阿里云
VPN网关

最佳实践

文档版本：20190919

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
	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。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能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，恢复业务所需时间约10分钟。
	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。	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。	单击 **确定**。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
##	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。	`swich` *{stand | slave}*

目录

1 在经典网络中使用SSL VPN

1.1 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Internet。
- 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。

完成以下操作，创建VPN网关：

1. 登录新版VPC管理控制台。

2. 在左侧导航栏，单击VPN > VPN网关 。
3. 在VPN网关页面，单击创建VPN网关。
4. 在购买页面，配置VPN网关，完成支付。本操作中VPN网关的配置如下：
   - 地域：选择VPN网关的地域。本操作中选择华东1（杭州）。

     说明:
     确保VPC的地域和VPN网关的地域相同。
   - 专有网络： 选择要连接的VPC。
   - 带宽规格：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
   - IPsec-VPN： 选择是否开启IPsec-VPN功能，IPsec-VPN功能适用于站点到站点的连接，可以根据您的实际需要选择开启。
   - SSL-VPN： 选择是否开启SSL-VPN功能。本操作选择开启。
   - SSL并发连接数： 选择您需要同时连接的客户端最大规格。

5. 返回VPN网关页面，查看创建的VPN网关。

   刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明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. 在专有网络的左侧导航栏，单击VPN > SSL服务端。
2. 单击创建SSL服务端。本操作中SSL服务端的配置如下：
   - 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。

步骤三 创建客户端证书

完成以下操作，创建客户端证书：

1. 在专有网络的左侧导航栏，单击VPN > SSL客户端 。
2. 单击创建SSL客户端证书。
3. 在创建客户端证书对话框，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，然后单击下载下载生成的客户端证书。

步骤四 配置客户端

完成以下操作，配置客户端：

1. 执行以下命令安装OpenVPN客户端。

```
yum install -y openvpn
```

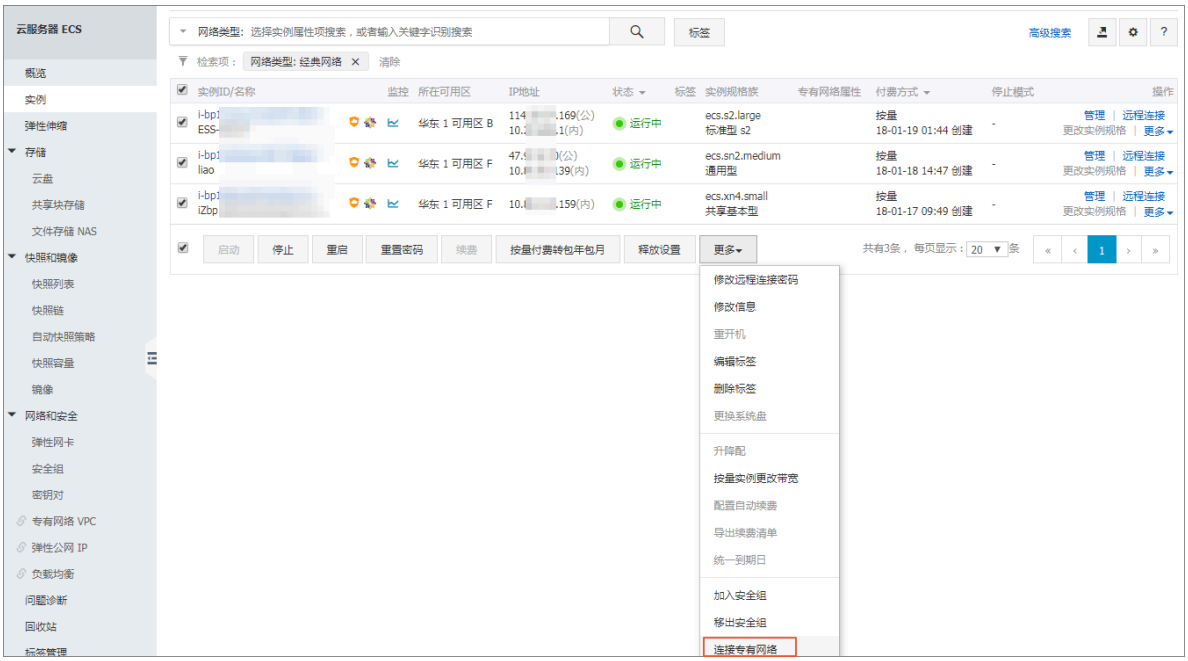
2. 将步骤三中下载的证书解压拷贝到*/etc/openvpn/conf/*目录。
3. 执行以下命令启动Openvpn客户端软件。

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

步骤五 建立ClassicLink连接

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ID链接。
3. 在专有网络详情页面，单击开启ClassicLink。
4. 在弹出的对话框，单击确定。
5. 登录ECS管理控制台。
6. 在左侧导航栏，单击实例。
7. 选择一个或多个目标经典网络的ECS实例，单击更多 > 连接专有网络 。



8. 在弹出的对话框中选择目标VPC，单击确定。
9. 在左侧导航栏，单击网络和安全 > 安全组 。

10.在安全组列表页面，单击内网入方向页签，然后单击添加安全组规则。按照如下配置添加安全组规则：

- 规则方向：入方向
- 授权策略：允许
- 协议类型：全部
- 授权类型：地址段访问
- 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。

11.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中连接状态，然后单击确定。

12.查看ECS实例的连接状态。

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。

1.2 Mac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Internet。
- 使用SSL-VPN功能，需要切换至新控制台，详情参见新控制台切换。
- 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。

完成以下操作，创建VPN网关：

1. 登录新版VPC管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关 。
3. 在VPN网关页面，单击创建VPN网关。
4. 在购买页面，配置VPN网关，完成支付。本操作中VPN网关的配置如下：
   - 地域：选择VPN网关的地域。本操作中选择华东1（杭州）。

     说明：

确保VPC的地域和VPN网关的地域相同。

- 专有网络： 选择要连接的VPC。
- 带宽规格：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
- IPsec-VPN： 选择是否开启IPsec-VPN功能，IPsec-VPN功能适用于站点到站点的连接，可以根据您的实际需要选择开启。
- SSL-VPN： 选择是否开启SSL-VPN功能。本操作选择开启。
- SSL并发连接数： 选择您需要同时连接的客户端最大规格。

