

阿里云 VPN网关

最佳实践




文档版本：20181129

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。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid Instance_ID</code>
[]或者[a b]	表示可选项，至多选择一个。	<code>ipconfig [-all/-t]</code>
{ }或者{a b}	表示必选项，至多选择一个。	<code>swich {stand slave}</code>

目录

法律声明.....	I
通用约定.....	I
1 本地网关配置.....	1
1.1 华三防火墙配置.....	1
1.2 strongSwan配置.....	6
2 配置多站点连接.....	9
3 VPN网关配合高速通道搭建高速全球网络.....	12
4 在经典网络中使用IPsec-VPN.....	16

1 本地网关配置

1.1 华三防火墙配置

使用IPsec-VPN建立站点到站点的连接时，在配置完阿里云VPN网关后，您还需在本地站点的网关设备中进行VPN配置。本文以华三防火墙为例介绍如何在本地站点中加载VPN配置。

前提条件

- 确保您已经在阿里云VPC内创建了IPsec连接，详情参见[配置站点到站点连接](#)。
- 创建IPsec连接后，获取的IPsec配置信息，详情参见[IPsec连接管理](#)。

本操作的IPsec连接配置如下表所示。

— IPsec协议信息

配置		示例值
IKE	认证算法	sha1
	加密算法	aes
	DH分组	group2
	IKE版本	ikev1
	生命周期	86400
	协商模式	main
	PSK	h3c
IPsec	认证算法	sha1
	加密算法	aes
	DH分组	group2
	IKE版本	ikev1
	生命周期	86400
	安全协议	esp

— 网络配置信息

配置		示例值
VPC配置	私网CIDR	192.168.10.0/24

配置		示例值
IDC网络配置	网关公网IP	101.xxx.xxx.127
	私网CIDR	192.168.66.0/24
	网关公网IP	122.xxx.xxx.248
	上行公网网口	Reth 1
	下行私网网口	G 2/0/10

操作步骤

1. 登录防火墙Web页面，单击网络 > VPN > IPsec > 策略。
2. 根据阿里云VPN连接的IPsec协议信息配置IDC的H3C防火墙IPsec策略。并在保护的数据流列表中单击添加加入保护的感兴趣流，感兴趣流源IP和目的IP分别为IDC和阿里云VPC的网段。

新建IPsec策略

基本配置

接口: Reth1 *

IP地址类型: ☒ IPv4 ☐ IPv6

优先级: 1 * (1-65535)

模式: ☒ 对等/分支节点 ☐ 中心节点

对端IP地址/主机名: 101.132.122.127 * (1-253字符)

协商模式: ☒ 主模式 ☐ 野蛮模式

认证方式: 预共享密钥

预共享密钥: ... * (1-128字符)

再次输入预共享密钥: ...

IKE提议: 优先级 (认证算法; 加密算法; DH) *

对端ID: IPv4 地址 101.132.122.127 *

本端ID: IPv4 地址 122.225.207.248

描述: (1-80字符)

保护的数据流

+ 添加 - 删除 + 插入

源IP地址	目的IP地址	协议	源端口	目的端口	动作
192.168.66.0/255.255....	192.168.10.0/255.255....	any	any	any	保护

3. 单击IKE提议 > 新建。

根据阿里云VPN连接的IKE协议信息配置IDC的IKE协议。

优先级	19	* (1-65535)
认证方式	预共享密钥	
认证算法	SHA1	
加密算法	AES-CBC-128	
DH	DH group 2	
IKE SA 生存周期	86400	秒 (60-604800)

确定 取消

4. 单击网络 > VPN > IPsec > 策略。
5. 选择刚刚新建的IPsec策略，单击高级配置配置IPsec协议。

根据阿里云VPN连接的IPsec协议信息配置IPsec协议。

共 1 条

高级配置

☒ IPsec参数

封装模式 ☒ 隧道模式 ☐ 传输模式

安全协议 ☒ ESP ☐ AH ☐ AH-ESP

ESP认证算法 SHA1

ESP加密算法 AES-CBC-128

PFS Group_2

IPsec SA生存时间 86400 秒 (180-604800)

