Multicloud Defense Gateway およびサービス VPC または VNet

Multicloud Defense Gateway は、Multicloud Defense Gateway インスタンスのクラスタを持つネットワークロードバランサで構成される、ネットワークベースのセキュリティプラットフォームです。これは、トラフィック負荷に応じてスケールアウトおよびスケールインする自動スケーリングおよび自己修復クラスタです。Multicloud Defense Controller とゲートウェイインスタンスは、状態、正常性、テレメトリに関する一定の連続的な情報を交換します。Multicloud Defense Controller は、ゲートウェイインスタンスから受信したテレメトリデータを測定することで、スケールアウト/スケールインを判断します。ゲートウェイは、可用性と復元力に優れたアーキテクチャを実現するために、複数の可用性ゾーンで実行するように設定できます。これにより、クラウド サービス プロバイダーの単一の可用性ゾーンで障害が発生しても、実行中のアプリケーションのセキュリティ態勢が損なわれることがありません。

（注） Multicloud Defense Gateway が何らかの理由で Multicloud Defense Controller への接続を失った場合、Multicloud Defense Gateway は既存のポリシーで引き続き機能します。

ゲートウェイおよび対応する VPC または VNet を設定したら、Multicloud Defense Controller の [ゲートウェイの詳細（Gateway Details）] ページを使用して、それらの状態を表示および管理できます。

ゲートウェイの詳細

すでに確立されているゲートウェイの **[Gateway Details]** ページを表示するには、**[インフラストラクチャ（Infrastructure）]** > > **[ゲートウェイ（Gateways）]** > > **[ゲートウェイ（Gateways）]** > で [Manage] [Gateways] をクリックします。このページからゲートウェイを追加したり、すべてのゲートウェイを管理したりできます。ゲートウェイの管理では、インスタンスの編集、アップグレード、有効化、無効化、エクスポート、または削除を行うことができます。変更を行う前に、変更するゲートウェイのチェックボックスをクリックする必要があります。

[詳細検索への切り替え（Switch to Advanced Search）] をクリックして、独自の検索条件を作成します。必要に応じて、検索バー内のドロップダウンオプションを使用して、自動生成された

検索条件の一部を利用します。検索を繰り返す必要がある場合は、検索条件を**コピー**または**保存**して後で使用することもできます。

ゲートウェイアクション

次のゲートウェイアクションはバックグラウンドで発生するため、追加のタスクや項目は必要ありません。

ゲートウェイの再試行

Multicloud Defense Gateway は Multicloud Defense の自己修復コンポーネントです。いずれかの時点でゲートウェイの展開が失敗するか、問題が発生した場合、**ゲートウェイの再試行**により、Multicloud Defense はゲートウェイの再展開を自動的に試みます。このアクションは、コントローラからゲートウェイを手動で無効にするか削除するまで、無限に発生します。

再試行アクションは、Terraform で次の 2 つの側面から設定できます。最初に、Multicloud Defense がゲートウェイの展開を再試行する回数を設定できます。再展開の最大試行回数に達すると、Multicloud Defense は再試行を停止します。次に、再試行を行う間隔を設定できます。たとえば、ゲートウェイ再試行を 1 時間ごとに 3 回行うように設定できます。これは、Multicloud Defense が 1 時間ごとにゲートウェイの展開を 3 回再試行し、その後停止することを意味します。このアクションは、ゲートウェイの問題が解決するまで、またはコントローラからゲートウェイを削除するまで繰り返されます。

ゲートウェイでのトンネルインスペクション

Multicloud Defense Gateway は、新しい GRE ヘッダーと外部 IP ヘッダーを追加して元のパケットをカプセル化することで、GRE トンネルインスペクションを自動化します。その後、カプセル化されたパケットは中間ネットワークを介して送信され、カプセル化されたパケットが GRE トンネルの接続先エンドポイントに到達すると、GRE ヘッダーと外部 IP ヘッダーが削除され、元のパケットが表示されます。その後、元のパケットは最終的な接続先に転送されます。

GRE 自体は暗号化を提供しませんが、IPSec（インターネットプロトコルセキュリティ）などの他のプロトコルと組み合わせて、カプセル化されたトラフィックを保護できます。IPSec は、GRE トンネルの機密性、完全性、および認証を提供できます。これはサイト間 VPN トンネル接続に特に有益であり、ルーティングプロトコルと組み合わせて使用することで、冗長性とフェールオーバー機能を提供できます。

- サポートされるゲートウェイのユースケース （2 ページ）
- サービス VPC およびサービス VNet の設定 （18 ページ）
- ゲートウェイの設定 （25 ページ）

サポートされるゲートウェイのユースケース

Firewall Threat Defense Virtual

Cisco Cisco Secure Firewall Threat Defense virtual は、シスコの次世代ファイアウォール機能を仮想環境にもたらします。物理環境、仮想環境、クラウド環境全体を通して、またクラウド間で一貫性のあるセキュリティポリシーを実現し、ワークロードをサポートします。

Cisco Security Cloud Control でテナントをプロビジョニングして、Firewall Threat Defense 仮想デバイスを導入準備して管理し、Multicloud Defense と クラウド提供型 Firewall Management Center の間を移動できます。

Firewall Threat Defense 仮想ゲートウェイの展開に関するガイドライン

Firewall Threat Defense 仮想ゲートウェイを Multicloud Defense を使用して展開することで、標準のインターネットサービスプロバイダーゲートウェイでは使用できない、高度なネットワークセキュリティおよび管理機能が得られます。Multicloud Defense を使用して Firewall Threat Defense 仮想ゲートウェイを展開する場合も、ネットワークを保護できます。

これは複数の製品を含むタスクであるため、手順を完了するには、Multicloud Defense と クラウド提供型 Firewall Management Center の両方の間を移動する必要があります。Multicloud Defense は、インターフェイス、ゲートウェイ設定、NAT ルール、プラットフォーム設定を含む Firewall Threat Defense 仮想デバイスを展開して登録します。これに対し、クラウド提供型 Firewall Management Center アカウントのアクセスポリシー、ルール、およびオブジェクトを編集します。

クラウド提供型 Firewall Management Center によって管理される Firewall Threat Defense 仮想を作成する場合は、次のガイドラインに従ってください。

- サービス VPC を作成し、Firewall Threat Defense 仮想環境にゲートウェイを適用すると、Multicloud Defense によってセカンダリインターフェイスのサブネットと対応するセキュリティグループが自動的に作成されます。
- 要件に基づいて、最適な数の Firewall Threat Defense 仮想ゲートウェイをテナント内の クラウド提供型 Firewall Management Center 階層に展開すると、最適な効率を得ることができます。アップグレード中、以前のインスタンスをデコミッションする前に、新しいインスタンスを起動するために、追加のキャパシティが一時的に必要になります。
- Azure 展開の場合、Firewall Threat Defense 仮想のデフォルトの SSH ユーザー名は centos であり、アクセスはゲートウェイの展開時にプロビジョニングされた SSH キーを使用して認証されます。

  または、Azure シリアルコンソールを使用して、ゲートウェイの展開中に提供された管理者ユーザー名とパスワードを使用して Firewall Threat Defense 仮想デバイスにログインできます。
- AWS では、East-West トラフィックの検査では、アクセス制御ポリシーで、送信元セキュリティゾーンと接続先セキュリティゾーンの両方に VNI を使用します。これは U ターントラフィックであるため、送信元と接続先のセキュリティゾーンは同じです。
- AWS では、出力トラフィックの場合、アクセス制御ポリシーで、VNI ゾーンを送信元セキュリティゾーンとして設定し、外部ゾーンを接続先セキュリティゾーンとして設定します。
- Azure では、East-West のトラフィック検査のために、アクセス制御ポリシーで内部ゾーンを送信元セキュリティゾーンおよび接続先セキュリティゾーンとして構成します。これは U リターントラフィックであるため、送信元と接続先のセキュリティゾーンは同じです。

- Azure では、出力トラフィックについて、アクセス制御ポリシーで、内部ゾーンを送信元セキュリティゾーンとして構成し、外部ゾーンを接続先セキュリティゾーンとして構成します。

Firewall Threat Defense Virtual Gateway を展開するための前提条件

- Cisco Security Cloud Control でテナントをプロビジョニングする必要があります。詳細については、「Cisco Security Cloud Control テナントの作成」を参照してください。
- アクティブな クラウド提供型 Firewall Management Center アカウントが必要です。
- アクティブな Multicloud Defense アカウントが必要です。

Firewall Threat Defense 仮想ゲートウェイを展開する際の制限事項

クラウド提供型 Firewall Management Centerによって管理される Firewall Threat Defense 仮想ゲートウェイを作成する場合は、次の制限事項を確認してください。

- クラスターモードで Firewall Threat Defense 仮想ゲートウェイを展開することはできません。
- VPN（サイト間およびリモートアクセス）はサポートされていません。
- 集中型モデルのみがサポートされています。
- **新しい**サービス VPC を作成する必要があります。この機能が導入される前に作成された VPC では、この機能がサポートされていません。新しい VPC は Multicloud Defense ゲートウェイと Firewall Threat Defense 仮想ゲートウェイの両方をサポートします。
- **Cisco Smart Licensing** を使用するには、シスコの販売者またはパートナーを介してライセンスを購入する必要があります。
- Multicloud Defense ダッシュボードを使用してソフトウェアアップグレードを実行します。
- Firewall Threat Defense 仮想ゲートウェイに加えられた Firewall Threat Defense 仮想設定の変更は、Multicloud Defense ダッシュボードを使用して行う必要があります。展開されたデバイスのセキュリティポリシーのみを Multicloud Defense から編集する必要があります。クラウド提供型 Firewall Management Center で直接変更を実行しないでください。アクセス制御ポリシーと NAT ポリシーを管理するためにのみ使用する必要があります。
- アクセス制御ポリシーの変更（セキュリティルールの追加や削除など）は、クラウド提供型 Firewall Management Center を介して行う必要があります。
- 現時点では、ジャンボフレームはサポートされていません。

Firewall Threat Defense Virtual Gateway を展開するためのライセンス要件

Multicloud Defense Gateway は、Multicloud Defense ライセンス、スマートライセンス、および Pay-As-You-Go（PAYG）ライセンスをサポートします。

Multicloud Defense ライセンスは、クラウドを介して提供されるソフトウェアへのサブスクリプションベースのアクセスであり、アクセスの容易さ、拡張性、定期的な更新などの利点があります。Multicloud Defense ライセンスは通常、定期的な料金が発生するサブスクリプションベースであり、多くの場合パッケージの一部としてメンテナンス、更新、およびサポートが含まれます。ほとんどの Multicloud Defense ライセンスモデルは拡張性を備えており、組織が現在のニーズに基づいてユーザー数や機能の数を簡単に調整できます。このライセンスモデルはクラウドに基づいているため、最新の機能やアップデートにすぐにアクセスできます。詳細については、『Cisco Multicloud Defense発注ガイド』を参照してください。

スマートライセンスは、特定の展開シナリオで既存のライセンスを活用してコストを削減する場合に適しています。スマートライセンスを選択すると、組織はクラウドまたはハイブリッド展開で事前購入済みライセンスを使用し、組織がすでに所有しているライセンスを活用してコスト効率を高めることができます。スマートライセンスは、クラウドシナリオやハイブリッドシナリオなどの特定の展開タイプで使用されることが多く、組織は新しいライセンスを取得せずに既存のワークロードを移行できます。

Pay-As-You-Go（PAYG）ライセンスは、オンデマンドでライセンスを使用できる従量制のモデルです。このライセンスモデルは、AWS でのみ使用できます。

Firewall Threat Defense 仮想のゲートウェイを作成する場合は、リソースに応じて、次の 3 つのオプションのいずれかを選択できます。

（注） Firewall Threat Defense 仮想デバイスを使用してゲートウェイを展開すると、ライセンスモデルを変更できません。選択したライセンスモデルのパフォーマンス階層を変更できます。ライセンスモデルを変更する場合は、新しいゲートウェイを展開する必要があります。

さまざまなタイプのライセンス：

- **基本ライセンス**：ステートフル ファイアウォール、ルーティング、NAT 機能など、基本的なファイアウォールおよびネットワーク機能を有効にします。これは、すべての展開に必須の標準的な基盤ライセンスです。
- **キャリアライセンス**：GPRS、M3UA、ストリーム制御送信などのプロトコルのインスペクションを有効にします。詳細については、「キャリアライセンス」を参照してください。
- **脅威ライセンス（脅威からの保護）**:侵入防御システム（IPS）機能へのアクセスが提供され、脅威の検出と防御が可能になります。また、既知の脆弱性や脅威に対する署名ベースの検出も含まれます。
- **マルウェアライセンス（Malware Defense）**：Cisco Advanced Malware Protection（AMP）を介した高度なマルウェア保護が有効になります。これには、ファイルトラジェクトリ、サンドボックス、およびレトロスペクティブ マルウェア検出機能が含まれます。
- **URL フィルタリングライセンス**：URL フィルタリングで Web トラフィックを制御およびモニターできるようにし、Web 分類用のシスコのグローバル脅威インテリジェンスへのアクセスを提供します。

