AWS WAF でできる Bot 対策

AWS Black Belt Online Seminar

森　啓
Amazon Web Services Japan G.K.
Solutions Architect
2022/06

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分け、アマゾン ウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです
- AWSの技術担当者が、AWSの各サービスについてテーマごとに動画を公開します
- お好きな時間、お好きな場所でご受講いただけるオンデマンド形式です
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます

内容についての注意点

- 本資料では 2022 年 5 月時点のサービス内容および価格についてご説明しています。
  最新の情報は AWS 公式ウェブサイト(http://aws.amazon.com)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。
  日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

自己紹介

名前： 森　啓（Mori Akira）

所属：アマゾン ウェブ サービス ジャパン合同会社
技術統括本部 西日本ソリューション本部
ソリューションアーキテクト

好きな AWS サービス：
Amazon CloudFront
AWS WAF, AWS Shield Advanced

本セミナーの対象者

- 学習できること
  - AWS WAF を活用した Bot 対策

  ※WAF のルールの運用方法の詳細については
  「AWS Managed Rules for AWS WAF の活用」をご参照ください

- 対象者
  - Web Application Firewall の一般的な知識をお持ちの方
  - AWS 環境へ適用する Bot 対策を検討中の方
  - AWS WAF の理解をより深めたい技術者の方

[AWS BlackBelt Online Seminar] AWS Managed Rules for AWS WAF の活用
https://www.youtube.com/watch?v=ceQ7eU_jkD4

アジェンダ

1. Bot 対策の必要性と従来の対策
2. AWS WAF Bot Control
3. Account Takeover Prevention (ATP)
4. CAPTCHA
5. 料金体系
6. まとめ

1. Bot 対策の必要性と従来の対策

AWS Shield 脅威インテリジェンスチームの調査

一般的なウェブアプリケーションに向けられたトラフィックの内
最大 51% が多種多様な Bot によるものと判明している

新機能 – AWS WAF Bot Control でウェブサイトの不要なトラフィックを削減

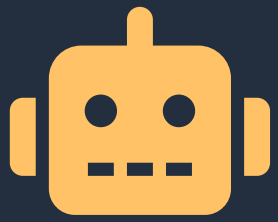
by Sébastien Stormacq | on 05 APR 2021 | in AWS WAF | Permalink | Share

AWS Shield の脅威調査チームが行った調査では、一般的なウェブアプリケーションに向けられたトラフィックの内の最大 51% は、マシン上で実行されるスクリプト (いわゆるボット) に由来することが判明しています。エンドポイントには、(望まいものや、そうではないものを含め) 多種多様なボット がヒットします。

適切なボットは、サイトをクロールしてインデックスを作成し、顧客から見つけやすくするためのものです。それ以外のボットは、サイトの可用性やパフォーマンスの監視を目的にしています。そして、こういったトラフィックの大部分は、不適切なボットによって生成されています。これらのスクリプトでは脆弱性を調査していたり、運営者の同意なしにコンテンツをコピーして別の場所に複製していたりします。これはセキュリティ上のリスクであるだけでなく、トラフィックを処理することでインフラストラクチャに対する不必要なプレッシャーとなり、コストも発生させます。

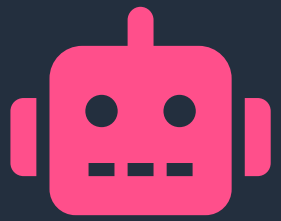
[AWS Blog] AWS WAF Bot Control でウェブサイトの不要なトラフィックを削減
https://aws.amazon.com/jp/blogs/news/reduce-unwanted-traffic-on-your-web-site-with-aws-bot-control/

Bot の種類



Good Bot

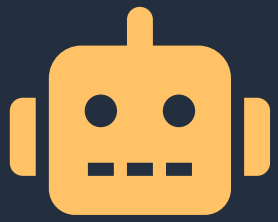
Human



Bad Bot

aws

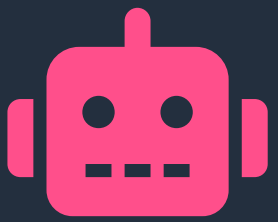
Bot の種類



Good Bot

クローラー
モニタリング 他

Human



Bad Bot

Layer7 DDoS
脆弱性スキャン
Webスクレイピング
Click / Download 他

aws

悪性の Bot による影響

インフラへの影響

- パフォーマンス低下、サービスダウン
- リソース消費
- コストの増大
- 運用負荷の増大

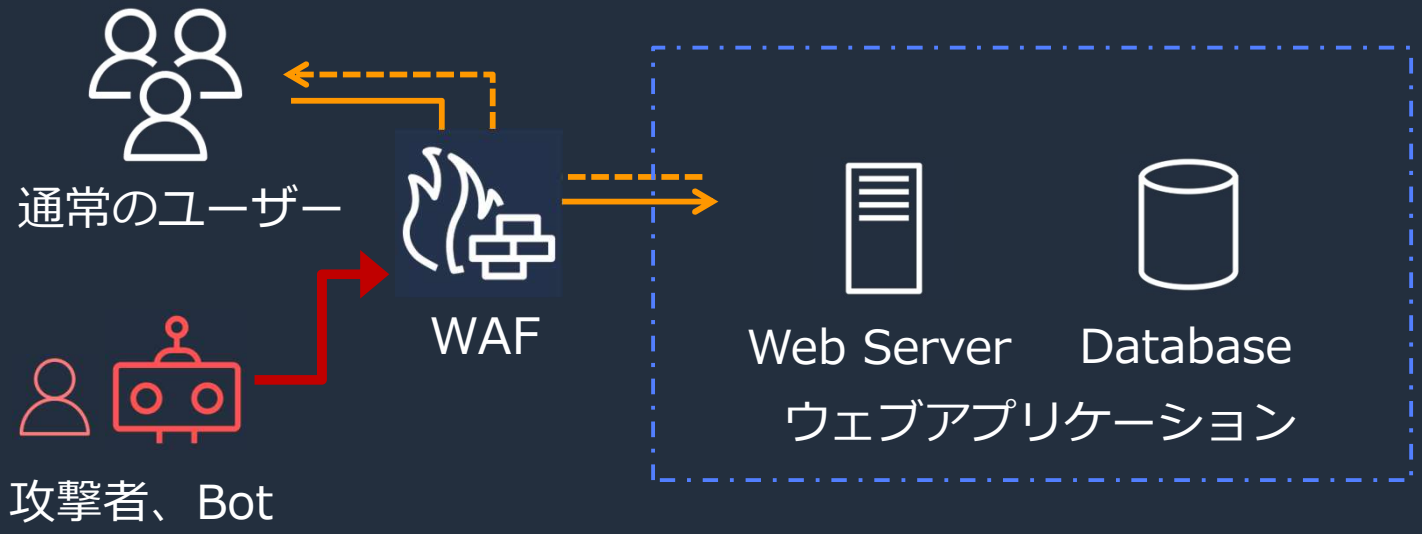
アプリケーションへの影響

- データの盗難
- 認証情報の漏洩
- スパム/フェイクレビュー
- 企業ブランドへの影響
- 財務上の影響

Web Application Firewall (WAF)

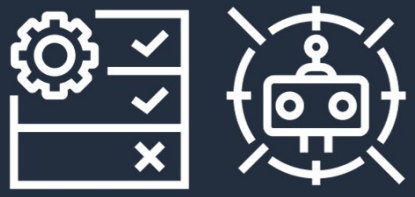
ウェブアプリケーションの通信内容を検査し、不正なアクセスを遮断するルールセットを持つセキュリティ対策ツール

脆弱性を悪用した攻撃等から、ウェブアプリケーションを保護することが目的



AWS WAF が提供する機能

悪意あるリクエストのブロック



- SQL インジェクション
- クロスサイトスクリプト
- AWS またはパートナーのマネージドルール
- Bot Control
- Account Takeover Prevention

