ホワイトペーパー

オンラインビジネスのセキュリティ、パフォーマンス、信頼性を最大化する5つの方法

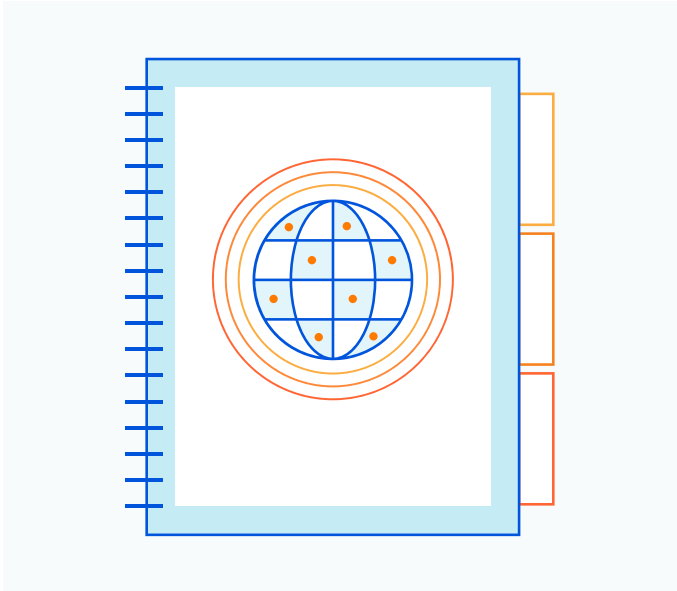
インターネットは急速に変化しており、それに伴って現代企業の性質も変わりつつあります。世界中のお客様に良質なオンライン体験を提供することは、今や必須です。Webベースのサービスとアプリケーションの需要が高まり、企業はWebサイトとアプリケーションの可能な限りの安全性、高速性、信頼性を維持すると同時に、お客様のニーズを満たしていかなければなりません。

企業はこうしてデジタル変革へ向け舵を切ることで、お客様のデジタルニーズの先取りと充足、Webベースの攻撃に対する強力な防御、遅延の克服、サイト障害の防止、ネットワークの接続性とパフォーマンスの維持といった新たな課題に直面しますが、それらは成長のチャンスでもあります。

オンラインのカスタマーエクスペリエンスを最適化する際、企業は堅牢なサイトセキュリティ、パフォーマンス、信頼性を統合する戦略を採用する必要があります。この戦略には多くのコンポーネントが含まれますが、ここでは考慮すべき点を5つ紹介します。企業が顧客のニーズに応えて、安全でシームレスなユーザー体験を提供するのに役立つことでしょう。

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

DNSとDNSSECのサポートを活用し、可用性と稼働率を最大化



インターネットの電話帳と呼ばれるドメインネームシステム（DNS）は、ブラウザがインターネットリソースを読み込めるように、ドメイン名をIPアドレスに変換します。DNSは与えられたすべてのアドレスを受け入れるように設計されているため、適切なDNSセキュリティ戦略を選択することが重要です。適切な戦略がなければ、企業はDNSハイジャック、中間者攻撃、機密性の高いユーザー情報の漏えいや喪失、フィッシング、そのほかの重大な脅威を含む、さまざまなリスクにさらされます。DNS攻撃が蔓延するようになるにつれて、耐障害性の高いDNSがないことが、セキュリティ戦略全般の弱点になっていることに気付く企業も増えています。

耐障害性の高いDNS戦略を展開するために企業が取れるアプローチがいくつかあります。その一つが、すべてのDNSレコードをホストし、世界各地に配置した複数ノードでクエリを解決して、統合型のDNSSECサポートを提供するマネージドDNSプロバイダーの利用です。DNSSECは、既存のDNSレコードに暗号署名を追加することによって、ドメインネームシステムにセキュリティ層を追加します。また、マルチDNS戦略を導入して冗長性を追加することもできます。そうすれば、プライマリDNSがダウンしても、セカンダリDNSがアプリケーションをオンラインに保ちます。独自のDNSインフラストラクチャを維持したい大企業なら、セカンダリDNSと一緒にDNSファイアウォールを実装することも可能です。