これらのライセンスタイプには、コストの最適化と拡張性を役立つ可能性のあるパフォーマンスとスループットを調整することを目的とした階層型ライセンスがあります。

- **FTDv5**：最大 100 Mbps。これは、Azure および GCP でのみサポートされています。
- **FTDv10**：最大 1 ギガビット/秒（Gbps）。これは、Azure および GCP でのみサポートされています。
- **FTDv20**：最大 3 Gbps
- **FTDv30**：最大 5 Gbps
- **FTDv50**: 最大 10 Gbps
- **FTDv100**：最大 16 Gbps

Firewall Threat Defense 仮想ゲートウェイの作成と展開

Firewall Threat Defense 仮想ゲートウェイを正常に作成して展開するには、次の手順を実行します。

1. Cisco Security Cloud Control テナントでのクラウド提供型 Firewall Management Center の有効化
2. CSP の導入準備。
3. サービス VPC の作成。
4. FTDv ゲートウェイの作成。
5. クラウド提供型 Firewall Management Center でのアクセスポリシーの設定。

Firewall Threat Defense Virtualでの自動スケーリング

自動スケーリングは、コスト効率を最適化しながら、パフォーマンスを維持するために必要なリソースをアプリケーションに提供します。

Firewall Threat Defense 仮想ゲートウェイでの自動スケーリングは、Multicloud Defense Gateway での自動スケーリングと同じではないことに注意してください。ネイティブの自動スケーリング機能については、「Multicloud Defense Gateway コンポーネントのゲートウェイ オート スケーリング」を参照してください。ここで提供される情報は、自動スケーリングが Firewall Threat Defense 仮想ゲートウェイにどのように影響するかについて説明しています。

- **監視対象メトリック** - 特定の環境で適切かつタイムリーに実行されるよう、システムメモリ、Snort CPU、およびデータプレーンに関連するメトリックが監視されます。
- **スケールアウト** - メトリックのいずれかが許容されるしきい値を超えるしきい値を登録すると、トラフィックのスパイクを処理するために、インスタンスに関連付けられた負荷またはリソースを対応するように環境がスケールアップまたはスケールアウトします。このトリガーされるイベントは、指定されたリージョンに対するものではなく、可用性ゾーンに対するものです。

（注） 環境をスケールアウトすると、デプロイメント時間は長くなります。

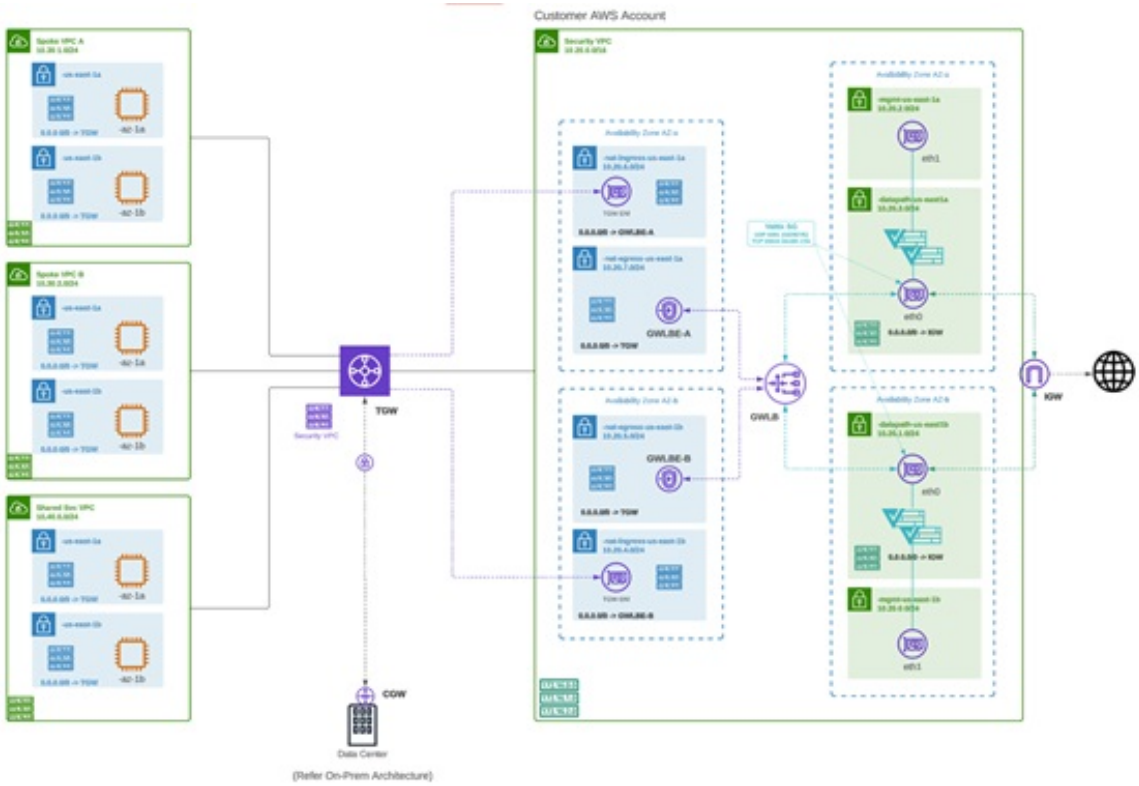
- **スケールイン** - いずれかのメトリックが許可されるしきい値を下回っている場合、効率を確保し、コストを削減するために、環境をスケールダウンまたはスケールインします。このトリガーされるイベントは、指定されたリージョンに対するものではなく、可用性ゾーンに対するものです。

Multicloud Defense 出力ゲートウェイ

出力/East-West ゲートウェイ

パブリック クラウドネットワークから発信されるトラフィックを保護するために出力/East-West ゲートウェイを展開します。エグレスゲートウェイは、完全な復号を実行し、侵入防御、マルウェア対策、データ損失防止、フルパス URL フィルタリングなどの高度なセキュリティ機能を組み込む透過的な転送プロキシとして機能します。必要に応じて転送モードで動作させることもできます。この場合、トラフィックのプロキシ接続や復号は行われませんが、悪意のある IP ブロッキングや FQDN フィルタリングなどのセキュリティ機能は適用されます。

次の図は、集中型モードの出力ゲートウェイを持つ AWS アカウントの例を示します。



出力の NAT ゲートウェイ

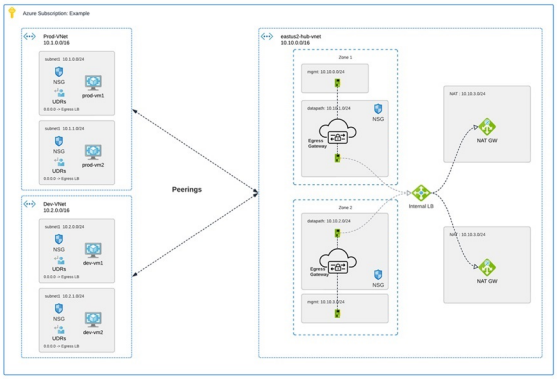
（注） 現時点で、Multicloud Defense は AWS および Azure の出力展開のみでネイティブゲートウェイをサポートしています。

ネットワークアドレス変換（NAT）ゲートウェイは、クラウド サービス プロバイダー内から発信するように設計されたゲートウェイです。出力トラフィックは、単一のIPアドレス、または可用性ゾーンごとに少なくとも1つのIPアドレスから発生します。ゲートウェイを構築し、クラウド環境内からホストすることで、効率を高め、コストを削減できる可能性があります。Multicloud Defense 内の VPC または VNet とクラウド サービス プロバイダーのゲートウェイとの関連付けが失敗した場合、障害対応のために、Multicloud Defense システムログにインスタンスがキャプチャされることに注意してください。

次の設定がサポートされています。

- Azure は 1 つのサブネットをサポートします。
- NAT ゲートウェイに少なくとも **1 つ** のパブリック IP アドレスが設定されている必要があります。

次の図は、集中型モードの出力ゲートウェイを持つ Azure アカウントの例です。



AWS CloudWAN

現時点で、Multicloud Defense は AWS の CloudWAN をエグレスゲートウェイに含めることをサポートしています。CloudWAN は、データセンター、ブランチ、および AWS ネットワークを統合する、インテント主導型のマネージド広域エリアネットワーク（WAN）サービスです。リージョン間で複数のトランジットゲートウェイを相互接続することでグローバルネットワークを作成することは可能ですが、CloudWAN には、コアネットワークポリシーに基づいてグローバルネットワークを構築および運用するために特別に設計された、組み込みの自動化、セグメンテーション、および設定管理機能が用意されています。

このオプションは、自動化された VPC アタッチメント、統合パフォーマンスモニタリング、一元化された設定などの拡張機能を提供し、これらはすべて AWS Network Manager 内で管理されます。これにより、AWS アカウント、リージョン、およびオンプレミスの場所全体で、

CloudWAN コアネットワークとトランジット ゲートウェイ ネットワークを一元的に管理および可視化できます。

主な利点：

- **簡素化されたネットワーク管理**：AWS CloudWAN は、AWS Network Manager を介した一元化ダッシュボードを提供し、ネットワーク設定、ポリシーの管理、およびトラフィックのモニタリングを行います。これにより、複数の異なるネットワーキング ソリューションの処理に伴う複雑さが大幅に軽減され、ネットワークの統合ビューが実現します。
- **拡張性**：ビジネスの成長に合わせてネットワークを簡単に拡張できます。組織のクラウドプレゼンスとグローバルフットプリントの拡大に合わせて、CloudWAN は増大する需要に対応でき、手作業での大掛かりな再設定は必要ありません。
- **最適化されたパフォーマンス**：AWS のグローバル インフラストラクチャを活用することで、CloudWAN はさまざまな地理的場所で高いパフォーマンスと低遅延の接続を確保し、アプリケーションのパフォーマンスとユーザー体験を向上させます。

CloudWAN による簡素化：

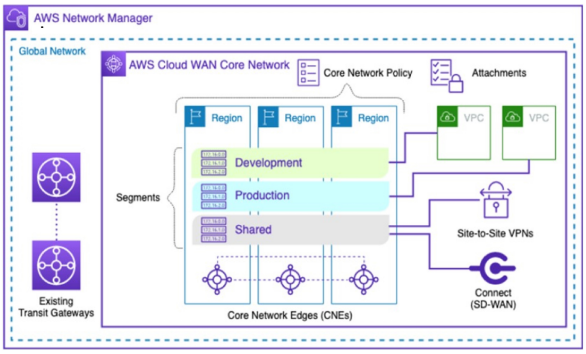
- **一元化されたポリシー管理**：宣言型言語で記述されたコアネットワークポリシーは、セグメント、AWS リージョンのルーティング、およびアタッチメントをセグメントにマッピングする方法を定義します。単一のネットワークポリシーを使用してネットワーク全体のルーティングとセキュリティポリシーを管理できるため、手動設定の必要性が減り、エラーを最小限に抑えることができます。
- **運用の自動化**：CloudWAN は、ルート伝達やポリシーの適用など、多くのネットワーク管理タスクを自動化し、IT チームがより戦略的なイニシアチブに集中できるようにします。
- **シームレスな統合**：他の AWS サービスやサードパーティのソリューションと統合することで、お客様は負担を最小限に抑えながら、まとまりのある包括的なネットワーク インフラストラクチャを構築できます。
- **可視化の強化**：AWS Network Manager には、ネットワークリソースをピンポイントで示す世界地図、CloudWatch イベントによるモニタリング、リアルタイムのイベントトラッキング、ネットワークのトポロジ図など、複数のダッシュボードの可視化が用意されています。これにより、グローバルネットワークをあらゆる面から簡単に管理およびモニターできます。

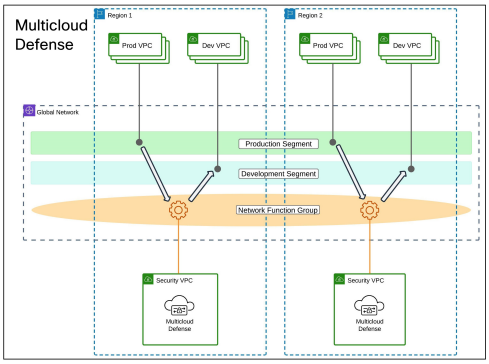
セキュリティサービスの挿入とは、セキュリティサービスをネットワークパスに直接統合するプラクティスを指します。Multicloud Defense でこれを実装する利点は次のとおりです。

