AWS ホワイトペーパー

AWS DDoSレジリエンシーのベストプラクティス

AWS DDoSレジリエンシーのベストプラクティス: AWS ホワイトペーパー

Table of Contents

AWS DDoSレジリエンシーのベストプラクティス

公開日: 2023 年 8 月 9 日 (ドキュメントの改訂)

Distributed Denial of Service (DDoS) 攻撃やその他のサイバー攻撃の影響からビジネスを保護することが重要です。アプリケーションの可用性と応答性を維持することで、お客様のサービスを信頼し続けることが最優先事項です。また、インフラストラクチャが攻撃に応じてスケールインする必要がある場合に、不要な直接コスト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不正行為者から保護するためのツール、ベストプラクティス、およびサービスを提供することに全力を注いでいます。から適切なサービスを使用すると、高可用性、セキュリティ、耐障害性を確保 AWS できます。

このホワイトペーパーでは、 AWS で実行されてい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 に提供します AWS。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して使用できる DDoSレジリエントな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、さまざまな攻撃タイプについても説明します。 AWS では、各攻撃タイプを管理するのに最も効果的なベストプラクティスについて説明します。さらに、DDoS緩和戦略に適合するサービスと機能の概要と、各サービスを使用してアプリケーションを保護する方法についても説明します。

このホワイトペーパーは、ネットワーク、セキュリティ、および の基本概念に精通している IT 意思決定者とセキュリティエンジニアを対象としています AWS。各セクションには、 AWS ベストプラクティスまたは機能の詳細を示すドキュメントへのリンクがあります。

AWS は、年間 100 万件を超えるDDoS攻撃を検出し、お客様に対して毎日数千件の攻撃を軽減します。Shield Response チーム (SRT) によると、DDoS攻撃によるビジネスへの影響を経験するほとんどのお客様は、このガイドの推奨事項を実装していません。

Well-Architected の実現状況の確認

AWS Well-Architected フレームワークは、クラウド内でのシステム構築に伴う意思決定の長所と短所を理解するのに役立ちます。このフレームワークの 6 つの柱により、信頼性、安全性、効率、費用対効果、持続可能性の高いシステムを設計および運用するための、アーキテクチャのベストプラクティスを確認できます。で無料で利用できる を使用して AWS Management Console (サインインが必要) AWS Well-Architected Tool、各柱の一連の質問に答えることで、これらのベストプラクティスに照らしてワークロードを確認できます。

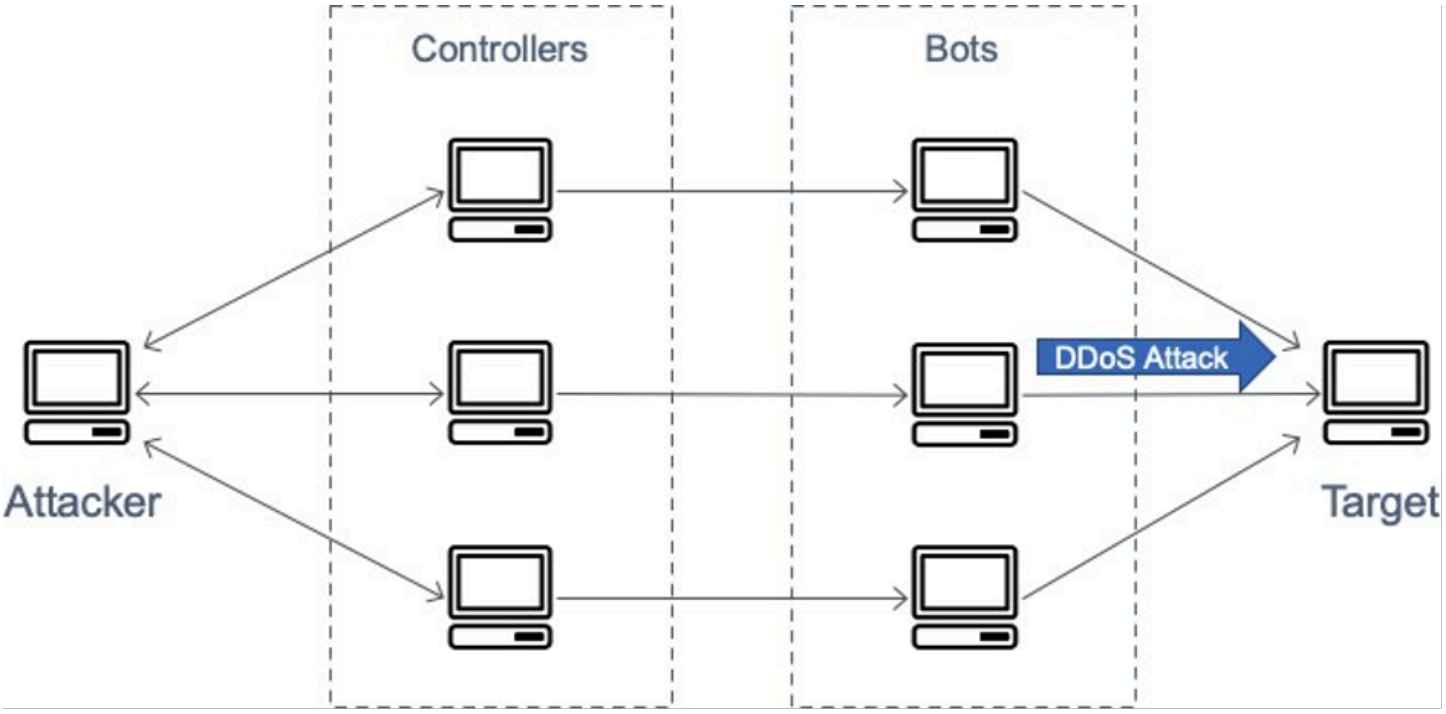
アーキテクチャのデプロイ、図、ホワイトペーパーを参照するなど、クラウドアーキテクチャに関する専門家によるガイダンスとベストプラクティスについては、AWS「アーキテクチャセンター」を参照してください。

サービス拒否攻撃の概要

サービス拒否 (DoS) 攻撃またはイベントは、ネットワークトラフィックでフラッディングするなど、ユーザーがウェブサイトまたはアプリケーションを使用できないようにする意図的な試みです。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結び付けたりして、正当なユーザーのアクセスを中断させるさまざまな手法を使用します。最も単純な形式では、次の図に示すように、唯一の攻撃者は単一のソースを使用してターゲットに対して DoS 攻撃を実行します。

DoS 攻撃を示す図

Distributed Denial of Service (DDoS) 攻撃では、攻撃者は複数のソースを使用してターゲットに対する攻撃を調整します。これらのソースには、マルウェアに感染したコンピュータ、ルーター、IoT デバイス、その他のエンドポイントの分散グループが含まれます。次の図は、攻撃に関与している侵害されたホストのネットワークを示しており、ターゲットを圧倒するパケットやリクエストのフラッドを生成します。



DDoS攻撃を示す図

Open Systems Interconnection (OSI) モデルには 7 つのレイヤーがあり、次の表で説明します。DDoS 攻撃は、レイヤー 3、4、6、および 7 で最も一般的です。

- レイヤー 3 および 4 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に対応します。このホワイトペーパーでは、 AWS 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びます。
- レイヤー 6 および 7 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に対応します。このホワイトペーパーでは、これらをアプリケーションレイヤー攻撃としてまとめて取り上げています。

このホワイトペーパーでは、以下のセクションでこれらの攻撃タイプについて説明します。

表 1 — OSIモデル

#	Layer	単位	説明	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	表現	[データ]	データ表現と暗号化	Transport Layer Security (TLS) の悪用
5	セッション	[データ]	ホスト間通信	該当なし
4	トランスポート	セグメント	E nd-to-end 接続と信頼性	（SYN) フラッドを同期する
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	ユーザーデータグラムプロトコル (UDP) リフレクション攻撃
2	データリンク	[フレーム]	物理的なアドレス指定	該当なし

#	Layer	単位	説明	ベクトルの例
1	物理	Bits	メディア、シグナル、バイナリ送信	該当なし

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とSYN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、これらの方法のいずれかを使用して、ネットワークの容量を浪費したり、サーバー、ファイアウォール、侵入防止システム (IPS) 、ロードバランサーなどのシステム上のリソースを結び付けたりする可能性のある大量のトラフィックを生成できます。これらの攻撃は簡単に特定できますが、効果的に軽減するには、インバウンドトラフィックのフラッドよりも迅速に容量をスケールアップするネットワークまたはシステムが必要です。この追加容量は、攻撃トラフィックを除外または吸収して、システムとアプリケーションを解放し、正当な顧客トラフィックに応答するために必要です。

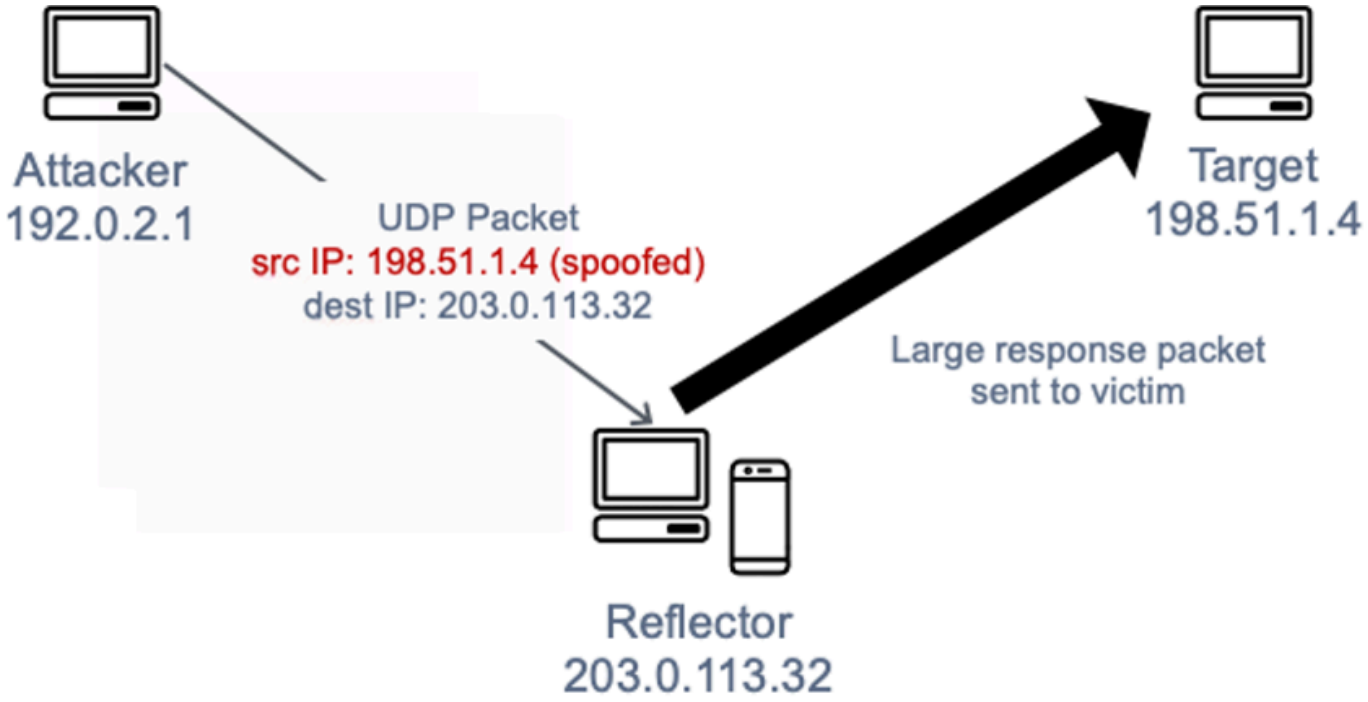
UDP リフレクション攻撃

UDP リフレクション攻撃UDPは、 がステートレスプロトコルであるという事実を悪用します。攻撃者は、攻撃ターゲットの IP アドレスをUDPソース IP アドレスとしてリストした有効なUDPリクエストパケットを作成できます。攻撃者は、UDPリクエストパケットの送信元 IP を改ざんし、なりすましました。UDP パケットにはなりすましソース IP が含まれており、攻撃者によって中間サーバーに送信されます。サーバーは、攻撃者の IP アドレスに戻すのではなく、ターゲットの被害者 IP にUDPレスポンスパケットを送信するようにだまされます。中間サーバーは、リクエストパケットよりも数倍大きいレスポンスを生成し、ターゲット IP アドレスに送信される攻撃トラフィックの量を効果的に増幅するため使用されます。

