阿里云
VPN网关

SSL-VPN入门

文档版本：20190415

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 教程概述

本教程为您介绍如何通过SSL-VPN功能远程接入VPC。

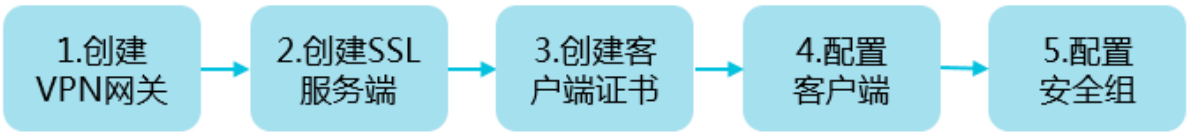
前提条件

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

配置流程说明

通过SSL-VPN功能远程接入VPC的流程图如下：



1. 创建VPN网关

   创建VPN网关并开启SSL-VPN功能。

2. 创建SSL服务端

   在SSL服务端中指定要连接的IP地址段和客户端连接时使用的IP地址段。

3. 创建客户端证书

   根据服务端配置，创建客户端证书，下载客户端证书和配置。

4. 配置客户端

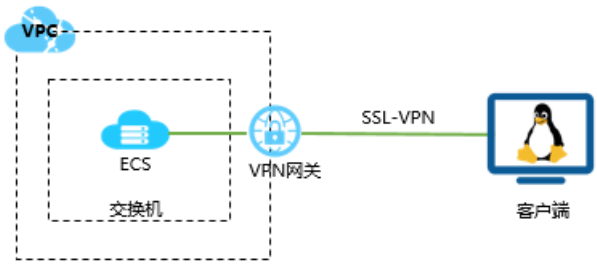
   在客户端中下载安装客户端VPN软件，加载客户端证书和配置，发起连接即可。

5. 配置安全组

   确保ECS的安全组规则允许客户端访问。

2 Linux客户端远程连接

本文以Linux操作系统的客户端为例介绍如何通过VPN网关拨号接入VPC。



开始之前

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

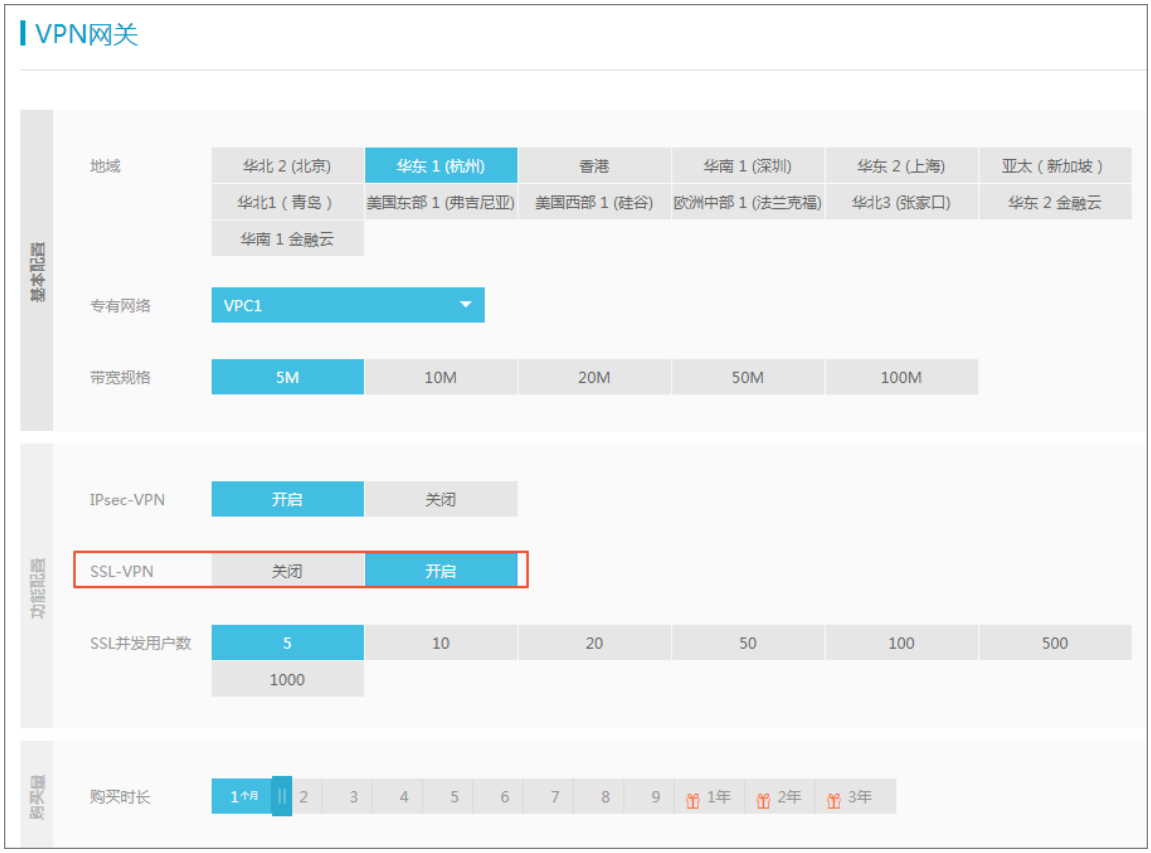
步骤一 创建VPN网关

1. 登录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。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。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。

     说明:

本选项只有在选择开启了SSL-VPN功能后才可配置。



5. 返回VPN网关页面，选择华东1地域，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

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网络。单击添加本端网段添加多个本端网段，本端网段可以是任何VPC或交换机的网段，也可以是本地网络的网段。
   - 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。
   - 高级配置：使用默认高级配置。

步骤三 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

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 连接测试

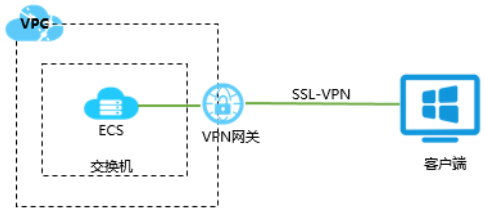
在客户端ping已连接的VPC内的一台ECS实例，测试连通性。

> **说明:**
> 确保测试的ECS实例的安全组规则允许客户端远程连接。详情参考*#unique_5*。


添加安全组规则
网卡类型：
内网
规则方向：
入方向
授权策略：
允许
协议类型：
全部
* 端口范围：
-1/-1
优先级：
1
授权类型：
地址段访问
* 授权对象：
10.10.0.0/24
教我设置
描述：
长度为2-256个字符，不能以http://或https://开头。
确定
取消