- **強化されたセキュリティ態勢**：ネットワークにセキュリティサービスを挿入することで、トラフィックをリアルタイムで検査、モニター、およびフィルタリングできるため、重要なリソースに影響が及ぶ前に脅威を検出し、軽減できます。
- **一貫したセキュリティポリシー**：セキュリティサービスの挿入により、基盤となるインフラストラクチャや地理的な場所に関係なく、一貫したセキュリティポリシーがネットワーク全体に適用されます。この統一性により、コンプライアンスとガバナンスが簡素化されます。

- **可視性と制御の向上**：セキュリティサービスを統合することで、ネットワークトラフィックと潜在的な脅威に対する可視性が向上します。管理者は、高度な分析およびモニタリングツールを活用して、より深いインサイトを取得し、セキュリティリスクをより効果的に管理できます。
- **遅延と複雑性の軽減**：個別のセキュリティアプライアンスを介してトラフィックをルーティングする代わりに、ネットワークパスにセキュリティ機能を組み込みます。それにより遅延が最小限に抑えられ、ネットワークの複雑さが軽減され、パフォーマンスの向上とネットワークアーキテクチャの簡素化が実現します。
- **柔軟性と拡張性**：Multicloud Defense を使用したセキュリティサービスの挿入により、組織は変化するネットワークの状態や新たな脅威に応じてセキュリティ対策を動的に拡張し、堅牢な保護を常に確保できます。
- **集中型セキュリティ**：セキュリティリソースを統合し、管理に伴う負担を軽減してインフラストラクチャのコストを削減します。
- **ルーティングの簡素化**：複雑なルーティング設定やサードパーティ製の自動化ツールを使用せずに、ネットワークトラフィックをセキュリティアプライアンスに簡単にステアリングできます。
- **マルチリージョンのセキュリティ検査**：マルチリージョンの展開を簡素化し、複雑な設定なしでリージョン内およびリージョン間のトラフィックがセキュリティインフラストラクチャを通過できるようにします。

AWS CloudWAN と Multicloud Defense を活用してセキュリティサービスを挿入することで、お客様は、ビジネスの成長と復元力のある運用をサポートする、高性能で安全な、簡単に管理できるネットワーク インフラストラクチャを実現できます。Multicloud Defense を使用すると、ユーザーはセキュリティサービス VPC を作成し、それを既存の CloudWAN にアタッチし、ネットワーク機能グループ（NFG）を作成し、ルーティングを更新してスポークセグメントを保護でき、これらの操作はすべて自動化されます。





AWS CloudWAN でサービス VPC を作成する方法

AWS CloudWAN でサービス VPC を正常に作成するには、次の手順を実行します。

- **サービス VPC を作成**：必要なゲートウェイを使用して、複数の CNE でサービス VPC を確立します。

- **ネットワーク機能グループ（NFG）を作成**します。
- **サービス VPC を NFG としてアタッチ**：アタッチメント ポリシー ルールを使用してサービス VPC をアタッチします。
- **ワークロード VPC をアタッチ**：アタッチメント ポリシー ルールを使用して、VPC をそれぞれのセグメントにアタッチします。
- **ルーティングを更新**：ポリシーとワークロード VPC を変更して、ルーティングを更新します。
- **コアネットワークポリシーを更新**：コアネットワークポリシーに必要な変更を適用して実行します。

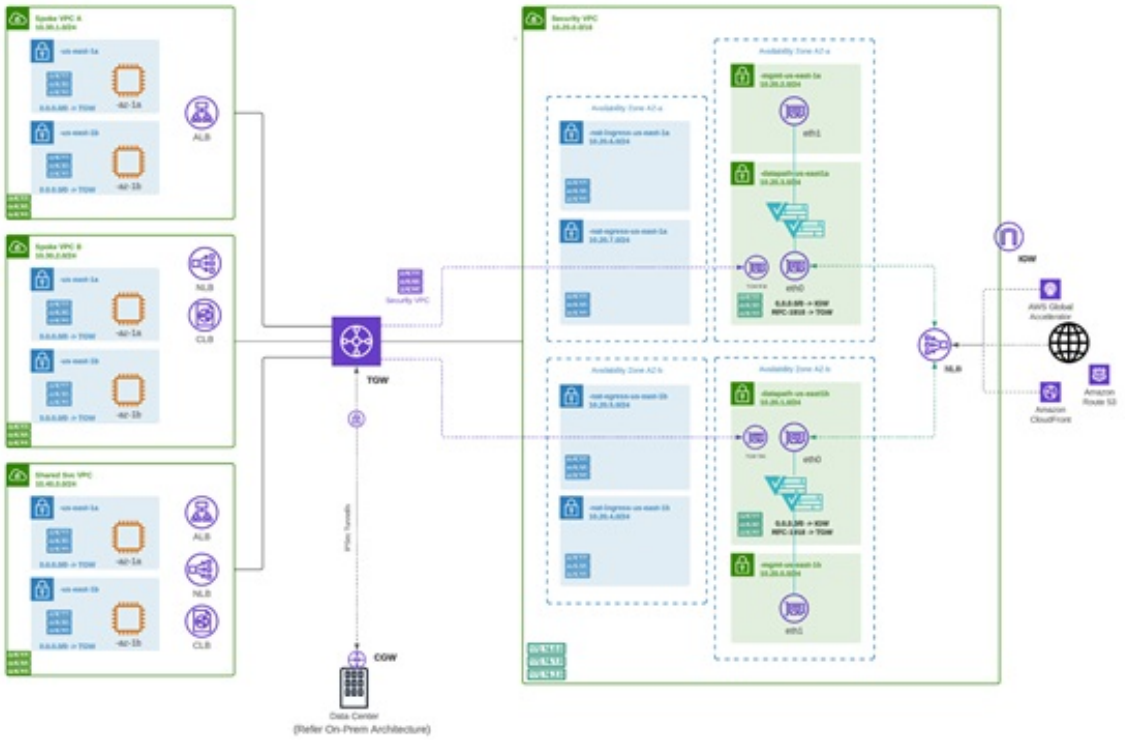
AWS CloudWAN でサービス VPC を作成する前に、次の制限事項を考慮してください。

- NAT ゲートウェイは、サービス VPC に必須です。
- デュアルホップとエッジ選択は、現在サポートされて**いません**。
- AWS CloudWAN には、転送用の SNAT 対応トラフィックをサポートしないという制限があるため、SNAT で設定されたポリシールールセットのトラフィックはドロップされます。Multicloud Defense ポリシールールセットで SNAT を無効化にすることを**強く**お勧めします。
- 別のリージョン（CNE）にサービス VPC を追加するには、次の 2 つのオプションのいずれかを実行します。
  - 新しい NFG アタッチメントのルーティングを更新するには、ポリシーを手動で実行して適用する必要があります。
  - コアネットワークを介したワークロード VPC のルートを使用して、新しいサービス VPC データパスサブネットのルーティングテーブルを手動で更新します。

Multicloud Defense 入力ゲートウェイ

イングレスゲートウェイを展開することで、一般公開されたアプリケーションを保護できます。イングレスゲートウェイは、完全な復号を実行し、侵入防御、マルウェア対策、 Web アプリケーション ファイアウォール（WAF）、フルパス URL フィルタリングなどの高度なセキュリティ機能を適用するリバースプロキシとして機能します。

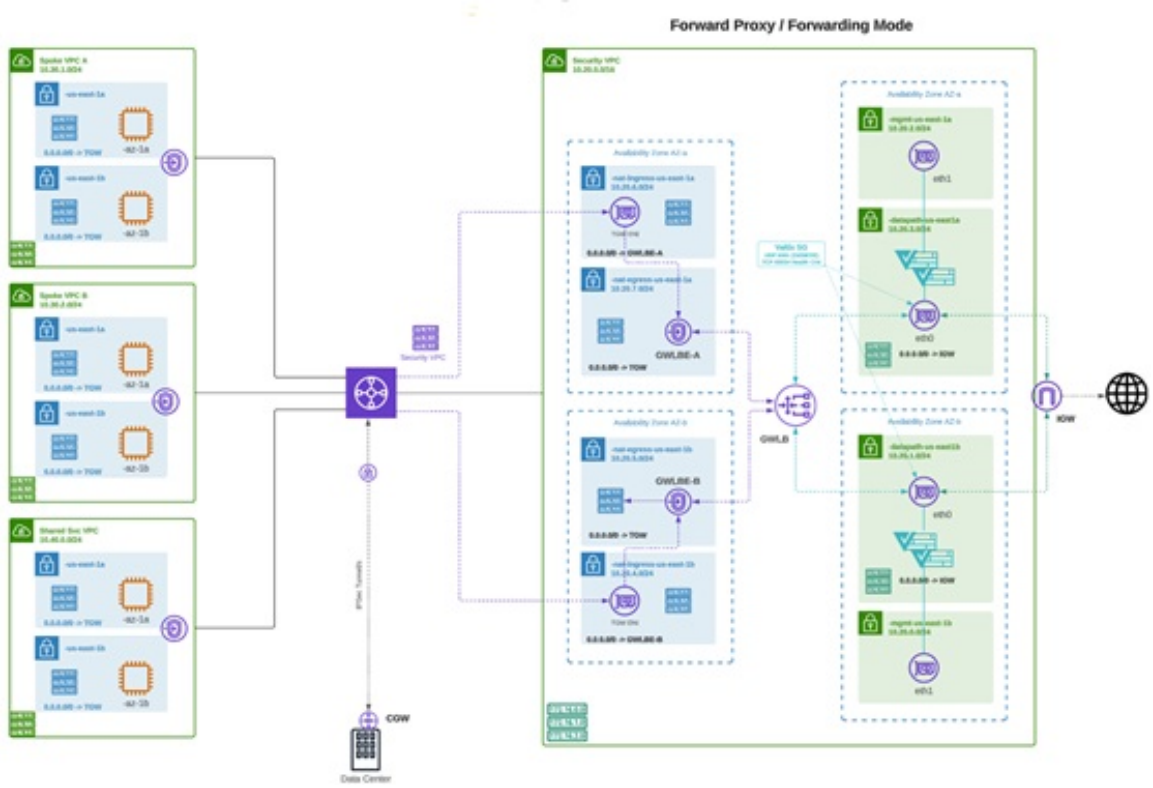
次の図は、集中型モードの入力ゲートウェイを持つ AWS アカウントの例を示します。



Multicloud Defense East-West ゲートウェイ

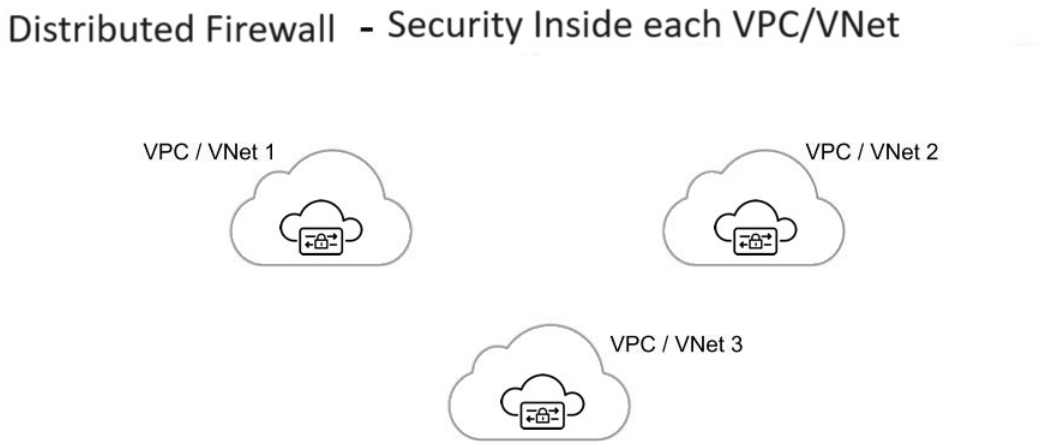
出力/East-West ゲートウェイの展開では、パブリッククラウド環境内のサブネットまたは VPC/Vnet 間に East-West L4 セグメンテーションが実装されます。ゲートウェイは、L4 ファイアウォールルールを使用した転送モードで機能し、オプションのロギングが有効化された状態で、設定されたパラメータに基づいてトラフィックを許可または拒否します。

次の図は、集中型モードの East-West ゲートウェイを持つ AWS アカウントの例を示します。



Multicloud Defense 分散型ゲートウェイ

複数の VPC/VNet でアプリケーションが実行されています。各 VPC/VNet に Multicloud Defense Gateway を展開します。



集中/ハブモードで展開されたゲートウェイ

複数の VPC/VNet でアプリケーションが実行されているとします。一元化されたセキュリティサービス VPC/VNet を介して、すべてのアプリケーションを保護したいと考えています。このモデルは、Multicloud Defense Gateway をサービス VPC に展開します。すべてのアプリケーション VPC（スポーク VPC）とサービス VPC を、AWS Transit Gateway または Azure および GCP の VNet/VPC ピアリングにアタッチします。Multicloud Defense は、AWS Transit Gateway、サービス VPC、およびスポーク VPC のアタッチメントをオーケストレーションするオプションを提供します。これは、展開を容易にし、複数のルートテーブルと Transit Gateway のアタッチメントの複雑さを排除するための推奨ソリューションです。

