# AWS Site-to-Site VPN

## ユーザーガイド

# AWS Site-to-Site VPN: ユーザーガイド

# Table of Contents

# AWS Site-to-Site VPN とは

デフォルトでは、Amazon VPC 内に起動されるインスタンスとお客様独自の (リモート) ネットワークとの通信はできません。VPC から独自のリモートネットワークへのアクセスを可能にするには、仮想プライベートゲートウェイを VPC に関連付け、カスタムルートテーブルを作成して、セキュリティグループ規則を更新し、AWS Site-to-Site VPN (Site-to-Site VPN) 接続を作成します。

VPN 接続という用語は一般的な用語ですが、このドキュメントにおいては、VPN 接続は VPC とお客様独自のオンプレミスのネットワーク間の接続を指します。Site-to-Site VPN は、インターネットプロトコルセキュリティ (IPsec) VPN 接続をサポートしています。

Site-to-Site VPN 接続は、AWS Classic VPN または AWS VPN のいずれかです。詳細については、「AWS Site-to-Site VPN カテゴリ (p. 3)」を参照してください。

> Important
>
> 現在、Site-to-Site VPN 接続による IPv6 トラフィックはサポートされていません。

目次



# Site-to-Site VPN のコンポーネント

Site-to-Site VPN 接続は以下のコンポーネントで構成されます。Site-to-Site VPN の制限の詳細については、『Amazon VPC ユーザーガイド』の「Amazon VPC 制限」を参照してください。

## 仮想プライベートゲートウェイ

仮想プライベートゲートウェイは、Site-to-Site VPN 接続の Amazon 側にある VPN コンセントレータです。仮想プライベートゲートウェイを作成し、Site-to-Site VPN 接続を作成する VPC にアタッチします。

仮想プライベートゲートウェイを作成するとき、Amazon 側のゲートウェイのプライベート自律システム番号 (ASN) 指定できます。ASN を指定しない場合、仮想プライベートゲートウェイはデフォルトの ASN (64512) で作成されます。仮想プライベートゲートウェイの作成後に ASN を変更することはできません。仮想プライベートゲートウェイの ASN を確認するには、Amazon VPC コンソールの [仮想プライベートゲートウェイ] 画面で詳細を表示するか、または、describe-vpn-gateways AWS CLI コマンドを使用します。

> Note
>
> 2018 年 6 月 30 日以前に仮想プライベートゲートウェイを作成した場合、デフォルトの ASN はアジアパシフィック (シンガポール) リージョンで 17493、アジアパシフィック (東京) リージョン

で 10124、欧州 (アイルランド) リージョンで 9059、その他すべてのリージョンでは 7224 となります。

## AWS Transit Gateway

仮想プライベートゲートウェイからの AWS Site-to-Site VPN 接続のターゲットゲートウェイを トランジットゲートウェイ に修正できます。トランジットゲートウェイ は仮想プライベートクラウド (VPC) とオンプレミスのネットワークの相互接続に使用できる中継ハブです。詳細については、「Site-to-Site VPN 接続のターゲットゲートウェイの変更 (p. 20)」を参照してください。

# カスタマーゲートウェイ

カスタマーゲートウェイは、Site-to-Site VPN 接続のユーザー側にある物理的なデバイスまたはソフトウェアアプリケーションです。

Site-to-Site VPN 接続を作成するには、AWS にカスタマーゲートウェイリソースを作成し、AWS にカスタマーゲートウェイデバイスに関する情報を提供する必要があります。以下の表は、カスタマーゲートウェイリソースを作成するのに必要な情報を示しています。

| 項目 | 説明 |
| --- | --- |
| カスタマーゲートウェイの外部インターフェイスの、インターネットでルーティング可能な IP アドレス (静的) | パブリック IP アドレスの値は静的な値である必要があります。カスタマーゲートウェイが NAT トラバーサル (NAT-T) が有効になっているネットワークアドレス変換 (NAT) の内側にある場合は、NAT デバイスのパブリック IP アドレスを使用し、UDP ポート 4500 をブロックしないようにファイアウォールルールを調整します。 |
| ルーティングのタイプ — 静的または動的。 | 詳細については、「Site-to-Site VPN ルーティングオプション (p. 8)」を参照してください。 |
| (動的ルーティングのみ) カスタマーゲートウェイのボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) です。 | ネットワークに割り当てられている既存の ASN を使用できます。既存の ASN がない場合は、プライベート ASN (64512 から 65534 までの範囲) を使用できます。<br><br>コンソールの VPC ウィザードを使用して VPC を設定すると、ASN として自動的に 65000 が使用されます。 |

また、Site-to-Site VPN 接続で Amazon VPC を使用するには、ユーザー自身またはネットワーク管理者がリモートネットワークのカスタマーゲートウェイデバイスまたはアプリケーションを設定する必要があります。Site-to-Site VPN 接続を作成するときに、設定に必要な情報が提供され、通常はネットワーク管理者がこの設定を行います。カスタマーゲートウェイの要件および設定については、Amazon VPC ネットワーク管理者ガイドの「カスタマーゲートウェイ」を参照してください。

VPN トンネルは、Site-to-Site VPN 接続のユーザー側からトラフィックが生成されると開始されます。仮想プライベートゲートウェイはイニシエータではないため、カスタマーゲートウェイがトンネルを開始する必要があります。Site-to-Site VPN 接続でアイドル時間 (通常は 10 秒ですが設定によって異なる) が生じた場合、トンネルがダウンすることがあります。アイドル時間が生じないように、ネットワークモニタリングツール (IP SLA など) を使用してキープアライブ ping を生成できます。

Amazon VPC でテスト済みのカスタマーゲートウェイの一覧を確認するには、「Amazon Virtual Private Cloud のよくある質問」を参照してください。

# AWS Site-to-Site VPN カテゴリ

Site-to-Site VPN 接続は、AWS Classic VPN 接続または AWS VPN 接続のいずれかです。新たに作成する Site-to-Site VPN 接続はすべて AWS VPN 接続です。以下の機能は AWS VPN 接続でのみサポートされています。

- Internet Key Exchange バージョン 2 (IKEv 2)
- NAT トラバーサル
- 4 バイト ASN (2 バイト ASN に加えて)
- CloudWatch メトリクス
- カスタマーゲートウェイのための再利用可能な IP アドレス
- 追加の暗号化オプション (AES 256 ビット暗号化、SHA-2 ハッシュ、および追加の Diffie-Hellman グループ)
- 設定可能なトンネルオプション
- Amazon 側の BGP セッションのためのカスタムプライベート ASN

Site-to-Site VPN 接続のカテゴリを見つけるには、Amazon VPC コンソール、またはコマンドラインツールを使用します。

### コンソールを使用して Site-to-Site VPN カテゴリを識別するには

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。
2. ナビゲーションペインで [Site-to-Site VPN Connections (接続)] を選択します。
3. Site-to-Site VPN 接続を選択し、詳細ペインの [カテゴリ] の値を確認します。`VPN` の値が、AWS VPN 接続を指しています。`VPN-Classic` の値が、AWS Classic VPN 接続を指しています。

### コマンドラインツールを使用して Site-to-Site VPN カテゴリを識別するには

- describe-vpn-connections AWS CLI コマンドを使用できます。返される出力で示された `Category` の値を書き留めます。`VPN` の値が、AWS VPN 接続を指しています。`VPN-Classic` の値が、AWS Classic VPN 接続を指しています。

  以下の例では、Site-to-Site VPN 接続は AWS VPN 接続です。

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-1a2b3c4d
```

```
{
    "VpnConnections": [
        {
            "VpnConnectionId": "vpn-1a2b3c4d",

            ...

