AWS ホワイトペーパー

DDoS 耐性を獲得するための AWS のベストプラクティス

DDoS 耐性を獲得するための AWS のベストプラクティス: AWS ホワイトペーパー

Table of Contents

DDoS 耐性を獲得するための AWS のベストプラクティス

公開日: 2021 年 9 月 21 日 (改訂履歴)

要約

DDoS (Distributed Denial of Service: 分散型サービス拒否) 攻撃などのサイバー攻撃による影響から、ビジネスを保護することが重要です。最優先事項は、アプリケーションの可用性と応答性の維持により、サービスに対するお客様の信頼を維持することです。また、攻撃への対応としてインフラストラクチャのスケーリングが必要になった場合にも、無用な直接経費を回避する必要があります。アマゾンウェブサービス (AWS) は、インターネット上の悪意のある攻撃から防御するためのツール、ベストプラクティス、およびサービスをお客様に提供することをお約束します。AWS の適切なサービスを使用することで、高可用性、セキュリティ、耐障害性を確保できます。

AWSこのホワイトペーパーでは、AWS で実行されるアプリケーションの耐障害性を向上させるための規範的な DDoS ガイダンスを提供します。これには、アプリケーションの可用性を保護するためのガイドとなる、DDoS 耐性に関するリファレンスアーキテクチャが含まれます。このホワイトペーパーでは、インフラストラクチャレイヤー攻撃やアプリケーションレイヤー攻撃などのさまざまな種類の攻撃についても説明します。AWS では、それぞれの攻撃タイプに対してどのベストプラクティスが特に有効であるかを提示します。また、DDoS 攻撃の緩和戦略に適した各サービスや各機能の概要と、それらをアプリケーション保護に役立てる方法をご紹介します。

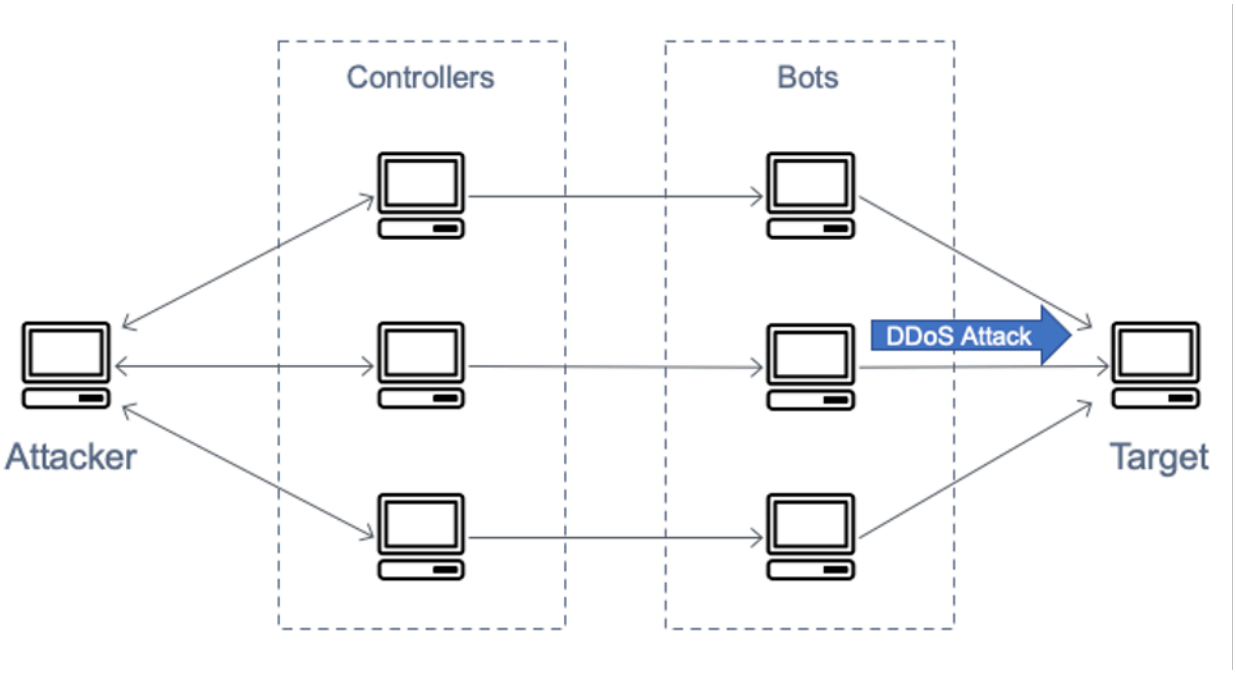
このホワイトペーパーは、ネットワーキング、セキュリティ、AWS の基本コンセプトに精通している IT 部門の意思決定者やセキュリティエンジニア向けに作成されたものです。各セクションには、ベストプラクティスや機能の詳細を記載した AWS ドキュメントへのリンクが掲載されています。

はじめに: サービス拒否攻撃

サービス拒否 (DoS) 攻撃とは、ウェブサイトやアプリケーションをユーザーが利用できなくなるように、意図的に大量のネットワークトラフィックを送信することです。これを行うために攻撃者は、大量のネットワーク帯域幅を消費したり、他のシステムリソースを拘束したりするさまざまな手法を使い、正規のユーザーによるアクセスを妨害します。この攻撃の最もシンプルな形態では、1 人の攻撃者が 1 つのソースを使い、ターゲットに対する DoS 攻撃を行います (下図を参照)。

図 1: DoS 攻撃の略図

DDoS 攻撃では、攻撃者が複数のソースを使用して、ターゲットに対する攻撃を編成します。この場合のソースには、マルウェアに感染したコンピューター、ルーター、IoT デバイス、その他のエンドポイントなどが分散した形で使用されることがあります。次の図は、侵害されたホストのネットワークが攻撃に参加し、大量のパケットまたは要求を生成してターゲットに過剰な負荷をかけていることを示しています。



DDoS 攻撃の略図

Open Systems Interconnection (OSI) モデルには 7 つのレイヤーがあり、それらについては Open Systems Interconnection (OSI) モデルの表で説明されています。DDoS 攻撃が最も生じやすいのは、レイヤー 3、4、6、7 です。レイヤー 3 と 4 での攻撃は、OSI モデルのネットワークレイヤーとトランスポートレイヤーでの攻撃を意味します。AWS はこのホワイトペーパーで、これらをまとめて

「インフラストラクチャレイヤー攻撃」と呼んでいます。レイヤー 6 および 7 での攻撃は、OSI モデルのプレゼンテーションレイヤーとアプリケーションレイヤーでの攻撃を意味します。AWS ではこれらをまとめて「アプリケーションレイヤー攻撃」と呼んでいます。これらの攻撃タイプの例については、次のセクションで説明します。

Open Systems Interconnection (OSI) モデル

番号	レイヤー	単位	説明	攻撃ベクトルの例
7	アプリケーション	データ	アプリケーションへのネットワークプロセス	HTTP フラッド、DNS クエリフラッド
6	プレゼンテーション	データ	データ表現と暗号化	TLSの悪用
5	セッション	データ	ホスト間の通信	該当なし
4	トランスポート	セグメント	エンドツーエンド接続と信頼性	SYN フラッド
3	ネットワーク	パケット	パスの決定と論理アドレス指定	UDP リフレクション攻撃
2	データリンク	フレーム	物理アドレス指定	該当なし
1	物理	ビット	メディア、信号、バイナリの送信	該当なし

トピック

インフラストラクチャレイヤー攻撃

最も一般的な DDoS 攻撃である、User Datagram Protocol (UDP) リフレクション攻撃および SYN (同期) フラッドは、インフラストラクチャレイヤー攻撃です。攻撃者はこのいずれかの方法を使って、大量のトラフィックを生成します。これによって、ネットワーク容量に余裕がなくなり、サーバー、ファイアウォール、IPS (intrusion prevention system: 侵入防止システム)、ロードバランサーなどのシステムのリソースが機能しなくなります。こうした攻撃は、簡単に特定することができるものの、効果的に緩和するには、インバウンドトラフィックでフラッドが生じる前に迅速にスケールアップできるネットワークやシステムが必要になります。スケールアップでの容量の追加によって攻撃トラフィックをフィルターで除外または吸収することができます。その結果、システムとアプリケーションが解放され、正規のお客様のトラフィックに応答できるようになります。

トピック

UDP リフレクション攻撃

User Datagram Protocol (UDP) リフレクション攻撃は、UDP がステートレスプロトコルであることを悪用した攻撃です。攻撃者は、UDP リクエストパケットに攻撃目標の IP アドレスを記載し、これを UDP 送信元 IP アドレスを持った有効なリクエストパケットとして偽装します。UDP リクエストパケットの送信元 IP の偽装が完了すると、次に攻撃者は、この偽装された送信元 IP を持った UDP パケットを中間サーバーに送信します。サーバーは、その UDP 応答パケットを攻撃者の IP アドレスではなく、攻撃目標の IP アドレスに送信してしまいます。中間サーバーが利用されるのは、これがリクエストパケットの数倍の大きさの応答パケットを生成するからです。その結果、攻撃目標の IP アドレスに送信される攻撃トラフィックはが増幅されます。

