Alibaba Cloud
VPN网关

プロダクト紹介

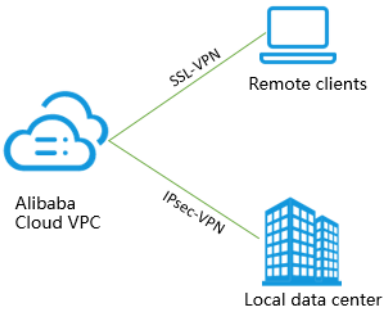
Document Version20200707

目次

1 VPN Gateway の概要

VPN Gateway とは、暗号化されたチャネルを介して企業のデータセンター、企業オフィスネットワーク、またはインターネット端末を Alibaba Cloud VPC に安全かつ確実に接続するインターネットベースのサービスです。 VPN Gateway は、IPsec-VPN 接続と SSL-VPN 接続の両方をサポートしています。

> 注：
> Alibaba Cloud VPN Gateway は、国内のポリシーおよび法律に従ってサービスを提供しており、インターネットにアクセスする機能は提供していません。



特徴

VPN Gateway には次の特徴があります。

- IPsec-VPN

  IPsec-VPN はサイト間 VPN 接続を提供しています。 IPsec-VPN 接続を使用して、VPC をローカルデータセンターに接続したり、２つの VPC を接続したりすることができます。 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、VPN Gateway に接続できます。 両方のプロトコルをサポートするデバイスには、 Huawei、H3C、Hillstone、Sangfor、Cisco、ASA、Juniper、SonicWall、Nokia、IBM、Yamaha および Ixia があります。

  詳細については、#unique_2 および #unique_3 をご参照ください。

- SSL-VPN

  SSL-VPN 接続を作成して、リモートクライアントを VPC にデプロイされたアプリケーションへ接続することができます。 デプロイメントの完了時、クライアントで証明書をロードして接続を開始するだけで済みます。

  詳細については、#unique_4、#unique_5 および #unique_6 をご参照ください。

利点

VPN Gateway には、次のような利点があります。

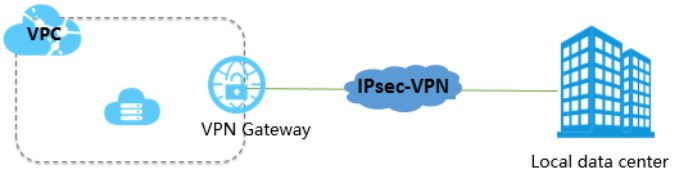
- 高セキュリティ性: IKE および IPsec プロトコルを使用して送信データを暗号化し、データのセキュリティと信頼性を確保できます。
- 高可用性: アクティブ/スタンバイホットバックアップアーキテクチャを使用すると、VPN Gateway は 1 秒以内に自動的にフェイルオーバーモードになります。 クライアントデータ処理への影響を最小限にすることができます。
- 低コスト: インターネットベースの暗号化チャネルは、専用回線よりも費用対効果が高いため、ハイブリッドクラウドを迅速に構築できます。
- 使いやすさ: 設定がシンプルで、すぐに使い始めることができます。

2 シナリオ

サイト間接続

IPsec VPN トンネルを作成することでハイブリッドクラウド環境を構築し、VPC をローカルデータセンターに接続することができます。

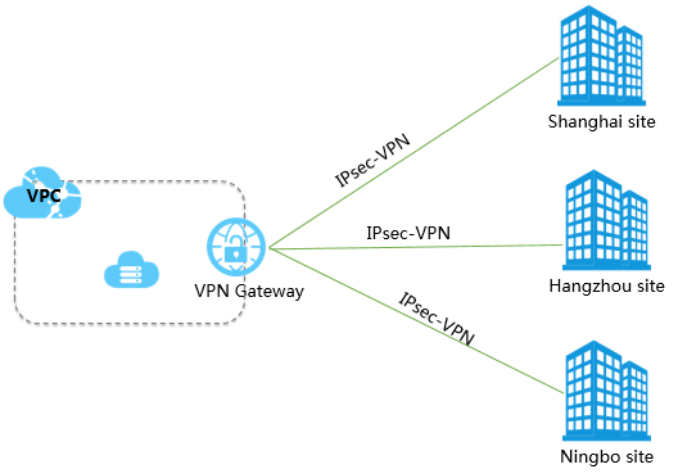
> 注：
> IPsec 接続では、ローカルデータセンターと VPC の IP アドレス範囲が互いに競合しないようにすることが必要です。 加えて、静的なパブリック IP がローカルゲートウェイデバイスに設定されている必要があります。



複数サイト接続

複数の IPsec-VPN 接続を作成して、複数サイトを VPC に接続することができます。 VPN Gateway が提供する VPN-Hub 機能により、各サイトは VPC と通信するだけでなく、互いに通信することもできます。 VPN-Hub は、大規模企業のニーズを満たし、さまざまなサイト間でイントラネット通信を確立します。

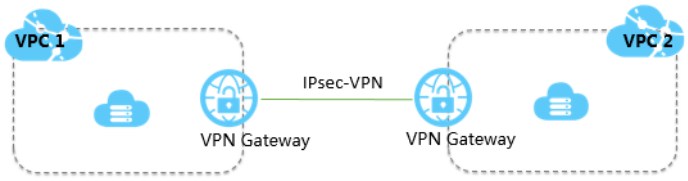
> 注：
> IPsec 接続では、各サイトの IP アドレス範囲が、接続する VPC の IP アドレス範囲と競合しないようにする必要があります。