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によって異なります。、ネットワークタイムプロトコル (NTP) 、Simple Service Directory Protocol ()DNS、Connectionless Lightweight Directory Access Protocol (SSDP) 、Memcached 、Character Generator Protocol (CLDAP) 、または Quote of the Day (CharGen) QOTD。

例えば、 の増幅係数は、元のバイト数の 28～54 倍にDNSすることができます。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、攻撃者は攻撃ターゲットに 3400 バイトを超える不要なトラフィックを生成できます。UDP リフレクション攻撃は、他の攻撃と

比較して、大量のトラフィックに対して責任を負います。次の図は、リフレクションの戦術と増幅効果を示しています。

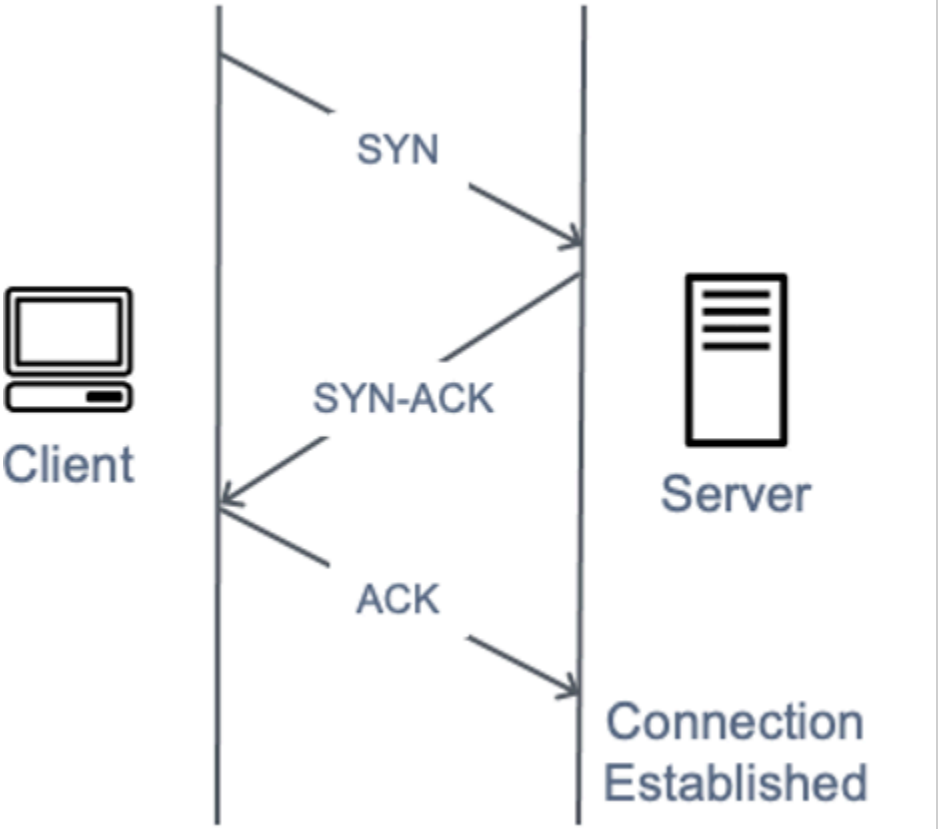


UDPリフレクション攻撃を示す図

リフレクション攻撃は、攻撃者に「無料の」増幅を提供する一方で、IP スプーフィング機能が必要であり、ネットワークプロバイダーの数が増えるにつれてソースアドレス検証 Everywhere (SAVE) または を採用するためBCP38、この機能は削除され、DDoSサービスプロバイダーはリフレクション攻撃を停止するか、ソースアドレス検証を実装していないデータセンターやネットワークプロバイダーに再配置する必要があることに注意してください。

SYN フラッド攻撃

ユーザーがウェブサーバーなどの Transmission Control Protocol (TCP) サービスに接続すると、クライアントはSYNパケットを送信します。サーバーは同期確認 (SYN-ACK) パケットを返し、最後にクライアントは確認 (ACK) パケットで応答し、予想される 3 方向ハンドシェイクを完了します。次の画像は、この一般的なハンドシェイクを示しています。



SYN三方向ハンドシェイクを示す図

SYN フラッド攻撃では、悪意のあるクライアントは多数のSYNパケットを送信しますが、ハンドシェイクを完了するために最終ACKパケットを送信することはありません。サーバーは半オープンTCP接続への応答を待っているままであり、ターゲットは最終的に容量を使い果たして新しいTCP接続を受け入れることができないため、新しいユーザーがサーバーに接続できないという考え方ですが、実際の影響はより微妙です。最新のオペレーティングシステムはすべて、SYN洪水攻撃によるステートテーブルの枯渇に対抗するメカニズムとして、デフォルトで SYNCookie を実装しています。SYN キューの長さが事前に決められたしきい値に達するとACK、サーバーはSYNキューにエントリを作成しなくても、細工された初期シーケンス番号SYNを含む で応答します。サーバーは、正しく増分された確認番号ACKを含む を受信すると、その状態テーブルにエントリを追加し、通常どおり続行できます。ターゲットデバイスに対するSYNフラッドの実際の影響は、ネットワーク容量とCPU枯渇である傾向がありますが、ファイアウォール (またはEC2セキュリティグループ接続追跡) などの中間ステートフルデバイスは、TCPステートテーブルの枯渇に悩まされ、新しい接続が切断される可能性があります。

TCP ミドルボックスリフレクション

この比較的新しい攻撃ベクトルは、2021 年 8 月に学術ホワイトペーパーで初めて公開されました。このホワイトペーパーでは、国家レベルのファイアウォールと市販のファイアウォールの両方がTCPコンプライアンス違反すると、これらのファイアウォールがTCP増幅ベクトルになる可能性があると説明されています。これらの攻撃は、2022 年初頭から「ワイルド」で発生しており、今日も引き続き発生しています。増幅係数は、ベンダーがこの「機能」を実装したさまざまな方法によって異なりますが、Memcached UDP増幅を超える可能性があります。

アプリケーションレイヤー攻撃

攻撃者は、レイヤー 7 またはアプリケーションレイヤー攻撃を使用してアプリケーション自体をターゲットにする可能性があります。これらの攻撃では、フラSYNッドインフラストラクチャ攻撃と同様に、攻撃者はアプリケーションの特定の機能をオーバーロードして、アプリケーションを正当なユーザーに利用できなくなったり、応答しなくなったりしようとします。これは、少量のネットワークトラフィックのみを生成する非常に低いリクエストボリュームで達成できる場合があります。これにより、攻撃の検出と軽減が困難になる可能性があります。アプリケーションレイヤー攻撃の例としては、HTTPフラッド、キャッシュバス攻撃、 WordPress XML-RPC フラッドなどがあります。

- HTTP 洪水攻撃では、攻撃者はウェブアプリケーションの有効なユーザーから送信されたと思われるHTTPリクエストを送信します。一部のHTTPフラッドは特定のリソースをターゲットとしていますが、より複雑なフラHTTPッドはアプリケーションとの人間のやり取りをエミュレートしようとします。これにより、リクエストレート制限などの一般的な緩和手法を使用する際の難しさが増す可能性があります。
- キャッシュバスティング攻撃は、クエリ文字列のバリエーションを使用してコンテンツ配信ネットワーク (CDN) キャッシュを回避するHTTPフラッドの一種です。キャッシュされた結果を返す代わりに、 はページリクエストごとにオリジンサーバーに連絡CDNする必要があり、これらのオリジンフェッチはアプリケーションウェブサーバーにさらなる負荷を与えます。
- pingback WordPress XMLフラッドとも呼ばれる -RPC フラッド攻撃では、攻撃者は 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をターゲットにします。WordPress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 機能を使用すると、 WordPress （ サイト A) でホストされているウェブサイトは、サイト A が WordPress サイト B に作成したリンクを介して別のサイト (サイト B) に通知できます。その後、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、攻撃者`WordPress:`はこの機能を悪用してサイト B にサイト A を攻撃させます。この種の攻撃には、通常、HTTPリクエストヘッダーの User-Agent に「」という明確な署名があります。

アプリケーションの可用性に影響を与える可能性のある悪意のあるトラフィックには、他にも種類があります。スクレイパーボットは、ウェブアプリケーションにアクセスしてコンテンツを盗んだり、価格などの競合情報を記録したりしようとする試みを自動化します。ブルートフォース攻撃と認証情報スタッフィング攻撃は、アプリケーションの安全な領域への不正アクセスをプログラムで試みます。これらは厳密にDDoS攻撃ではありませんが、その自動化された性質はDDoS攻撃に似ているように見え、このホワイトペーパーで説明しているのと同じベストプラクティスの一部を実装することで軽減できます。

アプリケーションレイヤー攻撃は、ドメインネームシステム (DNS) サービスをターゲットにすることもできます。これらの攻撃の最も一般的なのは、攻撃者が多くの適切な形式のクエリを使用してDNSサーバーのリソースを使い果たすDNSクエリフラDNSッドです。これらの攻撃には、攻撃者がサブドメイン文字列をランダム化して特定のリゾルバーのローカルDNSキャッシュをバイパスするキャッシュバスティングコンポーネントも含まれます。その結果、リゾルバーはキャッシュされたドメインクエリを利用できず、代わりに攻撃を増幅する権威DNSサーバーに繰り返し連絡する必要があります。

ウェブアプリケーションが Transport Layer Security (TLS) TLS 経由で配信された場合、攻撃者はネゴシエーションプロセスを攻撃することもできます。TLS は計算コストが高いため、攻撃者はサーバー上に追加のワークロードを生成して、読み取り不可能なデータ (または理解できない (暗号文)) を正当なハンドシェイクとして処理することで、サーバーの可用性を低下させることができます。この攻撃のバリエーションでは、攻撃者はTLSハンドシェイクを完了しますが、暗号化方法を永続的に再ネゴシエートします。攻撃者は、多数のTLSセッションを開いたり閉じたりして、サーバーリソースを使い果たそうとすることもできます。