このセットアップにより、セキュリティ層がオンプレミスのDNSインフラストラクチャに追加され、全体的なDNS冗長性が確保されます。

導入事例

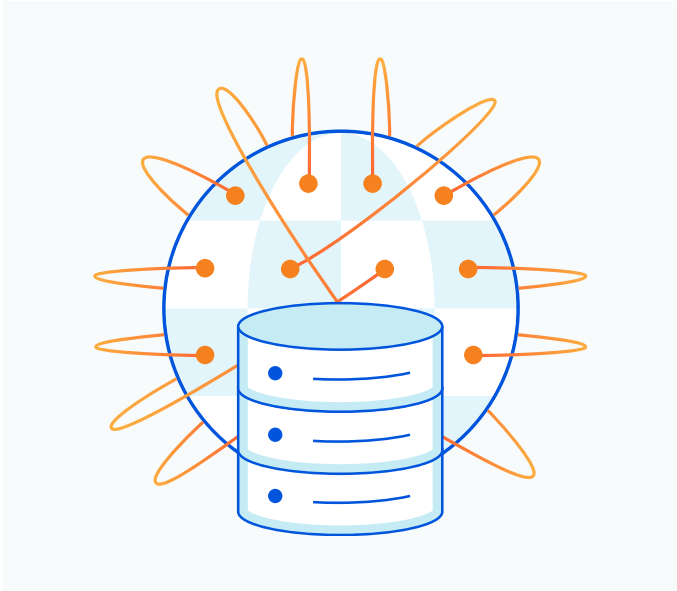
ブロックチェーンと対話するためのオープンソースのクライアント側ツールを提供する暗号通貨取引会社は、高度なDNS攻撃を受けてすべてのクエリがなりすましWebサイトに再ルーティングされたため、DNSセキュリティの強化が必要でした。ハッカーは、同社Webサイトへのクエリはすべて新しい宛先に向けられるべきであると、権威サーバーの1つに信じ込ませることに成功しました。なりすましWebサイトは同社のサイトと見た目は同じでしたが、デュープ（複製）機能を使ってユーザーのプライベートキーをハッカーに転送し、攻撃者は大量の暗号通貨へのアクセスをまんまと手に入れたのです。

この暗号通貨取引会社のサイトは、インターネット上の多くのWebサイトと同様に、インターネットのコアインフラストラクチャに重大な脆弱性があったために標的にされ、結果的に顧客の信頼を失いました。そこで同社は、こうしたことが二度と起こらないように、Cloudflare DNSを採用しました。Cloudflareへの移行は、最も簡単なDNSSEC導入方法でした。一元化された使いやすいダッシュボードからプロトコルのプロビジョニングと管理を行えるため、セキュリティ環境の耐障害性を高めるだけでなく、暗号資産の保護を同社に依存する顧客に安全性と効率性の高いユーザー体験を提供できます。

DNSおよびDNSSECの統合の詳細については、Cloudflare DNSをご覧ください。

輻輳が最も少ない経路でトラフィックをルーティングしコンテンツ配信を加速

現在、AmazonやFacebookといった大手サイトを含む、Webトラフィックの大部分はコンテンツ配信ネットワーク（CDN）経由で提供されます。CDNとは、世界中に散在するユーザーにインターネットコンテンツを高速に配信してくれる地理的に分散したサーバー群のことです。帯域幅コストの削減にも役立ちます。



世界の複数箇所にサーバーが配置されているため、CDNはWebサイト訪問者に近い場所でコンテンツを配信できます。それにより、固有のネットワーク遅延を低減し、ページ読み込み時間を短縮します。また、CDNは、ネットワーク各所のキャッシュから静的アセットを提供することで、ホストされたWebサーバーに対するリクエスト数を減らし、帯域幅コストとホスティングコストを削減します。

