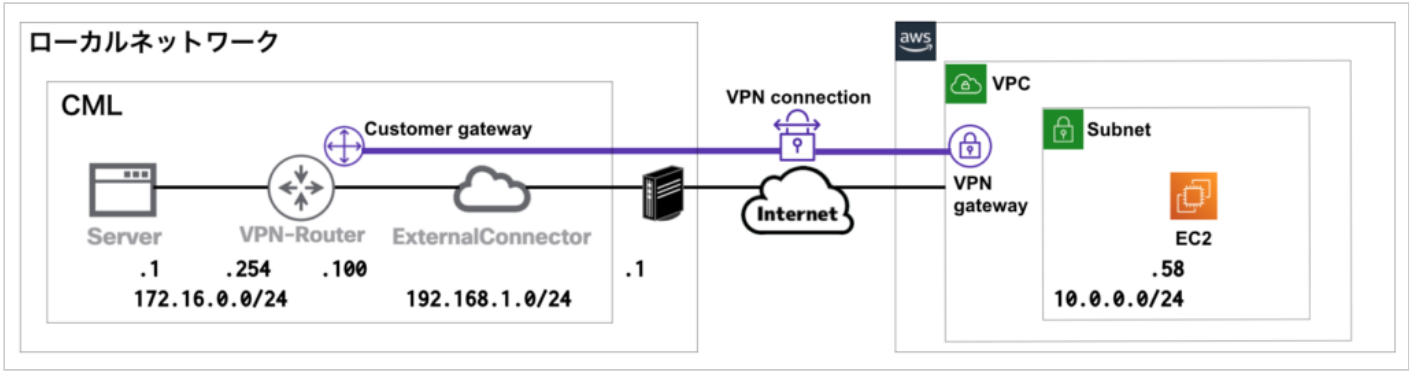
AWSサイト間VPNの構築（3.AWSのVPN構築）

2021.09.20　2021.08.12

【前回】AWSサイト間VPNの構築（2.AWSのEC2構築）
【次回】AWSサイト間VPNの構築（4.CMLの構築）

ネットワーク構成

下記のネットワーク構成で、CML上のLAN(172.16.0.0/24)とAWSのサブネット(10.0.0.0/24)が直接通信できるようにします。
※Server(172.16.0.1)からEC2(10.0.0.58)にPingによる疎通確認ができるようにしていきます。



