ALIBABA CLOUD

阿里云

VPN网关
最佳实践

文档版本：20220510

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.建立VPC到VPC的连接

本文介绍如何使用IPsec-VPN在两个专有网络VPC（Virtual Private Cloud）之间建立安全连接，实现两个VPC内的资源互访。

场景示例

某企业在华东1（杭州）地域拥有一个VPC1，在华北1（青岛）地域拥有一个VPC2。两个VPC均已使用云服务器ECS（Elastic Compute Service）部署了业务，企业因后续发展，现在需要VPC1和VPC2中的业务可以互相访问。

出于建设安全的网络环境考虑，企业计划使用VPN网关产品，通过在两个VPC之间建立IPsec-VPN连接，对数据进行加密传输，实现资源的安全互访。

前提条件

- 您已经在阿里云华东1（杭州）地域和华北1（青岛）地域分别创建了VPC1和VPC2，两个VPC中均使用ECS部署了相关业务。具体操作，请参见搭建IPv4专有网络。

  本示例VPC1和VPC2的配置如下表所示。

  > **说明** 您可以自行规划VPC实例的网段，请确保要互通的网段之间没有重叠。

VPC实例名称	VPC实例所属地域	VPC实例的网段	VPC实例ID	ECS实例名称	ECS实例的IP地址
VPC1	华东1（杭州）	192.168.0.0/16	vpc-bp1e0yx3nsosmitth****	ECS1	192.168.20.161
VPC2	华北1（青岛）	10.0.0.0/16	vpc-m5e83sapxp88cgp5f****	ECS2	10.0.1.110

- 您已经了解两个VPC中ECS实例所应用的安全组规则，并确保安全组规则允许两个ECS实例互访。具体操作，请参见查询安全组规则和添加安全组规则。

配置流程

步骤一：创建VPN网关

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例所属的地域。

   本示例选择**华东1（杭州）**。

   > **说明** VPN网关实例的地域和待关联的VPC实例的地域需相同。

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。

配置项	说明
实例名称	输入VPN网关实例的名称。本示例输入*VPN网关1*。
地域和可用区	选择VPN网关实例所属的地域。本示例选择**华东1（杭州）**。
网关类型	选择VPN网关实例的类型。本示例选择**普通型**。
VPC	选择VPN网关实例关联的VPC实例。本示例选择VPC1。
指定交换机	是否指定VPN网关创建在VPC实例中的某一个交换机下。本示例选择**否**。
带宽规格	选择VPN网关实例的公网带宽峰值。单位：Mbps。
IPsec-VPN	选择开启或关闭IPsec-VPN功能。本示例选择**开启**。
SSL-VPN	选择开启或关闭SSL-VPN功能。本示例选择**关闭**。
计费周期	选择购买时长。 您可以选择是否自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。
服务关联角色	单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。 VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。 若本配置项显示为**已创建**，则表示您的账号下已创建了该角色，无需重复创建。

   更多信息，请参见创建VPN网关实例。

5. 返回**VPN网关**页面，查看已创建的VPN网关实例。

   创建VPN网关实例后，其状态是**准备中**，约1~5分钟会变成**正常**状态。**正常**状态表明VPN网关实例已经完成了初始化，可以正常使用。

6. 重复步骤至步骤，在**华北1（青岛）**地域创建一个名称为*VPN网关2*的VPN网关实例，该VPN网关实例关联VPC2，其余配置与VPN网关1相同。

   创建完成后，两个VPN网关实例的信息如下表所示。

地域	VPN网关实例的名称	VPN网关实例关联的VPC实例名称	VPN网关实例ID	VPN网关IP地址
华东1（杭州）	VPN网关1	VPC1	vpn-bp1l5zihic47jprwa****	120.XX.XX.40
华北1（青岛）	VPN网关2	VPC2	vpn-m5eqjnr4ii6jajpms****	118.XX.XX.20

步骤二：创建用户网关

1. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。
2. 在顶部菜单栏，选择用户网关实例的地域。

   > **说明** 用户网关实例的地域必须和待连接的VPN网关实例的地域相同。

3. 在**用户网关**页面，单击**创建用户网关**。
4. 在**创建用户网关**面板，根据以下信息配置用户网关实例，然后单击**确定**。

   您需要在华东1（杭州）地域和华北1（青岛）地域分别创建一个用户网关实例，用户网关实例的配置请参见下表。

配置项	配置项说明	华东1（杭州）	华北1（青岛）
名称	输入用户网关实例的名称。	*Customer1*	*Customer2*
IP地址	输入用户网关实例的公网IP地址。	本示例输入VPN网关2的IP地址*118.XX.XX.20*。 **说明** 在本示例中VPC1和VPC2互为对方的用户网关。	本示例输入VPN网关1的IP地址*120.XX.XX.40*。

   更多信息，请参见创建用户网关。

   配置完成后，VPN网关实例、用户网关实例与VPC实例之间的对应关系如下表所示。

地域	VPC实例名称	VPN网关实例名称	用户网关实例名称	用户网关实例ID	用户网关IP地址
华东1（杭州）	VPC1	VPN网关1	Customer1	cgw-bp1er5cw26c2b35vm****	118.XX.XX.20
华北1（青岛）	VPC2	VPN网关2	Customer2	cgw-m5e6qdvuxquse3fvm****	120.XX.XX.40

步骤三：创建IPsec连接

VPN网关和用户网关创建完成后，您需要分别创建两个IPsec连接建立VPN加密通道。

1. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
2. 在顶部菜单栏，选择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**。

   您需要在华东1（杭州）地域和华北1（青岛）地域分别创建一个IPsec连接，IPsec连接的配置请参见下表。

配置项	配置项说明	华东1（杭州）	华北1（青岛）
名称	输入IPsec连接的名称。	*IPsec连接1*	*IPsec连接2*
VPN网关	选择已创建的VPN网关实例。	VPN网关1	VPN网关2
用户网关	选择已创建的用户网关实例。	Customer1	Customer2
路由模式	选择路由模式。	选择**目的路由模式**。	选择**目的路由模式**。
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**否**。	本示例选择**否**。
预共享密钥	输入预共享密钥。 如果不输入该值，系统默认生成一个16位的随机字符串。	*fddsFF123***** **注意** 两个IPsec连接的预共享密钥必须相同。	

   其他选项使用默认配置。更多信息，请参见创建IPsec连接。

5. 在**创建成功**对话框中，单击**确定**。

步骤四：配置路由

1. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，单击实例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**面板，根据以下信息配置目的路由，然后单击**确定**。

   您需要分别为VPN网关1和VPN网关2配置路由条目，配置信息如下表所示。

配置项	配置说明	VPN网关1	VPN网关2
目标网段	输入待互通的目标网段。	输入VPC2的私网网段*10.0.0.0/16*。	输入VPC1的私网网段*192.168.0.0/16*。

配置项	配置说明	VPN网关1	VPN网关2
下一跳类型	选择下一跳的类型。	选择**IPsec连接**。	选择**IPsec连接**。
下一跳	选择下一跳。	选择IPsec连接1。	选择IPsec连接2。
发布到VPC	选择是否将新添加的路由发布到VPN网关关联的VPC中。	本示例选择**是**。	本示例选择**是**。
权重	选择路由的权重值。 ○ **100**：高优先级。 ○ **0**：低优先级。	本示例保持默认值100。	本示例保持默认值100。

更多信息，请参见添加目的路由。

步骤五：测试连通性

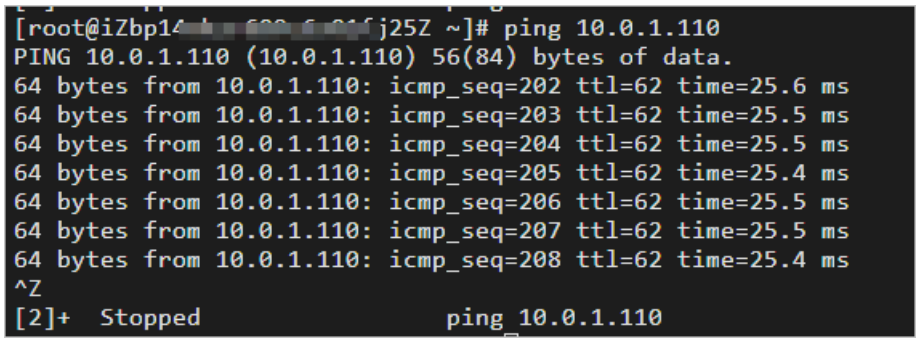
1. 登录VPC1内的ECS1实例。

   关于如何登录ECS实例，请参见连接方式概述。

2. 执行**ping**命令，访问ECS2实例，验证两个VPC之间的资源是否可以互访。

```
ping <ECS2实例IP地址>
```

收到如下所示的回复报文，则证明两个VPC之间的资源可以正常互访。



2.在经典网络中使用SSL VPN

2.1. Linux客户端

本文将介绍如何使用VPN网关的SSL-VPN功能从Linux客户端远程访问部署在经典网络中的云资源。

如果您已经配置了SSL-VPN，您仅需要根据文档中的步骤五将经典网络中的ECS实例连接到VPC，即可实现通过SSL-VPN远程接入经典网络的需求。

前期条件

- 客户端能访问互联网。
- 建议您创建一个新的VPC，并将VPC的网段设置为172.16.0.0/12。如果您选择用已有的VPC，VPC必须满足下表中的约束条件：

VPC网段	限制
172.16.0.0/12	该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 您可以在VPC控制台的路由表详情页面查看已添加的路由条目。
192.168.0.0/16	○ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ○ 需要在经典网络ECS实例中增加192.168.0.0/16指向私网网卡的路由。您可以使用提供的脚本添加路由，单击此处下载路由脚本。 **说明** 在运行脚本前，请仔细阅读脚本中包含的readme文件。

步骤一：创建VPN网关

如果您是经典网络，在VPC内购买的VPN网关配合ClassicLink功能也可以在经典网络中使用。

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPC所属的地域。本示例选择**华东1（杭州）**。

   说明 确保VPC实例的地域与VPN网关实例的地域相同。

3. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
4. 在**VPN网关**页面，单击**创建VPN网关**。
5. 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。

配置	说明
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。本示例选择**华东1（杭州）**。
网关类型	选择网关类型。
VPC	选择要连接的VPC。
指定交换机	是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。
带宽规格	选择VPN网关的带宽规格。 带宽规格是VPN网关所能使用的公网带宽，单位：Mbps。
IPsec-VPN	选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。本示例选择**否**。
SSL-VPN	选择开启或关闭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VPC。本示例选择**否**。
SSL连接数	选择您需要同时连接的客户端最大规格。本示例选择**5**。 **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。 您可以选择是否到期自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。

6. 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**状态就表明VPN网关完成了初始化，可以正常使用了。

步骤二：创建SSL服务端

1. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
2. 在顶部菜单栏，选择SSL服务端的地域。
3. 在**SSL服务端**页面，单击**创建SSL服务端**，然后在**创建SSL服务端**面板，根据以下信息配置SSL服务端。
   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择步骤一中创建的VPN网关。

- **本端网段**：以CIDR地址块的形式输入要连接的经典网络ECS实例的内网网段。单击**添加本端网段**添加多个本端网段。

  在本例中，本端网段为10.1.0.0/16和10.2.0.0/16。

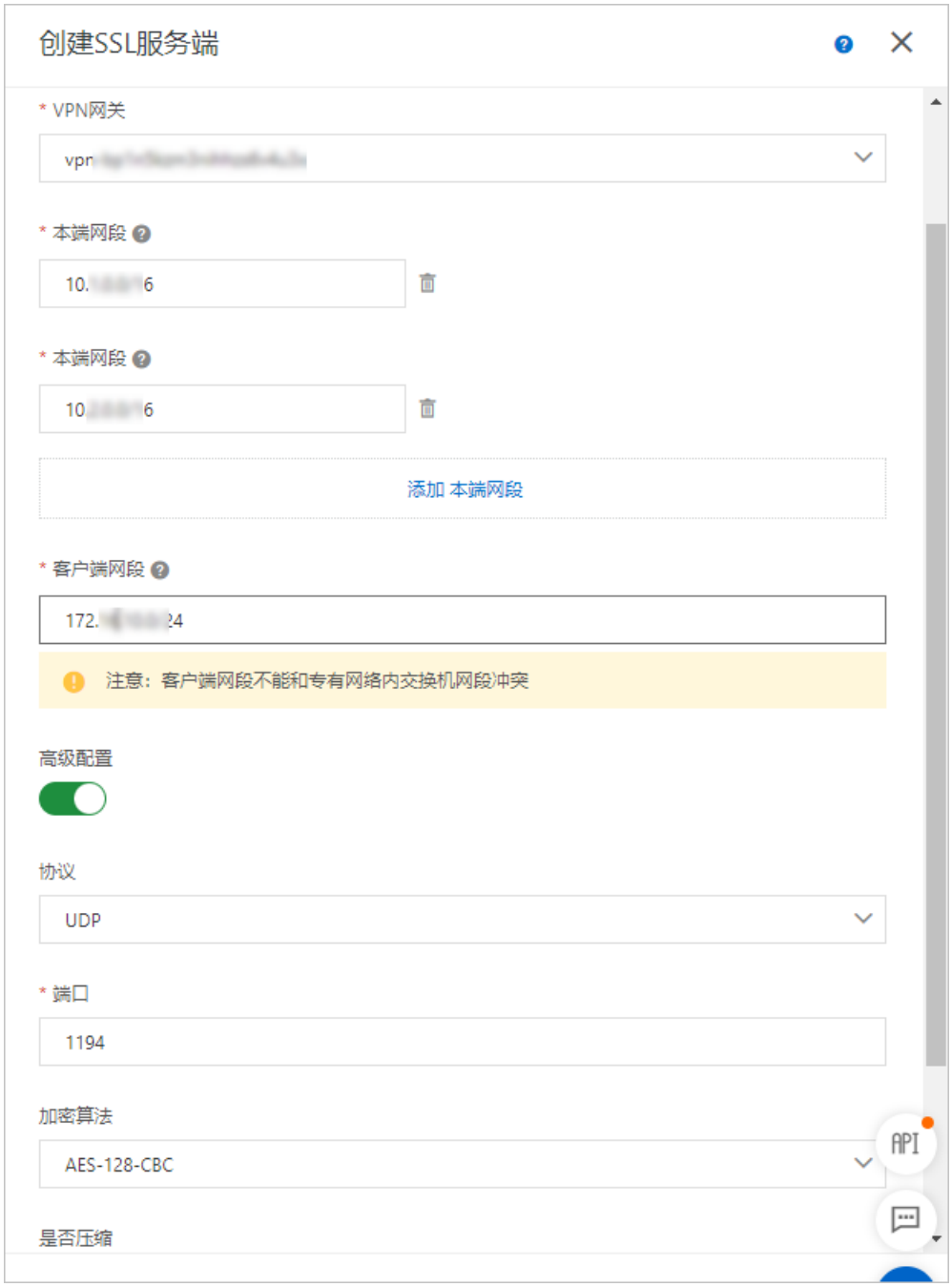
  > **说明** 如果新建ECS实例的IP地址不在已配置的本端网段内，需要添加对应的本端网段。

- **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的IP地址。该客户端网段必须是VPN网关所在的VPC的网段的子集。

  在本例中，客户端网段为172.16.10.0/24。

  > **说明** 客户端网段不是您本地的客户端现有的地址，而是用来分配给客户端通过SSL-VPN访问的IP地址。

- **高级配置**：使用默认高级配置。
- **双因子认证**：开启或关闭双因子认证。如果开启双因子认证，您还需要选择IDaaS实例。



步骤三：创建客户端证书

1. 在左侧导航栏，选择**网关互联 > VPN > SSL客户端** 。
2. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
3. 在**创建SSL客户端证书**对话框，根据以下信息配置SSL客户端证书，然后单击**确定**。
   - **名称**：输入SSL客户端证书的名称。
   - **SSL服务端**：选择步骤二中创建的SSL服务端。
4. 在**SSl客户端**页面，找到已创建的客户端证书，然后在**操作**列单击**下载**，客户端证书会下载到本地。

步骤四：配置客户端

1. 执行以下命令安装OpenVPN客户端。

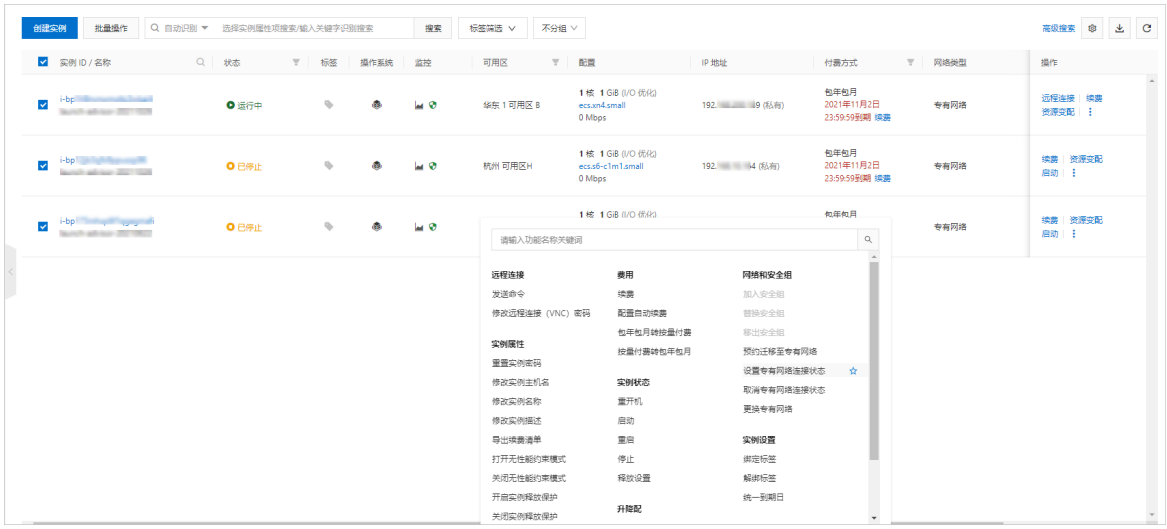
```
yum install -y openvpn
```

2. 将步骤三中下载的证书解压拷贝到*/etc/openvpn/conf/*目录。
3. 执行以下命令启动Openvpn客户端软件。

```
openvpn --config /etc/openvpn/conf/config.ovpn --daemon
```

步骤五：建立ClassicLink连接

1. 登录专有网络管理控制台。
2. 选择目标专有网络的地域，然后单击目标专有网络的实例ID。
3. 在**专有网络详情**页面，单击**开启ClassicLink**。
4. 登录ECS管理控制台。
5. 在左侧导航栏，选择**实例与镜像 > 实例**。
6. 选择一个或多个目标经典网络的ECS实例，选择**更多 > 设置专有网络连接状态** 。



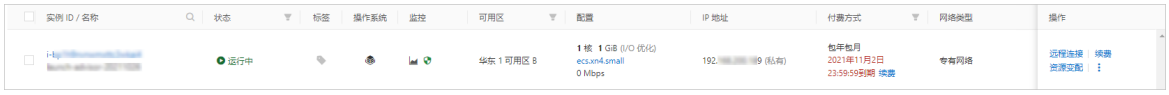
7. 在弹出的**连接专有网络**对话框中选择目标VPC，单击**确定**。
8. 在左侧导航栏，选择**网络和安全 > 安全组** 。
9. 在**安全组**页面，单击**创建安全组**，然后按照如下配置添加访问规则：
   - **规则方向**：入方向。
   - **添加方式**：手动添加。
   - **授权策略**：允许。
   - **优先级**：1。
   - **协议类型**：全部。

- **端口范围**：全部。
- **授权对象**：输入需要通过VPN网关访问本ECS实例的私网地址，如172.16.3.44/32。

  在Linux终端执行**ifconfig**命令，在返回的网络配置信息中找到类似 `inet 172.16.10.6 --> 172.16.10.5 netmask 0xffffffff` 的信息，其中 `172.16.10.6` 就是客户端IP（安全组中配置的授权对象）。

  > **说明** 如果无法通过VPN网关访问ECS实例，可能是客户端IP发生了变化，您需要重新添加安全组规则。

10. 查看ECS实例的状态。



配置完成后，您就可以从Linux客户端访问已连接的经典网络ECS实例中部署的应用了。

2.2. Mac客户端

本文将介绍如何使用VPN网关的SSL-VPN功能从Mac客户端远程访问部署在经典网络中的云资源。

如果您已经配置了SSL-VPN，您仅需要根据文档中步骤五的步骤将经典网络中的ECS实例连接到VPC即可实现通过SSL-VPN远程接入经典网络的需求。

前提条件

在开始之前，确保您的环境满足以下条件：

- 客户端能访问互联网。
- 建议您创建一个新的VPC，并将VPC的网段设置为172.16.0.0/12。如果您选择用已有的VPC，VPC必须满足下表中的约束条件：

VPC网段	限制
172.16.0.0/12	该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 您可以在VPC控制台的路由表详情页面查看已添加的路由条目。

VPC网段	限制
192.168.0.0/16	○ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ○ 需要在经典网络ECS实例中增加192.168.0.0/16指向私网网卡的路由。您可以使用提供的脚本添加路由，单击此处下载路由脚本。 **说明** 在运行脚本前，请仔细阅读脚本中包含的readme文件。

步骤一：创建VPN网关

如果您是经典网络，在VPC内购买的VPN网关配合ClassicLink功能也可以在经典网络中使用。

完成以下操作，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，根据以下信息配置VPN网关，然后单击**立即购买**并完成支付。

配置	说明
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。本示例选择**华东1（杭州）**。
网关类型	选择网关类型。默认为**普通型**。
网络类型	选择网络类型。默认为**公网**。
VPC	选择要连接的VPC。
指定交换机	是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。
带宽规格	选择VPN网关的带宽规格。 带宽规格是VPN网关所能使用的公网带宽，单位：Mbps。
IPsec-VPN	选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。本示例选择**否**。
SSL-VPN	选择开启或关闭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VPC。本示例选择**否**。
计费周期	选择购买时长。 您可以选择是否到期自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。

配置	说明
服务关联角色	单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。 **说明** VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。 若本配置项显示为**已创建**，则表示您的账号下已创建了该角色，无需重复创建。

4. 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。正常状态就表明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SSL服务端

完成以下操作，创建SSL服务端：

1. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
2. 在顶部菜单栏，选择SSL服务端的地域。
3. 在**SSL服务端**页面，单击**创建SSL服务端**，然后在**创建SSL服务端**面板，根据以下信息配置SSL服务端。
   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择步骤一中创建的VPN网关。
   - **本端网段**：以CIDR地址块的形式输入要连接的经典网络ECS实例的内网网段。单击**添加本端网段**添加多个本端网段。

     在本例中，本端网段为10.1.0.0/16和10.2.0.0/16。

     说明 如果新建ECS实例的IP地址不在已配置的本端网段内，需要添加对应的本端网段。
   - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的IP地址。该客户端网段必须是VPN网关所在的VPC的网段的子集。

     在本例中，客户端网段为172.16.10.0/24。

     说明 客户端网段不是您本地的客户端现有的地址，而是用来分配给客户端通过SSL-VPN访问的IP地址。
   - **高级配置**：使用默认高级配置。
   - **双因子认证**：开启或关闭双因子认证。如果开启双因子认证，您还需要选择IDaaS实例。

步骤三：创建客户端证书

完成以下操作，创建客户端证书：

1. 在左侧导航栏，选择**网关互联 > VPN > SSL客户端** 。
2. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
3. 在**创建SSL客户端证书**对话框，根据以下信息配置SSL客户端证书，然后单击**确定**。
   - **名称**：输入SSL客户端证书的名称。
   - **SSL服务端**：选择步骤二中创建的SSL服务端。
4. 在**SSl客户端**页面，找到已创建的客户端证书，然后在**操作**列单击**下载**，客户端证书会下载到本地。

