Alibaba Cloud
VPN网关

IPsec-VPN クイックスタート

Document Version20200707

目次

1 チュートリアルの概要.....**1**
2 サイト間接続の設定.....**3**

1 チュートリアルの概要

本ページでは、IPsec-VPN を使用して VPC をローカルデータセンターに接続する方法を説明するためのチュートリアルが含まれています。 また、IPsec-VPN を使用して 2 つの VPC を接続する方法を説明するチュートリアルも含まれています。

前提条件

サイト間 VPN 接続を作成する前に、次の条件が満たされていることをご確認ください。

- ローカルデータセンターのゲートウェイデバイスが、IKEv1 プロトコルと IKEv2 プロトコルをサポート

  IPsec-VPN は、IKEv1 プロトコルと IKEv2 プロトコルをサポートしています。 この 2 つのプロトコルをサポートするデバイスは Alibaba Cloud VPN Gateway に接続できます。 サポートされるデバイスには、Huawei、H3C、SANGFOR、Cisco、ASN、Juniper、SonicWall、Nokia、IBM、Yamaha および Ixia が含まれます。
- ローカルゲートウェイに静的 IP アドレスが設定されている
- 接続する VPC とローカルデータセンターの IP アドレス範囲が互いに競合していない

サイト間接続の作成

IPsec-VPN を使用して異なるサイトを接続するには、次の手順を実行する必要があります。

1. IPsec-VPN を有効化した VPN Gateway の作成

   VPN Gateway 内で最大 10 の IPsec 接続を確立できます。
2. 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と、ローカルゲートウェイの設定を Alibaba Cloud にアップロードできるようになります。 カスタマーゲートウェイは、複数の VPN Gateway に接続可能です。
3. IPsec 接続の作成

   IPsec コネクションを作成して、VPN Gateway とカスタマーゲートウェイを接続し、暗号化された通信トンネルを確立します。
4. ローカルゲートウェイの設定

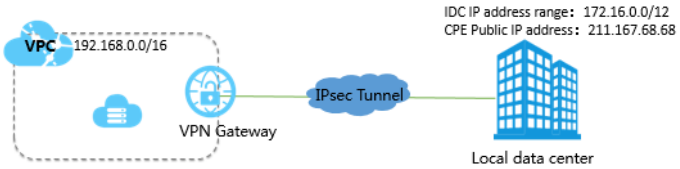
   IPsec コネクションの設定に従って、ローカルゲートウェイを設定します。 詳細については、#unique_2、Yamaha RTX ルーター設定例および #unique_3 をご参照ください。

5. ルートとセキュリティグループの設定

最後に、データ転送を完了させるため、対応する VPC のルーティングを設定する必要があります。

2 サイト間接続の設定

本ページでは、ローカルデータセンターと VPC を接続するためのサイト間接続を作成する方法を説明します。



前提条件

IPsec 接続を作成する前に、次の要件を満たす必要があります。

- ローカルデータセンターのゲートウェイデバイスをご確認ください。 Alibaba Cloud VPN ゲートウェイは、標準の IKEv1 および IKEv2 プロトコルをサポートしています。 この 2 つのプロトコルをサポートするデバイスは、Alibaba VPN Gateway に接続できます。 サポートしているデバイスには、Huawei、H3C、Cisco、ASN、Juniper、SonicWall、Nokia、IBM、Yamaha および Ixia があります。
- ローカルゲートウェイに静的 IP アドレスが設定されていること。
- 接続する VPC とローカルデータセンターの IP アドレス範囲が互いに競合していないこと。

