aws

ユーザーガイド

AWS Site-to-Site VPN

AWS Site-to-Site VPN: ユーザーガイド

Table of Contents

AWS Site-to-Site VPN の概要

デフォルトでは、Amazon VPC 内に起動されるインスタンスとユーザー独自の (リモート) ネットワークとの通信はできません。VPC からリモートネットワークへのアクセスを有効にするには、AWS Site-to-Site VPN (Site-to-Site VPN) 接続を作成し、接続を経由してトラフィックを渡すようにルーティングを設定します。

VPN 接続という用語は一般的な用語ですが、このドキュメントでの VPN 接続は VPC とユーザーのオンプレミスネットワークの間の接続を指します。Site-to-Site VPN ではインターネットプロトコルセキュリティ (IPsec) VPN 接続がサポートされています。

目次

概念

Site-to-Site VPN の主な概念は次のとおりです。

- VPN 接続: オンプレミス機器と VPC 間の安全な接続。
- VPN トンネル: お客様のネットワークと AWS の間でデータを送受信できる暗号化されたリンク。

  各 VPN 接続には、高可用性のために同時に使用できる 2 つの VPN トンネルが含まれています。
- カスタマーゲートウェイ: カスタマーゲートウェイデバイスに関する情報を AWS に提供する AWS リソース。
- カスタマーゲートウェイデバイス: 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。
- ターゲットゲートウェイ: Site-to-Site VPN 接続の Amazon 側にある VPN エンドポイントの総称。
- 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、単一の VPC にアタッチできる Amazon 側の Site-to-Site VPN 接続の VPN エンドポイントです。
- 転送ゲートウェイ: 複数の VPC とオンプレミスネットワークを相互接続するために使用でき、Site-to-Site VPN 接続の Amazon 側の VPN エンドポイントとして使用できる転送ハブ。

Site-to-Site VPN 機能

以下の機能は AWS Site-to-Site 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
- 仮想プライベートゲートウェイ (VGW) 構成の場合、1～2147483647 の範囲の 4 バイトの ASN。詳細については、「Site-to-Site VPN 接続のカスタマーゲートウェイオプション」を参照してください。
- 1～65535 の範囲のカスタマーゲートウェイ (CGW) 用の 2 バイトの ASN。詳細については、「Site-to-Site VPN 接続のカスタマーゲートウェイオプション」を参照してください。
- 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
- による下位 CA からのプライベート証明書AWS Private Certificate Authority
- トランジットゲートウェイでの VPN 接続の IPv6 トラフィックのサポート

Site-to-Site VPN の制限

Site-to-Site VPN 接続には次の制限があります。

- IPv6 トラフィックは、仮想プライベートゲートウェイの VPN 接続ではサポートされません。
- AWS VPN 接続は、パス MTU 検出をサポートしていません。

さらに、Site-to-Site VPN を使用する場合は次の点を考慮してください。

- VPC を共通のオンプレミスネットワークに接続する場合は、ネットワークに重複しない CIDR ブロックを使用することをお勧めします。

Site-to-Site VPN の使用

次のインターフェイスのいずれかを使用して、Site-to-Site VPN リソースの作成、アクセス、管理を行うことができます。

- AWS Management Console — Site-to-Site VPN リソースへのアクセスに使用できるウェブインターフェイスを提供します。
- AWS Command Line Interface (AWS CLI) — Amazon VPC を含むさまざまな AWS サービス用のコマンドを備えており、Windows、macOS、Linux でサポートされています。詳細については、「AWS Command Line Interface」を参照してください。
- AWS SDK — 言語固有の API を提供し、署名の計算、リクエストの再試行処理、エラー処理など、接続のさまざまな詳細を処理します。詳細については、AWS SDK をご参照ください。
- クエリ API— HTTPS リクエストを使用して呼び出す低レベル API アクションを提供します。クエリ API の使用は、Amazon VPC の最も直接的なアクセス方法ですが、リクエストに署名するハッシュの生成やエラー処理など、低レベルの詳細な作業をアプリケーションで処理する必要があります。詳細については、Amazon EC2 API リファレンスを参照してください。

料金

VPN 接続がプロビジョニングされ、利用可能な VPN 接続時間ごとに課金されます。詳細については、「AWS Site-to-Site VPN および高速化された Site-to-Site VPN 接続の料金」を参照してください。

Amazon EC2 からインターネットへのデータ転送に対して課金されます。詳細については、「Amazon EC2 オンデマンド料金」ページの「データ転送」を参照してください。

高速 VPN 接続を作成すると、2 つのアクセラレーターが作成および管理されます。アクセラレーターごとに、時間単位の料金とデータ転送料金が課金されます。詳細については、AWS Global Accelerator 料金表を参照してください。

AWS Site-to-Site VPN の仕組み

Site-to-Site VPN 接続は次のコンポーネントで構成されます。

- 仮想プライベートゲートウェイまたはトランジットゲートウェイ
- カスタマーゲートウェイデバイス
- カスタマーゲートウェイ

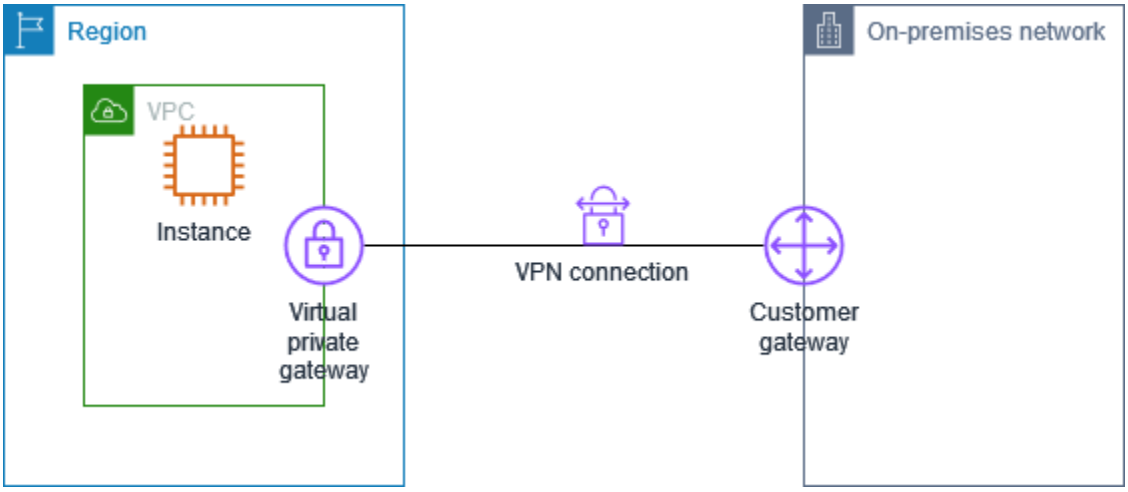
VPN 接続は、仮想プライベートゲートウェイまたは AWS 側のトランジットゲートウェイと、オンプレミス側のカスタマーゲートウェイの間に 2 つの VPN トンネルを提供します。

Site-to-Site VPN クォータの詳細については、「Site-to-Site VPN のクォータ」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、サイト間 VPN 接続にアクセスする必要があるリソースを含む仮想プライベートクラウド (VPC) にアタッチします。

次の図は、仮想プライベートゲートウェイを使用した VPC とオンプレミスネットワーク間の VPN 接続を示しています。



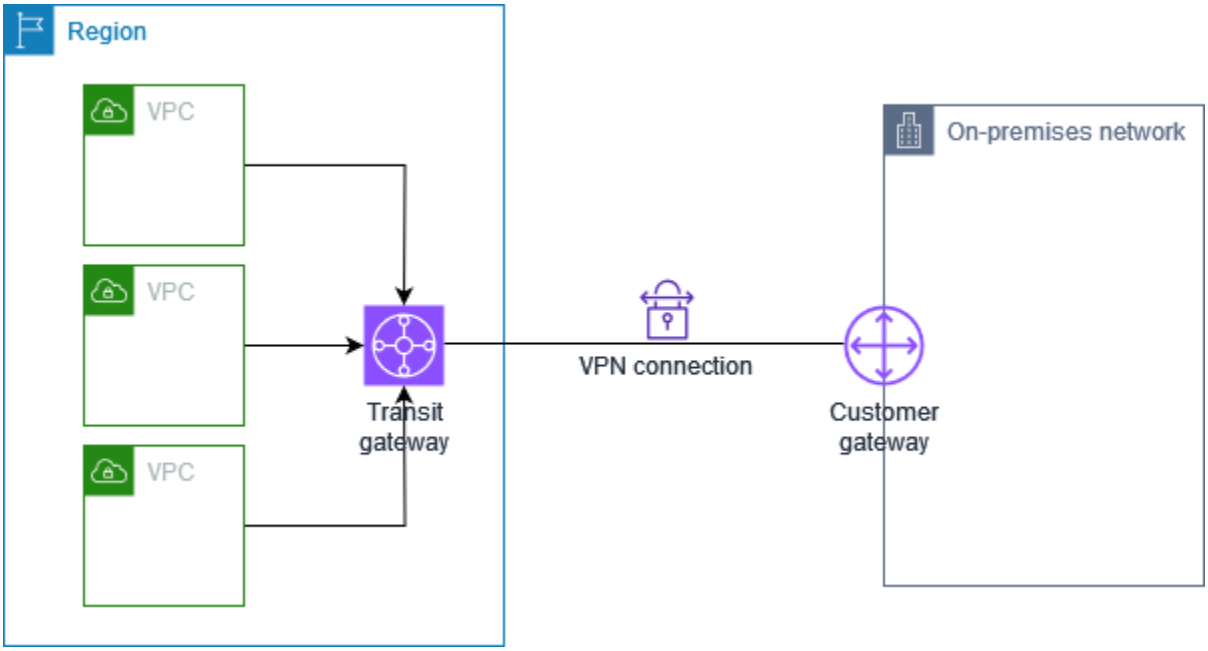
仮想プライベートゲートウェイを作成するとき、Amazon 側のゲートウェイのプライベート自律システム番号 (ASN) 指定できます。ASN を指定しない場合、仮想プライベートゲートウェイはデフォル

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] ページで詳細を表示するか、describe-vpn-gateways AWS CLI コマンドを使用します。

トランジットゲートウェイ

トランジットゲートウェイは、VPC とオンプレミスネットワークを相互接続するために使用できる中継ハブです。詳細については、Amazon VPC トランジットゲートウェイを参照してください。Site-to-Site VPN 接続は、トランジットゲートウェイのアタッチメントとして作成できます。

次の図は、トランジットゲートウェイを使用した複数の VPC とオンプレミスネットワーク間の VPN 接続を示しています。トランジットゲートウェイには、3 つの VPC アタッチメントと 1 つの VPN アタッチメントがあります。



トランジットゲートウェイの Site-to-Site VPN 接続は、VPN トンネル内の IPv4 トラフィックまたは IPv6 トラフィックのいずれかをサポートできます。詳細については、「IPv4 および IPv6 トラフィック」を参照してください。

Site-to-Site VPN のターゲットゲートウェイ接続を、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修正できます。詳細については、「the section called “VPN 接続のターゲットゲートウェイを変更する”」を参照してください。

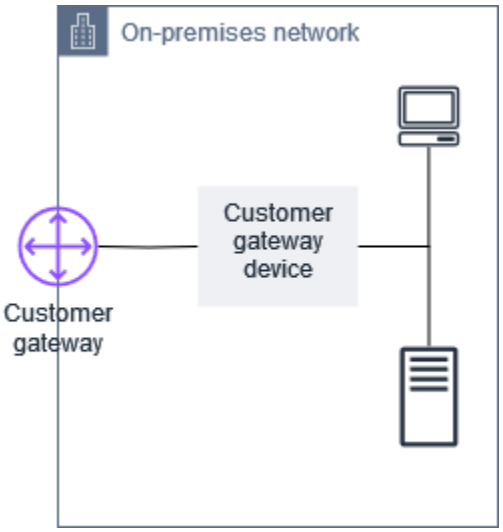
カスタマーゲートウェイデバイス

カスタマーゲートウェイデバイスは、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 接続で動作するようデバイスを構成します。詳細については、「カスタマーゲートウェイデバイス」を参照してください。

デフォルトでは、カスタマーゲートウェイデバイスは、トラフィックを生成して Internet Key Exchange (IKE) ネゴシエーションプロセスを開始することで、Site-to-Site VPN 接続のトンネルを開始する必要があります。Site-to-Site VPN 接続の設定で、代わりに AWS が IKE ネゴシエーションプロセスを開始するように指定することもできます。詳細については、「Site-to-Site VPN トンネル開始オプション」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、AWS に作成するリソースで、オンプレミスネットワーク内のカスタマーゲートウェイデバイスを表します。カスタマーゲートウェイを作成するときは、デバイスに関する情報を に提供しますAWS 詳細については、「the section called “カスタマーゲートウェイのオプション”」を参照してください。

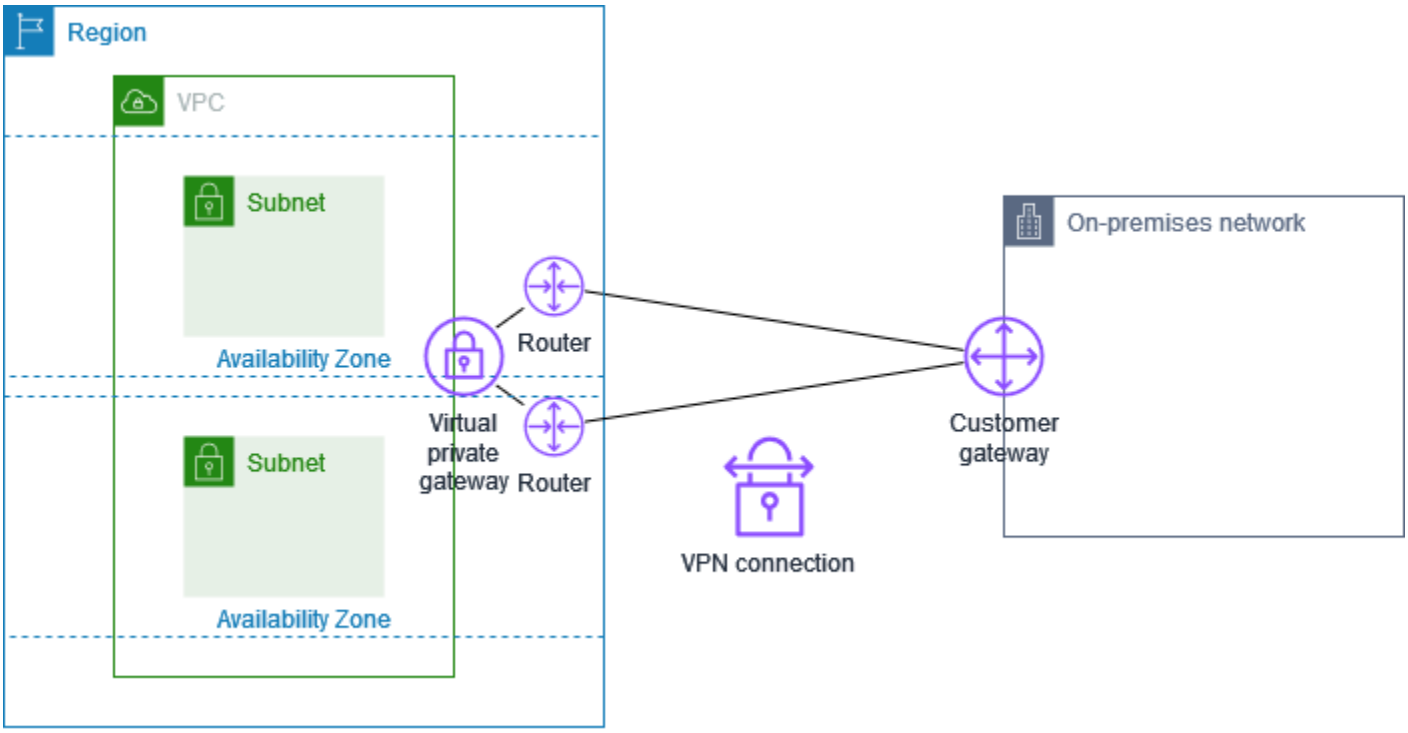


また、Site-to-Site VPN 接続で Amazon VPC を使用するには、ユーザー自身またはネットワーク管理者がリモートネットワークのカスタマーゲートウェイデバイスまたはアプリケーションを設定する必要があります。Site-to-Site VPN 接続を作成するときに、設定に必要な情報が提供され、通常はネットワーク管理者がこの設定を行います。カスタマーゲートウェイの要件および設定については、「カスタマーゲートウェイデバイス」を参照してください。

Site-to-Site VPN 接続のトンネルオプション

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、VPN 接続の 2 つのトンネルを示しています。可用性を高めるため、各トンネルは異なるアベイラビリティーゾーンで終了します。オンプレミスネットワークから AWS へのトラフィックは、両方のトンネルを使用します。AWS からオンプレミスネットワークへのトラフィックは一方のトンネルを優先しますが、AWS 側で障害が発生した場合、もう一方のトンネルに自動的にフェールオーバーできます。



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。

> **Note**
>
> Site-to-Site VPN トンネルエンドポイントは、カスタマーゲートウェイからの提案の順序に関係なく、以下のリストの最小設定値から順に、カスタマーゲートウェイからの提案を評価します。`modify-vpn-connection-options` コマンドを使用して、AWS エンドポイントが受け入れるオプションのリストを制限できます。詳細については、Amazon EC2 コマンドラインリファレンスの「modify-vpn-connection-options」をご参照ください。

設定できるトンネルオプションは以下のとおりです。

デッドピア検出 (DPD) タイムアウト

DPD タイムアウトが発生するまでの秒数。DPD タイムアウトが 40 秒の場合、VPN エンドポイントは、最初に失敗したキープアライブの 30 秒後にピアが停止したと見なします。30 以上を指定できます。

デフォルト: 40

DPD タイムアウトアクション

デッドピア検出 (DPD) タイムアウトが発生した後に実行するアクション。以下を指定することができます。

- `Clear`: DPD タイムアウトが発生したときに IKE セッションを終了する (トンネルを停止してルートをクリアする)
- `None`: DPD タイムアウトが発生しても何もアクションを実行しない
- `Restart`: DPD タイムアウトが発生したときに IKE セッションを再起動する

詳細については、「Site-to-Site VPN トンネル開始オプション」を参照してください。

デフォルト: `Clear`

VPN ログ記録オプション

Site-to-Site VPN ログを使用すると、IP セキュリティ (IPsec) トンネル確立、インターネットキー交換 (IKE) ネゴシエーション、およびデッドピア検出 (DPD) プロトコルメッセージの詳細にアクセスできます。

詳細については、「AWS Site-to-Site VPN ログ」を参照してください。

使用可能なログ形式: `json`、`text`

IKE バージョン

VPN トンネルで許可される IKE バージョン。1 つ以上のデフォルト値を指定できます。

デフォルト: `ikev1`、`ikev2`

トンネル内部 IPv4 CIDR

VPN トンネルの内部 (内部) IPv4 アドレスの範囲です。`169.254.0.0/16` 範囲からのサイズ /30 の CIDR ブロックを指定できます。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。

> **Note**
>
> CIDR ブロックは、トランジットゲートウェイ上のすべての接続にわたって一意である必要はありません。ただし、一意でない場合は、カスタマーゲートウェイで競合が発生する可能性があります。トランジットゲートウェイ上の Site-to-Site VPN 接続で同じ CIDR ブロックを再使用する場合は、慎重に進めてください。

以下の CIDR ブロックは予約済みで使用できません。

- `169.254.0.0/30`
- `169.254.1.0/30`
- `169.254.2.0/30`
- `169.254.3.0/30`
- `169.254.4.0/30`
- `169.254.5.0/30`
- `169.254.169.252/30`

デフォルト: `169.254.0.0/16` 範囲からのサイズ /30 の IPv4 CIDR ブロック。

トンネル内部 IPv6 CIDR

(IPv6 VPN 接続のみ) VPN トンネルの内部 (内部) IPv6 アドレスの範囲。ローカル `fd00::/8` 範囲からのサイズ /126 の CIDR ブロックを指定できます。CIDR ブロックは、同じトランジッ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ことが必要です。

デフォルト: ローカル `fd00::/8` 範囲からのサイズ /126 の IPv6 CIDR ブロック。

ローカル IPv4 ネットワーク CIDR

(IPv4 VPN 接続のみ) VPN トンネルを介した通信が許可される、カスタマーゲートウェイ (オンプレミス) 側の IPv4 CIDR 範囲。

デフォルト: 0.0.0.0/0

リモート IPv4 ネットワーク CIDR

(IPv4 VPN 接続のみ) VPN トンネルを介して通信できる AWS 側の IPv4 CIDR 範囲。

デフォルト: 0.0.0.0/0

ローカル IPv6 ネットワーク CIDR

(IPv6 VPN 接続のみ) VPN トンネルを介した通信が許可される、カスタマーゲートウェイ (オンプレミス) 側の IPv6 CIDR 範囲。

デフォルト: ::/0

リモート IPv6 ネットワーク CIDR

(IPv6 VPN 接続のみ) VPN トンネルを介して通信できる AWS 側の IPv6 CIDR 範囲。

デフォルト: ::/0

フェーズ 1 Diffie-Hellman (DH) グループ番号

フェーズ 1 IKE ネゴシエーションで VPN トンネルに対して許可される Diffie-Hellman グループ番号。1 つ以上のデフォルト値を指定できます。

デフォルト: 2、14、15、16、17、18、19、20、21、22、23、24

フェーズ 2 Diffie-Hellman (DH) グループ番号

フェーズ 2 IKE ネゴシエーションで VPN トンネルに対して許可される Diffie-Hellman グループ番号。1 つ以上のデフォルト値を指定できます。

デフォルト: 2、5、14、15、16、17、18、19、20、21、22、23、24

フェーズ 1 暗号化アルゴリズム

フェーズ 1 IKE ネゴシエーションで VPN トンネルで許可される暗号化アルゴリズム。1 つ以上のデフォルト値を指定できます。

デフォルト: AES128、AES256、AES128-GCM-16、AES256-GCM-16

フェーズ 2 暗号化アルゴリズム

フェーズ 2 IKE ネゴシエーションで VPN トンネルで許可される暗号化アルゴリズム。1 つ以上のデフォルト値を指定できます。

デフォルト: AES128、AES256、AES128-GCM-16、AES256-GCM-16

フェーズ 1 整合性アルゴリズム

フェーズ 1 IKE ネゴシエーションで VPN トンネルで許可される整合性アルゴリズム。1 つ以上のデフォルト値を指定できます。

デフォルト: SHA-1、SHA2-256、SHA2-384、SHA2-512

フェーズ 2 整合性アルゴリズム

フェーズ 2 IKE ネゴシエーションで VPN トンネルで許可される整合性アルゴリズム。1 つ以上のデフォルト値を指定できます。

デフォルト: SHA-1、SHA2-256、SHA2-384、SHA2-512

フェーズ 1 ライフタイム

> **Note**
>
> AWS は、フェーズ 1 ライフタイムフィールドとフェーズ 2 ライフタイムフィールドで設定されたタイミング値を使用してキーの更新を開始します。このようなライフタイムがネゴシエートされたハンドシェイク値と異なる場合、トンネル接続が中断される可能性があります。

フェーズ 1 IKE ネゴシエーションのライフタイム (秒)。値は 900 から 28,800 まで指定できます。

デフォルト: 28,800 (8 時間)

フェーズ 2 ライフタイム

> **Note**
>
> AWS は、フェーズ 1 ライフタイムフィールドとフェーズ 2 ライフタイムフィールドで設定されたタイミング値を使用してキーの更新を開始します。このようなライフタイムがネ

ゴシエートされたハンドシェイク値と異なる場合、トンネル接続が中断される可能性があります。

フェーズ 2 IKE ネゴシエーションのライフタイム (秒)。値は 900 から 3,600 まで指定できます。指定する値は、フェーズ 1 のライフタイムの秒数よりも小さくする必要があります。

デフォルト: 3,600 (1 時間)

事前共有キー (PSK)

ターゲットゲートウェイとカスタマーゲートウェイ間に最初の Internet Key Exchange (IKE) Security Association を確立するための事前共有キー (PSK)。

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。

デフォルト: 32 文字の英数字の文字列。

キー再生成ファズ

キー再生成時間がランダムに選択される、キー再生成ウィンドウ (キー再生成マージン時間によって決定される) の割合。

0 ~ 100 のパーセント値を指定できます。

デフォルト: 100

キー再生成のマージンタイム

フェーズ 1 およびフェーズ 2 のライフタイムが期限切れになるまでのマージン時間 (秒単位)。この間、VPN 接続の AWS 側が IKE キー再生成を実行します。

60 からフェーズ 2 のライフタイム秒の値の半分までの数値を指定できます。

キー再生成の正確な時間は、キー再生成ファズの値に基づいてランダムに選択されます。

デフォルト: 270 (4.5 分)

再生ウィンドウのサイズパケット

IKE 再生ウィンドウ内のパケット数。

64 から 2048 までの値を指定できます。

デフォルト: 1024

開始アクション

VPN 接続のトンネルを確立するときに実行するアクション。以下を指定することができます。

- `Start`: AWS が IKE ネゴシエーションを開始してトンネルを開始する カスタマーゲートウェイが IP アドレスで設定されている場合にのみサポートされます。
- `Add`: カスタマーゲートウェイデバイスが IKE ネゴシエーションを開始してトンネルを開始する

詳細については、「Site-to-Site VPN トンネル開始オプション」を参照してください。

デフォルト: `Add`

トンネルエンドポイントのライフサイクル制御

トンネルエンドポイントのライフサイクル制御により、エンドポイントの置き換えスケジュールを制御できます。

詳細については、「トンネルエンドポイントのライフサイクル制御」を参照してください。

デフォルト: `Off`

Site-to-Site VPN 接続の作成時にトンネルオプションを指定するか、既存の VPN 接続のトンネルオプションを変更できます。詳細については、次のトピックを参照してください。

- ステップ 5: VPN 接続を作成する
- Site-to-Site VPN トンネルオプションを変更する

Site-to-Site VPN トンネル認証オプション

事前共有キーまたは証明書を使用して、Site-to-Site VPN トンネルエンドポイントを認証できます。

事前共有キー

事前共有キーは、デフォルトの認証オプションです。

事前共有キーは、Site-to-Site VPN トンネルの作成時に指定できる、Site-to-Site VPN トンネルオプションです。

事前共有キーは、カスタマーゲートウェイデバイスを設定するときに入力する文字列です。文字列を指定しない場合は、文字列が自動的に生成されます。詳細については、「カスタマーゲートウェイデバイス」を参照してください。

AWS Private Certificate Authority からのプライベート証明書

事前共有キーを使用しない場合は、AWS Private Certificate Authority からのプライベート証明書を使用して VPN を認証できます。

AWS Private Certificate Authority (AWS Private CA) を使用して、下位 CA からプライベート証明書を作成する必要があります。ACM 下位 CA に署名するために、ACM ルート CA または外部 CA を使用できます。プライベート証明書の作成の詳細については、AWS Private Certificate Authority ユーザーガイドの「プライベート CA の作成と管理」を参照してください。

Site-to-Site VPN トンネルエンドポイントの AWS 側の証明書を生成して使用するには、サービスリンクロールを作成する必要があります。詳細については、「the section called “サービスリンクロール”」を参照してください。

プライベート証明書を生成したら、カスタマーゲートウェイの作成時に証明書を指定し、カスタマーゲートウェイデバイスに適用します。

カスタマーゲートウェイデバイスの IP アドレスを指定しない場合、IP アドレスは確認されません。このオペレーションにより、VPN 接続を再設定することなく、カスタマーゲートウェイデバイスを別の IP アドレスに移動できます。

Site-to-Site VPN トンネル開始オプション

デフォルトでは、カスタマーゲートウェイデバイスは、トラフィックを生成して Internet Key Exchange (IKE) ネゴシエーションプロセスを開始することで、Site-to-Site VPN 接続のトンネルを開始する必要があります。VPN トンネルの設定で、代わりに AWS が IKE ネゴシエーションプロセスを開始または再開するように指定することもできます。

VPN トンネル IKE 開始オプション

以下の IKE 開始オプションを使用できます。Site-to-Site VPN 接続のトンネルの一方または両方に対して、1 つまたは両方のオプションを設定できます。これらの設定やその他のトンネルオプション設定の詳細については、「VPN トンネルオプション」を参照してください。

- 開始アクション: 新規または変更された VPN 接続の VPN トンネルを確立するときに実行するアクション。デフォルトでは、カスタマーゲートウェイデバイスが IKE ネゴシエーションプロセスを開始してトンネルを開始します。代わりに AWS が IKE ネゴシエーションプロセスを開始するように指定することもできます。

- DPD タイムアウトアクション: デッドピア検出 (DPD) タイムアウトが発生した後に実行するアクション。デフォルトでは、IKE セッションが停止し、トンネルが停止して、ルートが削除されます。DPD タイムアウトが発生したときに AWS が IKE セッションを再起動するように指定できます。または、DPD タイムアウトが発生しても AWS が何もアクションを実行しないように指定することもできます。

ルールと制限

以下のルールと制限が適用されます。

- IKE ネゴシエーションを開始するには、AWS でカスタマーゲートウェイデバイスのパブリック IP アドレスが必要です。VPN 接続に証明書ベースの認証を設定していて、AWS でカスタマーゲートウェイリソースを作成したときに IP アドレスを指定しなかった場合は、新しいカスタマーゲートウェイを作成して IP アドレスを指定する必要があります。その後、VPN 接続を変更し、新しいカスタマーゲートウェイを指定します。詳細については、「Site-to-Site VPN 接続のカスタマーゲートウェイを変更する」を参照してください。
- VPN 接続の AWS 側からの IKE 開始 (起動アクション) は IKEv2 でのみサポートされています。
- VPN 接続の AWS 側から IKE 開始を使用する場合、タイムアウト設定は含まれません。接続が確立されるまで、継続して接続が試みられます。さらに、VPN 接続の AWS 側は、カスタマーゲートウェイから SA の削除メッセージを受信すると、IKE ネゴシエーションを再開します。
- カスタマーゲートウェイデバイスがネットワークアドレス変換 (NAT) を使用するファイアウォールまたはその他のデバイスの背後にある場合は、ID (IDr) を設定する必要があります。IDr の詳細については、RFC 7296 を参照してください。

VPN トンネルの AWS 側からの IKE 開始を設定しておらず、VPN 接続でアイドル時間が発生する場合 (設定によっては通常 10 秒)、トンネルが終了することがあります。この問題が発生しないように、ネットワークモニタリングツールを使用してキープアライブ ping を生成できます。

VPN トンネル開始オプションの使用

VPN トンネル開始オプションの使用の詳細については、以下のトピックを参照してください。

- 新しい VPN 接続を作成し、VPN トンネル開始オプションを指定するには: ステップ 5: VPN 接続を作成する
- 既存の VPN 接続の VPN トンネル開始オプションを変更するには: Site-to-Site VPN トンネルオプションを変更する

Site-to-Site VPN トンネルエンドポイントの置換

Site-to-Site VPN 接続は、冗長性のために 2 つの VPN トンネルで構成されます。AWS がトンネルの更新を実行するとき、または VPN 接続を変更するときに、VPN トンネルエンドポイントの一方または両方が置き換えられることがあります。トンネルエンドポイントの置換中に、新しいトンネルエンドポイントがプロビジョニングされている間、トンネルを介した接続が中断されることがあります。

トピック

お客様によるエンドポイントの置き換え

VPN 接続の以下のコンポーネントを変更すると、トンネルエンドポイントの一方または両方が置き換えられます。

変更	API アクション	トンネルインパクト
VPN 接続のターゲットゲートウェイを変更する	ModifyVpnConnection	新しいトンネルエンドポイントがプロビジョニングされている間は、どちらのトンネルも使用できません。
VPN 接続のカスタマーゲートウェイを変更する	ModifyVpnConnection	新しいトンネルエンドポイントがプロビジョニングされている間は、どちらのトンネルも使用できません。
VPN 接続オプションを変更する	ModifyVpnConnectionOptions	新しいトンネルエンドポイントがプロビジョニングされている間は、どちらのトンネルも使用できません。
VPN トンネルオプションを変更する	ModifyVpnTunnelOptions	更新中は、変更されたトンネルを使用できません。

AWS マネージドのエンドポイントの置き換え

AWS Site-to-Site VPN はマネージド型サービスであり、定期的に VPN トンネルエンドポイントに更新を適用します。これらの更新は、以下のようなさまざまな理由で発生します。

- パッチ、回復性の向上、その他の機能強化など、一般的なアップグレードを適用するため
- 基盤となるハードウェアをリタイアするため
- VPN トンネルエンドポイントが非正常であることが自動モニタリングによって判断された場合

AWS は、トンネルエンドポイントの更新を一度に VPN 接続の 1 つのトンネルに適用します。トンネルエンドポイントの更新中、VPN 接続の冗長性が短時間失われる可能性があります。したがって、高可用性を実現するために、VPN 接続で両方のトンネルを設定することが重要です。

トンネルエンドポイントのライフサイクル制御

トンネルエンドポイントのライフサイクル制御により、エンドポイントの置き換えスケジュールを制御し、AWS マネージドのトンネルエンドポイントの置き換え中における接続の中断を最小限に抑えることができます。この機能を使用すると、ビジネスに最適なタイミングでトンネルエンドポイントへの AWS マネージド更新を受け入れるように選択できます。この機能は、短期的なビジネスニーズがある場合や、VPN 接続ごとに 1 つのトンネルのみサポートできる場合に使用します。

> **Note**
>
> まれに、トンネルエンドポイントのライフサイクル制御機能が有効になっていても、AWS は重要な更新をトンネルエンドポイントに直ちに適用する場合があります。

トピック

トンネルエンドポイントのライフサイクル制御の仕組み

VPN 接続内の個々のトンネルに対してトンネルエンドポイントのライフサイクル制御機能を有効にします。VPN の作成時に有効にするか、既存の VPN 接続のトンネルオプションを変更することで有効にすることができます。

トンネルエンドポイントのライフサイクル制御を有効にすると、次の 2 つの方法で今後のトンネルメンテナンスイベントをより詳細に把握できます。

- 今後のトンネルエンドポイントの置き換えに関する AWS Health 通知が届きます。
- 保留中のメンテナンスのステータスは、メンテナンスを自動的に適用するタイムスタンプおよび最終メンテナンスを適用するタイムスタンプと共に AWS Management Console で確認できます。または、get-vpn-tunnel-replacement-status AWS CLI コマンドを使用して確認できます。

トンネルエンドポイントのメンテナンスが利用可能な場合、指定したメンテナンスを自動的に適用するタイムスタンプの前に、都合の良いタイミングで更新を受け入れる機会があります。

メンテナンスを自動的に適用する日付の前に更新を適用しない場合、AWS は、通常のメンテナンス更新サイクルの一環として、トンネルエンドポイントの置き換えを自動的に実行します。

トンネルエンドポイントのライフサイクル制御を有効にする

この機能を有効にするには、AWS Management Console または AWS CLI を使用します。

> **Note**
>
> デフォルトでは、この機能を既存の VPN 接続で有効にすると、トンネルエンドポイントの置き換えが同時に開始されます。この機能を有効にしても、トンネルエンドポイントの置き換えをすぐに開始しない場合は、[トンネルの置き換えをスキップ] オプションを使用できます。

Existing VPN connection

以下の手順は、既存の VPN 接続でトンネルエンドポイントのライフサイクル制御を有効にする方法を示しています。

AWS Management Console を使用してトンネルエンドポイントのライフサイクル制御を有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. 左側のナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [VPN 接続] で適切な接続を選択します。
4. [アクション]、[VPN トンネルオプションを変更] の順に選択します。
5. 適切な [IP アドレス外の VPN トンネル] を選択し、変更するトンネルを選択します。
6. [トンネルエンドポイントのライフサイクル制御] で、[有効化] チェックボックスをオンにします。
7. (オプション) [トンネルの置き換えをスキップ] を選択します。
8. [変更の保存] をクリックします。

AWS CLI を使用してトンネルエンドポイントのライフサイクル制御を有効にするには

modify-vpn-tunnel-options コマンドを使用して、トンネルエンドポイントのライフサイクル制御を有効にします。

New VPN connection

以下の手順は、新しい VPN 接続の作成時にトンネルエンドポイントのライフサイクル制御を有効にする方法を示しています。

AWS Management Console を使用して新しい VPN 接続の作成時にトンネルエンドポイントのライフサイクル制御を有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN Connections] (Site-to-Site VPN 接続) を選択します。
3. [Create VPN connection] (VPN 接続の作成) を選択します。
4. [トンネル 1 のオプション] セクションと [トンネル 2 のオプション] セクションの [トンネルエンドポイントのライフサイクル制御] で、[有効化] を選択します。
5. [VPN 接続の作成] を選択します。

AWS CLI を使用して新しい VPN 接続の作成時にトンネルエンドポイントのライフサイクル制御を有効にするには

create-vpn-connection コマンドを使用して、トンネルエンドポイントのライフサイクル制御を有効にします。

トンネルエンドポイントのライフサイクル制御が有効になっているかどうかを確認する

AWS Management Console または CLI を使用して、トンネルエンドポイントのライフサイクル制御が既存の VPN トンネルで有効になっているかどうかを確認できます。

AWS Management Console を使用してトンネルエンドポイントのライフサイクル制御が有効になっているかどうかを確認するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. 左側のナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [VPN 接続] で適切な接続を選択します。
4. [トンネルの詳細] タブを選択します。
5. トンネルの詳細で、[トンネルエンドポイントのライフサイクル制御] を探し、この機能が [有効] になっているか、[無効] になっているかを確認します。

AWS CLI を使用してトンネルエンドポイントのライフサイクル制御が有効になっているかどうかを確認するには

describe-vpn-connections コマンドを使用して、トンネルエンドポイントのライフサイクル制御が有効になっているかどうかを確認します。

利用可能な更新を確認する

トンネルエンドポイントのライフサイクル制御機能を有効にすると、AWS Management Console または CLI を使用して VPN 接続のメンテナンス更新が利用可能かどうかを確認できます。

AWS Management Console を使用して利用可能な更新を確認するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. 左側のナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [VPN 接続] で適切な接続を選択します。
4. [トンネルの詳細] タブを選択します。

5. [保留中のメンテナンス] 列を確認します。ステータスは [利用可能] または [なし] のいずれかです。

AWS CLI を使用して利用可能な更新を確認するには

get-vpn-tunnel-replacement-status コマンドを使用して、利用可能な更新があるかどうかを確認します。

メンテナンス更新を受け入れる

メンテナンス更新が利用可能である場合、AWS Management Console または CLI を使用して更新を受け入れることができます。

AWS Management Console を使用して利用可能なメンテナンス更新を受け入れるには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. 左側のナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [VPN 接続] で適切な接続を選択します。
4. [アクション]、[VPN トンネルを置き換え] の順に選択します。
5. 適切な [IP アドレス外の VPN トンネル] を選択し、置き換えるトンネルを選択します。
6. [Replace (置換)] を選択します。

AWS CLI を使用して利用可能なメンテナンス更新を受け入れるには

replace-vpn-tunnel コマンドを使用して、利用可能なメンテナンス更新を受け入れます。

トンネルエンドポイントのライフサイクル制御をオフにする

トンネルエンドポイントのライフサイクル制御機能を使用する必要がなくなった場合は、AWS Management Console または AWS CLI を使用してオフにできます。この機能をオフにすると、AWS は、メンテナンス更新を定期的に自動デプロイし、これらの更新を営業時間中に行う場合があります。ビジネスへの影響を回避するために、VPN 接続で両方のトンネルを設定して高可用性を確保することを強くお勧めします。

> **Note**
>
> 保留中の利用可能なメンテナンスがある場合、この機能をオフにしている間は、[トンネルの置き換えをスキップ] オプションを指定することはできません。この機能は、[トンネルの

置き換えをスキップ] オプションを使わなくても、いつでもオフにできます。ただし、AWS は、トンネルエンドポイントの置き換えをすぐに開始して、保留中の利用可能なメンテナンス更新を自動的にデプロイします。

AWS Management Console を使用してトンネルエンドポイントのライフサイクル制御をオフにするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. 左側のナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [VPN 接続] で適切な接続を選択します。
4. [アクション]、[VPN トンネルオプションを変更] の順に選択します。
5. 適切な [IP アドレス外の VPN トンネル] を選択し、変更するトンネルを選択します。
6. トンネルエンドポイントのライフサイクル制御をオフにするには、[トンネルエンドポイントのライフサイクル制御] の [有効化] チェックボックスをオフにします。
7. (オプション) [トンネルの置き換えをスキップ] を選択します。
8. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用してトンネルエンドポイントのライフサイクル制御をオフにするには

modify-vpn-tunnel-options コマンドを使用して、トンネルエンドポイントのライフサイクル制御をオフにします。

Site-to-Site VPN 接続のカスタマーゲートウェイオプション

次の表は、 で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 AWS

項目	説明
(オプション) 名前タグ。	「名前」のキーと指定した値を含むタグを作成します。
(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。	1 ~ 2,147,483,647 の範囲の ASN がサポートされています。ネットワークに割り当てられている既存のパブリック ASN を使用できます。ただし、次の場合を除きます。

項目	説明
	• 7224 - すべてのリージョンで予約されています • 9059 - eu-west-1 リージョンで予約されています • 10124 - ap-northeast-1 リージョンで予約されています • 17943 - ap-southeast-1 リージョンで予約されています 既存の ASN がない場合は、プライベート ASN (64512 ~ 65534 の範囲) を使用できます。デフォルトの ASN は 65000 です。カスタマーゲートウェイは、4,200,000,000 ~ 4,294,967,294 の範囲でプライベート ASN をサポートしていません。ルーティングの詳細については、「Site-to-Site VPN のルーティングオプション」を参照してください。
(オプション) カスタマーゲートウェイデバイスの外部インターフェイスの IP アドレス。	IP アドレスは静的である必要があります。 カスタマーゲートウェイデバイスがネットワークアドレス変換 (NAT) の背後にある場合は、NAT デバイスの IP アドレスを使用します。また、ポート 500 (および NAT トラバーサルが使用されている場合はポート 4500) の UDP パケットがネットワークと AWS Site-to-Site VPN エンドポイントの間で通過できることを確認します。詳細については、「ファイアウォールルール」を参照してください。 からのプライベート証明書 AWS Private Certificate Authority とパブリック VPN を使用している場合、IP アドレスは必要ありません。

項目	説明
(オプション) AWS Certificate Manager (ACM) を使用した下位 CA からのプライベート証明書。	証明書ベースの認証を使用する場合は、カスタマーゲートウェイデバイスで使用される ACM プライベート証明書の ARN を指定します。 カスタマーゲートウェイを作成するときに、AWS Private Certificate Authority プライベート証明書を使用して Site-to-Site VPN を認証するようにカスタマーゲートウェイを設定できます。 このオプションを使用する場合は、組織で内部使用できるように、完全に AWSホストされたプライベート認証機関 (CA) を作成します。ルート CA 証明書と下位 CA 証明書の両方が によって保存および管理されます AWS Private CA。 カスタマーゲートウェイを作成する前に、 を使用して下位 CA からプライベート証明書を作成し AWS Private Certificate Authority、カスタマーゲートウェイを設定するときに証明書を指定します。プライベート証明書の作成の詳細については、AWS Private Certificate Authority ユーザーガイドの「プライベート CA の作成と管理」を参照してください。
(オプション) デバイス。	このカスタマーゲートウェイに関連するカスタマーゲートウェイデバイスの名前。

Site-to-Site VPN 接続の高速化

オプションで、Site-to-Site VPN 接続のアクセラレーションを有効にできます。高速 Site-to-Site VPN 接続 (高速 VPN 接続) では、 AWS Global Accelerator を使用してオンプレミスネットワークからカスタマーゲートウェイデバイスに最も近い AWS エッジロケーションにトラフィックをルーティングします。 は、輻輳のない AWS グローバルネットワークを使用して、最適なアプリケーション