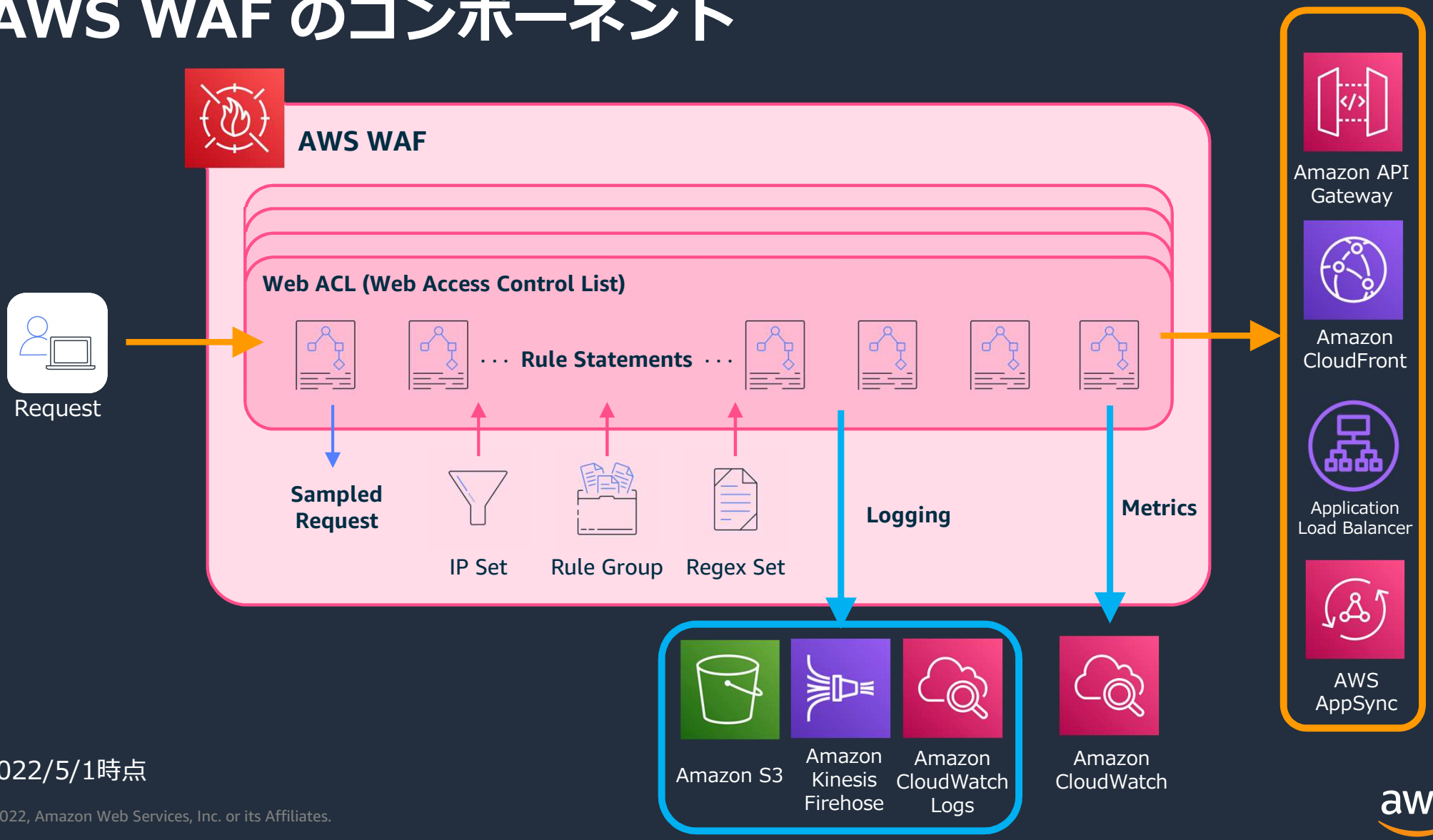
カスタムルールに基づいた Web トラフィックのフィルタ

- Rate-based rules
- IP & Geo-IP filters
- 正規表現パターン、文字列
- サイズ制限
- アクション：許可/拒否
- Label

モニタリングとチューニング

- Amazon CloudWatch
- メトリクス / アラーム
- サンプルログ
- Full logs
- カウントアクションモード（検知モード）

AWS WAF のコンポーネント



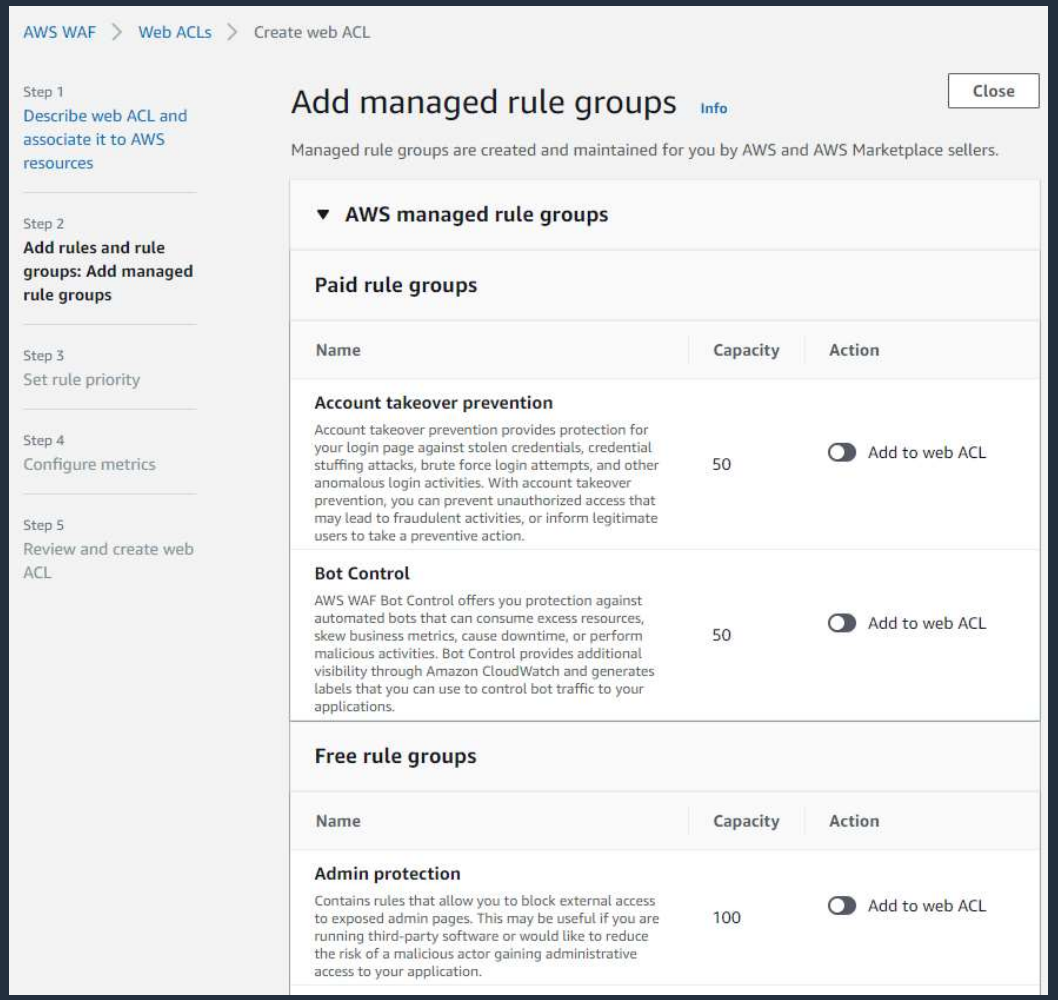
2022/5/1時点

Managed Rule Groups とは

ウェブアプリケーションに利用可能な事前構成済みのルールセット

- 様々な脅威、リスクの高い脆弱性を悪用する攻撃手法に幅広く対応
- 脅威インテリジェンスチームによるルールの追加・メンテナンスを実施
- ユースケース別に無料で使えるルールも提供

オプションで Bot 対策や不正ログイン対策に有効なルールを提供

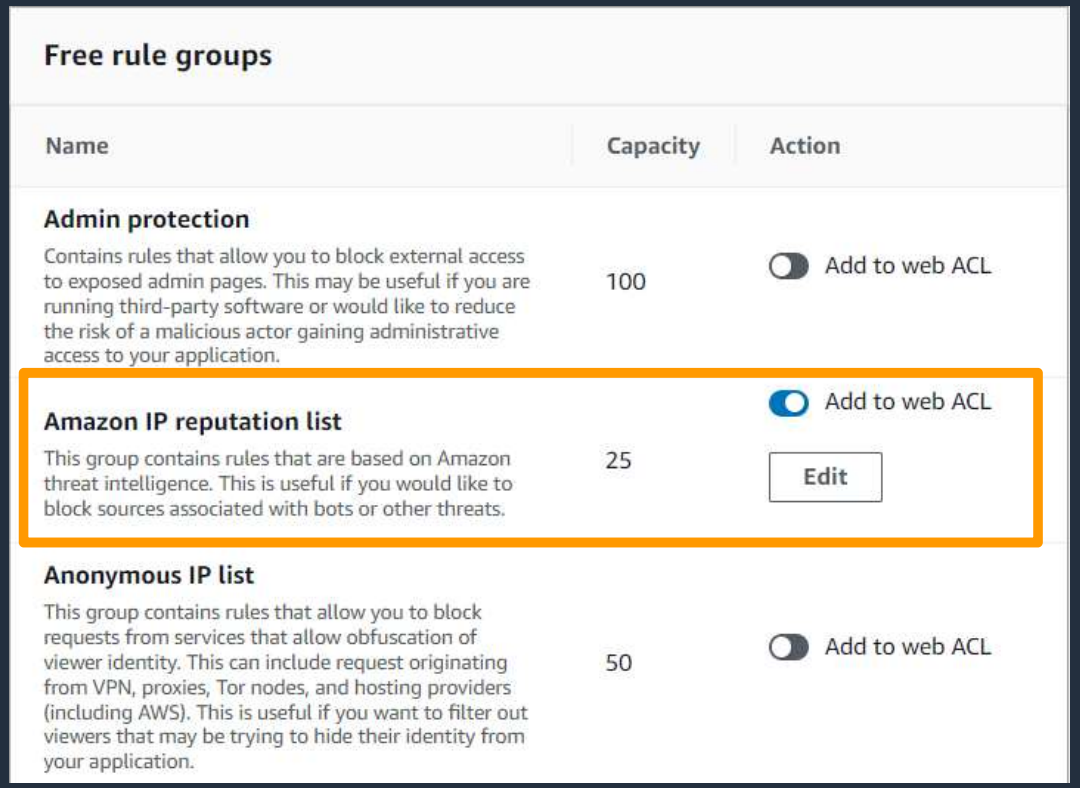


※WAF のルールの運用方法については
「AWS Managed Rules for AWS WAF の活用」をご参照ください

従来のボット対策: AWS WAF

Managed Rule Groups の Amazon IP reputation list は脅威インテリジェンスチームがアップデートする IP のリスト

アクセス元の送信元 IP アドレスから 匿名プロキシ、Bot IP などをカウントまたはブロック



AWS Marketplace Managed Rules for AWS WAF

aws

ボット対策における代表的なパートナー

aws

2. AWS WAF Bot Control

AWS WAF Bot Control

Bot と判断されるトラフィックを検知、アクションを行う

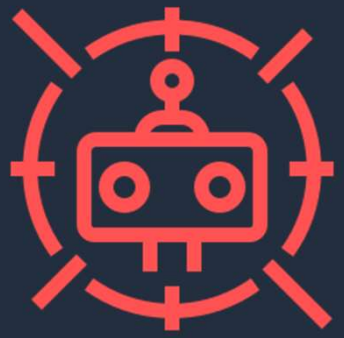
- リクエストの特徴から、Bot の種別を表すラベルを追加
- ラベル内にカテゴリと特徴（シグナル）を表す情報を付加