増幅係数は、レスポンスサイズとリクエストサイズの比率であり、攻撃者が使用するプロトコル (DNS、NTP、SSDP、CLDAP、Memcached、CharGen、QOTD) によって異なります。たとえば、DNS の増幅係数は、元のバイト数の 28 から 54 倍になります。したがって、攻撃者が 64 バイトのリクエストペイロードを DNS サーバーに送信すると、3400 バイト以上の不要なトラフィックが攻撃目標に送信されることになります。UDP リフレクション攻撃では、他の攻撃より多い、大量のトラフィックが生じます。図「UDP リフレクション攻撃」は、リフレクション手法とその増幅効果を示しています。

UDP リフレクション攻撃

SYN フラッド攻撃

ユーザーがウェブサーバーなどの TCP (Transmission Control Protocol) サービスに接続すると、そのクライアントは SYN (同期) パケットをサーバーに送信します。サーバーは、確認のために SYN/ACK パケットをクライアントに返します。最後にクライアントが ACK (acknowledgement: 確認) パケットをサーバーに返します。こうして目的の 3 ウェイハンドシェイクが完了します。次の図は、この典型的なハンドシェイクを示しています。

SYN 3 ウェイハンドシェイク

SYNフラッド攻撃では、悪意のあるクライアントは大量の SYN パケットを送信しますが、最後の ACK パケットを送信しないため、ハンドシェイクが完了しません。サーバーは、各 TCP 接続を半開にしたまま応答を待ち続けることになり、最終的には、新たな TCP 接続を受け入れるための容量を使い果たしてしまいます。このため、新たなユーザーはこのサーバーに接続することができません。この攻撃は、正規の接続でリソースを使用できないように、使用可能なサーバー接続を拘束しようとしています。SYN フラッドは最大で数百 Gbps に達することがありますが、攻撃の目的は SYN トラフィック量を増加させることではありません。

アプリケーションレイヤー攻撃

レイヤー 7 攻撃、すなわちアプリケーションレイヤー攻撃では、アプリケーションそのものが標的になります。こうした攻撃は、SYN フラッドによるインフラストラクチャ攻撃と同様、アプリケーションの特定の機能に過度な負荷をかけることにより、そのアプリケーションの可用性や正規のユーザーへの応答を妨害しようとするものです。この攻撃は、小さなトラフィック量しか生成しない非常に小さなリクエスト量だけで達成できる場合があります。そのため、攻撃を検出し緩和することが難しくなります。アプリケーションレイヤー攻撃には、HTTP フラッド、キャッシュバスティング攻撃、WordPress XML-RPC フラッドなどがあります。

HTTP フラッド攻撃では、攻撃者はウェブアプリケーションの正規ユーザーから送られてきたように見える HTTP リクエストを送信します。一部の HTTP フラッド攻撃では、特定のリソースを標的にしますが、巧妙な HTTP フラッド攻撃の中には、アプリケーションによって人間のインタラクションを模倣するものもあります。したがって、リクエストレート制限のような一般的な緩和技術を利用することが難しくなります。

キャッシュバスティング攻撃は、HTTP フラッドの一種で、クエリ文字列のバリエーションを利用して、コンテンツ配信ネットワーク (CDN) のキャッシングを迂回するというものです。CDN は、キャッシュされた結果を返すことができないため、ページリクエストごとにオリジンサーバーにコン

タクトしなければならず、こうしたオリジンフェッチによって、アプリケーションウェブサーバーに余計な負担がかかることになります。

WordPress XML-RPC フラッド攻撃 (WordPress Pingback フラッド) では、WordPress コンテンツ管理ソフトウェアでホストされているウェブサイトが標的になります。攻撃者は XML-RPC API 関数を悪用して、大量の HTTP リクエストを生成します。Pingback 機能では、WordPress によってホストされているウェブサイト (サイト A) から、別の WordPress サイト (サイト B) に、サイト A がサイト B へのリンクを作成したことが通知されます。次に、サイト B はサイト A を取得してリンクの存在を確認しようとします。Pingback フラッドでは、サイト B からサイト A を攻撃するためにこの機能が悪用されます。このタイプの攻撃には明確な特徴があり、通常は HTTP リクエストヘッダーの User-Agent に、WordPress が存在します。

アプリケーションの可用性に悪影響を及ぼす悪意あるトラフィックには、他の形態もあります。スクレイパーボットとは、コンテンツを盗んだり、価格などの競合情報を記録するためにウェブアプリケーションにアクセスする試みを自動化するというものです。ブルートフォース攻撃とクレデンシャルスタッフィング攻撃は、アプリケーションの安全領域への不正アクセスを可能にするようにプログラムされた試みです。厳密に言えば、これらは DDoS 攻撃ではありません。しかし、このような自動化特性を持つため、DDoS 攻撃に類似しています。したがって、このホワイトペーパーで紹介する同様のベストプラクティスを実施することで、この攻撃を緩和できる可能性があります。

アプリケーションレイヤー攻撃では、ドメインネームシステム (DNS) も標的になります。これらの攻撃で最も一般的なのは DNS クエリフラッドで、攻撃者は正しい形式の DNS クエリを大量に使用して DNS サーバーのリソースを枯渇させます。これらの攻撃には、キャッシュバスティングの要素も含まれていて、攻撃者はサブドメインの文字列をランダム化し、指定したリゾルバーのローカル DNS キャッシュをバイパスします。その結果、リゾルバーはキャッシュされたドメインのクエリを利用することができず、代わりに信頼できる DNS サーバーに繰り返しコンタクトしなければなりません。これにより、この攻撃が増幅されることになります。

ウェブアプリケーションが Transport Layer Security (TLS) を介して配信される場合、攻撃者が TLS ネゴシエーションプロセスを攻撃することも考えられます。TLS ではコンピューティング負荷が大きくなるため、攻撃者は、読み取り不能なデータ (または判読不能な暗号文) を正当なハンドシェイクとして送信し、それを処理させることでサーバーに余分な負荷をかけることにより、サーバーの可用性を低下させることができます。この攻撃の変形としては、攻撃者が TLS ハンドシェイクを完了しても、継続的に暗号化方式の再ネゴシエーションを繰り返すものがあります。攻撃者は多数の TLS セッションの開始と終了を繰り返すことで、サーバーのリソースを枯渇させようと試みることもあります。

緩和テクニック

AWS のサービスには、いくつかの DDoS 緩和策が最初から含まれています。以下の各セクションで説明するサービスを備えた AWS アーキテクチャを使用し、ユーザーとアプリケーション間のネットワークフローの各部分に追加のベストプラクティスを実装することで、DDoS 耐性をさらに向上させることができます。

AWS のお客様はすべて、追加料金なしで AWS Shield Standard の自動保護を利用できます。AWS Shield Standard は、ネットワークレイヤーおよびトランスポートレイヤーで、ウェブサイトやアプリケーションを標的として頻繁に発生する一般的な DDoS 攻撃を防御します。この保護は静的なもので、レポート作成や分析は行われません。事前構成済みで、常に有効になっています。AWS のすべてのサービスとすべての AWS リージョンで利用できます。AWS リージョンで DDoS 攻撃を検出する Shield Standard システムは、自動的にトラフィックのベースラインを決め、異常を特定します。さらに、必要に応じて、影響の拡大防止策も講じます。AWS Shield Standard を導入して、DDoS 耐性の高いアーキテクチャを構築すれば、ウェブアプリケーションもそれ以外のアプリケーションも保護できます。

また、Amazon CloudFront、Global Accelerator、Route 53 など、エッジロケーションから運用される AWS のサービスを利用して、既知のインフラストラクチャレイヤー攻撃に対する包括的な可用性保護態勢を構築することもできます。AWS Global Edge Network の一部であるこれらのサービスは、アプリケーションの DDoS 耐性を改善でき、世界中に分散したエッジロケーションからのあらゆるタイプのアプリケーショントラフィックを扱う場合に威力を発揮します。どの AWS リージョンでもアプリケーションを実行し、これらのサービスを使用してアプリケーションの可用性を保護して、正規のエンドユーザー向けにアプリケーションのパフォーマンスを最適化できます。

Amazon CloudFront、Global Accelerator、および Amazon Route 53 の使用には次のような利点があります。

- AWS Global Edge Network 全体でインターネットと DDoS の緩和機能にアクセスできます。これは、テラビット規模に達する可能性のある、大規模な攻撃を軽減するために役立ちます。
- AWS Shield の DDoS 緩和システムを AWS エッジサービスに統合して、緩和に要する時間を分単位から 1 秒未満に短縮できます。
- ステートレス SYN フラッドに対する緩和テクニックにより、着信接続を中継し、その内容を確認したうえで、保護対象のサービスに渡します。これにより、有効な接続のみがアプリケーションに到達できるようになり、誤検知によって遮断されることのないよう正当なエンドユーザーを保護できます。

