AWS クライアント VPN

管理者ガイド

AWS クライアント VPN: 管理者ガイド

Table of Contents

AWS Client VPN とは? 1
クライアント VPN の機能 1
クライアント VPN のコンポーネント 1
クライアント VPN の使用 2
クライアント VPN の制限とルール 3
クライアント VPN の料金 4
クライアント VPN の仕組み 5
クライアント認証と認可 6
認証 6
Authorization 13
接続承認 14
要件と考慮事項 15
Lambda インターフェイス 15
体制評価のためのクライアント接続ハンドラーの使用 17
クライアント接続ハンドラーの有効化 17
サービスにリンクされたロール 17
接続承認失敗のモニタリング 17
分割トンネルクライアント VPN 18
分割トンネルの利点 19
ルーティングに関する考慮事項 20
分割トンネルの有効化 20
接続ログ 20
接続ログエントリ 20
スケーリングに関する考慮事項 21
シナリオと例 23
VPC へのアクセス 23
ピア接続先 VPC へのアクセス 25
オンプレミスのネットワークへのアクセス 26
インターネットへのアクセス 28
クライアント間のアクセス 30
ネットワークへのアクセスを制限する 32
セキュリティグループを使用してアクセスを制限する 32
ユーザーグループに基づいてアクセスを制限する 34
開始方法 35
Prerequisites 36
ステップ 1: サーバーおよびクライアント証明書とキーの生成 36
ステップ 2: クライアント VPN エンドポイントを作成する 36
ステップ 3: クライアントの VPN 接続を有効にする 37
ステップ 4: クライアントのネットワークへのアクセスを承認する 38
ステップ 5: (オプション) 追加のネットワークへのアクセスを有効にする 38
ステップ 6: クライアント VPN エンドポイント設定ファイルをダウンロードする 39
ステップ 7: クライアント VPN エンドポイントに接続する 40
クライアント VPN の使用 41
クライアント VPN エンドポイント 41
クライアント VPN エンドポイントを作成する 41
クライアント VPN エンドポイントを変更する 43
クライアント設定ファイルをエクスポートして設定する 45
クライアント VPN エンドポイントを表示する 48
クライアント VPN エンドポイントを削除する 48
ターゲットネットワーク 48
ターゲットネットワークをクライアント VPN エンドポイントに関連付ける 49
セキュリティグループをターゲットネットワークに適用する 50
ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除する 50
ターゲットネットワークの表示 51

承認ルール 51
クライアント VPN エンドポイントへの承認ルールの追加 51
クライアント VPN エンドポイントから承認ルールを削除する 52
承認ルールの表示 53
ルート 53
クライアント VPN エンドポイントの分割トンネルに関する考慮事項 53
エンドポイントルートの作成 53
エンドポイントルートの表示 54
エンドポイントルートの削除 54
クライアント証明書失効リスト 55
クライアント証明書失効リストの生成 55
クライアント証明書失効リストのインポート 56
クライアント証明書失効リストのエクスポート 56
クライアント接続 57
クライアント接続の表示 57
クライアント接続の終了 57
接続ログ 58
新しいクライアント VPN エンドポイントの接続ログを有効にする 58
既存のクライアント VPN エンドポイントの接続ログを有効にする 59
接続ログの表示 59
接続ログの無効化 59
セキュリティ 61
データ保護 61
転送時の暗号化 62
インターネットトラフィックのプライバシー 62
クライアント VPN の Identity and Access Management 62
サービスにリンクされたロールの使用 64
ログ記録とモニタリング 65
耐障害性 66
高可用性対応の複数のターゲットネットワーク 66
インフラストラクチャセキュリティ 66
ベストプラクティス 66
IPv6 に関する考慮事項 67
クライアント VPN のモニタリング 69
CloudWatch によるモニタリング 69
CloudWatch メトリクスの表示 71
CloudTrail によるモニタリング 71
CloudTrail でのクライアント VPN 情報 72
クライアント VPN ログファイルエントリの概要 72
クライアント VPN クォータ 73
クライアント VPN クォータ 73
ユーザーとグループのクォータ 74
一般的な考慮事項 74
AWS クライアント VPN のトラブルシューティング 75
クライアント VPN エンドポイント DNS 名を解決できない 75
トラフィックがサブネット間で分割されていない 76
Active Directory グループの承認ルールが想定どおりに機能しない 76
クライアントがピア接続 VPC、Amazon S3、またはインターネットにアクセスできない 77
ピア接続 VPC、Amazon S3、またはインターネットへのアクセスが断続的である 79
クライアントソフトウェアが TLS エラーを返す 80
クライアントソフトウェアがユーザー名とパスワードのエラーを返す (Active Directory 認証) 81
クライアントが接続できない (相互認証) 81
クライアントから、認証情報が最大サイズを超えるというエラーが返される (フェデレーション認証) 81
クライアントでブラウザが開かない (フェデレーション認証) 82
クライアントから、使用可能なポートがないというエラーが返される (フェデレーション認証) 82
クライアント VPN エンドポイントの帯域幅制限を確認する 82
ドキュメント履歴 84

AWS Client VPN とは?

AWS Client VPN は、AWS リソースやオンプレミスネットワーク内のリソースに安全にアクセスできるようにする、クライアントベースのマネージド VPN サービスです。クライアント VPN を使用すると、OpenVPN ベースの VPN クライアントを使用して、どこからでもリソースにアクセスできます。

目次

- クライアント VPN の機能 (p. 1)
- クライアント VPN のコンポーネント (p. 1)
- クライアント VPN の使用 (p. 2)
- クライアント VPN の制限とルール (p. 3)
- クライアント VPN の料金 (p. 4)

クライアント VPN の機能

クライアント VPN には、以下の機能があります。

- 安全な接続 — OpenVPN クライアントを使用して、あらゆる場所から安全な TLS 接続を提供します。
- マネージド型サービス — これは AWS マネージドサービスであるため、サードパーティー製のリモートアクセス VPN ソリューションをデプロイして管理するという運用上の負担を取り除きます。
- 高可用性と高伸縮性 — AWS リソースとオンプレミスリソースに接続しているユーザー数に自動的に対応します。
- 認証 — Active Directory を使用したクライアント認証、フェデレーション認証、および証明書ベースの認証がサポートされます。
- きめ細かい制御 — ネットワークベースのアクセスルールを定義することで、カスタムセキュリティ管理を実装できます。これらのルールは、Active Directory グループの詳細度で設定できます。セキュリティグループを使用してアクセス制御を実装することもできます。
- 使いやすさ — 単一の VPN トンネルを使用して、AWS リソースとオンプレミスリソースにアクセスできます。
- 管理性 — クライアントの接続試行に関する詳細を提供する接続ログを表示できます。アクティブなクライアント接続を終了する機能で、アクティブなクライアント接続を管理することもできます。
- 高度な統合 — AWS Directory Service や Amazon VPC などの既存の AWS サービスと統合します。

クライアント VPN のコンポーネント

クライアント VPN の主な概念は次のとおりです。

クライアント VPN エンドポイント

クライアント VPN エンドポイントは、クライアント VPN セッションを有効にして管理するために作成して設定するリソースです。これは、すべてのクライアント VPN セッションが終端するリソースです。

ターゲットネットワーク

ターゲットネットワークは、クライアント VPN エンドポイントに関連付けるネットワークです。VPC からのサブネットはターゲットネットワークです。サブネットをクライアント VPN エンド

ポイントに関連付けると、VPN セッションを確立できます。高可用性を実現するために、複数のサブネットをクライアント VPN エンドポイントに関連付けることができます。すべてのサブネットは同一の VPC に存在する必要があります。各サブネットは異なるアベイラビリティーゾーンに属している必要があります。

ルート

各クライアント VPN エンドポイントには、利用可能な送信先ネットワークルートを説明したルートテーブルがあります。ルートテーブル内の各ルートは、特定のリソースまたはネットワークへのトラフィックのパスを指定します。

承認ルール

承認ルールは、ネットワークにアクセスできるユーザーを制限します。指定のネットワークに対して、アクセスを許可する Active Directory または ID プロバイダー (IdP) グループを構成します。このグループに属するユーザーだけが、指定のネットワークにアクセスできます。デフォルトでは承認ルールはありません。ユーザーがリソースやネットワークにアクセスできるように承認ルールを設定する必要があります。

クライアント

VPN セッションを確立するためにクライアント VPN エンドポイントに接続するエンドユーザー。エンドユーザーは、OpenVPN クライアントをダウンロードし、作成した Client VPN 設定ファイルを使用して VPN セッションを確立する必要があります。

クライアント CIDR 範囲

クライアント IP アドレスの割り当て元となる IP アドレスの範囲。クライアント VPN エンドポイントへの各接続には、クライアント CIDR 範囲から固有の IP アドレスが割り当てられます。クライアント CIDR 範囲を選択します (例: `10.2.0.0/16`)。

クライアント VPN ポート

AWS Client VPN は、TCP と UDP の両方のポート 443 および 1194 をサポートします。デフォルトはポート 443 です。

クライアント VPN ネットワークインターフェイス

サブネットをクライアント VPN エンドポイントに関連付けると、そのサブネットにクライアント VPN ネットワークインターフェイスが作成されます。クライアント VPN エンドポイントから VPC に送信されるトラフィックは、クライアント VPN ネットワークインターフェイスを介して送信されます。次に、ソースネットワークアドレス変換 (SNAT) が適用され、クライアント CIDR 範囲からのソース IP アドレスがクライアント VPN ネットワークインターフェイス IP アドレスに変換されます。

接続ログ

クライアント VPN エンドポイントの接続ログを有効にして、接続イベントをログに記録できます。この情報を使用してフォレンジックを実行したり、クライアント VPN エンドポイントがどのように使用されているかを分析したり、接続の問題をデバッグしたりできます。

セルフサービスポータル

クライアント VPN は、エンドユーザーが AWS VPN Desktop クライアントの最新バージョンとクライアント VPN エンドポイント設定ファイルの最新バージョンをダウンロードするためのウェブページとなるセルフサービスポータルです。このファイルには、エンドポイントへの接続に必要な設定が含まれています。クライアント VPN エンドポイント管理者は、クライアント VPN エンドポイントのセルフサービスポータルを有効または無効にすることができます。セルフサービスポータルは、アジアパシフィック (東京)、米国東部 (バージニア北部)、欧州 (アイルランド)、および AWS GovCloud (米国西部) リージョンのサービススタックによってサポートされるグローバルサービスです。

クライアント VPN の使用

クライアント VPN は、次のいずれかの方法で使用できます。

Amazon VPC コンソール

Amazon VPC コンソールは、クライアント VPN 用のウェブベースのユーザーインターフェイスを提供します。AWS アカウントにサインアップした場合は、Amazon VPC コンソールにサインインして、ナビゲーションペインで [クライアント VPN] を選択できます。

AWS Command Line Interface (CLI)

AWS CLI では、クライアント VPN のパブリック API への直接アクセスが可能です。Windows、macOS、Linux でサポートされています。AWS CLI の使用開始に関する詳細については、「AWS Command Line Interface ユーザーガイド」を参照してください。クライアント VPN のコマンドの詳細については、AWS CLI コマンドリファレンスを参照してください。

AWS Tools for Windows PowerShell

AWS は、PowerShell 環境でスクリプトを作成するユーザー向けに、さまざまな AWS 製品用のコマンドを提供しています。AWS Tools for Windows PowerShell の使用開始に関する詳細については、「AWS Tools for Windows PowerShell ユーザーガイド」を参照してください。クライアント VPN のコマンドレットの詳細については、「AWS Tools for Windows PowerShell コマンドレットリファレンス」を参照してください。

クエリ API

クライアント VPN HTTPS クエリ API を使用すると、クライアント VPN および AWS にプログラムでアクセスできます。HTTPS クエリ API を使用すると、HTTPS リクエストを直接サービスに発行できます。HTTPS API を使用する場合は、認証情報を使用してリクエストにデジタル署名するコードを含める必要があります。詳細については、「AWS Client VPN アクション」を参照してください。

クライアント VPN の制限とルール

クライアント VPN には、次のルールと制限があります。

- クライアント CIDR 範囲は、関連付けられたサブネットが配置されている VPC のローカル CIDR、またはクライアント VPN エンドポイントのルートテーブルに手動で追加されたルートと重複することはできません。
- クライアント CIDR 範囲は、ブロックサイズが /22 以上、/12 以下でなければなりません。
- クライアント CIDR 範囲内のアドレスの一部は、クライアント VPN エンドポイントの可用性モデルをサポートするために使用され、クライアントに割り当てることはできません。したがって、クライアント VPN エンドポイントでサポートする予定の同時接続の最大数を有効にするために必要な IP アドレスの数の 2 倍の数を含む CIDR ブロックを割り当てることをお勧めします。
- クライアント VPN エンドポイントの作成後にクライアント CIDR 範囲を変更することはできません。
- クライアント VPN エンドポイントに関連付けられているサブネットは、同じ VPC 内にある必要があります。
- 1 つのアベイラビリティーゾーンの複数のサブネットをクライアント VPN エンドポイントに関連付けることはできません。
- クライアント VPN エンドポイントは、専有テナント VPC でのサブネットの関連付けをサポートしていません。
- クライアント VPN は、IPv4 トラフィックのみをサポートしています。IPv6 の詳細については、「IPv6 に関する考慮事項 (p. 67)」を参照してください。
- クライアント VPN は、連邦情報処理規格 (FIPS) に準拠していません。
- Active Directory で Multi-Factor Authentication (MFA) が無効になっている場合、ユーザーパスワードを次の形式にすることはできません。

```
SCRV1:<base64_encoded_string>:<base64_encoded_string>
```

- セルフサービスポータルは、相互認証を使用して認証するクライアントでは利用できません。

- Client VPN エンドポイントにIP アドレスを使用して接続することはお勧めしません。Client VPN はマネージドサービスであるため、DNS 名が解決する IP アドレスが変化する場合があります。さらに、Client VPN ネットワークインターフェイスが削除され、Cloud Trail ログに再作成されることもありますが、これは予想される動作です。Client VPN エンドポイントへの接続には、提供された DNS 名を使用することをお勧めします。

クライアント VPN の料金

クライアント VPN エンドポイントごとにアクティブアソシエーションごとに時間単位で請求されます。請求額は、時間単位で案分されます。

各クライアントの1 時間あたりの VPN 接続に対して請求されます。請求額は、時間単位で案分されます。

詳細については、「AWS Client VPN の料金」を参照してください。

クライアント VPN エンドポイントの接続ログを有効にする場合は、アカウントに CloudWatch Logs ロググループを作成する必要があります。ロググループの使用には料金がかかります。詳細については、「Amazon CloudWatch の料金」を参照してください。

クライアント VPN エンドポイントでクライアント接続ハンドラーを有効にする場合は、Lambda 関数を作成して呼び出す必要があります。Lambda 関数の呼び出しには料金がかかります。詳細については、「AWS Lambda 料金表」を参照してください。

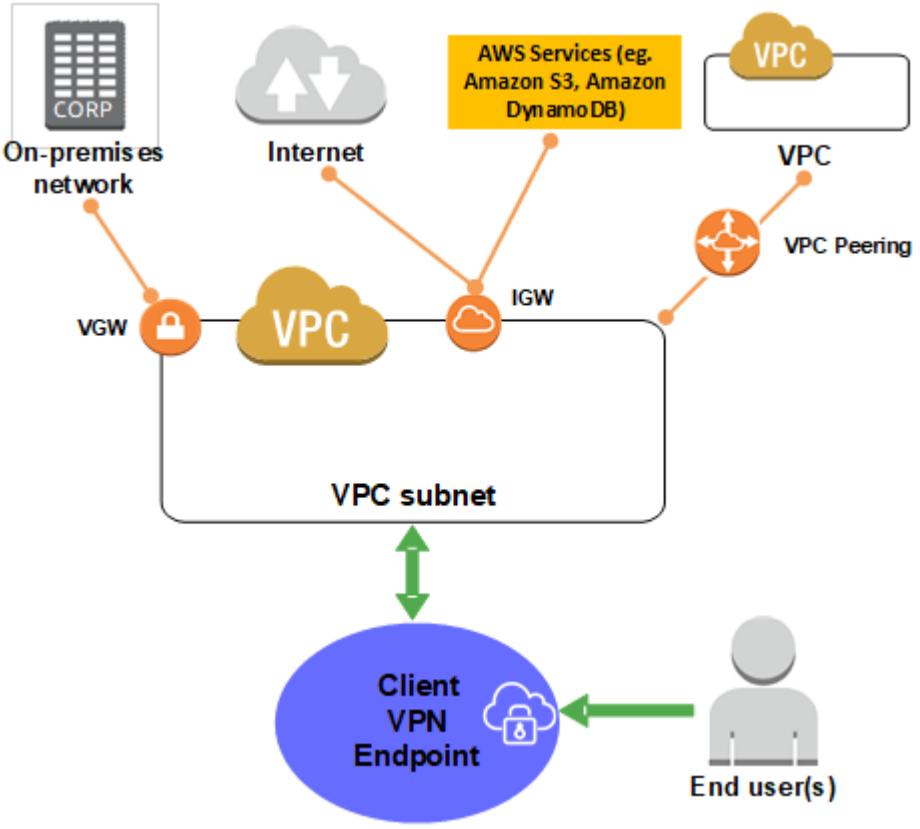
AWS クライアント VPN の仕組み

AWS クライアント VPN には、クライアント VPN エンドポイントの管理者およびクライアントとやり取りする 2 つのタイプのユーザーがいます。

管理者は、サービスの設定と設定を担当します。このプロセスには、クライアント VPN エンドポイントの作成、ターゲットネットワークの関連付け、認証ルールの設定、および追加のルート (必要な場合) の設定が含まれます。クライアント VPN エンドポイントを設定した後、管理者はクライアント VPN エンドポイント設定ファイルをダウンロードして、アクセスが必要なクライアントに配布します。クライアント VPN エンドポイント設定ファイルには、クライアント VPN エンドポイントの DNS 名と、VPN セッションを確立するために必要な認証情報が含まれています。サービス設定の詳細については、「クライアント VPN の開始方法 (p. 35)」を参照してください。

クライアントはエンドユーザーです。これは、VPN セッションを確立するためにクライアント VPN エンドポイントに接続する人です。クライアントは OpenVPN ベースの VPN クライアントアプリケーションを使用して、ローカルコンピュータまたはモバイルデバイスから VPN セッションを確立します。VPN セッションが確立されたら、関連付けられているサブネットが存在する VPC のリソースに安全にアクセスできます。必要なルートと認証ルールが設定されている場合は、AWS、オンプレミスネットワーク、または他のクライアントの他のリソースにもアクセスできます。VPN セッションを確立するためのクライアント VPN エンドポイントへの接続の詳細については、AWS クライアント VPN ユーザーガイドの「開始方法」を参照してください。

次の図は、基本的なクライアント VPN アーキテクチャを示しています。



クライアント認証と認可

クライアント VPN には認証および認可機能が用意されています。

目次

- Authentication (p. 6)
- Authorization (p. 13)

Authentication

認証は AWS クラウドへの最初のエントリポイントで実装されます。クライアントがクライアント VPN エンドポイントへの接続を許可されているかどうかを判断するために使用されます。認証が成功すると、クライアントはクライアント VPN エンドポイントに接続して VPN セッションを確立します。認証が失敗すると、接続は拒否され、クライアントは VPN セッションを確立できなくなります。

クライアント VPN では、次のタイプのクライアント認証を使用できます。

- Active Directory 認証 (p. 6) (ユーザーベース)
- 相互認証 (p. 7) (証明書ベース)
- シングルサインオン (SAML ベースのフェデレーション認証) (p. 9) (ユーザーベース)

次のいずれか、または組み合わせを使用できます。

- 相互認証とフェデレーション認証
- 相互認証と Active Directory 認証

> **Important**
>
> クライアント VPN エンドポイントを作成するには、使用する認証のタイプに関係なく、AWS Certificate Manager でサーバー証明書のプロビジョニングを行う必要があります。サーバー証明書の作成とプロビジョニングの詳細については、「相互認証 (p. 7)」の手順を参照してください。

Active Directory 認証

クライアント VPN は と統合することによって Active Directory サポートを提供しますAWS Directory Service Active Directory 認証では、クライアントは既存の Active Directory グループに対して認証されます。AWS Directory Service を使用して、クライアント VPN は AWS またはオンプレミスネットワークでプロビジョニングされた既存の Active Directory に接続できます。これにより、既存のクライアント認証インフラストラクチャを使用することができます。オンプレミスの Active Directory を使用していて、既存の AWS Managed Microsoft AD がない場合は、Active Directory Connector (AD Connector) を設定する必要があります。1 つの Active Directory サーバーを使用してユーザーを認証できます。Active Directory 統合の詳細については、AWS Directory Service 管理ガイドを参照してください。

クライアント VPN は、AWS Managed Microsoft AD または AD Connector で有効になっている場合、多要素認証 (MFA) をサポートします。MFA が有効になっている場合、クライアントはクライアント VPN エンドポイントに接続するときにユーザー名、パスワード、および MFA コードを入力する必要があります。MFA を有効にする詳細については、AWS Directory Service 管理ガイドの「AWS Managed Microsoft AD の多要素認証を有効にするには」および「AD Connector の多要素認証を有効にするには」を参照してください。

Active Directory でユーザーとグループを設定するためのクォータとルールについては、「ユーザーとグループのクォータ (p. 74)」を参照してください。

相互認証

相互認証では、クライアント VPN は証明書を使用してクライアントとサーバー間の認証を実行します。証明書とは、認証機関 (CA) によって発行された識別用デジタル形式です。クライアントがクライアント VPN エンドポイントに接続を試みると、サーバーはクライアント証明書を使用してクライアントを認証します。サーバー証明書とキー、および少なくとも 1 つのクライアント証明書とキーを作成する必要があります。

サーバー証明書は AWS Certificate Manager (ACM) にアップロードし、クライアント VPN エンドポイントの作成時に指定する必要があります。サーバー証明書を ACM にアップロードするときは、認証局 (CA) も指定します。クライアント証明書を ACM にアップロードする必要があるのは、クライアント証明書の CA がサーバー証明書の CA と異なる場合だけです。ACM の詳細については、AWS Certificate Manager ユーザーガイドを参照してください。

クライアント VPN エンドポイントに接続するクライアントごとに、個別のクライアント証明書とキーを作成できます。これにより、ユーザーが組織を離れた場合に、特定のクライアント証明書を取り消すことができます。この場合、クライアント VPN エンドポイントを作成するときに、クライアント証明書がサーバー証明書と同じ CA によって発行されていれば、クライアント証明書のサーバー証明書 ARN を指定できます。

クライアント VPN エンドポイントは、1024 ビットおよび 2048 ビットの RSA キーサイズのみサポートしています。

Linux/macOS

次の手順では、OpenVPN easy-rsa を使用してサーバーとクライアントの証明書とキーを生成してから、そのサーバーの証明書とキーを ACM にアップロードします。詳細については、「Easy-RSA 3 Quickstart README」を参照してください。

サーバーとクライアントの証明書とキーを生成し、それらを ACM にアップロードするには

1. OpenVPN easy-rsa リポジトリのクローンをローカルコンピュータに作成して、`easy-rsa/easyrsa3` フォルダに移動します。

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

```
$ cd easy-rsa/easyrsa3
```

2. 新しい PKI 環境を初期化します。

```
$ ./easyrsa init-pki
```

3. 新しい認証局 (CA) を構築するには、このコマンドを実行し、プロンプトに従います。

```
$ ./easyrsa build-ca nopass
```

4. サーバー証明書とキーを生成します。

```
$ ./easyrsa build-server-full server nopass
```

5. クライアント証明書とキーを生成します。

   クライアント証明書とクライアントプライベートキーは、クライアントを設定するときに必要になるため、必ず保存してください。

```
$ ./easyrsa build-client-full client1.domain.tld nopass
```

必要に応じて、クライアント証明書とキーを必要とするクライアント (エンドユーザー) ごとにこの手順を繰り返すことができます。

6. サーバー証明書とキー、およびクライアント証明書とキーをカスタムフォルダにコピーしてから、カスタムフォルダに移動します。

   証明書とキーをコピーする前に、mkdir コマンドを使用してカスタムフォルダを作成します。次の例では、ホームディレクトリにカスタムフォルダを作成します。

   ```
   $ mkdir ~/custom_folder/
   $ cp pki/ca.crt ~/custom_folder/
   $ cp pki/issued/server.crt ~/custom_folder/
   $ cp pki/private/server.key ~/custom_folder/
   $ cp pki/issued/client1.domain.tld.crt ~/custom_folder
   $ cp pki/private/client1.domain.tld.key ~/custom_folder/
   $ cd ~/custom_folder/
   ```

7. サーバー証明書とキー、およびクライアント証明書とキーを ACM にアップロードします。必ずクライアント VPN エンドポイントを作成する予定のリージョンと同じリージョンにアップロードしてください。以下のコマンドは、AWS CLI を使用して証明書をアップロードします。代わりに ACM コンソールを使用して証明書をアップロードするには、AWS Certificate Manager ユーザーガイドの「証明書のインポート」を参照してください。

   ```
   $ aws acm import-certificate --certificate fileb://server.crt --private-key
    fileb://server.key --certificate-chain fileb://ca.crt
   ```

   ```
   $ aws acm import-certificate --certificate fileb://client1.domain.tld.crt --
   private-key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
   ```