WAF ユーザーは Bot Control を有効化する前に一定の可視性が得られる

- 事前にトラフィックの状況を確認、利用を検討することができる

ユースケース

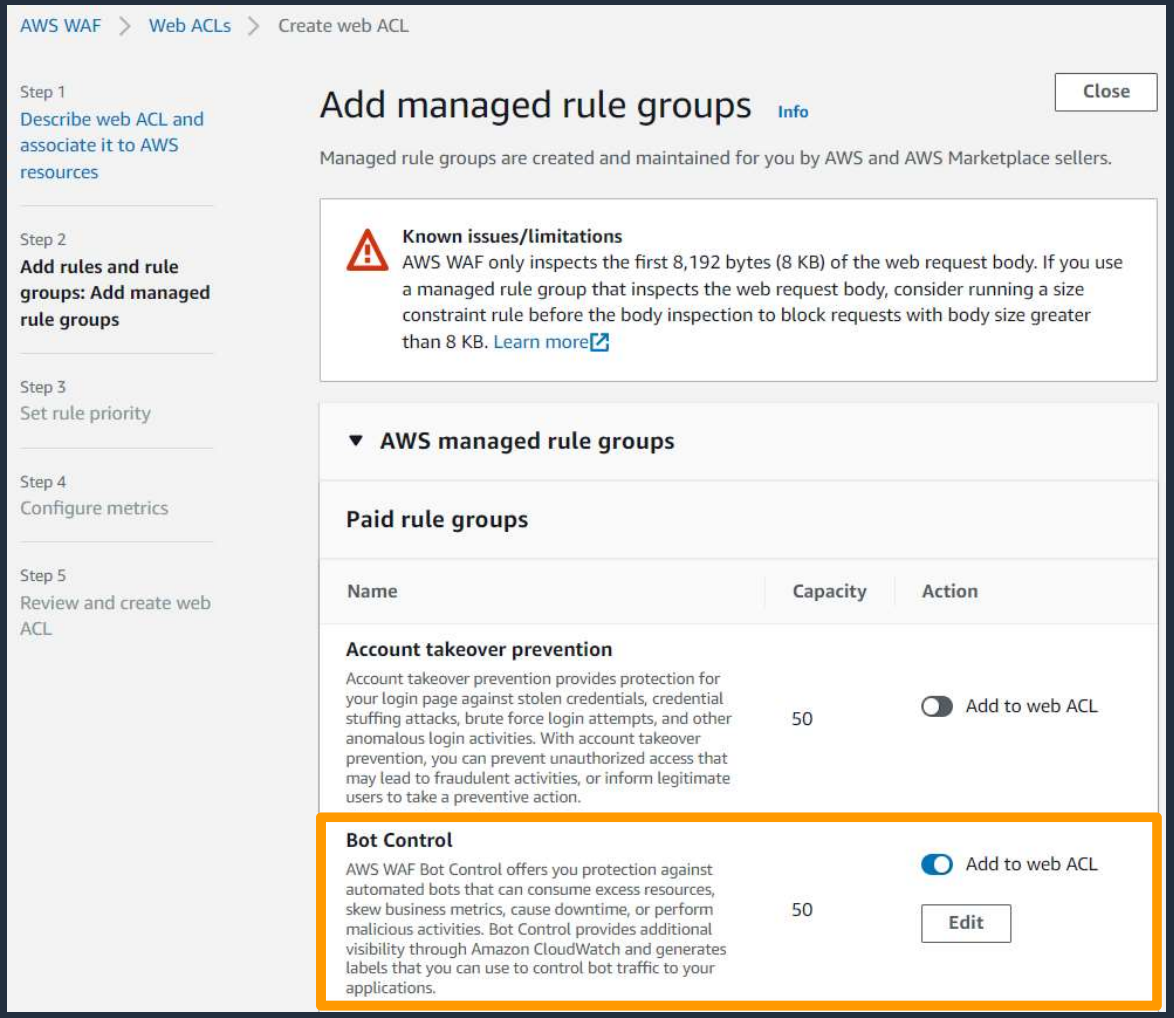
- Bot の種類を検知して、不要なトラフィックを排除する
- 自動化された Bot に対し、効果の高い緩和機能を適用する
- Bot トラフィックを可視化して把握する



AWS WAF Bot Control
https://aws.amazon.com/waf/features/bot-control/

Managed Rule Group: Bot Control

- WebACL へルールグループを追加
- WebACL Capacity Unit (WCU) 50 が必要
- カウントアクションモードでの利用開始を推奨
- スコープダウンステートメントで検査する範囲を限定可能



ラベル機能

リクエストに対し AWS WAF で追加するメタデータ

- Bot Control に関連するラベルを提供
- ラベルの値により、後続のルールで柔軟なアクションが可能
- CloudWatch メトリクスやログに追加される

ユースケース

- 特定のトラフィックをルールから除外する
- ルールに該当した内容を記録し、別のルールで処理する
  例: Bot の種類によって別のアクションを行う
- メトリクスの収集や可視性を提供する

Bot Control とラベル

- bot:category: Bot のタイプ
  例）search_engine, content_fetcher など
- bot:name: Bot の名前
  例）slurp, googlebot, pocket_parser など
- bot:verified: 検証済の Bot かどうか
- signal: Bot の振る舞い
  例）non_browser_user_agent など

Bot Control が生成したラベルをマッチ条件に利用することで、ユーザー独自のラベリングも可能

Bot Category
advertising
archiver
chatbot
content_fetcher
http_library
link_checker
miscellaneous
monitoring
scraper
security
seo
social_media
tools
bot_signals

etc..

AWS WAF Bot Control ルールグループ
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/aws-managed-rule-groups-bot.html

Verified bots

Verified bot は多くの場合、アプリケーションに対して危険性が少なく、用途がはっきりしているものに分類される

- 検索エンジンやソーシャルメディアのクローラー等利用されている IP, DNS, AS 番号等から総合的に判断
- Velified bot はデフォルトでブロックしないカテゴリーになっているが、ラベルを利用して後続のルールでブロックする事も可能
- bot:verified, bot:name:<name> のラベルを生成
- Verified の場合 signal: ラベルは生成されない

Bot Category	Bot Name
search_engine	petalbot
search_engine	googlebot
search_engine	bingbot
search_engine	yandexbot
search_engine	applebot
search_engine	duckduckbot
search_engine	yahoo
search_engine	baidu
search_engine	sogou
social_media	pinterest
social_media	twitter
social_media	linkedin
social_media	telegram

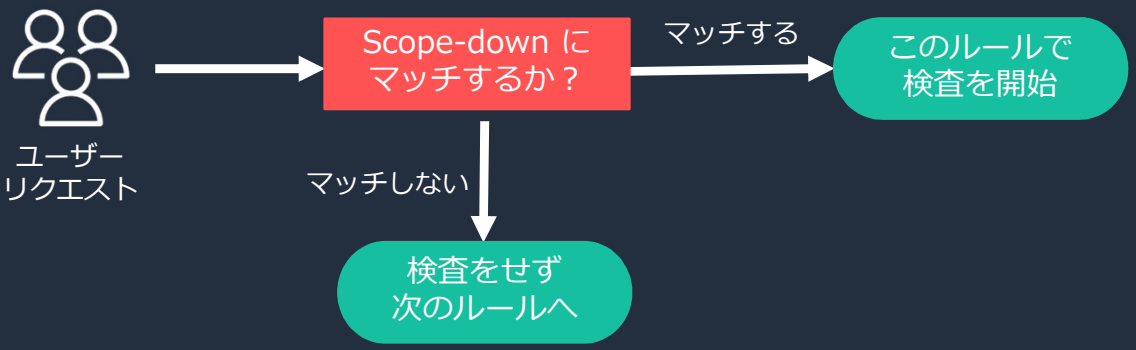
etc..