図 *1 : AWS* : *AWS Transit Gateway* の使用

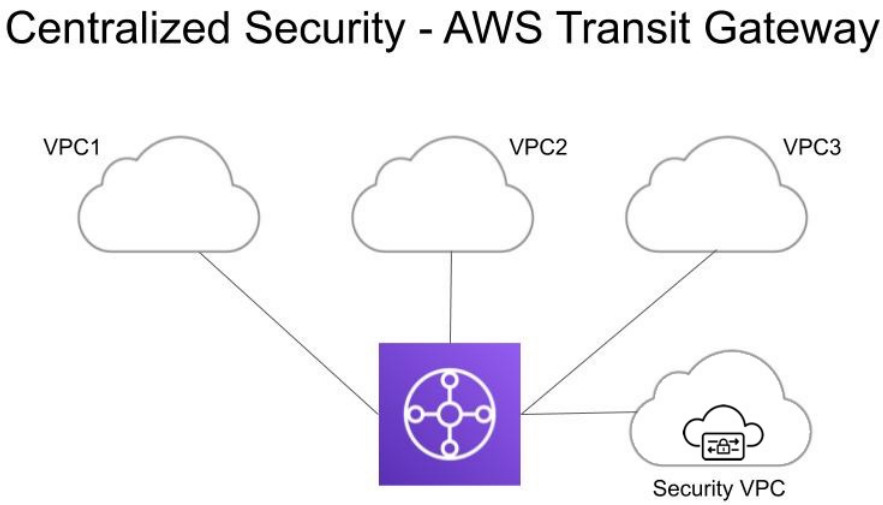


図 *2 : Azure - VNet* ピアリング

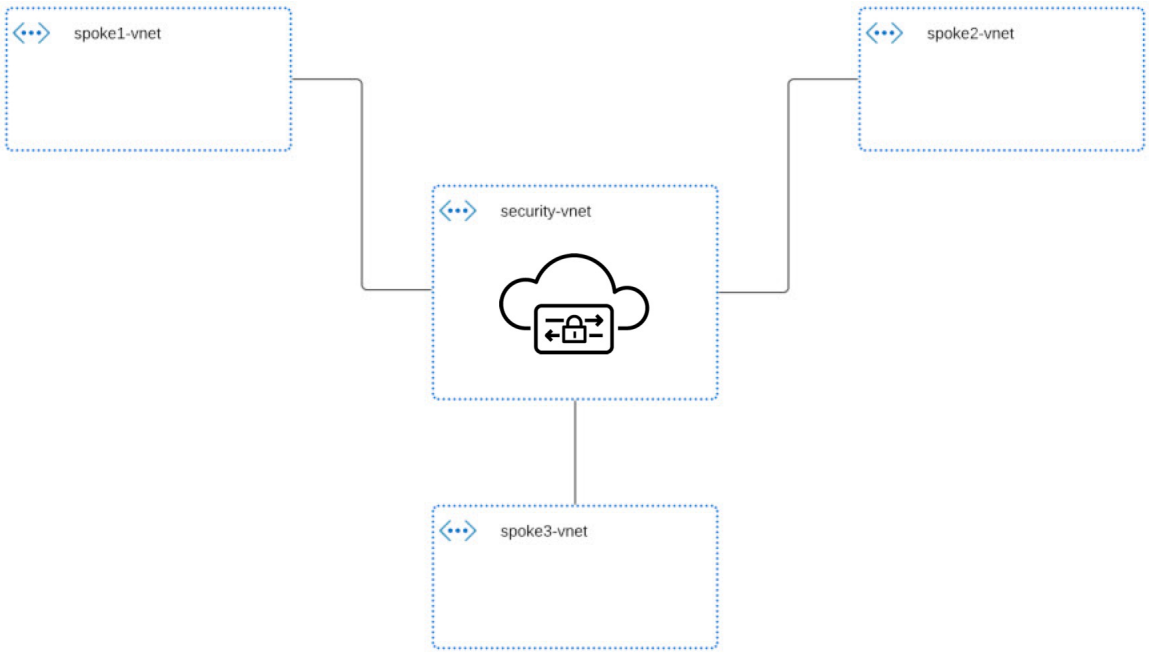
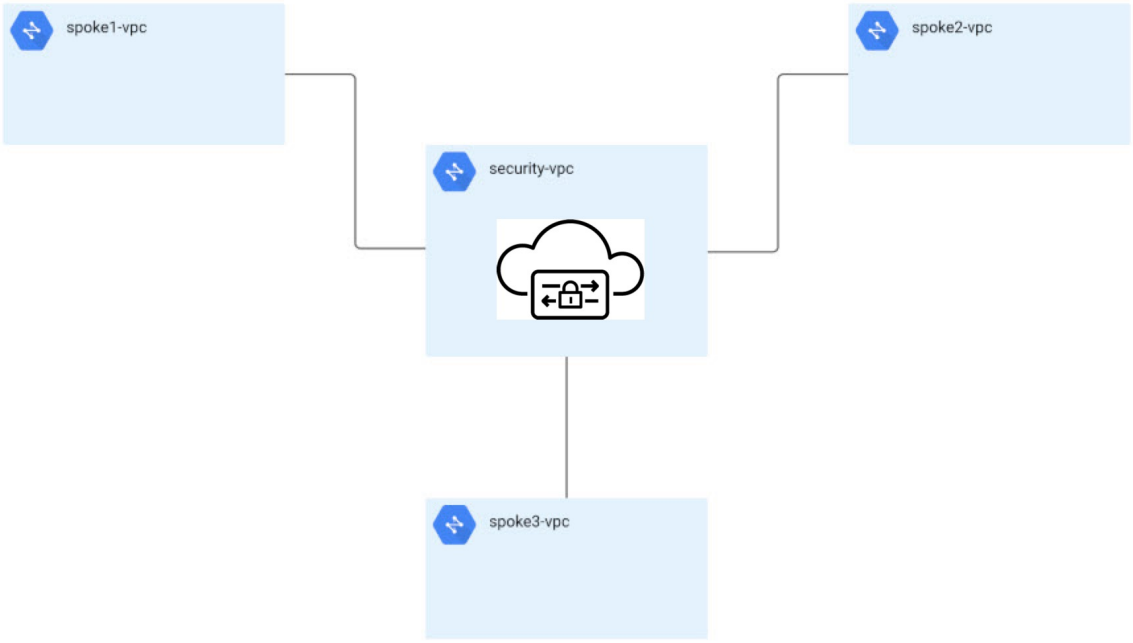


図 *3: GCP*： *VPC* ピアリング



高度なゲートウェイ設定：独自のロードバランサの使用

Multicloud Defense Gateway を作成するときに、AWS または Azure にネイティブなロードバランサを使用できます。AWS と Azure は異なるプラットフォームであるため、「ロードバランサ」に使用する単語は異なりますが、以下で説明する機能はパフォーマンス的には同じです。現在ご利用のクラウド サービス プロバイダーに該当する説明を引き続きお読みください。

独自のロードバランサを使用するように Multicloud Defense Gateway を設定するには、「ゲートウェイの追加」を参照してください。

（注） これらの設定はどちらも、**イングレスゲートウェイ**の展開のみをサポートすることに注意してください。

AWS グローバルアクセラレータ

Multicloud Defense は、Multicloud Defense Gateway インスタンス間でトラフィックをロードバランシングするための入力点として使用する、1 つ以上の AWS グローバルアクセラレータのセットと統合できます。これは、イングレスゲートウェイが展開されたときに Multicloud Defense によって作成および管理される AWS ネットワークロードバランサに似ていますが、アプリケーションとワークロードを保護するためのイングレスゲートウェイの代替的な入力点を提供します。

アクセラレータは、グローバルアクセラレータのリスナーエンドポイントグループを管理して、エンドポイントグループにゲートウェイインスタンスのアクティブなセットがあることを

確認します。クライアント IP アドレスは、グローバルアクセラレータを介して Multicloud Defense イングレスゲートウェイに渡される間、保持されます。

Multicloud Defense をグローバルアクセラレータと統合するには、まず AWS 内でグローバルアクセラレータを作成し、目的のリスナーを定義し、空のエンドポイントグループ（または既存の Multicloud Defense イングレス ゲートウェイ インスタンスを含むエンドポイントグループ）を作成する必要があります。AWS リソースが存在するようになったら、Multicloud Defense イングレスゲートウェイをグローバルアクセラレータと統合するように設定します。

その他の設定情報については、『Amazon AWS のドキュメント』を参照してください。

Azure Load Balancer

Azure クラウドサービス プロバイダーを使用している場合は、Multicloud Defense Gateway の一部として Azure から独自のロードバランサを使用できるようになりました。Azure ロードバランサは、Multicloud Defense Gateway インスタンスのクラスタを少なくとも 1 つ含むシステム提供のバックエンドプールに、複数のプロキシサーバーからのトラフィックを集めて処理します。このシナリオは、非 HTTP トラフィックを処理する複数のプロキシサーバーのセキュリティポリシーを作成する場合に最適です。

この機能を使用できるようにするには、Azure ロードバランサに従う Multicloud Defense Gateway を作成する必要があります。次の前提条件と制限事項に注意してください。

- Azure ロードバランサがすでに設定されている**必要があります**。
- ロードバランサを機能させるには、ロードバランサルールのフローティング IP を有効にする**必要があります** 。
- カスタムロードバランサ用に Azure でバックエンドプールを作成し、設定することを**強く**お勧めします。この時点では、バックエンドプールにリソースを含める必要はなく、後で変更できます。
- リソースグループを含む Azure ロードバランサを構成する場合は、Azure リソースグループと Multicloud Defense Gateway のリソースグループを同じリージョンで設定する必要があります。
- リソースグループを含む Azure ロードバランサを構成する場合、ロードバランサのリソースグループと Multicloud Defense Gateway リソースグループが同じである必要は**ない**ことにご注意ください。
- Azure ロードバランサの正常性プローブは設定できますが、必須ではありません。
- Multicloud Defense Gateway の仮想ネットワークと Azure ロードバランサの仮想ネットワークは同じである必要があります。
- Multicloud Defense Gateway のデータパスサブネットと Azure ロードバランサのサブネットは同じである必要があります。
- 少なくとも 1 つの可用性ゾーンを持つ VPC にゲートウェイをアタッチする**必要があります**。

Azure ロードバランサを作成、変更、または完了する方法については、『Microsoft Azure のドキュメント』を参照してください。

Azure UDP フラグメンテーション

一般にフラグメンテーションを回避することが推奨されますが、フラグメンテーションが発生し、Azure ロードバランサがパケットをドロップするシナリオもあります。

フラグメンテーションのサポートを有効にするには、シスコサポートにお問い合わせください。

サービス VPC およびサービス VNet の設定

厳密には必須ではありませんが、展開プロセスの一環として VPC または VNet を作成し、Multicloud Defense Gateway に接続することを**強く**推奨します。VPC および VNet は、ファイアウォールゲートウェイと統合する際に、ネットワークリソースを保護、整理、および効率的に管理するために必要なフレームワークを提供します。

VPC または VNet をアタッチすると、ネットワークが次のような利点があります。

- **分離とセキュリティ**：VPC/VNetを使用すると、クラウドプロバイダー内で論理的に分離されたネットワークを作成でき、リソースを他のユーザーから確実に分離できます。また、リソースから送受信されるインバウンドおよびアウトバウンドトラフィックを制御するセキュリティルールを定義し、ファイアウォールゲートウェイを使用してこれらのルールを適用することにより、アクセスを制御できます。
- **カスタマイズ可能なネットワークアーキテクチャ**：VPC または VNet 内にサブネットを作成し、リソースを整理してセグメント化する機能。また、IP アドレス範囲も管理し、ルーティングテーブルをカスタマイズしてネットワーク内のトラフィックを効率的に誘導できます。
- **リソース管理による拡張性と柔軟性**：リソースの追加や削除、ネットワークの拡張、および変化する要求に合わせた設定の調整が容易です。

これを行わなければ、環境はセキュリティリスクが高まり、制御が低下します。

はじめる前に

ゲートウェイの VPC または VNet を作成する前に、次の前提条件を確認することを推奨します。これらの一部は、使用しているクラウド サービス プロバイダーに固有です。

前提条件

- ネイティブゲートウェイ（NAT ゲートウェイ）を使用して VPC または VNet を設定する場合は、クラウド サービス プロバイダーからネイティブゲートウェイを設定する必要があります。詳細については、クラウド サービス プロバイダーのマニュアルを参照してください。