5. 返回VPN网关页面，查看创建的VPN网关。

刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明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. 在专有网络的左侧导航栏，单击VPN > SSL服务端。
2. 单击创建SSL服务端。本操作中SSL服务端的配置如下：
   - 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。**

步骤三 创建客户端证书

完成以下操作，创建客户端证书：

1. **在专有网络的左侧导航栏，单击VPN > SSL客户端 。**
2. **单击创建SSL客户端证书。**
3. **在创建客户端证书对话框，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，然后单击下载下载生成的客户端证书。**

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：

   a. 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/*
   ```

   b. 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，比如： */Users/example/Downloads/certs6.zip*

   c. 执行以下命令解压证书文件：

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

   d. 执行以下命令发起连接：

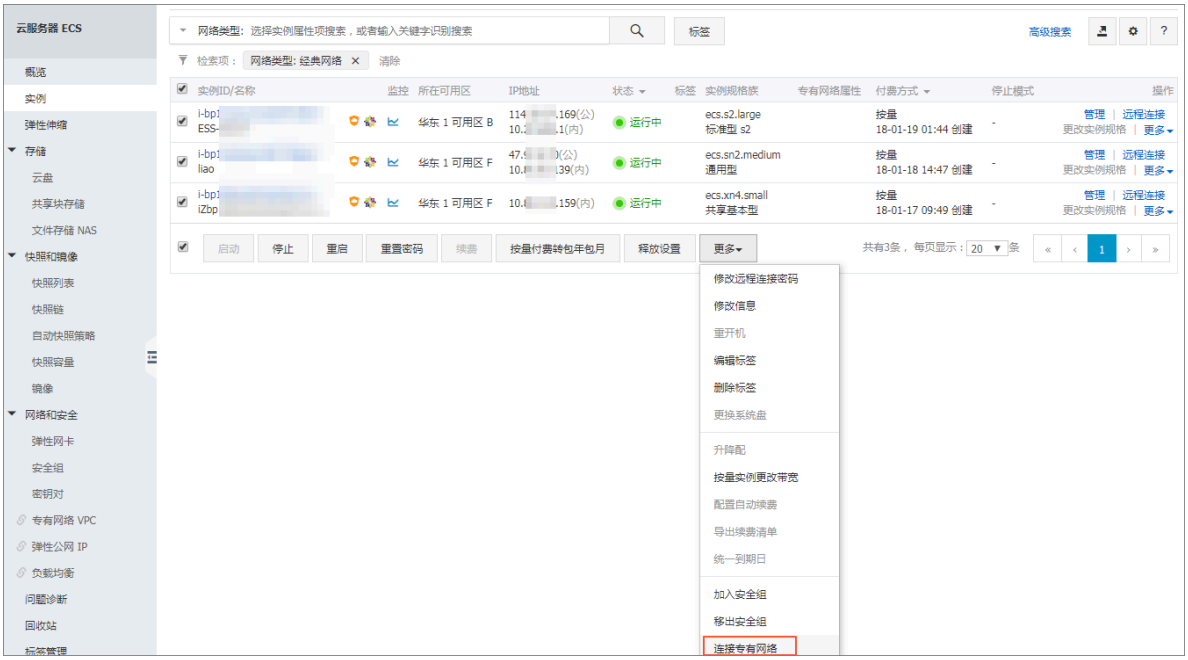
   ```
   sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
   ```

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ID链接。
3. 在专有网络详情页面，单击开启ClassicLink。
4. 在弹出的对话框，单击确定。
5. 登录ECS管理控制台。
6. 在左侧导航栏，单击实例。

7. 选择一个或多个目标经典网络的ECS实例，单击更多 > 连接专有网络 。



8. 在弹出的对话框中选择目标VPC，单击确定。
9. 在左侧导航栏，单击网络和安全 > 安全组 。
10. 在安全组列表页面，单击内网入方向页签，然后单击添加安全组规则。按照如下配置添加安全组规则：

   - 规则方向：入方向
   - 授权策略：允许
   - 协议类型：全部
   - 授权类型：地址段访问
   - 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Mac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。