手順 1：VPN Gateway の作成

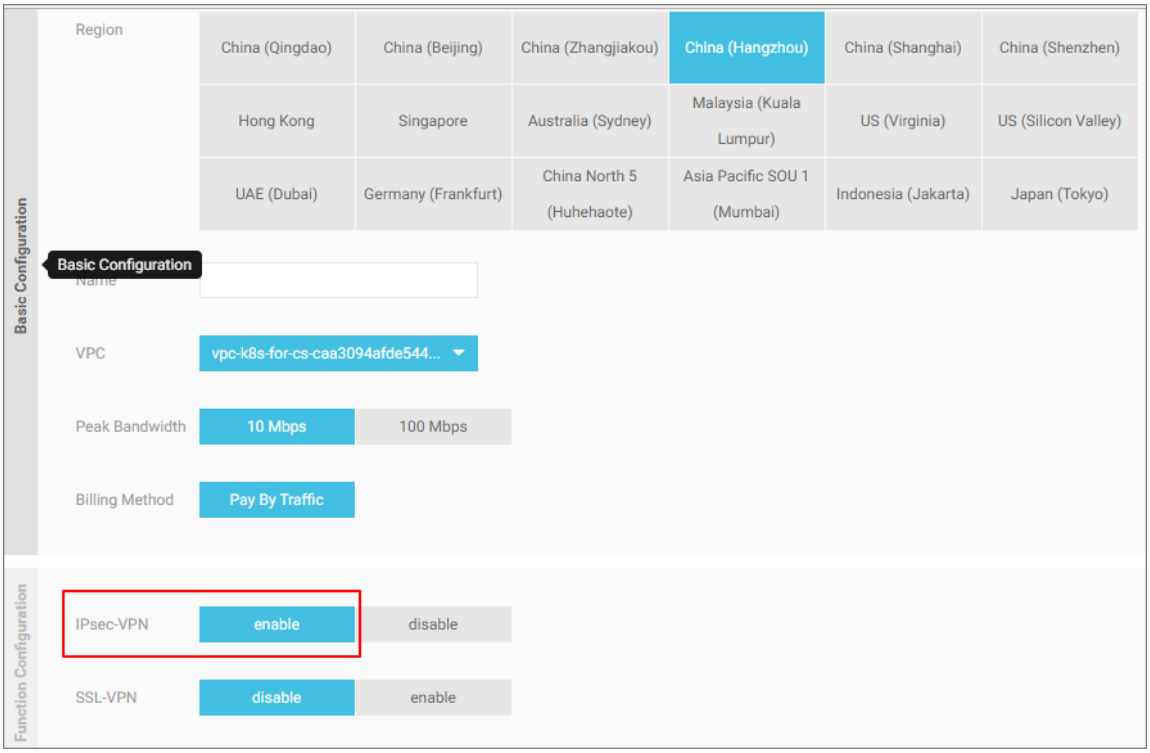
1. VPC コンソールにログインします。
2. 左側のナビゲーションウインドウで、**[VPN] > [VPN Gateways]** をクリックします。
3. VPN Gateway ページで、**[VPN Gateway** の作成**]** をクリックします。
4. 購入ページで、VPN Gateway を設定して支払いを完了させます。 このチュートリアルでは、VPN Gateway は次の設定を使用します。
   - <p data-spm-anchor-id="a2762.11472859.0.i12.7588203beUXIor">**Region**: VPN Gateway 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：

VCP とVPN ゲートウェイ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**：帯域幅指定をクリックします。 帯域幅指定は、VPN ゲートウェイのインターネット帯域幅です。
- **IPsec-VPN**：IPsec-VPN 機能を有効にするかをクリックします。
- **SSL-VPN**：SSL-VPN 機能を有効にするかを設定します。 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クリックします。