- Azure NAT ゲートウェイを使用してサービス VNet を展開する場合は、作成および展開の前に、Azure ダッシュボード内のカスタムロールにすべての権限があることを確認してください。権限の完全なリストについては、「アプリケーションに割り当てるカスタムロールの作成」を参照してください。
- 独自のトランジットゲートウェイを提供する場合は、複数の VPC または VNet をアタッチできます。ゲートウェイを再展開せずに、既存の VPC または VNet を新しいものに置き換えることもできます。
- FTDv ゲートウェイ用にサービス VPC を作成する場合、AWS および Azure アカウントのみがサポートされます。

GCP での共有 VPC

GCP 環境で共有 VPC を作成する場合、またはすでに作成している場合は、Multicloud Defense Controller でインベントリを有効にする追加の手順を実行する必要があります。これらの権限がないと、アセットの検出に失敗し、[Inventory] ページは信頼できません。GCP ホストプロジェクト（共有 VPC）の[IAM]ページにアクセスし、サービスプロジェクトから Multicloud Defense Controller サービスアカウントへのアクセスを許可します。このアクセスは、サービスプロジェクトが共有ネットワークリソースと対話できるようにするために必要です。共有 VPC に関連付けられている**すべての** GCP プロジェクトに、次の IAM ロールを付与する必要があります。

- 計算ビューア
- コンピュート ネットワーク ユーザー

重要 GCP で共有 VPC セットアップがあり、インスタンスが別の GPC プロジェクトにアタッチされている場合、 Multicloud Defense Gateway は GCP から受信したすべてのログを無視します。Multicloud Defense は、インスタンス**と**ネットワークの両方が配置されている単一のプロジェクトから DNS ログを送信することを想定しているため、これがデフォルトアクションです。

サービス VPC または VNet の作成

VPC および VNet の「開始する前に」セクションで、特定のクラウド サービス プロバイダーに影響する前提条件とユースケースを必ず確認してください。次の手順を使用して、サービス VPC または VNet を作成します。

手順

ステップ 1 Multicloud Defense Controller から、 に移動します。

ステップ 2 [サービスVPC/VNetの作成（Create Service VPC/VNet）] をクリックします。

ステップ 3 入力パラメータ値：

- [名前（Name）]：サービス VPC/VNet の名前を指定します。
- [CSPアカウント（CSP Account）]：サービス VPC/VNet を作成する CSP アカウントを選択します。
- [リージョン（Region）]：サービス VPC を展開するリージョンを選択します。
- (AWS/Azure) **CIDRブロック（CIDR Block）** – サービス VNet の CIDR ブロック。これは、スポーク（アプリケーション）VNet と重複してはなりません。
- (GCP のみ)**データパスCIDRブロック（Datapath CIDR Block）** - Multicloud Defense Gateway データパスサービス VPC の CIDR ブロック。この CIDR ブロックは、スポーク（アプリケーション）VPC のアドレス範囲と重複してはなりません。
- (GCP のみ)**データパス2 CIDRブロック（Datapath 2 CIDR Block）** - Multicloud Defense Gateway データパスサービス VPC の CIDR ブロック。この CIDR ブロックは、スポーク（アプリケーション）VPC のアドレス範囲と重複してはなりません。
- （GCP のみ）**管理CIDRブロック（Management CIDR Block）** - Multicloud Defense Gateway管理サービス VPC の CIDR ブロック。この CIDR ブロックは、スポーク（アプリケーション）VPC のアドレス範囲と重複してはなりません。
- **可用性ゾーン（Availability Zones）** - このサービス VPC を AWS または Azure NAT ゲートウェイにアタッチする場合は、少なくとも 1 つの可用性ゾーンを設定する必要があります。エッジまたは集中型モードで展開する場合は、AWS サービス VPC に可用性ゾーンを追加したら、ゾーンを追加または削除するために編集することはできません。サービス VNet の場合、Multicloud Defense では、レジリエンスを高めるために 2 つ以上の可用性ゾーンを選択することを推奨しています。
- （AWS CloudWAN のみ）[ネットワークタイプ（Network Type）]：[CloudWAN] を選択します。
- （AWS CloudWAN のみ）[ネットワークID（Network ID）]：ドロップダウンメニューを展開して、AWS アカウントのグローバルネットワークに関連付けられているコアネットワークを選択します。
- （AWS CloudWAN のみ）[ネットワーク機能グループ（Network Function Group）]：ドロップダウンメニューを使用して、既存のネットワーク機能グループを選択します。この選択により、サービス VPC がコアネットワークのネットワーク機能グループにアタッチされます。または、[新規作成（Create New）] を選択して、この VPC の新しいグループを作成します。新しいネットワーク機能グループを作成する場合は、この [サービスVPC（Service VPC）] ウィンドウで、ネットワーク機能グループの新しい名前を入力するように求められます。
- （Azure のみ）[リソースグループ（Resource Group）]：サービス VNet を展開するリソースグループ。
- （AWS のみ）[トランジットゲートウェイ（Transit Gateway）]：トランジットゲートウェイは、中央ハブを介して仮想プライベートクラウドとオンプレミスネットワークを接続します。ドロップダウンメニューを使用して、この VPC の既存のゲートウェイを選択します。選択できる既存のゲートウェイがない場合は、[新規作成（Create_new）] を選択します。このオプションを使用すると、Multicloud Defense は VPC 作成プロセスの一部としてゲートウェイを作成できます。
- （AWS のみ）[トランジットゲートウェイ名（Transit Gateway Name）]：新しいトランジットゲートウェイを作成することを選択した場合は、このフィールドにゲートウェイの名前を入力します。

- （AWS のみ）[共有アタッチメントの自動受け入れ（Auto accept shared attachments）]：新しいトランジットゲートウェイを作成し、この VPC をマルチアカウント ハブ ゲートウェイの展開に使用することを選択した場合は、このオプションをオンにします。
- （AWS および Azure のみ）[NATゲートウェイを使用（Use NAT Gateway）]：すべての出力トラフィックが NAT ゲートウェイを通過するようにする場合は、このオプションを有効にします。Azure アカウントに NAT ゲートウェイを使用している場合は、このサービス VNet の作成を完了する前に、Azure ダッシュボード内のカスタムロールにすべての権限があることを確認してください。権限の完全なリストについては、「アプリケーションに割り当てるカスタムロールの作成」を参照してください。

  注意
  このサービス VPC を展開して AWS または Azure 環境に Multicloud Defense VPN ゲートウェイを展開する場合は、この NAT ゲートウェイオプションを有効に**しない**でください。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

AWS または GCP アカウントのサービス VPC を作成したばかりの場合は、まず「サービス VPC/VNet の管理 （23 ページ）」を実行してから、「ゲートウェイの追加」を実行し、VPC または VNet をゲートウェイに関連付ける必要があります。

FTDv ゲートウェイ用のサービス VPC を作成する場合は、 Firewall Threat Defense 仮想ゲートウェイの作成 （32 ページ）

Azure のサービス VNet を作成した場合は、「ゲートウェイの追加」を実行することを強くお勧めします。

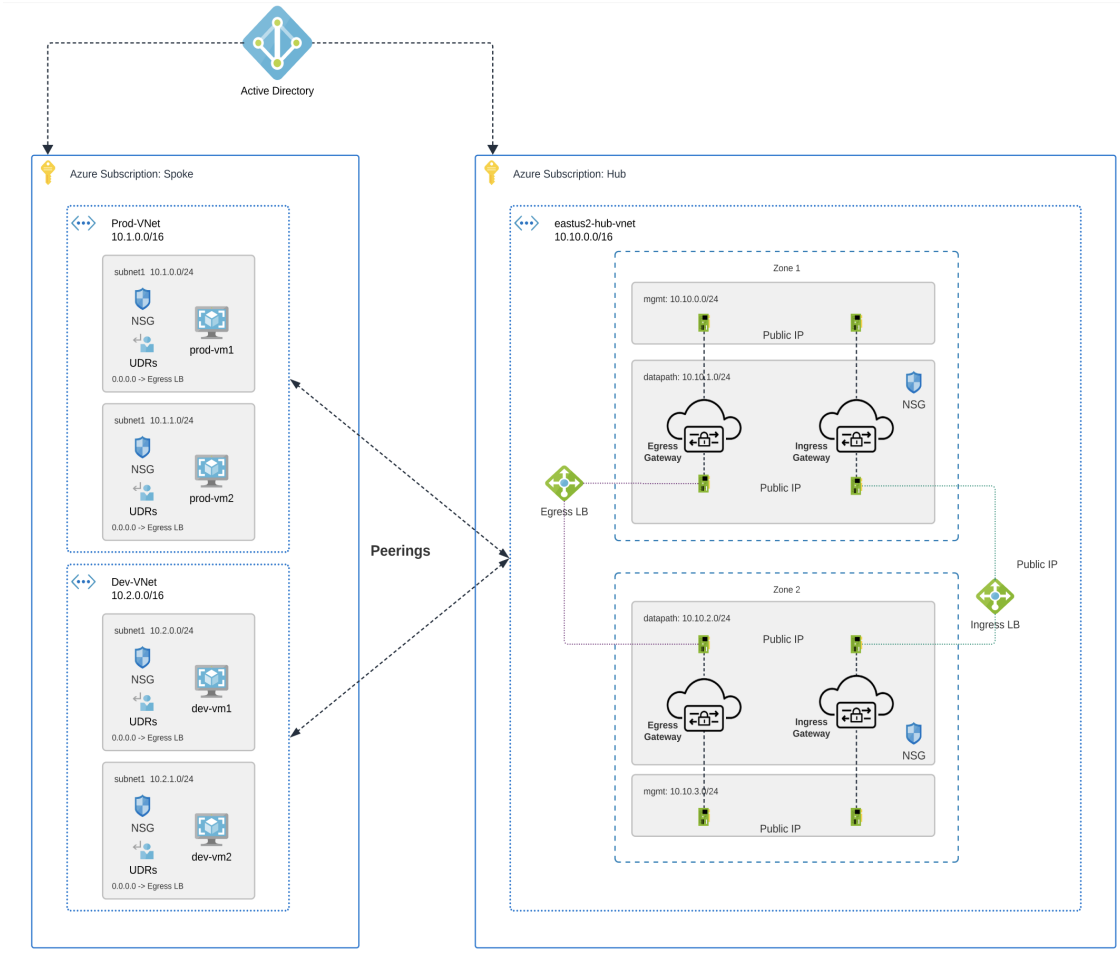
スポーク VPC または VNet の保護

スポーク VPC を保護することで、セキュリティの脅威に対応できる、より堅牢で復元力のあるネットワークを作成できます。スポーク VPC の保護により、サービス VPC とスポーク VPC の間で送信される可能性のある機密データを保護できます。これは、全体的な攻撃対象領域を縮小し、スポーク VPC での適切なセキュリティ対策が、潜在的なセキュリティインシデントの拡散を制限するための重要な戦略であるネットワーク セグメンテーションをサポートすることに役立ちます。

ゲートウェイを作成または追加する前に、AWS および GCP アカウントのスポーク VPC を保護することを強くお勧めします。

スポーク VPC がネットワークと対話する方法の例を次に示します。

図 *4 : Azure* 複合ハブ：マルチサブスクリプション



前提条件と制限事項

スポーク VPC または VNet を保護する前に、次の要件を満たします。

AWS

- AWS は、エッジモードまたは集中モードで展開された環境向けにサービス VPC が作成された後の、可用性ゾーンの追加または削除をサポートしていません。サービス VPC の作成後に可用性ゾーンを変更する必要がある場合は、正しいゾーンを含めた新しい VPC を作成する必要があります。
- CloudWAN を使用する AWS アカウントでは、スポーク VPC の保護またはゲートウェイの追加の前に、AWS Network Manager を使用して次のように設定する必要があります。
  - すでにオンボーディングされている AWS アカウントの場合は、AWS ダッシュボードの権限リストを手動で変更して、MCDControllerRole IAM ポリシーに `networkmanager:*` を含めます。詳細については、AWS の「Adding and removing IAM Identity permission」のドキュメントを参照してください。

- 出力/East-West ゲートウェイをサービス VPC にアタッチする必要があります。
- 少なくとも 1 つのグローバルネットワークが設定されている必要があります。
- 少なくとも 1 つのコアネットワークがすでに作成されている必要があります。すでにセグメントが含まれている必要はありません。