- 自動トラフィックエンジニアリングシステムにより、大規模な DDoS 攻撃の影響を分散または隔離できます。これらすべてのサービスによって、攻撃がオリジンに到達する前にソースで隔離されるため、これらのサービスで保護されているシステムへの影響が小さくなります。
- AWS WAF との組み合わせにより、アプリケーションレイヤーに対する攻撃から防御できます。現在のアプリケーションアーキテクチャ (AWS リージョン、オンプレミスのデータセンターなど) を変更する必要はありません。

AWS 上のインバウンドデータ転送に対する料金は発生しません。また、AWS Shield によって緩和された DDoS 攻撃のトラフィックについても料金を支払う必要はありません。次のアーキテクチャ図には、AWS Global Edge Network サービスが含まれています。

このアーキテクチャには、ウェブアプリケーションで DDoS 攻撃に対する耐障害性を高めるために役立つ複数の AWS サービスが含まれています。「ベストプラクティスのまとめ」の表には、これらのサービスと、そのサービスが提供できる機能の概要が示されています。AWS では、このドキュメント内で参照しやすいように、各サービスにベストプラクティスインジケータ (BP1、BP2 など) を付けました。たとえば、Amazon CloudFront および Global Accelerator が提供する機能に関するセクションには、BP1 というベストプラクティスインジケータが付いています。

表 2 - ベストプラクティスのまとめ

AWS エッジ	AWS リージョン					
	Amazon CloudFront (BP1) を AWS WAF (BP2) と共に使用	Global Accelerator (BP1) を使用	Amazon Route 53 (BP3) を使用	Elastic Load Balancing (BP6) を AWS WAF (BP2) と共に使用	Amazon VPC でセキュリティグループとネットワーク ACL (BP5) を使用	Amazon EC2 Auto Scaling (BP7) を使用
レイヤー 3 攻撃 (UDP リフレクションなど	✓	✓	✓	✓	✓	✓

AWS エッジ	AWS リージョン					
) に対する緩和						
レイヤー 4 攻撃 (SYN フラッドなど) に対する緩和	✓	✓	✓	✓		
レイヤー 6 攻撃 (TLS など) に対する緩和	✓	✓	✓	✓		
攻撃対象領域の縮小	✓	✓	✓	✓	✓	
アプリケーションレイヤーのトラフィックをスケールして吸収	✓	✓	✓	✓	✓	✓
レイヤー 7 (アプリケーション層) 攻撃に対する緩和	✓	✓(*)	✓	✓	✓(*)	✓(*)

AWS エッジ	AWS リージョン					
過剰なトラフィックや大規模な DDoS 攻撃を地理的に隔離、分散	✓	✓	✓			
✓ (*): AWS WAF を Application Load Balancer と共に使用する場合						

DDoS 攻撃に対応して緩和できるように備える方法は、AWS Shield Advanced をサブスクライブすることです。

お客様には、以下に基づいて適切な検出サービスが提供されます。

- アプリケーションの特定なトラフィックパターン。
- レイヤー 7 DDoS 攻撃に対する保護 (追加コストなしで AWS WAF を含む)。
- AWS SRT からの専門サポート (24 時間 365 日)。
- AWS Firewall Manager による、セキュリティポリシーの一元管理。
- DDoS 関連の使用量の急増に起因するスケーリング料金の発生を防ぐためのコスト保護。

このようなオプションの DDoS 緩和サービスは、どの AWS リージョンにおいても、ホストされているアプリケーションの保護を支援します。このサービスは、CloudFront、Route 53、および Global Accelerator で世界中で利用できます。Shield Advanced を Elastic IP アドレスと共に使用すれば、Network Load Balancer (NLB) や Amazon EC2 のインスタンスを保護できます。

AWS Shield Advanced の使用には、次のような利点があります。

- DDoS 攻撃によりアプリケーションの可用性が損なわれた場合に、AWS SRT にアクセスし、支援を求めることができます。
- AWS Management Console、API、Amazon CloudWatch のメトリクスとアラームにより、DDoS 攻撃の状況を視覚的に把握できます。
- 過去 13 か月間のすべての DDoS イベントの履歴にアクセスできます。
- AWS ウェブアプリケーションファイアウォール (AWS WAF) に追加料金なしでアクセスし、アプリケーションレイヤーへの DDoS 攻撃を緩和できます (Amazon CloudFront または Application Load Balancer と併用した場合)。
- ウェブトラフィックの属性に関する自動ベースラインを使用できます (AWS WAF と併用した場合)。
- AWS Firewall Manager にアクセスし (追加料金なし)、自動的にポリシーを適用できます。
- 検出のしきい値をきめ細かく設定することで、トラフィックを DDoS 緩和システムに早期にルーティングして、Amazon EC2 や Network Load Balancer に対する攻撃を緩和するまでの時間を短縮できます (Elastic IP アドレスと併用した場合)。
- DDoS 攻撃によって生じたスケーリング関連のコストの一部について、コスト保護を利用して返金を求めることができます。
- AWS Shield Advanced のお客様には、拡張された専用のサービスレベルアグリーメントが適用されます。
- Shield イベントが検出された場合は、AWS SRT からプロアクティブなエンゲージメントが提供されます。
- リソースをバンドルできる保護グループにより、複数のリソースを 1 つのユニットとして扱うことで、アプリケーションに対する攻撃の検出と緩和の範囲をセルフサービスでカスタマイズできます。リソースのグループ化により、検出の精度が向上し、誤検出を最小限に抑えることができます。新しく作成されたリソースの自動保護が容易になり、1 つのアプリケーションを構成する多数のリソースに対する攻撃を緩和するまでの時間を短縮できます。保護グループの詳細については、「Shield Advanced 保護グループ」を参照してください。

AWS Shield Advanced の機能の完全なリストおよび AWS Shield の詳細については、「AWS Shield の仕組み」を参照してください。

トピック

- AWS での DDoS 緩和のベストプラクティス
- AWS エッジロケーションをスケールに活用 (BP1、BP3)
- アプリケーションレイヤーの防御 (BP1、BP2)

AWS での DDoS 緩和のベストプラクティス

以下の各セクションでは、DDoS 緩和の手段として推奨されている各ベストプラクティスについて、詳しく説明しています。静的または動的なウェブアプリケーション用の DDoS 緩和レイヤーを迅速に構築して容易に実装するためのガイドについては、「How to Help Protect Dynamic Web Applications Against DDoS Attacks」を参照してください。

インフラストラクチャレイヤーの防御 (BP1、BP3、BP6、BP7)

従来のデータセンター環境では、インフラストラクチャレイヤーに対する DDoS 攻撃に対抗するために、キャパシティのオーバープロビジョニング、DDoS 緩和システムのデプロイ、DDoS 緩和サービスによるトラフィックのスクラブなどの対策を講じていました。AWS には DDoS 耐性が組み込まれていますが、この緩和機能を充分に活かし過剰なトラフィックに応じてスケールを調整できるアーキテクチャを選択することによって、アプリケーションの DDoS 耐性を最適化することもできます。

大量の DDoS 攻撃を緩和するためには主に、充分な中継能力および多様性の許容、Amazon EC2 インスタンスなどの AWS リソースを攻撃トラフィックから保護する方法などを考慮する必要があります。

Amazon EC2 インスタンスタイプの中には、最大 100 Gbps のネットワーク帯域幅のインターフェイスや拡張ネットワーキングなど、より簡単に大量のトラフィックを処理するための機能をサポートしているものもあります。これは、Amazon EC2 インスタンスに到達したトラフィックによる、インターフェイスの輻輳を防ぐために役立ちます。拡張ネットワーキングをサポートするインスタンスでは、従来の実装より、高い I/O パフォーマンス、広い帯域幅、低い CPU 使用率になります。これにより、インスタンスで大量のトラフィックを処理する能力が向上し、最終的にはパケット/秒 (pps) の負荷に対する耐障害性が高まります。

この高レベルの耐障害性を実現するために、AWS で使用が推奨されているのは、Amazon EC2 ハードウェア専有インスタンスか、高いネットワークスループットと最大 100 Gbps のネットワーク帯域幅の拡張ネットワーキングをサポートする N サフィックスの Amazon EC2 インスタンスです。例えば、c6gn.16xlarge や c5n.18xlarge の他、c5n.metal などの metal インスタンスを選択できます。

100 ギガビットネットワークインターフェイスおよび拡張ネットワーキングをサポートする Amazon EC2 インスタンスの詳細については、「Amazon EC2 インスタンスタイプ」を参照してください。

拡張ネットワーキングに必要なモジュールと必要な enaSupport 属性セットは、Amazon Linux 2 および最新バージョンの Amazon Linux AMI に含まれています。したがって、サポートされるインスタンスタイプで HVM バージョンの Amazon Linux を使用してインスタンスを起動した場合、拡張ネッ

