Alibaba Cloud
VPN网关

ユーザーガイド

Document Version20191114

目次

1 VPN Gateway の管理

1.1 VPN Gateway の管理

SSL-VPN および **IPsec-VPN** 接続を有効にするために **VPN** ゲートウェイを作成します。 **VPN Gateway** が作成された後、パブリック **IP** が割り当てられます。

VPN Gateway の作成

VPN Gateway を作成するには、次の手順を実行します。

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インドウで、**[VPN]** > **[VPN Gateways]** とクリックします。
3. **[VPN Gateways]** ページで、**[VPN Gateway** の作成**]** をクリックします。
4. 次の情報に従って **VPN Gateway** を設定し、**[**今すぐ購入**]** をクリックします。

設定項目	説明
Region	**VPN Gateway** のリージョンを選択します。 **IPsec-VPN** を使用して **VPC** をローカルデータセンターまたは他の **VPC** に接続する場合は、**VPN Gateway** と **VPC** が同じリージョンであることをご確認ください。
VPC	**VPN Gateway** に関連付けられた **VPC** を選択します。
Bandwidth	**VPN Gateway** のインターネットの帯域幅を選択します。 帯域幅の指定は、**VPN** ゲートウェイのインターネット帯域幅です。
IPsec-VPN	**IPsec-VPN** を有効にします。 **IPsec-VPN** を有効化すると、**IPsec** トンネルを介してサイト間コネクションを作成し、ローカルデータセンターを **VPC** に接続するか、２つの **VPC** を接続することができます。
SSL-VPN	**SSL-VPN** を有効にします。 **SSL-VPN** を有効にすると、ポイント対サイトコネクションを作成できます。 クライアントは、クライアントゲートウェイを設定しなくても、リモートロケーションから直接 **VPC** にアクセスできます。
Purchase Duration	購入期間を選択します。

設定項目	説明
Auto renew	自動更新を有効にするかどうかを選択します。 ・ **VPN Gateway** は月単位で課金され、更新サイクルは１か月です。 ・ **VPN Gateway** が年単位で課金される場合、自動更新サイクルは１年です。

VPN ゲートウェイの編集

VPN Gateway の名前と説明を編集するには、次の手順を実行します。

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インドウで、**[VPN]** > **[VPN Gateways]** とクリックします。
3. **VPN Gateways** ページで、**VPN Gateway** のリージョンをクリックします。
4. 対象の **VPN Gateway** の アクション 列で **[編集]** をクリックします 。

1.2 VPN Gateway の変更

このトピックでは、**VPN Gateway** を変更する方法について説明します。 **VPN Gateway** の作成後、**VPN Gateway** の名前と説明を変更できます。

VPN Gateway が作成されていること。 詳細は、「*VPN Gateway の管理*」をご参照ください。

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 Gateways]** を選択します。
3. ターゲット **VPN Gateway** のリージョンを選択します。
4. **[VPN Gateways]** ページで、ターゲット **VPN Gateway** を見つけ、**[ID/名前]** 列の  アイコンをクリックしてインスタンス名を変更します。

   名前は **2**～**100** 文字でなければなりません。数字、アンダースコア (_)、ハイフン (-) を含めることができます。 名前は文字で始める必要があります。
5. **[説明]** 列の  アイコンをクリックして説明を変更します。

   説明は **2**～**256** 文字でなければなりません。 **http://** または **https://** で始めることはできません。

1.3 SSL-VPN および IPsec-VPN の有効化

VPN Gateway の作成時に **SSL-VPN** または **IPsec-VPN** を有効にしていない場合、後で有効化できます。

> 注：
> **2018** 年 **1** 月 **20** 日以前に作成された **VPN Gateway** の **SSL-VPN** 機能を有効にするには、チケットを起票し、サポートセンターへお問い合わせください。 **2018** 年 **1** 月 **20** 日以降に作成された **VPN Gateway** の場合、コンソール上で直接、機能を有効にすることができます。

IPsec-VPN の有効化

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インドウで、**[VPN]** > **[VPN Gateway]** をクリックします。
3. 対象の **VPN Gateway** のリージョンを選択します。
4. 対象の **VPN Gateway** の **"IPsec** の有効化" から **[**有効化**]** をクリックします。
5. 購入ページで、支払いを完了します。

SSL-VPN の有効化

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インドウで、**[VPN]** > **[VPN Gateway]** をクリックします。
3. 対象の **VPN Gateway** のリージョンを選択します。
4. 対象の **VPN Gateway** の **"SSL** の有効化" から、**[**有効化**]** をクリックします。
5. 購入ページで、支払いを完了します。

2 カスタマーゲートウェイの管理

2.1 カスタマーゲートウェイの管理

IPsec-VPN コネクションを使用してサイト間コネクションを構築する場合、カスタマーゲートウェイを作成する必要があります。 カスタマーゲートウェイを作成することで、ローカルゲートウェイの設定を **Alibaba Cloud** に登録できます。 １つのカスタマーゲートウェイを複数の **VPN Gateway** に接続することができます。

カスタマーゲートウェイの作成

カスタマーゲートウェイを作成するには、次の手順を実行します。

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]** > **[**カスタマーゲートウェイ**]** とクリックします。
3. カスタマーゲートウェイのリージョンをクリックします。

   接続するカスタマーゲートウェイと **VPN Gateway** は、同じリージョンでなければなりません。
4. カスタマーゲートウェイ ページで、**[**カスタマーゲートウェイ の作成**]** をクリックします。
5. 次の情報に従って、カスタマーゲートウェイを設定します。

設定項目	説明
Name	カスタマーゲートウェイの名前。 名前には２～１２８文字の英字、数字、ハイフン、または下線が使用でき、英字で始まる必要があります。
IP Address	ローカルデータセンターのゲートウェイ用に設定された静的パブリック **IP** アドレス。
Description	カスタマーゲートウェイの説明。 説明には **2** ～**256** 文字を使用でき、**http://** または **https://** で始めることはできません。

6. **(**オプション**)** 別のカスタマーゲートウェイを追加するには、**[**+ 追加**]** をクリックします。
7. **[OK]** をクリックします。

