
AWS Site-to-Site VPN

ユーザーガイド



AWS Site-to-Site VPN: ユーザーガイド

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、お客様に混乱を招く可能性が高い方法、または Amazon の評判もしくは信用を損なう方法で、Amazon が所有しない製品またはサービスと関連付けて使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon と提携していたり、関連しているわけではありません。また、Amazon の後援を受けているとはかぎりません。

Table of Contents

Site-to-Site VPN とは	1
概念	1
Site-to-Site VPN の使用	1
Site-to-Site VPN の制限	2
料金	2
AWS Site-to-Site VPN の仕組み	3
Site-to-Site VPN コンポーネント	3
仮想プライベートゲートウェイ	3
トランジットゲートウェイ	3
カスタマーゲートウェイデバイス	4
カスタマーゲートウェイ	4
IPv4 および IPv6 のサポート	4
Site-to-Site VPN カテゴリ	4
Site-to-Site VPN トンネルオプション	5
Site-to-Site VPN トンネル認証オプション	10
事前共有キー	10
AWS Certificate Manager Private Certificate Authority からのプライベート証明書	10
Site-to-Site VPN トンネル開始オプション	10
VPN トンネル IKE 開始オプション	10
ルールと制限	11
VPN トンネル開始オプションの使用	11
エンドポイントの置換	11
VPN トンネルアップデート中のエンドポイントの置換	11
VPN 接続の変更時のエンドポイントの置換	12
カスタマーゲートウェイのオプション	12
Site-to-Site VPN 接続の高速化	13
高速化を有効にする	14
ルールと制限	14
料金	14
Site-to-Site VPN のルーティングオプション	14
静的および動的ルーティング	15
ルートテーブルと VPN ルーティングの優先度	15
VPN トンネルエンドポイント更新中のルーティング	17
IPv4 および IPv6 トラフィック	17
開始方法	18
Prerequisites	18
カスタマーゲートウェイを作成する	19
ターゲットゲートウェイを作成する	20
仮想プライベートゲートウェイの作成	20
トランジットゲートウェイを作成する	20
ルーティングを設定する	21
(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	21
(トランジットゲートウェイ) ルートテーブルにルートを追加します	22
セキュリティグループを更新する	22
サイト間 VPN 接続の作成	22
設定ファイルをダウンロードする	24
カスタマーゲートウェイデバイスを設定する	24
アーキテクチャ	25
単一および複数接続の例	25
単一の Site-to-Site VPN 接続	25
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	25
複数の Site-to-Site VPN 接続	26
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	26
AWS Direct Connect との Site-to-Site VPN 接続	27

AWS VPN CloudHub	27
概要	28
料金	29
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	29
カスタマーゲートウェイデバイス	32
設定ファイルの例	33
カスタマーゲートウェイデバイスの要件	35
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	38
複数の VPN 接続シナリオ	39
カスタマーゲートウェイデバイスのルーティング	40
静的ルーティングの設定例	40
設定ファイルの例	40
静的ルーティングのユーザーインターフェイス手順	42
Cisco デバイスの追加情報	51
Testing	52
動的ルーティング (BGP) の設定例	52
設定ファイルの例	52
動的ルーティングのユーザーインターフェイス手順	54
Cisco デバイスの追加情報	60
Juniper デバイスの追加情報	61
Testing	61
カスタマーゲートウェイデバイスとしての Windows Server	61
Windows インスタンスの設定	62
ステップ 1: VPN 接続を作成し、VPC を設定する	62
ステップ 2: VPN 接続の設定ファイルをダウンロードする	63
ステップ 3: Windows Server を設定する	64
ステップ 4: VPN トンネルを設定する	65
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	71
ステップ 6: VPN 接続をテストする	71
トラブルシューティング	72
BGP を使用するデバイス	72
BGP なしのデバイス	75
Cisco ASA	78
Cisco IOS	81
BGP なしの Cisco IOS	85
Juniper JunOS	89
Juniper ScreenOS	92
Yamaha	95
Site-to-Site VPN の使用	99
Site-to-Site VPN 接続の識別	99
AWS Classic VPN から AWS VPN への移行	100
オプション 1: 新しい仮想プライベートゲートウェイに直接移行する	100
オプション 2: トランジットゲートウェイを使用して移行する	102
オプション 3: (AWS Direct Connect の VPN 接続のバックアップ) VPN 接続を削除して再作成する	104
トランジットゲートウェイ VPN アタッチメントの作成	105
Site-to-Site VPN 接続のテスト	106
Site-to-Site VPN 接続の削除	107
Site-to-Site VPN 接続の削除	107
カスタマーゲートウェイの削除	108
仮想プライベートゲートウェイのデタッチと削除	108
Site-to-Site VPN 接続のターゲットゲートウェイの変更	109
ステップ 1: トランジットゲートウェイを作成する	109
ステップ 2: 静的ルート (静的 VPN 接続のトランジットゲートウェイへの移行に必要な) を削除する	110
ステップ 3: 新しいゲートウェイに移行する	110
ステップ 4: VPC ルートテーブルを更新する	111

ステップ 5: トランジットゲートウェイルーティングの更新 (新しいゲートウェイがトランジットゲートウェイである場合に必須)	111
ステップ 6: カスタマーゲートウェイ ASN を更新する (新しいゲートウェイに古いゲートウェイとは異なる ASN がある場合に必要)	112
Site-to-Site VPN 接続オプションの変更	112
Site-to-Site VPN トンネルオプションの変更	112
Site-to-Site VPN 接続の静的ルートの編集	113
Site-to-Site VPN 接続のカスタマーゲートウェイの変更	114
漏洩した認証情報の置き換え	114
Site-to-Site VPN トンネルエンドポイント証明書の更新	115
セキュリティ	116
データ保護	116
インターネットトラフィックのプライバシー	117
Identity and access management	118
Site-to-Site VPN 接続の IAM ポリシー	118
サービスにリンクされたロール	121
ログ記録とモニタリング	122
耐障害性	122
VPN 接続ごとに 2 つのトンネル	122
冗長性	123
インフラストラクチャセキュリティ	123
Site-to-Site VPN 接続のモニタリング	124
モニタリングツール	124
自動モニタリングツール	124
手動モニタリングツール	125
アマゾン CloudWatch を使用した VPN トンネルのモニタリング	125
VPN トンネルのメトリクスとディメンション	126
VPN トンネル CloudWatch メトリクスの表示	126
VPN トンネルをモニタリングする CloudWatch アラームの作成	127
AWS Health イベントを使用した VPN 接続のモニタリング	129
トンネルエンドポイント交換通知	129
単一トンネル VPN 通知	129
クォータ	130
Site-to-Site VPN リソース	130
Routes	130
帯域幅とスループット	131
最大送信単位 (MTU)	131
その他のクォータリソース	131
ドキュメント履歴	132

AWS Site-to-Site VPN とは

デフォルトでは、Amazon VPC 内に起動されるインスタンスとユーザー独自の (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。

Site-to-Site VPN 接続は、AWS Classic VPN または AWS VPN のいずれかです。詳細については、[Site-to-Site VPN カテゴリ \(p. 4\)](#) を参照してください。

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。
- 仮想プライベートゲートウェイ: サイト間 VPN 接続の Amazon 側にある VPN コンセントレータ。サイト間 VPN 接続の Amazon 側のゲートウェイとして、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使用します。
- トランジットゲートウェイ: 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トランジットハブ。サイト間 VPN 接続の Amazon 側のゲートウェイとして、トランジットゲートウェイまたは仮想プライベートゲートウェイを使用します。

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](#) を参照してください。
- 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。

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。

料金

料金については、[AWS VPN の料金](#)を参照してください。

AWS Site-to-Site VPN の仕組み

Site-to-Site VPN コンポーネント

Site-to-Site 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、リモート (オンプレミス) 側のカスタマーゲートウェイ (VPN デバイスを表す) の間に 2 つの VPN トンネルを提供します。

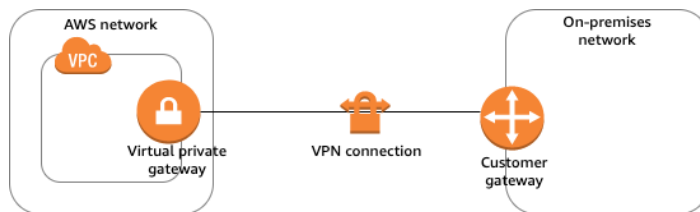
Site-to-Site VPN 接続は次のコンポーネントで構成されます。Site-to-Site VPN クォータの詳細については、「[Site-to-Site VPN のクォータ \(p. 130\)](#)」を参照してください。

目次

- [仮想プライベートゲートウェイ \(p. 3\)](#)
- [トランジットゲートウェイ \(p. 3\)](#)
- [カスタマーゲートウェイデバイス \(p. 4\)](#)
- [カスタマーゲートウェイ \(p. 4\)](#)

仮想プライベートゲートウェイ

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



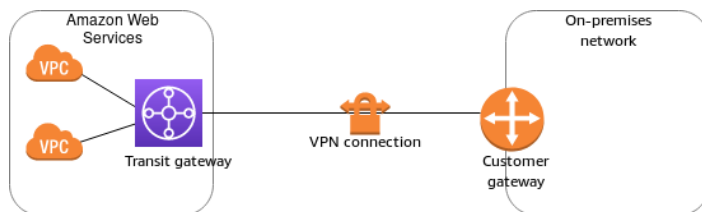
仮想プライベートゲートウェイを作成するとき、Amazon 側のゲートウェイのプライベート自律システム番号 (ASN) 指定できます。ASN を指定しない場合、仮想プライベートゲートウェイはデフォルトの ASN (64512) で作成されます。仮想プライベートゲートウェイの作成後に ASN を変更することはできません。仮想プライベートゲートウェイの ASN を確認するには、Amazon VPC コンソールの [仮想プライベートゲートウェイ] 画面で詳細を表示するか、[describe-vpn-gateways](#) AWS CLI コマンドを使用します。

Note

2018 年 6 月 30 日以前に仮想プライベートゲートウェイを作成した場合、デフォルトの ASN はアジアパシフィック (シンガポール) リージョンで 17493、アジアパシフィック (東京) リージョンで 10124、欧州 (アイルランド) リージョンで 9059、その他すべてのリージョンでは 7224 になります。

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、Virtual Private Cloud (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。



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、「」を参照してください[the section called “Site-to-Site VPN 接続のターゲットゲートウェイの変更” \(p. 109\)](#)

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、「」を参照してください[カスタマーゲートウェイデバイス \(p. 32\)](#)

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、「」を参照してください[Site-to-Site VPN トンネル開始オプション \(p. 10\)](#)

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提供しますAWS 詳細については、「」を参照してください[the section called “カスタマーゲートウェイのオプション” \(p. 12\)](#)

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 \(p. 32\)](#)」を参照してください。

IPv4 および IPv6 のサポート

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、「」を参照してください[IPv4 および IPv6 トラフィック \(p. 17\)](#)

Site-to-Site VPN カテゴリ

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

- Internet Key Exchange バージョン 2 (IKEv2)
- NAT トラバース

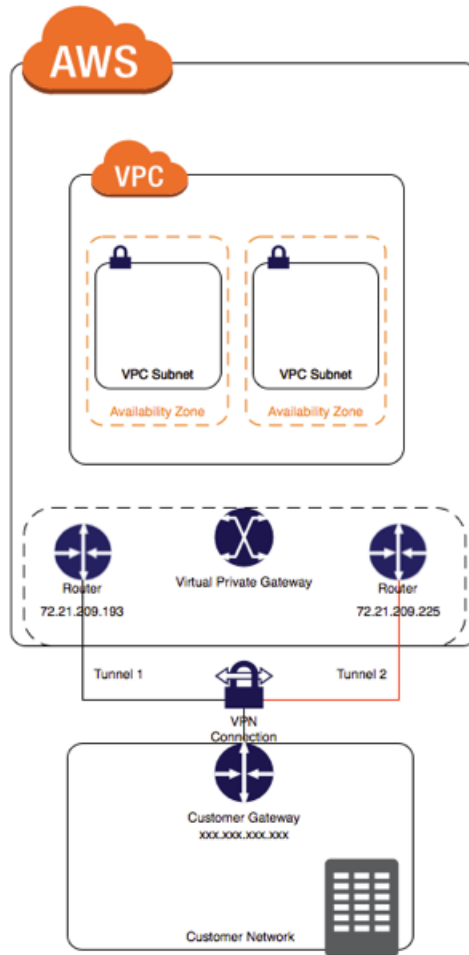
- 仮想プライベートゲートウェイ (VGW) 構成の場合、1~2147483647 の範囲の 4 バイトの ASN。詳細については、「[Site-to-Site VPN 接続のカスタマーゲートウェイオプション \(p. 12\)](#)」を参照してください。
- 1~65535 の範囲のカスタマーゲートウェイ (CGW) 用の 2 バイトの ASN。詳細については、「[Site-to-Site VPN 接続のカスタマーゲートウェイオプション \(p. 12\)](#)」を参照してください。
- CloudWatch メトリクス
- カスタマーゲートウェイのための再利用可能な IP アドレス
- 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 Certificate Manager 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

接続の識別と移行の詳細については、「[the section called “Site-to-Site VPN 接続の識別” \(p. 99\)](#)」および「[the section called “AWS Classic VPN から AWS VPN への移行” \(p. 100\)](#)」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仮想プライベートゲートウェイのパブリック IP アドレスを使用します。冗長性を確保するために両方のトンネルを設定することが重要です。1 つのトンネルが使用できなくなったとき (たとえばメンテナンスのために停止)、ネットワークトラフィックはその特定の Site-to-Site VPN 接続用に使用可能なトンネルへ自動的にルーティングされます。

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



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

Note

サイト間 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期間 (秒)。30 以上を指定できます。

デフォルト: 30

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、「」を参照してください[Site-to-Site VPN トンネル開始オプション \(p. 10\)](#)

デフォルト: `clear`

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。

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)

仮想プライベートゲートウェイとカスタマーゲートウェイ間に最初の 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 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: 540 (9 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、「」を参照してください[Site-to-Site VPN トンネル開始オプション \(p. 10\)](#)

デフォルト: Add

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。AWS Classic VPN 接続のトンネルオプションを設定することはできません。詳細については、次のトピックを参照してください。

- [サイト間 VPN 接続の作成 \(p. 22\)](#)
- [Site-to-Site VPN トンネルオプションの変更 \(p. 112\)](#)

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 \(p. 32\)](#)」を参照してください。

AWS Certificate Manager 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 Certificate Manager 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 Certificate Manager Private Certificate Authority (ACM 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 Certificate Manager 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、サービスにリンクされた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 “サービスにリンクされたロールによって付与されるアクセス許可” \(p. 121\)](#) 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。VPN トンネルの一方または両方のオプションを実装できます。

- 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。

Site-to-Site VPN 接続の VPN トンネルの一方または両方に IKE 開始オプションを設定できます。

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の変更 \(p. 114\)](#) を参照してください。
- AWS Classic VPN 接続には IKE 開始オプションを設定できません。
- 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。
- 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: [サイト間 VPN 接続の作成 \(p. 22\)](#)
- 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の変更 \(p. 112\)](#)

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。

トンネルエンドポイントが置き換えられた場合、AWS は AWS Personal Health Dashboard イベントを通じて通知を送信します。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 \(p. 129\)](#) を参照してください。

VPN トンネルアップデート中のエンドポイントの置換

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 は一度に VPN 接続の 1 つのトンネルにトンネルエンドポイントの更新を適用し、その間、VPN 接続では短時間冗長性が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。

VPN 接続の変更時のエンドポイントの置換

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	トンネルインバクト
VPN 接続のターゲットゲートウェイを変更する (p. 109)	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 (p. 114)	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 (p. 112)	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 (p. 112)	ModifyVpnTunnelOptions	更新中は、変更されたトンネルを使用できません。

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) 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、インターネットでルーティング可能な IP アドレス (静的)	<p>パブリック IP アドレスの値は静的な値である必要があります。カスタマーゲートウェイが NAT トラバーサル (NAT-T) が有効になっているネットワークアドレス変換 (NAT) の内側にある場合は、NAT デバイスのパブリック IP アドレスを使用し、UDP ポート 4500 をブロックしないようにファイアウォールルールを調整します。</p> <p>からのプライベート証明書を使用している場合、これは必須ではありませんAWS Certificate Manager Private Certificate Authority</p>
ルーティングのタイプ — 静的または動的	詳細については、「」を参照してください Site-to-Site VPN のルーティングオプション (p. 14)