            "State": "available",
            "VpnGatewayId": "vgw-11aa22bb",
            "CustomerGatewayId": "cgw-ab12cd34",
            "Type": "ipsec.1",
            "Category": "VPN"
        }
    ]
}
```

または、以下のコマンドの 1 つを使用します。

- DescribeVpnConnections (Amazon EC2 Query API)
- Get-EC2VpnConnection (Tools for Windows PowerShell)

# AWS Classic VPN から AWS VPN への移行

既存の Site-to-Site VPN 接続が AWS Classic VPN 接続の場合、新しい仮想プライベートゲートウェイと Site-to-Site VPN 接続を作成し、古い仮想プライベートゲートウェイを VPC からデタッチして、新しい仮想プライベートゲートウェイを VPC にアタッチすることで、AWS VPN 接続に移行することができます。

既存の仮想プライベートゲートウェイが複数の Site-to-Site VPN 接続に関連付けられている場合は、新しい仮想プライベートゲートウェイのためにそれぞれの Site-to-Site VPN 接続を再作成する必要があります。仮想プライベートゲートウェイに複数の AWS Direct Connect プライベート仮想インターフェイスがアタッチされている場合は、新しい仮想プライベートゲートウェイのためにそれぞれの プライベート仮想インターフェイスを再作成する必要があります。詳細については、AWS Direct Connect ユーザーガイドの「仮想インターフェイスの作成」を参照してください。

既存の Site-to-Site VPN 接続が AWS VPN 接続である場合、AWS Classic VPN 接続に移行することはできません。

> Note
>
> この手順の間に、ルート伝播を無効にして古い仮想プライベートゲートウェイを VPC からデタッチするとき、現在の VPC 接続による接続は中断されます。新しい仮想プライベートゲートウェイが VPC にアタッチされ、新しい Site-to-Site VPN 接続が有効になると、接続は回復します。予期されるダウンタイムのために必ず計画を立ててください。

AWS VPN 接続へ移行するには

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。
2. ナビゲーションペインで [仮想プライベートゲートウェイ]、[仮想プライベートゲートウェイの作成] の順に選択して、仮想プライベートゲートウェイを作成します。
3. ナビゲーションペインで [Site-to-Site VPN Connections (接続)]、[VPN 接続の作成] を選択します。以下の情報を指定し、[はい、作成する] を選択します。
   - [仮想プライベートゲートウェイ]: 前のステップで作成した仮想プライベートゲートウェイを選択します。
   - [カスタマーゲートウェイ]: [既存] を選択し、現在の AWS Classic VPN 接続の既存のカスタマーゲートウェイを選択します。
   - 必要に応じてルーティングオプションを指定します。
4. 新しい Site-to-Site VPN 接続を選択してから、[設定のダウンロード] を選択します。カスタマーゲートウェイデバイスに適した設定ファイルをダウンロードします。
5. 設定ファイルを使用して、カスタマーゲートウェイデバイスの VPN トンネルを設定します。例については、Amazon VPC ネットワーク管理者ガイドを参照してください。トンネルはまだ有効にしないでください。新しく設定したトンネルを無効にしておくためのガイダンスが必要な場合は、ベンダーにお問い合わせください。
6. (オプション) テスト VPC を作成し、仮想プライベートゲートウェイをテスト VPC にアタッチします。必要に応じて、暗号化ドメイン/ソース送信先アドレスを変更して、ローカルネットワークのホストからテスト VPC 内のテストインスタンスへの接続をテストします。
7. ルートテーブルでルート伝播を使用している場合は、ナビゲーションペインで、[ルートテーブル] を選択します。VPC のルートテーブルを選択してから、[ルート伝播]、[Edit (編集)] の順に選択します。古い仮想プライベートゲートウェイのチェックボックスをオフにし、[Save (保存)] を選択します。

   > Note
   >
   > このステップ以降、新しい仮想プライベートゲートウェイがアタッチされ、新しい Site-to-Site VPN 接続が有効になるまで接続が中断します。

8. ナビゲーションペインで [仮想プライベートゲートウェイ] を選択します。古い仮想プライベートゲートウェイを選択してから、[アクション]、[VPC からデタッチ]、[はい、デタッチする] の順に選択します。新しい仮想プライベートゲートウェイを選択し、[アクション]、[VPC にアタッチ] の順に選択します。Site-to-Site VPN 接続の VPC を指定し、[はい、アタッチする] を選択します。
9. ナビゲーションペインで、[ルートテーブル] を選択します。VPC のルートテーブルを選択し、以下のいずれか 1 つを実行します。
   - ルート伝播を使用している場合は、[ルート伝播]、[Edit (編集)] の順に選択します。VPC にアタッチされた新しい仮想プライベートゲートウェイを選択してから、[Save (保存)] を選択します。
   - 静的ルートを使用している場合は、[ルート]、[Edit (編集)] の順に選択します。新しい仮想プライベートゲートウェイを指すようにルートを変更して、[Save (保存)] を選択します。
10. カスタマーゲートウェイデバイスの新しいトンネルを有効にして、古いトンネルを無効にします。トンネルを起動するには、ローカルネットワークから接続を開始する必要があります。

    該当する場合は、ルートテーブルをチェックしルートが伝播していることを確認します。VPN トンネルのステータスが `UP` の場合、ルートはルートテーブルに伝播しています。

    Note

    以前の設定に戻す必要がある場合は、新しい仮想プライベートゲートウェイをデタッチし、ステップ 8 と 9 に従って古い仮想プライベートゲートウェイに再度アタッチしてルートを更新します。
11. AWS Classic VPN を今後必要とせず、その料金が引き続き発生するのを避けるには、カスタマーゲートウェイデバイスから以前のトンネル設定を取り除き、Site-to-Site VPN 接続を削除します。これを行うには、[Site-to-Site VPN 接続] へ移動し、Site-to-Site VPN 接続を選択して、[削除] を選択します。

    Important

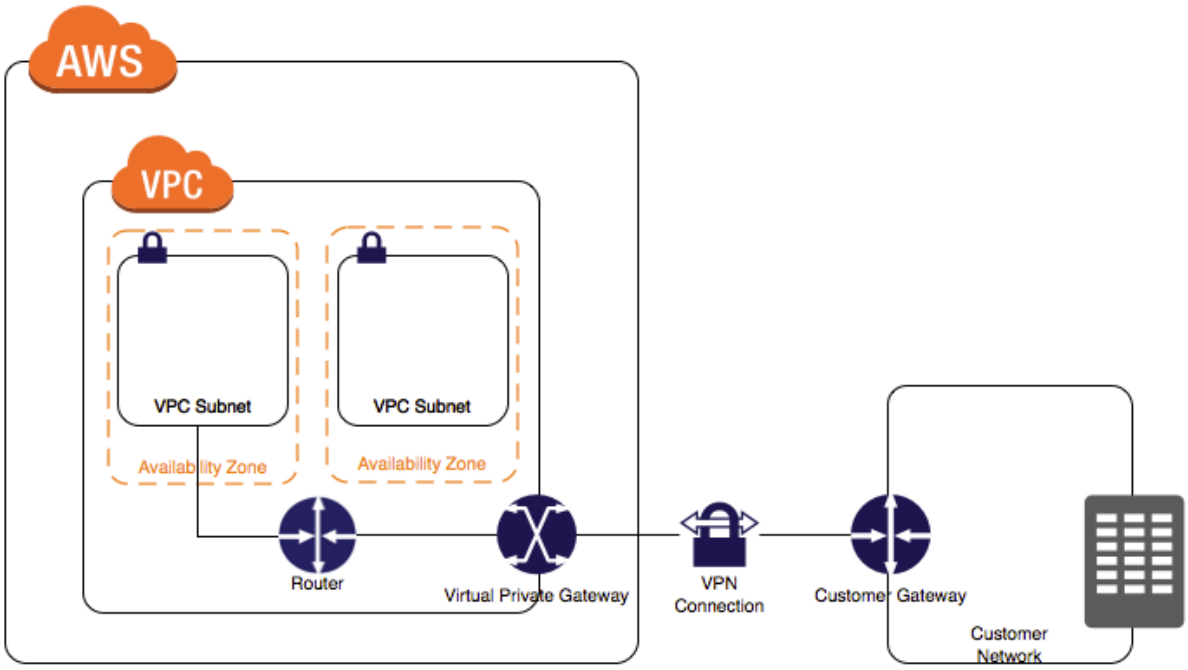
    AWS Classic VPN 接続を削除した後に、新しい AWS VPN 接続を元の AWS Classic VPN 接続に戻す、または移行することはできません。

# Site-to-Site VPN の設定例

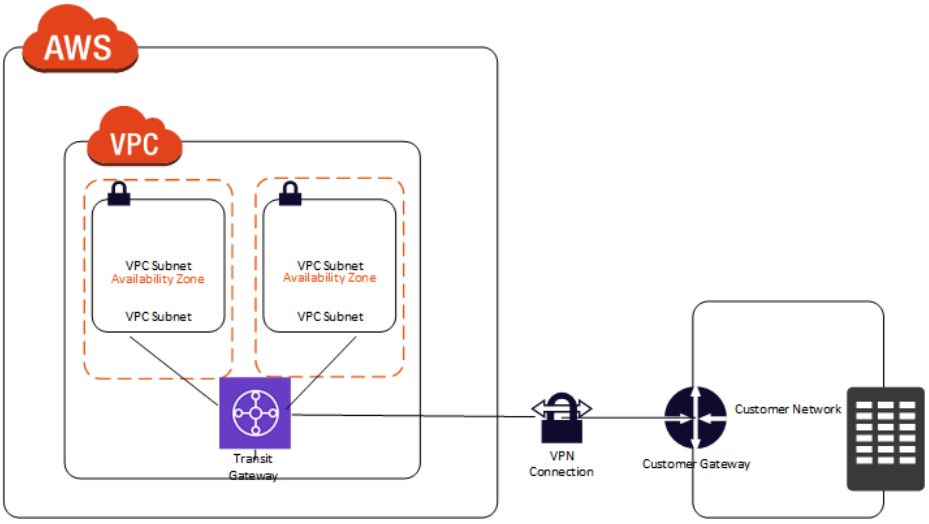
以下の図に単一および複数の Site-to-Site VPN 接続を示します。VPC には仮想プライベートゲートウェイが関連付けられていて、リモートネットワークにはカスタマーゲートウェイが使用されています。カスタマーゲートウェイは、Site-to-Site VPN 接続を有効にするように設定する必要があります。ルーティングを設定して、VPC からユーザーネットワークに向けてのトラフィックが仮想プライベートゲートウェイにルーティングされるようにします。

単一の VPC に対して複数の Site-to-Site VPN 接続を作成する場合、2 番目のカスタマーゲートウェイを設定して、外部にある同一の場所への冗長な接続を作成できます。また、複数の地理的な場所への Site-to-Site VPN 接続を作成することもできます。

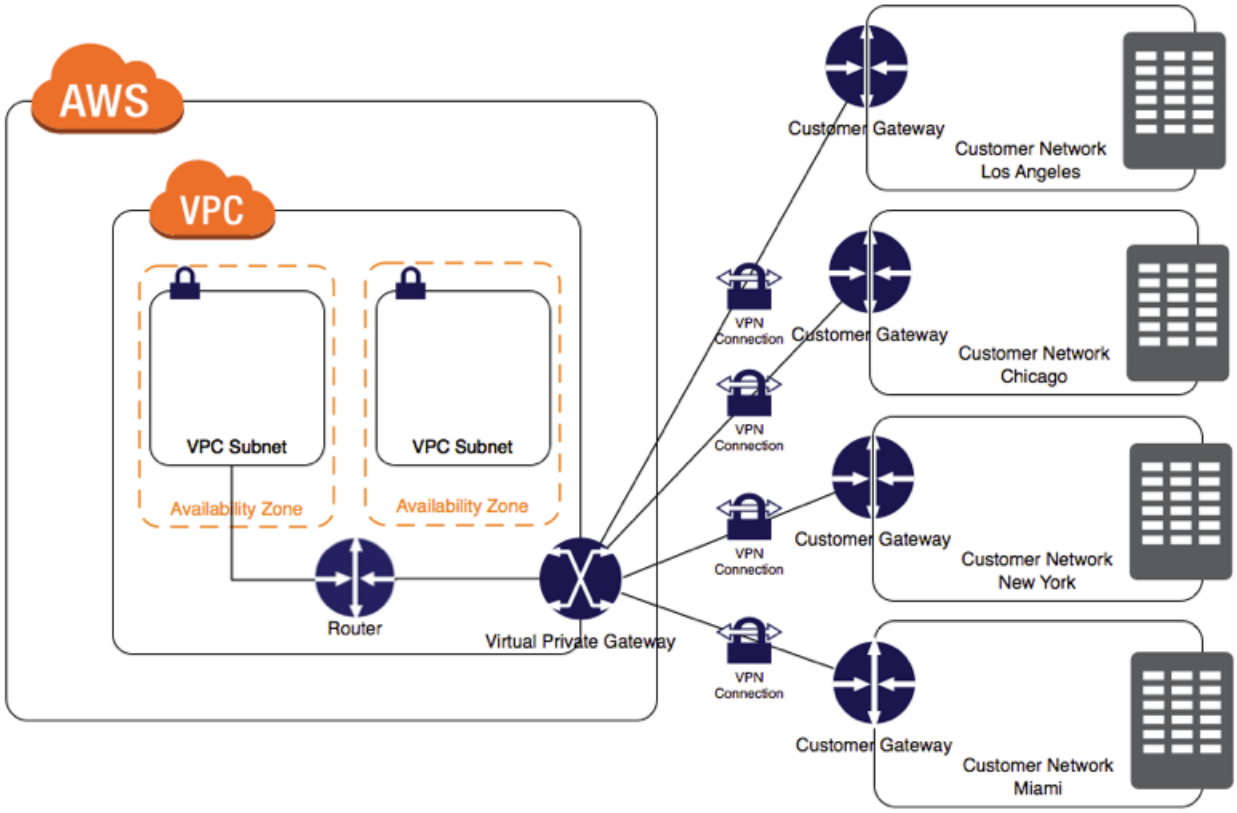
# 単一の Site-to-Site VPN 接続



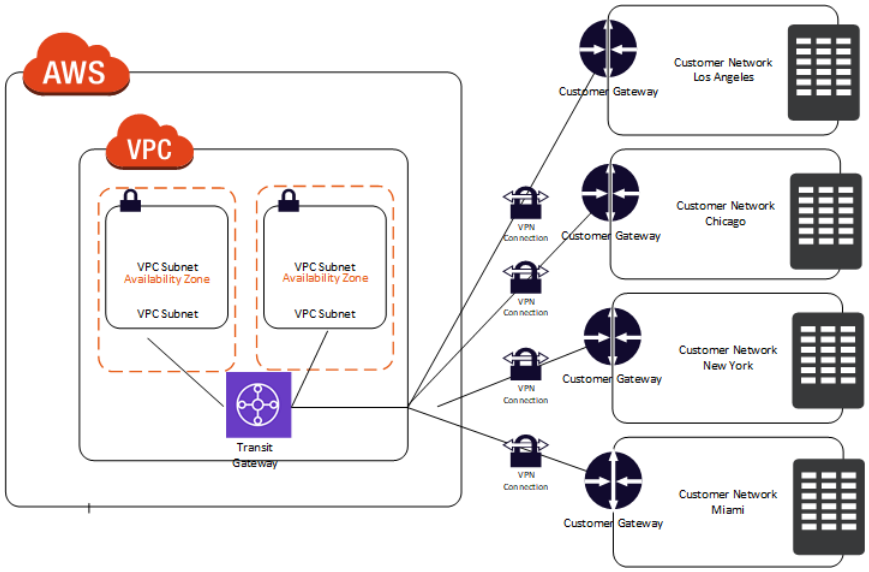

# トランジットゲートウェイを持つ単一の Site-to-Site VPN 接続



# 複数の Site-to-Site VPN 接続




# トランジットゲートウェイを持つ複数の Site-to-Site VPN 接続



# Site-to-Site VPN ルーティングオプション

Site-to-Site VPN 接続を作成する場合、以下を実行する必要があります。

- 使用予定のルーティングのタイプ (静的または動的) を指定する
- サブネットのルートテーブルを更新する

ルートテーブルに追加できるルートの数には制限があります。詳細については、『Amazon VPC ユーザーガイド』の「Amazon VPC の制限」セクションを参照してください。

## 静的および動的ルーティング

選択するルーティングのタイプは、VPN デバイスの構成とモデルによって異なります。VPN デバイスがボーダーゲートウェイプロトコル (BGP) をサポートしている場合は、Site-to-Site VPN 接続を設定するときに動的ルーティングを指定します。デバイスが BGP をサポートしていない場合は、静的ルーティングを指定します。Amazon VPC でテスト済みの静的ルーティングデバイスと動的ルーティングデバイスの一覧を確認するには、「Amazon Virtual Private Cloud のよくある質問」を参照してください。