導入事例

世界最大級のオンデマンドフード宅配サービス会社が、ある問題に悩まされていました。米国内の何千もの都市にパートナーを擁し、オンラインプラットフォームとスマートフォンアプリを使ってドアツードア（店舗からお客様の玄関先まで）のサービスを提供する同社にとって、常にスピーディで信頼性の高いユーザー体験を提供することは極めて重要です。それが拡大するユーザー基盤を支え、地元のレストランや加盟店とのパートナーシップを強化するのです。

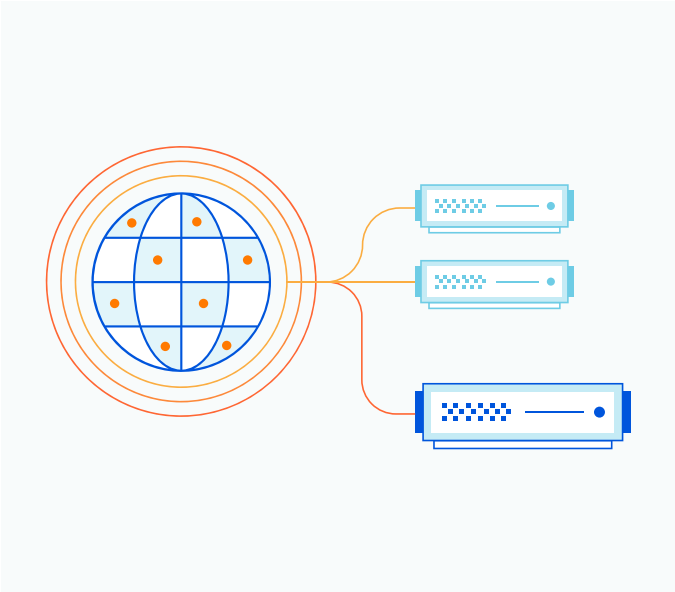
当初、この企業はパフォーマンスの面でいくつかの課題に直面していました。耐障害性のあるCDNと画像のサイズ変更ソリューションが欠如していました。このソリューションは、スムーズなユーザー体験の提供する能力で鍵となります。このサイトを訪れる顧客には、さまざまなフードオプションの高解像写真を閲覧してもらう必要があり、企業の成長に伴ってユーザーに提供するメニューも増えました。それまで利用していた画像サイズ変更ソリューションでは、毎月数千ドルのコストがかかっており、自社のプラットフォーム経由で大量の高品質画像を提供するために、画像配信を最適化し、レイテンシーを低減するソリューションを見つけることが不可欠となりました。

Cloudflareは、Cloudflareコンテンツ配信ネットワーク（CDN）で、このフード宅配サービス会社がユーザー体験を高速化するお手伝いをしています。数百万のインターネットプロパティに及ぶグローバルネットワークに支えられたCloudflare CDNは、可能な限りエンドユーザーに近い場所で静的コンテンツをキャッシュし、Argo Smart Routingと連携してコンテンツリクエストを最速のパスでインテリジェントにルーティングします。同社はさらに、Cloudflare Image Resizing（画像リサイズ）を使って画像をキャッシュし、遅延を短縮し、CPU使用率を20%下げました。

CDNが企業のコンテンツ配信をいかに高速化できるかについては、Cloudflare CDNをご覧ください。

トラフィックのグローバル負荷分散を実施することでサイトの障害リスクを最小化する

サーバーのリソースと効率性を最大化することは、微妙なバランスを取る必要がある場合があります。過負荷状態になるサーバーまたはエンドユーザーから地理的に離れすぎているサーバーは、レイテンシーやサーバー障害の発生につながる可能性が高く、収益の損失、顧客の信頼の失墜、ブランド力の低下を招く恐れがあるため、ビジネスに悪影響を及ぼす可能性があります。



