개발자 가이드

AWS WAF, AWS Firewall Manager, 및 AWS Shield Advanced

AWS WAF, AWS Firewall Manager, 및 AWS Shield Advanced: 개발자 가이드

Table of Contents

AWS WAF, AWS Shield Advanced; 및 란 AWS Firewall Manager무엇입니까?

AWS WAF,AWS Shield, 를 AWS Firewall Manager 함께 사용하여 포괄적인 보안 솔루션을 만들 수 있습니다. AWS WAF 최종 사용자가 애플리케이션에 보내는 웹 요청을 모니터링하고 콘텐츠에 대한 액세스를 제어하는 데 사용할 수 있는 웹 애플리케이션 방화벽입니다. Shield Advanced는 네트워크 및 전송 계층 (계층 3 및 4) 과 애플리케이션 계층 (계층 7) 에서 AWS 리소스에 대한 분산 서비스 거부 (DDoS) 공격으로부터 보호합니다. AWS Firewall Manager 새 리소스가 추가되는 경우에도 계정 AWS WAF 및 리소스 전반에 걸쳐 Shield Advanced와 같은 보호 기능을 관리할 수 있습니다.

주제

이게 AWS WAF뭐예요?

AWS WAF 보호된 웹 애플리케이션 리소스로 전달되는 HTTP 및 HTTPS 요청을 모니터링할 수 있는 웹 애플리케이션 방화벽입니다. 다음 리소스 유형을 보호할 수 있습니다.

- 아마존 CloudFront 디스트리뷰션
- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 사용자 풀
- AWS App Runner 서비스
- AWS 검증된 액세스 인스턴스

AWS WAF 콘텐츠에 대한 액세스를 제어할 수 있습니다. 요청이 허용되는 IP 주소나 쿼리 문자열의 값으로부터 지정하는 조건 등 지정하는 조건에 따라, 보호된 리소스는 요청된 콘텐츠나 HTTP 403 상태 코드(금지됨), 사용자 지정 응답으로 요청에 응답합니다.

가장 간단한 수준에서 다음 동작 중 하나를 AWS WAF 선택할 수 있습니다.

- 지정한 요청을 제외한 모든 요청 허용 - Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner AWS 또는 Verified Access에서 공개 웹 사이트의 콘텐츠를 제공하되 공격자의 요청도 차단하려는 경우에 유용합니다.
- 지정한 항목을 제외하고 모든 요청을 차단 - 이 동작은 웹 사이트를 검색하기 위해 사용하는 IP 주소와 같은 웹 요청의 속성을 통해 사용자를 즉시 식별할 수 있는 제한된 웹 사이트에 콘텐츠를 서비스하려는 경우에 유용합니다.
- 기준에 맞는 요청 수 계산 — 처리 방법을 수정하지 않고도 Count 작업을 사용하여 웹 트래픽을 추적할 수 있습니다. 이를 일반 모니터링에 사용할 수 있으며 새 웹 요청 처리 규칙을 테스트하는 데도 사용할 수 있습니다. 웹 요청의 새 속성을 기반으로 요청을 허용하거나 차단하려는 경우 먼저 해당 속성과 일치하는 요청을 AWS WAF 계산하도록 구성할 수 있습니다. 이렇게 하면 일치 요청을 허용하거나 차단하도록 규칙을 전환하기 전에 새 구성 설정을 확인할 수 있습니다.
- 기준에 맞는 요청에 대해 CAPTCHA 또는 챌린지 검사 실행 — 요청에 대해 CAPTCHA 및 자동 챌린지 제어를 구현하여 보호된 리소스로 향하는 봇 트래픽을 줄일 수 있습니다.

를 사용하면 다음과 AWS WAF 같은 여러 가지 이점이 있습니다.

- 지정하는 기준을 사용하여 웹 공격에 대한 추가 보호를 제공합니다. 다음과 같은 웹 요청의 특성을 사용하여 기준을 정의할 수 있습니다.
  - 요청이 시작되는 IP 주소
  - 요청이 시작되는 국가
  - 요청 헤더 값
  - 요청에 나타나는 문자열(특정 문자열 또는 정규식 패턴과 일치하는 문자열)
  - 요청 길이
  - 악성일 가능성이 있는 SQL 코드의 존재(SQL 명령어 주입이라고 알려짐)
  - 악성일 가능성이 있는 스크립트의 존재(교차 사이트 스크립팅이라고 알려짐)
- 지정된 기준을 충족하는 웹 요청을 허용, 차단 또는 계수할 수 있는 규칙. 또는 규칙을 사용하여 지정된 기준을 충족할 뿐만 아니라 1분 또는 5분 내에 지정된 요청 수를 초과하는 웹 요청을 차단하거나 카운트할 수 있습니다.
- 여러 웹 애플리케이션에 재사용할 수 있는 규칙
- AWS 및 AWS Marketplace 판매자의 관리형 규칙 그룹.
- 실시간 지표 및 샘플링된 웹 요청
- AWS WAF API를 사용한 자동 관리.

리소스에 추가되는 보호를 자세히 제어하고 싶다면 AWS WAF 야 말로 탁월한 선택입니다. 에 대한 자세한 내용은 AWS WAF을 참조하십시오AWS WAF.

이게 뭐야 AWS Shield Advanced?

AWS WAF 웹 액세스 제어 목록 (웹 ACL) 을 사용하여 DDoS (분산 서비스 거부) 공격의 영향을 최소화할 수 있습니다. DDoS 공격에 대한 추가 보호를 위해 및 AWS 도 제공합니다. AWS Shield Standard AWS Shield Advanced AWS Shield Standard 이미 지불한 금액 AWS WAF 및 기타 AWS 서비스 외에 추가 비용 없이 자동으로 포함됩니다.

Shield Advanced는 Amazon EC2 인스턴스, Elastic Load Balancing 로드 밸런서, 배포 CloudFront , Route 53 호스팅 영역 및 표준 액셀러레이터에 대한 확장된 DDoS 공격 보호를 제공합니다. AWS Global Accelerator Shield Advanced에는 추가 요금이 부과됩니다. Shield Advanced 옵션 및 기능에는 자동 애플리케이션 계층 DDoS 완화, 고급 이벤트 가시성, Shield Response Team(SRT)의 전담 지원이 포함됩니다. 방문객이 많은 웹 사이트를 소유하고 있거나 빈번하게 DDoS 공격이 이루어지기 쉬운 경우 Shield Advanced가 제공하는 추가 보호 기능을 구입하는 것도 좋습니다. 자세한 내용은 AWS Shield Advanced 기능 및 옵션 및 AWS Shield Advanced 구독 여부 및 추가 보호 적용 여부 결정을 참조하세요.

이게 뭐예요? AWS Firewall Manager

AWS Firewall Manager AWS Shield Advanced Amazon VPC 보안 그룹 및 네트워크 ACL AWS WAF, Amazon Route 53 Resolver DNS 방화벽을 비롯한 다양한 보호를 위해 여러 계정 및 리소스에서 관리 AWS Network Firewall및 유지 관리 작업을 간소화합니다. Firewall Manager를 사용하여 보호 기능을 한 번만 설정하면 새로운 계정과 리소스를 추가할 때도 서비스가 자동으로 계정과 리소스 전체에 보호 기능을 적용합니다.

Firewall Manager에 대한 자세한 내용은 AWS Firewall Manager를 참조하세요.

서비스를 사용하기 위한 계정 설정

이 항목에서는 계정 생성과 같은 사용 AWS WAF준비를 위한 예비 단계에 대해 설명합니다 AWS Shield Advanced. AWS Firewall Manager이러한 예비 항목에 대해서는 요금이 부과되지 않습니다. 사용한 AWS 서비스에 대해서만 요금이 부과됩니다.

주제

가입해 보세요 AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요 AWS 계정 루트 사용자

1. Root user를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자 (콘솔) 에 대한 가상 MFA 디바이스 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM IDentity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

도구 다운로드

에는 AWS WAF AWS Shield Advanced AWS Firewall Manager, 및 용 콘솔이 AWS Management Console 포함되어 있지만 프로그래밍 방식으로 서비스에 액세스하려면 다음을 참조하십시오.

- API 가이드는 서비스가 지원하는 작업을 문서화하고 관련 SDK 및 CLI 설명서에 대한 링크를 제공합니다.
  - AWS WAF API Reference
  - AWS Shield Advanced API Reference
  - AWS Firewall Manager API Reference
- 원시 HTTP 요청 어셈블링과 같은 저수준 세부 정보를 처리하지 않고도 API를 호출하려면 SDK를 사용할 수 있습니다. AWS AWS SDK는 서비스 기능을 캡슐화하는 함수와 데이터 유형을 제공합니다. AWS AWS SDK를 다운로드하고 설치 지침에 액세스하려면 해당 페이지를 참조하십시오.
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  AWS SDK의 전체 목록은 Amazon Web Services용 도구를 참조하십시오.
- AWS Command Line Interface (AWS CLI) 를 사용하여 명령줄에서 여러 AWS 서비스를 제어할 수 있습니다. 또한, 스크립트를 사용하여 명령을 자동화할 수 있습니다. 자세한 정보는 AWS Command Line Interface을 참조하세요.
- AWS Tools for Windows PowerShell 이러한 AWS 서비스를 지원합니다. 자세한 내용은 AWS Tools for PowerShell Cmdlet 참조를 참조하세요.

AWS WAF

AWS WAF 보호된 웹 응용 프로그램 리소스에 전달되는 HTTP (S) 요청을 모니터링할 수 있는 웹 응용 프로그램 방화벽입니다. 다음 리소스 유형을 보호할 수 있습니다.

- 아마존 CloudFront 디스트리뷰션
- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 사용자 풀
- AWS App Runner 서비스
- AWS 검증된 액세스 인스턴스

AWS WAF 콘텐츠에 대한 액세스를 제어할 수 있습니다. 요청이 허용되는 IP 주소나 쿼리 문자열의 값으로부터 지정하는 조건 등 지정하는 기준에 따라, 보호된 리소스와 연결된 서비스는 요청된 콘텐츠나 HTTP 403 상태 코드(금지됨) 또는 사용자 지정 응답으로 요청에 응답합니다.

> **Note**
>
> 또한 Amazon Elastic Container Service (Amazon ECS) 컨테이너에서 호스팅되는 애플리케이션을 보호하는 AWS WAF 데 사용할 수 있습니다. Amazon ECS는 클러스터에서 Docker 컨테이너를 손쉽게 실행, 중지 및 관리할 수 있게 해주는 컨테이너 관리 서비스로서 확장성과 속도가 뛰어납니다. 이 옵션을 사용하려면 서비스 내 작업 전반에서 HTTP (S) 계층 7 트래픽을 라우팅하고 보호할 수 있는 Application Load Balancer를 사용하도록 AWS WAF Amazon ECS를 구성해야 합니다. 자세한 내용은 Amazon Elastic Container Service 개발자 안내서에서 서비스 로드 밸런싱을 참조하세요.

주제

- AWS WAF 규칙
- 에서 크기 초과 요청 구성 요소 처리 AWS WAF
- 정규 표현식 패턴 매칭 AWS WAF
- IP 세트 및 정규식 패턴 세트 AWS WAF
- AWS WAF의 사용자 지정된 웹 요청 및 응답
- AWS WAF 웹 요청의 레이블
- AWS WAF 지능형 위협 완화
- AWS WAF 웹 ACL 트래픽 로깅
- AWS WAF 보호 기능 테스트 및 조정
- Amazon CloudFront 기능 사용 방법 AWS WAF
- AWS WAF 서비스 사용 시 보안
- AWS WAF 할당량
- AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF

AWS WAF 작동 방식

보호된 리소스가 HTTP (S) 웹 요청에 응답하는 방식을 제어하는 데 사용합니다 AWS WAF . 웹 액세스 제어 목록(ACL)을 정의하고 나서 이 목록을 보호할 하나 이상의 웹 애플리케이션 리소스에 연결하여 이 작업을 수행할 수 있습니다. 연결된 리소스는 들어오는 요청을 웹 ACL의 검사를 AWS WAF 위해 해당 주소로 전달합니다.

웹 ACL에서는 규칙을 만들어 요청에서 확인할 트래픽 패턴을 정의하고 일치하는 요청에 대해 수행할 작업을 지정할 수 있습니다. 작업 선택 사항에는 다음이 포함됩니다.

- 처리 및 응답을 위해 요청이 보호된 리소스로 전달되도록 허용합니다.
- 요청을 차단합니다.
- 요청 수를 계산합니다.
- 요청에 대해 CAPTCHA 또는 챌린지 검사를 실행하여 실제 사용자 및 표준 브라우저 사용을 확인합니다.

AWS WAF 구성 요소

의 핵심 구성 요소는 다음과 AWS WAF같습니다.

- 웹 ACL - 웹 액세스 제어 목록 (ACL) 을 사용하여 리소스 세트를 보호합니다. AWS 규칙을 추가하여 웹 ACL을 생성하고 보호 전략을 정의합니다. 규칙은 웹 요청을 검사하기 위한 기준을 정의하고 기준과 일치하는 요청을 처리하는 작업을 지정합니다. 또한 규칙에서 아직 차단하거나 허용하지 않은 요청을 차단할지 허용할지 여부를 나타내는 웹 ACL의 기본 동작을 설정할 수도 있습니다. 웹 ACL에 대한 자세한 내용은 AWS WAF 웹 액세스 제어 목록 (웹 ACL) 섹션을 참조하세요.

  웹 ACL은 리소스입니다. AWS WAF
- 규칙 – 각 규칙에는 검사 기준을 정의하는 문과 웹 요청이 기준을 충족하는 경우 수행할 작업이 포함됩니다. 웹 요청이 이 기준을 충족하면 일치하는 것입니다. 일치하는 요청을 차단 또는 허용하거나, 개수를 계산하거나, 아니면 CAPTCHA 퍼즐 또는 자동 클라이언트 브라우저 챌린지를 사용하는 요청에 대해 Bot Control을 실행하도록 규칙을 구성할 수 있습니다. 규칙에 대한 자세한 내용은 AWS WAF 규칙 단원을 참조하세요.

  규칙은 AWS WAF 리소스가 아닙니다. 규칙은 웹 ACL 또는 규칙 그룹의 컨텍스트에만 존재합니다.
- 규칙 그룹 - 웹 ACL 내에서 직접 또는 재사용 가능한 규칙 그룹에서 규칙을 정의할 수 있습니다. AWS 관리형 규칙 및 AWS Marketplace 판매자는 사용자가 사용할 수 있는 관리형 규칙 그룹을 제공합니다. 사용자 고유의 규칙 그룹을 정의할 수도 있습니다. 규칙 그룹에 대한 자세한 내용은 AWS WAF 규칙 그룹 단원을 참조하세요.

  규칙 그룹은 AWS WAF 리소스입니다.

주제

- AWS WAF 웹 ACL 용량 단위 (WCU)
- 보호할 수 있는 리소스 AWS WAF

AWS WAF 웹 ACL 용량 단위 (WCU)

AWS WAF 웹 ACL 용량 단위 (WCU) 를 사용하여 규칙, 규칙 그룹 및 웹 ACL을 실행하는 데 필요한 운영 리소스를 계산하고 제어합니다. AWS WAF 규칙 그룹 및 웹 ACL을 구성할 때 WCU 제한을 적용합니다. WCU는 웹 트래픽을 검사하는 방법에 AWS WAF 영향을 주지 않습니다.

AWS WAF 규칙, 규칙 그룹 및 웹 ACL의 용량을 관리합니다.

규칙 WCU

AWS WAF 규칙을 생성하거나 업데이트할 때 규칙 용량을 계산합니다. AWS WAF 각 규칙의 상대적 비용을 반영하여 각 규칙 유형별로 용량을 다르게 계산합니다. 실행 비용이 적게 드는 간단한 규칙은

처리 능력을 더 많이 사용하는 복잡한 규칙에 비해 WCU를 적게 사용합니다. 예를 들어 크기 제한 규칙 명령문에는 정규식 패턴 집합을 사용하여 요청을 검사하는 명령문보다 더 적은 WCU가 사용됩니다.

규칙 용량 요구 사항은 일반적으로 규칙 유형의 기본 비용에서 시작하여 예를 들어 검사 전에 텍스트 변환을 추가하거나 JSON 본문을 검사하는 경우 등 복잡성에 따라 증가합니다. 규칙 용량 요구 사항에 대한 자세한 내용은 규칙 문 기본 사항의 규칙 문 목록을 참조하세요.

규칙 그룹 WCU

규칙 그룹의 WCU 요구 사항은 규칙 그룹 내에서 정의하는 규칙에 따라 결정됩니다. 규칙 그룹의 최대 용량은 5,000WCU입니다.

각 규칙 그룹마다 변경할 수 없는 용량 설정이 있으며, 이 설정은 소유자가 생성 시 할당합니다. 이는 관리형 규칙 그룹과 이를 통해 AWS WAF생성한 규칙 그룹의 경우에도 마찬가지입니다. 규칙 그룹을 수정할 때 변경 사항은 규칙 그룹의 WCU가 해당 용량 내에 유지되도록 해야 합니다. 이렇게 하면 규칙 그룹을 사용하는 웹 ACL이 해당 용량 요구 사항 내에서 유지됩니다.

규칙 그룹에서 사용 중인 WCU는 해당 규칙의 WCU 합계에서 규칙의 동작을 조합하여 얻을 수 있는 처리 최적화를 뺀 AWS WAF 값입니다. 예를 들어 동일한 웹 요청 구성 요소를 검사하기 위해 두 개의 규칙을 정의하고 각 규칙이 구성 요소를 검사하기 전에 특정 변환을 적용하는 경우 변환 적용 요금만 한 번만 AWS WAF 청구될 수 있습니다. 웹 ACL의 규칙 그룹을 사용하는 데 드는 WCU 비용은 항상 규칙 그룹 생성 시 정의한 고정 WCU 설정입니다.

규칙 그룹을 생성할 때는 규칙 그룹의 전체 수명 기간 동안 사용하려는 규칙을 수용할 수 있을 만큼 용량을 충분히 높게 설정해야 합니다.

웹 ACL WCU

웹 ACL의 WCU 요구 사항은 웹 ACL 내에서 사용하는 규칙 및 규칙 그룹에 따라 결정됩니다.

- 웹 ACL에서 규칙 그룹을 사용하는 데 드는 비용은 규칙 그룹의 용량 설정입니다.
- 규칙 사용 비용은 규칙의 계산된 WCU에서 웹 ACL의 규칙 조합으로 얻을 수 있는 처리 최적화를 뺀 AWS WAF 값입니다. 예를 들어 동일한 웹 요청 구성 요소를 검사하기 위해 두 개의 규칙을 정의하고 각 규칙이 구성 요소를 검사하기 전에 특정 변환을 적용하는 경우 변환 적용 요금만 한 번만 AWS WAF 청구될 수 있습니다.

웹 ACL의 기본 가격에는 최대 1,500개 WCU가 포함됩니다. 1,500개 이상의 WCU를 사용하면 계층화된 가격 책정 모델에 따라 추가 요금이 발생합니다. AWS WAF 웹 ACL WCU 사용량 변화에 따라 웹 ACL 가격을 자동으로 조정합니다. 요금에 대한 자세한 내용은 AWS WAF Pricing을 참조하세요.

웹 ACL의 최대 용량은 5,000WCU입니다.

규칙 그룹 또는 웹 ACL의 WCU 결정

이전 섹션에서 설명한 것처럼, 규칙 그룹 또는 웹 ACL에서 사용되는 총 WCU는 규칙 그룹 또는 웹 ACL에 정의된 모든 규칙의 WCU 합계와 같거나 작습니다.

AWS WAF 콘솔에서 웹 ACL 또는 규칙 그룹에 규칙을 추가할 때 소비된 용량을 확인할 수 있습니다. 콘솔에는 규칙을 추가할 때 사용되는 현재 용량 단위가 표시됩니다.

API를 통해 웹 ACL 또는 규칙 그룹에서 사용하려는 규칙의 최대 용량 요구 사항을 확인할 수 있습니다. 이렇게 하려면 용량 확인 호출에 규칙의 JSON 목록을 제공합니다. 자세한 내용은 AWS WAF V2 API 참조를 참조하십시오 CheckCapacity.

보호할 수 있는 리소스 AWS WAF

AWS WAF 웹 ACL을 사용하여 글로벌 또는 지역 리소스 유형을 보호할 수 있습니다. 보호하려는 리소스에 웹 ACL을 연결하여 이 작업을 수행할 수 있습니다. 웹 ACL과 웹 ACL에서 사용하는 모든 AWS WAF 리소스는 관련 리소스가 위치한 지역에 있어야 합니다. Amazon CloudFront 배포의 경우 이 값은 미국 동부 (버지니아 북부) 로 설정됩니다.

아마존 CloudFront 디스트리뷰션

AWS WAF 콘솔 또는 API를 사용하여 AWS WAF 웹 ACL을 CloudFront 배포와 연결할 수 있습니다. CloudFront 배포 자체를 생성하거나 업데이트할 때 웹 ACL을 배포에 연결할 수도 있습니다. 에서 AWS CloudFormation연결을 구성하려면 CloudFront 배포 구성을 사용해야 합니다. Amazon에 대한 자세한 내용은 Amazon CloudFront CloudFront 개발자 안내서의 콘텐츠 액세스 제어를 위한 사용을 AWS WAF 참조하십시오.

AWS WAF 전 세계적으로 CloudFront 배포할 수 있지만 웹 ACL과 웹 ACL에 사용되는 모든 리소스 (예: 규칙 그룹, IP 세트, 정규식 패턴 세트) 를 생성하려면 미국 동부 (버지니아 북부) 지역을 사용해야 합니다. 일부 인터페이스에서는 “Global ()" 이라는 지역 선택 옵션을 제공합니다. CloudFront 이 옵션을 선택하는 것은 미국 동부(버지니아 북부) 리전 또는 “us-east-1“를 선택하는 것과 같습니다.

리전 리소스

사용 가능한 모든 지역의 AWS WAF 지역 리소스를 보호할 수 있습니다. Amazon Web Services 일반 참조에서 AWS WAF 엔드포인트와 할당량에서 목록을 확인할 수 있습니다.

를 AWS WAF 사용하여 다음과 같은 지역 리소스 유형을 보호할 수 있습니다.

- Amazon API Gateway REST API
- Application Load Balancer
- AWS AppSync GraphQL API
- Amazon Cognito 사용자 풀
- AWS App Runner 서비스
- AWS 검증된 액세스 인스턴스

웹 ACL은 AWS 리전안에 있는 Application Load Balancer에만 연결할 수 있습니다. 예를 들어, AWS Outposts에 있는 Application Load Balancer에는 웹 ACL을 연결할 수 없습니다.

웹 ACL 및 웹 ACL에서 사용하는 기타 모든 AWS WAF 리소스는 보호된 리소스와 동일한 지역에 있어야 합니다. 보호 대상 지역 리소스에 대한 웹 요청을 모니터링하고 관리할 때는 모든 데이터를 보호 대상 리소스와 동일한 지역에 AWS WAF 보관합니다.

다중 리소스 연결에 대한 제한 사항

다음과 같은 제한 사항을 제외하고 단일 웹 ACL을 하나 이상의 AWS 리소스와 연결할 수 있습니다.

- 각 AWS 리소스를 하나의 웹 ACL과만 연결할 수 있습니다. 웹 ACL과 AWS 리소스 간의 관계는 다음과 같습니다. one-to-many
- 웹 ACL을 하나 이상의 CloudFront 배포와 연결할 수 있습니다. CloudFront 배포와 연결한 웹 ACL을 다른 AWS 리소스 유형과 연결할 수 없습니다.

시작하기 AWS WAF

이 자습서에서는 를 사용하여 다음 작업을 수행하는 AWS WAF 방법을 보여줍니다.

- 설정 AWS WAF.
- AWS WAF 콘솔에서 마법사를 사용하여 웹 액세스 제어 목록 (웹 ACL) 을 생성합니다.
- 웹 요청을 AWS WAF 검사하려는 AWS 리소스를 선택합니다. 이 자습서에서는 Amazon의 단계를 다룹니다 CloudFront. Amazon API Gateway REST API, 애플리케이션 로드 밸런서, GraphQL API, Amazon Cognito 사용자 풀 AWS AppSync , 서비스 또는 검증된 액세스 인스턴스의 AWS App Runner 프로세스는 기본적으로 동일합니다. AWS
- 웹 요청을 필터링하는 데 사용할 규칙 및 규칙 그룹을 추가합니다. 예를 들어, 요청이 시작되는 IP 주소와 요청에서 공격자만 사용하는 값을 지정할 수 있습니다. 각 규칙에 대해 일치하는 웹 요청을 처

리하는 방법을 지정합니다. 요청을 차단하거나 개수를 계산하는 등의 작업을 수행하고 CAPTCHA와 같은 봇 챌린지를 실행할 수 있습니다. 웹 ACL 내에서 정의하는 각 규칙과 규칙 그룹 내에서 정의하는 각 규칙에 대해 작업을 정의할 수 있습니다.

- 웹 ACL에 대한 기본 동작을 Block 또는 Allow으로 지정합니다. 이는 웹 ACL의 규칙이 요청을 명시적으로 허용 또는 차단하지 않을 때 요청에 대해 AWS WAF 수행하는 작업입니다.

> **Note**
>
> AWS 일반적으로 이 자습서에서 생성한 리소스에 대해 일일 US $0.25 미만의 요금이 청구됩니다. 자습서를 완료하면 불필요한 요금 발생을 방지하기 위해 리소스를 삭제하는 것이 좋습니다.

주제

1단계: 설정 AWS WAF

서비스를 사용하기 위한 계정 설정에서 아직 일반적인 설정 단계를 따르지 않은 경우 지금 실행합니다.

2단계: 웹 ACL 생성

AWS WAF 콘솔은 사용자가 지정하는 기준 (예: 요청이 시작된 IP 주소 또는 요청의 값) 에 따라 웹 요청을 차단하거나 AWS WAF 허용하도록 구성하는 프로세스를 안내합니다. 이 단계에서는 웹 ACL을 생성합니다. AWS WAF 웹 ACL에 대한 자세한 내용은 을 참조하십시오. AWS WAF 웹 액세스 제어 목록 (웹 ACL)

웹 ACL을 생성하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

2. AWS WAF 홈페이지에서 웹 ACL 생성을 선택합니다.
3. 이름에 이 웹 ACL을 식별하는 데 사용할 이름을 입력합니다.

> **Note**
>
> 웹 ACL을 생성한 후에는 명칭을 변경할 수 없습니다.

4. (선택 사항) 원할 경우 Description - optional(설명 - 선택 사항)에 웹 ACL에 대한 자세한 설명을 입력합니다.
5. CloudWatch 메트릭 이름의 경우 해당하는 경우 기본 이름을 변경하십시오. 유효한 문자를 보려면 콘솔의 지침을 따르십시오. 이름에는 특수 문자, 공백 또는 “All” 및 “Default_Action” 등 AWS WAF에 예약된 지표 이름을 포함할 수 없습니다.

> **Note**
>
> 웹 ACL을 생성한 후에는 CloudWatch 지표 이름을 변경할 수 없습니다.

6. 리소스 유형에서는 CloudFront 배포를 선택합니다. 배포의 경우 지역이 자동으로 글로벌(CloudFront) 으로 채워집니다. CloudFront
7. (선택 사항) 관련 AWS 리소스 - 선택 사항의 경우 리소스 추가를 AWS 선택합니다. 대화 상자에서 연결할 리소스를 선택한 다음 추가를 선택합니다. AWS WAF 는 웹 ACL 설명 및 연결 AWS 리소스 설명 페이지로 돌아갑니다.
8. 다음을 선택합니다.

3단계: 문자열 일치 규칙 추가

이 단계에서는 문자열 일치 문을 사용하여 규칙을 생성하고 일치 요청으로 수행할 작업을 지정합니다. 문자열 일치 규칙 문은 AWS WAF 를 사용하여 요청에서 검색할 문자열을 식별합니다. 일반적으로 문자열은 인쇄 가능한 ASCII 문자로 구성되지만, 16진수 0x00에서 0xFF(십진수 0에서 255) 사이의 어떤 문자든지 지정할 수 있습니다. 검색할 문자열을 지정하는 것 외에도 헤더, 쿼리 문자열 또는 요청 본문과 같이 검색할 웹 요청 구성 요소를 지정합니다.

이 문은 웹 요청 구성 요소에서 작동하며 작동을 위해선 다음과 같은 요청 구성 요소 설정이 필요합니다.

- 요청 구성 요소 – 검사할 웹 요청 부분(예: 쿼리 문자열 또는 본문).

> **Warning**
>
> 요청 구성 요소 본문, JSON 본문, 헤더 또는 쿠키를 검사하는 경우 AWS WAF 검사할 수 있는 콘텐츠 양에 대한 제한 사항을 읽어보세요. 에서 크기 초과 요청 구성 요소 처리 AWS WAF

웹 요청 구성 요소에 대한 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.

- 선택적 텍스트 변환 — 요청 구성 요소를 검사하기 전에 요청 구성 요소에 대해 AWS WAF 수행하려는 변환입니다. 예를 들어, 소문자로 변환하거나 공백을 정규화할 수 있습니다. 변형을 두 개 이상 지정하는 경우, 나열된 순서대로 AWS WAF 처리합니다. 자세한 내용은 텍스트 변환 옵션을 참조하세요.

AWS WAF 규칙에 대한 자세한 내용은 을 참조하십시오AWS WAF 규칙.

문자열 일치 규칙 문을 생성하려면

1. Add rules and rule groups(규칙 및 규칙 그룹 추가) 페이지에서 규칙 빌더 추가, Add my own rules and rule groups(자체 규칙 및 규칙 그룹 추가), 규칙 빌더 및 Rule visual editor(규칙 시각적 편집기)를 차례로 선택합니다.

   > **Note**
   >
   > 콘솔은 Rule visual editor(규칙 시각적 편집기)와 Rule JSON editor(규칙 JSON 편집기)를 제공합니다. JSON 편집기는 웹 ACL 간에 구성을 쉽게 복사할 수 있게 해주므로 여러 수준의 중첩이 있는 규칙 집합과 같이 보다 복잡한 규칙 집합에 필요합니다.
   > 이 절차에서는 Rule visual editor(규칙 시각적 편집기)를 사용합니다.

2. 이름에 이 규칙을 식별하는 데 사용할 이름을 입력합니다.
3. 유형에서 Regular rule(일반 규칙)을 선택합니다.
4. If a request(요청의 경우)에서 matches the statement(문 일치)를 선택합니다.

   다른 옵션은 논리적 규칙문 유형에 사용됩니다. 이러한 논리적 규칙문 유형을 사용하여 다른 규칙 명령문의 결과를 결합하거나 무효화할 수 있습니다.
5. 명령문의 Inspect에서 드롭다운을 열고 AWS WAF 검사하려는 웹 요청 구성 요소를 선택합니다. 이 예에서는 헤더를 선택합니다.

헤더를 선택할 때 AWS WAF 에서 검사할 헤더도 지정합니다. **`User-Agent`**을 입력합니다. 이 값은 대소문자를 구분하지 않습니다.

6. 일치 유형에서 지정된 문자열이 `User-Agent` 헤더에 나타날 위치를 선택합니다.

   이 예제에서는 Exactly matches string(문자열에 정확히 일치)을 선택합니다. 이는 각 웹 요청의 user-agent 헤더를 AWS WAF 검사하여 지정한 문자열과 동일한 문자열을 찾는다는 것을 나타냅니다.

7. String to match(일치 시킬 문자열)에 AWS WAF 에서 검색할 문자열을 지정합니다. String to match(일치 시킬 문자열)의 최대 길이는 200자입니다. base64로 인코딩된 값을 지정하려는 경우, 인코딩하기 전에 최대 200자를 지정할 수 있습니다.

   이 예제에서는 를 입력합니다. MyAgent AWS WAF 웹 요청의 `User-Agent` 헤더에서 값을 `MyAgent` 검사합니다.

8. Text transformation(텍스트 변형)은 없음으로 설정된 상태로 둡니다.
9. 작업에서 웹 요청과 일치할 때 규칙에서 수행할 작업을 선택합니다. 예를 들면 개수를 선택하고 다른 선택 항목은 그대로 둡니다. 카운트 작업으로 규칙과 일치하는 웹 요청에 대한 지표가 생성되지만 요청의 허용 또는 차단 여부에는 영향을 주지 않습니다. 작업 선택에 대한 자세한 내용은 규칙 작업 및 웹 ACL 규칙 및 규칙 그룹 평가 섹션을 참조하세요.
10. 규칙 추가를 선택합니다.

4단계: AWS 관리형 규칙 규칙 그룹 추가

AWS 관리형 규칙은 사용자가 사용할 수 있는 관리형 규칙 그룹 세트를 제공하며, 대부분 AWS WAF 고객에게 무료로 제공됩니다. 규칙 그룹에 대한 자세한 내용은 AWS WAF 규칙 그룹을 참조하세요. 이 웹 ACL에 AWS 관리형 규칙 그룹을 추가할 예정입니다.

AWS 관리형 규칙 그룹을 추가하려면

1. Add rules and rule groups(규칙 및 규칙 그룹 추가) 페이지에서 규칙 추가를 선택한 다음 Add managed rule groups(관리형 규칙 그룹 추가)를 선택합니다.
2. 관리형 규칙 그룹 추가 페이지에서 AWS 관리형 규칙 그룹의 목록을 확장합니다. (AWS Marketplace 판매자에게 제공되는 목록도 볼 수 있습니다. 해당 오퍼링을 구독한 다음 AWS 관리형 규칙 그룹과 동일한 방식으로 사용할 수 있습니다.
3. 추가할 규칙 그룹에 대해 다음을 수행합니다.

   a. 작업 열에서 웹 ACL에 추가 토글을 켭니다.

b. 편집을 선택하고 규칙 그룹의 규칙 목록에서 모든 규칙 작업 재정의 드롭다운을 열고 Count를 선택합니다. 이렇게 하면 계산할 규칙 그룹의 모든 규칙에 대한 작업만 설정됩니다. 따라서 규칙 그룹을 사용하기 전에 웹 요청과 함께 규칙 그룹의 모든 규칙이 어떻게 동작하는지 확인할 수 있습니다.

c. 규칙 저장을 선택합니다.

4. 관리형 규칙 그룹 추가 페이지에서 규칙 추가를 선택합니다. 그러면 규칙 및 규칙 그룹 추가 페이지로 돌아갑니다.

5단계: 웹 ACL 구성 완료

웹 ACL 구성에 규칙 및 규칙 그룹을 추가했으면 웹 ACL에서 규칙의 우선 순위를 관리하고 지표, 태그 지정 및 로깅과 같은 설정을 구성하여 절차를 마칩니다.

웹 ACL 구성을 완료하려면

1. Add rules and rule groups(규칙 및 규칙 그룹 추가) 페이지에서 다음을 선택합니다.
2. 규칙 우선순위 설정 페이지에서 웹 ACL의 규칙 및 규칙 그룹에 대한 처리 순서를 확인할 수 있습니다. AWS WAF 목록의 맨 위부터 시작하여 처리합니다. 규칙을 위아래로 이동하여 처리 순서를 변경할 수 있습니다. 이렇게 하려면 목록에서 하나를 선택하고 위로 이동 또는 아래로 이동을 선택합니다. 규칙 우선 순위에 대한 자세한 내용은 웹 ACL의 규칙 및 규칙 그룹 처리 순서 단원을 참조하세요.
3. 다음을 선택합니다.
4. 지표 구성 페이지에서 Amazon CloudWatch 지표의 경우 규칙 및 규칙 그룹에 대한 계획된 지표와 웹 요청 샘플링 옵션을 볼 수 있습니다. 샘플링된 요청 보기에 대한 자세한 내용은 웹 요청 샘플 보기 섹션을 참조하세요. Amazon CloudWatch 지표에 대한 자세한 내용은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.

   AWS WAF 콘솔의 트래픽 개요 탭 아래에 있는 웹 ACL 페이지에서 웹 트래픽 지표 요약에 액세스할 수 있습니다. 콘솔 대시보드는 웹 ACL의 Amazon 지표에 대한 요약을 거의 실시간으로 제공합니다. CloudWatch 자세한 정보는 웹 ACL 트래픽 개요 대시보드을 참조하세요.
5. 다음을 선택하세요.
6. Review and create web ACL(웹 ACL 검토 및 생성) 페이지에서 설정을 검토한 다음 Create web ACL(웹 ACL 생성)을 선택합니다.

마법사가 새 웹 ACL이 나열된 Web ACL(웹 ACL) 페이지로 돌아갑니다.

6단계: 리소스 정리

이제 자습서를 성공적으로 완료했습니다. 계정에 추가 AWS WAF 요금이 발생하지 않도록 하려면 생성한 객체를 정리하십시오. AWS WAF 또는 실제로 관리하려는 웹 요청과 일치하도록 구성을 변경할 수 있습니다. AWS WAF

> **Note**
>
> AWS 일반적으로 이 자습서에서 생성한 리소스에 대해 일일 US $0.25 미만의 요금이 청구됩니다. 작업을 마치면 불필요한 요금 발생을 방지하기 위해 리소스를 삭제하는 것이 좋습니다.

요금이 부과되는 AWS WAF 객체를 삭제하려면

1. Web ACL(웹 ACL) 페이지의 목록에서 웹 ACL을 선택하고 편집을 선택합니다.
2. 연결된 AWS 리소스 탭의 각 관련 리소스에 대해 리소스 이름 옆에 있는 라디오 버튼을 선택한 다음 연결 해제를 선택합니다. 이렇게 하면 웹 ACL이 리소스에서 분리됩니다. AWS
3. 다음 각 화면에서 다음을 계속 선택하여 Web ACL 페이지로 돌아갑니다.

   Web ACL(웹 ACL) 페이지의 목록에서 웹 ACL을 선택하고 삭제를 선택합니다.

규칙 및 규칙 문은 규칙 그룹 및 웹 ACL 정의의 범위를 벗어나 존재하지 않습니다. 웹 ACL을 삭제하면 웹 ACL에 정의된 개별 규칙들이 모두 삭제됩니다. 웹 ACL에서 규칙 그룹을 제거하면 규칙 그룹에 대한 참조만 제거됩니다.

AWS WAF 웹 액세스 제어 목록 (웹 ACL)

웹 액세스 제어 목록(웹 ACL)은 보호된 리소스가 응답하는 모든 HTTP(S) 웹 요청을 세부적으로 제어할 수 있게 해줍니다. Amazon CloudFront, Amazon API Gateway, 애플리케이션 로드 밸런서 AWS AppSync, Amazon Cognito AWS App Runner AWS 및 검증된 액세스 리소스를 보호할 수 있습니다.

다음과 같은 기준을 사용하여 요청을 허용하거나 차단할 수 있습니다.

- 요청의 출처 IP 주소
- 요청의 출처 국가
- 요청의 일부로 포함된 문자열 일치 또는 정규 표현식(정규식) 일치
- 요청의 특정 부분의 크기

- 악성 SQL 코드 또는 스크립팅 감지

또한 이러한 조건의 조합을 테스트할 수 있습니다. 지정된 조건을 충족할 뿐만 아니라 지정된 요청 수를 초과하는 웹 요청을 1분 내에 차단하거나 카운트할 수 있습니다. 논리적 연산자를 사용하여 조건을 결합할 수 있습니다. 또한 CAPTCHA 퍼즐을 실행하고 요청에 대해 클라이언트 세션 챌린지를 자동으로 실행할 수도 있습니다.

일치 기준과 일치 시 취해야 할 조치를 AWS WAF 규칙 설명에 입력합니다. 웹 ACL 내에서 직접 그리고 웹 ACL에서 사용하는 재사용 가능한 규칙 그룹에서 규칙문을 정의할 수 있습니다. 옵션의 전체 목록은 규칙 문 기본 사항 및 규칙 작업 단원을 참조하세요.

웹 요청 검사 및 처리 기준을 지정하려면 다음 작업을 수행합니다.

1. 지정한 조건 중 하나와 일치하지 않는 웹 요청에 대해 웹 ACL 기본 작업(Allow 또는 Block)을 선택합니다. 자세한 정보는 웹 ACL 기본 동작을 참조하세요.
2. 웹 ACL에서 사용할 규칙 그룹을 추가합니다. 관리형 규칙 그룹에는 일반적으로 웹 요청을 차단하는 규칙이 포함됩니다. 규칙 그룹에 대한 자세한 내용은 AWS WAF 규칙 그룹 단원을 참조하세요.
3. 하나 이상의 규칙에 추가 일치 기준 및 처리 지침을 지정합니다. 규칙을 하나 이상을 추가하려면, AND 또는 OR 규칙 문으로 시작하고 그 아래에 결합하려는 규칙을 중첩합니다. 규칙 옵션을 부정하려면 규칙을 NOT 문에 중첩합니다. 선택에 따라 일반 규칙 대신에 비율 기반 규칙을 사용하여 조건을 충족하는 모든 IP 주소의 요청 수를 제한할 수 있습니다. 규칙에 대한 자세한 내용은 AWS WAF 규칙 단원을 참조하세요.

웹 ACL에 규칙을 두 개 이상 추가하는 경우 웹 ACL에 나열된 순서대로 규칙을 AWS WAF 평가합니다. 자세한 정보는 웹 ACL 규칙 및 규칙 그룹 평가을 참조하세요.

웹 ACL을 생성할 때 사용할 리소스 유형을 지정합니다. 자세한 내용은 웹 ACL 생성을 참조하세요. 웹 ACL을 정의한 후 리소스와 연결하여 리소스에 보호 기능을 제공할 수 있습니다. 자세한 정보는 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.

AWS 리소스가 다음과 같은 응답 지연을 처리하는 방법 AWS WAF

경우에 따라 요청을 허용할지 차단할지에 대한 관련 AWS 리소스에 대한 응답이 지연되는 내부 오류가 AWS WAF 발생할 수 있습니다. 이러한 경우 CloudFront 일반적으로 요청을 허용하거나 콘텐츠를 제공하는 반면, 지역 서비스는 일반적으로 요청을 거부하고 콘텐츠를 제공하지 않습니다.

주제

- 웹 ACL 규칙 및 규칙 그룹 평가

- 웹 ACL 기본 동작
- 신체 검사 크기 제한 관리
- CAPTCHA, 챌린지 및 토큰에 대한 구성
- 웹 ACL 작업

웹 ACL 규칙 및 규칙 그룹 평가

웹 ACL이 웹 요청을 처리하는 방법은 다음에 따라 다릅니다.

- 웹 ACL 및 규칙 그룹 내부에 있는 규칙의 숫자 우선 순위 설정
- 규칙 및 웹 ACL에 대한 작업 설정
- 추가하는 규칙 그룹의 규칙에 적용하는 모든 재정의

규칙 작업 설정 목록은 규칙 작업을 참조하세요.

규칙 작업 설정 및 기본 웹 ACL 작업에 요청 및 응답 처리를 사용자 지정할 수 있습니다. 자세한 내용은 AWS WAF의 사용자 지정된 웹 요청 및 응답 섹션을 참조하세요.

주제

- 웹 ACL의 규칙 및 규칙 그룹 처리 순서
- 웹 ACL에서 규칙 및 규칙 그룹 작업을 AWS WAF 처리하는 방법
- 규칙 그룹의 작업 재정의 옵션

웹 ACL의 규칙 및 규칙 그룹 처리 순서

웹 ACL과 모든 규칙 그룹 내에서 숫자 우선 순위 설정을 사용하여 규칙의 평가 순서를 결정합니다. 웹 ACL의 각 규칙에 대해 해당 웹 ACL 내에서 고유한 우선 순위 설정을 지정하고, 규칙 그룹의 각 규칙에 대해 해당 규칙 그룹 내에서 고유한 우선 순위 설정을 지정해야 합니다.

> **Note**
>
> 콘솔을 통해 규칙 그룹과 웹 ACL을 관리하는 경우 목록에 있는 규칙의 순서에 따라 고유한 숫자 우선 순위 설정을 AWS WAF 할당합니다. AWS WAF 목록 상단의 규칙에 가장 낮은 숫자 우선 순위를 할당하고 맨 아래에 있는 규칙에 가장 높은 숫자 우선 순위를 할당합니다.

웹 요청을 기준으로 웹 ACL 또는 규칙 그룹을 평가할 때는 AWS WAF 가장 낮은 숫자 우선 순위 설정부터 시작하여 평가를 종료하거나 모든 규칙을 모두 소진시키는 일치 항목을 찾을 때까지 규칙을 평가합니다.

예를 들어 웹 ACL에 다음과 같이 우선 순위가 지정된 다음 규칙 및 규칙 그룹이 있다고 가정해 보겠습니다.

- 규칙 1 — 우선순위 0
- RuleGroupA — 우선순위 100
  - 규칙 A1 — 우선순위 10,000
  - 규칙 A2 — 우선순위 20,000
- 규칙 2 — 우선순위 200
- RuleGroupB — 프라이어리티 300
  - 규칙 B1 — 우선순위 0
  - 규칙 B2 — 우선순위 1

AWS WAF 이 웹 ACL의 규칙을 다음 순서로 평가합니다.

- 규칙 1
- RuleGroupA: 규칙 A1
- RuleGroupA 규칙 A2
- 규칙 2
- RuleGroupB 규칙 B1
- RuleGroupB 룰 B2

웹 ACL에서 규칙 및 규칙 그룹 작업을 AWS WAF 처리하는 방법

규칙 및 규칙 그룹을 구성할 때 일치하는 웹 요청을 처리할 AWS WAF 방법을 선택합니다.

- Allow 및 Block에서 작업 종료 중 - Allow 및 Block 작업이 일치하는 웹 요청에서 웹 ACL의 다른 모든 처리를 중지합니다. 웹 ACL의 규칙이 요청과 일치하는 항목을 찾았는데 규칙 동작이 Allow '또'인 경우Block, 해당 일치에 따라 웹 ACL에 대한 웹 요청의 최종 처리가 결정됩니다. AWS WAF 웹 ACL에서 일치하는 규칙 뒤에 오는 다른 규칙은 처리하지 않습니다. 이러한 원칙은 웹 ACL에 직접 추가하는 규칙과 추가된 규칙 그룹 내에 있는 규칙에 적용됩니다. Block 작업을 수행하면 보호된 리소스가 웹 요청을 받거나 처리하지 않습니다.

- Count는 비종료 작업임 – Count 작업이 있는 규칙이 요청과 일치하면 AWS WAF 은 요청을 계수한 다음 웹 ACL 규칙 집합에 따르는 규칙을 계속 처리합니다.
- CAPTCHA비종료 또는 종료 작업일 Challenge 수 있음 — 이러한 작업 중 하나가 포함된 규칙이 요청과 일치하면 해당 토큰 AWS WAF 상태를 확인합니다. 요청에 유효한 토큰이 있는 경우 일치 항목을 일치와 유사하게 처리한 Count 다음 웹 ACL 규칙 집합에서 따르는 규칙을 계속 AWS WAF 처리합니다. 요청에 유효한 토큰이 없는 경우 평가를 AWS WAF 종료하고 클라이언트에게 해결해야 할 CAPTCHA 퍼즐 또는 자동 백그라운드 클라이언트 세션 챌린지를 보냅니다.

규칙 평가 결과 종료 작업이 발생하지 않는 경우 웹 ACL 기본 작업을 요청에 AWS WAF 적용합니다. 자세한 내용은 웹 ACL 기본 동작을 참조하세요.

웹 ACL에서는 규칙 그룹 내 규칙에 대한 작업 설정을 재정의하고 규칙 그룹에서 반환되는 작업을 재정의할 수 있습니다. 자세한 내용은 규칙 그룹의 작업 재정의 옵션을 참조하세요.

작업과 우선 순위 설정 간의 상호 작용

웹 요청에 AWS WAF 적용되는 작업은 웹 ACL에 있는 규칙의 숫자 우선 순위 설정의 영향을 받습니다. 예를 들어 웹 ACL에 Allow 작업을 포함하고 숫자 우선 순위가 50인 규칙과 Count 작업을 포함하고 숫자 우선 순위가 100인 규칙이 있다고 가정해 보겠습니다. AWS WAF 는 가장 낮은 설정부터 시작하여 우선 순위에 따라 웹 ACL의 규칙을 평가하므로 개수 규칙보다 허용 규칙을 먼저 평가합니다. 두 규칙과 일치하는 웹 요청은 허용 규칙과 먼저 일치합니다. Allow는 종료 작업이므로 이 경기에서 평가를 중단하고 개수 규칙에 따라 요청을 평가하지 않을 AWS WAF 것입니다.

- 허용 규칙과 일치하지 않는 요청만 개수 규칙 지표에 포함하려는 경우에는 규칙의 우선 순위 설정이 적합합니다.
- 반면 허용 규칙과 일치하는 요청에도 개수 규칙의 개수 지표를 적용하려면 허용 규칙보다 더 낮은 숫자 우선 순위 설정을 개수 규칙에 지정하여 먼저 실행되도록 해야 합니다.

우선 순위 설정에 대한 자세한 내용은 웹 ACL의 규칙 및 규칙 그룹 처리 순서 섹션을 참조하세요.

규칙 그룹의 작업 재정의 옵션

웹 ACL에 규칙 그룹을 추가하면 일치하는 웹 요청에 대해 수행하는 작업을 재정의할 수 있습니다. 웹 ACL 구성 내의 규칙 그룹에 대한 작업을 재정의해도 규칙 그룹 자체는 변경되지 않습니다. 웹 AWS WAF ACL의 컨텍스트에서 규칙 그룹을 사용하는 방법만 변경됩니다.

규칙 그룹 규칙 작업 재정의

이제 규칙 그룹에 있는 규칙의 작업을 유효한 규칙 작업 중 하나로 재정의할 수 있습니다. 이렇게 하면 구성된 규칙의 작업이 재정의 설정인 것처럼 일치 요청이 정확하게 처리됩니다.

> **Note**
>
> 규칙 작업은 종료일 수도 있고 종료되지 않을 수도 있습니다. 종료 작업은 요청의 웹 ACL 평가를 중지하고 보호된 애플리케이션을 계속 실행하도록 허용하거나 차단합니다.

다음은 규칙 작업 옵션입니다.

- Allow— AWS WAF 요청을 보호된 AWS 리소스로 전달하여 처리 및 응답을 받을 수 있습니다. 이 작업은 종료 작업입니다. 정의한 규칙에서는 요청을 보호된 리소스로 전달하기 전에 사용자 지정 헤더를 요청에 삽입할 수 있습니다.
- Block— 요청을 AWS WAF 차단합니다. 이 작업은 종료 작업입니다. 기본적으로 보호된 AWS 리소스는 HTTP `403 (Forbidden)` 상태 코드로 응답합니다. 정의한 규칙에서 응답을 사용자 지정할 수 있습니다. 요청을 AWS WAF 차단하면 Block 작업 설정에 따라 보호된 리소스가 클라이언트에 다시 보내는 응답이 결정됩니다.
- Count— 요청 AWS WAF 수를 계산하지만 허용할지 차단할지는 결정하지 않습니다. 이 작업을 비종료 작업입니다. AWS WAF 는 웹 ACL의 나머지 규칙을 계속 처리합니다. 정의한 규칙에서 요청에 사용자 지정 헤더를 삽입하면 다른 규칙과 일치시킬 수 있는 레이블을 추가할 수 있습니다.
- CAPTCHA및 Challenge — CAPTCHA 퍼즐과 사일런트 챌린지를 AWS WAF 사용하여 봇이 보낸 요청이 아닌지 확인하고 토큰을 AWS WAF 사용하여 최근에 성공한 클라이언트 응답을 추적합니다.

  CAPTCHA 퍼즐과 사일런트 챌린지는 브라우저가 HTTPS 엔드포인트에 액세스할 때만 실행할 수 있습니다. 토큰을 획득하려면 브라우저 클라이언트가 안전한 환경에서 실행되고 있어야 합니다.

  > **Note**
  >
  > 규칙 중 하나에서 또는 규칙 그룹 내 규칙 작업 재정의로서 CAPTCHA 또는 Challenge 규칙 작업을 사용하는 경우 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

  이러한 규칙 작업은 요청의 토큰 상태에 따라 종료되거나 종료되지 않을 수 있습니다.

- 만료되지 않은 유효한 토큰에 대한 비종료 — 토큰이 구성된 CAPTCHA 또는 챌린지 면역 시간에 따라 유효하고 만료되지 않은 경우 조치와 유사하게 요청을 처리합니다. AWS WAF Count AWS WAF 웹 ACL의 나머지 규칙을 기반으로 웹 요청을 계속 검사합니다. Count 구성과 마찬가지로, 정의한 규칙에서도 요청에 삽입할 사용자 지정 헤더를 사용하여 이러한 작업을 선택적으로 구성하고 다른 규칙과 일치시킬 수 있는 레이블을 추가할 수 있습니다.
- 유효하지 않거나 만료된 토큰에 대한 요청이 차단되어 종료 — 토큰이 유효하지 않거나 표시된 타임스탬프가 만료된 경우, 웹 요청 검사가 AWS WAF 종료되고 요청이 차단됩니다. 이는 조치와 유사합니다. Block AWS WAF 그런 다음 사용자 지정 응답 코드로 클라이언트에 응답합니다. 의 경우 요청 내용에 클라이언트 브라우저에서 처리할 수 있다고 표시되면 인간 클라이언트와 봇을 구분하도록 설계된 JavaScript 전면 광고를 통해 CAPTCHA 퍼즐을 AWS WAF 전송합니다. CAPTCHA Challenge액션의 경우 일반 브라우저와 봇이 실행하는 세션을 구분하도록 설계된 자동 챌린지가 포함된 JavaScript 전면 광고를 AWS WAF 보냅니다.

자세한 내용은 CAPTCHA그리고 Challenge 안에 AWS WAF 섹션을 참조하세요.

이 옵션을 사용하는 방법에 대한 자세한 방법은 규칙 그룹에 대한 규칙 작업 재정의 섹션을 참조하세요.

규칙 작업을 Count로 재정의

규칙 작업 재정의의 가장 일반적인 사용 사례는 규칙 그룹을 프로덕션 환경에 배치하기 전에 규칙 그룹의 동작을 테스트 및 모니터링하기 위해 규칙 작업의 일부 또는 전체를 Count로 재정의하는 것입니다.

또한 이 방법을 사용하여 거짓 긍정을 생성하는 규칙 그룹의 문제를 해결할 수도 있습니다. 거짓 긍정은 차단될 것으로 예상되지 않는 트래픽을 규칙 그룹에서 차단할 때 발생합니다. 규칙 그룹 내에서 허용하려는 요청을 차단하는 규칙을 식별한 경우 해당 규칙에 대한 계산 작업 재정의를 유지하여 해당 규칙이 요청에 적용되지 않고 제외되도록 할 수 있습니다.

테스트에서 규칙 작업 재정의를 사용하는 방법에 대한 자세한 내용은 AWS WAF 보호 기능 테스트 및 조정 섹션을 참조하세요.

JSON 목록: **`RuleActionOverrides`**에서 **`ExcludedRules`** 대체

2022년 10월 27일 이전에 웹 ACL Count 구성에서 규칙 그룹 규칙 동작을 로 설정한 경우, 재정의를 웹 ACL JSON에 로 AWS WAF 저장했습니다. `ExcludedRules` 이제 규칙을 Count로 재정의하기 위한 JSON 설정은 `RuleActionOverrides` 설정에 있습니다.

AWS WAF 콘솔을 사용하여 기존 규칙 그룹 설정을 편집하면 콘솔은 재정의 작업이 로 설정된 상태로 JSON의 모든 `ExcludedRules` 설정을 `RuleActionOverrides` 설정으로 자동 변환합니다. Count

- 현재 설정 예:

```
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "RuleActionOverrides": [
            {
              "Name": "AdminProtection_URIPATH",
              "ActionToUse": {
                "Count": {}
              }
            }
          ]
```

- 이전 설정 예:

```
OLD SETTING
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAdminProtectionRuleSet",
          "ExcludedRules": [
            {
              "Name": "AdminProtection_URIPATH"
            }
          ]
OLD SETTING
```

작업이 Count로 설정되어 있는 상태에서 JSON 목록의 모든 `ExcludedRules` 설정을 `RuleActionOverrides` 설정으로 업데이트하는 것이 좋습니다. API는 두 설정 중 하나를 허용하지만 새 `RuleActionOverrides` 설정만 사용하는 경우 콘솔 작업과 API 작업 간에 JSON 목록의 일관성이 유지됩니다.

규칙 그룹은 액션 오버라이드를 다음으로 반환합니다. Count

규칙 그룹이 반환하는 작업을 Count로 설정하여 재정의할 수 있습니다.

> **Note**
>
> 이 옵션은 규칙 그룹 자체의 AWS WAF 평가 방식을 변경하지 않으므로 규칙 그룹에서 규칙을 테스트하는 데는 적합하지 않습니다. 규칙 그룹 평가에서 웹 ACL로 반환된 결과를 AWS WAF

처리하는 방법에만 영향을 줍니다. 규칙 그룹의 규칙을 테스트하려면 이전 섹션인 규칙 그룹 규칙 작업 재정의에 설명된 옵션을 사용하십시오.

규칙 그룹 작업을 로 Count 재정의하면 규칙 그룹 평가가 정상적으로 AWS WAF 처리됩니다.

규칙 그룹에 일치하는 규칙이 없거나 모든 일치 규칙에 Count 작업이 있는 경우 이 재정의는 규칙 그룹 또는 웹 ACL의 처리에 영향을 주지 않습니다.

규칙 그룹에서 웹 요청과 일치하고 종료 규칙 작업이 있는 첫 번째 규칙은 규칙 그룹 평가를 중단하고 종료 작업 결과를 웹 ACL 평가 수준으로 반환합니다. AWS WAF 이 시점에서 웹 ACL 평가에서 이 재정의가 적용됩니다. AWS WAF 규칙 그룹 평가 결과가 작업만 되도록 종료 작업을 재정의합니다. Count AWS WAF 그런 다음 웹 ACL에서 나머지 규칙을 계속 처리합니다.

이 옵션을 사용하는 방법에 대한 자세한 방법은 규칙 그룹의 평가 결과를 Count로 재정의 섹션을 참조하세요.

웹 ACL 기본 동작

웹 ACL을 생성하고 구성할 때는 웹 ACL 기본 작업을 설정해야 합니다. AWS WAF 는 종료 작업을 적용하지 않고 모든 웹 ACL의 규칙 평가를 통과하는 모든 웹 요청에 이 작업을 적용합니다. 종료 작업은 요청의 웹 ACL 평가를 중지하고 보호된 애플리케이션을 계속 실행하도록 허용하거나 차단합니다. 규칙 작업에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.

웹 ACL 기본 작업은 웹 요청의 최종 처리를 결정해야 하므로 종료 작업입니다.

- Allow – 대부분의 사용자가 웹 사이트에 액세스할 수 있도록 허용하려고 하지만 지정된 IP 주소에서 요청이 시작되거나 요청에 악성 SQL 코드 도는 지정된 값이 포함된 것으로 보이는 공격자에게는 액세스를 차단하려는 경우 기본 작업으로 Allow을 선택합니다. 그런 다음 웹 ACL에 규칙을 추가할 때 차단할 특정 요청을 식별하고 차단하는 규칙을 추가합니다. 이 작업에서는 요청을 보호된 리소스로 전달하기 전에 사용자 지정 헤더를 요청에 삽입할 수 있습니다.
- Block – 대부분의 사용자가 웹 사이트에 액세스하지 못하도록 하려고 하지만 지정된 IP 주소에서 요청이 시작되거나 요청에 지정된 값이 포함된 사용자에게 액세스를 허용하려는 경우 기본 작업으로 Block을 선택합니다. 그런 다음 웹 ACL에 규칙을 추가할 때 허용할 특정 요청을 식별하고 허용하는 규칙을 추가합니다. 기본적으로 Block 작업의 경우 AWS 리소스는 HTTP `403 (Forbidden)` 상태 코드로 응답하지만 응답을 사용자 지정할 수 있습니다.

요청 및 응답을 사용자 지정하는 방법에 대한 자세한 내용은 AWS WAF의 사용자 지정된 웹 요청 및 응답 섹션을 참조하세요.

자체 규칙 및 규칙 그룹의 구성은 대부분의 웹 요청을 허용할지 또는 차단할지에 따라 부분적으로 달라집니다. 예를 들어 대부분의 요청을 허용하려면 웹 ACL 기본 작업을 Allow하도록 설정한 후 다음과 같이 차단할 웹 요청을 식별하는 규칙을 추가합니다.

- 합당하지 않은 수의 요청을 수행하는 IP 주소에서 기원되는 요청
- 사업을 운영하지 않거나 공격이 빈번하게 발생하는 국가에서 시작되는 요청
- `User-agent` 헤더에 가짜 값이 포함된 요청
- 악성 SQL 코드가 포함된 것으로 보이는 요청

관리형 규칙 그룹 규칙은 일반적으로 Block 작업을 사용하지만 그렇지 않은 규칙도 있습니다. 예를 들면 Bot Control에 사용되는 일부 규칙에는 CAPTCHA 및 Challenge 작업 설정이 사용됩니다. 관리형 규칙 그룹에 대한 자세한 내용은 관리형 규칙 그룹 단원을 참조하세요.

신체 검사 크기 제한 관리

본문 검사 크기 제한은 검사할 수 있는 최대 요청 본문 크기입니다. AWS WAF 웹 요청 본문이 한도보다 크면 기본 호스트 서비스는 검사를 AWS WAF 위해 제한 범위 내에 있는 콘텐츠만 전달합니다.

- Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB (8,192바이트) 로 고정되어 있습니다.
- API Gateway, Amazon Cognito, 앱 러너, 검증된 액세스의 경우 기본 제한은 16KB (16,384바이트) 이며, 모든 리소스 유형에 대해 16KB씩 최대 64KB까지 제한을 늘릴 수 있습니다. CloudFront 설정 옵션은 16KB, 32KB, 48KB 및 64KB입니다.

너무 큰 본문 처리

웹 트래픽에 한도보다 큰 본문이 포함된 경우 구성된 크기 초과 처리가 적용됩니다. 크기 초과 처리 옵션에 대한 자세한 내용은 을 참조하십시오. 에서 크기 초과 요청 구성 요소 처리 AWS WAF

한도 설정 상향 조정을 위한 가격 고려 사항

AWS WAF 리소스 유형의 기본 한도 내에 있는 트래픽을 검사할 경우 기본 요금을 부과합니다.

API Gateway, Amazon Cognito, App Runner, 검증된 액세스 리소스의 경우 제한 설정을 늘리면 AWS WAF 검사할 수 있는 트래픽에 새 한도까지의 신체 크기가 포함됩니다. CloudFront 본문 크기가 기본값인 16KB보다 큰 요청을 검사하는 경우에만 추가 요금이 부과됩니다. 요금에 대한 자세한 내용은 AWS WAF 요금 부분을 참조하세요.

신체 검사 크기 제한을 수정하기 위한 옵션

API Gateway, Amazon Cognito CloudFront, 앱 러너 또는 검증된 액세스 리소스에 대한 신체 검사 크기 제한을 구성할 수 있습니다.

웹 ACL을 생성하거나 편집할 때 리소스 연결 구성에서 본문 검사 크기 제한을 수정할 수 있습니다. API의 경우 에서 웹 ACL의 연결 구성을 참조하십시오. AssociationConfig 콘솔의 경우 웹 ACL의 관련 리소스를 지정하는 페이지의 구성을 참조하십시오. 콘솔 구성에 대한 지침은 웹 ACL 작업 섹션을 참조하세요.

CAPTCHA, 챌린지 및 토큰에 대한 구성

CAPTCHA또는 Challenge 규칙 작업을 사용하는 규칙과 관리형 보호를 위해 사일런트 클라이언트 챌린지를 관리하는 애플리케이션 통합 SDK에 대해 웹 ACL의 옵션을 구성할 수 있습니다. AWS WAF

이러한 기능을 사용하면 최종 사용자에게 CAPTCHA 퍼즐을 제시하고 클라이언트 세션에 자동 챌린지를 제공하여 봇 활동을 줄일 수 있습니다. 클라이언트가 성공적으로 응답하면 AWS WAF 는 웹 요청에 사용할 토큰을 클라이언트에 제공합니다. 이 토큰에는 마지막으로 성공한 퍼즐 및 챌린지 응답이 타임스탬프로 지정됩니다. 자세한 정보는 AWS WAF 지능형 위협 완화을 참조하세요.

웹 ACL 구성에서 이러한 토큰을 관리하는 방법을 AWS WAF 구성할 수 있습니다.

- CAPTCHA 및 챌린지 면제 시간 — CAPTCHA 또는 챌린지 타임스탬프가 유효 상태로 유지되는 시간을 지정합니다. 웹 ACL 설정은 자체 면제 시간 설정이 구성되어 있지 않은 모든 규칙과 애플리케이션 통합 SDK에 상속됩니다. 자세한 정보는 타임스탬프 만료: AWS WAF 토큰 면역 시간을 참조하세요.
- 토큰 도메인 - 기본적으로 웹 ACL이 연결된 리소스의 도메인에만 토큰을 AWS WAF 허용합니다. 토큰 도메인 목록을 구성하는 경우 목록에 있는 모든 도메인과 관련 리소스의 도메인에 대해 토큰을 AWS WAF 수락합니다. 자세한 내용은 AWS WAF 웹 ACL 토큰 도메인 목록 구성을(를) 참조하세요.

웹 ACL 작업

이 섹션에서는 AWS 콘솔을 통해 웹 ACL을 생성, 관리 및 사용하는 절차를 제공합니다.

사용 중인 웹 ACL의 경우 AWS WAF 콘솔의 트래픽 개요 탭 아래에 있는 웹 ACL 페이지에서 웹 트래픽 지표의 요약에 액세스할 수 있습니다. 콘솔 대시보드는 애플리케이션 웹 트래픽을 평가할 때 AWS WAF 수집하는 Amazon CloudWatch 지표의 요약을 거의 실시간으로 제공합니다. 대시보드에 대한 자세한 내용은 웹 ACL 트래픽 개요 대시보드 섹션을 참조하세요. 웹 ACL 트래픽 모니터링에 대한 추가적인 내용은 모니터링 및 조정 섹션을 참조하세요.

프로덕션 트래픽 위험

프로덕션 트래픽용 웹 ACL에 변경 사항을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 변경 사항을 테스트하고 조정하십시오. 그런 다음 업데이트된 규칙을 프로덕션 트래픽과 함께 계산 모드에서 테스트하고 조정한 다음 활성화하십시오. 자세한 지침은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

Note

웹 ACL에서 1,500개가 넘는 WCU를 사용하면 기본 웹 ACL 가격을 초과하는 비용이 발생합니다. 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 및 AWS WAF 요금을 참조하세요.

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 생성하거나 변경할 때 리소스가 저장된 모든 영역에 변경 사항이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

주제

- 웹 ACL 생성
- 웹 ACL 편집
- 웹 ACL에서 규칙 그룹 동작 관리
- 웹 ACL을 리소스와 연결 또는 연결 해제 AWS
- 웹 ACL 삭제

웹 ACL 생성

새 웹 ACL을 생성하려면 이 페이지의 절차에 따라 웹 ACL 생성 마법사를 사용합니다.

> **⚠ 프로덕션 트래픽 위험**
>
> 프로덕션 트래픽용 웹 ACL에 변경 사항을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 변경 사항을 테스트하고 조정하십시오. 그런 다음 업데이트된 규칙을 프로덕션 트래픽과 함께 계산 모드에서 테스트하고 조정한 다음 활성화하십시오. 자세한 지침은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

> **Note**
>
> 웹 ACL에서 1,500개가 넘는 WCU를 사용하면 기본 웹 ACL 가격을 초과하는 비용이 발생합니다. 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 및 AWS WAF 요금을 참조하세요.

웹 ACL을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 Web ACLs(웹 ACL)을 선택한 다음 Create web ACL(웹 ACL 생성)을 선택합니다.
3. 이름에 이 웹 ACL을 식별하는 데 사용할 이름을 입력합니다.

   > **Note**
   >
   > 웹 ACL을 생성한 후에는 명칭을 변경할 수 없습니다.

4. (선택 사항) 원할 경우 Description - optional(설명 - 선택 사항)에 웹 ACL에 대한 자세한 설명을 입력합니다.
5. CloudWatch 메트릭 이름의 경우 해당하는 경우 기본 이름을 변경하십시오. 유효한 문자를 보려면 콘솔의 지침을 따르십시오. 이름에는 특수 문자, 공백 또는 전용 지표 이름 (예 AWS WAF: “All” 및 “Default_Action”) 을 포함할 수 없습니다.

> **Note**
>
> 웹 ACL을 생성한 후에는 CloudWatch 메트릭 이름을 변경할 수 없습니다.

6. 리소스 유형에서 이 웹 ACL과 연결할 AWS 리소스 범주 (Amazon CloudFront 배포 또는 지역 리소스) 를 선택합니다. 자세한 정보는 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.
7. 지역의 경우 지역 리소스 유형을 선택한 경우 웹 AWS WAF ACL을 저장할 지역을 선택합니다.

   리전 리소스 유형에 대해서만 이 옵션을 선택해야 합니다. CloudFront 배포의 경우 글로벌 () 애플리케이션의 경우 지역이 미국 동부 (버지니아 북부) 지역으로 하드 코딩됩니다. `us-east-1` CloudFront
8. (CloudFront, API Gateway, Amazon Cognito, 앱 러너, 검증된 액세스) 웹 요청 검사 크기 제한의 경우 - 선택 사항입니다. 다른 신체 검사 크기 제한을 지정하려면 제한을 선택합니다. 기본값인 16KB를 초과하는 신체 크기를 검사할 경우 추가 비용이 발생할 수 있습니다. 이 옵션에 대한 자세한 내용은 신체 검사 크기 제한 관리 단원을 참조하세요.
9. (선택 사항) 관련 AWS 리소스의 경우 - 선택 사항입니다. 리소스를 지금 지정하려면 리소스 추가를 AWS 선택합니다. 대화 상자에서 연결하려는 리소스를 선택한 다음 추가를 선택합니다. AWS WAF 웹 ACL 및 관련 AWS 리소스 설명 페이지로 돌아갑니다.
10. 다음을 선택합니다.
11. (선택 사항) 관리형 규칙 그룹을 추가하고 싶으면 Add rules and rule groups(규칙 및 규칙 그룹 추가) 페이지에서 규칙 추가를 선택한 다음 Add managed rule groups(관리형 규칙 그룹 추가)를 선택합니다. 추가할 각 관리형 규칙 그룹에 대해 다음을 수행합니다.

    a. 관리형 규칙 그룹 추가 페이지에서 AWS 관리형 규칙 그룹 또는 원하는 AWS Marketplace 셀러의 목록을 확장하십시오.

    b. 추가하려는 규칙 그룹에 대해 작업 열에서 웹 ACL에 추가 토글을 켭니다.

       웹 ACL에서 규칙 그룹을 사용하는 방식을 사용자 지정하려면 편집을 선택합니다. 다음은 일반적인 사용자 지정 설정입니다.

       - 일부 또는 모든 규칙의 규칙 작업을 재정의합니다. 규칙에 대한 재정의 작업을 정의하지 않는 경우 평가 시 규칙 그룹 내부에 정의된 규칙 작업이 사용됩니다. 이 옵션에 대한 자세한 내용은 규칙 그룹의 작업 재정의 옵션 단원을 참조하세요.
       - 범위 축소문을 추가하여 규칙 그룹이 검사하는 웹 요청의 범위를 줄입니다. 이 옵션에 대한 자세한 내용은 범위 축소 문 단원을 참조하세요.

- 일부 관리형 규칙 그룹에서는 추가 구성을 제공해야 합니다. 관리형 규칙 그룹 공급자가 제공한 설명서를 참조하세요. AWS 관리형 규칙 그룹과 관련된 자세한 내용은 을 참조하십시오AWS 에 대한 관리형 규칙 AWS WAF.

설정을 완료했으면 규칙 저장을 선택합니다.

규칙 추가를 선택하여 관리형 규칙 추가를 완료하고 Add rules and rule groups(규칙 및 규칙 그룹 추가) 페이지로 돌아갑니다.

12. (선택 사항) 자체 규칙 그룹을 추가하려면 Add rules and rule groups(규칙 및 규칙 그룹 추가) 페이지에서 규칙 추가를 선택한 다음, Add my own rules and rule groups(자체 규칙 및 규칙 그룹 추가)를 선택합니다. 추가할 각 규칙 그룹에 대해 다음을 수행합니다.

    a. Add my own rules and rule group(자체 규칙 및 규칙 그룹 추가)에서 Rule group(규칙 그룹)을 선택합니다.

    b. 이름에 이 웹 ACL의 규칙 그룹 규칙에 사용할 이름을 입력합니다. `AWS`, `Shield`, `PreFM` 또는 `PostFM`으로 시작하는 이름은 사용하면 안 됩니다. 이러한 문자열은 예약되어 있거나 다른 서비스에서 관리되는 규칙 그룹과 혼동될 수 있습니다. 다른 서비스에서 제공하는 규칙 그룹 섹션을 참조하십시오.

    c. 목록에서 규칙 그룹을 선택합니다.

    > **Note**
    >
    > 자체 규칙 그룹에 대한 규칙 동작을 재정의하려면 먼저 웹 ACL에 저장한 다음 웹 ACL의 규칙 목록에서 웹 ACL과 규칙 그룹 참조 문을 편집하십시오. 관리형 규칙 그룹과 마찬가지로 규칙 동작을 임의의 유효한 작업 설정으로 재정의할 수 있습니다.

    d. 규칙 추가를 선택합니다.

13. (선택 사항) 자체 규칙 그룹을 추가하려면 Add rules and rule groups(규칙 및 규칙 그룹 추가) 페이지에서 규칙 추가, Add my own rules and rule groups(자체 규칙 및 규칙 그룹 추가), 규칙 빌더, 그리고 Rule visual editor(규칙 시각적 편집기)를 차례로 선택합니다.

> **Note**
>
> 콘솔의 규칙 시각적 편집기에서는 한 수준의 중첩을 지원합니다. 예를 들어 단일 논리적 `AND` 또는 `OR` 문을 사용하고 그 안에 한 수준의 다른 명령문을 중첩할 수 있지만 논리적 문 내에 논리적 문을 중첩할 수는 없습니다. 보다 복잡한 규칙 문을 관리하려면 규칙 JSON

편집기를 사용합니다. 규칙의 모든 옵션에 대한 자세한 내용은 AWS WAF 규칙 단원을 참조하세요.
이 절차에서는 규칙 시각적 편집기에 대해 설명합니다.

a. 이름에 이 규칙을 식별하는 데 사용할 이름을 입력합니다. `AWS`, `Shield`, `PreFM` 또는 `PostFM`으로 시작하는 이름은 사용하면 안 됩니다. 이러한 문자열은 예약되어 있거나 다른 서비스에서 관리되는 규칙 그룹과 혼동될 수 있습니다.

b. 필요에 따라 규칙 정의를 입력합니다. 논리적 `AND` 및 `OR` 규칙 문 내에서 규칙을 결합할 수 있습니다. 마법사는 컨텍스트에 따라 각 규칙에 대한 옵션을 안내합니다. 규칙 옵션에 대한 자세한 내용은 AWS WAF 규칙 단원을 참조하세요.

c. 작업에서 웹 요청과 일치할 때 규칙에서 수행할 작업을 선택합니다. 선택 사항에 대한 자세한 내용은 규칙 작업 및 웹 ACL 규칙 및 규칙 그룹 평가 단원을 참조하세요.

CAPTCHA 또는 Challenge작업을 사용하는 경우 규칙에 필요한 만큼 면제 시간 구성을 조정하십시오. 설정을 지정하지 않으면 규칙이 웹 ACL에서 설정을 상속합니다. 웹 ACL 면제 시간 설정을 수정하려면 웹 ACL을 생성한 후 편집합니다. 면제 시간에 대한 자세한 내용은 타임스탬프 만료: AWS WAF 토큰 면역 시간 섹션을 참조하세요.

> **Note**
>
> 규칙 중 하나에서 또는 규칙 그룹 내 규칙 작업 재정의로서 CAPTCHA 또는 Challenge 규칙 작업을 사용하는 경우 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

요청 또는 응답을 사용자 지정하려면 해당 옵션을 선택하고 사용자 지정의 세부 정보를 입력합니다. 자세한 정보는 AWS WAF의 사용자 지정된 웹 요청 및 응답을 참조하세요.

규칙을 통해 일치하는 웹 요청에 레이블이 추가되도록 하려면 해당 옵션을 선택하고 레이블 세부 정보를 채웁니다. 자세한 정보는 AWS WAF 웹 요청의 레이블을 참조하세요.

d. 규칙 추가를 선택합니다.

14. 웹 ACL에 대한 기본 작업을 Block 또는 Allow으로 선택합니다. 이는 웹 ACL의 규칙이 요청을 명시적으로 허용 또는 차단하지 않을 때 요청에 대해 AWS WAF 취하는 조치입니다. 자세한 정보는 웹 ACL 기본 동작을 참조하세요.

기본 작업을 사용자 지정하려면 해당 옵션을 선택하고 사용자 지정의 세부 정보를 입력합니다. 자세한 정보는 AWS WAF의 사용자 지정된 웹 요청 및 응답을 참조하세요.

15. 토큰 도메인 목록을 정의하여 보호된 애플리케이션 간에 토큰을 공유하도록 할 수 있습니다. 토큰은 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP), AWS WAF 사기 통제 계정 탈취 방지 (ATP) 및 봇 제어를 위한 AWS 관리형 규칙 그룹을 사용할 때 구현하는 및 Challenge 작업과 애플리케이션 통합 SDK에서 사용됩니다. CAPTCHA AWS WAF

    공개 접미사는 허용되지 않습니다. 예를 들면 `gov.au` 또는 `co.uk`를 토큰 도메인으로 사용할 수 없습니다.

    기본적으로 보호된 리소스의 도메인에 대한 토큰만 AWS WAF 허용합니다. 이 목록에 토큰 도메인을 추가하는 경우 목록에 있는 모든 도메인과 관련 리소스의 도메인에 대해 토큰을 AWS WAF 수락합니다. 자세한 정보는 AWS WAF 웹 ACL 토큰 도메인 목록 구성을 참조하세요.

16. 다음을 선택하세요.
17. 규칙 우선순위 설정 페이지에서 규칙과 규칙 그룹을 선택하고 AWS WAF 처리하려는 순서대로 이동합니다. AWS WAF 목록 상단에서 시작하여 규칙을 처리합니다. 웹 ACL은 저장하면 AWS WAF는 나열된 순서대로 규칙에 숫자 우선 순위 설정을 할당합니다. 자세한 정보는 웹 ACL의 규칙 및 규칙 그룹 처리 순서을 참조하세요.
18. 다음을 선택하세요.
19. 지표 구성 페이지에서 옵션을 검토하고 필요한 업데이트를 적용합니다. 여러 소스에 동일한 CloudWatch 지표 이름을 제공하여 여러 소스의 지표를 결합할 수 있습니다.
20. 다음을 선택합니다.
21. Review and create web ACL(웹 ACL 검토 및 생성) 페이지에서 사용자 정의를 확인합니다. 영역을 변경하려면 해당 영역에 대해 편집을 선택합니다. 그러면 웹 ACL 마법사의 페이지로 돌아갑니다. 변경한 후 페이지에서 계속 다음을 선택하여 웹 ACL 검토 및 생성 페이지로 돌아옵니다.
22. Create web ACL(웹 ACL 생성)을 선택합니다. 새 웹 ACL이 Web ACLs(웹 ACL) 페이지에 나열됩니다.

웹 ACL 편집

웹 ACL에서 규칙을 추가 또는 제거하거나 구성 설정을 변경하려면 이 페이지의 절차를 사용하여 웹 ACL에 액세스합니다. 웹 ACL을 업데이트하는 동안 웹 ACL과 연결된 리소스를 지속적으로 AWS WAF 제공합니다.

프로덕션 트래픽 위험

프로덕션 트래픽용 웹 ACL에 변경 사항을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 변경 사항을 테스트하고 조정하십시오. 그런 다음 업데이트된 규칙을 프로덕션 트래픽과 함께 계산 모드에서 테스트하고 조정한 다음 활성화하십시오. 자세한 지침은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

Note

웹 ACL에서 1,500개가 넘는 WCU를 사용하면 기본 웹 ACL 가격을 초과하는 비용이 발생합니다. 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 및 AWS WAF 요금을 참조하세요.

웹 ACL을 편집하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. 편집하려는 웹 ACL의 명칭을 선택합니다. 콘솔에서 웹 ACL의 설명으로 이동합니다.

   Note

   에서 관리하는 웹 ACL의 AWS Firewall Manager 이름은 로 `FMManagedWebACLV2-` 시작합니다. 방화벽 관리자 관리자는 방화벽 관리자 AWS WAF 정책에서 이러한 사항을 관리합니다. 이러한 웹 ACL에는 추가하고 관리하는 규칙 또는 규칙 그룹의 양쪽에 있는 웹 ACL에서 첫 번째 및 마지막으로 실행하도록 지정된 규칙 그룹 집합이 포함될 수 있습니다. 이러한 첫 번째 및 마지막 규칙 그룹 사양 중 어느 것도 변경할 수 없습니다. 첫 번째 및 마지막 규칙 그룹에는 각각 `PREFMManaged-` 및 `POSTFMManaged-`로 시작하는 이름이 지정됩니다. 이러한 정책에 대한 자세한 내용은 AWS WAF 정책을 참조하세요.

4. 필요에 따라 웹 ACL을 편집합니다. 관심 있는 구성 영역의 탭을 선택하고 변경 가능한 설정을 편집합니다. 편집하는 각 설정에 대해 저장을 선택하고 웹 ACL의 설명 페이지로 돌아가면 콘솔에서 웹 ACL에 대한 변경 내용이 저장됩니다.

   다음 목록에는 웹 ACL 구성 구성 요소를 포함하는 탭이 나와 있습니다.

   - 규칙 탭

- 웹 ACL에 정의된 규칙 - 웹 ACL을 생성할 때와 마찬가지로 웹 ACL에 정의한 규칙을 편집하고 관리할 수 있습니다.

  > **Note**
  >
  > 웹 ACL에 직접 추가하지 않은 규칙의 이름은 변경하면 안 됩니다. 다른 서비스를 사용하여 규칙을 관리하는 경우 해당 서비스의 이름을 변경하면 의도한 보호 기능을 제공하는 기능이 제거되거나 저하될 수 있습니다. AWS Shield Advanced AWS Firewall Manager 둘 다 웹 ACL에 규칙을 생성합니다. 자세한 내용은 다른 서비스에서 제공하는 규칙 그룹을 참조하세요.

  > **Note**
  >
  > 규칙 이름을 변경하고 규칙의 지표 이름에 변경 내용이 반영되도록 하려면 지표 이름도 업데이트해야 합니다. AWS WAF 규칙 이름을 변경할 때 규칙의 지표 이름을 자동으로 업데이트하지 않습니다. 콘솔에서 규칙을 편집할 때 규칙 JSON 편집기를 사용하여 지표 이름을 변경할 수 있습니다. API와 웹 ACL 또는 규칙 그룹을 정의하는 데 사용하는 JSON 목록을 통해 두 이름을 모두 변경할 수도 있습니다.

  규칙 및 규칙 그룹 설정에 대한 자세한 내용은 AWS WAF 규칙 및 AWS WAF 규칙 그룹 섹션을 참조하세요.
- 사용된 웹 ACL 규칙 용량 단위 - 웹 ACL의 현재 용량 사용량입니다. 보기 전용입니다.
- 어떤 규칙과도 일치하지 않는 요청에 대한 기본 웹 ACL 작업 - 이 설정에 대한 자세한 내용은 웹 ACL 기본 동작 섹션을 참조하세요.
- 웹 ACL CAPTCHA 및 챌린지 구성 — 이러한 면제 시간은 CAPTCHA 또는 챌린지 토큰의 획득 후 유효 기간을 결정합니다. 이 설정은 웹 ACL을 생성한 후에만 여기에서 수정할 수 있습니다. 이 설정에 대한 내용은 타임스탬프 만료: AWS WAF 토큰 면역 시간을 참조하세요.
- 토큰 도메인 목록 - 목록에 있는 모든 도메인과 관련 리소스의 도메인에 대한 토큰을 AWS WAF 수락합니다. 자세한 정보는 AWS WAF 웹 ACL 토큰 도메인 목록 구성을 참조하세요.

- 관련 AWS 리소스 탭
  - 웹 요청 검사 크기 제한 - CloudFront 배포를 보호하는 웹 ACL에만 포함됩니다. 신체 검사 크기 제한에 따라 검사를 위해 AWS WAF 전달되는 신체 구성품의 양이 결정됩니다. 이 설정에 대한 자세한 내용을 알아보려면 신체 검사 크기 제한 관리 섹션을 참조하세요.

    - 관련 AWS 리소스 — 웹 ACL이 현재 연결되고 보호하고 있는 리소스 목록입니다. 웹 ACL과 동일한 리전 내에 있는 리소스를 찾아 웹 ACL에 연결할 수 있습니다. 자세한 정보는 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.
  - 사용자 지정 응답 본문 탭
    - 작업이 Block으로 설정된 웹 ACL 규칙에서 사용할 수 있는 사용자 지정 응답 본문입니다. 자세한 정보는 Block 작업에 대한 사용자 지정 응답을 참조하세요.
  - 로깅 및 지표 탭
    - 로깅 - 웹 ACL에서 평가하는 트래픽에 대한 로깅입니다. 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅을 참조하세요.
    - 샘플링된 요청 - 웹 요청과 일치하는 규칙에 대한 정보입니다. 샘플링된 요청 보기에 대한 자세한 내용은 웹 요청 샘플 보기 섹션을 참조하세요.
    - CloudWatch 메트릭 - 웹 ACL의 규칙에 대한 메트릭입니다. Amazon CloudWatch 지표에 대한 자세한 내용은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 생성하거나 변경할 때 리소스가 저장된 모든 영역에 변경 사항이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

웹 ACL에서 규칙 그룹 동작 관리

이 단원에서는 웹 ACL에서 규칙 그룹을 사용하는 방법을 수정하는 옵션에 대해 설명합니다. 이 정보는 모든 규칙 그룹 유형에 적용됩니다. 웹 ACL에 규칙 그룹을 추가한 후 규칙 그룹에 있는 개별 규칙의 작업을 Count 또는 다른 유효한 규칙 작업 설정으로 재정의할 수 있습니다. 또한 규칙 그룹의 결과 작업

을 Count로 재정의할 수 있으며, 이 경우 규칙 그룹 내에서 규칙이 평가되는 방식에는 영향이 미치지 않습니다.

이러한 옵션에 대한 자세한 내용은 규칙 그룹의 작업 재정의 옵션 섹션을 참조하세요.

규칙 그룹에 대한 규칙 작업 재정의

웹 ACL의 각 규칙 그룹에서 모든 규칙 또는 일부 규칙에 대해 포함된 규칙의 작업을 재정의할 수 있습니다.

가장 일반적인 사용 사례는 규칙 작업을 Count로 재정의하여 새 규칙 또는 업데이트된 규칙을 테스트하는 경우입니다. 지표를 활성화한 경우 재정의한 각 규칙에 대한 지표를 받게 됩니다. 테스트에 대한 자세한 내용은 AWS WAF 보호 기능 테스트 및 조정 섹션을 참조하세요.

규칙 그룹에 대한 규칙 작업을 재정의하려면

웹 ACL에 관리형 규칙 그룹을 추가할 때 이러한 변경을 수행할 수 있으며 웹 ACL을 편집할 때 모든 유형의 규칙 그룹에 적용할 수 있습니다. 이러한 지침은 웹 ACL에 이미 추가된 규칙 그룹에 적용됩니다. 이 옵션에 대한 추가 정보는 에서 참조하십시오. 규칙 그룹 규칙 작업 재정의

1. 웹 ACL을 편집합니다.
2. 웹 ACL 페이지의 규칙 탭에서 규칙 그룹을 선택한 다음 편집을 선택합니다.
3. 규칙 그룹의 규칙 섹션에서 필요에 따라 작업 설정을 관리합니다.
   - 모든 규칙 - 규칙 그룹의 모든 규칙에 대해 재정의 작업을 설정하려면 모든 규칙 작업 재정의 드롭다운을 열고 재정의 작업을 선택합니다. 모든 규칙의 재정의를 제거하려면 모든 재정의 제거를 선택합니다.
   - 단일 규칙 - 단일 규칙에 대해 재정의 작업을 설정하려면 규칙의 드롭다운을 열고 재정의 작업을 선택합니다. 규칙의 재정의를 제거하려면 규칙의 드롭다운을 열고 재정의 제거를 선택합니다.
4. 변경 작업을 마치면 규칙 저장을 선택합니다. 규칙 작업 및 재정의 작업 설정은 규칙 그룹 페이지에 나열되어 있습니다.

다음의 JSON 목록 예제는 규칙 `CategoryVerifiedSearchEngine` 및 `CategoryVerifiedSocialMedia`에 대한 규칙 작업을 Count로 재정의하는 웹 ACL 내부의 규칙 그룹 선언을 보여줍니다. JSON에서는 각 개별 규칙마다 `RuleActionOverrides` 항목을 제공하여 모든 규칙 작업을 재정의합니다.

```
{
```

```
    "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesBotControlRuleSet",
        "RuleActionOverrides": [
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSearchEngine"
          },
          {
            "ActionToUse": {
              "Count": {}
            },
            "Name": "CategoryVerifiedSocialMedia"
          }
        ],
        "ExcludedRules": []
    },
   "VisibilityConfig": {
       "SampledRequestsEnabled": true,
       "CloudWatchMetricsEnabled": true,
       "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

규칙 그룹의 평가 결과를 Count로 재정의

규칙 그룹의 규칙이 구성되거나 평가되는 방식을 변경하지 않고도 규칙 그룹 평가로 인해 발생하는 작업을 재정의할 수 있습니다. 이 옵션은 일반적으로 사용되지 않습니다. 규칙 그룹의 규칙 중 하나라도 일치하는 경우 이 재정의는 규칙 그룹의 결과 동작을 Count로 설정합니다.

> **Note**
>
> 이는 흔하지 않은 사용 사례입니다. 대부분의 작업 재정의는 에 설명된 대로 규칙 그룹 내의 규칙 수준에서 수행됩니다. 규칙 그룹에 대한 규칙 작업 재정의

규칙 그룹을 추가하거나 편집할 때 웹 ACL에서 규칙 그룹의 결과 작업을 재정의할 수 있습니다. 콘솔에서 규칙 그룹의 규칙 그룹 재정의(선택 사항) 창을 열고 재정의를 활성화합니다. JSON에서는 다음 예제 목록에 표시된 것처럼 규칙 그룹 문에서 `OverrideAction`을 설정합니다.

```
{
   "Name": "AWS-AWSBotControl-Example",
   "Priority": 5,
   "Statement": {
    "ManagedRuleGroupStatement": {
     "VendorName": "AWS",
     "Name": "AWSManagedRulesBotControlRuleSet"
     }
   },
    "OverrideAction": {
       "Count": {}
    },
   "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSBotControl-Example"
   }
}
```

웹 ACL을 리소스와 연결 또는 연결 해제 AWS

를 AWS WAF 사용하여 웹 ACLS와 리소스 간에 다음과 같은 연결을 생성할 수 있습니다.

- 리전 웹 ACL을 아래 나열된 리전 리소스 중 하나와 연결합니다. 이 옵션의 경우 웹 ACL이 리소스와 동일한 리전에 있어야 합니다.
  - Amazon API Gateway REST API
  - Application Load Balancer
  - AWS AppSync GraphQL API
  - Amazon Cognito 사용자 풀
  - AWS App Runner 서비스
  - AWS 검증된 액세스 인스턴스
- 글로벌 웹 ACL을 Amazon CloudFront 배포와 연결합니다. 글로벌 웹 ACL에 미국 동부 (버지니아 북부) 리전이 하드 코딩됩니다.

CloudFront 배포 자체를 생성하거나 업데이트할 때 웹 ACL을 배포에 연결할 수도 있습니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 콘텐츠 액세스 제어를 위한 사용을 AWS WAF 참조하십시오.

다중 연결에 대한 제한 사항

다음 제한 사항에 따라 단일 웹 ACL을 하나 이상의 AWS 리소스와 연결할 수 있습니다.

- 각 AWS 리소스를 하나의 웹 ACL과만 연결할 수 있습니다. 웹 ACL과 AWS 리소스 간의 관계는 다음과 같습니다. one-to-many
- 웹 ACL을 하나 이상의 CloudFront 배포와 연결할 수 있습니다. CloudFront 배포와 연결한 웹 ACL을 다른 AWS 리소스 유형과 연결할 수 없습니다.

추가 제한 사항

웹 ACL 연결에 적용되는 추가 제한은 다음과 같습니다.

- 웹 ACL은 AWS 리전안에 있는 Application Load Balancer에만 연결할 수 있습니다. 예를 들어, AWS Outposts에 있는 Application Load Balancer에는 웹 ACL을 연결할 수 없습니다.
- Amazon Cognito 사용자 풀을 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 관리 규칙 그룹 `AWSManagedRulesACFPRuleSet` 또는 사기 통제 계정 탈취 방지 (ATP) 관리 규칙 그룹을 사용하는 웹 ACL과 연결할 수 없습니다. AWS WAF `AWSManagedRulesATPRuleSet` 계정 생성 사기 방지에 대한 자세한 내용은 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 섹션을 참조하세요. 계정 탈취 방지에 대한 자세한 내용은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 섹션을 참조하세요.

> ⚠ 프로덕션 트래픽 위험
>
> 프로덕션 트래픽용 웹 ACL을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 변경 사항을 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 계수 모드에서 테스트하고 조정한 다음 활성화합니다. 자세한 지침은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

웹 ACL을 리소스에 연결하려면 AWS

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 [Web ACLs]를 선택합니다.

3. 리소스와 연결할 웹 ACL 이름을 선택합니다. 콘솔에서 웹 ACL의 설명으로 이동하여 여기에서 설명을 편집할 수 있습니다.
4. 관련 AWS 리소스 탭에서 AWS 리소스 추가를 선택합니다.
5. 메시지가 표시되면 리소스 유형을 선택하고 연결할 리소스 옆에 있는 라디오 버튼을 선택한 다음 추가를 선택합니다.

리소스에서 웹 ACL의 연결을 끊으려면 AWS

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. 리소스에서 연결을 해제할 웹 ACL의 이름을 선택합니다. 콘솔에서 웹 ACL의 설명으로 이동하여 여기에서 설명을 편집할 수 있습니다.
4. 관련 AWS 리소스 탭에서 이 웹 ACL의 연결을 끊을 리소스를 선택합니다.

> **Note**
>
> 한 번에 하나의 리소스만 연결 해제해야 합니다. 리소스를 여러 개 선택하지 마세요.

5. 연결 해제를 선택합니다. 콘솔에 확인 대화상자가 열립니다. 리소스에서 웹 ACL의 연결을 끊으려면 선택을 확인하십시오. AWS

웹 ACL 삭제

웹 ACL을 삭제하려면 먼저 웹 ACL에서 모든 AWS 리소스 연결을 끊습니다. 다음 절차를 수행하십시오.

웹 ACL을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. 삭제하려는 웹 ACL의 이름을 선택합니다. 콘솔에서 웹 ACL의 설명으로 이동하여 여기에서 설명을 편집할 수 있습니다.
4. 연결된 리소스 탭에서 각 관련 AWS 리소스에 대해 리소스 이름 옆에 있는 라디오 버튼을 선택한 다음 연결 해제를 선택합니다. 이렇게 하면 웹 ACL이 리소스에서 분리됩니다. AWS

5. 탐색 창에서 [Web ACLs]를 선택합니다.
6. 삭제할 웹 ACL 옆에 있는 라디오 단추를 선택한 다음 삭제를 선택합니다.

AWS WAF 규칙 그룹

규칙 그룹은 웹 ACL에 추가할 수 있는 재사용 가능한 규칙 집합입니다. 웹 ACL에 대한 자세한 내용은 AWS WAF 웹 액세스 제어 목록 (웹 ACL) 섹션을 참조하세요..

규칙 그룹은 다음 주요 범주로 나뉩니다.

- 생성 및 유지 관리하는 자체 규칙 그룹
- 관리형 규칙 팀이 사용자를 위해 생성하고 AWS 관리하는 관리형 규칙 그룹입니다.
- AWS Marketplace 셀러가 대신 생성하고 유지 관리하는 관리형 규칙 그룹.
- Shield AWS Firewall Manager Advanced와 같은 다른 서비스에서 소유하고 관리하는 규칙 그룹

규칙 그룹과 웹 ACL 간의 차이점

규칙 그룹과 웹 ACL 모두 두 위치에서 동일한 방식으로 정의된 규칙을 포함합니다. 규칙 그룹은 다음과 같은 방식으로 웹 ACL과 다릅니다.

- 규칙 그룹은 규칙 그룹 참조 문을 포함할 수 없습니다.
- 각 웹 ACL에 규칙 그룹 참조 문을 추가하여 단일 규칙 그룹을 여러 웹 ACL에서 재사용할 수 있습니다. 웹 ACL은 재사용할 수 없습니다.
- 규칙 그룹에는 기본 작업이 없습니다. 웹 ACL에서는 포함하는 각 규칙 또는 규칙 그룹에 대해 기본 작업을 설정합니다. 규칙 그룹 또는 웹 ACL 내의 각 개별 규칙에는 정의된 작업이 있습니다.
- 규칙 그룹을 AWS 리소스에 직접 연결할 수는 없습니다. 규칙 그룹을 사용하여 리소스를 보호하려면 웹 ACL에서 규칙 그룹을 사용합니다.
- 웹 ACL에는 5,000 웹 ACL 용량 단위(WCU)의 시스템 정의 최대 용량이 있습니다. 각 규칙 그룹에는 생성 시 설정해야 하는 WCU 설정이 있습니다. 이 설정을 통해 규칙 그룹을 사용하여 웹 ACL에 추가할 추가 용량 요구 사항을 계산할 수 있습니다. WCU에 대한 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 섹션을 참조하세요.

규칙에 대한 자세한 내용은 AWS WAF 규칙 단원을 참조하세요.

이 섹션에서는 자체 규칙 그룹을 생성하고 관리하도록 필요한 지침을 제공하고, 사용자에게 제공되는 관리형 규칙 그룹에 대해 설명하며, 관리형 규칙 그룹을 사용하는 데 필요한 지침을 제공합니다.

주제

관리형 규칙 그룹

관리형 규칙 그룹은 AWS Marketplace 셀러가 대신 작성하고 유지 관리하는 사전 정의된 ready-to-use 규칙 모음입니다. AWS 기본 AWS WAF 가격은 모든 관리형 규칙 그룹 사용에 적용됩니다. AWS WAF 가격 정보는 AWS WAF 요금을 참조하십시오.

- AWS WAF 봇 제어, ATP (AWS WAF 사기 통제 계정 탈취 방지) 및 ACFP (AWS WAF 사기 통제 계정 생성 사기 방지) 에 대한 AWS 관리형 규칙 그룹은 기본 요금 외에 추가 비용을 지불하고 이용할 수 있습니다. AWS WAF 요금에 대한 자세한 내용은 AWS WAF Pricing을 참조하세요.
- AWS WAF 고객은 다른 모든 AWS 관리형 규칙 규칙 그룹을 추가 비용 없이 사용할 수 있습니다.
- AWS Marketplace 구독을 통해 관리형 규칙 그룹을 사용할 수 AWS Marketplace있습니다. 각 규칙 그룹은 AWS Marketplace 판매자가 소유하고 관리합니다. AWS Marketplace 관리형 규칙 그룹을 사용하기 위한 가격 정보는 AWS Marketplace 판매자에게 문의하십시오.

일부 관리형 규칙 그룹은 Joomla 또는 PHP와 같은 WordPress 특정 유형의 웹 애플리케이션을 보호하는 데 도움이 되도록 설계되었습니다. 다른 관리형 규칙 그룹은 알려진 위협 또는 일반적인 웹 애플리케이션 취약성(예: OWASP Top 10에 나열된 취약성)에 대한 폭넓은 보호를 제공합니다. PCI 또는 HIPAA 등의 규제를 준수해야 하는 경우 관리형 규칙 그룹을 사용하여 웹 애플리케이션 방화벽 요구 사항을 충족할 수 있습니다.

자동 업데이트

끊임없이 변화하는 위협 환경을 놓치지 않고 파악하려면 많은 시간과 비용이 들 수 있습니다. 관리형 규칙 그룹은 AWS WAF구현 및 사용 시 시간을 절약할 수 있습니다. 많은 AWS Marketplace 판매자들은 새로운 취약성 AWS 및 위협이 발견되면 관리형 규칙 그룹을 자동으로 업데이트하고 새 버전의 규칙 그룹을 제공합니다.

여러 비공개 공개 AWS 커뮤니티에 참여하고 있기 때문에 공개되기 전에 새로운 취약성에 대한 알림을 받는 경우도 있습니다. 이러한 경우 새로운 위협이 널리 알려지기 전에도 AWS Managed Rules 규칙 그룹을 업데이트하여 배포할 AWS 수 있습니다.

관리형 규칙 그룹의 규칙에 대한 제한된 액세스

각 관리형 규칙 그룹은 보호를 위해 설계된 공격 유형 및 취약성에 대한 포괄적인 설명을 제공합니다. 규칙 그룹 제공자의 지적 재산을 보호하기 위해 규칙 그룹 내의 개별 규칙에 대한 모든 세부 정보를 볼 수 없습니다. 이러한 제한을 통해 악의적인 사용자가 게시된 규칙을 교묘하게 회피하는 위협을 설계하는 것을 방지할 수 있습니다.

주제

- 버전이 지정된 관리형 규칙 그룹
- 관리형 규칙 그룹 작업
- AWS 에 대한 관리형 규칙 AWS WAF
- AWS Marketplace 관리형 규칙 그룹

버전이 지정된 관리형 규칙 그룹

많은 관리형 규칙 그룹 공급자는 버전 관리를 사용하여 규칙 그룹의 옵션과 기능을 업데이트합니다. 일반적으로 관리형 규칙 그룹의 특정 버전은 정적 버전입니다. 예를 들어, 공급자는 새로운 보안 위협에 대응하기 위해 관리형 규칙 그룹의 일부 또는 모든 정적 버전을 업데이트해야 할 수 있습니다.

웹 ACL에서 버전이 지정된 관리형 규칙 그룹을 사용하는 경우 기본 버전을 선택하여 공급자가 사용하는 정적 버전을 관리하도록 하거나 사용자가 특정 정적 버전을 선택할 수 있습니다.

원하는 버전을 찾을 수 없나요?

규칙 그룹의 버전 목록에 버전이 없으면 해당 버전은 만료 예정이거나 이미 만료되었을 수 있습니다. 버전 만료가 예약된 후에는 더 AWS WAF 이상 규칙 그룹에 사용할 버전을 선택할 수 없습니다.

AWS 관리형 규칙 규칙 그룹에 대한 SNS 알림

AWS 관리형 규칙 그룹은 IP 평판 규칙 그룹을 제외한 모든 버전 관리 및 SNS 업데이트 알림을 제공합니다. 알림을 제공하는 AWS 관리형 규칙 그룹은 모두 동일한 SNS 주제 Amazon 리소스 이름 (ARN)을 사용합니다. SNS 알림을 신청하려면 을 참조하십시오새 버전 및 업데이트에 대한 알림 받기.

주제

- 관리형 규칙 그룹의 버전 수명 주기
- 관리형 규칙 그룹의 버전 만료
- 관리형 규칙 그룹 버전 처리 모범 사례

관리형 규칙 그룹의 버전 수명 주기

공급자는 관리형 규칙 그룹 정적 버전의 다음 수명 주기 단계를 처리합니다.

- 릴리스 및 업데이트 — 관리형 규칙 그룹 공급자는 Amazon Simple Notification Service(Amazon SNS) 주제에 대한 알림을 통해 관리형 규칙 그룹의 향후 및 새로운 정적 버전을 발표합니다. 공급자는 이 주제를 사용하여 긴급 필수 업데이트와 같은 규칙 그룹에 대한 기타 중요한 정보를 전달할 수도 있습니다.

  규칙 그룹의 주제를 구독하고 알림 수신 방법을 구성할 수 있습니다. 자세한 내용은 새 버전 및 업데이트에 대한 알림 받기단원을 참조하세요.
- 만료 예약 — 관리형 규칙 그룹 공급자가 규칙 그룹의 이전 버전이 만료되도록 예약합니다. 만료될 예정인 버전은 웹 ACL 규칙에 추가할 수 없습니다. 특정 버전의 만료가 예약된 후 CloudWatch Amazon에서 카운트다운 지표를 사용하여 만료를 AWS WAF 추적합니다.
- 버전 만료 - 관리형 규칙 그룹의 만료된 버전을 사용하도록 웹 ACL을 구성한 경우 웹 ACL 평가 중에 규칙 그룹의 기본 버전이 AWS WAF 사용됩니다. 또한 규칙 그룹을 제거하지 않거나 해당 버전을 만료되지 않은 버전으로 변경하지 않는 웹 ACL의 모든 업데이트를 AWS WAF 차단합니다.

AWS Marketplace 관리형 규칙 그룹을 사용하는 경우 공급자에게 버전 수명 주기에 대한 추가 정보를 문의하세요.

관리형 규칙 그룹의 버전 만료

특정 버전의 규칙 그룹을 사용하는 경우 만료 날짜가 지난 버전을 계속 사용해서는 안 됩니다. 규칙 그룹의 SNS 알림과 Amazon CloudWatch 지표를 통해 버전 만료를 모니터링할 수 있습니다.

웹 ACL에서 사용 중인 버전이 만료된 경우, 규칙 그룹을 만료되지 않은 버전으로 이동하는 것을 포함하지 않는 웹 ACL 업데이트를 모두 AWS WAF 차단합니다. 규칙 그룹을 사용 가능한 버전으로 업데이트하거나 웹 ACL에서 제거할 수 있습니다.

관리형 규칙 그룹의 만료 처리는 규칙 그룹 공급자에 따라 다릅니다. AWS 관리형 규칙 규칙 그룹의 경우 만료된 버전이 규칙 그룹의 기본 버전으로 자동 변경됩니다. AWS Marketplace 규칙 그룹의 경우 공급자에게 만료 처리 방법을 문의하세요.

공급자는 새 버전의 규칙 그룹을 생성할 때 해당 버전의 예상 수명을 설정합니다. 버전이 만료될 예정은 없지만 Amazon CloudWatch 지표 값은 예측 수명 설정으로 설정되며, 이 경우 지표에 CloudWatch 대한 고정 값이 표시됩니다. 공급자가 지표 만료를 예약한 후에는 만료일이 되어 0에 도달할 때까지 지표 값이 매일 감소합니다. 만료 모니터링에 대한 자세한 내용은 을 참조하십시오. 버전 만료 추적

관리형 규칙 그룹 버전 처리 모범 사례

버전이 관리되는 관리형 규칙 그룹을 사용하는 경우 이 모범 사례 지침에 따라 버전 관리를 처리합니다.

웹 ACL에서 관리형 규칙 그룹을 사용하는 경우 규칙 그룹의 특정 정적 버전을 사용하거나 기본 버전을 사용하도록 선택할 수 있습니다.

- 기본 버전 - AWS WAF 항상 기본 버전을 공급자가 현재 권장하는 정적 버전으로 설정합니다. 공급자가 권장 정적 버전을 업데이트하는 경우 AWS WAF 에서 웹 ACL의 규칙 그룹에 대한 기본 버전 설정이 자동으로 업데이트됩니다.

  관리형 규칙 그룹의 기본 버전을 사용하는 경우 모범 사례로서 다음을 수행합니다.

  - 알림 구독 — 규칙 그룹 변경 사항에 대한 알림을 구독하여 최신 상태를 유지합니다. 대부분의 공급자는 새로운 정적 버전과 기본 버전 변경에 대한 고급 알림을 보냅니다. 이를 통해 기본 버전을 AWS 전환하기 전에 새 정적 버전의 영향을 확인할 수 있습니다. 자세한 내용은 새 버전 및 업데이트에 대한 알림 받기단원을 참조하세요.
  - 기본 버전을 정적 버전으로 설정하기 전에 정적 버전 설정의 영향을 검토하고 필요에 따라 조정 - 기본 버전을 새 정적 버전으로 설정하기 전에 정적 버전이 웹 요청의 모니터링 및 관리에 미치는 영향을 검토합니다. 새 정적 버전에는 검토해야 할 새 규칙이 있을 수 있습니다. 규칙 그룹 사용 방식을 수정해야 하는 경우 거짓 긍정이나 기타 예기치 않은 동작이 있는지 살펴봅니다. 예를 들어, 새 동작을 어떻게 처리할지 결정하는 동안 트래픽을 차단하지 못하도록 규칙을 count로 설정할 수 있습니다. 자세한 정보는 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.
- 정적 버전 - 정적 버전을 사용하기로 선택한 경우 규칙 그룹의 새 버전을 채택할 준비가 되면 버전 설정을 수동으로 업데이트해야 합니다.

  관리형 규칙 그룹의 정적 버전을 사용하는 경우 모범 사례로서 다음을 수행합니다.

  - 버전을 최신 상태로 유지 - 관리형 규칙 그룹을 가능한 최신 버전으로 유지합니다. 새 버전이 출시되면 이를 테스트하고 필요에 따라 설정을 조정하여 적시에 구현합니다. 테스트에 대한 자세한 내용은 AWS WAF 보호 기능 테스트 및 조정 섹션을 참조하세요.
  - 알림 구독 — 규칙 그룹 변경에 대한 알림을 구독하여 공급자가 언제 새로운 정적 버전을 출시하는지 알 수 있습니다. 대부분의 공급자는 버전 변경에 대한 사전 알림을 제공합니다. 또한 공급자는 보안 허점을 제거하거나 그 밖의 긴급한 이유로 사용 중인 정적 버전을 업데이트해야 할 수도 있습니다. 공급자의 알림을 구독하면 현 상황을 파악할 수 있습니다. 자세한 정보는 새 버전 및 업데이트에 대한 알림 받기을 참조하세요.
  - 버전 만료 방지 — 정적 버전을 사용하는 동안 만료되지 않도록 하세요. 공급자의 만료된 버전에 대한 처리는 다양할 수 있으며, 여기에는 사용 가능한 버전으로의 강제 업그레이드 또는 예상치 못

한 결과를 초래할 수 있는 기타 변경 사항이 포함될 수 있습니다. AWS WAF 만료 지표를 추적하고 지원되는 버전으로 성공적으로 업그레이드할 수 있는 충분한 일수를 알려주는 경보를 설정하십시오. 자세한 내용은 버전 만료 추적을(를) 참조하세요.

관리형 규칙 그룹 작업

이 섹션에서는 관리형 규칙 그룹에 액세스하고 관리하기 위한 지침을 제공합니다.

웹 ACL에 관리형 규칙 그룹을 추가할 때 자체 규칙 그룹과 동일한 구성 옵션과 추가 설정을 선택할 수 있습니다.

콘솔을 통해 웹 ACL에서 규칙을 추가하고 편집하는 과정에서 관리형 규칙 그룹 정보에 액세스할 수 있습니다. API와 명령줄 인터페이스(CLI)를 통해 관리형 규칙 그룹 정보를 직접 요청할 수 있습니다.

웹 ACL에서 관리형 규칙 그룹을 사용하는 경우 다음 설정을 편집할 수 있습니다.

- 버전 - 규칙 그룹의 버전이 관리되는 경우에만 사용할 수 있습니다. 자세한 정보는 버전이 지정된 관리형 규칙 그룹을 참조하세요.
- 규칙 작업 재정의 - 규칙 그룹에 있는 규칙에 대한 작업을 모든 작업으로 재정의할 수 있습니다. 작업을 Count로 설정하면 규칙 그룹을 사용하기 전에 테스트할 수 있어 웹 요청을 관리하는 데 유용합니다. 자세한 정보는 규칙 그룹 규칙 작업 재정의을 참조하세요.
- 범위 축소 명령문 — 범위 축소 문을 추가하면 규칙 그룹을 사용하여 평가하지 않을 웹 요청을 필터링할 수 있습니다. 자세한 정보는 범위 축소 문을 참조하세요.
- 규칙 그룹 작업 재정의 - 규칙 그룹 평가의 결과로 발생하는 작업을 재정의하고 이 작업을 Count 전용으로 설정할 수 있습니다. 이 옵션은 일반적으로 사용되지 않습니다. 규칙 그룹의 규칙 AWS WAF 평가 방법은 바뀌지 않습니다. 자세한 정보는 규칙 그룹은 액션 오버라이드를 다음으로 반환합니다. Count을 참조하세요.

웹 ACL에서 관리형 규칙 그룹 설정을 편집하려면

- 콘솔
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가할 때 편집을 선택하여 설정을 보고 편집할 수 있습니다.
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가한 후 웹 ACL 페이지에서 방금 생성한 웹 ACL을 선택합니다. 이렇게 하면 웹 ACL 편집 페이지로 이동합니다.
    - 규칙을 선택합니다.

    - 규칙 그룹을 선택한 다음 편집을 선택하여 설정을 보고 편집합니다.
- API 및 CLI — 콘솔 외부에서 웹 ACL을 생성하고 업데이트할 때 관리형 규칙 그룹 설정을 관리할 수 있습니다.

관리형 규칙 그룹 목록 검색

웹 ACL에서 사용할 수 있는 관리형 규칙 그룹의 목록을 검색할 수 있습니다. 목록에는 다음이 포함됩니다.

- 모든 AWS 관리형 규칙 규칙 그룹
- 구독한 AWS Marketplace 규칙 그룹.

> **Note**
>
> AWS Marketplace 규칙 그룹 구독에 대한 자세한 내용은 을 참조하십시오. AWS Marketplace 관리형 규칙 그룹

관리형 규칙 그룹 목록을 검색하면 반환되는 목록은 사용 중인 인터페이스에 따라 달라집니다.

- 콘솔 - 콘솔을 통해 아직 구독하지 않은 규칙 그룹을 비롯한 모든 관리형 AWS Marketplace 규칙 그룹을 볼 수 있습니다. 아직 구독하지 않은 사용자의 경우 인터페이스에서 사용자에게 구독을 안내하는 링크를 제공합니다.
- API 및 CLI — 콘솔 외부에서 요청은 사용 가능한 규칙 그룹만 반환합니다.

관리형 규칙 그룹 목록을 검색하려면

- 콘솔 – 웹 ACL을 생성하는 동안 규칙 및 규칙 그룹 추가 페이지에서 관리형 그룹 추가를 선택합니다. 최상위 수준에는 공급업체 이름이 나열됩니다. 각 공급업체 목록을 확장하여 관리형 규칙 그룹 목록을 확인합니다. 버전 관리된 규칙 그룹의 경우 이 수준에 표시된 정보는 기본 버전에 적용됩니다. 관리형 규칙 그룹을 웹 ACL에 추가하면 콘솔에 명명 체계 `<Vendor Name>-<Managed Rule Group Name>`에 따라 해당 그룹이 나열됩니다.
- API –
    - `ListAvailableManagedRuleGroups`
- CLI –

- `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

관리형 규칙 그룹의 규칙 검색

관리형 규칙 그룹의 규칙 목록을 검색할 수 있습니다. API 및 CLI 호출은 JSON 모델에서 또는 이를 통해 참조할 수 있는 규칙 사양을 반환합니다. AWS CloudFormation

관리형 규칙 그룹의 규칙 목록을 검색하려면

- 콘솔
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가할 때 편집을 선택하여 규칙을 볼 수 있습니다.
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가한 후 웹 ACL 페이지에서 방금 생성한 웹 ACL을 선택합니다. 이렇게 하면 웹 ACL 편집 페이지로 이동합니다.
    - 규칙을 선택합니다.
    - 규칙 목록을 보려는 규칙 그룹을 선택한 다음 편집을 선택합니다. AWS WAF 규칙 그룹의 규칙 목록을 표시합니다.
- API – `DescribeManagedRuleGroup`
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

관리형 규칙 그룹에 대해 사용 가능한 버전 검색

관리형 규칙 그룹의 사용 가능한 버전은 아직 만료가 예정되지 않은 버전입니다. 목록에 규칙 그룹에 대한 현재 기본 버전이 표시됩니다.

관리형 규칙 그룹의 사용 가능한 버전 목록을 검색하려면

- 콘솔
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가할 때 편집을 선택하여 규칙 그룹의 정보를 확인합니다. 버전 드롭다운을 확장하여 사용 가능한 버전 목록을 확인합니다.
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가한 후 웹 ACL에서 편집을 선택한 다음 규칙 그룹 규칙을 선택하고 편집합니다. 버전 드롭다운을 확장하여 사용 가능한 버전 목록을 확인합니다.
- API –
  - `ListAvailableManagedRuleGroupVersions`
- CLI –

- `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

콘솔을 통해 웹 ACL에 관리형 규칙 그룹 추가

이 지침은 모든 AWS 관리형 규칙 그룹 및 구독한 AWS Marketplace 규칙 그룹에 적용됩니다.

> **⚠ 프로덕션 트래픽 위험**
>
> 프로덕션 트래픽용 웹 ACL에 변경 사항을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 변경 사항을 테스트하고 조정하십시오. 그런 다음 업데이트된 규칙을 프로덕션 트래픽과 함께 계산 모드에서 테스트하고 조정한 다음 활성화하십시오. 자세한 지침은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

> **Note**
>
> 웹 ACL에서 1,500개가 넘는 WCU를 사용하면 기본 웹 ACL 가격을 초과하는 비용이 발생합니다. 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 및 AWS WAF 요금을 참조하세요.

콘솔을 통해 웹 ACL에 관리형 규칙 그룹을 추가하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 웹 ACL를 선택합니다.
3. 웹 ACL 페이지의 웹 ACL 목록에서 규칙 그룹을 추가할 대상 ACL을 선택합니다. 이렇게 하면 단일 웹 ACL에 대한 페이지로 이동합니다.
4. 웹 ACL의 페이지에서 규칙 탭을 선택합니다.
5. 규칙 창에서 규칙 추가를 선택한 다음 관리형 규칙 그룹 추가를 선택합니다.
6. 관리형 규칙 그룹 추가 페이지에서 규칙 그룹 공급자의 선택 항목을 확장하여 사용 가능한 규칙 그룹 목록을 확인합니다.
7. 추가하려는 각 규칙 그룹에 대해 웹 ACL에 추가를 선택합니다. 규칙 그룹에 대한 웹 ACL의 구성을 변경하려면 편집을 선택하고 변경한 다음 규칙 저장을 선택합니다. 옵션에 대한 자세한 내용은

버전이 지정된 관리형 규칙 그룹의 버전 관리 지침 및 웹 ACL의 관리형 규칙 그룹 사용 지침을 참조하세요. 관리형 규칙 그룹 문

8. 관리형 규칙 그룹 추가 페이지 하단에서 규칙 추가를 선택합니다.
9. 규칙 우선 순위 설정 페이지에서 필요에 따라 규칙 실행 순서를 조정한 다음 저장을 선택합니다. 자세한 정보는 웹 ACL의 규칙 및 규칙 그룹 처리 순서을 참조하세요.

웹 ACL 페이지의 규칙 탭 아래에는 추가한 관리형 규칙 그룹이 나열됩니다.

보호 기능을 프로덕션 트래픽에 사용하기 전에 AWS WAF 보호 기능의 변경 사항을 테스트하고 조정하십시오. 자세한 내용은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 생성하거나 변경하는 경우 리소스가 저장된 모든 영역에 변경 사항이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

관리형 규칙 그룹의 새 버전 및 업데이트에 대한 알림 받기

관리형 규칙 그룹 공급자는 SNS 알림을 사용하여 출시될 새 버전 및 긴급 보안 업데이트와 같은 규칙 그룹 변경 사항을 알립니다.

SNS 알림을 구독하는 방법

규칙 그룹의 알림을 구독하려면 미국 동부(버지니아 북부) 리전 us-east-1에서 규칙 그룹의 Amazon SNS 주제 ARN에 대한 Amazon SNS 구독을 생성합니다.

구독하는 방법에 대한 정보는 Amazon Simple Notification Service 개발자 안내서를 참조하세요.

> **Note**
>
> us-east-1 리전에서만 SNS 주제에 대한 구독을 생성하십시오.

버전이 지정된 AWS 관리형 규칙 그룹은 모두 동일한 SNS 주제 Amazon 리소스 이름 (ARN) 을 사용합니다. AWS 관리형 규칙 규칙 그룹 알림에 대한 자세한 내용은 을 참조하십시오. 배포 알림

관리형 규칙 그룹에 대한 Amazon SNS 주제 ARN을 찾을 수 있는 위치

AWS 관리형 규칙 규칙 그룹은 단일 SNS 주제 ARN을 사용하므로 규칙 그룹 중 하나에서 주제 ARN을 검색하고 이를 구독하면 SNS 알림을 제공하는 모든 AWS 관리형 규칙 그룹에 대한 알림을 받을 수 있습니다.

- 콘솔
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가할 때 편집을 선택하여 규칙 그룹의 Amazon SNS 주제 ARN을 포함한 규칙 그룹의 정보를 확인합니다.
  - (선택 사항) 웹 ACL에 관리형 규칙 그룹을 추가한 후 웹 ACL에서 편집을 선택한 다음 규칙 그룹 규칙을 선택하고 편집하여 규칙 그룹의 Amazon SNS 주제 ARN을 확인합니다.
- API – `DescribeManagedRuleGroup`
- CLI – `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Amazon SNS 알림 형식과 수신한 알림을 필터링하는 방법에 대한 일반적인 정보는 Amazon Simple Notification Service 개발자 안내서의 메시지 형식 구문 분석 및 Amazon SNS 구독 필터 정책을 참조하세요.

규칙 그룹의 버전 만료 추적

특정 버전의 규칙 그룹을 사용하는 경우 만료 날짜가 지난 버전을 계속 사용해서는 안 됩니다.

> **Tip**
>
> 관리형 규칙 그룹에 대한 Amazon SNS 알림에 가입하고 관리형 규칙 그룹 버전을 최신 상태로 유지하십시오. 규칙 그룹의 up-to-date 보호 기능을 최대한 활용하고 만료에 미리 대비할 수 있습니다. 자세한 내용은 새 버전 및 업데이트에 대한 알림 받기을 참조하세요.

Amazon을 통해 관리형 규칙 그룹의 만료 일정을 모니터링하려면 CloudWatch

1. 에서 CloudWatch 관리형 규칙 그룹의 만료 지표를 찾으십시오. AWS WAF 지표에는 다음과 같은 지표 이름과 측정기준이 있습니다.
   - 지표 이름: DaysToExpiry
   - 지표 차원: Region, ManagedRuleGroup, Vendor 및 Version

   웹 ACL에 트래픽을 평가하는 관리형 규칙 그룹이 있는 경우 이에 대한 지표를 얻게 됩니다. 사용하지 않는 규칙 그룹에는 지표를 사용할 수 없습니다.
2. 관심 있는 지표에 경보를 설정하여 새 버전의 규칙 그룹으로 전환하라는 알림을 제때 받을 수 있도록 하세요.

Amazon CloudWatch 지표 사용 및 경보 구성에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

JSON 및 YAML의 관리형 규칙 그룹 구성 예

API 및 CLI 호출은 JSON 모델에서 또는 이를 통해 참조할 수 있는 관리형 규칙 그룹의 모든 규칙 목록을 반환합니다. AWS CloudFormation

JSON

JSON을 사용하여 규칙 문 내에서 관리형 규칙 그룹을 참조하고 수정할 수 있습니다. 다음 목록은 AWS 관리형 규칙 그룹을 JSON `AWSManagedRulesCommonRuleSet` 형식으로 보여줍니다. RuleActionOverrides 사양에는 해당 작업이 Count로 재정의된 규칙이 나열되어 있습니다.

```
{
    "Name": "AWS-AWSManagedRulesCommonRuleSet",
    "Priority": 0,
    "Statement": {
      "ManagedRuleGroupStatement": {
        "VendorName": "AWS",
        "Name": "AWSManagedRulesCommonRuleSet",
        "RuleActionOverrides": [

          {

            "ActionToUse": {

              "Count": {}
```

```
            },

            "Name": "NoUserAgent_HEADER"

          }

        ],
        "ExcludedRules": []
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesCommonRuleSet"
    }
}
```

YAML

AWS CloudFormation YAML 템플릿을 사용하여 규칙 문 내에서 관리형 규칙 그룹을 참조하고 수정할 수 있습니다. 다음 목록은 AWS CloudFormation 템플릿의 AWS 관리 규칙 그룹 (AWSManagedRulesCommonRuleSet,) 을 보여줍니다. RuleActionOverrides 사양에는 해당 작업이 Count로 재정의된 규칙이 나열되어 있습니다.

```
Name: AWS-AWSManagedRulesCommonRuleSet
Priority: 0
Statement:
  ManagedRuleGroupStatement:
    VendorName: AWS
    Name: AWSManagedRulesCommonRuleSet
    RuleActionOverrides:
    - ActionToUse:
        Count: {}
      Name: NoUserAgent_HEADER
    ExcludedRules: []
OverrideAction:
  None: {}
VisibilityConfig:
  SampledRequestsEnabled: true
  CloudWatchMetricsEnabled: true
```