基于时间

基于流量

IPsec SA 空闲超时时间 122.225.207.248 秒 (60-86400)

DPD检测 ☒ 开启

QoS预分类 ☒ 开启

确定 取消

分别创建上行安全策略和下行安全策略：

- 从阿里云VPC到本地IDC的安全策略配置如下图所示。

6. 单击策略 > 安全策略 > 新建。

从阿里云VPC到本地IDC的安全策略配置如下图所示。

名称	<input type="text" value="aliyun_to_h3c"/>	* (1-127
源安全域	<input type="text" value="Untrust"/>	[多选]
目的安全域	<input type="text" value="Trust"/>	[多选]
类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	
描述信息	<div></div>	(1-127字
动作	<input checked="" type="radio"/> 允许 <input type="radio"/> 拒绝	
源IP地址	<input type="text" value="192.168.10.0/24"/>	[多选]
目的IP地址	<input type="text" value="192.168.66.0/24"/>	[多选]
服务	<input type="text" value="请选择服务"/>	[多选]
应用	<input type="text" value="请选择应用"/>	[多选]
应用组	<input type="text" value="请选择应用组"/>	[多选]
用户	<input type="text" value="请选择或输入用户"/>	[多选]
时间段	<input type="text" value="请选择时间段"/>	
VRF	<input type="text" value="公网"/>	
内容安全		
IPS策略	<input type="text" value="-NONE-"/>	
数据过滤策略	<input type="text" value="-NONE-"/>	
文件过滤策略	<input type="text" value="-NONE-"/>	
防病毒策略	<input type="text" value="-NONE-"/>	
URL过滤策略	<input type="text" value="-NONE-"/>	
记录日志	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭	
开启策略匹配统计	<input type="radio"/> 开启 <input checked="" type="radio"/> 关闭	
会话老化时间	<input type="checkbox"/> 启用	
<div>确定取消</div>		

从本地IDC到阿里云VPC的安全策略配置如下图所示。

名称

h3c_to_aliyun

*

(1-127字符)

源安全域

Trust

[多选]

目的安全域

Untrust

[多选]

类型

☒ IPv4

☐ IPv6

描述信息

(1-127字符)

动作

☒ 允许

☐ 拒绝

源IP地址

192.168.66.0/24

[多选]

目的IP地址

192.168.10.0/24

[多选]

服务

请选择服务

[多选]

应用

请选择应用

[多选]

应用组

请选择应用组

[多选]

用户

请选择或输入用户

[多选]

时间段

请选择时间段

VRF

公网

内容安全

IPS策略

-NONE-

数据过滤策略

-NONE-

文件过滤策略

-NONE-

防病毒策略

-NONE-

URL过滤策略

-NONE-

记录日志

☐ 开启

☒ 关闭

开启策略匹配统计

☐ 开启

☒ 关闭

会话老化时间

☐ 启用

确定

取消

7. 单击网络 > 路由 > 静态路由。
8. 添加缺省路由，使出方向流量走上行接口，本例中下行接口为直连路由，无需配置。

新建IPv4静态路由

VRF

公网

目的IP地址

0.0.0.0

掩码长度

0

下一跳

☒ 下一跳所属的VRF

公网

☐ 出接口

下一跳IP地址

122.225.207.1

路由优先级

60

路由标记

0

描述

确定

取消

1.2 strongSwan配置

使用IPsec-VPN建立站点到站点的连接时，在配置完阿里云VPN网关后，您还需在本地站点的网关设备中进行VPN配置。本文以strongSwan为例介绍如何在本地站点中加载VPN配置。

本文以strongSwan为例介绍如何在本地站点中加载VPN配置。本操作中作为示例的配置信息如下：

- 阿里云VPC的网段是192.168.10.0/24
- 本地IDC的网段是172.16.2.0/24
- strongSwan的公网IP地址是59.110.165.70



前提条件

- 确保您已经在阿里云VPC内创建了IPsec连接，详情参见[配置站点到站点连接](#)。
- 创建IPsec连接后，获取的IPsec配置信息，详情参见[IPsec连接管理](#)。