クラウドベースのLoad Balancerは、トラフィックのスパイクを処理するために複数のサーバーを通してリクエストを分散します。負荷分散の決定は、ユーザーに近いネットワークエッジで行われます。こうすることで、応答時間を短縮し、サーバー障害のリスクを最小限に抑えつつ、インフラストラクチャの最適化を効率的に行うことができます。たとえ一つのサーバーで障害が発生しても、Load Balancerが他のサーバー間でトラフィックにリダイレクトして再分散できます。お客様が決して大きなレイテンシー悩まされることもサイトの中断を経験することもありません。Load Balancerがアクティブヘルスチェックを行うことで、企業はパフォーマンスが悪いサーバーを特定し、実際に故障する前に予防措置を講じることができます。

導入事例

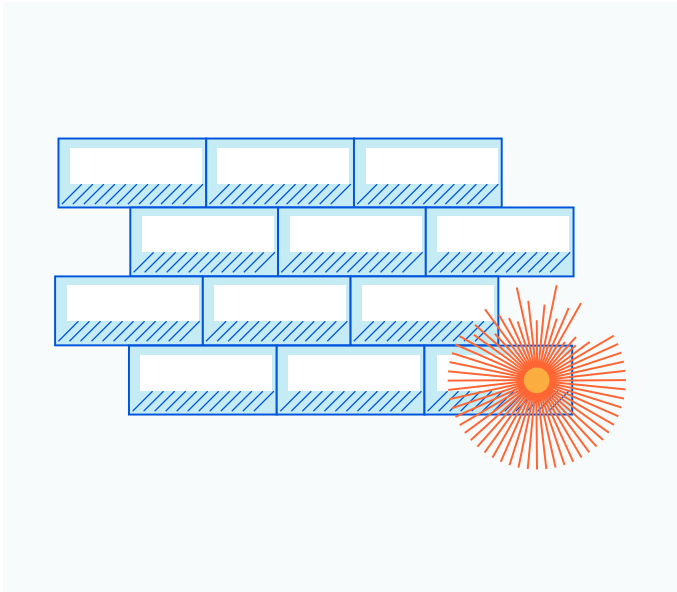
カナダに本社を置き、世界175か国で利用される大規模なeコマースプラットフォームでは、パフォーマンスとセキュリティを提供する統合型ソリューションが必要でした。実装しやすく、インフラストラクチャコストが抑えられるプロバイダーを、探していたのです。Cloudflareへの移行も、このプラットフォームを頼りにする100万以上の企業に支障をきたさないよう、シームレスに行う必要がありました。このeコマース会社は、Cloudflareのグローバルネットワーク上に各サイトを置くことによって、加盟店がより速いカスタマーエクスペリエンスを提供できるようにし、プラットフォーム全体の売上増大を実現しました。

こうしたパフォーマンス上の利点の中心となるのがCloudflareの負荷分散で、この企業は動的なステアリングが利用できるようになりました。つまり、それぞれのユーザーが使える最速の配信元サーバープールにトラフィックを導いて、レイテンシーを短縮し、さらにトラフィックをスピードアップさせることができるということです。現在、この企業は配信元サーバー間でのトラフィックの分散に対するきめ細かな制御ができるようになっており、こうしたネットワークエンジンにおける決定から、パフォーマンスや正確性において大きなメリットを生み出しています。

Cloudflare Load Balancingを使用してアプリケーションのパフォーマンスと可用性を向上させる方法をご覧ください。

悪意ある攻撃からアプリケーションを保護

インターネットは、Webベースのビジネスを、発信源も複雑度もさまざまな多岐にわたる攻撃にさらします。Webアプリケーションやその他のビジネスクリティカルなプロパティを保護する際は、階層型セキュリティ戦略が多種多様な脅威に対する防御に役立ちます。



A. Webアプリケーションファイアウォールによる保護

Webアプリケーションファイアウォール（WAF）は、HTTPトラフィックのフィルタリングやモニタリングを行うことでWebアプリケーションを保護します。企業はWAFの導入によってゼロデイ攻撃を防止し、クロスサイトリクエストフォージェリ（CSRF）、クロスサイトスクリプティング（XSS）、SQLインジェクション攻撃など、サーバーの安全性を損ないデータの窃盗や改ざんを起こしかねない一般的な脅威からアプリケーションを保護することができます。