カスタマーゲートウェイの編集

カスタマーゲートウェイの名前と説明を編集するには、次の手順を実行します。

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]** > **[**カスタマーゲートウェイ**]** とクリックします。
3. 対象のカスタマーゲートウェイのリージョンをクリックします。
4. ターゲットカスタマーゲートウェイの アクション列 で、 **[**編集**]** をクリックします。
5. カスタマーゲートウェイの名前と説明を修正します。

ユーザゲートウェイの削除

カスタマーゲートウェイを削除するには、次の手順を実行します。

> 注 :
> カスタマーゲートウェイを削除する前に、まずカスタマーゲートウェイに関連する **IPsec** コネクションを削除する必要があります。

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]** > **[**カスタマーゲートウェイ**]** とクリックします。
3. 対象のカスタマーゲートウェイのリージョンをクリックします。
4. ターゲットカスタマーゲートウェイの アクション 列で、**[**削除**]** をクリックします。
5. 表示されるダイアログボックスで、**[**確認**]**をクリックします。

3 IPsec-VPN 接続の構成

3.1 ローカルゲートウェイの設定

3.1.1 USG シリーズ次世代ファイアウォールデバイス（Huawei）を通じた IPsec-VPN 接続の設定

このドキュメントでは、**Huawei** の **USG** シリーズ次世代ファイアウォールデバイス（**USG** シリーズ **Huawei** デバイスとも呼ばれる）を通じて **IPsec-VPN** 接続を設定し、オンプレミスデータセンターに接続する方法を説明します。 **IPsec-VPN** を使用してサイト間の接続を作成するため、**Alibaba Cloud VPN Gateway** 用に設定された **IPsec-VPN** 接続に基づいてローカルゲートウェイを設定する必要があります。

Alibaba Cloud VPN Gateway は、標準の **IKEv1** および **IKEv2** プロトコルをサポートしています。 したがって、これらの **2** つのプロトコルをサポートするデバイス **(Huawei**、**H3C**、**Hillstone**、**Sangfor**、**Cisco ASA**、**Juniper**、**SonicWall**、**Nokia**、**IBM**、および **Ixia** など**)** は、**VPN Gateway** に接続できます。

次のセクションでは、**Huawei** 社の **USG** シリーズデバイスを例にしてネットワークシナリオを説明し、次の表に対応するネットワーク設定について説明します。

ネットワークの設定		値の例
VPC	**VSwitch** の **CIDR** ブロック	**192.168.10.0/24, 192.168.11.0/24**
	VPN Gateway のパブリック **IP** アドレス	**47.97.161.10**
オンプレミスデータセンター	イントラネットの **CIDR** ブロック	**10.10.10.0/24**
	ファイアウォールのパブリック **IP** アドレス	**124.90.34.215/26**
	アップストリームインターネットインターフェイス	**10GE1/0/0**
	ダウンストリームイントラネットインターフェイス	**10GE1/0/1**

注：

オンプレミスデータセンター側が VPC と接続する複数の CIDR ブロックに関連付けられている場合、Alibaba Cloud 上に同数の IPsec-VPN 接続を作成し、VPN ゲートウェイを追加することを推奨します。

IKEv1 VPN の設定

前提条件

- Alibaba Cloud VPC で IPsec-VPN 接続を作成します。 詳細は、*#unique_10* をご参照ください.
- IPsec-VPN 接続の設定を取得しています。 この例では、以下の表に示す設定が使用されています。

プロトコル	設定	値の例
IKE	認証アルゴリズム	**SHA-1**
	暗号化アルゴリズム	**AES-128**
	DH Group	グループ 2
	IKE Version	**IKE v1**
	SA ライフサイクル	**86400**
	ネゴシエーションモード	メイン
	PSK	**123456**
IPsec	認証アルゴリズム	**SHA-1**
	Encryption Algorithm	**AES-128**
	DH Group	グループ 2
	IKE Version	**IKE v1**
	SA ライフサイクル	**86400**
	ネゴシエーションモード	**esp**

手順

ユーザーのゲートウェイ設定を USG シリーズ Huawei デバイスにロードするには、次の手順に従います。

1. Huawei のファイアウォール管理ページに移動します。
2. ネットワーク > インターフェイス > インターフェイスリスト をクリックします untrust セキュリティゾーンにアップストリームインターネットインターフェイス 10GE1/0/0 を追加してから、パブリック IP アドレスを設定します。ダウンストリームイントラネットインター

フェイス **10GE1/0/1** を **trust** セキュリティゾーンに追加してから、プライベート **IP** アドレスを設定します。

3. ポリシー > セキュリティポリシー > 追加 をクリックして、セキュリティーポリシーを作成します。
4. ネットワーク > **IPSec** > **IPSec**ポリシーリスト > 追加をクリックします。 次を参照してピアサイトを設定します。
   - ローカルインターフェイス ：アップストリームインターネットインターフェイスを選択します。 この例では、**10GE1/0/0** を選択します。
   - ピアアドレス：**Alibaba Cloud VPN** ゲートウェイのパブリック **IP** アドレスを入力します。 この例では、 **47.97.161.10** と入力します。
   - 事前共有キー ：事前共有キーは **Alibaba Cloud** 側の **PSK** と同様です。 この例では、**123456** と入力します。
5. 暗号化待ちデータフローページで、 追加をクリックします。 次の情報に従って、**VPC** 内のすべての **VSwitch CIDR** ブロックに対して暗号化するデータフローを追加します。
   - 送信元アドレス/アドレスセット：オンプレミスデータセンターのプライベート **IP** アドレスセグメントを入力します。 この例では、**10.10.10.0/24** と入力します。
   - 宛先アドレス/アドレスセット：**VPC** の **VSwitch IP** アドレスセグメントを入力します。 この例では、**192.168.10.0/24** と **192.168.11.0/24** を入力します。
6. **IKE / IPsec** プロトコルページで、詳細をクリックします。 ダウンロードした **IPsec-VPN** 接続の設定に基づいて、**IKE** パラメータと **IPSec** パラメータを構成します。
7. ネットワーク > ルート > スタティックルート > スタティックルートリスト > 追加 をクリックしてファイアウォール用のスタティックルートを設定します。 デフォルトルートを追加すると、ネクストホップはファイアウォールのパブリック **IP** アドレスになります。 **VPC** にルートを追加すると、ネクストホップは **VPN Gateway** のパブリック **IP** アドレスになります。