VPC 間接続

IPsec VPN トンネルを介して 2 つの VPC 間接続を作成できます。

> 注：
> VPC の IP アドレス範囲は互いに競合することはできません。

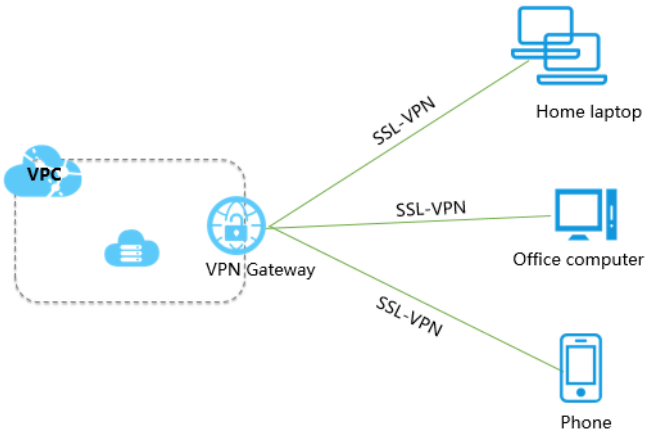


ポイント対サイト接続

SSL VPN トンネルを介してクライアントを VPC に接続することで、リモート作業のニーズに対応できます。 SSL-VPN コネクションでは、インターネットアクセスを利用できる限り、VPC にデプロイされたアプリケーションに安全にアクセスできます。

SSL-VPN 接続は、Windows、Linux、Mac、IOS、Android など、さまざまなオペレーティングシステムのクライアントからのリモートアクセスをサポートしています。

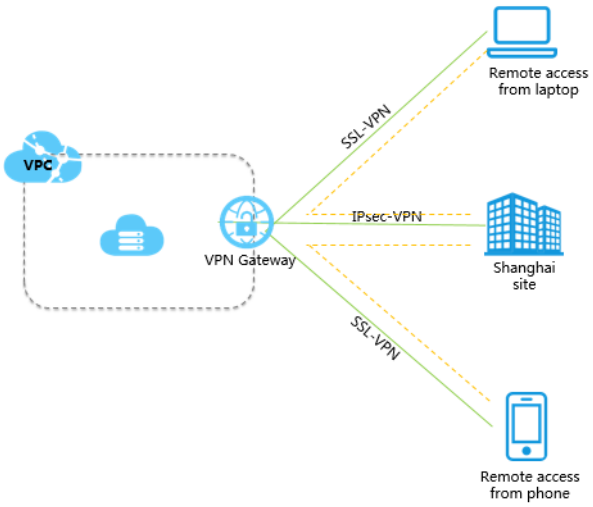
> 注：
> VPC アクセスに使用されるクライアントの IP アドレス範囲は、VPC の IP アドレス範囲と競合することはできません。



IPsec-VPN 接続と SSL-VPN 接続

IPsec と SSL-VPN 接続を組み合わせて、ネットワークトポロジーを拡張することができます。 接続が確立されると、クライアントは接続された VPC にデプロイされているアプリケーションにアクセスでき、また、接続されたオフィスサイトにデプロイされているアプリケーションにもアクセスすることができます。

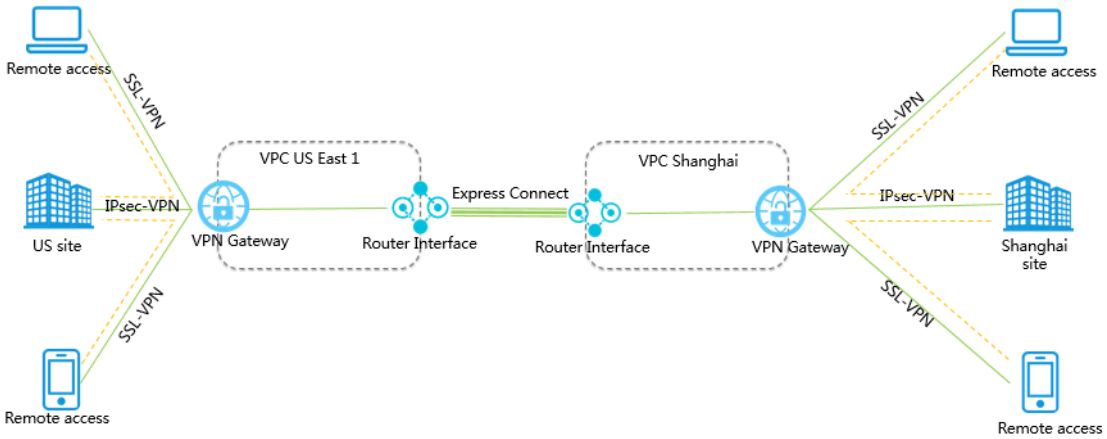
> 注：
> 接続されるすべてのプライベート IP アドレス範囲は互いに競合することはできません。



複数のイントラネット接続 (VPN Gateway と Express Connect)

多国籍企業の場合、Express Connect を使用して 2 つの VPC を低レイテンシで接続し、また VPN Gateway を使用して低コストでローカルサイトに接続して安全で信頼性の高いイントラネット接続を構築することが可能です。

> 注：
> 接続されるすべてのプライベート IP アドレス範囲は互いに競合することはできません。



3 制限

リソース	デフォルト制限	例外
1アカウントあたりの VPN Gateway 数	30	クォータを増加させるためにはチケットを起票ください
リージョン内のカスタマーゲートウェイの数	30	なし
1 VPN Gateway ごとの IPsec 接続数	10	なし
1 VPN Gateway ごとのSSLサーバー数	1	なし
SSL サーバーポート	以下のポートは許可されていません。 22、2222、22222、9000、9001、9002、7505、80、443、53、68、123、4510、4560、500、4500	なし
1 SSL サーバーごとのクライアント	50	なし
最大 SSL クライアント作成数	100 回	なし
SSL クライアント証明書の有効期間	3 年間	なし