

Alibaba Cloud VPN网关

SSL-VPN クイックスタート

Document Version20191023

目次

1 チュートリアル概要.....	1
2 Linux クライアントリモートアクセス.....	2
3 Windows クライアントリモートアクセス.....	7
4 Mac クライアントリモートアクセス.....	12

1 チュートリアル の概要

チュートリアルでは、**Linux**、**Windows**、および **Mac** オペレーティングシステムを使用して、**SSL-VPN** を使用したリモートコンピューターから **VPC** に接続する方法を説明します。

前提条件

新しい **VPC** コンソールに切り替えます。

手順

SSL-VPN 機能を使用してクライアントから **VPC** にアクセスするには、次の手順に従ってください。

1. VPN Gateway の作成

SSL-VPN を有効化した **VPN Gateway** を作成します。

2. SSL サーバー の作成

SSL サーバの **IP** アドレス範囲と、クライアントが接続に使用する **IP** アドレス範囲を指定します。

3. クライアント証明書の作成

サーバーの設定に従ってクライアント証明書を作成し、クライアント証明書と設定をダウンロードします。

4. クライアントの設定

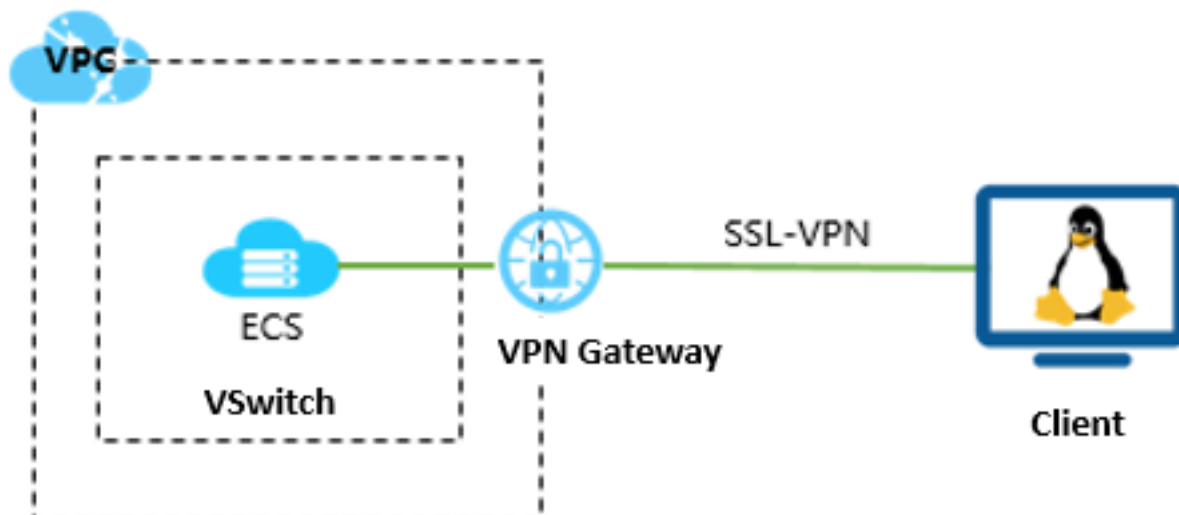
クライアントにクライアント **VPN** ソフトウェアをダウンロードしてインストールし、クライアント証明書と設定をロードして、接続を開始します。

5. セキュリティルールの設定

ECS インスタンスのセキュリティグループルールが、リモートアクセスを許可していることをご確認ください。

2 Linux クライアントリモートアクセス

ここでは、**SSL-VPN** を使用して **VPC** を **Linux** オペレーティングシステムのリモートコンピューターから接続する方法を説明します。



前提条件

VPN Gateway をデプロイする前に、次の条件が満たされていることをご確認ください。

- ・ **VPC** とリモートコンピューターの **IP** アドレス範囲が競合していない
- ・ クライアントはインターネットにアクセス可能

手順 1: VPN Gateway の作成

1. **VPC** コンソールにログインします。
2. 左側のナビゲーションウィンドウで、**[VPN] > [VPN Gateway]** をクリックします。
3. **VPN Gateway** ページで、**[VPN Gateway の作成]** をクリックします。
4. 購入ページで、**VPN Gateway** を設定し、支払いを完了します。このチュートリアルでは、**VPN Gateway** は次の設定を使用します。

