# 阿里云 VPN网关

# SSL-VPN入门

文档版本: 20190415

为了无法计算的价值 | []阿里云

### <u>法律声明</u>

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。

- 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。
- 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。
A	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。	道 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 listinstanceid 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。	<pre>swich {stand   slave}</pre>

### 目录

法律声明	I
通用约定	I
1 教程概述	1
2 Linux客户端远程连接	2
4 Mac客户端远程连接	12

### 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)。



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。





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。

<b>送</b> 说明 VPN网关的	<ul><li>说明:VPN网关的创建一般需要1-5分钟。</li></ul>										
VPN网关										切换到日版>>	
44개L 1 44개L 2 44개L 3	华北5 华东1 华	¥东 2 4	¥南 1   香港   亚太东北 1 (东京)	亚太东南 1 (新加	坡) 亚太东	南 2 (悉尼) 亚太东南3 (吉翰	(現金) 美国东部1(売吉尼亚)	美国西部 1 (硅谷) 中	r东东部 1 (迪拜)   欧洲中部 1	(法兰克福)	
创建VPN网关剧新	自定义										
ID/名称	IP地址	监控	VPC	状态	带宽	计费方式	开启IPSec	开启SSL	SSL并发连接数规格	操作	
vpn-bp1ffgb0cxvxrcibr1fwj VPN网关 旨	118 149	Ł	vpc-bp15k6sx6fhdz2)w4daz0 k8s_vpc	<ul> <li>正常</li> </ul>	5M 变配	预付费 2018/2/9 00:00:00 到期	已开启	开启		编辑 续费	
vpn-bp18in10ga65vrrw55r5z ∨PN_Gateway ≦	121. 143	⊵	vpc-bp1hiv5hmp6em9ikpxtut VPC2	<ul> <li>正常</li> </ul>	5M 变配	预付费 2018/2/9 00:00:00 到期	已开启	已开启	5 变配	编辑 续费	

#### 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。

↓SSL服务端	创建SSL服务端	
総化1 総化2 総化3 総化5 <u>単仮1</u> 総仮2 経衛1 香港 美国东部1(売舎尼亚) 美国西部1(造谷) 中东东部1(造铎) 欧洲中部1(法兰売福)	* 名称① server	6/128 🛇
· 创建SSL服装饰 剧新	VPN网关 VPN_Gateway/	vpn-bp18in10ga65vrrw55r5z 🗸
ID/名称         IP地址         VPN网关	本端网段 192 • 1	68 • 0 • 0 / 16 ~ + 法加本端网段
vss-bp19govcqm7kdaumimdk 121.196.192.143 vpn-bp18in1 server ≧ VPN_Gatewi	客户端网段 10 • 1	
	<ol> <li>注意:客户端 高级配置</li> </ol>	网段不能和VPC内交换机网段冲突
	协议 UDP	$\checkmark$
	端口 1194	
	加密算法 AES-128-CBC	$\checkmark$
	是否压缩 否	$\checkmark$

#### 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。

SSL客户端												切换到日版>>		
华北 1	华北2 华	볼려比 3 1	¥411. 5	华东 1	华东 2	华南 1	香港	亚太东北 1 (东京)	亚太东	南 1 (新加坡)	亚太东南 2	(悉尼)	亚太东南3 (吉隆坡)	
<ul> <li>美国东部1(弗吉尼亚) 美国西部1(硅谷) 中东东部1(违拜) 欧洲中部1(法兰売福)</li> <li>创建SSL客户装证书</li> <li>別新</li> </ul>														
ID/名称			SSL服务	· 満		状态		创建时间		到期时间		操作		
vsc-bp1fa test ≌	vsc-bp1faadnquufotk4rv3d7 vss-bp19qovcqm7kdaur test 🖬 server		laurmmdk	• E	10 <del>1</del>	2018/1/8 17:24:47		2021/1/7 17:24	47	下载	删除			

#### 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。



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	2 组规则			? ×
	网卡类型:	内网	Ψ	
	规则方向:	入方向	<b>v</b>	
	授权策略:	允许	•	
	协议类型:	全部	•	
	★ 端□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	以http://或https://开头。	
			确定	取消
			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。