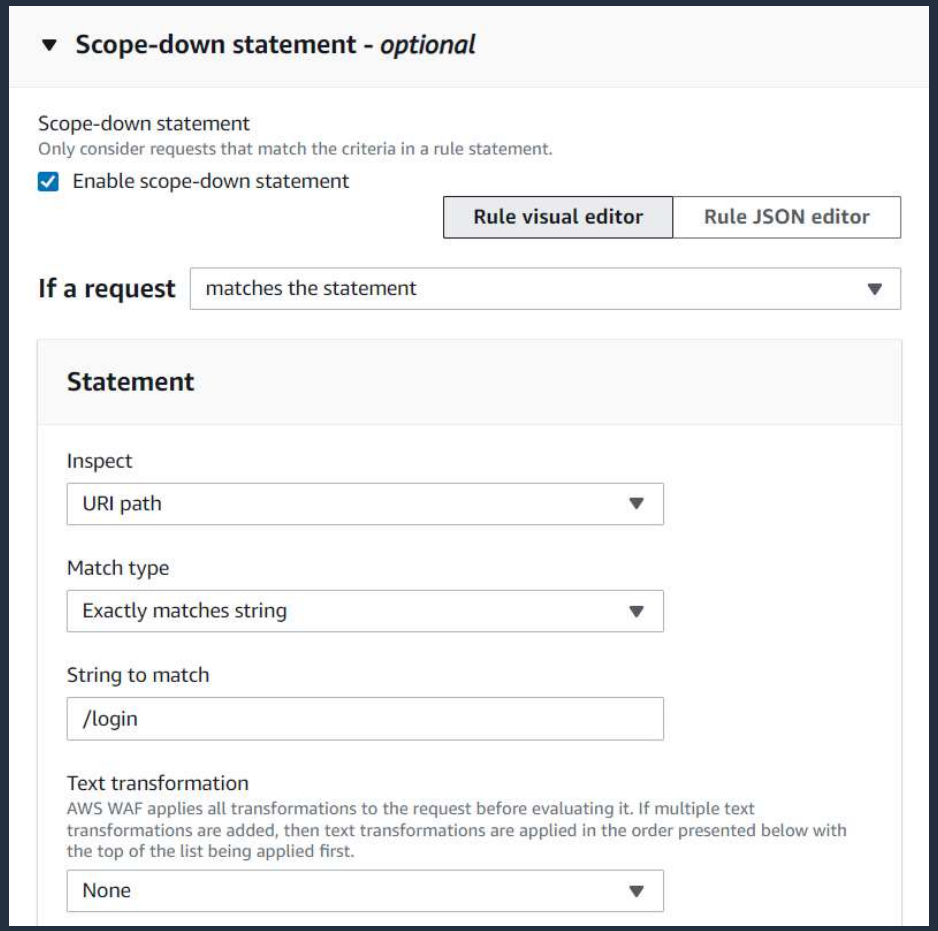
aws

スコープダウンステートメント

- ルールの適用範囲を限定する機能を提供（対象を絞り込む）
- 他の AWS Managed Rule にも適用可能

右の例では /login のパスに完全一致するリクエストがルールの検査対象となる

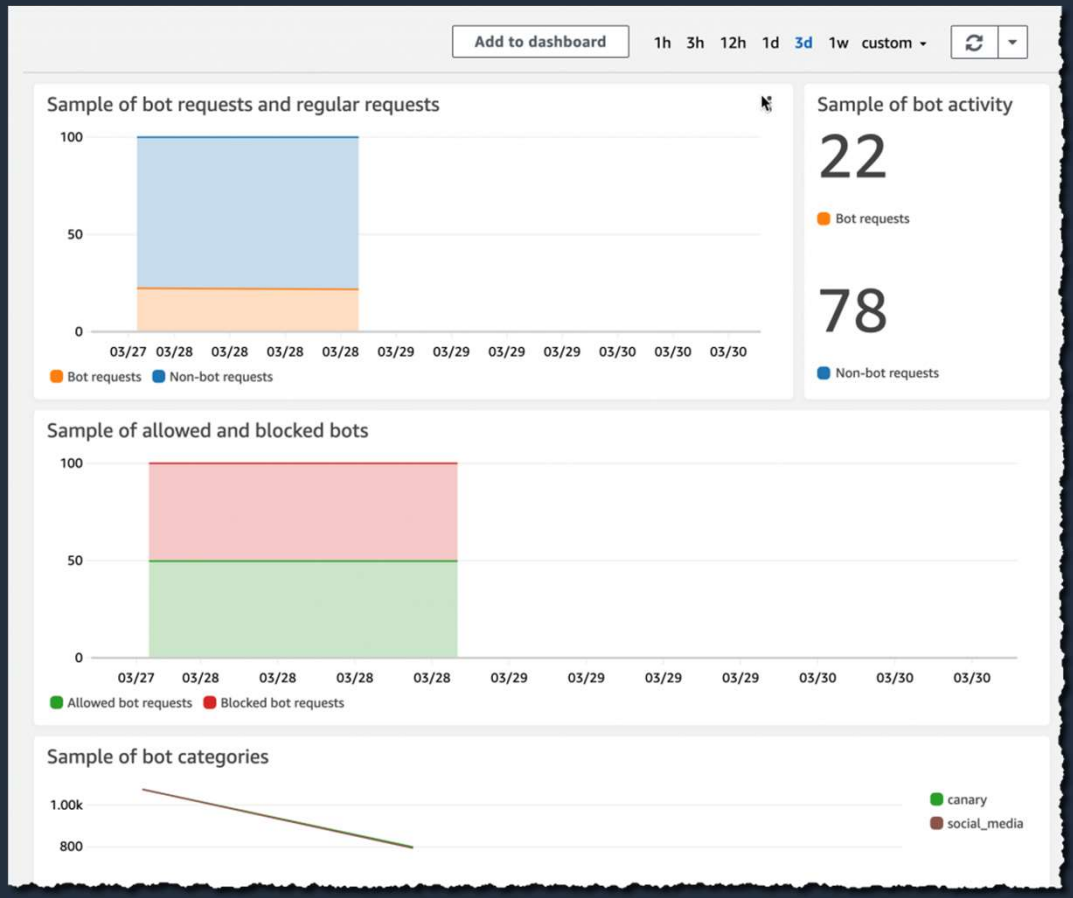




※ If a request match the statement の場合

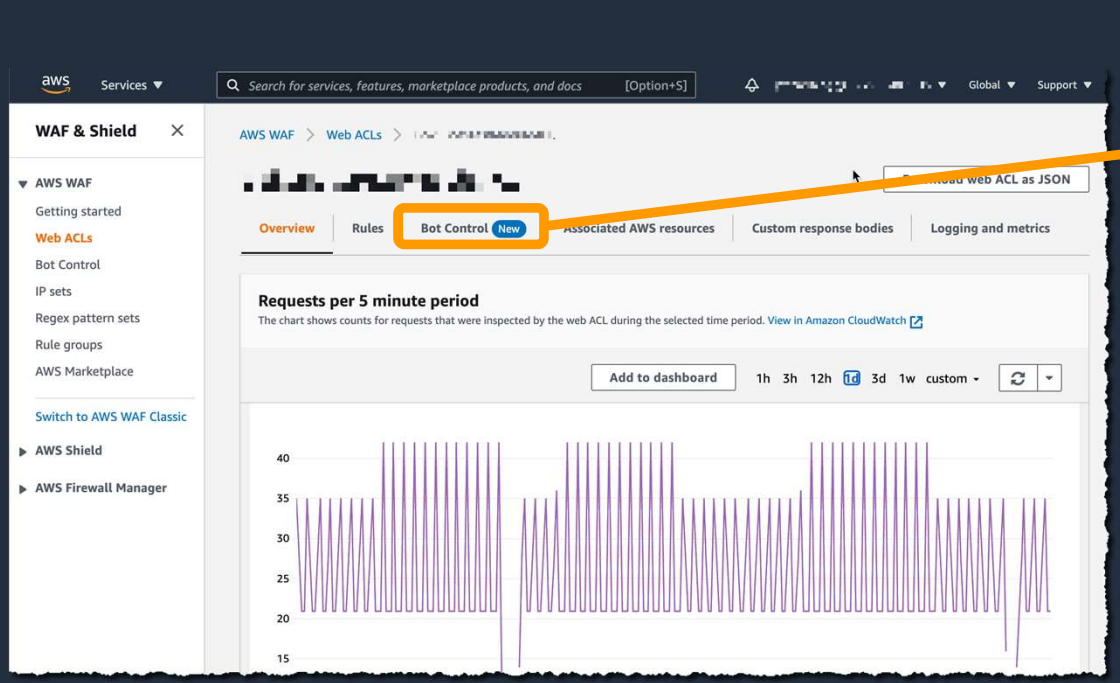
Bot Control レポート（無料）

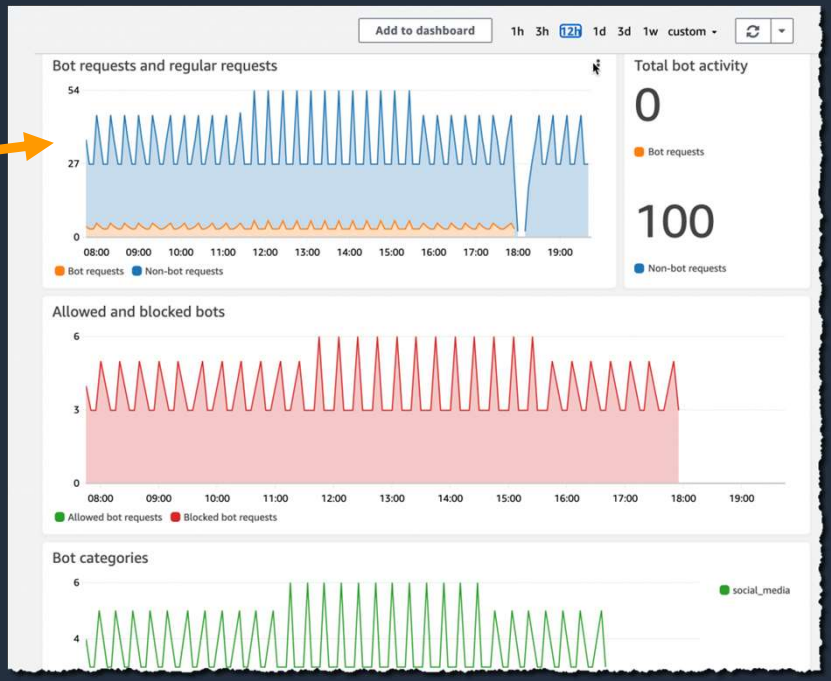
AWS WAF をご利用中のお客様は Bot Control を適用する前にダッシュボードから Bot トラフィックの概要が参照可能



Bot Control レポート

Bot Control を適用すると、詳細なレポートを参照可能





Bot Control と組み合わせて便利な機能

カスタムレスポンス

例）異なるレスポンスコードやページを返すことによって Bot に対応

リクエストヘッダーの追加

例）WAF の追加したヘッダーをオリジンで検査して、異なるレスポンスを返却

ログフィルタリング

例）ブロックされたリクエストのみログを保存
Kinesis、CloudWatch、S3 へ転送するログやストレージコストの削減

カスタムレスポンス

ルールに該当した場合に、クライアントに対して直接任意のレスポンスを返すことができる機能

- 従来は HTTP 403 Forbidden のみ

カスタマイズできる内容

- Response code: 3xx,4xx,5xx を応答可能
- Response Headers
- Response body: エラーメッセージを出力可能

AWS WAF のカスタマイズされたウェブリクエストとレスポンス
https://docs.aws.amazon.com/waf/latest/developerguide/waf-custom-request-response.html