```
        options=63<RXCSUM,TXCSUM,TSO4,TSO6>
        ether 6a:00:03:2f:1a:e0
        Configuration:
                id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
                maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
                root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
                ipfilter disabled flags 0x2
        member: en1 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 8 priority 0 path cost 0
        member: en2 flags=3<LEARNING,DISCOVER>
                ifmaxaddr 0 port 9 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
        options=6403<RXCSUM,TXCSUM,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        inet6 fe80::ded0:1bcd:d6f7:1d55%utun0 prefixlen 64 scopeid 0xb
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
        options=6403<RXCSUM,TXCSUM,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        inet 172.16.10.6 --> 172.16.10.5 netmask 0xffffffff
                k-Pro:~ $
                -Pro:~
```

11.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中连接状态，然后单击确定。

12.查看ECS实例的连接状态。

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。

1.3 Windows客户端

本文将介绍如何使用VPN网关的SSL-VPN功能从Windows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Internet。
- 使用SSL-VPN功能，需要切换至新控制台，详情参见新控制台切换。
- 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。

完成以下操作，创建VPN网关：

1. 登录新版VPC管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关 。
3. 在VPN网关页面，单击创建VPN网关。

4. 在购买页面，配置VPN网关，完成支付。本操作中VPN网关的配置如下：

- 地域：选择VPN网关的地域。本操作中选择华东1（杭州）。

> **说明：**
> 确保VPC的地域和VPN网关的地域相同。

- 专有网络： 选择要连接的VPC。
- 带宽规格：选择一个带宽规格。带宽规格是VPN网关所具备的公网带宽。
- IPsec-VPN： 选择是否开启IPsec-VPN功能，IPsec-VPN功能适用于站点到站点的连接，可以根据您的实际需要选择开启。
- SSL-VPN： 选择是否开启SSL-VPN功能。本操作选择开启。
- SSL并发连接数： 选择您需要同时连接的客户端最大规格。

5. 返回VPN网关页面，查看创建的VPN网关。

   刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态就表明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. 在专有网络的左侧导航栏，单击VPN > SSL服务端。
2. 单击创建SSL服务端。本操作中SSL服务端的配置如下：
   - 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。

步骤三 创建客户端证书

完成以下操作，创建客户端证书：

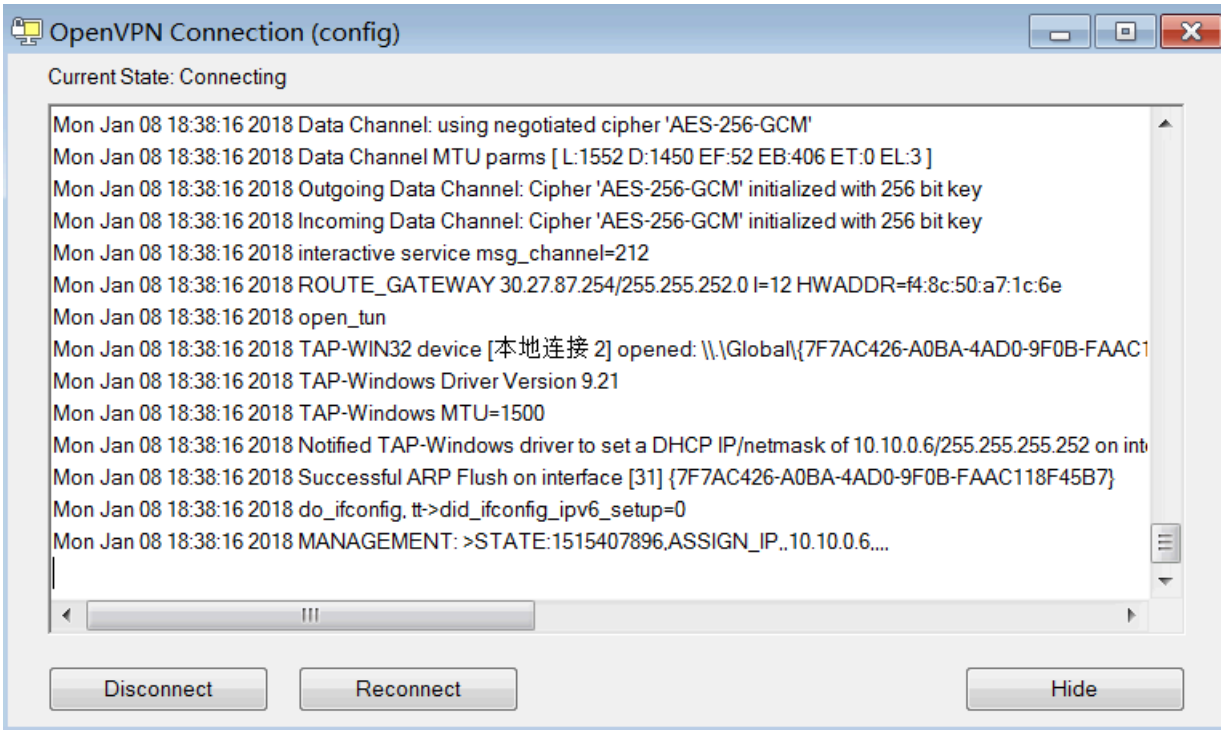
1. 在专有网络的左侧导航栏，单击VPN > SSL客户端 。
2. 单击创建SSL客户端证书。
3. 在创建客户端证书对话框，输入客户端证书名称并选择对应的SSL服务端，然后单击确定。
4. 在SSL客户端页面，找到已创建的客户端证书，然后单击下载下载生成的客户端证书。

步骤四 客户端配置

完成以下操作，配置客户端：

1. 下载并安装OpenVPN客户端。

2. 将步骤三中下载的证书解压后复制到OpenVPN安装目录中的*config*文件夹中。
3. 单击Connect发起连接。

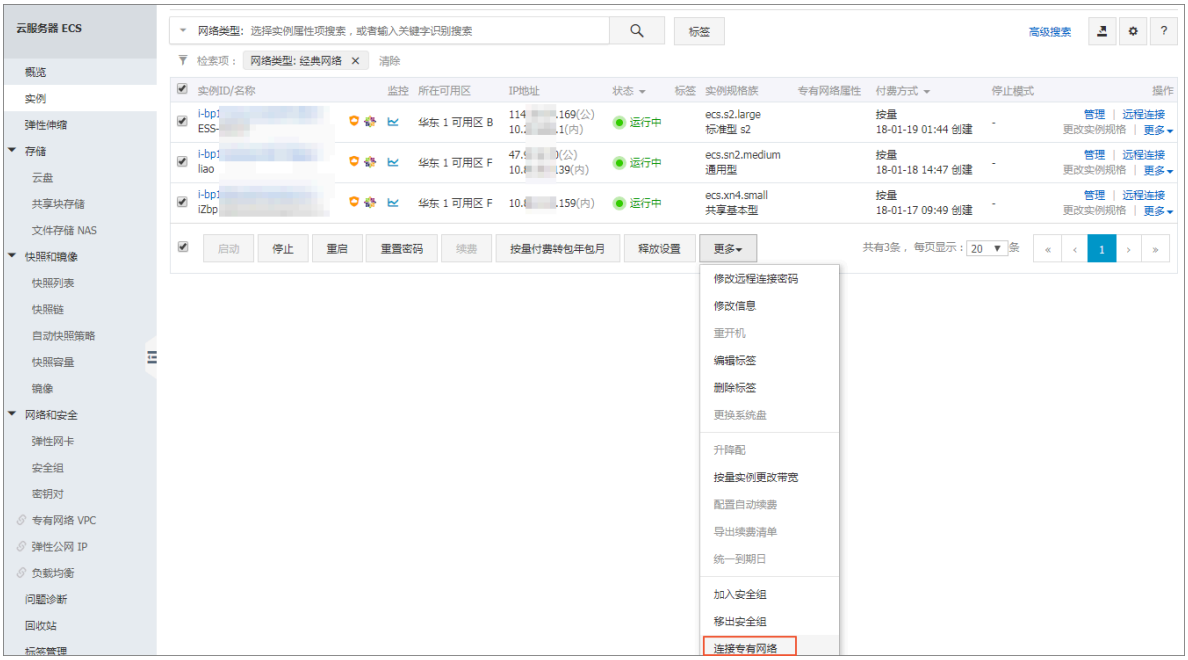


步骤五 建立ClassicLink连接

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ID链接。
3. 在专有网络详情页面，单击开启ClassicLink。
4. 在弹出的对话框，单击确定。
5. 登录ECS管理控制台。
6. 在左侧导航栏，单击实例。

7. 选择一个或多个目标经典网络的ECS实例，单击更多 > 连接专有网络 。



8. 在弹出的对话框中选择目标VPC，单击确定。

9. 在左侧导航栏，单击网络和安全 > 安全组 。

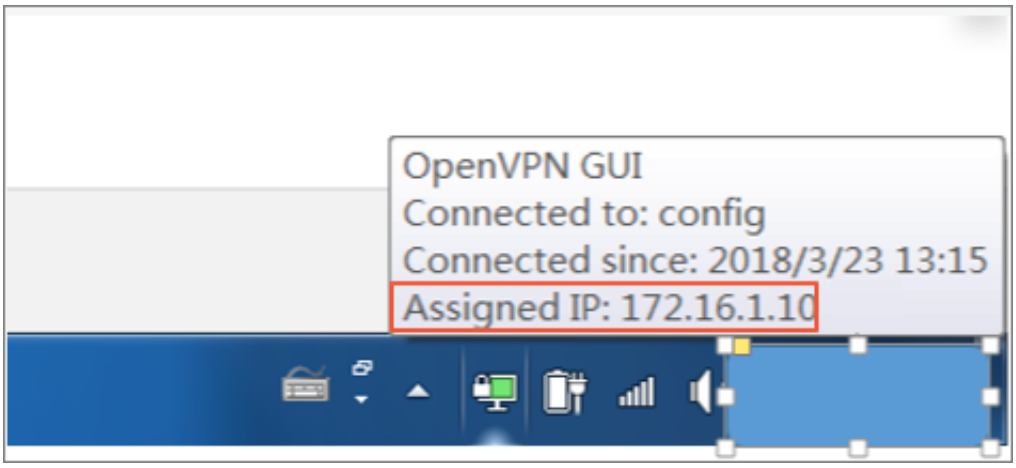
10. 在安全组列表页面，单击内网入方向页签，然后单击添加安全组规则。按照如下配置添加安全组规则：

   - 规则方向：入方向
   - 授权策略：允许
   - 协议类型：全部
   - 授权类型：地址段访问
   - 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172.16.1.10。

     您可以通过安装的OpenVPN客户端查看客户端IP，如下图所示。

     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。