3 Windows客户端远程连接

本文以Windows操作系统的客户端为例介绍如何通过VPN网关拨号接入VPC。



开始之前

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

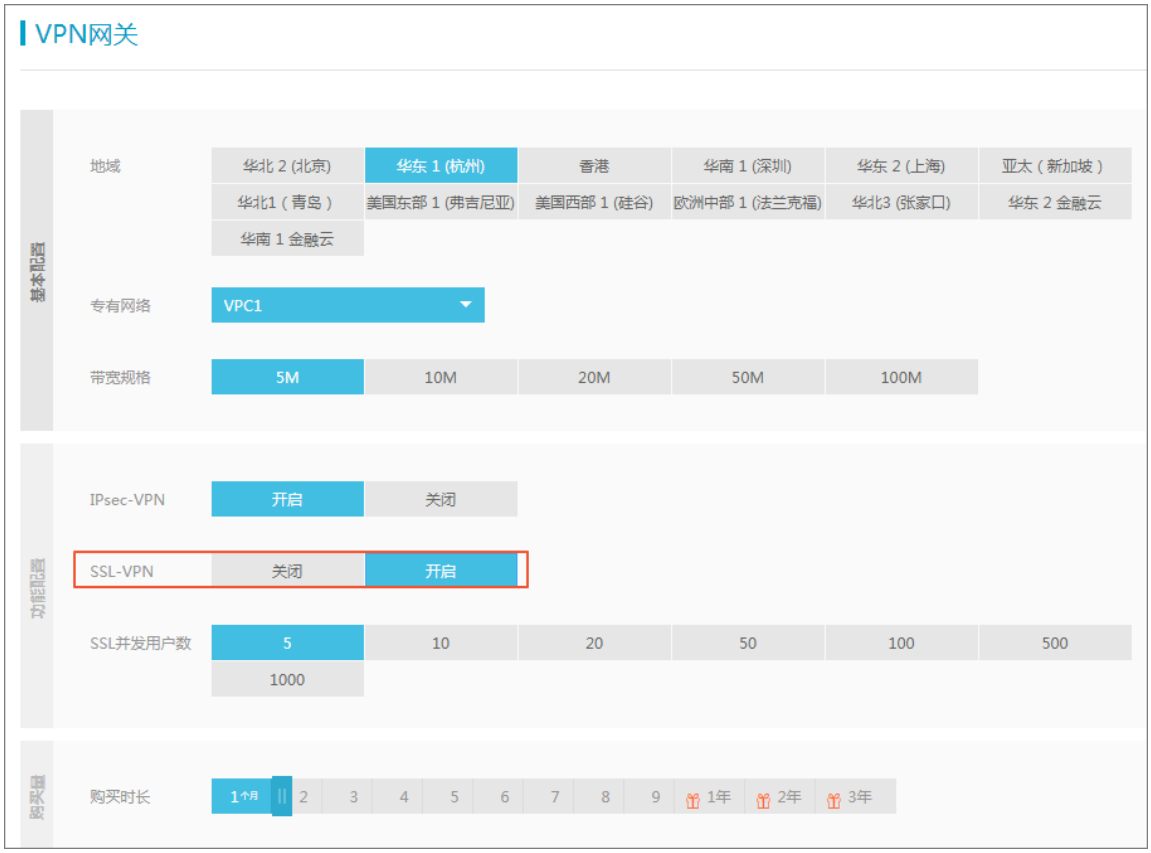
步骤一 创建VPN网关

1. 登录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。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。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。

     说明：

本选项只有在选择开启了SSL-VPN功能后才可配置。



5. 返回VPN网关页面，选择华东1地域，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

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网络。单击添加本端网段添加多个本端网段，本端网段可以是任何VPC或交换机的网段，也可以是本地网络的网段。