トワーキングは既にインスタンスで有効になっています。詳細については、「拡張ネットワーキングが有効化されているかどうかのテスト」を参照してください。拡張ネットワーキングを有効にする方法の詳細については、「Linux での拡張ネットワーキング」を参照してください。

Amazon EC2 でオートスケーリングを使用 (BP7)

インフラストラクチャおよびアプリケーションレイヤーに対する攻撃があったとき、拡張 (スケールアウト) して対処するという方法もあります。ウェブアプリケーションを運用する際には、ロードバランサーを使って Amazon EC2 インスタンスにトラフィックを分散しますが、このインスタンスを多めに準備する、あるいは自動的に拡張 (スケールアウト) するよう設定できます。こうしておけば、フラッシュクラウド、アプリケーション層に対する DDoS 攻撃などにより、突発的にトラフィックが増加しても対処できるのです。Amazon CloudWatch のアラームに応じて Auto Scaling を起動するよう設定すると、CPU、RAM、ネットワーク I/O、あるいはカスタムメトリクスなどについて定義したイベントに応じて、自動的に Amazon EC2 のフリートサイズがスケーリングされます。このアプローチにより、想定以上にリクエスト量が増えても、アプリケーションの可用性が損なわれることはありません。アプリケーションで Amazon CloudFront、Application Load Balancer、Classic Load Balancer、または Network Load Balancer を使用すると、TLS ネゴシエーションがディストリビューション (Amazon CloudFront) またはロードバランサーによって処理されます。これらの機能は、正当なリクエストも TLS を悪用した攻撃も処理できるようにスケーリングすることによって、TLS ベースの攻撃による影響が及ばないようにインスタンスを保護します。

Amazon CloudWatch による Auto Scaling の起動について詳しくは、「Auto Scaling グループとインスタンスの CloudWatch メトリクスをモニタリングする」を参照してください。

Amazon EC2 では、コンピューティング性能の規模を変更できます。要件の変化に応じて、迅速にスケールアップまたはスケールダウンが可能です。アプリケーションにインスタンスを自動的に追加することで水平方向にスケーリングするには、Amazon EC2 Auto Scaling グループのサイズをスケーリングします。垂直方向にスケーリングするには、より大きな EC2 インスタンスタイプを使用します。

Elastic Load Balancing (BP6)

大規模な DDoS 攻撃を受けると、単一の Amazon EC2 インスタンスの処理能力では対処しきれないことがあります。Elastic Load Balancing (ELB) を導入すると、多数のバックエンドインスタンスにトラフィックを分散することにより、アプリケーションに過剰な負荷がかかるリスクを軽減できます。フラッシュクラウドや DDoS 攻撃により、予期しない過剰なトラフィックが発生すると、Elastic Load Balancing により自動的に拡張 (スケールアウト) が行われ、より大きなボリュームの処理が可能になります。Amazon VPC 内に構築したアプリケーションについては、その種類に

応じて、Application Load Balancer (ALB)、Classic Load Balancer (CLB)、Network Load Balancer (NLB) という 3 種類の ELB を考慮する必要があります。

ウェブアプリケーションには Application Load Balancer が有効です。トラフィックをその内容に基づいて振り分け、正当なウェブ要求のみ受け入れるようにします。Application Load Balancer は、SYN フラッドや UDP リフレクション攻撃など、一般的な DDoS 攻撃の多くをブロックすることで、アプリケーションを攻撃から保護します。このような攻撃が検出されると、過剰なトラフィックを吸収できるように、Application Load Balancer によって自動的にスケーリングが行われます。インフラストラクチャレイヤー攻撃によるスケーリング処理は、AWS のお客様が意識する必要はなく、料金にも影響しません。

Application Load Balancer によるウェブアプリケーションの保護の詳細については、「Application Load Balancer の開始方法」を参照してください。

TCP ベースのアプリケーションには Network Load Balancer が有効です。Amazon EC2 インスタンスなどのターゲットへのトラフィックのルーティングで、レイテンシーはほとんど生じません。Network Load Balancer に関する重要な考慮事項は、有効なリスナーを介してロードバランサーに到達したトラフィックが、吸収されるのではなくターゲットにルーティングされるという点です。Shield Advanced を使用すると、Elastic IP アドレスの DDoS 保護を設定できます。アベイラビリティーゾーンごとに Elastic IP アドレスがネットワークロードバランサーに割り当てられると、Shield Advanced は Network Load Balancer のトラフィックに関連する DDoS 保護を適用します。

Network Load Balancer による TCP アプリケーションの保護の詳細については、「Network Load Balancer の開始方法」を参照してください。

AWS エッジロケーションをスケールに活用 (BP1、BP3)

拡張性に優れた多様なインターネット接続へのアクセスにより、アプリケーションの可用性への影響を最小限に抑えながら、ユーザーに対するレイテンシーとスループットを最適化し、DDoS 攻撃を吸収して、障害を分離する能力が大幅に向上します。AWS エッジロケーションは、ネットワークインフラストラクチャの追加レイヤーとして、Amazon CloudFront、Global Accelerator、および Amazon Route 53 を使用するすべてのウェブアプリケーションにこれらの利点を提供します。これらのサービスにより、AWS リージョンから実行されるアプリケーションをエッジで包括的に保護できます。

エッジでのウェブアプリケーションの配信 (BP1)

Amazon CloudFront は、静的、動的、ストリーミング、またはインタラクティブなコンテンツなど、ウェブサイト全体の配信に使用できるサービスです。配信するコンテンツがキャッシュ可能なものでない場合も、永続的な接続と可変の有効期限 (TTL) 設定により、オリジンからのトラフィックの負荷を軽減します。これらの CloudFront 機能を使用すると、オリジンへのリクエスト数と TCP 接続の数が減り、HTTP フラッド攻撃からウェブアプリケーションを保護するために役立ちます。CloudFront は正当な接続のみを受理することにより、SYN フラッドや UDP リフレクションなど、よく知られたさまざまな DDoS 攻撃がオリジンに到達しないよう防御します。さらに、DDoS 攻撃を地理的に攻撃元に近い場所に隔離して、トラフィックの影響が他の場所に及ばないようにします。このような機能により、大規模な DDoS 攻撃を受けている間でも、正当なユーザー向けにトラフィックを配信し続ける能力が大幅に向上します。CloudFront を使用すると、AWS またはその他のインターネット上の場所にあるオリジンを保護できます。

Simple Storage Service (Amazon S3) を使ってインターネット上で静的コンテンツを提供している場合、AWS では、Amazon CloudFront によるバケットの保護をお勧めします。Origin Access Identify (OAI) を使えば、ユーザーが CloudFront URL を使ってオブジェクトにアクセスするよう強制できます。

OAI について詳しくは、「オリジンアクセスアイデンティティ (OAI) を使用して Amazon S3 コンテンツへのアクセスを制限する」を参照してください。

Amazon CloudFront を使ってウェブアプリケーションを保護し、そのパフォーマンスを最適化する方法については、「Amazon CloudFront の開始方法」を参照してください。

AWS Global Accelerator を使用して、オリジンからのネットワークトラフィックをさらに保護 (BP1)

Global Accelerator は、ユーザートラフィックの可用性とパフォーマンスを最大 60% 向上させるネットワークサービスです。これは、ユーザーに最も近いエッジロケーションでトラフィックを受信し、アプリケーションが実行されている AWS リージョンが単一か複数かにかかわらず、AWS グローバルネットワークインフラストラクチャを介してトラフィックをアプリケーションにルーティングすることで実現されます。

Global Accelerator は、ユーザーに最も近い AWS リージョンのパフォーマンスに基づいて、TCP および UDP トラフィックを最適なエンドポイントにルーティングします。アプリケーションに障害が発生した場合、Global Accelerator は 2 番目に適しているエンドポイントに 30 秒以内にフェイルオーバーします。Global Accelerator では、アプリケーションを保護するために、AWS グローバル

ネットワークの膨大なキャパシティと Shield との統合を使用します (新しい接続を試行し、正規のエンドユーザーのみにサービスを提供するステートレス SYN プロキシ機能など)。

CloudFront でサポートされていないプロトコルをアプリケーションで使用している場合や、グローバル静的 IP アドレスを必要とするウェブアプリケーションを運用している場合でも、エッジでのウェブアプリケーション配信のベストプラクティスと同じ多くの利点を提供する DDoS 耐性アーキテクチャを実装できます。例えば、エンドユーザーがファイアウォールの許可リストに追加でき、AWS の他のお客様には使用されない IP アドレスが必要になったとします。このようなシナリオでは、Global Accelerator を使用して、Application Load Balancer で実行されているウェブアプリケーションを保護し、AWS WAF と連携して、ウェブアプリケーションレイヤーでのリクエストフラッドを検出して緩和することもできます。

Global Accelerator を使用したネットワークトラフィックの保護とパフォーマンスの最適化の詳細については、「Global AcceleratorGlobal Accelerator の開始方法」を参照してください。

エッジでのドメイン名の解決 (BP3)