   クライアント証明書の CA がサーバー証明書の CA と異なる場合を除いて、クライアント証明書を ACM にアップロードする必要はありません。上記の手順では、サーバー証明書と同じ CA がクライアント証明書にも使用されます。ただしここでは、完全なプロセスを示すために、クライアント証明書をアップロードする手順も含めています。

Windows

次の手順では、OpenVPN ソフトウェアをインストールし、それを使用してサーバーとクライアントの証明書およびキーを生成します。

サーバーとクライアントの証明書とキーを生成し、それらを ACM にアップロードするには

1. OpenVPN コミュニティのダウンロードページを開き、お使いの Windows のバージョン用の Windows インストーラをダウンロードして、インストーラーを実行します。
2. EasyRSA リリースページを開き、お使いの Windows のバージョン用の ZIP ファイルをダウンロードします。ZIP ファイルを解凍し、EasyRSA フォルダを \Program Files\OpenVPN フォルダにコピーします。
3. 管理者としてコマンドプロンプトを開き、\Program Files\OpenVPN\EasyRSA ディレクトリに移動し、次のコマンドを実行して EasyRSA 3 シェルを開きます。

   ```
   C:\Program Files\OpenVPN\EasyRSA> EasyRSA-Start
   ```

4. 新しい PKI 環境を初期化します。

   ```
   # ./easyrsa init-pki
   ```

5. 新しい認証局 (CA) を構築するには、このコマンドを実行し、プロンプトに従います。

```
# ./easyrsa build-ca nopass
```

6. サーバー証明書とキーを生成します。

```
# ./easyrsa build-server-full server nopass
```

7. クライアント証明書とキーを生成します。

```
# ./easyrsa build-client-full client1.domain.tld nopass
```

必要に応じて、クライアント証明書とキーを必要とするクライアント (エンドユーザー) ごとにこの手順を繰り返すことができます。

8. EasyRSA 3 シェルを終了します。

```
# exit
```

9. サーバー証明書とキー、およびクライアント証明書とキーをカスタムフォルダにコピーしてから、カスタムフォルダに移動します。

証明書とキーをコピーする前に、mkdir コマンドを使用してカスタムフォルダを作成します。以下の例では、C:\ ドライブにカスタムフォルダを作成します。

```
C:\Program Files\OpenVPN\EasyRSA> mkdir C:\custom_folder
C:\Program Files\OpenVPN\EasyRSA> copy pki\ca.crt C:\custom_folder
C:\Program Files\OpenVPN\EasyRSA> copy pki\issued\server.crt C:\custom_folder
C:\Program Files\OpenVPN\EasyRSA> copy pki\private\server.key C:\custom_folder
C:\Program Files\OpenVPN\EasyRSA> copy pki\issued\client1.domain.tld.crt C:
\custom_folder
C:\Program Files\OpenVPN\EasyRSA> copy pki\private\client1.domain.tld.key C:
\custom_folder
C:\Program Files\OpenVPN\EasyRSA> cd C:\custom_folder
```

10. サーバー証明書とキー、およびクライアント証明書とキーを ACM にアップロードします。必ずクライアント VPN エンドポイントを作成する予定のリージョンと同じリージョンにアップロードしてください。以下のコマンドは、AWS CLI を使用して証明書をアップロードします。代わりに ACM コンソールを使用して証明書をアップロードするには、AWS Certificate Manager ユーザーガイドの「証明書のインポート」を参照してください。

```
aws acm import-certificate --certificate fileb://server.crt --private-key fileb://
server.key --certificate-chain fileb://ca.crt
```

```
aws acm import-certificate --certificate fileb://client1.domain.tld.crt --private-
key fileb://client1.domain.tld.key --certificate-chain fileb://ca.crt
```

クライアント証明書の CA がサーバー証明書の CA と異なる場合を除いて、クライアント証明書を ACM にアップロードする必要はありません。上記の手順では、サーバー証明書と同じ CA がクライアント証明書にも使用されます。ただしここでは、完全なプロセスを示すために、クライアント証明書をアップロードする手順も含めています。

シングルサインオン (SAML 2.0 ベースのフェデレーション認証)

AWS Client VPN はクライアント VPN エンドポイントに対して、Security Assertion Markup Language 2.0 (SAML 2.0) を使用して ID フェデレーションをサポートしています。SAML 2.0 をサポートする ID プロバイダー (IdP) を使用して、一元化されたユーザー ID を作成できます。その後、SAML ベースのフェデレー

ション認証が使用されるようにクライアント VPN エンドポイントを設定し、IdP に関連付けることができます。その後、ユーザーは、一元化された認証情報を使用してクライアント VPN エンドポイントに接続します。

SAML ベースの IdP をクライアント VPN エンドポイントに使用するには、次の操作を行う必要があります。

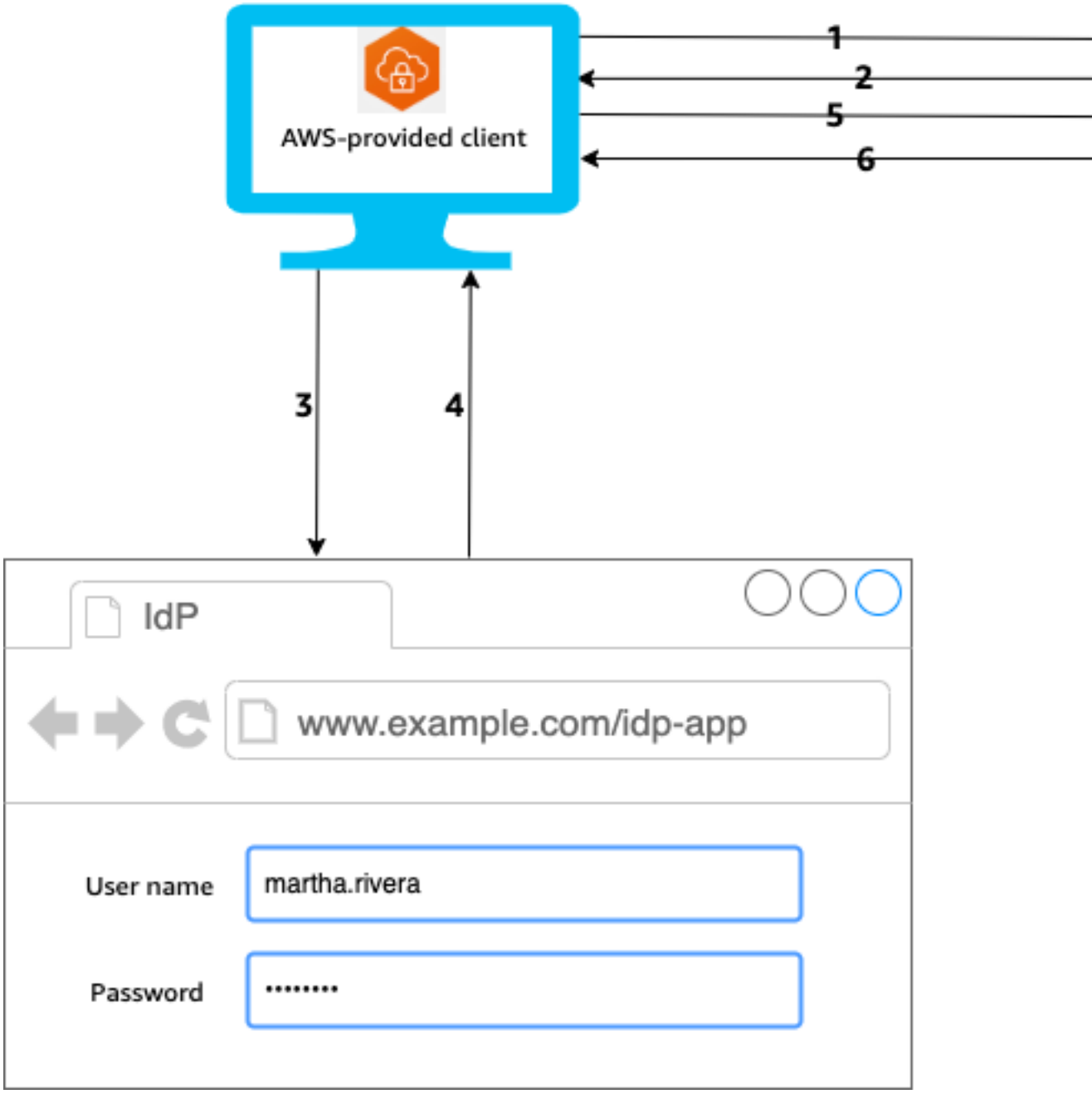
1. AWS Client VPN と連携するには、選択した IdP で SAML ベースのアプリを作成するか、既存のアプリを使用します。
2. との信頼関係を確立するために IdP を設定しますAWS リソースについては、「SAML ベースの IdP 設定リソース (p. 12)」を参照してください。
3. IdP で、組織を IdP として定義するフェデレーションメタデータドキュメントを生成し、ダウンロードします。この署名付き XML ドキュメントは、AWS と IdP の間の信頼関係を確立するために使用されます。
4. クライアント VPN エンドポイントと同じ AWS アカウントに IAM SAML ID プロバイダーを作成します。IAM SAML ID プロバイダーは、IdP によって生成されたメタデータドキュメントを使用して、組織の IdP と AWS の信頼関係を定義します。詳細については、IAM ユーザーガイドの「SAML ID プロバイダーの作成」を参照してください。後で IdP のアプリ設定を更新する場合は、新しいメタデータドキュメントを生成し、IAM SAML ID プロバイダーを更新します。

   Note

   IAM SAML ID プロバイダーを使用するために IAM ロールを作成する必要はありません。
5. クライアント VPN エンドポイントを作成します。認証タイプとしてフェデレーション認証を指定し、作成した IAM SAML ID プロバイダーを指定します。詳細については、「」を参照してくださいクライアント VPN エンドポイントを作成する (p. 41)
6. クライアント設定ファイルを (p. 45)エクスポートし、ユーザーに配布します。AWS が提供するクライアントの最新バージョンをダウンロードし、これを使用して設定ファイルをロードして、クライアント VPN エンドポイントに接続するようにユーザーに指示します。または、クライアント VPN エンドポイントのセルフサービスポータルを有効にした場合は、セルフサービスポータルにアクセスして設定ファイルと AWS が提供するクライアントを取得するようにユーザーに指示します。詳細については、「」を参照してくださいセルフサービスポータルにアクセスする (p. 47)

認証ワークフロー

次の図に、SAML ベースのフェデレーション認証を使用するクライアント VPN エンドポイントの認証ワークフローの概要を示します。クライアント VPN エンドポイントを作成および設定するときは、IAM SAML ID プロバイダーを指定します。



1. ユーザーは AWS が提供するクライアントをデバイスで開き、クライアント VPN エンドポイントへの接続を開始します。
2. クライアント VPN エンドポイントは、IAM SAML ID プロバイダーで提供された情報に基づいて IdP URL と認証リクエストをクライアントに送信します。
3. AWS が提供するクライアントは、ユーザーのデバイスで新しいブラウザウィンドウを開きます。ブラウザは IdP にリクエストを送信し、ログインページを表示します。
4. ユーザーがログインページに認証情報を入力し、IdP は署名付き SAML アサーションをクライアントに返します。
5. AWS が提供するクライアントは、クライアント VPN エンドポイントに SAML アサーションを送信します。

6. クライアント VPN エンドポイントはアサーションを検証し、ユーザーへのアクセスを許可または拒否します。

SAML ベースのフェデレーション認証の要件と考慮事項

SAML ベースのフェデレーション認証の要件と考慮事項を次に示します。

- SAML ベースの IdP でユーザーとグループを設定するためのクォータとルールについては、「ユーザーとグループのクォータ (p. 74)」を参照してください。
- SAML 応答は署名済みで、暗号化されていない必要があります。
- SAML 応答でサポートされる最大サイズは 128 KB です。
- AWS Client VPN では署名付き認証リクエストが提供されません。
- SAML シングルログアウトはサポートされていません。ユーザーは、AWS が提供するクライアントから切断してログアウトすることも、接続を終了 (p. 57)することもできます。
- 1 つのクライアント VPN エンドポイントでサポートされるのは、単一の IdP のみです。
- IdP で有効になっている場合は Multi-Factor Authentication (MFA) がサポートされます。
- ユーザーは AWS が提供するクライアントを使用して、クライアント VPN エンドポイントに接続する必要があります。バージョン 1.2.0 以降を使用する必要があります。詳細については、「AWS が提供するクライアントを使用して接続する」「を参照してください。
- IdP 認証は、Apple Safari、Google Chrome、Microsoft Edge、Mozilla Firefox の各ブラウザでサポートされています。
- AWS が提供するクライアントは、SAML 応答用にユーザーのデバイス上の TCP ポート 35001 を予約します。
- 正しくない URL または悪意のある URL で IAM SAML ID プロバイダーのメタデータドキュメントが更新されると、ユーザーの認証の問題が発生したり、フィッシング攻撃につながる可能性があります。このため、IAM SAML ID プロバイダーに対して行われる更新は、AWS CloudTrail を使用してモニタリングすることをお勧めします。詳細については、IAM ユーザーガイドの「AWS CloudTrail を使用した IAM および AWS STS 呼び出しのログ記録」を参照してください。
- AWS Client VPN は、HTTP リダイレクトバインディングを介して IdP に AuthN リクエストを送信します。このため、HTTP リダイレクトバインディングが IdP でサポートされ、IdP のメタデータドキュメントに存在する必要があります。
- SAML アサーションでは、`NameID` 属性に E メールアドレス形式を使用する必要があります。

SAML ベースの IdP 設定リソース

次の表に、AWS Client VPN での使用がテストされている SAML ベースの IdP と、IdP の設定に役立つリソースを示します。

IdP	リソース
Okta	SAML を使用した AWS Client VPN ユーザーの認証
Microsoft Azure Active Directory (Azure AD)	詳細については、Microsoft のドキュメントウェブサイトの「チュートリアル: Azure Active Directory シングルサインオン (SSO) と AWS ClientVPN との統合」を参照してください。

アプリを作成するためのサービスプロバイダー情報

上の表に記載されていない IdP を使用して SAML ベースのアプリを作成するには、次の情報を使用して AWS Client VPN サービスプロバイダー情報を設定します。

- Assertion Consumer Service (ACS) URL: `http://127.0.0.1:35001`
- Audience URI: `urn:amazon:webservices:clientvpn`

以下の属性は必須です:

属性	説明
`NameID`	ユーザーの E メールアドレス。
`FirstName`	ユーザーの名。
`LastName`	ユーザーの姓。
`memberOf`	ユーザーが属するグループ (複数も可)。

属性は大文字と小文字が区別され、指定されたとおりに設定する必要があります。

セルフサービスポータルのサポート

クライアント VPN エンドポイントでセルフサービスポータルを有効にした場合、ユーザーは SAML ベースの IdP 認証情報を使用してポータルにログインします。

IdP が複数の Assertion Consumer Service (ACS) URL をサポートしている場合は、次の ACS URL をアプリに追加します。

```
https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

GovCloud リージョンで Client VPN エンドポイントを使用している場合は、代わりに次の ACS URL を使用します。同じ IDP アプリを使用して標準リージョンと GovCloud リージョンの両方で認証する場合は、両方の URL を追加できます。

```
https://gov.self-service.clientvpn.amazonaws.com/api/auth/sso/saml
```

IdP が複数の ACS URL をサポートしていない場合は、以下を実行します。

1. IdP に追加の SAML ベースのアプリを作成し、次の ACS URL を指定します。

   ```
   https://self-service.clientvpn.amazonaws.com/api/auth/sso/saml
   ```

2. フェデレーションメタデータドキュメントを生成し、ダウンロードします。
3. クライアント VPN エンドポイントと同じ AWS アカウントに IAM SAML ID プロバイダーを作成します。詳細については、IAM ユーザーガイドの「SAML ID プロバイダーの作成」を参照してください。

   Note

   メインアプリ用に作成 (p. 9)したプロバイダーに加えて、この IAM SAML ID プロバイダーを作成します。
4. クライアント VPN エンドポイントを作成し (p. 41)、作成した IAM SAML ID プロバイダーを両方指定します。

Authorization

クライアント VPN では 2 種類の認証がサポートされています。セキュリティグループとネットワークベースの認証 (認証ルールを使用) です。

セキュリティグループ

クライアント VPN エンドポイントを作成するときに、特定の VPC からセキュリティグループを指定して、クライアント VPN エンドポイントに適用できます。サブネットをクライアント VPN エンドポイントに関連付けると、VPC のデフォルトセキュリティグループが自動的に適用されます。クライアント VPN エンドポイントを作成した後で、セキュリティグループを変更できます。詳細については、「」を参照してくださいセキュリティグループをターゲットネットワークに適用する (p. 50) セキュリティグループはクライアント VPN ネットワークインターフェイスに関連付けられます。

アプリケーションのセキュリティグループにルールを追加して、関連付けに適用されたセキュリティグループからのトラフィックを許可することで、クライアント VPN ユーザーが VPC 内のアプリケーションにアクセスできるようにすることができます。

クライアント VPN エンドポイントセキュリティグループからのトラフィックを許可するルールを追加するには

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、[Security Groups] を選択します。
3. リソースまたはアプリケーションに関連付けられているセキュリティグループを選択し、[アクション]、[インバウンドルールの編集] の順に選択します。
4. [Add rule] を選択します。
5. [Type] で、[All traffic] を選択します。または、特定のタイプのトラフィック (SSH など) へのアクセスを制限することもできます。

   [Source (ソース)] に、クライアント VPN エンドポイントのターゲットネットワーク (サブネット) に関連付けられているセキュリティグループの ID を指定します。
6. [Save Rules (ルールの保存)] を選択します。

逆に、関連付けに適用されたセキュリティグループを指定しないか、クライアント VPN エンドポイントセキュリティグループを参照するルールを削除することで、クライアント VPN ユーザーのアクセスを制限できます。必要なセキュリティグループルールは、設定する VPN アクセスの種類によっても異なる場合があります。詳細については、「」を参照してくださいシナリオと例 (p. 23)

VPC セキュリティグループの詳細については、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。

ネットワークベースの承認

ネットワークベースの承認は承認ルールを使用して実装されます。アクセスを有効にするネットワークごとに、アクセス権を持つユーザーを制限する承認ルールを設定する必要があります。指定のネットワークに対して、アクセスを許可する Active Directory グループまたは SAML ベースの IdP グループを構成します。指定されたグループに属するユーザーのみが、指定されたネットワークにアクセスできます。Active Directory または SAML ベースのフェデレーション認証を使用していない場合、またはすべてのユーザーにアクセスを許可したい場合は、すべてのクライアントにアクセスを許可するルールを指定できます。詳細については、「」を参照してください承認ルール (p. 51)

接続承認

クライアント VPN エンドポイントのクライアント接続ハンドラーを設定できます。ハンドラーを使用すると、デバイス、ユーザー、および接続属性に基づいて、新しい接続を許可するカスタムロジックを実行できます。クライアント接続ハンドラーは、クライアント VPN サービスがデバイスとユーザーを認証した後に実行されます。

クライアント VPN エンドポイントのクライアント接続ハンドラーを設定するには、デバイス、ユーザー、および接続属性を入力として受け取り、新しい接続を許可または拒否する決定をクライアント VPN サービスに返す AWS Lambda 関数を作成します。クライアント VPN エンドポイントで Lambda 関数を指定します。デバイスがクライアント VPN エンドポイントに接続すると、クライアント VPN サービスはユーザーに代わって Lambda 関数を呼び出します。Lambda 関数によって承認された接続に対して、クライアント VPN エンドポイントへの接続が許可されます。

Note

現在、サポートされているクライアント接続ハンドラーのタイプは Lambda 関数だけです。

要件と考慮事項

クライアント接続ハンドラーの要件と考慮事項を次に示します。

- Lambda 関数の名前は、 `AWSClientVPN-` プレフィックスで始まる必要があります。
- 認定済みの Lambda 関数がサポートされています。
- Lambda 関数は、クライアント VPN エンドポイントと同じ AWS リージョンおよび同じ AWS アカウントに存在する必要があります。
- Lambda 関数は 30 秒後にタイムアウトします。この値は変更できません。
- Lambda 関数は同期的に呼び出されます。これは、デバイスとユーザーの認証後、および承認ルールが評価される前に呼び出されます。
- 新しい接続に対して Lambda 関数が呼び出され、クライアント VPN サービスが関数から期待されるレスポンスを取得しない場合、クライアント VPN サービスは接続要求を拒否します。これは、Lambda 関数がスロットルされた、タイムアウトした、またはその他の予期しないエラーが発生した場合、関数のレスポンスが有効な形式でない場合などに発生します。
- Lambda 関数にプロビジョニングされた同時実行数を設定して、レイテンシーの変動なしに関数をスケーリングできるようにすることをお勧めします。
- Lambda 関数を更新しても、クライアント VPN エンドポイントへの既存の接続は影響を受けません。既存の接続を終了してから、新しい接続を確立するようクライアントに指示できます。詳細については、「」を参照してくださいクライアント接続の終了 (p. 57)
- クライアントが AWS 提供のクライアントを使用してクライアント VPN エンドポイントに接続する場合、Windows ではバージョン 1.2.6 以降、macOS ではバージョン 1.2.4 以降を使用する必要があります。詳細については、「AWS が提供するクライアントを使用して接続する」「を参照してください。

Lambda インターフェイス

Lambda 関数は、クライアント VPN サービスからの入力として、デバイス属性、ユーザー属性、および接続属性を受け取ります。その後、クライアント VPN サービスに接続を許可または拒否するかどうかを決定する必要があります。

リクエストスキーマ

Lambda 関数は、次のフィールドを含む JSON BLOB を入力として受け取ります。

```
{
    "connection-id": <connection ID>,
    "endpoint-id": <client VPN endpoint ID>,
    "common-name": <cert-common-name>,
    "username": <user identifier>,
    "platform": <OS platform>,
    "platform-version": <OS version>,
    "public-ip": <public IP address>,
    "client-openvpn-version": <client OpenVPN version>,
```

```
    "groups": <group identifier>,
    "schema-version": "v2"
}
```

- connection-id — クライアント VPN エンドポイントへのクライアント接続の ID。
- endpoint-id — クライアント VPN エンドポイントの ID。
- common-name — デバイス識別子。デバイス用に作成するクライアント証明書では、共通名によってデバイスが一意に識別されます。
- username — ユーザー ID (該当する場合)。Active Directory 認証の場合、これはユーザー名です。SAML ベースのフェデレーション認証の場合、これは NameID です。相互認証の場合、このフィールドは空です。
- platform — クライアントのオペレーティングシステムプラットフォーム。
- platform-version — オペレーティングシステムのバージョン。クライアント VPN サービスは、クライアントがクライアント VPN エンドポイントに接続するとき、およびクライアントが Windows プラットフォームを実行しているときに --push-peer-info ディレクティブが OpenVPN クライアント設定に存在する場合に値を提供します。
- public-ip — 接続デバイスのパブリック IP アドレス。
- client-openvpn-version — クライアントが使用している OpenVPN バージョン。
- groups — グループ ID (該当する場合)。Active Directory 認証の場合、これはActive Directory グループの一覧になります。SAML ベースのフェデレーション認証の場合、これは ID プロバイダー (IdP) グループの一覧になります。相互認証の場合、このフィールドは空です。
- schema-version — スキーマバージョン。デフォルト: v2。

レスポンススキーマ

Lambda 関数は次のフィールドを返す必要があります。

```
{
    "allow": boolean,
    "error-msg-on-denied-connection": "",
    "posture-compliance-statuses": [],
    "schema-version": "v2"
}
```

- allow — 必須。新しい接続を許可または拒否するかどうかを示すブール値 (true | false)。
- error-msg-on-denied-connection — 必須。Lambda 関数によって接続が拒否された場合に、クライアントにステップとガイダンスを提供するために使用できる最大 255 文字の文字列。Lambda 関数の実行中に障害が発生した場合 (スロットリングなどの理由で)、次のデフォルトメッセージがクライアントに返されます。

