# AWS VPN

AWS サイト間 VPN、高速サイト間 VPN、Client VPN 接続のいずれかを使用して、安全に、プライベートでクラウドリソースにアクセスします。

# AWS サイト間 VPN の機能

# 高速サイト間 VPN

高速サイト間 VPN では、お客様がオンプレミスロケーションと AWS クラウド間を接続する際の VPN トラフィックを、最も近い AWS エッジロケーションにルーティングします。高速 VPN は、AWS の国際光ファイバーネットワークの信頼性と性能を活用しながら、インターフェース上で共有されているデータ間の距離を縮小することで、高速サイト間 VPN のパフォーマンスを向上させます。高速サイト間 VPN は、オンプレミスおよび AWS の両方において、ビジネス上重要なロケーション同士を、国際ネットワークを使用して接続するのに最適です。AWS サイト間 VPN および AWS Global Accelerator の両方をご利用した場合、高速 VPN に追加料金が発生します。

## 安全性の高い接続

AWS Client VPN は、TLS で暗号化された制御チャネルを使用してデータチャネルパラメータの取り決めを行う OpenVPN を使用しています。データチャネルは SSL ベースですが、さらなる安全対策が追加されています (HMAC、ハッシュ、x.509 証明書 など)。

## 高可用性

AWS サイト間 VPN 使うことで、AWS Direct Connect を使用したフェイルオーバーと CloudHub ソリューションを作成できるようになります。CloudHub では、リモートサイト間において、必ずしも VPC を使用しなくても通信が可能です。この機能は、VPC の有無を問わず使用できる、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、リモートオフィス間におけるプライマリあるいはバックアップの接続に、便利でコスト削減も可能なハブアンドスポークモデルを実装したいとお考えで、複数の支店と既存のインターネット接続があるお客様に適しています。

## カスタマイズ

AWS サイト間 VPN では、内部トンネル IP アドレス、事前共有キー、ボーダーゲートウェイプロトコル自律システム番号 (BGP ASN) を含む、カスタマイズ可能なトンネルオプションを利用できます。これらにより、複数のセキュアな VPN トンネルをセットアップできるので、アプリケーション、もしくはダウンタイムからの復旧力を、より大きな帯域幅で強化できます。さらに、AWS Transit Gateway での AWS サイト間 VPN では、複数のパスにおいてトラフィック帯域幅を向上するのに役立つ、コスト均等なマルチパス (ECMP) ルーティングも利用可能です。

# インスタンスでネットワークアドレス変換 (NAT) トラバーサル

AWS サイト間 VPN は NAT トラバーサルアプリケーションをサポートしているので、インターネットに接続されている単一のパブリック IP アドレスを使用するルーターに隠れたプライベートネットワーク上でプライベート IP アドレスを使用することができます。

# モニタリング

AWS サイト間 VPN は CloudWatch にメトリクスを送信し、可視性とモニタリングを向上します。CloudWatch ではさらに、カスタムメトリクスとデータポイントを任意の順番で、選択したレートで送信することができます。これらのデータポイントの統計を、時系列データのオーダーされたセットとして取得できます。

# AWS Client VPN の特徴

AWS Client VPN は、インターネット接続および OpenVPN に互換性のあるクライアントを使用すればどこからでもアクセスできる、完全マネージド型の VPN ソリューションを提供します。これは伸縮自在であり、需要に合わせた自動的なスケーリングをご提供します。ユーザー側からは、AWS およびオンプレミスネットワークに接続できるようになります。AWS Client VPN は Amazon VPC と AWS Directory Service を含む既存の AWS インフラストラクチャサービスにシームレスに統合するので、ネットワークトポロジーを変更する必要はありません。

# 認証

AWS Client VPN は Active Directory あるいは証明書を使用して認証します。Client VPN は、既存のオンプレミス Active Directory と接続する AWS Directory Services と統合します。したがって、既存の Active Directory からクラウドにデータをレプリケートする必要はありません。Client VPN を使用した証明書ベースの認証は AWS Certificate Manager と統合され、簡単に証明書のプロビジョニング、管理、デプロイができるようになります。

# 認証

AWS Client VPN ではネットワークベースの認証が提供されるので、Active Directory グループに基づき特定のネットワークへのアクセスを制限するアクセスコントロールルールを定義できます。

# 安全性の高い接続

AWS Client VPN は、トラフィックの暗号化のため安全性の高い TLS VPN トンネルプロトコルを使用します。単一の VPN トンネルはそれぞれの Client VPN エンドポイントで終了し、ユーザーにすべての AWS およびオンプレミスリソースへのアクセスを提供します。

# 接続管理

Amazon CloudWatch Logs を使用して、AWS Client VPN 接続ログのログファイルの管理、保存、接続ができます。関連するログデータは CloudWatch Logs から取得することができます。モニタリングが容易になり、フォレンジック分析が行えるので、ネットワークへのアクセス権がある相手を管理しながら特定の接続を終了することが可能です。

# 従業員のデバイスとの互換性

AWS Client VPN はデバイスをネットワークに接続するよう設計されています。OpenVPN ベースからクライアントを選べるため、従業員は Windows、Mac、iOS、Android、Linux ベースの環境を含む複数の選択肢から使用したいデバイスを選ぶことが可能です。