   - 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。
   - 高级配置：使用默认高级配置。

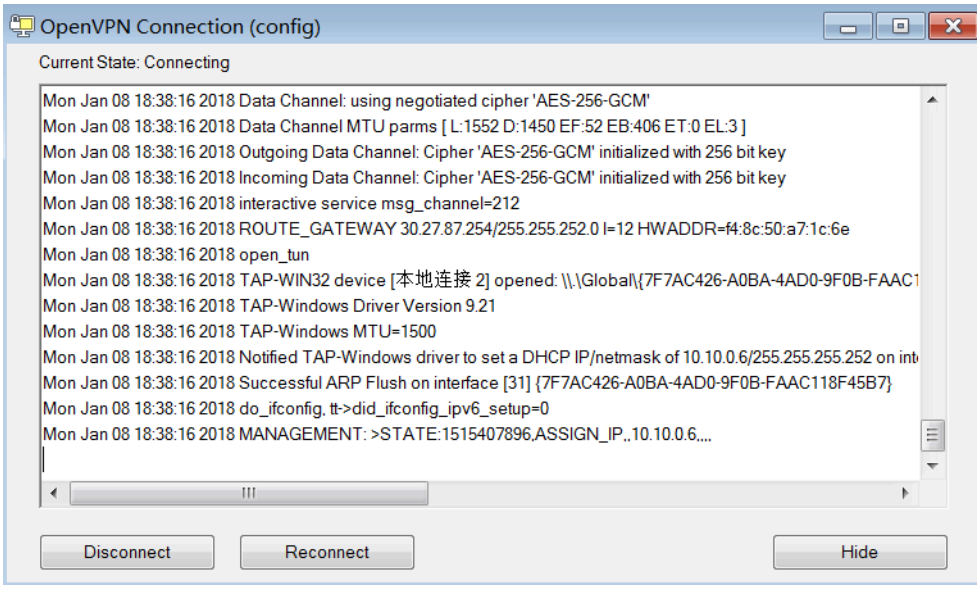
步骤三 创建客户端证书

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

> **注意:**
> 需要以管理员身份运行客户端。

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 连接测试

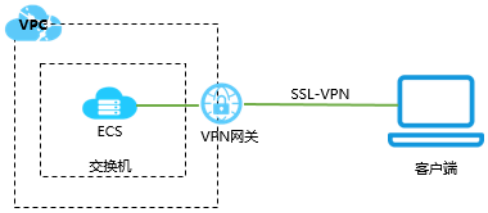
在客户端ping已连接的VPC内的一台ECS实例，测试连通性。

> **说明:**
> 确保测试的ECS实例的安全组规则允许客户端远程连接。详情参考*#unique_5*。


添加安全组规则
网卡类型：
内网
规则方向：
入方向
授权策略：
允许
协议类型：
全部
* 端口范围：
-1/-1
优先级：
1
授权类型：
地址段访问
* 授权对象：
10.10.0.0/24
教我设置
描述：
长度为2-256个字符，不能以http://或https://开头。
确定
取消

