AWS デバイスの設定

この章は、次のセクションで構成されています。

AWS VPC 接続ログイン情報の更新

AWS VPC に接続するための新しいアクセスキーとシークレットアクセスキーを作成する場合は、Security Cloud Control で接続ログイン情報を更新する必要があります。更新するには、まず AWS コンソールでログイン情報を更新します。次に、この手順を使用して Security Cloud Control コンソールでログイン情報を更新します。詳細については、*IAM* ユーザー用のアクセスキーの管理に関する資料（https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html）または *AWS* アカウントルートユーザー用のアクセスキーの作成、無効か、および削除に関する資料（https://docs.aws.amazon.com/general/latest/gr/managing-aws-access-keys.html）を参照してください。

アクセスキーまたはシークレットアクセスキーを Security Cloud Control から変更することは**できません**。この接続ログイン情報は、AWS コンソールまたは AWS CLI コンソールを使用して手動で管理する必要があります。

（注） 複数の AWS VPC を Security Cloud Control テナントにオンボーディングしている場合は、一度に 1 つのデバイスのログイン情報を更新する必要があります。

手順

ステップ 1 **セキュリティデバイス**を選択します。

ステップ 2 [デバイス（Device）] タブをクリックしてから、[AWS VPC] をクリックします。

ステップ 3 接続ログイン情報を更新する AWS VPC を選択します。

必要なデバイスを見つけるには、フィルタおよび検索機能を使用します。

ステップ 4 [デバイスアクション（Device Actions）] で、[ログイン情報の更新（Update Credentials）] をクリックします。

ステップ 5 AWS VPC への接続に使用する新しい [アクセスキー（Access Key）] と [シークレットアクセスキー（Secret Access Key）] を入力します。

ステップ 6 **[更新（Update）]**をクリックします。

（注）
Security Cloud Control がデバイスの同期に失敗した場合、Security Cloud Control の接続ステータスに [無効なログイン情報（Invalid Credentials）] と表示されることがあります。その場合は、無効なユーザー名とパスワードの組み合わせを入力した可能性があります。無効なログイン情報への障害対応の詳細については、無効なログイン情報のトラブルシューティング を参照してください。

関連情報

AWS VPC のオンボーディング

AWS Transit Gateway を使用して AWS VPC トンネルを監視する

Amazon Web Services（AWS）Transit Gateway は、クラウドルータとして機能します。中央ハブを介してエンタープライズ仮想プライベートクラウド（VPC）を AWS VPC に接続し、シンプル化されたピアリング関係を可能にします。

Security Cloud Control を使用すると、AWS Transit Gateway を使用してオンボードされた AWS VPC の接続ステータスを監視できます。

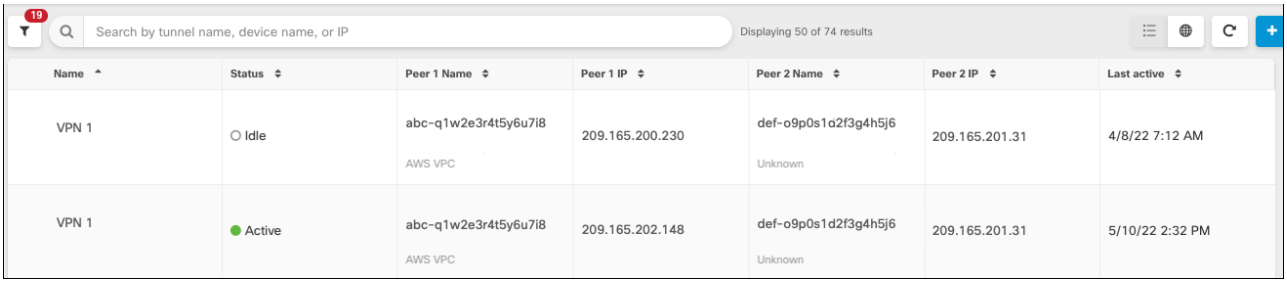
手順

ステップ 1 **[セキュアな接続（Secure Connections）] > [ネットワーク接続（Network Connections）] > [サイト間VPN（Site to Site VPN）]**を選択します。

[VPNトンネル（VPN Tunnels）] ページには、Security Cloud Control テナントによって管理されるすべてのネットワークトンネルの接続ステータスが表示されます。VPN トンネルの接続ステータスは、アクティブまたはアイドルです。