- ・ **リージョン:** **VPN Gateway** のリージョンを選択します。このチュートリアルでは、**[中国 (杭州)]** を選択します。



注:

VPC と VPN Gateway が同じリージョンであることをご確認ください。

- ・ **VPC:** 接続する VPC を選択します。
- ・ **帯域幅の仕様:** 帯域幅の仕様を選択します。帯域幅の仕様は、**VPN Gateway** のインターネット帯域幅です。
- ・ **IPsec-VPN:** IPsec-VPN 機能を有効にするかを選択します。IPSec-VPN 機能はサイト間接続に適用され、実際のニーズに応じて有効にできます。
- ・ **SSL-VPN:** SSL-VPN 機能を有効にするかを選択します。SSL-VPN 機能を使用すると、単一のコンピューターから VPC に接続することができます。このチュートリアルでは、[有効] を選択します。
- ・ **同時 SSL 接続:** 同時に接続するクライアントの最大数を選択します。



注:

このオプションを設定できるのは、**SSL-VPN 機能を有効にした後**だけです。

Basic Configuration	Region	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
		Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
		UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
		UK(London)					
Duration	Name	<input type="text"/>					
	VPC	emr_test_vpc					
	Peak Bandwidth	10 Mbps		100 Mbps			
	Billing Method	Pay By Traffic					
	IPsec-VPN	enable		disable			
SSL-VPN	disable		enable				

5. **VPN Gateway** ページに戻り、"中国 (杭州)" リージョンを選択すると、作成した **VPN Gateway** が表示されます。

VPN Gateway の初期状態は、"Preparing" です。約 2 分で "Normal" に変わります。"Normal" に変わると、**VPN Gateway** が使用可能になったことを示します。



注:

通常、VPN Gateway の作成には 1 ~ 5 分かかります。

Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Enable IPsec	Enable SSL	Concurrent SSL Connections	Description	Actions
vpn2	47.97.193.13		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 01/25/2018, 14:41:45 Created	Enabled	Enable SSL	-	-	Delete
vpn1	47.97.209.47		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 02/11/2018, 17:53:25 Created	Enabled	Enabled	5 Upgrade downgrade	-	Delete

手順 2: SSL サーバーの作成

1. 左側のナビゲーションウィンドウで、[VPN] > [SSL サーバー] をクリックします。
2. [SSL サーバーの作成] をクリックします。このチュートリアルでは、SSL サーバーの設定は次のとおりです。

- ・ 名前: SSL サーバの名前を入力します。
- ・ VPN Gateway: 作成した VPN Gateway を選択します。
- ・ ローカルネットワーク: 接続するネットワークの CIDR ブロックを入力します。[ローカルネットワークの追加] をクリックし、複数のローカルネットワークを追加します。ローカルネットワークは、任意の VPC または VSwitch の CIDR ブロック、またはローカルネットワークの CIDR ブロックを選択することができます。
- ・ クライアントサブネット: CIDR ブロックの形式でサーバーに接続するために、クライアントが使用する IP アドレスを入力します。
- ・ 詳細設定: デフォルトの詳細設定を使用します。

SSL Servers

Create SSL Server Refresh Custom

Instance ID/Name	IP Address	VPN Gateway
vss-bp15prztev8ivop9b74d2server1	47.97.209.47	vpn-bp19uhloxy47kqf5acw1