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。



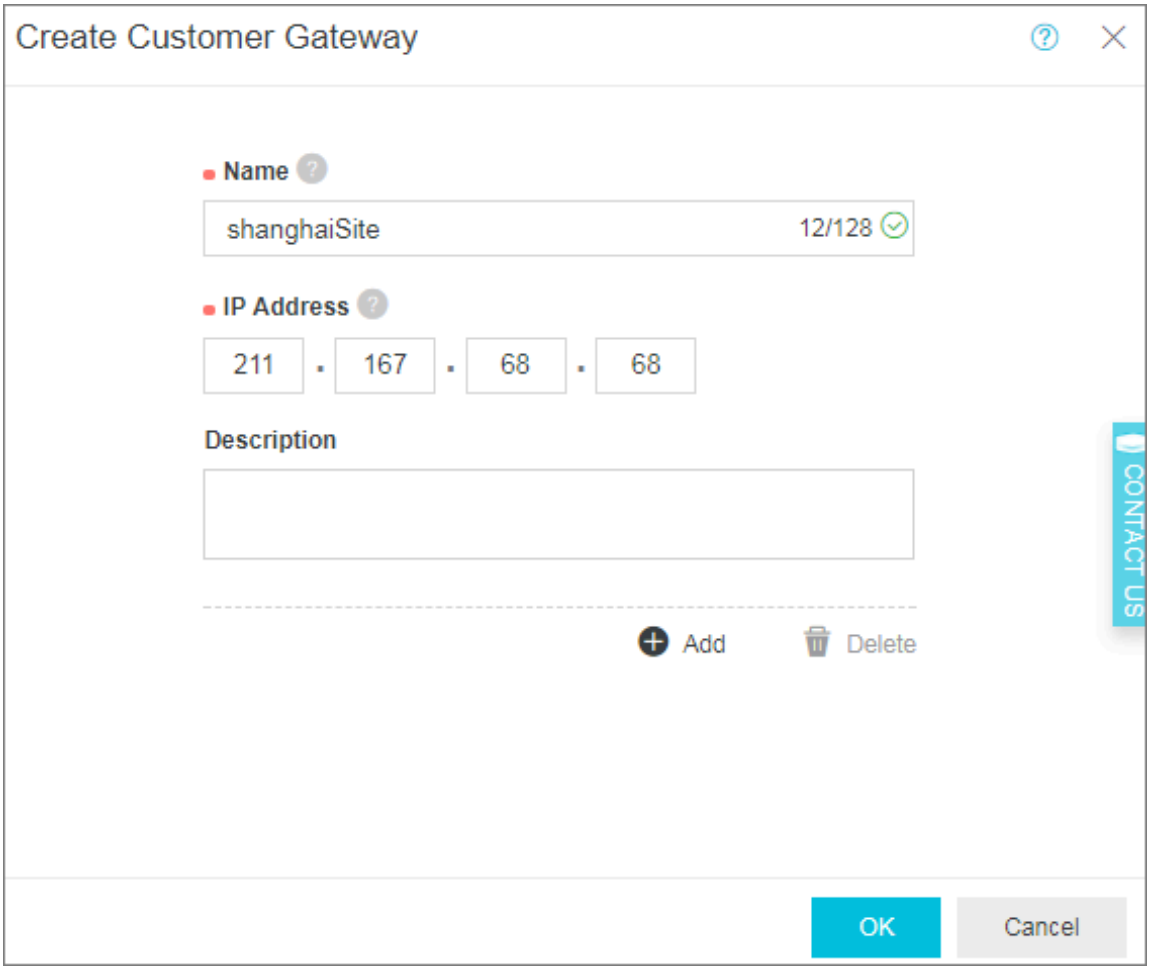
5. VPN Gateway ページに戻り、**[中国 (杭州)]** リージョンをクリックすると、作成した VPN Gateway が表示されます。

   VPN Gateway の初期ステータスは、"Preparing" です。 約 2 分で "Normal" に変わります。ステータスが "Normal"に変わると、VPN Gateway が使用可能になります。

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

手順 2：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、**[VPN] > [**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名を入力します。
   - **IP Address**：ローカルゲートウェイ用に設定されたパブリック IP を入力します。 このチュートリアルでは、211.167.68.68 を使用します。
   - **Description**: カスタマーゲートウェイの説明を入力します。



