ホワイトペーパー

CLOUDFLARE

DDoS攻撃を軽減するための5つのベストプラクティス

急速に進化する分散サービス妨害の脅威への防御と全レイヤーの脆弱性に対処する方法

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

目次

概要

分散サービス妨害(DDoS)攻撃は依然として、サイバー犯罪者が使用する最も効果的な手法の1つで、全世界の企業に財務上、業務上、評判上の甚大な損失をもたらします。この攻撃には様々な形態がありますが、目的は常に、不正アクセスしたデバイスやネットワークを利用して、標的とするサーバー、サービス、ネットワークに大量のトラフィックを送りつけて正常な機能を奪うことです。

企業が防御を強化すれば、サイバー犯罪者は新たな種類の攻撃や大容量の攻撃でそれに応酬します。こうした攻撃のいくつかは、Open Systems Interconnection (OSI)モデルの第3層と第4層を新しい方法で標的とし、毎秒1 TB (Tbps)以上のネットワークトラフィック急増を発生させます。そのほかの攻撃は、セキュリティ網をかいくぐって1つまたは複数のサービスゲートウェイとアプリケーション層を標的とするように設計された低速・低強度の第7層攻撃です。

DDoS攻撃に関連する困難を乗り切るためには、全ての層で全ての脅威に対応できる包括的なアプローチが必要となります。しかし、セキュリティを強化してもパフォーマンスを犠牲にしては意味がありません。オンプレミスのツールはその一部を実現することは可能ですが、より堅牢なソリューションとしては、パフォーマンスを担保しつつ、ネットワークエッジで機能するスケーラブルなクラウドベースの軽減策によって、最大限の機敏性と制限のない処理能力を提供することが好ましいでしょう。

1部

DDoS攻撃とは？

分散サービス妨害(DDoS)攻撃とは、大量のインターネットトラフィックで過負荷状態にすることで、標的となるサーバー、アプリケーション、ネットワークを使用不能またはオフライン状態にしようとする悪意のある攻撃のことです。

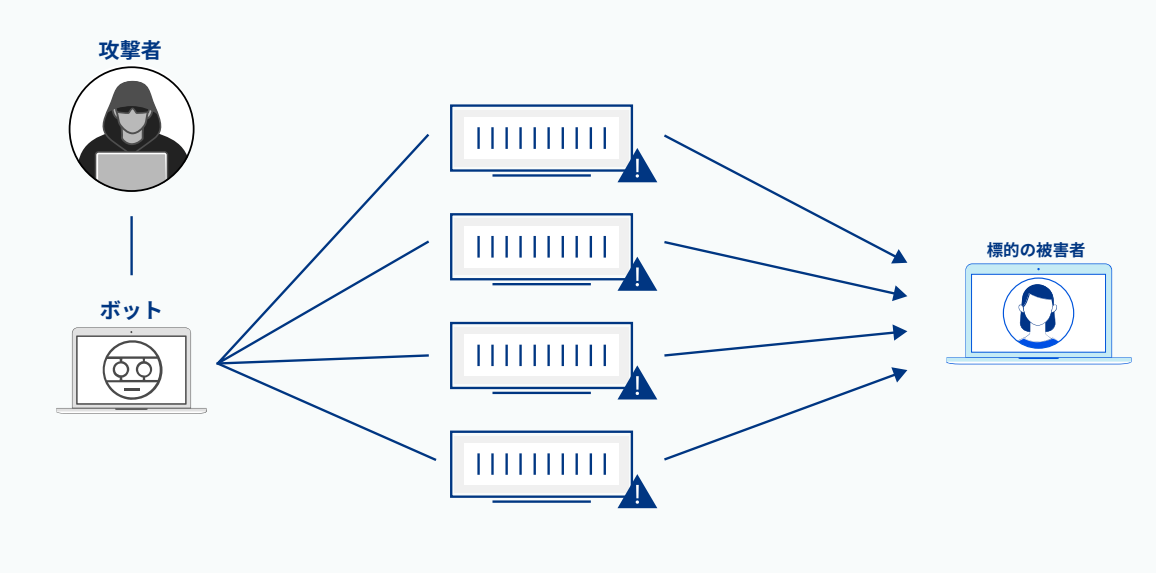
DDoS攻撃者はマルウェアを使用して、オンラインのコンピューター、ルーター、IoTアプライアンス、およびその他のデバイスを制御し、攻撃トラフィックの送信元として使用します。感染したデバイスはしばしばボットと呼ばれ、それらのグループは「ボットネット」と呼ばれます。攻撃中、ボットネット内の各デバイスが、トラフィック容量の制限を超過させることを目的とした標的に対する同時リクエストを送信することで、正当なトラフィックに対するサービス妨害が発生します。