安装strongSwan

1. 运行以下命令安装strongSwan。

```
# yum install strongswan
```

2. 运行以下命令查看安装的软件版本。

```
# strongswan version
```

配置strongSwan

1. 运行以下命令打开ipsec.conf配置文件。

```
# vi /etc/strongswan/ipsec.conf
```

2. 参考以下配置，更改ipsec.conf的配置。

```
# ipsec.conf - strongSwan IPsec configuration file
# basic configuration
config setup
    uniqueids=never
conn %default
    authby=psk
    type=tunnel
conn tomyidc
    keyexchange=ikev1
    left=59.110.165.70
    leftsubnet=172.16.2.0/24
    leftid=59.110.165.70 ( IDC网关设备的公网IP )
    right=119.23.227.125
    rightsubnet=192.168.10.0/24
    rightid=119.23.227.125 ( VPN网关的公网IP )
    auto=route
```

```
ike=aes-sha1-modp1024
ikelifetime=86400s
esp=aes-sha1-modp1024
lifetime=86400s
type=tunnel
```

3. 配置`ipsec.secrets`文件。

a. 运行以下命令打开配置文件。

```
# vi /etc/strongswan/ipsec.secrets
```

b. 添加如下配置。

```
59.110.165.70 119.23.227.125 : PSK yourpassword
```

4. 打开系统转发配置。

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

更多场景配置样例，参见[场景配置样例](#)。

5. 执行以下命令启动strongSwan服务。

```
# systemctl enable strongswan
# systemctl start strongswan
```

6. 设置IDC客户端到strongSwan网关及网关下行到客户端路由。

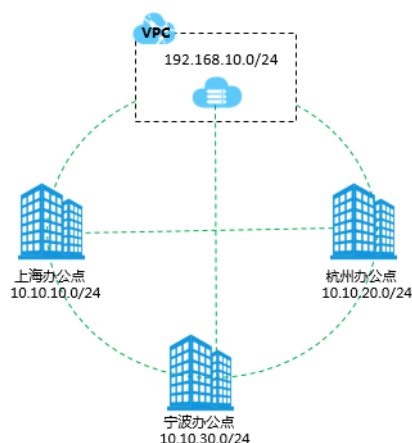
2 配置多站点连接

您可以通过VPN-Hub功能在多个站点之间建立安全通信，使各个站点不仅可以和云上VPC互通，并且远程站点之间可以彼此通信。VPN-Hub连接可满足大型企业在各个办公点之间建立内网通信的需求。

VPN-Hub介绍

VPN-Hub功能随VPN网关默认开启，您只需要配置各个办公点到云上的IPsec连接，不需要额外付款或者额外的配置。每个VPN网关最多可支持10个连接，即购买一个VPN网关，就可以将10个不同地点的办公点连接起来。

本文以下图中的应用场景为例，演示如何创建多个IPsec连接将上海、杭州、宁波三个办公点连接起来。在开始之前，确保您已经获取各办公点的网关设备的公网IP地址。

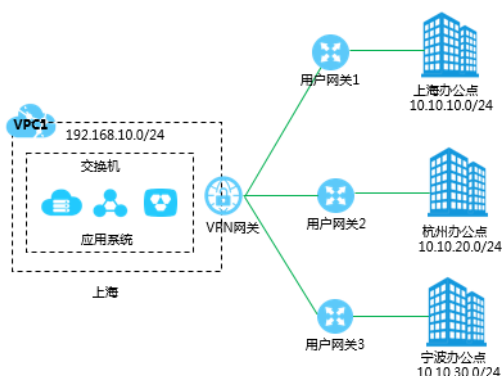


如下图所示，要将上海、杭州、宁波三个办公点连接起来，您只需要创建一个VPN网关，三个用户网关，建立三个IPsec连接即可。



说明：

确保所有的IP地址段都不冲突，否则无法进行通信。



步骤一 创建VPN网关

在VPC的所属地域创建一个VPN网关，该VPN网关将建立三个IPsec连接，分别连接上海、杭州和宁波办公点。详情参见[VPN网关管理](#)。



说明：

确保开启IPsec-VPN功能。

步骤二 建立上海办公点的IPsec连接

1. 创建用户网关，将本地网关设备的公网IP地址注册到云上用来建立IPsec连接。

用户网关的IP地址是上海办公点的网关设备的公网IP地址，详情参见[创建用户网关](#)。

2. 创建IPsec连接。

创建一个IPsec连接，将VPN网关和用户网关连接起来。本操作中的网段配置如下，详情参见[创建IPsec连接](#)。

- 本端网段：输入0.0.0.0/0。



说明：

建议您VPN连接阿里云侧网段设置为0.0.0.0/0，这样可以极大地简化网络拓扑，每个办公点只需要建立一条到云端的VPN连接，且后续增加新的办公点不需要修改已有的配置。