```
  MetricName: AWS-AWSManagedRulesCommonRuleSet
```

AWS 에 대한 관리형 규칙 AWS WAF

AWS Managed AWS WAF Rules는 일반적인 애플리케이션 취약성이나 기타 원치 않는 트래픽으로부터 보호하는 관리형 서비스입니다. 각 웹 ACL에 대해 AWS 관리형 규칙에서 최대 웹 ACL 용량 단위(WCU) 한도까지 하나 이상의 규칙 그룹을 선택할 수 있습니다.

거짓 긍정을 완화하고 규칙 그룹 변경 테스트

프로덕션 환경에서 관리형 규칙 그룹을 사용하기 전에 AWS WAF 보호 기능 테스트 및 조정의 지침에 따라 비프로덕션 환경에서 테스트합니다. 웹 ACL에 규칙 그룹을 추가할 때, 새 버전의 규칙 그룹을 테스트할 때, 그리고 규칙 그룹이 필요한 시점에 웹 트래픽을 처리하지 못할 때마다 테스트 및 조정 지침을 따르십시오.

공유 보안 책임

AWS 관리형 규칙은 일반적인 웹 위협으로부터 사용자를 보호하도록 설계되었습니다. 설명서에 따라 AWS 관리형 규칙 그룹을 사용하면 애플리케이션에 또 다른 보안 계층이 추가됩니다. 하지만 AWS 관리형 규칙 규칙 그룹은 선택한 AWS 리소스에 따라 결정되는 보안 책임을 대체하기 위한 것이 아닙니다. 공동 책임 모델을 참조하여 AWS 리소스가 적절하게 보호되도록 하세요.

AWS 관리형 규칙 규칙 그룹 목록

AWS 관리형 규칙 규칙 그룹의 규칙에 대해 게시하는 정보는 규칙을 사용하기에 충분한 정보를 제공하는 동시에 악의적인 공격자가 규칙을 우회하는 데 사용할 수 있는 정보는 제공하지 않기 위한 것입니다. 이 설명서의 내용 외에 더 많은 정보가 필요한 경우 AWS Support 센터에 문의하십시오.

이 섹션에서는 AWS 관리형 규칙 그룹의 최신 버전을 설명합니다. 관리형 규칙 그룹을 웹 ACL에 추가하면 콘솔에서 이러한 목록이 나타납니다. API를 통해 이 목록을 `ListAvailableManagedRuleGroups` 호출하여 구독한 AWS Marketplace 관리형 규칙 그룹과 함께 검색할 수 있습니다.

> **Note**
>
> AWS 관리형 규칙 그룹 버전 검색에 대한 자세한 내용은 을 참조하십시오. 관리형 규칙 그룹에 대해 사용 가능한 버전 검색

모든 AWS 관리형 규칙 그룹은 레이블 지정을 지원하며, 이 섹션의 규칙 목록에는 레이블 사양이 포함됩니다. `DescribeManagedRuleGroup`를 호출하여 API를 통해 관리형 규칙 그룹의 레이블을 검색할

수 있습니다. 레이블은 응답의 AvailableLabels 속성에 나열됩니다. 라벨링에 대한 자세한 내용은 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.

보호 기능을 프로덕션 트래픽에 사용하기 전에 AWS WAF 보호 기능의 변경 사항을 테스트하고 조정하세요. 자세한 내용은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

AWS 관리형 규칙 규칙 그룹

- 기준 규칙 그룹
  - 핵심 규칙 세트(CRS) 관리형 규칙 그룹
  - 관리 보호 관리형 규칙 그룹
  - 관리형 규칙 그룹의 알려진 잘못된 입력
- 사용 사례별 규칙 그룹
  - SQL 데이터베이스 관리형 규칙 그룹
  - Linux 운영 체제 관리형 규칙 그룹
  - POSIX 운영 체제 관리형 규칙 그룹
  - Windows 운영 체제 관리형 규칙 그룹
  - PHP 애플리케이션 관리형 규칙 그룹
  - WordPress 애플리케이션 관리형 규칙 그룹
- IP 평판 규칙 그룹
  - Amazon IP 신뢰도 목록 관리형 규칙 그룹
  - 익명 IP 목록 관리형 규칙 그룹
- AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹
  - 이 규칙 그룹 사용 시 고려할 사항
  - 이 규칙 그룹에서 추가한 레이블
    - 토큰 레이블
    - ACFP 레이블
  - 계정 생성 사기 방지 규칙 목록
- AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹
  - 이 규칙 그룹 사용 시 고려할 사항
  - 이 규칙 그룹에서 추가한 레이블
    - 토큰 레이블
    - ATP 레이블

기준 규칙 그룹

기준 관리형 규칙 그룹은 다양한 일반적인 위협에 대한 일반적인 보호 기능을 제공합니다. 이러한 규칙 그룹 중 하나 이상을 선택하여 리소스에 대한 기준 보호를 설정합니다.

> **Note**
>
> AWS 관리형 규칙 규칙 그룹의 규칙에 대해 게시하는 정보는 규칙을 사용하기에 충분한 정보를 제공하는 동시에 악의적인 공격자가 규칙을 우회하는 데 사용할 수 있는 정보는 제공하지 않기 위한 것입니다. 이 설명서의 내용 외에 더 많은 정보가 필요한 경우 AWS Support 센터에 문의하십시오.

핵심 규칙 세트(CRS) 관리형 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesCommonRuleSet`, WCU: 700

핵심 규칙 집합(CRS, Core rule set) 규칙 그룹에는 일반적으로 웹 애플리케이션에 적용할 수 있는 규칙이 포함되어 있습니다. 이를 통해 OWASP Top 10과 같은 OWASP 게시물에 설명된 자주 발생하고 위험성 높은 일부 취약성을 비롯한 광범위한 취약성 도용을 막을 수 있습니다. 모든 사용 사례에 이 규칙 그룹을 AWS WAF 사용하는 것을 고려해 보세요.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`NoUserAgent_HEADER`	HTTP `User-Agent` 헤더가 누락된 요청을 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
`UserAgent_BadBots_HEADER`	요청이 불량 봇임을 나타내는 공통 `User-Agent` 헤더 값이 있는지 검사합니다. 예제 패턴에는 `nessus` 및 `nmap`이 포함되어 있습니다. 봇 관리에 대한 자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:BadBots_Header`
`SizeRestrictions_QUERYSTRING`	URI 쿼리 문자열이 2,048바이트를 초과하는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString`

규칙 이름	설명 및 레이블
SizeRestrictions_Cookie_HEADER	쿠키 헤더가 10,240바이트를 초과하늕 검사합니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header
SizeRestrictions_BODY	요청 본문이 8KB(8,192바이트)를 초과하는지 검사합니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:core-rule-set:SizeRestrictions_Body
SizeRestrictions_URIPATH	URI 경로가 1,024바이트를 초과하는지 검사합니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath

규칙 이름	설명 및 레이블
`EC2MetaDataSSRF_BODY`	요청 본문에서 Amazon EC2 메타데이터를 빼내려는 시도가 있는지 검사합니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`
`EC2MetaDataSSRF_COOKIE`	요청 쿠키에서 Amazon EC2 메타데이터를 빼내려는 시도가 있는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie`

규칙 이름	설명 및 레이블
`EC2MetaDataSSRF_URIPATH`	요청 URI 경로에서 Amazon EC2 메타데이터를 빼내려는 시도가 있는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath`
`EC2MetaDataSSRF_QUERYARGUMENTS`	요청 쿼리 인수에서 Amazon EC2 메타데이터를 빼내려는 시도가 있는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments`
`GenericLFI_QUERYARGUMENTS`	쿼리 인수에 로컬 파일 포함(LFI, Local File Inclusion) 도용이 있는지 검사합니다. 예를 들면 `../../` 같은 기술을 사용한 경로 탐색 시도가 있을 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments`

규칙 이름	설명 및 레이블
`GenericLFI_URIPATH`	URI 경로에 로컬 파일 포함(LFI, Local File Inclusion) 도용이 있는지 검사합니다. 예를 들면 `../../` 같은 기술을 사용한 경로 탐색 시도가 있을 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:GenericLFI_URIPath`

규칙 이름	설명 및 레이블
`GenericLFI_BODY`	요청 본문에 로컬 파일 포함(LFI, Local File Inclusion) 도용이 있는지 검사합니다. 예를 들면 `../../` 같은 기술을 사용한 경로 탐색 시도가 있을 수 있습니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:GenericLFI_Body`

규칙 이름	설명 및 레이블
RestrictedExtensions_URIPATH	URI 경로에 읽거나 실행하기에 안전하지 않은 시스템 파일 확장자가 포함된 요청이 있는지 검사합니다. 예제 패턴에는 .log 및 .ini 같은 확장명이 포함됩니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath
RestrictedExtensions_QUERYARGUMENTS	쿼리 인수가 클라이언트가 읽거나 실행하기에 안전하지 않은 시스템 파일 확장명인 요청을 검사합니다. 예제 패턴에는 .log 및 .ini 같은 확장명이 포함됩니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments
GenericRFI_QUERYARGUMENTS	모든 쿼리 매개 변수의 값을 검사하여 IPv4 주소가 포함된 URL을 포함하여 웹 애플리케이션에서 RFI(Remote File Inclusion)를 악용하려는 시도가 있는지 확인합니다. 예를 들면, 악용 시도에는 IPv4 호스트 헤더가 있는 http://, https://,ftp://,ftps:// 및 file:// 등의 패턴이 있습니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments

규칙 이름	설명 및 레이블
`GenericRFI_BODY`	IPv4 주소가 포함된 URL을 포함하여 웹 애플리케이션에서 RFI(Remote File Inclusion)를 악용하려는 시도가 있는지 알아보기 위해 요청 본문을 검사합니다. 예를 들면, 악용 시도에는 IPv4 호스트 헤더가 있는 `http://`, `https://`,`ftp://`,`ftps://` 및 `file://` 등의 패턴이 있습니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:GenericRFI_Body`

규칙 이름	설명 및 레이블
`GenericRFI_URIPATH`	IPv4 주소가 포함된 URL을 포함하여 웹 애플리케이션에서 RFI(Remote File Inclusion)를 악용하려는 시도가 있는지 알아보기 위해 URI 경로를 검사합니다. 예를 들면, 악용 시도에는 IPv4 호스트 헤더가 있는 `http://`, `https://`,`ftp://`,`ftps://` 및 `file://` 등의 패턴이 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:GenericRFI_URIPath`
`CrossSiteScripting_COOKIE`	내장 기능을 사용하여 쿠키 헤더의 값에 일반적인 XSS (크로스 사이트 스크립팅) 패턴이 있는지 검사합니다. AWS WAF 교차 사이트 스크립팅 공격 규칙 문 예제 패턴에는 `<script>alert("hello")</script>` 같은 스크립트가 포함됩니다. **Note** AWS WAF 로그의 규칙 일치 세부 정보는 이 규칙 그룹의 버전 2.0에 대해 채워지지 않았습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

규칙 이름	설명 및 레이블
`CrossSiteScripting_QUERYARGUMENTS`	내장 기능을 사용하여 일반적인 크로스 사이트 스크립팅 (XSS) 패턴에 대한 쿼리 인수 값을 검사합니다. AWS WAF 교차 사이트 스크립팅 공격 규칙 문 예제 패턴에는 `<script>alert("hello")</script>` 같은 스크립트가 포함됩니다. **Note** AWS WAF 로그의 규칙 일치 세부 정보는 이 규칙 그룹의 버전 2.0에 대해 채워지지 않았습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

규칙 이름	설명 및 레이블
`CrossSiteScripting_BODY`	기본 제공을 사용하여 요청 본문에서 일반적인 XSS (사이트 간 스크립팅) 패턴을 검사합니다. AWS WAF 교차 사이트 스크립팅 공격 규칙 문 예제 패턴에는 `<script>alert("hello")</script>` 같은 스크립트가 포함됩니다. **Note** AWS WAF 로그의 규칙 일치 세부 정보는 이 규칙 그룹의 버전 2.0에 대해 채워지지 않았습니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block

규칙 이름	설명 및 레이블
	Label(레이블): `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`
`CrossSiteScripting_URIPATH`	내장 기능을 사용하여 일반적인 XSS (크로스 사이트 스크립팅) 패턴의 URI 경로 값을 검사합니다. AWS WAF 교차 사이트 스크립팅 공격 규칙 문 예제 패턴에는 `<script>alert("hello")</script>` 같은 스크립트가 포함됩니다. **Note** AWS WAF 로그의 규칙 일치 세부 정보는 이 규칙 그룹의 버전 2.0에 대해 채워지지 않았습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

관리 보호 관리형 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesAdminProtectionRuleSet`, WCU: 100

관리 보호 규칙 그룹에는 노출된 관리 페이지에 대한 외부 액세스를 차단할 수 있는 규칙이 포함되어 있습니다. 서드 파티 소프트웨어를 실행 중이거나, 악성 액터가 애플리케이션에 대한 관리 액세스 권한을 얻게 되는 위험을 줄이려면 이 방법이 유용할 수 있습니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트

릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`AdminProtection_URIPATH`	일반적으로 웹 서버 또는 애플리케이션의 관리를 위해 예약되어 있는 URI 경로가 있는지 검사합니다. 예제 패턴에는 `sqlmanager` 가 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

관리형 규칙 그룹의 알려진 잘못된 입력

VendorName:`AWS`, 이름:`AWSManagedRulesKnownBadInputsRuleSet`, WCU: 200

알려진 잘못된 입력 규칙 그룹에는 유효하지 않은 것으로 알려져 있으며 취약성의 도용 또는 발견과 관련된 요청 패턴을 차단하는 규칙이 포함되어 있습니다. 이렇게 하면 악성 액터가 취약한 애플리케이션을 발견하는 위험을 줄일 수 있습니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`JavaDeserializationRCE_HEADER`	Spring Core and Cloud Function RCE 취약점(CVE-2022-22963, CVE-2022-22965)과 같은 Java 역직렬화 원격 명령 실행(RCE) 시도를 나타내는 패턴이 있는지 HTTP 요청 헤더의 키와 값을 검사합니다. 예제 패턴에는 `(java.lang.Runtime).getRuntime().exec("whoami")` 가 포함됩니다. **Warning** 이 규칙은 요청 헤더의 처음 8KB 또는 처음 200개 헤더(둘 중 먼저 도달하는 제한)만 검사하며 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header`
`JavaDeserializationRCE_BODY`	Spring Core and Cloud Function RCE 취약성(CVE-2022-22963, CVE-2022-22965)과 같은 Java 역직렬화 원격 명령 실행(RCE) 시도를 나

규칙 이름	설명 및 레이블
	타내는 패턴이 있는지 요청 본문을 검사합니다. 예제 패턴에는 `(java.lang.Runtime).getRuntime().exec("whoami")` 가 포함됩니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:JavaDeserialization RCE_Body`

규칙 이름	설명 및 레이블
JavaDeserializationRCE_URIPATH	Spring Core and Cloud Function RCE 취약성(CVE-2022-22963, CVE-2022-22965)과 같은 Java 역직렬화 원격 명령 실행(RCE) 시도를 나타내는 패턴이 있는지 요청 URI를 검사합니다. 예제 패턴에는 `(java.lang.Runtime).getRuntime().exec("whoami")` 가 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_URIPath`
JavaDeserializationRCE_QUERYSTRING	Spring Core and Cloud Function RCE 취약성(CVE-2022-22963, CVE-2022-22965)과 같은 Java 역직렬화 원격 명령 실행(RCE) 시도를 나타내는 패턴이 있는지 요청 쿼리 문자열을 검사합니다. 예제 패턴에는 `(java.lang.Runtime).getRuntime().exec("whoami")` 가 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_QueryString`

규칙 이름	설명 및 레이블
Host_localhost_HEADER	로컬 호스트를 나타내는 패턴에 대한 요청의 호스트 헤더를 검사합니다. 예제 패턴에는 localhost 가 포함됩니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header
PROPFIND_METHOD	HEAD와 유사하지만 XML 객체를 빼내려는 의도가 추가된 PROPFIND에 대한 요청의 HTTP 메서드를 검사합니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:known-bad-inputs:Propfind_Method
ExploitablePaths_URIPATH	URI 경로에서 도용 가능한 웹 애플리케이션 경로에 대한 액세스 시도를 검사합니다. 예제 패턴에는 web-inf와 같은 경로가 포함됩니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath

규칙 이름	설명 및 레이블
`Log4JRCE_HEADER`	요청 헤더의 키와 값을 검사하여 Log4j 취약점(CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)이 있는지 확인하고 원격 코드 실행(RCE) 시도로부터 보호합니다. 예제 패턴에는 `${jndi:ldap://example.com/}` 가 포함됩니다. **Warning** 이 규칙은 요청 헤더의 처음 8KB 또는 처음 200개 헤더(둘 중 먼저 도달하는 제한)만 검사하며 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header`

규칙 이름	설명 및 레이블
`Log4JRCE_QUERYSTRING`	쿼리 문자열을 검사하여 Log4j 취약성 (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)이 있는지 확인하고 원격 코드 실행(RCE) 시도로부터 보호합니다. 예제 패턴에는 `${jndi:ldap://example.com/}` 가 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

규칙 이름	설명 및 레이블
`Log4JRCE_BODY`	본문을 검사하여 Log4j 취약성(CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)이 있는지 확인하고 원격 코드 실행(RCE) 시도로부터 보호합니다. 예제 패턴에는 `${jndi:ldap://example.com/}` 가 포함됩니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

규칙 이름	설명 및 레이블
`Log4JRCE_URIPATH`	URI 경로를 검사하여 Log4j 취약성(CVE-2021-44228, CVE-2021-45046, CVE-2021-45105)이 있는지 확인하고 원격 코드 실행(RCE) 시도로부터 보호합니다. 예제 패턴에는 `${jndi:ldap://example.com/}` 가 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

사용 사례별 규칙 그룹

사용 사례별 규칙 그룹은 다양한 사용 사례에 대해 점진적인 보호를 제공합니다. AWS WAF 애플리케이션에 적용되는 규칙 그룹을 선택합니다.

> **Note**
>
> AWS 관리형 규칙 규칙 그룹의 규칙에 대해 게시하는 정보는 규칙을 사용하기에 충분한 정보를 제공하는 동시에 악의적인 공격자가 규칙을 우회하는 데 사용할 수 있는 정보는 제공하지 않기 위한 것입니다. 이 설명서의 내용 외에 더 많은 정보가 필요한 경우 AWS Support 센터에 문의하십시오.

SQL 데이터베이스 관리형 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesSQLiRuleSet`, WCU: 200

SQL 데이터베이스 규칙 그룹에는 SQL 명령어 주입 공격과 같은 SQL 데이터베이스 도용과 관련된 요청 패턴을 차단하는 규칙이 포함되어 있습니다. 이렇게 하면 승인되지 않은 쿼리가 원격으로 삽입되는 것을 방지할 수 있습니다. 애플리케이션이 SQL 데이터베이스와 접속하는 경우 이 규칙 그룹을 사용할 수 있는지 평가합니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트

릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
SQLi_QUERYARGUMENTS	민감도 수준을 로 설정한 상태로 기본 제공 기능을 AWS WAF SQL 주입 공격 규칙 문 사용하여 모든 쿼리 파라미터 값에서 악성 SQL 코드와 일치하는 패턴이 있는지 검사합니다. Low 규칙 작업: Block Label(레이블): awswaf:managed:aws:sql-database:SQLi_QueryArguments
SQLiExtendedPatterns_QUERYARGUMENTS	모든 쿼리 파라미터의 값에서 악성 SQL 코드와 일치하는 패턴을 검사합니다. 이 규칙이 검사하는 패턴은 SQLi_QUERYARGUMENTS 규칙의 검사 범위에 포함되지 않습니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
SQLi_BODY	민감도 수준을 로 설정한 상태로 기본 제공 기능을 AWS WAF SQL 주입 공격 규칙 문 사용하여 요청 본문에서 악성 SQL 코드와 일치하는 패턴이 있는지 검사합니다. Low

규칙 이름	설명 및 레이블
	Warning 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:sql-database:SQLi_Body`

규칙 이름	설명 및 레이블
`SQLiExtendedPatterns_BODY`	요청 본문에 악성 SQL 코드와 일치하는 패턴이 있는지 검사합니다. 이 규칙이 검사하는 패턴은 `SQLi_BODY` 규칙의 검사 범위에 포함되지 않습니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body`

규칙 이름	설명 및 레이블
`SQLi_COOKIE`	민감도 수준을 로 설정한 상태로 기본 제공 기능을 AWS WAF SQL 주입 공격 규칙 문 사용하여 요청 쿠키 헤더에서 악성 SQL 코드와 일치하는 패턴이 있는지 검사합니다. Low 규칙 작업: Block Label(레이블): `awswaf:managed:aws:sql-database:SQLi_Cookie`

Linux 운영 체제 관리형 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesLinuxRuleSet`, WCU: 200

Linux 운영 체제 규칙 그룹에는 Linux 관련 로컬 파일 포함(LFI, Local File Inclusion) 공격을 포함하여 Linux에 특정한 취약성 도용과 관련된 요청 패턴을 차단하는 규칙이 포함되어 있습니다. 이렇게 하면 파일 내용을 노출하거나 공격자가 액세스 권한을 가져서는 안 되는 코드를 실행하는 공격을 방지할 수 있습니다. 애플리케이션의 일부가 Linux에서 실행되는 경우 이 규칙 그룹을 평가해야 합니다. 이 규칙 그룹은 POSIX 운영 체제 규칙 그룹과 함께 사용해야 합니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`LFI_URIPATH`	웹 애플리케이션의 로컬 파일 포함(LFI, Local File Inclusion) 취약성을 도용하려는 시도가 있

규칙 이름	설명 및 레이블
	는지 요청 경로를 검사합니다. 예제 패턴에는 공격자에게 운영 체제 정보를 제공할 수 있는 `/proc/version` 등의 파일이 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:linux-os:LFI_URIPath`
`LFI_QUERYSTRING`	웹 애플리케이션의 로컬 파일 포함(LFI, Local File Inclusion) 취약성을 도용하려는 시도가 있는지 쿼리 문자열을 검사합니다. 예제 패턴에는 공격자에게 운영 체제 정보를 제공할 수 있는 `/proc/version` 등의 파일이 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:linux-os:LFI_QueryString`

규칙 이름	설명 및 레이블
LFI_HEADER	웹 애플리케이션의 로컬 파일 포함(LFI, Local File Inclusion) 취약성을 도용하려는 시도가 있는지 요청 헤더를 검사합니다. 예제 패턴에는 공격자에게 운영 체제 정보를 제공할 수 있는 `/proc/version` 등의 파일이 포함됩니다. **Warning** 이 규칙은 요청 헤더의 처음 8KB 또는 처음 200개 헤더(둘 중 먼저 도달하는 제한)만 검사하며 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:linux-os:LFI_Header`

POSIX 운영 체제 관리형 규칙 그룹

VendorName:`AWS`, 이름:, WCU: `AWSManagedRulesUnixRuleSet` 100

POSIX 운영 체제 규칙 그룹에는 로컬 파일 포함(LFI, Local File Inclusion) 공격을 포함하여 POSIX 및 POSIX 유사 운영 체제에 특정한 취약성 도용과 관련된 요청 패턴을 차단하는 규칙이 포함되어 있습니다. 이렇게 하면 파일 내용을 노출하거나 공격자가 액세스 권한을 가져서는 안 되는 코드를 실행하는 공격을 방지할 수 있습니다. 애플리케이션의 일부가 POSIX 또는 POSIX 유사 운영 체제(예: Linux, AIX, HP-UX, macOS, Solaris, FreeBSD, OpenBSD)에서 실행되는 경우 이 규칙 그룹을 평가해야 합니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트

릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`UNIXShellCommandsVariables_QUERYSTRING`	Unix 시스템에서 실행되는 웹 응용 프로그램의 명령 삽입, LFI 및 경로 탐색 취약성을 악용하려는 시도가 있는지 쿼리 문자열 값을 검사합니다. 예로는 `echo $HOME` 및 `echo $PATH` 같은 패턴이 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`
`UNIXShellCommandsVariables_BODY`	Unix 시스템에서 실행되는 웹 애플리케이션에서 명령 주입, LFI 및 경로 탐색 취약성을 도용하려는 시도가 있는지 요청 본문을 검사합니다. 예로는 `echo $HOME` 및 `echo $PATH` 같은 패턴이 있습니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액

규칙 이름	설명 및 레이블
	세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body`

규칙 이름	설명 및 레이블
`UNIXShellCommandsVariables_HEADER`	Unix 시스템에서 실행되는 웹 애플리케이션의 명령 삽입, LFI 및 경로 탐색 취약성을 악용하려는 시도가 있는지 모든 요청 헤더를 검사합니다. 예로는 `echo $HOME` 및 `echo $PATH` 같은 패턴이 있습니다. **Warning** 이 규칙은 요청 헤더의 처음 8KB 또는 처음 200개 헤더(둘 중 먼저 도달하는 제한)만 검사하며 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header`

Windows 운영 체제 관리형 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesWindowsRuleSet`, WCU: 200

Windows 운영 체제 규칙 그룹에는 명령의 원격 실행과 같은 Windows 고유의 취약성 악용과 관련된 요청 패턴을 차단하는 규칙이 포함되어 있습니다. PowerShell 이를 통해 공격자가 권한이 없는 명령을 실행하거나 악성 코드를 실행할 수 있는 취약성 악용을 방지할 수 있습니다. 애플리케이션의 일부가 Windows 운영 체제에서 실행되는 경우 이 규칙 그룹을 평가합니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트

릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`WindowsShellCommands_COOKIE`	웹 애플리케이션에서 WindowsShell 명령 삽입 시도가 있는지 요청 쿠키 헤더를 검사합니다. 일치 패턴은 명령을 나타냅니다WindowsShell . 예제 패턴에는 `||nslookup` 및 `;cmd`이 포함되어 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:windows-os:WindowsShellCommands_Cookie`
`WindowsShellCommands_QUERYARGUMENTS`	웹 응용 프로그램의 WindowsShell 명령 삽입 시도에 대한 모든 쿼리 매개 변수 값을 검사합니다. 일치 패턴은 WindowsShell 명령을 나타냅니다. 예제 패턴에는 `||nslookup` 및 `;cmd`이 포함되어 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`
`WindowsShellCommands_BODY`	웹 애플리케이션의 WindowsShell 명령 삽입 시도에 대한 요청 본문을 검사합니다. 일치 패턴은

규칙 이름	설명 및 레이블
	WindowsShell 명령을 나타냅니다. 예제 패턴에는 `||nslookup` 및 `;cmd`이 포함되어 있습니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:windows-os:WindowsShellCommands_Body`

규칙 이름	설명 및 레이블
PowerShellCommands_COOKIE	웹 애플리케이션의 PowerShell 명령 삽입 시도에 대한 요청 쿠키 헤더를 검사합니다. 일치 패턴은 명령을 나타냅니다PowerShell . 예를 들어 `Invoke-Expression` 입니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:windows-os:PowerShellCommands_Cookie`
PowerShellCommands_QUERYARGUMENTS	웹 응용 프로그램의 PowerShell 명령 삽입 시도에 대한 모든 쿼리 매개 변수 값을 검사합니다. 일치 패턴은 PowerShell 명령을 나타냅니다. 예를 들어 `Invoke-Expression` 입니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:windows-os:PowerShellCommands_QueryArguments`

규칙 이름	설명 및 레이블
`PowerShellCommands_BODY`	웹 애플리케이션의 PowerShell 명령 삽입 시도에 대한 요청 본문을 검사합니다. 일치 패턴은 PowerShell 명령을 나타냅니다. 예를 들어 `Invoke-Expression` 입니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:windows-os:PowerShellCommands_Body`

PHP 애플리케이션 관리형 규칙 그룹

VendorName:`AWS`, 이름:, WCU: `AWSManagedRulesPHPRuleSet` 100

PHP 애플리케이션 규칙 그룹에는 안전하지 않은 PHP 함수의 주입을 포함하여 PHP 프로그래밍 언어 사용에 특정한 취약성 도용과 관련된 요청 패턴을 차단하는 규칙이 포함되어 있습니다. 이렇게 하면 공

격자가 권한이 부여되지 않은 코드나 명령을 원격으로 실행할 수 있는 취약성 악용을 방지할 수 있습니다. 애플리케이션이 접속하는 서버에 PHP가 설치되어 있는 경우 이 규칙 그룹을 평가합니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`PHPHighRiskMethodsVariables_HEADER`	PHP 스크립트 코드 주입 시도가 있는지 모든 헤더를 검사합니다. 예제 패턴에는 `fsockopen` 같은 함수 및 `$_GET` superglobal 변수가 포함됩니다. **Warning** 이 규칙은 요청 헤더의 처음 8KB 또는 처음 200개 헤더(둘 중 먼저 도달하는 제한)만 검사하며 과대 콘텐츠 처리에 대해 `Continue` 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header`

규칙 이름	설명 및 레이블
PHPHighRiskMethodsVariables_QUERYSTRING	요청 URL의 첫 번째 ? 이후의 모든 부분을 검사하여 PHP 스크립트 코드 삽입 시도를 찾습니다. 예제 패턴에는 fsockopen 같은 함수 및 $_GET superglobal 변수가 포함됩니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString

규칙 이름	설명 및 레이블
PHPHighRiskMethodsVariables_BODY	PHP 스크립트 코드 주입 시도가 있는지 요청 본문의 값을 검사합니다. 예제 패턴에는 fsockopen 같은 함수 및 $_GET superglobal 변수가 포함됩니다. **Warning** 이 규칙은 웹 ACL 및 리소스 유형에 대한 본문 크기 제한까지만 요청 본문을 검사합니다. Application Load Balancer 및 의 AWS AppSync경우 제한은 8KB로 고정되어 있습니다. API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스의 경우 기본 한도는 16KB이며 웹 ACL 구성에서 제한을 최대 64KB까지 늘릴 수 있습니다. CloudFront 이 규칙은 과대 콘텐츠 처리에 대해 Continue 옵션을 사용합니다. 자세한 정보는 에서 크기 초과 요청 구성 요소 처리 AWS WAF을 참조하세요. 규칙 작업: Block Label(레이블): awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body

WordPress 애플리케이션 관리형 규칙 그룹

VendorName:AWS, 이름:AWSManagedRulesWordPressRuleSet, WCU: 100

WordPress 응용 프로그램 규칙 그룹에는 사이트 고유의 취약성 악용과 관련된 요청 패턴을 차단하는 규칙이 포함되어 있습니다. WordPress 실행 중인 경우 이 규칙 그룹을 평가해야 합니다. WordPress 이 규칙 그룹은 SQL 데이터베이스 및 PHP 애플리케이션 규칙 그룹과 함께 사용해야 합니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

> **Note**
>
> 이 표는 이 규칙 그룹의 최신 정적 버전을 설명합니다. 다른 버전의 경우 API 명령을 사용하십시오 DescribeManagedRuleGroup.

규칙 이름	설명 및 레이블
`WordPressExploitableCommands_QUERYSTRING`	요청 쿼리 문자열에 취약한 설치 또는 플러그인에서 악용될 수 있는 고위험 WordPress 명령이 있는지 검사합니다. 예제 패턴에는 `do-reset-wordpress` 같은 명령이 포함됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	쉽게 악용될 수 있는 취약점이 있는 것으로 알려진 와 같은 WordPress `xmlrpc.php` 파일의 요청 URI 경로를 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

IP 평판 규칙 그룹

IP 평판 규칙 그룹을 사용하면 소스 IP 주소에 따라 요청을 차단합니다.

> **Note**
>
> 이 규칙은 웹 요청 오리진의 소스 IP 주소를 사용합니다. 하나 이상의 프록시 또는 로드 밸런서를 통과하는 트래픽이 있는 경우 웹 요청 오리진에는 클라이언트의 최초 주소가 아닌 마지막 프록시의 주소가 포함됩니다.

봇 트래픽에 대한 노출 또는 도용 시도를 줄이고 싶거나 콘텐츠에 대해 지리적 제한을 적용 중인 경우 이러한 규칙 그룹 중 하나 이상을 선택합니다. 봇 관리에 대한 자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.

이 범주의 규칙 그룹은 버전 관리 또는 SNS 업데이트 알림을 제공하지 않습니다.

> **Note**
>
> AWS 관리형 규칙 규칙 그룹의 규칙에 대해 당사가 게시하는 정보는 규칙을 사용하기에 충분한 정보를 제공하는 동시에 악의적인 공격자가 규칙을 우회하는 데 사용할 수 있는 정보는 제공하지 않기 위한 것입니다. 이 설명서의 내용 외에 더 많은 정보가 필요한 경우 AWS Support 센터에 문의하십시오.

Amazon IP 신뢰도 목록 관리형 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesAmazonIpReputationList`, WCU: 25

Amazon IP 평판 목록 규칙 그룹에는 Amazon 내부 위협 인텔리전스를 기반으로 하는 규칙이 포함되어 있습니다. 이는 일반적으로 봇이나 다른 위협과 연결된 IP 주소를 차단하려는 경우에 유용합니다. 이러한 IP 주소를 차단하면 봇을 완화하고 악성 액터가 취약한 애플리케이션을 발견하는 위험을 줄일 수 있습니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

규칙 이름	설명 및 레이블
`AWSManagedIPReputationList`	악의적인 활동에 적극적으로 관여하는 것으로 확인된 IP 주소를 검사합니다. AWS WAF Amazon이 사이버 범죄로부터 고객을 보호하는 데 사용하는 위협 인텔리전스 도구를 비롯한 MadPot 다양한 출처로부터 IP 주소 목록을 수집합니다. 에 대한 자세한 내용은 MadPot 을 참조하십시오https://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList`
`AWSManagedReconnaissanceList`	IP 주소의 연결을 검사하여 AWS 리소스에 대한 정찰을 수행하고 있는지 확인합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList`
`AWSManagedIPDDoSList`	DDoS 활동에 적극적으로 관여하는 것으로 식별된 IP 주소가 있는지 검사합니다. 규칙 작업: Count Label(레이블): `awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

익명 IP 목록 관리형 규칙 그룹

VendorName:AWS, 이름:AWSManagedRulesAnonymousIpList, WCU: 50

익명 IP 목록 규칙 그룹에는 최종 사용자 ID 난독화를 허용하는 서비스의 요청을 차단하는 규칙이 포함되어 있습니다. 여기에는 VPN, 프록시, Tor 노드 및 웹 호스팅 공급자의 요청이 포함됩니다. 이 규칙 그룹은 애플리케이션에서 자신의 ID를 숨기려고 하는 최종 사용자를 필터링하려는 경우에 유용합니다. 이러한 서비스의 IP 주소를 차단하면 봇을 완화하고 지리적 제한을 피할 수 있습니다.

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

규칙 이름	설명 및 레이블
AnonymousIPList	TOR 노드, 임시 프록시 및 기타 마스킹 서비스 등 클라이언트 정보를 익명화하는 것으로 알려진 소스의 IP 주소 목록을 검사합니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:anonymous-ip-list:AnonymousIPList
HostingProviderIPList	최종 사용자 트래픽을 소싱할 가능성이 적은 웹 호스팅 공급자 및 클라우드 공급자의 IP 주소 목록을 검사합니다. IP 목록에는 AWS IP 주소가 포함되지 않습니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList

AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesACFPRuleSet`, WCU: 50

AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 는 부정 계정 생성 시도의 일부일 수 있는 요청을 규칙 그룹 레이블로 지정하고 관리합니다. 이 규칙 그룹은 클라이언트가 애플리케이션의 등록 및 계정 생성 엔드포인트로 보내는 계정 생성 요청을 검사하여 이 작업을 수행합니다.

ACFP 규칙 그룹은 계정 생성 시도를 다양한 방식으로 검사하여 사용자가 잠재적으로 악의적인 상호 작용을 파악하고 제어할 수 있도록 합니다. 규칙 그룹은 요청 토큰을 사용하여 클라이언트 브라우저에 대한 정보와 계정 생성 요청 생성 시 사용자 상호 작용 수준에 대한 정보를 수집합니다. 규칙 그룹은 IP 주소 및 클라이언트 세션별로 요청을 집계하고 실제 주소 및 전화 번호와 같은 제공된 계정 정보별로 집계하여 대량 계정 생성 시도를 탐지하고 관리합니다. 또한 규칙 그룹은 손상된 보안 인증 정보를 사용한 새 계정의 생성을 탐지하고 차단하므로 애플리케이션과 새 사용자의 보안 상태를 보호하는 데 도움이 됩니다.

이 규칙 그룹 사용 시 고려할 사항

이 규칙 그룹에는 애플리케이션의 계정 등록 및 계정 생성 경로 사양을 포함하는 사용자 지정 구성이 필요합니다. 별도로 언급되는 경우를 제외하고, 이 규칙 그룹의 규칙은 클라이언트가 이 두 엔드포인트로 보내는 모든 요청을 검사합니다. 이 규칙 그룹을 구성하고 구현하려면 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP)의 지침을 참조하세요.

> **Note**
>
> 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

이 규칙 그룹은 AWS WAF에 지능형 위협 완화 보호의 일부로 포함됩니다. 자세한 내용은 AWS WAF 지능형 위협 완화을 참조하세요.

지속적으로 비용을 절감하고 웹 트래픽이 필요에 맞게 관리되도록 하려면 지능형 위협 완화 모범 사례의 지침에 따라 이 규칙 그룹을 사용하십시오.

이 규칙 그룹은 Amazon Cognito 사용자 풀과 함께 사용할 수 없습니다. 이 규칙 그룹을 사용하는 웹 ACL을 사용자 풀과 연결할 수 없으며, 이미 사용자 풀과 연결된 웹 ACL에 이 규칙 그룹을 추가할 수 없습니다.

이 규칙 그룹에서 추가한 레이블

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

토큰 레이블

이 규칙 그룹은 AWS WAF 토큰 관리를 사용하여 토큰 상태에 따라 웹 요청을 검사하고 AWS WAF 레이블을 지정합니다. AWS WAF 토큰을 사용하여 클라이언트 세션을 추적하고 확인합니다.

토큰 및 토큰 관리에 대한 자세한 내용은 AWS WAF 웹 요청 토큰을(를) 참조하십시오.

여기에 설명된 레이블 구성 요소에 대한 자세한 내용은 AWS WAF 레이블 구문 및 이름 지정 요구 사항을(를) 참조하십시오.

클라이언트 세션 레이블

`awswaf:managed:token:id:`*`identifier`*라벨에는 AWS WAF 토큰 관리가 클라이언트 세션을 식별하는 데 사용하는 고유 식별자가 들어 있습니다. 클라이언트가 새 토큰을 획득하는 경우(예: 사용하고 있던 토큰을 폐기한 후) 식별자가 변경될 수 있습니다.

> **Note**
>
> AWS WAF 이 라벨에 대한 Amazon CloudWatch 메트릭을 보고하지 않습니다.

토큰 상태 레이블: 레이블 네임스페이스 접두사

토큰 상태 레이블은 토큰 및 챌린지 상태와 토큰에 포함된 CAPTCHA 정보를 보고합니다.

각 토큰 상태 레이블은 다음 네임스페이스 접두사 중 하나로 시작합니다.

- `awswaf:managed:token:` – 토큰의 일반 상태를 보고하고 토큰의 챌린지 정보 상태를 보고하는 데 사용됩니다.
- `awswaf:managed:captcha:` – 토큰의 CAPTCHA 정보 상태를 보고하는 데 사용됩니다.

토큰 상태 레이블: 레이블 이름

접두사 뒤에 오는 라벨의 나머지 부분은 자세한 토큰 상태 정보를 제공합니다.

- `accepted` – 요청 토큰이 존재하며 다음을 포함합니다.
  - 유효한 챌린지 또는 CAPTCHA 솔루션.
  - 만료되지 않은 챌린지 또는 CAPTCHA 타임스탬프.
  - 웹 ACL에 대해 유효한 도메인 사양입니다.

  예: 레이블 `awswaf:managed:token:accepted`은(는) 웹 요청의 토큰에 유효한 인증 확인 솔루션, 만료되지 않은 챌린지 타임스탬프 및 유효한 도메인이 있음을 나타냅니다.
- `rejected` – 요청 토큰이 존재하지만 수락 기준을 충족하지 않습니다.

  거부된 레이블과 함께 토큰 관리는 사용자 지정 레이블 네임스페이스 및 이름을 추가하여 이유를 나타냅니다.
  - `rejected:not_solved` – 토큰에 챌린지 또는 CAPTCHA 솔루션이 없습니다.
  - `rejected:expired` – 웹 ACL의 구성된 토큰 면역 시간에 따라 토큰의 챌린지 또는 CAPTCHA 타임스탬프가 만료되었습니다.
  - `rejected:domain_mismatch` – 토큰의 도메인이 웹 ACL의 토큰 도메인 구성과 일치하지 않습니다.
  - `rejected:invalid`— AWS WAF 표시된 토큰을 읽을 수 없습니다.

  예: 레이블 `awswaf:managed:captcha:rejected` 및 `awswaf:managed:captcha:rejected:expired`은(는) 토큰의 CAPTCHA 타임스탬프가 웹 ACL에 구성된 CAPTCHA 토큰 면역 시간을 초과했기 때문에 요청이 거부되었음을 나타냅니다.
- `absent` – 요청에 토큰이 없거나 토큰 관리자가 토큰을 읽을 수 없습니다.

  예: 레이블 `awswaf:managed:captcha:absent`은(는) 요청에 토큰이 없음을 나타냅니다.

ACFP 레이블

이 규칙 그룹은 네임스페이스 접두사 `awswaf:managed:aws:acfp:` 다음에 사용자 지정 네임스페이스와 레이블 이름이 이어지는 레이블을 생성합니다. 이 규칙 그룹은 요청 하나에 둘 이상의 레이블을 추가할 수도 있습니다.

`DescribeManagedRuleGroup`를 호출하여 API를 통해 규칙 그룹의 모든 레이블을 검색할 수 있습니다. 레이블은 응답의 `AvailableLabels` 속성에 나열됩니다.

계정 생성 사기 방지 규칙 목록

이 섹션에는 `AWSManagedRulesACFPRuleSet`의 ACFP 규칙과 규칙 그룹의 규칙이 웹 요청에 추가하는 레이블이 나열되어 있습니다.

> **Note**
>
> AWS 관리형 규칙 그룹의 규칙에 대해 Google이 게시하는 정보는 규칙을 사용하기에 충분한 정보를 제공하는 동시에 악의적인 공격자가 규칙을 우회하는 데 사용할 수 있는 정보는 제공하지 않기 위한 것입니다. 이 설명서의 내용 외에 더 많은 정보가 필요한 경우 AWS Support 센터에 문의하십시오.

이 규칙 그룹의 모든 규칙에는 처음 두 `UnsupportedCognitoIDP` 및 `AllRequests`의 경우를 제외하고는 웹 요청 토큰이 필요합니다. 토큰이 제공하는 정보에 대한 설명은 AWS WAF 토큰 특성 섹션을 참조하세요.

별도로 언급된 경우를 제외하고, 이 규칙 그룹의 규칙은 클라이언트가 규칙 그룹 구성에 제공되는 계정 등록 및 계정 생성 페이지 경로로 보내는 모든 요청을 검사합니다. 이 규칙 그룹의 구성에 대한 자세한 내용은 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 섹션을 참조하세요.

규칙 이름	설명 및 레이블
`UnsupportedCognitoIDP`	Amazon Cognito 사용자 풀로 이동하는 웹 트래픽을 검사합니다. ACFP는 Amazon Cognito 사용자 풀과 함께 사용할 수 없으므로, 이 규칙은 다른 ACFP 규칙 그룹 규칙이 사용자 풀 트래픽을 평가하는 데 사용되지 않도록 하는 데 도움이 됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:unsupported:cognito_idp`
`AllRequests`	등록 페이지 경로에 액세스하는 요청에 규칙 작업을 적용합니다. 규칙 그룹을 구성할 때 등록 페이지 경로를 구성합니다.

규칙 이름	설명 및 레이블
	기본적으로 이 규칙은 요청에 Challenge를 적용합니다. 이 작업의 적용으로 규칙은 규칙 그룹의 나머지 규칙에서 요청을 평가하기 전에 클라이언트가 챌린지 토큰을 획득하도록 합니다. 최종 사용자가 계정 생성 요청을 제출하기 전에 등록 페이지 경로를 로드하도록 해야 합니다. 토큰은 클라이언트 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 토큰을 가장 효율적으로 획득하려면 애플리케이션 통합 SDK를 사용하는 것이 좋습니다. 자세한 정보는 AWS WAF 클라이언트 애플리케이션 통합을 참조하세요. 규칙 작업: Challenge 레이블: 없음

규칙 이름	설명 및 레이블
RiskScoreHigh	계정 생성 요청이 매우 의심스러운 것으로 간주되는 IP 주소 또는 기타 요인을 포함하는지 검사합니다. 이 평가는 일반적으로 여러 기여 요인을 기반으로 하며, 이러한 요인은 규칙 그룹이 요청에 추가하는 risk_score 레이블에서 확인할 수 있습니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:acfp:risk_score:high 이 규칙은 요청에 medium 또는 low 위험 점수 레이블을 적용할 수도 있습니다. 웹 요청의 위험 점수를 평가하지 AWS WAF 못하면 규칙에 따라 레이블이 추가됩니다. awswaf:managed:aws:acfp:risk_score:evaluation_failed 또한 이 규칙은 네임스페이스가 awswaf:managed:aws:acfp:risk_score:contributor: 인 레이블을 추가하는데, 이 레이블에는 IP 신뢰도 및 도용된 보안 인증 정보 평가와 같은 특정 위험 점수 참여자에 대한 위험 점수 평가 상태 및 결과가 포함됩니다.

규칙 이름	설명 및 레이블
`SignalCredentialCompromised`	도용된 보안 인증 정보 데이터베이스에서 계정 생성 요청에 제출된 보안 인증 정보를 검색합니다. 이 규칙을 사용하면 신규 클라이언트가 확실한 보안 태세를 갖춘 상태에서 자신들의 계정을 초기화할 수 있습니다. **Note** 사용자 지정 차단 응답을 추가하여 최종 사용자에게 문제를 설명하고 진행 방법을 알려줄 수 있습니다. 자세한 내용은 ACFP 예제: 손상된 보안 인증 정보에 대한 사용자 지정 응답을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:signal:credential_compromised` 규칙 그룹은 다음과 같은 관련 레이블을 적용하지만 계정 생성 시 모든 요청에 `awswaf:managed:aws:acfp:signal:missing_credential` 보안 인증 정보가 있는 것은 아니기 때문에 이러한 레이블에 대해 아무런 작업도 수행하지 않습니다.

규칙 이름	설명 및 레이블
`SignalClientHumanInteractivityAbsentLow`	계정 생성 요청 토큰에서 애플리케이션과 사용자의 비정상적인 상호 작용을 나타내는 데이터가 있는지 검사합니다. 사용자 상호 작용은 마우스 동작 및 키 누름과 같은 상호 작용을 통해 탐지됩니다. 페이지에 HTML 양식이 있는 경우 사용자 상호 작용에는 양식과의 상호 작용이 포함됩니다. **Note** 이 규칙은 계정 생성 경로에 대한 요청만 검사하며 애플리케이션 통합 SDK를 구현한 경우에만 평가됩니다. SDK 구현은 사용자 상호 작용을 수동적으로 캡처하여 요청 토큰에 정보를 저장합니다. 자세한 내용은 AWS WAF 토큰 특성 및 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. 규칙 작업: CAPTCHA 레이블: 없음. 이 규칙은 다양한 요인을 기반으로 일치 항목을 결정하므로 가능한 모든 일치 시나리오에 적용되는 개별 레이블은 없습니다. 규칙 그룹은 다음 레이블 중 하나 이상을 요청에 적용할 수 있습니다. `awswaf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high`

규칙 이름	설명 및 레이블
	awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data awswaf:managed:aws:acfp:signal:form_detected .
SignalAutomatedBrowser	요청에 클라이언트 브라우저가 자동화될 수 있음을 나타내는 표시자가 있는지 검사합니다. 규칙 작업: Block Label(레이블): awswaf:managed:aws:acfp:signal:automated_browser
SignalBrowserInconsistency	요청 토큰에 일치하지 않는 브라우저 질문 데이터가 있는지 검사합니다. 자세한 정보는 AWS WAF 토큰 특성을 참조하세요. 규칙 작업: CAPTCHA Label(레이블): awswaf:managed:aws:acfp:signal:browser_inconsistency

규칙 이름	설명 및 레이블
`VolumetricIpHigh`	개별 IP 주소에서 대용량의 계정 생성 요청이 전송되었는지 검사합니다. 대량이란 10분의 시간 동안 20개가 넘는 요청을 의미합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 대량의 경우 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: CAPTCHA Label(레이블): `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` 이 규칙은 중간 용량 (10분당 요청 15개 초과) 및 저용량 (10분당 요청 10개 초과) 의 요청에 다음 레이블을 적용하지만 이에 대해서는 아무런 조치도 취하지 않습니다`awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low` . `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium`

규칙 이름	설명 및 레이블
`VolumetricSessionHigh`	개별 클라이언트 세션에서 대량의 계정 생성 요청이 전송되었는지 검사합니다. 대량이란 30분의 시간 동안 10개가 넘는 요청을 의미합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:high` 규칙 그룹은 중간 볼륨 (30분당 요청 5개 초과) 및 저용량 (30분 창당 요청 1개 초과) 의 요청에 다음 레이블을 적용하지만 이에 대해서는 아무런 조치도 취하지 않습니다`awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:low` . `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:medium`

규칙 이름	설명 및 레이블
`AttributeUsernameTraversalHigh`	단일 클라이언트 세션에서 다양한 사용자 이름을 사용하는 계정 생성 요청의 비율이 높은지 검사합니다. 30분 동안 요청 수가 10개가 넘으면 높음으로 평가됩니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` 규칙 그룹은 사용자 이름 순회 요청의 중간 볼륨 (30분당 요청 5개 초과) 및 저용량 (30분당 요청 1개 이상) 이 있는 요청에 다음 레이블을 적용하지만 이에 대해서는 아무런 조치도 취하지 않습니다`awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low` . `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium`

규칙 이름	설명 및 레이블
`VolumetricPhoneNumberHigh`	동일한 전화번호를 사용하는 계정 생성 요청이 많은지 검사합니다. 30분 동안 요청 수가 10개가 넘으면 높음으로 평가됩니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high` 규칙 그룹은 중간 볼륨 (30분당 요청 5개 초과) 및 저용량 (30분당 요청 1개 초과) 의 요청에 다음 레이블을 적용하지만 이에 대해서는 아무런 조치도 취하지 않습니다`awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low` . `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium`

규칙 이름	설명 및 레이블
`VolumetricAddressHigh`	동일한 실제 주소를 사용하는 계정 생성 요청이 많은지 검사합니다. 30분 동안 요청 수가 100개가 넘으면 높음으로 평가됩니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:aggregate:volumetric:address:high`

규칙 이름	설명 및 레이블
`VolumetricAddressLow`	소량 및 중간 용량의 계정 생성 요청에서 동일한 물리적 주소가 사용되는지 검사합니다. 중간 평가의 임계값은 30분 기간당 요청 50개 이상이고, 낮은 평가의 임계값은 30분 기간당 요청 10개 이상입니다. 이 규칙은 중간 용량 또는 소량에 모두 작업을 적용합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: CAPTCHA 레이블: `awswaf:managed:aws:acfp:aggregate:volumetric:address:low` 또는 `awswaf:managed:aws:acfp:aggregate:volumetric:address:medium`

규칙 이름	설명 및 레이블
`VolumetricIPSuccessfulResponse`	단일 IP 주소에 대한 성공적인 계정 생성 요청이 많은지 검사합니다. 이 규칙은 계정 생성 요청에 대한 보호된 리소스의 성공 응답을 집계합니다. 10분 동안 요청 수가 10개가 넘으면 높음으로 평가됩니다. 이 규칙은 대량 계정 생성 시도를 방지하는 데 도움이 됩니다. 이 규칙은 요청만 계산하는 `VolumetricIpHigh` 규칙보다 임계값이 낮습니다. 응답 본문이나 JSON 구성 요소를 검사하도록 규칙 그룹을 구성한 경우 이러한 구성 요소 유형의 처음 65,536바이트 (64KB) 에서 성공 또는 실패 지표를 AWS WAF 검사할 수 있습니다. 이 규칙은 동일한 IP 주소에서 발생한 최근 로그인 시도에 대한 보호된 리소스의 성공 및 실패 응답을 기반으로 IP 주소의 새 웹 요청에 규칙 작업 및 레이블링을 적용합니다. 규칙 그룹을 구성할 때 성공과 실패를 계산하는 방법을 정의합니다. **Note** AWS WAF Amazon CloudFront 배포를 보호하는 웹 ACL에서만 이 규칙을 평가합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 클라

규칙 이름	설명 및 레이블
	이언트는 규칙이 후속 시도에서 매칭을 시작하기 전에 허용되는 횟수보다 더 많은 성공 계정 생성 시도 횟수를 전송할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high` 또한 규칙 그룹은 어떠한 연결된 작업도 없이 다음과 같은 관련 레이블을 요청에 적용합니다. 모든 개수는 10분 기간 기준입니다. 성공 요청이 5개 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium`, 성공 요청이 1개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low`, 실패 요청이 10개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high`, 실패 요청이 5개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium`, 그리고 실패 요청이 1개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low` 입니다.

규칙 이름	설명 및 레이블
`VolumetricSessionSuccessful Response`	단일 클라이언트 세션에서 전송되는 계정 생성 요청에 대해 보호된 리소스의 성공 응답이 적은지 검사합니다. 이는 대량 계정 생성 시도를 방지하는 데 도움이 됩니다. 30분 기간당 요청 수가 1개가 넘으면 낮음으로 평가됩니다. 이는 대량 계정 생성 시도를 방지하는 데 도움이 됩니다. 이 규칙은 요청만 추적하는 `VolumetricSessionHigh` 규칙보다 낮은 임계값을 사용합니다. 응답 본문 또는 JSON 구성 요소를 검사하도록 규칙 그룹을 구성한 경우 이러한 구성 요소 유형의 처음 65,536바이트 (64KB) 에서 성공 또는 실패 지표를 AWS WAF 검사할 수 있습니다. 이 규칙은 동일한 클라이언트 세션에서 발생한 최근 로그인 시도에 대한 보호된 리소스의 성공 및 실패 응답을 기반으로 클라이언트 세션의 새 웹 요청에 규칙 작업 및 레이블링을 적용합니다. 규칙 그룹을 구성할 때 성공과 실패를 계산하는 방법을 정의합니다. **Note** AWS WAF Amazon CloudFront 배포를 보호하는 웹 ACL에서만 이 규칙을 평가합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 클라

규칙 이름	설명 및 레이블
	이언트는 규칙이 후속 시도에서 매칭을 시작하기 전에 허용되는 횟수보다 더 많은 실패 계정 생성 시도 횟수를 전송할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low` 또한 규칙 그룹은 다음과 같은 관련 레이블을 요청에 적용합니다. 모든 개수는 30분 기간 기준입니다. 성공 요청이 10개 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high` , 성공 요청이 5개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:medium` , 실패 요청이 10개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high` , 실패 요청이 5개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium` , 그리고 실패 요청이 1개가 넘는 경우 `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low` 입니다.

규칙 이름	설명 및 레이블
`VolumetricSessionTokenReuseIp`	5개가 넘는 고유 IP 주소에서 단일 토큰이 사용되는 계정 생성 요청이 있는지 검사합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesATPRuleSet`, WCU: 50

AWS WAF 사기 방지 계정 탈취 방지 (ATP) 는 악의적인 계정 탈취 시도의 일부일 수 있는 요청에 규칙 그룹 레이블을 지정하고 요청을 관리합니다. 규칙 그룹은 클라이언트가 애플리케이션의 로그인 엔드포인트로 보내는 로그인 시도를 검사하여 이 작업을 수행합니다.

- 요청 검사 — ATP를 사용하면 비정상적인 로그인 시도 및 보안 인증 정보를 도용한 로그인 시도를 파악하고 제어할 수 있으므로 사기 행위로 이어질 수 있는 계정 탈취를 방지할 수 있습니다. ATP는 도용된 보안 인증 정보 데이터베이스에서 이메일과 암호 조합을 검사합니다. 이 데이터베이스는 유출된 보안 인증 정보가 다크 웹에서 발견될 때마다 정기적으로 업데이트됩니다. ATP는 IP 주소 및 클라이언트 세션별로 데이터를 집계하여 의심스러운 요청을 너무 많이 보내는 클라이언트를 탐지하고 차단합니다.
- 응답 검사 — CloudFront 배포의 경우 ATP 규칙 그룹은 들어오는 로그인 요청을 검사하는 것 외에도 로그인 시도에 대한 애플리케이션의 응답을 검사하여 성공률과 실패율을 추적합니다. ATP는 이 정보를 사용하여 로그인 실패가 너무 많은 클라이언트 세션 또는 IP 주소를 일시적으로 차단할 수 있습

니다. AWS WAF 는 응답 검사를 비동기적으로 수행하므로 이 작업으로 인해 웹 트래픽의 지연 시간이 증가하지 않습니다.

이 규칙 그룹 사용 시 고려할 사항

이 규칙 그룹에는 특정 구성이 필요합니다. 이 규칙 그룹을 구성하고 구현하려면 AWS WAF 사기 방지 계정 탈취 방지 (ATP)의 지침을 참조하세요.

이 규칙 그룹은 AWS WAF에 지능형 위협 완화 보호의 일부로 포함됩니다. 자세한 내용은 AWS WAF 지능형 위협 완화을 참조하세요.

> **Note**
>
> 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

지속적으로 비용을 절감하고 웹 트래픽이 필요에 맞게 관리되도록 하려면 지능형 위협 완화 모범 사례의 지침에 따라 이 규칙 그룹을 사용하십시오.

이 규칙 그룹은 Amazon Cognito 사용자 풀과 함께 사용할 수 없습니다. 이 규칙 그룹을 사용하는 웹 ACL을 사용자 풀과 연결할 수 없으며, 이미 사용자 풀과 연결된 웹 ACL에 이 규칙 그룹을 추가할 수 없습니다.

이 규칙 그룹에서 추가한 레이블

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

토큰 레이블

이 규칙 그룹은 AWS WAF 토큰 관리를 사용하여 토큰 상태에 따라 웹 요청을 검사하고 AWS WAF 레이블을 지정합니다. AWS WAF 토큰을 사용하여 클라이언트 세션을 추적하고 확인합니다.

토큰 및 토큰 관리에 대한 자세한 내용은 AWS WAF 웹 요청 토큰을(를) 참조하십시오.

여기에 설명된 레이블 구성 요소에 대한 자세한 내용은 AWS WAF 레이블 구문 및 이름 지정 요구 사항을(를) 참조하십시오.

클라이언트 세션 레이블

`awswaf:managed:token:id:`*`identifier`*라벨에는 AWS WAF 토큰 관리가 클라이언트 세션을 식별하는 데 사용하는 고유 식별자가 들어 있습니다. 클라이언트가 새 토큰을 획득하는 경우(예: 사용하고 있던 토큰을 폐기한 후) 식별자가 변경될 수 있습니다.

> **Note**
>
> AWS WAF 이 라벨에 대한 Amazon CloudWatch 메트릭을 보고하지 않습니다.

토큰 상태 레이블: 레이블 네임스페이스 접두사

토큰 상태 레이블은 토큰 및 챌린지 상태와 토큰에 포함된 CAPTCHA 정보를 보고합니다.

각 토큰 상태 레이블은 다음 네임스페이스 접두사 중 하나로 시작합니다.

- `awswaf:managed:token:` – 토큰의 일반 상태를 보고하고 토큰의 챌린지 정보 상태를 보고하는 데 사용됩니다.
- `awswaf:managed:captcha:` – 토큰의 CAPTCHA 정보 상태를 보고하는 데 사용됩니다.

토큰 상태 레이블: 레이블 이름

접두사 뒤에 오는 라벨의 나머지 부분은 자세한 토큰 상태 정보를 제공합니다.

- `accepted` – 요청 토큰이 존재하며 다음을 포함합니다.
  - 유효한 챌린지 또는 CAPTCHA 솔루션.
  - 만료되지 않은 챌린지 또는 CAPTCHA 타임스탬프.
  - 웹 ACL에 대해 유효한 도메인 사양입니다.

  예: 레이블 `awswaf:managed:token:accepted`은(는) 웹 요청의 토큰에 유효한 인증 확인 솔루션, 만료되지 않은 챌린지 타임스탬프 및 유효한 도메인이 있음을 나타냅니다.
- `rejected` – 요청 토큰이 존재하지만 수락 기준을 충족하지 않습니다.

  거부된 레이블과 함께 토큰 관리는 사용자 지정 레이블 네임스페이스 및 이름을 추가하여 이유를 나타냅니다.
  - `rejected:not_solved` – 토큰에 챌린지 또는 CAPTCHA 솔루션이 없습니다.

  - `rejected:expired` – 웹 ACL의 구성된 토큰 면역 시간에 따라 토큰의 챌린지 또는 CAPTCHA 타임스탬프가 만료되었습니다.
  - `rejected:domain_mismatch` – 토큰의 도메인이 웹 ACL의 토큰 도메인 구성과 일치하지 않습니다.
  - `rejected:invalid`— AWS WAF 표시된 토큰을 읽을 수 없습니다.

  예: 레이블 `awswaf:managed:captcha:rejected` 및 `awswaf:managed:captcha:rejected:expired`은(는) 토큰의 CAPTCHA 타임스탬프가 웹 ACL에 구성된 CAPTCHA 토큰 면역 시간을 초과했기 때문에 요청이 거부되었음을 나타냅니다.
- `absent` – 요청에 토큰이 없거나 토큰 관리자가 토큰을 읽을 수 없습니다.

  예: 레이블 `awswaf:managed:captcha:absent`은(는) 요청에 토큰이 없음을 나타냅니다.

ATP 레이블

ATP 관리형 규칙 그룹은 네임스페이스 접두사 `awswaf:managed:aws:atp:` 다음에 사용자 지정 네임스페이스와 레이블 이름이 이어지는 레이블을 생성합니다.

규칙 그룹은 규칙 목록에 나와 있는 레이블 외에도 다음 레이블 중 하나를 추가할 수 있습니다.

- `awswaf:managed:aws:atp:signal:credential_compromised` - 요청에서 제출된 보안 인증 정보가 도용된 보안 인증 정보 데이터베이스에 있음을 나타냅니다.
- `awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint`— 보호 대상 Amazon CloudFront 배포에만 사용할 수 있습니다. 클라이언트 세션에서 의심스러운 TLS 핑거프린트를 사용한 요청을 여러 번 보냈음을 나타냅니다.
- `awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip` - 단일 토큰이 5개 이상의 고유 IP 주소에서 사용되었음을 나타냅니다. 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 레이블이 적용되기 전에 몇 개의 요청이 제한을 초과할 수 있습니다.

`DescribeManagedRuleGroup`를 호출하여 API를 통해 규칙 그룹의 모든 레이블을 검색할 수 있습니다. 레이블은 응답의 `AvailableLabels` 속성에 나열됩니다.

계정 탈취 방지 규칙 목록

이 섹션에는 `AWSManagedRulesATPRuleSet`의 ATP 규칙과 규칙 그룹의 규칙이 웹 요청에 추가하는 레이블이 나열되어 있습니다.

> **Note**
>
> AWS 관리형 규칙 규칙 그룹의 규칙에 대해 당사가 게시하는 정보는 규칙을 사용하기에 충분한 정보를 제공하는 동시에 악의적인 행위자가 규칙을 우회하는 데 사용할 수 있는 정보는 제공하지 않기 위한 것입니다. 이 설명서의 내용 외에 더 많은 정보가 필요한 경우 AWS Support 센터에 문의하십시오.

규칙 이름	설명 및 레이블
`UnsupportedCognitoIDP`	Amazon Cognito 사용자 풀로 이동하는 웹 트래픽을 검사합니다. ATP는 Amazon Cognito 사용자 풀과 함께 사용할 수 없으므로, 이 규칙은 다른 ATP 규칙 그룹 규칙이 사용자 풀 트래픽을 평가하는 데 사용되지 않도록 하는 데 도움이 됩니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:unsupported:cognito_idp`
`VolumetricIpHigh`	개별 IP 주소에서 대용량의 요청이 전송되었는지 검사합니다. 대량이란 10분의 시간 동안 20개가 넘는 요청을 의미합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 대량의 경우 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Block

규칙 이름	설명 및 레이블
	Label(레이블): `awswaf:managed:aws:atp:aggregate:volumetric:ip:high` 규칙 그룹은 중간 볼륨 (10분당 요청 15개 이상) 및 저용량 (10분 창당 요청 10개 초과) 의 요청에 다음 레이블을 적용하지만 이에 대해서는 아무런 조치도 취하지 않습니다. `awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` `awswaf:managed:aws:atp:aggregate:volumetric:ip:low`

규칙 이름	설명 및 레이블
`VolumetricSession`	개별 클라이언트 세션에서 대용량의 요청이 전송되었는지 검사합니다. 30분 동안 요청 수가 20개를 초과하는 것이 임계값입니다. 이 검사는 웹 요청에 토큰이 있는 경우에만 적용됩니다. 토큰은 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 자세한 정보는 AWS WAF 웹 요청 토큰을 참조하세요. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:aggregate:volumetric:session`
`AttributeCompromisedCredentials`	동일한 클라이언트 세션의 여러 요청에서 도용된 보안 인증 정보가 사용되는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials`

규칙 이름	설명 및 레이블
`AttributeUsernameTraversal`	사용자 이름 순회를 사용하는 동일한 클라이언트 세션에서 여러 요청이 있는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:aggregate:attribute:username_traversal`
`AttributePasswordTraversal`	암호 탐색을 사용하는 동일한 사용자 이름을 사용하는 여러 요청이 있는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:aggregate:attribute:password_traversal`
`AttributeLongSession`	오래 지속되는 세션을 사용하는 동일한 클라이언트 세션에서 여러 요청이 있는지 검사합니다. 임계값은 6시간 이상의 트래픽으로, 30분마다 로그인 요청이 하나 이상 발생하는 경우입니다. 이 검사는 웹 요청에 토큰이 있는 경우에만 적용됩니다. 토큰은 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 자세한 정보는 AWS WAF 웹 요청 토큰을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:aggregate:attribute:long_session`

규칙 이름	설명 및 레이블
`TokenRejected`	토큰 관리에 의해 AWS WAF 거부된 토큰이 포함된 요청이 있는지 검사합니다. 이 검사는 웹 요청에 토큰이 있는 경우에만 적용됩니다. 토큰은 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 자세한 정보는 AWS WAF 웹 요청 토큰을 참조하세요. 규칙 작업: Block 레이블: 없음. 거부된 토큰이 있는지 확인하려면 레이블 일치 규칙 `awswaf:managed:token:rejected` 를 사용하여 레이블을 일치시킵니다.
`SignalMissingCredential`	사용자 이름 또는 암호가 누락된 보안 인증 정보를 포함하는 요청이 있는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:signal:missing_credential`

규칙 이름	설명 및 레이블
`VolumetricIpFailedLoginResponseHigh`	최근에 로그인 시도 실패율이 너무 높은 IP 주소가 있는지 검사합니다. 대용량이란 10분의 시간 동안 한 IP 주소에서 10개가 넘는 로그인 요청 실패가 있음을 의미합니다. 응답 본문이나 JSON 구성 요소를 검사하도록 규칙 그룹을 구성한 경우 이러한 구성 요소 유형의 처음 65,536바이트 (64KB) 에서 성공 또는 실패 지표를 AWS WAF 검사할 수 있습니다. 이 규칙은 동일한 IP 주소에서 발생한 최근 로그인 시도에 대한 보호된 리소스의 성공 및 실패 응답을 기반으로 IP 주소의 새 웹 요청에 규칙 작업 및 레이블링을 적용합니다. 규칙 그룹을 구성할 때 성공과 실패를 계산하는 방법을 정의합니다. **Note** AWS WAF Amazon CloudFront 배포를 보호하는 웹 ACL에서만 이 규칙을 평가합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 클라이언트는 규칙이 후속 시도에서 매칭을 시작하기 전에 허용되는 횟수보다 더 많은 실패 로그인 시도 횟수를 전송할 수 있습니다.

규칙 이름	설명 및 레이블
	규칙 작업: Block Label(레이블): awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high 또한 규칙 그룹은 어떠한 연결된 작업도 없이 다음과 같은 관련 레이블을 요청에 적용합니다. 모든 개수는 10분 기간 기준입니다. 실패 요청이 5개 넘는 경우 awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium , 실패 요청이 1개가 넘는 경우 awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low , 성공 요청이 10개가 넘는 경우 awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high , 성공 요청이 5개가 넘는 경우 awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:medium , 그리고 성공 요청이 1개가 넘는 경우 awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low 입니다.

규칙 이름	설명 및 레이블
`VolumetricSessionFailedLogi nResponseHigh`	최근에 로그인 시도 실패율이 너무 높은 클라이언트 세션이 있는지 검사합니다. 대용량이란 30분의 시간 동안 한 클라이언트 세션에서 10개가 넘는 로그인 요청 실패가 있음을 의미합니다. 응답 본문 또는 JSON 구성 요소를 검사하도록 규칙 그룹을 구성한 경우 이러한 구성 요소 유형의 처음 65,536바이트 (64KB) 에서 성공 또는 실패 지표를 AWS WAF 검사할 수 있습니다. 이 규칙은 동일한 클라이언트 세션에서 발생한 최근 로그인 시도에 대한 보호된 리소스의 성공 및 실패 응답을 기반으로 클라이언트 세션의 새 웹 요청에 규칙 작업 및 레이블링을 적용합니다. 규칙 그룹을 구성할 때 성공과 실패를 계산하는 방법을 정의합니다. **Note** AWS WAF Amazon CloudFront 배포를 보호하는 웹 ACL에서만 이 규칙을 평가합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 클라이언트는 규칙이 후속 시도에서 매칭을 시작하기 전에 허용되는 횟수보다 더 많은 실패 로그인 시도 횟수를 전송할 수 있습니다.

규칙 이름	설명 및 레이블
	이 검사는 웹 요청에 토큰이 있는 경우에만 적용됩니다. 토큰은 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 자세한 정보는 AWS WAF 웹 요청 토큰을 참조하세요. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high` 또한 규칙 그룹은 어떠한 연결된 작업도 없이 다음과 같은 관련 레이블을 요청에 적용합니다. 모든 개수는 30분 기간 기준입니다. 실패 요청이 5개 넘는 경우 `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium` , 실패 요청이 1개가 넘는 경우 `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:low` , 성공 요청이 10개가 넘는 경우 `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:high` , 성공 요청이 5개가 넘는 경우 `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium` , 그리고 성공 요청이 1개가 넘는 경우 `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low` 입니다.

AWS WAF 봇 컨트롤 규칙 그룹

VendorName:`AWS`, 이름:`AWSManagedRulesBotControlRuleSet`, WCU: 50

Bot Control 관리형 규칙 그룹은 봇의 요청을 관리하는 규칙을 제공합니다. 봇은 과도한 리소스를 소비하고, 비즈니스 지표를 왜곡하며, 가동 중지를 유발하고, 악의적인 활동을 수행할 수 있습니다.

보호 수준

Bot Control 관리형 규칙 그룹은 선택할 수 있는 두 가지 보호 수준을 제공합니다.

- 일반 - 웹 스크레이핑 프레임워크, 검색 엔진 및 자동 브라우저 등 다양한 자체 식별 봇을 탐지합니다. 이 수준의 Bot Control 보호는 정적 요청 데이터 분석과 같은 기존 봇 탐지 기술을 사용하여 일반적인 봇을 식별합니다. 이 규칙은 이러한 봇의 트래픽에 레이블을 지정하고 확인할 수 없는 트래픽은 차단합니다.
- 대상 - 공통 수준의 보호 기능을 포함하고 자체 식별이 불가능한 정교한 봇에 대한 대상 탐지 기능을 추가합니다. 대상 보호는 속도 제한과 CAPTCHA 및 백그라운드 브라우저 챌린지를 함께 사용하여 봇 활동을 완화합니다.
  - **`TGT_`** - 대상 보호를 제공하는 규칙의 이름은 `TGT_`로 시작합니다. 모든 대상 보호는 브라우저 질의, 지문 및 행동 휴리스틱과 같은 탐지 기술을 사용하여 잘못된 봇 트래픽을 식별합니다.
  - **`TGT_ML_`**— 기계 학습을 사용하는 대상 보호 규칙의 이름은 `TGT_ML_`로 시작합니다. 이 규칙은 웹사이트 트래픽 통계에 대한 자동화된 기계 학습 분석을 사용하여 분산되고 조정된 봇 활동을 나타내는 비정상적인 동작을 탐지합니다. AWS WAF 타임스탬프, 브라우저 특성, 이전 방문 URL 등 웹사이트 트래픽에 대한 통계를 분석하여 Bot Control 머신 러닝 모델을 개선합니다. 기계 학습 기능은 기본적으로 활성화되지만 규칙 그룹 구성에서 비활성화할 수 있습니다. 기계 학습이 비활성화된 경우 이러한 규칙을 평가하지 AWS WAF 않습니다.

대상 보호 수준과 AWS WAF 속도 기반 규칙 설명 모두 속도 제한을 제공합니다. 두 옵션에 대한 비교는 속도 기반 규칙 및 대상 지정 Bot Control 규칙의 속도 제한 옵션 섹션을 참조하세요.

이 규칙 그룹 사용 시 고려할 사항

이 규칙 그룹은 AWS WAF에 지능형 위협 완화 보호의 일부로 포함됩니다. 자세한 내용은 AWS WAF 지능형 위협 완화을 참조하세요.

> **Note**
>
> 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

지속적으로 비용을 절감하고 웹 트래픽이 필요에 맞게 관리되도록 하려면 지능형 위협 완화 모범 사례의 지침에 따라 이 규칙 그룹을 사용하십시오.

당사는 봇 예측을 개선하기 위해 대상 보호 수준 ML 기반 규칙에 맞게 기계 학습 (ML) 모델을 주기적으로 업데이트합니다. ML 기반 규칙에는 로 시작하는 이름이 있습니다. `TGT_ML_` 이러한 규칙으로 인해 봇 예측에 갑작스럽고 상당한 변화가 있는 경우 계정 관리자를 통해 문의하거나 센터에서 사례를 개설하십시오.AWS Support

이 규칙 그룹에서 추가한 레이블

이 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 이 레이블은 웹 ACL에서 이 규칙 그룹 이후에 실행되는 규칙에 사용할 수 있습니다. AWS WAF 또한 레이블을 Amazon CloudWatch 메트릭에 기록합니다. 레이블 및 레이블 지표에 대한 일반적인 내용은 웹 요청의 레이블 및 레이블 지표 및 차원 섹션을 참조하세요.

토큰 레이블

이 규칙 그룹은 AWS WAF 토큰 관리를 사용하여 토큰 상태에 따라 웹 요청을 검사하고 AWS WAF 레이블을 지정합니다. AWS WAF 토큰을 사용하여 클라이언트 세션을 추적하고 확인합니다.

토큰 및 토큰 관리에 대한 자세한 내용은 AWS WAF 웹 요청 토큰을(를) 참조하십시오.

여기에 설명된 레이블 구성 요소에 대한 자세한 내용은 AWS WAF 레이블 구문 및 이름 지정 요구 사항을(를) 참조하십시오.

클라이언트 세션 레이블

`awswaf:managed:token:id:`*`identifier`*라벨에는 AWS WAF 토큰 관리가 클라이언트 세션을 식별하는 데 사용하는 고유 식별자가 들어 있습니다. 클라이언트가 새 토큰을 획득하는 경우(예: 사용하고 있던 토큰을 폐기한 후) 식별자가 변경될 수 있습니다.

> **Note**
>
> AWS WAF 이 라벨에 대한 Amazon CloudWatch 메트릭을 보고하지 않습니다.

토큰 상태 레이블: 레이블 네임스페이스 접두사

토큰 상태 레이블은 토큰 및 챌린지 상태와 토큰에 포함된 CAPTCHA 정보를 보고합니다.

각 토큰 상태 레이블은 다음 네임스페이스 접두사 중 하나로 시작합니다.

- `awswaf:managed:token:` – 토큰의 일반 상태를 보고하고 토큰의 챌린지 정보 상태를 보고하는 데 사용됩니다.
- `awswaf:managed:captcha:` – 토큰의 CAPTCHA 정보 상태를 보고하는 데 사용됩니다.

토큰 상태 레이블: 레이블 이름

접두사 뒤에 오는 라벨의 나머지 부분은 자세한 토큰 상태 정보를 제공합니다.

- `accepted` – 요청 토큰이 존재하며 다음을 포함합니다.
  - 유효한 챌린지 또는 CAPTCHA 솔루션.
  - 만료되지 않은 챌린지 또는 CAPTCHA 타임스탬프.
  - 웹 ACL에 대해 유효한 도메인 사양입니다.

  예: 레이블 `awswaf:managed:token:accepted`은(는) 웹 요청의 토큰에 유효한 인증 확인 솔루션, 만료되지 않은 챌린지 타임스탬프 및 유효한 도메인이 있음을 나타냅니다.
- `rejected` – 요청 토큰이 존재하지만 수락 기준을 충족하지 않습니다.

  거부된 레이블과 함께 토큰 관리는 사용자 지정 레이블 네임스페이스 및 이름을 추가하여 이유를 나타냅니다.
  - `rejected:not_solved` – 토큰에 챌린지 또는 CAPTCHA 솔루션이 없습니다.
  - `rejected:expired` – 웹 ACL의 구성된 토큰 면역 시간에 따라 토큰의 챌린지 또는 CAPTCHA 타임스탬프가 만료되었습니다.
  - `rejected:domain_mismatch` – 토큰의 도메인이 웹 ACL의 토큰 도메인 구성과 일치하지 않습니다.
  - `rejected:invalid`— AWS WAF 표시된 토큰을 읽을 수 없습니다.

  예: 레이블 `awswaf:managed:captcha:rejected` 및 `awswaf:managed:captcha:rejected:expired`은(는) 토큰의 CAPTCHA 타임스탬프가 웹 ACL에 구성된 CAPTCHA 토큰 면역 시간을 초과했기 때문에 요청이 거부되었음을 나타냅니다.
- `absent` – 요청에 토큰이 없거나 토큰 관리자가 토큰을 읽을 수 없습니다.

예: 레이블 `awswaf:managed:captcha:absent`은(는) 요청에 토큰이 없음을 나타냅니다.

Bot Control 레이블

Bot Control 관리형 규칙 그룹은 네임스페이스 접두사 `awswaf:managed:aws:bot-control:` 다음에 사용자 지정 네임스페이스와 레이블 이름이 이어지는 레이블을 생성합니다. 이 규칙 그룹은 요청 하나에 둘 이상의 레이블을 추가할 수도 있습니다.

각 레이블에는 Bot Control 규칙 결과가 반영됩니다.

- `awswaf:managed:aws:bot-control:bot:` – 요청과 관련된 봇에 대한 정보.
  - `awswaf:managed:aws:bot-control:bot:name:<name>` - 봇 이름(사용 가능한 경우) 예: 사용자 지정 네임스페이스 `bot:name:slurp`, `bot:name:googlebot` 및 `bot:name:pocket_parser`.
  - `awswaf:managed:aws:bot-control:bot:category:<category>`— 봇의 범주 (예: `bot:category:search_engine` 및 로 AWS WAF정의 됨)`bot:category:content_fetcher`.
  - `awswaf:managed:aws:bot-control:bot:organization:<organization>`— 봇의 게시자. 예: `bot:organization:google`.
  - `awswaf:managed:aws:bot-control:bot:verified` - Bot Control이 확인할 수 있는 자체 식별형 봇을 나타내는 데 사용됩니다. 이 레이블은 일반적으로 선호되는 봇에 사용되며, 카테고리 레이블(`bot:category:search_engine`)이나 이름 레이블(`bot:name:googlebot`)과 함께 사용할 경우 유용할 수 있습니다.

    > **Note**
    >
    > Bot Control은 웹 요청 오리진의 IP 주소를 사용하여 봇이 확인되는지 여부를 결정할 수 있도록 도와줍니다. AWS WAF 전달된 IP 구성을 사용하여 다른 IP 주소 소스를 검사하도록 구성할 수는 없습니다. 프록시나 로드 밸런서를 통해 라우팅되는 봇을 확인한 경우 Bot Control 규칙 그룹보다 먼저 실행되는 규칙을 추가하여 이를 지원할 수 있습니다. 전달된 IP 주소를 사용하고 확인된 봇의 요청을 명시적으로 허용하도록 새 규칙을 구성합니다. 전달된 IP 주소 사용에 대한 자세한 내용은 전달된 IP 주소 섹션을 참조하세요.

  - `awswaf:managed:aws:bot-control:bot:user_triggered:verified` - 확인된 봇과 비슷하지만 최종 사용자가 직접 호출할 수 있는 봇을 나타내는 데 사용됩니다. Bot Control 규칙은 이 범주의 봇을 확인되지 않은 봇처럼 취급합니다.

  - `awswaf:managed:aws:bot-control:bot:developer_platform:verified` - 확인된 봇과 비슷하지만 개발자 플랫폼(예: Google Apps Script)에서 스크립팅용으로 사용되는 봇을 나타내는 데 사용됩니다. . Bot Control 규칙은 이 범주의 봇을 확인되지 않은 봇처럼 취급합니다.
  - `awswaf:managed:aws:bot-control:bot:unverified` - 자체 식별형이어서 이름을 지정하고 분류할 수는 있지만 ID를 독립적으로 확인하는 데 사용할 수 있는 정보를 게시하지 않는 봇을 나타내는 데 사용됩니다. 이러한 유형의 봇 서명은 위조될 수 있으므로 확인되지 않은 것으로 간주됩니다.
- `awswaf:managed:aws:bot-control:targeted:<additional-details>` — Bot Control 대상 보호와 관련된 레이블에 사용됩니다.
- `awswaf:managed:aws:bot-control:signal:<signal-details>` 및 `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` - 일부 상황에서 요청에 대한 추가 정보를 제공하는 데 사용됩니다.

  다음은 신호 레이블의 예입니다. 이 목록은 전체 목록이 아닙니다.

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension` – Selenium IDE와 같이 자동화를 지원하는 브라우저 확장 프로그램이 탐지되었음을 나타냅니다.

    이 레이블은 사용자가 해당 확장 프로그램을 적극적으로 사용하지 않는 경우에도 사용자가 이러한 유형의 확장 프로그램을 설치할 때마다 추가됩니다. 이에 대한 레이블 일치 규칙을 구현하는 경우 규칙 로직 및 작업 설정에서 오탐이 발생할 가능성에 유의하세요. 예를 들어, 자동화가 사용되고 있음을 더욱 확신하기 위해 Block 대신 CAPTCHA 작업을 사용하거나 이 레이블 일치를 다른 레이블 일치와 결합할 수 있습니다.
  - `awswaf:managed:aws:bot-control:signal:automated_browser` - 요청에 클라이언트 브라우저가 자동화될 수 있음을 의미하는표시자가 포함되어 있음을 나타냅니다.
  - `awswaf:managed:aws:bot-control:targeted:signal:automated_browser`— 요청 AWS WAF 토큰에 클라이언트 브라우저가 자동화될 수 있다는 지표가 포함되어 있음을 나타냅니다.

`DescribeManagedRuleGroup`를 호출하여 API를 통해 규칙 그룹의 모든 레이블을 검색할 수 있습니다. 레이블은 응답의 `AvailableLabels` 속성에 나열됩니다.

Bot Control 관리형 규칙 그룹은 일반적으로 허용되는 확인 가능한 봇 집합에 레이블을 적용합니다. 규칙 그룹은 이러한 확인된 봇을 차단하지 않습니다. 원하는 경우 Bot Control 관리형 규칙 그룹에서 적용한 레이블을 사용하는 사용자 지정 규칙을 작성하여 이러한 봇을 차단하거나 그 중 일부를 차단할 수 있습니다. 이것과 예제에 대한 자세한 내용은 AWS WAF 봇 컨트롤 섹션을 참조하세요.

Bot Control 규칙 목록

이 섹션에는 Bot Control 규칙이 나열되어 있습니다.

> **Note**
>
> AWS 관리형 규칙 규칙 그룹의 규칙에 대해 게시하는 정보는 규칙을 사용하기에 충분한 정보를 제공하는 동시에 악의적인 공격자가 규칙을 우회하는 데 사용할 수 있는 정보는 제공하지 않기 위한 것입니다. 이 설명서의 내용 외에 더 많은 정보가 필요한 경우 AWS Support 센터에 문의하십시오.

규칙 이름	설명
`CategoryAdvertising`	광고 목적으로 사용되는 봇이 있는지 검사합니다. 예를 들어 웹 사이트에 프로그래밍 방식으로 액세스해야 하는 타사 광고 서비스를 사용할 수 있습니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:advertising` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`CategoryArchiver`	아카이브 목적으로 사용되는 봇이 있는지 검사합니다. 이러한 봇은 아카이브를 생성할 목적으로 웹을 크롤링하고 콘텐츠를 캡처합니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block

규칙 이름	설명
	Label(레이블): `awswaf:managed:aws:bot-control:bot:category:archiver` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`CategoryContentFetcher`	RSS 피드와 같은 콘텐츠를 가져오거나 콘텐츠를 확인 또는 검증하기 위해 사용자를 대신하여 애플리케이션 웹 사이트를 방문하는 봇이 있는지 검사합니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:content_fetcher` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`CategoryEmailClient`	이메일 안에 애플리케이션 웹 사이트를 가리키는 링크를 확인하는 봇이 있는지 검사합니다. 여기에는 기업 및 이메일 제공업체가 이메일의 링크를 확인하고 의심스러운 이메일에 플래그를 지정하기 위해 실행하는 봇이 포함될 수 있습니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:email_client` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`CategoryHttpLibrary`	다양한 프로그래밍 언어의 HTTP 라이브러리에서 봇이 생성하는 요청이 있는지 검사합니다. 여기에는 허용 또는 모니터링하기로 선택한 API 요청이 포함될 수 있습니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:http_library` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`CategoryLinkChecker`	끊긴 링크가 있는지 확인하는 봇이 있는지 검사합니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:link_checker` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`CategoryMiscellaneous`	다른 범주와 일치하지 않는 기타 봇이 있는지 검사합니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:miscellaneous` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`CategoryMonitoring`	모니터링 목적으로 사용되는 봇이 있는지 검사합니다. 예를 들면 애플리케이션 웹 사이트에 주기적으로 핑을 보내는 봇 모니터링 서비스를 사용하여 성능 및 가동 시간 등을 모니터링할 수 있습니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:monitoring` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`CategoryScrapingFramework`	크롤링을 자동화하고 웹 사이트에서 콘텐츠를 추출하는 데 사용되는 웹 스크래핑 프레임워크의 봇이 있는지 검사합니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:scraping_framework` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`CategorySearchEngine`	웹 사이트를 크롤링하여 콘텐츠를 인덱싱하고 검색 엔진 결과에 해당 정보를 제공하는 검색 엔진 봇이 있는지 검사합니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:search_engine` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`CategorySecurity`	웹 애플리케이션의 취약성을 검사하거나 보안 감사를 수행하는 봇이 있는지 검사합니다. 예를 들어 웹 애플리케이션의 보안을 검사, 모니터링 또는 감사하는 타사 보안 공급업체를 이용할 수 있습니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:security` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`CategorySeo`	검색 엔진 최적화에 사용되는 봇이 있는지 검사합니다. 예를 들어 사이트를 크롤링하는 검색 엔진 도구를 사용하여 검색 엔진 순위를 높일 수 있습니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:seo` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`CategorySocialMedia`	소셜 미디어 플랫폼에서 사용자가 콘텐츠를 공유할 때 콘텐츠 요약을 제공하는 데 사용하는 봇이 있는지 검사합니다. 확인되지 않은 봇에만 적용되는 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:social_media` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`CategoryAI`	인공 지능(AI) 봇이 있는지 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:bot:category:ai`
`SignalAutomatedBrowser`	요청에 클라이언트 브라우저가 자동화될 수 있음을 나타내는 표시자가 있는지 검사합니다. 자동화된 브라우저를 테스트 또는 스크레이핑에 사용할 수 있습니다. 예를 들어, 이러한 유형의 브라우저를 사용하여 애플리케이션 웹 사이트를 모니터링하거나 확인할 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:signal:automated_browser`
`SignalKnownBotDataCenter`	봇에서 일반적으로 사용되는 데이터 센터의 지표를 검사합니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:signal:known_bot_data_center`

규칙 이름	설명
`SignalNonBrowserUserAgent`	웹 브라우저에서 가져온 것으로 여겨지지 않는 사용자 에이전트 문자열을 검사합니다. 이 범주에는 API 요청이 포함될 수 있습니다. 규칙 작업: Block Label(레이블): `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`

규칙 이름	설명
TGT_VolumetricIpTokenAbsent	지난 5분 동안 클라이언트로부터 유효한 챌린지 토큰이 포함되지 않은 요청을 5개 이상 받았는지 검사합니다. 토큰에 대한 자세한 내용은 AWS WAF 웹 요청 토큰 섹션을 참조하세요. **Note** 최근에 동일한 클라이언트의 요청에 토큰이 누락된 경우 토큰이 있는 요청과 이 규칙이 일치할 수 있습니다. 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 이 규칙은 누락된 토큰을 토큰 레이블링 awswaf:managed:token:absent 과 다르게 처리합니다. 토큰 레이블링은 토큰이 없는 개별 요청에 레이블을 지정합니다. 이 규칙은 각 클라이언트 IP에 대해 토큰이 누락된 요청 수를 유지하며 제한을 초과하는 클라이언트를 기준으로 일치를 수행합니다. 확인된 봇이 아닌 클라이언트에만 적용되는 규칙 작업: Challenge Label(레이블): awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:ip:token_absent 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 awswaf:managed:aws:bot-control:bot:verified 레이블을 추가합니다.

규칙 이름	설명
`TGT_VolumetricSession`	5분 기간 동안 클라이언트 세션의 요청 수가 비정상적으로 많은지 검사합니다. 평가는 과거 트래픽 패턴을 사용하여 AWS WAF 유지 관리하는 표준 볼륨 측정 기준과의 비교를 기반으로 합니다. 이 검사는 웹 요청에 토큰이 있는 경우에만 적용됩니다. 토큰은 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 자세한 정보는 AWS WAF 웹 요청 토큰을 참조하세요. **Note** 이 규칙은 활성화한 후 적용되는 데 5분이 걸릴 수 있습니다. Bot Control은 현재 트래픽을 계산되는 트래픽 기준선과 비교하여 웹 트래픽의 비정상적인 동작을 식별합니다. AWS WAF 확인된 봇이 아닌 클라이언트에만 적용되는 규칙 작업: CAPTCHA Label(레이블): `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high` 규칙 그룹은 최소 임계값을 초과하는 중간 용량 및 저용량 요청에 다음 레이블을 적용합니다. `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` 및 `awswaf:managed:aws:bot-`

규칙 이름	설명
	`control:targeted:aggregate:volumetric:session:low` 수준의 경우 클라이언트 확인 여부와 상관없이 규칙이 아무런 작업도 수행하지 않습니다. 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.
`TGT_SignalAutomatedBrowser`	클라이언트 브라우저가 자동화될 수 있음을 나타내는 표시자가 있는지 요청의 토큰을 검사합니다. 자세한 정보는 AWS WAF 토큰 특성을 참조하세요. 이 검사는 웹 요청에 토큰이 있는 경우에만 적용됩니다. 토큰은 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 자세한 정보는 AWS WAF 웹 요청 토큰을 참조하세요. 확인된 봇이 아닌 클라이언트에만 적용되는 규칙 작업: CAPTCHA Label(레이블): `awswaf:managed:aws:bot-control:targeted:signal:automated_browser` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`TGT_SignalBrowserInconsistency`	일치하지 않는 브라우저 질문 데이터가 있는지 검사합니다. 자세한 정보는 AWS WAF 토큰 특성을 참조하세요. 이 검사는 웹 요청에 토큰이 있는 경우에만 적용됩니다. 토큰은 애플리케이션 통합 SDK와 규칙 작업 CAPTCHA 및 Challenge에 의해 요청에 추가됩니다. 자세한 정보는 AWS WAF 웹 요청 토큰을 참조하세요. 확인된 봇이 아닌 클라이언트에만 적용되는 규칙 작업: CAPTCHA Label(레이블): `awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
`TGT_TokenReuseIp`	5개가 넘는 고유 IP 주소에서 단일 토큰이 사용되는지 검사합니다. **Note** 이 규칙이 적용하는 임계값은 지연 시간으로 인해 약간 다를 수 있습니다. 규칙 작업이 적용되기 전에 몇 개의 요청이 한도를 초과할 수 있습니다. 규칙 작업: Count Label(레이블): `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip`

규칙 이름	설명
`TGT_ML_CoordinatedActivityMedium` 및 `TGT_ML_CoordinatedActivityHigh`	분산되고 조정된 봇 활동과 일치하는 이상 동작이 있는지 검사합니다. 규칙 수준은 요청 그룹이 협동 공격에 참여하는지에 대한 신뢰 수준을 나타냅니다. **Note** 이러한 규칙은 규칙 그룹이 기계 학습(ML)을 사용하도록 구성된 경우에만 실행됩니다. 이 선택 사항의 구성에 대한 자세한 내용은 웹 ACL에 AWS WAF 봇 제어 관리 규칙 그룹 추가 섹션을 참조하세요. AWS WAF 웹사이트 트래픽 통계의 기계 학습 분석을 통해 이 검사를 수행합니다. AWS WAF 몇 분마다 웹 트래픽을 분석하고 여러 IP 주소에 분산되어 있는 저강도, 장기간 지속되는 봇을 탐지할 수 있도록 분석을 최적화합니다. 이러한 규칙이 매우 적은 수의 요청과 일치하고 나면 협동 공격이 진행 중이지 않은 것으로 결정됩니다. 따라서 한 두 개만 일치하는 경우 결과가 거짓 긍정일 수도 있습니다. 하지만 이러한 규칙과 일치하는 항목이 많이 나오면 협동 공격을 받고 있는 상태일 것입니다. **Note** ML 옵션으로 Bot Control 대상 규칙을 활성화한 후에는 이러한 규칙이 적용되는 데 최대 24시간이 걸릴 수 있습니다. Bot Control은 현재 트래픽을 계산된 트

규칙 이름	설명
	래픽 기준선과 비교하여 웹 트래픽의 이상 행동을 식별합니다. AWS WAF AWS WAF Bot Control 대상 규칙을 ML 옵션과 함께 사용하는 동안에만 기준선을 계산하며, 의미 있는 기준을 설정하는 데 최대 24시간이 걸릴 수 있습니다. 봇 예측을 개선하기 위해 이러한 규칙에 대한 기계 학습 모델을 주기적으로 업데이트합니다. 이러한 규칙으로 인해 봇 예측에 갑작스럽고 큰 변화가 있는 것을 발견하면 계정 관리자에게 문의하거나 센터에서AWS Support 케이스를 개설하세요. 확인된 봇이 아닌 클라이언트에만 적용되는 규칙 작업: • Medium: Count • 높음: Count 레이블: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` 및 `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` 확인된 봇의 경우 규칙 그룹은 아무 작업도 하지 않지만 규칙 레이블과 `awswaf:managed:aws:bot-control:bot:verified` 레이블을 추가합니다.

규칙 이름	설명
	또한, 규칙 그룹은 낮은 신뢰 수준을 나타내는 레이블 `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` 을(를) 추가하지만 이러한 요청에 대해 규칙을 적용하거나 조치를 취하지는 않습니다.

버전이 지정된 관리형 AWS 규칙 그룹 배포

AWS 버전이 지정된 AWS 관리 규칙 그룹의 변경 내용을 릴리스 후보 버전, 정적 버전, 기본 버전의 세 가지 표준 배포로 배포합니다. 또한 예외 배포를 릴리스하거나 기본 버전 배포를 롤백해야 하는 AWS 경우도 있습니다.

> **Note**
>
> 이 섹션은 버전이 지정된 AWS 관리형 규칙 규칙 그룹에만 적용됩니다. 버전이 지정되지 않은 유일한 규칙 그룹은 IP 평판 규칙 그룹입니다.

주제

- AWS 관리형 규칙 규칙 그룹 배포에 대한 알림
- 관리형 규칙의 표준 배포 개요 AWS
- AWS 관리형 규칙의 일반적인 버전 상태
- 관리형 규칙의 출시 후보 AWS 배포
- 관리형 규칙을 위한 AWS 정적 버전 배포
- 관리형 규칙의 AWS 기본 버전 배포
- AWS 관리형 규칙의 예외 배포
- AWS 관리형 규칙의 기본 배포 롤백

AWS 관리형 규칙 규칙 그룹 배포에 대한 알림

버전이 지정된 AWS 관리형 규칙 그룹은 모두 배포에 대한 SNS 업데이트 알림을 제공하며 모두 동일한 SNS 주제 Amazon Resource Name (ARN) 을 사용합니다. 버전이 지정되지 않은 유일한 규칙 그룹은 IP 평판 규칙 그룹입니다.

기본 버전 변경과 같이 보호 기능에 영향을 미치는 배포의 경우, AWS 는 계획된 배포와 배포 시작 시기를 알려주는 SNS 알림을 제공합니다. 릴리스 후보 버전 및 정적 버전 배포와 같이 보호 기능에 영향을 미치지 않는 배포의 경우 배포가 시작된 후 또는 완료된 후에도 AWS 에서 알림을 제공할 수 있습니다. 새 정적 버전 배포가 완료되면 의 변경 AWS 관리형 규칙 변경 로그 로그와 의 문서 기록 페이지에서 이 안내서를 AWS 업데이트합니다. 문서 기록

AWS 관리형 규칙 규칙 그룹에 대한 모든 업데이트를 받으려면 이 가이드의 HTML 페이지에서 RSS 피드를 구독하고 AWS 관리형 규칙 규칙 그룹에 대한 SNS 주제를 구독하십시오. AWS SNS 알림 구독에 대한 자세한 내용은 을 참조하십시오. 관리형 규칙 그룹의 새 버전 및 업데이트에 대한 알림 받기

SNS 알림의 내용

Amazon SNS 알림의 필드에는 항상 제목, 메시지 및 가 포함됩니다 MessageAttributes.
추가 필드는 메시지 유형과 알림의 대상인 관리형 규칙 그룹에 따라 달라집니다. 다음은 `AWSManagedRulesCommonRuleSet`에 대한 알림 목록의 예입니다.

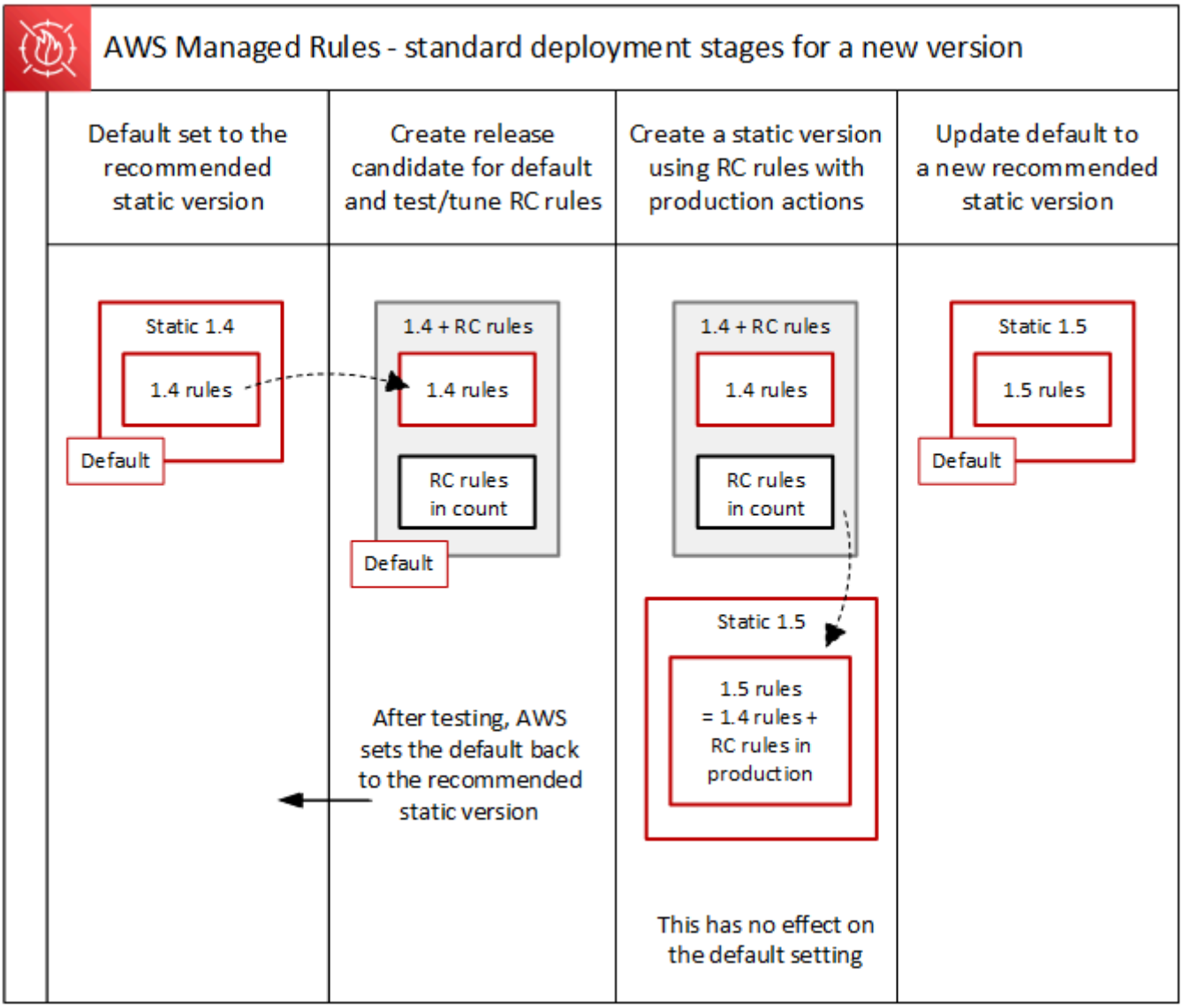
```
{
    "Type": "Notification",
    "MessageId": "4286b830-a463-5e61-bd15-e1ae72303868",
    "TopicArn": "arn:aws:sns:us-west-2:123456789012:MyTopic",
    "Subject": "New version available for rule group AWSManagedRulesCommonRuleSet",
    "Message": "Welcome to AWSManagedRulesCommonRuleSet version 1.5! We've updated
 the regex specification in this version to improve protection coverage, adding
 protections against insecure deserialization. For details about this change, see
 http://updatedPublicDocs.html. Look for more exciting updates in the future! ",
    "Timestamp": "2021-08-24T11:12:19.810Z",
    "SignatureVersion": "1",
    "Signature": "EXAMPLEHXgJm...",
    "SigningCertURL": "https://sns.us-west-2.amazonaws.com/SimpleNotificationService-
f3ecfb7224c7233fe7bb5f59f96de52f.pem",
    "SubscribeURL": "https://sns.us-west-2.amazonaws.com/?
Action=ConfirmSubscription&TopicArn=arn:aws:sns:us-
west-2:123456789012:MyTopic&Token=2336412f37...",
    "MessageAttributes": {
        "major_version": {
            "Type": "String",
            "Value": "v1"
        },
        "managed_rule_group": {
            "Type": "String",
            "Value": "AWSManagedRulesCommonRuleSet"
        }
```

```
    }
}
```

관리형 규칙의 표준 배포 개요 AWS

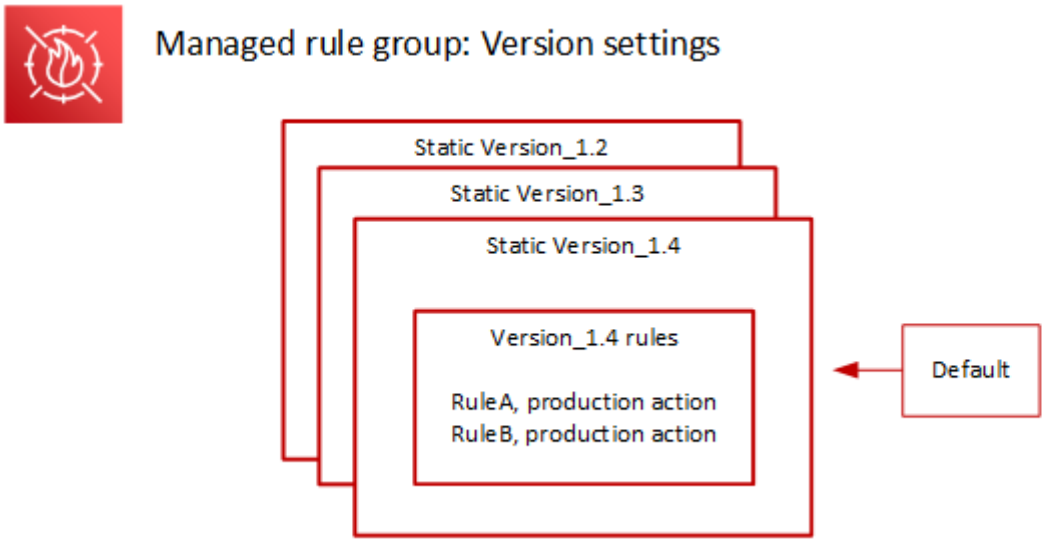
AWS 릴리스 후보, 정적 버전, 기본 버전의 세 가지 표준 배포 단계를 사용하여 새로운 AWS 관리형 규칙 기능을 출시합니다.

다음 다이어그램은 이러한 표준 배포를 보여줍니다. 다음 섹션에서는 각각에 대해 자세히 설명합니다.



AWS 관리형 규칙의 일반적인 버전 상태

일반적으로 버전이 지정된 관리형 규칙 그룹에는 만료되지 않은 정적 버전이 여러 개 있으며, 기본 버전은 권장되는 정적 버전을 가리킵니다. AWS 다음 그림은 일반적인 정적 버전 및 기본 설정 집합의 예를 보여줍니다.



정적 버전에서 대부분의 규칙에 대한 프로덕션 작업은 Block이지만 다른 것으로 설정될 수도 있습니다. 규칙 작업 설정에 대한 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록에서 각 규칙 그룹의 규칙 목록을 참조하세요.

관리형 규칙의 출시 후보 AWS 배포

관리형 규칙 그룹에 대한 규칙 변경 후보 세트가 있는 경우 임시 릴리스 후보 배포에서 해당 규칙을 테스트합니다. AWS AWS 카운트 모드의 후보 규칙을 프로덕션 트래픽과 비교하여 평가하고 오탐 완화를 포함한 최종 조정 작업을 수행합니다. AWS 테스트에서는 규칙 그룹의 기본 버전을 사용하는 모든 고객을 대상으로 이 방식으로 후보 규칙을 릴리스합니다. 릴리스 후보 배포는 규칙 그룹의 정적 버전을 사용하는 고객에게는 적용되지 않습니다.

기본 버전을 사용하는 경우 릴리스 후보 배포는 규칙 그룹에서 웹 트래픽이 관리되는 방식을 변경하지 않습니다. 후보 규칙을 테스트하는 동안 다음과 같은 현상이 나타날 수 있습니다.

- 기본 버전 이름이 `Default (using Version_X.Y)`에서 `Default (using Version_X.Y_PLUS_RC_COUNT)`로 변경됩니다.
- CloudWatch Amazon의 추가 카운트 `RC_COUNT` 메트릭에는 이름이 포함되어 있습니다. 이는 릴리스 후보 규칙에 의해 생성됩니다.

AWS 출시 후보를 약 1주일 동안 테스트한 후 이를 제거하고 기본 버전을 현재 권장 정적 버전으로 재설정합니다.

AWS 릴리스 후보 배포를 위해 다음 단계를 수행합니다.

1. 릴리스 후보 생성 - 현재 권장 정적 버전 (기본값이 가리키는 버전) 을 기반으로 릴리스 후보 버전을 AWS 추가합니다.

   릴리스 후보 이름은 _PLUS_RC_COUNT가 추가된 추가된 정적 버전 이름입니다. 예를 들어 현재 권장되는 정적 버전이 Version_2.1인 경우 릴리스 후보 이름에는 Version_2.1_PLUS_RC_COUNT가 지정됩니다.

   릴리스 후보에는 다음 규칙이 포함됩니다.

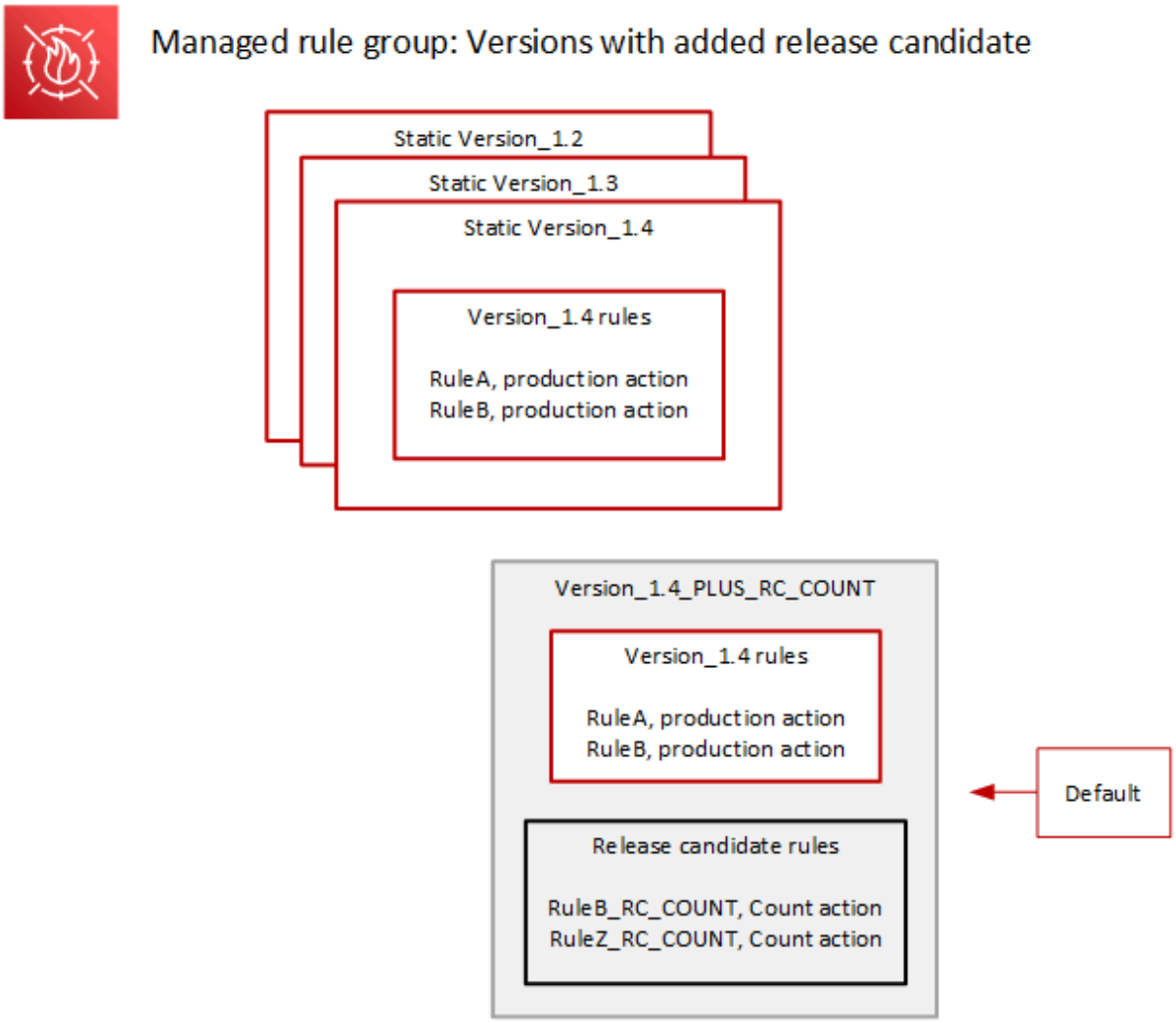
   - 규칙은 규칙 구성을 변경하지 않고 현재 권장 정적 버전에서 정확히 복사됩니다.
   - 규칙 동작이 Count로 설정되고 이름이 _RC_COUNT로 끝나는 새 규칙을 후보로 선정합니다.

     대부분의 후보 규칙은 규칙 그룹에 이미 있는 규칙에 대해 제안된 개선 사항을 제공합니다. 각 규칙의 이름은 기존 규칙 이름에 _RC_COUNT가 추가된 이름입니다.

2. 기본 버전을 릴리스 후보 버전으로 설정 및 테스트 - AWS 새 릴리스 후보를 가리키도록 기본 버전을 설정하여 프로덕션 트래픽을 대상으로 테스트를 수행합니다. 테스트에는 보통 일주일 정도 소요됩니다.

   기본 버전의 이름이 정적 버전만 나타내는 이름(예: Default (using Version_1.4))에서 정적 버전과 릴리스 후보 규칙을 나타내는 이름(예: Default (using Version_1.4_PLUS_RC_COUNT))으로 변경됩니다. 이 이름 지정 체계를 통해 웹 트래픽을 관리하는 데 사용 중인 정적 버전을 식별할 수 있습니다.

   다음 다이어그램은 이 시점의 예제 규칙 그룹 버전 상태를 보여줍니다.



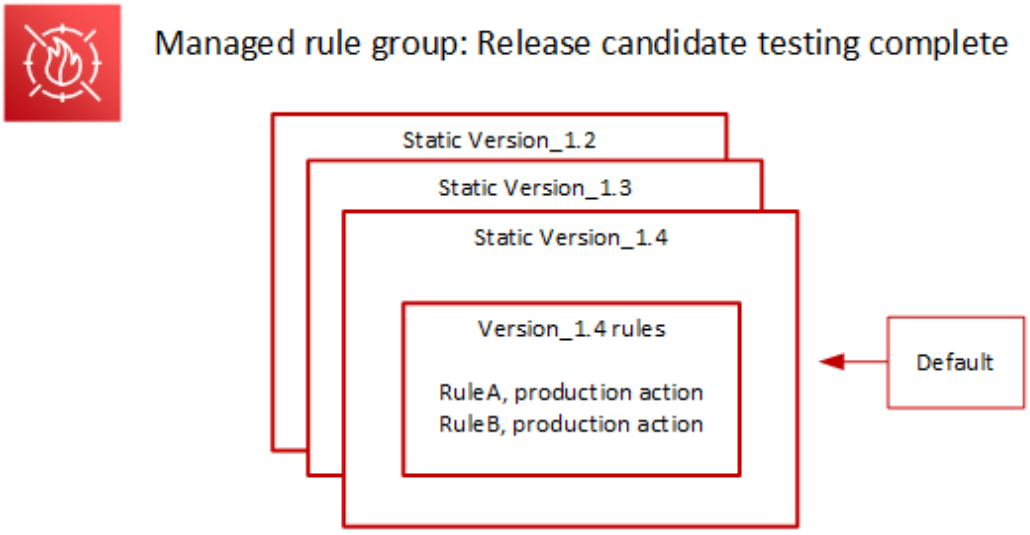
릴리스 후보 규칙은 항상 Count 작업으로 구성되므로 규칙 그룹에서 웹 트래픽을 관리하는 방식이 변경되지 않습니다.

출시 후보 규칙은 행동을 확인하고 오탐을 식별하는 데 AWS 사용하는 Amazon CloudWatch 개수 지표를 생성합니다. AWS 릴리스 후보 개수 규칙의 동작을 조정하기 위해 필요에 따라 조정합니다.

릴리스 후보 버전은 정적 버전이 아니므로 정적 규칙 그룹 버전 목록에서 선택할 수 없습니다. 기본 버전 사양에서는 릴리스 후보 버전의 이름만 볼 수 있습니다.

3. 기본 버전을 권장 정적 버전으로 되돌리기 — 릴리스 후보 규칙을 테스트한 후 기본 버전을 현재 권장 정적 버전으로 다시 AWS 설정합니다. 기본 버전 이름 설정은 _PLUS_RC_COUNT 엔딩을 삭제하고, 규칙 그룹은 릴리스 후보 규칙에 대한 CloudWatch 개수 지표 생성을 중단합니다. 이러한 변경은 자동으로 이루어지며 기본 버전 롤백 배포와는 다릅니다.

   다음 다이어그램은 릴리스 후보 테스트 완료 이후의 예제 규칙 그룹 버전의 상태를 보여줍니다.



타이밍 및 알림

AWS 필요에 따라 릴리스 후보 버전을 배포하여 규칙 그룹의 개선 사항을 테스트합니다.

- SNS — AWS 배포 시작 시 SNS 알림을 보냅니다. 알림에는 릴리스 후보를 테스트할 예상 시간이 표시됩니다. 테스트가 완료되면 두 번째 알림 없이 AWS 자동으로 기본값을 정적 버전 설정으로 되돌립니다.
- 변경 로그 - 이 유형의 배포에 대한 변경 로그나 이 가이드의 다른 부분은 AWS 업데이트되지 않습니다.

관리형 규칙을 위한 AWS 정적 버전 배포

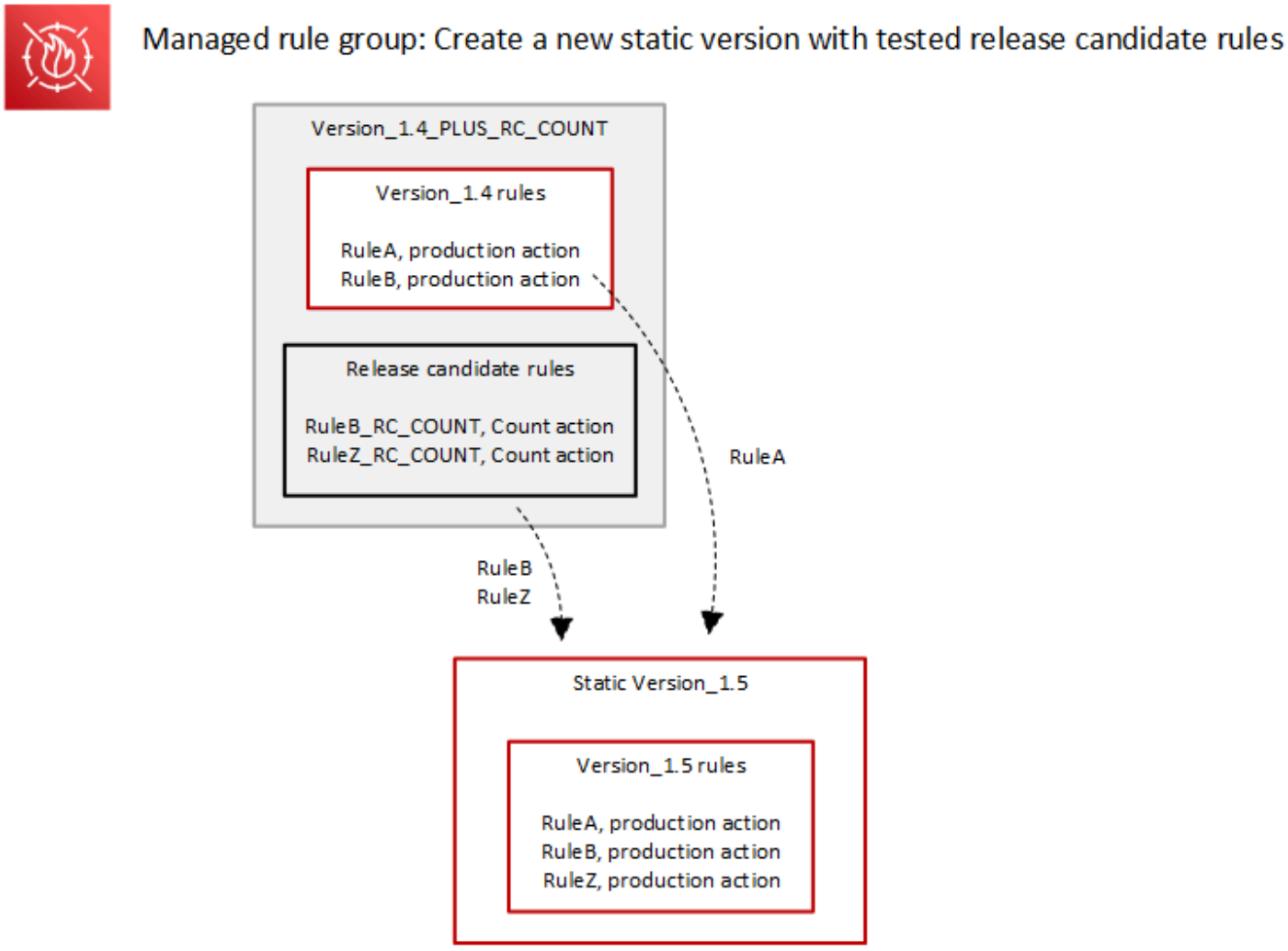
릴리스 후보가 규칙 그룹에 중요한 변경 사항을 제공한다고 AWS 판단되면 릴리스 후보를 기반으로 규칙 그룹의 새 정적 버전을 AWS 배포합니다. 이 배포는 규칙 그룹의 기본 버전을 변경하지 않습니다.

새 정적 버전에는 릴리스 후보의 다음 규칙이 포함됩니다.

- 이전 정적 버전에 포함된 규칙으로, 릴리스 후보 규칙 중에 대체 후보가 없는 규칙.
- 다음과 같이 변경된 릴리스 후보 규칙:
  - AWS 릴리스 후보 접미사를 _RC_COUNT 제거하여 규칙 이름을 변경합니다.
  - AWS 규칙 조치를 에서 해당 생산 규칙 Count 조치로 변경합니다.

  이전 기존 규칙을 대체하는 릴리스 후보 규칙의 경우 해당 규칙이 새 정적 버전의 이전 규칙 기능을 대체합니다.

다음 다이어그램은 릴리스 후보에서 새 정적 버전을 생성하는 과정을 보여줍니다.



배포 후에는 원하는 경우 새 정적 버전을 프로덕션에서 테스트 및 사용할 수 있습니다. AWS 관리형 규칙 규칙 그룹 목록의 규칙 그룹 규칙 목록에서 신규 및 업데이트된 규칙 작업 및 설명을 검토할 수 있습니다.

정적 버전은 배포 후에는 변경할 수 없으며 AWS 만료될 때만 변경됩니다. 버전 수명 주기에 대한 자세한 내용은 버전이 지정된 관리형 규칙 그룹 섹션을 참조하세요.

타이밍 및 알림

AWS 규칙 그룹 기능의 개선 사항을 배포하기 위해 필요에 따라 새 정적 버전을 배포합니다. 정적 버전의 배포는 기본 버전 설정에 영향을 주지 않습니다.

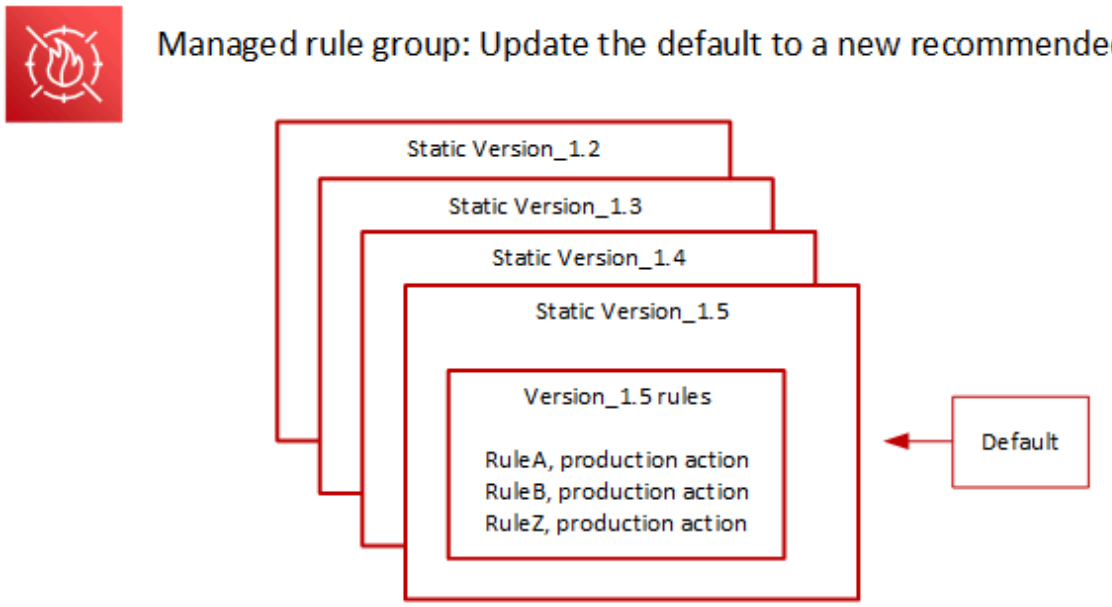
- SNS — 배포가 완료되면 SNS 알림을 AWS 보냅니다.

- 변경 로그 — 사용 가능한 모든 곳에서 AWS WAF 배포가 완료되면 필요에 따라 이 가이드의 규칙 그룹 정의를 AWS 업데이트한 다음 AWS Managed Rules 규칙 그룹 변경 로그와 설명서 기록 페이지에 릴리스를 알립니다.

관리형 규칙의 AWS 기본 버전 배포

새 정적 버전이 현재 기본 버전과 비교하여 규칙 그룹에 대한 향상된 보호 기능을 제공한다고 AWS 판단되면 기본 버전을 새 정적 버전으로 AWS 업데이트합니다. AWS 규칙 그룹의 기본 버전으로 승격하기 전에 여러 정적 버전을 릴리스할 수 있습니다.

다음 다이어그램은 기본 버전 설정을 새 정적 버전으로 AWS 이동한 후의 예제 규칙 그룹 버전 상태를 보여줍니다.



이 변경 사항을 기본 버전에 배포하기 전에 향후 변경 사항을 테스트하고 준비할 수 있도록 알림을 AWS 제공합니다. 기본 버전을 사용하는 경우 아무 작업도 수행할 필요가 없으며 업데이트될 때까지 기본 버전을 계속 사용할 수 있습니다. 대신 새 버전으로의 전환을 연기하려면 계획된 기본 버전 배포 시작 전에 기본값으로 설정된 정적 버전을 사용하도록 규칙 그룹을 명시적으로 구성할 수 있습니다.

타이밍 및 알림

AWS 규칙 그룹에 대해 현재 사용 중인 것과 다른 정적 버전을 권장하면 기본 버전을 업데이트합니다.

- SNS — 대상 배포일 최소 1주일 전에 SNS 알림을 보내고, 배포일 (배포 시작 시) 에 또 다른 SNS 알림을 AWS 보냅니다. 각 알림에는 규칙 그룹 이름, 기본 버전이 업데이트되는 정적 버전, 배포 날짜, 업데이트가 수행되는 각 AWS 지역의 예정된 배포 시기가 포함됩니다.

- 변경 로그 — 이 유형의 배포에 대한 변경 로그나 이 가이드의 다른 부분은 AWS 업데이트되지 않습니다.

AWS 관리형 규칙의 예외 배포

AWS 중요한 보안 위험을 해결하는 업데이트를 신속하게 배포하기 위해 표준 배포 단계를 우회할 수 있습니다. 예외 배포에는 모든 표준 배포 유형이 포함될 수 있으며 AWS 지역 전체에 빠르게 배포될 수 있습니다.

AWS 예외 배포에 대해 가능한 한 많은 사전 알림을 제공합니다.

타이밍 및 알림

AWS 필요한 경우에만 예외 배포를 수행합니다.

- SNS — 대상 배포일보다 최대한 앞서 SNS 알림을 보내고 배포 시작 시 또 다른 알림을 AWS 보냅니다. 각 알림에는 규칙 그룹 이름, 변경 내용, 배포 날짜가 포함됩니다.
- 변경 로그 — 정적 버전용 배포인 경우, 사용 가능한 모든 곳에서 AWS WAF 배포가 완료된 후 필요에 따라 이 가이드의 규칙 그룹 정의를 AWS 업데이트한 다음 AWS Managed Rules 규칙 그룹 변경 로그와 설명서 기록 페이지에서 릴리스를 발표합니다.

AWS 관리형 규칙의 기본 배포 롤백

특정 조건에서는 AWS 기본 버전을 이전 설정으로 롤백할 수 있습니다. 모든 AWS 지역에서 롤백하는 데 걸리는 시간은 보통 10분 미만입니다.

AWS 정적 버전에서 허용할 수 없을 정도로 높은 수준의 오탐과 같은 심각한 문제를 완화하기 위해서만 롤백을 수행합니다.

기본 버전 설정을 롤백한 후에는 문제가 있는 정적 버전의 만료와 문제를 해결하기 위한 새 정적 버전의 릴리스가 모두 앞당겨집니다. AWS

타이밍 및 알림

AWS 필요한 경우에만 기본 버전 롤백을 수행합니다.

- SNS — 롤백 시 단일 SNS 알림을 AWS 보냅니다. 알림에는 규칙 그룹 이름, 기본 버전으로 설정된 버전 및 배포 날짜가 포함됩니다. 이 배포 유형은 매우 빠르므로 알림은 리전에 대한 타이밍 정보를 제공하지 않습니다.

- 변경 로그 — 이 유형의 배포에 대한 변경 로그나 이 가이드의 다른 부분은 AWS 업데이트되지 않습니다.

AWS 관리형 규칙 고지 사항

AWS 관리형 규칙은 일반적인 웹 위협으로부터 사용자를 보호하도록 설계되었습니다. 설명서에 따라 AWS 관리형 규칙 그룹을 사용하면 애플리케이션에 또 다른 보안 계층이 추가됩니다. 하지만 AWS 관리형 규칙 규칙 그룹은 선택한 AWS 리소스에 따라 결정되는 보안 책임을 대체하기 위한 것이 아닙니다. 공동 책임 모델을 참조하여 AWS 리소스가 적절하게 보호되도록 하세요.

AWS 관리형 규칙 변경 로그

이 섹션에는 2019년 11월 릴리스 AWS WAF 이후 변경된 AWS 관리형 규칙이 나열되어 있습니다.

> **Note**
>
> 이 변경 로그는 AWS 관리형 규칙의 규칙 및 규칙 그룹에 대한 변경 사항을 보고합니다. AWS WAF
> 의 IP 평판 규칙 그룹 경우 이 변경 로그는 규칙 및 규칙 그룹의 변경 사항을 보고하고 규칙이 사용하는 IP 주소 목록의 소스에 대한 중요한 변경 사항을 보고합니다. IP 주소 목록 자체의 동적 특성 때문에 IP 주소 목록 자체에 대한 변경 사항은 보고되지 않습니다. IP 주소 목록에 대한 질문이 있는 경우 계정 관리자에게 문의하거나 AWS Support 센터에서 사례를 여십시오.

규칙 그룹 및 규칙	설명	날짜
Linux 운영 체제 관리형 규칙 그룹 모든 규칙	이 규칙 그룹의 정적 버전 2.3이 릴리스되었습니다. 이렇게 해도 기본 버전 설정은 변경되지 않습니다. 탐지 기능을 개선하기 위해 서명을 추가했습니다.	2024-06-06
AWS WAF 봇 컨트롤 규칙 그룹	봇 및 사기 규칙 그룹은 이제 버전이 지정되었습니다. 이러한 규칙 그룹을 사용 중인 경우, 이번 업데이트로 인해 웹 트래픽	2024-05-29

규칙 그룹 및 규칙	설명	날짜
AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹	처리 방식이 바뀌지는 않습니다. 이 업데이트는 현재 규칙 그룹 버전을 정적 버전 1.0으로 설정하고 이를 가리키도록 기본 버전을 설정합니다. 버전이 지정된 관리형 규칙에 대한 자세한 내용은 다음을 참조하십시오. • 버전이 지정된 관리형 규칙 그룹 • 버전이 지정된 관리형 AWS 규칙 그룹 배포 • 관리형 규칙 그룹의 새 버전 및 업데이트에 대한 알림 받기	

규칙 그룹 및 규칙	설명	날짜
POSIX 운영 체제 관리형 규칙 그룹 • UNIXShellCommandsVariables_QUERYARGUMENTS • UNIXShellCommandsVariables_QUERYSTRING • UNIXShellCommandsVariables_HEADER • UNIXShellCommandsVariables_BODY	이 규칙 그룹의 정적 버전 3.0을 릴리스했습니다. 이렇게 해도 기본 버전 설정은 변경되지 않습니다. UNIXShellCommandsVariables_QUERYARGUMENTS 제거하고 로 UNIXShellCommandsVariables_QUERYSTRING 교체했습니다. 레이블에 일치하는 규칙이 있는 경우 이 버전을 사용할 때는 레이블의 규칙과 일치하도록 변경하십시오UNIXShellCommandsVariables_QUERYSTRING . UNIXShellCommandsVariables_QUERYARGUMENTS 새 라벨은 입니다awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString . 모든 헤더에 일치하는 규칙을 UNIXShellCommandsVariables_HEADER 추가했습니다. 탐지 로직이 개선되어 관리형 규칙 그룹의 모든 규칙이 업데이트되었습니다. 에 대한 레이블의 문서화된 대소문자를 수정했습니다.	2024-05-28

규칙 그룹 및 규칙	설명	날짜
	UNIXShellCommandsVariables_BODY	
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • CrossSiteScripting*	이 규칙 그룹의 정적 버전 1.12를 릴리스했습니다. 탐지를 개선하고 오탐을 줄이기 위해 모든 사이트 간 스크립팅 규칙에 서명이 추가되었습니다.	2024-05-21
SQL 데이터베이스 관리형 규칙 그룹 • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLiExtendedPatterns_QUERYARGUMENTS	이 규칙 그룹의 정적 버전 1.2를 릴리스했습니다. 나열된 규칙에 JS_DECODE 텍스트 변환을 추가했습니다.	2024-05-14
관리형 규칙 그룹의 알려진 잘못된 입력 • JavaDeserializationRCE_BODY • JavaDeserializationRCE_QUERYSTRING • Log4JRCE_QUERYSTRING • Log4JRCE_BODY • Log4JRCE_HEADER	이 규칙 그룹의 정적 버전 1.22를 릴리스했습니다. 나열된 규칙에 JS_DECODE 텍스트 변환을 추가했습니다.	2024-05-08
POSIX 운영 체제 관리형 규칙 그룹	이 규칙 그룹의 정적 버전 2.2이 릴리스되었습니다. 두 규칙 모두에 JS_DECODE 텍스트 변환을 추가했습니다.	2024-05-08

규칙 그룹 및 규칙	설명	날짜
Windows 운영 체제 관리형 규칙 그룹 • PowerShellCommands_BODY	이 규칙 그룹의 정적 버전 2.1이 릴리스되었습니다. 탐지를 개선하기 위해 서명을 추가했습니다. PowerShellCommands_BODY	2024-05-03
Amazon IP 신뢰도 목록 관리형 규칙 그룹 • AWSManagedIPReputationList	악의적인 활동에 적극적으로 참여하는 주소의 식별을 개선하고 오탐을 줄이기 위해 IP 평판 목록의 출처를 업데이트했습니다. 이 규칙 그룹은 버전이 지정되지 않았으므로 이 업데이트에는 새 버전이 포함되지 않습니다.	2024-03-13
관리형 규칙 그룹의 알려진 잘못된 입력	이 규칙 그룹의 정적 버전 1.21이 릴리스되었습니다. 탐지를 개선하고 오탐을 줄이기 위해 서명이 추가되었습니다.	2023-12-16

규칙 그룹 및 규칙	설명	날짜
관리형 규칙 그룹의 알려진 잘못된 입력 • `ExploitablePaths_URIPATH`	이 규칙 그룹의 정적 버전 1.20이 릴리스되었습니다. Atlassian Confluence CVE-2023-22518 부적절한 권한 취약성과 일치하는 요청에 대한 탐지를 추가하도록 `ExploitablePaths_URIPATH` 규칙을 업데이트했습니다. 이 취약성은 모든 버전의 Confluence 데이터 센터 및 서버에 영향을 줍니다. 자세한 내용은NIST: National Vulnerability Database: CVE-2023-22518 Detail을 참조하십시오.	2023-12-14
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • `CrossSiteScripting*`	이 규칙 그룹의 정적 버전 1.11이 릴리스되었습니다. 탐지를 개선하고 오탐을 줄이기 위해 모든 사이트 간 스크립팅 규칙에 서명이 추가되었습니다.	2023-12-06
AWS WAF 봇 컨트롤 규칙 그룹 • 새 레이블: `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low`	규칙 그룹의 대상 보호 수준 레이블에 조정 활동 하위 레이블이 추가되었습니다. 이 레이블은 어떤 규칙과도 연결되어 있지 않습니다. 이 레이블 지정은 중간 및 높은 수준 규칙 및 레이블에 추가됩니다.	2023-12-05

규칙 그룹 및 규칙	설명	날짜
Bot Control 레이블 • Label(레이블): `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`	자동화를 지원하는 브라우저 확장 프로그램의 탐지를 나타내는 신호 레이블이 규칙 그룹에 추가되었습니다. 이 레이블은 개별 규칙에만 국한되지 않습니다.	2023-11-14
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • `EC2MetaDataSSRF_QUERYARGUMENTS`	이 규칙 그룹의 정적 버전 1.10이 릴리스되었습니다. 탐지를 개선하고 거짓 긍정을 줄이기 위해 규칙 하나를 업데이트했습니다.	2023-11-02
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_URIPATH` • `EC2MetaDataSSRF_QUERYARGUMENTS`	이 규칙 그룹의 정적 버전 1.9가 릴리스되었습니다. 감지를 개선하고 거짓 긍정을 줄이기 위해 규칙 하나를 업데이트했습니다.	2023-10-30

규칙 그룹 및 규칙	설명	날짜
POSIX 운영 체제 관리형 규칙 그룹 • UNIXShellCommandsVariables_QUERYARGUMENTS	이 규칙 그룹의 정적 버전 2.1이 릴리스되었습니다. 탐지를 개선하기 위해 쿼리 인수를 업데이트했습니다.	2023-10-12
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • GenericLFI_QUERYARGUMENTS • GenericLFI_URIPATH • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	이 규칙 그룹의 정적 버전 1.8이 릴리스되었습니다. 탐지 기능을 개선하기 위해 규칙을 업데이트했습니다.	2023-10-11

규칙 그룹 및 규칙	설명	날짜
관리형 규칙 그룹의 알려진 잘못된 입력 • `ExploitablePaths_URIPATH`	예외 배포: 이 규칙 그룹의 정적 버전 1.19이 릴리스되었습니다. 버전 1.19를 사용하도록 기본 버전을 업데이트했습니다. Atlassian Confluence CVE-2023-22515 권한 에스컬레이션 취약성과 일치하는 요청에 대한 탐지를 추가하도록 `ExploitablePaths_URIPATH` 규칙을 업데이트했습니다. 이 취약성은 Atlassian Confluence의 일부 버전에 영향을 미칩니다. 자세한 내용은NIST: National Vulnerability Database: CVE-2023-22515 Detail 및 Atlassian Support: FAQ for CVE-2023-22515를 참조하세요. 이 배포 유형에 대한 자세한 내용은 AWS 관리형 규칙의 예외 배포 섹션을 참조하세요.	2023-10-04

규칙 그룹 및 규칙	설명	날짜
관리형 규칙 그룹의 알려진 잘못된 입력 • Host_localhost_HEADER • Log4J* • JavaDeserialization*	예외 배포: 이 규칙 그룹의 정적 버전 1.18이 릴리스되었습니다. 버전 1.19의 생성 및 출시를 지원하기 위해 이 정적 버전을 서둘러 출시했습니다. 탐지 개선을 위해 Host_localhost_HEADER 규칙과 모든 Log4J 및 Java 역직렬화 규칙을 업데이트했습니다. 이 배포 유형에 대한 자세한 내용은 AWS 관리형 규칙의 예외 배포 섹션을 참조하세요.	2023-10-04
AWS WAF 봇 컨트롤 규칙 그룹 • TGT_TokenReuseIp • TGT_ML_CoordinatedActivityMedium • TGT_ML_CoordinatedActivityHigh	Count 작업을 포함하는 규칙 그룹에 규칙을 추가했습니다. 토큰 재사용 IP 규칙은 IP 주소 간에 토큰 공유를 탐지하고 계산합니다. 조정된 활동 규칙은 웹사이트 트래픽에 대한 자동화된 기계 학습(ML) 분석을 사용하여 봇 관련 활동을 탐지합니다. 규칙 그룹 구성에서 ML 사용을 옵트아웃할 수 있습니다. 이번 릴리스에서는 현재 대상 보호 수준을 사용하고 있는 고객이 ML 사용에 옵트인되어 있습니다. 옵트아웃하면 조정된 활동 규칙이 비활성화됩니다.	2023-09-06

규칙 그룹 및 규칙	설명	날짜
AWS WAF 봇 컨트롤 규칙 그룹 • CategoryAI	CategoryAI 규칙을 규칙 그룹에 추가했습니다.	2023-08-30
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • EC2MetaDataSSRF_COOKIE • EC2MetaDataSSRF_QUERYARGUMENTS • EC2MetaDataSSRF_BODY • EC2MetaDataSSRF_URIPATH	이 규칙 그룹의 정적 버전 1.7이 릴리스되었습니다. 탐지를 개선하고 거짓 긍정을 줄이기 위해 제한된 확장 및 EC2 메타데이터 SSRF 규칙을 업데이트했습니다.	2023-07-26
AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 새 규칙 그룹의 모든 규칙	AWSManagedRulesACFPRuleSet 규칙 그룹을 추가했습니다.	2023-06-13

규칙 그룹 및 규칙	설명	날짜
Linux 운영 체제 관리형 규칙 그룹 • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	이 규칙 그룹의 정적 버전 2.2이 릴리스되었습니다. 탐지 기능을 개선하기 위해 서명을 추가했습니다.	2023-05-22
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	이 규칙 그룹의 정적 버전 1.6이 릴리스되었습니다. 탐지를 개선하고 거짓 긍정을 줄이기 위해 크로스 사이트 스크립팅(XSS) 및 제한된 확장 규칙을 업데이트했습니다.	2023-04-28

규칙 그룹 및 규칙	설명	날짜
PHP 애플리케이션 관리형 규칙 그룹 • PHPHighRiskMethodsVariables_BODY 업데이트됨 • PHPHighRiskMethodsVariables_QUERYARGUMENTS 제거됨 • PHPHighRiskMethodsVariables_QUERYSTRING 추가됨 • PHPHighRiskMethodsVariables_HEADER 추가됨	이 규칙 그룹의 정적 버전 2.0이 릴리스되었습니다. 모든 규칙에서 탐지 기능을 개선하기 위해 서명을 추가했습니다. 쿼리 인수만 검사하는 대신 전체 쿼리 문자열을 검사하도록 PHPHighRiskMethodsVariables_QUERYARGUMENTS 규칙을 PHPHighRiskMethodsVariables_QUERYSTRING 규칙으로 대체했습니다. PHPHighRiskMethodsVariables_HEADER 규칙을 추가하여 모든 헤더를 포함하도록 적용 범위를 확장했습니다. 표준 관리형 규칙 라벨링에 맞게 다음 라벨을 업데이트했습니다. AWS • 이전 이름: PHPHighRiskMethodsVariables_BODY 새 이름: PHPHighRiskMethodsVariables_Body • 이전 이름: PHPHighRiskMethodsVariables_QUERYARGUMENTS 새 이름: PHPHighRi	2023-02-27

규칙 그룹 및 규칙	설명	날짜
	skMethodsVariables_QueryString	
AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 • VolumetricIpFailedLoginResponseHigh • VolumetricSessionFailedLoginResponseHigh	보호된 Amazon CloudFront 배포와 함께 사용하기 위한 로그인 응답 검사 규칙을 추가했습니다. 이러한 규칙은 최근에 너무 많은 로그인 시도 실패의 원인이 된 IP 주소 및 클라이언트 세션으로부터의 새로운 로그인 시도를 차단할 수 있습니다.	2023-02-15
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	이 규칙 그룹의 정적 버전 1.5가 릴리스되었습니다. 탐지를 개선하기 위해 크로스 사이트 스크립팅 (XSS) 필터를 업데이트했습니다.	2023-01-25

규칙 그룹 및 규칙	설명	날짜
Linux 운영 체제 관리형 규칙 그룹 • LFI_COOKIE - 제거됨 • LFI_HEADER - 추가됨 • LFI_URIPATH • LFI_QUERYSTRING	이 규칙 그룹의 정적 버전 2.1 이 릴리스되었습니다. LFI_COOKIE 규칙 및 관련 awswaf:managed:aws:linux-os:LFI_Cookie 레이블을 제거하고 새 규칙 LFI_HEADER 및 관련 레이블 awswaf:managed:aws:linux-os:LFI_Header 로 교체했습니다. 이 변경으로 검사 범위가 여러 헤더로 확대되었습니다. 탐지를 개선하기 위해 모든 규칙에 텍스트 변환 및 서명을 추가했습니다.	2022-12-15
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	이 규칙 그룹의 정적 버전 1.4 가 릴리스되었습니다. 모든 null 바이트를 NoUserAgent_HEADER 제거하기 위한 텍스트 변환을 추가했습니다. 탐지를 개선하기 위해 크로스 사이트 스크립팅(XSS) 규칙의 필터를 업데이트했습니다.	2022-12-05

규칙 그룹 및 규칙	설명	날짜
관리형 규칙 그룹의 알려진 잘못된 입력 • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER	이 규칙 그룹의 정적 버전 1.17이 릴리스되었습니다. Java 역직렬화 규칙을 업데이트하여 1.10.0 이전 버전의 Apache Commons Text 버전에서 원격 코드 실행(RCE) 취약점인 Apache CVE-2022-42889 매칭 요청에 대한 탐지를 추가했습니다. 자세한 내용은 NIST: National Vulnerability Database: CVE-2022-42889 Detail 및 CVE-2022-42889: Apache Commons Text prior to 1.10.0 allows RCE when applied to untrusted input due to insecure interpolation defaults를 참조하세요. Host_localhost_HEADER 의 탐지 기능이 개선되었습니다.	2022-10-20
관리형 규칙 그룹의 알려진 잘못된 입력 • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY	이 규칙 그룹의 정적 버전 1.16이 릴리스되었습니다. 버전 1.15에서 AWS 식별된 오탐이 제거되었습니다.	2022-10-05

규칙 그룹 및 규칙	설명	날짜
POSIX 운영 체제 관리형 규칙 그룹 PHP 애플리케이션 관리형 규칙 그룹 WordPress 애플리케이션 관리형 규칙 그룹	문서화된 레이블 이름을 수정했습니다.	2022-09-19
IP 평판 규칙 그룹 • `AWSManagedIPDDoSList`	이 변경으로 규칙 그룹의 웹 트래픽 처리 방식은 변경되지 않습니다. Amazon 위협 인텔리전스에 따라 DDoS 활동에 적극적으로 관여하는 IP 주소를 검사하는 Count 작업을 포함하는 새 규칙을 추가했습니다.	2022-08-30

규칙 그룹 및 규칙	설명	날짜
관리형 규칙 그룹의 알려진 잘못된 입력 • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	이 규칙 그룹의 정적 버전 1.15가 릴리스되었습니다. 거짓 긍정을 보다 세밀하게 모니터링하고 관리할 수 있도록 Log4JRCE를 제거하고 Log4JRCE_HEADER Log4JRCE_QUERYSTRING Log4JRCE_URI 및 Log4JRCE_BODY 로 대체했습니다. 모든 JavaDeserializationRCE* 및 Log4JRCE* 규칙에 대한 탐지 및 차단을 개선하기 위해 PROPFIND_METHOD 서명을 추가했습니다. Host_localhost_HEADER 과 모든 JavaDeserializationRCE* 규칙의 대소문자를 수정하도록 레이블을 업데이트했습니다. JavaDeserializationRCE_HEADER 의 설명을 수정했습니다.	2022-08-22

규칙 그룹 및 규칙	설명	날짜
AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 • UnsupportedCognitoIDP	Amazon Cognito 사용자 풀 웹 트래픽에 대해 계정 탈취 방지 관리형 규칙 그룹의 사용을 방지하는 규칙을 추가했습니다.	2022-08-11
핵심 규칙 세트(CRS) 관리형 규칙 그룹	AWS 버전 Version_1.2 및 규칙 그룹의 만료일이 예정되어 있습니다Version_2.0 . 이들 버전은 2022년 9월 9일에 만료됩니다. 버전 만료에 대한 자세한 내용은 버전이 지정된 관리형 규칙 그룹 섹션을 참조하세요.	2022-06-09
핵심 규칙 세트(CRS) 관리형 규칙 그룹 • GenericLFI_URIPATH GenericRFI_URIPATH	이 규칙 그룹의 정적 버전 1.3 이 릴리스되었습니다. 이번 릴리스에서는 탐지를 개선하기 위해 GenericLFI_URIPATH 및 GenericRFI_URIPATH 규칙의 일치 서명을 업데이트합니다.	2022-05-24
AWS WAF 봇 컨트롤 규칙 그룹 • CategoryEmailClient	CategoryEmailClient 규칙을 규칙 그룹에 추가했습니다.	2022-04-06

규칙 그룹 및 규칙	설명	날짜
관리형 규칙 그룹의 알려진 잘못된 입력 • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	이 규칙 그룹의 정적 버전 1.14가 릴리스되었습니다. 네 가지 JavaDeserializtion RCE 규칙이 Block 모드로 전환됩니다.	2022-03-31
관리형 규칙 그룹의 알려진 잘못된 입력 • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	이 규칙 그룹의 정적 버전 1.13이 릴리스되었습니다. Spring Core and Cloud Function RCE 취약성에 대한 텍스트 변환을 업데이트했습니다. 이러한 규칙은 계수 모드에서 지표를 수집하고 일치하는 패턴을 평가하는 데 사용됩니다. 이 레이블을 사용하여 사용자 지정 규칙의 요청을 차단할 수 있습니다. 이들 규칙이 차단 모드에서 사용되는 후속 버전을 배포할 예정입니다.	2022-03-31

규칙 그룹 및 규칙	설명	날짜
관리형 규칙 그룹의 알려진 잘못된 입력 • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	이 규칙 그룹의 정적 버전 1.12가 릴리스되었습니다. Spring Core and Cloud Function RCE 취약성에 대한 서명을 추가했습니다. 이러한 규칙은 계수 모드에서 지표를 수집하고 일치하는 패턴을 평가하는 데 사용됩니다. 이 레이블을 사용하여 사용자 지정 규칙의 요청을 차단할 수 있습니다. 이들 규칙이 차단 모드에서 사용되는 후속 버전을 배포할 예정입니다. Log4JRCE_HEADER , Log4JRCE_QUERYSTRING , Log4JRCE_URI 및 Log4JRCE_BODY 규칙을 제거하고 Log4JRCE 규칙으로 대체했습니다.	2022-03-30
IP 평판 규칙 그룹 • AWSManagedReconnaissanceList	AWSManagedReconnaissanceList 규칙을 업데이트하여 계산에서 차단으로 작업을 변경했습니다.	2022-02-15

규칙 그룹 및 규칙	설명	날짜
AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 새 규칙 그룹의 모든 규칙	규칙 그룹을 추가했습니다AWSManagedRulesATPRuleSet .	2022-02-11
관리형 규칙 그룹의 알려진 잘못된 입력 • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY	이 규칙 그룹의 정적 버전 1.9가 릴리스되었습니다. 이 기능을 유연하게 사용할 수 있도록 Log4JRCE 규칙을 제거하고 Log4JRCE_HEADER , Log4JRCE_QUERYSTRING , Log4JRCE_URI 및 Log4JRCE_BODY 규칙으로 대체했습니다. 탐지 및 차단을 개선하기 위해 서명을 추가했습니다.	2022-01-28
핵심 규칙 집합(CRS, Core rule set) • CrossSiteScripting_URIPATH • CrossSiteScripting_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_COOKIE	이 규칙 그룹의 정적 버전 2.0이 릴리스되었습니다. 이러한 규칙의 경우 탐지 서명을 조정하여 거짓 긍정을 줄였습니다. URL_DECODE 텍스트 변환을 이중 URL_DECODE_UNI 텍스트 변환으로 대체했습니다. HTML_ENTITY_DECODE 텍스트 변환을 추가했습니다.	2022-01-10

규칙 그룹 및 규칙	설명	날짜
핵심 규칙 집합(CRS, Core rule set) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS	이 규칙 그룹의 버전 2.0 릴리스의 일환으로 URL_DECODE_UNI 텍스트 변환을 추가했습니다. RestrictedExtensions_URIPATH 에서 URL_DECODE 텍스트 변환을 제거했습니다.	2022-01-10
SQL 데이터베이스 • SQLi_BODY • SQLi_QUERYARGUMENTS • SQLi_COOKIE • SQLi_URIPATH • SQLiExtendedPatterns_BODY • SQLiExtendedPatterns_QUERYARGUMENTS	이 규칙 그룹의 정적 버전 2.0이 릴리스되었습니다. URL_DECODE 텍스트 변환을 이중 URL_DECODE_UNI 텍스트 변환으로 대체했고, COMPRESS_WHITE_SPACE 텍스트 변환을 추가했습니다. SQLiExtendedPatterns_QUERYARGUMENTS 에 더 많은 탐지 서명을 추가했습니다. SQLi_BODY 에 JSON 검사를 추가했습니다. SQLiExtendedPatterns_BODY 규칙을 추가했습니다. SQLi_URIPATH 규칙을 삭제했습니다.	2022-01-10
알려진 잘못된 입력 • Log4JRCE	헤더 검사 및 일치 기준이 개선된 Log4JRCE 규칙의 1.8 버전이 릴리스되었습니다.	2021-12-17

규칙 그룹 및 규칙	설명	날짜
알려진 잘못된 입력 • Log4JRCE	일치 기준이 조정되고 추가 헤더를 검사하는 Log4JRCE 규칙의 1.4 버전이 릴리스되었습니다. 일치 기준이 조정된 버전 1.5 버전이 릴리스되었습니다.	2021-12-11
알려진 잘못된 입력 • Log4JRCE • BadAuthToken_COOKIE_AUTHORIZATION	Log4j 내에서 최근에 공개된 보안 문제에 대한 대응으로 Log4JRCE 규칙 버전 1.2를 추가했습니다. 자세한 내용은 CVE-2021-44228을 참조하세요. 이 규칙은 공통 URI 경로, 쿼리 문자열, 요청 본문의 처음 8KB 및 공통 헤더를 검사합니다. 이 규칙은 이중 URL_DECODE_UNI 텍스트 변환을 사용합니다. 일치 기준이 조정되고 추가 헤더를 검사하는 Log4JRCE의 1.3 버전이 릴리스되었습니다. BadAuthToken_COOKIE_AUTHORIZATION 규칙을 삭제했습니다.	2021-12-10

다음 표는 2021년 12월 이전의 변경 사항이 나열되어 있습니다.

규칙 그룹 및 규칙	설명	날짜	
Amazon IP 평판 목록	AWSManageDReconnaissanceList	모니터링/계산 모드에 AWSManageDReconnaissanceList 규칙을 추가했습니다. 이	2021-11-23

규칙 그룹 및 규칙	설명	날짜	
		규칙에는 리소스에 대한 정찰을 수행하는 IP 주소가 포함됩니다. AWS	

규칙 그룹 및 규칙	설명	날짜	
Windows 운영 체제	WindowsShellCommands PowerShellCommands	WindowsShell 명령에 대한 세 가지 새 규칙 (WindowsShellCommands_COOKIE , WindowsShellCommands_QUERYARGUMENTS 및) 이 추가되었습니다. WindowsShellCommands_BODY 새 PowerShell 규칙 추가:PowerShellCommands_COOKIE . _Set1 및 _Set2 문자열을 제거하여 PowerShellComands 규칙 이름 지정을 재구성했습니다. PowerShellRules 에 보다 포괄적인 탐지 서명을 추가했습니다. 모든 Windows 운영 체제 규칙에 URL_DECODE_UNI 텍스트 변환을 추가했습니다.	2021-11-23	

규칙 그룹 및 규칙	설명	날짜	
Linux 운영 체제	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	이중 URL_DECODE 텍스트 변환을 이중 URL_DECODE_UNI 로 대체했습니다. 두 번째 텍스트 변환으로 NORMALIZE_PATH_WIN 을 추가했습니다. LFI_BODY 규칙을 LFI_COOKIE 규칙으로 대체했습니다. 모든 LFI 규칙에 대해 보다 포괄적인 감지 서명을 추가했습니다.	2021-11-23
핵심 규칙 집합(CRS, Core rule set)	SizeRestrictions_BODY	본문 페이로드가 8KB보다 큰 웹 요청을 차단하도록 크기 제한을 낮췄습니다. 이전에는 제한이 10KB였습니다.	2021-10-27

규칙 그룹 및 규칙	설명	날짜	

핵심 규칙 집합(CRS, Core rule set)	`EC2MetaDataSSRF_BODY`
	
	`EC2MetaDataSSRF_COOKIE`
	
	`EC2MetaDataSSRF_URIPATH`
	
	`EC2MetaDataSSRF_QUERYARGUMENTS`
		더 많은 탐지 서명을 추가했습니다. 차단을 개선하기 위해 이중 유니코드 URL 디코딩을 추가했습니다.	2021-10-27

핵심 규칙 집합(CRS, Core rule set)	`GenericLFI_QUERYARGUMENTS`
	
	`GenericLFI_URIPATH`
	
	`RestrictedExtensions_URIPATH`
	
	`RestrictedExtensions_QUERYARGUMENTS`
		차단을 개선하기 위해 이중 유니코드 URL 디코딩을 추가했습니다.	2021-10-27

핵심 규칙 집합(CRS, Core rule set)	`GenericRFI_QUERYARGUMENTS`
	
	`GenericRFI_BODY`
	
	`GenericRFI_URIPATH`
		고객 피드백을 기반으로 거짓 긍정을 줄이기 위해 규칙 서명을 업데이트했습니다. 차단을 개선하기 위해 이중 유니코드 URL 디코딩을 추가했습니다.	2021-10-27

규칙 그룹 및 규칙	설명	날짜	
모두	모든 규칙	AWS WAF 레이블 지정을 아직 지원하지 않는 모든 규칙에 레이블 지원이 추가되었습니다.	2021-10-25
Amazon IP 평판 목록	`AWSManagedIPReputationList_xxxx`	IP 평판 목록을 재구성하고, 규칙 이름에서 접미사를 제거하고, 레이블 지원을 추가했습니다. AWS WAF	2021-05-04

익명 IP 목록	`AnonymousIPList`
	
	`HostingProviderList`
		라벨에 대한 지원이 추가되었습니다. AWS WAF	2021-05-04

Bot Control	모두	Bot Control 규칙 세트를 추가했습니다.	2021-04-01
핵심 규칙 집합(CRS, Core rule set)	`GenericRFI_QUERYARGUMENTS`	이중 URL 디코딩을 추가했습니다.	2021-03-03
핵심 규칙 집합(CRS, Core rule set)	`RestrictedExtensions_URIPATH`	규칙 구성을 개선하고 추가 URL 디코딩을 추가했습니다.	2021-03-03
관리 보호	`AdminProtection_URIPATH`	이중 URL 디코딩을 추가했습니다.	2021-03-03
알려진 잘못된 입력	`ExploitablePaths_URIPATH`	규칙 구성을 개선하고 추가 URL 디코딩을 추가했습니다.	2021-03-03

규칙 그룹 및 규칙	설명	날짜	
Linux 운영 체제	`LFI_QUERYARGUMENTS`	규칙 구성을 개선하고 추가 URL 디코딩을 추가했습니다.	2021-03-03
Windows 운영 체제	모두	규칙 구성을 개선했습니다.	2020-09-23

PHP 애플리케이션	`PHPHighRiskMethodsVariables_QUERYARGUMENTS`
	
	`PHPHighRiskMethodsVariables_BODY`
		차단을 개선하기 위해 텍스트 변환을 HTML 디코딩에서 URL 디코딩으로 변경했습니다.	2020-09-16

POSIX 운영 체제	`UNIXShellCommandsVariables_QUERYARGUMENTS`
	
	`UNIXShellCommandsVariables_BODY`
		차단을 개선하기 위해 텍스트 변환을 HTML 디코딩에서 URL 디코딩으로 변경했습니다.	2020-09-16

핵심 규칙 집합	`GenericLFI_QUERYARGUMENTS`
	
	`GenericLFI_URIPATH`
	
	GenericLFI_BODY
		차단을 개선하기 위해 텍스트 변환을 HTML 디코딩에서 URL 디코딩으로 변경했습니다.	2020-08-07

규칙 그룹 및 규칙	설명	날짜	

Linux 운영 체제	`LFI_URIPATH`
	
	`LFI_QUERY ARGUMENTS`
	
	`LFI_BODY`
		검색 및 차단을 개선하기 위해 텍스트 변환을 HTML 엔터티 디코딩에서 URL 디코딩으로 변경했습니다.	2020-05-19

익명 IP 목록	모두	최종 사용자 ID 난독화를 허용하는 서비스의 요청을 차단하는 새 규칙 그룹을 IP 평판 규칙 그룹에서 사용하면 봇을 완화하고 지리적 제한을 피할 수 있습니다.	2020-03-06
WordPress 애플리케이션	`WordPress Exploitable Commands_QUERYSTRING`	쿼리 문자열에서 악용 가능한 명령을 확인하는 새 규칙입니다.	2020-03-03

핵심 규칙 집합(CRS, Core rule set)	`SizeRestrictions_QUERYSTRING`
	
	`SizeRestrictions_Cookie_HEADER`
	
	`SizeRestrictions_BODY`
	
	`SizeRestrictions_URIPATH`
		정확도를 높이기 위해 크기 값 제약 조건을 조정했습니다.	2020-03-03

규칙 그룹 및 규칙	설명	날짜	
SQL 데이터베이스	`SQLi_URIPATH`	이제 규칙은 메시지 URI를 확인합니다.	2020-01-23

SQL 데이터베이스	`SQLi_BODY`
	
	`SQLi_QUERYARGUMENTS`
	
	`SQLi_COOKIE`
		텍스트 변환을 업데이트했습니다.	2019-12-20

핵심 규칙 집합(CRS, Core rule set)	`CrossSiteScripting_URIPATH`
	
	`CrossSiteScripting_BODY`
	
	`CrossSiteScripting_QUERYARGUMENTS`
	
	`CrossSiteScripting_COOKIE`
		텍스트 변환을 업데이트했습니다.	2019-12-20

AWS Marketplace 관리형 규칙 그룹

AWS Marketplace 관리형 규칙 그룹은 AWS Marketplace 콘솔을 통해 구독하여 사용할 수 AWS Marketplace있습니다. AWS Marketplace 관리형 규칙 그룹을 구독한 후에는 에서 사용할 수 있습니다 AWS WAF. AWS Firewall Manager AWS WAF 정책에서 AWS Marketplace 규칙 그룹을 사용하려면 조직의 각 계정이 규칙 그룹에 가입해야 합니다.

보호 기능을 프로덕션 트래픽에 사용하기 전에 AWS WAF 보호 기능의 변경 사항을 테스트하고 조정하세요. 자세한 내용은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

AWS Marketplace 규칙 그룹 가격 책정

AWS Marketplace 규칙 그룹은 장기 계약 및 최소 약정 없이 사용할 수 있습니다. 규칙 그룹을 구독하면 월간 요금(시간별 비례 할당으로 계산됨) 및 볼륨을 기반으로 한 지속적인 요청 요금이 부과됩니다. 자세한 내용은 에서 각 AWS Marketplace 규칙 그룹의 AWS WAF 가격 및 설명을 참조하십시오. AWS Marketplace

AWS Marketplace 규칙 그룹에 대해 궁금한 점이 있나요?

AWS Marketplace 셀러가 관리하는 규칙 그룹에 대한 질문이 있거나 기능 변경을 요청하려면 공급자의 고객 지원 팀에 문의하세요. 연락처 정보를 찾으려면 AWS Marketplace의 공급자 목록을 참조하세요.

AWS Marketplace 규칙 그룹 공급자는 규칙 그룹 관리 방법 (예: 규칙 그룹 업데이트 방법, 규칙 그룹 버전 관리 여부) 을 결정합니다. 또한 공급자는 규칙, 규칙 작업 그리고 규칙이 일치하는 웹 요청에 추가하는 모든 레이블을 포함하여 규칙 그룹의 세부 정보를 결정합니다.

관리형 규칙 그룹 구독 AWS Marketplace

콘솔에서 AWS Marketplace 규칙 그룹을 구독하거나 구독을 취소할 수 있습니다. AWS WAF

> **Important**
>
> AWS Firewall Manager 정책에서 AWS Marketplace 규칙 그룹을 사용하려면 조직의 각 계정이 먼저 해당 규칙 그룹에 가입해야 합니다.

AWS Marketplace 관리형 규칙 그룹에 가입하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 AWS Marketplace를 선택합니다.
3. [Available marketplace products] 섹션에서 규칙 그룹의 이름을 선택하여 세부 정보 및 요금 정보를 봅니다.
4. 규칙 그룹을 구독하려면 [Continue]를 선택합니다.

   > **Note**
   >
   > 이 규칙 그룹을 구독하지 않으려면 브라우저에서 이 페이지를 닫으면 됩니다.

5. [Set up your account]를 선택합니다.

6. 개별 규칙을 추가하는 방법과 비슷한 방법으로 웹 ACL에 규칙 그룹을 추가합니다. 자세한 내용은 웹 ACL 생성 또는 웹 ACL 편집을 참조하세요.

> **Note**
>
> 웹 ACL에 규칙 그룹을 추가할 때 규칙 그룹에 있는 규칙의 작업 및 규칙 그룹 결과의 규칙 작업을 재정의할 수 있습니다. 자세한 정보는 규칙 그룹의 작업 재정의 옵션을 참조하세요.

규칙 그룹에 가입하면 다른 관리형 AWS Marketplace 규칙 그룹과 마찬가지로 웹 ACL에서 해당 규칙 그룹을 사용할 수 있습니다. 자세한 내용은 웹 ACL 생성을 참조하세요.

관리형 규칙 그룹 구독 취소 AWS Marketplace

콘솔에서 AWS Marketplace 규칙 그룹 구독을 취소할 수 있습니다. AWS WAF

> **Important**
>
> AWS Marketplace 관리형 규칙 그룹에 대한 구독 요금을 중지하려면 구독을 취소하는 것 외에도 Firewall Manager AWS WAF 정책에 있는 모든 웹 ACL에서 AWS WAF 해당 그룹을 제거해야 합니다. AWS Marketplace 관리형 규칙 그룹에서 구독을 취소하고 웹 ACL에서 제거하지 않으면 구독 요금이 계속 청구됩니다.

관리형 규칙 그룹에서 구독을 취소하려면 AWS Marketplace

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 모든 웹 ACL에서 규칙 그룹을 제거합니다. 자세한 정보는 웹 ACL 편집을 참조하세요.
3. 탐색 창에서 AWS Marketplace를 선택합니다.
4. [Manage your subscriptions]를 선택합니다.
5. 구독을 취소할 규칙 그룹의 이름 옆에 있는 [Cancel subscription]을 선택합니다.
6. 예, 구독 취소를 선택합니다.

AWS Marketplace 규칙 그룹 문제 해결

AWS Marketplace 규칙 그룹이 합법적인 트래픽을 차단하고 있는 경우 다음 단계를 수행하여 문제를 해결할 수 있습니다.

AWS Marketplace 규칙 그룹의 문제를 해결하려면

1. 합법적인 트래픽을 차단하는 규칙 수로 작업을 재정의합니다. AWS WAF 샘플링된 요청이나 로그를 사용하여 특정 요청을 차단하는 규칙을 식별할 수 있습니다. AWS WAF 로그의 `ruleGroupId` 필드 또는 샘플링된 요청의 `RuleWithinRuleGroup`를 확인하여 규칙을 식별할 수 있습니다. 패턴 `<Seller Name>#<RuleGroup Name>#<Rule Name>`에서 규칙을 식별할 수 있습니다.
2. 특정 규칙을 요청 수만 계산하도록 설정해도 문제가 해결되지 않는 경우 모든 규칙 동작을 재정의하거나 AWS Marketplace 규칙 그룹 자체에 대한 작업을 재정의 없음에서 재정의 개수로 변경할 수 있습니다. 그러면 규칙 그룹 내의 개별 규칙 작업에 관계없이 웹 요청이 통과할 수 있습니다.
3. 개별 규칙 조치 또는 전체 규칙 그룹 작업을 재정의한 후에는 AWS Marketplace 규칙 그룹 공급자의 고객 지원 팀에 문의하여 문제를 추가로 해결하십시오. 연락처 정보는 AWS Marketplace의 제품 목록 페이지에 나열된 규칙 그룹을 참조하세요.

지원팀에 문의 AWS

문제가 AWS WAF 있거나 관리하는 AWS규칙 그룹에 대해서는 문의하세요 AWS Support. AWS Marketplace 셀러가 관리하는 규칙 그룹에 문제가 있는 경우 공급자의 고객 지원 팀에 문의하세요. 연락처 정보를 찾으려면 공급자의 목록을 참조하십시오 AWS Marketplace.

자체 규칙 그룹 관리

자체 규칙 그룹을 생성하여 관리형 규칙 그룹 옵션에서 찾을 수 없거나 직접 처리하는 것을 선호하는 규칙 모음을 다시 사용할 수 있습니다.

웹 ACL과 마찬가지로 보류 규칙을 생성하는 규칙 그룹이며, 웹 ACL에서와 같은 방법으로 규칙 그룹에 규칙을 추가합니다. 자체 규칙 그룹을 생성할 때는 변경이 불가능한 최대 용량을 설정해야 합니다.

주제

- 규칙 그룹 생성
- 규칙 그룹 편집
- 웹 ACL에서 규칙 그룹 사용
- 다른 계정과 규칙 그룹 공유

- 규칙 그룹 삭제

규칙 그룹 생성

새 규칙 그룹을 만들려면 이 페이지의 절차를 따르십시오.

규칙 그룹을 생성하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 Rule groups(규칙 그룹)와 Create rule group(규칙 그룹 생성)을 차례로 선택합니다.
3. 규칙 그룹의 이름과 설명을 입력합니다. 이름과 설명은 관리 및 사용할 규칙 그룹을 식별하는 데 사용됩니다.

   `AWS`, `Shield`, `PreFM` 또는 `PostFM`으로 시작하는 이름은 사용하면 안 됩니다. 이러한 문자열은 예약되어 있거나 다른 서비스에서 관리되는 규칙 그룹과 혼동될 수 있습니다. 다른 서비스에서 제공하는 규칙 그룹를 참조하세요.

   > **Note**
   >
   > 규칙 그룹을 생성한 후에는 이름을 변경할 수 없습니다.

4. 리전에서 규칙 그룹을 저장할 리전을 선택합니다. Amazon CloudFront 배포를 보호하는 웹 ACL의 규칙 그룹을 사용하려면 글로벌 설정을 사용해야 합니다. 리전별 애플리케이션에서도 전역 설정을 사용할 수 있습니다.
5. 다음을 선택합니다.
6. 웹 ACL 관리에서와 마찬가지로 규칙 빌더 마법사를 사용하여 규칙 그룹에 규칙을 추가합니다. 유일한 차이점은 규칙 그룹을 다른 규칙 그룹에 추가할 수 없다는 것입니다.
7. 용량에서 규칙 그룹의 웹 ACL 용량 단위(WCU) 사용에 대한 최대값을 설정합니다. 이것은 변경 불가능한 설정입니다. WCU에 대한 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

   규칙 그룹에 규칙을 추가하면 Add rules and set capacity(규칙 추가 및 용량 설정) 창에 이미 추가한 규칙에 따라 필요한 최소 용량이 표시됩니다. 규칙 그룹에서 이 계획과 향후 계획을 사용하면 규칙 그룹에 필요한 용량을 예측할 수 있습니다.
8. 규칙 그룹에 대한 설정을 검토하고 생성을 선택합니다.

규칙 그룹 편집

규칙 그룹에서 규칙을 추가 또는 제거하거나 구성 설정을 변경하려면 이 페이지의 절차를 사용하여 규칙 그룹에 액세스합니다.

> **⚠ 프로덕션 트래픽 위험**
>
> 웹 ACL에서 현재 사용 중인 규칙 그룹을 변경하는 경우 해당 변경 내용은 사용 중인 웹 ACL 동작에 영향을 미칩니다. 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 모든 변경 사항을 테스트하고 조정합니다. 그런 다음 업데이트된 규칙을 프로덕션 트래픽과 함께 계산 모드에서 테스트하고 조정한 다음 활성화하십시오. 자세한 지침은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

규칙 그룹을 편집하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 Rule groups(규칙 그룹)를 선택합니다.
3. 편집할 규칙 그룹 이름을 선택합니다. 콘솔에서 규칙 그룹 페이지로 이동합니다.
4. 필요에 따라 규칙 그룹을 편집합니다. 생성 중에 했던 것과 마찬가지로 규칙 그룹의 변경 가능한 속성을 편집할 수 있습니다. 콘솔에 편집하는 변경 내용이 저장됩니다.

> **Note**
>
> 규칙 이름을 변경하고 규칙의 지표 이름에 변경 내용이 반영되도록 하려면 지표 이름도 업데이트해야 합니다. AWS WAF 규칙 이름을 변경할 때 규칙의 지표 이름을 자동으로 업데이트하지 않습니다. 콘솔에서 규칙을 편집할 때 규칙 JSON 편집기를 사용하여 지표 이름을 변경할 수 있습니다. API와 웹 ACL 또는 규칙 그룹을 정의하는 데 사용하는 JSON 목록을 통해 두 이름을 모두 변경할 수도 있습니다.

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 생성하거나 변경할 때 리소스가 저장된 모든 영역에 변경 사항이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

웹 ACL에서 규칙 그룹 사용

웹 ACL에서 규칙 그룹을 사용하려면 규칙 그룹 참조문을 통해 해당 그룹을 웹 ACL에 추가합니다.

> **⚠ 프로덕션 트래픽 위험**
>
> 프로덕션 트래픽용 웹 ACL에 변경 사항을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 변경 사항을 테스트하고 조정하십시오. 그런 다음 업데이트된 규칙을 프로덕션 트래픽과 함께 계산 모드에서 테스트하고 조정한 다음 활성화하십시오. 자세한 지침은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

> **Note**
>
> 웹 ACL에서 1,500개가 넘는 WCU를 사용하면 기본 웹 ACL 가격을 초과하는 비용이 발생합니다. 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 및 AWS WAF 요금을 참조하세요.

콘솔을 통해 웹 ACL에서 규칙을 추가하거나 업데이트할 때 규칙 및 규칙 그룹 추가 페이지에서 규칙 추가를 선택한 다음, 자체 규칙 및 규칙 그룹 추가를 선택합니다. 그런 다음 Rule group(규칙 그룹)을 선택하고 목록에서 규칙 그룹을 선택합니다.

웹 ACL에서는 개별 규칙 작업을 Count 또는 다른 작업으로 설정하여 규칙 그룹 및 해당 규칙의 동작을 변경할 수 있습니다. 이를 통해 규칙 그룹을 테스트하고, 규칙 그룹의 규칙에서 거짓 긍정지를 식별하며 관리형 규칙 그룹이 요청을 처리하는 방식을 사용자 지정하는 등의 작업을 수행할 수 있습니다. 자세한 정보는 규칙 그룹의 작업 재정의 옵션을 참조하세요.

규칙 그룹에 속도 기반 명령문이 포함된 경우 규칙 그룹을 사용하는 각 웹 ACL에는 규칙 그룹을 사용하는 다른 웹 ACL과는 별개로 속도 기반 규칙에 대한 별도의 고유한 속도 추적 및 관리 기능이 있습니다. 자세한 정보는 비율 기반 규칙 문을 참조하세요.

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 만들거나 변경할 때 리소스가 저장된 모든 영역에 변경 내용이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

다른 계정과 규칙 그룹 공유

규칙 그룹을 다른 계정과 공유하여 해당 계정에서 사용할 수 있습니다. 하나 이상의 특정 계정과 공유할 수 있으며 조직의 모든 계정과 공유할 수 있습니다.

이렇게 하려면 AWS WAF API를 사용하여 원하는 규칙 그룹 공유를 위한 정책을 생성해야 합니다. 자세한 내용은 AWS WAF API PutPermissionPolicy참조를 참조하십시오.

규칙 그룹 삭제

규칙 그룹을 삭제하려면 이 단원의 지침을 따르십시오.

참조된 세트 및 규칙 그룹 삭제

IP 세트, 정규식 패턴 세트 또는 규칙 그룹과 같이 웹 ACL에서 사용할 수 있는 엔티티를 삭제하면 해당 엔티티가 현재 웹 ACL에서 사용되고 AWS WAF 있는지 확인합니다. 사용 중인 것으로 확인되면 경고를 표시합니다. AWS WAF AWS WAF 웹 ACL에서 엔티티를 참조하고 있는지 여부를 거의 항상 확인할 수 있습니다. 그러나 드물지만 이러한 작업을 수행할 수 없는 경우도 있습니다. 현재 아무 것도 엔티티를 사용하고 있지 않음을 확인해야 하는 경우에는 해당 엔티티를 삭제하기 전에 해당 웹 ACL에서 확

인하십시오. 엔티티가 참조된 세트인 경우에도 어떤 규칙 그룹도 해당 엔티티를 사용하고 있지 않음을 확인합니다.

규칙 그룹을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 Rule groups(규칙 그룹)를 선택합니다.
3. 삭제하려는 규칙 그룹을 선택한 다음 삭제를 선택합니다.

다른 서비스에서 제공하는 규칙 그룹

사용자 또는 조직의 관리자가 를 AWS Firewall Manager 사용하거나 AWS Shield Advanced 를 사용하여 AWS WAF리소스 보호를 관리하는 경우 계정의 웹 ACL에 추가된 규칙 그룹 참조 설명을 볼 수 있습니다.

이러한 규칙 그룹의 이름이 다음 문자열로 시작합니다.

- **`ShieldMitigationRuleGroup`**— 이러한 규칙 그룹은 보호된 AWS Shield Advanced 응용 프로그램 계층 (계층 7) 리소스에 대한 자동 응용 프로그램 계층 DDoS 완화를 제공하는 데 사용되며 이를 통해 관리됩니다.

  보호된 리소스에 대해 자동 애플리케이션 계층 DDoS 완화를 활성화하면 Shield Advanced에서 리소스와 연결된 웹 ACL에 이러한 규칙 그룹 중 하나를 추가합니다. Shield Advanced는 규칙 그룹 참조 문에 10,000,000의 우선 순위 설정을 할당하여 웹 ACL에서 구성한 규칙 이후에 실행되도록 합니다. 이 규칙 그룹에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화 섹션을 참조하세요.

  > **Warning**
  >
  > 웹 ACL에서 이 규칙 그룹을 수동으로 관리하려고 하지 마십시오. 특히 웹 ACL에서 `ShieldMitigationRuleGroup` 규칙 그룹 참조 설명을 수동으로 삭제하지 마십시오. 이로 인해 웹 ACL과 연결된 모든 리소스에 의도하지 않은 결과가 발생할 수 있습니다. 대신 Shield Advanced를 사용하여 웹 ACL과 연결된 리소스에 대한 자동 완화를 비활성화합니다. Shield Advanced는 자동 완화에 필요하지 않은 경우 규칙 그룹을 자동으로 제거합니다.

- **`PREFMManaged`**및 **`POSTFMManaged`** — 이러한 규칙 그룹은 에서 관리합니다. AWS Firewall Manager방화벽 관리자는 방화벽 관리자가 생성하고 관리하는 웹 ACL 내에서 이러한 정보를 제공합

니다. 웹 ACL의 이름은 FMManagedWebACLV2로 시작합니다. 이 웹 ACL 및 규칙 그룹에 대한 자세한 내용은 AWS WAF 정책 섹션을 참조하세요.

AWS WAF 규칙

AWS WAF 규칙은 HTTP (S) 웹 요청을 검사하는 방법과 검사 기준과 일치하는 요청에 대해 취할 조치를 정의합니다. 웹 ACL 또는 규칙 그룹의 컨텍스트에 있는 규칙만 정의합니다.

규칙은 그 자체로는 존재하지 않습니다. AWS WAF AWS 리소스가 아니며 Amazon 리소스 이름 (ARN) 도 없습니다. 규칙 그룹 또는 규칙이 정의된 웹 ACL에서 이름으로 규칙에 액세스할 수 있습니다. 규칙 그룹 또는 규칙이 포함된 웹 ACL의 JSON 보기를 사용하여 규칙을 관리하고 다른 웹 ACL로 복사할 수 있습니다. 웹 ACL 및 규칙 그룹에 사용할 수 있는 AWS WAF 콘솔 규칙 빌더를 통해 관리할 수도 있습니다.

규칙 이름

각 규칙에는 이름이 지정해야 합니다. AWS로 시작하는 이름과 다른 서비스에서 관리하는 규칙 그룹 또는 규칙에 사용되는 이름은 사용하지 마십시오. 다른 서비스에서 제공하는 규칙 그룹 섹션을 참조하십시오.

> **Note**
>
> 규칙 이름을 변경하고 규칙의 지표 이름에 변경 내용이 반영되도록 하려면 지표 이름도 업데이트해야 합니다. AWS WAF 규칙 이름을 변경할 때 규칙의 지표 이름을 자동으로 업데이트하지 않습니다. 콘솔에서 규칙을 편집할 때 규칙 JSON 편집기를 사용하여 지표 이름을 변경할 수 있습니다. API와 웹 ACL 또는 규칙 그룹을 정의하는 데 사용하는 JSON 목록을 통해 두 이름을 모두 변경할 수도 있습니다.

규칙 문

또한 각 규칙에는 규칙이 웹 요청을 검사하는 방법을 정의하는 규칙 문이 필요합니다. 규칙 문은 규칙 및 문 유형에 따라 기타 모든 깊이에 중첩된 문이 포함될 수 있습니다. 일부 규칙 문에는 일련의 기준이 적용됩니다. 예를 들어, IP 집합 일치 규칙에 대해 최대 10,000개의 IP 주소 또는 IP 주소 범위를 지정할 수 있습니다.

다음과 같이 기준을 검사하는 규칙을 정의할 수 있습니다.

- 악성일 가능성이 있는 스크립트입니다. 공격자는 웹 애플리케이션의 취약성을 악용할 수 있는 스크립트를 포함시킵니다. 이것은 XXS(교차 사이트 스크립팅)이라고 알려져 있습니다.
- 요청이 시작되는 IP 주소 또는 주소 범위입니다.
- 요청이 시작되는 국가 또는 지리적 위치입니다.
- 쿼리 문자열과 같은 요청에서 지정된 부분의 길이입니다.
- 악성일 가능성이 있는 SQL 코드입니다. 공격자는 악성 SQL 코드를 웹 요청에 포함시켜서 데이터베이스에서 데이터를 추출하려고 시도합니다. 이것은 SQL 명령어 주입이라고 알려져 있습니다.
- 요청에 나타나는 문자열입니다. 예를 들어 `User-Agent` 헤더에 나타나는 값 또는 쿼리 문자열에 나타나는 텍스트 문자열입니다. 정규식을 사용하여 이러한 문자열을 지정할 수도 있습니다.
- 웹 ACL의 이전 규칙이 요청에 추가한 레이블입니다.

위 목록에 있는 것과 같이 웹 요청 검사 기준이 있는 명령문 외에도 `AND`, `OR`, 및 에 대한 논리문을 AWS WAF 지원하여 규칙의 명령문을 `NOT` 조합하는 데 사용합니다.

예를 들어 공격자에게서 확인한 최근 요청에 따라 다음과 같은 중첩 문을 결합하는 논리적 `AND` 문을 사용하여 규칙을 생성할 수 있습니다.

- 요청이 192.0.2.44에서 나옵니다.
- 요청의 `User-Agent` 헤더에 `BadBot`라는 값이 포함되어 있습니다.
- 요청의 쿼리 문자열에 유사 SQL 코드가 포함되어 있는 것으로 보입니다.

이 경우 모든 문은 최상위 `AND` 문이 일치하도록 매치되어야 합니다.

주제

- 규칙 작업
- 규칙 문 기본 사항
- 일치 규칙 문
- 논리적 규칙 문
- 비율 기반 규칙 문
- 규칙 그룹 규칙 문

규칙 작업

규칙 동작은 규칙에 정의된 기준과 일치하는 웹 요청을 어떻게 AWS WAF 처리할지 지시합니다. 필요에 따라 각 규칙 작업에 사용자 지정 동작을 추가할 수 있습니다.

> **Note**
>
> 규칙 작업은 종료일 수도 있고 종료되지 않을 수도 있습니다. 종료 작업은 요청의 웹 ACL 평가를 중지하고 보호된 애플리케이션을 계속 실행하도록 허용하거나 차단합니다.

다음은 규칙 작업 옵션입니다.

- Allow— AWS WAF 요청을 보호된 AWS 리소스로 전달하여 처리 및 응답을 받을 수 있습니다. 이 작업은 종료 작업입니다. 정의한 규칙에서는 요청을 보호된 리소스로 전달하기 전에 사용자 지정 헤더를 요청에 삽입할 수 있습니다.
- Block— 요청을 AWS WAF 차단합니다. 이 작업은 종료 작업입니다. 기본적으로 보호된 AWS 리소스는 HTTP `403 (Forbidden)` 상태 코드로 응답합니다. 정의한 규칙에서 응답을 사용자 지정할 수 있습니다. 요청을 AWS WAF 차단하면 Block 작업 설정에 따라 보호된 리소스가 클라이언트에 다시 보내는 응답이 결정됩니다.
- Count— 요청 AWS WAF 수를 계산하지만 허용할지 차단할지는 결정하지 않습니다. 이 작업을 비종료 작업입니다. AWS WAF 는 웹 ACL의 나머지 규칙을 계속 처리합니다. 정의한 규칙에서 요청에 사용자 지정 헤더를 삽입하면 다른 규칙과 일치시킬 수 있는 레이블을 추가할 수 있습니다.
- CAPTCHA및 Challenge — CAPTCHA 퍼즐과 사일런트 챌린지를 AWS WAF 사용하여 봇이 보낸 요청이 아닌지 확인하고 토큰을 AWS WAF 사용하여 최근에 성공한 클라이언트 응답을 추적합니다.

  CAPTCHA 퍼즐과 사일런트 챌린지는 브라우저가 HTTPS 엔드포인트에 액세스할 때만 실행할 수 있습니다. 토큰을 획득하려면 브라우저 클라이언트가 안전한 환경에서 실행되고 있어야 합니다.

  > **Note**
  >
  > 규칙 중 하나에서 또는 규칙 그룹 내 규칙 작업 재정의로서 CAPTCHA 또는 Challenge 규칙 작업을 사용하는 경우 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

  이러한 규칙 작업은 요청의 토큰 상태에 따라 종료되거나 종료되지 않을 수 있습니다.

- 만료되지 않은 유효한 토큰에 대한 비종료 — 토큰이 구성된 CAPTCHA 또는 챌린지 면역 시간에 따라 유효하고 만료되지 않은 경우 조치와 유사하게 요청을 처리합니다. AWS WAF Count AWS WAF 웹 ACL의 나머지 규칙을 기반으로 웹 요청을 계속 검사합니다. Count 구성과 마찬가지로, 정의한 규칙에서도 요청에 삽입할 사용자 지정 헤더를 사용하여 이러한 작업을 선택적으로 구성하고 다른 규칙과 일치시킬 수 있는 레이블을 추가할 수 있습니다.
- 유효하지 않거나 만료된 토큰에 대한 요청이 차단되어 종료 — 토큰이 유효하지 않거나 표시된 타임스탬프가 만료된 경우, 웹 요청 검사가 AWS WAF 종료되고 요청이 차단됩니다. 이는 조치와 유사합니다. Block AWS WAF 그런 다음 사용자 지정 응답 코드로 클라이언트에 응답합니다. 의 경우 요청 내용에 클라이언트 브라우저에서 처리할 수 있다고 명시되어 있는 경우 인간 클라이언트와 봇을 구분하도록 설계된 JavaScript 전면 광고 형식으로 CAPTCHA 퍼즐을 AWS WAF 전송하기 때문입니다. CAPTCHA Challenge액션의 경우 일반 브라우저와 봇이 실행하는 세션을 구분하도록 설계된 자동 챌린지가 포함된 JavaScript 전면 광고를 AWS WAF 보냅니다.

자세한 내용은 CAPTCHA그리고 Challenge 안에 AWS WAF 섹션을 참조하세요.

요청 및 응답을 사용자 지정하는 방법에 대한 자세한 내용은 AWS WAF의 사용자 지정된 웹 요청 및 응답 섹션을 참조하세요.

레이블을 추가하여 요청을 일치하는 방법에 대한 자세한 내용은 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.

웹 ACL 및 규칙 설정이 상호 작용하는 방벙에 대한 자세한 내용은 웹 ACL 규칙 및 규칙 그룹 평가 섹션을 참조하세요.

규칙 문 기본 사항

규칙 명령문은 웹 요청을 검사하는 AWS WAF 방법을 알려주는 규칙의 일부입니다. 웹 요청에서 검사 기준을 AWS WAF 찾으면 해당 웹 요청이 명령문과 일치한다고 말합니다. 모든 규칙 문은 문 유형에 따라 찾을 내용과 방법을 지정합니다.

의 모든 AWS WAF 규칙에는 다른 명령문을 포함할 수 있는 하나의 최상위 규칙 명령문이 있습니다. 규칙 문은 매우 간단할 수 있습니다. 예를 들어 웹 요청을 검사할 출처 국가 집합을 제공하는 명령문을 사용하거나 규칙 그룹만 참조하는 웹 ACL 내 규칙 문을 사용할 수 있습니다. 규칙 문은 매우 복잡할 수도 있습니다. 예를 들어 다른 많은 문을 논리적 AND, OR 및 NOT 문과 결합하는 문이 있을 수 있습니다.

대부분의 규칙의 경우 매칭 요청에 사용자 지정 AWS WAF 레이블을 추가할 수 있습니다. AWS 관리형 규칙 그룹의 규칙은 매칭 요청에 레이블을 추가합니다. 규칙이 추가하는 레이블은 나중에 웹 ACL과 AWS WAF 로그 및 지표에서 평가되는 규칙에 대한 요청 정보를 제공합니다. 레이블 지정에 대한 자세한 내용은 AWS WAF 웹 요청의 레이블 및 을 참조하십시오. 레이블 일치 규칙 문

중첩 규칙 문

AWS WAF 여러 규칙 명령문에 대해 중첩을 지원하지만 모든 규칙 문에 대한 중첩을 지원하지는 않습니다. 예를 들어 규칙 그룹 문을 다른 문 안에 중첩할 수 없습니다. 범위 축소 문, 논리 문 등의 일부 시나리오에서는 중첩을 사용해야 합니다. 다음 규칙 문 목록과 규칙 세부 정보는 각 범주 및 규칙의 중첩 기능 및 요구 사항을 설명합니다.

콘솔의 규칙 시각적 편집기에서는 규칙 문에 대해 한 수준의 중첩만 지원합니다. 예를 들어 여러 유형의 명령문을 논리적 AND 또는 OR 규칙 안에 중첩할 수 있지만, 두 번째 중첩 수준이 필요하므로 다른 AND 또는 OR 규칙은 중첩할 수 없습니다. 여러 수준의 중첩을 구현하려면 콘솔의 JSON 규칙 편집기나 API를 통해 JSON으로 규칙 정의를 제공하십시오.

주제

- 웹 요청 구성 요소 사양 및 처리
- 범위 축소 문
- 집합 또는 규칙 그룹을 참조하는 문

웹 요청 구성 요소 사양 및 처리

이 섹션에서는 웹 요청의 구성 요소를 검사하는 규칙 문에서 지정할 수 있는 설정에 대해 설명합니다. 사용에 대한 자세한 내용은 일치 규칙 문에서 개별 규칙 문을 참조하세요.

이러한 웹 요청 구성 요소의 하위 집합을 속도 기반 규칙에서 사용자 지정 요청 집계 키로 사용할 수도 있습니다. 자세한 내용은 속도 기반 규칙 집계 옵션 및 키을 참조하세요.

요청 구성 요소 설정의 경우 구성 요소 유형 자체와 구성 요소 유형에 따라 추가 옵션을 지정합니다. 예를 들어 텍스트가 포함된 구성 요소 유형을 검사할 때는 검사하기 전에 텍스트 변형을 적용할 수 있습니다.

> **Note**
>
> 달리 명시되지 않는 한, 웹 요청에 규칙 문에 지정된 요청 구성 요소가 없는 경우 요청이 규칙 기준과 일치하지 않는 것으로 AWS WAF 평가합니다.

목차

  - 단일 헤더
  - 모든 헤더
  - 헤더 순서
  - 쿠키
  - URI 경로
  - JA3 지문
  - 쿼리 문자열
  - 단일 쿼리 파라미터
  - 모든 쿼리 파라미터
  - 본문
  - JSON 본문
- 전달된 IP 주소
- HTTP/2 유사 헤더 검사 옵션
- 텍스트 변환 옵션

요청 구성 요소 옵션

이 섹션에서는 검사용으로 지정할 수 있는 웹 요청의 구성 요소를 설명합니다. 웹 요청 내에서 패턴을 찾는 일치 규칙 문에 대해 요청 구성 요소를 지정합니다. 이러한 유형의 문에는 문자열 일치, 정규식 일치, 크기 제약 조건 및 SQL 주입 공격 문이 포함됩니다. 이러한 요청 구성 요소 설정을 사용하는 방법에 대한 자세한 내용은 일치 규칙 문에서 개별 규칙 문을 참조하세요.

달리 명시되지 않는 한, 웹 요청에 규칙 설명에 지정된 요청 구성 요소가 없는 경우 요청이 규칙 기준과 일치하지 않는 것으로 AWS WAF 평가합니다.

> **Note**
>
> 요청 구성 요소가 필요한 각 규칙 문에 대해 단일 요청 구성 요소를 지정합니다. 요청 구성 요소를 두 개 이상 검사하려면 각 구성 요소에 대한 규칙 문을 만듭니다.

AWS WAF 콘솔 및 API 설명서는 다음 위치의 요청 구성 요소 설정에 대한 지침을 제공합니다.

- 콘솔의 규칙 작성기 – 정규 규칙 유형에 대한 명령문 설정에서는 검사 대화 상자의 요청 구성 요소에서 검사할 구성 요소를 선택합니다.

- API 문 내용 – `FieldToMatch`

이 섹션의 나머지 부분에서는 검사할 웹 요청의 일부에 대한 옵션을 설명합니다.

주제

HTTP 메서드

요청의 HTTP 메서드를 검사합니다. HTTP 메서드는 `POST` 또는 `GET` 등 웹 요청이 보호된 리소스에게 수행을 요구하고 있는 작업 유형을 나타냅니다.

단일 헤더

요청에서 이름이 지정된 단일 헤더를 검사합니다.

이 옵션의 경우 헤더 이름(예: `User-Agent` 또는`Referer`)을 지정합니다. 이름에 대한 문자열 일치에서는 대/소문자를 구분하지 않습니다.

모든 헤더

쿠키를 포함한 모든 요청 헤더를 검사합니다. 필터를 적용하여 모든 헤더 중 일부를 검사할 수 있습니다.

이 옵션에 대해 다음 사양을 제공합니다.

- 일치 패턴 - 검사할 헤더의 하위 집합을 가져오는 데 사용하는 필터입니다. AWS WAF 헤더 키에서 이러한 패턴을 찾습니다.

  일치 패턴 설정은 다음 중 하나일 수 있습니다.

  - 모두 — 모든 키를 일치시킵니다. 모든 헤더의 규칙 검사 기준을 평가합니다.
  - 제외된 헤더 – 여기에 지정된 문자열과 키가 일치하지 않는 헤더만 검사합니다. 키에 대한 문자열 일치에서는 대/소문자를 구분하지 않습니다.
  - 포함된 헤더 – 여기에 지정된 문자열 중 하나와 일치하는 키가 있는 헤더만 검사합니다. 키에 대한 문자열 일치에서는 대/소문자를 구분하지 않습니다.
- 일치 범위 - 규칙 검사 기준에 따라 AWS WAF 검사해야 하는 헤더 부분. 키, 값 또는 모두를 지정하여 키와 값이 둘 다 일치하는지 검사할 수 있습니다.

  모두의 경우 키와 값에 모두 일치 항목을 찾아야 할 필요는 없습니다. 일치하는 키 또는 값을 찾거나 둘 다 일치하는 항목을 찾으면 됩니다. 키와 값이 일치하도록 하려면 논리 AND 문을 사용하여 키를 검사하는 규칙 하나와 값을 검사하는 규칙 하나, 이렇게 두 가지 일치 규칙을 결합합니다.
- 오버사이즈 처리 — AWS WAF 검사할 수 있는 것보다 큰 헤더 데이터가 있는 요청을 어떻게 AWS WAF 처리해야 할까요? AWS WAF 요청 헤더의 처음 8KB (8,192바이트), 최대 처음 200개의 헤더를 검사할 수 있습니다. 첫 번째 제한에 도달할 때까지 콘텐츠를 AWS WAF 검사할 수 있습니다. 검사를 계속하거나 검사를 건너뛰고 요청을 규칙과 일치하거나 일치하지 않는 것으로 표시할 수 있습니다. 과대 콘텐츠 처리에 대한 자세한 내용은 에서 크기 초과 요청 구성 요소 처리 AWS WAF 섹션을 참조하세요.

헤더 순서

검사 요청을 AWS WAF 받은 웹 요청에 나타나는 순서대로 요청의 헤더 이름 목록이 들어 있는 문자열을 검사합니다. AWS WAF 문자열을 생성한 다음 이 문자열을 필드로 사용하여 검사 시 구성 요소를 일치시킵니다. AWS WAF 예를 들어 문자열의 헤더 이름을 공백 없이 콜론으로 구분합니다.
`host:user-agent:accept:authorization:referer`

이 옵션에 대해 다음 사양을 제공합니다.

- 크기 초과 처리 — 검사할 수 있는 것보다 AWS WAF 많거나 큰 헤더 데이터가 있는 요청을 어떻게 AWS WAF 처리해야 할까요? AWS WAF 요청 헤더의 처음 8KB (8,192바이트), 최대 처음 200개의 헤더를 검사할 수 있습니다. 첫 번째 제한에 도달할 때까지 콘텐츠를 AWS WAF 검사할 수 있습니다. 사용할 수 있는 헤더 검사를 계속하거나 검사를 건너뛰고 요청을 규칙과 일치하거나 일치하지 않는 것으로 표시할 수 있습니다. 과대 콘텐츠 처리에 대한 자세한 내용은 에서 크기 초과 요청 구성 요소 처리 AWS WAF 섹션을 참조하세요.

쿠키

모든 요청 쿠키를 검사합니다. 필터를 적용하여 모든 쿠키의 하위 집합을 검사할 수 있습니다.

이 옵션에 대해 다음 사양을 제공합니다.

- 일치 패턴 - 검사할 쿠키의 하위 집합을 가져오는 데 사용하는 필터입니다. AWS WAF 는 쿠키 키에서 이러한 패턴을 찾습니다.

  일치 패턴 설정은 다음 중 하나일 수 있습니다.

  - 모두 — 모든 키를 일치시킵니다. 모든 쿠키의 규칙 검사 기준을 평가합니다.
  - 제외된 쿠키 – 여기에 지정된 문자열과 키가 일치하지 않는 쿠키만 검사합니다. 키의 문자열 일치는 대소문자를 구분하며 정확해야 합니다.
  - 포함된 쿠키 – 여기에 지정된 문자열 중 하나와 일치하는 키가 있는 쿠키만 검사합니다. 키의 문자열 일치는 대소문자를 구분하며 정확해야 합니다.
- 범위 일치 — 규칙 검사 기준에 따라 AWS WAF 검사해야 하는 쿠키 부분입니다. 키와 값 둘 다에 대해 키, 값 또는 모두를 지정할 수 있습니다.

  모두의 경우 키와 값에 모두 일치 항목을 찾아야 할 필요는 없습니다. 일치하는 키 또는 값을 찾거나 둘 다 일치하는 항목을 찾으면 됩니다. 키와 값이 일치하도록 하려면 논리 AND 문을 사용하여 키를 검사하는 규칙 하나와 값을 검사하는 규칙 하나, 이렇게 두 가지 일치 규칙을 결합합니다.
- 크기 초과 처리 — AWS WAF 검사할 수 있는 것보다 큰 쿠키 데이터가 있는 요청을 어떻게 AWS WAF 처리해야 할까요? AWS WAF 요청 쿠키의 처음 8KB (8,192바이트), 최대 처음 200개의 쿠키를 검사할 수 있습니다. 첫 번째 제한에 도달할 때까지 콘텐츠를 AWS WAF 검사할 수 있습니다. 검사를 계속하거나 검사를 건너뛰고 요청을 규칙과 일치하거나 일치하지 않는 것으로 표시할 수 있습니다. 과대 콘텐츠 처리에 대한 자세한 내용은 에서 크기 초과 요청 구성 요소 처리 AWS WAF 섹션을 참조하세요.

URI 경로

리소스를 식별하는 URL의 부분을 검사합니다(예: `/images/daily-ad.jpg`). 자세한 설명은 Uniform Resource Identifier (URI): Generic Syntax 섹션을 참조하세요.

이 옵션과 함께 텍스트 변환을 사용하지 AWS WAF 않으면 URI를 정규화하지 않고 요청에서 클라이언트로부터 수신한 그대로 URI를 검사합니다. 텍스트 변환에 대한 자세한 내용은 텍스트 변환 옵션 섹션을 참조하세요.

JA3 지문

요청의 JA3 지문을 검사합니다.

> **Note**
>
> JA3 지문 검사는 Amazon CloudFront 배포 및 애플리케이션 로드 밸런서에만 사용할 수 있습니다.

JA3 자문은 수신 요청의 TLS 클라이언트 Hello에서 파생된 32자 해시입니다. 이 지문은 클라이언트 TLS 구성의 고유 식별자 역할을 합니다. AWS WAF 계산에 필요한 충분한 TLS Client Hello 정보가 있는 각 요청에 대해 이 핑거프린트를 계산하고 기록합니다. 거의 모든 웹 요청에는 이 정보가 포함됩니다.

클라이언트용 JA3 지문을 가져오는 방법

웹 ACL 로그에서 클라이언트 요청에 대한 JA3 지문을 얻을 수 있습니다. 핑거프린트를 계산할 수 있는 경우 로그에 해당 AWS WAF 핑거프린트가 포함됩니다. 로깅 필드에 대한 자세한 내용은 로그 필드 섹션을 참조하세요.

규칙 문 요구 사항

제공하는 문자열과 정확히 일치하도록 설정된 문자열 일치 문 내에서만 JA3 지문을 검사할 수 있습니다. 문자열 일치 문 사양의 로그에서 JA3 지문 문자열을 제공하여 동일한 TLS 구성을 갖는 향후 요청과 일치시킵니다. 문자열 일치 문에 대한 자세한 내용은 문자열 일치 규칙 문 섹션을 참조하세요.

이 규칙 문에 대한 폴백 동작을 제공해야 합니다. 폴백 동작은 JA3 핑거프린트를 계산할 수 없는 경우 AWS WAF 웹 요청에 AWS WAF 할당하려는 일치 상태입니다. 일치시키도록 선택하면 AWS WAF 에서 요청을 규칙 문과 일치하는 것으로 처리하며 규칙 동작을 요청에 적용합니다. 일치하지 않도록 선택하면 요청이 규칙 AWS WAF 설명과 일치하지 않는 것으로 처리됩니다.

이 일치 옵션을 사용하려면 웹 ACL 트래픽을 기록해야 합니다. 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅을 참조하세요.

쿼리 문자열

? 문자(있는 경우) 뒤에 나타나는 URL의 부분을 검사합니다.

> **Note**
>
> 사이트 간 스크립팅 일치 명령문의 경우 쿼리 문자열 대신 모든 쿼리 파라미터를 선택하는 것이 좋습니다. 모든 쿼리 파라미터를 선택하면 기본 비용에 WCU 10개가 추가됩니다.

단일 쿼리 파라미터

쿼리 문자열의 일부로 정의한 단일 쿼리 매개변수를 검사합니다. AWS WAF 지정한 매개 변수의 값을 검사합니다.

이 옵션의 경우 쿼리 인수도 지정합니다. 예를 들어 URL이 `www.xyz.com?UserName=abc&SalesRegion=seattle`인 경우 쿼리 인수로 `UserName` 또는 `SalesRegion`를 지정할 수 있습니다. 인수의 최대 길이는 30자입니다. 이름은 대소문자를 구분하지 않으므로 `UserName`을 지정하면 AWS WAF 는 `username` 및 `UsERName`을 포함한 `UserName`의 모든 변형과 일치합니다.

쿼리 문자열에 지정한 쿼리 인수 인스턴스가 두 개 이상 포함된 경우 는 로직을 사용하여 OR 모든 값이 일치하는지 AWS WAF 검사합니다. 예를 들어 URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle`에서 AWS WAF 은 `boston` 및 `seattle`에 대해 지정한 이름을 평가합니다. 둘 중 하나가 일치하는 경우 검사는 일치입니다.

모든 쿼리 파라미터

ㅌ요청의 모든 쿼리 파라미터를 검사합니다. 이는 단일 쿼리 파라미터 구성 요소 선택과 비슷하지만 쿼리 문자열 내 모든 인수의 값을 AWS WAF 검사합니다. 예를 들어, URL이 `www.xyz.com?UserName=abc&SalesRegion=seattle`인 경우 AWS WAF 는 `UserName` 또는 `SalesRegion`의 값이 검사 기준과 일치하는 경우 일치를 트리거합니다.

이 옵션을 선택하면 기본 비용에 WCU 10개가 추가됩니다.

본문

요청 본문을 일반 텍스트로 평가해 검사합니다. JSON 콘텐츠 유형을 사용하여 본문을 JSON으로 평가할 수도 있습니다.

요청 본문은 요청 헤더 바로 뒤에 오는 요청 부분입니다. 여기에는 웹 요청에 필요한 추가 데이터(예: 양식의 데이터)가 포함됩니다.

- 콘솔의 콘텐츠 유형 옵션에서 일반 텍스트를 선택하여 요청 옵션에서 본문을 선택합니다.
- API의 규칙 `FieldToMatch` 사양에서 요청 본문을 일반 텍스트로 검사하도록 `Body`를 지정합니다.

Application Load Balancer 및 의 AWS AppSync경우 요청 본문의 처음 8KB를 AWS WAF 검사할 수 있습니다. 의 경우 CloudFront 기본적으로 API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스는 처음 16KB를 AWS WAF 검사할 수 있으며 웹 ACL 구성에서는 제한을 최대 64KB까지 늘릴 수 있습니다. 자세한 정보는 신체 검사 크기 제한 관리을 참조하세요.

이 구성 요소 유형에 대한 과대 처리를 지정해야 합니다. 오버사이즈 처리는 검사할 수 있는 양보다 큰 본문 데이터가 있는 요청을 AWS WAF 처리하는 방법을 정의합니다. AWS WAF 검사를 계속하거나 검사를 건너뛰고 요청을 규칙과 일치하거나 일치하지 않는 것으로 표시할 수 있습니다. 과대 콘텐츠 처리에 대한 자세한 내용은 에서 크기 초과 요청 구성 요소 처리 AWS WAF 섹션을 참조하세요.

또한 본문을 구문 분석된 JSON으로 평가할 수도 있습니다. 자세한 내용은 이어지는 섹션을 참조하세요.

JSON 본문

JSON으로 평가된 요청 본문을 검사합니다. 본문을 일반 텍스트로 평가할 수도 있습니다.

요청 본문은 요청 헤더 바로 뒤에 오는 요청 부분입니다. 여기에는 웹 요청에 필요한 추가 데이터(예: 양식의 데이터)가 포함됩니다.

- 콘솔의 콘텐츠 유형 옵션에서 JSON을 선택하여 요청 옵션에서 본문을 선택합니다.
- API의 규칙 `FieldToMatch` 사양에서 `JsonBody`를 지정합니다.

Application Load Balancer 및 의 AWS AppSync경우 요청 본문의 처음 8KB를 AWS WAF 검사할 수 있습니다. 의 경우 CloudFront 기본적으로 API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스는 처음 16KB를 AWS WAF 검사할 수 있으며 웹 ACL 구성에서는 제한을 최대 64KB까지 늘릴 수 있습니다. 자세한 정보는 신체 검사 크기 제한 관리을 참조하세요.

이 구성 요소 유형에 대한 과대 처리를 지정해야 합니다. 오버사이즈 처리는 검사할 수 있는 양보다 큰 본문 데이터가 있는 요청을 AWS WAF 처리하는 방법을 정의합니다. AWS WAF 검사를 계속하거나 검사를 건너뛰고 요청을 규칙과 일치하거나 일치하지 않는 것으로 표시할 수 있습니다. 과대 콘텐츠 처리에 대한 자세한 내용은 에서 크기 초과 요청 구성 요소 처리 AWS WAF 섹션을 참조하세요.

이 옵션을 선택하면 일치 문의 기본 비용 WCU가 두 배로 늘어납니다. 예를 들어 JSON 구문 분석을 사용하지 않는 일치 문 기본 비용이 5WCU인 경우 JSON 구문 분석을 사용하면 비용이 두 배가 되어 10WCU로 됩니다.

JSON 본문 검사 단계 및 옵션

웹 요청 본문을 JSON으로 AWS WAF 검사하는 경우 본문을 파싱하고 검사를 위해 JSON 요소를 추출하는 단계를 수행합니다. 다음은 이 요청 구성 요소 유형에 대한 단계 및 추가 구성 옵션 목록입니다.

1. 본문 내용 AWS WAF 분석 - 검사에 사용할 JSON 요소를 추출하기 위해 웹 요청 본문의 내용을 구문 분석합니다. AWS WAF 본문의 전체 내용을 분석하는 데 최선을 다하지만 내용의 다양한 오류 상태로 인해 구문 분석이 실패할 수 있습니다. 잘못된 문자, 중복된 키, 잘림, 루트 노드가 객체나 배열이 아닌 콘텐츠 등을 예로 들 수 있습니다.

   옵션 본문 파싱 폴백 동작은 JSON 본문을 완전히 AWS WAF 파싱하지 못할 경우의 조치를 결정합니다.

   - 없음 (기본 동작) - 구문 분석 오류가 발생한 지점까지만 콘텐츠를 AWS WAF 평가합니다.
   - 문자열로 평가 - 본문을 일반 텍스트로 검사합니다. AWS WAF JSON 검사를 위해 정의한 텍스트 변환과 검사 기준을 본문 텍스트 문자열에 적용합니다.
   - 일치 - 웹 요청을 규칙 설명과 일치하는 것으로 취급합니다. AWS WAF 요청에 규칙 조치를 적용합니다.
   - 일치하지 않음 - 웹 요청을 규칙 문과 일치하지 않는 것으로 처리합니다.

   > **Note**
   >
   > 이 폴백 동작은 JSON 문자열을 파싱하는 동안 AWS WAF 오류가 발생한 경우에만 트리거됩니다.

   파싱은 JSON을 완전히 검증하지 않습니다.

   AWS WAF 파싱은 입력 JSON 문자열을 완전히 검증하지 않으므로 유효하지 않은 JSON에 대해서도 파싱이 성공할 수 있습니다.

   예를 들어 다음과 같은 잘못된 JSON을 AWS WAF 오류 없이 파싱합니다.

   - 쉼표 누락: `{"key1":"value1""key2":"value2"}`
   - 콜론 누락: `{"key1":"value1","key2""value2"}`
   - 추가 콜론: `{"key1"::"value1","key2""value2"}`

   예를 들어 구문 분석에 성공했지만 결과가 완전히 유효한 JSON이 아닌 경우 평가 후속 단계의 결과가 달라질 수 있습니다. 추출 시 일부 요소가 누락되거나 규칙 평가 시 예상치 못한 결과가 발생할 수 있습니다. 애플리케이션에서 수신한 JSON의 유효성을 검사하고 필요에 따라 잘못된 JSON을 처리하는 것이 좋습니다.

2. JSON 요소 추출 - 설정에 따라 검사할 JSON 요소의 하위 집합을 AWS WAF 식별합니다.

   - JSON 일치 범위 옵션은 검사해야 하는 JSON의 요소 유형을 지정합니다. AWS WAF

     키와 값 둘 다에 대해 키, 값 또는 모두를 지정할 수 있습니다.

     모두의 경우 키와 값에 모두 일치 항목을 찾아야 할 필요는 없습니다. 일치하는 키 또는 값을 찾거나 둘 다 일치하는 항목을 찾으면 됩니다. 키와 값이 일치하도록 하려면 논리 AND 문을 사용하여 키를 검사하는 규칙 하나와 값을 검사하는 규칙 하나, 이렇게 두 가지 일치 규칙을 결합합니다.
   - 검사할 콘텐츠 옵션은 검사하려는 AWS WAF 하위 집합으로 요소 세트를 필터링하는 방법을 지정합니다.

     다음 중 하나를 지정해야 합니다.

     - 전체 JSON 콘텐츠 - 모든 요소를 평가합니다.
     - 포함된 요소만 - 경로가 제공된 JSON 포인터 기준과 일치하는 요소만 평가합니다. 이 옵션을 사용하여 JSON의 모든 경로를 표시하지 마세요. 대신 전체 JSON 콘텐츠를 사용하세요.

       JSON 포인터 구문에 대한 자세한 내용은 IETF (인터넷 엔지니어링 태스크 포스) 문서 JavaScript 객체 표기법 (JSON) 포인터를 참조하십시오.

       예를 들어, 콘솔에서 다음을 제공할 수 있습니다.

       ```
       /dogs/0/name
       /dogs/1/name
       ```

       API 또는 CLI에서 다음을 제공할 수 있습니다.

       ```
       "IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
       ```

예를 들어 검사할 콘텐츠 설정은 포함된 요소만이고 포함된 요소 설정은 다음과 같다고 가정해 보겠습니다. /a/b

다음 예시 JSON 본문의 경우:

```
{
  "a":{
    "c":"d",
    "b":{
      "e":{
        "f":"g"
```

```
        }
      }
    }
  }
```

각 JSON 일치 범위 설정을 AWS WAF 검사할 요소 집합은 다음과 같습니다. 포함된 요소 경로의 b 일부인 키는 평가되지 않는다는 점에 유의하세요.

- 모두: e f, 및g.
- 키: e 및f.
- 값:g.

3. JSON 요소 세트 검사 - 추출된 JSON 요소에 지정한 모든 텍스트 변형을 AWS WAF 적용한 다음 결과 요소 세트를 규칙 명령문의 일치 기준과 일치시킵니다. 이는 다른 웹 요청 구성 요소와 동일한 변환 및 평가 동작입니다. 추출된 JSON 요소 중 하나라도 일치하는 경우 웹 요청은 규칙과 일치하는 것으로 간주됩니다.

전달된 IP 주소

이 섹션은 웹 요청의 IP 주소를 사용하는 규칙 설명에 적용됩니다. 기본적으로 웹 요청 출처의 IP 주소를 AWS WAF 사용합니다. 웹 요청이 하나 이상의 프록시 또는 로드 밸런서를 통과할 경우 웹 요청 오리진에는 클라이언트의 최초 주소가 아닌 마지막 프록시의 주소가 포함됩니다. 이 경우 발신 클라이언트 주소는 일반적으로 다른 HTTP 헤더를 통해 전달됩니다. 이 헤더는 일반적으로 `X-Forwarded-For`(XFF)지만 다른 헤더일 수도 있습니다.

IP 주소를 사용하는 규칙 문

IP 주소를 사용하는 규칙 문은 다음과 같습니다.

- IP 집합 일치 - IP 주소가 IP 집합에 정의된 주소와 일치하는지 검사합니다.
- 지리적 일치- IP 주소를 사용하여 오리진 국가 및 리전을 결정하고 오리진 국가를 국가 목록과 비교합니다.
- 비율 기반 규칙 문 - 개별 IP 주소가 너무 높은 속도로 요청을 보내지 않도록 IP 주소별로 요청을 집계할 수 있습니다. IP 주소 집계를 단독으로 사용하거나 다른 집계 키와 함께 사용할 수 있습니다.

이러한 규칙 명령문에 웹 요청의 출처를 사용하는 대신 `X-Forwarded-For` 헤더나 다른 HTTP 헤더에서 전달된 IP 주소를 사용하도록 AWS WAF 지시할 수 있습니다. 사양을 제공하는 방법에 대한 자세한 내용은 개별 규칙 문 유형에 대한 지침을 참조하세요.

> **Note**
>
> 지정한 헤더가 요청에 없는 경우 웹 요청에 규칙을 전혀 적용하지 AWS WAF 않습니다.

폴백 동작

전달된 IP 주소를 사용하면 요청의 지정된 위치에 유효한 IP 주소가 없는 경우 웹 요청에 AWS WAF 할당할 일치 상태를 지정합니다.

- MATCH - 웹 요청을 규칙 설명과 일치하는 것으로 취급합니다. AWS WAF 요청에 규칙 조치를 적용합니다.
- 일치하지 않음 - 웹 요청을 규칙 문과 일치하지 않는 것으로 처리합니다.

AWS WAF 봇 컨트롤에 사용되는 IP 주소

봇 컨트롤 관리 규칙 그룹은 의 IP 주소를 사용하여 봇을 확인합니다. AWS WAF Bot Control을 사용하고 프록시나 로드 밸런서를 통해 라우팅되는 봇을 확인한 경우 사용자 지정 규칙을 사용하여 봇을 명시적으로 허용해야 합니다. 예를 들어, 전달된 IP 주소를 사용하여 확인된 봇을 탐지하고 허용하는 사용자 지정 IP 집합 일치 규칙을 구성할 수 있습니다. 규칙을 사용하여 다양한 방식으로 봇 관리를 사용자 지정할 수 있습니다. 자세한 내용 및 예제는 AWS WAF 봇 컨트롤 섹션을 참조하세요.

전달된 IP 주소 사용에 대한 일반 고려 사항

전달된 IP 주소를 사용하기 전에 다음과 같은 일반적인 주의 사항을 참고하십시오.

- 헤더는 과정 중에 프록시를 통해 수정될 수 있으며, 프록시는 다양한 방식으로 헤더를 처리할 수 있습니다.
- 공격자가 AWS WAF 검사를 우회하기 위해 헤더의 내용을 변경할 수 있습니다.
- 헤더 내 IP 주소는 형식이 잘못되었거나 유효하지 않을 수 있습니다.
- 지정한 헤더가 요청에 전혀 없을 수도 있습니다.

다음과 같이 전달된 IP 주소를 사용할 때 고려할 사항 AWS WAF

다음 목록은 에서 전달된 IP 주소를 사용하기 위한 요구 사항 및 주의 사항을 설명합니다. AWS WAF

- 단일 규칙의 경우 전달된 IP 주소에 헤더 하나를 지정할 수 있습니다. 헤더 사양은 대/소문자를 구분하지 않습니다.

- 속도 기반 규칙 문의 경우 중첩된 범위 지정 문이 전달된 IP 구성을 상속하지 않습니다. 전달된 IP 주소를 사용하는 각 명령문의 구성을 지정하십시오.
- 지역 일치 및 속도 기반 규칙의 경우 헤더의 첫 번째 주소를 AWS WAF 사용합니다. 예를 들어, 헤더에 용도가 포함된 경우 `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF `10.1.1.1`
- IP 집합 일치의 경우, 헤더의 첫 번째 주소, 마지막 주소 또는 임의 주소와 일치시킬지 여부를 지정합니다. 하나를 지정하는 경우 헤더의 모든 주소를 AWS WAF 검사하여 일치하는 주소가 있는지 확인합니다 (최대 10개 주소). 헤더에 10개가 넘는 주소가 포함된 경우 마지막 10개를 AWS WAF 검사합니다.
- 주소가 여러 개 포함된 헤더는 주소 사이에 쉼표 구분 기호를 사용해야 합니다. 요청에 쉼표 이외의 구분자를 사용하는 경우 AWS WAF 는 헤더의 IP 주소 형식을 잘못된 것으로 간주합니다.
- 헤더 내의 IP 주소 형식이 잘못되었거나 유효하지 않은 경우 AWS WAF 는 사용자가 전달된 IP 구성에 지정하는 폴백 동작에 따라 웹 요청을 규칙과 일치하거나 일치하지 않는 것으로 지정합니다.
- 지정한 헤더가 요청에 없는 경우 요청에는 규칙이 전혀 적용되지 AWS WAF 않습니다. 즉 AWS WAF , 규칙 동작이 적용되지 않고 폴백 동작도 적용되지 않습니다.
- IP 주소에 대해 전달된 IP 헤더를 사용하는 규칙 문은 웹 요청 오리진에서 보고하는 IP 주소를 사용하지 않습니다.

다음과 같이 전달된 IP 주소를 사용하는 모범 사례 AWS WAF

전달된 IP 주소를 사용하는 경우 다음 모범 사례를 따르십시오.

- 전달된 IP 구성을 활성화하기 전에 요청 헤더의 가능한 모든 상태를 신중하게 고려하십시오. 원하는 동작을 얻기 위해 둘 이상의 규칙을 사용해야 할 수도 있습니다.
- 여러 개의 전달된 IP 헤더를 검사하거나 웹 요청 오리진 및 전달된 IP 헤더를 검사하려면 각 IP 주소 소스에 대해 하나의 규칙을 사용하십시오.
- 유효하지 않은 헤더를 포함하는 웹 요청을 차단하려면 규칙 작업을 차단으로 설정하고 전달된 IP 구성의 폴백 동작을 일치시키도록 설정하십시오.

전달된 IP 주소에 대한 JSON 예제

다음 지역 일치문은 오리진 국가가 US인 IP만 `X-Forwarded-For` 헤더에 포함되는 경우에 일치합니다.

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
```

```
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

다음 속도 기반 규칙은 X-Forwarded-For 헤더의 첫 번째 IP를 기준으로 요청을 집계합니다. 규칙은 중첩된 지역 일치 문과 일치하는 요청 수만 계산하고 리전 일치 문과 일치하는 요청만 차단합니다. 또한 중첩된 지역 일치문은 X-Forwarded-For 헤더를 사용하여 IP 주소에 오리진 국가로 US가 표시되는지 여부를 결정합니다. 이 경우 또는 헤더가 있지만 형식이 잘못된 경우 지역 일치 문에서 일치하는 항목을 반환합니다.

