Azure VPN Gateway の基礎

100 XP

10 分

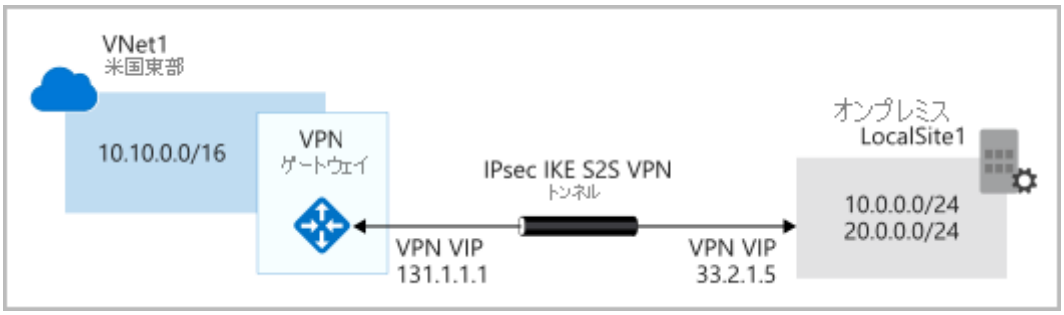
VPN では、別のネットワーク内で暗号化されたトンネルが使用されます。 それらは通常、信頼された 2 つ以上のプライベート ネットワークを、信頼されていないネットワーク (通常はパブリック インターネット) を介して相互に接続するためにデプロイされます。 傍受やその他の攻撃を防ぐために、信頼されていないネットワークを通過中のトラフィックは暗号化されます。

Tailwind Traders のシナリオでは、VPN を使用して、複数ある支社の場所間で機密情報を共有できます。 たとえば、北米の東海岸地域にある支社が会社の非公開の顧客データにアクセスする必要があるとします。このデータは、西海岸地域に物理的に配置されているサーバーに格納されています。 東海岸の支社を西海岸のサーバーに接続する VPN により、会社は非公開の顧客データに安全にアクセスできます。

VPN ゲートウェイ

VPN ゲートウェイは仮想ネットワーク ゲートウェイの一種です。 Azure Virtual Network インスタンスに Azure VPN Gateway インスタンスがデプロイされ、次の接続が可能になります。

- オンプレミス データセンターを "サイト間" 接続を介して仮想ネットワークに接続する。
- 個々のデバイスを "ポイント対サイト" 接続を介して仮想ネットワークに接続する。
- 仮想ネットワークを "ネットワーク対ネットワーク" 接続を介して他の仮想ネットワークに接続する。



転送されるデータはすべて、インターネットを通過するときに、プライベート トンネル内で暗号化されます。 各仮想ネットワークにデプロイできるのは 1 つの VPN ゲートウェイのみですが、1 つのゲートウェイを使用して、他の仮想ネットワークやオンプレミス データセンターなどの複数の場所に接続することができます。

VPN ゲートウェイをデプロイする場合は、VPN の種類として、"ポリシーベース" または"ルートベース" のいずれかを指定します。 これら 2 種類の VPN の主な違いは、暗号化するトラフィックを指定する方法です。 Azure では、どちらの種類の VPN ゲートウェイでも、唯一の認証方法として事前共有キーが使用されます。 また、どちらの種類も、バージョン 1 またはバージョン 2 のインターネット キー交換とインターネット プロトコル セキュリティ (IPSec) に依存しています。 IKE は 2 つのエンドポイント間のセキュリティ アソシエーション (暗号化の契約) を設定するために使

用されます。 そして、このアソシエーションは IPSec スイートに渡され、それにより VPN トンネル内でカプセル化されるデータ パケットの暗号化と暗号化解除が行われます。

ポリシーベースの VPN

ポリシーベースの VPN ゲートウェイでは、各トンネル間で暗号化する必要があるパケットの IP アドレスを静的に指定します。 この種類のデバイスでは、そのような IP アドレスのセットに対してすべてのデータ パケットが評価され、そのパケットの送信先となるトンネルが選択されます。

Azure のポリシーベースの VPN ゲートウェイの主な機能を次に示します。

- IKEv1 のみのサポート。
- "静的ルーティング" の使用。両方のネットワークからのアドレス プレフィックスの組み合わせによって、VPN トンネルを通じてトラフィックを暗号化および暗号化解除する方法が制御されます。 トンネリングされたネットワークの送信元と送信先はポリシーで宣言され、ルーティング テーブルで宣言する必要はありません。
- ポリシーベースの VPN は、これらを必要とする特定のシナリオで使用する必要があります。たとえば、従来のオンプレミス VPN デバイスとの互換性を保つ場合です。

