Azure DDoS Protection を使用して DDoS 攻撃から保護する

100 XP

3 分

すべての大企業は、大規模なネットワーク攻撃の対象になる可能性があります。 Tailwind Traders 社も例外ではありません。 攻撃者は、声明を出すためや単なる挑戦のために、ネットワークを麻痺させることがあります。 Tailwind Traders 社では、クラウドに移行するにあたって、Azure で分散型サービス拒否 (DDoS) やその他の攻撃をどのように防止できるかを理解したいと考えています。

ここでは、DDoS 攻撃から Azure リソースを保護するために Azure DDoS Protection (Standard サービス レベル) がどのように役立つかについて説明します。 最初に、DDoS 攻撃とは何かを定義しましょう。

DDoS 攻撃とは?

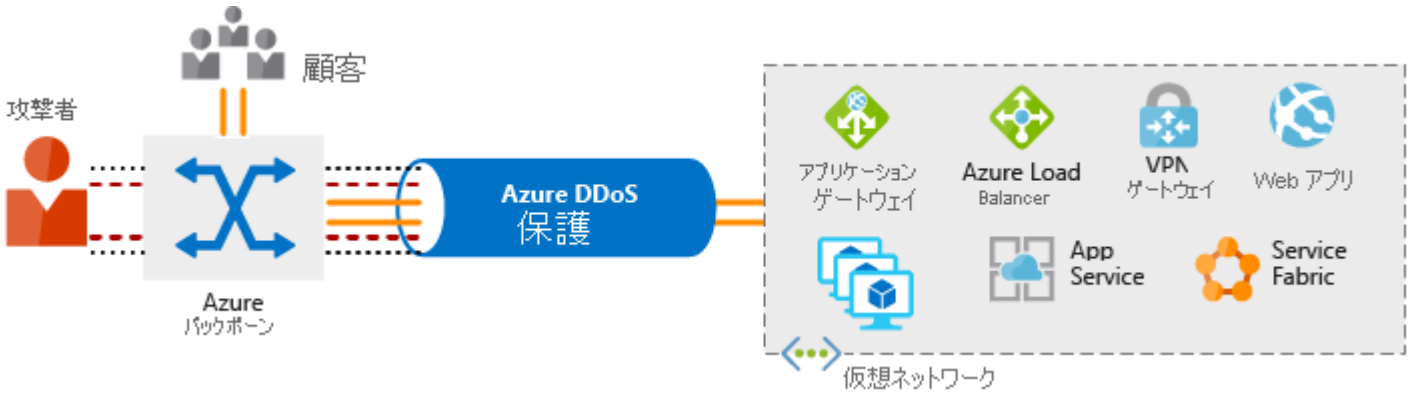
分散型サービス拒否 攻撃は、アプリケーションのリソースを過剰に消費して使い尽くすことによって、アプリケーションを遅くしたり、正当なユーザーに反応しない状態にしようとします。 DDoS 攻撃は、インターネット経由でパブリックに到達可能なすべてのリソース (Web サイトも含まれます) を標的にすることができます。

Azure DDoS Protection とは何か?

Azure DDoS Protection (Standard) は、DDoS 攻撃から Azure リソースを保護するために役立ちます。

DDoS Protection を推奨されるアプリケーション設計プラクティスと組み合わせると、DDoS 攻撃に対する防御を用意できます。 DDoS Protection では、Microsoft のグローバル ネットワークのスケールと弾力性を利用して、すべての Azure リージョンで DDoS を軽減できます。 DDoS Protection サービスでは、サービスの可用性に影響が及ぶ前に、Azure ネットワークの境界で DDoS トラフィックを分析して破棄することによって、Azure アプリケーションを保護します。

この図は、顧客と攻撃者の両方から Azure に流入するネットワーク トラフィックを示しています。



DDoS Protection では、ネットワークを過負荷にしようとする攻撃者の試みが識別され、攻撃者からのトラフィックがこれ以上 Azure サービスに到達することがないようにブロックされます。 顧客からの正当なトラフィックは、サービスの中断なく、引き続き Azure に流れます。

DDoS Protection によって、クラウドの使用量を管理することもできます。 オンプレミスで実行する場合、コンピューティング リソースの数は固定されています。 しかし、クラウドでは、エラスティック コンピューティングとは需要に合わせてデプロイを自動的にスケールアウトできることを意味します。 巧妙に設計された DDoS 攻撃では、リソースの割り当ての増加によって、不要な費用が発生する可能性があります。 DDoS Protection Standard では、処理するネットワーク負荷に、顧客の使用量を確実に反映させることができます。 DDoS 攻撃中にスケールアウトされたリソースに対して発生したコストのクレジットを受け取ることもできます。

DDoS Protection で利用できるサービス レベル

Azure DDoS Protection には、次のサービス レベルがあります。

- **Basic**

  Basic サービス レベルは、Azure サブスクリプションの一部として自動的に無料で有効になります。

  常時接続のトラフィック監視および一般的なネットワーク レベル攻撃のリアルタイムの軽減策によって、Microsoft のオンライン サービスによって使用されるのと同じ防御が提供されます。 Basic サービス レベルでは、大規模な DDoS 攻撃で Azure インフラストラクチャ自体が影響を受けないことが保証されます。

  Azure のグローバル ネットワークを使用して、Azure リージョンに対する攻撃トラフィックが分散されて軽減されます。

- **Standard**

  Standard サービス レベルでは、特に Azure Virtual Network リソースに特化してチューニングされた追加の軽減機能が提供されます。 DDoS Protection Standard は比較的簡単に有効化でき、アプリケーションの変更は不要です。

  Standard レベルでは、常時接続のトラフィック監視とネットワーク レベルの一般的な攻撃のリアルタイムの軽減が提供されます。 Microsoft のオンライン サービスによって使用される

のと同じ防御が提供されます。

保護ポリシーは、専用のトラフィック監視および機械学習アルゴリズムによってチューニングされます。 ポリシーは、Azure Load Balancer や Application Gateway などの仮想ネットワーク内にデプロイされたリソースに関連付けられたパブリック IP アドレスに適用されます。

Azure のグローバル ネットワークを使用して、Azure リージョンに対する攻撃トラフィックが分散されて軽減されます。

DDoS Protection による防御が有効な攻撃の種類

Standard サービス レベルでは、以下を防ぐことができます。

- **帯域幅消費型攻撃**

  この攻撃の目的は、膨大な量の一見正当なトラフィックを使用してネットワーク層を麻痺させることです。

- **プロトコル攻撃**

  これらの攻撃では、プロトコル スタックの第 3 層と第 4 層の弱点が悪用され、ターゲットにアクセスできなくなります。

- **リソース層 (アプリケーション層) 攻撃 (Web アプリケーション ファイアウォールのみ使用)**

  これらの攻撃は、ホスト間のデータ転送を妨害するために Web アプリケーション パケットをターゲットにします。 L7 攻撃を防ぐには、Web アプリケーション ファイアウォール (WAF) が必要です。 DDoS Protection Standard では、帯域幅消費型攻撃とプロトコル攻撃から WAF が保護されます。