- 对端网段：本地IDC的网段，本教程中是上海办公点的网段即10.10.10.0/24。

3. 在本地办公点网关设备中加载VPN配置。

根据本地办公点网关设备的要求，加载VPN配置。详情参见[本地网关配置](#)。

步骤三 建立杭州和宁波办公点的IPsec连接

参考步骤二，分别建立杭州和宁波办公点的IPsec连接。

步骤四 在VPC中配置路由

1. 登录专有网络管理控制台。
2. 在左侧导航栏，单击路由表，找到目标VPC的路由表，然后单击管理。
3. 在路由表页面，单击添加路由条目添加如下三条路由。

目标网段	下一跳类型	下一跳
10.10.10.0/24	VPN网关	步骤一中创建的VPN网关
10.10.20.0/24	VPN网关	步骤一中创建的VPN网关
10.10.30.0/24	VPN网关	步骤一中创建的VPN网关

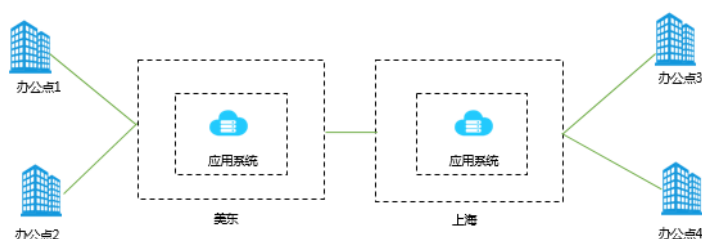
至此三个办公点的VPN连接已经建立，三个办公点之间和VPC之间彼此可以进行内网通信。

3 VPN网关配合高速通道搭建高速全球网络

对于跨国企业，可以利用高速通道降低跨国线路延迟，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。



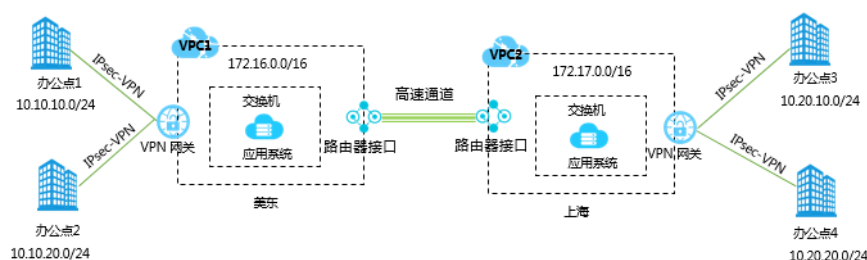
方案概述

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网关和高速通道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间通过高速通道连接，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

您可以通过VPN网关的VPN-Hub功能实现多个办公点间和VPC之间的内网通信，详情参见[配置多站点连接](#)。

1. 为美东地域的VPC创建一个VPN网关，详情参见[创建VPN网关](#)。
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，详情参见[创建用户网关](#)。

3. 创建两个IPsec连接，将VPN网关和用户网关连接起来。详情参见[创建IPsec连接](#)。

- 本端网段：输入0.0.0.0/0。



说明：

建议您VPN连接阿里云侧网段设置为0.0.0.0/0，这样可以极大地简化网络拓扑，每个办公点只需要建立一条到云端的VPN连接，且后续增加新的办公点不需要修改已有的配置。

