AWS 決定ガイド

AWS WAF または AWS Shield?

AWS WAF または AWS Shield?: AWS 決定ガイド

Table of Contents

AWS WAF または AWS Shield?

違いを理解し、自分に合ったものを選択する

目的	AWS WAF または がウェブアプリケーションセキュリティサービスのニーズ AWS Shield を満たしているかどうかを判断するのに役立ちます。
最終更新日	2024 年 9 月 17 日
対象サービス	• AWS WAF • AWS Shield

序章

AWS WAF (ウェブアプリケーションファイアウォール) と AWS Shieldは、分散型サービス拒否 (DDoS) 攻撃やその他のウェブアプリケーションの脆弱性など、さまざまなタイプのサイバー攻撃からウェブアプリケーションを保護するのに役立ちます。

- AWS WAF は、一般的なウェブエクスプロイトからウェブアプリケーションを保護することに重点を置いています。を使用して AWS WAF 、悪意のあるトラフィックをフィルタリングし、SQL インジェクションやクロスサイトスクリプティング (XSS) などの攻撃から保護し、他の と統合するためのカスタマイズ可能なウェブセキュリティルールを作成します AWS のサービス。
- AWS Shield はマネージド DDoS 保護サービスです。 AWS Shield を使用して、常時オンの検出と自動緩和を有効にし、ネットワークレイヤーとトランスポートレイヤーでの一般的な DDoS 攻撃から保護します。

AWS Shield は大規模なネットワークレベルの攻撃から保護しますが、 AWS Shield Advanced では、 AWS WAF ウェブ ACL をリソースに関連付けて、アプリケーションレイヤーで保護できます。は、アプリケーション固有の脆弱性に対するより詳細な保護 AWS WAF を提供します。両方のサービスを多層防御戦略に連携させて使用し、さまざまなネットワークレイヤーにわたる幅広い潜在的な脅威からアプリケーションを保護します。

これらのサービスの主な違いの概要を次に示します。

カテゴリ	 AWS WAF	 AWS Shield
主な目的	ウェブアプリケーション (SQL インジェクションや XSS など) のエクスプロイトから保護します。	DDoS 攻撃 (SYN や UDP フラッドなど) から保護する
保護レイヤー	アプリケーションレイヤー (L7)	ネットワーク、トランスポート、アプリケーションレイヤー (L3/L4/L7)
デプロイメント	明示的に設定する必要があります	AWS Shield すべてのカスタマーアカウントに含まれる標準保護
カスタマイズ	カスタムルールで高度にカスタマイズ可能	アプリケーションレイヤー DDoS 保護の自動緩和を有効にするオプションを使用して、 AWS Shield アドバンストを有効または無効にする
マネージドルール	AWS マネージドルールとサードパーティールールを含む	該当しない
料金モデル	ルールとリクエストの数に基づくPay-as-you-go	AWS Shield 標準込み。 AWS Shield 高度な には追加コストがかかります
攻撃対応チーム	該当しない	AWS Shield Advanced (24/7 DDoS Response Team) で利用可能
リアルタイムモニタリング	はい	あり
トラフィック検査	リクエストレベル	パケットレベル

AWS WAF と の違い AWS Shield

AWS Shield 保護レイヤー AWS WAF、デプロイ、カスタマイズ、マネージドルール、料金モデル、攻撃対応チーム、リアルタイムモニタリング、トラフィック検査をカバーする、 と の 8 つの主な違い領域について説明します。

Layer of protection

AWS WAF

- アプリケーションレイヤー (レイヤー 7) で動作します。HTTP/S トラフィックをフィルタリングしてモニタリングすることで、ウェブアプリケーションを保護します。 AWS WAF は、SQL インジェクション、クロスサイトスクリプティング (XSS)、クロスサイトリクエスト偽造 (CSRF) などの一般的なウェブエクスプロイトから保護します。IP アドレス、クエリ文字列、ヘッダーなど、さまざまな基準に基づいて悪意のあるリクエストをブロックするカスタムルールを作成できます。

AWS Shield

- 主にネットワーク (レイヤー 3) レイヤーとトランスポート (レイヤー 4) レイヤーで動作します。これは、SYN/ACK フラッド、UDP リフレクション攻撃、ボリューメトリック攻撃などのネットワークリソースを圧倒することを目的とした分散型サービス拒否 (DDoS) 攻撃を軽減するように設計されています。 は、攻撃を受けている場合でも、リソースに到達する AWS ネットワークトラフィックを引き続き利用できる AWS Shield ようにします。 AWS Shieldの保護は、ネットワークトラフィックパターンを分析し、 AWS ネットワークエッジで特定された脅威を自動的に軽減することで機能します。