Create SSL Server

VPN Gateway
vpn2/vpn-bp111s8uqu8782zr8ee43

Local Network
192.168.0.0/16

Add Local Network

Client Subnet
10.10.0.0/24

Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Advanced Configuration

Protocol
UDP

Port
1194

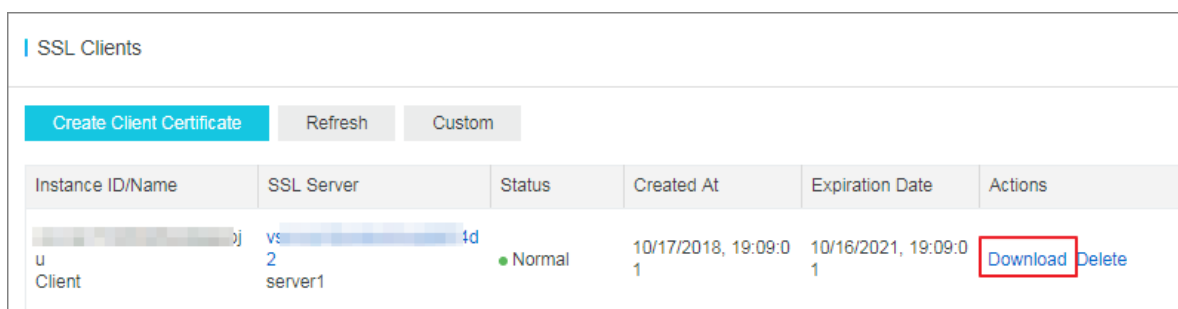
Encryption Algorithm
AES-128-CBC

Enable Compression
No

OK Cancel

手順 3: クライアント証明書の作成

1. 左側のナビゲーションウィンドウで、[VPN] > [SSL クライアント] をクリックします。
2. [クライアント証明書の作成] をクリックします。
3. クライアント証明書の作成 ページで、名前を入力し、関連する **SSL** サーバーを選択します。
[OK] をクリックします。
4. **SSL** クライアント ページで、作成した **SSL** クライアント証明書を検索し、[ダウンロード] をクリックします。



Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
u Client	vs- server1	● Normal	10/17/2018, 19:09:0 1	10/16/2021, 19:09:0 1	Download Delete

手順 4: Linux クライアントの設定

1. 次のコマンドを実行し、**OpenVPN** クライアントをインストールします。

```
yum install -y openvpn
```

2. 手順 3 でダウンロードしたクライアント証明書を抽出し、`/etc/openvpn/conf/` ディレクトリに証明書をコピーします。
3. 次のコマンドを実行し、**OpenVPN** を起動します。

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

手順 5: 接続の確認

クライアントで、接続された **VPC** ネットワーク内の **ECS** インスタンスのプライベート **IP** アドレスに **ping** を実行して、接続を確認します。



注：

ECS インスタンスのセキュリティルールが、リモートアクセスを許可していることをご確認ください。詳細については、[#unique_3](#)をご参照ください。

Add Security Group Rule ? Add security group rules

NIC: Internal Network

Rule Direction: Ingress

Action: Allow

Protocol Type: All

* Port Range: -1/-1

Priority: 1

Authorization Type: CIDR

* Authorization Objects: 10.10.0.0/24 [Tutorial](#)

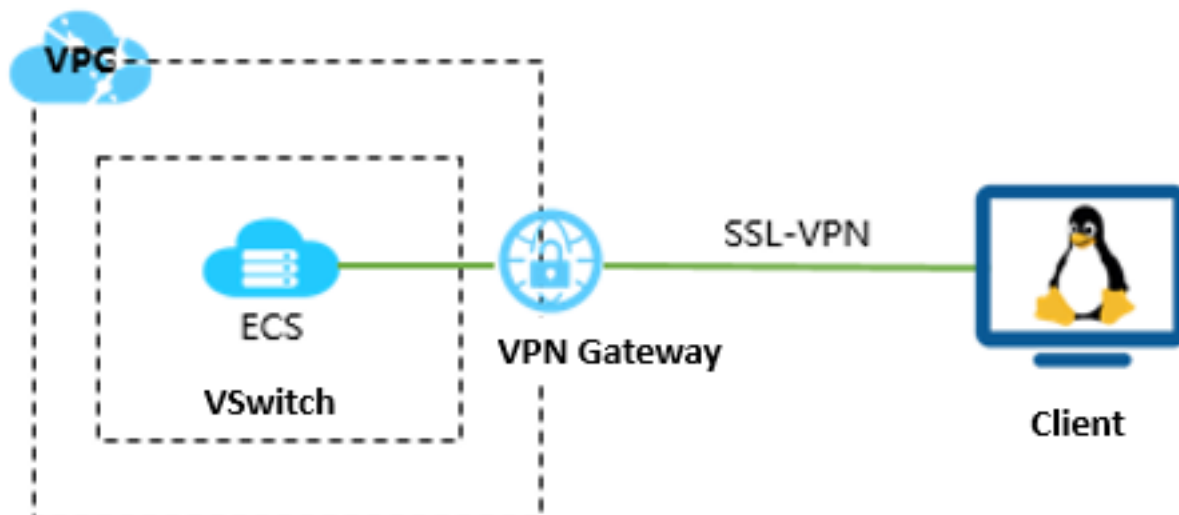
Description:

It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK Cancel

3 Windows クライアントリモートアクセス

本ページでは、SSL-VPN を使用して、Windows オペレーティングシステムのリモートコンピュータから VPC を接続する方法を説明します。



前提条件

VPN Gateway をデプロイする前に、次の条件が満たされていることをご確認ください。

- ・ VPC とリモートコンピュータの IP アドレス範囲が競合していない
- ・ クライアントがインターネットにアクセス可能であること

手順 1: VPN Gateway の作成

1. VPC コンソールにログインします。
2. 左側のナビゲーションペインで、[VPN] > [VPN Gateway] の順にクリックします。
3. VPN Gateway ページで、[VPN Gateway の作成] をクリックします。
4. 購入ページで、VPN Gateway を設定し、支払いを完了させます。このチュートリアルでは、VPN Gateway は次の設定を使用します。
 - ・ **Region** : VPN Gateway のリージョンをクリックします。このチュートリアルでは、[中国 (杭州)] をクリックします。



注：

VPN とVPN Gateway が同じリージョンであることをご確認ください。

- ・ **VPC** : 接続する VPC をクリックしてください。
- ・ **Bandwidth specification** : 帯域幅の仕様をクリックします。帯域幅指定は、VPN Gateway のインターネット帯域幅です。
- ・ **IPsec-VPN** : IPsec-VPN 機能を有効にするかを選択します。IPSec-VPN 機能は、サイト間接続に適用され、実際のニーズに応じて有効にできます。
- ・ **SSL-VPN** : SSL-VPN 機能を有効にするかどうかを選択します。SSL-VPN 機能を使用すると、単一のコンピューターから VPC に接続できます。このチュートリアルでは、[有効にする] をクリックします。
- ・ **Concurrent SSL Connections** : 同時に接続するクライアントの最大数を選択します。



注：

このオプションを設定できるのは、SSL-VPN 機能を有効にした後だけです。

Basic Configuration	Region	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
		Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
		UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
		UK(London)					
	Name	<input type="text"/>					
	VPC	emr_test_vpc					
	Peak Bandwidth	10 Mbps		100 Mbps			
	Billing Method	Pay By Traffic					
Duration	IPsec-VPN	enable		disable			
	SSL-VPN	disable		enable			

5. VPN Gateway ページに戻り、[中国 (杭州)] リージョンをクリックすると、作成した VPN Gateway が表示されます。

VPN Gateway の初期状態は、"準備中" です。約 2 分で "正常" に変わります。状態が "正常" に変わると、VPN Gateway が使用可能になったことを示します。



注：

通常、VPN Gateway の作成には1～5分かかります。

Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Enable IPsec	Enable SSL	Concurrent SSL Connections	Description	Actions
vpn2	47.97.193.13		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 01/25/2018, 14:41:45 Created	Enabled	Enable SSL	-	-	Delete
vpn1	47.97.209.47		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 02/11/2018, 17:53:25 Created	Enabled	Enabled	5 Upgrade downgrade	-	Delete

手順2: SSL サーバの作成

1. 左側のナビゲーションペインで、[VPN] > [SSL サーバー] の順にクリックします。
2. [SSLサーバーの作成] をクリックします。このチュートリアルでは、SSL サーバの構成は次のとおりです。

- **Name** : SSL サーバの名前を入力します。
- **VPN Gateway** : 作成した VPN Gateway をクリックします。
- **Local Network** : 接続するネットワークの CIDR ブロックを入力します。ローカルネットワークの追加 をクリックし、複数のローカルネットワークを追加します。ローカルネットワークは、任意の VPC または VSwitch の CIDR ブロック、またはローカルネットワークの CIDR ブロックにすることができます。
- **クライアントサブネット**: クライアントがサーバーに接続するために使用する IP アドレスを CIDR ブロックの形式で入力します。
- **詳細設定**: デフォルトの詳細設定を使用します。

SSL Servers

Create SSL Server Refresh Custom

Instance ID/Name	IP Address	VPN Gateway
vss-bp15prztev8ivop9b74d2server1	47.97.209.47	vpn-bp19uhloxy47krf5acw1