パフォーマンスを提供するエンドポイントにトラフィックをルーティングします (詳細については、AWS Global Accelerator「」を参照してくださいAWS Global Accelerator)。高速 VPN 接続を使用すると、トラフィックがパブリックインターネット経由でルーティングされるときに発生する可能性のあるネットワークの中断を回避できます。

高速 VPN 接続を作成すると、VPN トンネルごとに 1 つずつ、2 つのアクセラレーターが作成および管理されます。 AWS Global Accelerator コンソールまたは APIs を使用して、これらのアクセラレータを自分で表示または管理することはできません。

高速 VPN 接続をサポートする AWS リージョンの詳細については、AWS 「高速 Site-to-Site VPN に関するFAQs」を参照してください。

高速化を有効にする

デフォルトでは、Site-to-Site VPN 接続を作成すると、アクセラレーションは無効になります。トランジットゲートウェイ上に新しいSite-to-Site VPN アタッチメントを作成する際に、オプションでアクセラレーションを有効にすることができます。詳細と手順については、「トランジットゲートウェイ VPN アタッチメントを作成する」を参照してください。

高速 VPN 接続では、トンネルエンドポイント IP アドレス用に別個の IP アドレスのプールが使用されます。2 つの VPN トンネルの IP アドレスは、2 つの別々のネットワークゾーンから選択されます。

ルールと制限

高速 VPN 接続を使用する場合は、次のルールが適用されます。

- アクセラレーションは、トランジットゲートウェイにアタッチされている Site-to-Site VPN接続でのみサポートされます。仮想プライベートゲートウェイは、高速化 VPN 接続をサポートしません。
- 高速 Site-to-Site VPN 接続は、 AWS Direct Connect パブリック仮想インターフェイスでは使用できません。
- 既存のサイト間 VPN 接続のアクセラレーションを有効または無効にすることはできません。代わりに、必要に応じてアクセラレーションを有効または無効にして、新しいサイト間 VPN 接続を作成することができます。次に、新しい Site-to-Site VPN 接続を使用するようにカスタマーゲートウェイデバイスを設定し、古い Site-to-Site VPN 接続を削除します。
- 高速化 VPN 接続には、NAT トラバーサル (NAT-T) が必要であり、デフォルトで有効になっています。Amazon VPC コンソールから設定ファイルをダウンロードした場合は、NAT-T 設定を確認し、必要に応じて調整します。

- 高速 VPN トンネルの IKE ネゴシエーションは、カスタマーゲートウェイデバイスから開始する必要があります。この動作に影響する 2 つのトンネルオプションは、`Startup Action`と ですDPD `Timeout Action`。詳細については、「VPN トンネルオプション」と「VPN トンネル開始オプション」を参照してください。
- 証明書ベースの認証を使用する Site-to-Site VPN 接続は、Global Accelerator でのパケットフラグメンテーションのサポートが制限されているため AWS Global Accelerator、 と互換性がない可能性があります。詳細については、AWS Global Accelerator の仕組みを参照してください。証明書ベースの認証を使用する高速 VPN 接続が必要な場合は、カスタマーゲートウェイデバイスが IKE の断片化をサポートしている必要があります。それ以外の場合は、VPN の高速化を有効にしないでください。

Site-to-Site VPN の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クォータがあります。詳細については、「Amazon VPC ユーザーガイド」で、「Amazon VPC クォータ」の「ルートテーブル」セクションを参照してください。

トピック

- 静的および動的ルーティング
- ルートテーブルと VPN ルーティングの優先度
- VPN トンネルエンドポイント更新中のルーティング
- IPv4 および IPv6 トラフィック

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、カスタマーゲートウェイデバイスの製造元とモデルによって異なります。カスタマーゲートウェイ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。カスタマーゲートウェイデバイスが 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。

BGP アドバタイズメントをサポートしている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ため、Site-to-Site VPN 接続への静的ルートを指定しません。BGP アドバタイズメント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。

オンプレミスのネットワークから Site-to-Site VPN 接続にトラフィックがルーティングされるように、カスタマーゲートウェイデバイスを設定する必要があります。設定は、デバイスの製造元とモデルによって異なります。詳細については、「カスタマーゲートウェイデバイス」を参照してください。

ルートテーブルと VPN ルーティングの優先度

ルートテーブルは、VPC からのネットワークトラフィックの転送先を指定します。VPC 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。

トラフィックと一致する最も具体的なルートをルートテーブルで使用して、トラフィックをルーティングする方法を決定します (最長プレフィックス一致)。ルートテーブルに重複または一致するルートがある場合は、次のルールが適用されます。

- Site-to-Site VPN 接続または AWS Direct Connect 接続から伝達されるルートが VPC のローカルルートと重複する場合は、伝達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 (プレフィックスの最長一致は適用できません) 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、トランジットゲートウェイ、またはゲートウェイ VPC エンドポイントの静的ルートが優先されます。

たとえば、次のルートテーブルにはインターネットゲートウェイへの静的ルート、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、送信先は 172.31.0.0/24 です。この場合、172.31.0.0/24 を送信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、伝達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-11223344556677889 (伝達済み)
172.31.0.0/24	igw-12345678901234567 (静的)

BGP アドバタイズ経由または静的ルートエントリ経由かを問わず、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 IPv6 トラフィックをサポートしません。

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、パスを選択してトラフィックをルーティングする方法を指定します。すべてのエンドポイントが正常であれば、最も長いプレフィックス一致が適用されます。トンネルエンドポイントの状態は、他のルーティング属性よりも優先されます。この優先は、仮想プライベートゲートウェイとトランジットゲートウェイ上の VPN に適用されます。プレフィックスが同じである場合、仮想プライベートゲートウェイは、次のようにルートに優先順位を付けます (優先度の高い順)。

- 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
- 各 Site-to-Site VPN 接続が BGP を使用しているプレフィックスのマッチングでは、AS PATH が比較され、最短の AS PATH を持っているプレフィックスが優先されます。

> **Note**
>
> AWS は、非対称ルーティングをサポートするカスタマーゲートウェイデバイスの使用を強く推奨します。

非対称ルーティングをサポートするカスタマーゲートウェイデバイスを使用する場合、両方のトンネルの AS PATH を等しくするために、AS PATH の付加をお勧めしません。これにより、VPN トンネルエンドポイントの更新中にトンネルに設定した multi-exit discriminator (MED) 値を使用して、トンネルの優先度を決定できます。
非対称ルーティングをサポートしていないカスタマーゲートウェイデバイスを使用する場合は、AS PATH プリペンドとローカル設定を使用して、一方のトンネルを他のトンネルよりも優先できます。ただし、出力パスが変更されると、これによりトラフィックがドロップする可能性があります。

- AS PATH が同じ長さで、AS_SEQUENCE 内の最初の AS が複数のパスで同じである場合、multi-exit discriminators (MED) が比較されます。最小の MED 値を持つパスが優先されます。

ルーティングの優先度は、VPN トンネルエンドポイントの更新中に影響を受けます。

Site-to-Site VPN 接続では、AWS は 2 つの冗長トンネルのうちの 1 つをプライマリ送信パスとして選択します。この選択は、ときどき変更される場合があるため、両方のトンネルの可用性を高めるよう設定し、非対称ルーティングを許可することを強くお勧めします。トンネルエンドポイントの状態は、他のルーティング属性よりも優先されます。この優先は、仮想プライベートゲートウェイとトランジットゲートウェイ上の VPN に適用されます。

仮想プライベートゲートウェイの場合、ゲートウェイ上のすべての Site-to-Site VPN 接続にまたがる 1 つのトンネルが選択されます。複数のトンネルを使用するには、トランジットゲートウェイ上の Site-to-Site VPN 接続でサポートされる Equal Cost Multipath (ECMP) について検討することをお勧めします。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」を参照してください。ECMP は、仮想プライベートゲートウェイの Site-to-Site VPN 接続ではサポートされません。

BGP を使用する Site-to-Site VPN 接続の場合、プライマリトンネルは multi-exit discriminator (MED) 値で識別できます。ルーティングの決定に影響を与えるために、より具体的な BGP ルートをアドバタイズすることをお勧めします。

静的ルーティングを使用する Site-to-Site VPN 接続の場合、プライマリトンネルはトラフィック統計情報またはメトリクスによって識別できます。

VPN トンネルエンドポイント更新中のルーティング

Site-to-Site VPN 接続は、カスタマーゲートウェイデバイスと仮想プライベートゲートウェイまたはトランジットゲートウェイの間の 2 つの VPN トンネルで構成されます。両方のトンネルに冗長性を設定することをお勧めします。AWS は、VPN 接続の定期的なメンテナンスも行っており、VPN 接

続の 2 つのトンネルのうち 1 つが一時的に無効になる場合があります。詳細については、「トンネルエンドポイント交換通知」を参照してください。

一方の VPN トンネルで更新を実行する場合、もう一方のトンネルでアウトバウンド multi-exit discriminator (MED) の値を低く設定します。両方のトンネルを使用するようにカスタマーゲートウェイデバイスを設定している場合、VPN 接続はトンネルエンドポイント更新プロセス中にもう一方の (アップ) トンネルを使用します。

> **Note**
>
> MED の低いアップトンネルが優先されるようにするには、カスタマーゲートウェイデバイスで、両方のトンネルに対して同じ重みおよびローカル優先設定の値が使用されていることを確認します (重みおよびローカル優先設定は MED よりも優先度が高くなります)。

IPv4 および IPv6 トラフィック

トランジットゲートウェイの Site-to-Site VPN 接続は、VPN トンネル内の IPv4 トラフィックまたは IPv6 トラフィックのいずれかをサポートできます。デフォルトでは、Site-to-Site VPN 接続は VPN トンネル内の IPv4 トラフィックをサポートします。VPN トンネル内の IPv6 トラフィックをサポートするように新しい Site-to-Site VPN 接続を設定できます。この場合、VPC とオンプレミスネットワークを IPv6 アドレス指定用に設定すると、VPN 接続を介して IPv6 トラフィックを送信できます。

Site-to-Site VPN 接続で VPN トンネルの IPv6 を有効にすると、各トンネルに 2 つの CIDR ブロックが割り当てられます。1 つはサイズ /30 の IPv4 CIDR ブロックで、もう 1 つはサイズ /126 の IPv6 CIDR ブロックです。

以下のルールが適用されます。

- IPv6 アドレスは、VPN トンネルの内部 IP アドレスでのみサポートされます。AWS エンドポイントの外部トンネル IP アドレスは IPv4 アドレスであり、カスタマーゲートウェイのパブリック IP アドレスは IPv4 アドレスであることが必要です。
- 仮想プライベートゲートウェイの Site-to-Site VPN 接続は IPv6 をサポートしません。
- 既存の Site-to-Site VPN 接続に対して IPv6 サポートを有効にすることはできません。
- Site-to-Site VPN 接続は、IPv4 トラフィックと IPv6 トラフィックの両方はサポートできません。

VPN 接続の作成の詳細については、「ステップ 5: VPN 接続を作成する」を参照してください。

AWS Site-to-Site VPN の開始方法

AWS Site-to-Site VPN 接続をセットアップするには、以下の手順を実行します。作成時に、ターゲットゲートウェイタイプに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で、または「関連付けられていない」を指定します。[関連付けなし] を指定する場合は、後でターゲットゲートウェイタイプを選択するか、AWS クラウド WAN に対し VPN アタッチメントとして使用することができます。このチュートリアルは、仮想プライベートゲートウェイを使用して VPN 接続を作成する方法について説明します。1 つ以上のサブネットを持つ既存の VPC があることを前提としています。

仮想プライベートゲートウェイを使用して VPN 接続を設定するには、以下のステップを実行します。

タスク

- 前提条件
- ステップ 1: カスタマーゲートウェイを作成する
- ステップ 2: ターゲットゲートウェイを作成する
- ステップ 3: ルーティングを設定する
- ステップ 4: セキュリティグループを更新する
- ステップ 5: VPN 接続を作成する
- ステップ 6: 設定ファイルをダウンロードする
- ステップ 7: カスタマーゲートウェイデバイスを設定する

関連タスク

- AWSクラウド WAN の VPN 接続を作成するには、「AWS クラウド WAN の VPN アタッチメントを作成する」を参照してください。
- トランジットゲートウェイで VPN 接続を作成するには、「トランジットゲートウェイ VPN アタッチメントを作成する」を参照してください 。

前提条件

VPN 接続のコンポーネントを設定および構成するには、次の情報が必要です。

項目	情報
カスタマーゲートウェイデバイス	VPN 接続のお客様側にある物理デバイスまたはソフトウェアデバイス。ベンダー (Cisco など)、プラットフォーム (ISR シリーズルーターなど)、およびソフトウェアバージョン (IOS 12.4 など) が必要です。
カスタマーゲートウェイ	AWS でカスタマーゲートウェイリソースを作成するには、次の情報が必要です。 • デバイスの外部インターフェイス用のインターネットルーティングが可能な IP アドレス。 • ルーティングのタイプ: 静的または動的 • 動的ルーティングの場合、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) • (オプション) VPN を認証するための AWS Private Certificate Authority のプライベート証明書 詳細については、「カスタマーゲートウェイのオプション」を参照してください。
(オプション) BGP セッションの AWS 側の ASN	これは、仮想プライベートゲートウェイまたは Transit Gateway を作成するときに指定します。値を指定していない場合、デフォルトの ASN が適用されます。詳細については、「仮想プライベートゲートウェイ」を参照してください。
VPN 接続	VPN 接続を作成するには、次の情報が必要です。 • 静的ルーティングの場合、プライベートネットワークの IP プレフィックス。

項目	情報
	• (オプション) 各 VPN トンネルのトンネルオプション。詳細については、「Site-to-Site VPN 接続のトンネルオプション」を参照してください。

ステップ 1: 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」を参照してください。

プライベート証明書を使用して VPN を認証する場合は、AWS Private Certificate Authority を使用して下位 CA からプライベート証明書を作成します。プライベート証明書の作成の詳細については、AWS Private Certificate Authority ユーザーガイドの「プライベート CA の作成と管理」を参照してください。

> **Note**
>
> プライベート証明書の IP アドレスまたは Amazon リソース名を指定する必要があります。

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) 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] を選択します。
3. [カスタマーゲートウェイの作成]] を選択します。
4. (オプション) [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。
5. [BGP ASN] に、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) を入力します。
6. (オプション) [IP アドレス] に、カスタマーゲートウェイデバイスのインターネットルーティング可能な静的 IP アドレスを入力します。カスタマーゲートウェイデバイスが 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。

7. (オプション) プライベート証明書を使用する場合は、[Certificate ARN (証明書 ARN)] で、プライベート証明書の Amazon リソース名を選択します。
8. (オプション) [デバイス] には、このカスタマーゲートウェイに関連するカスタマーゲートウェイデバイスの名前を入力します。
9. [カスタマーゲートウェイの作成]] を選択します。

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)

ステップ 2: ターゲットゲートウェイを作成する

VPC とオンプレミスネットワークの間に VPN 接続を確立するには、接続の AWS 側でターゲットゲートウェイを作成する必要があります。ターゲットゲートウェイは、仮想プライベートゲートウェイまたは Transit Gateway にすることができます。

仮想プライベートゲートウェイの作成

仮想プライベートゲートウェイを作成するときは、Amazon 側のゲートウェイのカスタムプライベート自律システム番号 (ASN) 指定するか、Amazon のデフォルト ASN を使用できます。ASN は、カスタマーゲートウェイに指定した 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 [仮想プライベートゲートウェイ] を選択します。
2. [Create virtual private gateway] (仮想プライベートゲートウェイの作成) を選択します。
3. (オプション) [名前タグ] に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。
4. [AS 番号 (ASN)] では、デフォルトの選択を使用するために 、デフォルトの選択 [Amazon のデフォルト ASN] 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。

5. [Create virtual private gateway] (仮想プライベートゲートウェイの作成) を選択します。
6. 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)、[Attach to VPC] (VPC にアタッチ) の順に選択します。
7. [使用可能な VPC] で VPC を選択し、次に [VPC にアタッチ] 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)

Transit Gateway を作成する

Transit Gateway の作成の詳細については、Amazon VPC Transit Gatewayの「Transit Gateway」を参照してください。

ステップ 3: ルーティングを設定する

VPC の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、VPN 接続で使用されるルートがルートテーブルに含まれるようにし、仮想プライベートゲートウェイまたはトランジットゲートウェイを指すように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) ルートテーブルでルート伝播を有効にする

ルートテーブルのルート伝播を有効にして、Site-to-Site VPN ルートを自動的に伝播することができます。

静的ルーティングでは、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、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**
>
> 接続が中断されても、VPN 接続が UP のままの場合、ルートテーブルにある伝播されたルートは自動的に削除されません。たとえば、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は、この点に注意してください。その場合、伝播されたルートを削除するには、ルートの伝播を無効にする必要があります。

コンソールを使用してルート伝達を有効にするには

1. ナビゲーションペインで、[Route tables] (ルートテーブル) を選択します。
2. 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。
3. [ルート伝播] タブで、[ルート伝達の編集] を選択します。前の手順で作成した仮想プライベートキーファイルを選択してから、[保存] を選択します。

> **Note**
>
> ルート伝播を有効にしない場合、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、[Routes]、[Edit] 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。[Target] では、仮想プライベートゲートウェイ ID を選択し、[Save] を選択します。

コンソールを使用してルート伝達を無効にするには

1. ナビゲーションペインで、[Route tables] (ルートテーブル) を選択します。
2. 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。
3. [ルート伝播] タブで、[ルート伝達の編集] を選択します。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ます。
4. [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達を有効にするには

- 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達を無効にするには

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

(Transit Gateway) ルートテーブルにルートを追加します

Transit Gateway のルートテーブルの伝播を有効にした場合、VPN アタッチメントのルートは Transit Gateway のルートテーブルに伝播されます。詳細については、Amazon VPC Transit Gatewaysの「ルーティング」を参照してください。

VPC を Transit Gateway にアタッチし、VPC 内のリソー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、サブネットルートテーブルにルートを追加して、Transit Gateway を指すようにする必要があります。

ルートを VPC ルートテーブルに追加するには

1. ナビゲーションペインで、[ルートテーブル] を選択します。
2. VPC に関連付けられているルートテーブルを選択します。
3. [Routes] タブで、[Edit routes] を選択します。
4. [Add Rule (ルートの追加)] を選択します。
5. [送信先] に、送信先の IP アドレス範囲を入力します。[Target (ターゲット)] で、Transit Gateway を選択します。
6. [Save changes] (変更の保存) をクリックします。

ステップ 4: 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、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) を選択します。
2. VPC のデフォルトのセキュリティグループを選択します。
3. [インバウンドルール] タブで、[インバウンドルールの編集] を選択します。
4. 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] を選択します。詳細については、「Amazon VPC ユーザーガイド」の「セキュリティグループの操作」を参照してください。

ステップ 5: VPN 接続を作成する

カスタマーゲートウェイと、前に作成した仮想プライベートゲートウェイまたは Transit Gateway を組み合わせて VPN 接続を作成します。

VPN 接続を作成するには

1. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
2. [Create VPN connection] (VPN 接続の作成) を選択します。
3. (オプション) [名前タグ] には、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。
4. [Target gateway type] (ターゲットゲートウェイタイプ) で、[仮想プライベートゲートウェイ] または [Transit gateway] (転送ゲートウェイ) を選択します。次に、以前に作成した仮想プライベートゲートウェイまたは Transit Gateway を選択します。
5. [カスタマーゲートウェイ] で [既存] を選択し、[カスタマーゲートウェイ ID] から、前に作成したカスタマーゲートウェイを選択します。
6. カスタマーゲートウェイ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かどうかに基づいて、ルーティングオプションのいずれかを選択します。
   - カスタマーゲートウェイデバイスが 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。
   - カスタマーゲートウェイデバイスが 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、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。
7. ターゲットゲートウェイタイプが転送ゲートウェイの場合、[トンネル内部 IP バージョン] で、VPN トンネルが IPv4 トラフィックをサポートするか、IPv6 トラフィックをサポートする

かを指定します。IPv6 トラフィックは、Transit Gateway の VPN 接続でのみサポートされます。

8. [トンネル内部 IP バージョン] で [IPv4] を指定した場合は、オプションとして、カスタマーゲートウェイ側と AWS 側で VPN トンネルを介した通信を許可する IPv4 CIDR 範囲を指定できます。デフォルトは `0.0.0.0/0` です。

   [トンネル内部 IP バージョン] で [IPv6] を指定した場合は、オプションとして、カスタマーゲートウェイ側と AWS 側で VPN トンネルを介した通信を許可する IPv6 CIDR 範囲を指定できます。両方の範囲のデフォルトは `::/0` です。

9. [外部 IP アドレスのタイプ] については、デフォルトオプションの [PublicIpv4] のままにします。

10. (オプション) [トンネルオプション] では、トンネルごとに次の情報を指定できます。

    - トンネル内部 IPv4 アドレスの `169.254.0.0/16` 範囲からサイズ /30 の IPv4 CIDR ブロック。
    - [トンネル内部 IP バージョン] で [IPv6] を指定した場合は、トンネル内部 IPv6 アドレスの `fd00::/8` 範囲から /126 の IPv6 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。
    - トンネルの詳細オプションを編集するには、[トンネルのオプションを編集する] を選択します。詳細については、「VPN トンネルオプション」を参照してください。

11. [Create VPN connection] (VPN 接続の作成) を選択します。VPN 接続の作成には数分かかる場合があります。

コマンドラインまたは API を使用して 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)

ステップ 6: 設定ファイルをダウンロードする

VPN 接続を作成した後、サンプル設定ファイルをダウンロードして、カスタマーゲートウェイデバイスを設定できます。

> **Important**
>
> 設定ファイルはほんの一例です。ユーザーの想定する VPN 接続設定とすべては一致しない場合があります。これは、ほとんどの AWS リージョンで AES128、SHA1、および Diffie-Hellman グループ 2、AWS GovCloud リージョンで AES128、SHA2、および Diffie-Hellman グループ 14 の VPN 接続の最小要件を指定します。また、認証用の事前共有キーも指定します。追加のセキュリティアルゴリズム、Diffie-Hellman グループ、プライベート証明書、IPv6 トラフィックを活用するには、サンプル設定ファイルを変更する必要があります。多くの一般的なカスタマーゲートウェイデバイスの設定ファイルに IKEv2 サポートが導入されており、時間の経過とともにファイルを追加していきます。IKEv2 をサポートする設定ファイルのリストは、「カスタマーゲートウェイデバイス」を参照してください。

許可

AWS Management Console から [設定のダウンロード] 画面を正しくロードするには、IAM ロールまたはユーザーが Amazon EC2 API、`GetVpnConnectionDeviceTypes` および `GetVpnConnectionDeviceSampleConfiguration` に対する許可を持っていることを確認する必要があります。

コンソールを使用して設定ファイルをダウンロードするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. VPN 接続を選択してから、[設定をダウンロード] を選択します。
4. カスタマーゲートウェイデバイスに対応する [ベンダー]、[プラットフォーム]、[ソフトウェア] および [IKE バージョン] を選択します。デバイスが一覧にない場合は、[Generic (汎用)] を選択します。
5. [Download] を選択します。

コマンドラインまたは API を使用して、サンプル設定ファイルをダウンロードするには

- GetVpnConnectionDeviceTypes (Amazon EC2 クエリ API)
- GetVpnConnectionDeviceSampleConfiguration (Amazon EC2 クエリ API)
- get-vpn-connection-device-types (AWS CLI)
- get-vpn-connection-device-sample-configuration (AWS CLI)

ステップ 7: カスタマーゲートウェイデバイスを設定する

サンプル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を設定します。カスタマーゲートウェイデバイスは、VPN 接続のお客様側の物理アプライアンスまたはソフトウェアアプライアンスです。詳細については、「カスタマーゲートウェイデバイス」を参照してください。

Site-to-Site VPN アーキテクチャ

Site-to-Site VPN の一般的なアーキテクチャは以下のとおりです。

- the section called “単一および複数の VPN 接続”
- the section called “冗長 VPN 接続”
- the section called “AWS VPN CloudHub”

Site-to-Site VPN 単一および複数の VPN 接続の例

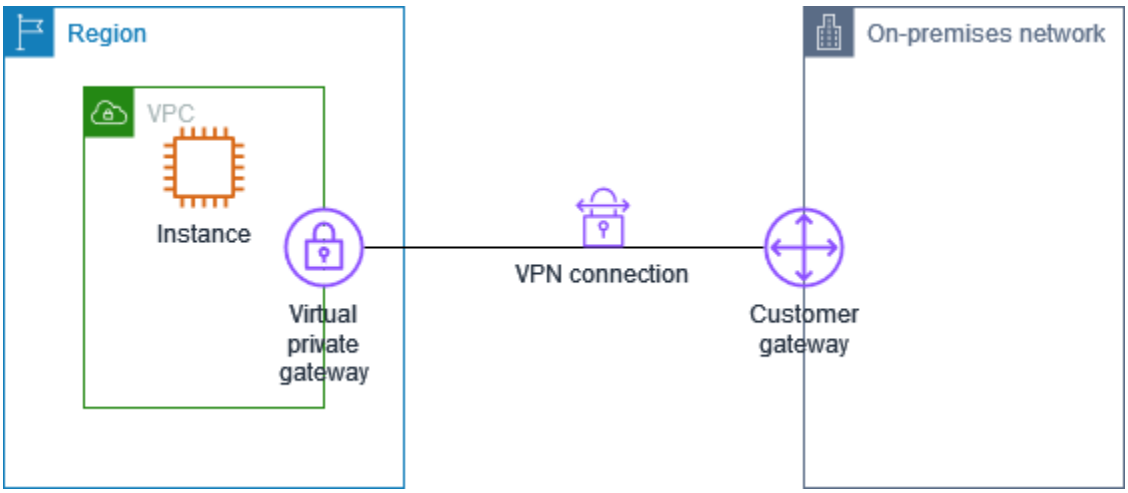
次の図に単一および複数の Site-to-Site VPN 接続を示します。

例

- 単一の Site-to-Site VPN 接続
- トランジットゲートウェイを使用した単一の 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使用した複数の Site-to-Site VPN 接続
- AWS Direct Connect との Site-to-Site VPN 接続
- AWS Direct Connect とのプライベート IP Site-to-Site VPN 接続

単一の Site-to-Site VPN 接続

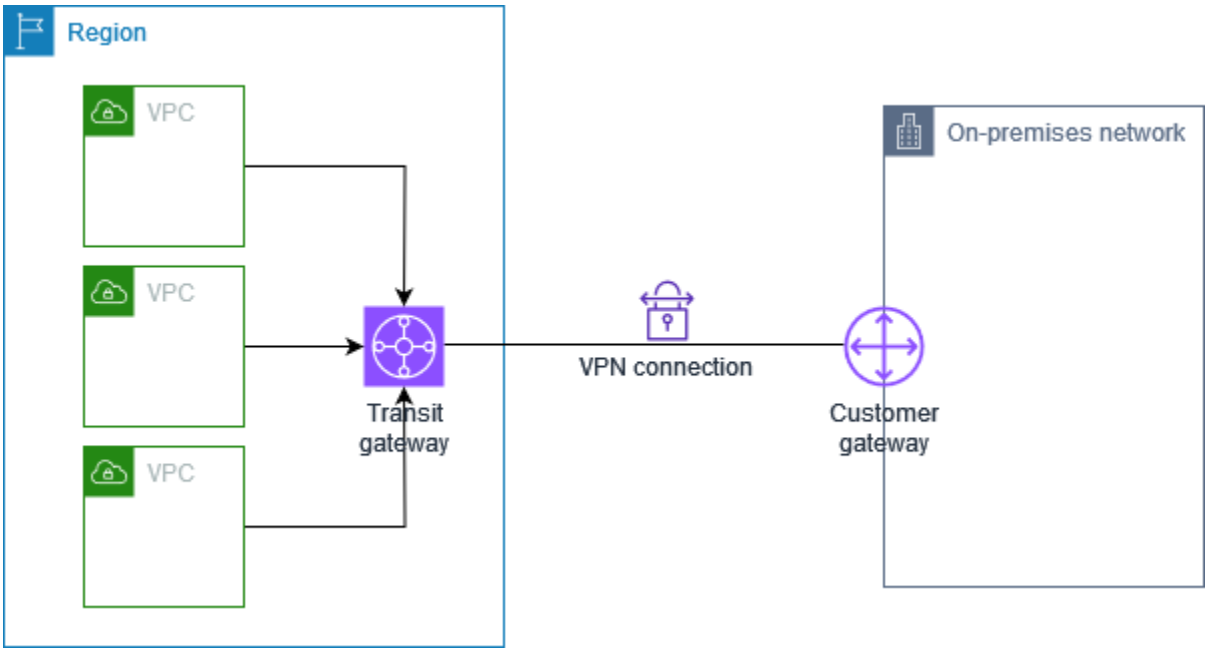
VPC には仮想プライベートゲートウェイが関連付けられていて、オンプレミス (リモート) ネットワークにはカスタマーゲートウェイが使用されています。カスタマーゲートウェイデバイスは、VPN 接続を有効にするように設定する必要があります。VPC ルートテーブルを更新して、VPC からユーザーネットワークに向けてのトラフィックが仮想プライベートゲートウェイに流れるようにします。



このシナリオを設定するステップについては、「AWS Site-to-Site VPN の開始方法」を参照してください。

トランジットゲートウェイを使用した単一の Site-to-Site VPN 接続

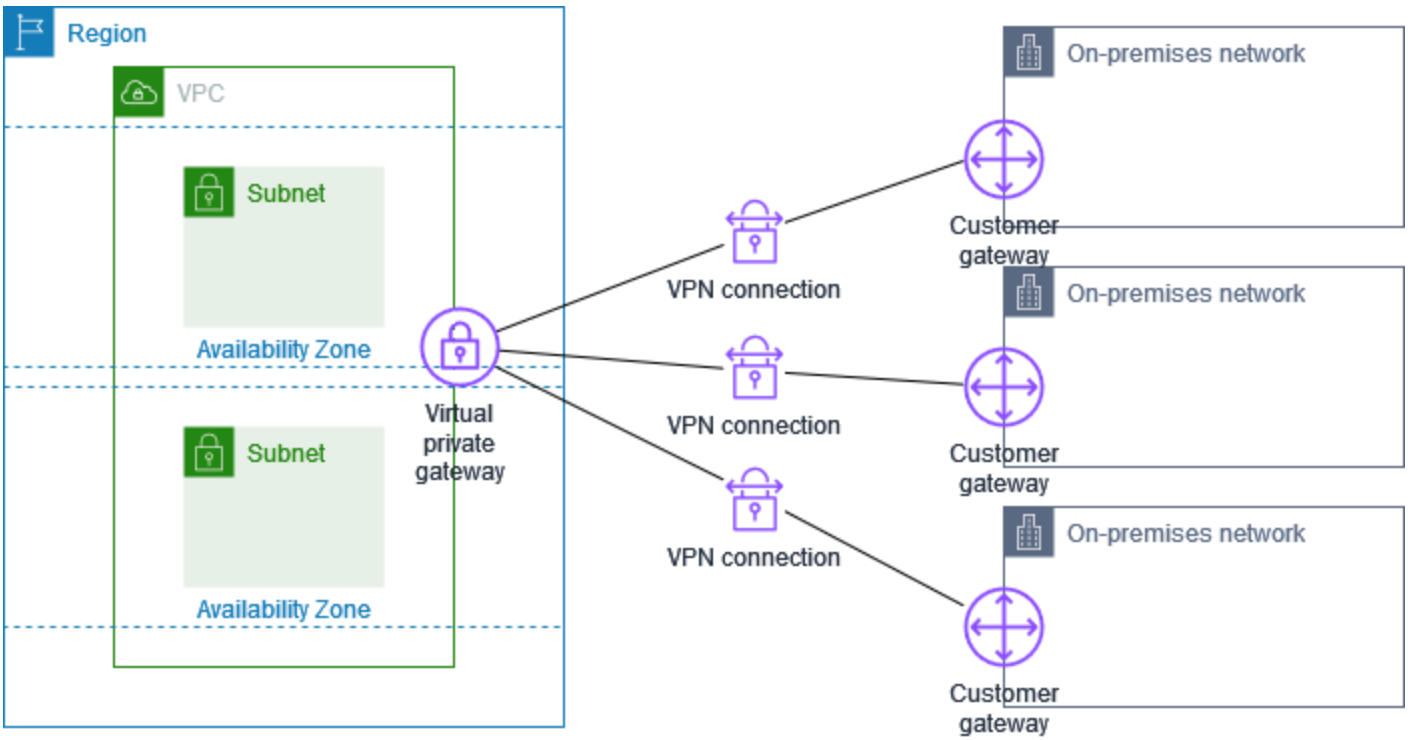
VPC にはトランジットゲートウェイがアタッチされていて、オンプレミス (リモート) ネットワークにはカスタマーゲートウェイデバイスが使用されています。カスタマーゲートウェイデバイスは、VPN 接続を有効にするように設定する必要があります。VPC ルートテーブルを更新して、VPC からユーザーネットワークに向けてのトラフィックがトランジットゲートウェイに流れるようにする必要があります。



このシナリオを設定するステップについては、「AWS Site-to-Site VPN の開始方法」を参照してください。

複数の Site-to-Site VPN 接続

VPC には仮想プライベートゲートウェイがアタッチされていて、複数のオンプレミスの場所への複数の Site-to-Site VPN 接続があります。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。

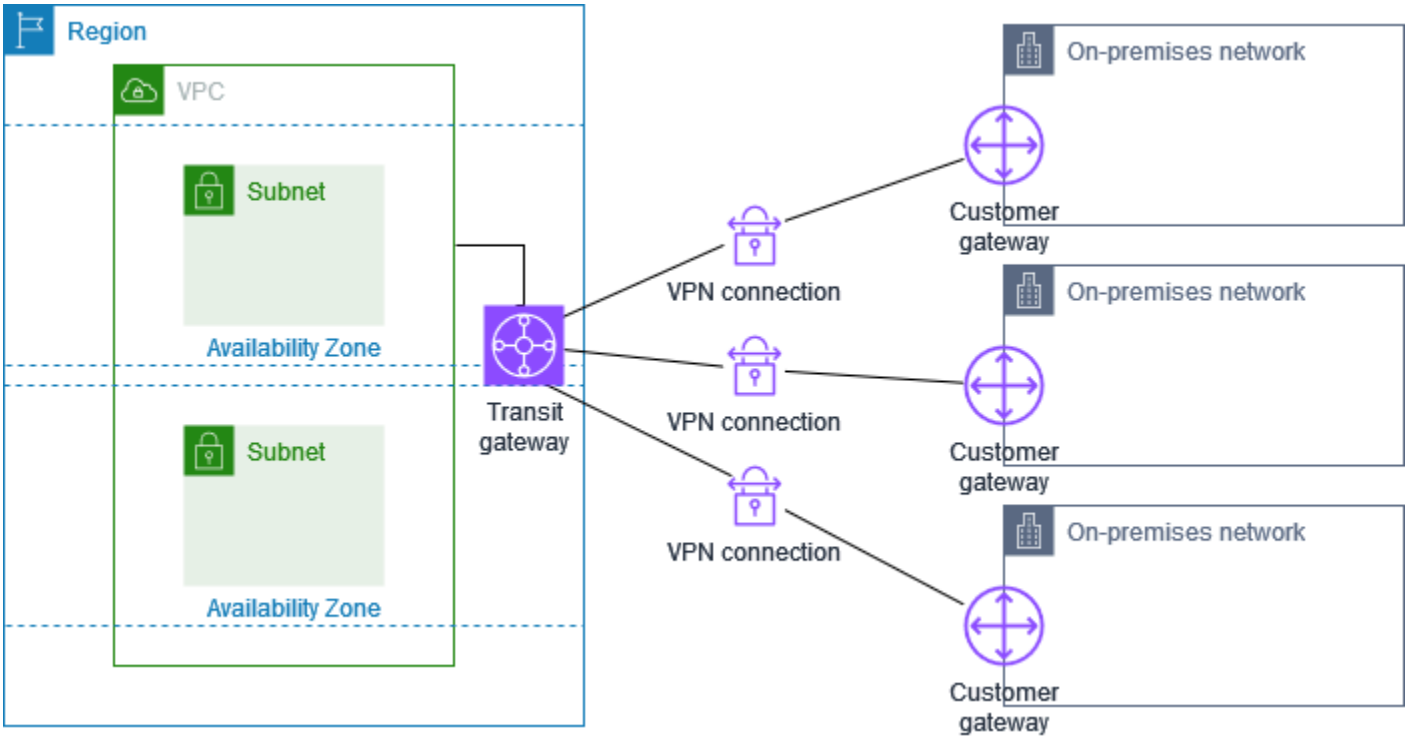


単一の VPC に対して複数の Site-to-Site VPN 接続を作成する場合、2 番目のカスタマーゲートウェイを設定して、外部にある同一の場所への冗長な接続を作成できます。詳細については、「冗長な Site-to-Site VPN 接続を使用してフェイルオーバーを提供する」を参照してください。

このシナリオを使用して、複数の地理的位置への Site-to-Site VPN 接続を作成し、サイト間の安全な通信を提供することもできます。詳細については、「VPN CloudHub を使用して安全なサイト間通信を提供する」を参照してください。

トランジットゲートウェイを使用した複数の Site-to-Site VPN 接続

VPC にはトランジットゲートウェイがアタッチされていて、複数のオンプレミスの場所への複数の Site-to-Site VPN 接続があります。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トランジットゲートウェイにルーティングされるようにします。

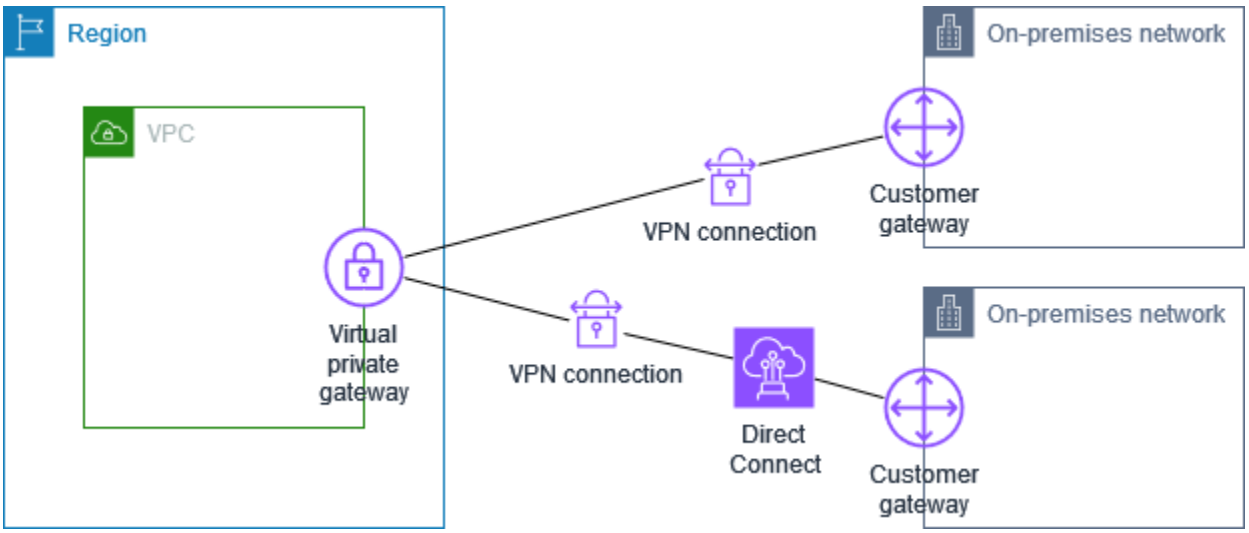


1 つのトランジットゲートウェイに対して複数の Site-to-Site VPN 接続を作成する場合、2 番目のカスタマーゲートウェイを設定して、外部にある同一の場所への冗長な接続を作成できます。

このシナリオを使用して、複数の地理的位置への Site-to-Site VPN 接続を作成し、サイト間の安全な通信を提供することもできます。

AWS Direct Connect との Site-to-Site VPN 接続

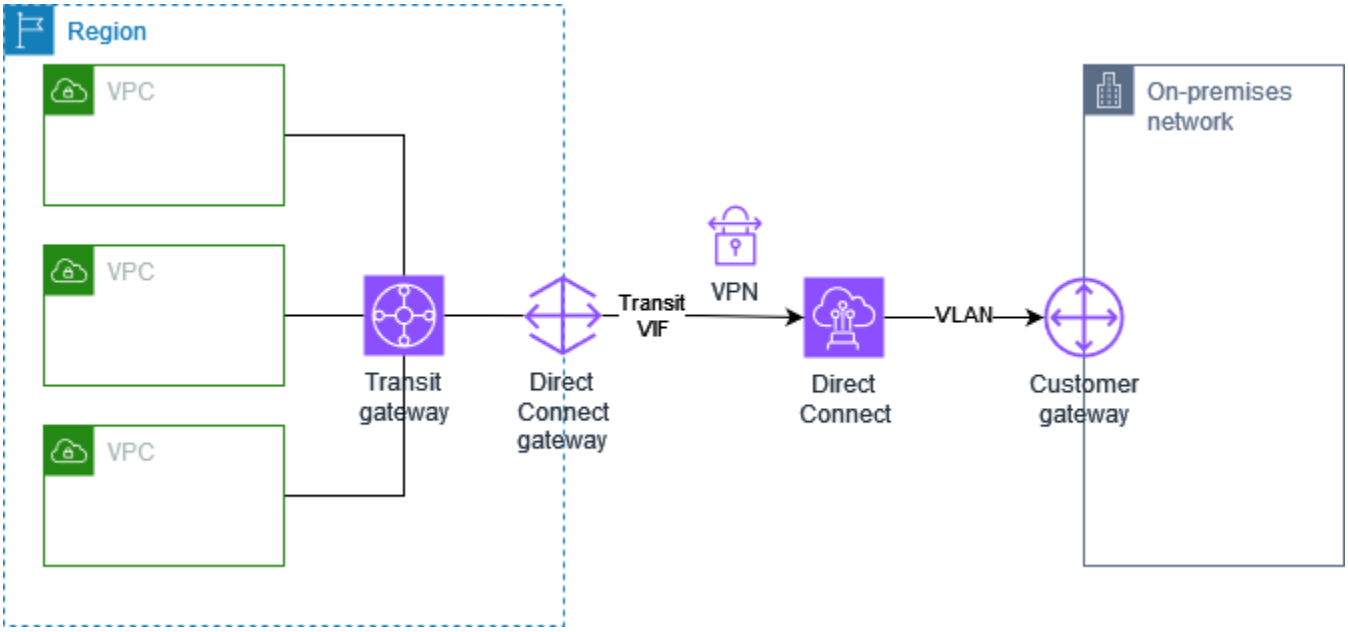
VPC には仮想プライベートゲートウェイがアタッチされており、AWS Direct Connect 経由でオンプレミス (リモート) ネットワークに接続します。AWS Direct Connect パブリック仮想インターフェイスを設定して、仮想プライベートゲートウェイを介してネットワークとパブリック AWS リソース間の専用ネットワーク接続を確立できます。VPC からのネットワークへのトラフィックが仮想プライベートゲートウェイと AWS Direct Connect 接続にルーティングされるように、ルーティングを設定します。



AWS Direct Connect と VPN 接続の両方が同じ仮想プライベートゲートウェイに設定されている場合、オブジェクトを追加または削除すると、仮想プライベートゲートウェイが「アタッチ中」状態になる場合があります。これは、中断とパケット損失を最小限に抑えるために、AWS Direct Connect と VPN 接続を切り替える内部ルーティングに変更が加えられようとしていることを示しています。これが完了すると、仮想プライベートゲートウェイは「アタッチ済み」状態に戻ります。