```
Error establishing connection. Please contact your administrator.
```

- posture-compliance-statuses — 必須。体制評価 (p. 17)に Lambda 関数を使用する場合、これは接続デバイスのステータスのリストです。デバイスの体制評価カテゴリ (compliant、quarantined、unknown など) に従って、ステータス名を定義します。各名前の最大長は 255 文字です。最大 10 個のステータスを指定できます。
- schema-version — 必須。スキーマバージョン。デフォルト: v2。

同じリージョン内の複数のクライアント VPN エンドポイントに対して、同じ Lambda 関数を使用できます。

Lambda 関数の作成の詳細については、AWS Lambda デベロッパーガイドの「AWS Lambda の開始方法」を参照してください。

体制評価のためのクライアント接続ハンドラーの使用

クライアント接続ハンドラーを使用して、クライアント VPN エンドポイントを既存のデバイス管理ソリューションと統合し、接続デバイスの体制コンプライアンスを評価できます。Lambda 関数がデバイス承認ハンドラーとして機能するには、クライアント VPN エンドポイントに相互認証 (p. 7)を使用します 。クライアント VPN エンドポイントに接続するクライアント (デバイス) ごとに、一意のクライアント証明書とキーを作成します。Lambda 関数は、クライアント証明書の一意の共通名 (クライアント VPN サービスから渡される) を使用して、デバイスを識別し、デバイス管理ソリューションから体制コンプライアンスステータスを取得できます。相互認証をユーザーベースの認証と組み合わせることができます。

または、Lambda 関数自体で基本的な体制評価を行うこともできます。たとえば、クライアント VPN サービスによって Lambda 関数に渡される `platform` および `platform-version` フィールドを評価できます。

クライアント接続ハンドラーの有効化

クライアント接続ハンドラーを有効にするには、クライアント VPN エンドポイントを作成または変更し、Lambda 関数の Amazon リソースネーム (ARN) を指定します。詳細については、「クライアント VPN エンドポイントを作成する (p. 41)」および「クライアント VPN エンドポイントを変更する (p. 43)」を参照してください。

サービスにリンクされたロール

AWS Client VPN は、AWSServiceRoleForClientVPNConnections というアカウントに、サービスにリンクされたロールを自動的に作成します。ロールには、クライアント VPN エンドポイントへの接続が行われたときに Lambda 関数を呼び出すアクセス許可があります。詳細については、「」を参照してくださいクライアント VPN のサービスにリンクされたロールの使用 (p. 64)

接続承認失敗のモニタリング

クライアント VPN エンドポイントへの接続の接続承認ステータスを表示できます。詳細については、「」を参照してくださいクライアント接続の表示 (p. 57)

体制評価にクライアント接続ハンドラーを使用すると、クライアント VPN エンドポイントに接続するデバイスの体制コンプライアンスステータスを接続ログに表示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接続ログ (p. 20)

デバイスが接続承認に失敗した場合、接続ログの `connection-attempt-failure-reason` フィールドから次の失敗理由のいずれかが返されます。

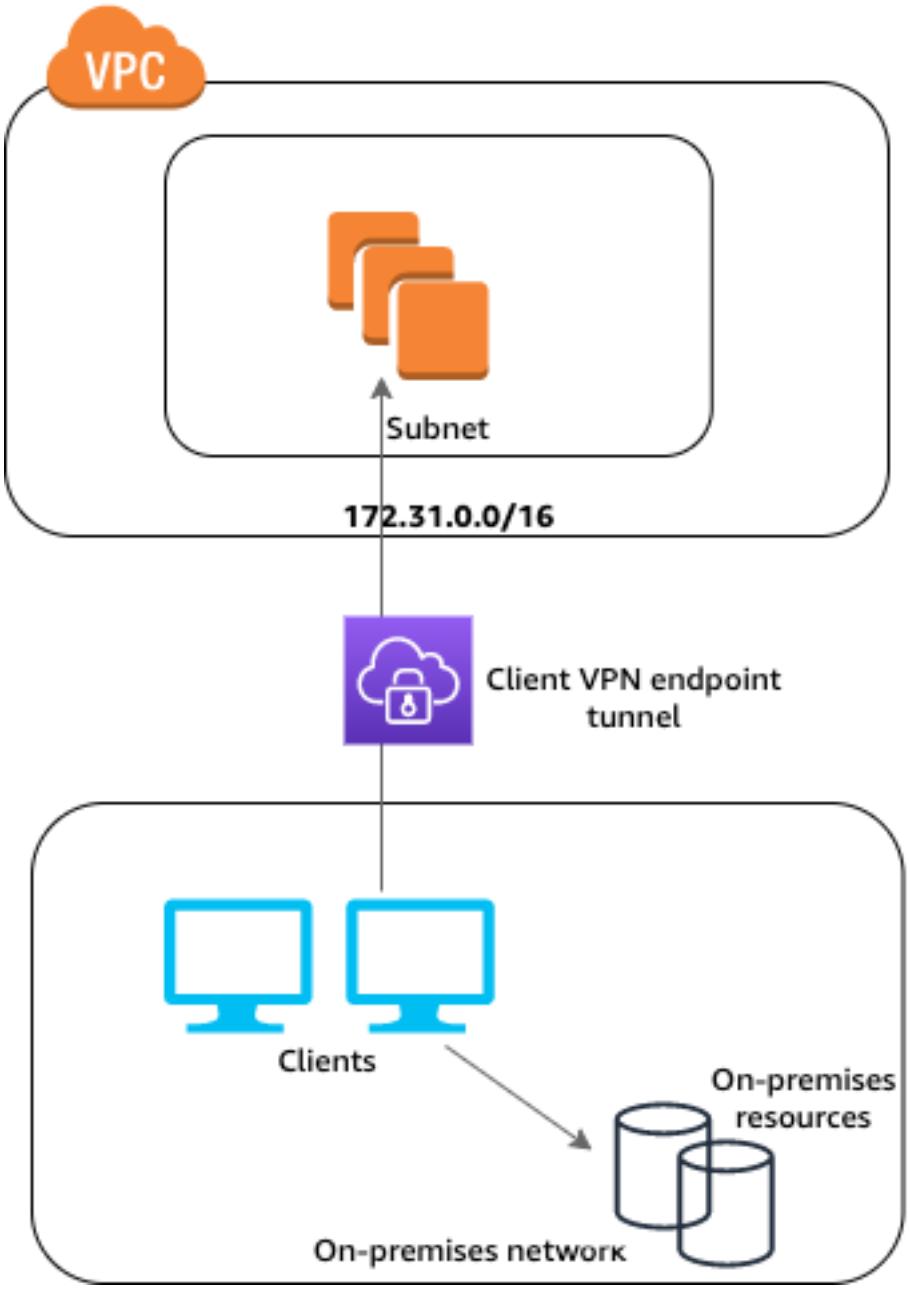
- `client-connect-failed` — Lambda 関数によって接続が確立されませんでした。
- `client-connect-handler-timed-out` — Lambda 関数がタイムアウトしました。
- `client-connect-handler-other-execution-error` — Lambda 関数で予期しないエラーが発生しました。
- `client-connect-handler-throttled` — Lambda 関数がスロットルされました。
- `client-connect-handler-invalid-response` — Lambda 関数が無効なレスポンスを返しました。
- `client-connect-handler-service-error` — 接続試行中にサービス側のエラーが発生しました。

AWS クライアント VPN エンドポイントの分割トンネル

デフォルトでは、クライアント VPN エンドポイントがある場合、クライアントからのすべてのトラフィックはクライアント VPN トンネル経由でルーティングされます。クライアント VPN エンドポイントで分割トンネルを有効にすると、クライアント VPN エンドポイントルートテーブル (p. 53)上のルートがクライアント VPN エンドポイントに接続されているデバイスにプッシュされます。これにより、クライアント VPN エンドポイントルートテーブルからのルートと一致するネットワークへの送信先を持つトラフィックだけがクライアント VPN トンネル経由でルーティングされます。

すべてのユーザートラフィックがクライアント VPN エンドポイントを通過しないようにする場合は、分割トンネルクライアント VPN エンドポイントを使用できます。

次の例では、クライアント VPN エンドポイントで分割トンネルが有効になっています。VPC (`172.31.0.0/16`) 宛てのトラフィックのみがクライアント VPN トンネル経由でルーティングされます。オンプレミスリソース宛てのトラフィックは、クライアント VPN トンネル経由でルーティングされません。



分割トンネルの利点

クライアント VPN エンドポイントの分割トンネルには、次の利点があります。

- AWS 宛てのトラフィックだけが VPN トンネルを通過できるようにすることで、クライアントからのトラフィックのルーティングを最適化できます。
- AWS からの送信トラフィックの量を減らして、データ転送コストを削減できます。

ルーティングに関する考慮事項

クライアント VPN エンドポイントで分割トンネルを有効にすると、VPN が確立された場合に、クライアント VPN ルートテーブル内のすべてのルートがクライアントルートテーブルに追加されます。この操作は、デフォルトのエンドポイントオペレーションとは異なります。デフォルトのクライアント VPN エンドポイントオペレーションでは、クライアントルートテーブルがエントリ 0.0.0.0/0 で上書きされ、すべてのトラフィックが VPN 経由でルーティングされます。

分割トンネルの有効化

新規または既存のクライアント VPN エンドポイントで分割トンネルを有効にできます。詳細については、以下のトピックを参照してください。

- クライアント VPN エンドポイントを作成する (p. 41)
- クライアント VPN エンドポイントを変更する (p. 43)

接続ログ

接続ログは、クライアント VPN エンドポイントの接続ログをキャプチャできる AWS Client VPN の機能です。

接続ログには、接続ログエントリが含まれます。各接続ログエントリには、クライアント (エンドユーザー) が接続するタイミング、接続を試行するタイミング、クライアント VPN エンドポイントから切断するタイミングなどの接続イベントに関する情報が含まれます。この情報を使用してフォレンジックを実行したり、クライアント VPN エンドポイントがどのように使用されているかを分析したり、接続の問題をデバッグしたりできます。

接続ログは、AWS クライアント VPN が使用可能なすべてのリージョンで使用できます。接続ログは、アカウントの CloudWatch Logs ロググループに発行されます。

接続ログエントリ

接続ログエントリは、キーと値のペアの JSON 形式の BLOB です。次に、接続ログエントリの例を示します。