```
{
  "Name": "XFFTestRateGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestRateGeo"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "FORWARDED_IP",
      "ScopeDownStatement": {
```

```
        "GeoMatchStatement": {
          "CountryCodes": [
            "US"
          ],
          "ForwardedIPConfig": {
            "HeaderName": "x-forwarded-for",
            "FallbackBehavior": "MATCH"
          }
        }
      },
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

HTTP/2 유사 헤더 검사 옵션

HTTP/2 트래픽을 지원하는 보호 AWS 리소스는 검사를 위해 HTTP/2 유사 헤더를 전달하지 않지만 검사하는 웹 요청 구성 요소에 유사 헤더의 AWS WAF 콘텐츠를 제공합니다. AWS WAF

다음 표에 나열된 유사 헤더만 AWS WAF 검사하는 데 사용할 수 있습니다.

웹 요청 구성 요소로 매핑된 HTTP/2 의사 헤더 콘텐츠

HTTP/2 의사 헤더	검사할 웹 요청 구성 요소	설명서
`:method`	HTTP 메서드	HTTP 메서드
`:authority`	`Host` 헤더	단일 헤더 모든 헤더
`:path` URI 경로	URI 경로	URI 경로
`:path` 쿼리	쿼리 문자열	쿼리 문자열 단일 쿼리 파라미터

HTTP/2 의사 헤더	검사할 웹 요청 구성 요소	설명서
		모든 쿼리 파라미터

텍스트 변환 옵션

패턴을 찾거나 제약 조건을 설정하는 명령문에서는 요청을 검사하기 전에 적용할 변환을 제공할 수 있습니다. AWS WAF 변환은 공격자가 AWS WAF를 우회하기 위해 사용하는 일부 비정상적인 서식을 제거하기 위해 웹 요청을 다시 포맷합니다.

이 옵션을 JSON 본문 요청 구성 요소 선택과 함께 사용하는 경우 AWS WAF 는 JSON에서 검사할 요소를 구문 분석하고 추출한 후 변환을 적용합니다. 자세한 정보는 JSON 본문을 참조하세요.

하나 이상의 변환을 제공하는 경우 AWS WAF 에서 변환을 적용하는 순서도 설정합니다.

WCU – 각 텍스트 변환은 10WCU입니다.

AWS WAF 콘솔 및 API 설명서는 다음 위치의 이러한 설정에 대한 지침도 제공합니다.

- 콘솔의 규칙 빌더 - 텍스트 변환. 이 옵션은 요청 구성 요소를 사용할 때 제공됩니다.
- API 문 내용 – `TextTransformations`

텍스트 변환을 위한 옵션

각 변환 목록에는 콘솔 및 API 사양과 설명이 차례로 표시됩니다.

Base64 decode – `BASE64_DECODE`

AWS WAF Base64로 인코딩된 문자열을 디코딩합니다.

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF Base64로 인코딩된 문자열을 디코딩하지만 유효하지 않은 문자는 무시하는 관용 구현을 사용합니다.

Command line – `CMD_LINE`

이 옵션은 공격자가 운영 체제 명령줄 명령을 주입하면서 특이한 형식을 사용하여 명령의 일부 또는 전체를 위장하는 상황을 완화합니다.

이 옵션을 사용하여 다음 변환을 수행합니다.

- 다음 문자 삭제: `\ " ' ^`

- 다음 문자 앞에 있는 공백 삭제: / (
- 다음 문자를 공백으로 바꿈: , ;
- 여러 개의 공백을 하나의 공백으로 바꿈
- 대문자 A-Z을 소문자 a-z로 변환

Compress whitespace – COMPRESS_WHITE_SPACE

AWS WAF 여러 공백을 한 공백으로 바꾸고 다음 문자를 공백 문자 (ASCII 32) 로 바꾸어 공백을 압축합니다.

- 폼피드(ASCII 12)
- 탭(ASCII 9)
- 새줄(ASCII 10)
- 캐리지 리턴(ASCII 13)
- 세로 탭(ASCII 11)
- 줄 바꿈하지 않는 공백(ASCII 160)

CSS decode – CSS_DECODE

AWS WAF CSS 2.x 이스케이프 규칙을 사용하여 인코딩된 문자를 디코딩합니다. syndata.html#characters 이 함수는 디코딩 프로세스에서 최대 2바이트를 사용하므로 일반적으로 인코딩되지 않는 CSS 인코딩을 사용하여 인코딩된 ASCII 문자를 찾는 데 도움이 될 수 있습니다. 또한 백슬래시와 16진수가 아닌 문자의 조합인 회피를 방지하는 데 유용합니다. 예를 들어 javascript의 경우 ja\vascript입니다.

Escape sequences decode – ESCAPE_SEQ_DECODE

AWS WAF ,,,,,,,, \xHH (16진수)\a,,,,\b, \f \n \r \t \v \\ \? \'\", (8진수) 등의 ANSI C 이스케이프 시퀀스를 디코딩합니다. \0000 유효하지 않은 인코딩은 출력에 남아 있습니다.

Hex decode – HEX_DECODE

AWS WAF 16진수 문자열을 이진수로 디코딩합니다.

HTML entity decode – HTML_ENTITY_DECODE

AWS WAF 16진수 형식 또는 10진수 형식으로 표시된 문자를 해당 문자로 바꿉니다. &#xhhhh; &#nnnn;

AWS WAF HTML로 인코딩된 다음 문자를 인코딩되지 않은 문자로 바꿉니다. 이 목록은 소문자 HTML 인코딩을 사용하지만 처리 방식은 예를 들어 대소문자를 구분하지 않으며 동일하게 취급됩니다. &QuOt; "

HTML로 인코딩된 문자	다음으로 바꿈
"	"
&	&
<	<
>	>
또는	줄 바꿈하지 않는 공백, 십진수 160
\n, 10진수 10
	\t, 10진수 9
{ 또는 {	{
|,| 또는		|
} 또는 }	}
!	!
#	#
$	$
&percent; 또는 %	%
'	\
(	(
)	)
* 또는 *	*
+	+
,	,

HTML로 인코딩된 문자	다음으로 바꿈
.	.
/	/
:	:
;	;
=	=
?	?
˜ 또는 ˜	~
−	-
[또는 [	[
\	\\
] 또는]	]
&hat;	^
_ 또는 &underbar;	_
` 또는 `	`

JS decode – JS_DECODE

AWS WAF 이스케이프 시퀀스를 디코딩합니다. JavaScript \uHHHH 코드가 FF01-FF5E의 전폭 ASCII 코드 범위에 있으면 상위 바이트를 사용하여 하위 바이트를 감지하고 조정합니다. 그렇지 않으면 하위 바이트만 사용되고 상위 바이트는 00이 되어 정보가 손실될 수 있습니다.

Lowercase – LOWERCASE

AWS WAF 대문자 (A-Z) 를 소문자 (a-z) 로 변환합니다.

MD5 – MD5

AWS WAF 입력 데이터에서 MD5 해시를 계산합니다. 계산된 해시는 원시 이진 형식입니다.

None – NONE

AWS WAF 텍스트 변환 없이 수신된 웹 요청을 검사합니다.

Normalize path – NORMALIZE_PATH

AWS WAF 입력의 시작 부분에 없는 다중 슬래시, 디렉터리 자체 참조 및 디렉터리 역참조를 제거하여 입력 문자열을 정규화합니다.

Normalize path Windows – NORMALIZE_PATH_WIN

AWS WAF 백슬래시 문자를 슬래시로 변환한 다음 변환을 사용하여 결과 문자열을 처리합니다. NORMALIZE_PATH

Remove nulls – REMOVE_NULLS

AWS WAF 입력에서 모든 NULL 바이트를 제거합니다.

Replace comments – REPLACE_COMMENTS

AWS WAF C 스타일 주석 (/*... */) 이 나올 때마다 단일 공백으로 바꿉니다. 연속으로 여러 번 나타나는 주석은 압축하지 않습니다. 종료되지 않은 주석도 공백(ASCII 0x20)으로 대체합니다. 주석(*/)의 독립형 종료는 변경되지 않습니다.

Replace nulls – REPLACE_NULLS

AWS WAF 입력의 각 NULL 바이트를 공백 문자 (ASCII 0x20) 로 바꿉니다.

SQL hex decode – SQL_HEX_DECODE

AWS WAF SQL 16진수 데이터를 디코딩합니다. 예를 들어, () 를 (0x414243) 로 AWS WAF 디코딩합니다. ABC

URL decode – URL_DECODE

AWS WAF URL로 인코딩된 값을 디코딩합니다.

URL decode Unicode – URL_DECODE_UNI

URL_DECODE와 비슷하지만 Microsoft 고유의 %u 인코딩을 지원합니다. 코드가 FF01-FF5E의 전폭 ASCII 코드 범위에 있으면 상위 바이트를 사용하여 하위 바이트를 감지하고 조정합니다. 그렇지 않으면 하위 바이트만 사용되며 상위 바이트는 0이 됩니다.

UTF8 to Unicode – `UTF8_TO_UNICODE`

AWS WAF 모든 UTF-8 문자 시퀀스를 유니코드로 변환합니다. 이렇게 하면 입력을 정규화하는 데 도움이 되며 영어가 아닌 언어의 오탐과 오탐을 최소화할 수 있습니다.

범위 축소 문

범위 축소 문은 관리형 규칙 그룹 문 또는 속도 기반 문 안에 추가하여 포함 규칙이 평가하는 요청 집합의 범위를 좁힐 수 있는 중첩 가능한 규칙 문입니다. 포함 규칙은 범위 축소 문과 처음 일치하는 요청만 평가합니다.

- 관리형 규칙 그룹 명령문 — 범위 축소 명령문을 관리형 규칙 그룹 문에 추가하는 경우 범위 축소 명령문과 일치하지 않는 모든 요청을 규칙 그룹과 일치하지 않는 것으로 AWS WAF 평가합니다. 범위 축소 문과 일치하는 요청만 규칙 그룹에 대해 평가됩니다. 평가되는 요청 수에 기반하여 요금이 적용되는 관리형 규칙 그룹의 경우 범위 축소 문을 사용하면 비용을 절감할 수 있습니다.

  관리형 규칙 그룹 문에 대한 자세한 내용은 관리형 규칙 그룹 문 섹션을 참조하세요.
- 속도 기반 규칙 문 - 범위 축소 문 속도를 사용하지 않는 속도 기반 규칙 문이 규칙에서 평가하는 모든 요청을 제한합니다. 특정 범주의 요청에 대한 속도만 제어하려면 속도 기반 규칙에 범위 축소 문을 추가하십시오. 예를 들어 특정 지리적 영역의 요청 속도만 추적하고 제어하려면 지리적 일치 문에 해당 리전을 지정하고 이를 속도 기반 규칙에 범위 축소 문으로 추가할 수 있습니다.

  속도 기반 규칙 문에 대한 자세한 내용은 비율 기반 규칙 문 섹션을 참조하세요.

범위 축소 문에서는 중첩 규칙을 사용할 수 있습니다. 사용 가능한 명령문을 보려면 일치 규칙 문 및 논리적 규칙 문 섹션을 참조하세요. 범위 축소 문에 대한 WCU는 그 안에 정의되는 규칙 문에 필요한 WCU입니다. 범위 축소 문 사용에 대한 추가 비용이 없습니다.

일반 규칙에서 명령문을 사용할 때와 같은 방식으로 범위 축소 문을 구성할 수 있습니다. 예를 들어 검사 중인 웹 요청 구성 요소에 텍스트 변환을 적용하고 IP 주소로 사용할 전달된 IP 주소를 지정할 수 있습니다. 이러한 구성은 범위 축소 문에만 적용되며 포함되는 관리형 규칙 그룹 또는 속도 기반 규칙 문에는 상속되지 않습니다.

예를 들어, 범위 축소 문의 쿼리 문자열에 텍스트 변환을 적용하는 경우 범위 축소 문은 변환을 적용한 후 쿼리 문자열을 검사합니다. 요청이 범위 축소 문 기준과 일치하면 AWS WAF 는 범위 축소 문의 변환 없이 원래 상태의 포함 규칙에 웹 요청을 전달합니다. 범위 축소 문을 포함하는 규칙은 자체적으로 텍스트 변환을 적용할 수 있지만 범위 축소 문에서 어떠한 것도 상속하지는 않습니다.

범위 축소 문을 사용하여 포함 규칙 문에 대한 어떠한 요청 검사 구성도 지정할 수 없습니다. 범위 축소 문을 포함 규칙 명령문의 웹 요청 프리프로세서로 사용할 수 없습니다. 범위 축소 문의 유일한 역할은 검사를 위해 포함 규칙 문에 전달되는 요청을 결정하는 것입니다.

집합 또는 규칙 그룹을 참조하는 문

일부 규칙에서는 재사용이 가능하고 귀하 또는 셀러가 웹 ACL 외부에서 관리하는 엔티티를 사용합니다. AWS AWS Marketplace 재사용 가능한 엔터티가 업데이트되면 AWS WAF 은 해당 업데이트를 규칙에 전파합니다. 예를 들어 웹 ACL에서 AWS 관리형 규칙 그룹을 사용하는 경우 규칙 그룹을 AWS 업데이트하면 변경 내용이 웹 ACL에 AWS 전파되어 동작이 업데이트됩니다. 규칙에서 IP set 문을 사용하는 경우 세트를 업데이트할 때 해당 세트를 참조하는 모든 규칙에 변경 내용이 AWS WAF 전파되므로 해당 규칙을 사용하는 모든 웹 ACL이 변경 내용과 함께 유지됩니다. up-to-date

다음은 규칙 문에서 사용할 수 있는 재사용 가능한 엔터티입니다.

- IP 집합 – 자체 IP 집합을 생성하고 관리합니다. 콘솔의 탐색 창에서 이러한 항목에 액세스할 수 있습니다. IP 집합 관리에 대한 자세한 내용은 IP 세트 및 정규식 패턴 세트 AWS WAF 단원을 참조하세요.
- 정규식 일치 집합 – 자체 정규식 일치 집합을 생성 및 관리합니다. 콘솔의 탐색 창에서 이러한 항목에 액세스할 수 있습니다. 정규식 패턴 집합 관리에 대한 자세한 내용은 IP 세트 및 정규식 패턴 세트 AWS WAF 단원을 참조하세요.
- AWS 관리형 규칙 그룹 - 이러한 규칙 그룹을 AWS 관리합니다. 콘솔에서 관리형 규칙 그룹을 웹 ACL에 추가할 때 사용할 수 있습니다. 이에 대한 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록 단원을 참조하세요.
- AWS Marketplace 관리형 규칙 그룹 — AWS Marketplace 셀러가 이러한 규칙 그룹을 관리하므로 셀러가 구독하여 사용할 수 있습니다. 구독을 관리하려면 콘솔의 탐색 창에서 AWS Marketplace을 선택합니다. AWS Marketplace 관리형 규칙 그룹은 웹 ACL에 관리형 규칙 그룹을 추가할 때 나열됩니다. 아직 구독하지 않은 규칙 그룹의 경우 해당 AWS Marketplace 페이지에서도 링크를 찾을 수 있습니다. AWS Marketplace 셀러 관리 규칙 그룹에 대한 자세한 내용은 을 참조하십시오AWS Marketplace 관리형 규칙 그룹.
- 자체 규칙 그룹 – 일반적으로 관리형 규칙 그룹을 통해 사용할 수 없는 일부 동작이 필요한 경우에 자체 규칙 그룹을 관리합니다. 콘솔의 탐색 창에서 이러한 항목에 액세스할 수 있습니다. 자세한 정보는 자체 규칙 그룹 관리을 참조하세요.

참조된 집합 또는 규칙 그룹 삭제

참조된 엔티티를 삭제할 때는 해당 엔티티가 현재 웹 ACL에서 사용되고 있는지 AWS WAF 확인합니다. 사용 AWS WAF 중인 것으로 확인되면 경고를 표시합니다. AWS WAF 웹 ACL에서 엔티티를 참조하고 있는지 여부를 거의 항상 확인할 수 있습니다. 그러나 드문 경우이지만 그렇게 하지 못할 수도 있습니다. 삭제하려는 엔터티가 사용 중인지 확인해야 하는 경우 삭제하기 전에 웹 ACL에서 해당 엔터티를 확인합니다.

일치 규칙 문

일치 문은 웹 요청이나 그 출처를 사용자가 제공하는 기준과 비교합니다. 이 유형의 명령문의 경우 콘텐츠 일치 요청의 특정 구성 요소를 AWS WAF 비교합니다.

일치 문은 중첩할 수 있습니다. 이러한 명령문을 논리적 규칙 문 안에 중첩하여 범위 축소 문에서 사용할 수 있습니다. 논리적 규칙 문에 대한 자세한 내용은 논리적 규칙 문 섹션을 참조하세요. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요.

이 표에서는 규칙에 추가할 수 있는 정규식 일치 문에 대해 설명하고 각각에 대한 웹 ACL 용량 단위(WCU) 사용량을 계산하기 위한 몇 가지 지침을 제공합니다. WCU에 대한 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

일치 문	설명	WCU
지리적 일치	요청의 오리진을 검사하고 오리진의 국가 및 리전에 대해 레이블을 적용합니다.	1
IP 집합 일치	IP 주소 및 주소 범위 집합에 대해 요청을 검사합니다.	대부분의 경우 1입니다. 전달된 IP 주소가 있는 헤더를 사용하도록 명령문을 구성하고 Any의 헤더에 위치를 지정하는 경우 WCU를 4만큼 늘리십시오.
레이블 일치 규칙 문	동일한 웹 ACL 내 다른 규칙에 의해 추가된 레이블에 대한 요청을 검사합니다.	1
정규식 일치 규칙 문	정규식 패턴을 지정된 요청 구성 요소와 비교합니다.	3, 기본 비용으로.

일치 문	설명	WCU
		요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.
정규식 패턴 집합	정규식 패턴을 지정된 요청 구성 요소와 비교합니다.	패턴 집합당 25, 기본 비용으로. 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.
크기 제약 조건	지정된 요청 구성 요소에 대해 크기 제약 조건을 검사합니다.	1, 기본 비용으로. 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

일치 문	설명	WCU
SQL 주입 공격	지정된 요청 구성 요소에서 악성 SQL 코드를 검사합니다.	20, 기본 비용으로. 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.
문자열 일치	문자열을 지정된 요청 구성 요소와 비교합니다.	기본 비용은 1~10으로, 문자열 일치 유형에 따라 달라집니다. 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.
XSS 스크립팅 공격	지정된 요청 구성 요소에서 사이트 간 스크립팅 공격을 검사합니다.	40, 기본 비용으로. 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

지리적 일치 규칙 문

지리적 또는 지역 일치 문을 사용하여 오리진 국가 및 리전을 기반으로 웹 요청을 관리할 수 있습니다. 지역 일치 문은 웹 요청에 오리진 국가 및 리전을 나타내는 레이블을 추가합니다. 명령문 기준이 요청과 일치하는지 여부에 관계없이 이러한 레이블을 추가합니다. 또한 지역 일치 문은 요청의 오리진을 기준으로 일치를 수행합니다.

지역 일치 문 사용 방법

다음과 같이 국가 또는 리전 일치에 지역 일치 문을 사용할 수 있습니다.

- 국가 - 지역 일치 규칙을 단독으로 사용하면 오리진 국가만을 기준으로 하여 요청을 관리할 수 있습니다. 규칙 문을 국가 코드와 비교하여 일치시킵니다. 오리진 국가 레이블과 일치하는 레이블 일치 규칙을 사용하여 지역 일치 규칙을 따를 수도 있습니다.
- 리전 - 지역 일치 규칙 다음에 레이블 일치 규칙을 사용하여 오리진 리전을 기준으로 요청을 관리합니다. 지역 일치 규칙만으로는 리전 코드와 일치시킬 수 없습니다.

레이블 일치 규칙 사용에 대한 자세한 내용은 레이블 일치 규칙 문 및 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.

지역 일치 문 작동 방식

geo match 문을 사용하여 각 웹 요청을 다음과 같이 AWS WAF 관리합니다.

1. 요청의 국가 및 지역 코드를 AWS WAF 결정합니다. — IP 주소를 기반으로 요청의 국가 및 지역을 결정합니다. 기본적으로 는 웹 요청 출처의 IP 주소를 AWS WAF 사용합니다. 예를 들어, 규칙 설명 설정에서 전달된 IP 구성을 AWS WAF 활성화하여 대체 요청 헤더의 IP 주소를 사용하도록 지시할 수 있습니다. `X-Forwarded-For`

   AWS WAF MaxMind GeoIP 데이터베이스를 사용하여 요청 위치를 결정합니다. MaxMind 국가 및 IP 유형과 같은 요인에 따라 정확도가 달라지지만 국가 수준에서 매우 높은 데이터 정확도를 보고합니다. 에 대한 MaxMind 자세한 내용은 MaxMind IP 지리적 위치를 참조하십시오. GeoIP 데이터가 잘못되었다고 생각되면 GeoIP2 데이터 MaxMind 수정에서 Maxmind에 수정 요청을 제출할 수 있습니다.

   AWS WAF 국제 표준화 기구 (ISO) 3166 표준의 알파-2 국가 및 지역 코드를 사용합니다. 다음 위치에서 코드를 찾을 수 있습니다.
   - ISO 웹사이트의 ISO 온라인 브라우징 플랫폼(OBP)에서 국가 코드를 검색할 수 있습니다.
   - 위키백과에서는 ISO 3166-2에 국가 코드가 나열되어 있습니다.

국가의 리전 코드는 URL `https://en.wikipedia.org/wiki/ISO_3166-2:`*`<ISO country code>`*에 나열되어 있습니다. 예를 들어 미국의 리전은 ISO 3166-2:US이고 우크라이나의 경우 ISO 3166-2:UA입니다.

2. 요청에 추가할 국가 레이블 및 리전 레이블 결정 - 레이블은 지역 일치 문에서 원본 IP를 사용하는지 아니면 전달된 IP 구성을 사용하는지를 나타냅니다.

   - 오리진 IP

     국가 레이블은 `awswaf:clientip:geo:country:`*`<ISO country code>`*입니다. 예를 들어, 미국의 경우 `awswaf:clientip:geo:country:US`입니다.

     리전 라벨은 `awswaf:clientip:geo:region:`*`<ISO country code>`*`-`*`<ISO region code>`*입니다. 예를 들어, 미국의 오리건인 경우 `awswaf:clientip:geo:region:US-OR`입니다.

   - 전달된 IP

     국가 레이블은 `awswaf:forwardedip:geo:country:`*`<ISO country code>`*입니다. 예를 들어, 미국의 경우 `awswaf:forwardedip:geo:country:US`입니다.

     리전 라벨은 `awswaf:forwardedip:geo:region:`*`<ISO country code>`*`-`*`<ISO region code>`*입니다. 예를 들어, 미국의 오리건인 경우 `awswaf:forwardedip:geo:region:US-OR`입니다.

   요청의 지정된 IP 주소에 해당 국가 또는 리전 코드를 사용할 수 없는 경우 AWS WAF 는 레이블에서 값 대신 `XX`를 사용합니다. 예를 들어, 레이블 `awswaf:clientip:geo:country:XX`는 국가 코드를 사용할 수 없는 클라이언트 IP용이고, `awswaf:forwardedip:geo:region:US-XX`는 국가는 미국이지만 리전 코드를 사용할 수 없는 전달된 IP용입니다.

3. 규칙 기준에 따라 요청 국가 코드 평가

지역 일치 문은 일치하는 항목을 찾았는지 여부와 관계없이 검사하는 모든 요청에 국가 및 리전 레이블을 추가합니다.

> **Note**
>
> AWS WAF 규칙의 웹 요청 평가 끝에 레이블을 추가합니다. 따라서 지역 일치 명령문의 레이블에 사용하는 모든 레이블 일치는 지역 일치 문이 포함된 규칙과는 별도의 규칙에 정의되어야 합니다.

리전 값만 검사하려는 경우 Count 작업과 단일 국가 코드 일치, 리전 레이블에 대한 레이블 일치 규칙을 포함하는 지역 일치 규칙을 작성할 수 있습니다. 이 접근 방식에서도 지역 일치 규칙을 평가하려면 국가 코드를 입력해야 합니다. 사이트에 대한 트래픽 소스가 될 것 같지 않은 국가를 지정하여 로깅과 계수 지표를 줄일 수 있습니다.

CloudFront 배포 및 CloudFront 지역 제한 기능

CloudFront 배포의 경우 CloudFront 지역 제한 기능을 사용하는 경우 이 기능은 차단된 요청을 전달하지 않는다는 점에 유의하세요. AWS WAF허용된 요청을 로 전달합니다. AWS WAF지역 및 지정할 수 있는 기타 기준에 따라 요청을 차단하려면 지역 일치 명령문을 사용하고 AWS WAF 지역 제한 기능은 사용하지 마세요. AWS WAF CloudFront

지역 일치 문 특성

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU – 1WCU.

설정 - 이 명령문은 다음 설정을 사용합니다.

- 국가 코드 — 지역 일치 여부를 확인하기 위해 비교할 국가 코드 배열. 이러한 코드는 ISO 3166 국제 표준의 alpha-2 국가 ISO 코드에서 나온 2자리 국가 코드(예: `["US","CN"]`)여야 합니다.
- (선택 사항) 전달된 IP 구성 — 기본적으로 웹 요청 출처의 IP 주소를 AWS WAF 사용하여 원산지를 결정합니다. 또는 HTTP 헤더에 전달된 IP를 대신 사용하도록 규칙을 구성할 수도 있습니다. `X-Forwarded-For` AWS WAF 헤더의 첫 번째 IP 주소를 사용합니다. 이 구성을 사용하면 헤더에 잘못된 형식의 IP 주소가 있는 웹 요청에 적용할 폴백 동작도 지정할 수 있습니다. 폴백 동작은 요청에 대한 일치 결과를 일치하거나 일치하지 않음으로 설정합니다. 자세한 정보는 전달된 IP 주소을 참조하세요.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 요청 옵션에서 출처 국가를 선택합니다.
- API — GeoMatchStatement

예제

지리적 일치 문을 사용하여 특정 국가 또는 리전의 요청을 관리할 수 있습니다. 예를 들어 특정 국가를 차단하되 해당 국가의 특정 IP 주소 집합에서 요청을 허용하려면 유사 코드에 나와 있는 대로 작업을 Block로 설정하고 다음과 같은 중첩된 문을 사용하여 규칙을 생성할 수 있습니다.

- AND 명령문
  - 차단하려는 국가를 나열하는 지역 일치 문
  - NOT 명령문
    - 다음을 통해 허용하려는 IP 주소를 지정하는 IP 집합 문

또는 특정 국가의 일부 리전을 차단하면서도 해당 국가의 다른 리전에서 들어오는 요청은 계속 허용하려는 경우 먼저 작업을 Count로 설정한 상태로 지역 일치 규칙을 정의할 수 있습니다. 그런 다음 추가된 지역 일치 레이블과 일치하는 레이블 일치 규칙을 정의하고 필요에 따라 요청을 처리합니다.

다음 의사 코드는 이 접근 방식의 예를 설명합니다.

1. 차단하려는 리전이 있지만 작업이 계산으로 설정된 국가를 나열하는 지역 일치 문. 이 문은 일치 상태에 관계없이 모든 웹 요청에 레이블을 지정하고 관심 국가의 개수 지표도 제공합니다.
2. 차단 작업을 포함하는 AND 문
   - 차단하려는 국가에 대해 레이블을 지정하는 레이블 일치 문
   - NOT 명령문
     - 허용하려는 국가에 대해 레이블을 지정하는 레이블 일치 문

다음 JSON 목록에는 이전 의사 코드에 설명된 두 규칙의 구현이 나와 있습니다. 이들 규칙은 오레곤 및 워싱턴에서 들어오는 트래픽을 제외하고 미국에서 들어오는 모든 트래픽을 차단합니다. 지역 일치 문은 검사하는 모든 요청에 국가 및 리전 레이블을 추가합니다. 레이블 일치 규칙은 지역 일치 규칙 이후에 실행되므로 지역 일치 규칙이 방금 추가한 국가 및 리전 레이블과 일치시킬 수 있습니다. 지역 일치 문은 전달된 IP 주소를 사용하므로 레이블 일치에서 전달된 IP 레이블도 지정합니다.

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
   "Statement": {
     "GeoMatchStatement": {
       "CountryCodes": [
         "US"
       ],
       "ForwardedIPConfig": {
           "HeaderName": "X-Forwarded-For",
           "FallbackBehavior": "MATCH"
       }
     }
   },
```

```
    "Action": {
      "Count": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "geoMatchForLabels"
    }
},
{
    "Name": "blockUSButNotOROrWA",
    "Priority": 11,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:forwardedip:geo:country:US"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                 "OrStatement": {
                   "Statements": [
                     {
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-OR"
                        }
                     },
                     {
                        "LabelMatchStatement": {
                          "Scope": "LABEL",
                          "Key": "awswaf:forwardedip:geo:region:US-WA"
                        }
                     }
                   ]
                 }
              }
            }
          }
        ]
```

```
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "blockUSButNotOROrWA"
    }
}
```

또 다른 예로 특정 국가 또는 리전의 사용자에게 리소스를 우선적으로 할당하려면, 속도 기반 규칙에 지역 일치 조건을 결합하면 됩니다. 사용자를 차별화하는 데 사용하는 각 지역 일치 또는 레이블 일치 문에 대해 서로 다른 속도 기반 문을 생성합니다. 선호하는 국가 또는 리전의 사용자에게는 요청률 한도를 더 높게 설정하고, 기타 사용자에게는 요청률 한도를 더 낮게 설정합니다.

다음 JSON 목록은 지역 일치 규칙과 미국에서 들어오는 트래픽 속도를 제한하는 속도 기반 규칙을 보여줍니다. 이러한 규칙을 사용하면 오리건 주에서 들어오는 트래픽이 미국 내 다른 리전에서 들어오는 트래픽보다 더 높은 속도로 유입될 수 있습니다.

```
{
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
```

```
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:clientip:geo:region:US-OR"
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
  }
},
{
  "Name": "rateLimitUSNotOR",
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:clientip:geo:country:US"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:clientip:geo:region:US-OR"
                  }
```

```
                }
              }
            }
          ]
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

IP 집합 일치 규칙 문

IP 집합 일치 문은 IP 주소 및 주소 범위의 집합에 대한 웹 요청의 IP 주소를 검사합니다. 요청이 시작된 IP 주소를 기반으로 웹 요청을 허용하거나 차단하려면 이 옵션을 사용합니다. 기본적으로 AWS WAF는 웹 요청 오리진의 IP 주소를 사용하지만 대신에 `X-Forwarded-For`와 같은 HTTP 헤더를 사용하도록 규칙을 구성할 수 있습니다.

AWS WAF 를 제외한 모든 IPv4 및 IPv6 CIDR 범위를 지원합니다. `/0` CIDR 표기법에 대한 자세한 내용은 클래스 없는 도메인 간 라우팅에 대한 Wikipedia 항목을 참조하세요. IP 집합에서는 최대 10,000개의 IP 주소 또는 IP 주소 범위를 확인할 수 있습니다.

> **Note**
>
> 각 IP 집합 일치 규칙은 규칙과 관계 없이 생성 및 유지 관리하는 IP 집합을 참조합니다. 단일 IP 세트를 여러 규칙에 사용할 수 있으며, 참조된 세트를 업데이트하면 해당 세트를 참조하는 모든 규칙이 AWS WAF 자동으로 업데이트됩니다.
>
> IP 집합의 생성 및 관리 방법에 대한 자세한 내용은 IP 집합 생성 및 관리 섹션을 참조하세요.

규칙 그룹 또는 웹 ACL에서 규칙을 추가하거나 업데이트할 때 IP set(IP 집합) 옵션을 선택하고 사용할 IP 집합의 이름을 선택합니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU - 대부분의 경우 1WCU입니다. 전달된 IP 주소를 사용하도록 문을 구성하고 ANY의 위치를 지정하는 경우 WCU 사용을 4만큼 늘리세요.

이 문은 다음 설정을 사용합니다.

- IP 집합 사양 – 목록에서 사용할 IP 집합을 선택하거나 새 IP 집합을 생성합니다.
- (선택 사항) 전달된 IP 구성 - 요청 오리진 대신 사용할 대체 전달 IP 헤더 이름입니다. 헤더의 첫 번째 주소, 마지막 주소 또는 임의 주소와 일치시킬지 여부를 지정합니다. 지정된 헤더에 잘못된 형식의 IP 주소가 있는 웹 요청에 적용할 폴백 동작도 지정할 수 있습니다. 폴백 동작은 요청에 대한 일치 결과를 일치하거나 일치하지 않음으로 설정합니다. 자세한 정보는 전달된 IP 주소을 참조하세요.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 요청 옵션에서 출처 IP 주소를 선택합니다.
- 콘솔의 자체 규칙 및 규칙 그룹 추가 페이지 - IP 집합 옵션을 선택합니다.
- API — IP SetReferenceStatement

레이블 일치 규칙 문

레이블 일치 문은 문자열 사양을 기준으로 웹 요청의 레이블을 검사합니다. 규칙에서 검사할 수 있는 레이블은 동일한 웹 ACL 평가의 다른 규칙에 의해 웹 요청에 이미 추가된 레이블입니다.

레이블은 웹 ACL 평가 외에는 유지되지 않지만 콘솔에서 레이블 지표에 액세스할 수 CloudWatch 있으며 모든 웹 ACL에 대한 레이블 정보 요약을 볼 수 있습니다. AWS WAF 자세한 내용은 레이블 지표 및 차원 및 모니터링 및 조정 섹션을 참조하세요. 로그에서 레이블을 확인할 수도 있습니다. 자세한 내용은 로그 필드을 참조하세요.

> **Note**
>
> 레이블 일치 문은 웹 ACL에서 이전에 평가된 규칙의 레이블만 볼 수 있습니다. 웹 ACL의 규칙 및 규칙 그룹을 AWS WAF 평가하는 방법에 대한 자세한 내용은 을 참조하십시오. 웹 ACL의 규칙 및 규칙 그룹 처리 순서

레이블 추가 및 일치에 대한 자세한 정보는 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCUs – 1WCU

이 문은 다음 설정을 사용합니다.

- 범위 일치 — 레이블 이름 및 필요에 따라 이전 네임스페이스 및 접두사와 일치시키려면 이 값을 레이블로 설정합니다. 일부 또는 모든 네임스페이스 사양 그리고 필요에 따라 이전 접두사와 일치시키려면 이 값을 네임스페이스로 설정합니다.
- 키 — 일치시키려는 문자열입니다. 네임스페이스 일치 범위를 지정하는 경우 네임스페이스와 접두사(필요 시) 및 콜론 구분 기호만 지정하면 됩니다. 레이블 일치 범위를 지정하는 경우 레이블 이름이 포함해야 하며 필요 시 이전 네임스페이스와 접두사를 포함할 수 있습니다.

이러한 설정에 대한 자세한 내용은 AWS WAF 레이블과 일치하는 규칙 및 AWS WAF 라벨 매칭 예제 섹션을 참조하세요.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 - 요청 옵션에서 레이블 있음을 선택합니다.
- API — LabelMatchStatement

정규식 일치 규칙 문

regex match 문은 요청 구성 요소를 단일 정규 표현식 (regex) 과 AWS WAF 일치시키도록 지시합니다. 지정하는 정규식과 요청 구성 요소가 일치하면 웹 요청이 해당 문을 일치시킵니다.

이 명령문 유형은 수학 논리를 사용하여 일치 기준을 결합하려는 경우 정규식 패턴 집합 일치 규칙 문에 대한 좋은 대안입니다. 예를 들어 요청 구성 요소를 일부 정규식 패턴과 일치시키고 다른 패턴과는 일치되지 않도록 하려는 경우 AND 규칙 문 및 NOT 규칙 문를 사용하여 정규식 일치 문을 결합할 수 있습니다.

AWS WAF 일부 예외를 제외하고 PCRE 라이브러리에서 사용하는 패턴 구문을 지원합니다. `libpcre` 이 라이브러리는 PCRE - Perl 호환 정규식에 문서화되어 있습니다. AWS WAF 지원에 대한 자세한 내용은 을 참조하십시오정규 표현식 패턴 매칭 AWS WAF.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU - 3WCU(기본 비용). 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

이 문은 웹 요청 구성 요소에서 작동하며 작동을 위해선 다음과 같은 요청 구성 요소 설정이 필요합니다.

- 요청 구성 요소 – 검사할 웹 요청 부분(예: 쿼리 문자열 또는 본문).

> **Warning**
>
> 요청 구성 요소 본문, JSON 본문, 헤더 또는 쿠키를 검사하는 경우 AWS WAF 검사할 수 있는 콘텐츠 양에 대한 제한 사항을 읽어보세요. 에서 크기 초과 요청 구성 요소 처리 AWS WAF

  웹 요청 구성 요소에 대한 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.
- 선택적 텍스트 변환 — 요청 구성 요소를 검사하기 전에 요청 구성 요소에 대해 AWS WAF 수행하려는 변환. 예를 들어, 소문자로 변환하거나 공백을 정규화할 수 있습니다. 변형을 두 개 이상 지정하는 경우, 나열된 순서대로 AWS WAF 처리합니다. 자세한 내용은 텍스트 변환 옵션을 참조하세요.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 - 일치 유형의 경우 정규식과 일치를 선택합니다.
- API — RegexMatchStatement

정규식 패턴 집합 일치 규칙 문

정규식 패턴 집합 일치는 정규식 패턴 집합 내에서 지정한 정규 표현식 패턴에 대해 지정한 웹 요청 부분을 검사합니다.

AWS WAF 일부 예외를 `libpcre` 제외하고 PCRE 라이브러리에서 사용하는 패턴 구문을 지원합니다. 이 라이브러리는 PCRE - Perl 호환 정규식에 문서화되어 있습니다. AWS WAF 지원에 대한 자세한 내용은 을 참조하십시오정규 표현식 패턴 매칭 AWS WAF.

> **Note**
>
> 각 정규식 패턴 집합 일치 규칙은 규칙과 관계 없이 생성 및 유지 관리하는 정규식 패턴 집합을 참조합니다. 여러 규칙에서 단일 정규식 패턴 세트를 사용할 수 있으며, 참조된 세트를 업데이트하면 해당 세트를 참조하는 모든 규칙이 AWS WAF 자동으로 업데이트됩니다.
> 정규식 패턴 집합을 생성 및 관리하는 방법은 정규식 패턴 집합 생성 및 관리 단원을 참조하세요.

regex 패턴 집합 일치 명령문은 선택한 요청 구성 요소 내의 집합에서 패턴을 AWS WAF 검색하도록 지시합니다. 요청 구성 요소가 집합의 패턴 중 하나와 일치하는 경우 웹 요청은 패턴 집합 규칙 문과 일치하게 됩니다.

로직을 사용하여 정규식 패턴 일치를 결합하려는 경우(예: 일부 정규식과 일치시키고 다른 정규식과는 일치하지 않도록 하려는 경우) 정규식 일치 규칙 문의 사용을 고려해 보십시오.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU - 25WCU(기본 비용). 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

이 문은 웹 요청 구성 요소에서 작동하며 작동을 위해선 다음과 같은 요청 구성 요소 설정이 필요합니다.

- 요청 구성 요소 – 검사할 웹 요청 부분(예: 쿼리 문자열 또는 본문).

  > **Warning**
  >
  > 요청 구성 요소 본문, JSON 본문, 헤더 또는 쿠키를 검사하는 경우 검사할 수 있는 콘텐츠 양에 대한 제한 사항을 읽어보세요. AWS WAF 에서 크기 초과 요청 구성 요소 처리 AWS WAF

  웹 요청 구성 요소에 대한 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.
- 선택적 텍스트 변환 — 요청 구성 요소를 검사하기 전에 요청 구성 요소에 대해 AWS WAF 수행하려는 변환. 예를 들어, 소문자로 변환하거나 공백을 정규화할 수 있습니다. 변형을 두 개 이상 지정하는 경우, 나열된 순서대로 AWS WAF 처리합니다. 자세한 내용은 텍스트 변환 옵션을 참조하세요.

이 문에는 다음 설정이 필요합니다.

- 정규식 패턴 집합 사양 - 사용할 정규식 패턴 집합을 선택하거나 새 정규식 패턴 집합을 생성합니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 - 일치 유형에서 문자열 일치 조건 > 정규 표현식 집합에서 패턴 일치를 선택합니다.
- API — RegexPatternSetReferenceStatement

크기 제약 조건 규칙 문

크기 제한 문은 웹 요청 구성 요소의 바이트 수를 사용자가 제공하는 바이트 수와 비교하고 비교 기준에 따라 일치시킵니다. 비교 기준은 보다 큼(>) 또는 보다 작음(<) 과 같은 연산자입니다. 예를 들어 크기가 100바이트보다 큰 쿼리 문자열이 있는 요청을 일치시킬 수 있습니다.

> **Note**
>
> 이 명령문은 웹 요청 구성 요소의 크기만 검사합니다. 구성 요소의 콘텐츠는 검사하지 않습니다.

URI 경로를 검사하면 경로에 있는 모든 /가 1자로 계산됩니다. 예컨대, URI 경로 `/logo.jpg`는 9자 길이입니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU - 1WCU(기본 비용). 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

이 문은 웹 요청 구성 요소에서 작동하며 작동을 위해선 다음과 같은 요청 구성 요소 설정이 필요합니다.

- 요청 구성 요소 – 검사할 웹 요청 부분(예: 쿼리 문자열 또는 본문). 웹 요청 구성 요소에 대한 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.

  크기 제약 문은 변환이 적용된 후 구성 요소의 크기만 검사합니다. 구성 요소의 내용은 검사하지 않습니다.
- 선택적 텍스트 변환 — 요청 구성 요소의 크기를 검사하기 전에 해당 구성 요소에서 수행하려는 AWS WAF 변환. 예를 들어, 공백을 압축하거나 HTML 엔티티를 디코딩할 수 있습니다. 변형을 두 개 이상 지정하는 경우, 나열된 순서대로 AWS WAF 처리합니다. 자세한 내용은 텍스트 변환 옵션을 참조하세요.

또한 이 문에는 다음 설정이 필요합니다.

- 크기 일치 조건 - 선택한 요청 구성 요소에 제공하는 크기를 비교하는 데 사용할 수치 비교 연산자를 나타냅니다. 목록에서 연산자를 선택합니다.

- 크기 – 비교에 사용할 크기 설정(바이트)입니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 일치 유형의 크기 일치 조건에서 사용할 조건을 선택합니다.
- API — SizeConstraintStatement

SQL 주입 공격 규칙 문

SQL 명령어 삽입 규칙 문은 악성 SQL 코드를 검사합니다. 공격자는 웹 요청에 악성 SQL 코드를 삽입하여 데이터베이스를 수정하거나 데이터베이스에서 데이터를 추출하는 등의 작업을 수행합니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU - 기본 비용은 규칙 문의 민감도 수준 설정에 따라 달라집니다(Low 비용 20, High 비용 30).

요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

이 문은 웹 요청 구성 요소에서 작동하며 작동을 위해선 다음과 같은 요청 구성 요소 설정이 필요합니다.

- 요청 구성 요소 – 검사할 웹 요청 부분(예: 쿼리 문자열 또는 본문).

> **Warning**
>
> 요청 구성 요소 본문, JSON 본문, 헤더 또는 쿠키를 검사하는 경우 AWS WAF 검사할 수 있는 콘텐츠 양에 대한 제한 사항을 읽어보세요. 에서 크기 초과 요청 구성 요소 처리 AWS WAF

  웹 요청 구성 요소에 대한 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.
- 선택적 텍스트 변환 — 요청 구성 요소를 검사하기 전에 요청 구성 요소에 대해 AWS WAF 수행하려는 변환. 예를 들어, 소문자로 변환하거나 공백을 정규화할 수 있습니다. 변형을 두 개 이상 지정하는 경우, 나열된 순서대로 AWS WAF 처리합니다. 자세한 내용은 텍스트 변환 옵션을 참조하세요.

또한 이 문에는 다음 설정이 필요합니다.

- 민감도 수준 - 이 설정은 SQL 명령어 삽입 일치 조건의 민감도를 조정합니다. 옵션은 LOW 및 HIGH입니다. 기본 설정은 LOW입니다.

  이 HIGH 설정은 더 많은 SQL 명령어 삽입 공격을 탐지하므로 이 설정은 권장 설정입니다. 이 설정은 민감도가 더 높기 때문에 특히 웹 요청에 일반적으로 비정상적인 문자열이 포함되어 있는 경우 거짓 긍정이 더 많이 발생합니다. 웹 ACL 테스트 및 조정 중에 거짓 긍정을 완화하기 위한 노력이 더 많이 필요할 수 있습니다. 자세한 내용은 AWS WAF 보호 기능 테스트 및 조정을 참조하세요.

  설정이 낮을수록 덜 엄격한 SQL 명령어 삽입 탐지가 제공되므로 거짓 긍정도 그만큼 감소합니다. LOW는 SQL 명령어 삽입 공격에 대한 다른 보호 기능이 있거나 거짓 긍정에 대한 허용 오차가 낮은 리소스에 더 적합합니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 일치 유형에서 공격 일치 조건 > SQL 명령어 삽입 공격 포함을 선택합니다.
- API — SqliMatchStatement

문자열 일치 규칙 문

문자열 일치 명령문은 요청에서 AWS WAF 검색하려는 문자열, 요청의 검색 위치 및 방법을 나타냅니다. 예를 들어 요청의 쿼리 문자열의 시작 부분에서 특정 문자열을 찾거나 요청의 `User-agent` 헤더와 정확히 일치하는 문자열을 찾을 수 있습니다. 일반적으로 문자열은 인쇄 가능한 ASCII 문자로 구성되지만, 16진수 0x00에서 0xFF(10진수 0~255) 사이의 어떤 문자든지 사용할 수 있습니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU – 기본 비용은 사용하는 일치 유형에 따라 다릅니다.

- 정확히 문자열과 일치 – 2
- 문자열로 시작 – 2
- 문자열로 끝 – 2
- 문자열 포함 – 10
- 단어 포함 – 10

요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

이 문은 웹 요청 구성 요소에서 작동하며 작동을 위해선 다음과 같은 요청 구성 요소 설정이 필요합니다.

- 요청 구성 요소 – 검사할 웹 요청 부분(예: 쿼리 문자열 또는 본문).

  > **Warning**
  >
  > 요청 구성 요소 본문, JSON 본문, 헤더 또는 쿠키를 검사하는 경우 AWS WAF 검사할 수 있는 콘텐츠 양에 대한 제한 사항을 읽어보세요. 에서 크기 초과 요청 구성 요소 처리 AWS WAF

  웹 요청 구성 요소에 대한 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.
- 선택적 텍스트 변환 — 요청 구성 요소를 검사하기 전에 요청 구성 요소에 대해 AWS WAF 수행하려는 변환. 예를 들어, 소문자로 변환하거나 공백을 정규화할 수 있습니다. 변형을 두 개 이상 지정하는 경우, 나열된 순서대로 AWS WAF 처리합니다. 자세한 내용은 텍스트 변환 옵션을 참조하세요.

또한 이 문에는 다음 설정이 필요합니다.

- 일치시킬 문자열 - 지정된 요청 구성 요소와 AWS WAF 비교하려는 문자열입니다. 일반적으로 문자열은 인쇄 가능한 ASCII 문자로 구성되지만, 16진수 0x00에서 0xFF(10진수 0~255) 사이의 어떤 문자든지 사용할 수 있습니다.
- 문자열 일치 조건 - AWS WAF 수행하려는 검색 유형을 나타냅니다.
  - 정확히 문자열과 일치) – 문자열과 요청 구성 요소의 값이 동일합니다.
  - 문자열로 시작 – 문자열이 요청 구성 요소의 시작 부분에 나타납니다.
  - 문자열로 끝 – 문자열이 요청 구성 요소의 끝에 나타납니다.
  - 문자열 포함 – 문자열이 요청 구성 요소의 아무 곳이나 나타납니다.
  - 단어 포함 – 지정한 문자열은 요청 구성 요소에 나타나야 합니다.

    이 옵션의 경우 지정하는 문자열에는 영숫자 또는 밑줄(A-Z, a-z, 0-9 또는 _)만 포함해야 합니다.

    요청이 일치하려면 다음 중 하나가 true여야 합니다.
    - 문자열은 헤더의 값 같은 요청 구성 요소의 값과 정확히 일치합니다.
    - 문자열이 요청 구성 요소의 시작 부분에 있고 그 뒤에 영숫자 또는 밑줄(_)을 제외한 다른 문자(예: `BadBot;`)가 있습니다.

- 문자열이 요청 구성 요소의 끝에 있고 그 앞에 영숫자 또는 밑줄(_)을 제외한 다른 문자(예: `;BadBot`)가 있습니다.
- 문자열이 요청 구성 요소의 중간에 있고 그 앞과 뒤에 영숫자 또는 밑줄(_)을 제외한 다른 문자(예: `-BadBot;`)이 있습니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 일치 유형에서 문자열 일치 조건을 선택한 다음, 일치시킬 문자열을 입력합니다.
- API — ByteMatchStatement

교차 사이트 스크립팅 공격 규칙 문

XSS(교차 사이트 스크립팅) 공격 문은 웹 요청 구성 요소의 악성 스크립트를 검사합니다. XSS 공격에서 공격자는 악성 클라이언트 사이트 스크립트를 다른 합법적 웹 브라우저에 삽입하는 수단으로 양성 웹 사이트의 취약점을 이용합니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU - 40WCU(기본 비용). 요청 구성 요소 모든 쿼리 파라미터를 사용하는 경우 10WCU를 추가하십시오. 요청 구성 요소 JSON 본문을 사용하는 경우 기본 비용 WCU를 두 배로 늘리십시오. 적용하는 각 텍스트 변환에 대해 10WCU를 추가하십시오.

이 문은 웹 요청 구성 요소에서 작동하며 작동을 위해선 다음과 같은 요청 구성 요소 설정이 필요합니다.

- 요청 구성 요소 – 검사할 웹 요청 부분(예: 쿼리 문자열 또는 본문).

> **Warning**
>
> 요청 구성 요소 본문, JSON 본문, 헤더 또는 쿠키를 검사하는 경우 AWS WAF 검사할 수 있는 콘텐츠 양에 대한 제한 사항을 읽어보세요. 에서 크기 초과 요청 구성 요소 처리 AWS WAF

  웹 요청 구성 요소에 대한 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.
- 선택적 텍스트 변환 — 요청 구성 요소를 검사하기 전에 요청 구성 요소에 대해 AWS WAF 수행하려는 변환. 예를 들어, 소문자로 변환하거나 공백을 정규화할 수 있습니다. 변형을 두 개 이상 지정하는 경우, 나열된 순서대로 AWS WAF 처리합니다. 자세한 내용은 텍스트 변환 옵션을 참조하세요.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 일치 유형에서 공격 일치 조건 > XSS 주입 공격 포함을 선택합니다.
- API — XssMatchStatement

논리적 규칙 문

논리적 규칙 문을 사용하여 다른 문을 결합하거나 결과를 무효화할 수 있습니다. 모든 논리적 규칙 문은 적어도 하나의 중첩 문을 사용합니다.

규칙 문 결과를 논리적으로 결합하거나 무효화하려면 해당 문을 논리적 규칙 문 아래에 중첩해야 합니다.

논리적 규칙 문을 중첩할 수 있습니다. 이를 다른 논리적 규칙 문 안에 중첩하여 범위 축소 문에서 사용할 수 있습니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요.

> **Note**
>
> 콘솔의 시각적 편집기는 여러 요구 사항에 대해 작동하는 한 수준의 규칙 문 중첩을 지원합니다. 더 많은 수준을 중첩하려면 콘솔에서 규칙의 JSON 표현을 편집하거나 API를 사용합니다.

이 표에서는 논리적 규칙 문에 대해 설명하고 각각에 대한 웹 ACL 용량 단위(WCU) 사용량을 계산하기 위한 몇 가지 지침을 제공합니다. WCU에 대한 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

논리적 문	설명	WCU
AND 로직	중첩된 문을 AND 로직과 결합합니다.	중첩 문 기반
NOT 로직	중첩된 문의 결과를 무효화합니다.	중첩 문 기반
OR 로직	중첩된 문을 OR 로직과 결합합니다.	중첩 문 기반

AND 규칙 문

AND 규칙 문은 중첩된 문을 논리적 AND 연산과 결합하므로 AND 문이 일치하도록 모든 중첩된 문이 일치해야 합니다. 여기에는 두 개 이상의 중첩된 명령문이 필요합니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU – 중첩된 문에 따라 다릅니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 요청의 경우에서 모든 문과 일치(AND)를 선택한 다음, 중첩된 문을 입력합니다.
- API — AndStatement

예제

다음 목록은 AND 및 NOT 논리 규칙 문을 사용하여 SQL 명령어 삽입 공격 문에 대한 일치 항목에서 거짓 긍정을 제거하는 방법을 보여줍니다. 이 예제의 경우 단일 바이트 일치 문을 작성하여 거짓 긍정을 초래하는 요청을 일치시킬 수 있다고 가정해 보겠습니다.

AND 문은 바이트 일치 문과 일치하지 않으면서 SQL 명령어 삽입 공격 문과 일치하는 요청과 일치합니다.

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "SearchString": "string identifying a false positive",
                    "FieldToMatch": {
                      "Body": {
                        "OversizeHandling": "MATCH"
                      }
                    },
                    "TextTransformations": [
                      {
                        "Priority": 0,
```

```
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "CONTAINS"
              }
            }
          }
        },
        {
          "SqliMatchStatement": {
            "FieldToMatch": {
              "Body": {
                "OversizeHandling": "MATCH"
              }
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "SQLiExcludeFalsePositives"
  }
}
```

콘솔 규칙 시각 편집기를 사용하면 비논리문 또는 NOT 문을 OR 또는 AND 문 아래에 중첩할 수 있습니다. NOT 문의 중첩은 이전 예제에 나와 있습니다.

콘솔 규칙 시각적 편집기를 사용하면 대부분의 중첩이 가능한 명령문을 이전 예제와 같은 논리적 규칙 문 아래에 중첩할 수 있습니다. 시각적 편집기를 사용하여 OR 또는 AND 문을 중첩할 수는 없습니다. 이러한 유형의 중첩을 구성하려면 규칙 문을 JSON으로 제공해야 합니다. 예를 들어, 다음 JSON 규칙 목록에는 AND 문 내에 중첩된 OR 문이 포함됩니다.

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
```

```
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

NOT 규칙 문

NOT 규칙 문은 중첩된 단일 명령문의 결과를 논리적으로 무효화하므로 중첩된 문이 매치할 NOT 문과 일치하지 않아야 하며, 그 반대의 경우도 마찬가지입니다. 이를 위해서는 하나의 중첩된 문이 필요합니다.

예를 들어 특정 국가가 출처가 아닌 요청을 차단하려면 작업을 차단으로 설정하여 NOT 문을 생성하고 국가를 지정하는 지역 일치 문을 중첩합니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU – 중첩된 문에 따라 다릅니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 요청의 경우에서 문과 일치하지 않음(NOT)을 선택한 다음, 중첩된 문을 입력합니다.
- API — NotStatement

OR 규칙 문

OR 규칙 문은 중첩된 문과 OR 로직을 결합하므로 중첩된 문 중 하나가 매치할 OR 문과 일치해야 합니다. 여기에는 두 개 이상의 중첩된 명령문이 필요합니다.

예를 들어 특정 국가에서 나온 요청이나 특정 쿼리 문자열이 포함된 요청을 차단하려는 경우에는 OR 문을 생성하고 해당 국가에 대한 지역 일치 문과 쿼리 문자열에 대한 문자열 일치 문을 중첩할 수 있습니다.

대신 특정 국가에서 나오지 않거나 특정 쿼리 문자열이 포함된 요청을 차단하려면 이전 OR 문을 수정하여 NOT 문 내부에서 지역 일치 문을 한 수준 낮게 중첩합니다. 콘솔은 한 수준의 중첩만 지원하므로 이러한 수준의 중첩을 위해서는 JSON 서식을 사용해야 합니다.

중첩 가능 – 이러한 문 유형을 중첩할 수 있습니다.

WCU – 중첩된 문에 따라 다릅니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 규칙 빌더 – 요청의 경우에서 최소 하나의 문과 일치(OR)를 선택한 다음, 중첩된 문을 입력합니다.
- API — OrStatement

예제

다음 목록은 OR를 사용하여 다른 두 명령문을 결합하는 방법을 보여줍니다. 중첩된 명령문 중 하나라도 일치하면 OR 문은 일치하는 것입니다.

```
{
  "Name": "neitherOfTwo",
  "Priority": 1,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "neitherOfTwo"
  },
  "Statement": {
    "OrStatement": {
      "Statements": [
```

```
        {
          "GeoMatchStatement": {
            "CountryCodes": [
              "CA"
            ]
          }
        },
        {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/ipset/test-ip-
set-22222222/33333333-4444-5555-6666-777777777777"
          }
        }
      ]
    }
  }
}
```

콘솔 규칙 시각적 편집기를 사용하면 대부분의 중첩 가능한 명령문을 논리적 규칙 문 아래에 중첩할 수 있지만 시각적 편집기를 사용하여 OR 또는 AND 문을 중첩할 수는 없습니다. 이러한 유형의 중첩을 구성하려면 규칙 문을 JSON으로 제공해야 합니다. 예를 들어, 다음 JSON 규칙 목록에는 AND 문 내에 중첩된 OR 문이 포함됩니다.

```
{
  "Name": "match_rule",
  "Priority": 0,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
          }
        },
        {
          "NotStatement": {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
              }
            }
```

```
          }
        },
        {
          "OrStatement": {
            "Statements": [
              {
                "GeoMatchStatement": {
                  "CountryCodes": [
                    "JM",
                    "JP"
                  ]
                }
              },
              {
                "ByteMatchStatement": {
                  "SearchString": "JCountryString",
                  "FieldToMatch": {
                    "Body": {}
                  },
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ],
                  "PositionalConstraint": "CONTAINS"
                }
              }
            ]
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

비율 기반 규칙 문

속도 기반 규칙은 요청이 너무 빠른 속도로 수신될 때 수신 요청 수를 계산하고 요청 속도를 제한합니다. 규칙은 기준에 따라 요청을 집계하고, 규칙의 평가 기간, 요청 제한 및 작업 설정을 기반으로 집계 그룹화를 개수 및 비율로 제한합니다.

> **Note**
>
> 또한 Bot Control 관리 AWS 규칙 규칙 그룹의 대상 보호 수준을 사용하여 웹 요청의 속도를 제한할 수 있습니다. 이 관리형 규칙 그룹을 사용하면 추가 요금이 발생합니다. 자세한 정보는 속도 기반 규칙 및 대상 지정 Bot Control 규칙의 속도 제한 옵션을 참조하세요.

AWS WAF 사용하는 속도 기반 규칙의 각 인스턴스에 대해 개별적으로 웹 요청을 추적하고 관리합니다. 예를 들어 두 개의 웹 ACL에 동일한 속도 기반 규칙 설정을 제공하는 경우 두 규칙 문은 각각 속도 기반 규칙의 개별 인스턴스를 나타내며 각각 고유한 추적 및 관리 기준을 따릅니다. AWS WAF규칙 그룹 내에 속도 기반 규칙을 정의한 다음 해당 규칙 그룹을 여러 위치에서 사용하면 각 사용자가 자체 추적 및 관리를 수행하는 속도 기반 규칙의 개별 인스턴스를 생성합니다. AWS WAF

중첩 불가능 – 다른 문 안에 이 문 유형을 중첩 할 수 없습니다. 웹 ACL 또는 규칙 그룹에 직접 포함시킬 수 있습니다.

범위 축소 명령문 — 이 규칙 유형은 범위 축소 명령문을 사용하여 규칙이 추적하는 요청의 범위와 속도 제한을 좁힐 수 있습니다. 범위 축소 명령문은 다른 규칙 구성 설정에 따라 선택 사항일 수도 있고 필수일 수도 있습니다. 자세한 내용은 이 섹션에서 다룹니다. 범위 축소 설명에 대한 일반 정보는 을 참조하십시오. 범위 축소 문

WCU - 2(기본 비용). 지정하는 각 사용자 지정 집계 키마다 30WCU를 추가하십시오. 규칙에서 범위 축소 문을 사용하는 경우 해당 문에 대한 WCU를 계산하여 추가합니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔의 웹 ACL 규칙 빌더 – 규칙에서 유형에 대해 속도 기반 규칙을 선택합니다.
- API — RateBasedStatement

주제

- 속도 기반 규칙 상위 수준 설정
- 요금 기반 규칙 경고

- 속도 기반 규칙 집계 옵션 및 키
- 속도 기반 규칙 집계 인스턴스 및 개수
- 속도 기반 규칙 요청 속도 제한 동작
- 속도 기반 규칙 예제
- 속도 기반 규칙에 의해 속도 제한이 적용되는 IP 주소 나열

속도 기반 규칙 상위 수준 설정

속도 기반 규칙 명령문은 다음과 같은 상위 수준 설정을 사용합니다.

- 평가 기간 - 현재 시간을 거슬러 올라가 요청 수에 AWS WAF 포함해야 하는 시간 (초) 입니다. 예를 들어 120으로 설정하는 경우 속도를 AWS WAF 확인할 때 현재 시간 바로 앞 2분 동안의 요청 수를 계산합니다. 유효한 설정은 60 (1분), 120 (2분), 300 (5분), 600 (10분) 이며 기본값은 300 (5분) 입니다.

  이 설정은 속도를 AWS WAF 확인하는 빈도를 결정하는 것이 아니라 확인할 때마다 얼마나 과거로 보이는지를 결정합니다. AWS WAF 평가 기간 설정과 무관한 타이밍으로 비율을 자주 확인합니다.
- 속도 제한 — 기준과 일치하는 요청 중 지정된 평가 기간 동안 AWS WAF 추적해야 하는 최대 요청 수입니다. 허용되는 최소 한도 설정은 100입니다. 이 한도를 위반하면 기준과 일치하는 추가 요청에 규칙 작업 설정이 AWS WAF 적용됩니다.

  AWS WAF 설정한 한도 근방에 속도 제한을 적용하지만 정확한 한도 일치를 보장하지는 않습니다. 자세한 정보는 속도 기반 규칙 주의 사항을 참조하세요.
- 요청 집계 - 속도 기반 규칙에서 개수를 계산하고 및 속도를 제한하는 웹 요청에 사용할 집계 기준입니다. 설정한 속도 한도는 각 집계 인스턴스에 적용됩니다. 자세한 내용은 집계 옵션 및 키 및 집계 인스턴스 및 개수 섹션을 참조하세요.
- 작업 - 규칙이 속도를 제한하는 요청에 대해 수행할 작업입니다. Allow를 제외한 모든 규칙 작업을 사용할 수 있습니다. 이는 평소와 같이 규칙 수준에서 설정되지만 속도 기반 규칙에만 적용되는 몇 가지 제한 및 동작이 있습니다. 규칙 작업에 대한 전체적인 내용은 규칙 작업 섹션을 참조하세요. 속도 제한과 관련된 자세한 내용은 이 속도 기반 규칙 요청 속도 제한 동작 섹션의 내용을 참조하십시오.
- 검사 및 속도 제한 범위 - 범위 축소 문을 추가하여 속도 기반 명령문이 추적하고 속도를 제한하는 요청의 범위를 좁힐 수 있습니다. 범위 축소 문을 지정하는 경우 규칙이 범위 축소 문과 일치하는 요청만 집계, 계산 및 속도를 제한합니다. 요청 집계 옵션 모두 계산을 선택한 경우 범위 축소 문이 필요합니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요.
- (선택 사항) 전달 IP 구성 - 이 옵션은 요청 집계의 헤더에 IP 주소를 단독으로 또는 사용자 지정 키 설정의 일부로 지정하는 경우에만 사용됩니다. AWS WAF 는 지정된 헤더에서 첫 번째 IP 주소를 검색

하고 이를 집계 값으로 사용합니다. 이 용도의 공통 헤더는 `X-Forwarded-For`지만 원하는 헤더를 지정할 수 있습니다. 자세한 내용은 전달된 IP 주소을(를) 참조하세요.

요금 기반 규칙 경고

AWS WAF 속도 제한은 가능한 가장 효율적이고 효과적인 방법으로 높은 요청률을 제어하고 애플리케이션의 가용성을 보호하도록 설계되었습니다. 이는 요청 속도를 정확히 제한하기 위함이 아닙니다.

- AWS WAF 최근 요청을 더 중요시하는 알고리즘을 사용하여 현재 요청 비율을 추정합니다. 따라서 AWS WAF 설정한 한도에 근접하여 속도 제한을 적용하지만 한도가 정확히 일치한다고 보장하지는 않습니다.
- 요청 비율을 AWS WAF 추정할 때마다 구성된 평가 기간 동안 들어온 요청 수를 다시 AWS WAF 살펴봅니다. 이러한 요인과 전파 지연과 같은 기타 요인으로 인해 요청이 AWS WAF 탐지되어 속도가 제한되기까지 최대 몇 분 동안 요청이 너무 높은 속도로 들어오는 경우가 발생할 수 있습니다. 마찬가지로, 요청 속도는 감소를 AWS WAF 감지하고 속도 제한 조치를 중단하기 전에 일정 기간 동안 한도 미만일 수 있습니다. 일반적으로 이 지연은 30초 미만입니다.
- 사용 중인 규칙에서 속도 제한 설정을 변경하면 규칙의 속도 제한 수가 재설정됩니다. 이렇게 하면 규칙의 속도 제한 활동이 최대 1분 동안 일시 중지될 수 있습니다. 속도 제한 설정은 평가 기간, 속도 제한, 요청 집계 설정, 전달된 IP 구성 및 검사 범위입니다.

속도 기반 규칙 집계 옵션 및 키

기본적으로 속도 기반 규칙은 요청 IP 주소에 기반하여 요청을 집계하고 속도를 제한합니다. 다양한 기타 집계 키와 키 조합을 사용하도록 규칙을 구성할 수 있습니다. 예를 들어 전달된 IP 주소, HTTP 메서드 또는 쿼리 인수를 기반으로 집계할 수 있습니다. IP 주소 및 HTTP 방법과 같은 집계 키 조합 또는 서로 다른 두 쿠키의 값을 지정할 수도 있습니다.

> **Note**
>
> 집계 키에 지정하는 모든 요청 구성 요소가 웹 요청에 있어야 규칙을 통해 요청을 평가하거나 속도를 제한할 수 있습니다.

다음 집계 옵션을 사용하여 속도 기반 규칙을 구성할 수 있습니다.

- 소스 IP 주소 - 웹 요청 오리진의 IP 주소만 사용하여 집계합니다.

소스 IP 주소는 발신 클라이언트의 주소를 포함하지 않을 수 있습니다. 웹 요청이 하나 이상의 프록시 또는 로드 밸런서를 통과하는 경우 여기에는 마지막 프록시의 주소가 포함됩니다.

- 헤더의 IP 주소 - HTTP 헤더의 클라이언트 주소만 사용하여 집계합니다. 이러한 주소를 전달된 IP 주소라고도 합니다.

  이 구성을 사용하면 헤더에 잘못된 형식의 IP 주소가 있는 웹 요청에 적용할 폴백 동작도 지정할 수 있습니다. 폴백 동작은 요청에 대한 일치 결과를 일치하거나 일치하지 않음으로 설정합니다. 일치하는 항목이 없는 경우애는 속도 기반 규칙이 요청 수를 계산하거나 요청의 속도를 제한하지 않습니다. 일치할 경우 속도 기반 규칙은 해당 요청을 지정된 헤더에 잘못된 IP 주소가 있는 다른 요청과 함께 그룹화합니다.

  프록시가 헤더를 일관성 없이 처리할 수 있고 검사를 우회하도록 헤더를 수정할 수도 있으므로 이 옵션에는 주의해야 합니다. 추가 정보와 정책 모범 사례는 전달된 IP 주소 섹션을 참조하세요.

- 모두 계산 - 규칙의 범위 축소 문과 일치하는 모든 요청 수를 계산하고 이들 요청의 속도를 제한합니다. 이 옵션에는 범위 축소 문이 필요합니다. 이는 일반적으로 특정 요청의 속도를 제한하는 데 사용됩니다(예: 특정 레이블이 있는 모든 요청 또는 특정 지리적 영역에서 들어오는 모든 요청).

- 사용자 지정 키 - 하나 이상의 사용자 지정 집계 키를 사용하여 집계합니다. IP 주소 옵션 중 하나를 다른 집계 키와 결합하려면 여기 사용자 지정 키에서 해당 옵션을 정의하십시오.

  사용자 지정 집계 키는 요청 구성 요소 옵션에 설명된 웹 요청 구성 요소 옵션의 하위 집합입니다.

  다음과 같은 키 옵션이 있습니다. 별도로 명시된 경우가 아니면 옵션을 여러 번 사용할 수 있습니다. 예: 헤더 2개 또는 레이블 네임스페이스 3개.

  - 레이블 네임스페이스 - 레이블 네임스페이스를 집계 키로 사용합니다. 지정된 레이블 네임스페이스가 있는 각각의 고유한 정규화된 레이블 이름이 집계 인스턴스에 포함됩니다. 사용자 지정 키로 사용하는 경우 각 레이블 이름만 사용하는 경우 각 레이블 이름만으로 집계 인스턴스가 정의됩니다.

    속도 기반 규칙은 웹 ACL에서 미리 평가되는 규칙에 의해 요청에 추가된 레이블만 사용합니다.

    레이블 네임스페이스와 이름에 대한 자세한 내용은 AWS WAF 레이블 구문 및 이름 지정 요구 사항 섹션을 참조하세요.

  - 헤더 - 이름이 지정된 헤더를 집계 키로 사용합니다. 헤더의 각 고유 값은 집계 인스턴스에 포함됩니다.

    헤더는 선택적 텍스트 변환을 사용합니다. 텍스트 변환 옵션를 참조하세요.

- 쿠키 - 이름이 지정된 쿠키를 집계 키로 사용합니다. 쿠키의 각 고유 값은 집계 인스턴스에 포함됩니다.

  쿠키는 선택적 텍스트 변환을 사용합니다. 텍스트 변환 옵션를 참조하세요.

- 쿼리 인수 - 요청의 단일 쿼리 인수를 집계 키로 사용합니다. 이름이 지정된 쿼리 인수에 대한 각각의 고유 값이 집계 인스턴스에 포함됩니다.

  쿼리 인수는 선택적 텍스트 변환을 사용합니다. 텍스트 변환 옵션를 참조하세요.

- 쿼리 문자열 - 요청의 전체 쿼리 문자열을 집계 키로 사용합니다. 각각의 고유한 쿼리 문자열이 집계 인스턴스에 포함됩니다. 이 키 유형은 한 번만 사용할 수 있습니다.

  쿼리 문자열은 선택적 텍스트 변환을 사용합니다. 텍스트 변환 옵션를 참조하세요.

- URI 경로 - 요청의 URI 경로를 집계 키로 사용합니다. 각각의 고유한 URI 경로가 집계 인스턴스에 포함됩니다. 이 키 유형은 한 번만 사용할 수 있습니다.

  URI 경로는 선택적 텍스트 변환을 사용합니다. 텍스트 변환 옵션를 참조하세요.

- HTTP 메서드 - 요청의 HTTP 메서드를 집계 키로 사용합니다. 각각의 고유한 HTTP 메서드가 집계 인스턴스에 포함됩니다. 이 키 유형은 한 번만 사용할 수 있습니다.

- IP 주소 - 웹 요청 오리진의 IP 주소를 다른 키와 함께 사용하여 집계합니다.

  여기에는 발신 클라이언트의 주소가 포함되지 않을 수 있습니다. 웹 요청이 하나 이상의 프록시 또는 로드 밸런서를 통과하는 경우 여기에는 마지막 프록시의 주소가 포함됩니다.

- 헤더의 IP 주소 - HTTP 헤더의 클라이언트 주소를 다른 키와 함께 사용하여 집계합니다. 이러한 주소를 전달된 IP 주소라고도 합니다.

  헤더가 프록시를 통해 일관되지 않게 처리되고 검사를 우회하도록 수정될 수 있으므로 이 옵션은 주의하여 사용해야 합니다. 추가 정보와 정책 모범 사례는 전달된 IP 주소 섹션을 참조하세요.

속도 기반 규칙 집계 인스턴스 및 개수

속도 기반 규칙이 집계 기준을 사용하여 웹 요청을 평가하는 경우, 규칙이 지정된 집계 키에 대해 찾는 각각의 고유한 값 집합이 고유한 집계 인스턴스를 정의합니다.

- 다중 키 - 사용자 지정 키를 여러 개 정의한 경우 각 키의 값이 집계 인스턴스 정의에 포함됩니다. 각각의 고유한 값 조합이 집계 인스턴스를 정의합니다.
- 단일 키 - 사용자 지정 키에서 또는 싱글톤 IP 주소 선택 항목 중 하나를 선택하여 단일 키를 선택한 경우 키의 각 고유 값이 집계 인스턴스를 정의합니다.

- 모두 계산 - 키 없음 - 모두 계산 옵션을 선택한 경우 규칙이 평가하는 모든 요청은 해당 규칙의 단일 집계 인스턴스에 속합니다. 이 옵션에는 범위 축소 문이 필요합니다.

속도 기반 규칙은 식별된 각 집계 인스턴스마다 별도로 웹 요청 수를 계산합니다.

예를 들어, 속도 기반 규칙이 다음 IP 주소 및 HTTP 메서드 값을 사용하여 웹 요청을 평가한다고 가정해 보겠습니다.

- IP 주소 10.1.1.1, HTTP 메서드 POST
- IP 주소 10.1.1.1, HTTP 메서드 GET
- IP 주소 127.0.0.0, HTTP 메서드 POST
- IP 주소 10.1.1.1, HTTP 메서드 GET

이 규칙은 집계 기준에 따라 다양한 집계 인스턴스를 생성합니다.

- 집계 기준이 단지 IP 주소인 경우 각 개별 IP 주소는 집계 인스턴스이며 각각에 대해 개별적으로 요청을 계산합니다. AWS WAF 이 예제의 집계 인스턴스와 요청 수는 다음과 같습니다.
  - IP 주소 10.1.1.1: 개수 3
  - IP 주소 127.0.0.0: 개수 1
- 집계 기준이 HTTP 메서드이면 각 개별 HTTP 메서드가 집계 인스턴스입니다. 이 예제의 집계 인스턴스와 요청 수는 다음과 같습니다.
  - HTTP 메서드 POST: 개수 2
  - HTTP 메서드 GET: 개수 2
- 집계 기준이 IP 주소 및 HTTP 메서드 둘 다인 경우 각 IP 주소와 각 HTTP 메서드가 통합 집계 인스턴스에 포함됩니다. 이 예제의 집계 인스턴스와 요청 수는 다음과 같습니다.
  - IP 주소 10.1.1.1, HTTP 메서드 POST: 개수 1
  - IP 주소 10.1.1.1, HTTP 메서드 GET: 개수 2
  - IP 주소 127.0.0.0, HTTP 메서드 POST: 개수 1

속도 기반 규칙 요청 속도 제한 동작

속도 기반 규칙에 대한 속도 제한 요청의 속도 제한 기준은 해당 규칙에 대한 요청을 집계하는 데 AWS WAF 사용하는 기준과 동일합니다. AWS WAF 규칙에 대한 범위 축소 명령문을 정의하는 경우 범위 축소 명령문과 일치하는 AWS WAF 요청만 집계, 개수 및 속도 제한 요청만 집계합니다.

웹 요청이 다음과 같은 일치 기준을 충족하는 경우 속도 기반 규칙은 해당 규칙 작업 설정을 특정 웹 요청에 적용합니다.

- 웹 요청은 규칙의 범위 축소 문(정의된 경우)과 일치합니다.
- 웹 요청이 요청 수가 현재 규칙 제한을 초과하는 집계 인스턴스에 속합니다.

규칙 조치는 AWS WAF 어떻게 적용됩니까?

속도 기반 규칙이 요청에 속도 제한을 적용하는 경우 규칙 조치가 적용되며, 조치 사양에 사용자 지정 처리 또는 레이블 지정을 정의한 경우 규칙이 해당 규칙을 적용합니다. 이 요청 처리는 일치 규칙이 해당 작업 설정을 일치하는 웹 요청에 적용하는 방식과 동일합니다. 속도 기반 규칙은 속도 제한이 적극적으로 적용되는 요청에 대해서만 레이블을 적용하거나 다른 작업을 수행합니다.

Allow를 제외한 모든 규칙 작업을 사용할 수 있습니다. 규칙 작업에 대한 전체적인 내용은 규칙 작업 섹션을 참조하세요.

다음 목록은 각 조치에 대한 속도 제한의 작동 방식을 설명합니다.

- Block— 요청을 AWS WAF 차단하고 사용자가 정의한 모든 사용자 지정 차단 동작을 적용합니다.
- Count— 요청을 AWS WAF 계산하고, 정의한 사용자 지정 헤더 또는 레이블을 적용하고, 요청의 웹 ACL 평가를 계속합니다.

  이 작업은 요청의 속도를 제한하지 않습니다. 한도를 초과하는 요청만 계산합니다.
- CAPTCHA 또는 Challenge - AWS WAF 가 요청 토큰의 상태에 따라 요청을 Block 또는 Count와 같이 처리합니다.

  이 작업은 유효한 토큰이 있는 요청의 비율을 제한하지 않습니다. 한도를 초과하고 유효한 토큰이 누락된 요청의 비율을 제한합니다.
  - 요청에 만료되지 않은 유효한 토큰이 없는 경우 이 작업은 요청을 차단하고 CAPTCHA 퍼즐 또는 브라우저 챌린지를 클라이언트로 다시 보냅니다.

    최종 사용자나 클라이언트 브라우저가 성공적으로 응답하면 클라이언트는 유효한 토큰을 받고 원래 요청을 자동으로 다시 보냅니다. 집계 인스턴스에 대한 속도 제한이 여전히 유효한 경우 유효하고 만료되지 않은 토큰이 포함된 이 새 요청에는 다음 글머리 항목에 설명된 대로 작업이 적용됩니다.
  - 요청에 유효하고 만료되지 않은 토큰이 있는 경우 CAPTCHA or Challenge 작업은 토큰을 확인하고 Count 작업과 마찬가지로 요청에 대해 아무런 작업도 수행하지 않습니다. 속도 기반 규칙은 종

료 조치를 취하지 않고 요청 평가를 웹 ACL에 반환하며, 웹 ACL은 요청에 대한 평가를 계속합니다.

자세한 내용은 CAPTCHA그리고 Challenge 안에 AWS WAF 섹션을 참조하세요.

IP 주소 또는 전달된 IP 주소만 속도를 제한하는 경우

전달된 IP 주소에 대한 IP 주소만 속도 제한하도록 규칙을 구성하면 규칙 인스턴스가 최대 10,000개의 IP 주소에 대해 속도 제한할 수 있습니다. 규칙 인스턴스가 속도를 제한할 10,000개가 넘는 IP 주소를 식별하는 경우 최상위 발신자 10,000명만 제한합니다.

이 구성을 사용하면 속도 기반 규칙이 현재 속도를 제한하는 IP 주소 목록을 검색할 수 있습니다. 범위 축소 명령문을 사용하는 경우 속도 제한이 적용되는 요청은 IP 목록에서 범위 축소 명령문과 일치하는 요청뿐입니다. IP 주소 목록 검색에 대한 자세한 내용은 속도 기반 규칙에 의해 속도 제한이 적용되는 IP 주소 나열 섹션을 참조하세요.

속도 기반 규칙 예제

이 섹션에서는 다양한 일반 속도 기반 규칙 사용 사례에 대한 예제 구성을 설명합니다.

각 예제는 사용 사례에 대한 설명을 제공하고 나서 사용자 지정 구성 규칙의 JSON 목록에 나와 있는 솔루션을 표시합니다.

> **Note**
>
> 이 예제에 표시된 JSON 목록은 콘솔에서 규칙을 구성하고 나서 규칙 JSON 편집기로 편집하여 생성한 것입니다.

주제

- 로그인 페이지에 대한 요청 속도 제한
- IP 주소, 사용자 에이전트 쌍으로부터의 로그인 페이지에 대한 요청 속도 제한
- 특정 헤더가 누락된 요청의 속도 제한
- 특정 레이블이 있는 요청의 속도 제한
- 지정된 레이블 네임스페이스가 있는 레이블에 대한 요청 속도 제한

로그인 페이지에 대한 요청 속도 제한

사이트의 나머지 부분에 대한 트래픽에 영향을 주지 않으면서 웹 사이트의 로그인 페이지에 대한 요청 수를 제한하려는 경우 로그인 페이지에 대한 요청과 일치하는 범위 축소 문과 모두 계산으로 설정된 요청 집계를 사용하여 속도 기반 규칙을 생성할 수 있습니다.

속도 기반 규칙은 로그인 페이지에 대한 모든 요청을 단일 집계 인스턴스로 계산하고 요청이 제한을 초과하면 규칙 작업을 적용합니다.

다음 JSON 목록은 이 규칙 구성의 예를 보여줍니다. 모두 계산 집계 옵션은 JSON에 `CONSTANT` 설정으로 나와 있습니다. 이 예제는 `/login`으로 시작하는 로그인 페이지와 일치합니다.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
```

```
    }
  }
}
```

IP 주소, 사용자 에이전트 쌍으로부터의 로그인 페이지에 대한 요청 속도 제한

제한을 초과하는 IP 주소, 사용자 에이전트 쌍의에 대한 로그인 페이지 요청 수를 제한하려면 요청 집계를 사용자 지정 키로 설정하고 집계 기준을 지정합니다.

다음 JSON 목록은 이 규칙 구성의 예를 보여줍니다. 이 예시에서는 IP 주소, 사용자 에이전트 쌍당 5분 동안 요청 한도를 100개로 설정했습니다.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "User-Agent",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        },
        {
          "IP": {}
        }
```

```
      ],
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

특정 헤더가 누락된 요청의 속도 제한

특정 헤더가 누락된 요청의 수를 제한하려는 경우 모든 계산 집계 옵션을 범위 축소 문과 함께 사용할 수 있습니다. 헤더가 존재하고 값이 있는 경우에만 true를 반환하는 명령문을 포함하는 논리 NOT 문을 사용하여 범위 축소 문을 구성합니다.

다음 JSON 목록은 이 규칙 구성의 예를 보여줍니다.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "AggregateKeyType": "CONSTANT",
```

```
      "EvaluationWindowSec": 300,
      "ScopeDownStatement": {
        "NotStatement": {
          "Statement": {
            "SizeConstraintStatement": {
              "FieldToMatch": {
                "SingleHeader": {
                  "Name": "user-agent"
                }
              },
              "ComparisonOperator": "GT",
              "Size": 0,
              "TextTransformations": [
                {
                  "Type": "NONE",
                  "Priority": 0
                }
              ]
            }
          }
        }
      }
    }
  }
}
```

특정 레이블이 있는 요청의 속도 제한

속도 제한을 요청에 레이블을 추가하는 규칙 또는 규칙 그룹과 결합하여 다양한 범주의 요청 수를 제한할 수 있습니다. 이렇게 하려면 다음과 같이 웹 ACL을 구성합니다.

- 레이블을 추가하는 규칙 또는 규칙 그룹을 추가하고 속도를 제한할 요청을 차단하거나 허용하지 않도록 구성합니다. 관리형 규칙 그룹을 사용하는 경우 Count에서 이 동작을 수행하려면 일부 규칙 그룹의 규칙 작업을 재정의해야 할 수 있습니다.
- 레이블 지정 규칙 및 규칙 그룹보다 높은 우선순위 번호 설정을 사용하여 웹 ACL에 속도 기반 규칙을 추가합니다. AWS WAF 가장 낮은 것부터 시작하여 숫자순으로 규칙을 평가하므로, 비율 기반 규칙은 레이블 지정 규칙 이후에 실행됩니다. 규칙의 범위 축소 문에 있는 레이블 일치와 레이블 집계를 조합하여 레이블에 대한 속도 제한을 구성합니다.

다음 예시에서는 Amazon IP 평판 목록 AWS 관리형 규칙 그룹을 사용합니다. 규칙 그룹 규칙은 `AWSManagedIPDDoSList`에서 DDoS 활동에 적극적으로 참여하는 것으로 알려진 IP의 요청을 탐지

하고 레이블을 지정합니다. 이 규칙의 동작은 규칙 그룹 정의에서 Count로 구성됩니다. 규칙 그룹에 대한 자세한 내용은 the section called “Amazon IP 평판 목록” 섹션을 참조하세요.

다음 웹 ACL JSON 목록은 IP 신뢰도 규칙 그룹과 레이블 일치 속도 기반 규칙을 차례로 사용합니다. 속도 기반 규칙은 범위 축소 문을 사용하여 규칙 그룹 규칙으로 표시된 요청을 필터링합니다. 속도 기반 규칙 명령문은 필터링된 요청을 해당 IP 주소별로 집계하고 속도를 제한합니다.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
```

```
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

지정된 레이블 네임스페이스가 있는 레이블에 대한 요청 속도 제한

Bot Control 관리형 규칙 그룹의 공통 수준 규칙은 다양한 범주의 봇에 레이블을 추가하지만 확인되지 않은 봇의 요청만 차단합니다. 이러한 규칙에 대한 자세한 내용은 Bot Control 규칙 목록 섹션을 참조하세요.

Bot Control 관리형 규칙 그룹을 사용하는 경우 확인된 개별 봇의 요청에 대해 속도 제한을 추가할 수 있습니다. 이를 위해 Bot Control 규칙 그룹 이후에 실행되어 봇 이름 레이블별로 요청을 집계하는 속도 기반 규칙을 추가합니다. Label 네임스페이스 집계 키를 지정하고 네임스페이스 키를 `awswaf:managed:aws:bot-control:bot:name:`으로 설정합니다. 지정된 네임스페이스가 있는 각 고유 레이블이 집계 인스턴스를 정의합니다. 예를 들어, 레이블 `awswaf:managed:aws:bot-control:bot:name:axios` 및 `awswaf:managed:aws:bot-control:bot:name:curl`이 각각 집계 인스턴스를 정의합니다.

다음 웹 ACL JSON 목록은 이 구성을 보여줍니다. 이 예제의 규칙은 2분 동안 단일 봇 집계 인스턴스에 대한 요청을 1,000개로 제한합니다.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
```

```
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "LabelNamespace": {
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

속도 기반 규칙에 의해 속도 제한이 적용되는 IP 주소 나열

속도 기반 규칙이 IP 주소 또는 전달된 IP 주소에서만 집계되는 경우 규칙이 현재 속도를 제한하는 IP 주소 목록을 검색할 수 있습니다. AWS WAF 이러한 IP 주소를 규칙의 관리 키 목록에 저장합니다.

> **Note**
>
> 이 옵션은 IP 주소만 또는 헤더의 IP 주소만 집계하는 경우에 한하여 사용할 수 있습니다. 사용자 지정 키 요청 집계를 사용하는 경우 사용자 지정 키에서 IP 주소 사양 중 하나를 사용하더라도 속도가 제한된 IP 주소의 목록을 검색할 수 없습니다.

속도 기반 규칙은 규칙의 범위 축소 문과 일치하는 규칙의 관리 키 목록에 있는 요청에 해당 규칙 작업을 적용합니다. 규칙에 범위 축소 문이 없는 경우 목록에 있는 IP 주소의 모든 요청에 작업이 적용됩니다. 규칙 작업은 기본적으로 Block이지만, Allow의 경우를 제외하고는 유효한 규칙 작업이면 어떤 것이든 사용할 수 있습니다. 단일 속도 기반 규칙 인스턴스를 사용하여 속도를 AWS WAF 제한할 수 있는 최대 IP 주소 수는 10,000개입니다. 10,000개 이상의 주소가 속도 AWS WAF 제한을 초과하는 경우 요금이 가장 높은 주소를 제한합니다.

CLI, API 또는 SDK를 사용하여 속도 기반 규칙의 관리형 키 목록에 액세스할 수 있습니다. 이 주제에서는 CLI 및 API를 사용한 액세스에 대해 설명합니다. 현재는 콘솔에서 목록에 대한 액세스를 제공하지 않습니다.

AWS WAF API의 경우 명령은 다음과 같습니다 GetRateBasedStatementManagedKeys.

AWS WAF CLI의 경우 명령은 -관리형 키입니다get-rate-based-statement.

다음은 Amazon 배포의 웹 ACL에서 사용되는 속도 기반 규칙에 대한 속도 제한 IP 주소 목록을 검색하는 구문을 보여줍니다. CloudFront

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

다음은 리전 애플리케이션, Amazon API Gateway REST API, 애플리케이션 로드 밸런서, GraphQL API, Amazon Cognito 사용자 풀 AWS AppSync , 서비스 또는 검증된 액세스 인스턴스의 AWS App Runner 구문을 보여줍니다. AWS

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF 웹 요청을 모니터링하고 웹 ACL, 선택적 규칙 그룹 및 속도 기반 규칙의 고유한 각 조합에 대해 독립적으로 키를 관리합니다. 예를 들어 규칙 그룹 내에서 속도 기반 규칙을 정의한 다음 웹 ACL의 규칙 그룹을 사용하는 경우 AWS WAF 는 웹 요청을 모니터링하고 해당 웹 ACL, 규칙 그룹 참조문 및 속도 기반 규칙 인스턴스에 대한 키를 관리합니다. 두 번째 웹 ACL에서 동일한 규칙 그룹을 사용하는 경우 첫 번째 사용과 완전히 독립적으로 두 번째 사용에 대한 웹 요청을 AWS WAF 모니터링하고 키를 관리합니다.

규칙 그룹 내에 정의한 속도 기반 규칙의 경우, 웹 ACL 이름 및 규칙 그룹 내 속도 기반 규칙 이름 외에도 요청에 규칙 그룹 참조 문의 이름을 제공해야 합니다. 다음은 속도 기반 규칙이 규칙 그룹 안에 정의되고 규칙 그룹이 웹 ACL에서 사용되는 지리적 응용 프로그램의 구문을 보여줍니다.

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --rule-name=RuleName
```

규칙 그룹 규칙 문

규칙 그룹 규칙 문은 중첩할 수 없습니다.

이 섹션에서는 웹 ACL에서 사용할 수 있는 규칙 그룹 규칙 문을 설명합니다. 규칙 그룹 웹 ACL 용량 단위(WCU)는 규칙 그룹 생성 시 규칙 그룹 소유자가 설정합니다. WCU에 대한 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

규칙 그룹 문	설명	WCU
관리형 규칙 그룹	지정된 관리형 규칙 그룹에 정의된 규칙을 실행합니다. 범위 축소 문을 추가하여 규칙 그룹이 평가하는 요청 범위를 좁힐 수 있습니다. 관리형 규칙 그룹 문을 다른 문 유형 안에 중첩할 수 없습니다.	규칙 그룹과 범위 축소 문에 대한 모든 추가 WCU에 의해 정의됩니다.
규칙 그룹	관리하는 규칙 그룹에 정의된 규칙을 실행합니다. 사용자 고유의 규칙 그룹 대한 규칙 그룹 참조 문에는 범위 축소 문을 추가할 수 없습니다. 규칙 그룹 문을 다른 문 유형 안에 중첩할 수 없습니다.	규칙 그룹을 생성할 때 규칙 그룹에 대해 WCU 제한을 정의합니다.

관리형 규칙 그룹 문

관리형 규칙 그룹 규칙 문은 웹 ACL 규칙 목록의 참조를 관리형 규칙 그룹에 추가합니다. 콘솔의 규칙 문 아래에 이 옵션이 표시되어 있지 않지만 웹 ACL의 JSON 형식으로 작업할 경우, 추가한 모든 관리형 규칙 그룹이 웹 ACL 규칙 아래에 이 유형으로 표시됩니다.

관리형 규칙 그룹은 대부분 AWS WAF 고객에게 무료로 제공되는 AWS 관리형 규칙 그룹이거나 AWS Marketplace 관리형 규칙 그룹입니다. 유료 AWS 관리형 규칙 규칙 그룹을 웹 ACL에 추가하면 자동으로 구독됩니다. 를 통해 AWS Marketplace AWS Marketplace관리형 규칙 그룹을 구독할 수 있습니다. 자세한 정보는 관리형 규칙 그룹을 참조하세요.

웹 ACL에 규칙 그룹을 추가할 때 그룹에 있는 규칙의 작업을 Count로 또는 다른 규칙 작업으로 재정의할 수 있습니다. 자세한 정보는 규칙 그룹의 작업 재정의 옵션을 참조하세요.

규칙 그룹으로 AWS WAF 평가되는 요청의 범위를 좁힐 수 있습니다. 이렇게 하려면 규칙 그룹 문 안에 범위 축소 문을 추가합니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요. 이렇게 하면 규칙 그룹이 트래픽에 미치는 영향을 관리하고 규칙 그룹 사용 시 트래픽 볼륨과 관련된 비용을 절감하는 데 도움이 될 수 있습니다. AWS WAF Bot Control 관리 규칙 그룹에서 범위 축소 명령문을 사용하는 방법에 대한 자세한 내용 및 예는 을 참조하십시오. AWS WAF 봇 컨트롤

중첩 불가능 – 다른 문 안에 이 문 유형을 중첩할 수 없으며, 규칙 그룹에 포함시킬 수 없습니다. 웹 ACL에 직접 포함시킬 수 있습니다.

(선택 사항) 범위 축소 문 - 이 규칙 유형은 선택적 범위 축소 문을 사용하여 규칙 그룹이 평가하는 요청의 범위를 좁힙니다. 자세한 정보는 범위 축소 문을 참조하세요.

WCU – 생성 시 규칙 그룹에 설정됩니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔 – 웹 ACL을 생성하는 동안 규칙 및 규칙 그룹 추가 페이지에서 관리형 규칙 그룹 추가를 선택하고 사용할 규칙 그룹을 찾아서 선택합니다.
- API — ManagedRuleGroupStatement

규칙 그룹 문

규칙 그룹 규칙 문은 웹 ACL 규칙 목록에 대한 참조를 관리하는 규칙 그룹에 추가합니다. 콘솔의 규칙 문 아래에 이 옵션이 표시되어 있지 않지만 웹 ACL의 JSON 형식으로 작업할 경우, 추가한 모든 자체 규칙 그룹이 웹 ACL 규칙 아래에 이 유형으로 표시됩니다. 자체 규칙 그룹 사용에 대한 자세한 내용은 자체 규칙 그룹 관리 단원을 참조하세요.

웹 ACL에 규칙 그룹을 추가할 때 그룹에 있는 규칙의 작업을 Count로 또는 다른 규칙 작업으로 재정의할 수 있습니다. 자세한 정보는 규칙 그룹의 작업 재정의 옵션을 참조하세요.

중첩 불가능 – 다른 문 안에 이 문 유형을 중첩할 수 없으며, 규칙 그룹에 포함시킬 수 없습니다. 웹 ACL에 직접 포함시킬 수 있습니다.

WCU – 생성 시 규칙 그룹에 설정됩니다.

이 규칙 문을 찾을 수 있는 위치

- 콘솔 – 웹 ACL을 생성하는 동안 규칙 및 규칙 그룹 추가 페이지에서 자체 규칙 및 규칙 그룹 추가, 규칙 그룹을 차례로 선택하고 사용할 규칙 그룹을 추가합니다.
- API — RuleGroupReferenceStatement

에서 크기 초과 요청 구성 요소 처리 AWS WAF

AWS WAF 웹 요청 구성 요소 본문, 헤더 또는 쿠키의 대용량 콘텐츠 검사를 지원하지 않습니다. 기본 호스트 서비스는 검사를 위해 AWS WAF 전달하는 대상에 대한 개수 및 크기 제한이 있습니다. 예를 들어 호스트 서비스는 200개 이상의 헤더를 전송하지 않으므로 헤더가 205개인 웹 요청의 경우 마지막 5개 헤더를 AWS WAF 검사할 수 없습니다. AWS WAF

보호된 리소스로 웹 요청을 진행하도록 AWS WAF 허용하면 검사할 수 AWS WAF 있었던 개수 및 크기 제한을 벗어난 콘텐츠를 포함한 전체 웹 요청이 전송됩니다.

구성 요소 검사 크기 제한

구성 요소 검사 크기 제한은 다음과 같습니다.

- **`Body`**및 **`JSON Body`** — Application Load Balancer 및 의 AWS AppSync경우 요청 본문의 처음 8KB를 AWS WAF 검사할 수 있습니다. 의 경우 CloudFront 기본적으로 API Gateway, Amazon Cognito, 앱 러너 및 검증된 액세스는 처음 16KB를 AWS WAF 검사할 수 있으며 웹 ACL 구성에서는 제한을 최대 64KB까지 늘릴 수 있습니다. 자세한 정보는 신체 검사 크기 제한 관리을 참조하세요.
- **`Headers`**— 요청 헤더의 처음 8KB (8,192바이트), 최대 처음 200개의 헤더를 검사할 AWS WAF 수 있습니다. 첫 번째 제한에 도달할 때까지 콘텐츠를 AWS WAF 검사할 수 있습니다.
- **`Cookies`**— AWS WAF 요청 쿠키의 처음 8KB (8,192바이트), 최대 처음 200개의 쿠키를 검사할 수 있습니다. 콘텐츠는 첫 번째 제한에 도달할 AWS WAF 때까지 검사할 수 있습니다.

규칙 문에 대한 과대 처리 옵션

이러한 요청 구성 요소 유형 중 하나를 검사하는 규칙 문을 작성할 때 과대 구성 요소를 처리하는 방법을 지정합니다. 크기 초과 처리는 규칙이 검사하는 요청 구성 요소가 크기 제한을 초과하는 경우 웹 요청을 어떻게 AWS WAF 처리할지 알려줍니다.

과대 처리 구성 요소의 옵션은 다음과 같습니다.

- Continue— 규칙 검사 기준에 따라 요청 구성 요소를 정상적으로 검사합니다. AWS WAF 크기 제한 내에 있는 요청 구성 요소 내용을 검사합니다.
- Match— 웹 요청을 규칙 설명과 일치하는 것으로 취급합니다. AWS WAF 규칙의 검사 기준과 비교하여 평가하지 않고 요청에 규칙 조치를 적용합니다.
- No match— 웹 요청을 규칙의 검사 기준에 따라 평가하지 않으면 규칙 설명과 일치하지 않는 것으로 간주합니다. AWS WAF 일치하지 않는 규칙과 마찬가지로 웹 ACL의 나머지 규칙을 사용하여 웹 요청을 계속 검사합니다.

AWS WAF 콘솔에서는 이러한 처리 옵션 중 하나를 선택해야 합니다. 콘솔 외부에서 기본 옵션은 Continue입니다.

동작이 Block로 설정된 규칙에서 Match 옵션을 사용하는 경우 규칙은 검사한 구성 요소의 크기가 너무 큰 요청을 차단합니다. 다른 구성을 사용할 경우 요청의 최종 처리는 웹 ACL의 다른 규칙 구성, 웹 ACL의 기본 작업 설정 등 다양한 요인에 따라 달라집니다.

사용자가 소유하지 않는 규칙 그룹의 과대 처리

구성 요소 크기 및 개수 제한은 사용자가 웹 ACL에서 사용하는 모든 규칙에 적용됩니다. 여기에는 관리형 규칙 그룹과 다른 계정이 사용자와 공유하는 규칙 그룹에서 사용자가 사용하지만 관리하지 않는 모든 규칙이 포함됩니다.

관리하지 않는 규칙 그룹을 사용하는 경우 제한된 요청 구성 요소를 검사하지만 사용자가 원하는 처리 방식으로 과대 콘텐츠를 처리하지 않는 규칙이 규칙 그룹에 있을 수 있습니다. AWS Managed Rules가 크기가 큰 구성 요소를 관리하는 방법에 대한 자세한 내용은 을 참조하십시오AWS 관리형 규칙 규칙 그룹 목록. 다른 규칙 그룹에 대한 자세한 내용은 규칙 그룹 공급자에게 문의하십시오.

웹 ACL에서 과대 구성 요소를 관리하기 위한 지침

웹 ACL에서 과대 구성 요소를 처리하는 방법은 요청 구성 요소 콘텐츠의 예상 크기, 웹 ACL의 기본 요청 처리, 그리고 웹 ACL의 다른 규칙이 요청을 일치시키고 처리하는 방법 등 여러 요인에 따라 달라질 수 있습니다.

과대 웹 요청 구성 요소를 관리하기 위한 일반 지침은 다음과 같습니다.

- 과대 구성 요소 콘텐츠를 포함하는 일부 요청을 허용해야 하는 경우 가능하면 그러한 요청만 명시적으로 허용하는 규칙을 추가합니다. 동일한 구성 요소 유형을 검사하는 다른 규칙보다 먼저 실행되도록 웹 ACL에서 해당 규칙의 우선 순위를 지정합니다. 이 접근 방식을 사용하면 보호된 리소스에 AWS WAF 전달하도록 허용한 크기 초과 구성 요소의 전체 콘텐츠를 검사하는 데 사용할 수 없습니다.
- 다른 모든 요청의 경우 제한을 초과하는 요청을 차단하여 추가 바이트가 전달되지 않도록 할 수 있습니다.
  - 규칙 및 규칙 그룹 - 크기 제한이 있는 구성 요소를 검사하는 규칙에서 제한을 초과하는 요청을 차단하도록 과대 처리를 구성합니다. 예를 들어, 규칙이 특정 헤더 콘텐츠를 포함하는 요청을 차단하는 경우 과대 처리를 과대 헤더 콘텐츠가 있는 요청과 일치하도록 설정합니다. 또는 웹 ACL이 기본적으로 요청을 차단하고 규칙에서 특정 헤더 콘텐츠를 허용하는 경우, 과대 헤더 콘텐츠가 있는 어떠한 요청과도 일치하지 않도록 규칙의 과대 처리를 구성합니다.
  - 관리하지 않는 규칙 그룹 - 관리하지 않는 규칙 그룹이 과대 요청 구성 요소를 허용하지 않도록 하려면 요청 구성 요소 유형을 검사하고 제한을 초과하는 요청을 차단하는 별도의 규칙을 추가할 수 있습니다. 규칙 그룹보다 먼저 실행되도록 웹 ACL에서 규칙의 우선 순위를 지정합니다. 예를 들어 본문 검사 규칙을 웹 ACL에서 실행하기 전에 과대 본문 콘텐츠가 있는 요청을 차단할 수 있습니다. 다음 절차에서 이 규칙 유형을 추가하는 방법을 설명합니다.

크기가 큰 웹 요청 구성 요소 차단

크기가 큰 구성 요소가 포함된 요청을 차단하는 규칙을 웹 ACL에 추가할 수 있습니다.

과대 콘텐츠를 차단하는 규칙을 추가하려면

1. 웹 ACL을 만들거나 편집할 때 규칙 설정에서 규칙 추가, 자체 규칙 및 규칙 그룹 추가, 규칙 빌더 및 규칙 시각 편집기를 순서대로 선택합니다. 웹 ACL 생성 또는 편집에 대한 지침은 웹 ACL 작업 섹션을 참조하세요.
2. 규칙의 이름을 입력하고 유형 설정은 일반 규칙으로 그대로 둡니다.
3. 다음 일치 설정을 기본값에서 다른 값으로 변경합니다.

   a. 명령문에서 검사의 드롭다운을 열고 필요한 웹 요청 구성 요소(본문, 헤더 또는 쿠키)를 선택합니다.

   b. 검색 유형에서 크기 초과를 선택합니다.

   c. 크기에는 구성 요소 유형의 최소 크기 이상인 숫자를 입력합니다. 헤더와 쿠키의 경우 다음을 입력합니다. 8192 Application Load Balancer 또는 AWS AppSync 웹 ACL에서 본문에 대해 다음을 입력합니다. 8192 API Gateway CloudFront, Amazon Cognito, 앱 러너 또는 검증

된 액세스 웹 ACL의 본문에 대해 기본 본문 크기 제한을 사용하는 경우 다음을 입력합니다. 16384 그렇지 않으면 웹 ACL에 정의한 본문 크기 제한을 입력하십시오.

d. 과대를 처리하려면 일치를 선택합니다.

4. 작업에서 차단을 선택합니다.
5. 규칙 추가를 선택합니다.
6. 규칙을 추가한 후에는 규칙 우선순위 설정 페이지에서 해당 규칙을 동일한 구성 요소 유형을 검사하는 웹 ACL의 모든 규칙 또는 규칙 그룹 위로 이동합니다. 이렇게 하면 새 규칙의 숫자 우선 순위 설정이 낮아져 규칙을 먼저 AWS WAF 평가하게 됩니다. 자세한 내용은 웹 ACL의 규칙 및 규칙 그룹 처리 순서을(를) 참조하세요.

정규 표현식 패턴 매칭 AWS WAF

AWS WAF PCRE 라이브러리에서 `libpcre` 사용하는 패턴 구문을 지원합니다. 이 라이브러리는 PCRE - Perl 호환 정규식에 문서화되어 있습니다.

AWS WAF 라이브러리의 모든 구문을 지원하지는 않습니다. 예를 들어 일부 제로 너비 어설션을 지원하지만, 모두 지원되는 것은 아닙니다. 지원되는 구문의 전체 목록은 제공하지 않습니다. 하지만 유효하지 않은 정규식 패턴을 제공하거나 지원되지 않는 구문을 사용하면 API에서 AWS WAF 오류를 보고합니다.

AWS WAF 다음 PCRE 패턴은 지원하지 않습니다.

- 역참조 및 캡처 하위식
- 서브루틴 참조 및 재귀 패턴
- 조건 패턴
- 백트래킹 제어 명령어
- \C 단일 바이트 명령
- \R 줄 바꿈 일치 명령
- \K 일치 시작 초기화 명령
- 설명선 및 포함된 코드
- 원자 그룹 지정 및 소유 수량자

IP 세트 및 정규식 패턴 세트 AWS WAF

AWS WAF 규칙에서 참조하여 사용하는 세트에 좀 더 복잡한 정보를 저장합니다. 이러한 각 집합에는 이름이 있으며 생성 시 Amazon 리소스 이름(ARN)이 할당됩니다. 규칙 문 내부에서 이러한 집합을 관리할 수 있으며. 콘솔 탐색 창을 통해 자체적으로 이를 액세스하고 관리할 수 있습니다.

규칙 그룹 또는 웹 ACL에서 관리 세트를 사용할 수 있습니다.

- IP 세트를 사용하려면 을 참조하십시오IP 집합 일치 규칙 문.
- 정규식 패턴 세트를 사용하려면 을 참조하십시오. 정규식 패턴 집합 일치 규칙 문

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 만들거나 변경하는 경우 리소스가 저장된 모든 영역에 변경 내용이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

주제

- IP 집합 생성 및 관리
- 정규식 패턴 집합 생성 및 관리

IP 집합 생성 및 관리

IP 집합은 규칙 문에서 함께 사용할 IP 주소 및 IP 주소 범위의 모음을 제공합니다. IP 세트는 AWS 리소스입니다.

웹 ACL 또는 규칙 그룹에서 IP 세트를 사용하려면 먼저 주소 사양을 `IPSet` 사용하여 AWS 리소스를 생성합니다. 그런 다음 IP 집합 규칙 문을 웹 ACL 또는 규칙 그룹에 추가할 때 해당 집합을 참조합니다.

주제

IP 집합 생성

이 단원의 절차에 따라 새 IP 집합을 생성합니다.

> **Note**
>
> 이 단원의 절차 외에도 웹 ACL 또는 규칙 그룹에 IP 일치 규칙을 추가할 때 새 IP 집합을 추가할 수 있는 옵션이 있습니다. 이 옵션을 선택하면 이 절차에 필요한 설정과 동일한 설정을 제공해야 합니다.

IP 집합을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 IP sets(IP 집합)과 Create IP set(IP 집합 생성)을 차례로 선택합니다.
3. IP 집합의 이름과 설명을 입력합니다. 이름과 설명은 사용 시 집합을 식별하는데 사용됩니다.

   > **Note**
   >
   > IP 집합을 생성한 후에는 이름을 변경할 수 없습니다.

4. 지역의 경우 글로벌 (CloudFront) 을 선택하거나 IP 세트를 저장할 지역을 선택합니다. 지리적 리소스를 보호하는 웹 ACL에서만 지역적 IP 세트를 사용할 수 있습니다. Amazon CloudFront 배포를 보호하는 웹 ACL에 설정된 IP를 사용하려면 Global () CloudFront 을 사용해야 합니다.
5. IP version(IP 버전)의 경우 사용할 버전을 선택합니다.
6. IP 주소 텍스트 상자에 CIDR 표기법으로 한 줄에 IP 주소 또는 IP 주소 범위를 하나씩 입력합니다. AWS WAF 를 제외한 모든 IPv4 및 IPv6 CIDR 범위를 지원합니다. `/0` CIDR 표기법에 대한 자세한 내용은 클래스 없는 도메인 간 라우팅에 대한 Wikipedia 문서를 참조하세요.

여기 몇 가지 예가 있습니다:

- IPv4 주소 192.0.2.44를 지정하려면 [192.0.2.44/32]를 입력합니다.
- IPv6 주소 2620:0:2d0:200:0:0:0:0을 지정하려면 2620:0:2d0:200:0:0:0:0/128을 입력합니다.
- 192.0.2.0부터 192.0.2.255까지의 IPv4 주소 범위를 지정하려면 [192.0.2.0/24]를 입력합니다.
- 2620:0:2d0:200:0:0:0:0부터 2620:0:2d0:200:ffff:ffff:ffff:ffff까지의 IPv6 주소 범위를 지정하려면 [2620:0:2d0:200::/64]를 입력합니다.

7. IP 집합에 대한 설정을 검토하고 Create IP set(IP 집합 생성)을 선택합니다.

IP 집합 삭제

참조된 집합을 삭제하려면 이 단원의 지침을 따르십시오.

참조된 세트 및 규칙 그룹 삭제

IP 세트, 정규식 패턴 세트 또는 규칙 그룹과 같이 웹 ACL에서 사용할 수 있는 엔티티를 삭제하면 해당 엔티티가 현재 웹 ACL에서 사용되고 AWS WAF 있는지 확인합니다. 사용 중인 것으로 확인되면 경고를 표시합니다. AWS WAF AWS WAF 웹 ACL에서 엔티티를 참조하고 있는지 여부를 거의 항상 확인할 수 있습니다. 그러나 드물지만 이러한 작업을 수행할 수 없는 경우도 있습니다. 현재 아무 것도 엔티티를 사용하고 있지 않음을 확인해야 하는 경우에는 해당 엔티티를 삭제하기 전에 해당 웹 ACL에서 확인하십시오. 엔티티가 참조된 세트인 경우에도 어떤 규칙 그룹도 해당 엔티티를 사용하고 있지 않음을 확인합니다.

IP 집합을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 IP sets(IP 집합)를 선택합니다.
3. 삭제하려는 IP 집합을 선택하고 삭제를 선택합니다.

정규식 패턴 집합 생성 및 관리

정규식 패턴 집합은 규칙 문에서 함께 사용할 정규 표현식 모음을 제공합니다. Regex 패턴 세트는 리소스입니다. AWS

웹 ACL 또는 규칙 그룹에서 정규식 패턴 세트를 사용하려면 먼저 정규식 패턴 사양을 `RegexPatternSet` 사용하여 AWS 리소스를 생성해야 합니다. 그런 다음 regex 패턴 세트 규칙 문을

웹 ACL 또는 규칙 그룹에 추가할 때 해당 집합을 참조합니다. 정규식 패턴 집합에는 하나 이상의 정규식 패턴이 포함되어야 합니다.

정규식 패턴 집합에 둘 이상의 정규식 패턴이 포함되어 있으면 규칙에서 사용될 때 패턴 일치가 OR 로직과 결합됩니다. 즉, 요청 구성 요소가 집합의 패턴 중 하나와 일치하는 경우 웹 요청은 패턴 집합 규칙문과 일치하게 됩니다.

AWS WAF PCRE 라이브러리에서 사용하는 패턴 구문을 지원합니다. 단, 몇 가지 예외가 있습니다. `libpcre` 이 라이브러리는 PCRE - Perl 호환 정규식에 문서화되어 있습니다. AWS WAF 지원에 대한 자세한 내용은 을 참조하십시오정규 표현식 패턴 매칭 AWS WAF.

주제

- 정규식 패턴 집합 생성
- 정규식 패턴 집합 삭제

정규식 패턴 집합 생성

이 단원의 절차에 따라 새 정규식 패턴 집합을 생성합니다.

정규식 패턴 집합을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 Regex pattern sets(정규식 패턴 집합)을 선택한 다음 Create regex pattern set(정규식 패턴 집합 생성)을 선택합니다.
3. 정규식 패턴 집합의 이름과 설명을 입력합니다. 집합을 사용하고자 할 때 이름과 설명을 사용해 식별합니다.

   > **Note**
   >
   > 정규식 패턴 집합을 생성한 후에는 이름을 변경할 수 없습니다.

4. 지역의 경우 글로벌 (CloudFront) 을 선택하거나 정규식 패턴 세트를 저장할 지역을 선택합니다. 지리적 리소스를 보호하는 웹 ACL에서만 리전 정규식 패턴 세트를 사용할 수 있습니다. Amazon CloudFront 배포를 보호하는 웹 ACL에 설정된 정규식 패턴을 사용하려면 Global () 을 사용해야 합니다. CloudFront
5. Regular expressions(정규 표현식) 텍스트 상자에 한 줄당 하나의 정규식 패턴을 입력합니다.

예를 들어, 정규식 `I[a@]mAB[a@]dRequest`는 `IamABadRequest`, `IamAB@dRequest`, `I@mABadRequest` 및 `I@mAB@dRequest` 문자열과 일치합니다.

AWS WAF 일부 예외를 제외하고 PCRE 라이브러리에서 사용하는 패턴 구문을 지원합니다. `libpcre` 이 라이브러리는 PCRE - Perl 호환 정규식에 문서화되어 있습니다. AWS WAF 지원에 대한 자세한 내용은 을 참조하십시오정규 표현식 패턴 매칭 AWS WAF.

6. 정규식 패턴 집합에 대한 설정을 검토하고 Create regex pattern set(정규식 패턴 집합 생성)을 선택합니다.

정규식 패턴 집합 삭제

참조된 집합을 삭제하려면 이 단원의 지침을 따르십시오.

참조된 세트 및 규칙 그룹 삭제

IP 세트, 정규식 패턴 세트 또는 규칙 그룹과 같이 웹 ACL에서 사용할 수 있는 엔티티를 삭제하면 해당 엔티티가 현재 웹 ACL에서 사용되고 AWS WAF 있는지 확인합니다. 사용 중인 것으로 확인되면 경고를 표시합니다. AWS WAF AWS WAF 웹 ACL에서 엔티티를 참조하고 있는지 여부를 거의 항상 확인할 수 있습니다. 그러나 드물지만 이러한 작업을 수행할 수 없는 경우도 있습니다. 현재 아무 것도 엔티티를 사용하고 있지 않음을 확인해야 하는 경우에는 해당 엔티티를 삭제하기 전에 해당 웹 ACL에서 확인하십시오. 엔티티가 참조된 세트인 경우에도 어떤 규칙 그룹도 해당 엔티티를 사용하고 있지 않음을 확인합니다.

정규식 패턴 집합을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 Regex pattern sets(정규식 패턴 집합)를 선택합니다.
3. 삭제하려는 정규식 패턴 집합을 선택하고 삭제를 선택합니다.

AWS WAF의 사용자 지정된 웹 요청 및 응답

AWS WAF 규칙 작업과 기본 웹 ACL 작업에 사용자 지정 웹 요청 및 응답 처리 동작을 추가할 수 있습니다. 연결된 작업이 적용될 때마다 사용자 지정 설정이 적용됩니다.

다음과 같은 방법으로 웹 요청 및 응답을 사용자 지정할 수 있습니다.

- Allow, Count, CAPTCHA 및 Challenge 작업을 사용하여 웹 요청에 사용자 지정 헤더를 삽입할 수 있습니다. AWS WAF 에서 웹 요청을 보호된 리소스에 전달할 때 해당 요청에 원래 요청 전체와 삽입한 사용자 지정 헤더가 포함됩니다. CAPTCHA 및 Challenge 작업의 경우 AWS WAF 는 요청이 CAPTCHA 또는 챌린지 토큰 검사를 통과하는 경우에만 사용자 지정을 적용합니다.

- Block 작업을 사용하면 응답 코드, 헤더, 본문이 포함된 완전한 사용자 지정 응답을 정의할 수 있습니다. 보호된 리소스는 에서 제공하는 사용자 지정 응답을 사용하여 요청에 응답합니다. AWS WAF사용자 지정 응답은 `403 (Forbidden)`의 기본 Block 작업 응답을 대체합니다.

사용자 지정할 수 있는 작업 설정

다음 작업 설정을 정의할 때 사용자 지정 요청 또는 응답을 지정할 수 있습니다.

- 규칙 작업. 자세한 내용은 규칙 작업을 참조하세요.
- 웹 ACL에 대한 기본 작업입니다. 자세한 내용은 웹 ACL 기본 동작을 참조하세요.

사용자 지정할 수 없는 작업 설정

웹 ACL에서 사용하는 규칙 그룹에 대한 재정의 작업에서는 사용자 지정 요청 처리를 지정할 수 없습니다. 웹 ACL 규칙 및 규칙 그룹 평가 섹션을 참조하십시오. 관리형 규칙 그룹 문 및 규칙 그룹 문도 참조하세요.

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 생성하거나 변경하는 경우 리소스가 저장된 모든 영역에 변경 내용이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

사용자 지정 요청 및 응답 사용 제한

AWS WAF 사용자 지정 요청 및 응답 사용에 대한 최대 설정을 정의합니다. 예: 웹 ACL 또는 규칙 그룹당 최대 요청 헤더 수, 단일 사용자 지정 응답 정의의 최대 사용자 지정 헤더 수. 자세한 내용은 AWS WAF 할당량 섹션을 참조하세요.

주제

- 차단되지 않은 작업에 대해 사용자 지정 요청 헤더 삽입
- Block 작업에 대한 사용자 지정 응답
- 사용자 지정 응답에 지원되는 상태 코드

차단되지 않은 작업에 대해 사용자 지정 요청 헤더 삽입

규칙 동작으로 요청이 차단되지 않는 경우 원본 HTTP 요청에 사용자 지정 헤더를 AWS WAF 삽입하도록 지시할 수 있습니다. 이 옵션을 사용하면 요청에만 추가할 수 있습니다. 원본 요청의 어떤 부분도 수정하거나 교체할 수 없습니다. 사용자 지정 헤더 삽입의 사용은 예를 들면, 삽입된 헤더에 따라 요청을 다르게 처리하도록 다운스트림 애플리케이션에 신호를 보내는 경우나 분석을 위해 요청에 플래그를 지정하는 경우입니다.

이 옵션은 Allow, Count, CAPTCHA 및 Challenge 규칙 작업과 Allow로 설정된 웹 ACL 기본 작업에 적용됩니다. 규칙 작업에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요. 기본 웹 ACL 작업에 대한 자세한 내용은 웹 ACL 기본 동작 섹션을 참조하세요.

사용자 지정 요청 헤더 이름

AWS WAF 이미 요청에 있는 헤더와 혼동되지 않도록 삽입되는 모든 요청 헤더에 접두사를 붙입니다. `x-amzn-waf-` 예를 들어, 헤더 이름을 `sample` 지정하는 경우 헤더가 AWS WAF 삽입됩니다. `x-amzn-waf-sample`

이름이 같은 헤더

요청에 삽입 중인 것과 동일한 이름의 헤더가 이미 있는 AWS WAF 경우 헤더를 AWS WAF 덮어씁니다. 따라서 이름이 동일한 여러 규칙에서 헤더를 정의하는 경우 요청을 검사하고 일치하는 항목을 찾는 마지막 규칙에 헤더가 추가되고 이전 규칙에는 헤더가 추가되지 않습니다.

비종료 규칙 작업이 포함된 사용자 지정 헤더

Allow작업과 달리 Count 작업은 웹 ACL의 나머지 규칙을 사용하여 웹 요청을 처리하는 AWS WAF 것을 중단하지 않습니다. 마찬가지로 요청 토큰이 유효하다고 Challenge 판단되는 경우에도 CAPTCHA

이러한 작업은 웹 요청 처리를 AWS WAF 중단하지 않습니다. 따라서 이러한 작업 중 하나와 함께 규칙을 사용하여 사용자 지정 헤더를 삽입하면 후속 규칙에서도 사용자 지정 헤더가 삽입될 수 있습니다. 규칙 작업 동작에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.

예를 들어 규칙의 우선 순위가 다음과 같다고 가정해 보겠습니다.

1. Count 작업과 `RuleAHeader` 이름의 사용자 지정 헤더가 있는 RuleA.
2. Allow 작업과 `RuleBHeader` 이름의 사용자 지정 헤더가 있는 RuleB.

요청이 RuleA와 RuleB와 모두 일치하는 경우 헤더와 `x-amzn-waf-RuleAHeader` RuleB를 AWS WAF 삽입한 다음 요청을 보호된 리소스에 전달합니다. `x-amzn-waf-RuleBHeader`

AWS WAF 요청 검사가 완료되면 웹 요청에 사용자 지정 헤더를 삽입합니다. 따라서 Count로 설정된 작업을 포함하는 규칙과 함께 사용자 지정 요청 처리를 사용하는 경우 추가하는 사용자 지정 헤더는 후속 규칙에서 검사되지 않습니다.

사용자 지정 요청 처리 예제

규칙의 작업 또는 웹 ACL의 기본 작업에 대한 사용자 지정 요청 처리를 정의합니다. 다음 목록은 웹 ACL의 기본 작업에 추가된 사용자 지정 처리를 위한 JSON을 보여줍니다.

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
 "Description": "Sample web ACL with custom request handling configured for default
 action.",
```

```
  "Rules": [],
  "VisibilityConfig": {
   "SampledRequestsEnabled": true,
   "CloudWatchMetricsEnabled": true,
   "MetricName": "SampleWebACL"
  }
}
```

Block 작업에 대한 사용자 지정 응답

로 설정된 규칙 작업 또는 웹 ACL 기본 작업에 대해 사용자 지정 HTTP 응답을 클라이언트에 다시 AWS WAF 보내도록 지시할 수 있습니다. Block 규칙 작업에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요. 기본 웹 ACL 작업에 대한 자세한 내용은 웹 ACL 기본 동작 섹션을 참조하세요.

Block 작업에 대한 사용자 지정 응답 처리를 정의할 때는 상태 코드, 헤더 및 응답 본문을 정의합니다. 함께 AWS WAF사용할 수 있는 상태 코드 목록은 다음 섹션을 참조하십시오. 사용자 지정 응답에 지원되는 상태 코드

사용 사례

사용자 지정 응답의 사용 예는 다음과 같습니다.

- 기본 상태 코드가 아닌 상태 코드를 다시 클라이언트로 보내는 경우
- 클라이언트에 사용자 지정 응답을 다시 보냅니다. `content-type`이라는 이름을 제외하고 모든 헤더 이름을 지정할 수 있습니다.
- 정적 오류 페이지를 클라이언트로 다시 보내는 경우
- 클라이언트를 다른 URL로 리디렉션하는 경우. 이렇게 하려면 `3xx` 리디렉션 상태 코드(예: `301 (Moved Permanently)` 또는`302 (Found)`) 중 하나를 지정한 다음 새 URL을 포함하는 `Location` 이름이 지정된 새 헤더를 지정합니다.

보호된 리소스에서 정의한 응답과의 상호 작용

AWS WAF Block작업에 대해 지정하는 사용자 지정 응답은 보호 리소스에 정의한 모든 응답 사양보다 우선합니다.

보호하는 데 사용하는 AWS 리소스의 호스트 서비스에서 웹 요청에 대한 사용자 지정 응답 처리를 AWS WAF 허용할 수 있습니다. 예는 다음과 같습니다.

- CloudFrontAmazon에서는 상태 코드를 기반으로 오류 페이지를 사용자 지정할 수 있습니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 사용자 지정 오류 응답 생성을 참조하십시오.

- Amazon API Gateway를 사용하면 게이트웨이에 대한 응답 및 상태 코드를 정의할 수 있습니다. 자세한 내용을 알아보려면 Amazon API Gateway 개발자 안내서의 API Gatewaydml 게이트웨이 응답 섹션을 참조하세요.

AWS WAF 사용자 지정 응답 설정을 보호된 AWS 리소스의 사용자 지정 응답 설정과 결합할 수 없습니다. 개별 웹 요청에 대한 응답 사양은 전적으로 AWS WAF 에서 또는 전적으로 보호된 리소스에서 가져옵니다.

AWS WAF 차단되는 웹 요청의 경우 우선 순위는 다음과 같습니다.

1. AWS WAF 사용자 지정 응답 - AWS WAF Block 작업에 사용자 지정 응답이 활성화된 경우 보호된 리소스는 구성된 사용자 지정 응답을 클라이언트에 다시 보냅니다. 보호된 리소스 자체에 정의했을 수 있는 응답 설정은 아무런 영향을 미치지 않습니다.
2. 보호된 리소스에 정의된 사용자 지정 응답 - 그렇지 않고 보호된 리소스에 사용자 지정 응답 설정이 지정된 경우 보호된 리소스는 이러한 설정을 사용하여 클라이언트에 응답합니다.
3. AWS WAF 기본 Block 응답 - 그렇지 않으면 보호된 리소스가 AWS WAF 기본 응답으로 클라이언트에 Block `403 (Forbidden)` 응답합니다.

AWS WAF 허용하는 웹 요청의 경우 보호된 리소스의 구성에 따라 클라이언트에 다시 보내는 응답이 결정됩니다. 허용된 요청에 AWS WAF 대해서는 응답 설정을 구성할 수 없습니다. 허용된 요청에 AWS WAF 대해 구성할 수 있는 유일한 사용자 지정은 요청을 보호된 리소스에 전달하기 전에 원래 요청에 사용자 지정 헤더를 삽입하는 것뿐입니다. 이 내용은 이전 섹션 차단되지 않은 작업에 대해 사용자 지정 요청 헤더 삽입에 설명되어 있습니다.

사용자 지정 응답 헤더

`content-type`이라는 이름을 제외하고 모든 헤더 이름을 지정할 수 있습니다.

사용자 지정 응답 본문

사용자 지정 응답을 사용하려는 웹 ACL 또는 규칙 그룹의 컨텍스트 내에서 사용자 지정 응답의 본문을 정의합니다. 사용자 지정 응답 본문을 정의한 후에는 이 본문을 생성했던 웹 ACL 또는 규칙 그룹 어디에서든 해당 본문을 참조로 사용할 수 있습니다. 개별 Block 작업 설정에서 사용할 사용자 지정 본문을 참조하고 사용자 지정 응답의 상태 코드와 헤더를 정의합니다.

콘솔에서 사용자 지정 응답을 생성할 때 이미 정의한 응답 본문 중에서 선택하거나 새 본문을 작성할 수 있습니다. 콘솔 외부에서는 웹 ACL 또는 규칙 그룹 수준에서 사용자 지정 응답 본문을 정의한 다음 웹 ACL 또는 규칙 그룹 내의 작업 설정에서 해당 본문을 참조합니다. 이 항목은 다음 섹션의 JSON 예제에 나와 있습니다.

사용자 지정 응답 예제

다음 예제는 사용자 지정 응답 설정이 있는 규칙 그룹의 JSON 목록입니다. 사용자 지정 응답 본문은 전체 규칙 그룹에 대해 정의된 후 규칙 작업에서 키를 사용하여 참조됩니다.

```
{
 "ARN": "test_rulegroup_arn",
 "Capacity": 1,

 "CustomResponseBodies": {
  "CustomResponseBodyKey1": {
   "Content": "This is a plain text response body.",
   "ContentType": "TEXT_PLAIN"
  }
 },

 "Description": "This is a test rule group.",
 "Id": "test_rulegroup_id",
 "Name": "TestRuleGroup",

 "Rules": [
  {
   "Action": {
    "Block": {
     "CustomResponse": {
      "CustomResponseBodyKey": "CustomResponseBodyKey1",
      "ResponseCode": 404,
      "ResponseHeaders": [
       {
        "Name": "BlockActionHeader1Name",
        "Value": "BlockActionHeader1Value"
       }
      ]
     }
    }
   },
   "Name": "GeoMatchRule",
   "Priority": 1,
   "Statement": {
    "GeoMatchStatement": {
     "CountryCodes": [
      "US"
     ]
    }
```

```
    },
    "VisibilityConfig": {
     "CloudWatchMetricsEnabled": true,
     "MetricName": "TestRuleGroupReferenceMetric",
     "SampledRequestsEnabled": true
    }
   }
  ],
  "VisibilityConfig": {
   "CloudWatchMetricsEnabled": true,
   "MetricName": "TestRuleGroupMetric",
   "SampledRequestsEnabled": true
  }
}
```

사용자 지정 응답에 지원되는 상태 코드

HTTP 상태 코드에 대한 자세한 내용은 IETF(Internet Engineering Task Force)의 상태 코드 및 Wikipedia의 HTTP 상태 코드 목록을 참조하세요.

다음은 사용자 지정 응답을 AWS WAF 지원하는 HTTP 상태 코드입니다.

- 2xx Successful
  - 200 – OK
  - 201 – Created
  - 202 – Accepted
  - 204 – No Content
  - 206 – Partial Content
- 3xx Redirection
  - 300 – Multiple Choices
  - 301 – Moved Permanently
  - 302 – Found
  - 303 –See Other
  - 304 – Not Modified
  - 307 – Temporary Redirect
  - 308 – Permanent Redirect
- 4xx Client Error

  - 400 – Bad Request
  - 401 – Unauthorized
  - 403 – Forbidden
  - 404 – Not Found
  - 405 – Method Not Allowed
  - 408 – Request Timeout
  - 409 – Conflict
  - 411 – Length Required
  - 412 – Precondition Failed
  - 413 – Request Entity Too Large
  - 414 – Request-URI Too Long
  - 415 – Unsupported Media Type
  - 416 – Requested Range Not Satisfiable
  - 421 – Misdirected Request
  - 429 – Too Many Requests
- 5xx Server Error
  - 500 – Internal Server Error
  - 501 – Not Implemented
  - 502 – Bad Gateway
  - 503 – Service Unavailable
  - 504 – Gateway Timeout
  - 505 – HTTP Version Not Supported

AWS WAF 웹 요청의 레이블

레이블은 규칙이 요청과 일치할 때 규칙에 의해 웹 요청에 추가되는 메타데이터입니다. 추가된 레이블은 웹 ACL 평가가 종료될 때까지 요청에서 계속 사용할 수 있습니다. 레이블 일치 문을 사용하여 웹 ACL 평가에서 나중에 실행되는 규칙의 레이블에 액세스할 수 있습니다. 자세한 내용은 레이블 일치 규칙 문단원을 참조하세요.

웹 요청의 레이블은 Amazon CloudWatch 레이블 메트릭을 생성합니다. 지표 및 차원 목록은 레이블 지표 및 차원 섹션을 참조하세요. 콘솔을 통해 또는 AWS WAF 콘솔을 통해 CloudWatch 지표 및 지표 요약에 액세스하는 방법에 대한 자세한 내용은 을 참조하십시오모니터링 및 조정.

레이블 사용 사례

AWS WAF 레이블의 일반적인 사용 사례는 다음과 같습니다.

- 요청에 조치를 취하기 전에 여러 규칙 명령문을 기준으로 웹 요청 평가 — 웹 ACL에서 규칙과 일치하는 항목을 찾은 후 규칙 작업으로 웹 ACL 평가가 종료되지 않으면 웹 ACL을 기준으로 요청을 AWS WAF 계속 평가합니다. 요청을 허용하거나 차단하기로 결정하기 전에 레이블을 사용하여 여러 규칙의 정보를 평가하고 수집할 수 있습니다. 이렇게 하려면 기존 규칙의 작업을 Count로 변경하고 일치하는 요청에 레이블을 추가하도록 구성합니다. 그런 다음 다른 규칙 다음에 실행할 하나 이상의 새 규칙을 추가하고 레이블 일치 조합에 따라 레이블을 평가하고 요청을 관리합니다.
- 지리적 리전별 웹 요청 관리 - 지리적 일치 규칙만 사용하여 오리진 국가별로 웹 요청을 관리할 수 있습니다. 위치를 리전 수준으로 세밀하게 조정하려면 Count 작업 뒤에 레이블 일치 규칙이 오는 지역 일치 규칙을 사용합니다. 지역 일치 규칙에 대한 자세한 내용은 지리적 일치 규칙 문 섹션을 참조하세요.
- 여러 규칙에서 로직 재사용 - 여러 규칙에서 동일한 로직을 재사용해야 하는 경우 레이블을 사용하여 로직을 단일 소싱하고 결과만 테스트할 수 있습니다. 중첩 규칙 명령문의 공통 하위 집합을 사용하는 복잡한 규칙이 여러 개 있는 경우 복잡한 규칙 전체에 공통 규칙 집합을 복제하면 시간이 많이 걸리고 오류가 발생하기 쉽습니다. 레이블을 사용하면 일치하는 요청의 수를 계산하고 이들 요청에 레이블을 추가하는 공통 규칙 하위 집합을 사용하여 새 규칙을 만들 수 있습니다. 새 규칙을 웹 ACL에 추가하여 원래의 복잡한 규칙보다 먼저 실행되도록 합니다. 그런 다음 원래 규칙에서 공유된 규칙 하위 집합을 레이블을 확인하는 단일 규칙으로 대체합니다.

  예를 들어 로그인 경로에만 적용하려는 규칙이 여러 개 있다고 가정해 보겠습니다. 각 규칙에 잠재적 로그인 경로와 일치시킬 동일한 로직을 지정하는 대신, 해당 로직을 포함하는 새 규칙 하나를 구현할 수 있습니다. 새 규칙에서 일치하는 요청에 레이블을 추가하여 로그인 경로에 대한 요청임을 나타냅니다. 웹 ACL에서 이 새 규칙에 원래 규칙보다 낮은 숫자 우선 순위 설정을 지정하여 먼저 실행되도록 합니다. 그런 다음 원래 규칙에서 공유 로직을 레이블 유무 검사로 대체합니다. 우선 순위 설정에 대한 자세한 내용은 웹 ACL의 규칙 및 규칙 그룹 처리 순서 섹션을 참조하세요.
- 규칙 그룹의 규칙에 대한 예외 생성 - 이 옵션은 보거나 변경할 수 없는 관리형 규칙 그룹에 특히 유용합니다. 많은 관리형 규칙 그룹 규칙은 일치하는 웹 요청에 레이블을 추가하여 일치하는 규칙을 표시하고 해당 일치에 대한 추가 정보를 제공합니다. 요청에 레이블을 추가하는 규칙 그룹을 사용하는 경우 일치 항목 수를 계산하도록 규칙 그룹 규칙을 재정의하고 나서, 규칙 그룹 이후에 규칙 그룹 레이블에 기반하여 웹 요청을 처리하는 규칙을 실행합니다. 모든 AWS 관리형 규칙은 일치하는 웹 요

청에 레이블을 추가합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록의 규칙 설명을 참조하세요.

- 레이블 지표를 사용하여 트래픽 패턴 모니터링 - 규칙을 통해 추가한 레이블의 지표와 웹 ACL에서 사용하는 관리형 규칙 그룹에서 추가한 지표에 액세스할 수 있습니다. 모든 AWS 관리형 규칙 그룹은 평가하는 웹 요청에 레이블을 추가합니다. 레이블 지표 및 차원 목록은 레이블 지표 및 차원 섹션을 참조하세요. 콘솔의 웹 ACL 페이지를 통하거나 이를 통해 지표 CloudWatch 및 지표 요약에 액세스할 수 있습니다. AWS WAF 자세한 내용은 모니터링 및 조정 섹션을 참조하세요.

AWS WAF 라벨링 작동 방식

규칙이 웹 요청과 일치하는 경우 규칙에 레이블이 정의되어 있으면 규칙 평가 종료 시 요청에 레이블을 AWS WAF 추가합니다. 웹 ACL에서 일치하는 규칙 다음에 평가되는 규칙이 일치하는 규칙에서 추가한 레이블과 일치할 수 있습니다.

요청에 레이블을 추가하는 요소

요청을 평가하는 웹 ACL 구성 요소는 요청에 레이블을 추가할 수 있습니다.

- 규칙 그룹 참조 문이 아닌 모든 규칙은 일치하는 웹 요청에 레이블을 추가할 수 있습니다. 레이블 지정 기준은 규칙 정의의 일부이며, 웹 요청이 규칙과 일치하면 규칙의 레이블이 요청에 AWS WAF 추가됩니다. 자세한 내용은 the section called “라벨을 추가하는 규칙”을 참조하세요.
- 지역 일치 규칙 문은 결과에 일치하는 문이 있는지 여부와 관계없이 검사하는 모든 요청에 국가 및 리전 레이블을 추가합니다. 자세한 내용은 the section called “지리적 일치”을 참조하세요.
- AWS WAF 모든 AWS 관리형 규칙은 검토하는 요청에 레이블을 추가합니다. 이러한 관리형 규칙은 규칙 그룹의 규칙 일치를 기반으로 일부 레이블을 추가하고 지능형 위협 완화 규칙 그룹을 사용할 때 추가되는 토큰 레이블 지정과 같이 관리형 규칙 그룹이 사용하는 AWS 프로세스에 기반하여 또 다른 일부 레이블을 추가합니다. 각 관리형 규칙 그룹에서 추가하는 레이블에 대한 자세한 내용은 the section called “AWS 관리형 규칙 규칙 그룹 목록” 섹션을 참조하세요.

라벨 AWS WAF 관리 방법

AWS WAF 규칙의 요청 검사가 끝날 때 규칙 레이블을 요청에 추가합니다. 레이블 지정은 작업과 마찬가지로 규칙 일치 활동의 일부입니다.

웹 ACL 평가가 종료된 후에는 레이블이 웹 요청과 함께 유지되지 않습니다. 규칙에서 추가한 레이블과 다른 규칙을 일치시키려면 규칙 작업에서 웹 ACL에 의한 웹 요청 평가가 종료되지 않아야 합니다. 규칙 작업은 Count, CAPTCHA 또는 Challenge로 설정해야 합니다. 웹 ACL 평가가 종료되지 않으면 웹

ACL의 후속 규칙이 요청에 대해 해당 레이블 일치 조건을 실행할 수 있습니다. 규칙 작업에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.

웹 ACL 평가 중 레이블에 액세스

추가된 AWS WAF 레이블은 웹 ACL을 기준으로 요청을 평가하는 한 요청에서 계속 사용할 수 있습니다. 웹 ACL의 모든 규칙은 동일한 웹 ACL에서 이미 실행된 규칙에 의해 추가된 레이블에 액세스할 수 있습니다. 여기에는 웹 ACL 내에서 직접 정의된 규칙과 웹 ACL에서 사용되는 규칙 그룹 안에 정의된 규칙이 포함됩니다.

- 레이블 일치 문을 사용하여 규칙의 요청 검사 기준에서 레이블을 일치시킬 수 있습니다. 요청에 연결된 모든 레이블과 일치시킬 수 있습니다. 명령문에 대한 자세한 내용은 레이블 일치 규칙 문 섹션을 참조하세요.
- 지리적 일치 문은 일치 여부와 무관하게 레이블을 추가하지만 명령문의 포함 웹 ACL 규칙이 요청 평가를 완료한 후에만 사용할 수 있습니다.
  - 단일 규칙(예: AND 논리문)을 사용하여 지리적 레이블에 대해 지역 일치 문을 실행하고 나서 레이블 일치 문을 실행할 수는 없습니다. 지역 일치 문이 포함된 규칙 다음에 실행되는 별도의 규칙에 레이블 일치 문을 추가해야 합니다.
  - 속도 기반 규칙 문 또는 관리형 규칙 그룹 참조 문 내에서 지역 일치 문을 범위 축소 문으로 사용하는 경우 포함 규칙 문에서 지역 일치 문이 추가하는 레이블을 검사할 수 없습니다. 속도 기반 규칙 문 또는 규칙 그룹에서 지리적 레이블 지정을 검사해야 하는 경우 이전에 실행되는 별도의 규칙에서 지리적 일치 문을 실행해야 합니다.

