サイト間 VPN トンネル接続

サイト間VPNトンネルは、地理的に異なる場所にあるネットワークを接続します。2つの異なる Multicloud Defense Gateway の間、または Multicloud Defense Gateway および関連するすべての標準に準拠するクラウド サービス プロバイダーの間に、サイト間 IPsec 接続を作成できます。VPN 接続が確立されると、ローカル ゲートウェイの背後にあるホストはセキュアな VPN トンネルを介して、リモート ゲートウェイの背後にあるホストに接続することができます。

通常、ダイナミックピアの IP アドレスを他方のピアは把握していないため、ダイナミックピアから接続を開始する必要があります。リモートピアが接続を確立しようとすると、他方のピアは事前共有キー、IKE 設定、および IPsec 設定を使用して接続を検証します。

VPN 接続はリモートピアが接続を開始した後にのみ確立されるため、VPN トンネルのトラフィックを許可するアクセス制御ルールに一致するすべての発信トラフィックは、接続が確立されるまでドロップされます。これにより、適切な暗号化と VPN 保護のないデータがネットワークから流出しないようになります。

現時点では、Multicloud Defense は次のプラットフォームまたは製品とのサイト間 VPNトンネル接続をサポートしています。

- AWS
- Azure
- GCP
- ASA デバイス
- FTD デバイス
- エクストラネットまたはサードパーティのファイアウォール

サイト間 VPN トンネルの前提条件と制限事項

サポートされる VPN トンネル接続エンドポイント

次のいずれかの設定で VPNトンネル接続を作成できます。

- Multicloud Defense Gateway から Multicloud Defense Gateway へ。
- Multicloud Defense Gateway からクラウド サービス プロバイダー（AWS、Azure、GCP）へ。
- Multicloud Defense Gateway から CDO でホストされている Cisco ASA デバイスへ。

Multicloud Defense Gateway の前提条件と制限事項

関与するデバイスまたはプラットフォームのタイプを問わず、VPN トンネルを作成する前に、次の前提条件を満たしている必要があります。

- Multicloud Defense Gateway バージョン 24.04 またはバージョン 24.04-01 を実行している**必要があります**。これには Terraform のバージョンが含まれます。
- ゲートウェイで **VPN** を有効にする必要があります。
- 少なくとも 1 つのクラウド サービス プロバイダーまたはサードパーティデバイスがすでに Multicloud Defense に接続されていること。
- クラウド サービス プロバイダーまたはサードパーティデバイスが、VPN トンネル接続を許可および作成するように設定されている必要があります。詳細については、サービスまたはプラットフォームのドキュメントを参照してください。
- 少なくとも **1 つの** IPSec プロファイルが必要です。このプロファイルを VPN トンネル接続にアタッチする必要があります。
- VPC と VNET が、両側でネットワークアドレス変換ゲートウェイ**なし**で展開されている必要があります。
- （任意）少なくとも1つのBGPプロファイルを作成することを推奨します。このプロファイルを、VPNトンネル接続に関連付けられたゲートウェイインスタンスにアタッチする必要があります。

（注） VPN トンネル用にゲートウェイを使用する場合は、Multicloud Defense Gateway を設定した後で BGP プロファイルを作成することを**強く**お勧めします。このプロファイルにより、ネットワーク内のトラフィックフローをさらに制御できるため、VPN トンネルは BGP プロファイルとペアリングするとより効果的です。詳細については、BGP プロファイルを参照してください。

VPN トンネル接続の作成時には、次の制限事項に注意してください。

- 選択する Multicloud Defense Gateway は、出力/East-West ゲートウェイである**必要があります**。
- AWS および Azure ゲートウェイは、**8 コア**のインスタンスタイプである必要があります。現時点では、2 コアと 4 コアはサポートされていません。
- サイト間 VPN 接続は、最大 10 個の VPN ピアのみをサポートします。
- AWS または Azure 環境の VPC および VNET は、**単一の**可用性ゾーンで作成する必要があります。現時点では、複数の可用性ゾーンはサポートされていません。
- サイト間 VPN トンネルは、現時点では転送プロキシ ファイアウォール ルールをサポート**していません**。
- 帯域幅は 800 Mbps 以上である必要があります。