11.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中连接状态，然后单击确定。

12.查看ECS实例的连接状态。

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 在经典网络中使用IPsec-VPN

您可以直接在专有网络中使用VPN网关通过IPSec-VPN功能建立站点到站点的连接。如果要在经典网络中使用VPN网关，需要配置ClassicLink。

前提条件

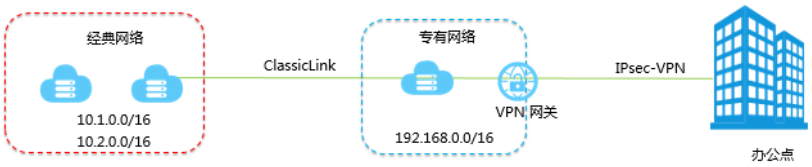
首先在开始前，需要做好网络规划：

- 本地客户端、办公点的私网网段必须属于VPC的私网网段，且不能和VPC内交换机的网段冲突，否则无法通信。
- 规划VPN网关所在的VPC，即云上VPN网关的网络环境，如果经典网络ECS不需要和已有VPC内的ECS通信，建议新建VPC用于经典网络的VPN连接。
- 您已经创建了一个VPC。VPC必须使用下表中的网段或其子集，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。
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。

背景信息

如果想在经典网络中使用VPN网关，首先在VPC内购买VPN网关，配置IPsec-VPN后IDC或者办公点可以接入VPC。然后经典网络ECS通过ClassicLink功能连接到VPC，再通过VPC中转实现本地办公点访问经典网络ECS。



操作步骤

1. 建立线下站点到VPC的IPsec-VPN连接。

   详情参见#unique_8。

2. 建立线下客户端到VPC的SSL-VPN连接。

   详情参见#unique_9。

3. 建立ClassicLink连接。

   详情参见#unique_10。

3 IPsec-VPN连接高可用

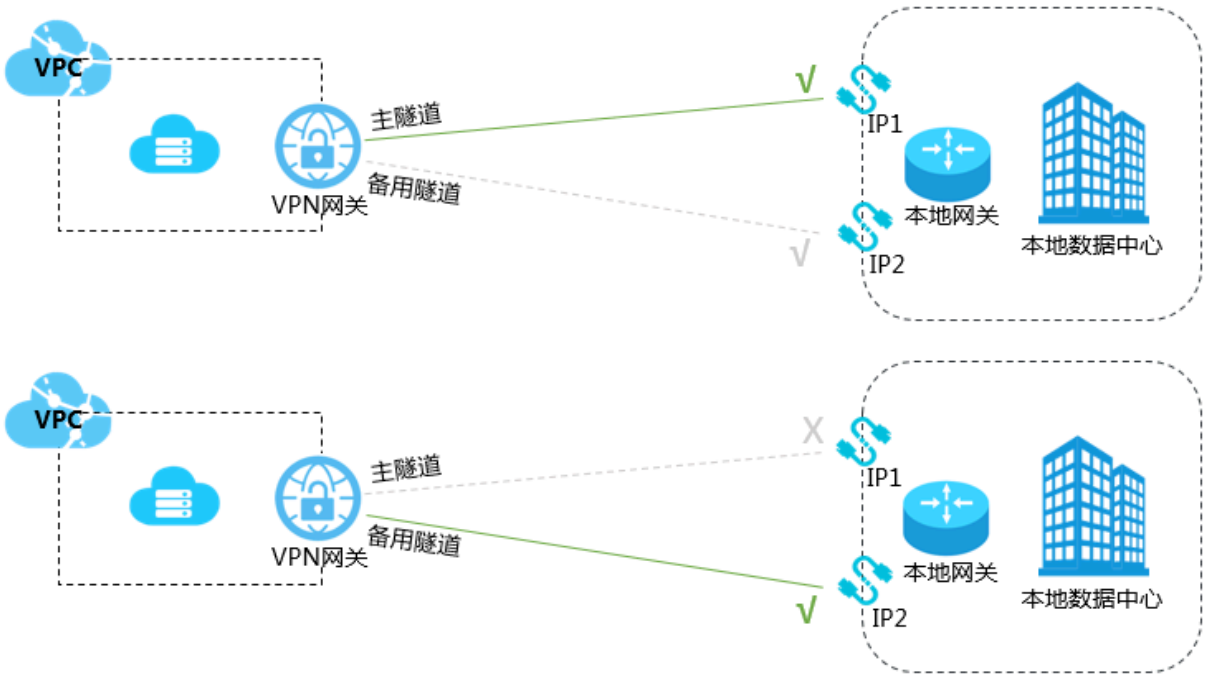
3.1 高可用-双IPsec隧道

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：

- 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，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和 Ixia等。
- 本地数据中心的网关已经配置了静态公网IP。
- 本地数据中心的网段和专有网络的网段不能重叠。

步骤一 创建VPN网关

完成以下操作，创建VPN网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关 。
3. 在VPN网关页面，单击创建VPN网关。
4. 在购买页面，根据以下信息配置VPN网关，然后单击立即购买完成支付。
   - 实例名称：输入VPN网关的实例名称。
   - 地域：选择VPN网关的地域。

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

     说明:
     本选项只有在选择开启了SSL-VPN功能后才可配置。
   - 计费周期：选择购买时长。
5. 返回VPN网关页面，查看创建的VPN网关。

   刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态表明VPN网关完成了初始化，可以正常使用了。

   说明:
   VPN网关的创建一般需要1-5分钟。

步骤二 创建用户网关

完成以下操作，创建两个用户网关，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

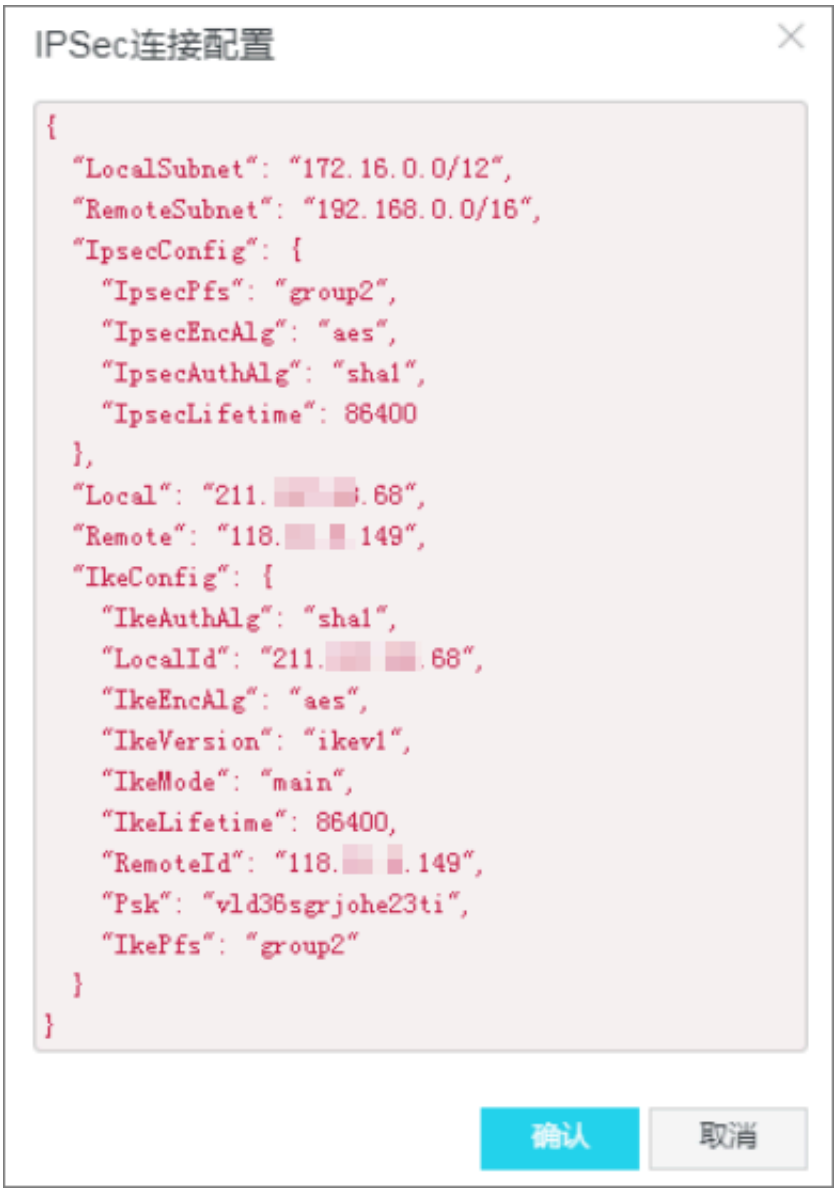
完成以下操作，在本地网关设备中加载VPN配置。

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。详细说明，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。

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
本地网关的私网网段	IPsec连接实例2	是	0

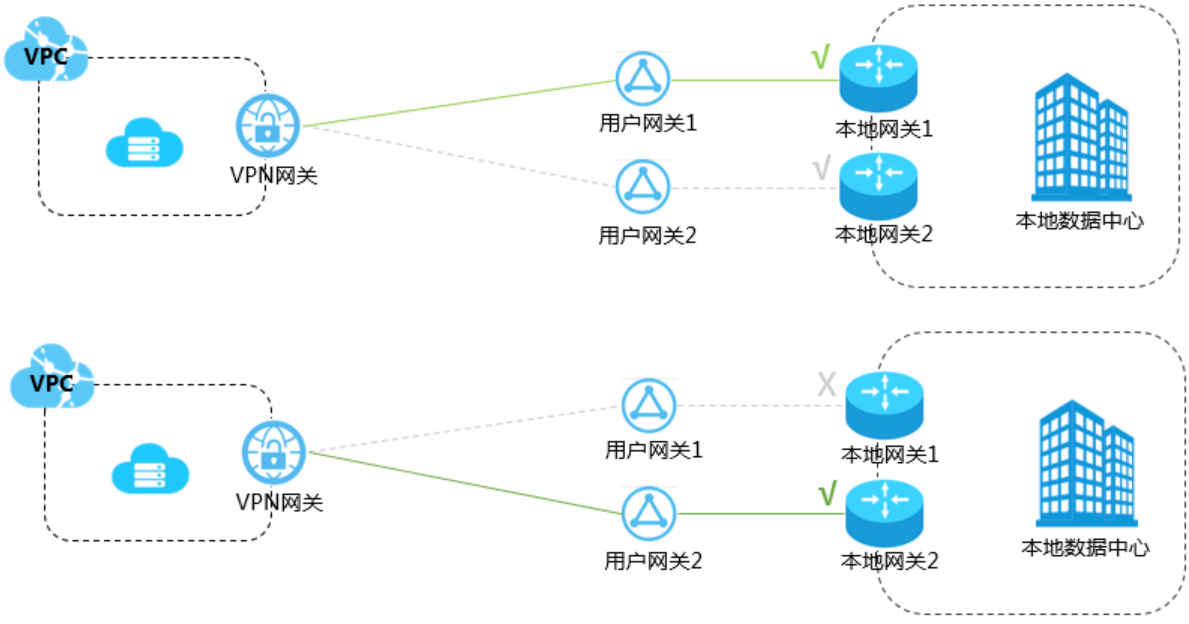
3.2 高可用-双用户网关

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，比如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM 和 Ixia等。
- 本地数据中心的网关已经配置了静态公网IP。
- 本地数据中心的网段和专有网络的网段不能重叠。

步骤一 创建VPN网关

完成以下操作，创建VPN网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关 。
3. 在VPN网关页面，单击创建VPN网关。
4. 在购买页面，根据以下信息配置VPN网关，然后单击立即购买完成支付。
   - 实例名称：输入VPN网关的实例名称。
   - 地域：选择VPN网关的地域。

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

     
     说明:
     本选项只有在选择开启了SSL-VPN功能后才可配置。
   - 计费周期：选择购买时长。

5. 返回VPN网关页面，查看创建的VPN网关。

   刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态表明VPN网关完成了初始化，可以正常使用了。

   说明:

   VPN网关的创建一般需要1-5分钟。

步骤二 创建用户网关

完成以下操作，创建两个用户网关，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

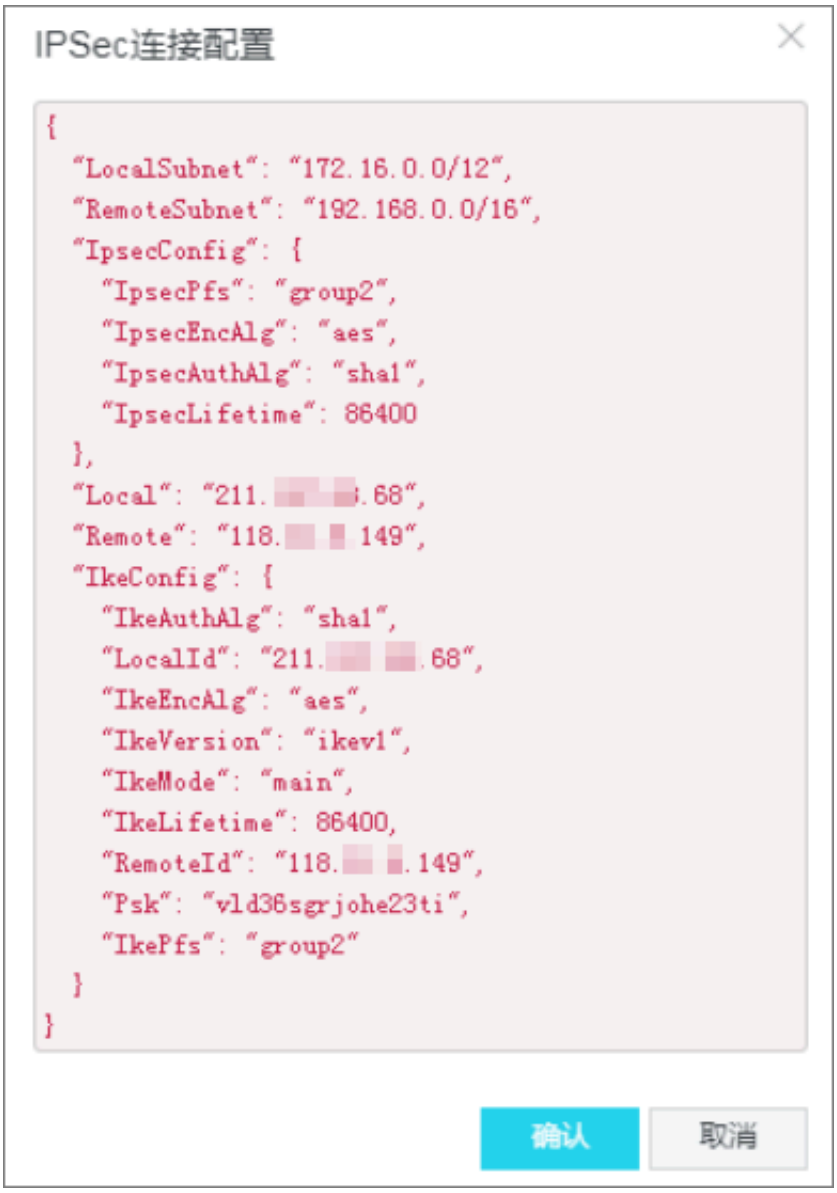
完成以下操作，分别在本地网关设备中加载VPN配置。

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。详细说明，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。

   本示例目的路由如下表：

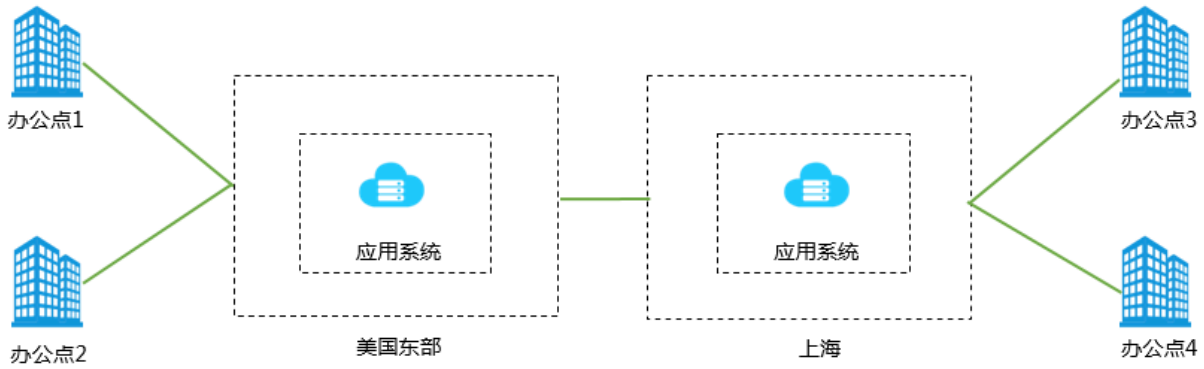
目标网段	下一跳	发布到VPC	权重
本地网关的私网网段	IPsec连接实例1	是	100
本地网关的私网网段	IPsec连接实例2	是	0