- 对端网段：分别为办公地点1和办公点2的网段，即10.10.10.0/24和10.10.20.0/24。

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。详情参见[本地网关配置](#)。

步骤二 创建上海办公点的IPsec连接

参考步骤一，创建上海办公点与VPC之间的IPsec连接。

步骤三 连接VPC

您可以通过使用高速通道的路由器接口功能，连接两个地域的VPC，详情参见[VPC互连](#)。

本操作中的路由器接口配置如下图所示。

高速通道（按量付费）

预付费

按量付费

连接场景

VPC互连

专线接入

创建路由场景

同时创建两端

只创建发起端

只创建接收端

路由器类型

VPC路由器

地域

华北2（北京）

华东1（杭州）

华东2（上海）

华南1（深圳）

华北1（青岛）

香港

亚太（新加坡）

美西（硅谷）

美东（弗吉尼亚）

欧洲中部1（法兰克福）

中东东部1（迪拜）

亚太东南2（悉尼）

华北3（张家口）

亚太东北1（东京）

马来西亚（吉隆坡）

内蒙古

本端VPC ID

vpc-2

对端地域

华北2（北京）

华东1（杭州）

华东2（上海）

华南1（深圳）

华北1（青岛）

香港

亚太（新加坡）

美西（硅谷）

美东（弗吉尼亚）

欧洲中部1（法兰克福）

中东东部1（迪拜）

亚太东南2（悉尼）

华北3（张家口）

亚太东北1（东京）

马来西亚（吉隆坡）

内蒙古

对端路由器类型

VPC路由器

对端VPC ID

vpc-2r

规格

大型2档(2Gb)

当前配置

连接场景

VPC互连

创建路由场景...

同时创建两端

路由器类型

VPC路由器

地域

本端VPC ID

对端地域

对端路由器类

对端VPC ID

规格

大型2档(2Gb)

计费周期

1天

配置费用

立即购买

步骤四 在VPC内配置路由

- 1. 登录专有网络管理控制台。
- 2. 在左侧导航栏，单击路由表，找到目标VPC的路由表，然后单击管理。
- 3. 在路由表页面，单击添加路由条目添加如下三条路由。

下表是美东VPC1 (172.16.0.0/16) 的路由配置：

目标网段	下一跳类型	下一跳	说明
10.10.10.0/24 (美东办公点1的网段)	VPN网关	VPC1的VPN网关	将去往该网段的流量转发到美东地域的VPN网关中。
10.10.20.0/24 (美东办公点2的网段)	VPN网关	VPC1的VPN网关	
172.17.0.0/16 (上海VPC的网段)	VPC	VPC2	将去往该网段的流量转发到上海地域的VPC2中。
10.20.10.0/24 (上海办公点3的网段)	VPC	VPC2	

目标网段	下一跳类型	下一跳	说明
10.20.20.0/24 (上海办公点4的网段)	VPC	VPC2	

4. 在VPC2内配置如下路由。

目标网段	下一跳类型	下一跳	说明
10.20.10.0/24 (上海办公点3的网段)	VPN网关	VPC2的VPN网关	将去往该网段的流量转发到上海地域的VPN网关中。
10.20.20.0/24 (上海办公点4的网段)	VPN网关	VPC2的VPN网关	
172.16.0.0/16 (美东VPC的网段)	VPC	VPC1	将去往该网段的流量转发到上海地域的VPC1中。
10.10.10.0/24 (美东办公点1的网段)	VPC	VPC1	
10.10.20.0/24 (美东办公点2的网段)	VPC	VPC1	

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。


4 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

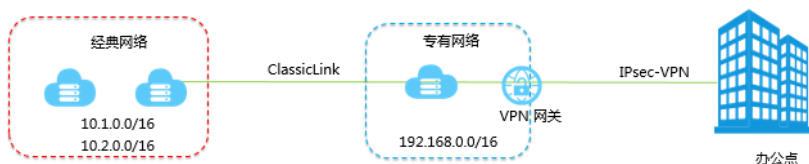
首先在开始前，需要做好网络规划：

- 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	<ul style="list-style-type: none">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。 <div> 说明： 在运行脚本前，请仔细阅读脚本中包含的readme文件。</div>

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[配置站点到站点连接](#)。

2. 建立线下客户端到VPC的SSL-VPN连接。

详情参见[Linux客户端远程连接](#)。

3. 建立ClassicLink连接。

详情参见[建立ClassicLink连接](#)。