IKEv2 VPN の設定

前提条件

- **Alibaba Cloud VPC** で **IPsec-VPN** 接続を作成しています。
- **IPsec-VPN** 接続の設定を取得しています。 この例では、以下の表に示す設定が使用されています。

プロトコル	設定	値の例
IKE	認証アルゴリズム	**SHA-1**
	暗号化アルゴリズム	**AES-128**

プロトコル	設定	値の例
	DH グループ	グループ **2**
	IKE バージョン	**IKE v2**
	SA ライフサイクル	**86400**
	PRF アルゴリズム	**SHA-1**
	PSK	**123456**
IPsec	認証アルゴリズム	**SHA-1**
	暗号化アルゴリズム	**AES-128**
	DH グループ	グループ **2**
	IKE バージョン	**IKE v2**
	SA ライフサイクル	**86400**
	ネゴシエーションモード	**esp**

手順

ユーザーのゲートウェイ設定を **USG** シリーズ **Huawei** デバイスにロードするには、次の手順に従います。

1. **Huawei** のファイアウォール管理ページに移動します。
2. ネットワーク > インターフェイス > インターフェースリスト をクリックします **untrust** セキュリティゾーンにアップストリームインターネットインターフェイス **10GE1/0/0** を追加してから、パブリック **IP** アドレスを設定します。ダウンストリームイントラネットインターフェイス **10GE1/0/1** を **trust** セキュリティゾーンに追加してから、プライベート **IP** アドレスを設定します。
3. ポリシー > セキュリティポリシー > 追加 をクリックして、セキュリティーポリシーを作成します。
4. ネットワーク > **IPSec** > **IPSec**ポリシーリスト > 追加をクリックします。 次を参照してピアサイトを設定します。

   - ローカルインターフェイス ：アップストリームインターネットインターフェイスを選択します。 この例では、**10GE1/0/0** を選択します。
   - ピアアドレス：**Alibaba Cloud VPN Gateway** のパブリック **IP** アドレスを入力します。この例では、 **47.97.161.10** と入力します。
   - 事前共有キー ：事前共有キーは **Alibaba Cloud** 側の **PSK** と同様です。 この例では、**123456** と入力します。

5. 暗号化待ちデータフローページで、 追加をクリックします。 次の情報に従って、**VPC** 内のすべての **VSwitch CIDR** ブロックに対して暗号化するデータフローを追加します。
   - 送信元アドレス/アドレスセット：オンプレミスデータセンターのプライベート **IP** アドレスセグメントを入力します。 この例では、**10.10.10.0/24** と入力します。
   - 宛先アドレス/アドレスセット：**VPC** の **VSwitch IP** アドレスセグメントを入力します。この例では、**192.168.10.0/24** と **192.168.11.0/24** を入力します。
6. **IKE / IPsec** プロトコルページで、詳細をクリックします。 ダウンロードした **IPsec-VPN** 接続の設定に基づいて、**IKE** パラメータと **IPSec** パラメータを構成します。
7. ネットワーク > ルート > スタティックルート > スタティックルートリスト > 追加 をクリックしてファイアウォール用のスタティックルートを設定します。 デフォルトルートを追加すると、ネクストホップはファイアウォールのパブリック **IP** アドレスになります。 **VPC** にルートを追加すると、ネクストホップは **VPN Gateway** のパブリック **IP** アドレスになります。

3.1.2 H3C ファイアウォールの設定

IPsec-VPN を使用してサイト間接続を作成する場合は、**Alibaba Cloud VPN Gateway** 用に設定された **IPsec** 接続により、ローカルゲートウェイを設定する必要があります。 ここでは、**H3C** ファイアウォールを例にとり、**VPN** の設定方法を説明します。

- **IPsec** 接続が設定されていることを確認します。 詳しくは、*#unique_12*をご参照ください。
- **IPsec** 接続を作成後、作成した **IPsec** 接続の設定をダウンロードします。

  このチュートリアルでは、**IPsec** 接続の設定は以下になります。

  - **IPsec** 設定

設定		値
IKE	認証アルゴリズム	**sha1**
	暗号化アルゴリズム	**aes**
	DH グループ	**group2**
	IKE バージョン	**ikev1**
	SA ライフサイクル (秒)	**86400**
	ネゴシエーションモード	メイン
	PSK	**h3c**
IPsec	認証アルゴリズム	**sha1**
	暗号化アルゴリズム	**aes**
	DH グループ	**group2**

設定		値
	IKE Version	**ikev1**
	SA ライフサイクル **(**秒**)**	**86400**

- ネットワーク設定

設定		値
VPC	プライベート **CIDR** ブロック	**192.168.10.0/24**
	VPN Gateway のパブリック **IP**	**101.xxx.xxx.127**
IDC	プライベート **CIDR** ブロック	**192.168.66.0/24**
	ローカルゲートウェイのパブリック **IP**	**122.xxx.xxx.248**
	アップリンクパブリックポート	**Reth 1**
	ダウンリンクプライベートポート	**G 2/0/10**

1. **H3C** ファイアーウォールのコンソールにログインし、**[**ネットワーク**]** > **[VPN]** > **[IPsec]** > **[**ポリシー**]** をクリックします。
2. **Alibaba Cloud VPN Gateway** の **IPsec** 設定に基づいて、**H3C** ファイアーウォール **IPsec** ポリシーを設定します。 **[**保護されたデータストリーム**]** で **[**追加**]** をクリックし、ソース **IP** への **IDC** の **IP** アドレスの範囲および送信先 **IP** への **IP** アドレスの範囲を設定します。
3. **[IKE** プロポーサル**]** > **[**作成**]** をクリックします。

   Alibaba Cloud VPN Gateway の **IKE** 構成より、**IKE** プロポーサルを設定します。
4. **[**ネットワーク**]** > **[VPN]** > **[IPsec]** > **[**ポリシー**]** をクリックします。
5. 新しい **IPsec** ポリシーを選択し、**[**高度な設定**]** をクリックし、**IPsec** プロトコルを設定します。

   Alibaba Cloud VPN Gateway 用に設定された **IPsec** 接続の **IPsec** 情報により、**IPsec** プロトコルを設定します。

