ALIBABA CLOUD

阿里云

VPN网关

SSL-VPN入门

文档版本：20220629

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.SSL-VPN入门概述

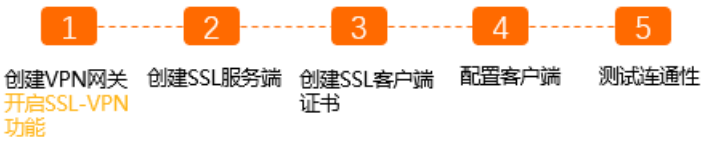
SSL-VPN支持将客户端远程接入专有网络VPC（Virtual Private Cloud），使客户端可以安全地访问VPC中部署的应用或服务。本文为您介绍SSL-VPN的使用流程。

环境要求

使用SSL-VPN功能建立客户端与VPC的连接前，请确保满足以下条件：

- 客户端的私网网段和VPC的私网网段没有重叠，否则无法通信。
- 客户端可以访问互联网。
- 您已了解VPC中所应用的安全组规则，并确保安全组规则允许客户端访问云上资源。具体操作，请参见查询安全组规则和添加安全组规则。

使用流程



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服务端中指定客户端要访问的私网网段和客户端访问时使用的网段。
3. 创建SSL客户端证书。
   根据SSL服务端配置，创建并下载客户端证书。
4. 配置客户端。
   在客户端中下载安装VPN软件、加载客户端证书，然后发起VPN连接。
5. 测试连通性。
   打开客户端的命令行窗口，执行ping命令，尝试访问VPC内的应用或服务，验证通信是否正常。

入门场景

客户端远程连接VPC

2.客户端远程连接VPC

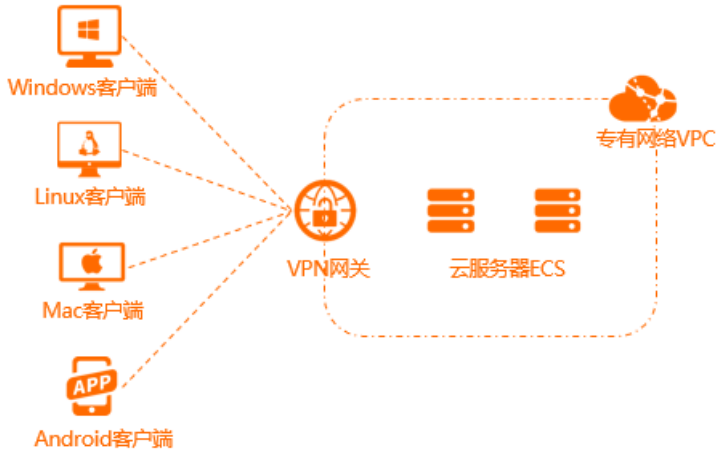
本文为您介绍Linux、Mac、Windows和Android客户端如何通过SSL-VPN连接专有网络VPC（Virtual Private Cloud）。

前提条件

- 您已经注册了阿里云账号。如未注册，请先完成账号注册。
- 客户端的私网网段和VPC的私网网段没有重叠。
- 客户端可以访问互联网。
- 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客户端访问云上资源。具体操作，请参见查询安全组规则和添加安全组规则。

背景信息

本文以下图场景为例，为您介绍Linux、Mac、Windows和Android客户端如何使用SSL-VPN连接VPC。



配置流程

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**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。
   - **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。

     > **说明** 确保VPC的地域和VPN网关的地域相同。

   - **网关类型**：选择待创建的VPN网关类型。本示例选择**普通型**。

- **VPC**：选择待连接的VPC。
- **指定交换机**：是否为VPN网关指定交换机实例。本示例选择**否**。
- **带宽规格**：选择VPN网关的带宽规格，单位：Mbps。
  带宽规格是VPN网关所具备的公网带宽峰值。
- **IPsec-VPN**：是否开启IPsec-VPN功能。本示例选择**关闭**。
- **SSL-VPN**：是否开启SSL-VPN功能。本示例选择**开启**。
- **SSL连接数**：选择需要连接的客户端的数量。

> **说明** 开启SSL-VPN功能后才可配置**SSL连接数**。

- **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分钟会变成**正常**状态。**正常**状态就表明VPN网关已完成初始化，可以正常使用。

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。

> **说明** 请确保SSL服务端的地域和已创建的VPN网关的地域相同。

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，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**：选择已创建的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**可添加多个本端网段，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网段。