Amazon Route 53 は、可用性および拡張性に優れたドメインネームシステム (DNS) サービスであり、トラフィックをウェブアプリケーションに導くために使用できます。トラフィックフロー、ヘルスチェックとモニタリング、レイテンシーに基づくルーティング、Geo DNS などの高度な機能が含まれています。これらの機能により、サービスが DNS 要求にどのように応答するかを制御して、ウェブアプリケーションのパフォーマンスを向上させ、サイトの停止を回避できます。

Amazon Route 53 では、DNS サービスが DDoS 攻撃の標的になっても、正当なユーザーがアプリケーションにアクセスできるように、シャッフルシャーディング、エニーキャストストライピングなどの手法が使用されます。

シャッフルシャーディングでは、委託セットの各ネームサーバーがエッジロケーションおよびインターネットパスの一意のセットに対応します。これにより、耐障害性が向上し、お客様間の重複が最小化されます。委託セットの 1 つのネームサーバーが利用できない場合、ユーザーは他のエッジロケーションにある別のネームサーバーに問い合わせ、応答を得ることができます。

エニーキャストストライピングには、各 DNS リクエストに対して最適なロケーションから応答するよう制御して、ネットワーク負荷を分散し、DNS の遅延を抑える働きがあります。これにより、ユーザーへの応答が速くなります。さらに、Amazon Route 53 は DNS クエリのソースとボリュームの異常を検出し、信頼できることが分かっているユーザーからのリクエストを優先させることができます。

Amazon Route 53 を使用してユーザーからのトラフィックをアプリケーションにルーティングする方法について詳しくは、「Amazon Route 53 の使用開始」を参照してください。

アプリケーションレイヤーの防御 (BP1、BP2)

ここまでで説明した手法の多くは、インフラストラクチャレイヤーでの DDoS 攻撃がアプリケーションの可用性に与える影響を軽減するというものです。アプリケーションレイヤーへの攻撃からの防御も行うためには、悪意のあるリクエストの検出、スケーリングによる吸収、ブロックを実行できるアーキテクチャを実装する必要があります。一般に、ネットワークベースの DDoS 緩和システムは、アプリケーションレイヤーを対象とする複雑な攻撃の緩和には効果がないので、この点を考慮するのは重要です。

悪意のあるウェブリクエストの検出とフィルタリング (BP1、BP2)

アプリケーションが AWS 上で稼働していれば、Amazon CloudFront と AWS WAF を活用して、アプリケーションレイヤーに対する DDoS 攻撃から防御できます。

Amazon CloudFront を使用すると、静的コンテンツをキャッシュして AWS エッジロケーションから配信できるため、オリジンへの負荷を軽減できます。また、ウェブ以外のトラフィックがオリジンに到達するのを防ぐことで、サーバーの負荷を軽減するためにも役立ちます。さらに CloudFront では、意図的に低速で読み書きを行う攻撃 (Slowloris など) を受けた場合に、自動的に接続を閉じることができます。

AWS WAF を使用すると、CloudFront ディストリビューションや Application Load Balancer にウェブアクセス制御リスト (ウェブ ACL) を設定することにより、リクエスト署名に基づいて不適格なリクエストをフィルターで選別し、ブロックできます。各ウェブ ACL には、リクエスト属性 (URI (Uniform Resource Identifier)、クエリ文字列、HTTPメソッド、ヘッダーキーなど) を文字列や正規表現と照合するためのルールを設定します。さらに、AWS WAF のレートベースのルールを使用することで、ルールに合致したリクエストが所定のしきい値を超えたときに、攻撃者の IP アドレスを自動的にブロックすることも可能です。

悪意のあるクライアントの IP アドレスからのリクエストには 403 Forbidden というエラー応答が返され、そのリクエストは、リクエストレートが所定のしきい値を下回るまで引き続きブロックされます。この方法は、正常なウェブトラフィックのように偽装した HTTP フラッド攻撃への緩和策として有用です。IP アドレス評価に基づいて攻撃をブロックするには、IP 照合条件を使用してルールを作成するか、AWS Marketplace の出品者が提供する AWS WAF 用マネージドルールを使用します。AWS WAF では、IP 評価ルールグループを選択できるマネージドサービスとして、AWS Managed Rules が直接提供されています。Amazon IP 評価リストルールグループには、Amazon 内部脅威インテリジェンスに基づくルールが含まれています。これは、ボットやその他の脅威に関連付けられていると考えられる IP アドレスをブロックする場合に便利です。匿名 IP リストルールグループには、ビューワー ID の難読化を許可するサービスからのリクエストをブロックするルールが含ま

れています。これには、VPN、プロキシ、Tor ノード、クラウドプラットフォーム (AWS など) からのリクエストが含まれます。AWS WAF と CloudFront では、地理的な制限を設定して、選択した国からのリクエストをブロックまたは許可することもできます。これにより、サービス提供対象ではない国や地域からの攻撃を遮断できます。

悪意のあるリクエストを特定するには、ウェブサーバーのログを確認するか、AWS WAF のログ機能や Sampled Requests 機能を使用します。AWS WAF のログ記録を有効にすると、ウェブ ACL によって分析されたトラフィックに関する詳細情報を取得できます。AWS WAF ではログフィルタリングがサポートされているため、どのウェブリクエストをログに記録し、どのリクエストを検査後にログから破棄するかを指定できます。

ログに記録される情報には、AWS リソースから AWS WAF がリクエストを受信した時刻、リクエストに関する詳細情報、リクエストされた各ルールに関する照合アクションが含まれます。Sampled Requests では、過去 3 時間以内に AWS WAF ルールの 1 つに一致したリクエストに関する詳細が表示されます。この情報を使用して、悪意がある可能性が高いトラフィックの特徴を見つけ、該当するリクエストを拒否するルールを作成できます。ランダムなクエリ文字列を含むリクエストが多数表示される場合は、アプリケーションのキャッシュに関連するクエリ文字列パラメータのみを許可するようにしてください。このテクニックは、オリジンへのキャッシュバスティング攻撃を緩和するために役立ちます。

AWS Shield Advanced をサブスクライブしている場合は、アプリケーションの可用性に悪影響を与えている攻撃を緩和するためのルールを作成できるように、AWS Shield Response Team (SRT) に支援を求めることも可能です。AWS SRT には、お客様のアカウントの Shield Advanced および AWS WAF API への制限付きアクセス権を付与できます。AWS SRT はこれらの API にアクセスし、お客様の明示的な承認がある場合に限り、お客様のアカウントに緩和策を適用します。詳細については、このドキュメントの「サポート」セクションを参照してください。

AWS Firewall Manager を使用すると、Shield Advanced による保護や AWS WAF ルールなどのセキュリティルールを組織全体で一元的に設定および管理できます。AWS Organizations の管理アカウントでは、Firewall Manager ポリシーの作成権限を持つ管理者アカウントを指定できます。これらのポリシーにより、リソースタイプやタグなど、どこにルールを適用するかを決定する条件を定義できます。これは、複数のアカウントがあり、保護を標準化する必要がある場合に便利です。

詳細については、以下を参照してください。

- AWS Managed Rules for AWS WAF については、「AWS Managed Rules for AWS WAF」を参照してください。
- Amazon CloudFront ディストリビューションに対するアクセスを地理的に制限する機能については、「コンテンツの地理的ディストリビューションの制限」を参照してください。

- AWS WAF の使用については、以下を参照してください。
  - AWS WAF の開始方法
  - ウェブ ACL トラフィック情報のログ記録
  - ウェブリクエストのサンプルの表示
- レートベースのルール設定については、「Protect Web Sites and Services Using Rate-Based Rules for AWS WAF」を参照してください。
- Firewall Manager を使用して AWS リソース全体にわたる AWS WAF ルールの展開を管理する方法については、以下を参照してください。
  - Firewall Manager AWS WAF ポリシーの開始方法
  - Firewall Manager Shield Advanced ポリシーの開始方法

攻撃対象領域の縮小

AWS ソリューションを設計する際には、攻撃者がアプリケーションを標的とする機会の制限も重要な考慮事項の 1 つです。この考え方に基づく防御方法を、攻撃対象領域の縮小といいます。インターネットに露出していないリソースは、攻撃がより困難であり、攻撃者がアプリケーションの可用性を標的にするための手段が限られることになります。

例えば、ユーザーによる直接操作用でないリソースは、インターネットからアクセスできないように保管してください。同様に、通信に必要のないポートやプロトコルでは、ユーザーや外部アプリケーションからのトラフィックを受け付けないようにしてください。

次のセクションでは、攻撃対象領域を縮小し、インターネットへのアプリケーションの露出を制限するための AWS のベストプラクティスを示します。

トピック

AWS リソースの難読化 (BP1、BP4、BP5)