4 IPsec-VPN配合云企业网搭建高速全球网络

对于跨国企业，可以利用云企业网（CEN）降低跨国线路延迟，利用VPN网关低成本解决最后一公里接入和终端接入问题，构建跨国企业网络。

案例分析

大型跨国公司经常有在多个国家部署应用系统并与世界各地的办公运维系统互连的需求，例如某企业需要在美国东部和上海分别部署两套应用系统，同时与位于各地的办公地点互连，如下图所示。



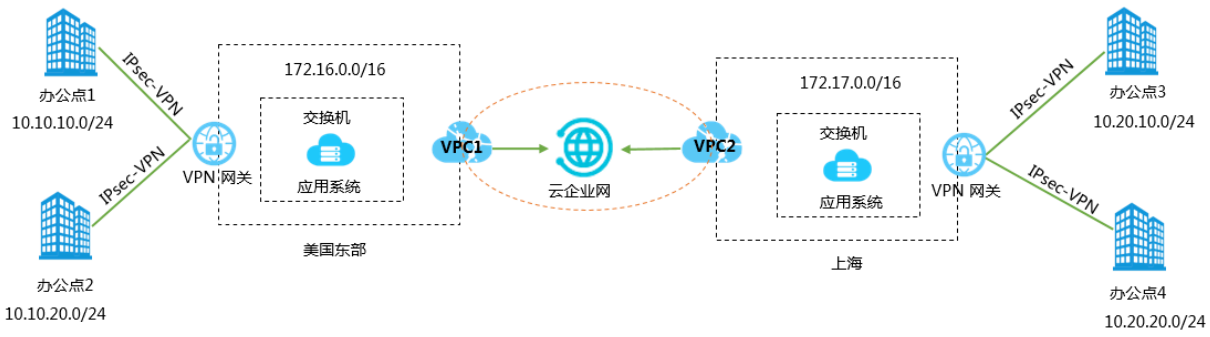
方案概述

对于全球办公地点间的通信需求，传统的解决方案和问题如下表所示。

传统解决方案	问题
通过Internet直接通信	内部数据直接暴露在Internet上且Internet的网络质量无法保证。
通过IPsec VPN通信	安全性高但是通信仍基于Internet，跨国通信时网络质量受Internet影响。
通过专线直连	安全性高且网络质量好，但成本极高。

阿里云提供一种安全性高、网络质量好且成本相对较低的解决方案，即通过VPN网关和云企业网连接世界各地的应用系统和办公地点。

如下图所示，若要实现美国东部和上海各办公点间的互连需求，您可以分别在美国东部和上海的VPC内部署应用系统，VPC间通过云企业网连接，两个地域的办公地点通过IPsec-VPN分别接入到两个VPC的VPN网关，实现全球办公网络互联。



前提条件

- 已部署好云上环境即创建了VPC和交换机，并部署了相关应用。
- 各办公点已经部署了本地网关，且配置了一个静态公网IP。
- 需要互连的各网段不能冲突。

步骤一 创建美国东部办公点的IPsec连接

1. 为美国东部的VPC创建一个VPN网关。详细说明，请参见#unique_16/unique_16_Connect_42_section_zv3_nyf_xdb。
2. 创建两个用户网关，将办公地点网关设备的公网IP地址注册到用户网关中用于建立IPsec连接。

   用户网关的IP地址是办公地点网关设备的公网IP地址。详细说明，请参见#unique_17/unique_17_Connect_42_section_mwf_lxc_xdb。
3. 创建两个IPsec连接，将VPN网关和用户网关连接起来。详细说明，请参见#unique_18/unique_18_Connect_42_section_mxd_fyc_xdb。
4. 在本地办公地点网关设备中加载VPN配置。

   根据本地办公地点网关设备的要求，加载VPN配置。详细说明，请参见本地网关配置。
5. 配置VPN网关路由。详细说明，请参见#unique_19。

步骤二 创建上海办公点的IPsec连接

参见步骤一，创建上海办公点与VPC之间的IPsec连接。

步骤三 连接VPC

您可以通过云企业网功能，连接两个地域的VPC。详细说明，请参见#unique_20。

步骤四 在CEN中宣告路由

您可以将VPC中指向VPN网关的路由发布到CEN中，CEN中其他加载的网络实例便可以学习到该条路由。

详细信息，请参见#unique_21/unique_21_Connect_42_section_qts_1ct_q2b。

步骤五 配置安全组

根据您的业务需求，为部署应用系统的ECS实例配置安全组规则。

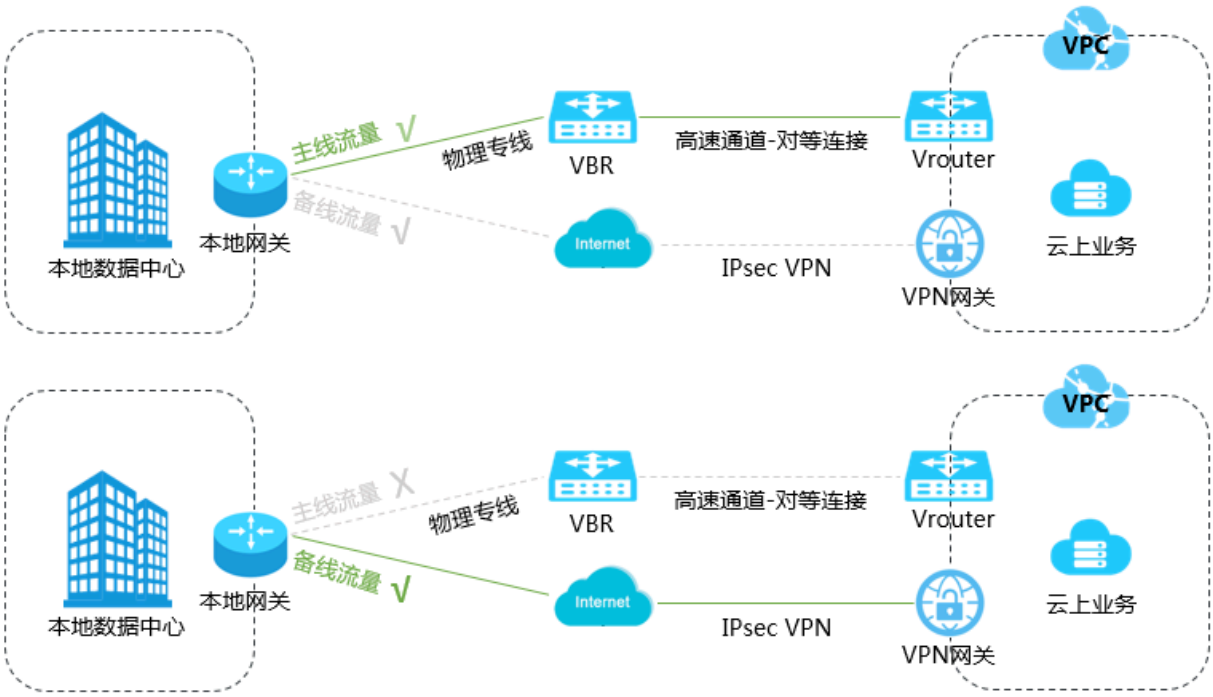
至此各个办公地点与应用系统间的连接建立完成，办公地点与应用系统间可以进行安全、高效的内网通信。