（注） ゲートウェイを無効または有効にする場合は、ゲートウェイに関連付けられているサイト間接続を削除し、VPN 接続を再作成する**必要があります**。

Multicloud Defense と Cisco ASA デバイス間の VPN トンネルの制限事項

Multicloud Defense Gateway と Cisco ASA デバイスの間に VPN トンネル接続を作成する場合は、次の制限に注意してください。

- VPN トンネルのエンドポイントを選択する場合は、少なくとも 1 つのエンドポイントが Cisco ASA デバイスであり、1 つのエンドポイントが Multicloud Defense Gateway であることを確認します（ステップ 4 ～ 6）。
- サードパーティまたはオンプレミスデバイスのサイト間 VPNトンネルを作成する場合、VPN 接続のテーブルには、Multicloud Defense の接続エンドポイントの IPSec プロファイルのステータスのみが表示されます。
- 自動スケーリングは現在サポートされていません。

CDO でホストされている Cisco ASA デバイスへの VPN トンネルの詳細については、「ASA Site-to-Site VPN Configuration」を参照してください。

（注） サードパーティデバイスまたは オンプレミス Management Center を使用している場合、この時点では、Multicloud Defense 側の IPSec ステータスのみが表示されます。

Multicloud Defense と FTD デバイス間の VPN トンネルの制限事項

Multicloud Defense Gateway と FTD デバイスの間に VPN トンネル接続を作成する場合は、次の制限に注意してください。

- IPsec IKEv1 および IKEv2 プロトコルの両方をサポート。
- 自動または手動の事前共有認証キー。
- IPv4 および IPv6 内部、外部のすべての組み合わせをサポート。
- IPsec IKEv2 サイト間 VPN トポロジにより、セキュリティ認定に準拠するための設定を提供。
- スタティック インターフェイスおよびダイナミック インターフェイス。
- エクストラネットデバイスのダイナミック IP アドレスをエンドポイントとしてサポート。

CDO でホストされている Cisco FTD デバイスへの VPN トンネルの詳細については、「Configure Site-to-Site VPN for an FDM-Managed Device」を参照してください。

ゲートウェイでの VPN の有効化

Multicloud Defense Controller ダッシュボードでゲートウェイの VPN を有効にするには、次の手順を実行します。

始める前に

Multicloud Defense を使用して 2 つのデバイス間で VPN 接続を確立する前に、IPSec プロファイルと BGP プロファイルの両方を使用できるようにゲートウェイを有効化する必要があります。IPSec プロファイルの選択は必須で、BGP プロファイルの選択は任意です。

（注） BGP プロファイルを使用する場合、BGP プロファイルはリモートピアとの IPSEC トンネル上で実行されます。

手順

ステップ 1 **[管理（Manage）] > [ゲートウェイ（Gateways）]**に移動します。

ステップ 2 [ゲートウェイの追加（Add Gateway）] をクリックして新しいゲートウェイを作成するか、既存のゲートウェイを選択して、[アクション（Actions）] ドロップダウンメニューで [編集（Edit）] を選択します。

ステップ 3 ゲートウェイを作成または編集する場合は、ウィンドウの下部までスクロールし、プロンプトが表示されたらドロップダウンメニューから [BGPプロファイル（BGP profile）] を選択します。

ステップ 4 [詳細設定（Advanced Settings）] で [VPN接続（VPN Connection）] オプションを探します。VPN トンネル接続を選択するには、[VPNの有効化（Enable VPN）] オプションをオンにします。

ステップ 5 [BGPプロファイル（BGP Profile）] ドロップダウンメニューを展開して、すでに作成済みのプロファイルを選択します。

次のタスク

サイト間 VPN 接続の作成。

サイト間 VPN 接続の作成

この手順では、 ゲートウェイと、Cisco ASA デバイス、Azure、AWS、および GCP クラウドサービスプロバイダー、または選択したサードパーティのファイアウォールとの間にサイト間 VPNトンネル接続を作成できます。

（注） **仮想インターフェイスの IP アドレス**を入力する場合は、Threat Defense の予約済み範囲である 169.254.1.x/24 を除き、169.254.xx/16 の範囲の IP を使用することを強くお勧めします。

ネットマスクには /30 を使用することを推奨します。これにより、仮想トンネルインターフェイス接続のエンドポイントに 2 つの IP アドレスのみを使用できます。例：169.254.100.1/30。

Multicloud Defense Controller ダッシュボードを使用してサイト間 VPNトンネルを作成するには、次の手順を実行します。

始める前に

VPN 接続トンネルを作成する前に、少なくとも 1 つの IPSec プロファイルを作成しておく必要があります。

VPN トンネル接続を作成する前に、BGP プロファイルを作成し、Multicloud Defense Gateway に追加することを**強く**お勧めします。詳細については、BGP プロファイルを参照してください。