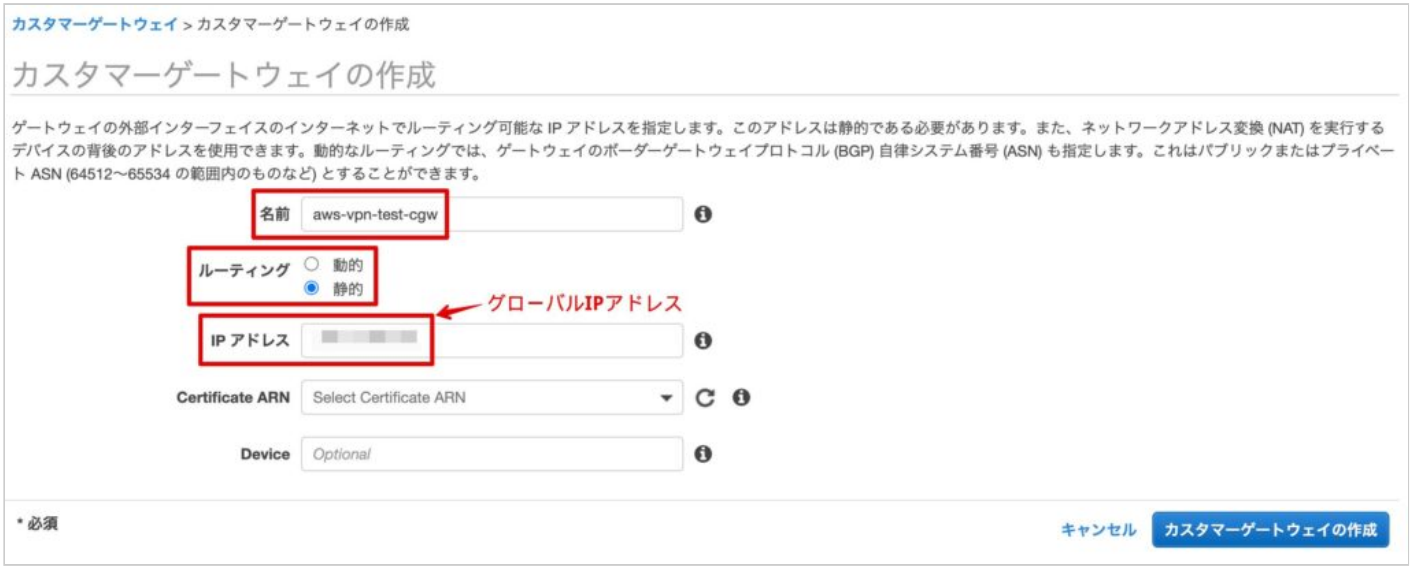
AWSのVPN構築

AWSのVPNを構築します。

カスタマーゲートウェイの作成

ローカルネットワーク側のVPNの起点となるカスタマーゲートウェイを作成します。まず、自身が利用しているグローバルIPアドレスを確認します。ここではCMANのIPアドレス確認ページで確認しています。