Deployment

AWS WAF

- 明示的なセットアップと設定が必要です。Amazon CloudFront AWS のサービス、Application Load Balancer (ALB)、Amazon API Gateway、 AWS AppSync など、複数の にデプロイできます。ウェブ ACLs (アクセスコントロールリスト) を作成してリソースに関連付け、特定のウェブリクエストを許可、ブロック、またはモニタリングするルールを定義する必要があります。 はカスタマイズ可能なデプロイオプション AWS WAF を提供し、特定のアプリケーションニーズに合わせてセキュリティポリシーを調整できます。

AWS Shield

- と自動的に統合 AWS のサービス され、常にオンになっているため、基本的な保護のための追加のセットアップは必要ありません。 AWS Shield Standard はすべての に自動的に含まれ AWS アカウント、Amazon EC2、Elastic Load Balancing (ELB)、Amazon CloudFront、Route 53 などのリソースが保護されます。Advanced で AWS Shield 保護を強化するには、特定のリソースに対して明示的に有効にする必要があります。デプロイはシームレスであり、一度 AWS Shield オンにすると追加の設定は必要ありません。

Customization

AWS WAF

- 広範なカスタマイズ機能を提供します。IP アドレス、HTTP ヘッダー、クエリ文字列パラメータなどに基づいてウェブリクエストを許可、ブロック、またはカウントするための特定の条件を定義するルールを使用して、カスタムウェブ ACLs (アクセスコントロールリスト) を作成できます。 は、 AWS またはサードパーティのマネージドルールグループ AWS WAF をサポートします。これは、特定のアプリケーションニーズに合わせてさらにカスタマイズできます。レートベースのルールを設定して、単一の IP アドレスからのリクエスト数を制限し、 AWS WAF と統合 AWS Lambda して、高度なリクエストの検査とレスポンスを実行することもできます。

AWS Shield

- 限られたカスタマイズオプションを提供します。Standard では AWS Shield 、保護は自動的に行われ、設定できません。 AWS Shield Advanced を使用すると、高度なメトリクスとアラートの有効化、ヘルスチェックの設定、 AWS DDoS レスポンスチーム (DRT) へのアクセスなど、いくつかのカスタマイズが可能になり、緩和サポートをカスタマイズできます。ただし、その焦点はユーザー定義の設定ではなく、自動 DDoS 保護にとどまります。AWS WAF ウェブ ACL をリソースに関連付けて、アプリケーションレイヤーの保護を有効にできます。

Managed rules

AWS WAF

- 一般的なウェブ脅威から保護するためにウェブアプリケーションに適用できるさまざまなマネージドルールを提供します。これらのマネージドルールは、 AWS またはサードパーティーのセキュリティベンダーによって事前設定されており、SQL インジェクション、クロスサイト

スクリプティング (XSS)、既知の不正な IP アドレスなど、さまざまなセキュリティシナリオを対象としています。これらのマネージドルールグループをサブスクライブしてウェブ ACLs に適用することで、新しい脆弱性や脅威に対応するために定期的に更新されるout-of-the-box使える保護を提供できます。マネージドルールをカスタマイズし、カスタムルールと組み合わせて、特定のアプリケーションニーズに合わせてセキュリティポリシーを調整できます。 には、マネージド型のインテリジェントな脅威軽減機能 AWS WAF も用意されています。これらは、悪意のあるボットやアカウント乗っ取りの試みなどの脅威から保護するために実装できる、高度で特殊な保護機能です。

AWS Shield

- 主に DDoS 保護に焦点を当てており、従来のマネージドルールは提供していません。 AWS Shield Standard は、一般的なネットワークおよびトランスポートレイヤー DDoS 攻撃に対して事前定義された一連の保護を自動的に適用します。 AWS Shield Advanced はこれらの保護を強化しますが、カスタマイズ可能なマネージドルールは提供しません。代わりに、より高度な緩和手法と、カスタマイズされた支援のための DDoS 対応チームへのアクセスを提供します。

Pricing model

AWS WAF

- pay-as-you-goモデルを使用します。料金は、作成したウェブ ACLs の数、各 ACL 内にデプロイしたルールの数、およびルールによって処理されたウェブリクエストの数に基づいて課金されます。このモデルでは、実際の使用量に基づいてスケーラブルなコストを実現できます。つまり、必要なリソースに対してのみ料金が発生します。 AWS またはサードパーティーベンダーが提供するマネージドルールグループには追加料金が適用されます。 は、リクエストごとの同様の料金モデルでボット制御と不正制御のマネージドルール AWS WAF も提供します。 は、提供されるキャプチャ試行とチャレンジレスポンスの数によって課金されるキャプチャ/チャレンジ機能 AWS WAF も提供します。

AWS Shield

- 階層型料金モデルがあります。 AWS Shield Standard はすべての に追加コストなしで含まれ AWS アカウント、基本的な DDoS 保護を提供します。 AWS Shield Advanced では、毎月のサブスクリプションと、特定のしきい値を超えるデータ転送と緩和のための追加料金に基づいて

料金が発生します。このサブスクリプションには、 AWS DDoS Response Team (DRT) への 24 時間 365 日アクセス、高度な攻撃診断、攻撃中のコスト保護が含まれます。

