ネットワーク セキュリティ グループを使用してネットワーク トラフィックをフィルター処理する

100 XP

2 分

外部ソースから送信されるトラフィックは Azure Firewall と Azure DDoS Protection によって制御できますが、Tailwind Traders 社では、Azure で内部ネットワークを保護する方法についても理解したいと考えています。 これを行うことで、攻撃に対する防御層がさらに追加されます。

ここでは、ネットワーク セキュリティ グループ (NSG) を検討します。

ネットワーク セキュリティ グループとは何か?

ネットワーク セキュリティ グループを使用して、Azure 仮想ネットワークの中で Azure リソースによって送受信されるネットワーク トラフィックをフィルター処理できます。 NSG は、内部ファイアウォールのようなものと考えることができます。 各 NSG には、送信元と送信先の IP アドレス、ポート、およびプロトコルでリソースとのトラフィックをフィルター処理できるようにする受信と送信のセキュリティ規則を複数含めることができます。

NSG の規則の指定方法

ネットワーク セキュリティ グループには、Azure サブスクリプションの制限内で必要な数の規則を含めることができます。 各規則には、次のプロパティが指定されます。

プロパティ	説明
Name	NSG の一意の名前。
Priority	100 ～ 4096 の数値。 規則は優先度順に処理され、小さい数値を持つ規則が大きな数値のものよりも前に処理されます。
送信元または送信先	単一の IP アドレスまたは IP アドレスの範囲、サービス タグ、またはアプリケーション セキュリティ グループ。
プロトコル	**TCP**、**UDP**、または **すべて**。
方向	規則の適用先 (受信または送信トラフィック)。
ポート範囲	単一のポートまたはポートの範囲。
操作	**許可** または **拒否**。

ネットワーク セキュリティ グループを作成すると、セキュリティのベースライン レベルを提供する一連の既定の規則が Azure によって作成されます。 既定の規則を削除することはできませんが、優先度の高い新しい規則を作成することでそれらをオーバーライドできます。