DDoS攻撃の種類

DDoS攻撃では、OSI　参照モデル内にある7つの「階層」のどれもが標的になり得ます。こうした攻撃は、いずれも悪意のあるトラフィックが標的を過負荷状態に陥れるもので、三つの異なるカテゴリーに分類できます。これらのカテゴリーは、攻撃が発生する場所または方法を示します。

帯域幅消費型攻撃

これらの攻撃は、他のどのタイプの攻撃よりもはるかに多くのトラフィックで標的とするサイトとネットワークを過負荷状態にします。また、DNSアンプリフィケーションやその他のブルートフォース技術を使用して、1秒あたりのビット数　(Bps)　で測定される大規模なトラフィックサージを生成することがよくあります。(DNSアンプリフィケーションでは、攻撃者はオープンDNSリゾルバーを使用して、増加させたトラフィックで標的を過負荷状態にします。)

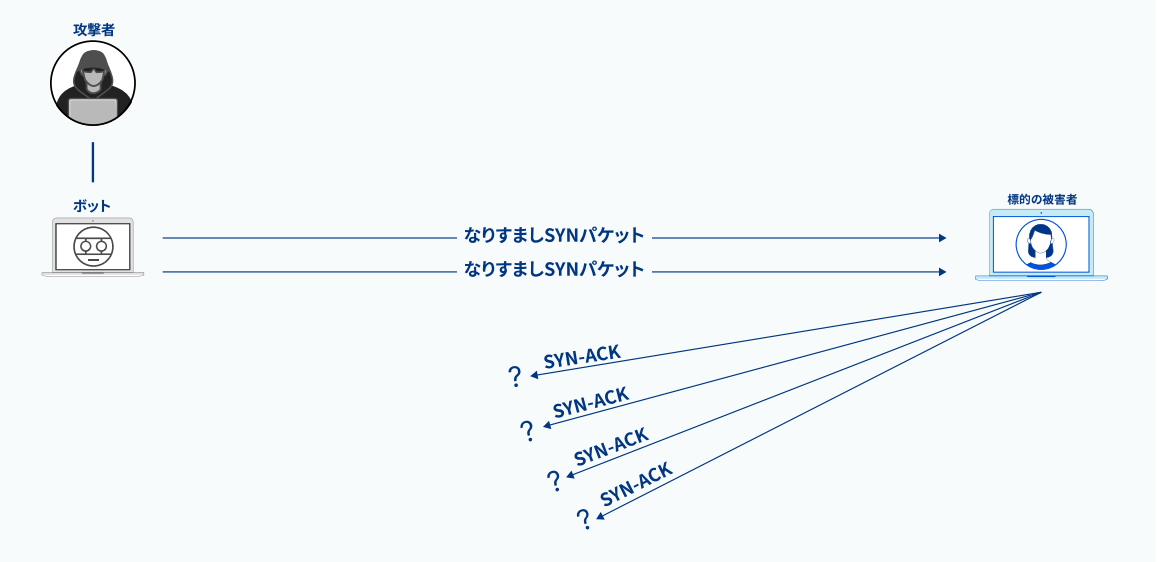


パート1 – DDOS攻撃とは？

プロトコル攻撃

プロトコル攻撃は、OSI 参照モデルの第3層(ネットワーク)と第4層(トランスポート)の脆弱性を標的とし、ファイアウォールやロードバランサーを含むWebサーバーまたはその中間リソースの利用可能なすべての処理能力を食い潰します。これらの攻撃には次のようなものがあり、すべて1秒あたりのパケット数 (Pps) で測定されます。