緩和手法

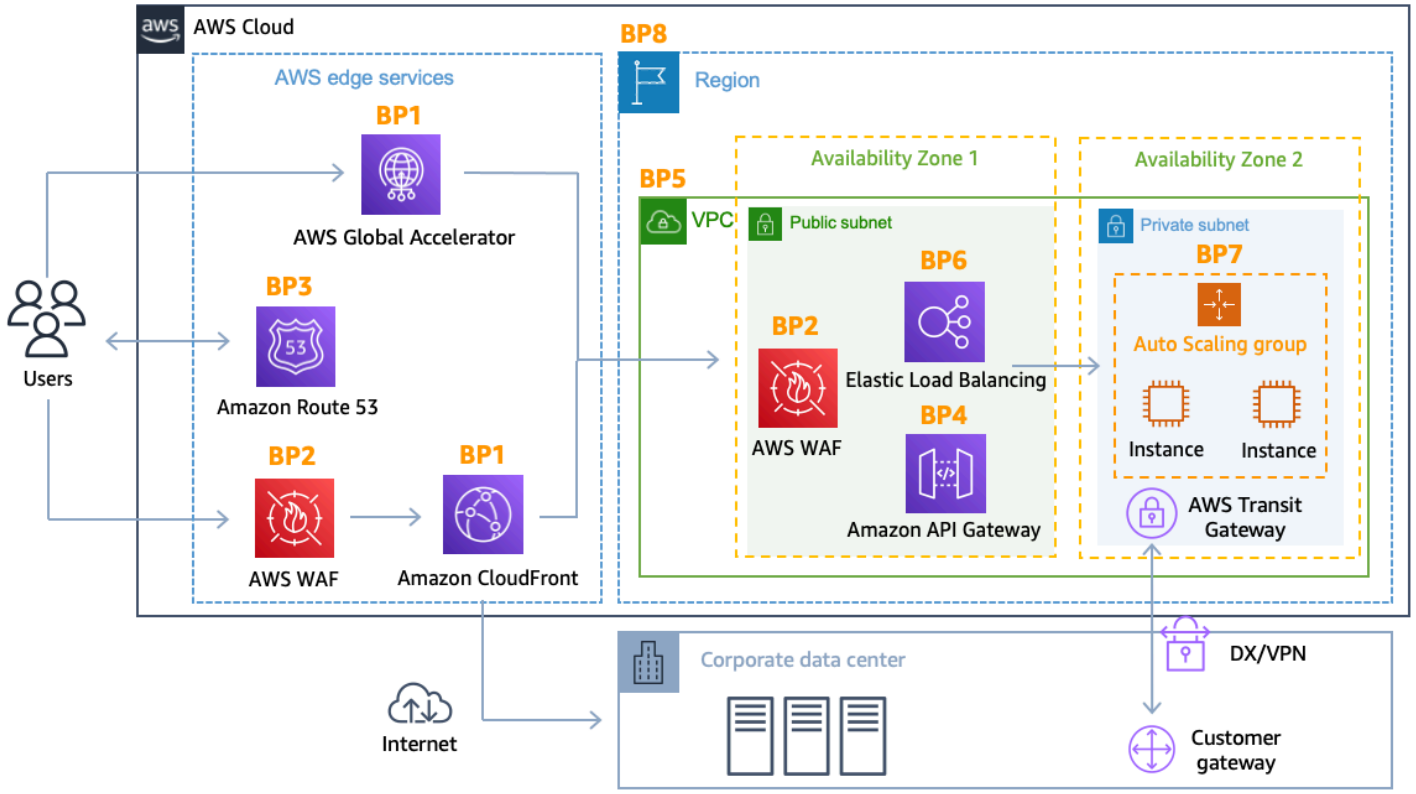
一部のDDoS緩和策は、 サービスに自動的に含まれます AWS 。DDoS レジリエンスは、以下のセクションで説明する特定の サービスで アーキテクチャを使用すること AWS 、およびユーザーとアプリケーション間のネットワークフローの各部分に追加のベストプラクティスを実装することで、さらに向上できます。

Amazon 、 CloudFront AWS Global Accelerator、Amazon Route 53 などのエッジロケーションから運用される AWS サービスを使用して、すべての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を構築できます。これらのサービスは AWS グローバルエッジネットワーク の一部であり、世界中に分散されているエッジロケーションからあらゆるタイプのアプリケーショントラフィックを処理する際のアプリケーションのDDoS耐障害性を向上させることができます。任意のでアプリケーションを実行し AWS リージョン、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、正当な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 を使用する利点は次のとおりです。

- グローバルエッジネットワーク全体のインターネットへのアクセスと容量のDDoS AWS 緩和。これは、テラビット規模に達する可能性のある大規模なボリューメトリック攻撃の軽減に役立ちます。
- AWS Shield DDoS 緩和システムは AWS エッジサービスと統合され、数分 time-to-mitigate から 1 秒未満に短縮されます。
- ステートレスSYNフラッド緩和は、保護されたサービスに渡す前に、SYNCookie を使用して受信接続を検証します。これにより、正当なエンドユーザーを誤検出ドロップから保護しながら、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ます。
- 大規模なボリューメトリックDDoS攻撃の影響を分散または分離する自動トラフィックエンジニアリングシステム。これらのサービスはすべて、オリジンに到達する前にソースで攻撃を分離します。つまり、これらのサービスで保護されるシステムへの影響は少なくなります。
- 現在のアプリケーションアーキテクチャを変更するAWS WAF必要がない (例えば、 AWS リージョン やオンプレミスのデータセンターなど) と組み合わせ CloudFront た場合のアプリケーションレイヤーの防御。

でのインバウンドデータ転送には料金はかかりません。 AWS また、 によって緩和されるDDoS攻撃トラフィックに対しては料金はかかりません AWS Shield。次のアーキテクチャ図には、 AWS グローバルエッジネットワークサービスが含まれています。



DDoS- 回復力のあるリファレンスアーキテクチャ

このアーキテクチャには、DDoS攻撃に対するウェブアプリケーションの耐障害性を向上させるのに役立ついくつかの AWS サービスが含まれています。次の表は、これらのサービスとそれらが提供できる機能の概要を示しています。 AWS は、このドキュメント内で簡単に参照できるように、各サービスにベストプラクティスインジケータ (BP1、BP2) をタグ付けしています。例えば、次のセクションでは、ベストプラクティスインジケータ を含む Amazon CloudFront と Global Accelerator が提供する機能について説明しますBP1。

表 2 - ベストプラクティスの概要

	AWS Edge			AWS リージョン		
	CloudFront（BP1）での Amazon AWS WAF（BP2）の使用	Global Accelerator の使用 (BP1)	Amazon Route 53 の使用 (BP3)	（BP6）での Elastic Load Balancing AWS WAF	Amazon ACLsでのセキュリティグループとネットワークの	Amazon Elastic Compute Cloud (Amazon EC2) Auto

	AWS Edge			AWS リージョン		
				(BP2) の使用	使用 VPC (BP5)	Scaling の使用 (BP7)
レイヤー 3 (UDPリフレクションなど) 攻撃の軽減	✓	✓	✓	✓	✓	✓
レイヤー 4 (フラSYNッドなど) 攻撃の軽減	✓	✓	✓	✓		
レイヤー 6 (などTLS) 攻撃の軽減	✓	✓	✓	✓		
アタックサーフェスを減らす	✓	✓	✓	✓	✓	
アプリケーションレイヤートラフィックを吸収するためのスケーリング	✓	✓	✓	✓	✓	✓

	AWS Edge			AWS リージョン		
レイヤー 7 (アプリケーションレイヤー) 攻撃の軽減	✓	✓(*)	✓	✓	✓(*)	✓(*)
過剰なトラフィックや大規模なDDoS攻撃の地理的分離と利用	✓	✓	✓			

✓(*): Application Load Balancer AWS WAF で と共に使用する場合

DDoS 攻撃に対応し、軽減する準備状況を向上させるもう 1 つの方法は、 にサブスクライブすることです AWS Shield Advanced。を使用する利点 AWS Shield Advanced は次のとおりです。

- オプションのプロアクティブエンゲージメント機能など、アプリケーションの可用性に影響を与えるDDoS攻撃の軽減を支援するために、AWS Shield レスポンスチーム (AWS SRT) からの 24 時間 365 日の専門サポートへのアクセス
- Elastic IP アドレスと併用すると、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、Amazon EC2 (Elastic Load Balancer を含む) または Network Load Balancer に対する time-to-mitigate 攻撃を改善できる機密性の高い検出しきい値
- で使用する場合のアプリケーションのベースライントラフィックパターンに基づく、カスタマイズされたレイヤー 7 検出 AWS WAF
- Shield Advanced がカスタム AWS WAF ルールを作成、評価、デプロイして検出されたDDoS攻撃に対応するアプリケーションレイヤーの自動DDoS緩和
- アプリケーションレイヤーDDoS攻撃の軽減のために追加料金 AWS WAF なしで にアクセスする (Amazon CloudFront または Application Load Balancer で使用する場合)
- 追加コストなしで、 を通じてセキュリティポリシーAWS Firewall Managerを一元管理できます。
- DDoS 攻撃によるスケーリング関連のコストの限定的な返金をリクエストできるコスト保護。
- AWS Shield Advanced お客様固有のサービスレベルアグリーメントの強化。

- リソースをバンドルできる保護グループ。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。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。
- DDoS 、AWS Management Console、および Amazon CloudWatch メトリクスとアラーム を使用してAPI、 が可視性を攻撃します。

このオプションDDoSの緩和サービスは、任意の でホストされているアプリケーションを保護するのに役立ちます AWS リージョン。このサービスは、、Route 53 CloudFront、および Global Accelerator でグローバルに利用できます。リージョンごとに、Application Load Balancer 、Classic Load Balancer、および Elastic IP アドレスを保護できます。これにより、Network Load Balancer () または Amazon インスタンスを保護できます。NLBs EC2

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

DDoS 緩和のベストプラクティス

以下のセクションでは、DDoS緩和のために推奨される各ベストプラクティスについて詳しく説明します。静的または動的ウェブアプリケーションのDDoS緩和レイヤーの構築に関する簡単な easy-to-implement ガイドについては、「Amazon と Amazon Route 53 を使用してDDoS攻撃から動的ウェブアプリケーションを保護する方法」を参照してください。 CloudFront

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、容量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、緩和サービスの活用によるトラフィックのスクラブなどの手法を使用して、インフラストラクチャレイヤーDDoS攻撃DDoSを軽減できます。では AWS、DDoS緩和機能が自動的に提供されますが、これらの機能を最大限に活用し、過剰なトラフィックに合わせてスケーリングできるアーキテクチャを選択することで、アプリケーションのDDoS耐障害性を最適化できます。

ボリューメトリックDDoS攻撃を軽減するための主な考慮事項には、十分なトランジットキャパシティと多様性を確保し、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ことが含まれます。

一部の Amazon EC2インスタンスタイプは、最大 100 Gbps のネットワーク帯域幅インターフェイスや拡張ネットワーキングなど、大量のトラフィックをより簡単に処理できる機能をサポートしています。これにより、Amazon EC2インスタンスに到達したトラフィックのインターフェイスの輻輳

を防ぐことができます。拡張ネットワーキングをサポートするインスタンスは、従来の実装と比較して、高い入出力 (I/O) パフォーマンス、高い帯域幅、低いCPU使用率を提供します。これにより、大量のトラフィックを処理するインスタンスの能力が向上し、最終的には 1 秒あたりのパケット数 (pps) の負荷に対する回復力が高まります。

この高レベルの耐障害性を実現するには、Amazon EC2 Dedicated Instances を使用する AWS か、N「」サフィックスを持つネットワークスループットが高い Amazon EC2インスタンスを使用し、最大 100 Gbps のネットワーク帯域幅で拡張ネットワーキングをサポートすることをお勧めします。例えば、 `c6gn.16xlarge` や `c5n.18xlarge` メタルインスタンス (など`c5n.metal`) 。

100 ギガビットのネットワークインターフェイスと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 に含まれていますAMI。したがって、サポートされているインスタンスタイプで Amazon Linux のハードウェア仮想マシン (HVM) バージョンを使用してインスタンスを起動すると、インスタンスの拡張ネットワーキングは既に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になっているかどうかのテスト」および「Linux での拡張ネットワーキング」を参照してください。

Amazon EC2と Auto Scaling (BP7)

インフラストラクチャとアプリケーションレイヤーの両方の攻撃を軽減するもう 1 つの方法は、大規模に運用することです。ウェブアプリケーションがある場合は、ロードバランサーを使用して、オーバープロビジョニングまたは自動スケーリングが設定された多数の Amazon EC2インスタンスにトラフィックを分散できます。これらのインスタンスは、フラッシュ群やアプリケーションレイヤーDDoS攻撃など、何らかの理由で発生した突然のトラフィックの急増を処理できます。、、ネットワーク I/O、さらにはカスタムメトリクスなどCPU、定義したイベントに応じて Amazon EC2フリートのサイズを自動的にスケーリング Auto Scaling するように RAMAmazon CloudWatch アラームを設定できます。

このアプローチは、リクエスト量が予期せず増加した場合にアプリケーションの可用性を保護します。アプリケーションで Amazon CloudFront、Application Load BalancerClassic Load Balancer、または Network Load Balancer TLS を使用する場合、ネゴシエーションは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、正当なリクエストやTLS不正使用攻撃を処理するようにスケーリングすることで、 TLSベースの攻撃の影響を受けるインスタンスを保護するのに役立ちます。

Amazon を使用して Auto Scaling CloudWatch を呼び出す方法の詳細については、「Auto Scaling グループとインスタンスの Amazon CloudWatch メトリクスのモニタリング Auto Scaling」を参照してください。 Auto Scaling

Amazon EC2では、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できるように、サイズ変更可能なコンピューティング容量を提供しています。Amazon EC2 Auto Scaling グループのサイズをスケーリングすることで、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でき、より大きなEC2インスタンスタイプを使用して垂直方向にスケーリングできます。