   ダウンリンクセキュリティポリシーおよびアップリンクセキュリティポリシーを作成します。

   Alibaba Cloud VPC からローカル **IDC** へのセキュリティポリシー設定は、以下の図のようになります。

6. [ポリシー] > [セキュリティポリシー] > [作成] をクリックします。

   Alibaba Cloud VPC からローカル **IDC** へのセキュリティポリシー設定は、以下の図のようになります。

   ローカル **IDC** から **Alibaba Cloud VPC** へのセキュリティポリシー設定は、以下の図のようになります。

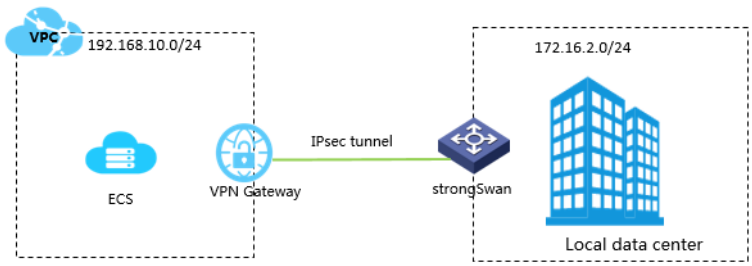
7. [ネットワーク] > [ルート] > [静的ルート] をクリックします。
8. デフォルトルートを追加し、アップリンクインターフェイスをアウトバウンドトラフィックのネクストホップとして設定します。 このチュートリアルでは、設定は不要です。

3.1.3 strongSwan の設定

IPsec-VPN を使用してサイト間接続を作成する場合、**Alibaba Cloud VPN Gateway** 用に設定された **IPsec** 接続によりローカルゲートウェイを設定する必要があります。 ここでは、**strongSwan** を例にとり、ローカルサイトでの **VPN** 設定の読み込み方法を解説します。

ここでは、**strongSwan** を例にとり **VPN** の設定方法を解説します。 ここで使用する設定は、以下のようになります。

- **Alibaba Cloud VPC** の **IP** アドレスの範囲は **"192.168.10.0/24"** となります。
- ローカルデータセンターの **IP** アドレスの範囲は **"172.16.2.0/24"** となります。
- **strongSwan** のパブリック **IP** は **"59.110.165.70"** となります。



前提条件

- **IPsec** 接続が設定されているか確認します。 詳しくは、*#unique_12*をご参照ください。
- **IPsec** 接続作成後、作成した **IPsec** 接続の設定をダウンロードします。 詳しくは、*#unique_10*をご参照ください。

strongSwan のインストール

1. 以下のコマンドを実行し、**strongSwan** をインストールします。

```
# yum install strongSwan
```

2. 以下のコマンドを実行し、インストールされたソフトウェアバージョンを参照します。

```
# strongswan version
```

strongSwan の設定

1. 以下のコマンドを実行し、*ipsec.conf* ファイルを開きます。

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

2. 以下の設定を参照し、*ipsec.conf* ファイルを更新します。

```
# 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 (Public IP of the loca gateway)
     right=119.23.227.125
     rightsubnet=192.168.10.0/24
     rightid=119.23.227.125 (Public IP of the VPN Gateway)
     auto=route
     ike=aes-sha1-modp1024
     ikelifetime=86400s
     esp=aes-sha1-modp1024
     lifetime=86400s
     type=tunnel
```

3. *ipsec.secrets* ファイルを設定します。

   a. 以下のコマンドを実行して、設定ファイルを開きます。

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

   b. 以下の設定を追加します。

```
59.110.165.70 119.23.227.125 : PSK yourpassword
```

4. システム転送を有効化します。

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

異なるシナリオでの設定例については、「異なるシナリオでの設定例」をご参照ください。

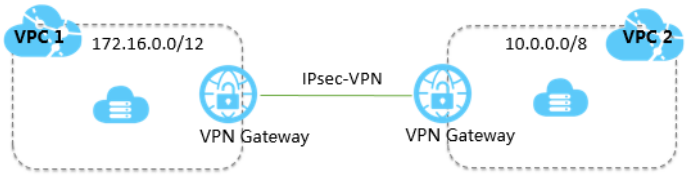
5. 以下のコマンドを実行し、**strongSwan** サービスを開始します。

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

6. **strongSwan** で **2** つのルーティングを設定します。 **1** つは **IDC** クライアントへ向かうリクエストの **strongSwan** へ転送に使用されます。 もう **1** つは **strongSwan** へ向かうリクエストのお使いの **IDC** クライアントへの転送に使用されます。

3.2 VPC 間接続の設定

このチュートリアルでは、**2** つの **VPC** を接続するため、 **IPsec-VPN** トンネルを介して **IPsec** 接続を作成する方法を説明します。



このチュートリアルでは、同じアカウントの **2** つの **VPC** を例として使用します。 異なるアカウントの **2** つの **VPC** を接続する手順は、同じアカウントで **2** つの **VPC** を接続する手順と同じです。 唯一の違いは、ピア **VPN Gateway** のパブリック **IP** アドレスを取得し、その **IP** アドレスを使用してカスタマーゲートウェイを作成する必要があることです。

VPC 名	VPC 名	VPC ID	VPC ID
VPC1	172.25.0.0/12	vpc-xxxxz0	ECS1
VPC2	10.0.0.0/8	vpc-xxxxut	ECS2

注：

VPN Gateways は、インターネット上に暗号化トンネルを作成することによって通信を可能にしているため、通信パフォーマンスはインターネット接続の品質によって異なります。通信品質に対する要求が高い場合は、 **Express Connect** を使用できます。 詳細については、*#unique_15*および *#unique_16*をご参照ください。