ルートベースの VPN

各トンネルの背後にある IP アドレスを定義することが煩雑すぎる場合は、ルートベースのゲートウェイを使用できます。 ルートベースのゲートウェイにより、IPSec トンネルはネットワーク インターフェイスまたは仮想トンネル インターフェイスとしてモデル化されます。 IP ルーティング (静的ルートまたは動的ルーティング プロトコル) により、各パケットを送信するときに、これらのトンネル インターフェイスのどちらを使用するかが決まります。 ルートベースの VPN は、オンプレミス デバイス用の接続方法として推奨されます。 そちらのほうが、新しいサブネットの作成などのトポロジの変更に対する回復性が高くなっています。

次のいずれかの種類の接続が必要な場合は、ルートベースの VPN ゲートウェイを使用します。

- 仮想ネットワーク間の接続
- ポイント対サイト接続
- マルチサイト接続
- Azure ExpressRoute ゲートウェイとの共存

Azure でのルートベースの VPN ゲートウェイの主な機能を次に示します。

- IKEv2 のサポート
- Any-to-Any (ワイルドカード) のトラフィック セレクターの使用
- ルーティング/転送テーブルによってトラフィックを別の IPSec トンネルに転送する "動的ルーティング プロトコル" を使用できる

この場合、送信元と送信先のネットワークは、ポリシーベースの VPN 内に存在するか静的ルーティングを使用するルートベース VPN 内にあるため、静的に定義されることはありません。 代わりに、Border Gateway Protocol (BGP) などのルーティング プロトコルを使用して動的に作成されたネットワーク ルーティング テーブルに基づいて、データ パケットが暗号化されます。

VPN ゲートウェイのサイズ

お客様の VPN ゲートウェイの機能は、お客様がデプロイする SKU またはサイズによって決まります。 次の表に、使用可能な各 SKU の主な機能を示します。

SKU	サイト間/ネットワーク間のトンネル	合計スループット ベンチマーク	Border Gatev
基本 [注を参照]	最大値: 10	100 Mbps	サポートされ
VpnGw1/Az	最大値: 30	650 Mbps	サポートされ
VpnGw2/Az	最大値: 30	1 Gbps	サポートされ
VpnGw3/Az	最大値: 30	1.25 Gbps	サポートされ

注意

Basic VPN ゲートウェイは、開発/テスト ワークロードにのみ使用する必要があります。 さらに、Basic から VpnGW1/2/3/Az の SKU に後で移行するには、ゲートウェイを削除して再デプロイする必要があります。

VPN ゲートウェイをデプロイする

VPN ゲートウェイをデプロイするには、事前に Azure リソースおよびオンプレミスのリソースがいくつか必要になります。

必要な Azure リソース

運用 VPN ゲートウェイをデプロイするには、事前に以下の Azure リソースが必要になります。

- **仮想ネットワーク**。 VPN ゲートウェイに対して必要になる追加のサブネット用の十分なアドレス空間を用意して仮想ネットワークをデプロイします。 この仮想ネットワークのアドレス空間が、接続するオンプレミス ネットワークと重複しないようにしてください。 仮想ネットワークには、VPN ゲートウェイを 1 つだけデプロイできます。

- **GatewaySubnet**。 VPN ゲートウェイ用の `GatewaySubnet` というサブネットをデプロイします。 少なくとも **/27** のアドレス マスクを使用し、将来の拡張を考慮してサブネット内に十分な IP アドレスが用意されていることを確認してください。 他のサービスでこのサブネットを使用することはできません。

- **パブリック IP アドレス**。 ゾーン非対応のゲートウェイを使用する場合は、Basic SKU の動的パブリック IP アドレスを作成します。 このアドレスでは、ご利用のオンプレミス VPN デバイスのターゲットとして、ルーティング可能なパブリック IP アドレスが提供されます。 この IP アドレスは動的ですが、VPN ゲートウェイを削除して再作成しない限り、変わりません。