웹 ACL 평가 이외의 레이블 정보에 대한 액세스

웹 ACL 평가가 종료된 후에는 레이블이 웹 요청과 함께 유지되지 않지만 AWS WAF 는 로그와 지표에 레이블 정보를 기록합니다.

- AWS WAF 단일 요청에서 처음 100개의 라벨에 대한 Amazon CloudWatch 메트릭을 저장합니다. 레이블 지표 액세스에 대한 자세한 내용은 아마존을 통한 모니터링 CloudWatch 및 레이블 지표 및 차원 섹션을 참조하세요.
- AWS WAF 콘솔의 웹 ACL 트래픽 개요 대시보드에 CloudWatch 레이블 지표를 요약합니다. AWS WAF 모든 웹 ACL 페이지에서 대시보드에 액세스할 수 있습니다. 자세한 정보는 웹 ACL 트래픽 개요 대시보드을 참조하세요.
- AWS WAF 요청 시 처음 100개의 레이블에 대해 로그에 레이블을 기록합니다. 레이블을 규칙 동작과 함께 사용하여 AWS WAF 에서 기록하는 로그를 필터링할 수 있습니다. 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅을 참조하세요.

웹 ACL 평가는 웹 요청에 100개 이상의 레이블을 적용하고 100개가 넘는 레이블과 대조할 수 있지만 로그와 지표에는 처음 AWS WAF 100개만 기록합니다.

AWS WAF 레이블 구문 및 이름 지정 요구 사항

레이블은 접두사, 선택적 네임스페이스 및 이름으로 구성된 문자열입니다. 레이블의 구성 요소는 콜론으로 구분됩니다. 레이블의 요구 사항 및 특성은 다음과 같습니다.

- 레이블은 대/소문자를 구분합니다.
- 각 레이블 네임스페이스 또는 레이블 이름은 최대 128자일 수 있습니다.
- 레이블에 최대 5개의 네임스페이스를 지정할 수 있습니다.
- 레이블의 구성 요소는 콜론(`:`)으로 구분됩니다.
- 레이블에 지정하는 네임스페이스나 이름에는 예약된 문자열(`awswaf`, `aws`, `waf`, `rulegroup`, `webacl`, `regexpatternset`, `ipset` 및 `managed`)을 사용할 수 없습니다.

레이블 구문

정규화된 레이블에는 접두사, 선택적 네임스페이스 및 레이블 이름이 포함됩니다. 접두사는 레이블을 추가한 규칙의 규칙 그룹 또는 웹 ACL 컨텍스트를 식별합니다. 네임스페이스는 레이블에 대한 더 많은 컨텍스트를 추가하는 데 사용될 수 있습니다. 레이블 이름은 레이블에 대한 가장 낮은 수준의 세부 정보를 제공합니다. 이는 흔히 요청에 레이블을 추가한 특정 규칙을 나타냅니다.

레이블 접두사는 오리진에 따라 다릅니다.

- 레이블 - 다음은 웹 ACL 및 규칙 그룹 규칙에서 생성하는 레이블의 전체 레이블 구문입니다. 엔터티 유형은 `rulegroup` 및 `webacl`입니다.

```
awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
 namespace>:...:<label name>
```

  - 레이블 네임스페이스 접두사: `awswaf:<entity owner account id>:<entity type>:<entity name>:`
  - 사용자 지정 네임스페이스 추가: `<custom namespace>:…:`

  규칙 그룹 또는 웹 ACL에서 규칙의 레이블을 정의하면 사용자 지정 네임스페이스 문자열과 레이블 이름을 제어할 수 있습니다. 나머지는 에서 자동으로 생성합니다 AWS WAF. AWS WAF 모든 레이블 앞에 `awswaf` 계정과 웹 ACL 또는 규칙 그룹 엔티티 설정을 자동으로 접두사로 붙입니다.

- 관리형 규칙 그룹 레이블 - 다음은 관리형 규칙 그룹의 규칙을 통해 생성되는 레이블의 전체 레이블 구문입니다.

```
awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
```

  - 레이블 네임스페이스 접두사: `awswaf:managed:<vendor>:<rule group name>:`
  - 사용자 지정 네임스페이스 추가: `<custom namespace>:…:`

  모든 AWS 관리형 규칙 그룹은 레이블을 추가합니다. 관리형 규칙 그룹에 대한 자세한 내용은 관리형 규칙 그룹 단원을 참조하세요.
- 다른 AWS 프로세스의 레이블 - 이러한 프로세스는 AWS 관리형 규칙 그룹에서 사용되므로 관리형 규칙 그룹을 사용하여 평가하는 웹 요청에 추가된 것을 확인할 수 있습니다. 다음은 관리형 규칙 그룹에서 호출하는 프로세스에 의해 생성되는 레이블의 전체 레이블 구문입니다.

```
awswaf:managed:<process>:<custom namespace>:...:<label name>
```

  - 레이블 네임스페이스 접두사: `awswaf:managed:<process>:`
  - 사용자 지정 네임스페이스 추가: `<custom namespace>:…:`

  AWS 프로세스를 호출하는 관리형 규칙 그룹에는 이 유형의 레이블이 나열됩니다. 관리형 규칙 그룹에 대한 자세한 내용은 관리형 규칙 그룹 단원을 참조하세요.

규칙의 예제 레이블

다음 예제 레이블은 111122223333 계정에 속하는 `testRules` 이름이 지정된 규칙 그룹의 규칙을 통해 정의됩니다.

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

다음 목록은 JSON으로 작성된 예제 레이블 사양입니다. 이들 레이블 이름에는 끝 레이블 이름 앞에 사용자 지정 네임스페이스 문자열이 포함됩니다.

```
Rule: {
```

```
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> 콘솔에서 규칙 JSON 편집기를 통해 이 유형의 목록에 액세스할 수 있습니다.

위의 예제 레이블과 동일한 규칙 그룹 및 계정에서 위 규칙을 실행하면 다음과 같은 정규화된 레이블이 생성됩니다.

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

관리형 규칙 그룹의 레이블 예제

다음은 AWS 관리형 규칙 규칙 그룹 및 해당 그룹이 호출하는 프로세스의 예제 레이블을 보여줍니다.

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF 레이블을 추가하는 규칙

거의 모든 규칙에서 레이블을 정의하여 모든 매칭 요청에 적용할 수 있습니다. AWS WAF

유일한 예외는 다음과 같은 규칙 유형입니다.

- 속도 기반 규칙은 속도 제한 시에만 레이블을 지정합니다. 속도 기반 규칙은 특정 집계 인스턴스의 속도가 제한되는 동안에만 웹 요청에 레이블을 추가합니다. AWS WAF속도 기반 규칙에 대한 자세한 내용은 비율 기반 규칙 문 섹션을 참조하세요.
- 규칙 그룹 참조 명령문에는 레이블을 지정할 수 없습니다. 콘솔에서는 이러한 규칙 유형에 대한 레이블을 허용하지 않습니다. API를 통해 두 명령문 유형 중 하나에 레이블을 지정하면 유효성 검사 예외가 발생합니다. 이 문 유형에 대한 자세한 내용은 관리형 규칙 그룹 문 및 규칙 그룹 문 섹션을 참조하세요.

WCU - 웹 ACL 또는 규칙 그룹 규칙에서 정의하는 레이블 5개당 1WCU.

이를 찾을 수 있는 위치

- 콘솔의 규칙 빌더 - 규칙의 작업 설정에서 레이블 아래에 있습니다.
- API 데이터 유형 - `Rule` `RuleLabels`

레이블 네임스페이스 접두사에 추가할 사용자 지정 네임스페이스 문자열과 이름을 지정하여 규칙에 레이블을 정의합니다. AWS WAF 규칙을 정의한 컨텍스트에서 접두사를 파생합니다. 이에 대한 자세한 내용은 AWS WAF 레이블 구문 및 이름 지정 요구 사항 아래의 레이블 구문 정보를 참조하세요.

AWS WAF 레이블과 일치하는 규칙

레이블 일치 문을 사용하여 웹 요청 레이블을 평가할 수 있습니다. 레이블과 일치시키거나(레이블 이름 필요) 네임스페이스와 일치시킬 수 있습니다(네임스페이스 사양 필요). 레이블 또는 네임스페이스의 경우 사양에 이전 네임스페이스와 접두사를 선택적으로 포함할 수 있습니다. 이 문 유형에 대한 전체적인 내용은 레이블 일치 규칙 문 섹션을 참조하세요.

레이블의 접두사는 레이블 규칙이 정의된 규칙 그룹 또는 웹 ACL의 컨텍스트를 정의합니다. 규칙의 레이블 일치 문에서 레이블 또는 네임스페이스 일치 문자열에 접두사가 지정되지 않은 경우 레이블 일치 규칙의 접두사를 AWS WAF 사용합니다.

- 웹 ACL 내에서 직접 정의된 규칙의 레이블에는 웹 ACL 컨텍스트를 지정하는 접두사가 있습니다.
- 규칙 그룹 내 규칙의 레이블에는 규칙 그룹 컨텍스트를 지정하는 접두사가 있습니다. 이 컨텍스트는 사용자 고유의 규칙 그룹일 수도 있고, 사용자 대신 관리되는 규칙 그룹일 수도 있습니다.

이에 대한 자세한 내용은 AWS WAF 레이블 구문 및 이름 지정 요구 사항 아래의 레이블 구문을 참조하세요.

> **Note**
>
> 일부 관리형 규칙 그룹은 레이블을 추가합니다. `DescribeManagedRuleGroup`을 호출하여 API를 통해 레이블을 검색할 수 있습니다. 레이블은 응답의 `AvailableLabels` 속성에 나열됩니다.

해당 규칙의 컨텍스트와 다른 컨텍스트에 있는 규칙과 일치시키려면 일치 문자열에 접두사를 입력해야 합니다. 예를 들어, 관리형 규칙 그룹의 규칙에서 추가한 레이블과 일치시키려는 경우 일치 문자열이 규칙 그룹의 접두사와 이어서 추가 일치 기준을 지정하는 레이블 일치 문을 사용하여 웹 ACL에서 규칙을 추가할 수 있습니다.

레이블 일치 문의 일치 문자열에서 레이블 또는 네임스페이스를 지정합니다.

- 레이블 - 일치 항목에 대한 레이블 사양은 레이블의 끝 부분으로 이루어집니다. 레이블 이름 바로 앞에 원하는 만큼의 연속 네임스페이스를 포함하고 그 뒤에 이름을 지정할 수 있습니다. 사양을 접두사로 시작하여 정규화된 레이블을 제공할 수도 있습니다.

  예제 사양:

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- 네임스페이스 - 일치 항목에 대한 네임스페이스 사양은 이름을 제외한 레이블 사양의 연속 하위 집합으로 구성됩니다. 접두사를 포함할 수 있으며 네임스페이스 문자열을 하나 이상 포함할 수 있습니다.

  예제 사양:

  - `testNS1:testNS2:`
  - `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF 라벨 매칭 예제

이 섹션에서는 레이블 일치 규칙 문에 대한 일치 사양의 예를 제공합니다.

> **Note**
>
> 이러한 JSON 목록은 콘솔에서 레이블 일치 사양과 함께 규칙을 웹 ACL에 추가한 다음 규칙을 편집하고 나서 규칙 JSON 편집기로 전환하여 생성했습니다. API 또는 명령줄 인터페이스를 통해 규칙 그룹 또는 웹 ACL에 대한 JSON을 가져올 수도 있습니다.

주제

로컬 레이블과 일치

다음 JSON 목록은 이 규칙과 동일한 컨텍스트에서 웹 요청에 로컬로 추가된 레이블에 대한 레이블 일치 문을 보여줍니다.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

웹 ACL `testWebACL`에 대해 정의하는 규칙에서 계정 111122223333에 이 일치 문을 사용하면 다음 레이블과 일치하게 됩니다.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

레이블 문자열이 정확히 일치하지 않기 때문에 다음 레이블과 일치하지 않을 수 있습니다.

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

컨텍스트가 동일하지 않아 접두사가 일치하지 않으므로 다음 레이블과 일치하지 않을 수 있습니다. 규칙이 정의된 웹 ACL `testWebACL`에 `productionRules` 규칙 그룹을 추가한 경우에도 마찬가지입니다.

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

다른 컨텍스트의 레이블과 일치

다음 JSON 목록은 사용자가 만든 규칙 그룹 내 규칙의 레이블과 일치하는 레이블 일치 규칙을 보여줍니다. 지정된 규칙 그룹에 속하지 않는 웹 ACL에서 실행되는 모든 규칙의 사양에는 접두사가 필요합니다. 이 예제 레이블 사양은 정확한 레이블만 일치시킵니다.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

관리형 규칙 그룹 레이블과 일치

이는 일치 규칙의 레이블이 아닌 다른 컨텍스트의 레이블을 대상으로 일치시키는 특별한 경우입니다. 다음 JSON 목록은 관리형 규칙 그룹 레이블의 레이블 일치 문을 보여줍니다. 이 경우 레이블 일치 문의 키 설정에 지정된 것과 정확히 일치하는 레이블만 일치시킵니다.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
```

```
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

로컬 네임스페이스와 일치

다음 JSON 목록은 로컬 네임스페이스의 레이블 일치 문을 보여줍니다.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
    Labels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

로컬 Label 일치와 마찬가지로, 웹 ACL testWebACL에 대해 정의하는 규칙에서 계정 111122223333에 이 명령문을 사용하면 다음 레이블과 일치하게 됩니다.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

계정이 동일하지 않아 접두사가 일치하지 않으므로 다음 레이블과 일치하지 않을 수 있습니다.

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

또한 다음과 같이 접두사가 관리형 규칙 그룹에서 적용한 어떤 레이블과도 일치하지 않습니다.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

관리형 규칙 그룹 네임스페이스와 일치

다음 JSON 목록은 관리형 규칙 그룹 네임스페이스의 레이블 일치 문을 보여줍니다. 소유한 규칙 그룹의 경우 규칙 컨텍스트 외부에 있는 네임스페이스와 일치시키려면 접두사도 제공해야 합니다.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

이 사양은 다음 예제 레이블과 일치합니다.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

다음 레이블과는 일치하지 않습니다.

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF 지능형 위협 완화

이 섹션에서는 에서 제공하는 관리형 지능형 위협 완화 기능을 다룹니다. AWS WAF이러한 기능은 악성 봇 및 계정 탈취 시도와 같은 위협으로부터 보호하기 위해 구현할 수 있는 전문적인 고급 보호 기능입니다.

> **Note**
>
> 여기에 설명된 기능에는 기본 사용 요금 외에 추가 비용이 발생합니다. AWS WAF자세한 내용은 AWS WAF 요금을 참조하십시오.

이 섹션에 제공된 지침은 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 만들고 관리하는 방법을 일반적으로 알고 있는 사용자를 대상으로 합니다. 이러한 주제는 이 안내서의 이전 섹션에 설명되어 있습니다.

주제

지능형 위협 완화 옵션

이 섹션에서는 지능형 위협 완화를 구현하기 위한 옵션을 자세히 비교합니다.

AWS WAF 지능형 위협 완화를 위해 다음과 같은 유형의 보호를 제공합니다.

- AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) - 애플리케이션의 가입 페이지에서 악의적인 계정 생성 시도를 탐지하고 관리합니다. 핵심 기능은 ACFP 관리형 규칙 그룹에서 제공합니다. 자세한 내용은 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 및 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요.
- AWS WAF 사기 방지 계정 탈취 방지 (ATP) - 애플리케이션의 로그인 페이지에서 악의적인 도용 시도를 탐지하고 관리합니다. 핵심 기능은 ATP 관리형 규칙 그룹에서 제공합니다. 자세한 내용은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 및 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 섹션을 참조하세요.
- AWS WAF 봇 컨트롤 — 우호적인 봇과 악의적인 봇을 모두 식별하고 레이블을 지정하고 관리합니다. 이 기능은 애플리케이션마다 고유한 서명을 사용하는 일반 봇과 특정 애플리케이션 관련 서명이 있는 대상 봇을 관리합니다. 핵심 기능은 Bot Control 관리형 규칙 그룹에서 제공합니다. 자세한 내용은 AWS WAF 봇 컨트롤 및 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.
- 클라이언트 애플리케이션 통합 SDK — 웹 페이지에서 클라이언트 세션과 최종 사용자를 검증하고 클라이언트가 웹 AWS WAF 요청에 사용할 토큰을 획득합니다. ACFP, ATP 또는 Bot Control을 사용하는 경우, 가능하면 클라이언트 애플리케이션에서 애플리케이션 통합 SDK를 구현하여 모든 규칙 그룹 기능을 최대한 활용하십시오. 이러한 규칙 그룹은 중요한 리소스를 신속하게 보호해야 하지만 SDK 통합을 위한 시간이 충분하지 않을 때 SDK 통합 없이 임시 방편으로만 사용할 것을 권장합니다. SDK 구현에 대한 정보는 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요.

- Challenge및 CAPTCHA 규칙 조치 — 클라이언트 세션 및 최종 사용자의 유효성을 검사하고 클라이언트가 웹 요청에 사용할 AWS WAF 토큰을 획득합니다. 이러한 작업은 규칙 내 규칙 작업을 지정하는 어느 위치에든 구현할 수 있으며 사용하는 규칙 그룹에서는 재정의로 구현할 수 있습니다. 이러한 작업에는 AWS WAF JavaScript 전면 광고를 사용하여 클라이언트 또는 최종 사용자를 조사하므로 이를 지원하는 클라이언트 애플리케이션이 필요합니다. JavaScript 자세한 정보는 CAPTCHA그리고 Challenge 안에 AWS WAF을 참조하세요.

지능형 위협 완화 AWS 관리 규칙 그룹 ACFP, ATP 및 봇 컨트롤은 고급 탐지에 토큰을 사용합니다. 규칙 그룹에서 토큰이 지원하는 기능에 대한 자세한 내용은 애플리케이션 통합 SDK를 ACFP와 함께 사용해야 하는 이유, 애플리케이션 통합 SDK를 ATP와 함께 사용해야 하는 이유 및 애플리케이션 통합 SDK를 Bot Control과 함께 사용해야 하는 이유 섹션을 참조하세요.

지능형 위협 완화를 구현하기 위한 옵션은 챌린지를 실행하고 토큰 획득을 강제하기 위한 규칙 조치의 기본 사용부터 지능형 위협 완화 관리 규칙 그룹에서 제공하는 고급 기능에 이르기까지 다양합니다. AWS

다음 표는 기본 기능과 고급 기능의 옵션을 자세히 비교한 것입니다.

주제

- 챌린지 및 토큰 획득 옵션
- 지능형 위협 완화 관리 규칙 그룹 옵션
- 속도 기반 규칙 및 대상 지정 Bot Control 규칙의 속도 제한 옵션

챌린지 및 토큰 획득 옵션

AWS WAF 애플리케이션 통합 SDK 또는 규칙 조치를 Challenge 사용하여 챌린지를 제공하고 토큰을 획득할 수 있습니다. CAPTCHA 대체로 규칙 조치는 구현하기가 더 쉽지만 추가 비용이 발생하고 고객 경험에 더 많은 영향을 미치며 요구 사항이 더 많이 발생합니다. JavaScript SDK는 클라이언트 애플리케이션에서 프로그래밍해야 하지만 더 나은 고객 경험을 제공할 수 있고 무료로 사용할 수 있으며 Android 또는 iOS 애플리케이션과 함께 JavaScript 또는 Android 또는 iOS 애플리케이션에서 사용할 수 있습니다. 다음 섹션에 설명된 유료 지능형 위협 완화 관리형 규칙 그룹 중 하나를 사용하는 웹 ACL과 함께 애플리케이션 통합 SDK만 사용할 수 있습니다.

챌린지 및 토큰 획득 옵션 비교

	Challenge 규칙 작업	CAPTCHA 규칙 작업	JavaScript SDK 챌린지	모바일 SDK 챌린지
정의	브라우저 클라이언트에게 사일런트 챌린지 AWS WAF 전면 광고를 제공하여 토큰 획득을 강제하는 규칙 조치	클라이언트 최종 사용자에게 시각 또는 청각 챌린지 전면 광고를 제시하여 AWS WAF 토큰 획득을 강제하는 규칙 조치	실행되는 클라이언트 브라우저 및 기타 장치를 위한 애플리케이션 통합 계층. JavaScript 자동 챌린지를 렌더링하고 토큰 획득	Android 및 iOS 애플리케이션용 애플리케이션 통합 계층. 자동 챌린지를 기본적으로 렌더링하고 토큰 획득
적합한 용도...	봇 세션에 대한 자동 검증 및 지원하는 클라이언트에 대한 토큰 획득 적용 JavaScript	다음을 지원하는 클라이언트에 대해 봇 세션에 대한 최종 사용자 및 자동 검증 및 토큰 획득 강제 적용 JavaScript	봇 세션에 대한 자동 검증 및 지원하는 클라이언트에 대한 토큰 획득 적용 JavaScript. SDK는 지연 시간을 최소화하고 애플리케이션에서 챌린지 스크립트가 실행되는 위치를 가장 잘 제어합니다.	Android 및 iOS의 네이티브 모바일 애플리케이션에 대해 봇 세션 자동 검증 및 토큰 획득 적용. SDK는 지연 시간을 최소화하고 애플리케이션에서 챌린지 스크립트가 실행되는 위치를 가장 잘 제어합니다.
구현 고려 사항	규칙 작업 설정으로 구현됨	규칙 작업 설정으로 구현됨	하지만 웹 ACL에서 유료 규칙 그룹 ACFP, ATP 또는 Bot Control 중 하나가 필요합니다.	하지만 웹 ACL에서 유료 규칙 그룹 ACFP, ATP 또는 Bot Control 중 하나가 필요합니다.

	Challenge 규칙 작업	CAPTCHA 규칙 작업	JavaScript SDK 챌린지	모바일 SDK 챌린지
			클라이언트 애플리케이션에서 코딩 필요	클라이언트 애플리케이션에서 코딩 필요
런타임 고려 사항	유효한 토큰이 없는 요청에 대한 개입형 흐름 클라이언트는 AWS WAF 챌린지 전면 광고로 리디렉션됩니다. 네트워크 왕복을 추가하며 웹 요청에 대한 2차 평가 필요	유효한 토큰이 없는 요청에 대한 개입형 흐름 클라이언트가 AWS WAF CAPTCHA 중간 광고로 리디렉션됩니다. 네트워크 왕복을 추가하며 웹 요청에 대한 2차 평가 필요	백그라운드에서 실행 가능 챌린지 환경에 대한 보다 세부적인 제어 가능	백그라운드에서 실행 가능 챌린지 환경에 대한 보다 세부적인 제어 가능
필요 JavaScript	예	예	예	아니요
지원 클라이언트	Javascript를 실행하는 브라우저 및 디바이스	Javascript를 실행하는 브라우저 및 디바이스	Javascript를 실행하는 브라우저 및 디바이스	Android 및 iOS 기기

	Challenge 규칙 작업	CAPTCHA 규칙 작업	JavaScript SDK 챌린지	모바일 SDK 챌린지
단일 페이지 애플리케이션(SPA) 지원	적용 전용. SDK와 함께 Challenge 작업을 사용하여 요청에 유효한 챌린지 토큰이 있는지 확인할 수 있습니다. 규칙 작업을 사용하여 페이지에 챌린지 스크립트를 전달할 수 없습니다.	적용 전용. SDK와 함께 CAPTCHA 작업을 사용하여 요청에 유효한 CAPTCHA 토큰이 있는지 확인할 수 있습니다. 규칙 작업을 사용하여 페이지에 CAPTCHA 스크립트를 전달할 수 없습니다.	예	N/A
추가 요금	예. 정의하는 규칙에 명시적으로 지정하는 작업 설정의 경우 또는 사용하는 규칙 그룹에서 규칙 작업 재정의로 지정하는 경우에 적용됩니다. 그 밖의 모든 경우에는 적용되지 않습니다.	예. 정의하는 규칙에 명시적으로 지정하는 작업 설정의 경우 또는 사용하는 규칙 그룹에서 규칙 작업 재정의로 지정하는 경우에 적용됩니다. 그 밖의 모든 경우에는 적용되지 않습니다.	아니요. 하지만 유료 규칙 그룹 ACFP, ATP 또는 Bot Control 중 하나가 필요합니다.	아니요. 하지만 유료 규칙 그룹 ACFP, ATP 또는 Bot Control 중 하나가 필요합니다.

이러한 옵션과 관련된 비용에 대한 자세한 내용은 AWS WAF 요금에서 지능형 위협 완화 정보를 참조하세요.

Challenge 또는 CAPTCHA 작업을 포함하는 규칙을 추가하기만 하면 간단히 챌린지를 실행하고 기본 토큰을 적용할 수 있습니다. 예를 들어 애플리케이션 코드에 액세스할 수 없는 경우에는 규칙 작업을 사용해야 할 수도 있습니다.

하지만 SDK를 구현할 수 있으면 클라이언트 웹 요청에 대한 웹 ACL 평가 시 Challenge 작업을 사용할 때보다 비용을 절감하고 지연 시간을 줄일 수 있습니다.

- 애플리케이션의 어느 시점에서든 챌린지를 실행하도록 SDK 구현을 작성할 수 있습니다. 고객의 작업으로 보호된 리소스에 웹 요청이 전송되는 상황이 발생하기 전에 백그라운드에서 토큰을 획득할 수 있습니다. 이렇게 하면 클라이언트의 첫 번째 요청과 함께 토큰을 전송할 수 있습니다.
- 대신 Challenge 작업을 포함하는 규칙을 구현하여 토큰을 획득하는 경우, 클라이언트가 요청을 처음 전송하고 토큰이 만료될 때마다 규칙과 작업에 대한 추가 웹 요청 평가 및 처리가 필요합니다. 이 Challenge 작업은 유효하고 만료되지 않은 토큰이 없는 요청을 차단하고 챌린지 중간 광고를 다시 클라이언트에게 전송합니다. 클라이언트가 챌린지에 성공적으로 응답하면 중간 광고는 유효한 토큰과 함께 원본 웹 요청을 다시 전송하고 웹 ACL에서 이를 다시 평가합니다.

지능형 위협 완화 관리 규칙 그룹 옵션

지능형 위협 완화 AWS 관리형 규칙 규칙 그룹은 기본 봇 관리, 정교한 악성 봇의 탐지 및 완화, 계정 탈취 시도의 탐지 및 완화, 사기성 계정 생성 시도의 탐지 및 완화 기능을 제공합니다. 이러한 규칙 그룹은 이전 섹션에서 설명한 애플리케이션 통합 SDK와 결합되어 최신 보호 기능 및 클라이언트 애플리케이션과의 보안 연결을 제공합니다.

관리형 규칙 그룹 옵션 비교

	ACFP	탭	Bot Control 일반 수준	Bot Control 대상 수준
정의	애플리케이션의 등록 및 가입 페이지에서 사기 계정 생성 시도의 일부일 수 있는 요청을 관리합니다. 봇을 관리하지 않습니다. AWS WAF 사기 방지 계정 생성 사기 방지	애플리케이션의 로그인 페이지에서 악의적인 탈취 시도의 일부일 수 있는 요청을 관리합니다. 봇을 관리하지 않습니다. AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙	애플리케이션 간에 고유한 서명을 사용하는 자체 식별이 가능한 일반 봇을 관리합니다. AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하십시오.	특정 애플리케이션 관련 서명이 있는 자체 식별이 불가능한 대상 봇을 관리합니다. AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하십시오.

	ACFP	탭	Bot Control 일반 수준	Bot Control 대상 수준
	(ACFP) 규칙 그룹 섹션을 참조하십시오.	그룹 섹션을 참조하십시오.		
적합한 용도...	계정 생성 트래픽에 대해 사용자 이름 탐색을 통한 생성 시도, 단일 IP 주소에서 많은 새 계정을 생성하는 등 사기 계정 생성 공격 여부 검사	로그인 트래픽의 계정 탈취 시도 공격(예: 암호 순회를 통한 로그인 시도, 동일 IP 주소에서의 다회 로그인 시도) 여부 검사. 토큰과 함께 사용할 경우 대량의 로그인 시도 실패에 대한 IP 및 클라이언트 세션 속도 제한과 같은 종합적인 보호 기능도 제공합니다.	일반 자동 봇 트래픽에 대한 기본 봇 보호 및 레이블 지정	클라이언트 세션 수준에서의 속도 제한, Selenium 및 Puppeteer와 같은 브라우저 자동화 도구의 탐지 및 완화 등 정교한 봇에 대한 대상 보호.
평가 결과를 나타내는 레이블 추가	예	예	예	예
토큰 레이블 추가	예	예	예	예
유효한 토큰이 없는 요청 차단	포함되지 않음 유효한 AWS WAF 토큰이 없는 요청 차단 섹션을 참조하십시오.	포함되지 않음 유효한 AWS WAF 토큰이 없는 요청 차단 섹션을 참조하십시오.	포함되지 않음 유효한 AWS WAF 토큰이 없는 요청 차단 섹션을 참조하십시오.	토큰 없이 5개의 요청을 보내는 클라이언트 세션을 차단합니다.

	ACFP	탭	Bot Control 일반 수준	Bot Control 대상 수준
AWS WAF 토큰이 필요합니다. `aws-waf-token`	모든 규칙에 필요합니다. 애플리케이션 통합 SDK를 ACFP와 함께 사용해야 하는 이유 섹션을 참조하십시오.	여러 규칙에 필요합니다. 애플리케이션 통합 SDK를 ATP와 함께 사용해야 하는 이유 섹션을 참조하세요.	아니요	예
토큰을 획득합니다. AWS WAF `aws-waf-token`	예, `AllRequests` 규칙에 의해 적용됩니다.	아니요	아니요	일부 규칙은 토큰을 획득하는 Challenge 또는 CAPTCHA 규칙 작업을 사용합니다.

이러한 옵션과 관련된 비용에 대한 자세한 내용은 AWS WAF 요금에서 지능형 위협 완화 정보를 참조하세요.

속도 기반 규칙 및 대상 지정 Bot Control 규칙의 속도 제한 옵션

목표 수준의 AWS WAF Bot Control 규칙 그룹과 속도 AWS WAF 기반 규칙 설명 모두 웹 요청 속도 제한을 제공합니다. 다음은 두 옵션을 비교하는 표입니다.

속도 기반 탐지 및 완화 옵션 비교

	AWS WAF 속도 기반 규칙	AWS WAF 봇 컨트롤 대상 규칙	
속도 제한 적용 방법	너무 빠른 속도로 들어오는 요청 그룹에 조치를 취합니다. 를 제외한 모든 작업을 적용할 수 Allow 있습니다.	요청 토큰을 사용하여 사람과 유사한 액세스 패턴과 동적 속도 제한을 적용합니다.	

	AWS WAF 속도 기반 규칙	AWS WAF 봇 컨트롤 대상 규칙	
과거 트래픽 기준 기반 여부	아니요	예	
과거 트래픽 기준이 축적되는 데 필요한 시간	N/A	동적 임계값의 경우 5분. 토큰이 없는 경우에는 해당되지 않습니다.	
완화 지연	보통 30-50초입니다. 최대 몇 분이 걸릴 수 있습니다.	일반적으로 10초 미만 최대 몇 분이 걸릴 수 있습니다.	
완화 목표	구성 가능. 범위 축소 명령문을 사용하고 하나 이상의 집계 키 (예: IP 주소, HTTP 메서드, 쿼리 문자열) 를 사용하여 요청을 그룹화할 수 있습니다.	IP 주소 및 클라이언트 세션	
완화 조치를 트리거하는 데 필요한 트래픽 볼륨 수준	중간 - 지정된 기간 내에 요청을 100개까지 줄일 수 있습니다.	낮음 - 느린 스크레이퍼와 같은 클라이언트 패턴을 탐지하기 위해서입니다.	
사용자 지정 가능한 임계값	예	아니요	

	AWS WAF 속도 기반 규칙	AWS WAF 봇 컨트롤 대상 규칙	
기본 완화 작업	콘솔 기본값은 Block입니다. API에는 기본 설정이 없으므로 설정해야 합니다. 를 제외한 모든 규칙 동작으로 설정할 수 Allow 있습니다.	규칙 그룹 규칙 작업 설정은 토큰이 없는 경우 Challenge이고 단일 클라이언트 세션에서 발생하는 대용량 트래픽의 경우 CAPTCHA입니다. 이러한 규칙 중 하나를 유효한 규칙 작업 중 하나로 설정할 수 있습니다.	
고도로 분산된 공격에 대한 복원력	미디엄 - 자체적으로 IP 주소를 제한하는 경우 최대 10,000개의 IP 주소	중간 - IP 주소와 토큰 간의 총 50,000개로 제한	
AWS WAF 요금	의 표준 요금에 AWS WAF포함됩니다.	목표 수준의 Bot Control 지능형 위협 완화 비용에 포함됩니다.	
자세한 정보	비율 기반 규칙 문	AWS WAF 봇 컨트롤 규칙 그룹	

지능형 위협 완화 모범 사례

이 섹션의 모범 사례를 따르면 지능형 위협 완화 기능을 가장 효율적이고 비용 효율적으로 구현할 수 있습니다.

- JavaScript 및 모바일 애플리케이션 통합 SDK 구현 — ACFP, ATP 또는 Bot Control 기능의 전체 세트를 최대한 효과적인 방법으로 사용할 수 있도록 애플리케이션 통합을 구현합니다. 관리형 규칙 그룹은 SDK에서 제공하는 토큰을 사용하여 세션 수준에서 합법적인 클라이언트 트래픽을 바람직하지

않은 트래픽과 분리합니다. 애플리케이션 통합 SDK에서는 이러한 토큰을 항상 사용할 수 있습니다. 세부 정보는 다음을 참조하세요.

- 애플리케이션 통합 SDK를 ACFP와 함께 사용해야 하는 이유
- 애플리케이션 통합 SDK를 ATP와 함께 사용해야 하는 이유
- 애플리케이션 통합 SDK를 Bot Control과 함께 사용해야 하는 이유

통합을 사용하여 클라이언트에서 문제를 구현하고 최종 사용자에게 JavaScript CAPTCHA 퍼즐이 제공되는 방식을 사용자 지정하십시오. 자세한 설명은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하십시오.

JavaScript API를 사용하여 CAPTCHA 퍼즐을 사용자 지정하고 웹 ACL의 어느 곳에서나 CAPTCHA 규칙 액션을 사용하는 경우 에서 클라이언트의 CAPTCHA 응답 처리 지침을 따르십시오. AWS WAF 에서 캡차 응답 처리하기 AWS WAF 이 지침은 ACFP 관리형 규칙 그룹의 규칙과 Bot Control 관리형 규칙 그룹의 대상 보호 수준을 포함하여 CAPTCHA 작업을 사용하는 모든 규칙에 적용됩니다.

- ACFP, ATP 및 봇 제어 규칙 그룹으로 보내는 요청을 제한하십시오. — 지능형 위협 완화 관리 규칙 그룹 사용 시 추가 요금이 발생합니다. AWS ACFP 규칙 그룹은 사용자가 지정한 계정 등록 및 생성 엔드포인트에 대한 요청을 검사합니다. ATP 규칙 그룹은 사용자가 지정한 로그인 엔드포인트에 대한 요청을 검사합니다. Bot Control 규칙 그룹은 웹 ACL 평가에서 로그인 엔드포인트에 도달한 모든 요청을 검사합니다.

  이러한 규칙 그룹의 사용을 줄이려면 다음과 같은 방법을 고려하십시오.

  - 관리형 규칙 그룹 문에서 범위 축소 문을 사용하여 검사에서 요청을 제외하십시오. 모든 중첩 가능한 명령문을 사용하여 이 작업을 수행할 수 있습니다. 자세한 내용은 범위 축소 문을 참조하세요.
  - 규칙 그룹 앞에 규칙을 추가하여 검사에서 요청을 제외시킵니다. 범위 축소 문에 사용할 수 없는 규칙의 경우, 그리고 레이블 지정 후 레이블 일치와 같은 좀 더 복잡한 상황의 경우 규칙 그룹보다 먼저 실행되는 규칙을 추가할 수 있습니다. 자세한 내용은 범위 축소 문 및 규칙 문 기본 사항 섹션을 참조하세요.
  - 비용이 더 저렴한 규칙 이후에 규칙 그룹을 실행합니다. 어떤 이유로든 요청을 차단하는 다른 표준 AWS WAF 규칙이 있는 경우 이러한 유료 규칙 그룹보다 먼저 실행하십시오. 규칙 및 규칙 관리에 대한 자세한 내용은 규칙 문 기본 사항 섹션을 참조하세요.
  - 지능형 위협 완화 관리형 규칙 그룹을 두 개 이상 사용하는 경우 비용을 낮추려면 Bot Control, ATP, ACFP 순으로 실행합니다.

  자세한 요금 정보는 AWS WAF 요금을 참조하세요.

- 정상적인 웹 트래픽 중 Bot Control 규칙 그룹의 표적 보호 수준 활성화 — 대상 보호 수준의 일부 규칙은 불규칙하거나 악의적인 트래픽 패턴을 인식하고 이에 대응하기 전에 정상적인 트래픽 패턴의

기준을 설정하는 데 시간이 필요합니다. 예를 들어, TGT_ML_* 규칙을 워밍업하려면 최대 24시간이 필요합니다.

공격이 발생하지 않을 때 이러한 보호 기능을 추가하고 공격에 적절하게 대응할 것으로 예상하기 전에 보호의 기준이 설정될 때까지 기다립니다. 공격 중에 이러한 규칙을 추가하면 공격이 진정된 후 공격 트래픽으로 인한 왜곡이 가중되므로 일반적으로 기준선을 설정하는 데 정상 소요 시간의 2배 ~3배가 걸리게 됩니다. 규칙 및 규칙에 필요한 준비 시간에 대한 자세한 내용은 규칙 목록 섹션을 참조하세요.

- 분산 서비스 거부 (DDoS) 방어의 경우 Shield Advanced 자동 애플리케이션 계층 DDoS 완화 사용 - 지능형 위협 완화 규칙 그룹은 DDoS 보호를 제공하지 않습니다. ACFP는 애플리케이션 가입 페이지에 대한 사기 계정 생성 시도로부터 보호합니다. ATP는 로그인 페이지에 대한 계정 탈취 시도로부터 보호합니다. Bot Control은 토큰을 사용하여 사람과 유사한 액세스 패턴을 적용하고 클라이언트 세션에 동적 속도 제한을 적용하는 데 중점을 둡니다.

  자동 애플리케이션 레이어 DDoS 완화가 활성화된 상태에서 Shield Advanced를 사용하면 Shield Advanced는 사용자 대신 사용자 지정 AWS WAF 완화 기능을 생성, 평가 및 배포하여 탐지된 DDoS 공격에 자동으로 대응합니다. Shield Advanced에 대한 자세한 내용은 AWS Shield Advanced 개요 및 AWS Shield Advanced 애플리케이션 계층 (계층 7) 보호 섹션을 참조하세요.
- 토큰 처리 조정 및 구성 - 최상의 사용자 환경을 제공할 수 있도록 웹 ACL의 토큰 처리를 조정합니다.
  - 운영 비용을 줄이고 최종 사용자 환경을 개선하려면 토큰 관리 면제 시간을 보안 요구 사항이 허용하는 최장 시간으로 조정합니다. 이를 통해 CAPTCHA 퍼즐과 자동 챌린지 사용을 최소화할 수 있습니다. 자세한 내용은 타임스탬프 만료: AWS WAF 토큰 면역 시간을 참조하세요.
  - 보호된 애플리케이션 간에 토큰을 공유할 수 있도록 하려면 웹 ACL의 토큰 도메인 목록을 구성하십시오. 자세한 내용은 AWS WAF 토큰 도메인 및 도메인 목록을 참조하세요.
- 임의 호스트 사양을 포함하는 요청 거부 - 웹 요청의 Host 헤더와 대상 리소스 간 일치가 필수 조건이 되도록 보호된 리소스를 구성하십시오. 단일 값 또는 특정 값 집합(예: myExampleHost.com 및)는 허용할 수 있지만 www.myExampleHost.com 호스트에 대해 임의의 값은 수락하지 마십시오.
- CloudFront 배포용 오리진인 애플리케이션 로드 밸런서의 경우 적절한 토큰 처리를 CloudFront 구성하고 AWS WAF 적용하십시오. - 웹 ACL을 Application Load Balancer에 연결하고 Application Load Balancer를 배포의 오리진으로 배포하는 경우에는 을 참조하십시오. CloudFront 오리진인 애플리케이션 로드 밸런서에 필요한 구성 CloudFront
- 배포 전 테스트 및 조정 - 웹 ACL에 변경 사항을 구현하기 전에 이 안내서의 테스트 및 조정 절차에 따라 예상대로 작동하는지 확인하십시오. 이 점은 이러한 유료 기능의 경우 특히 중요합니다. 일반적인 지침은 AWS WAF 보호 기능 테스트 및 조정 섹션을 참조하세요. 유료 관리형 규칙 그룹과 관련된 자세한 내용은 ACFP 테스트 및 배포, ATP 테스트 및 배포 및 AWS WAF 봇 컨트롤 테스트 및 배포 섹션을 참조하세요.

AWS WAF 웹 요청 토큰

AWS WAF 토큰은 AWS WAF 지능형 위협 완화가 제공하는 향상된 보호 기능의 필수적인 부분입니다. 핑거프린트라고도 하는 토큰은 클라이언트가 전송하는 모든 웹 요청에 저장하고 제공하는 단일 클라이언트 세션에 대한 정보 모음입니다. AWS WAF 토큰을 사용하여 악의적인 클라이언트 세션을 식별하고 합법적인 세션과 분리합니다. 둘 다 단일 IP 주소에서 시작된 경우에도 마찬가지입니다. 토큰 사용으로 인해 합법적인 사용자에게는 무시할 만한 비용이 부과되지만 봇넷의 경우 높은 비용이 발생합니다.

AWS WAF 토큰을 사용하여 애플리케이션 통합 SDK와 규칙 조치 및 를 통해 제공되는 브라우저 및 최종 사용자 챌린지 기능을 지원합니다. Challenge CAPTCHA 또한 토큰을 사용하면 AWS WAF Bot Control 및 계정 탈취 방지 관리 규칙 그룹의 기능을 사용할 수 있습니다.

AWS WAF 조용한 챌린지와 CAPTCHA 퍼즐에 성공적으로 대응하는 클라이언트를 위해 토큰을 생성, 업데이트 및 암호화합니다. 토큰이 있는 클라이언트가 웹 요청을 보내면 암호화된 토큰을 포함하고 토큰을 AWS WAF 해독하고 내용을 확인합니다.

주제

토큰 AWS WAF 사용 방법

AWS WAF 토큰을 사용하여 다음 유형의 클라이언트 세션 검증을 기록하고 확인합니다.

- CAPTCHA - CAPTCHA 퍼즐은 봇을 인간 사용자와 구분하는 데 도움이 됩니다. CAPTCHA는 CAPTCHA 규칙 작업을 통해서만 실행됩니다. 퍼즐을 성공적으로 완료하면 CAPTCHA 스크립트는 토큰의 CAPTCHA 타임스탬프를 업데이트합니다. 자세한 정보는 CAPTCHA그리고 Challenge 안에 AWS WAF을 참조하세요.
- 챌린지 - 챌린지는 자동으로 실행되어 일반 클라이언트 세션을 봇 세션과 구분할 수 있도록 도와주고 봇의 운영 비용을 증가시킵니다. 챌린지가 성공적으로 완료되면 챌린지 스크립트는 필요한 AWS WAF 경우 새 토큰을 자동으로 조달한 다음 토큰의 챌린지 타임스탬프를 업데이트합니다.

AWS WAF 다음과 같은 상황에서 챌린지를 실행합니다.

- 애플리케이션 통합 SDK - 애플리케이션 통합 SDK는 클라이언트 애플리케이션 세션 내에서 실행되며 클라이언트가 챌린지에 성공적으로 응답한 후에만 로그인 시도가 허용되도록 합니다. 자세한 정보는 AWS WAF 클라이언트 애플리케이션 통합을 참조하세요.
- Challenge 규칙 작업 – 자세한 내용은 CAPTCHA그리고 Challenge 안에 AWS WAF 섹션을 참조하세요.
- CAPTCHA— CAPTCHA 중간 광고를 실행할 때 클라이언트에 아직 토큰이 없는 경우 스크립트는 자동으로 챌린지를 먼저 실행하여 클라이언트 세션을 확인하고 토큰을 초기화합니다.

지능형 위협 AWS 관리 규칙 규칙 그룹의 많은 규칙에는 토큰이 필요합니다. 이들 규칙은 토큰을 사용하여 세션 수준에서 클라이언트 구분, 브라우저 특성 결정, 애플리케이션 웹 페이지의 사용자 상호 작용 수준 파악 등의 작업을 수행합니다. 이러한 규칙 그룹은 AWS WAF 토큰 관리를 호출하여 토큰 레이블링을 적용한 다음 규칙 그룹이 검사합니다.

- AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) — ACFP 규칙에서는 유효한 토큰이 포함된 웹 요청을 요구합니다. 규칙에 대한 자세한 내용은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요.
- AWS WAF 사기 방지 계정 탈취 방지 (ATP) — 대량의 클라이언트 세션이 오래 지속되는 것을 방지하는 ATP 규칙에 따라 유효한 토큰이 있고 만료되지 않은 챌린지 타임스탬프가 있는 웹 요청에는 웹 요청에는 유효한 토큰이 있어야 합니다. 자세한 정보는 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹을 참조하세요.
- AWS WAF 봇 컨트롤 — 이 규칙 그룹의 대상 규칙은 클라이언트가 유효한 토큰 없이 보낼 수 있는 웹 요청 수를 제한하며, 세션 수준 모니터링 및 관리를 위해 토큰 세션 추적을 사용합니다. 이들 규칙은 필요에 따라 Challenge 및 CAPTCHA 규칙 작업을 적용하여 토큰 획득 및 유효한 클라이언트 동작을 요구합니다. 자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹을(를) 참조하세요.

AWS WAF 토큰 특성

각 토큰의 특성은 다음과 같습니다.

- 토큰은 `aws-waf-token` 이름이 지정된 쿠키에 저장됩니다.
- 토큰은 암호화됩니다.
- 토큰은 다음 정보가 포함된 세분화된 고정 식별자로 클라이언트 세션을 핑거프린팅합니다.
  - 자동 챌린지에 대한 클라이언트의 최근 성공 응답의 타임스탬프.

- CAPTCHA에 대한 최종 사용자의 최근 성공 응답의 타임스탬프. 이는 보호 기능에서 CAPTCHA를 사용하는 경우에만 나타납니다.
- 합법적인 클라이언트를 원하지 않는 트래픽으로부터 분리하는 데 도움이 될 수 있는 클라이언트 및 클라이언트 행동에 대한 추가 정보. 이 정보에는 자동화된 활동을 탐지하는 데 사용할 수 있는 다양한 클라이언트 식별자와 클라이언트 측 신호가 포함됩니다. 수집된 정보는 고유하지 않으므로 각 개인에게 매핑할 수 없습니다.
  - 모든 토큰에는 자동화 및 브라우저 설정 불일치 표시와 같은 클라이언트 브라우저 질의 데이터가 포함됩니다. 이 정보는 Challenge 작업과 클라이언트 애플리케이션 SDK에 의해 실행되는 스크립트를 통해 검색됩니다. 이러한 스크립트는 브라우저에 능동적으로 질의하고 그 결과를 토큰에 넣습니다.
  - 또한 클라이언트 애플리케이션 통합 SDK를 구현하면 토큰에 최종 사용자의 애플리케이션 페이지 상호 작용에 대해 수동적으로 수집된 정보가 포함됩니다. 상호 작용에는 마우스 이동, 키 누름 및 페이지에 있는 모든 HTML 양식과의 상호 작용이 포함됩니다. 이 정보는 AWS WAF 에서 클라이언트의 사용자 상호 작용 수준을 탐지하여 사람으로 여겨지지 않는 사용자에게 챌린지를 제시하는 데 도움이 됩니다. 클라이언트측 통합에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요.

보안상의 이유로 토큰 내용에 대한 전체 설명이나 AWS WAF 토큰 암호화 프로세스에 대한 자세한 정보는 제공하지 AWS 않습니다.

타임스탬프 만료: AWS WAF 토큰 면역 시간

AWS WAF 챌린지 및 CAPTCHA 면역 시간을 사용하여 단일 클라이언트 세션에 챌린지 또는 CAPTCHA를 표시할 수 있는 빈도를 제어합니다. 최종 사용자가 CAPTCHA에 성공적으로 응답한 후 CAPTCHA 면제 시간에 따라 최종 사용자가 다른 CAPTCHA를 받지 않는 기간이 결정됩니다. 마찬가지로, 챌린지 면제 시간은 클라이언트 세션이 챌린지에 성공적으로 응답한 후 다시 챌린지를 받지 않는 기간을 결정합니다.

AWS WAF 토큰 내의 해당 타임스탬프를 업데이트하여 챌린지 또는 CAPTCHA에 대한 성공적인 응답을 기록합니다. 토큰에서 챌린지 또는 CAPTCHA를 AWS WAF 검사할 때 현재 시간에서 타임스탬프를 빼냅니다. 결과가 구성된 면제 시간보다 크면 타임스탬프가 만료됩니다.

웹 ACL과 CAPTCHA 또는 Challenge 규칙 작업을 사용하는 모든 규칙에서 챌린지 및 CAPTCHA 면제 시간을 구성할 수 있습니다.

- 두 면제 시간에 대한 기본 웹 ACL 설정은 300초입니다.

- CAPTCHA 또는 Challenge 작업을 사용하는 모든 규칙의 면제 시간을 지정할 수 있습니다. 규칙에 대한 면제 시간을 지정하지 않으면 웹 ACL에서 설정을 상속합니다.
- CAPTCHA 또는 Challenge 작업을 사용하는 규칙 그룹 내 규칙의 경우 규칙에 대한 면제 시간을 지정하지 않으면 규칙 그룹을 사용하는 각 웹 ACL의 설정이 상속됩니다.
- 애플리케이션 통합 SDK는 웹 ACL의 챌린지 면제 시간을 사용합니다.

제한 시간의 최소 챌린지 면제 시간 값은 300초입니다. 제한 시간의 최소 CAPTCHA 면제 시간 값은 60초입니다. 두 면제 시간의 최대값은 259,200초, 즉 3일입니다.

웹 ACL 및 규칙 수준 면제 시간 설정을 사용하여 CAPTCHA 작업, Challenge 또는 SDK 챌린지 관리 동작을 조정할 수 있습니다. 예를 들어, 면제 시간이 짧고 매우 민감한 데이터에 대한 액세스를 제어하는 규칙을 구성한 다음 다른 규칙 및 SDK가 상속할 더 높은 면제 시간을 웹 ACL에서 설정할 수 있습니다.

특히 CAPTCHA의 경우 퍼즐은 고객의 웹 사이트 경험을 저하시킬 수 있으므로 CAPTCHA 면제 시간을 조정하면 원하는 보호 기능을 제공하면서 고객 경험에 미치는 영향을 완화하는 데 도움이 될 수 있습니다.

Challenge 및 CAPTCHA 규칙 작업의 사용 면제 시간 조정에 대한 자세한 내용은 CAPTCHA 및 Challenge 작업 사용 모범 사례 섹션을 참조하세요.

AWS WAF 토큰 면역 시간 설정 위치

웹 ACL과 Challenge 및 CAPTCHA 규칙 작업을 사용하는 규칙에서 면제 시간을 설정할 수 있습니다.

웹 ACL 및 관련 규칙의 관리에 대한 일반적인 정보는 웹 ACL 작업 섹션을 참조하세요.

웹 ACL 면제 시간을 설정할 위치

- 콘솔 - 웹 ACL을 편집할 때 규칙 탭에서 웹 ACL CAPTCHA 구성 및 웹 ACL 챌린지 구성 창에서 설정을 편집하고 변경합니다. 콘솔에서는 웹 ACL을 생성한 후에만 웹 ACL CAPTCHA 및 챌린지 면제 시간을 구성할 수 있습니다.
- 콘솔 외부 - 웹 ACL 데이터 유형에는 사용자가 구성하여 웹 ACL의 생성 및 업데이트 작업에 제공할 수 있는 CAPTCHA 및 챌린지 구성 매개변수가 있습니다.

규칙 면제 시간을 설정할 위치

- 콘솔 - 규칙을 만들거나 편집하고 CAPTCHA 또는 Challenge 작업을 지정할 때 규칙 면제 시간 설정을 수정할 수 있습니다.

- 콘솔 외부 - 규칙 데이터 유형에는 규칙을 정의할 때 구성할 수 있는 CAPTCHA 및 챌린지 구성 매개 변수가 있습니다.

AWS WAF 토큰 도메인 및 도메인 목록

클라이언트용 토큰을 AWS WAF 생성할 때 토큰 도메인으로 구성합니다. AWS WAF 는 웹 요청에서 토큰을 검사할 때 해당 도메인이 웹 ACL에 유효한 것으로 간주되는 도메인과 일치하지 않는 경우 토큰을 유효하지 않은 것으로 간주하여 거부합니다.

기본적으로 도메인 설정이 웹 ACL과 연결된 리소스의 호스트 도메인과 정확히 일치하는 AWS WAF 토큰만 허용합니다. 웹 요청의 `Host` 헤더 값입니다. 브라우저의 JavaScript `window.location.hostname` 속성 및 주소 표시줄에 표시되는 주소에서 이 도메인을 찾을 수 있습니다.

다음 섹션에 설명된 바와 같이 웹 ACL 구성에서 허용 가능한 토큰 도메인을 지정할 수도 있습니다. 이 경우 호스트 헤더와 정확히 일치하는 항목과 토큰 도메인 목록에 있는 도메인과 일치하는 항목을 모두 AWS WAF 수락합니다.

도메인을 설정하고 웹 ACL에서 AWS WAF 토큰을 평가할 때 사용할 토큰 도메인을 지정할 수 있습니다. `gov.au`와 같은 공개 접미사는 도메인으로 지정할 수 없습니다. 사용할 수 없는 도메인의 경우 공개 접미사 목록의 https://publicsuffix.org/list/public_suffix_list.dat 목록을 참조하세요.

AWS WAF 웹 ACL 토큰 도메인 목록 구성

허용하려는 AWS WAF 추가 도메인이 포함된 토큰 도메인 목록을 제공하여 여러 보호된 리소스 간에 토큰을 공유하도록 웹 ACL을 구성할 수 있습니다. 토큰 도메인 목록을 AWS WAF 사용해도 여전히 리소스의 호스트 도메인을 수락합니다. 또한 접두사가 붙은 하위 도메인을 포함하여 토큰 도메인 목록의 모든 도메인을 허용합니다.

예를 들어 토큰 도메인 목록의 도메인 사양 `example.com`은 `example.com`(`http://example.com/`), `api.example.com`(`http://api.example.com/`) 및 `www.example.com`(`http://www.example.com/`)와 일치합니다. `example.api.com`(`http://example.api.com/`) 또는 `apiexample.com`(`http://apiexample.com/`)과는 일치하지 않습니다.

웹 ACL을 만들거나 편집할 때 웹 ACL에서 토큰 도메인 목록을 구성할 수 있습니다. 웹 ACL의 관리에 대한 일반적인 정보는 웹 ACL 작업 섹션을 참조하세요.

AWS WAF 토큰 도메인 설정

AWS WAF 챌린지 스크립트의 요청에 따라 토큰을 생성하며, 이 토큰은 애플리케이션 통합 SDK와 Challenge 및 CAPTCHA 규칙 작업에 의해 실행됩니다.

토큰에 AWS WAF 설정하는 도메인은 토큰을 요청하는 챌린지 스크립트의 유형과 제공하는 추가 토큰 도메인 구성에 따라 결정됩니다. AWS WAF 토큰의 도메인을 구성에서 찾을 수 있는 가장 짧고 가장 일반적인 설정으로 설정합니다.

- JavaScript SDK — 하나 이상의 도메인을 포함할 수 있는 토큰 도메인 사양으로 JavaScript SDK를 구성할 수 있습니다. 구성하는 도메인은 보호된 호스트 도메인과 웹 ACL의 토큰 도메인 목록을 기반으로 AWS WAF 수락할 도메인이어야 합니다.

  클라이언트용 토큰을 AWS WAF 발급할 때 토큰 도메인은 호스트 도메인과 일치하고 구성된 목록에 있는 도메인 중에서 호스트 도메인과 일치하고 가장 짧은 도메인으로 설정합니다. 예를 들어, 호스트 도메인이 `api.example.com` 이고 토큰 도메인 목록에 있는 경우 토큰은 `example.com` 호스트 도메인과 일치하고 길이가 더 짧기 때문에 토큰을 AWS WAF 사용합니다`example.com`. JavaScript API 구성에서 토큰 도메인 목록을 제공하지 않는 경우 도메인을 보호된 리소스의 호스트 도메인으로 AWS WAF 설정합니다.

  자세한 정보는 토큰에 사용할 도메인 제공을 참조하세요.

- 모바일 SDK - 애플리케이션 코드에서 토큰 도메인 속성을 사용하여 모바일 SDK를 구성해야 합니다. 이 속성은 AWS WAF 에서 보호된 호스트 도메인과 웹 ACL의 토큰 도메인 목록에 기반하여 허용할 도메인이어야 합니다.

  클라이언트용 토큰을 AWS WAF 발행할 때는 이 속성을 토큰 도메인으로 사용합니다. AWS WAF 모바일 SDK 클라이언트용으로 발행하는 토큰에는 호스트 도메인을 사용하지 않습니다.

  자세한 내용은 AWS WAF 모바일 SDK 사양의 `WAFConfiguration` `domainName` 설정을 참조하세요.

- Challenge조치 — 웹 ACL에서 토큰 도메인 목록을 지정하는 경우, 호스트 도메인과 목록에 있는 도메인 중에서 호스트 도메인과 일치하고 가장 짧은 도메인으로 토큰 도메인을 AWS WAF 설정합니다. 예를 들어, 호스트 도메인이 `api.example.com` 이고 토큰 도메인 목록에 있는 경우`example.com`, 호스트 도메인과 일치하고 더 짧기 때문에 토큰을 AWS WAF 사용합니다`example.com`. 웹 ACL에서 토큰 도메인 목록을 제공하지 않는 경우 도메인을 보호된 리소스의 호스트 도메인으로 AWS WAF 설정합니다.

AWS WAF 봇 및 사기 관리 규칙 그룹에 의한 토큰 라벨링

이 섹션에서는 AWS WAF 토큰 관리가 웹 요청에 추가하는 레이블에 대해 설명합니다. 레이블에 대한 일반 정보는 을 참조하십시오AWS WAF 웹 요청의 레이블.

AWS WAF 봇 또는 사기 방지 관리 규칙 그룹을 사용하는 경우 규칙 그룹은 AWS WAF 토큰 관리를 사용하여 웹 요청 토큰을 검사하고 요청에 토큰 레이블링을 적용합니다. 관리형 규칙 그룹에 대한 자세한 설명은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹, AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 및 AWS WAF 봇 컨트롤 규칙 그룹을(를) 참조하십시오.

> **Note**
>
> AWS WAF 이러한 지능형 위협 완화 관리 규칙 그룹 중 하나를 사용하는 경우에만 토큰 레이블을 적용합니다.

토큰 관리는 웹 요청에 다음 레이블을 추가할 수 있습니다.

클라이언트 세션 레이블

`awswaf:managed:token:id:`*`identifier`*레이블에는 AWS WAF 토큰 관리가 클라이언트 세션을 식별하는 데 사용하는 고유 식별자가 들어 있습니다. 클라이언트가 새 토큰을 획득하는 경우(예: 사용하고 있던 토큰을 폐기한 후) 식별자가 변경될 수 있습니다.

> **Note**
>
> AWS WAF 이 라벨에 대한 Amazon CloudWatch 메트릭을 보고하지 않습니다.

토큰 상태 레이블: 레이블 네임스페이스 접두사

토큰 상태 레이블은 토큰 및 챌린지 상태와 토큰에 포함된 CAPTCHA 정보를 보고합니다.

각 토큰 상태 레이블은 다음 네임스페이스 접두사 중 하나로 시작합니다.

- `awswaf:managed:token:` – 토큰의 일반 상태를 보고하고 토큰의 챌린지 정보 상태를 보고하는 데 사용됩니다.
- `awswaf:managed:captcha:` – 토큰의 CAPTCHA 정보 상태를 보고하는 데 사용됩니다.

토큰 상태 레이블: 레이블 이름

접두사 뒤에 오는 라벨의 나머지 부분은 자세한 토큰 상태 정보를 제공합니다.

- `accepted` – 요청 토큰이 존재하며 다음을 포함합니다.
  - 유효한 챌린지 또는 CAPTCHA 솔루션.
  - 만료되지 않은 챌린지 또는 CAPTCHA 타임스탬프.
  - 웹 ACL에 대해 유효한 도메인 사양입니다.

  예: 레이블 `awswaf:managed:token:accepted`은(는) 웹 요청의 토큰에 유효한 인증 확인 솔루션, 만료되지 않은 챌린지 타임스탬프 및 유효한 도메인이 있음을 나타냅니다.
- `rejected` – 요청 토큰이 존재하지만 수락 기준을 충족하지 않습니다.

  거부된 레이블과 함께 토큰 관리는 사용자 지정 레이블 네임스페이스 및 이름을 추가하여 이유를 나타냅니다.
  - `rejected:not_solved` – 토큰에 챌린지 또는 CAPTCHA 솔루션이 없습니다.
  - `rejected:expired` – 웹 ACL의 구성된 토큰 면역 시간에 따라 토큰의 챌린지 또는 CAPTCHA 타임스탬프가 만료되었습니다.
  - `rejected:domain_mismatch` – 토큰의 도메인이 웹 ACL의 토큰 도메인 구성과 일치하지 않습니다.
  - `rejected:invalid`— AWS WAF 표시된 토큰을 읽을 수 없습니다.

  예: 레이블 `awswaf:managed:captcha:rejected` 및 `awswaf:managed:captcha:rejected:expired`은(는) 토큰의 CAPTCHA 타임스탬프가 웹 ACL에 구성된 CAPTCHA 토큰 면역 시간을 초과했기 때문에 요청이 거부되었음을 나타냅니다.
- `absent` – 요청에 토큰이 없거나 토큰 관리자가 토큰을 읽을 수 없습니다.

  예: 레이블 `awswaf:managed:captcha:absent`은(는) 요청에 토큰이 없음을 나타냅니다.

유효한 AWS WAF 토큰이 없는 요청 차단

지능형 위협 AWS 관리 규칙 그룹 `AWSManagedRulesACFPRuleSet` `AWSManagedRulesATPRuleSetAWSManagedRulesBotControlRuleSet`, 및 을 사용하는 경우 규칙 그룹은 AWS WAF 토큰 관리를 호출하여 웹 요청 토큰의 상태를 평가하고 그에 따라 요청에 레이블을 지정합니다.

> **Note**
>
> 토큰 레이블 지정은 이러한 관리형 규칙 그룹 중 하나를 사용하여 평가하는 웹 요청에만 적용됩니다.

토큰 관리에서 적용하는 레이블 지정에 대한 내용은 앞의 AWS WAF 봇 및 사기 관리 규칙 그룹에 의한 토큰 라벨링 섹션을 참조하세요.

그러면 지능형 위협 완화 관리형 규칙 그룹이 다음과 같이 토큰 요구 사항을 처리합니다.

- `AWSManagedRulesACFPRuleSet` `AllRequests` 규칙은 모든 요청에 대해 Challenge 작업을 실행하여 `accepted` 토큰 레이블이 없는 요청을 효과적으로 차단하도록 구성됩니다.
- `AWSManagedRulesATPRuleSet`는 `rejected` 토큰 레이블이 있는 요청을 차단하지만 `absent` 토큰 레이블이 있는 요청은 차단하지 않습니다.
- `AWSManagedRulesBotControlRuleSet` 대상 보호 수준에서는 클라이언트가 `accepted` 토큰 레이블 없이 요청을 5회 전송하고 나면 클라이언트에 챌린지를 제시합니다. 이 수준은 유효한 토큰이 없는 개별 요청을 차단하지는 않습니다. 이 규칙 그룹의 공통 보호 수준은 토큰 요구 사항을 관리하지 않습니다.

지능형 위협 규칙 그룹에 대한 자세한 내용은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹, AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 및 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.

Bot Control 또는 ATP 관리형 규칙 그룹을 사용할 때 토큰이 누락된 요청을 차단하려면

Bot Control 및 ATP 규칙 그룹을 사용하면 유효한 토큰이 없는 요청에 대해 규칙 그룹 평가를 종료하고 웹 ACL에서 계속 평가할 수 있습니다.

토큰이 없거나 토큰이 거부된 모든 요청을 차단하려면 관리형 규칙 그룹 바로 뒤에 실행되도록 규칙을 추가하여 해당 규칙 그룹이 처리하지 않는 요청이 캡처 및 차단되도록 합니다.

다음은 ATP 관리형 규칙 그룹을 사용하는 웹 ACL의 예제 JSON 목록입니다. 웹 ACL에는 `awswaf:managed:token:absent` 레이블을 캡처하고 처리하는 규칙이 추가되었습니다. 이 규칙은 평가 범위를 로그인 엔드포인트로 이동하는 웹 요청으로 좁혀서 ATP 규칙 그룹의 범위와 일치시킵니다. 추가된 규칙은 굵게 표시됩니다.

```
{
  "Name": "exampleWebACL",
```

```
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  }
                },
                "ResponseInspection": {
                  "StatusCode": {
                    "SuccessCodes": [
                      200
                    ],
                    "FailureCodes": [
                      401,
                      403,
                      500
                    ]
                  }
                }
              }
            }
          ]
        }
```

```
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesATPRuleSet"
      }
    },
    {
      "Name": "RequireTokenForLogins",
      "Priority": 2,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "Statement": {
                "LabelMatchStatement": {
                  "Scope": "LABEL",
                  "Key": "awswaf:managed:token:absent"
                }
              }
            },
            {
              "ByteMatchStatement": {
                "SearchString": "/web/login",
                "FieldToMatch": {
                  "UriPath": {}
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "STARTS_WITH"
              }
            },
            {
              "ByteMatchStatement": {
                "SearchString": "POST",
                "FieldToMatch": {
                  "Method": {}
```

```
                },
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ],
                "PositionalConstraint": "EXACTLY"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RequireTokenForLogins"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "exampleWebACL"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
}
```

오리진인 애플리케이션 로드 밸런서에 필요한 구성 CloudFront

웹 ACL을 애플리케이션 로드 밸런서에 연결하고 Application Load Balancer를 배포의 오리진으로 배포하는 경우 이 섹션을 읽어보세요. CloudFront

이 아키텍처를 사용하는 경우 토큰 정보가 올바르게 처리되도록 하려면 다음과 같은 추가 구성을 제공해야 합니다.

- `aws-waf-token`쿠키를 Application Load Balancer에 CloudFront 전달하도록 구성합니다. 기본적으로 오리진에 전달하기 전에 웹 요청에서 쿠키를 CloudFront 제거합니다. 토큰 쿠키를 웹 요청과 함

께 보관하려면 토큰 쿠키만 포함하거나 모든 쿠키를 포함하도록 CloudFront 캐시 동작을 구성하십시오. 이를 수행하는 방법에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 쿠키 기반 콘텐츠 캐싱을 참조하십시오.

- CloudFront배포 도메인을 유효한 토큰 도메인으로 AWS WAF 인식하도록 구성하십시오. 기본적으로 `Host` 헤더를 Application Load Balancer 오리진으로 CloudFront 설정하고 이를 보호된 리소스의 도메인으로 AWS WAF 사용합니다. 하지만 클라이언트 브라우저에서는 CloudFront 배포를 호스트 도메인으로 간주하고 클라이언트용으로 생성된 토큰은 도메인을 토큰 CloudFront 도메인으로 사용합니다. 추가 구성 없이 토큰 도메인과 비교하여 보호된 리소스 도메인을 AWS WAF 검사할 때 불일치가 발생합니다. 이 문제를 해결하려면 웹 ACL 구성의 토큰 도메인 목록에 CloudFront 배포 도메인 이름을 추가하세요. 이를 위한 자세한 방법은 AWS WAF 웹 ACL 토큰 도메인 목록 구성 섹션을 참조하세요.

AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP)

계정 생성 사기는 공격자가 하나 이상의 허위 계정을 만들려고 하는 온라인 불법 활동입니다. 공격자는 허위 계정을 사용하여 프로모션 및 가입 보너스를 남용하거나 누군가를 사칭하는 사기 활동과 피싱 등의 사이버 공격을 수행합니다. 허위 계정이 존재하면 고객에 대해 평판이 손상되고 금융 사기에 노출되어 비즈니스에 부정적인 영향이 미칠 수 있습니다.

사기 통제 계정 생성 사기 방지 (ACFP) 기능을 구현하여 계정 생성 AWS WAF 사기 시도를 모니터링하고 통제할 수 있습니다. AWS WAF 보조 애플리케이션 통합 `AWSManagedRulesACFPRuleSet` SDK와 함께 AWS Managed Rules 규칙 그룹에서 이 기능을 제공합니다.

ACFP 관리형 규칙 그룹은 악의적인 계정 생성 시도의 일부일 수 있는 요청에 레이블을 지정하고 관리합니다. 규칙 그룹은 클라이언트가 애플리케이션의 계정 가입 엔드포인트로 보내는 계정 생성 시도를 검사하여 이 작업을 수행합니다.

ACFP는 비정상적인 활동에 대한 계정 가입 요청을 모니터링하고 의심스러운 요청을 자동으로 차단하여 계정 가입 페이지를 보호합니다. 규칙 그룹은 요청 식별자, 행동 분석 및 기계 학습을 사용하여 사기성 요청을 탐지합니다.

- 요청 검사 - ACFP는 비정상적인 계정 생성 시도 및 탈취한 보안 인증 정보를 사용하는 시도에 대한 가시성과 제어를 제공하여 사기 계정 생성을 방지합니다. ACFP는 도용된 보안 인증 정보 데이터베이스에서 이메일과 암호 조합을 검사합니다. 이 데이터베이스는 새로 유출된 보안 인증 정보가 다크웹에서 발견될 때마다 정기적으로 업데이트됩니다. ACFP는 이메일 주소에 사용되는 도메인을 평가하고 전화번호 및 주소 필드의 사용을 모니터링하여 입력 내용을 확인하고 사기 행위를 탐지합니다. ACFP는 IP 주소 및 클라이언트 세션별로 데이터를 집계하여 의심스러운 요청을 너무 많이 보내는 클라이언트를 감지하고 차단합니다.

- 응답 검사 — CloudFront 배포의 경우 ACFP 규칙 그룹은 들어오는 계정 생성 요청을 검사하는 것 외에도 계정 생성 시도에 대한 애플리케이션의 응답을 검사하여 성공률과 실패율을 추적합니다. ACFP는 이 정보를 사용하여 계정 생성 시도 실패가 너무 많은 클라이언트 세션 또는 IP 주소를 일시적으로 차단할 수 있습니다. AWS WAF 는 응답 검사를 비동기적으로 수행하므로 이 작업으로 인해 웹 트래픽의 지연 시간이 증가하지 않습니다.

> **Note**
>
> 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

> **Note**
>
> Amazon Cognito 사용자 풀에는 ACFP 기능을 사용할 수 없습니다.

주제

AWS WAF ACFP 구성 요소

사기 방지 계정 생성 AWS WAF 사기 방지 (ACFP) 의 주요 구성 요소는 다음과 같습니다.

- **`AWSManagedRulesACFPRuleSet`**— 이 AWS 관리형 규칙 규칙 그룹의 규칙은 다양한 유형의 부정 계정 생성 활동을 탐지, 분류 및 처리합니다. 규칙 그룹은 클라이언트가 지정된 계정 등록 엔드포인트로 보내는 HTTP `GET` 텍스트/html 요청과 클라이언트가 지정된 계정 등록 엔드포인트로 보내는 `POST` 웹 요청을 검사합니다. 보호된 CloudFront 배포의 경우 규칙 그룹은 배포가 계정 생성 요청에 다시 보내는 응답도 검사합니다. 이 규칙 그룹의 규칙 목록은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요. 관리형 규칙 그룹 참조 문을 사용하여 웹 ACL에 이 규칙 그룹을 포함할 수 있습니다. 이 규칙 그룹 사용에 대한 자세한 내용은 ACFP 관리형 규칙 그룹을 웹 ACL에 추가 섹션을 참조하세요.

> **Note**
>
> 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

- 애플리케이션의 계정 등록 및 생성 페이지에 대한 세부 정보 - `AWSManagedRulesACFPRuleSet` 규칙 그룹을 웹 ACL에 추가할 때 계정 등록 및 생성 페이지에 대한 정보를 제공해야 합니다. 이렇게 하면 규칙 그룹이 검사하는 요청의 범위를 좁히고 계정 생성 웹 요청을 적절하게 검증할 수 있습니다. 등록 페이지는 `GET` 텍스트/html 요청을 수락해야 합니다. 계정 생성 경로에서 `POST` 요청을 수락해야 합니다. ACFP 규칙 그룹은 이메일 형식의 사용자 이름을 사용합니다. 자세한 정보는 ACFP 관리형 규칙 그룹을 웹 ACL에 추가을 참조하세요.
- 보호된 CloudFront 배포의 경우 애플리케이션이 계정 생성 시도에 어떻게 대응하는지에 대한 세부 정보 — 계정 생성 시도에 대한 애플리케이션의 응답에 대한 세부 정보를 제공하면 ACFP 규칙 그룹이 단일 IP 주소 또는 단일 클라이언트 세션에서 대량 계정 생성 시도를 추적하고 관리합니다. 이 옵션의 구성에 대한 자세한 내용은 ACFP 관리형 규칙 그룹을 웹 ACL에 추가 섹션을 참조하세요.
- JavaScript 및 모바일 애플리케이션 통합 SDK — ACFP 구현과 함께 AWS WAF JavaScript 및 모바일 SDK를 구현하여 규칙 그룹이 제공하는 모든 기능을 사용할 수 있도록 하십시오. 많은 ACFP 규칙은 합법적인 클라이언트 트래픽을 봇 트래픽과 분리하는 데 필요한 세션 수준 클라이언트 확인 및 행동 집계에 대해 SDK에서 제공하는 정보를 사용합니다. SDK에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합을 참조하세요.

ACFP 구현을 다음과 결합하여 보호 기능을 모니터링, 조정 및 사용자 지정할 수 있습니다.

- 로깅 및 지표 — 웹 ACL에 대한 로그, Amazon Security Lake 데이터 수집 및 Amazon CloudWatch 지표를 구성 및 활성화하여 트래픽을 모니터링하고 ACFP 관리 규칙 그룹이 이에 미치는 영향을 이해할 수 있습니다. 웹 요청에 `AWSManagedRulesACFPRuleSet` 추가되는 레이블은 데이터에 포함됩니다. 옵션에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅아마존을 통한 모니터링 CloudWatch, 및 Amazon Security Lake란 무엇입니까? 를 참조하십시오. .

  요구 사항과 표시되는 트래픽에 따라 `AWSManagedRulesACFPRuleSet` 구현을 사용자 지정해야 할 수도 있습니다. 예를 들어 ACFP 평가에서 일부 트래픽을 제외하거나 범위 축소 설명 또는 레이블 매칭 규칙과 같은 AWS WAF 기능을 사용하여 식별되는 일부 계정 생성 사기 시도를 처리하는 방식을 변경할 수 있습니다.
- 레이블 및 레이블 일치 규칙 - `AWSManagedRulesACFPRuleSet`에 있는 모든 규칙의 경우 차단 동작을 계산으로 전환한 다음, 규칙에 의해 추가되는 레이블과 일치시킬 수 있습니다. 이 접근 방식을 사용하여 ACFP 관리형 규칙 그룹으로 식별되는 웹 요청을 처리하는 방식을 사용자 지정할 수 있

습니다. 레이블 일치 문의 레이블 지정 및 사용에 대한 자세한 내용은 레이블 일치 규칙 문 및 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.

- 사용자 지정 요청 및 응답 - 허용하는 요청에 사용자 지정 헤더를 추가하고 차단한 요청에 대해 사용자 지정 응답을 보낼 수 있습니다. 이렇게 하려면 레이블 일치를 AWS WAF 사용자 지정 요청 및 응답 기능과 페어링해야 합니다. 요청 및 응답을 사용자 지정하는 방법에 대한 자세한 내용은 AWS WAF의 사용자 지정된 웹 요청 및 응답 섹션을 참조하세요.

애플리케이션 통합 SDK를 ACFP와 함께 사용해야 하는 이유

ACFP 규칙 그룹을 가장 효율적으로 사용하려면 애플리케이션 통합 SDK를 구현하는 것이 좋습니다.

- 전체 규칙 그룹 기능 — ACFP 규칙 `SignalClientHumanInteractivityAbsentLow`에는 애플리케이션 통합에서 작성된 토큰만 사용됩니다. 이 규칙은 애플리케이션 페이지와의 비정상적인 사용자 상호 작용을 탐지하고 관리합니다. 애플리케이션 통합 SDK는 마우스 이동, 키 누름 및 기타 측정을 통해 인간의 정상적인 상호 작용을 탐지할 수 있습니다. 규칙 작업 CAPTCHA 및 Challenge를 통해 전송되는 중간 광고는 이러한 유형의 데이터를 제공할 수 없습니다.
- 지연 시간 감소 - 규칙 그룹 규칙 `AllRequests`는 아직 챌린지 토큰이 없는 모든 요청에 Challenge 규칙 작업을 적용합니다. 이러한 상황이 발생할 경우 규칙 그룹은 해당 요청을 두 번 평가합니다. 즉, 한 번은 토큰이 없는 상태로, 두 번째는 Challenge 작업 중간 광고를 통해 토큰을 획득한 후에 평가합니다. `AllRequests` 규칙만 사용하는 경우에는 추가 요금이 부과되지 않지만, 이 접근 방식은 웹 트래픽에 오버헤드를 추가하고 최종 사용자 환경에 지연 시간을 추가합니다. 애플리케이션 통합을 사용하여 클라이언트 측에서 토큰을 획득하는 경우 계정 생성 요청을 보내기 전에 ACFP 규칙 그룹이 요청을 한 번 평가합니다.

규칙 그룹 기능에 대한 자세한 내용은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요.

SDK에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. AWS WAF 토큰에 대한 자세한 내용은 을 참조하십시오AWS WAF 웹 요청 토큰. 규칙 작업에 대한 자세한 내용은 CAPTCHA그리고 Challenge 안에 AWS WAF 섹션을 참조하세요.

ACFP 관리형 규칙 그룹을 웹 ACL에 추가

웹 트래픽의 계정 생성 사기 활동을 인식하도록 ACFP 관리형 규칙 그룹을 구성하려면 클라이언트가 등록 페이지에 액세스하여 계정 생성 요청을 해당 애플리케이션에 보내는 방법에 대한 정보를 제공합니다. 보호 대상 Amazon CloudFront 배포의 경우 애플리케이션이 계정 생성 요청에 어떻게 응답하는지에 대한 정보도 제공합니다. 이 구성은 관리형 규칙 그룹의 일반 구성에 추가됩니다.

규칙 그룹 설명 및 규칙 목록은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요.

> **Note**
>
> ACFP 도용된 보안 인증 정보 데이터베이스에는 이메일 형식의 사용자 이름만 포함됩니다.

이 지침은 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 만들고 관리하는 방법을 일반적으로 알고 있는 사용자를 대상으로 합니다. 이러한 주제는 이 안내서의 이전 섹션에 설명되어 있습니다. 웹 ACL에 관리형 규칙 그룹을 추가하는 방법에 대한 기본 정보는 콘솔을 통해 웹 ACL에 관리형 규칙 그룹 추가 섹션을 참조하세요.

모범 사례 따르기

지능형 위협 완화 모범 사례의 모범 사례에 따라 ACFP 규칙 그룹을 사용하십시오.

웹 ACL에서 **`AWSManagedRulesACFPRuleSet`** 규칙 그룹을 사용하려면

1. AWS 관리형 규칙 그룹을 웹 ACL에 추가하고 `AWSManagedRulesACFPRuleSet` 저장하기 전에 규칙 그룹 설정을 편집하십시오.

   > **Note**
   >
   > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

2. 규칙 그룹 구성 창에서 ACFP 규칙 그룹이 계정 생성 요청을 검사하는 데 사용하는 정보를 제공합니다.

   a. 등록 및 계정 생성 페이지 경로 사양에 맞게 정규 표현식 일치를 AWS WAF 수행하려면 경로에 정규 표현식 사용의 옵션을 활성화하십시오.

      AWS WAF 일부 예외를 제외하고 PCRE 라이브러리에서 `libpcre` 사용하는 패턴 구문을 지원합니다. 이 라이브러리는 PCRE - Perl 호환 정규식에 문서화되어 있습니다. AWS WAF 지원에 대한 자세한 내용은 을 참조하십시오정규 표현식 패턴 매칭 AWS WAF.

   b. 등록 페이지 경로에 애플리케이션의 등록 페이지 엔드포인트 경로를 제공합니다. 이 페이지는 `GET` 텍스트/html 요청을 수락해야 합니다. 이 규칙 그룹은 지정된 등록 페이지 엔드포인트에 대한 HTTP `GET` 텍스트/html 요청만 검사합니다.

> **Note**
>
> 엔드포인트에 대한 일치는 대/소문자를 구분하지 않습니다. Regex 사양에는 대소문자를 구분하지 않는 일치를 비활성화하는 플래그 `(?-i)`이(가) 포함되어서는 안 됩니다. 문자열 사양은 슬래시 `/`로 시작해야 합니다.

예를 들어, URL `https://example.com/web/registration`의 경우 문자열 경로 사양 `/web/registration`을(를) 제공할 수 있습니다. 입력한 경로로 시작하는 등록 페이지 경로는 일치하는 것으로 간주됩니다. 예를 들어, `/web/registration`는 등록 경로 `/web/registration`, `/web/registration/`, `/web/registrationPage` 및 `/web/registration/thisPage`와 일치하지만, `/home/web/registration` 또는 `/website/registration` 경로와는 일치하지 않습니다.

> **Note**
>
> 최종 사용자가 계정 생성 요청을 제출하기 전에 등록 페이지를 로드하도록 해야 합니다. 이렇게 하면 클라이언트의 계정 생성 요청에 유효한 토큰이 포함되도록 할 수 있습니다.

c. 계정 생성 경로의 경우 완성된 새 사용자 세부 정보를 받아들이는 웹 사이트의 URI를 제공하세요. 이 URI는 `POST` 요청을 수락해야 합니다.

> **Note**
>
> 엔드포인트에 대한 일치는 대/소문자를 구분하지 않습니다. Regex 사양에는 대소문자를 구분하지 않는 일치를 비활성화하는 플래그 `(?-i)`이(가) 포함되어서는 안 됩니다. 문자열 사양은 슬래시 `/`로 시작해야 합니다.

예를 들어, URL `https://example.com/web/newaccount`의 경우 문자열 경로 사양 `/web/newaccount`을(를) 제공할 수 있습니다. 입력한 경로로 시작하는 계정 생성 경로는 일치하는 것으로 간주됩니다. 예를 들어 `/web/newaccount`는 계정 생성 경로 `/web/newaccount`, `/web/newaccount/`, `/web/newaccountPage` 및 `/web/newaccount/thisPage`와 일치하지만, `/home/web/newaccount` 또는 `/website/newaccount` 경로와는 일치하지 않습니다.

d. 요청 검사의 경우 요청 본문에서 사용자 이름, 암호 및 기타 계정 생성 세부 정보를 입력하는 필드 이름과 요청 페이로드 유형을 제공하여 애플리케이션에서 계정 생성 시도를 수락하는 방식을 지정합니다.

> **Note**
>
> 기본 주소 및 전화번호 필드의 경우 요청 페이로드에 나타나는 순서대로 필드를 입력합니다.

필드 이름 사양은 페이로드 유형에 따라 달라집니다.

- JSON 페이로드 유형 - JSON 포인터 구문으로 필드 이름을 지정합니다. JSON 포인터 구문에 대한 자세한 내용은 IETF (인터넷 엔지니어링 태스크 포스) 문서 JavaScript객체 표기법 (JSON) 포인터를 참조하십시오.

  예를 들어 다음 JSON 페이로드 예제의 경우 사용자 이름 필드 사양은 `/signupform/username`이고 기본 주소 필드 사양은 `/signupform/addrp1`, `/signupform/addrp2` 및 `/signupform/addrp3`입니다.

```
{
    "signupform": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD",
        "addrp1": "PRIMARY_ADDRESS_LINE_1",
        "addrp2": "PRIMARY_ADDRESS_LINE_2",
        "addrp3": "PRIMARY_ADDRESS_LINE_3",
        "phonepcode": "PRIMARY_PHONE_CODE",
        "phonepnumber": "PRIMARY_PHONE_NUMBER"
    }
}
```

- FORM_ENCODED 페이로드 유형 - HTML 양식 이름을 사용합니다.

  예를 들어 사용자 및 암호 입력 요소의 이름이 `username1` 및 `password1` 인 HTML 양식의 경우 사용자 이름 필드 사양은 `username1`이고 암호 필드 사양은 `password1`입니다.

e. Amazon CloudFront 배포를 보호하는 경우 응답 검사에서 애플리케이션이 계정 생성 시도에 대한 응답의 성공 또는 실패를 어떻게 표시하는지 지정하십시오.

> **Note**
>
> ACFP 응답 검사는 배포를 보호하는 웹 ACL에서만 사용할 수 있습니다. CloudFront

ACFP에서 검사할 단일 구성 요소를 계정 생성 응답에 지정합니다. 본문 및 JSON 구성 요소 유형의 경우 구성 요소의 처음 65,536바이트 (64KB) 를 AWS WAF 검사할 수 있습니다.

인터페이스에 지정된 구성 요소 유형에 대한 검사 기준을 제공합니다. 구성 요소에서 검사할 성공 및 실패 기준을 모두 제공해야 합니다.

예를 들어 애플리케이션이 응답의 상태 코드에 계정 생성 시도의 상태를 표시하고 성공 시 `200 OK` 그리고 실패 시 `401 Unauthorized` 또는 `403 Forbidden`을 사용한다고 가정해 보겠습니다. 응답 검사 구성 요소 유형을 상태 코드로 설정한 다음 성공 텍스트 상자에 `200`을 입력하고, 실패 텍스트 상자의 첫 번째 줄에 `401` 그리고 두 번째 줄에 `403`을 입력합니다.

ACFP 규칙 그룹은 성공 또는 실패 검사 기준과 일치하는 응답만 계산합니다. 규칙 그룹의 규칙은 대량 계정 생성 시도를 줄이기 위해 계수된 응답 중 성공률이 너무 높은 클라이언트에게 적용됩니다. 규칙 그룹의 규칙이 정확한 작동하려면 성공 및 실패한 계정 생성 시도 모두에 대한 전체 정보를 제공해야 합니다.

계정 생성 응답을 검사하는 규칙을 보려면 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹의 규칙 목록에서 `VolumetricIPSuccessfulResponse` 및 `VolumetricSessionSuccessfulResponse`를 찾아보십시오.

3. 규칙 그룹에 사용할 추가 구성을 모두 제공합니다.

   관리형 규칙 그룹 문에 범위 축소 문을 추가하여 규칙 그룹이 검사하는 요청의 범위를 추가 제한할 수 있습니다. 예를 들어 특정 쿼리 인수 또는 쿠키가 있는 요청만 검사할 수 있습니다. 규칙 그룹은 범위 축소 문의 기준과 일치하고 규정 그룹 구성에 지정된 계정 등록 및 계정 생성 경로로 전송된 요청만 검사합니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요.

4. 웹 ACL에 대한 변경 사항을 저장합니다.

프로덕션 트래픽용 ACFP 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 이를 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 개수 모드에서 테스트하고 조정한 다음 활성화합니다. 지침은 다음 섹션을 참조하세요.

ACFP 테스트 및 배포

이 섹션에서는 사이트에 대한 사기 방지 계정 생성 AWS WAF 사기 방지 (ACFP) 구현을 구성하고 테스트하기 위한 일반적인 지침을 제공합니다. 따르기로 선택한 구체적인 단계는 요구 사항, 리소스 및 수신하는 웹 요청에 따라 달라집니다.

이 정보는 AWS WAF 보호 기능 테스트 및 조정에 제공된 테스트 및 조정에 대한 일반 정보 외의 정보입니다.

> **Note**
>
> AWS 관리형 규칙은 일반적인 웹 위협으로부터 사용자를 보호하도록 설계되었습니다. 설명서에 따라 AWS 관리형 규칙 그룹을 사용하면 애플리케이션에 또 다른 보안 계층이 추가됩니다. 하지만 AWS 관리형 규칙 규칙 그룹은 선택한 AWS 리소스에 따라 결정되는 보안 책임을 대체하기 위한 것이 아닙니다. 공동 책임 모델을 참조하여 AWS 리소스가 적절하게 보호되도록 하세요.

> **⚠ 프로덕션 트래픽 위험**
>
> 프로덕션 트래픽용 ACFP 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 이를 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 개수 모드에서 테스트하고 조정한 다음 활성화합니다.

AWS WAF ACFP 구성을 확인하는 데 사용할 수 있는 테스트 자격 증명을 제공합니다. 다음 절차에서는 ACFP 관리형 규칙 그룹을 사용하도록 테스트 웹 ACL을 구성하고, 규칙 그룹에서 추가한 레이블을 캡처하도록 규칙을 구성한 다음, 이러한 테스트 보안 인증 정보를 사용하여 계정 생성 시도를 실행합니다. 계정 생성 시도에 대한 Amazon CloudWatch 지표를 확인하여 웹 ACL이 시도를 제대로 관리했는지 확인할 수 있습니다.

이 지침은 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 만들고 관리하는 방법을 일반적으로 알고 있는 사용자를 대상으로 합니다. 이러한 주제는 이 안내서의 이전 섹션에 설명되어 있습니다.

AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 구현을 구성하고 테스트하려면

이러한 단계를 먼저 테스트 환경에서 수행한 다음, 프로덕션 환경에서 수행합니다.

1. 카운트 모드에서 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 관리 규칙 그룹을 추가합니다.

   > **Note**
   >
   > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

   AWS 관리형 규칙 규칙 그룹을 `AWSManagedRulesACFPRuleSet` 새 웹 ACL이나 기존 웹 ACL에 추가하고 현재 웹 ACL 동작을 변경하지 않도록 구성합니다. 이 규칙 그룹의 규칙 및 레이블에 대한 자세한 내용은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요.

   - 관리형 규칙 그룹을 추가할 때는 해당 규칙 그룹을 편집하고 다음을 수행합니다.
     - 규칙 그룹 구성 창에서 애플리케이션의 계정 등록 및 생성 페이지의 세부 정보를 제공합니다. ACFP 규칙 그룹은 이 정보를 사용하여 로그인 활동을 모니터링합니다. 자세한 정보는 ACFP 관리형 규칙 그룹을 웹 ACL에 추가을 참조하세요.
     - 규칙 창에서 모든 규칙 모든 규칙 작업 재정의 드롭다운을 열고 Count를 선택합니다. 이 구성을 사용하면 AWS WAF 는 요청에 레이블을 여전히 추가하면서 규칙 그룹의 모든 규칙과 비교하여 요청을 평가한 후 일치하는 항목 수만 계산합니다. 자세한 정보는 규칙 그룹에 대한 규칙 작업 재정의을 참조하세요.

       이 재정의를 통해 ACFP 관리형 규칙의 잠재적 영향을 모니터링하여 내부 사용 사례에 대한 예외와 같은 예외를 추가할지 여부를 결정할 수 있습니다.
   - 이미 사용 중인 규칙 또는 규칙 그룹보다 높은 우선 순위를 지정하여 웹 ACL의 기존 규칙 다음에 평가되도록 규칙 그룹을 배치합니다. 자세한 정보는 웹 ACL의 규칙 및 규칙 그룹 처리 순서을 참조하세요.

     이렇게 하면 현재의 트래픽 처리가 중단되지 않습니다. 예를 들어 SQL 명령어 삽입이나 교차 사이트 스크립팅과 같은 악성 트래픽을 탐지하는 규칙이 있는 경우 이들 규칙이 이러한 트래픽을 계속 탐지하고 기록합니다. 또는 악의적이지 않은 알려진 트래픽을 허용하는 규칙이 있는 경우 해당 트래픽을 ACFP 관리형 규칙 그룹을 통해 차단하지 않고 계속 허용할 수 있습니다. 테스트 및 조정 활동 중에 처리 순서를 조정하기로 결정할 수 있습니다.
2. 애플리케이션 통합 SDK를 구현합니다.

   AWS WAF JavaScript SDK를 브라우저의 계정 등록 및 계정 생성 경로에 통합하세요. AWS WAF 또한 iOS와 안드로이드 장치를 통합하기 위한 모바일 SDK를 제공합니다. SDK 통합에 대한 자세

한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. 이 권장 사항에 대한 자세한 내용은 애플리케이션 통합 SDK를 ACFP와 함께 사용해야 하는 이유 섹션을 참조하세요.

> **Note**
>
> 애플리케이션 통합 SDK를 사용할 수 없는 경우 웹 ACL에서 편집하고 `AllRequests` 규칙에 적용한 재정의를 제거하여 ACFP 규칙 그룹을 테스트할 수 있습니다. 이렇게 하면 규칙의 Challenge 작업 설정이 활성화되어 요청에 유효한 챌린지 토큰을 포함할 수 있습니다.
>
> 먼저 이 작업을 테스트 환경에서 수행한 다음 프로덕션 환경에서 세심한 주의를 기울여 다시 수행합니다. 이 접근 방식은 사용자를 차단할 가능성이 있습니다. 예를 들어 등록 페이지 경로에서 `GET` 텍스트/html 요청을 수락하지 않는 경우 이 규칙 구성을 통해 등록 페이지의 모든 요청을 효과적으로 차단할 수 있습니다.

3. 웹 ACL에 대한 로깅 및 메트릭을 활성화합니다.

   필요에 따라 로깅, Amazon Security Lake 데이터 수집, 요청 샘플링 및 웹 ACL에 대한 Amazon CloudWatch 지표를 구성합니다. 이러한 가시성 도구를 사용하여 ACFP 관리형 규칙 그룹과 트래픽 간의 상호 작용을 모니터링할 수 있습니다.

   - 로깅에 대한 추가 정보는 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.
   - 아마존 시큐리티 레이크에 대한 자세한 내용은 아마존 시큐리티 레이크란 무엇입니까? 를 참조하십시오. 및 Amazon Security Lake 사용 설명서의 AWS 서비스에서 데이터 수집
   - Amazon CloudWatch 지표에 대한 자세한 내용은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.
   - 웹 요청 샘플링에 대한 자세한 내용은 웹 요청 샘플 보기 섹션을 참조하세요.

4. 웹 ACL을 리소스와 연결

   웹 ACL이 아직 테스트 리소스와 연결되지 않은 경우 해당 리소스를 연결하십시오. 자세한 내용은 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.

5. 트래픽과 ACFP 규칙 일치 모니터링

   트래픽이 정상적으로 흐르고 있고 ACFP 관리형 규칙의 그룹 규칙이 일치하는 웹 요청에 레이블을 추가하고 있는지 확인하십시오. 로그에서 레이블을 볼 수 있고 Amazon CloudWatch 지표에서 ACFP 및 레이블 지표를 볼 수 있습니다. 로그에서 규칙 그룹에서 개수하도록 재정의한 규칙은 계수로 설정된 `action`과 재정의한 구성된 규칙 작업을 나타내는 `overriddenAction`을 포함하는 `ruleGroupList`로 표시됩니다.

6. 규칙 그룹의 보안 인증 정보 검사 기능 테스트

   테스트용 손상된 보안 인증 정보으로 계정 생성을 시도하고 규칙 그룹이 예상대로 보안 인증 정보과 일치하는지 확인합니다.

   a. 보호된 자원의 계정 등록 페이지에 액세스하여 새 계정을 추가해 봅니다. 다음 AWS WAF 테스트 자격 증명 쌍을 사용하여 원하는 테스트를 입력하십시오.

      - 사용자: `WAF_TEST_CREDENTIAL@wafexample.com`
      - 암호: `WAF_TEST_CREDENTIAL_PASSWORD`

      이러한 테스트 보안 인증 정보는 손상된 보안 인증 정보으로 분류되며, ACFP 관리형 규칙 그룹은 로그에서 확인할 수 있는 계정 생성 요청에 `awswaf:managed:aws:acfp:signal:credential_compromised` 레이블을 추가합니다.

   b. 웹 ACL 로그의 테스트 계정 생성 요청에 대한 로그 항목 `labels` 필드에서 `awswaf:managed:aws:acfp:signal:credential_compromised` 레이블을 찾아 봅니다. 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 단원을 참조하세요.

   규칙 그룹이 손상된 보안 인증 정보를 예상대로 캡처하는지 확인한 후에는 보호된 리소스에 필요한 대로 구현을 구성하는 단계를 수행할 수 있습니다.

7. CloudFront 배포의 경우 대량 계정 생성 시도에 대한 규칙 그룹의 관리를 테스트하십시오.

   ACFP 규칙 그룹에 대해 구성한 각 성공 응답 기준에 대해 이 테스트를 실행합니다. 테스트마다 30분 이상의 대기 시간을 둡니다.

   a. 각 성공 기준마다 응답에서 해당 성공 기준을 충족할 계정 생성 시도를 식별합니다. 그런 다음 단일 고객 세션에서 30분 이내에 최소 5번의 성공적인 계정 생성 시도를 수행합니다. 일반적으로 사용자는 사이트에서 단 하나의 계정만 생성합니다.

      계정을 처음 성공적으로 생성한 후에는 `VolumetricSessionSuccessfulResponse` 규칙이 규칙 작업 재정의에 따라 나머지 계정 생성 응답에 대해 일치, 레이블 지정 및 계산을 시작합니다. 이 규칙은 지연 시간으로 인해 처음 한두 개를 놓칠 수 있습니다.

   b. 웹 ACL 로그의 테스트 계정 생성 요청에 대한 로그 항목 `labels` 필드에서 `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_` 레이블을 찾아봅니다. 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 단원을 참조하세요.

이 테스트는 규칙에서 집계된 성공 수가 규칙의 임계값을 초과하는지 확인하여 성공 기준과 응답의 일치 여부를 확인합니다. 임계값에 도달한 후에도 동일한 세션에서 계정 생성 요청을 계속 보내면 성공률이 임계값 아래로 떨어질 때까지 규칙이 계속 일치합니다. 임계값을 초과한 경우 이 규칙은 세션 주소에서의 성공하거나 실패한 계정 생성 시도를 모두 일치시킵니다.

8. ACFP 웹 요청 처리 사용자 지정

   필요에 따라 요청을 명시적으로 허용하거나 차단하는 자체 규칙을 추가하여 ACFP 규칙이 요청을 처리하는 방식을 변경합니다.

   예를 들어 ACFP 레이블을 사용하여 요청을 허용 또는 차단하거나 요청 처리를 사용자 지정할 수 있습니다. ACFP 관리형 규칙 그룹 뒤에 레이블 일치 규칙을 추가하여 적용할 처리에 대해 레이블이 지정된 요청을 필터링할 수 있습니다. 테스트 후에는 관련 ACFP 규칙을 계산 모드로 유지하고 사용자 지정 규칙에서 요청 처리 결정을 유지하십시오. 예시는 ACFP 예제: 손상된 보안 인증 정보에 대한 사용자 지정 응답단원을 참조하세요.

9. 테스트 규칙을 제거하고 ACFP 관리형 규칙 그룹 설정을 활성화합니다.

   상황에 따라 일부 ACFP 규칙을 계산 모드로 유지하기로 결정할 수도 있습니다. 규칙 그룹 내부에 구성된 대로 실행할 규칙의 경우 웹 ACL 규칙 그룹 구성에서 계산 모드를 비활성화합니다. 테스트를 마치면 테스트 레이블 일치 규칙을 제거할 수도 있습니다.

10. 모니터링 및 조정

    웹 요청이 원하는 대로 처리되도록 하려면 사용하려는 ACFP 기능을 활성화한 후 트래픽을 면밀히 모니터링합니다. 규칙 그룹의 규칙 수 재정의 및 자체 규칙을 사용하여 필요에 따라 동작을 조정합니다.

ACFP 규칙 그룹 구현 테스트를 마친 후 아직 브라우저의 계정 등록 및 계정 생성 페이지에 AWS WAF JavaScript SDK를 통합하지 않았다면 그렇게 하는 것이 좋습니다. AWS WAF 또한 iOS와 안드로이드 장치를 통합하기 위한 모바일 SDK를 제공합니다. SDK 통합에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. 이 권장 사항에 대한 자세한 내용은 애플리케이션 통합 SDK를 ACFP와 함께 사용해야 하는 이유 섹션을 참조하세요.

AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 예제

이 섹션에서는 AWS WAF 사기 제어 계정 생성 사기 방지(ACFP) 구현의 일반적인 사용 사례를 충족하는 예제 구성을 보여줍니다.

각 예제는 사용 사례에 대한 설명을 제공하고 나서 사용자 지정 구성 규칙의 JSON 목록에 나와 있는 솔루션을 표시합니다.

> **Note**
>
> 콘솔 웹 ACL JSON 다운로드 또는 규칙 JSON 편집기를 통해, 또는 API 및 명령줄 인터페이스의 `getWebACL` 작업을 통해 이 예제에 표시된 것과 같은 JSON 목록을 검색할 수 있습니다.

주제

ACFP 예제: 단순 구성

다음 JSON 목록은 사기 방지 계정 생성 AWS WAF 사기 방지 (ACFP) 관리 규칙 그룹이 있는 예제 웹 ACL을 보여줍니다. 확인을 위해 추가 `CreationPath` 및 `RegistrationPagePath` 구성을 적어두고, 페이로드 유형과 페이로드에서 새 계정 정보를 찾는 데 필요한 정보도 함께 적어둡니다. 규칙 그룹은 이 정보를 사용하여 계정 생성 요청을 모니터링하고 관리합니다. 이 JSON에는 레이블 네임스페이스 및 웹 ACL의 애플리케이션 통합 URL과 같은 웹 ACL의 자동 생성 설정이 포함됩니다.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
```

```
            "AWSManagedRulesACFPRuleSet": {
              "CreationPath": "/web/signup/submit-registration",
              "RegistrationPagePath": "/web/signup/registration",
              "RequestInspection": {
                "PayloadType": "JSON",
                "UsernameField": {
                  "Identifier": "/form/username"
                },
                "PasswordField": {
                  "Identifier": "/form/password"
                },
                "EmailField": {
                  "Identifier": "/form/email"
                },
                "PhoneNumberFields": [
                  {
                    "Identifier": "/form/country-code"
                  },
                  {
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenumber"
                  }
                ],
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "EnableRegexInPath": false
```

```
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

ACFP 예제: 손상된 보안 인증 정보에 대한 사용자 지정 응답

기본적으로 AWSManagedRulesACFPRuleSet 규칙 그룹에서 수행하는 보안 인증 정보 검사는 요청에 레이블을 지정하고 이를 차단하여 손상된 보안 인증 정보를 처리합니다. 규칙 그룹 및 규칙 동작에 대한 자세한 내용은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요.

사용자가 제공한 계정 보안 인증 정보가 손상되었음을 사용자에게 알리려면 다음과 같이 하면 됩니다.

- **SignalCredentialCompromised** 규칙을 Count로 재정의 - 이렇게 하면 규칙이 일치 요청의 수만을 계산하고 레이블을 지정합니다.
- 사용자 지정 처리가 포함된 레이블 일치 규칙 추가 - ACFP 레이블과 일치하고 사용자 지정 처리를 수행하도록 이 규칙을 구성합니다.

다음 웹 ACL 목록은 SignalCredentialCompromised 규칙 작업이 계산으로 재정의된 이전 예제의 ACFP 관리형 규칙 그룹을 보여줍니다. 이 구성을 사용하면 이 규칙 그룹이 손상된 보안 인증 정보를 사용하는 웹 요청을 평가할 때 요청에 레이블을 지정하지만 차단하지는 않습니다.

또한 웹 ACL에는 이제 aws-waf-credential-compromised 이름이 지정된 사용자 지정 응답과 AccountSignupCompromisedCredentialsHandling 이름이 지정된 새 규칙이 있습니다. 이 규칙은 우선 순위 숫자가 규칙 그룹보다 더 높게 설정되어 있으므로 웹 ACL 평가에서 규칙 그룹 다음에 실행됩니다. 새 규칙은 모든 요청을 규칙 그룹의 손상된 보안 인증 정보 레이블과 일치시킵니다. 규칙에서 일치하는 항목을 찾으면 사용자 지정 응답 본문을 사용하여 요청에 Block 작업을 적용합니다. 사용자 지정 응답 본문은 최종 사용자에게 보안 인증 정보가 손상되었다는 정보를 제공하고 취해야 할 조치를 제안합니다.

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
```

```
                    "Identifier": "/form/country-code"
                  },
                  {
                    "Identifier": "/form/region-code"
                  },
                  {
                    "Identifier": "/form/phonenumber"
                  }
                ],
                "AddressFields": [
                  {
                    "Identifier": "/form/name"
                  },
                  {
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "EnableRegexInPath": false
            }
          }
        ],
        "RuleActionOverrides": [
          {
            "Name": "SignalCredentialCompromised",
            "ActionToUse": {
              "Count": {}
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
```

```
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    },
    {
      "Name": "AccountSignupCompromisedCredentialsHandling",
      "Priority": 1,
      "Statement": {
        "LabelMatchStatement": {
          "Scope": "LABEL",
          "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
            "ResponseCode": 406,
            "CustomResponseBodyKey": "aws-waf-credential-compromised",
            "ResponseHeaders": [
              {
                "Name": "aws-waf-credential-compromised",
                "Value": "true"
              }
            ]
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AccountSignupCompromisedCredentialsHandling"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
```

```
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

ACFP 예제: 대응 검사 구성

다음 JSON 목록은 원본 응답을 검사하도록 구성된 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 관리 규칙 그룹이 있는 예제 웹 ACL을 보여줍니다. 성공 및 응답 상태 코드를 지정하는 응답 검사 구성을 참고하십시오. 헤더, 본문 및 본문 JSON 일치를 기반으로 성공 및 응답 설정을 구성할 수도 있습니다. 이 JSON에는 레이블 네임스페이스 및 웹 ACL의 애플리케이션 통합 URL과 같은 웹 ACL의 자동 생성 설정이 포함됩니다.

> **Note**
>
> ATP 응답 검사는 배포를 보호하는 웹 ACL에서만 사용할 수 있습니다. CloudFront

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
```

```
        "CreationPath": "/web/signup/submit-registration",
        "RegistrationPagePath": "/web/signup/registration",
        "RequestInspection": {
          "PayloadType": "JSON",
          "UsernameField": {
            "Identifier": "/form/username"
          },
          "PasswordField": {
            "Identifier": "/form/password"
          },
          "EmailField": {
            "Identifier": "/form/email"
          },
          "PhoneNumberFields": [
            {
              "Identifier": "/form/country-code"
            },
            {
              "Identifier": "/form/region-code"
            },
            {
              "Identifier": "/form/phonenumber"
            }
          ],
          "AddressFields": [
            {
              "Identifier": "/form/name"
            },
            {
              "Identifier": "/form/street-address"
            },
            {
              "Identifier": "/form/city"
            },
            {
              "Identifier": "/form/state"
            },
            {
              "Identifier": "/form/zipcode"
            }
          ]
        },
        "ResponseInspection": {
          "StatusCode": {
```

```
                    "SuccessCodes": [
                      200
                    ],
                    "FailureCodes": [
                      401
                    ]
                  }
                },
                "EnableRegexInPath": false
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
  }
```

AWS WAF 사기 방지 계정 탈취 방지 (ATP)

계정 탈취는 공격자가 개인 계정에 무단으로 액세스하는 온라인 불법 활동입니다. 공격자는 도용된 보안 인증 정보를 사용하거나 일련의 시도를 통해 피해자의 암호를 추측하는 등 다양한 방법으로 이를 수행할 수 있습니다. 공격자는 액세스 권한을 얻으면 피해자의 돈, 정보 또는 서비스를 훔칠 수 있습니다. 공격자는 피해자로 가장하여 피해자가 소유한 다른 계정에 액세스하거나 다른 사람 또는 조직의 계정에 액세스할 수 있습니다. 또한 피해자가 자신의 계정에 접근하지 못하도록 차단하기 위해 사용자의 비밀번호를 변경하려고 시도할 수도 있습니다.

AWS WAF 사기 통제 계정 탈취 방지 (ATP) 기능을 구현하여 계정 탈취 시도를 모니터링하고 통제할 수 있습니다. AWS WAF AWS Managed Rules 규칙 그룹 `AWSManagedRulesATPRuleSet` 및 동반 애플리케이션 통합 SDK에서 이 기능을 제공합니다.

ATP 관리형 규칙 그룹은 사기 계정 탈취 시도의 일부일 수 있는 요청에 레이블을 지정하여 관리합니다. 규칙 그룹은 클라이언트가 애플리케이션의 로그인 엔드포인트로 보내는 로그인 시도를 검사하여 이 작업을 수행합니다.

- 요청 검사 — ATP를 사용하면 비정상적인 로그인 시도 및 보안 인증 정보를 도용한 로그인 시도를 파악하고 제어할 수 있으므로 사기 행위로 이어질 수 있는 계정 탈취를 방지할 수 있습니다. ATP는 도용된 보안 인증 정보 데이터베이스에서 이메일과 암호 조합을 검사합니다. 이 데이터베이스는 유출된 보안 인증 정보가 다크 웹에서 발견될 때마다 정기적으로 업데이트됩니다. ATP는 IP 주소 및 클라이언트 세션별로 데이터를 집계하여 의심스러운 요청을 너무 많이 보내는 클라이언트를 탐지하고 차단합니다.
- 응답 검사 — CloudFront 배포의 경우 ATP 규칙 그룹은 들어오는 로그인 요청을 검사하는 것 외에도 로그인 시도에 대한 애플리케이션의 응답을 검사하여 성공률과 실패율을 추적합니다. ATP는 이 정보를 사용하여 로그인 실패가 너무 많은 클라이언트 세션 또는 IP 주소를 일시적으로 차단할 수 있습니다. AWS WAF 는 응답 검사를 비동기적으로 수행하므로 이 작업으로 인해 웹 트래픽의 지연 시간이 증가하지 않습니다.

> **Note**
>
> 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

> **Note**
>
> Amazon Cognito 사용자 풀에는 ATP 기능을 사용할 수 없습니다.

주제

- AWS WAF 사기 통제 계정 탈취 방지 (ATP) 예제

AWS WAF ATP 컴포넌트

AWS WAF 사기 방지 계정 탈취 방지 (ATP) 의 주요 구성 요소는 다음과 같습니다.

- **`AWSManagedRulesATPRuleSet`**— 이 AWS 관리형 규칙 규칙 그룹의 규칙은 다양한 유형의 계정 탈취 활동을 탐지, 분류 및 처리합니다. 이 규칙 그룹은 클라이언트가 지정된 로그인 엔드포인트로 보내는 HTTP POST 웹 요청을 검사합니다. 보호된 CloudFront 배포의 경우 규칙 그룹은 배포가 이러한 요청에 다시 보내는 응답도 검사합니다. 규칙 그룹의 규칙 목록은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 섹션을 참조하세요. 관리형 규칙 그룹 참조 문을 사용하여 웹 ACL에 이 규칙 그룹을 포함할 수 있습니다. 이 규칙 그룹 사용에 대한 자세한 내용은 ATP 관리형 규칙 그룹을 새 웹 ACL에 추가 섹션을 참조하세요.

  > **Note**
  >
  > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

- 애플리케이션의 로그인 페이지에 대한 세부 정보 - `AWSManagedRulesATPRuleSet` 규칙 그룹을 웹 ACL에 추가할 때 로그인 페이지에 대한 정보를 제공해야 합니다. 이렇게 하면 규칙 그룹이 검사하는 요청의 범위를 좁히고 웹 요청의 보안 인증 정보 사용을 적절하게 검증할 수 있습니다. ATP 규칙 그룹은 이메일 형식의 사용자 이름을 사용합니다. 자세한 정보는 ATP 관리형 규칙 그룹을 새 웹 ACL에 추가을 참조하세요.
- 보호 CloudFront 배포의 경우 응용 프로그램이 로그인 시도에 응답하는 방법에 대한 세부 정보 - 로그인 시도에 대한 응용 프로그램의 응답에 대한 세부 정보를 제공하면 규칙 그룹은 실패한 로그인 시도를 너무 많이 보내는 클라이언트를 추적하고 관리합니다. 이 옵션의 구성에 대한 자세한 내용은 ATP 관리형 규칙 그룹을 새 웹 ACL에 추가 섹션을 참조하세요.
- JavaScript 및 모바일 애플리케이션 통합 SDK — ATP 구현과 함께 AWS WAF JavaScript 및 모바일 SDK를 구현하여 규칙 그룹이 제공하는 모든 기능을 사용할 수 있도록 하십시오. 많은 ATP 규칙은 합법적인 클라이언트 트래픽을 봇 트래픽과 분리하는 데 필요한 세션 수준 클라이언트 확인 및 행동 집계에 대해 SDK에서 제공하는 정보를 사용합니다. SDK에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합을 참조하세요.

ATP 구현을 다음과 결합하여 보호 기능을 모니터링, 조정 및 사용자 지정할 수 있습니다.

- 로깅 및 지표 — 웹 ACL에 대한 로그, Amazon Security Lake 데이터 수집 및 Amazon CloudWatch 지표를 구성 및 활성화하여 트래픽을 모니터링하고 ACFP 관리 규칙 그룹이 이에 미치는 영향을 이해할 수 있습니다. 웹 요청에 `AWSManagedRulesATPRuleSet` 추가되는 레이블은 데이터에 포함됩니다. 옵션에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅아마존을 통한 모니터링 CloudWatch, 및 Amazon Security Lake란 무엇입니까? 를 참조하십시오. .

  요구 사항과 표시되는 트래픽에 따라 `AWSManagedRulesATPRuleSet` 구현을 사용자 지정해야 할 수도 있습니다. 예를 들어 ATP 평가에서 일부 트래픽을 제외하거나 범위 축소 명령문 또는 레이블 매칭 규칙과 같은 AWS WAF 기능을 사용하여 ATP 평가에서 식별되는 일부 계정 탈취 시도를 처리하는 방식을 변경할 수 있습니다.
- 레이블 및 레이블 일치 규칙 - `AWSManagedRulesATPRuleSet`에 있는 모든 규칙의 경우 차단 동작을 계산으로 전환한 다음, 규칙에 의해 추가되는 레이블과 일치시킬 수 있습니다. 이 접근 방식을 사용하여 ATP 관리형 규칙 그룹으로 식별되는 웹 요청을 처리하는 방식을 사용자 지정할 수 있습니다. 레이블 일치 문의 레이블 지정 및 사용에 대한 자세한 내용은 레이블 일치 규칙 문 및 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.
- 사용자 지정 요청 및 응답 - 허용하는 요청에 사용자 지정 헤더를 추가하고 차단한 요청에 대해 사용자 지정 응답을 보낼 수 있습니다. 이렇게 하려면 레이블 일치를 AWS WAF 사용자 지정 요청 및 응답 기능과 페어링해야 합니다. 요청 및 응답을 사용자 지정하는 방법에 대한 자세한 내용은 AWS WAF의 사용자 지정된 웹 요청 및 응답 섹션을 참조하세요.

애플리케이션 통합 SDK를 ATP와 함께 사용해야 하는 이유

ATP 관리형 규칙 그룹에는 애플리케이션 통합 SDK가 생성하는 챌린지 토큰이 필요합니다. 이러한 토큰을 사용하면 규칙 그룹이 제공하는 모든 보호 기능을 사용할 수 있습니다.

ATP 규칙 그룹을 가장 효율적으로 사용하려면 애플리케이션 통합 SDK를 구현하는 것이 좋습니다. 규칙 그룹이 스크립트에서 획득한 토큰을 활용하도록 하려면 ATP 규칙 그룹보다 먼저 챌린지 스크립트를 실행해야 합니다. 이는 애플리케이션 통합 SDK를 사용하여 자동으로 수행됩니다. 또는 SDK를 사용할 수 없는 경우 ATP 규칙 그룹에서 검사할 모든 요청에 대해 Challenge 또는 CAPTCHA 규칙 작업을 실행하도록 웹 ACL을 구성할 수도 있습니다. Challenge 또는 CAPTCHA 규칙 작업을 사용하는 경우 추가 비용이 발생할 수 있습니다. 요금에 대한 자세한 내용은 AWS WAF Pricing을 참조하세요.

토큰이 필요하지 않은 ATP 규칙 그룹의 기능

웹 요청에 토큰이 없는 경우 ATP 관리형 규칙 그룹은 다음 유형의 트래픽을 차단할 수 있습니다.

- 로그인 요청을 많이 하는 단일 IP 주소.
- 단시간에 실패한 로그인 요청이 많이 발생하는 단일 IP 주소.

- 동일한 사용자 이름을 사용하지만 암호를 변경하며 암호 순회로 로그인을 시도합니다.

토큰이 필요한 ATP 규칙 그룹의 기능

챌린지 토큰에 제공된 정보는 규칙 그룹 및 전체 클라이언트 애플리케이션 보안의 기능을 확장합니다.

토큰은 각 웹 요청과 함께 클라이언트 정보를 제공하여 ATP 규칙 그룹이 정상적인 클라이언트 세션을 잘못된 클라이언트 세션과 분리할 수 있도록 합니다. 둘 다 단일 IP 주소에서 시작된 경우에도 마찬가지입니다. 규칙 그룹은 탐지 및 완화를 세부적으로 조정하기 위해 토큰 정보를 사용하여 클라이언트 세션 요청 동작을 집계합니다.

웹 요청에서 토큰을 사용할 수 있는 경우 ATP 규칙 그룹은 세션 수준에서 다음과 같은 추가 범주의 클라이언트를 탐지하고 차단할 수 있습니다.

- SDK가 관리하는 자동 챌린지에 실패한 클라이언트 세션
- 사용자 이름 또는 암호를 순회하는 클라이언트 세션. 이를 보안 인증 정보 스터핑이라고도 합니다.
- 도용된 보안 인증 정보를 반복적으로 사용하여 로그인하는 클라이언트 세션
- 로그인을 시도하는 데 오랜 시간이 걸리는 클라이언트 세션.
- 로그인 요청이 많은 클라이언트 세션 ATP 규칙 그룹은 IP 주소를 기준으로 클라이언트를 차단할 수 있는 AWS WAF 속도 기반 규칙보다 더 나은 클라이언트 격리를 제공합니다. 또한 ATP 규칙 그룹은 더 낮은 임계값을 사용합니다.
- 짧은 시간 내에 실패 로그인 요청이 많은 클라이언트 세션 이 기능은 보호된 Amazon CloudFront 배포에 사용할 수 있습니다.

규칙 그룹 기능에 대한 자세한 내용은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 섹션을 참조하세요.

SDK에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. AWS WAF 토큰에 대한 자세한 내용은 을 참조하십시오AWS WAF 웹 요청 토큰. 규칙 작업에 대한 자세한 내용은 CAPTCHA그리고 Challenge 안에 AWS WAF 섹션을 참조하세요.

ATP 관리형 규칙 그룹을 새 웹 ACL에 추가

웹 트래픽의 계정 탈취 활동을 인식하도록 ATP 관리형 규칙 그룹을 구성하려면 클라이언트가 로그인 요청을 해당 애플리케이션에 보내는 방법에 대한 정보를 제공합니다. 보호 대상 Amazon CloudFront 배포의 경우 애플리케이션이 로그인 요청에 응답하는 방식에 대한 정보도 제공합니다. 이 구성은 관리형 규칙 그룹의 일반 구성에 추가됩니다.

규칙 그룹 설명 및 규칙 목록은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 섹션을 참조하세요.

> **Note**
>
> ATP 도용된 보안 인증 데이터베이스에는 이메일 형식의 사용자 이름만 포함됩니다.

이 지침은 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 만들고 관리하는 방법을 일반적으로 알고 있는 사용자를 대상으로 합니다. 이러한 주제는 이 안내서의 이전 섹션에 설명되어 있습니다. 웹 ACL에 관리형 규칙 그룹을 추가하는 방법에 대한 기본 정보는 콘솔을 통해 웹 ACL에 관리형 규칙 그룹 추가 섹션을 참조하세요.

모범 사례 따르기

지능형 위협 완화 모범 사례의 모범 사례에 따라 ATP 규칙 그룹을 사용합니다.

웹 ACL에서 **`AWSManagedRulesATPRuleSet`** 규칙 그룹을 사용하려면

1. AWS 관리형 규칙 그룹을 웹 ACL에 추가하고 `AWSManagedRulesATPRuleSet` 저장하기 전에 규칙 그룹 설정을 편집하십시오.

   > **Note**
   >
   > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

2. 규칙 그룹 구성 창에서 ATP 규칙 그룹이 로그인 요청을 검사하는 데 사용하는 정보를 제공합니다.

   a. 경로에 정규 표현식 사용의 경우 로그인 페이지 경로 사양에 맞는 정규 표현식 일치를 AWS WAF 수행하려면 이 옵션을 켜십시오.

      AWS WAF 일부 예외를 제외하고 PCRE 라이브러리에서 `libpcre` 사용하는 패턴 구문을 지원합니다. 이 라이브러리는 PCRE - Perl 호환 정규식에 문서화되어 있습니다. AWS WAF 지원에 대한 자세한 내용은 을 참조하십시오정규 표현식 패턴 매칭 AWS WAF.

   b. 로그인 경로에 애플리케이션의 로그인 엔드포인트 경로를 입력합니다. 이 규칙 그룹은 지정된 로그인 엔드포인트에 대한 HTTP POST 요청만 검사합니다.

> **Note**
>
> 엔드포인트에 대한 일치는 대/소문자를 구분하지 않습니다. Regex 사양에는 대소문자를 구분하지 않는 일치를 비활성화하는 플래그 `(?-i)`이(가) 포함되어서는 안 됩니다. 문자열 사양은 슬래시 `/`로 시작해야 합니다.

예를 들어, URL `https://example.com/web/login`의 경우 문자열 경로 사양 `/web/login`을(를) 제공할 수 있습니다. 입력한 경로로 시작하는 로그인 경로는 일치하는 것으로 간주됩니다. 예를 들어 `/web/login`는 로그인 경로 `/web/login`, `/web/login/`, `/web/loginPage` 및 `/web/login/thisPage`와 일치하지만, `/home/web/login` 또는 `/website/login` 로그인 경로와는 일치하지 않습니다.

c. 요청 검사의 경우 요청 본문에서 사용자 이름 및 암호를 입력하는 필드 이름과 요청 페이로드 유형을 제공하여 애플리케이션에서 로그인 시도를 수락하는 방식을 지정합니다. 필드 이름 사양은 페이로드 유형에 따라 달라집니다.

- JSON 페이로드 유형 - JSON 포인터 구문으로 필드 이름을 지정합니다. JSON 포인터 구문에 대한 자세한 내용은 IETF (인터넷 엔지니어링 태스크 포스) 문서 JavaScript객체 표기법 (JSON) 포인터를 참조하십시오.

  예를 들어 다음 JSON 페이로드 예제의 경우 사용자 이름 필드 사양은 `/login/username`이고 암호 필드 사양은 `/login/password`입니다.

  ```
  {
      "login": {
          "username": "THE_USERNAME",
          "password": "THE_PASSWORD"
      }
  }
  ```

- FORM_ENCODED 페이로드 유형 - HTML 양식 이름을 사용합니다.

  예를 들어 입력 요소의 이름이 `username1` 및 `password1`인 HTML 양식의 경우 사용자 이름 필드 사양은 `username1`이고 암호 필드 사양은 `password1`입니다.

d. Amazon CloudFront 배포를 보호하는 경우 응답 검사에서 애플리케이션이 로그인 시도에 대한 응답의 성공 또는 실패를 표시하는 방법을 지정하십시오.

> **Note**
>
> ATP 응답 검사는 배포를 보호하는 웹 ACL에서만 사용할 수 있습니다. CloudFront

ATP에서 검사할 단일 구성 요소를 로그인 응답에 지정합니다. 본문 및 JSON 구성 요소 유형의 경우 AWS WAF 구성 요소의 처음 65,536바이트(64KB)를 검사할 수 있습니다.

인터페이스에 지정된 구성 요소 유형에 대한 검사 기준을 제공합니다. 구성 요소에서 검사할 성공 및 실패 기준을 모두 제공해야 합니다.

예를 들어 애플리케이션이 응답의 상태 코드에 로그인 시도의 상태를 표시하고 성공 시 `200 OK` 그리고 실패 시 `401 Unauthorized` 또는 `403 Forbidden`을 사용한다고 가정해 보겠습니다. 응답 검사 구성 요소 유형을 상태 코드로 설정한 다음 성공 텍스트 상자에 `200`을 입력하고, 실패 텍스트 상자의 첫 번째 줄에 `401` 그리고 두 번째 줄에 `403`을 입력합니다.

ATP 규칙 그룹은 성공 또는 실패 검사 기준과 일치하는 응답만 계산합니다. 규칙 그룹 규칙은 계산된 응답 중 실패율이 너무 높은 클라이언트에 적용됩니다. 규칙 그룹의 규칙이 정확하게 작동하려면 성공 및 실패한 로그인 시도 모두에 대한 전체 정보를 제공해야 합니다.

로그인 응답을 검사하는 규칙을 보려면 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹의 규칙 목록에서 `VolumetricIpFailedLoginResponseHigh` 및 `VolumetricSessionFailedLoginResponseHigh`를 찾아보십시오.

3. 규칙 그룹에 사용할 추가 구성을 모두 제공합니다.

   관리형 규칙 그룹 문에 범위 축소 문을 추가하여 규칙 그룹이 검사하는 요청의 범위를 추가 제한할 수 있습니다. 예를 들어 특정 쿼리 인수 또는 쿠키가 있는 요청만 검사할 수 있습니다. 규칙 그룹은 범위 축소 문의 기준과 일치하는 지정된 로그인 엔드포인트에 대한 HTTP POST 요청만 검사합니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요.

4. 웹 ACL에 대한 변경 사항을 저장합니다.

프로덕션 트래픽용 ATP 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 이를 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 개수 모드에서 테스트하고 조정한 다음 활성화합니다. 지침은 다음 섹션을 참조하세요.

ATP 테스트 및 배포

이 섹션에서는 사이트에 대한 AWS WAF 사기 통제 계정 도용 방지 (ATP) 구현을 구성하고 테스트하기 위한 일반적인 지침을 제공합니다. 따르기로 선택한 구체적인 단계는 요구 사항, 리소스 및 수신하는 웹 요청에 따라 달라집니다.

이 정보는 AWS WAF 보호 기능 테스트 및 조정에 제공된 테스트 및 조정에 대한 일반 정보 외의 정보입니다.

> **Note**
>
> AWS 관리형 규칙은 일반적인 웹 위협으로부터 사용자를 보호하도록 설계되었습니다. 설명서에 따라 AWS 관리형 규칙 그룹을 사용하면 애플리케이션에 또 다른 보안 계층이 추가됩니다. 하지만 AWS 관리형 규칙 규칙 그룹은 선택한 AWS 리소스에 따라 결정되는 보안 책임을 대체하기 위한 것이 아닙니다. 공동 책임 모델을 참조하여 AWS 리소스가 적절하게 보호되도록 하세요.

> **⚠ 프로덕션 트래픽 위험**
>
> 프로덕션 트래픽용 ATP 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 이를 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 개수 모드에서 테스트하고 조정한 다음 활성화합니다.

AWS WAF ATP 구성을 검증하는 데 사용할 수 있는 테스트 인증서를 제공합니다. 다음 절차에서는 ATP 관리형 규칙 그룹을 사용하도록 테스트 웹 ACL을 구성하고, 규칙 그룹에서 추가한 레이블을 캡처하도록 규칙을 구성한 다음, 이러한 테스트 보안 인증을 사용하여 로그인 시도를 실행합니다. 로그인 시도에 대한 Amazon CloudWatch 지표를 확인하여 웹 ACL이 시도를 제대로 관리했는지 확인할 수 있습니다.

이 지침은 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 만들고 관리하는 방법을 일반적으로 알고 있는 사용자를 대상으로 합니다. 이러한 주제는 이 안내서의 이전 섹션에 설명되어 있습니다.

AWS WAF 사기 통제 계정 탈취 방지 (ATP) 구현을 구성하고 테스트하려면

이러한 단계를 먼저 테스트 환경에서 수행한 다음, 프로덕션 환경에서 수행합니다.

1. AWS WAF 사기 방지 계정 인수 방지 (ATP) 관리 규칙 그룹을 카운트 모드에 추가합니다.

   > **Note**
   >
   > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

   AWS 관리형 규칙 규칙 그룹을 `AWSManagedRulesATPRuleSet` 새 웹 ACL이나 기존 웹 ACL에 추가하고 현재 웹 ACL 동작을 변경하지 않도록 구성합니다. 이 규칙 그룹의 규칙 및 레이블에 대한 자세한 내용은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 섹션을 참조하세요.

   - 관리형 규칙 그룹을 추가할 때는 해당 규칙 그룹을 편집하고 다음을 수행합니다.
     - 규칙 그룹 구성 창에서 애플리케이션의 로그인 페이지의 세부 정보를 제공합니다. ATP 규칙 그룹은 이 정보를 사용하여 로그인 활동을 모니터링합니다. 자세한 정보는 ATP 관리형 규칙 그룹을 새 웹 ACL에 추가을 참조하세요.
     - 규칙 창에서 모든 규칙 모든 규칙 작업 재정의 드롭다운을 열고 Count를 선택합니다. 이 구성을 사용하면 AWS WAF 는 요청에 레이블을 여전히 추가하면서 규칙 그룹의 모든 규칙과 비교하여 요청을 평가한 후 일치하는 항목 수만 계산합니다. 자세한 정보는 규칙 그룹에 대한 규칙 작업 재정의을 참조하세요.

       이 재정의를 통해 ATP 관리형 규칙의 잠재적 영향을 모니터링하여 내부 사용 사례에 대한 예외와 같은 예외를 추가할지 여부를 결정할 수 있습니다.
   - 이미 사용 중인 규칙 또는 규칙 그룹보다 높은 우선 순위를 지정하여 웹 ACL의 기존 규칙 다음에 평가되도록 규칙 그룹을 배치합니다. 자세한 정보는 웹 ACL의 규칙 및 규칙 그룹 처리 순서을 참조하세요.

     이렇게 하면 현재의 트래픽 처리가 중단되지 않습니다. 예를 들어 SQL 명령어 삽입이나 교차 사이트 스크립팅과 같은 악성 트래픽을 탐지하는 규칙이 있는 경우 이들 규칙이 이러한 트래픽을 계속 탐지하고 기록합니다. 또는 악의적이지 않은 알려진 트래픽을 허용하는 규칙이 있는 경우 해당 트래픽을 ATP 관리형 규칙 그룹을 통해 차단하지 않고 계속 허용할 수 있습니다. 테스트 및 조정 활동 중에 처리 순서를 조정하기로 결정할 수 있습니다.

2. 웹 ACL에 대한 로깅 및 메트릭을 활성화합니다.

   필요에 따라 로깅, Amazon Security Lake 데이터 수집, 요청 샘플링 및 웹 ACL에 대한 Amazon CloudWatch 지표를 구성합니다. 이러한 가시성 도구를 사용하여 ATP 관리형 규칙 그룹과 트래픽 간의 상호 작용을 모니터링할 수 있습니다.

- 로깅 구성 및 사용에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.
- 아마존 시큐리티 레이크에 대한 자세한 내용은 아마존 시큐리티 레이크란 무엇입니까? 를 참조하십시오. 및 Amazon Security Lake 사용 설명서의 AWS 서비스에서 데이터 수집
- Amazon CloudWatch 지표에 대한 자세한 내용은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.
- 웹 요청 샘플링에 대한 자세한 내용은 웹 요청 샘플 보기 섹션을 참조하세요.

3. 웹 ACL을 리소스와 연결

   웹 ACL이 아직 테스트 리소스와 연결되지 않은 경우 해당 리소스를 연결하십시오. 자세한 내용은 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.

4. 트래픽과 ATP 규칙 일치 모니터링

   트래픽이 정상적으로 흐르고 있고 ATP 관리형 규칙의 그룹 규칙이 일치하는 웹 요청에 레이블을 추가하고 있는지 확인하십시오. 로그에서 레이블을 볼 수 있고 Amazon CloudWatch 지표에서 ATP 및 레이블 지표를 볼 수 있습니다. 로그에서 규칙 그룹에서 개수하도록 재정의한 규칙은 계수로 설정된 `action`과 재정의한 구성된 규칙 작업을 나타내는 `overriddenAction`을 포함하는 `ruleGroupList`로 표시됩니다.

5. 규칙 그룹의 보안 인증 정보 검사 기능 테스트

   테스트용 손상된 보안 인증 정보로 로그인을 시도하고 규칙 그룹이 예상대로 보안 인증 정보와 일치하는지 확인합니다.

   a. 다음 AWS WAF 테스트 자격 증명 쌍을 사용하여 보호된 리소스의 로그인 페이지에 로그인합니다.

      - 사용자: `WAF_TEST_CREDENTIAL@wafexample.com`
      - 암호: `WAF_TEST_CREDENTIAL_PASSWORD`

      이러한 테스트 보안 인증 정보는 손상된 보안 인증 정보으로 분류되며, ACFP 관리형 규칙 그룹은 로그에서 확인할 수 있는 계정 생성 요청에 `awswaf:managed:aws:atp:signal:credential_compromised` 레이블을 추가합니다.

   b. 웹 ACL 로그의 테스트 로그인 웹 요청에 대한 로그 항목 `labels` 필드에서 `awswaf:managed:aws:atp:signal:credential_compromised` 레이블을 찾아 봅니다. 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 단원을 참조하세요.

규칙 그룹이 손상된 보안 인증 정보를 예상대로 캡처하는지 확인한 후에는 보호된 리소스에 필요한 대로 구현을 구성하는 단계를 수행할 수 있습니다.

6. CloudFront 배포의 경우 규칙 그룹의 로그인 실패 관리를 테스트하세요.

   a. ATP 규칙 그룹에 대해 구성한 각 성공 응답 기준에 대해 이 테스트를 실행합니다. 테스트마다 10분 이상의 대기 시간을 둡니다.

      단일 실패 기준을 테스트하려면 응답에서 해당 기준에 따라 실패할 로그인 시도를 식별합니다. 그런 다음 단일 클라이언트 IP 주소에서 10분 이내에 10회 이상의 로그인 실패를 시도합니다.

      볼륨 측정 실패 로그인 규칙은 처음 6회 실패 후 나머지 시도와의 일치, 레이블 지정 및 계산을 시작해야 합니다. 이 규칙은 지연 시간으로 인해 처음 한두 개를 놓칠 수 있습니다.

   b. 웹 ACL 로그의 테스트 로그인 웹 요청에 대한 로그 항목 `labels` 필드에서 `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` 레이블을 찾아 봅니다. 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 단원을 참조하세요.

   이러한 테스트는 실패한 로그인 수가 `VolumetricIpFailedLoginResponseHigh` 규칙의 임계값을 초과하는지 확인하여 실패 기준이 응답과 일치하는지 확인합니다. 임계값에 도달한 후에도 동일한 IP 주소에서 로그인 요청을 계속 보내면 성공률이 임계값 아래로 떨어질 때까지 규칙이 계속 일치합니다. 임계값을 초과한 경우 이 규칙은 IP 주소에서의 성공하거나 실패한 로그인 시도를 모두 일치시킵니다.

7. ATP 웹 요청 처리를 사용자 지정합니다.

   필요에 따라 요청을 명시적으로 허용하거나 차단하는 자체 규칙을 추가하여 ATP 규칙이 요청을 처리하는 방식을 변경합니다.

   예를 들어 ATP 레이블을 사용하여 요청을 허용 또는 차단하거나 요청 처리를 사용자 지정할 수 있습니다. ATP 관리형 규칙 그룹 뒤에 레이블 일치 규칙을 추가하여 적용할 처리에 대해 레이블이 지정된 요청을 필터링할 수 있습니다. 테스트 후에는 관련 ATP 규칙을 계수 모드로 유지하고 요청 처리 결정을 사용자 지정 규칙에서 유지하십시오. 예시는 ATP 예제: 분실 및 손상된 보안 인증 정보에 대한 사용자 지정 처리단원을 참조하세요.

8. 테스트 규칙을 제거하고 ATP 관리형 규칙 그룹 설정을 활성화합니다.

   상황에 따라 일부 ATP 규칙이 계수 모드에서 나가도록 결정할 수도 있습니다. 규칙 그룹 내부에 구성된 대로 실행할 규칙의 경우 웹 ACL 규칙 그룹 구성에서 계산 모드를 비활성화합니다. 테스트를 마치면 테스트 레이블 일치 규칙을 제거할 수도 있습니다.

9. 모니터링 및 조정

   웹 요청이 원하는 대로 처리되도록 하려면 사용하려는 ATP 기능을 활성화한 후 트래픽을 면밀히 모니터링합니다. 규칙 그룹의 규칙 수 재정의 및 자체 규칙을 사용하여 필요에 따라 동작을 조정합니다.

ATP 규칙 그룹 구현 테스트를 마친 후 아직 구현하지 않았다면 탐지 기능을 강화하기 위해 AWS WAF JavaScript SDK를 브라우저 로그인 페이지에 통합하는 것이 좋습니다. AWS WAF 또한 iOS와 안드로이드 장치를 통합하기 위한 모바일 SDK를 제공합니다. SDK 통합에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. 이 권장 사항에 대한 자세한 내용은 애플리케이션 통합 SDK를 ATP와 함께 사용해야 하는 이유 섹션을 참조하세요.

AWS WAF 사기 통제 계정 탈취 방지 (ATP) 예제

이 섹션에서는 AWS WAF 사기 제어 계정 탈취 방지(ATP) 구현의 일반적인 사용 사례를 충족하는 예제 구성을 보여줍니다.

각 예제는 사용 사례에 대한 설명을 제공하고 나서 사용자 지정 구성 규칙의 JSON 목록에 나와 있는 솔루션을 표시합니다.

> **Note**
>
> 콘솔 웹 ACL JSON 다운로드 또는 규칙 JSON 편집기를 통해, 또는 API 및 명령줄 인터페이스의 `getWebACL` 작업을 통해 이 예제에 표시된 것과 같은 JSON 목록을 검색할 수 있습니다.

주제

- ATP 예제: 단순 구성
- ATP 예제: 분실 및 손상된 보안 인증 정보에 대한 사용자 지정 처리
- ATP 예제: 대응 검사 구성

ATP 예제: 단순 구성

다음 JSON 목록은 AWS WAF 사기 통제 계정 탈취 방지 (ATP) 관리 규칙 그룹이 있는 예제 웹 ACL을 보여줍니다. 참고로, 추가 로그인 페이지 구성은 로그인 요청을 모니터링하고 관리하는 데 필요한 정보를 규칙 그룹에 제공합니다. 이 JSON에는 레이블 네임스페이스 및 웹 ACL의 애플리케이션 통합 URL과 같은 웹 ACL의 자동 생성 설정이 포함됩니다.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
                              "EnableRegexInPath": false
```

```
                            }
                        }
                    ]
                }
            }
        }
    ],
    "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "ATPValidationAcl"
    },
    "DefaultAction": {
        "Allow": {}
    },
    "ManagedByFirewallManager": false,
    "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
    "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
    "Name": "ATPModuleACL"
},
"ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
"LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

ATP 예제: 분실 및 손상된 보안 인증 정보에 대한 사용자 지정 처리

기본적으로 규칙 그룹 AWSManagedRulesATPRuleSet에서 수행하는 보안 인증 정보 검사는 웹 요청을 다음과 같이 처리합니다.

- 보안 인증 정보 누락 - 요청에 레이블을 지정하고 차단합니다.
- 손상된 보안 인증 정보 - 요청에 레이블을 지정하지만, 차단하거나 개수를 계산하지 않습니다.

규칙 그룹 및 규칙 동작에 대한 자세한 내용은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 섹션을 참조하세요.

다음을 수행하여 보안 인증 정보가 누락되거나 손상된 웹 요청에 대한 사용자 지정 처리를 추가할 수 있습니다.

- **MissingCredential** 규칙을 Count로 재정의 - 이 규칙 작업 재정의는 규칙이 일치 요청만 계산하고 레이블을 지정하도록 합니다.

- 사용자 지정 처리가 포함된 레이블 일치 규칙 추가 - ATP 레이블과 일치하고 사용자 지정 처리를 수행하도록 이 규칙을 구성합니다. 예를 들어, 고객을 가입 페이지로 리디렉션할 수 있습니다.

다음 규칙은 `MissingCredential` 규칙 작업이 계수로 재정의된 이전 예제의 ATP 관리형 규칙 그룹을 보여줍니다. 이로 인해 규칙은 일치하는 요청에 해당 레이블을 적용하고 나서 요청을 차단하는 대신 해당 요청의 개수만 계산합니다.

```
"Rules": [
    {
        "Priority": 1,
        "OverrideAction": {
            "None": {}
        },
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AccountTakeOverValidationRule"
        },
        "Name": "DetectCompromisedUserCredentials",
        "Statement": {
            "ManagedRuleGroupStatement": {
                "ManagedRuleGroupConfigs": [
                  {
                    "AWSManagedRulesATPRuleSet": {
                      "LoginPath": "/web/login",
                      "RequestInspection": {
                        "PayloadType": "JSON",
                        "UsernameField": {
                          "Identifier": "/form/username"
                        },
                        "PasswordField": {
                          "Identifier": "/form/password"
                        }
                      },
                      "EnableRegexInPath": false
                    }
                  }
                ]
                "VendorName": "AWS",
                "Name": "AWSManagedRulesATPRuleSet",
                "RuleActionOverrides": [
                  {
```

```
                    "ActionToUse": {
                      "Count": {}
                    },
                    "Name": "MissingCredential"
                  }
                ],
                "ExcludedRules": []
            }
        }
    }
],
```

이 구성을 사용하면 이 규칙 그룹이 분실 또는 손상된 보안 인증 정보를 사용하는 웹 요청을 평가할 때 요청에 레이블을 지정하지만 차단하지는 않습니다.

다음 규칙의 우선 순위 설정 숫자 값은 이전 규칙 그룹보다 더 높습니다. AWS WAF 는 가장 낮은 값부터 순서대로 규칙을 평가하므로 이 규칙은 규칙 그룹 평가 후에 평가됩니다. 규칙은 보안 인증 정보 레이블 중 하나와 일치하고 일치 요청에 대한 사용자 지정 응답을 보내도록 구성됩니다.

```
"Name": "redirectToSignup",
      "Priority": 10,
      "Statement": {
        "OrStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:missing_credential"
              }
            },
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:atp:signal:credential_compromised"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {
          "CustomResponse": {
             your custom response settings
```

```
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "redirectToSignup"
      }
```

ATP 예제: 대응 검사 구성

다음 JSON 목록은 원본 응답을 검사하도록 구성된 AWS WAF 사기 통제 계정 인수 방지 (ATP) 관리 규칙 그룹이 있는 예제 웹 ACL을 보여줍니다. 성공 및 응답 상태 코드를 지정하는 응답 검사 구성을 참고하십시오. 헤더, 본문 및 본문 JSON 일치를 기반으로 성공 및 응답 설정을 구성할 수도 있습니다. 이 JSON에는 레이블 네임스페이스 및 웹 ACL의 애플리케이션 통합 URL과 같은 웹 ACL의 자동 생성 설정이 포함됩니다.

> **Note**
>
> ATP 응답 검사는 배포를 보호하는 웹 ACL에서만 사용할 수 있습니다. CloudFront

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
```

```
                    "VendorName": "AWS",
                    "Name": "AWSManagedRulesATPRuleSet",
                    "ManagedRuleGroupConfigs": [
                      {
                        "AWSManagedRulesATPRuleSet": {
                          "LoginPath": "/web/login",
                          "RequestInspection": {
                            "PayloadType": "JSON",
                            "UsernameField": {
                              "Identifier": "/form/username"
                            },
                            "PasswordField": {
                              "Identifier": "/form/password"
                            }
                          },
                          "ResponseInspection": {
                            "StatusCode": {
                              "SuccessCodes": [
                                200
                              ],
                              "FailureCodes": [
                                401
                              ]
                            }
                          },
                          "EnableRegexInPath": false
                        }
                      }
                    ]
                }
            }
        }
    ],
    "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "ATPValidationAcl"
    },
    "DefaultAction": {
        "Allow": {}
    },
    "ManagedByFirewallManager": false,
    "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
```

```
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

AWS WAF 봇 컨트롤

Bot Control을 사용하면 스크레이퍼, 스캐너, 크롤러, 상태 모니터, 검색 엔진 등 봇을 쉽게 모니터링 및 차단할 수 있고 속도를 제한할 수 있습니다. 규칙 그룹의 대상 검사 수준을 사용하는 경우 자체 식별이 불가능한 봇도 차단할 수 있으므로 악성 봇이 웹 사이트를 공격하기가 더 어려워지고 비용이 더 많이 듭니다. Bot Control 관리 규칙 그룹을 단독으로 사용하거나 다른 AWS 관리형 규칙 그룹 및 자체 사용자 지정 규칙과 함께 사용하여 애플리케이션을 보호할 수 있습니다. AWS WAF

Bot Control에는 요청 샘플링을 기반으로 봇에서 발생하는 현재 트래픽의 양을 보여주는 콘솔 대시보드가 포함되어 있습니다. 웹 ACL에 Bot Control 관리형 규칙 그룹을 추가하면 봇 트래픽에 대응하여 작업을 수행하고 애플리케이션으로 들어오는 일반적인 봇 트래픽에 대한 자세한 실시간 정보를 받을 수 있습니다.

> **Note**
>
> 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

Bot Control 관리형 규칙 그룹은 자체 식별 봇에 레이블을 추가하고, 일반적으로 선호되는 봇을 확인하며, 신뢰도가 높은 봇 서명을 탐지하는 기본적이고 일반적인 보호 수준을 제공합니다. 이를 통해 봇 트래픽의 일반적인 범주를 모니터링하고 제어할 수 있습니다.

또한 Bot Control 규칙 그룹은 자체 식별이 불가능한 정교한 봇에 대한 탐지를 추가하는 표적 보호 수준을 제공합니다. 모든 대상 보호는 브라우저 질의, 핑거프린팅 및 행동 휴리스틱과 같은 감지 기술을 사용하여 잘못된 봇 트래픽을 식별합니다. 또한 대상 보호 기능은 봇 관련 활동을 탐지하기 위해 웹 사이트 트래픽 통계에 대한 자동화된 기계 학습 분석을 선택적으로 제공합니다. 기계 학습을 활성화하면 AWS WAF 는 타임스탬프, 브라우저 특성, 이전 방문 URL 등 웹사이트 트래픽에 대한 통계를 사용하여 Bot Control 기계 학습 모델을 개선합니다.

Bot Control 관리형 규칙 그룹에 대한 자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.

Bot Control 관리 규칙 그룹과 비교하여 웹 요청을 AWS WAF 평가할 때, 규칙 그룹은 봇과 관련된 것으로 탐지된 요청에 레이블을 추가합니다 (예: 봇 범주 및 봇 이름). 자체 AWS WAF 규칙에서 이러한 레이블을 대조하여 처리를 사용자 지정할 수 있습니다. Bot Control 관리 규칙 그룹에서 생성된 레이블은 Amazon CloudWatch 지표와 웹 ACL 로그에 포함됩니다.

또한 AWS Firewall Manager AWS WAF 정책을 사용하여 조직에 속한 여러 계정의 애플리케이션 전체에 Bot Control 관리 규칙 그룹을 배포할 수 있습니다. AWS Organizations

AWS WAF 봇 컨트롤 컴포넌트

Bot Control 구현의 주요 구성 요소는 다음과 같습니다.

- **`AWSManagedRulesBotControlRuleSet`**— 다양한 범주의 봇을 탐지하고 처리하는 규칙을 포함하는 Bot Control 관리형 규칙 그룹입니다. 이 규칙 그룹은 봇 트래픽으로 탐지한 웹 요청에 레이블을 추가합니다.

  > **Note**
  >
  > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

  Bot Control 관리형 규칙 그룹은 선택할 수 있는 두 가지 보호 수준을 제공합니다.

  - 일반 - 웹 스크레이핑 프레임워크, 검색 엔진 및 자동 브라우저 등 다양한 자체 식별 봇을 탐지합니다. 이 수준의 Bot Control 보호는 정적 요청 데이터 분석과 같은 기존 봇 탐지 기술을 사용하여 일반적인 봇을 식별합니다. 이 규칙은 이러한 봇의 트래픽에 레이블을 지정하고 확인할 수 없는 트래픽은 차단합니다.
  - 대상 - 공통 수준의 보호 기능을 포함하고 자체 식별이 불가능한 정교한 봇에 대한 대상 탐지 기능을 추가합니다. 대상 보호는 속도 제한과 CAPTCHA 및 백그라운드 브라우저 챌린지를 함께 사용하여 봇 활동을 완화합니다.
    - **`TGT_`** - 대상 보호를 제공하는 규칙의 이름은 `TGT_`로 시작합니다. 모든 대상 보호는 브라우저 질의, 지문 및 행동 휴리스틱과 같은 탐지 기술을 사용하여 잘못된 봇 트래픽을 식별합니다.
    - **`TGT_ML_`**— 기계 학습을 사용하는 대상 보호 규칙의 이름은 `TGT_ML_`로 시작합니다. 이 규칙은 웹사이트 트래픽 통계에 대한 자동화된 기계 학습 분석을 사용하여 분산되고 조정된 봇 활동을 나타내는 비정상적인 행동을 탐지합니다. AWS WAF 타임스탬프, 브라우저 특성, 이전 방문

URL 등 웹사이트 트래픽에 대한 통계를 분석하여 Bot Control 머신 러닝 모델을 개선합니다. 기계 학습 기능은 기본적으로 활성화되지만 규칙 그룹 구성에서 비활성화할 수 있습니다. 기계 학습이 비활성화된 경우 이러한 규칙을 평가하지 AWS WAF 않습니다.

규칙 그룹의 규칙에 대한 정보를 포함한 자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.

관리형 규칙 그룹 참조 문을 사용하고 사용하려는 검사 수준을 나타내어 웹 ACL에 이 규칙 그룹을 포함합니다. 대상 수준에 대해 기계 학습을 활성화할지 여부도 지정할 수 있습니다. 웹 ACL에 이 관리형 규칙 그룹을 추가하는 방법에 대한 자세한 내용은 웹 ACL에 AWS WAF 봇 제어 관리 규칙 그룹 추가 섹션을 참조하세요.

- Bot Control 대시보드 - 웹 ACL용 봇 모니터링 대시보드로, 웹 ACL Bot Control 탭을 통해 사용할 수 있습니다. 이 대시보드를 사용하여 트래픽을 모니터링하고 다양한 유형의 봇에서 발생하는 트래픽의 양을 파악할 수 있습니다. 이는 이 항목에 설명된 대로 봇 관리를 사용자 지정하는 출발점이 될 수 있습니다. 또한 이를 사용하여 변경 사항을 확인하고 다양한 봇 및 봇 범주의 활동을 모니터링할 수 있습니다.
- JavaScript 및 모바일 애플리케이션 통합 SDK — Bot Control 규칙 그룹의 대상 보호 수준을 사용하는 경우 AWS WAF JavaScript 및 모바일 SDK를 구현해야 합니다. 대상 규칙은 악의적인 봇에 대한 탐지 성능을 개선하기 위해 SDK에서 제공하는 정보를 클라이언트 토큰에서 사용합니다. SDK에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합을 참조하세요.
- 로깅 및 지표 — 웹 ACL을 위해 AWS WAF 로그, Amazon Security Lake 및 Amazon별로 수집된 데이터를 연구하여 봇 트래픽을 모니터링하고 Bot Control 관리 규칙 그룹이 트래픽을 평가하고 처리하는 방식을 이해할 수 있습니다. CloudWatch Bot Control이 웹 요청에 추가하는 레이블은 데이터에 포함됩니다. 이러한 옵션에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅아마존을 통한 모니터링 CloudWatch, 및 Amazon Security Lake란 무엇입니까? 를 참조하십시오. .

  요구 사항과 표시되는 트래픽에 따라 Bot Control 구현을 사용자 지정해야 할 수도 있습니다. 다음은 가장 일반적으로 사용되는 몇 가지 옵션입니다.

- 범위 축소 문 — Bot Control 관리형 규칙 그룹 참조 문 내에 범위 축소 문을 추가하여 Bot Control 관리형 규칙 그룹이 평가하는 웹 요청에서 일부 트래픽을 제외할 수 있습니다. 모든 중첩 가능한 규칙 문은 범위 축소 문이 될 수 있습니다. 요청이 범위 축소 명령문과 일치하지 않는 경우, 규칙 그룹과 비교하여 AWS WAF 평가하지 않고 규칙 그룹 참조 명령문과 일치하지 않는 것으로 평가합니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요.

Bot Control 관리형 규칙 그룹의 요금은 AWS WAF 에서 해당 그룹을 사용하여 평가하는 웹 요청의 수에 따라 증가합니다. 범위 축소 문을 사용하여 규칙 그룹이 평가하는 요청을 제한함으로써 이러한 비용을 줄일 수 있습니다. 예를 들어 봇을 포함한 모든 사용자가 홈페이지가 로드되도록 허용한 다음

애플리케이션 API로 전송되거나 특정 유형의 콘텐츠가 포함된 요청에 규칙 그룹 규칙을 적용할 수 있습니다.

- 레이블 및 레이블 매칭 규칙 — Bot Control 규칙 그룹이 레이블 일치 규칙 문을 사용하여 식별하는 일부 봇 트래픽을 처리하는 방식을 사용자 지정할 수 있습니다. AWS WAF Bot Control 규칙 그룹은 웹 요청에 레이블을 추가합니다. Bot Control 레이블과 일치하는 Bot Control 규칙 그룹 뒤에 레이블 일치 규칙을 추가하고 필요한 처리를 적용할 수 있습니다. 레이블 일치 문의 레이블 지정 및 사용에 대한 자세한 내용은 레이블 일치 규칙 문 및 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.
- 사용자 지정 요청 및 응답 — 레이블 매칭을 사용자 지정 요청 및 응답 기능과 페어링하여 허용하는 요청에 사용자 지정 헤더를 추가하고 차단한 요청에 대해 AWS WAF 사용자 지정 응답을 보낼 수 있습니다. 요청 및 응답을 사용자 지정하는 방법에 대한 자세한 내용은 AWS WAF의 사용자 지정된 웹 요청 및 응답 섹션을 참조하세요.

애플리케이션 통합 SDK를 Bot Control과 함께 사용해야 하는 이유

Bot Control 관리형 규칙 그룹에는 애플리케이션 통합 SDK가 생성하는 챌린지 토큰이 필요합니다. 요청 시 챌린지 토큰이 필요하지 않은 규칙은 Bot Control 공통 수준 보호 및 대상 수준의 기계 학습 규칙입니다. 규칙 그룹의 보호 수준 및 규칙에 대한 설명은 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.

Bot Control 규칙 그룹을 가장 효율적으로 사용하려면 애플리케이션 통합 SDK를 구현하는 것이 좋습니다. 규칙 그룹이 스크립트에서 획득한 토큰을 활용하도록 하려면 Bot Control 규칙 그룹보다 먼저 챌린지 스크립트를 실행해야 합니다.

- 애플리케이션 통합 SDK를 사용하면 스크립트가 자동으로 실행됩니다.
- 또는 SDK를 사용할 수 없는 경우 Bot Control 규칙 그룹에서 검사할 모든 요청에 대해 Challenge 또는 CAPTCHA 규칙 작업을 실행하도록 웹 ACL을 구성할 수도 있습니다. Challenge 또는 CAPTCHA 규칙 작업을 사용하는 경우 추가 비용이 발생할 수 있습니다. 요금에 대한 자세한 내용은 AWS WAF Pricing을 참조하세요.

클라이언트에서 애플리케이션 통합 SDK를 구현하거나 챌린지 스크립트를 실행하는 규칙 작업 중 하나를 사용하면 규칙 그룹과 전체 클라이언트 애플리케이션 보안의 기능이 확장됩니다.

토큰은 각 웹 요청과 함께 클라이언트 정보를 제공합니다. 이 추가 정보는 Bot Control 규칙 그룹이 정상적인 클라이언트 세션을 잘못된 클라이언트 세션과 분리할 수 있도록 합니다. 둘 다 단일 IP 주소에서 시작된 경우에도 마찬가지입니다. 규칙 그룹은 대상 보호 수준에서 제공하는 탐지 및 완화를 세부적으로 조정하기 위해 토큰 정보를 사용하여 클라이언트 세션 요청 동작을 집계합니다.

SDK에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. AWS WAF 토큰에 대한 자세한 내용은 을 참조하십시오AWS WAF 웹 요청 토큰. 규칙 작업에 대한 자세한 내용은 CAPTCHA그리고 Challenge 안에 AWS WAF 섹션을 참조하세요.

웹 ACL에 AWS WAF 봇 제어 관리 규칙 그룹 추가

Bot Control 관리형 규칙 그룹 `AWSManagedRulesBotControlRuleSet`에는 구현하려는 보호 수준을 식별하기 위한 추가 구성이 필요합니다.

규칙 그룹 설명 및 규칙 목록은 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.

이 지침은 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 만들고 관리하는 방법을 일반적으로 알고 있는 사용자를 대상으로 합니다. 이러한 주제는 이 안내서의 이전 섹션에 설명되어 있습니다. 웹 ACL에 관리형 규칙 그룹을 추가하는 방법에 대한 기본 정보는 콘솔을 통해 웹 ACL에 관리형 규칙 그룹 추가 섹션을 참조하세요.

모범 사례 따르기

지능형 위협 완화 모범 사례의 모범 사례에 따라 Bot Control 규칙 그룹을 사용하십시오.

웹 ACL에서 **`AWSManagedRulesBotControlRuleSet`** 규칙 그룹을 사용하려면

1. 웹 ACL에 AWS 관리형 규칙 그룹을 추가합니다. `AWSManagedRulesBotControlRuleSet` 전체 규칙 그룹 설명은 the section called “Bot Control 규칙 그룹” 섹션을 참조하세요.

   > **Note**
   >
   > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

   규칙 그룹을 추가할 때는 규칙 그룹을 편집하여 규칙 그룹의 구성 페이지를 엽니다.
2. 규칙 그룹 구성 페이지의 검사 수준 창에서 사용하려는 검사 수준을 선택합니다.

   - 일반 - 웹 스크레이핑 프레임워크, 검색 엔진 및 자동 브라우저 등 다양한 자체 식별 봇을 탐지합니다. 이 수준의 Bot Control 보호는 정적 요청 데이터 분석과 같은 기존 봇 탐지 기술을 사용하여 일반적인 봇을 식별합니다. 이 규칙은 이러한 봇의 트래픽에 레이블을 지정하고 확인할 수 없는 트래픽은 차단합니다.

- 대상 - 공통 수준의 보호 기능을 포함하고 자체 식별이 불가능한 정교한 봇에 대한 대상 탐지 기능을 추가합니다. 대상 보호는 속도 제한과 CAPTCHA 및 백그라운드 브라우저 챌린지를 함께 사용하여 봇 활동을 완화합니다.
  - **TGT_** - 대상 보호를 제공하는 규칙의 이름은 TGT_로 시작합니다. 모든 대상 보호는 브라우저 질의, 지문 및 행동 휴리스틱과 같은 탐지 기술을 사용하여 잘못된 봇 트래픽을 식별합니다.
  - **TGT_ML_**— 기계 학습을 사용하는 대상 보호 규칙의 이름은 TGT_ML_로 시작합니다. 이 규칙은 웹사이트 트래픽 통계에 대한 자동화된 기계 학습 분석을 사용하여 분산되고 조정된 봇 활동을 나타내는 비정상적인 행동을 탐지합니다. AWS WAF 타임스탬프, 브라우저 특성, 이전 방문 URL 등 웹사이트 트래픽에 대한 통계를 분석하여 Bot Control 머신 러닝 모델을 개선합니다. 기계 학습 기능은 기본적으로 활성화되지만 규칙 그룹 구성에서 비활성화할 수 있습니다. 기계 학습이 비활성화된 경우 이러한 규칙을 평가하지 AWS WAF 않습니다.

3. 대상 보호 수준을 사용 중이고 기계 학습 (ML) AWS WAF 을 사용하여 조정된 분산된 봇 활동에 대한 웹 트래픽을 분석하지 않으려면 기계 학습 옵션을 비활성화하십시오. 이름이 TGT_ML_로 시작하는 Bot Control 규칙에는 기계 학습이 필요합니다. 이러한 규칙에 대한 자세한 내용은 Bot Control 규칙 목록 섹션을 참조하세요.
4. 사용 비용을 포함하도록 규칙 그룹에 대해 범위 축소 문을 추가합니다. 범위 축소 문은 규칙 그룹이 검사하는 요청 집합의 범위를 좁힙니다. 예를 들면 사용 사례는 봇 컨트롤 예제: 로그인 페이지에만 봇 컨트롤 사용 및 봇 컨트롤 예제: 동적 콘텐츠에만 봇 컨트롤 사용로 시작합니다.
5. 규칙 그룹에 필요한 추가 구성을 모두 제공합니다.
6. 웹 ACL에 대한 변경 사항을 저장합니다.

프로덕션 트래픽용 Bot Control 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 이를 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 개수 모드에서 테스트하고 조정한 다음 활성화합니다. 지침은 다음 섹션을 참조하세요.

AWS WAF 봇 컨트롤을 통한 오탐

우리는 오탐을 최소화하기 위해 AWS WAF Bot Control 관리 규칙 그룹에서 규칙을 신중하게 선택했습니다. 전 세계 트래픽을 대상으로 규칙을 테스트하고 테스트 웹 ACL에 미치는 영향을 모니터링합니다. 하지만 트래픽 패턴의 변화로 인해 여전히 거짓 긍정이 발생할 수 있습니다. 또한 일부 사용 사례는 거짓 긍정을 유발하는 것으로 알려져 있으며 웹 트래픽에 맞게 사용자 지정해야 합니다.