通常、ユーザーが迅速かつ簡単にアプリケーションを利用するために、AWS リソースがすべてインターネットに公開されている必要はありません。たとえば、Amazon EC2 インスタンスが Elastic Load Balancing の背後にある場合、これらのインスタンス自体をパブリックアクセス可能な状態にしておく必要はありません。代わりに、特定の TCP ポートで Elastic Load Balancing へのアクセスをユーザーに提供し、Elastic Load Balancing のみにインスタンスとの通信を許可することができます。これは、Amazon Virtual Private Cloud (VPC) 内に、セキュリティグループとネットワークアクセス制御リスト (NACL) を作成することによって設定できます。Amazon VPC では、AWS クラウド上に、論理的に隔離されたセクションをプロビジョニングできます。そこでは、ユーザーが定義した仮想ネットワーク内で AWS リソースを起動することができます。

セキュリティグループとネットワーク ACL は、VPC 内での AWS リソースへのアクセスを制御できるという点で似ています。ただし、セキュリティグループではインスタンスレベルでインバウンドおよびアウトバウンドのトラフィックを制御しますが、ネットワーク ACL では同様の機能を VPC のサブネットレベルで提供します。セキュリティグループやネットワーク ACL の使用に追加料金はかかりません。

セキュリティグループとネットワークアクセス制御リスト (ネットワーク ACL) (BP5)

セキュリティグループをインスタンスの起動時に指定することも、必要になった時点で、インスタンスにセキュリティグループを関連付けることもできます。許可ルールで明示的にトラフィックを許可しない限り、セキュリティグループに対するインターネットトラフィックはすべて、暗黙的に拒否されます。例えば、ウェブアプリケーションで Elastic Load Balancing と複数の Amazon EC2 インスタンスを使用している場合に、Elastic Load Balancing 用に 1 つのセキュリティグループ (Elastic Load Balancing セキュリティグループ) を作成し、インスタンス用に 1 つのセキュリティグループ (ウェブアプリケーションサーバーセキュリティグループ) を作成するとします。そのうえで、インターネットから ELB セキュリティグループ、ELB セキュリティグループからウェブアプリケーションサーバーセキュリティグループのそれぞれについて、トラフィックを許可するルールを作成します。こうすれば、インターネットトラフィックは Amazon EC2 インスタンスと直接通信できないため、攻撃者がアプリケーションに関する情報を得て何らかの影響を及ぼすことが困難になります。

ネットワーク ACL には許可ルールと拒否ルールの両方を指定できます。拒否ルールは、特定のタイプのトラフィックを明示的に拒否したい場合に使います。たとえば、IP アドレス (CIDR 範囲の形で)、プロトコル、送信先ポートを定義して、全サブネットに対するアクセスを拒否できます。TCP トラフィックのみを対象としたアプリケーションであれば、UDP トラフィックをすべて拒否するルールを作成できます (逆も同様)。この機能は DDoS 攻撃への対抗手段として有用です。攻撃元の特徴 (IP アドレスなど) が分かっていれば、攻撃に対抗するための独自ルールを作成できるためです。

AWS Shield Advanced をサブスクライブしている場合は、保護されたリソースとして Elastic IP アドレスを登録できます。保護されたリソースとして登録した Elastic IP アドレスに対する DDoS 攻撃は、より迅速に検出できるため、より短い時間で対処できます。DDoS 緩和システムは攻撃を検出すると、その標的である Elastic IP に対応したネットワーク ACL を読み込み、AWS ネットワーク境界でそのルールを適用します。これにより、インフラストラクチャレイヤーのさまざまな DDoS 攻撃による影響を、大幅に軽減できます。

DDoS 耐性を最適化するためのセキュリティグループおよびネットワーク ACL の設定については、「How to Help Prepare for DDoS Attacks by Reducing Your Attack Surface.」を参照してください。

保護されたリソースとして Shield Advanced と Elastic IP アドレスを使用する方法の詳細については、「AWS Shield Advanced のサブスクライブ」の手順を参照してください。

オリジンの保護 (BP1、BP5)

VPC 内のオリジンで Amazon CloudFront を使用している場合に、CloudFront ディストリビューションのみがリクエストをオリジンに転送できるようにしたいことがあります。Edge-to-Origin リクエストヘッダーを使用すると、CloudFront からオリジンにリクエストを転送する際に、既存のリクエストヘッダーの値への追加または上書きが可能です。X-Shared-Secret ヘッダーなどの Origin カスタムヘッダーを使用すると、オリジンに対して行われたリクエストが CloudFront から送信されたことを検証できます。

オリジンカスタムヘッダーによるオリジンの保護について詳しくは、「オリジンリクエストへのカスタムヘッダーの追加」および「Application Load Balancers へのアクセスを制限する」を参照してください。

オリジンアクセス制限用にオリジンカスタムヘッダーの値を自動的にローテーションするためのサンプルソリューションの実装に関するガイドについては、「How to enhance Amazon CloudFront origin security with AWS WAF and Secrets Manager」を参照してください。

または、CloudFront トラフィックのみを許可するようにセキュリティグループルールを自動的に更新する AWS Lambda 関数を使用することもできます。これはオリジンのセキュリティ向上に効果的です。悪意あるユーザーがウェブアプリケーションにアクセスする際、CloudFront や AWS WAF を迂回できないからです。

セキュリティグループの自動更新によるオリジンの保護について詳しくは、「X-Shared-Secret ヘッダー」および「How to Automatically Update Your Security Groups for Amazon CloudFront and AWS WAF by Using AWS Lambda」を参照してください。

API エンドポイントの保護 (BP4)

通常、API を公開した場合、この API のフロントエンドが DDoS 攻撃の対象になる危険性があります。このリスクを軽減するには、Amazon EC2 や AWS Lambda などで動作するアプリケーションに到る通路として、Amazon API Gateway を使用できます。Amazon API Gateway を使用すると、API フロントエンドのために独自のサーバーを用意する必要がなくなります。アプリケーションの他のコンポーネントは難読化することができます。アプリケーションのコンポーネントが外部から検出しにくければ、AWS リソースが DDoS 攻撃の標的になるリスクも軽減されます。

Amazon API Gateway を用いる際、API エンドポイントは 2 つの種類から選択できます。1 つ目 (デフォルトの選択肢) はエッジ最適化された API エンドポイントで、Amazon CloudFront ディストリビューション経由でアクセスされます。ディストリビューションは API ゲートウェイが作成、管理するようになっているため、制御はできません。2 番目のオプションは、REST API がデプロイされ

ているのと同じ AWS リージョンからアクセスされるリージョン API エンドポイントを使用する方法です。AWS では、この 2 番目のタイプのエンドポイントを使用して、独自の Amazon CloudFront ディストリビューションに関連付けることをお勧めしています。これにより、Amazon CloudFront ディストリビューションを管理し、AWS WAF を使ってアプリケーションレイヤーを保護できるようになります。このモードでは、AWS グローバルエッジネットワーク全体でスケーリングされた DDoS 緩和機能にアクセスできます。

Amazon CloudFront および AWS WAF を Amazon API Gateway と組み合わせて使用する場合は、以下のオプションを設定してください。

- ディストリビューションに対するキャッシュの動作については、API Gateway リージョンのエンドポイントにヘッダーをすべて転送するよう設定します。CloudFront はコンテンツが動的に変化するものとして扱い、キャッシュとして保存しないようになります。
- API Gateway を直接アクセスから保護するため、ディストリビューションにオリジンのカスタムヘッダー `x-api-key` が含まれるよう、API Gateway の API キーの値を設定します。
- バックエンドを過剰なトラフィックから保護するには、REST API の各メソッドに対し、標準レートまたはバーストレートの制限を設定します。

Amazon API Gateway での API 作成について詳しくは、「Amazon API Gateway ご利用開始にあたって」を参照してください。

オペレーションテクニック

このホワイトペーパーで説明する手法を取り入れると、DDoS 攻撃に対する耐性があるアプリケーションを構築できます。多くの場合、アプリケーションに対する DDoS 攻撃を検知し、対処するためにも有用です。このセクションでは、異常な動作の視覚的な把握、アラートと自動化、拡張 (スケールアウト) による保護の管理、AWS の活用によるサポートの獲得について、ベストプラクティスを紹介します。

トピック

可視性

重要なオペレーションメトリクスが想定値を大幅に逸脱している場合、アプリケーションの可用性を標的とした攻撃を受けている可能性があります。アプリケーションの正常な挙動を充分に把握していれば、異常を検出した際、より迅速に対処できます。AWS で稼働するアプリケーションを Amazon CloudWatch でモニタリングすることが、その役に立ちます。メトリクスを収集し追跡する、ログファイルを収集し監視する、アラームを設定する、AWS リソースの変化に対して自動的に応答する、といったことが可能です。

DDoS 耐性に優れたリファレンスアーキテクチャに基づいてアプリケーションを設計していれば、インフラストラクチャレイヤーに対する一般的な攻撃は、アプリケーションに到達する前にブロックできます。AWS Shield Advanced をサブスクライブすると、さまざまな CloudWatch メトリクスにアクセスして、アプリケーションが攻撃対象になっているかどうかを確認できます。例えば、DDoS 攻撃が進行している場合に通知するようにアラームを設定できます。通知があれば、アプリケーションの正常性を調べ、AWS SRT に支援を求めるかどうかを判断できます。`DDoSDetected` メトリクスを設定すると、攻撃が検出された場合に通知を受けることができます。攻撃量に基づいたアラートを受け取るには、メトリクス `DDoSAttackBitsPerSecond`、`DDoSAttackPacketsPerSecond`、または `DDoSAttackRequestsPerSecond` を使用することもできます。これらのメトリクスは、独自に用意したツールに Amazon CloudWatch を統合するか、Slack や PagerDuty などのサードパーティ製ツールを使用して監視できます。