項目	説明
(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。	<p>CGW では、1～65535 の範囲の 2 バイト 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 を使用できません。既存の ASN がない場合は、プライベート ASN (64512 から 65534 までの範囲) を使用できます。デフォルトの ASN は 65000 です。</p> <p>Amazon EC2 では、1～2147483647 の範囲 (以下を除く) の 4 バイトの ASN の番号がサポートされています。</p> <ul style="list-style-type: none"> 7224 - us-east-1 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 17943 - ap-southeast-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
(オプション) AWS Certificate Manager (ACM) を使用する下位 CA からのプライベート証明書	<p>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する ACM プライベート証明書の ARN を指定します。</p> <p>カスタマーゲートウェイを作成するときに、AWS Certificate Manager 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。</p> <p>このオプションを使用する場合は、組織が内部で使用するために、完全に AWS がホストするプライベート認証局 (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、ACM Private CA によって保存および管理されます。</p> <p>カスタマーゲートウェイを作成する前に、AWS Certificate Manager 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、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 Certificate Manager 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。</p>

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) 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。AWS Global Accelerator 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、ネットワークパスを最適化します (詳細については、[AWS Global Accelerator](#) を参照してください)。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 API を使用して、これらのアクセラレーターを自分で表示または管理することはできません。

Accelerated 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 Accelerated Site-to-Site VPN のよくある質問](#)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 アタッチメントの作成 \(p. 105\)](#)」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 \(p. 24\)](#)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。
- トンネルを維持するには、高速 VPN トンネルの IKE キー再生成を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。
- 証明書ベースの認証を使用する Site-to-Site VPN 接続は、グローバルアクセラレーター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。

料金

Site-to-Site VPN 接続には、時間単位の料金が適用されます。詳細については、[AWS VPN の料金](#)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 の料金](#)を参照してください。

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 ユーザーガイドの「[Amazon VPC クォータ](#)」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](#) (p. 15)
- [ルートテーブルと VPN ルーティングの優先度](#) (p. 15)
- [VPN トンネルエンドポイント更新中のルーティング](#) (p. 17)
- [IPv4 および IPv6 トラフィック](#) (p. 17)

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](#) (p. 32)」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。

AWS では、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、宛先は 172.31.0.0/24 です。この場合、172.31.0.0/24 を宛先とするすべてのトラフィックはインターネットゲートウェイにルーティングされます。これは静的ルートであるため、伝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。最長のプレフィックス一致が適用されます。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

両方のトンネルの AS PATH が等しくなるように、AS PATH の前置を使用することはお勧めしません。これにより、multi-exit discriminator (MED) 値 ([VPN トンネルエンドポイントの更新 \(p. 17\)](#)中にトンネルに設定したもの) を使用して、トンネルの優先度を決定できます。

- 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 \(p. 17\)](#)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。

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。ときどき、AWS は、VPN 接続の定期メンテナンスも実行します。これにより、VPN 接続の 2 つのトンネルの 1 つが短時間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 \(p. 129\)](#) 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、「[サイト間 VPN 接続の作成 \(p. 22\)](#)」を参照してください。

開始方法

AWS Site-to-Site VPN 接続を手動でセットアップするには、次の手順を実行します。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をターゲットゲートウェイとして使用して、Site-to-Site VPN 接続を作成できます。

Site-to-Site VPN 接続を設定するには、以下のステップを実行します。

- [Prerequisites \(p. 18\)](#)
- ステップ 1: [カスタマーゲートウェイを作成する \(p. 19\)](#)
- ステップ 2: [ターゲットゲートウェイを作成する \(p. 20\)](#)
- ステップ 3: [ルーティングを設定する \(p. 21\)](#)
- ステップ 4: [セキュリティグループを更新する \(p. 22\)](#)
- ステップ 5: [サイト間 VPN 接続の作成 \(p. 22\)](#)
- 手順 6: [設定ファイルをダウンロードする \(p. 24\)](#)
- 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 \(p. 24\)](#)

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

トランジットゲートウェイで Site-to-Site VPN 接続を作成するステップについては、「[トランジットゲートウェイ VPN アタッチメントの作成 \(p. 105\)](#)」を参照してください。

Prerequisites

Site-to-Site 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	<p>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。</p> <ul style="list-style-type: none">• 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 (p. 14)• 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 Certificate Manager Private Certificate Authority のプライベート証明書 <p>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 (p. 12)」を参照してください。</p>

項目	情報
(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トランジットゲートウェイ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、「」を参照してください 仮想プライベートゲートウェイ (p. 3)
VPN 接続	VPN 接続を作成するには、次の情報が必要です。 <ul style="list-style-type: none">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。(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、「」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 (p. 5)

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、「」を参照してください[カスタマーゲートウェイ \(p. 4\)](#)

プライベート証明書を使用して VPN を認証する場合は、AWS Certificate Manager 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 Certificate Manager 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

- Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
- ナビゲーションペインで [Customer Gateways] を選択してから、[Create Customer Gateway] をクリックします。
- 以下を入力し、[Create Customer Gateway] を選択します。
 - (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。
 - [Routing] では、ルーティングタイプを選択します。
 - 動的ルーティングの場合、[BGP ASN] に、ボーダーゲートウェイプロトコル (BGP) 自律システム番号 (ASN) を入力します。
 - (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。
 - (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。

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)

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トランジットゲートウェイ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、オプションで、Amazon 側のゲートウェイのプライベート自律システム番号 (ASN) 指定できます。ASN は、カスタマーゲートウェイに指定した BGP ASN とは異なっている必要があります。

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

仮想プライベートゲートウェイを作成して VPC にアタッチするには

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

トランジットゲートウェイを作成する

トランジットゲートウェイの作成の詳細については、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](#)」を参照してください。

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

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

Note

ルート伝達を有効にしない場合、Site-to-Site VPN 接続で使用される静的ルートを手動で入力する必要があります。これを行うには、ルートテーブルを選択し、[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] を選択後、サブネットに関連付けられたルートテーブルを選択します。
2. [ルート伝播]、[ルート伝播の編集] の順に選択します。仮想プライベートゲートウェイの [Propagate] チェックボックスをオフにし、[Save] 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)

(トランジットゲートウェイ) ルートテーブルにルート を追加します

トランジットゲートウェイ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トランジットゲートウェイ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 をトランジットゲートウェイにアタッチし、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、トランジットゲートウェイ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、[Route Tables (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 (ルート)] タブを選択し、[Edit routes (ルートの編集)] を選択します。
4. [ルート追加] を選択します。
5. [Destination (送信先)] 列に、送信先の IP アドレス範囲を入力します。[Target (ターゲット)] で、トランジットゲートウェイを選択します。
6. [Save routes (ルートの保存)] を選択し、次に、[閉じる] を選択します。

セキュリティグループを更新する

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

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

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

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

サイト間 VPN 接続の作成

カスタマーゲートウェイと、以前に作成した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使用して Site-to-Site VPN 接続を作成します。

Site-to-Site 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 Connections (Site-to-Site VPN 接続)]、[Create VPN Connection (VPN 接続の作成)] の順に選択します。

2. (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。
3. [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 (トランジットゲートウェイ)] 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トランジットゲートウェイを選択します。
4. [カスタマーゲートウェイ ID] で、以前に作成したカスタマーゲートウェイを選択します。
5. 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。[Static IP Prefixes (静的 IP プレフィックス)] では、Site-to-Site VPN 接続のプライベートネットワークのそれぞれの IP プレフィックスを指定します。
6. (オプション) [Tunnel Inside IP Version (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、トランジットゲートウェイの VPN 接続でのみサポートされます。
7. (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: 0.0.0.0/0。

[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: 0.0.0.0/0。

[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。

8. (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。
 - [Tunnel Inside IP Version (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。
 - 高度なトンネル情報。次の情報が含まれます。
 - IKE ネゴシエーションのフェーズ 1 および 2 の暗号化アルゴリズム
 - IKE ネゴシエーションのフェーズ 1 および 2 の整合性アルゴリズム
 - IKE ネゴシエーションのフェーズ 1 および 2 の Diffie-Hellman グループ
 - IKE バージョン
 - フェーズ 1 および 2 のライフタイム
 - キー再生成のマージンタイム
 - キー再生成ファズ
 - 再生ウィンドウのサイズ
 - デッドピア検出の間隔
 - デッドピア検出タイムアウトアクション
 - 開始アクション

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 \(p. 5\)](#)を参照してください。

9. [Create VPN Connection (VPN 接続の作成)] を選択します。Site-to-Site 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 Site-to-Site VPN 接続を作成するには

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

設定ファイルをダウンロードする

Site-to-Site 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

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。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 Site-to-Site 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。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。IKEv2 をサポートする設定ファイルの完全なリストは、「[カスタマーゲートウェイデバイス \(p. 32\)](#)」を参照してください。

AWS Management Console から設定ファイルをダウンロードするには

Note

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次の 2 つの Amazon EC2 API に対する許可を持っていることを確認してください: `GetVpnConnectionDeviceTypes` および `GetVpnConnectionDeviceSampleConfiguration`。

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. カスタマーゲートウェイデバイスに対応する、`vendor`、`platform`、`software` および `IKE version` を選択します。デバイスが一覧にない場合は、[Generic] を選択します。
5. [Download] を選択します。

AWS 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)

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、Site-to-Site 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、「」を参照してください。[カスタマーゲートウェイデバイス \(p. 32\)](#)

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。

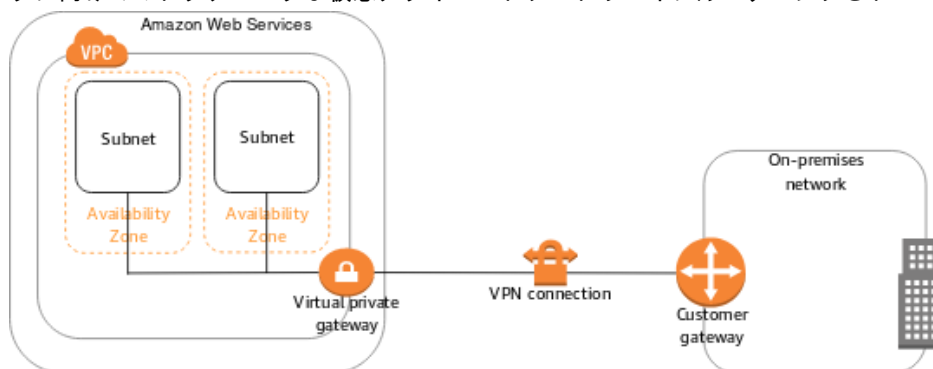
- the section called “単一および複数接続の例” (p. 25)
- the section called “冗長な Site-to-Site VPN 接続を使用してフェイルオーバーを提供する” (p. 29)
- the section called “AWS VPN CloudHub” (p. 27)

単一および複数の Site-to-Site 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。

単一の Site-to-Site VPN 接続

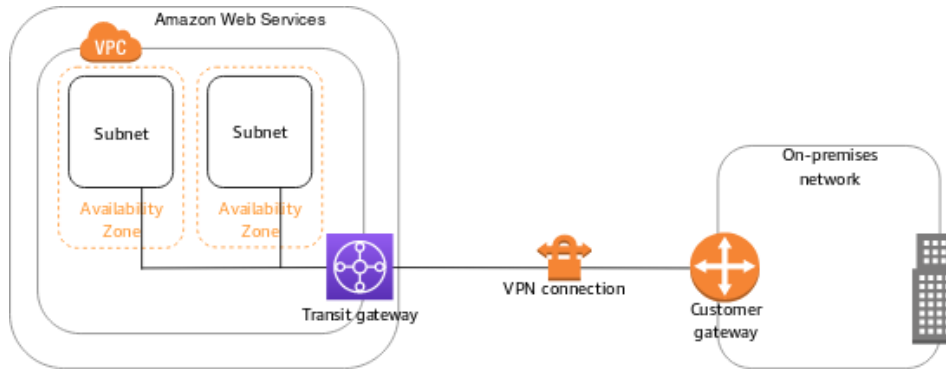
VPC には仮想プライベートゲートウェイが関連付けられていて、オンプレミス (リモート) ネットワークにはカスタマーゲートウェイが使用されています。カスタマーゲートウェイデバイスは、Site-to-Site VPN 接続を有効にするように設定する必要があります。ルーティングを設定して、VPC からユーザーネットワークに向けてのトラフィックが仮想プライベートゲートウェイにルーティングされるようにします。



このシナリオを設定するステップについては、「[開始方法 \(p. 18\)](#)」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、Site-to-Site VPN 接続を有効にするように設定する必要があります。ルーティングを設定して、VPC からユーザーネットワークに向けてのトラフィックが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。

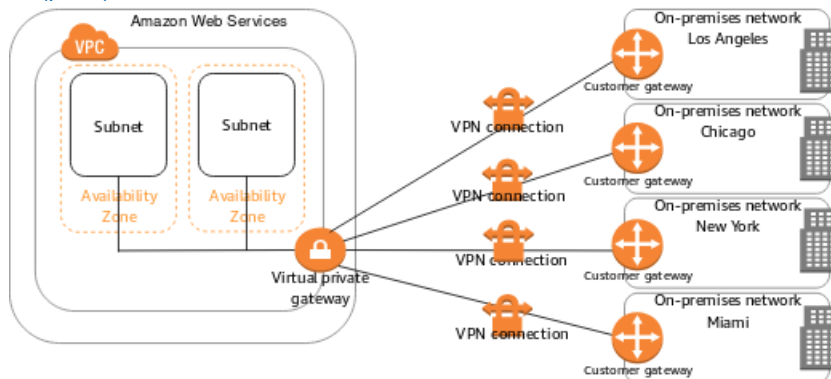


このシナリオを設定するステップについては、「[開始方法 \(p. 18\)](#)」を参照してください。

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。

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 \(p. 27\)](#)」を参照してください。

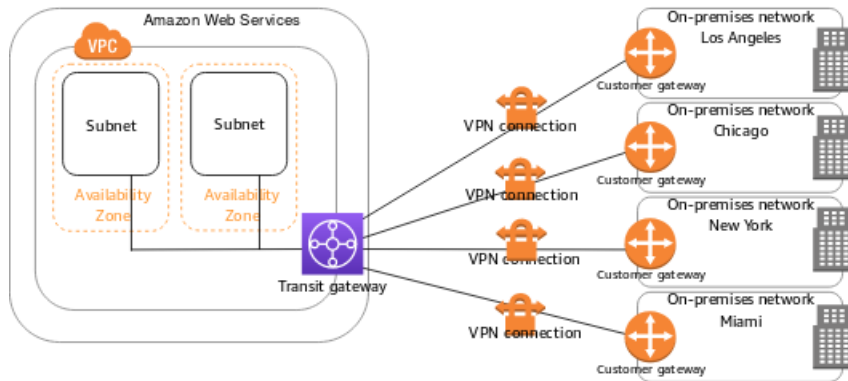


単一の VPC に対して複数の Site-to-Site VPN 接続を作成する場合、2 番目のカスタマーゲートウェイを設定して、外部にある同一の場所への冗長な接続を作成できます。詳細については、「[冗長な Site-to-Site VPN 接続を使用してフェイルオーバーを提供する \(p. 29\)](#)」を参照してください。

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。

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。



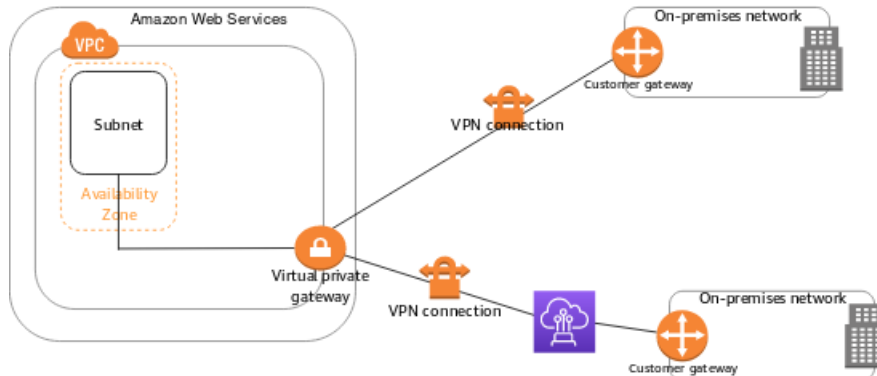
1つのトランジットゲートウェイに対して複数の Site-to-Site VPN 接続を作成する場合、2 番目のカスタマーゲートウェイを設定して、外部にある同一の場所への冗長な接続を作成できます。