Amazon RDS Proxy を使用すると、アプリケーションがデータベース接続をプールして共有し、データベーストラフィックの予期しない急増をスケーリングおよび処理する能力を向上させることができます。また、Amazon RDS データベースインスタンスのストレージの自動スケーリングを有効にすることもできます。詳細については、「Amazon RDSストレージの自動スケーリングによる容量の自動管理」を参照してください。

Elastic Load Balancing (BP6)

大規模なDDoS攻撃は、単一の Amazon EC2インスタンスの容量を圧倒する可能性があります。Elastic Load Balancing (ELB) を使用すると、多く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で、アプリケーションの過負荷のリスクを減らすことができます。Elastic Load Balancing は自動的にスケーリングできるため、フラッシュの群集やDDoS攻撃など、予期しない余分なトラフィックがある場合に、より大きなボリュームを管理できます。Amazon 内に構築されたアプリケーションの場合VPC、アプリケーションタイプに応じて、Application Load Balancer (ALB) 、Network Load Balancer ()、Classic Load Balancer (NLB) の 3 つのタイプELBsを考慮する必要がありますCLB。 Load Balancer

ウェブアプリケーションの場合、Application Load Balancer を使用してコンテンツに基づいてトラフィックをルーティングし、適切な形式のウェブリクエストのみを受け入れることができます。Application Load Balancer は、SYNフラッドDDoS攻撃やUDPリフレクション攻撃など、多くの一般的な攻撃をブロックし、攻撃からアプリケーションを保護します。Application Load Balancer は、これらのタイプの攻撃が検出されると、追加のトラフィックを吸収するように自動的にスケーリングします。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アクティビティは、お客様にとって AWS 透過的であり、請求には影響しません。

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。

HTTP/HTTPS 以外のアプリケーションでは、Network Load Balancer を使用して、超低レイテンシーでトラフィックをターゲット (Amazon EC2インスタンスなど) にルーティングできます。Network Load Balancer の重要な考慮事項の 1 つは、有効なリスナーのロードバランサーに到達する TCPSYNまたは UDPトラフィックは、吸収されずにターゲットにルーティングされることです。ただし、TCP接続を終了する TLSリスナーには適用されません。TCP リスナーを備えた Network Load Balancer では、SYN洪水を防ぐために Global Accelerator をデプロイすることをお勧めします。

Shield Advanced を使用して、Elastic IP アドレスDDoSの保護を設定できます。Elastic IP アドレスがアベイラビリティーゾーンごとに Network Load Balancer に割り当てられると、Shield Advanced は Network Load Balancer 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およびUDP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。 Load Balancer

> **Note**
>
> セキュリティグループの設定によっては、セキュリティを使用して リソースをグループ化し、接続追跡を使用してトラフィックに関する情報を追跡する必要があります。これは、追跡される接続の数が制限されるため、ロードバランサーが新しい接続を処理する能力に影響を与える可能性があります。
> 任意の IP アドレス (`0.0.0.0/0`や など`::/0`) からのトラフィックを受け入れるイングレスルールを含むが、応答トラフィックを許可する対応するルールがないセキュリティグループ設定では、セキュリティグループは接続追跡情報を使用して応答トラフィックの送信を許可します。攻撃が発生した場合DDoS、追跡される接続の最大数を使い果たす可能性があります。パブリック向け Application Load Balancer または Classic Load Balancer のDDoS耐障害性を向上させるには、ロードバランサーに関連付けられたセキュリティグループが接続追跡 (追跡されていない接続) を使用しないように設定されていることを確認し、トラフィックフローが接続追跡制限の対象にならないようにします。
> そのためには、 インバウンドルールが任意の IP アドレス (`0.0.0.0/0` または `::/0`) からのTCPフローを受け入れることを許可するルールでセキュリティグループを設定します。 および は、このリソースがすべてのポート (0～65535`::/0`) の応答トラフィック (任意の IP アドレス`0.0.0.0/0`または のアウトバウンド範囲を許可) を送信できるようにするアウトバウンド方向に対応するルールを追加します。 セキュリティグループルールに基づいてレスポンストラフィックが許可されるようにします。 追跡情報ではなく 。この設定では、 Classic および Application Load Balancer は、ロードバランサーノードへの新しい接続の確立に影響を与える可能性のある、エグゼート接続の追跡制限の対象ではありません。 と では、DDoS攻撃発生時のトラフィックの増加に基づいてスケーリングできます。追跡されていない接続の詳

細については、以下を参照してください。 セキュリティグループ接続の追跡： 追跡されていない接続 。
セキュリティグループ接続の追跡を回避すると、DDoSトラフィックがセキュリティグループで許可されているソースから発信される場合にのみ役立ちます。DDoSセキュリティグループで許可されていないソースからのトラフィックは、接続の追跡には影響しません。このような場合、接続の追跡を避けるためにセキュリティグループを再設定する必要はありません。例えば、セキュリティグループの許可リストが、企業のファイアウォールや信頼できる送信や IPs など、高い信頼度を持つ IP VPN 範囲で構成されている場合などですCDNs。

スケールに AWS エッジロケーションを使用する (BP1、BP3)

高度にスケールされた多様なインターネット接続にアクセスすると、ユーザーへの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、障害を分離しながら、アプリケーションの可用性への影響を最小限に抑える能力が大幅に向上します。 AWS エッジロケーションは、Amazon 、Global Accelerator CloudFront、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するネットワークインフラストラクチャの追加レイヤーを提供します。これらのサービスを使用すると、 から実行されているアプリケーションをエッジで包括的に保護できます AWS リージョン。

エッジでのウェブアプリケーション配信 (BP1)

Amazon CloudFront は、静的コンテンツ、動的コンテンツ、ストリーミングコンテンツ、インタラクティブコンテンツなど、ウェブサイト全体を配信するために使用できるサービスです。キャッシュ可能なコンテンツを提供していなくても、永続的な接続と可変 time-to-live （ TTL) 設定を使用して、オリジンからトラフィックをオフロードできます。これらの CloudFront 機能を使用すると、オリジンに戻るリクエストとTCP接続の数が減り、ウェブアプリケーションをHTTPフラッドから保護できます。

CloudFront は、適切な形式の接続のみを受け入れ、SYNフラッドやUDPリフレクションDDoS攻撃などの多くの一般的な攻撃がオリジンに到達するのを防ぐのに役立ちます。DDoS また、攻撃はソースの近くで地理的に分離されているため、トラフィックが他のロケーションに影響を与えるのを防ぐことができます。これらの機能により、大規模なDDoS攻撃中にユーザーにトラフィックを提供し続ける能力が大幅に向上します。 CloudFront を使用して、インターネット上の AWS または他の場所でオリジンを保護できます。

Amazon Simple Storage Service (Amazon S3) を使用してインターネットで静的コンテンツを提供する場合は、 では、バケット CloudFront を保護するために Amazon を使用する AWS ことをお勧めします。これには以下の利点があります。

- Amazon S3 バケットへのアクセスを制限して、パブリックにアクセスできないようにします。
- ビューワー (ユーザー) が、指定された CloudFront ディストリビューションを介してのみバケット内のコンテンツにアクセスできるようにします。つまり、バケットから直接、または意図しない CloudFront ディストリビューションを介してコンテンツにアクセスできないようにします。

これを実現するには、認証されたリクエスト CloudFront を Amazon S3 に送信するように を設定し、 からの認証されたリクエストへのアクセスのみを許可するように Amazon S3 を設定します CloudFront。 CloudFront は、認証されたリクエストを Amazon S3 オリジンに送信する 2 つの方法として、オリジンアクセスコントロール (OAC) とオリジンアクセスアイデンティティ () を提供しますOAI。以下をサポートするOACため、 を使用することをお勧めします。

- 2022 年 12 月以降に開始されたオプトインリージョンを含む AWS リージョン、すべての のすべての Amazon S3 バケット
- AWS KMS (-KMS) による Amazon S3 SSE サーバー側の暗号化
- Amazon S3 に対する動的なリクエスト (PUT と DELETE)

OAC および の詳細についてはOAI、Amazon S3オリジンへのアクセスの制限」を参照してください。

Amazon によるウェブアプリケーションのパフォーマンスの保護と最適化の詳細については CloudFront、「Amazon の開始方法 CloudFront」を参照してください。

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

Global Accelerator は、ユーザーの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、トラフィックをユーザーに最も近いエッジロケーションに取り込み、単一または複数の で実行されているかどうかにかかわらず、 AWS グローバルネットワークインフラストラクチャ経由で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 AWS リージョン。

Global Accelerator は、ユーザーに最も近い のパフォーマンスに基づいて、最適なエンドポイント AWS リージョン に TCPとUDPトラフィックを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 30 秒以内に次善のエンドポイントへのフェイルオーバーを提供します。Global Accelerator は、新しい接続試行にチャレンジし、正当な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、 AWS グローバルネットワークと Shield との統合の膨大な容量を使用してアプリケーションを保護します。

アプリケーションが でサポートされていないプロトコルを使用しているか、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 CloudFront 運用している場合でも、エッジのベストプラクティスでウェブアプリケーション配信と同じ利点の多くを提供するDDoS回復力のある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、他の AWS 顧客では使用されない IP アドレスが必要になる場合があります。これらのシナリオでは、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、 と組み合わせて、ウェブアプリケーションレイヤーリクエストのフラッドを検出して軽減 AWS WAF 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パフォーマンスの保護と最適化の詳細については、「Global 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解決 (BP3)

トピック

- DNS 可用性のための Route 53 の使用
- NXDOMAIN 攻撃からのコスト保護のための Route 53 の設定

DNS 可用性のための Route 53 の使用

Amazon Route 53 は、トラフィックをウェブアプリケーションに転送するために使用できる、可用性が高くスケーラブルなドメインネームシステム (DNS) サービスです。これには、トラフィックフロー、ヘルスチェックとモニタリング、レイテンシーベースのルーティング、Geo などの高度な機能が含まれていますDNS。これらの高度な機能により、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するために、サービスがDNSリクエストにどのように応答するかを制御できます。これは、データプレーンの可用性が 100% である唯一の AWS サービスですSLA。

Amazon Route 53 は、シャッフルシャーディングやエニーキャストストライピングなどの手法を使用します。これは、DNSサービスがDDoS攻撃のターゲットであっても、ユーザーがアプリケーションにアクセスするのに役立ちます。

シャッフルシャーディングでは、委任セット内の各ネームサーバーは、エッジロケーションと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、顧客間の重複が最小限に抑えられます。委任セット内の 1 つのネームサーバーが使用できない場合、ユーザーは別のエッジロケーションにある別のネームサーバーからレスポンスを再試行して受信できます。

エニーキャストストライピングにより、各DNSリクエストを最適なロケーションで処理できるため、ネットワーク負荷が分散され、DNSレイテンシーが短縮されます。これにより、ユーザー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、信頼性が高いことがわかっているユーザーからのリクエストに優先順位を付けることができます。

Amazon Route 53 を使用してユーザーをアプリケーションにルーティングする方法の詳細については、「Amazon Route 53 の開始方法」を参照してください。

NXDOMAIN 攻撃からのコスト保護のための Route 53 の設定

NXDOMAIN 攻撃は、攻撃者が、多くの場合既知の「良い」リゾルバーを介して、存在しないサブドメインのホストゾーンに大量のリクエストを送信したときに発生します。これらの攻撃の目的は、再帰リゾルバーのキャッシュや信頼できるリゾルバーの可用性に影響を与えることや、ホストゾーンレコードを検出しようとするDNS偵察の一形態である可能性があります。信頼できるリゾルバーに Route 53 を使用すると、可用性/パフォーマンスへの影響のリスクを軽減できますが、その結果、Route 53 の月額コストが大幅に増加する可能性があります。コストの増加を防ぐには、Route 53 の料金を利用して、次の条件の両方に当てはまる場合にDNSクエリが無料になります。

- クエリ内のドメインまたはサブドメイン名 (`example.com` または `store.example.com`) とレコードタイプ (`A`) がエイリアスレコードと一致します。
- エイリアスターゲットは、別の Route 53 レコード以外の AWS リソースです。

例えば、EC2インスタンス、Elastic Load Balancer、 CloudFront ディストリビューションなどの AWS リソースを指すタイプ `A` (エイリアス) `*.example.com`を使用してワイルドカードレコードを作成します。これにより、 のクエリが行われると、リソースの IP `qwerty12345.example.com` が返され、クエリに対して課金されません。