前提条件

これら **2** つの **VPC** の **IP** アドレス範囲は競合しません。

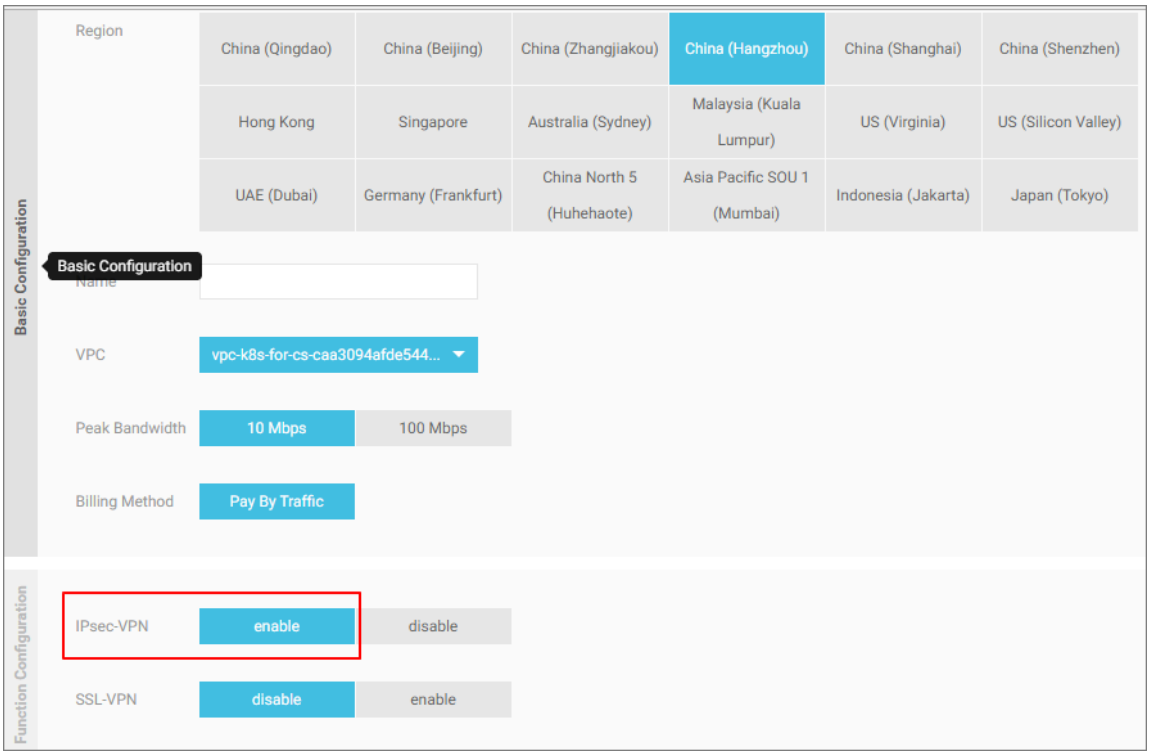
手順 1: VPN Gateway **を** 2 **つ作成**

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インドウで、**[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 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：
     VPC と**VPN Gateway** が同じリージョンであることを確認します。
   - **VPC :** 接続する **VPC** をクリックします。
   - **Bandwidth specification:** 帯域幅指定ををクリックします。 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。
   - **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からどこにいても **VPC** に接続できます。
   - **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。

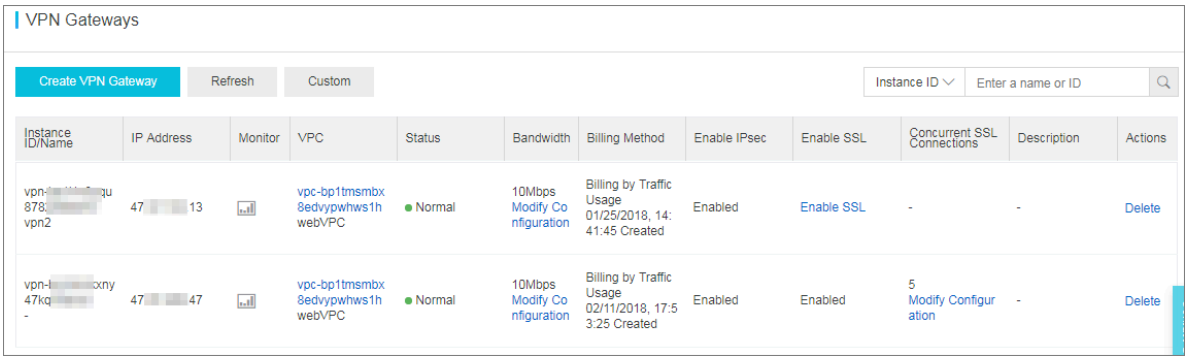
     注：
     このオプションは、 **SSL-VPN** 機能を有効にした後にのみ設定できます。



5. 他の VPC 用の VPN Gateway を作成するには、上記の手順を繰り返します。

   VPN Gateway の初期状態は、"Preparing" です。 約 2 分で "Normal" に変わります。 状態が "Normal" に変わると、 VPN Gateway が使用可能になります。 VPN Gateway が作成されると、 システムは自動的にインターネット IP を 2 つ割り当てます。

   注 :
   通常、 VPN Gateway の作成には 1～5 分かかります 。



   このチュートリアルでは、割り当てられている IP アドレスは 、以下の表のとおり、121. XXX. XX.143 および 118. XXX. XX.149 です。

VPC	VPN Gateway	IP アドレス
VPC 名: VPC1 ID : vpc-xxxxz0 IP アドレスの範囲: 172.16.0.0/12	vpn-xxxxxqwj	118.xxx.xx.149
VPC 名: VPC2 ID : vpc-xxxxut IP アドレスの範囲: 10.0.0.0/8	vpn-xxxxxl5z	121. XXX. XX.143

手順 2: 2 つのカスタマーゲートウェイの作成

1. 左側のナビゲーションウインドウで、[VPC] をクリックし、 >[カスタマーゲートウェイ] をクリックします。 .
2. [中国（杭州)] リージョンをクリックします。
3. カスタマーゲートウェイページで、[カスタマーゲートウェイの作成] をクリックします。

4. 次の情報に従って、カスタマーゲートウェイを設定します。
   - **Name :** カスタマーゲートウェイの名前を入力します。
   - **IP Address :** ピア **VPC** の **VPN Gateway** のパブリック **IP** アドレスを入力します。
   - **Description :** カスタマーゲートウェイの説明を入力します。
5. これらの手順を繰り返し、もう一方の **VPN Gateway** のパブリック **IP** アドレスを使用して、別のカスタマーゲートウェイを作成します。

   このチュートリアルでカスタマーゲートウェイを **2** つ作成した後の**VPC**、**VPN**ゲートウェイ、およびカスタマーゲートウェイの関係は次のとおりです。