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。

Note

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。



VPN CloudHub を使用して安全なサイト間通信を提供する

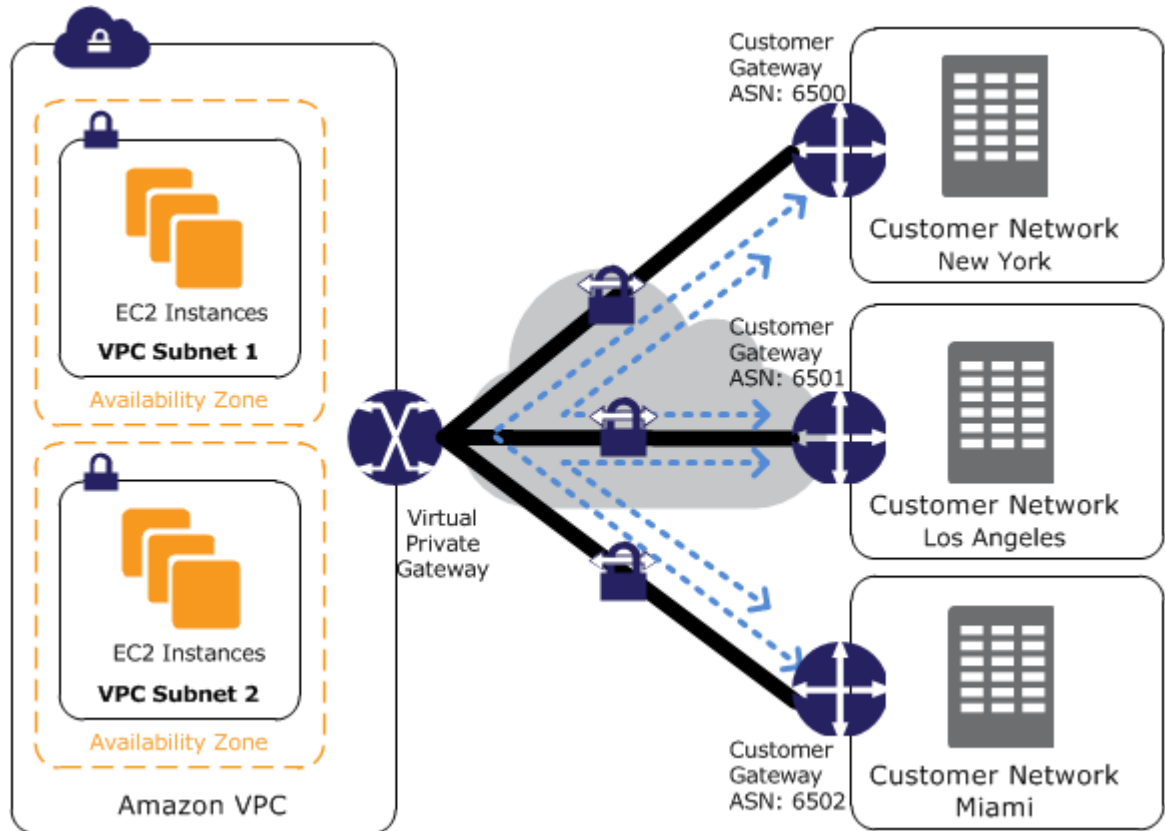
複数の AWS Site-to-Site VPN 接続がある場合は、AWS VPN CloudHub を使用して、安全な Site-to-Site 通信を提供することができます。これで、リモートサイトを有効にして、VPC のみではなく、相互に通信します。VPN CloudHub は、VPC の有無にかかわらず使用できるシンプルなハブアンドスポークモデルで動作します。この設計は、複数のブランチオフィスと既存のインターネット接続があり、リモートオフィ

ス間でプライマリ接続またはバックアップ接続を実現するために、便利でコストを抑えられる可能性のあるハブアンドスポークモデルを実装したいと考えている場合に適しています。

サイト間で IP 範囲が重複することは許可されません。

概要

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



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 \(p. 21\)](#)」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。

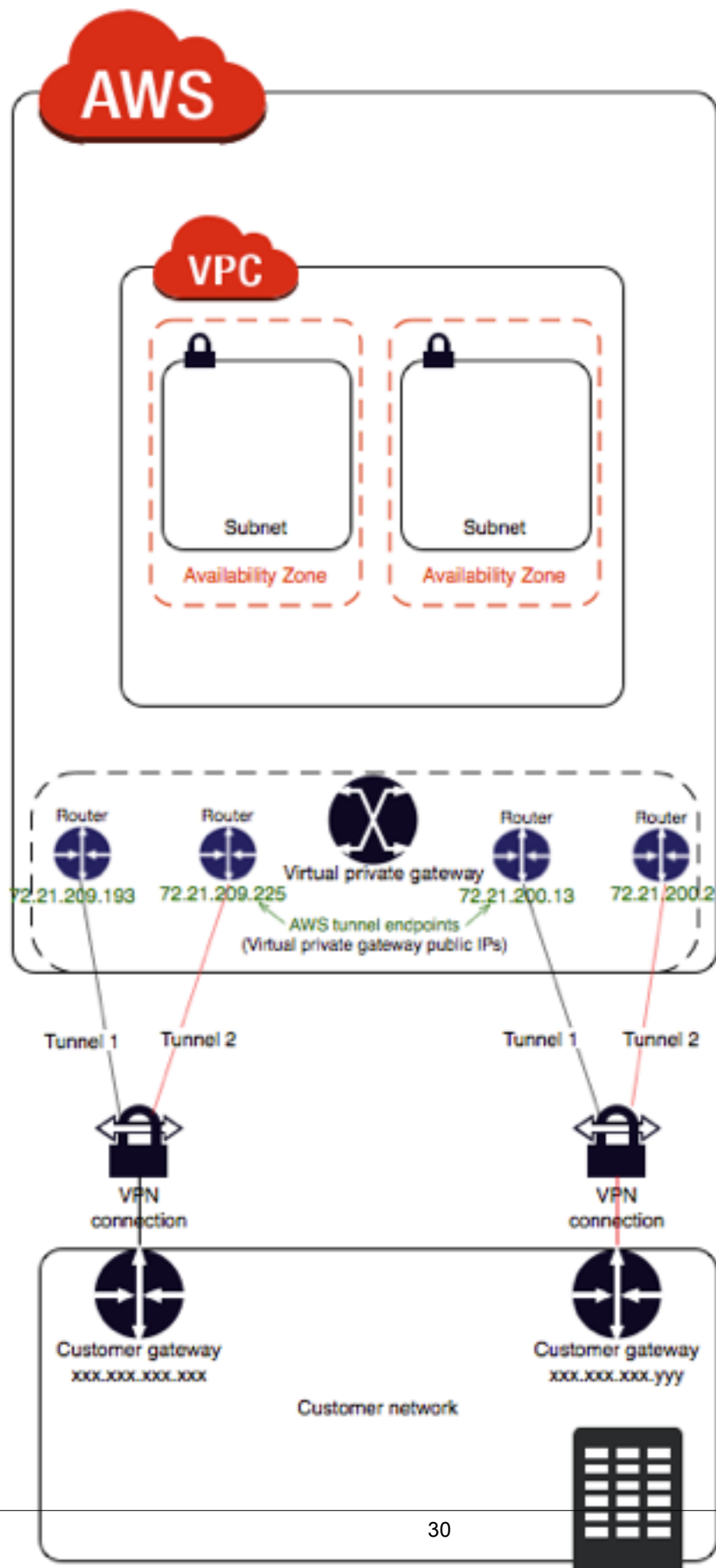
たとえば、ロサンゼルスとニューヨークのそれぞれにサイトがあり、両方のサイトに、仮想プライベートゲートウェイへの Site-to-Site VPN 接続が存在する場合は、Site-to-Site VPN 接続ごとに支払いが発生します (0.05 USD/時間の場合、合計 0.10 USD/時間)。各 Site-to-Site VPN 接続を通過するロサンゼルスからニューヨークへ (またはその逆に) 送信するすべてのデータについて、標準の AWS データ転送料金の支払いが発生します。仮想プライベートゲートウェイに Site-to-Site VPN 接続経由で送信されるネットワークトラフィックは無料ですが、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使用して、VPC および仮想プライベートゲートウェイへの 2 番目の Site-to-Site VPN 接続を設定できます。冗長な Site-to-Site VPN 接続とカスタマーゲートウェイ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 番目のカスタマーゲートウェイの Site-to-Site VPN 接続を通してトラフィックの送信を継続することができます。

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



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。

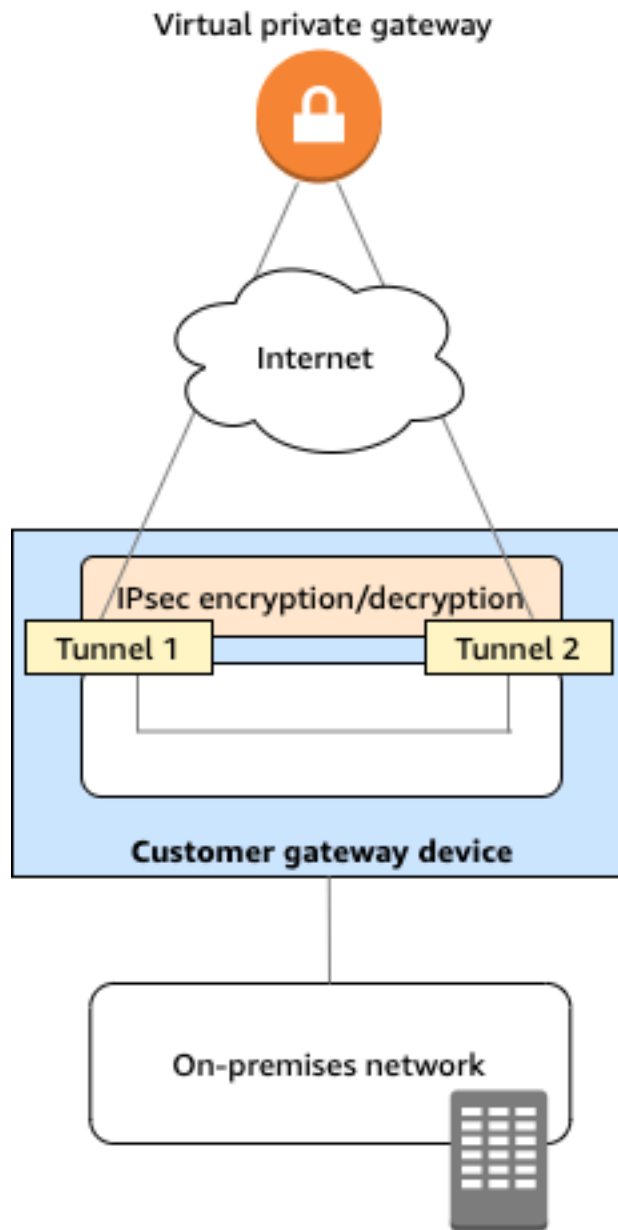
動的にルーティングされる Site-to-Site VPN 接続では、ボーダーゲートウェイプロトコル (BGP) を使用して、カスタマーゲートウェイと仮想プライベートゲートウェイ間で情報をルーティングします。静的にルーティングされる Site-to-Site VPN 接続では、カスタマーゲートウェイのユーザー側でリモートネットワークの静的ルートを入力する必要があります。BGP でアドバタイズされ、静的に入力されたルート情報によって、双方のゲートウェイで使用可能なトンネルが判別され、障害発生時にトラフィックが再ルーティングされます。BGP (使用可能な場合) で提供されるルーティング情報を使用し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、「[開始方法 \(p. 18\)](#)」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 VPN 接続 (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接続) を示しています。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の間の 2 つの線は、VPN 接続のトンネルを表しています。AWS でデバイス障害が発生した場合、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て、アクセスが中断されないようにします。ときどき、AWS は、VPN 接続の定期メンテナンスも実行します。これにより、VPN 接続の 2 つのトンネルの 1 つが短時間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 \(p. 11\)](#)」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、「[開始方法 \(p. 18\)](#)」を参照してください。このプロセス中に、AWS 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、デバイスのパブリック IP アドレスなど、デバイスに関する情報を AWS 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 \(p. 12\)](#)」を参照してください。AWS のカスタマーゲートウェイリソースは、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。

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、「[設定ファイルを](#)

[ダウンロードする \(p. 24\)](#)」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” \(p. 40\)](#)
- 動的設定: [the section called “設定ファイルの例” \(p. 52\)](#)

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。

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。

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。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 Site-to-Site 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。

Note





これらのデバイス固有の設定ファイルは AWS によって、ベストエフォートベースで提供されています。AWS によってテストされていますが、このテストは限られています。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、追加のサポートを依頼する必要があります。

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
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。

	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 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。
	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。
	(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。VPN 接続を設定して、代わりに接続の AWS 側から IKE ネゴシエーション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 \(p. 10\)](#)」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るとフェーズ 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 	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コードとして AWS Certificate Manager Private Certificate Authority 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の間に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。 AWS で VPN 接続を作成するとき、各トンネルのための独自の事前共有キーを指定するか、または AWS で新しい

要件	RFC	コメント
		<p>事前共有キーを生成できます。または、AWS Certificate Manager Private Certificate Authority を使用して、カスタマーゲートウェイデバイスで使用するよう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 (p. 5)」を参照してください。</p> <p>IKEv1 および IKEv2 バージョンがサポートされています。</p> <p>メインモードは IKEv1 でのみサポートされています。</p> <p>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。</p>
<p>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</p> 	RFC 4301	<p>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。</p>
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	<p>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。</p> <p>以下のグループがサポートされます。</p> <ul style="list-style-type: none"> 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
暗号化前に IP パケットをフラグメント化する	RFC 4459	パケットが送信するには大きすぎる場合は、フラグメント化する必要があります。フラグメント化されて暗号化されたパケットは、再アセンブルされません。したがって、VPN デバイスは、VPN ヘッダーでカプセル化する前にパケットをフラグメント化する必要があります。フラグメントはリモートホストに個別に送信され、そこで再アセンブルされます。
(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、代替の IPsec トンネルが使用されます。

要件	RFC	コメント
(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) 	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 	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。

接続はパケットを追加のネットワークヘッダー (IPsec を含む) でカプセル化するため、1 つのパケットで送信できるデータの量は減少します。IPsec トンネルを介して送信できるデータ量に関連する問題を最小限にするために、次の表で挙げられている手法を使用することをお勧めします。

手法	RFC	コメント
VPN トンネルに入る TCP パケットの最大セグメントサイズ (MSS) を調整する	RFC 4459	<p>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。一部のゲートウェイでは、TCP パケットの最大セグメントサイズ (MSS) のパラメータを変更できます。これにより、TCP エンドポイント (クライアント、サーバー) は、各パケットで送信されるデータの量を減らします。VPN デバイスに届くパケットが小さくなってカプセル化および送信が可能になるため、これは最適な方法です。</p> <p>SHA2-384 または SHA2-512 ハッシュアルゴリズムを使用する場合は、カスタマーゲートウェイデバイスの MSS を 1359 に設定することをお勧めします。この設定は、より大きいヘッダーに対応するために必要です。</p>
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	RFC 791	<p>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。</p>

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 \(p. 38\)](#)」を参照してください。

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仮想プライベートゲートウェイに接続する IPsec トンネルのエンドポイントとして使用するには、インターネットでルーティングが可能な IP アドレスが必要です。ファイアウォールがインターネットとゲートウェイ間にある場合、IPsec トンネルを確立するには、以下の表のルールに従う必要があります。仮想プライベートゲートウェイ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)

入カルール I1	
送信元 IP	仮想プライベートゲートウェイ 1
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
入カルール I2	
送信元 IP	仮想プライベートゲートウェイ 2
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
送信先ポート	500
入カルール I3	
送信元 IP	仮想プライベートゲートウェイ 1
送信先 IP	カスタマーゲートウェイ
プロトコル	IP 50 (ESP)
入カルール I4	
送信元 IP	仮想プライベートゲートウェイ 2
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)

出カルール O1	
送信元 IP	カスタマーゲートウェイ

送信先 IP	仮想プライベートゲートウェイ 1
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	
送信元 IP	カスタマーゲートウェイ
送信先 IP	仮想プライベートゲートウェイ 2
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	
送信元 IP	カスタマーゲートウェイ
送信先 IP	仮想プライベートゲートウェイ 1
プロトコル	IP 50 (ESP)
出カルール O4	
送信元 IP	カスタマーゲートウェイ
送信先 IP	仮想プライベートゲートウェイ 2
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。

デバイスで NAT トラバーサル (NAT-T) を使用している場合、ポート 4500 経由で UDP アクセスを許可するルールを含める必要があります。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 \(p. 29\)](#)」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 (AWS VPN CloudHub) への複数のカスタマーゲートウェイデバイス

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、複数のロケーションを AWS VPN CloudHub に接続できます。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 \(p. 27\)](#)」を参照してください。複数の地理的ロケーションにカスタマーゲートウェイデバイスがある場合、各デバイスは、ロ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 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、BGP ルートをより具体的にアドバタイズすることをお勧めしています。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 \(p. 15\)](#)」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

- [設定ファイルの例 \(p. 40\)](#)
- [静的ルーティングのユーザーインターフェイス手順 \(p. 42\)](#)
- [Cisco デバイスの追加情報 \(p. 51\)](#)
- [Testing \(p. 52\)](#)

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、「[設定ファイルをダウンロードする \(p. 24\)](#)」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](#)