步骤四：客户端配置

完成以下操作，配置客户端：

1. 执行以下命令安装OpenVPN客户端。

```
brew install openvpn
```

> **说明** 如果尚未安装homebrew，先安装homebrew。

2. 将步骤三中下载的证书解压拷贝到配置目录并建立连接：
   i. 备份默认配置文件，然后执行以下命令删除默认配置文件：

   ```
   rm /usr/local/etc/openvpn/*
   ```

   ii. 执行以下命令将文件拷贝到配置目录：

   ```
   cp cert_location /usr/local/etc/openvpn/
   ```

   `cert_location` 是步骤三中下载的证书路径，例如： */Users/example/Downloads/certs6.zip*
   iii. 执行以下命令解压证书文件：

   ```
   unzip /usr/local/etc/openvpn/certs6.zip
   ```

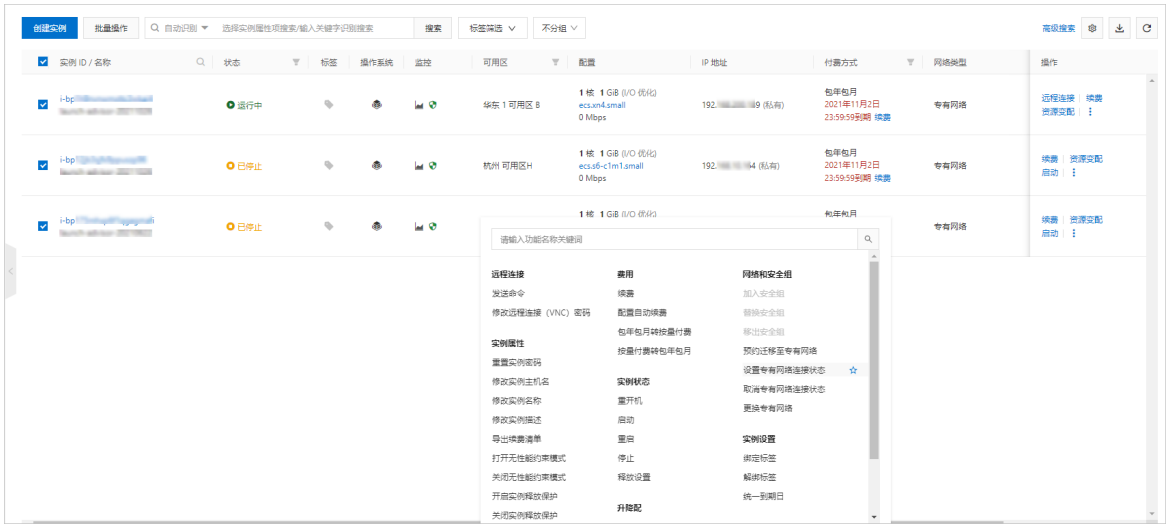
   iv. 执行以下命令发起连接：

   ```
   sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
   ```

步骤五：建立ClassicLink连接

完成以下操作，建立ClassicLink连接：

1. 登录专有网络管理控制台。
2. 选择目标专有网络的地域，然后单击目标专有网络的实例ID。
3. 在**专有网络详情**页面，单击**开启ClassicLink**。
4. 登录ECS管理控制台。
5. 在左侧导航栏，选择**实例与镜像 > 实例**。
6. 选择一个或多个目标经典网络的ECS实例，选择**更多 > 设置专有网络连接状态** 。



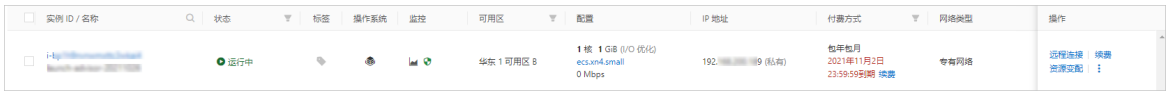
7. 在弹出的**连接专有网络**对话框中选择目标VPC，单击**确定**。
8. 在左侧导航栏，选择**网络和安全 > 安全组** 。
9. 在**安全组**页面，单击**创建安全组**，然后按照如下配置添加访问规则：

- **规则方向**：入方向。
- **添加方式**：手动添加。
- **授权策略**：允许。
- **优先级**：1。
- **协议类型**：全部。
- **端口范围**：全部。
- **授权对象**：输入需要通过VPN网关访问本ECS实例的私网地址，如172.16.3.44/32。

  在Linux终端执行**ifconfig**命令，在返回的网络配置信息中找到类似 `inet 172.16.10.6 --> 172.16.10.5 netmask 0xffffffff` 的信息，其中 `172.16.10.6` 就是客户端IP（安全组中配置的授权对象）。

  > **说明** 如果无法通过VPN网关访问ECS实例，可能是客户端IP发生了变化，您需要重新添加安全组规则。

10. 查看ECS实例的状态。



配置完成后，您就可以从Linux客户端访问已连接的经典网络ECS实例中部署的应用了。

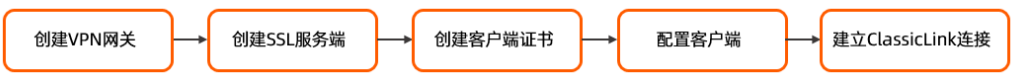
2.3. 在经典网络中使用SSL-VPN

本文为您介绍如何在Linux、Mac和Windows客户端通过阿里云经典网络建立SSL-VPN连接，实现客户端远程访问部署在经典网络中的云资源。

场景示例

本文以下图场景为例。客户端需要先与专有网络VPC（Virtual Private Cloud）建立SSL-VPN连接，然后通过VPC的ClassicLink功能将经典网络连接至该VPC，使该VPC作为流量中转站，建立客户端与经典网络的连接。

配置流程



> **说明** 如果您已经配置了SSL-VPN，您只需要在经典网络中的ECS实例与VPC之间建立ClassicLink连接，即可实现通过SSL-VPN远程接入经典网络的需求。具体操作，请参见步骤五：建立ClassicLink连接。

前提条件

- 您已经创建了一个VPC。具体操作，请参见搭建IPv4专有网络。

  VPC的网段需满足对应的约束条件：

VPC网段	限制
172.16.0.0/12	该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。
10.0.0.0/8	○ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ○ 确保和经典网络ECS实例通信的交换机的网段在10.111.0.0/16内。
192.168.0.0/16	○ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ○ 需要在经典网络ECS实例中增加192.168.0.0/16指向私网网卡的路由。您可以使用提供的脚本添加路由，下载路由脚本。 **说明** 在运行脚本前，请仔细阅读脚本中包含的readme.txt文件。

- 本地IDC中要与经典网络互通的私网网段必须属于VPC的网段，且不能和VPC内交换机的网段冲突，否则无法通信。

步骤一：创建VPN网关

在使用SSL-VPN功能前，您必须创建一个VPN网关。成功创建VPN网关后，系统会为VPN网关分配一个公网IP地址。

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**VPN网关（包月）**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。

配置	说明
实例名称	VPN网关的实例名称。
地域和可用区	选择VPN网关的地域。本示例选择华东1（杭州）。 **说明** 确保VPN网关的地域和VPC的地域相同。
网关类型	选择待创建的VPN网关类型。本示例选择**普通型**。
网络类型	选择待创建的VPN的网络类型。本示例选择**公网**。
VPC	选择要连接的VPC。

配置	说明
指定交换机	选择是否指定VPN网关所属的交换机。本示例选择**否**。
带宽规格	选择VPN网关的带宽规格。带宽规格是VPN网关所具备的公网带宽峰值。
IPsec-VPN	选择是否开启IPsec-VPN功能。本示例选择**关闭**。
SSL-VPN	选择是否开启SSL-VPN功能。本示例选择**开启**。
SSL连接数	选择您需要同时连接的客户端最大规格。
计费周期	选择购买时长。关于计费的更多信息， 请参见计费说明。
服务关联角色	单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。 VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。 若本配置项显示为**已创建**，则表示您的账号下已经创建了该角色，无需重复创建。

4. 返回**VPN网关**页面，查看创建的VPN网关。

   VPN网关的创建一般需要1~5分钟，刚创建的VPN网关状态是准备中，约2分钟后会变成正常状态。正常状态表示VPN网关完成初始化，可以正常使用。

步骤二：创建SSL服务端

创建VPN网关后，您需要使用VPN网关创建一个SSL服务端，为后续创建SSL-VPN连接做准备。

1. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
2. 在顶部菜单栏，选择SSL服务端的地域。
3. 在**SSL服务端**页面，单击**创建SSL服务端**。
4. 在**创建SSL服务端**面板，配置SSL服务端，然后单击**确定**。

配置	说明
名称	输入SSL服务端的名称。
VPN网关	选择步骤一中创建的VPN网关。
本端网段	以CIDR地址块的形式输入要连接的经典网络ECS实例的内网网段。单击**添加本端网段**可添加多个本端网段。 本示例中，本端网段为10.1.0.0/16和10.2.0.0/16。 **说明** 如果新建ECS实例的IP地址不在已配置的本端网段内，需要添加对应的本端网段。

配置	说明
客户端网段	以CIDR地址块的形式输入客户端连接服务端时使用的网段，系统将从该网段中为客户端分配IP地址，客户端将使用被分配的IP地址访问VPC中的资源。该客户端网段必须是VPN网关所在的VPC网段的子集。 本示例中，客户端网段为172.16.10.0/24。
高级配置	使用默认高级配置。

步骤三：创建客户端证书

创建SSL服务端后，您还需根据SSL服务端创建SSL客户端证书。

1. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
2. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
3. 在**创建SSL客户端证书**面板，输入客户端证书名称并选择对应的SSL服务端，然后单击**确定**。
4. 在**SSL客户端**页面，找到已创建的客户端证书，然后在**操作**列单击**下载**，下载生成的客户端证书。

步骤四：配置客户端

下载SSL客户端证书后，您需要将客户端证书安装到客户端，安装完成后，客户端可以与VPN网关建立SSL-VPN连接。以下内容分别为您介绍如何配置Linux、Mac和Windows客户端。

配置Linux客户端

1. 执行以下命令，安装OpenVPN客户端。

   ```
   yum install -y openvpn
   ```

2. 将下载的客户端证书解压并拷贝至*/etc/openvpn/conf/*目录。
3. 执行以下命令，启动Openvpn客户端软件。

   ```
   openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   ```

配置Mac客户端

1. 打开命令行窗口。
2. 如果您的客户端尚未安装homebrew，执行以下命令安装homebrew。

   ```
   /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
   ```

3. 执行以下命令安装OpenVPN客户端。

   ```
   brew install openvpn
   ```

4. 将下载的SSL客户端证书解压并拷贝至配置目录。
   i. 备份*/usr/local/etc/openvpn*文件夹下的所有配置文件。
   ii. 执行以下命令删除OpenVPN的配置文件。

   ```
   rm /usr/local/etc/openvpn/*
   ```

iii. 执行以下命令拷贝已经下载的SSL客户端证书到*/usr/local/etc/openvpn/*配置目录。

```
cp cert_location /usr/local/etc/openvpn/
```

`cert_location` 是SSL客户端证书所在路径，例如：*/Users/example/Downloads/certs6.zip*。

5. 执行以下命令解压证书。

```
cd  /usr/local/etc/openvpn/
unzip /usr/local/etc/openvpn/certs6.zip
```

6. 执行以下命令建立VPN连接。