WAFはまた、アプリケーションの脆弱性を保護し新たな脅威から防御するルールを設定することによって、セキュリティポリシーをきめ細かく調整することができます。一般に、クラウドベースのWAFは、ユーザー側に追加の作業や費用を発生させることなく新たな脅威から防御できるように常にアップデートできるので、実装の柔軟性と費用対効果が最も高いソリューションです。

導入事例

「フォーチュン500」にランクインする多国籍金融企業が、各地域で追加のマーケティングWebサイトをオンボーディングするとなったときに、これが大きな問題となりました。この企業は、グローバルオンラインプレゼンスを確立する必要がありましたが、複雑な設定を外注委託するか、以前から利用していたプロバイダーのプロによる高額なサービスに料金を支払うか、どちらかの選択肢しかありませんでした。これは非常に長い時間と法外な費用がかかる作業です。必要だったのは、Webプロパティに対してきめ細かな制御ができて、オンプレミスデータセンターとクラウドベースのアプリケーションの間でマルチクラウドアプローチをバランス良く活用できる最新のアーキテクチャソリューションでした。

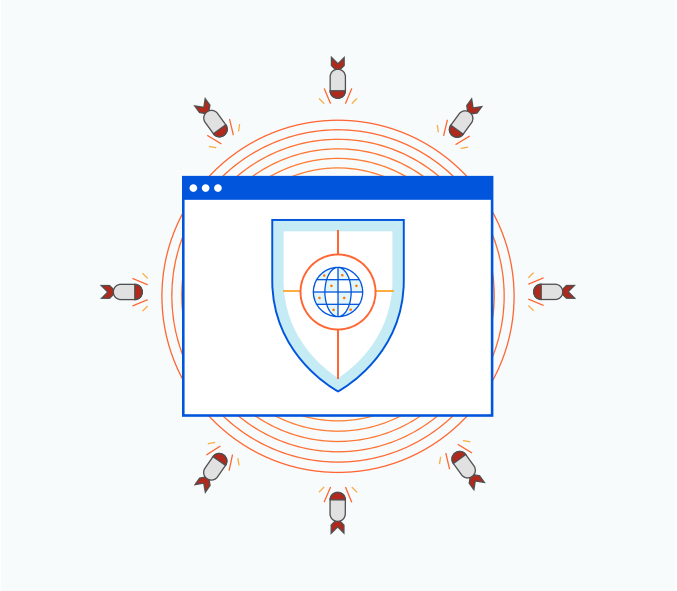
Cloudflareに切り替えた後に、同社は700以上のWebプロパティを追加費用なしに数分以内に保護することができました。今では、より柔軟なセルフサービス環境のメリットを得て、時間と貴重な社内リソースの両方を節約しています。

同社のWebサイトの多くは、銀行がデジタルカードサービスにアクセスしてほかの機密データを処理することを許可しているので、階層型セキュリティ戦略を採用することは同社にとって最優先事項です。1回の攻撃が成功しただけで、ブランドの評判が損なわれ、業者や顧客からの信頼が失われることになります。CloudflareのWebアプリケーションファイアウォール（WAF）と高度なDDoS攻撃対策があれば、すべてのサイトは攻撃や悪意のある脅威から保護されます。

CloudflareのWebアプリケーションファイアウォールを使用してビジネスクリティカルなWebアプリケーションを悪意のある攻撃から保護する方法をご覧ください。

B. DDoS攻撃対策

大部分のWebサイトにとって、大量のWebトラフィックは良いことであり、より多くのコンバージョン、お客様、売上につながります。しかし、Webトラフィックの急増は、ネットワーク接続を遮断し、サーバーを圧倒し、正当なユーザーがサイトにアクセスするのを妨げることを目的としたサイバー攻撃が原因で起きる場合もあります。