Azure

- VNet ペアリングは、同じ CSP タイプ内のアカウント間でサポートされます。アカウント内およびアカウント間でスポーク VPC/VNet を追加できます。Azure では、サブスクリプション間でピアリングするスポーク VPC の場合、同じアプリケーション登録を使用して CSP アカウントをオンボードする必要があり、サブスクリプションは同じ Active Directory 内にある必要があります。
- Azure 環境では、スポーク VPC/VNet を保護する**前**に、ルートテーブルをアタッチする必要があります。詳細については、Azure ユーザーガイドの「Associate a route table to a subnet」の章を参照してください。
- Azure は、エッジモードまたは集中モードで展開された環境向けにサービス VPC が作成された後の、可用性ゾーンの追加または削除をサポートしていません。サービス VPC の作成後に可用性ゾーンを変更する必要がある場合は、正しいゾーンを含めた新しい VPC を作成する必要があります。

GCP

- GCP は、エッジモードまたは集中モードで展開された環境向けにサービス VPC が作成された後の、可用性ゾーンの追加または削除をサポートしていません。これは、エッジモードで展開された環境の Azure 、GCP、および OCI にも適用されます。サービス VPC の作成後に可用性ゾーンを変更する必要がある場合は、正しいゾーンを含めた新しい VPC を作成する必要があります。

OCI

- OCI は、エッジモードまたは集中モードで展開された環境向けにサービス VPC が作成された後の、可用性ゾーンの追加または削除をサポートしていません。サービス VPC の作成後に可用性ゾーンを変更する必要がある場合は、正しいゾーンを含めた新しい VPC を作成する必要があります。

サービス VPC/VNet の管理

スポーク VPC またはスポーク VNet を管理するには、次の手順を実行します。

始める前に

AWS CloudWAN を使用するように設定された AWS サービス VPC を保護する場合、このページに示す表には、エッジリージョンごとに個別の行があります。セグメントを追加/削除することで、サービス VPC を使用してセグメントを保護できます。各セグメントは、セグメントにアタッチまたはアタッチを解除できる VPC のリストを使用して編集できます。セグメント

を通過するトラフィックは、VPC で設定されたネットワーク機能グループによって保護されます。このテーブルに表示されるセグメントから転送されたものはすべて、VPC で設定されたネットワーク機能グループを通過します。

手順

ステップ 1 Multicloud Defense Controller ダッシュボードから、 に移動します。

ステップ 2 サービス VPC またはサービス VNet を選択し、[アクション（Actions）] をクリックします。

ステップ 3 [スポークVPC/VNetの管理（Manage Spoke VPC/VNet）] をクリックします。

ステップ 4 テーブルに表示されている VPC または VNet にアタッチされているリージョンにセグメントを追加するには、[追加（Add）] をクリックします。

ステップ 5 ドロップダウンメニューを使用して、使用可能なネットワークセグメントを選択します。このアクションにより、既存のネットワークセグメントがサービス VPC またはサービス VPC 内のネットワーク機能グループに割り当てられます。Multicloud Defense はネットワークセグメントを作成しないことに注意してください。AWS アカウントのコアネットワークの一部として、ネットワークセグメントを作成する必要があります。

ステップ 6 ネットワークセグメントを**削除**するには、セグメントを選択し、[Remove] をクリックします。

ステップ 7 [+ VPCの追加（+ Add VPC）] をクリックして VPC を追加し、ユーザーVPC をネットワークセグメントに関連付けます。

a) [VPCをセグメントに追加（Add VPC to Segment）] ウィンドウで、ウィンドウの左側にあるすべてのスポーク VPC または VNet を選択し、[>] をクリックしてセグメントに割り当てます。または、既存の VPC または VNet を選択し、[<] をクリックしてセグメントから削除します。

b) [保存（Save）] をクリックして、VPC の変更を確定します。

ステップ 8 [保存（Save）] をクリックして、ネットワークセグメントの変更を確定します。これらの変更が有効になり、影響を受ける VPC または VNet が「アクティブ」になるまでに最大 30 分かかる場合があることに注意してください。

スポーク VPC または VNet のエクスポート

スポーク VPC または VNet の設定をエクスポートするには、次の手順を実行します。

手順

ステップ 1 Multicloud Defense Controller ダッシュボードから、 に移動します。

ステップ 2 テーブルからサービス VPC またはサービス VNet を選択し、[アクション（Actions）] をクリックします。

ステップ 3 [エクスポート（Export）] をクリックします。

ステップ 4 Multicloud Defense でエクスポートウィザードが生成されます。

ステップ 5 [ダウンロード（Download）] をクリックして Terraform をローカルにダウンロードするか、下にスクロールして [コードのコピー（Copy Code）] をクリックして JSON リソースをコピーします。

ステップ 6 Terraform スクリプトに手動で貼り付けます。

ステップ 7 Terraform プロンプト内で、ウィンドウの下半分に表示されるコマンドを実行します。

ステップ 8 Terraform プロンプト内のプロンプトに従って、タスクを完了します。エクスポートウィンドウを閉じます。

スポーク VPC または Vnet の削除

アカウント設定からスポーク VPC または VNet を削除するには、次の手順を実行します。クラウド サービス プロバイダーのダッシュボードで削除を確認する必要がある場合がありますので、注意してください。

手順

ステップ 1 Multicloud Defense Controller ダッシュボードから、 に移動します。

ステップ 2 テーブルからサービス VPC またはサービス VNet を選択し、[アクション（Actions）] をクリックします。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 サービス VPC または VNet の削除を確認し、[はい（Yes）] をクリックします。

ゲートウェイの設定

Multicloud Defense Gateway に と統計を表示します。このページから、ゲートウェイの検索とフィルタリングを実行したり、各ゲートウェイに関連付けられているクラウド サービス プロバイダー、現在のインスタンスの数とタイプなどを表示したりできます。

特定のゲートウェイ環境でサポートされるユースケースの詳細については、サポートされるゲートウェイのユースケース （2 ページ）を参照してください。

はじめる前に

また、Multicloud Defense Gateway を介してトランジットゲートウェイをオーケストレーションしたり、既存のトランジットゲートウェイをアタッチすることもできます。

Multicloud Defense Gateway の前提条件と制限事項

前提条件

サポートされるクラウド サービス プロバイダー（AWS、Azure、GCP、OCI）は、独自の用語とゲートウェイ環境を使用する個別のエンティティです。Multicloud Defense Controller で使用

可能なすべてのオプションが、お使いのクラウド サービス プロバイダーに対応しているわけではありません。たとえば、AWS は独自のトランジットゲートウェイを使用しており、そこに VPC を追加できますが、Azure はロードバランサを使用して Web トラフィックとアプリケーションを管理しており、そこに追加できるのは VNet です。続行する際は、この点に注意してください。

（注） AWS 環境の場合、集中型モードでスポーク VPC を保護する場合、Multicloud Defense はサービス VPC に関連付けられているトランジットゲートウェイに VPC をアタッチします。デフォルトで、Multicloud Defense は、トランジットゲートウェイへのアタッチ用に各可用性ゾーンのサブネットをランダムに選択します。VPC を追加するときにこのオプションを変更したり、すでにゲートウェイに割り当てられている VPC を変更したりできます。

制限事項

Multicloud Defense Gateway の作成時には、次の制限事項に注意してください。

- IPSec プロファイルを含むサイト間 VPN トンネルを使用する Multicloud Defense Gateway を展開する場合は、サービス VPC またはサービス VNet を**使用し**、VPN 接続の両側でネットワークアドレス変換（NAT）ゲートウェイを**使用せずに**ゲートウェイを展開する必要があります。
- 自動スケーリングは、IPSec プロファイルを含むゲートウェイではサポートされていません。
- ゲートウェイ内のポリシールールは転送のみである**必要があります**。
- AWS または Azure アカウントの Multicloud Defense Gateway に IPSec プロファイルを含める場合は、ゲートウェイインスタンスを `core 8` で設定する **必要があります**。Multicloud Defense Gateway は現在、core 2 または core 4 オプションのゲートウェイをサポートしていません。

FTDv ゲートウェイの前提条件と制限事項

Multicloud Defense ゲートウェイを作成、展開、および維持するプロセスのみをオーケストレーションします。ポリシーまたはルールの作成はクラウド提供型 Firewall Management Center で行われます。ゲートウェイを作成する前に、両方の管理製品の統合をサポートするための以下の前提条件、制限事項、および推奨事項を考慮してください。

前提条件

FTDv の Multicloud Defense Gateway を作成する前に、次の手順を完了し、設定する必要があります。

- **新しい**サービス VPC を作成する必要があります。この機能より前に作成された VPC は、この機能をサポートしていません。新しい VPC を作成しても、 Multicloud Defense ゲートウェイと FTDv ゲートウェイの両方に使用できることに注意してください。

- Multicloud Defense テナントにオンボーディングされたクラウド サービス プロバイダーが必要です。
- FTDv ゲートウェイの指定クラウド サービス プロバイダーとして AWS アカウントを使用している場合は、AWS マーケットプレイスのサービス利用条件に手動で同意する**必要があります**。送信しないと、Multicloud Defense Controller は必要な API リクエストを送信できません。
- シスコの販売者またはパートナーを通じて購入したライセンスを 1 つ以上持っている必要があります。
- クラウド提供型 Firewall Management Center へのサブスクリプションが必要です。

この環境の制限事項と要件については、Firewall Threat Defense Virtual （2 ページ） を参照してください。

Multicloud Defense が作成するリソース

次のリソースは、ゲートウェイ、VPC、または VNet を作成するときに Multicloud Defense によって作成されます。これらはプロセスの一部として作成され、ユーザーによる追加のアクションは必要ありません。クラウド サービス プロバイダーの要件ごとに異なるリソースが作成されることに注意してください。

GCP リソース

Multicloud Defense は、2 つのサービス VPC と 4 つのファイアウォールを作成します。正確なリソースの割り当てについては、次を参照してください。

サービス VPC

- 管理
- データパス

ファイアウォール ルール

- 管理（入力）
- 管理（出力）
- データパス（入力）
- データパス（出力）

（注） サービス VPC CIDR をスポーク VPC と重複させることは**できません**。

AWS リソース

Multicloud Defense は、サポートされるユースケース（入力、出力/East-West）に対応するために 3 つのサービス VPC を作成します。次に示すものがこれらの各 VPC で作成され、関連付けられます。

- 可用性ゾーンごとに 4 つのサブネット。
- サブネットごとに 1 つのルートテーブル。
- 2 つのセキュリティグループ：管理とデータパス。
- 1 つのトランジットゲートウェイ。

（注） このトランジットゲートウェイはサービス VPC の作成時に作成され、ゲートウェイにアタッチされます。このゲートウェイは、他のサービス VPC で再利用できます。

- トランジットゲートウェイのルートテーブル。

（注） ルートテーブルは、作成プロセスの一部としてサービス VPC にアタッチされます。

（注） AWS ゲートウェイロードバランサ（GWLB）は、GWLB の初期展開後の可用性ゾーンの追加/削除をサポートしていません。可用性ゾーンを変更する必要がある場合は、サービス VPC を再展開する必要があります。詳細については、AWS マニュアルを参照してください。

Azure のリソース

Multicloud Defense は次のリソースを使用して 1 つのサービス VNet を作成しました。

- 1 つの VNet。
- 2 つのネットワーク セキュリティ グループ。

サービス VNet の CIDR 値は、スポーク VNet と重複してはなりません。

FTDv リソース

Multicloud Defense は、Cisco Secure Firewall Firewall Threat Defense 仮想（FTDv）デバイスで使用されるサービス VPC に次のリソースを作成します。

- 管理サブネット。
- データパス 1 サブネット。

- データパス 2 サブネット。
- サブネットに対応する 3 つのセキュリティグループ。

Multicloud Defense Gateway の追加

クラウド サービス プロバイダーの Multicloud Defense Gateway を追加するには、次の手順を実行します。

始める前に

ゲートウェイを作成する前に、はじめる前に （25 ページ） で特定の環境に関連する情報や要件について確認してください。

AWS グローバルアクセラレータまたは Azure ロードバランサの使用を計画している場合は、Multicloud Defense Gateway に追加する前にロードバランサがすでに設定されていることを確認してください。詳細については、高度なゲートウェイ設定：独自のロードバランサの使用 （16 ページ）を参照してください。

手順

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > > **[ゲートウェイ（Gateways）]** > > **[ゲートウェイ（Gateways）]** > にアクセスします。

ステップ 2 [ゲートウェイの追加（Add Gateway）] をクリックします。

ステップ 3 ゲートウェイを追加するクラウド サービス プロバイダーを選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 ゲートウェイ情報を入力します。

- [インスタンスタイプ（Instance Type）]：クラウド サービス プロバイダーのタイプを選択します。クラウド サービス プロバイダーによって、異なるインスタンスタイプが表示される場合があります。
  - （Azure のみ）VPN を作成し、ベース オペレーティング システムとして Red Hat Enterprise Linux 9（RHEL 9）を使用する場合は、Dsv5 シリーズ V5 インスタンスタイプの代わりに、Dsv3 シリーズ V3 インスタンスタイプを使用することを推奨します。V5 インスタンスタイプには互換性がない可能性があるためです。
- [ゲートウェイタイプ（Gateway Type）]：[イングレス（Ingress）] または [エグレス（Egress）] を選択します。