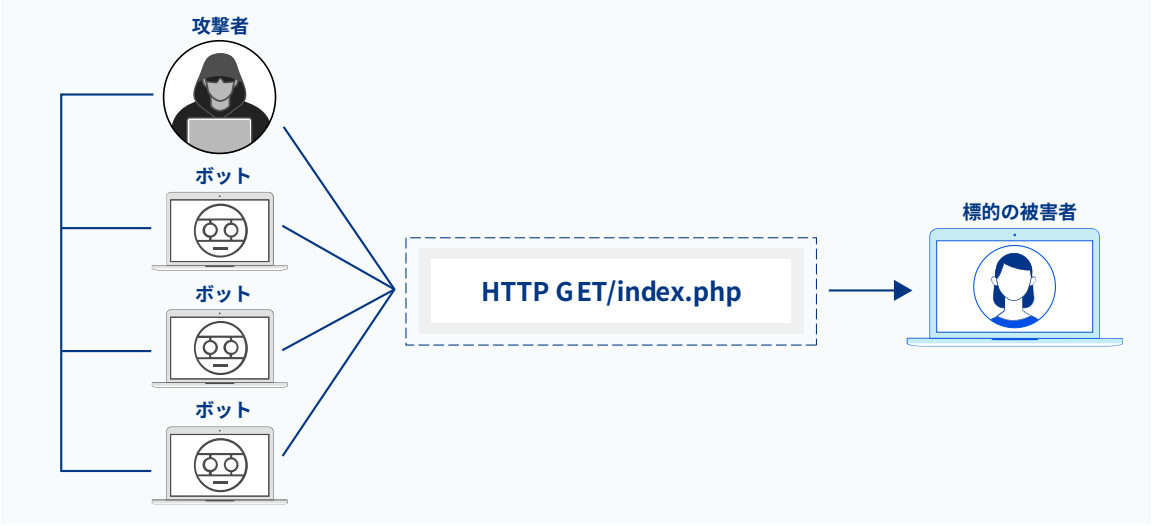
- SYNフラッド: この攻撃では、初期接続要求 (SYN) パケットを繰り返し送信して、標的サーバーで使用可能なすべてのポートを過負荷状態に陥れます。
- Ping of Death攻撃: 攻撃者は標的に最大許容サイズを超えるパケットを送信し、フリーズまたはクラッシュを引き起こします。
- SMURF DDoS: この攻撃では、脅威アクターがインターネット制御メッセージプロトコル (ICMP) パケットでサーバーを過負荷状態にします。



パート1 – DDOS攻撃とは？

アプリケーション層への攻撃

これらの攻撃が狙うのは、HTTPまたはHTTPSリクエストに応じてサーバー上でWebページが生成され配信されるOSIレイヤー7です。この攻撃は一度に多数の異なるコンピューター上でWebページの更新を繰り返し実行するのに似ていて、結果として、大量のHTTPまたはHTTPSのリクエストが1秒あたりのリクエスト数 (Rps) で測定されます。



こうした攻撃タイプには重複するものもあります。たとえば、プロトコル攻撃の一部は、帯域幅消費型攻撃でもあります。そして、攻撃者が同時にプロトコルスタックの複数の層を標的にする、または攻撃対象が取る対策に基づいて変化するマルチベクトル型攻撃があります。

DDoS攻撃の影響

DDoS攻撃が成功した場合に直接表れる影響は、標的とされたサービスのパフォーマンスの低下または完全な停止です。サービスの一部またはすべてがサービスが停止する場合があります。

このようなパフォーマンスが被る困難は、より広範な影響があります。Webアプリケーションの場合、パフォーマンスの低下は、バウンス率の上昇、コンバージョンの低下、ブランドの評判の低下など、多くの悪影響をもたらします。企業ネットワークの場合、パフォーマンス低下により、従業員は日常の多くのタスクを実行できなくなります。