```
{
    "connection-log-type": "connection-attempt",
    "connection-attempt-status": "successful",
    "connection-reset-status": "NA",
    "connection-attempt-failure-reason": "NA",
    "connection-id": "cvpn-connection-abc123abc123abc12",
    "client-vpn-endpoint-id": "cvpn-endpoint-aaa111bbb222ccc33",
    "transport-protocol": "udp",
    "connection-start-time": "2020-03-26 20:37:15",
    "connection-last-update-time": "2020-03-26 20:37:15",
    "client-ip": "10.0.1.2",
    "common-name": "client1",
    "device-type": "mac",
    "device-ip": "98.247.202.82",
    "port": "50096",
    "ingress-bytes": "0",
    "egress-bytes": "0",
    "ingress-packets": "0",
    "egress-packets": "0",
    "connection-end-time": "NA"
}
```

接続ログエントリには、次のキーが含まれます。

- `connection-log-type` — 接続ログエントリのタイプ (`connection-attempt` または `connection-reset`)。
- `connection-attempt-status` — 接続リクエストのステータス (`successful`、`failed`、`waiting-for-assertion`、または `NA`)。
- `connection-reset-status` — 接続リセットイベントのステータス (`NA` または `assertion-received`)。
- `connection-attempt-failure-reason` — 接続エラーの理由 (該当する場合)。
- `connection-id` — 接続の ID。
- `client-vpn-endpoint-id` — 接続が行われたクライアント VPN エンドポイントの ID。
- `transport-protocol` — 接続に使用されたトランスポートプロトコル。
- `connection-start-time` — 接続の開始時刻。
- `connection-last-update-time` — 接続の最終更新時刻。この値は、ログ内で定期的に更新されます。
- `client-ip` — クライアントの IP アドレス。クライアント VPN エンドポイントのクライアント IPv4 CIDR 範囲から割り当てられます。
- `common-name` — 証明書ベースの認証に使用される証明書の共通名。
- `device-type` — エンドユーザーが接続に使用するデバイスのタイプ。
- `device-ip` — デバイスのパブリック IP アドレス。
- `port` — 接続のポート番号。
- `ingress-bytes` — 接続の受信 (インバウンド) バイト数。この値は、ログ内で定期的に更新されます。
- `egress-bytes` — 接続の送信 (アウトバウンド) バイト数。この値は、ログ内で定期的に更新されます。
- `ingress-packets` — 接続の受信 (インバウンド) パケット数。この値は、ログ内で定期的に更新されます。
- `egress-packets` — 接続の送信 (アウトバウンド) パケット数。この値は、ログ内で定期的に更新されます。
- `connection-end-time` — 接続の終了時刻。この値は、接続がまだ進行中の場合や接続の試行が失敗した場合は `NA` です。
- `posture-compliance-statuses` — クライアント接続ハンドラー (p. 14)によって返される体制コンプライアンスステータス (該当する場合)。

接続ログの有効化の詳細については、「接続ログの操作 (p. 58)」を参照してください。

クライアント VPN スケーリングに関する考慮事項

クライアント VPN エンドポイントを作成するときは、サポートする予定の同時 VPN 接続の最大数を考慮してください。現在サポートしているクライアントの数と、必要に応じてクライアント VPN エンドポイントが追加需要を満たすことができるかどうかを考慮する必要があります。

以下の要因は、クライアント VPN エンドポイントでサポートできる同時 VPN 接続の最大数に影響します。

クライアント CIDR 範囲のサイズ

クライアント VPN エンドポイントを作成 (p. 41)するときは、クライアント CIDR 範囲を指定する必要があります。これは、/12 と /22 ネットマスクの間の IPv4 CIDR ブロックです。クライアント VPN エンドポイントへのそれぞれの VPN 接続には、クライアント CIDR 範囲から固有の IP アドレスが割り当てられます。クライアント CIDR 範囲内のアドレスの一部は、クライアント VPN エンドポ

イントの可用性モデルをサポートするためにも使用され、クライアントに割り当てることはできません。クライアント VPN エンドポイントの作成後にクライアント CIDR 範囲を変更することはできません。

一般に、クライアント VPN エンドポイントでサポートする予定の IP アドレス (つまり同時接続) の 2 倍の数を含むクライアント CIDR 範囲を指定することをお勧めします。

関連付けられたサブネットの数

サブネットをクライアント VPN エンドポイントに関連付ける (p. 48)と、ユーザーはクライアント VPN エンドポイントへの VPN セッションを確立できるようになります。複数のサブネットを 1 つのクライアント VPN エンドポイントに関連付けると、高可用性を実現し、追加の接続キャパシティを有効にできます。

クライアント VPN エンドポイントのサブネットの関連付けの数に基づく、サポートされる同時 VPN 接続の数を次に示します。

サブネットの関連付け	サポートされる接続数
1	7,000
2	36,500
3	66,500
4	96,500
5	126,000

1 つのアベイラビリティーゾーンの複数のサブネットをクライアント VPN エンドポイントに関連付けることはできません。したがって、サブネットの関連付けの数は、AWS リージョンで使用可能なアベイラビリティーゾーンの数にも依存します。

例えば、クライアント VPN エンドポイントへの 8,000 の VPN 接続をサポートすることが予想される場合は、クライアント CIDR 範囲の最小サイズ `/18` (16,384 IP アドレス) を指定し、少なくとも 2 つのサブネットをクライアント VPN エンドポイントに関連付けます。

クライアント VPN エンドポイントで予想される VPN 接続の数がわからない場合は、`/16` CIDR ブロックのサイズ以上を指定することをお勧めします。

クライアント CIDR 範囲とターゲットネットワークの操作に関する規則と制限の詳細については、「クライアント VPN の制限とルール (p. 3)」を参照してください 。

クライアント VPN エンドポイントのクォータの詳細については、「AWS クライアント VPN クォータ (p. 73)」を参照してください 。

シナリオと例

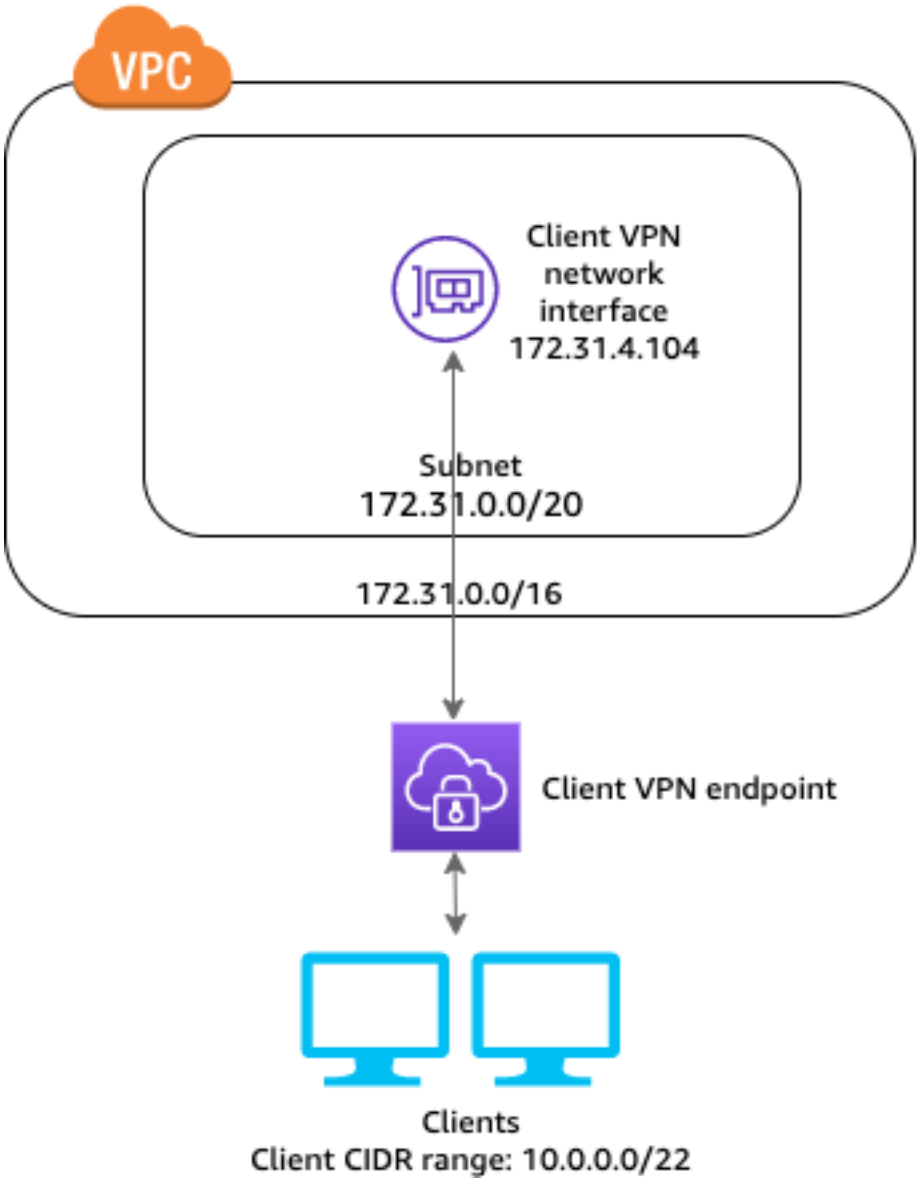
このセクションでは、クライアントの VPN アクセスを作成して設定するための例について説明します。

目次

- VPC へのアクセス (p. 23)
- ピア接続先 VPC へのアクセス (p. 25)
- オンプレミスのネットワークへのアクセス (p. 26)
- インターネットへのアクセス (p. 28)
- クライアント間のアクセス (p. 30)
- ネットワークへのアクセスを制限する (p. 32)

VPC へのアクセス

このシナリオの設定には、単一のターゲット VPC が含まれています。クライアントに単一の VPC 内のリソースへのアクセスのみを許可する必要がある場合は、この設定をお勧めします。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントに関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。詳細については、Amazon VPC ユーザーガイドの「VPC とサブネット」を参照してください。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- クライアント VPN の制限とルール (p. 3) のクライアント VPN エンドポイントのルールと制限を確認します。

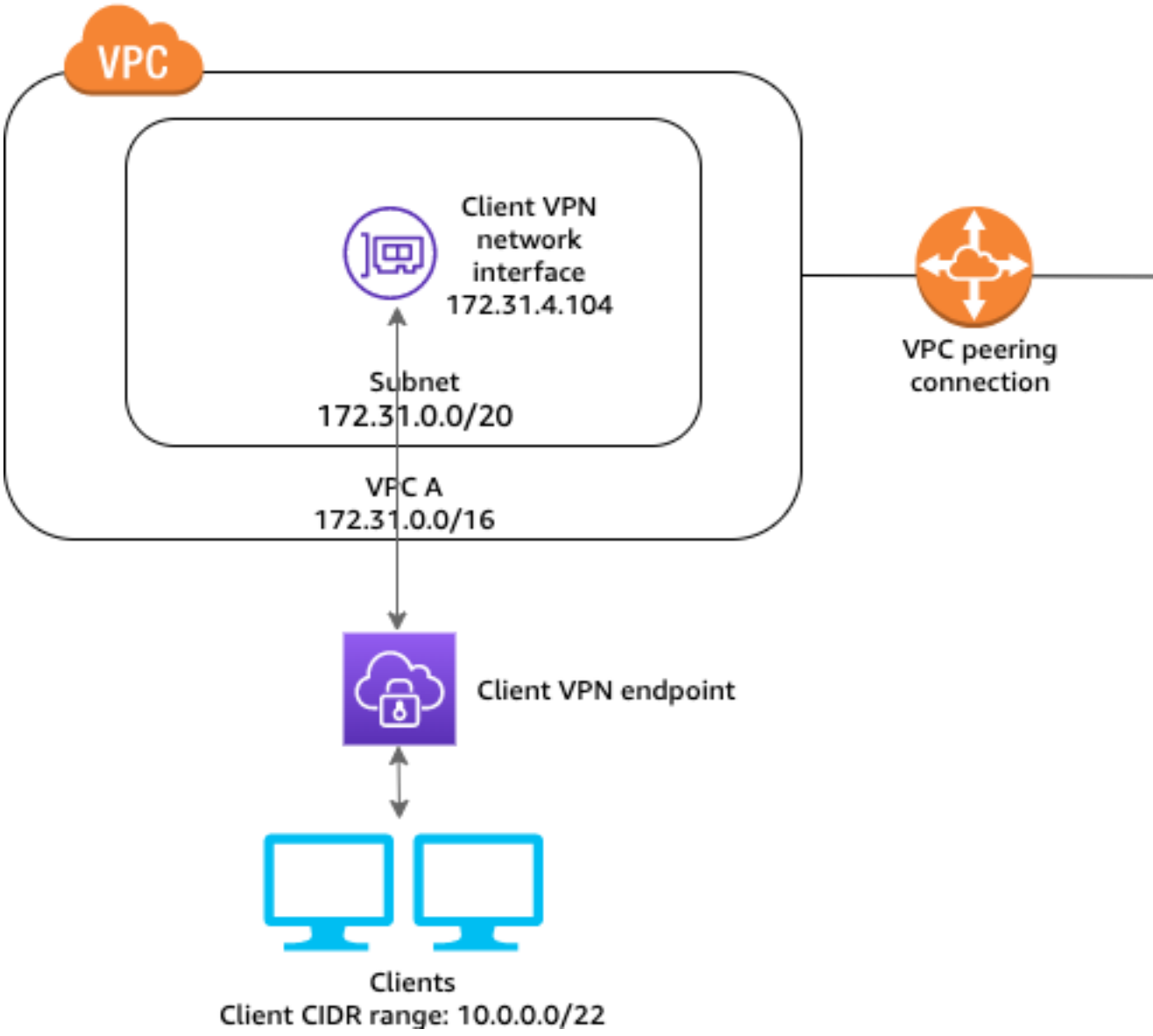
この設定を実装するには

1. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する (p. 41)」で説明されているステップを実行します。

2. サブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける (p. 49)」で説明されているステップを実行し、先ほど確認した VPC およびサブネットを選択します。
3. 許可ルールを追加して、クライアントに VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行し、[Destination network (送信先ネットワーク)] で、VPC の IPv4 CIDR 範囲を入力します。
4. リソースのセキュリティグループにルールを追加して、ステップ 2 でサブネットの関連付けに適用されたセキュリティグループからのトラフィックを許可します。詳細については、「セキュリティグループ (p. 14)」を参照してください。

ピア接続先 VPC へのアクセス

このシナリオの設定には、追加の VPC (VPC B) とピア接続されているターゲット VPC (VPC A) が含まれます。クライアントにターゲット VPC およびそれとピア接続されている他の VPC (VPC B など) にあるリソースへのアクセスを許可する必要がある場合は、この設定をお勧めします。



開始する前に、以下を実行します:

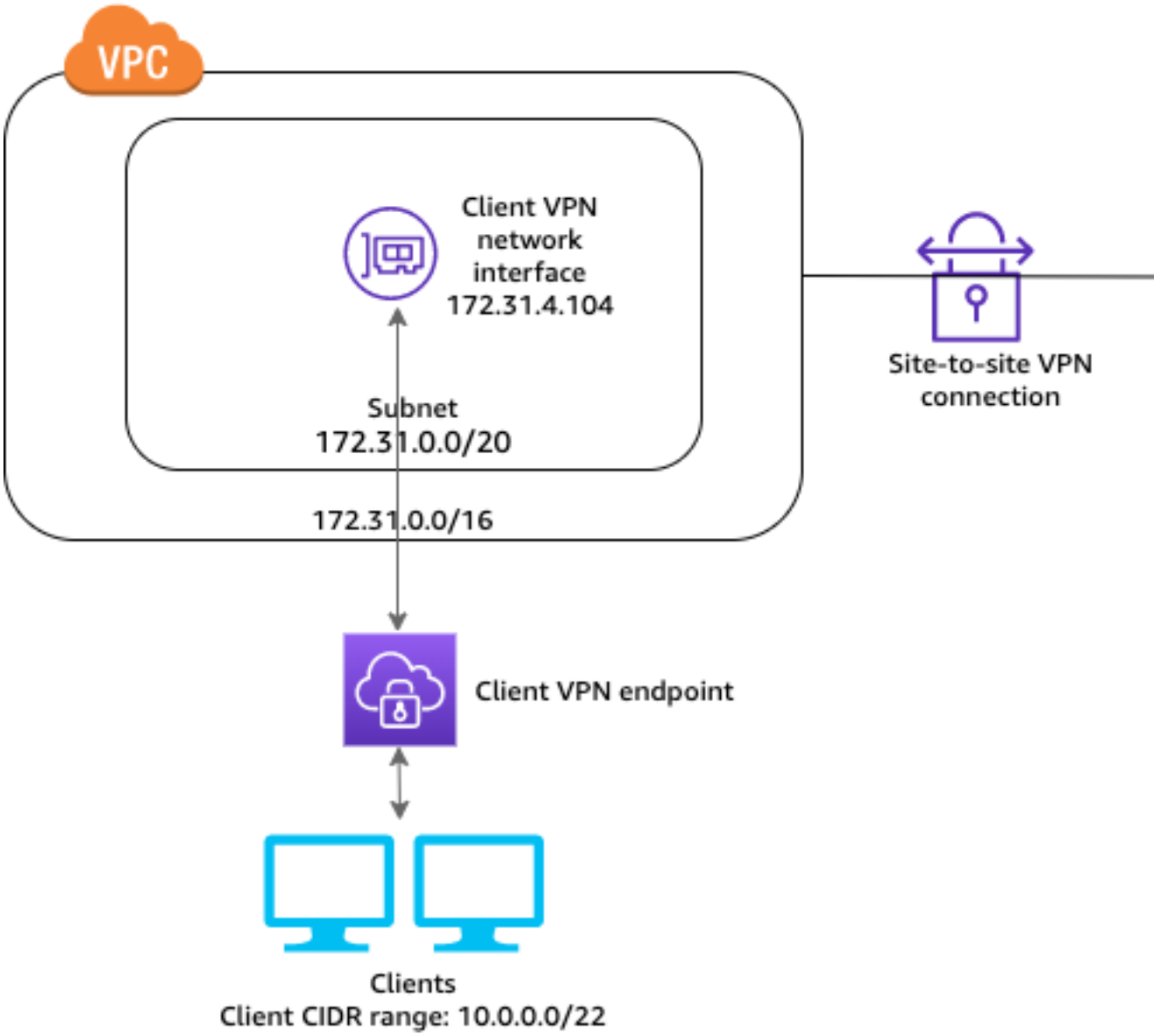
- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントに関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。詳細については、Amazon VPC ユーザーガイドの「VPC とサブネット」を参照してください。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- クライアント VPN の制限とルール (p. 3) のクライアント VPN エンドポイントのルールと制限を確認します。

この設定を実装するには

1. VPC 間の VPC ピア接続を確立します。Amazon VPC ピアリングガイドの「VPC ピア接続の作成と承認」のステップに従います。
2. VPC ピアリング接続をテストします。どちらの VPC のインスタンスも、同じネットワーク内に存在しているかのように相互に通信できることを確認します。ピアリング接続が正常に機能する場合は、次のステップに進みます。
3. ターゲット VPC と同じリージョンに、クライアント VPN エンドポイントを作成します。これは、前の例では VPC A です。「クライアント VPN エンドポイントを作成する (p. 41)」に説明されているステップを実行します。
4. 以前に確認したサブネットを、作成したクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける (p. 49)」で説明されているステップを実行し、サブネットと VPC を選択します。
5. 許可ルールを追加して、クライアントにターゲット VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行し、[Destination network to enable (有効にする送信先ネットワーク)] で、VPC の IPv4 CIDR 範囲を入力します。
6. ピア VPC にトラフィックを送信するルートを追加します。これは、前の例では VPC B です。これを行うには、「エンドポイントルートの作成 (p. 53)」に説明されているステップを実行します。[ルート送信先] で、ピア接続 VPC の IPv4 CIDR 範囲を入力して、[ターゲット VPC サブネット ID] で、クライアント VPN エンドポイントに関連付けたサブネットを選択します。
7. クライアントにピア接続 VPC へのアクセスを許可するための承認ルールを追加します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行します。[Destination network to enable (有効にする送信先ネットワーク)] で、ピア接続先 VPC の IPv4 CIDR 範囲を入力します。
8. VPC A および VPC B のリソースのセキュリティグループにルールを追加して、ステップ 2 でサブネットの関連付けに適用されたセキュリティグループからのトラフィックを許可します。詳細については、「セキュリティグループ (p. 14)」を参照してください。

オンプレミスのネットワークへのアクセス

このシナリオの設定には、オンプレミスネットワークへのアクセスのみが含まれています。クライアントにオンプレミスネットワーク内のリソースへのアクセスのみを許可する必要がある場合は、この設定をお勧めします。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントに関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。詳細については、Amazon VPC ユーザーガイドの「VPC とサブネット」を参照してください。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- クライアント VPN の制限とルール (p. 3) のクライアント VPN エンドポイントのルールと制限を確認します。

この設定を実装するには

1. AWS Site-to-Site VPN 接続を介した VPC と独自のオンプレミスネットワーク間の通信を有効にします。これを行うには、AWS Site-to-Site VPN ユーザーガイドの「開始方法」で説明されているステップを実行します。

Note

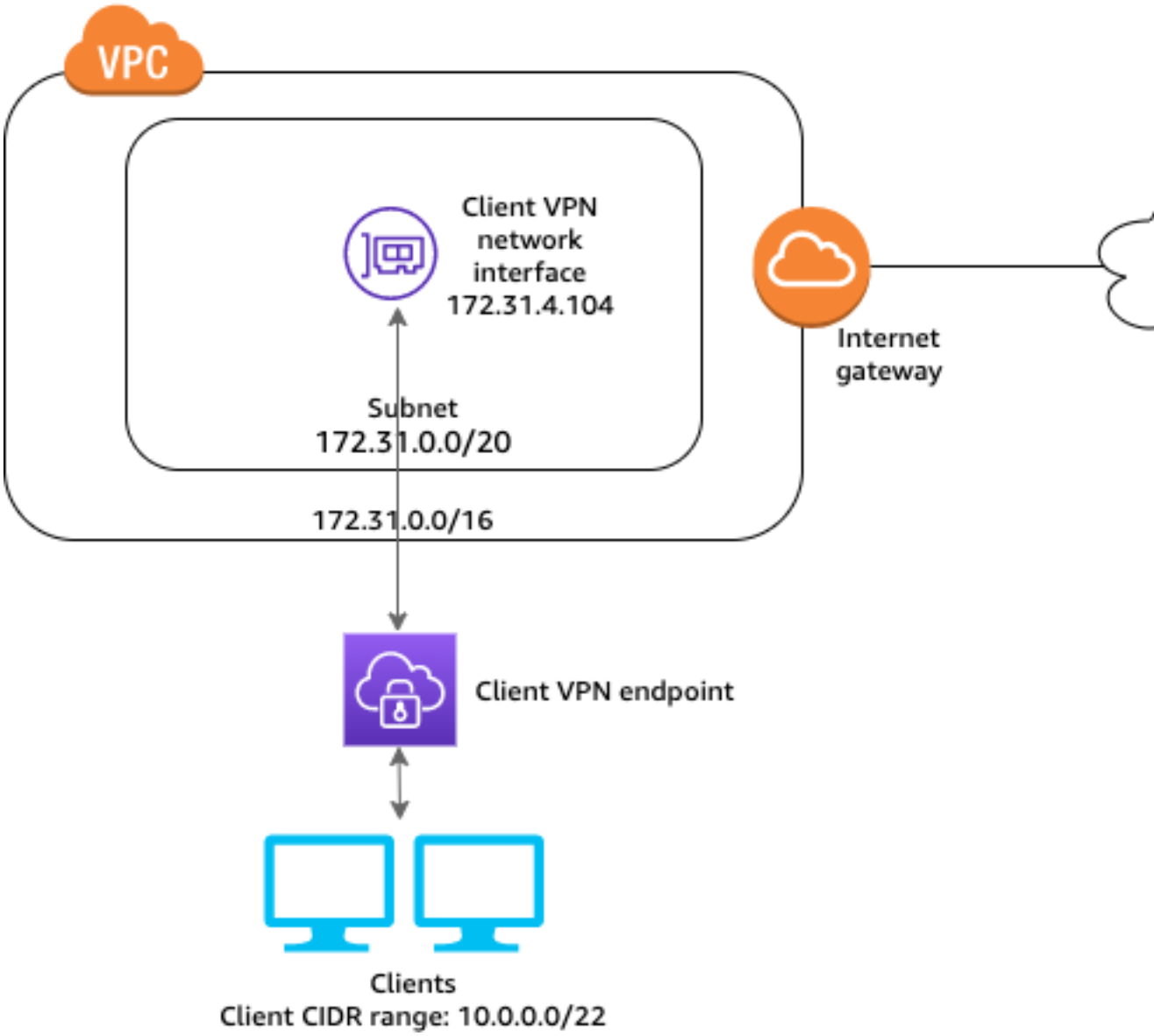
または、VPC とオンプレミスネットワーク間の AWS Direct Connect 接続を使用して、このシナリオを実装することもできます。詳細については、AWS Direct Connect ユーザーガイドを参照してください。

2. 前のステップで作成した AWS Site-to-Site VPN 接続をテストします。これを行うには、AWS Site-to-Site VPN ユーザーガイドの「Site-to-Site VPN 接続のテスト」で説明されているステップを実行します。VPN 接続が正常に機能する場合は、次のステップに進みます。
3. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する (p. 41)」で説明されているステップを実行します。
4. 以前に特定したサブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける (p. 49)」で説明されているステップを実行し、VPC とサブネットを選択します。
5. AWS Site-to-Site VPN 接続へのアクセスを許可するルートを追加します。これを行うには、「エンドポイントルートの作成 (p. 53)」で説明されているステップを実行します。[Route destination] (ルートの送信先) には、AWS Site-to-Site VPN 接続の IPv4 CIDR 範囲を入力し、[Target VPC Subnet ID,] (ターゲット VPC サブネット ID) には、クライアント VPN エンドポイントに関連付けたサブネットを選択します。
6. クライアントに、AWS Site-to-Site VPN 接続へのアクセス権を付与する許可ルールを追加します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行します。[Destination network] (送信先ネットワーク) で、AWS Site-to-Site VPN 接続の IPv4 CIDR 範囲を入力します。

インターネットへのアクセス

このシナリオの設定には、単一のターゲット VPC とインターネットへのアクセスが含まれています。クライアントに単一のターゲット VPC 内のリソースへのアクセスを許可し、インターネットへのアクセスを許可する必要がある場合は、この設定をお勧めします。

クライアント VPN の開始方法 (p. 35) チュートリアルが完了している場合、このシナリオはすでに実装されていることになります。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントに関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。詳細については、Amazon VPC ユーザーガイドの「VPC とサブネット」を参照してください。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- クライアント VPN の制限とルール (p. 3) のクライアント VPN エンドポイントのルールと制限を確認します。

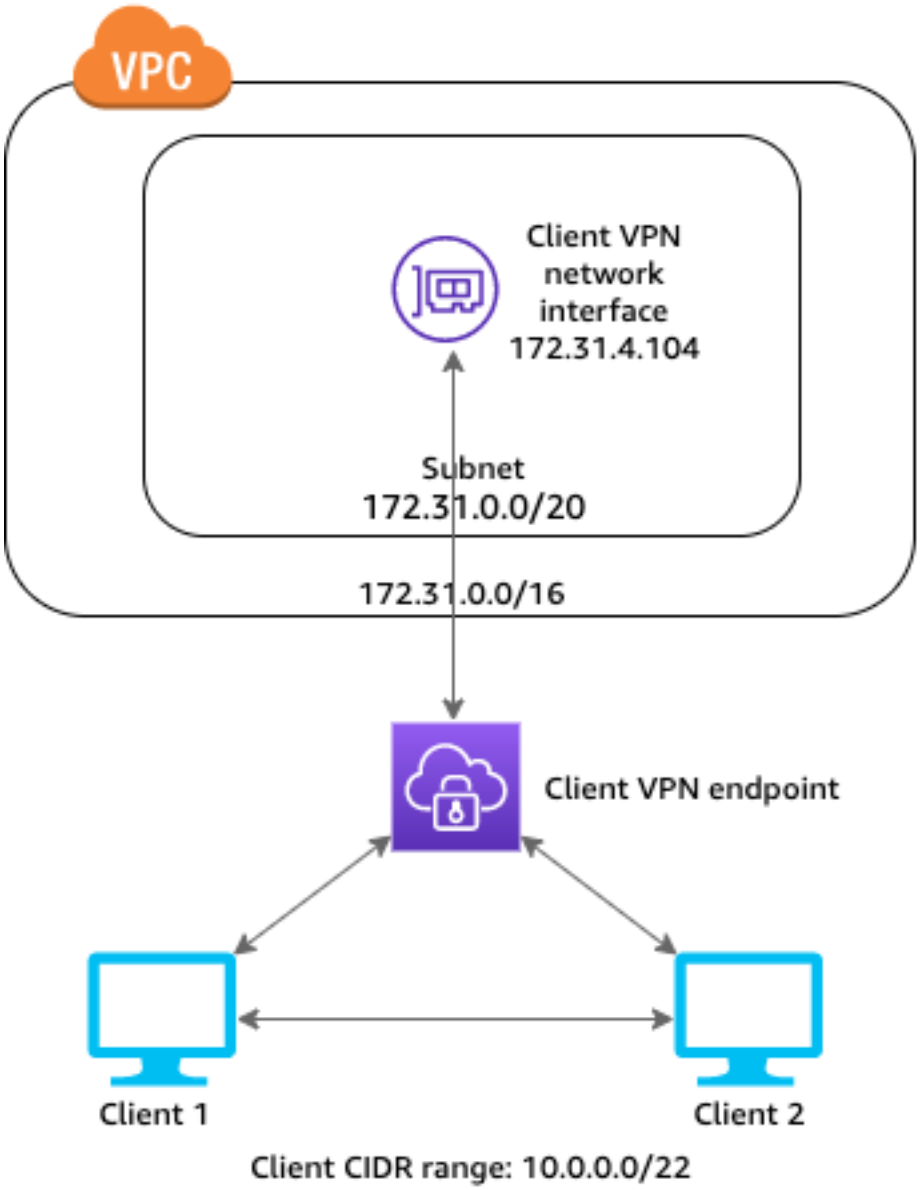
この設定を実装するには

1. クライアント VPN エンドポイントに使用するセキュリティグループで、インターネットとの間の送受信トラフィックが許可されていることを確認します。これを行うには、HTTP および HTTPS トラフィック に対して 0.0.0.0/0 との間のトラフィックを許可するインバウンドルールとアウトバウンドルールを追加します。

2. インターネットゲートウェイを作成して VPC にアタッチします。詳細については、Amazon VPC ユーザーガイドの「インターネットゲートウェイの作成とアタッチ 」を参照してください。
3. インターネットゲートウェイへのルートをそのルートテーブルに追加して、サブネットを公開します。[VPC コンソール] で、[サブネット] を選択し、クライアント VPN エンドポイントに関連付ける予定のサブネットを選択します。[Route Table (ルートテーブル)] を選択し、次にルートテーブル ID を選択します。[アクション] を選択し、[Edit routes (ルートの編集)] を選択して、[Add route (ルートの追加)] を選択します。[送信先] に、`0.0.0.0/0` を入力し、[ターゲット] で、前のステップからインターネットゲートウェイを選択します。
4. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する (p. 41)」で説明されているステップを実行します。
5. 以前に特定したサブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける (p. 49)」で説明されているステップを実行し、VPC とサブネットを選択します。
6. 許可ルールを追加して、クライアントに VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行します。[Destination network to enable (有効にする送信先ネットワーク)] で、VPC の IPv4 CIDR 範囲を入力します。
7. インターネットへのトラフィックを可能にするルートを追加します。これを行うには、「エンドポイントルートの作成 (p. 53)」で説明されているステップを実行します。[Route destination (ルートの送信先)] に `0.0.0.0/0` を入力し、[Target VPC Subnet ID (ターゲット VPC サブネット ID)] でクライアント VPN エンドポイントに関連付けたサブネットを選択してください。
8. 承認ルールを追加して、クライアントにインターネットへのアクセスを許可します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行します。送信先ネットワークで `0.0.0.0/0` を入力します。
9. ステップ 5 のサブネット関連付けのセキュリティグループに、インターネットアクセスを許可するアウトバウンドルールが設定されていることを確認します (宛先は `0.0.0.0/0`)。

クライアント間のアクセス

このシナリオの設定では、クライアントは単一の VPC にアクセスでき、クライアントが相互にトラフィックをルーティングできます。同じクライアント VPN エンドポイントに接続するクライアントも相互に通信する必要がある場合は、この設定をお勧めします。クライアントは、クライアント VPN エンドポイントに接続するときに、クライアントの CIDR 範囲から割り当てられた一意の IP アドレスを使用して相互に通信できます。



開始する前に、以下を実行します:

- 少なくとも 1 つのサブネットを持つ VPC を作成または識別します。クライアント VPN エンドポイントに関連付ける VPC のサブネットを特定し、その IPv4 CIDR 範囲をメモしておきます。詳細については、Amazon VPC ユーザーガイドの「VPC とサブネット」を参照してください。
- VPC CIDR と重複しないクライアント IP アドレスに適切な CIDR 範囲を特定します。
- クライアント VPN の制限とルール (p. 3) のクライアント VPN エンドポイントのルールと制限を確認します。

> **Note**
>
> Active Directory グループまたは SAML ベースの IdP グループを使用するネットワークベースの承認規則は、このシナリオではサポートされません。

この設定を実装するには

1. VPC と同じリージョンにクライアント VPN エンドポイントを作成します。これを行うには、「クライアント VPN エンドポイントを作成する (p. 41)」で説明されているステップを実行します。
2. 以前に特定したサブネットをクライアント VPN エンドポイントに関連付けます。これを行うには、「ターゲットネットワークをクライアント VPN エンドポイントに関連付ける (p. 49)」で説明されているステップを実行し、VPC とサブネットを選択します。
3. ルートテーブルのローカルネットワークにルートを追加します。これを行うには、「エンドポイントルートの作成 (p. 53)」で説明されているステップを実行します。[Route destination (ルート送信先)] に、クライアントの CIDR 範囲を入力し、[Target VPC Subnet ID (ターゲット VPC サブネット ID)] で `local` を指定します。
4. 許可ルールを追加して、クライアントに VPC へのアクセスを提供します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行します。[Destination network to enable (有効にする宛先ネットワーク)] に、VPC の IPv4 CIDR 範囲を入力します。
5. クライアントにクライアントの CIDR 範囲へのアクセスを許可するための承認ルールを追加します。これを行うには、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」で説明されているステップを実行します。[Destination network to enable (有効にする宛先ネットワーク)] に、クライアントの CIDR 範囲を入力します。

ネットワークへのアクセスを制限する

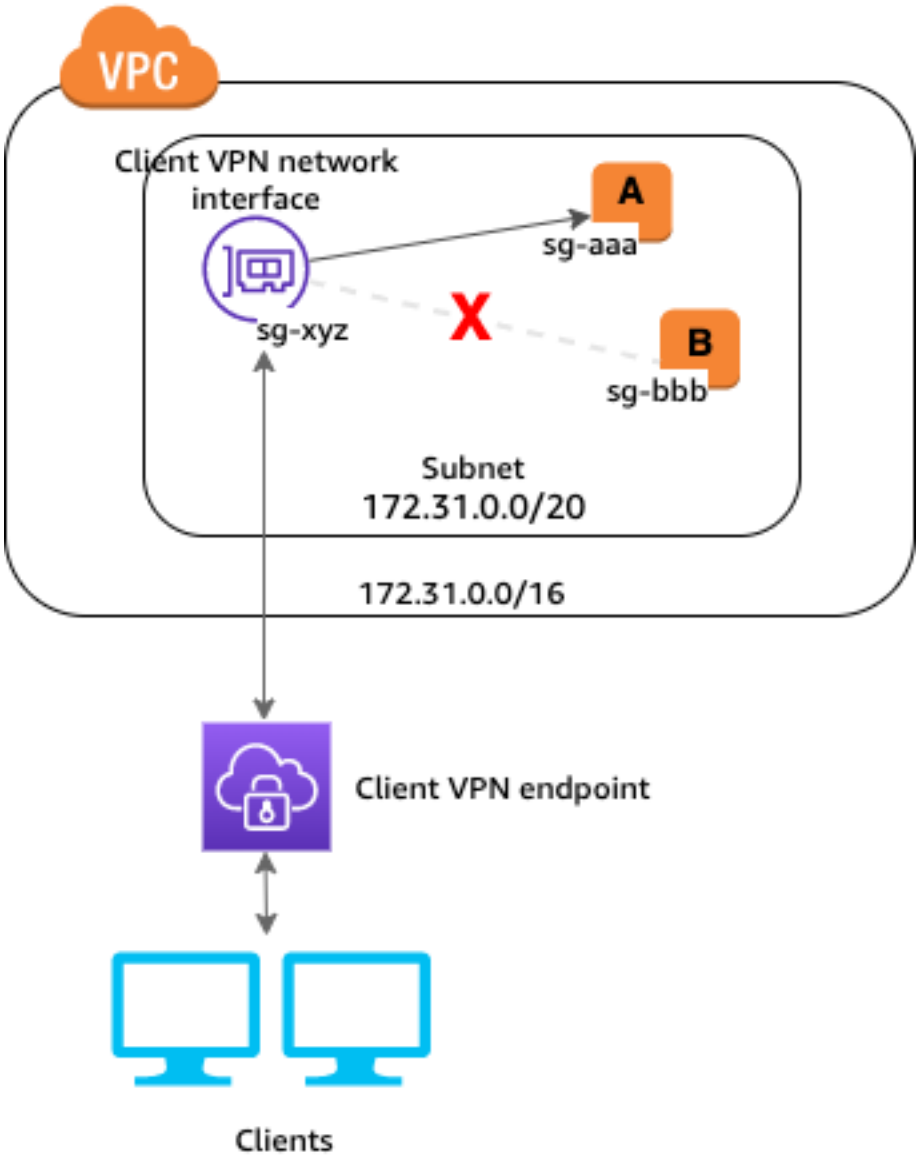
クライアント VPN エンドポイントを設定して、VPC 内の特定のリソースへのアクセスを制限することができます。ユーザーベースの認証の場合、クライアント VPN エンドポイントにアクセスするユーザーグループに基づいて、ネットワークの一部へのアクセスを制限することもできます。

セキュリティグループを使用してアクセスを制限する

ターゲットネットワーク関連付けに適用されたセキュリティグループ (クライアント VPN セキュリティグループ) を参照するセキュリティ グループルールを追加または削除することで、VPC 内の特定のリソースへのアクセスを許可または拒否することができます。この設定は「VPC へのアクセス (p. 23)」で説明されているシナリオに拡張します。この設定は、そのシナリオで設定された認証ルールに加えて適用されます。

特定のリソースへのアクセスを許可するには、リソースが実行されているインスタンスに関連付けられているセキュリティグループを特定します。次に、クライアント VPN セキュリティグループからのトラフィックを許可するルールを作成します。

次の例では、`sg-xyz` はクライアント VPN セキュリティグループです。セキュリティグループ `sg-aaa` はインスタンス A に関連付けられ、セキュリティグループ `sg-bbb` はインスタンス B に関連付けられています。`sg-aaa` からのアクセスを許可するルールを `sg-xyz` に追加すると、クライアントはインスタンス A のリソースにアクセスできます。セキュリティグループ `sg-bbb` には、`sg-xyz` またはクライアント VPN ネットワークインターフェイスからのアクセスを許可するルールがありません。クライアントはインスタンス B のリソースにアクセスできません。



開始する前に、クライアント VPN セキュリティグループが VPC 内の他のリソースに関連付けられているかどうかを確認します。クライアント VPN セキュリティグループを参照するルールを追加または削除すると、他の関連するリソースへのアクセスを許可または拒否することができます。これを防ぐには、クライアント VPN エンドポイント専用として使用するために作成されたセキュリティグループを使用します。

セキュリティグループルールを作成するには

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、[Security Groups] を選択します。
3. リソースが実行されているインスタンスに関連付けられているセキュリティグループを選択します。
4. [アクション]、[Edit inbound rules (インバウンドルールの編集)] の順に選択します。
5. [ルールの追加] を選択し、次の操作を行います。

   - [タイプ] で、[すべてのトラフィック]、または許可する特定のタイプのトラフィックを選択します。
   - [ソース] で [カスタム] を選択し、クライアント VPN セキュリティグループの ID を入力または選択します。

6. [Save Rules (ルールの保存)] を選択します。

特定のリソースへのアクセスを削除するには、リソースが実行されているインスタンスに関連付けられているセキュリティグループを確認します。クライアント VPN セキュリティグループからのトラフィックを許可するルールがある場合は、それを削除します。

セキュリティグループルールを確認するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Security Groups] を選択します。
3. [Inbound Rules (インバウンドルール)] を選択します。
4. ルールのリストを確認します。[ソース] がクライアント VPN セキュリティグループであるルールがある場合は、[Edit Rules (ルールの編集)] を選択し、そのルールの [削除] (x アイコン) を選択します。[Save Rules (ルールの保存)] を選択します。

ユーザーグループに基づいてアクセスを制限する

クライアント VPN エンドポイントがユーザーベースの認証用に設定されている場合は、特定のユーザーグループにネットワークの特定の部分へのアクセスを許可できます。そのためには、以下のステップを完了します。

1. AWS Directory Service または IdP でユーザーとグループを設定します。詳細については、次のトピックを参照してください。
   - Active Directory 認証 (p. 6)
   - SAML ベースのフェデレーション認証の要件と考慮事項 (p. 12)
2. クライアント VPN エンドポイントの許可ルールを作成して、指定したグループがネットワークの全部または一部に アクセスできるようにします。詳細については、「承認ルール (p. 51)」を参照してください。

クライアント VPN エンドポイントが相互認証用に設定されている場合は、ユーザーグループを設定できません。承認ルールを作成するときは、すべてのユーザーにアクセスを許可する必要があります。特定のユーザーグループがネットワークの特定の部分にアクセスできるようにするには、複数の クライアント VPN エンドポイントを作成します。たとえば、ネットワークにアクセスするユーザーグループごとに、次の操作を実行します。

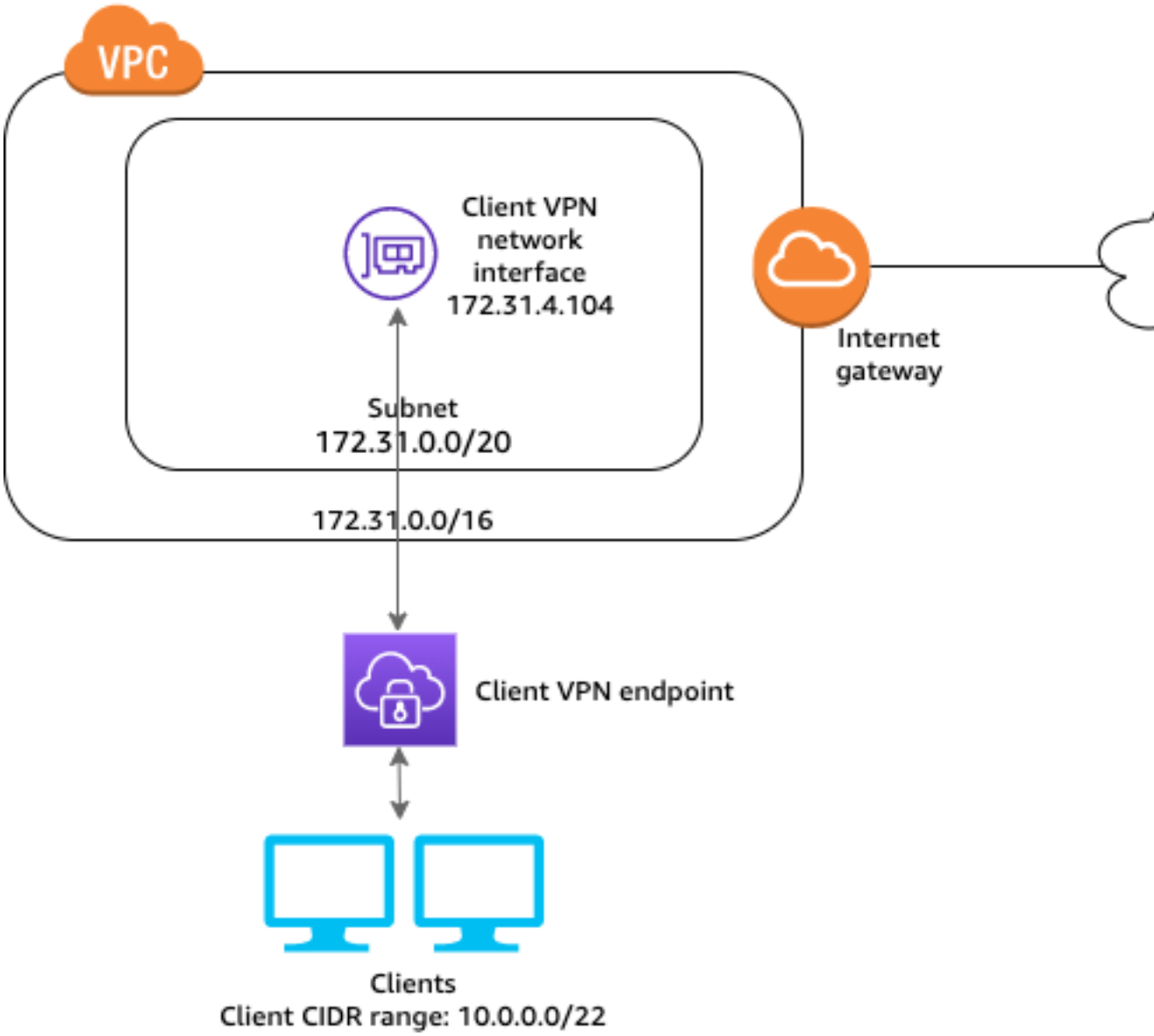
1. そのユーザーグループに対して、サーバー証明書、クライアント証明書、およびキーのセットを作成します。詳細については、「相互認証 (p. 7)」を参照してください。
2. クライアント VPN エンドポイントを作成します。詳細については、「クライアント VPN エンドポイントを作成する (p. 41)」を参照してください。
3. ネットワークのすべてまたは一部へのアクセスを許可する承認ルールを作成します。たとえば、管理者が使用するクライアント VPN エンドポイントの場合、ネットワーク全体へのアクセスを許可する許可ルールを作成できます。詳細については、「クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)」を参照してください。

クライアント VPN の開始方法

以下のタスクは、クライアント VPN に慣れるのに役立ちます。このチュートリアルでは、次の処理を実行するクライアント VPN エンドポイントを作成します。

- すべてのクライアントが 1 つの VPC にアクセスできるようにします。
- すべてのクライアントがインターネットにアクセスできるようにします。
- 相互認証 (p. 7)を使用します。

次の図は、このチュートリアルを完了した後の VPC とクライアント VPN エンドポイントの設定を示しています。



ステップ

- Prerequisites (p. 36)
- ステップ 1: サーバーおよびクライアント証明書とキーの生成 (p. 36)
- ステップ 2: クライアント VPN エンドポイントを作成する (p. 36)
- ステップ 3: クライアントの VPN 接続を有効にする (p. 37)
- ステップ 4: クライアントのネットワークへのアクセスを承認する (p. 38)
- ステップ 5: (オプション) 追加のネットワークへのアクセスを有効にする (p. 38)
- ステップ 6: クライアント VPN エンドポイント設定ファイルをダウンロードする (p. 39)
- ステップ 7: クライアント VPN エンドポイントに接続する (p. 40)

Prerequisites

この入門チュートリアルを完了するには、以下が必要です。

- クライアント VPN エンドポイントを操作するために必要なアクセス許可。
- 少なくとも 1 つのサブネットとインターネットゲートウェイを持つ VPC。サブネットに関連付けられているルートテーブルには、インターネットゲートウェイへのルートが必要です。

ステップ 1: サーバーおよびクライアント証明書とキーの生成

このチュートリアルでは、相互認証が使用されます。相互認証では、クライアント VPN は証明書を使用してクライアントとサーバー間の認証を実行します。

サーバーとクライアント証明書とキーを生成する手順の詳細については、「相互認証 (p. 7)」を参照してください。

ステップ 2: クライアント VPN エンドポイントを作成する

クライアント VPN エンドポイントを作成するとき、VPN 接続を確立するためにクライアントが接続できる VPN 構造を作成します。

クライアント VPN エンドポイ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 [Client VPN Endpoint (クライアント VPN エンドポイント)] を選択し、[Create Client VPN Endpoint (クライアント VPN エンドポイントの作成)] を選択します。
3. (オプション) クライアント VPN エンドポイントの名前と説明を入力します。
4. [Client IPv4 CIDR (クライアント IPv4 CIDR)] に、CIDR 表記で IP アドレス範囲を指定し、そこからクライアント IP アドレスを割り当てます。たとえば、`10.0.0.0/22` と指定します。

   Note

   IP アドレス範囲は、ターゲットネットワークまたはクライアント VPN エンドポイントに関連するいずれかのルートと重複できません。クライアント CIDR は、/12 ~ /22 の範囲のブロックサイズが必要で、VPC CIDR またはルートテーブル内のその他のルートと重複できま

せん。クライアント VPN エンドポイントの作成後にクライアント CIDR を変更することはできません。

5. [Server certificate ARN (サーバー証明書 ARN)] に、サーバーによって使用される TLS 証明書の ARN を指定します。クライアントは、接続先のクライアント VPN エンドポイントを認証するためにサーバー証明書を使用します。

   Note

   サーバー証明書は AWS Certificate Manager (ACM) でプロビジョニングする必要があります。

6. VPN 接続を確立するとき、クライアントを認証するために使用する認証方法を指定します。このチュートリアルでは、[相互認証の使用] を選択し、[クライアント証明書 ARN] で、ステップ 1 (p. 36) で生成したクライアント証明書の ARN を指定します。
7. [クライアント接続の詳細を記録しますか?] で、[いいえ] を選択します。
8. デフォルト設定のまま、[Create Client VPN Endpoint (クライアント VPN エンドポイントの作成)] を選択します。

クライアント VPN エンドポイントの作成時に指定できるその他のオプションの詳細については、「クライアント VPN エンドポイントを作成する (p. 41)」を参照してください。

クライアント VPN エンドポイントを作成すると、その状態は `pending-associate` になります。クライアントは、少なくとも 1 つのターゲットネットワークを関連付けた後でのみ、VPN 接続を確立できます。

ステップ 3: クライアントの VPN 接続を有効にする

クライアントが VPN セッションを確立できるようにするため、ターゲットネットワークをクライアント VPN エンドポイントに関連付ける必要があります。ターゲットネットワークは、VPC のサブネットです。

サブネットをクライアント VPN エンドポイントに関連付けるには

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. サブネットを関連付けるクライアント VPN エンドポイントを選択し、[Associations (関連付け)]、[Associate (関連付ける)] を選択します。
4. [VPC] でサブネットが配置されている VPC を選択します。クライアント VPN エンドポイントの作成時に VPC を指定した場合は、同じ VPC である必要があります。
5. [Subnet to associate (関連付けるサブネット)] でクライアント VPN エンドポイントに関連付けるサブネットを選択します。
6. [Associate] を選択します。

   Note

   承認ルールで許可されている場合、クライアントが VPC のネットワーク全体にアクセスするには、1 つのサブネット関連付けで十分です。アベイラビリティーゾーンの 1 つがダウンした場合の高可用性を維持するために、追加のサブネットを関連付けることができます。

最初のサブネットをクライアント VPN エンドポイントに関連付けると、次の処理が実行されます。

- クライアント VPN エンドポイントの状態が `available` に変わります。これで、クライアントは VPN 接続を確立できるようになりましたが、認証ルールを追加するまで VPC 内のリソースにアクセスすることはできません。

- VPC のローカルルートは、クライアント VPN エンドポイントルートテーブルに自動的に追加されます。
- VPC のデフォルトのセキュリティグループが、サブネットの関連付けに自動的に適用されます。

ステップ 4: クライアントのネットワークへのアクセスを承認する

関連付けられているサブネットが存在する VPC へのアクセスをクライアントに承認するには、承認ルールを作成する必要があります。承認ルールには、どのクライアントが VPC にアクセスできるかを指定します。このチュートリアルでは、すべてのユーザーにアクセス許可を付与します。

ネットワークターゲットに承認ルールを追加するには

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. 承認ルールを追加するクライアント VPN エンドポイントを選択し、[Authorization (承認)]、続いて [Authorize Ingress (受信を承認する)] を選択します。
4. [Destination network to enable (有効にする送信先ネットワーク)] に、アクセスを許可するネットワークの CIDR を入力します。たとえば、VPC 全体へのアクセスを許可するには、VPC の IPv4 CIDR ブロックを指定します。
5. [アクセスを付与する対象] で、[すべてのユーザーにアクセスを許可する] を選択します。
6. [説明] に承認ルールの簡単な説明を入力します。
7. [Add authorization rule (承認ルールを追加する)] を選択します。
8. VPC 内のリソースのセキュリティグループに、サブネット関連付け (p. 37)のセキュリティグループからのアクセスを許可するルールがあることを確認します。これにより、クライアントが VPC 内のリソースにアクセスできるようになります。詳細については、「」を参照してくださいセキュリティグループ (p. 14)

ステップ 5: (オプション) 追加のネットワークへのアクセスを有効にする

AWS サービス、ピア接続 VPC、およびオンプレミスのネットワークなど、VPC に接続されている追加のネットワークへのアクセスを可能できます。追加のネットワークごとにネットワークへのルートを追加し、クライアントアクセスに付与する承認ルールを設定する必要があります。

このチュートリアルでは、インターネットへのルートを追加し (`0.0.0.0/0`)、すべてのユーザーにアクセス許可を付与する承認ルールを追加します。

インターネットへのアクセスを有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. ルートを追加するクライアント VPN エンドポイントを選択し、[Route Table (ルートテーブル)]、次に [Create Route (ルートの作成)] を選択します。
4. [Route destination (ルートの宛先)] に「`0.0.0.0/0`」を入力します。[Target VPC Subnet ID (ターゲット VPC サブネット ID)] には、トラフィックをルーティングするサブネットの ID を指定します。

5. [Create Route (ルートの作成)] を選択します。
6. [Authorization (承認)] を選択し、[Authorize Ingress (入力の承認)] を選択します。
7. [Destination network to enable (有効にする送信先ネットワーク)] で、「`0.0.0.0/0`」と入力し、[すべてのユーザーにアクセスを許可する] を選択します。
8. [Add authorization rule (承認ルールを追加する)] を選択します。
9. トラフィックのルーティングに使用しているサブネットに関連付けられているセキュリティグループで、インターネットとの間の送受信トラフィックが許可されていることを確認します。これを行うには、`0.0.0.0/0` との間のインターネットトラフィックを許可するインバウンドルールとアウトバウンドルールを追加します。

ステップ 6: クライアント VPN エンドポイント設定ファイルをダウンロードする

最後のステップでは、クライアント VPN エンドポイント設定ファイルをダウンロードして準備します。設定ファイルには、クライアント VPN エンドポイントと VPN 接続を確立するために必要な証明書情報が含まれています。VPN 接続を確立するためにクライアント VPN エンドポイントに接続する必要があるクライアントにこのファイルを指定する必要があります。クライアントは、VPN クライアントアプリケーションにこのファイルをアップロードします。

クライアント VPN エンドポイント設定ファイルをダウンロードして準備するには

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント VPN エンドポイントを選択し、[Download Client Configuration (クライアント設定のダウンロード)] を選択します。
4. ステップ 1 (p. 36) で生成されたクライアント証明書とキーを見つけます。クライアント証明書とキーは、クローンされた OpenVPN easy-rsa repo の次の場所にあります。
   - クライアント証明書 — `easy-rsa/easyrsa3/pki/issued/client1.domain.tld.crt`
   - クライアントキー — `easy-rsa/easyrsa3/pki/private/client1.domain.tld.key`
5. 任意のテキストエディタを使用してクライアント VPN エンドポイント設定ファイルを開き、`<cert></cert>` タグ間にクライアント証明書の内容を追加し、`<key></key>` タグ間にプライベートキーの内容を追加します。