VPC	VPN Gateway	IP アドレス	カスタマーゲートウェイ
VPC 名: VPC1 **ID : vpc-xxxxz0** **IP アドレスの範囲: 172.16.0.0/12**	**vpn-xxxxxqwj**	**121.xxx.xx.143**	**user_VPC1**
VPC 名: VPC2 **ID : vpc-xxxxut** **IP アドレスの範囲: 10.0.0.0/8**	**vpn-xxxxxl5z**	**118.xxx.xx.149**	**user_VPC**

手順 3: 2 **つの** IPsec **接続の作成**

VPN ゲートウェイとカスタマーゲートウェイを作成後、**2** つの **IPsec** 接続を作成して **VPN** チャネルを構築する必要があります。

1. 左側のナビゲーションウインドウで、 **[VPN]** をクリックし、 > **[IPsec** 接続**]** をクリックします。**.**
2. **[**中国（杭州**)]** リージョンをクリックします。
3. **IPsec** 接続 ページで**[**ピアリング接続の作成**]** をクリックします。

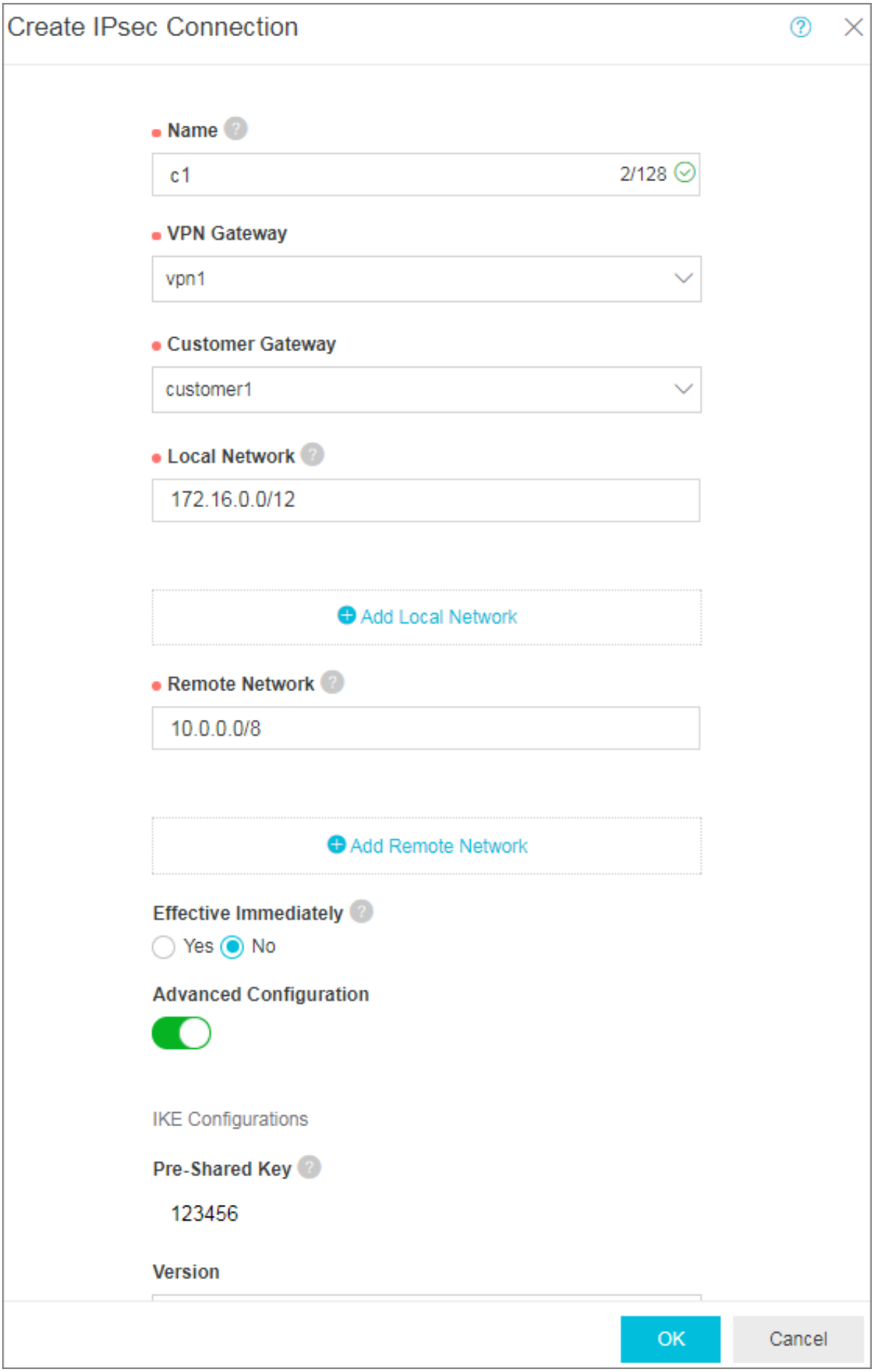
4. 次の情報に従って、 **IPsec** 接続を設定します。

   - **Name : IPsec** 接続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。 このチュートリアルでは、 **VPC1** の **VPN Gateway vpn-xxxxxqwj** を使用しています。
   - **Customer Gateway:** ピア **VPN Gateway** のパブリック **IP** を使用して作成したカスタマーゲートウェイをクリックします。 このチュートリアルでは、 **VPC2** のカスタマーゲートウェイ **user_VPC2** を使用しています。