```
sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
```

配置Windows客户端

1. 下载并安装OpenVPN客户端。

   下载OpenVPN客户端安装包。

2. 将已经下载的SSL客户端证书解压拷贝到OpenVPN客户端安装路径下的*OpenVPN\config*目录。
3. 启动OpenVPN客户端软件，单击**Connect**发起连接。

步骤五：建立ClassicLink连接

VPC提供ClassicLink功能，使经典网络的ECS实例可以和专有网络中的云资源通过内网互通。

1. 开启ClassicLink功能。
   i. 登录专有网络管理控制台。
   ii. 在顶部菜单栏处，选择专有网络的地域。
   iii. 在**专有网络**页面，找到目标专有网络，单击专有网络的ID。
   iv. 在专有网络详情页面，单击页面右上方的**开启ClassicLink**。
   v. 在**开启ClassicLink**对话框中，单击**确定**。

   开启ClassicLink后，ClassicLink的状态变更为**已开启**。

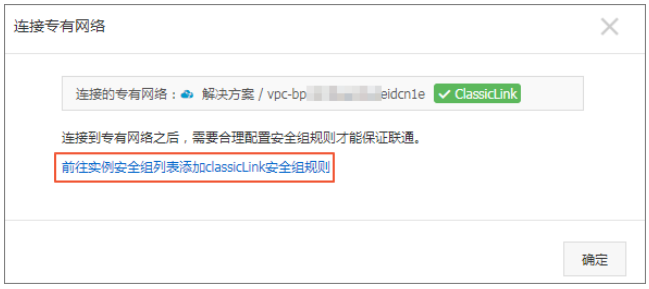
2. 登录ECS管理控制台。
3. 在左侧导航栏，选择**实例与镜像 > 实例**。
4. 选择ECS实例所属的地域。
5. 连接专有网络。
   i. 在**实例列表**页面，找到目标经典网络实例，然后在**操作**列选择**更多 > 网络和安全组 > 设置专有**

网络连接状态。

ii. 在**连接专有网络**对话框，选择要连接的专有网络，然后单击**确定**。

6. 配置ClassicLink安全组规则。

i. 单击**前往实例安全组列表添加classicLink安全组规则**，然后单击**添加ClassicLink安全组规则**。



ii. 在**添加ClassicLink安全组规则**对话框，根据以下信息配置ClassicLink安全组规则，然后单击**确定**。

配置	说明
经典网络安全组	显示经典网络安全组的名称。
选择专有网络安全组	选择专有网络的安全组。
授权方式	选择一种授权方式： ■ 经典网络 <=> 专有网络：相互授权访问，推荐使用这种授权方式。 ■ 经典网络 => 专有网络：授权经典网络ECS访问专有网络内的云资源。 ■ 专有网络 => 经典网络：授权专有网络内的云资源访问经典网络ECS。
协议类型	选择授权通信的协议。
端口范围	选择授权通信的端口。端口的输入格式为xx/xx，例如授权80端口，则输入80/80。
优先级	设置该规则的优先级。数字越小，优先级越高。
描述	输入安全组描述。

7. 返回ECS管理控制台，单击右侧的配置图标，在弹出的对话框中选择**连接状态**，然后单击**确定**，查看ECS实例的连接状态。

自定义列表选项

连接状态选项

已连接状态

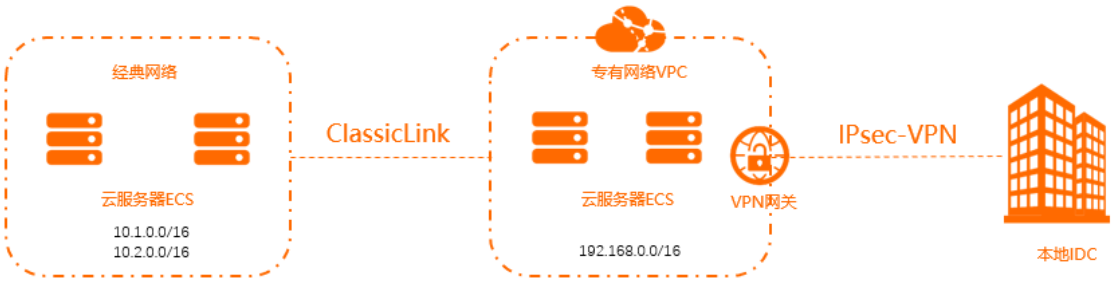
配置完成后，您可以从客户端远程访问已连接的经典网络ECS实例中部署的应用。

3.在经典网络中使用IPsec-VPN

本文为您介绍如何使本地数据中心IDC（Internet Data Center）与阿里云经典网络建立IPsec-VPN连接，实现本地IDC与经典网络中的资源安全互通。

背景信息

本地IDC要与经典网络建立IPsec-VPN连接，需借助专有网络VPC（Virtual Private Cloud）。本地IDC先与VPC建立IPsec-VPN连接，然后通过VPC的ClassicLink功能将经典网络连接至该VPC，使该VPC作为流量中转站，实现本地IDC与经典网络的互通。



前提条件

- 您已经创建了一个VPC。具体操作，请参见搭建IPv4专有网络。

  VPC的网段需满足对应的约束条件：

VPC网段	限制
172.16.0.0/12	该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。
10.0.0.0/8	○ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ○ 确保和经典网络ECS实例通信的交换机的网段在10.111.0.0/16内。
192.168.0.0/16	○ 该VPC中不存在目标网段为10.0.0.0/8的自定义路由条目。 ○ 需要在经典网络ECS实例中增加192.168.0.0/16指向私网网卡的路由。您可以使用提供的脚本添加路由，下载路由脚本。 **说明** 在运行脚本前，请仔细阅读脚本中包含的readme.txt文件。

- 本地IDC中要与经典网络互通的私网网段必须属于VPC的网段，且不能和VPC内交换机的网段冲突，否则无法通信。

配置步骤

1. 建立本地IDC至VPC的IPsec-VPN连接。

   具体操作，请参见建立VPC到本地数据中心的连接。

2. 开启ClassicLink功能。

具体操作，请参见开启ClassicLink功能。

3. 建立ClassicLink连接。

   具体操作，请参见建立ClassicLink连接。

4. 测试连通性。

   使用 `ping` 命令，从本地IDC访问经典网络中的一个ECS实例，测试本地IDC和经典网络的连通性。

4.SSL-VPN双因子认证

4.1. Windows客户端双因子认证

本文以Windows客户端为例介绍如何通过SSL-VPN双因子认证后接入专有网络VPC。

前提条件

开始前，请确保满足以下条件：

- 您已经购买了应用身份服务（IDaaS）实例，并且已经在阿里云上维护了IDaaS的用户信息。更多信息，请参见组织机构和账户。

  > **说明** 阿里云云盾应用身份服务IDaaS（Alibaba Cloud Identity as a Service）致力于统一身份认证领域，实现一个账号打通所有应用服务。开启并选择IDaaS实例后，SSL拨号客户端不仅要完成证书密钥认证，在启动OpenVPN后还需要用户名和密码的认证，认证通过后才可以访问云上资源，减少SSL-VPN登录认证风险。

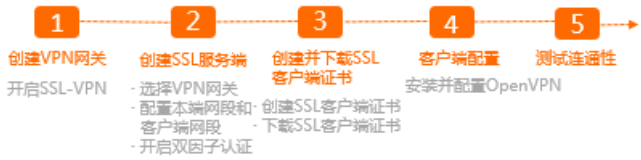
- 您已经创建了专有网络。具体操作，请参见创建和管理专有网络。

背景信息

某公司在华东1（杭州）地域创建了专有网络VPC，网段为192.168.1.0/24。因业务发展，出差员工需要使用Windows客户端访问云上VPC资源。

如上图，您可以在云上创建VPN网关，配置SSL服务端并开启双因子认证。Windows客户端通过SSL-VPN接入云上VPC，不仅要完成证书认证，还需要完成双因子认证，认证通过后才可以访问云上资源，提高了VPN连接的安全性和可管理性。

配置步骤



步骤一：创建VPN网关

VPN网关是一款基于互联网的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络安全可靠的连接。

> **注意** 请确保您的VPN网关是2020年03月05日00时00分之后创建的，否则不支持双因子认证功能。

1.

2. 在顶部菜单栏处，选择专有网络的地域。

   本示例选择**华东1（杭州）**。

   > **说明** 确保VPC的地域和VPN网关的地域相同。

3. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
4. 在**VPN网关**页面，单击**创建VPN网关**。
5. 在VPN网关的购买页面，根据以下信息配置VPN网关然后单击**立即购买**完成支付。

配置	说明
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。本示例选择**华东1（杭州）**。
网关类型	选择网关类型。
VPC	选择要连接的VPC。
指定交换机	是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。
带宽规格	选择VPN网关的带宽规格。 带宽规格是VPN网关所能使用的公网带宽，单位：Mbps。
IPsec-VPN	选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。本示例选择**否**。
SSL-VPN	选择开启或关闭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VPC。本示例选择**否**。
SSL连接数	选择您需要同时连接的客户端最大规格。本示例选择**5**。 **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。 您可以选择是否到期自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。

步骤二：创建SSL服务端

SSL-VPN基于OpenVPN架构，您需要通过SSL-VPN服务端来指定要连接的IP地址段和客户端连接时使用的IP地址段，并开启双因子认证。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏处，选择SSL服务端的地域。

本示例选择**华东1（杭州）**。

4. 在**SSL服务端**页面，单击**创建SSL服务端**。
5. 在**创建SSL服务端**面板，根据以下信息配置SSL服务端，然后单击**确定**。
   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择步骤一中创建的VPN网关。
   - **本端网段**：以CIDR地址块的形式输入客户端通过SSL-VPN连接要访问的网段。本示例输入**192.168.0.0/24**。
   - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。本示例输入**10.0.0.0/24**。
   - **高级配置**：打开高级配置，并完成以下配置。
     - **协议**：选择SSL连接使用的协议，支持UDP和TCP。本示例使用默认配置。
     - **端口**：SSL连接使用的端口。本示例使用默认配置。
     - **加密算法**：SSL连接使用的加密算法，支持AES-128-CBC、AES-192-CBC、AES-256-CBC。本示例使用默认配置。
     - **是否压缩**：是否对传输数据进行压缩处理。本示例使用默认配置。
     - **双因子认证**：打开双因子认证，然后选择IDaaS实例。

       > **说明** 如果您是首次使用双因子认证功能，请先完成授权后再创建SSL服务端。

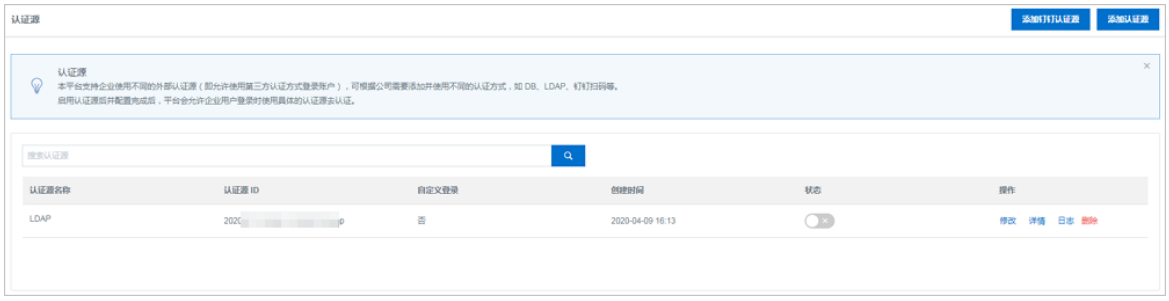
（可选）步骤三：配置云产品AD认证

双因子认证默认支持使用IDaaS的用户名和密码进行认证，您可以选择配置AD认证。配置成功后，SSL-VPN具备AD认证能力。如果您仅需要使用IDaaS的用户名和密码进行认证，请忽略该步骤。

1. 登录云盾IDaaS管理控制台。
2. 在**实例列表**页面，找到目标IDaaS实例，在**操作**列单击**管理**。
3. 在左侧导航栏，选择**认证 > 认证源**，然后单击**添加认证源**。
4. 在**添加认证源**页面，找到**LDAP**，在其**操作**列单击**添加认证源**。
5. 在**添加认证源（LDAP）**面板，创建LDAP认证源。

   详细信息，请参见LDAP认证登录。

   认证源创建成功后，您可以查看创建的认证源。



6. 在**认证源**页面，找到目标认证源，在其**状态**列单击 图标，然后在弹出的对话框中，单击**确定**。
7. 在左侧导航栏，选择**设置 > 安全设置**。
8. 在**安全设置**页面，单击**云产品AD认证**页签。

9. 选择创建的AD认证源，启用该功能并单击**保存设置**。

步骤四：创建并下载SSL客户端证书

根据SSL服务端配置，创建并下载SSL客户端证书。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
3. 在顶部菜单栏处，选择SSL客户端的地域。

   本示例选择**华东1（杭州）**。
4. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
5. 在**创建SSL客户端证书**面板，根据以下信息配置SSL客户端证书，然后单击**确定**。
   - **名称**：输入SSL客户端证书的名称。
   - **SSL服务端**：选择步骤二中创建的SSL服务端。
6. 在**SSL客户端**页面，找到已创建的SSL客户端证书，然后在**操作**列单击**下载**。

   SSL客户端证书会下载到本地。

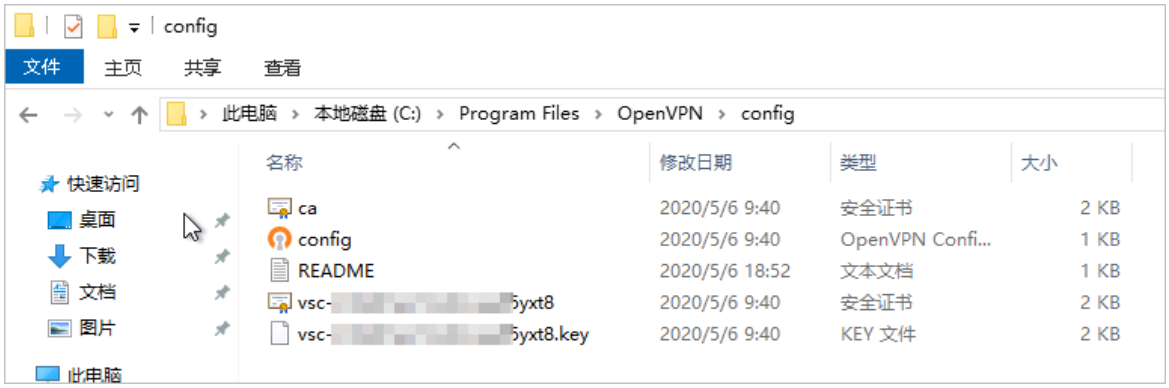
步骤五：配置客户端

完成以下操作，配置Windows客户端。

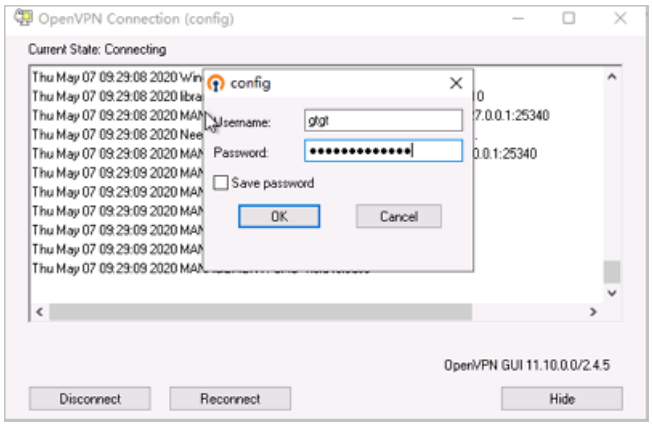
1. 下载并安装OpenVPN客户端。

   下载OpenVPN。
2. 将步骤四中下载的证书解压拷贝到*OpenVPN\config*目录。

   本示例将证书解压拷贝到*C:\Program Files\OpenVPN\config*目录，请您根据安装路径将证书解压拷贝到实际的目录。



3. 启动Openvpn客户端软件，并完成用户名和密码认证。



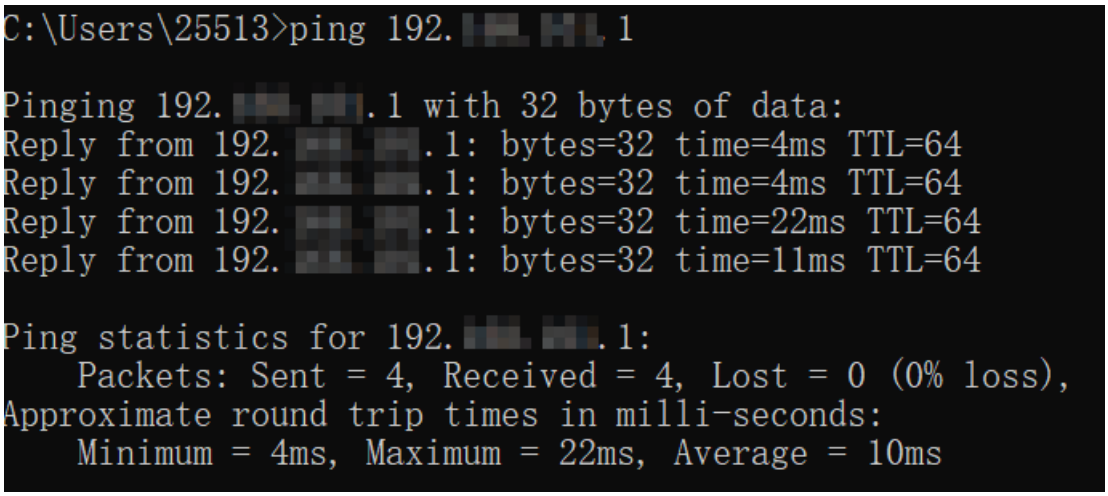
步骤六：测试连通性

完成以下操作，测试Windows客户端与云上VPC的连通性。

1. 打开Windows客户端的cmd窗口。
2. 通过 `ping` 命令 `ping` VPC下的ECS实例的IP地址，验证通信是否正常。

> **说明** 请确保测试的ECS实例的安全组规则允许Windows客户端远程连接。详细信息，请参见安全组应用案例ECS安全组配置操作指南。

经测试，Windows客户端可以正常访问ECS实例。



4.2. Linux客户端双因子认证

本文以Linux客户端为例为您介绍如何通过SSL-VPN双因子认证后接入专有网络VPC。

前提条件

开始前，请确保满足以下条件：

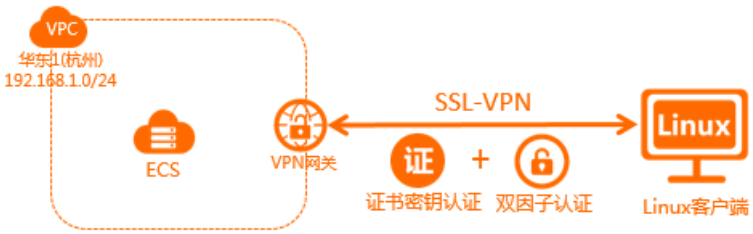
- 您已经购买了应用身份服务（IDaaS）实例，并且已经在阿里云上维护了IDaaS的用户信息。更多信息，请参见组织机构和账户。

> **说明** 阿里云云盾应用身份服务IDaaS（Alibaba Cloud Identity as a Service）致力于统一身份认证领域，实现一个账号打通所有应用服务。开启并选择IDaaS实例后，SSL拨号客户端不仅要完成证书密钥认证，在启动OpenVPN后还需要用户名和密码的认证，认证通过后才可以访问云上资源，减少SSL-VPN登录认证风险。

- 您已经创建了专有网络。具体操作，请参见创建和管理专有网络。

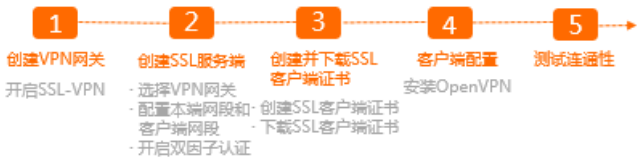
场景示例

某公司在华东1（杭州）地域创建了专有网络VPC，网段为192.168.1.0/24。因业务发展，出差员工需要使用Linux客户端访问云上VPC资源。



如上图，您可以在云上创建VPN网关，配置SSL服务端并开启双因子认证。Linux客户端通过SSL-VPN接入云上VPC，不仅要完成证书认证，还需要完成双因子认证，认证通过后才可以访问云上资源，此过程提高了VPN连接的安全性和可管理性。

配置步骤



步骤一：创建VPN网关

VPN网关是一款基于互联网的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络安全可靠的连接。

> **注意** 请确保您的VPN网关是2020年03月05日00时00分之后创建的，否则不支持双因子认证功能。

1.
2. 在顶部菜单栏处，选择专有网络的地域。

   本示例选择**华东1（杭州）**。

   > **说明** 确保VPC的地域和VPN网关的地域相同。

3. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
4. 在**VPN网关**页面，单击**创建VPN网关**。
5. 在VPN网关的购买页面，根据以下信息配置VPN网关然后单击**立即购买**完成支付。

配置	说明
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。本示例选择**华东1（杭州）**。
网关类型	选择网关类型。
VPC	选择要连接的VPC。
指定交换机	是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。
带宽规格	选择VPN网关的带宽规格。 带宽规格是VPN网关所能使用的公网带宽，单位：Mbps。
IPsec-VPN	选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。本示例选择**否**。
SSL-VPN	选择开启或关闭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VPC。本示例选择**否**。
SSL连接数	选择您需要同时连接的客户端最大规格。本示例选择**5**。 **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。 您可以选择是否到期自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。

步骤二：创建SSL服务端

SSL-VPN基于OpenVPN架构，您需要通过SSL-VPN服务端来指定要连接的IP地址段和客户端连接时使用的IP地址段，并开启双因子认证。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏处，选择SSL服务端的地域。

   本示例选择**华东1（杭州）**。
4. 在**SSL服务端**页面，单击**创建SSL服务端**。
5. 在**创建SSL服务端**面板，根据以下信息配置SSL服务端，然后单击**确定**。
   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择步骤一中创建的VPN网关。
   - **本端网段**：以CIDR地址块的形式输入客户端通过SSL-VPN连接要访问的网段。本示例输入**192.168.0.0/24**。
   - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。本示例输入**10.0.0.0/24**。

- **高级配置**：打开高级配置，并完成以下配置。
  - **协议**：选择SSL连接使用的协议，支持UDP和TCP。本示例使用默认配置。
  - **端口**：SSL连接使用的端口。本示例使用默认配置。
  - **加密算法**：SSL连接使用的加密算法，支持AES-128-CBC、AES-192-CBC、AES-256-CBC。本示例使用默认配置。
  - **是否压缩**：是否对传输数据进行压缩处理。本示例使用默认配置。
  - **双因子认证**：打开双因子认证，然后选择IDaaS实例。

    > **说明** 如果您是首次使用双因子认证功能，请先完成授权后再创建SSL服务端。

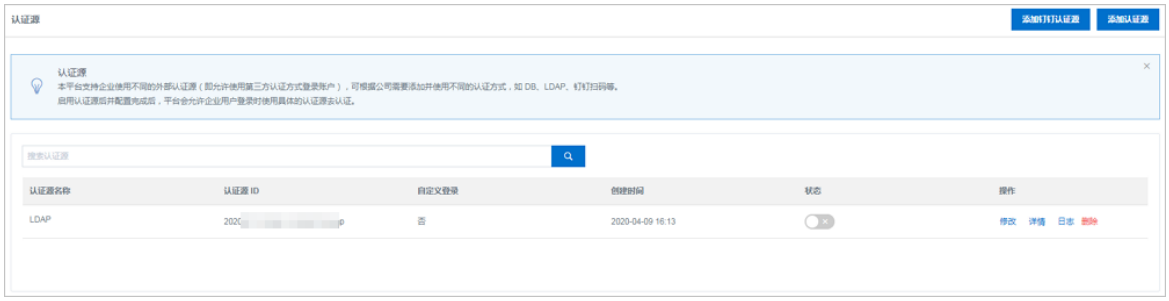
（可选）步骤三：配置云产品AD认证

双因子认证默认支持使用IDaaS的用户名和密码进行认证，您可以选择配置AD认证。配置成功后，SSL-VPN具备AD认证能力。如果您仅需要使用IDaaS的用户名和密码进行认证，请忽略该步骤。

1. 登录云盾IDaaS管理控制台。
2. 在**实例列表**页面，找到目标IDaaS实例，在**操作**列单击**管理**。
3. 在左侧导航栏，选择**认证 > 认证源**，然后单击**添加认证源**。
4. 在**添加认证源**页面，找到**LDAP**，在其**操作**列单击**添加认证源**。
5. 在**添加认证源（LDAP）**面板，创建LDAP认证源。

   详细信息，请参见LDAP认证登录。

   认证源创建成功后，您可以查看创建的认证源。



6. 在**认证源**页面，找到目标认证源，在其**状态**列单击 图标，然后在弹出的对话框中，单击**确定**。
7. 在左侧导航栏，选择**设置 > 安全设置**。
8. 在**安全设置**页面，单击**云产品AD认证**页签。
9. 选择创建的AD认证源，启用该功能并单击**保存设置**。

步骤四：创建并下载SSL客户端证书

根据SSL服务端配置，创建并下载SSL客户端证书。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
3. 在顶部菜单栏处，选择SSL客户端的地域。

   本示例选择**华东1（杭州）**。
4. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
5. 在**创建SSL客户端证书**面板，根据以下信息配置SSL客户端证书，然后单击**确定**。
   - **名称**：输入SSL客户端证书的名称。
   - **SSL服务端**：选择步骤二中创建的SSL服务端。
6. 在**SSL客户端**页面，找到已创建的SSL客户端证书，然后在**操作**列单击**下载**。

   SSL客户端证书会下载到本地。

步骤五：配置客户端

完成以下操作，配置Linux客户端。

1. 在Linux客户端，执行以下命令安装OpenVPN客户端。

   ```
   yum install -y openvpn
   ```
2. 将步骤四中下载的证书解压拷贝到*/etc/openvpn/conf/*目录。
   i. 执行以下命令将文件拷贝到配置目录：

   ```
   cp cert_location /usr/local/etc/openvpn/conf/
   ```

   ii. 执行以下命令解压证书文件

   ```
   unzip /usr/local/etc/openvpn/conf/certs6.zip
   ```
3. 执行以下命令启动Openvpn客户端软件，并完成用户名密码验证。

   ```
   openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   ```

   ```
   [root@iZ8ps conf]# openvpn --config /etc/openvpn/conf/config.ovpn --daemon
   Enter Auth Username: dgtt
   Enter Auth Password: **********
   ```

步骤六：测试连通性

完成以下操作，测试Linux客户端与云上VPC的连通性。

1. 登录Linux客户端。
2. 通过 `ping` 命令访问VPC下的ECS实例的IP地址，验证通信是否正常。

   > **说明** 请确保测试的ECS实例的安全组规则允许Linux客户端远程连接。详细信息，请参见ECS安全组配置案例。

   经测试，Linux客户端可以正常访问ECS实例。

4.3. Mac客户端双因子认证

本文以Mac客户端为例为您介绍如何通过SSL-VPN双因子认证后接入专有网络VPC。

前提条件

开始前，请确保满足以下条件：

- 您已经购买了应用身份服务（IDaaS）实例，并且已经在阿里云上维护了IDaaS的用户信息。更多信息，请参见组织机构和账户。

  > **说明** 阿里云云盾应用身份服务IDaaS（Alibaba Cloud Identity as a Service）致力于统一身份认证领域，实现一个账号打通所有应用服务。开启并选择IDaaS实例后，SSL拨号客户端不仅要完成证书密钥认证，在启动OpenVPN后还需要用户名和密码的认证，认证通过后才可以访问云上资源，减少SSL-VPN登录认证风险。

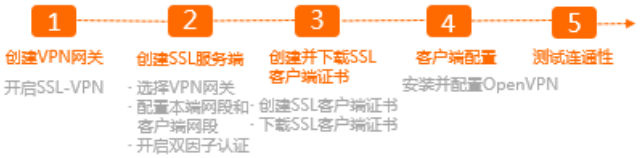
- 您已经创建了专有网络。具体操作，请参见创建和管理专有网络。
- 您已经安装了homebrew。若您尚未安装homebrew，请先安装homebrew。

场景示例

某公司在华东1（杭州）地域创建了专有网络VPC，网段为192.168.1.0/24。因业务发展，出差员工需要使用Mac客户端访问云上VPC资源。

如上图，您可以在云上创建VPN网关，配置SSL服务端并开启双因子认证。Mac客户端通过SSL-VPN接入云上VPC，不仅要完成证书认证，还需要完成双因子认证，认证通过后才可以访问云上资源，提高了VPN连接的安全性和可管理性。

配置步骤



步骤一：创建VPN网关

VPN网关是一款基于互联网的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络安全可靠的连接。

> **注意** 请确保您的VPN网关是2020年03月05日00时00分之后创建的，否则不支持双因子认证功能。

1.
2. 在顶部菜单栏处，选择专有网络的地域。

   本示例选择**华东1（杭州）**。

   > **说明** 确保VPC的地域和VPN网关的地域相同。

3. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
4. 在**VPN网关**页面，单击**创建VPN网关**。
5. 在VPN网关的购买页面，根据以下信息配置VPN网关然后单击**立即购买**完成支付。

配置	说明
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。本示例选择**华东1（杭州）**。
网关类型	选择网关类型。
VPC	选择要连接的VPC。
指定交换机	是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。
带宽规格	选择VPN网关的带宽规格。 带宽规格是VPN网关所能使用的公网带宽，单位：Mbps。
IPsec-VPN	选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。本示例选择**否**。
SSL-VPN	选择开启或关闭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VPC。本示例选择**否**。
SSL连接数	选择您需要同时连接的客户端最大规格。本示例选择**5**。 **说明** 本选项只有在选择开启了SSL-VPN功能后才可配置。

配置	说明
计费周期	选择购买时长。 您可以选择是否到期自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。

步骤二：创建SSL服务端

SSL-VPN基于OpenVPN架构，您需要通过SSL-VPN服务端来指定要连接的IP地址段和客户端连接时使用的IP地址段，并开启双因子认证。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL服务端**。
3. 在顶部菜单栏处，选择SSL服务端的地域。

   本示例选择**华东1（杭州）**。
4. 在**SSL服务端**页面，单击**创建SSL服务端**。
5. 在**创建SSL服务端**面板，根据以下信息配置SSL服务端，然后单击**确定**。
   - **名称**：输入SSL服务端的名称。
   - **VPN网关**：选择步骤一中创建的VPN网关。
   - **本端网段**：以CIDR地址块的形式输入客户端通过SSL-VPN连接要访问的网段。本示例输入**192.168.0.0/24**。
   - **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。本示例输入**10.0.0.0/24**。
   - **高级配置**：打开高级配置，并完成以下配置。
     - **协议**：选择SSL连接使用的协议，支持UDP和TCP。本示例使用默认配置。
     - **端口**：SSL连接使用的端口。本示例使用默认配置。
     - **加密算法**：SSL连接使用的加密算法，支持AES-128-CBC、AES-192-CBC、AES-256-CBC。本示例使用默认配置。
     - **是否压缩**：是否对传输数据进行压缩处理。本示例使用默认配置。
     - **双因子认证**：打开双因子认证，然后选择IDaaS实例。

       > **说明** 如果您是首次使用双因子认证功能，请先完成授权后再创建SSL服务端。

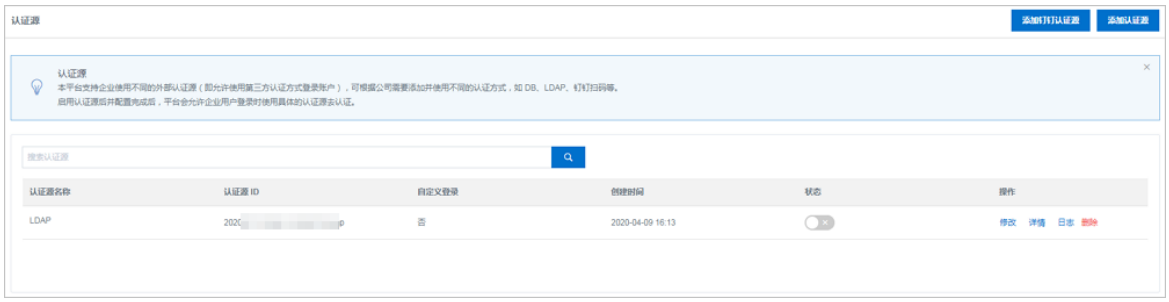
（可选）步骤三：配置云产品AD认证

双因子认证默认支持使用IDaaS的用户名和密码进行认证，您可以选择配置AD认证。配置成功后，SSL-VPN具备AD认证能力。如果您仅需要使用IDaaS的用户名和密码进行认证，请忽略该步骤。

1. 登录云盾IDaaS管理控制台。
2. 在**实例列表**页面，找到目标IDaaS实例，在**操作**列单击**管理**。
3. 在左侧导航栏，选择**认证 > 认证源**，然后单击**添加认证源**。
4. 在**添加认证源**页面，找到**LDAP**，在其**操作**列单击**添加认证源**。
5. 在**添加认证源（LDAP）**面板，创建LDAP认证源。

详细信息，请参见LDAP认证登录。

认证源创建成功后，您可以查看创建的认证源。



6. 在**认证源**页面，找到目标认证源，在其**状态**列单击 图标，然后在弹出的对话框中，单击**确定**。
7. 在左侧导航栏，选择**设置 > 安全设置**。
8. 在**安全设置**页面，单击**云产品AD认证**页签。
9. 选择创建的AD认证源，启用该功能并单击**保存设置**。

步骤四：创建并下载SSL客户端证书

根据SSL服务端配置，创建并下载SSL客户端证书。

1. 登录VPN网关管理控制台。
2. 在左侧导航栏，选择**网间互联 > VPN > SSL客户端**。
3. 在顶部菜单栏处，选择SSL客户端的地域。

   本示例选择**华东1（杭州）**。
4. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
5. 在**创建SSL客户端证书**面板，根据以下信息配置SSL客户端证书，然后单击**确定**。
   - **名称**：输入SSL客户端证书的名称。
   - **SSL服务端**：选择步骤二中创建的SSL服务端。
6. 在**SSL客户端**页面，找到已创建的SSL客户端证书，然后在**操作**列单击**下载**。

   SSL客户端证书会下载到本地。

步骤五：配置客户端

完成以下操作，配置Mac客户端。

1. 在Mac客户端，执行以下命令安装OpenVPN客户端。

```
brew install openvpn
```

> **说明** homebrew操作方便，建议您使用Homebrew。

2. 执行以下命令删除默认配置文件。

```
rm /usr/local/etc/openvpn/*
```

3. 执行以下命令将文件拷贝到配置目录。

```
cp cert_location /usr/local/etc/openvpn/
```

`cert_location` 是步骤四中下载的证书路径，例如：*/Users/example/Downloads/certs.zip*。

4. 执行以下命令将步骤四中下载的证书解压。

```
cd  /usr/local/etc/openvpn
unzip /usr/local/etc/openvpn/certs.zip
```

5. 执行以下命令发起连接，并完成用户名和密码验证。

```
sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
```

步骤六：测试连通性

完成以下操作，测试Mac客户端与云上VPC的连通性。

1. 打开Mac客户端的命令行窗口。
2. 通过 `ping` 命令访问VPC下的ECS实例的IP地址，验证通信是否正常。

> **说明** 请确保测试的ECS实例的安全组规则允许Mac客户端远程连接。详细信息，请参见ECS安全组配置案例。

4.4. 通过LDAP认证建立SSL-VPN连接

本文为您介绍如何通过应用身份服务IDaaS（Alibaba Cloud Identity as a Service）LDAP认证建立SSL-VPN连接。

背景信息

某公司在美国（硅谷）地域创建了VPC，网段为192.168.0.0/16。因业务发展，出差员工需要使用客户端访问云上VPC资源。

该公司拥有自己的AD（Active Directory）系统，为安全起见，公司希望出差的员工可以在通过公司AD系统的身份认证后，再访问云上的VPC资源。

如上图，您可以在云上创建VPN网关，配置SSL服务端并开启双因子认证，指定IDaaS实例进行LDAP认证。在员工通过SSL-VPN登录时，需要先到IDaaS系统中进行LDAP认证，LDAP认证会将员工的用户名和密码发送到公司的AD系统中去进行验证，并返回验证结果。只有在员工输入的账户信息验证通过后，VPN网关才会帮员工建立SSL-VPN连接，进而允许其访问云上VPC资源。