AWS Direct Connect とのプライベート IP Site-to-Site VPN 接続

プライベート IP Site-to-Site VPN を使用すると、パブリック IP アドレスを使用せずに、オンプレミスネットワークと AWS 間の AWS Direct Connect トラフィックを暗号化できます。AWS Direct Connect 経由のプライベート IP VPN は、AWS とオンプレミスネットワーク間のトラフィックを安全かつプライベートに確保し、お客様は規制およびセキュリティの義務を遵守できます。



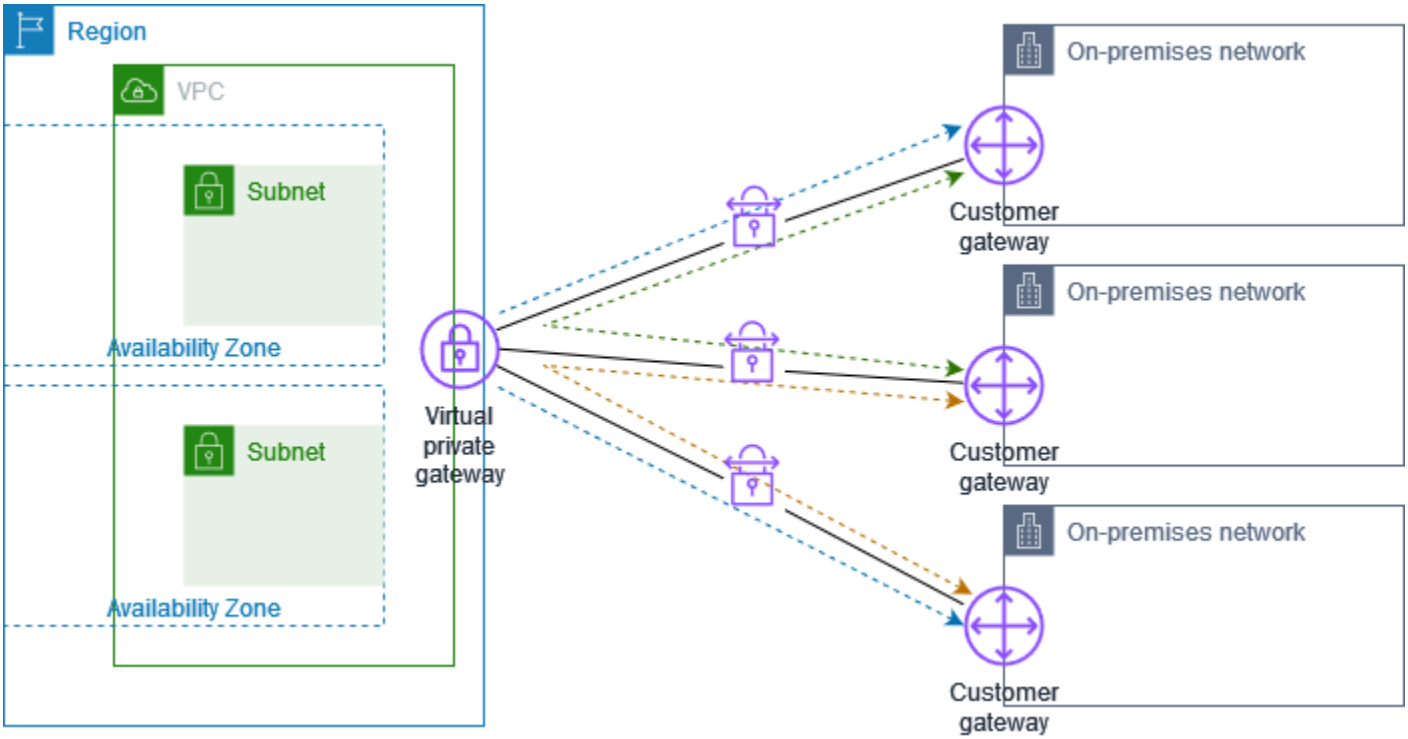
詳細については、ブログ記事「Introducing AWS Site-to-Site VPN Private IP VPNs」を参照してください。

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、サイトは VPC のリソースのみとではなく、相互に通信できます。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があり、これらのサイト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。

概要

VPN CloudHub アーキテクチャを次の図に示します。破線は、VPN 接続を介してルーティングされ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。サイト間で IP 範囲が重複することは許可されません。



このシナリオでは、次の操作を行います。

1. 単一の仮想プライベートゲートウェイを作成します。

2. ゲートウェイのパブリック IP アドレスを持つ複数のカスタマーゲートウェイを作成します。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。
3. 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に動的にルーティングされる Site-to-Site VPN 接続を作成します。
4. 仮想プライベートゲートウェイにサイト固有のプレフィックス (10.0.0.0/24、10.0.1.0/24 など) をアドバタイズするように、カスタマーゲートウェイデバイスを設定します。これらのルーティングアドバタイズメントが受信され、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。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。
5. サブネットルートテーブルのルートを設定して、VPC のインスタンスがサイトと通信できるようにします。詳細については、「(仮想プライベートゲートウェイ) ルートテーブルでルート伝播を有効にする」を参照してください。ルートテーブルに集約ルート (10.0.0.0/16 など) を設定できます。カスタマーゲートウェイデバイスと仮想プライベートゲートウェイ間により具体的なプレフィックスを使用します。

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。例えば、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。

料金

AWS VPN CloudHub を使用するには、一般的な 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の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 接続ごとに支払いが発生します (0.05 USD/時間の場合、合計 0.10 USD/時間)。各 Site-to-Site VPN 接続を通過するロサンゼルスからニューヨークへ (またはその逆に) 送信するすべてのデータについて、標準の AWS データ転送料金の支払いが発生します。仮想プライベートゲートウェイに Site-to-Site VPN 接続経由で送信されるネットワークトラフィックは無料ですが、仮想プライベートゲートウェイからエンドポ

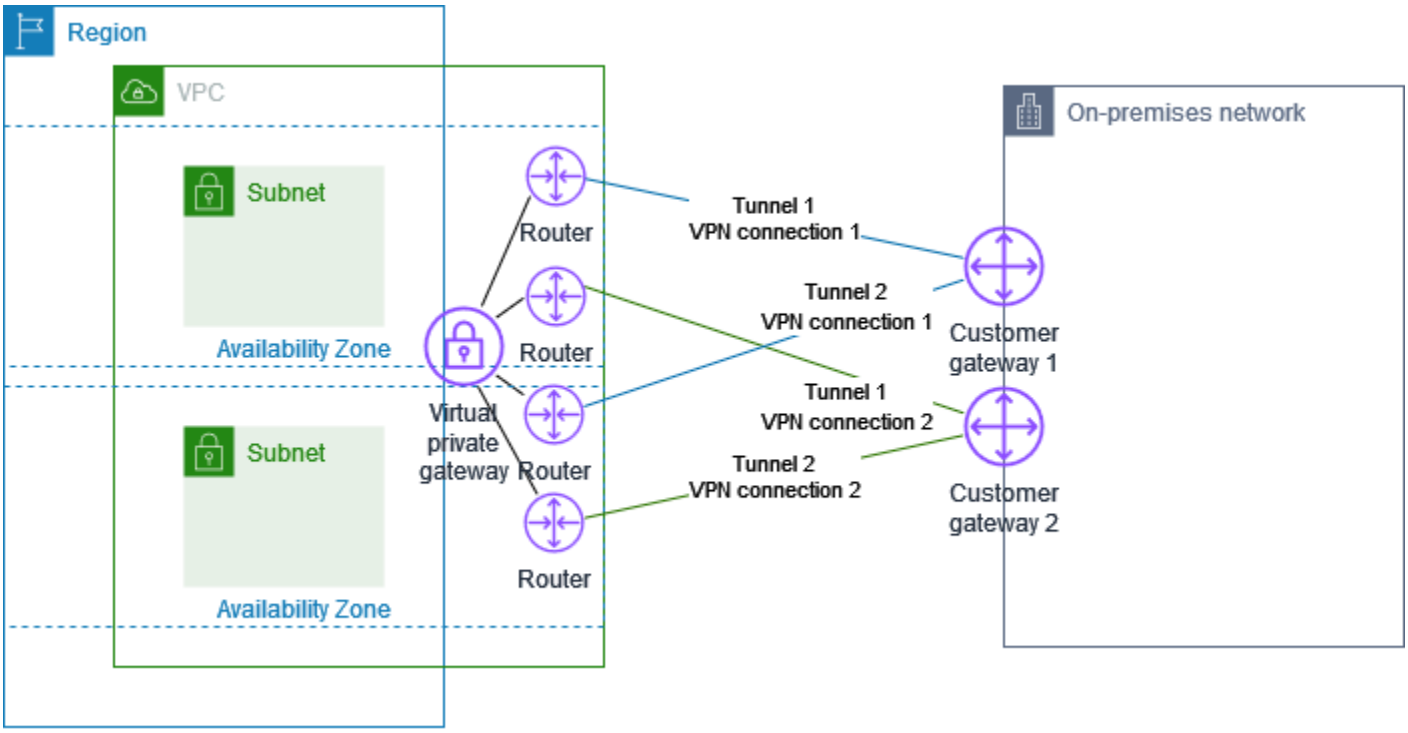
イントに Site-to-Site VPN 接続経由で送信されるネットワークトラフィックは、標準の AWS データ転送レートで課金されます。

詳細については、「Site-to-Site VPN 接続料金」を参照してください。

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

カスタマーゲートウェイデバイス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デバイスを追加して、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 VPN 接続とカスタマーゲートウェイデバイスを使用すれば、1 つのデバイスでメンテナンスを実行しながら、2 番目の 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。

2 つの VPN 接続は、以下の図のようになります。各 VPN 接続には、独自のトンネルと独自のカスタマーゲートウェイがあります。



このシナリオでは、次の操作を行います。

- 同じ仮想プライベートゲートウェイを使用し、新しいカスタマーゲートウェイを作成して、2 番目の Site-to-Site VPN 接続をセットアップします。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。

- 2 つ目のカスタマーゲートウェイデバイスを設定します。どちらのデバイスも、同じ IP 範囲を仮想プライベートゲートウェイにアドバタイズする必要があります。当社は BGP ルーティングを使用してトラフィックのパスを特定しています。1 つのカスタマーゲートウェイデバイスが失敗した場合、仮想プライベートゲートウェイが、すべてのトラフィックを動作中のカスタマーゲートウェイデバイスに送信します。

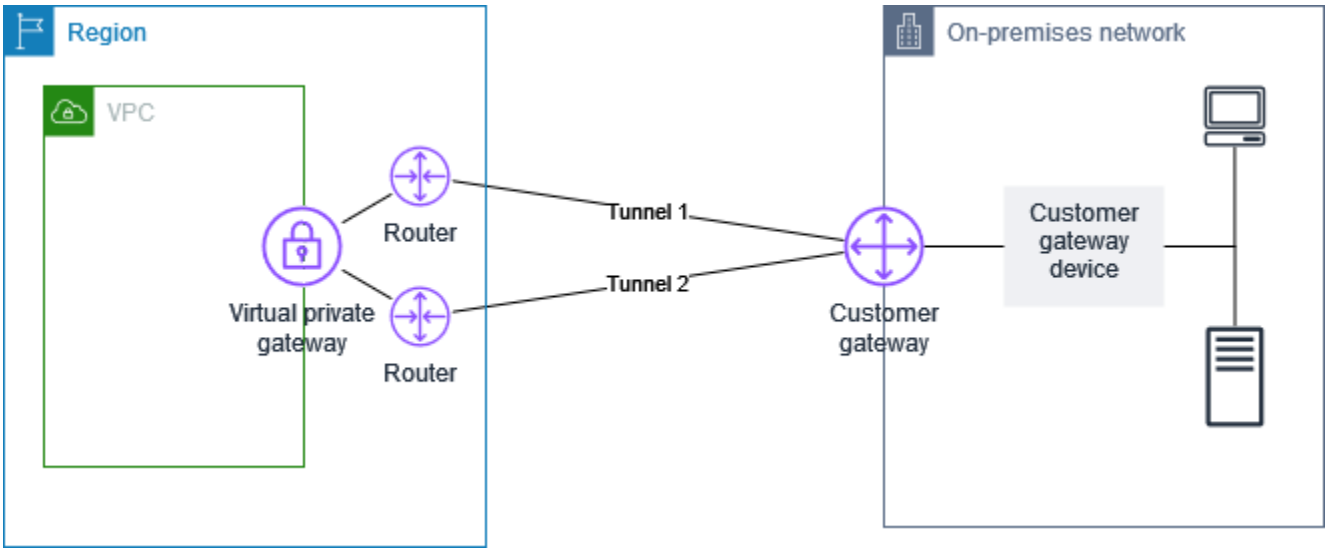
動的にルーティングされる Site-to-Site VPN 接続では、ボーダーゲートウェイプロトコル (BGP) を使用して、カスタマーゲートウェイと仮想プライベートゲートウェイ間で情報をルーティングします。静的にルーティングされる Site-to-Site VPN 接続では、カスタマーゲートウェイのユーザー側でリモートネットワークの静的ルートを入力する必要があります。BGP でアドバタイズされ、静的に入力されたルート情報によって、双方のゲートウェイで使用可能なトンネルが判別され、障害発生時にトラフィックが再ルーティングされます。BGP (使用可能な場合) で提供されるルーティング情報を使用し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。

カスタマーゲートウェイと Site-to-Site VPN 接続の作成および設定の詳細については、「AWS Site-to-Site VPN の開始方法」を参照してください。

カスタマーゲートウェイデバイス

カスタマーゲートウェイデバイスは、オンプレミスネットワーク (Site-to-Site VPN 接続のユーザー側) で所有または管理している物理アプライアンスまたはソフトウェアアプライアンスです。ユーザーまたはネットワーク管理者は、Site-to-Site VPN 接続で動作するようにデバイスを設定する必要があります。

次の図は、ネットワーク、カスタマーゲートウェイデバイス、および 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への VPN 接続を示しています。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の 2 つの線は、VPN 接続のトンネルを表しています。内でデバイス障害が発生した場合 AWS、VPN 接続は自動的に 2 番目のトンネルにフェイルオーバーするため、アクセスが中断されることはありません。は VPN 接続の定期メンテナンス AWS も実行するため、VPN 接続の 2 つのトンネルのうち 1 つが一時的に無効になる場合があります。詳細については、「Site-to-Site VPN トンネルエンドポイントの置換」を参照してください。したがって、カスタマーゲートウェイデバイスを設定するときは、両方のトンネルを使用するように設定することが重要です。



VPN 接続を設定するステップについては、「AWS Site-to-Site VPN の開始方法」を参照してください。このプロセスでは、 でカスタマーゲートウェイリソースを作成します。このリソースは AWS、デバイスのパブリック IP アドレスなど、デバイス AWS に関する情報を に提供します。詳細については、「Site-to-Site VPN 接続のカスタマーゲートウェイオプション」を参照してください。のカスタマーゲートウェイリソース AWS は、カスタマーゲートウェイデバイスを設定または作成しません。このデバイスは、自分で設定する必要があります。

AWS Marketplace でソフトウェア VPN アプライアンスを検索することもできます。

トピック

設定ファイルの例

VPN 接続を作成すると、Amazon VPC コンソールから、または EC2 API を使用して、 AWS が提供するサンプル設定ファイルをダウンロードするオプションが追加されます。詳細については、「ステップ 6: 設定ファイルをダウンロードする」を参照してください。静的ルーティングと動的ルーティング専用のサンプル設定の.zip ファイルをダウンロードすることもできます。

.zip ファイルをダウンロード

- 静的設定: the section called “設定ファイルの例”
- 動的設定: the section called “設定ファイルの例”

AWSが提供するサンプル設定ファイルには、カスタマーゲートウェイデバイスの設定に使用できる VPN 接続に固有の情報が含まれています。場合によっては、AWS でテスト済みのデバイス用に、デバイス固有の設定ファイルが用意されています。特定のカスタマーゲートウェイデバイスが一覧に表示されていない場合は、汎用設定ファイルをダウンロードして開始できます。

> **Important**
>
> この設定ファイルはあくまでも一例です。お客様が想定する Site-to-Site VPN 接続設定とは一致しない場合があります。ほとんどのリージョンでは AES128, SHA1、および Diffie-Hellman グループ 2、 AWS リージョンでは AES128, SHA2、および Diffie-Hellman グループ 14 の Site-to-Site VPN 接続の最小要件を指定します AWS GovCloud 。また、認証用の事

前共有キーも指定します。追加のセキュリティアルゴリズム、Diffie-Hellman グループ、プライベート証明書、IPv6 トラフィックを活用するには、サンプル設定ファイルを変更する必要があります。

> **Note**
>
> これらのデバイス固有の設定ファイルは、ベストエフォートベース AWS で によって提供されます。によってテストされていますが AWS、このテストは制限されています。設定ファイルに問題がある場合は、特定のベンダーに問い合わせて、追加のサポートを依頼する必要があります。

次の表に、IKEv2 をサポートするように更新された、ダウンロード可能な設定ファイルの例があるデバイスのリストを示します。多くの一般的なカスタマーゲートウェイデバイスの設定ファイルに IKEv2 サポートが導入されており、時間の経過とともにファイルを追加していきます。このリストは、設定ファイルの例が追加されると更新されます。

Vendor	プラットフォーム	ソフトウェア
Checkpoint	Gaia	R80.10+
Cisco Meraki	MX シリーズ	15.12+ (WebUI)
Cisco Systems, Inc。	ASA 5500 シリーズ	ASA 9.7+ VTI
Cisco Systems, Inc。	CSRv AMI	IOS 12.4 以降
Fortinet	FortiGate 40+ シリーズ	FortiOS 6.4.4+ (GUI)
Juniper Networks, Inc。	J シリーズルーター	JunOS 9.5 以降
Juniper Networks, Inc。	SRX ルーター	JunOS 11.0 以降
Mikrotik	RouterOS	6.44.3
Palo Alto Networks	PA シリーズ	PANOS 7.0 以降
SonicWall	NSA、TZ	OS 6.5

Vendor	プラットフォーム	ソフトウェア
Sophos	Sophos ファイアウォール	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	RTX ルーター	Rev.10.01.16 以降

カスタマーゲートウェイデバイスの要件

上記の例の一覧にないデバイスを使用している場合、このセクションでは、デバイスを使用して Site-to-Site VPN 接続を確立するために必要なデバイスの要件について説明します。

カスタマーゲートウェイデバイスの設定には、4 つの主要部分があります。次の記号は、構成の各部分を表しています。

IKE	インターネットキー交換 (IKE) セキュリティアソシエーション。IPsec セキュリティアソシエーションを確立するために使用されるキーの交換に必要です。
IPsec	IPsec セキュリティアソシエーション。これは、トンネルの暗号化、認証などを処理します。
Tunnel	トンネルインターフェイス。トンネルを通じて送受信されるトラフィックを受け取ります。
BGP	(オプション) Border Gateway Protocol (BGP) ピア接続。BGP を使用するデバイスの場合、カスタマーゲートウェイデバイスと仮想プライベートゲートウェイ間でルートを交換します。

次の表は、カスタマーゲートウェイデバイスの要件、関連する RFC (参照用)、および要件に関するコメントの一覧です。

各 VPN 接続は 2 つの個別のトンネルで構成されています。各トンネルには、IKE セキュリティアソシエーション、IPsec セキュリティアソシエーション、および BGP ピア接続が含まれています。トンネルごとに 1 つの一意のセキュリティアソシエーション (SA) ペア (受信用に 1 つと送信用に 1 つ) に制限されるため、2 つのトンネルで合計 2 つの一意の SA ペア (4 つの SA) になります。一部のデバイスは、ポリシーベースの VPN を使用して、ACL エントリと同数の SA を作成します。そのた

め、不要なトラフィックを許可しないように、ルールを統合してからフィルタリングする必要がある場合があります。

デフォルトでは、トラフィックが生成され、VPN 接続のユーザー側から IKE ネゴシエーションが開始されると、VPN トンネルが開始されます。代わりに VPN 接続を設定して、接続の AWS 側から IKE ネゴシエーションを開始できます。詳細については、「Site-to-Site VPN トンネル開始オプション」を参照してください。

VPN エンドポイントはキー再生成をサポートしており、カスタマーゲートウェイデバイスが再ネゴシエーショントラフィックを送信しなくなってフェーズ 1 の期限が切れそうになると、再ネゴシエーションを開始できます。

要件	RFC	コメント
IKE セキュリティアソシエーションを確立する IKE	RFC 2409 RFC 7296	IKE セキュリティアソシエーションは、事前共有キーまたは認証子 AWS Private Certificate Authority としてを使用するプライベート証明書を使用して、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デバイス間で最初に確立されます。IKE は確立されると、一時キーをネゴシエートして今後の IKE メッセージを保護します。暗号化パラメータや認証パラメータなど、パラメータ間で完全な合意が必要です。 で VPN 接続を作成するときに AWS、トンネルごとに独自の事前共有キーを指定するか、 で AWS 生成できます。または、 AWS Private Certificate Authority を使用してカスタマーゲートウェイデバイスに使用するプライベート証明書を指定することもできます。VPN トンネルの設定の詳細については、「Site-to-Site VPN 接続のトンネルオプション」を参照してください。 IKEv1 および IKEv2 バージョンがサポートされています。 メインモードは IKEv1 でのみサポートされています。 Site-to-Site VPN サービスは、ルートベースのソリューションです。ポリシーベースの設定を使用する

要件	RFC	コメント
		場合は、設定を 1 つのセキュリティアソシエーション (SA) に制限する必要があります。
トンネルモードで IPsec セキュリティアソシエーションを確立する IPsec	RFC 4301	IKE の一時キーを使用すると、IPsec セキュリティアソシエーション (SA) を形成するために、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デバイス間でキーが確立されます。この SA を使用して、ゲートウェイ間のトラフィックの暗号化および暗号化の解除を行います。IPsec SA 内のトラフィックの暗号化に使用される一時キーは、通信の機密性を確保するために、定期的なローテーションで IKE によって自動的に変更されます。
AES 128 ビット暗号化または AES 256 ビット暗号化関数を使用する	RFC 3602	この暗号化機能は、IKE と IPsec の両方のセキュリティアソシエーションでプライバシーを確保するために使用されます。
SHA-1 または SHA-2 (256) ハッシュ関数を使用する	RFC 2404	このハッシュ関数は、IKE と IPsec の両方のセキュリティアソシエーションを認証するために使用されます。
Diffie-Hellman Perfect Forward Secrecy を使用する。	RFC 2409	IKE は、カスタマーゲートウェイデバイスと仮想プライベートゲートウェイ間のすべての通信を保護するために、Diffie-Hellman を使用して一時キーを確立します。 以下のグループがサポートされます。 • フェーズ 1 グループ: 2、14 ~ 24 • フェーズ 2 グループ: 2、5、14 ~ 24

要件	RFC	コメント
(動的にルーティングされた VPN 接続) IPsec Dead Peer Detection を使用する	RFC 3706	Dead Peer Detection を使用すると、VPN デバイスは、ネットワークの状態によりインターネットでのパケット配信が妨げられていることをすばやく特定できます。この場合、ゲートウェイはセキュリティアソシエーションを削除し、新しいアソシエーションを作成しようとします。このプロセス中、可能であれば、代わりの IPsec トンネルが使用されます。
(動的にルーティングされた VPN 接続) トンネルを論理インターフェイスにバインドする (ルートベースの VPN) Tunnel	なし	デバイスは、IPsec トンネルを論理インターフェイスにバインドできる必要があります。論理インターフェイスには、仮想プライベートゲートウェイへの BGP ピア接続を確立するために使用される IP アドレスが含まれています。この論理インターフェイスは、追加のカプセル化 (たとえば、GRE、IP in IP) を実行しないでください。インターフェイスは、1399 バイトの最大送信単位 (MTU) に設定する必要があります。
(動的にルーティングされた VPN 接続) BGP ピア接続を確立する BGP	RFC 4271	BGP は、カスタマーゲートウェイデバイスと BGP を使用するデバイスの仮想プライベートゲートウェイ間でルートを交換するために使用されます。すべての BGP トラフィックは、IPsec Security Association を通じて暗号化され、送信されます。BGP は、両方のゲートウェイが IPsec SA を通じて到達可能な IP プレフィックスを交換するために必要です。

AWS VPN 接続はパス MTU 検出 (RFC 1191) をサポートしていません。

カスタマーゲートウェイデバイスとインターネット間にファイアウォールがある場合は、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照してください。

カスタマーゲートウェイデバイスのベストプラクティス

パケットの [フラグメント化しない] フラグをリセットする

一部のパケットには、フラグメント化しない (DF) と呼ばれるフラグがあり、パケットがフラグメント化されないように指示することができます。パケットにフラグが設定されていれば、ゲートウェイは ICMP Path MTU Exceeded メッセージを生成します。場合によっては、これらの ICMP メッセージを処理し、各パケットで送信されるデータの量を削減するための適切な仕組みがアプリケーションに備わっていません。一部の VPN デバイスでは、必要に応じて DF フラグをオーバーライドし、無条件でパケットをフラグメント化できます。カスタマーゲートウェイデバイスにこの機能がある場合は、必要に応じてこの機能を使用することをお勧めします。詳細については「RFC 791」を参照してください。

暗号化前に IP パケットをフラグメント化する

Site-to-Site VPN 接続を介して に送信されるパケットが MTU サイズを超える場合は、フラグメント化する必要があります。パフォーマンスの低下を避けるため、暗号化する前にパケットをフラグメント化するようにカスタマーゲートウェイデバイスを設定することをお勧めします。Site-to-Site VPN は、フラグメント化されたパケットを次の宛先に転送する前に再アセンブルし、 AWS ネットワークを通過する packet-per-second フローを増やします。詳細については「RFC 4459」を参照してください。

パケットサイズが送信先ネットワークの MTU を超えないようにする

Site-to-Site VPN は、カスタマーゲートウェイデバイスから受信したフラグメント化されたパケットを次の宛先に転送する前に再アセンブルするため、 など、送信先ネットワークではパケットサイズ/MTU を考慮して、これらのパケットが次に転送される場合があります AWS Direct Connect。

使用中のアルゴリズムに従って MTU および MSS サイズを調整する

多くの場合、TCP パケットは IPsec トンネル間で最も一般的なタイプのパケットです。Site-to-Site VPN は 1446 バイトの最大伝送ユニット（MTU）と 1406 バイトの対応する最大セグメントサイズ（MSS）をサポートします。ただし、暗号化アルゴリズムにはさまざまなヘッダーサイズがあり、これらの最大値を達成できない可能性があります。フラグメンテーションを回避して最適なパフォーマンスを得るには、使用するアルゴリズムに基づいて MTU と MSS を設定することをお勧めします。

次の表を使用して、フラグメンテーションを回避し、最適なパフォーマンスを実現するように MTU/MSS を設定します。

暗号化アルゴリズム	ハッシュ生成アルゴリズム	NAT トラバーサル	MTU	MSS (IPv4)	MSS (IPv6-in-IPv4)
AES-GCM-16	該当なし	無効	1446	1406	1386

暗号化アルゴリズム	ハッシュ生成アルゴリズム	NAT トラバーサル	MTU	MSS (IPv4)	MSS (IPv6-in-IPv4)
AES-GCM-16	該当なし	有効	1438	1398	1378
AES-CBC	SHA1/SHA2-256	無効	1438	1398	1378
AES-CBC	SHA1/SHA2-256	有効	1422	1382	1362
AES-CBC	SHA2-384	無効	1422	1382	1362
AES-CBC	SHA2-384	有効	1422	1382	1362
AES-CBC	SHA2-512	無効	1422	1382	1362
AES-CBC	SHA2-512	有効	1406	1366	1346

> **Note**
>
> AES-GCM アルゴリズムは暗号化と認証の両方をカバーするため、MTU に影響する明確な認証アルゴリズムの選択はありません。

インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定

カスタマーゲートウェイデバイスを エンドポイントに接続する IPsec トンネルのエンドポイントとして使用する静的 IP アドレスが必要です。 AWS Site-to-Site VPN ファイアウォールが AWS とカスタマーゲートウェイデバイス間にある場合、IPsec トンネルを確立するには、次の表のルールを設定する必要があります。 AWS側の IP アドレスは設定ファイルにあります。

インバウンド (インターネットから)

入力ルール I1

[Source IP] (送信元 IP) Tunnel1 外部 IP

送信先 IP	カスタマーゲートウェイ
プロトコル	UDP
ソースポート	500
送信先	500
入力ルール I2	
[Source IP] (送信元 IP)	Tunnel2 外部 IP
送信先 IP	カスタマーゲートウェイ
プロトコル	UDP
ソースポート	500
発信先ポート	500
入力ルール I3	
[Source IP] (送信元 IP)	Tunnel1 外部 IP
送信先 IP	カスタマーゲートウェイ
プロトコル	IP 50 (ESP)
入力ルール I4	
[Source IP] (送信元 IP)	Tunnel2 外部 IP
送信先 IP	カスタマーゲートウェイ
プロトコル	IP 50 (ESP)

アウトバウンド (インターネットへ)

出力ルール O1	
[Source IP] (送信元 IP)	カスタマーゲートウェイ

送信先 IP	Tunnel1 外部 IP
プロトコル	UDP
ソースポート	500
発信先ポート	500
出カルール O2	
[Source IP] (送信元 IP)	カスタマーゲートウェイ
送信先 IP	Tunnel2 外部 IP
プロトコル	UDP
ソースポート	500
発信先ポート	500
出カルール O3	
[Source IP] (送信元 IP)	カスタマーゲートウェイ
送信先 IP	Tunnel1 外部 IP
プロトコル	IP 50 (ESP)
出カルール O4	
[Source IP] (送信元 IP)	カスタマーゲートウェイ
送信先 IP	Tunnel2 外部 IP
プロトコル	IP 50 (ESP)

ルール I1、I2、O1、および O2 は、IKE パケットの送信を有効にします。ルール I3、I4、O3、および O4 は、暗号化されたネットワークトラフィックを含む IPsec パケットの送信を有効にします。

> **Note**
>
> デバイスで NAT トラバーサル (NAT-T) を使用している場合は、ポート 4500 の UDP トラフィックもネットワークと AWS Site-to-Site VPN エンドポイント間で通過できることを確認してください。デバイスが NAT-T をアドバタイズしているかどうかを確認します。

複数の VPN 接続シナリオ

次に、1 つ以上のカスタマーゲートウェイデバイスを使用して複数の VPN 接続を作成するシナリオを示します。

同じカスタマーゲートウェイデバイスを使用した複数の VPN 接続

同じカスタマーゲートウェイデバイスを使用して、オンプレミスの場所から他の VPC に追加の VPN 接続を作成できます。それらの VPN 接続ごとに同じカスタマーゲートウェイ IP アドレスを再利用できます。

2 番目のカスタマーゲートウェイデバイスを使用した冗長 VPN 接続

カスタマーゲートウェイデバイス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デバイスを使用して、2 番目の VPN 接続を設定できます。詳細については、「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」を参照してください。1 つの場所に冗長なカスタマーゲートウェイデバイスを確立した場合は、両方のデバイスが同じ IP 範囲をアドバタイズする必要があります。

単一の仮想プライベートゲートウェイへの複数のカスタマーゲートウェイデバイス (AWS VPN CloudHub)

複数のカスタマーゲートウェイデバイスから。単一の仮想プライベートゲートウェイに対して、複数の VPN 接続を確立できます。これにより、複数の口ケーションを AWS VPN に接続できます CloudHub。詳細については、「VPN CloudHub を使用して安全なサイト間通信を提供する」を参照してください。複数の地理的口ケーションにカスタマーゲートウェイ工バイスがある場合、各デバイスは、口ケーションに固有の一意な IP 範囲のセットをアドバタイズする必要があります。

カスタマーゲートウェイデバイスのルーティング

AWS では、仮想プライベートゲートウェイのルーティングの決定に影響を与えるために、特定の BGP ルートをアドバタイズすることを推奨しています。お使いのデバイス特有のコマンドについては、ベンダーのマニュアルを参照してください。

複数の VPN 接続を作成すると、仮想プライベートゲートウェイは静的に割り当てられたルートを使用するか、BGP ルートアドバタイズを使用して、適切な VPN 接続にネットワークトラフィックを送信します。どちらのルートを使用するかは、VPN 接続がどのように設定されているかによって決まります。仮想プライベートゲートウェイに同一のルートが存在している場合は、BGP でアドバタイズされるルートよりも、静的に割り当てられたルートの方が適しています。BGP アドバタイズを使用するオプションを選択している場合は、静的ルートを指定できません。

ルーティングの優先度の詳細については、「ルートテーブルと VPN ルーティングの優先度」 を参照してください。

静的ルーティングのカスタマーゲートウェイデバイス設定の例

トピックス

設定ファイルの例

Site-to-Site VPN 接続設定に固有の値を含むサンプル設定ファイルをダウンロードするには、Amazon VPC コンソール、AWS コマンドラインまたは Amazon EC2 API を使用します。詳細については、「ステップ 6: 設定ファイルをダウンロードする」を参照してください。

また、Site-to-Site VPN 接続設定に固有の値を含まないスタティックルーティング用の汎用設定ファイルの例をダウンロードすることもできます。static-routing-examples.zip

これらのファイルは、一部のコンポーネントにプレースホルダー値を使用します。たとえば、以下を使用します。

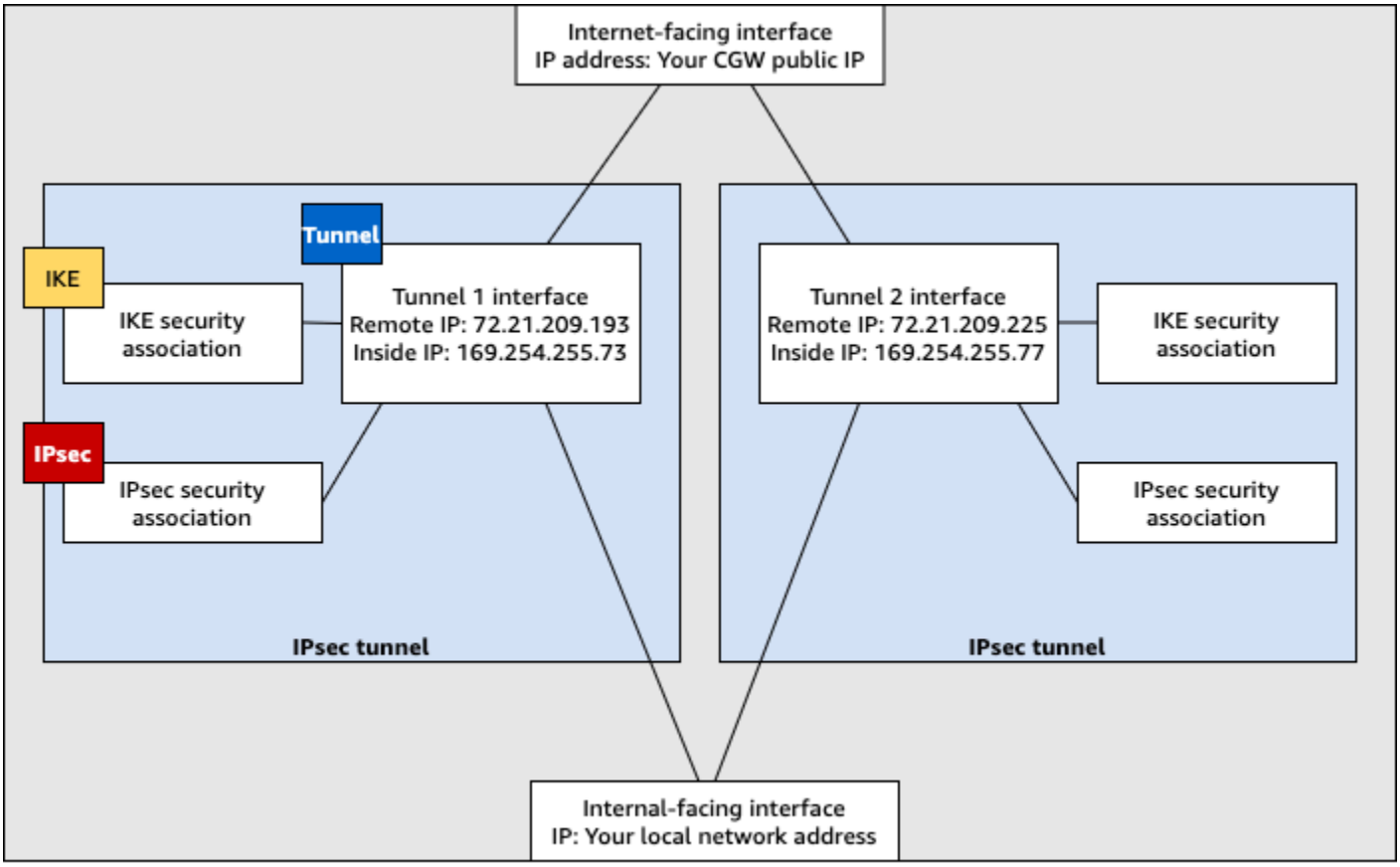
- VPN 接続 ID 、カスタマーゲートウェイ ID および仮想プライベートゲートウェイ ID の値の例
- リモート (外部) IP アドレス AWS エンドポイント (*AWS_ENDPOINT_1* および *AWS_ENDPOINT_2*) のプレースホルダー
- カスタマーゲートウェイデバイスのインターネットルーティング可能な外部インターフェイスの IP アドレスのプレースホルダー (*your-cgw-ip-address*)
- 事前共有キー値のプレースホルダ (事前共有キー)

- トンネルの内部 IP アドレスの値の例。
- MTU 設定の値の例。

> **Note**
>
> サンプルコンフィギュレーションファイルで提供されている MTU 設定は、例にすぎません。状況に応じた最適な MTU 値の設定については、「カスタマーゲートウェイデバイスのベストプラクティス」を参照してください。

このファイルは、プレースホルダー値を提供することに加えて、ほとんどの AWS リージョンで AES128、SHA1、および Diffie-Hellman グループ 2、および AWS GovCloud リージョンで AES128、SHA2、および Diffie-Hellman グループ 14 を指定します。また、認証用の事前共有キーも指定します。追加のセキュリティアルゴリズム、Diffie-Hellman グループ、プライベート証明書、IPv6 トラフィックを活用するには、サンプル設定ファイルを変更する必要があります。

次の図は、カスタマーゲートウェイデバイスに設定されているさまざまなコンポーネントの概要を示しています。これには、トンネルインターフェイスの IP アドレスの値の例が含まれます。



Customer gateway device

静的ルーティングのユーザーインターフェイス手順

以下は、ユーザーインターフェイス (使用可能な場合) を使用してカスタマーゲートウェイデバイスを設定する手順の例です。

Check Point

以下は、デバイスが R77.10 以降を実行する Check Point Security Gateway デバイスで、デバイスが Gaia オペレーティングシステムと Check Point SmartDashboard を使用している場合に、カスタマーゲートウェイデバイスを設定するステップです。Check Point Support Center の Check Point Security Gateway IPsec VPN to Amazon Web Services VPC の記事も参照できます。

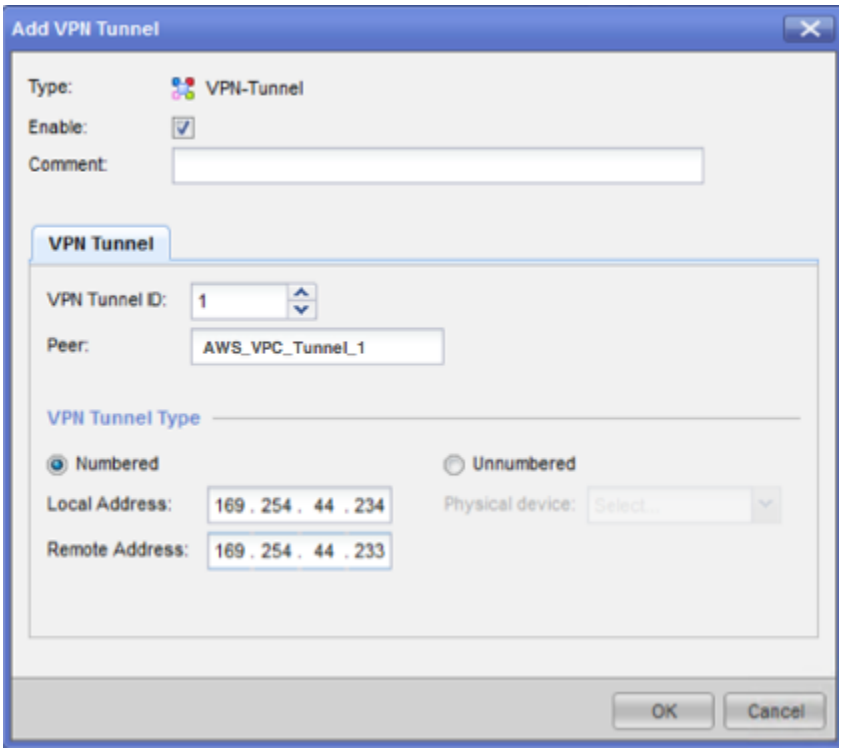
トンネルインターフェイスを設定するには

最初のステップは、VPN トンネルを作成し、各トンネル用の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プライベート (内部) IP アドレスを提供することです。最初のトンネルを作成するには、設定ファイルの `IPSec Tunnel #1` セクションで提供される情報を使用しま

す。2 番目のトンネルを作成するには、設定ファイルの IPSec Tunnel #2 セクションで提供される値を使用します。

1. Check Point Security Gateway デバイスの Gaia ポータルを開きます。
2. [Network Interfaces]、[Add]、[VPN tunnel] の順に選択します。
3. ダイアログボックスで次のように設定し、完了したら [OK] を選択します。

   - [VPN Tunnel ID] には、1 など一意の値を入力します。
   - [Peer] には、AWS_VPC_Tunnel_1 または AWS_VPC_Tunnel_2 など、トンネル用の一意の名前を入力します。
   - [Numbered] が選択されていることを確認して、[Local Address (ローカルアドレス)] に設定ファイルの CGW Tunnel IP で指定されている IP アドレス (例: 169.254.44.234) を入力します。
   - [Remote Address] には、設定ファイルの VGW Tunnel IP に指定された IP アドレス (例: 169.254.44.233) を入力します。



4. SSH でセキュリティゲートウェイに接続します。デフォルト以外のシェルを使用している場合は、次のコマンドを実行して、clish に変更します。clish
5. トンネル 1 の場合は、次のコマンドを実行します。

```
set interface vpnt1 mtu 1436
```