```
<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>
```

6. クライアント VPN エンドポイントの DNS 名の先頭にランダムな文字列を追加します。クライアント VPN エンドポイントの DNS 名を指定する行を見つけ、その前にランダム文字列を追加します。フォーマットは *`random_string.displayed_DNS_name`* になります。次に例を示します。
   - 元の DNS 名: `cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`
   - 変更された DNS 名: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.prod.clientvpn.us-west-2.amazonaws.com`

Note

上記のように、設定ファイルでは、Client VPN エンドポイントに指定された DNS 名を常に使用することをお勧めします。DNS 名が解決する IP アドレスは変更される可能性があります。

7. クライアント VPN エンドポイント設定ファイルを保存して閉じます。
8. クライアント VPN エンドポイント設定ファイルをクライアントに配布します。

クライアント VPN エンドポイント設定ファイルの詳細については、「クライアント設定ファイルをエクスポートして設定する (p. 45)」を参照してください。

ステップ 7: クライアント VPN エンドポイントに接続する

AWS が提供するクライアントまたは別の OpenVPN ベースのクライアントアプリケーションを使用して、クライアント VPN エンドポイントに接続できます。詳細については、AWS Client VPN ユーザーガイドをご参照ください。

クライアント VPN の使用

Amazon VPC コンソールまたは AWS CLI を使用して、クライアント VPN を操作できます。

目次

- クライアント VPN エンドポイント (p. 41)
- ターゲットネットワーク (p. 48)
- 承認ルール (p. 51)
- ルート (p. 53)
- クライアント証明書失効リスト (p. 55)
- クライアント接続 (p. 57)
- 接続ログの操作 (p. 58)

クライアント VPN エンドポイント

すべてのクライアント VPN セッションは、クライアント VPN エンドポイントで終了します。クライアント VPN エンドポイントによってすべてのクライアント VPN セッションが管理、制御されるよう設定を行います。

目次

- クライアント VPN エンドポイントを作成する (p. 41)
- クライアント VPN エンドポイントを変更する (p. 43)
- クライアント設定ファイルをエクスポートして設定する (p. 45)
- クライアント VPN エンドポイントを表示する (p. 48)
- クライアント VPN エンドポイントを削除する (p. 48)

クライアント VPN エンドポイントを作成する

クライアントが VPN セッションを確立できるようにするには、クライアント VPN エンドポイントを作成します。

クライアント VPN は、該当するターゲットネットワークがプロビジョニングされているのと同じ AWS アカウントに作成する必要があります。

前提条件

作業を開始する前に、次のことを必ず実行してください。

- クライアント VPN の制限とルール (p. 3) のルールと制限を確認します。
- サーバー証明書を生成し、必要に応じてクライアント証明書を取得します。詳細については、「Authentication (p. 6)」を参照してください。

クライアント VPN エンドポイントを作成するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. (オプション) [説明] に、クライアント VPN エンドポイントの簡単な説明を入力します。
4. [Client IPv4 CIDR (クライアント IPv4 CIDR)] に、CIDR 表記で IP アドレス範囲を指定し、そこからクライアント IP アドレスを割り当てます。
5. [Server certificate ARN (サーバー証明書 ARN)] に、サーバーによって使用される TLS 証明書の ARN を指定します。クライアントは、接続先のクライアント VPN エンドポイントを認証するためにサーバー証明書を使用します。

   Note

   サーバー証明書は AWS Certificate Manager (ACM) でプロビジョニングする必要があります。
6. VPN 接続を確立するとき、クライアントを認証するために使用する認証方法を指定します。認証方法を選択する必要があります。

   - ユーザーベースの認証を使用するには、[ユーザーベースの認証を使用] を選択し、次のいずれかを選択します。
     - Active Directory 認証: Active Directory 認証の場合はこのオプションを選択します。[ディレクトリ ID] には、使用する Active Directory の ID を指定します。
     - フェデレーション認証: SAML ベースのフェデレーション認証の場合は、このオプションを選択します。

       [SAML プロバイダー ARN] には、IAM SAML ID プロバイダーの ARN を指定します。

       (オプション) [Self-service SAML provider ARN (セルフサービス SAML プロバイダー ARN)] で、セルフサービスポータルをサポート (p. 13)するために作成した IAM SAML ID プロバイダーの ARN を指定します (該当する場合)。
   - 相互証明書認証を使用するには、[Use mutual authentication] (相互認証の使用) を選択し、[Client certificate ARN] (クライアント証明書 ARN) で AWS Certificate Manager (ACM) でプロビジョニングしたクライアント証明書の ARN を指定します。

     Note

     クライアント証明書が、サーバー証明書と同じ認証機関 (発行者) によって発行されている場合、引き続きそのクライアント証明書 ARN に対してサーバー証明書 ARN を使用することができます。サーバー証明書と同じ CA を使用して、ユーザーごとに個別のクライアント証明書とキーを生成した場合は、サーバー証明書の ARN を使用できます。
7. Amazon CloudWatch Logs を使用してクライアント接続に関するデータをログに記録するかどうかを指定します。[Do you want to log the details on client connections? (クライアント接続の詳細を記録しますか?)] で、次のいずれかの操作を行います。

   - クライアント接続のログ記録を有効にするには、[はい] を選択します。[CloudWatch Logs ロググループ名] に、使用するロググループの名前を入力します。[CloudWatch Logs ログストリーム名] に、使用するログストリームの名前を入力するか、このオプションを空白のままにしておくとログストリームが自動的に作成されます。
   - クライアント接続のログ記録を無効にするには、[いいえ] を選択します。
8. (オプション) [Client Connect Handler (クライアント接続ハンドラー)] で、[はい] を選択して、クライアント接続ハンドラー (p. 14)でクライアント VPN エンドポイントへの新しい接続を許可または拒否するカスタムコードを実行できるようにします。[Client Connect Handler ARN (クライアント接続ハンドラー ARN)] で、接続を許可または拒否するロジックを含む Lambda 関数の Amazon リソースネーム (ARN) を指定します。
9. (オプション) DNS 解決に使用する DNS サーバーを指定します。カスタム DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] と [DNS Server 2 IP address (DNS サーバー 2 IP アドレス)] に、使用する DNS サーバーの IP アドレスを指定します。VPC DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] または [DNS Server 2

IP address (DNS サーバー 2 IP アドレス)] のいずれかに IP アドレスを指定し、VPC DNS サーバー IP アドレスを追加します。

Note

クライアントが DNS サーバーに到達できることを確認します。

10. (オプション) エンドポイントをスプリットトンネル VPN エンドポイントにするには、[Enable split-tunnel (スプリットトンネルの有効化)] を選択します。

    デフォルトでは、VPN エンドポイントの分割トンネルは無効になっています。

11. (オプション) デフォルトでは、クライアント VPN サーバーは `UDP` 転送プロトコルを使用します。代わりに `TCP` トランスポートプロトコルを使用するには、[Transport Protocol (トランスポートプロトコル)] の [TCP] を選択します。

    Note

    UDP は通常、TCP よりも優れたパフォーマンスが得られます。クライアント VPN エンドポイントを作成した後で、トランスポートプロトコルを変更することはできません。

12. (オプション) [VPC ID] で、クライアント VPN エンドポイントに関連付ける VPC を選択します。[セキュリティグループ ID] で、クライアント VPN エンドポイントに適用する VPC のセキュリティグループを 1 つ以上選択します。
13. (オプション) [VPN port (VPN ポート)] で、VPN ポート番号を選択します。デフォルトは 443 です。
14. (オプション) クライアントのセルフサービスポータルの URL (p. 47) を生成するには、[Enable self-service portal (セルフサービスポータルを有効にする)] を選択します。
15. [クライアント VPN エンドポイントの作成] を選択します。

クライアント VPN エンドポイントを作成したら、次の手順を実行して設定を完了し、クライアントが接続できるようにします。

- クライアント VPN エンドポイントの初期状態は `pending-associate` です。最初のターゲットネットワーク (p. 49)を関連付けて初めて、クライアントがクライアント VPN エンドポイントに接続できるようになります。
- 承認ルール (p. 51)を作成して、ネットワークにアクセスできるクライアントを指定します。
- クライアントに配布するクライアント VPN エンドポイント設定ファイル (p. 45)をダウンロードして準備します。
- AWS 提供のクライアントまたは別の OpenVPN ベースのクライアントアプリケーションを使用して、クライアント VPN エンドポイントに接続するようクライアントに指定します。詳細については、AWS Client VPN ユーザーガイドを参照してください。

クライアント VPN エンドポイントを作成するには (AWS CLI)

create-client-vpn-endpoint コマンドを使用します。

クライアント VPN エンドポイントを変更する

クライアント VPN を作成した後、次の設定を変更できます。

- 説明
- サーバー証明書
- クライアント接続ログオプション
- DNS サーバー
- スプリットトンネルオプション

- VPC とセキュリティグループの関連付け
- VPN ポート番号
- クライアント接続ハンドラーのオプション
- セルフサービスポータルオプション

クライアント VPN エンドポイントの作成後に、クライアントの IPv4 CIDR 範囲、認証オプション、またはトランスポートプロトコルを変更することはできません。

クライアント VPN エンドポイントで次のいずれかのパラメータを変更すると、接続がリセットされます。

- サーバー証明書
- DNS サーバー
- スプリットトンネルオプション (サポートをオンまたはオフ)
- ルート (スプリットトンネルオプションを使用する場合)

- 証明書失効リスト (CRL)
- 承認ルール
- VPN ポート番号

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントを変更できます。

クライアント VPN エンドポイントを変更するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. 変更するクライアント VPN エンドポイントを選択し、[アクション]、[クライアント VPN エンドポイントの変更] の順に選択します。
4. (オプション) [Description] (説明) で、クライアント VPN エンドポイントの簡単な説明を入力します。
5. [Client IPv4 CIDR (クライアント IPv4 CIDR)] に、CIDR 表記で IP アドレス範囲を指定し、そこからクライアント IP アドレスを割り当てます。
6. [Server certificate ARN (サーバー証明書 ARN)] に、サーバーによって使用される TLS 証明書の ARN を指定します。クライアントは、接続先のクライアント VPN エンドポイントを認証するためにサーバー証明書を使用します。

   Note

   サーバー証明書は AWS Certificate Manager (ACM) でプロビジョニングする必要があります。
7. Amazon CloudWatch Logs を使用してクライアント接続に関するデータをログに記録するかどうかを指定します。[Do you want to log the details on client connections? (クライアント接続の詳細を記録しますか?)] で、次のいずれかの操作を行います。

   - クライアント接続のログ記録を有効にするには、[はい] を選択します。[CloudWatch Logs ロググループ名] に、使用するロググループの名前を入力します。[CloudWatch Logs ログストリーム名] に、使用するログストリームの名前を入力するか、このオプションを空白のままにしておくとログストリームが自動的に作成されます。
   - クライアント接続のログ記録を無効にするには、[いいえ] を選択します。
8. [Client Connect Handler] (クライアント接続ハンドラー) で、[Yes] (はい) を選択して、 クライアント接続ハンドラー (p. 14)でクライアント VPN エンドポイントへの新しい接続を許可または拒否するカスタムコードを実行できるようにします。[Client Connect Handler ARN (クライアント接続ハンドラー

ARN)] で、接続を許可または拒否するロジックを含む Lambda 関数の Amazon リソースネーム (ARN) を指定します。

9. DNS 解決に使用する DNS サーバーを指定します。カスタム DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] と [DNS Server 2 IP address (DNS サーバー 2 IP アドレス)] に、使用する DNS サーバーの IP アドレスを指定します。VPC DNS サーバーを使用するには、[DNS Server 1 IP address (DNS サーバー 1 IP アドレス)] または [DNS Server 2 IP address (DNS サーバー 2 IP アドレス)] のいずれかに IP アドレスを指定し、VPC DNS サーバー IP アドレスを追加します。

   Note

   クライアントが DNS サーバーに到達できることを確認します。
10. エンドポイントをスプリットトンネル VPN エンドポイントにするには、[Enable split-tunnel] (スプリットトンネルの有効化) を選択します。

    デフォルトでは、VPN エンドポイントの分割トンネルは無効になっています。
11. ([VPC ID] で、クライアント VPN エンドポイントに関連付ける VPC を選択します。[セキュリティグループ ID] で、クライアント VPN エンドポイントに適用する VPC のセキュリティグループを 1 つ以上選択します。
12. [VPN port] (VPN ポート) で、VPN ポート番号を選択します。デフォルトは 443 です。
13. クライアントのセルフサービスポータルの URL (p. 47) を生成するには、[Enable self-service portal] (セルフサービスポータルを有効にする) を選択します。
14. [クライアント VPN エンドポイントの変更] を選択します。

クライアント VPN エンドポイントを変更するには (AWS CLI)

modify-client-vpn-endpoint コマンドを使用します。

クライアント設定ファイルをエクスポートして設定する

クライアント VPN エンドポイント設定ファイルは、クライアント (ユーザー) がクライアント VPN エンドポイントとの VPN 接続を確立するために使用するファイルです。このファイルをダウンロード (エクスポート) し、VPN へのアクセスを必要とするすべてのクライアントに配布する必要があります。または、クライアント VPN エンドポイントのセルフサービスポータルを有効にした場合、クライアントはポータルにログインして、構成ファイルを自身でダウンロードできます。詳細については、「セルフサービスポータルにアクセスする (p. 47)」を参照してください。

クライアント VPN エンドポイントが相互認証を使用する場合は、ダウンロードする .ovpn 設定ファイルにクライアント証明書とクライアントプライベートキーを追加 (p. 46)する必要があります。お客様が情報を追加した後、クライアントは .ovpn ファイルを OpenVPN クライアントソフトウェアにインポートできます。

Important

クライアント証明書とクライアントプライベートキー情報をファイルに追加しない場合、相互認証を使用して認証するクライアントはクライアント VPN エンドポイントに接続できません。

デフォルトでは、OpenVPN クライアント設定の「-remote-random-hostname」オプションは、ワイルドカード DNS を有効にします。ワイルドカード DNS が有効になっているため、クライアントはエンドポイントの IP アドレスをキャッシュしません。そのため、エンドポイントの DNS 名に ping を実行することはできません。

クライアント VPN エンドポイントが Active Directory 認証を使用しており、クライアント設定ファイルの配布後にディレクトリで Multi-Factor Authentication (MFA) を有効にした場合は、新しいファイルをダウン

ロードしてクライアントに再配布する必要があります。クライアントは、以前の設定ファイルを使用してクライアント VPN エンドポイントに接続することはできません。

クライアント設定ファイルをエクスポートする

コンソールまたは AWS CLI を使用して、クライアント設定をエクスポートできます。

クライアント設定をエクスポートするには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント設定をダウンロードするクライアント VPN エンドポイントを選択し、[クライアント設定のダウンロード] を選択します。

クライアント設定をエクスポートするには (AWS CLI)

export-client-vpn-client-configuration コマンドを使用し、出力ファイル名を指定します。