거짓 긍정이 발생할 수 있는 상황은 다음과 같습니다.

- 모바일 앱에는 일반적으로 `SignalNonBrowserUserAgent` 규칙에서 기본적으로 차단되는 비 브라우저 사용자 에이전트가 있습니다. 모바일 앱에서 발생하는 트래픽이나 비 브라우저 사용자 에이전트를 통한 기타 합법적인 트래픽이 예상되면 예외를 추가하여 허용해야 합니다.
- 가동 시간 모니터링, 통합 테스트 또는 마케팅 도구 등의 경우 특정 봇 트래픽에 의존해야 합니다. Bot Control이 사용자가 허용하고자 하는 봇 트래픽을 식별하여 차단하는 경우 자체 규칙을 추가하여 처리 방식을 변경해야 합니다. 이것이 모든 고객을 대상으로 하는 거짓 긍정 시나리오는 아니지만, 본인에게 해당하는 시나리오라면 거짓 긍정과 동일하게 처리해야 합니다.
- Bot Control 관리 규칙 그룹은 의 IP 주소를 사용하여 봇을 확인합니다. AWS WAF Bot Control을 사용하고 프록시나 로드 밸런서를 통해 라우팅되는 봇을 확인한 경우 사용자 지정 규칙을 사용하여 봇을 명시적으로 허용해야 할 수 있습니다. 이 유형의 사용자 지정 규칙을 생성하는 방법에 대한 자세한 내용은 전달된 IP 주소 섹션을 참조하세요.
- 글로벌 거짓 긍정률이 낮은 Bot Control 규칙은 특정 디바이스나 애플리케이션에 심각한 영향을 미칠 수 있습니다. 예를 들어, 테스트 및 검증 과정에서 트래픽이 적은 애플리케이션이나 자주 사용되지 않는 브라우저 또는 디바이스에서 들어 오는 요청을 관찰하지 못했을 수 있습니다.
- 과거에 거짓 긍정률이 낮았던 Bot Control 규칙의 경우 유효한 트래픽에 대한 거짓 긍정이 증가했을 수 있습니다. 이는 유효한 트래픽과 함께 등장한 새로운 트래픽 패턴 또는 요청 특성으로 인한 것일 수 있으며, 이로 인해 이전에는 일치하지 않았던 규칙과의 일치가 발생할 수 있습니다. 이러한 변화는 다음과 같은 상황으로 인해 발생할 수 있습니다.
  - 로드 밸런서 또는 콘텐츠 배포 네트워크(CDN)와 같은 네트워크 어플라이언스를 통해 트래픽이 전송될 때 변경되는 트래픽 세부 정보입니다.
  - 트래픽 데이터의 새로운 변경 사항(예: 새 브라우저 또는 기존 브라우저의 새 버전)

AWS WAF Bot Control 관리형 규칙 그룹에서 발생할 수 있는 거짓 긍정을 처리하는 방법에 대한 자세한 내용은 다음에 이어지는 AWS WAF 봇 컨트롤 테스트 및 배포 섹션의 지침을 참조하세요.

AWS WAF 봇 컨트롤 테스트 및 배포

이 섹션에서는 사이트의 AWS WAF Bot Control 구현을 구성하고 테스트하기 위한 일반적인 지침을 제공합니다. 따르기로 선택한 구체적인 단계는 요구 사항, 리소스 및 수신하는 웹 요청에 따라 달라집니다.

이 정보는 AWS WAF 보호 기능 테스트 및 조정에 제공된 테스트 및 조정에 대한 일반 정보 외의 정보입니다.

> **Note**
>
> AWS 관리형 규칙은 일반적인 웹 위협으로부터 사용자를 보호하도록 설계되었습니다. 설명서에 따라 AWS 관리형 규칙 그룹을 사용하면 애플리케이션에 또 다른 보안 계층이 추가됩니다. 하지만 AWS 관리형 규칙 규칙 그룹은 선택한 AWS 리소스에 따라 결정되는 보안 책임을 대체하기 위한 것이 아닙니다. 공동 책임 모델을 참조하여 AWS 리소스가 적절하게 보호되도록 하세요.

> **⚠ 프로덕션 트래픽 위험**
>
> 프로덕션 트래픽용 Bot Control 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 이를 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 개수 모드에서 테스트하고 조정한 다음 활성화합니다.

이 지침은 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 만들고 관리하는 방법을 일반적으로 알고 있는 사용자를 대상으로 합니다. 이러한 주제는 이 안내서의 이전 섹션에 설명되어 있습니다.

Bot Control 구현을 구성하고 테스트하려면

이러한 단계를 먼저 테스트 환경에서 수행한 다음, 프로덕션 환경에서 수행합니다.

1. Bot Control 관리형 규칙 그룹 추가

   > **Note**
   >
   > 이 관리형 규칙 그룹은 사용 시 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

   새 웹 ACL 또는 기존 웹 `AWSManagedRulesBotControlRuleSet` ACL에 관리형 AWS 규칙 그룹을 추가하고 현재 웹 ACL 동작이 변경되지 않도록 구성하십시오.

   - 관리형 규칙 그룹을 추가할 때는 해당 규칙 그룹을 편집하고 다음을 수행합니다.
     - 검사 수준 창에서 사용하려는 검사 수준을 선택합니다.
       - 일반 - 웹 스크레이핑 프레임워크, 검색 엔진 및 자동 브라우저 등 다양한 자체 식별 봇을 탐지합니다. 이 수준의 Bot Control 보호는 정적 요청 데이터 분석과 같은 기존 봇 탐지 기술을

사용하여 일반적인 봇을 식별합니다. 이 규칙은 이러한 봇의 트래픽에 레이블을 지정하고 확인할 수 없는 트래픽은 차단합니다.

- 대상 - 공통 수준의 보호 기능을 포함하고 자체 식별이 불가능한 정교한 봇에 대한 대상 탐지 기능을 추가합니다. 대상 보호는 속도 제한과 CAPTCHA 및 백그라운드 브라우저 챌린지를 함께 사용하여 봇 활동을 완화합니다.
  - **TGT_** - 대상 보호를 제공하는 규칙의 이름은 TGT_로 시작합니다. 모든 대상 보호는 브라우저 질의, 지문 및 행동 휴리스틱과 같은 탐지 기술을 사용하여 잘못된 봇 트래픽을 식별합니다.
  - **TGT_ML_**— 기계 학습을 사용하는 대상 보호 규칙의 이름은 TGT_ML_로 시작합니다. 이 규칙은 웹사이트 트래픽 통계에 대한 자동화된 기계 학습 분석을 사용하여 분산되고 조정된 봇 활동을 나타내는 비정상적인 동작을 탐지합니다. AWS WAF 타임스탬프, 브라우저 특성, 이전 방문 URL 등 웹사이트 트래픽에 대한 통계를 분석하여 Bot Control 머신 러닝 모델을 개선합니다. 기계 학습 기능은 기본적으로 활성화되지만 규칙 그룹 구성에서 비활성화할 수 있습니다. 기계 학습이 비활성화된 경우 이러한 규칙을 평가하지 AWS WAF 않습니다.

  이 옵션에 대한 자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.
- 규칙 창에서 모든 규칙 모든 규칙 작업 재정의 드롭다운을 열고 Count를 선택합니다. 이 구성을 사용하면 요청에는 AWS WAF 레이블을 추가하면서 규칙 그룹의 모든 규칙에 대해 요청을 평가한 다음 일치하는 항목만 계산합니다. 자세한 정보는 규칙 그룹에 대한 규칙 작업 재정의을 참조하세요.

  이 재정의를 통해 Bot Control 규칙이 트래픽에 미치는 잠재적 영향을 모니터링하여 내부 사용 사례 또는 원하는 봇과 같은 항목에 예외를 추가할지 여부를 결정할 수 있습니다.

- 이미 사용 중인 규칙 또는 규칙 그룹보다 높은 우선 순위를 지정하여 웹 ACL에서 마지막으로 평가되도록 규칙 그룹을 배치합니다. 자세한 정보는 웹 ACL의 규칙 및 규칙 그룹 처리 순서을 참조하세요.

  이렇게 하면 현재의 트래픽 처리가 중단되지 않습니다. 예를 들어 SQL 명령어 삽입이나 교차 사이트 스크립팅과 같은 악성 트래픽을 탐지하는 규칙이 있는 경우 이들 규칙이 이러한 요청을 계속 탐지하고 기록합니다. 또는 악의적이지 않은 알려진 트래픽을 허용하는 규칙이 있는 경우 해당 트래픽을 Bot Control 관리형 규칙 그룹을 통해 차단하지 않고 계속 허용할 수 있습니다. 테스트 및 조정 활동 중에 처리 순서를 조정하기로 결정할 수 있지만 좋은 시작 방법은 아닙니다.

2. 웹 ACL에 대한 로깅 및 메트릭을 활성화합니다.

   필요에 따라 로깅, Amazon Security Lake 데이터 수집, 요청 샘플링 및 웹 ACL에 대한 Amazon CloudWatch 지표를 구성합니다. 이러한 가시성 도구를 사용하여 Bot Control 관리 규칙 그룹과 트래픽의 상호 작용을 모니터링할 수 있습니다.

   - 로깅에 대한 추가 정보는 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.
   - 아마존 시큐리티 레이크에 대한 자세한 내용은 아마존 시큐리티 레이크란 무엇입니까? 를 참조하십시오. 및 Amazon Security Lake 사용 설명서의 AWS 서비스에서 데이터 수집
   - Amazon CloudWatch 지표에 대한 자세한 내용은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.
   - 웹 요청 샘플링에 대한 자세한 내용은 웹 요청 샘플 보기 섹션을 참조하세요.

3. 웹 ACL을 리소스와 연결

   웹 ACL이 아직 리소스와 연결되지 않은 경우 해당 리소스를 연결합니다. 자세한 내용은 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.

4. 트래픽과 Bot Control 규칙 일치 모니터링

   트래픽이 흐르고 있고 Bot Control 관리형 규칙의 그룹 규칙이 일치하는 웹 요청에 레이블을 추가하고 있는지 확인하십시오. 로그에서 라벨을 볼 수 있고 Amazon CloudWatch 메트릭에서 봇 및 라벨 메트릭을 볼 수 있습니다. 로그에서 규칙 그룹에서 개수하도록 재정의한 규칙은 계수로 설정된 `action`과 재정의한 구성된 규칙 작업을 나타내는 `overriddenAction`을 포함하는 `ruleGroupList`로 표시됩니다.

   > **Note**
   >
   > Bot Control 관리형 규칙 그룹은 AWS WAF의 IP 주소를 사용하여 봇을 확인합니다. Bot Control을 사용하고 프록시나 로드 밸런서를 통해 라우팅되는 봇을 확인한 경우 사용자 지정 규칙을 사용하여 봇을 명시적으로 허용해야 할 수 있습니다. 사용자 지정 규칙을 생성하는 방법에 대한 자세한 내용은 전달된 IP 주소 섹션을 참조하세요. 규칙을 사용하여 Bot Control 웹 요청 처리를 사용자 지정하는 방법에 대한 자세한 내용은 다음 단계를 참조하세요.

   웹 요청 처리를 주의 깊게 검토하여 사용자 지정 처리로 완화해야 하는 거짓 긍정이 있는지 확인하십시오. 거징 긍정의 예는 AWS WAF 봇 컨트롤을 통한 오탐 섹션을 참조하세요.

5. Bot Control 웹 요청 처리 사용자 지정

   필요에 따라 요청을 명시적으로 허용하거나 차단하는 자체 규칙을 추가하여 Bot Control 규칙이 요청을 처리하는 방식을 변경합니다.

   이를 수행하는 방법은 사용 사례에 따라 다르지만 일반적인 해결 방법은 다음과 같습니다.

   - Bot Control 관리형 규칙 그룹 앞에 추가하는 규칙으로 요청을 명시적으로 허용합니다. 이렇게 하면 허용된 요청이 평가 대상 규칙 그룹에 도달하지 않습니다. 이를 통해 Bot Control 관리형 규칙 그룹 사용 비용을 억제할 수 있습니다.
   - Bot Control 관리형 규칙 그룹 문 안에 범위 축소 문을 추가하여 Bot Control 평가에서 요청을 제외시킵니다. 이 기능은 이전 옵션과 동일합니다. 범위 축소 문과 일치하지 않는 요청은 규칙 그룹 평가에 도달하지 않으므로 Bot Control 관리형 규칙 그룹의 사용 비용을 줄이는 데 도움이 됩니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요.

     예를 들어, 다음을 참조하세요.

     - 봇 관리에서 IP 범위 제외
     - 제어하는 봇에서 들어오는 트래픽 허용
   - 요청 처리 시 Bot Control 레이블을 사용하여 요청을 허용하거나 차단할 수 있습니다. Bot Control 관리형 규칙 그룹 뒤에 레이블 일치 규칙을 추가하여 허용하려는 레이블이 지정된 요청과 차단하려는 요청을 필터링합니다.

     테스트 후에는 관련 Bot Control 규칙을 계수 모드로 유지하고 요청 처리 결정을 사용자 지정 규칙에서 유지하십시오. 레이블 일치 문에 대한 자세한 내용은 레이블 일치 규칙 문 섹션을 참조하세요.

     이러한 유형의 사용자 지정에 대한 예는 다음을 참조하세요.

     - 차단된 사용자 에이전트에 대한 예외 생성
     - 차단된 특정 봇 허용
     - 확인된 봇 차단

   추가 예제는 다음(AWS WAF 봇 컨트롤 예제)을 참조하십시오.

6. 필요에 따라 Bot Control 관리형 규칙 그룹 설정을 활성화

   상황에 따라 일부 Bot Control 규칙을 계수 모드로 유지하기로 결정하거나 다른 작업 재정의를 결정할 수도 있습니다. 규칙 그룹 내부에 구성된 대로 실행하려는 규칙의 경우 일반 규칙 구성을 활성화합니다. 이렇게 하려면 웹 ACL에서 규칙 그룹 문을 편집하고 규칙 창에서 변경합니다.

AWS WAF 봇 컨트롤 예제

이 섹션에서는 AWS WAF Bot Control 구현의 다양한 일반 사용 사례를 충족하는 예제 구성을 보여줍니다.

각 예제는 사용 사례에 대한 설명을 제공하고 나서 사용자 지정 구성 규칙의 JSON 목록에 나와 있는 솔루션을 표시합니다.

> **Note**
>
> 이 예제에 표시된 JSON 목록은 콘솔에서 규칙을 구성하고 나서 규칙 JSON 편집기로 편집하여 생성한 것입니다.

주제

봇 컨트롤 예제: 간단한 구성

다음 JSON 목록은 AWS WAF 봇 제어 관리 규칙 그룹이 있는 예제 웹 ACL을 보여줍니다. 모니터링 목적으로 요청 샘플과 AWS WAF 메트릭을 저장해야 하는 가시성 구성을 참고하세요.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
```

```
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
         "Name": "AWS-AWSBotControl-Example",
         "Priority": 5,
         "Statement": {
            "ManagedRuleGroupStatement": {
               "VendorName": "AWS",
               "Name": "AWSManagedRulesBotControlRuleSet",
               "ManagedRuleGroupConfigs": [
                 {
                   "AWSManagedRulesBotControlRuleSet": {
                     "InspectionLevel": "COMMON"
                   }
                 }
               ],
               "RuleActionOverrides": [],
               "ExcludedRules": []
            },
            "VisibilityConfig": {
               "SampledRequestsEnabled": true,
               "CloudWatchMetricsEnabled": true,
               "MetricName": "AWS-AWSBotControl-Example"
             }
          }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

봇 컨트롤 예제: 검증된 봇을 명시적으로 허용

AWS WAF Bot Control은 일반적이고 검증 가능한 봇으로 알려진 AWS 봇을 차단하지 않습니다. Bot Control은 웹 요청이 확인된 봇으로부터 온 것으로 식별되면 봇의 이름을 지정하는 레이블과 해당 봇이

확인된 봇임을 나타내는 레이블을 추가합니다. Bot Control은 정상 작동이 확인된 봇이 차단되는 것을 방지하기 위해 신호 레이블과 같은 다른 레이블을 추가하지 않습니다.

검증된 봇을 차단하는 다른 AWS WAF 규칙이 있을 수 있습니다. 확인된 봇이 허용되도록 하려면 Bot Control 레이블에 따라 허용할 사용자 지정 규칙을 추가합니다. 새 규칙은 Bot Control 관리형 규칙 그룹 다음에 실행해야만 레이블과 일치할 수 있습니다.

다음 규칙은 확인된 봇을 명시적으로 허용합니다.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

봇 컨트롤 예제: 검증된 봇 차단

확인된 봇을 차단하려면 AWS WAF Bot Control 관리형 규칙 그룹 이후에 실행되는 차단 규칙을 추가해야 합니다. 이렇게 하려면 차단할 봇 이름을 식별하고 레이블 일치 문을 사용하여 해당 봇을 식별하고 차단합니다. 확인된 봇을 모두 차단하려는 경우 `bot:name:` 레이블과 일치하는 항목을 생략할 수 있습니다.

다음 규칙은 `bingbot` 확인된 봇만 차단합니다. 이 규칙은 Bot Control 관리형 규칙 그룹 다음에 실행해야 합니다.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
```

```
            }
          },
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:verified"
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
  }
```

다음 규칙은 확인된 모든 봇을 차단합니다.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

봇 컨트롤 예제: 차단된 특정 봇 허용

봇이 둘 이상의 Bot Control 규칙에 의해 차단될 수 있습니다. 각 차단 규칙마다 다음 절차를 통해 실행합니다.

AWS WAF 봇 제어 규칙이 차단하고 싶지 않은 봇을 차단하는 경우 다음과 같이 하십시오.

1. 로그를 확인하여 봇을 차단하는 Bot Control 규칙을 식별합니다. 차단 규칙은 이름이 `terminatingRule`로 시작하는 필드의 로그에 지정됩니다. 웹 ACL 로그에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요. 참고로, 규칙이 요청에 추가하는 레이블입니다.

2. 웹 ACL에서 차단 규칙의 작업을 계산으로 재정의합니다. 콘솔에서 이 작업을 수행하려면 웹 ACL에서 규칙 그룹 규칙을 편집하고 규칙에 대해 Count의 규칙 작업 재정의를 선택합니다. 이렇게 하면 봇이 규칙에 의해 차단되지 않지만 규칙은 여전히 해당 레이블을 일치 요청에 적용합니다.
3. Bot Control 관리형 규칙 그룹 다음에 웹 ACL에 레이블 일치 규칙을 추가합니다. 재정의된 규칙의 레이블과 일치하도록 규칙을 구성하고, 차단하지 않을 봇을 제외한 모든 일치 요청을 차단하도록 구성합니다.

   이제 허용할 봇이 로그를 통해 식별된 차단 규칙에 의해 더 이상 차단되지 않도록 웹 ACL이 구성됩니다.

트래픽과 로그를 다시 확인하여 봇의 통과가 허용되는지 확인합니다. 그렇지 않은 경우 위 절차를 다시 실행합니다.

예를 들어, `pingdom`을 제외한 모든 모니터링 봇을 차단하고자 한다고 가정해 보겠습니다. 이 경우, 개수를 계산하도록 `CategoryMonitoring` 규칙을 재정의하고 나서 봇 이름 레이블이 `pingdom`인 것을 제외하고 모든 모니터링 봇을 차단하는 규칙을 작성합니다.

다음 규칙은 Bot Control 관리형 규칙 그룹을 사용하지만 개수를 계산하도록 `CategoryMonitoring`에 대한 규칙 작업을 재정의합니다. 범주 모니터링 규칙은 평소와 같이 일치 요청에 해당 레이블을 적용하지만 일반적인 차단 작업을 수행하는 대신 요청의 수만 계산합니다.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
```

```
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

다음 규칙은 이전 CategoryMonitoring 규칙이 일치하는 웹 요청에 추가하는 범주 모니터링 레이블과 일치합니다. 범주 모니터링 요청 중에서 이 규칙은 봇 이름 pingdom에 대한 레이블이 있는 요청을 제외한 모든 요청을 차단합니다.

다음 규칙은 웹 ACL 처리 순서에서 이전 Bot Control 관리형 규칙 그룹 다음에 실행해야 합니다.

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
```

```
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
      }
}
```

봇 컨트롤 예제: 차단된 사용자 에이전트에 대한 예외 생성

브라우저가 아닌 일부 사용자 에이전트의 트래픽이 잘못 차단되는 경우 문제가 되는 AWS WAF Bot Control 규칙을 카운트로 설정한 다음 `SignalNonBrowserUserAgent` 규칙의 레이블을 예외 기준과 결합하여 예외를 생성할 수 있습니다.

> **Note**
>
> 모바일 앱에는 일반적으로 `SignalNonBrowserUserAgent` 규칙에서 기본적으로 차단되는 비 브라우저 사용자 에이전트가 있습니다.

다음 규칙은 Bot Control 관리형 규칙 그룹을 사용하지만 개수를 계산하도록 `SignalNonBrowserUserAgent`에 대한 규칙 작업을 재정의합니다. 신호 규칙은 평소와 같이 일치 요청에 해당 레이블을 적용하지만 일반적인 차단 작업을 수행하는 대신 요청의 수만 계산합니다.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
```

```
          "ActionToUse": {
            "Count": {}
          },
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

다음 규칙은 Bot Control `SignalNonBrowserUserAgent` 규칙이 일치하는 웹 요청에 추가하는 신호 레이블과 일치합니다. 신호 요청 중에서 이 규칙은 허용하려는 사용자 에이전트가 있는 요청을 제외한 모든 요청을 차단합니다.

다음 규칙은 웹 ACL 처리 순서에서 이전 Bot Control 관리형 규칙 그룹 다음에 실행해야 합니다.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
```

```
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "match_rule"
    }
}
```

봇 컨트롤 예제: 로그인 페이지에만 봇 컨트롤 사용

다음 예시에서는 scope-down 문을 사용하여 URI 경로로 식별되는 웹 사이트의 로그인 페이지로 들어오는 트래픽에만 AWS WAF 봇 제어를 적용합니다. `login` 로그인 페이지의 URI 경로는 애플리케이션과 환경에 따라 예제와 다를 수 있습니다.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
```

```
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "ByteMatchStatement": {
        "SearchString": "login",
        "FieldToMatch": {
          "UriPath": {}
        },
        "TextTransformations": [
          {
            "Priority": 0,
            "Type": "NONE"
          }
        ],
        "PositionalConstraint": "CONTAINS"
      }
    }
  }
}
```

봇 컨트롤 예제: 동적 콘텐츠에만 봇 컨트롤 사용

이 예제에서는 scope-down 명령문을 사용하여 동적 콘텐츠에만 AWS WAF 봇 제어를 적용합니다.

scope-down 명령문은 정규식 패턴 집합에 대한 일치 결과를 무효화하여 정적 콘텐츠를 제외합니다.

- 정규식 패턴 집합은 정적 콘텐츠의 확장자와 일치하도록 구성됩니다. 예를 들어, 정규식 패턴 집합 사양은 `(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`일 수 있습니다. 정규식 패턴 집합 관리에 대한 자세한 내용은 정규식 패턴 집합 일치 규칙 문 섹션을 참조하세요.
- 범위 축소 문에서는 NOT 문 안에 정규식 패턴 설정 문을 중첩하여 일치하는 정적 콘텐츠를 제외합니다. NOT 문에 대한 자세한 내용은 NOT 규칙 문 섹션을 참조하세요.

```
{
  "Name": "AWS-AWSBotControl-Example",
```

```
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
   "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "RegexPatternSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/regexpatternset/
excludeset/00000000-0000-0000-0000-000000000000",
            "FieldToMatch": {
              "UriPath": {}
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
      }
    }
  }
}
```

봇 제어 예제: 봇 관리에서 IP 범위 제외

웹 트래픽의 일부를 AWS WAF 봇 제어 관리에서 제외하고 규칙 명령문을 사용하여 해당 하위 집합을 식별하려면 Bot Control 관리 규칙 그룹 문에 scope-down 문을 추가하여 제외하십시오.

다음 규칙은 특정 IP 주소 범위에서 들어오는 웹 요청을 제외한 모든 웹 트래픽에 대해 일반적인 Bot Control 봇 관리를 수행합니다.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "IPSetReferenceStatement": {
            "ARN": "arn:aws:wafv2:us-east-1:123456789:regional/ipset/
friendlyips/00000000-0000-0000-0000-000000000000"
          }
        }
      }
    }
  }
}
```

봇 제어 예제: 제어하는 봇의 트래픽 허용

일부 사이트 모니터링 봇과 사용자 지정 봇이 사용자 지정 헤더를 전송하도록 구성할 수 있습니다. 이러한 유형의 봇으로부터 들어오는 트래픽을 허용하려면 헤더에 공유 암호를 추가하도록 구성할 수 있습니다. 그런 다음 AWS WAF Bot Control 관리 규칙 그룹 문에 scope-down 명령문을 추가하여 헤더가 있는 메시지를 제외할 수 있습니다.

다음 예제 규칙은 비밀 헤더가 있는 트래픽을 Bot Control 검사에서 제외합니다.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
            },
            "TextTransformations": [
              {
```

```
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
    }
  }
}
```

봇 컨트롤 예제: 대상 검사 수준

보호 수준을 높이려면 AWS WAF Bot Control 관리 규칙 그룹에서 대상 검사 수준을 활성화할 수 있습니다.

다음 예시에서는 기계 학습 기능이 활성화되어 있습니다. 로 설정하여 이 동작을 `EnableMachineLearning` 거부할 수 `false` 있습니다.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    }
```

```
  }
}
```

Bot Control 예제: 두 개의 명령문을 사용하여 대상 검사 수준의 사용을 제한하십시오.

비용 최적화를 위해 웹 ACL에서 별도의 검사 수준과 범위를 지정하는 두 개의 AWS WAF Bot Control 관리 규칙 그룹 명령문을 사용할 수 있습니다. 예를 들어, 대상 검사 수준 설명의 범위를 더 민감한 애플리케이션 엔드포인트로만 지정할 수 있습니다.

다음 예제의 두 명령문에는 상호 배타적인 범위가 있습니다. 이 구성을 사용하지 않으면 요청 시 평가 요금이 두 번 청구될 수 있습니다.

> **Note**
>
> 콘솔의 시각적 편집기에서는 다중 명령문 참조가 `AWSManagedRulesBotControlRuleSet` 지원되지 않습니다. 대신 JSON 편집기를 사용하세요.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
       "Name": "AWS-AWSBotControl-Common",
       "Priority": 5,
       "Statement": {
          "ManagedRuleGroupStatement": {
             "VendorName": "AWS",
             "Name": "AWSManagedRulesBotControlRuleSet",
             "ManagedRuleGroupConfigs": [
               {
                 "AWSManagedRulesBotControlRuleSet": {
                   "InspectionLevel": "COMMON"
                 }
```

```
            }
          ],
          "RuleActionOverrides": [],
          "ExcludedRules": []
       },
       "VisibilityConfig": {
          "SampledRequestsEnabled": true,
          "CloudWatchMetricsEnabled": true,
          "MetricName": "AWS-AWSBotControl-Common"
        },
        "ScopeDownStatement": {
           "NotStatement": {
             "Statement": {
               "ByteMatchStatement": {
                 "FieldToMatch": {
                   "UriPath": {}
                 },
                 "PositionalConstraint": "STARTS_WITH",
                 "SearchString": "/sensitive-endpoint",
                 "TextTransformations": [
                   {
                     "Type": "NONE",
                     "Priority": 0
                   }
                 ]
               }
             }
           }
         }
     }
   },
   {
    "Name": "AWS-AWSBotControl-Targeted",
    "Priority": 6,
    "Statement": {
       "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "TARGETED",
                "EnableMachineLearning": true
              }
```

```
                }
             ],
             "RuleActionOverrides": [],
             "ExcludedRules": []
          },
          "VisibilityConfig": {
             "SampledRequestsEnabled": true,
             "CloudWatchMetricsEnabled": true,
             "MetricName": "AWS-AWSBotControl-Targeted"
           },
           "ScopeDownStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "UriPath": {}
                  },
                  "PositionalConstraint": "STARTS_WITH",
                  "SearchString": "/sensitive-endpoint",
                  "TextTransformations": [
                    {
                      "Type": "NONE",
                      "Priority": 0
                    }
                  ]
                }
              }
            }
        }
      }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

AWS WAF 클라이언트 애플리케이션 통합

AWS WAF 클라이언트 애플리케이션 통합 API를 사용하여 클라이언트 측 보호를 AWS 서버 측 웹 ACL 보호와 결합하여 보호된 리소스에 웹 요청을 보내는 클라이언트 애플리케이션이 대상 클라이언트인지, 최종 사용자가 사람인지 확인할 수 있습니다.

클라이언트 통합을 사용하여 자동 브라우저 챌린지와 CAPTCHA 퍼즐을 관리하고, 성공적인 브라우저 및 최종 사용자 응답에 대한 증거가 있는 토큰을 확보하고, 보호된 엔드포인트에 대한 요청에 이러한 토큰을 포함할 수 있습니다. 토큰에 대한 일반 정보는 을 참조하십시오. AWS WAF AWS WAF 웹 요청 토큰

리소스에 액세스하기 위해 유효한 토큰을 필요로 하는 웹 ACL 보호와 클라이언트 통합을 결합합니다. 다음 섹션인 지능형 위협 통합 및 AWS 관리형 규칙에 나열된 것과 같이 챌린지 토큰을 확인하고 모니터링하는 규칙 그룹을 사용할 수 있으며 CAPTCHA그리고 Challenge 안에 AWS WAF에 설명된 대로 CAPTCHA 및 Challenge 규칙 작업을 사용하여 검사할 수 있습니다.

AWS WAF JavaScript 애플리케이션에 대해 두 가지 수준의 통합을 제공하고, 다른 하나는 모바일 애플리케이션을 위한 통합을 제공합니다.

- 지능형 위협 통합 — 클라이언트 애플리케이션을 검증하고 AWS 토큰 획득 및 관리를 제공합니다. 이는 AWS WAF Challenge 규칙 조치에서 제공하는 기능과 유사합니다. 이 기능은 클라이언트 애플리케이션을 `AWSManagedRulesACFPRuleSet` 관리형 규칙 그룹, `AWSManagedRulesATPRuleSet` 관리형 규칙 그룹 및 `AWSManagedRulesBotControlRuleSet` 관리형 규칙 그룹의 대상 보호 수준과 완벽하게 통합합니다.

  지능형 위협 통합 API는 AWS WAF 사일런트 브라우저 챌린지를 사용하여 보호된 리소스에 대한 로그인 시도 및 기타 호출이 클라이언트가 유효한 토큰을 획득한 후에만 허용되도록 합니다. API는 클라이언트 애플리케이션 세션의 토큰 인증을 관리하고 클라이언트에 대한 정보를 수집하여 클라이언트가 봇에 의해 운영되는지 아니면 사람에 의해 운영되는지 여부를 결정합니다.

  > **Note**
  >
  > 이 기능은 Android JavaScript 및 iOS 모바일 애플리케이션에서 사용할 수 있습니다.

- CAPTCHA 통합 - 애플리케이션에서 관리하는 사용자 지정 CAPTCHA 퍼즐로 최종 사용자를 확인합니다. 이 기능은 AWS WAF CAPTCHA 규칙 액션에서 제공하는 기능과 비슷하지만 퍼즐 배치 및 동작에 대한 추가 제어 기능이 있습니다.

  이 통합은 JavaScript 지능형 위협 통합을 활용하여 사일런트 챌린지를 실행하고 고객 페이지에 AWS WAF 토큰을 제공합니다.

  > **Note**
  >
  > 이는 JavaScript 애플리케이션에서 사용할 수 있습니다.

주제

지능형 위협 통합 및 AWS 관리형 규칙

지능형 위협 통합 API는 지능형 위협 규칙 그룹을 사용하여 이러한 고급 관리형 규칙 그룹의 모든 기능을 활성화하는 웹 ACL과 함께 작동합니다.

- AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 관리 규칙 그룹. `AWSManagedRulesACFPRuleSet`

  계정 생성 사기는 공격자가 가입 보너스를 받거나 누군가를 사칭하는 등의 목적으로 애플리케이션에 유효하지 않은 계정을 생성하는 온라인 불법 활동입니다. ACFP 관리형 규칙 그룹은 악의적인 계정 생성 시도의 일부일 수 있는 요청을 차단하고, 여기에 레이블을 지정하고, 이를 관리하기 위한 규칙을 제공합니다. API를 통해 ACFP 규칙이 유효한 클라이언트 트래픽을 악성 트래픽과 구분하는 데 사용하는 미세 조정된 클라이언트 브라우저 확인 및 사용자 상호 작용 정보를 사용할 수 있습니다.

  자세한 내용은 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 및 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 섹션을 참조하세요.
- AWS WAF 사기 방지 계정 탈취 방지 (ATP) 관리 규칙 그룹. `AWSManagedRulesATPRuleSet`

  계정 탈취는 공격자가 개인 계정에 무단으로 액세스하는 온라인 불법 활동입니다. ATP 관리형 규칙 그룹은 악의적인 계정 탈취 시도의 일부일 수 있는 요청을 차단, 레이블 지정 및 관리하는 규칙을 제공합니다. API에서는 ATP 규칙이 유효한 클라이언트 트래픽을 악성 트래픽과 구분하는 데 사용하는 미세 조정된 클라이언트 확인 및 동작 집계를 사용할 수 있습니다.

  자세한 내용은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 및 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 섹션을 참조하세요.
- AWS WAF Bot Control 관리 규칙 그룹의 대상 보호 수준. `AWSManagedRulesBotControlRuleSet`

  봇은 대부분의 검색 엔진 및 크롤러와 같이 자체 식별이 가능하고 유용한 봇부터 웹 사이트를 공격하고 자체 식별이 불가능한 악성 봇에 이르기까지 다양합니다. Bot Control 관리형 규칙 그룹은 웹 트래픽의 봇 활동을 모니터링하고 레이블을 지정하며 관리하는 규칙을 제공합니다. 이 규칙 그룹의 대상

보호 수준을 사용하면 대상 규칙이 API가 제공하는 클라이언트 세션 정보를 사용하여 악성 봇을 더 잘 탐지합니다.

자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹 및 AWS WAF 봇 컨트롤 섹션을 참조하세요.

이러한 관리형 규칙 그룹 중 하나를 웹 ACL에 추가하려면, ACFP 관리형 규칙 그룹을 웹 ACL에 추가, ATP 관리형 규칙 그룹을 새 웹 ACL에 추가 및 웹 ACL에 AWS WAF 봇 제어 관리 규칙 그룹 추가 절차를 참조하세요.

> **Note**
>
> 관리형 규칙 그룹은 현재 토큰이 누락된 요청을 차단하지 않습니다. 토큰이 누락된 요청을 차단하려면 애플리케이션 통합 API를 구현한 후 유효한 AWS WAF 토큰이 없는 요청 차단의 지침을 따르십시오.

AWS WAF 클라이언트 애플리케이션 통합 API 액세스

JavaScript 통합 API는 일반적으로 사용할 수 있으며, 이를 실행하는 브라우저 및 기타 장치에 사용할 수 있습니다. JavaScript

AWS WAF Android 및 iOS 모바일 앱을 위한 맞춤형 지능형 위협 통합 SDK를 제공합니다.

- 안드로이드 모바일 앱의 경우 AWS WAF SDK는 안드로이드 API 버전 23 (안드로이드 버전 6) 이상에서 작동합니다. Android 버전에 대한 자세한 내용은 SDK 플랫폼 릴리스 노트를 참조하세요.
- iOS 모바일 앱의 경우 AWS WAF SDK는 iOS 버전 13 이상에서 작동합니다. iOS 버전에 대한 자세한 내용은 iOS 및 iPadOS 릴리스 노트를 참조하세요.

콘솔을 통해 통합 API에 액세스하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 애플리케이션 통합을 선택하고 원하는 탭을 선택합니다.

   - 지능형 위협 통합은 모든 모바일 애플리케이션에 JavaScript 사용할 수 있습니다.

     해당 탭에는 다음이 포함되어 있습니다.

    - 지능형 위협 애플리케이션 통합에 사용할 수 있는 웹 ACL 목록입니다. 이 목록에는 `AWSManagedRulesACFPRuleSet` 관리형 규칙 그룹, `AWSManagedRulesATPRuleSet` 관리형 규칙 그룹 또는 `AWSManagedRulesBotControlRuleSet` 관리형 규칙 그룹의 대상 보호 수준을 사용하는 각 웹 ACL이 포함됩니다. 지능형 위협 API를 구현할 때는 통합하려는 웹 ACL의 통합 URL을 사용합니다.
    - 액세스 권한이 있는 API. JavaScript API는 항상 사용할 수 있습니다. 모바일 SDK에 액세스하려면 AWS에 문의를 통해 지원 팀을 문의하십시오.
- CAPTCHA 통합은 애플리케이션에 사용할 수 있습니다. JavaScript

  해당 탭에는 다음이 포함되어 있습니다.

    - 통합에 사용할 통합 URL.
    - 클라이언트 애플리케이션 도메인용으로 생성한 API 키. CAPTCHA API를 사용하려면 클라이언트에게 도메인에서 CAPTCHA에 액세스할 AWS WAF 수 있는 권한을 부여하는 암호화된 API 키가 필요합니다. 통합하는 각 클라이언트마다 클라이언트 도메인이 포함된 API 키를 사용합니다. 이러한 요구 사항 및 이러한 키 관리에 대한 자세한 내용은 JS 캡차 API를 위한 API 키 관리 섹션을 참조하세요.

AWS WAF JavaScript 통합

JavaScript 통합 API를 사용하여 실행되는 브라우저 및 기타 기기에서 AWS WAF 애플리케이션 통합을 구현할 수 있습니다. JavaScript

CAPTCHA 퍼즐과 사일런트 챌린지는 브라우저가 HTTPS 엔드포인트에 액세스할 때만 실행할 수 있습니다. 토큰을 획득하려면 브라우저 클라이언트가 안전한 환경에서 실행되고 있어야 합니다.

- 지능형 위협 API를 사용하면 클라이언트 측 자동 브라우저 챌린지를 통해 토큰 인증을 관리하고 보호된 리소스로 보내는 요청에 토큰을 포함할 수 있습니다.
- CAPTCHA 통합 API가 지능형 위협 API에 추가되므로 클라이언트 애플리케이션에서 CAPTCHA 퍼즐의 배치와 특성을 사용자 지정할 수 있습니다. 이 API는 지능형 위협 API를 활용하여 최종 사용자가 CAPTCHA 퍼즐을 성공적으로 완료한 후 해당 페이지에서 사용할 AWS WAF 토큰을 획득합니다.

이러한 통합을 사용하면 클라이언트의 원격 프로시저 호출에 유효한 토큰이 포함되도록 할 수 있습니다. 애플리케이션 페이지에 이러한 통합 API가 있으면 유효한 토큰을 포함하지 않은 요청을 차단하는 등 완화 규칙을 웹 ACL에 구현할 수 있습니다. 규칙의 Challenge 또는 CAPTCHA 작업을 사용하여 클라이언트 애플리케이션이 획득한 토큰을 강제로 사용하도록 하는 규칙을 구현할 수도 있습니다.

다음 목록은 웹 애플리케이션 페이지의 지능형 위협 API의 일반적인 구현의 기본 구성 요소를 보여줍니다.

```
<head>
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></
script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

CAPTCHA 통합 API를 사용하면 최종 사용자의 CAPTCHA 퍼즐 환경을 사용자 지정할 수 있습니다. CAPTCHA 통합은 브라우저 검증 및 토큰 관리를 위한 JavaScript 지능형 위협 통합을 활용하고 CAPTCHA 퍼즐을 구성하고 렌더링하는 기능을 추가합니다.

다음 목록은 웹 애플리케이션 페이지에 JavaScript CAPTCHA API를 일반적으로 구현하는 기본 구성 요소를 보여줍니다.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Use WAF token to access protected resources
```

```
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

주제

- 토큰에 사용할 도메인 제공
- 콘텐츠 보안 정책과 함께 JavaScript API 사용
- 지능형 위협 JavaScript API 사용
- 캡차 API JavaScript 사용

토큰에 사용할 도메인 제공

기본적으로 토큰을 AWS WAF 생성할 때는 웹 ACL과 연결된 리소스의 호스트 도메인을 사용합니다. JavaScript API용으로 AWS WAF 생성하는 토큰에 추가 도메인을 제공할 수 있습니다. 이렇게 하려면 하나 이상의 토큰 도메인으로 글로벌 변수`window.awsWafCookieDomainList`를 구성합니다.

토큰을 AWS WAF 생성할 때는 웹 ACL과 연결된 리소스의 호스트 도메인과 내 도메인의 조합 중에서 가장 `window.awsWafCookieDomainList` 적절하고 가장 짧은 도메인을 사용합니다.

예제 설정:

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

이 목록에는 공개 접미사를 사용할 수 없습니다. 예를 들면 `gov.au` 또는 `co.uk`를 목록의 토큰 도메인으로 사용할 수 없습니다.

이 목록에서 지정하는 도메인은 다른 도메인 및 도메인 구성과 호환되어야 합니다.

- 도메인은 보호된 호스트 도메인과 웹 ACL용으로 구성된 토큰 도메인 목록을 기반으로 AWS WAF 허용할 도메인이어야 합니다. 자세한 정보는 AWS WAF 웹 ACL 토큰 도메인 목록 구성을 참조하세요.
- JavaScript CAPTCHA API를 사용하는 경우 CAPTCHA API 키에 있는 하나 이상의 도메인이 있는 토큰 도메인 중 하나와 정확히 `window.awsWafCookieDomainList` 일치하거나 해당 토큰 도메인 중 하나의 최상위 도메인이어야 합니다.

  예를 들어 토큰 도메인 `mySubdomain.myApex.com`의 경우 API 키 `mySubdomain.myApex.com`은 정확히 일치하고 API 키 `myApex.com`은 apex 도메인입니다. 두 키 중 하나가 토큰 도메인과 일치합니다.

  API 키에 대한 자세한 내용은 JS 캡차 API를 위한 API 키 관리 섹션을 참조하세요.

`AWSManagedRulesACFPRuleSet` 관리형 규칙 그룹을 사용하는 경우 규칙 그룹 구성에 제공한 계정 생성 경로의 도메인과 일치하는 도메인을 구성할 수 있습니다. 이 구성에 대한 자세한 정보는 ACFP 관리형 규칙 그룹을 웹 ACL에 추가 섹션을 참조하세요.

`AWSManagedRulesATPRuleSet` 관리형 규칙 그룹을 사용하는 경우 규칙 그룹 구성에 제공한 로그인 경로의 도메인과 일치하는 도메인을 구성할 수 있습니다. 이 구성에 대한 자세한 정보는 ATP 관리형 규칙 그룹을 새 웹 ACL에 추가 섹션을 참조하세요.

콘텐츠 보안 정책과 함께 JavaScript API 사용

리소스에 콘텐츠 보안 정책 (CSP) 을 적용하는 경우 JavaScript 구현이 제대로 작동하려면 AWS WAF apex 도메인을 허용 목록에 추가해야 합니다. `awswaf.com` JavaScript SDK는 다양한 AWS WAF 엔드포인트를 호출하므로 이 도메인을 허용하면 SDK가 작동하는 데 필요한 권한이 제공됩니다.

다음은 apex 도메인을 허용 목록에 추가하는 예제 구성입니다. AWS WAF

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

CSP를 사용하는 리소스에 JavaScript SDK를 사용하려고 하는데 AWS WAF 도메인을 허용 목록에 추가하지 않은 경우 다음과 같은 오류가 발생합니다.

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

지능형 위협 JavaScript API 사용

지능형 위협 API는 사용자 브라우저에 대해 자동 챌린지를 실행하고, 챌린지 성공 증명 및 CAPTCHA 응답을 제공하는 AWS WAF 토큰을 처리하는 작업을 제공합니다.

먼저 테스트 환경에서 JavaScript 통합을 구현한 다음 프로덕션 환경에서 구현하십시오. 추가 코딩 지침은 다음 섹션을 참조하세요

지능형 위협 API를 사용하려면

1. API 설치

   CAPTCHA API를 사용할 경우 이 단계를 건너뛸 수 있습니다. CAPTCHA API를 설치하면 스크립트가 지능형 위협 API를 자동으로 설치합니다.

   a. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   b. 탐색 창에서 애플리케이션 통합을 선택합니다. 애플리케이션 통합 페이지에서 탭으로 구분된 옵션을 볼 수 있습니다.

   c. 지능형 위협 통합을 선택합니다.

   d. 탭에서 통합할 웹 ACL을 선택합니다. 웹 ACL 목록에는 `AWSManagedRulesACFPRuleSet` 관리형 규칙 그룹, `AWSManagedRulesATPRuleSet` 관리형 규칙 그룹 또는 `AWSManagedRulesBotControlRuleSet` 관리형 규칙 그룹의 대상 보호 수준을 사용하는 웹 ACL만 포함됩니다.

   e. JavaScript SDK 패널을 열고 통합에 사용할 스크립트 태그를 복사합니다.

   f. 애플리케이션 페이지 코드의 <head> 섹션에 웹 ACL용으로 복사한 스크립트 태그를 삽입합니다. 이 포함으로 인해 클라이언트 애플리케이션은 페이지 로드 시 백그라운드에서 토큰을 자동으로 검색합니다.

   ```
   <head>
       <script type="text/javascript" src="Web ACL integration URL/challenge.js”
    defer></script>
   <head>
   ```

이 <script> 목록은 defer 속성으로 구성되지만 페이지에 다른 동작을 적용하려는 경우 설정을 async로 변경할 수 있습니다.

2. (선택 사항) 클라이언트 토큰용 도메인 구성 추가 - 기본적으로 토큰을 AWS WAF 생성할 때 웹 ACL과 연결된 리소스의 호스트 도메인을 사용합니다. JavaScript API에 추가 도메인을 제공하려면 의 지침을 따르십시오. 토큰에 사용할 도메인 제공
3. 지능형 위협 통합 코딩 - 클라이언트가 보호되는 엔드포인트로 요청을 보내기 전에 토큰 검색이 완료되도록 코드를 작성합니다. 이미 fetch API를 사용하여 호출하고 있는 경우 AWS WAF 통합 fetch 래퍼를 대체할 수 있습니다. fetchAPI를 사용하지 않는 경우 AWS WAF 통합 getToken 작업을 대신 사용할 수 있습니다. 코딩 지침은 다음 섹션을 참조하세요.
4. 웹 ACL에 토큰 확인 추가 - 클라이언트가 보내는 웹 요청에서 유효한 챌린지 토큰이 있는지 확인하는 하나 이상의 규칙을 웹 ACL에 추가합니다. Bot Control 관리형 규칙 그룹의 대상 수준과 같이 챌린지 토큰을 확인하고 모니터링하는 규칙 그룹을 사용할 수 있으며, CAPTCHA그리고 Challenge 안에 AWS WAF에 설명된 대로 Challenge 규칙 작업을 사용하여 확인할 수 있습니다.

   웹 ACL 추가는 보호된 엔드포인트에 대한 요청에 클라이언트 통합에서 획득한 토큰이 포함되어 있는지 확인합니다. 유효하고 만료되지 않은 토큰이 포함된 요청은 Challenge 검사를 통과하므로 클라이언트에게 자동 챌린지를 다시 보내지 않습니다.
5. (선택 사항) 토큰이 누락된 요청 차단 - ACFP 관리형 규칙 그룹, ATP 관리형 규칙 그룹 또는 Bot Control 규칙 그룹의 대상 규칙과 함께 API를 사용하는 경우 이러한 규칙은 누락된 토큰이 있는 요청을 차단하지 않습니다. 토큰이 누락된 요청을 차단하려면 유효한 AWS WAF 토큰이 없는 요청 차단의 지침을 따르십시오.

주제

- 지능형 위협 API 사양
- 통합 fetch 래퍼 사용 방법
- getToken 통합의 사용 방법

지능형 위협 API 사양

이 섹션에는 지능형 위협 완화 JavaScript API의 방법 및 속성에 대한 사양이 나열되어 있습니다. 지능형 위협 및 CAPTCHA 통합에 이러한 API를 사용합니다.

`AwsWafIntegration.fetch()`

AWS WAF 통합 구현을 사용하여 서버에 HTTP fetch 요청을 보냅니다.

`AwsWafIntegration.getToken()`

저장된 AWS WAF 토큰을 검색하여 현재 페이지의 쿠키에 이름 `aws-waf-token` 및 토큰 값으로 설정된 값과 함께 저장합니다.

`AwsWafIntegration.hasToken()`

`aws-waf-token` 쿠키가 현재 만료되지 않은 토큰을 보유하고 있는지 여부를 나타내는 부울을 반환합니다.

CAPTCHA 통합도 사용하는 경우 캡차 API JavaScript 사양에서 해당 사양을 참조하세요.

통합 **`fetch`** 래퍼 사용 방법

`AwsWafIntegration`네임스페이스에서 `fetch` API에 대한 일반 `fetch` 호출을 변경하여 AWS WAF `fetch` 래퍼를 사용할 수 있습니다. AWS WAF 래퍼는 표준 JavaScript `fetch` API 호출과 동일한 옵션을 모두 지원하며 통합을 위한 토큰 처리를 추가합니다. 이 접근 방식은 일반적으로 애플리케이션을 통합하는 가장 간단한 방법입니다.

래퍼를 구현하기 전

다음 예제 목록은 `AwsWafIntegration` `fetch` 래퍼를 구현하기 전의 표준 코드를 보여줍니다.

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

래퍼를 구현한 후

다음 목록은 `AwsWafIntegration` `fetch` 래퍼 구현과 동일한 코드를 보여줍니다.

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

getToken 통합의 사용 방법

AWS WAF 현재 토큰의 값으로 이름이 지정된 aws-waf-token 쿠키를 포함하도록 보호된 엔드포인트에 대한 요청이 필요합니다.

getToken 작업은 저장된 AWS WAF 토큰을 검색하여 이름이 aws-waf-token인 현재 페이지의 쿠키에 저장하는 비동기식 API 직접 호출이며, 해당 값은 토큰 값으로 설정됩니다. 필요에 따라 페이지에서 이 토큰 쿠키를 사용할 수 있습니다.

getToken를 을 호출하면 다음과 같은 작업을 수행합니다.

- 만료되지 않은 토큰을 이미 사용할 수 있는 경우 호출 시 해당 토큰이 즉시 반환됩니다.
- 그렇지 않으면 호출 시 토큰 공급자로부터 새 토큰을 검색하고 토큰 획득 워크플로가 제한 시간 초과 전에 완료될 때까지 최대 2초간 기다립니다. 작업 제한 시간이 초과되면 오류가 발생하며, 호출 코드에서 이를 처리해야 합니다.

getToken 작업에는 aws-waf-token 쿠키가 현재 만료되지 않은 토큰을 보유하고 있는지 여부를 나타내는 hasToken 작업이 함께 제공됩니다.

AwsWafIntegration.getToken()유효한 토큰을 검색하여 쿠키로 저장합니다. 대부분의 클라이언트 호출은 이 쿠키를 자동으로 연결하지만 일부는 그렇지 않습니다. 예를 들어 호스트 도메인에서 이루어진 호출에는 쿠키가 첨부되지 않습니다. 이어지는 구현 세부 정보에서는 두 가지 유형의 클라이언트 호출을 모두 처리하는 방법을 보여줍니다.

기본 **getToken** 구현, **aws-waf-token** 쿠키를 첨부하는 호출의 경우

다음 예제 목록은 로그인 요청으로 getToken 작업을 구현하기 위한 표준 코드를 보여줍니다.

```
const login_response = await AwsWafIntegration.getToken()
     .catch(e => {
         // Implement error handling logic for your use case
     })
     // The getToken call returns the token, and doesn't typically require special
 handling
     .then(token => {
         return loginToMyPage()
     })

 async function loginToMyPage() {
     // Your existing login code
 }
```

getToken에서 토큰을 사용할 수 있게 된 후에만 양식을 제출하십시오.

다음 목록은 유효한 토큰을 사용할 수 있을 때까지 양식 제출을 가로채는 이벤트 리스너를 등록하는 방법을 보여줍니다.

```
<body>
   <h1>Login</h1>
   <p></p>
   <form id="login-form" action="/web/login" method="POST" enctype="application/x-www-
form-urlencoded">
     <label for="input_username">USERNAME</label>
     <input type="text" name="input_username" id="input_username"><br>
     <label for="input_password">PASSWORD</label>
     <input type="password" name="input_password" id="input_password"><br>
     <button type="submit">Submit<button>
   </form>

 <script>
   const form = document.querySelector("#login-form");

   // Register an event listener to intercept form submissions
   form.addEventListener("submit", (e) => {
       // Submit the form only after a token is available
       if (!AwsWafIntegration.hasToken()) {
           e.preventDefault();
           AwsWafIntegration.getToken().then(() => {
               e.target.submit();
           }, (reason) => { console.log("Error:"+reason) });
         }
     });
 </script>
 </body>
```

클라이언트가 기본적으로 **aws-waf-token** 쿠키를 연결하지 않을 때 토큰 연결

AwsWafIntegration.getToken()유효한 토큰을 검색하여 쿠키로 저장하지만 모든 클라이언트 호출이 기본적으로 이 쿠키를 첨부하지는 않습니다. 예를 들어 호스트 도메인에서 이루어진 호출에는 쿠키가 연결되지 않습니다.

fetch래퍼는 이러한 경우를 자동으로 처리하지만 fetch 래퍼를 사용할 수 없는 경우 사용자 지정 x-aws-waf-token 헤더를 사용하여 처리할 수 있습니다. AWS WAF 쿠키에서 토큰을 읽는 것 외에도 이 헤더에서 토큰을 읽습니다. aws-waf-token 다음 코드는 헤더 설정의 예를 보여줍니다.

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
});
```

기본적으로 요청된 호스트 도메인과 동일한 도메인을 포함하는 AWS WAF 토큰만 허용합니다. 모든 크로스 도메인 토큰에는 웹 ACL 토큰 도메인 목록에 해당하는 항목이 있어야 합니다. 자세한 정보는 AWS WAF 웹 ACL 토큰 도메인 목록 구성을 참조하세요.

도메인 간 토큰 사용에 대한 추가 정보는 aws-samples/ -를 참조하십시오. aws-waf-bot-control api-protection-with-captcha

캡차 API JavaScript 사용

CAPTCHA JavaScript API를 사용하면 CAPTCHA 퍼즐을 구성하고 클라이언트 애플리케이션에서 원하는 위치에 배치할 수 있습니다. 이 API는 지능형 위협 API의 기능을 활용하여 최종 사용자가 JavaScript CAPTCHA 퍼즐을 성공적으로 완료한 후 AWS WAF 토큰을 획득하고 사용합니다.

먼저 테스트 환경에서 JavaScript 통합을 구현한 다음 프로덕션 환경에서 구현하십시오. 추가 코딩 지침은 다음 섹션을 참조하세요

CAPTCHA 통합 API를 사용하려면

1. API 설치

   a. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   b. 탐색 창에서 애플리케이션 통합을 선택합니다. 애플리케이션 통합 페이지에서 탭으로 구분된 옵션을 볼 수 있습니다.

   c. CAPTCHA 통합을 선택합니다.

   d. 나열된 JavaScript 통합 스크립트 태그를 복사하여 통합에 사용하십시오.

   e. 애플리케이션 페이지 코드의 <head> 섹션에 복사한 스크립트 태그를 삽입합니다. 이 포함으로 CAPTCHA 퍼즐을 구성 및 사용할 수 있게 됩니다.

```
<head>
    <script type="text/javascript" src="integrationURL/jsapi.js" defer></
script>
```

```
</head>
```

이 <script> 목록은 defer 속성으로 구성되지만 페이지에 다른 동작을 적용하려는 경우 설정을 async로 변경할 수 있습니다.

또한 CAPTCHA 스크립트는 지능형 위협 통합 스크립트가 아직 없는 경우 자동으로 로드합니다. 지능형 위협 통합 스크립트는 클라이언트 애플리케이션이 페이지 로드 시 백그라운드에서 토큰을 자동으로 검색하도록 하고 CAPTCHA API 사용에 필요한 기타 토큰 관리 기능을 제공합니다.

2. (선택 사항) 클라이언트 토큰의 도메인 구성 추가 - 기본적으로 토큰을 AWS WAF 생성할 때 웹 ACL과 연결된 리소스의 호스트 도메인을 사용합니다. JavaScript API에 추가 도메인을 제공하려면 의 지침을 따르십시오. 토큰에 사용할 도메인 제공
3. 클라이언트의 암호화된 API 키 가져오기 - CAPTCHA API에는 유효한 클라이언트 도메인 목록이 포함된 암호화된 API 키가 필요합니다. AWS WAF 이 키를 사용하여 통합에 사용 중인 클라이언트 도메인이 CAPTCHA를 사용하도록 AWS WAF 승인되었는지 확인합니다. API 키를 생성하려면 JS 캡차 API를 위한 API 키 관리의 지침을 따르십시오.
4. CAPTCHA 위젯 구현 코딩 - 페이지 내 renderCaptcha() API 호출을 사용할 위치에서 호출을 구현합니다. 이 함수의 구성 및 사용에 대한 자세한 내용은 캡차 API JavaScript 사양 및 CAPTCHA 퍼즐을 렌더링하는 방법 섹션을 참조하세요.

   CAPTCHA 구현은 토큰 관리 및 토큰을 사용하는 페치 호출 실행을 위해 지능형 위협 통합 API와 통합됩니다. AWS WAF 이러한 API 사용에 대한 지침은 지능형 위협 JavaScript API 사용 섹션을 참조하세요.
5. 웹 ACL에 토큰 확인 추가 - 클라이언트가 보내는 웹 요청에서 유효한 CAPTCHA 토큰이 있는지 확인하는 하나 이상의 규칙을 웹 ACL에 추가합니다. CAPTCHA그리고 Challenge 안에 AWS WAF에 설명된 대로 CAPTCHA 규칙 작업을 사용하여 확인할 수 있습니다.

   웹 ACL 추가는 보호된 엔드포인트에 대한 요청에 클라이언트 통합에서 획득한 토큰이 포함되어 있는지 확인합니다. 유효하고 만료되지 않은 CAPTCHA 토큰을 포함하는 요청은 CAPTCHA 규칙 작업 검사를 통과하므로 최종 사용자에게 또 다른 CAPTCHA 퍼즐을 제시하지 않습니다.

주제

- 캡차 API JavaScript 사양
- CAPTCHA 퍼즐을 렌더링하는 방법
- 에서 캡차 응답 처리하기 AWS WAF
- JS 캡차 API를 위한 API 키 관리

캡차 API JavaScript 사양

이 섹션에는 CAPTCHA API의 메서드 및 속성에 대한 사양이 나열되어 있습니다. JavaScript CAPTCHA JavaScript API를 사용하여 클라이언트 애플리케이션에서 사용자 지정 CAPTCHA 퍼즐을 실행할 수 있습니다.

이 API는 토큰 획득 및 사용을 구성 및 관리하는 데 사용하는 지능형 위협 API를 기반으로 합니다. AWS WAF 지능형 위협 API 사양 섹션을 참조하세요.

`AwsWafCaptcha.renderCaptcha(container, configuration)`

최종 사용자에게 AWS WAF CAPTCHA 퍼즐을 제시하고, 성공하면 CAPTCHA 검증을 통해 클라이언트 토큰을 업데이트합니다. 이 방법은 CAPTCHA 통합에서만 사용할 수 있습니다. 이 호출을 지능형 위협 API와 함께 사용하여 토큰 검색을 관리하고 `fetch` 호출에 토큰을 제공합니다. 지능형 위협 API 사양에서 지능형 위협 API를 참조하세요.

AWS WAF 전송하는 CAPTCHA 전면 광고와 달리 이 방법으로 렌더링된 CAPTCHA 퍼즐은 초기 제목 화면 없이 퍼즐을 즉시 표시합니다.

`container`

페이지에 있는 대상 컨테이너 요소의 `Element` 객체입니다. 이는 일반적으로 `document.getElementById()` 또는 `document.querySelector()` 호출을 통해 검색됩니다.

필수 항목 여부: 예

유형: `Element`

구성

다음과 같은 CAPTCHA 구성 설정이 포함된 객체입니다.

`apiKey`

클라이언트 도메인에 대한 권한을 활성화하는 암호화된 API 키입니다. AWS WAF 콘솔을 사용하여 클라이언트 도메인용 API 키를 생성합니다. 최대 5개의 도메인에 대해 1개 키를 사용할 수 있습니다. 자세한 내용은 JS 캡차 API를 위한 API 키 관리을 참조하세요.

필수 항목 여부: 예

유형: `string`

onSuccess: (wafToken: string) => void;

최종 사용자가 CAPTCHA AWS WAF 퍼즐을 성공적으로 완료하면 유효한 토큰과 함께 호출됩니다. 웹 ACL로 보호하는 엔드포인트에 보내는 요청에는 토큰을 사용하십시오. AWS WAF 토큰은 가장 최근에 퍼즐을 성공적으로 완료했다는 증거와 타임스탬프를 제공합니다.

필수 항목 여부: 예

onError?: (error: CaptchaError) => void;

CAPTCHA 작업 중에 오류가 발생하면 오류 객체와 함께 호출됩니다.

필수 여부: 아니요

CaptchaError 클래스 정의 - onError 핸들러는 다음 클래스 정의와함께 오류 유형을 제공합니다.

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- kind - 반환된 오류의 종류.
- statusCode - HTTP 상태 코드(있는 경우). 이러한 클래스는 HTTP 오류로 인해 오류가 발생한 network_error에서 사용됩니다.

onLoad?: () => void;

새 CAPTCHA 퍼즐이 로드될 때 호출됩니다.

필수 여부: 아니요

onPuzzleTimeout?: () => void;

CAPTCHA 퍼즐이 만료되기 전에 완료되지 않을 때 호출됩니다.

필수 여부: 아니요

onPuzzleCorrect?: () => void;

CAPTCHA 퍼즐에 정답이 제공될 때 호출됩니다.

필수 여부: 아니요

onPuzzleIncorrect?: () => void;

CAPTCHA 퍼즐에 오답이 제공될 때 호출됩니다.

필수 여부: 아니요

defaultLocale

CAPTCHA 퍼즐에 사용할 기본 로케일입니다. CAPTCHA 퍼즐에 대한 서면 지침이 아랍어(ar-SA), 중국어 간체(zH-CN), 네덜란드어(nl-NL), 영어(en-US), 프랑스어(fr-FR), 독일어(de-DE), 이탈리아어(it-IT), 일본어(Ja-JP), 포르투갈어(Pt-Br), 스페인어(es-ES) 및 터키어(tr-TR)로 제공됩니다. 오디오 지침은 기본적으로 영어인 중국어와 일본어를 제외한 모든 서면 언어에 사용할 수 있습니다. 기본 언어를 변경하려면 국제 언어 및 로케일 코드를 입력하십시오(예:). `ar-SA`

기본값: 최종 사용자의 브라우저에서 현재 사용 중인 언어

필수 여부: 아니요

유형: `string`

disableLanguageSelector

`true`로 설정하면 CAPTCHA 퍼즐이 언어 선택기를 숨깁니다.

기본값: `false`

필수 여부: 아니요

유형: `boolean`

dynamicWidth

`true`로 설정하면 CAPTCHA 퍼즐의 너비가 브라우저 창 너비와 호환되도록 너비가 변경됩니다.

기본값: `false`

필수 여부: 아니요

유형: `boolean`

skipTitle

`true`로 설정하면 CAPTCHA 퍼즐에 퍼즐 풀기라는 제목이 표시되지 않습니다.

기본값: `false`

필수 여부: 아니요

유형: `boolean`

CAPTCHA 퍼즐을 렌더링하는 방법

클라이언트 인터페이스에서 원하는 곳에서 AWS WAF `renderCaptcha` 통화를 사용할 수 있습니다. 호출은 CAPTCHA 퍼즐을 검색하여 렌더링하고 확인을 위해 결과를 로 보냅니다. AWS WAF AWS WAF 전화를 걸 때 퍼즐 렌더링 구성과 최종 사용자가 퍼즐을 완료했을 때 실행할 콜백을 제공합니다. 옵션에 대한 자세한 내용은 앞 섹션인 캡차 API JavaScript 사양 섹션을 참조하세요.

이 호출을 지능형 위협 통합 API의 토큰 관리 기능과 함께 사용하십시오. 이 호출은 CAPTCHA 퍼즐의 성공적인 완료를 확인하는 토큰을 클라이언트에게 제공합니다. 지능형 위협 통합 API를 사용하여 토큰을 관리하고 웹 ACL로 보호되는 엔드포인트에 대한 클라이언트 호출에서 토큰을 제공할 수 있습니다. AWS WAF 지능형 위협 API에 대한 자세한 내용은 지능형 위협 JavaScript API 사용 섹션을 참조하세요.

예제 구현

다음 예제 목록은 섹션의 AWS WAF 통합 URL 배치를 포함한 표준 CAPTCHA 구현을 보여줍니다. `<head>`

이 목록은 지능형 위협 통합 API의 `AwsWafIntegration.fetch` 래퍼를 사용하는 성공 콜백으로 `renderCaptcha` 함수를 구성합니다. 이 함수에 대한 자세한 내용은 통합 `fetch` 래퍼 사용 방법 섹션을 참조하세요.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
        // Captcha completed. wafToken contains a valid WAF token. Store it for
        // use later or call AwsWafIntegration.fetch() to use it easily.
        // It will expire after a time, so calling AwsWafIntegration.getToken()
```

```
        // again is advised if the token is needed later on, outside of using the
        // fetch wrapper.

        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            headers: {
                "Content-Type": "application/json",
            },
            body: "{ ... }" /* body content */
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

예제 구성 설정

다음 예제 목록은 너비 및 제목 옵션이 기본값이 아닌 값으로 설정된 `renderCaptcha`를 보여줍니다.

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
            skipTitle: true
        });
```

구성 옵션에 대한 전체 정보는 캡차 API JavaScript 사양 섹션을 참조하세요.

에서 캡차 응답 처리하기 AWS WAF

CAPTCHA작업이 포함된 AWS WAF 규칙은 요청에 유효한 CAPTCHA 타임스탬프가 있는 토큰이 없는 경우 일치하는 웹 요청에 대한 평가를 종료합니다. 요청이 GET text/html 호출인 경우 CAPTCHA 작업은 CAPTCHA 퍼즐이 포함된 중간 광고를 클라이언트에게 제공합니다. CAPTCHA JavaScript API를

통합하지 않으면 전면 광고에서 퍼즐을 실행하고 최종 사용자가 문제를 성공적으로 해결하면 자동으로 요청을 다시 제출합니다.

CAPTCHA JavaScript API를 통합하고 CAPTCHA 처리를 사용자 지정하는 경우 종료되는 CAPTCHA 응답을 감지하고 사용자 지정 CAPTCHA를 제공한 다음 최종 사용자가 문제를 성공적으로 해결하면 클라이언트의 웹 요청을 다시 제출해야 합니다.

다음 코드 예제에서는 이를 수행하는 방법을 보여줍니다.

> **Note**
>
> AWS WAF CAPTCHA작업 응답의 상태 코드는 HTTP 405이며, 이 코드를 사용하여 이 코드에서 응답을 인식합니다. CAPTCHA 보호된 엔드포인트가 HTTP 405 상태 코드를 사용하여 동일한 호출에 대해 다른 유형의 응답을 전달하는 경우 이 예제 코드는 이러한 응답에 대해 CAPTCHA 퍼즐도 랜더링합니다.

```
<!DOCTYPE html>
<html>
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>
<body>
    <div id="my-captcha-box"></div>
    <div id="my-output-box"></div>

    <script type="text/javascript">
    async function loadData() {
        // Attempt to fetch a resource that's configured to trigger a CAPTCHA
        // action if the rule matches. The CAPTCHA response has status=HTTP 405.
        const result = await AwsWafIntegration.fetch("/protected-resource");

        // If the action was CAPTCHA, render the CAPTCHA and return

        // NOTE: If the endpoint you're calling in the fetch call responds with HTTP
 405
        // as an expected response status code, then this check won't be able to tell
 the
        // difference between that and the CAPTCHA rule action response.

        if (result.status === 405) {
```

```
            const container = document.querySelector("#my-captcha-box");
            AwsWafCaptcha.renderCaptcha(container, {
                apiKey: "...API key goes here...",
                onSuccess() {
                    // Try loading again, now that there is a valid CAPTCHA token
                    loadData();
                },
            });
            return;
        }

        const container = document.querySelector("#my-output-box");
        const response = await result.text();
        container.innerHTML = response;
    }

    window.addEventListener("load", () => {
        loadData();
    });
    </script>
</body>
</html>
```

JS 캡차 API를 위한 API 키 관리

JavaScript API를 사용하여 AWS WAF CAPTCHA를 클라이언트 애플리케이션에 통합하려면 CAPTCHA 퍼즐을 실행하려는 클라이언트 도메인의 JavaScript API 통합 태그와 암호화된 API 키가 필요합니다.

CAPTCHA 애플리케이션 통합은 암호화된 API 키를 JavaScript 사용하여 클라이언트 애플리케이션 도메인에 CAPTCHA API 사용 권한이 있는지 확인합니다. AWS WAF 클라이언트에서 CAPTCHA API를 호출할 때는 현재 JavaScript 클라이언트의 도메인이 포함된 도메인 목록이 포함된 API 키를 제공합니다. 암호화된 키 하나에 도메인을 최대 5개까지 나열할 수 있습니다.

API 키 요구 사항

CAPTCHA 통합에 사용하는 API 키에는 키를 사용하는 클라이언트에 적용되는 도메인이 포함되어야 합니다.

- 클라이언트의 지능형 위협 통합에서 `window.awsWafCookieDomainList`를 지정하는 경우 API 키의 하나 이상의 도메인이 `window.awsWafCookieDomainList`의 해당 토큰 도메인 중 하나와 정확히 일치하거나 해당 토큰 도메인 중 하나의 apex 도메인이어야 합니다.

예를 들어 토큰 도메인 `mySubdomain.myApex.com`의 경우 API 키 `mySubdomain.myApex.com`은 정확히 일치하고 API 키 `myApex.com`은 apex 도메인입니다. 두 키 중 하나가 토큰 도메인과 일치합니다.

토큰 도메인 목록 설정에 대한 자세한 내용은 토큰에 사용할 도메인 제공 섹션을 참조하세요.

- 그렇지 않으면 현재 도메인이 API 키에 포함되어야 합니다. 현재 도메인은 브라우저 주소 표시줄에서 볼 수 있는 도메인입니다.

사용하는 도메인은 보호된 호스트 도메인 및 웹 ACL용으로 구성된 토큰 도메인 목록을 기반으로 AWS WAF 허용할 도메인이어야 합니다. 자세한 정보는 AWS WAF 웹 ACL 토큰 도메인 목록 구성을 참조하세요.

API 키에 사용할 지역을 선택하는 방법

AWS WAF 사용 가능한 모든 지역에서 AWS WAF CAPTCHA API 키를 생성할 수 있습니다.

일반적으로 CAPTCHA API 키에는 웹 ACL에 사용하는 것과 동일한 지역을 사용해야 합니다. 하지만 전 세계 사용자가 지역 웹 ACL을 사용할 것으로 예상되는 경우 범위가 지정된 CAPTCHA JavaScript 통합 태그와 범위가 지정된 API 키를 확보하여 지역 웹 CloudFront ACL과 함께 사용할 수 있습니다. CloudFront 이 접근 방식을 사용하면 클라이언트가 가장 가까운 지역에서 CAPTCHA 퍼즐을 로드하여 지연 시간을 줄일 수 있습니다.

범위를 제외한 지역으로 범위가 지정된 CAPTCHA API 키는 CloudFront 여러 지역에서 사용할 수 없습니다. 범위가 지정된 지역에서만 사용할 수 있습니다.

클라이언트 도메인용 API 키 생성하려면

콘솔을 통해 통합 URL을 얻고 API 키를 생성 및 검색합니다.

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 애플리케이션 통합을 선택합니다.
3. 애플리케이션 통합이 활성화된 웹 ACL 창에서 API 키에 사용할 지역을 선택합니다. CAPTCHA 통합 탭의 API 키 창에서 지역을 선택할 수도 있습니다.
4. CAPTCHA 통합 탭을 선택합니다. 이 탭은 통합에 사용할 수 있는 CAPTCHA JavaScript 통합 태그와 API 키 목록을 제공합니다. 두 지역 모두 선택한 지역으로 범위가 지정됩니다.
5. API 키 창에서 키 생성을 선택합니다. 키 생성 대화 상자가 나타납니다.

6. 키에 포함할 클라이언트 도메인을 입력합니다. 최대 5개를 입력할 수 있습니다. 작업을 마쳤으면 키 생성을 선택합니다. 인터페이스가 새 키가 나열된 CAPTCHA 통합 탭으로 돌아갑니다.

   API 키는 생성하고 나면 변경할 수 없습니다. 키를 변경해야 하는 경우 새 키를 생성하여 대신 사용하십시오.

7. (선택 사항) 통합에 사용할 수 있도록 새로 생성된 키를 복사합니다.

이 작업에 REST API 또는 언어별 AWS SDK 중 하나를 사용할 수도 있습니다. REST API 호출은 API 키 생성과 목록 API 키입니다.

API 키를 삭제하려면

API 키를 삭제하려면 REST API 또는 언어별 AWS SDK 중 하나를 사용해야 합니다. REST API 호출은 API 키 삭제입니다. 콘솔을 사용하여 키를 삭제할 수는 없습니다.

키를 삭제한 후 모든 지역에서 키 사용을 AWS WAF 금지하는 데 최대 24시간이 걸릴 수 있습니다.

AWS WAF 모바일 애플리케이션 통합

AWS WAF 모바일 SDK를 사용하여 Android 및 iOS 모바일 애플리케이션을 위한 AWS WAF 지능형 위협 통합 SDK를 구현할 수 있습니다.

- Android 모바일 앱의 경우 AWS WAF SDK는 Android API 버전 23 (Android 버전 6) 이상에서 작동합니다. Android 버전에 대한 자세한 내용은 SDK 플랫폼 릴리스 노트를 참조하세요.
- iOS 모바일 앱의 경우 AWS WAF SDK는 iOS 버전 13 이상에서 작동합니다. iOS 버전에 대한 자세한 내용은 iOS 및 iPadOS 릴리스 노트를 참조하세요.

모바일 SDK를 사용하면 토큰 인증을 관리하고 보호된 리소스에 보내는 요청에 토큰을 포함할 수 있습니다. SDK를 사용하면 클라이언트의 원격 프로시저 호출에 유효한 토큰이 포함되도록 할 수 있습니다. 또한 애플리케이션 페이지에 이러한 통합이 있으면 유효한 토큰을 포함하지 않는 요청을 차단하는 등 완화 규칙을 웹 ACL에 구현할 수 있습니다.

모바일 SDK에 액세스하려면 AWS에 문의를 통해 지원 팀을 문의하십시오.

> **Note**
>
> AWS WAF 모바일 SDK는 CAPTCHA 사용자 지정에 사용할 수 없습니다.

SDK를 사용하는 기본 접근 방식은 구성 객체를 사용하여 토큰 공급자를 만든 다음 토큰 공급자를 사용하여 토큰을 가져오는 것입니다. AWS WAF기본적으로 토큰 공급자는 검색된 토큰을 보호된 리소스에 대한 웹 요청에 포함합니다.

다음은 주요 구성 요소를 보여주는 SDK 구현의 부분 목록입니다. 더 많은 예제를 보려면 AWS WAF 모바일 SDK용 코드 작성 단원을 참조하세요.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
 String domainName = "Domain name";
 WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
 WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);
 WAFToken token = tokenProvider.getToken();
```

AWS WAF 모바일 SDK 설치

모바일 SDK에 액세스하려면 AWS에 문의를 통해 지원 팀을 문의하십시오.

먼저 테스트 환경에서 모바일 SDK를 구현한 다음 프로덕션 환경에서 구현합니다.

AWS WAF 모바일 SDK를 설치하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 애플리케이션 통합을 선택합니다.
3. 지능형 위협 통합 탭에서 다음을 수행합니다.

a. 애플리케이션 통합용으로 활성화되는 웹 ACL 창애서 통합하려는 웹 ACL을 찾습니다. 구현에 사용할 웹 ACL 통합 URL을 복사하여 저장합니다. API 호출 `GetWebACL`을 통해 이 URL을 얻을 수도 있습니다.

b. 모바일 장치 유형과 버전을 선택한 다음 다운로드를 선택합니다. 원하는 버전을 선택할 수 있지만 최신 버전을 사용하는 것이 좋습니다. AWS WAF 장치용 `zip` 파일을 표준 다운로드 위치에 다운로드합니다.

4. 앱 개발 환경에서 선택한 작업 위치로 파일의 압축을 풉니다. zip 파일의 최상위 디렉터리에서 `README`을 찾아 엽니다. `README`파일의 지침에 따라 모바일 앱 코드에 사용할 AWS WAF 모바일 SDK를 설치합니다.

5. 다음 섹션의 지침에 따라 앱을 프로그래밍합니다.

AWS WAF 모바일 SDK 사양

이 섹션에는 사용 가능한 최신 버전의 AWS WAF 모바일 SDK에 대한 SDK 객체, 작업 및 구성 설정이 나열되어 있습니다. 다양한 구성 설정 조합에 적합한 토큰 공급자 및 작업의 작동 방식에 대한 자세한 내용은 AWS WAF 모바일 SDK 작동 방식 섹션을 참조하세요.

`WAFToken`

AWS WAF 토큰을 보관합니다.

`getValue()`

`WAFToken`의 `String` 표현을 가져옵니다.

`WAFTokenProvider`

모바일 앱에서 토큰을 관리합니다. `WAFConfiguration` 객체를 사용하여 이를 구현합니다.

`getToken()`

백그라운드 새로 고침이 활성화된 경우 캐시된 토큰이 반환됩니다. 백그라운드 새로 고침이 비활성화된 경우 새 토큰을 AWS WAF 검색하기 위한 동기 차단 호출이 이루어집니다.

`onTokenReady(WAFTokenResultCallback)`

활성 토큰이 준비되면 토큰 공급자에게 토큰을 새로 고치고 제공된 콜백을 호출하도록 지시합니다. 토큰이 캐시되고 준비되면 토큰 공급자는 백그라운드 스레드에서 콜백을 호출합니다. 이 콜백은 앱을 처음 로드할 때와 활성 상태로 복원될 때호출합니다. 활성 상태로 복원하는 방법에 대한 자세한 내용은 the section called “앱 비활성 이후 토큰 검색” 섹션을 참조하세요.

Android 또는 iOS 앱의 경우 요청된 토큰이 준비되었을 때 토큰 공급자가 호출할 작업을 WAFTokenResultCallback으로 설정할 수 있습니다. WAFTokenResultCallback의 구현에는 WAFToken, SdkError 파라미터를 사용해야 합니다. iOS 앱의 경우 인라인 함수를 번갈아 생성할 수 있습니다.

storeTokenInCookieStorage(WAFToken)

지정된 AWS WAF 토큰을 SDK의 쿠키 관리자에 WAFTokenProvider 저장하도록 지시합니다. 기본적으로 토큰은 처음 획득했을 때와 새로 고칠 때만 쿠키 저장소에 추가됩니다. 애플리케이션이 어떤 이유로든 공유 쿠키 저장소를 지우는 경우 SDK는 다음 새로고침 시까지 AWS WAF 토큰을 자동으로 다시 추가하지 않습니다.

WAFConfiguration

WAFTokenProvider의 구현을 위해 구성을 보관합니다. 이를 구현할 때는 웹 ACL의 통합 URL, 토큰에 사용할 도메인 이름, 토큰 공급자가 사용할 기본 이외의 모든 설정을 제공합니다.

다음 목록은 WAFConfiguration 객체에서 관리할 수 있는 구성 설정을 지정합니다.

applicationIntegrationUrl

애플리케이션 통합 URL. AWS WAF 콘솔이나 getWebACL API 호출을 통해 가져올 수 있습니다.

필수 항목 여부: 예

유형: 앱별 URL. iOS의 경우 iOS URL을 참조하세요. Android의 경우 java.net URL을 참조하세요.

backgroundRefreshEnabled

토큰 공급자가 백그라운드에서 토큰을 새로 고치도록 할지 여부를 나타냅니다. 이를 설정하면 토큰 공급자가 자동 토큰 새로 고침 활동을 제어하는 구성 설정에 따라 백그라운드에서 토큰을 새로 고칩니다.

필수 여부: 아니요

유형: Boolean

기본 값: TRUE

domainName

토큰에 사용할 도메인으로, 토큰 획득 및 쿠키 저장에 사용됩니다. 예: example.com 또는 aws.amazon.com. 일반적으로 이 도메인은 웹 요청을 보내는 웹 ACL과 연결된 리소스의 호

스트 도메인입니다. ACFP 관리형 규칙 그룹 AWSManagedRulesACFPRuleSet의 경우 이는 일반적으로 규칙 그룹 구성에 제공한 계정 생성 경로의 도메인과 일치하는 단일 도메인입니다. ATP 관리형 규칙 그룹 AWSManagedRulesATPRuleSet의 경우 이는 일반적으로 규칙 그룹 구성에 제공한 로그인 경로의 도메인과 일치하는 단일 도메인입니다.

공개 접미사는 허용되지 않습니다. 예를 들어 gov.au 또는 co.uk를 토큰 도메인으로 사용할 수 없습니다.

도메인은 보호된 호스트 도메인과 웹 ACL의 토큰 도메인 목록을 기반으로 AWS WAF 수락할 도메인이어야 합니다. 자세한 정보는 AWS WAF 웹 ACL 토큰 도메인 목록 구성을 참조하세요.

필수 항목 여부: 예

유형: String

maxErrorTokenRefreshDelayMsec

시도 실패 후 토큰 새로 고침을 반복할 때까지 대기하는 최대 시간 (밀리초) 입니다. 이 값은 토큰 검색이 실패하고 maxRetryCount회 재시도된 후에 사용됩니다.

필수 여부: 아니요

유형: Integer

기본값: 5000(5초)

허용된 최소값: 1(1밀리초)

허용된 최대값: 30000(30초)

maxRetryCount

토큰 요청 시 지수 백오프를 사용하여 수행할 최대 재시도 횟수입니다.

필수 여부: 아니요

유형: Integer

기본값: 백그라운드 새로 고침이 활성화된 경우, 5입니다. 그렇지 않을 경우 3입니다.

허용된 최소값: 0

허용되는 최대값: 10

setTokenCookie

SDK의 쿠키 관리자를 통해 요청에 토큰 쿠키를 추가할지 여부를 나타냅니다. 기본적으로 이렇게 설정하면 모든 요청에 토큰 쿠키가 추가됩니다. 쿠키 관리자는 tokenCookiePath에 지정된 경로 아래에 경로가 있는 모든 요청에 토큰 쿠키를 추가합니다.

필수 여부: 아니요

유형: Boolean

기본 값: TRUE

tokenCookiePath

setTokenCookie가 TRUE일 때 사용됩니다. SDK의 쿠키 관리자를 통해 토큰 쿠키를 추가하려는 최상위 경로를 나타냅니다. 관리자는 이 경로와 모든 하위 경로로 보내는 모든 요청에 토큰 쿠키를 추가합니다.

예를 들어, 이 값을 /web/login로 설정하면 관리자는 받는 모든 항목 /web/login 및 하위 경로(예: /web/login/help)로 전송된 모든 것에 대한 토큰 쿠키를 포함합니다. /, /web 또는 /web/order와 같은 다른 경로로 전송된 요청에 대한 토큰은 포함하지 않습니다.

필수 여부: 아니요

유형: String

기본 값: /

tokenRefreshDelaySec

백그라운드 새로 고침에 사용됩니다. 백그라운드 토큰 새로 고침 최대 시간 간격(초).

필수 여부: 아니요

유형: Integer

기본 값: 88

허용된 최소값: 88

허용된 최대값: 300(5분)

AWS WAF 모바일 SDK 작동 방식

모바일 SDK는 토큰 검색 및 사용에 사용할 수 있는 구성 가능한 토큰 공급자를 제공합니다. 토큰 공급자는 허용한 요청이 합법적인 고객의 요청인지 확인합니다. 보호 대상 AWS 리소스에 요청을 보낼 때는 토큰을 쿠키에 포함시켜 요청의 유효성을 검사합니다. AWS WAF토큰 쿠키는 수동으로 처리하거나 토큰 공급자에게 대신 처리하도록 할 수 있습니다.

이 섹션에서는 모바일 SDK에 포함된 클래스, 속성 및 메서드 간의 상호 작용을 다룹니다. SDK 사양에 대한 내용은 AWS WAF 모바일 SDK 사양 섹션을 참조하세요.

토큰 검색 및 캐싱

모바일 앱에서 토큰 공급자 인스턴스를 생성할 때 토큰 및 토큰 검색을 관리하는 방법을 구성합니다. 앱의 웹 요청에 사용할 수 있도록 유효하고 만료되지 않은 토큰을 유지하는 방법을 선택하는 것이 가장 좋습니다.

- 백그라운드 새로 고침이 활성화됨 – 기본값입니다. 토큰 공급자는 백그라운드에서 토큰을 자동으로 새로 고쳐 캐시합니다. 백그라운드 새로 고침이 활성화된 상태에서 `getToken()`을 호출하면 캐시된 토큰이 검색됩니다.

  토큰 공급자는 구성 가능한 간격으로 토큰 새로 고침을 수행하므로 애플리케이션이 활성 상태인 동안 만료되지 않은 토큰을 캐시에서 항상 사용할 수 있습니다. 애플리케이션이 비활성 상태인 동안에는 백그라운드 새로 고침이 일시 중지됩니다. 이에 대한 자세한 내용은 앱 비활성 이후 토큰 검색 섹션을 참조하세요.
- 백그라운드 새로 고침 비활성화 - 백그라운드 토큰 새로 고침을 비활성화하고 나서, 온디맨드로만 토큰을 검색할 수 있습니다. 온디멘드 검색 토큰은 캐시되지 않으며 원하는 경우 두 개 이상을 검색할 수 있습니다. 각 토큰은 검색하는 다른 토큰과 독립적이며 각 토큰에는 만료를 계산하는 데 사용되는 고유한 타임스탬프가 있습니다.

  백그라운드 새로 고침이 비활성화된 경우 다음과 같은 토큰 검색 옵션을 선택할 수 있습니다.

  - **`getToken()`**— 백그라운드 새로 고침이 비활성화된 `getToken()` 상태에서 호출하면 호출은 새 토큰을 동기적으로 검색합니다. AWS WAF이 호출은 메인 스레드에서 호출할 경우 앱 응답성에 영향을 줄 수 있는 잠재적으로 차단된 호출입니다.
  - **`onTokenReady(WAFTokenResultCallback)`** - 이 호출은 새 토큰을 비동기적으로 검색한 다음 토큰이 준비되면 백그라운드 스레드에서 제공된 결과 콜백을 호출합니다.

토큰 공급자가 실패한 토큰 검색을 재시도하는 방법

토큰 공급자는 검색에 실패하면 자동으로 토큰 검색을 다시 시도합니다. 재시도는 처음에 지수 백오프를 사용하여 수행되며 시작 재시도 대기 시간은 100ms입니다. 지수 재시도에 대한 자세한 내용은 AWS의 오류 재시도 및 지수 백오프 섹션을 참조하세요.

재시도 횟수가 구성된 `maxRetryCount`회에 도달하면 토큰 공급자는 토큰 검색 유형에 따라 시도를 중단하거나 `maxErrorTokenRefreshDelayMsec`밀리초마다 시도하도록 전환합니다.

- **`onTokenReady()`** - 토큰 공급자는 각 시도 사이 대기(`maxErrorTokenRefreshDelayMsec`밀리초)로 전환하고 토큰 검색을 계속 시도합니다.
- 백그라운드 새로 고침 - 토큰 공급자는 각 시도 사이 대기(`maxErrorTokenRefreshDelayMsec`밀리초)로 전환하고 토큰 검색을 계속 시도합니다.
- 백그라운드 새로 고침이 비활성화되었을 때 온디맨드 **`getToken()`** 호출 - 토큰 공급자가 토큰 검색 시도를 중단하고 이전 토큰 값을 반환하거나, 이전 토큰이 없는 경우 null 값을 반환합니다.

앱 비활성 이후 토큰 검색

앱이 해당 앱 유형에 맞게 활성화된 것으로 간주되는 경우에만 백그라운드 새로 고침이 수행됩니다.

- iOS - 앱이 포그라운드에 있을 때 백그라운드 새로 고침이 수행됩니다.
- Android - 앱이 포그라운드 또는 백그라운드에 있는지 여부와 관계없이 앱이 닫히지 않은 경우 백그라운드 새로 고침이 수행됩니다.

앱이 구성된 `tokenRefreshDelaySec`초보다 더 긴 시간 동안 백그라운드 새로 고침을 지원하지 않는 상태로 유지되는 경우 토큰 공급자는 백그라운드 새로 고침을 일시 중지합니다. 예를 들어 iOS 앱의 경우 `tokenRefreshDelaySec`는 300이고 앱이 종료되거나 300초 넘게 백그라운드에 있으면 토큰 공급자는 토큰 새로 고침을 중단합니다. 앱이 활성 상태로 돌아오면 토큰 공급자는 백그라운드 새로 고침을 자동으로 다시 시작합니다.

앱이 다시 활성 상태로 복원되면 토큰 공급자가 새 토큰을 검색하고 캐시했을 때 알림을 받을 수 있도록 `onTokenReady()`을 호출합니다. 캐시에 현재 유효한 토큰이 아직 포함되어 있지 않을 수 있으므로 무작정 `getToken()`을 호출해서는 안 됩니다.

AWS WAF 모바일 SDK용 코드 작성

이 섹션에서는 모바일 SDK를 사용한 코드 예제를 제공합니다.

토큰 공급자 초기화 및 토큰 가져오기

구성 객체를 사용하여 토큰 공급자 인스턴스를 시작합니다. 그러고 나면 사용 가능한 작업을 사용하여 토큰을 검색할 수 있습니다. 다음은 필요한 코드의 기본 구성 요소입니다.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
let tokenProvider = WAFTokenProvider(configuration)

//onTokenReady can be add as an observer for
 UIApplication.willEnterForegroundNotification
self.tokenProvider.onTokenReady() { token, error in
 if let token = token {
 //token available
 }

 if let error = error {
 //error occurred after exhausting all retries
 }
}

//getToken()
let token = tokenProvider.getToken()
```

Android

자바 예제:

```
String applicationIntegrationURL = "Web ACL integration URL";
//Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);

// implement a token result callback
```

```
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
WAFToken token = tokenProvider.getToken();
```

Kotlin 예제:

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "Web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
   .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
  wafTokenProvider.onTokenReady {
```

```
    wafToken, sdkError ->
   run {
    println("WAF Token:" + wafToken.value)
   }
  }
}
```

SDK가 HTTP 요청에서 토큰 쿠키를 제공하도록 허용

`setTokenCookie`가 `TRUE`이면 토큰 공급자는 `tokenCookiePath`에 지정된 경로 아래의 모든 위치에 대한 웹 요청에 토큰 쿠키를 포함합니다. 기본적으로 `setTokenCookie`는 `TRUE`이고 `tokenCookiePath`은 `/`입니다.

토큰 쿠키 경로를 지정하여 토큰 쿠키가 포함된 요청의 범위를 좁힐 수 있습니다(예: `/web/login`). 이렇게 하는 경우 AWS WAF 규칙이 다른 경로로 보내는 요청의 토큰을 검사하지 않는지 확인하세요. `AWSManagedRulesACFPRuleSet` 규칙 그룹을 사용할 때 계정 등록 및 생성 경로를 구성하면 규칙 그룹이 해당 경로로 전송되는 요청의 토큰을 확인합니다. 자세한 정보는 ACFP 관리형 규칙 그룹을 웹 ACL에 추가을 참조하세요. 마찬가지로 `AWSManagedRulesATPRuleSet` 규칙 그룹을 사용할 때 로그인 경로를 구성하면 규칙 그룹이 해당 경로로 전송되는 요청의 토큰을 확인합니다. 자세한 정보는 ATP 관리형 규칙 그룹을 새 웹 ACL에 추가을 참조하세요.

iOS

`setTokenCookie`TRUE인 경우 토큰 제공자는 AWS WAF 토큰을 `HTTPCookieStorage.shared` a에 저장하고 사용자가 지정한 도메인에 대한 요청에 자동으로 쿠키를 포함합니다`WAFConfiguration`.

```
let request = URLRequest(url: URL(string: domainEndpointUrl)!)
//The token cookie is set automatically as cookie header
let task = URLSession.shared.dataTask(with: request) { data, urlResponse, error  in
}.resume()
```

Android

`setTokenCookie`TRUE인 경우 토큰 제공자는 애플리케이션 전체에서 공유되는 `CookieHandler` 인스턴스에 AWS WAF 토큰을 저장합니다. 토큰 공급자는 `WAFConfiguration`에 지정한 도메인에 대한 요청에 쿠키를 자동으로 포함합니다.

Java 예제:

```
URL url = new URL("Domain name");
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Kotlin 예제:

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

CookieHandler 기본 인스턴스를 이미 초기화한 경우 토큰 공급자는 이를 사용하여 쿠키를 관리합니다. 그렇지 않은 경우 토큰 제공자는 토큰으로 새 CookieManager 인스턴스를 초기화한 다음 이 새 인스턴스를 에서 CookieHandler 기본 인스턴스로 설정합니다. AWS WAF CookiePolicy.ACCEPT_ORIGINAL_SERVER

다음 코드는 앱에서 쿠키 관리자 및 쿠키 핸들러를 사용할 수 없을 때 SDK가 쿠키 관리자와 쿠키 핸들러를 초기화하는 방법을 보여줍니다.

Java 예제:

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Kotlin 예제:

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

HTTP 요청에서 토큰 쿠키를 수동으로 제공

`setTokenCookie`를 `FALSE`로 설정하면 보호된 엔드포인트에 대한 요청에 토큰 쿠키를 수동으로 쿠키 HTTP 요청 헤더로서 제공해야 합니다. 다음 코드에서는 이를 수행하는 방법을 보여줍니다.

iOS

```
var request = URLRequest(url: wafProtectedEndpoint)
request.setValue("aws-waf-token=token from token provider", forHTTPHeaderField:
 "Cookie")
request.httpShouldHandleCookies = true
URLSession.shared.dataTask(with: request) { data, response, error in }
```

Android

자바 예제:

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Kotlin 예제:

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHA그리고 Challenge 안에 AWS WAF

규칙의 검사 기준과 일치하는 웹 요청에 대해 CAPTCHA 또는 Challenge 조치를 실행하도록 AWS WAF 규칙을 구성할 수 있습니다. 또한 CAPTCHA 퍼즐과 브라우저 챌린지를 로컬에서 실행하도록 JavaScript 클라이언트 애플리케이션을 프로그래밍할 수 있습니다.

CAPTCHA 퍼즐과 사일런트 챌린지는 브라우저가 HTTPS 엔드포인트에 액세스할 때만 실행할 수 있습니다. 토큰을 획득하려면 브라우저 클라이언트가 안전한 환경에서 실행되고 있어야 합니다.

- CAPTCHA— 최종 사용자가 CAPTCHA 퍼즐을 풀어 사람이 요청을 보내고 있다는 것을 증명해야 합니다. CAPTCHA 퍼즐은 사람이 비교적 쉽고 빠르게 완료할 수 있는 반면, 컴퓨터는 성공적으로 완료하거나 무작위 방식을 통해 유의미한 성공률로 완료하기가 어렵습니다.

  웹 ACL 규칙에서 CAPTCHA는 특정 Block 작업으로 인해 합법적인 요청이 너무 많이 중단될 때 일반적으로 사용되지만 모든 트래픽을 허용하면 봇과 같은 원치 않는 요청이 용납할 수 없을 정도로 많아질 때 사용됩니다. 규칙 작업 동작에 대한 자세한 내용은 을 참조하십시오. AWS WAFCAPTCHA 및 Challenge 규칙 작업의 작동 방식

  클라이언트 애플리케이션 통합 API에서 CAPTCHA 퍼즐 구현을 프로그래밍할 수도 있습니다. 이렇게 하면 클라이언트 애플리케이션에서 퍼즐의 동작과 배치를 사용자 정의할 수 있습니다. 자세한 정보는 AWS WAF 클라이언트 애플리케이션 통합을 참조하세요.

- Challenge— 클라이언트 세션에서 봇이 아닌 브라우저인지 확인하도록 요구하는 자동 챌린지를 실행합니다. 이 확인은 최종 사용자의 개입 없이 백그라운드에서 실행됩니다. 이 옵션은 CAPTCHA 퍼즐로 최종 사용자 환경에 부정적인 영향을 주지 않으면서 유효하지 않다고 의심되는 클라이언트를 확인할 수 있는 좋은 옵션입니다. 규칙 동작 동작에 대한 자세한 내용은 을 참조하십시오AWS WAFCAPTCHA 및 Challenge 규칙 작업의 작동 방식.

  Challenge 규칙 작업은 AWS WAF 클라이언트 애플리케이션 통합에서 설명한 클라이언트 지능형 위협 통합 API에서 실행되는 챌린지와 유사합니다.

> **Note**
>
> 규칙 중 하나에서 또는 규칙 그룹 내 규칙 작업 재정의로서 CAPTCHA 또는 Challenge 규칙 작업을 사용하는 경우 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

모든 규칙 작업 옵션에 대한 설명은 을 참조하십시오규칙 작업.

주제

- AWS WAF 캡차 퍼즐
- AWS WAFCAPTCHA 및 Challenge 규칙 작업의 작동 방식
- CAPTCHA 및 Challenge 작업 사용 모범 사례

AWS WAF 캡차 퍼즐

AWS WAF 사용자가 자신이 인간임을 확인할 수 있도록 하는 표준 CAPTCHA 기능을 제공합니다. CAPTCHA는 완전 자동화된 컴퓨터와 사람 판별 공개 튜링 테스트(Completely Automated Public Turing test to tell Computers and Humans Apart)의 약자입니다. CAPTCHA 퍼즐은 사람이 요청을 보내고 있는지 확인하고 웹 스크레이핑, 보안 인증 정보 스터핑 및 스팸과 같은 활동을 방지하도록 고안되었습니다. CAPTCHA 퍼즐로는 원치 않는 요청을 모두 제거할 수 없습니다. 많은 퍼즐이 기계 학습과 인공 지능을 사용하여 해결되었습니다. CAPTCHA를 우회하기 위해 일부 조직에서는 사람의 개입을 통해 자동화 기술을 보완하기도 합니다. 그럼에도 불구하고 CAPTCHA는 덜 정교한 봇 트래픽을 방지하고 대규모 운영에 필요한 리소스를 늘리는 데 계속 유용한 도구로 사용되고 있습니다.

AWS WAF CAPTCHA 퍼즐을 무작위로 생성하여 회전을 통해 사용자에게 고유한 도전 과제를 제시할 수 있도록 합니다. AWS WAF 정기적으로 새로운 유형과 스타일의 퍼즐을 추가하여 자동화 기법에 효과적으로 대응하고 있습니다. 퍼즐 외에도 AWS WAF CAPTCHA 스크립트는 클라이언트에 대한 데이터를 수집하여 사람이 작업을 완료했는지 확인하고 리플레이 공격을 방지합니다.

각 CAPTCHA 퍼즐에는 최종 사용자가 새 퍼즐을 요청하고, 시청각 퍼즐을 전환하고, 추가 지침에 액세스하고, 퍼즐 솔루션을 제출할 수 있는 표준 컨트롤 집합이 포함되어 있습니다. 모든 퍼즐에는 스크린 리더, 키보드 컨트롤 및 색상 대비 지원이 포함됩니다.

AWS WAF CAPTCHA 퍼즐은 웹 콘텐츠 접근성 지침 (WCAG) 의 요구 사항을 충족합니다. 자세한 내용은 World Wide Web Consortium 웹 사이트의 웹 콘텐츠 접근성 지침 (WCAG) 개요를 참조하세요.

주제

- 캡차 퍼즐 언어 지원
- 캡차 퍼즐 예제

캡차 퍼즐 언어 지원

CAPTCHA 퍼즐은 클라이언트 브라우저 언어로 작성된 지침으로 시작되며, 브라우저 언어가 지원되지 않는 경우 영어로 작성된 지침으로 시작됩니다. 이 퍼즐은 드롭다운 메뉴를 통해 대체 언어 옵션을 제공합니다.

사용자는 페이지 하단에 있는 헤드폰 아이콘을 선택하여 오디오 지침으로 전환할 수 있습니다. 퍼즐의 오디오 버전은 사용자가 텍스트 상자에 입력해야 하는 텍스트에 대한 음성 안내를 제공하며 배경 소음과 겹쳐져 있습니다.

다음 표에는 CAPTCHA 퍼즐의 서면 지침에 대해 선택할 수 있는 언어와 각 선택 항목에 대한 오디오 지원이 나와 있습니다.

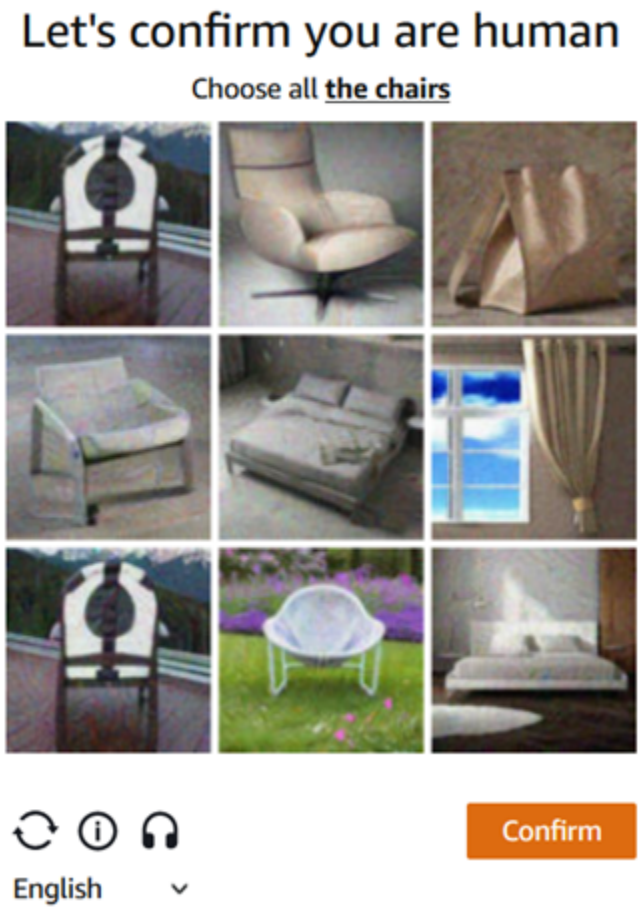
AWS WAF CAPTCHA 퍼즐 지원 언어

서면 지침, 지원	로케일 코드	오디오 지침 지원
아랍어	AR-SA	아랍어
중국어 간체	zh-CN	영어 오디오
네덜란드어	nl-NL	네덜란드어
영어	en-US	영어
프랑스어	fr-FR	프랑스어
독일어	de-DE	독일어
이탈리아어	it-IT	이탈리아어
일본어	ja-JP	영어 오디오
브라질 (포르투갈어)	pt-BR	브라질 포르투갈어
스페인어	es-ES	스페인어
터키어	tr-TR	터키어

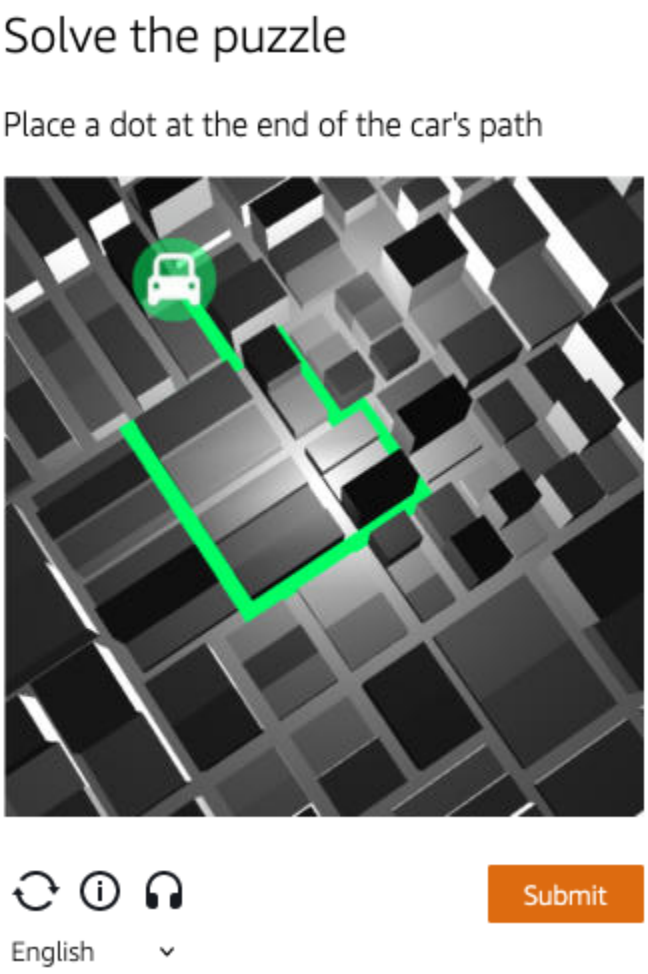
캡차 퍼즐 예제

일반적인 시각적 CAPTCHA 퍼즐에서는 사용자가 하나 이상의 이미지를 이해하고 상호작용할 수 있다는 것을 보여주기 위한 상호작용이 필요합니다.

다음 스크린샷은 그림 격자 퍼즐의 예를 보여줍니다. 이 퍼즐을 풀려면 그리드에서 특정 유형의 개체가 포함된 모든 그림을 선택해야 합니다.

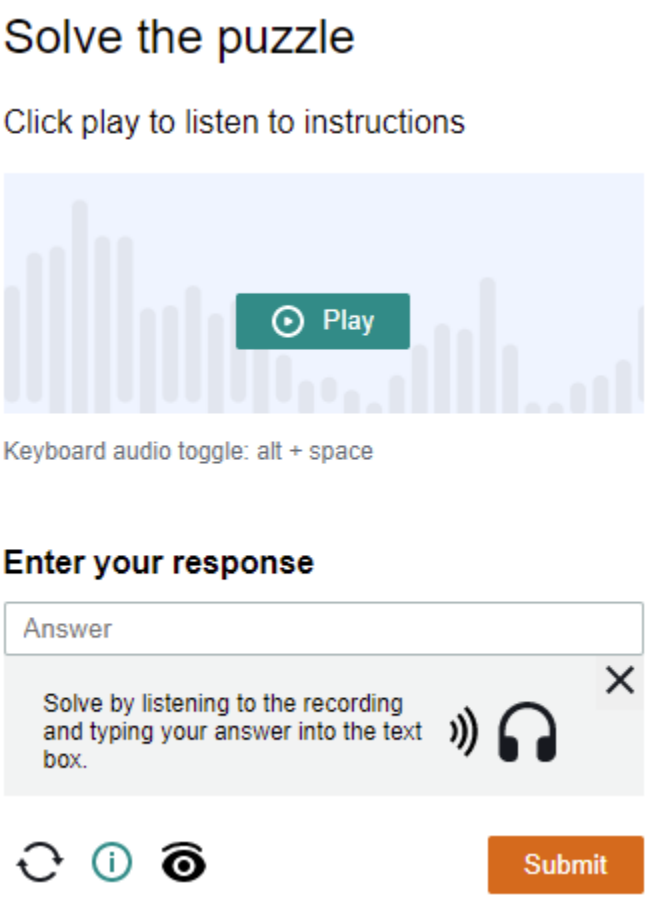


다음 스크린샷은 도면에서 자동차 경로의 끝점을 식별해야 하는 예제 퍼즐을 보여줍니다.



오디오 퍼즐은 사용자가 텍스트 상자에 입력해야 하는 텍스트에 대한 음성 안내와 함께 배경 잡음을 제공합니다.

다음 스크린샷은 오디오 퍼즐 선택 화면을 보여줍니다.



AWS WAFCAPTCHA 및 Challenge 규칙 작업의 작동 방식

AWS WAF CAPTCHA표준 규칙 동작이므로 비교적 쉽게 구현할 수 있습니다. Challenge 둘 중 하나를 사용하려면 검사할 요청을 식별하는 규칙에 대한 검사 기준을 만든 다음 두 규칙 작업 중 하나를 지정합니다. 각 작업의 옵션에 대한 일반적인 정보는 규칙 작업 섹션을 참조하세요.

서버 측에서 사일런트 챌린지와 CAPTCHA 퍼즐을 구현하는 것 외에도 사용자, JavaScript iOS 및 Android 클라이언트 애플리케이션에 사일런트 챌린지를 통합하고 클라이언트에서 CAPTCHA 퍼즐을 렌더링할 수 있습니다. JavaScript 이러한 통합을 통해 최종 사용자에게 더 나은 성능과 CAPTCHA 퍼즐 경험을 제공할 수 있으므로, 최종 사용자는 규칙 조치 및 지능형 위협 완화 규칙 그룹 사용과 관련된 비용을 줄일 수 있습니다. 이러한 옵션에 대한 자세한 내용은 AWS WAF 클라이언트 애플리케이션 통합 섹션을 참조하세요. 요금 정보는 AWS WAF 요금을 참조하세요.

주제

- CAPTCHA 및 Challenge 작업 동작
- 로그 및 지표의 CAPTCHA 및 Challenge 작업

CAPTCHA 및 Challenge 작업 동작

웹 요청이 규칙 CAPTCHA 또는 Challenge 조치의 검사 기준과 일치하는 경우 토큰 상태 및 면역 시간 구성에 따라 요청을 처리하는 방법을 AWS WAF 결정합니다. AWS WAF 또한 요청이 CAPTCHA 퍼즐 또는 챌린지 스크립트 전면 광고를 처리할 수 있는지 여부도 고려합니다. 스크립트는 HTML 콘텐츠로 처리되도록 설계되었으며 HTML 콘텐츠를 필요로 하는 클라이언트만 올바르게 처리할 수 있습니다.

> **Note**
>
> 규칙 중 하나에서 또는 규칙 그룹 내 규칙 작업 재정의로서 CAPTCHA 또는 Challenge 규칙 작업을 사용하는 경우 추가 요금이 부과됩니다. 자세한 내용은 AWS WAF 요금을 참조하십시오.

작업에서 웹 요청을 처리하는 방법

AWS WAF CAPTCHAor Challenge 액션을 다음과 같이 웹 요청에 적용합니다.

- 유효한 토큰 — Count 액션과 유사하게 AWS WAF 처리합니다. AWS WAF 규칙 작업에 대해 구성한 모든 레이블과 요청 사용자 지정을 적용한 다음 웹 ACL의 나머지 규칙을 사용하여 요청을 계속 평가합니다.
- 누락되거나 유효하지 않거나 만료된 토큰 — 요청에 대한 웹 ACL 평가를 AWS WAF 중단하고 요청이 의도한 목적지로 전송되지 않도록 차단합니다.

  AWS WAF 규칙 작업 유형에 따라 응답을 생성하여 클라이언트에 다시 보냅니다.

  - Challenge – AWS WAF 에서는 응답에 다음 항목을 포함합니다.
    - `challenge` 값을 갖는 헤더 `x-amzn-waf-action`입니다.

      > **Note**
      >
      > 클라이언트 브라우저에서 실행되는 JavaScript 애플리케이션에서는 이 헤더를 사용할 수 없습니다. 자세한 정보는 다음 섹션을 참조하세요.

    - HTTP 상태 코드 `202 Request Accepted`.
    - 요청에 값이 인 `Accept` 헤더가 포함된 경우 응답에는 `text/html` 챌린지 스크립트가 포함된 JavaScript 페이지 전면 광고가 포함됩니다.
  - CAPTCHA— AWS WAF 응답에 다음을 포함합니다.
    - `captcha` 값을 갖는 헤더 `x-amzn-waf-action`입니다.

> **Note**
>
> 클라이언트 브라우저에서 실행되는 JavaScript 애플리케이션에서는 이 헤더를 사용할 수 없습니다. 자세한 정보는 다음 섹션을 참조하세요.

- HTTP 상태 코드 `405 Method Not Allowed`.
- 요청에 값이 인 `Accept` 헤더가 포함된 경우 응답에는 `text/html` CAPTCHA 스크립트가 포함된 JavaScript 페이지 전면 광고가 포함됩니다.

웹 ACL 또는 규칙 수준에서 토큰 만료 시기를 구성하려면 타임스탬프 만료: AWS WAF 토큰 면역 시간 섹션을 참조하세요.

클라이언트 브라우저에서 실행되는 JavaScript 애플리케이션에서는 헤더를 사용할 수 없습니다.

CAPTCHA 또는 챌린지 AWS WAF 응답으로 클라이언트 요청에 응답할 때는 원본 간 리소스 공유 (CORS) 헤더가 포함되지 않습니다. CORS 헤더는 애플리케이션에서 사용할 수 있는 도메인, HTTP 메서드, HTTP 헤더를 클라이언트 웹 브라우저에 알려주는 액세스 제어 헤더 세트입니다. JavaScript CORS 헤더가 없으면 클라이언트 브라우저에서 실행되는 JavaScript 애플리케이션에 HTTP `x-amzn-waf-action` 헤더에 대한 액세스 권한이 부여되지 않으므로 및 응답에 제공된 헤더를 읽을 수 없습니다. CAPTCHA Challenge

챌린지와 CAPTCHA 중간 광고의 기능

챌린지 중간 광고가 실행되면 클라이언트가 성공적으로 응답한 후, 아직 토큰이 없는 경우 중간 광고에서 토큰을 초기화합니다. 그런 다음 챌린지 풀기 타임스탬프로 토큰을 업데이트합니다.

CAPTCHA 중간 광고가 실행될 때 클라이언트에 아직 토큰이 없는 경우 CAPTCHA 전면 광고는 먼저 챌린지 스크립트를 호출하여 브라우저에서 챌린지를 실행하고 토큰을 초기화합니다. 그러면 중간 광고는 CAPTCHA 퍼즐을 실행합니다. 최종 사용자가 퍼즐을 성공적으로 완료하면 중간 광고는 CAPTCHA 풀기 타임스탬프로 토큰을 업데이트합니다.

어느 경우든 클라이언트가 성공적으로 응답하고 스크립트가 토큰을 업데이트하면 스크립트는 업데이트된 토큰을 사용하여 원래 웹 요청을 다시 제출합니다.

토큰 처리 방법을 AWS WAF 구성할 수 있습니다. 자세한 내용은 AWS WAF 웹 요청 토큰 섹션을 참조하세요.

로그 및 지표의 CAPTCHA 및 Challenge 작업

CAPTCHA 및 Challenge 작업은 비 종료형(예: Count)일 수도 있고 종료형일 수도 있습니다(예: Block). 결과는 작업 유형에 대해 만료되지 않은 타임스탬프가 있는 유효한 토큰이 요청에 있는지 여부에 따라 달라집니다.

- 유효한 토큰 - 작업이 유효한 토큰을 찾고 요청을 차단하지 않는 경우 다음과 같이 지표와 로그를 AWS WAF 캡처합니다.
  - `CaptchaRequests` 및 `RequestsWithValidCaptchaToken` 또는 `ChallengeRequests` 및 `RequestsWithValidChallengeToken`에 대한 지표를 늘립니다.
  - 일치 항목을 CAPTCHA 또는 Challenge 작업이 있는 `nonTerminatingMatchingRules` 항목으로 로그에 기록합니다. 다음 목록은 CAPTCHA 작업이 있는 이 유형의 일치 항목에 대한 로그 섹션을 보여줍니다.

```
  "nonTerminatingMatchingRules": [
  {
    "ruleId": "captcha-rule",
    "action": "CAPTCHA",
    "ruleMatchDetails": [],
    "captchaResponse": {
      "responseCode": 0,
      "solveTimestamp": 1632420429
    }
  }
]
```

- 누락, 무효 또는 만료된 토큰 - 작업이 누락되거나 유효하지 않은 토큰으로 인해 요청을 차단하면 다음과 같이 지표와 로그를 AWS WAF 캡처합니다.
  - 또는 `CaptchaRequests` 또는 `ChallengeRequests`에 대한 지표를 늘립니다.
  - 일치 항목을 HTTP `405` 상태 코드가 있는 `CaptchaResponse` 항목 또는 HTTP `202` 상태 코드가 있는 `ChallengeResponse` 항목으로 로그에 기록합니다. 로그는 요청에 토큰이 누락되었는지 아니면 타임스탬프가 만료되었는지 여부를 나타냅니다. 또한 로그에는 CAPTCHA 전면 광고 페이지를 클라이언트에 AWS WAF 보냈는지 아니면 클라이언트 브라우저에 자동 챌린지를 보냈는지도 표시됩니다. 다음 목록은 CAPTCHA 작업이 있는 이 유형의 일치 항목에 대한 로그 섹션을 보여줍니다.

```
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
```

```
    "terminatingRuleMatchDetails": [],
    ...
    "responseCodeSent": 405,
    ...
    "captchaResponse": {
      "responseCode": 405,
      "solveTimestamp": 0,
      "failureReason": "TOKEN_MISSING"
    }
```

로그에 대한 자세한 내용은 을 AWS WAF 참조하십시오. AWS WAF 웹 ACL 트래픽 로깅

AWS WAF 지표에 대한 자세한 내용은 을 참조하십시오AWS WAF 지표 및 차원.

규칙 작업 옵션에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.

CAPTCHA 및 Challenge 작업 사용 모범 사례

이 섹션의 지침에 따라 AWS WAF CAPTCHA 또는 챌린지를 계획하고 구현하십시오.

CAPTCHA 및 챌린지 구현 계획

웹사이트 사용량, 보호하려는 데이터의 민감도 및 요청 유형에 따라 CAPTCHA 퍼즐이나 자동 챌린지를 배치할 위치를 결정합니다. 필요에 따라 퍼즐을 제시하도록 CAPTCHA를 적용할 요청을 선택하되, 유용하지 않고 사용자 경험을 저하시킬 수 있는 경우에는 제시하지 마십시오. 이 Challenge 작업을 사용하면 최종 사용자에게 미치는 영향은 적지만 JavaScript 활성화된 브라우저에서 요청이 오는지 확인하는 데 도움이 되는 자동 챌린지를 실행할 수 있습니다.

CAPTCHA 퍼즐과 사일런트 챌린지는 브라우저가 HTTPS 엔드포인트에 액세스할 때만 실행할 수 있습니다. 토큰을 획득하려면 브라우저 클라이언트가 안전한 환경에서 실행되고 있어야 합니다.

클라이언트에서 CAPTCHA 퍼즐과 자동 챌린지를 실행할 위치 결정

CAPTCHA의 영향을 받지 않도록 할 요청(예: CSS 또는 이미지 요청)을 식별합니다. 필요한 경우에만 CAPTCHA를 사용하십시오. 예를 들어 로그인 시 CAPTCHA 검사를 실시할 계획이고 사용자가 항상 로그인 화면에서 다른 화면으로 직접 이동하는 경우 두 번째 화면에서 CAPTCHA 검사 요구는 아마도 필요하지 않을 것이며 최종 사용자 경험을 저하시킬 것입니다.

요청에 대한 Challenge 응답으로 CAPTCHA 퍼즐과 사일런트 AWS WAF 챌린지만 전송하도록 설정하고 CAPTCHA 사용하십시오. `GET text/html` `POST` 요청, 교차 오리진 리소스 공유(CORS) 프리플라

이트 OPTIONS 요청 또는 기타 비 GET 요청 유형에 대한 응답으로는 퍼즐이나 챌린지를 실행할 수 없습니다. 다른 요청 유형의 브라우저 동작은 다를 수 있으며 중간 광고를 제대로 처리하지 못할 수 있습니다.

클라이언트가 HTML을 허용하지만 여전히 CAPTCHA 또는 챌린지 중간 광고를 처리하지 못할 수 있습니다. 예를 들어 작은 iFrame을 포함하는 웹 페이지의 위젯은 HTML은 허용하지만 CAPTCHA를 표시하거나 처리하지 못할 수 있습니다. HTML을 허용하지 않는 요청과 마찬가지로 이러한 유형의 요청에는 규칙 작업을 배치하지 마십시오.

CAPTCHA또는 Challenge 를 사용하여 이전 토큰 획득을 확인합니다.

합법적인 사용자가 항상 토큰을 보유해야 하는 위치에서는 유효한 토큰의 존재 여부를 확인하는 용도로만 규칙 조치를 사용할 수 있습니다. 이러한 상황에서는 요청이 전면 광고를 처리할 수 있는지 여부는 중요하지 않습니다.

예를 들어 JavaScript 클라이언트 애플리케이션 CAPTCHA API를 구현하고 보호된 엔드포인트에 첫 번째 요청을 보내기 직전에 클라이언트에서 CAPTCHA 퍼즐을 실행하는 경우 첫 번째 요청에는 항상 챌린지와 CAPTCHA 모두에 유효한 토큰이 포함되어야 합니다. 클라이언트 애플리케이션 통합에 대한 JavaScript 자세한 내용은 을 참조하십시오. AWS WAF JavaScript 통합

이 상황에서는 웹 ACL에서 이 첫 번째 호출과 일치하는 규칙을 추가하고 Challenge 또는 CAPTCHA 규칙 작업을 사용하여 해당 규칙을 구성할 수 있습니다. 규칙이 합법적인 최종 사용자와 브라우저에 대해 일치하는 경우 이 작업은 유효한 토큰을 찾게 되므로 요청을 차단하거나 이에 대한 응답으로 챌린지 또는 CAPTCHA 퍼즐을 보내지 않습니다. 규칙 작업 작동 방식에 대한 자세한 내용은 CAPTCHA 및 Challenge 작업 동작 섹션을 참조하세요.

CAPTCHA 및 Challenge를 사용하여 민감한 비 HTML 데이터 보호

다음 접근 방식을 통해 API와 같은 민감한 비 HTML 데이터에 CAPTCHA 및 Challenge 보호 기능을 사용할 수 있습니다.

1. 민감한 비 HTML 데이터에 대한 요청과 매우 근접한 곳에서 실행되는 요청과 HTML 응답을 받는 요청을 식별합니다.
2. HTML 요청과 일치하고 민감한 데이터에 대한 요청과 일치하는 CAPTCHA 또는 Challenge 규칙을 작성합니다.
3. 일반적인 사용자 상호 작용의 경우 클라이언트가 HTML 요청에서 획득한 토큰을 민감한 데이터에 대한 요청에서 사용할 수 있고 만료되지 않도록 하려면 CAPTCHA 및 Challenge 면제 시간 설정을 조정합니다. 조정 정보는 타임스탬프 만료: AWS WAF 토큰 면역 시간 섹션을 참조하세요.

민감한 데이터에 대한 요청이 CAPTCHA 또는 Challenge 규칙과 일치하더라도 클라이언트가 이전 퍼즐 또는 챌린지의 유효한 토큰을 여전히 가지고 있다면 해당 요청은 차단되지 않습니다. 토큰을 사용할 수 없거나 타임스탬프가 만료되면 민감한 데이터에 대한 액세스 요청이 실패합니다. 규칙 작업 작동 방식에 대한 자세한 내용은 CAPTCHA 및 Challenge 작업 동작 섹션을 참조하세요.

CAPTCHA 및 Challenge를 사용하여 기존 규칙을 조정합니다.

기존 규칙을 검토하여 이들 규칙을 변경할지 아니면 이들 규칙에 추가할지 알아봅니다. 고려해야 할 몇 가지 일반 시나리오는 다음과 같습니다.

- 트래픽을 차단하는 속도 기반 규칙이 있지만 합법적인 사용자를 차단하지 않기 위해 속도 제한을 비교적 높게 유지하는 경우 차단 규칙 다음에 두 번째 속도 기반 규칙을 추가하는 것을 고려해 보십시오. 두 번째 규칙에는 차단 규칙보다 낮은 제한을 지정하고 규칙 작업은 CAPTCHA 또는 Challenge로 설정합니다. 차단 규칙은 너무 높은 속도로 들어오는 요청을 여전히 차단하며, 새 규칙은 더 낮은 속도의 대부분의 자동화된 트래픽을 차단합니다. 속도 기반 규칙에 대한 자세한 내용은 비율 기반 규칙 문 섹션을 참조하세요.
- 요청을 차단하는 관리형 규칙 그룹이 있는 경우 일부 또는 모든 규칙의 동작을 Block에서 CAPTCHA 또는 Challenge로 전환할 있습니다. 이렇게 하려면 관리형 규칙 그룹 구성에서 규칙 작업 설정을 재정의합니다. 규칙 작업 재정의에 대한 자세한 내용은 규칙 그룹 규칙 작업 재정의 섹션을 참조하세요.

배포하기 전에 CAPTCHA 및 챌린지 테스트

모든 새 기능에 대해서는 the section called “보호 기능 테스트 및 튜닝”의 지침을 따르십시오.

테스트 중에 토큰 타임스탬프 만료 요구 사항을 검토하고 웹 ACL 및 규칙 수준 면제 시간 구성을 설정하여 웹 사이트에 대한 액세스 제어와 우수한 고객 경험 사이에서 적절한 균형을 이룰 수 있습니다. 자세한 내용은 타임스탬프 만료: AWS WAF 토큰 면역 시간 섹션을 참조하세요.

AWS WAF 웹 ACL 트래픽 로깅

로깅을 활성화하여 웹 ACL에서 분석한 트래픽에 대한 자세한 정보를 기록할 수 있습니다. 로깅되는 정보에는 AWS 리소스로부터 웹 요청을 AWS WAF 받은 시간, 요청에 대한 세부 정보, 요청과 일치하는 규칙에 대한 세부 정보가 포함됩니다. 웹 ACL 로그를 Amazon Logs 로그 그룹, Amazon CloudWatch Simple Storage Service (Amazon S3) 버킷 또는 Amazon 데이터 파이어호스 전송 스트림으로 보낼 수 있습니다.

기타 데이터 수집 및 분석 옵션

로깅 외에도 다음과 같은 데이터 수집 및 분석 옵션을 활성화할 수 있습니다.

- Amazon Security Lake — 웹 ACL 데이터를 수집하도록 보안 레이크를 구성할 수 있습니다. Security Lake는 정규화, 분석 및 관리를 위해 다양한 소스에서 로그 및 이벤트 데이터를 수집합니다. 이 옵션에 대한 자세한 내용은 Amazon Security Lake란 무엇입니까? 를 참조하십시오. 및 Amazon Security Lake 사용 설명서의 AWS 서비스에서 데이터 수집

  AWS WAF 이 옵션 사용에 따른 비용은 청구되지 않습니다. 요금 정보는 Amazon Security Lake 사용 설명서의 Security Lake 요금 및 Security Lake 요금이 결정되는 방식을 참조하십시오.
- 요청 샘플링 — 평가하는 웹 요청을 샘플링하여 애플리케이션이 수신하는 트래픽 유형을 파악하도록 웹 ACL을 구성할 수 있습니다. 이 옵션에 대한 자세한 내용은 웹 요청 샘플 보기 단원을 참조하세요.

> **Note**
>
> 웹 ACL 로깅 구성은 로그에만 영향을 줍니다. AWS WAF 특히 로깅을 위해 수정된 필드 구성은 요청 샘플링이나 Security Lake 데이터 수집에 영향을 주지 않습니다. Security Lake 데이터 수집은 전적으로 Security Lake 서비스를 통해 구성됩니다. 샘플링된 요청에서 필드를 제외하는 유일한 방법은 웹 ACL의 샘플링을 비활성화하는 것입니다.

주제

웹 ACL 트래픽 정보 로깅 요금

웹 ACL 트래픽 정보 로깅에는 각 로그 대상 유형과 관련된 비용에 따라 요금이 부과됩니다. 이러한 요금은 AWS WAF사용 요금에 추가로 부과됩니다. 비용은 선택하는 대상 유형이나 기록하는 데이터 양과 같은 요인에 따라 달라질 수 있습니다.

다음은 각 로깅 대상 유형에 대한 요금 정보의 링크를 제공합니다.

- CloudWatch 로그 - 요금은 벤더 로그 전송에 대한 요금입니다. Amazon CloudWatch 로그 요금을 참조하십시오. 유료 등급에서 로그 탭을 선택한 다음 벤디드 로그에서 Delivery to CloudWatch Logs에 대한 정보를 참조하십시오.
- Amazon S3 버킷 — Amazon S3 요금은 Amazon S3 버킷으로의 CloudWatch 로그 전송 로그 전송 요금과 Amazon S3 사용에 대한 요금을 합산한 요금입니다.
  - Amazon S3은 Amazon S3 요금을 참조하세요.
  - Amazon S3로의 CloudWatch 로그 벤더 로그 전송에 대한 내용은 Amazon CloudWatch 로그 요금을 참조하십시오. 유료 티어에서 로그 탭을 선택한 다음 판매 로그에서 S3로 전송에 대한 정보를 참조하세요.
- Firehose — 아마존 데이터 파이어호스 요금을 참조하십시오.

AWS WAF 요금에 대한 자세한 내용은 요금을 참조하십시오AWS WAF .

AWS WAF 로깅 목적지

이 섹션에서는 AWS WAF 로그에 대해 선택할 수 있는 로깅 옵션에 대해 설명합니다. 각 섹션에서는 대상 유형에 특정된 동작에 대한 정보를 포함하여 로로깅을 구성하기 위한 지침을 제공합니다. 로깅 대상을 구성한 후 웹 ACL 로깅 구성에 해당 사양을 제공하여 로깅을 시작할 수 있습니다.

주제

- 아마존 CloudWatch 로그 로그 그룹
- Amazon 심플 스토리지 서비스 버킷
- Amazon Data Firehose 전송 스트림

아마존 CloudWatch 로그 로그 그룹

이 주제에서는 웹 ACL 트래픽 로그를 로그 로그 그룹으로 전송하는 데 필요한 정보를 제공합니다. CloudWatch

> **Note**
>
> AWS WAF사용 요금 외에 로그인 요금이 부과됩니다. 자세한 내용은 웹 ACL 트래픽 정보 로깅 요금을 참조하세요.

Amazon Logs로 CloudWatch 로그를 보내려면 CloudWatch Logs 로그 그룹을 생성합니다. 로그인을 AWS WAF활성화하면 로그 그룹 ARN을 제공합니다. 웹 ACL에 대한 로깅을 활성화하면 로그 스트림의 로그 로그 그룹에 CloudWatch 로그를 AWS WAF 전달합니다.

CloudWatch 로그를 사용하면 콘솔에서 웹 ACL의 로그를 탐색할 수 있습니다. AWS WAF 웹 ACL 페이지에서 로깅 인사이트 탭을 선택합니다. 이 옵션은 CloudWatch 콘솔을 통해 CloudWatch 로그에 대해 제공되는 로깅 인사이트에 추가됩니다.

웹 ACL과 동일한 지역에 있고 AWS WAF 웹 ACL을 관리하는 데 사용한 것과 동일한 계정을 사용하여 웹 ACL 로그에 대한 로그 그룹을 구성합니다. 로그 로그 그룹 구성에 대한 자세한 내용은 CloudWatch 로그 그룹 및 로그 스트림 작업을 참조하십시오.

CloudWatch 로그 로그 그룹 할당량

CloudWatch 로그에는 기본적으로 최대 처리량 할당량이 있으며, 이는 지역 내 모든 로그 그룹에서 공유되며, 이 할당량을 늘리도록 요청할 수 있습니다. 로깅 요구 사항이 현재 처리량 설정에 비해 너무 높으면 계정에 `PutLogEvents` 대한 제한 측정항목이 표시됩니다. Service Quotas 콘솔에서 한도를 확인하고 증가를 요청하려면 로그 할당량을 참조하세요CloudWatch . PutLogEvents

로그 그룹 이름 지정

로그 그룹 이름은 `aws-waf-logs-`로 시작해야 하며 예를 들어 `aws-waf-logs-testLogGroup2` 등 끝에는 원하는 접미사를 붙일 수 있습니다.

결과 ARN 형식은 다음과 같습니다.

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

로그 스트림의 이름 지정 형식은 다음과 같습니다.

```
Region_web-acl-name_log-stream-number
```

다음은 리전 `us-east-1`의 웹 `TestWebACL` ACL에 대한 예제 로그 스트림입니다.

```
us-east-1_TestWebACL_0
```

로그를 로그에 게시하는 데 필요한 권한 CloudWatch

로그 CloudWatch 로그 그룹에 대한 웹 ACL 트래픽 로깅을 구성하려면 이 섹션에 설명된 권한 설정이 필요합니다. 권한은 AWS WAF 전체 액세스 관리형 정책 (`AWSWAFConsoleFullAccess`또

는AWSWAFFullAccess) 중 하나를 사용할 때 자동으로 설정됩니다. 로깅 및 AWS WAF 리소스에 대한 보다 세밀한 액세스를 관리하려면 권한을 직접 설정할 수 있습니다. 권한 관리에 대한 자세한 내용은 IAM 사용 설명서의 AWS 리소스 액세스 관리를 참조하십시오. AWS WAF 관리형 정책에 대한 자세한 내용은 AWS 에 대한 관리형 정책 AWS WAF을 참조하세요.

이러한 권한을 통해 웹 ACL 로깅 구성을 변경하고, 로그에 대한 로그 전달을 구성하고, CloudWatch 로그 그룹에 대한 정보를 검색할 수 있습니다. 이러한 권한은 AWS WAF를 관리하는 데 사용하는 사용자에게 연결되어야 합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[

            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      }
      {
         "Sid":"WebACLLoggingCWL",
         "Action":[
            "logs:CreateLogDelivery",
            "logs:DeleteLogDelivery",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
}
```

모든 AWS 리소스에 대해 작업이 허용되면 정책에 "Resource" 설정이 지정되어 표시됩니다. "*" 즉, 각 작업이 지원하는 모든 AWS 리소스에 대해 해당 작업이 허용됩니다. 예를 들어 wafv2:PutLoggingConfiguration 작업은 wafv2 로깅 구성 리소스에서만 지원됩니다.

Amazon 심플 스토리지 서비스 버킷

이 주제는 Amazon S3 버킷으로 웹 ACL 트래픽 로그를 전송하기 위한 정보를 제공합니다.

> **Note**
>
> AWS WAF사용 요금 외에 로그인 요금이 부과됩니다. 자세한 내용은 웹 ACL 트래픽 정보 로깅 요금을 참조하세요.

웹 ACL 트래픽 로그를 Amazon S3으로 보내려면 웹 ACL을 관리하는 데 사용하는 것과 동일한 계정에서 Amazon S3 버킷을 설정하고 버킷 이름을 aws-waf-logs-로 시작합니다. 로그인을 활성화할 때 버킷 이름을 제공합니다. AWS WAF로깅 버킷 생성에 대한 자세한 내용을 알아보려면 Amazon Simple Storage Service 사용 설명서의 버킷 생성을 참조하세요.

Amazon Athena 대화형 쿼리 서비스를 사용하여 Amazon S3 로그에 액세스하고 분석할 수 있습니다. Athena에서 표준 SQL을 사용해 Amazon S3의 데이터를 손쉽게 직접 분석할 수 있습니다. 에서 몇 가지 작업을 수행하면 Athena에게 Amazon S3에 저장된 데이터를 알려주고 표준 SQL을 사용하여 임시 쿼리를 실행하고 결과를 빠르게 얻을 수 있습니다. AWS Management Console자세한 내용은 Amazon Athena AWS WAF 사용 설명서의 로그 쿼리를 참조하십시오. 추가 샘플 Amazon Athena 쿼리는 웹 사이트의 waf-log-sample-athenaaws-samples/ -query를 참조하십시오. GitHub

> **Note**
>
> AWS WAF 키 유형 아마존 S3 키 (SSE-S3) 및 AWS Key Management Service (SSE-KMS) 에 대해 Amazon S3 버킷을 사용한 암호화를 지원합니다. AWS KMS keys AWS WAF 에서 관리하는 AWS Key Management Service 키에 대한 암호화는 지원하지 않습니다. AWS

웹 ACL이 해당 로그 파일을 5분 간격으로 Amazon S3 버킷에 게시합니다. 각 로그 파일에는 이전 5분 동안 기록된 트래픽에 대한 로그 레코드가 포함됩니다.

로그 파일의 최대 크기는 75MB입니다. 로그 파일이 5분 내에 파일 크기 한도에 도달하는 경우, 로그는 레코드의 로그 파일로의 추가를 중단하고 Amazon S3 버킷에 게시한 다음 새로운 로그 파일을 생성합니다.

로그 파일은 압축된 상태입니다. Amazon S3 콘솔을 사용해 파일을 열면 Amazon S3에서 로그 레코드의 압축을 해제하고 이를 표시합니다. 로그 파일을 다운로드하는 경우, 압축을 해제해야 레코드를 볼 수 있습니다.

단일 로그 파일에는 여러 레코드와 함께 인터리브 항목이 포함되어 있습니다. 웹 ACL의 모든 로그 파일을 보려면 웹 ACL 이름, 리전 및 계정 ID별로 집계된 항목을 찾아봅니다.

요구 사항 및 구문 이름 지정

AWS WAF 로깅용 버킷 이름은 원하는 접미사로 `aws-waf-logs-` 시작하고 원하는 접미사로 끝날 수 있습니다. 예를 들어 `aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`입니다.

버킷 위치

버킷 위치에서는 다음 구문이 사용됩니다.

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

버킷 ARN

Amazon 리소스 이름(ARN) 버킷의 형식은 다음과 같습니다.

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

접두사가 있는 버킷 위치

객체 키 이름에 접두사를 사용하여 버킷에 저장하는 데이터를 구성하는 경우 로깅 버킷 이름에 접두사를 제공할 수 있습니다.

> **Note**
>
> 콘솔에서는 이 옵션을 사용할 수 없습니다. AWS WAF API, CLI 또는 을 사용하십시오. AWS CloudFormation

Amazon S3에서 접두어 사용에 대한 자세한 내용을 알아보려면 Amazon Simple Storage Service 사용 설명서의 접두어를 사용한 객체 구성을 참조하세요.

접두사가 있는 버킷 위치에는 다음 구문이 사용됩니다.

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

버킷 폴더 및 파일 이름

버킷 내에서 제공한 접두사에 따라 계정 ID, 지역, 웹 ACL 이름, 날짜 및 시간에 따라 결정되는 폴더 구조 아래에 AWS WAF 로그가 기록됩니다.

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

폴더 안에 있는 로그 파일 이름은 비슷한 형식을 따릅니다.

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

폴더 구조 및 로그 파일 이름에 사용되는 시간 지정은 타임스탬프 형식 사양인 YYYYMMddTHHmmZ를 준수합니다.

다음은 이름이 DOC-EXAMPLE-BUCKET인 Amazon S3 버킷의 로그 파일 예제를 보여줍니다. 입니다. AWS 계정 11111111111 웹 ACL은 TEST-WEBACL이고 리전은 us-east-1입니다.

```
s3://DOC-EXAMPLE-BUCKET/AWSLogs/11111111111/WAFLogs/us-east-1/
TEST-WEBACL/2021/10/28/19/50/11111111111_waflogs_us-east-1_TEST-
WEBACL_20211028T1950Z_e0ca43b5.log.gz
```

> **Note**
>
> AWS WAF 로깅용 버킷 이름은 원하는 접미사로 aws-waf-logs- 시작하고 끝나야 합니다.

Amazon S3에 로그를 게시하는 데 필요한 권한

Amazon S3 버킷에 대한 웹 ACL 트래픽 로깅을 구성하려면 다음과 같은 권한 설정이 필요합니다. 이러한 권한은 AWS WAF 전체 액세스 관리형 정책(AWSWAFConsoleFullAccess 또는 AWSWAFFullAccess) 중 하나를 사용할 때 자동으로 설정됩니다. 로깅 및 AWS WAF 리소스에 대한 보다 세밀한 액세스를 관리하려면 이러한 권한을 직접 설정할 수 있습니다. 권한 관리에 관한 자세한 내용은 IAM 사용 설명서의 AWS 리소스에 대한 액세스 관리를 참조하세요. AWS WAF 관리형 정책에 대한 자세한 내용은 을 참조하십시오. AWS 에 대한 관리형 정책 AWS WAF

다음 권한을 통해 웹 ACL 로깅 구성을 변경하고 로그가 Amazon S3 버킷으로 전송되도록 구성할 수 있습니다. 이러한 권한은 AWS WAF를 관리하는 데 사용하는 사용자에게 연결되어야 합니다.

> **Note**
>
> 아래 나열된 권한을 설정하면 AWS CloudTrail 로그에 액세스가 거부되었음을 나타내는 오류가 표시될 수 있지만 AWS WAF 로깅에 사용할 수 있는 권한은 정확합니다.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {

       "Sid":"WebACLLogDelivery",

       "Action":[

          "logs:CreateLogDelivery",

          "logs:DeleteLogDelivery"

       ],

       "Resource": "*",

       "Effect":"Allow"

    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
```

```
            ],
            "Resource": [
                  "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET"
            ],
            "Effect":"Allow"
        }
    ]
}
```

모든 AWS 리소스에 대해 작업이 허용되면 정책에 "Resource" 설정이 지정되어 표시됩니다"*". 즉, 각 작업이 지원하는 모든 AWS 리소스에 대해 해당 작업이 허용됩니다. 예를 들어 wafv2:PutLoggingConfiguration 작업은 wafv2 로깅 구성 리소스에서만 지원됩니다.

기본적으로 Amazon S3 버킷과 버킷에 포함된 객체는 비공개입니다. 버킷 소유자만이 해당 버킷과 그 안에 저장된 객체에 액세스할 수 있습니다. 그러나 버킷 소유자는 액세스 정책을 작성하여 다른 리소스 및 사용자에게 액세스를 허용할 수 있습니다.

로그를 생성하는 사용자가 버킷을 소유한 경우, 해당 서비스에서는 다음 정책을 해당 버킷에 자동으로 연결하여 로그를 버킷에 게시할 로그 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/AWSLogs/account-id/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    },
    {
```

```
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    }
  ]
}
```

> **Note**
>
> AWS WAF 로깅용 버킷 이름은 원하는 접미사로 `aws-waf-logs-` 시작하고 원하는 접미사로 끝날 수 있습니다.

로그를 생성하는 사용자가 버킷을 소유하지 않거나 해당 버킷에 대한 `GetBucketPolicy`와 `PutBucketPolicy`가 없는 경우, 로그 생성이 실패합니다. 이 경우 버킷 소유자가 이전 정책을 수동으로 버킷에 추가하고 로그 생성자의 AWS 계정 ID를 지정해야 합니다. 자세한 내용은 Amazon Simple Storage Service Console 사용 설명서의 S3 버킷 정책을 추가하려면 어떻게 해야 합니까?를 참조하세요. 버킷이 여러 계정으로부터 로그를 수신하는 경우, `Resource` 요소 입력 내용을 각 계정의 `AWSLogDeliveryWrite` 정책 설명에 추가합니다.

예를 들어, 다음 버킷 정책은 다음과 같은 이름의 버킷에 로그를 AWS 계정 111122223333 게시할 수 있도록 허용합니다. `aws-waf-logs-DOC-EXAMPLE-BUCKET`

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/
AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

AWS Key Management Service 를 KMS 키와 함께 사용하기 위한 권한

로깅 대상이 AWS Key Management Service (SSE-KMS) 에 저장된 키를 사용한 서버 측 암호화를 사용하고 고객 관리 키 (KMS 키) 를 사용하는 경우 KMS 키를 사용할 권한을 AWS WAF 부여해야 합니다. 이렇게 하기 위해서는 선택한 대상의 KMS 키에 키 정책을 추가합니다. 이렇게 하면 AWS WAF 로깅을 통해 대상에 로그 파일을 쓸 수 있습니다.

Amazon S3 버킷에 로그인할 수 AWS WAF 있도록 KMS 키에 다음 키 정책을 추가합니다.

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Amazon S3 로그 파일에 액세스하는 데 필요한 권한

Amazon S3는 ACL(액세스 제어 목록)을 사용하여 AWS WAF 로그에서 생성한 로그 파일에 대한 액세스를 관리합니다. 기본적으로 버킷 소유자는 각 로그 파일에 대한 FULL_CONTROL 권한을 보유합니다. 로그 전송 소유자가 버킷 소유자와 다른 경우에는 권한이 없습니다. 로그 전송 계정에는 READ 및 WRITE 권한이 부여됩니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 액세스 제어 목록(ACL) 개요를 참조하세요.

Amazon Data Firehose 전송 스트림

이 섹션에서는 Amazon Data Firehose 전송 스트림으로 웹 ACL 트래픽 로그를 전송하는 데 필요한 정보를 제공합니다.

> **Note**
>
> AWS WAF사용 요금 외에 로그인 요금이 부과됩니다. 자세한 내용은 웹 ACL 트래픽 정보 로깅 요금을 참조하세요.

Amazon Data Firehose에 로그를 보내려면 웹 ACL에서 Firehose에서 구성한 Amazon Data Firehose 전송 스트림으로 로그를 전송합니다. 로깅을 활성화하면 Firehose의 HTTPS 엔드포인트를 통해 스토리지 대상에 로그를 AWS WAF 전달합니다.

AWS WAF 로그 하나는 Firehose 레코드 하나와 같습니다. 일반적으로 초당 10,000개의 요청을 수신하고 전체 로그를 활성화하는 경우 Firehose에서 초당 10,000개의 레코드를 설정해야 합니다. Firehose를 올바르게 구성하지 않으면 모든 로그가 AWS WAF 기록되지 않습니다. 자세한 내용은 Amazon Kinesis Data Firehose 할당량을 참조하십시오.

Amazon Data Firehose 전송 스트림을 생성하고 저장된 로그를 검토하는 방법에 대한 자세한 내용은 Amazon Data Firehose란 무엇입니까? 를 참조하십시오.

전송 스트림 생성에 대한 자세한 내용은 Amazon Data Firehose 전송 스트림 생성을 참조하십시오.

웹 ACL을 위한 Amazon Data Firehose 전송 스트림 구성

다음과 같이 웹 ACL에 대한 Amazon Data Firehose 전송 스트림을 구성합니다.

- 웹 ACL을 관리하는 데 사용하는 것과 동일한 계정을 사용하여 생성합니다.
- 웹 ACL과 동일한 리전에서 생성합니다. CloudFrontAmazon의 로그를 캡처하는 경우 미국 동부 (버지니아 북부) 지역에서 파이어호스를 생성하십시오. `us-east-1`
- Data Firehose에 `aws-waf-logs-` 접두사로 시작하는 이름을 지정합니다. 예를 들어 `aws-waf-logs-us-east-2-analytics`입니다.
- 직접 입력으로 구성하여 애플리케이션이 전송 스트림에 직접 액세스할 수 있도록 합니다. Amazon Data Firehose 콘솔에서 전송 스트림 소스 설정으로 다이렉트 PUT 또는 기타 소스를 선택합니다. API를 통해 전송 스트림 속성 `DeliveryStreamType`을 `DirectPut`로 설정합니다.

> **Note**
>
> `Kinesis stream`을 소스로 사용하지 마십시오.

Amazon Data Firehose 전송 스트림에 로그를 게시하는 데 필요한 권한

Kinesis Data Firehose 구성에 필요한 권한을 이해하려면 Amazon Kinesis Data Firehose를 사용한 액세스 제어를 참조하세요.

Amazon Data Firehose 전송 스트림을 사용하여 웹 ACL 로깅을 성공적으로 활성화하려면 다음 권한이 있어야 합니다.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

서비스 연결 역할 및 `iam:CreateServiceLinkedRole` 권한에 대한 자세한 내용은 서비스 연결 역할 사용 AWS WAF 섹션을 참조하세요.

웹 ACL 로깅 구성

언제든지 웹 ACL에 대한 로깅을 활성화하거나 비활성화할 수 있습니다.

> **Note**
>
> AWS WAF사용 요금 외에 로그인 요금이 부과됩니다. 자세한 내용은 웹 ACL 트래픽 정보 로깅 요금을 참조하세요.

로그에서 로그 레코드를 찾을 수 없는 경우

드문 경우이긴 하지만 AWS WAF 로그 전달이 100% 미만으로 떨어질 수 있으며, 이때 로그는 최선의 노력을 기울여 전달됩니다. AWS WAF 아키텍처는 다른 모든 고려 사항보다 애플리케이션의 보안을 우선시합니다. 로깅 흐름에 트래픽 제한이 발생하는 경우와 같은 일부 상황에서는 레코드가 삭제될 수 있습니다. 이는 몇 개 이상의 레코드에는 영향을 미치지 않아야 합니다. 누락된 로그 항목이 여러 개 발견되면 AWS Support 센터에 문의하세요.

웹 ACL의 로깅 구성에서 로그로 AWS WAF 보내는 내용을 사용자 지정할 수 있습니다.

- 필드 수정 – 해당하는 일치 설정을 사용하는 규칙에 대한 로그 레코드에서 URI 경로, 쿼리 문자열, 단일 헤더 및 HTTP 메서드 필드를 수정할 수 있습니다. 삭제된 필드는 로그에서 REDACTED로 표시됩니다. 예를 들어 쿼리 문자열 필드를 수정하면 로그에서 쿼리 문자열 일치 구성 요소 설정을 사용하는 모든 규칙에 대해 해당 필드가 REDACTED로 나열됩니다. 교정은 규칙에서 일치하도록 지정한 요청 구성 요소에만 적용되므로 단일 헤더 구성 요소의 수정은 헤더와 일치하는 규칙에는 적용되지 않습니다. 로그 필드 목록은 로그 필드 섹션을 참조하세요.

  > **Note**
  >
  > 이 설정은 요청 샘플링에 영향을 주지 않습니다. 요청 샘플링의 경우 필드를 제외하는 유일한 방법은 웹 ACL의 샘플링을 비활성화하는 것입니다.

- 로그 필터링 - 필터링을추가하여 로그에 보관되는 웹 요청과 삭제되는 웹 요청을 지정할 수 있습니다. 웹 요청 평가 중에 AWS WAF 적용되는 설정을 기준으로 필터링합니다. 다음 설정을 기준으로 필터링할 수 있습니다.
  - 정규화된 레이블 – 정규화된 레이블에는 접두사, 선택적 네임스페이스 및 레이블 이름이 포함됩니다. 접두사는 레이블을 추가한 규칙의 규칙 그룹 또는 웹 ACL 컨텍스트를 식별합니다. 레이블에 대한 자세한 내용은 AWS WAF 웹 요청의 레이블 섹션을 참조하세요.

- 규칙 작업 - 규칙 그룹 규칙에 대해 모든 일반 규칙 작업 설정과 규칙 그룹 규칙의 레거시 `EXCLUDED_AS_COUNT` 재정의 옵션을 기준으로 필터링할 수 있습니다. 규칙 작업 설정에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요. 규칙 그룹 규칙의 현재 및 레거시 규칙 작업 재정의에 대한 자세한 내용은 규칙 그룹의 작업 재정의 옵션 섹션을 참조하세요.
  - 일반 규칙 작업 필터는 규칙에 구성된 작업뿐만 아니라 현재의 규칙 그룹 규칙 작업 재정의 옵션을 사용하여 구성된 작업에도 적용됩니다.
  - `EXCLUDED_AS_COUNT` 로그 필터는 `Count` 작업 로그 필터와 중복됩니다. `EXCLUDED_AS_COUNT`는 규칙 그룹 규칙 작업을 Count로 재정의하기 위해 현재 옵션과 레거시 옵션을 모두 필터링합니다.

웹 ACL에 대한 로깅 활성화

웹 ACL에 대한 로깅을 활성화하려면 로깅 대상을 이미 구성해야 합니다. 대상 옵션 및 각 옵션의 요구 사항에 대한 자세한 내용은 AWS WAF 로깅 목적지 섹션을 참조하세요.

웹 ACL에 대해 로깅을 활성화하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. 로깅을 활성화하려는 웹 ACL의 이름을 선택합니다. 콘솔에서 웹 ACL의 설명으로 이동하여 여기에서 설명을 편집할 수 있습니다.
4. 로깅 탭에서 로깅 활성화를 선택합니다.
5. 로깅 대상 유형을 선택한 다음 구성한 로깅 대상을 선택합니다. 이름이 `aws-waf-logs-`로 시작하는 로깅 대상을 선택해야 합니다.
6. (선택 사항) 일부 필드를 로그에 포함하지 않으려면 해당 필드를 수정합니다. 삭제할 필드를 선택한 후 추가를 선택합니다. 필요에 따라 이 작업을 반복하여 추가 필드를 삭제합니다.

   > **Note**
   >
   > 이 설정은 요청 샘플링에 영향을 주지 않습니다. 요청 샘플링의 경우 필드를 제외하는 유일한 방법은 웹 ACL의 샘플링을 비활성화하는 것입니다.

7. (선택 사항) 모든 요청을 로그로 전송하지 않으려면 필터링 기준과 동작을 추가합니다. 필터 로그에서 적용하려는 각 필터에 대해 필터 추가를 선택한 다음 기준과 일치하는 요청을 유지할지 아니면 삭제할지 여부를 지정합니다. 필터 추가를 완료할 때 필요 시 기본 로깅 동작을 수정합니다.

8. 로깅 활성화를 선택합니다.

> **Note**
>
> 로깅을 성공적으로 AWS WAF 활성화하면 로깅 대상에 로그를 쓰는 데 필요한 권한을 가진 서비스 연결 역할이 생성됩니다. 자세한 내용은 서비스 연결 역할 사용 AWS WAF을(를) 참조하세요.

로그 필드

다음 목록에서는 가능한 로그 필드에 대해 설명합니다.

작업

요청에 AWS WAF 적용된 종료 조치. 이는 허용, 차단, CAPTCHA 또는 챌린지를 나타냅니다. 웹 요청에 유효한 토큰이 없으면 CAPTCHA 및 Challenge 작업이 종료됩니다.

args

쿼리 문자열.

captchaResponse

요청에 작업이 적용될 때 채워지는 요청의 CAPTCHA CAPTCHA 작업 상태입니다. 이 필드는 종료 여부에 관계없이 모든 CAPTCHA 작업에 대해 채워집니다. 요청에 CAPTCHA 작업이 여러 번 적용된 경우 이 필드는 작업이 마지막으로 적용된 시점부터 채워집니다.

요청에 토큰이 포함되지 않은 경우 또는 토큰이 유효하지 않거나 만료된 경우 CAPTCHA 작업에서 웹 요청 검사를 종료합니다. CAPTCHA작업이 종료되는 경우 이 필드에는 응답 코드와 실패 이유가 포함됩니다. 작업이 종료되지 않는 경우 이 필드에는 해결 타임스탬프가 포함됩니다. 종료 작업과 종료되지 않은 작업을 구분하기 위해 이 필드에서 비어 있지 않은 속성을 필터링할 수 있습니다. `failureReason`

challengeResponse

요청에 작업이 적용될 때 채워지는 요청의 챌린지 Challenge 작업 상태입니다. 이 필드는 종료 또는 비종료 여부에 관계없이 모든 Challenge 작업에 대해 입력됩니다. 요청에 Challenge 작업이 여러 번 적용된 경우 이 필드는 작업이 마지막으로 적용된 시점부터 채워집니다.

요청에 토큰이 포함되지 않은 경우 또는 토큰이 유효하지 않거나 만료된 경우 Challenge 작업에서 웹 요청 검사를 종료합니다. Challenge작업이 종료되는 경우 이 필드에는 응답 코드와 실패 이유

가 포함됩니다. 작업이 종료되지 않는 경우 이 필드에는 해결 타임스탬프가 포함됩니다. 종료 작업과 종료되지 않은 작업을 구분하기 위해 이 필드에서 비어 있지 않은 속성을 필터링할 수 있습니다.

`failureReason`

clientIp

클라이언트가 요청을 보내는 IP 주소.

country

요청의 출처 국가. 원산지를 확인할 수 없는 경우 이 AWS WAF 필드는 로 설정됩니다. -

excludedRules

규칙 그룹 규칙에만 사용됩니다. 규칙 그룹에서 제외한 규칙의 목록입니다. 이 규칙에 대한 작업은 Count로 설정됩니다.

규칙 재정의 작업 옵션을 사용하여 규칙을 개수로 재정의하는 경우 일치 항목이 여기에 나열되지 않습니다. 이들 항목은 작업 쌍인 `action` 및 `overriddenAction`으로 나열됩니다.

exclusionType

제외된 규칙에 Count 작업이 있음을 나타내는 유형입니다.

ruleId

규칙 그룹 내에서 제외된 규칙의 ID입니다.

formatVersion

로그의 포맷 버전.

헤더

헤더 목록.

httpMethod

요청의 HTTP 메서드.

httpRequest

요청에 대한 메타데이터.

httpSourceId

연결된 리소스의 ID입니다.

- Amazon CloudFront 배포의 경우 ARN 구문의 ID는 *`distribution-id`* 다음과 같습니다.

  `arn:`*`partition`*`cloudfront::`*`account-id`*`:distribution/`*`distribution-id`*

- Application Load Balancer의 경우 ARN 구문에서 ID는 *load-balancer-id*입니다.

  arn:*partition*:elasticloadbalancing:*region*:*account-id*:loadbalancer/app/*load-balancer-name*/*load-balancer-id*

- Amazon API Gateway REST API의 경우 ARN 구문에서 ID는 *api-id*입니다.

  arn:*partition*:apigateway:*region*::/restapis/*api-id*/stages/*stage-name*

- AWS AppSync GraphQL API의 경우 ARN 구문의 ID는 다음과 같습니다*GraphQLApiId*.

  arn:*partition*:appsync:*region*:*account-id*:apis/*GraphQLApiId*

- Amazon Cognito 사용자 풀의 경우 ARN 구문의 ID는 *user-pool-id*입니다.

  arn:*partition*:cognito-idp:*region*:*account-id*:userpool/*user-pool-id*

- AWS App Runner 서비스의 경우 ARN 구문의 ID는 *apprunner-service-id* 다음과 같습니다.

  arn:*partition*:apprunner:*region*:*account-id*:service/*apprunner-service-name*/*apprunner-service-id*

httpSourceName

요청의 소스. 가능한 값: 아마존의 CF 경우 CloudFront, APIGW Amazon API Gateway의 ALB 경우, 애플리케이션 로드 APPSYNC 밸런서용, Amazon Cognito의 COGNITOIDP 경우 AWS AppSync, 앱 러너용APPRUNNER, 검증된 액세스용 값입니다. VERIFIED_ACCESS

httpVersion

HTTP 버전.

ja3Fingerprint

요청의 JA3 지문.

> **Note**
>
> JA3 지문 검사는 Amazon CloudFront 배포 및 애플리케이션 로드 밸런서에만 사용할 수 있습니다.

JA3 자문은 수신 요청의 TLS 클라이언트 Hello에서 파생된 32자 해시입니다. 이 지문은 클라이언트 TLS 구성의 고유 식별자 역할을 합니다. AWS WAF 계산에 필요한 충분한 TLS Client Hello 정보가 있는 각 요청에 대해 이 핑거프린트를 계산하고 기록합니다.

웹 ACL 규칙에서 JA3 지문 일치를 구성할 때 이 값을 제공합니다. JA3 지문과의 일치 생성에 대한 자세한 내용은 규칙 문에 대한 요청 구성 요소 옵션의 JA3 지문 섹션을 참조하세요.

labels

웹 요청의 레이블 이러한 레이블은 요청을 평가하는 데 사용된 규칙에 따라 적용되었습니다. AWS WAF 처음 100개의 레이블을 기록합니다.

nonTerminatingMatching규칙

요청과 일치하는 종료되지 않는 규칙 목록. 목록의 각 항목에는 다음 정보가 포함됩니다.

작업

요청에 AWS WAF 적용된 조치. 이는 개수, CAPTCHA 또는 챌린지를 나타냅니다. 웹 요청에 유효한 토큰이 포함된 경우 CAPTCHA 및 Challenge가 종료되지 않습니다.

ruleId

요청에 부합되는 비 종료 규칙의 ID.

ruleMatchDetails

요청과 일치하는 규칙에 대한 자세한 정보입니다. 이 필드는 SQL 명령어 삽입 및 크로스 사이트 스크립팅(XSS) 일치 규칙 문에 대해서만 채워집니다. 일치 규칙에는 둘 이상의 검사 기준에 대한 일치가 필요할 수 있으므로 이러한 일치 세부 정보는 일치 기준 배열로 제공됩니다.

각 규칙에 대해 제공되는 추가 정보는 규칙 구성, 규칙 일치 유형, 일치 세부 정보 등의 요소에 따라 달라집니다. 예를 들어, CAPTCHA 또는 Challenge 동작이 있는 규칙의 경우 `captchaResponse` OR가 `challengeResponse` 나열됩니다. 일치 규칙이 규칙 그룹에 있고 구성된 규칙 동작을 재정의한 경우 구성된 작업이 에서 제공됩니다. `overriddenAction`

oversizeFields

웹 ACL에서 검사한 웹 요청 중 검사 한도를 초과한 필드 목록. AWS WAF 필드 크기가 너무 크지만 웹 ACL이 해당 필드를 검사하지 않는 경우 여기에 나열되지 않습니다.

이 목록에는 `REQUEST_BODY`, `REQUEST_JSON_BODY`, `REQUEST_HEADERS` 및 `REQUEST_COOKIES` 값 중 0개 이상이 포함될 수 있습니다. 과대 필드에 대한 자세한 내용은 에서 크기 초과 요청 구성 요소 처리 AWS WAF 섹션을 참조하세요.

rateBasedRule목록

요청에 작용하는 속도 기반 규칙의 목록. 속도 기반 규칙에 대한 자세한 내용은 비율 기반 규칙 문 섹션을 참조하세요.

rateBasedRule아이디

요청에 작용하는 비율 기반 규칙의 ID입니다. 이 규칙이 요청을 종료한 경우 `rateBasedRuleId`의 ID는 `terminatingRuleId`의 ID와 동일합니다.

rateBasedRule이름

요청에 작용하는 비율 기반 규칙의 이름입니다.

limitKey

규칙이 사용하는 집계 유형. 사용 가능한 값은 웹 요청 오리진에는 `IP`, 요청의 헤더에 전달된 IP에는 `FORWARDED_IP`, 사용자 지정 집계 키 설정에는 `CUSTOMKEYS`, 그리고 집계 없이 모든 요청 수를 계산하려는 경우 `CONSTANT`입니다.

리밋-밸류

단일 IP 주소 유형에 의해 속도를 제한할 때만 사용됩니다. 요청에 유효하지 않은 IP 주소가 포함된 경우 `limitvalue`는 `INVALID`입니다.

maxRateAllowed

특정 집계 인스턴스에 대해 지정된 기간 동안 허용되는 최대 요청 수입니다. 집계 인스턴스는 속도 기반 규칙 `limitKey` 구성에서 제공한 추가 키 사양을 더하여 정의됩니다.

evaluationWindowSec

요청 수에 AWS WAF 포함된 시간 (초).

customValues

요청의 속도 기반 규칙에 의해 식별된 고유 값. 문자열 값의 경우 로그는 문자열 값의 처음 32자를 출력합니다. 키 유형에 따라 이러한 값은 HTTP 메서드 또는 쿼리 문자열과 같이 키에만 사용할 수 있는 값일 수도 있고 헤더 및 헤더 이름과 같은 키와 이름에 모두 사용할 수 있는 값일 수도 있습니다.

requestHeadersInserted

사용자 지정 요청 처리를 위해 삽입된 헤더 목록.

requestId

기본 호스트 서비스에 의해 생성되는 요청의 ID입니다. Application Load Balancer의 경우 추적 ID입니다. 다른 모든 경우 이것이 요청 ID입니다.

responseCodeSent

사용자 지정 응답과 함께 전송된 응답 코드입니다.

ruleGroupId

규칙 그룹의 ID. 규칙에서 요청을 차단한 경우 `ruleGroupID`의 ID는 `terminatingRuleId`의 ID와 동일합니다.

ruleGroupList

일치 정보가 포함된 이 요청에 작용하는 규칙 그룹의 목록.

terminatingRule

요청을 종료한 규칙. 이 항목이 있는 경우 다음과 같은 정보가 포함됩니다.

작업

요청에 AWS WAF 적용된 종료 조치. 이는 허용, 차단, CAPTCHA 또는 챌린지를 나타냅니다. 웹 요청에 유효한 토큰이 없으면 CAPTCHA 및 Challenge 작업이 종료됩니다.

ruleId

요청과 일치하는 규칙의 ID입니다.

ruleMatchDetails

요청과 일치하는 규칙에 대한 자세한 정보입니다. 이 필드는 SQL 명령어 삽입 및 크로스 사이트 스크립팅(XSS) 일치 규칙 문에 대해서만 채워집니다. 일치 규칙에는 둘 이상의 검사 기준에 대한 일치가 필요할 수 있으므로 이러한 일치 세부 정보는 일치 기준 배열로 제공됩니다.

각 규칙에 대해 제공되는 추가 정보는 규칙 구성, 규칙 일치 유형, 일치 세부 정보 등의 요소에 따라 달라집니다. 예를 들어, CAPTCHA 또는 Challenge 동작이 있는 규칙의 경우 `captchaResponse` OR가 `challengeResponse` 나열됩니다. 일치 규칙이 규칙 그룹에 있고 구성된 규칙 동작을 재정의한 경우 구성된 작업이 에서 제공됩니다. `overriddenAction`

terminatingRuleId

요청을 종료한 규칙의 ID. 요청을 종료하는 규칙이 없으면 이 값은 `Default_Action`입니다.

terminatingRuleMatch세부 정보

요청과 일치하는 종료 규칙에 대한 자세한 정보입니다. 종료 규칙에는 웹 요청에 대한 검사 프로세스를 종료하는 작업이 포함되어 있습니다. 종료 규칙에 사용 가능한 작업으로는 Allow, Block, CAPTCHA 및 Challenge가 있습니다. 웹 요청을 검사하는 동안 요청과 일치하고 종료 작업이 있는 첫 번째 규칙에서 검사를 AWS WAF 중지하고 작업을 적용합니다. 웹 요청에는 일치하는 종료 규칙에 대해 로그에 보고된 위협 외에도 다른 위협이 포함될 수 있습니다.

이는 SQL 명령어 삽입 및 크로스 사이트 스크립팅(XSS) 일치 규칙 문에 대해서만 채워집니다. 일치 규칙에는 둘 이상의 검사 기준에 대한 일치가 필요할 수 있으므로 이러한 일치 세부 정보는 일치 기준 배열로 제공됩니다.

terminatingRuleType

요청을 종료한 규칙의 유형. 가능한 값: RATE_BASED, REGULAR, GROUP 및 MANAGED_RULE_GROUP.

타임스탬프

밀리초 단위의 타임스탬프.

uri

요청의 URI.

webaclId

웹 ACL의 GUID.

로그 예제

Example 속도 기반 규칙 1: **`Header:dogname`**으로 설정된 키 하나를 포함하는 규칙 구성

```
{
  "Name": "RateBasedRule",
  "Priority": 1,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "CUSTOM_KEYS",
      "CustomKeys": [
        {
          "Header": {
            "Name": "dogname",
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ]
          }
        }
```

```
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example 속도 기반 규칙 1: 속도 기반 규칙에 의해 차단된 요청의 로그 입력

```
{
   "timestamp":1683355579981,
   "formatVersion":1,
   "webaclId": ...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
         "rateBasedRuleId": ...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            }
```

```
        ]
      }
   ],
   "nonTerminatingMatchingRules":[

   ],
   "requestHeadersInserted":null,
   "responseCodeSent":null,
   "httpRequest":{
      "clientIp":"52.46.82.45",
      "country":"FR",
      "headers":[
         {
            "name":"X-Forwarded-For",
            "value":"52.46.82.45"
         },
         {
            "name":"X-Forwarded-Proto",
            "value":"https"
         },
         {
            "name":"X-Forwarded-Port",
            "value":"443"
         },
         {
            "name":"Host",
            "value":"rjvegx5guh.execute-api.eu-west-3.amazonaws.com"
         },
         {
            "name":"X-Amzn-Trace-Id",
            "value":"Root=1-645566cf-7cb058b04d9bb3ee01dc4036"
         },
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"RateBasedRuleTestKoipOneKeyModulePV2"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
```

```
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"Ed0AiHF_CGYF-DA="
   }
}
```

Example 속도 기반 규칙 2: **Header:dogname** 및 **Header:catname**으로 설정된 두 키를 포함하는 규칙 구성

```
    {
      "Name": "RateBasedRule",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "Header": {
                "Name": "dogname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            },
            {
              "Header": {
                "Name": "catname",
                "TextTransformations": [
                  {
                    "Priority": 0,
                    "Type": "NONE"
                  }
                ]
              }
            }
          ]
```

```
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "RateBasedRule"
      }
    }
```

Example 속도 기반 규칙 2: 속도 기반 규칙에 의해 차단된 요청의 로그 입력

```
{
   "timestamp":1633322211194,
   "formatVersion":1,
   "webaclId":...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
         "rateBasedRuleId":...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
               "name":"dogname",
               "value":"ella"
            },
            {
```

```
            "key":"HEADER",
            "name":"catname",
            "value":"goofie"
         }
      ]
   }
],
"nonTerminatingMatchingRules":[

],
"requestHeadersInserted":null,
"responseCodeSent":null,
"httpRequest":{
   "clientIp":"52.46.82.35",
   "country":"FR",
   "headers":[
      {
         "name":"X-Forwarded-For",
         "value":"52.46.82.35"
      },
      {
         "name":"X-Forwarded-Proto",
         "value":"https"
      },
      {
         "name":"X-Forwarded-Port",
         "value":"443"
      },
      {
         "name":"Host",
         "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
      },
      {
         "name":"X-Amzn-Trace-Id",
         "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
      },
      {
         "name":"catname",
         "value":"goofie"
      },
      {
         "name":"dogname",
         "value":"ella"
      },
```

```
         {
            "name":"User-Agent",
            "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"EdzmlH5OCGYF1vQ="
   }
}
```

Example SQLi 탐지 시 트리거된 규칙의 로그 출력(종료)

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
```

```
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example SQLi 감지 시 트리거된 규칙의 로그 출력(비종료)

```
{
    "timestamp":1592357192516
    ,"formatVersion":1
    ,"webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"Default_Action"
```

```
    ,"terminatingRuleType":"REGULAR"
    ,"action":"ALLOW"
    ,"terminatingRuleMatchDetails":[]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":[]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":
    [{
        "ruleId":"TestRule"
        ,"action":"COUNT"
        ,"ruleMatchDetails":
        [{
            "conditionType":"SQL_INJECTION"
            ,"sensitivityLevel": "HIGH"
            ,"location":"HEADER"
            ,"matchedData":[
                "10"
                ,"and"
                ,"1"]
            }]
    }]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":[
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader","myValue":"10 AND 1=1"}
            ]
            ,"uri":"/myUri","args":""
            ,"httpVersion":"HTTP/1.1"
            ,"httpMethod":"GET"
            ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 규칙 그룹 내에서 트리거된 여러 규칙에 대한 로그 출력(RuleA-XSS는 종료이고 Rule-B는 비종료)

```
{
    "timestamp":1592361810888,
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
                    ,"and"
                    ,"1"]
            }]
        }]
```

```
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
        ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 콘텐츠 유형이 JSON인 요청 본문 검사를 위해 트리거된 규칙의 로그 출력

AWS WAF 현재 JSON 본문 검사 위치를 로 UNKNOWN 보고합니다.