准备工作

在您执行以下操作前，请确保您已经满足以下条件：

- 您已经购买了标准版IDaaS实例。具体操作，请参见开通和试用流程。

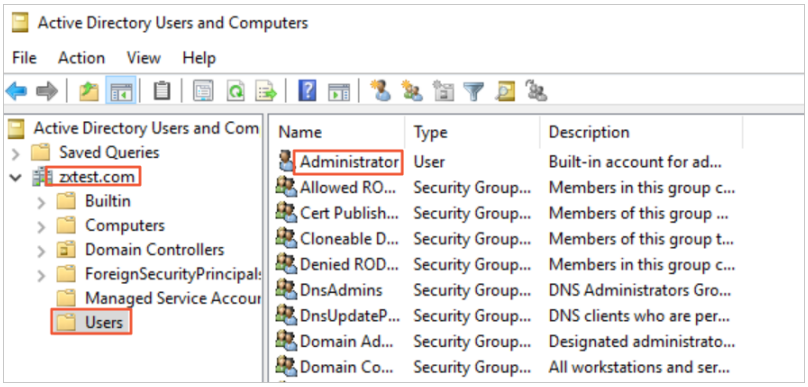
  本文示例中，已在新加坡地域购买了标准版IDaaS实例。
- 您已经创建了专有网络VPC（Virtual Private Cloud）。更多信息，请参见创建和管理专有网络。

  本文示例中，已在美国（硅谷）地域创建了VPC，VPC的网段为192.168.0.0/16。其中，ECS使用网段为192.168.0.0/24。
- 您已知您AD系统所在服务器（本文也称作LDAP服务器）的公网IP地址和服务端口。

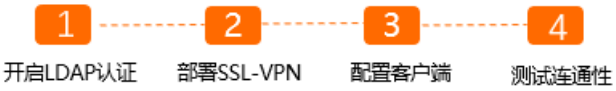
  本文示例中，AD系统部署在Windows Server 2019系统中，其公网IP地址为*47.XX.XX.8*，服务端口为*389*。
- 您已知您LDAP服务器的Base DN。

  本文示例中，LDAP服务器的Base DN为*dc=zxtest,dc=com*。
- 您已知您LDAP服务器管理员的DN、用户名和密码。

本文示例中，管理员账户名为Administrator，密码为1****2。其DN为*cn=Administrator,cn=Users,dc=zxtest,dc=com*，如下图所示。



配置步骤



步骤一：开启LDAP认证

在您建立SSL-VPN连接前，您需要在IDaaS实例中开启LDAP认证功能并同步账户数据，用于后续的身份验证。

1. 添加LDAP认证源。
   i. 登录IDaaS管理控制台。
   ii. 在左侧导航栏，单击**EIAM实例列表**。
   iii. 在**实例列表**页面，单击目标实例ID。
   iv. 在左侧导航栏，单击**认证源**。
   v. 在**认证源**页面的右上角，单击**添加认证源**。
   vi. 在**添加认证源**页面，找到LDAP图标，在**操作**列单击**添加认证源**。

vii. 在**添加认证源（LDAP）**面板，配置LDAP服务器信息，然后单击**提交**。

- **认证源ID**：由系统自动生成。
- **认证源名称**：输入自定义名称。
- **LDAP URL**：LDAP服务器连接地址，LDAP服务器即指您部署AD系统的服务器。地址填写格式例如：*ldap://127.0.0.1:389/*本示例输入*ldap://47.XX.XX.8:389/*。

  若主机的IP地址为IPv6地址格式，则地址需放在中括号（[]）内，例如：*ldap://[0000:0000:0000:0000:0000:0000:0000:0001]:389/*。

  > **说明** IDaaS目前只支持公网访问，LDAP服务器需要提供公网地址，并开启389端口。您可以在您LDAP服务器的安全组策略中设置只允许IDaaS的公网IP可以访问LDAP服务器，关于IDaaS公网IP地址信息，请提交工单至阿里云IDaaS团队咨询。

- **LDAP Base**：LDAP服务器Base DN。本示例输入*dc=zxtest,dc=com*。
- **LDAP账户**：LDAP服务器管理账户DN。本示例输入*cn=Administrator,cn=Users,dc=zxtest,dc=com*。
- **LDAP账户密码**：LDAP服务器管理账户密码。
- **过滤条件**：查询用户名的过滤条件。本示例输入*(sAMAccountName=$username$)*。

  具体匹配规则，请参见LDAP官方文档LDAP Filters。其中$username$为IDaaS系统用户名参数，为固定值。

更多参数说明，请参见LDAP认证登录。

viii. 在**认证源**页面，找到目标认证源，在其**状态**列单击 图标，然后在弹出的对话框中，单击**确定**，开启LDAP认证源。

2. LDAP账户同步配置，将LDAP服务器中的账户数据导入到IDaaS系统中。
   i. 在左侧导航栏，单击**机构及组**。
   ii. 在**机构及组**页面的右上角，单击**配置LDAP**。在**LDAP配置**面板，单击**新建配置**。

iii. 在**LDAP配置**面板的**服务器链接**页签下，配置以下信息，然后单击**保存**。

- **AD/LDAP名称**：输入自定义名称。
- **服务器地址**：输入您LDAP服务器的公网IP地址。本示例输入*47.XX.XX.8*。
- **端口号**：输入您LDAP服务器提供服务的端口号。本示例输入*389*。
- **Base DN**：输入要同步账户的节点DN。本示例输入*dc=zxtest,dc=com*。

> **说明** 此项在添加完成后不可更改，因为在IDaaS系统与LDAP（或AD）服务器进行同步数据时，如果Base DN发生改变会使双方组织机构目录无法对应而导致数据同步失败，想要同步不同目录的数据建议添加多个LDAP配置来完成。

- **管理员DN**：请输入管理员账户DN。本示例输入*cn=Administrator,cn=Users,dc=zxtest,dc=com*。
- **密码**：输入管理员账户的密码。
- **类型选择**：选择您LDAP服务器的类型。本示例选择**Windows AD**。
- **所属OU节点**：账户数据导入IDaaS系统中组织机构的节点位置，若不选择，则导入到根OU下。本示例保持默认值。
- **LDAP同步至本系统**：启用该项后，可以手动从LDAP服务器同步数据到IDaaS系统。本示例选择**启用**。
- **本系统同步至LDAP**：启用该项后，可以从IDaaS系统同步数据到LDAP服务器。本示例选择**启用**。

在您完成上述配置后，您可以单击**测试连接**来测试服务器的连通性。如果测试失败，请检查网络连通性，以及配置的连接参数是否正确。

iv. 在**LDAP配置**面板的**字段匹配规则**页签下，配置以下信息，然后单击**保存**。

字段匹配规则为IDaaS系统的字段与LDAP服务器中属性的对应匹配规则，例如LDAP服务器中的cn字段对应为IDaaS系统中的用户名。

- **用户名**：本示例输入cn 。

> **说明** 如果您AD系统中的账户的cn字段值为中文，则该账户无法拉取到IDaaS系统。建议您使用sAMAccountName字段。

- **外部ID**：Windows AD为objectGUID, OpenLdap为uid。本示例输入objectGUID 。
- **密码属性**：Windows AD为unicodePwd, OpenLdap为userPassword。本示例输入unicodePwd 。
- **用户唯一标识**：Windows AD为DistinguishedName, OpenLdap为EntryDN。本示例输入DistinguishedName 。
- **邮箱**：本示例输入mail 。

更多信息，请参见LDAP账户同步配置。

v. 在**机构及组**页面，选择**导入 > LDAP > 组织结构**。

vi. 在**LDAP列表**面板，找到目标LDAP，单击**导入**，在弹出的对话框中，单击**确定**。在**组织机构临时数据**面板确认组织机构信息，单击**确定导入**。

vii. 在当前页面的**组织架构**区域，选择目标组织机构，在组织机构的详情区域，选择**导入 > LDAP > 账户**。

viii. 在**LDAP列表**面板，找到目标LDAP，单击**导入**，在弹出的对话框中，单击**确定**。在**账户临时数据LDAP列表**面板中确认账户信息，单击**确定导入**，实现LDAP服务器账户信息同步到IDaaS系统。

3. 开启云产品LDAP认证。
   i. 在左侧导航栏，选择**设置 > 安全设置**。
   ii. 在**安全设置**页面，单击**云产品AD认证**页签。
   iii. 选择刚刚创建的LDAP认证源，启用该功能并单击**保存设置**。

步骤二：部署SSL-VPN

在开启LDAP认证后，您可以开始部署SSL-VPN，并开启SSL-VPN的双因子认证功能，关联已部署好的IDaaS实例，实现通过LDAP认证建立SSL-VPN连接。

1. 创建VPN网关。
   i. 登录VPN网关管理控制台。
   ii. 在左侧导航栏，选择**VPN > VPN网关**。
   iii. 在**VPN网关**页面，单击**创建VPN网关**。

iv. 在VPN网关的购买页面，根据以下信息配置VPN网关，然后单击**立即购买**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。 本示例选择**美国（硅谷）**。

  > **说明** 确保已创建VPC的地域和VPN网关的地域相同。

- **网关类型**：选择要创建的VPN网关类型。本示例选择**普通型**。
- **VPC**： 选择要连接的VPC。
- **指定交换机**：是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。

  如果您选择了**是**，您还需要指定具体的**虚拟交换机**。
- **带宽规格**：选择VPN网关的带宽规格，带宽规格是VPN网关所具备的公网带宽。本示例选择**10 Mbps**。
- **IPsec-VPN**： 选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以将本地数据中心与VPC或不同的VPC之间进行连接。本示例选择**关闭**。
- **SSL-VPN**： 选择开启或关闭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VPC。本示例选择**开启**。
- **SSL连接数**： 选择您需要同时连接的客户端最大规格。 本示例选择**5**。

  > **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。

2. 创建SSL服务端。

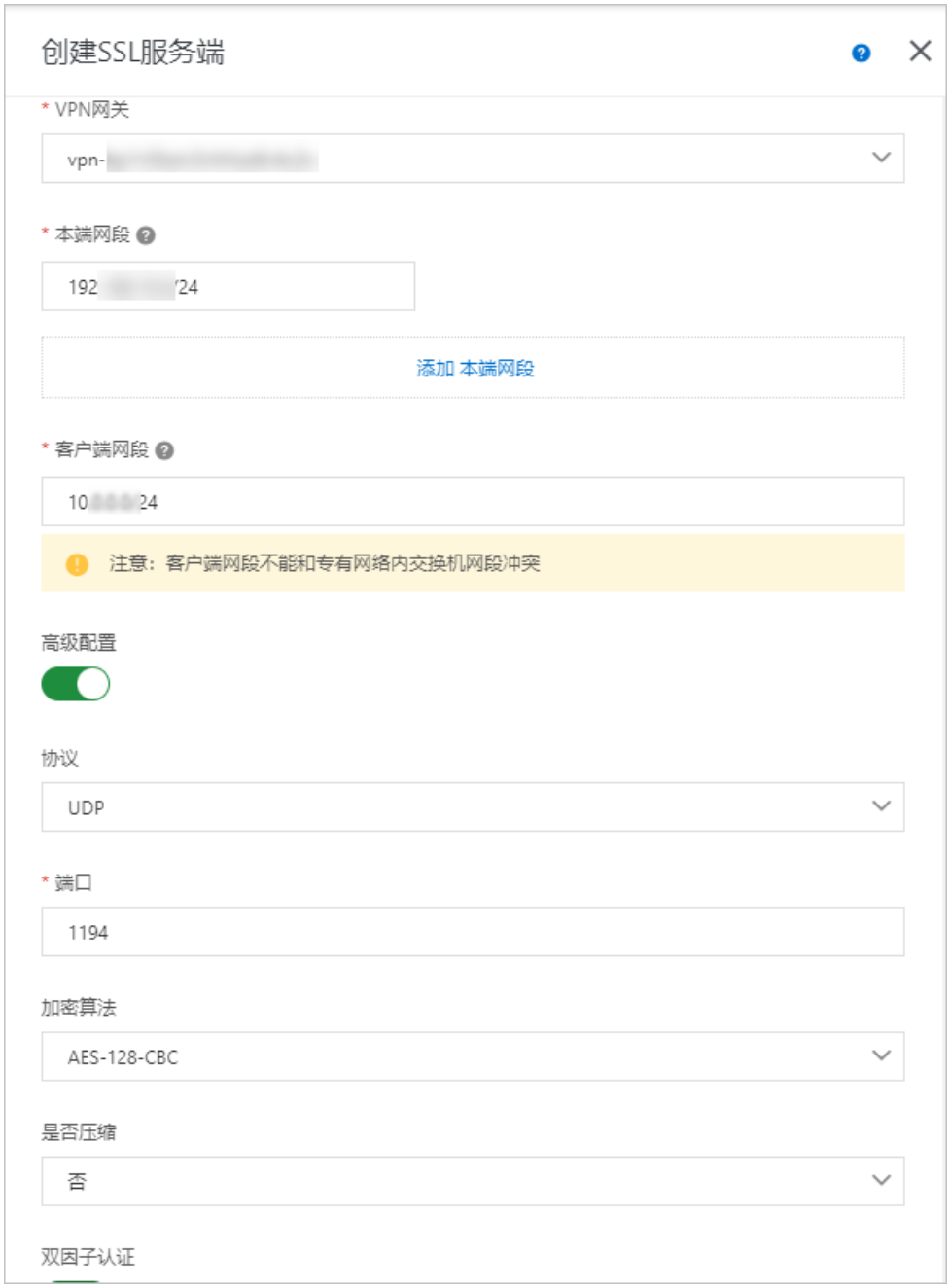
i. 在左侧导航栏，选择**VPN > SSL服务端**。

ii. 在顶部菜单栏处，选择SSL服务端的地域。

本示例选择**美国（硅谷）**。

iii. 在**SSL服务端**页面，单击**创建SSL服务端**。

iv. 在**创建SSL服务端**面板，根据以下信息配置SSL服务端，然后单击**确定**。



- **名称**：输入SSL服务端的名称。

  长度为2~128个字符，以英文大小写字母或中文开头，可包含数字、下划线（_）和短划线（-）。
- **VPN网关**：选择刚刚创建的VPN网关。
- **本端网段**：以CIDR地址块的形式输入客户端通过SSL-VPN连接要访问的网段。本示例输入**192.168.0.0/24**。
- **客户端网段**：以CIDR地址块的形式输入客户端连接服务端时使用的网段。本示例输入**10.0.0.0/24**。

- **高级配置**：打开高级配置，并完成以下配置。
  - **协议**：选择SSL连接使用的协议，支持UDP和TCP。本示例使用默认配置**UDP**。
  - **端口**：SSL连接使用的端口。本示例使用默认配置**1194**。
  - **加密算法**：SSL连接使用的加密算法，支持AES-128-CBC、AES-192-CBC、AES-256-CBC。本示例使用默认配置**AES-128-CBC**。
  - **是否压缩**：是否对传输数据进行压缩处理。本示例使用默认配置**否**。
  - **双因子认证**：打开双因子认证，然后选择IDaaS实例。
    - **IDaaS 实例所在地域**：IDaaS实例所在地域。本示例选择**新加坡**。
    - **IDaaS实例**：选择目标IDaaS实例。

> **说明** 如果您是首次使用双因子认证功能，请先完成授权后再创建SSL服务端。

3. 创建并下载SSL客户端证书。
   i. 在左侧导航栏，选择**VPN > SSL客户端**。
   ii. 在顶部菜单栏处，选择SSL客户端的地域。

   本示例选择**美国（硅谷）**。
   iii. 在**SSL客户端**页面，单击**创建SSL客户端证书**。
   iv. 在**创建SSL客户端证书**面板，根据以下信息配置SSL客户端证书，然后单击**确定**。
   - **名称**：输入SSL客户端证书的名称。

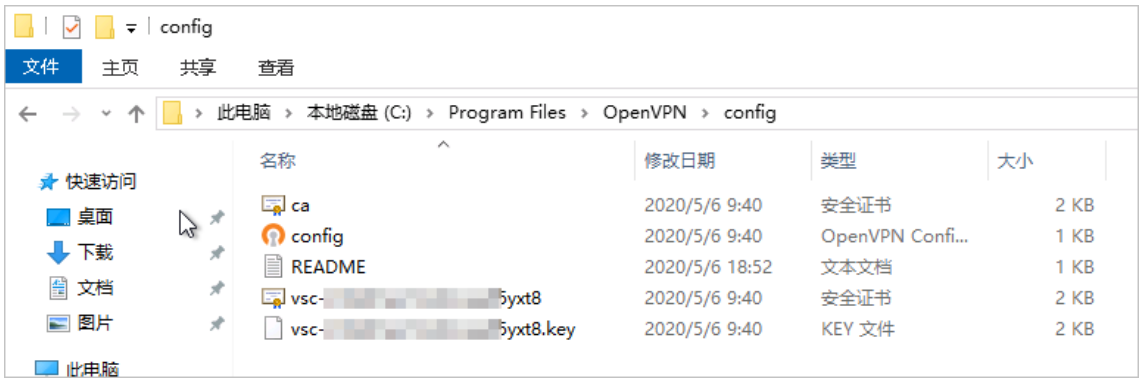
     长度为2~128个字符，以英文大小写字母或中文开头，可包含数字、下划线（_）和短划线（-）。
   - **SSL服务端**：选择刚刚创建的SSL服务端。

   v. 在**SSL客户端**页面，找到已创建的SSL客户端证书，然后在**操作**列单击**下载**。

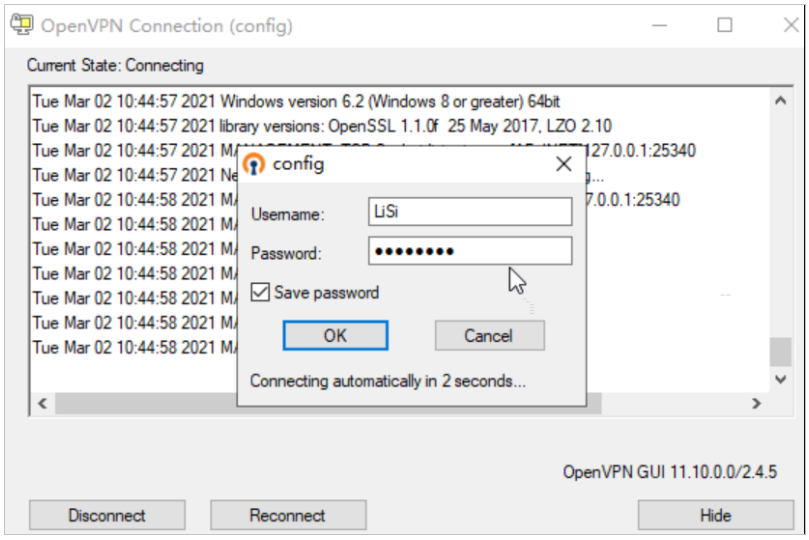
   SSL客户端证书会下载到您本地。

步骤三：配置客户端

- 如果您使用的是Windows客户端，请参见以下步骤配置客户端。
  i. 将已经下载的SSL客户端证书解压拷贝到*OpenVPN\conf*目录。本示例将证书解压拷贝到*C:\Program Files\OpenVPN\config*目录，请您根据安装路径将证书解压拷贝到实际的目录。



  ii. 启动Openvpn客户端软件，并完成用户名和密码认证。



- 如果您使用的是Linux客户端，请参见以下步骤配置客户端。
  i. 执行以下命令安装OpenVPN客户端。

  ```
  yum install -y openvpn
  ```

  ii. 将已经下载的SSL客户端证书解压拷贝到*/etc/openvpn/conf/*目录。
  iii. 执行以下命令启动OpenVPN客户端软件，并完成用户名密码验证。

  ```
  openvpn --config /etc/openvpn/conf/config.ovpn --daemon
  ```

  ```
  [root@iZ8ps^ conf]# openvpn --config /etc/openvpn/conf/config.ovpn --daemon
  Enter Auth Username: dgtt
  Enter Auth Password: **********
  ```

- 如果您使用的是Mac客户端，请参见以下步骤配置客户端。
  i. 执行以下命令安装OpenVPN客户端。

  ```
  brew install openvpn
  ```

  > **说明** 如果尚未安装homebrew，请先安装homebrew。

  ii. 执行以下命令删除默认配置文件。

  ```
  rm /usr/local/etc/openvpn/*
  ```

  iii. 执行以下命令将文件拷贝到配置目录。

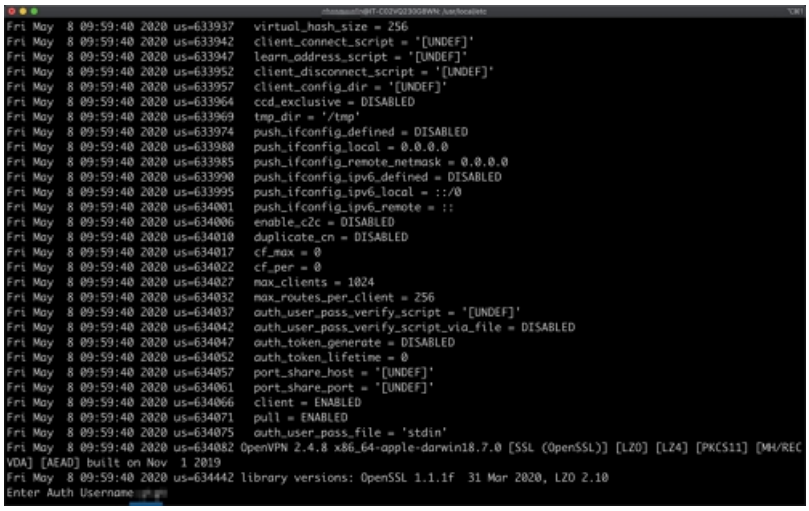
  ```
  cp cert_location /usr/local/etc/openvpn/
  ```

  `cert_location` 是SSL客户端证书的下载路径，例如： */Users/example/Downloads/certs.zip*。
  iv. 执行以下命令将已经下载的证书解压拷贝到配置目录。

  ```
  cd  /usr/local/etc/openvpn
  unzip /usr/local/etc/openvpn/certs.zip
  ```

  v. 执行以下命令发起连接，并完成用户名和密码验证。

```
sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
```