```
$ aws ec2 export-client-vpn-client-configuration --client-vpn-endpoint-id endpoint_id --
output text>config_filename.ovpn
```

クライアント証明書とキー情報を追加する (相互認証)

クライアント VPN エンドポイントが相互認証を使用する場合は、ダウンロードする .ovpn 設定ファイルにクライアント証明書とクライアントプライベートキーを追加する必要があります。

相互認証を使用する場合は、クライアント証明書を変更できません。

クライアント証明書とキー情報を追加するには (相互認証)

次のオプションの 1 つを使用できます。

(オプション 1) クライアント証明書とキーを、クライアント VPN エンドポイント設定ファイルとともにクライアントに配布します。この場合、設定ファイルで証明書とキーへのパスを指定します。任意のテキストエディタを使用して設定ファイルを開き、以下をファイルの最後に追加します。*/path/* をクライアント証明書とキーの場所に置き換えます (この場所は、エンドポイントに接続しているクライアントから見た相対的な位置です)。

```
cert /path/client1.domain.tld.crt
key /path/client1.domain.tld.key
```

(オプション 2) <cert></cert> タグ間のクライアント証明書の内容と、<key></key> タグ間のプライベートキーの内容を設定ファイルに追加します。このオプションを選択した場合、設定ファイルのみをクライアントに配布します。

クライアント VPN エンドポイントに接続するユーザーごとに個別のクライアント証明書とキーを生成した場合は、ユーザーごとにこのステップを繰り返します。

クライアント証明書とキーを含むクライアント VPN 設定ファイルの形式の例を次に示します。

```
client
dev tun
proto udp
remote asdf.cvpn-endpoint-0011abcabcabcabc1.prod.clientvpn.eu-west-2.amazonaws.com 443
remote-random-hostname
```

```
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
cipher AES-256-GCM
verb 3

<ca>
Contents of CA
</ca>

<cert>
Contents of client certificate (.crt) file
</cert>

<key>
Contents of private key (.key) file
</key>

reneg-sec 0
```

セルフサービスポータルにアクセスする

クライアント VPN エンドポイントでセルフサービスポータルを有効にした場合、セルフサービスポータルの URL をクライアントに提供できます。クライアントは、ウェブブラウザでポータルにアクセスし、ユーザーベースの認証情報を使用してログインできます。ポータルでは、クライアントはクライアント VPN エンドポイント設定ファイルをダウンロードでき、AWS 提供のクライアントの最新バージョンをダウンロードできます。

以下のルールが適用されます。

- セルフサービスポータルは、相互認証を使用して認証するクライアントでは利用できません。
- セルフサービスポータルで利用できる設定ファイルは、Amazon VPC コンソールまたは AWS CLI を使用してエクスポートする設定ファイルと同じです。クライアントへの配布前に設定ファイルをカスタマイズする必要がある場合は、カスタマイズしたファイルを自分自身でクライアントに配布する必要があります。
- クライアント VPN エンドポイントに対してセルフサービスポータルオプションを有効にする必要があります。有効にしないと、クライアントはポータルにアクセスできません。このオプションが有効になっていない場合は、クライアント VPN エンドポイントを変更して有効にすることができます。

セルフサービスポータルオプションを有効にした後、次の URL のいずれかをクライアントに提供します。

- `https://self-service.clientvpn.amazonaws.com/`

  クライアントがこの URL を使用してポータルにアクセスする場合、クライアントは、ログインする前にクライアント VPN エンドポイントの ID を入力する必要があります。
- `https://self-service.clientvpn.amazonaws.com/endpoints/<endpoint-id>`

  上記の URLの *<endpoint-id>* をクライアント VPN エンドポイントの ID (たとえば、`cvpn-endpoint-0123456abcd123456`) に置き換えます。

セルフサービスポータルの URL は、describe-client-vpn-endpoints AWS CLI コマンドの出力にも表示できます。または、URL は Amazon VPC コンソールの [クライアント VPN エンドポイント (Client VPN Endpoints)] ページの [概要] タブに表示されます。

フェデレーション認証で使用するためのセルフサービスポータルの設定の詳細については、「セルフサービスポータルのサポート (p. 13)」を参照してください。

クライアント VPN エンドポイントを表示する

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントに関する情報を表示できます。

コンソールを使用してクライアント VPN エンドポイントを表示するには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. 表示するクライアント VPN エンドポイントを選択します。
4. タブを使って、関連付けられたターゲットネットワークや承認ルール、ルート、クライアント接続を表示します。

   フィルターを使用すると、検索を絞り込むことができます。

AWS CLI を使用してクライアント VPN エンドポイントを表示するには

describe-client-vpn-endpoints コマンドを使用します。

クライアント VPN エンドポイントを削除する

クライアント VPN エンドポイントを削除すると、そのステータスは `deleting` に変わり、クライアントが接続できなくなります。クライアント VPN エンドポイントを削除する前に、関連付けられているすべてのターゲットネットワークの関連付けを解除する必要があります。

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントを削除できます。

クライアント VPN エンドポイントを削除するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. 削除するクライアント VPN エンドポイントを選択し、[アクション]、[クライアント VPN エンドポイントの削除]、[はい、削除します] の順に選択します。

クライアント VPN エンドポイントを削除するには (AWS CLI)

delete-client-vpn-endpoint コマンドを使用します。

ターゲットネットワーク

ターゲットネットワークは、VPC のサブネットです。クライアントがクライアント VPN エンドポイントに接続し、VPN 接続を確立するためには、クライアント VPN エンドポイントに少なくとも 1 つのターゲットネットワークが必要です。

設定できるアクセスの種類 (クライアントからインターネットへのアクセスなど) の詳細については、「シナリオと例 (p. 23)」を参照してください。

目次

- ターゲットネットワークをクライアント VPN エンドポイントに関連付ける (p. 49)

- セキュリティグループをターゲットネットワークに適用する (p. 50)
- ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除する (p. 50)
- ターゲットネットワークの表示 (p. 51)

ターゲットネットワークをクライアント VPN エンドポイントに関連付ける

1 つ以上のターゲットネットワーク (サブネット) をクライアント VPN エンドポイントに関連付けることができます。

以下のルールが適用されます。

- サブネットには、少なくとも /27 ビットマスク (10.0.0.0/27 など) を持つ CIDR ブロックが必要です。サブネットには最低 8 個の利用可能な IP アドレスも必要です。
- サブネットの CIDR ブロックは、クライアント VPN エンドポイントのクライアント CIDR 範囲と重複できません。
- 複数のサブネットをクライアント VPN エンドポイントに関連付ける場合、各サブネットは異なるアベイラビリティーゾーンに存在する必要があります。アベイラビリティーゾーンの冗長性を提供するために、少なくとも 2 つのサブネットを関連付けることをお勧めします。
- クライアント VPN エンドポイントの作成時に VPC を指定した場合、サブネットは同じ VPC 内にある必要があります。VPC をクライアント VPN エンドポイントにまだ関連付けていない場合、任意の VPC 内のサブネットを選択できます。

  それ以降のすべてのサブネットの関連付けは、同じ VPC から行う必要があります。別の VPC からのサブネットを関連付けるには、まずクライアント VPN エンドポイントを変更し、それに関連付けられている VPC を変更する必要があります。詳細については、「クライアント VPN エンドポイントを変更する (p. 43)」を参照してください。

サブネットをクライアント VPN エンドポイントに関連付けると、そのサブネットがプロビジョニングされたところの VPC のローカルルートが自動的にクライアント VPN エンドポイントのルートテーブルに追加されます。

> Note
>
> ターゲットネットワークが関連付けられた後に、アタッチされた VPC に CIDR をさらに追加したり、削除したりする場合は、次のいずれかの操作を実行して、クライアント VPN エンドポイントルートテーブルのローカルルートを更新する必要があります。
>
> - クライアント VPN エンドポイントの関連付けをターゲットネットワークから解除してから、クライアント VPN エンドポイントをターゲットネットワークに関連付けます。
> - クライアント VPN エンドポイントルートテーブルにルートを手動で追加するか、クライアント VPN エンドポイントルートテーブルからルートを削除します。

最初のサブネットをクライアント VPN エンドポイントに関連付けると、クライアント VPN エンドポイントのステータスが `pending-associate` から `available` に変わり、クライアントが VPN 接続を確立できるようになります。

ターゲットネットワークをクライアント VPN エンドポイントに関連付けるには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。

3. ターゲットネットワークを関連付けるクライアント VPN エンドポイントを選択し、[Associations (関連付け)]、続いて [Associate (関連付ける)] をクリックします。
4. [VPC] でサブネットが配置されている VPC を選択します。クライアント VPN エンドポイントの作成時に VPC を指定した場合、または以前のサブネットの関連付けがある場合は、同じ VPC である必要があります。
5. [Subnet to associate (関連付けるサブネット)] でクライアント VPN エンドポイントに関連付けるサブネットを選択します。
6. [Associate] を選択します。

ターゲットネットワークをクライアント VPN エンドポイントに関連付けるには (AWS CLI)

associate-client-vpn-target-network コマンドを使用します。

セキュリティグループをターゲットネットワークに適用する

クライアント VPN エンドポイントを作成するときに、ターゲットネットワークに適用するセキュリティグループを指定できます。1 つ目のターゲットネットワークをクライアント VPN エンドポイントに関連付けると、関連付けられたサブネットが位置している VPC のデフォルトのセキュリティグループが自動的に適用されます。詳細については、「セキュリティグループ (p. 14)」を参照してください。

クライアント VPN エンドポイントのセキュリティグループを変更できます。必要なセキュリティグループルールは、設定する VPN アクセスの種類によって異なります。詳細については、「シナリオと例 (p. 23)」を参照してください。

ターゲットネットワークにセキュリティグループを適用するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. セキュリティグループを適用するクライアント VPN エンドポイントを選択します。
4. [セキュリティグループ] を選択してから、現在のセキュリティグループを選択し、[Apply Security Groups (セキュリティグループを適用する)] を選択します。
5. リストで新しいセキュリティグループを選択し、[Apply Security Groups (セキュリティグループを適用する)] を選択します。

ターゲットネットワークにセキュリティグループを適用するには (AWS CLI)

apply-security-groups-to-client-vpn-target-network コマンドを使用します。

ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除する

すべてのターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除すると、クライアントは VPN 接続を確立できなくなります。サブネットの関連付けを解除した場合は、関連付けを行った際に自動的に作成されたルートが削除されます。

ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. ターゲットネットワークが関連付けられているクライアント VPN エンドポイントを選択し、[Associations (関連付け)] を選択します。
4. 関連付けを解除するターゲットネットワークを選択し、[関連付け解除] 、続いて [はい、関連付けを解除する]を選択します。

ターゲットネットワークとクライアント VPN エンドポイントの関連付けを解除するには (AWS CLI)

disassociate-client-vpn-target-network コマンドを使用します。

ターゲットネットワークの表示

クライアント VPN エンドポイントに関連付けられたターゲットを表示するには、コンソールまたは AWS CLI を使用します。

ターゲットネットワークを表示するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント VPN エンドポイントを選択し、[Associations (関連付け)] を選択します。

AWS CLI を使用してターゲットネットワークを表示するには

describe-client-vpn-target-networks コマンドを使用します。

承認ルール

承認ルールは、ネットワークへのアクセス許可を与えるファイアウォールルールとして機能します。アクセス許可の対象となるネットワークそれぞれに、承認ルールが必要となります。

目次

- クライアント VPN エンドポイントへの承認ルールの追加 (p. 51)
- クライアント VPN エンドポイントから承認ルールを削除する (p. 52)
- 承認ルールの表示 (p. 53)

クライアント VPN エンドポイントへの承認ルールの追加

承認ルールを追加することで、特定のクライアントに対し、特定のネットワークへのアクセス許可を与えます。

コンソールと AWS CLI を使用して、クライアント VPN エンドポイントに承認ルールを追加できます。

クライアント VPN エンドポイントに承認ルールを追加するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。

3. 承認ルールを追加するクライアント VPN エンドポイントを選択し、[Authorization (承認)]、続いて [Authorize ingress (受信を承認する)] を選択します。
4. [Destination network (送信先ネットワーク)] に、ユーザーがアクセスするネットワークの IP アドレス (VPC の CIDR ブロックなど) を CIDR 表記で入力します。
5. 指定したネットワークにアクセスしてもよいクライアントを指定します。[For grant access to (アクセス権の付与対象)] で、以下のいずれかを行います。

   - すべてのクライアントにアクセス許可を与えるには、[Allow access to all users (すべてのユーザーにアクセスを許可する)] を選択します。
   - 特定のクライアントへのアクセスを制限するには、[特定のアクセスグループのユーザーへのアクセスを許可する] を選択し、[アクセスグループ ID] に、アクセス権限を付与するグループの ID を入力します。たとえば、Active Directory グループのセキュリティ識別子 (SID) か、SAML ベースの ID プロバイダー (IdP) で定義されたグループの ID/名前を指定します。
     - (Active Directory) SID を取得するには、たとえば次のように、Microsoft Powershell の Get-ADGroup コマンドレットを使用できます。

       ```
       Get-ADGroup -Filter 'Name -eq "<Name of the AD Group>"'
       ```

       または、[Active Directory Users and Computers (Active Directory ユーザーとコンピュータ)] ツールを開き、グループのプロパティを表示します。続いて、[Attribute Editor (属性エディタ)] タブに移動し、`objectSID` の値を取得します。必要に応じて、まず [View (表示)]、[Advanced Features (高度な機能)] の順に選択して、[Attribute Editor (属性エディタ)] タブを有効にします。
     - (SAML ベースのフェデレーション認証) グループの ID/名前は、SAML アサーションで返されるグループ属性情報と一致する必要があります。
6. [説明] に承認ルールの簡単な説明を入力します。
7. [Add authorization rule (承認ルールを追加する)] を選択します。

クライアント VPN エンドポイントに承認ルールを追加するには (AWS CLI)

authorize-client-vpn-ingress コマンドを使用します。

クライアント VPN エンドポイントから承認ルールを削除する

承認ルールを削除すると、指定のネットワークへのアクセス許可が削除されます。

クライアント VPN エンドポイントから承認ルールを削除するには、コンソールまたは AWS CLI を使用します。

クライアント VPN エンドポイントから承認ルールを削除するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. 承認ルールが追加されているクライアント VPN エンドポイントを選択し、[Authorization (承認)] を選択します。
4. 削除する承認ルールを選択し、[Revoke ingress (受信の取り消し)]、続いて [Revoke ingress (受信を取り消す)] を選択します。

クライアント VPN エンドポイントから承認ルールを削除するには (AWS CLI)

revoke-client-vpn-ingress コマンドを使用します。

承認ルールの表示

特定のクライアント VPN エンドポイントの承認ルールを表示するには、コンソールまたは AWS CLI を使用します。

承認ルールを表示するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. 承認ルールを表示するクライアント VPN エンドポイントを選択し、[Authorization (承認)] を選択します。

承認ルールを表示するには (AWS CLI)

describe-client-vpn-authorization-rules コマンドを使用します。

ルート

各クライアント VPN エンドポイントには、利用可能な送信先ネットワークルートを説明したルートテーブルがあります。ルートテーブルのルートによって、ネットワークトラフィックの振り分け先が決まります。送信先ネットワークにどのクライアントがアクセスできるかを指定するため、各クライアント VPN エンドポイントルートに対して承認ルールを設定する必要があります。

VPC のサブネットをクライアント VPN エンドポイントに関連付けると、クライアント VPN エンドポイントのルートテーブルにその VPC 用のルートが自動的に追加されます。ピア接続 VPC、オンプレミスネットワーク、ローカルネットワーク (クライアントが相互に通信できるようにする場合)、インターネットなど、追加のネットワークへのアクセスを有効にするには、クライアント VPN エンドポイントのルートテーブルにルートを手動で追加する必要があります。

目次

- クライアント VPN エンドポイントの分割トンネルに関する考慮事項 (p. 53)
- エンドポイントルートの作成 (p. 53)
- エンドポイントルートの表示 (p. 54)
- エンドポイントルートの削除 (p. 54)

クライアント VPN エンドポイントの分割トンネルに関する考慮事項

クライアント VPN エンドポイントで分割トンネルを使用する場合、VPN が確立されると、クライアント VPN ルートテーブル内のすべてのルートがクライアントルートテーブルに追加されます。VPN の確立後にルートを追加する場合は、新しいルートがクライアントに送信されるように接続をリセットする必要があります。

クライアント VPN エンドポイントルートテーブルを変更する前に、クライアントデバイスが処理できるルート数を考慮することをお勧めします。

エンドポイントルートの作成

ルートを作成する際、送信先ネットワークへのトラフィックをどのように振り分けるかを指定します。

クライアントがインターネットにアクセスできるようにするには、送信先 `0.0.0.0/0` ルートを追加します。

コンソールと AWS CLI を使用して、クライアント VPN エンドポイントにルートを追加できます。

クライアント VPN エンドポイントルートを作成するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. ルートを追加するクライアント VPN エンドポイントを選択し、[Route Table (ルートテーブル)]、次に [Create Route (ルートの作成)] を選択します。
4. [Route destination (ルートの送信先)] で、送信先ネットワークの IPv4 CIDR 範囲を指定します。以下に例を示します。
   - インターネット接続用のルートを追加するには、「`0.0.0.0/0`」を入力します。
   - ピア接続 VPC 用のルートを追加するには、ピア接続 VPC の IPv4 CIDR 範囲を入力します。
   - オンプレミスネットワーク用のルートを追加するには、AWS Site-to-Site VPN 接続の IPv4 CIDR 範囲を入力します。
   - ローカルネットワークのルートを追加するには、クライアントの CIDR 範囲を入力します。
5. [ターゲット VPC サブネット ID] で、クライアント VPN エンドポイントに関連付けられているサブネットを選択します。

   または、ローカルネットワークのルートを追加する場合は、`local` を選択します。
6. [説明] にルートの簡単な説明を入力します。
7. [Create Route (ルートの作成)] を選択します。

クライアント VPN エンドポイントルートを作成するには (AWS CLI)

create-client-vpn-route コマンドを使用します。

エンドポイントルートの表示

コンソールまたは AWS CLI を使用して、特定のクライアント VPN エンドポイントのルートを表示できます。

クライアント VPN エンドポイントルートを表示するには (コンソール)

1. ナビゲーションペインで、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
2. ルートを表示するクライアント VPN エンドポイントを選択し、[ルートテーブル] を選択します。

クライアント VPN エンドポイントルートを表示するには (AWS CLI)

describe-client-vpn-routes コマンドを使用します。

エンドポイントルートの削除

削除できるのは、手動で追加したルートに限られます。クライアント VPN エンドポイントにサブネットを関連付けた際に自動的に追加されたルートは、削除できません。自動的に追加されたルートを削除するには、その作成のきっかけとなったサブネットのクライアント VPN エンドポイントへの関連付けを解除する必要があります。

コンソールまたは AWS CLI を使用して、クライアント VPN エンドポイントからルートを削除できます。

クライアント VPN エンドポイントルートを削除するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. ルートを削除するクライアント VPN エンドポイントを選択し、[ルートテーブル] を選択します。
4. 削除するルートを選択し、[Delete Route (ルートの削除)]、続いて [Delete Route (ルートを削除する)] を選択します。

クライアント VPN エンドポイントルートを削除するには (AWS CLI)

delete-client-vpn-route コマンドを使用します。

クライアント証明書失効リスト

クライアント証明書失効リストを使用して、特定のクライアント証明書のクライアント VPN エンドポイントへのアクセスを取り消すことができます。

Note

サーバーとクライアント証明書の生成の詳細については、「相互認証 (p. 7)」を参照してください。

クライアント証明書失効リストに追加できるエントリ数の詳細については、「クライアント VPN クォータ (p. 73)」を参照してください。

目次

- クライアント証明書失効リストの生成 (p. 55)
- クライアント証明書失効リストのインポート (p. 56)
- クライアント証明書失効リストのエクスポート (p. 56)

クライアント証明書失効リストの生成

Linux/macOS

次の手順では、クライアント証明書失効リストの生成に OpenVPN の Easy-RSA というコマンドラインユーティリティを使用してください。

OpenVPN Easy-RSA を使ってクライアント証明書失効リストを生成するには

1. ローカルコンピュータに OpenVPN Easy-RSA レポジトリのクローンを作成します。

```
$ git clone https://github.com/OpenVPN/easy-rsa.git
```

2. ローカルリポジトリの `easy-rsa/easyrsa3` フォルダに移動します。

```
$ cd easy-rsa/easyrsa3
```

3. クライアント証明書を取り消し、クライアント失効リストを生成します。

```
$ ./easyrsa revoke client_certificate_name
$ ./easyrsa gen-crl
```

プロンプトが表示されたら、「 yes」と入力します。

Windows

次の手順では、OpenVPN ソフトウェアを使用してクライアント失効リストを生成します。ここでは、OpenVPN ソフトウェアを使用してクライアントとサーバーの証明書およびキーを生成するステップ (p. 7)に従っていることを前提としています。

クライアント証明書失効リストを生成するには

1. コマンドプロンプトを開き、OpenVPN ディレクトリに移動します。

```
C:\> cd \Program Files\OpenVPN\easy-rsa
```

2. vars.bat ファイルを実行します。

```
C:\> vars
```

3. クライアント証明書を取り消し、クライアント失効リストを生成します。

```
C:\> revoke-full client_certificate_name
C:\> more crl.pem
```

クライアント証明書失効リストのインポート

インポートするクライアント証明書失効リストを持っている必要があります。クライアント証明書失効リストの生成の詳細については、「クライアント証明書失効リストの生成 (p. 55)」を参照してください。

クライアント証明書失効リストのインポートには、コンソールと AWS CLI が使用できます。

クライアント証明書失効リストをインポートするには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント証明書失効リストをインポートするクライアント VPN エンドポイントを選択します。
4. [Actions] を選択し、[Import Client Certificate CRL (クライアント証明書 CRL のインポート)] を選択します。
5. [Certificate Revocation List (証明書失効リスト)] で、クライアント証明書失効リストファイルの内容を入力し、[Import CRL (CRL のインポート)] を選択します。

クライアント証明書失効リストをインポートするには (AWS CLI)

import-client-vpn-client-certificate-revocation-list コマンドを使用します。