> **注意**
> - 客户端网段的子网掩码位数在16至29位之间。
> - 请确保客户端网段和本端网段不冲突。
> - 在指定客户端网段时，建议您使用10.0.0.0/8、172.16.0.0/12和192.168.0.0/16网段及其子网网段。如果您的客户端网段需要指定为公网网段，您需要将公网网段设置为VPC的用户网段，以确保VPC可以访问到该公网网段。关于用户网段的更多信息，请参见什么是用户网段？和如何配置用户网段？。

   - **高级配置**：使用默认高级配置。

   更多信息，请参见创建SSL服务端。

步骤三：创建并下载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**。

步骤四：配置客户端

以下内容为您介绍如何配置Linux、Windows、Mac和Android客户端。

1. 打开命令行窗口。
2. 执行以下命令安装OpenVPN客户端。

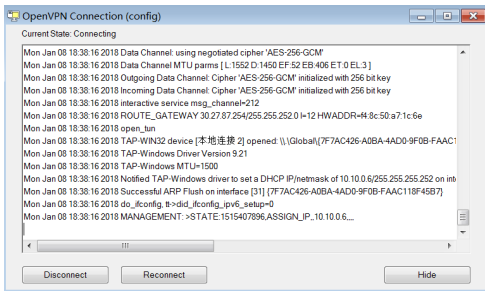
```
yum install -y openvpn
```

3. 将已下载的SSL客户端证书解压拷贝至*/etc/openvpn/conf/*目录。
4. 进入*/etc/openvpn/conf/*目录，执行以下命令建立VPN连接。

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

1. 下载并安装OpenVPN客户端（Windows版本）。
2. 将已经下载的SSL客户端证书解压拷贝至*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至您真实的目录。
3. 启动OpenVPN客户端，单击**Connect**建立VPN连接。



以下内容为您介绍如何使用Tunnelblick软件在Mac客户端与VPN网关之间建立VPN连接。

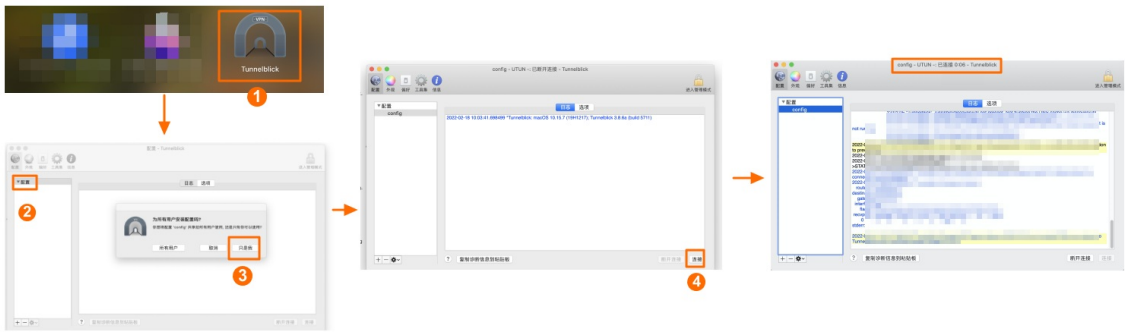
1. 下载Tunnelblick软件。

   本示例使用3.8.6a版本的Tunnelblick软件。
2. 安装Tunnelblick软件。

序号	说明
①	双击已下载的Tunnelblick软件安装包。
②	双击Tunnelblick图标。

序号	说明
③	选择**我有配置文件**。
④	单击**确定**。

3. 将在步骤三中下载的SSL客户端证书解压。
4. 将已解压的 `config.ovpn` 文件上传至Tunnelblick软件，建立VPN连接。



序号	说明
①	双击Tunnelblick图标，打开Tunnelblick软件。
②	将已解压的文件 `config.ovpn` 拖动至**配置**文件夹下。
③	选择**只有我**。
④	单击**连接**。

以下内容为您介绍如何使用OpenVPN软件在Mac客户端与VPN网关之间建立VPN连接。

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. 将在步骤三中下载的SSL客户端证书解压拷贝至配置目录。
   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. 执行以下命令将已经下载的SSL客户端证书拷贝到配置目录。

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

`cert_location` 是步骤三中下载的SSL客户端证书的路径，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。

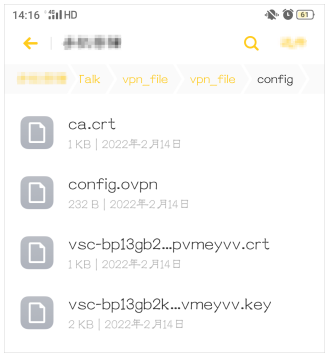
```
sudo /usr/local/opt/openvpn/sbin/openvpn --config /usr/local/etc/openvpn/config.ovpn
```