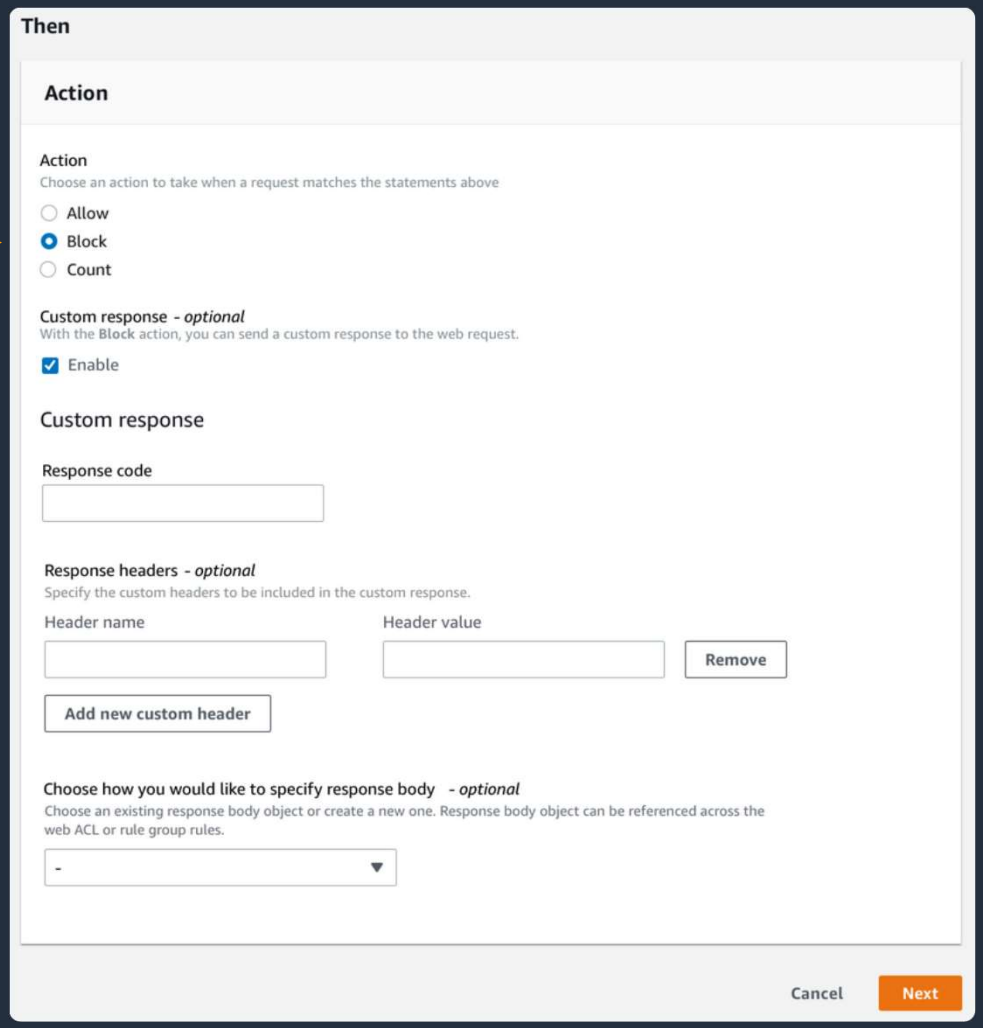
aws

カスタムレスポンスの設定

Block アクションに
対して設定可能

レスポンスコード
ヘッダーなどを設定

レスポンスボディは
同じ WebACL の他の
ルールでも再利用可能



AWS WAF のクォータ
https://docs.aws.amazon.com/waf/latest/developerguide/limits.html

リクエストヘッダーの追加

WAF ルールで許可した場合に HTTP ヘッダーを追加する機能

- オリジン側で WAF ルールに合致したリクエストか判別できる
- ヘッダーでオリジンに情報を伝え、レスポンスを変えることが可能

- オリジナルのリクエストは改変できない
- ヘッダーの追加のみ
- “x-amzn-waf-” の Prefix から始まる

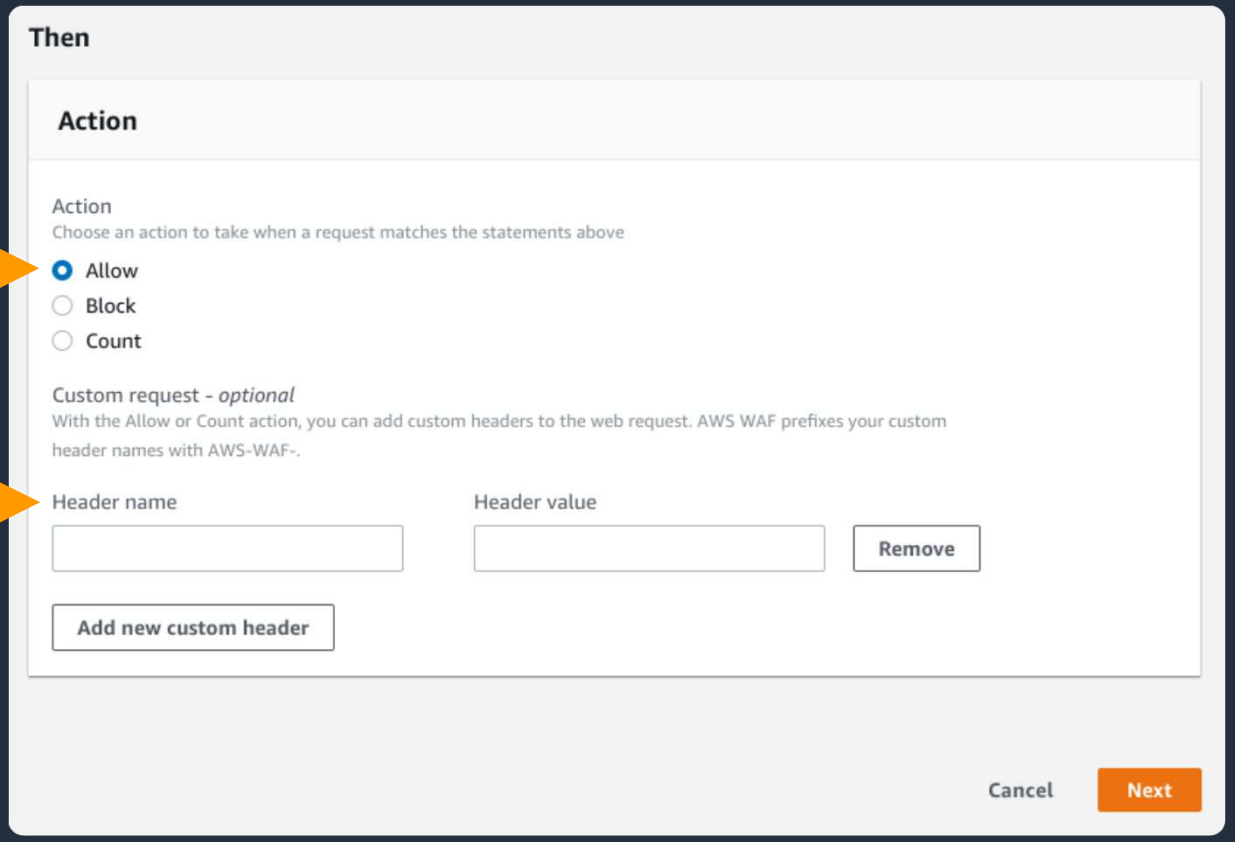
許可、カウント、および CAPTCHA アクションのカスタムリクエストヘッダーの挿入
https://docs.aws.amazon.com/waf/latest/developerguide/customizing-the-incoming-request.html

リクエストヘッダーの追加

Count または Allow アクションに対して設定可能

追加するヘッダーを設定

WebACL のデフォルトアクションとしても設定可能

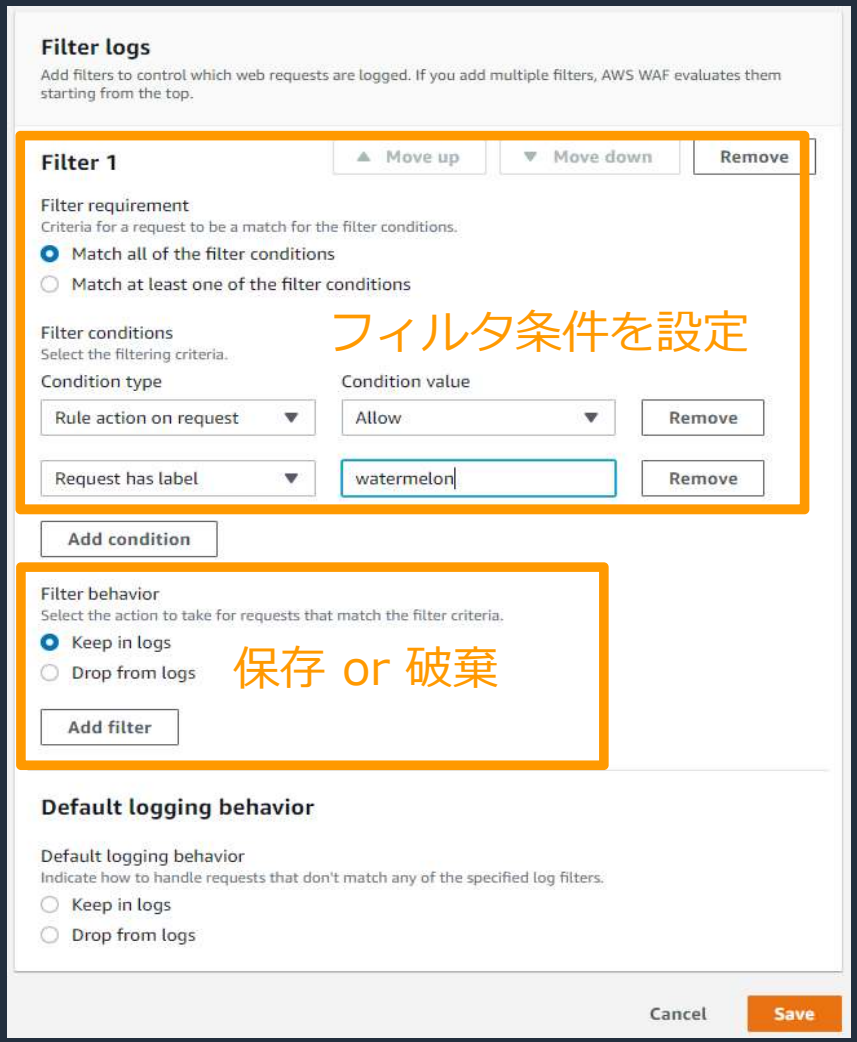


ログフィルタリング

ルールによって取られたアクション、
または設定されたラベルでログを
フィルタリング

フィルタ条件は上から順番に評価

必要なログのみをフィルタリングして
Kinesis やストレージコストを最適化



ウェブ ACL トラフィックのログ記録
https://docs.aws.amazon.com/waf/latest/developerguide/logging.html