「aws-vpn-test-cgw」という名前で、ルーティングは「静的」を選択し、IPアドレスは確認した「グローバルIPアドレス」を設定します。



「使用可能」となれば、作成完了です。

仮想プライゲートゲートウェイの作成

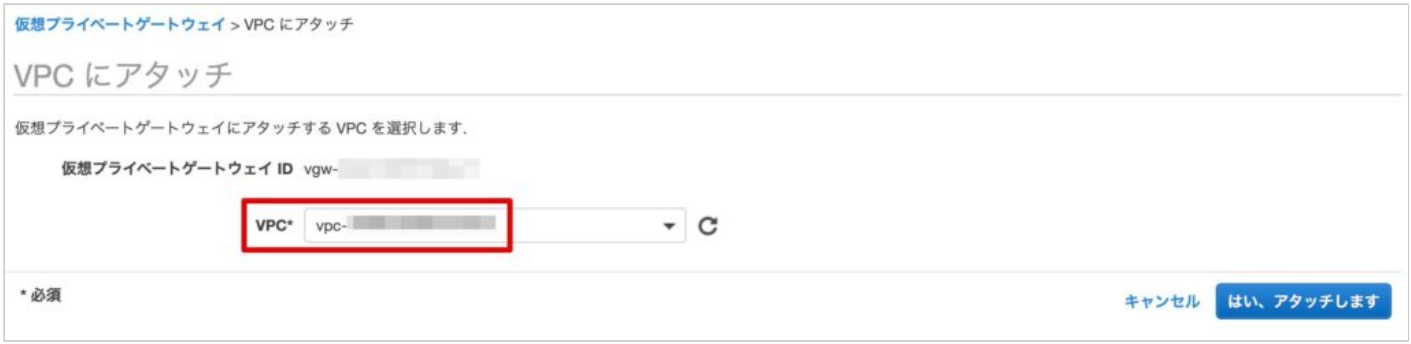
AWS側のVPNの起点となる仮想プライベートゲートウェイを作成します。

「aws-vpn-test-vgw」という名前で作成しています。

作成後は状態が「detached」となっているため、VPCにアタッチします。

「アクション」→「VPCにアタッチ」を選択します。

作成したVPCを選択しアタッチします。



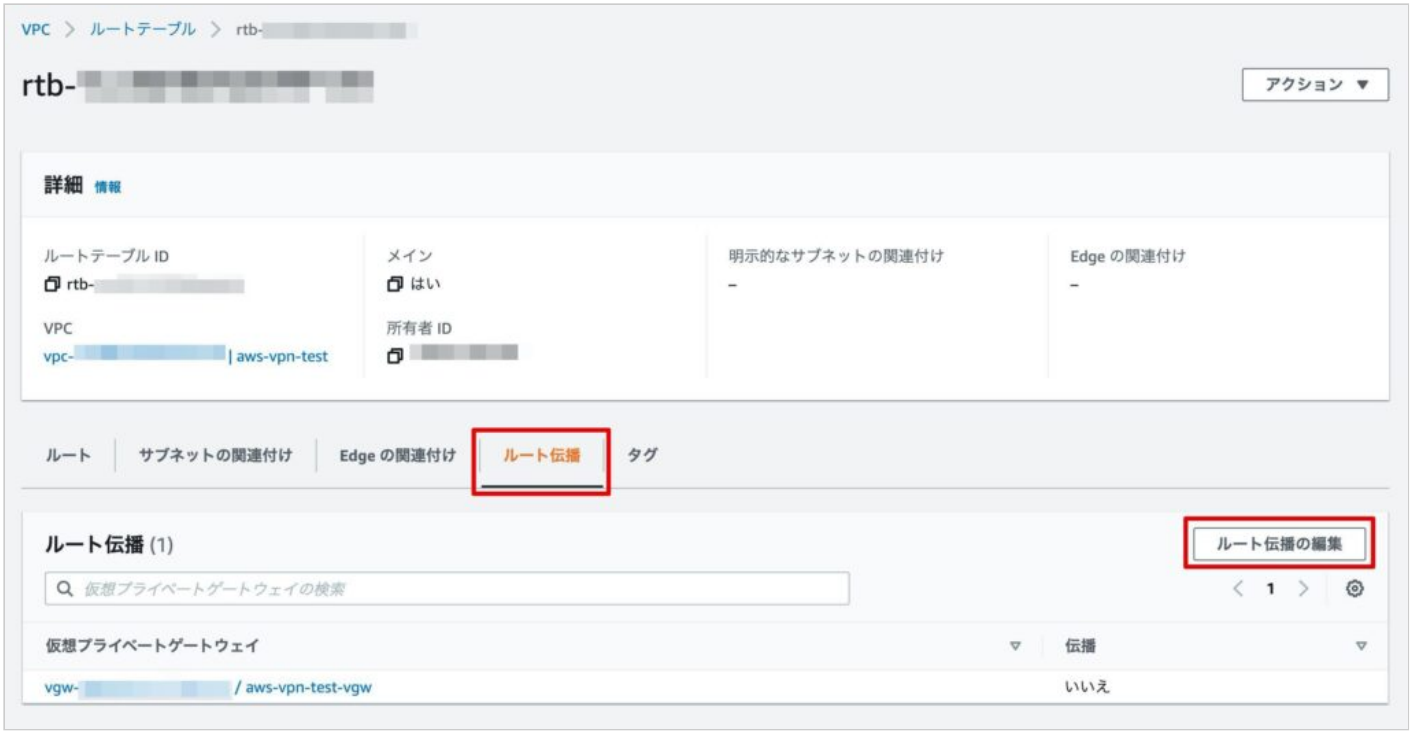
「attaching」の状態を経由し、

「attached」となれば、作成完了です。

ルートテーブルの設定

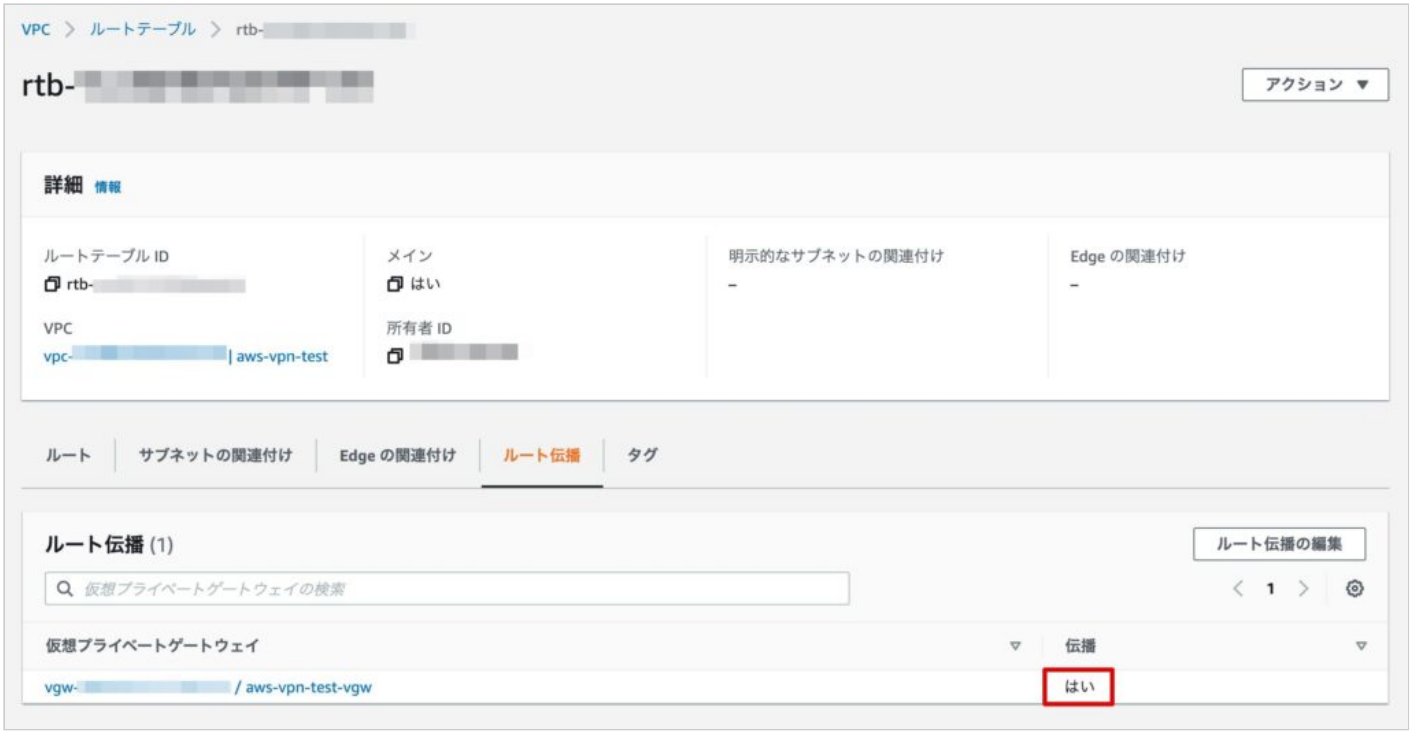
仮想プライベートゲートウェイからVPC内にルートを伝播するための設定を行います。

ルートテーブルの「ルート伝播」タブを選択し、「ルート伝播の編集」をクリックします。



作成した仮想プライベートゲートウェイの伝播の「有効化」にチェックを入れます。

伝播が「はい」となれば、設定完了です。



サイト間のVPN接続の作成

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の間でVPNを構築するため、サイト間のVPN接続を下記の通りで作成します。