BGP デバイスを使用する場合は、BGP を使用してデバイスから仮想プライベートゲートウェイにルートがアドバタイズされるので、Site-to-Site VPN 接続への静的ルートを指定する必要はありません。BGP 広告をサポートしているデバイスを使用する場合は、静的ルーティングを指定できません。BGP をサポートしていないデバイスを使用する場合は、静的ルーティングを選択し、仮想プライベートゲートウェイに通知するネットワークのルート (IP プレフィックス) を入力する必要があります。

使用可能な場合は BGP に対応したデバイスを使用することをお勧めします。BGP プロトコルは安定したライブ状態検出チェックが可能であり、1 番目のトンネル停止時の 2 番目の VPN トンネルへのフェイルオーバーに役立ちます。BGP をサポートしていないデバイスでも、ヘルスチェックを実行することによって、必要時に 2 番目のトンネルへのフェイルオーバーを支援できます。

## ルートテーブルと VPN ルートの優先度

ルートテーブルはネットワークトラフィックの転送先を指定します。ルートテーブルで、リモートネットワークのルートを追加し、仮想プライベートゲートウェイをターゲットとして指定する必要があります。これにより、リモートネットワーク向けの VPC からのトラフィックが、仮想プライベートゲートウェイおよび、いずれかの VPN トンネルを経由してルーティングされます。ルートテーブルのルート伝播を有効にすると、ネットワークルートは自動的にテーブルに伝播されます。

BGP アドバタイズ経由または静的ルートエントリ経由を問わず、VPC からのトラフィックを受信できるのは、仮想プライベートゲートウェイに対して既知の IP プレフィックスのみです。仮想プライベートゲートウェイでは、受信した BGP アドバタイズ、静的なルートエントリ、またはアタッチされた VPC CIDR の外部向けの他のトラフィックはルーティングされません。

仮想プライベートゲートウェイはルーティング情報を受け取ると、パスを選択してリモートネットワークにトラフィックをルーティングする方法を指定します。プレフィックス最長一致が適用されます。または、以下のルールが適用されます。

- Site-to-Site VPN 接続または AWS Direct Connect 接続から伝播されるルートが VPC のローカルルートと重複する場合は、伝播されたルートがより詳細であっても、ローカルルートが最優先されます。
- Site-to-Site VPN 接続または AWS Direct Connect 接続から伝播されるルートと他の既存静的ルート (最も長いプレフィックスの一致が適用されます) が同じ宛先 CIDR ブロックの場合は、ターゲットがインターネットゲートウェイ、仮想プライベートゲートウェイ、ネットワークインターフェイス、インスタンス ID、VPC ピアリング接続、NAT ゲートウェイまたは VPC エンドポイントの静的ルートが優先されます。

Site-to-Site VPN 接続内で重複するルートがあり、最も長いプレフィックスの一致を適用できない場合、最も好ましいものから最も好ましくないものまで、以下のように Site-to-Site VPN 接続でルートの優先順位が付けられます。

- AWS Direct Connect 接続から BGP で伝播されたルート
- Site-to-Site VPN 接続用に手動で追加された静的ルート
- Site-to-Site VPN 接続から BGP で伝播されたルート

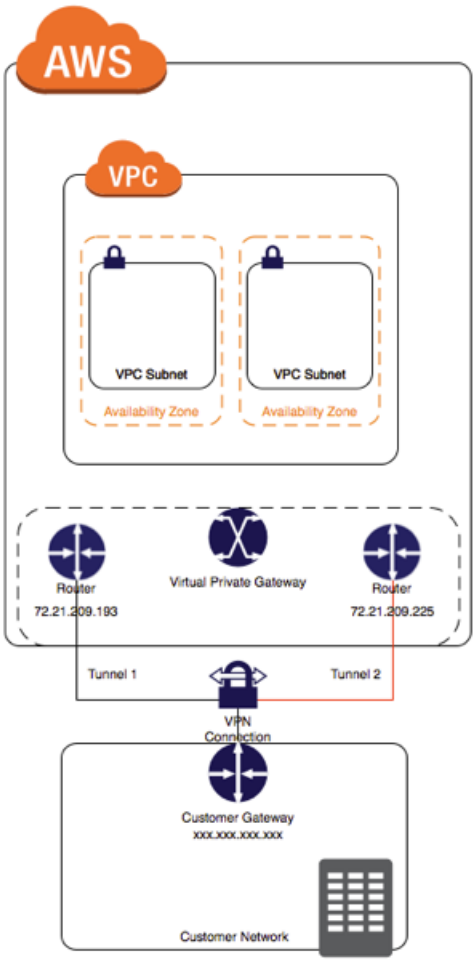
この例の場合、ルートテーブルにはインターネットゲートウェイへの (手動で追加した) 静的ルート、および仮想プライベートゲートウェイへの伝播されたルートがあります。両方のルートとも、宛先は `172.31.0.0/24` です。この場合、`172.31.0.0/24` を宛先とするすべてのトラフィックはインターネットゲートウェイにルーティングされます。これは静的ルートであるため、伝播されたルートよりも優先順位が高くなります。

| 送信先 | ターゲット |
|---|---|
| 10.0.0.0/16 | ローカル |
| 172.31.0.0/24 | vgw-1a2b3c4d (伝播済み) |
| 172.31.0.0/24 | igw-11aa22bb |

# Site-to-Site VPN 接続用に VPN トンネルを設定する

リモートネットワークを VPC に接続するには、Site-to-Site VPN 接続を使用します。各 Site-to-Site VPN 接続には 2 つのトンネルがあり、それぞれのトンネルが固有の仮想プライベートゲートウェイのパブリック IP アドレスを使用します。冗長性を確保するために両方のトンネルを設定することが重要です。1 つのトンネルが使用できなくなったとき (たとえばメンテナンスのために停止)、ネットワークトラフィックはその特定の Site-to-Site VPN 接続用に使用可能なトンネルへ自動的にルーティングされます。

以下の図は、Site-to-Site VPN 接続の 2 つのトンネルを示しています。




Site-to-Site VPN 接続を作成するとき、カスタマーゲートウェイデバイスに固有の、デバイスを設定するための情報、および各トンネルの設定のための情報を含んだ設定ファイルをダウンロードします。Site-to-Site VPN 接続を作成するとき、オプションで、いくつかのトンネルオプションを独自に指定することができます。そうしない場合、AWS によりデフォルト値が指定されます。

以下の表に、設定できるトンネルオプションを示します。

| 項目 | 説明 | AWS により指定されたデフォルト値 |
|---|---|---|
| トンネル内部の CIDR | VPN トンネルの内部 IP アドレスの範囲です。`169.254.0.0/16` の範囲から CIDR ブロックのサイズを /30 に指定できます。CIDR ブロックは、同じ仮想プライベートゲートウェイを使用するすべての Site-to-Site VPN 接続にわたって一意である必要があります。<br><br>以下の CIDR ブロックは予約済みで使用できません。<br><br>• `169.254.0.0/30` | `169.254.0.0/16` の範囲からのサイズ /30 の CIDR ブロック。 |

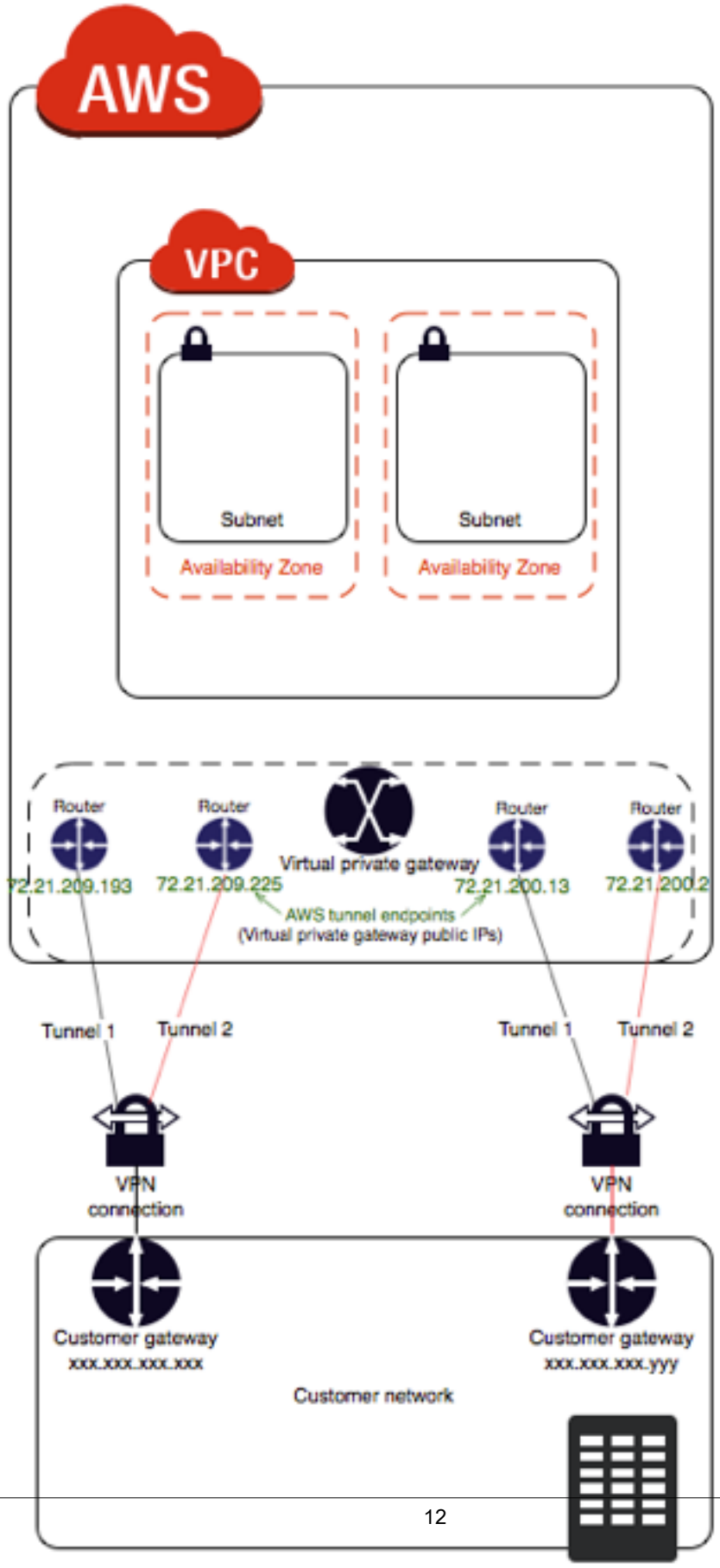
| 項目 | 説明 | AWS により指定されたデフォルト値 |
|---|---|---|
| | • 169.254.1.0/30<br>• 169.254.2.0/30<br>• 169.254.3.0/30<br>• 169.254.4.0/30<br>• 169.254.5.0/30<br>• 169.254.169.252/30 | |
| 事前共有キー (PSK) | 仮想プライベートゲートウェイとカスタマーゲートウェイ間に最初の IKE Security Association を確立するための事前共有キー (PSK)。<br><br>PSK は、8 ~ 64 文字の長さにする必要があり、ゼロ (0) から始めることはできません。使用できる文字は、英数字、ピリオド (.)、および下線 (_) です。 | 32 文字の英数字の文字列。 |

Site-to-Site VPN 接続を作成した後にトンネルオプションを変更することはできません。既存の接続の初期の内部トンネル IP アドレスまたは PSK を変更するには、Site-to-Site VPN 接続を削除し、新しく作成する必要があります。AWS Classic VPN 接続のトンネルオプションを設定することはできません。

# 冗長な Site-to-Site VPN 接続を使用してフェイルオーバーを提供する

前述のように、Site-to-Site VPN 接続では、Site-to-Site VPN 接続の 1 つが使用できなくなった場合に備えて 2 つのトンネルを設定します。カスタマーゲートウェイが使用できなくなった場合に接続が失われるのを防ぐために、2 番目のカスタマーゲートウェイを使用して、VPC および仮想プライベートゲートウェイへの 2 番目の Site-to-Site VPN 接続を設定できます。冗長な Site-to-Site VPN 接続とカスタマーゲートウェイを使用すれば、1 つのカスタマーゲートウェイでメンテナンスを実行しながら、2 番目のカスタマーゲートウェイの Site-to-Site VPN 接続を通してトラフィックの送信を継続することができます。冗長な Site-to-Site VPN 接続とカスタマーゲートウェイをリモートネットワークに確立するには、2 番目の Site-to-Site VPN 接続をセットアップする必要があります。2 番目の Site-to-Site VPN 接続用カスタマーゲートウェイの IP アドレスは、パブリックにアクセス可能である必要があります。

以下の図は、各 Site-to-Site VPN 接続の 2 つのトンネルと 2 つのカスタマーゲートウェイを示しています。


AWS
VPC
Subnet
Availability Zone
Subnet
Availability Zone
Router
Router
Virtual private gateway
Router
Router
72.21.209.193
72.21.209.225
72.21.200.13
72.21.200.2
AWS tunnel endpoints
(Virtual private gateway public IPs)
Tunnel 1
Tunnel 2
Tunnel 1
Tunnel 2
VPN
connection
VPN
connection
Customer gateway
xxx.xxx.xxx.xxx
Customer gateway
xxx.xxx.xxx.yyy
Customer network