アプリケーションレイヤーの防御 (BP1、BP2)

このホワイトペーパーでこれまでに説明した手法の多くは、インフラストラクチャレイヤー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のに役立ちます。また、アプリケーションレ

イヤー攻撃から保護するには、悪意のあるリクエストを具体的に検出、スケールして吸収、ブロックできるアーキテクチャを実装する必要があります。ネットワークベースのDDoS緩和システムは、複雑なアプリケーションレイヤー攻撃の軽減に一般的に効果がないため、これは重要な考慮事項です。

悪意のあるウェブリクエストを検出してフィルタリングする (BP1、BP2)

アプリケーションで を実行すると AWS、Amazon CloudFront （ およびそのキャッシュ機能) HTTP と Shield Advanced 自動アプリケーションレイヤー保護を活用して AWS WAF、アプリケーションレイヤーDDoS攻撃中に不要なリクエストがオリジンに到達するのを防ぐことができます。

Amazon CloudFront

Amazon CloudFront は、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できます。 CloudFront アプリケーションにリクエストを送信するには、完了したTCPハンドシェイクを通じて有効な IP アドレスで接続を確立する必要があります。これは偽装できません。さらに、 CloudFront は、読み取りが遅い攻撃者や書き込みが遅い攻撃者 (Slowloris など) から自動的に接続を閉じることができます。

CDN キャッシュ

CloudFront では、 AWS エッジロケーションから動的コンテンツと静的コンテンツの両方を提供できます。CDN キャッシュからプロキシキャッシュ可能なコンテンツを提供することで、キャッシュの期間中、特定のエッジキャッシュノードからのリクエストがオリジンに到達するのを防ぐことができますTTL。有効期限が切れているがキャッシュ可能なコンテンツのリクエストが折りたたまれると、非常に短い場合でも、そのコンテンツのリクエストフラッド中にごくわずかな数のリクエストがオリジンに到達するTTLことを意味します。さらに、CloudFront Origin Shield などの機能を有効にすると、オリジンの負荷をさらに軽減できます。キャッシュヒット率を向上させるためにできることは、影響のあるリクエストフラッド攻撃と影響のないリクエストフラッド攻撃の違いを意味します。

AWS WAF

を使用すると AWS WAF、グローバル CloudFront ディストリビューションまたはリージョンリソースでウェブアクセスコントロールリスト (Web ACLs) を設定して、リクエスト署名に基づいてリクエストをフィルタリング、モニタリング、ブロックできます。リクエストを許可またはブロックするかどうかを決定するには、IP アドレスまたは発信国、リクエスト内の特定の文字列またはパターン、リクエストの特定部分のサイズ、悪意のあるSQLコードまたはスクリプティングの存在などの要因を考慮できます。リクエストに対してCAPTCHAパズルやサイレントクライアントセッションチャレンジを実行することもできます。

また CloudFront 、 AWS WAF と の両方で、地理的制限を設定して、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、ユーザーにサービスを提供しないことが予想される地理的場所からの攻撃をブロックまたはレート制限することができます。の詳細な地理的一致ルールステートメントを使用すると AWS WAF、リージョンレベルまでアクセスを制御できます。

スコープダウンステートメントを使用して、ルールが評価するリクエストの範囲を絞り込み、ウェブリクエストのコストを節約し、リクエストに一致するルールが一致結果を同じウェブ で後で評価されるルールに伝達できるようにしますACL。複数のルールで同じロジックを再利用するには、このオプションを選択します。

レスポンスコード、ヘッダー、本文を使用して、完全なカスタムレスポンスを定義することもできます。

悪意のあるリクエストを特定するには、ウェブサーバーログを確認するか、 AWS WAFのログ記録と sampling.By リクエストを使用して AWS WAF ログ記録を有効にすると、ウェブ によって分析されたトラフィックに関する詳細情報が得られますACL。 はログフィルタリング AWS WAF をサポートしているため、検査後にログに記録するウェブリクエストとログから破棄されるリクエストを指定できます。

ログに記録される情報には、 が AWS リソースからリクエストを AWS WAF 受信した時間、リクエストに関する詳細情報、およびリクエストされた各ルールの一致するアクションが含まれます。

サンプルリクエストは、過去 3 時間以内にいずれかの AWS WAF ルールに一致したリクエストに関する詳細を提供します。この情報を使用して、潜在的に悪意のあるトラフィック署名を特定し、それらのリクエストを拒否する新しいルールを作成できます。ランダムなクエリ文字列を持つ多数のリクエストが表示される場合は、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してください。この手法は、オリジンに対するキャッシュの破壊攻撃を軽減するのに役立ちます。

AWS WAF – レートベースのルール

AWS では、5 分間のスライディングウィンドウで受信したHTTPリクエストの数が定義したしきい値を超えた場合に、不正なアクターの IP アドレスを自動的にブロック AWS WAF するために、レートベースのルールを使用してリクエストフラッドから保護することを強くお勧めします。問題のあるクライアント IP アドレスは、403 の禁止レスポンス (または設定されたブロックエラーレスポンス) を受け取り、リクエスト率がしきい値を下回るまでブロックされたままになります。

レートベースのルールをレイヤー化して保護を強化し、以下を行うことをお勧めします。

- 大規模なHTTPフラッドからアプリケーションを保護するための一括レートベースのルール。
- 一括レートベースのルールよりも制限の厳しいレートURIsで特定の を保護する 1 つ以上のレートベースのルール。

例えば、5 分間に 500 リクエストの制限がある一括レートベースのルール (スコープダウンステートメントなし) を選択し、スコープダウンステートメントを使用して、500 (5 分間に 100 リクエストまで) より低い制限の次のレートベースのルールを 1 つ以上作成できます。

- ファイル拡張子のないリソースのリクエストがさらに保護`if NOT uri_path contains '.'`されるように、「」のようなスコープダウンステートメントでウェブページを保護します。これにより、頻繁にターゲットにされるURIパスであるホームページ (/) も保護されます。
- 「」のようなスコープダウンステートメントで動的エンドポイントを保護する`if method exactly matches 'post' (convert lowercase)`
- データベースに到達する、または「」のようなスコープダウンでワンタイムパスワード (OTP) を呼び出す大量のリクエストを保護する`if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

「ブロック」モードのレートベースは、リクエストの defense-in-depth WAFフラッドから保護するための設定の基礎であり、コスト保護リクエストを承認するための要件 AWS Shield Advanced です。以下のセクションでは、追加の defense-in-depth WAF設定について説明します。

AWS WAF – IP の評価

IP アドレスの評価に基づく攻撃を防ぐには、IP マッチングを使用してルールを作成するか、 の マネージドルールを使用します AWS WAF。

Amazon の IP 評価リストルールグループには、Amazon の内部脅威インテリジェンスに基づくルールが含まれます。これらのルールは、ボット、 AWS リソースに対する偵察の実行、またはDDoSアクティビティへの積極的な関与である IP アドレスを探します。この`AWSManagedIPDDoSList`ルールは、悪意のあるリクエストのフラッドの 90% 以上をブロックしていることが確認されています。

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、VPNs、プロキシ、Tor ノード、クラウドプラットフォーム (を除く AWS) からのリクエストが含まれます。

さらに、Security Automations for AWS WAF solution の IP Lists パーサーコンポーネントを使用して、サードパーティーの IP 評価リストを使用することもできます。

AWS WAF - インテリジェントな脅威の軽減

ボットネットは重大なセキュリティ上の脅威であり、スパムの送信、機密データの盗難、ランサムウェア攻撃の開始、不正クリックによる広告詐欺のコミット、分散 denial-of-service （ DDoS) 攻撃の開始などの違法または有害な活動を実行するために一般的に使用されます。ボット攻撃を防ぐには、AWS WAF Bot Control マネージドルールグループを使用します。このルールグループは、自己識別ボットにラベルを追加し、一般的に望ましいボットを検証し、高い信頼性のボット署名を検出し、自己識別しない高度なボットの検出を追加する「ターゲット」保護レベルを提供する基本的な「共通」保護レベルを提供します。

ターゲットを絞った保護では、ブラウザ調査、フィンガープリント、動作ヒューリスティックなどの高度な検出手法を使用して不正なボットトラフィックを特定し、レート制限やチャレンジルールアクションなどの緩和コントロールを適用CAPTCHAします。Targeted には、人間のようなアクセスパターンを適用し、リクエストトークンを使用して動的レート制限を適用するためのレート制限オプションも用意されています。詳細については、AWS WAF 「Bot Control ルールグループ」を参照してください。 アプリケーションのログインページで悪意のある乗っ取りの試みを検出および管理するには、 AWS WAF Fraud Control アカウント乗っ取り防止 (ATP) ルールグループを使用できます。ルールグループは、クライアントがアプリケーションのログインエンドポイントに送信するログイン試行を検査し、ログイン試行に対するアプリケーションの応答も検査して、成功率と失敗率を追跡します。

アカウント作成の不正行為は、攻撃者が 1 つ以上の偽のアカウントの作成を試みるオンライン上の違法行為です。攻撃者は、プロモーションやサインアップボーナスの濫用、なりすまし、フィッシングなどのサイバー攻撃などの不正行為のために偽のアカウントを使用します。偽のアカウントの存在は、顧客からの評判に傷をつけたり、金銭的な被害を伴う不正行為のリスクを生じさせたりするものであり、ビジネスに悪影響を及ぼす可能性があります。

Fraud Control アカウント作成の不正防止 (ACFP) AWS WAF 機能を実装することで、アカウント作成の不正試行をモニタリングおよび制御できます。 AWS WAF は、コンパニオンアプリケーション統合 `AWS ManagedRulesACFPRuleSet` を使用して AWS マネージドルール ルールグループでこの機能を提供しますSDKs。

これらの保護の詳細については、AWS WAF インテリジェントな脅威の軽減 を参照してください。

アプリケーションレイヤーDDoSイベントを自動的に緩和する (BP1、BP2、BP6)

にサブスクライブしている場合は AWS Shield Advanced、Shield Advanced 自動アプリケーションレイヤーDDoS緩和 を有効にできます。この機能は、ユーザーに代わってレイヤー 7 DDoSイベントを軽減するためのルールを自動的に作成、評価、デプロイ AWS WAF します。

AWS Shield Advanced は、WAFウェブ に関連付けられた保護されたリソースごとにトラフィックベースラインを確立しますACL。確立されたベースラインから大幅に逸脱したトラフィックは、潜在的なDDoSイベントとしてフラグが付けられます。イベントが検出されると、イベントを構成するウェブリクエストの署名を識別 AWS Shield Advanced しようとし、署名が特定されると、その署名でトラフィックを軽減するための AWS WAF ルールが作成されます。

ルールが履歴ベースラインに対して評価され、安全であると判断された場合、ルールは Shield マネージドルールグループに追加され、ルールがカウントモードまたはブロックモードでデプロイされるかどうかを選択できます。Shield Advanced は、イベントが完全に沈静化されたと判断すると、AWS WAF ルールを自動的に削除します。

Engage SRT (Shield Advanced サブスクライバーのみ)

さらに、Shield Advanced にサブスクライブすると、 をエンゲージ AWS SRTして、アプリケーションの可用性を損なう攻撃を軽減するためのルールを作成できます。アカウントの AWS Shield Advanced と への制限付きアクセスを許可 AWS SRTできます AWS WAF APIs。 AWS SRT はこれらにアクセスしてAPIs、明示的な認可がある場合にのみアカウントに緩和策を配置します。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 を使用して、組織全体で AWS Shield Advanced 保護やルールなどのセキュリティ AWS WAF ルールを一元的に設定および管理できます。 AWS Organizations 管理アカウントは、Firewall Manager ポリシーの作成が許可されている管理者アカウントを指定できます。これらのポリシーでは、リソースタイプやタグなどの条件を定義して、ルールが適用される場所を決定できます。これは、複数のアカウントがあり、保護を標準化する場合に便利です。

以下についての詳細:

- AWS マネージドルール については AWS WAF、「」のAWS マネージドルールAWS WAF「」を参照してください。
- 地理的制限を使用して CloudFront ディストリビューションへのアクセスを制限するには、「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。

