Azure 仮想 WAN の仮想ネットワーク接続を構成する

仮想 WAN の概要

Azure クラウドサービスを使用する場合、仮想 WAN（VWAN）を作成して、オンプレミスのネットワーク、ブランチオフィス、およびリモートユーザー間のネットワーク接続をオーケストレーションおよび簡素化できます。サービス VNet と仮想ハブ（vHub）間の仮想ネットワーク接続とルート伝達をオーケストレーションすることで、Multicloud Defense を Azure VWAN と統合できます。

通常、vHub 内では、Multicloud Defense はネットワーク仮想アプライアンス（NVA）としてサポートされていません。代わりに、VWAN ルートオーケストレーションを使用してこれに対処できます。Multicloud Defense を使用して Azure 上のアプリケーションを保護するには、VWAN 内のサービス VNet から vHub への仮想ネットワーク接続の作成をオーケストレーションできます。vHub と Multicloud Defense の間でルートを伝播できます。Multicloud Defense は出力モードでのみ VWAN をサポートします。Azure VWAN は Multicloud Defense ゲートウェイ でのみサポートされていることにご注意ください。セキュアなハブ間でのトラフィックのルーティングに問題があるため、Azure では VWAN の East-West トラフィックはサポートされていません。

Azure vHub への Virtual WAN 接続のガイドライン

前提条件

- VWAN および vHub を含む Azure サブスクリプションを設定する必要があります。
- サービス VNet とスポーク VNet は、Azure で設定する必要があります。

- Multicloud Defense Gateway は、サービス VNet に展開する必要があります。
- Azure で仮想ネットワーク接続とルートテーブルを作成して管理するには、権限が利用可能である必要があります。
- vHub 接続を有効化および無効化するには、権限が利用可能である必要があります。

制限事項

- Multicloud Defense は vHub 内の NVA としてサポートされていません。
- クラスレスインタードメインルーティング（CIDR）の選択は、VNet の作成中ではなく、編集フェーズ中にのみ使用できます。
- ルート伝達は、出力または入力ゲートウェイの設定に依存します。

Virtual WAN アタッチメントを使用したサービス VPC の作成

アカウントを保護するときに、**簡単なセットアップ**ウィザードを使用して、VWAN アタッチメントを使用してサービス VPC を作成できます。詳細については、「集中型モデル：VPC または VNet の追加」を参照してください。

次の手順を使用して、サービス VPC を作成し、VWAN をアタッチします。

手順

ステップ 1 Multicloud Defense コントローラから、**[インフラストラクチャ（Infrastructure）]** > > **[ゲートウェイ（Gateways）]** > > **[VPC/VNet（VPC/VNets）]** > に移動します。

ステップ 2 **[Create Service VPC/VNet]** をクリックして、サービス VPC を作成します。

ステップ 3 名前を入力します。

ステップ 4 [Region]ドロップダウンリストから、リージョンを選択します。

ステップ 5 **[CSP Account]** ドロップダウンリストから、アカウントを選択します。

ステップ 6 **[CIDR Block]** の詳細を入力します。

ステップ 7 **[Availability Zones]** ドロップダウンリストから、ゾーンを選択します。

ステップ 8 **[Resource Group]** ドロップダウンリストから、リソースグループを選択します。

ステップ 9 **[Use NAT Gateway]** チェックボックスをオンにして、NAT ゲートウェイを経由してトラフィックを誘導します。

ステップ 10 **[vWAN Attachment]** セクションで、トグルを **[Enabled]** に設定します。

ステップ 11 **[vHub]** ドロップダウンリストから、ハブを選択します。

ステップ 12 **[Associate Route Table]** ドロップダウンリストから、関連付けるルートテーブルを選択します。

ステップ 13 **[Propagate Route Tables]** ドロップダウンリストから、伝播するルートテーブルを選択します。

ステップ 14 [保存（Save）] をクリックします。

サービス VPC は、Azure VWAN への vHub 接続を使用して作成されます。Azure アカウントに加えられた構成の変更を表示することもできます。

（注）
Multicloud Defense でサービス VPC を削除すると、VWAN と Azure サービス VPC 間の vHub 接続も削除されます。

Virtual WAN アタッチメントがあるサービス VPC の変更

手順

ステップ 1 Multicloud Defense コントローラから、**[インフラストラクチャ（Infrastructure）]** > > **[ゲートウェイ（Gateways）]** > > **[VPC/VNet（VPC/VNets）]** > に移動します。

ステップ 2 リストから編集するサービス VPC を選択します。

ステップ 3 [編集（Edit）] をクリックします。

ステップ 4 **[vWAN Attachment]** セクションで、トグルを **[Enabled]** に設定します。

ステップ 5 **[vHub]** ドロップダウンリストから、ハブを選択します。

ステップ 6 **[Associated Route Table]** ドロップダウンリストからルートテーブルを選択します。

ステップ 7 **[Propagate Route Tables]** ドロップダウンリストからルートテーブルを選択します。

ステップ 8 すべてのスポーク CIDR を vHub に伝播するには、トグルを **[Always]** に設定します。

（注）
ルートテーブルに複数のスポーク VPC を追加するには、リストビルダーを使用して、スポーク VPC を **[Available]** セクションから **[Selected]** セクションに移動します。VPC を **[Selected]** セクションに移動すると、VPC が追加されます。

ステップ 9 [保存（Save）] をクリックします。

サービス VPC は、Azure の vHub およびスポーク VPC を含む VWAN に接続します。ルートテーブルに加えられた変更は、Azureでも更新されることに注意してください。

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。