DDoS攻撃は、大量の不正なインターネットトラフィックを送り付けて、サーバー、デバイス、ネットワーク、または周辺のインフラストラクチャを過負荷状態にしようとする悪意のある行為です。こうした攻撃は、ターゲットデバイスとインターネット間の利用可能なすべての帯域幅を消費することにより、深刻なサービスの中断を引き起こすだけでなく、お客様がその企業のリソースにアクセスできなくなるため、ビジネスに大きな悪影響を及ぼします。

導入事例

インド最大のチケット発行会社は、顧客数6000万人以上、スクリーンビューは月間50億前後で、年間のチケット売上枚数は2億枚を超えます。このサービスが成功するには、高速で安全なユーザー体験の提供が何よりも大事です。顧客は、不愉快な体験をすると競合他社へと流れてしまいかねません。この企業に対する大規模なDDoS攻撃は、同社プラットフォームにとって大きなリスクでした。

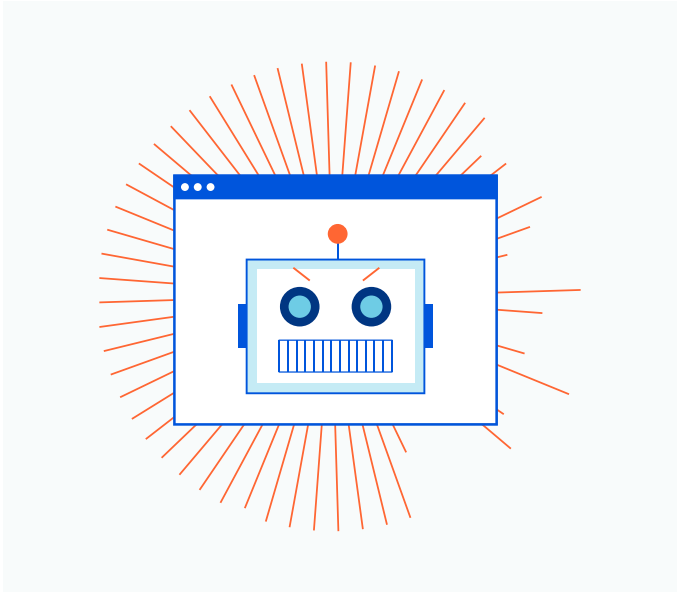
しかし、Cloudflareの高度なDDoS攻撃対策を導入したおかげで、攻撃を軽減するために「パニックモード」に入る必要はありませんでした。ネットワーク容量が121Tbps以上のCloudflareのDDoS攻撃対策は、使いやすく管理も簡単なようにデザインされており、ネットワークエッジで攻撃をブロックして、配信元サーバーがオンプレミス、ハイブリッド、マルチクラウドのいずれであっても、稼働し利用可能な状態に保ちます。

Cloudflareは、毎秒50ギガバイトまでの悪意のあるトラフィックを即座にブロックし始めました。そして、DDoS攻撃が運用を妨げたり、サイトをスローダウンさせないように効果的に防止したのです。これによって、このチケット発行会社はセキュリティ体制を改善できた上に、将来的に完全な信頼性と運用効率性を確保しました。

階層型セキュリティアプローチの採用に関する詳細は、Cloudflareの高度なDDoS攻撃対策をご覧ください。

C. 悪意のあるボットの軽減

顧客データやWebアプリケーションをサイバー脅威から十分に保護するには、階層型のアプローチが必要です。他の一般的なサイバーセキュリティ脅威に加え、悪意のあるボットの標的になると、サイトが侵害される可能性があります。悪意あるボットは、Webサーバーを過負荷状態にする、分析データを歪める、ユーザーがWebページにアクセスできないようにする、ユーザーデータを盗む、重要なビジネス機能を損なう、といった問題を起こしかねません。