5. カスタマーゲイトウェイの作成ページで、**[**追加 **+]** をクリックして複数のカスタマーゲートウェイを追加します。

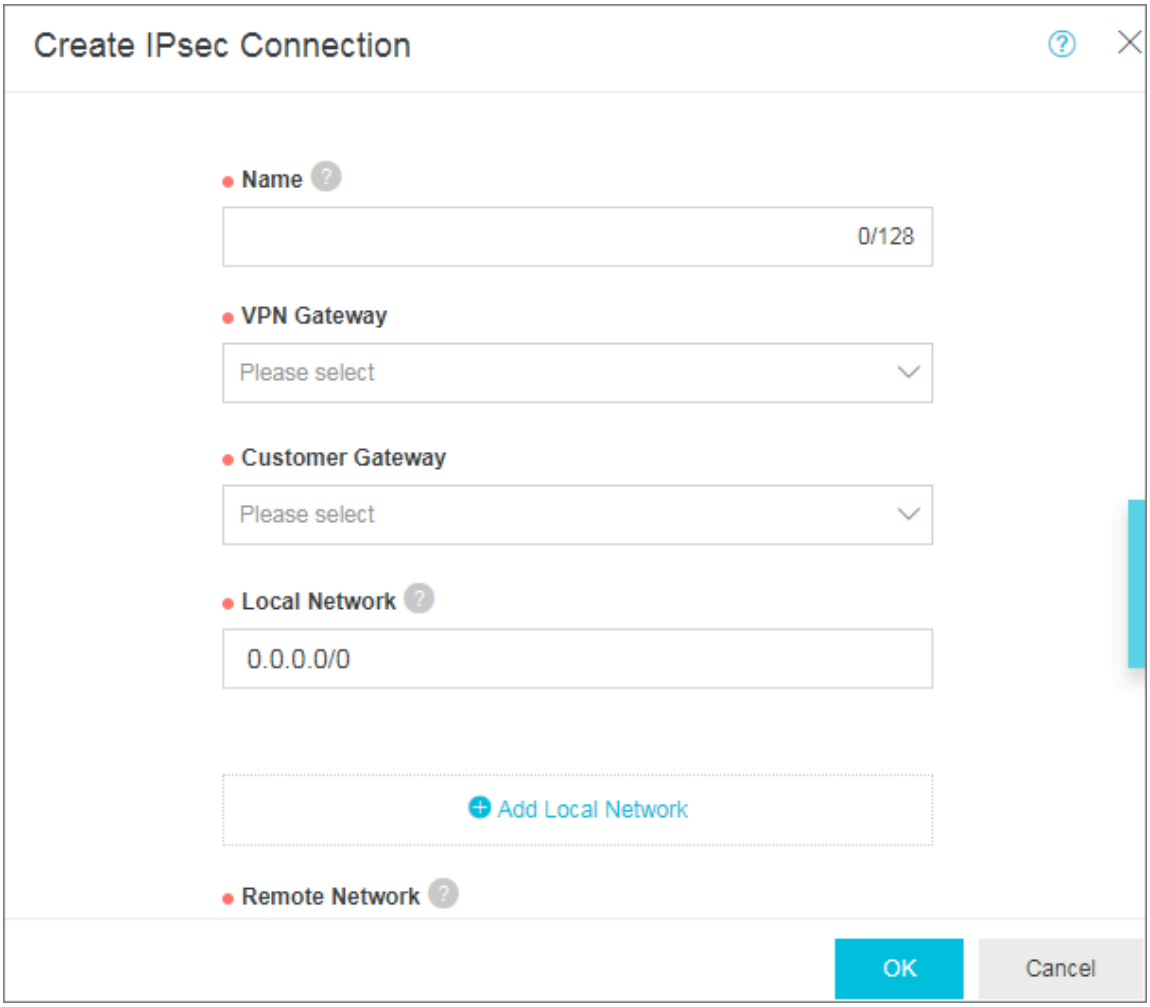
手順 3：IPsec 接続の作成

1. 左側のナビゲーションウインドウで、**[VPN] > [Psec** 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、**[IPsec** 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。

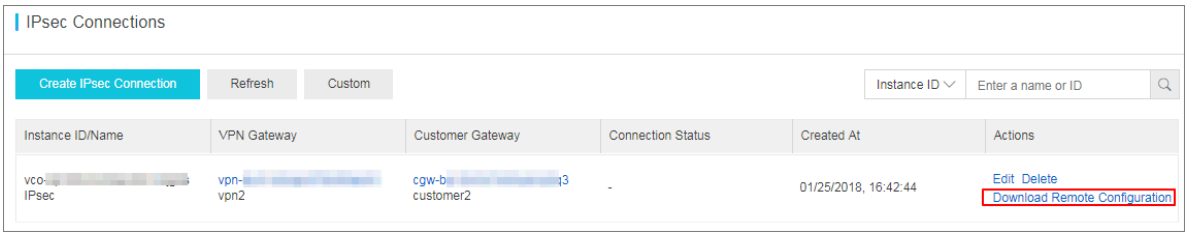
   - **Name**: IPsec 接続の名前を入力します。
   - **VPN Gateway**: 作成した VPN Gateway をクリックします。
   - **Customer Gateway**: 作成したカスタマーゲートウェイをクリックします。
   - **Local Network**: VPC の IP アドレス範囲を入力します。 このチュートリアルでは、192.168.0.0/16 を使用します。
   - **Remote Network**: ローカルデータセンターの CIDR ブロックを入力します。 このチュートリアルでは、172.16.0.0/12 を使用します。
   - **Pre-Shared Key**: 事前共有キーを入力します。 この値は、ローカルゲートウェイで設定した値と同じでなければなりません。

   他のオプションにはデフォルト設定を使用してください。



ステップ 4 : ローカルゲートウェイの設定

1. 左側のナビゲーションウインドウで、**[VPN]** > **[IPsec Connections]** の順に、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. 対象の IPsec 接続を検索し、**[Download Config]** をクリックします。