さらに、一部のDDoS攻撃には、他の攻撃の目くらましであり、攻撃者が別のベクトルを介して最終的な目標を追求している間、セキュリティチームの注意をそらし続けるものもあります。このような状況では、標的になった組織は、望まないアプリケーションへアクセス、マルウェア感染、データ損失、またはより一層悪い事態に見舞われる可能性があります。

2部

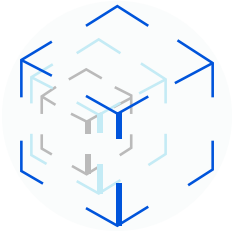
DDoS攻撃の新たな傾向

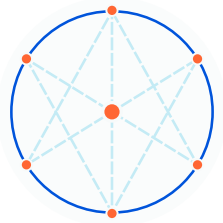
一般的に、企業は自分たちを守るためにいくつかのコア機能を必要としていますDDoS攻撃：

- 攻撃のトラフィックと正当なトラフィックを区別する
- 正当なユーザートラフィックを遮断することなく、悪性ボットを検出し、悪意のあるボットトラフィックをブロックする
- トラフィックを分析して悪意のあるパターンを見つけ、防御の改善に役立てる

しかし、いくつかの新たな傾向がDDoSセキュリティをさらに困難なものとしています。

パート2 – DDOS攻撃の新たな傾向





帯域幅消費型攻撃の存続と規模拡大

帯域幅消費型攻撃は、保護されていない組織を簡単に圧倒することができます。このような攻撃の規模が拡大し続けることはよくありません。

2021年11月に、Cloudflareは、ピーク時で2 Tbpsに及ぶ記録的なマルチベクトルDDoS攻撃を自動的に遮断しました。Cloudflareがこれまでに観測した中で最大の攻撃は、Miraiボットネットコードの亜種を実行する15,000のボットに関連していました。残念ながら、有名なMiraiボットネットとそのコードの亜種に関連する攻撃が最近になって再浮上しています。

たとえば、2021年の夏に、別のMirai型ボットネットがUDPベースおよびTCPベースの攻撃を開始しました。これは1 Tbpsを超えることが複数あり、ピークは約1.2 Tbpsでした。

Cloudflareネットワークデータは、Mirai関連の攻撃以外では攻撃の大半が500 Mbps未満に留まっていることを示しています。しかしながら、2021年の第3四半期には、500 Mbps～1 Gbpsの攻撃は前四半期比(QoQ)で289%増となり、1 Gbps～100 Gbpsの範囲の攻撃は126%増となりました。

ネットワーク帯域幅は、組織の規模と使用するアプリケーションによって大きく異なる可能性があります。つまり、一部の組織は、保護されていない場合、比較的小さな攻撃によって簡単にサービスが停止する恐れがあります。そのため、帯域幅消費型攻撃の規模が大きくなるにつれて、企業はDDoS軽減ソリューションの能力を評価する必要があります。

攻撃の複雑化

マルチベクトル型攻撃の蔓延は、DDoS攻撃の複雑さが増していることを反映しています。

マルチベクトル型攻撃の例は、Voice over Internet Protocol (VoIP)プロバイダーに対する最近の攻撃の急増です。VoIPプロバイダーは、音声やビデオなどを使用してインターネット経由で通信する技術に特化しています。これらの攻撃は、重要なHTTP Webサイトおよびapiエンドポイントを標的とするL7攻撃と、VoIPサーバーインフラストラクチャを標的とするL3/4攻撃を組み合わせたものです。

マルチベクトル型攻撃では、攻撃者は複数の攻撃ベクトルを(多くの場合動的に)使用するため、正当なトラフィックと悪意のあるトラフィックを区別することがますます困難になります。残念ながら、攻撃がこの対策の回避に適応している場合、トラフィックをドロップまたは制限する試みは役に立ちません。

新しい攻撃手法の出現—または以前は一般的ではなかった手法の台頭—は、DDoSの複雑さのもう1つの例です。たとえば、Cloudflareでは、2021年の第3四半期に、DTLSアンプリフィケーション攻撃が前四半期から3,549%増となったことが判明しています。同様に、Cloudflareネットワークデータは、Quote of the Day (QOTD)プロトコルを悪用するDDoSアンプ攻撃が、2021年の第2四半期に前四半期比で123%増となったことを示しています。同じ四半期に、QUICプロトコルに対する攻撃は前四半期比で109%増となりました。

