DDoS軽減サービスプロバイダーへの5つの質問

DDoS 攻撃は頻度も複雑性も高まっています。そんな中、正しいDDoS 軽減サービスを選ぶことは、ネットワークとユーザーを保護する上で不可欠なことです。しかし、すべてのサービスが同じように作られているわけではなく、間違ったサービスを選んでしまうと、予期せぬ悩みの種、パフォーマンスの問題、ダウンタイムなどにつながる可能性があります。

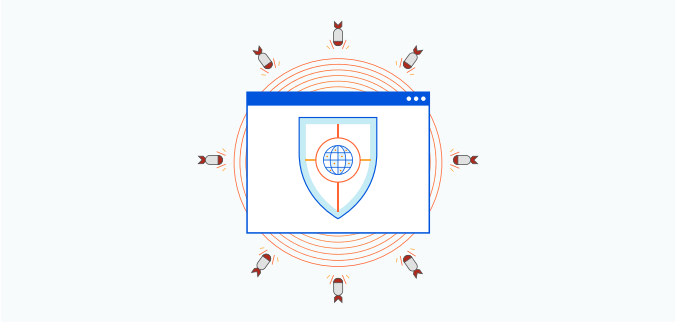
ここに、DDoS 軽減サービスプロバイダーを評価する際に、次の5つの質問について考慮する必要があります。

1. そのサービスはクラウドネイティブですか？

DDoS 軽減サービスが効力を発揮するためには、クラウドデータセンターで仮想化およびホストされているオンプレミステクノロジーではなく、クラウドネイティブである必要があります。2つの違いは？クラウドネイティブの軽減サービスは、人為的パフォーマンスによるボトルネックを強要することなく、ビジネスニーズに合わせてシームレスに拡張することができます。その一方、クラウドホスト型の仮想アプライアンスは、それでもオンプレミスハードウェアに関連する管理上の複雑性がともないます。

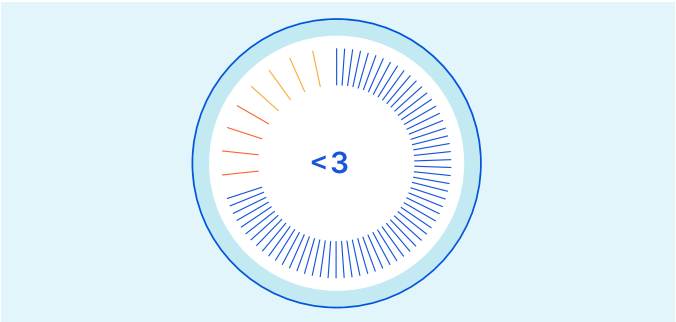
2. そのプロバイダーが提供するネットワーク容量は？

DDoS 攻撃が2020年にAWSの顧客を標的とした2.3Tbps攻撃のように大規模だったら、DDoSを吸収するのに十分なネットワーク容量を持たないサービスプロバイダーを圧倒できてしまいます。この規模の攻撃に対抗するには、ダウンタイムやパフォーマンスの低下を引き起こさないで、攻撃に耐え得るのに十分なネットワーク容量を提供するプロバイダーを選ばなければなりません。



3. そのサービスは、どのくらいの速さでDDoS 攻撃を検出し、対処できますか？

攻撃に直面した場合、time-to-mitigate（攻撃を検出し、軽減する時間）が短いことは不可欠です。ダウンタイムが数秒を超えると、顧客体験、ブランドの評判、収益に不可逆的な損害を与える可能性があります。



4. そのサービスは、どのデータセンターでも利用できますか？

DDoSスクラビング機能がどのデータセンターでも利用できるようでなければ、トラフィックは専用の「スクラビングセンター」を経由するように強制的に戻されるため、遅延がが増加し、アプリケーションのパフォーマンスに影響を与えます。トラフィックを最適なパスに維持しながら、どのデータセンターでも軽減サービスを提供できるプロバイダーを選んでください。

5. そのサービスは自動化されていますか？

堅牢なDDoS 軽減サービスは、一つのダッシュボード、またはAPIから自動化と自己保守性を提供し、迅速に脅威からの保護を有効化して管理できる状態である必要があります。簡単なやりとりだけで迅速に対応でき、観察されるサービスのダウンタイムに影響を与えず、脅威の検出とその軽減を積極的に行うプロバイダーを探してください。

Cloudflare Magic Transitは、ネットワークトラフィックを加速させながら、DDoS 攻撃からIPサブネット全体を保護します。Cloudflareのグローバルネットワークは200か所以上に広がるデータセンターを備え、1日平均700億の脅威をブロックしています。その中には、史上最大のDDoS 攻撃もいくつかあります。

Magic Transitを始めるには、無料のデモをいますぐリクエストしてください。