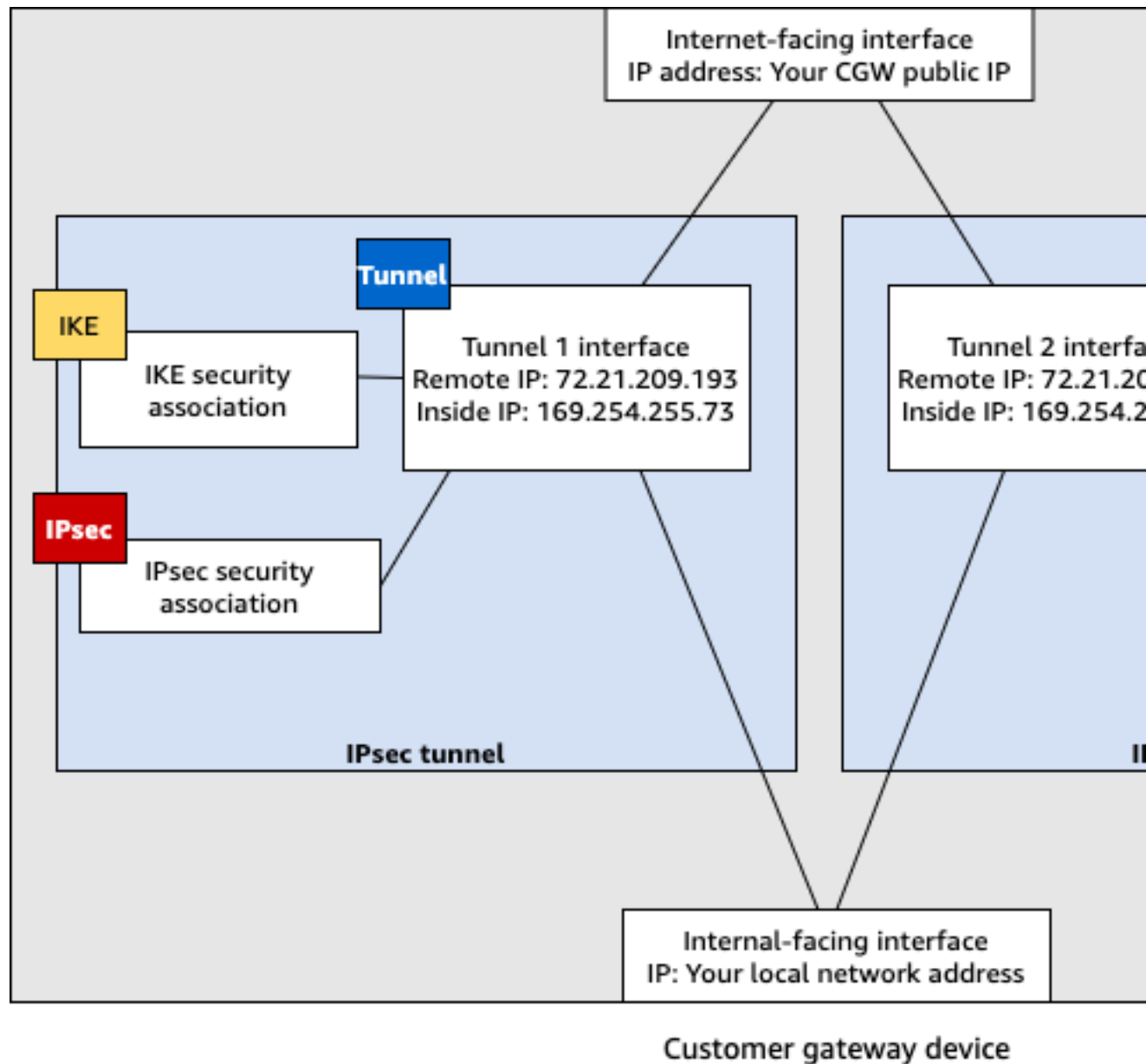
これらのファイルは、一部のコンポーネントにプレースホルダー値を使用します。たとえば、以下を使用します。

- 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。

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 \(p. 10\)](#)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。



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。

The screenshot shows the 'Add VPN Tunnel' dialog box. The 'Type' is 'VPN-Tunnel'. The 'Enable' checkbox is checked. The 'Comment' field is empty. The 'VPN Tunnel' tab is selected. The 'VPN Tunnel ID' is 1. The 'Peer' is 'AWS_VPC_Tunnel_1'. The 'VPN Tunnel Type' is 'Numbered'. The 'Local Address' is '169.254.44.234' and the 'Remote Address' is '169.254.44.233'. The 'Physical device' is set to 'Select...'. The 'OK' and 'Cancel' buttons are at the bottom right.

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。

Edit Destination Route: 10.28.13.0/24

Destination: 10.28.13.0/24

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send *unreachable* messages.
Black Hole: Drop packets, but don't send *unreachable* messages.

Rank: Default: 60

Local Scope: ☐

Comment:

Add Gateway

Ping: ☐

Add Gateway Edit Delete

Gateway	Priority
169.254.44.233	1
169.254.44.5	2

Save Cancel

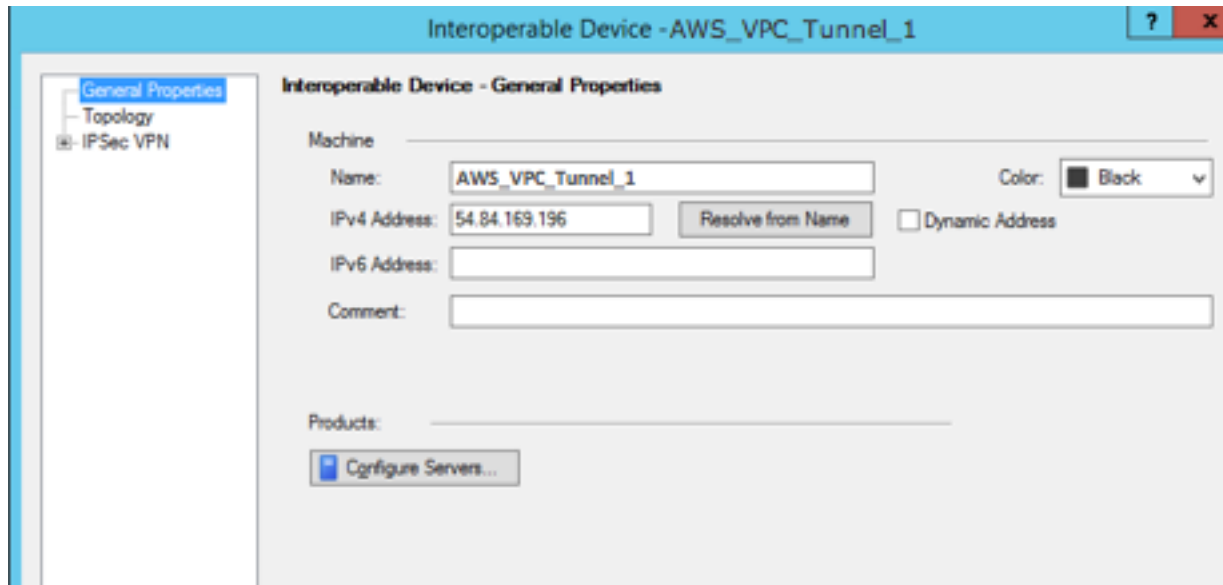
7. [Save] を選択します。

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] を選択します。

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。

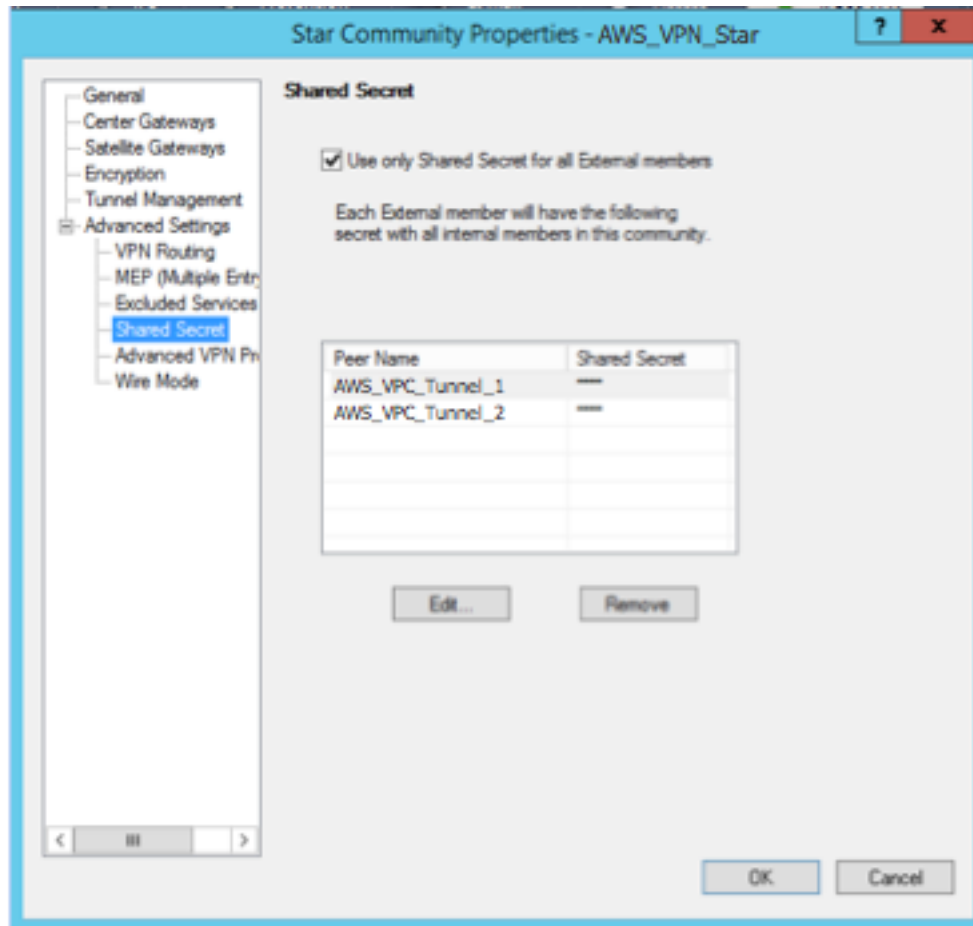
Note

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. GuiDBedit 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。

Log Info		Rule	
Product	 Security Gateway/Management	Action	 Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	 Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-4650-3989E658CF04}
Source	 Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	 10.28.13.28	Encryption Scheme	 IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 (group 2)
Protocol	 icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	 eth0	Subproduct	 VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	 Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

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] を選択します。[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。

Testing

Site-to-Site VPN 接続のテストの詳細については、「[Site-to-Site VPN 接続のテスト \(p. 106\)](#)」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

- [設定ファイルの例 \(p. 52\)](#)
- [動的ルーティングのユーザーインターフェイス手順 \(p. 54\)](#)
- [Cisco デバイスの追加情報 \(p. 60\)](#)
- [Juniper デバイスの追加情報 \(p. 61\)](#)
- [Testing \(p. 61\)](#)

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、「[設定ファイルをダウンロードする \(p. 24\)](#)」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](#)

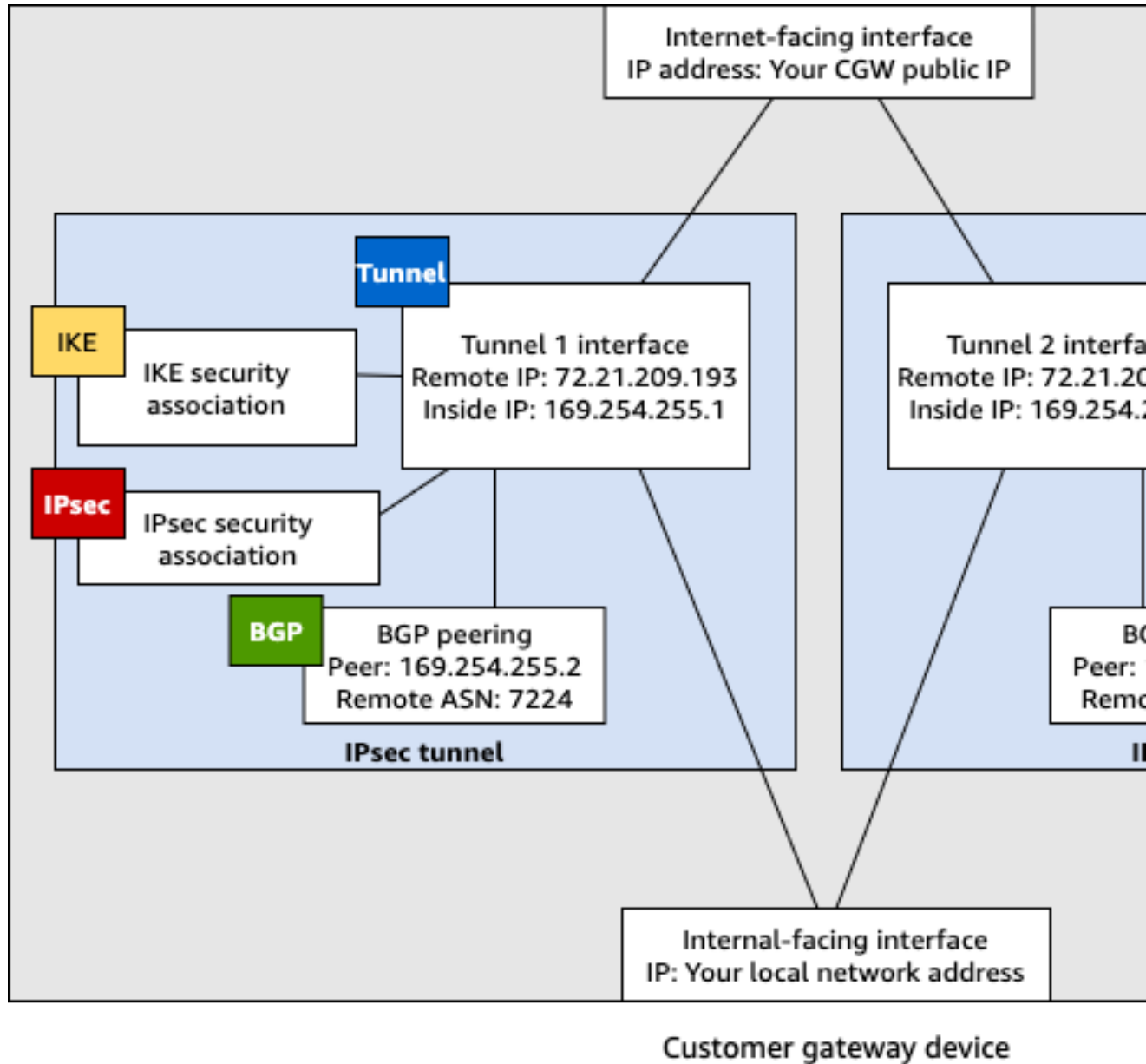
これらのファイルは、一部のコンポーネントにプレースホルダー値を使用します。たとえば、以下を使用します。

- VPN 接続 ID、カスタマーゲートウェイ仮想プライベートゲートウェイ 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](#) and [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。

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 \(p. 10\)](#)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

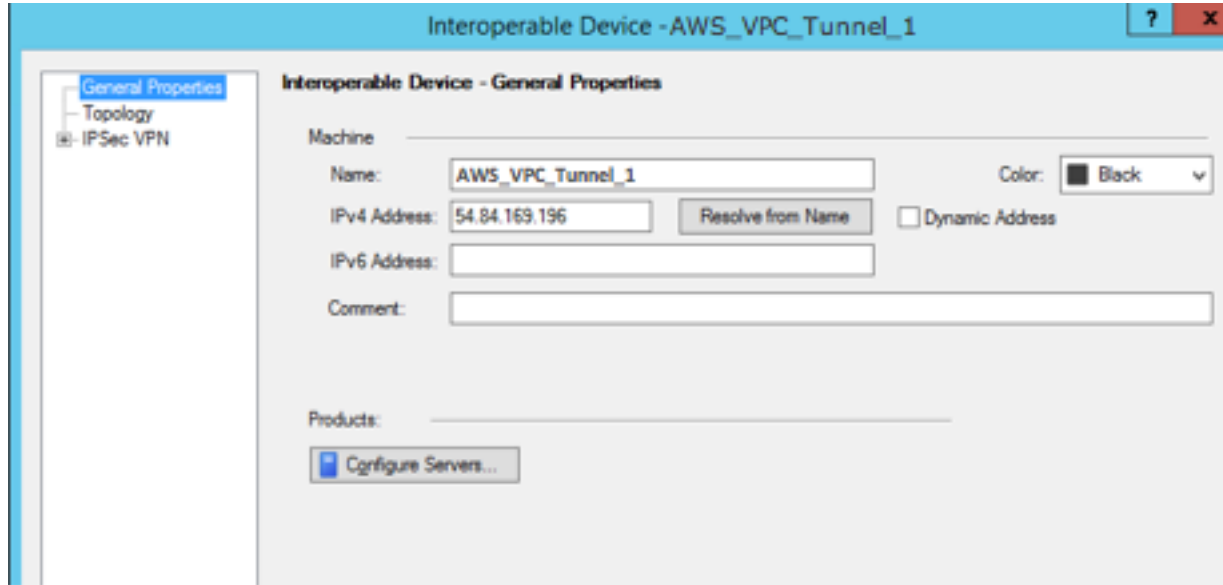
次のステップは、ローカルインターフェイスルートを分散するためのものです。また、静的ルーティングや、動的ルーティングプロトコルによって得られたルーティングなど、さまざまなソースからのルートを再分散できます。詳細については、「[Gaia Advanced Routing R77 Versions Administration Guide](#)」を参照してください。