4 Mac客户端远程连接

本文以Mac客户端为例介绍如何通过VPN网关拨号接入VPC。



开始之前

在部署VPN网关前，确保您的环境满足以下条件：

- 本地设备和VPC的私网IP地址段不能相同，否则无法通信。
- 客户端必须能访问Internet。

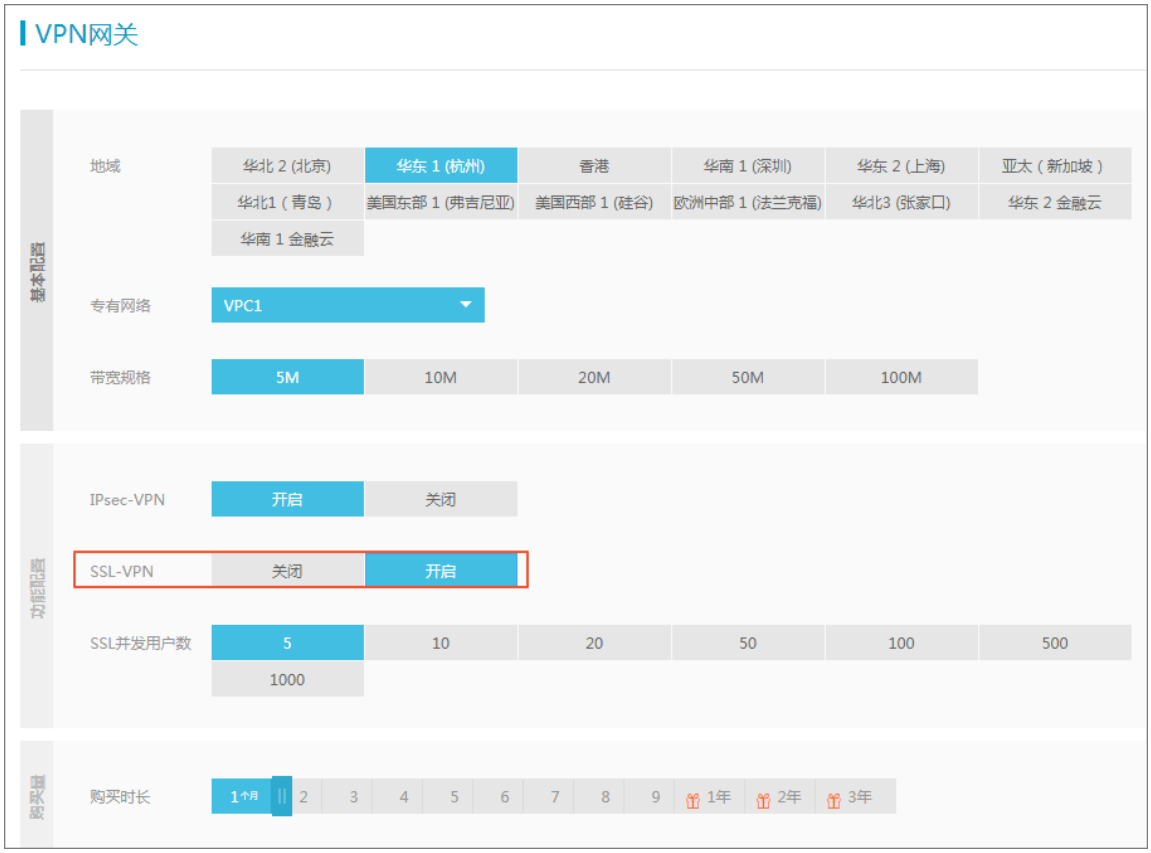
步骤一 创建VPN网关

1. 登录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。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。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。

     说明：

本选项只有在选择开启了SSL-VPN功能后才可配置。



5. 返回VPN网关页面，选择华东1地域，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

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网络。单击添加本端网段添加多个本端网段，本端网段可以是任何VPC或交换机的网段，也可以是本地网络的网段。
   - 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。
   - 高级配置：使用默认高级配置。

步骤三 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

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：

   ```
   cd  /usr/local/certificates
   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 连接测试

在客户端ping已连接的VPC内的一台ECS实例，测试连通性。

> 说明:
> 确保测试的ECS实例的安全组规则允许客户端远程连接。详情参考#unique_5。


添加安全组规则
网卡类型：
内网
规则方向：
入方向
授权策略：
允许
协议类型：
全部
* 端口范围：
-1/-1
优先级：
1
授权类型：
地址段访问
* 授权对象：
10.10.0.0/24
教我设置
描述：
长度为2-256个字符，不能以http://或https://开头。
确定
取消