Attack response team

AWS WAF

- サービスの一部として専用の攻撃対応チームは含まれません。代わりに、セキュリティルール自体を作成、管理、調整できるツールと機能を提供します。脅威の状況に基づいてトラフィックをモニタリングしACLs をリアルタイムで変更することはできますが、攻撃の軽減のために専門のサポートチームに直接アクセスすることはできません。

AWS Shield

- Advanced サービスの一環として AWS Shield 、 AWS DDoS Response Team (DRT) へのアクセスを提供します。DRT は、リアルタイムの攻撃の軽減と対応を支援する 24 時間 365 日のエキスパートチームです。DDoS 攻撃を受けている場合は、DRT に連絡して、脅威を効果的に管理および軽減するためのカスタマイズされたアドバイスとサポートを受けることができます。これには、 AWS リソースへの影響を最小限に抑えるためのベストプラクティス、インシデント分析、調整された対応に関するガイダンスが含まれます。

Real-time monitoring

AWS WAF

- AWS CloudWatch と統合することでリアルタイムのモニタリングを提供し、ブロックまたは許可されたリクエスト、リクエストレート、特定のルールの有効性などのメトリクスを追跡できます。 AWS WAF は、 AWS マネジメントコンソール または APIs。 AWS WAF メトリクスに基づいてカスタム CloudWatch アラームを設定して、潜在的な脅威や異常なトラフィックパターンに迅速に対応できます。

AWS Shield

- 主に AWS Shield Advanced を通じてリアルタイムモニタリングを提供します。 AWS CloudWatch と統合して、DDoS 攻撃に関連するほぼリアルタイムのメトリクスとアラートを提供します。攻撃診断、トラフィックパターン、緩和策の有効性をモニタリングできます。

AWS Shield Advanced は、詳細なレポートと攻撃ベクトルの可視性も提供し、脅威に応じて自動的にスケールし、 を通じてインサイトを提供します AWS マネジメントコンソール。

どちらのサービスも、攻撃パターンとトラフィックの傾向を視覚化するためのダッシュボードを提供します。 AWS Shieldのモニタリングでは、ネットワークレベルの異常とボリューメトリック攻撃に焦点を当て、アプリケーションレイヤーのリクエストとルールの有効性に関するより深いインサイト AWS WAF を提供します。

Traffic inspection

AWS WAF

- アプリケーションレイヤー (レイヤー 7) のトラフィックを検査し、HTTP/S リクエストの内容を分析します。ユーザー定義のルールに対してウェブトラフィックを評価し、SQL インジェクション、クロスサイトスクリプティング (XSS)、リクエスト本文、ヘッダー、URL パラメータ内の他の悪意のあるペイロードなどの特定の攻撃パターンをチェックします。

AWS Shield

- DDoS 攻撃からの保護に重点を置き、主にネットワーク (レイヤー 3) レイヤーとトランスポート (レイヤー 4) レイヤーのトラフィックを検査します。アプリケーションレイヤートラフィック (HTTP/S) の内容を検査するのではなく、トラフィック量が異常に多い、プロトコルの誤用など、DDoS 攻撃に典型的なパターンを探します。 AWS Shield は、ユーザー定義のルールやコンテンツベースの検査なしでこれらの脅威を自動的に軽減し、攻撃 AWS のサービス 対象のの可用性を確保します。

使用アイテム

AWS WAF

- とは AWS WAF

  AWS WAF を使用して、一般的なウェブエクスプロイトからウェブアプリケーションをモニタリングおよび保護する方法について説明します。

  ガイドを見る

- Amazon CloudWatch AWS WAF Logs でのログの分析

Amazon CloudWatch logs へのネイティブ AWS WAF ログ記録を設定し、ログ内のデータを視覚化および分析します。

ブログを読む

- Amazon CloudWatch ダッシュボードを使用して AWS WAF ログを視覚化する

  Amazon CloudWatch を使用して、CloudWatch メトリクス、Contributor Insights、および Logs Insights AWS WAF を使用してアクティビティをモニタリングおよび分析します。

  ブログを読む

AWS Shield

- とは AWS Shield

  を使用して AWS Shield 、ネットワークレイヤーとトランスポートレイヤーでの一般的な DDoS 攻撃からウェブアプリケーションを保護する方法について説明します。

  ガイドを見る

- Advanced の開始方法 AWS Shield

  Advanced コンソール AWS Shield を使用して AWS Shield Advanced の使用を開始します。

  ガイドを見る

- AWS Shield 高度なワークショップ

  インターネットに公開されているリソースを DDoS 攻撃から保護し、インフラストラクチャに対する DDoS 攻撃をモニタリングして、適切なチームに通知します。

  ワークショップの詳細

ドキュメント履歴

次の表に、この決定ガイドの重要な変更点を示します。このガイドの更新に関する通知については、RSS フィードをサブスクライブできます。

変更	説明	日付
初版発行	ガイドが最初に公開されました。	2024 年 9 月 17 日