アプリケーションレイヤーに対する攻撃が発生すると、多くの Amazon CloudWatch メトリクスの値が上昇します。AWS WAF を使用している場合は、許可、カウント、ブロックするように

AWS WAF に設定したリクエストの状況を CloudWatch で監視し、値が増えていればアラームとして通知できます。この機能を使用すると、トラフィック量がアプリケーションで処理可能な範囲を越えた場合に、通知を受け取ることができます。また、CloudWatch で記録した、Amazon CloudFront、Amazon Route 53、Application Load Balancer、Network Load Balancer、Amazon EC2、Auto Scaling の各メトリクスに基づき、DDoS 攻撃の兆候であるような変化を検出することも可能です。

DDoS 攻撃を検出して対応するために一般的に使用される CloudWatch メトリクスについては、CloudWatch の推奨メトリクスの表を参照してください。

表 3: Amazon CloudWatch の推奨メトリクス

トピック	メトリクス	説明
AWS Shield Advanced	DDoSDetected	所定の Amazon Resource Name (ARN) に対する DDoS イベントを検出した旨。
AWS Shield Advanced	DDoSAttackBitsPerSecond	特定の ARN に対する DDoS イベントで検出されたバイト数。このメトリクスは、レイヤー 3/4 の DDoS イベントでのみ使用できます。
AWS Shield Advanced	DDoSAttackPacketsPerSecond	特定の ARN に対する DDoS イベントで検出されたパケットの数。このメトリクスは、レイヤー 3/4 の DDoS イベントでのみ使用できます。
AWS Shield Advanced	DDoSAttackRequestsPerSecond	特定の ARN に対する DDoS イベントで検出されたリクエスト数。このメトリクスはレイヤー 7 の DDoS イベントでのみ使用できます。特に重要なレイヤー 7 イベントのみが報告されます。

トピック	メトリクス	説明
AWS WAF	AllowedRequests	許可されたウェブリクエストの数。
AWS WAF	BlockedRequests	ブロックされたウェブリクエストの数。
AWS WAF	CountedRequests	カウントされたウェブリクエストの数。
AWS WAF	PassedRequests	通過したリクエストの数。どのルールグループのルールにも一致せずにルールグループ評価を通過するリクエストにのみ使用されます。
Amazon CloudFront	Requests	HTTP/S リクエストの数。
Amazon CloudFront	TotalErrorRate	HTTP ステータスコードが 4xx または 5xx であるすべてのリクエストの割合。
Amazon Route 53	HealthCheckStatus	ヘルスチェックのエンドポイントのステータス。
Application Load Balancer	ActiveConnectionCount	クライアントからロードバランサーに、およびロードバランサーからターゲットに到る、アクティブな同時 TCP 接続の総数。
Application Load Balancer	ConsumedLCUs	ロードバランサーの LCU (Load balancer Capacity Unit) 使用量。
Application Load Balancer	HTTPCode_ELB_5XX_Count HTTPCode_ELB_4XX_Count	ロードバランサーで生成された HTTP 4xx または 5xx クライアントエラーコードの数。

トピック	メトリクス	説明
Application Load Balancer	NewConnectionCount	クライアントからロードバランサーに、およびロードバランサーからターゲットに到る、新たに確立された TCP 接続の総数。
Application Load Balancer	ProcessedBytes	ロードバランサーが処理した総バイト数。
Application Load Balancer	RejectedConnectionCount	ロードバランサーの最大接続数に達したために拒否された接続の数。
Application Load Balancer	RequestCount	処理したリクエストの数。
Application Load Balancer	TargetConnectionErrorCount	ロードバランサーとターゲットの間で、正常に確立されなかった接続の数。
Application Load Balancer	TargetResponseTime	ロードバランサーがリクエストを送信した後、ターゲットから応答が届くまでの経過時間 (秒)。
Application Load Balancer	UnHealthyHostCount	異常と判断したターゲットの数。
Network Load Balancer	ActiveFlowCount	クライアントからターゲットに到る、同時 TCP フロー (または接続) の総数。
Network Load Balancer	ConsumedLCUs	ロードバランサーの LCU (Load balancer Capacity Unit) 使用量。

トピック	メトリクス	説明
Network Load Balancer	NewFlowCount	所定の期間内にクライアントからターゲットに確立された、新規 TCP フロー (または接続) の総数。
Network Load Balancer	ProcessedBytes	ロードバランサーが処理した合計バイト数 (TCP/IP ヘッダーを含む)。
Global Accelerator	NewFlowCount	期間内にクライアントからエンドポイントに対して確立された新しい TCP および UDP フロー (または接続) の合計数。
Global Accelerator	ProcessedBytesIn	アクセラレータによって処理された着信バイトの総数 (TCP/IP ヘッダーを含む)。
Auto Scaling	GroupMaxSize	Auto Scaling グループの最大サイズ。
Amazon EC2	CPUUtilization	割り当て済み EC2 計算ユニットのうち、現在使用中のものの比率。
Amazon EC2	NetworkIn	インスタンスが受信したバイト数 (すべてのネットワークインターフェースが対象)。

Amazon CloudWatch を使用してアプリケーションに対する DDoS 攻撃を検出する方法について詳しくは、「Amazon CloudWatch の開始方法」を参照してください。

上の表のメトリクスを使用して構築されたダッシュボードの例については、「カスタムベースライン監視システム」を参照してください。

AWS には他にも、攻撃に関する通知や、アプリケーションのリソースの監視に役立つメトリクスおよびアラームがあります。AWS Shield のコンソールまたは API を使用すると、検出された攻撃に関する概要および詳細を確認できます。

さらに、グローバル脅威環境ダッシュボードには、AWS で検出されたすべての DDoS 攻撃の概要が表示されます。この情報は、多数のアプリケーションにおける DDoS の脅威を深く理解して攻撃の傾向を把握し、実際に検出された攻撃と比較するために役立ちます。

AWS Shield Advanced をサブスクライブしている場合、サービスダッシュボードには、保護対象リソースで検出されたイベントに関する追加の検出および緩和メトリクスと、ネットワークトラフィックの詳細が表示されます。AWS Shield は、保護対象リソースへのトラフィックを複数のディメンションで評価します。異常が検出されると、AWS Shield はイベントを作成し、異常が検出されたトラフィックディメンションをレポートします。緩和機能を使用すると、過剰なトラフィックや、既知の DDoS イベントの特徴と一致するトラフィックをリソースが受信しないように保護できます。

ウェブ ACL が保護対象リソースに関連付けられている場合、サンプリングされたネットワークフローまたは AWS WAF ログに基づく検出メトリクスが使用されます。緩和メトリクスは、Shield の DDoS 緩和システムによって監視されるトラフィックに基づいています。緩和メトリクスは、リソースへのトラフィックをより正確に測定したものです。

ネットワークの上位寄与要因メトリクスは、検出されたイベント中にトラフィックがどこから来ているかを示すインサイトを提供します。ボリュームが最も大きな寄与要因を確認し、プロトコル、送信元ポート、TCP フラグなどの要素別に並べ替えることができます。上位寄与要因メトリクスには、さまざまなディメンションに沿ってリソースで検出されたすべてのトラフィックに関するメトリクスが含まれます。これにより、イベント中にリソースに送信されるネットワークトラフィックを把握するために使用できる、追加のメトリクスディメンションが提供されます。

サービスダッシュボードには、DDoS 攻撃を軽減するために自動的に実行されるアクションの詳細も表示されます。この情報により、異常の調査や、トラフィックのディメンションの確認が容易になり、可用性の確保のために実行される Shield Advanced のアクションについて理解しやすくなります。

もう 1 つ、アプリケーションに向かうトラフィックの状況を視覚的に把握できるツールとして、VPC フローログがあります。従来型のネットワークでは、ネットワークフローログを調べて、接続やセキュリティに関する問題に対処したり、ネットワークアクセスのルールが想定通りに機能しているか確認したりしていました。VPC Flow Logs を使えば、VPC のネットワークインターフェイス間でやり取りされる、IP トラフィックに関する情報を取得できます。

フローログの各レコードには、送信元と送信先の IP アドレス、送信元と送信先のポート、プロトコル、キャプチャウィンドウ中に転送されたパケット数およびバイト数が記録されます。この情報を使って、ネットワークトラフィックの異常を検知し、攻撃者がアクセス権限を奪うために用いた経路 (攻撃ベクトル) を調べることができます。たとえば、ほとんどの UDP リフレクション攻撃には、特定の送信元ポートがあります (例: DNS リフレクション攻撃では送信元ポート 53)。これは、攻撃の明らかな特徴であり、フローログレコードで識別できます。対応として、インスタンスレベルで特定の送信元ポートをブロックすることも、アプリケーションが必要としないプロトコル全体をブロックするためのネットワーク ACL ルールを作成できます。