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] を選択します。
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] を選択します。

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。

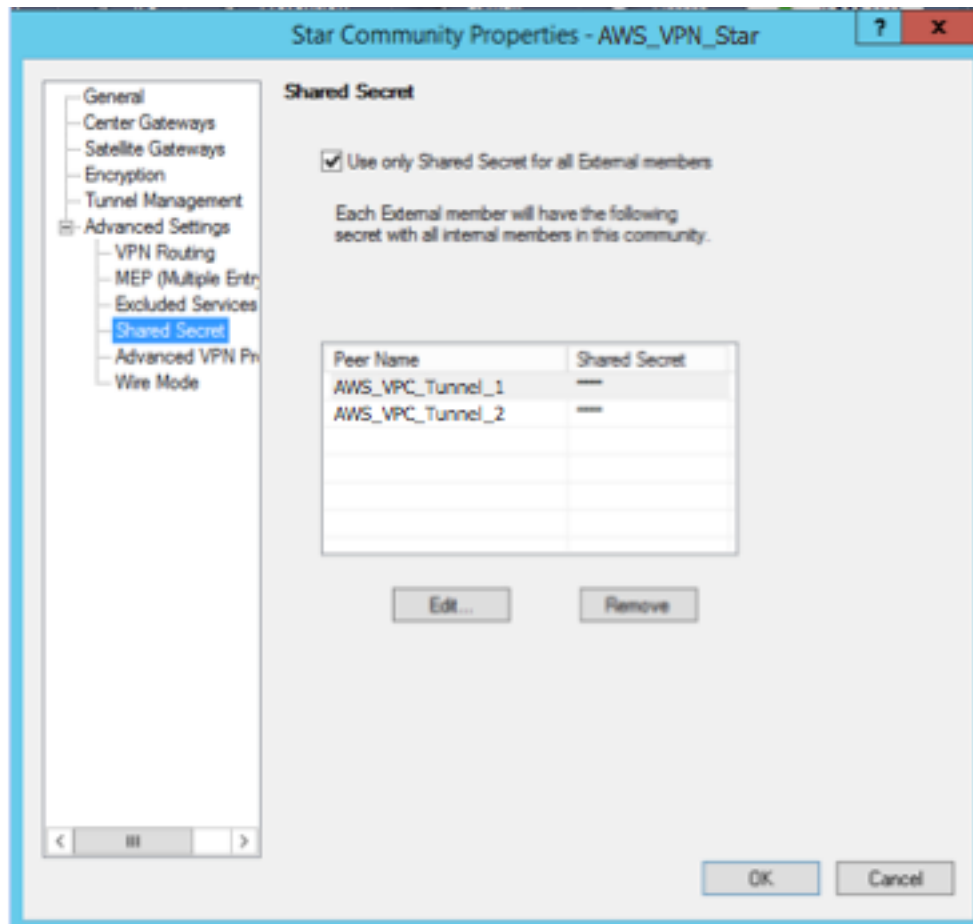
1. ゲートウェイのプロパティから、カテゴリペインの [IPsec VPN] を選択します。
2. [Communities]、[New]、[Star Community] の順に選択します。
3. コミュニティの名前 (例: AWS_VPN_Star) を指定し、カテゴリペインの [Center Gateways] を選択します。
4. [Add] を選択して、ゲートウェイまたはクラスターを参加ゲートウェイのリストに追加します。
5. カテゴリペインで、[Satellite Gateways]、[Add (追加)] の順に選択し、先に作成した相互運用デバイス (AWS_VPC_Tunnel_1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



- 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。

- 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。
- [Enable VPN Directional Match in VPN Column] を選択し、[OK] を選択します。
- 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。
- 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。
- [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`
- SmartDashboard で、[Policy]、[Install] の順に選択します。
- 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。

- 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. GuiDBedit 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。

Log Info		Rule	
Product	 Security Gateway/Management	Action	 Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	 Log	User	---
Origin	cpgw-997695	More	
Traffic		Rule UID	{0AA18015-FF7B-46503989E658CF04}
Source	 Management_PC (192.168.1.116)	Community	AWS_VPN_Star
Destination	 10.28.13.28	Encryption Scheme	 IKE
Service	---	Data Encryption Methods	ESP: AES-128 + SHA1 (group 2)
Protocol	 icmp	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Interface	 eth0	Subproduct	 VPN
Source Port	---	VPN Feature	VPN
Policy		Product Family	 Network
Policy Name	Standard	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

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 \(p. 42\)](#)」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)。

Testing

Site-to-Site VPN 接続のテストの詳細については、「[Site-to-Site VPN 接続のテスト \(p. 106\)](#)」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 \(p. 62\)](#)
- [ステップ 1: VPN 接続を作成し、VPC を設定する \(p. 62\)](#)
- [ステップ 2: VPN 接続の設定ファイルをダウンロードする \(p. 63\)](#)
- [ステップ 3: Windows Server を設定する \(p. 64\)](#)
- [ステップ 4: VPN トンネルを設定する \(p. 65\)](#)
- [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 \(p. 71\)](#)
- [ステップ 6: VPN 接続をテストする \(p. 71\)](#)

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 \(p. 20\)](#)」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、「[サイト間 VPN 接続の作成 \(p. 22\)](#)」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 \(p. 21\)](#)」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:              xCjNLsLoCmKsawcdR9yX6GsEXAMPLE
```

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 \(p. 66\)](#)
- [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 \(p. 66\)](#)

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 \(p. 70\)](#)」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 \(p. 69\)](#)」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 \(p. 67\)](#)
- [トンネルの設定を確認する \(p. 69\)](#)
- [マスターキー PFS \(Perfect Forward Secrecy\) を有効にする \(p. 69\)](#)
- [Windows ファイアウォールを設定する \(p. 70\)](#)

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。

New Connection Security Rule Wizard

Tunnel Endpoints
Specify the endpoints for the IPsec tunnel defined by this rule.

Steps:

- Rule Type
- Tunnel Type
- Requirements
- Tunnel Endpoints**
- Authentication Method
- Profile
- Name

Which computers are in Endpoint 1?

172.31.0.0/16 [Add... Edit... Remove]

What is the local tunnel endpoint (closest to computers in Endpoint 1)?

IPv4 address: 172.31.13.36 [Edit...]
IPv6 address: []

☐ Apply IPsec tunnel authorization as specified on the IPsec Settings tab of Windows Firewall with Advanced Security Properties.

What is the remote tunnel endpoint (closest to computers in Endpoint 2)?

IPv4 address: 54.240.204.89 [Edit...]
IPv6 address: []

Which computers are in Endpoint 2?

10.0.0.0/16 [Add...]

[< Back] [Next >]

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 接続のテスト \(p. 106\)](#)」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 \(p. 62\)](#)」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 \(p. 62\)](#)」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 \(p. 62\)](#)」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

次のステップは、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 接続のテスト \(p. 106\)](#)」を参照してください。

トピック

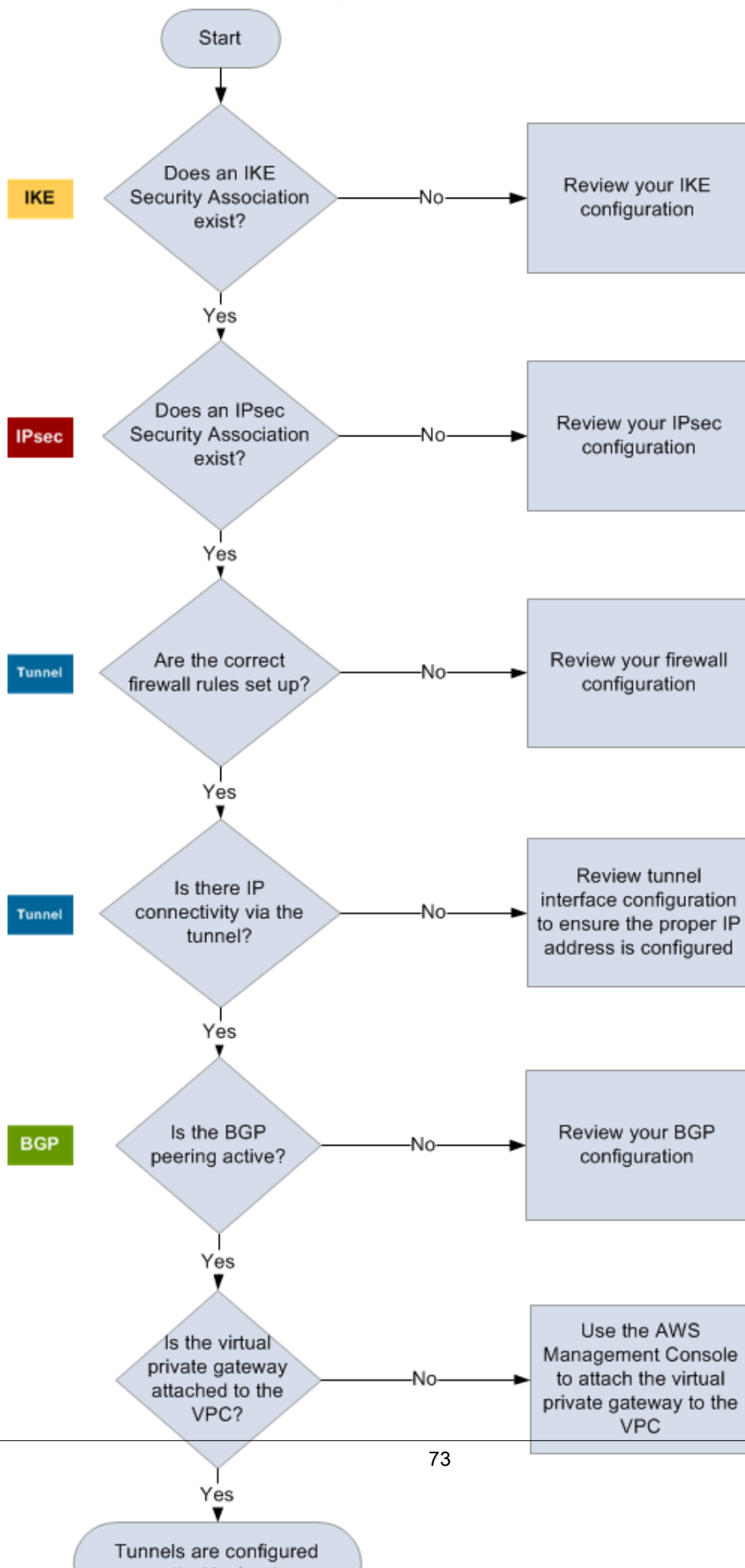
- [ボーダーゲートウェイプロトコルを使用する場合の接続のトラブルシューティング \(p. 72\)](#)
- [ボーダーゲートウェイプロトコルを使用しない接続のトラブルシューティング \(p. 75\)](#)
- [Cisco ASA カスタマーゲートウェイデバイスの接続のトラブルシューティング \(p. 78\)](#)
- [Cisco IOS カスタマーゲートウェイデバイスの接続のトラブルシューティング \(p. 81\)](#)
- [ボーダーゲートウェイプロトコル接続を使用しない Cisco IOS カスタマーゲートウェイデバイスのトラブルシューティング \(p. 85\)](#)
- [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 \(p. 89\)](#)
- [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 \(p. 92\)](#)
- [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 \(p. 95\)](#)

その他のリソース

- [アマゾン 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

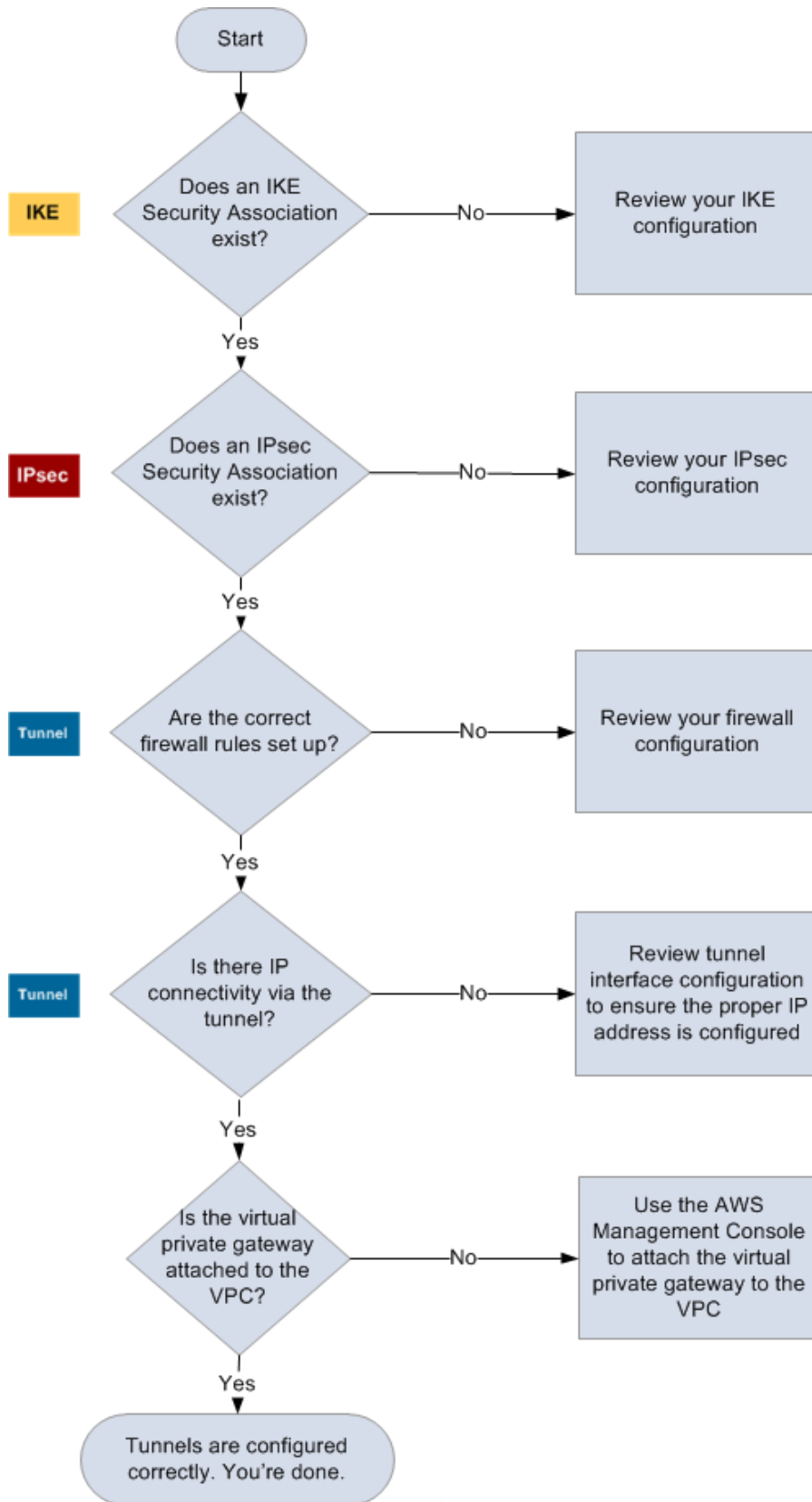
次の図と表は、ボーダーゲートウェイプロトコル (BGP) を使用するカスタマーゲートウェイデバイスをトラブルシューティングする、一般的な手順を示しています。また、デバイスのデバッグ機能を有効にすることをお勧めします。詳細については、ゲートウェイデバイスのベンダーにお問い合わせください。



IKE	<p>IKE Security Association が存在するかどうかを確認します。</p> <p>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。</p> <p>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。</p> <p>IKE Security Association が存在する場合は、「IPsec」に進みます。</p>
IPsec	<p>IPsec Security Association (SA) が存在するかどうかを確認します。</p> <p>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。</p> <p>IPsec SA が存在しない場合は、IPsec 設定を確認します。</p> <p>IPsec SA が存在する場合は、「トンネル」に進みます。</p>
トンネル	<p>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 (p. 38)」を参照)。セットアップされている場合は、次に進みます。</p> <p>トンネル経由の IP 接続があるかどうかを確認します。</p> <p>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。</p> <p>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。</p> <p>ping が成功した場合は、「BGP」に進みます。</p>
BGP	<p>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。</p> <p>各トンネルについて、以下を実行します。</p> <ul style="list-style-type: none">• 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。 <p>トンネルがこの状態にない場合は、BGP 設定を確認します。</p> <p>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。</p>

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お問い合わせください。



IKE	<p>IKE Security Association が存在するかどうかを確認します。</p> <p>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。</p> <p>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。</p> <p>IKE Security Association が存在する場合は、「IPsec」に進みます。</p>
IPsec	<p>IPsec Security Association (SA) が存在するかどうかを確認します。</p> <p>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。</p> <p>IPsec SA が存在しない場合は、IPsec 設定を確認します。</p> <p>IPsec SA が存在する場合は、「トンネル」に進みます。</p>
トンネル	<p>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 (p. 38)」を参照)。セットアップされている場合は、次に進みます。</p> <p>トンネル経由の IP 接続があるかどうかを確認します。</p> <p>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。</p> <p>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。</p> <p>ping が成功した場合は、「静的ルート」に進みます。</p>
静的ルート	<p>各トンネルについて、以下を実行します。</p> <ul style="list-style-type: none">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。 <p>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。</p> <p>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。</p>

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

次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り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

次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

次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

次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 pcsp 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 pcsp 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 pcsp 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 pcg 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 \(p. 38\)](#)」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続けます。