動的にルーティングされる Site-to-Site VPN 接続では、ボーダーゲートウェイプロトコル (BGP) を使用して、カスタマーゲートウェイと仮想プライベートゲートウェイ間で情報をルーティングします。静的にルーティングされる Site-to-Site VPN 接続では、カスタマーゲートウェイのユーザー側でリモートネットワークの静的ルートを入力する必要があります。BGP でアドバタイズされ、静的に入力されたルート情報によって、双方のゲートウェイで使用可能なトンネルが判別され、障害発生時にトラフィックが再ルーティングされます。BGP (使用可能な場合) で提供されるルーティング情報を使用して使用可能なパスを選択するようネットワークを設定することをお勧めします。正確な設定はネットワークのアーキテクチャーによって異なります。

# 開始方法

AWS Site-to-Site VPN 接続を手動でセットアップするには、以下の手順を実行します。または、VPC 作成ウィザードを使用して多くのステップを自動的に実行することもできます。VPC 作成ウィザードを使用して仮想プライベートゲートウェイを設定する方法について詳細は、『Amazon VPC ユーザーガイド』の「シナリオ 3: パブリックとプライベートサブネットを持つ VPC および AWS Site-to-Site VPN アクセス」または「シナリオ 4: プライベートサブネットのみを持つ VPC および AWS Site-to-Site VPN アクセス」を参照してください。

Site-to-Site VPN 接続をセットアップするには、以下のステップを完了する必要があります。

- ステップ 1: カスタマーゲートウェイを作成する (p. 14)
- ステップ 2: 仮想プライベートゲートウェイを作成する (p. 15)
- ステップ 3: ルートテーブルでルート伝播を有効にする (p. 15)
- ステップ 4: セキュリティグループを更新する (p. 16)
- ステップ 5: Site-to-Site VPN 接続を作成して、カスタマーゲートウェイを設定する (p. 17)

この手順では、1 つ以上のサブネットのある VPC があるものと仮定しています。

# カスタマーゲートウェイを作成する

カスタマーゲートウェイは、カスタマーゲートウェイデバイスまたはソフトウェアアプリケーションに関する情報を AWS に提供します。詳細については、「カスタマーゲートウェイ (p. 2)」を参照してください。

### コンソールを使用してカスタマーゲートウェイを作成するには

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[カスタマーゲートウェイ]、[カスタマーゲートウェイの作成] の順に選択します。
3. 以下を入力し、[カスタマーゲートウェイの作成] を選択します。
   - (オプション) [Name (名前)] には、カスタマーゲートウェイの名前を入力します。これにより、`Name` というキーと指定した値を含むタグが作成されます。
   - [ルーティング] で、ルーティングタイプを選択します。
   - 動的なルーティングでは、[BGP ASN] に、ボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を入力します。
   - [IP アドレス] には、ルーティング可能な、カスタマーゲートウェイデバイスの静的 IP アドレスを入力します。カスタマーゲートウェイが NAT-T が有効な NAT デバイスの内側にある場合は、NAT デバイスのパブリック IP アドレスを使用します。

### コマンドラインまたは API を使用してカスタマーゲートウェイを作成するには

- CreateCustomerGateway (Amazon EC2 Query API)
- create-customer-gateway (AWS CLI)
- New-EC2CustomerGateway (AWS Tools for Windows PowerShell)

# 仮想プライベートゲートウェイを作成する

仮想プライベートゲートウェイを作成するとき、オプションで、Amazon 側のゲートウェイのプライベート自律システム番号 (ASN) 指定できます。ASN は、カスタマーゲートウェイのために指定した BGP ASN とは異なっている必要があります。

仮想プライベートゲートウェイを作成した後は、VPC にアタッチする必要があります。

### 仮想プライベートゲートウェイを作成して VPC にアタッチするには

1. ナビゲーションペインで、[Virtual Private Gateways]、[Create Virtual Private Gateway] を選択します。
2. (オプション) 仮想プライベートゲートウェイの名前を入力します。これにより、`Name` というキーと指定した値を含むタグが作成されます。
3. [ASN] では、デフォルトの Amazon ASN を使用するためにデフォルトの選択のままにします。それ以外の場合は、[カスタム ASN] を選択して値を入力します。16 ビット ASN では、値は 64512 から 65534 の範囲内である必要があります。32 ビット ASN では、値は 4200000000 から 4294967294 の範囲内である必要があります。
4. [仮想プライベートゲートウェイの作成] を選択します。
5. 作成した仮想プライベートゲートウェイを選択した後、[Actions (アクション)]、[VPC にアタッチ] を選択します。
6. リストから VPC を選択し、[はい、アタッチする] を選択します。

### コマンドラインまたは API を使用して仮想プライベートゲートウェイを作成するには

- CreateVpnGateway (Amazon EC2 Query API)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

### コマンドラインまたは API を使用して仮想プライベートゲートウェイを VPC にアタッチするには

- AttachVpnGateway (Amazon EC2 Query API)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

# ルートテーブルでルート伝播を有効にする

VPC で、インスタンスがカスタマーゲートウェイに到達できるようにするには、Site-to-Site VPN 接続で使用されるルートを含め、仮想プライベートゲートウェイを指すようにルートテーブルを設定する必要があります。ルート伝播を有効にして、これらのルートを自動的にテーブルに伝播することができます。

静的ルーティングでは、Site-to-Site VPN 接続の状態が `UP` であるときに、VPN 設定に指定した静的 IP プレフィックスがルートテーブルに伝播されます。同様に、動的なルーティングでは、Site-to-Site VPN 接続の状態が `UP` のときに、カスタマーゲートウェイから BGP でアドバタイズされたルートがルートテーブルに伝播されます。

> **Note**
>
> 接続が中断された場合、ルートテーブルの伝播済みルートは自動的に削除されません。伝播済みルートを削除するには、ルート伝播の無効化が必要になる場合があります (トラフィックを静的ルートにフェイルオーバーする場合など)。

### コンソールを使用してルート伝播を有効にするには

1. ナビゲーションペインで [ルートテーブル] を選択し、サブネットと関連付けられたルートテーブルを選択します。デフォルトでは、これは VPC のメインルートテーブルです。
2. 詳細ペインの [ルート伝播] タブで [Edit (編集)] を選択し、前の手順で作成した仮想プライベートゲートウェイを選択してから、[Save (保存)] を選択します。

   Note

   静的ルーティングでは、ルート伝播を有効にしない場合、Site-to-Site VPN 接続で使用される静的ルートを手動で入力する必要があります。これを行うには、ルートテーブルを選択し、[ルート]、[Edit (編集)] を選択します。[Destination (送信先)] では、Site-to-Site VPN 接続で使用される静的ルートを追加します。[ターゲット] で、仮想プライベートゲートウェイ ID を選択してから、[Save (保存)] を選択します。

### コンソールを使用してルート伝播を無効にするには

1. ナビゲーションペインで、[ルートテーブル] を選択後、サブネットに関連付けられたルートテーブルを選択します。
2. [ルート伝播]、[Edit (編集)] の順に選択します。仮想プライベートゲートウェイの [伝播] チェックボックスをオフにし、[Save (保存)] を選択します。

### コマンドラインまたは API を使用してルート伝播を有効にするには

- EnableVgwRoutePropagation (Amazon EC2 Query API)
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

### コマンドラインまたは API を使用してルート伝播を無効にするには

- DisableVgwRoutePropagation (Amazon EC2 Query API)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

# セキュリティグループを更新する

ネットワークから VPC 内のインスタンスにアクセスするのを許可するには、セキュリティグループのルールを更新して、インバウンド SSH、RDP、および ICMP アクセスを有効にする必要があります。

### セキュリティグループにルールを追加して、インバウンド SSH、RDP、ICMP アクセスを有効にするには

1. ナビゲーションペインで [Security Groups (セキュリティグループ)] を選択し、VPC のデフォルトのセキュリティグループを選択します。