トンネル 2 の場合は、次のコマンドを実行します。

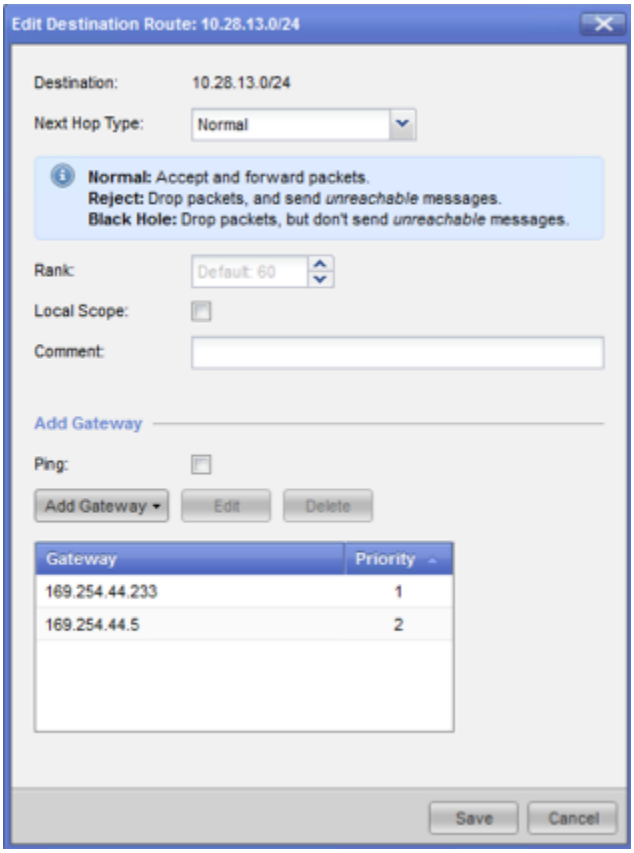
```
set interface vpnt2 mtu 1436
```

6. 2 番目のトンネルを作成するには、設定ファイルの IPSec Tunnel #2 セクション内の情報を使用して、ステップを繰り返します。

静的ルートを設定するには

このステップでは、各トンネルで VPC のサブネットへの静的ルートを指定し、トラフィックをトンネルインターフェイス経由で送信できるようにします。2 番目のトンネルにより、最初のトンネルに問題がある場合のフェイルオーバーが可能になります。問題が検出されると、ポリシーベースの静的ルートがルーティングテーブルから削除され、2 番目のルートが有効化されます。また、トンネルのもう一方の端に ping を打ち、トンネルが稼働しているかどうかを確認するために、Check Point ゲートウェイを有効にする必要があります。

1. Gaia ポータルで、[IPv4 Static Routes]、[Add] の順に選択します。
2. サブネットの CIDR (例: 10.28.13.0/24) を指定します。
3. [Add Gateway]、[IP Address] の順に選択します。
4. 設定ファイルの VGW Tunnel IP に指定された IP アドレス (例: 169.254.44.233) を入力し、優先順位を 1 にします。
5. [Ping] を選択します。
6. 2 つめのトンネルに対して、設定ファイルの VGW Tunnel IP セクションにある IPSec Tunnel #2 の値を使用してステップ 3 および 4 を繰り返します。優先順位を 2 にします。



7. [Save] を選択します。

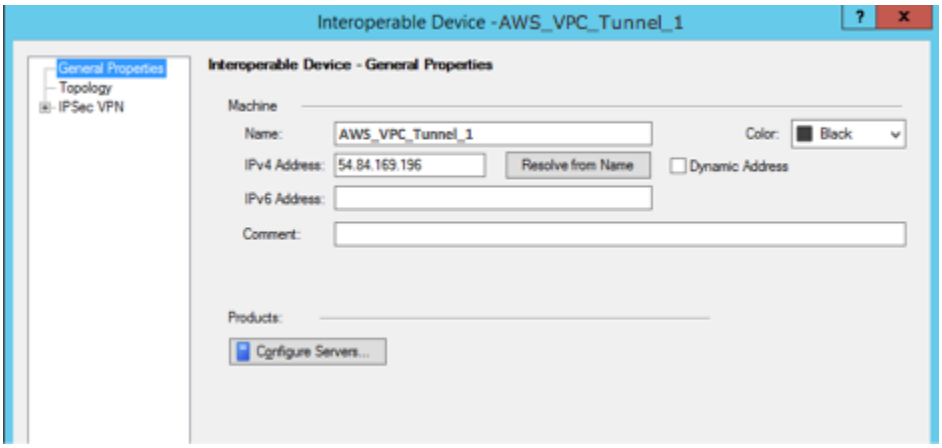
クラスターを使用している場合は、クラスターの他のメンバーで上記のステップを繰り返します。

新しいネットワークオブジェクトを定義するには

このステップでは、仮想プライベートゲートウェイのパブリック (外部) IP アドレスを指定することで各 VPN トンネル用のネットワークオブジェクトを作成します。後で、VPN コミュニティのサテライトゲートウェイとしてこれらのオブジェクトを追加します。また、VPN ドメインのプレースホルダーとして機能する空グループを作成する必要があります。

1. Check Point SmartDashboard を開きます。
2. [Groups] では、コンテキストメニューを開き、[Groups]、[Simple Group] の順に選択します。各ネットワークオブジェクトに対して同じグループを使用できます。
3. [Network Objects] では、コンテキストメニュー (右クリック) を開き、[New]、[Interoperable Device] の順に選択します。

4. [Name (名前)] には、トンネル用に指定した名前 (例: `AWS_VPC_Tunnel_1` または `AWS_VPC_Tunnel_2`) を入力します。
5. [IPv4 Address] には、設定ファイルで提供される仮想プライベートゲートウェイの外部 IP アドレス (例: `54.84.169.196`) を入力します。設定を保存して、このダイアログボックスを閉じます。



6. SmartDashboard でゲートウェイのプロパティを開き、カテゴリーペインで [Topology] を選択します。
7. インターフェイス設定を取得するには、[Get Topology] を選択します。
8. [VPN Domain (VPN ドメイン)] セクションで、[Manually defined (手動で定義)] を選択し、ステップ 2 で作成した空のシンプルなグループを参照して選択します。[OK] をクリックします。

> **Note**
>
> 設定済みの既存の VPN ドメインは保持できます。ただし、特に VPN ドメインが自動的に取得されている場合は、新しい VPN 接続で使用または提供されるドメインとホストがその VPN ドメインで宣言されていないことを確認してください。

9. 2 番目のネットワークオブジェクトを作成するには、設定ファイルの `IPSec Tunnel #2` セクション内の情報を使用して、ステップを繰り返します。

> **Note**
>
> クラスターを使用している場合は、トポロジーを編集してインターフェイスをクラスターインターフェイスとして定義します。設定ファイルで指定された IP アドレスを使用します。

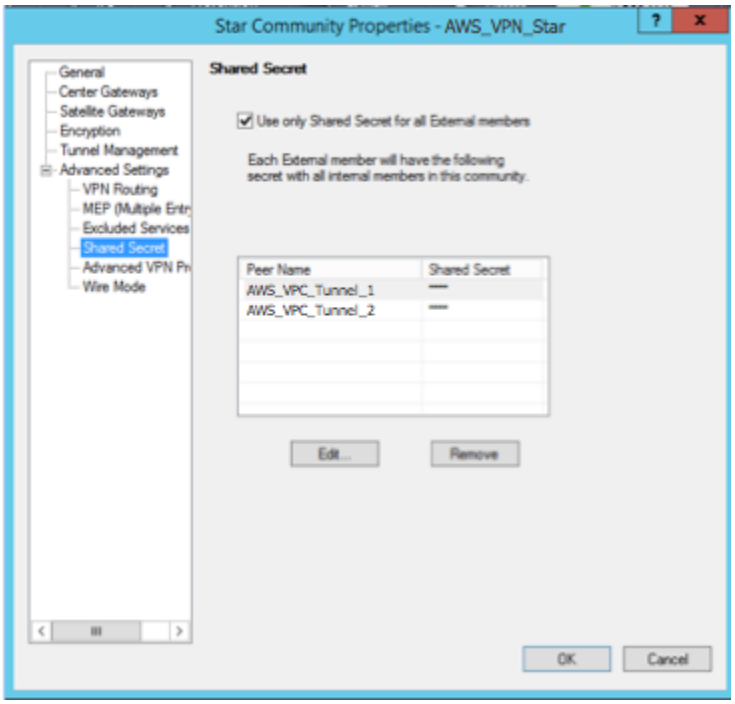
VPN コミュニティ、IKE、および IPsec 設定の作成と設定

このステップでは、Check Point ゲートウェイに VPN コミュニティを作成し、そこに各トンネルのネットワークオブジェクト (相互運用デバイス) を追加します。また、Internet Key Exchange (IKE) および IPsec を設定します。

1. ゲートウェイのプロパティから、カテゴリーペインの [IPSec VPN] を選択します。
2. [Communities]、[New]、[Star Community] の順に選択します。
3. コミュニティの名前 (例: `AWS_VPN_Star`) を指定し、カテゴリーペインの [Center Gateways] を選択します。
4. [Add] を選択して、ゲートウェイまたはクラスターを参加ゲートウェイのリストに追加します。
5. カテゴリーペインで、[Satellite Gateways]、[Add (追加)] の順に選択し、先に作成した相互運用デバイス (`AWS_VPC_Tunnel_1` および `AWS_VPC_Tunnel_2`) を参加ゲートウェイのリストに追加します。
6. カテゴリーペインで、[Encryption] を選択します。[Encryption Method] セクションで、[IKEv1 only] を選択します。[Encryption Suite] セクションで、[Custom]、[Custom Encryption] の順に選択します。
7. ダイアログボックスで次のように暗号化プロパティを設定し、完了したら [OK] を選択します。

   - IKE Security Association (フェーズ 1) のプロパティ
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Security Association (フェーズ 2) のプロパティ
     - Perform IPsec data encryption with: AES-128
     - Perform data integrity with: SHA-1

8. カテゴリーペインで [Tunnel Management] を選択します。[Set Permanent Tunnels]、[On all tunnels in the community] の順に選択します。[VPN Tunnel Sharing] セクションで、[One VPN tunnel per Gateway pair] を選択します。
9. カテゴリーペインで [Advanced Settings] を展開し、[Shared Secret] を選択します。
10. 最初のトンネルのピア名を選択し、[Edit (編集)] を選択して、設定ファイルの `IPSec Tunnel #1` セクションで指定されている事前共有キーを入力します。
11. 2 番目のトンネルのピア名を選択し、[Edit (編集)] を選択して、設定ファイルの `IPSec Tunnel #2` セクションで指定されている事前共有キーを入力します。



12. さらに [Advanced Settings (詳細設定)] カテゴリで [Advanced VPN Properties (詳細な VPN プロパティ)] を選択し、プロパティを次のように設定して、完了したら [OK] を選択します。
    - IKE (フェーズ 1):
        - Use Diffie-Hellman group: `Group 2`
        - Renegotiate IKE security associations every `480` minutes
    - IPsec (フェーズ 2):
        - [Use Perfect Forward Secrecy] を選択します。
        - Use Diffie-Hellman group: `Group 2`
        - Renegotiate IPsec security associations every `3600` seconds

ファイアウォールルールを作成するには

このステップでは、ファイアウォールルールとディレクショナルマッチルールを使用し、VPC とローカルネットワーク間での通信を許可するポリシーを設定します。その後、ゲートウェイにポリシーをインストールします。

1. SmartDashboard で、ゲートウェイの [Global Properties] を選択します。カテゴリーペインで [VPN] を展開し、[Advanced] を選択します。
2. [Enable VPN Directional Match in VPN Column] を選択し、変更を保存します。
3. SmartDashboard で [Firewall] を選択し、次のルールでポリシーを作成します。
   - VPC サブネットに対して必須プロトコル経由でのローカルネットワークとの通信を許可する。
   - ローカルネットワークに対して必須プロトコル経由での VPC サブネットとの通信を許可する。
4. VPN 列のセルのコンテキストメニューを開いて、[Edit Cell] を選択します。
5. [VPN Match Conditions] ダイアログボックスで、[Match traffic in this direction only] を選択します。それぞれで [Add] を選択してディレクショナルマッチルールを作成し、完了したら [OK] を選択します。
   - `internal_clear` > VPN コミュニティ (先に作成した VPN スターコミュニティ。例: `AWS_VPN_Star`)
   - VPN コミュニティ > VPN コミュニティ
   - VPN コミュニティ > `internal_clear`
6. SmartDashboard で、[Policy]、[Install] の順に選択します。
7. ダイアログボックスでゲートウェイを選択し、[OK] を選択してポリシーをインストールします。

tunnel_keepalive_method プロパティを変更するには

Check Point ゲートウェイでは、IKE の関連付けが停止したときに Dead Peer Detection (DPD) を使用して識別できます。永続トンネルに対して DPD を設定するには、永続トンネルが AWS VPN コミュニティで設定されている必要があります (ステップ 8 を参照)。

デフォルトでは、VPN ゲートウェイの `tunnel_keepalive_method` プロパティは `tunnel_test` に設定されます。この値を dpd に変更する必要があります。DPD モニタリングが必要な VPN コミュニティ内の各 VPN ゲートウェイは、サードパーティー製 VPN ゲートウェ

イを含め、tunnel_keepalive_method プロパティで設定する必要があります。同じゲートウェイに対して異なるモニタリングメカニズムを設定することはできません。

GuiDBedit ツールを使用して tunnel_keepalive_method プロパティを更新できます。

1. Check Point SmartDashboard を開き、[Security Management Server]、[Domain Management Server] の順に選択します。
2. [File]、[Database Revision Control...] の順に選択し、リビジョンのスナップショットを作成します。
3. SmartDashboard、SmartView Tracker、SmartView Monitor など、すべての SmartConsole ウィンドウを閉じます。
4. GuiBDedit ツールを起動します。詳細については、Check Point サポートセンターの「Check Point Database Tool」という記事を参照してください。
5. [Security Management Server]、[Domain Management Server] の順に選択します。
6. 左上のペインで、[Table]、[Network Objects]、[network_objects] の順に選択します。
7. 右上のペインで、関連する [Security Gateway]、[Cluster] オブジェクトを選択します。
8. Ctrl+F キーを押すか、[Search] メニューを使用して以下を検索します。tunnel_keepalive_method
9. 下のペインで、[tunnel_keepalive_method] のコンテキストメニューを開き、[Edit... (編集...)] を選択します。[dpd] を選択し、[OK] を選択します。
10. AWS VPN コミュニティの一部である各ゲートウェイに対して、ステップ 7～9 を繰り返します。
11. [File]、[Save All] の順に選択します。
12. GuiDBedit ツールを閉じます。
13. Check Point SmartDashboard を開き、[Security Management Server]、[Domain Management Server] の順に選択します。
14. 関連する [Security Gateway]、[Cluster] オブジェクトにポリシーをインストールします。

詳細については、Check Point Support Center の「New VPN features in R77.10」という記事を参照してください。

TCP MSS クランプを有効にするには

TCP MSS クランプは TCP パケットの最大セグメントサイズを小さくしてパケット断片化を防ぎます。

1. 次のディレクトリに移動します。`C:\Program Files (x86)\CheckPoint\SmartConsole\R77.10\PROGRAM\`
2. `GuiDBEdit.exe` ファイルを実行して Check Point Database Tool を開きます。
3. [Table]、[Global Properties]、[properties] の順に選択します。
4. `fw_clamp_tcp_mss` で、[Edit] を選択します。値を `true` に変更し、[OK] を選択します。

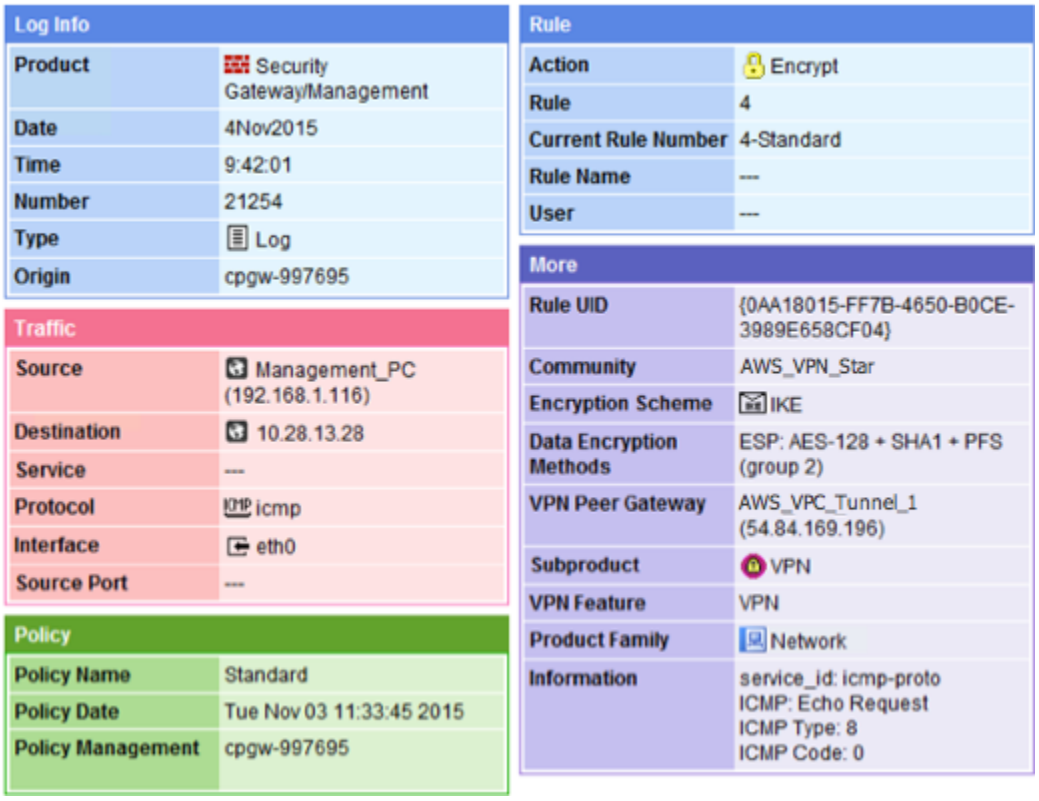
トンネルのステータスを確認するには

エキスパートモードのコマンドラインツールから次のコマンドを実行して、トンネルの状態を確認できます。

```
vpn tunnelutil
```

表示されたオプションで、IKE 関連付けを検証するには [1] を、IPsec 関連付けを検証するには [2] を選択します。

また、Check Point Smart Tracker Log を使用して、接続内のパケットが暗号化されていることを検証できます。たとえば次のログは、VPC へのパケットがトンネル 1 経由で送信され、暗号化されていることを示します。



SonicWALL

次の手順では、SonicOS 管理インターフェイスを使用して SonicWALL デバイスに VPN トンネルを設定する方法を説明します。

トンネルを設定するには

1. SonicWALL SonicOS 管理インターフェイスを開きます。
2. 左側のペインで、[VPN]、[Settings] の順に選択します。[VPN Policies] の下で、[Add...] を選択します。
3. [General] タブの VPN ポリシーウィンドウで、次の情報を入力します。
   - [Policy Type: [Tunnel Interface] を選択します。
   - [Authentication Method]: [IKE using Preshared Secret] を選択します。
   - [Name]: VPN ポリシーの名前を入力します。設定ファイルに記載されている通り、VPN ID 名を使用することをお勧めします。
   - IPsec Primary Gateway Name or Address: 設定ファイルに記載されている通り、仮想プライベートゲートウェイの IP アドレス (例: `72.21.209.193`) を入力します。
   - IPsec Secondary Gateway Name or Address: デフォルト値のままにします。
   - Shared Secret: 設定ファイルに記載されている通りに事前共有キーを入力後、[Confirm Shared Secret] で再入力します。
   - Local IKE ID: カスタマーゲートウェイ (SonicWALL デバイス) の IPv4 アドレスを入力します。
   - Peer IKE ID: 仮想プライベートゲートウェイの IPv4 アドレスを入力します。
4. [Network] タブで、次の情報を入力します。
   - [Local Networks] で、[Any address] を選択します。このオプションを使用して、ローカルネットワーク接続の問題を防ぐことをお勧めします。
   - [Remote Networks] で、[Choose a destination network from list] を選択します。 内に VPC の CIDR を持つアドレスオブジェクトを作成しますAWS
5. [Proposals (提案)] タブで、次の情報を入力します。
   - [IKE (Phase 1) Proposal] で、以下の作業を行います。
     - Exchange: [Main Mode] を選択します。
     - DH Group: Diffie-Hellman Group の値 (例: 2) を入力します。
     - Encryption: [AES-128] または [AES-256] を選択します。

- Authentication: [SHA1] または [SHA256] を選択します。
- Life Time: `28800` と入力します。

- [IKE (Phase 2) Proposal] で、以下の作業を行います。
  - Protocol: [ESP] を選択します。
  - Encryption: [AES-128] または [AES-256] を選択します。
  - Authentication: [SHA1] または [SHA256] を選択します。
  - [Enable Perfect Forward Secrecy] チェックボックスをオンにし、Diffie-Hellman group を選択します。
  - Life Time: `3600` と入力します。

> **Important**
>
> 仮想プライベートゲートウェイを作成したのが 2015 年 10 月より前の場合は、両方のフェーズで Diffie-Hellman group 2、AES-128、SHA1 を指定する必要があります。

6. [Advanced] タブで、次の情報を入力します。

   - [Enable Keep Alive] を選択します。
   - [Enable Phase2 Dead Peer Detection] を選択し、次のように入力します。
     - [Dead Peer Detection Interval] に、`60` (SonicWALL デバイスで入力可能な最小値) と入力します。
     - [Failure Trigger Level] で、`3` と入力します。
   - [VPN Policy bound to] で、[Interface X1] を選択します。パブリック IP アドレスで一般的に指定されたインターフェイスです。
7. [OK] をクリックします。[Settings] ページで、トンネルの [Enable] チェックボックスをデフォルトでオンにします。緑の点は、トンネルが稼働していることを表します。

Cisco デバイスの追加情報

一部の Cisco ASA ではアクティブ/スタンバイモードのみがサポートされています。これらの Cisco ASA を使用する場合は、アクティブなトンネルを一度に 1 個のみ保持できます。最初のトンネルが利用不可になった場合は、他方のスタンバイトンネルがアクティブになります。この冗長化では、常にいずれかのトンネルを経由して VPC への接続を保持する必要があります。

バージョン 9.7.1 以降の Cisco ASA は、アクティブ/アクティブモードをサポートします。これらの Cisco ASA を使用する場合は、両方のトンネルを同時にアクティブにすることができます。この冗長化では、常にいずれかのトンネルを経由して VPC への接続を保持する必要があります。

Cisco デバイスの場合は、次の作業を行う必要があります。

- 外部インターフェイスを設定します。
- Crypto ISAKMP Policy Sequence の数値が一意であることを確認します。
- Crypto List Policy Sequence の数値が一意であることを確認します。
- Crypto IPsec Transform Set および Crypto ISAKMP Policy Sequence と、デバイスに設定された他のすべての IPsec トンネルの整合性が確保されていることを確認します。
- SLA モニタリング番号が一意であることを確認します。
- カスタマーゲートウェイデバイスとローカルネットワークとの間でトラフィックを動かす内部ルーティングをすべて設定します。

テスト

Site-to-Site VPN 接続のテストの詳細については、「Site-to-Site VPN 接続をテストする」を参照してください。

動的ルーティング (BGP) のカスタマーゲートウェイデバイス設定の例

トピックス

設定ファイルの例

Site-to-Site VPN 接続設定に固有の値を含むサンプル設定ファイルをダウンロードするには、Amazon VPC コンソール、AWS コマンドラインまたは Amazon EC2 API を使用します。詳細については、「ステップ 6: 設定ファイルをダウンロードする」を参照してください。

また、Site-to-Site VPN 接続設定に固有の値を含まないダイナミックルーティング用の汎用設定ファイルの例をダウンロードすることもできます。dynamic-routing-examples.zip

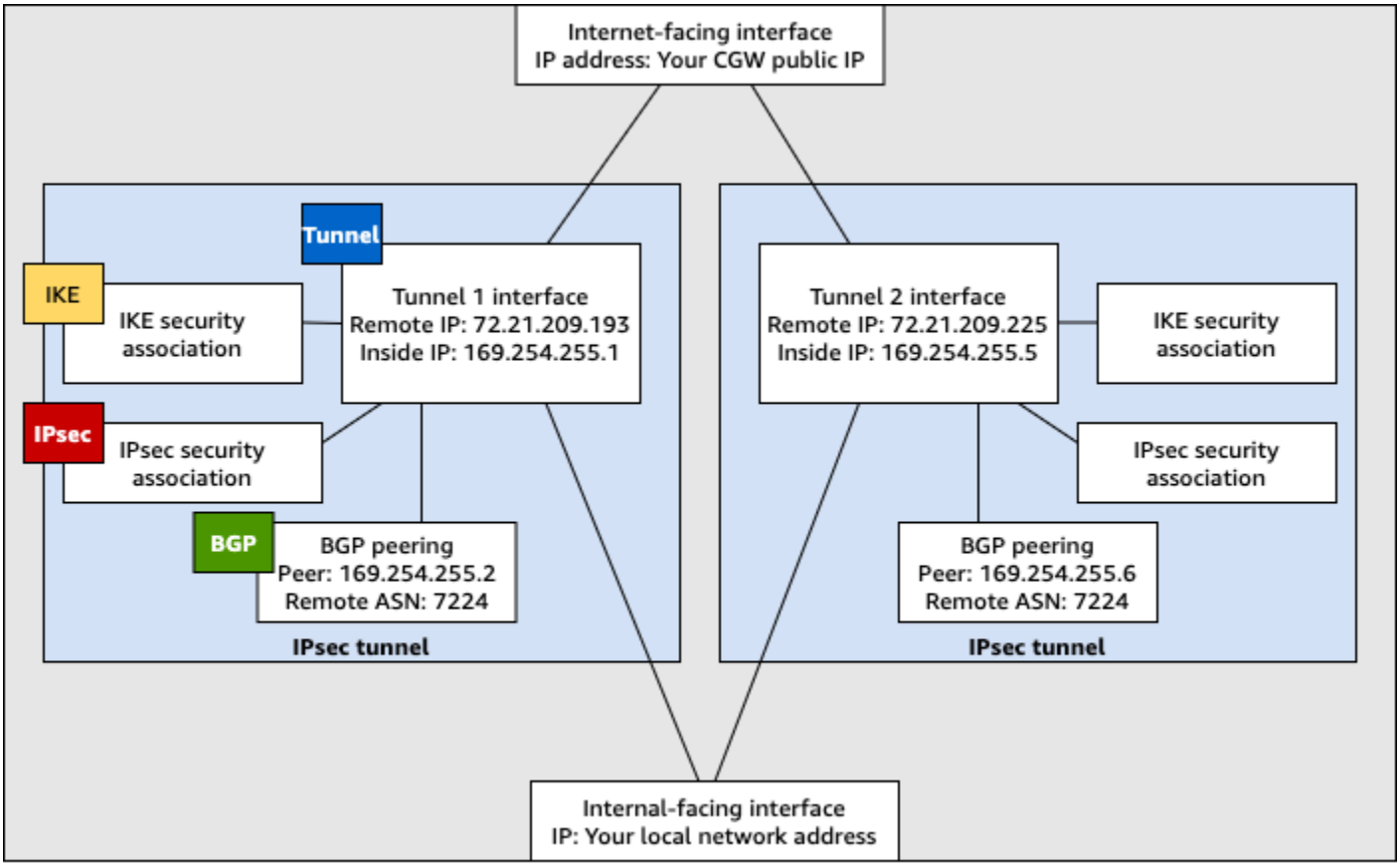
これらのファイルは、一部のコンポーネントにプレースホルダー値を使用します。たとえば、以下を使用します。

- VPN 接続 ID 、カスタマーゲートウェイ ID および仮想プライベートゲートウェイ ID の値の例
- リモート (外部) IP アドレス AWS エンドポイント (*AWS_ENDPOINT_1* および *AWS_ENDPOINT_2*) のプレースホルダー
- カスタマーゲートウェイデバイスのインターネットルーティング可能な外部インターフェイスの IP アドレスのプレースホルダー (*your-cgw-ip-address*)
- 事前共有キー値のプレースホルダ (事前共有キー)
- トンネルの内部 IP アドレスの値の例。
- MTU 設定の値の例。

> **Note**
>
> サンプルコンフィギュレーションファイルで提供されている MTU 設定は、例にすぎません。状況に応じた最適な MTU 値の設定については、「カスタマーゲートウェイデバイスのベストプラクティス」を参照してください。

このファイルは、プレースホルダー値を提供することに加えて、ほとんどの AWS リージョンで AES128、SHA1、および Diffie-Hellman グループ 2、および AWS GovCloud リージョンで AES128、SHA2、および Diffie-Hellman グループ 14 を指定します。また、認証用の事前共有キーも指定します。追加のセキュリティアルゴリズム、Diffie-Hellman グループ、プライベート証明書、IPv6 トラフィックを活用するには、サンプル設定ファイルを変更する必要があります。

次の図は、カスタマーゲートウェイデバイスに設定されているさまざまなコンポーネントの概要を示しています。これには、トンネルインターフェイスの IP アドレスの値の例が含まれます。



動的ルーティングのユーザーインターフェイス手順

以下は、ユーザーインターフェイス (使用可能な場合) を使用してカスタマーゲートウェイデバイスを設定する手順の例です。

Check Point

以下は、Gaia ウェブポータルと Check Point SmartDashboard を使用して、R77.10 以降を実行する Check Point Security Gateway デバイスを設定するステップです。また、Check Point Support Center の Amazon Web Services (AWS) VPN BGP の記事も参照してください。

トンネルインターフェイスを設定するには

最初のステップは、VPN トンネルを作成し、各トンネル用の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プライベート (内部) IP アドレスを提供することです。最初のトンネルを作成するには、設定ファイルの `IPSec Tunnel #1` セクションで提供される情報を使用します。2 番目のトンネルを作成するには、設定ファイルの `IPSec Tunnel #2` セクションで提供される値を使用します。

1. SSH でセキュリティゲートウェイに接続します。デフォルト以外のシェルを使用している場合は、次のコマンドを実行して、clish に変更します。clish
2. 次のコマンドを使実行して、カスタマーゲートウェイ ASN (AWS でカスタマーゲートウェイが作成されたときに提供された ASN) を設定します。

```
set as 65000
```

3. 設定ファイルの IPSec Tunnel #1 セクションで提供されている情報を使用して、最初のトンネル用のトンネルインターフェイスを作成します。AWS_VPC_Tunnel_1 など、トンネルに一意の名前をつけます。

```
add vpn tunnel 1 type numbered local 169.254.44.234 remote 169.254.44.233
 peer AWS_VPC_Tunnel_1
set interface vpnt1 state on
set interface vpnt1 mtu 1436
```

4. 2 番目のトンネルを作成するには、設定ファイルの IPSec Tunnel #2 セクションで提供されている情報を使用して、コマンドを繰り返します。AWS_VPC_Tunnel_2 など、トンネルに一意の名前をつけます。

```
add vpn tunnel 1 type numbered local 169.254.44.38 remote 169.254.44.37
 peer AWS_VPC_Tunnel_2
set interface vpnt2 state on
set interface vpnt2 mtu 1436
```

5. 仮想プライベートゲートウェイ ASN を設定します。

```
set bgp external remote-as 7224 on
```

6. 最初のトンネルの BGP を、設定ファイルの IPSec Tunnel #1 セクションで提供される情報を使用して設定します。

```
set bgp external remote-as 7224 peer 169.254.44.233 on
set bgp external remote-as 7224 peer 169.254.44.233 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.233 keepalive 10
```

7. 2 番目のトンネルの BGP を、設定ファイルの IPSec Tunnel #2 セクションで提供される情報を使用して設定します。

```
set bgp external remote-as 7224 peer 169.254.44.37 on
```

```
set bgp external remote-as 7224 peer 169.254.44.37 holdtime 30
set bgp external remote-as 7224 peer 169.254.44.37 keepalive 10
```

8. 設定を保存します。

```
save config
```

BGP ポリシーを作成するには

次に、 によってアドバタイズされたルートのインポートを許可する BGP ポリシーを作成します AWS 次に、ローカルルートを にアドバタイズするようにカスタマーゲートウェイを設定します AWS

1. Gaia WebUI で、[Advanced Routing]、[Inbound Route Filters] を選択します。[Add] を選択し、[Add BGP Policy (Based on AS)] を選択します。
2. [Add BGP Policy (BGP ポリシーの追加)] の最初のフィールドで 512 から 1024 までの範囲の値を選択し、2 番目のフィールドに仮想プライベートゲートウェイ ASN (例: 7224) を入力します。
3. [Save] を選択します。

ローカルルートをアドバタイズするには

次のステップは、ローカルインターフェイスルートを分散するためのものです。また、静的ルーティングや、動的ルーティングプロトコルによって得られたルーティングなど、さまざまなソースからのルートを再分散できます。詳細については、「Gaia Advanced Routing R77 Versions Administration Guide」を参照してください。

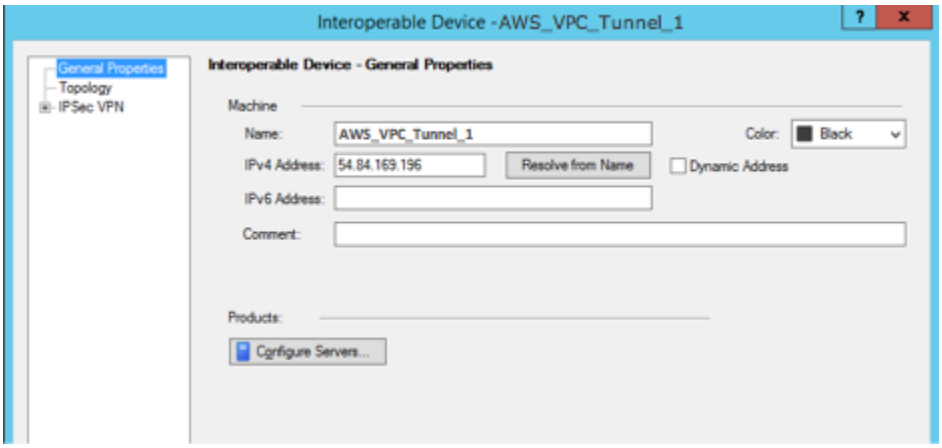
1. Gaia WebUI で、[Advanced Routing]、[Routing Redistribution] の順に選択します。[Add Redistribution From]、[Interface (インターフェイス)] の順に選択します。
2. [To Protocol] で、仮想プライベートゲートウェイ ASN; (例: 7224) を選択します。
3. [Interface] では内部インターフェイスを選択します。[Save] を選択します。

新しいネットワークオブジェクトを定義するには

次に、仮想プライベートゲートウェイのパブリック (外部) IP アドレスを指定して、各 VPN トンネル用のネットワークオブジェクトを作成します。後で、VPN コミュニティのサテライトゲート

ウェイとしてこれらのオブジェクトを追加します。また、VPN ドメインのプレースホルダーとして機能する空グループを作成する必要があります。

1. Check Point SmartDashboard を開きます。
2. [Groups] では、コンテキストメニューを開き、[Groups]、[Simple Group] の順に選択します。各ネットワークオブジェクトに対して同じグループを使用できます。
3. [Network Objects] では、コンテキストメニュー (右クリック) を開き、[New]、[Interoperable Device] の順に選択します。
4. [Name (名前)] には、ステップ 1 でトンネル用に指定した名前 (例: `AWS_VPC_Tunnel_1` または `AWS_VPC_Tunnel_2`) を入力します。
5. [IPv4 Address] には、設定ファイルで提供される仮想プライベートゲートウェイの外部 IP アドレス (例: `54.84.169.196`) を入力します。設定を保存して、このダイアログボックスを閉じます。



6. 左のカテゴリーペインで、[Topology] を選択します。
7. [VPN Domain (VPN ドメイン)] セクションで、[Manually defined (手動で定義)] を選択し、ステップ 2 で作成した空のシンプルなグループを参照して選択します。[OK] をクリックします。
8. 2 番目のネットワークオブジェクトを作成するには、設定ファイルの `IPSec Tunnel #2` セクション内の情報を使用して、ステップを繰り返します。
9. ゲートウェイネットワークオブジェクトに移動してゲートウェイまたはクラスターオブジェクトを開き、[Topology] を選択します。
10. [VPN Domain (VPN ドメイン)] セクションで、[Manually defined (手動で定義)] を選択し、ステップ 2 で作成した空のシンプルなグループを参照して選択します。[OK] をクリックします。

> **Note**
>
> 設定済みの既存の VPN ドメインは保持できます。ただし、特に VPN ドメインが自動的に取得されている場合は、新しい VPN 接続で使用または提供されるドメインとホストがその VPN ドメインで宣言されていないことを確認してください。

> **Note**
>
> クラスターを使用している場合は、トポロジーを編集してインターフェイスをクラスターインターフェイスとして定義します。設定ファイルで指定された IP アドレスを使用します。

VPN コミュニティ、IKE、および IPsec 設定の作成と設定

次に、Check Point ゲートウェイに VPN コミュニティを作成し、そこに各トンネルのネットワークオブジェクト (相互運用デバイス) を追加します。また、Internet Key Exchange (IKE) および IPsec を設定します。

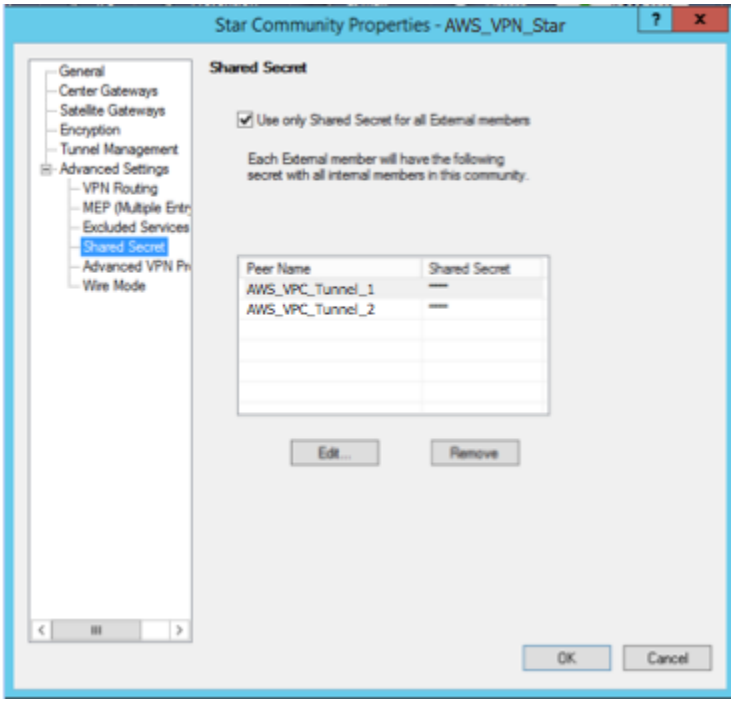
1. ゲートウェイのプロパティから、カテゴリーペインの [IPSec VPN] を選択します。
2. [Communities]、[New]、[Star Community] の順に選択します。
3. コミュニティの名前 (例: `AWS_VPN_Star`) を指定し、カテゴリーペインの [Center Gateways] を選択します。
4. [Add] を選択して、ゲートウェイまたはクラスターを参加ゲートウェイのリストに追加します。
5. カテゴリーペインで、[Satellite Gateways]、[Add (追加)] の順に選択し、先に作成した相互運用デバイス (`AWS_VPC_Tunnel_1` および `AWS_VPC_Tunnel_2`) を参加ゲートウェイのリストに追加します。
6. カテゴリーペインで、[Encryption] を選択します。[Encryption Method] セクションで、[IKEv1 for IPv4 and IKEv2 for IPv6] を選択します。[Encryption Suite] セクションで、[Custom]、[Custom Encryption] の順に選択します。

> **Note**
>
> IKEv1 機能の [IKEv1 for IPv4 and IKEv2 for IPv6] オプションを選択します。

7. ダイアログボックスで次のように暗号化プロパティを設定し、完了したら [OK] を選択します。

   - IKE Security Association (フェーズ 1) のプロパティ
     - Perform key exchange encryption with: AES-128
     - Perform data integrity with: SHA-1
   - IPsec Security Association (フェーズ 2) のプロパティ
     - Perform IPsec data encryption with: AES-128
     - Perform data integrity with: SHA-1

8. カテゴリーペインで [Tunnel Management] を選択します。[Set Permanent Tunnels]、[On all tunnels in the community] の順に選択します。[VPN Tunnel Sharing] セクションで、[One VPN tunnel per Gateway pair] を選択します。
9. カテゴリーペインで [Advanced Settings] を展開し、[Shared Secret] を選択します。
10. 最初のトンネルのピア名を選択し、[Edit (編集)] を選択して、設定ファイルの `IPSec Tunnel #1` セクションで指定されている事前共有キーを入力します。
11. 2 番目のトンネルのピア名を選択し、[Edit (編集)] を選択して、設定ファイルの `IPSec Tunnel #2` セクションで指定されている事前共有キーを入力します。



12. さらに [Advanced Settings (詳細設定)] カテゴリで [Advanced VPN Properties (詳細な VPN プロパティ)] を選択し、プロパティを次のように設定して、完了したら [OK] を選択します。

    - IKE (フェーズ 1):
      - Use Diffie-Hellman group: `Group 2 (1024 bit)`
      - Renegotiate IKE security associations every `480` minutes
    - IPsec (フェーズ 2):
      - [Use Perfect Forward Secrecy] を選択します。
      - Use Diffie-Hellman group: `Group 2 (1024 bit)`
      - Renegotiate IPsec security associations every `3600` seconds

ファイアウォールルールを作成するには

次に、ファイアウォールルールとディレクショナルマッチルールを使用し、VPC とローカルネットワーク間での通信を許可するポリシーを設定します。その後、ゲートウェイにポリシーをインストールします。

1. SmartDashboard で、ゲートウェイの [Global Properties] を選択します。カテゴリーペインで [VPN] を展開し、[Advanced] を選択します。
2. [Enable VPN Directional Match in VPN Column] を選択し、[OK] を選択します。

3. SmartDashboard で [Firewall] を選択し、次のルールでポリシーを作成します。

   - VPC サブネットに対して必須プロトコル経由でのローカルネットワークとの通信を許可する。
   - ローカルネットワークに対して必須プロトコル経由での VPC サブネットとの通信を許可する。
4. VPN 列のセルのコンテキストメニューを開いて、[Edit Cell] を選択します。
5. [VPN Match Conditions] ダイアログボックスで、[Match traffic in this direction only] を選択します。それぞれで [Add (追加)] を選択して以下のディレクショナルマッチルールを作成し、完了したら [OK] を選択します。

   - `internal_clear` > VPN コミュニティ (先に作成した VPN スターコミュニティ。例: `AWS_VPN_Star`)
   - VPN コミュニティ > VPN コミュニティ
   - VPN コミュニティ > `internal_clear`
6. SmartDashboard で、[Policy]、[Install] の順に選択します。
7. ダイアログボックスでゲートウェイを選択し、[OK] を選択してポリシーをインストールします。

tunnel_keepalive_method プロパティを変更するには

Check Point ゲートウェイでは、IKE の関連付けが停止したときに Dead Peer Detection (DPD) を使用して識別できます。永続トンネルに対して DPD を設定するには、永続トンネルが AWS VPN コミュニティで設定されている必要があります。

デフォルトでは、VPN ゲートウェイの `tunnel_keepalive_method` プロパティは `tunnel_test` に設定されます。この値を `dpd` に変更する必要があります。DPD モニタリングが必要な VPN コミュニティ内の各 VPN ゲートウェイは、サードパーティー製 VPN ゲートウェイを含め、`tunnel_keepalive_method` プロパティで設定する必要があります。同じゲートウェイに対して異なるモニタリングメカニズムを設定することはできません。

GuiDBedit ツールを使用して `tunnel_keepalive_method` プロパティを更新できます。

1. Check Point SmartDashboard を開き、[Security Management Server]、[Domain Management Server] の順に選択します。
2. [File]、[Database Revision Control...] の順に選択し、リビジョンのスナップショットを作成します。

3. SmartDashboard、SmartView Tracker、SmartView Monitor など、すべての SmartConsole ウィンドウを閉じます。
4. GuiBDedit ツールを起動します。詳細については、Check Point サポートセンターの「Check Point Database Tool」という記事を参照してください。
5. [Security Management Server]、[Domain Management Server] の順に選択します。
6. 左上のペインで、[Table]、[Network Objects]、[network_objects] の順に選択します。
7. 右上のペインで、関連する [Security Gateway]、[Cluster] オブジェクトを選択します。
8. Ctrl+F キーを押すか、[Search] メニューを使用して以下を検索します。`tunnel_keepalive_method`
9. 下のペインで、[`tunnel_keepalive_method`] のコンテキストメニューを開き、[Edit...] を選択します。[dpd]、[OK] の順に選択します。
10. AWS VPN コミュニティの一部である各ゲートウェイに対して、ステップ 7～9 を繰り返します。
11. [File]、[Save All] の順に選択します。
12. GuiDBedit ツールを閉じます。
13. Check Point SmartDashboard を開き、[Security Management Server]、[Domain Management Server] の順に選択します。
14. 関連する [Security Gateway]、[Cluster] オブジェクトにポリシーをインストールします。