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
```

```
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example 유효하고 만료되지 않은 CAPTCHA 토큰을 사용하는 웹 요청에 대한 CAPTCHA 규칙의 로그 출력

다음 로그 목록은 CAPTCHA 작업을 포함하는 규칙과 일치하는 웹 요청에 대한 것입니다. 웹 요청에는 유효하고 만료되지 않은 CAPTCHA 토큰이 있으며, 작업의 동작과 유사하게 CAPTCHA 일치 항목으로만 기록됩니다 AWS WAF. Count 이 CAPTCHA 일치는 `nonTerminatingMatchingRules` 아래에 나와 있습니다.

```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
```

```
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
```

```
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
```

```
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example CAPTCHA 토큰이 없는 웹 요청에 대한 CAPTCHA 규칙의 로그 출력

다음 로그 목록은 CAPTCHA 작업을 포함하는 규칙과 일치하는 웹 요청에 대한 것입니다. 웹 요청에는 CAPTCHA 토큰이 없었고 에 의해 차단되었습니다. AWS WAF


```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
```

```
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
```

```
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
}
```

AWS WAF 보호 기능 테스트 및 조정

AWS WAF 웹 ACL의 변경 사항을 웹 사이트 또는 웹 애플리케이션 트래픽에 적용하기 전에 테스트하고 조정하는 것이 좋습니다.

> **⚠ 프로덕션 트래픽 위험**
>
> 프로덕션 트래픽용 웹 ACL 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 스테이징 또는 테스트 환경에서 이를 테스트하고 조정합니다. 그런 다음 프로덕션 트래픽을 사용하여 규칙을 개수 모드에서 테스트하고 조정한 다음 활성화합니다.

이 섹션에서는 AWS WAF 웹 ACL, 규칙, 규칙 그룹, IP 세트 및 정규식 패턴 세트를 테스트하고 조정하기 위한 지침을 제공합니다.

또한 이 섹션에서는 다른 사람이 관리하는 규칙 그룹의 사용을 테스트하기 위한 일반적인 지침을 제공합니다. 여기에는 AWS 관리형 규칙 규칙 그룹, AWS Marketplace 관리형 규칙 그룹, 다른 계정에서 공유한 규칙 그룹이 포함됩니다. 이러한 규칙 그룹의 경우 규칙 그룹 공급자로부터 받은 지침도 따르십시오.

- Bot Control AWS 관리 규칙 그룹에 대한 자세한 내용은 을 참조하십시오AWS WAF 봇 컨트롤 테스트 및 배포.
- 계정 탈취 방지 AWS 관리 규칙 규칙 그룹에 대한 자세한 내용은 을 참조하십시오ATP 테스트 및 배포.
- 계정 생성 사기 방지 AWS 관리 규칙 규칙 그룹에 대한 자세한 내용은 을 참조하십시오ACFP 테스트 및 배포.

업데이트 중 일시적인 불일치

웹 ACL 또는 기타 AWS WAF 리소스를 만들거나 변경하는 경우 리소스가 저장된 모든 영역에 변경 사항이 적용되는 데 약간의 시간이 걸립니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다.

다음은 변경 전파 중에 표시될 수 있는 일시적 불일치의 예입니다.

- 웹 ACL을 생성한 후 이를 리소스에 연결하려고 하면 웹 ACL을 사용할 수 없다는 예외가 발생할 수 있습니다.
- 웹 ACL에 규칙 그룹을 추가한 후 새 규칙 그룹 규칙이 웹 ACL이 사용되는 한 영역에는 적용되고 다른 영역에서는 적용되지 않을 수 있습니다.
- 규칙 작업 설정을 변경한 후 일부 위치에서 이전 작업이 표시되고 다른 위치에서는 새 작업이 표시될 수 있습니다.
- 차단 규칙에서 사용되는 IP 세트에 IP 주소를 추가한 후 새 주소가 한 영역에서는 차단되는데 다른 영역에서 계속 허용될 수도 있습니다.

상위 단계 테스트 및 조정

이 섹션은 웹 ACL에서 사용하는 규칙 또는 규칙 그룹을 포함하여 웹 ACL의 변경 사항을 테스트하는 단계의 체크리스트를 제공합니다.

> **Note**
>
> 이 섹션의 지침을 따르려면 웹 ACL, 규칙, 규칙 그룹과 같은 AWS WAF 보호를 생성하고 관리하는 방법을 이해해야 합니다. 이 정보는 이 가이드의 이전 섹션에 설명되어 있습니다.

웹 ACL을 테스트 및 조정하려면

이러한 단계를 먼저 테스트 환경에서 수행한 다음, 프로덕션 환경에서 수행합니다.

1. 테스트 준비

   모니터링 환경을 준비하고, 새 AWS WAF 보호 기능을 테스트용 카운트 모드로 전환하고, 필요한 리소스 연결을 생성하십시오.

   테스트 준비 섹션을 참조하십시오.
2. 테스트 및 프로덕션 환경 모니터링 및 조정

   먼저 테스트 또는 스테이징 환경에서 AWS WAF 보호 기능을 모니터링하고 조정한 다음 프로덕션 환경에서 필요한 만큼 트래픽을 처리할 수 있다고 확신할 때까지 모니터링하고 조정하십시오.

   모니터링 및 조정 섹션을 참조하십시오.
3. 프로덕션 환경에서 보호 활성화

   테스트 보호 기능에 만족하는 경우 프로덕션 모드로 전환하고 불필요한 테스트 아티팩트를 모두 정리한 후 계속 모니터링합니다.

   프로덕션 환경에서 보호 기능을 활성화하십시오 섹션을 참조하십시오.

변경 사항 구현을 완료한 후에는 프로덕션 환경에서 웹 트래픽 및 보호 기능을 계속 모니터링하여 원하는 대로 작동하는지 확인합니다. 웹 트래픽 패턴이 시간이 지남에 따라 변경될 수 있으므로 보호 기능을 가끔 조정해야 할 수도 있습니다.

테스트 준비

이 섹션에서는 AWS WAF 보호 기능을 테스트하고 조정하도록 설정하는 방법을 설명합니다.

> **Note**
>
> 이 섹션의 지침을 따르려면 웹 ACL, 규칙, 규칙 그룹과 같은 AWS WAF 보호를 생성하고 관리하는 방법을 일반적으로 이해해야 합니다. 이 정보는 이 가이드의 이전 섹션에 설명되어 있습니다.

테스트를 준비하려면

1. 웹 ACL에 대한 웹 ACL 로깅, Amazon CloudWatch 지표 및 웹 요청 샘플링을 활성화합니다.

   로깅, 지표 및 샘플링을 사용하여 웹 ACL 규칙과 웹 트래픽의 상호 작용을 모니터링합니다.

- 로깅 — 웹 ACL이 평가하는 웹 요청을 AWS WAF 기록하도록 구성할 수 있습니다. 로그를 로그, Amazon S3 버킷 또는 Amazon Data Firehose 전송 스트림으로 전송할 수 있습니다. CloudWatch 필드를 수정하고 필터링을 적용할 수 있습니다. 자세한 정보는 AWS WAF 웹 ACL 트래픽 로깅을 참조하세요.
- Amazon Security Lake — 웹 ACL 데이터를 수집하도록 보안 레이크를 구성할 수 있습니다. Security Lake는 정규화, 분석 및 관리를 위해 다양한 소스에서 로그 및 이벤트 데이터를 수집합니다. 이 옵션에 대한 자세한 내용은 Amazon Security Lake란 무엇입니까? 를 참조하십시오. 및 Amazon Security Lake 사용 설명서의 AWS 서비스에서 데이터 수집
- Amazon CloudWatch 지표 — 웹 ACL 구성에서 모니터링하려는 모든 항목에 대한 지표 사양을 제공하십시오. AWS WAF 및 CloudWatch 콘솔을 통해 지표를 볼 수 있습니다. 자세한 정보는 아마존을 통한 모니터링 CloudWatch을 참조하세요.
- 웹 요청 샘플링 — 웹 ACL이 평가하는 모든 웹 요청의 샘플을 볼 수 있습니다. 웹 요청 샘플링에 대한 자세한 내용은 웹 요청 샘플 보기 섹션을 참조하세요.

2. 보호 기능을 Count 모드로 설정합니다.

   웹 ACL 구성에서 테스트하려는 모든 항목을 계산 모드로 전환합니다. 이렇게 하면 테스트 보호 기능이 요청 처리 방식을 변경하지 않고도 웹 요청과의 일치 항목을 기록할 수 있습니다. 지표, 로그 및 샘플링된 요청에서 일치하는 항목을 보고 일치 기준을 확인하며 웹 트래픽에 미칠 수 있는 영향을 파악할 수 있습니다. 일치 요청에 레이블을 추가하는 규칙은 규칙 작업에 상관없이 레이블을 추가합니다.

   - 웹 ACL에 정의된 규칙 - 웹 ACL에서 규칙을 편집하고 Count의 작업을 설정합니다.
   - 규칙 그룹 - 웹 ACL 구성에서 규칙 그룹의 규칙 문을 편집한 후 규칙 창에서 모든 규칙 작업 재정의 드롭다운을 열고 Count를 선택합니다. JSON에서 웹 ACL을 관리하는 경우 `ActionToUse`가 Count로 설정된 상태에서 규칙 그룹 참조 문의 `RuleActionOverrides` 설정에 규칙을 추가합니다. 다음 예제 목록은 `AWSManagedRulesAnonymousIpList` AWS 관리형 규칙 그룹의 두 규칙에 대한 재정의를 보여줍니다.

```
"ManagedRuleGroupStatement": {
  "VendorName": "AWS",
  "Name": "AWSManagedRulesAnonymousIpList",
    "RuleActionOverrides": [
      {
        "ActionToUse": {
          "Count": {}
        },
        "Name": "AnonymousIPList"
```

```
        },
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "HostingProviderIPList"
        }
      ],
      "ExcludedRules": []
    }
  },
```

규칙 작업 재정의에 대한 자세한 내용은 규칙 그룹에 대한 규칙 작업 재정의 섹션을 참조하세요.

자체 규칙 그룹의 경우 규칙 그룹 자체에서 규칙 작업을 수정하면 안 됩니다. Count 작업을 포함하는 규칙 그룹 규칙은 테스트에 필요한 지표 또는 기타 아티팩트를 생성하지 않습니다. 또한 규칙 그룹을 변경하면 해당 규칙을 사용하는 모든 웹 ACL에 영향을 미치는 반면, 웹 ACL 구성 내의 변경 사항은 단일 웹 ACL에만 영향을 미칩니다.

- 웹 ACL - 새 웹 ACL을 테스트하는 경우 요청을 허용하도록 웹 ACL의 기본 작업을 설정합니다. 이렇게 하면 트래픽에 영향을 주지 않고 웹 ACL을 테스트할 수 있습니다.

일반적으로 계산 모드는 프로덕션보다 더 많은 일치 항목을 생성합니다. 그 이유는 요청 수를 계산하는 규칙이 웹 ACL의 요청 평가를 중단하지 않으므로 웹 ACL에서 나중에 실행되는 규칙도 요청과 일치할 수 있기 때문입니다. 규칙 작업을 프로덕션 설정으로 변경하면 요청을 허용하거나 차단하는 규칙이 일치하는 요청에 대한 평가를 종료합니다. 따라서 일반적으로 웹 ACL에서 더 적은 규칙으로 일치 요청을 검사하게 됩니다. 규칙 작업이 웹 요청의 전체 평가에 미치는 영향에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.

이러한 설정을 사용하면 새 보호 기능이 웹 트래픽을 변경하지 않으면서 지표, 웹 ACL 로그 및 요청 샘플에서 일치 정보를 생성합니다.

3. 웹 ACL을 리소스와 연결

   웹 ACL이 아직 리소스와 연결되지 않은 경우, 웹 ACL을 연결합니다.

   웹 ACL을 리소스와 연결 또는 연결 해제 AWS를 참조하세요.

이제 웹 ACL을 모니터링하고 조정할 준비가 되었습니다.

모니터링 및 조정

이 섹션에서는 AWS WAF 보호 기능을 모니터링하고 조정하는 방법을 설명합니다.

> **Note**
>
> 이 섹션의 지침을 따르려면 웹 ACL, 규칙, 규칙 그룹과 같은 AWS WAF 보호를 생성하고 관리하는 방법을 일반적으로 이해해야 합니다. 이 정보는 이 가이드의 이전 섹션에 설명되어 있습니다.

웹 트래픽과 규칙 일치를 모니터링하여 웹 ACL의 동작을 확인합니다. 문제가 발견되면 규칙을 조정하여 수정하고 나서 모니터링하여 조정 사항을 확인합니다.

웹 ACL이 필요에 맞게 웹 트래픽을 관리할 때까지 다음 절차를 반복합니다.

모니터링하고 조정하려면

1. 트래픽과 규칙 일치 모니터링

   트래픽 흐름이 존재하고 테스트 규칙에서 일치하는 요청을 찾고 있는지 확인합니다.

   테스트 중인 보호 기능에 대한 다음 정보를 찾아 봅니다.

   - 로그 - 웹 요청과 일치하는 규칙에 대한 정보에 액세스합니다.
     - 규칙 - 웹 ACL에서 Count 작업이 있는 규칙이 `nonTerminatingMatchingRules` 아래에 나열됩니다. Allow 또는 Block을 포함하는 규칙은 `terminatingRule`로 나열됩니다. CAPTCHA 또는 Challenge를 포함하는 규칙은 종료형 또는 비 종료형일 수 있으므로 규칙 일치 결과에 따라 두 범주 중 하나에 나열됩니다.
     - 규칙 그룹 - 규칙 그룹은 `ruleGroupId` 필드에서 식별되며, 해당 규칙 일치 항목은 독립형 규칙과 동일하게 분류됩니다.
     - 레이블 - 규칙이 요청에 적용한 레이블이 `Labels` 필드에 나열됩니다.

     자세한 정보는 로그 필드을 참조하세요.
   - Amazon CloudWatch 지표 — 웹 ACL 요청 평가를 위해 다음 지표에 액세스할 수 있습니다.
     - 규칙 — 지표는 규칙 조치별로 그룹화됩니다. 예를 들어, Count 모드에서 규칙을 테스트하면 일치하는 규칙이 웹 ACL의 `Count` 지표로 나열됩니다.
     - 규칙 그룹 — 규칙 그룹의 지표는 규칙 그룹 지표 아래에 나열됩니다.

- 다른 계정이 소유한 규칙 그룹 - 규칙 그룹 지표는 일반적으로 규칙 그룹 소유자만 볼 수 있습니다. 하지만 규칙에 대한 규칙 동작을 재정의하면 해당 규칙의 지표가 웹 ACL 지표 아래에 나열됩니다. 또한 모든 규칙 그룹에서 추가한 레이블은 웹 ACL 지표에 나열됩니다.

  이 범주의 규칙 그룹은 다른 계정에서 공유한 AWS 에 대한 관리형 규칙 AWS WAF AWS Marketplace 관리형 규칙 그룹다른 서비스에서 제공하는 규칙 그룹,, 및 규칙 그룹입니다.
- 레이블 - 평가 중에 웹 요청에 추가된 레이블은 웹 ACL 레이블 지표에 나열됩니다. 레이블이 자신의 규칙 및 규칙 그룹에 의해 추가되었는지 또는 다른 계정이 소유한 규칙 그룹의 규칙에 의해 추가되었는지에 관계없이 모든 레이블의 지표에 액세스할 수 있습니다.

자세한 정보는 웹 ACL 지표 보기을 참조하세요.

- 웹 ACL 트래픽 개요 대시보드 - AWS WAF 콘솔의 웹 ACL 페이지로 이동한 다음 트래픽 개요 탭을 열어 웹 ACL이 평가한 웹 트래픽의 요약에 액세스할 수 있습니다.

  트래픽 개요 대시보드는 애플리케이션 웹 트래픽을 평가할 때 AWS WAF 수집하는 Amazon CloudWatch 지표의 요약을 거의 실시간으로 제공합니다.

  자세한 정보는 웹 ACL 트래픽 개요 대시보드을 참조하세요.
- 샘플링된 웹 요청 - 웹 요청 샘플과 일치하는 규칙에 대한 액세스 정보입니다. 샘플 정보는 웹 ACL의 규칙에 대한 지표 이름으로 일치 규칙을 식별합니다. 규칙 그룹의 경우 지표는 규칙 그룹 참조 문을 식별합니다. 규칙 그룹 내 규칙의 경우 샘플에는 `RuleWithinRuleGroup`의 일치하는 규칙 이름이 나열됩니다.

  자세한 정보는 웹 요청 샘플 보기을 참조하세요.

2. 거짓 긍정을 해결하기 위한 완화 조치 구성

   규칙이 일치되어서는 안 되는 웹 요청과 일치되어 거짓 긍정이 발생하고 있다고 판단되는 경우, 다음 옵션을 통해 웹 ACL 보호를 조정하여 이 문제를 완화할 수 있습니다.

   규칙 검사 기준 수정

   자체 규칙의 경우 대체로 웹 요청을 검사하는 데 사용하는 설정을 조정하기만 하면 됩니다. 예로는 정규식 패턴 집합의 사양을 변경하거나, 검사 전에 요청 구성 요소에 적용하는 텍스트 변환을 조정하거나, 전달된 IP 주소를 사용하도록 전환하는 것 등이 있습니다. 문제를 일으키는 규칙 유형에 대한 지침은 규칙 문 기본 사항 섹션을 참조하세요.

   더 복잡한 문제 해결

제어할 수 없는 검사 기준과 일부 복잡한 규칙의 경우 요청을 명시적으로 허용 또는 차단하거나 문제가 되는 규칙에 의한 평가에서 요청을 제외하는 규칙을 추가하는 등 기타 변경을 수행해야 할 수 있습니다. 관리형 규칙 그룹에는 대체로 이러한 유형의 완화가 필요하지만 다른 규칙에도 필요할 수 있습니다. 속도 기반 규칙 문 및 SQL 명령어 삽입 공격 규칙 문을 예로 들 수 있습니다.

거짓 긍정을 줄이기 위해 수행하는 작업은 사용 사례에 따라 다릅니다. 다음은 일반적인 접근 방식입니다.

- 완화 규칙 추가 - 새 규칙보다 먼저 실행되고 거짓 긍정을 유발하는 요청을 명시적으로 허용하는 규칙을 추가합니다. 웹 ACL의 규칙 평가 순서에 대한 자세한 내용은 웹 ACL의 규칙 및 규칙 그룹 처리 순서 섹션을 참조하세요.

  이 방법을 사용하면 허용된 요청이 보호된 리소스로 전송되므로 새 평가 규칙에 도달하지 않습니다. 새 규칙이 유료 관리형 규칙 그룹인 경우 이 방법은 규칙 그룹의 사용 비용을 억제하는 데도 도움이 될 수 있습니다.

- 완화 규칙을 포함하는 논리적 규칙 추가 - 논리적 규칙 문을 사용하여 거짓 긍정을 배제하는 규칙과 새 규칙을 결합할 수 있습니다. 자세한 내용은 논리적 규칙 문을 참조하세요.

  예를 들어 요청 범주에 대해 거짓 긍정을 생성하는 SQL 명령어 삽입 공격 일치 문을 추가한다고 가정해 보겠습니다. 이러한 요청과 일치하는 규칙을 만든 다음 논리적 규칙 문을 사용하는 규칙을 결합하면 둘 다 거짓 긍정 기준과 일치하지 않고 SQL 명령어 삽입 공격 기준과 일치하는 요청만 일치하게 됩니다.

- 범위 축소 문 추가 - 속도 기반 문 및 관리형 규칙 그룹 참조 문의 경우 주 명령문 안에 범위 축소 문을 추가하여 거짓 긍정이 발생하는 요청을 평가 대상에서 제외합니다.

  범위 축소 문과 일치하지 않는 요청은 규칙 그룹 또는 속도 기반 평가에 절대 도달하지 않습니다. 범위 축소 문에 대한 자세한 내용은 범위 축소 문 섹션을 참조하세요. 예시는 봇 관리에서 IP 범위 제외을 확인하세요.

- 레이블 일치 규칙 추가 - 레이블 지정을 사용하는 규칙 그룹의 경우 문제가 되는 규칙이 요청에 적용하는 레이블을 식별합니다. 규칙 그룹 규칙을 계산 모드에서 설정해야 할 수도 있습니다(아직 설정하지 않은 경우). 문제가 되는 규칙에 의해 추가되는 레이블과 일치하며 규칙 그룹 다음에 실행되도록 배치된 레이블 일치 규칙을 추가합니다. 레이블 일치 규칙에서 허용하려는 요청과 차단하려는 요청을 필터링할 수 있습니다.

  이 방법을 사용하는 경우 테스트를 마쳤을 때 문제가 되는 규칙을 규칙 그룹에서 계산 모드로 유지하고 사용자 지정 레이블 일치 규칙을 그대로 유지합니다. 레이블 일치 문에 대한 자세한 내용

은 레이블 일치 규칙 문 섹션을 참조하세요. 예제는 차단된 특정 봇 허용 및 ATP 예제: 분실 및 손상된 보안 인증 정보에 대한 사용자 지정 처리 단원을 참조하세요.

- 관리형 규칙 그룹 버전 변경 - 버전이 지정된 관리형 규칙 그룹의 경우 사용 중인 버전을 변경합니다. 예를 들어, 성공적으로 사용하고 있던 마지막 정적 버전으로 다시 전환할 수 있습니다.

  이는 일반적으로 임시 해결책입니다. 테스트 또는 스테이징 환경에서 최신 버전을 계속 테스트하거나 공급자로부터 호환성이 더 좋은 버전을 기다리는 동안 프로덕션 트래픽의 버전을 변경할 수 있습니다. 관리형 규칙 그룹에 대한 자세한 내용은 관리형 규칙 그룹 섹션을 참조하세요.

새 규칙이 필요한 요청과 일치하는 것으로 확인되면 테스트의 다음 단계로 이동하여 이 절차를 반복합니다. 프로덕션 환경에서 테스트 및 조정의 마지막 단계를 수행하십시오.

웹 ACL 지표 보기

웹 ACL을 하나 이상의 AWS 리소스와 연결한 후 Amazon CloudWatch 그래프에서 연결에 대한 결과 지표를 볼 수 있습니다.

AWS WAF 지표에 대한 자세한 내용은 을 참조하십시오AWS WAF 지표 및 차원. CloudWatch 지표에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

웹 ACL의 각 규칙과 관련 리소스가 웹 AWS WAF ACL에 전달하는 모든 요청에 대해 다음을 CloudWatch 수행할 수 있습니다.

- 이전 한 시간 또는 이전 세 시간 동안의 데이터 보기
- 데이터 요소 간의 간격 변경
- 데이터에 대해 CloudWatch 수행하는 계산 (예: 최대값, 최소값, 평균 또는 합계) 을 변경합니다.

> **Note**
>
> AWS WAF with CloudFront 는 글로벌 서비스이며 지표는 에서 미국 동부 (버지니아 북부) 지역을 선택한 경우에만 사용할 수 있습니다. AWS Management Console다른 지역을 선택하면 CloudWatch 콘솔에 AWS WAF 지표가 표시되지 않습니다.

웹 ACL에서 규칙에 대한 데이터를 보려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.

2. 필요한 경우 해당 지역을 AWS 리소스가 위치한 지역으로 변경하십시오. 에서 미국 동부 (버지니아 북부) 지역을 선택합니다. CloudFront
3. 탐색 창의 지표에서 모든 지표를 선택한 다음 찾아보기 탭에서 `AWS::WAFV2`를 검색하십시오.
4. 데이터를 보려는 웹 ACL의 확인란을 선택합니다.
5. 해당되는 설정을 변경합니다.

   통계

   데이터에 대해 CloudWatch 수행할 계산을 선택합니다.

   시간 범위

   이전 한 시간 동안의 데이터를 볼지 또는 이전 세 시간 동안의 데이터를 볼지를 선택합니다.

   기간

   그래프에서 데이터 요소 간의 간격을 선택합니다.

   규칙

   데이터를 보려는 규칙을 선택합니다.

   > **Note**
   >
   > 규칙 이름을 변경하고 규칙의 지표 이름에 변경 내용이 반영되도록 하려면 지표 이름도 업데이트해야 합니다. AWS WAF 규칙 이름을 변경할 때 규칙의 지표 이름을 자동으로 업데이트하지 않습니다. 콘솔에서 규칙을 편집할 때 규칙 JSON 편집기를 사용하여 지표 이름을 변경할 수 있습니다. API와 웹 ACL 또는 규칙 그룹을 정의하는 데 사용하는 JSON 목록을 통해 두 이름을 모두 변경할 수도 있습니다.

   유념할 사항:

   - 최근에 웹 ACL을 AWS 리소스와 연결한 경우 그래프에 데이터가 나타나고 사용 가능한 지표 목록에 웹 ACL에 대한 지표가 나타날 때까지 몇 분 정도 기다려야 할 수 있습니다.
   - 둘 이상의 리소스를 웹 ACL과 연결하는 경우 CloudWatch 데이터에는 모든 리소스에 대한 요청이 포함됩니다.
   - 데이터 요소 위에 커서를 놓으면 추가 정보를 볼 수 있습니다.

- 그래프는 자동으로 새로 고침되지 않습니다. 표시 내용을 업데이트하려면 새로 고침 () 아이콘을 선택합니다.

CloudWatch 지표에 대한 자세한 내용은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.

웹 ACL 트래픽 개요 대시보드

이 섹션에서는 콘솔의 웹 ACL 트래픽 개요 대시보드에 대해 설명합니다. AWS WAF 웹 ACL을 하나 이상의 AWS 리소스와 연결하고 웹 ACL에 대한 메트릭을 활성화한 후에는 콘솔에서 웹 ACL의 트래픽 개요 탭으로 이동하여 웹 ACL이 평가하는 웹 트래픽 요약에 액세스할 수 있습니다. AWS WAF 대시보드에는 애플리케이션 웹 트래픽을 평가할 때 AWS WAF 수집하는 Amazon CloudWatch 지표의 거의 실시간 요약이 포함됩니다.

> **Note**
>
> 대시보드에 아무것도 표시되지 않는 경우 웹 ACL에 대한 지표가 활성화되어 있는지 확인하십시오.

웹 ACL의 트래픽 개요 탭에는 다음 정보 범주에 대한 탭으로 구분된 대시보드가 포함됩니다.

- 모든 트래픽 - 웹 ACL이 평가하는 모든 웹 요청입니다.

  대시보드는 작업 종료에 초점을 맞추고 있으나 다음 위치에서 카운트 규칙과 일치하는 항목을 볼 수 있습니다.
  - 이 대시보드의 상위 10개 규칙 창. 카운트 동작으로 전환을 토글하여 일치하는 카운트 규칙을 표시합니다.
  - 웹 ACL 페이지의 샘플 요청 탭 이 새 탭에는 모든 규칙 일치 그래프가 포함됩니다. 자세한 내용은 웹 요청 샘플 보기을 참조하세요.
- Bot Control - 웹 ACL이 Bot Control 관리형 규칙 그룹을 사용하여 평가하는 웹 요청입니다.

  웹 ACL에서 이 규칙 그룹을 사용하지 않는 경우 이 탭에는 Bot Control 규칙에 대한 웹 트래픽 샘플을 평가한 결과가 표시됩니다. 무료로 제공되는 이 기능을 통해 애플리케이션에서 수신되는 봇 트래픽을 파악할 수 있습니다.

  이 규칙 그룹은 제공하는 지능형 위협 완화 옵션의 일부입니다. AWS WAF 자세한 내용은 AWS WAF 봇 컨트롤 및 AWS WAF 봇 컨트롤 규칙 그룹 섹션을 참조하세요.

- 계정 탈취 방지 — 웹 ACL이 AWS WAF 사기 통제 계정 도용 방지 (ATP) 관리 규칙 그룹을 사용하여 평가하는 웹 요청입니다. 이 탭은 웹 ACL에서 이 규칙 그룹을 사용하는 경우에만 사용할 수 있습니다.

  ATP 규칙 그룹은 AWS WAF 지능형 위협 완화 제공의 일부입니다. 자세한 내용은 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 및 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹 섹션을 참조하세요.
- 계정 생성 사기 방지 — 웹 ACL이 사기 통제 계정 생성 AWS WAF 사기 방지 (ACFP) 관리 규칙 그룹을 사용하여 평가하는 웹 요청입니다. 이 탭은 웹 ACL에서 이 규칙 그룹을 사용하는 경우에만 사용할 수 있습니다.

  ACFP 규칙 그룹은 AWS WAF 지능형 위협 완화 제공의 일부입니다. 자세한 내용은 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 및 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP) 규칙 그룹 섹션을 참조하세요.

대시보드는 웹 ACL의 CloudWatch 지표를 기반으로 하며 그래프를 통해 의 해당 지표에 액세스할 수 있습니다. CloudWatch Bot Control과 같은 지능형 위협 완화 대시보드의 경우 사용되는 지표는 주로 레이블 지표입니다.

- AWS WAF 제공하는 지표 목록은 을 참조하십시오. AWS WAF 지표 및 차원
- CloudWatch 지표에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

대시보드는 선택한 종료 작업과 날짜 범위에 대한 트래픽 패턴의 요약을 제공합니다. 지능형 위협 완화 대시보드에는 관리형 규칙 그룹 자체가 종료 작업을 적용하는지 여부와 상관없이 해당 관리형 규칙 그룹에서 평가되는 요청이 포함됩니다. 예를 들어 Block을 선택하면 ATP 관리형 규칙 그룹에서 평가되었다가 웹 ACL 평가 중 특정 시점에 차단된 모든 웹 요청에 대한 정보가 계정 도용 방지 대시보드에 포함됩니다. 요청은 ATP 관리형 규칙 그룹, 웹 ACL의 규칙 그룹 이후에 실행된 규칙 또는 웹 ACL 기본 작업에 의해 차단될 수 있습니다.

웹 ACL의 대시보드 보기

이 섹션의 절차에 따라 웹 ACL 대시보드에 액세스하고 데이터 필터링 기준을 설정합니다. 최근에 웹 ACL을 AWS 리소스와 연결한 경우 대시보드에서 데이터를 사용할 수 있을 때까지 몇 분 정도 기다려야 할 수 있습니다.

대시보드에는 웹 ACL과 연결된 모든 리소스에 대한 요청이 포함됩니다.

웹 ACL용 트래픽 개요 대시보드를 보려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 웹 ACL을 선택한 다음 찾아볼 웹 ACL을 검색합니다.
3. 웹 ACL을 선택합니다. 콘솔에서 웹 ACL 페이지로 이동합니다. 트래픽 개요 탭이 기본적으로 선택되어 있습니다.
4. 필요에 따라 데이터 필터 설정을 변경합니다.

    - 종료 규칙 작업 - 대시보드에 포함할 종료 작업을 선택합니다. 대시보드에 웹 ACL 평가를 통해 선택한 작업 중 하나가 적용된 웹 요청에 대한 지표가 요약됩니다. 사용 가능한 작업을 모두 선택하면 평가된 모든 웹 요청이 대시보드에 포함됩니다. 작업에 대한 자세한 내용은 웹 ACL에서 규칙 및 규칙 그룹 작업을 AWS WAF 처리하는 방법 섹션을 참조하세요.
    - 시간 범위 - 대시보드에서 확인할 시간 간격을 선택합니다. 예를 들어 최근 3시간 또는 지난 주와 같이 현재를 기준으로 한 기간을 표시하도록 선택한 후, 달력에서 절대 시간 범위를 선택할 수 있습니다.
    - 시간대 - 이 설정은 절대 시간 범위를 지정할 때 적용됩니다. 브라우저의 현지 시간대 또는 UTC(협정 세계시)를 사용할 수 있습니다.

원하는 탭의 정보를 검토합니다. 데이터 필터 선택은 모든 대시보드에 적용됩니다. 그래프 창에서 데이터 포인트 또는 영역을 커서로 가리키면 추가 세부 정보를 볼 수 있습니다.

Count 작업 규칙

두 위치 중 하나에서 작업 일치 횟수에 대한 정보를 볼 수 있습니다.

- 이 트래픽 개요 탭의 모든 트래픽 대시보드에서 상위 10개 규칙 창을 찾아 실행 횟수로 전환을 토글합니다. 이 토글을 켜면 창에 종료 규칙 일치 대신 규칙 일치 개수가 표시됩니다.
- 웹 ACL의 샘플링된 요청 탭에서 트래픽 개요 탭에서 설정한 시간 범위에 대한 모든 규칙 일치 및 조치의 그래프를 볼 수 있습니다. 샘플링된 요청 탭에 대한 내용은 웹 요청 샘플 보기을(를) 참조하세요.

아마존 CloudWatch 메트릭스

대시보드 그래프 창에서 그래프로 표시된 데이터의 CloudWatch 지표에 액세스할 수 있습니다. 그래프 창 상단이나 창 내의 :(세로 생략 부호) 드롭다운 메뉴에서 옵션을 선택합니다.

대시보드 새로 고침

대시보드는 자동으로 새로 고쳐지지 않습니다. 표시 내용을 업데이트하려면 새로 고침  아이콘을 선택합니다.

웹 ACL용 트래픽 개요 대시보드의 예제

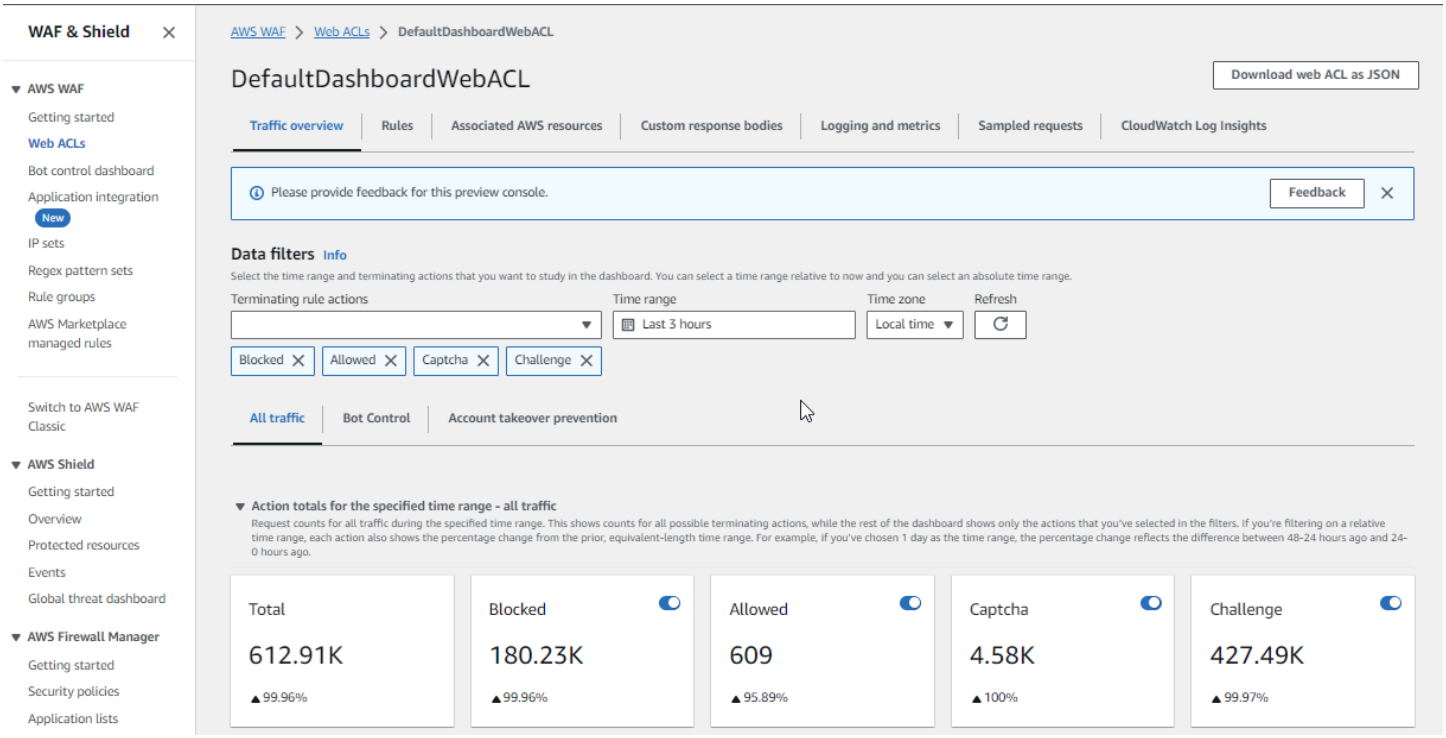
이 섹션에서는 웹 ACL용 트래픽 개요 대시보드의 예제 화면을 보여줍니다.

> **Note**
>
> 애플리케이션 리소스를 보호하기 AWS WAF 위해 이미 사용하고 있는 경우 콘솔의 해당 페이지에서 모든 웹 ACL의 대시보드를 볼 수 있습니다. AWS WAF 자세한 내용은 웹 ACL의 대시보드 보기을 참조하세요.

예제 화면: 데이터 필터 및 모든 트래픽 대시보드 작업 개수

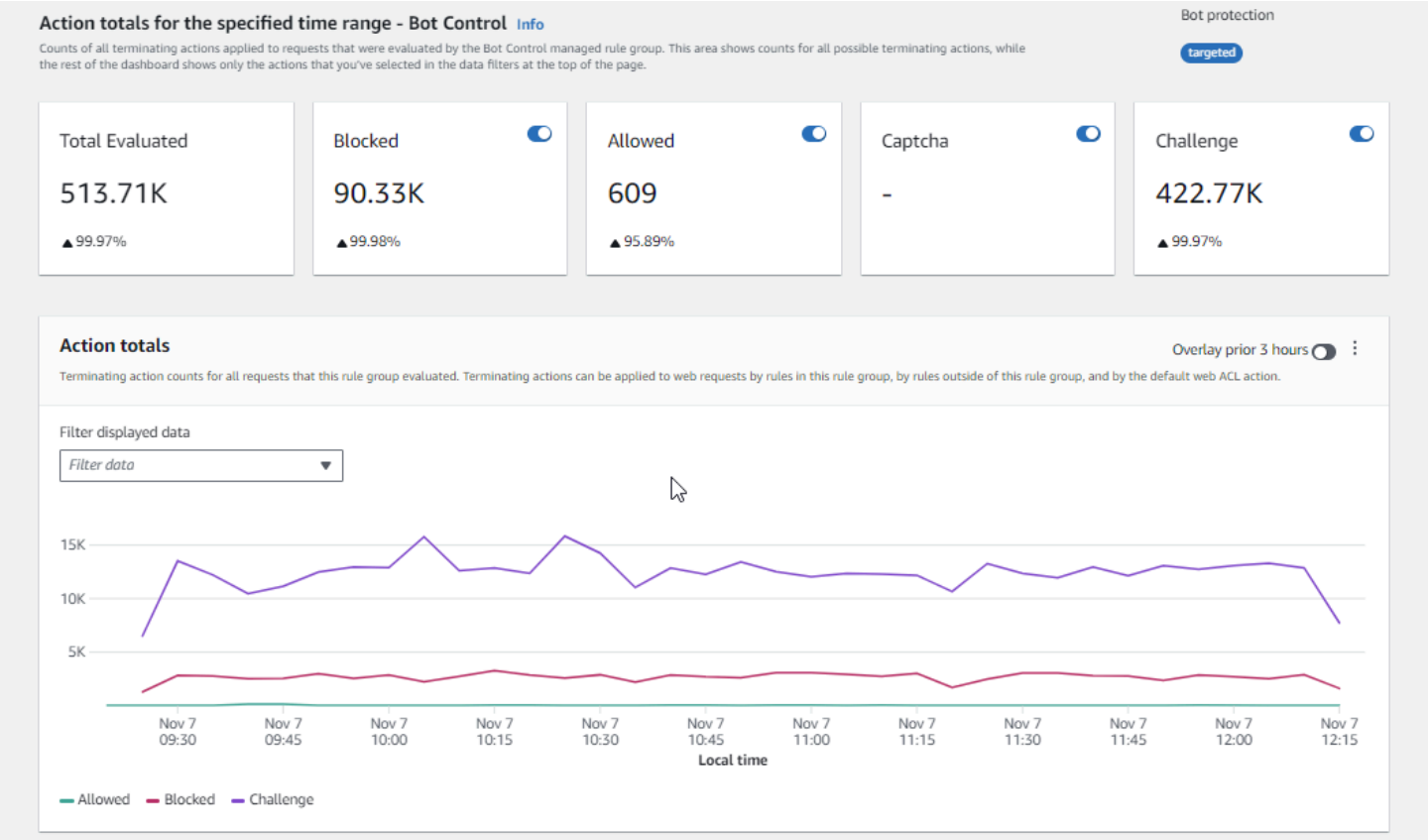
다음 스크린샷은 모든 트래픽 탭이 선택된 웹 ACL의 트래픽 개요를 보여줍니다. 데이터 필터는 지난 3시간 동안의 모든 종료 작업(기본값)으로 설정되어 있습니다.

전체 트래픽 대시보드 안에는 다양한 종료 작업에 대한 작업 합계가 표시됩니다. 각 창에는 요청 개수가 나열되고 이전 3시간 범위 이후의 변경을 나타내는 위쪽/아래쪽 화살표가 표시됩니다.



예제 화면: Bot Control 대시보드 작업 수

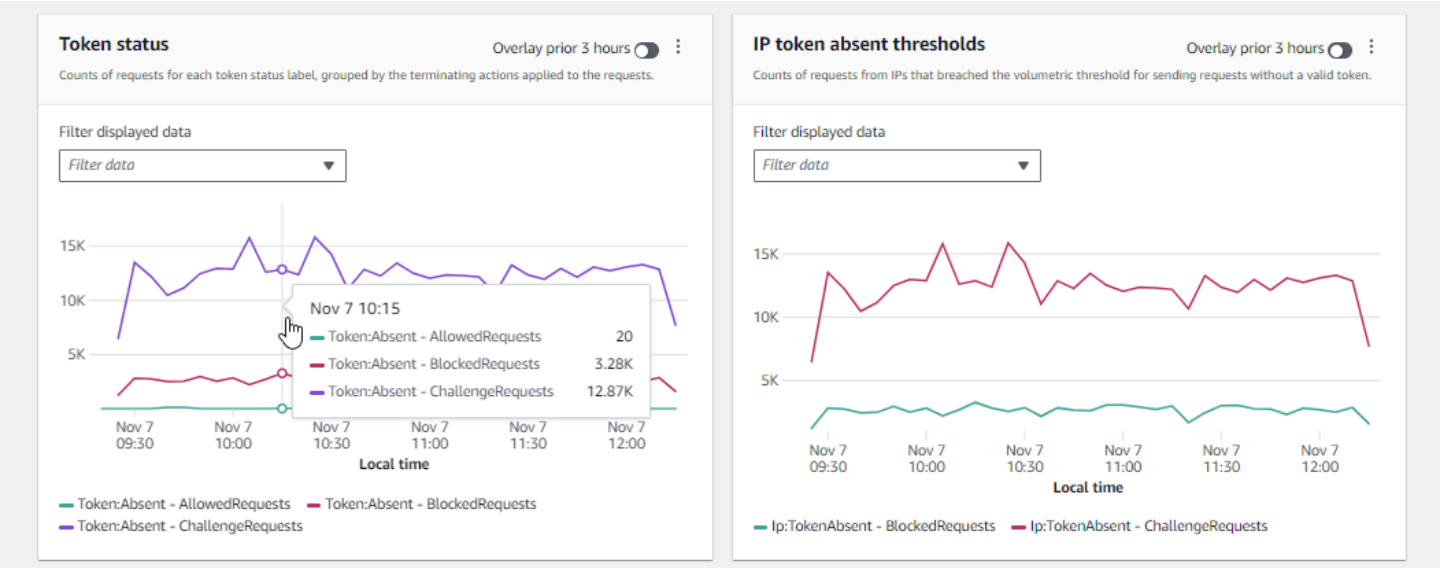
다음 스크린샷은 Bot Control 대시보드의 작업 수를 보여줍니다. 이 그림은 시간 범위에 대해 동일한 총계 창을 보여주지만, 개수는 Bot Control 규칙 그룹이 평가한 요청의 수만 표시합니다. 더 아래쪽에 있는 작업 합계 창에서는 지정된 3시간 범위 동안의 작업 수를 볼 수 있습니다. 이 기간 동안에는 규칙 그룹이 평가한 어떤 요청에도 CAPTCHA 작업이 적용되지 않았습니다.



예제 화면: Bot Control 대시보드 토큰 상태 요약 그래프

다음 스크린샷은 Bot Control 대시보드에서 사용할 수 있는 두 가지 요약 그래픽을 보여줍니다. 토큰 상태 창에는 요청에 적용된 규칙 작업과 함께 다양한 토큰 상태 레이블 개수가 표시됩니다. IP 토큰 없는 임계값 창에는 토큰 없이 너무 많은 요청을 보낸 IP의 요청에 대한 데이터가 표시됩니다.

그래프의 아무 영역이나 마우스로 가리키면 사용 가능한 세부 정보가 표시됩니다. 이 스크린샷의 토큰 상태 창에서 마우스로 그래프 선이 아닌 특정 시점을 가리키면 콘솔에 해당 시점의 모든 라인에 대한 데이터가 표시됩니다.



이 섹션에서는 웹 ACL 트래픽 개요 대시보드에 제공되는 몇 가지 트래픽 요약만 보여줍니다. 웹 ACL의 대시보드를 보려면 콘솔에서 웹 ACL 페이지를 엽니다. 이를 위한 자세한 방법은 웹 ACL의 대시보드 보기 섹션을 참조하세요.

웹 요청 샘플 보기

이 섹션에서는 콘솔의 웹 ACL 샘플 요청 탭에 대해 설명합니다. AWS WAF 이 탭에서는 검사된 웹 요청과 일치하는 모든 규칙의 그래프를 볼 수 있습니다. AWS WAF 또한 웹 ACL에 요청 샘플링을 활성화한 경우 검사한 웹 요청 샘플의 테이블 보기를 볼 수 있습니다. AWS WAF API 호출을 통해 샘플링된 요청 정보를 검색할 수도 있습니다. `GetSampledRequests`

요청 샘플에는 웹 ACL의 규칙에 대한 기준과 일치하는 최대 100개의 요청과 규칙과 일치하지 않고 웹 ACL 기본 작업이 적용된 요청에 대한 다른 100개의 요청이 포함되어 있습니다. 샘플의 요청은 이전 3시간 동안 콘텐츠에 대해 요청을 수신한 모든 보호된 리소스에서 나옵니다.

웹 요청이 규칙의 기준과 일치하고 해당 규칙에 대한 작업으로 요청 평가가 종료되지 않는 경우 웹 ACL의 후속 규칙을 사용하여 웹 요청을 AWS WAF 계속 검사합니다. 이로 인해 웹 요청이 여러 번 나타날 수 있습니다. 규칙 작업 동작에 관한 내용은 규칙 작업을(를) 참조하세요.

모든 규칙 그래프와 샘플링된 요청을 보려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. 요청을 보려는 웹 ACL의 이름을 선택합니다. 콘솔에서 웹 ACL의 설명으로 이동하여 여기에서 설명을 편집할 수 있습니다.

4. 샘플링된 요청 탭에서 다음을 확인할 수 있습니다.

   - 모든 규칙 그래프 - 이 그래프는 표시된 시간 범위 동안 수행된 모든 웹 요청 평가에 대한 일치 규칙 및 규칙 작업을 보여줍니다.

     > **Note**
     >
     > 이 그래프에 대한 시간 범위는 데이터 필터 섹션에 있는 웹 ACL의 트래픽 개요 탭에서 설정됩니다. 자세한 내용은 웹 ACL의 대시보드 보기을 참조하세요.

   - 샘플링된 요청 테이블 – 이 테이블에는 지난 3시간 동안 샘플링된 요청 데이터가 표시됩니다. 테이블에는 각 항목에 대해 다음 데이터가 표시됩니다.

     지표 이름

     요청과 일치하는 웹 ACL 규칙의 CloudWatch 메트릭 이름. 웹 요청이 웹 ACL의 어떤 규칙과도 일치하지 않는 경우 이 값은 기본값입니다.

     > **Note**
     >
     > 규칙 이름을 변경하고 규칙의 지표 이름에 변경 내용이 반영되도록 하려면 지표 이름도 업데이트해야 합니다. AWS WAF 규칙 이름을 변경할 때 규칙의 지표 이름을 자동으로 업데이트하지 않습니다. 콘솔에서 규칙을 편집할 때 규칙 JSON 편집기를 사용하여 지표 이름을 변경할 수 있습니다. API와 웹 ACL 또는 규칙 그룹을 정의하는 데 사용하는 JSON 목록을 통해 두 이름을 모두 변경할 수도 있습니다.

     소스 IP

     요청이 시작된 IP 주소 또는 최종 사용자가 HTTP 프록시나 Application Load Balancer를 사용하여 요청을 전송한 경우 프록시 또는 Application Load Balancer의 IP 주소입니다.

     URI

     리소스를 식별하는 URL의 부분입니다(예: `/images/daily-ad.jpg`).

     규칙 그룹 내부 규칙

     지표 이름이 규칙 그룹 참조 문을 식별하는 경우 이 항목은 규칙 그룹 내부에서 요청과 일치했던 규칙을 식별합니다.

작업

해당 규칙에 대한 작업을 나타냅니다. 가능한 규칙 작업에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.

Time

보호된 리소스로부터 요청을 AWS WAF 받은 시간.

웹 요청 구성 요소에 대한 추가 정보를 표시하려면 해당 요청의 행에서 URI 이름을 선택합니다.

프로덕션 환경에서 보호 기능을 활성화하십시오

프로덕션 환경에서 테스트 및 튜닝의 최종 단계를 완료했으면 프로덕션 모드에서 보호 기능을 활성화하십시오.

프로덕션 트래픽 위험

프로덕션 트래픽용 웹 ACL 구현을 배포하기 전에 트래픽에 대한 잠재적 영향을 파악할 때까지 테스트 환경에서 이를 테스트하고 조정합니다. 또한 프로덕션 트래픽에 대한 보호를 활성화하기 전에 프로덕션 트래픽을 사용하여 계산 모드에서 트래픽을 테스트 및 조정합니다.

Note

이 섹션의 지침을 따르려면 웹 ACL, 규칙, 규칙 그룹과 같은 AWS WAF 보호를 생성하고 관리하는 방법을 일반적으로 이해해야 합니다. 이 정보는 이 가이드의 이전 섹션에 설명되어 있습니다.

이러한 단계를 먼저 테스트 환경에서 수행한 다음, 프로덕션 환경에서 수행합니다.

프로덕션 환경에서 AWS WAF 보호 기능을 활성화하세요.

1. 프로덕션 보호 기능으로 전환

   웹 ACL을 업데이트하고 프로덕션 설정을 전환합니다.

a. 필요하지 않은 테스트 규칙을 모두 제거합니다.

   프로덕션 환경에서 필요하지 않은 테스트 규칙을 추가했다면 삭제합니다. 레이블 일치 규칙을 사용하여 관리형 규칙 그룹 규칙의 결과를 필터링하는 경우 해당 규칙을 그대로 두어야 합니다.

b. 프로덕션 작업으로 전환

   새 규칙의 작업 설정을 의도한 프로덕션 설정으로 변경합니다.

   - 웹 ACL에 정의된 규칙 - 웹 ACL에서 규칙을 편집하고 Count의 작업을 해당 프로덕션 작업으로 변경합니다.
   - 규칙 그룹 - 규칙 그룹의 웹 ACL 구성에서 테스트 및 조정 활동의 결과에 따라 자체 작업을 사용하는 규칙으로 전환하거나 규칙을 그대로 유지하면서 Count 작업을 재정의합니다. 레이블 일치 규칙을 사용하여 규칙 그룹 규칙의 결과를 필터링하는 경우 해당 규칙에 대한 재정의를 그대로 두어야 합니다.

     규칙의 작업을 사용하도록 전환하려면 웹 ACL 구성에서 규칙 그룹의 규칙 문을 편집하고 규칙에 대한 Count 재정의를 제거합니다. JSON에서 웹 ACL을 관리하는 경우 규칙 그룹 참조 문에서 `RuleActionOverrides` 목록의 규칙 항목을 제거합니다.
   - 웹 ACL - 테스트의 웹 ACL 기본 작업을 변경한 경우 프로덕션 설정으로 전환합니다.

   이러한 설정을 사용하면 새로운 보호 기능이 웹 트래픽을 의도한 대로 관리하게 됩니다.

   웹 ACL을 저장하면 연결된 리소스가 프로덕션 설정을 사용하게 됩니다.

2. 모니터링 및 조정

   웹 요청이 원하는 대로 처리되도록 하려면 새 기능을 활성화한 후 트래픽을 면밀히 모니터링합니다. 조정 작업에서 모니터링하던 계산 작업 대신 프로덕션 규칙 작업에 대한 지표와 로그를 모니터링하게 됩니다. 계속 모니터링하면서 필요에 따라 동작을 조정하여 웹 트래픽의 변화에 맞춥니다.

Amazon CloudFront 기능 사용 방법 AWS WAF

웹 ACL을 생성할 때 AWS WAF 검사하려는 하나 이상의 CloudFront 배포를 지정할 수 있습니다. AWS WAF 웹 ACL에서 식별한 기준에 따라 해당 배포에 대한 웹 요청을 검사 및 관리하기 시작합니다. CloudFront 기능을 향상시키는 몇 가지 기능을 제공합니다. AWS WAF 이 장에서는 공동 작업을 더 잘

CloudFront 만들고 더 잘 CloudFront AWS WAF 작동하도록 구성할 수 있는 몇 가지 방법을 설명합니다.

주제

CloudFront 사용자 지정 오류 AWS WAF 페이지와 함께 사용

기본적으로 지정한 기준에 따라 웹 요청을 AWS WAF 차단하면 뷰어에 HTTP 상태 코드가 반환되고 `403 (Forbidden)` 뷰어에게 CloudFront 해당 상태 코드가 CloudFront 반환됩니다. 최종 사용자에게는 다음과 유사한 짧고 불완전한 형식의 기본 메시지가 표시됩니다.

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

사용자 지정 응답을 정의하여 AWS WAF 웹 ACL 규칙에서 이 동작을 재정의할 수 있습니다. AWS WAF 규칙을 사용하여 응답 동작을 사용자 지정하는 방법에 대한 자세한 내용은 을 참조하십시오. Block 작업에 대한 사용자 지정 응답

> **Note**
>
> AWS WAF 규칙을 사용하여 사용자 지정하는 응답은 사용자 CloudFront 지정 오류 페이지에 정의한 응답 사양보다 우선합니다.

웹 사이트의 나머지 부분과 동일한 형식을 사용하여 사용자 지정 오류 메시지를 표시하려는 경우 사용자 지정 오류 메시지가 포함된 개체 (예: HTML 파일) 를 CloudFront 뷰어에 CloudFront 반환하도록 구성할 수 있습니다.

> **Note**
>
> CloudFront 오리진에서 반환되는 HTTP 상태 코드 403과 요청이 AWS WAF 차단되었을 때 반환되는 HTTP 상태 코드 403을 구분할 수 없습니다. 따라서 HTTP 상태 코드 403의 다른 원인을 기반으로 다른 사용자 지정 오류 페이지를 반환할 수 없습니다.

CloudFront 사용자 지정 오류 페이지에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 사용자 지정 오류 응답 생성을 참조하십시오.

자체 HTTP 서버에서 실행되는 CloudFront 애플리케이션에 AWS WAF with 사용

를 AWS WAF 사용하면 CloudFront Amazon Elastic Compute Cloud (Amazon EC2) 에서 실행되는 웹 서버이든 비공개로 관리하는 웹 서버이든 관계없이 모든 HTTP 웹 서버에서 실행되는 애플리케이션을 보호할 수 있습니다. 또한 자체 웹 서버 간에는 물론 최종 사용자 CloudFront 간에도 HTTPS를 CloudFront 요구하도록 구성할 수 있습니다. CloudFront

자체 웹 서버와 웹 서버 간에 CloudFront HTTPS가 필요함

자체 웹 서버 간에 CloudFront HTTPS를 요구하려면 CloudFront 사용자 지정 오리진 기능을 사용하고 특정 오리진에 대한 오리진 프로토콜 정책 및 오리진 도메인 이름 설정을 구성할 수 있습니다. CloudFront 구성에서 오리진에서 객체를 가져올 때 사용할 포트 및 프로토콜과 함께 서버의 DNS 이름을 지정할 수 있습니다. CloudFront 또한 사용자 지정 오리진 서버의 SSL/TLS 인증서가 구성한 원본 도메인 이름과 일치하는지 확인해야 합니다. 외부에서 자체 HTTP 웹 서버를 사용하는 경우 Comodo 또는 Symantec과 같은 신뢰할 수 있는 타사 인증 기관 (CA) 에서 서명한 인증서를 사용해야 합니다. AWS DigiCert 자체 웹 서버 간 통신을 위해 HTTPS를 요구하는 방법에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 사용자 지정 CloudFront 오리진과 사용자 지정 오리진 간의 CloudFront 통신을 위한 HTTPS 요구 항목을 참조하십시오.

시청자와 사용자 간에 HTTPS를 요구합니다. CloudFront

최종 사용자 CloudFront 간에 HTTPS를 요구하려면 배포에서 하나 이상의 캐시 동작에 대한 뷰어 프로토콜 정책을 변경할 수 있습니다. CloudFront 최종 사용자와 최종 사용자 간 HTTPS 사용에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 “최종 사용자 간 통신을 위한 HTTPS 필요” 주제를 참조하십시오. CloudFront CloudFront 또한 자체 SSL 인증서를 가져와서 시청자가 자신의 도메인 이름 (예: https://www.mysite.com) 을 사용하여 HTTPS를 통해 CloudFront 배포에 연결할 수 있도록 할 수도 있습니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 대체 도메인 이름 및 HTTPS 구성 항목을 참조하십시오.

CloudFront응답하는 HTTP 메서드 선택

Amazon CloudFront 웹 배포를 생성할 때 처리하고 오리진에 CloudFront 전달하려는 HTTP 메서드를 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

- **`GET`**, **`HEAD`** — 오리진에서 객체를 가져오거나 객체 헤더를 가져오는 CloudFront 데만 사용할 수 있습니다.

- **GET**,**HEAD**, **OPTIONS** — 오리진에서 객체를 가져오거나, 객체 헤더를 가져오거나, 오리진 서버가 지원하는 옵션 목록을 검색하는 CloudFront 데만 사용할 수 있습니다.
- **GET**,**HEAD**,**OPTIONS**,**PUT**, **POSTPATCH**, **DELETE** — 객체를 가져오고, 추가하고, 업데이트하고, 삭제하고, 객체 헤더를 가져오는 CloudFront 데 사용할 수 있습니다. 또한 웹 양식에서 데이터를 제출하는 등의 기타 POST 작업을 수행할 수 있습니다.

에 설명된 대로 AWS WAF 바이트 일치 규칙 문을 사용하여 HTTP 메서드에 따라 요청을 허용하거나 차단할 수도 있습니다. 문자열 일치 규칙 문 GET및 와 HEAD 같이 CloudFront 지원하는 메서드를 조합하여 사용하려는 경우 다른 방법을 사용하는 요청을 AWS WAF 차단하도록 구성하지 않아도 됩니다. , GETHEAD, 같이 CloudFront 지원하지 않는 메서드의 조합을 허용하려면 모든 메서드에 CloudFront 응답하도록 구성한 다음 를 사용하여 다른 방법을 사용하는 요청을 AWS WAF 차단할 수 있습니다. POST

CloudFront 응답하는 메서드를 선택하는 방법에 대한 자세한 내용은 Amazon CloudFront Developer Guide의 웹 배포를 만들거나 업데이트할 때 지정하는 값 항목의 허용된 HTTP 메서드를 참조하십시오.

AWS WAF 서비스 사용 시 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

> **Note**
>
> 이 섹션에서는 AWS WAF 서비스 및 해당 AWS 리소스 (예: AWS WAF 웹 ACL 및 규칙 그룹) 사용에 대한 표준 AWS 보안 지침을 제공합니다.
> 를 사용하여 AWS AWS WAF리소스를 보호하는 방법에 대한 자세한 내용은 AWS WAF 가이드의 나머지 부분을 참조하십시오.

보안은 두 사람 AWS 사이의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오. AWS WAF

- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 데이터의 민감도, 조직의 요건 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 공동 책임 모델을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 AWS WAF됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 AWS WAF 충족하도록 구성하는 방법을 보여 줍니다. 또한 AWS WAF 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

의 데이터 보호 AWS WAF

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS WAF. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.

- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS WAF 또는 AWS 서비스 SDK를 사용하거나 다른 방법으로 작업하는 경우가 포함됩니다. AWS CLI AWS 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

AWS WAF 중국 (베이징), 중국 (닝샤) 등 암호화를 사용할 수 없는 특정 지역을 제외하고 웹 ACL, 규칙 그룹, IP 세트와 같은 엔티티는 저장 시 암호화됩니다. 리전마다 고유한 암호화 키가 사용됩니다.

AWS WAF 리소스 삭제

AWS WAF에서 생성하는 리소스를 삭제할 수 있습니다. 다음 섹션에 설명된 각 리소스 유형에 대한 지침을 참조하세요.

- 웹 ACL 삭제
- 규칙 그룹 삭제
- IP 집합 삭제
- 정규식 패턴 집합 삭제

에 대한 ID 및 액세스 관리 AWS WAF

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. AWS WAF IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리

- AWS WAF IAM과의 작동 방식
- AWS WAF에 대한 자격 증명 기반 정책 예시
- AWS 에 대한 관리형 정책 AWS WAF
- AWS WAF ID 및 액세스 문제 해결
- 서비스 연결 역할 사용 AWS WAF

고객

사용하는 방식 AWS Identity and Access Management (IAM) 은 수행하는 작업에 따라 다릅니다. AWS WAF

서비스 사용자 - AWS WAF 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS WAF 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS WAF의 기능에 액세스할 수 없는 경우 AWS WAF ID 및 액세스 문제 해결을 참조하세요.

서비스 관리자 — 회사에서 AWS WAF 리소스를 담당하는 경우 전체 액세스 권한이 있을 수 AWS WAF있습니다. 서비스 사용자가 액세스해야 하는 AWS WAF 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사에서 IAM을 어떻게 사용할 수 있는지 자세히 AWS WAF알아보려면 을 참조하십시오AWS WAF IAM과의 작동 방식.

IAM 관리자 - IAM 관리자라면 AWS WAF에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 AWS WAF ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF에 대한 자격 증명 기반 정책 예시

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사

례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을

사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.

  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

AWS WAF IAM과의 작동 방식

IAM을 사용하여 액세스를 AWS WAF관리하기 전에 어떤 IAM 기능과 함께 사용할 수 있는지 알아보세요. AWS WAF

함께 사용할 수 있는 IAM 기능 AWS WAF

IAM 특성	AWS WAF 지원
ID 기반 정책	예
리소스 기반 정책	예
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

AWS WAF 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

ID 기반 정책은 다음과 같습니다. AWS WAF

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에

적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

AWS WAF ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF에 대한 자격 증명 기반 정책 예시

내 리소스 기반 정책 AWS WAF

리소스 기반 정책 지원	예

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

AWS WAF 리소스 기반 정책을 사용하여 계정 간 규칙 그룹 공유를 지원합니다. AWS WAF API 호출 `PutPermissionPolicy` 또는 동등한 CLI 또는 SDK 호출에 리소스 기반 정책 설정을 제공하여 소유한 규칙 그룹을 다른 AWS 계정과 공유할 수 있습니다. 사용 가능한 다른 언어에 대한 예제 및 설명서 링크를 포함한 추가 정보는 API Reference를 참조하십시오 PutPermissionPolicy. AWS WAF 콘솔이나 AWS CloudFormation같은 다른 방법으로는 이 기능을 사용할 수 없습니다.

에 대한 정책 조치 AWS WAF

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

각각에 대한 AWS WAF 작업 및 권한 목록을 보려면 서비스 권한 부여 참조의 AWS WAF V2에서 정의한 작업을 참조하십시오.

정책 조치는 조치 앞에 다음 접두사를 AWS WAF 사용합니다.

```
wafv2
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어 로 List 시작하는 모든 작업을 지정하려면 다음 작업을 포함하세요. AWS WAF

```
"Action": "wafv2:List*"
```

AWS WAF ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF에 대한 자격 증명 기반 정책 예시

추가 권한 설정이 필요한 작업

일부 작업에는 서비스 권한 부여 참조의 AWS WAF V2에서 정의한 작업에서 완전히 설명할 수 없는 권한이 필요합니다. 이 섹션에서는 추가 권한 정보를 제공합니다.

주제

- AssociateWebACL 권한
- DisassociateWebACL 권한
- GetWebACLForResource 권한

- ListResourcesForWebACL 권한

`AssociateWebACL` 권한

이 섹션에는 AWS WAF 작업을 `AssociateWebACL`을 사용하여 웹 ACL을 리소스에 연결하는 데 필요한 권한이 나열되어 있습니다.

Amazon CloudFront 배포의 경우 이 작업 대신 작업을 사용하십시오. CloudFront `UpdateDistribution` 자세한 내용은 Amazon CloudFront API 레퍼런스를 참조하십시오 UpdateDistribution.

Amazon API Gateway REST API

REST API 리소스 `SetWebACL` 유형에서 API Gateway를 호출하고 웹 AWS WAF `AssociateWebACL` ACL에서 호출할 수 있는 권한이 필요합니다.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

Application Load Balancer 리소스 유형에서 `elasticloadbalancing:SetWebACL` 작업을 호출하고 웹 ACL을 AWS WAF `AssociateWebACL` 호출할 수 있는 권한이 필요합니다.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

GraphQL API 리소스 유형을 AWS AppSync `SetWebACL` 호출하고 웹 ACL을 AWS WAF `AssociateWebACL` 호출할 수 있는 권한이 필요합니다.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
```

```
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito 사용자 풀

사용자 풀 리소스 유형에서 Amazon Cognito `AssociateWebACL` 작업을 호출하고 웹 ACL을 AWS WAF `AssociateWebACL` 호출할 수 있는 권한이 필요합니다.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 서비스

App Runner 서비스 리소스 유형에서 App Runner `AssociateWebACL` 작업을 호출하고 웹 ACL을 AWS WAF `AssociateWebACL` 호출할 수 있는 권한이 필요합니다.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
```

```
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 검증된 액세스 인스턴스

Verified Access 인스턴스 리소스 유형에서 `ec2:AssociateVerifiedAccessInstanceWebAcl` 작업을 호출하고 웹 ACL을 AWS WAF `AssociateWebACL` 호출할 수 있는 권한이 필요합니다.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`DisassociateWebACL` 권한

이 섹션에는 AWS WAF 작업 `DisassociateWebACL`을 사용하여 웹 ACL을 리소스에서 연결 해제하는 데 필요한 권한이 나열되어 있습니다.

Amazon CloudFront 배포의 경우 이 작업 대신 빈 웹 ACL ID가 `UpdateDistribution` 있는 CloudFront 작업을 사용하십시오. 자세한 내용은 Amazon CloudFront API 레퍼런스를 참조하십시오 UpdateDistribution.

Amazon API Gateway REST API

REST API 리소스 유형에서 API Gateway `SetWebACL`을 호출할 수 있는 권한이 필요합니다. 호출 권한이 필요하지 않습니다 AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

Application Load Balancer 리소스 유형에 대해 `elasticloadbalancing:SetWebACL` 작업을 호출할 수 있는 권한이 필요합니다. 통화 허가가 필요하지 않습니다 AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync GraphQL API

GraphQL AWS AppSync `SetWebACL` API 리소스 유형을 호출하려면 권한이 필요합니다. 호출 권한이 필요하지 않습니다. AWS WAF `DisassociateWebACL`

```
{
```

```
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Amazon Cognito 사용자 풀

사용자 풀 리소스 유형에서 Amazon Cognito `DisassociateWebACL` 작업을 호출하고 호출할 수 있는 권한이 필요합니다. AWS WAF `DisassociateWebACL`

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:DisassociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 서비스

App Runner 서비스 리소스 유형에서 App Runner `DisassociateWebACL` 작업을 호출하고 호출할 수 있는 권한이 필요합니다. AWS WAF `DisassociateWebACL`

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
```

```
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DisassociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 검증된 액세스 인스턴스

Verified Access 인스턴스 리소스 유형에 대한 `ec2:DisassociateVerifiedAccessInstanceWebAcl` 작업을 호출하고 호출할 수 있는 권한이 필요합니다 AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL1",
    "Effect": "Allow",
    "Action": "wafv2:DisassociateWebACL",
    "Resource": "*"
},
{
    "Sid": "DisassociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DisassociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

`GetWebACLForResource` 권한

이 섹션에는 AWS WAF 작업 `GetWebACLForResource`을 사용하여 보호된 리소스에 대해 웹 ACL을 가져오는 데 필요한 권한이 나열되어 있습니다.

Amazon CloudFront 배포의 경우 이 작업 대신 작업을 사용하십시오. CloudFront `GetDistributionConfig` 자세한 내용은 Amazon CloudFront API 레퍼런스를 참조하십시오 GetDistributionConfig.

> **Note**
>
> `GetWebACLForResource`는 `GetWebACL`을 호출하는 데 권한이 필요합니다. 이 AWS WAF 컨텍스트에서는 `GetWebACLForResource` 반환되는 웹 ACL에 액세스하는 데 필요한 권한이 계정에 있는지 확인하는 `GetWebACL` 데만 사용됩니다. 전화를 `GetWebACLForResource` 걸면 해당 계정에 `wafv2:GetWebACL` 리소스에서 작업을 수행할 권한이 없다는 오류 메시지가 표시될 수 있습니다. AWS WAF AWS CloudTrail 이벤트 기록에 이러한 유형의 오류를 추가하지 않습니다.

아마존 API 게이트웨이 REST API, 애플리케이션 로드 밸런서, AWS AppSync GraphQL API

웹 ACL을 AWS WAF `GetWebACLForResource` 호출하고 `GetWebACL` 실행하려면 권한이 필요합니다.

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Amazon Cognito 사용자 풀

사용자 풀 리소스 유형에서 Amazon Cognito `GetWebACLForResource` 작업을 호출하고 및 를 AWS WAF `GetWebACLForResource` 호출할 수 있는 권한이 필요합니다. `GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
```

```
            "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
        ]
    },
    {
        "Sid": "GetWebACLForResource2",
        "Effect": "Allow",
        "Action": [
            "cognito-idp:GetWebACLForResource"
        ],
        "Resource": [
            "arn:aws:cognito-idp:*:account-id:userpool/*"
        ]
    }
```

AWS App Runner 서비스

App Runner 서비스 리소스 유형에서 App Runner `DescribeWebAclForService` 작업을 호출하고 및 를 AWS WAF `GetWebACLForResource` 호출할 수 있는 권한이 필요합니다. `GetWebACL`

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "apprunner:DescribeWebAclForService"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS 검증된 액세스 인스턴스

Verified Access 인스턴스 리소스 유형에 대한 ec2:GetVerifiedAccessInstanceWebAcl 작업을 호출하고 및 를 AWS WAF GetWebACLForResource 호출할 수 있는 권한이 필요합니다GetWebACL.

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

ListResourcesForWebACL 권한

이 섹션에는 AWS WAF 작업인 ListResourcesForWebACL을 사용하여 웹 ACL의 보호된 리소스 목록을 검색하는 데 필요한 권한이 나열되어 있습니다.

Amazon CloudFront 배포의 경우 이 작업 대신 작업을 사용하십시오. CloudFront ListDistributionsByWebACLId 자세한 내용은 Amazon CloudFront API ListDistributionsByWeb 참조의 aclID를 참조하십시오.

아마존 API 게이트웨이 REST API, 애플리케이션 로드 밸런서, AWS AppSync GraphQL API

웹 AWS WAF ListResourcesForWebACL ACL을 호출하려면 권한이 필요합니다.

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
```

```
            "wafv2:ListResourcesForWebACL"
        ],
        "Resource": [
            "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
        ]
}
```

Amazon Cognito 사용자 풀

사용자 풀 리소스 유형에 대해 Amazon Cognito `ListResourcesForWebACL` 작업을 호출하고 AWS WAF `ListResourcesForWebACL`을 호출할 수 있는 권한이 필요합니다.

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner 서비스

App Runner 서비스 리소스 유형에서 App Runner `ListAssociatedServicesForWebAcl` 작업을 호출하고 호출할 수 있는 권한이 필요합니다. AWS WAF `ListResourcesForWebACL`

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
```

```
            "wafv2:ListResourcesForWebACL"
        ],
        "Resource": [
            "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
        ]
    },
    {
        "Sid": "ListResourcesForWebACL2",
        "Effect": "Allow",
        "Action": [
            "apprunner:ListAssociatedServicesForWebAcl"
        ],
        "Resource": [
            "arn:aws:apprunner:*:account-id:service/*/*"
        ]
    }
```