手順

ステップ 1 **[管理（Manage）]** > **[ネットワーキング（Networking）]** > **[サイト間接続（Site-2-Site Connections）]**に移動します。

ステップ 2 [Create VPN Connection] をクリックします。

ステップ 3 [名前（Name）] に接続の名前を入力します。

ステップ 4 [デバイス1（Device 1）] ドロップダウンメニューを展開して Multicloud Defense Gateway を選択するか、リモートエンドポイントのパブリック IP アドレスを手動で入力します。

ステップ 5 **デバイス 1 の仮想インターフェイス IP** アドレスを入力します。このフィールドを最適化する方法については、この手順の最初にある**注**を参照してください。

ステップ 6 [デバイス2（Device 2）] ドロップダウンメニューを展開して Multicloud Defense Gateway を選択するか、リモートエンドポイントのパブリック IP アドレスを手動で入力します。デバイス 1 とデバイス 2 の両方に同じデバイスまたはゲートウェイを使用することはしないでください。

ステップ 7 **デバイス 2 の仮想インターフェイス IP** アドレスを入力します。このフィールドを最適化する方法については、この手順の最初にある**注**を参照してください。

ステップ 8 トンネルの [認証値（Authentication Value）] を入力します。現時点では、[事前共有キー（PreShared Key）] が推奨される認証方式です。

ステップ 9 [IPSecプロファイル（IPSec Profile）] ドロップダウンメニューを展開して、すでに作成済みのプロファイルを選択します。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

接続ステータスを表示して、接続の両端での着信および発信バイトの統計を確認します。

BGP プロファイルを VPNトンネル接続に関連付ける場合は、ゲートウェイを作成するか、既存のゲートウェイを編集して、目的の BGP プロファイルを追加します。VPN 接続の IPSec プロファイルはプライマリプロファイルとしてそのまま使用され、BGPプロファイルはリモートピアとの IPSEC トンネル上で実行されることに注意してください。

サイト間 VPN トンネルの編集

Multicloud Defense Controller ダッシュボードを使用して既存のサイト間 VPN 接続を編集するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）] > [ネットワーキング（Networking）] > [サイト間接続（Site-2-Site Connections）]**に移動します。

ステップ 2 VPN 接続を選択して強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューで [編集（Edit）] を選択します。

ステップ 4 次の情報のいずれかを変更します。

- 名前
- デバイス 1。
- デバイス 1 の仮想インターフェイス IP。
- デバイス 2。
- デバイス 1 の仮想インターフェイス IP。
- 認証値。
- IPSec プロファイルの選択。

ステップ 5 [保存（Save）] をクリックします。[キャンセル（Cancel）] をクリックするといつでもキャンセルできます。

サイト間 VPN トンネル接続の複製

Multicloud Defense Controller ダッシュボードを使用して VPN トンネル接続を複製するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]** > **[ネットワーキング（Networking）]** > **[サイト間接続（Site-2-Site Connections）]**に移動します。

ステップ 2 VPN 接続を選択して強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューで [複製（Clone）] を選択します。

ステップ 4 [名前（Name）]に接続の名前を入力します。複製しようとしている接続とは異なる名前にする必要があります。

ステップ 5 複製された次の情報のいずれかを変更します。

- デバイス 1。
- デバイス 1 の仮想インターフェイス IP。
- デバイス 2。
- デバイス 1 の仮想インターフェイス IP。
- IPSec プロファイルの選択。

ステップ 6 認証タイプは複製されますが、そのキー値は複製されません。トンネルの [認証値（Authentication Value）] を入力します。

ステップ 7 **[保存（Save）]** をクリックします。

VPN トンネル接続の削除

Multicloud Defense Controller ダッシュボードを使用して VPN トンネル接続を削除するには、次の手順を実行します。

手順

ステップ 1 **[管理（Manage）]** > **[ネットワーキング（Networking）]** > **[サイト間接続（Site-2-Site Connections）]**に移動します。

ステップ 2 VPN 接続を選択して強調表示します。

ステップ 3 [アクション（Actions）] ドロップダウンメニューで [削除（Delete）] を選択します。

ステップ 4 [削除（Delete）] をクリックして、削除アクションを確認します。

次のタスク

削除した VPN トンネル用に作成した BGP プロファイルを削除することを強く推奨します。

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。