- を使用して AWS WAF、以下を参照してください。
  - の開始方法 AWS WAF
  - 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の設定については、「 のレートベースのルールを使用してウェブサイトとサービスを保護する AWS WAF」を参照してください。
- Firewall Manager を使用して AWS リソース全体のルールのデプロイ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。

アタックサーフェスリダクション

AWS ソリューションを設計する際のもう 1 つの重要な考慮事項は、攻撃者がアプリケーションをターゲットにする機会を制限することです。この概念は、アタックサーフェスリダクション と呼ばれます。インターネットに公開されていないリソースは攻撃するのが難しく、攻撃者がアプリケーションの可用性をターゲットにするためのオプションが制限されます。

例えば、ユーザーが特定のリソースと直接やり取りすることを期待しない場合は、それらのリソースにインターネットからアクセスできないことを確認してください。同様に、通信に必要のないポートやプロトコルで、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入れないでください。

次のセクション AWS では、攻撃対象領域を減らし、アプリケーションのインターネットへの露出を制限する際のベストプラクティスを提供します。

難読化 AWS リソース (BP1、BP4、BP5)

通常、ユーザーは AWS リソースをインターネットに完全に公開することなく、迅速かつ簡単にアプリケーションを使用できます。

セキュリティグループとネットワーク ACLs (BP5)

Amazon Virtual Private Cloud (Amazon VPC) では、 の論理的に分離されたセクションをプロビジョニングできます。 AWS クラウド ここでは、定義した仮想ネットワークで AWS リソースを起動できます。

セキュリティグループとネットワークACLsは、 内の AWS リソースへのアクセスを制御できる点で似ていますVPC。ただし、セキュリティグループを使用すると、インバウンドトラフィックとアウトバウンドトラフィックをインスタンスレベルで制御できますが、ネットワークACLsはVPCサブネットレベルで同様の機能を提供します。セキュリティグループまたはネットワーク の使用には追加料金はかかりませんACLs。

インスタンスの起動時にセキュリティグループを指定するか、後でインスタンスをセキュリティグループに関連付けるかを選択できます。セキュリティグループへのすべてのインターネットトラフィックは、トラフィックを許可する許可ルールを作成しない限り、暗黙的に拒否されます。

例えば、Elastic Load Balancer の背後に Amazon EC2インスタンスがある場合、インスタンス自体がパブリックにアクセス可能である必要はなく、プライベートIPsのみを持つ必要があります。代わりに、ターゲットグループサブネットのネットワークアクセスコントロールリスト () と組み

合わせて 0.0.0.0/0 へのアクセスを許可するセキュリティグループルールを使用して、Elastic Load Balancing に必要なNACLターゲットリスナーポートへのアクセスを Elastic Load Balancer に提供し、Elastic Load Balancing IP 範囲のみがインスタンスと通信できるようにすることができます。Elastic Load Balancing これにより、インターネットトラフィックが 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ついて学習し、アプリケーションに影響を与えることがより困難になります。

ネットワーク を作成するときにACLs、許可ルールと拒否ルールの両方を指定できます。これは、アプリケーションへの特定のタイプのトラフィックを明示的に拒否する場合に便利です。例えば、サブネット全体へのアクセスを拒否される IP アドレス (CIDR範囲) 、プロトコル、送信先ポートを定義できます。アプリケーションがTCPトラフィックにのみ使用される場合は、すべてのUDPトラフィックを拒否するルールを作成することも、その逆を行うこともできます。このオプションは、DDoSソースIPsやその他の署名がわかっている場合に攻撃を軽減するための独自のルールを作成できるため、攻撃に対応するときに便利です。

にサブスクライブしている場合は AWS Shield Advanced、Elastic IP アドレスを保護されたリソースとして登録できます。DDoS 保護されたリソースとして登録されている Elastic IP アドレスに対する攻撃は、より迅速に検出されるため、緩和までの時間が短縮される可能性があります。攻撃が検出されると、DDoS緩和システムはターゲットの Elastic IP アドレスACLに対応するネットワークを読み取り、サブネットレベルではなく AWS ネットワークボーダーに強制します。これにより、多くのインフラストラクチャレイヤーDDoS攻撃による影響のリスクが大幅に軽減されます。

DDoS 回復性を最適化ACLsするようにセキュリティグループとネットワークを設定する方法の詳細については、DDoS「攻撃対象領域を減らすことで攻撃に備える方法」を参照してください。

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

オリジンの保護 (BP1、BP5)

内のオリジン CloudFront で Amazon を使用している場合はVPC、 CloudFront ディストリビューションのみがオリジンにリクエストを転送できるようにすることをお勧めします。Edge-to-Origin リクエストヘッダーを使用すると、 がリクエストをオリジン CloudFront に転送するときに、既存のリクエストヘッダーの値を追加または上書きできます。オリジンカスタムヘッダー 、例えば `X-Shared-Secret`ヘッダーを使用して、オリジンに対して行われたリクエストが から送信されたことを検証できます CloudFront。

オリジンカスタムヘッダー によるオリジンの保護の詳細については、「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 Balancer へのアクセスの制限」を参照してくだ

さい。 https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/add-origin-custom-headers.html

オリジンアクセス制限の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サンプルソリューションを実装するガイドについては、「 AWS WAF および Secrets Manager で Amazon CloudFront オリジンセキュリティを強化する方法」を参照してください。

または、 AWS Lambda関数を使用して、 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こともできます。これにより、悪意の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 AWS WAF ときに CloudFront および をバイパスできないようにすることで、オリジンのセキュリティが向上します。

セキュリティグループと X-Shared-Secretヘッダーを自動的に更新してオリジンを保護する方法の詳細については、「Amazon のセキュリティグループを自動的に更新する方法 CloudFront 」および AWS WAFAWS Lambda「」を参照してください。

ただし、このソリューションでは、Lambda 関数の実行に追加の設定とコストがかかります。これを簡素化するために、オリジン向け IP アドレスのみ CloudFrontからオリジンへのインバウンドHTTP/HTTPSトラフィックを制限する AWSの マネージドプレフィックスリスト CloudFrontが導入されました。 AWSマネージドプレフィックスリストは によって作成および管理 AWS され、追加料金なしで使用できます。(Amazon VPC) セキュリティグループルール、サブネットルートテーブル、 を使用した一般的なセキュリティグループルール、およびマネージドプレフィックスリスト を使用できるその他の AWS リソース CloudFront で AWS Firewall Manager、 のマネージドプレフィックスリストを参照できます。

Amazon の AWSマネージドプレフィックスリストの使用の詳細については CloudFront、「Amazon の AWSマネージドプレフィックスリストを使用してオリジンへのアクセスを制限する CloudFront」を参照してください。

> **Note**
>
> このドキュメントの他のセクションで説明したように、オリジンを保護するためにセキュリティグループに依存すると、リクエストのフラッド中にセキュリティグループ接続の追跡が潜在的なボトルネックとして追加される可能性があります。キャッシュを有効にするキャッシュポリシー CloudFront を使用して悪意のあるリクエストをフィルタリングできる場合を除き、前述のオリジンカスタムヘッダー を使用して、オリジンに対して行われたリクエストがセキュリティグループを使用するのではなく CloudFront、 から送信されたことを検証することをお勧めします。Application Load Balancer リスナールールでカスタムリクエストヘッダーを使用すると、ロードバランサーへの新しい接続の確立に影響する可能性のある追跡

制限によるスロットリングを防ぐことができます。これにより、Application Load Balancer は、DDoS攻撃発生時のトラフィックの増加に基づいてスケーリングできます。

API エンドポイントの保護 (BP4)

API を一般に公開する必要がある場合、APIフロントエンドがDDoS攻撃のターゲットになるリスクがあります。リスクを軽減するために、Amazon API Gateway を Amazon EC2、、 AWS Lambda またはその他の場所で実行されているアプリケーションへのエントリウェイとして使用できます。Amazon API Gateway を使用すると、APIフロントエンドに独自のサーバーが不要になり、アプリケーションの他のコンポーネントを難読化できます。アプリケーションのコンポーネントを検出しにくくすることで、これらの AWS リソースがDDoS攻撃のターゲットにならないようにすることができます。

Amazon API Gateway を使用する場合、2 種類のAPIエンドポイントから選択できます。1 つ目は、Amazon CloudFront ディストリビューションを介してアクセスされるエッジ最適化APIエンドポイントのデフォルトのオプションです。ただし、ディストリビューションは API Gateway によって作成および管理されるため、ユーザーはディストリビューションを制御できません。2 番目のオプションは、 が AWS リージョン RESTAPIデプロイされているのと同じ 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ことです。 AWS では、2 番目のタイプのエンドポイントを使用し、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ます。これにより、Amazon CloudFront ディストリビューションを制御し、アプリケーションレイヤーの保護に AWS WAF を使用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緩和性能にアクセスできます。

Amazon Gateway AWS WAF で Amazon CloudFront および API を使用する場合は、次のオプションを設定します。

- すべてのヘッダーを API Gateway リージョンエンドポイントに転送するようにディストリビューションのキャッシュ動作を設定します。これにより、 はコンテンツを動的として扱い、コンテンツのキャッシュをスキップ CloudFront します。
- API Gateway でAPIキー値を設定して、オリジンカスタムヘッダー を含めるようにディストリビューションを設定することで x-api-key、APIゲートウェイを直接アクセスから保護します。
- でメソッドごとに標準またはバーストレート制限を設定することで、過剰なトラフィックからバックエンドを保護しますRESTAPIs。

Amazon API Gateway APIsで を作成する方法の詳細については、「Amazon API Gateway 入門」を参照してください。

運用手法

このホワイトペーパーの緩和手法は、本質的にDDoS攻撃に対して回復力のあるアプリケーションを設計するのに役立ちます。多くの場合、DDoS攻撃がアプリケーションをターゲットにしているタイミングを把握して、緩和措置を講じることも役立ちます。このセクションでは、異常な動作の可視化、アラートと自動化、大規模な保護の管理、追加のサポート AWS への関与に関するベストプラクティスについて説明します。

負荷テスト

ホワイトペーパーの「負荷テストアプリケーション」のガイドラインに従って、予想されるトラフィックレベルと予想されるトラフィックレベルの両方でアプリケーションを定期的に負荷テストします。これにより、アーキテクチャの有効性、Auto Scaling ポリシーの仕組み、エラー処理の機能を確認できます。予想されるトラフィックのスケールアップとスケールダウン、および「フラッシュクラウド」タイプの動作をテストします。定期的に、またはメジャーリリースの前に再テストします。SYN フラッドなどのレイヤー 3 または 4 DDoSシミュレーションテストについては、DDoSシミュレーションテストポリシー に従ってください。

メトリクスおよびアラーム

ベストプラクティスとして、インフラストラクチャとアプリケーションのモニタリングツールを使用してアプリケーションの可用性をチェックし、アプリケーションがDDoSイベントの影響を受けないようにする必要があります。オプションとして、 リソースのアプリケーションとインフラストラクチャの Route 53 ヘルスチェックを設定して、DDoSイベントの検出を改善できます。ヘルスチェックの詳細については、、AWS WAF Firewall Manager、Shield Advanced デベロッパーガイドを参照してください。

主要な運用メトリクスが想定値から大幅に逸脱すると、攻撃者がアプリケーションの可用性をターゲットにしようとしている可能性があります。アプリケーションの通常の動作に精通していることは、異常を検出したときにより迅速にアクションを実行できることを意味します。Amazon CloudWatch は、 で実行するアプリケーションをモニタリングすることで役立ちます AWS。例えば、メトリクスの収集と追跡、ログファイルの収集とモニタリング、アラームの設定、 AWS リソースの変更への自動応答を行うことができます。

アプリケーションを設計するときに DDoSレジリエントなリファレンスアーキテクチャに従うと、アプリケーションに到達する前に一般的なインフラストラクチャレイヤー攻撃がブロックされます。に

サブスクライブしている場合は AWS Shield Advanced、アプリケーションがターゲットになっていることを示す多数の CloudWatchメトリクスにアクセスできます。

