Alibaba Cloud vpn gateway

FAQ

Document Version20190702

目次

1 VPN Gateway

1. VPN Gateway はクラシックネットワークをサポートしていますか。

サポートしていません。 VPN Gateway は VPC ネットワークのみのサポートです。 クラシックネットワークで VPN Gateway を使用する場合は、VPC で ClassicLink 機能を有効化する必要があります。 詳しくは、クラシックネットワークでの IPsec-VPN の利用をご参照ください。

2. ローカルサイトが IPsec-VPN 機能を通じて VPC にアクセスするための前提条件は何ですか。

静的パブリック IP および、IKEv1 と IKEv2 をサポートするゲートウェイデバイスが必要です。 VPC の CIDR ブロックおよびローカルサイトの CIDR ブロックがお互いに重複できません。 詳しくは、サイト間接続の設定をご参照ください。

3. 異なるリージョンでの VPC により、相互通信を行うために VPN Gateway を使用できますか。

できます。 詳しくは、*#unique_4*をご参照ください。

4. どのローカルゲートウェイが VPN Gateway をサポートしますか。

IPsec 接続は IKEv1 プロトコルおよび IKEv2 プロトコルをサポートします。 そのため、これら 2 つのプロトコルをサポートするどのデバイスでも、Alibaba Cloud VPN Gateway に接続できます。 サポートするデバイスは、Huawei 製、H3C 製、Cisco 製、ASN 製、Juniper 製、SonicWall 製、Nokia 製、IBM 製および Ixia 製のものです。 詳しくは、*#unique_5*をご参照ください。

5. VPN Gateway は SSL-VPN はサポートしていますか。

サポートしています。 詳しくは、チュートリアルの概要をご参照ください。

6. それぞれの VPN Gateway にいくつの IPsec 接続を作成できますか。

それぞれの VPN Gateway は最大 10 個の IPsec 接続をサポートできます。 さらに IPsec 接続が必要な場合は、さらに VPN Gateway を作成します。

7. VPN Gateway を利用してインターネットへアクセスできますか。

いいえ、できません。 VPN Gateway により VPC へのイントラネットアクセスのみ提供されます。 インターネットへのアクセスは提供されません。

8. VPN Gateway により接続された 2 つの VPC 間のトラフィックはインターネットを介しますか。

介しません。 リージョン間の VPC 相互接続は VPN を通して行われ、トラフィックは、インターネットの代わりに Alibaba Cloud ネットワークを通過します。

9. 1 つの IPsec 接続で複数のリモートネットワークを設定できますか。

できます。 コンマによりネットワークを分けることができます。 IKEv2 プロトコルの利用を推奨します。

10. VPN Gateway 設定をダウングレードできますか。

できます。 設定のダウングレードには、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。

11. SSL-VPN 機能の起動前に購入した VPN Gateway インスタンスで SSL-VPN 機能を使用できますか。

SSL-VPN 機能の起動前に購入した VPN Gateway インスタンスで SSL-VPN 機能を直接有効化できません。 このような状況で SSL-VPN 機能を有効化する場合は、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。

2 IPsec 接続

1. IPsec 接続ステータスが "IKE トンネルネゴシエーションのフェーズ 1 が失敗しました" となる場合、どうしたらいいですか。

もっとも多い最初のフェーズでのネゴシエーションエラーの原因は、パラメーター設定の不一致によるものです。 十分に注意し、Alibaba Cloud VPN Gateway の最初のフェーズの設定とローカル VPN ゲートウェイの間のパラメーター設定を行います。 最初のフェーズでのネゴシエーションエラーの可能性は以下のものがあります。

- 事前共有キーが一致しない。
- IKE プロトコルのバージョンが一致しない。
- ネゴシエーションモードが一致しない。
- "LocalId" または "RemoteId" が一致しない。
- 暗号化アルゴリズムまたは認証アルゴリズムが一致しない。
- DH グループが一致しない。 一部のデバイスでは、手動でパラメーターを設定する必要があります。
- ローカルデータセンターの VPN ゲートウェイで NATトラバーサルが有効化されていない。

一部の極端な場合、パラメーターが完全に一致していてもネゴシエーションが失敗することがあります。 このような状況では、ネゴシエーションモードをアグレッシブモードに変更することを推奨します。

2. IPsec 接続ステータスが "IKE トンネルネゴシエーションのフェーズ 2 が失敗しました" となる場合、どうしたらいいですか。

2 番目のフェーズでのネゴシエーションエラーの可能性は以下のものがあります。

- Alibaba Cloud VPN Gateway で設定されたローカルネットワーク または リモートネットワークが、ローカルデータセンターの VPN ゲートウェイで設定されたものと一致しない。 一部のローカル VPN ゲートウェイでは、ACL を使用してローカルネットワーク または リモートネットワークを設定できます。 この際、関連する操作マニュアルを参照する必要があります。
- 暗号化アルゴリズムまたは認証アルゴリズムが一致しない。
- DH グループが一致しない。 一部のデバイスでは、手動でパラメーターを設定する必要があります。

3. IPsec 接続ステータスが "IKE トンネルネゴシエーションのフェーズ 2 が成功しました" となっても、VPC の ECS インスタンスがローカルデータセンターのサーバーにアクセスできないのはなぜですか。

ローカルデータセンターがプライベート IP としてパブリック IP を使用している場合、ローカルデータセンターの ECS インスタンスがインターネットにアクセスできます。 以下を参照し、ルート設定を確認できます。

- VRouter のルート設定を確認します。
- ローカルデータセンターの firewall/iptables 設定を確認し、VPC のプライベートネットワークからのアクセスが許可されていることを確認します。

4. IPsec 接続ステータスが "IKE トンネルネゴシエーションのフェーズ 2 が成功しました" となっても、ローカルデータセンターのサーバーは VPC の ECS インスタンスにアクセスできないのはなぜですか。

1. ローカルデータセンターのルートおよび ACL 設定で、VPC へ送信されるトラフィックが VPN トンネルに入ることが許可されているかどうか確認します。
2. ECS インスタンスのセキュリティグループルールが、ローカルデータセンターのプライベートネットワークからのアクセスが許可されているかどうか確認します。

5. IPsec 接続ステータスが "IKE トンネルネゴシエーションのフェーズ 2 が成功しました" となっても、マルチネットワークシナリオで、一部のネットワークが正常に接続され、一部のネットワークが正常に接続されないのはなぜですか。

マルチネットワークシナリオでは、IKE V2 プロトコルの利用を推奨します。

IKE V2 プロトコルを使用していても問題が継続する場合は、ローカルデータセンターの VPN ゲートウェイの SA (Security Association) ステータスを確認することを推奨します。 通常、SA は 1 つのみです。 たとえば、172.30.96.0/19 === 10.0.0.0/8 172.30.128.0/17 となります。

複数の SA がある場合、ローカルデータセンターの VPN ゲートウェイは標準 IKE V2 プロトコルではありません。 この場合、複数の IPsec 接続を使用したネットワーク接続のみ可能です。 たとえば、IPsec 接続 "172.30.96.0/19 <=> 10.0.0.0/8 172.30.128.0/17" を IPsec 接続 A: "172.30.96.0/19 <=> 10.0.0.0/8" および IPsec 接続 B: "172.30.96.0/19 <=> 172.30.128.0/17" に分割できます。

 注 :

2 つに分割された IPsec 接続は最初のフェーズの SA を共有する必要があるため、2 つの IPsec 接続の最初のフェースのネゴシエーションパラメーターが一致する必要があります。