ステップ 2 VPC を選択してから、[アクション（Actions）] で [接続の確認（Check Connectivity）] をクリックします。クリックすると、トンネルに対するリアルタイムの接続確認がトリガーされ、トンネルの現在の状態（アクティブまたはアイドル）が識別されます。オンデマンド接続チェックリンクをクリックしない限り、すべてのオンボーディング済みデバイスのすべてのトンネルでのチェックが 10 分ごとに実行されます。

（注）
VPN トンネルの接続がダウンすると、Security Cloud Control から通知が表示されます。リンクが復旧すると、通知は表示されません。



サイト間 VPN トンネルを検索してフィルタ処理する

フィルタサイドバー を検索フィールドと組み合わせて使用して、VPN トンネル図に示されている VPN トンネルの検索を絞り込みます。

手順

ステップ 1 **[セキュアな接続（Secure Connections）] > [ネットワーク接続（Network Connections）] > [サイト間VPN（Site to Site VPN）]** の順に選択します。

ステップ 2 フィルタアイコン をクリックしてフィルタペインを開きます。

ステップ 3 これらのフィルタを使用して検索を絞り込みます。

- [デバイスによるフィルタ（Filter by Device）]：[デバイスによるフィルタ（Filter by Device）] をクリックし、[デバイスタイプ（Device Type）] タブを選択して、フィルタリングで検索するデバイスをチェックします。
- [トンネルの問題（Tunnel Issues）]：トンネルの各サイドで問題が検出されたかどうかを示します。たとえば、デバイスに関連するインターフェイス、ピア IP アドレス、アクセスリストが欠落している

か、IKEv1 プロポーザルの不一致が存在する可能性があります。（トンネルの問題の検出は、AWS VPC VPN トンネルではまだ使用できません）

- [デバイス/サービス（Devices/Services）]：デバイスのタイプでフィルタリングします。
- [ステータス（Status）]：トンネルのステータスがアクティブか、それともアイドルかを示します
  - [アクティブ（Active）]：セッションが開かれ、ネットワークパケットが VPN トンネルを通過している、または正常なセッションが確立され、タイムアウトになっていない場合。[アクティブ（Active）] ステータスは、トンネルが稼働しており、関連付けられていることを示します。
  - [アイドル（Idle）]：Security Cloud Control はこのトンネルのオープンセッションを検出できません。トンネルが使用されていないか、このトンネルに問題がある可能性があります。
- [オンボーディング済み（Onboarded）]：デバイスは、Security Cloud Control によって管理される場合と、Security Cloud Control によって管理されない場合（管理対象外）があります。
  - [管理対象（Managed）]：Security Cloud Control が管理するデバイスでフィルタリングします。
  - [管理対象外（Unmanaged）]：Security Cloud Control が管理しないデバイスでフィルタリングします。
- [デバイスタイプ（Device Types）]：トンネルの各サイドがライブデバイス（接続済み）かモデルデバイスかを示します。

ステップ 4 検索バーにデバイス名または IP アドレスを入力して、フィルタ処理された結果を検索することもできます。検索では大文字と小文字は区別されません。

AWS VPC トンネルに加えられた変更の履歴を表示する

AWS VPC トンネルに加えられた変更の履歴を表示するには、次の手順に従います。

手順

ステップ 1 **[イベントとログ（Events & Logs）]** > **[ログ（Logs）]** > **[変更ログ（Change Log）]** を選択します。

ステップ 2 [変更ログ（Change Log）] ページで、フィルタアイコンをクリックし、[デバイスでフィルタリング（Filter by device）] タブを選択して、[AWS VPC] をクリックします。

ステップ 3 履歴を確認する AWS VPC を選択して、[OK] をクリックします。

関連情報

Security Cloud Control での変更ログの管理

AWS VPC ポリシー

Security Cloud Control は、Amazon Web Services（AWS）アカウントに関連付けられた AWS 仮想プライベートクラウド（VPC）全体でセキュリティポリシーの一貫性を維持する機能をユーザーに提供します。Security Cloud Control を使用して、複数のデバイスタイプ間でオブジェクトを共有することもできます。詳細については、次のトピックを参照してください。

AWS VPC セキュリティグループルール

AWS セキュリティグループは、セキュリティグループに関連付けられているすべての AWS EC2 インスタンスおよびその他のエンティティへのインバウンドおよびアウトバウンドのネットワークトラフィックを管理するルールのコレクションです。Amazon Web Services（AWS）コンソールと同様、Security Cloud Control では各ルールが個別に表示されます。