```
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

次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

次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

次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 pcsp 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 pcsp 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 pcsp 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 pcsp 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 \(p. 38\)](#)」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続けます。

```
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

次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

次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 \(p. 38\)](#)」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続けます。

```
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

次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
```

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
```

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

次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 \(p. 38\)](#)」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続けます。

```
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

次のコマンドを実行します。

```
s5g5-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。

```
s5g5-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。

IKE

次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

次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 \(p. 38\)](#)」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続けます。

```
# 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

次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 の使用

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。

目次

- [Site-to-Site VPN 接続の識別 \(p. 99\)](#)
- [AWS Classic VPN から AWS VPN への移行 \(p. 100\)](#)
- [トランジットゲートウェイ VPN アタッチメントの作成 \(p. 105\)](#)
- [Site-to-Site VPN 接続のテスト \(p. 106\)](#)
- [Site-to-Site VPN 接続の削除 \(p. 107\)](#)
- [Site-to-Site VPN 接続のターゲットゲートウェイの変更 \(p. 109\)](#)
- [Site-to-Site VPN 接続オプションの変更 \(p. 112\)](#)
- [Site-to-Site VPN トンネルオプションの変更 \(p. 112\)](#)
- [Site-to-Site VPN 接続の静的ルートの編集 \(p. 113\)](#)
- [Site-to-Site VPN 接続のカスタマーゲートウェイの変更 \(p. 114\)](#)
- [漏洩した認証情報の置き換え \(p. 114\)](#)
- [Site-to-Site VPN トンネルエンドポイント証明書の更新 \(p. 115\)](#)

Site-to-Site VPN 接続の識別

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

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

1. 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. Site-to-Site VPN 接続を選択し、詳細ペインの [カテゴリ] の値を確認します。VPN の値が、AWS VPN 接続を指しています。VPN-Classic の値が、AWS Classic VPN 接続を指しています。

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

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

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

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

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

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

または、以下のコマンドの 1 つを使用します。

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

AWS Classic VPN から AWS VPN への移行

既存の Site-to-Site VPN 接続が AWS Classic VPN 接続であれば、AWS VPN 接続に移行することができます。新しい仮想プライベートゲートウェイに直接移行することも (オプション 1)、またはトランジットゲートウェイを使用して移行することもできます (オプション 2)。オプション 1 の手順では、古い仮想プライベートゲートウェイを VPC からデタッチすると、Site-to-Site VPN 接続が一時的に中断されます。オプション 2 の手順では、Site-to-Site VPN 接続は中断されませんが、[トランジットゲートウェイの追加コスト](#)が発生します。

AWS Classic VPN 接続を AWS Direct Connect 接続のバックアップとして使用する場合、Site-to-Site VPN 接続を削除して再作成できます (オプション 3)。オプション 3 の手順では、AWS Direct Connect プライベート仮想インターフェイスのダウンタイムは発生しません。

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

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

トピック

- [オプション 1: 新しい仮想プライベートゲートウェイに直接移行する \(p. 100\)](#)
- [オプション 2: トランジットゲートウェイを使用して移行する \(p. 102\)](#)
- [オプション 3: \(AWS Direct Connect の VPN 接続のバックアップ\) VPN 接続を削除して再作成する \(p. 104\)](#)

オプション 1: 新しい仮想プライベートゲートウェイに直接移行する

このオプションでは、新しい仮想プライベートゲートウェイと Site-to-Site VPN 接続を作成し、古い仮想プライベートゲートウェイを VPC からデタッチし、新しい仮想プライベートゲートウェイを VPC にアタッチします。

Note

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

AWS VPN 接続へ移行するには

1. 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 [Virtual Private Gateways]、[Create Virtual Private Gateway] を選択して、仮想プライベートゲートウェイを作成します。
3. ナビゲーションペインで、[Site-to-Site VPN Connections (Site-to-Site VPN 接続)]、[Create VPN Connection (VPN 接続の作成)] の順に選択します。以下の情報を指定し、[Yes, Create] を選択します。
 - [Virtual Private Gateway]: 前のステップで作成した仮想プライベートゲートウェイを選択します。
 - [カスタマーゲートウェイ]: [既存] を選択し、現在の AWS Classic VPN 接続の既存のカスタマーゲートウェイを選択します。
 - 必要に応じてルーティングオプションを指定します。
4. 新しい Site-to-Site VPN 接続を選択し、[Download Configuration] を選択します。カスタマーゲートウェイデバイスに適した設定ファイルをダウンロードします。
5. 設定ファイルを使用して、カスタマーゲートウェイデバイスの VPN トンネルを設定します。詳細については、「」を参照してください。[カスタマーゲートウェイデバイス \(p. 32\)](#) トンネルはまだ有効にしないでください。新しく設定したトンネルを無効にしておくためのガイダンスが必要な場合は、ベンダーにお問い合わせください。
6. (オプション) テスト VPC を作成し、仮想プライベートゲートウェイをテスト VPC にアタッチします。必要に応じて、暗号化ドメイン/ソース送信先アドレスを変更して、ローカルネットワークのホストからテスト VPC 内のテストインスタンスへの接続をテストします。
7. ルートテーブルでルート伝達を使用している場合は、ナビゲーションペインで、[Route Tables] を選択します。VPC のルートテーブルを選択し、[ルート伝播]、[Edit route propagation (ルート伝播の編集)] の順に選択します。古い仮想プライベートゲートウェイのチェックボックスをオフにし、[Save] を選択します。

Note

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

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

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

Note

以前の設定に戻す必要がある場合は、新しい仮想プライベートゲートウェイをデタッチし、ステップ 8 と 9 に従って古い仮想プライベートゲートウェイに再度アタッチしてルートを更新します。

11. AWS Classic VPN 接続を今後必要とせず、その料金が引き続き発生するのを避けるには、カスタマーゲートウェイデバイスから以前のトンネル設定を取り除き、Site-to-Site VPN 接続を削除します。これを行うには、[Site-to-Site VPN 接続] に移動し、[Site-to-Site VPN 接続] を選択して、[削除] を選択します。

Important

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

オプション 2: トランジットゲートウェイを使用して移行する

このオプションでは、トランジットゲートウェイを作成し、Site-to-Site VPN 接続が存在する VPC にアタッチし、既存のカスタマーゲートウェイを使用して、トランジットゲートウェイで一時的な Site-to-Site VPN 接続を作成します。次に、新しい仮想プライベートゲートウェイで新しい Site-to-Site VPN 接続を構成しながら、トランジットゲートウェイ VPN 接続を介してトラフィックをルーティングします。

または、このオプションを使用して、Site-to-Site VPN 接続を直接トランジットゲートウェイに移行することもできます。この場合には、新しい VPN 接続を新しい仮想プライベートゲートウェイではなく、トランジットゲートウェイに作成します。

ステップ 1: トランジットゲートウェイと VPN 接続を作成する

トランジットゲートウェイと 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、[Transit Gateways (トランジットゲートウェイ)]、[Create Transit Gateway (トランジットゲートウェイの作成)] の順に選択し、デフォルトのオプションを使用してトランジットゲートウェイを作成します。
3. ナビゲーションペインで、[Transit Gateway Attachments (トランジットゲートウェイのアタッチメント)]、[Create Transit Gateway Attachment (トランジットゲートウェイのアタッチメントの作成)] の順に選択します。以下の情報を指定し、[Create attachment (アタッチメントの作成)] を選択します。
 - [トランジットゲートウェイ ID (Transit Gateway ID)] で、作成したトランジットゲートウェイを選択します。
 - [VPC ID] で、トランジットゲートウェイにアタッチする VPC を選択します。
4. [Create Transit Gateway Attachment (トランジットゲートウェイのアタッチメントの作成)] を再度選択し、次の情報を指定して、[Create attachment (アタッチメントの作成)] を選択します。
 - [トランジットゲートウェイ ID (Transit Gateway ID)] で、作成したトランジットゲートウェイを選択します。
 - [アタッチメントタイプ] で、[VPN] を選択します。
 - [Customer Gateway ID (カスタマーゲートウェイ ID)] で、既存の Site-to-Site VPN 接続のカスタマーゲートウェイを選択し、必要なルーティングオプションを選択します。

ステップ 2: 新しい仮想プライベートゲートウェイを作成する

新しい仮想プライベートゲートウェイと新しい Site-to-Site VPN 接続を作成します。このステップは、新しい仮想プライベートゲートウェイに移行する場合にのみ必要です。VPN 接続をトランジットゲートウェイに移行する場合は、これらのステップを省略して[ステップ 3 \(p. 103\)](#) に直接進んでください。

新しい Site-to-Site VPN 接続を作成するには

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]、[仮想プライベートゲートウェイの作成] の順に選択して、新しい仮想プライベートゲートウェイを作成します。
2. ナビゲーションペインで、[Site-to-Site VPN Connections (Site-to-Site VPN 接続)]、[Create VPN Connection (VPN 接続の作成)] の順に選択します。
3. [仮想プライベートゲートウェイ] で、作成した仮想プライベートゲートウェイを選択します。
4. [カスタマーゲートウェイ ID] で、既存の Site-to-Site VPN 接続用の既存のカスタマーゲートウェイを選択し、ルーティングのタイプを指定します。[Create VPN Connection (VPN 接続の作成)] を選択します。
5. 新しい Site-to-Site VPN 接続を選択し、[Download Configuration (設定のダウンロード)] を選択して、サンプル設定ファイルをダウンロードします。カスタマーゲートウェイデバイスで VPN 接続を設定しますが、トラフィックをまだルーティングしないでください (静的ルートを作成したり BGP アナウンスを除外したりしないでください)。

ステップ 3: 新しい VPN 接続に切り替える

この手順では、トラフィックをトランジットゲートウェイに切り替えてから、新しい Site-to-Site VPN 接続に切り替えるときに、VPN トラフィックの非対称ルーティングを一時的に有効にします。

新しい Site-to-Site VPN 接続に切り替えるには

1. トランジットゲートウェイで 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ます (必要に応じて、静的ルートを指定するか BGP アナウンスを許可します)。これにより、非対称トラフィックルーティングが開始されます。
2. ナビゲーションペインで [ルートテーブル] を選択し、VPC のルートテーブルを選択して、[アクション]、[Edit routes (ルートの編集)] の順に選択します。
3. オンプレミスネットワークを指すルートを追加し、ターゲットとしてトランジットゲートウェイを選択します。宛先ルートには、より具体的なルートを入力します。たとえば、オンプレミスネットワークが 10.0.0.0/16 であるなら、10.0.0.0/17 を指すルートと 10.0.128.0/17 を指す別のルートを作成します。非対称トラフィックルーティングが停止し、すべてのトラフィックがトランジットゲートウェイを介してルーティングされます。

Note

VPN 接続を新しい仮想プライベートゲートウェイの代わりにトランジットゲートウェイに移行する場合は、ここで終了です。

4. ナビゲーションペインで [Virtual Private Gateways] を選択します。
5. VPC にアタッチされている古い仮想プライベートゲートウェイを選択し、[アクション]、[VPC からデタッチ] の順に選択します。[Yes, Detach] を選択します。
6. 以前に作成した新しい仮想プライベートゲートウェイを選択し、[アクション]、[VPC にアタッチする] の順に選択します。VPC を選択し、[はい、アタッチする] を選択します。
7. ナビゲーションペインで、[Route Tables] を選択します。VPC のルートテーブルを選択し、[ルート伝播]、[Edit route propagation (ルート伝播の編集)] の順に選択します。新しい仮想プライベートゲートウェイのチェックボックスを選択し、[Save (保存)] を選択します。ルートが VPC ルートテーブルに伝播されていることを確認します。

8. 新しい仮想プライベートゲートウェイ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、静的ルートまたは BGP を使用して、オンプレミスネットワークから VPC にトラフィックをルーティングします。これにより、非対称ルーティングが開始されます。
9. ナビゲーションペインで、[Route Tables] を選択します。VPC のルートテーブルを選択し、[アクション]、[Edit route (ルートの編集)] の順に選択します。トランジットゲートウェイへのより具体的なルートを削除します。これにより、非対称トラフィックフローが停止し、すべてのトラフィックが新しい Site-to-Site VPN 接続を介してルーティングされます。

ステップ 4: クリーンアップする

AWS Classic VPN 接続が不要になった場合は、削除できます。新しい仮想プライベートゲートウェイに移行した場合は、移行用に作成したトランジットゲートウェイ VPN 接続とトランジットゲートウェイを削除することもできます。

リソースをクリーンアップするには

1. カスタマーゲートウェイデバイスで、トランジットゲートウェイでの一時的な VPN 接続の設定と、古い VPN 接続の設定を削除します。
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、古い Site-to-Site VPN 接続を選択して、[操作]、[削除] の順に選択します。
3. 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、古い仮想プライベートゲートウェイを選択して、[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。VPN 接続をトランジットゲートウェイに移行した場合は、ここで停止できます。
4. 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、トランジットゲートウェイ VPN 接続を選択します。[Actions] で、[Delete] を選択します。
5. ナビゲーションペインで、[Transit Gateway Attachments (トランジットゲートウェイのアタッチメント)] を選択し、VPC アタッチメントを選択します。[Actions] で、[Delete] を選択します。
6. ナビゲーションペインで、[Transit Gateways (トランジットゲートウェイ)] を選択し、トランジットゲートウェイを選択します。[Actions] で、[Delete] を選択します。

オプション 3: (AWS Direct Connect の VPN 接続のバックアップ) VPN 接続を削除して再作成する

このオプションは、同じ仮想プライベートゲートウェイ上に AWS Direct Connect 接続と AWS Classic VPN 接続があり、VPN 接続を AWS Direct Connect 接続のバックアップとして使用する場合に使用します。このオプションでは、仮想プライベートゲートウェイ上の既存の AWS Classic VPN 接続を削除します。AWS Classic VPN 接続が `deleted` 状態になったとき、同じ仮想プライベートゲートウェイ上に新しい VPN 接続を作成することで、AWS VPN 接続に移行できます。既存の AWS Direct Connect プライベート仮想インターフェイスに変更を加える必要はありません。

Important

この手順を実行する間、AWS Direct Connect プライベート仮想インターフェイス経由の接続は中断されませんが、Site-to-Site VPN 接続経由での接続は失われます (冗長性が失われますが、ダウンタイムは発生しません)。VPN 接続が仮想プライベートゲートウェイで再作成されると、VPN 接続を介した接続が復元されます。この冗長性の喪失に備えて確実に計画してください。AWS Classic VPN 接続を削除した後に、新しい AWS VPN 接続を元の AWS Classic VPN 接続に戻す、または移行することはできません。

AWS VPN 接続へ移行するには

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、AWS Classic VPN 接続を選択します。[Actions] で、[Delete] を選択します。

3. カスタマーゲートウェイデバイスから以前のトンネル設定を削除します。
4. 前の 2 つの手順を繰り返して、仮想プライベートゲートウェイの既存の AWS Classic VPN 接続をすべて削除します。VPN 接続が `deleted` 状態になるのを待ちます。
5. [Create VPN Connection (VPN 接続の作成)] を選択します。以下の情報を指定し、[VPN 接続の作成] を選択します。
 - [仮想プライベートゲートウェイ]: AWS Classic VPN 接続に使用した仮想プライベートゲートウェイを選択します。
 - [カスタマーゲートウェイ]: [既存] を選択し、現在の AWS Classic VPN 接続の既存のカスタマーゲートウェイを選択します。
 - 必要に応じてルーティングオプションを指定します。
6. 新しい Site-to-Site VPN 接続を選択し、[Download Configuration] を選択します。カスタマーゲートウェイデバイスに適した設定ファイルをダウンロードします。
7. 設定ファイルを使用して、カスタマーゲートウェイデバイスの VPN トンネルを設定します。詳細については、「」を参照してください[カスタマーゲートウェイデバイス \(p. 32\)](#)
8. カスタマーゲートウェイデバイスで新しいトンネルを有効にします。トンネルを起動するには、ローカルネットワークから接続を開始する必要があります。