例えば、進行中のDDoS攻撃が発生したときに通知するようにアラームを設定して、アプリケーションの状態をチェックし、 をエンゲージするかどうかを決定できます AWS SRT。攻撃が検出されたかどうかを通知するように DDoSDetectedメトリクスを設定できます。攻撃量に基づいてアラートを受け取る場合は、DDoSAttackBitsPerSecond、、DDoSAttackPacketsPerSecondまたは DDoSAttackRequestsPerSecondメトリクスを使用することもできます。これらのメトリクスは、独自のツール CloudWatch と統合するか、Slack や などのサードパーティーが提供するツールを使用してモニタリングできます PagerDuty。

アプリケーションレイヤー攻撃は、多くの Amazon CloudWatch メトリクスを昇格させることができます。を使用している場合は AWS WAF、 CloudWatch を使用して、 で許可、カウント、またはブロック AWS WAF するように設定したリクエストの増加に対するアラームをモニタリングおよびアクティブ化できます。これにより、トラフィックのレベルがアプリケーションが処理できるレベルを超えた場合に通知を受け取ることができます。で追跡される Amazon CloudFront、Amazon Route 53、Application Load BalancerNetwork Load Balancer、Amazon 、および Auto Scaling メトリクス CloudWatch を使用してEC2、DDoS攻撃を示す可能性のある変更を検出することもできます。

次の表に、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 メトリクスの説明を示します。

表 3 - 推奨される Amazon CloudWatch メトリクス

トピック	メトリクス	説明
AWS Shield Advanced	DDoSDetected	特定の Amazon リソースネーム () のDDoSイベントを示しますARN。
AWS Shield Advanced	DDoSAttackBitsPerSecond	特定の のDDoSイベント中に観測されたバイト数ARN。このメトリクスは、レイヤー 3 または 4 DDoSイベントでのみ使用できます。
AWS Shield Advanced	DDoSAttackPacketsPerSecond	特定の のDDoSイベント中に観測されたパケットの数ARN。このメトリクスは、レ

トピック	メトリクス	説明
		イヤー 3 または 4 DDoSイベントでのみ使用できます。
AWS Shield Advanced	DDoSAttackRequests PerSecond	特定の のDDoSイベント中に観測されたリクエストの数 ARN。このメトリクスは、レイヤー 7 DDoSイベントでのみ使用でき、最も重要なレイヤー 7 イベントでのみ報告されます。
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	渡されたリクエストの数。これは、ルールグループのルールのいずれとも一致せず、ルールグループ評価を通過するリクエストについてのみ使用されます。
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 であるすべてのリクエストの割合5xx。
Amazon Route 53	HealthCheckStatus	ヘルスチェックエンドポイントのステータス。

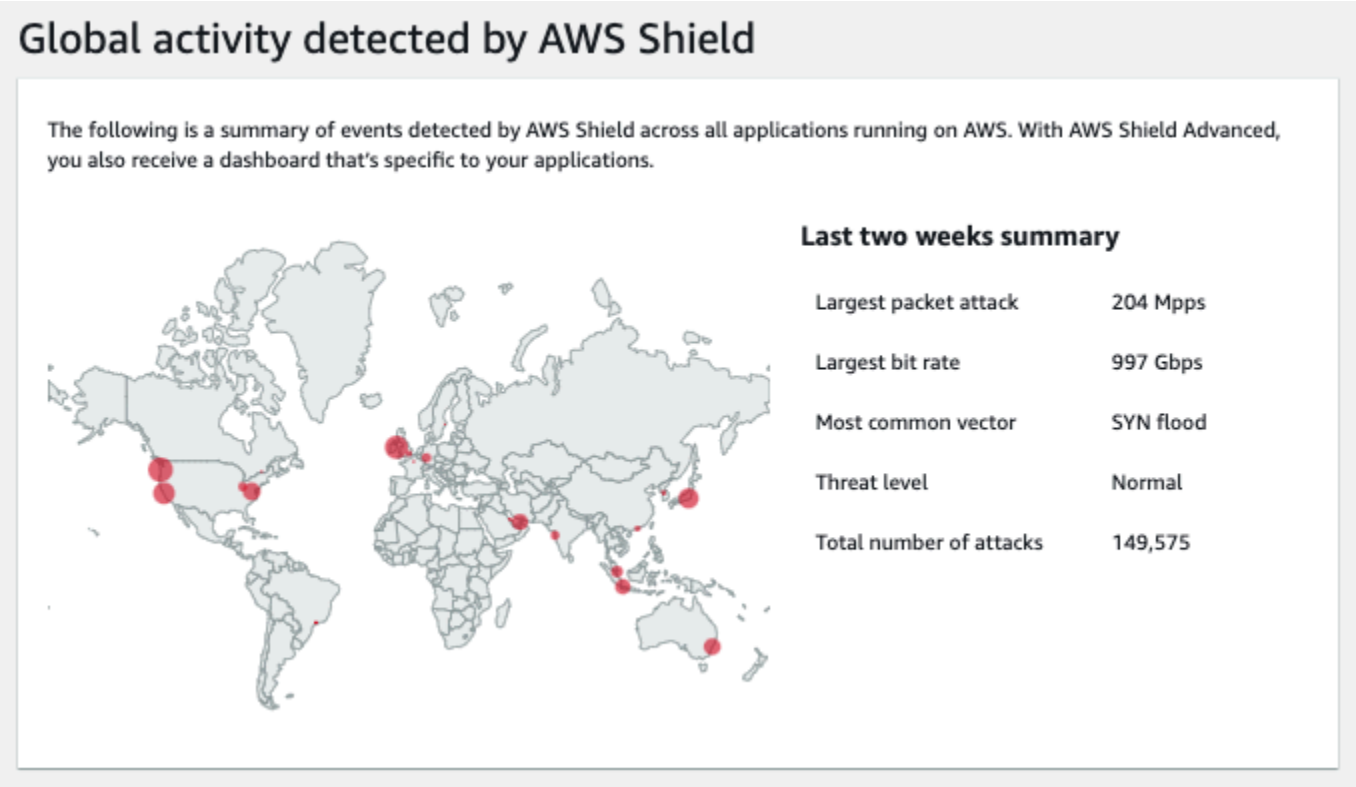
トピック	メトリクス	説明
Application Load Balancer	ActiveConnectionCount	クライアントからロードバランサー、およびロードバランサーからターゲットへのアクティブな同時TCP接続の合計数。
Application Load Balancer	ConsumedLCUs	ロードバランサーが使用するロードバランサーキャパシティーユニット (LCU) の数。
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	ロードバランサーによって生成された HTTP4xxまたは5xxクライアントエラーコードの数。
Application Load Balancer	NewConnectionCount	クライアントからロードバランサー、およびロードバランサーからターゲットに確立された新しいTCP接続の合計数。
Application Load Balancer	ProcessedBytes	ロードバランサーによって処理される総バイト数。
Application Load Balancer	RejectedConnectionCount	ロードバランサーが接続の最大数に達したため、拒否された接続の数。
Application Load Balancer	RequestCount	処理されたリクエストの数。
Application Load Balancer	TargetConnectionErrorCount	ロードバランサーとターゲット間で正常に確立されなかった接続数。

トピック	メトリクス	説明
Application Load Balancer	TargetResponseTime	リクエストがロードバランサーを離れた後、ターゲットからのレスポンスが受信されるまでの経過時間を秒単位で表します。
Application Load Balancer	UnHealthyHostCount	異常とみなされるターゲットの数。
Network Load Balancer	ActiveFlowCount	クライアントからターゲットへの同時TCPフロー (または接続) の合計数。
Network Load Balancer	ConsumedLCUs	ロードバランサーが使用するロードバランサーキャパシティーユニット (LCU) の数。
Network Load Balancer	NewFlowCount	期間中にクライアントからターゲットに確立された新しいTCPフロー (または接続) の合計数。
Network Load Balancer	ProcessedBytes	TCP/IP ヘッダーを含む、ロードバランサーによって処理された合計バイト数。
Global Accelerator	NewFlowCount	期間中にクライアントからエンドポイントに確立された新しい TCPおよび UDPフロー (または接続) の合計数。
Global Accelerator	ProcessedBytesIn	TCP/IP ヘッダーを含む、アクセラレーターによって処理された受信バイトの合計数。
Auto Scaling	GroupMaxSize	Auto Scaling グループの最大サイズ。

トピック	メトリクス	説明
Amazon EC2	`CPUUtilization`	現在使用中の割り当て済みEC2コンピューティングユニットの割合。
Amazon EC2	`NetworkIn`	すべてのネットワークインターフェイスを通じ、このインスタンスによって受信されたバイトの数。

Amazon を使用してアプリケーションに対するDDoS攻撃 CloudWatch を検出する方法の詳細については、「Amazon の開始方法 CloudWatch」を参照してください。

AWS には、攻撃について通知したり、アプリケーションのリソースをモニタリングしたりするために、いくつかの追加のメトリクスとアラームが含まれています。 AWS Shield コンソールまたはは、アカウントごとのイベントの概要と、検出された攻撃に関する詳細APIを提供します。



によって検出されたグローバルアクティビティ AWS Shield

さらに、 グローバル脅威環境ダッシュボードには、 によって検出されたすべてのDDoS攻撃に関する概要情報が表示されます AWS。この情報は、攻撃の傾向に加えて、より多くのアプリケーション全体のDDoS脅威をよりよく理解し、観察した可能性のある攻撃と比較するのに役立ちます。

にサブスクライブしている場合 AWS Shield Advanced、サービスダッシュボードには、保護されたリソースで検出されたイベントの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、保護されたリソースへのトラフィックを複数のディメンションに沿って評価します。異常が検出されると、 はイベント AWS Shield を作成し、異常が観察されたトラフィックディメンションを報告します。緩和策を講じることで、リソースが過剰なトラフィックや既知のDDoSイベント署名に一致するトラフィックを受信することを防ぎます。

検出メトリクスは、ウェブACLが保護された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 ログに基づいています。緩和メトリクスは、Shield の DDoS緩和システムによって観測された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ます。

ネットワークトップコントリビューターメトリクスは、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についてのインサイトを提供します。最もボリュームの多い寄稿者を表示したり、プロトコル、ソースポート、TCPフラグなどの側面でソートしたりできます。上位の寄稿者メトリクスには、さまざまなディメンションに沿ってリソースで観測されたすべてのトラフィックのメトリクスが含まれます。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を提供します。非リフレクションレイヤー 3 または 4 攻撃では、ソース IP アドレスがなりすまされ、依存できない可能性があることに注意してください。

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たアクションに関する詳細も含まれています。この情報は、異常の調査、トラフィックのディメンションの調査、可用性を保護するために Shield Advanced が実行するアクションの理解を容易にします。

ログ記録

アプリケーション所有者向けのログ記録とモニタリングガイドに従って、すべてのサービスで便利なログ記録を有効にして、可視性を最大化し、トラブルシューティングを支援します。これには以下が含まれますが、これらに限定されません。