詳細については、Check Point Support Center の「New VPN features in R77.10」という記事を参照してください。

TCP MSS クランプを有効にするには

TCP MSS クランプは TCP パケットの最大セグメントサイズを小さくしてパケット断片化を防ぎます。

1. 次のディレクトリに移動します。`C:\Program Files (x86)\CheckPoint \SmartConsole\R77.10\PROGRAM\`
2. `GuiDBEdit.exe` ファイルを実行して Check Point Database Tool を開きます。
3. [Table]、[Global Properties]、[properties] の順に選択します。
4. `fw_clamp_tcp_mss` で、[Edit] を選択します。値を `true` に変更し、[OK] を選択します。

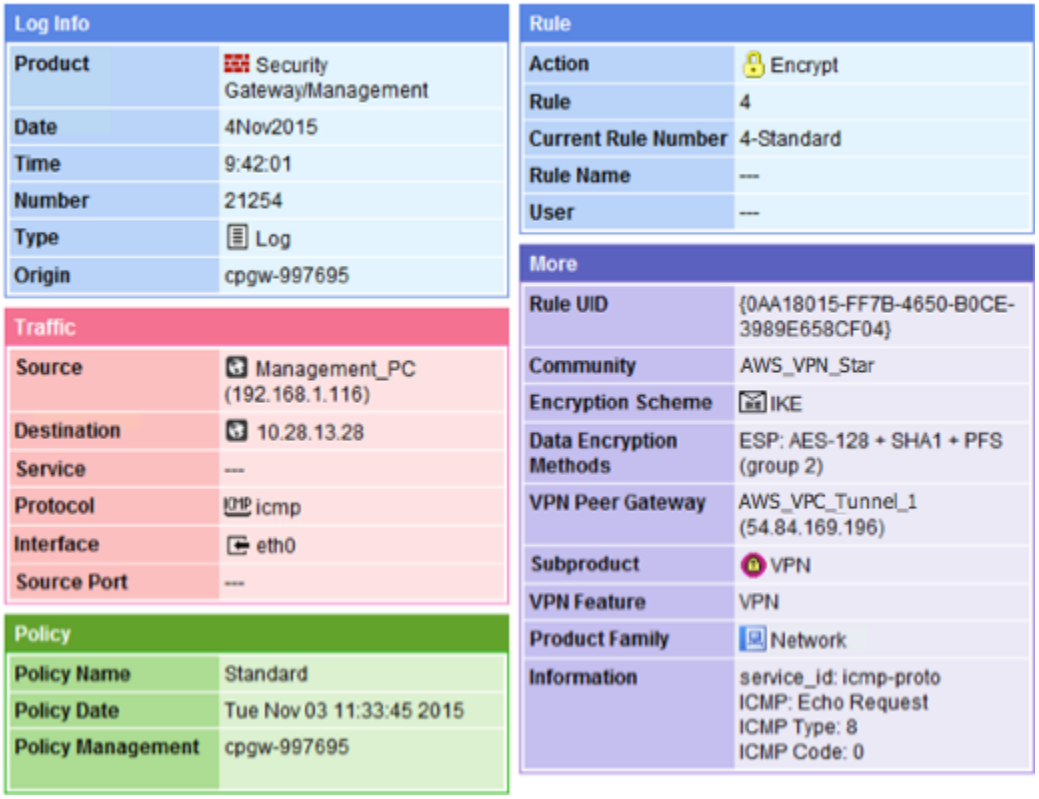
トンネルのステータスを確認するには

エキスパートモードのコマンドラインツールから次のコマンドを実行して、トンネルの状態を確認できます。

```
vpn tunnelutil
```

表示されたオプションで、IKE 関連付けを検証するには [1] を、IPsec 関連付けを検証するには [2] を選択します。

また、Check Point Smart Tracker Log を使用して、接続内のパケットが暗号化されていることを検証できます。たとえば次のログは、VPC へのパケットがトンネル 1 経由で送信され、暗号化されていることを示します。



SonicWALL

SonicOS 管理インターフェイスを使用して SonicWALL デバイスを設定できます。トンネルの設定方法の詳細については、「静的ルーティングのユーザーインターフェイス手順」を参照してください。

このSonicOS 管理インターフェイスを使用して、デバイスの BGP を設定することはできません。代わりに、設定ファイル例の [BGP] というセクションの下にあるコマンドライン手順を使用します。

Cisco デバイスの追加情報

一部の Cisco ASA ではアクティブ/スタンバイモードのみがサポートされています。これらの Cisco ASA を使用する場合は、アクティブなトンネルを一度に 1 個のみ保持できます。最初のトンネルが利用不可になった場合は、他方のスタンバイトンネルがアクティブになります。この冗長化では、常にいずれかのトンネルを経由して VPC への接続を保持する必要があります。

バージョン 9.7.1 以降の Cisco ASA は、アクティブ/アクティブモードをサポートします。これらの Cisco ASA を使用する場合は、両方のトンネルを同時にアクティブにすることができます。この冗長化では、常にいずれかのトンネルを経由して VPC への接続を保持する必要があります。

Cisco デバイスの場合は、次の作業を行う必要があります。

- 外部インターフェイスを設定します。
- Crypto ISAKMP Policy Sequence の数値が一意であることを確認します。
- Crypto List Policy Sequence の数値が一意であることを確認します。
- Crypto IPsec Transform Set および Crypto ISAKMP Policy Sequence と、デバイスに設定された他のすべての IPsec トンネルの整合性が確保されていることを確認します。
- SLA モニタリング番号が一意であることを確認します。
- カスタマーゲートウェイデバイスとローカルネットワークとの間でトラフィックを動かす内部ルーティングをすべて設定します。

Juniper デバイスの追加情報

次の情報は、Juniper J シリーズおよび SRX カスタマーゲートウェイデバイスの設定ファイルの例に適用されます。

- 外部インターフェイスは *ge-0/0/0.0* と呼ばれます。
- トンネルインターフェイス ID は *st0.1* および *st0.2* と呼ばれます。
- アップリンクインターフェイスのセキュリティゾーンを確実に特定します (設定情報ではデフォルトゾーンの 'untrust' を使用します)。
- 内部インターフェイスのセキュリティゾーンを確実に特定します (設定情報ではデフォルトゾーンの 'trust' を使用します)。

テスト

Site-to-Site VPN 接続のテストの詳細については、「Site-to-Site VPN 接続をテストする」を参照してください。

Windows Server のカスタマーゲートウェイデバイスとしての設定

Windows Server を実行するサーバーを VPC のカスタマーゲートウェイデバイスとして設定できます。Windows Server を VPC 内の EC2 インスタンスで実行しているか独自のサーバーで実行しているかに関わらず、次のプロセスを使用します。次の手順は、Windows Server 2012 R2 以降に適用されます。

目次

Windows インスタンスの設定

Windows AMI から起動した EC2 インスタンスで Windows Server を設定する場合は、次の手順を実行します。

- インスタンスの送信元/送信先チェックを無効にします。
  1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
  2. Windows Server インスタンスを選択して、[Actions]、[Networking]、[Change source/destination check] と選択します。[Stop] を選択してから、[Save] を選択します。
- 他のインスタンスからトラフィックをルーティングできるように、アダプタの設定を更新します。
  1. Windows インスタンスに接続します。詳細については、「Windows インスタンスへの接続」を参照してください。
  2. [コントロールパネル] を開き、[デバイスマネージャー] を起動します。

3. [ネットワークアダプター] ノードを展開します。
4. ネットワークアダプタ (インスタンスタイプに応じて、Amazon Elastic ネットワークアダプタまたは Intel 82599 仮想関数) を選択し、[Action]、[Properties] の順に選択します。
5. [詳細設定] タブで、[IPv4 Checksum Offload]、[TCP Checksum Offload (IPv4)]、および [UDP Checksum Offload (IPv4)] の各プロパティを無効にし、[OK] を選択します。

- Elastic IP アドレスをアカウントに割り当てて、インスタンスに関連付けます。詳細については、「Elastic IP アドレスの操作」を参照してください。このアドレスは書き留めておきます。VPC でカスタマーゲートウェイを作成するときに必要になります。
- インスタンスのセキュリティグループのルールでアウトバウンドの IPsec トラフィックが許可されていることを確認します。デフォルトでは、セキュリティグループは、すべてのアウトバウンドトラフィックを許可します。ただし、セキュリティグループのアウトバウンドルールが元の状態から変更されている場合、IPsec トラフィック用にアウトバウンドのカスタムプロトコルルール (IP プロトコル 50、IP プロトコル 51、UDP 500) を作成する必要があります。

Windows インスタンスが配置されているネットワークの CIDR 範囲 (`172.31.0.0/16` など) を書き留めます。

ステップ 1: VPN 接続を作成し、VPC を設定する

VPC から VPN 接続を作成するには、次の手順を実行します。

1. 仮想プライベートゲートウェイを作成し、VPC にアタッチします。詳細については、「仮想プライベートゲートウェイの作成」を参照してください。
2. VPN 接続と新しいカスタマーゲートウェイを作成します。カスタマーゲートウェイの場合、Windows Server のパブリック IP アドレスを指定します。VPN 接続の場合は、静的ルーティングを選択し、Windows Server が配置されているネットワークの CIDR 範囲 (例: `172.31.0.0/16`) を入力します。詳細については、「ステップ 5: VPN 接続を作成する」を参照してください。

VPN 接続を作成したら、VPN 接続を介した通信を有効にするように VPC を設定します。

VPC を設定するには

- Windows Server と通信するインスタンスを起動するためのプライベートサブネットを VPC で作成します (まだ、ない場合)。詳細については、「VPC でサブネットを作成する」を参照してください。

> **Note**
>
> プライベートサブネットは、インターネットゲートウェイへのルートがないサブネットです。このサブネットのルーティングについては、次の項目で説明します。

- VPN 接続のルートテーブルを更新します。
  - 仮想プライベートゲートウェイをターゲットに指定し、Windows Server のネットワーク (CIDR 範囲) を宛先に指定して、プライベートサブネットのルートテーブルにルートを追加します。詳細については、Amazon VPC ユーザーガイドの「ルートテーブルでルートを追加および削除する」を参照してください。
  - 仮想プライベートゲートウェイのルート伝達を有効にします。詳細については、「(仮想プライベートゲートウェイ) ルートテーブルでルート伝播を有効にする」を参照してください。
- VPC とネットワーク間の通信を許可する、インスタンスのセキュリティグループを作成します。
  - ネットワークからのインバウンド RDP または SSH アクセスを許可するルールを追加します。これにより、ネットワークから VPC のインスタンスに接続できます。たとえば、ネットワークのコンピュータが VPC 内の Linux インスタンスにアクセスできるようにするには、SSH タイプのインバウンドルールを作成し、ソースをネットワークの CIDR 範囲 (例: `172.31.0.0/16`) に設定します。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。
  - ネットワークからのインバウンド ICMP アクセスを許可するルールを追加します。これにより、Windows Server から VPC 内のインスタンスへの ping を実行して、VPN 接続をテストできます。

ステップ 2: VPN 接続の設定ファイルをダウンロードする

Amazon VPC コンソールを使用して、VPN 接続用の Windows Server 設定ファイルをダウンロードできます。

設定ファイルをダウンロードするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN Connections (Site-to-Site VPN 接続)] を選択します。
3. 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。

4. ベンダーとして [Microsoft]、プラットフォームとして [Windows Server]、ソフトウェアとして [2012 R2] を選択します。[Download] を選択します。ファイルを開くか保存できます。

設定ファイルには、次の例のような情報のセクションが含まれます。 この情報は、2 回 (トンネルごとに 1 回ずつ) 記述されています。

```
vgw-1a2b3c4d Tunnel1
------------------------------------------------------------------
Local Tunnel Endpoint:       203.0.113.1
Remote Tunnel Endpoint:      203.83.222.237
Endpoint 1:                  [Your_Static_Route_IP_Prefix]
Endpoint 2:                  [Your_VPC_CIDR_Block]
Preshared key:               xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE
```

`Local Tunnel Endpoint`

VPN 接続の作成時にカスタマーゲートウェイ用に指定した IP アドレスです。

`Remote Tunnel Endpoint`

仮想プライベートゲートウェイの 2 つの IP アドレスのうちの 1 つで、AWS 側の VPN 接続の終端です。

`Endpoint 1`

VPN 接続を作成したときに静的ルートとして指定した IP プレフィックスです。VPN 接続を使用して VPC にアクセスすることを許可された、ネットワークの IP アドレスです。

`Endpoint 2`

仮想プライベートゲートウェイにアタッチされた VPC の IP アドレス範囲 (CIDR ブロック) (例: 10.0.0.0/16) です。

`Preshared key`

`Local Tunnel Endpoint` と `Remote Tunnel Endpoint` との間で IPsec VPN 接続を確立するために使用される事前共有キーです。

両方のトンネルを VPN 接続の一部として設定することをお勧めします。 各トンネルは、VPN 接続の Amazon 側にある別個の VPN コンセントレータに接続します。一度に起動できるトンネルは 1 つだけですが、1 番目のトンネルが停止すると、2 番目のトンネルが自動的に接続を確立します。 冗長なトンネルを設定することで、デバイス障害の発生時にも可用性を継続的に維持できます。一度に使

用できるトンネルは 1 つだけであるため、その 1 つのトンネルが停止したことが VPC コンソールに表示されます。これは予期されている動作のため、お客様が操作を行う必要はありません。

トンネルを 2 つ設定しておけば、AWS でデバイス障害が発生した場合、VPN 接続は仮想プライベートゲートウェイの 2 番目のトンネルに数分以内に自動的にフェイルオーバーします。カスタマーゲートウェイデバイスを設定するときは、両方のトンネルを設定することが重要です。

> **Note**
>
> AWS はときどき、仮想プライベートゲートウェイに対して定期的にメンテナンスを実行します。このメンテナンスにより、VPN 接続 の 2 つのトンネルのうち 1 つが短時間無効になることがあります。このメンテナンスの実行中、VPN 接続は自動的に 2 番目のトンネルにフェイルオーバーします。

Internet Key Exchange (IKE) および IPsec Security Associations (SA) についての追加情報が、ダウンロードした設定ファイルに記述されています。

```
MainModeSecMethods:         DHGroup2-AES128-SHA1
MainModeKeyLifetime:        480min,0sess
QuickModeSecMethods:        ESP:SHA1-AES128+60min+100000kb
QuickModePFS:               DHGroup2
```

`MainModeSecMethods`

IKE SA 用の暗号化および認証のアルゴリズムです。これらは、VPN 接続用の推奨設定と、Windows Server IPsec VPN 接続用のデフォルト設定です。

`MainModeKeyLifetime`

IKE SA キーの有効期間です。 これは VPN 接続用の推奨設定であり、Windows Server IPsec VPN 接続用のデフォルト設定です。

`QuickModeSecMethods`

IPsec SA 用の暗号化および認証のアルゴリズムです。これらは、VPN 接続用の推奨設定と、Windows Server IPsec VPN 接続用のデフォルト設定です。

`QuickModePFS`

IPsec セッションにはマスターキー PFS (Perfect Forward Secrecy) を使用することを推奨します。

ステップ 3: Windows Server を設定する

VPN トンネルを設定する前に、Windows Server でルーティングとリモートアクセスサービスをインストールして設定する必要があります。これにより、リモートユーザーがお客様のネットワーク上のリソースにアクセスできるようになります。

ルーティングおよびリモートアクセスサービスをインストールするには

1. Windows Server にログオンします。
2. [Start] メニューに移動し、[Server Manager] を選択します。
3. ルーティングおよびリモートアクセスサービスをインストールします。

    a. [Manage]メニューから、[Add Roles and Features] を選択します。

    b. [Before You Begin] ページで、サーバーが前提条件を満たしていることを確認し、[Next] を選択します。

    c. [Role-based or feature-based installation] を選択し、次に [Next] を選択します。

    d. [Select a server from the server pool] を選択し、Windows Server を選択して [Next] を選択します。

    e. リストで [Network Policy and Access Services] を選択します。表示されるダイアログボックスで、[Add Features] を選択してこのロールに必要な機能を確認します。

    f. 同じリストで、[リモート アクセス]、[次へ] の順に選択します。

    g. [Select features] ページで、[Next] を選択します。

    h. [Network Policy and Access Services] ページで、[Next] を選択します。

    i. [Remote Access] ページで、[Next] を選択します。次のページで、[DirectAccess and VPN (RAS)] を選択します。表示されるダイアログボックスで、[Add Features] を選択してこのロールサービスに必要な機能を確認します。同じリストで、[Routing] を選択し、次に [Next] を選択します。

    j. [Web Server Role (IIS)] ページで、[Next] を選択します。デフォルトの選択のまま残して、[Next] を選択します。

    k. [Install] を選択します。インストールが完了したら、[Close] を選択します。

ルーティングおよびリモートアクセスサーバーを設定して有効にするには

1. ダッシュボードで、[Notifications] (フラグのアイコン) を選択します。デプロイ後の設定を完了するためのタスクが必要になる場合があります。[Open the Getting Started Wizard] リンクを選択します。
2. [Deploy VPN only] を選択します。
3. [Routing and Remote Access] ダイアログボックスで、サーバー名を選択します。さらに [アクション] を選択して [Configure and Enable Routing and Remote Access (Routing and Remote Access の設定と有効化)] を選択します。
4. [Routing and Remote Access Server Setup Wizard] の最初のページで、[Next] を選択します。
5. [構成] ページで、[カスタム構成]、[次へ] の順に選択します。
6. [LAN ルーティング]、[次へ]、[完了] の順に選択します。
7. [Routing and Remote Access] ダイアログボックスにメッセージが表示されたら、[Start service] を選択します。

ステップ 4: VPN トンネルを設定する

ダウンロードした設定ファイルに含まれている netsh スクリプトを実行するか、Windows Server のユーザーインターフェイスを使用して、VPN トンネルを設定できます。

> **Important**
>
> IPsec セッションにはマスターキー PFS (Perfect Forward Secrecy) を使用することを推奨します。 netsh スクリプトを実行することを選択した場合、スクリプトには PFSを有効にするためのパラメータ (`qmpfs=dhgroup2`) が含まれています。Windows のユーザーインターフェイスを使用して PFS を有効にすることはできません。コマンドラインを使用して有効にする必要があります。

Options

- オプション 1: netsh スクリプトを実行する
- オプション 2: Windows Server ユーザーインターフェイスを使用する

オプション 1: netsh スクリプトを実行する

ダウンロードした設定ファイルから netsh スクリプトをコピーし、変数を置き換えます。スクリプトの例を次に示します。

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsakwcdoR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

[Name]: 推奨された名前 (`vgw-1a2b3c4d Tunnel 1`)) を選択した名前で置き換えることができます。

[LocalTunnelEndpoint]: ネットワークの Windows Server のプライベート IP アドレスを入力します。

[Endpoint1]: Windows Server が存在するネットワークの CIDR ブロック (たとえば、`172.31.0.0/16`) です。この値を二重引用符 (") で囲みます。

[Endpoint2]: VPC または VPC のサブネットの CIDR ブロック (たとえば、`10.0.0.0/16`) です。この値を二重引用符 (") で囲みます。

更新したスクリプトを Windows Server のコマンドプロンプトウィンドウで実行します。(^ を使用すると、コマンド行で折り返しテキストの切り取りと貼り付けができます)。 この VPN 接続に 2 番目の VPN トンネルを設定するには、設定ファイルにある 2 番目の netsh スクリプトを使用してこのプロセスを繰り返します。

作業が終了したら、「Windows ファイアウォールを設定する」を参照してください。

netsh パラメータの詳細については、Microsoft TechNet ライブラリの Netsh AdvFirewall Consec Commands を参照してください。

オプション 2: Windows Server ユーザーインターフェイスを使用する

Windows Server ユーザーインターフェイスを使用して VPN トンネルを設定することもできます。

> **Important**
>
> Windows Server ユーザーインターフェイスを使用してマスターキー PFS (Perfect Forward Secrecy) を有効にすることはできません。PFS を有効にするには、「マスターキー PFS (Perfect Forward Secrecy) を有効にする」で説明されているように、コマンドラインを使う必要があります。

タスク

- VPN トンネル用のセキュリティルールを設定する
- トンネルの設定を確認する
- マスターキー PFS (Perfect Forward Secrecy) を有効にする
- Windows ファイアウォールを設定する

VPN トンネル用のセキュリティルールを設定する

このセクションでは、Windows Server のセキュリティルールを設定して VPN トンネルを作成します。

VPN トンネル用のセキュリティルールを設定するには

1. Server Manager を開き、[Tools] を選択し、[Windows Defender Firewall with Advanced Security] を選択します。
2. [Connection Security Rules] を選択し、[Action] を選択して [New Rule] を選択します。
3. [New Connection Security Rule] ウィザードの [Rule Type] ページで、[Tunnel] を選択し、[Next] を選択します。
4. [Tunnel Type] ページの [What type of tunnel would you like to create] で、[Custom Configuration] を選択します。[Would you like to exempt IPsec-protected connections from this tunnel] で、デフォルト値を選択したまま ([No. Send all network traffic that matches this connection security rule through the tunnel]) にして、[Next] を選択します。
5. [Requirements] ページで、[Require authentication for inbound connections.Do not establish tunnels for outbound connections] を選択し、[Next] を選択します。
6. [Tunnel Endpoints (トンネルエンドポイント)] ページの [Which computers are in Endpoint 1 (Endpoint 1 のコンピュータ)] で、[Add (追加)] を選択します。ネットワーク (Windows Server カスタマーゲートウェイデバイスの背後にある) の CIDR 範囲 (`172.31.0.0/16` など) を入力し、

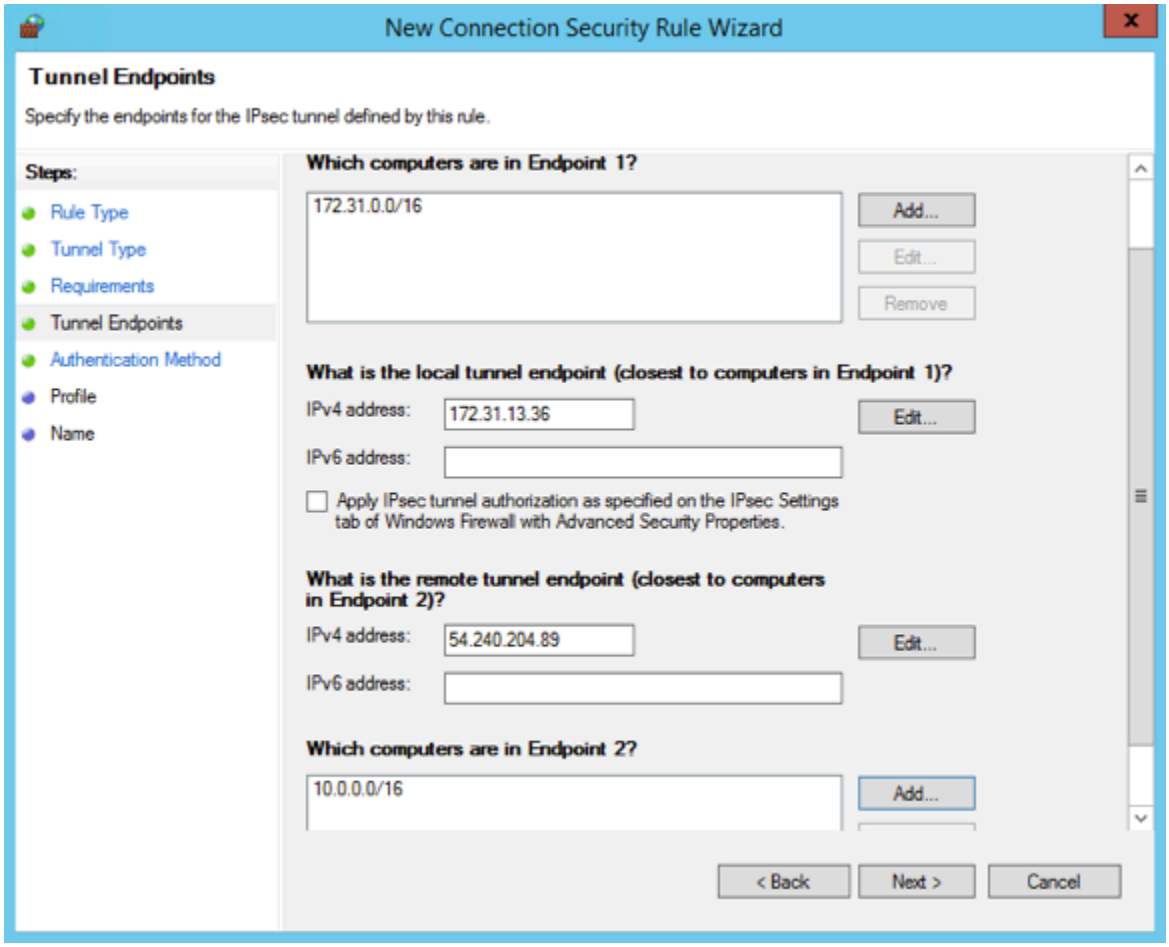
[OK] を選択します。この範囲にはカスタマーゲートウェイデバイスの IP アドレスを含めることができます。

7. [What is the local tunnel endpoint (closest to computer in Endpoint 1)] で、[Edit] を選択します。[IPv4 address] フィールドに Windows Server のプライベート IP アドレスを入力し、[OK] を選択します。
8. [What is the remote tunnel endpoint (closest to computers in Endpoint 2)] で、[Edit] を選択します。[IPv4 address] フィールドに、設定ファイルにあるトンネル 1 の仮想プライベートゲートウェイの IP アドレス (「`Remote Tunnel Endpoint`」を参照) を入力し、[OK] を選択します。

> **Important**
>
> トンネル 2 に対してこの手順を繰り返す場合は、トンネル 2 のエンドポイントを選択してください。

9. [Which computers are in Endpoint 2] で、[Add] を選択します。[This IP address or subnet field] に VPC の CIDR ブロックを入力して、[OK] を選択します。

> **Important**
>
> [Which computers are in Endpoint 2] が表示されるまでダイアログボックスをスクロールします。このステップが完了するまで、[Next] を選択しないでください。サーバーに接続できなくなります。



10. 指定したすべての設定が正しいことを確認し、[次へ] を選択します。
11. [認証方法] ページで、[詳細設定]、[カスタマイズ] の順に選択します。
12. [First authentication methods] で、[Add] を選択します。
13. [Preshared key (事前共有キー)] を選択し、設定ファイルにある事前共有キーの値を入力して、[OK] を選択します。

> **Important**
>
> トンネル 2 に対してこの手順を繰り返す場合は、トンネル 2 の事前共有キーを選択してください。

14. [First authentication is optional] が選択されていないことを確認し、[OK] を選択します。
15. [次へ] を選択します。

16. [プロファイル] ページで、[ドメイン]、[プライベート]、[パブリック] の 3 つのチェックボックスをすべてオンにします。[次へ] を選択します。
17. [Name] ページで、接続ルールの名前 (`VPN to Tunnel 1` など) を入力し、[完了] を選択します。

上記の手順を繰り返し、設定ファイルにあるトンネル 2 のデータを指定します。

完了すると、VPN 接続に 2 つのトンネルが設定されます。

トンネルの設定を確認する

トンネルの設定を確認するには

1. Server Manager を開き、[Tools] を選択して、[Windows Firewall with Advanced Security] を選択します。次に [Connection Security Rules] を選択します。
2. 両方のトンネルについて次の設定を確認します。
   - [Enabled] は `Yes`。
   - [Endpoint 1] はネットワークの CIDR ブロックです。
   - [Endpoint 2] は VPC の CIDR ブロックです。
   - 認証モード は `Require inbound and clear outbound` です
   - [Authentication method] は `Custom`。
   - [Endpoint 1 port] は `Any`。
   - [Endpoint 2 port] は `Any`。
   - [Protocol] は `Any`。
3. 最初のルールを選択し、[Properties] を選択します。
4. [Authentication (認証)] タブの [Method (方法)] で、[Customize (カスタマイズ)] を選択します。[First authentication methods (最初の認証方法)] に、設定ファイルにあるトンネルの正しい事前共有キーが指定されていることを確認し、[OK] を選択します。
5. [Advanced] タブで、[Domain]、[Private]、および [Public] がすべて選択されていることを確認します。
6. [IPsec tunneling] の [Customize] を選択します。IPsec トンネリングが次のように設定されていることを確認して [OK] を選択します。再度 [OK] を選択してダイアログボックスを閉じます。
   - [Use IPsec tunneling] が選択されている。

- [Local tunnel endpoint (closest to Endpoint 1)] に、Windows Server の IP アドレスが設定されている。カスタマーゲートウェイデバイスが EC2 インスタンスである場合、これはインスタンスのプライベート IP アドレスです。
- [Remote tunnel endpoint (closest to Endpoint 2)] に、このトンネルの仮想プライベートゲートウェイの IP アドレスが設定されている。

7. 2 番目のトンネルのプロパティを開きます。このトンネルに対してステップ 4 から 7 までを繰り返します。

マスターキー PFS (Perfect Forward Secrecy) を有効にする

マスターキー PFS (Perfect Forward Secrecy) を有効にするにはコマンドラインを使用できます。ユーザーインターフェイスを使用してこの機能を有効にすることはできません。

マスターキー PFS (Perfect Forward Secrecy) を有効にするには

1. Windows Server で、新しいコマンドプロンプトウィンドウを開きます。
2. 次のコマンドを入力します。`rule_name` は最初の接続ルールに指定した名前に置き換えます。

```
netsh advfirewall consec set rule name="rule_name" new QMPFS=dhgroup2
 QMSecMethods=ESP:SHA1-AES128+60min+100000kb
```

3. 2 番目のトンネルにステップ 2 を繰り返します。今回は `rule_name` を 2 番目の接続ルールに指定した名前に置き換えます。

Windows ファイアウォールを設定する

サーバーのセキュリティルールを設定した後、仮想プライベートゲートウェイと連動するように基本的な IPsec 設定を行います。

Windows ファイアウォールを設定するには

1. Server Manager を開き、[Tools] を選択して [Windows Defender Firewall with Advanced Security] を選択します。次に [Properties] を選択します。
2. [IPsec Settings] タブの [IPsec exemptions] で、[Exempt ICMP from IPsec] が [No (default)] になっていることを確認します。[IPsec tunnel authorization] が [None] であることを確認します。
3. [IPsec defaults] の [Customize] を選択します。
4. [Key exchange (Main Mode)] の [Advanced] を選択し、[Customize] を選択します。

5. [Customize Advanced Key Exchange Settings (キー交換の詳細設定のカスタマイズ)] の [Security Method (セキュリティメソッド)] で、最初のエントリに次のデフォルト値が使用されていることを確認します。

   - 整合性: SHA-1
   - 暗号化: AES-CBC 128
   - キー交換アルゴリズム: Diffie-Hellman Group 2
   - [Key lifetimes] で、[Minutes] が `480` で [Sessions] が `0` であることを確認します。

   これらの設定は、設定ファイルの次のエントリに対応します。

   ```
   MainModeSecMethods: DHGroup2-AES128-SHA1,DHGroup2-3DES-SHA1
   MainModeKeyLifetime: 480min,0sec
   ```

6. [Key exchange options] の [Use Diffie-Hellman for enhanced security] を選択し、[OK] を選択します。
7. [Data protection (Quick Mode)] の [Advanced] を選択し、[Customize] を選択します。
8. [Require encryption for all connection security rules that use these settings] を選択します。
9. [Data integrity and encryption] は次のようにデフォルト値のままにします。

   - プロトコル: ESP
   - 整合性: SHA-1
   - 暗号化: AES-CBC 128
   - 有効期間: 60 分

   これらの値は設定ファイルの以下のエントリに対応します。

   ```
   QuickModeSecMethods:
   ESP:SHA1-AES128+60min+100000kb
   ```

10. [OK] を選択して [IPsec の設定のカスタマイズ] ダイアログボックスに戻り、再度 [OK] を選択して設定を保存します。

ステップ 5: 停止しているゲートウェイの検出を有効にする

次に、ゲートウェイが使用できなくなったら検出するように TCP を設定します。それには、レジストリキー `HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters` を変更します。このステップは、これより前のセクションを完了してから実行してください。レジストリキーの変更後、サーバーを再起動する必要があります。

停止しているゲートウェイを検出するには

1. Windows Server でコマンドプロンプトまたは PowerShell セッションを起動し、regedit と入力してレジストリエディタを起動します。
2. [HKEY_LOCAL_MACHINE]、[SYSTEM]、[CurrentControlSet]、[Services]、[Tcpip]、[Parameters] の順に展開します。
3. [Edit] メニューの [New] を選択し、[DWORD (32-bit) Value] を選択します。
4. 名前として [EnableDeadGWDetect] を入力します。
5. [EnableDeadGWDetect] を選択してから、[編集] メニューの [変更] を選択します。
6. [Value data] に「1」と入力し、[OK] を選択します。
7. レジストリエディタを終了し、サーバーを再起動します。

詳細については、Microsoft TechNet Library の「EnableDeadGWDetect」を参照してください。

ステップ 6: VPN 接続をテストする

VPN 接続が正常に動作していることテストするには、インスタンスを VPC 内で起動し、インターネットに接続されていないことを確認します。インスタンスを起動した後、Windows Server からプライベート IP アドレスに対して ping を実行します。VPN トンネルは、カスタマーゲートウェイデバイスからトラフィックが生成されるときに開始されます。したがって、ping コマンドも VPN 接続を開始します。

VPN 接続をテストするステップについては、「Site-to-Site VPN 接続をテストする」を参照してください。

`ping` コマンドが失敗した場合、次の情報を確認します。

- VPC 内のインスタンスに対して ICMP が許容されるように、セキュリティグループのルールが設定されていることを確認します。Windows Server が EC2 インスタンスである場合は、セキュリティグループのアウトバウンドルールで IPsec トラフィックが許可されていることを確認します。詳細については、「Windows インスタンスの設定」を参照してください。

- ping 対象のインスタンスのオペレーティングシステムが ICMP に応答するように設定されていることを確認します。Amazon Linux AMI のいずれかを使用することをお勧めします。
- ping 対象のインスタンスが Windows インスタンスである場合は、そのインスタンスに接続し、Windows ファイアウォールでインバウンド ICMPv4 を有効にします。
- VPC またはサブネットのルートテーブルが正しく設定されていることを確認します。詳細については、「 ステップ 1: VPN 接続を作成し、VPC を設定する」を参照してください。
- カスタマーゲートウェイデバイスが EC2 インスタンスである場合は、インスタンスに対して送信元/送信先チェックが無効になっていることを確認します。詳細については、「Windows インスタンスの設定」を参照してください。

Amazon VPC コンソールの [VPN Connections] ページで、使用している VPN 接続を選択します。1 番目のトンネルは起動状態です。2 番目のトンネルは、最初のトンネルが停止するまで使用されませんが、設定は必要です。暗号化されたトンネルを確立するのに数分かかることがあります。

カスタマーゲートウェイデバイスのトラブルシューティング

次のトピックは、カスタマーゲートウェイデバイスの接続の問題のトラブルシューティングに役立ちます。

一般的なテストの説明については、「Site-to-Site VPN 接続をテストする」を参照してください。

このセクションのトピック以外にも、AWS Site-to-Site VPN ログを使用すると、VPN 接続の問題のトラブルシューティングや解決に役立つ場合があります。

トピック

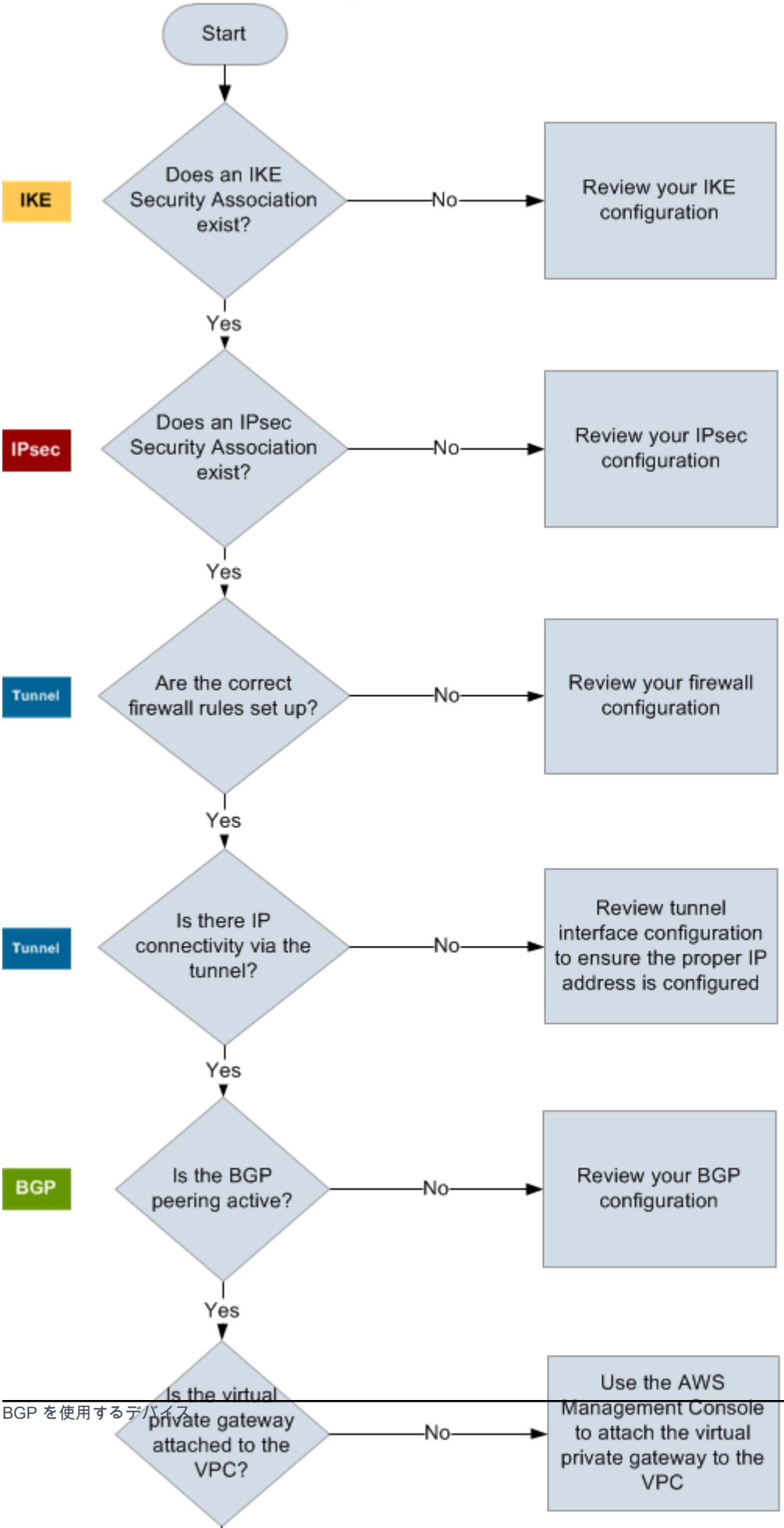
- ボーダーゲートウェイプロトコルを使用する場合の接続のトラブルシューティング
- ボーダーゲートウェイプロトコルを使用しない接続のトラブルシューティング
- Cisco ASA カスタマーゲートウェイデバイスの接続のトラブルシューティング
- Cisco IOS カスタマーゲートウェイデバイスの接続のトラブルシューティング
- ボーダーゲートウェイプロトコル接続を使用しない Cisco IOS カスタマーゲートウェイデバイスのトラブルシューティング
- Juniper JunOS カスタマーゲートウェイデバイスの接続のトラブルシューティング
- Juniper ScreenOS カスタマーゲートウェイデバイスの接続のトラブルシューティング
- Yamaha 製カスタマーゲートウェイデバイスの接続のトラブルシューティング

その他のリソース

- Amazon VPC フォーラム
- Amazon VPC への VPN トンネル接続の問題をトラブルシューティングするにはどうすればよいですか?