2. 詳細ペインの [インバウンド] タブで、ネットワークからのインバウンド SSH、RDP、ICMP アクセスを許可するルール追加し、[Save (保存)] を選択します。インバウンドルールの追加の詳細については、『Amazon VPC ユーザーガイド』の「ルールを追加、削除、および更新する」を参照してください。

AWS CLI を使用したセキュリティグループの操作の詳細については、『Amazon VPC ユーザーガイド』の「VPC のセキュリティグループ」を参照してください。

# Site-to-Site VPN 接続を作成して、カスタマーゲートウェイを設定する

Site-to-Site VPN 接続を作成した後に、設定情報をダウンロードして、カスタマーゲートウェイデバイスまたはソフトウェアアプリケーションを設定するために使用します。

Site-to-Site VPN 接続を作成して、カスタマーゲートウェイを設定するには

1. ナビゲーションペインで [Site-to-Site VPN Connections (接続)]、[VPN 接続の作成] を選択します。
2. 以下の情報を入力し、[VPN 接続の作成] を選択します。
   - (オプション) [Name タグ] には、Site-to-Site VPN 接続の名前を入力します。これにより、`Name` というキーと指定した値を含むタグが作成されます。
   - 前の手順で作成した仮想プライベートゲートウェイを選択します。
   - 前の手順で作成したカスタマーゲートウェイを選択します。
   - VPN ルートがボーダーゲートウェイプロトコル (BGP) をサポートしているかどうかに基づいて、いずれかのルーティングオプションを選択します。
     - VPN ルーターが BGP をサポートしている場合は、[動的 (BGP が必要)] を選択します。
     - VPN ルーターが BGP をサポートしていない場合は、[静的] を選択します。[静的 IP プレフィックス] で、Site-to-Site VPN 接続のプライベートネットワークのそれぞれの IP プレフィックスを指定します。
   - [トンネルオプション] で、各トンネルに対して以下の情報をオプションで指定できます。
     - 内部トンネル IP アドレスの `169.254.0.0/16` の範囲からのサイズ /30 の CIDR ブロック。
     - IKE 事前共有キー (PSK)。IKEv1 または IKEv2 バージョンがサポートされています。

     これらのパラメータの詳細については、Site-to-Site VPN 接続用に VPN トンネルを設定する (p. 9)を参照してください。

   Site-to-Site VPN 接続の作成には数分かかる場合があります。準備が整ったら、接続を選択し、[設定のダウンロード] を選択します。
3. [設定のダウンロード] ダイアログボックスで、カスタマーゲートウェイのデバイスまたはソフトウェアに対応するベンダー、プラットフォーム、およびソフトウェアを選択し、[はい、ダウンロードする] を選択します。
4. このガイド (Amazon VPC ネットワーク管理者ガイド) と共に設定ファイルをネットワーク管理者に渡します。ネットワーク管理者がカスタマーゲートウェイを設定した後、Site-to-Site VPN 接続が機能するようになります。

コマンドラインまたは API を使用して Site-to-Site VPN 接続を作成するには

- CreateVpnConnection (Amazon EC2 Query API)
- create-vpn-connection (AWS CLI)
- New-EC2VpnConnection (AWS Tools for Windows PowerShell)

# Site-to-Site VPN 接続の静的ルートの編集

静的ルーティングでは、VPN 設定の静的ルートを追加、変更、または削除できます。

静的ルートを追加、変更、または削除するには

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。

2. ナビゲーションペインで [Site-to-Site VPN Connections (接続)] を選択します。
3. [静的ルート]、[Edit (編集)] を選択します。
4. 既存の静的 IP プレフィックスを変更するか、[Remove (削除)] を選択して削除します。[別のルールの追加] を選択して、新しい IP プレフィックスを設定に追加します。完了したら、[保存] を選択します。

   Note

   ルートテーブルでルート伝播を有効にしていない場合、ルートテーブルで手動でルートを更新し、更新された静的 IP プレフィックスを Site-to-Site VPN 接続に反映する必要があります。詳細については、「ルートテーブルでルート伝播を有効にする (p. 15)」を参照してください。

コマンドラインまたは API を使用して静的ルートを追加するには

- CreateVpnConnectionRoute (Amazon EC2 Query API)
- create-vpn-connection-route (AWS CLI)
- New-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

コマンドラインまたは API を使用して静的ルートを削除するには

- DeleteVpnConnectionRoute (Amazon EC2 Query API)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

# 漏洩した認証情報の置き換え

Site-to-Site VPN 接続のトンネル認証情報が漏洩したと思われる場合は、IKE 事前共有キーを変更できます。そのためには、Site-to-Site VPN 接続を削除し、同じ仮想プライベートゲートウェイを使用して新しい接続を作成して、カスタマーゲートウェイに新しいキーを設定します。Site-to-Site VPN 接続を作成するときに、独自の事前共有キーを指定できます。また、トンネルの内部のアドレスと外部のアドレスが一致することを確認することも必要です。Site-to-Site VPN 接続を再作成するとアドレスが変更されることがあるためです。この手順を実行する間、VPC 内のインスタンスとの通信は停止しますが、インスタンスは中断されずに実行を継続します。ネットワーク管理者が新しい設定情報を実装した後、Site-to-Site VPN 接続に新しい認証情報が使用されるようになり、VPC 内のインスタンスへのネットワーク接続が再開されます。

Important

この手順にはネットワーク管理者グループの助けが必要です。

IKE 事前共有キーを変更するには

1. Site-to-Site VPN 接続を削除します。詳細については、「Site-to-Site VPN 接続の削除 (p. 23)」を参照してください。VPC または仮想プライベートゲートウェイを削除する必要はありません。
2. 新しい Site-to-Site VPN 接続を作成してトンネルのための独自の事前共有キーを指定する、または、AWS で新しい事前共有キーを生成します。詳細については、「Site-to-Site VPN 接続を作成して、カスタマーゲートウェイを設定する (p. 17)」を参照してください。
3. 新しい設定ファイルをダウンロードします。

# Site-to-Site VPN 接続のテスト

AWS Site-to-Site VPN 接続を作成してカスタマーゲートウェイを設定した後、インスタンスを起動し、インスタンスへの ping を実行して接続をテストできます。ping リクエストに応答する AMI を使用し、インスタンスのセキュリティグループが、インバウンド ICMP を有効にするように設定されていることを確認する必要があります。Amazon Linux AMI のいずれかを使用することをお勧めします。ご使用のインスタンスで Windows Server を実行している場合、インスタンスへの ping を実行するには、インスタンスにログインし、Windows ファイアウォールでインバウンド ICMPv4 を有効にする必要があります。

> **Important**
>
> インバウンドおよびアウトバウンドの ICMP トラフィックを許可するために、インスタンスへのトラフィックをフィルタするセキュリティグループまたはネットワーク ACL を VPC 内に設定する必要があります。

### エンドツーエンド接続をテストするには

1. https://console.aws.amazon.com/ec2/) にある Amazon EC2 コンソールを開きます。
2. ダッシュボードで、[インスタンスの作成] を選択します。
3. [Amazon マシンイメージ (AMI)] ページで、AMI を選択し、[Select (選択)] を選択します。
4. インスタンスタイプを選択し、[次の手順: インスタンスの詳細の設定] を選択します。
5. [インスタンスの詳細の設定] ページの [Network (ネットワーク)] で VPC を選択します。[Subnet (サブネット)] で、サブネットを選択します。[セキュリティグループの設定] ページが表示されるまで、[Next (次へ)] を選択します。
6. [既存のセキュリティグループを選択する] オプションを選択し、前に変更したデフォルトのグループを選択します。[確認と作成] を選択します。
7. 選択した設定を確認します。必要な変更を行い、[作成] を選択し、キーペアを選択してインスタンスを起動します。
8. インスタンスが実行中になった後、そのプライベート IP アドレス ( 例えば `10.0.0.4` ) を取得します。Amazon EC2 コンソールにインスタンスの詳細の一部としてアドレスが表示されます。
9. ネットワークでカスタマーゲートウェイの背後にあるコンピュータから、インスタンスのプライベート IP アドレスを指定した `ping` コマンドを実行します。正常な応答は以下のようになります。