AWS 검증된 액세스 인스턴스

확인된 액세스 인스턴스 리소스 유형에 대해 `ec2:DescribeVerifiedAccessInstanceWebAclAssociations` 작업을 호출하고 AWS WAF `ListResourcesForWebACL`을 호출하는 데 권한이 필요합니다.

```
{
    "Sid": "ListResourcesForWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "ListResourcesForWebACL2",
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVerifiedAccessInstanceWebAclAssociations"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

에 대한 정책 리소스 AWS WAF

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS WAF 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 참조의 AWS WAF V2에서 정의한 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 V2에서 정의한 AWS WAF 작업을 참조하십시오. 리소스 하위 집합에 대한 액세스를 허용하거나 거부하려면 정책 `resource` 요소에 AWS WAF 리소스의 ARN을 포함하세요.

AWS WAF `wafv2`리소스 ARN의 형식은 다음과 같습니다.

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

ARN 사양에 대한 일반 정보는 Amazon Web Services 일반 참조의 Amazon 리소스 이름(ARN)을 참조하세요.

다음은 `wafv2` 리소스의 ARN과 관련된 요구 사항 목록입니다.

- *`region`*: Amazon CloudFront 배포를 보호하는 데 사용하는 AWS WAF 리소스의 경우 이 값을 로 `us-east-1` 설정하십시오. 그렇지 않으면 보호 대상 리전 리소스에서 사용하는 리전으로 설정합니다.
- *`scope`*: Amazon `global` CloudFront 배포판에서 사용하거나 AWS WAF 지원하는 모든 지역 리소스와 함께 `regional` 사용할 수 있도록 범위를 설정합니다. 리전 리소스는 Amazon API Gateway REST API, 애플리케이션 로드 밸런서, GraphQL API AWS AppSync , Amazon Cognito 사용자 풀, 서비스, 검증된 액세스 AWS App Runner 인스턴스입니다. AWS

- *### ##*: webacl, rulegroup, ipset, regexpatternset 또는 managedruleset 값 중 하나를 지정합니다.
- *resource-name*: AWS WAF 리소스에 지정한 이름을 지정하거나 와일드카드(*)를 지정하여 ARN의 나머지 사양을 충족하는 모든 리소스를 나타냅니다. 리소스 이름과 리소스 ID를 지정하거나 두 가지 모두에 대해 와일드카드를 지정해야 합니다.
- *resource-id*: AWS WAF 리소스의 ID를 지정하거나 와일드카드(*)를 지정하여 ARN의 나머지 사양을 충족하는 모든 리소스를 나타냅니다. 리소스 이름과 리소스 ID를 지정하거나 두 가지 모두에 대해 와일드카드를 지정해야 합니다.

예를 들어 다음 ARN은 us-west-1 리전에서 계정 111122223333에 대한 리전 범위가 있는 모든 웹 ACL을 지정합니다.

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

다음 ARN은 us-east-1 리전의 111122223333 계정에 대해 글로벌 범위를 사용하는 MyIPManagementRuleGroup이라는 이름이 지정된 규칙 그룹을 지정합니다.

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

AWS WAF ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF에 대한 자격 증명 기반 정책 예시

에 대한 정책 조건 키 AWS WAF

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 AND 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

또한 IAM AWS WAF 정책에 대한 세밀한 필터링을 제공하는 데 사용할 수 있는 다음과 같은 조건 키를 지원합니다.

- wafv2: LogDestinationResource

  이 조건 키는 로깅 대상에 대한 Amazon 리소스 이름 (ARN) 사양을 사용합니다. REST API 호출을 사용할 때 로깅 대상으로 제공하는 ARN입니다. `PutLoggingConfiguration`

  ARN을 명시적으로 지정하고 ARN에 대한 필터링을 지정할 수 있습니다. 다음 예제는 특정 위치 및 접두사가 있는 Amazon S3 버킷 ARN에 대한 필터링을 지정합니다.

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- wafv2: LogScope

  이 조건 키는 문자열로 로깅 구성의 소스를 정의합니다. 현재 이 값은 항상 기본값인 로 설정되어 있는데`Customer`, 이는 로깅 대상이 사용자 소유이며 관리됨을 나타냅니다.

AWS WAF 조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS WAF V2용 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 AWS WAF V2에서 정의한 작업을 참조하십시오.

AWS WAF ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF에 대한 자격 증명 기반 정책 예시

내 ACL AWS WAF

ACL 지원	아니요

ACL(액세스 통제 목록)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC 포함 AWS WAF

ABAC(정책 내 태그) 지원	부분

ABAC(속성 기반 액세스 통제)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

다음과 같은 임시 자격 증명 사용 AWS WAF

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자

격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

서비스를 위한 포워드 액세스 세션 AWS WAF

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS WAF의 서비스 역할

서비스 역할 지원	예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

> **Warning**
>
> 서비스 역할의 권한을 변경하면 AWS WAF 기능이 중단될 수 있습니다. 서비스 역할을 편집하기 위한 지침이 AWS WAF 제공되는 경우에만 서비스 역할을 편집하십시오.

서비스 연결 역할은 다음과 같습니다. AWS WAF

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

AWS WAF 서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. 서비스 연결 역할 사용 AWS WAF

AWS WAF에 대한 자격 증명 기반 정책 예시

기본적으로 사용자 및 역할에는 AWS WAF 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 ARN 형식을 비롯하여 에서 정의한 AWS WAF작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS WAF V2용 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- AWS WAF 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- AWS WAF, CloudFront 및 에 대한 읽기 전용 액세스 권한을 부여합니다. CloudWatch
- AWS WAF, CloudFront 및 에 대한 전체 액세스 권한을 부여하십시오. CloudWatch
- 단일 사용자에게만 액세스 권한을 부여합니다. AWS 계정
- 단일 웹 ACL에 대한 액세스 권한 부여
- 웹 ACL 및 규칙 그룹에 대한 CLI 액세스 권한 부여

정책 모범 사례

ID 기반 정책은 누군가가 계정에서 AWS WAF 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이

는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 관리형 정책을 참조하세요.

- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하세요.
- Use conditions in IAM policies to further restrict access(IAM 정책의 조건을 사용하여 액세스 추가 제한) – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 생성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

AWS WAF 콘솔 사용

AWS WAF 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 AWS WAF 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 AWS WAF 콘솔을 사용할 수 있도록 하려면 최소한 AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS 관리형 정책을 엔티티에 연결해야 합니다. 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책: AWSWAFConsoleReadOnlyAccess 섹션을 참조하세요. 관리

형 정책을 사용자에게 연결하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS WAF, CloudFront 및 에 대한 읽기 전용 액세스 권한을 부여합니다. CloudWatch

다음 정책은 사용자에게 AWS WAF 리소스, Amazon CloudFront 웹 배포 및 Amazon CloudWatch 지표에 대한 읽기 전용 액세스 권한을 부여합니다. 권한이 필요한 사용자는 AWS WAF 조건, 규칙 및 웹 ACL의 설정을 보고, 어떤 배포가 웹 ACL과 연결되어 있는지 확인하고, 내 지표와 요청 샘플을 모니터링하는 데 유용합니다. CloudWatch 이러한 사용자는 AWS WAF 리소스를 생성, 업데이트 또는 삭제할 수 없습니다.

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:Get*",
            "wafv2:List*",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

AWS WAF, CloudFront 및 에 대한 전체 액세스 권한을 부여하십시오. CloudWatch

다음 정책을 통해 사용자는 모든 AWS WAF 작업을 수행하고, CloudFront 웹 배포에서 모든 작업을 수행하고, 지표와 요청 샘플을 모니터링할 수 있습니다. CloudWatch AWS WAF 관리자인 사용자에게 유용합니다.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:*",
            "cloudfront:CreateDistribution",
```

```
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:UpdateDistribution",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:DeleteDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

관리 권한이 있는 사용자에 대해 멀티 팩터 인증(MFA)을 구성하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS에서 멀티 팩터 인증(MFA) 기기 사용하기를 참조하세요.

단일 사용자에게만 액세스 권한을 부여합니다. AWS 계정

이 정책은 444455556666 계정에 다음과 같은 권한을 부여합니다.

- 모든 AWS WAF 운영 및 리소스에 대한 전체 액세스 권한
- 모든 CloudFront 배포에 대한 읽기 및 업데이트 액세스를 통해 웹 ACL과 CloudFront 배포를 연결할 수 있습니다.
- 콘솔에서 CloudWatch 데이터와 요청 샘플을 볼 수 있도록 모든 CloudWatch 지표 및 지표 통계에 대한 읽기 액세스 권한을 제공합니다. AWS WAF

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
            "arn:aws:wafv2:us-east-1:444455556666:*"
         ]
      },
```

```
      {
         "Effect": "Allow",
         "Action": [
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudfront:UpdateDistribution",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```

단일 웹 ACL에 대한 액세스 권한 부여

다음 정책을 통해 사용자는 계정의 444455556666 특정 웹 ACL에서 콘솔을 통해 모든 AWS WAF 작업을 수행할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
```

```
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

웹 ACL 및 규칙 그룹에 대한 CLI 액세스 권한 부여

다음 정책은 사용자가 계정의 특정 웹 ACL 및 특정 규칙 그룹에서 CLI를 통해 모든 AWS WAF 작업을 수행할 수 있도록 합니다. 444455556666

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

다음 정책을 통해 사용자는 계정의 특정 웹 ACL에서 콘솔을 통해 모든 AWS WAF 작업을 수행할 수 있습니다. 444455556666

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:*"
            ],
```

```
            "Resource": [
                "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
            ]
        },
        {
            "Sid": "consoleAccess",
            "Effect": "Allow",
            "Action": [
                "wafv2:ListWebACLs",
                "ec2:DescribeRegions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

AWS 에 대한 관리형 정책 AWS WAF

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하십시오.

AWS 관리형 정책: AWSWAFReadOnlyAccess

이 정책은 사용자가 Amazon, Amazon API Gateway, Application Load Balancer, Amazon Cognito CloudFront AWS AppSync, Verified Access와 같은 통합 서비스의 리소스 및 AWS WAF 리소스에 액세스할 수 있는 읽기 전용 권한을 부여합니다. AWS App Runner AWS 이 정책을 IAM ID에 연결할 수

있습니다. AWS WAF 또한 사용자를 AWS WAF 대신하여 작업을 수행할 수 있는 서비스 역할에 이 정책을 연결합니다.

이 정책에 대한 자세한 내용은 IAM AWSWAFReadOnlyAccess콘솔을 참조하십시오.

AWS 관리형 정책: AWSWAFFullAccess

이 정책은 Amazon, Amazon API Gateway, Application Load Balancer CloudFront, Amazon Cognito AWS App Runner, AWS 검증된 액세스와 같은 통합 서비스의 리소스 및 AWS WAF 리소스에 대한 전체 액세스 권한을 부여합니다. AWS AppSync이 정책을 IAM ID에 연결할 수 있습니다. AWS WAF 또한 사용자를 AWS WAF 대신하여 작업을 수행할 수 있는 서비스 역할에 이 정책을 연결합니다.

이 정책에 대한 자세한 내용은 IAM AWSWAFFullAccess콘솔을 참조하십시오.

AWS 관리형 정책: AWSWAFConsoleReadOnlyAccess

이 정책은 AWS WAF 콘솔에 읽기 전용 권한을 부여합니다. 이 권한에는 Amazon, Amazon API Gateway, Application Load Balancer CloudFront, Amazon Cognito AWS AppSync, 검증된 AWS WAF 액세스와 같은 통합 서비스를 위한 리소스와 해당 서비스를 위한 리소스가 포함됩니다. AWS App Runner AWS 이 정책을 IAM ID에 연결할 수 있습니다. AWS WAF 또한 이 정책을 aiam/home#/policies/arn:aws:iam: :aws:policy/ $ 서비스 역할에 연결하여 사용자를 대신하여 작업을 수행할 수 있게 합니다. AWSWAFConsoleFullAccess serviceLevelSummary AWS WAF

이 정책에 대한 자세한 내용은 IAM AWSWAFConsoleReadOnlyAccess콘솔을 참조하십시오.

AWS 관리형 정책: AWSWAFConsoleFullAccess

이 정책은 Amazon, Amazon API Gateway, Application Load Balancer, Amazon Cognito CloudFront AWS App Runner, AWS 검증된 AWS WAF 액세스와 같은 통합 서비스를 위한 리소스와 통합 서비스를 위한 리소스를 포함하는 AWS WAF 콘솔에 대한 전체 액세스 권한을 부여합니다. AWS AppSync이 정책을 IAM ID에 연결할 수 있습니다. AWS WAF 또한 사용자를 AWS WAF 대신하여 작업을 수행할 수 있는 서비스 역할에 이 정책을 연결합니다.

이 정책에 대한 자세한 내용은 IAM AWSWAFConsoleFullAccess콘솔을 참조하십시오.

AWS 관리형 정책: WAFV2 LoggingServiceRolePolicy

이 정책은 Amazon Data Firehose에 로그를 쓸 수 있도록 허용합니다 AWS WAF . 이 정책은 로그인을 활성화한 경우에만 사용됩니다. AWS WAF이 정책은 `AWSServiceRoleForWAFV2Logging` 서비스 역할에 연결됩니다. 서비스 링크 역할에 대한 자세한 내용은 서비스 연결 역할 사용 AWS WAF을(를) 참조하세요.

이 정책에 대한 자세한 내용은 IAM LoggingServiceRolePolicy 콘솔의 WAFV2 항목을 참조하십시오.

AWS WAFAWS 관리형 정책 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 AWS WAF 이후의 AWS 관리형 정책 업데이트에 대한 세부 정보를 볼 수 있습니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 의 AWS WAF 문서 기록 페이지에서 RSS 피드를 구독하십시오. 문서 기록

정책	변경 내용 설명	날짜
`WAFV2LoggingServiceRolePolicy` 이 정책은 Amazon Data Firehose에 로그를 쓸 수 있도록 허용합니다 AWS WAF . 로깅을 활성화한 경우에만 사용됩니다. IAM 콘솔의 세부 정보: WAFV2LoggingServiceRolePolicy.	이 정책이 연결된 서비스 연결 역할의 권한 설정에 Sid (명령문 ID) 를 추가했습니다.	2024-06-03
`AWSServiceRoleForWAFV2Logging` 이 서비스 연결 역할은 Amazon Data AWS WAF Firehose에 로그를 쓸 수 있는 권한 정책을 제공합니다. IAM 콘솔의 세부 정보:. AWSServiceRoleForWAFV2Logging	권한 설정에 명령문 ID (SID) 를 추가했습니다.	2024-06-03
AWS WAF 변경 내용 추적에 대한 추가 사항	AWS WAF 관리형 정책 `WAFV2LoggingServiceRolePolicy` 및 서비스 연결 역할에 대한 변경 사항 추적	2024-06-03

정책	변경 내용 설명	날짜
	을 시작했습니다. `AWSServiceRoleForWAFV2Logging`	
`AWSWAFFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFFullAccess	보호할 수 있는 AWS WAF 리소스 유형에 AWS Verified Access 인스턴스를 추가할 수 있도록 권한을 확장했습니다.	2023-06-17
`AWSWAFReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFReadOnlyAccess	보호할 수 있는 AWS WAF 리소스 유형에 AWS Verified Access 인스턴스를 추가할 수 있도록 권한을 확장했습니다.	2023-06-17
`AWSWAFConsoleFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleFullAccess	보호할 수 있는 AWS WAF 리소스 유형에 AWS Verified Access 인스턴스를 추가할 수 있도록 권한을 확장했습니다.	2023-06-17

정책	변경 내용 설명	날짜
`AWSWAFConsoleReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleReadOnlyAccess	보호할 수 있는 AWS WAF 리소스 유형에 AWS Verified Access 인스턴스를 추가할 수 있도록 권한을 확장했습니다.	2023-06-17
`AWSWAFFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFFullAccess	AWS App Runner 서비스의 액세스 설정을 수정할 수 있도록 권한을 확장했습니다.	2023-06-06
`AWSWAFReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFReadOnlyAccess	AWS App Runner 서비스의 액세스 설정을 수정할 수 있도록 권한을 확장했습니다.	2023-06-06

정책	변경 내용 설명	날짜
`AWSWAFConsoleFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleFullAccess	AWS App Runner 서비스의 액세스 설정을 수정할 수 있도록 권한을 확장했습니다.	2023-06-06
`AWSWAFConsoleReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleReadOnlyAccess	AWS App Runner 서비스의 액세스 설정을 수정할 수 있도록 권한을 확장했습니다.	2023-06-06
`AWSWAFFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFFullAccess	보호할 수 있는 AWS WAF리소스 유형에 AWS App Runner 서비스를 추가할 수 있도록 권한을 확장했습니다.	2023-03-30

정책	변경 내용 설명	날짜
`AWSWAFReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFReadOnlyAccess	보호할 수 있는 AWS WAF리소스 유형에 AWS App Runner 서비스를 추가할 수 있도록 권한을 확장했습니다.	2023-03-30
`AWSWAFConsoleFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleFullAccess	보호할 수 있는 AWS WAF리소스 유형에 AWS App Runner 서비스를 추가할 수 있도록 권한을 확장했습니다.	2023-03-30
`AWSWAFConsoleReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleReadOnlyAccess	보호할 수 있는 AWS WAF리소스 유형에 AWS App Runner 서비스를 추가할 수 있도록 권한을 확장했습니다.	2023-03-30

정책	변경 내용 설명	날짜
`AWSWAFFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFFullAccess	보호할 수 있는 리소스 유형에 Amazon Cognito 사용자 풀을 추가할 수 있는 권한이 확장되었습니다. AWS WAF	2022-08-25
`AWSWAFReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFReadOnlyAccess	보호할 수 있는 리소스 유형에 Amazon Cognito 사용자 풀을 추가할 수 있는 권한이 확장되었습니다. AWS WAF	2022-08-25
`AWSWAFConsoleFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleFullAccess	보호할 수 있는 리소스 유형에 Amazon Cognito 사용자 풀을 추가할 수 있는 권한이 확장되었습니다. AWS WAF	2022-08-25

정책	변경 내용 설명	날짜
`AWSWAFConsoleReadOnlyAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleReadOnlyAccess	보호할 수 있는 리소스 유형에 Amazon Cognito 사용자 풀을 추가할 수 있는 권한이 확장되었습니다. AWS WAF	2022-08-25
`AWSWAFFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFFullAccess	Amazon Simple Storage 서비스 (Amazon S3) 및 CloudWatch Amazon Logs의 로그 전송 권한 설정을 수정했습니다. 이 변경으로 로깅 구성 중에 발생했던 액세스 거부 오류가 해결되었습니다. 웹 ACL 트래픽 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.	2022-01-11
`AWSWAFConsoleFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleFullAccess	Amazon Simple Storage 서비스 (Amazon S3) 및 CloudWatch Amazon Logs의 로그 전송 권한 설정을 수정했습니다. 이 변경으로 로깅 구성 중에 발생했던 액세스 오류가 해결되었습니다. 웹 ACL 트래픽 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.	2022-01-11

정책	변경 내용 설명	날짜
`AWSWAFFullAccess` 이 정책을 통해 통합 AWS WAF 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFFullAccess	확장된 로깅 옵션에 대한 새 권한을 추가했습니다. 이 변경으로 인해 추가 로깅 대상인 Amazon Simple Storage 서비스 (Amazon S3) 및 Amazon CloudWatch Logs에 AWS WAF 액세스할 수 있습니다. 웹 ACL 트래픽 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.	2021-11-15
`AWSWAFConsoleFullAccess` 이 정책을 통해 AWS WAF 통합 서비스 내에서 AWS WAF 사용자를 대신하여 AWS 콘솔 리소스 및 기타 AWS 리소스를 관리할 수 있습니다. IAM 콘솔의 세부 정보:. AWSWAFConsoleFullAccess	확장된 로깅 옵션에 대한 새 권한을 추가했습니다. 이 변경으로 인해 추가 로깅 대상인 Amazon Simple Storage 서비스 (Amazon S3) 및 Amazon CloudWatch Logs에 AWS WAF 액세스할 수 있습니다. 웹 ACL 트래픽 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.	2021-11-15
AWS WAF 변경 사항 추적 시작	AWS WAF AWS 관리형 정책의 변경 사항 추적을 시작했습니다.	2021-3-01

AWS WAF ID 및 액세스 문제 해결

다음 정보를 사용하면 및 IAM을 사용할 때 발생할 수 있는 일반적인 문제를 AWS WAF 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS WAF
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 AWS WAF 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

저는 다음과 같은 작업을 수행할 권한이 없습니다. AWS WAF

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojackson`IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`*리소스에 대한 세부 정보를 보려고 하지만 가상 `wafv2:`*`GetWidget`*권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

이 경우 `wafv2:`*`GetWidget`*작업을 사용하여 *`my-example-widget`*리소스에 액세스할 수 있도록 `mateojackson`사용자 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 AWS WAF에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 AWS WAF에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 AWS WAF 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- 이러한 기능의 AWS WAF 지원 여부를 알아보려면 을 참조하십시오AWS WAF IAM과의 작동 방식.
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서에서 자신이 소유한 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 페더레이션)을 참조하십시오.
- 교차 계정 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

서비스 연결 역할 사용 AWS WAF

AWS WAF AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS WAF서비스 연결 역할은 사전 정의되며 서비스가 사용자를 AWS WAF 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스에 연결된 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 설정이 AWS WAF 더 쉬워집니다. AWS WAF 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 해당 역할만 AWS WAF 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 이 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

먼저 역할의 관련 리소스를 삭제해야 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 AWS WAF 리소스에 대한 액세스 권한을 실수로 제거할 수 없으므로 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조해 서비스 연결 역할 열이 예(Yes)인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

에 대한 서비스 연결 역할 권한 AWS WAF

AWS WAF 서비스 연결 역할을 사용하여 Amazon Data `AWSServiceRoleForWAFV2Logging` Firehose에 로그를 기록합니다. 이 역할은 로그인을 활성화한 경우에만 사용됩니다. AWS WAF로깅에 대한 추가 정보는 AWS WAF 웹 ACL 트래픽 로깅 섹션을 참조하세요.

이 서비스 연결 역할은 AWS 관리형 정책에 연결됩니다. `WAFV2LoggingServiceRolePolicy` 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책: WAFV2 LoggingServiceRolePolicy섹션을 참조하세요.

`AWSServiceRoleForWAFV2Logging` 서비스 연결 역할은 역할을 수임하기 위해 `wafv2.amazonaws.com` 서비스를 신뢰합니다.

역할의 권한 정책을 통해 지정된 리소스에서 다음 작업을 AWS WAF 완료할 수 있습니다.

- Amazon 데이터 Firehose 작업: `PutRecord` 및 로 시작하는 이름을 가진 `PutRecordBatch` Firehose 데이터 스트림 리소스에서. `aws-waf-logs-` 예를 들어 `aws-waf-logs-us-east-2-analytics`입니다.
- AWS Organizations 조치: `DescribeOrganization` Organizations 조직 리소스에 관한 조치

IAM 콘솔에서 전체 서비스 연결 역할을 참조하십시오. AWSServiceRoleForWAFV2Logging

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

AWS WAF에 대한 서비스 링크 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 에서 AWS WAF 로그온을 AWS Management Console활성화하거나 AWS WAF CLI 또는 AWS WAF API에서 `PutLoggingConfiguration` 요청하면 서비스 연결 AWS WAF 역할이 자동으로 생성됩니다.

로깅을 활성화하려면 `iam:CreateServiceLinkedRole` 권한이 있어야 합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AWS WAF 로깅을 활성화하면 서비스 연결 역할이 다시 AWS WAF 생성됩니다.

AWS WAF에 대한 서비스 링크 역할 편집

AWS WAF `AWSServiceRoleForWAFV2Logging`서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습

니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 편집을 참조하세요.

AWS WAF에 대한 서비스 링크 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> AWS WAF 서비스가 역할을 사용하고 있을 때 리소스를 삭제하려고 하면 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 AWS WAF 리소스를 삭제하려면 **`AWSServiceRoleForWAFV2Logging`**

1. AWS WAF 콘솔에서 모든 웹 ACL에서 로깅을 제거합니다. 자세한 정보는 AWS WAF 웹 ACL 트래픽 로깅을 참조하세요.
2. API 또는 CLI를 사용하여 로깅이 활성화된 각 웹 ACL에 대한 `DeleteLoggingConfiguration` 요청을 제출합니다. 자세한 내용은 AWS WAF API 참조를 참조하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 `AWSServiceRoleForWAFV2Logging` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

AWS WAF 서비스 링크 역할이 지원되는 리전

AWS WAF 서비스를 사용할 수 있는 모든 지역에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS WAF 엔드포인트 및 할당량을 참조하세요.

로그인 및 모니터링 AWS WAF

모니터링은 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 AWS WAF 있어 중요한 부분입니다. 다중 지점 장애가 발생할 경우 이를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 합니다. AWS AWS WAF 리소스를 모니터링하고 잠재적 이벤트에 대응하기 위한 여러 도구를 제공합니다.

아마존 CloudWatch 알람

CloudWatch 경보를 사용하면 지정한 기간 동안 단일 지표를 관찰할 수 있습니다. 지표가 지정된 임계값을 초과하는 경우 Amazon SNS 주제 또는 AWS Auto Scaling 정책에 알림을 CloudWatch 보냅니다. 자세한 정보는 아마존을 통한 모니터링 CloudWatch을 참조하세요.

AWS CloudTrail 로그

CloudTrail 에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공합니다 AWS WAF. 에서 수집한 CloudTrail 정보를 사용하여 요청을 받은 사람 AWS WAF, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다. 자세한 정보는 을 사용하여 AWS CloudTrail API 호출 로깅을 참조하세요.

AWS WAF 웹 ACL 트래픽 로깅

AWS WAF 웹 ACL이 분석하는 트래픽에 대한 로깅을 제공합니다. 로그에는 보호된 AWS 리소스로부터 요청을 AWS WAF 받은 시간, 요청에 대한 세부 정보, 요청이 일치하는 규칙의 작업 설정과 같은 정보가 포함됩니다. 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅을(를) 참조하세요.

에 대한 규정 준수 검증 AWS WAF

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수

프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.

- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

내에서의 레질리언스 AWS WAF

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다 AWS 리전 . AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS WAF에서 인프라 보안

관리형 서비스로서 AWS 글로벌 네트워크 보안으로 AWS WAF 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 액세스할 AWS WAF 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증 정보를 생성하여 요청에 서명할 수 있습니다.

AWS WAF 할당량

> **Note**
>
> 의 최신 AWS WAF버전입니다. AWS WAF 클래식에 대해서는 을 참조하십시오AWS WAF 클래식.

AWS WAF 에는 다음과 같은 할당량 (이전에는 한도라고 함) 이 적용됩니다. 이러한 할당량은 사용 가능한 모든 지역에서 동일합니다. AWS WAF 각 리전에 이러한 할당량이 개별적으로 적용됩니다. 할당량은 리전을 교차하여 누적되지 않습니다.

AWS WAF 계정당 보유할 수 있는 최대 법인 수에 대한 기본 할당량이 있습니다. 이 할당량의 증가를 요청할 수 있습니다.

Resource	리전별 계정당 기본 할당량
최대 웹 ACL 수	100
최대 규칙 그룹 수	100
최대 IP 집합 수	100
웹 ACL당 초당 최대 요청 수	25,000
웹 ACL 또는 규칙 그룹당 사용자 지정 요청 헤더 최대 수	100
웹 ACL 또는 규칙 그룹당 사용자 지정 응답 헤더 최대 수	100
웹 ACL 또는 규칙 그룹당 최대 사용자 지정 응답 본문 최대 수	50
웹 ACL 토큰 도메인 목록의 최대 토큰 도메인 수	10

허용되는 최대 RPS (초당 요청 수) CloudFront 는 개발자 AWS WAF 가이드에서 설정하고 개발자 CloudFront 가이드에 설명되어 있습니다. CloudFront

AWS WAF 지역별 계정별 다음 엔티티 설정의 할당량을 수정했습니다. 이러한 할당량은 변경할 수 없습니다.

Resource	리전별 계정당 할당량
웹 ACL당 최대 웹 ACL 용량 단위(WCU)	5,000
규칙 그룹당 최대 WCU	5,000

Resource	리전별 계정당 할당량
규칙 그룹당 최대 참조 문 수 규칙 그룹에서 참조문은 IP 집합 또는 정규식 패턴 집합을 참조할 수 있습니다.	50
웹 ACL당 최대 참조 문 수. 웹 ACL에서 참조문은 규칙 그룹, IP 집합 또는 정규식 패턴 집합을 참조할 수 있습니다.	50
IP 집합당 CIDR 표기법으로 표기된 최대 IP 주소 수	10,000개
웹 ACL당 최대 속도 기반 규칙 수	10
규칙 그룹당 최대 속도 기반 규칙 수	4
비율 기반 규칙에 대해 정의할 수 있는 최소 요청 비율	100
요금제 기반 규칙당 속도 제한할 수 있는 최대 고유 IP 주소 수	10,000개
문자열 일치 문에 허용되는 최대 문자 수	200
각 정규식 패턴에 허용되는 최대 문자 수	200
정규식 집합당 고유한 최대 정규식 패턴 수	10
최대 정규식 집합 수	10
Application Load AWS AppSync Balancer 및 보호를 위해 검사할 수 있는 웹 요청 본문의 최대 크기	8KB
API Gateway, Amazon Cognito CloudFront, 앱 러너 및 검증된 액세스 보호를 검사할 수 있는 웹 요청 본문의 최대 크기**	64KB
규칙 문당 최대 텍스트 변환 횟수	10
단일 사용자 지정 응답 정의에 대한 사용자 지정 응답 본문 콘텐츠의 최대 크기	4KB
단일 사용자 지정 응답 정의에 대한 최대 사용자 지정 헤더 수	10
단일 사용자 지정 요청 정의에 대한 사용자 지정 헤더 최대 수	10

Resource	리전별 계정당 할당량
단일 규칙 그룹 또는 단일 웹 ACL에 대한 모든 응답 본문 콘텐츠를 합산한 최대 크기	50KB

*웹 ACL에서 1,500개가 넘는 WCU를 사용하면 기본 웹 ACL 가격을 초과하는 비용이 발생합니다. 자세한 내용은 AWS WAF 웹 ACL 용량 단위 (WCU) 및 AWS WAF 요금을 참조하세요.

**기본적으로 API Gateway, Amazon CognitoCloudFront, 앱 러너 및 검증된 액세스 리소스에 대한 본문 검사 한도는 16KB로 설정되어 있지만, 웹 ACL 구성의 모든 리소스에 대해 나열된 최대값까지 이 한도를 늘릴 수 있습니다. 자세한 정보는 신체 검사 크기 제한 관리을 참조하세요.

AWS WAF 지역별 계정당 호출 할당량은 다음과 같이 고정되어 있습니다. 이러한 할당량은 CLI, AWS CloudFormation, REST API, SDK 등 사용 가능한 수단을 통한 전체 서비스 호출 수에 적용됩니다. 이러한 할당량은 변경할 수 없습니다.

호출 유형	리전별 계정당 할당량
`AssociateWebACL` 에 대한 최대 호출 수	2초당 요청 한 개
`DisassociateWebACL` 에 대한 최대 호출 수	2초당 요청 한 개
`GetWebACLForResource` 에 대한 최대 호출 수	1초당 요청 한 개
`ListResourcesForWebACL` 에 대한 최대 호출 수	1초당 요청 한 개
개별 `Get` 또는 `List` 작업에 대한 최대 호출 수(다른 할당량이 정의되지 않은 경우)	1초당 요청 다섯 개
개별 `Create`, `Put`, 또는 `Update` 작업에 대한 최대 호출 수(다른 할당량이 정의되지 않은 경우)	1초당 요청 한 개

AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF

이 섹션에서는 규칙 및 웹 ACL을 Classic에서 AWS WAF Classic으로 마이그레이션하기 위한 지침을 제공합니다. AWS WAF AWS WAF 은 2019년 11월에 릴리스되었습니다. Classic을 사용하여 규칙 및 웹 ACL과 같은 리소스를 생성한 경우 AWS WAF AWS WAF Classic을 사용하여 작업하거나 이 최신 버전으로 마이그레이션해야 합니다.

마이그레이션 작업을 시작하기 전에 먼저 끝까지 읽어보고 숙지하세요. AWS WAF AWS WAF

주제

- 로 마이그레이션해야 하는 AWS WAF이유
- 마이그레이션 작동 방식
- 마이그레이션 경고 및 제한 사항
- 웹 ACL을 클래식에서 클래식으로 마이그레이션 AWS WAFAWS WAF

로 마이그레이션해야 하는 AWS WAF이유

의 최신 버전은 사용자에게 익숙한 개념과 용어를 대부분 유지하면서 이전 버전에 비해 많은 개선 사항을 AWS WAF 제공합니다.

다음 목록은 최신 AWS WAF의 주요 변경 사항에 대해 설명합니다. 마이그레이션을 계속하기 전에 잠시 시간을 내어 이 목록을 검토하고 가이드의 나머지 부분을 숙지하시기 바랍니다. AWS WAF

- AWS 관리형 규칙 대상 AWS WAF - 이제 AWS 관리형 규칙을 통해 사용할 수 있는 규칙 그룹은 일반적인 웹 위협으로부터 보호합니다. 이러한 규칙 그룹은 대부분 무료로 포함되어 있습니다 AWS WAF. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록 및 AWS 관리형 규칙 발표 블로그 게시물을 참조하십시오. AWS WAF
- 새 AWS WAF API — 새 API를 사용하면 단일 API 세트를 사용하여 모든 AWS WAF 리소스를 구성할 수 있습니다. 리전 애플리케이션과 글로벌 애플리케이션을 구분하기 위해 새 API에는 `scope` 설정이 포함되어 있습니다. API에 대한 자세한 내용은 AWS WAFV2 작업 및 AWS WAFV2 데이터 유형 섹션을 참조하세요.

  API, SDK, CLI 및 AWS WAF Classic에서는 이름 지정 체계를 유지하며 AWS CloudFormation, 컨텍스트에 따라 이 최신 버전의 OR이 AWS WAF V2 추가되어 참조됩니다. v2

- 단순화된 서비스 할당량 (제한) — AWS WAF 이제 웹 ACL당 더 많은 규칙을 허용하고 더 긴 정규식 패턴을 표현할 수 있습니다. 자세한 정보는 AWS WAF 할당량을 참조하세요.
- 웹 ACL 제한은 이제 컴퓨팅 요구 사항을 기반으로 합니다. 웹 ACL 한도는 이제 웹 ACL 용량 단위 (WCU) 를 기반으로 합니다. AWS WAF 규칙을 실행하는 데 필요한 운영 용량에 따라 규칙의 WCU를 계산합니다. 웹 ACL의 WCU는 웹 ACL에서 모든 규칙 및 규칙 그룹의 WCU를 합산한 결과입니다.

  WCU에 대한 일반적인 정보는 AWS WAF 작동 방식 섹션을 참조하세요. 각 규칙의 WCU 사용에 대한 자세한 내용은 규칙 문 기본 사항 섹션을 참조하세요.
- 문서 기반 규칙 작성 – 이제 규칙, 규칙 그룹 및 웹 ACL을 JSON 형식으로 작성하고 표현할 수 있습니다. 더 이상 개별 API 호출을 사용하여 다른 조건을 생성한 후 조건을 규칙에 연결할 필요가 없습니다. 이렇게 하면 더욱 쉽게 코드를 작성하고 유지 관리할 수 있습니다. Download web ACL as JSON(웹 ACL을 JSON으로 다운로드)을 선택하면 웹 ACL을 볼 때 콘솔에서 JSON 형식의 웹 ACL에 액세스할 수 있습니다 . 고유한 규칙을 생성할 때 Rule JSON editor(규칙 JSON 편집기)를 선택하면 해당 JSON 표현에 액세스할 수 있습니다.
- 규칙 중첩 및 전체 논리적 작업 지원 – 논리적 규칙 문을 사용하고 중첩을 사용하여 복잡한 결합 규칙을 작성할 수 있습니다. `[A AND NOT(B OR C)]` 같은 문을 작성할 수 있습니다. 자세한 정보는 논리적 규칙 문을 참조하세요.
- 개선된 속도 기반 규칙 - 최신 버전에서는 규칙이 평가하는 기간 및 규칙이 요청을 집계하는 방식을 사용자 지정할 수 있습니다. AWS WAF여러 웹 요청 특성을 조합하여 집계를 사용자 지정할 수 있습니다. 또한 최신 속도 기반 규칙은 트래픽 변화에 더 빠르게 반응합니다. 자세한 정보는 비율 기반 규칙 문을 참조하세요.
- IP 집합에 대한 가변적 CIDR 범위 지원 – 이제 IP 집합 사양에서 IP 범위의 유연성이 높아졌습니다. IPv4의 경우 지원한다. AWS WAF /1 /32 IPv6의 경우 다음을 지원합니다. AWS WAF /1 /128 IP 집합에 대한 자세한 내용은 IP 집합 일치 규칙 문 단원을 참조하세요.
- 체인 가능한 텍스트 변환 — 웹 요청 콘텐츠를 검사하기 전에 웹 AWS WAF 요청 콘텐츠에 대해 여러 텍스트 변환을 수행할 수 있습니다. 자세한 정보는 텍스트 변환 옵션을 참조하세요.
- 콘솔 환경 개선 — 새 콘솔은 시각적 규칙 빌더와 보다 직관적인 사용자 편의성을 갖춘 AWS WAF 콘솔 디자인을 제공합니다.
- Firewall Manager AWS WAF 정책에 대한 확장된 옵션 - 이제 AWS WAF 웹 ACL의 Firewall Manager 관리에서 먼저 AWS WAF 처리하는 규칙 그룹과 마지막으로 AWS WAF 처리하는 규칙 그룹 세트를 생성할 수 있습니다. AWS WAF 정책을 적용한 후 로컬 계정 소유자는 이 두 세트 사이에서 AWS WAF 처리하는 자체 규칙 그룹을 추가할 수 있습니다. Firewall Manager AWS WAF 정책에 대한 자세한 내용은 AWS WAF 정책 섹션을 참조하세요.

- AWS CloudFormation 모든 규칙 문 유형 지원 - AWS WAF in은 AWS WAF 콘솔 및 API가 AWS CloudFormation 지원하는 모든 규칙 문 유형을 지원합니다. 또한 JSON 형식으로 작성한 규칙을 YAML 형식으로 쉽게 변환할 수 있습니다.

마이그레이션 작동 방식

자동 마이그레이션은 대부분의 AWS WAF 클래식 웹 ACL 구성을 그대로 유지하므로 수동으로 처리해야 하는 몇 가지 사항이 남습니다.

다음은 웹 ACL을 마이그레이션하기 위한 고급 단계 목록입니다.

1. 자동 마이그레이션은 Classic에서 아무것도 수정하거나 삭제하지 않고도 기존 웹 ACL과 관련된 모든 내용을 읽습니다. AWS WAF 다음과 호환되는 웹 ACL 및 관련 리소스의 표현을 생성합니다. AWS WAF새 웹 ACL에 대한 AWS CloudFormation 템플릿을 생성하여 Amazon S3 버킷에 저장합니다.
2. 에서 웹 ACL 및 관련 리소스를 다시 만들려면 템플릿을 에 AWS CloudFormation배포합니다. AWS WAF
3. 웹 ACL을 검토하고 마이그레이션을 수동으로 완료하면 새 웹 ACL에서 최신 AWS WAF기능을 모두 이용할 수 있습니다.
4. 보호 리소스를 새 웹 ACL로 수동 전환합니다.

마이그레이션 경고 및 제한 사항

마이그레이션한다고 해서 모든 설정이 전달되는 것은 아니고, AWS WAF Classic의 설정이 그대로 전달됩니다. 관리형 규칙 같은 몇 가지 사항은 두 버전 간에 정확히 매핑되지 않습니다. 그 밖에 AWS 보호 리소스와 웹 ACL의 연결 같은 설정은 처음에 새 버전에서 비활성화되어 있기 때문에 나중에 준비되었을 때 추가하면 됩니다.

다음 목록에서는 마이그레이션 경고와 경고에 대응하여 취할 수 있는 조치에 대해 설명합니다. 마이그레이션을 계획할 때는 아래 개요를 사용하십시오. 자세한 마이그레이션 단계는 나중에 마이그레이션 권장 단계를 통해 알아보겠습니다.

- 단일 계정 - 모든 계정의 AWS WAF Classic 리소스를 동일한 계정의 AWS WAF 리소스로만 마이그레이션할 수 있습니다.
- 관리형 규칙 — 마이그레이션 시 AWS Marketplace 셀러의 관리형 규칙은 가져오지 않습니다. 일부 AWS Marketplace 판매자는 동일한 관리 규칙을 제공하므로 다시 AWS WAF 구독할 수 있습니다.

이렇게 하기 전에 최신 버전의 에서 제공되는 AWS 관리형 규칙을 AWS WAF검토하십시오. 이들 중 대부분은 AWS WAF 사용자에게 무료로 제공됩니다. 관리형 규칙에 대한 자세한 내용은 관리형 규칙 그룹 단원을 참조하세요.

- 웹 ACL 연결 – 마이그레이션하더라도 웹 ACL과 보호 리소스 간 연결까지 가져오지는 않습니다. 기본적으로 프로덕션 워크로드에 영향을 미치지 않도록 설계되어 있기 때문입니다. 따라서 모든 것이 올바르게 마이그레이션되었는지 확인한 후 새 웹 ACL을 리소스와 연결하십시오.
- 로깅 – 마이그레이션된 웹 ACL에 대한 로깅은 기본적으로 비활성화됩니다. 이것은 설계에 따른 것입니다. AWS WAF Classic에서 전환할 준비가 되면 로깅을 AWS WAF활성화하십시오.
- AWS Firewall Manager 규칙 그룹 - 마이그레이션은 Firewall Manager에서 관리하는 규칙 그룹을 처리하지 않습니다. Firewall Manager에서 관리하는 웹 ACL은 마이그레이션이 가능하지만 규칙 그룹까지 가져오지는 못합니다. 이러한 웹 ACL에 마이그레이션 도구를 사용하는 것보다는 Firewall Manager에서 새 AWS WAF 에 대한 정책을 다시 생성하십시오.

  > **Note**
  >
  > Firewall Manager가 AWS WAF 클래식용으로 관리하는 규칙 그룹은 방화벽 관리자 규칙 그룹이었습니다. 새 버전의 AWS WAF규칙 그룹은 규칙 그룹입니다 AWS WAF . 하지만 기능적으로는 두 규칙 그룹 모두 동일합니다.

- AWS WAF 보안 자동화 — 보안 자동화를 마이그레이션하려고 하지 마십시오.AWS WAF 마이그레이션하더라도 Lambda 함수는 변환되지 않습니다. 자동화에서 사용될 수도 있기 때문입니다. 최신 AWS WAF버전과 호환되는 새 AWS WAF 보안 자동화 솔루션이 출시되면 해당 솔루션을 재배포하십시오.

웹 ACL을 클래식에서 클래식으로 마이그레이션 AWS WAFAWS WAF

웹 ACL을 마이그레이션하여 전환하려면 먼저 자동 마이그레이션을 실행한 후 수동으로 몇 가지 단계를 이어서 완료합니다.

주제

- 웹 ACL 마이그레이션: 자동 마이그레이션
- 웹 ACL 마이그레이션: 수동 후속 단계
- 웹 ACL 마이그레이션: 추가 고려 사항
- 웹 ACL 마이그레이션: 전환

웹 ACL 마이그레이션: 자동 마이그레이션

웹 ACL 구성을 AWS WAF Classic에서 다음으로 자동 마이그레이션하려면 AWS WAF

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.
2. AWS WAF 클래식으로 전환을 선택하고 웹 ACL의 구성 설정을 검토하십시오. 이전 단원 마이그레이션 경고 및 제한 사항에서 설명한 경고 및 제한 사항을 생각하면서 설정을 기록합니다.
3. 상단의 정보 대화 상자에서 웹 ACL 마이그레이션으로 시작하는 문장을 찾아 마이그레이션 마법사로 연결되는 링크를 선택합니다. 그러면 마이그레이션 마법사가 시작됩니다.

   정보 대화 상자가 보이지 않는다면 AWS WAF 클래식 콘솔을 실행한 이후에 대화 상자를 닫았을 수 있습니다. 내비게이션 바에서 신규로 전환을 선택한 AWS WAF다음 AWS WAF 클래식으로 전환을 선택하면 정보 대화 상자가 다시 나타납니다.
4. 마이그레이션할 웹 ACL을 선택합니다.
5. 마이그레이션 구성에서 템플릿에 사용할 Amazon S3 버킷을 입력합니다. 생성된 AWS CloudFormation 템플릿을 저장하려면 마이그레이션 API에 맞게 구성된 Amazon S3 버킷이 필요합니다.

   - 버킷이 암호화된 경우 Amazon S3(SSE-S3) 키를 사용해야 합니다. 마이그레이션은 AWS Key Management Service (SSE-KMS) 키를 사용한 암호화를 지원하지 않습니다.
   - 버킷 이름은 `aws-waf-migration-`로 시작해야 합니다. 예를 들어 `aws-waf-migration-my-web-acl`입니다.
   - 버킷은 템플릿을 배포할 리전에 속해야 합니다. 예를 들어 `us-west-2`의 웹 ACL이라고 가정할 경우 `us-west-2`에 속한 Amazon S3 버킷을 사용하고, 템플릿 스택을 `us-west-2`에 배포해야 합니다.
6. S3 bucket policy(S3 버킷 정책)에서는 Auto apply the bucket policy required for migration(마이그레이션에 필요한 버킷 정책을 자동 적용)을 선택하는 것이 좋습니다. 그 밖에 버킷을 직접 관리하고 싶다면 다음 버킷 정책을 수동으로 적용해야 합니다.

   - 글로벌 Amazon CloudFront 애플리케이션의 경우 (`waf`):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "apiv2migration.waf.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

- 리전 Amazon API Gateway 또는 Application Load Balancer 애플리케이션(`waf-regional`)의 경우:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

7. Choose how to handle rules that cannot be migrated(마이그레이션할 수 없는 규칙 처리 방법 선택)에서 마이그레이셔할 수 없는 규칙을 제외하거나 마이그레이션을 중지하도록 선택합니다. 마이그레이션할 수 없는 규칙에 대한 자세한 내용은 마이그레이션 경고 및 제한 사항 단원을 참조하세요.
8. 다음을 선택합니다.
9. AWS CloudFormation 템플릿 생성에서 설정을 확인한 다음 AWS CloudFormation 템플릿 생성 시작을 선택하여 마이그레이션 프로세스를 시작합니다. 이 작업은 웹 ACL의 복잡성에 따라 몇 분 정도 걸릴 수 있습니다.
10. 마이그레이션을 완료하기 위해 AWS CloudFormation 스택 생성 및 실행에서 AWS CloudFormation 콘솔로 이동하여 템플릿에서 스택을 생성하고 새 웹 ACL과 해당 리소스를 생성하도록 선택할 수 있습니다. 이렇게 하려면 AWS CloudFormation 스택 생성을 선택합니다.

자동 마이그레이션 프로세스가 완료되면 수동 후속 단계를 진행할 수 있습니다. 웹 ACL 마이그레이션: 수동 후속 단계 섹션을 참조하세요.

웹 ACL 마이그레이션: 수동 후속 단계

자동 마이그레이션이 완료되면 새롭게 생성된 웹 ACL을 검토하고 마이그레이션으로도 가져올 수 없는 구성 요소를 입력합니다. 다음 절차에서는 마이그레이션에서 처리하지 못하는 웹 ACL 관리의 측면을 다룹니다. 목록은 마이그레이션 경고 및 제한 사항 단원을 참조하세요.

기본 마이그레이션을 완료하려면 - 수동 단계

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.
2. 콘솔은 자동으로 최신 버전을 사용해야 합니다 AWS WAF. 이를 확인하려면 탐색 창에 AWS WAF 클래식으로 전환 옵션이 표시되는지 확인합니다. 새 AWS WAF버전으로 전환이 표시되면 해당 버전을 선택하여 최신 버전으로 전환하십시오.
3. 탐색 창에서 [Web ACLs]를 선택합니다.
4. Web ACLs(웹 ACL) 페이지에서 새 웹 ACL을 생성한 리전의 목록에서 새 웹 ACL을 찾습니다. 웹 ACL의 이름을 선택하여 웹 ACL에 대한 설정을 표시합니다.
5. 새 웹 ACL의 모든 설정을 이전 AWS WAF 클래식 웹 ACL과 비교하여 검토하십시오. 기본적으로 로깅 및 보호 리소스 연결은 비활성화됩니다. 이 두 가지 설정은 나중에 전환할 준비가 되었을 때 활성화합니다.
6. AWS WAF 클래식 웹 ACL에 조건이 포함된 속도 기반 규칙이 있는 경우 마이그레이션 시 조건이 전달되지 않았습니다. 이때는 새 웹 ACL에서 조건을 규칙에 추가할 수 있습니다.

   a. 웹 ACL 설정 페이지에서 규칙 탭을 선택합니다.

   b. 목록에서 비율 기반 규칙을 찾아 선택한 다음 편집을 선택합니다.

   c. Criteria to count request towards rate limit(요청을 비율 한도에 포함시키는 기준)에서 Only consider requests that match the criteria in a rule statement(규칙 문의 기준과 일치하는 요청만 고려)을 선택한 다음 추가 기준을 입력합니다. 논리적 문을 포함해 중첩 가능한 규칙 문을 사용해 기준을 추가할 수 있습니다. 선택 가능한 규칙 문에 대한 자세한 내용은 비율 기반 규칙 문 단원을 참조하세요.
7. AWS WAF 클래식 웹 ACL에 관리형 규칙 그룹이 있는 경우 마이그레이션 시 규칙 그룹 포함이 적용되지 않았습니다. 하지만 관리형 규칙 그룹을 새 웹 ACL에 추가할 수 있습니다. 에서 새 버전에서 사용할 수 있는 관리형 규칙 목록을 포함하여 AWS 관리형 규칙 그룹에 대한 정보를 검토하십시오. AWS WAF관리형 규칙 그룹 관리형 규칙 그룹을 추가하려면 다음을 수행합니다.

a. 웹 ACL 설정 페이지에서 웹 ACL 규칙 탭을 선택합니다.
b. 규칙 추가를 선택한 다음 Add managed rule groups(관리형 규칙 그룹 추가)를 선택합니다.
c. 원하는 공급업체 목록을 확장하고 추가할 규칙 그룹을 선택합니다. AWS Marketplace 셀러의 경우 규칙 그룹에 가입해야 할 수 있습니다. 웹 ACL에서 관리형 규칙 그룹 사용에 대한 자세한 내용은 관리형 규칙 그룹 및 웹 ACL 규칙 및 규칙 그룹 평가 단원을 참조하세요.

기본 마이그레이션 프로세스를 마친 후에는 자신의 요건을 검토하고 추가 옵션의 필요성을 살펴보는 것이 좋습니다. 그래야만 새로운 구성 효율을 최대한 높이는 동시에 최신 보안 옵션을 사용할 수 있기 때문입니다. 웹 ACL 마이그레이션: 추가 고려 사항 섹션을 참조하세요.

웹 ACL 마이그레이션: 추가 고려 사항

새 웹 ACL을 검토하고 새 AWS WAF 웹 ACL에서 사용할 수 있는 옵션을 고려하여 구성이 최대한 효율적이고 사용 가능한 최신 보안 옵션을 사용하고 있는지 확인하십시오.

추가 AWS 관리형 규칙

웹 ACL에 추가 AWS 관리형 규칙을 구현하여 애플리케이션의 보안 태세를 강화하는 것을 고려해 보세요. 이는 추가 비용 없이 포함됩니다. AWS WAF AWS 관리형 규칙에는 다음과 같은 유형의 규칙 그룹이 있습니다.

- 기본 규칙 그룹은 알려진 잘못된 입력이 애플리케이션에 삽입되지 않도록 막거나 관리자 페이지 액세스를 차단하는 등 여러 가지 일반적인 위협에서 보호하는 기능을 제공합니다.
- 사용 사례별 규칙 그룹은 다양한 사용 사례 및 환경에 대해 점진적 보호 기능을 제공합니다.
- IP 평판 목록은 클라이언트의 소스 IP를 기반으로 위협 인텔리전스를 제공합니다.

자세한 정보는 AWS 에 대한 관리형 규칙 AWS WAF을 참조하세요.

규칙 최적화 및 정리

이전 규칙을 다시 살펴보고 다시 작성하거나 오래된 규칙을 제거하여 최적화하는 것이 좋습니다. 예를 들어 과거에 OWASP 10대 웹 응용 프로그램 취약성에 대한 기술 문서, OWASP 상위 10대 웹 응용 프로그램 취약성에 대비하기 AWS WAF 및 새 백서를 사용하여 AWS CloudFormation 템플릿을 배포했다면 이를 관리형 규칙으로 대체하는 것을 고려해야 합니다. AWS 문서에 있는 개념은 여전히 적용 가능하며 규칙을 직접 작성하는 데 도움이 될 수 있지만 템플릿으로 만든 규칙은 대부분 관리형 규칙으로 대체되었습니다. AWS

아마존 CloudWatch 메트릭스 및 알람

Amazon CloudWatch 메트릭을 다시 살펴보고 필요에 따라 알람을 설정하십시오. 마이그레이션으로 CloudWatch 경보가 이월되지 않으므로 지표 이름이 원하는 것과 다를 수 있습니다.

애플리케이션 팀과 검토

애플리케이션 팀과 협력하여 보안 상태를 확인하십시오. 애플리케이션에서 자주 구문 분석하는 필드를 찾아 그에 따른 입력 내용을 검열할 수 있는 규칙을 추가합니다. 극단적 사례가 있는지 확인하고, 애플리케이션의 비즈니스 로직이 이러한 사례를 처리하지 못할 경우 해당 사례를 찾아낼 수 있는 규칙을 추가합니다.

전환 계획

애플리케이션 팀과 함께 전환 시점을 계획합니다. 이전 웹 ACL 연결에서 새 웹 ACL 연결로의 전환 시 리소스가 저장된 모든 영역으로 전파되기까지 약간의 시간이 걸릴 수 있습니다. 전파 시간은 몇 초~몇 분이 걸릴 수 있습니다. 이 기간 동안 일부 요청은 이전 웹 ACL에서 처리되고 다른 요청은 새 웹 ACL에서 처리됩니다. 전환 내내 리소스가 보호되지만 전환이 진행될 때는 요청 처리에서 불일치 사항이 발견될 수 있습니다.

전환할 준비가 되면 웹 ACL 마이그레이션: 전환의 절차를 따르십시오.

웹 ACL 마이그레이션: 전환

새 웹 ACL 설정을 확인한 후 AWS WAF Classic 웹 ACL 대신 사용할 수 있습니다.

새 AWS WAF 웹 ACL 사용을 시작하려면

1. 의 지침에 따라 AWS WAF 웹 ACL을 보호하려는 리소스에 연결합니다. 웹 ACL을 리소스와 연결 또는 연결 해제 AWS 이렇게 하면 이전 웹 ACL에서 리소스 연결이 자동으로 해제됩니다.

   전환 시 전파하는 데는 몇 초~몇 분이 걸릴 수 있습니다. 이 기간 동안 일부 요청은 이전 웹 ACL에서 처리되고 다른 요청은 새 웹 ACL에서 처리될 수 있습니다. 전환 내내 리소스가 보호되지만 완료될 때까지는 요청 처리에서 불일치 사항이 발견될 수 있습니다.
2. AWS WAF 웹 ACL 트래픽 로깅의 지침에 따라 새 웹 ACL에 대한 로깅을 구성합니다.
3. (선택 사항) AWS WAF 클래식 웹 ACL이 더 이상 리소스와 연결되지 않는 경우 Classic에서 AWS WAF 완전히 제거하는 것이 좋습니다. 자세한 내용은 웹 ACL 삭제 섹션을 참조하세요.

AWS WAF 클래식

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF Classic은 Amazon API Gateway API, Amazon CloudFront 또는 애플리케이션 로드 밸런서로 전달되는 HTTP 및 HTTPS 요청을 모니터링할 수 있는 웹 애플리케이션 방화벽입니다. AWS WAF 또한 Classic을 사용하면 콘텐츠에 대한 액세스를 제어할 수 있습니다. 요청이 시작되는 IP 주소 또는 쿼리 문자열 값과 같이 지정한 조건에 따라 API Gateway 또는 Application Load Balancer는 요청된 콘텐츠 CloudFront 또는 HTTP 403 상태 코드 (금지됨) 를 사용하여 요청에 응답합니다. 요청이 차단될 때 사용자 지정 오류 페이지를 CloudFront 반환하도록 구성할 수도 있습니다.

주제

AWS WAF 클래식 설정

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

이 항목에서는 사용자 계정 생성과 같은 AWS WAF Classic 사용 준비를 위한 예비 단계를 설명합니다. 이에 대해서는 요금이 청구되지 않습니다. 사용한 AWS 서비스에 대해서만 요금이 부과됩니다.

> **Note**
>
> 새 사용자인 경우 이 AWS WAF Classic 설정 단계를 따르지 마세요. AWS WAF대신, 의 최신 버전에 대한 단계를 따르세요서비스를 사용하기 위한 계정 설정. AWS WAF

이 단계를 완료한 후 AWS WAF 클래식 시작하기 AWS WAF Classic을 계속 시작하려면 을 참조하십시오.

> **Note**
>
> AWS Shield Standard AWS WAF Classic에 포함되어 있으며 추가 설정이 필요하지 않습니다. 자세한 정보는 AWS Shield 앤 쉴드 어드밴스드 작동 방식을 참조하세요.

AWS WAF AWS Shield Advanced Classic을 사용하기 전에 또는 처음 사용하기 전에 이 섹션의 단계를 완료하십시오.

주제

- 가입하여 AWS 계정
- 관리자 액세스 권한이 있는 사용자 생성
- 도구 다운로드

가입하여 AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요. AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 AWS Management Console소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면AWS 로그인 사용 설명서의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자 (콘솔) 에 대한 가상 MFA 디바이스 활성화를 참조하십시오.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.

2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM IDentity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.

2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

도구 다운로드

AWS WAF Classic용 콘솔이 AWS Management Console 포함되어 있지만, 프로그래밍 방식으로 AWS WAF Classic에 액세스하려면 다음을 참조하십시오.

- 원시 HTTP 요청 조합과 같은 저수준 세부 정보를 처리할 필요 없이 AWS WAF Classic API를 호출하려는 경우 SDK를 사용할 수 있습니다. AWS AWS SDK는 Classic 및 기타 서비스의 기능을 캡슐화하는 함수와 데이터 유형을 제공합니다. AWS WAF AWS AWS SDK를 다운로드하려면 사전 요구 사항 및 설치 지침이 포함된 해당 페이지를 참조하십시오.
  - Java
  - JavaScript
  - .NET
  - Node.js

- PHP
- Python
- Ruby

  AWS SDK의 전체 목록은 Amazon Web Services용 도구를 참조하십시오.
- SDK를 제공하지 AWS 않는 프로그래밍 언어를 사용하는 경우, AWS WAF API 참조는 AWS WAF Classic에서 지원하는 작업을 문서화합니다.
- AWS Command Line Interface (AWS CLI) 는 AWS WAF 클래식을 지원합니다. 를 AWS CLI 사용하면 명령줄에서 여러 AWS 서비스를 제어하고 스크립트를 통해 서비스를 자동화할 수 있습니다. 자세한 정보는 AWS Command Line Interface을 참조하세요.
- AWS Tools for Windows PowerShell AWS WAF 클래식을 지원합니다. 자세한 내용은 AWS Tools for PowerShell Cmdlet 참조를 참조하세요.

AWS WAF 클래식 작동 방식

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF Classic을 사용하여 API Gateway, Amazon CloudFront 또는 애플리케이션 로드 밸런서가 웹 요청에 응답하는 방식을 제어할 수 있습니다. 먼저 조건, 규칙 및 웹 ACL(웹 액세스 제어 목록)을 생성합니다. 조건을 정의하고, 조건을 규칙에 결합하며 규칙을 웹 ACL에 결합합니다.

> **Note**
>
> 또한 AWS WAF 클래식을 사용하여 Amazon Elastic Container Service (Amazon ECS) 컨테이너에 호스팅되는 애플리케이션을 보호할 수 있습니다. Amazon ECS는 클러스터에서 Docker 컨테이너를 손쉽게 실행, 중지 및 관리할 수 있게 해주는 컨테이너 관리 서비스로서 확장성과 속도가 뛰어납니다. 이 옵션을 사용하려면 AWS WAF 클래식 지원 Application Load Balancer를 사용하여 서비스 내 작업 전반에서 HTTP/HTTPS (계층 7) 트래픽을 라우팅하고 보호하도록

Amazon ECS를 구성해야 합니다. 자세한 내용은 Amazon Elastic Container Service 개발자 안내서에서 서비스 로드 밸런싱 항목을 참조하세요.

조건

조건은 AWS WAF Classic이 웹 요청에서 감시할 기본 특성을 정의합니다.

- 악성일 가능성이 있는 스크립트입니다. 공격자는 웹 애플리케이션의 취약성을 악용할 수 있는 스크립트를 포함시킵니다. 이것은 교차 사이트 스크립팅이라고 알려져 있습니다.
- 요청이 시작되는 IP 주소 또는 주소 범위입니다.
- 요청이 시작되는 국가 또는 지리적 위치입니다.
- 쿼리 문자열과 같은 요청에서 지정된 부분의 길이입니다.
- 악성일 가능성이 있는 SQL 코드입니다. 공격자는 악성 SQL 코드를 웹 요청에 포함시켜서 데이터베이스에서 데이터를 추출하려고 시도합니다. 이것은 SQL 명령어 주입이라고 알려져 있습니다.
- 요청에 나타나는 문자열입니다. 예를 들어 `User-Agent` 헤더에 나타나는 값 또는 쿼리 문자열에 나타나는 텍스트 문자열입니다. 정규식을 사용하여 이러한 문자열을 지정할 수도 있습니다.

일부 조건에는 여러 개의 값이 있습니다. 예를 들어, IP 조건에 최대 10,000개의 IP 주소 또는 IP 주소 범위를 지정할 수 있습니다.

규칙

조건을 규칙으로 결합하여 허용, 차단 또는 집계하려는 요청을 정확하게 타겟팅할 수 있습니다. AWS WAF Classic은 두 가지 유형의 규칙을 제공합니다.

일반 규칙

일반 규칙은 조건만 사용하여 특정 요청을 대상으로 선택합니다. 예를 들어 공격자로부터 확인한 최근 요청을 기반으로 다음 조건이 포함된 규칙을 생성할 수 있습니다.

- 요청이 192.0.2.44에서 나옵니다.
- 요청의 `User-Agent` 헤더에 `BadBot`라는 값이 포함되어 있습니다.
- 요청의 쿼리 문자열에 유사 SQL 코드가 포함되어 있는 것으로 보입니다.

이 예제에서와 같이 한 규칙에 여러 조건이 모두 포함되면 AWS WAF Classic은 모든 조건과 모두 일치하는 요청을 찾습니다. 다시 말해서 조건을 `AND`(으)로 함께 연결합니다.

일반 규칙에는 적어도 하나의 조건을 추가해야 합니다. 조건 없는 일반 규칙은 어떤 요청과도 일치할 수 없으므로 규칙의 작업(허용, 계산 또는 차단)이 절대 트리거되지 않습니다.

비율 기반 규칙

비율 기반 규칙은 비율 제한이 추가된 일반 규칙과 비슷합니다. 비율 기반 규칙은 규칙의 조건을 충족하는 IP 주소로부터 도달한 요청을 계산합니다. IP 주소의 요청이 5분 내에 비율 제한을 초과하는 경우 규칙은 작업을 트리거할 수 있습니다. 작업이 트리거되는 데 1~2분 정도 소요될 수 있습니다.

비율 기반 규칙에서는 조건이 선택 사항입니다. 비율 기반 규칙에 조건을 추가하지 않으면 비율 제한이 모든 IP 주소에 적용됩니다. 조건을 비율 제한과 결합하면 조건과 일치하는 IP 주소에 비율 제한이 적용됩니다.

예를 들어 공격자로부터 확인한 최근 요청을 기반으로 다음 조건이 포함된 비율 기반 규칙을 생성할 수 있습니다.

- 요청이 192.0.2.44에서 나옵니다.
- 요청의 `User-Agent` 헤더에 `BadBot`라는 값이 포함되어 있습니다.

이 비율 기반 규칙에서 비율 제한도 정의합니다. 이 예에서는 비율 제한을 1,000으로 정의했다고 가정하겠습니다. 위의 두 조건을 모두 충족하고 5분간 1,000개 요청을 초과하는 요청은 웹 ACL에 정의된 대로 규칙의 작업(차단 또는 허용)을 트리거합니다.

두 조건을 모두 충족하지 않은 요청은 비율 제한으로 계산되지 않으며 이 규칙의 영향을 받지 않습니다.

두 번째 예로, 웹 사이트의 특정 페이지에 대한 요청을 제한하는 경우를 가정해 보겠습니다. 이렇게 하려면 다음과 같은 문자열 일치 조건을 비율 기반 규칙에 추가할 수 있습니다.

- [Part of the request to filter on]은 `URI`입니다.
- [Match Type]은 [`Starts with`]입니다.
- [Value to match]는 [`login`]입니다.

여기에 [`RateLimit`]를 1,000으로 지정합니다.

웹 ACL에 이 비율 기반 규칙을 추가함으로써 사이트의 나머지 페이지에는 영향을 주지 않고 로그인 페이지에 대한 요청을 제한할 수 있습니다.

웹 ACL

조건을 규칙으로 결합한 후 규칙을 웹 ACL로 결합합니다. 이 위치에서 각 규칙에 대한 작업(허용, 차단 또는 계산) 및 기본 작업을 정의합니다.

각 규칙에 대한 작업

웹 요청이 규칙의 모든 조건과 일치하는 경우 AWS WAF Classic은 요청을 차단하거나 요청이 API Gateway API, CloudFront 배포 또는 Application Load Balancer로 전달되도록 허용할 수 있습니다. 각 규칙에 대해 AWS WAF Classic에서 수행할 작업을 지정합니다.

AWS WAF Classic은 규칙을 나열한 순서대로 요청을 웹 ACL의 규칙과 비교합니다. AWS WAF 그러면 Classic은 요청이 일치하는 첫 번째 규칙과 관련된 작업을 수행합니다. 예를 들어 웹 요청이 요청을 허용하는 규칙 하나와 요청을 차단하는 다른 규칙과 일치하는 경우 AWS WAF Classic은 처음에 나열된 규칙에 따라 요청을 허용하거나 차단합니다.

새 규칙을 사용하기 전에 테스트하려는 경우 규칙의 모든 조건을 충족하는 요청을 계산하도록 AWS WAF Classic을 구성할 수도 있습니다. 요청을 허용하거나 차단하는 규칙과 마찬가지로, 요청을 계산하는 규칙은 웹 ACL의 규칙 목록에 있는 위치에 따라 영향을 받습니다. 예를 들어, 웹 요청이 요청을 허용하는 규칙 하나 및 요청을 계산하는 다른 규칙 하나와 일치하는 경우 요청을 허용하는 규칙이 먼저 나열되면 요청은 계산되지 않습니다.

기본 작업

기본 동작은 AWS WAF Classic에서 웹 ACL에 있는 규칙의 모든 조건에 부합하지 않는 요청을 허용할지 차단할지를 결정합니다. 예를 들어, 웹 ACL을 생성하고 전에 정의한 규칙만 추가한다고 가정합니다.

- 요청이 192.0.2.44에서 나옵니다.
- 요청의 `User-Agent` 헤더에 `BadBot`라는 값이 포함되어 있습니다.
- 요청의 쿼리 문자열에 악성 SQL 코드가 포함되어 있는 것으로 보입니다.

요청이 규칙의 세 가지 조건을 모두 충족하지 않고 기본 동작이 인 경우 AWS WAF Classic은 `ALLOW` 요청을 API Gateway CloudFront 또는 Application Load Balancer로 전달하고 서비스는 요청된 객체로 응답합니다.

웹 ACL에 규칙을 두 개 이상 추가하는 경우 AWS WAF Classic은 요청이 규칙의 모든 조건을 충족하지 않는 경우에만 기본 작업을 수행합니다. 예를 들어, 조건 하나가 포함된 두 번째 규칙을 추가한다고 가정합니다.

- `User-Agent` 헤더에 `BIGBadBot`라는 값이 포함된 규칙입니다.

AWS WAF Classic은 요청이 첫 번째 규칙의 세 가지 조건을 모두 충족하지 않고 두 번째 규칙의 한 가지 조건을 충족하지 않는 경우에만 기본 작업을 수행합니다.

경우에 따라 Amazon API Gateway, Amazon CloudFront 또는 Application Load Balancer에 대한 요청 허용 또는 차단 여부에 대한 응답이 지연되는 내부 오류가 AWS WAF 발생할 수 있습니다. 이

러한 CloudFront 경우에는 일반적으로 요청을 허용하거나 콘텐츠를 제공합니다. API Gateway 및 Application Load Balancer는 일반적으로 요청을 거부하고 콘텐츠를 제공하지 않습니다.

AWS WAF 클래식 가격

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF Classic에서는 직접 생성한 웹 ACL 및 규칙, 그리고 AWS WAF Classic에서 검사한 HTTP 요청 수에 대해서만 비용을 지불하면 됩니다. 자세한 내용은 AWS WAF Classic 요금을 참조하세요.

AWS WAF 클래식 시작하기

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

이 자습서에서는 AWS WAF Classic을 사용하여 다음 작업을 수행하는 방법을 보여줍니다.

- AWS WAF 클래식 설정.
- AWS WAF 클래식 콘솔을 사용하여 웹 ACL (액세스 제어 목록) 을 만들고 웹 요청을 필터링하는 데 사용할 조건을 지정합니다. 예를 들어, 요청이 기원되는 IP 주소와 요청에서 공격자만 사용하는 값을 지정할 수 있습니다.

- 규칙에 조건을 추가합니다. 규칙을 사용하여 차단하거나 허용할 웹 요청을 대상으로 설정할 수 있습니다. AWS WAF Classic에서 지정한 조건에 따라 요청을 차단하거나 허용하려면 먼저 웹 요청이 규칙의 모든 조건과 일치해야 합니다.
- 웹 ACL에 규칙을 추가합니다. 여기서 각 규칙에 추가하는 조건에 근거하여 웹 요청을 차단할지 또는 허용할지를 지정합니다.
- 기본 조치를 지정합니다(차단 또는 허용). 이는 웹 요청이 규칙과 일치하지 않을 때 AWS WAF Classic에서 취하는 조치입니다.
- AWS WAF Classic에서 웹 요청을 검사할 Amazon CloudFront 배포를 선택합니다. 이 자습서에서는 Application Load Balancer의 단계만 다루지만 Amazon API Gateway API의 프로세스는 기본적으로 동일합니다. CloudFront AWS WAF 클래식 CloudFront 형식은 누구나 사용할 수 있습니다. AWS 리전 AWS WAF API Gateway 또는 Application Load Balancer와 함께 사용할 수 있는 클래식은 AWS 서비스 엔드포인트에 나열된 지역에서 사용할 수 있습니다.

> **Note**
>
> AWS 일반적으로 이 자습서에서 생성한 리소스에 대해 하루 USD 0.25 미만의 요금이 청구됩니다. 자습서를 완료하면 불필요한 요금 발생을 방지하기 위해 리소스를 삭제하는 것이 좋습니다.

주제

1단계: 클래식 설정 AWS WAF

AWS WAF 클래식 설정에서 아직 일반적인 설정 단계를 따르지 않은 경우 지금 실행합니다.

2단계: 웹 ACL 생성

AWS WAF Classic 콘솔은 사용자가 지정하는 조건 (예: 요청이 시작된 IP 주소 또는 요청의 값) 에 따라 웹 요청을 차단하거나 허용하도록 AWS WAF Classic을 구성하는 프로세스를 안내합니다. 이 단계에서는 웹 ACL을 생성합니다.

웹 ACL을 생성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 클래식을 처음 사용하는 경우 AWS WAF 클래식으로 이동을 AWS WAF 선택한 다음 웹 ACL 구성을 선택합니다.

   이전에 AWS WAF 클래식을 사용한 적이 있다면 탐색 창에서 웹 ACL을 선택한 다음 웹 ACL 생성을 선택합니다.
3. [Name web ACL] 페이지에서 [Web ACL name]에 명칭을 입력합니다.

   > **Note**
   >
   > 웹 ACL을 생성한 후에는 명칭을 변경할 수 없습니다.

4. CloudWatch metric name(지표 이름)에 이름을 입력합니다. 명칭에는 영숫자(A-Z, a-z, 0-9)만 포함될 수 있습니다. 공백은 포함될 수 없습니다.

   > **Note**
   >
   > 웹 ACL을 생성한 후에는 명칭을 변경할 수 없습니다.

5. 지역에서 지역을 선택합니다. 이 웹 ACL을 CloudFront 배포에 연결하려면 글로벌 () 을 선택합니다. CloudFront
6. 연계할AWS 리소스의 경우, 웹 ACL과 연계할 리소스를 선택한 후 다음을 선택합니다.

3단계: IP 매칭 조건 생성

IP 매칭 조건은 웹 요청이 기원되는 IP 주소 또는 IP 주소 범위를 지정합니다. 이 단계에서 IP 매칭 조건을 생성합니다. 이후 단계에서 지정된 IP 주소에서 기원되는 요청을 허용할지 또는 요청을 차단할지를 지정합니다.

> **Note**
>
> IP 매칭 조건에 대한 자세한 설명은 IP 매칭 조건 작업 섹션을 참조하세요.

IP 매칭 조건을 생성하려면

1. [Create conditions] 페이지의 [IP match conditions]에서 [Create condition]을 선택합니다.
2. [Create IP match condition] 대화 상자에서 [Name]에 명칭을 입력합니다. 명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다.
3. [Address]에 192.0.2.0/24를 입력합니다. CIDR 표기법으로 지정된 IP 주소 범위에는 192.0.2.0부터 192.0.2.255까지의 IP 주소가 포함됩니다. 예컨대, 192.0.2.0/24 IP 주소 범위는 예약되어 있으므로 이러한 IP 주소에서는 웹 요청이 기원되지 않습니다.

   AWS WAF 클래식은 IPv4 주소 범위 (/8) 와 /16에서 /32 사이의 모든 범위를 지원합니다. AWS WAF 클래식은 IPv6 주소 범위 (/24, /32, /48, /56, /64, /128) 를 지원합니다. (192.0.2.44와 같은 단일 IP 주소를 지정하려면 192.0.2.44/32를 입력합니다.) 기타 범위는 지원되지 않습니다.

   CIDR 표기법에 대한 자세한 설명은 클래스 없는 도메인 간 라우팅에 대한 Wikipedia 문서를 참조하세요.
4. 생성을 선택하세요.

4단계: 지리 매칭 조건 생성

지리 매칭 조건은 요청이 기원되는 해당 국가 또는 여러 국가를 지정합니다. 이 단계에서 지리 매칭 조건을 생성합니다. 이후 단계에서 지정된 국가에서 시작되는 요청을 허용할지 또는 차단할지 지정합니다.

> **Note**
>
> 지리 매칭 조건에 대한 자세한 설명은 지리 매칭 조건 작업 섹션을 참조하세요.

지리 매칭 조건을 생성하려면

1. [Create conditions] 페이지의 [Geo match conditions]에서 [Create condition]을 선택합니다.
2. [Create geo match condition] 대화 상자의 [Name]에 명칭을 입력합니다. 명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다.
3. [Location type] 및 국가를 선택합니다. 현재, [Location type]은 국가만 가능합니다.
4. [Add location]을 선택합니다.
5. 생성을 선택하세요.

5단계: 문자열 매칭 조건 생성

문자열 일치 조건은 AWS WAF Classic에서 요청에서 검색하려는 문자열 (예: 헤더 또는 쿼리 문자열의 지정된 값) 을 식별합니다. 일반적으로 문자열은 인쇄 가능한 ASCII 문자로 구성되지만, 16진수 0x00에서 0xFF(십진수 0에서 255) 사이의 어떤 문자든지 지정할 수 있습니다. 이 단계에서는 문자열 매칭 조건을 생성합니다. 이후 단계에서 지정된 문자열에 포함된 요청을 허용할지 또는 차단할지를 지정합니다.

> **Note**
>
> 문자열 매칭 조건에 대한 자세한 설명은 문자열 매칭 조건 작업 섹션을 참조하세요.

문자열 매칭 조건을 생성하려면

1. [Create conditions] 페이지의 [String and regex match conditions]에서 [Create condition]을 선택합니다.
2. [Create string match condition] 대화 상자에서 다음 값을 입력합니다.

   명칭

   명칭을 입력합니다. 명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다.

   타입

   [String match]를 선택합니다.

요청 중 필터링할 부분

AWS WAF Classic에서 지정된 문자열에 대해 검사할 웹 요청 부분을 선택합니다.

이 예에서는 헤더를 선택합니다.

> **Note**
>
> 필터링할 요청의 일부 값으로 Body를 선택하면 AWS WAF Classic은 처음 8192바이트만 검사 대상으로 CloudFront 전달하므로 처음 8192바이트 (8KB) 만 검사합니다. 본문이 8192바이트보다 긴 요청을 허용하거나 차단하려면 크기 제약 조건을 생성할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.) 자세한 정보는 크기 제약 조건 작업을 참조하세요.

헤더("요청 중 필터링할 부분"이 "헤더"인 경우, 필수)

요청의 일부로 필터링 기준으로 헤더를 선택했으므로 AWS WAF Classic에서 검사할 헤더를 지정해야 합니다. User-Agent를 입력합니다. (이 값은 대소문자를 구분하지 않습니다.)

일치 타입

지정된 문자열이 [User-Agent] 헤더에 나타나야 하는 위치를 선택합니다(예: 시작 부분, 끝 부분 또는 문자열 내 어디든지).

이 예시에서는 Exactly matchs를 선택합니다. 이는 AWS WAF Classic이 지정한 값과 동일한 헤더 값에 대해 웹 요청을 검사한다는 것을 나타냅니다.

변환

AWS WAF Classic을 우회하기 위해 공격자는 웹 요청에 공백을 추가하거나 요청의 일부 또는 전체를 URL 인코딩하는 등 특이한 형식을 사용합니다. 변환은 공백을 제거하거나 요청을 URL 디코딩하거나 그 밖에 공격자가 자주 사용하는 대부분의 이상한 형식을 제거하는 작업을 수행하여 웹 요청을 표준에 더 가까운 형식으로 변환합니다.

단일 타입의 텍스트 변환만을 지정할 수 있습니다.

이 예에서는 [None]을 선택합니다.

값이 base64로 인코딩됨

[Value to match]에 입력한 값이 이미 base64로 인코딩된 경우, 이 확인란을 선택합니다.

이 예에서는 확인란을 선택하지 마십시오.

매칭시킬 값

필터링할 요청의 일부에 지정한 웹 요청 부분에서 AWS WAF Classic에서 검색하려는 값을 지정하십시오.

이 예제에서는 를 입력합니다 BadBot. AWS WAF Classic은 웹 요청의 `User-Agent` 헤더에서 값을 BadBot검사합니다.

[Value to match]의 최대 길이는 50자입니다. base64로 인코딩된 값을 지정하려는 경우, 인코딩하기 전에 최대 50자를 제공할 수 있습니다.

3. AWS WAF Classic에서 여러 값 (예: 포함된 `User-Agent` 헤더 `BadBot` 및 포함하는 쿼리 문자열) 에 대한 웹 요청을 검사하도록 하려면 다음 두 가지 방법을 사용할 수 있습니다. `BadParameter`

   - 두 값이 모두 포함된 경우에만 웹 요청을 허용하거나 차단하려는 경우(AND) 각 값이 대해 하나의 문자열 매칭 조건을 생성합니다.
   - 두 값 중 하나 또는 둘 다 포함된 경우, 웹 요청을 허용하거나 차단하려는 경우(OR) 두 값을 모두 동일한 문자열 매칭 조건에 추가합니다.

   이 예에서는 [Create]를 선택합니다.

5A단계: 정규식 조건 생성(선택 사항)

정규 표현식 조건은 문자열 일치 조건의 일종으로, AWS WAF Classic에서 요청에서 검색할 문자열 (예: 헤더 또는 쿼리 문자열의 지정된 값) 을 식별한다는 점에서 비슷합니다. 주요 차이점은 정규 표현식 (regex) 을 사용하여 AWS WAF Classic에서 검색할 문자열 패턴을 지정한다는 것입니다. 이 단계에서는 정규식 매칭 조건을 생성합니다. 이후 단계에서 지정된 문자열에 포함된 요청을 허용할지 또는 차단할지를 지정합니다.

> **Note**
>
> 정규식 매칭 조건에 대한 자세한 설명은 정규식 매칭 조건 작업 섹션을 참조하세요.

정규식 매칭 조건을 생성하려면

1. [Create conditions] 페이지의 [String match and regex conditions]에서 [Create condition]을 선택합니다.
2. [Create string match condition] 대화 상자에서 다음 값을 입력합니다.

   명칭

   명칭을 입력합니다. 명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다.

   타입

   [Regex match]를 선택합니다.

   요청 중 필터링할 부분

   AWS WAF Classic에서 지정된 문자열에 대해 검사할 웹 요청 부분을 선택합니다.

   이 예에서는 [Body]를 선택합니다.

   > **Note**
   >
   > 필터링할 요청의 일부 값으로 Body를 선택하면 AWS WAF Classic은 처음 8192바이트만 검사 대상으로 CloudFront 전달하므로 처음 8192바이트 (8KB) 만 검사합니다. 본문이 8192바이트보다 긴 요청을 허용하거나 차단하려면 크기 제약 조건을 생성할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.) 자세한 정보는 크기 제약 조건 작업을 참조하세요.

   변환

   AWS WAF Classic을 우회하기 위해 공격자는 웹 요청에 공백을 추가하거나 요청의 일부 또는 전체를 URL 인코딩하는 등 특이한 형식을 사용합니다. 변환은 공백을 제거하거나 요청을 URL 디코딩하거나 그 밖에 공격자가 자주 사용하는 대부분의 이상한 형식을 제거하는 작업을 수행하여 웹 요청을 표준에 더 가까운 형식으로 변환합니다.

   단일 타입의 텍스트 변환만을 지정할 수 있습니다.

   이 예에서는 [None]을 선택합니다.

요청과 일치하는 정규식 패턴

[Create regex pattern set]를 선택합니다.

새 패턴 세트 명칭

이름을 입력한 다음 Classic에서 검색할 정규식 패턴을 지정합니다. AWS WAF

그런 다음 I [a@] mAb [a@] Request 정규 표현식을 입력합니다. AWS WAF Classic은 웹 요청의 `User-Agent` 헤더에서 값을 검사합니다.

- iAMA BadRequest
- IamAB@dRequest
- I @mA BadRequest
- I@mAB@dRequest

3. [Create pattern set and add filter]를 선택합니다.
4. 생성을 선택하세요.

6단계: SQL 명령어 주입 매칭 조건 생성

SQL 삽입 일치 조건은 헤더 또는 쿼리 문자열과 같은 웹 요청에서 AWS WAF Classic이 악성 SQL 코드를 검사하도록 하려는 부분을 식별합니다. 공격자는 SQL 쿼리를 사용하여 데이터베이스에서 데이터를 추출합니다. 이 단계에서는 SQL 명령어 주입 매칭 조건을 생성합니다. 이후 단계에서 악성 SQL 코드가 포함된 것으로 보이는 요청을 허용할지 또는 차단할지를 지정합니다.

> **Note**
> 문자열 매칭 조건에 대한 자세한 설명은 SQL 명령어 주입 매칭 조건 작업 섹션을 참조하세요.

SQL 명령어 주입 매칭 조건을 생성하려면

1. [Create conditions] 페이지의 [SQL injection match conditions]에서 [Create condition]을 선택합니다.
2. [Create SQL injection match condition] 대화 상자에서 다음 값을 입력합니다.

명칭

명칭을 입력합니다.

요청 중 필터링할 부분

AWS WAF Classic에서 악성 SQL 코드를 검사하도록 하려는 웹 요청 부분을 선택합니다.

이 예에서는 쿼리 문자열을 선택합니다.

> **Note**
>
> 필터링할 요청의 일부 값으로 Body를 선택하면 AWS WAF Classic은 처음 8192바이트만 검사 대상으로 CloudFront 전달하므로 처음 8192바이트 (8KB) 만 검사합니다. 본문이 8192바이트보다 긴 요청을 허용하거나 차단하려면 크기 제약 조건을 생성할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.) 자세한 정보는 크기 제약 조건 작업을 참조하세요.

변환

이 예에서는 [URL decode]를 선택합니다.

공격자는 Classic을 AWS WAF 우회하기 위해 URL 인코딩과 같은 특이한 형식을 사용합니다. URL 디코딩 옵션을 선택하면 AWS WAF Classic이 요청을 검사하기 전에 웹 요청에서 해당 형식이 제거됩니다.

단일 타입의 텍스트 변환만을 지정할 수 있습니다.

3. 생성을 선택하세요.
4. 다음을 선택합니다.

7단계: (선택 사항) 추가 조건 생성

AWS WAF 클래식에는 다음과 같은 기타 조건이 포함됩니다.

- 크기 제한 조건 — 헤더 또는 쿼리 문자열과 같이 AWS WAF Classic에서 길이를 확인할 웹 요청 부분을 식별합니다. 자세한 정보는 크기 제약 조건 작업을 참조하세요.
- 사이트 간 스크립팅 일치 조건 - 헤더 또는 쿼리 문자열과 같은 웹 요청에서 악성 스크립트가 있는지 AWS WAF 검사하려는 부분을 식별합니다. 자세한 정보는 교차 사이트 스크립팅 매칭 조건 작업을 참조하세요.

선택적으로 이 조건을 지금 생성하거나 8단계: 규칙 생성 및 조건 추가로 건너뛸 수 있습니다.

8단계: 규칙 생성 및 조건 추가

AWS WAF Classic에서 웹 요청에서 검색할 조건을 지정하는 규칙을 생성합니다. 규칙에 조건을 두 개 이상 추가하는 경우 AWS WAF Classic에서 해당 규칙에 따라 요청을 허용하거나 차단하려면 웹 요청이 규칙의 모든 조건과 일치해야 합니다.

> **Note**
>
> 규칙에 대한 자세한 설명은 규칙 작업 섹션을 참조하세요.

규칙을 생성하고 조건을 추가하려면

1. [Create rules] 페이지에서 [Create rule]을 선택합니다.
2. [Create rule] 대화 상자에서 다음 값을 입력합니다.

   명칭

   명칭을 입력합니다.

   CloudWatch 지표 이름

   AWS WAF Classic에서 생성하여 규칙과 연결할 CloudWatch 지표의 이름을 입력합니다. 명칭에는 영숫자(A-Z, a-z, 0-9)만 포함될 수 있습니다. 공백은 포함될 수 없습니다.

   규칙 타입

   일반 규칙 또는 비율 기반 규칙을 선택합니다. 비율 기반 규칙은 일반 규칙과 동일하지만, 식별된 IP 주소로부터 5분 동안 도달하는 요청의 개수도 고려합니다. 이러한 규칙 타입에 대한 자세한 설명은 AWS WAF 클래식 작동 방식 섹션을 참조하세요. 이 예에서는 [`Regular rule`]을 선택합니다.

   비율 제한

   비율 기반 규칙의 경우, 규칙의 조건과 일치하는 IP 주소로부터 5분 동안 허용할 최대 요청 수를 입력합니다.
3. 규칙에 추가할 첫 번째 조건에 대해 다음 설정을 지정합니다.

   - 웹 요청이 조건의 설정과 일치하는지 여부에 따라 AWS WAF Classic에서 요청을 허용할지 차단할지를 선택합니다.

이 예에서는 [does]를 선택합니다.

- 규칙에 추가할 조건의 타입을 선택합니다. IP 일치 세트 조건, 문자열 일치 세트 조건 또는 SQL 명령어 주입 세트 조건을 선택할 수 있습니다.

  이 예에서는 IP 주소에서 기원을 선택합니다.
- 규칙에 추가할 조건을 선택합니다.

  이 예에서는 이전 작업에서 생성한 IP 매칭 조건을 선택합니다.

4. 조건 추가를 선택합니다.
5. 앞에서 생성한 지리 매칭 조건을 추가합니다. 다음 값을 지정하십시오:
   - When a request does
   - originate from a geographic location in
   - 지리 매칭 조건을 선택합니다.
6. 다른 백분율 추가를 선택합니다.
7. 앞에서 생성한 문자열 매칭 조건을 추가합니다. 다음 값을 지정하십시오:
   - When a request does
   - match at least one of the filters in the string match condition
   - 문자열 매칭 조건을 선택합니다.
8. 조건 추가를 선택합니다.
9. 앞에서 생성한 SQL 명령어 주입 매칭 조건을 추가합니다. 다음 값을 지정하십시오:
   - When a request does
   - match at least one of the filters in the SQL injection match condition
   - SQL 명령어 주입 매칭 조건을 선택합니다.
10. 조건 추가를 선택합니다.
11. 앞에서 생성한 크기 제약 조건을 추가합니다. 다음 값을 지정하십시오:
    - When a request does
    - match at least one of the filters in the size constraint condition
    - 크기 제약 조건을 선택합니다.
12. 다른 조건을 생성한 경우(예: 정규식 조건), 비슷한 방식으로 추가합니다.
13. 생성을 선택하세요.

14. [Default action]에서 [Allow all requests that don't match any rules]를 선택합니다.
15. 검토 및 생성을 선택합니다.

9단계: 웹 ACL에 규칙 추가

웹 ACL에 규칙을 추가할 때 다음 설정을 지정합니다.

- 규칙의 모든 조건 (요청 허용, 차단 또는 개수) 과 일치하는 웹 요청에 대해 AWS WAF Classic에서 수행하려는 조치.
- 웹 ACL에 대한 기본 조치. 규칙의 모든 조건과 일치하지 않는 웹 요청에 대해 AWS WAF Classic에서 수행하려는 조치 (요청 허용 또는 차단) 입니다.

AWS WAF Classic에서는 다음 조건을 모두 충족하는 CloudFront 웹 요청 (및 사용자가 추가했을 수 있는 기타 모든 요청) 을 차단하기 시작합니다.

- `User-Agent` 헤더의 값이 `BadBot`임
- (정규식 조건을 생성하여 추가한 경우) `Body` 값은 패턴 `I[a@]mAB[a@]dRequest`와 일치하는 네 개의 문자열 중 하나임
- 요청이 192.0.2.0-192.0.2.255 범위의 IP 주소에서 기원됨
- 요청이 지리 매칭 조건에서 선택한 국가에서 기원됨.
- 요청의 쿼리 문자열에 악성 SQL 코드가 포함되어 있는 것으로 보임

AWS WAF Classic에서는 CloudFront 이러한 세 가지 조건을 모두 충족하지 않는 모든 요청에 응답할 수 있습니다.

10단계: 리소스 정리

이제 자습서를 성공적으로 완료했습니다. 계정에 AWS WAF Classic 요금이 추가로 발생하지 않도록 하려면 생성한 AWS WAF Classic 객체를 정리해야 합니다. 또는 실제로 허용, 차단 및 계산할 웹 요청과 일치하도록 구성을 변경할 수 있습니다.

> **Note**
>
> AWS 일반적으로 이 자습서에서 생성한 리소스에 대해 일일 US $0.25 미만의 요금이 청구됩니다. 작업을 마치면 불필요한 요금 발생을 방지하기 위해 리소스를 삭제하는 것이 좋습니다.

AWS WAF Classic에서 요금을 청구하는 객체를 삭제하려면

1. 배포에서 웹 ACL을 분리하세요. CloudFront

   a. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

      탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

   b. 삭제하려는 웹 ACL의 명칭을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.

   c. 오른쪽 창의 규칙 탭에서 이 웹 ACL을 사용하는AWS 리소스 섹션으로 이동합니다. 웹 ACL을 연결한 CloudFront 배포의 경우 유형 열에서 x를 선택합니다.

2. 규칙에서 조건을 제거합니다.

   a. 탐색 창에서 규칙을 선택합니다.

   b. 자습서를 진행하는 동안 생성한 규칙을 선택합니다.

   c. [Edit rule]을 선택합니다.

   d. 각 조건 머리글의 오른쪽에서 [x]를 선택합니다.

   e. 업데이트를 선택합니다.

3. 웹 ACL에서 규칙을 제거하고 웹 ACL을 삭제합니다.

   a. 탐색 창에서 [Web ACLs]를 선택합니다.

   b. 자습서를 진행하는 동안 생성한 웹 ACL의 명칭을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.

   c. [Rules] 탭에서 [Edit web ACL]을 선택합니다.

   d. 규칙 머리글 오른쪽에 있는 [x]를 선택합니다.

   e. [Actions]를 선택한 다음 [Delete web ACL]을 선택합니다.

4. 규칙을 삭제합니다.

   a. 탐색 창에서 규칙을 선택합니다.

   b. 자습서를 진행하는 동안 생성한 규칙을 선택합니다.

   c. 삭제를 선택합니다.

   d. [Delete] 대화 상자에서 [Delete]를 다시 선택하여 확인합니다.

AWS WAF Classic은 조건에 따라 요금이 부과되지 않지만 정리를 완료하려면 다음 절차를 수행하여 조건에서 필터를 제거하고 조건을 삭제하십시오.

필터 및 조건을 삭제하려면

1. IP 매칭 조건에서 IP 주소 범위를 삭제하고 IP 매칭 조건을 삭제합니다.
    a. AWS WAF 클래식 콘솔의 탐색 창에서 IP 주소를 선택합니다.
    b. 자습서를 진행하는 동안 생성한 IP 매칭 조건을 선택합니다.
    c. 추가한 IP 주소 범위에 대한 확인란을 선택합니다.
    d. [Delete IP address or range]를 선택합니다.
    e. [IP match conditions] 창에서 [Delete]를 선택합니다.
    f. [Delete] 대화 상자에서 [Delete]를 다시 선택하여 확인합니다.
2. SQL 명령어 주입 조건에서 필터를 삭제하고 SQL 명령어 주입 매칭 조건을 삭제합니다.
    a. 탐색 창에서 [SQL injection]을 선택합니다.
    b. 자습서를 진행하는 동안 생성한 SQL 명령어 주입 매칭 조건을 선택합니다.
    c. 추가한 필터에 대한 확인란을 선택합니다.
    d. [Delete filter]를 선택합니다.
    e. [SQL injection match conditions] 창에서 [Delete]를 선택합니다.
    f. [Delete] 대화 상자에서 [Delete]를 다시 선택하여 확인합니다.
3. 문자열 매칭 조건에서 필터를 삭제하고 문자열 매칭 조건을 삭제합니다.
    a. 탐색 창에서 [String and regex matching]을 선택합니다.
    b. 자습서를 진행하는 동안 생성한 문자열 매칭 조건을 선택합니다.
    c. 추가한 필터에 대한 확인란을 선택합니다.
    d. [Delete filter]를 선택합니다.
    e. [String match conditions] 창에서 [Delete]를 선택합니다.
    f. [Delete] 대화 상자에서 [Delete]를 다시 선택하여 확인합니다.
4. 생성한 경우, 정규식 매칭 조건에서 필터를 삭제한 후 정규식 매칭 조건을 삭제합니다.
    a. 탐색 창에서 [String and regex matching]을 선택합니다.
    b. 자습서를 진행하는 동안 생성한 정규식 매칭 조건을 선택합니다.
    c. 추가한 필터에 대한 확인란을 선택합니다.

d. [Delete filter]를 선택합니다.

e. [Regex match conditions] 창에서 [Delete]를 선택합니다.

f. [Delete] 대화 상자에서 [Delete]를 다시 선택하여 확인합니다.

5. 크기 제약 조건에서 필터를 삭제하고 크기 제약 조건을 삭제합니다.

a. 탐색 창에서 [Size constraints]를 선택합니다.

b. 자습서를 진행하는 동안 생성한 크기 제약 조건을 선택합니다.

c. 추가한 필터에 대한 확인란을 선택합니다.

d. [Delete filter]를 선택합니다.

e. [Size constraint conditions] 창에서 [Delete]를 선택합니다.

f. [Delete] 대화 상자에서 [Delete]를 다시 선택하여 확인합니다.

웹 ACL(웹 액세스 제어 목록) 생성 및 구성

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 액세스 제어 목록 (웹 ACL) 을 사용하면 Amazon API Gateway API, 아마존 CloudFront 배포 또는 애플리케이션 로드 밸런서가 응답하는 웹 요청을 세밀하게 제어할 수 있습니다. 다음 타입의 요청을 허용하거나 차단할 수 있습니다:

- 특정 IP 주소 또는 IP 주소 범위에서 기원됨
- 특정 국가 또는 국가들에서 기원됨
- 요청 중 특정 부분에 지정된 문자열을 포함시키거나 정규식 패턴과 일치시킴
- 지정된 길이를 초과함
- 악성 SQL 코드(SQL 명령어 주입이라고 알려짐)가 포함된 것으로 보임
- 악성 스크립트(교차 사이트 스크립팅이라고 알려짐)가 포함된 것으로 보임

또한 이러한 조건의 어떤 조합도 테스트할 수 있으며, 지정된 조건을 충족할 뿐 아니라 5분간 지정된 요청 수를 초과하는 웹 요청을 차단하거나 계수할 수도 있습니다.

콘텐츠에 액세스할 수 있도록 허용하려는 요청 또는 차단하려는 요청을 선택하려면 다음 작업을 수행합니다.

1. 지정한 조건 중 하나와 일치하지 않는 웹 요청에 대한 기본 조치(허용 또는 차단)을 선택합니다. 자세한 설명은 웹 ACL에 대한 기본 조치 결정 섹션을 참조하세요.
2. 요청을 허용하거나 차단할 조건을 지정합니다.
   - 요청에 악성 스크립트가 포함되는 것으로 보이는지 여부에 근거하여 요청을 허용하거나 차단하려면 교차 사이트 스크립팅 매칭 조건을 생성합니다. 자세한 설명은 교차 사이트 스크립팅 매칭 조건 작업 섹션을 참조하세요.
   - 요청이 기원되는 IP 주소에 근거하여 요청을 허용하거나 차단하려면 IP 주소 매칭 조건을 생성합니다. 자세한 설명은 IP 매칭 조건 작업 섹션을 참조하세요.
   - 요청이 기원되는 국가에 근거하여 요청을 허용하거나 차단하려면 지리 매칭 조건을 생성합니다. 자세한 설명은 지리 매칭 조건 작업 섹션을 참조하세요.
   - 요청이 지정된 길이를 초과하는지 여부에 근거하여 요청을 허용하거나 차단하려면 크기 제약 조건을 생성합니다. 자세한 설명은 크기 제약 조건 작업 섹션을 참조하세요.
   - 요청에 악성 SQL 코드가 포함되는 것으로 보이는지 여부에 근거하여 요청을 허용하거나 차단하려면 SQL 명령어 주입 매칭 조건을 생성합니다. 자세한 설명은 SQL 명령어 주입 매칭 조건 작업 섹션을 참조하세요.
   - 요청에 나타나는 문자열에 근거하여 요청을 허용하거나 차단하려면 문자열 매칭 조건을 생성합니다. 자세한 설명은 문자열 매칭 조건 작업 섹션을 참조하세요.
   - 요청에 나타나는 정규식 패턴에 근거하여 요청을 허용하거나 차단하려면 정규식 매칭 조건을 생성합니다. 자세한 설명은 정규식 매칭 조건 작업 섹션을 참조하세요.
3. 하나 이상의 규칙에 조건을 추가합니다. 동일한 규칙에 조건을 두 개 이상 추가하는 경우 AWS WAF Classic이 규칙에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건과 일치해야 합니다. 자세한 정보는 규칙 작업을 참조하세요. 필요한 경우, 일반 규칙 대신에 비율 기반 규칙을 사용하여 조건을 충족하는 모든 IP 주소의 요청 수를 제한할 수 있습니다.
4. 웹 ACL에 규칙을 추가합니다. 각 규칙에 대해 규칙에 추가한 조건에 따라 AWS WAF Classic에서 요청을 허용할지 차단할지를 지정하십시오. 웹 ACL에 규칙을 두 개 이상 추가하는 경우 AWS WAF Classic은 웹 ACL에 나열된 순서대로 규칙을 평가합니다. 자세한 정보는 웹 ACL 작업을 참조하세요.

   새 규칙을 추가하거나 기존 규칙을 업데이트할 때 이러한 변경 사항이 표시되어 웹 ACL 및 리소스에서 활성화되는 데 최대 1분이 소요될 수 있습니다.

주제

조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

조건은 요청을 허용하거나 차단할 시기를 지정합니다.

- 요청에 악성 스크립트가 포함되는 것으로 보이는지 여부에 근거하여 요청을 허용하거나 차단하려면 교차 사이트 스크립팅 매칭 조건을 생성합니다. 자세한 설명은 교차 사이트 스크립팅 매칭 조건 작업 섹션을 참조하세요.
- 요청이 기원되는 IP 주소에 근거하여 요청을 허용하거나 차단하려면 IP 주소 매칭 조건을 생성합니다. 자세한 설명은 IP 매칭 조건 작업 섹션을 참조하세요.
- 요청이 기원되는 국가에 근거하여 요청을 허용하거나 차단하려면 지리 매칭 조건을 생성합니다. 자세한 설명은 지리 매칭 조건 작업 섹션을 참조하세요.
- 요청이 지정된 길이를 초과하는지 여부에 근거하여 요청을 허용하거나 차단하려면 크기 제약 조건을 생성합니다. 자세한 설명은 크기 제약 조건 작업 섹션을 참조하세요.
- 요청에 악성 SQL 코드가 포함되는 것으로 보이는지 여부에 근거하여 요청을 허용하거나 차단하려면 SQL 명령어 주입 매칭 조건을 생성합니다. 자세한 설명은 SQL 명령어 주입 매칭 조건 작업 섹션을 참조하세요.
- 요청에 나타나는 문자열에 근거하여 요청을 허용하거나 차단하려면 문자열 매칭 조건을 생성합니다. 자세한 설명은 문자열 매칭 조건 작업 섹션을 참조하세요.
- 요청에 나타나는 정규식 패턴에 근거하여 요청을 허용하거나 차단하려면 정규식 매칭 조건을 생성합니다. 자세한 내용은 정규식 매칭 조건 작업을(를) 참조하세요.

주제

교차 사이트 스크립팅 매칭 조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

때로 공격자는 웹 애플리케이션의 취약성을 악용하기 위해 스크립트를 웹 요청에 삽입합니다. AWS WAF Classic에서 악성 스크립트가 있는지 검사하려는 웹 요청 부분 (예: URI 또는 쿼리 문자열) 을 식별하는 사이트 간 스크립팅 일치 조건을 하나 이상 만들 수 있습니다. 이 프로세스에서 나중에 웹 ACL을 생성할 때 악성 스크립트가 포함된 것으로 보이는 요청을 허용할지 또는 차단할지를 지정합니다.

주제

교차 사이트 스크립팅 매칭 조건 생성

교차 사이트 스크립팅 매칭 조건을 만들 때 필터를 지정합니다. 필터는 AWS WAF Classic에서 URI나 쿼리 문자열과 같은 악성 스크립트가 있는지 검사할 웹 요청 부분을 나타냅니다. 교차 사이트 스크립팅

매칭 조건에 두 개 이상의 필터를 추가하거나 각 필터에 대해 별도의 조건을 생성할 수 있습니다. 각 구성이 AWS WAF Classic 동작에 미치는 영향은 다음과 같습니다.

- 사이트 간 스크립팅 일치 조건당 둘 이상의 필터 (권장) - 여러 필터가 포함된 사이트 간 스크립팅 일치 조건을 규칙에 추가하고 규칙을 웹 ACL에 추가하는 경우, AWS WAF Classic의 사이트 간 스크립팅 일치 조건에 있는 필터 중 하나와만 웹 요청이 일치해야 해당 조건에 따라 요청을 허용하거나 차단할 수 있습니다.

  예를 들어, 교차 사이트 스크립팅 매칭 조건 하나를 생성하고 조건에 두 개의 필터가 포함되는 경우를 가정합시다. 한 필터는 AWS WAF Classic에 악성 스크립트가 있는지 URI를 검사하도록 지시하고 다른 필터는 AWS WAF Classic이 쿼리 문자열을 검사하도록 지시합니다. AWS WAF Classic은 URI 또는 쿼리 문자열에 악성 스크립트가 포함된 것으로 보이는 경우 요청을 허용하거나 차단합니다.
- 사이트 간 스크립팅 일치 조건당 필터 하나 - 별도의 사이트 간 스크립팅 일치 조건을 규칙에 추가하고 규칙을 웹 ACL에 추가하는 경우 AWS WAF Classic에서 조건에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건과 일치해야 합니다.

  두 개의 조건을 생성하고 각 조건에 이전 예에서 사용한 두 개의 필터 중 하나가 포함되어 있다고 가정합시다. 동일한 규칙에 두 조건을 모두 추가하고 규칙을 웹 ACL에 추가하면 AWS WAF Classic은 URI와 쿼리 문자열 모두에 악성 스크립트가 포함된 것으로 보이는 경우에만 요청을 허용하거나 차단합니다.

> **Note**
>
> 규칙에 사이트 간 스크립팅 일치 조건을 추가할 때 악성 스크립트가 포함되어 있지 않은 것으로 보이는 웹 요청을 허용하거나 차단하도록 AWS WAF Classic을 구성할 수도 있습니다.

교차 사이트 스크립팅 매칭 조건을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Cross-site scripting]을 선택합니다.
3. [Create condition]을 선택합니다.

4. 해당 필터 설정값을 지정합니다. 자세한 설명은 교차 사이트 스크립팅 매칭 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.
5. [Add another filter]를 선택합니다.
6. 다른 필터를 추가하려는 경우, 4 ~ 5단계를 반복합니다.
7. 필터 추가를 완료했으면 [Create]를 선택합니다.

교차 사이트 스크립팅 매칭 조건을 생성하거나 편집할 때 지정하는 값

교차 사이트 스크립팅 매칭 조건을 생성하거나 업데이트할 때 다음 값을 지정하십시오:

명칭

교차 사이트 스크립팅 매칭 조건의 명칭.

명칭은 문자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 조건을 생성한 후에는 조건의 명칭을 변경할 수 없습니다.

요청 중 필터링할 부분

각 웹 요청에서 AWS WAF Classic에서 악성 스크립트를 검사하도록 하려는 부분을 선택하십시오.

헤더

지정된 요청 헤더입니다(예: `User-Agent` 또는 `Referer` 헤더). [Header]를 선택하는 경우, [Header] 필드에서 헤더의 명칭을 지정합니다.

HTTP 메서드

요청이 오리진에게 수행할 것을 요구하고 있는 작업의 타입을 표시하는 HTTP 메서드입니다. CloudFront `DELETE`,,,, `GET` `HEAD` `OPTIONS` `PATCH`POST, 및 등의 메서드를 지원합니다PUT.

쿼리 문자열

URL 중 ? 문자 뒤에 나타나는 부분입니다(있는 경우).

> **Note**
>
> 사이트 간 스크립팅 매칭 조건의 경우, 요청 중 필터링할 부분에 대한 쿼리 문자열 대신 모든 쿼리 파라미터(값만)를 선택하는 것이 좋습니다.

URI

리소스를 식별하는 요청의 URI 경로(예: `/images/daily-ad.jpg`). 여기에는 URI의 쿼리 문자열 또는 조각 구성 요소는 포함되지 않습니다. 자세한 설명은 Uniform Resource Identifier (URI): Generic Syntax 섹션을 참조하세요.

변환이 지정되지 않는 한 URI는 정규화되지 않고 요청의 일부로 클라이언트로부터 AWS 수신하는 것처럼 검사됩니다. Transformation(변환)은 지정된 대로 URI를 다시 포맷합니다.

본문

요청 중 HTTP 요청 본문으로서 웹 서버에 보낼 추가 데이터(예: 양식의 데이터)가 들어 있는 부분입니다.

> **Note**
>
> 요청 중 필터링할 부분 값으로 본문을 선택하는 경우, AWS WAF Classic은 처음 8192바이트(8KB)만 검사합니다. 본문이 8192바이트보다 긴 요청을 허용하거나 차단하려면 크기 제약 조건을 생성할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.) 자세한 정보는 크기 제약 조건 작업을 참조하세요.

단일 쿼리 파라미터(값만 해당)

쿼리 문자열의 일부로 정의한 모든 파라미터입니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =Seattle”인 경우 or 매개 변수에 필터를 추가할 수 있습니다. UserNameSalesRegion

Single query parameter (value only)(단일 쿼리 파라미터(값만 해당))를 선택하는 경우, Query parameter name(쿼리 파라미터 명칭)도 지정합니다. 검사할 쿼리 문자열의 매개 변수입니다 (예: 또는). UserNameSalesRegion Query parameter name(쿼리 파라미터 명칭)의 최대 길이는 30자입니다. Query parameter name(쿼리 파라미터 명칭)은 대/소문자를 구분하지 않습니다. 예를 들어 Query 매개 변수 이름으로 지정하는 UserName경우 이 이름은 사용자 이름 및 UserName과 같은 모든 변형과 일치합니다. UserName

모든 쿼리 파라미터(값만 해당)

AWS WAF Classic은 단일 쿼리 매개 변수 (값만 해당) 와 유사하지만 단일 매개 변수의 값을 검사하지 않고 쿼리 문자열 내의 모든 매개 변수 값에 악성 스크립트가 있는지 검사합니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =sitle"이고 모든 쿼리 매개 변수

(값만) 를 선택하면 AWS WAF Classic은 악성 스크립트의 값이거나 악성 스크립트가 포함되어 있을 경우 일치 항목을 트리거합니다. UserNameSalesRegion

헤더

필터링 기준으로 사용할 요청의 일부로 헤더를 선택한 경우 공통 헤더 목록에서 헤더를 선택하거나 Classic에서 악성 스크립트가 있는지 검사할 헤더 이름을 입력하십시오. AWS WAF

변환

변환은 AWS WAF Classic에서 요청을 검사하기 전에 웹 요청을 다시 포맷합니다. 이렇게 하면 공격자가 Classic을 우회하기 위해 웹 요청에 사용하는 일부 특이한 형식이 제거됩니다. AWS WAF

단일 타입의 텍스트 변환만을 지정할 수 있습니다.

변환 기능을 사용하여 다음 작업을 수행할 수 있습니다.

None

AWS WAF Classic에서는 Value 내의 문자열이 일치하는지 검사하기 전에는 웹 요청에서 텍스트 변형을 수행하지 않습니다.

소문자로 변환

AWS WAF Classic은 대문자 (A-Z) 를 소문자 (a-z) 로 변환합니다.

HTML 디코딩

AWS WAF Classic은 HTML로 인코딩된 문자를 인코딩되지 않은 문자로 대체합니다.

- `&quot;`를 &로 바꿈
- ` `를 줄 바꿈하지 않는 공백으로 바꿈
- `&lt;`를 <로 바꿈
- `&gt;`를 >로 바꿈
- 16진수 형식으로 표현된 문자 `&#xhhhh;`를 해당 문자로 바꿈
- 십진수 형식으로 표현된 문자 `&#nnnn;`을 해당 문자로 바꿈

공백 표준화

AWS WAF Classic은 다음 문자를 공백 문자 (십진수 32) 로 바꿉니다.

- \f, 양식 피드, 십진수 12
- \t, 탭, 십진수 9
- \n, 줄 바꿈, 십진수 10

- \r, 캐리지 리턴, 십진수 13
- \v, 세로 탭, 십진수 11
- 줄 바꿈하지 않는 공백, 십진수 160

또한 이 옵션은 여러 개의 공백을 하나의 공백으로 바꿉니다.

명령행 간소화

작동 시스템 명령행 명령이 포함된 요청의 경우, 이 옵션을 사용하여 다음 변환을 수행합니다.

- 다음 문자를 삭제: \ " ' ^
- 다음 문자 앞에 있는 공백 삭제: / (
- 다음 문자를 공백으로 바꿈: , ;
- 여러 개의 공백을 하나의 공백으로 바꿈
- 대문자(A-Z)를 소문자(a-z)로 변환

URL 디코딩

URL 인코딩된 요청을 디코딩합니다.

교차 사이트 스크립팅 매칭 조건에서 필터 추가 및 삭제

교차 사이트 스크립팅 매칭 조건에서 필터를 추가하거나 삭제할 수 있습니다. 필터를 변경하려면 새 명칭을 추가하고 기존 명칭을 삭제합니다.

교차 사이트 스크립팅 매칭 조건에서 필터를 추가하거나 삭제하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Cross-site scripting]을 선택합니다.
3. 필터를 추가하거나 삭제하려는 조건을 선택합니다.
4. 필터를 추가하려면 다음 단계를 수행합니다.

   a. [Add filter]를 선택합니다.

   b. 해당 필터 설정값을 지정합니다. 자세한 설명은 교차 사이트 스크립팅 매칭 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.

   c. 추가(Add)를 선택합니다.

5. 필터를 삭제하려면 다음 단계를 수행합니다.

   a. 삭제하려는 필터를 선택합니다.

   b. [Delete filter]를 선택합니다.

교차 사이트 스크립팅 매칭 조건 삭제

교차 사이트 스크립팅 매칭 조건을 삭제하려는 경우, 먼저 다음 절차의 설명에 따라 조건에 있는 모든 필터를 삭제하고 조건을 사용하고 있는 모든 규칙에서 조건을 제거해야 합니다.

교차 사이트 스크립팅 매칭 조건을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 탐색 창에서 [Cross-site scripting]을 선택합니다.
3. [Cross-site scripting match conditions] 창에서 삭제하려는 교차 사이트 스크립팅 매칭 조건을 선택합니다.
4. 오른쪽 창에서 [Associated rules] 탭을 선택합니다.

   이 교차 사이트 스크립팅 매칭 조건을 사용하는 규칙 목록이 비어 있는 경우, 6단계로 이동합니다. 목록에 규칙이 포함되어 있는 경우, 규칙을 기록하고 5단계로 계속합니다.

5. 교차 사이트 스크립팅 매칭 조건을 사용하고 있는 규칙에서 해당 조건을 제거하려면 다음 단계를 수행합니다.

   a. 탐색 창에서 규칙을 선택합니다.

   b. 삭제하려는 교차 사이트 스크립팅 매칭 조건을 사용하고 있는 규칙의 명칭을 선택합니다.

   c. 오른쪽 창에서, 규칙에서 제거하려는 교차 사이트 스크립팅 매칭 조건을 선택하고 [Remove selected condition]을 선택합니다.

   d. 삭제하려는 교차 사이트 스크립팅 매칭 조건을 사용하고 있는 나머지 모든 규칙에 대해 b단계와 c단계를 반복합니다.

   e. 탐색 창에서 [Cross-site scripting]을 선택합니다.

   f. [Cross-site scripting match conditions] 창에서 삭제하려는 교차 사이트 스크립팅 매칭 조건을 선택합니다.

6. [Delete]를 선택하여 선택한 조건을 삭제합니다.

IP 매칭 조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

요청이 기원되는 IP 주소에 근거하여 웹 요청을 허용하거나 차단하려는 경우, IP 매칭 조건을 하나 이상 생성합니다. IP 매칭 조건은 요청이 기원되는 IP 주소 또는 IP 주소 범위를 최대 10,000개까지 열거합니다. 프로세스에서 나중에 웹 ACL을 생성할 때 해당 IP 주소의 요청을 허용할지 또는 차단할지를 지정합니다.

주제

- IP 매칭 조건 생성
- IP 매칭 조건 편집
- IP 매칭 조건 삭제

IP 매칭 조건 생성

요청이 기원되는 IP 주소에 근거하여 일부 웹 요청을 허용하고 다른 일부 웹 요청을 차단하려는 경우, 허용하려는 IP 주소에 대한 IP 매칭 조건과 차단하려는 IP 주소에 대한 다른 IP 매칭 조건을 생성합니다.

> **Note**
>
> 규칙에 IP 일치 조건을 추가할 때 조건에 지정한 IP 주소에서 시작되지 않은 웹 요청을 허용하거나 차단하도록 AWS WAF Classic을 구성할 수도 있습니다.

IP 매칭 조건을 생성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 탐색 창에서 [IP addresses]를 선택합니다.
3. [Create condition]을 선택합니다.
4. 명칭 필드에 명칭을 입력합니다.

   명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 조건을 생성한 후에는 조건의 명칭을 변경할 수 없습니다.
5. 올바른 IP 버전을 선택하고 CIDR 표기법을 사용하여 IP 주소 또는 IP 주소 범위를 지정합니다. 여기 몇 가지 예가 있습니다:

   - IPv4 주소 192.0.2.44를 지정하려면 [192.0.2.44/32]를 입력합니다.
   - IPv6 주소 0:0:0:0:0:ffff:c000:22c를 지정하려면 [0:0:0:0:0:ffff:c000:22c/128]을 입력합니다.
   - 192.0.2.0부터 192.0.2.255까지의 IPv4 주소 범위를 지정하려면 [192.0.2.0/24]를 입력합니다.
   - 2620:0:2d0:200:0:0:0:0부터 2620:0:2d0:200:ffff:ffff:ffff:ffff까지의 IPv6 주소 범위를 지정하려면 [2620:0:2d0:200::/64]를 입력합니다.

   AWS WAF 클래식은 IPv4 주소 범위 (/8) 와 /16에서 /32 사이의 모든 범위를 지원합니다. AWS WAF 클래식은 IPv6 주소 범위 (/24, /32, /48, /56, /64, /128) 를 지원합니다. CIDR 표기법에 대한 자세한 설명은 클래스 없는 도메인 간 라우팅에 대한 Wikipedia 항목을 참조하세요.
6. [Add another IP address or range]를 선택합니다.
7. 다른 IP 주소 또는 범위를 추가하려면 5 ~ 6단계를 반복합니다.
8. 값 추가를 완료했으면 [Create IP match condition]을 선택합니다.

IP 매칭 조건 편집

IP 매칭 조건에 IP 주소 범위를 추가하거나 범위를 삭제할 수 있습니다. 범위를 변경하려면 새 명칭을 추가하고 기존 명칭을 삭제합니다.

IP 매칭 조건을 편집하려면

1. 에 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 콘솔을 엽니다. AWS Management ConsoleAWS WAF

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [IP addresses]를 선택합니다.

3. [IP match conditions] 창에서 편집하려는 IP 매칭 조건을 선택합니다.
4. IP 주소 범위를 추가하려면:
   a. 오른쪽 창에서 Add IP address or range(IP 주소 또는 범위 추가)를 선택합니다.
   b. 올바른 IP 버전을 선택하고 CIDR 표기법을 사용하여 IP 주소 범위를 입력합니다. 여기 몇 가지 예가 있습니다:
      - IPv4 주소 192.0.2.44를 지정하려면 [192.0.2.44/32]를 입력합니다.
      - IPv6 주소 0:0:0:0:0:ffff:c000:22c를 지정하려면 [0:0:0:0:0:ffff:c000:22c/128]을 입력합니다.
      - 192.0.2.0부터 192.0.2.255까지의 IPv4 주소 범위를 지정하려면 [192.0.2.0/24]를 입력합니다.
      - 2620:0:2d0:200:0:0:0:0부터 2620:0:2d0:200:ffff:ffff:ffff:ffff까지의 IPv6 주소 범위를 지정하려면 [2620:0:2d0:200::/64]를 입력합니다.

      AWS WAF 클래식은 IPv4 주소 범위 (/8) 와 /16에서 /32 사이의 모든 범위를 지원합니다. AWS WAF 클래식은 IPv6 주소 범위 (/24, /32, /48, /56, /64, /128) 를 지원합니다. CIDR 표기법에 대한 자세한 설명은 클래스 없는 도메인 간 라우팅에 대한 Wikipedia 항목을 참조하세요.
   c. IP 주소를 추가하려면 Add another IP address(다른 IP 주소 추가)를 선택한 다음 값을 입력합니다.
   d. 추가를 선택합니다.
5. IP 주소 또는 범위를 삭제하려면:
   a. 오른쪽 창에서 삭제할 값을 선택합니다.
   b. [Delete IP address or range]를 선택합니다.

IP 매칭 조건 삭제

IP 매칭 조건을 삭제하려는 경우, 먼저 다음 절차의 설명에 따라 조건에 있는 IP 주소와 범위를 모두 삭제하고 조건을 사용하고 있는 모든 규칙에서 조건을 제거해야 합니다.

IP 매칭 조건을 삭제하려면

1. 에 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 콘솔을 엽니다. AWS Management ConsoleAWS WAF

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 탐색 창에서 [IP addresses]를 선택합니다.
3. [IP match conditions] 창에서 삭제하려는 IP 매칭 조건을 선택합니다.
4. 오른쪽 창에서 [Rules] 탭을 선택합니다.

   이 IP 매칭 조건을 사용하는 규칙 목록이 비어 있는 경우, 6단계로 이동합니다. 목록에 규칙이 포함되어 있는 경우, 규칙을 기록하고 5단계로 계속합니다.
5. IP 매칭 조건을 사용하고 있는 규칙에서 해당 조건을 제거하려면 다음 단계를 수행합니다.

   a. 탐색 창에서 규칙을 선택합니다.
   b. 삭제하려는 IP 매칭 조건을 사용하고 있는 규칙의 명칭을 선택합니다.
   c. 오른쪽 창에서, 규칙에서 제거하려는 IP 매칭 조건을 선택하고 [Remove selected condition]을 선택합니다.
   d. 삭제하려는 IP 매칭 조건을 사용하고 있는 나머지 모든 규칙에 대해 b단계와 c단계를 반복합니다.
   e. 탐색 창에서 [IP match conditions]를 선택합니다.
   f. [IP match conditions] 창에서 삭제하려는 IP 매칭 조건을 선택합니다.
6. [Delete]를 선택하여 선택한 조건을 삭제합니다.

지리 매칭 조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

요청이 기원되는 국가에 근거하여 웹 요청을 허용하거나 차단하려는 경우, 지리 매칭 조건을 하나 이상 생성합니다. 지리 매칭 조건은 요청이 기원되는 국가를 열거합니다. 이 프로세스에서 나중에 웹 ACL을 생성할 때 그러한 국가의 요청을 허용할지 또는 차단할지 지정합니다.

지역 일치 조건을 다른 AWS WAF Classic 조건 또는 규칙과 함께 사용하여 정교한 필터링을 구축할 수 있습니다. 예컨대, 특정 국가를 차단하고 싶으나 해당 국가의 특정 IP 주소는 허용하려는 경우, 지리 매칭 조건 및 IP 매칭 조건을 포함하는 규칙을 생성할 수 있습니다. 해당 국가에서 기원되며 승인된 IP 주

소와 일치하지 않는 요청을 차단하도록 규칙을 구성합니다. 또 다른 예로 특정 국가의 사용자에게 리소스를 우선적으로 할당하려면, 두 개의 요청률 기반 규칙에 지리 매칭 조건을 포함시키면 됩니다. 선호하는 국가의 사용자에게는 요청률 한도를 더 높게 설정하고, 기타 모든 사용자에게는 요청률 한도를 더 낮게 설정합니다.

> **Note**
>
> CloudFront 지역 제한 기능을 사용하여 특정 국가의 콘텐츠 액세스를 차단하는 경우 해당 국가의 모든 요청이 차단되며 Classic으로 전달되지 않습니다. AWS WAF 따라서 지역 및 기타 AWS WAF Classic 조건에 따라 요청을 허용하거나 차단하려는 경우 지역 제한 기능을 사용하지 않아야 합니다. CloudFront 대신 AWS WAF 클래식 지역 일치 조건을 사용해야 합니다.

주제

- 지리 매칭 조건 생성
- 지리 매칭 조건 편집
- 지리 매칭 조건 삭제

지리 매칭 조건 생성

요청이 기원되는 국가에 근거하여 일부 웹 요청은 허용하고 다른 웹 요청은 차단하려는 경우, 허용하려는 국가에 대한 지리 매칭 조건과 차단하려는 국가에 대한 다른 지리 매칭 조건을 생성합니다.

> **Note**
>
> 규칙에 지역 일치 조건을 추가할 때 조건에 지정한 국가에서 시작되지 않은 웹 요청을 허용하거나 차단하도록 AWS WAF Classic을 구성할 수도 있습니다.

지리 매칭 조건을 생성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Geo match]를 선택합니다.
3. [Create condition]을 선택합니다.

4. 명칭 필드에 명칭을 입력합니다.

   명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 조건을 생성한 후에는 조건의 명칭을 변경할 수 없습니다.
5. 리전을 선택합니다.
6. [Location type] 및 국가를 선택합니다. 현재, [Location type]은 국가만 가능합니다.
7. [Add location]을 선택합니다.
8. 생성을 선택하세요.

지리 매칭 조건 편집

지리 매칭 조건에서 국가를 추가하거나 삭제할 수 있습니다.

지리 매칭 조건을 편집하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Geo match]를 선택합니다.
3. [Geo match conditions] 창에서 편집하려는 지리 매칭 조건을 선택합니다.
4. 국가를 추가하려면:
   a. 오른쪽 창에서 [Add filter]를 선택합니다.
   b. [Location type] 및 국가를 선택합니다. 현재, [Location type]은 국가만 가능합니다.
   c. 추가를 선택합니다.
5. 국가를 삭제하려면:
   a. 오른쪽 창에서 삭제할 값을 선택합니다.
   b. [Delete filter]를 선택합니다.

지리 매칭 조건 삭제

지리 매칭 조건을 삭제하려는 경우, 다음 절차의 설명에 따라 먼저 조건에 있는 국가를 모두 삭제한 후 조건을 사용하고 있는 모든 규칙에서 조건을 제거해야 합니다.

지리 매칭 조건을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 지리 매칭 조건을 사용하고 있는 규칙에서 해당 조건을 제거합니다.

   a. 탐색 창에서 규칙을 선택합니다.

   b. 삭제하려는 지리 매칭 조건을 사용하고 있는 규칙의 명칭을 선택합니다.

   c. 오른쪽 창에서 [Edit rule]을 선택합니다.

   d. 삭제하려는 조건 옆의 [X]를 선택합니다.

   e. 업데이트를 선택합니다.

   f. 삭제하려는 지리 매칭 조건을 사용하고 있는 나머지 모든 규칙에 대해 반복합니다.
3. 삭제하려는 조건에서 필터를 제거합니다.

   a. 탐색 창에서 [Geo match]를 선택합니다.

   b. 삭제하려는 지리 매칭 조건의 명칭을 선택합니다.

   c. 오른쪽 창에서 [Filter] 옆의 확인란을 선택하여 필터를 모두 선택합니다.

   d. [Delete filter]를 선택합니다.
4. 탐색 창에서 [Geo match]를 선택합니다.
5. [Geo match conditions] 창에서 삭제하려는 지리 매칭 조건을 선택합니다.
6. [Delete]를 선택하여 선택한 조건을 삭제합니다.

크기 제약 조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

요청에서 지정된 부분의 길이에 근거하여 웹 요청을 허용하거나 차단하려는 경우, 크기 제약 조건을 하나 이상 생성합니다. 크기 제한 조건은 Classic에서 살펴보려는 웹 요청 부분, AWS WAF Classic에서 찾으려는 AWS WAF 바이트 수, 연산자 (예: 초과 (>) 또는 미만 (<) 등의 연산자를 식별합니다. 예를 들어, 크기 제약 조건을 사용하여 100바이트보다 긴 쿼리 문자열을 찾을 수 있습니다. 프로세스에서 나중에 웹 ACL을 생성할 때 해당 설정에 근거하여 요청을 허용할지 또는 차단할지를 지정합니다.

참고로, 요청 본문을 검사하도록 AWS WAF Classic을 구성하면 (예: 본문에서 지정된 문자열 검색) AWS WAF Classic은 처음 8192바이트 (8KB) 만 검사합니다. 웹 요청에 대한 요청 본문이 8192바이트를 절대 초과하지 않을 경우, 크기 제약 조건을 생성하고 요청 본문이 8192바이트보다 큰 요청을 차단할 수 있습니다.

주제

크기 제약 조건 생성

크기 제한 조건을 만들 때는 AWS WAF Classic에서 길이를 평가하려는 웹 요청 부분을 식별하는 필터를 지정합니다. 크기 제약 조건에 두 개 이상의 필터를 추가하거나 각 필터에 대해 별도의 조건을 생성할 수 있습니다. 각 구성이 AWS WAF Classic 동작에 미치는 영향은 다음과 같습니다.

- 크기 제약 조건당 필터 1개 - 규칙에 별도의 크기 제약 조건을 추가하고 웹 ACL에 규칙을 추가하는 경우 AWS WAF Classic에서 조건에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건과 일치해야 합니다.

  예컨대, 두 개의 조건을 생성한다고 가정합시다. 하나는 쿼리 문자열이 100바이트보다 큰 웹 요청과 일치합니다. 다른 하나는 요청 본문이 1024바이트보다 큰 웹 요청과 일치합니다. 동일한 규칙에 두 조건을 모두 추가하고 웹 ACL에 규칙을 추가하면 AWS WAF Classic은 두 조건이 모두 참일 때만 요청을 허용하거나 차단합니다.
- 크기 제약 조건당 하나 이상의 필터 — 여러 필터가 포함된 크기 제한 조건을 규칙에 추가하고 규칙을 웹 ACL에 추가하는 경우, AWS WAF Classic의 크기 제약 조건에 있는 필터 중 하나와 웹 요청만 일치하면 해당 조건에 따라 요청을 허용하거나 차단할 수 있습니다.

조건을 두 개 대신 한 개 만들고 한 조건에 이전 예와 같은 두 개의 필터가 포함되어 있다고 가정해 보겠습니다. AWS WAF Classic은 쿼리 문자열이 100바이트보다 크거나 요청 본문이 1024바이트를 초과하는 경우 요청을 허용하거나 차단합니다.

> **Note**
>
> 규칙에 크기 제한 조건을 추가할 때 조건의 값과 일치하지 않는 웹 요청을 허용하거나 차단하도록 AWS WAF Classic을 구성할 수도 있습니다.

크기 제약 조건을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Size constraints]를 선택합니다.
3. [Create condition]을 선택합니다.
4. 해당 필터 설정값을 지정합니다. 자세한 설명은 크기 제약 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.
5. [Add another filter]를 선택합니다.
6. 다른 필터를 추가하려는 경우, 4 ~ 5단계를 반복합니다.
7. 필터 추가를 완료했으면 [Create size constraint condition]을 선택합니다.

크기 제약 조건을 생성하거나 편집할 때 지정하는 값

크기 제약 조건을 생성하거나 업데이트할 때 다음 값을 지정합니다.

명칭

크기 제약 조건의 명칭을 입력합니다.

명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 조건을 생성한 후에는 조건의 명칭을 변경할 수 없습니다.

요청 중 필터링할 부분

AWS WAF Classic에서 길이를 평가할 각 웹 요청 부분을 선택합니다.

헤더

지정된 요청 헤더입니다(예: `User-Agent` 또는 `Referer` 헤더). [Header]를 선택하는 경우, [Header] 필드에서 헤더의 명칭을 지정합니다.

HTTP 메서드

요청이 오리진에게 수행할 것을 요구하고 있는 작업의 타입을 표시하는 HTTP 메서드입니다. CloudFront `DELETE`,,,, `GET` `HEAD` `OPTIONS` `PATCH`POST, 및 등의 메서드를 지원합니다PUT.

쿼리 문자열

URL 중 ? 문자 뒤에 나타나는 부분입니다(있는 경우).

URI

리소스를 식별하는 요청의 URI 경로(예: `/images/daily-ad.jpg`). 여기에는 URI의 쿼리 문자열 또는 조각 구성 요소는 포함되지 않습니다. 자세한 설명은 Uniform Resource Identifier (URI): Generic Syntax 섹션을 참조하세요.

변환이 지정되지 않는 한 URI는 정규화되지 않고 요청의 일부로 클라이언트로부터 AWS 수신하는 것처럼 검사됩니다. Transformation(변환)은 지정된 대로 URI를 다시 포맷합니다.

본문

요청 중 HTTP 요청 본문으로서 웹 서버에 보낼 추가 데이터(예: 양식의 데이터)가 들어 있는 부분입니다.

단일 쿼리 파라미터(값만 해당)

쿼리 문자열의 일부로 정의한 모든 파라미터입니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =시애틀”인 경우 or 매개 변수에 필터를 추가할 수 있습니다. UserNameSalesRegion

Single query parameter (value only)(단일 쿼리 파라미터(값만 해당))를 선택하는 경우, Query parameter name(쿼리 파라미터 명칭)도 지정합니다. 이 매개 변수는 검사할 쿼리 문자열의 매개 변수입니다 (예:). UserName Query parameter name(쿼리 파라미터 명칭)의 최대 길이는 30자입니다. Query parameter name(쿼리 파라미터 명칭)은 대/소문자를 구분하지 않습니다. 예를 들어 Query 매개 변수 이름으로 지정하는 UserName경우 이 이름은 사용자 이름 및 UserName과 같은 모든 변형과 일치합니다. UserName

모든 쿼리 파라미터(값만 해당)

AWS WAF Classic은 단일 쿼리 매개 변수 (값만 해당) 와 유사하지만 단일 매개 변수의 값을 검사하지 않고 쿼리 문자열 내 모든 매개 변수 값의 크기 제한을 검사합니다. 예를 들어 URL이

"www.xyz.com? UserName =abc& SalesRegion =satle"이고 모든 쿼리 매개 변수 (값만) 를 선택하면 AWS WAF Classic은 지정된 크기 중 하나 또는 초과할 경우 해당 값과 일치하는 값을 트리거합니다. UserNameSalesRegion

헤더("요청 중 필터링할 부분"이 "헤더"인 경우에만)

필터링 기준으로 사용할 요청의 일부로 헤더를 선택한 경우 공통 헤더 목록에서 헤더를 선택하거나 Classic에서 길이를 평가할 헤더의 이름을 입력합니다. AWS WAF

비교 연산자

AWS WAF Classic에서 [크기] 에 지정한 값을 기준으로 웹 요청의 쿼리 문자열 길이를 평가하는 방법을 선택합니다.

예를 들어, 비교 연산자에서 Is greater th를 선택하고 크기에 100을 입력하면 AWS WAF Classic은 100바이트보다 긴 쿼리 문자열에 대한 웹 요청을 평가합니다.

크기

AWS WAF Classic에서 쿼리 문자열에서 확인할 길이를 바이트 단위로 입력합니다.

> **Note**
>
> 요청 중 필터링할 부분 값으로 URI를 선택하면 URI의 /가 한 문자로 계수됩니다. 예컨대, URI 경로 `/logo.jpg`는 9자 길이입니다.

변환

변환은 AWS WAF Classic이 요청의 지정된 부분 길이를 평가하기 전에 웹 요청을 다시 포맷합니다. 이렇게 하면 공격자가 Classic을 우회하기 위해 웹 요청에 사용하는 특이한 형식이 일부 제거됩니다. AWS WAF

> **Note**
>
> 필터링할 요청의 일부로 본문을 선택하면 검사를 위해 처음 8192바이트만 전달되므로 변환을 수행하도록 AWS WAF Classic을 구성할 수 없습니다. 하지만 여전히 HTTP 요청의 크기에 근거하여 트래픽을 필터링하고 없음의 변환을 지정할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.)

단일 타입의 텍스트 변환만을 지정할 수 있습니다.

변환 기능을 사용하여 다음 작업을 수행할 수 있습니다.

None

AWS WAF Classic은 길이를 확인하기 전에는 웹 요청에서 텍스트 변환을 수행하지 않습니다.

소문자로 변환

AWS WAF Classic은 대문자 (A-Z) 를 소문자 (a-z) 로 변환합니다.

HTML 디코딩

AWS WAF Classic은 HTML로 인코딩된 문자를 인코딩되지 않은 문자로 대체합니다.

- "를 &로 바꿈
- 를 줄 바꿈하지 않는 공백으로 바꿈
- <를 <로 바꿈
- >를 >로 바꿈
- 16진수 형식으로 표현된 문자 &#xhhhh;를 해당 문자로 바꿈
- 십진수 형식으로 표현된 문자 &#nnnn;을 해당 문자로 바꿈

공백 표준화

AWS WAF Classic은 다음 문자를 공백 문자 (십진수 32) 로 바꿉니다.

- \f, 양식 피드, 십진수 12
- \t, 탭, 십진수 9
- \n, 줄 바꿈, 십진수 10
- \r, 캐리지 리턴, 십진수 13
- \v, 세로 탭, 십진수 11
- 줄 바꿈하지 않는 공백, 십진수 160

또한 이 옵션은 여러 개의 공백을 하나의 공백으로 바꿉니다.

명령행 간소화

작동 시스템 명령행 명령이 포함된 요청의 경우, 이 옵션을 사용하여 다음 변환을 수행합니다.

- 다음 문자를 삭제: \ " ' ^
- 다음 문자 앞에 있는 공백 삭제: / (
- 다음 문자를 공백으로 바꿈: , ;
- 여러 개의 공백을 하나의 공백으로 바꿈

- 대문자(A-Z)를 소문자(a-z)로 변환

URL 디코딩

URL 인코딩된 요청을 디코딩합니다.

크기 제약 조건에서 필터 추가 및 삭제

크기 제약 조건에서 필터를 추가하거나 삭제할 수 있습니다. 필터를 변경하려면 새 명칭을 추가하고 기존 명칭을 삭제합니다.

크기 제약 조건에서 필터를 추가하거나 삭제하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Size constraint]를 선택합니다.
3. 필터를 추가하거나 삭제하려는 조건을 선택합니다.
4. 필터를 추가하려면 다음 단계를 수행합니다.

   a. [Add filter]를 선택합니다.
   b. 해당 필터 설정값을 지정합니다. 자세한 설명은 크기 제약 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.
   c. 추가(Add)를 선택합니다.
5. 필터를 삭제하려면 다음 단계를 수행합니다.

   a. 삭제하려는 필터를 선택합니다.
   b. [Delete filter]를 선택합니다.

크기 제약 조건 삭제

크기 제약 조건을 삭제하려는 경우, 먼저 다음 절차의 설명에 따라 조건에 있는 모든 필터를 삭제하고 조건을 사용하고 있는 모든 규칙에서 조건을 제거해야 합니다.

크기 제약 조건을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 탐색 창에서 [Size constraints]를 선택합니다.
3. [Size constraint conditions] 창에서 삭제하려는 크기 제약 조건을 선택합니다.
4. 오른쪽 창에서 [Associated rules] 탭을 선택합니다.

   이 크기 제약 조건을 사용하는 규칙의 목록이 비어 있는 경우, 6단계로 이동합니다. 목록에 규칙이 포함되어 있는 경우, 규칙을 기록하고 5단계로 계속합니다.
5. 크기 제약 조건을 사용하고 있는 규칙에서 해당 조건을 제거하려면 다음 단계를 수행합니다.

   a. 탐색 창에서 규칙을 선택합니다.
   b. 삭제하려는 크기 제약 조건을 사용하고 있는 규칙의 명칭을 선택합니다.
   c. 오른쪽 창에서, 규칙에서 제거하려는 크기 제약 조건을 선택한 다음 [Remove selected condition]을 선택합니다.
   d. 삭제하려는 크기 제약 조건을 사용하고 있는 나머지 모든 규칙에 대해 b단계와 c단계를 반복합니다.
   e. 탐색 창에서 [Size constraint]를 선택합니다.
   f. [Size constraint conditions] 창에서 삭제하려는 크기 제약 조건을 선택합니다.
6. [Delete]를 선택하여 선택한 조건을 삭제합니다.

SQL 명령어 주입 매칭 조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

때로 공격자는 데이터베이스에서 데이터를 추출하기 위해 웹 요청에 악성 SQL 코드를 삽입합니다. 악성 SQL 코드가 포함된 것으로 보이는 웹 요청을 허용하거나 차단하려면 SQL 명령어 주입 매칭 조건을 하나 이상 생성합니다. SQL 인젝션 일치 조건은 URI 경로나 쿼리 문자열과 같이 AWS WAF Classic에서 검사하려는 웹 요청 부분을 식별합니다. 이 프로세스에서 나중에 웹 ACL을 생성할 때 악성 SQL 코드가 포함된 것으로 보이는 요청을 허용할지 또는 차단할지를 지정합니다.

주제

SQL 명령어 주입 매칭 조건 생성

SQL 삽입 일치 조건을 만들 때는 필터를 지정합니다. 이 필터는 AWS WAF Classic에서 URI나 쿼리 문자열과 같은 악성 SQL 코드를 검사하도록 하려는 웹 요청 부분을 나타냅니다. 두 개 이상의 필터를 SQL 명령어 주입 매칭 조건에 추가하거나 각 필터에 대해 별도의 조건을 생성할 수 있습니다. 각 구성이 AWS WAF Classic 동작에 미치는 영향은 다음과 같습니다.

- SQL 인젝션 일치 조건당 둘 이상의 필터 (권장) - 여러 필터를 포함하는 SQL 인젝션 일치 조건을 규칙에 추가하고 해당 규칙을 웹 ACL에 추가하는 경우, AWS WAF Classic에서 해당 조건에 따라 요청을 허용하거나 차단하려면 웹 요청이 SQL 삽입 일치 조건에 있는 필터 중 하나와 일치하기만 하면 됩니다.

  예를 들어, SQL 명령어 주입 매칭 조건을 하나 생성하고 조건에 두 개의 필터가 포함된다고 가정합시다. 한 필터는 AWS WAF Classic이 URI에서 악성 SQL 코드를 검사하도록 지시하고, 다른 필터는 Classic이 URI에 악성 SQL 코드를 검사하도록 지시하고, 다른 필터는 AWS WAF Classic에 쿼리 문자열을 검사하도록 지시합니다. AWS WAF Classic은 URI나 쿼리 문자열에 악성 SQL 코드가 포함된 것으로 보이는 경우 요청을 허용하거나 차단합니다.
- SQL 삽입 일치 조건당 필터 하나 - 별도의 SQL 삽입 일치 조건을 규칙에 추가하고 규칙을 웹 ACL에 추가하는 경우 AWS WAF Classic에서 조건에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건과 일치해야 합니다.

  두 개의 조건을 생성하고 각 조건에 이전 예에서 사용한 두 개의 필터 중 하나가 포함되어 있다고 가정합시다. 동일한 규칙에 두 조건을 추가하고 웹 ACL에 규칙을 추가하면 AWS WAF Classic은 URI와 쿼리 문자열 모두에 악성 SQL 코드가 포함된 것으로 보이는 경우에만 요청을 허용하거나 차단합니다.

> **Note**
>
> SQL 삽입 일치 조건을 규칙에 추가할 때 악성 SQL 코드가 포함되어 있지 않은 것으로 보이는 웹 요청을 허용하거나 차단하도록 AWS WAF Classic을 구성할 수도 있습니다.

SQL 명령어 주입 매칭 조건을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [SQL injection]을 선택합니다.
3. [Create condition]을 선택합니다.
4. 해당 필터 설정값을 지정합니다. 자세한 설명은 SQL 명령어 주입 매칭 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.
5. [Add another filter]를 선택합니다.
6. 다른 필터를 추가하려는 경우, 4 ~ 5단계를 반복합니다.
7. 필터 추가를 완료했으면 [Create]를 선택합니다.

SQL 명령어 주입 매칭 조건을 생성하거나 편집할 때 지정하는 값

SQL 명령어 주입 매칭 조건을 생성하거나 업데이트할 때 다음 값을 지정합니다.

명칭

SQL 명령어 주입 매칭 조건의 명칭입니다.

명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 조건을 생성한 후에는 조건의 명칭을 변경할 수 없습니다.

요청 중 필터링할 부분

각 웹 요청에서 AWS WAF Classic에서 악성 SQL 코드를 검사하도록 하려는 부분을 선택하십시오.

헤더

지정된 요청 헤더입니다(예: `User-Agent` 또는 `Referer` 헤더). [Header]를 선택하는 경우, [Header] 필드에서 헤더의 명칭을 지정합니다.

HTTP 메서드

요청이 오리진에게 수행할 것을 요구하고 있는 작업의 타입을 표시하는 HTTP 메서드입니다. CloudFront `DELETE`,,,, `GET` `HEAD` `OPTIONS` `PATCHPOST`, 및 등의 메서드를 지원합니다`PUT`.

쿼리 문자열

URL 중 ? 문자 뒤에 나타나는 부분입니다(있는 경우).

> **Note**
>
> SQL 명령어 삽입 매칭 조건의 경우, 요청 중 필터링할 부분에 대한 쿼리 문자열 대신 모든 쿼리 파라미터(값만)를 선택하는 것이 좋습니다.

URI

리소스를 식별하는 요청의 URI 경로(예: `/images/daily-ad.jpg`). 여기에는 URI의 쿼리 문자열 또는 조각 구성 요소는 포함되지 않습니다. 자세한 설명은 Uniform Resource Identifier (URI): Generic Syntax 섹션을 참조하세요.

변환이 지정되지 않는 한 URI는 정규화되지 않고 요청의 일부로 클라이언트로부터 AWS 수신하는 것처럼 검사됩니다. Transformation(변환)은 지정된 대로 URI를 다시 포맷합니다.

본문

요청 중 HTTP 요청 본문으로서 웹 서버에 보낼 추가 데이터(예: 양식의 데이터)가 들어 있는 부분입니다.

> **Note**
>
> 요청 중 필터링할 부분 값으로 본문을 선택하는 경우, AWS WAF Classic은 처음 8192 바이트(8KB)만 검사합니다. 본문이 8192바이트보다 긴 요청을 허용하거나 차단하려면 크기 제약 조건을 생성할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.) 자세한 정보는 크기 제약 조건 작업을 참조하세요.

단일 쿼리 파라미터(값만 해당)

쿼리 문자열의 일부로 정의한 모든 파라미터입니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =Seattle”인 경우 or 매개 변수에 필터를 추가할 수 있습니다. UserNameSalesRegion

Single query parameter (value only)(단일 쿼리 파라미터(값만 해당))를 선택하는 경우, Query parameter name(쿼리 파라미터 명칭)도 지정합니다. 검사할 쿼리 문자열의 매개 변수입니다 (예: 또는). UserNameSalesRegion Query parameter name(쿼리 파라미터 명칭)의 최대 길이는 30자입니다. Query parameter name(쿼리 파라미터 명칭)은 대/소문자를 구분하지 않습니다. 예를 들어 Query 매개 변수 이름으로 지정하는 UserName경우 이 이름은 사용자 이름 및 UserName과 같은 모든 변형과 일치합니다. UserName

모든 쿼리 파라미터(값만 해당)

AWS WAF Classic은 단일 쿼리 매개 변수 (값만 해당) 와 유사하지만 단일 매개 변수의 값을 검사하지 않고 쿼리 문자열 내의 모든 매개 변수 값에 악성 SQL 코드가 있는지 검사합니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =Seattle”이고 모든 쿼리 매개 변수 (값만) 를 선택하면 AWS WAF Classic에서 해당 값에 악성 SQL 코드가 포함되어 있거나 있을 수 있는 경우 일치 항목이 트리거됩니다. UserNameSalesRegion

헤더

요청의 일부로 필터링할 헤더를 선택한 경우 공통 헤더 목록에서 헤더를 선택하거나 Classic에서 악성 SQL 코드를 검사할 헤더 이름을 입력하십시오. AWS WAF

변환

변환은 AWS WAF Classic에서 요청을 검사하기 전에 웹 요청을 다시 포맷합니다. 이렇게 하면 공격자가 Classic을 우회하기 위해 웹 요청에 사용하는 일부 특이한 형식이 제거됩니다. AWS WAF

단일 타입의 텍스트 변환만을 지정할 수 있습니다.

변환 기능을 사용하여 다음 작업을 수행할 수 있습니다.

None

AWS WAF Classic에서는 Value 내의 문자열이 일치하는지 검사하기 전에는 웹 요청에서 텍스트 변형을 수행하지 않습니다.

소문자로 변환

AWS WAF Classic은 대문자 (A-Z) 를 소문자 (a-z) 로 변환합니다.

HTML 디코딩

AWS WAF Classic은 HTML로 인코딩된 문자를 인코딩되지 않은 문자로 대체합니다.

- `&quot;`를 &로 바꿈
- ` `를 줄 바꿈하지 않는 공백으로 바꿈
- `<`를 <로 바꿈
- `>`를 >로 바꿈
- 16진수 형식으로 표현된 문자 `&#xhhhh;`를 해당 문자로 바꿈
- 십진수 형식으로 표현된 문자 `&#nnnn;`을 해당 문자로 바꿈

공백 표준화

AWS WAF Classic은 다음 문자를 공백 문자 (십진수 32) 로 바꿉니다.

- \f, 양식 피드, 십진수 12
- \t, 탭, 십진수 9
- \n, 줄 바꿈, 십진수 10
- \r, 캐리지 리턴, 십진수 13
- \v, 세로 탭, 십진수 11
- 줄 바꿈하지 않는 공백, 십진수 160

또한 이 옵션은 여러 개의 공백을 하나의 공백으로 바꿉니다.

명령행 간소화

작동 시스템 명령행 명령이 포함된 요청의 경우, 이 옵션을 사용하여 다음 변환을 수행합니다.

- 다음 문자를 삭제: \ " ' ^
- 다음 문자 앞에 있는 공백 삭제: / (
- 다음 문자를 공백으로 바꿈: , ;
- 여러 개의 공백을 하나의 공백으로 바꿈
- 대문자(A-Z)를 소문자(a-z)로 변환

URL 디코딩

URL 인코딩된 요청을 디코딩합니다.

SQL 명령어 주입 매칭 조건에서 필터 추가 및 삭제

SQL 명령어 주입 매칭 조건에서 필터를 추가하거나 삭제할 수 있습니다. 필터를 변경하려면 새 명칭을 추가하고 기존 명칭을 삭제합니다.

SQL 명령어 주입 매칭 조건에서 필터를 추가하거나 삭제하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [SQL injection]을 선택합니다.
3. 필터를 추가하거나 삭제하려는 조건을 선택합니다.
4. 필터를 추가하려면 다음 단계를 수행합니다.

a. [Add filter]를 선택합니다.

b. 해당 필터 설정값을 지정합니다. 자세한 설명은 SQL 명령어 주입 매칭 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.

c. 추가(Add)를 선택합니다.

5. 필터를 삭제하려면 다음 단계를 수행합니다.

a. 삭제하려는 필터를 선택합니다.

b. [Delete filter]를 선택합니다.

SQL 명령어 주입 매칭 조건 삭제

SQL 명령어 주입 매칭 조건을 삭제하려는 경우, 먼저 다음 절차의 설명에 따라 조건에 있는 모든 필터를 삭제하고 조건을 사용하고 있는 모든 규칙에서 조건을 제거해야 합니다.

SQL 명령어 주입 매칭 조건을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 탐색 창에서 [SQL injection]을 선택합니다.
3. [SQL injection match conditions] 창에서 삭제하려는 SQL 명령어 주입 매칭 조건을 선택합니다.
4. 오른쪽 창에서 [Associated rules] 탭을 선택합니다.

   이 SQL 명령어 주입 매칭 조건을 사용하는 규칙 목록이 비어 있는 경우, 6단계로 이동합니다. 목록에 규칙이 포함되어 있는 경우, 규칙을 기록하고 5단계로 계속합니다.

5. SQL 명령어 주입 매칭 조건을 사용하고 있는 규칙에서 해당 조건을 제거하려면 다음 단계를 수행합니다.

a. 탐색 창에서 규칙을 선택합니다.

b. 삭제하려는 SQL 명령어 주입 매칭 조건을 사용하고 있는 규칙의 명칭을 선택합니다.

c. 오른쪽 창에서, 규칙에서 제거하려는 SQL 명령어 주입 매칭 조건을 선택하고 [Remove selected condition]을 선택합니다.

d. 삭제하려는 SQL 명령어 주입 매칭 조건을 사용하고 있는 나머지 모든 규칙에 대해 b단계와 c단계를 반복합니다.

e. 탐색 창에서 [SQL injection]을 선택합니다.

f. [SQL injection match conditions] 창에서 삭제하려는 SQL 명령어 주입 매칭 조건을 선택합니다.

6. [Delete]를 선택하여 선택한 조건을 삭제합니다.

문자열 매칭 조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

요청에 나타나는 문자열에 근거하여 웹 요청을 허용하거나 차단하려는 경우, 문자열 매칭 조건을 하나 이상 생성합니다. 문자열 일치 조건은 검색하려는 문자열과 AWS WAF Classic에서 해당 문자열에 대해 검사하려는 웹 요청의 일부 (예: 지정된 헤더 또는 쿼리 문자열) 를 식별합니다. 이 프로세스에서 나중에 웹 ACL을 생성할 때 문자열이 포함된 요청을 허용할지 또는 차단할지를 지정합니다.

주제

- 문자열 매칭 조건 생성
- 문자열 매칭 조건을 생성하거나 편집할 때 지정하는 값
- 문자열 매칭 조건에서 필터 추가 및 삭제
- 문자열 매칭 조건 삭제

문자열 매칭 조건 생성

문자열 일치 조건을 만들 때는 검색하려는 문자열과 해당 문자열에 대해 AWS WAF Classic에서 검사할 웹 요청의 일부 (예: URI 또는 쿼리 문자열) 를 식별하는 필터를 지정합니다. 문자열 매칭 조건에 두 개 이상의 필터를 추가하거나 각 필터에 대해 별도의 문자열 매칭 조건을 생성할 수 있습니다. 각 구성이 AWS WAF Classic 동작에 미치는 영향은 다음과 같습니다.

- 문자열 일치 조건당 필터 하나 - 별도의 문자열 일치 조건을 규칙에 추가하고 규칙을 웹 ACL에 추가하는 경우 AWS WAF Classic에서 조건에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건과 일치해야 합니다.

예컨대, 두 개의 조건을 생성한다고 가정합시다. 하나는 `User-Agent` 헤더에 `BadBot`라는 값이 포함된 웹 요청과 일치합니다. 다른 하나는 쿼리 문자열에 `BadParameter`라는 값이 포함된 웹 요청과 일치합니다. 동일한 규칙에 두 조건을 모두 추가하고 웹 ACL에 규칙을 추가하면 AWS WAF Classic은 두 값이 모두 포함된 경우에만 요청을 허용하거나 차단합니다.

- 문자열 일치 조건당 필터 두 개 이상 - 여러 필터를 포함하는 문자열 일치 조건을 규칙에 추가하고 규칙을 웹 ACL에 추가하는 경우 Classic에서 문자열 일치 조건에 있는 필터 중 하나와 일치하기만 하면 AWS WAF Classic에서 하나의 조건에 따라 요청을 허용하거나 차단하려면 웹 요청이 문자열 일치 조건에 있는 필터 중 하나와 일치해야 합니다.

  조건을 두 개 대신 한 개 만들고 한 조건에 이전 예와 같은 두 개의 필터가 포함되어 있다고 가정해 보겠습니다. AWS WAF Classic은 `User-Agent` 헤더나 쿼리 `BadBot` 문자열에 둘 중 하나가 포함된 요청을 허용하거나 `BadParameter` 차단합니다.

> **Note**
>
> 문자열 일치 조건을 규칙에 추가할 때 조건의 값과 일치하지 않는 웹 요청을 허용하거나 차단하도록 AWS WAF Classic을 구성할 수도 있습니다.

문자열 매칭 조건을 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [String and regex matching]을 선택합니다.
3. [Create condition]을 선택합니다.
4. 해당 필터 설정값을 지정합니다. 자세한 설명은 문자열 매칭 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.
5. [Add filter]를 선택합니다.
6. 다른 필터를 추가하려는 경우, 4 ~ 5단계를 반복합니다.
7. 필터 추가를 완료했으면 [Create]를 선택합니다.

문자열 매칭 조건을 생성하거나 편집할 때 지정하는 값

문자열 매칭 조건을 생성하거나 업데이트할 때 다음 값을 지정합니다.

명칭

문자열 매칭 조건의 명칭을 입력합니다. 명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 조건을 생성한 후에는 조건의 명칭을 변경할 수 없습니다.

타입

[String match]를 선택합니다.

요청 중 필터링할 부분

각 웹 요청에서 일치하는 값에 지정한 문자열이 있는지 AWS WAF Classic에서 검사할 부분을 선택합니다.

헤더

지정된 요청 헤더입니다(예: `User-Agent` 또는 `Referer` 헤더). [Header]를 선택하는 경우, [Header] 필드에서 헤더의 명칭을 지정합니다.

HTTP 메서드

요청이 오리진에게 수행할 것을 요구하고 있는 작업의 타입을 표시하는 HTTP 메서드입니다. CloudFront `DELETE`,,,, `GET` `HEAD` `OPTIONS` `PATCH`POST, 및 등의 메서드를 지원합니다PUT.

쿼리 문자열

URL 중 ? 문자 뒤에 나타나는 부분입니다(있는 경우).

URI

리소스를 식별하는 요청의 URI 경로(예: `/images/daily-ad.jpg`). 여기에는 URI의 쿼리 문자열 또는 조각 구성 요소는 포함되지 않습니다. 자세한 설명은 Uniform Resource Identifier (URI): Generic Syntax 섹션을 참조하세요.

변환이 지정되지 않는 한 URI는 정규화되지 않고 요청의 일부로 클라이언트로부터 AWS 수신하는 것처럼 검사됩니다. Transformation(변환)은 지정된 대로 URI를 다시 포맷합니다.

본문

요청 중 HTTP 요청 본문으로서 웹 서버에 보낼 추가 데이터(예: 양식의 데이터)가 들어 있는 부분입니다.

> **Note**
>
> 요청 중 필터링할 부분 값으로 본문을 선택하는 경우, AWS WAF Classic은 처음 8192 바이트(8KB)만 검사합니다. 본문이 8192바이트보다 긴 요청을 허용하거나 차단하려면 크기 제약 조건을 생성할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.) 자세한 정보는 크기 제약 조건 작업을 참조하세요.

단일 쿼리 파라미터(값만 해당)

쿼리 문자열의 일부로 정의한 모든 파라미터입니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =Seattle”인 경우 or 매개 변수에 필터를 추가할 수 있습니다. UserNameSalesRegion

쿼리 문자열에 중복 파라미터가 표시될 경우, 값이 "OR"로 평가됩니다. 즉, 두 값 중 하나가 일치를 트리거합니다. 예를 들어 URL “www.xyz.com? SalesRegion =boston& SalesRegion =시애틀”에서 일치할 값에 “보스턴” 또는 “시애틀”을 입력하면 매칭이 트리거됩니다.

Single query parameter (value only)(단일 쿼리 파라미터(값만 해당))를 선택하는 경우, Query parameter name(쿼리 파라미터 명칭)도 지정합니다. 검사할 쿼리 문자열의 매개 변수입니다 (예: 또는). UserNameSalesRegion Query parameter name(쿼리 파라미터 명칭)의 최대 길이는 30자입니다. Query parameter name(쿼리 파라미터 명칭)은 대/소문자를 구분하지 않습니다. 예를 들어 Query 매개 변수 이름으로 지정하는 UserName경우 이 이름은 사용자 이름 및 UserName과 같은 모든 변형과 일치합니다. UserName

모든 쿼리 파라미터(값만 해당)

AWS WAF Classic은 단일 쿼리 매개 변수 (값만 해당) 와 유사하지만 단일 매개 변수의 값을 검사하지 않고 쿼리 문자열에 있는 모든 매개 변수의 값이 일치하는지 검사합니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =satle"이고 모든 쿼리 매개 변수 (값만) 를 선택하면 AWS WAF Classic은 일치하는 값으로 또는 UserName이 값이 지정되면 일치를 트리거합니다. SalesRegion

헤더("요청 중 필터링할 부분"이 "헤더"인 경우에만)

필터링 대상 요청 부분 목록에서 헤더를 선택한 경우 공통 헤더 목록에서 헤더를 선택하거나 AWS WAF Classic에서 검사하려는 헤더의 이름을 입력하십시오.

일치 타입

AWS WAF Classic에서 검사하려는 요청 부분 내에서 Value to match의 문자열이 이 필터와 일치하도록 표시되어야 하는 위치를 선택하십시오.

포함

문자열이 요청의 지정된 부분에 아무 곳이나 나타납니다.

단어 포함

웹 요청의 지정된 부분에 [Value to match]가 포함되어야 하며 [Value to match]에는 영숫자 문자 또는 밑줄(A-Z, a-z, 0-9 또는 _)만 포함되어야 합니다. 또한 [Value to match]는 하나의 단어여야 합니다. 따라서 이 값은 다음 중 하나일 수 있습니다.

- [Value to match]가 웹 요청의 지정된 부분의 값(예: 헤더의 값)과 정확히 일치합니다.
- [Value to match]가 웹 요청의 지정된 부분의 시작 부분에 있고 그 뒤에 영숫자 또는 밑줄(_)을 제외한 다른 문자가 있습니다(예: `BadBot;`).
- [Value to match]가 웹 요청의 지정된 부분의 끝 부분에 있고 그 앞에 영숫자 또는 밑줄(_)을 제외한 다른 문자가 있습니다(예: `;BadBot`).
- [Value to match]가 웹 요청의 지정된 부분의 중간에 있고 그 앞과 뒤에 영숫자 또는 밑줄(_)을 제외한 다른 문자가 있습니다(예: `-BadBot;`).

정확히 일치

문자열과 요청의 지정된 부분의 값이 같습니다.

다음으로 시작

문자열이 요청의 지정된 부분의 시작 부분에 나타납니다.

다음으로 끝남

문자열이 요청의 지정된 부분의 끝에 나타납니다.

변환

변환은 AWS WAF Classic에서 요청을 검사하기 전에 웹 요청을 다시 포맷합니다. 이렇게 하면 공격자가 Classic을 우회하기 위해 웹 요청에 사용하는 일부 특이한 형식이 제거됩니다. AWS WAF

단일 타입의 텍스트 변환만을 지정할 수 있습니다.

변환 기능을 사용하여 다음 작업을 수행할 수 있습니다.

None

AWS WAF Classic에서는 Value 내의 문자열이 일치하는지 검사하기 전에는 웹 요청에서 텍스트 변형을 수행하지 않습니다.

소문자로 변환

AWS WAF Classic은 대문자 (A-Z) 를 소문자 (a-z) 로 변환합니다.

HTML 디코딩

AWS WAF Classic은 HTML로 인코딩된 문자를 인코딩되지 않은 문자로 대체합니다.

- "를 &로 바꿈
- 를 줄 바꿈하지 않는 공백으로 바꿈
- <를 <로 바꿈
- >를 >로 바꿈
- 16진수 형식으로 표현된 문자 &#xhhhh;를 해당 문자로 바꿈
- 십진수 형식으로 표현된 문자 &#nnnn;을 해당 문자로 바꿈

공백 표준화

AWS WAF Classic은 다음 문자를 공백 문자 (십진수 32) 로 바꿉니다.

- \f, 양식 피드, 십진수 12
- \t, 탭, 십진수 9
- \n, 줄 바꿈, 십진수 10
- \r, 캐리지 리턴, 십진수 13
- \v, 세로 탭, 십진수 11
- 줄 바꿈하지 않는 공백, 십진수 160

또한 이 옵션은 여러 개의 공백을 하나의 공백으로 바꿉니다.

명령행 간소화

공격자가 작동 시스템 명령행 명령을 삽입하고 이상한 형식을 사용하여 명령의 일부 또는 전부를 위장하고 있는지 우려되는 경우, 이 옵션을 사용하여 다음 변환을 수행합니다.

- 다음 문자를 삭제: \ " ' ^
- 다음 문자 앞에 있는 공백 삭제: / (
- 다음 문자를 공백으로 바꿈: , ;
- 여러 개의 공백을 하나의 공백으로 바꿈
- 대문자(A-Z)를 소문자(a-z)로 변환

URL 디코딩

URL 인코딩된 요청을 디코딩합니다.

값이 base64로 인코딩됨

[Value to match]의 값이 base64로 인코딩되는 경우, 이 확인란을 선택합니다. base64 인코딩을 사용하여 공격자가 요청에 포함시키는 인쇄할 수 없는 문자(예: 탭 및 줄 바꿈)를 지정합니다.

매칭시킬 값

AWS WAF Classic에서 웹 요청에서 검색하려는 값을 지정합니다. 최대 길이는 50바이트입니다. 값을 base64로 인코딩하는 경우, 값을 인코딩하기 전에 50바이트 최대 길이가 값에 적용됩니다.

문자열 매칭 조건에서 필터 추가 및 삭제

문자열 매칭 조건에 필터를 추가하거나 필터를 삭제할 수 있습니다. 필터를 변경하려면 새 명칭을 추가하고 기존 명칭을 삭제합니다.

문자열 매칭 조건에서 필터를 추가하거나 삭제하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [String and regex matching]을 선택합니다.
3. 필터를 추가하거나 삭제하려는 조건을 선택합니다.
4. 필터를 추가하려면 다음 단계를 수행합니다.

   a. [Add filter]를 선택합니다.

   b. 해당 필터 설정값을 지정합니다. 자세한 설명은 문자열 매칭 조건을 생성하거나 편집할 때 지정하는 값 섹션을 참조하세요.

   c. 추가(Add)를 선택합니다.
5. 필터를 삭제하려면 다음 단계를 수행합니다.

   a. 삭제하려는 필터를 선택합니다.

   b. [Delete Filter]를 선택합니다.

문자열 매칭 조건 삭제

문자열 매칭 조건을 삭제하려는 경우, 먼저 다음 절차의 설명에 따라 조건에 있는 모든 필터를 삭제하고 조건을 사용하고 있는 모든 규칙에서 조건을 제거해야 합니다.

문자열 매칭 조건을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 문자열 매칭 조건을 사용하고 있는 규칙에서 해당 조건을 제거합니다.

   a. 탐색 창에서 규칙을 선택합니다.

   b. 삭제하려는 문자열 매칭 조건을 사용하고 있는 규칙의 명칭을 선택합니다.

   c. 오른쪽 창에서 [Edit rule]을 선택합니다.

   d. 삭제하려는 조건 옆의 [X]를 선택합니다.

   e. 업데이트를 선택합니다.

   f. 삭제하려는 문자열 매칭 조건을 사용하고 있는 나머지 모든 규칙에 대해 반복합니다.
3. 삭제하려는 조건에서 필터를 제거합니다.

   a. 탐색 창에서 [String and regex matching]을 선택합니다.

   b. 삭제하려는 문자열 매칭 조건의 명칭을 선택합니다.

   c. 오른쪽 창에서 [Filter] 옆의 확인란을 선택하여 필터를 모두 선택합니다.

   d. [Delete filter]를 선택합니다.
4. 탐색 창에서 [String and regex matching]을 선택합니다.
5. [String and regex match conditions] 창에서 삭제하려는 문자열 매칭 조건을 선택합니다.
6. [Delete]를 선택하여 선택한 조건을 삭제합니다.

정규식 매칭 조건 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

요청에 나타나며 정규식 패턴과 일치하는 문자열에 근거하여 웹 요청을 허용하거나 차단하려는 경우, 정규식 매칭 조건을 하나 이상 생성합니다. 정규식 일치 조건은 검색하려는 패턴과 AWS WAF Classic에서 패턴을 검사하려는 웹 요청의 일부 (예: 지정된 헤더 또는 쿼리 문자열) 를 식별하는 문자열 일치 조건의 한 유형입니다. 이 프로세스에서 나중에 웹 ACL을 생성할 때 패턴이 포함된 요청을 허용할지 또는 차단할지 지정합니다.

주제

- 정규식 매칭 조건 생성
- RegEx 일치 조건을 만들거나 편집할 때 지정하는 값
- 정규식 매칭 조건 편집

정규식 매칭 조건 생성

정규식 매칭 조건을 생성할 때 검색하려는 문자열(정규식 사용)을 식별하는 패턴 세트를 지정합니다. 그런 다음 해당 패턴 세트를 AWS WAF Classic에서 검사할 웹 요청 부분 (예: URI 또는 쿼리 문자열) 을 지정하는 필터에 해당 패턴 세트를 추가합니다.

패턴 세트 하나에 여러 정규식을 추가할 수 있습니다. 이렇게 하면 해당 정규식이 OR과 결합됩니다. 즉 해당 요청 부분이 열거된 정규식과 일치하면 웹 요청이 패턴 세트와 일치합니다.

규칙에 정규식 일치 조건을 추가할 때 조건의 값과 일치하지 않는 웹 요청을 허용하거나 차단하도록 AWS WAF Classic을 구성할 수도 있습니다.

AWS WAF 클래식은 대부분의 표준 Perl 호환 정규 표현식 (PCRE) 을 지원합니다. 단, 다음은 지원하지 않습니다:

- 역참조 및 캡처 하위식
- 임의의 제로 너비 어설션
- 서브루틴 참조 및 재귀 패턴
- 조건 패턴
- 백트래킹 제어 명령어
- \C 단일 바이트 명령
- \R 줄 바꿈 일치 명령
- \K 일치 시작 초기화 명령
- 설명선 및 포함된 코드
- 원자 그룹 지정 및 소유 수량자

정규식 매칭 조건을 생성하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [String and regex matching]을 선택합니다.
3. [Create condition]을 선택합니다.
4. 해당 필터 설정값을 지정합니다. 자세한 설명은 RegEx 일치 조건을 만들거나 편집할 때 지정하는 값 섹션을 참조하세요.
5. 새 패턴 세트를 생성한 경우, [Create pattern set and add filter]를 선택하고, 기존 패턴 세트를 사용한 경우, [Add filter]를 선택합니다.
6. 생성을 선택하세요.

RegEx 일치 조건을 만들거나 편집할 때 지정하는 값

정규식 매칭 조건을 생성하거나 업데이트할 때 다음 값을 지정합니다.

명칭

정규식 매칭 조건의 명칭을 입력합니다. 명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 조건을 생성한 후에는 조건의 명칭을 변경할 수 없습니다.

타입

[Regex match]를 선택합니다.

요청 중 필터링할 부분

각 웹 요청에서 Value to Match에 지정한 패턴을 검사하여 AWS WAF Classic에서 검사할 부분을 선택합니다.

헤더

지정된 요청 헤더입니다(예: `User-Agent` 또는 `Referer` 헤더). [Header]를 선택하는 경우, [Header] 필드에서 헤더의 명칭을 지정합니다.

HTTP 메서드

요청이 오리진에게 수행할 것을 요구하고 있는 작업의 타입을 표시하는 HTTP 메서드입니다. CloudFront `DELETE`,,,, `GET` `HEAD` `OPTIONS` `PATCH`POST, 및 등의 메서드를 지원합니다PUT.

쿼리 문자열

URL 중 ? 문자 뒤에 나타나는 부분입니다(있는 경우).

URI

리소스를 식별하는 요청의 URI 경로(예: `/images/daily-ad.jpg`). 여기에는 URI의 쿼리 문자열 또는 조각 구성 요소는 포함되지 않습니다. 자세한 설명은 Uniform Resource Identifier (URI): Generic Syntax 섹션을 참조하세요.

변환이 지정되지 않는 한 URI는 정규화되지 않고 요청의 일부로 클라이언트로부터 AWS 수신하는 것처럼 검사됩니다. Transformation(변환)은 지정된 대로 URI를 다시 포맷합니다.

본문

요청 중 HTTP 요청 본문으로서 웹 서버에 보낼 추가 데이터(예: 양식의 데이터)가 들어 있는 부분입니다.

> **Note**
>
> 요청 중 필터링할 부분 값으로 본문을 선택하는 경우, AWS WAF Classic은 처음 8192 바이트(8KB)만 검사합니다. 본문이 8192바이트보다 긴 요청을 허용하거나 차단하려면 크기 제약 조건을 생성할 수 있습니다. (AWS WAF Classic은 요청 헤더에서 본문 길이를 가져옵니다.) 자세한 정보는 크기 제약 조건 작업을 참조하세요.

단일 쿼리 파라미터(값만 해당)

쿼리 문자열의 일부로 정의한 모든 파라미터입니다. 예를 들어 URL이 “www.xyz.com? UserName =abc& SalesRegion =Seattle”인 경우 or 매개 변수에 필터를 추가할 수 있습니다. UserNameSalesRegion

쿼리 문자열에 중복 파라미터가 표시될 경우, 값이 "OR"로 평가됩니다. 즉, 두 값 중 하나가 일치를 트리거합니다. 예를 들어 URL “www.xyz.com? SalesRegion =boston& SalesRegion =시애틀”에서 일치할 가치의 “보스턴” 또는 “시애틀”과 일치하는 패턴이 있으면 매칭이 트리거됩니다.

Single query parameter (value only)(단일 쿼리 파라미터(값만 해당))를 선택하는 경우, Query parameter name(쿼리 파라미터 명칭)도 지정합니다. 검사할 쿼리 문자열의 매개 변수입니다 (예: 또는). UserNameSalesRegion Query parameter name(쿼리 파라미터 명칭)의 최대 길이는 30자입니다. Query parameter name(쿼리 파라미터 명칭)은 대/소문자를 구분하지 않습니다. 예를 들어 Query 매개 변수 이름으로 지정하는 UserName경우 이 이름은 사용자 이름 및 UserName과 같은 모든 변형과 일치합니다. UserName

모든 쿼리 파라미터(값만 해당)

AWS WAF Classic은 단일 쿼리 매개 변수 (값만 해당) 와 유사하지만 단일 매개 변수의 값을 검사하지 않고 쿼리 문자열 내의 모든 매개 변수 값을 검사하여 일치하는 값에 지정된 패턴을 확인합니다. 예를 들어 URL “www.xyz.com? UserName =abc& SalesRegion =Seattle” URL에서 값이 일치하거나 일치하는 패턴이 일치하면 일치 항목이 트리거됩니다. UserNameSalesRegion

헤더("요청 중 필터링할 부분"이 "헤더"인 경우에만)

필터링 대상 요청 부분 목록에서 헤더를 선택한 경우 공통 헤더 목록에서 헤더를 선택하거나 Classic에서 검사하려는 헤더의 이름을 입력하십시오. AWS WAF

변환

변환은 AWS WAF Classic에서 요청을 검사하기 전에 웹 요청을 다시 포맷합니다. 이렇게 하면 공격자가 Classic을 우회하기 위해 웹 요청에 사용하는 일부 특이한 형식이 제거됩니다. AWS WAF

단일 타입의 텍스트 변환만을 지정할 수 있습니다.

변환 기능을 사용하여 다음 작업을 수행할 수 있습니다.

None

AWS WAF Classic에서는 Value 내의 문자열이 일치하는지 검사하기 전에는 웹 요청에서 텍스트 변형을 수행하지 않습니다.

소문자로 변환

AWS WAF Classic은 대문자 (A-Z) 를 소문자 (a-z) 로 변환합니다.

HTML 디코딩

AWS WAF Classic은 HTML로 인코딩된 문자를 인코딩되지 않은 문자로 대체합니다.

- "를 &로 바꿈
- 를 줄 바꿈하지 않는 공백으로 바꿈
- <를 <로 바꿈
- >를 >로 바꿈
- 16진수 형식으로 표현된 문자 &#xhhhh;를 해당 문자로 바꿈
- 십진수 형식으로 표현된 문자 &#nnnn;을 해당 문자로 바꿈

공백 표준화

AWS WAF Classic은 다음 문자를 공백 문자 (십진수 32) 로 바꿉니다.

- \f, 양식 피드, 십진수 12
- \t, 탭, 십진수 9
- \n, 줄 바꿈, 십진수 10
- \r, 캐리지 리턴, 십진수 13
- \v, 세로 탭, 십진수 11
- 줄 바꿈하지 않는 공백, 십진수 160

또한 이 옵션은 여러 개의 공백을 하나의 공백으로 바꿉니다.

명령행 간소화

공격자가 작동 시스템 명령행 명령을 삽입하고 이상한 형식을 사용하여 명령의 일부 또는 전부를 위장하고 있는지 우려되는 경우, 이 옵션을 사용하여 다음 변환을 수행합니다.

- 다음 문자를 삭제: \ " ' ^
- 다음 문자 앞에 있는 공백 삭제: / (
- 다음 문자를 공백으로 바꿈: , ;
- 여러 개의 공백을 하나의 공백으로 바꿈
- 대문자(A-Z)를 소문자(a-z)로 변환

URL 디코딩

URL 인코딩된 요청을 디코딩합니다.

요청과 매칭시킬 정규식 패턴

기존 패턴 세트를 선택하거나 새 패턴 세트를 생성할 수 있습니다. 새 패턴 세트를 생성하는 경우, 다음을 지정하십시오:

새 패턴 세트 명칭

이름을 입력한 다음 Classic에서 검색할 정규식 패턴을 지정합니다. AWS WAF

패턴 세트 하나에 여러 정규식을 추가하면 해당 정규식은 OR과 결합됩니다. 즉 해당 요청 부분이 열거된 정규식과 일치하면 웹 요청이 패턴 세트와 일치합니다.

[Value to match]의 최대 길이는 70자입니다.

정규식 매칭 조건 편집

기존의 정규식 매칭 조건을 다음과 같이 변경할 수 있습니다.

- 기존 패턴 세트에서 패턴 삭제
- 기존 패턴 세트에 패턴 추가
- 기존의 정규식 매칭 조건에서 필터 삭제
- 기존 정규식 매칭 조건에 필터 추가(정규식 매칭 조건에는 필터를 하나만 사용할 수 있습니다. 따라서 필터를 추가하기 위해서는 기존 필터를 먼저 삭제해야 합니다.)
- 기존의 정규식 매칭 조건 삭제

> **Note**
>
> 기존 필터에서 패턴 세트를 추가하거나 삭제할 수 없습니다. 패턴 세트를 편집하거나 필터를 삭제한 후, 새 패턴 세트로 새 필터를 생성해야 합니다.

기존 패턴 세트에서 패턴을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [String and regex matching]을 선택합니다.
3. [View regex pattern sets]를 선택합니다.
4. 편집하려는 패턴 세트의 명칭을 선택합니다.
5. 편집을 선택합니다.
6. 삭제하려는 패턴 옆의 [X]를 선택합니다.
7. 저장을 선택합니다.

기존 패턴 세트에 패턴을 추가하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [String and regex matching]을 선택합니다.
3. [View regex pattern sets]를 선택합니다.
4. 편집할 패턴 세트의 명칭을 선택합니다.

5. 편집을 선택합니다.
6. 새 정규식 패턴을 입력합니다.
7. 새 패턴 옆의 [+]를 선택합니다.
8. 저장을 선택합니다.

기존의 정규식 매칭 조건에서 필터를 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [String and regex matching]을 선택합니다.
3. 삭제하려는 필터가 있는 조건의 명칭을 선택합니다.
4. 삭제하려는 필터 옆의 상자를 선택합니다.
5. [Delete filter]를 선택합니다.

정규식 매칭 조건을 삭제하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 정규식 조건에서 필터를 삭제합니다. 해당 지침은 기존의 정규식 매칭 조건에서 필터를 삭제하려면을 참조하세요.
3. 정규식 매칭 조건을 사용하고 있는 규칙에서 해당 조건을 제거합니다.
   a. 탐색 창에서 규칙을 선택합니다.
   b. 삭제하려는 정규식 매칭 조건을 사용하고 있는 규칙의 명칭을 선택합니다.
   c. 오른쪽 창에서 [Edit rule]을 선택합니다.
   d. 삭제하려는 조건 옆의 [X]를 선택합니다.
   e. 업데이트를 선택합니다.
   f. 삭제하려는 정규식 매칭 조건을 사용하고 있는 나머지 모든 규칙에 대해 반복합니다.
4. 탐색 창에서 [String and regex matching]을 선택합니다.
5. 삭제하려는 조건 옆의 버튼을 선택합니다.

6. 삭제를 선택합니다.

기존의 정규식 매칭 조건에 필터를 추가하거나 변경하려면

정규식 매칭 조건 하나에 필터 한 개만 허용됩니다. 필터를 추가하거나 변경하려면 먼저 기존 필터를 삭제해야 합니다.

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 변경하려는 정규식 조건에서 필터를 삭제합니다. 해당 지침은 기존의 정규식 매칭 조건에서 필터를 삭제하려면을 참조하세요.
3. 탐색 창에서 [String and regex matching]을 선택합니다.
4. 변경하려는 조건의 명칭을 선택합니다.
5. [Add filter]를 선택합니다.
6. 새 필터에 대한 적절한 값을 입력한 후 [Add]를 선택합니다.

규칙 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

규칙을 사용하면 Classic에서 감시할 조건을 정확히 지정하여 AWS WAF Classic에서 허용하거나 차단할 웹 요청을 정확하게 타겟팅할 수 있습니다. AWS WAF 예를 들어 AWS WAF Classic은 요청이 시작된 IP 주소, 요청에 포함된 문자열 및 문자열이 나타나는 위치, 요청에 악성 SQL 코드가 포함된 것으로 보이는지 여부를 감시할 수 있습니다.

주제

- 규칙 생성 및 조건 추가

- 규칙에서 조건 추가 및 제거
- 규칙 삭제
- AWS Marketplace 규칙 그룹

규칙 생성 및 조건 추가

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

규칙에 조건을 두 개 이상 추가하는 경우 AWS WAF Classic에서 해당 규칙에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건과 일치해야 합니다.

규칙을 생성하고 조건을 추가하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 규칙을 선택합니다.
3. 규칙 생성을 선택합니다.
4. 다음 값을 입력합니다.

   명칭

   명칭을 입력합니다.

   CloudWatch 지표 이름

   AWS WAF Classic에서 생성하여 규칙과 연결할 CloudWatch 지표의 이름을 입력합니다. 명칭은 최대 길이 128자 및 최소 길이 1자가 가능하며 영숫자(A-Z, a-z, 0-9)만 포함할 수 있습니다. 여기에는 “All” 및 “Default_Action”을 포함하여 AWS WAF 클래식용으로 예약된 공백 또는 지표 이름을 포함할 수 없습니다.

규칙 타입

`Regular rule` 또는 `Rate-based rule`을 선택합니다. 속도 기반 규칙은 일반 규칙과 동일하지만, IP 주소로부터 5분 내에 도달하는 요청의 개수도 고려합니다. 이러한 규칙 타입에 대한 자세한 설명은 AWS WAF 클래식 작동 방식 섹션을 참조하세요.

비율 제한

비율 기반 규칙의 경우, 규칙의 조건과 일치하는 IP 주소로부터 5분 동안 허용할 최대 요청 수를 입력합니다. 속도 제한은 최소한 100 이상이어야 합니다.

비율 제한만 지정하거나 비율 제한 및 조건을 지정할 수 있습니다. 속도 제한만 지정하는 경우 모든 IP AWS WAF 주소에 제한이 적용됩니다. 속도 제한 및 조건을 지정하는 경우 AWS WAF 조건과 일치하는 IP 주소를 제한합니다.

IP 주소가 속도 제한 임계값에 도달하면 일반적으로 30초 이내에 최대한 빨리 할당된 작업 (블록 또는 카운트) 을 AWS WAF 적용합니다. 조치가 취해진 후 IP 주소의 요청 없이 5분이 경과하면 카운터가 0으로 AWS WAF 재설정됩니다.

5. 조건을 규칙에 추가하려면 다음 값을 지정합니다.

요청이 다음과 같을 때/같지 않을 때

AWS WAF Classic에서 조건의 필터를 기반으로 요청을 허용하거나 차단하도록 하려면 dose를 선택하십시오. 예를 들어 IP 일치 조건에 192.0.2.0/24의 IP 주소 범위가 포함되고 AWS WAF Classic에서 해당 IP 주소에서 오는 요청을 허용하거나 차단하도록 하려면 [확인] 을 선택합니다.

AWS WAF Classic에서 조건에 있는 필터의 역수를 기준으로 요청을 허용하거나 차단하도록 하려면 허용하지 않음을 선택하십시오. 예를 들어 IP 일치 조건에 192.0.2.0/24의 IP 주소 범위가 포함되고 AWS WAF Classic에서 해당 IP 주소에서 오지 않는 요청을 허용 또는 차단하도록 하려면 [안 함] 을 선택합니다.

일치/시작

규칙에 추가할 조건 타입을 선택합니다.

- 교차 사이트 스크립팅 매칭 조건 - 교차 사이트 스크립팅 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
- IP 매칭 조건 - IP 주소에서 기원을 선택합니다.
- 지리 매칭 조건 - 지리적 위치에서 기원을 선택합니다.
- 크기 제약 조건 - 크기 제약 조건에서 필터 1개 이상과 일치를 선택합니다.

- SQL 명령어 주입 매칭 조건 - SQL 명령어 주입 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
- 문자열 매칭 조건 - 문자열 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
- 정규식 매칭 조건 - 정규식 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.

조건 명칭

규칙에 추가할 조건을 선택합니다. 이 목록에는 이전 단계에서 선택한 타입의 조건만 표시됩니다.

6. 규칙에 다른 조건을 추가하려는 경우, [Add another condition]을 선택하고 4~5단계를 반복합니다. 유념할 사항:
   - 조건을 두 개 이상 추가하는 경우 AWS WAF Classic에서 해당 규칙에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건에서 하나 이상의 필터와 일치해야 합니다.
   - 동일한 규칙에 두 개의 IP 일치 조건을 추가하면 AWS WAF Classic은 두 IP 일치 조건에 모두 나타나는 IP 주소에서 시작된 요청만 허용하거나 차단합니다.
7. 조건 추가를 완료했으면 [Create]를 선택합니다.

규칙에서 조건 추가 및 제거

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

조건을 추가하거나 제거하여 규칙을 변경할 수 있습니다.

규칙에서 조건을 추가하거나 제거하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 규칙을 선택합니다.

3. 조건을 추가하거나 제거하려는 규칙의 명칭을 선택합니다.
4. 규칙 추가를 선택합니다.
5. 조건을 추가하려면 [Add condition]을 선택하고 다음 값을 지정합니다.

   요청이 다음과 같을 때/같지 않을 때

   AWS WAF Classic에서 특정 조건의 필터를 기반으로 요청을 허용하거나 차단하도록 하려면 (예: 192.0.2.0/24 IP 주소 범위에서 시작되는 웹 요청) 허용을 선택하십시오.

   AWS WAF Classic에서 조건에 있는 필터의 역수를 기준으로 요청을 허용 또는 차단하도록 하려면 [안 함] 을 선택합니다. 예를 들어 IP 일치 조건에 192.0.2.0/24의 IP 주소 범위가 포함되고 AWS WAF Classic에서 해당 IP 주소에서 오지 않는 요청을 허용 또는 차단하도록 하려면 [안 함] 을 선택합니다.

   일치/시작

   규칙에 추가할 조건 타입을 선택합니다.

   - 교차 사이트 스크립팅 매칭 조건 - 교차 사이트 스크립팅 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
   - IP 매칭 조건 - IP 주소에서 기원을 선택합니다.
   - 지리 매칭 조건 - 지리적 위치에서 기원을 선택합니다.
   - 크기 제약 조건 - 크기 제약 조건에서 필터 1개 이상과 일치를 선택합니다.
   - SQL 명령어 주입 매칭 조건 - SQL 명령어 주입 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
   - 문자열 매칭 조건 - 문자열 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
   - 정규식 매칭 조건 - 정규식 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.

   조건 명칭

   규칙에 추가할 조건을 선택합니다. 이 목록에는 이전 단계에서 선택한 타입의 조건만 표시됩니다.
6. 조건을 제거하려면 해당 조건 명칭 오른쪽의 [X]를 선택합니다.
7. 업데이트를 선택합니다.

규칙 삭제

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

규칙을 삭제하려는 경우, 먼저 규칙을 사용하고 있는 웹 ACL에서 규칙을 제거하고 규칙에 포함된 조건을 제거해야 합니다.

규칙을 삭제하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 규칙을 사용하고 있는 웹 ACL에서 규칙을 제거하려면 웹 ACL 각각에 대해 다음 단계를 수행하십시오:

   a. 탐색 창에서 [Web ACLs]를 선택합니다.

   b. 삭제하려는 규칙을 사용하고 있는 웹 ACL의 명칭을 선택합니다.

   c. [Rules] 탭을 선택합니다.

   d. [Edit web ACL]을 선택합니다.

   e. 삭제하려는 규칙의 오른쪽에 있는 X를 선택한 후 업데이트를 선택합니다.
3. 탐색 창에서 규칙을 선택합니다.
4. 삭제하려는 규칙의 명칭을 선택합니다.
5. 삭제를 선택합니다.

AWS Marketplace 규칙 그룹

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF Classic은 리소스를 보호하는 데 도움이 되는 AWS Marketplace 규칙 그룹을 제공합니다. AWS Marketplace 규칙 그룹은 AWS 파트너 회사와 파트너 회사에서 작성하고 업데이트하는 사전 정의된 ready-to-use 규칙 모음입니다. AWS

일부 AWS Marketplace 규칙 그룹은 Joomla 또는 PHP와 같은 WordPress 특정 유형의 웹 애플리케이션을 보호하는 데 도움이 되도록 설계되었습니다. 다른 AWS Marketplace 규칙 그룹은 알려진 위협이나 OWASP Top 10에 나열된 것과 같은 일반적인 웹 애플리케이션 취약성으로부터 광범위한 보호를 제공합니다.

선호하는 AWS 파트너의 단일 AWS Marketplace 규칙 그룹을 설치할 수 있으며, 보호 강화를 위해 사용자 지정된 AWS WAF Classic 규칙을 추가할 수도 있습니다. PCI 또는 HIPAA 등의 규제를 준수해야 하는 경우 AWS Marketplace 규칙 그룹을 사용하여 웹 애플리케이션 방화벽 요구 사항을 충족할 수 있습니다.

AWS Marketplace 규칙 그룹은 장기 계약 및 최소 약정 없이 사용할 수 있습니다. 규칙 그룹을 구독하면 월간 요금(시간별 비례 할당으로 계산됨) 및 볼륨을 기반으로 한 지속적인 요청 요금이 부과됩니다. 자세한 내용은 AWS WAF 클래식 가격 책정 및 각 AWS Marketplace 규칙 그룹에 대한 AWS Marketplace설명을 참조하십시오.

자동 업데이트

끊임없이 변화하는 위협 환경에 대한 최신 정보를 파악하려면 시간과 비용이 많이 들 수 있습니다. AWS Marketplace AWS WAF Classic을 구현하고 사용할 때 규칙 그룹을 사용하면 시간을 절약할 수 있습니다. 또 다른 이점은 새로운 AWS 취약성과 위협이 나타나면 AWS 파트너가 AWS Marketplace 규칙 그룹을 자동으로 업데이트한다는 것입니다.

널리 공개되기 전에 많은 파트너에게 새로운 취약성에 대해 알립니다. 파트너는 새로운 위협이 널리 알려지기 전에 규칙 그룹을 업데이트한 후 이를 배포할 수 있습니다. 또한 가장 관련된 규칙을 작성하기 위해 가장 최근 위협을 조사하고 분석하는 위협 연구 팀도 있습니다.

규칙 그룹의 규칙에 대한 AWS Marketplace 액세스

각 AWS Marketplace 규칙 그룹은 차단하도록 설계된 공격 및 취약성 유형에 대한 포괄적인 설명을 제공합니다. 규칙 그룹 제공자의 지적 재산을 보호하기 위해 규칙 그룹 내의 개별 규칙은 볼 수 없습니다. 이러한 제한을 통해 악의적인 사용자가 게시된 규칙을 교묘하게 회피하는 위협을 설계하는 것을 방지할 수 있습니다.

규칙 그룹의 개별 규칙은 볼 수 없으므로 AWS Marketplace 규칙 그룹의 규칙도 편집할 수 없습니다. AWS Marketplace 하지만 규칙 그룹에서 특정 규칙을 제외할 수 있습니다. 이 기능을 "규칙 그룹 제외"라고 합니다. 규칙을 제외해도 해당 규칙이 제거되지 않습니다. 그 대신, 규칙에 대한 작업이 COUNT로 변경됩니다. 따라서 제외된 규칙과 일치하는 요청은 가산되지만 차단되지 않습니다. 제외된 각 규칙에 대한 COUNT 지표가 수신됩니다.

규칙을 제외하면 예기치 않게 트래픽을 차단하는 규칙 그룹의 문제(거짓 긍정)를 해결할 때 도움이 될 수 있습니다. 문제 해결 기법 중 하나는 규칙 그룹 내에서 원하는 트래픽을 차단하는 특정 규칙을 식별한 다음 해당 특정 규칙을 비활성화(제외)하는 것입니다.

특정 규칙을 제외하는 것 외에도 전체 규칙 그룹을 활성화하거나 비활성화하고 수행할 규칙 그룹 작업을 선택하여 보호를 세분화할 수 있습니다. 자세한 정보는 AWS Marketplace 규칙 그룹 사용을 참조하세요.

할당량

AWS Marketplace 규칙 그룹은 하나만 활성화할 수 있습니다. 를 사용하여 생성한 사용자 지정 규칙 그룹 하나를 활성화할 수도 AWS Firewall Manager있습니다. 이러한 규칙 그룹은 웹 ACL당 10개의 규칙 최대 할당량에 가산됩니다. 따라서 단일 웹 ACL에 AWS Marketplace 규칙 그룹 1개, 사용자 지정 규칙 그룹 1개, 사용자 지정 규칙 최대 8개를 포함할 수 있습니다.

요금

AWS Marketplace 규칙 그룹 요금에 대해서는 AWS WAF 클래식 가격 책정 및 의 각 AWS Marketplace 규칙 그룹에 대한 AWS Marketplace설명을 참조하십시오.

AWS Marketplace 규칙 그룹 사용

AWS WAF Classic 콘솔에서 AWS Marketplace 규칙 그룹을 구독하거나 구독을 취소할 수 있습니다. 하지만 규칙 그룹에서 특정 규칙을 제외할 수도 있습니다.

AWS Marketplace 규칙 그룹을 구독하고 사용하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 탐색 창에서 [Marketplace]를 선택합니다.
3. [Available marketplace products] 섹션에서 규칙 그룹의 이름을 선택하여 세부 정보 및 요금 정보를 봅니다.
4. 규칙 그룹을 구독하려면 [Continue]를 선택합니다.

> **Note**
>
> 이 규칙 그룹을 구독하지 않으려면 브라우저에서 이 페이지를 닫으면 됩니다.

5. [Set up your account]를 선택합니다.
6. 개별 그룹을 추가한 것처럼 웹 ACL에 규칙 그룹을 추가합니다. 자세한 내용은 웹 ACL 생성 또는 웹 ACL 편집을 참조하세요.

> **Note**
>
> 웹 ACL에 규칙 그룹을 추가할 때 규칙 그룹에 대해 설정한 작업(No override(재정의 없음) 또는 Override to count(가산하도록 재정의))을 규칙 그룹 재정의 작업이라고 합니다. 자세한 정보는 규칙 그룹 재정의을 참조하세요.

AWS Marketplace 규칙 그룹의 구독을 취소하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 모든 웹 ACL에서 규칙 그룹을 제거합니다. 자세한 정보는 웹 ACL 편집을 참조하세요.
3. 탐색 창에서 [Marketplace]를 선택합니다.
4. [Manage your subscriptions]를 선택합니다.
5. 구독을 취소할 규칙 그룹의 이름 옆에 있는 [Cancel subscription]을 선택합니다.
6. 예, 구독 취소를 선택합니다.

규칙 그룹에서 규칙을 제외하려면(규칙 그룹 제외)

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 아직 활성화하지 않은 경우 AWS WAF 클래식 로깅을 활성화하십시오. 자세한 정보는 웹 ACL 트래픽 정보 로깅을 참조하세요. AWS WAF 클래식 로그를 사용하여 제외하려는 규칙의 ID를 식별하십시오. 이러한 규칙은 일반적으로 정당한 요청을 차단하는 규칙입니다.
3. 탐색 창에서 [Web ACLs]를 선택합니다.
4. 편집하려는 웹 ACL의 명칭을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.

   > **Note**
   >
   > 규칙 그룹에서 규칙을 제외하려면 먼저 편집할 규칙 그룹을 웹 ACL과 연결해야 합니다.

5. 오른쪽 창의 [Rules] 탭에서 [Edit web ACL]을 선택합니다.
6. Rule group exceptions(규칙 그룹 제외) 섹션에서 편집할 규칙 그룹을 확장합니다.
7. 제외할 규칙 옆에 있는 X를 선택합니다. AWS WAF 클래식 로그를 사용하면 올바른 규칙 ID를 식별할 수 있습니다.
8. 업데이트를 선택합니다.

   규칙을 제외해도 규칙 그룹에서 해당 규칙이 제거되지 않습니다. 그 대신, 규칙에 대한 작업이 COUNT로 변경됩니다. 따라서 제외된 규칙과 일치하는 요청은 가산되지만 차단되지 않습니다. 제외된 각 규칙에 대한 COUNT 지표가 수신됩니다.

   > **Note**
   >
   > 이와 동일한 절차를 사용하여 AWS Firewall Manager에서 생성한 사용자 지정 규칙 그룹에서 규칙을 제외할 수 있습니다. 하지만 이러한 단계를 사용하여 사용자 지정 규칙 그룹에서 규칙을 제외하는 대신, AWS WAF 클래식 규칙 그룹에서 규칙 추가 및 삭제에 설명된 단계를 사용하여 사용자 지정 규칙 그룹을 간편하게 편집할 수도 있습니다.

규칙 그룹 재정의

AWS Marketplace 규칙 그룹에는 재정의 없음과 개수 재정의라는 두 가지 동작이 있습니다. 규칙 그룹을 테스트하려면 작업을 [Override to count]로 설정합니다. 이 규칙 그룹 작업은 그룹 내에 포함된 개별 규칙에 따라 지정되는 모든 block 작업을 재정의합니다. 즉, 규칙 그룹의 작업이 [Override to count]로 설정되면 그룹 내 개별 규칙의 작업에 따라 일치하는 요청을 잠재적으로 차단하는 대신 해당 요청이 계산됩니다. 반대로, 규칙 그룹의 작업을 [No override]로 설정하면 그룹 내 개별 규칙의 작업이 사용됩니다.

AWS Marketplace 규칙 그룹 문제 해결

AWS Marketplace 규칙 그룹이 합법적인 트래픽을 차단하고 있는 경우 다음 단계를 수행하십시오.

AWS Marketplace 규칙 그룹의 문제를 해결하려면

1. 정당한 트래픽을 차단하는 특정 규칙을 제외합니다. AWS WAF 클래식 로그를 사용하여 어떤 규칙이 어떤 요청을 차단하는지 식별할 수 있습니다. 규칙 제외에 대한 자세한 내용은 규칙 그룹에서 규칙을 제외하려면(규칙 그룹 제외) 단원을 참조하세요.
2. 특정 규칙을 제외해도 문제가 해결되지 않는 경우, AWS Marketplace 규칙 그룹의 동작을 재정의 없음에서 오버라이드 투 카운트로 변경할 수 있습니다. 그러면 규칙 그룹 내의 개별 규칙 작업에 관계없이 웹 요청이 통과할 수 있습니다. 또한 규칙 그룹에 대한 Amazon CloudWatch 지표도 제공됩니다.
3. AWS Marketplace 규칙 그룹 작업을 Override to count로 설정한 후에는 규칙 그룹 공급자의 고객 지원 팀에 문의하여 문제를 추가로 해결하십시오. 연락처 정보는 AWS Marketplace의 제품 목록 페이지에 나열된 규칙 그룹을 참조하세요.

고객 지원 팀에 문의

AWS WAF Classic 또는 에서 관리하는 AWS규칙 그룹에 문제가 있는 경우 문의하세요. AWS Support 파트너가 관리하는 규칙 그룹에 문제가 있는 경우 해당 AWS 파트너의 고객 지원 팀에 문의하세요. 파트너 연락처 정보를 찾으려면 파트너 목록을 참조하십시오 AWS Marketplace.

AWS Marketplace 규칙 그룹 생성 및 판매

AWS Marketplace 규칙 그룹을 판매하려면 소프트웨어 판매 방법을 참조하십시오 AWS Marketplace. AWS Marketplace

웹 ACL 작업

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 ACL에 규칙을 추가할 때 규칙의 조건에 따라 AWS WAF Classic에서 요청을 허용할지 차단할지를 지정합니다. 웹 ACL에 규칙을 두 개 이상 추가하는 경우 AWS WAF Classic은 웹 ACL에 규칙을 나열한 순서대로 각 요청을 규칙과 비교하여 평가합니다. 웹 요청이 규칙의 모든 조건과 일치하면 AWS WAF Classic은 즉시 해당 조치 (허용 또는 차단) 를 취하고 웹 ACL의 나머지 규칙 (있는 경우) 에 대해 요청을 평가하지 않습니다.

웹 요청이 웹 ACL의 어떤 규칙과도 일치하지 않는 경우 AWS WAF Classic은 웹 ACL에 지정된 기본 작업을 수행합니다. 자세한 정보는 웹 ACL에 대한 기본 조치 결정을 참조하세요.

요청을 허용하거나 차단하는 데 규칙을 사용하기 전에 규칙을 테스트하려는 경우 규칙의 조건과 일치하는 웹 요청을 계산하도록 AWS WAF Classic을 구성하면 됩니다. 자세한 내용은 웹 ACL 테스트을(를) 참조하세요.

주제

웹 ACL에 대한 기본 조치 결정

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 ACL을 만들고 구성할 때 가장 먼저 내려야 하는 가장 중요한 결정은 AWS WAF Classic에서 웹 요청을 허용할지 아니면 웹 요청을 차단할지 여부입니다. 기본 동작은 사용자가 지정한 모든 조건에 대해 웹 요청을 검사한 후 AWS WAF Classic에서 수행하려는 작업을 나타내며, 웹 요청이 해당 조건 중 하나와 일치하지 않는 경우 Classic에서 수행할 작업을 나타냅니다.

- 허용 - 대부분의 사용자가 웹사이트에 액세스할 수 있도록 허용하려고 하지만 지정된 IP 주소에서 요청이 기원되거나 요청에 악성 SQL 코드 또는 지정된 값이 포함된 것으로 보이는 공격자에게는 액세스를 차단하려는 경우, 기본 조치로 허용을 선택합니다.
- 차단 - 대부분의 예비 사용자가 웹사이트에 액세스하지 못하도록 하려고 하지만 지정된 IP 주소에서 요청이 기원되거나 요청에 지정된 값이 포함된 사용자에게 액세스를 허용하려는 경우, 기본 조치로 차단을 선택합니다.

기본 조치를 결정한 후 수행하는 많은 결정은 대부분의 웹 요청을 허용할지 또는 차단할지에 따라 결정됩니다. 예를 들어, 대부분의 요청을 허용하려는 경우, 일반적으로 생성하는 매칭 조건은 차단하려는 웹 요청을 지정해야 합니다. 예를 들면 다음과 같습니다:

- 합당하지 않은 수의 요청을 수행하는 IP 주소에서 기원되는 요청
- 사업을 운영하지 않거나 공격이 빈번하게 발생하는 국가에서 시작되는 요청
- [User-Agent] 헤더에 가짜 값이 포함된 요청
- 악성 SQL 코드가 포함된 것으로 보이는 요청

웹 ACL 생성

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 ACL을 생성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.

2. 클래식을 처음 사용하는 경우 AWS WAF 클래식으로 이동을 AWS WAF 선택한 다음 웹 ACL 구성을 선택합니다. 이전에 AWS WAF 클래식을 사용한 적이 있다면 탐색 창에서 웹 ACL을 선택한 다음 웹 ACL 생성을 선택합니다.
3. 웹 ACL 명칭에서 명칭을 입력합니다.

   > **Note**
   >
   > 웹 ACL을 생성한 후에는 그 명칭을 변경할 수 없습니다.

4. CloudWatch 메트릭 이름의 경우 해당하는 경우 기본 이름을 변경하십시오. 명칭은 최대 길이 128자 및 최소 길이 1자가 가능하며 영숫자(A-Z, a-z, 0-9)만 포함할 수 있습니다. 여기에는 “All” 및 “Default_Action”을 포함하여 AWS WAF 클래식용으로 예약된 공백 또는 지표 이름을 포함할 수 없습니다.

   > **Note**
   >
   > 웹 ACL을 생성한 후에는 명칭을 변경할 수 없습니다.

5. 지역에서 지역을 선택합니다.
6. AWS 리소스에서 이 웹 ACL과 연계할 리소스를 선택한 후 다음을 선택합니다.

7. AWS WAF Classic에서 웹 요청을 검사하는 데 사용할 조건을 이미 만든 경우 [다음] 을 선택하고 다음 단계를 계속하십시오.

   조건을 아직 생성하지 않은 경우, 지금 생성합니다. 자세한 정보는 다음 주제를 참조하십시오:

   - 교차 사이트 스크립팅 매칭 조건 작업
   - IP 매칭 조건 작업
   - 지리 매칭 조건 작업
   - 크기 제약 조건 작업
   - SQL 명령어 주입 매칭 조건 작업
   - 문자열 매칭 조건 작업
   - 정규식 매칭 조건 작업

8. 이 웹 ACL에 추가하려는 규칙 또는 규칙 그룹을 이미 생성했거나 AWS Marketplace 규칙 그룹에 가입한 경우 웹 ACL에 규칙을 추가하십시오.

   a. [Rules] 목록에서 규칙을 선택합니다.

   b. [Add rule to web ACL]을 선택합니다.

   c. 이 웹 ACL에 추가하려는 규칙을 모두 추가할 때까지 a단계와 b단계를 반복합니다.

   d. 10단계로 이동합니다.

9. 규칙을 아직 생성하지 않은 경우, 지금 규칙을 추가할 수 있습니다.

   a. Create rule을 선택합니다.

   b. 다음 값을 입력합니다.

      명칭

         명칭을 입력합니다.

      CloudWatch 지표 이름

         AWS WAF Classic에서 생성하여 규칙과 연결할 CloudWatch 지표의 이름을 입력합니다. 명칭은 최대 길이 128자 및 최소 길이 1자가 가능하며 영숫자(A-Z, a-z, 0-9)만 포함할 수 있습니다. "All" 및 "Default_Action"을 포함하여 AWS WAF Classic에 예약된 공백 또는 지표 명칭은 포함할 수 없습니다.

> **Note**
>
> 규칙을 생성한 후에는 척도 명칭을 변경할 수 없습니다.

c. 조건을 규칙에 추가하려면 다음 값을 지정합니다.

요청이 다음과 같을 때/같지 않을 때

AWS WAF Classic에서 특정 조건의 필터를 기반으로 요청을 허용하거나 차단하도록 하려면 (예: IP 주소 192.0.2.0/24 범위에서 시작된 웹 요청) 을 허용하거나 차단하도록 하려면 [확인] 을 선택하십시오.

AWS WAF Classic에서 조건에 있는 필터의 역수를 기준으로 요청을 허용 또는 차단하도록 하려면 [안 함] 을 선택합니다. 예를 들어 IP 일치 조건에 192.0.2.0/24의 IP 주소 범위가 포함되고 AWS WAF Classic에서 해당 IP 주소에서 오지 않는 요청을 허용 또는 차단하도록 하려면 [안 함] 을 선택합니다.

일치/시작

규칙에 추가할 조건 타입을 선택합니다.

- 교차 사이트 스크립팅 매칭 조건 - 교차 사이트 스크립팅 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
- IP 매칭 조건 - IP 주소에서 기원을 선택합니다.
- 지리 매칭 조건 - 지리적 위치에서 기원을 선택합니다.
- 크기 제약 조건 - 크기 제약 조건에서 필터 1개 이상과 일치를 선택합니다.
- SQL 명령어 주입 매칭 조건 - SQL 명령어 주입 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
- 문자열 매칭 조건 - 문자열 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.
- 정규식 매칭 조건 - 정규식 매칭 조건에서 필터 1개 이상과 일치를 선택합니다.

조건 명칭

규칙에 추가할 조건을 선택합니다. 이 목록에는 이전 목록에서 선택한 타입의 조건만 표시됩니다.

d. 규칙에 다른 조건을 추가하려면 다른 조건 추가를 선택한 다음 b단계 및 c단계를 반복합니다. 유념할 사항:

- 조건을 두 개 이상 추가하는 경우 AWS WAF Classic에서 해당 규칙에 따라 요청을 허용하거나 차단하려면 웹 요청이 모든 조건에서 하나 이상의 필터와 일치해야 합니다.
- 동일한 규칙에 두 개의 IP 일치 조건을 추가하는 경우 AWS WAF Classic은 두 IP 일치 조건에 모두 나타나는 IP 주소에서 시작된 요청만 허용하거나 차단합니다.

e. 이 웹 ACL에 추가하려는 규칙을 모두 생성할 때까지 9단계를 반복합니다.

f. 생성을 선택하세요.

g. 10단계로 계속합니다.

10. 웹 ACL의 각 규칙 또는 규칙 그룹에 대해 다음과 같이 AWS WAF Classic에서 제공할 관리 유형을 선택합니다.

- 각 규칙에 대해 규칙의 조건에 따라 AWS WAF Classic에서 웹 요청을 허용할지, 차단할지 또는 카운트할지 선택합니다.
  - 허용 — API Gateway CloudFront 또는 애플리케이션 로드 밸런서가 요청된 객체로 응답합니다. 의 CloudFront 경우 객체가 엣지 캐시에 없는 경우 요청을 CloudFront 오리진에 전달합니다.
  - 차단 — API Gateway CloudFront 또는 애플리케이션 로드 밸런서가 HTTP 403 (금지됨) 상태 코드로 요청에 응답합니다. CloudFront 또한 사용자 지정 오류 페이지로 응답할 수 있습니다. 자세한 정보는 AWS WAF Classic을 CloudFront 사용자 지정 오류 페이지와 함께 사용하기을 참조하세요.
  - 개수 — AWS WAF Classic은 규칙의 조건과 일치하는 요청의 카운터를 늘린 다음 웹 ACL의 나머지 규칙을 기반으로 웹 요청을 계속 검사합니다.

    웹 ACL을 사용하여 웹 요청을 허용하거나 차단하기 전에 개수를 사용하여 웹 ACL을 테스트하는 방법에 대한 자세한 설명은 웹 ACL에서 규칙과 일치하는 웹 요청 계산 섹션을 참조하세요.
- 각 규칙 그룹에서 규칙 그룹에 대한 작업 재정의를 설정합니다.
  - 재정의 없음 - 사용할 규칙 그룹 내에서 개별 규칙의 작업을 실행합니다.
  - 계수로 재정의 - 일치하는 모든 요청만 계수되도록 그룹 내 개별 규칙에 의해 지정된 모든 차단된 작업을 재정의합니다.

  자세한 정보는 규칙 그룹 재정의을 참조하세요.

11. 웹 ACL에서 규칙의 순서를 변경하려면 순서 열의 화살표를 사용하십시오. AWS WAF Classic은 웹 ACL에 규칙이 나타나는 순서를 기준으로 웹 요청을 검사합니다.

12. 웹 ACL에 추가한 규칙을 제거하려는 경우, 규칙에 대한 행에서 [x]를 선택합니다.

13. 웹 ACL에 대한 기본 조치를 선택합니다. 이는 웹 요청이 이 웹 ACL에 있는 규칙의 조건 중 하나와 일치하지 않을 때 AWS WAF Classic에서 취하는 조치입니다. 자세한 정보는 웹 ACL에 대한 기본 조치 결정을 참조하세요.
14. 검토 및 생성을 선택합니다.
15. 웹 ACL에 대한 설정을 검토한 후 [Confirm and create]를 선택합니다.

웹 ACL을 Amazon API Gateway API, CloudFront 배포 또는 애플리케이션 로드 밸런서와 연결 해제하기

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 ACL을 연계하거나 연계을 해제하려면 적용 가능한 절차를 수행합니다. 배포를 만들거나 업데이트할 때 웹 ACL을 CloudFront 배포에 연결할 수도 있다는 점에 유의하십시오. 자세한 내용은 Amazon CloudFront 개발자 안내서의 AWS WAF Classic을 사용하여 콘텐츠에 대한 액세스 제어를 참조하십시오.

ACL 웹과 연계할 때 적용되는 제한은 다음과 같습니다.

- 각 API Gateway API, 애플리케이션 로드 밸런서 및 CloudFront 배포는 하나의 웹 ACL에만 연결할 수 있습니다.
- CloudFront 배포와 연결된 웹 ACL은 애플리케이션 로드 밸런서 또는 API Gateway API와 연결할 수 없습니다. 하지만 웹 ACL은 다른 배포와 연결할 수 있습니다. CloudFront

웹 ACL을 API Gateway API, CloudFront 배포 또는 애플리케이션 로드 밸런서와 연결하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Web ACLs]를 선택합니다.

3. API Gateway API, CloudFront 배포 또는 애플리케이션 로드 밸런서와 연결할 웹 ACL의 이름을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.
4. 규칙 탭의 이 웹 ACL을 사용하는AWS 리소스에서 연계 추가를 선택합니다.
5. 메시지가 표시되면 리소스 목록을 사용하여 이 웹 ACL을 연결할 API Gateway API, CloudFront 배포 또는 애플리케이션 로드 밸런서를 선택합니다. Application Load Balancer를 선택할 경우, 지역도 지정해야 합니다.
6. 추가를 선택합니다.
7. 이 웹 ACL을 추가 API Gateway API, CloudFront 배포 또는 다른 애플리케이션 로드 밸런서와 연결하려면 4~6단계를 반복합니다.

API Gateway API, CloudFront 배포 또는 애플리케이션 로드 밸런서에서 웹 ACL을 분리하려면

1. https://console.aws.amazon.com/wafv2/ 에서 AWS Management Console 로그인하고 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. API Gateway API, CloudFront 배포 또는 애플리케이션 로드 밸런서에서 연결을 해제하려는 웹 ACL의 이름을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.
4. 규칙 탭의 이 웹 ACL을 사용하는AWS 리소스에서 이 웹 ACL의 연결을 해제하려는 각 API Gateway API, CloudFront 배포 또는 Application Load Balancer의 x를 선택합니다.

웹 ACL 편집

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 ACL에서 규칙을 추가 또는 제거하거나 동작을 변경하려면 다음 절차를 수행합니다.

웹 ACL을 편집하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. 편집하려는 웹 ACL의 명칭을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.
4. 오른쪽 창의 [Rules] 탭에서 [Edit web ACL]을 선택합니다.
5. 웹 ACL에 규칙을 추가하려면 다음 단계를 수행합니다.

   a. [Rules] 목록에서 추가할 규칙을 선택합니다.

   b. [Add rule to web ACL]을 선택합니다.

   c. 원하는 규칙을 모두 추가할 때까지 a단계와 b단계를 반복합니다.
6. 웹 ACL에서 규칙의 순서를 변경하려면 순서 열의 화살표를 사용하십시오. AWS WAF Classic은 웹 ACL에 규칙이 나타나는 순서를 기준으로 웹 요청을 검사합니다.
7. 웹 ACL에서 규칙을 제거하려면 해당 규칙에 대한 행의 오른쪽에 있는 [x]를 선택합니다. 이렇게 하면 AWS WAF Classic에서 규칙이 삭제되는 것이 아니라 이 웹 ACL에서 규칙이 제거될 뿐입니다.
8. 규칙에 대한 작업 또는 웹 ACL에 대한 기본 조치를 변경하려면 선호하는 옵션을 선택합니다.

   > **Note**
   >
   > 규칙 그룹 또는 AWS Marketplace 규칙 그룹 (단일 규칙이 아님) 에 대한 작업을 설정하는 경우 규칙 그룹에 대해 설정하는 작업 (재정의 없음 또는 개수에 맞게 재정의) 을 재정의 작업이라고 합니다. 자세한 내용은 규칙 그룹 재정의 섹션을 참조하세요.
9. 변경 사항 저장를 선택합니다.

웹 ACL 삭제

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경

우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 ACL을 삭제하려면 웹 ACL에 포함된 규칙을 제거하고 웹 ACL에서 모든 CloudFront 배포와 애플리케이션 로드 밸런서의 연결을 끊어야 합니다. 다음 절차를 수행하십시오.

웹 ACL을 삭제하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 콘솔을 엽니다. AWS WAF

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 [Web ACLs]를 선택합니다.
3. 삭제하려는 웹 ACL의 명칭을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.
4. 오른쪽 창의 [Rules] 탭에서 [Edit web ACL]을 선택합니다.
5. 웹 ACL에서 모든 규칙을 제거하려면 각 규칙에 대한 행의 오른쪽에 있는 [x]를 선택합니다. 이렇게 해도 AWS WAF Classic에서 규칙이 삭제되는 것이 아니라 이 웹 ACL에서 규칙이 제거될 뿐입니다.
6. 업데이트를 선택합니다.
7. 모든 CloudFront 배포와 애플리케이션 로드 밸런서에서 웹 ACL을 분리하십시오. 규칙 탭의 이 웹 ACL을 사용하는AWS 리소스에서 각 API Gateway API, CloudFront 배포 또는 Application Load Balancer의 x를 선택합니다.
8. 웹 ACL 페이지에서 삭제할 웹 ACL이 선택되어 있는지 확인한 다음 삭제를 선택합니다.

웹 ACL 테스트

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.

의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

허용하거나 차단하려는 요청을 차단하도록 AWS WAF Classic을 실수로 구성하지 않도록 하려면 웹 사이트 또는 웹 애플리케이션에서 사용하기 전에 웹 ACL을 철저하게 테스트하는 것이 좋습니다.

주제

- 웹 ACL에서 규칙과 일치하는 웹 요청 계산
- API Gateway CloudFront 또는 애플리케이션 로드 밸런서가 클래식에 전달한 웹 요청 샘플 보기 AWS WAF

웹 ACL에서 규칙과 일치하는 웹 요청 계산

웹 ACL에 규칙을 추가할 때 AWS WAF Classic에서 해당 규칙의 모든 조건에 맞는 웹 요청을 허용할지, 차단할지 또는 계산할지 여부를 지정합니다. 다음 구성으로 시작하는 것이 좋습니다.

- 웹 요청을 계산하도록 웹 ACL의 모든 규칙 구성
- 요청을 허용하도록 웹 ACL에 대한 기본 작업 설정

이 구성에서 AWS WAF Classic은 첫 번째 규칙의 조건을 기반으로 각 웹 요청을 검사합니다. 웹 요청이 해당 규칙의 모든 조건과 일치하는 경우 AWS WAF Classic은 해당 규칙에 대한 카운터를 증가시킵니다. 그러면 AWS WAF Classic은 다음 규칙의 조건에 따라 웹 요청을 검사합니다. 요청이 해당 규칙의 모든 조건과 일치하는 경우 AWS WAF Classic은 규칙에 대한 카운터를 증가시킵니다. 이는 AWS WAF Classic이 모든 규칙의 조건을 기반으로 요청을 검사할 때까지 계속됩니다.

요청을 계산하도록 웹 ACL의 모든 규칙을 구성하고 웹 ACL을 Amazon API Gateway API, CloudFront 배포 또는 애플리케이션 로드 밸런서와 연결하면 Amazon 그래프에서 결과 수를 볼 수 있습니다. CloudWatch 웹 ACL의 각 규칙 및 API Gateway CloudFront 또는 Application Load Balancer가 웹 CloudWatch ACL을 AWS WAF 위해 클래식으로 전달하는 모든 요청에 대해 다음을 수행할 수 있습니다.

- 이전 한 시간 또는 이전 세 시간 동안의 데이터 보기
- 데이터 요소 간의 간격 변경
- 데이터에 대해 CloudWatch 수행하는 계산 (예: 최대값, 최소값, 평균 또는 합계) 을 변경하십시오.

> **Note**
>
> AWS WAF CloudFront Classic은 글로벌 서비스이며 지표는 에서 미국 동부 (버지니아 북부) 지역을 선택한 경우에만 사용할 수 있습니다. AWS Management Console다른 지역을 선택하면 CloudWatch 콘솔에 AWS WAF Classic 지표가 표시되지 않습니다.

웹 ACL에서 규칙에 대한 데이터를 보려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창의 [Metrics]에서 [WAF]를 선택합니다.
3. 데이터를 보려는 웹 ACL의 확인란을 선택합니다.
4. 해당되는 설정을 변경합니다.

   통계

   데이터에 대해 CloudWatch 수행할 계산을 선택합니다.

   시간 범위

   이전 한 시간 동안의 데이터를 볼지 또는 이전 세 시간 동안의 데이터를 볼지를 선택합니다.

   기간

   그래프에서 데이터 요소 간의 간격을 선택합니다.

   규칙

   데이터를 보려는 규칙을 선택합니다.

   유념할 사항:

   - 웹 ACL을 API Gateway API, CloudFront 배포 또는 Application Load Balancer와 방금 연결한 경우 그래프에 데이터가 나타나고 웹 ACL에 대한 지표가 사용 가능한 지표 목록에 나타날 때까지 몇 분 정도 기다려야 할 수 있습니다.
   - 두 개 이상의 API Gateway API, CloudFront 배포 또는 Application Load Balancer를 웹 ACL과 연결하는 경우 CloudWatch 데이터에는 웹 ACL과 연결된 모든 배포에 대한 모든 요청이 포함됩니다.
   - 데이터 요소 위에 마우스 커서를 놓으면 추가 정보를 볼 수 있습니다.

- 그래프는 자동으로 새로 고침되지 않습니다. 표시 내용을 업데이트하려면 새로 고침 () 아이콘을 선택합니다.

5. (선택 사항) API Gateway CloudFront 또는 Application Load Balancer가 클래식에 전달한 개별 요청에 대한 세부 정보를 확인합니다. AWS WAF 자세한 정보는 API Gateway CloudFront 또는 애플리케이션 로드 밸런서가 클래식에 전달한 웹 요청 샘플 보기 AWS WAF을 참조하세요.
6. 가로채지 않아야 할 요청을 규칙이 가로채는 것으로 확인되면 해당 설정을 변경합니다. 자세한 정보는 웹 ACL(웹 액세스 제어 목록) 생성 및 구성을 참조하세요.

   모든 규칙이 올바른 요청만 가로채는 것으로 확인되는 경우 각 규칙에 대한 작업을 [Allow] 또는 [Block]으로 변경합니다. 자세한 정보는 웹 ACL 편집을 참조하세요.

API Gateway CloudFront 또는 애플리케이션 로드 밸런서가 클래식에 전달한 웹 요청 샘플 보기 AWS WAF

AWS WAF 클래식 콘솔에서는 API Gateway CloudFront 또는 Application Load Balancer가 검사를 위해 AWS WAF 클래식에 전달한 요청 샘플을 볼 수 있습니다. 샘플링된 각 요청에 대해 요청에 대한 세부 데이터를 볼 수 있습니다(예: 요청이 시작되는 IP 주소 및 요청에 포함된 헤더). 요청이 어떤 규칙과 일치하는지, 규칙이 요청을 허용하도록 구성되어 있는지 또는 차단하도록 구성되어 있는지도 볼 수 있습니다.

요청 샘플에는 각 규칙의 모든 조건과 일치하는 최대 100개의 요청과 특정 규칙의 모든 조건과 일치하는 않는 규칙에 적용되는 기본 작업에 대한 다른 100개의 요청이 포함되어 있습니다. 샘플의 요청은 지난 15분 동안 콘텐츠에 대한 요청을 받은 모든 API Gateway API, CloudFront 엣지 로케이션 또는 애플리케이션 로드 밸런서에서 제공됩니다.

API Gateway CloudFront 또는 애플리케이션 로드 밸런서가 클래식에 전달한 웹 요청의 샘플을 보려면 AWS WAF

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 요청을 보려는 웹 ACL을 선택합니다.
3. 오른쪽 창에서 [Requests] 탭을 선택합니다.

   [Sampled requests] 테이블에는 각 요청에 대해 다음과 같은 값이 표시됩니다.

소스 IP

요청이 시작된 IP 주소 또는 최종 사용자가 HTTP 프록시나 Application Load Balancer를 사용하여 요청을 전송한 경우 프록시 또는 Application Load Balancer의 IP 주소입니다.

URI

리소스를 식별하는 요청의 URI 경로(예: `/images/daily-ad.jpg`). 여기에는 URI의 쿼리 문자열 또는 조각 구성 요소는 포함되지 않습니다. 자세한 설명은 Uniform Resource Identifier (URI): Generic Syntax 섹션을 참조하세요.

일치 규칙

웹 요청이 모든 조건과 일치하는 웹 ACL의 첫 번째 규칙을 식별합니다. 웹 요청이 웹 ACL의 한 규칙이 있는 모든 조건과 일치하지 않는 경우 [Matches rule]의 값은 [Default]입니다.

참고로 웹 요청이 규칙의 모든 조건과 일치하고 해당 규칙의 동작이 카운트인 경우 AWS WAF Classic은 웹 ACL의 후속 규칙을 기반으로 웹 요청을 계속 검사합니다. 이 경우 샘플링된 요청 목록에 웹 요청이 두 번 나타날 수 있습니다. [Count] 작업이 있는 규칙에 대해 한 번 나타나고 후속 규칙 또는 기본 작업에 대해 다시 한 번 나타납니다.

작업

해당 규칙에 대한 작업이 [Allow]인지, [Block]인지 또는 [Count]인지를 나타냅니다.

Time

AWS WAF Classic이 API Gateway CloudFront 또는 애플리케이션 로드 밸런서로부터 요청을 받은 시간

4. 요청에 대한 추가 정보를 표시하려면 해당 요청의 IP 주소 왼쪽에 있는 화살표를 선택하십시오. AWS WAF Classic은 다음 정보를 표시합니다.

소스 IP

테이블의 [Source IP] 열에 있는 값과 동일한 IP 주소입니다.

국가

요청이 시작되는 국가의 2자 국가 코드입니다. 최종 사용자가 HTTP 프록시 또는 Application Load Balancer를 사용하여 요청을 전송한 경우 이 값은 HTTP 프록시 또는 Application Load Balancer가 있는 국가의 2자 국가 코드입니다.

2자 국가 코드 및 해당 국가 이름의 목록은 Wikipedia 항목 ISO 3166-1 alpha-2를 참조하세요.

메서드

요청에 대한 HTTP 요청 메서드입니다. GET, HEAD, OPTIONS, PUT, POST, PATCH 또는 DELETE를 선택할 수 있습니다.

URI

테이블의 [URI] 열에 있는 값과 동일한 URI입니다.

요청 헤더

요청 헤더 및 요청의 헤더 값입니다.

5. 샘플 요청의 목록을 새고 고치려면 [Get new samples]를 선택합니다.

에서 사용할 AWS WAF 클래식 규칙 그룹 사용 AWS Firewall Manager

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF 클래식 규칙 그룹은 AWS WAF 클래식 AWS Firewall Manager 정책에 추가하는 규칙 세트입니다. 고유한 규칙 그룹을 만들거나 에서 관리형 규칙 그룹을 구입할 수 AWS Marketplace있습니다.

> **Important**
>
> Firewall Manager 정책에 AWS Marketplace 규칙 그룹을 추가하려면 먼저 조직의 각 계정이 해당 규칙 그룹에 가입해야 합니다. 모든 계정이 가입한 후 규칙 그룹을 정책에 추가할 수 있습니다. 자세한 내용은 AWS Marketplace 규칙 그룹을(를) 참조하세요.

주제

- AWS WAF 클래식 규칙 그룹 생성

- AWS WAF 클래식 규칙 그룹에서 규칙 추가 및 삭제

AWS WAF 클래식 규칙 그룹 생성

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

함께 AWS Firewall Manager사용할 AWS WAF 클래식 규칙 그룹을 생성할 때는 그룹에 추가할 규칙을 지정합니다.

규칙 그룹을 생성하려면 (콘솔)

1. 사전 요구 사항에서 설정한 AWS Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다. https://console.aws.amazon.com/wafv2/fms

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 2단계: AWS Firewall Manager 기본 관리자 계정 생성을 참조하세요.

2. 탐색 창에서 클래식으로 전환을 AWS WAF 선택합니다.
3. AWS WAF 클래식 탐색 창에서 규칙 그룹을 선택합니다.
4. 규칙 그룹 생성을 선택합니다.

   > **Note**
   >
   > 규칙 그룹에 비율 기반 규칙을 추가할 수 없습니다.

5. 규칙 그룹에 추가할 규칙을 이미 생성한 경우, 이 규칙 그룹에 기존 규칙 사용을 선택합니다. 규칙 그룹에 추가할 새 규칙을 생성하려면 Create rules and conditions for this rule group(이 규칙 그룹의 규칙 및 조건 생성)을 선택합니다.

6. 다음을 선택합니다.
7. 규칙을 생성하기로 선택한 경우, 규칙 생성 및 조건 추가에서 다음 단계에 따라 규칙을 만듭니다.

> **Note**
>
> AWS WAF 클래식 콘솔을 사용하여 규칙을 만들 수 있습니다.

   필요한 모든 규칙을 생성했으면 다음 단계로 이동합니다.
8. 규칙 그룹 명칭을 입력합니다.
9. 규칙을 규칙 그룹에 추가하려면 규칙을 선택한 후 Add rule(규칙 추가)을 선택합니다. 규칙의 조건과 일치하는 요청을 허용, 차단 또는 계수할지 여부를 선택합니다. 선택 사항에 대한 자세한 설명은 AWS WAF 클래식 작동 방식 섹션을 참조하세요.
10. 규칙 추가가 끝나면 생성을 클릭합니다.

규칙 그룹을 WebACL에 추가하고 AWS WAF WebACL 작업을 개수로 재정의로 설정하여 규칙 그룹을 테스트할 수 있습니다. 이 작업은 그룹에 포함된 규칙에 대해 선택한 모든 작업을 재정의하고 일치하는 요청만 계수합니다. 자세한 내용은 웹 ACL 생성을(를) 참조하세요.

AWS WAF 클래식 규칙 그룹에서 규칙 추가 및 삭제

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF 클래식 규칙 그룹에서 규칙을 추가하거나 삭제할 수 있습니다.

규칙 그룹에서 규칙을 삭제해도 규칙 자체가 삭제되지는 않습니다. 규칙 그룹에서만 규칙이 제거됩니다.

규칙 그룹에서 규칙을 추가하거나 삭제하려면(콘솔)

1. 사전 요구 사항에서 설정한 AWS Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다. https://console.aws.amazon.com/wafv2/fms

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 2단계: AWS Firewall Manager 기본 관리자 계정 생성을 참조하세요.

2. 탐색 창에서 클래식으로 전환을 AWS WAF 선택합니다.
3. AWS WAF 클래식 탐색 창에서 규칙 그룹을 선택합니다.
4. 편집할 규칙 그룹을 선택합니다.
5. Edit rule group(규칙 그룹 편집)을 선택합니다.
6. 규칙을 추가하려면 다음 단계를 수행합니다.

   a. 규칙을 선택한 후 규칙을 규칙 그룹에 추가를 선택합니다. 규칙의 조건과 일치하는 요청을 허용, 차단 또는 계수할지 여부를 선택합니다. 선택 사항에 대한 자세한 설명은 AWS WAF 클래식 작동 방식 섹션을 참조하세요. 규칙 그룹에 규칙을 더 추가하려면 이 과정을 반복합니다.

   > **Note**
   >
   > 규칙 그룹에 비율 기반 규칙을 추가할 수 없습니다.

   b. 업데이트를 선택합니다.
7. 규칙을 삭제하려면 다음 단계를 수행합니다.

   a. 삭제할 규칙 옆의 X를 선택합니다. 규칙 그룹에서 규칙을 더 삭제하려면 이 과정을 반복합니다.

   b. 업데이트를 선택합니다.

AWS WAF 클래식 규칙 활성화 AWS Firewall Manager 시작하기

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

를 AWS Firewall Manager 사용하여 AWS WAF 규칙, AWS WAF 클래식 규칙, AWS Shield Advanced 보호 및 Amazon VPC 보안 그룹을 활성화할 수 있습니다. 설정하기 위한 단계는 각각의 경우에 약간 다릅니다.

- Firewall Manager를 사용하여 최신 버전의 AWS WAF규칙을 활성화하려면 이 항목을 사용하지 마십시오. 그 대신 AWS Firewall ManagerAWS WAF 정책 시작하기 섹션의 단계를 따릅니다.
- Firewall Manager를 사용하여 AWS Shield Advanced 보호 기능을 활성화하려면 의 AWS Firewall ManagerAWS Shield Advanced 정책 시작하기 단계를 따르십시오.
- Firewall Manager를 사용하여 Amazon VPC 보안 그룹을 활성화하려면 AWS Firewall Manager Amazon VPC 보안 그룹 정책 시작하기의 단계를 따릅니다.

Firewall Manager를 사용하여 AWS WAF 클래식 규칙을 활성화하려면 다음 단계를 순서대로 수행하십시오.

주제

1단계: 필수 구성 요소 완성

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 2단계: 규칙 생성으로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: 규칙 생성

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

이 단계에서는 AWS WAF Classic을 사용하여 규칙을 생성합니다. 함께 AWS Firewall Manager사용하려는 AWS WAF 클래식 규칙이 이미 있는 경우 이 단계를 건너뛰고 으로 이동하십시오3단계: 규칙 그룹 생성.

> **Note**
>
> AWS WAF 클래식 콘솔을 사용하여 규칙을 생성하십시오.

AWS WAF 클래식 규칙을 만들려면 (콘솔)

- 규칙을 생성한 후 규칙에 조건을 추가합니다. 자세한 설명은 규칙 생성 및 조건 추가 섹션을 참조하세요.

이제 3단계: 규칙 그룹 생성으로 이동할 준비가 되었습니다.

3단계: 규칙 그룹 생성

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

규칙 그룹은 특정한 조건 세트가 충족되면 수행할 작업을 정의하는 규칙 세트입니다. 에서 관리형 규칙 그룹을 사용할 수 AWS Marketplace있으며 자체 규칙 그룹을 만들 수 있습니다. 관리형 규칙 그룹에 대한 자세한 설명은 AWS Marketplace 규칙 그룹 섹션을 참조하세요.

자체 규칙 그룹을 만들려면 다음 절차를 수행합니다.

규칙 그룹을 생성하려면 (콘솔)

1. 사전 요구 사항에서 설정한 AWS Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다. https://console.aws.amazon.com/wafv2/fms
2. 탐색 창에서 보안 정책을 선택합니다.
3. 사전 조건을 충족하지 않으면 문제 해결 방법에 대한 지침이 콘솔에 표시됩니다. 지침에 따른 후 이 단계(규칙 그룹 생성)를 다시 시작합니다. 사전 조건을 충족한 경우, 닫기를 선택합니다.
4. 정책 생성(Create policy)을 선택합니다.

   정책 타입에서 AWS WAF Classic을 선택합니다.
5. [AWS Firewall Manager 정책 만들기] 를 선택하고 새 규칙 그룹을 추가합니다.
6. 를 선택한 후 다음을 선택합니다. AWS 리전

7. 이미 규칙을 만들었으므로 조건을 만들 필요가 없습니다. 다음을 선택합니다.
8. 이미 규칙을 만들었으므로 규칙을 만들 필요가 없습니다. 다음을 선택합니다.
9. 규칙 그룹 생성을 선택합니다.
10. 명칭에 기억하기 쉬운 명칭을 입력합니다.
11. AWS WAF Classic에서 생성하여 규칙 그룹과 연결할 CloudWatch 지표의 이름을 입력합니다. 명칭은 영숫자(A-Z, a-z, 0-9) 또는 특수 문자(_-!"#`+*},./)만 포함할 수 있습니다. 공백은 포함될 수 없습니다.
12. 규칙을 선택한 후 규칙 추가를 선택합니다. 규칙에는 규칙의 조건과 일치하는 요청을 허용, 차단 또는 계수할지 여부를 선택할 수 있는 작업 설정이 있습니다. 본 자습서에서는 계수를 선택합니다. 원하는 규칙을 모두 규칙 그룹에 추가할 때까지 규칙 추가를 반복합니다.
13. 생성을 선택하세요.

이제 4단계: AWS Firewall ManagerAWS WAF 클래식 정책 생성 및 적용으로 이동할 준비가 되었습니다.

4단계: AWS Firewall ManagerAWS WAF 클래식 정책 생성 및 적용

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

규칙 그룹을 생성한 후 AWS Firewall Manager AWS WAF 정책을 생성합니다. Firewall Manager AWS WAF 정책에는 리소스에 적용할 규칙 그룹이 포함되어 있습니다.

방화벽 관리자 AWS WAF 정책을 만들려면 (콘솔)

1. 규칙 그룹을 생성한 후(이전 절차의 마지막 단계 3단계: 규칙 그룹 생성) 콘솔에 규칙 그룹 요약 페이지가 표시됩니다. 다음을 선택합니다.
2. 명칭에 기억하기 쉬운 명칭을 입력합니다.
3. 정책 타입에서 WAF를 선택합니다.

4. 지역의 경우 를 선택합니다 AWS 리전. Amazon CloudFront 리소스를 보호하려면 글로벌을 선택하십시오.

   여러 지역의 리소스 (CloudFront 리소스 제외) 를 보호하려면 각 지역에 대해 별도의 Firewall Manager 정책을 만들어야 합니다.
5. 추가할 규칙 그룹을 선택한 후 Add rule group(규칙 그룹 추가)을 선택합니다.
6. 정책에는 Action set by rule group(규칙 그룹에 설정된 작업) 및 Count(계산)라는 두 가지 가능한 작업이 있습니다. 정책과 규칙 그룹을 테스트하려면 작업을 Count(계산)로 설정합니다. 이 작업은 정책에 포함된 규칙 그룹으로 지정한 모든 차단 작업을 재정의합니다. 즉, 정책의 작업이 Count(계산)로 설정되면 요청이 계산되기만 하고 차단되지는 않습니다. 반대로 정책의 작업을 Action set by rule group(규칙 그룹에 설정된 작업)으로 설정하면 정책에 포함된 규칙 그룹의 작업이 사용됩니다. 본 자습서에서는 계산를 선택합니다.
7. 다음을 선택합니다.
8. 정책에 특정 계정만 포함시키려 하거나 정책에서 특정 계정을 제외하려면, Select accounts to include/exclude from this policy (optional)(이 정책에서 포함/제외하려는 계정 선택(선택 사항))를 선택합니다. Include only these accounts in this policy(이 정책에 이러한 계정만 포함) 또는 Exclude these accounts from this policy(이 정책에서 이러한 계정 제외)를 선택합니다. 옵션을 하나만 선택할 수 있습니다. 추가를 선택합니다. 포함하거나 제외할 계정 번호를 선택한 다음 확인을 선택합니다.

   > **Note**
   >
   > 이 옵션을 선택하지 않으면 Firewall Manager는 AWS Organizations에서 해당 조직의 모든 계정에 정책을 적용합니다. 조직에 새 계정을 추가하면 Firewall Manager에서 자동으로 해당 계정에 정책을 적용합니다.
9. 보호할 리소스 타입을 선택합니다.
10. 특정 태그가 있는 리소스만 보호하거나 특정 태그가 있는 리소스를 제외하려면 Use tags to include/exclude resources(태그를 사용하여 리소스 포함/제외)를 선택하고 태그를 입력한 다음 Include(포함) 또는 Exclude(제외)를 선택합니다. 옵션을 하나만 선택할 수 있습니다.

    태그를 2개 이상 입력하고(쉼표로 구분) 리소스에 해당 태그 중 하나라도 있으면 일치한다고 간주합니다.

    태그에 대한 자세한 설명은 Tag Editor 작업을 참조하세요.
11. Create and apply this policy to existing and new resources(이 정책을 생성하고 기존 리소스와 새 리소스에 적용)를 선택합니다.

이 옵션은 조직 내 각 해당 계정에 웹 ACL을 만들고 웹 ACL을 계정의 지정된 리소스와 연결합니다. AWS Organizations앞에서 설명한 기준(리소스 타입 및 태그)에 맞는 모든 새 리소스에 정책을 적용합니다. 또는 이 정책을 생성하지만 기존 리소스나 새로운 리소스에 적용 안 함를 선택할 경우, Firewall Manager는 조직 내의 각 해당하는 계정에 웹 ACL을 생성하지만 리소스에 웹 ACL을 적용하지는 않습니다. 나중에 정책을 리소스에 적용해야 합니다.

12. Replace existing associated web ACLs(기존 웹 ACL 연계 바꾸기)를 기본 설정 그대로 둡니다.

    이 옵션을 선택하면 Firewall Manager가 범위 내 리소스에서 기존 웹 ACL 연계을 모두 제거한 후 새 정책의 웹 ACL을 연계합니다.

13. 다음을 선택합니다.
14. 새 정책을 검토합니다. 변경하려면 Edit(편집)를 선택합니다. 정책이 마음에 들면 정책 생성를 선택합니다.

자습서: 계층적 규칙을 사용한 AWS Firewall Manager정책 생성

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

를 사용하여 계층적 규칙이 포함된 AWS WAF 클래식 보호 정책을 만들고 적용할 수 있습니다. AWS Firewall Manager즉, 특정 규칙을 중앙에서 생성하고 적용할 수 있지만, 계정별 규칙의 생성과 유지 관리를 다른 개인에게 위임할 수 있습니다. 중앙에서 적용된(범용) 규칙을 모니터링하여 우발적인 제거 또는 처리 오류를 확인할 수 있으며, 이러한 방법으로 해당 규칙이 올바르게 적용되도록 보장할 수 있습니다. 계정별 규칙은 개별 팀의 필요에 맞게 사용자 지정된 추가 보호를 추가합니다.

> **Note**
>
> 최신 AWS WAF버전에서는 이 기능이 기본 제공되므로 특별한 처리가 필요하지 않습니다. 아직 AWS WAF Classic을 사용하고 있지 않다면 최신 버전을 대신 사용하세요. 에 대한 AWS Firewall Manager 정책 생성 AWS WAF 섹션을 참조하세요.

다음 자습서에서는 계층적 보호 규칙 세트를 생성하는 방법을 설명합니다.

주제

1단계: Firewall Manager 관리자 계정 지정

사용하려면 AWS Firewall Manager조직의 계정을 Firewall Manager 관리자 계정으로 지정해야 합니다. 이 계정은 조직의 관리 계정 또는 멤버 계정일 수 있습니다.

Firewall Manager 관리자 계정을 사용하여 조직의 다른 계정에 적용하는 범용 규칙 세트를 생성할 수 있습니다. 조직의 다른 계정은 중앙에서 적용된 이러한 규칙을 변경할 수 없습니다.

계정을 Firewall Manager 관리자 계정으로 지정하고 Firewall Manager에 대한 다른 사전 조건을 완료하려면 AWS Firewall Manager 전제 조건의 지침을 참조하세요. 사전 조건을 이미 완료한 경우 이 자습서의 2단계로 건너뛸 수 있습니다.

이 자습서에서는 관리자 계정을 **`Firewall-Administrator-Account`**이라고 합니다.

2단계: Firewall Manager 관리자 계정을 사용하여 규칙 그룹 생성

다음에는 **`Firewall-Administrator-Account`**를 사용하여 규칙 그룹을 생성합니다. 이 규칙 그룹에는 다음 단계에서 생성하는 정책을 따르는 모든 멤버 계정에 적용할 범용 규칙이 포함됩니다. **`Firewall-Administrator-Account`**만 이러한 규칙과 컨테이너 규칙 그룹을 변경할 수 있습니다.

이 자습서에서는 이 컨테이너 규칙 그룹을 **`Common-Rule-Group`**이라고 합니다.

규칙 그룹을 생성하려면 AWS WAF 클래식 규칙 그룹 생성의 지침을 참조하세요. 이 지침을 따를 때는 Firewall Manager 관리자 계정(**`Firewall-Administrator-Account`**)을 사용하여 콘솔에 로그인해야 합니다.

3단계: Firewall Manager 정책 생성 및 공통 규칙 그룹 연결

`Firewall-Administrator-Account`을 사용해 Firewall Manager 정책 생성. 이 정책을 생성하는 경우 다음을 수행해야 합니다.

- **Common-Rule-Group**을 새 정책에 추가합니다.
- **Common-Rule-Group**을 적용할 조직의 모든 계정을 포함시킵니다.
- **Common-Rule-Group**을 적용할 모든 리소스를 추가합니다.

정책 생성 지침은 AWS Firewall Manager 정책 생성을 참조하세요.

이렇게 하면 지정된 각 계정에 웹 ACL가 생성되고 **Common-Rule-Group**이 각 해당 웹 ACL에 추가됩니다. 정책을 생성한 후에는 이 웹 ACL과 범용 규칙이 모든 지정된 계정에 배포됩니다.

이 자습서에서는 이 웹 ACL을 **Administrator-Created-ACL**이라고 합니다. 이제 조직의 각 지정된 멤버 계정에 고유의 **Administrator-Created-ACL**이 존재합니다.

4단계: 계정별 규칙 추가

이제 조직의 각 멤버 계정은 계정에 존재하는 **Administrator-Created-ACL**에 고유의 계정별 규칙을 추가할 수 있습니다. 기존 공통 규칙이 새로운 계정별 규칙과 함께 **Administrator-Created-ACL** 계속 적용됩니다. AWS WAF 웹 ACL에 규칙이 나타나는 순서를 기준으로 웹 요청을 검사합니다. 이 동작은 **Administrator-Created-ACL** 및 계정별 규칙에 모두 적용됩니다.

Administrator-Created-ACL에 규칙을 추가하는 방법은 웹 ACL 편집을 참고하십시오.

결론

이제 Firewall Manager 관리자 계정이 관리하는 범용 규칙과 각 멤버 계정이 관리하는 계정별 규칙이 포함된 웹 ACL이 있습니다.

각 계정의 **Administrator-Created-ACL**은 단일 **Common-Rule-Group**을 참조합니다. 따라서 향후 Firewall Manager 관리자 계정이 **Common-Rule-Group**을 변경하면 해당 변경 사항은 즉시 각 멤버 계정에서 효과를 나타냅니다.

멤버 계정은 **Common-Rule-Group**에서 범용 규칙을 변경하거나 제거할 수 없습니다.

계정별 규칙은 다른 계정에 영향을 미치지 않습니다.

웹 ACL 트래픽 정보 로깅

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경

우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

> **Note**
>
> Amazon Security Lake를 사용하여 AWS WAF 클래식 데이터를 수집할 수는 없습니다.

로깅을 활성화하여 웹 ACL에서 분석한 트래픽에 대한 자세한 정보를 기록할 수 있습니다. 로그에 포함된 정보에는 AWS WAF Classic이 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 세부 정보, 각 요청이 일치하는 규칙에 대한 조치 등이 포함됩니다.

시작하려면 Amazon Kinesis Data Firehose를 설정합니다. 이 과정에서 로그를 저장할 대상 위치를 선택합니다. 그런 다음 로깅을 활성화하려는 웹 ACL을 선택합니다. 로깅을 활성화하면 파이어호스를 통해 로그를 저장 대상으로 AWS WAF 전달합니다.

Amazon Kinesis Data Firehose를 생성하고 저장된 로그를 검토하는 방법에 대한 자세한 내용은 Amazon Data Firehose란 무엇입니까? 를 참조하십시오. Kinesis Data Firehose 구성에 필요한 권한을 이해하려면 Amazon Kinesis Data Firehose를 사용한 액세스 제어를 참조하세요.

로깅을 활성화하려면 다음 권한이 있어야 합니다.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

서비스 연결 역할 및 `iam:CreateServiceLinkedRole` 권한에 대한 자세한 내용은 Classic용 서비스 연결 역할 사용 AWS WAF 섹션을 참조하세요.

웹 ACL에 대해 로깅을 활성화하려면

1. aws-waf-logs접두사 "- “로 시작하는 이름을 사용하여 Amazon Kinesis Data Firehose를 생성합니다 (예:). `aws-waf-logs-us-east-2-analytics` 작업하려는 리전에서 PUT 소스를 사용하여 Data Firehose를 생성합니다. CloudFrontAmazon의 로그를 캡처하는 경우 미국 동부 (버지니아 북부) 에서 파이어호스를 생성하십시오. 자세한 내용은 Creating an Amazon Data Firehose Delivery Stream 섹션을 참조하세요.

> **Important**
>
> `Kinesis stream`을 소스로 선택하지 마십시오.
> AWS WAF 클래식 로그 1개는 Firehose 레코드 1개와 동일합니다. 일반적으로 초당 10,000개의 요청을 수신하고 전체 로그를 활성화하는 경우 Firehose에서 초당 10,000개의 레코드를 설정해야 합니다. Firehose를 올바르게 구성하지 않으면 AWS WAF Classic에서 모든 로그를 기록하지 않습니다. 자세한 내용은 Amazon Kinesis Data Firehose 할당량을 참조하세요.

2. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
3. 탐색 창에서 [Web ACLs]를 선택합니다.
4. 로깅을 활성화하려는 웹 ACL의 이름을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.
5. 로깅 탭에서 로깅 활성화를 선택합니다.
6. 첫 단계에서 생성한 Kinesis Data Firehose를 선택합니다. “aws-waf-logs-”로 시작하는 소방호스를 선택해야 합니다.
7. (선택 사항) 로그에 포함된 특정 필드와 그 값이 필요하지 않은 경우 해당 필드를 삭제합니다. 삭제할 필드를 선택한 후 추가를 선택합니다. 필요에 따라 이 작업을 반복하여 추가 필드를 삭제합니다. 삭제된 필드는 로그에서 `REDACTED`(으)로 표시됩니다. 예를 들어 cookie 필드를 삭제한 경우 로그에서 cookie 필드가 `REDACTED`(으)로 나타납니다.
8. 로깅 활성화를 선택합니다.

> **Note**
>
> 로깅을 성공적으로 활성화하면 AWS WAF 클래식은 Amazon Kinesis Data Firehose에 로그를 쓰는 데 필요한 권한을 가진 서비스 연결 역할을 생성합니다. 자세한 정보는 Classic용 서비스 연결 역할 사용 AWS WAF을 참조하세요.

웹 ACL에 대한 로깅을 비활성화하려면

1. 탐색 창에서 [Web ACLs]를 선택합니다.

2. 로깅을 비활성화하려는 웹 ACL의 이름을 선택합니다. 이렇게 하면 오른쪽 창에 웹 ACL의 세부 정보가 있는 페이지가 열립니다.
3. 로깅 탭에서 로깅 비활성화를 선택합니다.
4. 대화 상자에서 로깅 비활성화를 선택합니다.

Example 로그 예


```
{

 "timestamp":1533689070589,
 "formatVersion":1,
 "webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
 "terminatingRuleId":"Default_Action",
 "terminatingRuleType":"REGULAR",
 "action":"ALLOW",
 "httpSourceName":"CF",
 "httpSourceId":"i-123",
 "ruleGroupList":[
                         {
                          "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                          "terminatingRule":null,
                          "nonTerminatingMatchingRules":[
                                                          {"action" : "COUNT",
                                                          "ruleId" :
 "4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                         ],
                          "excludedRules":               [
                                                          {"exclusionType" :
 "EXCLUDED_AS_COUNT",
                                                           "ruleId" :
 "5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                         ]
                         }
                        ],

 "rateBasedRuleList":[
                             {
                              "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                              "limitKey":"IP",
```

```
                                "maxRateAllowed":100

                               },
                               {
                                "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                                "limitKey":"IP",
                                "maxRateAllowed":100
                                }
                                ],

 "nonTerminatingMatchingRules":[
                                        {"action" : "COUNT",

                                        "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                       ],

 "httpRequest":{
                        "clientIp":"192.10.23.23",

                        "country":"US",

                        "headers":[

                                   {
                                    "name":"Host",
                                    "value":"127.0.0.1:1989"
                                   },
                                   {
                                    "name":"User-Agent",
                                    "value":"curl/7.51.2"
                                   },
                                   {
                                    "name":"Accept",
                                    "value":"*/*"
                                   }
                                 ],
                      "uri":"REDACTED",
                      "args":"usernam=abc",
                      "httpVersion":"HTTP/1.1",
                      "httpMethod":"GET",
                      "requestId":"cloud front Request id"
                      }
```

```
}
```

다음은 이러한 로그에 나열되는 각 항목에 대한 설명입니다.

타임스탬프

밀리초 단위의 타임스탬프.

formatVersion

로그의 포맷 버전.

webaclId

웹 ACL의 GUID.

terminatingRuleId

요청을 종료한 규칙의 ID. 요청을 종료하는 규칙이 없으면 이 값은 `Default_Action`입니다.

terminatingRuleType

요청을 종료한 규칙의 유형. 가능한 값: RATE_BASED, REGULAR 및 GROUP.

작업

작업. 종료 규칙의 가능한 값: ALLOW 및 BLOCK. COUNT는 종료 규칙의 유효한 값이 아닙니다.

terminatingRuleMatch세부 정보

요청과 일치하는 종료 규칙에 대한 자세한 정보입니다. 종료 규칙에는 웹 요청에 대한 검사 프로세스를 종료하는 작업이 포함되어 있습니다. 종료 규칙에 가능한 작업은 ALLOW 및 BLOCK입니다. 이는 SQL 명령어 삽입 및 크로스 사이트 스크립팅(XSS) 일치 규칙 문에 대해서만 채워집니다. 두 개 이상의 항목을 검사하는 모든 규칙 문과 마찬가지로 AWS WAF 에서는 첫 번째 일치하는 항목에 작업을 적용하고 웹 요청 검사를 중지합니다. 종료 작업을 포함하고 있는 웹 요청에는 로그에 보고된 위협 외에 다른 위협이 있을 수 있습니다.

httpSourceName

요청의 소스. 가능한 값은 CF (소스가 아마존인 경우 CloudFront), APIGW (소스가 Amazon API Gateway인 경우), ALB (원본이 애플리케이션 로드 밸런서인 경우) 입니다.

httpSourceId

소스 ID. 이 필드에는 연결된 Amazon CloudFront 배포의 ID, API Gateway용 REST API 또는 애플리케이션 로드 밸런서의 이름이 표시됩니다.

ruleGroupList

이 요청에 작용하는 규칙 그룹의 목록. 위의 코드 예제에서는 하나만 있습니다.

ruleGroupId

규칙 그룹의 ID. 규칙에서 요청을 차단한 경우 `ruleGroupID`의 ID는 `terminatingRuleId`의 ID와 동일합니다.

terminatingRule

요청을 종료한 규칙 그룹 내의 규칙. 이 항목이 null이 아닌 값인 경우 ruleid 및 action도 포함됩니다. 이 경우 이 작업은 항상 BLOCK입니다.

nonTerminatingMatching규칙

요청에 부합되는 규칙 그룹의 규칙 목록. 이 항목은 항상 COUNT 규칙입니다(일치하는 비 종료 규칙).

조치 (nonTerminatingMatching규칙 그룹)

이 항목은 항상 COUNT입니다(일치하는 비 종료 규칙).

규칙 ID (규칙 그룹) nonTerminatingMatching

규칙 그룹에서 요청에 부합되는 비 종료 규칙의 ID. 즉. COUNT 규칙입니다.

excludedRules

규칙 그룹에서 제외한 규칙의 목록입니다. 이 규칙에 대한 작업은 COUNT로 설정됩니다.

exclusionType(excludedRules 그룹)

제외된 규칙에 COUNT 작업이 있음을 나타내는 유형입니다.

ruleId(excludedRules 그룹)

규칙 그룹 내에서 제외된 규칙의 ID입니다.

rateBasedRule목록

요청에 작용하는 속도 기반 규칙의 목록.

rateBasedRule아이디

요청에 작용하는 비율 기반 규칙의 ID입니다. 이 규칙이 요청을 종료한 경우 `rateBasedRuleId`의 ID는 `terminatingRuleId`의 ID와 동일합니다.

limitKey

요청이 단일 소스에서 도착하여 속도 모니터링 대상일 가능성이 있는지 판단하는 데 AWS WAF 사용하는 필드입니다. 가능한 값: IP.

maxRateAllowed

5분 기간 동안 허용되는 요청의 최대 수입니다. 이 항목의 값은 `limitKey`을(를) 통해 지정된 필드의 값과 동일합니다. 요청 수가 을 `maxRateAllowed` 초과하고 규칙에 지정된 다른 조건도 충족되면 이 규칙에 지정된 작업이 AWS WAF 트리거됩니다.

httpRequest

요청에 대한 메타데이터.

clientIp

클라이언트가 요청을 보내는 IP 주소.

country

요청의 출처 국가. 원산지를 확인할 수 없는 경우 AWS WAF 이 필드를 로 설정합니다. -

헤더

헤더 목록.

uri

요청의 URI. 위의 코드 예제는 이 필드가 삭제된 경우 값이 어떻게 되는지를 보여 줍니다.

args

쿼리 문자열.

httpVersion

HTTP 버전.

httpMethod

요청의 HTTP 메서드.

requestId

요청의 ID입니다.

비율 기반 규칙에서 차단한 IP 주소 나열

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF Classic은 속도 기반 규칙에 의해 차단된 IP 주소 목록을 제공합니다.

비율 기반 규칙에서 차단한 IP 주소를 보려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF 콘솔을 엽니다.

   탐색 창에 AWS WAF 클래식으로 전환이 표시되면 선택하십시오.
2. 탐색 창에서 규칙을 선택합니다.
3. [Name] 열에서 비율 기반 규칙을 하나 선택합니다.

   목록에 규칙이 현재 차단하는 IP 주소가 나열됩니다.

AWS WAF Classic이 Amazon CloudFront 기능과 함께 작동하는 방식

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

웹 ACL을 만들 때 AWS WAF Classic에서 검사할 CloudFront 배포를 하나 이상 지정할 수 있습니다. AWS WAF Classic에서는 웹 ACL에서 식별한 조건에 따라 해당 배포에 대한 웹 요청을 허용, 차단 또는 개수를 계산하기 시작합니다. CloudFront AWS WAF Classic 기능을 향상시키는 몇 가지 기능을 제공합니다. 이 장에서는 AWS WAF Classic이 함께 더 잘 CloudFront 작동하도록 CloudFront 구성할 수 있는 몇 가지 방법에 대해 설명합니다.

주제

AWS WAF Classic을 CloudFront 사용자 지정 오류 페이지와 함께 사용하기

AWS WAF Classic은 지정한 조건에 따라 웹 요청을 차단하면 HTTP 상태 코드 403 (금지됨) 을 에게 CloudFront 반환합니다. 그런 다음 해당 상태 코드를 뷰어에게 CloudFront 반환합니다. 최종 사용자에게는 다음과 유사한 짧고 불완전한 형식의 기본 메시지가 표시됩니다.