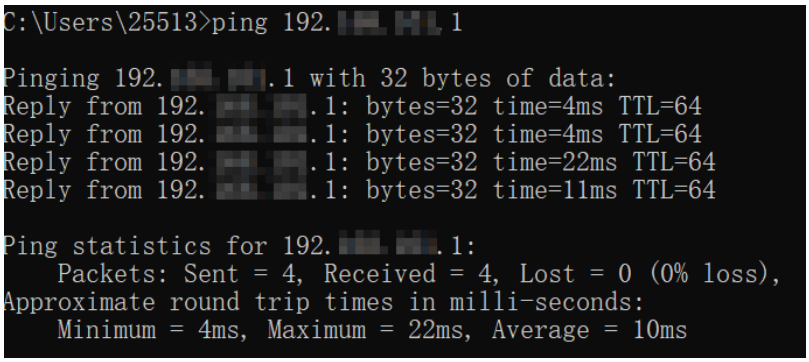
步骤四：测试连通性

配置完成后，您可以通过 `ping` 命令测试与云上VPC的连通性。以下内容以Windows客户端为例，为您展示如何测试与云上VPC的连通性。

1. 打开Windows客户端的cmd窗口。
2. 通过 `ping` 命令 `ping` VPC下的ECS实例的IP地址，验证通信是否正常。

> **说明** 请确保测试的ECS实例的安全组规则允许Windows客户端远程连接。更多信息，请参见安全组应用案例ECS安全组配置操作指南。

经测试，Windows客户端可以正常访问ECS实例。



5.IPsec-VPN连接高可用

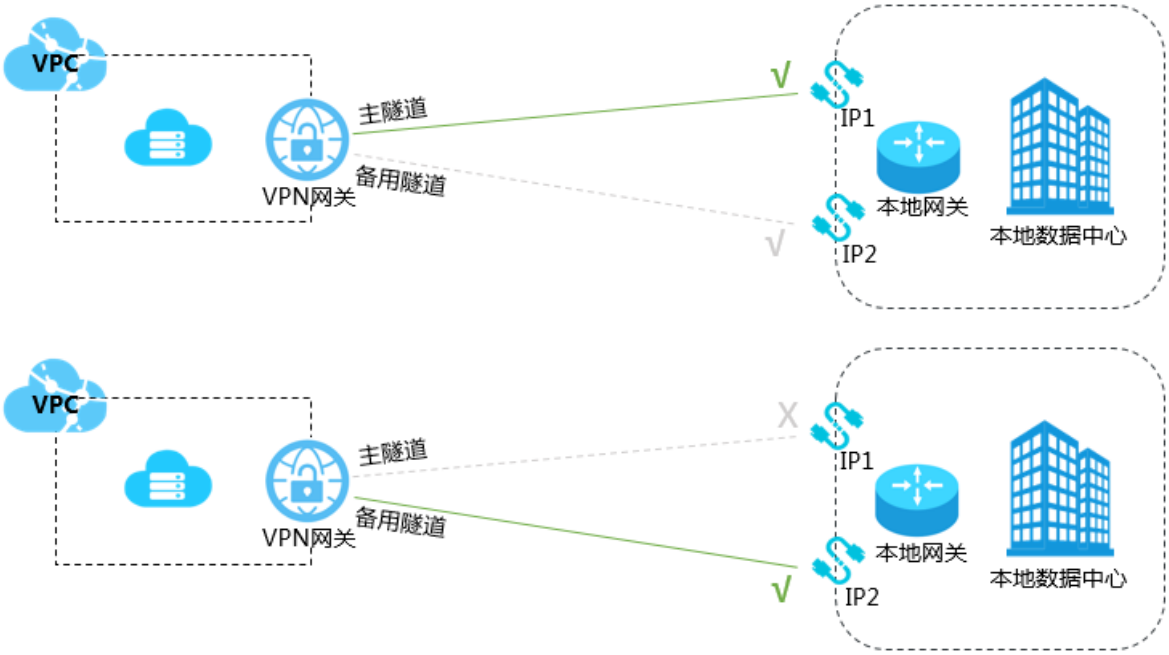
5.1. 高可用-双IPsec隧道

如果您的本地网关有双公网IP，您可以分别与VPN网关建立IPsec隧道，以实现主备隧道冗余。

方案概述

本地网关拥有两条Internet链路，每条Internet链路对应一个公网IP。VPN网关分别与本地网关的两个公网IP建立IPsec连接并开启健康检查，通过设置不同的路由权重区分主备路由。主路由关联的IPsec隧道为主隧道，备用路由关联的IPsec隧道为备用隧道。

- 当基于IP1的Internet链路正常时，本地数据中心与VPC之间的所有流量只通过主隧道转发。
- 当基于IP1的Internet链路异常时，本地数据中心与VPC之间的所有流量切换到备用隧道。



前提条件

在开始之前，确保您的环境满足以下条件：

- 您已经注册了阿里云账号。如未注册，请先完成账号注册。
- 确保本地数据中心的网关设备支持IKEv1和IKEv2协议，只要支持这两种协议的本地网关设备均可以和云上VPN网关互连。
- 本地数据中心的网关设备已经配置了静态公网IP。
- 本地数据中心和VPC互通的网段没有重叠。
- 您已经了解VPC中的ECS实例所应用的安全组规则，并确保安全组规则允许本地数据中心的网关设备访问云上资源。具体操作，请参见查询安全组规则和添加安全组规则。

步骤一：创建VPN网关

1.
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网关所属的地域。

     > **说明** 确保VPC的地域和VPN网关的地域相同。

   - **网关类型**：选择要创建的VPN网关类型。本示例选择**普通型**。
   - **VPC**：选择要连接的VPC。
   - **指定交换机**：是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。

     如果您选择了**是**，您还需要指定具体的**虚拟交换机**。
   - **带宽规格**：选择VPN网关的公网带宽峰值。单位为Mbps。
   - **IPsec-VPN**：选择是否开启IPsec-VPN功能。本示例选择**开启**。
   - **SSL-VPN**：选择是否开启SSL-VPN功能。本示例选择**关闭**。
   - **计费周期**：选择购买时长。关于计费的更多信息， 请参见计费说明。
4. 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1~5分钟左右会变成**正常**状态。**正常**状态表明VPN网关已经完成了初始化，可以正常使用。

步骤二：创建用户网关

完成以下操作，创建两个用户网关，将本地网关的两个公网IP地址注册到用户网关中用于建立IPsec连接。

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. 根据以下信息配置用户网关：
   - **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。
   - **描述**：输入用户网关的描述信息。
5. 在**创建用户网关**页面，单击**+添加** 添加另一用户网关。

步骤三：创建IPsec连接

完成以下操作，创建两个IPsec连接，将VPN网关分别和两个用户网关连接起来，并开启健康检查。

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，单击**创建IPsec连接**。
4. 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。
   - **对端网段**：输入本地数据中心的网段。
   - **是否立即生效**：选择是否立即协商。
     - 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，该值必须与用于本地网关设备的值匹配。
   - **健康检查**：开启健康检查并输入目的IP、源IP、重试间隔和重试次数。

     其他选项使用默认配置。
5. 重复以上操作，创建与另一用户网关的IPsec连接。

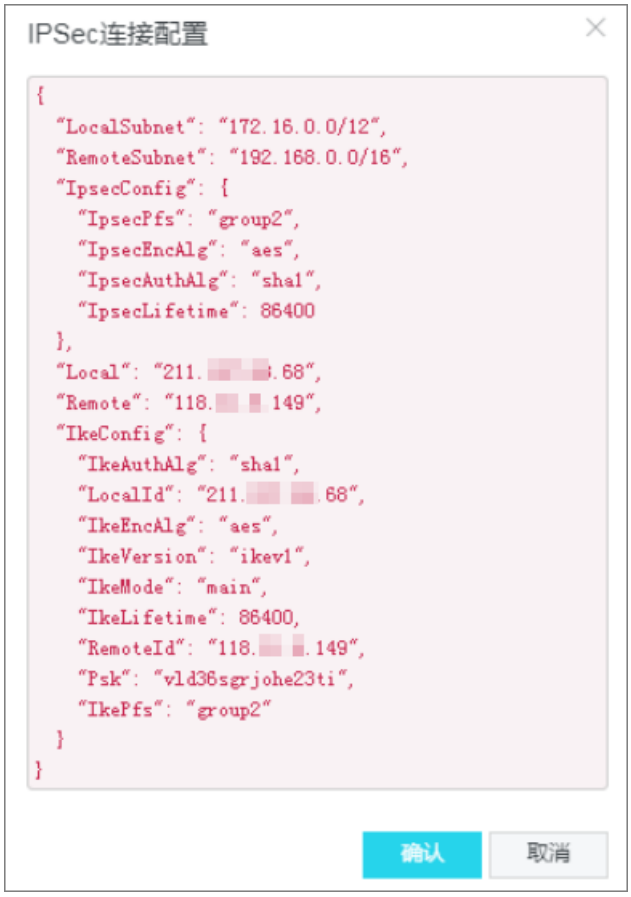
步骤四：在本地网关设备中加载VPN配置

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. 找到目标IPsec连接，然后单击**下载配置**。

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。具体操作，请参见本地网关配置。

   下载配置中的RemoteSubnet和LocalSubnet与创建IPsec连接时的本端网段和对端网段正好是相反的。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，RemoteSubnet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IPsec-VPN网关路由。

1. 在左侧导航栏，单击**VPN > VPN网关**。
2. 在**VPN网关**页面，选择VPN网关的地域。
3. 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. 根据以下信息配置两条目的路由，然后单击**确定**。
   - **目标网段**：输入本地网关的私网网段。
   - **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。
   - **权重**：选择权重值。

   > **注意** 通过设置不同的路由权重来区分主备路由，两条目的路由的权重不能同时设置为100，也不能同时设置为0。

   本示例目的路由如下表：

目标网段	下一跳	发布到VPC	权重
本地网关的私网网段	IPsec连接实例1	是	100

目标网段	下一跳	发布到VPC	权重
本地网关的私网网段	IPsec连接实例2	是	0

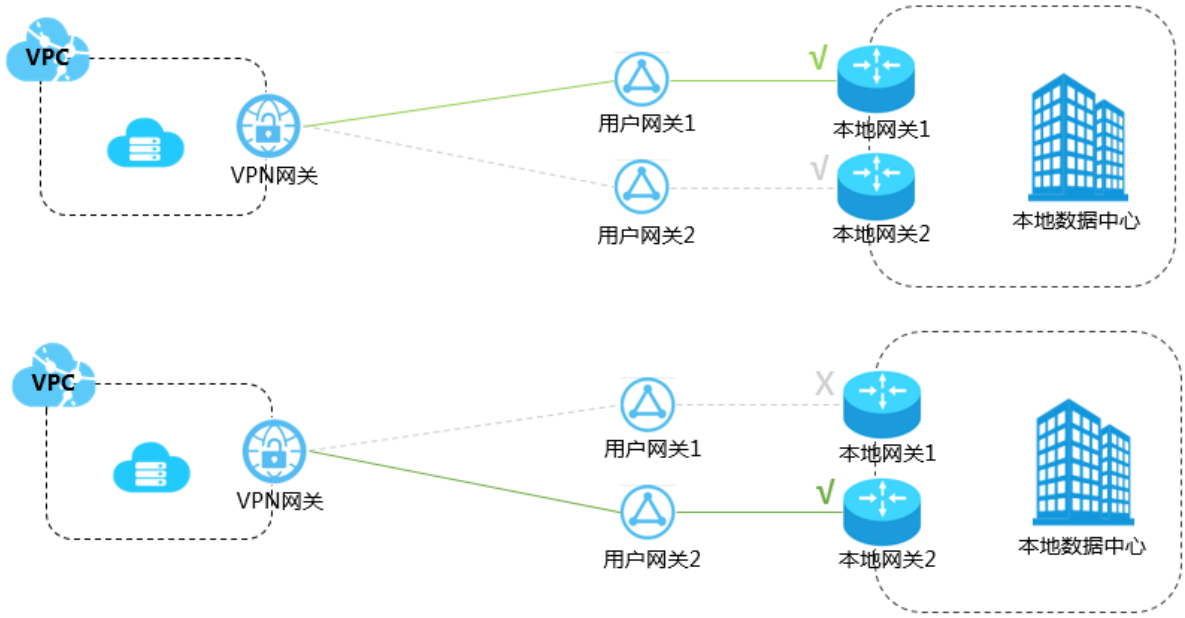
5.2. 高可用-双用户网关

您可以在本地部署两个CPE网关，VPN网关分别与两个用户网关建立IPsec VPN连接，以实现多VPN连接冗余。

方案概述

阿里云侧部署一个VPN网关，用户侧部署两个用户网关。

两个用户网关同时连接一个阿里云VPN网关，每个用户网关与VPN网关建立一条IPsec隧道，并为IPsec连接配置健康检查，两条IPsec隧道均为协商成功状态。当健康检查检测用户网关不可用时，路由自动切换到另外一个用户网关。



前提条件

在开始之前，确保您的环境满足以下条件：

- 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，例如华三、华为、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。

步骤一：创建VPN网关

1.
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网关所属的地域。

  > **说明** 确保VPC的地域和VPN网关的地域相同。

- **网关类型**：选择要创建的VPN网关类型。本示例选择**普通型**。
- **VPC**：选择要连接的VPC。
- **指定交换机**：是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。

  如果您选择了**是**，您还需要指定具体的**虚拟交换机**。
- **带宽规格**：选择VPN网关的公网带宽峰值。单位为Mbps。
- **IPsec-VPN**：选择是否开启IPsec-VPN功能。本示例选择**开启**。
- **SSL-VPN**：选择是否开启SSL-VPN功能。本示例选择**关闭**。
- **计费周期**：选择购买时长。关于计费的更多信息， 请参见计费说明。

4. 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1~5分钟左右会变成**正常**状态。**正常**状态表明VPN网关已经完成了初始化，可以正常使用。

步骤二：创建用户网关

完成以下操作，创建两个用户网关，将本地网关设备的公网IP地址注册到用户网关中用于建立IPsec连接。

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**页面，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。
   - **描述**：输入用户网关的描述信息。
   - **+添加**：添加另一用户网关。

步骤三：创建IPsec连接

完成以下操作，创建两个IPsec连接，将VPN网关分别和两个用户网关连接起来，并开启健康检查。

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，单击**创建IPsec连接**。
4. 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。
   - **对端网段**：输入本地数据中心的网段。

- **是否立即生效**：选择是否立即协商。
  - 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，该值必须与用于本地网关设备的值匹配。
- **健康检查**：开启健康检查并输入目的IP、源IP、重试间隔和重试次数。

  其他选项使用默认配置。

5. 重复以上操作，创建与另一用户网关的IPsec连接。

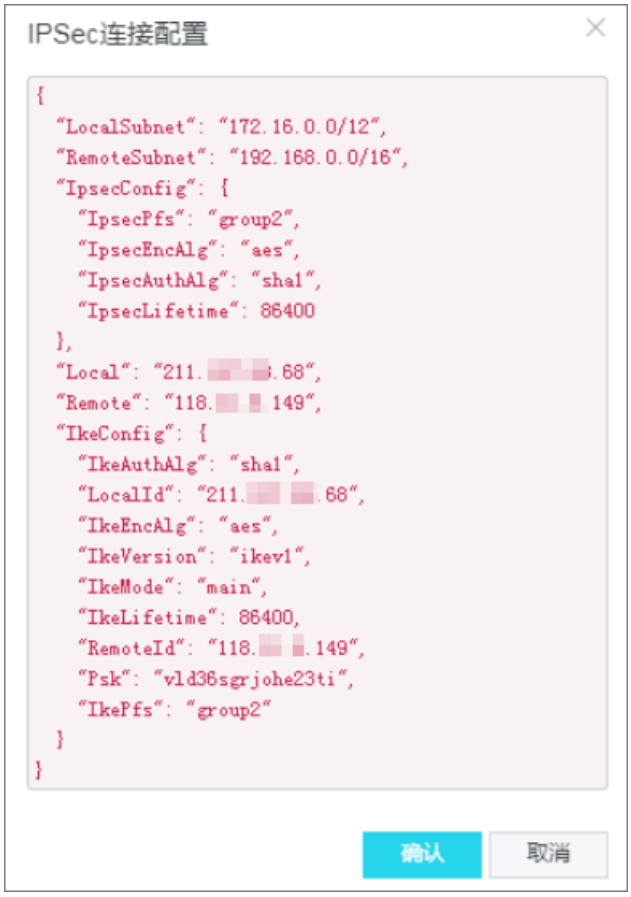
步骤四：在本地网关设备中加载VPN配置

完成以下操作，分别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. 找到目标IPsec连接，然后单击**下载配置**。

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。具体操作，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正好是相反的。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IPsec-VPN网关路由。

1. 在左侧导航栏，单击**VPN > VPN网关**。
2. 在**VPN网关**页面，选择VPN网关的地域。
3. 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. 根据以下信息配置两条目的路由，然后单击**确定**。
   - **目标网段**：输入本地网关的私网网段。
   - **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。
   - **权重**：选择权重值。

   > **注意** 通过设置不同的路由权重来区分主备路由，两条目的路由的权重不能同时设置为100，也不能同时设置为0。

   本示例目的路由如下表：

目标网段	下一跳	发布到VPC	权重
本地网关的私网网段	IPsec连接实例1	是	100

目标网段	下一跳	发布到VPC	权重
本地网关的私网网段	IPsec连接实例2	是	0

6.IPsec-VPN配合云企业网搭建高速全球网络

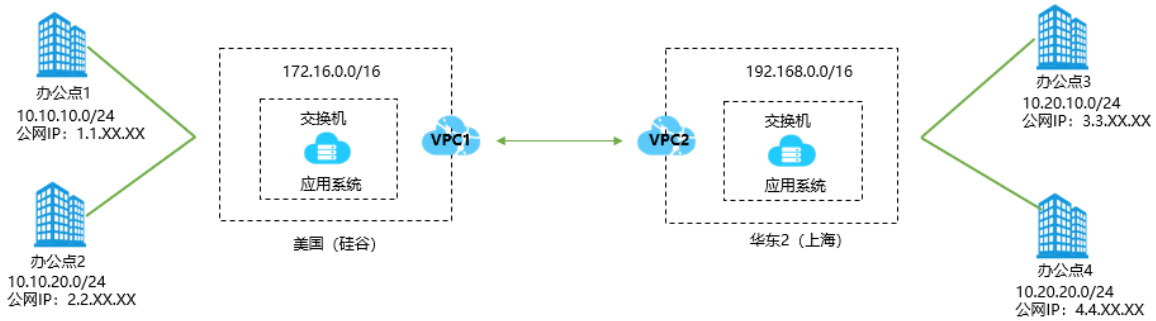
本教程介绍如何组合使用VPN网关和云企业网，实现客户IDC上云，并构建高质量、低成本的跨国企业网络。

前提条件

开始操作前，请确保满足以下条件：

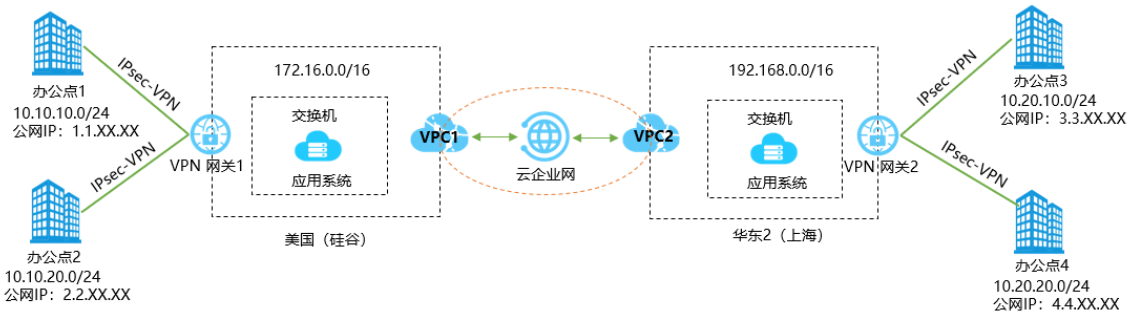
- 创建了专有网络，并部署了相关应用。具体操作，请参见创建和管理专有网络。
- 各办公点已经部署了本地网关设备，且配置了一个静态公网IP。
- 创建了云企业网实例。具体操作，请参见创建云企业网实例。
- 购买了云企业网带宽包并设置了跨地域互通带宽。具体操作，请参见使用带宽包和跨地域互通带宽。
- 需要互通的各网段不能冲突。

背景信息



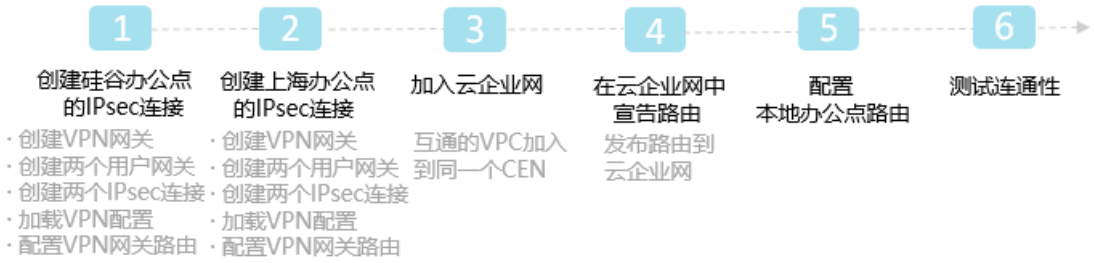
某跨国公司在美国硅谷和中国上海均有两个办公点，且该跨国公司在美国（硅谷）和华东2（上海）地域分别创建了VPC1和VPC2，并在两个VPC中部署了应用系统。因业务发展，需要美国硅谷的两个办公点、中国上海的两个办公点、VPC1、VPC2全互通。各网络的网段如下表。

网络	网段
美国（硅谷）办公点1	10.10.10.0/24
美国（硅谷）办公点2	10.10.20.0/24
美国（硅谷）VPC1	172.16.0.0/16
华东2（上海）办公点3	10.20.10.0/24
华东2（上海）办公点4	10.20.20.0/24
华东2（上海）VPC2	192.168.0.0/16



如上图，您可以通过VPN网关1将美国硅谷的办公点1、办公点2与VPC1连接起来，通过VPN网关2将上海的办公点3、办公点4与VPC2连接起来，然后再将VPC1和VPC2加载到同一云企业网中，实现全球网络全互通。

配置流程



步骤一：创建美国硅谷办公点的IPsec连接

完成以下操作，创建美国硅谷办公点的IPsec连接，将办公点1、办公点2与VPC1连接起来。

1. 为美国（硅谷）地域的VPC创建一个VPN网关。

   VPN网关的参数如下：

   - **实例名称**：*VPN网关1*。
   - **地域和可用区**：**美国（硅谷）**。
   - **网关类型**：**普通型**。
   - **VPC**：选择**美国（硅谷）**地域的VPC。
   - **指定交换机**：**否**。
   - **带宽规格**：**5Mbps**。
   - **IPsec-VPN**：**开启**。
   - **SSL-VPN**：**关闭**。
   - **计费周期**：**1个月**。
   - **服务关联角色**：单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。

     > **说明** VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。

     若本配置项显示为**已创建**，则表示您的账号下已创建了该角色，无需重复创建。

具体操作，请参见创建和管理VPN网关实例。

2. 创建两个用户网关，将办公点1、办公点2网关设备的公网IP地址注册到用户网关中用于建立IPsec连接。

   办公点1用户网关的参数如下：

   - **名称**：*用户网关1*。
   - **IP地址**：输入本地办公点1网关设备的静态公网IP地址，本示例输入*1.1.XX.XX*。

   办公点2用户网关的参数如下：

   - **名称**：*用户网关2*。
   - **IP地址**：输入本地办公点2网关设备的静态公网IP地址，本示例输入*2.2.XX.XX*。

   具体操作，请参见创建用户网关。

3. 创建两个IPsec连接，将办公点1、办公点2网关设备与VPN网关连接起来。

   办公点1与VPN网关间的IPsec连接的配置如下：

   - **名称**：*IPsec连接1*。
   - **VPN网关**：选择美国（硅谷）地域VPC配置的VPN网关，本示例选择的VPN网关实例的名称为VPN网关1。
   - **用户网关**：选择待连接的用户网关，本示例选择用户网关1。
   - **路由模式**：选择**感兴趣流模式**。
   - **本端网段**：输入需要和本地办公点互连的VPC侧的网段，本示例输入*172.16.0.0/16*。
   - **对端网段**：输入需要和VPC互连的本地办公点的网段，本示例输入*10.10.10.0/24*。
   - **立即生效**：选择是否立即协商，本示例选择**是**。
     - **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**：用于IPsec-VPN网关与用户网关之间的身份认证，本示例输入*123456*。

   其他选项使用默认配置。

   办公点2与VPN网关间的IPsec连接的配置如下：

   - **名称**：*IPsec连接2*。
   - **VPN网关**：选择美国（硅谷）地域VPC配置的VPN网关，本示例选择的VPN网关实例的名称为VPN网关1。
   - **用户网关**：选择待连接的用户网关，本示例选择用户网关2。
   - **路由模式**：选择**感兴趣流模式**。
   - **本端网段**：输入需要和本地办公点互连的VPC侧的网段，本示例输入*172.16.0.0/16*。
   - **对端网段**：输入需要和VPC互连的本地办公点的网段，本示例输入*10.10.20.0/24*。
   - **立即生效**：选择是否立即协商，本示例选择**是**。
     - **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**：用于IPsec-VPN网关与用户网关之间的身份认证，本示例输入*123456*。