ボーダーゲートウェイプロトコルを使用する場合の接続のトラブルシューティング

次の図と表は、ボーダーゲートウェイプロトコル (BGP) を使用するカスタマーゲートウェイデバイスをトラブルシューティングする、一般的な手順を示しています。また、デバイスのデバッグ機能を有効にすることをお勧めします。詳細については、ゲートウェイデバイスのベンダーに問い合わせてください。

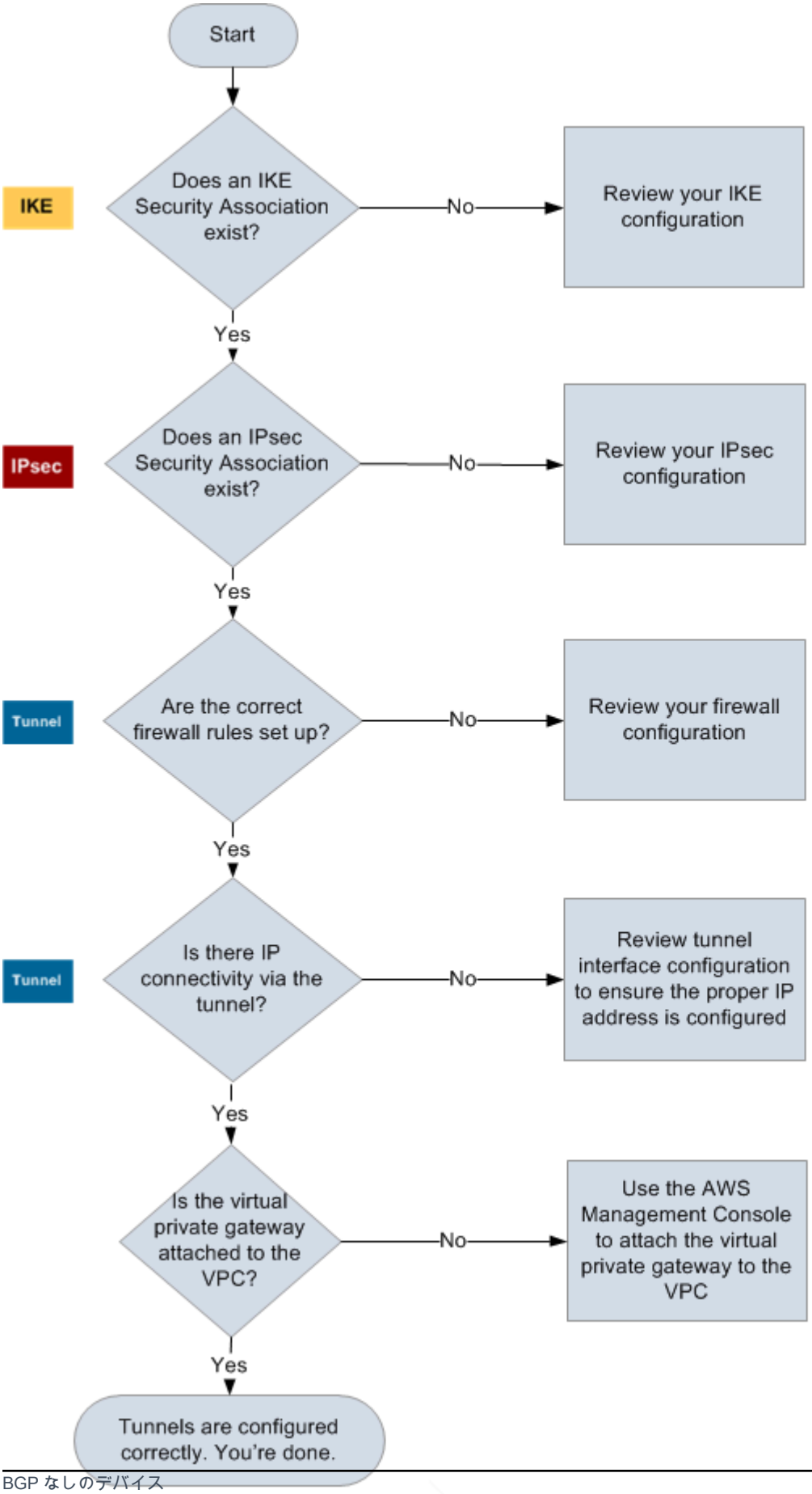

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
BGP
Is the BGP peering active?
No
Review your BGP configuration
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC

IKE	IKE Security Association が存在するかどうかを確認します。 IKE Security Association は、IPsec Security Association を確立するために使用されるキーの交換に必要です。 IKE Security Association がない場合は、IKE 設定を確認します。設定ファイルに示されている、暗号化、認証、Perfect Forward Secrecy、およびモードのパラメータを設定する必要があります。 IKE Security Association が存在する場合は、「IPsec」に進みます。
IPsec	IPsec Security Association (SA) が存在するかどうかを確認します。 IPsec SA はトンネル自体です。カスタマーゲートウェイデバイスにクエリを実行し、IPsec SA がアクティブかどうかを確認します。設定ファイルに示されている、暗号化、認証、Perfect Forward Secrecy、およびモードのパラメータが設定されていることを確認します。 IPsec SA が存在しない場合は、IPsec 設定を確認します。 IPsec SA が存在する場合は、「トンネル」に進みます。
トンネル	必須のファイアウォールルールがセットアップされていることを確認します (ルールのリストについては、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照)。セットアップされている場合は、次に進みます。 トンネル経由の IP 接続があるかどうかを確認します。 トンネルのそれぞれの側に、設定ファイルで指定された IP アドレスが含まれます。仮想プライベートゲートウェイアドレスは、BGP ネイバーアドレスとして使用されます。カスタマーゲートウェイデバイスから、このアドレスに対する ping を実行し、IP トラフィックが正しく暗号化および復号化されているかどうかを確認します。 ping が失敗した場合は、トンネルインターフェイス設定を確認し、正しい IP アドレスが設定されていることを確認します。 ping が成功した場合は、「BGP」に進みます。

BGP	BGP ピアリングセッションがアクティブかどうかを確認します。 各トンネルについて、以下を実行します。 • カスタマーゲートウェイデバイスで、BGP ステータスが `Active` または `Established` であるかどうかを確認します。BGP ピアがアクティブになるまで約 30 秒かかる場合があります。 • カスタマーゲートウェイデバイスが仮想プライベートゲートウェイへのデフォルトルート (0.0.0.0/0) をアドバタイズしていることを確認します。 トンネルがこの状態にない場合は、BGP 設定を確認します。 BGP ピアが確立された場合は、プレフィックスを受け取り、プレフィックスをアドバタイズして、トンネルが正しく設定されます。両方のトンネルがこの状態であることを確認します。

ボーダーゲートウェイプロトコルを使用しない接続のトラブルシューティング

次の図と表は、ボーダーゲートウェイプロトコル (BGP) を使用しないカスタマーゲートウェイデバイスをトラブルシューティングする、一般的な手順を示しています。また、デバイスのデバッグ機能を有効にすることをお勧めします。詳細については、ゲートウェイデバイスのベンダーに問い合わせてください。


Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the tunnel?
No
Review tunnel interface configuration to ensure the proper IP address is configured
Yes
Is the virtual private gateway attached to the VPC?
No
Use the AWS Management Console to attach the virtual private gateway to the VPC
Yes
Tunnels are configured correctly. You're done.

IKE	IKE Security Association が存在するかどうかを確認します。 IKE Security Association は、IPsec Security Association を確立するために使用されるキーの交換に必要です。 IKE Security Association がない場合は、IKE 設定を確認します。設定ファイルに示されている、暗号化、認証、Perfect Forward Secrecy、およびモードのパラメータを設定する必要があります。 IKE Security Association が存在する場合は、「IPsec」に進みます。
IPsec	IPsec Security Association (SA) が存在するかどうかを確認します。 IPsec SA はトンネル自体です。カスタマーゲートウェイデバイスにクエリを実行し、IPsec SA がアクティブかどうかを確認します。設定ファイルに示されている、暗号化、認証、Perfect Forward Secrecy、およびモードのパラメータが設定されていることを確認します。 IPsec SA が存在しない場合は、IPsec 設定を確認します。 IPsec SA が存在する場合は、「トンネル」に進みます。
トンネル	必須のファイアウォールルールがセットアップされていることを確認します (ルールのリストについては、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照)。セットアップされている場合は、次に進みます。 トンネル経由の IP 接続があるかどうかを確認します。 トンネルのそれぞれの側に、設定ファイルで指定された IP アドレスが含まれます。仮想プライベートゲートウェイアドレスは、BGP ネイバーアドレスとして使用されます。カスタマーゲートウェイデバイスから、このアドレスに対する ping を実行し、IP トラフィックが正しく暗号化および復号化されているかどうかを確認します。 ping が失敗した場合は、トンネルインターフェイス設定を確認し、正しい IP アドレスが設定されていることを確認します。 ping が成功した場合は、「静的ルート」に進みます。

静的ルート	各トンネルについて、以下を実行します。 • トンネルで次のホップとして VPC CIDR への静的ルートが追加されていることを確認します。 • Amazon VPC コンソールで静的ルートが追加されていることを確認し、トラフィックを内部ネットワークにルーティングするように仮想プライベートゲートウェイに指示します。 トンネルがこの状態にない場合は、デバイス設定を確認します。 トンネルがいずれもこの状態であることを確認したら、終了です。

Cisco ASA カスタマーゲートウェイデバイスの接続のトラブルシューティング

Cisco のカスタマーゲートウェイデバイスの接続をトラブルシューティングする場合は、IKE、IPsec、ルーティングを考慮します。これらの領域を任意の順序でトラブルシューティングできますが、IKE から (ネットワークスタックの下から) 開始して上に進むことをお勧めします。

> **Important**
>
> 一部の Cisco ASA ではアクティブ/スタンバイモードのみがサポートされています。これらの Cisco ASA を使用する場合は、アクティブなトンネルを一度に 1 個のみ保持できます。最初のトンネルが利用不可になった場合にのみ、他方のスタンバイトンネルがアクティブになります。スタンバイトンネルは、ログファイルで次のエラーを生成する場合がありますが、このエラーは無視できます。`Rejecting IPSec tunnel: no matching crypto map entry for remote proxy 0.0.0.0/0.0.0.0/0/0 local proxy 0.0.0.0/0.0.0.0/0/0 on interface outside`

IKE

以下のコマンドを使用します。このレスポンスは、IKE が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
ciscoasa# show crypto isakmp sa
```

```
   Active SA: 2
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 2

1   IKE Peer: AWS_ENDPOINT_1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

トンネル内で指定されたリモートゲートウェイの src 値を含む 1 つ以上の行が表示されます。state は MM_ACTIVE、status は ACTIVE となります。エントリがない場合、またはエントリが別の状態になっている場合は、IKE が正しく設定されていないことを示しています。

さらにトラブルシューティングする場合は、次のコマンドを実行して診断情報を提供するログメッセージを有効にします。

```
router# term mon
router# debug crypto isakmp
```

デバッグを無効にするには、次のコマンドを使用します。

```
router# no debug crypto isakmp
```

IPsec

以下のコマンドを使用します。このレスポンスは、IPsec が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
ciscoasa# show crypto ipsec sa
```

```
interface: outside
    Crypto map tag: VPN_crypto_map_name, seq num: 2, local addr: 172.25.50.101

      access-list integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
      current_peer: integ-ppe1

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
      #pkts compressed: 0, #pkts decompressed: 0
```

```
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.25.50.101, remote crypto endpt.: AWS_ENDPOINT_1

      path mtu 1500, ipsec overhead 74, media mtu 1500
      current outbound spi: 6D9F8D3B
      current inbound spi : 48B456A6

    inbound esp sas:
      spi: 0x48B456A6 (1219778214)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
    outbound esp sas:
      spi: 0x6D9F8D3B (1839172923)
         transform: esp-aes esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 2, }
         slot: 0, conn_id: 4710400, crypto-map: VPN_cry_map_1
         sa timing: remaining key lifetime (kB/sec): (4374000/3593)
         IV size: 16 bytes
         replay detection support: Y
         Anti replay bitmap:
         0x00000000 0x00000001
```

各トンネルインターフェイスに対して、`inbound esp sas` と `outbound esp sas` がいずれも表示されます。これは、SA が示され (例: `spi: 0x48B456A6`)、IPsec が正しく設定されていることを前提としています。

Cisco ASA では、IPsec は、対象となるトラフィック (暗号化する必要があるトラフィック) が送信された場合にのみ表示されます。IPsec を常にアクティブにするには、SLA モニターを設定することをお勧めします。SLA モニターは、対象となるトラフィックを引き続き送信し、IPsec を常にアクティブにします。

また、次の ping コマンドを使用して、ネゴシエーションを開始して上に移動することを IPsec に強制することもできます。

```
ping ec2_instance_ip_address
```

```
Pinging ec2_instance_ip_address with 32 bytes of data:

Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: bytes=32 time<1ms TTL=128
Reply from ec2_instance_ip_address: 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
```

さらにトラブルシューティングする場合は、次のコマンドを使用してデバッグを有効にします。

```
router# debug crypto ipsec
```

デバッグを無効にするには、次のコマンドを使用します。

```
router# no debug crypto ipsec
```

ルーティング

トンネルのもう一方の端で ping を実行します。機能している場合は、IPsec を確立する必要があります。機能していない場合は、アクセスリストを確認し、前の IPsec セクションを参照します。

インスタンスに到達できない場合は、次の情報を確認します。

1. アクセスリストが、暗号化マップに関連付けられたトラフィックを許可するように設定されていることを確認します。

   これを行うには、次のコマンドを実行します。

   ```
   ciscoasa# show run crypto
   ```

   ```
   crypto ipsec transform-set transform-amzn esp-aes esp-sha-hmac
   crypto map VPN_crypto_map_name 1 match address access-list-name
   crypto map VPN_crypto_map_name 1 set pfs
   crypto map VPN_crypto_map_name 1 set peer AWS_ENDPOINT_1 AWS_ENDPOINT_2
   ```

```
crypto map VPN_crypto_map_name 1 set transform-set transform-amzn
crypto map VPN_crypto_map_name 1 set security-association lifetime seconds 3600
```

2. 次のコマンドを使用して、アクセスリストを確認します。

```
ciscoasa# show run access-list access-list-name
```

```
access-list access-list-name extended permit ip any vpc_subnet subnet_mask
```

3. アクセスリストが正しいことを確認します。次のアクセスリスト例では、VPC サブネット 10.0.0.0/16 へのすべての内部トラフィックを許可しています。

```
access-list access-list-name extended permit ip any 10.0.0.0 255.255.0.0
```

4. Cisco ASA デバイスから traceroute を実行し、Amazon ルーター (たとえば、*AWS_ENDPOINT_1*/*AWS_ENDPOINT_2*) に到達するかどうかを確認します。

   これが Amazon ルーターに到達したら、Amazon VPC コンソールで追加した静的ルートと、特定のインスタンスのセキュリティグループを確認します。

5. さらにトラブルシューティングする場合は、設定を確認します。

Cisco IOS カスタマーゲートウェイデバイスの接続のトラブルシューティング

Cisco のカスタマーゲートウェイデバイスの接続をトラブルシューティングする場合は、IKE、IPsec、トンネル、BGP の 4 つの要素を考慮します。これらの領域を任意の順序でトラブルシューティングできますが、IKE から (ネットワークスタックの下から) 開始して上に進むことをお勧めします。

IKE

以下のコマンドを使用します。このレスポンスは、IKE が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
192.168.37.160  72.21.209.193   QM_IDLE           2001    0 ACTIVE
```

```
192.168.37.160  72.21.209.225   QM_IDLE           2002    0 ACTIVE
```

トンネル内で指定されたリモートゲートウェイの src 値を含む 1 つ以上の行が表示されます。state は QM_IDLE、status は ACTIVE となります。エントリがない場合、またはエントリが別の状態になっている場合は、IKE が正しく設定されていないことを示しています。

さらにトラブルシューティングする場合は、次のコマンドを実行して診断情報を提供するログメッセージを有効にします。

```
router# term mon
router# debug crypto isakmp
```

デバッグを無効にするには、次のコマンドを使用します。

```
router# no debug crypto isakmp
```

IPsec

以下のコマンドを使用します。このレスポンスは、IPsec が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 192.168.37.160

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

     local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.225
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
     current outbound spi: 0xB8357C22(3090512930)
```

```
     inbound esp sas:
      spi: 0x6ADB173(112046451)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB8357C22(3090512930)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
       sa timing: remaining key lifetime (k/sec): (4467148/3189)
       IV size: 16 bytes
       replay detection support: Y  replay window size: 128
       Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:

interface: Tunnel2
     Crypto map tag: Tunnel2-head-0, local addr 174.78.144.73

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 72.21.209.193 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
     #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0
```

```
      local crypto endpt.: 174.78.144.73, remote crypto endpt.: 72.21.209.193
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
      current outbound spi: 0xF59A3FF6(4120526838)

      inbound esp sas:
       spi: 0xB6720137(3060924727)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xF59A3FF6(4120526838)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
        sa timing: remaining key lifetime (k/sec): (4387273/3492)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:
```

各トンネルインターフェイスに対して、`inbound esp sas` と `outbound esp sas` がいずれも表示されます。SA が示され (例: `spi: 0xF95D2F3C`)、`Status` が `ACTIVE` となっていれば、IPsec は正しく設定されています。

さらにトラブルシューティングする場合は、次のコマンドを使用してデバッグを有効にします。

```
router# debug crypto ipsec
```

次のコマンドを使用して、デバッグを無効にします。

```
router# no debug crypto ipsec
```

トンネル

最初に、必要なファイアウォールルールがあることを確認します。詳細については、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照してください。

ファイアウォールルールが正しくセットアップされた場合は、次のコマンドでトラブルシューティングを継続します。

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

`line protocol` が実行されていることを確認します。トンネルのソース IP アドレス、ソースインターフェイス、および宛先がそれぞれ、IP アドレス外部のカスタマーゲートウェイデバイス、インターフェイス、および IP アドレス外部の仮想プライベートゲートウェイのトンネル設定に対応することを確認します。`Tunnel protection via IPSec` が存在することを確認します。両方のトン

ネルインターフェイスでコマンドを実行します。問題を解決するには、設定を確認し、カスタマーゲートウェイデバイスへの物理的な接続を確認します。

また、次のコマンドを使用して、169.254.255.1 を仮想プライベートゲートウェイの内部 IP アドレスで置き換えます。

```
router# ping 169.254.255.1 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.255.1, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

5 個の感嘆符が表示されます。

さらにトラブルシューティングする場合は、設定を確認します。

BGP

以下のコマンドを使用します。

```
router# show ip bgp summary
```

```
BGP router identifier 192.168.37.160, local AS number 65000
BGP table version is 8, main routing table version 8
2 network entries using 312 bytes of memory
2 path entries using 136 bytes of memory
3/1 BGP path/bestpath attribute entries using 444 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 32 bytes of memory
BGP using 948 total bytes of memory
BGP activity 4/1 prefixes, 4/1 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
169.254.255.1   4  7224     363     323        8    0    0 00:54:21        1
169.254.255.5   4  7224     364     323        8    0    0 00:00:24        1
```

両方のネイバーが表示されます。それぞれに対して、1 の State/PfxRcd 値が表示されます。

BGP ピアリングが起動している場合は、カスタマーゲートウェイデバイスが VPC へのデフォルトルート (0.0.0.0/0) をアドバタイズしていることを確認します。

```
router# show bgp all neighbors 169.254.255.1 advertised-routes
```

```
For address family: IPv4 Unicast
BGP table version is 3, local router ID is 174.78.144.73
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
     r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Originating default network 0.0.0.0

Network             Next Hop            Metric   LocPrf Weight Path
*> 10.120.0.0/16    169.254.255.1          100        0   7224    i

Total number of prefixes 1
```

さらに、VPC に対応するプレフィックスを仮想プライベートゲートウェイから受け取っていることを確認します。

```
router# show ip route bgp
```

```
 10.0.0.0/16 is subnetted, 1 subnets
B       10.255.0.0 [20/0] via 169.254.255.1, 00:00:20
```

さらにトラブルシューティングする場合は、設定を確認します。

ボーダーゲートウェイプロトコル接続を使用しない Cisco IOS カスタマーゲートウェイデバイスのトラブルシューティング

Cisco のカスタマーゲートウェイデバイスの接続をトラブルシューティングする場合は、IKE、IPsec、トンネルの 3 つの要素を考慮します。これらの領域を任意の順序でトラブルシューティングできますが、IKE から (ネットワークスタックの下から) 開始して上に進むことをお勧めします。

IKE

以下のコマンドを使用します。このレスポンスは、IKE が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
router# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
174.78.144.73 205.251.233.121 QM_IDLE           2001    0 ACTIVE
174.78.144.73 205.251.233.122 QM_IDLE           2002    0 ACTIVE
```

トンネル内で指定されたリモートゲートウェイの src 値を含む 1 つ以上の行が表示されます。state は QM_IDLE、status は ACTIVE となります。エントリがない場合、またはエントリが別の状態になっている場合は、IKE が正しく設定されていないことを示しています。

さらにトラブルシューティングする場合は、次のコマンドを実行して診断情報を提供するログメッセージを有効にします。

```
router# term mon
router# debug crypto isakmp
```

デバッグを無効にするには、次のコマンドを使用します。

```
router# no debug crypto isakmp
```

IPsec

以下のコマンドを使用します。このレスポンスは、IPsec が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
router# show crypto ipsec sa
```

```
interface: Tunnel1
    Crypto map tag: Tunnel1-head-0, local addr 174.78.144.73

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
    current_peer 72.21.209.225 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 149, #pkts encrypt: 149, #pkts digest: 149
     #pkts decaps: 146, #pkts decrypt: 146, #pkts verify: 146
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
```

```
      #pkts not decompressed: 0, #pkts decompress failed: 0
      #send errors 0, #recv errors 0

      local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.121
      path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
      current outbound spi: 0xB8357C22(3090512930)

      inbound esp sas:
       spi: 0x6ADB173(112046451)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: Motorola SEC 2.0:1, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xB8357C22(3090512930)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2, flow_id: Motorola SEC 2.0:2, crypto map: Tunnel1-head-0
        sa timing: remaining key lifetime (k/sec): (4467148/3189)
        IV size: 16 bytes
        replay detection support: Y  replay window size: 128
        Status: ACTIVE

      outbound ah sas:

      outbound pcp sas:

interface: Tunnel2
      Crypto map tag: Tunnel2-head-0, local addr 205.251.233.122

      protected vrf: (none)
      local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer 72.21.209.193 port 500
       PERMIT, flags={origin_is_acl,}
      #pkts encaps: 26, #pkts encrypt: 26, #pkts digest: 26
```

```
    #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

    local crypto endpt.: 174.78.144.73, remote crypto endpt.:205.251.233.122
    path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0
    current outbound spi: 0xF59A3FF6(4120526838)

    inbound esp sas:
     spi: 0xB6720137(3060924727)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 3, flow_id: Motorola SEC 2.0:3, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

    outbound esp sas:
     spi: 0xF59A3FF6(4120526838)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 4, flow_id: Motorola SEC 2.0:4, crypto map: Tunnel2-head-0
      sa timing: remaining key lifetime (k/sec): (4387273/3492)
      IV size: 16 bytes
      replay detection support: Y  replay window size: 128
      Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
```

各トンネルインターフェイスに対して、インバウンドの esp sas とアウトバウンドの esp sas がいずれも表示されます。これは、SA が示され (例: spi: 0x48B456A6)、ステータスが ACTIVE で、IPsec が正しく設定されていることを前提としています。

さらにトラブルシューティングする場合は、次のコマンドを使用してデバッグを有効にします。

```
router# debug crypto ipsec
```

デバッグを無効にするには、次のコマンドを使用します。

```
router# no debug crypto ipsec
```

トンネル

最初に、必要なファイアウォールルールがあることを確認します。詳細については、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照してください。

ファイアウォールルールが正しくセットアップされた場合は、次のコマンドでトラブルシューティングを継続します。

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

line protocol が実行されていることを確認します。トンネルのソース IP アドレス、ソースインターフェイス、および宛先がそれぞれ、IP アドレス外部のカスタマーゲートウェイデバイス、インターフェイス、および IP アドレス外部の仮想プライベートゲートウェイのトンネル設定に対応することを確認します。Tunnel protection through IPSec が存在することを確認します。両方のトンネルインターフェイスでコマンドを実行します。問題を解決するには、設定を確認し、カスタマーゲートウェイデバイスへの物理的な接続を確認します。

また、次のコマンドを使用して、169.254.249.18 を仮想プライベートゲートウェイの内部 IP アドレスで置き換えます。

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
```

5 個の感嘆符が表示されます。

ルーティング

静的ルートテーブルを表示するには、次のコマンドを使用します。

```
router# sh ip route static
```

```
     1.0.0.0/8 is variably subnetted
S       10.0.0.0/16 is directly connected, Tunnel1
is directly connected, Tunnel2
```

両方のトンネルを経由した VPC CIDR の静的ルートが存在していることを確認します。存在しない場合は、次に示すように静的ルートを追加します。

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

SLA モニターの確認

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

```
IPSLAs Latest Operation Statistics

IPSLA operation id: 200
        Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul  15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

Number of successes の値は、SLA モニターが正常にセットアップされたかどうかを示します。

さらにトラブルシューティングする場合は、設定を確認します。

Juniper JunOS カスタマーゲートウェイデバイスの接続のトラブルシューティング

Juniper のカスタマーゲートウェイデバイスの接続をトラブルシューティングする場合は、IKE、IPsec、トンネル、BGP の 4 つの要素を考慮します。これらの領域を任意の順序でトラブルシューティングできますが、IKE から (ネットワークスタックの下から) 開始して上に進むことをお勧めします。

IKE

以下のコマンドを使用します。このレスポンスは、IKE が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
user@router> show security ike security-associations
```

```
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       72.21.209.225   UP     c4cd953602568b74  0d6d194993328b02  Main
3       72.21.209.193   UP     b8c8fb7dc68d9173  ca7cb0abaedeb4bb  Main
```

トンネル内で指定されたリモートゲートウェイのリモートアドレスを含む 1 つ以上の行が表示されます。State は UP になっている必要があります。エントリがない場合、またはエントリが別の状態になっている場合 (DOWN など) は、IKE が正しく設定されていないことを示しています。

さらにトラブルシューティングする場合は、設定ファイルの例で推奨されているように、IKE トレースオプションを有効にします。次に、以下のコマンドを実行すると、さまざまなデバッグメッセージが画面に表示されます。

```
user@router> monitor start kmd
```

外部ホストから、次のコマンドでログファイル全体を取得できます。

```
scp username@router.hostname:/var/log/kmd
```

IPsec

以下のコマンドを使用します。このレスポンスは、IPsec が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
user@router> show security ipsec security-associations
```

```
Total active tunnels: 2
ID      Gateway        Port  Algorithm        SPI      Life:sec/kb Mon vsys
<131073 72.21.209.225  500   ESP:aes-128/sha1 df27aae4 326/ unlim   -   0
>131073 72.21.209.225  500   ESP:aes-128/sha1 5de29aa1 326/ unlim   -   0
<131074 72.21.209.193  500   ESP:aes-128/sha1 dd16c453 300/ unlim   -   0
>131074 72.21.209.193  500   ESP:aes-128/sha1 c1e0eb29 300/ unlim   -   0
```

具体的には、(リモートゲートウェイに対応する) ゲートウェイアドレスごとに 2 行以上が表示されます。各行の先頭にあるキャレット (< >) は、特定のエントリのトラフィックの方向を示しています。出力には、インバウンドトラフィック (仮想プライベートゲートウェイからこのカスタマーゲートウェイデバイスへのトラフィック、「<」で表されます) およびアウトバウンドトラフィック (「>」で表されます) が別々の行として含まれます。

さらにトラブルシューティングする場合は、IKE のトレースオプションを有効にします (詳細については、IKE に関する前のセクションを参照してください)。

トンネル

最初に、必要なファイアウォールルールがあることをもう一度確認します。ルールのリストについては、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照してください。

ファイアウォールルールが正しくセットアップされた場合は、次のコマンドでトラブルシューティングを継続します。

```
user@router> show interfaces st0.1
```

```
Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
   Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
   Input packets : 8719
   Output packets: 41841
   Security: Zone: Trust
   Allowed host-inbound traffic : bgp ping ssh traceroute
   Protocol inet, MTU: 9192
     Flags: None
     Addresses, Flags: Is-Preferred Is-Primary
     Destination: 169.254.255.0/30, Local: 169.254.255.2
```

Security: Zone が正しいことを確認し、Local のアドレスがカスタマーゲートウェイデバイスのトンネル内部のアドレスと一致することを確認します。

次に、以下のコマンドを使用して、169.254.255.1 を仮想プライベートゲートウェイの内部 IP アドレスで置き換えます。次に示すようなレスポンスが結果として返されます。

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

さらにトラブルシューティングする場合は、設定を確認します。

BGP

以下のコマンドを実行します。

```
user@router> show bgp summary
```

```
Groups: 1 Peers: 2 Down peers: 0
Table          Tot Paths  Act Paths Suppressed    History Damp State    Pending
inet.0                 2          1          0          0          0          0
Peer                     AS      InPkt     OutPkt    OutQ   Flaps Last Up/Dwn State|
#Active/Received/Accepted/Damped...
169.254.255.1          7224          9         10       0       0        1:00 1/1/1/0
            0/0/0/0
169.254.255.5          7224          8          9       0       0          56 0/1/1/0
            0/0/0/0
```

さらにトラブルシューティングする場合は、次のコマンドを使用して、169.254.255.1 を仮想プライベートゲートウェイの内部 IP アドレスで置き換えます。

```
user@router> show bgp neighbor 169.254.255.1
```

```
Peer: 169.254.255.1+179 AS 7224 Local: 169.254.255.2+57175 AS 65000
  Type: External    State: Established    Flags: <ImportEval Sync>
  Last State: OpenConfirm   Last Event: RecvKeepAlive
  Last Error: None
  Export: [ EXPORT-DEFAULT ]
  Options: <Preference HoldTime PeerAS LocalAS Refresh>
  Holdtime: 30 Preference: 170 Local AS: 65000 Local System AS: 0
  Number of flaps: 0
  Peer ID: 169.254.255.1    Local ID: 10.50.0.10       Active Holdtime: 30
  Keepalive Interval: 10         Peer index: 0
  BFD: disabled, down
  Local Interface: st0.1
  NLRI for restart configured on peer: inet-unicast
  NLRI advertised by peer: inet-unicast
  NLRI for this session: inet-unicast
  Peer supports Refresh capability (2)
  Restart time configured on the peer: 120
  Stale routes from peer are kept for: 300
  Restart time requested by this peer: 120
  NLRI that peer supports restart for: inet-unicast
```

```
  NLRI that restart is negotiated for: inet-unicast
  NLRI of received end-of-rib markers: inet-unicast
  NLRI of all end-of-rib markers sent: inet-unicast
  Peer supports 4 byte AS extension (peer-as 7224)
  Table inet.0 Bit: 10000
    RIB State: BGP restart is complete
    Send state: in sync
    Active prefixes:              1
    Received prefixes:            1
    Accepted prefixes:            1
    Suppressed due to damping:    0
    Advertised prefixes:          1
Last traffic (seconds): Received 4    Sent 8    Checked 4
Input messages:  Total 24     Updates 2       Refreshes 0     Octets 505
Output messages: Total 26     Updates 1       Refreshes 0     Octets 582
Output Queue[0]: 0
```

ここでは、Received prefixes および Advertised prefixes がそれぞれ 1 になっています。これは、Table inet.0 セクション内にあります。

State が Established でない場合は、Last State および Last Error を確認し、問題の修正に必要なことを詳しく確認します。

BGP ピアリングが起動している場合は、カスタマーゲートウェイデバイスが VPC へのデフォルトルート (0.0.0.0/0) をアドバタイズしていることを確認します。

```
user@router> show route advertising-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 0.0.0.0/0               Self                                    I
```

さらに、VPC に対応するプレフィックスを仮想プライベートゲートウェイから受け取っていることを確認します。

```
user@router> show route receive-protocol bgp 169.254.255.1
```

```
inet.0: 10 destinations, 11 routes (10 active, 0 holddown, 0 hidden)
  Prefix                  Nexthop              MED     Lclpref    AS path
* 10.110.0.0/16           169.254.255.1        100                7224 I
```

Juniper ScreenOS カスタマーゲートウェイデバイスの接続のトラブルシューティング

Juniper ScreenOS ベースのカスタマーゲートウェイデバイスの接続をトラブルシューティングする場合は、IKE、IPsec、トンネル、BGP の 4 つの要素を考慮します。これらの領域を任意の順序でトラブルシューティングできますが、IKE から (ネットワークスタックの下から) 開始して上に進むことをお勧めします。

IKE と IPsec

以下のコマンドを使用します。このレスポンスは、IKE が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
ssg5-serial-> get sa
```

```
total configured sa: 2
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000002<   72.21.209.225  500 esp:a128/sha1 80041ca4  3385 unlim A/-    -1 0
00000002>   72.21.209.225  500 esp:a128/sha1 8cdd274a  3385 unlim A/-    -1 0
00000001<   72.21.209.193  500 esp:a128/sha1 ecf0bec7  3580 unlim A/-    -1 0
00000001>   72.21.209.193  500 esp:a128/sha1 14bf7894  3580 unlim A/-    -1 0
```

トンネル内で指定されたリモートゲートウェイのリモートアドレスを含む 1 つ以上の行が表示されます。Sta 値は A/-、SPI は 00000000 以外の 16 進数になっている必要があります。その他の状態のエントリは、IKE が正しく設定されていないことを示しています。

さらにトラブルシューティングする場合は、設定ファイルの例で推奨されているように、IKE トレースオプションを有効にします。

トンネル

最初に、必要なファイアウォールルールがあることをもう一度確認します。ルールのリストについては、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照してください。

ファイアウォールルールが正しくセットアップされた場合は、次のコマンドでトラブルシューティングを継続します。

```
ssg5-serial-> get interface tunnel.1
```

```
  Interface tunnel.1:
  description tunnel.1
  number 20, if_info 1768, if_index 1, mode route
  link ready
  vsys Root, zone Trust, vr trust-vr
  admin mtu 1500, operating mtu 1500, default mtu 1500
  *ip 169.254.255.2/30
  *manage ip 169.254.255.2
  route-deny disable
  bound vpn:
    IPSEC-1

  Next-Hop Tunnel Binding table
  Flag Status Next-Hop(IP)    tunnel-id  VPN

  pmtu-v4 disabled
  ping disabled, telnet disabled, SSH disabled, SNMP disabled
  web disabled, ident-reset disabled, SSL disabled

  OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
  PIM: not configured  IGMP not configured
  NHRP disabled
  bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
             configured ingress mbw 0kbps, current bw 0kbps
             total allocated gbw 0kbps
```

link:ready が表示され、IP アドレスがカスタマーゲートウェイデバイスのトンネルの内部のアドレスと一致することを確認します。

次に、以下のコマンドを使用して、169.254.255.1 を仮想プライベートゲートウェイの内部 IP アドレスで置き換えます。次に示すようなレスポンスが結果として返されます。

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort

Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms
```

さらにトラブルシューティングする場合は、設定を確認します。

BGP

以下のコマンドを実行します。

```
ssg5-serial-> get vrouter trust-vr protocol bgp neighbor
```

```
Peer AS Remote IP       Local IP          Wt Status   State     ConnID Up/Down
------------------------------------------------------------------------------
   7224 169.254.255.1   169.254.255.2    100 Enabled  ESTABLISH     10 00:01:01
   7224 169.254.255.5   169.254.255.6    100 Enabled  ESTABLISH     11 00:00:59
```

両方の BGP ピアの状態が ESTABLISH である必要があります。これは、仮想プライベートゲートウェイへの BGP 接続がアクティブであることを示します。

さらにトラブルシューティングする場合は、次のコマンドを使用して、169.254.255.1 を仮想プライベートゲートウェイの内部 IP アドレスで置き換えます。

```
ssg5-serial-> get vr trust-vr prot bgp neigh 169.254.255.1
```

```
peer: 169.254.255.1,  remote AS: 7224, admin status: enable
type: EBGP, multihop: 0(disable), MED: node default(0)
connection state: ESTABLISH, connection id: 18 retry interval: node default(120s), cur
 retry time 15s
configured hold time: node default(90s), configured keepalive: node default(30s)
configured adv-interval: default(30s)
designated local IP: n/a
local IP address/port: 169.254.255.2/13946, remote IP address/port: 169.254.255.1/179
router ID of peer: 169.254.255.1, remote AS: 7224
negotiated hold time: 30s, negotiated keepalive interval: 10s
route map in name: , route map out name:
weight: 100 (default)
self as next hop: disable
send default route to peer: disable
ignore default route from peer: disable
send community path attribute: no
reflector client: no
Neighbor Capabilities:
  Route refresh: advertised and received
  Address family IPv4 Unicast:  advertised and received
force reconnect is disable
total messages to peer: 106, from peer: 106
```

```
update messages to peer: 6, from peer: 4
Tx queue length 0, Tx queue HWM: 1
route-refresh messages to peer: 0, from peer: 0
last reset 00:05:33 ago, due to BGP send Notification(Hold Timer Expired)(code 4 :
 subcode 0)
number of total successful connections: 4
connected: 2 minutes 6 seconds
Elapsed time since last update: 2 minutes 6 seconds
```

BGP ピアリングが起動している場合は、カスタマーゲートウェイデバイスが VPC へのデフォルトルート (0.0.0.0/0) をアドバタイズしていることを確認します。このコマンドは、ScreenOS バージョン 6.2.0 以降に適用されます。

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 advertised
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
------------------------------------------------------------------------------
>i          0.0.0.0/0         0.0.0.0 32768   100     0  IGP
Total IPv4 routes advertised: 1
```

さらに、VPC に対応するプレフィックスを仮想プライベートゲートウェイから受け取っていることを確認します。このコマンドは、ScreenOS バージョン 6.2.0 以降に適用されます。

```
ssg5-serial-> get vr trust-vr protocol bgp  rib neighbor 169.254.255.1 received
```

```
i: IBGP route, e: EBGP route, >: best route, *: valid route
               Prefix         Nexthop    Wt  Pref   Med Orig    AS-Path
------------------------------------------------------------------------------
>e*     10.0.0.0/16   169.254.255.1   100   100   100  IGP   7224
Total IPv4 routes received: 1
```

Yamaha 製カスタマーゲートウェイデバイスの接続のトラブルシューティング

Yamaha のカスタマーゲートウェイデバイスの接続をトラブルシューティングする場合は、IKE、IPsec、トンネル、BGP の 4 つの要素を考慮します。これらの領域を任意の順序でトラブルシューティングできますが、IKE から (ネットワークスタックの下から) 開始して上に進むことをお勧めします。

> **Note**
>
> IKE のフェーズ 2 で使用される `proxy ID` 設定は、Yamaha ルーターではデフォルトで無効になっています。これにより、Site-to-Site VPN への接続で問題が発生する可能性があります。ルーターで `proxy ID` が設定されていない場合は、Yamaha を適切に設定するために AWS が提供している設定ファイルの例を参照してください。

IKE

以下のコマンドを実行します。このレスポンスは、IKE が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
# show ipsec sa gateway 1
```

```
sgw  flags local-id                    remote-id        # of sa
------------------------------------------------------------------------
1    U K   YOUR_LOCAL_NETWORK_ADDRESS     72.21.209.225    i:2 s:1 r:1
```

トンネル内で指定されたリモートゲートウェイの `remote-id` 値を含む行が表示されます。トンネル番号を省略すると、すべての Security Association (SA) を表示できます。

さらにトラブルシューティングする場合は、次のコマンドを実行して、診断情報を提供する DEBUG レベルログメッセージを有効にします。

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

ログに記録された項目をキャンセルするには、次のコマンドを実行します。

```
# no ipsec ike log
# no syslog debug on
```

IPsec

以下のコマンドを実行します。このレスポンスは、IPsec が正しく設定されたカスタマーゲートウェイデバイスを示しています。

```
# show ipsec sa gateway 1 detail
```

```
SA[1] Duration: 10675s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit

SPI: 6b ce fd 8a d5 30 9b 02 0c f3 87 52 4a 87 6e 77
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[2] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: send
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: a6 67 47 47
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[3] Duration: 1719s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Direction: receive
Protocol: ESP (Mode: tunnel)
Algorithm: AES-CBC (for Auth.: HMAC-SHA)
SPI: 6b 98 69 2b
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
SA[4] Duration: 10681s
Local ID: YOUR_LOCAL_NETWORK_ADDRESS
Remote ID: 72.21.209.225
Protocol: IKE
Algorithm: AES-CBC, SHA-1, MODP 1024bit
SPI: e8 45 55 38 90 45 3f 67 a8 74 ca 71 ba bb 75 ee
Key: ** ** ** ** **  (confidential)   ** ** ** ** **
-------------------------------------------------
```

各トンネルインターフェイスに対して、receive sas と send sas がいずれも表示されます。

さらにトラブルシューティングする場合は、次のコマンドを使用してデバッグを有効にします。

```
# syslog debug on
# ipsec ike log message-info payload-info key-info
```

次のコマンドを実行して、デバッグを無効にします。

```
# no ipsec ike log
# no syslog debug on
```

トンネル

最初に、必要なファイアウォールルールがあることを確認します。ルールのリストについては、「インターネットとカスタマーゲートウェイデバイス間のファイアウォールの設定」を参照してください。

ファイアウォールルールが正しくセットアップされた場合は、次のコマンドでトラブルシューティングを継続します。

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds  connection.
  Received:    (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
  Transmitted: (IPv4) 3933 packets [241407 octets]
               (IPv6) 0 packet [0 octet]
```

current status 値がオンラインで Interface type が IPsec になっていることを確認します。両方のトンネルインターフェイスでコマンドを実行することを確認します。ここですべての問題を解決するには、設定を確認します。

BGP

以下のコマンドを実行します。

```
# show status bgp neighbor
```

```
BGP neighbor is 169.254.255.1, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
```

```
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.1, Foreign port: 0

BGP neighbor is 169.254.255.5, remote AS 7224, local AS 65000, external link
  BGP version 0, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:00:00, hold time is 0, keepalive interval is 0 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Connection established 0; dropped 0
  Last reset never
Local host: unspecified
Foreign host: 169.254.255.5, Foreign port:
```

両方のネイバーが表示されます。それぞれに対して、Active の BGP state 値が表示されます。

BGP ピアリングが起動している場合は、カスタマーゲートウェイデバイスが VPC へのデフォルトルート (0.0.0.0/0) をアドバタイズしていることを確認します。

```
# show status bgp neighbor 169.254.255.1 advertised-routes
```

```
Total routes: 1
*: valid route
  Network            Next Hop        Metric LocPrf Path
* default            0.0.0.0              0        IGP
```

さらに、VPC に対応するプレフィックスを仮想プライベートゲートウェイから受け取っていることを確認します。

