Azure サービスを組み合わせて完全なネットワーク セキュリティ ソリューションを作成する

100 XP

3 分

Azure のセキュリティ ソリューションを検討する場合は、多層防御のすべての要素を考慮してください。

Azure サービスを組み合わせて完全なネットワーク セキュリティ ソリューションを作成する方法に関する推奨事項を次に示します。

境界層をセキュリティで保護する

境界層は、ネットワークベースの攻撃から組織のリソースを保護することを目的としています。 ネットワークの安全性を保つには、これらの攻撃を識別し、適切なセキュリティ チームにアラートを出し、影響を排除することが重要です。 これを行うには、次の手順を実行します。

- Azure DDoS Protection を使用して、ユーザーに対するサービス拒否が発生する前に大規模な攻撃をフィルター処理します。
- Azure Firewall と境界ファイアウォールを使用して、ネットワークに対する悪意のある攻撃を識別してアラートを発行します。

ネットワーク層をセキュリティで保護する

この層では、すべてのリソースに対するネットワーク接続を制限して、必要な接続のみを許可することに重点が置かれます。 リソースをセグメント化し、ネットワークレベルの制御を使用して、必要な通信のみに制限します。

接続を制限することで、ネットワークで水平方向に攻撃が拡大するリスクを軽減します。 ネットワーク セキュリティ グループを使用して、この層で許可される受信通信と送信通信を定義します。 推奨されるプラクティスを次に示します。

- ネットワークをセグメント化し、アクセス制御を構成することで、リソース間の通信を制限します。
- 既定で拒否します。
- 必要に応じて、受信インターネット アクセスを限定し、発信を制限します。
- オンプレミス ネットワークへのセキュリティで保護された接続を実装します。

サービスを組み合わせる

ネットワーク セキュリティを管理し、階層型保護を強化するために、Azure ネットワーク サービスとセキュリティ サービスを組み合わせることができます。 サービスの組み合わせ方法には次の 2 つがあります。

- **ネットワーク セキュリティ グループと Azure Firewall**

  Azure Firewall によって、ネットワーク セキュリティ グループの機能が補完されます。 それらがまとまって、より高度な多層防御ネットワーク セキュリティが実現されきます。

  ネットワーク セキュリティ グループは、分散ネットワーク層トラフィック フィルターを提供して、各サブスクリプションの仮想ネットワーク内のリソースへのトラフィックを制限します。

  Azure Firewall は、サービスとして完全にステートフルな、一元化されたネットワーク ファイアウォールです。 さまざまなサブスクリプションと仮想ネットワークにわたって、ネットワークレベルとアプリケーションレベルでの保護が提供されます。

- **Azure Application Gateway Web アプリケーション ファイアウォールと Azure Firewall**

  Web アプリケーション ファイアウォール (WAF) は、一般的な悪用や脆弱性に対する一元的な受信保護を Web アプリケーションに提供する Azure Application Gateway の機能です。

  Azure Firewall では次が提供されます。
  - 非 HTTP/S プロトコルの受信保護 (RDP、SSH、FTP など)。
  - すべてのポートとプロトコルに対する送信ネットワークレベルの保護。
  - 送信 HTTP/S のアプリケーションレベルの保護。

  これらを組み合わせることで、より多くの保護が提供されます。