良性のボットとは、Webページ上のコンテンツのスキャンからWebサイト上のお客様からの問い合わせへの対応まで、有益なタスクを実行するようプログラミングされているソフトウェアアプリケーションのことを指します。しかし、ボットもハッカーによって侵害され、クレデンシャルスタッフィング攻撃から機密データの漏えい、SEOコンテンツの盗難、業務妨害まで、悪意のある行為を行うのに使用されることがあります。ボット管理ソリューションを実装することで、良性のボットと悪性のボットを区別して、悪意のある行為がユーザー体験を損なわないようにすることができます。

導入事例

マーケティングオートメーションソフトウェア業界の有力企業がその例で、同社のWebフォームにスパムボットのアクティビティが集中し、問題を引き起こしました。同社のフォームはボットに頻繁に狙われたため、正当なユーザーがページに迅速かつ簡単にアクセスすることはまず無理になり、顧客にシームレスな体験を提供する能力が損なわれました。

そしてユーザー体験を低下させることなく、悪意のあるリクエストをブロックすることができるボット軽減ソリューションを求めて、Cloudflareへ依頼することになりました。Cloudflareのボット管理は、良性ボットと正当なトラフィックの通過を許可しつつ、Webトラフィックパターンを検出し、ボット攻撃、悪意のある攻撃をブロックするために機械学習を用います。現在、ユーザーがその企業のマーケティングソフトウェアをサービスの中断や機密データの損失のリスクを冒すことなく活用できるように、Cloudflareは毎日100万件以上の悪意のあるボットリクエストの軽減に役立てています。

Cloudflareのボット管理で、ボットの攻撃を軽減し、良性ボットと悪性ボットをリアルタイムで管理しましょう。

ネットワーク稼働率を高い水準で維持

A. ネットワークインフラストラクチャの保護

Webサーバーを保護するだけでは不十分です。多くの場合、企業はパブリック環境またはプライベート環境のデータセンターにてホストされているオンプレミスネットワークインフラストラクチャを持っています。それらについてもDDoS攻撃から保護する必要があります。多くのDDoS軽減プロバイダーは、攻撃を阻止するのに、スクラビングセンターまたはハードウェアボックスを使用したトラフィックのオンプレミスのスキャンおよびフィルタリングのいずれかの方法に依存します。両方のアプローチの問題は、レイテンシーが発生してビジネスに悪影響を及ぼすことです。

スクラビング（浄化）では、悪意のあるトラフィックを振い落とし、正常なトラフィックのみを通すために、指定した位置にある集中型スクラビングサーバーにネットワークトラフィックを再ルーティングする必要があります。すべてのトラフィックを地理的に離れたスクラビングセンターに再ルーティングすると、ほとんどのアプリケーションで許容できない追加のレイテンシーが発生してしまいます。

もう1つのDDoS軽減手法は、オンプレミスのハードウェアボックスを使ってトラフィックをスキャンし、悪意のあるリクエストをフィルターで排除するというものです。スクラビングと同様、スキャニングするハードウェアも、スキャン処理のためにネットワークトラフィックをボックス経由で再ルーティングするというボトルネックの性質を持つため、ネットワークの遅延とパフォーマンスの低下を引き起こします。多くの場合、オンプレミスのDDoS攻撃対策アプライアンスには、デフォルトで帯域幅制限が設定されています。この制限は、その企業のネットワーク容量とボックスのハードウェア容量の組み合わせに基づいて定められます。

DDoS攻撃の検出と軽減は、発信源に近いネットワークエッジで行う方が効果的です。グローバルに分散したネットワーク内の最寄りのデータセンターでトラフィックをスキャンすることにより、大規模なDDos攻撃の最中であっても、サービスの高可用性を確保することができます。このアプローチにより、不審なトラフィックを地理的に離れたスクラビングセンターにルーティングすることで発生する遅延を低減でき、攻撃への応答時間も短縮できます。

導入事例

Alexaランキングトップ10のWebサイトの1つを運用する非営利団体が、深刻な遅延とサイト停止の問題を抱えていた時、ネットワーク層の攻撃を軽減し、迅速にオンライン復帰できるソリューションが必要でした。