攻撃者は常に新しい方法を見つけ、より複雑な攻撃を仕掛けてくるため、組織はすべてのレイヤーでDDoS攻撃から身を守ることが極めて重要です。

パート2 – DDOS攻撃の新たな傾向

増加を続けるランサムDDoS攻撃

もう1つの重要な傾向はランサムDDoS攻撃の増加です。ランサムDDoS攻撃では、攻撃者は身代金と引き換えにDDoS攻撃で組織を脅迫します。場合によっては、攻撃者は小規模なDDoS攻撃を仕掛け、自分たちが脅威を完全に実行できることを証明することもあります。身代金は通常、ビットコインまたは他の形式の暗号通貨で要求されます。

2021年の前半に、Cloudflareの顧客のうち、DDoS攻撃の標的となった調査対象の11%が、事前に攻撃者から脅迫や身代金要求受けたと回答しています。

例として、Cloudflareは2020年に「フォーチュン500」企業を対象にCloudflareMagic Transit (オンプレミスネットワークにDDoS攻撃対策などを提供) に迎え入れました。同社はサイバー犯罪グループから20ビットコインを要求する身代金要求メッセージを受け取りました。彼らの意思を証明するために、グループはすでに単一のサーバーに対するギガビット級の攻撃を開始していました。

こうした要件と進化する傾向に基づき、企業が優先するべきDDoS軽減に関する5つのベストプラクティスをご紹介します。

3部

DDoS軽減に関するベストプラクティス

- 保護戦術の強化
- 2つの最重要指標の優先順位付け—処理能力と軽減されるまでの時間
- 常時稼動型とオンデマンド型の保護の考察
- パフォーマンスを犠牲にしないセキュリティ対策
- 攻撃者の1歩先を行くための脅威インテリジェンスの採用

1. 保護戦術の強化

DDoS攻撃はOSIスタックの複数のレイヤーで発生する可能性があるため、包括的な保護を採用することが重要です。ただし、これに取り組む方法は、従来のDDoS対策ソリューションだけではありません。次の戦術では、DDoS対策ソリューションを補完し、サーバーとネットワークを保護することができます。

リバースプロキシによるサーバーの保護

Webサーバーを保護することを目的とする場合、リバースプロキシを使用することで攻撃者によってサーバーのIPアドレスを特定され、標的にされることから保護します。彼らは、代わりにリバースプロキシしか標的にできないため、サーバーが保護されることになります。

独自のリバースプロキシを構築またはデプロイしている企業もありますが、これは集中的なソフトウェアリソースとエンジニアリングリソース、物理的なハードウェアへの多額の投資を必要とします。

リバースプロキシのメリットを実現するための最も簡単で費用対効果の高い方法の1つは、コンテンツ配信ネットワーク(CDN)を使用することです。CDNは、プロキシサーバーの分散ネットワークであり、コンテンツをエンドユーザーの近くにキャッシュ(またはコピーを保存)することで遅延を低減します。

グローバルなサーバーの負荷分散機能を搭載したCDNを探し、サイトを世界中の複数のサーバーに分散できるようにします。このようにして、DDoS攻撃は、パフォーマンスに影響を与えることなく、攻撃元の近くで軽減されます。(セキュリティとパフォーマンスのトレードオフの詳細については、Tip 4を参照してください。)

ネットワークの保護

ネットワークインフラストラクチャを保護することを目的とする場合Border Gateway Protocol (BGP)の再ルーティング機能を利用して悪意のあるトラフィックのフィルター機能を持つスクラブセンターへとトラフィックをリダイレクトすることができます。とは言え、地理的に離れていて数が限られているスクラブセンターにトラフィックすべてを再ルーティングすると、かなりの遅延が発生することにもなりかねません。

