Azure Firewall を使用して仮想ネットワークを保護する

100 XP

5 分

"ファイアウォール" は、ネットワークの送受信トラフィックを監視し、定義されたセキュリティ規則セットに基づいて特定のトラフィックを許可するかブロックするかを決定するネットワーク セキュリティ デバイスです。 IP アドレスの範囲を指定するファイアウォール規則を作成できます。 この範囲内の IP アドレスを付与されたクライアントのみが、ターゲット サーバーにアクセスできます。 ファイアウォール規則には、特定のネットワーク プロトコルとポート情報を含めることもできます。

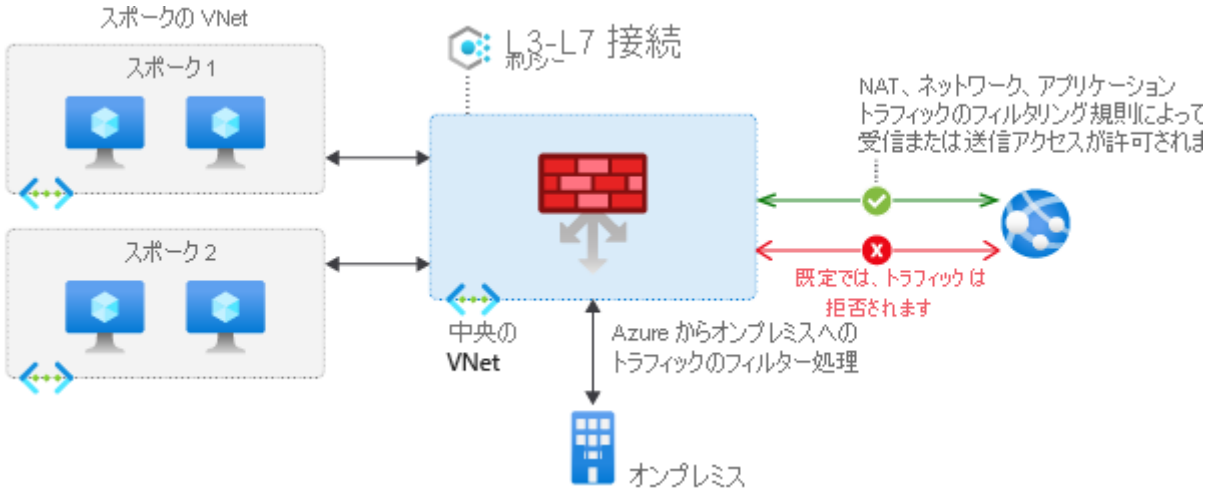
Tailwind Traders 社では、現在、ハードウェアとソフトウェアを組み合わせたファイアウォール アプライアンスを実行して、オンプレミス ネットワークを保護しています。 これらのファイアウォール アプライアンスでは、運用するために毎月ライセンス料が必要であり、IT スタッフが定期メンテナンスを実施する必要があります。 Tailwind Traders 社がクラウドに移行するにあたって、IT マネージャーは、クラウド ネットワークとオンプレミス ネットワークの両方を保護できる Azure サービスを把握したいと考えています。

ここでは、Azure Firewall について説明します。

Azure Firewall とは

Azure Firewall は、Azure 仮想ネットワーク内のリソースを保護するクラウドベースのマネージド ネットワーク セキュリティ サービスです。 仮想ネットワークは、ご自身のデータセンターで運用している従来のネットワークに似ています。 それは、仮想マシンやその他のコンピューティング リソースの相互通信や、インターネットとオンプレミス ネットワークでの安全な通信を実行できるようにするプライベート ネットワークの基本的な構成要素です。

次の図は、基本的な Azure Firewall の実装を示したものです。



Azure Firewall は "ステートフル" ファイアウォールです。 ステートフル ファイアウォールでは、ネットワーク トラフィックの個々のパケットだけでなく、ネットワーク接続の完全なコンテキス

トが分析されます。 Azure Firewall は、高可用性と制限のないクラウドのスケーラビリティを特徴としています。

Azure Firewall によって、サブスクリプションと仮想ネットワーク向けのアプリケーションとネットワークの接続ポリシーを作成、適用、およびログに記録するための一元的な場所が提供されます。 Azure Firewall では、仮想ネットワークのリソースに対して静的な (変更されない) パブリック IP アドレスが使用されます。これにより、仮想ネットワークから発信されたトラフィックを外部のファイアウォールが識別することができます。 このサービスは、ログ記録と分析を可能にするために Azure Monitor に統合されています。

Azure Firewall には、次のような多くの機能があります。

- 組み込みの高可用性。
- 制限のないクラウドのスケーラビリティ。
- 送信と受信のフィルタリング規則。
- 受信宛先ネットワークアドレス変換 (DNAT) のサポート。
- Azure Monitor ログ記録。

通常、Azure Firewall は、一般的なネットワーク アクセスを制御する中央仮想ネットワークにデプロイされます。

この短いビデオでは、Azure Firewall によって、定義された一連のセキュリティ規則に基づき受信および送信ネットワーク トラフィックが監視されるしくみについて説明します。 また、ビデオでは Azure Firewall と従来のファイアウォール アプライアンスとの比較についても説明します。

Azure Firewall で構成できるもの

Azure Firewall を使用して、次のルールを構成できます。

- アプリケーション ルール: サブネットからアクセスできる完全修飾ドメイン名 (FQDN) を定義します。
- ネットワーク ルール: 送信元アドレス、プロトコル、宛先ポート、送信先アドレスを定義します。
- 受信要求を変換する宛先 IP アドレスとポートを定義するネットワーク アドレス変換 (NAT) 規則。

Azure Application Gateway でも、"*Web* アプリケーション ファイアウォール" (WAF) と呼ばれるファイアウォールが提供されています。 WAF では、Web アプリケーションの一般的な悪用と脆弱性に対する一元化された受信保護が行われます。 Azure Front Door と Azure Content Delivery Network でも、WAF サービスが提供されます。