Create SSL Server

VPN Gateway
vpn2/vpn-bp111s8uqu8782zr8ee43

Local Network
192.168.0.0/16

Add Local Network

Client Subnet
10.10.0.0/24

Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Advanced Configuration

Protocol
UDP

Port
1194

Encryption Algorithm
AES-128-CBC

Enable Compression
No

OK Cancel

手順3: クライアント証明書の作成

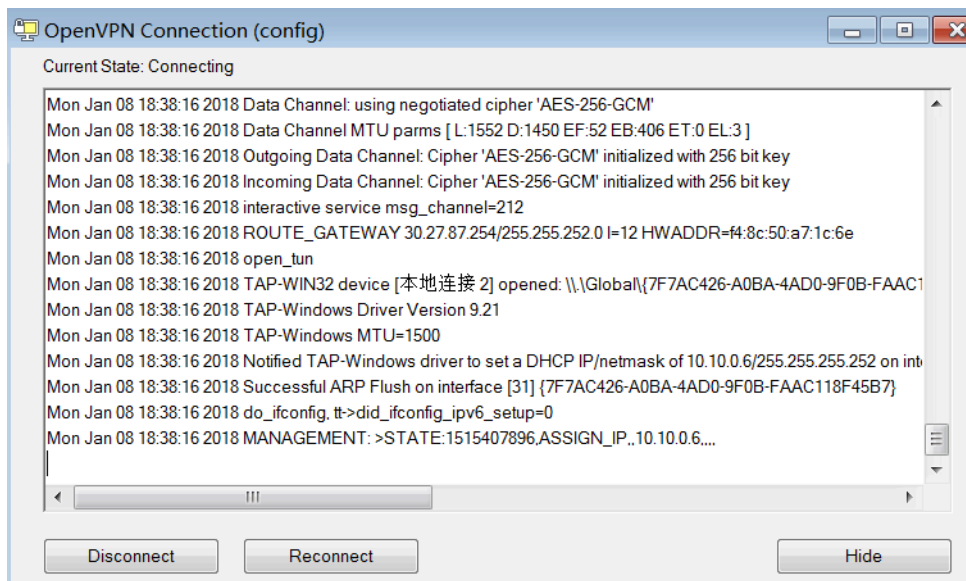
1. 左側のナビゲーションウィンドウで、[VPN] > [SSL クライアント] の順にクリックします。
2. [クライアント証明書の作成] をクリックします。
3. クライアント証明書の作成 ページで、名前を入力し、関連する **SSL** サーバーを選択します。
[確認] をクリックします。
4. **SSL** クライアント ページで、作成した **SSL** クライアント証明書を探し、ダウンロード をクリックします。

SSL Clients					
Create Client Certificate Refresh Custom					
Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
u Client	vs server1	● Normal	10/17/2018, 19:09:0 1	10/16/2021, 19:09:0 1	Download Delete

手順4: Windows クライアントの設定

クライアントを管理者として実行する必要があります。

1. **OpenVPN** クライアントをダウンロードしてインストールします。
2. 手順3でダウンロードしたクライアント証明書を抽出し、`/etc/openvpn/conf/` ディレクトリに証明書をコピーします。
3. **接続** をクリックして接続を開始します。



手順5: 接続の確認

クライアントで、接続された VPC ネットワーク内の ECS インスタンスのプライベート IP アドレスに **ping** を実行して、接続を確認します。



注:

ECS インスタンスのセキュリティルールが、リモートアクセスを許可していることをご確認ください。詳細については、[#unique_3](#)をご参照ください。

Add Security Group Rule ⓘ Add security group rules

NIC: Internal Network ▼

Rule Direction: Ingress ▼

Action: Allow ▼

Protocol Type: All ▼

* Port Range: -1/-1 ⓘ

Priority: 1 ⓘ

Authorization Type: CIDR ▼

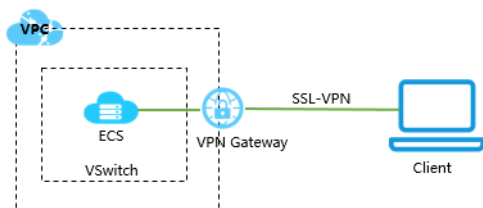
* Authorization Objects: 10.10.0.0/24 ⓘ Tutorial

Description:
It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK Cancel

4 Mac クライアントリモートアクセス

このドキュメントでは、**SSL-VPN** を使用して **VPC** を **Mac** オペレーティングシステムのクライアントから接続する方法を説明します。