このため、十分な規模のクラウドベースのDDoS軽減ソリューションをお勧めします。クラウドベースの軽減策では、自律システム番号(ASN)は軽減策プロバイダーが通知するため、トラフィックはオリジンサーバーに向かう代わりに、直接スクラブへとルーティングされます。このセットアップで、トラフィックは攻撃のソースにより近いところでフィルターにかけられ、遅延もさらに削減できます。

2. 2つの最重要指標の優先順位付け— 処理能力と軽減されるまでの時間

DDoS攻撃対策で最も重要な要素は、保護の強度(処理能力)と、攻撃を無力化するためにどれだけ迅速に機能するか(軽減されるまでの時間)です。

処理能力

DDoS攻撃によって生成されるトラフィックの急増に対応するための従来のアプローチは、オンプレミスのハードウェアに投資することでした。しかし、企業は個々の攻撃に対応するために特別に購入した処理能力に対して費用を支払う必要があるため、この方法はすぐに高額になり、頻繁に使用されるものではなくなります。さらに、最も堅牢なエンタープライズグレードのインフラストラクチャでさえ、最大の帯域幅消費型攻撃に圧倒される可能性があります。

レート制限(サーバーが一定期間中に受け入れるリクエストの量を制限)を適用することは効果的です。しかし、レート制限だけでは、正当なトラフィックが急増した時にパフォーマンスが低下し、より複雑な攻撃に耐えることはできません。

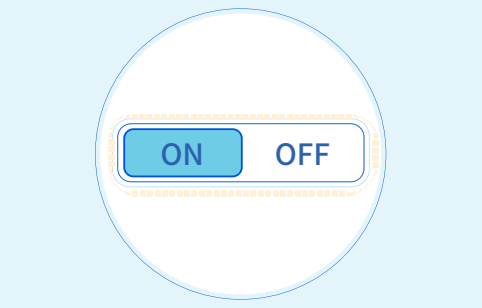
したがって、高い処理能力のソリューションを優先することが重要です。クラウドベースのDDoS軽減機能は、大規模な攻撃にも対応できるようにリソースが拡張できるため、組織を無傷に保つことができます。

軽減までの時間

可用性が少しでも低下すると、収益性と生産性が大幅に低下する可能性がある場合は、軽減までの時間(TTM)が最優先事項になります。TTMを削減するには、障害が発生した場合にトラフィックが代替サイトにフェイルオーバーできるようにする必要があります。しかし、それはインフラストラクチャが過負荷状態になるよりもずっと前にしか機能することができません。

対照的に、エッジでのクラウドベースのDDoS攻撃対策は、攻撃が攻撃元の近くで軽減されるため、TTMの削減に役立ちます。

3. 常時稼動型とオンデマンド型の保護の考察



オンデマンド型の軽減サービスの場合、潜在的なDDoS攻撃が検出されるまで、トラフィックは通常どおり流れます。その時点で、トラフィックはクラウド軽減サービスに再ルーティングされ、元のサーバーに戻されます。

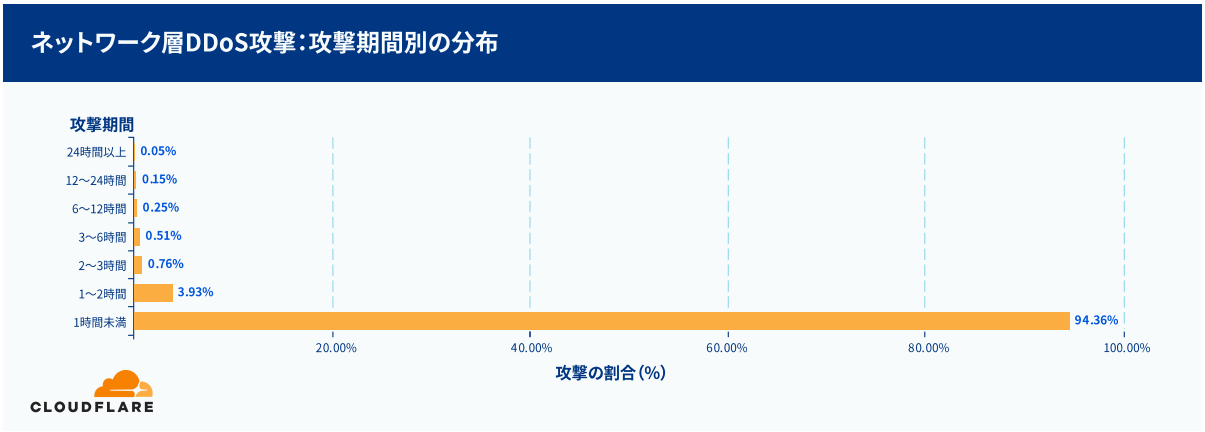
DDoS軽減の費用は、必要な場合にのみ支払うため、管理や追加のリソースは必要ありません。ただし、特にTTMに関しては、トレードオフがあります。トラフィックスパイクが特定のしきい値に到達してから分析を開始して、誰かが手動で軽減サービスを有効オンにする必要があるため、攻撃の停止には時間がかかります。