```
ping 10.0.0.4
```

```
Pinging 10.0.0.4 with 32 bytes of data:

Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128
Reply from 10.0.0.4: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.4:
Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

これで SSH または RDP を使用して、VPC のインスタンスに接続できるようになりました。Linux インスタンスに接続する方法については、「Linux インスタンス用 Amazon EC2 ユーザーガイド」の Connect to Your Linux Instance を参照してください。Windows インスタンスに接続する方法については、『Windows インスタンスの Amazon EC2 ユーザーガイド』の Connect to Your Windows Instance を参照してください。

# Site-to-Site VPN 接続のターゲットゲートウェイの変更

AWS Site-to-Site VPN 接続のターゲットゲートウェイを変更できます。以下の移行オプションを使用できます。

- トランジットゲートウェイ への既存の仮想プライベートゲートウェイ
- 別の仮想プライベートゲートウェイへの既存の仮想プライベートゲートウェイ
- 別の トランジットゲートウェイ への既存の トランジットゲートウェイ
- 仮想プライベートゲートウェイへの既存の トランジットゲートウェイ

以下のタスクは、新しいゲートウェイへの移行を完了するのに役立ちます。

タスク

- ステップ 1: トランジットゲートウェイを作成する (p. 20)
- ステップ 2: 静的ルート (静的 VPN 接続のトランジットゲートウェイへの移行に必要) を削除する (p. 20)
- ステップ 3: 新しいゲートウェイに移行する (p. 21)
- ステップ 4: VPC ルートテーブルを更新する (p. 21)
- ステップ 5: トランジットゲートウェイルーティングの更新 (新しいゲートウェイがトランジットゲートウェイである場合に必須) (p. 22)

## ステップ 1: トランジットゲートウェイを作成する

新しいゲートウェイへの移行を実行する前に、新しいゲートウェイを設定する必要があります。仮想プライベートゲートウェイを追加する方法については、「the section called “仮想プライベートゲートウェイを作成する” (p. 15)」を参照してください。トランジットゲートウェイ を追加する方法については、『Amazon VPC トランジットゲートウェイ』の「トランジットゲートウェイを作成する」を参照してください。

新しいターゲットが トランジットゲートウェイ である場合、トランジットゲートウェイ に VPC をアタッチします。VPC アタッチメントの詳細については、『Amazon VPC トランジットゲートウェイ』の「VPC へのトランジットゲートウェイのアタッチメント」を参照してください。

## ステップ 2: 静的ルート (静的 VPN 接続のトランジットゲートウェイへの移行に必要) を削除する

このステップは、静的ルートを持つ仮想プライベートゲートウェイから トランジットゲートウェイ に移行する際に必要になります。

新しいゲートウェイに移行する前に静的ルートを削除する必要があります。

> **Tip**
>
> 静的ルートを削除する前に、必ずコピーを取ってください。VPN 接続の移行が完了した後、これらのルートを トランジットゲートウェイ に再度追加する必要が出てきます。

ルートをルートテーブルから削除するには

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。
2. ナビゲーションペインで [ルートテーブル] を選択して、ルートテーブルを選択します。
3. [ルート] タブで [Edit (編集)] を選択し、仮想プライベートゲートウェイへの静的ルートで [Remove (削除)] を選択します。
4. 完了したら、[保存] を選択します。

# ステップ 3: 新しいゲートウェイに移行する

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。
2. ナビゲーションペインで [Site-to-Site VPN Connections (接続)] を選択します。
3. Site-to-Site VPN 接続を選択して、[アクション]、[Modify VPN Connection (VPN 接続の変更)] の順に選択します。
4. [Change Target (ターゲットの変更)] で、次の操作を実行します。

   a. [ターゲットの種類] でゲートウェイの種類を選択します。

   b. 接続ターゲットの設定:

      [Target VPN Gateway ID (ターゲット VPN ゲートウェイ ID)] の [仮想プライベートゲートウェイ] で、仮想プライベートゲートウェイ ID を選択します。

      [Target トランジットゲートウェイ ID] の [Transit Gateway (トランジットゲートウェイ)] で、トランジットゲートウェイ ID を選択します。
5. [保存] を選択します。

コマンドラインまたは API を使用して Site-to-Site VPN 接続を変更するには

- ModifyVpnConnection (Amazon EC2 Query API)
- modify-vpn-connection (AWS CLI)

# ステップ 4: VPC ルートテーブルを更新する

新しいゲートウェイに移行した後、VPC のルートテーブルを変更する必要がある場合があります。次の表に、実行する必要があるアクションについての情報を示します。VPC ルートテーブルの更新に関する詳細については、『Amazon VPC ユーザーガイド』の「ルートテーブル」を参照してください。

VPN ゲートウェイターゲットの修正に必要な VPC ルートテーブルの更新

| 既存のゲートウェイ | 新しいゲートウェイ | VPC のルートテーブルの変更 |
|---|---|---|
| 伝播されたルートを持つ仮想プライベートゲートウェイ | トランジットゲートウェイ | トランジットゲートウェイ ID を指すルートを追加します。 |
| 伝播されたルートを持つ仮想プライベートゲートウェイ | 伝播されたルートを持つ仮想プライベートゲートウェイ | 必要なアクションはありません。 |
| 伝播されたルートを持つ仮想ゲートウェイ | 静的ルートを持つ仮想プライベートゲートウェイ | 新しい仮想プライベートゲートウェイ ID が格納されているエントリを追加します。 |

| 既存のゲートウェイ | 新しいゲートウェイ | VPC のルートテーブルの変更 |
|---|---|---|
| 静的ルートを持つ仮想ゲートウェイ | トランジットゲートウェイ | VPC ルートテーブルを更新して、仮想プライベートゲートウェイ ID を格納するエントリをトランジットゲートウェイ ID に変更します。 |
| 静的ルートを持つ仮想ゲートウェイ | 静的ルートを持つ仮想プライベートゲートウェイ | 仮想プライベートゲートウェイ ID を指すエントリを新しい仮想プライベートゲートウェイ ID に更新します。 |
| 静的ルートを持つ仮想ゲートウェイ | 伝播されたルートを持つ仮想プライベートゲートウェイ | 仮想プライベートゲートウェイ ID を含むエントリを削除します。 |
| トランジットゲートウェイ | 静的ルートを持つ仮想プライベートゲートウェイ | トランジットゲートウェイ を格納するエントリを仮想プライベートゲートウェイ ID に更新します。 |
| トランジットゲートウェイ | 伝播されたルートを持つ仮想プライベートゲートウェイ | トランジットゲートウェイ ID を含むエントリを削除します。 |
| トランジットゲートウェイ | トランジットゲートウェイ | トランジットゲートウェイ ID を格納するエントリを、新しいトランジットゲートウェイ ID に更新します。 |

# ステップ 5: トランジットゲートウェイルーティングの更新 (新しいゲートウェイがトランジットゲートウェイである場合に必須)

新しいゲートウェイが トランジットゲートウェイ である場合、トランジットゲートウェイのルートテーブルを変更して VPC と Site-to-Site VPN 間のトラフィックを許可します。トランジットゲートウェイ ルーティングの詳細については、『Amazon VPC トランジットゲートウェイ』の「トランジットゲートウェイルートテーブル」を参照してください。

Important

VPN 静的ルートを削除した場合、トランジットゲートウェイ ルートテーブルに静的ルートを追加する必要があります。

# Site-to-Site VPN 接続の削除

AWS Site-to-Site VPN 接続が不要になった場合には、それを削除することができます。

> **Important**
>
> Site-to-Site VPN 接続を削除し、新しい VPN 接続を作成する場合は、新しい設定情報をダウンロードし、ネットワーク管理者にカスタマーゲートウェイを再設定してもらう必要があります。

### コンソールを使用して Site-to-Site VPN 接続を削除するには

1. https://console.aws.amazon.com/vpc/にある Amazon VPC コンソールを開きます。
2. ナビゲーションペインで [Site-to-Site VPN Connections (接続)] を選択します。
3. Site-to-Site VPN 接続を選択し、[Actions (アクション)]、[Delete (削除)] の順に選択します。
4. [Delete (削除)] を選択します。

カスタマーゲートウェイが不要になった場合には、それを削除することができます。Site-to-Site VPN 接続で使用中のカスタマーゲートウェイを削除することはできません。

### コンソールを使用してカスタマーゲートウェイを削除するには

1. ナビゲーションペインで、[カスタマーゲートウェイ] を選択します。
2. 削除するカスタマーゲートウェイを選択し、[Actions (アクション)]、[カスタマーゲートウェイの削除] を選択します。
3. [Yes, Delete] を選択します。