  （注）
  East-West ネットフローがある場合は、[エグレス（Egress）] を選択します。
- [インスタンスの最小数（Minimum Instances）]：展開するインスタンスの最小数を選択します。

- [インスタンスの最大数（Minimum Instances）]：展開するインスタンスの最大数を選択します。これは、各可用性ゾーンで自動スケーリングに使用される最大数です。
- [ヘルスチェックポート（HealthCheck Port）]：デフォルトは 65534 です。Multicloud Defense ロードバランサがインスタンスの正常性をチェックするために使用するポート番号です。インスタンスに割り当てられたデータパス セキュリティ グループは、このポートのトラフィックを許可する必要があります。
- （任意）[パケットキャプチャプロファイル（Packet Capture Profile）]：脅威およびフロー PCAP のパケット キャプチャ プロファイル。
- （任意）[診断プロファイル（Diagnostics Profile）]：テクニカルサポート情報を保存するために使用される診断プロファイル。
- （任意）[ログプロファイル（Log Profile）]：イベント/ログを SIEM に転送するために使用されるログ転送プロファイル。
- （任意）**NTP プロファイル（NTP Profile）**：時刻同期用の Network Time Protocol（NTP）。
- （任意）[BGPプロファイル（BGP profile）]：VPN 接続をサポートするために使用されるボーダー ゲートウェイ プロトコル（BGP）。サイト間 VPN トンネルを使用する場合は、Multicloud Defense Gatewayこのプロファイルを**必ず**含める必要があります。

ステップ 6 [Next] をクリックします。

ステップ 7 次のパラメータを指定します。

- [セキュリティ（Security）]：[エグレス（Egress）] または [イングレス（Ingress）] を選択します。

  （注）
  East-West ネットフローがある場合は、[エグレス（Egress）] を選択します。

- [ゲートウェイイメージ（Gateway Image）]：展開するイメージ。
- [ポリシールールセット（Policy Ruleset）]：このゲートウェイに関連付けるポリシールールセットを選択します。
- [リージョン（Region）]：このゲートウェイを展開するリージョンを選択します。
- [リソースグループ（Resource Groups）]：ゲートウェイを関連付けるリソースグループを選択します。
- [SSH公開キー（SSH Public Key）]：SSH 公開キーを貼り付けます。コントローラは、このキーを使用して、展開されたゲートウェイインスタンスの CLI にアクセスしてデバッグおよびモニタリングを行います。
- [VNet ID]：ゲートウェイに関連付ける VNet を選択します。
- （Azure のみ）[ユーザー割り当てアイデンティティID（User Assigned Identity ID）]：このゲートウェイに関連付けるクラウドサービスプロバイダーのアイデンティティを入力します。ユーザー割り当てマネージド ID は、リソースのクレデンシャルの代わりに使用できます。Azure サービスの場合、

これらのアイデンティティは Azure Key Vault に保存されている秘密キーにアクセスしたり、Azure Blob Storage に PCAP ファイルを書き込むことができます。

- [管理セキュリティグループ（Mgmt. Security Group）]：管理インターフェイスに関連付けるセキュリティグループを選択します。
- [データパスセキュリティグループ（Datapath Security Group）]：データパスインターフェイスに関連付けるセキュリティグループを選択します。
- [ディスク暗号化（Disk Encryption）]：ドロップダウンメニューから適切なオプションを選択します。お客様が管理する暗号化キーを使用している場合は、暗号化キーのリソース ID を入力します。

ステップ 8 [可用性ゾーン（Availability Zone）]、[管理サブネット（Mgmt Subnet）]、および [データパスサブネット（DatapathSubnet）] を選択します。使用可能なサブネットは、上記で選択した VPC または VNet に基づきます。高可用性を実現するために、ゲートウェイインスタンスを複数の可用性ゾーンに展開できます。プラスボタンをクリックして新しい可用性ゾーンを追加し、選択したゾーンのパラメータを選択します。一部のクラウドサービスプロバイダーのリージョンは、複数の可用性ゾーンをサポートしていません。このようなリージョンでは、ゲートウェイインスタンスは単一のゾーンにのみ展開されます。

（注）
ゲートウェイがハブモードで展開されている場合、最初の展開後に可用性ゾーンを編集することはできません。展開する前にゾーンを再確認してください。

ステップ 9 （Azure のみ、任意）アプリケーションと同じ VNet で Multicloud Defense Gateway を使用して分散モデルで展開する場合は、次の手順を実行してください。

- Azure ポータルでルートテーブルを追加し、そのルートテーブルをすべてのサブネットに関連付けます。
- **next-hop** をゲートウェイ ネットワーク ロード バランサの IP アドレスとして、0.0.0.0/0 のデフォルトルートを追加します。

ステップ 10 [次へ（Next）] をクリックして、[詳細設定（Advanced Settings）] を表示します。

ステップ 11 デフォルトで、Multicloud Defense Gateway は使用可能なルータのパブリック IP の使用を有効にします。有効にしない場合は、[パブリックIPを無効化（Disable Public IP）] チェックボックスをオンにします。

ステップ 12 （AWS および Azure のみ）**ロードバランサをアタッチ**します。[ロードバランサの追加（Add Load Balancer）] をクリックして、カスタムロードバランサの行を作成します。不要な行を選択して **削除**をクリックすることで、不要な行を削除することもできます。

a) [ロードバランサ（Load Balancer）] ドロップダウンを展開して、AWS または Azure クラウド サービス プロバイダーからロードバランサを選択します。
b) [バックエンドプール（Backend Pool）] ドロップダウンを展開して、ゲートウェイに関連付けるバックエンドプールを選択します。

ステップ 13 [保存（Save）] をクリックします。

次のタスク

Multicloud Defense がゲートウェイを展開します。

スポーク VPC/VNet を保護する前に、少なくとも 1 つのルールセットをゲートウェイにアタッチする**必要があります**。詳細については、ルールセットとルールセットグループを参照してください。

Firewall Threat Defense 仮想ゲートウェイの作成

次の手順を使用して、Firewall Threat Defense 仮想ゲートウェイを作成します。

入力、出力、および East-West トラフィック用に、AWS、Azure、または GCP の Firewall Threat Defense 仮想ゲートウェイを作成します。

始める前に

ゲートウェイを作成する前に、情報または環境の制限事項について はじめる前に （25 ページ） を確認してください。

手順

ステップ 1 **[インフラストラクチャ（Infrastructure）]** > > **[ゲートウェイ（Gateways）]** > > **[ゲートウェイ（Gateways）]** > にアクセスします。

ステップ 2 [ゲートウェイの追加（Add Gateway）] をクリックします。

ステップ 3 ゲートウェイを追加するクラウド サービス プロバイダーを選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 次の**ゲートウェイ情報**を入力します。機能を有効にしていない場合、「ゲートウェイタイプ」のオプションは異なる場合があるため、「ゲートウェイの追加」を参照してください。

- **アカウント（Account）** - ドロップダウンメニューを展開し、Multicloud Defense Controller にすでに接続されているクラウド サービス プロバイダーのアカウントを選択します。現時点では、AWS および Azure アカウントのみがサポートされています。
- **ゲートウェイタイプ（Gateway Type）** - ドロップダウンメニューを展開し、**[FTDv ゲートウェイ]**を選択します。
- **名前（Name）** - Multicloud Defense Controller に表示されるゲートウェイの名前を入力します。
- （任意）**説明（Description）** - クラウドゲートウェイの説明を入力します。このゲートウェイを、同様の名前または目的を持つ可能性のある他のゲートウェイと区別するために、一意の識別子を使用することを推奨します。
- [インスタンスタイプ（Instance Type）]：クラウド サービス プロバイダーのタイプを選択します。この選択は、前述の [Account] フィールドで選択したクラウド サービス プロバイダーと一致する必要があります。使用しているクラウドサービスプロバイダーに応じて、インスタンスに複数のバリエーションが存在する場合があることに注意してください。

- [インスタンスの最小数（Minimum Instances）]：展開するインスタンスの最小数を選択します。
- [インスタンスの最大数（Minimum Instances）]：展開するインスタンスの最大数を選択します。これは、各可用性ゾーンで自動スケーリングに使用される最大数です。
- [ヘルスチェックポート（HealthCheck Port）]：デフォルトは 65534 です。Multicloud Defense ロードバランサがインスタンスの正常性をチェックするために使用するポート番号です。インスタンスに割り当てられたデータパスセキュリティグループは、このポートのトラフィックを許可する必要があります。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 必要に応じて、次のパラメータを指定します。このゲートウェイ用に作成したサービス VPC の設定に基づいて、複数のフィールドが自動的に入力されることに注意してください。詳細については、サービス VPC または VNet の作成 （19 ページ）を参照してください。

- **セキュリティ（Security）** - 要件に基づいて、[Ingress]、[Egress]、または[East-West]を選択します。
  - AWS - 入力、出力、または East-West を選択できます。
  - Azure - 入力または East-West および出力を選択できます。
  - GCP - 入力または East-West および出力を選択できます。
- **FTDvバージョン（FTDv Version）** - Multicloud Defense がデバイスを作成して展開するときに、FTDv デバイスで実行するソフトウェアのバージョンを選択します。
- **ポリシールールセット（Policy Ruleset）** - このゲートウェイに関連付けるポリシールールセットを選択します。アクセスポリシーの準備がまだできない場合は、デフォルトポリシーを使用するか、このメニューから新しいポリシーを作成できます。
- **管理者パスワード（Admin Password）** - FTDv デバイスの管理者のパスワードを入力します。画面に表示される指示に従って、パスワードを変更します。
- **ライセンスモデル（License Model）** - トグルをクリックして、優先するライセンスモデルを強調表示します。
  - **Multicloud Defense ライセンス（Licensing）** - Multicloud Defense ライセンスモデルでは、Cisco スマートライセンスアカウントで個々の機能ライセンスを購入せずに、すべての Firewall Threat Defense 仮想機能を使用できます。
  - **スマートライセンス（Smart Licensing）** - ライセンスを購入する予定の場合、または Cisco スマートアカウントで購入した未使用のライセンスがある場合は、このオプションを選択します。
  - **ペイアズユーゴー（PAYG）ライセンス（Pay-As-You-Go (PAYG) Licensing）** - ライセンスをオンデマンドで使用する場合は、このオプションを選択します。
- **パフォーマンス階層（Performance Tier）** - ドロップダウンメニューを展開し、デバイスに適切なパフォーマンス階層を選択します。FTDv50 が自動的に選択されていることに注意してください。「ライセンス」に記載されている階層を参照してください。

- **ライセンスタイプ（License Types）** - ドロップダウンメニューを展開し、購入済みまたは今後購入する適切なライセンスタイプを選択します。**基本**ライセンスは自動的に選択されます。「ライセンス」に記載されているさまざまなライセンスタイプを参照してください。
- [リージョン（Region）]：このゲートウェイを展開するリージョンを選択します。
- **VPC/VNet ID** - ゲートウェイに関連付けるサービス VPC または VNet の ID を選択します。この手順でサービス VPC または VNet を特定すると、管理およびデータパス セキュリティ グループ、ならびに可用性ゾーンが確認されます。これらの値を変更するには、新しいサービス VPC を作成し、このゲートウェイに追加します。
- (AWS のみ) **キーペア（Key Pair）** - ドロップダウンメニューを展開し、前の画面で選択したクラウドアカウントに関連付けられているキーペアを選択します。
- (Azure および GCP のみ) **キーの選択（Key Selection）** - キーのタイプ、サイズ、アクティベーション日、および期限日を選択します。**SSH 公開キー**または**SSH キーペア**のいずれかを選択します。選択内容に基づいて、プロンプトが表示されたらテキストフィールドに適切な情報を入力します。
- [リソースグループ（Resource Groups）]：ゲートウェイを関連付けるリソースグループを選択します。
- (AWS のみ) **ゲートウェイ IAM ロール（Gateway IAM Role）** - ドロップダウンメニューを展開し、ゲートウェイが AWS アカウントで READ および WRITE 操作を実行できる IAM ロールを選択します。ゲートウェイを保存して展開すると、Multicloud Defense がこのロールを作成します。
- （Azure のみ）[ユーザー割り当てアイデンティティID（User Assigned Identity ID）]：このゲートウェイに関連付けるクラウドサービスプロバイダーのアイデンティティを入力します。ユーザー割り当てマネージドIDは、リソースのクレデンシャルの代わりに使用できます。ユーザー割り当てマネージド ID は、Azure Key Vault に保存されている秘密キーなど、Azure サービス向けに使用したり、Azure Blob Storage に PCAP ファイルを書き込んだりするために使用することができます。
- [管理セキュリティグループ（Mgmt. Security Group）]：管理インターフェイスに関連付けるセキュリティグループを選択します。
- **データパスセキュリティグループ 1（DataPath Security Group 1）**：データパス 1 インターフェイスに関連付けるセキュリティグループを選択します。
- **データパスセキュリティグループ 2（DataPath Security Group 2）** - データパス 2 インターフェイスに関連付けるセキュリティグループを選択します。
- （GCP のみ） **データパス VPC（Datapath VPC）** - VPC を選択します。
- （GCP のみ） **データパスネットワークタグ 1（Datapath Network Tag 1）** - ドロップダウンリストからセキュリティグループを選択します。
- （GCP のみ） **データパスネットワークタグ 2（Datapath Network Tag 2）** - ドロップダウンリストからセキュリティグループを選択します。
- （GCP のみ） **管理 VPC（Management VPC）** - ドロップダウンリストから管理 VPC を選択します。
- （GCP のみ） **管理ネットワークタグ（Management Network Tag）** - ドロップダウンリストから管理ネットワークタグを選択します。

