Azure Virtual Network の基礎

100 XP

8 分

Tailwind Traders 社のオンプレミスのデータセンターは維持する予定ですが、Azure でホストされる仮想マシン (VM) を使用して、ピーク時のトラフィックをオフロードしたいと考えています。 既存の IP アドレス指定スキームとネットワーク アプライアンスを維持しながら、すべてのデータ転送をセキュリティで保護することを望んでいます。

仮想ネットワークで Azure Virtual Network を使用すると、目標の達成に役立ちます。

Azure 仮想ネットワークとは

"*Azure* 仮想ネットワーク" を使用すると、VM、Web アプリ、データベースなどの Azure リソースの相互通信、インターネット上のユーザーとの通信、オンプレミスのクライアント コンピューターとの通信が可能になります。 Azure ネットワークは、他の Azure リソースとリンクするリソースのセットと見なすことができます。

Azure 仮想ネットワークには、次の主要なネットワーク機能が含まれます。

- 分離とセグメント化
- インターネット通信
- Azure リソース間の通信
- オンプレミス リソースとの通信
- ネットワーク トラフィックのルーティング
- ネットワーク トラフィックのフィルター処理
- 仮想ネットワークの接続

仮想マシンのネットワーク構成

分離とセグメント化

Virtual Network では、分離された仮想ネットワークを複数作成できます。 仮想ネットワークを設定するときに、パブリックまたはプライベートの IP アドレス範囲のいずれかを使用して、プライベート IP アドレス空間を定義します。 その IP アドレス空間をサブネットに分割し、定義したアドレス空間の一部をそれぞれの名前付きサブネットに割り当てることができます。

名前解決には、Azure に組み込まれている名前解決サービスを使用できます。 内部または外部の DNS サーバーを使用するように仮想ネットワークを構成することもできます。

インターネット通信

Azure 内の VM は、既定でインターネットに接続できます。 パブリック IP アドレスまたはパブリック ロード バランサーを定義することで、インターネットからの受信接続を有効にできます。 VM 管理には、Azure CLI、リモート デスクトップ プロトコル、または Secure Shell 経由で接続できます。

Azure リソース間の通信

Azure リソースが相互に安全に通信できるようにする必要があります。 次の 2 つの方法のいずれかでこれを実現します。

- **仮想ネットワーク**

  仮想ネットワークでは、VM だけではなく、App Service Environment for Power Apps、Azure Kubernetes Service、Azure 仮想マシン スケール セットなどの他の Azure リソースにも接続できます。

- **サービス エンドポイント**

  サービス エンドポイントを使用して、Azure SQL データベースやストレージ アカウントなど、他の Azure リソースの種類に接続することができます。 この方法を使用すると、複数の Azure リソースを仮想ネットワークにリンクすることができ、セキュリティの向上とリソース間の最適なルーティングを実現できます。

オンプレミス リソースとの通信

Azure 仮想ネットワークを使用すると、オンプレミス環境と Azure サブスクリプション内でリソースをリンクできます。 実質的に、ローカルとクラウドの環境にまたがるネットワークを作成できます。 この接続を実現するためのメカニズムが 3 つあります。

- **ポイント対サイト仮想プライベート ネットワーク**

  仮想プライベート ネットワーク (VPN) 接続に対する一般的なアプローチは、組織外のコンピューターから企業ネットワークに戻ることです。 ここでは、クライアント コンピューターから、暗号化された VPN 接続が開始され、そのコンピューターが Azure 仮想ネットワークに接続されます。

- **サイト間仮想プライベート ネットワーク**

  サイト間 VPN を使用して、オンプレミスの VPN デバイスまたはゲートウェイを、仮想ネットワーク内の Azure VPN ゲートウェイにリンクします。 実際には、Azure 内のデバイスはローカル ネットワーク上にあるものとして表示できます。 接続は暗号化され、インターネット経由で動作します。

- **Azure ExpressRoute**

より広い帯域幅とさらに高いレベルのセキュリティが必要な環境には、Azure ExpressRoute が最適な方法です。 ExpressRoute では、インターネットを経由しない Azure への専用プライベート接続が用意されます (ExpressRoute の詳細については、このモジュールの後半にある別のユニットで学習します)。

ネットワーク トラフィックのルーティング

既定では、Azure のトラフィックは、接続されている仮想ネットワークのサブネット、オンプレミス ネットワーク、およびインターネットとの間でルーティングされます。 次のように、ルーティングの制御と各設定のオーバーライドを実行することもできます。

- **ルート テーブル**

  ルート テーブルを使用して、トラフィックの転送先に関する規則を定義できます。 サブネット間でパケットがルーティングされる方法を制御する、カスタム ルート テーブルを作成できます。

- **Border Gateway Protocol**

  Border Gateway Protocol (BGP) は、Azure VPN Gateway または ExpressRoute と共に動作して、オンプレミスの BGP ルートを Azure 仮想ネットワークに反映させます。

ネットワーク トラフィックのフィルター処理

Azure 仮想ネットワークでは、次の方法を使用してサブネット間のトラフィックをフィルター処理できます。

- **ネットワーク セキュリティ グループ**

  ネットワーク セキュリティ グループは、受信と送信に関するセキュリティ規則を複数含めることができる Azure リソースです。 送信元と送信先の IP アドレス、ポート、プロトコルなどの要素に基づいて、トラフィックを許可またはブロックする各規則を定義できます。

- **ネットワーク仮想アプライアンス**

  ネットワーク仮想アプライアンスは、堅牢化されたネットワーク アプライアンスに対応する特殊な VM です。 ネットワーク仮想アプライアンスにより、ファイアウォールの実行やワイド エリア ネットワーク (WAN) の最適化の実行などの特定のネットワーク機能が実行されます。

仮想ネットワークの接続

仮想ネットワークの "ピアリング" を使用して、仮想ネットワーク同士をリンクできます。 ピアリングを使用すると、各仮想ネットワーク内のリソースを相互に通信させることができます。 これ

らの仮想ネットワークを異なるリージョンに配置し、Azure を通じてグローバルに相互接続されたネットワークを作成できます。

UDR はユーザー定義のルーティングです。 UDR は、Azure Virtual Network にとって重要な更新です。これによりネットワーク管理者は、VNet 内のサブネット間、および Vnet 間でルーティング テーブルを制御できるようになり、ネットワーク トラフィック フローをより細かく制御できるようになります。