```
# show ip route
```

```
Destination         Gateway          Interface       Kind  Additional Info.
default             ***.***.***.***   LAN3(DHCP)    static
10.0.0.0/16         169.254.255.1    TUNNEL[1]       BGP  path=10124
```

Site-to-Site VPN を使用する

Amazon VPC コンソールまたは AWS CLI を使用して、Site-to-Site VPN リソースを操作できます。

内容

AWS クラウド WAN の Site-to-Site VPN アタッチメントを作成する

下の手順に従って、AWS クラウド WAN のSite-to-Site VPN アタッチメントを作成します。

コンソールを使用して AWS クラウド WAN の VPN アタッチメントを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [Create VPN connection] (VPN 接続の作成) を選択します。
4. (オプション) [名前タグ] には、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。
5. [ターゲットゲートウェイタイプ] で、[Not associated] (関連付けられていません) を選択します。
6. [カスタマーゲートウェイ] で、以下のいずれかを実行します。

- 既存のカスタマーゲートウェイを使用するには、[既存] を選択してから、カスタマーゲートウェイを選択します。
- カスタマーゲートウェイを作成するには、[New (新規)] を選択します。[IP address] (IP アドレス) に、静的パブリック IP アドレスを入力します。[Certificate ARN (証明書 ARN)] で、プライベート証明書の ARN を選択します (証明書ベースの認証を使用している場合)。[BGP ASN] に、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) を入力します。詳細については、「カスタマーゲートウェイのオプション」を参照してください。

7. [ルーティングオプション] で、[動的] と [静的] のどちらを使用するかを選択します。
8. [トンネル内部の IP バージョン] で、[IPv4] または [IPv6] を選択します。
9. (オプション) [Enable acceleration] (アクセラレーションの有効化) で、チェックボックスをオンにしてアクセラレーションを有効にします。詳細については、「高速 VPN 接続」を参照してください。

   アクセラレーションを有効にすると、VPN 接続で使用されるアクセラレーターが 2 つ作成されます。別途 料金がかかります。
10. (オプション) [Local IPv4 network CIDR] (ローカル IPv4 ネットワーク CIDR) で、VPN トンネルを介した通信を許可するカスタマーゲートウェイ (オンプレミス) 側の IPv4 CIDR 範囲を指定します。デフォルトは `0.0.0.0/0` です。

    [リモート IPv4 ネットワーク CIDR] で、VPN トンネルを介した通信を許可する AWS 側の IPv4 CIDR 範囲を指定します。デフォルトは `0.0.0.0/0` です。

    [トンネル内部 IP バージョン] で [IPv6] を指定した場合は、カスタマーゲートウェイ側と AWS 側で、VPN トンネルを介した通信を許可する IPv6 CIDR 範囲を指定します。両方の範囲のデフォルトは `::/0` です。
11. (オプション) [トンネルオプション] では、トンネルごとに次の情報を指定できます。

    - トンネル内部 IPv4 アドレスの `169.254.0.0/16` 範囲からサイズ /30 の IPv4 CIDR ブロック。
    - [トンネル内部 IP バージョン] で [IPv6] を指定した場合は、トンネル内部 IPv6 アドレスの `fd00::/8` 範囲から /126 の IPv6 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。
    - トンネルの詳細オプションを編集するには、[トンネルのオプションを編集する] を選択します。詳細については、「VPN トンネルオプション」を参照してください。
12. [Create VPN connection] (VPN 接続の作成) 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 接続を作成するには

- CreateVpnConnection (Amazon EC2 Query API)
- create-vpn-connection (AWS CLI)

トランジットゲートウェイ VPN アタッチメントを作成する

トランジットゲートウェイで VPN アタッチメントを作成するには、トランジットゲートウェイとカスタマーゲートウェイを指定する必要があります。この手順を実行する前に、トランジットゲートウェイを作成する必要があります。Transit Gateway の作成の詳細については、Amazon VPC Transit Gatewayの「Transit Gateway」を参照してください。

コンソールを使用してトランジットゲートウェイで VPN アタッチメントを作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [Create VPN connection] (VPN 接続の作成) を選択します。
4. (オプション) [名前タグ] には、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。
5. [ターゲットゲートウェイタイプ] で、[トランジットゲートウェイ] を選択してから、トランジットゲートウェイを選択します。
6. [カスタマーゲートウェイ] で、以下のいずれかを実行します。
   - 既存のカスタマーゲートウェイを使用するには、[既存] を選択してから、カスタマーゲートウェイを選択します。

     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。
   - カスタマーゲートウェイを作成するには、[New (新規)] を選択します。[IP Address (IP アドレス)] に、静的パブリック IP アドレスを入力します。[Certificate ARN (証明書 ARN)] で、プライベート証明書の ARN を選択します (証明書ベースの認証を使用している場合)。[BGP ASN] に、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) を入力します。詳細については、「カスタマーゲートウェイのオプション」を参照してください。
7. [ルーティングオプション] で、[動的] と [静的] のどちらを使用するかを選択します。

8. [トンネル内部 IP バージョン] で、VPN トンネルが IPv4 トラフィックをサポートするか、IPv6 トラフィックをサポートするかを指定します。IPv6 トラフィックは、Transit Gateway の VPN 接続でのみサポートされます。
9. (オプション) [Enable acceleration] (アクセラレーションの有効化) で、チェックボックスをオンにしてアクセラレーションを有効にします。詳細については、「高速 VPN 接続」を参照してください。

   アクセラレーションを有効にすると、VPN 接続で使用されるアクセラレーターが 2 つ作成されます。別途 料金がかかります。
10. (オプション) [Local IPv4 network CIDR] (ローカル IPv4 ネットワーク CIDR) で、VPN トンネルを介した通信を許可するカスタマーゲートウェイ (オンプレミス) 側の IPv4 CIDR 範囲を指定します。デフォルトは `0.0.0.0/0` です。

    [リモート IPv4 ネットワーク CIDR] で、VPN トンネルを介した通信を許可する AWS 側の IPv4 CIDR 範囲を指定します。デフォルトは `0.0.0.0/0` です。

    [トンネル内部 IP バージョン] で [IPv6] を指定した場合は、カスタマーゲートウェイ側と AWS 側で、VPN トンネルを介した通信を許可する IPv6 CIDR 範囲を指定します。両方の範囲のデフォルトは `::/0` です。
11. (オプション) [トンネルオプション] では、トンネルごとに次の情報を指定できます。

    - トンネル内部 IPv4 アドレスの `169.254.0.0/16` 範囲からサイズ /30 の IPv4 CIDR ブロック。
    - [トンネル内部 IP バージョン] で [IPv6] を指定した場合は、トンネル内部 IPv6 アドレスの `fd00::/8` 範囲から /126 の IPv6 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。
    - トンネルの詳細オプションを編集するには、[トンネルのオプションを編集する] を選択します。詳細については、「VPN トンネルオプション」を参照してください。
12. [Create VPN connection] (VPN 接続の作成) を選択します。

AWS CLI を使用して VPN アタッチメントを作成するには

create-vpn-connection コマンドを使用して、`--transit-gateway-id` オプションのトランジットゲートウェイ ID を指定します。

Site-to-Site VPN 接続をテストする

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。

開始する前に、以下を確認してください。

- ping リクエストに応答する AMI を使用します。Amazon Linux AMI のいずれかを使用することをお勧めします。
- 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リングするセキュリティグループまたはネットワーク ACL を VPC 内に設定します。これにより、インスタンスは `ping` リクエストを受信できるようになります。
- 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、インスタンスに接続し、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。
- (静的ルーティング) カスタマーゲートウェイデバイスに VPC への静的ルートがあり、VPN 接続に静的ルートがあり、トラフィックがカスタマーゲートウェイデバイスに戻れることを確認します。
- (動的ルーティング) カスタマーゲートウェイデバイスの BGP ステータスが確立されていることを確認します。BGP ピアセッションが確立されるまでに約 30 秒かかります。トラフィックがカスタマーゲートウェイに戻ることができるように、ルートが BGP を使用して正しくアドバタイズされ、サブネットルートテーブルに表示されることを確認します。両方のトンネルが BGP ルーティングを使用して設定されていることを確認します。
- VPN 接続のサブネットルートテーブルでルーティングが設定されていることを確認します。

接続をテストするには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. ダッシュボードで、[Launch Instance (インスタンスの起動)] を選択します。
3. (オプション) [名前] に、インスタンスのわかりやすい名前を入力します。
4. [アプリケーションおよび OS イメージ (Amazon マシンイメージ)] で、[クイックスタート] を選択し、インスタンスのオペレーティングシステムを選択します。
5. [キーペア名] で、既存のキーペアを使用するか、新しいキーペアを作成するかを選択します。
6. [ネットワーク設定] で [既存のセキュリティグループの選択] を選択してから、設定済みのセキュリティグループを選択します。
7. [Summary] (サマリー) パネルで、[Launch instance] (インスタンスの起動) を選択します。

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 (たとえば 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デバイス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 アドレスを指定して ping コマンドを実行します。

   ```
   ping 10.0.0.4
   ```

   正常な応答は次のようになります。

   ```
   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
   ```

   トンネルフェイルオーバーをテストするため、カスタマーゲートウェイデバイスのトンネルの 1 つを一時的に無効化し、このステップを繰り返すことができます。VPN 接続の AWS 側のトンネルを無効化することはできません。
10. AWS からオンプレミスネットワークへの接続をテストするには、SSH または RDP を使用してネットワークからインスタンスに接続できます。次に、ネットワーク内の別のコンピュータのプライベート IP アドレスを使用して ping コマンドを実行し、接続の両側でリクエストを開始および受信できることを検証します。

    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「Linux インスタンスに接続する」を参照してください。Windows インスタンスに接続する方法の詳細については、「Amazon Elastic Compute Cloud Windows インスタンス用ユーザーガイド」の「Windows インスタンスに接続する」を参照してください。

Site-to-Site VPN 接続を削除する

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。Site-to-Site VPN 接続を削除した場合、Site-to-Site VPN 接続に関連付けられていたカスタマーゲートウェイや仮

想プライベートゲートウェイは削除されません。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が不要になった場合は、それらを削除できます。

> **Warning**
>
> Site-to-Site VPN 接続を削除してから新しい VPN 接続を作成する場合は、新しい設定ファイルをダウンロードして、カスタマーゲートウェイデバイスを再設定する必要があります。

タスク

- VPN 接続を削除する
- カスタマーゲートウェイを削除する
- 仮想プライベートゲートウェイをデタッチおよび削除する

VPN 接続を削除する

Site-to-Site VPN 接続を削除すると、しばらくの間、`deleted` の状態が表示されたままになり、その後、エントリは自動的に削除されます。

コンソールを使用して VPN 接続を削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. VPN 接続を選択し、[アクション]、[VPN 接続を削除] の順に選択します。
4. 確認を求められたら、「**`delete`**」と入力し、[削除] を選択します。

コマンドラインまたは API を使用して VPN 接続を削除するには

- DeleteVpnConnection (Amazon EC2 クエリ API)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

カスタマーゲートウェイを削除する

不要になったカスタマーゲートウェイは削除できます。Site-to-Site VPN 接続で使用されている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、[アクション]、[カスタマーゲートウェイを削除] を選択します。
3. 確認を求められたら、「**delete**」と入力し、[削除] を選択します。

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削除するには

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

仮想プライベートゲートウェイをデタッチおよび削除する

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、VPC からそれをデタッチできます。

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、[Actions]、[Detach from VPC] を選択します。
3. [仮想プライベートゲートウェイのデタッチ] 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。仮想プライベートゲートウェイを削除すると、しばらくの間、`deleted` の状態が表示されたままとなります。クリックすると、エントリは自動的に削除されます。

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、[アクション]、[仮想プライベートゲートウェイの削除] を選択します。
3. 確認を求められたら、「**delete**」と入力し、[削除] 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デタッチするには

- DetachVpnGateway (Amazon EC2 クエリ 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 クエリ API)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Site-to-Site VPN 接続のターゲットゲートウェイを変更する

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

ターゲットゲートウェイの変更後、新しいエンドポイントのプロビジョニング中に短時間、Site-to-Site VPN 接続が一時的に利用できなくなります。

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: 新しいターゲットゲートウェイを作成する
- ステップ 2: 静的ルートを削除する (条件付き)
- ステップ 3: 新しいゲートウェイに移行する
- ステップ 4: VPC ルートテーブルを更新する
- ステップ 5: ターゲットゲートウェイのルーティングを更新する (条件付き)
- ステップ 6: カスタマーゲートウェイ ASN を更新する (条件付き)

ステップ 1: 新しいターゲットゲートウェイを作成する

新しいターゲットゲートウェイへの移行を実行する前に、まず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の作成”」を参照してください。トランジットゲートウェイの追加の詳細については、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を作成する」を参照してください。

新しいターゲットゲートウェイがトランジットゲートウェイの場合は、VPC をトランジットゲートウェイにアタッチします。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アタッチメント」を参照してください。

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ターゲットを変更する場合、オプションでトランジットゲートウェイ ASN を仮想プライベートゲートウェイ ASN と同じ値に設定できます。別の ASN を使用する場合は、カスタマーゲートウェイデバイスの ASN をトランジットゲートウェイ ASN に設定する必要があります。詳細については、「the section called “ステップ 6: カスタマーゲートウェイ ASN を更新する (条件付き)”」を参照してください。

ステップ 2: 静的ルートを削除する (条件付き)

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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [ルートテーブル] (Route tables) を選択して、ルートテーブルを選択します。
3. [Routes] タブで、[Edit routes] を選択します。
4. 仮想プライベートゲートウェイへの静的ルートで [削除] を選択します。
5. [Save changes] (変更の保存) をクリックします。

ステップ 3: 新しいゲートウェイに移行する

ターゲットゲートウェイを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. VPN 接続を選択して、[アクション]、[VPN 接続を変更] の順に選択します。
4. [ターゲットタイプ] でゲートウェイタイプを選択します。
   a. 新しいターゲットゲートウェイが仮想プライベートゲートウェイの場合は、[VPN ゲートウェイ] を選択します。
   b. 新しいターゲットゲートウェイがトランジットゲートウェイの場合は、[トランジットゲートウェイ] を選択します。
5. [Save changes] (変更の保存) をクリックします。

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。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。

次の表に、VPN ゲートウェイターゲットを変更した後に実行する VPC ルートテーブルの更新に関する情報を示します。

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
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の ID が格納されているルートを削除します。
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。

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	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の ID が格納されているルートを追加します。
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	トランジットゲートウェイの ID への仮想プライベートゲートウェイの ID を格納するルートを更新します。
静的ルートを持つ仮想プライベートゲートウェイ	静的ルートを持つ仮想プライベートゲートウェイ	新しい仮想プライベートゲートウェイの ID への仮想プライベートゲートウェイの ID を格納するルートを更新します。
静的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	仮想プライベートゲートウェイの ID を含むルートを削除します。
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	仮想プライベートゲートウェイの ID へのトランジットゲートウェイの ID を格納するルートを更新します。
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の ID を含むルートを削除します。
トランジットゲートウェイ	トランジットゲートウェイ	新しいトランジットゲートウェイの ID へのトランジットゲートウェイの ID を格納するルートを更新します。

ステップ 5: ターゲットゲートウェイのルーティングを更新する (条件付き)

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。詳細については、「Amazon VPC Transit Gateway」の「Transit Gateway ルートテーブル」を参照してください。

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。

仮想プライベートゲートウェイとは異なり、トランジットゲートウェイは VPN 添付のすべてのトンネルでマルチエグジット識別子 (MED) に同じ値を設定します。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し、トンネル選択の MED 値に依存している場合は、接続の問題を回避するためにルーティングを変更することをお勧めします。例えば、トランジットゲートウェイで特定のルートをアドバタイズできます。詳細については、「ルートテーブルと VPN ルーティングの優先度」を参照してください。

ステップ 6: カスタマーゲートウェイ ASN を更新する (条件付き)

新しいゲートウェイに古いゲートウェイとは異なる ASN がある場合は、新しい ASN を指すようにカスタマーゲートウェイデバイスの ASN を更新する必要があります。詳細については、「Site-to-Site VPN 接続のカスタマーゲートウェイオプション」を参照してください。

Site-to-Site VPN 接続オプションを変更する

Site-to-Site VPN 接続の接続オプションを変更できます。以下のオプションを変更できます。

- VPN トンネルを介して通信できる VPN 接続のローカル (カスタマーゲートウェイ) 側とリモート (AWS) 側の IPv4 CIDR 範囲。両方の範囲のデフォルトは `0.0.0.0/0` です。
- VPN トンネルを介して通信できる VPN 接続のローカル (カスタマーゲートウェイ) 側とリモート (AWS) 側の IPv6 CIDR 範囲。両方の範囲のデフォルトは `::/0` です。

VPN 接続オプションを変更しても、AWS 側の VPN エンドポイント IP アドレスは変更されず、トンネルオプションも変更されません。VPN 接続が更新されている間、VPN 接続は一時的に利用できなくなります。

コンソールを使用して VPN 接続オプションを変更するには

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

2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. VPN 接続を選択し、[アクション]、[VPN 接続オプションを変更] の順に選択します。
4. 必要に応じて、新しい CIDR 範囲を入力します。
5. [Save changes] (変更の保存) をクリックします。

コマンドラインまたは API を使用して VPN 接続オプションを変更するには

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

Site-to-Site VPN トンネルオプションを変更する

Site-to-Site VPN 接続の VPN トンネルのトンネルオプションを変更できます。一度に 1 つの VPN トンネルを変更できます。

> **Important**
>
> VPN トンネルを変更すると、トンネル経由の接続が最大数分間中断されます。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。

コンソールを使用して VPN トンネルオプションを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 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]、[VPN トンネルオプションを変更] の順に選択します。
4. [VPN トンネル外部 IP アドレス] で、VPN トンネルのトンネルエンドポイント IP を選択します。
5. 必要に応じて、トンネルオプションの新しい値を選択または入力します。詳細については、「VPN トンネルオプション」を参照してください。
6. [Save changes] (変更の保存) をクリックします。

コマンドラインまたは API を使用して VPN トンネルオプションを変更するには

- (AWS CLI) 現在のトンネルオプションを表示するには describe-vpn-connections を使用し、トンネルオプションを変更するには modify-vpn-tunnel-options を使用します。
- (Amazon EC2 Query API) 現在のトンネルオプションを表示するには DescribeVpnConnections を使用し、トンネルオプションを変更するには ModifyVpnTunnelOptions を使用します。

Site-to-Site VPN 接続の静的ルートを編集する

静的ルーティング用に設定された仮想プライベートゲートウェイ上の Site-to-Site VPN 接続の場合は、VPN 設定の静的ルートを追加、変更、または削除できます。

コンソールを使用して静的ルートを追加または削除するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. VPN 接続を選択します。
4. [静的ルートの編集] を選択します。
5. 必要に応じて、ルートを追加または削除します。
6. [Save changes] (変更の保存) をクリックします。
7. 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 VPN 接続に反映する必要があります。詳細については、「(仮想プライベートゲートウェイ) ルートテーブルでルート伝播を有効にする」を参照してください。
8. トランジットゲートウェイ上の VPN 接続の場合は、トランジットゲートウェイルートテーブルで静的ルートを追加、変更、または削除します。詳細については、「Amazon VPC Transit Gateway」の「Transit Gateway ルートテーブル」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)

Site-to-Site VPN 接続のカスタマーゲートウェイを変更する

Amazon VPC コンソールまたはコマンドラインツールを使用して、Site-to-Site VPN 接続のカスタマーゲートウェイを変更できます。

カスタマーゲートウェイの変更後、新しいエンドポイントのプロビジョニング中に短時間、VPN 接続が一時的に利用できなくなります。

コンソールを使用してカスタマーゲートウェイを変更するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. VPN 接続を選択します。
4. [アクション]、[VPN 接続を変更] を選択します。
5. [ターゲットタイプ] で、[カスタマーゲートウェイ] を選択します。
6. [ターゲットカスタマーゲートウェイ] では、新しいカスタマーゲートウェイを選択します。
7. [Save changes] (変更の保存) をクリックします。

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変更するには

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

Site-to-Site VPN 接続の漏洩した認証情報を置き換える

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するか、ACM 証明書を変更できます。使用する方法は、VPN トンネルに使用した認証オプションによって異なります。詳細については、「Site-to-Site VPN トンネル認証オプション」を参照してください。

IKE 事前共有キーを変更するには

VPN 接続のトンネルオプションを変更し、トンネルごとに新しい IKE 事前共有キーを指定できます。詳細については、「Site-to-Site VPN トンネルオプションを変更する」を参照してください。

または、VPN 接続を削除することもできます。詳細については、「VPN 接続を削除する」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。次に、同じ仮想プライベートゲートウェイを使用して新しい VPN 接続を作成し、カスタマーゲートウェイデバイスに新しいキーを設定します。トンネルのための独自の事前共有キーを指定するか、AWS で新しい事前共有キーを生成します。VPN 接続の作成の詳細については、「VPN 接続を作成する」を参照してください。VPN 接続を再作成すると、トンネルの内部アドレスと外部アドレスが変更されることがあります。

トンネルエンドポイントの AWS 側の証明書を変更するには

証明書を更新します。詳細については、「VPN トンネルエンドポイント証明書をローテーションする」を参照してください。

カスタマーゲートウェイデバイスの証明書を変更するには

1. 新しい証明書を作成します。詳細については、AWS Certificate Manager ユーザーガイドの「証明書の発行と管理」を参照してください。
2. カスタマーゲートウェイデバイスに証明書を追加します。

Site-to-Site VPN トンネルエンドポイント証明書をローテーションする

Amazon VPC コンソールを使用して、AWS 側のトンネルエンドポイントの証明書を更新できます。トンネルエンドポイントの証明書の有効期限が近づくと、AWS はサービスにリンクされたロールを使用して証明書を自動的に更新します。詳細については、「the section called “サービスリンクロール”」を参照してください。

コンソールを使用して Site-to-Site VPN トンネルエンドポイント証明書を更新するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. Site-to-Site VPN 接続を選択し、[アクション]、[VPN トンネル証明書を変更] を選択します。
4. トンネルエンドポイントを選択します。

5. [Save (保存)] を選択します。

AWS CLI を使用して Site-to-Site VPN トンネルエンドポイント証明書を更新するには

modify-vpn-tunnel-certificate コマンドを使用します。

とのプライベート IP VPN AWS Direct Connect

プライベート IP VPN を使用すると、 経由で IPsec VPN をデプロイして AWS Direct Connect、パブリック IP アドレスや追加のサードパーティー VPN 機器を使用せずに AWS、オンプレミスネットワークと 間のトラフィックを暗号化できます。

を介したプライベート IP VPN の主なユースケースの 1 つは、金融、医療、連邦業界のお客様が規制およびコンプライアンスの目標を達成できるように支援 AWS Direct Connect することです。を介したプライベート IP VPN により、 AWS とオンプレミスネットワーク間のトラフィックは安全でプライベート AWS Direct Connect であることが保証され、お客様は規制とセキュリティの義務に準拠できます。

コンテンツ

プライベート IP VPN の利点

- ネットワーク管理と運用の簡素化： プライベート IP VPN を使用しない場合、お客様はサードパーティ VPN とルーターをデプロイして、 AWS Direct Connect ネットワーク経由でプライベート VPNsを実装する必要があります。プライベート IP VPN 機能を使用すると、お客様は独自の VPN インフラストラクチャをデプロイして管理する必要はありません。これにより、ネットワークオペレーションが簡素化され、コストが削減されます。

- セキュリティ体制の改善： 以前は、VPN エンドポイントのパブリック IP アドレスを必要とする AWS Direct Connect、 経由のトラフィックの暗号化にパブリック AWS Direct Connect 仮想インターフェイス (VIF) を使用する必要がありました。パブリック IP を使用すると、外部 (DOS) 攻撃の可能性が高まり、その結果、お客様はネットワーク保護のために追加のセキュリティギアをデプロイする必要があります。また、パブリック VIF は、すべての AWS パブリックサービスとお客様のオンプレミスネットワーク間のアクセスを開き、リスクの重要度を高めます。プライベート IP VPN 機能を使用すると、プライベート IP VIFs の代わりに) AWS Direct Connect トランジット VIFs で暗号化できます。 IPs これにより、暗号化に加えて end-to-end プライベート接続が提供され、全体的なセキュリティ体制が向上します。
- ルートスケールの向上： プライベート IP VPN 接続は、現在 200 のアウトバウンドルートと 100 のインバウンドルートの制限がある AWS Direct Connect のみと比較して、ルート制限 (5000 のアウトバウンドルートと 1000 のインバウンドルート) が高くなります。

プライベート IP VPN の仕組み

プライベート IP Site-to-Site VPN は、 AWS Direct Connect トランジット仮想インターフェイス (VIF) を介して動作します。 AWS Direct Connect ゲートウェイとトランジットゲートウェイを使用して、オンプレミスネットワークと AWS VPC を相互接続します。プライベート IP VPN 接続には、AWS 側のトランジットゲートウェイと、オンプレミス側のカスタマーゲートウェイデバイスに終了ポイントがあります。IPsec トンネルのトランジットゲートウェイとカスタマーゲートウェイデバイスの両方の末尾にプライベート IP アドレス (RFC1918) を割り当てる必要があります。

トランジットゲートウェイにプライベート IP VPN 接続をアタッチします。そして、VPN アタッチメントと、トランジットゲートウェイにアタッチされている VPC (または他のネットワーク) の間でトラフィックをルーティングします。これを行うには、ルートテーブルを VPN アタッチメントに関連付けます。逆方向では、VPC に関連付けられているルートテーブルを使用して、VPC からプライベート IP VPN アタッチメントにトラフィックをルーティングできます。

VPN アタッチメントに関連付けられているルートテーブルは、基盤となる AWS Direct Connect アタッチメントに関連付けられているルートテーブルと同じでも異なるものでも構いません。これにより、VPC とオンプレミスのネットワーク間で、暗号化されたトラフィックと暗号化されていないトラフィックの両方を同時にルーティングできます。

VPN から出るトラフィックパスの詳細については、AWS Direct Connect 「 ユーザーガイド」の「プライベート仮想インターフェイスとトランジット仮想インターフェイスのルーティングポリシー」を参照してください。

前提条件

AWS Direct Connect 経由のプライベート IP VPN のセットアップを完了するには、次のリソースが必要です。

- オンプレミスネットワークと 間の AWS Direct Connect 接続 AWS
- 適切なトランジット AWS Direct Connect ゲートウェイと関連付けられている ゲートウェイ
- 使用可能なプライベート IP CIDR ブロックを持つトランジットゲートウェイ
- オンプレミスネットワーク内のカスタマーゲートウェイデバイスと対応する AWS カスタマーゲートウェイ

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、 で作成するリソースです AWS。オンプレミスネットワーク内のカスタマーゲートウェイデバイスを表します。カスタマーゲートウェイを作成するときは、デバイスに関する情報を に提供します AWS。詳細については、「カスタマーゲートウェイ」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. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) 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] を選択します。
3. [カスタマーゲートウェイの作成]] を選択します。
4. (オプション) [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。
5. [BGP ASN] に、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) を入力します。
6. IP アドレスで、カスタマーゲートウェイデバイスのプライベート IP アドレスを入力します。
7. (オプション) [デバイス] に、このカスタマーゲートウェイをホストするデバイスの名前を入力します。
8. [カスタマーゲートウェイの作成]] を選択します。

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 クエリ API)
- create-customer-gateway (AWS CLI)

トランジットゲートウェイの準備

トランジットゲートウェイは、VPC とオンプレミスネットワークを相互接続するために使用できるネットワークの中継ハブです。プライベート IP VPN 接続には、新しいトランジットゲートウェイを作成するか、既存のトランジットゲートウェイを使用できます。トランジットゲートウェイを作成するとき、または既存のトランジットゲートウェイを変更する場合は、接続のためのプライベート IP CIDR ブロックを指定します。

> **Note**
>
> プライベート IP VPN に関連付けるトランジットゲートウェイ CIDR ブロックを指定する場合は、CIDR ブロックがトランジットゲートウェイ上の他のネットワークアタッチメントの IP アドレスと重複しないようにしてください。IP CIDR ブロックが重複している場合は、カスタマーゲートウェイデバイスで設定上の問題が発生する可能性があります。

プライベート IP VPN に使用するトランジットゲートウェイを作成または変更する具体的な AWS コンソール手順については、「Amazon VPC Transit Gateways ガイド」の「トランジットゲートウェイ」を参照してください。

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

- CreateTransitGateway (Amazon EC2 クエリ API)
- create-transit-gateway (AWS CLI)

AWS Direct Connect ゲートウェイを作成する

AWS Direct Connect 「 AWS Direct Connect ユーザーガイド」の「Direct Connect ゲートウェイの作成」手順に従って、 ゲートウェイを作成します。

コマンドラインまたは API を使用して AWS Direct Connect ゲートウェイを作成するには

- CreateDirectConnectGateway (AWS Direct Connect クエリ API)
- create-direct-connect-gateway (AWS CLI)

トランジットゲートウェイの関連付けの作成

AWS Direct Connect ゲートウェイを作成したら、ゲートウェイのトランジット AWS Direct Connect ゲートウェイの関連付けを作成します。許可されたプレフィックスリストで以前に識別されたトランジットゲートウェイのプライベート IP CIDR を指定します。

詳細については、AWS Direct Connect ユーザーガイドの「Transit Gateway の関連付け」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 AWS Direct Connect ゲートウェイの関連付けを作成するには

- CreateDirectConnectGatewayAssociation (AWS Direct Connect クエリ API)
- create-direct-connect-gateway-association (AWS CLI)

VPN 接続の作成

プライベート IP アドレスを使用して VPN 接続を作成するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN 接続] を選択します。
3. [Create VPN connection] (VPN 接続の作成) を選択します。
4. (オプション) [名前タグ] 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。
5. [Target gateway type] (ターゲットゲートウェイタイプ) で、[Transit gateway] (転送ゲートウェイ) を選択します。次に、以前に特定したトランジットゲートウェイを選択します。
6. [Customer gateway] (カスタマーゲートウェイ) で、[Existing] (既存) を選択します。次に、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。
7. カスタマーゲートウェイ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かどうかに基づいて、ルーティングオプションのいずれかを選択します。
   - カスタマーゲートウェイデバイスが 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。
   - カスタマーゲートウェイデバイスが BGP をサポートしていない場合は、[静的] を選択します。
8. [トンネル内部 IP バージョン] で、VPN トンネルが IPv4 トラフィックをサポートするか、IPv6 トラフィックをサポートするかを指定します。

9. （オプション) IP バージョン 内でトンネル に IPv4 を指定した場合は、VPN トンネルを介した通信を許可するカスタマーゲートウェイと AWS 側の IPv4 CIDR 範囲をオプションで指定できます。 デフォルトは `0.0.0.0/0` です。

   IP バージョン 内のトンネル に IPv6 を指定した場合、オプションで、VPN トンネルを介した通信を許可するカスタマーゲートウェイと AWS 側の IPv6 CIDR 範囲を指定できます。 両方の範囲のデフォルトは `::/0` です。
10. 外部 IP アドレスタイプ では、PrivateIpv4 を選択します。
11. トランスポートアタッチメント ID で、適切なゲートウェイのトランジット AWS Direct Connect ゲートウェイアタッチメントを選択します。
12. [Create VPN connection] (VPN 接続の作成) を選択します。

> **Note**
>
> [Enable acceleration] (アクセラレーションを有効にする) オプションは、 AWS Direct Connect 経由の VPN 接続には適用されません。

AWS Site-to-Site VPN のセキュリティ

AWS クラウドセキュリティは最優先事項です。 AWS お客様は、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャの恩恵を受けることができます。

AWS セキュリティはお客様とお客様との間で共有される責任です。責任共有モデル では、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS AWS AWS クラウドクラウド内でサービスを実行するインフラストラクチャを保護する責任があります。 AWS また、安全に使用できるサービスも提供します。第三者監査人は、AWS、当社のセキュリティの有効性を定期的にテストおよび検証しています。AWS Site-to-Site VPN に適用されるコンプライアンスプログラムについては、「AWS コンプライアンスプログラム別の対象サービス」「」を参照してください。
- クラウド内のセキュリティ — お客様の責任は、 AWS 使用するサービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Site-to-Site VPN を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するように Site-to-Site VPN を設定する方法について説明します。また、Site-to-Site VPN AWS リソースの監視と保護に役立つ他のサービスの使用方法についても学びます。

コンテンツ

AWS Site-to-Site VPN でのデータ保護

AWS https://aws.amazon.com/compliance/shared-responsibility-model/、 AWS Site-to-Site VPN のデータ保護に適用されます。このモデルで説明したように AWS 、はすべてを実行するグローバルインフラストラクチャを保護する責任があります。 AWS クラウドお客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS

のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよびGDPR」のブログ記事を参照してください。

データ保護のため、 AWS アカウント 認証情報を保護し、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用してリソースと通信します。 AWS TLS 1.2、できれば TLS 1.3 が必要です。
- を使用して API とユーザーアクティビティのロギングを設定します。 AWS CloudTrail
- AWS 暗号化ソリューションと、 AWS のサービスその中に含まれるデフォルトのセキュリティコントロールをすべて使用してください。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介してアクセスするときに FIPS 140-2 で検証された暗号モジュールが必要な場合は、FIPS エンドポイントを使用してください。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの機密情報やセンシティブ情報は、タグや名前フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これには、コンソール、API AWS CLI、または AWS SDK AWS のサービス を使用してSite-to-Site VPN やその他のものを操作する場合も含まれます。名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

インターネットトラフィックのプライバシー

Site-to-Site VPN 接続は、VPC をオンプレミスネットワークにプライベートに接続します。お客様の VPC とネットワーク間で転送されるデータは、転送中データの機密性と整合性を維持するために、暗号化された VPN 接続を介してルーティングします。Amazon 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。IPsec は、データストリームの各 IP パケットを認証して暗号化することによって、安全に IP 通信を行うためのプロトコルです。

各Site-to-Site VPN 接続は、 AWS ネットワークとリンクする 2 つの暗号化された IPSec VPN トンネルで構成されています。各トンネルのトラフィックでは、暗号化に AES128 あるいは AES256 を、キー交換に Diffie-Hellman グループを使用することで、Perfect Forward Secrecy を提供しています。 AWS は SHA1 または SHA2 ハッシュ関数で認証します。

VPC のインスタンスでは、Site-to-Site VPN 接続の反対側のリソースに接続するためのパブリック IP アドレスは必要ありません。インスタンスは、Site-to-Site VPN 接続を介してインターネットトラフィックをオンプレミスネットワークにルーティングできます。その後、既存のアウトバウンドトラフィックポイントとネットワークセキュリティおよびモニタリングデバイスを介してインターネットにアクセスできます。

詳細については、以下のトピックを参照してください:

- Site-to-Site VPN 接続のトンネルオプション: 各トンネルで使用できる IPsec および Internet Key Exchange (IKE) オプションに関する情報を提供します。
- Site-to-Site VPN トンネル認証オプション: VPN トンネルエンドポイントの認証オプションに関する情報を提供します。
- カスタマーゲートウェイデバイスの要件: VPN 接続のユーザー側のカスタマーゲートウェイデバイスの要件に関する情報を提供します。
- VPN CloudHub を使用して安全なサイト間通信を提供する: Site-to-Site VPN 接続が複数ある場合は、VPN を使用してオンプレミスサイト間の安全な通信を提供できます。 AWS CloudHub

AWS Site-to-Site VPN の ID とアクセス管理

AWS Identity and Access Management (IAM) は、 AWS のサービス 管理者がリソースへのアクセスを安全に制御できるようにするものです。 AWS IAM 管理者は、誰を認証 (サインイン) し、誰に Site-to-Site VPN リソースの使用を許可する (アクセス許可を持たせる) かを制御します。IAM AWS のサービス は追加料金なしで使用できるアプリです。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- AWS Site-to-Site VPN と IAM の連携の仕組み
- Site-to-Site VPN の ID AWS ベースのポリシーの例

- AWS Site-to-Site VPN の ID とアクセスのトラブルシューティング
- Site-to-Site VPN のサービスにリンクされたロールの使用

対象者

AWS Identity and Access Management (IAM) の使用方法は、Site-to-Site VPN で行う作業によって異なります。

サービスユーザー - Site-to-Site VPN サービスを使用してジョブを実行する場合は、必要なアクセス許可と認証情報を管理者が用意します。作業を実行するためにさらに多くの Site-to-Site VPN の機能を使用するとき、追加の許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Site-to-Site VPN の機能にアクセスできない場合は、「AWS Site-to-Site VPN の ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Site-to-Site VPN リソースを担当している場合は、通常、Site-to-Site VPN へのフルアクセスがあります。サービスのユーザーがどの Site-to-Site VPN 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。お客様の会社で Site-to-Site VPN で IAM を利用する方法の詳細については、AWS Site-to-Site VPN と IAM の連携の仕組み をご参照ください。

IAM 管理者 - IAM 管理者は、Site-to-Site VPN へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Site-to-Site VPN アイデンティティベースのポリシーの例を表示するには、Site-to-Site VPN の ID AWS ベースのポリシーの例 を参照してください。

アイデンティティを使用した認証

認証とは、ID AWS 認証情報を使用してサインインする方法です。IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) する必要があります。

ID ソースを通じて提供された認証情報を使用して、フェデレーション ID AWS としてサインインできます。 AWS IAM Identity Center フェデレーテッド ID の例としては、(IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google や Facebook の認証情報などがあります。フェデレーションアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。 AWS フェデレーションを使用してアクセスすると、間接的にロールを引き継ぐことになります。

ユーザーのタイプによっては、 AWS Management Console AWS またはアクセスポータルにサインインできます。へのサインインについて詳しくは AWS、『AWS サインイン ユーザーガイド』の「AWS アカウントにサインインする方法」を参照してください。

AWS プログラムでアクセスする場合は、認証情報を使用してリクエストに暗号署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨方法を使用して自分でリクエストに署名する方法の詳細については、IAM ユーザーガイドの「 AWS API リクエストへの署名」を参照してください。

使用する認証方法を問わず、セキュリティ情報の提供を追加でリクエストされる場合もあります。たとえば、アカウントのセキュリティを強化するために多要素認証 (MFA) AWS を使用することを推奨しています。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント root ユーザー

を作成するときは AWS アカウント、 AWS のサービス アカウント内のすべてのリソースに完全にアクセスできる 1 つのサインイン ID から始めます。この ID は AWS アカウント root ユーザーと呼ばれ、アカウントの作成に使用したメールアドレスとパスワードでサインインすることでアクセスされます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行してください。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーション ID

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID AWS のサービス プロバイダーとのフェデレーションを使用して一時的な認証情報を使用してアクセスするように要求します。

フェデレーテッド ID とは、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、Identity Center ディレクトリのユーザー、または ID AWS のサービス ソースを通じて提供された認証情報を使用してアクセスする任意のユーザーです。 AWS Directory Serviceフェデレーテッド ID がアクセスすると AWS アカウント、そのユーザーがロールを引き受け、そのロールが一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成したり、独自のアイデンティティソース内のユーザーや

グループに接続して同期したりして、すべてのアプリケーションで使用することができます。 AWS アカウント IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「IAM Identity Center とは？」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定の権限を持つ社内の AWS アカウント ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループ は、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、 AWS アカウント 特定の権限を持つ社内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。 AWS Management Console ロールを切り替えることで、の IAM ロールを一時的に引き受けることができます。 AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用してロールを引き受けることができます。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

一時的な認証情報を持った IAM ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーションアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーションアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与さ

れます。フェデレーションの詳細については、「IAM ユーザーガイド」の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、ロールをプロキシとして使用する代わりに AWS のサービス、ポリシーをリソースに直接アタッチできるものもあります。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — AWS のサービス AWS のサービス他の機能を使用するものもあります。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、あなたはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 AWS のサービス を呼び出したプリンシパルの権限をリクエスト元と組み合わせて使用して AWS のサービス、ダウンストリームサービスにリクエストを行います。FASリクエストは、AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
  - サービスにリンクされたロール — サービスにリンクされたロールは、にリンクされているサービスロールの一種です。 AWS のサービスサービスは、ユーザーに代わってアクションを実行す

るロールを引き受けることができます。 AWS アカウント サービスにリンクされたロールはに表示され、そのサービスが所有します。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されるアプリケーション — IAM ロールを使用して、EC2 インスタンスで実行され、 AWS API AWS CLI リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 AWS インスタンスにロールを割り当て、そのロールをそのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされるインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか」を参照してください。

ポリシーを使用したアクセスの管理

AWS ポリシーを作成して AWS ID またはリソースにアタッチすることで、アクセスを制御します。ポリシーとは、ID またはリソースに関連付けると権限を定義するオブジェクトです。 AWS AWS プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON AWS ドキュメントとして保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザは AWS Management Console、、 AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらに インラインポリシー または マネージドポリシー に分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。 AWS アカウント管理ポリシーには、 AWS 管理ポリシーと顧客管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーが添付されているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザ、ロール、フェデレーティッドユーザ、またはを含めることができます。 AWS のサービス

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。IAM AWS の管理ポリシーをリソースベースのポリシーで使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

ACL をサポートするサービスの例としては AWS WAF、Amazon S3、、および Amazon VPC があります。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS あまり一般的ではないポリシータイプもサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる許可の上限を設定する高度な機能です。エンティティに権限の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとその権限の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、権限の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、許可は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCP) — SCP は、組織または組織単位 (OU) の最大権限を指定する JSON ポリシーです。 AWS Organizations AWS Organizations は、 AWS アカウント 企業が所有する複数のものをグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各エンティティを含むメンバーアカウント内のエンティティの権限を制限します。 AWS アカウントのルートユーザー Organizations と SCP の詳細については、AWS Organizations ユーザーガイド の「SCP の仕組み」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーティッドユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限される範囲は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、許可は無効になります。詳細については、 IAM ユーザーガイド の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。 AWS 複数のポリシータイプが関係している場合にリクエストを許可するかどうかを決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

AWS Site-to-Site VPN と IAM の連携の仕組み

IAM を使用して Site-to-Site VPN へのアクセスを管理する前に、Site-to-Site VPN で利用できる IAM の機能について学びます。

AWS Site-to-Site VPN で使用できる IAM 機能

IAM 機能	Site-to-Site VPN サポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	いいえ
ポリシーアクション	Yes
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	No
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	Yes
プリンシパル権限	Yes
サービスロール	あり
サービスリンクロール	Yes

Site-to-Site VPN AWS やその他のサービスがほとんどの IAM 機能でどのように機能するかを大まかに把握するには、IAM ユーザーガイドの「IAM AWS と連携するサービス」を参照してください。

Site-to-Site VPN のアイデンティティベースのポリシー

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Site-to-Site VPN のアイデンティティベースのポリシーの例

Site-to-Site VPN アイデンティティベースのポリシーの例を表示するには、「Site-to-Site VPN の ID AWS ベースのポリシーの例」を参照してください。

Site-to-Site VPN 内のリソースベースのポリシー

リソースベースのポリシーのサポート	なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーが添付されているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、またはが含まれます。AWS のサービス

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス権限を付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチ

することで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Site-to-Site VPN のポリシーアクション

ポリシーアクションに対するサポート	Yes

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションは通常、関連する AWS API オペレーションと同じ名前です。一致する API オペレーションのない 許可のみのアクション など、いくつかの例外があります。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Site-to-Site VPN アクションのリストを表示するには、『サービス認証リファレンス』の「AWS Site-to-Site VPN で定義されるアクション」を参照してください。

Site-to-Site VPN のポリシーアクションは、アクションの前に以下のプレフィックス を使用します。

```
ec2
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "ec2:action1",
      "ec2:action2"
         ]
```

Site-to-Site VPN アイデンティティベースのポリシーの例を表示するには、「Site-to-Site VPN の ID AWS ベースのポリシーの例」を参照してください。

Site-to-Site VPN のポリシーリソース

ポリシーリソースに対するサポート	Yes

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシーの要素は、オブジェクトあるいはアクションが適用されるオブジェクトを指定します。ステートメントには、`Resource` または `NotResource`要素を含める必要があります。ベストプラクティスとしては、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、 リソースレベルの許可 と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

Site-to-Site VPN リソースタイプとその ARN のリストを確認するには、『サービス認証リファレンス』の「AWS Site-to-Site VPN で定義されるリソース」を参照してください。各リソースの ARN を指定できるアクションについては、「AWS Site-to-Site VPN で定義されるアクション」を参照してください。

Site-to-Site VPN アイデンティティベースのポリシーの例を表示するには、「Site-to-Site VPN の ID AWS ベースのポリシーの例」を参照してください。

Site-to-Site VPN のポリシー条件キー

サービス固有のポリシー条件キーのサポート	はい

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どの プリンシパル がどの リソース に対してどのような条件下 で アクション を実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition要素を指定する場合、または 1 つの Condition要素に複数のキーを指定する場合、 AWS では AND論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 AWS OR論理演算を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、 IAM ユーザーガイド の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS グローバル条件キーとサービス固有の条件キーをサポートします。 AWS すべてのグローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

Site-to-Site VPN の条件キーのリストを確認するには、『サービス認証リファレンス』の「AWS Site-to-Site VPN の条件キー」を参照してください。条件キーを使用できるアクションとリソースについては、「AWS Site-to-Site VPN で定義されるアクション」を参照してください。

Site-to-Site VPN アイデンティティベースのポリシーの例を表示するには、「Site-to-Site VPN の ID AWS ベースのポリシーの例」を参照してください。

Site-to-Site VPN の ACL

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Site-to-Site VPN による ABAC

ABAC (ポリシー内のタグ) のサポート	いいえ

属性ベースのアクセス制御 (ABAC) は、属性に基づいて権限を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) AWS や多くのリソースにタグを付けることができます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。次に、プリンシパルのタグがアクセスを試行するリソースのタグと一致したときにオペレーションを許可するよう、ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys`の条件キーを使用して、ポリシーの条件要素 でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値は Yes です。サービスが一部のリソースタイプに対してのみ 3 つの条件キーすべてをサポートする場合、値は Partial です。

ABAC の詳細については、IAM ユーザーガイドの「ABAC とは?」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

Site-to-Site VPN での一時的な認証の使用

一時的な認証情報のサポート	Yes

AWS のサービス 一時的な認証情報を使用してサインインすると機能しないものもあります。 AWS のサービス 一時的な認証情報で機能するものなど、追加情報については、『IAM ユーザーガイド』の「IAM と連携する」を参照してくださいAWS のサービス 。

ユーザー名とパスワード以外の方法でにサインインすると、 AWS Management Console 一時的な認証情報が使用されることになります。たとえば、会社のシングルサインオン (SSO) AWS リンクを使用してアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、 IAM ユーザーガイド の「ロールへの切り替え (コンソール)」を参照してください。

または API を使用して一時的な認証情報を手動で作成できます。 AWS CLI AWS その後、その一時的な認証情報を使用してアクセスできます AWS。 AWS 長期アクセスキーを使用する代わりに、一

時的な認証情報を動的に生成することをおすすめします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Site-to-Site VPN のクロスサービスプリンシパル許可

フォワードアクセスセッション (FAS) をサポート	Yes

IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、そのユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FASは、を呼び出したプリンシパルの権限と AWS のサービス、 AWS のサービス ダウンストリームサービスにリクエストを行うリクエストを組み合わせて使用します。FASリクエストは、 AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Site-to-Site VPN のサービスロール

サービスロールに対するサポート	あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Site-to-Site VPN の機能が破損する可能性があります。Site-to-Site VPN が指示する場合以外は、サービスロールを編集しないでください。

Site-to-Site VPN のサービスにリンクされたロール

サービスリンクロールのサポート	Yes

サービスにリンクされたロールは、にリンクされているサービスロールの一種です。 AWS のサービスサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。AWS アカウント サービスにリンクされたロールはに表示され、そのサービスが所有します。IAM 管理者は、サービスリンクロールの権限を表示できますが、編集することはできません。

サービスリンクロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、サービスにリンクされたロール 列に Yesと記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

Site-to-Site VPN の ID AWS ベースのポリシーの例

デフォルトでは、ユーザーおよびロールには Site-to-Site VPN リソースを作成または変更する許可はありません。また、、 AWS Command Line Interface (AWS CLI) AWS Management Console、API を使用してタスクを実行することもできません。 AWS IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドの「IAM ポリシーの作成」を参照してください。

各リソースタイプの ARN の形式など、Site-to-Site VPN によって定義されるアクションとリソースタイプの詳細については、サービス認証リファレンスの「AWS Site-to-Site VPN のアクション、リソース、および条件キー」を参照してください。

トピック

- ポリシーのベストプラクティス
- Site-to-Site VPN コンソールの使用
- 特定のSite-to-Site VPN 接続について説明する
- 接続に必要なリソースの作成と説明 AWS Site-to-Site VPN

ポリシーのベストプラクティス

アイデンティティベースのポリシーは、ユーザーのアカウントで誰かが Site-to-Site VPN リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースのポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください。

- AWS 管理ポリシーから始めて、最小権限の権限に移行する — ユーザーとワークロードへの権限の付与を開始するには、AWS 多くの一般的なユースケースで権限を付与する管理ポリシーを使用してください。これらのポリシーは、で利用できます。 AWS アカウント AWS ユースケースに固有のカスタマー管理ポリシーを定義して、権限をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定するときは、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、 最小特権アクセス許可 とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。サービスアクションがなどの特定の用途で使用された場合は AWS のサービス、条件を使用してサービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) が必要 — IAM ユーザーまたは root ユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA をオンにしてください。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

Site-to-Site VPN コンソールの使用

AWS Site-to-Site VPN コンソールにアクセスするには、最低限の権限が必要です。これらの権限により、内のSite-to-Site VPN リソースの詳細を一覧表示して表示できる必要があります。 AWS アカウント最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、その

ポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または API のみを呼び出しているユーザーには、最低限のコンソール権限を与える必要はありません。 AWS 代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

ユーザーとロールが引き続きSite-to-Site VPN コンソールを使用できるようにするには、Site-to-Site VPN `AmazonVPCFullAccess` `AmazonVPCReadOnlyAccess` AWS または管理ポリシーもエンティティにアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

特定のSite-to-Site VPN 接続について説明する

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": [
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-04d5cc9b88example",
         "arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-903004f88example",
         ]
      }
   ]
}
```