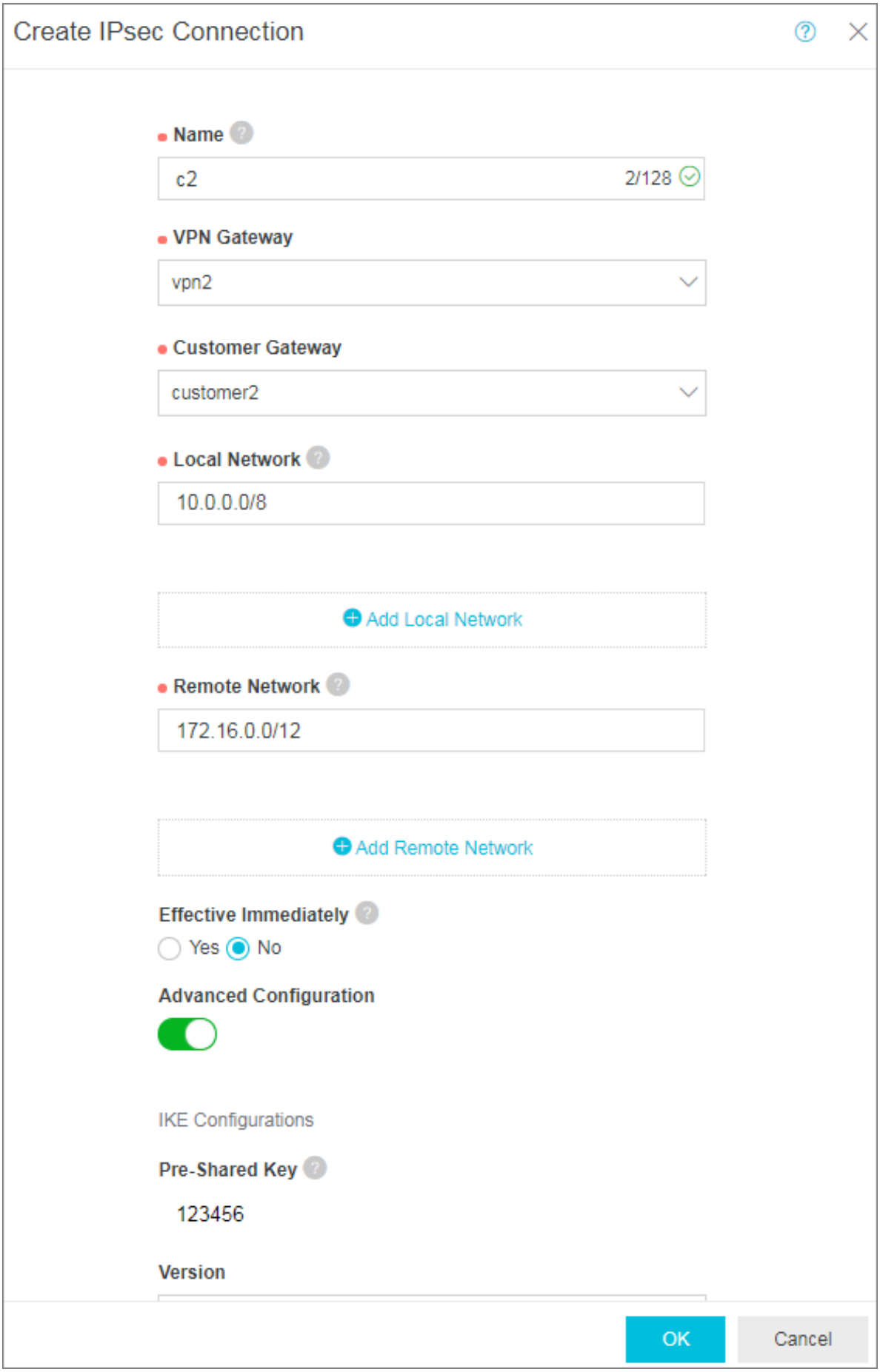
     .
   - **Local Network :** クリックした **VPN Gateway** が属する **VCP** の **IP** アドレス範囲を入力します。 このチュートリアルでは、 **VPC1** の **IP** アドレス範囲 **172.16.0.0/12** を入力しています。
   - **Remote Network:** ピア **VPC** の **IP** アドレス範囲を入力します。 このチュートリアルでは、 **VPC1** の **IP** アドレス範囲**10.0.0.0/8** を入力しています。
   - **Pre-Shared Key:** 事前共有キーを入力します。 このチュートリアルでは、**123456** を入力しています。 この値は、もう一方の **IPsec** 接続で設定した値と同じでなければなりません。

5. 別の **IPsec** 接続を作成するには、この手順を繰り返します。

   このチュートリアルでは、 **VPC1** の **IPsec** の接続構成は次のとおりです。


Create IPsec Connection
Name
c1
2/128
VPN Gateway
vpn1
Customer Gateway
customer1
Local Network
172.16.0.0/12
Add Local Network
Remote Network
10.0.0.0/8
Add Remote Network
Effective Immediately
Yes
No
Advanced Configuration
IKE Configurations
Pre-Shared Key
123456
Version
OK
Cancel

このチュートリアルでは、 **VPC2** の **IPsec** の接続構成は次のとおりです。


Create IPsec Connection
Name
c2
2/128
VPN Gateway
vpn2
Customer Gateway
customer2
Local Network
10.0.0.0/8
Add Local Network
Remote Network
172.16.0.0/12
Add Remote Network
Effective Immediately
Yes
No
Advanced Configuration
IKE Configurations
Pre-Shared Key
123456
Version
OK
Cancel

手順 4: ルートの設定

1. 左側のナビゲーションウインドウで、 [ルートテーブル] をクリックします。
2. 接続先 VPC が属する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。
3. VPC1 を検索し、 [管理] をクリックします。
4. ルートテーブル ページで、[ルートエントリの追加] をクリックします。
5. 次の情報に従ってルートテーブルを設定し、[OK] をクリックします。
   - **Destination CIDR Block:** ピア VPC の IP アドレス範囲を入力します。 このチュートリアルでは、 VPC2 の IP アドレス範囲 10.0.0.0/8 が入力されています。
   - **Next Hop Type:** [VPN Gateway] をクリックします。
   - **VPN Gateway:** ローカル VPC にデプロイされた VPN Gateway をクリックします。 このチュートリアルでは、 VPC1 用に作成された VPN ゲートウェイを選択しています。
6. これらの手順を繰り返して、 VPC2 のルートエントリを追加します。 ルートエントリでは、ターゲット CIDR ブロックは 172.16.0.0/12 であり、 次のホップは VPC2 の VPN Gatewayです。

   このチュートリアルでは、ルート設定は次のとおりです。

VPC	Destination CIDR block	Next hop type	Next hop
VPC1	10.0.0.0/8	VPN Gateway	このチュートリアルで VPC1 用に作成された VPN Gateway は vpn-xxxxxqwj です。
VPC2	172.25.0.0/12	VPN Gateway	このチュートリアルで VPC2 用に作成された VPN Gateway は vpn-xxxxxl5z です。