5 IPsec-VPN配合专线实现主备冗余

您可以通过VPN网关配合高速通道物理专线实现主备冗余，保证本地应用的高可用。

本地数据中心与VPC既通过物理专线连接，又通过IPsec-VPN连接。

- 当物理专线正常时，本地数据中心与VPC之间的所有流量只通过物理专线转发。
- 当物理专线异常时，本地数据中心与VPC之间的所有流量切换至VPN线路。



前提条件

您已经接入物理专线，实现了VPC和本地IDC的互通。

详细信息，请参见#unique_23。

步骤一 创建VPN网关

完成以下操作，创建VPN网关。

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击VPN > VPN网关 。
3. 在VPN网关页面，单击创建VPN网关。

4. 在购买页面，根据以下信息配置VPN网关，然后单击立即购买完成支付。
   - 实例名称：输入VPN网关的实例名称。
   - 地域：选择VPN网关的地域。

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

     说明:
     本选项只有在选择开启了SSL-VPN功能后才可配置。
   - 计费周期：选择购买时长。
5. 返回VPN网关页面，查看创建的VPN网关。

   刚创建好的VPN网关的状态是准备中，约两分钟左右会变成正常状态。正常状态表明VPN网关完成了初始化，可以正常使用了。

   说明:
   VPN网关的创建一般需要1-5分钟。

步骤二 创建用户网关

完成以下操作，创建一个用户网关，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。

步骤三 创建IPsec连接

完成以下操作，创建IPsec连接。

1. 在左侧导航栏，单击VPN > IPSec连接。
2. 选择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。

步骤四 在本地网关设备中加载VPN配置

完成以下操作，在本地网关设备中加载VPN配置。

1. 在左侧导航栏，单击VPN > IPsec连接。
2. 选择IPsec连接的地域。
3. 在IPsec连接页面，找到目标IPsec连接，然后单击操作列下的下载对端配置。
4. 根据本地网关设备的配置要求，将下载的配置添加到本地网关设备中。详细信息，请参见本地网关配置。

   下载配置中的RemotSubnet和LocalSubnet与创建IPsec连接时的本端网段和对端网段是相反的。因为从阿里云VPN网关的角度看，对端是用户IDC的网段，本端是VPC网段；而从本地网关设备的角度看，LocalSubnet就是指本地IDC的网段，RemotSubnet则是指阿里云VPC的网段。

步骤五 配置VPN网关路由

完成以下操作，配置VPN网关路由。

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

步骤六 配置VBR专线健康检查

您需要为VBR专线配置健康检查，确保阿里云VPC内网络能感知专线状态，并在专线异常时，主动将流量切换到VPN线路。

详细信息，请参见#unique_24。

步骤七 配置本地网关

您需要在专线接入设备上配置指向VPC的主备路由，并配置针对物理专线的健康探测，当物理专线异常时，主动将流量切换到VPN线路。