- （AWS のみ） **EBS 暗号化（EBS Encryption）** - ドロップダウンメニューを展開し、特定の AWS アカウントに適切な EBS 暗号化を選択します。
- (Azure) **ディスク暗号化（Disk Encryption）** - ドロップダウンメニューから適切なオプションを選択します。カスタマーマネージド暗号化キーの場合、ユーザーは暗号化キーのリソース ID を入力する必要があります。

ステップ 8 **インスタンスの詳細**は、選択した VPC に基づいて自動入力されます。ゲートウェイを展開する前に、VPC 設定を確認してください。[次へ（Next）] をクリックします。

ステップ 9 （オプション）**[Advanced Settings]** ウィンドウで、**[Disable Public IP]** チェックボックスをオンにします。この手順を無効にすると、外部の脅威にさらされるネットワークのリスクが軽減されます。プライベート IP アドレスは、不正アクセスや潜在的な攻撃から保護するのに役立ちます。また、内部トラフィックの制御が改善されます。

ステップ 10 [次へ（Next）] をクリックします。

ステップ 11 ゲートウェイの設定を見直します。ゲートウェイに問題がなく、これを展開する場合は、**[Finish]**をクリックします。設定を変更する場合は、**[Back]** をクリックします。

次のタスク

この手順の最後に **[Finish]** をクリックすると、ゲートウェイが展開されます。ゲートウェイの作成と展開には最大 30 分かかる場合があります。Multicloud Defense はゲートウェイを展開しますが、便宜上ゲートウェイインスタンスを クラウド提供型 Firewall Management Center に登録し、適切なインターフェイスのサブネットとセキュリティグループを作成して適用し、この手順で選択したアクセスポリシーを適用します。

ゲートウェイが展開され、クラウド提供型 Firewall Management Center に表示されたら、ポリシーに必要な更新または含めることを推奨します。ポリシーに関連付けられているネットワークオブジェクトは共有され、可視性のために Multicloud Defense の [Object] ページに **[Network]** オブジェクトとして表示されます。ポリシーのオーケストレーションと管理はクラウド提供型 Firewall Management Center を介して実行されます。

ゲートウェイが展開されたら、次のアクションを強く推奨します：

- VPC のセキュリティを確保し保護します。Firewall Threat Defense 仮想のスポーク VPC を保護すると、拡張性と分離を維持しながら、セキュリティが集中します。
- クラウド提供型 Firewall Management Center アカウントにアクセスし、アクセス制御ポリシーを変更してください。詳細については、「アクセス制御の概要」を参照してください。
- クラウド提供型 Firewall Management Center で NAT ポリシーを作成します。詳細については、『クラウド提供型 Firewall Management Center 設定ガイド』を参照してください。

Multicloud Defense Gateway の編集

ゲートウェイは、有効か無効かにかかわらず、どの状態でも編集できます。

（注） FTDv デバイスに接続されているゲートウェイを編集する場合、ライセンスモデルは変更できず、スマートライセンスのパフォーマンス階層のみ変更できます。

既存の Multicloud Defense Gateway を編集するには、次の手順を実行します。

手順

ステップ 1 にアクセスします。

ステップ 2 編集する Multicloud Defense Gateway をテーブルで選択し、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を展開し、[編集（Edit）] をクリックします。

ステップ 4 必要に応じてゲートウェイ設定を変更します。

FTDvデバイスに関連付けられているゲートウェイのライセンスパフォーマンス階層を変更する場合、既存のインスタンスが クラウド提供型 Firewall Management Center で自動的に更新されることに注意してください。Multicloud Defense は、新しいライセンス設定をサポートする新しいインスタンスを作成し、クラウド提供型 Firewall Management Center と同期します。

ステップ 5 [保存（Save）] をクリックして、変更を確定します。または、[キャンセル（Cancel）] をクリックして変更を終了します。

Multicloud Defense Gatewayのアップグレード

Multicloud Defense Gateway は、自動スケーリングで自己修復を行うサービスとしてのプラットフォーム（PaaS）として機能し、インライン ネットワーク ベースのセキュリティ施行ノードとして機能します。従来のファイアウォールとは異なり、Multicloud Defense では、仮想ファイアウォールの構築、高可用性セットアップの設定、またはソフトウェアインストールの管理を行う必要がありません。

Multicloud Defense Gateway インスタンスは高度に最適化されたソフトウェア上で動作し、効率的なトラフィック処理と高度なセキュリティの適用のための単一パスのデータパスパイプラインを組み込んでいます。各ゲートウェイインスタンスは、ポリシーの適用を担当する「ワーカー」プロセス、トラフィック分散とセッション管理を行う「ディストリビュータ」プロセス、コントローラと通信する「エージェント」プロセスの 3 つのコアプロセスで構成されます。ゲートウェイインスタンスは、「データパスの再起動」のために「サービス中」にシームレスに移行できるため、トラフィックフローを中断することなくスムーズなアップグレードが可能になります。

新しいインスタンスは、新しいイメージでスピンアップされます。インスタンスが完全に起動すると、ロードバランサ（ゲートウェイインスタンスへのフローのレイヤ 4 スプレイヤ）のターゲットプールに配置されます。古いインスタンスは、それらを通過する既存のフローに対してフロードレインモードまたはフロータイムアウトモードになります。新しいフローは新し

いインスタンスにヒットします。タイムアウト（Azure）またはフローがドレイン（AWS）されると、古いインスタンスはコントローラによって取得されます。

次の作業を実行するには、次の手順を使用します。

手順

ステップ 1 に移動します。

ステップ 2 アップグレードするゲートウェイのチェックボックスをオンにします。この時点で選択できるのは 1 つのみです。

ステップ 3 **[アクション（Actions）] > [アップグレード（Upgrade）]**の順に選択します。

ステップ 4 [ゲートウェイイメージ（Gateway Image）] リストから、対象のイメージを選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 クラウドサービスプロバイダーに、アップグレードに必要なリソースが割り当てられていることを確認します。

ステップ 7 リソースの割り当てが十分な場合は、[はい（Yes）]をクリックします。リソースの割り当てが不十分な場合は [いいえ（No）] をクリックし、クラウド サービス プロバイダーのリソースの割り当てを増やしてから、戻ってアップグレードを続行します。

（注）
アップグレードの進行状況と、ゲートウェイのインスタンス情報から作成されている新しいゲートウェイインスタンスを表示できます。ゲートウェイを選択し、[詳細（Details）]ペインで[インスタンス（Instances）]を表示します。

Firewall Threat Defense 仮想デバイスのアップグレード

この手順では、クラウド サービス プロバイダーおよび Multicloud Defense Gateway に関連付けられている Firewall Threat Defense 仮想デバイスをアップグレードする方法について説明します。Multicloud Defense Controller を使用して FTDv デバイスをアップグレードすることを強く推奨します。

手順

ステップ 1 **[Infrastructure] > [Gateways] > [Gateways]**に移動し、Firewall Threat Defense 仮想デバイスに関連付けられているゲートウェイを選択します。

ステップ 2 **[Actions]** をクリックし、**[Upgrade]** を選択します。

ステップ 3 **[FTDv Version]** ドロップダウンメニューを展開し、アップグレードするバージョンを選択します。バージョンが表示されていない場合は、ドロップダウンメニューの右側にある更新アイコンをクリックするか、Cisco

Secure Firewall Threat Defense リリースノートを使用して、新しいバージョンが公開されているかどうかを確認します。

ステップ 4 **[Save]**をクリックします。Multicloud Defense はアップグレードを開始し、そのゲートウェイを再展開します。

Multicloud Defense Gateway の中止

現在進行中のゲートウェイの更新を実行している Multicloud Defense Gateway のみを中止できます。

既存の Multicloud Defense Gatewayを中止するには、次の手順を実行します。

手順

ステップ 1 に移動します。

ステップ 2 中止する Multicloud Defense Gateway をテーブルで選択し、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を展開し、[中止（Abort）] をクリックします。

ステップ 4 [はい（Yes）]をクリックして、ゲートウェイを中止することを確認します。アクションを取り消すには、[いいえ（No）] をクリックします。

Multicloud Defense Gateway の有効化

無効になっているゲートウェイのみを有効にできます。を有効にするには、次の手順を実行します。

手順

ステップ 1 に移動します。

ステップ 2 有効にする Multicloud Defense Gateway をテーブルで選択し、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を展開し、[有効化（Enable）] をクリックします。

ステップ 4 Multicloud Defense はゲートウェイの設定を検証します。検証に成功すると、現在のリソースとアップグレードに必要なリソースのテーブルが確認用に生成されます。ゲートウェイリソースの割り当てを承認する場合は、[はい（Yes）] をクリックしてアクションを確認します。

次のタスク

Multicloud Defense Gateway が正常に有効化されるまで数分待ちます。

Multicloud Defense Gateway を無効にし、それに関連付けられているサイト間 VPN トンネルを削除した場合は、新しいサイト間 VPNトンネル接続を作成するか、以前の VPNトンネル接続を再作成してゲートウェイに追加する**必要があります**。ゲートウェイを無効にすると、Multicloud Defense は VPN トンネルに関連付けられたパブリック IP アドレスを削除します。ゲートウェイインスタンスの新しいIPを確立するには、新しいトンネル接続を作成する必要があります。

Multicloud Defense Gateway の無効化

Multicloud Defense Gateway は、現在有効な場合にのみ無効化できます。すでに無効になっているゲートウェイを無効化することはできません。

Multicloud Defense Gateway を無効にするには、次の手順を実行します。

手順

ステップ 1 に移動します。

ステップ 2 無効にする Multicloud Defense Gateway をテーブルで選択し、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を展開し、[無効化（Disable）] をクリックします。

ステップ 4 [はい（Yes）]をクリックして、ゲートウェイを無効化することを確認します。このアクションを取り消すには、[いいえ（No）] をクリックします。

次のタスク

ゲートウェイが正常に無効化されるまで数分待ちます。

ゲートウェイを完全に無効化するには、ゲートウェイに関連付けられているサイト間 VPN トンネルを削除する**必要があります**。

Multicloud Defense Gateway のエクスポート

Multicloud Defense Gateway の設定をエクスポートするには、次の手順を実行します。

手順

ステップ 1 に移動します。

ステップ 2 エクスポートする Multicloud Defense Gateway をテーブルで選択し、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を展開し、[エクスポート（Export）]をクリックします。

ステップ 4 Multicloud Defense でエクスポートウィザードが生成されます。

ステップ 5 [ダウンロード（Download）] をクリックして Terraform をローカルにダウンロードするか、下にスクロールして [コードのコピー（Copy Code）] をクリックして JSON リソースをコピーします。

ステップ 6 Terraform スクリプトに手動で貼り付けます。

ステップ 7 Terraform プロンプト内で、ウィンドウの下半分に表示されるコマンドを実行します：`terraform import "ciscomcd_gateway"."object-name" <object name>`。

ステップ 8 Terraform プロンプト内のプロンプトに従って、タスクを完了します。[閉じる（Close）] をクリックして Multicloud Defense のエクスポートウィンドウを閉じます。ダッシュボードではこれ以上の手順はありません。

Multicloud Defense Gatewayの削除

Multicloud Defense Gateway を削除するには、次の手順を実行します。このアクションは、ゲートウェイの無効化とは異なることに注意してください。

手順

ステップ 1 に移動します。

ステップ 2 削除する Multicloud Defense Gateway をテーブルで選択し、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を展開し、[削除（Delete）] をクリックします。

ステップ 4 アクションを確認し、[Yes] をクリックします。削除アクションを取り消すには、[キャンセル（Cancel）] をクリックします。

次のタスク

このゲートウェイがゲートウェイテーブルから正常に削除された後で、このゲートウェイに関連付けられていたサイト間 VPN トンネル接続を削除することを強くお勧めします。

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。