   其他选项使用默认配置。

   具体操作，请参见创建IPsec连接。

4. 在本地办公点1和办公点2网关设备中加载VPN配置。

   具体操作，请参见本地网关配置。

5. 配置VPN网关路由。

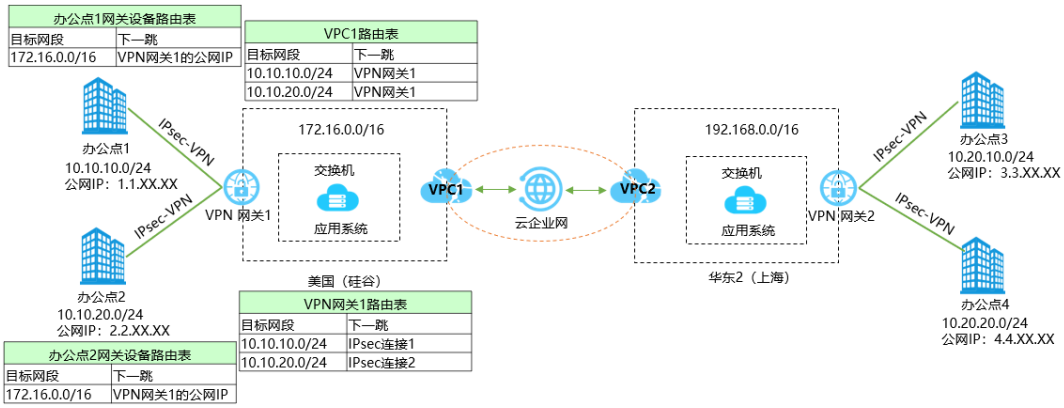
   VPN网关1指向办公点1的路由配置如下：

   - **目标网段**：输入要访问的私网网段，本示例输入*10.10.10.0/24*。
   - **下一跳类型**：选择IPsec连接。
   - **下一跳**：选择需要建立VPN连接的IPsec连接实例，本示例选择IPsec连接1。
   - **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**。
     - （推荐）**是**：将新添加的路由发布到VPC路由表。
     - **否**：不发布新添加的路由到VPC路由表。
   - **权重**：选择权重值，本示例选择**0**。

   VPN网关1指向办公点2的路由配置如下：

   - **目标网段**：输入要访问的私网网段，本示例输入*10.10.10.0/24*。
   - **下一跳类型**：选择IPsec连接。
   - **下一跳**：选择需要建立VPN连接的IPsec连接实例，本示例选择IPsec连接2。
   - **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**。
     - （推荐）**是**：将新添加的路由发布到VPC路由表。
     - **否**：不发布新添加的路由到VPC路由表。
   - **权重**：选择权重值，本示例选择**0**。

   美国硅谷办公点的IPsec连接后，办公点1、办公点2、VPN网关1、VPC1的路由表如下图。



步骤二：创建上海办公点的IPsec连接

完成以下操作，创建上海办公点的IPsec连接，将办公点3、办公点4与VPC2连接起来。

1. 为华东2（上海）地域的VPC创建一个VPN网关。

   VPN网关的参数如下：

   - **实例名称**：*VPN网关2*。
   - **地域和可用区**：**美国（硅谷）**。

- **网关类型**：**普通型**。
- **VPC**：选择**美国（硅谷）**地域的VPC。
- **指定交换机**：**否**。
- **带宽规格**：**5Mbps**。
- **IPsec-VPN**：**开启**。
- **SSL-VPN**：**关闭**。
- **计费周期**：**1个月**。
- **服务关联角色**：单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。

  > **说明** VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。

  若本配置项显示为**已创建**，则表示您的账号下已创建了该角色，无需重复创建。

具体操作，请参见创建和管理VPN网关实例。

2. 创建两个用户网关，将办公点3、办公点4网关设备的公网IP地址注册到用户网关中用于建立IPsec连接。

   办公点3用户网关的参数如下：

   - **名称**：*用户网关3*。
   - **IP地址**：输入本地办公点3网关设备的静态公网IP地址，本示例输入3.3.XX.XX。

   办公点4用户网关的参数如下：

   - **名称**：*用户网关4*。
   - **IP地址**：输入本地办公点4网关设备的静态公网IP地址，本示例输入4.4.XX.XX。

   具体操作，请参见创建用户网关。

3. 创建两个IPsec连接，将办公点3、办公点4网关设备与VPN网关连接起来。

   办公点3与VPN网关间的IPsec连接的配置如下：

   - **名称**：*IPsec连接3*。
   - **VPN网关**：选择华东2（上海）地域VPC配置的VPN网关，本示例选择的VPN网关实例的名称为VPN网关2。
   - **用户网关**：选择待连接的用户网关，本示例选择用户网关3。
   - **路由模式**：选择**感兴趣流模式**。
   - **本端网段**：输入需要和本地办公点互连的VPC侧的网段，本示例输入*192.168.0.0/16*。
   - **对端网段**：输入需要和VPC互连的本地办公点的网段，本示例输入*10.20.10.0/24*。
   - **立即生效**：选择是否立即协商，本示例选择**是**。
     - **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**：用于IPsec-VPN网关与用户网关之间的身份认证，本示例输入*123456*。

   其他选项使用默认配置。

   办公点4与VPN网关间的IPsec连接的配置如下：

   - **名称**：*IPsec连接4*。

- **VPN网关**：选择华东2（上海）地域VPC配置的VPN网关，本示例选择的VPN网关实例的名称为VPN网关2。
- **用户网关**：选择待连接的用户网关，本示例选择用户网关4。
- **路由模式**：选择感兴趣流模式
- **本端网段**：输入需要和本地办公点互连的VPC侧的网段，本示例输入*192.168.0.0/16*。
- **对端网段**：输入需要和VPC互连的本地办公点的网段，本示例输入*10.20.20.0/24*。
- **立即生效**：选择是否立即协商，本示例选择**是**。
  - **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**：用于IPsec-VPN网关与用户网关之间的身份认证，本示例输入*654321*。

其他选项使用默认配置。

具体操作，请参见创建IPsec连接。

4. 在本地办公点3和办公点4网关设备中加载VPN配置。

   具体操作，请参见本地网关配置。

5. 配置VPN网关路由。

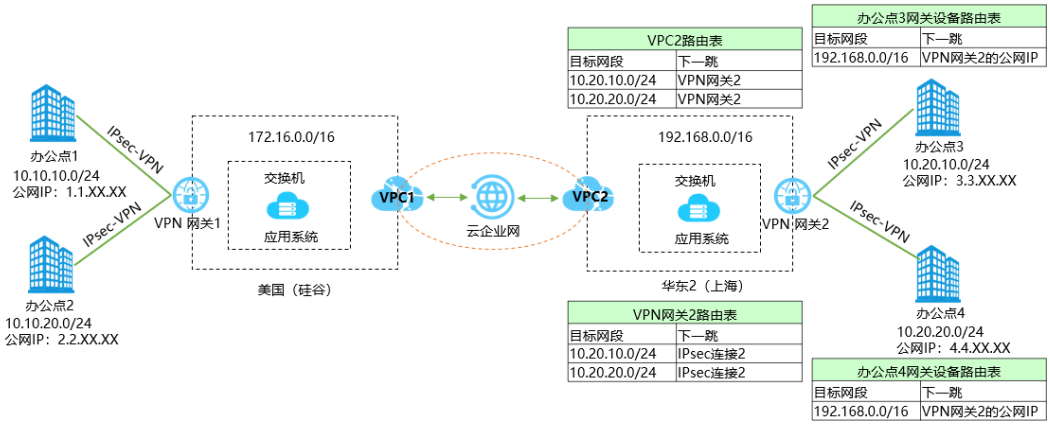
   VPN网关2指向办公点3的路由配置如下：

   - **目标网段**：输入要访问的私网网段，本示例输入*10.20.10.0/24*。
   - **下一跳类型**：选择IPsec连接。
   - **下一跳**：选择需要建立VPN连接的IPsec连接实例，本示例选择IPsec连接3。
   - **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**。
     - （推荐）**是**：将新添加的路由发布到VPC路由表。
     - **否**：不发布新添加的路由到VPC路由表。
   - **权重**：选择权重值，本示例选择**0**。

   VPN网关2指向办公点4的路由配置如下：

   - **目标网段**：输入要访问的私网网段，本示例输入*10.20.20.0/24*。
   - **下一跳类型**：选择IPsec连接。
   - **下一跳**：选择需要建立VPN连接的IPsec连接实例，本示例选择IPsec连接4。
   - **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**。
     - （推荐）**是**：将新添加的路由发布到VPC路由表。
     - **否**：不发布新添加的路由到VPC路由表。
   - **权重**：选择权重值，本示例选择**0**。

上海办公点的IPsec连接后，办公点3、办公点4、VPN网关2、VPC2的路由表如下图。



步骤三：加入云企业网

完成本地办公点上云后，您需要将要互通的VPC1和VPC2加入到同一个云企业网。

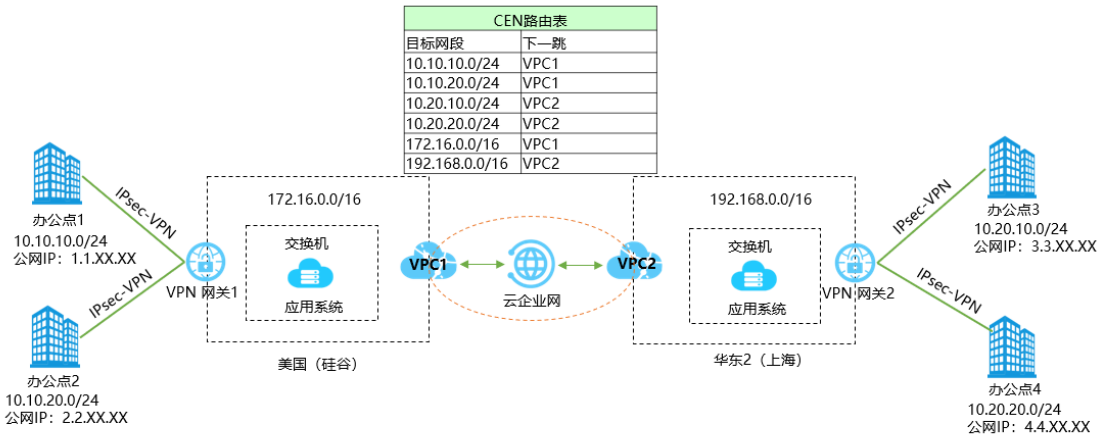
> **说明** 本教程使用云企业网的旧版控制台。关于如何进入旧版控制台，请参见旧版控制台使用说明。

1. 登录云企业网控制台。
2. 在**云企业网实例**页面，单击已创建的CEN实例ID。
3. 在**网络实例管理**页签，单击**加载网络实例**。
4. 单击**同账号**页签。
5. 根据以下信息加载网络实例，然后单击**确定**。
   - **实例类型**：选择**专有网络（VPC）**。
   - **地域**：选择**美国（硅谷）**。
   - **网络实例**：选择VPC1。
6. 根据上述步骤将VPC2加入到同一CEN实例。

步骤四：在云企业网中宣告路由

为了能够让云企业网内其他VPC学习到指向本地办公点的路由，需要在美国（硅谷）VPC和华东2（上海）VPC将指向VPN网关的路由发布到云企业网。具体操作，请参见发布路由至云企业网。

发布路由后，云企业网的路由表如下图。



步骤五：配置本地办公点路由

在CEN中宣告路由后，您需要在硅谷办公点网关设备配置指向上海办公点的路由，在上海办公点的网关设备配置指向硅谷办公点的路由。

示例仅供参考，不同厂商的设备可能会有所不同。

办公点	路由

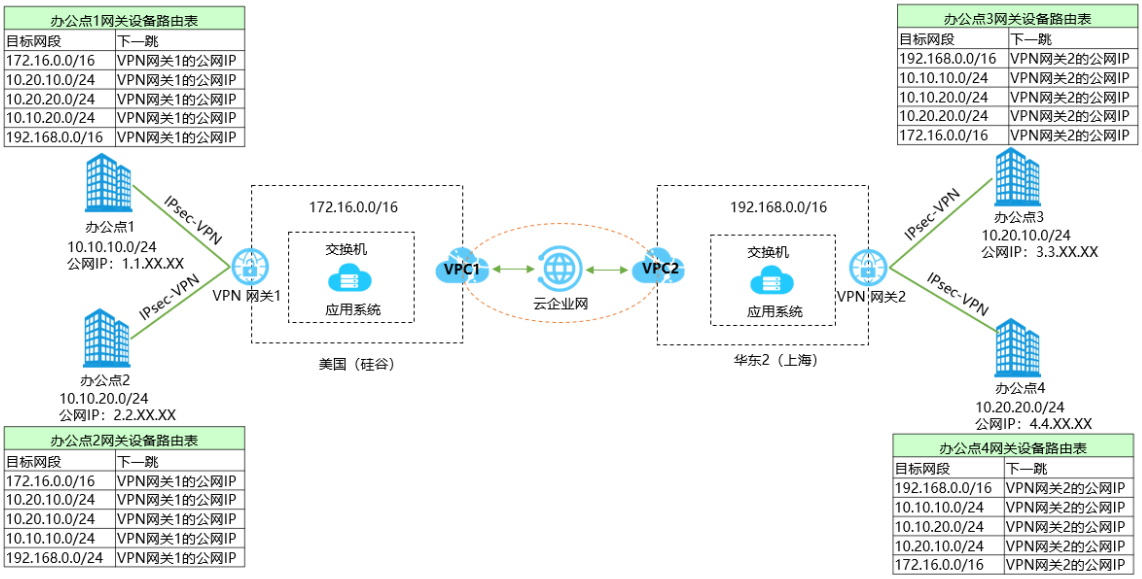
办公点1	`ip route 192.168.0.0/16 5.5.XX.XX`
	`ip route 10.20.10.0/24 5.5.XX.XX`
	`ip route 10.20.20.0/24 5.5.XX.XX`
	`ip route 10.10.20.0/24 5.5.XX.XX  #5.5.XX.XX为VPN网关1的公网IP`

办公点2	`ip route 192.168.0.0/16 5.5.XX.XX`
	`ip route 10.20.10.0/24 5.5.XX.XX`
	`ip route 10.20.20.0/24 5.5.XX.XX`
	`ip route 10.10.10.0/24 5.5.XX.XX  #5.5.XX.XX为VPN网关1的公网IP`

办公点3	`ip route 172.16.0.0/16 6.6.XX.XX`
	`ip route 10.10.10.0/24 6.6.XX.XX`
	`ip route 10.10.20.0/24 6.6.XX.XX`
	`ip route 10.20.20.0/24 6.6.XX.XX  #6.6.XX.XX为VPN网关2的公网IP`

办公点4	`ip route 172.16.0.0/16 6.6.XX.XX`
	`ip route 10.10.10.0/24 6.6.XX.XX`
	`ip route 10.10.20.0/24 6.6.XX.XX`
	`ip route 10.20.10.0/24 6.6.XX.XX  #6.6.XX.XX为VPN网关2的公网IP`

本地办公点的路由表如下图。



步骤六：测试连通性

本操作以在办公点1下的客户端访问办公点2、办公点3、办公点4下的客户端为例，测试本地各办公点间的连通性。

1. 在本地办公点1下，打开客户端的命令行窗口。
2. 执行 `ping` 命令，ping办公点2、办公点3、办公点4下客户端的IP地址，如果收到回复报文，表示连接成功。

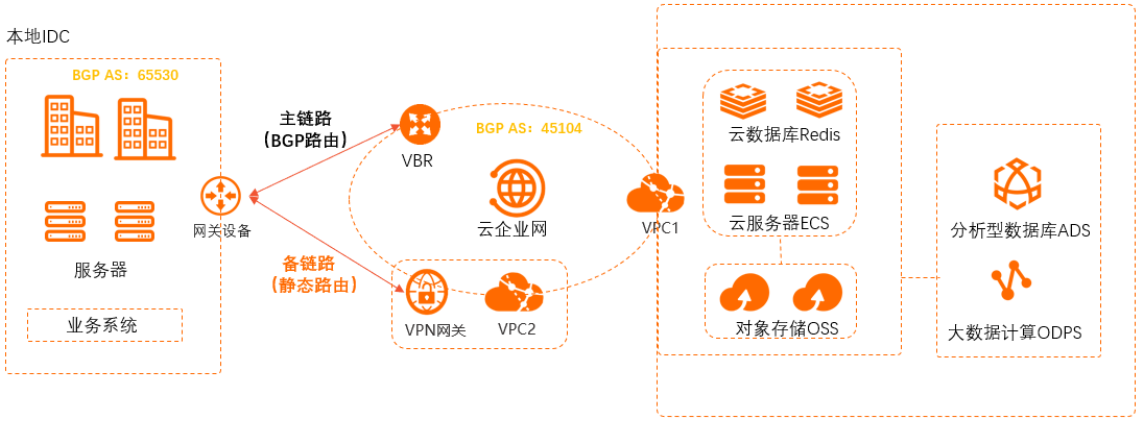
7.IPsec-VPN联合物理专线实现主备链路上云

本文为您介绍如何组合使用IPsec-VPN和物理专线，实现本地数据中心IDC（Internet Data Center）通过主备链路上云并和云上专有网络VPC（Virtual Private Cloud）互通。

场景说明

本文以下图场景为例，为您介绍IPsec-VPN联合物理专线实现主备链路上云方案。某企业在杭州拥有一个本地IDC，且企业已经在阿里云华东1（杭州）地域部署了业务VPC1，VPC1中通过云服务器ECS（Elastic Compute Service）等云产品部署了应用业务和数据分析服务，用于后续业务交互和数据分析。企业现在需要部署上云的主备链路，以实现云下IDC和云上VPC1的互联互通。链路说明如下：

- VPN网关将关联至一个独立的VPC（VPC2）。VPC2中不部署任何业务，仅作为中转VPC为本地IDC和云上搭建VPN链路。
- 在物理专线和VPN链路都正常的情况下，本地IDC与VPC1之间的所有流量只通过物理专线进行转发；当物理专线异常时，本地IDC与VPC1之间的所有流量将切换至VPN链路进行转发。



准备工作

- 您需要为本地IDC和网络实例规划路由协议。本文路由协议规划如下：
  - 本地IDC网关设备与VPN网关之间配置静态路由。
  - 本地IDC网关设备与边界路由器VBR（Virtual border router）之间运行BGP动态路由协议。

> **说明** 在VPN网关作为物理专线备份链路的场景下，路由协议说明如下：
>
> - 如果VPN网关关联至一个独立的VPC（例如本文的VPC2）中，则VBR必须使用BGP动态路由协议，VPN网关可以使用静态路由或BGP动态路由协议。
> - 如果VPN网关关联至业务VPC（例如本文的VPC1）中，则VBR和VPN网关均需要使用BGP动态路由协议。

- 您需要为本地IDC和网络实例规划网段，请确保网段之间没有重叠。本文网段规划如下。

配置目标	网段规划	IP地址
VPC1	192.168.0.0/16	云服务器地址：192.168.20.161

配置目标	网段规划	IP地址
VPC2	10.0.0.0/16	不涉及
VBR	10.1.0.0/30	○ VLAN ID：0 ○ 阿里云侧IPv4互联IP：10.1.0.1/30 ○ 客户侧IPv4互联IP：10.1.0.2/30 本文中客户侧指本地IDC的网关设备
本地IDC	172.16.0.0/16	客户端地址：172.16.1.188
本地IDC的网关设备	10.1.0.0/30	○ 公网IP地址：211.XX.XX.68 ○ 与物理专线连接的端口IP地址：10.1.0.2/30 ○ BGP AS号：65530

- 您已经在阿里云华东1（杭州）地域创建了VPC1和VPC2。其中，VPC1部署有应用业务和数据分析服务；VPC2暂不部署业务，仅关联VPN网关，作为中转VPC为云下和云上搭建VPN链路。具体操作，请参见创建和管理专有网络。
- 请检查本地IDC网关设备，确保网关设备支持标准的IKEv1和IKEv2协议，以便和阿里云VPN网关建立连接。关于网关设备是否支持标准的IKEv1和IKEv2协议，请咨询网关设备厂商。
- 您已经为本地IDC网关设备配置了静态公网IP。
- 您已经了解VPC1中的ECS实例所应用的安全组规则，并确保安全组规则允许本地IDC访问VPC1中的ECS实例。具体操作，请参见查询安全组规则和添加安全组规则。

配置流程

步骤一：部署物理专线

1. 创建物理专线。

   您需要在华东1（杭州）地域申请一条物理专线。具体操作，请参见创建独享专线连接或共享专线连接概述。

2. 创建VBR。

   i. 登录高速通道管理控制台。

   ii. 在左侧导航栏，单击**边界路由器（VBR）**。

   iii. 在顶部状态栏，选择要创建的VBR的地域。

   本示例选择**华东1（杭州）**地域。

   iv. 在**边界路由器（VBR）**页面，单击**创建边界路由器**。

v. 在**创建边界路由器**面板，根据以下信息进行配置，然后单击**确定**。
- **账号类型**：本示例选择**当前账号**。
- **名称**：本示例输入VBR。
- **物理专线接口**：选择已申请的物理专线接口。
- **VLAN ID**：0。
- **阿里云侧IPv4互联IP**：10.1.0.1。
- **客户侧IPv4互联IP**：10.1.0.2。
- **IPv4子网掩码**：255.255.255.252。

3. 配置BGP组。
i. 在**边界路由器（VBR）**页面，单击目标实例ID。
ii. 在边界路由器实例详情页面，单击**BGP组**页签，然后单击**创建BGP组**。
iii. 在**创建BGP组**面板，根据以下信息配置BGP组，然后单击**确定**。
- **名称**：BGP组的名称。本示例输入test。
- **Peer AS号**：本地IDC侧网关设备的AS号。本示例输入65530。
- **BGP密钥**：BGP组的密钥。本示例不配置该项。
- **描述**：BGP组的描述信息。本示例输入test。

4. 配置BGP邻居。
i. 在边界路由器实例详情页面，单击**BGP邻居**页签，然后单击**创建BGP邻居**。
ii. 在**创建BGP邻居**面板，配置BGP邻居信息，然后单击**确定**。
- **BGP组**：选择要加入的BGP组。本示例选择已创建的BGP组。
- **BGP邻居IP**：BGP邻居的IP地址。本示例输入本地IDC侧网关设备的端口IP地址10.1.0.2。

步骤二：部署VPN网关

1. 创建VPN网关。
i. 登录VPN网关管理控制台。
ii. 在顶部菜单栏，选择**华东1（杭州）**地域。
iii. 在**VPN网关**页面，单击**创建VPN网关**。

iv. 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。

  本示例将VPN网关关联到VPC2上，确保VPC2和VPN网关的地域相同。本示例选择**华东1（杭州）**。
- **网关类型**：选择要创建的VPN网关类型。本示例选择**普通型**。
- **VPC**：选择要连接的VPC。本示例选择VPC2。
- **指定交换机**：是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择**否**。

  如果您选择了**是**，您还需要指定具体的**虚拟交换机**。
- **带宽规格**：选择VPN网关的带宽规格，带宽规格是VPN网关所具备的公网带宽。
- **IPsec-VPN**：选择开启或关闭IPsec-VPN功能，IPsec-VPN功能可以在本地IDC与VPC之间或不同VPC之间建立连接。本示例选择**开启**。
- **SSL-VPN**：选择开启或关闭SSL-VPN功能，SSL-VPN功能允许您从任何位置的单台计算机连接到VPC。本示例选择**关闭**。
- **计费周期**：选择购买时长。

v. 返回**VPN网关**页面，查看创建的VPN网关并记录VPN网关公网IP地址，用于后续本地IDC侧路由配置。

刚创建好的VPN网关的状态是**准备中**，约1～5分钟会变成**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。