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

トランジットゲートウェイ VPN アタッチメントの作成

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、カスタマーゲートウェイを指定する必要があります。トランジットゲートウェイの作成の詳細については、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](#)」を参照してください。

コンソールを使用して 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 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. [Target Gateway Type (ターゲットゲートウェイタイプ)] で、[Transit Gateway] を選択し、アタッチメントを作成するトランジットゲートウェイを選択します。
5. [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、[Existing (既存)] を選択してから、使用する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。[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、「[Site-to-Site VPN 接続のカスタマーゲートウェイオプション \(p. 12\)](#)」を参照してください。[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)。

[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。

6. (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、「」を参照してください[Site-to-Site VPN 接続の高速化 \(p. 13\)](#)

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。追加の変更が適用されます。

7. [トンネルオプション] については、「[Site-to-Site VPN 接続のトンネルオプション \(p. 5\)](#)」を参照してください。
8. [Create VPN Connection (VPN 接続の作成)] を選択します。

を使用して VPN アタッチメントを作成するには AWS CLI

`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 接続のテスト

AWS Site-to-Site VPN 接続を作成してカスタマーゲートウェイを設定した後、インスタンスを起動し、インスタンスへの ping を実行して接続をテストできます。

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] を選択します。
3. [Choose an Amazon Machine Image (AMI)] ページで、AMI を選択し、[Select] を選択します。
4. インスタンスタイプを選択し、[Next: Configure Instance Details] を選択します。
5. [Configure Instance Details] ページの [Network] で VPC を選択します。[Subnet] で、サブネットを選択します。[Configure Security Group] ページが表示されるまで、[Next] を選択します。
6. [Select an existing security group (既存のセキュリティグループを選択する)] オプションを選択し、前に設定したグループを選択します。[Review and Launch] を選択します。
7. 選択した設定を確認します。必要な変更を行い、[Launch] を選択し、キーペアを選択してインスタンスを起動します。

8. インスタンスが実行中になった後、そのプライベート IP アドレス (例えば 10.0.0.4) を取得します。Amazon EC2 コンソールにインスタンスの詳細の一部としてアドレスが表示されます。
9. ネットワークでカスタマーゲートウェイ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。正常な応答は次のようになります。

```
ping 10.0.0.4
```

```
Pinging 10.0.0.4 with 32 bytes of data:

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

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

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

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、上記の手順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。

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 インスタンスへの接続](#)」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、Windows インスタンス用 Amazon EC2 ユーザーガイドの「[Windows インスタンスへの接続](#)」を参照してください。

Site-to-Site VPN 接続の削除

AWS Site-to-Site VPN 接続が不要になった場合は、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。

Important

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。

トピック

- [Site-to-Site VPN 接続の削除 \(p. 107\)](#)
- [カスタマーゲートウェイの削除 \(p. 108\)](#)
- [仮想プライベートゲートウェイのデタッチと削除 \(p. 108\)](#)

Site-to-Site VPN 接続の削除

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 Site-to-Site 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 Connections (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]、[削除] の順に選択します。
4. [削除] を選択します。

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

- [DeleteVpnConnection](#) (Amazon EC2 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の削除

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、[Customer Gateways] を選択します。
2. 削除するカスタマーゲートウェイを選択し、[Actions]、[Delete Customer Gateway] を選択します。
3. [Yes, Delete] を選択します。

コマンドラインまたは API を使用して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のデタッチと削除

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 [Virtual Private Gateways] 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. [Yes, Detach] を選択します。

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

コンソールを使用して仮想プライベートゲートウェイを削除するには

1. ナビゲーションペインで [Virtual Private Gateways] 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、[Actions]、[Delete Virtual Private Gateway] を選択します。
3. [Yes, Delete] を選択します。

コマンドラインまたは API を使用して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の変更

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

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

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: トランジットゲートウェイを作成する](#) (p. 109)
- [ステップ 2: 静的ルート \(静的 VPN 接続のトランジットゲートウェイへの移行に必要な\) を削除する](#) (p. 110)
- [ステップ 3: 新しいゲートウェイに移行する](#) (p. 110)
- [ステップ 4: VPC ルートテーブルを更新する](#) (p. 111)
- [ステップ 5: トランジットゲートウェイルーティングの更新 \(新しいゲートウェイがトランジットゲートウェイである場合に必須\)](#) (p. 111)
- [ステップ 6: カスタマーゲートウェイ ASN を更新する \(新しいゲートウェイに古いゲートウェイとは異なる ASN がある場合に必要\)](#) (p. 112)

ステップ 1: トランジットゲートウェイを作成する

新しいゲートウェイへの移行を実行する前に、新しいゲートウェイを設定する必要があります。仮想プライベートゲートウェイを追加する方法については、「[the section called “仮想プライベートゲートウェイの作成” \(p. 20\)](#)」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、「」を参照してください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 (新しいゲートウェイに古いゲートウェイとは異なる ASN がある場合に必要)” (p. 112)

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

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

新しいゲートウェイに移行する前に静的ルートを削除する必要があります。

Tip

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

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 [Route Tables] を選択して、ルートテーブルを選択します。
3. [ルート] タブで [編集] を選択し、仮想プライベートゲートウェイへの静的ルートで [削除] を選択します。
4. 完了したら、[保存] を選択します。

ステップ 3: 新しいゲートウェイに移行する

1. 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. Site-to-Site VPN 接続を選択して、[アクション]、[Modify VPN Connection (VPN 接続の変更)] の順に選択します。
4. [Change Target (ターゲットの変更)] で、次の操作を実行します。

- a. [ターゲットの種類] でゲートウェイの種類を選択します。
- b. 接続ターゲットの設定:

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

[トランジットゲートウェイ] [Target transit gateway ID (ターゲットトランジットゲートウェイ ID)] で、トランジットゲートウェイ ID を選択します。

5. [保存] を選択します。

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

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

ステップ 4: VPC ルートテーブルを更新する

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

VPN ゲートウェイターゲットの修正に必要な VPC ルートテーブルの更新

既存のゲートウェイ	新しいゲートウェイ	VPC のルートテーブルの変更
伝播されたルートを持つ仮想プライベートゲートウェイ	トランジットゲートウェイ	トランジットゲートウェイ ID を指すルートを追加します。
伝播されたルートを持つ仮想プライベートゲートウェイ	伝播されたルートを持つ仮想プライベートゲートウェイ	必要なアクションはありません。
伝播されたルートを持つ仮想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 ID が格納されているエントリを追加します。
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	VPC ルートテーブルを更新して、仮想プライベートゲートウェイ ID を格納するエントリをトランジットゲートウェイ ID に変更します。
静的ルートを持つ仮想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	仮想プライベートゲートウェイ ID を指すエントリを新しい仮想プライベートゲートウェイ ID に更新します。
静的ルートを持つ仮想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 ID を含むエントリを削除します。
トランジットゲートウェイ	静的ルートを持つ仮想プライベートゲートウェイ	トランジットゲートウェイを格納するエントリを仮想プライベートゲートウェイ ID に更新します。
トランジットゲートウェイ	伝播されたルートを持つ仮想プライベートゲートウェイ	トランジットゲートウェイ ID を含むエントリを削除します。
トランジットゲートウェイ	トランジットゲートウェイ	トランジットゲートウェイ ID を含むエントリを新しいトランジットゲートウェイ ID に更新します。

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

新しいゲートウェイがトランジットゲートウェイである場合、トランジットゲートウェイのルートテーブルを変更して VPC と Site-to-Site VPN 間のトラフィックを許可します。トランジットゲートウェイルー

デバッグの詳細については、Amazon VPC トランジットゲートウェイの「[トランジットゲートウェイルートテーブル](#)」を参照してください。

Important

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

ステップ 6: カスタマーゲートウェイ ASN を更新する (新しいゲートウェイに古いゲートウェイとは異なる ASN がある場合に必要)

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 \(p. 12\)](#)」を参照してください。

Site-to-Site VPN 接続オプションの変更

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 Connections (Site-to-Site VPN 接続)] を選択します。
3. VPN 接続を選択し、[Actions (アクション)]、[Modify VPN Connection Options (VPN 接続オプションの変更)] の順に選択します。
4. 変更するオプションの新しい値を入力します。
5. [保存] を選択します。

コマンドラインまたは API を使用して 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の変更

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 Connections (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]、[Modify VPN Tunnel Options (VPN トンネルオプションの変更)] の順に選択します。
4. [VPN Tunnel Outside IP Address (VPN トンネル外部 IP アドレス)] で、オプションを変更する 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. 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、「[Site-to-Site VPN 接続のトンネルオプション \(p. 5\)](#)」を参照してください。
6. [Save] を選択します。

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 接続の静的ルートの編集

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。

静的ルートを追加、変更、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 Connections (Site-to-Site VPN 接続)] を選択します。
3. [Static Routes]、[Edit] を選択します。
4. 既存の静的 IP プレフィックスを変更するか、[Remove] を選択して削除します。[Add Another Rule] を選択して、新しい IP プレフィックスを設定に追加します。完了したら、[Save] を選択します。

Note

ルートテーブルでルート伝達を有効にしていない場合、ルートテーブルで手動でルートを更新し、更新された静的 IP プレフィックスを Site-to-Site VPN 接続に反映する必要があります。詳細については、「[\(仮想プライベートゲートウェイ\) ルートテーブルでルート伝播を有効にする \(p. 21\)](#)」を参照してください。

トランジットゲートウェイ上の Site-to-Site 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、「[トランジットゲートウェイルートテーブル](#)」を参照してください。

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の変更

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、Site-to-Site 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 Connections (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]、[Modify VPN Connection (VPN 接続の変更)] の順に選択します。
4. [Target Type (ターゲットの種類)] で、[Customer Gateway (カスタマーゲートウェイ)] を選択します。
5. [Target Customer Gateway ID (ターゲットカスタマーゲートウェイ ID)] で、接続に使用するカスタマーゲートウェイの ID 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変更するには

- [ModifyVpnTunnelC](#) (Amazon EC2 Query API)
- [modify-vpn-tunnel](#) (AWS CLI)

漏洩した認証情報の置き換え

Site-to-Site VPN 接続のトンネル認証情報が漏洩したと思われる場合は、IKE 事前共有キーを変更するか、ACM 証明書を変更できます。使用方法は、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 \(p. 10\)](#)」を参照してください。

IKE 事前共有キーを変更するには

Site-to-Site 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の変更 \(p. 112\)](#)」を参照してください。

または、Site-to-Site VPN 接続を削除することもできます。詳細については、「[Site-to-Site VPN 接続の削除 \(p. 107\)](#)」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 Site-to-Site 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。詳細については、[サイト間 VPN 接続の作成 \(p. 22\)](#) を参

照してください。Site-to-Site 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、「[the section called “Site-to-Site VPN トンネルエンドポイント証明書の更新” \(p. 115\)](#)」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。ACM 証明書の作成については、AWS Certificate Manager ユーザーガイドの[開始方法](#)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の更新

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 “サービスにリンクされたロールによって付与されるアクセス許可” \(p. 121\)](#)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 Connections (Site-to-Site VPN 接続)] を選択します。
3. Site-to-Site VPN 接続を選択し、[Actions, Rotate Tunnel Certificates (アクション、トンネル証明書の更新)] を選択します。
4. 証明書を更新するトンネルエンドポイントを選択します。
5. [Save] 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。

AWS Site-to-Site VPN でのセキュリティ

AWS では、クラウドのセキュリティが最優先事項です。AWS のお客様は、セキュリティを最も重視する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ーから利点を得られます。

セキュリティは、AWS とお客様の間の共有責任です。[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説明しています。

- クラウドのセキュリティ – AWS は、AWS クラウド内で AWS 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を担います。また、AWS は、使用するサービスを安全に提供します。[AWS コンプライアンスプログラム](#)の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Site-to-Site VPN に適用するコンプライアンスプログラムの詳細については、[コンプライアンスプログラムによる対象範囲内の AWS のサービス](#)を参照してください。
- クラウド内のセキュリティ – お客様の責任はお客様が使用する AWS のサービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

Site-to-Site VPN は Amazon VPC サービスの一部です。Amazon VPC のセキュリティの詳細については、Amazon VPC ユーザーガイドの「[セキュリティ](#)」を参照してください。

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 の特定のコンポーネントを設定する方法について説明します。

目次

- [AWS Site-to-Site VPN でのデータ保護 \(p. 116\)](#)
- [AWS Site-to-Site VPN のアイデンティティとアクセス管理 \(p. 118\)](#)
- [ログ記録とモニタリング \(p. 122\)](#)
- [AWS Site-to-Site VPN での耐障害性 \(p. 122\)](#)
- [AWS Site-to-Site VPN でのインフラストラクチャセキュリティ \(p. 123\)](#)

AWS Site-to-Site VPN でのデータ保護

AWS [責任共有モデル](#)は、AWS Site-to-Site VPN のデータ保護に適用されます。このモデルで説明されているように、AWS は、AWS クラウド の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を担います。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。このコンテンツには、使用する AWS サービスのセキュリティ設定および管理タスクが含まれます。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の「[The AWS Shared Responsibility Model and GDPR](#)」を参照してください。

データを保護するため、AWS アカウント の認証情報を保護し、AWS Identity and Access Management (IAM) を使用して個々のユーザーアカウントをセットアップすることをお勧めします。この方法により、

それぞれの職務を遂行するために必要な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 AWS リソースと通信します。TLS 1.2 以降が推奨されています。
- AWS CloudTrail で API とユーザーアクティビティログをセットアップします。
- AWS 暗号化ソリューションを、AWS サービス内のすべてのデフォルトのセキュリティ管理と一緒に使用します。
- 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。これにより、Amazon S3 に保存される個人データの検出と保護が支援されます。
- コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。使用可能な 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。

顧客の 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。これは、コンソール、API、AWS CLI、または AWS SDK によって Site-to-Site VPN や他の AWS のサービスを使用する場合も同様です。タグまたは名前に使用する自由形式のフィールドに入力したデータは、請求ログまたは診断ログに使用できます。外部サーバーへの URL を指定する場合は、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 に含めないことを強くお勧めします。

Site-to-Site VPN の設定情報

Site-to-Site VPN 接続を作成すると、事前共有キー (該当する場合) など、カスタマーゲートウェイデバイスのセットアップに使用する設定情報が生成されます。設定情報への不正アクセスを防ぐには、必要なアクセス許可のみを IAM ユーザーに付与してください。Amazon VPC コンソールから設定ファイルをダウンロードする場合は、カスタマーゲートウェイデバイスを設定するユーザーだけに配布します。詳細については、次のトピックを参照してください。

- [Site-to-Site VPN トンネル認証オプション \(p. 10\)](#)
- [AWS Site-to-Site VPN のアイデンティティとアクセス管理 \(p. 118\)](#)

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 とお客様のネットワークをリンクする 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 \(p. 5\)](#): 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 \(p. 10\)](#): 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 \(p. 35\)](#): 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 \(p. 27\)](#): 複数の Site-to-Site VPN 接続がある場合は、AWS VPN CloudHub 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 Site-to-Site VPN のアイデンティティとアクセス管理

AWS ではセキュリティ認証情報を使用して、ユーザーを識別し、AWS リソースへのアクセスを付与します。AWS Identity and Access Management (IAM) の機能を使用して、他のユーザー、サービス、およびアプリケーションが完全にまたは制限付きでお客様の AWS リソースを使用できるようにします。その際、お客様のセキュリティ認証情報は共有されません。

デフォルトでは、IAM ユーザーには、AWS リソースを作成、表示、変更するための許可はありません。IAM ユーザーが Site-to-Site VPN 接続、仮想プライベートゲートウェイ、カスタマーゲートウェイなどのリソースにアクセスし、タスクを実行できるようにするには、次の操作を行う必要があります。

- 必要な特定のリソースと API アクションを使用するアクセス許可を IAM ユーザーに付与する IAM ポリシーを作成します。
- IAM ユーザーまたは IAM ユーザーが属するグループに、そのポリシーをアタッチします。

ポリシーをユーザーまたはユーザーのグループにアタッチする場合、ポリシーによって特定リソースの特定タスクを実行するユーザーの権限が許可または拒否されます。

Site-to-Site VPN は Amazon VPC の一部であり、その API 名前空間を Amazon EC2 と共有します。Site-to-Site VPN 接続、仮想プライベートゲートウェイ、カスタマーゲートウェイを操作するには、次の AWS 管理ポリシーのいずれかがニーズを満たす場合があります。

- PowerUserAccess
- ReadOnlyAccess
- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess

ユーザーに `ec2:DescribeVpnConnections` のアクションを使用するアクセス許可を付与するには注意が必要です。このアクションにより、ユーザーはアカウント内の Site-to-Site VPN 接続のカスタマーゲートウェイ設定情報を表示できます。

その他の例については、Amazon VPC ユーザーガイドの「[Amazon VPC の Identity and Access Management](#)」および Amazon EC2 ユーザーガイドの「[Amazon EC2 の IAM ポリシー](#)」を参照してください。

Site-to-Site VPN 接続の IAM ポリシー

リソースレベルのアクセス許可を使用して、ユーザーが API を呼び出すときに使用できるリソースを制限できます。IAM アクセス許可ポリシーステートメント (`arn:aws:ec2:us-west-2:123456789012:vpn-connection/vpn-0d4e855ab7d3536fb` など) の `Resource` 要素で、VPN 接続の Amazon リソースネーム (ARN) を指定できます。

次のアクションは、VPN 接続リソースのリソースレベルのアクセス許可をサポートします。

- `ec2:CreateVpnConnection`
- `ec2:ModifyVpnConnection`
- `ec2:ModifyVpnTunnelOptions`

サポートされている条件キーは次のとおりです。

条件キー	説明	有効な値	タイプ
<code>ec2:AuthenticationType</code>	VPN トンネルエンドポイントの認証タイプ。	事前共有キー、証明書	文字列
<code>ec2:DPDTimeoutSeconds</code>	DPD タイムアウトが発生するまでの時間。	0 ~ 30 までの整数	数値
<code>ec2:GatewayType</code>	VPN 接続の AWS 側にある VPN エンドポイントのゲートウェイタイプ。	VGW、TGW	文字列
<code>ec2:IKEVersions</code>	VPN トンネルで許可されているインターネットキー交換 (IKE) バージョン。	ikev1、ikev2	文字列
<code>ec2:InsideTunnelCidr</code>	VPN トンネルの内部 IP アドレスの範囲です。	「 Site-to-Site VPN 接続のトンネルオプション (p. 5) 」を参照してください。	文字列
<code>ec2:Phase1DHGroupNumber</code>	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。	2、14、15、16、17、18、 19	数値 20、21、22、23、24
<code>ec2:Phase2DHGroupNumber</code>	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。	2、5、14、15、16、17、 18	数値 22、23、24
<code>ec2:Phase1EncryptionAlgorithm</code>	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。	AES128、AES256、AES128-GCM-16、AES256-GCM-16	文字列
<code>ec2:Phase2EncryptionAlgorithm</code>	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。	AES128、AES256	文字列
<code>ec2:Phase1IntegrityAlgorithm</code>	フェーズ 1 IKE ネゴシエーションの VPN トンネルで許可される整合性アルゴリズム。	SHA1、SHA2-256	文字列
<code>ec2:Phase2IntegrityAlgorithm</code>	フェーズ 2 IKE ネゴシエーションの VPN トン	SHA1、SHA2-384、SHA2-256、 SHA2-512	文字列 SHA2-512

条件キー	説明	有効な値	タイプ
	ネルで許可される整合性アルゴリズム。		
ec2:Phase1LifetimeSeconds	IKE ネゴシエーションのフェーズ 1 のライフタイム (秒)。	900 ~ 28,800 の整数	数値
ec2:Phase2LifetimeSeconds	IKE ネゴシエーションのフェーズ 2 のライフタイム (秒)。	900 ~ 3,600 の整数	数値
ec2:PresharedKeys	仮想プライベートゲートウェイとカスタマーゲートウェイ間に最初の IKE Security Association を確立するための事前共有キー (PSK)。	「 Site-to-Site VPN 接続のトンネルオプション (p. 5) 」を参照してください。	文字列
ec2:RekeyFuzzPercentage	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 の整数	数値
ec2:RekeyMarginTimeSeconds	フェーズ 2 の有効期限が切れる前のマージン時間。この間、AWS は IKE キー再生成を実行します。	60 以上の整数	数値
ec2:RoutingType	VPN 接続のルーティングタイプ。	スタティック、BGP	文字列

IAM 条件演算子を使用して、サポートされている条件キーごとに特定の値を許可または拒否できます。詳細については、IAM ユーザーガイドの「[IAM JSON ポリシー要素: 条件](#)」を参照してください。

次のポリシー例では、ユーザーは VPN 接続を作成できますが、静的ルーティングタイプの VPN 接続のみが許可されています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpnConnection"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:RoutingType": [
            "static"
          ]
        }
      }
    }
  ]
}
```

```
}  
]  
}
```