※VPN接続を作成すると利用料金が発生します※ 利用料金の説明 →こちら

名前タグ：aws-vpn-test ※任意の名前
ターゲットゲートウェイタイプ：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：作成した仮想プライベートゲートウェイを選択
カスタマーゲートウェイ：既存
カスタマーゲートウェイID：作成したカスタマーゲートウェイを選択
ルーティングオプション：静的
静的IPプレフィックス：ローカルネットワーク(192.168.1.0/24)、CMLのLAN(172.16.0.0/24)を追加

トンネルオプションは設定変更不要です。

作成したVPN接続を確認します。

「詳細」タブで、「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」と「カスタマーゲートウェイアドレス(ローカル側のグローバルIPアドレス)」が正しく設定されていることを確認します。

「トンネル詳細」タブで、トンネルの設定を確認します。
AWSのVPN接続では、冗長化のためにデフォルトで2つのトンネルが作成されます。
外部IPアドレスは「グローバルIPアドレス」、トンネルインターフェースのIPアドレスは「リンクローカルアドレス」が利用されます。

「静的ルート」タブで、ローカルネットワーク(192.168.1.0/24)、CMLのLAN(172.16.0.0/24)が「使用可能」となっていることを確認します。

これで、AWSサイト間VPN接続のためのAWSのVPN構築は完了です！