手順 5: 接続の確認

ECS1 にログインし、ECS2 のプライベート IP アドレスに ping を実行して、接続が確立されているかどうかを確認します。

```
root@i                              :~# ping 10.0.   .100
PING 10.0.182.100 (10.0.182.100) 56(84) bytes of data.
64 bytes from 10.0.   .100: icmp_seq=1 ttl=62 time=3.41 ms
64 bytes from 10.0.   .100: icmp_seq=2 ttl=62 time=2.40 ms
64 bytes from 10.0.   .100: icmp_seq=3 ttl=62 time=2.32 ms
64 bytes from 10.0.   .100: icmp_seq=4 ttl=62 time=2.43 ms

--- 10.0.   .100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.327/2.646/3.414/0.445 ms
```

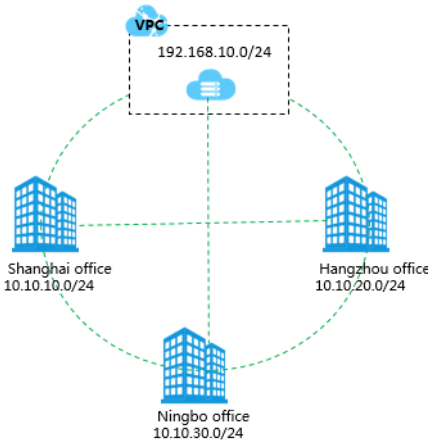
3.3 マルチサイト接続の設定

複数のサイトと拠点の間に **IPsec-VPN** 接続を作成できます。 **VPN-Hub** 機能を使用すると、接続されたサイトは接続された **VPC** と通信することができ、他のサイトとも通信できます。 **VPN-Hub** は、複数のサイト間でイントラネット通信を確立する大規模エンタープライズのニーズを満たします。

VPN-Hub の概要

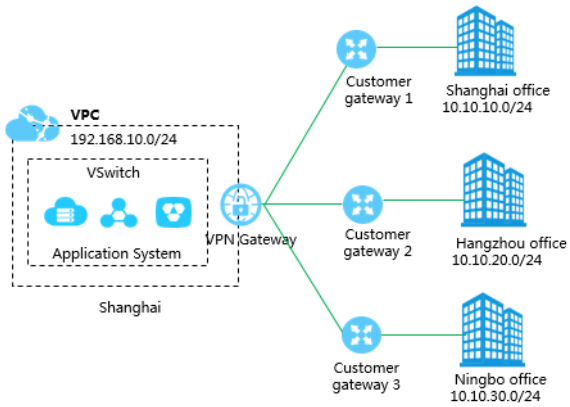
VPN-Hub 機能はデフォルトで有効になっています。 マルチサイト接続を実現するには、対応する **IPsec-VPN** 接続を作成する必要があります。 **VPN Gateway** は、最大 **10** 個の **IPsec-VPN** 接続を設定することができます。 したがって、**1** つの **VPN Gateway** に最大 **10** のオフィスサイトを接続できます。

次のシナリオを使用して、上海、杭州、寧波のオフィスサイトを接続する方法を説明します。 開始する前に、各オフィスサイトのゲートウェイデバイスのパブリック **IP** アドレスを取得するようにしてください。



次の図に示すように、3 つのオフィスサイト (上海、杭州、寧波) を接続するには、VPN Gateway と 3 つのカスタマーゲートウェイの作成、および 3 つの IPsec-VPN 接続の確立のみが必要です。

> 注：
> 接続されるすべてのサイトの IP アドレス範囲が互いに競合しないことを確認してください。



手順 1：VPN Gateway の作成

VPC が属するリージョンに VPN Gateway を作成します。 この VPN Gateway に対して 3 つの IPsec-VPN 接続を確立し、上海、杭州、寧波のオフィスサイトに接続します。 詳細は、「*#unique_18*」をご参照ください。

> 注：
> IPsec-VPN 機能が有効になっていることを確認してください。

手順 2：上海オフィスへの IPsec-VPN 接続の作成

1. カスタマーゲートウェイを作成し、ローカルゲートウェイデバイスのパブリック IP アドレスを Alibaba Cloud に登録して、IPsec-VPN 接続を確立します。

   カスタマーゲートウェイの IP アドレスは、上海オフィスのゲートウェイデバイスのパブリック IP アドレスです。 詳細は、「*#unique_19*」をご参照ください。

2. IPsec-VPN 接続を作成します。

   IPsec 接続を作成して、VPN Gateway とカスタマーゲートウェイを接続します。 詳細は、「*#unique_20*」をご参照ください。

3. ローカルオフィスサイトのゲートウェイデバイスに VPN 設定をロードします。

   ローカルオフィスサイトのゲートウェイデバイスの要件に合わせて、VPN 設定をロードします。 詳細は、「ローカルゲートウェイ設定」をご参照ください。

手順 3：他の 2 つのサイトへの IPsec-VPN 接続の作成

手順 **2** と同じ手順で、杭州オフィスと寧波オフィス用の **2** つの **IPsec** 接続を作成します。

手順 4：VPN Gateway ルートの設定

VPN Gateway ルートを設定するには、次の手順を実行します。

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 Gateways]** を選択します。
3. **[VPN Gateways]** ページで、**VPN Gateway** のリージョンを選択します。
4. ターゲット **VPN Gateway** を見つけ、**[ID/名前]** 列のインスタンス **ID** をクリックします。
5. **[宛先ベースルーティング]** ページで、**[ルートエントリの追加]** をクリックします。
6. 次の情報に従って **3** つのルートエントリを設定し、**[OK]** をクリックします。
   - 宛先 **CIDR** ブロック：アクセスするプライベート **CIDR** ブロックを入力します。
   - ネクストホップ：ターゲット **IPsec-VPN** 接続インスタンスを選択します。
   - **VPC** に公開：新しいルートを **VPC** ルートテーブルに公開するかどうかを選択します。
   - 重み：重みを選択します。

   この例では、次の宛先ベースルートを設定します。

宛先 CIDR ブロック	ネクストホップ	VPC に公開	重み
10.10.10.0/24	**IPsec-VPN** 接続インスタンス **1**	はい	**100**
10.10.20.0/24	**IPsec-VPN** 接続インスタンス **2**	はい	**100**
10.10.30.0/24	**IPsec-VPN** 接続インスタンス **3**	はい	**100**

これで、**3** つのオフィスサイトへの **IPsec-VPN** 接続が確立されました。 各オフィスサイトは **VPC** との通信が可能になり、イントラネットを介して他のオフィスサイトと通信できるようになりました。