VPC 用の仮想プライベートゲートウェイが不要になった場合には、それをアタッチ解除することができます。

### コンソールを使用して仮想プライベートゲートウェイをデタッチするには

1. ナビゲーションペインで [仮想プライベートゲートウェイ] を選択します。
2. 仮想プライベートゲートウェイを選択してから、[Actions (アクション)]、[VPC からデタッチ] の順に選択します。
3. [はい、デタッチする] を選択します。

デタッチした仮想プライベートゲートウェイが不要になった場合は、削除することができます。VPC にアタッチされている仮想プライベートゲートウェイを削除することはできません。

### コンソールを使用して仮想プライベートゲートウェイを削除するには

1. ナビゲーションペインで [仮想プライベートゲートウェイ] を選択します。
2. 削除する仮想プライベートゲートウェイを選択してから、[Actions (アクション)]、[仮想プライベートゲートウェイの削除] の順に選択します。
3. [Yes, Delete] を選択します。

### コマンドラインまたは API を使用して Site-to-Site VPN 接続を削除するには

- DeleteVpnConnection (Amazon EC2 Query API)
- delete-vpn-connection (AWS CLI)

- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

### コマンドラインまたは API を使用してカスタマーゲートウェイを削除するには

- DeleteCustomerGateway (Amazon EC2 Query API)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

### コマンドラインまたは API を使用して仮想プライベートゲートウェイをデタッチするには

- DetachVpnGateway (Amazon EC2 Query API)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (AWS Tools for Windows PowerShell)

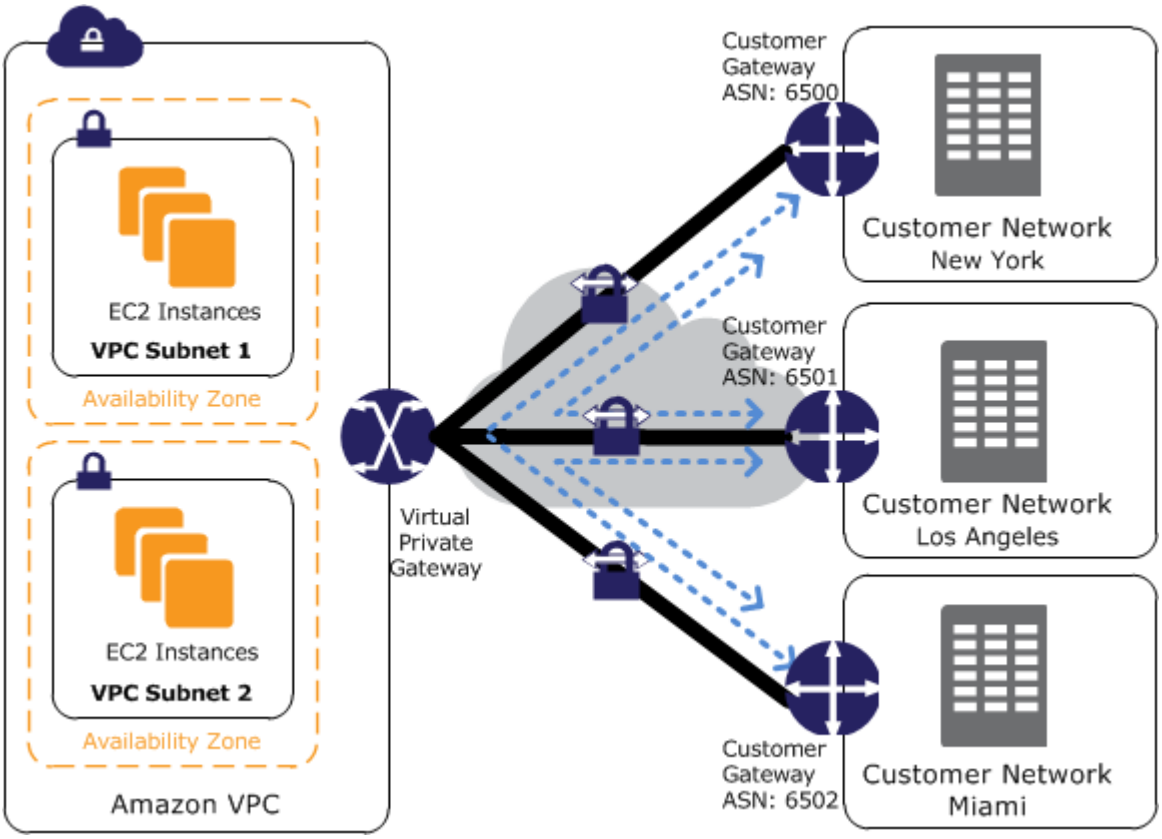
### コマンドラインまたは API を使用して仮想プライベートゲートウェイを削除するには

- DeleteVpnGateway (Amazon EC2 Query API)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

# VPN CloudHub を使用して安全なサイト間通信を提供する

複数の AWS Site-to-Site VPN 接続がある場合は、AWS VPN CloudHub を使用して、安全なサイト間通信を提供することができます。これで、リモートサイトを有効にして、VPC のみとではなく、相互に通信します。VPN CloudHub は、VPC の有無にかかわらず使用できるシンプルなハブアンドスポークモデルで動作します。この設計は、複数のブランチオフィスと既存のインターネット接続を持つ顧客が、リモートオフィス間でプライマリ接続またはバックアップ接続を実現するために、便利でコストを抑えられる可能性のあるハブアンドスポークモデルを実装したいと考えている場合に適しています。

以下の図は VPN CloudHub アーキテクチャーです。青色の点線は、Site-to-Site VPN 接続を介してルーティングされているリモートサイト間のネットワークトラフィックを示しています。




AWS VPN CloudHub を使用するには、複数のカスタマーゲートウェイを使って仮想プライベート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の一意のボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を使用する必要があります。カスタマーゲートウェイは、適切なルート (BGP プレフィックス) をその Site-to-Site VPN 接続にアドバタイズします。これらのルーティングアドバタイズが受信され、各 BGP ピアに再アドバタイズされることで、サイト間でのデータの送受信が可能になります。サイト間で IP 範囲が重複することは許可されません。各サイトが、標準の Site-to-Site VPN 接続を使用しているように、VPC とデータを送受信することもできます。

仮想プライベートゲートウェイへの AWS Direct Connect 接続を使用するサイトを、AWS VPN CloudHub に含めることもできます。たとえば、ニューヨーク本社で VPC への AWS Direct Connect 接続を確立しな

がら、ブランチオフィスで VPC への Site-to-Site VPN 接続を使用できます。ロサンゼルスとマイアミのブランチオフィスは、AWS VPN CloudHub を使用して、相互にデータを送受信したり、本社とデータを送受信したりできます。

AWS VPN CloudHub を設定するには、AWS マネジメントコンソール を使用して、複数のカスタマーゲートウェイを作成します。このそれぞれに、ゲートウェイのパブリック IP アドレスと ASN があります。次に、各カスタマーゲートウェイから一般的な仮想プライベートゲートウェイへの Site-to-Site VPN 接続を作成します。各 Site-to-Site VPN 接続が、その特定の BGP ルートをアドバタイズする必要があります。これを行うには、Site-to-Site VPN 接続の VPN 設定ファイルでネットワークステートメントを使用します。ネットワークステートメントは、使用するルーターの種類によって少し違いがあります。

AWS VPN CloudHub を使用する場合は、通常の Amazon VPC Site-to-Site VPN 接続料金を支払います。各 VPN が仮想プライベートゲートウェイに接続されている間は、1 時間ごとに接続料金が発生します。AWS VPN CloudHub を使用してサイト間でデータを送信する場合、サイトから仮想プライベートゲートウェイへのデータ送信にはコストがかかりません。仮想プライベートゲートウェイからエンドポイントに中継されるデータに対しては、標準の AWS データ転送料金のみがかかります。たとえば、ロサンゼルスとニューヨークそれぞれにサイトがあり、両方のサイトに、仮想プライベートゲートウェイへの Site-to-Site VPN 接続が存在する場合は、Site-to-Site VPN 接続ごとに 0.05 USD/時間 (合計 0.10 USD/時間) の支払いが発生します。また、ロサンゼルスからニューヨーク (およびその逆) に Site-to-Site VPN 接続経由でデータを送信すると、そのデータすべてに対して標準の AWS データ転送料金が発生します。Site-to-Site VPN 接続経由で仮想プライベートゲートウェイに送信されるネットワークトラフィックは無料ですが、Site-to-Site VPN 接続経由で仮想プライベートゲートウェイからエンドポイントに送信されるネットワークトラフィックには、標準の AWS データ転送料金がかかります。詳細については、「Site-to-Site VPN 接続料金表」を参照してください。

# Site-to-Site VPN 接続のモニタリング

モニタリングは、AWS Site-to-Site VPN 接続の信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。ただし、Site-to-Site VPN 接続のモニタリングを開始する前に、以下の質問に対する回答を反映したモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- モニタリングの対象となるリソースとは?
- どのくらいの頻度でこれらのリソースをモニタリングしますか?
- 使用するモニタリングツールは?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

次のステップでは、さまざまなタイミングと負荷条件でパフォーマンスを測定することにより、お客様の環境で通常の VPN パフォーマンスのベースラインを確定します。VPN のモニタリングでは、過去のモニタリングデータを保存し、現在のパフォーマンスデータと比較することで、パフォーマンスの通常パターンと異常パターンを特定し、問題に対処する方法を考案できます。

ベースラインを確立するには、次の項目をモニタリングする必要があります。

- VPN トンネルの状態
- トンネルへのデータ
- トンネルからのデータ

目次



# モニタリングツール

AWS では、Site-to-Site VPN 接続のモニタリングに使用できるさまざまなツールを提供しています。これらのツールの中には、自動モニタリングを設定できるものもあれば、手操作を必要とするものもあります。モニタリングタスクをできるだけ自動化することをお勧めします。

## 自動モニタリングツール

次に示す自動化されたモニタリングツールを使用すると、Site-to-Site VPN 接続の監視が行われ、問題が検出されたときにレポートが返されます。

- [Amazon CloudWatch アラーム] – 指定した期間にわたって単一のメトリクスを監視し、複数の期間にわたり既定のしきい値に関連するメトリクス値に基づいて 1 つ以上のアクションを実行します。アクションは、Amazon SNS トピックに送信される通知です。CloudWatch アラームは、単に特定の状態にあるというだけではアクションを呼び出しません。状態が変わり、それが指定した数の期間にわたって持続する必要があります。詳細については、「Amazon CloudWatch を使用した VPN トンネルのモニタリング (p. 28)」を参照してください。
- [AWS CloudTrail ログモニタリング] – アカウント間でログファイルを共有する、CloudWatch Logs にログタイムを送信してリアルタイムで CloudTrail ログファイルをモニタリングする、Java でログ処理アプ