接続に必要なリソースの作成と説明 AWS Site-to-Site VPN

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
         "ec2:DescribeVpnConnections",
         "ec2:DescribeVpnGateways",
         "ec2:DescribeCustomerGateways",
```

```
            "ec2:CreateCustomerGateway",
            "ec2:CreateVpnGateway",
            "ec2:CreateVpnConnection"
            ],
            "Resource": [
               "*"
            ]
         },
      {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
            "Condition": {
               "StringLike": {
                  "iam:AWSServiceName":"s2svpn.amazonaws.com"
               }
            }
         }
      ]
}
```

AWS Site-to-Site VPN の ID とアクセスのトラブルシューティング

次の情報は、Site-to-Site VPN と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- Site-to-Site VPN でアクションを実行する権限がない
- 私にはiam を実行する権限がありません:PassRole
- 自分以外のユーザーがSite-to-Site VPN AWS アカウント リソースにアクセスできるようにしたい

Site-to-Site VPN でアクションを実行する権限がない

「I am not authorized to perform an action in Amazon Bedrock」というエラーが表示された場合、そのアクションを実行できるようにポリシーを更新する必要があります。

次の例は、mateojackson という IAM ユーザーがコンソールを使用して架空の *my-example-widget* リソースに関する詳細を表示しようとしたとき、架空の ec2:*GetWidget* アクセス許可がない場合に発生するエラーを示しています。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:GetWidget on resource: my-example-widget
```

この場合、ec2:*GetWidget* アクションを使用して *my-example-widget*リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、管理者に問い合わせてください。 AWS サインイン資格情報を提供した担当者が管理者です。

私にはiam を実行する権限がありません:PassRole

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Site-to-Site VPN にロールを渡せるようにする必要があります。

新しいサービスロールやサービスにリンクされたロールを作成する代わりに、 AWS のサービス 既存のロールをそのサービスに渡すことができるものもあります。そのためには、サービスにロールを渡すアクセス許可が必要です。

以下のエラー例は、marymajor という名前の IAM ユーザーがコンソールを使用して Site-to-Site VPN でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。Mary には、ロールをサービスに渡す権限がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、メアリーのポリシーを更新してメアリーに iam:PassRoleアクションの実行を許可する必要があります。

サポートが必要な場合は、管理者に問い合わせてください。 AWS サインイン資格情報を提供した担当者が管理者です。

自分以外のユーザーがSite-to-Site VPN AWS アカウント リソースにアクセスできるようにしたい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまた

はアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- Site-to-Site VPN がこれらの機能をサポートするかどうかについては、「AWS Site-to-Site VPN と IAM の連携の仕組み」を参照してください。
- AWS アカウント 所有しているリソース全体のリソースへのアクセスを提供する方法については、『IAM ユーザーガイド』の「AWS アカウント 所有する別の IAM ユーザーへのアクセスの提供」を参照してください。
- リソースへのアクセスを第三者に提供する方法については AWS アカウント、IAM ユーザーガイドの「AWS アカウント 第三者が所有するリソースへのアクセスの提供」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いの詳細については、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Site-to-Site VPN のサービスにリンクされたロールの使用

AWS Site-to-Site VPN は AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。 サービスにリンクされたロールは、Site-to-Site VPN に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールはSite-to-Site VPN によって事前定義されており、 AWS ユーザーに代わってサービスが他のサービスを呼び出すために必要なすべての権限が含まれます。

サービスにリンクされたロールを使用することで、必要なアクセス権限を手動で追加する必要がなくなるため、Site-to-Site VPN の設定が簡単になります。Site-to-Site VPN は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、Site-to-Site VPN のみがそのロールを引き受けることができます。定義された権限には、信頼ポリシーと権限ポリシーに含まれており、その権限ポリシーを他の IAM エンティティにアタッチすることはできません。

サービスリンクロールは、まずその関連リソースを削除しなければ削除できません。これにより、リソースへの意図しないアクセスによる許可の削除が防止され、Site-to-Site VPN リソースは保護されます。

サービスにリンクされたロールをサポートする他のサービスについては、「IAM と連動するAWS のサービス」を参照し、Service-linked roles (サービスにリンクされたロール) の列内で Yes (はい) と

表記されたサービスを確認してください。そのサービスに関するサービスリンクロールのドキュメントを表示するには、リンクが設定されている [Yes (はい)] を選択します。

Site-to-Site VPN のサービスにリンクされたロールのアクセス許可

Site-to-Site VPN は、「Site-to-Site VPN を許可する」AWSServiceRoleForVPCS2SVPNというサービスにリンクされたロールを使用して、VPN 接続に関連するリソースの作成と管理を行います。

AWSServiceRoleForVPCS2SVPN サービスにリンクされたロールは、以下のサービスを信頼してロールを引き受けます。

- `AWS Certificate Manager`
- `AWS Private Certificate Authority`

AWSVPCS2SVpnServiceRolePolicy という名前のロール権限ポリシーにより、Site-to-Site VPN は指定されたリソースに対して次のアクションを実行できます。

- アクション: `Resource: "*"` 上で `acm:ExportCertificate`
- アクション: `Resource: "*"` 上で `acm:DescribeCertificate`
- アクション: `Resource: "*"` 上で `acm:ListCertificates`
- アクション: `acm-pca:DescribeCertificateAuthority` 上で `Resource: "*"`

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、権限を設定する必要があります。詳細については、「IAM User Guide」(IAM ユーザーガイド) の「Service-linked role permissions」(サービスリンクロールのアクセス権限) を参照してください。

Site-to-Site VPN のサービスにリンクされたロールの作成

サービスリンクロールを手動で作成する必要はありません。、、または AWS API に関連付けられた ACM プライベート証明書を使用してカスタマーゲートウェイを作成すると AWS Management Console、Site-to-Site VPN によってサービスにリンクされたロールが自動的に作成されます。 AWS CLI

このサービスリンクロールを削除した後で再度作成する必要が生じた場合は、同じ方法でアカウントにロールを再作成できます。関連付けられた ACM プライベート証明書を使用してカスタマーゲートウェイを作成すると、Site-to-Site VPN によってサービスにリンクされたロールが再度作成されます。

Site-to-Site VPN のサービスにリンクされたロールの編集

Site-to-Site VPN では、 AWSServiceRoleForVPCS2SVPN サービスにリンクされたロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロールの説明の編集はできます。詳細については、「IAM ユーザーガイド」の「サービスリンクロールの編集」を参照してください。

Site-to-Site VPN のサービスにリンクされたロールの削除

サービスリンクロールが必要な機能またはサービスが不要になった場合には、そのロールを削除することをお勧めします。そうすることで、積極的にモニタリングまたは保守されていない未使用のエンティティを排除できます。ただし、手動で削除する前に、サービスリンクロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、Site-to-Site VPN サービスでそのロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから操作を再試行してください。

が使用するSite-to-Site VPN リソースを削除するには AWSServiceRoleForVPCS2SVPN

このサービスにリンクされたロールは、関連付けられた ACM プライベート証明書を持つすべてのカスタマーゲートウェイを削除した後にのみ削除できます。これにより、Site-to-Site VPN 接続で使用されている ACM 証明書へのアクセス許可を誤って削除してしまうことがなくなります。

サービスにリンクされたロールを IAM で手動削除するには

IAM コンソール、、または AWS API を使用して AWS CLI、サービスにリンクされたロールを削除します。 AWSServiceRoleForVPCS2SVPN詳細については、IAM ユーザーガイドの「サービスリンクロールの削除」を参照してください。

のレジリエンス AWS Site-to-Site VPN

AWS AWS グローバルインフラストラクチャはリージョンとアベイラビリティーゾーンを中心に構築されています。 AWS リージョンには、物理的に分離され隔離された複数のアベイラビリティーゾーンがあり、低レイテンシー、高スループット、冗長性の高いネットワークで接続されています。

アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョンとアベイラビリティーゾーンの詳細については、「グローバルインフラストラクチャ」を参照してください。AWS

AWS グローバルなインフラストラクチャに加えて、Site-to-Site VPN は、データの回復力とバックアップのニーズをサポートする機能も提供します。

VPN 接続ごとに 2 つのトンネル

Site-to-Site VPN 接続は 2 つのトンネルで構成され、それぞれが異なるアベイラビリティーゾーンで終端されるため、VPC の可用性が向上します。内部でデバイスに障害が発生した場合 AWS、VPN 接続は自動的に 2 番目のトンネルにフェールオーバーされるため、アクセスが中断されることはありません。 AWS また、時々 VPN 接続の定期メンテナンスを実施します。これにより、VPN 接続の 2 つのトンネルのうちの 1 つが一時的に無効になることがあります。詳細については、「Site-to-Site VPN トンネルエンドポイントの置換」を参照してください。したがって、カスタマーゲートウェイを設定するときは、両方のトンネルを設定することが重要です。

冗長性

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 つ目の Site-to-Site VPN 接続をセットアップできます。詳細については、次のドキュメントを参照してください。

- 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
- Amazon Virtual Private Cloud Connectivity Options
- スケーラブルで安全なマルチ VPC AWS ネットワークインフラストラクチャの構築

AWS Site-to-Site VPN のインフラストラクチャセキュリティ

マネージドサービスとして、 AWS Site-to-Site VPN AWS はグローバルネットワークセキュリティによって保護されています。 AWS AWS セキュリティサービスとインフラストラクチャの保護方法については、「AWS クラウドセキュリティ」を参照してください。 AWS インフラストラクチャセキュリティのベストプラクティスを使用して環境を設計するには、「Security Pillar AWS Well-Architected Framework におけるインフラストラクチャ保護」を参照してください。

AWS 公開されている API 呼び出しを使用して、ネットワーク経由でSite-to-Site VPN にアクセスします。クライアントは以下をサポートする必要があります:

- Transport Layer Security (TLS)。TLS 1.2、できれば TLS 1.3 が必要です。
- DHE (Ephemeral Diffie-Hellman) や ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) などの Perfect Forward Secrecy (PFS) を使用した暗号スイート。これらのモードは、Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストには、アクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、AWS Security Token ServiceAWS STS を使用して、一時的なセキュリティ認証情報を生成し、リクエストに署名することもできます。

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、 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?
- どのリソースをモニタリングしますか?
- 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?
- どのモニタリングツールを利用しますか?
- 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 には、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が用意されています。これらのツールの一部はモニタリングを行うように設定できますが、一部のツールは手動による介入が必要です。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、複数の期間にわたる特定のしきい値に対するメトリクスの値に基づいて 1 つ以上のアクションを実行します。アクションは、Amazon SNS topic. CloudWatch alarms に送信される通知です。アクションは、単に特定の状態にあるというだけでは呼び出されません。状態が変わり、それが指定された期間にわたって持続している必要があります。詳細については、「Amazon を使用した VPN トンネルのモニタリング CloudWatch」を参照してください。
- AWS CloudTrail ログのモニタリング – アカウント間でログファイルを共有し、 CloudTrail ログを CloudWatch Logs に送信してリアルタイムでログファイルをモニタリングし、Java でログ処理アプリケーションを記述して、 による配信後にログファイルが変更されていないことを確認します CloudTrail。詳細については、「Amazon EC2 API リファレンス」の「 を使用した API コールのログ記録 AWS CloudTrail」および「 AWS CloudTrail ユーザーガイド」の CloudTrail 「ログファイルの操作」を参照してください。
- AWS Health イベント – Site-to-Site VPN トンネルのヘルス状態の変化、ベストプラクティス設定の推奨事項、またはスケーリング制限に近づいたときに関連するアラートと通知を受信します。Personal Health Dashboard のイベントを使用して、自動フェイルオーバーをトリガーしたり、トラブルシューティング時間を短縮したり、接続を最適化して高可用性を実現したりします。詳細については、「AWS Health イベントを使用した VPN 接続のモニタリング」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 と CloudWatch コンソールのダッシュボードには、 AWS 環境の状態 at-a-glance が表示されます。

> **Note**
>
> Amazon VPC コンソールでは、「ステータス」や「最終ステータス変更」などの Site-to-Site VPN トンネル状態パラメータは、一時的な状態の変化や一時的なトンネルフラッドを反映していない場合があります。トンネル状態変更の詳細な更新には、 CloudWatch メトリクスとログを使用することをお勧めします。

- 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)]、サイト間 VPN 接続、[トンネル詳細] の順に選択します)
- CloudWatch ホームページには以下が表示されます。
  - 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
  - サービスのヘルスステータス

  さらに、 CloudWatch を使用して次の操作を実行できます。
  - 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します
  - 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
  - すべての AWS リソースメトリクスを検索および参照する
  - 問題があることを通知するアラームを作成/編集する

AWS Site-to-Site VPN ログ

AWS Site-to-Site VPN ログを使用すると、Site-to-Site VPN デプロイをより詳細に把握できます。この機能を使用すると、IP セキュリティ (IPsec)トンネル確立、インターネットキー交換 (IKE) ネゴシエーション、およびデッドピア検出 (DPD) プロトコルメッセージの詳細を示す Site-to-Site VPN 接続ログにアクセスできます。

Site-to-Site VPN ログは Amazon CloudWatch Logs に発行できます。この機能により、単一の一貫した方法で、すべての Site-to-Site VPN 接続の詳細なログにアクセスして分析できます。

コンテンツ

Site-to-Site VPN ログの利点

- VPN のトラブルシューティングの簡素化： Site-to-Site VPN ログは、 と AWS カスタマーゲートウェイデバイス間の設定の不一致を特定し、VPN 接続の初期の問題に対処するのに役立ちます。VPN 接続は、設定の誤り (不適切なタイムアウトの調整など) が原因で、時間の経過とともに断続的にフラップすることがあります。また、基盤となるトランスポートネットワークに問題 (インターネットの不安定など) が発生したり、ルーティングの変更やパスの障害によって VPN 経由の接続が中断されたりすることがあります。この機能により、断続的な接続障害の原因を正確に診断し、低レベルのトンネル設定を微調整して信頼性の高い動作を実現できます。
- 一元的な AWS Site-to-Site VPN 可視性： Site-to-Site VPN ログは、インターネットと AWS Direct Connect トランスポートの両方を使用して、Site-to-Site VPN が接続されているすべてのさまざまな方法のトンネルアクティビティログを提供できます。仮想ゲートウェイ、トランジットゲートウェイ CloudHub、および です。この機能により、単一の一貫した方法で、すべての Site-to-Site VPN 接続の詳細なログにアクセスして分析できます。
- セキュリティとコンプライアンス： Site-to-Site VPN ログを Amazon CloudWatch Logs に送信して、VPN 接続のステータスとアクティビティを時系列で遡及的に分析できます。これはコンプライアンスおよび規制要件に準拠するのに役立ちます。

Amazon CloudWatch Logs リソースポリシーのサイズ制限

CloudWatch ログリソースポリシーは 5,120 文字に制限されています。 CloudWatch Logs は、ポリシーがこのサイズ制限に近づいていることを検出すると、 で始まるロググループを自動的に有効にします`/aws/vendedlogs/`。ログ記録を有効にすると、Site-to-Site VPN は、指定したロググループで CloudWatch Logs リソースポリシーを更新する必要があります。 CloudWatch Logs リソースポリシーのサイズ制限に達しないようにするには、ロググループ名の前に を付けます`/aws/vendedlogs/`。

Site-to-Site VPN ログの内容

Site-to-Site VPN トンネルのアクティビティログに含まれる情報は以下のとおりです。

フィールド	説明
VpnLogCreationTimestamp	人間が読める形式でのログ作成タイムスタンプ。
VpnConnectionId	VPN 接続の識別子。
TunnelOutsideIPAddress	ログエントリを生成した VPN トンネルの外部 IP。
TunnelDPDEnabled	デッドピア検出プロトコルの有効ステータス (True/False)。
TunnelCGWNATTDetectionStatus	カスタマーゲートウェイデバイスでの NAT-T の検出 (True/False)。
TunnelIKEPhase1State	IKE フェーズ 1 プロトコル状態 (確立済み | キー更新中 | ネゴシエーション中 | ダウン)。
TunnelIKEPhase2State	IKE フェーズ 2 プロトコル状態 (確立済み | キー更新中 | ネゴシエーション中 | ダウン)。
VpnLogDetail	IPsec、IKE、および DPD プロトコルの詳細メッセージ。

コンテンツ

IKEv1 エラーメッセージ

メッセージ	説明
ピアが応答しない - ピア停止が宣言される	ピアが DPD メッセージに応答しなかったため、DPD タイムアウトアクションが強制されます。
AWS 事前共有キーが無効であるため、トンネルペイロードの復号に失敗しました	両方の IKE ピアに同じ事前共有キーを設定する必要があります。
によって一致する提案が見つかりませんでしたAWS	フェーズ 1 で提案された属性 (暗号化、ハッシュ、DH グループ) は AWS VPN エンドポイントではサポートされていません。例: 3DES
一致する提案が見つかりませんでした。「提案が選択されていません」と通知される	IKE ピアのフェーズ 2 で正しい提案/ポリシーを設定する必要があることを通知するため、「提案が選択されていません」というエラーメッセージがピア間で交換されます。
AWS トンネルは、SPI: xxxx のフェーズ 2 SA の DELETE を受け取りました	CGW はフェーズ 2 の Delete_SA メッセージを送信しました
AWS トンネルが CGW から IKE_SA の DELETE を受信しました	CGW はフェーズ 1 の Delete_SA メッセージを送信しました

IKEv2 エラーメッセージ

メッセージ	説明
AWS {retry_count} の再送信後にトンネル DPD がタイムアウトしました	ピアが DPD メッセージに応答しなかったため、DPD タイムアウトアクションが強制されます。
AWS トンネルが CGW から IKE_SA の DELETE を受信しました	ピアは親/IKE_SA に Delete_SA メッセージを送信しました

メッセージ	説明
AWS トンネルは、SPI: xxxx のフェーズ 2 SA の DELETE を受け取りました	ピアは CHILD_SA に Delete_SA メッセージを送信しました
AWS トンネルが (CHILD_REKEY) 衝突を CHILD_DELETE として検出しました	CGW は Active SA に Delete_SA メッセージを送信しました。このメッセージはキー変更中です。
AWS トンネル (CHILD_SA) の冗長 SA は、検出された衝突により削除されています	衝突により、冗長 SA が生成されると、ピアは RFC に従ってノンス値と一致させた後で冗長 SA を閉じます
AWS フェーズ 1 を維持している間、 トンネルフェーズ 2 を確立できませんでした	提案の誤りなどのネゴシエーションエラーにより、ピアは CHILD_SA を確立できませんでした。
AWS: トラフィックセレクタ: TS_UNACCEPLABLE: レスポンダから受信	ピアが不正なトラフィックセレクタ/暗号化ドメインを提案しました。ピアは、同一の正しい CIDR で設定する必要があります。
AWS トンネルは応答として AUTHENTICATION_FAILED を送信しています	ピアは IKE_AUTH メッセージ内容の検証によりピアを認証できません
AWS トンネルは cgw: xxxx との事前共有キーの不一致を検出しました	両方の IKE ピアに同じ事前共有キーを設定する必要があります。
AWS トンネルタイムアウト: cgw: xxxx を持つ確立されていないフェーズ 1 IKE_SA の削除	ピアがネゴシエーションを進めていないため、半分開いている IKE_SA を削除しています
一致する提案が見つかりませんでした。「提案が選択されていません」と通知される	IKE ピアには正しい提案を設定する必要があることを通知する、「提案が選択されていません」というエラーメッセージがピア間で交換されます。
によって一致する提案が見つかりませんでした AWS	フェーズ 1 で提案された属性 (暗号化、ハッシュ、DH グループ) は AWS VPN エンドポイントではサポートされていません。例: 3DES

IKEv2 ネゴシエーションメッセージ

メッセージ	説明
AWS トンネルは、CREATE_CHILD_SA のリクエスト (id=xxx) を処理しました	AWS が CGW から CREATE_CHILD_SA リクエストを受信しました
AWS トンネルは CREATE_CHILD_SA のレスポンス (id=xxx) を送信しています	AWS は CREATE_CHILD_SA レスポンスを CGW に送信しています
AWS トンネルは CREATE_CHILD_SA のリクエスト (id=xxx) を送信しています	AWS は CREATE_CHILD_SA リクエストを CGW に送信しています
AWS トンネルは CREATE_CHILD_SA のレスポンス (id=xxx) を処理しました	AWS は CGW から CREATE_CHILD_SA レスポンスフォームを受信しました

CloudWatch ログに発行する IAM 要件

ログ機能が正しく動作するためには、機能の設定に使用されている IAM プリンシパルにアタッチされた IAM ポリシーに、少なくとも以下のアクセス許可が含まれている必要があります。詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「特定の AWS サービスからのログ記録を有効にする」セクションにも記載されています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
```

```
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Site-to-Site VPN ログ設定を表示する

現在のトンネルログ記録設定を表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN Connections] (Site-to-Site VPN 接続) を選択します。
3. 表示する VPN 接続を [VPN connections] (VPN 接続) リストから選択します。
4. [Tunnel details] (トンネルの詳細) タブを選択します。
5. [Tunnel 1 options] (トンネル 1 オプション) セクションと [Tunnel 2 options] (トンネル 2 オプション) セクションを展開して、すべてのトンネル設定詳細を表示します。
6. ログ記録機能の現在のステータスは、トンネル VPN ログ で確認できます。また、現在設定 CloudWatchされているロググループ (存在する場合) はCloudWatch 、ロググループ で確認できます。

AWS コマンドラインまたは API を使用して Site-to-Site VPN 接続の現在のトンネルログ記録設定を表示するには

- DescribeVpnConnections (Amazon EC2 クエリ API)
- describe-vpn-connections (AWS CLI)

Site-to-Site VPN ログを有効にする

> **Note**
>
> 既存の VPN 接続トンネルで Site-to-Site VPN ログを有効にする場合、そのトンネルを介した接続が数分間中断される可能性があります。ただし、各 VPN 接続は高可用性を確保するために 2 つのトンネルを提供しているため、一度に 1 つのトンネルでログ記録を有効にし、変更していないトンネルを介して接続を維持できます。詳細については、「Site-to-Site VPN トンネルエンドポイントの置換」を参照してください。

新しい Site-to-Site VPN 接続の作成中に VPN ログ記録を有効にするには

「」の手順に従います。ステップ 5: VPN 接続を作成するステップ 9 の「トンネルオプション」では、両方のトンネルで使用するすべてのオプション (VPN ログ記録オプションを含む) を指定できます。これらのパラメータの詳細については、「Site-to-Site VPN 接続のトンネルオプション」を参照してください。

AWS コマンドラインまたは API を使用して新しい Site-to-Site VPN 接続でトンネルログ記録を有効にするには

- CreateVpnConnection (Amazon EC2 クエリ API)
- create-vpn-connection (AWS CLI)

既存の Site-to-Site VPN 接続のトンネルログ記録を有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN Connections] (Site-to-Site VPN 接続) を選択します。
3. 変更する VPN 接続を [VPN connections] (VPN 接続) リストから選択します。
4. [Actions] (アクション)、[Modify VPN tunnel options] (VPN トンネルオプションを変更) の順に選択します。
5. [VPN tunnel outside IP address] (IP アドレス外の VPN トンネル) リストから適切な IP アドレスを選択し、変更するトンネルを選択します。
6. [Tunnel activity log] (トンネルアクティビティログ) で、[Enable] (有効化) を選択します。
7. Amazon CloudWatch ロググループ で、 CloudWatch ログを送信する Amazon ロググループを選択します。

8. (オプション) [Output format] (出力形式) で、希望するログ出力の形式 (json またはテキスト) を選択します。
9. [Save Changes] (変更を保存) を選択します。
10. (オプション) 必要に応じて、他のトンネルに対してステップ 4〜9 を繰り返します。

AWS コマンドラインまたは API を使用して既存の Site-to-Site VPN 接続でトンネルログ記録を有効にするには

- ModifyVpnTunnelOptions (Amazon EC2 クエリ API)
- modify-vpn-tunnel-options (AWS CLI)

Site-to-Site VPN ログを無効にする

Site-to-Site VPN 接続のトンネルログ記録を無効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Site-to-Site VPN Connections] (Site-to-Site VPN 接続) を選択します。
3. 変更する VPN 接続を [VPN connections] (VPN 接続) リストから選択します。
4. [Actions] (アクション)、[Modify VPN tunnel options] (VPN トンネルオプションを変更) の順に選択します。
5. [VPN tunnel outside IP address] (IP アドレス外の VPN トンネル) リストから適切な IP アドレスを選択し、変更するトンネルを選択します。
6. [Tunnel activity log] (トンネルアクティビティログ) で、[Enable] (有効化) を選択します。
7. [Save Changes] (変更を保存) を選択します。
8. (オプション) 必要に応じて、他のトンネルに対してステップ 4〜7 を繰り返します。

AWS コマンドラインまたは API を使用して Site-to-Site VPN 接続のトンネルログ記録を無効にするには

- ModifyVpnTunnelOptions (Amazon EC2 クエリ API)
- modify-vpn-tunnel-options (AWS CLI)

Amazon 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 CloudWatch、VPN サービスから raw 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。

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

コンテンツ

VPN のメトリクスとディメンション

Site-to-Site VPN 接続では、次の CloudWatch 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 ESTABLISHED を示し、0 は他のすべての状態に使用されます。どちらのタイプの VPN でも、0 ~ 1 の値は、少なくとも 1 つのトンネルが UP 状態ではないことを示します。 単位: 0 から 1 までの少数値
`TunnelDataIn` †	カスタマーゲートウェイから VPN トンネルを介して接続の AWS 側で受信したバイト数。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。

メトリクス	説明
	このメトリクスは、復号化の後のデータをカウントします。 単位: バイト
TunnelDataOut †	VPN トンネルを介してカスタマーゲートウェイに接続の AWS 側から送信されたバイト数。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。 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。 単位: バイト

† これらのメトリクスは、トンネルがダウンしている場合でも、ネットワーク使用状況をレポートできます。これは、トンネルで定期的なステータスチェックが実行され、バックグラウンド ARP および BGP リクエストのためです。

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 CloudWatch メトリクスの表示

Site-to-Site VPN 接続を作成すると、VPN サービスは VPN 接続に関するメトリクスが利用可能になると CloudWatch、 に送信します。次のように、VPN 接続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/ で 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. メトリクスを表示するメトリクスディメンション (VPN トンネルメトリクス など) を選択します。

> **Note**
>
> VPN 名前空間は、表示している AWS リージョンで Site-to-Site VPN 接続が作成されるまで CloudWatch コンソールに表示されません。

を使用してメトリクスを表示するには AWS CLI

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"
```

VPN トンネルをモニタリングする CloudWatch アラームの作成

CloudWatch アラームの状態が変わったときに Amazon SNS メッセージを送信するアラームを作成できます。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。

例えば、1 つのVPN トンネルの状態をモニタリングし、15 分以内に 3 つのデータポイントでトンネルがダウン状態になったときに通知を送信するようなアラームを作成できます。

1 つの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/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[アラーム] を展開し、[すべてのアラーム] を選択します。
3. [アラームの作成] を選択し、[メトリクスの選択] を選択します。

4. [VPN] を選択し、[VPN トンネルのメトリクス] を選択します。
5. TunnelState メトリクスと同じ行で、目的のトンネルの IP アドレスを選択します。[メトリクスの選択] を選択します。
6. Forever TunnelState is... の場合は、「低」を選択し、「以下」の入力フィールドに「1」と入力します。
7. [追加設定] で、[アラーム対象のデータポイント] として「3 つのうち 3」と設定します。
8. [次へ] を選択します。
9. [通知を以下の SNS トピックに送信] で、既存の通知リストを選択するか、新しいリストを作成します。
10. [次へ] を選択します。
11. アラームの名前を入力します。[次へ] を選択します。
12. アラームの設定を確認し、[アラームの作成] をクリックします。

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。例えば、1 つまたは両方のトンネルのダウン状態が 5 分間 (1 つの期間) 連続した場合に通知を送信するアラームを作成できます。

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/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[アラーム] を展開し、[すべてのアラーム] を選択します。
3. [アラームの作成] を選択し、[メトリクスの選択] を選択します。
4. [VPN] を選択し、[VPN 接続のメトリクス] を選択します。
5. Site-to-Site VPN 接続と TunnelStateメトリクスを選択します。[メトリクスの選択] を選択します。
6. [統計] で、[最大] 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、[最小] 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。
7. [Whenever] (次の時) で、[Lower/Equal (<=)] (以下 (<=)) を選択し、0 と入力します (または、少なくとも 1 つのトンネルがダウンしている場合は 0.5 と入力します)。[次へ] を選択します。
8. [SNS トピックの選択] で、既存の通知リストを選択するか、[新しいリスト] をクリックして新しいリストを作成します。[次へ] を選択します。
9. アラームの名前と説明を入力します。[次へ] を選択します。

10. アラームの設定を確認し、[アラームの作成] をクリックします。

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/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[アラーム] を展開し、[すべてのアラーム] を選択します。
3. [アラームの作成] を選択し、[メトリクスの選択] を選択します。
4. [VPN] を選択し、[VPN トンネルのメトリクス] を選択します。
5. VPN トンネルの IP アドレスと TunnelDataInメトリクスを選択します。[メトリクスの選択] を選択します。
6. [統計] で、[合計] を指定します。
7. [期間] で、[15 分] を選択します。
8. [Whenever] (次の時) で、[Greater/Equal(>=)] (以上 (>=)) を選択し、5000000 と入力します。[次へ] を選択します。
9. [SNS トピックの選択] で、既存の通知リストを選択するか、[新しいリスト] をクリックして新しいリストを作成します。[次へ] を選択します。
10. アラームの名前と説明を入力します。[次へ] を選択します。
11. アラームの設定を確認し、[アラームの作成] をクリックします。

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/ で CloudWatch コンソールを開きます。
2. ナビゲーションペインで、[アラーム] を展開し、[すべてのアラーム] を選択します。
3. [アラームの作成] を選択し、[メトリクスの選択] を選択します。
4. [VPN] を選択し、[VPN トンネルのメトリクス] を選択します。
5. VPN トンネルの IP アドレスと TunnelDataOutメトリクスを選択します。[メトリクスの選択] を選択します。

6. [統計] で、[合計] を指定します。
7. [期間] で、[15 分] を選択します。
8. [次の時] で、[以下 (<=)] を選択し、「1000000」と入力します。[次へ] を選択します。
9. [SNS トピックの選択] で、既存の通知リストを選択するか、[新しいリスト] をクリックして新しいリストを作成します。[次へ] を選択します。
10. アラームの名前と説明を入力します。[次へ] を選択します。
11. アラームの設定を確認し、[アラームの作成] をクリックします。

アラームの作成のその他の例については、「Amazon 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。 CloudWatch

AWS Health イベントを使用した VPN 接続のモニタリング

AWS Site-to-Site VPN は、 AWS Health API AWS AWS Health Dashboardを使用する (PHD) に通知を自動的に送信します。このダッシュボードはセットアップを必要とせず、認証された AWS ユーザーに使用できる状態です。 AWS Health Dashboardを使用して、イベント通知に対応して複数のアクションを設定できます

AWS Health Dashboard には、VPN 接続に関する次のタイプの通知が用意されています。

- トンネルエンドポイント交換通知
- 単一トンネル VPN 通知

トンネルエンドポイント交換通知

VPN 接続の VPN トンネルエンドポイントの一方または両方が置き換えられると、トンネルエンドポイントの置き換え通知が に表示されます。 AWS Health Dashboard トンネルエンドポイントは、AWS がトンネルの更新を実行するとき、または VPN 接続を変更したときに交換されます。詳細については、「Site-to-Site VPN トンネルエンドポイントの置換」を参照してください。

トンネルエンドポイントの交換が完了すると、 は イベントを通じて AWS Health Dashboard トンネルエンドポイント交換通知 AWS を送信します。

単一トンネル VPN 通知

Site-to-Site VPN 接続は、冗長性のために 2 つのトンネルで構成されています。両方のトンネルの可用性を高めるよう設定することを強くお勧めします。VPN 接続で 1 つのトンネルはアップしている

が、もう 1 つが 1 日に 1 時間以上ダウンしている場合は、 AWS Health Dashboard イベントを通じて 毎月、VPN 単一トンネル通知が送信されます。このイベントは、新しい VPN 接続が単一トンネルとして検出されると毎日更新され、通知は毎週送信されます。毎月新しいイベントが作成され、これによって単一トンネルとして検出されなくなった VPN 接続がすべてクリアされます。

Site-to-Site VPN のクォータ

AWS アカウントには、Site-to-Site VPN に関連する、以下のクォータ (以前は制限と呼ばれていました) があります。特に明記されていない限り、クォータはリージョンごとに存在します。一部のクォータについては引き上げをリクエストできますが、その他のクォータについてはリクエストできません。

調整可能なクォータについて、クォータの引き上げをリクエストするには、[Adjustable] (調整可能) 列で [Yes] (はい) を選択します。詳細については、「Service Quotas ユーザーガイド」の「クォータ引き上げのリクエスト」を参照してください。

Site-to-Site VPN リソース

名前	デフォルト	調整可能
リージョンあたりのカスタマーゲートウェイの数	50	はい
リージョンあたりの仮想プライベートゲートウェイの数	5	はい
リージョンあたりの Site-to-Site VPN 接続の数	50	はい
仮想プライベートゲートウェイあたりの Site-to-Site VPN 接続の数	10	はい
リージョンあたりの高速化 Site-to-Site VPN 接続の数	10	[Yes (はい)]
リージョンあたりの関連付けられていない Site-to-Site VPN 接続の数	10	[Yes (はい)]

> **Note**
>
> 高速化接続と関連付けられていない接続の両方が、リージョンあたりの Site-to-Site VPN 接続の合計数にカウントされます。

一度に VPC にアタッチできる仮想プライベートゲートウェイは 1 つです。同じ Site-to-Site VPN 接続を複数の VPC に接続するには、代わりにトランジットゲートウェイを使用して調べることをお勧めします。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」を参照してください。

トランジットゲートウェイの Site-to-Site VPN 接続は、トランジットゲートウェイアタッチメントの合計制限の対象となります。詳細については、「Transit Gateway のクォータ」を参照してください。

ルート

アドバタイズされたルートソースには、VPC ルート、他の VPN ルート、および AWS Direct Connect 仮想インターフェイスからのルートが含まれます。アドバタイズされたルートは、VPN アタッチメントに関連付けられているルートテーブルから取得されます。

> **Note**
>
> 仮想プライベートゲートウェイを使用していて、VPC ルートテーブルでルート伝達が有効になっている場合、動的ルートと静的ルートの両方が VPN 接続に自動的に追加されます (VPC のルートテーブルの上限まで)。詳細については、Amazon VPC ユーザーガイドの「Amazon VPC クォータ」を参照してください。

名前	デフォルト	調整可能
カスタマーゲートウェイデバイスから仮想プライベートゲートウェイ上の Site-to-Site VPN 接続にアドバタイズされる動的ルート	100	いいえ
仮想プライベートゲートウェイ上の Site-to-Site VPN 接続からカスタマーゲートウェイデバイスにアドバタイズされるルート	1,000	いいえ
カスタマーゲートウェイデバイスから Transit Gateway 上の Site-to-Site VPN 接続にアドバタイズされる動的ルート	1,000	いいえ

名前	デフォルト	調整可能
Transit Gateway 上の Site-to-Site VPN 接続からカスタマーゲートウェイデバイスにアドバタイズされるルート	5,000	No
仮想プライベートゲートウェイ上のカスタマーゲートウェイデバイスから Site-to-Site VPN 接続への静的ルート	100	No

帯域幅とスループット

Site-to-Site VPN 接続を通じて実現される帯域幅に影響を与える要因には、パケットサイズ、トラフィックミックス (TCP/UDP)、中間ネットワークのシェーピングまたはスロットリングポリシー、インターネットの状況、特定のアプリケーション要件を始めとして多くのものがあります。

名前	デフォルト	調整可能
VPN トンネルごとの最大帯域幅	最大 1.25 Gbps	いいえ
VPN トンネルあたりの最大パケット/秒 (PPS)	最大 140,000	いいえ

トランジットゲートウェイ上の Site-to-Site VPN 接続の場合、ECMP を使用すると、複数の VPN トンネルを集約して、より高い VPN 帯域幅を確保できます。ECMP を使用するには、VPN 接続を動的ルーティング用に設定する必要があります。ECMP は、静的ルーティングを使用する VPN 接続ではサポートされません。詳細については、「トランジットゲートウェイ」を参照してください。

最大送信単位 (MTU)

Site-to-Site VPN は 1446 バイトの最大伝送ユニット（MTU）と 1406 バイトの対応する最大セグメントサイズ（MSS）をサポートします。ただし、大きな TCP ヘッダーを使用する特定のアルゴリズムでは、その最大値を効果的に減らすことができます。フラグメンテーションを回避するには、選択したアルゴリズムに基づいて MTU と MSS を設定することをお勧めします。MTU、MSS、および最適値の詳細については、カスタマーゲートウェイデバイスのベストプラクティス を参照してください。

ジャンボフレームはサポートされていません。詳細については、Linux インスタンス用 Amazon EC2 ユーザーガイドの「ジャンボフレーム」を参照してください。

Site-to-Site VPN 接続は、パス MTU 検出をサポートしていません。

その他のクォータリソース

トランジットゲートウェイのアタッチメントの数など、トランジットゲートウェイに関連するクォータについては、Amazon VPC トランジットゲートウェイガイドの「トランジットゲートウェイのクォータ」を参照してください。

VPC のその他のクォータについては、 Amazon VPC ユーザーガイドの「 Amazon VPC のクォータ」を参照してください。

Site-to-Site VPN ユーザーガイドのドキュメント履歴

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
クラシック VPN 情報が削除されました	ガイドからクラシック VPN に関する情報を削除しました。	2023 年 1 月 19 日
VPN ログメッセージの例	Site-to-Site VPN 接続のサンプルログを追加しました。	2022 年 12 月 9 日
更新されたダウンロード設定ユーティリティ	Site-to-Site VPN のお客様は、互換性のあるカスタマーゲートウェイ (CGW) デバイス用の設定テンプレートを生成できるため、AWS への VPN 接続を簡単に作成できます。この更新プログラムは、多くの一般的な CGW デバイスのインターネットキーエクスチェンジバージョン 2 (IKEv2) パラメーターのサポートを追加し、2 つの新しい API (GetVPnConnectionDeviceTypes と GetVPnConnectionDeviceSampleConfiguration) が含まれています。	2021 年 9 月 21 日
VPN 接続通知	Site-to-Site VPN は、VPN 接続に関する通知を AWS Health Dashboard に自動的に送信します。	2020 年 10 月 29 日
VPN トンネルの開始	AWS がトンネルを開始するように VPN トンネルを設定できます。	2020 年 8 月 27 日

VPN 接続オプションを変更する	Site-to-Site VPN 接続の接続オプションを変更できます。	2020 年 8 月 27 日
追加のセキュリティアルゴリズム	VPN トンネルに追加のセキュリティアルゴリズムを適用できます。	2020 年 8 月 14 日
IPv6 サポート	VPN トンネルは、トンネル内の IPv6 トラフィックをサポートできます。	2020 年 8 月 12 日
AWS Site-to-Site VPN マージガイド	このリリースでは、AWS Site-to-Site VPN ネットワーク管理者ガイドの内容がこのガイドにマージされます。	2020 年 3 月 31 日
高速 AWS Site-to-Site VPN 接続	AWS Site-to-Site VPN 接続の高速化を有効にできます。	2019 年 12 月 3 日
AWS Site-to-Site VPN トンネルオプションの変更	AWS Site-to-Site VPN 接続の VPN トンネルのオプションを変更できます。追加のトンネルオプションを設定することもできます。	2019 年 8 月 29 日
AWS Private Certificate Authority プライベート証明書のサポート	VPN を認証するための AWS Private Certificate Authority のプライベート証明書を使用できます。	2019 年 8 月 15 日
新しい Site-to-Site VPN ユーザーガイド	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

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。	2018 年 12 月 18 日
カスタム ASN	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。	2017 年 10 月 10 日
VPN トンネルオプション	VPN トンネルの内部トンネル CIDR ブロックとカスタム事前共有キーを指定できます。	2017 年 10 月 3 日
VPN メトリクス	VPN 接続の CloudWatch メトリクスを表示できます。	2017 年 5 月 15 日
VPN の機能強化	VPN 接続では、接続のフェーズ 1 およびフェーズ 2 中に、AES 256 ビットの暗号化関数、SHA-256 ハッシュ関数、NAT トラバーサル、および追加の Diffie-Hellman グループをサポートするようになりました。さらに、同じカスタマーゲートウェイデバイスを使用する各 VPN 接続用に同じカスタマーゲートウェイ IP アドレスを使用できるようになりました。	2015 年 10 月 28 日

静的なルーティング設定を使用した VPN 接続	静的なルーティング設定を使用して Amazon VPC への IPsec VPN 接続を作成できます。以前は、VPN 接続にはボーダーゲートウェイプロトコル (BGP) を使用する必要がありました。現在では両方のタイプの接続をサポートしており、Cisco ASA や Microsoft Windows Server 2008 R2 など、BGP をサポートしていないデバイスからの接続も可能です。	2012 年 9 月 13 日
ルートの自動伝播	VPN および AWS Direct Connect リンクから VPC ルーティングテーブルへのルートの自動伝播を設定できるようになりました。	2012 年 9 月 13 日
AWS VPN CloudHub と冗長な VPN 接続	VPC の有無にかかわらず、1 つのサイトから別のサイトに安全に通信できます。冗長な VPN 接続を使用して、VPC へのフォールトトレラントな接続ができます。	2011 年 9 月 29 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。