPsec策略。相关配置说明请参见**表3-7**和**表3-8**。	自定义配置

表 3-7 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● MD5（此算法安全性较低，请慎用） ● SHA1（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
DH算法	Diffie-Hellman密钥交换算法，支持的算法： ● Group 1（此算法安全性较低，请慎用） ● Group 2（此算法安全性较低，请慎用） ● Group 5（此算法安全性较低，请慎用） ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 默认配置为：Group 14。 协商双方的dh算法必须一致，否则会导致协商失败。	Group 14
版本	IKE密钥交换协议版本，支持的版本： ● v1（有安全风险不推荐） ● v2 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400

表 3-8 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用） ● MD5（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法： ● DH group 1（此算法安全性较低，请慎用） ● DH group 2（此算法安全性较低，请慎用） ● DH group 5（此算法安全性较低，请慎用） ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 默认配置为：DH group 14。	DH group 14
传输协议	IPsec传输和封装用户数据时使用的安全协议，目前支持的协议： ● ESP ● AH ● AH-ESP 默认配置为：ESP。	ESP

参数	说明	取值样例
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

⚠ 注意

以下算法安全性较低，请慎用：

认证算法：SHA1、MD5。

加密算法：3DES。

DH算法：Group 1、Group 2、Group 5。

7. 确认购买的VPN网关信息，单击“提交”。

   VPN网关创建成功后，系统会分配一个公网出口IP，即VPN网关列表中“网关IP”对应显示的IP地址。该网关IP也是用户侧VPN网络配置对应的远端网关IP。如图3-2所示。

图 3-2 VPN 网关列表

3.4 创建 VPN 连接

操作场景

您需要将VPC中的弹性云服务器和您的数据中心或私有网络连通，创建VPN网关后需要创建VPN连接。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 图标，选择区域和项目。
3. 在系统首页，单击“网络 > 虚拟专用网络”。
4. 在左侧导航栏选择“虚拟专用网络 > 经典版-VPN连接”。

   如果所在region已同步上线企业版VPN，请选择“虚拟专用网络 > 经典版”。
5. 在“VPN连接”页面，单击“创建VPN连接”。
6. 根据界面提示配置参数，并单击“立即购买”。VPN连接参数请参见表3-9。

表 3-9 VPN 连接参数说明

参数	说明	取值样例
区域	不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。	华北-北京四
名称	VPN连接名称。	vpn-001
VPN网关	VPN连接挂载的VPN网关名称。	vpcgw-001
本端子网	本端子网指需要通过VPN访问用户本地网络的VPC子网。支持以下方式设置本端子网： ● 选择子网，表示用户数据中心或者私有网络与您选择的子网进行互通。 ● 手动输入网段，表示用户数据中心或者私有网络与您配置的网段之间进行互通。 **说明** 多个本端子网不支持子网网段重叠。	192.168.1.0/24， 192.168.2.0/24
远端网关	您的数据中心或私有网络中VPN的公网IP地址，用于与VPC内的VPN互通。	-
远端子网	远端子网指需要通过VPN访问VPC的用户本地子网。远端子网网段不能被本端子网网段覆盖，也不能与本端VPC已有的对等连接网段、专线/云连接的远端子网网段重复。 **说明** 多个远端子网不支持子网网段重叠。	192.168.3.0/24， 192.168.4.0/24
预共享密钥	配置在云上VPN连接的密钥，需要与本地网络VPN设备配置的密钥一致。此密钥用于VPN连接协商。 取值范围： ● 取值长度：6~128个字符。 ● 只能包括以下几种字符： – 数字 – 大小写字母 – 特殊符号：包括“~”、“`”、“!”、“@”、“#”、“$”、“%”、“^”、“(”、“)”、“-”、“_”、“+”、“=”、“[”、“]”、“{”、“}”、“|”、"\"、";"、":"、"/"、“:”和“'”	Test@123
确认密钥	再次输入预共享密钥。	Test@123

参数	说明	取值样例
高级配置	• 默认配置 • 已有配置 • 自定义配置：包含IKE策略和IPsec策略，用于指定VPN隧道加密算法。相关配置说明请参见表3-10和表3-11。	自定义配置

表 3-10 IKE 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： • MD5（此算法安全性较低，请慎用） • SHA1（此算法安全性较低，请慎用） • SHA2-256 • SHA2-384 • SHA2-512 默认配置为：SHA2-256。	SHA2-256
加密算法	加密算法，支持的算法： • AES-128 • AES-192 • AES-256 • 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128

参数	说明	取值样例
DH算法	Diffie-Hellman密钥交换算法，支持的算法： ● Group 1（此算法安全性较低，请慎用） ● Group 2（此算法安全性较低，请慎用） ● Group 5（此算法安全性较低，请慎用） ● Group 14 ● Group 15 ● Group 16 ● Group 19 ● Group 20 ● Group 21 默认配置为：Group 14。	Group 14
版本	IKE密钥交换协议版本，支持的版本： ● v1（有安全风险不推荐） ● v2 默认配置为：v2。	v2
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：86400。	86400

表 3-11 IPsec 策略

参数	说明	取值样例
认证算法	认证哈希算法，支持的算法： ● SHA1（此算法安全性较低，请慎用） ● MD5（此算法安全性较低，请慎用） ● SHA2-256 ● SHA2-384 ● SHA2-512 默认配置为：SHA2-256。	SHA2-256

参数	说明	取值样例
加密算法	加密算法，支持的算法： ● AES-128 ● AES-192 ● AES-256 ● 3DES（此算法安全性较低，请慎用） 默认配置为：AES-128。	AES-128
PFS	PFS（Perfect Forward Secrecy）即完美前向安全功能，用来配置IPsec隧道协商时使用。 PFS组支持的算法： ● DH group 1（此算法安全性较低，请慎用） ● DH group 2（此算法安全性较低，请慎用） ● DH group 5（此算法安全性较低，请慎用） ● DH group 14 ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 默认配置为：DH group 14。	DH group 14
传输协议	IPsec传输和封装用户数据时使用的安全协议，目前支持的协议： ● AH ● ESP ● AH-ESP 默认配置为：ESP。	ESP
生命周期（秒）	安全联盟（SA—Security Association）的生存时间，单位：秒。 在超过生存时间后，安全联盟将被重新协商。 默认配置为：3600。	3600

说明

IKE策略指定了IPsec隧道在协商阶段的加密和认证算法，IPsec策略指定了IPsec在数据传输阶段所使用的协议，加密以及认证算法；这些参数在VPC上的VPN连接和您数据中心的VPN中需要进行相同的配置，否则会导致VPN无法建立连接。

以下算法安全性较低，请慎用：

- **认证算法：**SHA1、MD5。
- **加密算法：**3DES。
- **DH算法：**Group 1、Group 2、Group 5。

7. 单击“提交”。
8. 因为隧道的对称性，还需要在您自己数据中心的路由器或者防火墙上进行IPsec VPN隧道配置。

3.5 配置对端设备

配置对端设备详细请参见**《虚拟专用网络管理员指南》**，该指南可以帮助您配置本地的VPN设备，实现您本地网络与华为云VPC子网的互联互通。

详细配置示例可参见：

- **示例：HUAWEI USG6600配置**
- **示例：Fortinet飞塔防火墙VPN配置**
- **示例：深信服防火墙配置**
- **示例：使用TheGreenBow IPsec VPN Client配置云上云下互通**
- **示例：使用Openswan配置云上云下互通**
- **示例：使用strongSwan配置云上云下互通**