1. 下载并安装OpenVPN客户端（Android版本）。

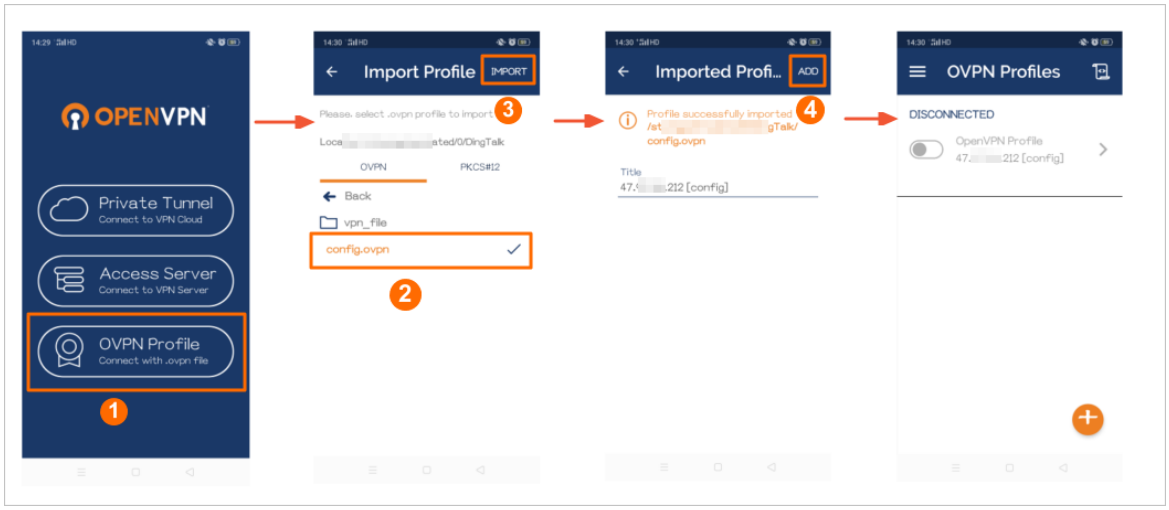
   本示例使用Android 9.0版本的客户端，并安装了3.0.5版本的OpenVPN客户端。

2. 将在步骤三中下载的SSL客户端证书传输至Android客户端，并解压证书。

> **说明**
>
> - 如果您的Android客户端无解压软件，您可以在电脑端解压证书然后将解压后的文件传输至Android客户端。
> - 请确保解压后的文件在同一个文件夹下，如下图所示。

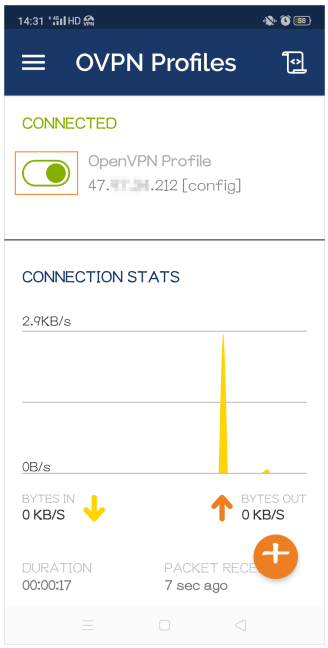


3. 打开OpenVPN客户端，导入 `config.ovpn` 文件，添加VPN连接。



序号	说明
①	选择**OVPN Profile**连接方式。
②	在存储目录中找到 `config.ovpn` 文件。
③	单击**IMPORT**，导入 `config.ovpn` 文件。
④	系统自动读取 `config.ovpn` 文件中的信息，显示待连接的VPN网关的公网IP地址。单击**ADD**，添加VPN连接。

4. 单击滑动按钮，开启VPN连接。



Linux客户端

Windows客户端

Mac客户端（Tunnelblick）

Mac客户端（OpenVPN）

Android客户端

步骤五：测试连通性

在客户端尝试访问VPC内的ECS实例，测试网络连通性。

常见问题

1. 打开Mac客户端的命令行窗口。
2. 执行以下命令搜索OpenVPN进程，并记录进程号。

```
ps aux | grep openvpn
```

3. 执行以下命令关闭OpenVPN进程。

```
kill -9 <进程号>
```

如果您使用的是M1版本的Mac客户端，建议您使用Tunnelblick软件建立VPN连接。具体操作，请参见Mac客户端（Tunnelblick）。

使用OpenVPN在Mac客户端建立VPN连接后，如何断开VPN连接？

M1版本的Mac客户端如何使用OpenVPN建立VPN连接？