3. Account Takeover Prevention (ATP)

Account Takeover Prevention (ATP)

不正アクセスからログインページを保護

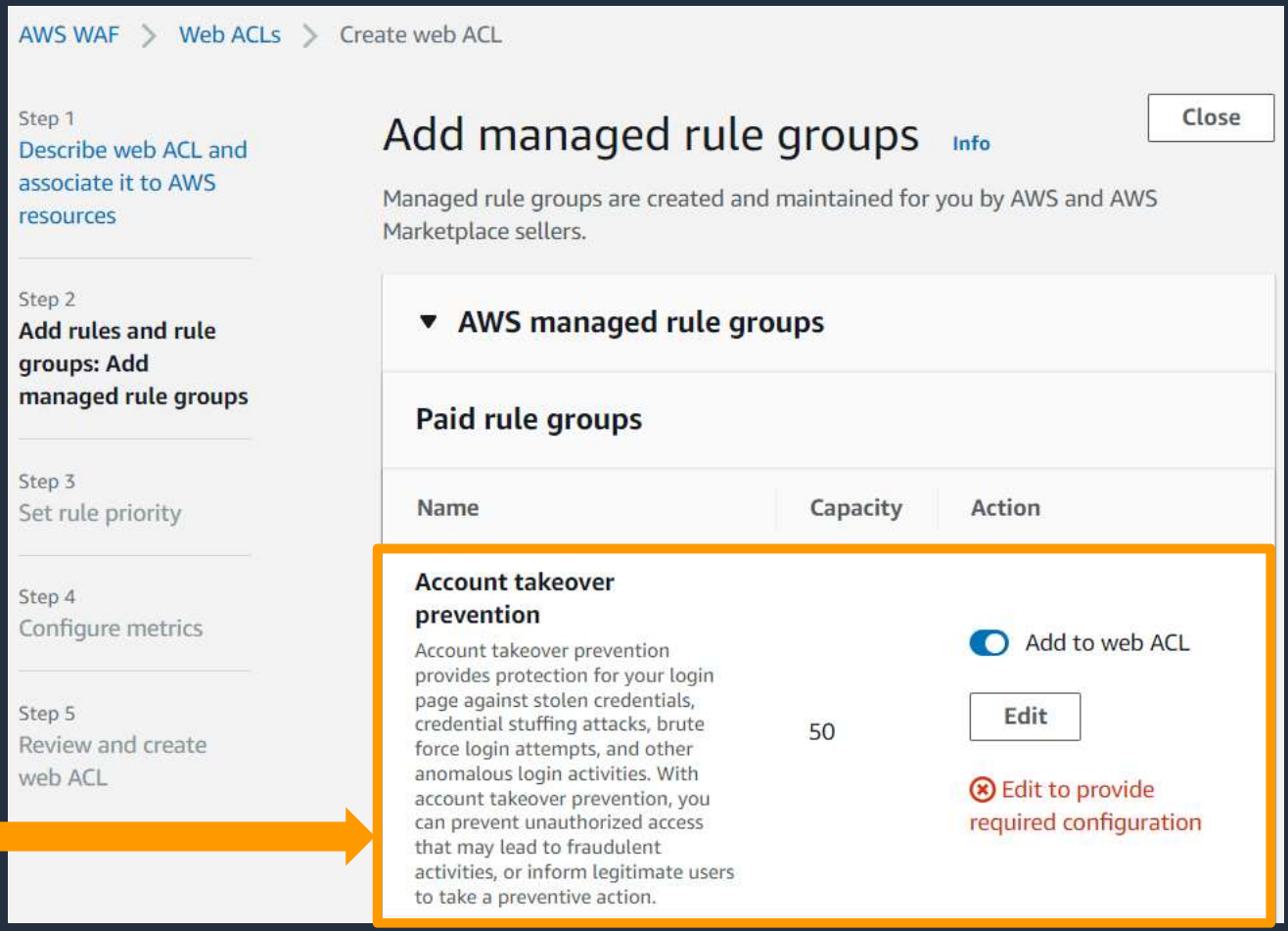
- 盗まれた認証情報を利用したログイン試行を可視化及び制御
  - クレデンシャルスタッフィング攻撃
  - ブルートフォース攻撃
  - その他の異常なログイン試行

- POST されたデータを盗まれたクレデンシャルのデータベースと照合
- ATP に特化したラベルを提供
- アプリケーション統合 SDK で Bot の検知能力を向上（オプション）

AWS WAF Fraud Control アカウント乗っ取り防止 (ATP)
https://docs.aws.amazon.com/waf/latest/developerguide/waf-atp.html

Managed Rule Group: Account takeover prevention

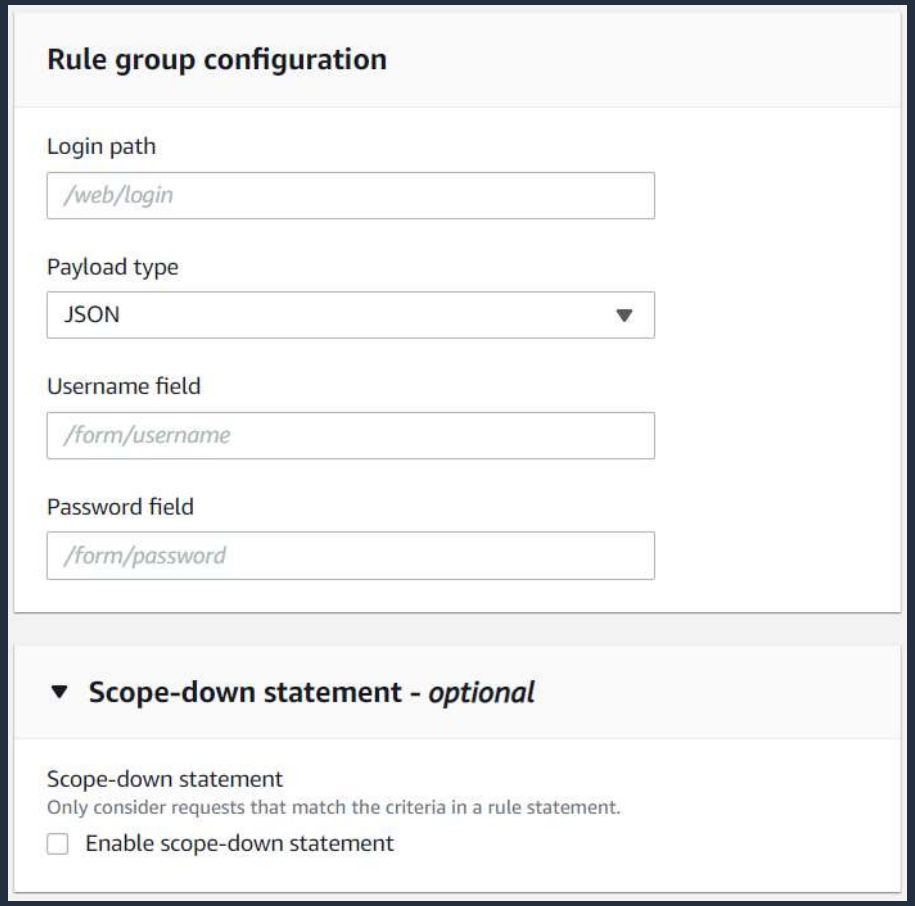
- Web ACL へルールグループを追加後、Edit ボタンから追加の設定が必要
- Web ACL Capacity Unit (WCU) 50 が必要
- カウントアクションモードでの利用開始を推奨



Rule Group の設定が必要

Managed Rule Group: Account takeover prevention

- ログインページのパスを設定
  例) URL が https://example.com/web/login の場合は /web/login を指定
- ATP は HTTP POST リクエストのみを検査
- JSON、FORM_ENCODED からペイロードタイプを選択
- ユーザーネームとパスワードのフィールド名を入力
- スコープダウンステートメントで検査する範囲を限定可能

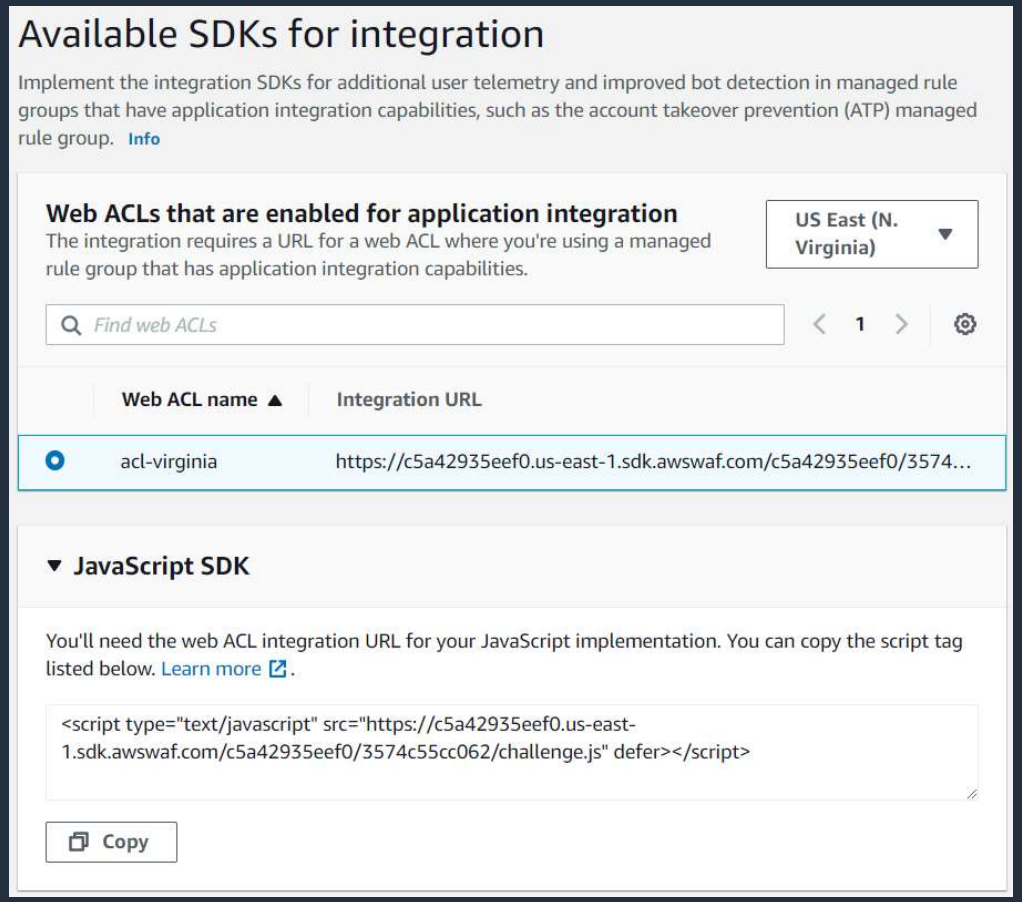


ATP マネージドルールグループの使用
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/waf-atp-rg-using.html