前提条件

VPN ゲートウェイを展開する前に、次の条件が満たされていることをご確認ください。

- ・ **VPC** とリモートコンピュータの **IP** アドレス範囲が競合していない。
- ・ クライアントはインターネットにアクセスできること。

手順 1: VPN Gateway の作成

1. **VPC** コンソールにログインします。
2. 左側のナビゲーションウィンドウで、**[VPN] > [VPN Gateways]** の順にクリックします。
3. **VPN Gateways** ページで、**[VPN Gateway の作成]** をクリックします。
4. 購入ページで、**VPN** ゲートウェイを設定し、支払いを完了させます。このチュートリアルでは、**VPN Gateway** は次の設定を使用します。

- ・ **Region : VPN Gateway** のリージョンをクリックします。このチュートリアルでは、**[中国 (杭州)]** をクリックします。



注：

VPC と VPN Gateway が同じリージョンであることをご確認ください。

- **VPC** : 接続する VPC をクリックします。
- **Bandwidth specification** : 帯域幅の仕様をクリックします。帯域幅仕様は、VPN Gateway のインターネット帯域幅です。
- **IPsec-VPN** : IPsec-VPN 機能を有効にするか選択します。IPSec-VPN 機能は、サイト間接続に適用され、実際のニーズに応じて有効にできます。
- **SSL-VPN** : SSL-VPN 機能を有効にするかどうかを選択します。SSL-VPN 機能を使用すると、単一のコンピュータから VPC に接続できます。このチュートリアルでは、[有効にする] をクリックします。
- **Concurrent SSL Connections**: 同時に接続するクライアントの最大数を設定します。



注：

このオプションを設定できるのは、**SSL-VPN 機能を有効にした後**だけです。

Basic Configuration	Region	China (Qingdao)	China (Beijing)	China (Zhangjiakou)	China (Hangzhou)	China (Shanghai)	China (Shenzhen)
		Hong Kong	Singapore	Australia (Sydney)	Malaysia (Kuala Lumpur)	US (Virginia)	US (Silicon Valley)
		UAE (Dubai)	Germany (Frankfurt)	China North 5 (Huhehaote)	Asia Pacific SOU 1 (Mumbai)	Indonesia (Jakarta)	Japan (Tokyo)
		UK(London)					
	Name	<input type="text"/>					
	VPC	emr_test_vpc					
	Peak Bandwidth	10 Mbps		100 Mbps			
	Billing Method	Pay By Traffic					
Duration	IPsec-VPN	enable		disable			
	SSL-VPN	disable		enable			

5. **VPN Gateways**ページに戻り、[中国 (杭州)] リージョンをクリックすると、作成した **VPN Gateway** が表示されます。

VPN Gateway の初期状態は、"準備中" です。約2分で "正常" に変わります。状態が "正常" に変わると、**VPN Gateway** が使用可能になったことを示します。



注：

通常、VPN Gateway の作成には 1～5 分かかります。

Instance ID/Name	IP Address	Monitor	VPC	Status	Bandwidth	Billing Method	Enable IPsec	Enable SSL	Concurrent SSL Connections	Description	Actions
vpn2	47.97.193.13		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 01/25/2018, 14:41:45 Created	Enabled	Enable SSL	-	-	Delete
vpn1	47.97.209.47		webVPC	Normal	10Mbps Upgrade	Billing by Traffic Usage 02/11/2018, 17:53:25 Created	Enabled	Enabled	5 Upgrade downgrade	-	Delete

手順 2: SSL サーバーの作成

1. 左側のナビゲーションウィンドウで、[VPN] > [SSL サーバー] の順にクリックします。
2. [SSL サーバーの作成] をクリックします。このチュートリアルでは、SSL サーバーの設定は次のとおりです。

- **Name** : SSL サーバの名前を入力します。
- **VPN Gateway** : 作成した VPN Gateway をクリックします。
- **Local Network** : 接続するネットワークの CIDR ブロックを入力します。[ローカルネットワークの追加] をクリックし、複数のローカルネットワークを追加します。ローカルネットワークは、任意の VPC または VSwitch の CIDR ブロック、またはローカルネットワークの CIDR ブロックにすることができます。
- **Client Subnet**: クライアントがサーバーに接続するために使用する IP アドレスを CIDR ブロックの形式で入力します。
- **Advanced Configuration**: デフォルトの詳細設定を使用します。

SSL Servers

Create SSL Server Refresh Custom

Instance ID/Name	IP Address	VPN Gateway
vss-bp15prztev8ivop9b74d2-server1	47.97.209.47	vpn-bp19uhloxy47kqf5acw1

Create SSL Server

VPN Gateway
vpn2/vpn-bp111s8uqu8782zr8ee43

Local Network
192.168.0.0/16

Add Local Network

Client Subnet
10.10.0.0/24

Note: The client subnet IP range cannot overlap the VPC VSwitch subnet IP range.