2. 创建用户网关。

i. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。

ii. 在**用户网关**页面，单击**创建用户网关**。

iii. 在**创建用户网关**面板，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VPC2要连接的本地IDC的网关设备的公网IP。本示例输入211.XX.XX.68。
- **自治系统号**：本地IDC网关设备的自治系统号。本示例无需配置该参数。
- **描述**：输入用户网关的描述信息。

3. 创建IPsec连接。

i. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。

ii. 在**IPsec连接**页面，单击**创建IPsec连接**。

iii. 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**：选择已创建的用户网关。
- **路由模式**：选择路由模式。本示例选择**目的路由模式**。
- **立即生效**：选择是否立即生效。本示例选择**否**。
  - **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，本地IDC网关设备的预共享密钥必须与该值一致。本示例使用默认生成的随机值。

  其他选项使用默认配置。

更多信息，请参见创建IPsec连接。

4. 配置VPN网关路由。

   您需要在VPN网关中将本地IDC的路由发布到VPC2中。

   i. IPsec连接创建成功后，在**创建成功**对话框，单击**确定**，去往VPN网关实例中进行路由发布。

   ii. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。

   iii. 在**VPN网关**页面，找到目标VPN网关，单击目标实例ID。

   iv. 在**目的路由表**页签，单击**添加路由条目**。

   v. 在**添加路由条目**面板，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的网段。本示例输入172.16.0.0/16。
   - **下一跳类型**：选择**IPsec连接**。
   - **下一跳**：选择已创建的IPsec连接实例。
   - **发布到VPC**：选择是否将新添加的路由发布到VPC2路由表。本示例选择**是**。
   - **权重**：选择路由的权重值。本示例使用默认值**100**，表示高优先级。

     > **说明** 若VPN网关中存在相同目标网段的目的路由，目的路由的权重值不支持同时设置为100。

5. 在本地IDC网关设备中加载VPN配置。

   i. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。

   ii. 在**IPsec连接**页面，找到目标IPsec连接，然后在**操作**列选择 > **下载对端配置**。

   iii. 根据本地IDC网关设备的配置要求，将下载的配置添加到本地IDC网关设备中。具体操作，请参见本地网关配置。

步骤三：配置云企业网

VBR和VPN网关配置完成后，您需要将VPC1、VPC2和VBR加入到云企业网中，云企业网可帮您实现本地IDC和VPC1间的互连互通。

1. 创建云企业网实例。

   i. 登录云企业网管理控制台。

ii. 在**云企业网实例**页面，单击**创建云企业网实例**。

iii. 在**创建云企业网实例**面板，根据以下信息配置云企业网实例，然后单击**确定**。

- **名称**：输入云企业网实例的名称。
- **描述**：输入云企业网实例的描述。
- **实例类型**：选择要加载的网络实例类型。本示例选择**专有网络（VPC）**。
- **地域**：选择网络实例所属的地域。本示例选择**华东1（杭州）**。
- **网络实例**：选择网络实例。本示例选择VPC2。

2. 在云企业网实例中加载VPC1、VBR实例。

i. 在**云企业网实例**页面，找到目标云企业网实例，单击目标实例ID。

ii. 在**网络实例管理**页签，单击**加载网络实例**。

iii. 在**加载网络实例**页面，单击**同账号**页签。

iv. 根据以下信息选择要加载的网络实例，然后单击**确定**。

- **实例类型**：选择要加载的网络实例类型。本示例选择**专有网络（VPC）**。
- **地域**：选择网络实例所属地域。本示例选择**华东1（杭州）**。
- **网络实例**：选择网络实例。本示例选择VPC1。

v. 重复上述步骤，将VBR实例加载至该云企业网实例。

3. 发布VPC2中的本地IDC路由至云企业网。

您在VPN网关中将本地IDC路由发布到VPC2中后，VPC2中本地IDC的路由默认是**未发布**状态。您需要手动将VPC2中的本地IDC路由发布到云企业网中，以便VPC1也能从VPC2学习到本地IDC的路由。

i. 登录云企业网管理控制台。

ii. 在**云企业网实例**页面，找到目标云企业网实例，单击实例ID。

iii. 在云企业网实例详情页面，单击**路由信息**页签。

iv. 在**路由信息**页签下，选择查看VPC2网络实例的路由条目，找到本地IDC的路由，在**发布状态**列单击**发布**。

v. 在**发布路由**对话框，单击**确定**。

4. 为物理专线配置健康检查。

您需要为物理专线配置健康检查，健康检查会以您指定的发包时间间隔发送探测报文，当连续发送的所有探测报文（即您指定的探测报文个数）都丢包时，云企业网会主动将流量切换到VPN链路。

i. 登录云企业网管理控制台。

ii. 在左侧导航栏，单击**健康检查**。

iii. 选择VBR的地域，然后单击**设置健康检查**。

iv. 在**设置健康检查**面板，根据以下信息配置健康检查，然后单击**确定**。

- **云企业网实例**：选择VBR加载的云企业网实例。
- **边界路由器（VBR）**：选择要监控的VBR实例。
- **源IP**：本示例选择**自动生成源IP**。

  使用**自动生成源IP**，系统将自动分配100.96.0.0/16地址段内的IP地址，探测链路的连通性。
- **目标IP**：输入VBR实例中客户侧IP地址。
- **发包时间间隔（秒）**：指定健康检查时发送连续探测报文的时间间隔。单位：秒。本示例使用默认值。
- **探测报文个数（个）**：指定健康检查时发送探测报文的个数。单位：个。本示例使用默认值。

步骤四：配置本地IDC网关设备

以下配置示例仅供参考。不同厂商的设备，配置命令可能会有所不同。具体命令，请咨询相关设备厂商。

```
#配置BGP动态路由协议，与VBR建立BGP邻居关系，同时宣告本地IDC私网网段至云上
interface GigabitEthernet 0/12          #该端口为本地IDC网关设备与物理专线连接的端口
no switchport
ip address 10.1.0.2 255.255.255.252     #端口的IP地址，需和VBR客户侧IPv4互联IP地址一致
router bgp 65530
bgp router-id 10.1.0.2
network 172.16.0.0 mask 255.255.0.0     #宣告本地IDC私网网段
neighbor 10.1.0.1 remote-as 45104       #和VBR建立BGP邻居关系
exit
#配置通过VPN网关去往VPC1的静态路由，使其优先级低于BGP路由
ip route 192.168.0.0 255.255.0.0 <VPN网关公网IP地址> preference 255
#配置健康检查探测报文的回程路由
ip route <健康检查源IP地址> 255.255.255.255 10.1.0.1
```

步骤五：测试连通性

1. 在本地IDC下，打开客户端的命令行窗口。
2. 执行 `ping` 命令，访问云上VPC1 192.168.0.0/16网段下的ECS实例IP地址，如果接收到回复报文，则表示本地IDC和VPC1连接成功。
3. 在本地IDC网关设备上，关闭连接物理专线的端口，切断物理专线连接。在客户端再次执行 `ping` 命令，测试本地IDC和VPC1的连通性，如果接收到回复报文，则表示备份VPN链路可用。

8.建立多站点连接以及多站点与VPC的连接

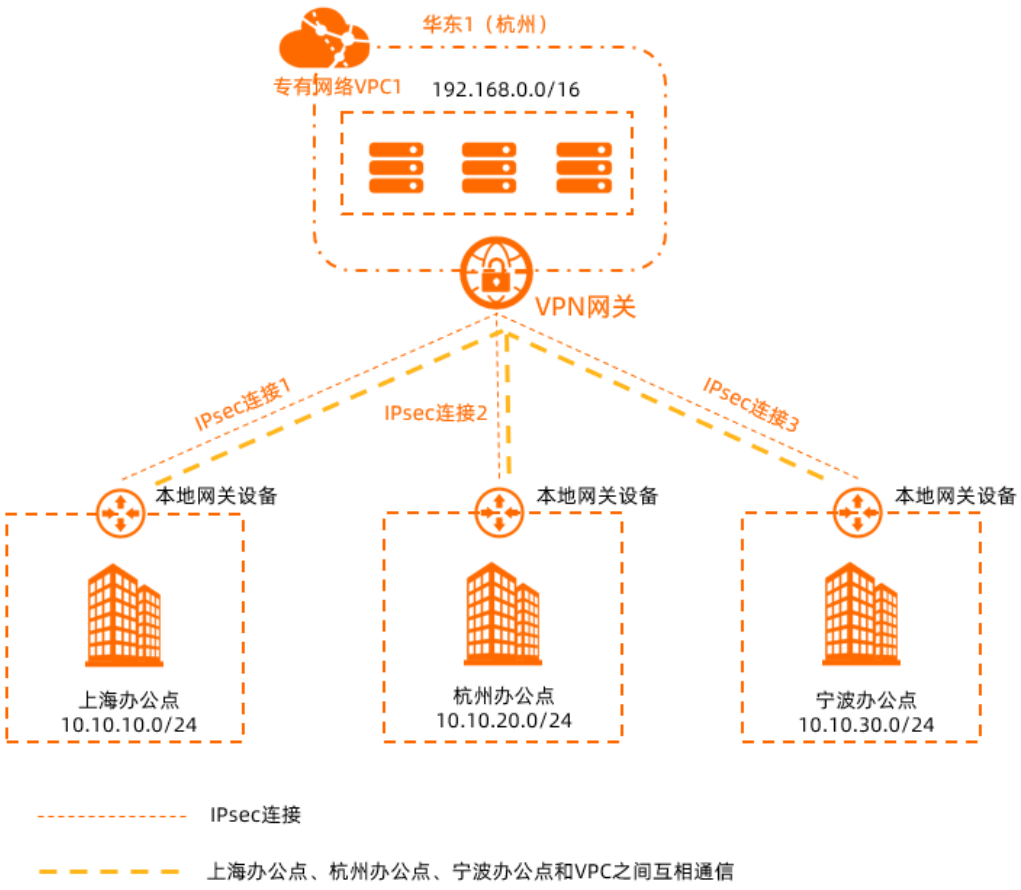
VPN网关的Hub功能可以满足大型企业在各个站点之间、各个站点与专有网络VPC（Virtual Private Cloud）之间建立内网通信的需求。本文为您介绍如何使用VPN网关的Hub功能在多站点之间、多站点与VPC之间建立连接。

VPN网关Hub功能介绍

创建VPN网关实例后，系统自动开启VPN网关实例的Hub功能。您只需要配置各个站点的用户网关以及各个站点到云上的IPsec连接，即可实现多站点之间、多站点与VPC之间的相互通信。

> **说明** 每个VPN网关实例支持创建10个IPsec连接。即一个VPN网关实例，可以连接10个位于不同地域的站点。

场景示例



本文以上图场景为例。某大型企业在上海、杭州、宁波各拥有一个办公点，在阿里云华东1（杭州）地域拥有一个VPC1，VPC1中使用云服务器ECS（Elastic Compute Service）部署了相关业务，当前各个办公点之间，各个办公点与VPC1之间互不相通。因业务发展，现在企业需要使用VPN网关产品，通过VPN网关的Hub功能快速实现上海办公点、杭州办公点、宁波办公点和VPC1之间相互通信。

前提条件

- 您已经获取各个办公点本地网关设备的公网IP地址。
- 您已经在阿里云华东1（杭州）地域创建了一个VPC1，VPC1中使用ECS部署了相关业务。具体操作，请参见搭建IPv4专有网络。

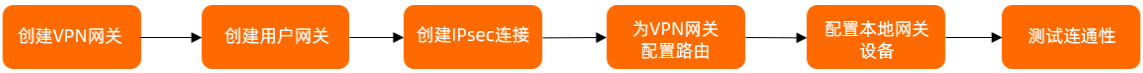
  本示例VPC1和各个办公点的网段规划如下表所示。

  > **说明** 您可以自行规划网段，请确保VPC1和各个办公点之间要互通的网段没有重叠。

站点	VPC1	上海办公点	杭州办公点	宁波办公点
待互通的网段	192.168.0.0/16	10.10.10.0/24	10.10.20.0/24	10.10.30.0/24
ECS实例IP地址	192.168.20.121	不涉及	不涉及	不涉及
本地网关设备公网IP地址	不涉及	1.XX.XX.1	2.XX.XX.2	3.XX.XX.3

- 您已经了解VPC1中ECS实例所应用的安全组规则及各个办公点所应用的访问控制规则，并确保ECS实例的安全组规则以及各个办公点的访问控制规则允许办公点之间、办公点与VPC1之间相互通信。具体操作，请参见查询安全组规则和添加安全组规则。

配置流程



步骤一：创建VPN网关

在VPC1实例所属的地域创建一个VPN网关实例，上海办公点、杭州办公点和宁波办公点将通过该VPN网关实例实现互相通信，以及与云上VPC1的通信。

1. 登录VPN网关管理控制台。
2. 在顶部菜单栏，选择VPN网关实例所属的地域。

   本示例选择**华东1（杭州）**。
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。

配置项	说明
实例名称	输入VPN网关实例的名称。本示例输入*VPN网关1*。
地域和可用区	选择VPN网关实例所属的地域。本示例选择**华东1（杭州）**。
网关类型	选择VPN网关实例的类型。本示例选择**普通型**。
VPC	选择VPN网关实例关联的VPC实例。本示例选择VPC1。
指定交换机	是否指定VPN网关创建在VPC实例中的某一个交换机下。本示例选择否。
带宽规格	选择VPN网关实例的公网带宽峰值。单位：Mbps。

配置项	说明
IPsec-VPN	选择开启或关闭IPsec-VPN功能。本示例选择**开启**。
SSL-VPN	选择开启或关闭SSL-VPN功能。本示例选择**关闭**。
计费周期	选择购买时长。 您可以选择是否自动续费： ○ 按月购买：自动续费周期为1个月。 ○ 按年购买：自动续费周期为1年。
服务关联角色	单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。 VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。 若本配置项显示为**已创建**，则表示您的账号下已创建了该角色，无需重复创建。

更多参数信息，请参见创建VPN网关实例。

5. 返回**VPN网关**页面，查看已创建的VPN网关实例。

   创建VPN网关实例后，其状态是**准备中**，约1~5分钟会变成**正常**状态。**正常**状态表明VPN网关实例已经完成了初始化，可以正常使用。

步骤二：创建用户网关

若要实现多个办公点通过一个VPN网关实例相互通信，在创建VPN网关实例后，您需要创建多个用户网关，一个用户网关对应一个办公点。

1. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。
2. 在顶部菜单栏，选择用户网关的地域。

   > **说明** 用户网关的地域必须和待连接的VPN网关实例的地域相同。

3. 在**用户网关**页面，单击**创建用户网关**。
4. 在**创建用户网关**面板，根据以下信息配置用户网关，然后单击**确定**。

   您需要为每个办公点创建一个用户网关，用户网关的配置请参见下表。

配置项	配置项说明	上海办公点	杭州办公点	宁波办公点
名称	输入用户网关的名称。	*Shanghai-customer1*	*Hangzhou-customer2*	*Ningbo-customer3*
IP地址	输入用户网关的公网IP地址。	本示例输入上海办公点本地网关设备的公网IP地址*1.XX.XX.1*。	本示例输入杭州办公点本地网关设备的公网IP地址*2.XX.XX.2*。	本示例输入宁波办公点本地网关设备的公网IP地址*3.XX.XX.3*。

更多参数信息，请参见创建用户网关。

步骤三：创建IPsec连接

您需要为上海办公点、杭州办公点、宁波办公点各创建一条IPsec连接，IPsec连接会将用户网关与VPN网关关联起来，进而将各个办公点连接至阿里云。

1. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
2. 在顶部菜单栏，选择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**。

   上海办公点、杭州办公点以及宁波办公点IPsec连接的配置请参见下表。

配置项	配置项说明	上海办公点	杭州办公点	宁波办公点
名称	输入IPsec连接的名称。	*IPsec连接1*	*IPsec连接2*	*IPsec连接3*
VPN网关	选择已创建的VPN网关实例。	选择VPN网关1。		
用户网关	选择已创建的用户网关实例。	选择Shanghai-customer1。	选择Hangzhou-customer2。	选择Ningbo-customer3。
路由模式	选择路由模式。	选择**目的路由模式**。	选择**目的路由模式**。	选择**感兴趣流模式**。
本端网段	输入需要和各个办公点互通的VPC的网段，用于第二阶段协商。	不涉及	不涉及	*192.168.0.0/16*
对端网段	输入需要和VPC互通的办公点的网段，用于第二阶段协商。			*10.10.30.0/24*
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**。	本示例选择**是**。	本示例选择**是**。
预共享密钥	输入预共享密钥。 如果不输入该值，系统默认生成一个16位的随机字符串。 **注意** 本地网关设备的预共享密钥需和IPsec连接的预共享密钥一致。	*fddsFF123*****	*TTTddd321*****	*PPPttt456*****

   其他选项使用默认配置。更多参数信息，请参见创建IPsec连接。

5. 在**创建成功**对话框中，单击**确定**。

步骤四：为VPN网关配置路由

IPsec连接创建完成后，您需要将上海办公点和杭州办公点待互通的网段添加至VPN网关实例的目的路由表中，并将上海办公点、杭州办公点和宁波办公点待互通的网段发布至VPC1中，为实现各个办公点之间、办公点与VPC1之间的相互通信做准备。

> **说明** 宁波办公点的IPsec连接使用的是感兴趣流的路由模式，IPsec连接创建完成后，系统自动将本端路由和对端路由添加至VPN网关实例的策略路由表中，因此您只需在策略路由表中将宁波办公点的网段直接发布至VPC1即可，无需再手动添加路由。

1. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
2. 在顶部菜单栏，选择VPN网关实例的地域。
3. 在**VPN网关**页面，找到目标VPN网关实例，单击实例ID。
4. 在VPN网关实例的**目的路由表**中添加并发布上海办公点和杭州办公点的网段。
   i. 在**目的路由表**页签，单击**添加路由条目**。
   ii. 在**添加路由条目**面板，根据以下信息配置目的路由条目，然后单击**确定**。

配置项	配置说明	路由条目1	路由条目2
目标网段	输入待互通的目标网段。	输入上海办公点的私网网段*10.10.10.0/24*。	输入杭州办公点的私网网段*10.10.20.0/24*。
下一跳类型	选择下一跳的类型。	选择**IPsec连接**。	选择**IPsec连接**。
下一跳	选择下一跳。	选择IPsec连接1。	选择IPsec连接2。
发布到VPC	选择是否将新添加的路由条目发布到VPN网关关联的VPC1中。	本示例选择**是**。	本示例选择**是**。
权重	选择路由条目的权重值。 ■ **100**：高优先级。 ■ **0**：低优先级。	本示例保持默认值**100**。	本示例保持默认值**100**。

   更多参数信息，请参见添加目的路由。
5. 在VPN网关实例的**策略路由表**中发布宁波办公点的网段。
   i. 在**策略路由表**中，找到**目标网段**为宁波办公点网段的路由条目，在**操作**列单击**发布**。
   ii. 在**发布路由**对话框，单击**确定**。

步骤五：配置本地网关设备

在阿里云侧完成VPN网关的配置后，还需要配置各个办公点的本地网关设备。您需要在**IPsec连接**页面下载本地网关设备的配置，并将配置添加至本地网关设备中，以便实现各个办公点之间、办公点与VPC1之间的相互通信。

1. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。
2. 在**IPsec连接**页面，找到目标IPsec连接，然后在**操作**列下选择 ⋮ **> 下载对端配置**。

   分别找到IPsec连接1、IPsec连接2和IPsec连接3，下载对端配置。
3. 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。具体操作，请参见本地网关配置。
   - 将通过IPsec连接1下载的对端配置添加至上海办公点的本地网关设备中。
   - 将通过IPsec连接2下载的对端配置添加至杭州办公点的本地网关设备中。

- 将通过IPsec连接3下载的对端配置添加至宁波办公点的本地网关设备中。

步骤六：测试连通性

完成上述配置后，上海办公点、杭州办公点、宁波办公点和VPC1之间已经可以互相通信。以下内容介绍如何测试连通性。

1. 测试办公点与VPC1之间的连通性。
   i. 登录VPC1内的ECS实例。

      关于如何登录ECS实例，请参见连接方式概述。
   ii. 执行ping命令，分别访问上海办公点、杭州办公点和宁波办公点的一台客户端。

      ```
      ping <客户端IP地址>
      ```

      如果均能够收到回复报文，则证明各个办公点与VPC1之间可以互相通信。
2. 测试办公点之间的连通性。
   i. 打开上海办公点一台客户端的命令行窗口。
   ii. 执行ping命令，分别访问杭州办公点和宁波办公点的一台客户端。

      ```
      ping <客户端IP地址>
      ```

      如果均能够收到回复报文，则证明上海办公点与杭州办公点、上海办公点与宁波办公点之间可以互相通信。
   iii. 打开杭州办公点一台客户端的命令行窗口。
   iv. 执行ping命令，访问宁波办公点的一台客户端。

      ```
      ping <客户端IP地址>
      ```

      如果收到回复报文，则证明杭州办公点与宁波办公点之间可以互相通信。

9.通过私网VPN网关实现专线私网流量加密通信

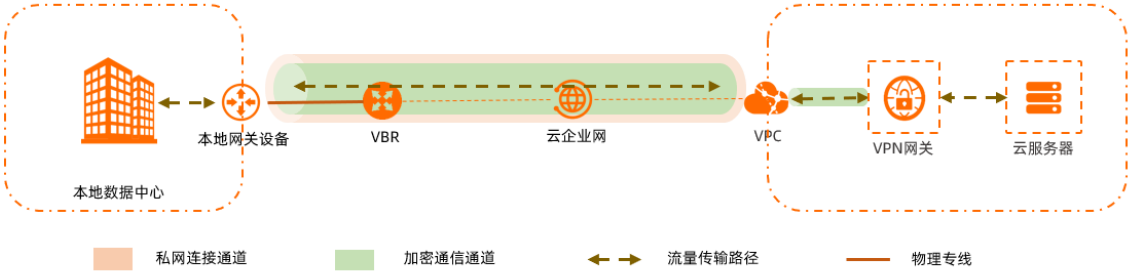
9.1. 方案概述

本地数据中心通过物理专线和云企业网与云上专有网络实现私网通信后，通信流量未经过加密处理，无法满足安全通信的高要求。使用私网VPN网关可帮您实现基于物理专线的私网流量（以下简称为私网流量）加密通信，提高网络的安全性。本文为您介绍私网流量加密通信原理和配置方案。

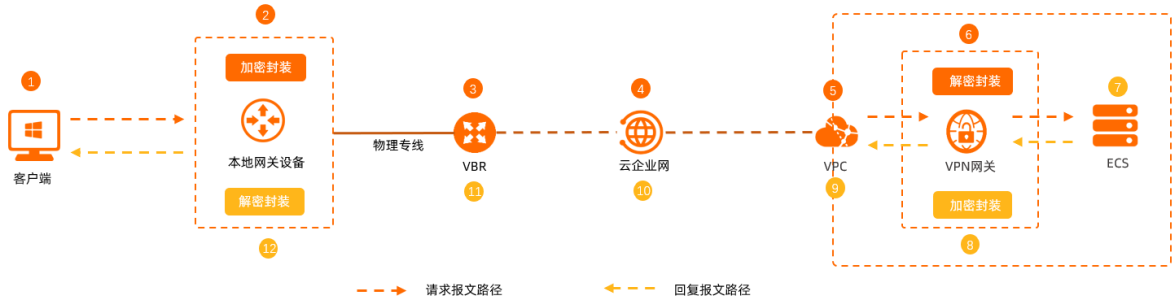
> **说明** 私网VPN网关正在邀测中，您可以向商务经理申请体验或者提交工单申请体验。