アプリケーション統合 SDK（オプション）

- トークン認証を管理、有効なトークンを取得した後にログインを許可
- ログインが実際のユーザーか Bot か判断する能力を向上
- JavaScript, iOS, Android をサポート

※モバイル用 SDK（iOS, Android）は AWS 担当者までお問い合わせください



AWS WAF クライアントアプリケーション統合
https://docs.aws.amazon.com/ja_jp/waf/latest/developerguide/waf-application-integration.html

Bot Control と ATP の使い分け

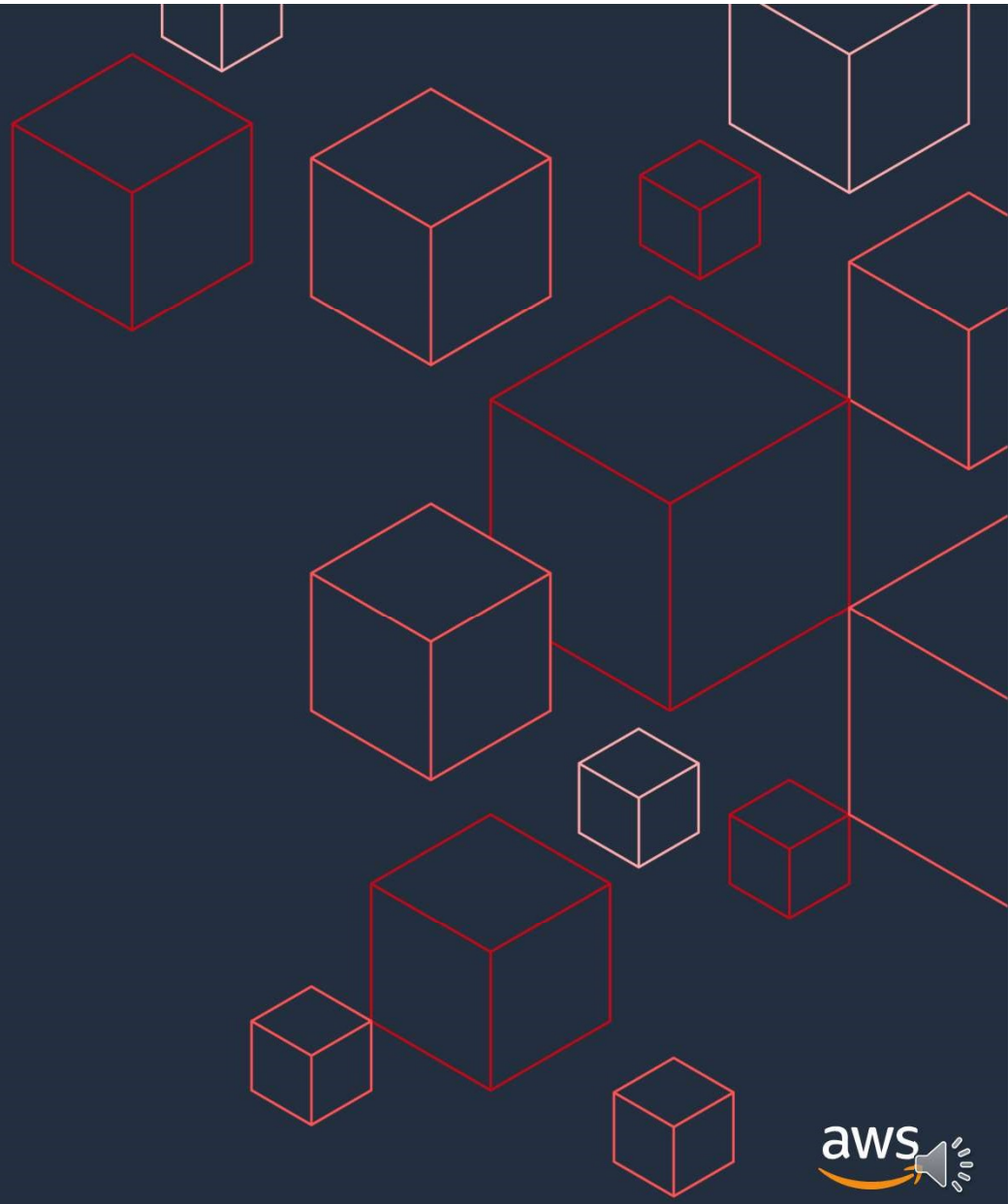
- Bot Control は一般的で広範な Bot トラフィックを可視化・制御
  - 既知の Bot シグネチャと照合
  - スクレーパー、スキャナー、クローラーの検出・分類 など

- ATP はログインページに対する不正なアクセスを可視化・保護
  - クレデンシャルスタッフィング攻撃対策
  - ブルートフォース攻撃対策 など

- Bot Control / ATP それぞれの特徴に合わせて適用箇所を検討
- 同じ WebACL で両方のルールグループを利用することも可能

FAQ: AWS WAF 不正対策 - Account Takeover Prevention
https://aws.amazon.com/jp/waf/faqs/#AWS_WAF_Fraud_Control_-_Account_Takeover_Prevention

4.CAPTCHA



CAPTCHA

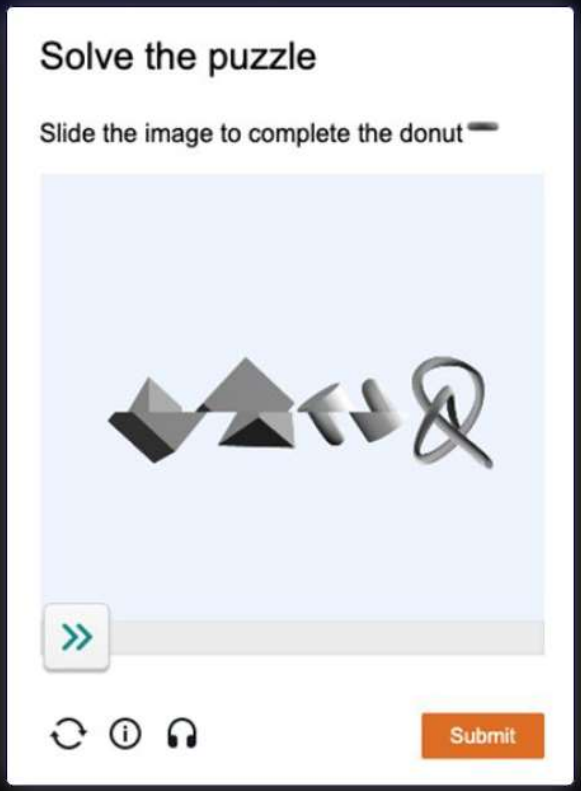
ユーザーにチャレンジを正常に完了することを要求して、
望ましくない Bot のトラフィックをブロックすることが可能

想定されるユースケース

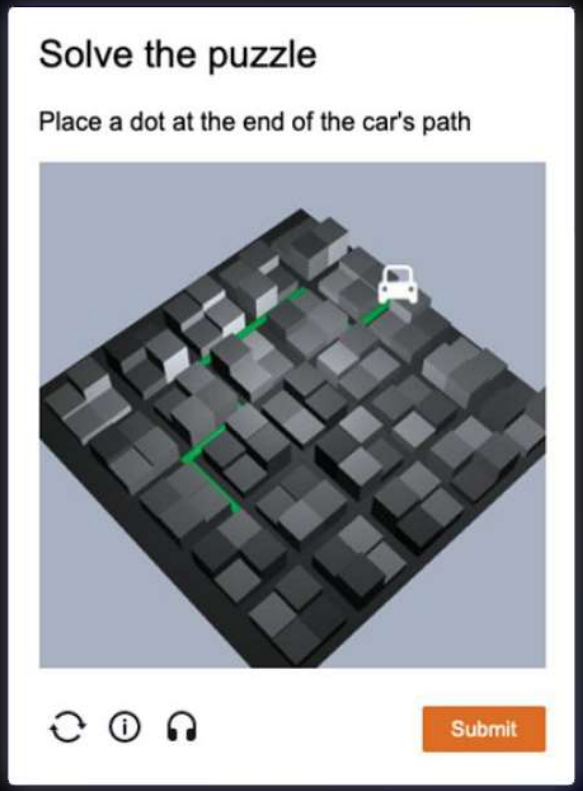
- ログイン、検索、フォーム送信などのリソースに適用
- クレデンシャルスタッフィング、ウェブスクレイピング、スパム対策に有効
- 他のルールをすり抜ける、巧妙な攻撃への対策として