```
$ aws ec2 import-client-vpn-client-certificate-revocation-list --certificate-revocation-
list file:path_to_CRL_file --client-vpn-endpoint-id endpoint_id --region region
```

クライアント証明書失効リストのエクスポート

クライアント証明書失効リストのエクスポートには、コンソールと AWS CLI が使用できます。

クライアント証明書失効リストをエクスポートするには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント証明書失効リストをエクスポートするクライアント VPN エンドポイントを選択します。
4. [Actions (アクション)]、[Export Client Certificate CRL (クライアント証明書 CRL のエクスポート)]、[Yes, Export (はい、エクスポートします)] の順に選択します。

クライアント証明書失効をエクスポートするには (AWS CLI)

export-client-vpn-client-certificate-revocation-list コマンドを使用します。

クライアント接続

接続とは、クライアントによって確立された VPN セッションを指します。クライアントがクライアント VPN エンドポイントに正常に接続したとき、接続が確立されたことになります。

目次

- クライアント接続の表示 (p. 57)
- クライアント接続の終了 (p. 57)

クライアント接続の表示

コンソールの表示には、コンソールと AWS CLI が使用できます。接続情報には、クライアント CIDR 範囲から割り当てられた IP アドレスが含まれます。

クライアント接続を表示するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント接続を表示するクライアント VPN エンドポイントを選択します。
4. [Connections (接続)] タブを選択します。[Connections (接続)] タブに、すべてのアクティブなクライアント接続と終了されたクライアント接続が一覧表示されます。

クライアント接続を表示するには (AWS CLI)

describe-client-vpn-connections コマンドを使用します。

クライアント接続の終了

クライアント接続を終了すると、VPN セッションが終了します。

クライアント接続の終了には、コンソールと AWS CLI が終了できます。

クライアント接続を終了するには (コンソール)

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、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。

3. クライアントが接続しているクライアント VPN エンドポイントを選択し、[Connections] を選択します。
4. 終了する接続を選択し、 [Terminate Connection (接続の終了)] 、続いて [Terminate Connection (接続の終了)] を選択します。

クライアント接続を終了するには (AWS CLI)

terminate-client-vpn-connections コマンドを使用します。

接続ログの操作

新規または既存のクライアント VPN エンドポイントの接続ログを有効にして、接続ログのキャプチャを開始できます。

開始する前に、アカウントに CloudWatch Logs ロググループが必要です。詳細については、Amazon CloudWatch Logs ユーザーガイドの「ロググループとログストリームを操作する」を参照してください。CloudWatch Logs の使用には料金が適用されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

接続ログを有効にすると、ロググループ内のログストリームの名前を指定できます。ログストリームを指定しない場合、クライアント VPN サービスによって自動的に作成されます。

新しいクライアント VPN エンドポイントの接続ログを有効にする

コンソールまたはコマンドラインを使用して新しいクライアント VPN エンドポイントを作成するときに、接続ログを有効にできます。

コンソールを使用して新しいクライアント VPN エンドポイントの接続ログを有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで [Client VPN Endpoint (クライアント VPN エンドポイント)] を選択し、[Create Client VPN Endpoint (クライアント VPN エンドポイントの作成)] を選択します。
3. [接続ログ] セクションが表示されるまでオプションを完了します。オプションの詳細については、「クライアント VPN エンドポイントを作成する (p. 41)」を参照してください。
4. [クライアント接続の詳細を記録しますか?] で、[はい] を選択します。
5. [CloudWatch Logs ロググループ名] で、CloudWatch Logs ロググループの名前を選択します。
6. (オプション) [CloudWatch Logs ログストリーム名] で、CloudWatch Logs ログストリームの名前を選択します。
7. [クライアント VPN エンドポイントの作成] を選択します。

AWS CLI を使用して新しいクライアント VPN エンドポイントの接続ログを有効にするには

create-client-vpn-endpoint コマンドを使用して、`--connection-log-options` パラメータを指定します。次の例に示すように、接続ログ情報を JSON 形式で指定できます。

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

既存のクライアント VPN エンドポイントの接続ログを有効にする

コンソールまたはコマンドラインを使用して、既存のクライアント VPN エンドポイントの接続ログを有効にできます。

コンソールを使用して既存のクライアント VPN エンドポイントの接続ログを有効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント VPN エンドポイントを選択し、[アクション]、続いて [クライアント VPN エンドポイントの変更] を選択します。
4. [接続ログ] で [はい] を選択し、次の操作を行います。
   - [CloudWatch ロググループ] で、CloudWatch Logs ロググループの名前を選択します。
   - (オプション) [CloudWatch Logs ログストリーム] で、CloudWatch Logs ログストリームの名前を選択します。
5. [クライアント VPN エンドポイントの変更] を選択します。

AWS CLI を使用して既存のクライアント VPN エンドポイントの接続ログを有効にするには

modify-client-vpn-endpoint コマンドを使用して、`--connection-log-options` パラメータを指定します。次の例に示すように、接続ログ情報を JSON 形式で指定できます。

```
{
    "Enabled": true,
    "CloudwatchLogGroup": "ClientVpnConnectionLogs",
    "CloudwatchLogStream": "NewYorkOfficeVPN"
}
```

接続ログの表示

CloudWatch Logs コンソールを使用して、接続ログを表示できます。

コンソールを使用して接続ログを表示するには

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、[ロググループ] を選択し、接続ログを含むロググループを選択します。
3. クライアント VPN エンドポイントのログストリームを選択します。

   Note

   [タイムスタンプ] 列には、接続の時刻ではなく、接続ログが CloudWatch Logs にパブリッシュされた時刻が表示されます。

ログデータの検索の詳細については、Amazon CloudWatch Logs ユーザーガイドの「フィルターパターンを使用したログデータ検索」を参照してください。

接続ログの無効化

コンソールまたはコマンドラインを使用して、クライアント VPN エンドポイントの接続ログを無効にすることができます。接続ログを無効にしても、CloudWatch Logs で既存の接続ログは削除されません。

コンソールを使用して接続ログを無効にするには

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
2. ナビゲーションペインで、[Client VPN Endpoints (クライアント VPN エンドポイント)] を選択します。
3. クライアント VPN エンドポイントを選択し、[アクション]、続いて [クライアント VPN エンドポイントの変更] を選択します。
4. [接続ログ] で [いいえ] を選択します。
5. [クライアント VPN エンドポイントの変更] を選択します。

AWS CLI を使用して接続ログを無効にするには

modify-client-vpn-endpoint コマンドを使用して、`--connection-log-options` パラメータを指定します。`Enabled` が `false` に設定されていることを確認します。

でのセキュリティAWS Client VPN

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負います。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。AWS Client 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 サービスをご覧ください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS のサービスに応じて異なります。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。

このドキュメントは、クライアント VPN を使用する際の責任共有モデルの適用方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するようクライアント VPN を設定する方法を示します。また、クライアント VPN リソースのモニタリングや保護に役立つその他の AWS のサービスを利用する方法についても説明します。

目次

- AWS Client VPN でのデータ保護 (p. 61)
- クライアント VPN の Identity and Access Management (p. 62)
- ログ記録とモニタリング (p. 65)
- AWS Client VPN での耐障害性 (p. 66)
- AWS Client VPN でのインフラストラクチャセキュリティ (p. 66)
- AWS Client VPN のセキュリティのベストプラクティス (p. 66)
- IPv6 に関する考慮事項 (p. 67)

AWS Client VPN でのデータ保護

AWS 責任共有モデルは、AWS Client VPN で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 で Client VPN または他の AWS 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。

転送時の暗号化

AWS Client VPN は、OpenVPN クライアントを使用して、あらゆる場所から安全な TLS 接続を提供します。

インターネットトラフィックのプライバシー

ネットワーク間アクセスの有効化

クライアントが、クライアント VPN エンドポイントを介して VPC および他のネットワークに接続できるようにすることができます。詳細な説明と例については、「シナリオと例 (p. 23)」を参照してください。

ネットワークへのアクセスを制限する

クライアント VPN エンドポイントを設定して、VPC 内の特定のリソースへのアクセスを制限することができます。ユーザーベースの認証の場合、クライアント VPN エンドポイントにアクセスするユーザーグループに基づいて、ネットワークの一部へのアクセスを制限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ネットワークへのアクセスを制限する (p. 32)

クライアントの認証

認証は AWS クラウドへの最初のエントリポイントで実装されます。クライアントがクライアント VPN エンドポイントへの接続を許可されているかどうかを判断するために使用されます。認証が成功すると、クライアントはクライアント VPN エンドポイントに接続して VPN セッションを確立します。認証が失敗すると、接続は拒否され、クライアントは VPN セッションを確立できなくなります。

クライアント VPN では、次のタイプのクライアント認証を使用できます。

- Active Directory 認証 (p. 6) (ユーザーベース)
- 相互認証 (p. 7) (証明書ベース)
- シングルサインオン (SAML ベースのフェデレーション認証) (p. 9) (ユーザーベース)

クライアント VPN の Identity and Access Management

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、変更するためのアクセス許可はありません。IAM ユーザーがクライアント VPN エンドポイント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、IAM ポリシーを作成する必要があります。このポリシーでは、IAM ユーザーに、必要な特定のリソースおよび API アクションを使用するアクセス許可を 付与する必要があります。次に、IAM ユーザーが属する IAM ユーザーまたは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。

たとえば、次のポリシーでは、読み取り専用アクセスを有効にします。ユーザーはクライアント VPN エンドポイントとそのコンポーネントを表示できますが、作成、変更、削除はできません。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeClientVpnRoutes",
                "ec2:DescribeClientVpnAuthorizationRules",
                "ec2:DescribeClientVpnConnections",
                "ec2:DescribeClientVpnTargetNetworks",
                "ec2:DescribeClientVpnEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

リソースレベルのアクセス許可を使用して、ユーザーがクライアント VPN アクションを呼び出すときに使用できるリソースを制限することもできます。たとえば、次のポリシーでは、クライアント VPN エンドポイントに `purpose=test` タグがある場合に限り、ユーザーにクライアント VPN エンドポイントの操作を許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteClientVpnEndpoint",
                "ec2:ModifyClientVpnEndpoint",
                "ec2:AssociateClientVpnTargetNetwork",
                "ec2:DisassociateClientVpnTargetNetwork",
                "ec2:ApplySecurityGroupsToClientVpnTargetNetwork",
                "ec2:AuthorizeClientVpnIngress",
                "ec2:CreateClientVpnRoute",
                "ec2:DeleteClientVpnRoute",
                "ec2:RevokeClientVpnIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:client-vpn-endpoint/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/purpose": "test"
                }
            }
        }
    ]
}
```

IAM の詳細については、IAM ユーザーガイドを参照してください。クライアント VPN アクションを含む Amazon EC2 アクションのリストについては、 IAM ユーザーガイドの「Amazon EC2 のアクション、リソース、条件キー」を参照してください。

クライアント VPN エンドポイントに接続するための認証と認可の詳細については、「クライアント認証と認可 (p. 6)」を参照してください。

クライアント VPN のサービスにリンクされたロールの使用

AWS クライアント VPC は、ユーザーに代わって他の AWS のサービスを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。

クライアント VPN のサービスにリンクされたロールのアクセス許可

AWS クライアント VPN は、クライアント VPN エンドポイントを使用するときに、AWSServiceRoleForClientVPN 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以下のアクションを呼び出します。

- `ec2:CreateNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeInternetGateways`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeAccountAttributes`
- `ds:AuthorizeApplication`
- `ds:DescribeDirectories`
- `ds:GetDirectoryLimits`
- `ds:ListAuthorizedApplications`
- `ds:UnauthorizeApplication`
- `lambda:GetFunctionConfiguration`
- `logs:DescribeLogStreams`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogGroups`
- `acm:GetCertificate`
- `acm:DescribeCertificate`

AWSServiceRoleForECS サービスにリンクされたロールは、ロールを継承するために clientvpn.amazonaws.com プリンシパルを信頼します。

クライアント VPN エンドポイントにクライアント接続ハンドラーを使用する場合、クライアント VPN は AWSServiceRoleForClientVPNConnections という名前のサービスにリンクされたロールを使用します。このロールは、クライアント VPN がユーザーに代わって Lambda 関数を呼び出すことを許可する ClientVPNServiceConnectionsRolePolicy ポリシーからアクセス許可を取得します。ポリシー

は、AWSClientVPN- プレフィックスが付いた Lambda 関数でのみ lambda:InvokeFunction アクションを許可します。詳細については、「接続承認 (p. 14)」を参照してください。

クライアント VPN のサービスにリンクされたロールの作成

AWSServiceRoleForClientVPN ロールまたは AWSServiceRoleForClientVPNConnections ロールを手動で作成する必要はありません。アカウントに最初のクライアント VPN エンドポイントを作成すると、クライアント VPN によってロールが作成されます。

クライアント VPN がユーザー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ユーザーに付与されている必要があります。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アクセス許可」を参照してください。

クライアント VPN のサービスにリンクされたロールの編集

AWSServiceRoleForClientVPN サービスにリンクされたロールまたは AWSServiceRoleForClientVPNConnections サービスにリンクされたロールを編集することはできません。

クライアント VPN のサービスにリンクされたロールの削除

クライアント VPN を使用する必要がなくなった場合は、 AWSServiceRoleForClientVPN サービスにリンクされたロールおよび AWSServiceRoleForClientVPNConnections サービスにリンクされたロールを削除することをお勧めします。

まず、関連するクライアント VPN リソースを削除する必要があります。これにより、リソースに対するアクセス許可を誤って削除することがなくなります。

サービスにリンクされたロールを削除するには、IAM コンソール、IAM CLI、または IAM API 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削除」を参照してください。

ログ記録とモニタリング

モニタリングは、クライアント VPN エンドポイントの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、ソリューションのすべての部分からモニタリングデータを収集する必要があります。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。クライアント VPN エンドポイントのメトリクスを収集および追跡できます。詳細については、Amazon CloudWatch でのモニタリング (p. 69) 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、AWS CloudTrail を使用したモニタリング (p. 71) を参照してください。

Amazon CloudWatch ログ

接続ログを表示して、クライアントがクライアント VPN エンドポイントに接続、接続試行、または切断したときなど、接続イベントに関する情報を取得できます。詳細については、「接続ログ (p. 20)」を参照してください。

AWS Client 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ー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ーゾーンがあります。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、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ー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。

AWS Client 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するための機能を提供しています。

高可用性対応の複数のターゲットネットワーク

クライアントが VPN セッションを確立できるようにするには、ターゲットネットワークをクライアント VPN エンドポイントに関連付けます。ターゲットネットワークは、VPC のサブネットです。クライアント VPN エンドポイントに関連付ける各サブネットは、異なるアベイラビリティーゾーンに属している必要があります。高可用性を実現するために、複数のサブネットをクライアント VPN エンドポイントに関連付けることができます。

AWS Client 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 Client 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 が公開した API 呼び出しを使用して、ネットワーク経由でクライアント 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。

AWS Client VPN のセキュリティのベストプラクティス

AWS Client VPN には、独自のセキュリティポリシーを開発および実装する際に考慮する必要のあるいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションに相当するものではありません。これらのベストプラクティスはお客様の環境に適切ではないか、十分ではない場合があるため、これらは処方箋ではなく、有用な考慮事項と見なしてください。

承認ルール

承認ルールを使用して、ネットワークにアクセスできるユーザーを制限します。詳細については、「承認ルール (p. 51)」を参照してください。

セキュリティグループ

セキュリティグループを使用して、VPC でユーザーがアクセスできるリソースを制御します。詳細については、「セキュリティグループ (p. 14)」を参照してください。

クライアント証明書失効リスト

クライアント証明書失効リストを使用して、特定のクライアント証明書のクライアント VPN エンドポイントへのアクセスを取り消すことができます。たとえば、ユーザーが組織を離れた場合です。詳細については、「クライアント証明書失効リスト (p. 55)」を参照してください。

モニタリングツール

モニタリングツールを使用して、クライアント VPN エンドポイントの可用性とパフォーマンスを追跡します。詳細については、「クライアント VPN のモニタリング (p. 69)」を参照してください。

Identity and access management

IAM ユーザーおよび IAM ロールの IAM ポリシーを使用して、クライアント VPN リソースと API へのアクセスを管理します。詳細については、「クライアント VPN の Identity and Access Management (p. 62)」を参照してください。

IPv6 に関する考慮事項

現在、クライアント VPN サービスは、VPN トンネルを経由する IPv6 トラフィックのルーティングをサポートしていません。ただし、IPv6 のリークを防ぐために、IPv6 トラフィックを VPN トンネルにルーティングする必要がある場合があります。IPv6 リークは、IPv4 と IPv6 の両方が有効で VPN に接続されているが、VPN が IPv6 トラフィックをトンネルにルーティングしない場合に発生する可能性があります。この場合、IPv6 が有効な送信先に接続したときに、ISP から提供された IPv6 アドレスを使用して接続していることになります。これにより、実際の IPv6 アドレスがリークします。次の手順では、IPv6 トラフィックを VPN トンネルにルーティングする方法について説明します。

IPv6 リークを防ぐために、次の IPv6 関連のディレクティブをクライアント VPN 設定ファイルに追加する必要があります。

```
ifconfig-ipv6 arg0 arg1
route-ipv6 arg0
```

次の例のようになります。

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/4
```

この例では、`ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1` によって、ローカルトンネルデバイスの IPv6 アドレスが `fd15:53b6:dead::2` に設定され、リモート VPN エンドポイント IPv6 アドレスが `fd15:53b6:dead::1` に設定されます。

次のコマンド `route-ipv6 2000::/4` は、`2000:0000:0000:0000:0000:0000:0000:0000` から `2fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff` の IPv6 アドレスを VPN 接続にルーティングします。

> **Note**
>
> 例えば、Windows の「TAP」デバイスルーティングの場合、`ifconfig-ipv6` の 2 つ目のパラメータが `--route-ipv6` のルートターゲットとして使用されます。

Organizations では、`ifconfig-ipv6` の 2 つのパラメータを自身で設定する必要があり、`100::/64` (`0100:0000:0000:0000:0000:0000:0000:0000` から `0100:0000:0000:0000:ffff:ffff:ffff:ffff`) または `fc00::/7` (`fc00:0000:0000:0000:0000:0000:0000:0000` から `fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff`) のアドレスを使用できます。`100::/64` は破棄専用アドレスブロックであり、`fc00::/7` は一意ローカルです。

別の例を紹介します。