SDC がインターネットにアクセスできる場合、次の環境の AWS 仮想プライベートクラウド（VPC）ルールを作成および管理できます。

- 同じ AWS VPC 内の別のセキュリティグループとの間で情報を送受信できるセキュリティグループ。
- IPv4 または IPv6 アドレスとの間で送受信できるセキュリティグループ。

AWS セキュリティグループを含む Security Cloud Control でルールを作成するときは、次の制限に注意してください。

- インバウンドトラフィックを許可するルールの場合、送信元は、同じ AWS VPC 内の 1 つ以上のセキュリティ グループ オブジェクト、IPv4 または IPv6 CIDR ブロック、あるいは単一の IPv4 または IPv6 アドレスにできます。インバウンドルールには、宛先として 1 つのセキュリティ グループ オブジェクトのみを設定できます。
- アウトバウンドトラフィックを許可するルールの場合、宛先は、同じ AWS VPC 内の 1 つ以上のセキュリティ グループ オブジェクト、プレフィックスリスト ID、IPv4 または IPv6 CIDR ブロック、単一の IPv4 または IPv6 アドレスにできます。アウトバウンドルールには、送信元として 1 つのセキュリティ グループ オブジェクトのみを設定できます。
- Security Cloud Control は、複数のポートやサブネットなど、複数のエンティティを含むルールを、AWS VPC に展開する前に個別のルールに変換します。
- ルールを追加または削除すると、セキュリティグループに関連付けられているすべての AWS エンティティに変更が自動的に適用されます。
- 1 つの AWS セキュリティグループでホストできるのは、最大 60 のインバウンドルールと 60 のアウトバウンドルールに制限されています。この制限は、IPv4 ルールと IPv6 ルールに個別に適用されます。Security Cloud Control で作成された追加のルールは、ルールの総数に含まれます。Security Cloud Control へのオンボーディングによって 60 のルールの制限を超えることはできません。

警告 既存のルールを編集すると、システムは編集したルールを削除し、更新された詳細情報を使用して新しいルールを作成します。その結果、ルールに依存するトラフィックが更新プロセス中に一時的にドロップされる可能性があります。まったく新しいルールを作成した場合、ドロップは発生しません。

AWS コンソールから作成できるルールのタイプに関する詳細については、AWS セキュリティグループ オブジェクトに関する資料を参照してください。AWS VPC に関連付けることができるオブジェクトの詳細については、AWS セキュリティグループとクラウド セキュリティ グループのオブジェクト を参照してください。

関連情報

- セキュリティグループルールの作成 （6 ページ）
- セキュリティグループルールの編集 （8 ページ）
- セキュリティグループルールの削除 （8 ページ）

セキュリティグループルールの作成

デフォルトでは、Amazon Web Services（AWS）の Virtual Private Cloud（VPC）はすべてのネットワークトラフィックをブロックします。結果として、トラフィックを [許可（Allow）] するように自動的にルールが設定されます。このアクションは編集できません。

（注） 新しいセキュリティグループルールを作成する際、作成したルールをセキュリティグループに関連付ける必要があります。

AWS コンソールは、複数の送信元や宛先を含むルールをサポートしていません。つまり、複数のエンティティを含む単一のセキュリティグループルールをデプロイすると、Security Cloud Control はそのルールを個別のルールに変換してから AWS VPC にデプロイします。たとえば、2 つのポート範囲から 1 つのクラウド セキュリティ グループ オブジェクトへのトラフィックを許可するインバウンドルールを作成する場合、Security Cloud Control はそれを 2 つの個別のルールに変換します。1 つは最初のポート範囲からセキュリティグループへのトラフィックを許可し、もう 1 つは第 2 のポート範囲からセキュリティグループへのトラフィックを許可します。

セキュリティグループルールを作成するには、次の手順を実行します。

手順

ステップ 1 **セキュリティデバイス**を選択します。

ステップ 2 [テンプレート（Template）] タブをクリックします。

ステップ 3 [AWS] タブをクリックし、アクセス コントロール ポリシーを編集する AWS VPC デバイステンプレートを選択します。

ステップ 4 [管理（Management）] ペインで、 [ポリシー（Policy）] を選択します。

ステップ 5 ルールを追加するセキュリティグループの横にある青いプラスボタンをクリックします。

ステップ 6 [インバウンド（Inbound）] または [アウトバウンド（Outbound）] をクリックします。

[インバウンド（Inbound）] ルール：送信元ネットワークには、1 つまたは複数の IPv4 アドレス、IPv6 アドレス、またはクラウドセキュリティ グループ オブジェクトを含めることができます。宛先ネットワークは、単一のクラウド セキュリティ グループ オブジェクトとして定義する**必要があります**。