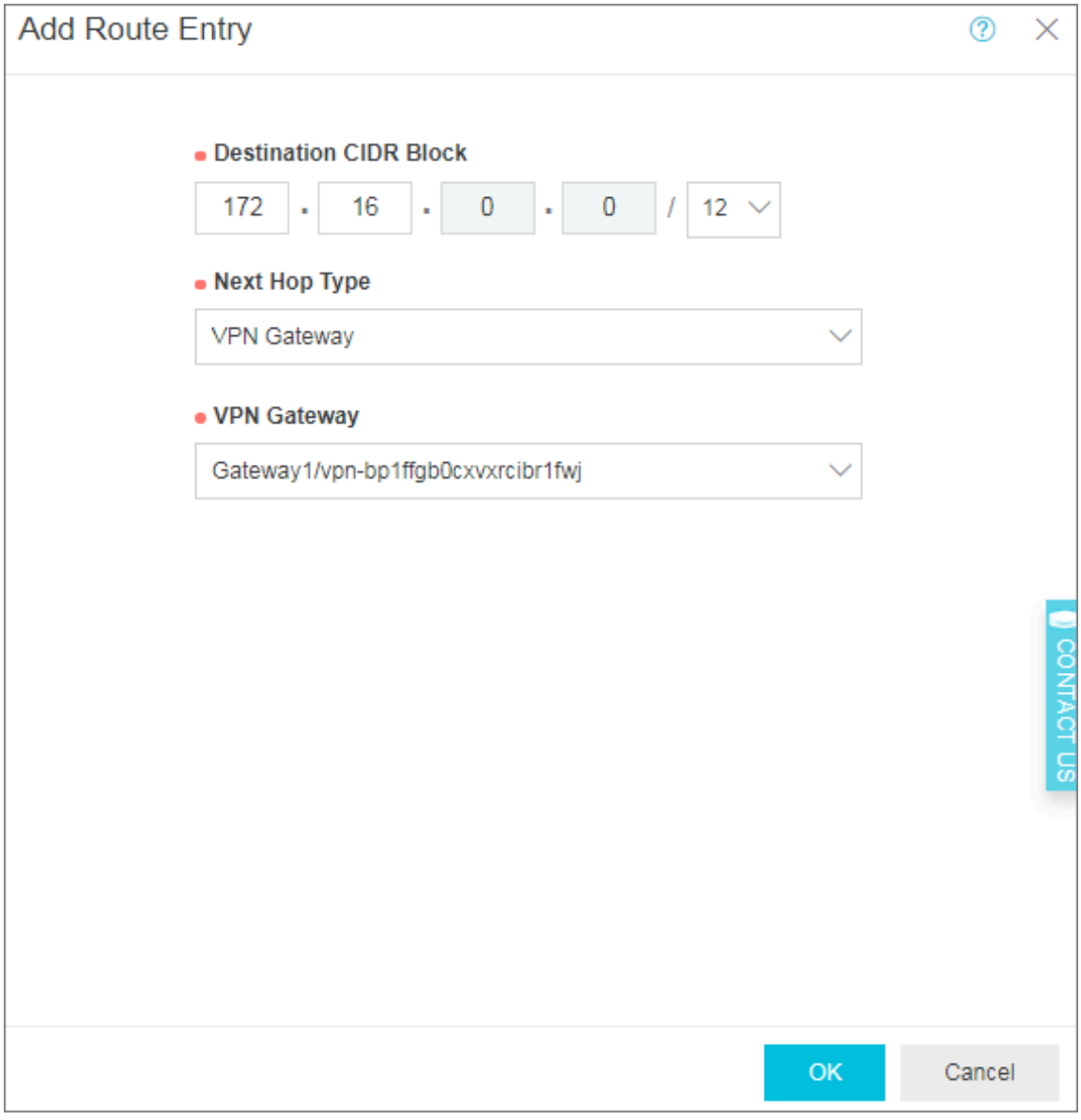


4. 適宜、ローカルゲートウェイを設定します。 詳細については、#unique_2、Yamaha RTX ルーター設定例および #unique_3をご参照ください。

   ダウンロード設定にある RemoteSubnet と LocalSubnet は、IPsec 接続作成時のローカルネットワークとリモートネットワークとは逆になります。 VPN Gateway の観点から、リモートネットワークはローカル IDC、ローカルネットワークは VPC です。

手順 5 : 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. 接続した VPC が属する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。
3. 対象のVPC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エントリを設定し、**[OK]** をクリックします。
   - **Destination CIDR Block**: ローカル IDC 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、172.16.0.0/12 を使用します。
   - **Next Hop Type**: VPN Gateway を選択します。
   - **VPN Gateway**: 作成した VPN Gateway を選択します。



手順 6: 接続の確認

接続されている VPC ネットワークの ECS インスタンスに (パブリック IP なしで) ログインします。 ローカルデータセンター内サーバーのプライベート 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。