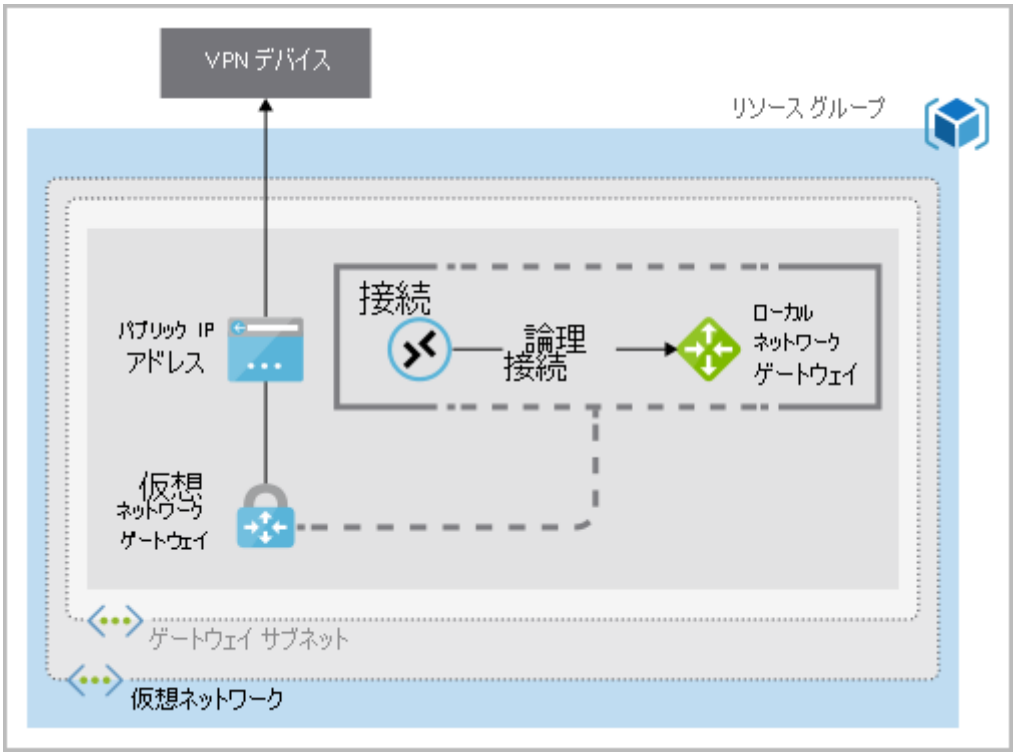
- **ローカル ネットワーク ゲートウェイ**。 オンプレミス ネットワークの構成 (VPN ゲートウェイの接続場所や対象など) を定義するためのローカル ネットワーク ゲートウェイを作成します。 この構成には、オンプレミス VPN デバイスのパブリック IPv4 アドレスと、ルーティング可能なオンプレミス ネットワークが含まれています。 この情報は、オンプレミス ネットワークが宛先となるパケットを IPSec トンネル経由でルーティングするために VPN ゲートウェイによって使用されます。

- **仮想ネットワーク ゲートウェイ**。 仮想ネットワークとオンプレミス データセンターまたは他の仮想ネットワークの間のトラフィックをルーティングするための仮想ネットワーク ゲートウェイを作成します。 仮想ネットワーク ゲートウェイには、VPN または ExpressRoute ゲートウェイのいずれかを使用できますが、このユニットでは VPN 仮想ネットワーク ゲートウェイのみを取り上げます (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)。

- **接続**。 VPN ゲートウェイとローカル ネットワーク ゲートウェイの間の論理接続を作成するための接続リソースを作成します。
  - ローカル ネットワーク ゲートウェイによる定義に従って、オンプレミス VPN デバイスの IPv4 アドレスへの接続が確立されます。
  - 仮想ネットワーク ゲートウェイとそれに関連付けられているパブリック IP アドレスから接続が行われます。

  複数の接続を作成することができます。

次の図に、このリソースの組み合わせとそれらの関係を示します。これは、VPN ゲートウェイのデプロイに必要なものの理解を深めるのに役立ちます。



必要なオンプレミス リソース

ご利用のデータセンターを VPN ゲートウェイに接続するには、次のオンプレミス リソースが必要です。

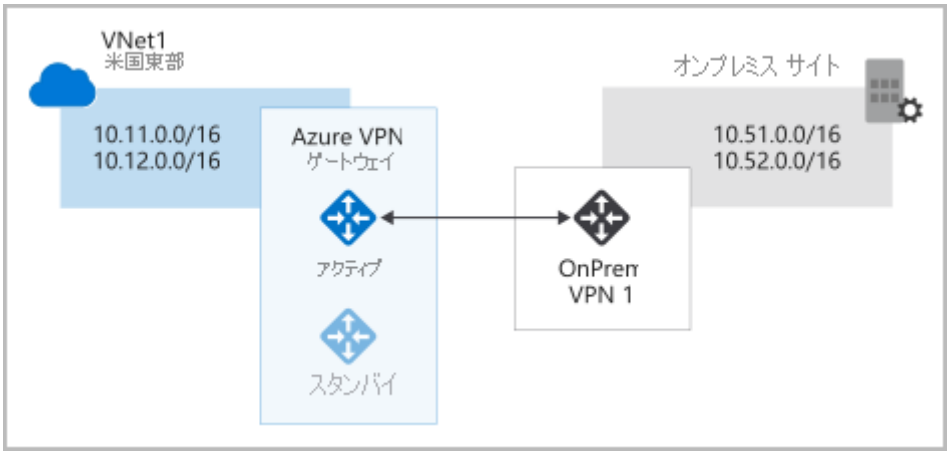
- ポリシーベースまたはルートベースの VPN ゲートウェイをサポートする VPN デバイス
- 公開された (インターネット ルーティング可能な) IPv4 アドレス