- AWS CloudTrail
- AWS WAF ログ
- CloudFront アクセスログ

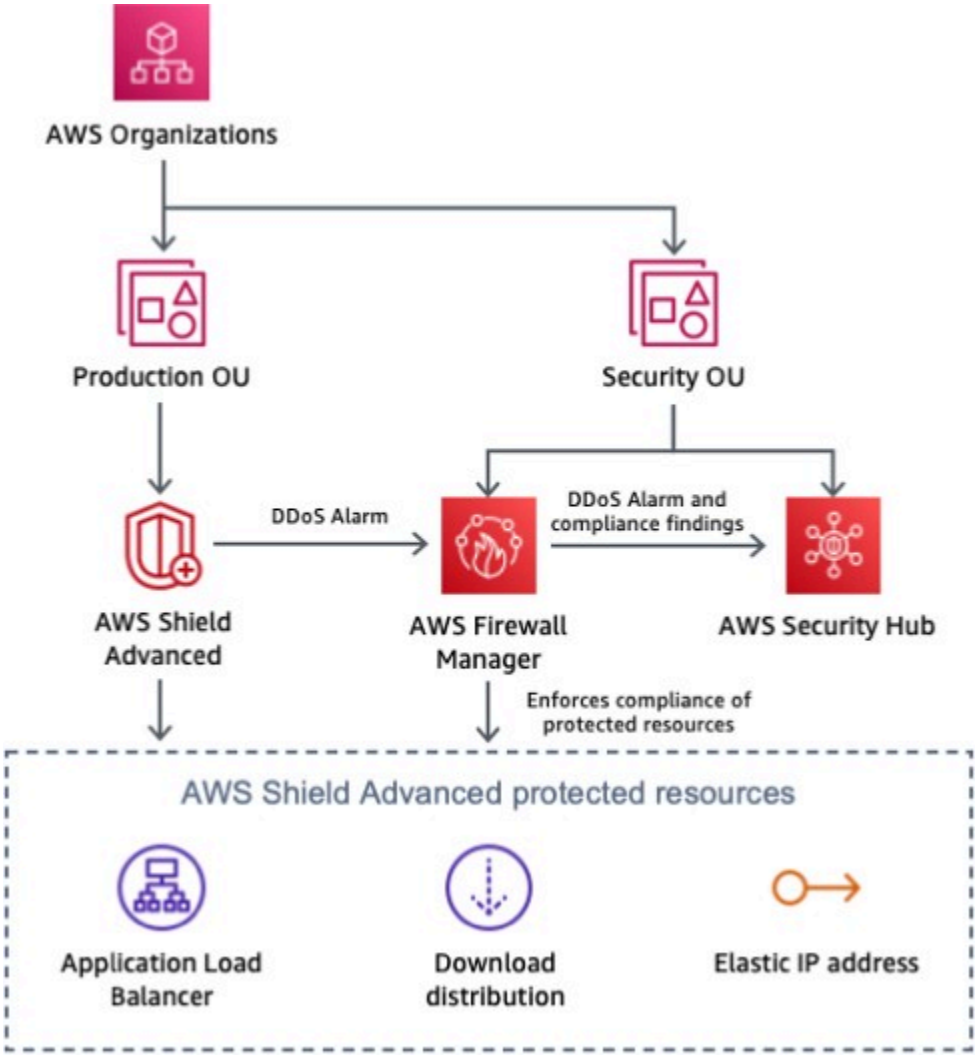
- VPC フローログ (「ログとネットワークトラフィックフローの表示」を参照) – 可視性を最大化するために、含まれているtcp-flagsフィールドに フィールドを含めます。
- ELB アクセスログ (ALB、CLB、NLB)
- ウェブサーバーHTTPアクセスログ
- オペレーティングシステムのセキュリティログ記録
- アプリケーションのログ記録

複数のアカウントにわたる可視性と保護の管理

複数の にまたがって運用 AWS アカウント し、保護する複数のコンポーネントがある場合、大規模な運用と運用オーバーヘッドの軽減を可能にする手法を使用すると、緩和機能が向上します。複数のアカウントで AWS Shield Advanced 保護されたリソースを管理する場合、 AWS Firewall Manager と を使用して一元的なモニタリングを設定できます AWS Security Hub。Firewall Manager を使用すると、すべてのアカウントで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、複数のアカウントで保護されたリソースを管理し、それらのリソースのモニタリングを一元化できます。

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ともに、単一のダッシュボードでセキュリティ結果を表示できます。

例えば、Shield Advanced がスコープ AWS アカウント 内の任意の で保護されたリソース宛ての異常なトラフィックを検出すると、この検出結果は Security Hub コンソールに表示されます。設定されている場合、Firewall Manager は、Shield Advanced で保護されたリソースとしてリソースを作成し、リソースが準拠状態にあるときに Security Hub を更新することで、リソースを自動的にコンプライアンス状態にすることができます。



Firewall Manager と Security Hub AWS Shieldを使用した で保護されたリソースのモニタリングを示すアーキテクチャ図

Shield で保護されたリソースの中央モニタリングの詳細については、「 DDoSイベントの集中モニタリングの設定」および「非準拠リソースの自動修復」を参照してください。

インシデント対応戦略とランブック

DDoS 攻撃インシデント対応戦略を策定し、それに関するセキュリティインシデント対応プロセスを構築することは、すべての組織にとって重要です。推奨されるアプローチは、証拠の収集、緩和、復旧、インシデント後分析の実行など、 NISTが提案したステップに基づいてレスポンスプレイブックをモデル化することです。例えば、ウェブアプリケーション DoS または DDoS攻撃のレスポンスプレイブックが例 として提供されています。その他のリソースについては、AWS 「セキュリティインシデント対応ガイド」を参照してください。

サポート

攻撃が発生した場合は、脅威の評価やアプリケーションのアーキテクチャの確認 AWS など、 のサポートの恩恵を受けることもできます。また、他のサポートをリクエストすることもできます。実際のイベントの前に、DDoS攻撃の対応計画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応型対策を目的としていますが、アプリケーションに対するDDoS攻撃は依然として発生する可能性があります。このセクションのオプションを確認して、シナリオに最適なサポートリソースを決定します。アカウントチームはユースケースとアプリケーションを評価し、特定の質問や課題に対応できます。

で本番稼働用ワークロードを実行している場合は AWS、ビジネスサポートにサブスクライブすることを検討してください。ビジネスサポートは、DDoS攻撃の問題を支援できるクラウドサポートエンジニアに 24 時間年中無休でアクセスを提供します。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、エンタープライズサポートを検討してください。エンタープライズサポートは、クリティカルなケースをオープンし、シニアクラウドサポートエンジニアから最速の応答を受け取る機能を提供します。

ビジネスサポート AWS Shield Advanced またはエンタープライズサポートのいずれかにサブスクライブしていて、サブスクライブもしている場合は、Shield 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、 リソースへの関連付け、および 24 時間 365 日のオペレーションの連絡先情報の提供が可能になります。Shield が の兆候を検出DDoSし、アプリケーションのヘルスチェックで低下の兆候が見られると、 AWS SRT は事前にお客様に連絡します。これは推奨されるエンゲージメントモデルです。これにより、応答時間が短縮 AWS SRTされ、問い合わせが確立される前にトラブルシューティング AWS SRTを開始できるためです。

詳細については、「Compare AWS Support Plans」を参照してください。

プロアクティブエンゲージメント機能では、アプリケーションのヘルスを正確に測定し、Shield Advanced で保護されたリソースに関連付ける Route 53 ヘルスチェックを設定する必要があります。Route 53 ヘルスチェックが Shield コンソールに関連付けられると、Shield Advanced 検出システムはアプリケーションのヘルスのインジケータとしてヘルスチェックステータスを使用します。Shield Advanced のヘルスベースの検出機能により、アプリケーションに異常がある場合に通知され、緩和策がより迅速に実行されます。 AWS SRT は、異常なアプリケーションがDDoS攻撃の対象であるかどうかをトラブルシューティングし、必要に応じて追加の緩和策を講じ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します。 AWS SRT はこの情報を使用してお客様に連絡します。最大 10 個の連絡先を設定し、特定の連絡先の要件または設定がある場合は追加のメモを提供できます。プロアクティブ

エンゲージメントの連絡先は、セキュリティオペレーションセンターやすぐに対応できる個人など、24 時間 365 日体制の口ールを保持する必要があります。

応答時間が重要なすべてのリソースまたは選択した主要な本番稼働用リソースに対して、プロアクティブエンゲージメントを有効にできます。これは、これらのリソースにのみヘルスチェックを割り当てることで実現されます。

また、AWS Support コンソールを使用して AWS Support ケースを作成するか (サインインが必要)、アプリケーションの可用性に影響する DDoS関連のイベントがある場合は サポートAPIを使用して、 に AWS SRTエスカレーションすることもできます。

結論

このホワイトペーパーで概説されているベストプラクティスは、多くの一般的なインフラストラクチャやアプリケーションレイヤーDDoS攻撃を防止することで、アプリケーションの可用性を保護する回復DDoS力のあるアーキテクチャを構築するのに役立ちます。アプリケーションを設計するときにこれらのベストプラクティスに従う範囲は、緩和できるDDoS攻撃のタイプ、ベクトル、量に影響します。DDoS 緩和サービスをサブスクライブしなくても、回復性を組み込むことができます。サブスクライブを選択すると、既に回復力のあるアプリケーションアーキテクチャをさらに保護するサポート、可視性、緩和、コスト保護機能 AWS Shield Advanced が追加されます。

寄稿者

本ドキュメントの寄稿者は次のとおりです。

- ロドリゴ・カロニ、 AWS セキュリティスペシャリスト TAM
- 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
- Joanna Knox、 AWS Support エンジニアリング
- Anuj Butail、 AWS ソリューションアーキテクト
- Harith Gaddamanugu、 AWS エッジスペシャリスト SA

詳細情報

詳細については、次を参照してください。

- 実装のガイドライン AWS WAF (AWS ホワイトペーパー)
- NIS301 – re:Inforce 2023: AWS 脅威インテリジェンスがマネージドファイアウォールルールになる方法 (YouTube ビデオ)
- NET314 - re:Invent 2022: を使用したDDoS耐障害性アプリケーションの構築 AWS Shield (YouTube ビデオ)
- SEC321 - re:Invent 2020: DDoSレスポンスチームのエスカレーションで先取りする (YouTube ビデオ)
- William Hill: High-Performance DDoS Protection with AWS - 2020 (YouTube ビデオ)
- SEC407 - re:Invent 2019: ウェブアプリケーションを構築する defense-in-depth アプローチ (YouTube ビデオ)
- でのDDoS緩和のベストプラクティス AWS – 2018 年 (YouTube ビデオ)
- SID324 – re:Invent 2017: クラウドでのDDoSレスポンスの自動化 (YouTube ビデオ)
- CTD304 – re:Invent 2017:"""" & Wall Street Journal's Journey to Manage Traffic Spikes While (YouTube ビデオ)
- 緩和DDoSとアプリケーションレイヤーの脅威 (YouTube ビデオ)
- CTD310 – re:Invent 2017: エッジで生きる、思っているよりも安全です。Amazon で強力な を構築する (YouTube ビデオ)
- CloudFront、 AWS Shield、および AWS WAF (YouTube ビデオ)

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ます。

変更	説明	日付
ホワイトペーパーの更新	CloudFront およびDNSワイルドカードコスト保護OACを追加しました。運用手法、キャッシュ、レートベースのルール、マネージドルールグループに関する説明を拡張しました。アーキテクチャ図にオンプレミスを追加し、重複を削除し、あいまいさを排除するためにテキストを明確化しました。	2023 年 8 月 9 日
ホワイトペーパーの更新	わかりやすくするために改訂されました。セキュリティグループ接続の追跡と Shield Advanced アプリケーションレイヤーの自動DDoS緩和に関する最新の推奨事項と機能を含めるように更新されました。	2022 年 4 月 13 日
ホワイトペーパーの更新	最新の推奨事項と機能を含めるように更新されました。 AWS Global Accelerator は、DDoSイベントの集中モニタリングと非準拠リソースの自動修復 AWS Firewall Manager のために、エッジでの包括的な保護の一部として追加されました。	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の跳ね返りELBと、Scale to Ab™ (BP6) セクションのALB使用状況を明確にするために更新されました。「リージョンの選択」とマークされた図と表 2 を更新しました。としてBP8。BP7 セクションを更新し、詳細を追加しました。	2019 年 12 月 18 日
ホワイトペーパーの更新	ベストプラクティスとして AWS WAF ログ記録を含めるように更新されました。	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、および関連するベストプラクティスを含むように更新されました。	2018 年 6 月 1 日
ホワイトペーパーの更新	規範的なアーキテクチャガイダンスを追加し、 を含めるように更新しました AWS WAF。	2016 年 6 月 1 日
初版発行	ホワイトペーパーの発行。	2015 年 6 月 1– 日

注意

お客様は、本書に記載されている情報を独自に評価する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ており、(b) 通知なしに変更される可能性がある現在の AWS 製品提供および慣行を表し、(c) AWS およびその関連会社、サプライヤー、または許諾者からのいかなる約束または保証も作成しません。 AWS 製品またはサービスは、明示または黙示を問わず、保証、表明、または条件なしに「現状のまま」提供されます。お客様 AWS に対する の責任と責任は AWS 契約によって管理され、本書は AWS とそのお客様との間の契約の一部でも変更もされません。

AWS 用語集

最新の AWS 用語については、「 AWS の用語集 リファレンス」のAWS 「 用語集」を参照してください。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。