[アウトバウンド（Outbound）] ルール：送信元ネットワークは、単一のクラウド セキュリティ グループ オブジェクトとして定義する**必要があります**。接続先ネットワークには、1 つまたは複数の IPv4 アドレス、IPv6 アドレス、またはセキュリティ グループ オブジェクトを含めることができます。

ステップ 7 ルール名を入力します。英数字、スペース、および特殊文字のプラス、ピリオド、下線、ハイフンを使用できます。

ステップ 8 次のタブ内の属性を任意に組み合わせて、トラフィック一致基準を定義します。

[送信元（Source）] : [送信元（Source）] タブをクリックして、ネットワーク（ネットワークと大陸を含む）を追加または削除します。ポートまたはポート範囲を送信元として定義することはできません。

[接続先（Destination）] : [接続先（Destination）] タブをクリックして、ネットワーク（ネットワークと大陸を含む）またはネットワークトラフィック着信ポートを追加または削除します。デフォルト値は、[任意（Any）] です。

（注）
ネットワークオブジェクトが定義されていない場合、AWS コンソールでは、IPv4（0.0.0.0/0）と IPv6（::0/0）の 2 つのルールに変換されます。

ステップ 9 [保存（Save）] をクリックします。

ステップ 10 行った変更を即座にレビューしてデプロイするか、待機してから複数の変更を一度にデプロイします。

注意
デプロイに失敗した場合、Security Cloud Control は AWS VPC を以前の状態に復元しようとします。復元は「ベストエフォート」ベースで実行されます。AWS は「状態」を維持しないため、このロールバックの試行は失敗する可能性があります。失敗した場合、AWS 管理コンソールにログインし、AWS VPC を以前の設定に手動で戻してから、Security Cloud Control に変更内容を読み込む必要があります。

セキュリティグループルールの編集

この手順を使用して、Security Cloud Control を使用して AWS VPC のアクセス制御ルールを編集します。

手順

ステップ 1 **セキュリティデバイス** を選択します。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [AWS] タブをクリックし、アクセス コントロール ポリシーを編集する AWS VPC を選択します。

ステップ 4 [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 既存のセキュリティグループルールを編集するには、ルールを選択し、[アクション（Actions）] ペインの編集アイコンをクリックします。編集モードを開始せずに、簡単なインライン編集を行うこともできます。ルールの制限事項と例外の詳細については、「AWS VPC セキュリティグループルール」を参照してください。

ステップ 6 [保存（Save）] をクリックします。

ステップ 7 行った変更を即座にレビューしてデプロイするか、時間をおいて複数の変更を一度にデプロイします。

注意
デプロイメントが失敗した場合、Security Cloud Control は AWS VPC を以前の状態に復元しようとします。復元は「ベストエフォート」ベースで実行されます。AWS は「状態」を維持しないため、このロールバックの試行は失敗する可能性があります。失敗した場合は、AWS 管理コンソールにログインして、AWS VPC の設定を手動で復元します。次に、AWS VPC デバイス設定と Security Cloud Control の設定の違いをポーリングします。

セキュリティグループルールの削除

手順

ステップ 1 **セキュリティデバイス**を選択します。

ステップ 2 [デバイス（Devices）] タブをクリックしてデバイスを見つけるか、[テンプレート（Templates）] タブをクリックしてモデルデバイスを見つけます。

ステップ 3 [AWS] タブをクリックし、アクセス コントロール ポリシーを編集する AWS VPC を選択します。

ステップ 4 [管理（Management）] ペインで、[ポリシー（Policy）] を選択します。

ステップ 5 不要になったセキュリティグループルールを削除するには、ルールを選択し、[アクション（Actions）] ペインで削除アイコンをクリックします。

ステップ 6 行った変更を即座にレビューしてデプロイするか、時間をおいて複数の変更を一度にデプロイします。

注意
デプロイメントが失敗した場合、Security Cloud Control は AWS VPC を以前の状態に復元しようとします。復元は「ベストエフォート」ベースで実行されます。AWS は「状態」を維持しないため、このロールバックの試行は失敗する可能性があります。失敗した場合は、AWS 管理コンソールにログインして、AWS VPC の設定を手動で復元します。次に、AWS VPC デバイス設定と Security Cloud Control の設定の違いをポーリングします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。