Cloudflareネットワークのデータによると、オンデマンドソリューションは攻撃の大半を占める短時間の攻撃に十分に耐えることができません。たとえば、2021年の第3四半期には、ネットワーク層攻撃の94%以上が1時間以下の攻撃でした。短時間の攻撃と言うと大したことがないように聞こえるかもしれませんが、オンデマンド保護が時間内に有効にならない場合、大きな影響を与える可能性があります。言うまでもなく、特定の状況では、数分のダウンタイムでも損害をもたらす場合があります。

攻撃者は、これらの攻撃を利用して、より大規模な攻撃を仕掛ける前に組織の防御力を試すこともできます。

パート3 - DDOS軽減に関するベストプラクティス

それに対して、常時稼働型の軽減策では継続してルーティングを行い、すべてのサイトトラフィックをフィルタリングするため、クリーンなトラフィックだけがお客様のサーバーに到達します。常時稼働型の軽減策はオンデマンド型のサービスよりも高額ではありますが、継続的な保護を実現します。これにより、サービスを手動で有効にする必要がないためTTMを削減します。



ソース： https://radar.cloudflare.com/notebooks/ddos-2021-q3

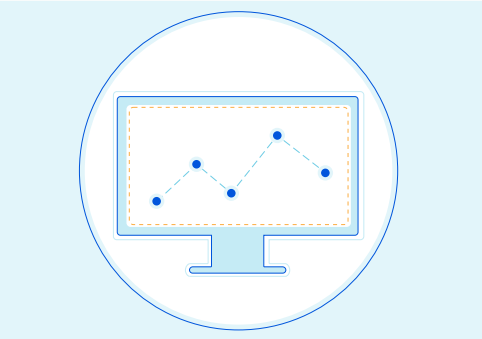
4. パフォーマンスを犠牲にしないセキュリティ対策

現在のインターネット利用者は、Webサイトとアプリケーションが常に利用可能であり、高速な読み込みができることを期待しています。実際、ほとんどのユーザーは、わずか100～120ミリ秒で遅延と感じます。ただし、遅延が1秒増えるごとにコンバージョン率が4.42%低下するため、遅延は単に不便であるだけではありません。したがって、パフォーマンスを低下させることなくDDoS攻撃から保護するには、慎重なバランスを取る必要があります。

多くの組織は、トラフィックをフィルタリングするスクラビングセンターにトラフィックをリダイレクトすることで、この問題を軽減しようとしています。しかし、これらのスクラビングセンターは、多くの場合、トラフィックの送信元や送信先ネットワークから遠く離れているため、遅延が増加するボトルネックが発生します。これにより、組織はパフォーマンスとセキュリティのどちらかを選択する必要があります。

エッジベースのクラウド型軽減サービスは、このバランスを取るためのソリューションを提供します。これらのソリューションは、一元化されたデータセンターで攻撃を軽減するのではなく、分散ネットワーク上に構築された、ネットワーク内すべてのサーバーで軽減対策が実行されます。つまり、検出と軽減措置が攻撃元のできる限り近くの場所で実行されるため、TTMを削減することができます。