高可用性のシナリオ

フォールト トレラント構成を確実に備えるためのオプションがいくつかあります。

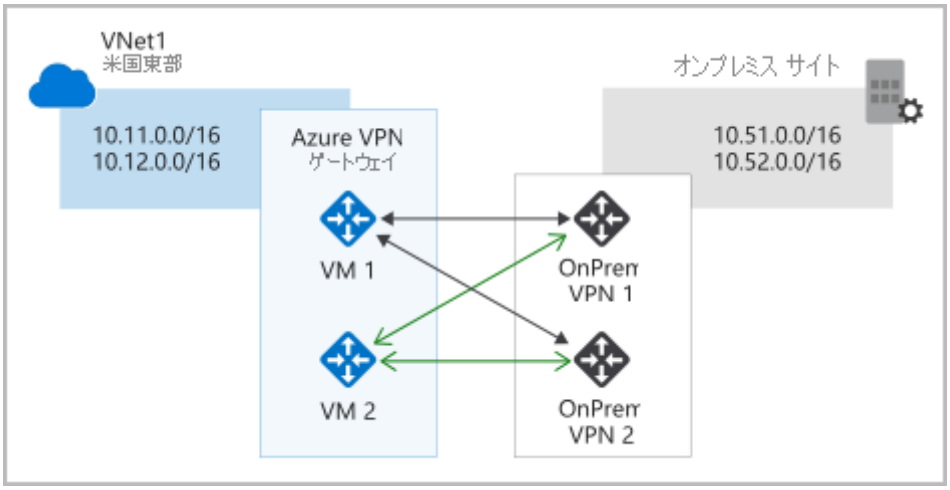
アクティブ/スタンバイ

既定では、VPN ゲートウェイは、Azure で 1 つの VPN ゲートウェイ リソースしか表示されない場合でも、"アクティブ/スタンバイ" 構成で 2 つのインスタンスとしてデプロイされます。 計画メンテナンスまたは計画外の中断がアクティブなインスタンスに影響を与える場合、スタンバイ インスタンスがユーザーの介入なしに自動的に接続の担当を引き受けます。 接続は、このフェールオーバー中には中断されますが、通常、計画メンテナンスでは数秒以内、計画外の中断では 90 秒以内に復元されます。



アクティブ/アクティブ

BGP ルーティング プロトコルのサポート開始により、VPN ゲートウェイをアクティブ/アクティブ構成でもデプロイできるようになりました。 この構成では、各インスタンスに一意のパブリック IP アドレスを割り当てます。 その後、オンプレミス デバイスから各 IP アドレスへの別のトンネルを作成します。 オンプレミスで追加の VPN デバイスをデプロイすることで、高可用性を拡張することができます。



ExpressRoute のフェールオーバー

もう 1 つの高可用性オプションは、ExpressRoute 接続用のセキュリティで保護されたフェールオーバー パスとして VPN ゲートウェイを構成することです。 ExpressRoute 回線には、回復性が組み込まれています。 ただし、接続を提供するケーブルに影響を与える物理的な問題や、ExpressRoute の場所全体に影響を与える停止の影響を免れることはできません。 ExpressRoute 回線の停止に関連するリスクが存在する高可用性のシナリオでは、接続の代替方法としてインターネットを使用する VPN ゲートウェイをプロビジョニングすることもできます。 この方法で、仮想ネットワークへの接続を常に維持することができます。

ゾーン冗長ゲートウェイ

可用性ゾーンがサポートされるリージョンでは、VPN ゲートウェイと ExpressRoute ゲートウェイをゾーン冗長構成でデプロイできます。 この構成によって、仮想ネットワーク ゲートウェイに回復性、スケーラビリティ、および高可用性が提供されます。 Azure 可用性ゾーンへの複数のゲートウェイのデプロイでは、オンプレミス ネットワークの Azure への接続をゾーンレベルの障害から保護すると同時に、ゲートウェイが 1 つのリージョン内で物理的かつ論理的に分離されます。 これらのゲートウェイには異なるゲートウェイ SKU が必要であり、Basic パブリック IP アドレスではなく Standard パブリック IP アドレスが使用されます。