リケーションを書き込む、そして CloudTrail による配信後にログファイルに変更がないことを検証します。詳細については、Amazon EC2 API Referenceの「AWS CloudTrail を使用した API コールのログ記録」および AWS CloudTrail User Guideの「CloudTrail ログファイルの操作」を参照してください。

## 手動モニタリングツール

Site-to-Site VPN 接続のモニタリングでもう 1 つ重要な点は、CloudWatch アラームの対象外の項目を手動でモニタリングすることです。Amazon VPC および CloudWatch のコンソールダッシュボードには、AWS 環境の状態が一目でわかるビューが表示されます。

- Amazon VPC ダッシュボードには、次の内容が表示されます。
  - リージョン別のサービス状態
  - Site-to-Site VPN 接続
  - VPN トンネルの状態 (ナビゲーションペインで、[Site-to-Site VPN Connections]、Site-to-Site VPN 接続、[Tunnel Details] の順に選択します)
- CloudWatch ホームページに表示されます。
  - 現在のアラームとステータス
  - アラームとリソースのグラフ
  - サービス状態ステータス

  さらに、CloudWatch を使用して次のことが行えます。
  - 重視するサービスをモニタリングするためのカスタマイズしたダッシュボードを作成する
  - メトリクスデータをグラフ化して、問題のトラブルシューティングを行い、傾向を確認する
  - AWS リソースのすべてのメトリクスを検索して、参照する
  - 問題があることを通知するアラームを作成/編集する

# Amazon CloudWatch を使用した VPN トンネルのモニタリング

CloudWatch を使用して VPN トンネルをモニタリングすることで、VPN サービスから未加工データを収集し、リアルタイムに近い読み取り可能なメトリクスに加工することができます。これらの統計は 15 か月間記録されるため、履歴情報にアクセスしてウェブアプリケーションやサービスの動作をより的確に把握できます。VPN メトリクスデータは、利用可能になると自動的に CloudWatch に送信されます。

> Important
>
> CloudWatch メトリクスは、AWS Classic VPN 接続ではサポートされません。詳細については、「AWS Site-to-Site VPN カテゴリ (p. 3)」を参照してください。

詳細については、『Amazon CloudWatch ユーザーガイド』を参照してください。

## VPN トンネルのメトリクスとディメンション

VPN トンネルでは、次のメトリクスを使用できます。

| メトリクス | 説明 |
| --- | --- |
| `TunnelState` | トンネルの状態。静的 VPN の場合、0 は DOWN を示し、1 は UP を示します。BGP VPN の場合、1 は |

| メトリクス | 説明 |
| --- | --- |
| | ESTABLISHED を示し、0 は他のすべての状態に使用されます。<br><br>単位: ブール |
| `TunnelDataIn` | VPN トンネル経由で受信されたバイト。各メトリクスのデータポイントは、前のデータポイント以降に受信されたバイトの数を表します。該当期間中に受信されたバイトの総数を表示するには Sum 統計を使用します。<br><br>このメトリクスは、復号の後のデータをカウントします。<br><br>単位: バイト |
| `TunnelDataOut` | VPN トンネル経由で送信されたバイト。各メトリクスのデータポイントは、前のデータポイント以降に送信されたバイトの数を表します。該当期間中に送信されたバイトの総数を表示するには Sum 統計を使用します。<br><br>このメトリクスは、暗号化の前のデータをカウントします。<br><br>単位: バイト |

メトリクスデータをフィルタリングするために以下のディメンションを使用します。

| ディメンション | 説明 |
| --- | --- |
| `VpnId` | Site-to-Site VPN 接続 ID でメトリクスデータをフィルタリングします。 |
| `TunnelIpAddress` | 仮想プライベートゲートウェイのトンネルの IP アドレスでメトリクスデータをフィルタリングします。 |

# VPN トンネル CloudWatch メトリクスの表示

新しい Site-to-Site VPN 接続を作成するときに、VPN サービスは VPN トンネルに関する次のメトリクスが利用可能になると、それを CloudWatch に送信します。以下のように、VPN トンネルのメトリクスを表示できます。

### CloudWatch コンソールを使用してメトリクスを表示するには

メトリクスはまずサービスの名前空間ごとにグループ化され、次に各名前空間内のさまざまなディメンションの組み合わせごとにグループ化されます。

1. https://console.aws.amazon.com/cloudwatch/にある CloudWatch コンソールを開きます。
2. ナビゲーションペインで メトリクスを選択します。
3. [All metrics] で、[VPN] メトリクス名前空間を選択します。
4. メトリクス (Site-to-Site VPN 接続用など) を表示するメトリクスディメンションを選択します。

### AWS CLI を使用してメトリクスを表示するには

コマンドプロンプトで、次のコマンドを使用します。

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

# CloudWatch アラームを作成して VPN トンネルをモニタリングする

CloudWatch アラームを作成できます。これは、アラームの状態が変わったときに Amazon SNS メッセージを送信します。アラームは指定された期間にわたって単一のメトリクスをモニタリングし、複数の期間にわたり既定のしきい値に関連するメトリクス値に基づいて Amazon SNS トピックに通知を送信します。

たとえば、VPN トンネルの状態をモニタリングして、トンネルのダウン状態が 5 分間、連続して 3 回発生した場合に通知を送信するアラームを作成できます。

### トンネル状態のアラームを作成するには

1. https://console.aws.amazon.com/cloudwatch/にある CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[Alarms]、[Create Alarm] の順に選択します。
3. [VPN Tunnel Metrics] を選択します。
4. VPN トンネルの IP アドレスと [TunnelState] メトリクスを選択します。[Next (次へ)] を選択します。
5. 次のようにアラームを設定し、終了したら [Create Alarm] を選択します。
   - [Alarm Threshold] で、アラームの名前と説明を入力します。[次の時] で [<=] を選択し、「0」と入力します。連続した期間として「3」を入力します。
   - [Actions] で、既存の通知のリストを選択するか、[New list] を選択して新しいリストを作成します。
   - [Alarm Preview] で、連続した期間として 5 分を選択し、統計情報として [Maximum] を指定します。

Site-to-Site VPN 接続の状態を監視するアラームを作成できます。たとえば、以下のアラームは、両方のトンネルのダウン状態が 5 分間連続して 1 回発生した場合に通知を送信します。

### Site-to-Site VPN 接続状態のアラームを作成するには

1. https://console.aws.amazon.com/cloudwatch/にある CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[Alarms]、[Create Alarm] の順に選択します。
3. [VPN Connection Metrics] を選択します。
4. Site-to-Site VPN 接続と [TunnelState] メトリクスを選択します。[Next (次へ)] を選択します。
5. 次のようにアラームを設定し、終了したら [Create Alarm] を選択します。
   - [Alarm Threshold] で、アラームの名前と説明を入力します。[次の時] で [<=] を選択し、「0」と入力します。連続した期間として「1」を入力します。
   - [Actions] で、既存の通知のリストを選択するか、[New list] を選択して新しいリストを作成します。
   - [Alarm Preview] で、連続した期間として 5 分を選択し、統計情報として [Maximum] を指定します。

     または、両方のトンネルがアップとなるように Site-to-Site VPN 接続を設定している場合は、[Minimum] の統計を指定し、少なくとも 1 つのトンネルがダウンとなったときに通知を送信することができます。

VPN トンネルに出入りするトラフィックの量をモニタリングするアラームを作成することもできます。たとえば、次のアラームはネットワークから VPN トンネルに入るトラフィックの量をモニタリングし、15 分の期間中にバイト数がしきい値の 5,000,000 に達したときに通知を送信します。

着信ネットワークトラフィック用のアラームを作成するには

1. https://console.aws.amazon.com/cloudwatch/にある CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[Alarms]、[Create Alarm] の順に選択します。
3. [VPN Tunnel Metrics] を選択します。
4. VPN トンネルの IP アドレスと [TunnelDataIn] メトリクスを選択します。[Next (次へ)] を選択します。
5. 次のようにアラームを設定し、終了したら [Create Alarm] を選択します。
   - [Alarm Threshold] で、アラームの名前と説明を入力します。[Whenever] で、[>=] を選択し、「5000000」と入力します。連続した期間として「1」を入力します。
   - [Actions] で、既存の通知のリストを選択するか、[New list] を選択して新しいリストを作成します。
   - [Alarm Preview] で、連続した期間として 15 分を選択し、統計情報として [Sum] を指定します。

次のアラームは、VPN トンネルからネットワークに出るトラフィックの量をモニタリングし、15 分の期間中にバイト数が 1,000,000 より少なくなると通知を送信します。

発信ネットワークトラフィック用のアラームを作成するには

1. https://console.aws.amazon.com/cloudwatch/にある CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[Alarms]、[Create Alarm] の順に選択します。
3. [VPN Tunnel Metrics] を選択します。
4. VPN トンネルの IP アドレスと [TunnelDataOut] メトリクスを選択します。[Next (次へ)] を選択します。
5. 次のようにアラームを設定し、終了したら [Create Alarm] を選択します。
   - [Alarm Threshold] で、アラームの名前と説明を入力します。[次の時] で [<=] を選択し、「1000000」と入力します。連続した期間として「1」を入力します。
   - [Actions] で、既存の通知のリストを選択するか、[New list] を選択して新しいリストを作成します。
   - [Alarm Preview] で、連続した期間として 15 分を選択し、統計情報として [Sum] を指定します。

アラーム作成のその他の例については、Amazon CloudWatch ユーザーガイド の「Amazon CloudWatch アラームの作成」を参照してください。

# ドキュメント履歴

次の表は、AWS Site-to-Site VPN ユーザーガイドの更新について説明しています。

| 変更 | 説明 | 日付 |
| --- | --- | --- |
| AWS Site-to-Site VPN 接続のターゲットゲートウェイを変更できます | AWS Site-to-Site VPN 接続のターゲットゲートウェイを変更できます。詳細については、「Site-to-Site VPN 接続のターゲットゲートウェイの変更 (p. 20)」を参照してください。 | 2018 年 12 月 18 日 |
| 初回リリース | このリリースでは、AWS Site-to-Site VPN (旧 AWS マネージド VPN) のコンテンツを Amazon VPC ユーザーガイド から切り離しました。 | 2018 年 12 月 18 日 |