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。											
VPN网关										切换到日版>>	
华北 1 华北 2 华北 3	华北5 华东1 华	i东 2 华南 1	香港 亚太东北 1 (东京)	亚太东南 1 (新加	g) 亚太东	南 2 (悉尼) 亚太东南3 (吉隆	i坡) 美国东部 1 (弗吉尼亚)	美国西部1(硅谷) 中:	东东部 1 (迪拜)   欧洲中部 1	(法兰克福)	
创建VPN网关剧新	自定义										
ID/名称	IP地址	监控 VF	PC	状态	带宽	计费方式	开启IPSec	开启SSL	SSL并发连接数规格	操作	
vpn-bp1ffgb0cxvxrcibr1fwj VPN网关 III	118 149		pc-bp15k6sx6fhdz2jw4daz0 is_vpc	<ul> <li>正常</li> </ul>	5M 受配	预付费 2018/2/9 00:00:00 到期	已开启	开启		編 <del>輯</del> 续费	
vpn-bp18in10ga65vrrw55r5z VPN_Gateway ≌	121. 143	₩ vr VF	oc-bp1hlv5hmp6em9ikpxtut PC2	● 正常	5M 变配	预付费 2018/2/9 00:00:00 到期	已开启	已开启	5 变配	编辑 续费	

#### 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。

↓ SSL服务端	创建SSL服务端	×
华北1 华北2 华北3 华北5 华东1 华东2 华南1 雪港 亚5	*名称① server 6/128 ④	)
美国东部1(弗吉尼亚) 美国西部1(硅谷) 中东东部1(迪拜) 欧洲中部1(法兰克福)	VPN同关 VPN_Gateway/vpn-bp18in10ga65vrrw55r5z い	·
台頭SSL服約666 開始新	本端网段 192 • 168 • 0 • 0 / 16 ∨	
ID/名称 IP地址 VPN网天	十 添加本端网段	
vs-bp19qovcqm/kdaurmmdk 121.196.192.143 vpn-bp18in10g server VPN_Gateway	客户端网段 10 · 10 · 0 · 0 / 24 ∨	
	① 注意:客户编网段不能和VPC内交换机网段冲突	
	HP20ARBUEL 協议 UDP 〜	,
	端口 1194	
	加密算法 AES-128-CBC ~	/
	是否压缩 否 🗸	
	和這	消

#### 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。

SSL客户端												切换到日版>>		
华北 1	华北 2	华北 3	华北 5	华东1	华东 2	华南 1	香港	亚太东北 1 (东京)	亚太东	南 1 (新加坡)	亚太东南 2	(悉尼)	亚太东南3 (吉隆坡)	
美国东部1(弗吉尼亚) 美国西部1(硅谷) 中东东部1(き年) 欧洲中部1(法兰売福)														
创建S	SL客户端证书	刷	训新											
ID/名称			SSL服务	骑		状态		创建时间		到期时间		操作		
vsc-bp1faadnquufotk4rv3d7 vss-bp19qovcqm7kdaumm test 🗑 server		laurmmdk	● 正 <sup>第</sup>	ŝ	2018/1/8 17:24:47		2021/1/7 17:24	:47	下载	删除				

#### 步骤四 客户端配置



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。

OpenVPN Connection (config)		
Current State: Connecting		
Mon Jan 08 18:38:16 2018 Data Channel: using negotiated cipher 'AES-256-GCM'		
Mon Jan 08 18:38:16 2018 Data Channel MTU parms [L:1552 D:1450 EF:52 EB:406 ET:0 EL:3]		
Mon Jan 08 18:38:16 2018 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key		
Mon Jan 08 18:38:16 2018 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key		
Mon Jan 08 18:38:16 2018 interactive service msg_channel=212		
Mon Jan 08 18:38:16 2018 ROUTE_GATEWAY 30.27.87.254/255.255.252.0 I=12 HWADDR=f4:8c:50:a7:	lc:6e	
Mon Jan 08 18:38:16 2018 open_tun		
Mon Jan 08 18:38:16 2018 TAP-WIN32 device [本地连接 2] opened: \\.\Global\{7F7AC426-A0BA-4AD	)-9F0B-FAAC1	1
Mon Jan 08 18:38:16 2018 TAP-Windows Driver Version 9.21		
Mon Jan 08 18:38:16 2018 TAP-Windows MTU=1500		
Mon Jan 08 18:38:16 2018 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.10.0.6/255.255	255.252 on inte	
Mon Jan 08 18:38:16 2018 Successful ARP Flush on interface [31] {7F7AC426-A0BA-4AD0-9F0B-FAAC	118F45B7}	
Mon Jan 08 18:38:16 2018 do_ifconfig, tt->did_ifconfig_ipv6_setup=0		
Mon Jan 08 18:38:16 2018 MANAGEMENT: >STATE:1515407896,ASSIGN_IP.,10.10.0.6,,,,		Ξ
		-
III	•	
Disconnect	Hide	