このように会社のサーバーを過負荷状態にして業務を全面停止させる悪意ある行為は「テイクダウン攻撃」と呼ばれ、ネットワーク層への不正なHTTPトラフィックをサーバーに殺到させました。そこで同団体から、攻撃を軽減してサイトへのアクセスを復元させると同時に、さらなる攻撃を予防するためにネットワーク層DDoS攻撃対策を実装して欲しいという依頼が、Cloudflareに入ったのです。

Cloudflare Magic Transitは、オンプレミスネットワークとデータセンターに、常時オンまたはオンデマンドの展開モードでDDoS保護を提供します。Cloudflareのグローバルネットワークを使用して、攻撃元に最も近いCloudflareデータセンター内で、DDoSトラフィックを検出および軽減します。Cloudflareの大規模なネットワークと堅牢なDDoS攻撃対策を配置し、攻撃の影響を迅速に回避し、エンドユーザー体験を通常レベルに戻すことができました。

ネットワークのDDoS攻撃対策の詳細については、Cloudflare Magic Transitをご覧ください。

B. TCP/UDPアプリケーションの保護

トランスポート層では、攻撃者はサーバー上の利用可能なポートをすべて過負荷状態にして、企業のサーバーリソースを標的にする場合があります。こうしたDDoS攻撃によって、正当なリクエストに対するサーバーの応答が遅れたり、まったく応答しなくなる恐れがあります。トランスポート層の攻撃を防止するには、攻撃パターンを自動的に検出して攻撃トラフィックをブロックできるセキュリティソリューションが必要になります。

導入事例

eスポーツ業界の有力企業でグローバルユーザー数2億人以上のゲーム制作会社において、DDoS攻撃が多数検出され、遠隔地ユーザーの一部がTCPベースのアプリケーションでユーザーエクスペリエンスの低下を経験していることが明らかになりました。ゲーム業界では、サービスのダウンタイムが顧客と収益に大幅減につながりかねないため、これはかなりの打撃です。

ゲームプロバイダーのインフラストラクチャは、ゲーマーが求める低遅延を実現するために設計された独自のネットワークプロトコルで動作します。そのため、DDoS攻撃を受けると、従来のセキュリティ製品ではカスタムプロトコルを保護することができません。

トランスポート層でパフォーマンスを向上させ、DDoS攻撃を軽減できるように、この企業はCloudflareに支援を依頼しました。どんなTCP/UDPプロトコルでも保護できるDDoS攻撃対策Cloudflare Spectrumは、エンドツーエンドのパフォーマンスを損なうことなく重要なカスタム通信プロトコルを保護し、サービスの遅延やブランドの評判低下を狙った攻撃を阻止します。また、Cloudflare SpectrumはTCP最適化やArgo Smart Routingも使って、Cloudflareネットワーク経由のTCPトラフィックを加速します。

Cloudflare Spectrumを使用して、お客様のTCP/UDPアプリケーションの速度、安全性、信頼性を向上させましょう。

まとめ

良質なオンライン体験を創出するには、適切なセキュリティ戦略とパフォーマンス戦略が必要です。そうした戦略は、企業がコンテンツ配信を加速化するだけでなく、ネットワークの信頼性を確保して各自のWebプロパティをサイトの停止、データの盗難、そのほかの重大な攻撃から保護することも可能にしなければなりません。

世界100か国以上、250都市以上に広がるネットワークを構築したCloudflareは、企業がアプリケーション（オンプレミス、クラウド、SaaS）のセキュリティ、パフォーマンス、信頼性を高めるのに役立つスケーラブルな統合グローバルクラウドプラットフォームを提供します。オンラインビジネスを保護する方法の詳細については、Cloudflare.comをご覧ください。

© 2022 Cloudflare Inc.無断転載を禁じます。Cloudflareロゴは、Cloudflareの商標です。
その他、記載されている企業名、製品名は、各社の商標または登録商標である場合があります。