Advanced Configuration

Protocol
UDP

Port
1194

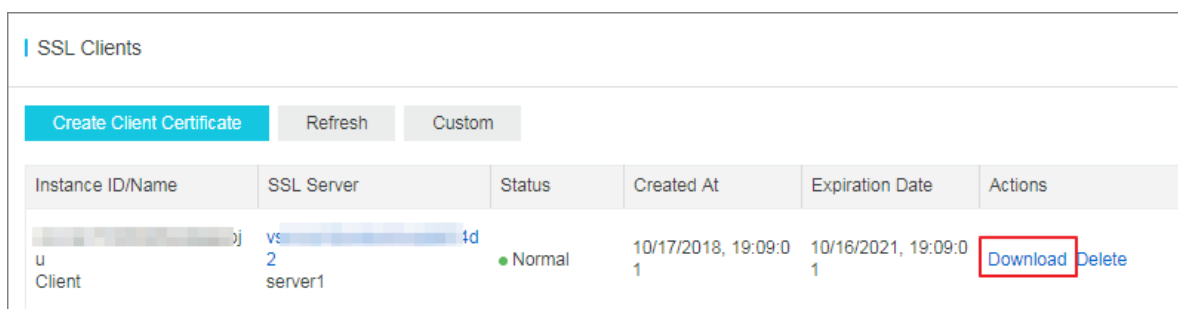
Encryption Algorithm
AES-128-CBC

Enable Compression
No

OK Cancel

手順3: クライアント証明書の作成

1. 左側のナビゲーションペインで、[VPN] > [SSL クライアント] の順にクリックします。
2. [クライアント証明書の作成] をクリックします。
3. クライアント証明書の作成 ページで、名前を入力し、関連する SSL サーバーを選択します。
[確認] をクリックします。
4. [SSL クライアント] ページで、作成した SSL クライアント証明書を探し、[ダウンロード] をクリックします。



Instance ID/Name	SSL Server	Status	Created At	Expiration Date	Actions
u Client	vs 2 server1	● Normal	10/17/2018, 19:09:0 1	10/16/2021, 19:09:0 1	Download Delete

手順4: Mac クライアントの設定

1. 次のコマンドを実行して **OpenVPN** クライアントをインストールします。

```
brew install openvpn
```



注:

Homebrew がインストールされていることをご確認ください。

2. デフォルトの設定をコピーしてから、次のコマンドを実行してデフォルトの設定を削除します。

- a. 次のコマンドを実行して、ダウンロードした証明書を設定フォルダにコピーします。

```
rm /usr/local/etc/openvpn/*
```

- b. 次のコマンドを実行して、ファイルを設定ディレクトリにコピーします。

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

`cert_location` は手順3でダウンロードした証明書のパスです。たとえば: `/Users/example/Downloads/certs6.zip`

- c. 次のコマンドを実行して証明書を抽出します。

```
cd /usr/local/certificates
```

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

d. 次のコマンドを実行して接続を開始します。

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

手順5: 接続の確認

クライアントで、接続された VPC ネットワーク内の ECS インスタンスのプライベート IP アドレスに **ping** を実行して、接続を確認します。



注:

ECS インスタンスのセキュリティルールで、リモートアクセスを許可するようにしてください。詳細については、[#unique_3](#)をご参照ください。

Add Security Group Rule ⓘ Add security group rules

NIC: Internal Network ▼

Rule Direction: Ingress ▼

Action: Allow ▼

Protocol Type: All ▼

* Port Range: -1/-1 ⓘ

Priority: 1 ⓘ

Authorization Type: CIDR ▼

* Authorization Objects: 10.10.0.0/24 ⓘ Tutorial

Description:
It can be 2 to 256 characters in length and cannot start with http:// or https://.

OK Cancel