VPC フローログの使用によるネットワークの異常および DDoS 攻撃ベクトルの検出については、「VPC フローログ」および「VPC Flow Logs – Log and View Network Traffic Flows」を参照してください。

複数のアカウントにまたがる可視性と保護の管理

オペレーションに複数の AWS アカウントを使用しており、保護すべきコンポーネントが複数ある場合は、オペレーションの拡張 (スケールアウト) とオーバーヘッドの削減を可能にする手法により、緩和能力を強化できます。AWS Shield Advanced で保護されたリソースを複数のアカウントで管理する場合は、AWS Firewall Manager および AWS Security Hub を使用して一元的なモニタリングをセットアップできます。Firewall Manager を使用すると、すべてのアカウントに DDoS 保護コンプライアンスを適用するセキュリティポリシーを作成できます。これら 2 つのサービスを組み合わせて使用すると、保護対象のリソースを複数のアカウントにわたって管理し、これらのリソースの監視を一元化できます。

Security Hub は Firewall Manager と自動的に統合されるため、Shield Advanced のお客様は、他の優先度の高いセキュリティアラートやコンプライアンスステータスと共に、セキュリティに関する問題点や検出された項目を 1 つのダッシュボードで確認できます。例えば、Shield Advanced がスコープ内で、いずれかの AWS アカウント内にある保護対象のリソースへの異常なトラフィックを検出すると、この情報が Security Hub コンソールに表示されます。Firewall Manager が設定されている場合は、リソースを Shield Advanced で保護されたリソースとして作成し、リソースがポリシーに準拠しているときに Security Hub を更新することで、リソースを自動的に準拠状態に移行できます。

Shield で保護されたリソースの一元的なモニタリングについて詳しくは、「Set up centralized monitoring for DDoS events and auto-remediate noncompliant resources」を参照してください。

サポート

実際に攻撃を受けた場合には、脅威の状況を評価してアプリケーションのアーキテクチャを検討する目的や、それ以外の支援を要求するために、AWS のサポートをご利用いただけます。実際に攻撃が起きる前に DDoS 攻撃に備え対応プランを作成することが重要です。このホワイトペーパーで概説するベストプラクティスは、アプリケーションを起動する前に実装する事前対策ですが、それでもアプリケーションに対する DDoS 攻撃が発生する可能性があります。このセクションでオプションを確認し、お客様のシナリオに最適なサポートリソースを決定しましょう。アカウントチームは、ユースケースおよびアプリケーションを評価し、特定の疑問点や現在の問題点に関するサポートを提供します。

AWS で本番ワークロードを実行している場合は、DDoS 攻撃への対処をサポートするクラウドサポートエンジニアに 24 時間 365 日アクセスできる、ビジネスサポートへの登録をご検討ください。ミッションクリティカルなワークロードを実行している場合は、重大な問題点が発生しても、それを報告することにより、最速でシニアクラウドエンジニアからの対応を得ることができるエンタープライズサポートをお勧めします。

AWS Shield Advanced をサブスクライブしていて、ビジネスサポートまたはビジネスサポートのいずれかに登録している場合には、Shield によるプロアクティブエンゲージメントを設定できます。これにより、ヘルスチェックの設定や、リソースへの関連付けができ、24 時間 365 日の連絡先情報が提供されます。Shield が DDoS の兆候を検出し、アプリケーションのヘルスチェックで状況悪化の兆候が見られる場合、AWS SRT は先を見越してお客様に連絡します。これは、お勧めのエンゲージメントモデルであり、AWS SRT から最速で応答を得ることができるだけでなく、お客様からの連絡がつながる前であっても AWS SRT がトラブルシューティングを開始できます。

プロアクティブエンゲージメント機能を使用するには、Route 53 ヘルスチェックを設定する必要があります。ヘルスチェックは、Shield Advanced によって保護されているリソースに関連付けられ、アプリケーションの正常性を正確に測定します。Shield コンソールで Route 53 ヘルスチェックの関連付けが行われると、Shield Advanced 検出システムはヘルスチェックのステータスをアプリケーションの正常性の指標として使用します。Shield Advanced による正常性ベースの検出機能により、アプリケーションに異常が発生した場合に、ユーザーに通知が届き、より迅速に緩和策が実施されるようになります。AWS SRT は、正常性に問題のあるアプリケーションが DDoS 攻撃の標的になっていないか、トラブルシューティングを行い、必要に応じて追加の緩和策を実施するために、お客様に連絡します。

プロアクティブエンゲージメントの設定を完了するには、Shield コンソールに連絡先情報を追加する必要があります。AWS SRT はお客様に連絡する際に、この情報を使用します。連絡先に関してご希望や注意事項がある場合は、最大 10 件の連絡先を設定し、追加のメモを登録できます。プロアク

ティブエンゲージメントの担当者には、セキュリティオペレーションセンターやすぐに連絡がとれる個人など、24 時間 365 日の対応が求められます。

プロアクティブエンゲージメントは、すべてのリソースを対象にすることも、応答時間が重要となる一部の重要な本番リソースを対象にして有効にすることもできます。これには、対象にリソースのみにヘルスチェックを割り当てます。

アプリケーションの可用性に影響するような DDoS 関連のイベントが発生した場合は、AWS Support コンソールまたは Support API を使用して AWS Support ケースを作成し、AWS SRT にエスカレーションすることもできます。

まとめ

このホワイトペーパーで概説しているベストプラクティスは、インフラストラクチャやアプリケーションレイヤーに対する一般的な多数の DDoS 攻撃を防ぐことで、アプリケーションの可用性を保護する DDoS 耐性アーキテクチャの構築に役立ちます。アプリケーションを構築する際、これらのベストプラクティスにどの程度従うかが、緩和できる DDoS 攻撃のタイプ、ベクトル、ボリュームに影響します。DDoS 緩和サービスをサブスクライブしなくても、耐障害性を組み込むことができます。AWS Shield Advanced をサブスクライブすると、さらにサポート、可視性、緩和、およびコスト保護の機能が加わり、既に耐障害性のあるアプリケーションアーキテクチャの保護を強化できます。

寄稿者

本書の作成における寄稿者

- AWS ペリメータ保護、Jeffrey Lyon
- AWS セキュリティスペシャリスト TAM、Rodrigo Ferroni
- AWS ソリューションアーキテクト、Dmitriy Novikov
- AWS ソリューションアーキテクト、Achraf Souk
- AWS ソリューションアーキテクト、Yoshihisa Nakatani

リソース

詳細情報:

- Best Practices for DDoS Mitigation on AWS
- AWS WAF 実装のガイドライン
- SID324 – re:Invent 2017: Automating DDoS Response in the Cloud
- CTD304 – re:Invent 2017: Dow Jones & Wall Street Journal's Journey to Manage Traffic Spikes While Mitigating DDoS & Application Layer Threats
- CTD310 – re:Invent 2017: Living on the Edge, It's Safer Than You Think! Building Strong with Amazon CloudFront, AWS Shield, and AWS WAF
- SEC407 - re:Invent 2019: A defense-in-depth approach to building web applications
- SEC321 - re:Invent 2020: Get ahead of the curve with DDoS Response Team escalations
- William Hill: High-performance DDOS Protection with AWS

ドキュメントの改訂

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードをサブスクライブしてください。

update-history-change	update-history-description	update-history-date
ホワイトペーパーの更新	最新の推奨事項と機能を追加しました。エッジでの包括的な保護の一環として AWS Global Accelerator を追加しました。AWS Firewall Manager について、DDoS イベントの一元的な監視と、コンプライアンスを満たしていないリソースの自動修正に関する記述を追加しました。	2021 年 9 月 21 日
ホワイトペーパーの更新	「悪意のあるウェブリクエストの検出とフィルタリング (BP1、BP2)」セクションのキャッシュバスティングと、「スケールしてトラフィックを吸収 (BP6)」セクションの ELB と ALB の用途を明確にしました。図と表 2 を更新し、「リージョンの選択」を BP8 としました。BP7 セクションに詳細情報を追加しました。	2019 年 12 月 18 日
ホワイトペーパーの更新	AWS WAF の口グ記録をベストプラクティスとして追加しました。	2018 年 12 月 1 日
ホワイトペーパーの更新	AWS Shield、AWS WAF 機能、AWS Firewall Manager、	2018 年 6 月 1 日

	および関連のベストプラクティスを追加しました。	
ホワイトペーパーの更新	規範的アーキテクチャガイダンスを追加し、AWS WAF を含めました。	2016 年 6 月 1 日
初版公開	ホワイトペーパーを公開しました。	2015 年 6 月 1 日

注意

お客様は、本書の情報について独自の評価を行う責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。