CAPTCHA で提供されるパズル

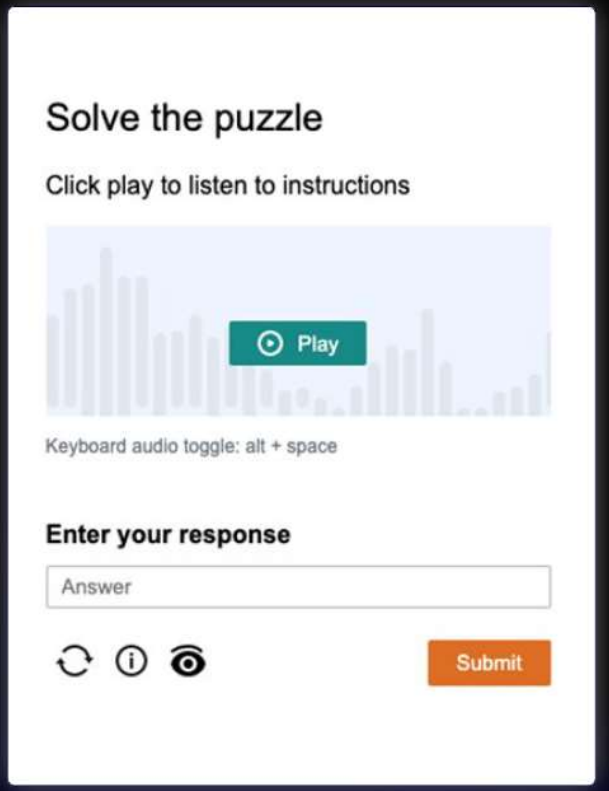
図形を完成させる



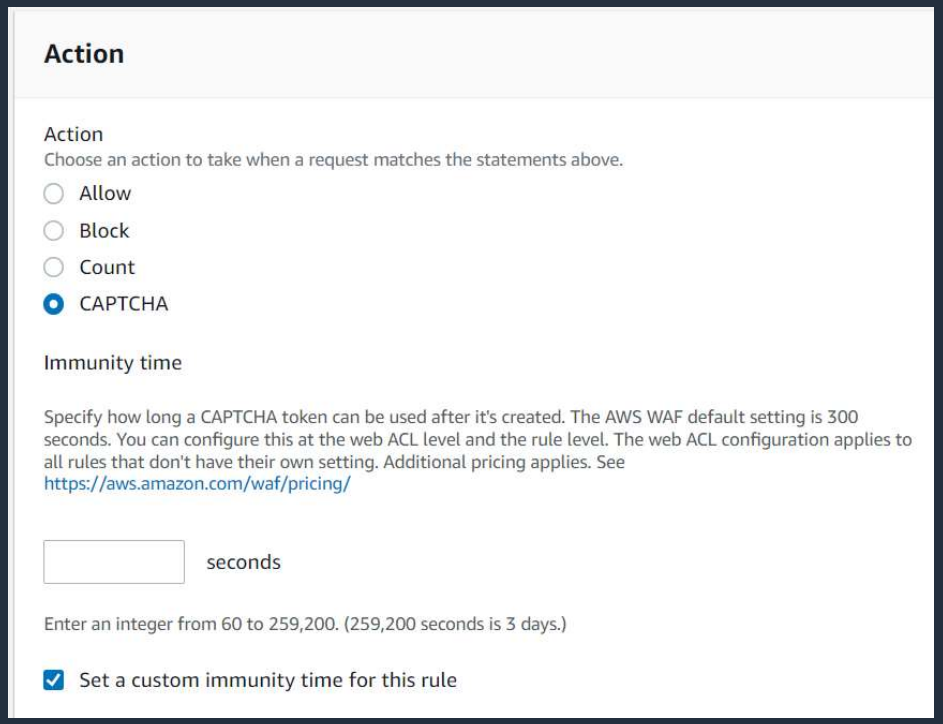
ルートをたどる



聞こえた音声を答える



設定の流れ

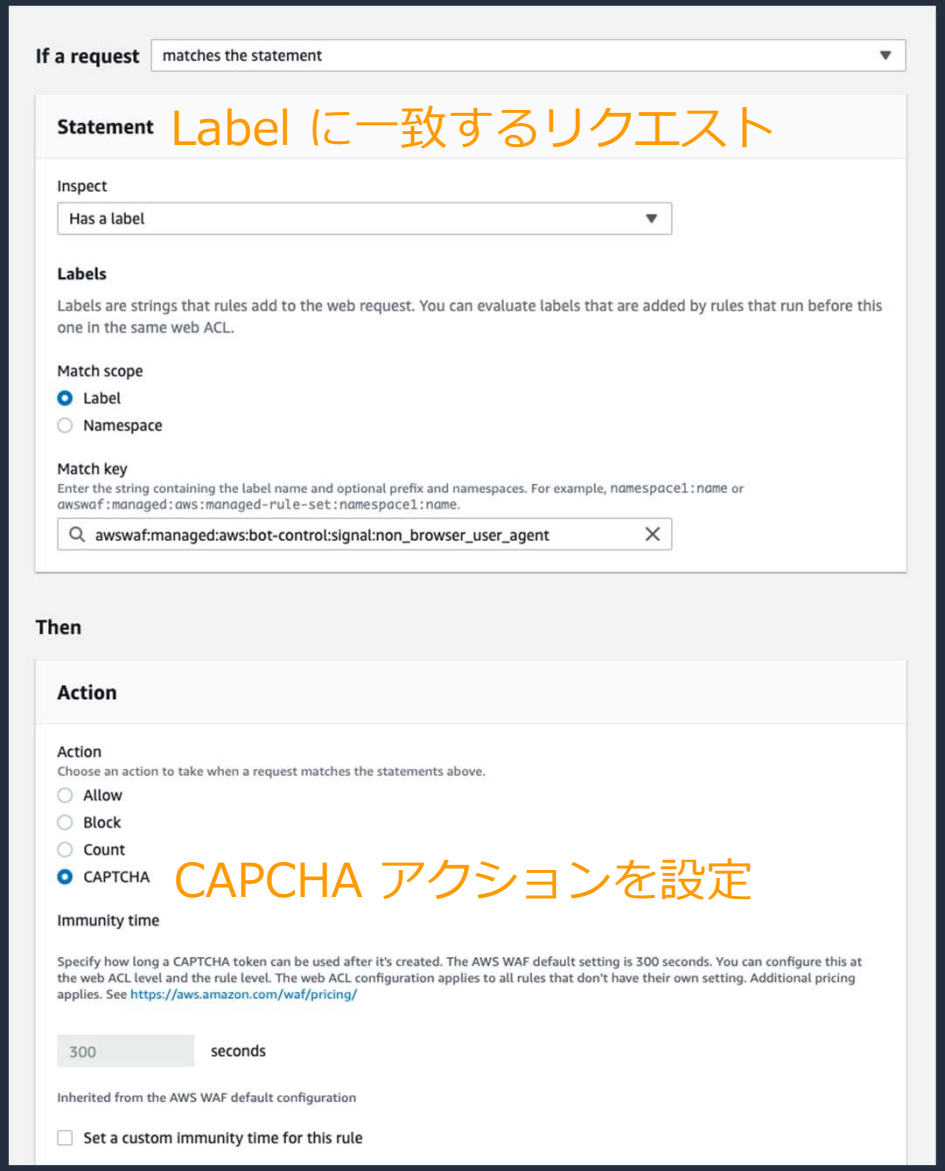


- カスタムルール内の Action にて設定
- 対象のリソースを Statement で限定させる
- Action として CAPTCHA を選択
- Immunity time (CAPTCHA トークンの有効期限) を設定
  - デフォルト 300秒
  - 60秒～3日間で設定可能
  - Web ACL 全体でも設定可能

ラベル機能との組み合わせ

- Bot Control のマネージドルールを Count に設定
- 後続のカスタムルールで特定ラベルの付いたトラフィックをマッチ
- Bot と疑われるリクエストに対し CAPCHA チャレンジを応答

右の例では non_browser-user-agent のラベルが付加されたリクエストに CAPCHA を応答



5.料金

AWS WAF の料金 2022/5/1時点

・基本料金として 100 万リクエスト毎に 0.6USD の料金と
月額で WebACL数 x 5USD、ルール数 x 1USD の料金（時間で按分）
・Shield Advanced 保護対象の WAF は基本料金部分は無料

+オプション	利用料金
Bot Control 検査するリクエスト数で変動	**1USD / 100万リクエスト +10USD/月（時間で按分）** ※毎月 1,000万リクエスト検査分は無料
Account Takeover Prevention (ATP) 分析するログイン試行数で変動	**1USD / 1,000ログイン試行 +10USD/月（時間で按分）** ※毎月 1万ログイン試行分は無料
CAPTCHA 分析するチャレンジ試行数で変動	**0.4USD / 1,000チャレンジ試行**

・AWS WAF パートナールールの費用は上記以外に発生します

AWS WAF の料金
https://aws.amazon.com/jp/waf/pricing/

6.まとめ

まとめ

- **AWS WAF で Bot トラフィックを管理**
- **マネージドルールでウェブサイトの運用負荷を軽減**
  - Bot Control： 一般的な Bot トラフィックを識別・制御
  - ATP： 不正アクセスからログインページを保護
- **CAPTCHA アクションは他のルールをすり抜ける攻撃の対策に**
- **ラベルやスコープダウンステートメントを活用**
  - Bot の種別に合わせて、柔軟なアクションが可能
  - 適用箇所を調整してコスト最適化

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料のAWSサポート窓口へ
  お問い合わせください
  - https://aws.amazon.com/jp/premiumsupport/
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
  お問い合わせください（マネジメントコンソールへのログインが必要です）
  - https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service
- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWSの日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWSのハンズオン資料の場所「AWS ハンズオン」で検索

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS 個別相談会

- 毎週「AWS 個別相談会」を実施中
  - AWSのソリューションアーキテクト（SA）に対策などを相談することも可能
- 申込みは下記のURLから
  - https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html

AWS 個別相談会 で[検索]

ご視聴ありがとうございました