私网流量加密通信原理

在本地数据中心IDC（Internet Data Center）通过物理专线和云企业网与云上专有网络VPC（Virtual Private Cloud）实现私网通信后，私网VPN网关可通过已建立的私网连接与本地网关设备建立加密通信通道。您可以通过相关路由配置引导本地IDC和VPC要互通的流量进入加密通信通道，实现私网流量加密通信。



以下内容以本地IDC的客户端访问VPC中的云服务器ECS（Elastic Compute Service）为例，为您介绍私网流量加密通信过程，方便您了解私网流量加密通信原理。



序号	转发流量的对象	转发说明
①	客户端	1. 客户端发起访问请求。 2. 客户端通过查询路由表，将请求报文转发至本地网关设备。

序号	转发流量的对象	转发说明
②	本地网关设备	1. 本地网关设备接收到请求报文后，依据请求报文的目的地址和IPsec配置，对请求报文进行加密封装。 请求报文被加密封装后，目的地址变更为VPN网关私网IP地址。 2. 本地网关设备依据请求报文被封装后的目的IP地址查询路由表，将请求报文转发至边界路由器VBR（Virtual border router）实例。
③	VBR实例	VBR实例接收到封装后的请求报文后，通过查询路由表将封装后的请求报文转发至云企业网。
④	云企业网	云企业网接收到封装后的请求报文后，通过查询路由表将封装后的请求报文转发至VPC。
⑤	VPC实例	VPC接收到封装后的请求报文后，通过查询路由表将封装后的请求报文转发至VPN网关。
⑥	VPN网关	1. VPN网关接收到封装后的请求报文后，对请求报文进行解密封装。 2. VPN网关依据请求报文被解密封装后的目的IP地址查询路由表，将请求报文转发至ECS。
⑦	ECS实例	1. ECS接收到请求报文后进行响应，向客户端发送回复报文。 2. ECS依据回复报文的目的地址查询路由表，将回复报文转发至VPN网关。
⑧	VPN网关	1. VPN网关接收到回复报文后，对回复报文进行加密封装。 回复报文被加密封装后，目的地址变更为本地网关设备VPN IP地址。 2. VPN网关依据回复报文被封装后的目的IP地址查询路由表，将回复报文转发至VPC。
⑨	VPC实例	VPC接收到封装后的回复报文后，通过查询路由表将封装后的回复报文转发至云企业网。
⑩	云企业网	云企业网接收到封装后的回复报文后，通过查询路由表将封装后的回复报文转发至VBR实例。
⑪	VBR实例	VBR实例接收到封装后的回复报文后，通过查询路由表将封装后的回复报文转发至本地网关设备。
⑫	本地网关设备	1. 本地网关设备接收到回复报文后，对回复报文进行解密封装。 2. 本地网关设备依据回复报文被解密封装后的目的IP地址查询路由表，将回复报文转发至客户端。

配置方案说明

在通过私网VPN网关实现私网流量加密通信的过程中，根据VBR实例和VPN网关运行的协议不同，可分为以下三个配置方案，下表为您介绍三个配置方案的区别以及相关配置教程。

配置方案	配置说明	配置教程	VPN网关连接中断后的通信影响
方案一	VBR实例和VPN网关均配置静态路由。	通过静态路由方式实现私网流量加密通信	• 私网通信流量不再被加密。 • 本地IDC与VPC之间的私网连接中断。 您可以手动撤销VPN网关中的路由发布，撤销后，本地IDC与VPC之间自动通过物理专线和云企业网恢复私网连接。
方案二	• VBR实例配置静态路由。 • VPN网关运行BGP动态路由协议。 说明 VBR实例运行BGP动态路由协议以及VPN网关配置静态路由的配置方案暂不支持。	通过静态和BGP路由方式实现私网流量加密通信	• 私网通信流量不再被加密。 • 系统将自动撤销通过VPN网关BGP动态路由协议发布的路由。 • 本地IDC与VPC之间自动通过物理专线和云企业网进行私网通信。
方案三	VBR实例和VPN网关均运行BGP动态路由协议。	通过BGP路由方式实现私网流量加密通信	• 私网通信流量不再被加密。 • 系统将自动撤销通过VPN网关BGP动态路由协议发布的路由。 • 本地IDC与VPC之间自动通过物理专线和云企业网进行私网通信。

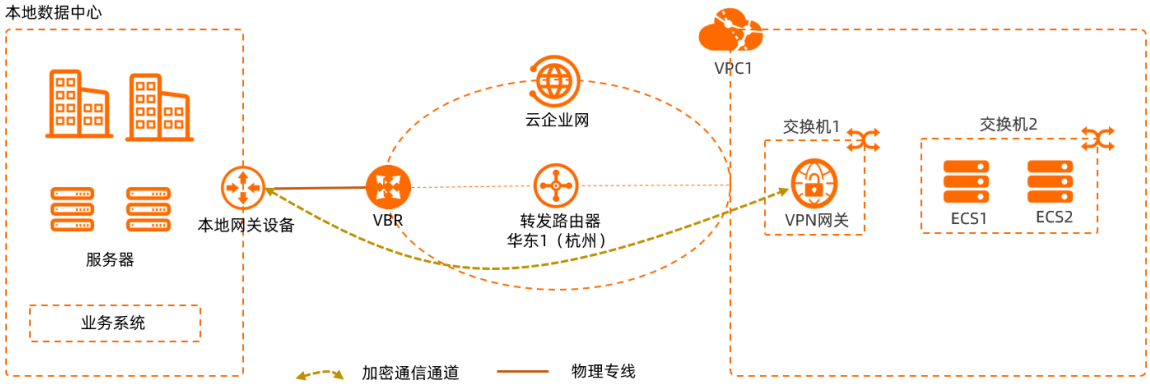
9.2. 通过静态路由方式实现私网流量加密通信

本文为您介绍在边界路由器VBR（Virtual border router）和私网VPN网关配置静态路由的场景下，如何通过私网VPN网关（以下简称VPN网关）实现私网流量加密通信。

背景信息

在您应用本方案前，建议您先了解私网加密通信原理和配置方案说明。更多信息，请参见方案概述。

场景示例



本文以上图场景为例。某企业在杭州拥有一个本地IDC，在阿里云华东1（杭州）地域拥有一个VPC1，VPC1中使用云服务器ECS（Elastic Compute Service）部署了相关服务。因业务发展，企业计划使用物理专线和云企业网实现本地IDC和VPC1的相互通信。同时，为了提高企业网络的安全性，企业希望本地IDC和VPC1之间的流量可以经过加密后再进行传输。

在本地IDC已和VPC1实现私网通信的情况下，企业可以在VPC1中创建私网VPN网关，与本地网关设备建立IPsec连接，同时为VBR实例和VPN网关配置静态路由，实现私网流量的加密传输。

准备工作

- 私网VPN网关正在邀测中，您已经向商务经理申请使用权限或者已提交工单申请使用权限。
- 您需要为本地IDC和网络实例规划网段，需确保要互通的网段之间没有重叠。本示例网段规划如下：

配置目标	网段规划	IP地址
VPC1	◦ 主网段：10.0.0.0/16 ◦ 交换机1所属子网段：10.0.0.0/24 ◦ 交换机2所属子网段：10.0.1.0/24	◦ ECS1：10.0.1.1 ◦ ECS2：10.0.1.2
VBR	10.0.0.0/30	◦ VLAN ID：0 ◦ 阿里云侧IPv4互联IP：10.0.0.2/30 ◦ 客户侧IPv4互联IP：10.0.0.1/30 本示例中客户侧指本地网关设备。
本地IDC	◦ 主网段：192.168.0.0/16 ◦ 子网段1：192.168.0.0/24 ◦ 子网段2：192.168.1.0/24	客户端地址：192.168.1.1
本地网关设备	◦ 10.0.0.0/30 ◦ 192.168.0.0/24	◦ VPN IP地址：192.168.0.251 VPN IP地址是指本地网关设备上待与阿里云VPN网关建立IPsec连接的接口的IP地址。 ◦ 与物理专线连接的接口IP地址：10.0.0.1

- 您已经在阿里云华东1（杭州）地域创建了VPC1并使用ECS部署了相关服务。具体操作，请参见创建和管

理专有网络。

请确保VPC1在华东1（杭州）地域企业版转发路由器支持的可用区中均拥有至少一个交换机实例，且每个交换机实例拥有至少一个空闲的IP地址，以便后续云企业网连接VPC1。更多信息，请参见创建VPC连接。

在本示例中，VPC1中包含2个交换机实例，交换机1位于可用区H，交换机2位于可用区I。交换机2用于部署ECS，交换机1仅用于后续关联VPN网关。

> **说明** 在您创建VPC实例时，建议您在VPC实例中单独创建一个交换机实例用于后续关联VPN网关，以便交换机实例可以分配私网IP地址至VPN网关。

- 请检查本地网关设备，确保本地网关设备支持标准的IKEv1和IKEv2协议，以便和阿里云VPN网关建立连接。关于本地网关设备是否支持标准的IKEv1和IKEv2协议，请咨询本地网关设备厂商。
- 您已经了解VPC1中的ECS实例所应用的安全组规则以及本地IDC中客户端所应用的访问控制规则，并确保ECS实例的安全组规则以及本地IDC客户端的访问控制规则允许本地IDC客户端与VPC1中的ECS实例互通。具体操作，请参见查询安全组规则和添加安全组规则。

配置流程

步骤一：部署物理专线

您需要部署物理专线将本地IDC连接至阿里云。

1. 创建物理专线。

   您需要在华东1（杭州）地域申请一条物理专线。具体操作，请参见创建独享专线连接或共享专线连接概述。

   本示例选择**创建独享专线连接**。

2. 创建VBR实例。

   i. 登录高速通道管理控制台。

   ii. 在左侧导航栏，单击**边界路由器（VBR）**。

   iii. 在顶部状态栏，选择待创建的VBR实例的地域。

   本示例选择**华东1（杭州）**地域。

   iv. 在**边界路由器（VBR）**页面，单击**创建边界路由器**。

v. 在**创建边界路由器**面板，根据以下信息进行配置，然后单击**确定**。

下表仅列举本示例强相关的配置项。如果您想要了解更多信息，请参见创建边界路由器。

配置项	说明
账号类型	本示例选择**当前账号**。
名称	本示例输入*VBR*。
物理专线接口	本示例选择**独享专线**类型，然后选择在步骤中创建的物理专线接口。
VLAN ID	本示例输入*0*。
设置VBR带宽值	选择VBR实例的带宽峰值。
阿里云侧IPv4互联IP	本示例输入*10.0.0.2*。
客户侧IPv4互联IP	本示例输入*10.0.0.1*。
IPv4子网掩码	本示例输入*255.255.255.252*。

3. 为VBR实例添加自定义路由条目。

通过添加自定义路由条目将本地IDC的网段发布至阿里云。

i. 在**边界路由器（VBR）**页面，单击VBR实例ID。

ii. 单击**路由条目**页签，然后单击**添加路由条目**。

iii. 在**添加路由条目**面板，根据以下信息进行配置，然后单击**确定**。

配置项	说明
下一跳类型	选择**物理专线接口**。
目标网段	输入本地IDC的网段。 本示例输入*192.168.0.0/16*。
下一跳	选择在步骤中创建的物理专线接口。

4. 配置本地网关设备。

您需要在本地网关设备上配置以下路由条目，引导本地IDC访问VPC1的流量进入物理专线。

以下配置示例仅供参考，不同厂商的设备配置命令可能会有所不同。具体命令，请咨询相关设备厂商。

```
ip route 10.0.0.0 255.255.0.0 10.0.0.2
```

步骤二：配置云企业网

您需要将VPC1和VBR连接至云企业网，连接后，本地IDC和VPC1可通过云企业网实现私网互通。

1. 创建云企业网实例。

i. 登录云企业网管理控制台。

ii. 在**云企业网实例**页面，单击**创建云企业网实例**。

iii. 在**创建云企业网实例**对话框，根据以下信息进行配置，然后单击**确认**。

- **名称**：输入云企业网实例的名称。

  本示例输入*CEN*。

- **描述**：输入云企业网实例的描述信息。

  本示例输入*CEN-for-test-private-VPN-Gateway*。

2. 连接VPC实例。

i. 在**云企业网实例**页面，单击在步骤中创建的云企业网实例ID。

ii. 在**基本信息**页签的**VPC**区域，单击⊕图标。

iii. 在**连接网络实例**页面，根据以下信息进行配置，然后单击**确定创建**。

配置项	说明
实例类型	选择待连接的网络实例类型。 本示例选择**专有网络（VPC）**。
地域	选择待连接的网络实例所在的地域。 本示例选择**华东1（杭州）**。
转发路由器	系统自动在该地域下创建转发路由器实例。
设定转发路由器的主/备可用区	选择转发路由器的主备可用区。 本示例配置如下： ■ **主可用区**为**杭州 可用区H** ■ **备可用区**为**杭州 可用区I**
资源归属UID	选择待连接的网络实例所属的账号类型。 本示例选择**同账号**。
付费方式	本示例保持默认值**按量付费**。 按量计费规则，请参见计费说明。
连接名称	输入网络实例连接的名称。 本示例输入*VPC1-test*。

配置项	说明
网络实例	选择待连接的网络实例。 本示例选择VPC1。
交换机	分别从转发路由器主备可用区中选择交换机实例。 本示例选择如下： ■ **杭州 可用区H（主）**：选择交换机1。 ■ **杭州 可用区I（备）**：选择交换机2。
高级配置	系统默认帮您选中以下三种高级功能。 ■ **自动关联至转发路由器的默认路由表** 开启本功能后，VPC连接会自动关联至转发路由器的默认路由表，转发路由器通过查询默认路由表转发VPC实例的流量。 ■ **自动传播系统路由至转发路由器的默认路由表** 开启本功能后，VPC实例会将自身的系统路由传播至转发路由器的默认路由表中，用于网络实例的互通。 ■ **自动为VPC的所有路由表配置指向转发路由器的路由** 开启本功能后，系统将在VPC实例的所有路由表内自动配置10.0.0.0/8、172.16.0.0/12、192.168.0.0/16三条路由条目，其下一跳均指向VPC连接。 本示例保持默认值。

iv. 单击**继续创建连接**，返回**连接网络实例**页面。

3. 连接VBR实例。

i. 在**连接网络实例**页面，根据以下信息进行配置，然后单击**确定创建**。

配置项	配置项说明
实例类型	选择待连接的网络实例类型。 本示例选择**边界路由器（VBR）**。
地域	选择待连接的网络实例所在的地域。 本示例选择**华东1（杭州）**。
转发路由器	系统自动显示当前地域已创建的转发路由器实例。
资源归属UID	选择待连接的网络实例所属的账号类型。 本示例选择**同账号**。
连接名称	输入网络实例连接的名称。 本示例输入*VBR-test*。
网络实例	选择待连接的网络实例。 本示例选择VBR。
高级配置	系统默认帮您选中以下三种高级功能。 ■ **自动关联至转发路由器的默认路由表** 开启本功能后，VBR连接会自动关联至转发路由器的默认路由表，转发路由器通过默认路由表转发VBR实例的流量。 ■ **自动传播系统路由至转发路由器的默认路由表** 开启本功能后，VBR实例的系统路由自动传播至转发路由器的默认路由表中。 ■ **自动发布路由到Vbr** 开启本功能后，系统自动将VBR连接关联的路由表中的路由发布到VBR实例中。 本示例保持默认值。

步骤三：部署VPN网关

完成上述步骤后，本地IDC和VPC1之间可以实现私网互通，但在通信过程中，信息未经过加密。您还需要在VPC1中部署VPN网关，与本地网关设备建立IPsec连接，才能实现私网流量加密通信。

1. 创建VPN网关。
   i. 登录VPN网关管理控制台。
   ii. 在顶部菜单栏，选择VPN网关的地域。
   VPN网关的地域需和待关联的VPC实例的地域相同。本示例选择**华东1（杭州）**地域。
   iii. 在**VPN网关**页面，单击**创建VPN网关**。

iv. 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。

配置项	说明
实例名称	输入VPN网关的名称。 本示例输入*VPN网关1*。
地域和可用区	选择VPN网关所属的地域。 本示例选择**华东1（杭州）**。
网关类型	选择VPN网关的类型。 本示例选择**普通型**。
网络类型	选择VPN网关的网络类型。 本示例选择**私网**。
VPC	选择VPN网关待关联的VPC实例。 本示例选择VPC1。
指定交换机	是否指定VPN网关关联在VPC实例中的某一个交换机实例下。 本示例选择**是**。
虚拟交换机	选择VPN网关待关联的交换机实例。 本示例选择交换机1。
带宽规格	选择VPN网关的带宽峰值。单位：Mbps。
IPsec-VPN	私网类型的VPN网关仅支持IPsec-VPN功能。 本示例保持默认值，即**开启**IPsec-VPN功能。
计费周期	选择购买时长。 您可以选择是否自动续费： ■ 按月购买：自动续费周期为1个月。 ■ 按年购买：自动续费周期为1年。
服务关联角色	单击**创建关联角色**，系统自动创建服务关联角色AliyunServiceRoleForVpn。 VPN网关使用此角色来访问其他云产品中的资源，更多信息，请参见AliyunServiceRoleForVpn。 若本配置项显示为**已创建**，则表示您的账号下已创建了该角色，无需重复创建。

v. 返回**VPN网关**页面，查看已创建的VPN网关并记录VPN网关的私网IP地址，用于后续IPsec连接的配置。

刚创建好的VPN网关的状态是**准备中**，约1～5分钟会变成**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。

2. 创建用户网关。

i. 在左侧导航栏，选择**网间互联 > VPN > 用户网关**。

ii. 在**用户网关**页面，单击**创建用户网关**。

iii. 在**创建用户网关**面板，根据以下信息进行配置，然后单击**确定**。

以下内容仅列举本示例强相关的配置项及示例值。如果您想要了解更多信息，请参见创建用户网关。

- **名称**：输入用户网关的名称。

  本示例输入*Customer-Gateway*。

- **IP地址**：输入VPN网关待连接的本地网关设备的VPN IP地址。

  本示例输入*192.168.0.251*。

3. 创建IPsec连接。

i. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。

ii. 在**IPsec连接**页面，单击**创建IPsec连接**。

iii. 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**。

以下内容仅列举本示例强相关的配置项及示例值。如果您想要了解更多信息，请参见创建IPsec连接。

配置项	配置项说明
名称	输入IPsec连接的名称。 本示例输入*IPsec连接1*。
VPN网关	选择已创建的VPN网关实例。 本示例选择VPN网关1。
用户网关	选择已创建的用户网关实例。 本示例选择Customer-Gateway。
路由模式	选择路由模式。 本示例选择**目的路由模式**。
立即生效	选择是否立即生效。取值： ■ **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。 如果不输入该值，系统默认生成一个16位的随机字符串。 **注意** 本地网关设备的预共享密钥需和IPsec连接的预共享密钥一致。 本示例输入*fddsFF123*****。

高级配置等均使用默认配置。

iv. IPsec连接创建成功后，在**创建成功**对话框，单击**确定**。

4. 在本地网关设备中加载VPN配置。

i. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。

ii. 在**IPsec连接**页面，找到目标IPsec连接，然后在**操作**列选择 **> 下载对端配置**。

iii. 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。具体操作，请参见本地网关配置。

步骤四：配置云上路由

完成上述配置后，本地网关设备和VPN网关之间已经可以建立加密通信通道了。您还需要为云上网络实例配置路由，引导云上和云下流量通信时进入加密通信通道。

1. 为VPC1添加自定义路由条目。
   i. 登录专有网络管理控制台。
   ii. 在左侧导航栏，单击**路由表**。
   iii. 在顶部状态栏处，选择路由表所属的地域。
   本示例选择**华东1（杭州）**地域。
   iv. 在**路由表**页面，找到目标路由表，单击路由表实例ID。
   本示例找到VPC1的系统路由表。
   v. 在**路由条目列表**页签下单击**自定义路由条目**页签，然后单击**添加路由条目**。
   vi. 在**添加路由条目**面板，配置以下信息，然后单击**确定**。

配置项	说明
名称	输入自定义路由条目的名称。
目标网段	输入自定义路由条目的目标网段。 本示例选择**IPv4网段**并输入本地网关设备VPN IP地址*192.168.0.251/32*。
下一跳类型	选择自定义路由条目的下一跳类型。 本示例选择**转发路由器**。
转发路由器	选择自定义路由条目的下一跳。 本示例选择VPC1-test。

2. 为VBR实例添加自定义路由条目。
   i. 登录高速通道管理控制台。
   ii. 在左侧导航栏，单击**边界路由器（VBR）**。
   iii. 在顶部状态栏处，选择VBR实例的地域。
   本示例选择**华东1（杭州）**地域。
   iv. 在**边界路由器（VBR）**页面，单击目标边界路由器的ID。
   v. 单击**路由条目**页签，然后单击**添加路由条目**。
   vi. 在**添加路由条目**面板，根据以下信息配置路由条目，然后单击**确定**。

配置项	说明
下一跳类型	选择**物理专线接口**。
目标网段	输入本地网关设备VPN IP地址。 本示例输入*192.168.0.251/32*。
下一跳	选择在步骤中创建的物理专线接口。

3. 为VPN网关添加路由条目。

> **注意** 为了引导VPC去往云下的流量进入VPN网关加密通信通道，在确保通信正常的情况下，您需要在VPN网关中添加比本地IDC网段更明细的路由（即路由的目标网段是本地IDC网段的真子集），并将该路由发布至VPC中。
>
> 例如，本示例中本地IDC的网段为192.168.0.0/16，则VPN网关中路由条目的目标网段需比该网段小，本示例VPN网关中路由条目的目标网段输入为*192.168.1.0/24*。

i. 登录VPN网关管理控制台。
ii. 在左侧导航栏，选择**网间互联 > VPN > VPN网关**。
iii. 在顶部状态栏处，选择VPN网关所属的地域。
本示例选择**华东1（杭州）**地域。
iv. 在**VPN网关**页面，找到目标VPN网关，单击目标实例ID。
v. 在**目的路由表**页签，单击**添加路由条目**。
vi. 在**添加路由条目**面板，根据以下信息配置目的路由，然后单击**确定**。

配置项	说明
目标网段	输入本地IDC的明细网段。 本示例输入*192.168.1.0/24*。
下一跳类型	选择**IPsec连接**。
下一跳	选择在步骤中已创建的IPsec连接。
发布到VPC	选择是否将新添加的路由发布至VPC实例的路由表。 本示例选择**是**，将路由发布至VPC1中。
权重	选择路由的权重值。 本示例使用默认值**100**，表示高优先级。

步骤五：测试验证

完成上述配置后，本地IDC和VPC1之间已经可以进行私网加密通信。以下内容为您介绍如何测试本地IDC和VPC1之间的私网连通性以及如何验证流量是否经过VPN网关加密。

1. 测试私网连通性。
i. 登录ECS1实例。具体操作，请参见ECS远程连接操作指南。
ii. 执行**ping**命令，访问本地IDC网段下的任意一台客户端，测试本地IDC和VPC1之间的私网连通性。

```
ping <本地IDC客户端私网IP地址>
```

如果收到回复报文，则证明本地IDC和VPC1之间已经实现私网互通。

2. 验证加密是否生效。
如果您可以在IPsec连接详情页面查看到流量监控数据，则证明私网流量传输过程已经过加密处理。
i. 登录VPN网关管理控制台。

ii. 在顶部状态栏处，选择VPN网关所属的地域。

本示例选择**华东1（杭州）**地域。

iii. 在左侧导航栏，选择**网间互联 > VPN > IPsec连接**。

iv. 在**IPsec连接**页面，找到在步骤中创建的IPsec连接，单击连接ID。
进入IPsec连接详情页面查看流量监控数据。