5. 攻撃者の1歩先を行くための脅威インテリジェンスの採用



複雑さを増すDDoS攻撃に対抗するために、単なる階層型アプローチ以上のものが必要となります。将来の攻撃を防ぐために必要な、インテリジェントかつ適応性のある防御策を構築できるように、悪意のあるパターンについて継続的にトラフィックを分析する必要があります。

クラウドベースのDDoS軽減システムは、多くの場合、機械学習を使用して、新たな攻撃が発生する前に検出して軽減します。これは脅威インテリジェンスと呼ばれます。クラウドベースの軽減サービスを評価する際、処理能力や転送速度、フィルタリング速度を見るだけでなく、ネットワークインテリジェンスを考慮することが大切です。軽減対策を施したネットワークがさらに大きく堅牢になるほど、進化する攻撃パターンについて提供できる情報は豊かになります。—そしてより先制的な保護になります。

Cloudflareのサービス

Cloudflareの階層型セキュリティアプローチは、複数のDDoS軽減機能と組み合わされて一つのサービスとなり、悪意のあるトラフィックによるサービスの停止を防ぎながら、クリーンなトラフィックの通過を許可します。当社では、Webサイト、アプリケーション、API、ネットワーク全体の稼働を維持し、高い可用性とパフォーマンスを実現しています。

100か国250都市以上にあるデータセンターと100Tbpsを超えるネットワーク容量を持ち合わせるCloudflareは、DDoS攻撃を発信元の近くで軽減します。

迅速な、自動化された被害の軽減

スクラビングセンターに依存する従来のソリューションとは異なり、Cloudflareはネットワーク内のすべてのサーバーでセキュリティサービスをホストし、あらゆるサイズや複雑さのDDoS攻撃から保護します。

包括的な保護

CloudflareのDDoS軽減はネットワークEdgeで第3層、第4層、第7層攻撃を検出してブロックします。さらに、Cloudflare Spectrumは、Cloudflareデータセンターを介してトラフィックをプロキシし、TCP/UDPアプリケーションを保護します。

グローバル規模の脅威インテリジェンス

CloudflareのDDoS攻撃対策を支えているのは、グローバルネットワークの情報であり、この情報で何百ものインターネット上の資産を保護しています。この情報により、異常なトラフィックを識別し、高度な攻撃や新たな攻撃から保護することができます。

コスト効率に優れた保護

すべてのCloudflareのプランで、DDoS攻撃に対し、攻撃の規模に関わらず無制限かつ定額制の軽減対策を追加料金なしで提供しています。また、攻撃関連のトラフィックスパイクによるペナルティも発生しません。

パート3 - DDOS軽減に関するベストプラクティス

使いやすく管理が容易

クラウドベースの常時稼働型のDDoS保護は、直感的な操作が可能なインターフェースをベースに構築されているため、DDoS攻撃の規模や複雑さにかかわらず、数回クリックするだけで、迅速かつ簡単にインターネット上の資産を保護することができます。

セキュリティとパフォーマンスの統合

当社の提供する保護機能は、Cloudflare Webアプリケーションファイアウォール、Cloudflareボット管理、Cloudflare Magic Transit、Cloudflare負荷分散、およびCloudflare CDNなど、その他のセキュリティやパフォーマンスソリューションとシームレスに統合し、学習し、動作するよう設計されています。

自分に合ったデータ分析

Cloudflare分析では、Cloudflareの統合ダッシュボードやGraphQLを通じたDDoSイベントの分析が可能です。また、Cloudflareのログを主要なサードパーティのセキュリティ情報およびイベント管理(SIEM)ツールと統合することもできます。

まとめ

DDoS攻撃に関連する困難を乗り切るために効果的な戦略には、すべての層ですべての脅威に対応する包括的なアプローチが必要です。オンプレミスのソリューションはその一部を実現することは可能ですが、すぐに経費がかさんでしまいます。より堅牢なソリューションでは、パフォーマンスを担保しつつ、ネットワークエッジでサービスを提供するスケーラブルなクラウドベースの軽減策によって、最大限の機敏性と制限のない処理能力を提供し、DDoS攻撃の規則性や複雑さにかかわらず、保護することができます。