```
ifconfig-ipv6 fd15:53b6:dead::2 fd15:53b6:dead::1
route-ipv6 2000::/3
route-ipv6 fc00::/7
```

この例では、設定により、現在割り当てられているすべての IPv6 トラフィックが VPN 接続にルーティングされます。

Verification

ご自身の組織で独自のテストを実施することになるでしょう。基本的な検証は、フルトンネル VPN 接続を設定してから、IPv6 アドレスを使用して IPv6 サーバーに対して ping6 を実行することです。サーバーの IPv6 アドレスは、`route-ipv6` コマンドによって指定された範囲内にある必要があります。この ping テストは失敗します。ただし、将来的に IPv6 サポートがクライアント VPN サービスに追加された場合は変わる可能性があります。ping が成功し、フルトンネルモードで接続しているときにパブリックサイトにアクセスできる場合は、さらにトラブルシューティングを行う必要があります。また、ipleak.org などの公開されているツールを使ってテストすることもできます。

クライアント VPN のモニタリング

モニタリングは、AWS クライアント VPN および他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要です。クライアント VPN エンドポイントをモニタリングするには、次の機能を使用して、トラフィックパターンの分析やクライアント VPN エンドポイントのトラブルシューティングを行います。

Amazon CloudWatch

AWS リソースと、AWS でリアルタイムに実行されるアプリケーションを監視します。メトリクスの収集と追跡、カスタマイズしたダッシュボードの作成、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。たとえば、CloudWatch で Amazon EC2 インスタンスの CPU 使用率などのメトリクスを追跡し、必要に応じて新しいインスタンスを自動的に起動することができます。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。

AWS CloudTrail

アカウントによって、または AWS アカウントに代わって行われた API 呼び出しおよび関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。AWS を呼び出したユーザーとアカウント、呼び出し元のソース IP アドレス、および呼び出しの発生日時を特定できます。詳細については、AWS CloudTrail ユーザーガイドを参照してください。

Amazon CloudWatch ログ

AWS Client VPN エンドポイントへの接続の試行をモニタリングできます。接続の試行とクライアント VPN 接続のリセットを表示できます。接続試行では、成功した接続試行と失敗した接続試行の両方を確認できます。接続の詳細をログに記録する CloudWatch Logs ログストリームを指定できます。詳細については、接続ログ (p. 20) および Amazon CloudWatch Logs ユーザーガイドを参照してください。

Amazon CloudWatch でのモニタリング

AWS クライアント VPN は、クライアント VPN エンドポイントについて、以下のメトリクスを Amazon CloudWatch に発行します。メトリクスは、5 分ごとに Amazon CloudWatch に公開されます。

メトリクス	説明
ActiveConnectionsCount	クライアント VPN エンドポイントへのアクティブな接続の数。 単位: Count
AuthenticationFailures	クライアント VPN エンドポイントの認証失敗の数。 単位: Count
CrlDaysToExpiry	クライアント VPN エンドポイントで設定されている証明書失効リスト (CRL) の有効期限が切れるまでの日数。 単位: 日数

メトリクス	説明
EgressBytes	クライアント VPN エンドポイントから送信されたバイト数。 単位: バイト
EgressPackets	クライアント VPN エンドポイントから送信されたパケットの数。 単位: Count
IngressBytes	クライアント VPN エンドポイントが受信したバイト数。 単位: バイト
IngressPackets	クライアント VPN エンドポイントが受信したパケット数。 単位: Count
SelfServicePortalClientConfigurationDownloads	セルフサービスポータルからの Client VPN エンドポイント設定ファイルのダウンロード数。 単位: 個

AWS クライアント VPN は、クライアント VPN エンドポイントについて、以下の体制評価 (p. 17)メトリクスを公開します。

メトリクス	説明
ClientConnectHandlerTimeouts	クライアント VPN エンドポイントへの接続用のクライアント接続ハンドラの呼び出し時のタイムアウト数。 単位: カウント
ClientConnectHandlerInvalidResponses	クライアント VPN エンドポイントへの接続用のクライアント接続ハンドラから返された無効な応答の数。 単位: カウント
ClientConnectHandlerOtherExecutionErrors	クライアント VPN エンドポイントへの接続用のクライアント接続ハンドラの実行中に発生した、予期されていなかったエラーの数。 単位: カウント
ClientConnectHandlerThrottlingErrors	クライアント VPN エンドポイントへの接続用のクライアント接続ハンドラの呼び出し時のスロットリングエラーの数。 単位: カウント
ClientConnectHandlerDeniedConnections	クライアント VPN エンドポイントへの接続用のクライアント接続ハンドラによって拒否された接続の数。

メトリクス	説明
	単位: カウント
ClientConnectHandlerFailedServiceErrors	クライアント VPN エンドポイントへの接続用のクライアント接続ハンドラの実行中に発生したサービス側のエラーの数。 単位: カウント

エンドポイントごとにクライアント VPN エンドポイントのメトリクスをフィルタリングできます。

CloudWatch を使用すると、それらのデータポイントについての統計を、順序付けられた時系列データのセット (メトリクスと呼ばれる) として取得できます。メトリクスは監視対象の変数、データポイントは時間の経過と共に変わる変数の値と考えることができます。各データポイントには、タイムスタンプと、オプションの測定単位が関連付けられています。

メトリクスを使用して、システムが正常に実行されていることを確認できます。たとえば、メトリクスが許容範囲外になる場合、CloudWatch アラームを作成して、指定されたメトリクスを監視し、アクション (E メールアドレスに通知を送信するなど) を開始することができます。

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。

CloudWatch メトリクスの表示

次のように、クライアント VPN エンドポイント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、[ClientVPN] のメトリクスの名前空間を選択します。
4. メトリクスを表示するには、エンドポイントごとに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て、クライアント VPN で利用可能なメトリクスを一覧表示します。

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

AWS CloudTrail を使用したモニタリング

AWS クライアント VPN は AWS CloudTrail と統合されています。このサービスは、ユーザーやロール、またはクライアント VPN の AWS のサービスによって実行されたアクションを記録するサービスです。CloudTrail は、クライアント VPN のすべての API 呼び出しをイベントとしてキャプチャします。キャプチャされたコールには、クライアント VPN コンソールからの呼び出しと、クライアント VPN API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、クライアント VPN のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、CloudTrail コンソールの [Event history (イベント履歴)] で最新のイベントを表示でき

ます。CloudTrail によって収集された情報を使用して、クライアント VPN に対して行われたリクエスト、リクエスト元の IP アドレス、リクエストの実行者、リクエストの実行日時、その他の詳細を判別します。

CloudTrail の使用方法の詳細については、AWS CloudTrail ユーザーガイドを参照してください。

CloudTrail でのクライアント VPN 情報

CloudTrail は、アカウント作成時に AWS アカウントで有効になります。クライアント VPN でアクティビティが発生すると、そのアクティビティは [Event history] (イベント履歴) の他の AWS のサービスのイベントとともに CloudTrail イベントに記録されます。最近のイベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「CloudTrail イベント履歴でのイベントの表示」を参照してください。

クライアント VPN のイベントなど、AWS アカウントのイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡では、AWS パーティションのすべてのリージョンからのイベントがログに記録され、指定した Amazon S3 バケットにログファイルが配信されます。さらに、その他の AWS のサービスを設定して、CloudTrail ログで収集されたデータをより詳細に分析し、それに基づく対応を行うことができます。詳細については、以下を参照してください。

- 証跡を作成するための概要
- CloudTrail のサポート対象サービスと統合
- Amazon SNS の CloudTrail 通知の設定
- CloudTrail ログファイルを複数のリージョンから受け取るおよび複数のアカウントから CloudTrail ログファイルを受け取る

すべてのクライアント VPN アクションは CloudTrail が記録します。これらのアクションは Amazon EC2 API リファレンスで説明されています。たとえば、`CreateClientVpnEndpoint`、`AssociateClientVpnTargetNetwork`、`AuthorizeClientVpnIngress` の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。この ID 情報は以下のことを確認するのに役立ちます。

- リクエストが、ルートと AWS Identity and Access Management (IAM)ユーザー認証情報のどちらを使用して送信されたか。
- リクエストが、ロールとフェデレーティッドユーザーのどちらの一時的なセキュリティ認証情報を使用して送信されたか.
- リクエストが、別の AWS のサービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity エレメント」を参照してください。

クライアント VPN ログファイルエントリの概要

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信するための設定です。CloudTrail ログファイルには、1 つ以上のログエントリがあります。イベントは任意の発生元からの 1 つのリクエストを表し、リクエストされたアクション、アクションの日時、リクエストのパラメータなどに関する情報が含まれます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

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 クライアント VPN クォータ

AWS アカウントには、クライアント VPN エンドポイントに関連する、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。

クライアント VPN クォータ

名前	デフォルト	調整可能
クライアント VPN エンドポイントあたりの承認ルール	50	はい
クライアント VPN 切断タイムアウト	24 時間	いいえ
リージョンあたりのクライアント VPN エンドポイント	5	はい
クライアント VPN エンドポイントあたりの同時実行クライアント接続	この値は、エンドポイントごとのサブネット関連付けの数によって異なります。 • 1 ~ 7,000 • 2 ~ 36,500 • 3 ~ 66,500 • 4 ~ 96,500 • 5 ~ 126,000	はい
クライアント VPN エンドポイントあたりの同時実行オペレーション †	10	いいえ
クライアント VPN エンドポイントのクライアント証明書の失効リストのエントリ	20,000	いいえ
クライアント VPN エンドポイントあたりのルート	10	[Yes (はい)]

† オペレーションは次のとおりです。

- サブネットの関連付けまたは関連付けの解除
- ルートの作成または削除
- インバウンドおよびアウトバウンドルールの作成または削除
- セキュリティグループの作成または削除

ユーザーとグループのクォータ

Active Directory または SAML ベースの IdP のユーザーおよびグループを設定する場合、次のクォータが適用されます。

- ユーザーは最大 200 個のグループに属することができます。200 番目を超えたグループは無視されます。
- グループ ID の最大長は 255 文字です。
- 名前 ID の最大長は 255 文字です。255 番目を超えた文字は切り捨てられます。

一般的な考慮事項

クライアント VPN エンドポイントを使用する場合は、次の点に注意してください。

- Active Directory を使用してユーザーを認証する場合、クライアント VPN エンドポイントは Active Directory 認証に使用される AWS Directory Service リソースと同じアカウントに属している必要があります。
- SAML ベースのフェデレーション認証を使用してユーザーを認証する場合、クライアント VPN エンドポイントは、IdP と AWS の信頼関係を定義するために作成する IAM SAML ID プロバイダーと同じアカウントに属している必要があります。IAM SAML ID プロバイダーは、同じ AWS アカウントの複数のクライアント VPN エンドポイントで共有できます。

クライアント VPN のトラブルシューティング

以下のトピックは、クライアント VPN エンドポイントに関する問題のトラブルシューティングに役立ちます。

クライアントがクライアント VPN への接続に使用する OpenVPN ベースのソフトウェアのトラブルシューティングに関する詳細は、AWS Client VPN ユーザーガイドのクライアント VPN 接続のトラブルシューティングを参照してください。

よくある問題

- クライアント VPN エンドポイント DNS 名を解決できない (p. 75)
- トラフィックがサブネット間で分割されていない (p. 76)
- Active Directory グループの承認ルールが想定どおりに機能しない (p. 76)
- クライアントがピア接続 VPC、Amazon S3、またはインターネットにアクセスできない (p. 77)
- ピア接続 VPC、Amazon S3、またはインターネットへのアクセスが断続的である (p. 79)
- クライアントソフトウェアが TLS エラーを返す (p. 80)
- クライアントソフトウェアがユーザー名とパスワードのエラーを返す (Active Directory 認証) (p. 81)
- クライアントが接続できない (相互認証) (p. 81)
- クライアントから、認証情報が最大サイズを超えるというエラーが返される (フェデレーション認証) (p. 81)
- クライアントでブラウザが開かない (フェデレーション認証) (p. 82)
- クライアントから、使用可能なポートがないというエラーが返される (フェデレーション認証) (p. 82)
- クライアント VPN エンドポイントの帯域幅制限を確認する (p. 82)

クライアント VPN エンドポイント DNS 名を解決できない

問題

クライアント VPN エンドポイントの DNS 名を解決できません。

原因

クライアント VPN エンドポイント設定ファイルには、`remote-random-hostname` というパラメータが含まれています。このパラメータは、DNS キャッシュを防止するために、クライアントが DNS 名の前にランダム文字列を追加するよう強制します。一部のクライアントではこのパラメータを認識しないため、必要なランダム文字列を DNS 名の前に追加しません。

ソリューション

任意のテキストエディタを使用して、クライアント VPN エンドポイント設定ファイルを開きます。クライアント VPN エンドポイントの DNS 名を指定する行を見つけ、その前にランダム文字列を追加します。フォーマットは *random_string.displayed_DNS_name* になります。以下に例を示します。

- 元の DNS 名: `cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`
- 変更された DNS 名: `asdfa.cvpn-endpoint-0102bc4c2eEXAMPLE.clientvpn.us-west-2.amazonaws.com`

トラフィックがサブネット間で分割されていない

問題

2 つのサブネット間でネットワークトラフィックを分割しようとしています。プライベートトラフィックはプライベートサブネット経由でルーティングし、インターネットトラフィックはパブリックサブネット経由でルーティングする必要があります。ただし、両方のルートをクライアント VPN エンドポイントルートテーブルに追加しても、1 つのルートしか使用されていません。

原因

クライアント VPN エンドポイントに複数のサブネットを関連付けることができますが、アベイラビリティーゾーンごとにサブネットを 1 つのみ関連付けることができます。複数サブネットの関連付けの目的は、クライアントに高可用性とアベイラビリティーゾーンの冗長性を提供することです。ただし、クライアント VPN では、クライアント VPN エンドポイントに関連付けられたサブネット間でトラフィックを選択的に分割することはできません。

クライアントは、DNS ラウンドロビンアルゴリズムに基づいてクライアント VPN エンドポイントに接続します。つまり、接続を確立するときに、関連付けられたサブネットのいずれかを経由してトラフィックがルーティングされます。したがって、必要なルートエントリを持たない関連付けられたサブネットを確定すると、接続の問題が発生する可能性があります。

たとえば、次のサブネットの関連付けとルートを設定するとします。

- サブネットの関連付け
  - 関連付け 1 : サブネット A (us-east-1a)
  - 関連付け 2 : サブネット B (us-east-1b)
- ルート
  - ルート 1: サブネット A にルーティングされる 10.0.0.0/16
  - ルート 2: サブネット B にルーティングされる 172.31.0.0/16

この例では、接続時にサブネット A を確定するクライアントはルート 2 にアクセスできず、接続時にサブネット B を確定するクライアントはルート 1 にアクセスできません。

ソリューション

クライアント VPN エンドポイントに、関連付けられた各ネットワークのターゲットを持つ同じルートエントリがあることを確認します。これにより、トラフィックがルーティングされるサブネットに関係なく、クライアントはすべてのルートにアクセスできます。

Active Directory グループの承認ルールが想定どおりに機能しない

問題

Active Directory グループの承認ルールを設定しましたが、想定どおりに機能していません。すべてのネットワークのトラフィックを承認するため `0.0.0.0/0` の承認ルールを追加しましたが、特定の送信先 CIDR のトラフィックはいまだに失敗します。

原因

承認ルールは、ネットワーク CIDR にインデックス化されます。承認ルールでは、特定のネットワーク CIDR へのアクセスを Active Directory グループに許可する必要があります。`0.0.0.0/0` の承認ルールは特殊なケースとして扱われるため、承認ルールの作成順序に関係なく、最後に評価されます。

例えば、次の順序で 5 つの承認ルールを作成するとします。

- ルール 1: グループ 1 は `10.1.0.0/16` にアクセスする
- ルール 2: グループ 1 は `0.0.0.0/0` にアクセスする
- ルール 3: グループ 2 は `0.0.0.0/0` にアクセスする
- ルール 4: グループ 3 は `0.0.0.0/0` にアクセスする
- ルール 5: グループ 2 は `172.131.0.0/16` にアクセスする

この例では、ルール 2、ルール 3、およびルール 4 が最後に評価されます。グループ 1 は `10.1.0.0/16` にのみアクセスでき、グループ 2 は `172.131.0.0/16` にのみアクセスできます。グループ 3 は `10.1.0.0/16` または `172.131.0.0/16` にアクセスできませんが、他のすべてのネットワークにアクセスできます。ルール 1 と 5 を削除すると、3 つのグループすべてがすべてのネットワークにアクセスできます。

さらに、クライアント VPN は、承認ルールを評価するときに、最長のプレフィックスマッチングを使用します。

ソリューション

Active Directory グループに特定のネットワーク CIDR へのアクセスを明示的に許可する承認ルールを作成することを確認します。`0.0.0.0/0` の承認ルールを追加する場合、そのルールは最後に評価され、以前の承認ルールによってアクセスを許可するネットワークが制限される可能性があることに注意してください。

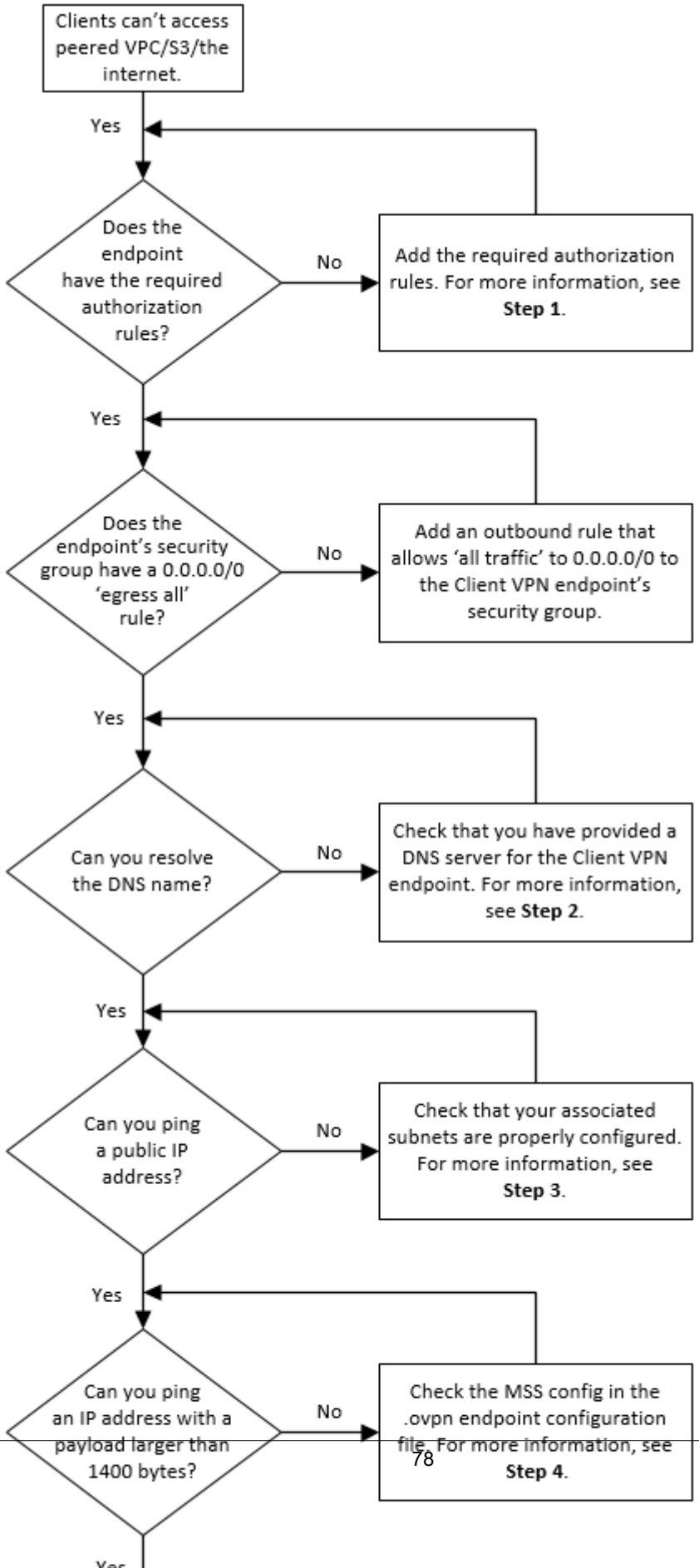
クライアントがピア接続 VPC、Amazon S3、またはインターネットにアクセスできない

問題

クライアント VPN エンドポイントルートを適切に設定しましたが、クライアントがピア接続 VPC、Amazon S3、またはインターネットにアクセスできません。

ソリューション

次のフローチャートには、インターネット、ピア接続 VPC、および Amazon S3 接続の問題を診断するステップが含まれています。


Clients can't access peered VPC/S3/the internet.
Yes
Does the endpoint have the required authorization rules?
No
Add the required authorization rules. For more information, see **Step 1**.
Yes
Does the endpoint's security group have a 0.0.0.0/0 'egress all' rule?
No
Add an outbound rule that allows 'all traffic' to 0.0.0.0/0 to the Client VPN endpoint's security group.
Yes
Can you resolve the DNS name?
No
Check that you have provided a DNS server for the Client VPN endpoint. For more information, see **Step 2**.
Yes
Can you ping a public IP address?
No
Check that your associated subnets are properly configured. For more information, see **Step 3**.
Yes
Can you ping an IP address with a payload larger than 1400 bytes?
No
Check the MSS config in the .ovpn endpoint configuration file. For more information, see **Step 4**.
Yes

1. インターネットにアクセスする場合は、`0.0.0.0/0` の承認ルールを追加します。

   ピア接続 VPC にアクセスする場合は、VPC の IPv4 CIDR 範囲の承認ルールを追加します。

   S3 にアクセスする場合は、Amazon S3 エンドポイントの IP アドレスを指定します。
2. DNS 名を解決できるかどうかを確認します。

   DNS 名を解決できない場合は、クライアント VPN エンドポイントの DNS サーバーが指定されていることを確認します。独自の DNS サーバーを管理する場合は、その IP アドレスを指定します。DNS サーバーが VPC からアクセスできることを確認します。

   DNS サーバーに指定する IP アドレスが不明な場合は、VPC の .2 IP アドレスに VPC DNS リゾルバーを指定します。
3. インターネットアクセスの場合は、パブリック IP アドレスまたはパブリックウェブサイト (`amazon.com` など) に ping できるかどうかを確認します。応答が得られない場合は、関連付けられたサブネットのルートテーブルに、インターネットゲートウェイまたは NAT ゲートウェイのいずれかをターゲットとするデフォルトルートがあることを確認します。ルートが設定されている場合は、関連付けられたサブネットに、インバウンドおよびアウトバウンドのトラフィックをブロックするネットワークアクセスコントロールリストのルールがないことを確認します。

   ピア接続 VPC に到達できない場合は、関連付けられたサブネットのルートテーブルにピア接続 VPC のルートエントリがあることを確認します。

   Amazon S3 に到達できない場合は、関連付けられたサブネットのルートテーブルにゲートウェイ VPC エンドポイントのルートエントリがあることを確認します。
4. 1400 バイトを超えるペイロードを持つパブリック IP アドレスに ping を実行できるかどうかを確認します。以下のいずれかのコマンドを使用します。

   - Windows

   ```
   C:\> ping  8.8.8.8 -l 1480 -f
   ```

   - Linux

   ```
   $ ping -s 1480 8.8.8.8 -M do
   ```

   1400 バイトを超えるペイロードを持つ IP アドレスに ping を実行できない場合は、任意のテキストエディタを使用してクライアント VPN エンドポイント `.ovpn` 設定ファイルを開き、以下を追加します。

   ```
   mssfix 1328
   ```

ピア接続 VPC、Amazon S3、またはインターネットへのアクセスが断続的である

問題

ピア接続 VPC、Amazon S3、またはインターネットへの接続時に断続的な接続の問題がありますが、関連付けられたサブネットへのアクセスには影響しません。接続の問題を解決するには、切断して再接続する必要があります。

原因

クライアントは、DNS ラウンドロビンアルゴリズムに基づいてクライアント VPN エンドポイントに接続します。つまり、接続を確立するときに、関連付けられたサブネットのいずれかを経由してトラフィックがルーティングされます。したがって、必要なルートエントリを持たない関連付けられたサブネットを確定すると、接続の問題が発生する可能性があります。

ソリューション

クライアント VPN エンドポイントに、関連付けられた各ネットワークのターゲットを持つ同じルートエントリがあることを確認します。これにより、トラフィックがルーティングされる関連付けられたサブネットに関係なく、クライアントはすべてのルートにアクセスできます。

たとえば、クライアント VPN エンドポイントに 3 つの関連付けられたサブネット (サブネット A、B、および C) があり、クライアントのインターネットアクセスを有効にするとします。これを行うには、関連付けられた各サブネットをターゲットとする `0.0.0.0/0` ルートを 3 つ追加する必要があります。

- ルート 1: サブネット A に `0.0.0.0/0`
- ルート 2: サブネット B に `0.0.0.0/0`
- ルート 3: サブネット C に `0.0.0.0/0`

クライアントソフトウェアが TLS エラーを返す

問題

以前はクライアントをクライアント VPN に正常に接続することができましたが、OpenVPN ベースのクライアントは、接続しようとすると次のエラーを返します。

```
TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network
 connectivity)
TLS Error: TLS handshake failed
```

考えられる原因

相互認証を使用し、クライアント証明書失効リストをインポートした場合、クライアント証明書失効リストの有効期限が切れていた可能性があります。認証フェーズでは、クライアント VPN エンドポイントは、インポートしたクライアント証明書失効リストと照合してクライアント証明書をチェックします。クライアント証明書失効リストの有効期限が切れている場合は、クライアント VPN エンドポイントに接続できません。

または、クライアントがクライアント VPN への接続に使用している OpenVPN ベースのソフトウェアに問題がある可能性があります。

ソリューション

OpenSSL ツールを使用して、クライアント証明書失効リストの有効期限を確認します。

```
$ openssl crl -in path_to_crl_pem_file -noout -nextupdate
```

出力には、有効期限の日時が表示されます。クライアント証明書失効リストの有効期限が切れている場合は、新しい証明書失効リストを作成してクライアント VPN エンドポイントにインポートする必要があります。詳細については、「クライアント証明書失効リスト (p. 55)」を参照してください。

OpenVPN ベースのソフトウェアのトラブルシューティングに関する詳細は、AWS Client VPN ユーザーガイドのクライアント VPN 接続のトラブルシューティングを参照してください。

クライアントソフトウェアがユーザー名とパスワードのエラーを返す (Active Directory 認証)

問題

クライアント VPN エンドポイントに Active Directory 認証を使用しています。以前はクライアントをクライアント VPN に正常に接続することができました。しかし、現在、クライアントは無効なユーザー名とパスワードのエラーを受け取っています。

考えられる原因

Active Directory 認証を使用し、クライアント設定ファイルを配布した後に Multi-Factor Authentication (MFA) を有効にした場合、ファイルにはユーザーに MFA コードの入力を求めるために必要な情報が含まれていません。ユーザー名とパスワードのみを入力するよう求められ、認証は失敗します。

ソリューション

新しいクライアント設定ファイルをダウンロードし、クライアントに配布します。新しいファイルに次の行が含まれていることを確認します。

```
static-challenge "Enter MFA code " 1
```

詳細については、「クライアント設定ファイルをエクスポートして設定する (p. 45)」を参照してください。クライアント VPN エンドポイントを使用せずに Active Directory の MFA 設定をテストし、MFA が想定どおりに機能していることを確認します。

クライアントが接続できない (相互認証)

問題

クライアント VPN エンドポイントに相互認証を使用しています。クライアントが TLS キーネゴシエーション失敗のエラーとタイムアウトエラーを受け取っています。

考えられる原因

クライアントに提供された設定ファイルにクライアント証明書とクライアントのプライベートキーが含まれていないか、証明書とキーが正しくありません。

ソリューション

設定ファイルに正しいクライアント証明書とキーが含まれていることを確認します。必要に応じて、設定ファイルを修正し、クライアントに再配布します。詳細については、「クライアント設定ファイルをエクスポートして設定する (p. 45)」を参照してください。

クライアントから、認証情報が最大サイズを超えるというエラーが返される (フェデレーション認証)

問題

クライアント VPN エンドポイントにフェデレーション認証を使用しています。クライアントが SAML ベースの ID プロバイダーの (IdP) ブラウザウィンドウにユーザー名とパスワードを入力したときに、認証情報について、サポートされている最大サイズを超えているというエラーが表示されます。

原因

IdP によって返される SAML 応答が、サポートされている最大サイズを超えています。詳細については、「SAML ベースのフェデレーション認証の要件と考慮事項 (p. 12)」を参照してください。

ソリューション

IdP でユーザーが属するグループの数を減らし、接続を再試行してください。

クライアントでブラウザが開かない (フェデレーション認証)

問題

クライアント VPN エンドポイントにフェデレーション認証を使用しています。クライアントがエンドポイントに接続しようとすると、クライアントソフトウェアによってブラウザウィンドウが開かれず、代わりにユーザー名とパスワードがポップアップウィンドウに表示されます。

原因

クライアントに提供された設定ファイルに、`auth-federate` フラグが含まれていません。

ソリューション

最新の設定ファイルをエクスポート (p. 45)し、AWS 提供のクライアントにインポートして、接続を再試行します。

クライアントから、使用可能なポートがないというエラーが返される (フェデレーション認証)

問題

クライアント VPN エンドポイントにフェデレーション認証を使用しています。クライアントがエンドポイントに接続しようとすると、クライアントソフトウェアが次のエラーを返します:

```
The authentication flow could not be initiated. There are no available ports.
```

原因

AWS 提供のクライアントでは、認証を完了するために TCP ポート 35001 を使用する必要があります。詳細については、SAML ベースのフェデレーション認証の要件と考慮事項 (p. 12) を参照してください。

ソリューション

クライアントのデバイスが TCP ポート 35001 をブロックしていないこと、または別のプロセスで使用していることを確認します。

クライアント VPN エンドポイントの帯域幅制限を確認する

問題

クライアント VPN エンドポイントの帯域幅制限を確認する必要があります。

原因

スループットは、現在地からの接続の容量や、コンピュータ上のクライアント VPN デスクトップアプリケーションと VPC エンドポイント間のネットワークレイテンシーなど、複数の要因によって異なります。

ソリューション

以下のコマンドを実行して、帯域幅を確認します。

```
sudo iperf3 -s -V
```

クライアント側:

```
sudo iperf -c server IP address -p port -w 512k -P 60
```

ドキュメント履歴

次の表では、AWS クライアント VPN 管理者ガイドの更新について説明します。

update-history-change	update-history-description	update-history-date
クライアント接続ハンドラー	クライアント VPN エンドポイントのクライアント接続ハンドラーを有効にして、新しい接続を許可するカスタムロジックを実行できます。	2020 年 11 月 4 日
セルフサービスポータル	クライアントの クライアント VPN エンドポイントでセルフサービスポータルを有効にできます。	2020 年 10 月 29 日
クライアント間のアクセス	クライアント VPN エンドポイントに接続するクライアントが相互に接続できるようにすることができます。	2020 年 9 月 29 日
SAML 2.0 ベースのフェデレーション認証	SAML 2.0 ベースのフェデレーション認証を使用して、クライアント VPN ユーザーを認証できます。	2020 年 5 月 19 日
作成中にセキュリティグループを指定する	AWS クライアント VPN エンドポイントの作成時に VPC とセキュリティグループを指定できます。	2020 年 3 月 5 日
設定可能な VPN ポート	AWS クライアント VPN エンドポイントでサポートされる VPN ポート番号を指定できます。	2020 年 1 月 16 日
多要素認証 (MFA) のサポート	AWS クライアント VPN エンドポイントが Active Directory で有効になっている場合、MFA をサポートしています。	2019 年 9 月 30 日
分割トンネルのサポート	AWS クライアント VPN エンドポイントでスプリットトンネルを有効にできます。	2019 年 7 月 24 日
初回リリース (p. 84)	このリリースでは、AWS クライアント VPN が導入されています。	2018 年 12 月 18 日