AWS Site-to-Site VPN サービスにリンクされたロール

AWS Site-to-Site VPN は、ユーザーに代わって他の AWS のサービス呼び出すために必要な許可を持つサービスにリンクされたロールを使用します。詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの使用](#)」を参照してください。

サービスにリンクされたロールによって付与されるアクセス許可

証明書ベースの認証を使用する Site-to-Site VPN 接続を使用する場合、Site-to-Site VPN は `AWSServiceRoleForVPCS2SVPN` という名前のサービスにリンクされたロールを使用して、ユーザーに代わって次の AWS Certificate Manager (ACM) アクションを呼び出します。

- `acm:ExportCertificate`
- `acm:DescribeCertificate`
- `acm:ListCertificates`
- `acm-pca:DescribeCertificateAuthority`

サービスにリンクされたロールの作成

`AWSServiceRoleForVPCS2SVPN` ロールを手動で作成する必要はありません。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 によってこのロールが作成されます。

Site-to-Site VPN ユーザーがお客様に代わってサービスにリンクされたロールを作成するには、必要なアクセス許可がお客様に付与されていなければなりません。サービスにリンクされたロールの詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールのアクセス許可](#)」を参照してください。

サービスにリンクされたロールを編集する

IAM を使用して、`AWSServiceRoleForVPCS2SVPN` の説明を編集できます。サービスにリンクされたロールの編集の詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの編集](#)」を参照してください。

サービスにリンクされたロールを削除する

証明書ベースの認証で Site-to-Site VPN 接続を使用する必要がなくなった場合は、`AWSServiceRoleForVPCS2SVPN` を削除することをお勧めします。

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は、IAM コンソール、IAM CLI、または IAM API を使用して削除することができます。サービスにリンクされたロールの削除の詳細については、IAM ユーザーガイドの「[サービスにリンクされたロールの削除](#)」を参照してください。

`AWSServiceRoleForVPCS2SVPN` を削除すると、Amazon VPC は、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のロールを再び作成します。

ログ記録とモニタリング

モニタリングは、AWS Site-to-Site VPN 接続の信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。AWS には、リソースをモニタリングし、潜在的なインシデントに対応するための複数のツールが用意されています。

Amazon CloudWatch

Amazon CloudWatch は、AWS のリソースおよび AWS で実行しているアプリケーションをリアルタイムでモニタリングします。Site-to-Site VPN トンネルのメトリクスの収集と追跡、および指定したメトリクスが指定したしきい値に達したときに通知またはアクションを実行するアラームの設定を行うことができます。詳細については、[Site-to-Site VPN 接続のモニタリング \(p. 124\)](#) を参照してください。

AWS CloudTrail

AWS CloudTrail は、AWS アカウントによって行われた、またはそのアカウントの代わりに行われた Amazon EC2 API 呼び出しとそれに関連するイベントを記録します。次に、指定した Amazon S3 バケットにログファイルが渡されます。詳細については、Amazon EC2 API リファレンスの [AWS CloudTrail を使用した Amazon EC2、Amazon EBS、および Amazon VPC API 呼び出しのログ記録](#) を参照してください。

AWS Trusted Advisor

AWS Trusted Advisor は、AWS の数十万のお客様にサービスを提供することにより得られた、運用実績から学んだベストプラクティスを活用しています。Trusted Advisor はお客様の AWS 環境を検査し、システムの可用性とパフォーマンスを向上させたりセキュリティギャップを埋めたりする機会がある場合には、推奨事項を作成します。

Trusted Advisor には、VPN トンネルの冗長性のチェックがあります。これは、各 VPN 接続でアクティブなトンネルの数をチェックします。

詳細については、AWS Support ユーザーガイドの [AWS Trusted Advisor](#) を参照してください。

AWS Site-to-Site VPN での耐障害性

AWS のグローバルインフラストラクチャは AWS リージョンとアベイラビリティゾーンを中心として構築されます。AWS リージョンには、低レイテンシー、高スループット、そして高冗長性のネットワークで接続されている複数の物理的に独立・隔離されたアベイラビリティゾーンがあります。アベイラビリティゾーンでは、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、耐障害性、および拡張性が優れています。

AWS リージョンとアベイラビリティゾーンの詳細については、「[AWS グローバルインフラストラクチャ](#)」を参照してください。

Site-to-Site VPN では、AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるように複数の機能を提供しています。

VPN 接続ごとに 2 つのトンネル

Site-to-Site VPN 接続には 2 つのトンネルがあるため、VPC の可用性が向上します。AWS でデバイス障害が発生した場合、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て、アクセスが中断されないようにします。ときどき、AWS は、VPN 接続の定期メンテナンスも実行します。これにより、VPN 接続の 2 つのトンネルの 1 つが短時間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 \(p. 11\)](#) 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 \(p. 29\)](#)
- [Amazon Virtual Private Cloud Connectivity Options](#)
- [スケーラブルでセキュアなマルチ VPC の 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 でのインフラストラクチャセキュリティ

管理型サービスである AWS Site-to-Site VPN は、ホワイトペーパーの[アマゾン ウェブ サービスのセキュリティプロセスの概要](#)に記載されているAWS グローバルネットワークセキュリティの手順で保護されています。

AWS が公開している 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。クライアントで Transport Layer Security (TLS) 1.0 以降がサポートされている必要があります。TLS 1.2 以降が推奨されています。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされています。

また、リクエストは、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 Service](#) (AWS 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うえで重要な部分です。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？
- モニタリングの対象となるリソースとは？
- どのくらいの頻度でこれらのリソースをモニタリングしますか？
- 使用するモニタリングツールは？
- 誰がモニタリングタスクを実行しますか？
- 問題が発生したときに誰が通知を受け取りますか？

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

ベースラインを確立するには、次の項目をモニタリングする必要があります。

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

目次

- [モニタリングツール \(p. 124\)](#)
- [アマゾン CloudWatch を使用した VPN トンネルのモニタリング \(p. 125\)](#)
- [AWS Health イベントを使用した VPN 接続のモニタリング \(p. 129\)](#)

モニタリングツール

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

自動モニタリングツール

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

- Amazon CloudWatch のアラーム – 単一のメトリクスを指定した期間モニタリングし、特定のしきい値に対する複数の期間にわた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 トピックに送信される通知です。CloudWatch のアラームは、メトリクスが特定の状態になっただけではアクションを呼び出しません。アクションを呼び出すには、状態が変化して、指定した期間継続している必要があります。詳細については、「[アマゾン CloudWatch を使用した VPN トンネルのモニタリング \(p. 125\)](#)」を参照してください。

- AWS CloudTrail の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 のログファイルを CloudWatch Logs に送信してリアルタイムでモニタリングします。また、ログを処理するアプリケーションを Java で作成し、CloudTrail からの提供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。詳細については、Amazon EC2 API リファレンスの「[AWS CloudTrail を使用した API 呼び出しのログ記録](#)」と、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 トンネルの状態の変化や、ベストプラクティスの設定の推奨事項に関連するアラートと通信を受信します。または、スケーリング制限に近づいたときにも受信します。[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 \(p. 129\)](#)」を参照してください。

手動モニタリングツール

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

- Amazon VPC ダッシュボードには、次の内容が表示されます。
 - リージョン別のサービス状態
 - Site-to-Site VPN 接続
 - VPN トンネルの状態 (ナビゲーションペインで、[Site-to-Site VPN Connections (Site-to-Site VPN 接続)]、[サイト間 VPN 接続]、[トンネル詳細] の順に選択します)
- CloudWatch のホームページには、以下の情報が表示されます。
 - 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
 - サービス状態ステータス

また、CloudWatch を使用して以下のことを行えます。

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

アマゾン CloudWatch を使用した VPN トンネルのモニタリング

CloudWatch を使用して VPN トンネルをモニタリングすることで、VPN サービスから 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。

Important

CloudWatch メトリクスは、AWS Classic VPN 接続ではサポートされません。詳細については、「[Site-to-Site VPN カテゴリ \(p. 4\)](#)」を参照してください。

詳細については、[Amazon CloudWatch ユーザーガイド](#)を参照してください。

VPN トンネルのメトリクスとディメンション

VPN トンネルでは、次のメトリクスを使用できます。

メトリクス	説明
TunnelState	トンネルの状態。静的 VPN の場合、0 は DOWN を示し、1 は UP を示します。BGP VPN の場合、1 は 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 トンネルを介した接続の 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。 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 トンネルを介した接続の AWS 側からカスタマーゲートウェイに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

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

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

VPN トンネル CloudWatch メトリクスの表示

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

CloudWatch コンソールを使用してメトリクスを表示するには

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

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

AWS CLI を使ってメトリクスを表示するには

コマンドプロンプトで、次のコマンドを使用します。

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

VPN トンネルをモニタリングする CloudWatch アラームの作成

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 Amazon CloudWatch のアラームを作成することができます。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。

たとえば、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。

トンネル状態のアラームを作成するには

1. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。
2. ナビゲーションペインで、[アラーム]、[アラームの作成] の順にクリックします。
3. [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 [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. [Next] を選択します。
7. 次のいずれかの操作を実行し、[Additional configuration] (その他の設定) で、アラームを送信するデータポイントとして 3 を入力します。[Next] を選択します。
 - 両方のトンネルがダウンする場合を監視するには、[Whenever] (次の時) で [Lower/Equal (<=)] (以下 (<=)) を選択し、0.5 を入力します。
 - いずれかのトンネルの DOWN 状態を監視するには、[Whenever] (次の時) で、[Lower (<)] (より低い (<)) を選択し、1 を入力します。
8. [SNS トピックの選択] で、既存の通知リストを選択するか、新しい通知リストを作成します。[Next] を選択します。
9. アラームの名前と説明を入力します。[Next] 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。

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. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。
2. ナビゲーションペインで、[アラーム]、[アラームの作成] の順にクリックします。
3. [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)。[Next] 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。[Next] を選択します。
9. アラームの名前と説明を入力します。[Next] 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. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。
2. ナビゲーションペインで、[アラーム]、[アラームの作成] の順にクリックします。
3. [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。[Next] 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。[Next] を選択します。
10. アラームの名前と説明を入力します。[Next] 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. CloudWatch コンソール (<https://console.aws.amazon.com/cloudwatch/>) を開きます。
2. ナビゲーションペインで、[アラーム]、[アラームの作成] の順にクリックします。
3. [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。[Next] 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。[Next] を選択します。
10. アラームの名前と説明を入力します。[Next] 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 CloudWatch ユーザーガイドの「[Amazon CloudWatch アラームの作成](#)」を参照してください。

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 を利用する AWS [AWS Personal Health Dashboard](#) (PHD) に通知を自動的に送信します。このダッシュボードのセットアップは必要ありません。認証済みの AWS ユーザーは、すぐに使い始めることができます。を使用して、イベント通知に応じて複数のアクションを設定できます [AWS Personal Health Dashboard](#)

AWS Personal Health Dashboard には、VPN 接続に関する次のタイプの通知が表示されます。

- [トンネルエンドポイント交換通知](#) (p. 129)
- [単一トンネル VPN 通知](#) (p. 129)

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交換されたときに、AWS Personal Health Dashboard にトンネルエンドポイント交換通知が表示されます。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](#) (p. 11)」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、AWS は AWS Personal Health Dashboard イベントを通じてトンネルエンドポイント交換通知を送信します。

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 つのトンネルがアップし、もう一方が 1 日に 1 時間以上ダウンしている場合は、AWS Personal Health Dashboard イベントを通じて VPN 単一トンネル通知が毎週送信されます。

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、クライアント VPN クォータテーブルで [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「[クォータの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	[Yes (はい)]

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。

Routes

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。

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

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 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
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	いいえ

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)

カスタマーゲートウェイデバイスの論理インターフェイスの MTU を 1399 バイトに設定する必要があります。詳細については、「[」](#)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要件 \(p. 35\)](#)

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。

SHA2-384 または SHA2-512 ハッシュアルゴリズムを使用する場合は、カスタマーゲートウェイデバイスの最大セグメントサイズ (MSS) を 1359 に設定することをお勧めします。

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。

ドキュメント履歴

次の表では、AWS Site-to-Site VPN ユーザーガイドの更新について説明します。

更新履歴の変更	更新 - 履歴 - 記述	更新 - 履歴 - 日付
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自動的に送信しますAWS Personal Health Dashboard	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 ガイドのマージ	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
AWS Site-to-Site VPN 接続の高速化	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を変更	AWS Site-to-Site VPN 接続で 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 Certificate Manager 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 Certificate Manager 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 (p. 132)	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 カテゴリ	VPN 接続の現在のカテゴリを表示できます。	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 (p. 132)	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 (p. 132)	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 (p. 132)	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 (p. 132)	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