#### 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。



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	全组规则				? ×
	网卡类型:	内网	Ŧ		
	规则方向:	入方向	•		
	授权策略:	允许	•		
	协议类型:	全部	•		
	★ 端□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	o://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。





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。

道 说明: VPN网关的创建一般需要1-5分钟。											
VPN网关										切换到日版>>	
华北 1 华北 2 华北 3	华北5 华东1 华	东2 华南1 香	灌 亚太东北 1 (东京)	亚太东南 1 (新加	坡) 亚太东	南 2 (悉尼) 亚大东南3 (吉隆	(坡) 美国东部1(弗吉尼亚)	美国西部1(硅谷) 中	东东部 1 (迪拜) 欧洲中部 1	(法兰克福)	
创建VPN网关	自定义										
ID/名称	IP地址	监控 VPC		状态	带宽	计费方式	开启IPSec	开启SSL	SSL并发连接数规格	操作	
vpn-bp1ffgb0cxvxrcibr1fwj VPN网关 Ⅲ	118 149	Vpc-bp15i k8s_vpc	6sx6fhdz2jw4daz0	<ul> <li>正常</li> </ul>	5M 変配	预付费 2018/2/9 00:00:00 到期	已开启	开启		编辑 续费	
vpn-bp18in10ga65vrrw55r5z VPN_Gateway ≌	121. 143	Vpc-bp1hi VPC2	/5hmp6em9ikpxtut	<ul> <li>正常</li> </ul>	5M 变配	预付费 2018/2/9 00:00:00 到期	已开启	已开启	5 变配	编辑 续费	

#### 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。

↓ SSL服务端	创建SSL服务端	×
柴北 1 柴北 2 柴北 3 柴北 5 柴东 1 柴东 2 柴南 1 香港 亚大	▲名称① server	6/128 ⊘
美国东部1(弗吉尼亚) 美国西部1(建谷) 中东东部1(迪拜) 欧洲中部1(法兰克福)	VPN Gateway/vpn-bp18in10ga85vrrw55rt	iz 🗸
	本端网段 192 ・ 168 ・ 0 ・	D / 16 🗸
UPANA VYNAJX	十 添加本端网段	
varup regroup regr	客户端网段 10 ・ 10 ・ 0 ・	D / 24 V
	<ul> <li>① 注意:各戶購內除不能和VPC內交換机內 高级配置</li> </ul>	殿冲突
	协议 UDP	~
	编口 1194	
	加密算法 AES-128-CBC	~
	是否压缩 否	$\sim$
		确定 取消

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。

U SSL客户端								切换到旧版>>						
华北 1	华北 2	华北 3	华北 5	华东1	华东 2	华南 1	香港	亚太东北 1 (东京)	亚太东	南 1 (新加坡)	亚太东南 2 (	悉尼) .	亚太东南3 (吉隆坡)	
美国东部 1 创建S	美国东部1(弗吉尼亚) 美国西部1(硅谷) 中东东部1(迪拜) 欧洲中部1(法兰売福) 创建SSL客户端证书 別新													
ID/名称			SSL服务	务端		状态		创建时间		到期时间		操作		
vsc-bp1fa test ≌	aadnquufotk4rv	3d7	vss-bp server	19qovcqrn7kd	laurmmdk	• E	10F	2018/1/8 17:24:47		2021/1/7 17:24	:47	下戴	删除	

#### 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。



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	自规则			? ×
	网 <del>卡类</del> 型:	内网	▼	
	规则方向:	入方向	•	
	授权策略:	允许	•	
	协议类型:	全部	•	
	★ 端□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