```
Forbidden: You don't have permission to access /myfilename.html on this
server.
```

웹 사이트의 나머지 부분과 동일한 형식을 사용하여 사용자 지정 오류 메시지를 표시하려는 경우 사용자 지정 오류 메시지가 포함된 개체 (예: HTML 파일) 를 뷰어에 CloudFront 반환하도록 구성할 수 있습니다.

> **Note**
>
> CloudFront 오리진에서 반환되는 HTTP 상태 코드 403과 요청이 차단되었을 때 AWS WAF Classic에서 반환되는 HTTP 상태 코드 403을 구분할 수 없습니다. 따라서 HTTP 상태 코드 403의 다른 원인을 기반으로 다른 사용자 지정 오류 페이지를 반환할 수 없습니다.

CloudFront 사용자 지정 오류 페이지에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 오류 응답 사용자 지정을 참조하십시오.

자체 HTTP 서버에서 실행되는 CloudFront 애플리케이션에 AWS WAF Classic 사용

AWS WAF Classic와 함께 CloudFront 사용하면 Amazon Elastic Compute Cloud (Amazon EC2) 에서 실행되는 웹 서버이든 비공개로 관리하는 웹 서버이든 관계없이 모든 HTTP 웹 서버에서 실행되는 애플리케이션을 보호할 수 있습니다. 또한 자체 웹 서버 간에는 물론 최종 사용자와 웹 서버 CloudFront 간에도 HTTPS를 CloudFront 요구하도록 구성할 수 있습니다. CloudFront

자체 웹 CloudFront 서버와 자체 웹 서버 사이에 HTTPS 요구

자체 웹 서버 간에 CloudFront HTTPS를 요구하려면 CloudFront 사용자 지정 오리진 기능을 사용하고 특정 오리진에 대한 오리진 프로토콜 정책 및 오리진 도메인 이름 설정을 구성할 수 있습니다. CloudFront 구성에서 오리진에서 객체를 가져올 때 사용할 포트 및 프로토콜과 함께 서버의 DNS 이름을 지정할 수 있습니다. CloudFront 또한 사용자 지정 오리진 서버의 SSL/TLS 인증서가 구성한 원본 도메인 이름과 일치하는지 확인해야 합니다. 외부에서 자체 HTTP 웹 서버를 사용하는 경우 Comodo 또는 Symantec과 같은 신뢰할 수 있는 타사 인증 기관 (CA) 에서 서명한 인증서를 사용해야 합니다. AWS DigiCert 자체 웹 서버 간 통신을 위해 HTTPS를 요구하는 방법에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 사용자 지정 CloudFront 오리진과 사용자 지정 오리진 간의 CloudFront 통신을 위한 HTTPS 요구 항목을 참조하십시오.

뷰어와 뷰어 사이에 HTTPS 요구 CloudFront

최종 사용자 CloudFront 간에 HTTPS를 요구하려면 배포에서 하나 이상의 캐시 동작에 대한 뷰어 프로토콜 정책을 변경할 수 있습니다. CloudFront 최종 사용자와 최종 사용자 간 HTTPS 사용에 대한 자세한 내용은 Amazon CloudFront 개발자 안내서의 “최종 사용자 간 통신을 위한 HTTPS 필요” 주제를 참조하십시오. CloudFront CloudFront 또한 자체 SSL 인증서를 가져와서 시청자가 자신의 도메인 이름 (예: https://www.mysite.com) 을 사용하여 HTTPS를 통해 CloudFront 배포에 연결할 수 있도록 할 수도 있습니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 대체 도메인 이름 및 HTTPS 구성 항목을 참조하십시오.

CloudFront응답하는 HTTP 메서드 선택

Amazon CloudFront 웹 배포를 생성할 때 처리하고 오리진에 CloudFront 전달하려는 HTTP 메서드를 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

- GET, HEAD — 오리진에서 객체를 가져오거나 객체 헤더를 가져오는 CloudFront 데만 사용할 수 있습니다.
- GET, HEAD, OPTIONS — 오리진에서 객체를 가져오거나, 객체 헤더를 가져오거나, 오리진 서버가 지원하는 옵션 목록을 검색하는 CloudFront 데만 사용할 수 있습니다.

- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE — 객체를 가져오고, 추가하고, 업데이트하고, 삭제하고, 객체 헤더를 가져오는 데 사용할 CloudFront 수 있습니다. 또한 웹 양식에서 데이터를 제출하는 등의 기타 POST 작업을 수행할 수 있습니다.

에 설명된 대로 AWS WAF 클래식 문자열 일치 조건을 사용하여 HTTP 메서드에 따라 요청을 허용하거나 차단할 수도 있습니다. 문자열 매칭 조건 작업 GET및 와 HEAD 같이 CloudFront 지원하는 메서드를 조합하여 사용하려는 경우 다른 방법을 사용하는 요청을 차단하도록 AWS WAF Classic을 구성하지 않아도 됩니다. , GETHEAD, 같이 CloudFront 지원하지 않는 메서드의 조합을 허용하려면 모든 메서드에 CloudFront 응답하도록 구성한 다음 AWS WAF Classic을 사용하여 다른 방법을 사용하는 요청을 차단할 수 있습니다. POST

CloudFront 응답하는 메서드를 선택하는 방법에 대한 자세한 내용은 Amazon CloudFront Developer Guide의 웹 배포를 만들거나 업데이트할 때 지정하는 값 항목의 허용된 HTTP 메서드를 참조하십시오.

AWS WAF 클래식의 보안

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. AWS WAF Classic에 적용되는 규정 준수 프로그램에 대해 알아보려면 규정 준수 프로그램별 범위 내AWS 서비스를 참조하십시오.

- 클라우드에서의 보안 - 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 데이터의 민감도, 조직의 요건 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 AWS WAF Classic을 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 AWS WAF Classic을 구성하는 방법을 보여줍니다. 또한 AWS WAF Classic 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

AWS WAF 클래식에서의 데이터 보호

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS 공동 책임 모델 모델은 AWS WAF Classic의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면

각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API 또는 SDK를 AWS 서비스 사용하여 AWS WAF Classic 또는 기타 버전으로 작업하는 경우가 포함됩니다. AWS CLI AWS 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

AWS WAF 중국 (베이징), 중국 (닝샤) 등 암호화를 사용할 수 없는 특정 지역을 제외하고 웹 ACL, 규칙 및 조건과 같은 클래식 엔티티는 저장 시 암호화됩니다. 리전마다 고유한 암호화 키가 사용됩니다.

AWS WAF 클래식 리소스 삭제

AWS WAF Classic에서 생성한 리소스는 삭제할 수 있습니다. 다음 섹션에 설명된 각 리소스 유형에 대한 지침을 참조하세요.

- 웹 ACL 삭제
- AWS WAF 클래식 규칙 그룹에서 규칙 추가 및 삭제
- 규칙 삭제

AWS WAF Classic의 ID 및 액세스 관리

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 Classic 리소스를 사용할 AWS WAF 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- AWS WAF 클래식과 IAM의 작동 방식
- AWS WAF Classic 자격 증명 기반 정책 예제
- AWS WAF 클래식 ID 및 액세스 문제 해결
- Classic용 서비스 연결 역할 사용 AWS WAF

고객

AWS Identity and Access Management Classic에서 수행하는 작업에 따라 사용 방법 (IAM) 이 다릅니다. AWS WAF

서비스 사용자 - AWS WAF 클래식 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS WAF 클래식 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. AWS WAF Classic의 기능에 액세스할 수 없는 경우 AWS WAF 클래식 ID 및 액세스 문제 해결(을)를 참조하세요.

서비스 관리자 — 회사에서 AWS WAF Classic 리소스를 담당하는 경우 Classic에 AWS WAF 대한 전체 액세스 권한이 있을 것입니다. 서비스 사용자가 액세스해야 하는 AWS WAF Classic 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사에서 IAM을 AWS WAF Classic과 함께 사용하는 방법에 대한 자세한 내용은 을 참조하십시오AWS WAF 클래식과 IAM의 작동 방식.

IAM 관리자 - IAM 관리자라면 Classic에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대해 자세히 알고 싶을 것입니다. AWS WAF IAM에서 사용할 수 있는 AWS WAF 클래식 ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF Classic 자격 증명 기반 정책 예제

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있

는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역

할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은

사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.

- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

AWS WAF 클래식과 IAM의 작동 방식

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

IAM을 사용하여 Classic에 대한 액세스를 관리하기 전에 AWS WAF Classic에서 사용할 수 있는 AWS WAF IAM 기능에 대해 알아보십시오.

클래식과 함께 사용할 수 있는 IAM 기능 AWS WAF

IAM 특성	AWS WAF 클래식 지원
ID 기반 정책	예

IAM 특성	AWS WAF 클래식 지원
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책 내 태그)	부분
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

AWS WAF Classic 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는AWS 서비스를 참조하십시오.

Classic의 ID 기반 정책 AWS WAF

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

AWS WAF Classic ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF Classic 자격 증명 기반 정책 예제

Classic 내의 리소스 기반 정책 AWS WAF

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Classic에 대한 정책 조치 AWS WAF

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

AWS WAF 클래식 작업 목록을 보려면 서비스 권한 부여 참조의 지역별로 정의된 작업 AWS WAF및 AWS WAF 지역별로 정의된 작업을 참조하십시오.

AWS WAF Classic의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
waf
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어List, 로 시작하는 AWS WAF Classic의 모든 작업을 지정하려면 다음 작업을 포함하십시오.

```
"Action": "waf:List*"
```

AWS WAF Classic ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF Classic 자격 증명 기반 정책 예제

Classic용 정책 리소스 AWS WAF

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS WAF Classic 리소스 유형 및 해당 ARN 목록을 보려면 서비스 권한 부여 참조의 지역별로 정의된 리소스 AWS WAF및 AWS WAF 지역별로 정의된 리소스를 참조하십시오. 각 리소스의 ARN을 지정할 수 있는 작업에 대해 알아보려면 지역별로 정의된 작업 AWS WAF및 지역별로 AWS WAF 정의된 작업을 참조하십시오. AWS WAF Classic 리소스의 일부에 대한 액세스를 허용하거나 거부하려면 해당 리소스의 ARN을 정책 `resource` 요소에 포함하세요.

AWS WAF Classic에서 리소스는 웹 ACL 및 규칙입니다. AWS WAF Classic은 바이트 일치, IP 일치, 크기 제한과 같은 조건도 지원합니다.

다음 표와 같이 이러한 리소스와 조건에는 고유한 Amazon 리소스 이름(ARN)이 연결되어 있습니다.

콘솔 내 이름 AWS WAF	AWS WAF SDK/CLI의 이름	ARN 형식
웹 ACL	`WebACL`	`arn:aws:waf::` *`account`*`:`*`webacl`*`/`*`ID`*
규칙	`Rule`	`arn:aws:waf::` *`account`*`:`*`rule`*`/`*`ID`*
문자열 일치 조건	`ByteMatchSet`	`arn:aws:waf::` *`account`*`:`*`bytematchset`*` /`*`ID`*
SQL 명령어 주입 일치 조건	`SqlInjectionMatchSet`	`arn:aws:waf::` *`account`*`:`*`sqlinjectionset`*` /`*`ID`*
크기 제약 조건	`SizeConstraintSet`	`arn:aws:waf::` *`account`*`:`*`sizeconstraintset`*` /`*`ID`*
IP 일치 조건	`IPSet`	`arn:aws:waf::` *`account`*`:`*`ipset`*`/`*`ID`*
교차 사이트 스크립팅 일치 조건	`XssMatchSet`	`arn:aws:waf::` *`account`*`:`*`xssmatchset`*` /`*`ID`*

AWS WAF Classic 리소스의 일부에 대한 액세스를 허용하거나 거부하려면 해당 리소스의 ARN을 정책 `resource` 요소에 포함하세요. AWS WAF 클래식용 ARN의 형식은 다음과 같습니다.

```
arn:aws:waf::account:resource/ID
```

account, *resource* 및 *ID* 변수를 유효한 값으로 대체합니다. 유효한 값은 다음과 같습니다.

- *##*: 사용자의 AWS 계정 ID. 값을 지정해야 합니다.
- *###*: AWS WAF 클래식 리소스의 유형입니다.
- *ID*: AWS WAF 클래식 리소스의 ID 또는 지정된 리소스와 연결된 지정된 유형의 모든 리소스를 나타내는 와일드카드 (*) AWS 계정

예를 들어, 다음 ARN은 계정 111122223333에 대한 모든 웹 ACL을 지정합니다.

```
arn:aws:waf::111122223333:webacl/*
```

클래식의 정책 조건 키 AWS WAF

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 AND 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

AWS WAF 클래식 조건 키 목록을 보려면 서비스 권한 부여 참조의 조건 키 AWS WAF 및 AWS WAF 지역별로 정의된 리소스를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 지역별로 정의된 작업 AWS WAF및 AWS WAF 지역별로 정의된 작업을 참조하십시오.

AWS WAF 클래식 ID 기반 정책의 예를 보려면 을 참조하십시오. AWS WAF Classic 자격 증명 기반 정책 예제

클래식의 ACL AWS WAF

ACL 지원	아니요

ACL(액세스 통제 목록)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC (클래식 포함) AWS WAF

ABAC(정책 내 태그) 지원	부분

ABAC(속성 기반 액세스 통제)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 엔티티 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Classic에서 임시 자격 증명 사용 AWS WAF

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 일부 자격 증명이 AWS 서비스 작동하지 않습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

Classic용 AWS WAF 포워드 액세스 세션

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하기 위한 요청과 함께 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS WAF Classic에 대한 서비스 역할

서비스 역할 지원	예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

> **Warning**
>
> 서비스 역할의 권한을 변경하면 AWS WAF Classic 기능이 작동하지 않을 수 있습니다. AWS WAF Classic에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하십시오.

Classic의 서비스 연결 역할 AWS WAF

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

AWS WAF 클래식 서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 을 참조하십시오. Classic용 서비스 연결 역할 사용 AWS WAF

AWS WAF Classic 자격 증명 기반 정책 예제

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

기본적으로 사용자 및 역할에는 AWS WAF Classic 리소스를 만들거나 수정할 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 ARN 형식을 비롯하여 AWS WAF Classic에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS WAF Regional (지역) 의 작업, 리소스, 조건 키 및 작업, 리소스 및 조건 키를 참조하십시오. AWS WAF

주제

- 정책 모범 사례
- 클래식 콘솔 사용 AWS WAF
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 다른 사람이 계정에서 AWS WAF Classic 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하세요.
- Use conditions in IAM policies to further restrict access(IAM 정책의 조건을 사용하여 액세스 추가 제한) – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 생성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하

여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.

- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

클래식 콘솔 사용 AWS WAF

AWS WAF 클래식 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 AWS WAF Classic 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

콘솔에 액세스하여 사용할 수 있는 사용자는 AWS WAF 클래식 AWS 콘솔에도 액세스할 수 있습니다. 추가 권한은 필요하지 않습니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

```
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS WAF 클래식 ID 및 액세스 문제 해결

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

다음 정보를 사용하면 AWS WAF Classic 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 해결하는 데 도움이 됩니다.

주제

- 저는 Classic에서 AWS WAF 작업을 수행할 권한이 없습니다.
- 저는 IAM을 수행할 권한이 없습니다. PassRole

- 제 외부 사용자가 제 AWS WAF Classic 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

저는 Classic에서 AWS WAF 작업을 수행할 권한이 없습니다.

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 waf:*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

이 경우 waf:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요하면 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류 메시지가 표시되면 iam:PassRole AWS WAF Classic에 역할을 넘길 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 AWS WAF Classic에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

제 외부 사용자가 제 AWS WAF Classic 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- AWS WAF Classic에서 이러한 기능을 지원하는지 알아보려면 을 참조하십시오AWS WAF 클래식과 IAM의 작동 방식.
- 소유하고 AWS 계정 있는 리소스에 대한 액세스 권한을 부여하는 방법을 알아보려면 IAM 사용 설명서에서 AWS 계정 자신이 소유한 다른 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- 자격 증명 연동을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하십시오.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

Classic용 서비스 연결 역할 사용 AWS WAF

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF 클래식은 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Classic에 직접 연결되는 고유한 유형의 IAM 역할입니다. AWS WAF 서비스 연결 역할은 AWS WAF Classic에서 미리 정의하며 서비스가 사용자를 대신하여 다른 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 AWS WAF Classic을 더 쉽게 설정할 수 있습니다. AWS WAF Classic은 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 AWS WAF Classic만이 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 이 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

먼저 역할의 관련 리소스를 삭제해야 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스 AWS WAF 액세스 권한을 실수로 제거할 수 없으므로 Classic 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

AWS WAF Classic에 대한 서비스 연결 역할 권한

AWS WAF Classic은 다음과 같은 서비스 연결 역할을 사용합니다.

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic은 이러한 서비스 연결 역할을 사용하여 Amazon Data Firehose에 로그를 기록합니다. 이러한 역할은 로그인을 활성화한 경우에만 사용됩니다. AWS WAF자세한 정보는 웹 ACL 트래픽 정보 로깅을 참조하세요.

`AWSServiceRoleForWAFLogging` 및 `AWSServiceRoleForWAFRegionalLogging` 서비스 연결 역할은 역할을 각각 수임하기 위해 다음 서비스를 신뢰합니다.

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

역할의 권한 정책을 통해 AWS WAF Classic은 지정된 리소스에서 다음 작업을 완료할 수 있습니다.

- 조치: `firehose:PutRecord` 그리고 Amazon Data `firehose:PutRecordBatch` Firehose에서 이름이 "aws-waf-logs- “로 시작하는 데이터 스트림 리소스 예를 들어 `aws-waf-logs-us-east-2-analytics`입니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 권한을 참조하세요.

AWS WAF Classic의 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. 에서 AWS WAF 클래식 로깅을 활성화하거나 Classic CLI 또는 AWS WAF AWS WAF Classic API에서 `PutLoggingConfiguration` 요청하면 Classic에서 서비스 연결 역할을 자동으로 생성합니다. AWS Management Console AWS WAF

로깅을 활성화하려면 `iam:CreateServiceLinkedRole` 권한이 있어야 합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. AWS WAF 클래식 로깅을 활성화하면 AWS WAF Classic에서 서비스 연결 역할을 다시 생성합니다.

AWS WAF Classic에 대한 서비스 연결 역할 편집

AWS WAF Classic에서는 역할 `AWSServiceRoleForWAFLogging` 및 `AWSServiceRoleForWAFRegionalLogging` 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 편집을 참조하세요.

AWS WAF Classic에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없어야 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> AWS WAF Classic 서비스가 리소스를 삭제하려고 할 때 역할을 사용하고 있는 경우 삭제가 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

`AWSServiceRoleForWAFLogging`및 에서 사용하는 AWS WAF Classic 리소스를 삭제하려면 `AWSServiceRoleForWAFRegionalLogging`

1. AWS WAF 클래식 콘솔에서 모든 웹 ACL에서 로깅을 제거합니다. 자세한 정보는 웹 ACL 트래픽 정보 로깅을 참조하세요.
2. API 또는 CLI를 사용하여 로깅이 활성화된 각 웹 ACL에 대한 `DeleteLoggingConfiguration` 요청을 제출합니다. 자세한 내용은 AWS WAF Classic API 참조를 참조하세요.

IAM을 사용하여 수동으로 서비스 링크 역할을 삭제하려면

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 `AWSServiceRoleForWAFLogging` 및 `AWSServiceRoleForWAFRegionalLogging` 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

AWS WAF Classic 서비스 연결 역할에 대해 지원되는 리전

AWS WAF Classic은 다음에서 서비스 연결 역할 사용을 지원합니다. AWS 리전

리전 이름	리전 자격 증명	AWS WAF 클래식 지원
미국 동부(버지니아 북부)	us-east-1	예
미국 동부(오하이오)	us-east-2	예
미국 서부(캘리포니아 북부)	us-west-1	예
미국 서부(오레곤)	us-west-2	예
아시아 태평양(뭄바이)	ap-south-1	예
아시아 태평양(오사카)	ap-northeast-3	예
아시아 태평양(서울)	ap-northeast-2	예
아시아 태평양(싱가포르)	ap-southeast-1	예
아시아 태평양(시드니)	ap-southeast-2	예
아시아 태평양(도쿄)	ap-northeast-1	예
캐나다(중부)	ca-central-1	예
유럽(프랑크푸르트)	eu-central-1	예
유럽(아일랜드)	eu-west-1	예
유럽(런던)	eu-west-2	예
유럽(파리)	eu-west-3	예
남아메리카(상파울루)	sa-east-1	예

AWS WAF 클래식에서의 로깅 및 모니터링

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

모니터링은 AWS WAF Classic과 AWS 솔루션의 신뢰성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. 다중 지점 오류가 발생할 경우 이를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 합니다. AWS AWS WAF Classic 리소스를 모니터링하고 잠재적 이벤트에 대응하기 위한 여러 도구를 제공합니다.

아마존 CloudWatch 알람

CloudWatch 경보를 사용하면 지정한 기간 동안 단일 지표를 관찰할 수 있습니다. 지표가 지정된 임계값을 초과하는 경우 Amazon SNS 주제 또는 AWS Auto Scaling 정책에 알림을 CloudWatch 보냅니다. 자세한 정보는 아마존을 통한 모니터링 CloudWatch을 참조하세요.

AWS CloudTrail 로그

CloudTrail AWS WAF Classic에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공합니다. 에서 수집한 CloudTrail 정보를 사용하여 AWS WAF Classic에 대한 요청, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다. 자세한 내용은 을 사용하여 AWS CloudTrail API 호출 로깅을(를) 참조하세요.

AWS WAF 클래식에 대한 규정 준수 검증

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

클래식에서의 AWS WAF 회복력

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS 글로벌 인프라는 가용 영역을 중심으로 AWS 리전 구축됩니다. AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS WAF 클래식의 인프라 보안

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 만들었고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF Classic은 관리형 서비스로서 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 AWS WAF Classic에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.

- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증 정보를 생성하여 요청에 서명할 수 있습니다.

AWS WAF 클래식 할당량

> **Note**
>
> 이것은 AWS WAF Classic 설명서입니다. 이 버전은 2019년 11월 AWS WAF 이전에 규칙 및 웹 ACL과 같은 AWS WAF 리소스를 생성했고 아직 최신 버전으로 마이그레이션하지 않은 경우에만 사용해야 합니다. 리소스를 마이그레이션하려면 AWS WAF Classic 리소스를 다음으로 마이그레이션하기 AWS WAF(을)를 참조하세요.
> 의 최신 버전에 대한 내용은 을 AWS WAF 참조하십시오. AWS WAF

AWS WAF Classic에는 다음과 같은 할당량 (이전에는 한도라고 함) 이 적용됩니다.

AWS WAF Classic에는 지역별 계정당 엔티티 수에 대한 기본 할당량이 있습니다. 이 할당량의 증가를 요청할 수 있습니다.

Resource	리전별 계정당 기본 할당량
웹 ACL	50
규칙	100
R ate-based-rules	5
리전별 계정당 조건 수	정규식 일치 및 지역 일치를 제외한 모든 조건의 경우 각 조건 유형당 100개입니

Resource	리전별 계정당 기본 할당량
	다. 100개의 크기 제약 조건 및 100개의 IP 일치 조건 등. 정규식 및 지역 일치 조건은 다음 표를 참조하세요.
초당 요청	웹 ACL당 25,000*

*이 할당량은 Application Load Balancer의 AWS WAF 클래식에만 적용됩니다. AWS WAF Classic CloudFront on의 초당 요청 수 (RPS) 할당량은 개발자 가이드에 설명된 RPS 할당량 지원과 동일합니다. CloudFront CloudFront

Classic 엔티티의 다음 할당량은 변경할 수 없습니다. AWS WAF

Resource	리전별 계정당 할당량
웹 ACL당 규칙 그룹	2:1 고객 생성 규칙 그룹과 1 규칙 그룹 AWS Marketplace
웹 ACL당 규칙	10
규칙당 조건	10
IP 일치 조건당 IP 주소 범위(CIDR 표기법 사용)	10,000개 한 번에 최대 1,000개의 주소를 업데이트할 수 있습니다. API 호

Resource	리전별 계정당 할당량
	출 `UpdateIPSet` 은 단일 요청으로 최대 1,000개의 주소를 수락합니다.
비율 기반 규칙에 따라 차단된 IP 주소	10,000개
5분당 최소 비율 기반 규칙 비율 제한	100
교차 사이트 스크립팅 일치 조건당 필터	10
크기 제약 조건당 필터	10
SQL 명령어 주입 일치 조건당 필터	10
문자열 일치 조건당 필터	10
문자열 일치 조건에서 HTTP 헤더 이름의 문자 수 (웹 요청의 헤더에서 지정된 값을 검사하도록 AWS WAF Classic을 구성한 경우)	40
문자열 일치 조건에서 AWS WAF Classic에서 검색하려는 값의 문자 수	50
정규식 일치 조건	10
정규식 일치 조건에서 AWS WAF Classic에서 검색하려는 패턴의 문자 수	70
정규식 일치 조건에서 패턴 세트당 패턴의 수	10
정규식 일치 조건에서 정규식 조건당 패턴 세트의 수	1
패턴 세트	5
지역 일치 조건	50
지역 일치 조건별 위치	50

AWS WAF Classic에는 지역별 계정당 통화 할당량이 다음과 같이 고정되어 있습니다. 이러한 할당량은 콘솔, CLI, REST API, SDK 등 사용 가능한 모든 수단을 통해 서비스에 대한 총 호출 수에 적용됩니다. AWS CloudFormation이러한 할당량은 변경할 수 없습니다.

호출 유형	리전별 계정당 할당량
`AssociateWebACL` 에 대한 최대 호출 수	2초당 1개의 요청
`DisassociateWebACL` 에 대한 최대 호출 수	2초당 1개의 요청
`GetWebACLForResource` 에 대한 최대 호출 수	1초당 1개의 요청
`ListResourcesForWebACL` 에 대한 최대 호출 수	1초당 1개의 요청
`CreateWebACLMigrationStack` 에 대한 최대 호출 수	1초당 1개의 요청
`GetChangeToken` 에 대한 최대 호출 수	초당 10개의 요청
`GetChangeTokenStatus` 에 대한 최대 호출 수	1초당 1개의 요청
개별 `List` 작업에 대한 최대 호출 수(다른 할당량이 정의되지 않은 경우)	1초당 5개의 요청
개별 `Create`, `Put`, `Get` 또는 `Update` 작업에 대한 최대 호출 수 (다른 할당량이 정의되지 않은 경우)	1초당 1개의 요청

AWS Shield

DDoS(분산 서비스 거부) 공격으로부터 보호하는 것은 인터넷 연계 애플리케이션에서 가장 중요합니다. 애플리케이션을 구축할 때 추가 비용 없이 AWS 제공되는 보호 기능을 사용할 수 있습니다. AWS또한 AWS Shield Advanced 관리형 위협 보호 서비스를 사용하여 추가 DDoS 탐지, 완화 및 대응 기능을 통해 보안 태세를 개선할 수 있습니다.

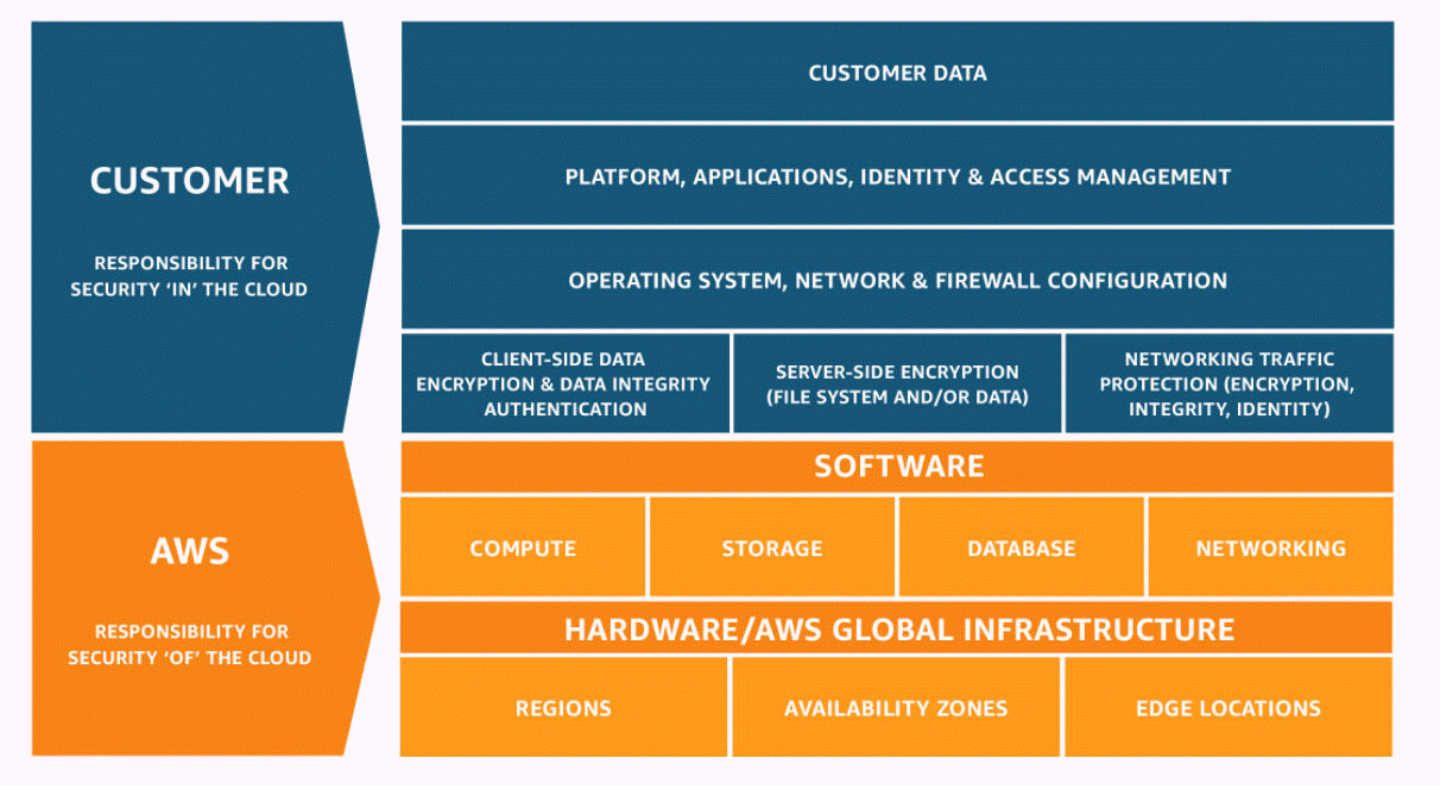
AWS 인터넷상의 악의적인 행위자에 대한 방어에 필요한 높은 가용성, 보안 및 탄력성을 보장하는 데 도움이 되는 도구, 모범 사례 및 서비스를 제공하기 위해 최선을 다하고 있습니다. 이 가이드는 IT 의사 결정권자와 보안 엔지니어가 Shield 및 Shield Advanced를 사용하여 DDoS 공격 및 기타 외부 위협으로부터 애플리케이션을 더 잘 보호하는 방법을 이해할 수 있도록 도움을 주기 위해 제공됩니다.

애플리케이션을 구축하면 UDP 리플렉션 공격 및 TCP SYN 플러드와 같은 일반적인 대량 DDoS 공격 AWS 벡터로부터 자동으로 보호됩니다. AWS DDoS 복원성을 위한 아키텍처를 설계하고 AWS 구성하여 이러한 보호 기능을 활용하여 실행 중인 애플리케이션의 가용성을 보장할 수 있습니다.

이 가이드에서는 DDoS 복원력을 위한 애플리케이션 아키텍처를 설계, 생성 및 구성하는 데 도움이 되는 권장 사항을 제공합니다. 이 가이드에 제공된 모범 사례를 준수하는 애플리케이션은 대규모 DDoS 공격과 광범위한 DDoS 공격 벡터의 표적이 될 때 가용성 연속성 개선의 이점을 누릴 수 있습니다. 또한 이 가이드에서는 Shield Advanced를 사용하여 중요한 애플리케이션에 최적화된 DDoS 보호 태세를 구현하는 방법을 보여줍니다. 여기에는 고객에게 일정 수준의 가용성을 보장한 애플리케이션과 DDoS 이벤트 발생 AWS 시 운영 지원이 필요한 애플리케이션이 포함됩니다.

보안은 사용자와 사용자 AWS 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Shield Advanced에 적용되는 규정 준수 프로그램에 대한 자세한 설명은 규정 준수 프로그램 제공 범위 내의AWS 서비스를 참조하세요.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 데이터의 민감도, 조직의 요건 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.



AWS Shield 앤 쉴드 어드밴스드 작동 방식

AWS Shield Standard 또한 네트워크 및 전송 계층 (계층 3 및 4) 과 애플리케이션 계층 (계층 7) 의 AWS 리소스에 대한 DDoS (분산 서비스 거부) 공격으로부터 AWS Shield Advanced 보호합니다. DDoS 공격은 손상된 여러 시스템이 표적에 트래픽을 폭주시키려고 시도하는 공격입니다. DDoS 공격은 합법적 사용자의 표적 서비스 액세스를 방해할 수 있으며 과도한 트래픽 볼륨으로 인해 표적에 충돌이 발생할 수 있습니다.

AWS Shield 알려진 다양한 DDoS 공격 벡터와 제로데이 공격 벡터로부터 보호합니다. Shield 탐지 및 완화 기능은 탐지 당시 서비스에 해당 위협이 명시적으로 알려지지 않았더라도 위협에 대한 적용 범위를 제공하도록 설계되었습니다. Shield Standard는 AWS사용 시 추가 비용 없이 자동으로 제공됩니다.

Shield가 탐지하는 공격 클래스는 다음과 같습니다.

- 네트워크 대규모 공격(계층 3) – 인프라 계층 공격 벡터의 하위 범주입니다. 이러한 벡터는 표적 네트워크 또는 리소스의 용량을 포화 상태로 만들어 합법적인 사용자에 대한 서비스를 거부하려고 합니다.
- 네트워크 프로토콜 공격(계층 4) – 인프라 계층 공격 벡터의 하위 범주입니다. 이러한 벡터는 프로토콜을 악용하여 대상 리소스에 대한 서비스를 거부합니다. 네트워크 프로토콜 공격의 일반적인 예로

는 서버, 로드 밸런서 또는 방화벽과 같은 리소스의 연결 상태를 고갈시킬 수 있는 TCP SYN flood가 있습니다. 네트워크 프로토콜 공격은 대규모 공격일 수도 있습니다. 예를 들어, TCP SYN flood가 커지면 네트워크 용량이 포화되는 동시에 대상 리소스 또는 중간 리소스의 상태가 고갈될 수 있습니다.

- 애플리케이션 계층 공격(계층 7) – 이 범주의 공격 벡터는 웹 요청 flood와 같이 대상에 유효한 쿼리를 애플리케이션에 폭주시켜 합법적인 사용자에 대한 서비스를 거부하려고 합니다.

목차

AWS Shield Standard 개요

AWS Shield 애플리케이션의 경계를 보호하는 관리형 위협 방지 서비스입니다. 경계는 네트워크 외부에서 들어오는 애플리케이션 트래픽의 첫 번째 진입점입니다. AWS

애플리케이션 경계의 위치를 결정하려면 사용자가 인터넷에서 애플리케이션에 액세스하는 방법을 고려해 보십시오. 첫 번째 진입점이 AWS 지역에 있는 경우 애플리케이션 경계는 Amazon VPC (Virtual Private Cloud) 입니다. Amazon Route 53이 사용자를 애플리케이션으로 안내하고 Amazon

CloudFront 또는 AWS Global Accelerator를 사용하여 애플리케이션에 먼저 액세스하는 경우 애플리케이션 경계는 AWS 네트워크 엣지에서 시작됩니다.

Shield는 실행 중인 모든 애플리케이션에 DDoS 탐지 및 완화 이점을 제공하지만 AWS, 애플리케이션 아키텍처를 설계할 때 내리는 결정은 DDoS 복원력 수준에 영향을 미칩니다. DDoS 복원력이란 공격 중에도 예상 파라미터 내에서 계속 작동할 수 있는 애플리케이션의 능력입니다.

모든 AWS 고객은 추가 비용 없이 Shield Standard의 자동 보호 기능을 이용할 수 있습니다. Shield Standard는 웹 사이트 또는 애플리케이션을 대상으로 하는 가장 흔하고 자주 발생하는 네트워크 및 전송 계층 DDoS 공격을 방어합니다. Shield Standard는 모든 AWS 고객을 보호하는 데 도움이 되지만 Amazon Route 53 호스팅 영역, Amazon CloudFront 배포 및 AWS Global Accelerator 표준 액셀러레이터를 사용하면 특별한 이점을 얻을 수 있습니다. 이러한 리소스는 알려진 모든 네트워크 및 전송 계층 공격에 대한 포괄적인 가용성 보호를 받습니다.

AWS Shield Advanced 개요

AWS Shield Advanced DDoS 공격, 볼류메트릭 봇, 취약성 악용 시도와 같은 외부 위협으로부터 애플리케이션을 보호하는 데 도움이 되는 관리형 서비스입니다. 공격으로부터 더 높은 수준의 보호를 위해 AWS Shield Advanced을(를) 구독할 수 있습니다.

Shield Advanced를 구독하고 리소스에 보호 기능을 추가하면 Shield Advanced는 해당 리소스에 대한 확장된 DDoS 공격 보호를 제공합니다. Shield Advanced에서 받는 보호 기능은 아키텍처 및 구성 선택에 따라 달라질 수 있습니다. 이 가이드의 정보를 사용하여 Shield Advanced를 사용하여 복원력이 뛰어난 애플리케이션을 구축 및 보호하고, 전문가의 도움이 필요한 경우 에스컬레이션하십시오.

쉴드 어드밴스드 구독 및 비용 AWS WAF

Shield Advanced를 구독하면 Shield Advanced로 보호하는 리소스의 표준 AWS WAF 기능을 사용하는 데 드는 비용이 포함됩니다. Shield Advanced 보호가 적용되는 표준 AWS WAF 요금은 웹 ACL당 비용, 규칙당 비용, 웹 요청 검사 요청 1백만 건당 기본 가격 (최대 1,500WCU 및 최대 기본 본체 크기) 입니다.

Shield Advanced 자동 애플리케이션 레이어 DDoS 완화를 활성화하면 150개의 웹 ACL 용량 단위 (WCU) 를 사용하는 규칙 그룹이 웹 ACL에 추가됩니다. 이러한 WCU는 웹 ACL의 WCU 사용량에 포함됩니다. 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화, Shield Advanced 규칙 그룹, AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

Shield Advanced를 구독해도 Shield Advanced를 사용하여 보호하지 않는 리소스에 AWS WAF 대한 사용은 포함되지 않습니다. 또한 보호 대상 리소스에 대한 추가 비표준 AWS WAF 비용도 포함되지 않

습니다. 비표준 AWS WAF 비용의 예로는 Bot Control, CAPTCHA 규칙 작업, 1,500개 이상의 WCU를 사용하는 웹 ACL, 기본 본문 크기를 초과하여 요청 본문을 검사하는 비용 등이 있습니다. 전체 목록은 요금 페이지에 나와 있습니다. AWS WAF

전체 정보 및 요금 예는 Shield 요금 및 AWS WAF 요금을 참조하세요.

Shield Advanced 구독 결제

AWS 채널 리셀러인 경우 계정 팀에 문의하여 정보와 지침을 얻으세요. 이 청구 정보는 AWS 채널 리셀러가 아닌 고객을 위한 것입니다.

그 외의 모든 경우에는 다음과 같은 가입 및 결제 지침이 적용됩니다.

- AWS Organizations 조직 구성원 계정의 경우 지급인 계정 자체가 구독되어 있는지 여부와 상관없이 Shield Advanced 구독을 조직의 지불자 계정에 대해 AWS 청구합니다.
- 동일한 AWS Organizations 통합 결제 계정 패밀리에 속하는 여러 계정에 가입하는 경우, 하나의 가입 요금이 패밀리 내 모든 가입 계정에 적용됩니다. 조직은 모든 AWS 계정 와(과) 모든 리소스를 소유해야 합니다.
- 여러 조직의 여러 계정에 가입하는 경우에도 모든 조직, 계정, 리소스를 소유하고 있다면 모든 조직, 계정, 리소스에 대해 하나의 가입 요금을 지불할 수 있습니다. 계정 관리자 또는 AWS 지원팀에 문의하여 한 조직을 제외한 모든 조직의 AWS Shield Advanced 구독 요금에 대한 수수료 면제를 요청하세요.

자세한 요금 정보 및 예는 AWS Shield 요금 섹션을 참조하세요.

주제

- AWS Shield Advanced 보호 대상 리소스
- AWS Shield Advanced 기능 및 옵션
- AWS Shield Advanced 구독 여부 및 추가 보호 적용 여부 결정

AWS Shield Advanced 보호 대상 리소스

> **Note**
>
> Shield Advanced 보호는 Shield Advanced에서 명시적으로 지정했거나 Shield Advanced 정책을 통해 보호하는 리소스에만 사용할 수 있습니다. AWS Firewall Manager Shield Advanced는 리소스를 자동으로 보호하지 않습니다.

다음 리소스 유형을 포함한 고급 모니터링 및 보호에 Shield Advanced를 사용할 수 있습니다.

- 아마존 CloudFront 배포판. CloudFront 지속적인 배포의 경우 Shield Advanced는 보호된 기본 배포와 관련된 모든 스테이징 배포를 보호합니다.
- Amazon Route 53 호스팅 영역.
- AWS Global Accelerator 표준 액셀러레이터.
- Amazon EC2 탄력적 IP 주소. Shield Advanced는 보호된 탄력적 IP 주소와 연결된 리소스를 보호합니다.
- Amazon EC2 인스턴스, Amazon EC2 탄력적 IP 주소와의 연결을 통해.
- 다음 유형의 Elastic Load Balancing(ELB) 로드 밸런서:
  - Application Load Balancers.
  - Classic Load Balancer
  - Network Load Balancer, Amazon EC2 탄력적 IP 주소와의 연결을 통해.

리소스 유형의 보호에 대한 추가 정보는 AWS Shield Advanced 리소스 유형별 보호 섹션을 참조하세요.

AWS Shield Advanced 기능 및 옵션

AWS Shield Advanced 서브스크립션에는 다음과 같은 기능 및 옵션이 포함됩니다. 여기에는 이미 제공되는 DDoS 탐지 및 완화 기능이 보완됩니다. AWS

- AWS WAF 통합 — Shield Advanced는 AWS WAF 웹 ACL, 규칙 및 규칙 그룹을 애플리케이션 계층 보호의 일부로 사용합니다. 에 대한 자세한 내용은 AWS WAF을 참조하십시오. AWS WAF 작동 방식

> **Note**
>
> Shield Advanced를 구독하면 Shield Advanced로 보호하는 리소스의 표준 AWS WAF 기능을 사용하는 데 드는 비용이 포함됩니다. Shield Advanced 보호가 적용되는 표준 AWS WAF 요금은 웹 ACL당 비용, 규칙당 비용, 웹 요청 검사 요청 1백만 건당 기본 가격 (최대 1,500WCU 및 최대 기본 본체 크기) 입니다.
> Shield Advanced 자동 애플리케이션 레이어 DDoS 완화를 활성화하면 150개의 웹 ACL 용량 단위 (WCU) 를 사용하는 규칙 그룹이 웹 ACL에 추가됩니다. 이러한 WCU는 웹 ACL의 WCU 사용량에 포함됩니다. 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화, Shield Advanced 규칙 그룹, AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

Shield Advanced를 구독해도 Shield Advanced를 사용하여 보호하지 않는 리소스에 AWS WAF 대한 사용은 포함되지 않습니다. 또한 보호 대상 리소스에 대한 추가 비표준 AWS WAF 비용도 포함되지 않습니다. 비표준 AWS WAF 비용의 예로는 Bot Control, CAPTCHA 규칙 작업, 1,500개 이상의 WCU를 사용하는 웹 ACL, 기본 본문 크기를 초과하여 요청 본문을 검사하는 비용 등이 있습니다. 전체 목록은 요금 페이지에 나와 있습니다. AWS WAF 전체 정보 및 요금 예는 Shield 요금 및 AWS WAF 요금을 참조하세요.

- 자동 애플리케이션 계층 DDoS 완화 – 보호된 리소스에 대한 애플리케이션 계층(계층 7) 공격을 완화하기 위해 자동으로 대응하도록 Shield Advanced를 구성할 수 있습니다. 자동 방어 기능을 갖춘 Shield Advanced는 알려진 DDoS 소스의 요청에 대해 AWS WAF 속도 제한을 적용하고 탐지된 DDoS 공격에 대응하여 사용자 지정 AWS WAF 보호 기능을 자동으로 추가하고 관리합니다. 공격의 일부인 웹 요청을 계수하거나 차단하도록 자동 완화를 구성할 수 있습니다.

  자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화 섹션을 참조하세요.

- 상태 기반 탐지 – Shield Advanced와 함께 Amazon Route 53 상태 확인을 사용하여 이벤트 탐지 및 완화 조치를 알릴 수 있습니다. 상태 확인은 사양에 따라 애플리케이션을 모니터링하여 사양이 충족되면 정상으로 보고하고, 충족되지 않으면 비정상으로 보고합니다. Shield Advanced와 함께 상태 확인을 사용하면 오탐지를 방지하고 보호된 리소스가 비정상일 때 더 빠르게 탐지 및 완화할 수 있습니다. Route 53 호스팅 영역을 제외한 모든 리소스 유형에 상태 기반 탐지를 사용할 수 있습니다. Shield Advanced 선제적 대응은 상태 기반 탐지가 활성화된 리소스에만 사용할 수 있습니다.

  자세한 내용은 상태 점검을 사용한 상태 기반 탐지 섹션을 참조하세요.

- 보호 그룹 – 보호 그룹을 사용하여 보호된 리소스를 논리적으로 그룹화하여 그룹 전체에 대한 탐지 및 완화 기능을 강화할 수 있습니다. 새로 보호된 리소스가 자동으로 포함되도록 보호 그룹의 멤버십 기준을 정의할 수 있습니다. 보호된 리소스는 다중 보호 그룹에 속할 수 있습니다.

  자세한 내용은 AWS Shield Advanced 보호 그룹 섹션을 참조하세요.

- DDoS 이벤트 및 공격에 대한 가시성 향상 – Shield Advanced는 고급 실시간 지표 및 보고서에 액세스하여 보호된 AWS 리소스에 대한 이벤트 및 공격에 대한 광범위한 가시성을 제공합니다. Shield Advanced API와 콘솔, 그리고 Amazon CloudWatch 지표를 통해 이 정보에 액세스할 수 있습니다.

  자세한 정보는 DDoS 이벤트에 대한 가시성을 참조하세요.

- AWS Firewall Manager(을)를 통한 Shield Advanced 보호의 중앙 집중식 관리 - Firewall Manager를 사용하여 새 계정 및 리소스에 Shield Advanced 보호를 자동으로 적용하고 웹 ACL에 AWS WAF 규칙을 배포할 수 있습니다. Shield Advanced 고객에게는 Firewall Manager Shield Advanced 보호 정책이 추가 비용 없이 포함됩니다. 또한 Amazon Simple Notification Service(SNS) 주제 또는 AWS

Security Hub와 함께 Firewall Manager를 사용하거나 계정에 대한 Shield Advanced 모니터링 활동을 중앙 집중식으로 관리할 수도 있습니다.

Firewall Manager를 사용하여 Shield Advanced 보호를 관리하는 방법에 대한 자세한 내용은 AWS Firewall Manager 및 AWS Shield Advanced 정책 섹션을 참조하세요. Firewall Manager 요금에 대한 자세한 내용은 AWS Firewall Manager 요금 섹션을 참조하세요.

- AWS Shield Response Team (SRT) — SRT는 Amazon.com과 그 자회사를 보호하는 데 있어 AWS 풍부한 경험을 가지고 있습니다. AWS Shield Advanced 고객으로서, 사용자는 애플리케이션 가용성에 영향을 미치는 DDoS 공격이 발생하는 동안 언제든지 SRT에 문의하여 지원을 받을 수 있습니다. 또한 SRT와 협력하여 리소스에 대한 사용자 지정 방어 수단을 만들고 관리할 수도 있습니다. SRT의 서비스를 사용하려면 Business Support 플랜 또는 Enterprise Support 플랜을 구독해야 합니다.

  자세한 내용은 Shield 대응 팀(SRT) 지원 섹션을 참조하세요.
- 선제적 대응 – 선제적 대응을 사용할 경우, Shield Advanced에서 탐지된 이벤트가 발생했을 때 보호된 리소스와 연결된 Amazon Route 53 상태 확인에서 위험한 것으로 나타나면 Shield 대응 팀(SRT)이 직접 연락을 드립니다. 따라서 수상한 공격으로 인해 애플리케이션을 사용하지 못할 수도 있는 상황이 발생했을 때 더 신속하게 전문가와 연락을 취할 수 있습니다.

  자세한 정보는 선제적 대응 구성을 참조하세요.
- 비용 보호 기회 — Shield Advanced는 보호된 리소스에 대한 DDoS 공격으로 인해 발생할 수 있는 비용 급증에 대비하여 비용을 어느 정도 보호합니다. AWS 여기에는 Shield Advanced 데이터 전송(DTO) 사용 요금 급증에 대한 보장이 포함될 수 있습니다. Shield Advanced는 Shield Advanced 서비스 크레딧의 형태로 모든 비용 보호를 제공합니다.

  자세한 내용은 크레딧 요청 AWS Shield Advanced을(를) 참조하세요.

AWS Shield Advanced 구독 여부 및 추가 보호 적용 여부 결정

구독할 AWS Shield Advanced 계정과 추가 보호를 적용할 위치를 결정하는 데 도움이 필요하면 이 섹션의 시나리오를 검토하십시오. Shield Advanced를 사용하면 통합 결제 계정으로 생성된 모든 계정에 대해 월 1회의 구독료와 전송된 데이터 GB를 기준으로 한 사용 요금을 지불합니다. Shield Advanced 요금에 대한 자세한 내용은 AWS Shield Advanced 요금 섹션을 참조하세요.

Shield Advanced를 사용하여 애플리케이션과 해당 리소스를 보호하려면 애플리케이션을 관리하는 계정을 Shield Advanced에 등록한 다음 애플리케이션 리소스에 보호 기능을 추가합니다. 계정 구독 및 리소스 보호에 대한 자세한 내용은 시작하기 AWS Shield Advanced 섹션을 참조하세요.

쉴드 어드밴스드 구독 및 비용 AWS WAF

Shield Advanced를 구독하면 Shield Advanced로 보호하는 리소스의 표준 AWS WAF 기능을 사용하는 데 드는 비용이 포함됩니다. Shield Advanced 보호가 적용되는 표준 AWS WAF 요금은 웹 ACL당 비용, 규칙당 비용, 웹 요청 검사 요청 1백만 건당 기본 가격 (최대 1,500WCU 및 최대 기본 본체 크기) 입니다.

Shield Advanced 자동 애플리케이션 레이어 DDoS 완화를 활성화하면 150개의 웹 ACL 용량 단위 (WCU) 를 사용하는 규칙 그룹이 웹 ACL에 추가됩니다. 이러한 WCU는 웹 ACL의 WCU 사용량에 포함됩니다. 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화, Shield Advanced 규칙 그룹, AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

Shield Advanced를 구독해도 Shield Advanced를 사용하여 보호하지 않는 리소스에 AWS WAF 대한 사용은 포함되지 않습니다. 또한 보호 대상 리소스에 대한 추가 비표준 AWS WAF 비용도 포함되지 않습니다. 비표준 AWS WAF 비용의 예로는 Bot Control, CAPTCHA 규칙 작업, 1,500개 이상의 WCU를 사용하는 웹 ACL, 기본 본문 크기를 초과하여 요청 본문을 검사하는 비용 등이 있습니다. 전체 목록은 요금 페이지에 나와 있습니다. AWS WAF

전체 정보 및 요금 예는 Shield 요금 및 AWS WAF 요금을 참조하세요.

Shield Advanced 구독 결제

AWS 채널 리셀러인 경우 계정 팀에 문의하여 정보와 지침을 얻으세요. 이 청구 정보는 AWS 채널 리셀러가 아닌 고객을 위한 것입니다.

그 외의 모든 경우에는 다음과 같은 가입 및 결제 지침이 적용됩니다.

- AWS Organizations 조직 구성원 계정의 경우 지급인 계정 자체가 구독되어 있는지 여부와 상관없이 Shield Advanced 구독을 조직의 지불자 계정에 대해 AWS 청구합니다.
- 동일한 AWS Organizations 통합 결제 계정 패밀리에 속하는 여러 계정에 가입하는 경우, 하나의 가입 요금이 패밀리 내 모든 가입 계정에 적용됩니다. 조직은 모든 AWS 계정 와(과) 모든 리소스를 소유해야 합니다.
- 여러 조직의 여러 계정에 가입하는 경우에도 모든 조직, 계정, 리소스를 소유하고 있다면 모든 조직, 계정, 리소스에 대해 하나의 가입 요금을 지불할 수 있습니다. 계정 관리자 또는 AWS 지원팀에 문의하여 한 조직을 제외한 모든 조직의 AWS Shield Advanced 구독 요금에 대한 수수료 면제를 요청하세요.

자세한 요금 정보 및 예는 AWS Shield 요금 섹션을 참조하세요.

보호할 애플리케이션 식별

다음 중 하나가 필요한 애플리케이션에는 Shield Advanced 보호를 구현하는 것을 고려해 보십시오.

- 애플리케이션 사용자의 가용성이 보장됩니다.
- 애플리케이션이 DDoS 공격의 영향을 받는 경우 DDoS 방어 전문가에게 신속하게 액세스할 수 있습니다.
- 애플리케이션이 DDoS 공격의 영향을 받을 수 AWS 있다는 점을 인지하고 보안 또는 운영 팀에 대한 공격 알림 AWS 및 에스컬레이션 작업을 진행하십시오.
- DDoS 공격이 AWS 서비스 사용에 영향을 미치는 시기를 포함하여 클라우드 비용을 예측할 수 있습니다.

애플리케이션 또는 해당 리소스에 위와 같은 사항이 필요한 경우 관련 계정에 대한 구독을 생성하는 것을 고려해 보십시오.

보호할 리소스 식별

각 구독 계정에 대해 다음과 같은 특징을 가진 각 리소스에 Shield Advanced 보호를 추가하는 것을 고려해 보십시오.

- 이 리소스는 인터넷 상의 외부 사용자에게 서비스를 제공합니다.
- 리소스는 인터넷에 노출되며 중요한 애플리케이션의 일부이기도 합니다. 인터넷에서 사용자가 액세스할 수 있도록 의도했는지 여부와 상관없이 노출된 모든 리소스를 고려하십시오.
- 리소스는 AWS WAF 웹 ACL로 보호됩니다.

리소스에 대한 보호를 생성하고 관리하는 방법에 대한 자세한 내용은 의 리소스 보호 AWS Shield Advanced 섹션을 참조하세요.

또한 이 가이드의 권장 사항을 따르면 DDoS 복원력을 위한 애플리케이션을 설계하고 최적의 보호를 위해 Shield Advanced의 기능을 적절하게 구성했는지 확인하는 데 도움이 됩니다.

DDoS 공격의 예시

AWS Shield Advanced 다양한 유형의 공격에 대한 확장된 보호를 제공합니다.

다음 목록에서는 몇 가지 일반적인 공격 유형에 대해 설명합니다.

UDP(User Datagram Protocol) 반사 공격

UDP 반사 공격 시 공격자는 요청의 소스를 스푸핑하고 UDP를 사용하여 서버에서 대규모 응답을 끌어낼 수 있습니다. 공격을 받는 스푸핑된 IP 주소에 추가 네트워크 트래픽이 유도되면 대상 서버

의 속도가 느려질 수 있으며 합법적인 최종 사용자가 필요한 리소스에 액세스하지 못할 수 있습니다.

TCP SYN flood

TCP SYN flood 공격의 목적은 연결을 절반 정도 열린 상태로 유지하여 시스템에서 사용 가능한 리소스가 고갈되도록 하는 것입니다. 사용자가 웹 서버와 같은 TCP 서비스에 연결하면 클라이언트는 TCP SYN 패킷을 전송합니다. 서버는 승인을 반환하고 클라이언트는 자체 승인을 반환하여 3방향 핸드셰이크를 완료합니다. TCP SYN flood에서 세 번째 승인은 반환되지 않고 서버는 응답을 대기하는 상태로 유지됩니다. 이로 인해 다른 사용자가 서버에 연결하지 못할 수 있습니다.

DNS 쿼리 flood

DNS 쿼리 플러드에서 공격자는 여러 DNS 쿼리를 사용하여 DNS 서버의 리소스를 소진시킵니다. AWS Shield Advanced Route 53 DNS 서버의 DNS 쿼리 플러드 공격으로부터 보호하는 데 도움이 될 수 있습니다.

HTTP flood/캐시 버스팅(계층 7) 공격

GET 및 POST flood를 포함한 HTTP flood 공격에서 공격자는 웹 애플리케이션의 실제 사용자로부터 나온 것처럼 보이는 여러 HTTP 요청을 전송합니다. 캐시 버스팅 공격은 HTTP 요청 쿼리 문자열에서 변형을 사용하여 에지 로케이션 캐시 콘텐츠 사용을 가로막고 콘텐츠가 오리진 웹 서버에서 제공되도록 강제하여 오리진 웹 서버에 손상을 일으킬 수 있는 추가 부담을 발생시키는 일종의 HTTP flood입니다.

이벤트 AWS Shield 감지 방법

AWS AWS 네트워크 및 개별 AWS 서비스에 대한 서비스 수준 탐지 시스템을 운영하여 DDoS 공격 중에도 계속 사용할 수 있도록 합니다. 또한 리소스 수준 탐지 시스템은 각 개별 리소스를 모니터링하여 AWS 리소스로 향하는 트래픽이 예상 매개변수 이내로 유지되도록 합니다. 이 조합은 알려진 불량 패킷을 삭제하고, 잠재적으로 악의적인 트래픽을 찾아내고, 최종 사용자의 트래픽에 우선 순위를 지정하는 완화 기능을 적용하여 대상 AWS 리소스와 AWS 서비스를 모두 보호합니다.

탐지된 이벤트는 Shield Advanced 이벤트 요약, 공격 세부 정보 및 Amazon CloudWatch 지표에 DDoS 공격 벡터의 이름으로 표시되거나 시그니처 대신 트래픽 볼륨을 기반으로 평가된 Volumetric 것처럼 표시됩니다. DDoSDetected CloudWatch지표 내에서 사용할 수 있는 공격 벡터 차원에 대한 자세한 내용은 다음을 참조하십시오. AWS Shield Advanced 측정 항목

주제

- 인프라 계층 위협에 대한 감지 로직

- 애플리케이션 계층 위협에 대한 감지 로직
- 애플리케이션 내 여러 리소스에 대한 감지 로직

인프라 계층 위협에 대한 감지 로직

인프라 계층 (계층 3 및 계층 4) 에서 DDoS 공격으로부터 표적 AWS 리소스를 보호하는 데 사용되는 탐지 로직은 리소스 유형과 리소스가 보호되는지 여부에 따라 달라집니다. AWS Shield Advanced

아마존 CloudFront 및 아마존 Route 53 탐지

Route CloudFront 53과 함께 웹 애플리케이션을 제공하는 경우, 완전한 인라인 DDoS 완화 시스템을 통해 애플리케이션으로 향하는 모든 패킷을 검사하므로 지연 시간이 거의 발생하지 않습니다. CloudFront 배포 및 Route 53 호스팅 영역에 대한 DDoS 공격은 실시간으로 완화됩니다. 이러한 보호는 AWS Shield Advanced사용 여부에 관계없이 적용됩니다.

DDoS 이벤트를 가장 빠르게 CloudFront 탐지하고 완화하려면 가능한 한 Route 53을 웹 애플리케이션의 진입점으로 사용하는 모범 사례를 따르세요.

탐지 대상 AWS Global Accelerator 및 지역 서비스

리소스 수준 탐지는 클래식 로드 밸런서, 애플리케이션 로드 밸런서, 엘라스틱 IP 주소 (EIP) 등 AWS 지역에서 시작되는 AWS Global Accelerator 표준 액셀러레이터 및 리소스를 보호합니다. 이러한 리소스 타입은 완화가 필요한 DDoS 공격의 존재를 나타낼 수 있는 트래픽 상승 여부를 모니터링합니다. 1분마다 각 AWS 리소스에 대한 트래픽이 평가됩니다. 리소스에 대한 트래픽이 증가하면 리소스의 용량을 측정하기 위한 추가 검사가 수행됩니다.

Shield는 다음과 같은 표준 검사를 수행합니다.

- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스, Amazon EC2 인스턴스에 연계된 EIP — Shield는 보호된 리소스에서 용량을 검색합니다. 용량은 대상의 인스턴스 타입, 인스턴스 크기 및 인스턴스가 향상된 네트워킹을 사용하는지 여부와 같은 기타 요인에 따라 달라집니다.
- Classic Load Balancer와 Application Load Balancer - Shield는 대상 로드 밸런서 노드에서 용량을 검색합니다.
- Network Load Balancer에 연계된 EIP - Shield는 대상 로드 밸런서에서 용량을 검색합니다. 용량은 대상 로드 밸런서의 그룹 구성과 무관합니다.
- AWS Global Accelerator 표준 가속기 — Shield는 엔드포인트 구성을 기반으로 용량을 검색합니다.

이러한 평가는 포트 및 프로토콜과 같은 다양한 네트워크 트래픽 차원에 걸쳐 이루어집니다. 대상 리소스의 용량이 초과되면 Shield는 DDoS 완화 조치를 취합니다. Shield가 도입한 완화 조치는 DDoS 트래픽을 감소시키지만 제거하지는 못할 수도 있습니다. Shield는 알려진 DDoS 공격 벡터와 일치하는 트래픽 차원에서 리소스 용량의 일부가 초과되는 경우에도 완화할 수 있습니다. Shield는 이 완화 조치를 TTL(Time to Live)로 설정하며, 이 기간은 공격이 진행되는 한 연장됩니다.

> **Note**
>
> Shield가 도입한 완화 조치는 DDoS 트래픽을 감소시키지만 제거하지는 못할 수도 있습니다. Shield는 애플리케이션에 유효하지 AWS Network Firewall 않거나 합법적인 최종 사용자가 생성하지 않은 트래픽을 애플리케이션이 처리하지 iptables 못하도록 하는 솔루션이나 호스트 방화벽과 같은 솔루션으로 강화할 수 있습니다.

Shield Advanced 보호 기능은 기존 Shield 감지 활동에 다음을 추가합니다.

- 더 낮은 감지 임계값 - Shield Advanced는 계산된 용량의 절반에 완화 기능을 적용합니다. 이렇게 하면 느리게 증가하는 공격을 더 빠르게 완화하고 볼륨 측정 시그니처가 더 모호한 공격을 완화할 수 있습니다.
- 간헐적 공격 보호 - Shield Advanced는 공격 빈도와 지속 시간을 기준으로 TTL(Time to Live)을 기하급수적으로 늘려 방어 체계를 구축합니다. 따라서 리소스를 자주 표적으로 삼는 경우와 짧은 시간에 공격이 발생하는 경우, 방어 조치를 더 오래 유지할 수 있습니다.
- 상태 기반 감지 - Route 53 상태 체크를 Shield Advanced의 보호 리소스와 연계하면 상태 체크의 상태가 감지 로직에 사용됩니다. 감지된 이벤트 중에 상태 체크가 정상이면 Shield Advanced는 완화 조치를 취하기 전에 해당 이벤트가 공격이라는 확신을 더 높여야 합니다. 대신 상태 체크가 정상적이지 않은 경우, Shield Advanced는 신뢰가 설정되기 전에도 완화 조치를 취할 수 있습니다. 이 기능을 사용하면 오감지를 방지하고 애플리케이션에 영향을 미치는 공격에 더 빠르게 대응할 수 있습니다. Shield Advanced의 상태 체크에 대한 자세한 설명은 상태 점검을 사용한 상태 기반 탐지을 참조하세요.

애플리케이션 계층 위협에 대한 감지 로직

AWS Shield Advanced 보호되는 Amazon CloudFront 배포 및 애플리케이션 로드 밸런서에 대한 웹 애플리케이션 계층 탐지를 제공합니다. Shield Advanced로 이러한 리소스 타입을 보호하는 경우, AWS WAF 웹 ACL을 보호 기능과 연계하여 웹 애플리케이션 계층 감지를 활성화할 수 있습니다. Shield Advanced는 관련 웹 ACL에 대한 요청 데이터를 사용하고 애플리케이션에 대한 트래픽 기준을 구축합니다. 웹 애플리케이션 계층 감지는 Shield Advanced와 AWS WAF간의 기본 통합에 근거하여 합니다.

AWS WAF 웹 ACL을 Shield Advanced 보호 리소스에 연결하는 것을 포함하여 애플리케이션 계층 보호에 대한 자세한 내용은 을 참조하십시오. AWS Shield Advanced 애플리케이션 계층 (계층 7) 보호

웹 애플리케이션 계층 감지의 경우, Shield Advanced는 애플리케이션 트래픽을 모니터링하고 이를 과거 기준선과 비교하여 이상 징후를 찾습니다. 이 모니터링은 총 볼륨과 트래픽 구성을 다룹니다. DDoS 공격 중에는 트래픽의 양과 구성이 모두 변할 것으로 예상되며, Shield Advanced는 이벤트를 선언하기 위해 두 가지 모두에 통계적으로 유의미한 편차가 있어야 합니다.

Shield Advanced는 과거 시간 창을 기준으로 측정을 수행합니다. 이 접근 방식은 트래픽 볼륨의 합법적인 변동이나 예상 패턴과 일치하는 트래픽 변화(예: 매일 같은 시간에 제공되는 판매)로 인한 오감지 알림을 줄입니다.

> **Note**
>
> Shield Advanced에 정상적이고 합법적인 트래픽 패턴을 표시하는 기준을 설정할 시간을 주어 오감지를 방지하세요. Shield Advanced는 웹 ACL을 보호된 리소스와 연결할 때 기준에 맞는 정보를 수집하기 시작합니다. 웹 트래픽에 비정상적인 패턴을 유발할 수 있는 계획된 이벤트가 발생하기 최소 24시간 전에 웹 ACL을 보호 대상 리소스와 연계하세요. Shield Advanced 웹 애플리케이션 계층 감지는 30일 동안 정상 트래픽을 관찰했을 때 가장 정확합니다.

Shield Advanced가 이벤트를 감지하는 데 걸리는 시간은 관찰되는 트래픽 양의 변화 정도에 영향을 받습니다. 볼륨 변화가 적은 경우, Shield Advanced는 이벤트가 발생하고 있다는 확신을 주기 위해 더 오랜 기간 동안 트래픽을 관찰합니다. 볼륨 변화가 많은 경우, Shield Advanced는 이벤트를 더 빠르게 감지하고 보고합니다.

웹 ACL의 속도 기반 규칙은 사용자가 추가했든 Shield Advanced 자동 애플리케이션 계층 완화 기능을 통해 추가되었든 관계없이 탐지 가능한 수준에 도달하기 전에 공격을 완화할 수 있습니다. 자동 애플리케이션 레이어 DDoS 완화에 대한 자세한 내용은 을 참조하십시오. Shield Advanced 자동 애플리케이션 계층 DDoS 완화

> **Note**
>
> 트래픽 증가나 부하 증가에 대응하여 확장되도록 애플리케이션을 설계하여 요청 플러드 규모가 작아도 영향을 받지 않도록 할 수 있습니다. Shield Advanced를 사용하면 보호된 리소스에 비용 보호가 적용됩니다. 이를 통해 DDoS 공격으로 인해 발생할 수 있는 예상치 못한 클라우드 요금 인상으로부터 보호할 수 있습니다. Shield Advanced 비용 보호에 대한 자세한 설명은 크레딧 요청 AWS Shield Advanced을 참조하세요.

애플리케이션 내 여러 리소스에 대한 감지 로직

AWS Shield Advanced 보호 그룹을 사용하여 동일한 응용 프로그램에 속하는 보호된 리소스 컬렉션을 만들 수 있습니다. 그룹에 배치할 보호 리소스를 선택하거나 동일한 타입의 모든 리소스를 하나의 그룹으로 취급하도록 지정할 수 있습니다. 예를 들어, 모든 Application Load Balancer로 구성된 그룹을 생성할 수 있습니다. 보호 그룹을 만들면 Shield Advanced 감지는 그룹 내 보호된 리소스에 대한 모든 트래픽을 집계합니다. 이는 리소스가 많고 각 리소스의 트래픽 양은 적지만 총 볼륨이 큰 경우에 유용합니다. 보호된 리소스 간에 트래픽이 전송되는 블루-그린 배포의 경우, 보호 그룹을 사용하여 애플리케이션 기준을 유지할 수도 있습니다.

다음 방법 중 하나로 보호 그룹의 트래픽을 집계하도록 선택할 수 있습니다.

- 합계 - 이 집계는 보호 그룹 내 리소스 전반의 모든 트래픽을 합산합니다. 이 집계를 사용하면 새로 만든 리소스에 기존 기준이 적용되도록 하고 감지 민감도를 낮춰 오감지를 방지할 수 있습니다.
- 평균 - 이 집계에는 보호 그룹 전체의 모든 트래픽의 평균이 사용됩니다. 로드 밸런서와 같이 리소스 간 트래픽이 균일한 애플리케이션에 이 집계를 사용할 수 있습니다.
- 최대 - 이 집계는 보호 그룹에 있는 모든 리소스 중 가장 많은 트래픽을 사용합니다. 보호 그룹에 여러 계층의 애플리케이션이 있는 경우, 이 집계를 사용할 수 있습니다. 예를 들어 CloudFront 배포, Application Load Balancer 오리진, Application Load Balancer의 Amazon EC2 인스턴스 대상을 포함하는 보호 그룹이 있을 수 있습니다.

또한 보호 그룹을 사용하여 여러 인터넷 경계 엘라스틱 IP 또는 AWS Global Accelerator 표준 액셀러레이터를 대상으로 하는 공격에 대해 Shield Advanced가 방어 조치를 적용하는 속도를 개선할 수 있습니다. 보호 그룹의 한 리소스를 대상으로 하는 경우, Shield Advanced는 그룹 내 다른 리소스에 대한 신뢰를 설정합니다. 이렇게 하면 Shield Advanced 감지에 대한 경고가 발생하여 추가 완화 조치를 만드는 데 필요한 시간을 줄일 수 있습니다.

보호 그룹에 대한 자세한 설명은 AWS Shield Advanced 보호 그룹 섹션을 참조하세요.

이벤트 AWS Shield 완화 방법

애플리케이션을 보호하는 완화 로직은 애플리케이션 아키텍처에 따라 달라질 수 있습니다. Amazon CloudFront 및 Amazon Route 53으로 웹 애플리케이션을 보호하면 웹 및 DNS 사용 사례에만 적용되고 서비스에 대한 모든 트래픽을 보호하는 완화 기능을 활용할 수 있습니다. 애플리케이션의 진입점이 AWS 지역에서 실행되는 리소스인 경우 완화 로직은 서비스, 리소스 유형 및 사용 용도에 따라 달라집니다. AWS Shield Advanced

AWS DDoS 방어 시스템은 Shield 엔지니어가 개발하며 서비스와 긴밀하게 AWS 통합됩니다. 엔지니어는 대상 리소스의 용량 및 상태와 같은 아키텍처 측면을 고려합니다. Shield 엔지니어는 DDoS 방어 시스템의 효과와 성능을 지속적으로 모니터링하며 새로운 위협이 발견되거나 예측되면 신속하게 대응할 수 있습니다.

트래픽이나 부하 증가에 대응하여 규모를 조정하도록 애플리케이션을 설계하여 요청 폭주 규모가 작아도 영향을 받지 않도록 할 수 있습니다. Shield Advanced를 사용하여 리소스를 보호하면 DDoS 공격으로 인해 발생할 수 있는 예상치 못한 클라우드 요금 증가에 대비할 수 있습니다.

인프라 완화

인프라 계층 공격의 경우 AWS 네트워크 경계와 엣지 로케이션에 AWS Shield DDoS 방어 시스템이 있습니다. AWS AWS 인프라 전체에 여러 수준의 보안 제어를 배치하면 클라우드 애플리케이션에 제공됩니다 defense-in-depth .

Shield는 인터넷의 모든 수신 지점에서 DDoS 방어 시스템을 유지 관리합니다. Shield는 DDoS 공격을 탐지하면 각 진입 지점에 대해 동일한 위치에 있는 DDoS 방어 시스템을 통해 트래픽을 다시 라우팅합니다. 이로 인해 지연 시간이 눈에 띄게 증가하지 않으며 모든 AWS 지역 및 모든 엣지 로케이션에서 TeraBits 초당 100Tbps (Tbps) 이상의 완화 용량이 제공됩니다. Shield는 트래픽을 외부 또는 원격 스크러빙 센터로 다시 라우팅하지 않고도 리소스 가용성을 보호하므로 지연 시간이 늘어날 수 있습니다.

- AWS 네트워크 경계에서 모든 AWS 서비스 또는 리소스에 대해 DDoS 방어 시스템은 인터넷에서 들어오는 인프라 계층 공격을 완화합니다. 시스템은 Shield 탐지 또는 Shield 대응 팀(SRT)의 엔지니어가 신호를 받으면 완화 조치를 수행합니다.
- AWS 엣지 CloudFront 로케이션에서 DDoS 완화 시스템은 Amazon 배포 및 Amazon Route 53 호스팅 영역으로 전달되는 모든 패킷을 출처와 상관없이 지속적으로 검사합니다. 필요한 경우 시스템은 웹 및 DNS 트래픽을 위해 특별히 설계된 완화 기능을 적용합니다. Amazon CloudFront 및 Amazon Route 53을 사용하여 웹 애플리케이션을 보호할 때 얻을 수 있는 또 다른 이점은 Shield 탐지 신호 없이도 DDoS 공격을 즉시 완화할 수 있다는 것입니다.

애플리케이션 계층 완화

Shield Advanced는 Shield Advanced CloudFront 보호를 활성화한 Amazon 배포판 및 애플리케이션 로드 밸런서를 위한 웹 애플리케이션 계층 완화 기능을 제공합니다. 보호를 활성화하면 AWS WAF 웹 ACL을 리소스에 연결하여 웹 애플리케이션 계층 탐지가 활성화됩니다. 또한 자동 애플리케이션 계층 완화를 활성화하여 Shield Advanced가 DDoS 공격 중에 보호 기능을 관리하도록 지시하는 옵션도 있습니다.

Shield는 Shield Advanced를 활성화한 리소스에 대한 애플리케이션 계층 공격에 대한 사용자 지정 완화 기능과 자동 애플리케이션 계층 완화만 제공합니다. 자동 방어 기능을 갖춘 Shield Advanced는 알려진 DDoS 소스의 요청에 대해 AWS WAF 속도 제한을 적용하고 탐지된 DDoS 공격에 대응하여 사용자 지정 AWS WAF 보호 기능을 자동으로 추가하고 관리합니다. 이러한 유형의 완화 조치에 대한 자세한 내용은 Shield Advanced가 자동 완화를 관리하는 방법 섹션을 참조하세요.

웹 ACL의 속도 기반 규칙 (사용자가 추가했든 Shield Advanced 자동 애플리케이션 계층 완화 기능을 통해 추가했든 상관없이) 은 탐지 가능한 수준에 도달하기 전에 공격을 완화할 수 있습니다. 탐지에 대한 자세한 내용은 을 참조하십시오. 애플리케이션 계층 위협에 대한 감지 로직

완화 기능

AWS Shield DDoS 완화의 주요 기능은 다음과 같습니다.

- 패킷 검증 — 이렇게 하면 검사된 모든 패킷이 예상 구조를 준수하고 해당 프로토콜에 유효한지 확인할 수 있습니다. 지원되는 프로토콜 검증에는 IP, TCP(헤더 및 옵션 포함), UDP, ICMP, DNS 및 NTP가 포함됩니다.
- 액세스 제어 목록(ACL) 및 셰이퍼 — ACL은 특정 속성을 기준으로 트래픽을 평가하여 일치하는 트래픽을 삭제하거나 셰이퍼에 매핑합니다. 셰이퍼는 대상에 도달하는 볼륨을 제한하기 위해 일치하는 트래픽의 패킷 속도를 제한하여 초과 패킷을 삭제합니다. AWS Shield 탐지 및 Shield Response Team (SRT) 엔지니어는 예상 트래픽에 전용 속도 할당을 제공하고 알려진 DDoS 공격 벡터와 일치하는 속성을 가진 트래픽에는 보다 제한적인 속도 할당을 제공할 수 있습니다. ACL이 일치시킬 수 있는 속성에는 포트, 프로토콜, TCP 플래그, 목적지 주소, 소스 국가, 패킷 페이로드의 임의 패턴 등이 있습니다.
- 의심 점수 산정 — Shield가 예상 트래픽을 파악하여 모든 패킷에 점수를 적용합니다. 알려진 정상 트래픽 패턴과 더 밀접하게 일치하는 패킷에는 더 낮은 의심 점수가 할당됩니다. 알려진 불량 트래픽 속성을 관찰하면 패킷의 의심 점수를 높일 수 있습니다. 속도 제한 패킷이 필요한 경우 Shield는 의심 점수가 높은 패킷을 먼저 삭제합니다. 이를 통해 Shield는 알려진 DDoS 공격과 제로 데이 DDoS 공격을 모두 완화하는 동시에 오탐지를 피할 수 있습니다.
- TCP SYN 프록시 — TCP SYN 쿠키를 전송하여 새 연결을 시도한 다음 보호된 서비스로 전달하도록 허용함으로써 TCP SYN flood를 방지합니다. Shield DDoS 방어 기능이 제공하는 TCP SYN 프록시는 상태 비저장 방식이므로, 알려진 최대 규모의 TCP SYN flood 공격을 상태 소진 없이 완화할 수 있습니다. 이는 클라이언트와 보호 대상 서비스 간에 지속적인 프록시를 유지하는 대신 AWS 서비스와 통합하여 연결 상태를 전달함으로써 달성됩니다. TCP SYN 프록시는 현재 아마존과 CloudFront 아마존 Route 53에서 사용할 수 있습니다.

- 속도 분산 — 이렇게 하면 보호된 리소스로 향하는 트래픽의 수신 패턴을 기반으로 위치별 셰이퍼 값이 지속적으로 조정됩니다. 이렇게 하면 네트워크에 균등하게 유입되지 않을 수 있는 고객 트래픽의 속도 제한을 방지할 수 있습니다. AWS

AWS Shield CloudFront 및 Route 53에 대한 완화 로직

Shield DDoS 완화는 Route 53의 트래픽을 지속적으로 검사합니다. CloudFront 이러한 서비스는 Shield의 DDoS 방어 기능에 대한 광범위한 액세스를 제공하고 최종 사용자에게 더 가까운 인프라에서 애플리케이션을 제공하는 전 세계에 분산된 AWS 엣지 로케이션 네트워크에서 운영됩니다.

- CloudFront— Shield DDoS 완화 기능은 웹 애플리케이션에 유효한 트래픽만 서비스로 전달하도록 허용합니다. 이를 통해 UDP 반사 공격과 같은 여러 일반적인 DDoS 벡터로부터 자동으로 보호됩니다.

  CloudFront 애플리케이션 오리진에 대한 지속적인 연결을 유지하고, Shield TCP SYN 프록시 기능과의 통합을 통해 TCP SYN 플러드를 자동으로 완화하며 엣지에서 전송 계층 보안 (TLS) 을 종료합니다. 이러한 결합 특성을 통해 애플리케이션 오리진은 올바른 형식의 웹 요청만 수신하고 하위 계층 DDoS 공격, 연결 flood 및 TLS 남용으로부터 보호됩니다.

  CloudFront DNS 트래픽 방향과 애니캐스트 라우팅을 함께 사용합니다. 이러한 기술은 소스에 가까운 공격을 완화하고, 장애를 격리하고, 알려진 최대 규모의 공격을 완화할 수 있는 용량에 대한 액세스를 보장함으로써 애플리케이션의 복원력을 개선합니다.
- Route 53 — Shield 완화 기능은 유효한 DNS 요청만 서비스에 도달하도록 허용합니다. Shield는 알려진 양호한 쿼리의 우선 순위를 지정하고 의심스럽거나 알려진 DDoS 공격 속성이 포함된 쿼리의 우선 순위를 낮추는 의심 점수를 사용하여 DNS 쿼리 flood를 완화합니다.

  Route 53은 셔플 샤딩을 사용하여 IPv4와 IPv6 모두에 대해 모든 호스팅 영역에 4개의 리졸버 IP 주소로 구성된 고유한 세트를 제공합니다. 각 IP 주소는 Route 53 위치의 다른 하위 집합에 해당합니다. 각 위치 하위 집합은 다른 하위 집합의 인프라와 부분적으로만 겹치는 신뢰할 수 있는 DNS 서버로 구성됩니다. 이렇게 하면 사용자 쿼리가 실패한 이유가 무엇이든 재시도 시 성공적으로 처리됩니다.

  Route 53은 애니캐스트 라우팅을 사용하여 네트워크 근접성을 기반으로 DNS 쿼리를 가장 가까운 엣지 로케이션에 전달합니다. 또한 애니캐스트는 DDoS 트래픽을 여러 엣지 로케이션으로 전송하여 공격이 단일 위치에 집중되는 것을 방지합니다.

Route 53은 완화 속도 외에도 전 세계에 분산된 Shield의 용량에 대한 광범위한 액세스를 제공합니다. CloudFront 이러한 기능을 활용하려면 이러한 서비스를 동적 또는 정적 웹 애플리케이션의 진입점으로 사용하십시오.

Route 53을 사용하여 웹 애플리케이션을 보호하는 방법에 대해 자세히 알아보려면 Amazon CloudFront CloudFront 및 Amazon Route 53을 사용하여 DDoS 공격으로부터 동적 웹 애플리케이션을 보호하는 방법을 참조하십시오. Route 53의 장애 격리에 대해 자세히 알아보려면 글로벌 장애 격리에 관한 사례 연구 섹션을 참조하세요.

AWS Shield 지역에 대한 AWS 완화 로직

AWS 지역에서 실행되는 리소스는 Shield 리소스 수준 탐지를 통해 설치된 AWS Shield DDoS 방어 시스템에 의해 보호됩니다. 리전 리소스에는 탄력적 IP(EIP), Classic Load Balancer, Application Load Balancer가 포함됩니다.

Shield는 완화 조치를 취하기 전에 대상 리소스와 해당 용량을 식별합니다. Shield는 용량을 사용하여 완화 기능을 통해 리소스에 전달할 수 있는 최대 총 트래픽을 결정합니다. 완화 기능에 포함된 액세스 제어 목록(ACL) 및 기타 셰이퍼를 사용하면 알려진 DDoS 공격 벡터와 일치하거나 대량으로 유입될 것으로 예상되지 않는 트래픽과 같은 일부 트래픽에 허용되는 볼륨이 감소할 수 있습니다. 이로 인해 UDP 반사 공격이나 TCP SYN 또는 FIN 플래그가 있는 TCP 트래픽에 대해 완화 방법으로 허용하는 트래픽의 양이 더욱 제한됩니다.

Shield는 용량을 결정하고 각 리소스 유형별로 완화 조치를 다르게 적용합니다.

- Amazon EC2 인스턴스 또는 Amazon EC2 인스턴스에 연결된 EIP의 경우, Shield는 인스턴스 유형 및 기타 인스턴스 속성(예: 인스턴스에 향상된 네트워킹 기능이 활성화되어 있는지 여부)을 기반으로 용량을 계산합니다.
- Application Load Balancer 또는 Classic Load Balancer의 경우, Shield는 로드 밸런서의 각 대상 노드에 대해 개별적으로 용량을 계산합니다. 이러한 리소스에 대한 DDoS 공격 완화는 Shield DDoS 완화와 로드 밸런서의 자동 규모 조정을 조합하여 제공됩니다. Shield 대응 팀(SRT)은 Application Load Balancer 또는 Classic Load Balancer 리소스에 대한 공격에 연루되면 추가 보호 조치로 규모 조정을 가속화할 수 있습니다.
- Shield는 기본 AWS 인프라의 가용 용량을 기반으로 일부 AWS 리소스의 용량을 계산합니다. 이러한 리소스 유형에는 NLB (네트워크 로드 밸런서) 및 게이트웨이 로드 밸런서를 통해 트래픽을 라우팅하는 리소스가 포함됩니다. AWS Network Firewall

> **Note**
>
> Shield Advanced로 보호되는 EIP를 연결하여 Network Load Balancer를 보호하십시오. SRT를 활용하여 기본 애플리케이션의 예상 트래픽 및 용량을 기반으로 맞춤형 완화 기능을 구축할 수 있습니다.

Shield가 완화 조치를 취하면 Shield가 완화 로직에서 정의한 초기 속도 제한이 모든 Shield DDoS 방어 시스템에 동일하게 적용됩니다. 예를 들어 Shield가 초당 100,000개의 패킷(pps) 한도로 완화 조치를 취한다면 처음에는 모든 위치에서 100,000pps를 허용할 것입니다. 그런 다음 Shield는 지속적으로 완화 지표를 집계하여 실제 트래픽 비율을 결정하고 이 비율을 사용하여 각 위치의 속도 제한을 조정합니다. 이렇게 하면 오탐지를 방지하고 완화 조치가 지나치게 관대하지 않도록 할 수 있습니다.

AWS ShieldAWS Global Accelerator 표준 가속기의 완화 로직

Shield 완화 기능은 유효한 트래픽만 Global Accelerator 표준 액셀러레이터의 리스너 엔드포인트에 도달하도록 허용합니다. 표준 액셀러레이터는 전 세계에 배포되며, 모든 지역의 AWS 리소스로 트래픽을 라우팅하는 데 사용할 수 있는 IP 주소를 제공합니다. AWS Shield가 Global Accelerator 완화 조치를 위해 적용하는 속도 제한은 표준 액셀러레이터가 트래픽을 라우팅하는 리소스의 용량을 기반으로 합니다. Shield는 총 트래픽이 결정된 속도를 초과하는 경우 및 알려진 DDoS 벡터에 대해 해당 속도의 일부가 초과되는 경우에 완화 조치를 취합니다.

표준 액셀러레이터를 구성할 때는 애플리케이션의 트래픽을 라우팅할 각 AWS 리전의 엔드포인트 그룹을 정의합니다. Shield는 완화 조치를 취하면 각 엔드포인트 그룹의 용량을 계산하고 이에 따라 각 Shield DDoS 방어 시스템의 속도 제한을 업데이트합니다. 트래픽이 인터넷에서 리소스로 라우팅되는 방식에 대한 Shield의 가정에 따라 각 위치마다 요금이 달라집니다. AWS 엔드포인트 그룹의 용량은 그룹 내 리소스 수에 그룹 내 리소스의 최소 용량을 곱한 값으로 계산됩니다. Shield는 정기적으로 애플리케이션 용량을 재계산하고 필요에 따라 속도 제한을 업데이트합니다.

> **Note**
>
> 트래픽 다이얼을 사용하여 엔드포인트 그룹으로 전달되는 트래픽의 비율을 변경해도 Shield가 속도 제한을 계산하거나 DDoS 방어 시스템에 분배하는 방식은 바뀌지 않습니다. 트래픽 다이얼을 사용하는 경우 리소스 유형 및 수량 측면에서 엔드포인트 그룹이 서로를 미러링하도록 구성하십시오. 이렇게 하면 Shield에서 계산한 용량이 애플리케이션의 트래픽을 처리하는 리소스를 대표하는지 확인할 수 있습니다.

Global Accelerator의 엔드포인트 그룹 및 트래픽 다이얼에 대한 자세한 내용은 AWS Global Accelerator 표준 액셀러레이터의 엔드포인트 그룹 섹션을 참조하세요.

AWS Shield Advanced 엘라스틱 IP에 대한 완화 로직

로 AWS Shield Advanced엘라스틱 IP (EIP) 를 보호하면 Shield Advanced는 Shield가 DDoS 이벤트 중에 적용하는 완화 기능을 강화합니다. Shield Advanced DDoS 완화 시스템은 EIP가 연결된 퍼블릭 서브넷의 네트워크 ACL(NACL) 구성을 복제합니다. 예를 들어 NACL이 모든 UDP 트래픽을 차단하도록 구성된 경우 Shield Advanced는 해당 규칙을 Shield가 적용하는 완화 기능에 병합합니다.

이 추가 기능을 사용하면 애플리케이션에 유효하지 않은 트래픽으로 인한 가용성 위험을 피할 수 있습니다. 또한 NACL을 사용하여 개별 소스 IP 주소 또는 소스 IP 주소 CIDR 범위를 차단할 수 있습니다. 이는 분산되지 않은 DDoS 공격에 대한 유용한 방어 도구가 될 수 있습니다. 또한 엔지니어의 개입 없이 자체 허용 목록을 쉽게 관리하거나 애플리케이션과 통신하지 않아야 하는 IP 주소를 차단할 수 있습니다. AWS

AWS Shield Advanced 웹 애플리케이션을 위한 완화 로직

AWS Shield Advanced 웹 애플리케이션 계층 공격을 완화하는 AWS WAF 데 사용합니다. AWS WAF Shield Advanced에 추가 비용 없이 포함되어 있습니다.

표준 애플리케이션 계층 보호

Shield Advanced로 Amazon CloudFront 배포 또는 애플리케이션 로드 밸런서를 보호하는 경우, 아직 연결되어 있지 않은 경우 Shield Advanced를 사용하여 AWS WAF 웹 ACL을 보호 리소스에 연결할 수 있습니다. 웹 ACL을 아직 구성하지 않은 경우, Shield Advanced 콘솔 마법사를 사용하여 ACL을 생성하고 속도 기반 규칙을 추가할 수 있습니다. 속도 기반 규칙은 각 IP 주소의 5분 기간당 요청 수를 제한하여 웹 애플리케이션 계층 요청 flood에 대한 기본적인 보호를 제공합니다. 최저 100부터 시작하여 속도를 구성할 수 있습니다. 자세한 정보는 Shield Advanced 애플리케이션 레이어 AWS WAF 웹 ACL 및 요금 기반 규칙을 참조하세요.

AWS WAF 서비스를 사용하여 웹 ACL을 관리할 수도 있습니다. 이를 통해 웹 ACL 구성을 확장하여 특정 웹 요청 구성 요소에 문자열 일치 또는 패턴을 검사하고 AWS WAF, 사용자 지정 요청 및 응답 처리를 추가하고, 요청 출처의 지리적 위치와 일치시키는 등의 작업을 수행할 수 있습니다. AWS WAF 규칙에 대한 자세한 내용은 을 참조하십시오. AWS WAF 규칙

자동 애플리케이션 계층 완화

보호 기능을 강화하려면 Shield Advanced 자동 애플리케이션 계층 완화를 활성화하십시오. 이 옵션을 사용하면 Shield Advanced는 알려진 DDoS 소스의 요청에 대한 AWS WAF 속도 제한 규칙을 유지하고 탐지된 DDoS 공격에 대한 사용자 지정 완화 기능을 제공합니다.

Shield Advanced가 보호된 리소스에 대한 공격을 탐지할 때, Shield Advanced는 애플리케이션으로 향하는 일반 트래픽으로부터 공격 트래픽을 분리하는 공격 시그니처를 식별하려고 시도합니다. Shield Advanced는 공격을 받고 있는 리소스뿐 아니라 동일한 웹 ACL과 연결된 다른 모든 리소스의 과거 트래픽 패턴을 기준으로 식별된 공격 시그니처를 평가합니다.

Shield Advanced는 공격 시그니처가 DDoS 공격과 관련된 트래픽만 격리한다고 판단하면 관련 웹 ACL 내의 AWS WAF 규칙에 서명을 구현합니다. Shield Advanced에 일치하는 트래픽만 계산하거나 차단하는 완화 기능을 배치하도록 지시할 수 있으며 언제든지 설정을 변경할 수 있습니다. Shield Advanced는 완화 규칙이 더 이상 필요하지 않다고 판단되면 해당 완화 규칙을 웹 ACL에서 제거합니다. 애플리케이션 계층 이벤트 완화에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화을(를) 참조하세요.

Shield Advanced 애플리케이션 계층 완화에 대한 자세한 정보는 AWS Shield Advanced 애플리케이션 계층 (계층 7) 보호을(를) 참조하세요.

DDoS에 복원력이 있는 기본 아키텍처의 예

DDoS 복원력이란 합법적인 최종 사용자에게 계속 서비스를 제공하면서 분산형 서비스 거부(DDoS) 공격을 견딜 수 있는 애플리케이션 아키텍처의 능력입니다. 복원력이 뛰어난 애플리케이션은 오류 또는 지연 시간과 같은 성능 지표에 미치는 영향을 최소화하면서 공격 중에도 계속 사용 가능한 상태로 유지될 수 있습니다. 이 섹션에서는 몇 가지 일반적인 아키텍처의 예를 보여주고 AWS 및 Shield Advanced에서 제공하는 DDoS 탐지 및 완화 기능을 사용하여 DDoS 복원력을 높이는 방법을 설명합니다.

이 섹션의 예제 아키텍처는 배포된 애플리케이션에 가장 큰 DDoS 복원력 이점을 제공하는 AWS 서비스를 강조합니다. 강조된 서비스의 이점은 다음과 같습니다.

- 전 세계에 분산된 네트워크 용량에 대한 액세스 — Amazon CloudFront 및 Amazon Route 53 서비스를 통해 AWS 글로벌 엣지 네트워크에서 인터넷 및 DDoS 완화 용량에 액세스할 수 있습니다. AWS Global Accelerator이는 테라비트에 이르는 대규모 공격을 완화하는 데 유용합니다. 어느 AWS 지역에서든 애플리케이션을 실행하고 이러한 서비스를 사용하여 합법적인 사용자를 위해 가용성을 보호하고 성능을 최적화할 수 있습니다.
- 웹 애플리케이션 계층 DDoS 공격 벡터로부터 보호 — 웹 애플리케이션 계층 DDoS 공격은 애플리케이션 규모와 웹 애플리케이션 방화벽(WAF) 조합을 통해 가장 효과적으로 완화할 수 있습니다. Shield Advanced는 웹 요청 검사 로그를 사용하여 자동으로 또는 SRT (AWS Shield Response Team) 와의 협력을 통해 완화할 수 있는 이상 현상을 탐지합니다. AWS WAF 자동 완화는 배포된 AWS WAF 속도 기반 규칙뿐만 아니라 Shield Advanced 애플리케이션 계층 DDoS 자동 완화를 통해서도 적용 가능합니다.

이러한 예를 검토하는 것 외에도, DDoS 복원력에 대한AWS 모범 사례에서 적용 가능한 모범 사례를 검토하고 따르십시오.

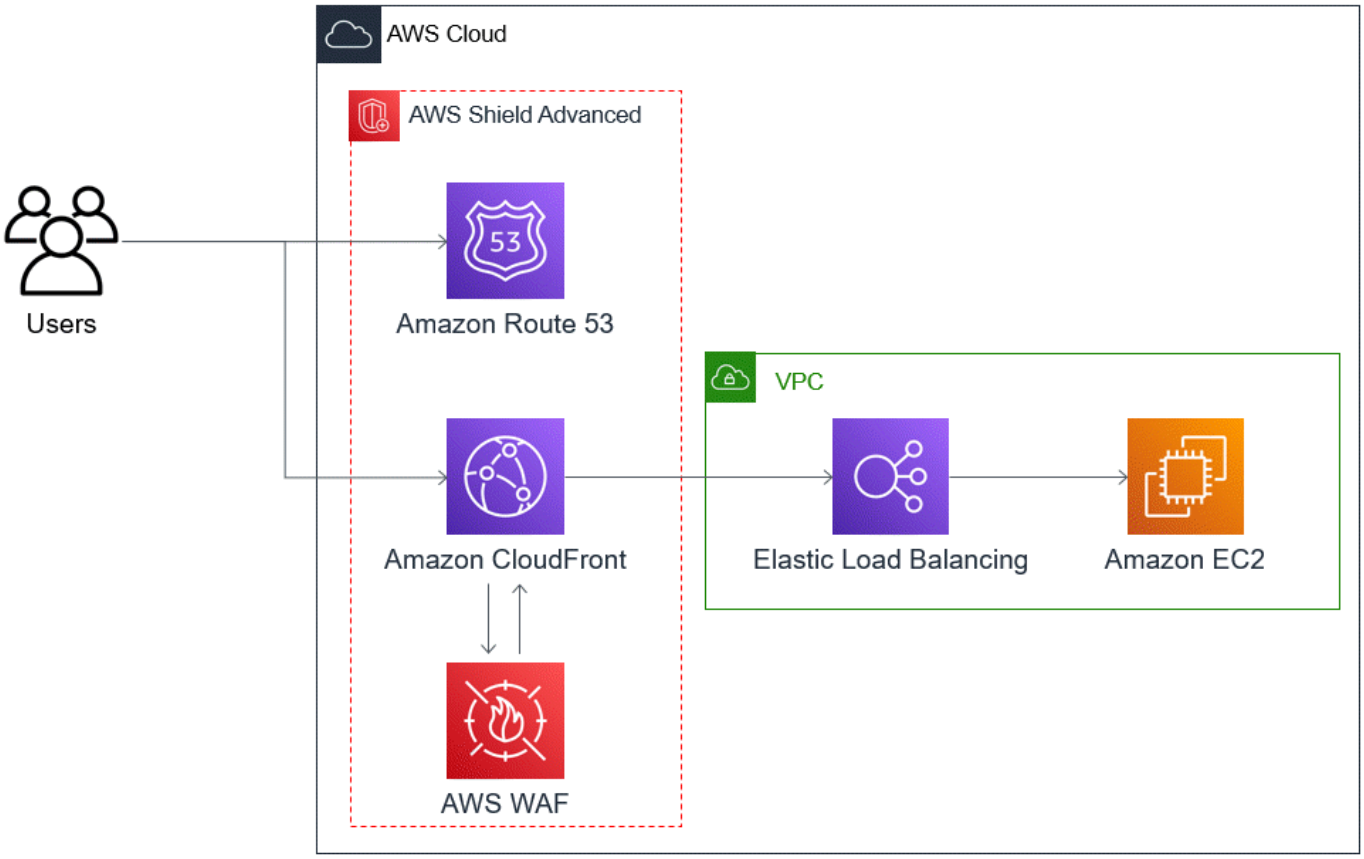
일반적인 웹 애플리케이션을 위한 DDoS 복원력 예제

어느 지역에서든 웹 애플리케이션을 구축하고 AWS 해당 지역에서 제공하는 탐지 및 완화 기능을 통해 자동 DDoS 보호를 받을 수 있습니다. AWS

이 예시는 Classic Load Balancer, Application Load Balancer, Network Load Balancer, AWS Marketplace 솔루션 또는 고객의 자체 프록시 계층과 같은 리소스를 사용하여 사용자를 웹 애플리케이션으로 라우팅하는 아키텍처를 위한 것입니다. 이러한 웹 애플리케이션 리소스와 사용자 사이에 Amazon Route 53 호스팅 영역, CloudFront Amazon 배포 AWS WAF 및 웹 ACL을 삽입하여 DDoS 복원력을 개선할 수 있습니다. 이러한 삽입으로 애플리케이션 오리진을 난독화하고, 최종 사용자에게 더 가까운 요청을 처리하고, 애플리케이션 계층 요청 폭주를 감지하고 완화할 수 있습니다. Route 53을 사용하여 CloudFront 사용자에게 정적 또는 동적 콘텐츠를 제공하는 애플리케이션은 인프라 계층 공격을 실시간으로 완화하는 통합된 완전 인라인 DDoS 완화 시스템으로 보호됩니다.

이러한 아키텍처 개선을 통해 Shield Advanced를 사용하여 Route 53 호스팅 영역과 CloudFront 배포를 보호할 수 있습니다. CloudFront 배포를 보호할 경우 Shield Advanced는 AWS WAF 웹 ACL을 연결하고 이에 대한 속도 기반 규칙을 생성하라는 메시지를 표시하고 자동 애플리케이션 계층 DDoS 완화 또는 사전 예방적 참여를 활성화할 수 있는 옵션을 제공합니다. 선제적 대응 및 자동 애플리케이션 계층 DDoS 완화는 리소스에 연결하는 Route 53 상태 확인을 사용합니다. 이러한 옵션에 대해 자세히 알아보려면 의 리소스 보호 AWS Shield Advanced(을)를 참조하세요.

다음 참조 다이어그램은 이러한 DDoS에 복원력이 있는 웹 애플리케이션용 아키텍처를 보여줍니다.



이 접근 방식이 웹 애플리케이션에 제공하는 이점은 다음과 같습니다.

- 탐지 지연 없이 자주 사용되는 인프라 계층(계층 3 및 계층 4) DDoS 공격으로부터 보호합니다. 또한 리소스가 자주 표적이 되는 경우 Shield Advanced는 완화 기능을 더 길게 적용합니다. 또한 Shield Advanced는 네트워크 ACL(NACL)에서 추론된 애플리케이션 컨텍스트를 사용하여 업스트림에서 원치 않는 트래픽을 차단합니다. 이를 통해 소스에 더 가까운 장애를 격리하여 합법적인 사용자에게 미치는 영향을 최소화합니다.
- TCP SYN flood로부터 보호합니다. Route 53과 CloudFront 통합된 DDoS 완화 시스템은 새로운 연결 시도에 도전하고 합법적인 사용자에게만 AWS Global Accelerator 서비스를 제공하는 TCP SYN 프록시 기능을 제공합니다.
- Route 53은 신뢰할 수 있는 DNS 응답을 처리하므로 DNS 애플리케이션 계층 공격으로부터 보호됩니다.
- 웹 애플리케이션 계층 요청 폭주로부터 보호합니다. AWS WAF 웹 ACL에서 구성한 속도 기반 규칙은 소스 IP가 규칙이 허용하는 것보다 더 많은 요청을 보내는 경우 소스 IP를 차단합니다.
- 이 옵션을 사용하도록 선택한 경우 CloudFront 배포에 대한 자동 애플리케이션 레이어 DDoS 완화. Shield Advanced는 자동 DDoS 완화 기능을 통해 알려진 DDoS 소스의 요청 양을 제한하는 속도 기

반 규칙을 배포의 관련 AWS WAF 웹 ACL에 유지합니다. 또한, Shield Advanced는 애플리케이션 상태에 영향을 미치는 이벤트를 탐지하면 웹 ACL에서 완화 규칙을 자동으로 생성, 테스트 및 관리합니다.

- 이 옵션을 활성화하기로 선택하는 경우, Shield 대응 팀(SRT)을 통한 선제적 대응이 적용됩니다. Shield Advanced가 애플리케이션 상태에 영향을 미치는 이벤트를 감지하면, SRT는 고객이 제공한 연락처 정보를 사용하여 이에 대응하고 고객의 보안 또는 운영 팀과 함께 사전에 대응합니다. SRT는 트래픽의 패턴을 분석하고 규칙을 업데이트하여 공격을 차단할 수 있습니다. AWS WAF

TCP 및 UDP 애플리케이션을 위한 DDoS 복원력 예제

이 예제는 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스 또는 탄력적 IP(EIP) 주소를 사용하는 AWS 리전의 TCP 및 UDP 애플리케이션을 위한 DDoS에 복원력이 있는 아키텍처를 보여줍니다.

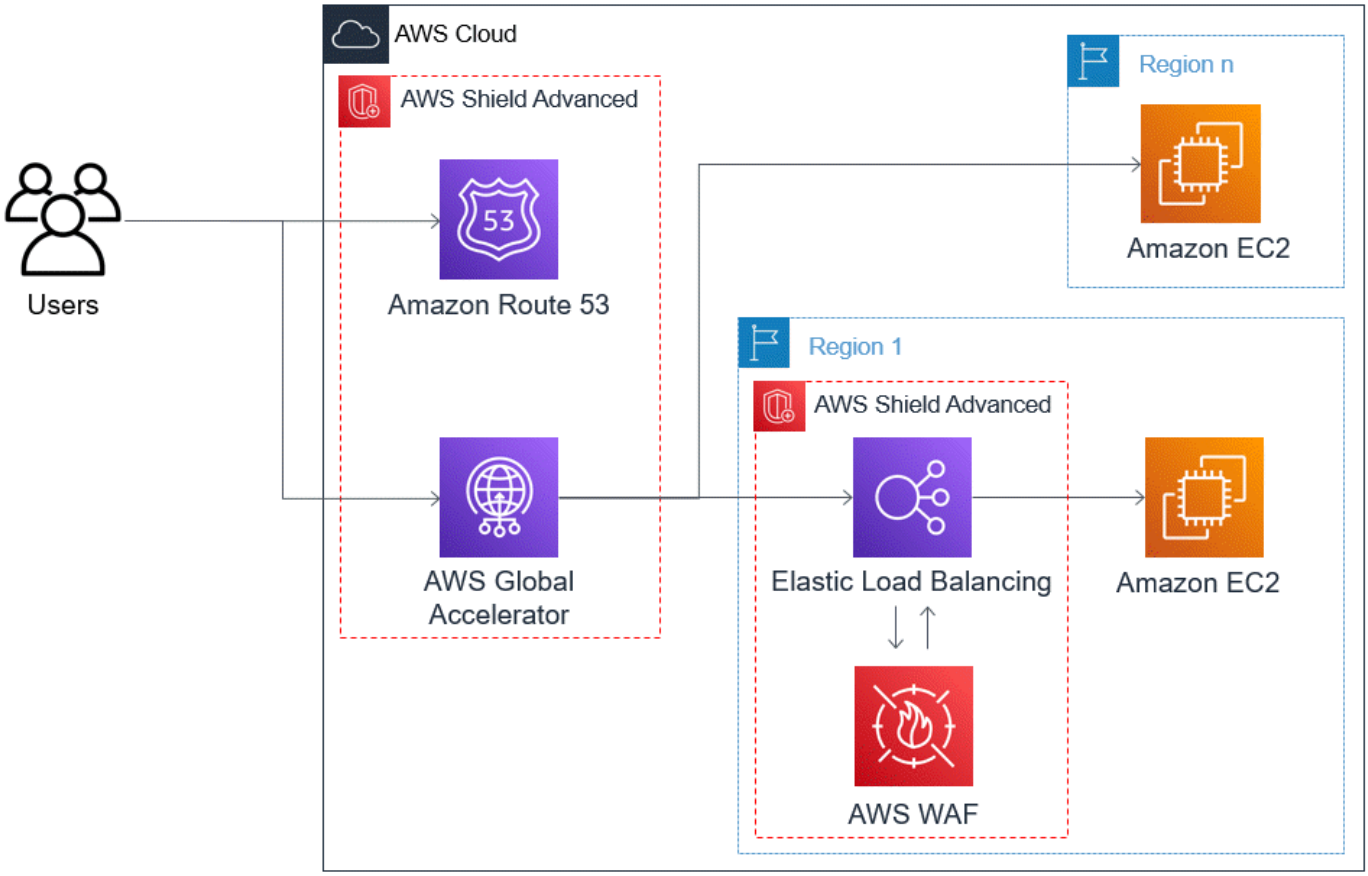
이러한 일반적인 예시를 따라 다음 애플리케이션 유형에 대한 DDoS 복원력을 개선할 수 있습니다.

- TCP 또는 UDP 애플리케이션. 게임, IoT, VoIP 등에 사용되는 애플리케이션을 예로 들 수 있습니다.
- 고정 IP 주소가 필요하거나 Amazon에서 CloudFront 지원하지 않는 프로토콜을 사용하는 웹 애플리케이션. 예를 들어 애플리케이션에는 사용자가 방화벽 허용 목록에 추가할 수 있지만 다른 AWS 고객은 사용하지 않는 IP 주소가 필요할 수 있습니다.

Amazon Route 53 및 AWS Global Accelerator을(를) 도입하여 이러한 애플리케이션 유형의 DDoS 복원력을 개선할 수 있습니다. 이러한 서비스는 사용자를 애플리케이션으로 라우팅하고 AWS 글로벌 엣지 네트워크 전체에서 애니캐스트 라우팅되는 고정 IP 주소를 애플리케이션에 제공할 수 있습니다. Global Accelerator 표준 액셀러레이터는 사용자 지연 시간을 최대 60%까지 개선할 수 있습니다. 웹 애플리케이션이 있는 경우, Application Load Balancer에서 애플리케이션을 실행한 다음 웹 ACL로 Application Load Balancer를 보호함으로써 웹 애플리케이션 계층 요청 플러드를 감지하고 완화할 수 있습니다. AWS WAF

애플리케이션을 구축한 후에는 Shield Advanced를 사용하여 Route 53 호스팅 영역, Global Accelerator 표준 액셀러레이터 및 모든 Application Load Balancer를 보호하십시오. 애플리케이션 로드 밸런서를 보호할 때 AWS WAF 웹 ACL을 연결하고 이에 대한 속도 기반 규칙을 생성할 수 있습니다. 신규 또는 기존의 Route 53 상태 확인을 연결하여 Global Accelerator 표준 액셀러레이터와 Application Load Balancer 모두에 대해 SRT를 통한 선제적 대응을 구성할 수 있습니다. 옵션에 대해 자세히 알아보려면 의 리소스 보호 AWS Shield Advanced(을)를 참조하세요.

다음 참조 다이어그램은 이러한 DDoS에 복원력이 있는 TCP 및 UDP 애플리케이션용 아키텍처 예시를 보여줍니다.



이 접근 방식이 애플리케이션에 제공하는 이점은 다음과 같습니다.

- 알려진 최대 규모의 인프라 계층(계층 3 및 계층 4) DDoS 공격으로부터 보호합니다. 공격의 볼륨으로 인해 업스트림에서 AWS혼잡이 발생하는 경우 장애가 소스에 더 가깝게 격리되어 합법적인 사용자에게 미치는 영향을 최소화합니다.
- Route 53은 신뢰할 수 있는 DNS 응답을 처리하므로 DNS 애플리케이션 계층 공격으로부터 보호됩니다.
- 웹 애플리케이션을 사용하는 경우, 이 접근 방식을 통해 웹 애플리케이션 계층 요청 폭주를 방지할 수 있습니다. AWS WAF 웹 ACL에서 구성한 속도 기반 규칙은 소스 IP를 차단하지만 소스 IP는 규칙이 허용하는 것보다 더 많은 요청을 전송합니다.
- 적합한 리소스에 대해 이 옵션을 활성화하기로 선택하는 경우의 Shield 대응 팀(SRT)을 통한 선제적 대응. Shield Advanced가 애플리케이션 상태에 영향을 미치는 이벤트를 감지하면, SRT는 고객이 제공한 연락처 정보를 사용하여 이에 대응하고 고객의 보안 또는 운영 팀과 함께 사전에 대응합니다.

Shield Advanced 사용 사례 예시

Shield Advanced를 사용하여 여러 타입의 시나리오에서 리소스를 보호할 수 있습니다. 그러나 일부 경우에는 보호 기능을 향상시키기 위해 다른 서비스를 사용하거나 다른 서비스를 Shield Advanced와 결합해야 합니다. 다음은 Shield Advanced 또는 기타 AWS 서비스를 사용하여 리소스를 보호하는 방법의 예입니다.

목표	제안된 서비스	관련 서비스 설명서
DDoS 공격에 대해 웹 애플리케이션 및 RESTful API 보호	아마존 CloudFront 배포판 및 애플리케이션 로드 밸런서를 보호하는 Shield Advanced	Elastic Load Balancing 설명서, 아마존 CloudFront 설명서
DDoS 공격에 대해 TCP 기반 애플리케이션 보호	AWS Global Accelerator 표준 액셀러레이터를 보호하는 Shield Advanced로 엘라스틱 IP 주소에 연결	AWS Global Accelerator 설명서, Elastic Load Balancing 설명서
DDoS 공격에 대해 UDP 기반 게임 서버 보호	탄력적 IP 주소에 연계된 Amazon EC2 인스턴스를 보호하는 Shield Advanced	Amazon Elastic Compute Cloud 설명서

예컨대, Shield Advanced를 사용하여 탄력적 IP 주소를 보호하는 경우, Shield Advanced는 이와 관련된 모든 리소스를 보호합니다. 공격 중에 Shield Advanced는 네트워크 ACL을 네트워크 경계에 자동으로 배포합니다 AWS . 네트워크 ACL이 네트워크의 경계에 있는 경우, Shield Advanced에서는 더 큰 DDoS 이벤트에 대한 보호를 제공할 수 있습니다. 일반적으로 네트워크 ACL은 Amazon VPC 내에서 근접한 Amazon EC2 인스턴스에 적용됩니다. 네트워크 ACL은 Amazon VPC와 인스턴스가 처리할 수 있을 정도의 큰 공격만 완화할 수 있습니다. Amazon EC2 인스턴스에 연계된 네트워크 인터페이스가 최대 10Gbps를 처리할 수 있는 경우, 10Gbps를 초과하는 볼륨은 느려지며 해당 인스턴스에 대한 트래픽이 차단될 수 있습니다. 공격 시에 Shield Advanced는 네트워크 ACL을 AWS 경계로 승격시켜 다수 테라바이트의 트래픽을 처리할 수 있습니다. 네트워크 ACL은 네트워크의 일반적인 용량 이상으로 리소스에 대한 보호를 제공할 수 있습니다. 네트워크 ACL에 대한 자세한 설명은 네트워크 ACL을 참조하세요.

시작하기 AWS Shield Advanced

이 튜토리얼은 Shield Advanced 콘솔 AWS Shield Advanced 사용을 시작하는 방법을 안내합니다.

> **Note**
>
> Shield Advanced는 구독이 필요하지만 AWS Shield Standard 구독은 필요하지 않습니다. Shield Standard에서 제공하는 보호는 모든 AWS 고객에게 무료로 제공됩니다.

Shield Advanced는 네트워크 계층(계층 3), 전송 계층(계층 4) 및 애플리케이션 계층(계층 7) 공격에 대한 첨단 DDoS 감지 및 완화 보호를 제공합니다. Shield Advanced에 대한 자세한 설명은 AWS Shield Advanced 개요 섹션을 참조하세요.

AWS 기술 커뮤니티는 IaC (코드형 인프라) 도구 AWS CloudFormation 및 Terraform을 사용하여 Shield Advanced를 구성하는 자동화된 프로세스의 예를 게시했습니다. 계정이 조직의 일부이고 Amazon Route 53 또는 이외의 모든 리소스 유형을 보호하는 경우 이 AWS Organizations 솔루션과 AWS Firewall Manager 함께 사용할 수 AWS Global Accelerator있습니다. 이 옵션을 살펴보려면 aws-samples/ aws-shield-advanced-one-click-Deployment의 코드 리포지토리와 Shield Advanced의 원클릭 배포에 있는 자습서를 참조하십시오.

> **Note**
>
> 분산 서비스 거부(DDoS) 이벤트가 발생하기 전에 Shield Advanced를 완전히 구성하는 것이 중요합니다. 구성을 완료하여 애플리케이션이 보호되고 애플리케이션이 DDoS 공격의 영향을 받는 경우, 대응할 준비가 되었는지 확인하십시오.

Shield Advanced를 사용하려면 다음 단계를 순서대로 수행하십시오.

목차

구독하기 AWS Shield Advanced

보호하려는 각 AWS 계정 항목에 대해 Shield Advanced에 가입해야 합니다. Shield Standard는 구독할 필요가 없습니다.

Shield Advanced 구독 결제

AWS 채널 리셀러인 경우 계정 팀에 문의하여 정보와 지침을 얻으세요. 이 청구 정보는 AWS 채널 리셀러가 아닌 고객을 위한 것입니다.

그 외의 모든 경우에는 다음과 같은 가입 및 결제 지침이 적용됩니다.

- AWS Organizations 조직 구성원 계정의 경우 지급인 계정 자체가 구독되어 있는지 여부와 상관없이 Shield Advanced 구독을 조직의 지불자 계정에 대해 AWS 청구합니다.
- 동일한 AWS Organizations 통합 결제 계정 패밀리에 속하는 여러 계정에 가입하는 경우, 하나의 가입 요금이 패밀리 내 모든 가입 계정에 적용됩니다. 조직은 모든 AWS 계정 와(과) 모든 리소스를 소유해야 합니다.
- 여러 조직의 여러 계정에 가입하는 경우에도 모든 조직, 계정, 리소스를 소유하고 있다면 모든 조직, 계정, 리소스에 대해 하나의 가입 요금을 지불할 수 있습니다. 계정 관리자 또는 AWS 지원팀에 문의하여 한 조직을 제외한 모든 조직의 AWS Shield Advanced 구독 요금에 대한 수수료 면제를 요청하세요.

자세한 요금 정보 및 예는 AWS Shield 요금 섹션을 참조하세요.

다음을 통해 구독을 간소화하십시오. AWS Firewall Manager

계정이 조직의 일부인 경우, 가능하면 AWS Firewall Manager 를 사용하여 조직에 대한 가입 및 보호를 자동화하는 것이 좋습니다. Firewall Manager는 Amazon Route 53 및 AWS Global Accelerator을 제외한 모든 보호 리소스 타입을 지원합니다. Firewall Manager를 사용하려면 AWS Firewall Manager 및 AWS Firewall ManagerAWS Shield Advanced 정책 시작하기을 참조하세요.

Firewall Manager를 사용하지 않는 경우, 보호할 리소스가 있는 각 계정에 대해 다음 절차를 사용하여 가입하고 보호 기능을 추가하십시오.

계정을 구독하려면 AWS Shield Advanced

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 모음에서 시작하기를 선택합니다. Shield Advanced 가입을 선택합니다.

3. Shield Advanced 가입 페이지에서 각 계약 약관을 읽은 후 모든 확인란을 선택하여 약관에 동의함을 나타냅니다. 통합 결제 패밀리에 속하는 계정의 경우, 각 계정의 약관에 동의해야 합니다.

   > **Important**
   >
   > 가입한 경우, 가입을 해지하려면 AWS Support에 문의해야 합니다.
   > 구독에 대한 자동 갱신을 비활성화하려면 Shield API 작업 UpdateSubscription또는 CLI 명령 업데이트 구독을 사용해야 합니다.

   Shield Advanced 가입을 선택합니다. 이렇게 하면 Shield Advanced에 계정에 가입하고 서비스가 활성화됩니다.

계정이 가입되었습니다. Shield Advanced로 계정의 리소스를 보호하려면 다음 단계를 계속 진행하세요.

> **Note**
>
> Shield Advanced는 가입 후 리소스를 자동으로 보호하지 않습니다. Shield Advanced에서 보호할 리소스를 지정하여 보호를 구성해야 합니다.

보호할 리소스 추가 및 보호 구성

Shield Advanced는 Shield Advanced를 통해 또는 Firewall Manager Shield Advanced 정책에서 지정한 리소스만 보호합니다. 가입한 계정의 리소스를 자동으로 보호하지는 않습니다.

보호를 위해 AWS Firewall Manager Shield Advanced 정책을 사용하는 경우 이 단계를 수행할 필요가 없습니다. 보호할 리소스 타입으로 정책을 구성하면 Firewall Manager가 정책 범위 내에 있는 리소스에 자동으로 보호를 추가합니다.

Firewall Manager를 사용하지 않는 경우, 보호할 리소스가 있는 각 계정에 대해 다음 절차를 진행합니다.

Shield Advanced를 사용하여 보호할 리소스를 선택하려면

1. 이전 절차의 가입 확인 페이지나 보호된 리소스 또는 개요 페이지에서 보호할 리소스 추가를 선택합니다.

2. Shield Advanced로 보호할 리소스 선택 페이지의 지역 및 리소스 타입 지정에서 보호하려는 리소스에 대해 지역 및 리소스 타입 사양을 제공합니다. 모든 지역을 선택하여 여러 지역의 리소스를 보호할 수 있으며, 글로벌을 선택하여 글로벌 리소스로 선택 범위를 좁힐 수 있습니다. 보호하지 않으려는 모든 리소스 타입을 선택 취소할 수 있습니다. 리소스 타입의 보호에 대한 자세한 설명은 AWS Shield Advanced 리소스 유형별 보호을 참조하세요.
3. 리소스 로딩을 선택합니다. Shield Advanced는 리소스 선택 섹션을 기준에 맞는 AWS 리소스로 채웁니다.
4. 리소스 선택 섹션에서, 리소스 목록에서 검색할 문자열을 입력하여 리소스 목록을 필터링할 수 있습니다.

   보호할 리소스를 선택합니다.
5. 태그 섹션에서 생성 중인 Shield Advanced 보호에 태그를 추가하려면 해당 태그를 지정하세요. AWS 리소스 태그 지정에 대한 자세한 설명은 태그 편집기 작업을 참조하세요.
6. Shield Advanced로 보호하기를 선택하세요. 이렇게 하면 리소스에 Shield Advanced 보호 기능이 추가됩니다.

콘솔 마법사 화면을 계속 진행하여 리소스 보호 구성을 완료하세요.

주제

- 다음을 사용하여 애플리케이션 계층 (계층 7) DDoS 보호를 구성합니다. AWS WAF
- 보호를 위한 상태 기반 감지 구성
- 경보 및 알림 구성
- 보호 구성 검토 및 완료

다음을 사용하여 애플리케이션 계층 (계층 7) DDoS 보호를 구성합니다. AWS WAF

애플리케이션 계층 리소스를 보호하기 위해 Shield Advanced는 속도 기반 규칙이 있는 AWS WAF 웹 ACL을 출발점으로 사용합니다. AWS WAF 애플리케이션 계층 리소스에 전달되는 HTTP 및 HTTPS 요청을 모니터링하고 요청의 특성에 따라 콘텐츠에 대한 액세스를 제어할 수 있게 해주는 웹 애플리케이션 방화벽입니다. 속도 기반 규칙은 요청 집계 기준에 따라 트래픽 양을 제한하여 애플리케이션에 기본적인 DDoS 보호를 제공합니다. 자세한 내용은 AWS WAF 작동 방식 및 비율 기반 규칙 문 섹션을 참조하세요.

또한 Shield Advanced의 자동 애플리케이션 계층 DDoS 완화를 활성화하여 Shield Advanced에서 알려진 DDoS 소스로부터의 제한 요청을 평가하고 자동으로 인시던트별 보호를 제공하도록 할 수도 있습니다.

> **Important**
>
> Shield Advanced 정책을 AWS Firewall Manager 사용하여 Shield Advanced 보호를 관리하는 경우 여기에서 애플리케이션 계층 보호를 관리할 수 없습니다. Firewall Manager Shield Advanced 정책에서 관리해야 합니다.

쉴드 어드밴스드 구독 및 비용 AWS WAF

Shield Advanced를 구독하면 Shield Advanced로 보호하는 리소스의 표준 AWS WAF 기능을 사용하는 데 드는 비용이 포함됩니다. Shield Advanced 보호가 적용되는 표준 AWS WAF 요금은 웹 ACL당 비용, 규칙당 비용, 웹 요청 검사 요청 1백만 건당 기본 가격 (최대 1,500WCU 및 최대 기본 본체 크기) 입니다.

Shield Advanced 자동 애플리케이션 레이어 DDoS 완화를 활성화하면 150개의 웹 ACL 용량 단위 (WCU) 를 사용하는 규칙 그룹이 웹 ACL에 추가됩니다. 이러한 WCU는 웹 ACL의 WCU 사용량에 포함됩니다. 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화, Shield Advanced 규칙 그룹, AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

Shield Advanced를 구독해도 Shield Advanced를 사용하여 보호하지 않는 리소스에 AWS WAF 대한 사용은 포함되지 않습니다. 또한 보호 대상 리소스에 대한 추가 비표준 AWS WAF 비용도 포함되지 않습니다. 비표준 AWS WAF 비용의 예로는 Bot Control, CAPTCHA 규칙 작업, 1,500개 이상의 WCU를 사용하는 웹 ACL, 기본 본문 크기를 초과하여 요청 본문을 검사하는 비용 등이 있습니다. 전체 목록은 요금 페이지에 나와 있습니다. AWS WAF

전체 정보 및 요금 예는 Shield 요금 및 AWS WAF 요금을 참조하세요.

지역에 대한 계층 7 DDoS 보호를 구성하려면

Shield Advanced는 선택한 리소스가 위치한 각 지역에 대해 계층 7 DDoS 완화를 구성할 수 있는 옵션을 제공합니다. 여러 지역에 보호 기능을 추가하는 경우, 마법사가 각 지역에 대해 다음 절차를 안내합니다.

1. 계층 7 DDoS 보호 구성 페이지에는 아직 웹 ACL과 연계되지 않은 각 리소스가 열거됩니다. 이들 각각에 대해 기존 웹 ACL을 선택하거나 새 웹 ACL을 생성하십시오. 이미 연결된 웹 ACL이 있는 리소스의 경우 먼저 현재 ACL의 연결을 해제하여 웹 ACL을 변경할 수 있습니다. AWS WAF자세한 정보는 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.

   아직 요금 기반 규칙이 없는 웹 ACL의 경우, 구성 마법사가 속도 기반 규칙을 추가하라는 메시지를 표시합니다. 속도 기반 규칙은 많은 양의 요청을 보내는 IP 주소의 트래픽을 제한합니다. 속도

기반 규칙은 웹 요청 플러드로부터 애플리케이션을 보호하는 데 도움이 되며, 잠재적인 DDoS 공격으로 이어질 수 있는 갑작스러운 트래픽 급증에 대한 알림을 제공할 수 있습니다. 속도 제한 규칙 추가를 선택한 다음 속도 제한 및 규칙 조치를 제공하여 속도 기반 규칙을 웹 ACL에 추가합니다. 를 통해 웹 ACL에서 추가 보호를 구성할 수 있습니다. AWS WAF

속도 기반 규칙의 추가 구성 옵션을 포함하여 Shield Advanced 보호에서 웹 ACL 및 속도 기반 규칙을 사용하는 방법에 대한 자세한 설명은 Shield Advanced 애플리케이션 레이어 AWS WAF 웹 ACL 및 요금 기반 규칙을 참조하세요.

2. 자동 애플리케이션 계층 DDoS 완화의 경우 Shield Advanced가 애플리케이션 계층 리소스에 대한 DDoS 공격을 자동으로 완화하도록 하려면 활성화를 선택한 다음 Shield Advanced가 사용자 지정 규칙에서 사용할 AWS WAF 규칙 작업을 선택합니다. 이 설정은 이 마법사 세션에서 관리하는 리소스의 모든 웹 ACL에 적용됩니다.

   Shield Advanced는 자동 애플리케이션 레이어 DDoS 완화 기능을 통해 알려진 DDoS 소스의 요청 양을 제한하는 속도 기반 규칙을 리소스의 AWS WAF 웹 ACL에 유지합니다. 또한, Shield Advanced는 현재 트래픽 패턴을 과거 트래픽 베이스라인과 비교하여 DDoS 공격을 표시할 수 있는 편차를 감지합니다. Shield Advanced는 DDoS 공격을 탐지하면 이에 대응하기 위한 사용자 지정 AWS WAF 규칙을 생성, 평가 및 배포하여 대응합니다. 맞춤 규칙이 사용자 대신 공격을 계수 또는 차단할지를 지정합니다.

   > **Note**
   >
   > 자동 애플리케이션 레이어 DDoS 완화는 최신 버전 (v2) 을 사용하여 만든 웹 ACL에서만 작동합니다. AWS WAF

   이 기능 사용에 대한 주의 사항 및 모범 사례를 포함하여 Shield Advanced 자동 애플리케이션 계층 DDoS 완화에 대한 자세한 내용은 을 참조하십시오. Shield Advanced 자동 애플리케이션 계층 DDoS 완화

3. 다음을 선택합니다. 콘솔 마법사는 상태 기반 감지 페이지로 이동합니다.

보호를 위한 상태 기반 감지 구성

상태 기반 탐지를 사용하여 공격 탐지 및 완화의 대응력과 정확성을 개선하도록 Shield Advanced를 구성하십시오. 이벤트를 정확하게 탐지하려면 잘 구성된 상태 점검이 필수적입니다. Route 53 호스팅 영역을 제외한 모든 리소스 유형에 대해 상태 기반 탐지를 구성할 수 있습니다.

상태 기반 탐지를 사용하려면 Route 53에서 리소스의 상태 확인을 정의한 다음 상태 확인을 Shield Advanced 보호와 연결합니다. 구성한 상태 체크가 리소스의 상태를 정확하게 반영하는 것이 중요합니다. Shield Advanced와 함께 사용할 상태 체크를 구성하는 방법에 대한 자세한 내용 및 예는 상태 점검을 사용한 상태 기반 탐지을 참조하세요.

Shield 대응팀(SRT)의 전향적 연계 지원을 위해서는 상태 체크가 필요합니다. 전향적 연계에 대한 자세한 설명은 선제적 대응 구성을 참조하세요.

> **Note**
>
> 상태 체크를 Shield Advanced 보호 기능과 연계할 때는 상태 체크가 건전 상태를 보고해야 합니다.

상태 기반 감지를 구성하려면

1. 연계된 상태 체크에서 보호와 연계하려는 상태 체크의 ID를 선택합니다.

   > **Note**
   >
   > 필요한 상태 체크가 보이지 않으면 Route 53 콘솔로 이동하여 상태 체크와 해당 ID를 확인하십시오. 자세한 설명은 상태 확인 생성 및 업데이트를 참조하세요.

2. 다음을 선택합니다. 콘솔 마법사가 경보 및 알림 페이지로 이동합니다.

경보 및 알림 구성

감지된 Amazon CloudWatch 경보 및 속도 기반 규칙 활동에 대한 Amazon 단순 알림 서비스 알림을 선택적으로 구성할 수 있습니다. 이를 사용하여 Shield가 보호된 리소스에서 이벤트를 감지하거나 속도 기반 규칙에 구성된 속도 제한이 초과될 때 알림을 받을 수 있습니다.

Shield Advanced CloudWatch 지표에 대한 자세한 내용은 을 참조하십시오AWS Shield Advanced 측정 항목. Amazon SNS에 대한 자세한 설명은 Amazon Simple Notification Service 개발자 가이드를 참조하세요.

경보 및 알림을 구성하려면

1. 알림을 받을 Amazon SNS 주제를 선택합니다. 모든 보호된 리소스 및 속도 기반 규칙에 대해 단일 Amazon SNS 주제를 사용하거나 조직에 맞게 맞춤된 다른 주제를 선택할 수 있습니다. 예를 들어, 특정 리소스 집합에 대한 인시던트 대응을 담당하는 각 팀을 위한 SNS 주제를 만들 수 있습니다.
2. 다음을 선택합니다. 콘솔 마법사는 리소스 보호 검토 페이지로 이동합니다.

보호 구성 검토 및 완료

설정을 검토 및 구성하려면

1. DDoS 완화 및 가시성 검토 및 구성 페이지에서 설정을 검토하십시오. 수정하려면 수정하려는 영역에서 편집을 선택합니다. 그러면 콘솔 마법사의 관련 페이지로 돌아갑니다. 변경한 후 DDoS 완화 및 가시성 검토 및 구성 페이지로 돌아갈 때까지 이후 페이지에서 다음을 선택합니다.
2. 구성 완료를 선택합니다. 보호된 리소스 페이지에는 새로 보호되는 리소스가 열거됩니다.

AWS SRT 지원 구성

Shield 대응팀(SRT)은 DDoS 이벤트 대응을 전문으로 하는 보안 엔지니어입니다. DDoS 이벤트 중에 SRT가 사용자를 대신하여 리소스를 관리할 수 있는 권한을 선택적으로 추가할 수 있습니다. 또한, 감지된 이벤트 중에 보호된 리소스와 관련된 Route 53 상태 체크가 비정상인 경우, 사전에 조치를 취하도록 SRT를 구성할 수 있습니다. 보호 기능에 이러한 두 가지 기능을 추가하면 DDoS 이벤트에 더 빠르게 대응할 수 있습니다.

> **Note**
>
> Shield 대응팀(SRT)의 서비스를 이용하려면 Business Support 플랜 또는 Enterprise Support 플랜에 가입해야 합니다.

SRT는 애플리케이션 계층 이벤트 중에 AWS WAF 요청 데이터와 로그를 모니터링하여 비정상적인 트래픽을 식별할 수 있습니다. 이를 통해 사용자 지정 AWS WAF 규칙을 만들어 문제가 되는 트래픽 소스를 완화할 수 있습니다. 필요에 따라 SRT는 리소스를 권장 사항에 더 잘 맞추는 데 도움이 되는 아키텍처 권장 사항을 제시할 수 있습니다. AWS

SRT에 대한 자세한 내용은 Shield 대응 팀(SRT) 지원(을)를 참조하세요.

SRT에 권한을 부여하려면

1. AWS Shield 콘솔 개요 페이지의 AWS SRT 지원 구성에서 SRT 액세스 편집을 선택합니다. 에디트 AWS 쉴드 대응팀 (SRT) 액세스 페이지가 열립니다.
2. SRT 액세스 설정의 경우, 다음 옵션 중 하나를 선택합니다.

   - SRT에 내 계정에 대한 액세스 권한을 부여하지 않음 - Shield는 이전에 SRT에 부여한 계정 및 리소스 액세스 권한을 제거합니다.
   - SRT가 내 계정에 액세스할 수 있도록 새 역할 만들기 - Shield는 SRT를 대표하는 서비스 주체 `drt.shield.amazonaws.com`를 신뢰하는 역할을 생성하고 여기에 관리형 정책 `AWSShieldDRTAccessPolicy`를 연결합니다. 관리형 정책을 통해 SRT는 사용자를 대신하여 AWS WAF API를 AWS Shield Advanced 호출하고 로그에 액세스할 수 있습니다 AWS WAF . 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책: AWSShieldDRTAccessPolicy섹션을 참조하세요.
   - SRT가 내 계정에 액세스할 수 있는 기존 역할 선택 — 이 옵션을 사용하려면 AWS Identity and Access Management (IAM) 의 역할 구성을 다음과 같이 수정해야 합니다.
     - 관리형 정책 `AWSShieldDRTAccessPolicy`를 역할에 연계하십시오. 이 관리형 정책을 통해 SRT는 사용자를 대신하여 AWS WAF API를 AWS Shield Advanced 호출하고 로그에 액세스할 수 있습니다. AWS WAF 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책: AWSShieldDRTAccessPolicy(을)를 참조하세요. 관리형 정책을 역할에 연계하는 방법에 대한 자세한 설명은 IAM 정책 연계 및 분리를 참조하세요.
     - 서비스 담당자 `drt.shield.amazonaws.com`을 신뢰하도록 역할을 수정합니다. 이는 SRT를 대표하는 서비스 담당자입니다. 자세한 설명은 IAM JSON 정책 요소: 담당자를 참조하세요.
3. 저장을 선택하여 변경 사항을 저장합니다.

SRT에 보호 및 데이터에 대한 액세스 권한을 부여하는 방법에 대한 자세한 설명은 Shield 대응 팀 (SRT) 액세스 권한 구성을 참조하세요.

SRT 전향적 연계를 활성화하려면

1. AWS Shield 콘솔 개요 페이지의 사전 참여 및 연락처 아래의 연락처 영역에서 편집을 선택합니다.

   연락처 편집 페이지에서 SRT가 전향적 연계를 위해 연락할 담당자의 연락처 정보를 입력합니다.

   둘 이상의 연락처를 제공하는 경우, 주에 각 연락처를 사용해야 하는 경우를 표시하십시오. 기본 및 보조 연락처 지정을 포함하고 각 연락처의 이용 가능 시간과 시간대를 제공하십시오.

연락처 메모 예시:

- 이 핫라인은 연중무휴 24시간 운영됩니다. 담당 분석가에게 문의하면 적절한 담당자를 통화 중에 연결해 드립니다.
- 5분 이내에 핫라인이 응답하지 않으면 저에게 연락하십시오.

2. 저장을 선택합니다.

   개요 페이지에는 업데이트된 연락처 정보가 반영됩니다.

3. 전향적 연계 기능 편집을 선택하고 활성화를 선택한 다음 저장을 선택하여 전향적 연계를 활성화합니다.

전향적 연계에 대한 자세한 설명은 선제적 대응 구성을 참조하세요.

에서 DDoS 대시보드 생성 CloudWatch 및 알람 설정 CloudWatch

Shield Advanced에서 원시 데이터를 수집하여 읽을 수 있는 거의 실시간 지표로 처리하는 CloudWatch Amazon을 사용하여 잠재적 DDoS 활동을 모니터링할 수 있습니다. 에서 CloudWatch 통계를 사용하여 웹 애플리케이션 또는 서비스 성능에 대한 관점을 얻을 수 있습니다. 사용에 CloudWatch 대한 자세한 내용은 Amazon 사용 CloudWatch 설명서의 내용을 참조하십시오. CloudWatch

- CloudWatch 대시보드 생성 지침은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.
- 대시보드에 추가할 수 있는 Shield Advanced 지표에 대한 설명은 AWS Shield Advanced 측정 항목 섹션을 참조하세요.

Shield Advanced는 진행 중인 이벤트가 없을 때보다 DDoS 이벤트가 발생하는 동안 CloudWatch 더 자주 리소스 지표를 보고합니다. Shield Advanced는 이벤트 중에는 1분에 한 번, 그리고 이벤트 종료 직후에 한 번 지표를 보고합니다. 진행 중인 이벤트가 없을 때 Shield Advanced는 지표를 하루에 한 번 리소스에 지정된 시간에 보고합니다. 이 정기 보고서는 지표를 활성 상태로 유지하여 사용자 지정 알람에 사용할 수 있도록 합니다. CloudWatch

이것으로 Shield Advanced 시작하기를 위한 자습서를 마칩니다. 선택한 보호 기능을 최대한 활용하려면 Shield Advanced의 기능 및 옵션을 계속 살펴보세요. 먼저, DDoS 이벤트에 대한 가시성 및 DDoS 이벤트에 대한 대응에서 이벤트를 보고 응답할 수 있는 옵션을 숙지하세요.

Shield 대응 팀(SRT) 지원

Shield 대응 팀(SRT)은 Shield Advanced 고객에게 추가 지원을 제공합니다. SRT는 DDoS 이벤트 대응을 전문으로 하는 보안 엔지니어입니다. AWS Support 계획에 대한 추가 지원 계층으로 SRT와 직접 협력하여 SRT의 전문 지식을 이벤트 대응 워크플로의 일부로 활용할 수 있습니다. 옵션 및 구성 지침에 대한 자세한 내용은 이어지는 항목을 참조하세요.

> **Note**
>
> Shield 대응팀(SRT)의 서비스를 이용하려면 Business Support 플랜 또는 Enterprise Support 플랜에 가입해야 합니다.

SRT 지원 활동

SRT와 관련된 대응의 주요 목표는 애플리케이션의 가용성과 성능을 보호하는 것입니다. DDoS 이벤트의 유형과 애플리케이션의 아키텍처에 따라 SRT는 다음 중 하나 이상의 조치를 수행할 수 있습니다.

- AWS WAF 로그 분석 및 규칙 - AWS WAF 웹 ACL을 사용하는 리소스의 경우 SRT는 AWS WAF 로그를 분석하여 애플리케이션 웹 요청의 공격 특성을 식별할 수 있습니다. 대응 기간 동안 고객의 승인을 받으면, SRT는 웹 ACL 변경 사항을 적용하여 식별된 공격을 차단할 수 있습니다.
- 맞춤형 네트워크 완화 장치 구축 — SRT는 인프라 계층 공격에 대비하여 고객을 대신하여 사용자 지정 완화 조치를 작성할 수 있습니다. SRT는 고객과 협력하여 애플리케이션에 예상되는 트래픽을 파악하고, 예상치 못한 트래픽을 차단하고, 초당 패킷 전송 속도 제한을 최적화할 수 있습니다. 자세한 정보는 Shield 대응 팀(SRT)을 통한 사용자 지정 완화 구성을 참조하세요.
- 네트워크 트래픽 엔지니어링 — SRT는 AWS 네트워킹 팀과 긴밀하게 협력하여 Shield Advanced 고객을 보호합니다. 필요한 경우 애플리케이션에 더 많은 완화 용량을 할당하기 위해 인터넷 트래픽이 AWS 네트워크에 도달하는 방식을 변경할 AWS 수 있습니다.
- 아키텍처 권장 사항 — SRT는 공격에 대한 최상의 방어 체계를 구축하려면 모범 사례에 맞게 아키텍처를 변경해야 한다고 판단할 수 있으며, 이러한 권장 사항은 이러한 방법을 구현하는 데 도움이 됩니다. AWS 자세한 내용은 DDoS 복원력에 대한AWS 모범 사례를 참조하세요.

주제

- Shield 대응 팀(SRT) 액세스 권한 구성
- 선제적 대응 구성
- Shield 대응 팀(SRT)에 문의하기

- Shield 대응 팀(SRT)을 통한 사용자 지정 완화 구성

Shield 대응 팀(SRT) 액세스 권한 구성

Shield Response Team (SRT) 이 사용자를 대신하여 AWS WAF 로그에 액세스하고 AWS Shield Advanced 및 AWS WAF API를 호출하여 보호를 관리할 수 있는 권한을 부여할 수 있습니다. 애플리케이션 레이어 DDoS 이벤트 중에 SRT는 AWS WAF 요청을 모니터링하여 비정상적인 트래픽을 식별하고 문제가 되는 트래픽 소스를 완화하기 위한 사용자 지정 규칙을 만드는 데 도움을 줄 수 있습니다. AWS WAF

또한 Application Load Balancer, CloudFront Amazon 또는 타사 소스의 패킷 캡처 또는 로그와 같이 Amazon S3 버킷에 저장한 다른 데이터에 대한 액세스 권한을 SRT에 부여할 수 있습니다.

> **Note**
>
> Shield 대응팀(SRT)의 서비스를 이용하려면 Business Support 플랜 또는 Enterprise Support 플랜에 가입해야 합니다.

SRT의 권한을 관리하려면

1. AWS Shield 콘솔 개요 페이지의 AWS SRT 지원 구성에서 SRT 액세스 편집을 선택합니다. 에디트 AWS 쉴드 대응팀 (SRT) 액세스 페이지가 열립니다.
2. SRT 액세스 설정의 경우, 다음 옵션 중 하나를 선택합니다.

   - SRT에 내 계정에 대한 액세스 권한을 부여하지 않음 - Shield는 이전에 SRT에 부여한 계정 및 리소스 액세스 권한을 제거합니다.
   - SRT가 내 계정에 액세스할 수 있도록 새 역할 만들기 - Shield는 SRT를 대표하는 서비스 주체 `drt.shield.amazonaws.com`를 신뢰하는 역할을 생성하고 여기에 관리형 정책 `AWSShieldDRTAccessPolicy`를 연결합니다. 관리형 정책을 통해 SRT는 사용자를 대신하여 AWS WAF API를 AWS Shield Advanced 호출하고 로그에 액세스할 수 있습니다 AWS WAF . 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책: AWSShieldDRTAccessPolicy섹션을 참조하세요.
   - SRT가 내 계정에 액세스할 수 있는 기존 역할 선택 — 이 옵션을 사용하려면 AWS Identity and Access Management (IAM) 의 역할 구성을 다음과 같이 수정해야 합니다.
     - 관리형 정책 `AWSShieldDRTAccessPolicy`를 역할에 연계하십시오. 이 관리형 정책을 통해 SRT는 사용자를 대신하여 AWS WAF API를 AWS Shield Advanced 호출하고 로그에

액세스할 수 있습니다. AWS WAF 관리형 정책에 대한 자세한 내용은 AWS 관리형 정책: AWSShieldDRTAccessPolicy(을)를 참조하세요. 관리형 정책을 역할에 연계하는 방법에 대한 자세한 설명은 IAM 정책 연계 및 분리를 참조하세요.

- 서비스 담당자 `drt.shield.amazonaws.com`을 신뢰하도록 역할을 수정합니다. 이는 SRT를 대표하는 서비스 담당자입니다. 자세한 내용은 IAM JSON 정책 요소: 보안 주체를 참조하세요.

3. 대상 (선택 사항): Amazon S3 버킷에 대한 SRT 액세스 권한을 부여하고, AWS WAF 웹 ACL 로그에 없는 데이터를 공유해야 하는 경우 이를 구성하십시오. Application Load Balancer 액세스 로그, Amazon CloudFront 로그 또는 타사 소스의 로그를 예로 들 수 있습니다.

> **Note**
>
> AWS WAF 웹 ACL 로그에는 이 작업을 수행할 필요가 없습니다. 계정에 대한 액세스 권한을 부여하면 SRT가 해당 액세스 권한을 얻습니다.

   a. 다음 지침을 따라 Amazon S3 버킷을 구성합니다.

      - 버킷 위치는 이전 단계 AWS Shield Response Team (SRT) 액세스 권한에서 SRT에 일반 액세스 권한을 부여한 위치와 AWS 계정 동일해야 합니다.
      - 버킷은 일반 텍스트이거나 SSE-S3로 암호화될 수 있습니다. Amazon S3 SSE-S3에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 관리형 암호화 키(SSE-S3)를 사용하는 서버 측 암호화로 데이터 보호를 참조하세요.

        SRT는 () 에 저장된 키로 암호화된 버킷에 저장된 로그를 보거나 처리할 수 없습니다. AWS Key Management Service AWS KMS

   b. Shield Advanced (선택 사항): SRT에 Amazon S3 버킷에 대한 액세스 권한 부여 섹션에서, 데이터 또는 로그가 저장된 각각의 Amazon S3 버킷에 대해 버킷 이름을 입력하고 버킷 추가를 선택합니다. 버킷을 최대 10개까지 추가할 수 있습니다.

      이렇게 하면 SRT에 각 버킷에 대한 `s3:GetBucketLocation`, `s3:GetObject` 및 `s3:ListBucket` 권한이 부여됩니다.

      10개 이상의 버킷에 액세스할 수 있는 권한을 SRT에 부여하려면 추가 버킷 정책을 편집하고 여기에 나열된 SRT용 권한을 수동으로 부여하면 됩니다.

      다음 내용은 정책 목록의 예를 보여줍니다.

```
{
    "Sid": "AWSDDoSResponseTeamAccessS3Bucket",
    "Effect": "Allow",
    "Principal": {
        "Service": "drt.shield.amazonaws.com"
    },
    "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::bucket-name",
        "arn:aws:s3:::bucket-name/*"
    ]
}
```

4. 저장을 선택하여 변경 사항을 저장합니다.

또한 IAM 역할을 생성하고 여기에 정책을 연결한 다음 이 역할을 AssociatedRrole 작업에 전달하여 API를 통해 AWSShieldDRTAccessPolicy SRT를 승인할 수 있습니다.

선제적 대응 구성

Shield 대응 팀(SRT)은 선제적 대응이 구성되어 있는 경우 가능한 공격으로 인해 애플리케이션의 가용성이나 성능이 영향을 받는 경우 고객에게 직접 연락을 취합니다. 이 대응 모델은 가장 빠른 SRT 대응을 제공하고 SRT가 고객과 연락을 취하기도 전에 문제 해결을 시작할 수 있으므로 이 대응 모델을 사용하는 것이 좋습니다.

Elastic IP 주소 및 AWS Global Accelerator 표준 가속기의 네트워크 계층 및 전송 계층 이벤트와 Amazon 배포 및 애플리케이션 로드 밸런서의 웹 요청 플러드에 대해 사전 예방적 참여를 사용할 수 있습니다. CloudFront 선제적 대응은 연결된 Amazon Route 53 상태 확인이 있는 Shield Advanced 리소스 보호에 한해 사용할 수 있습니다. 상태 확인 관리 및 사용에 대한 자세한 내용은 상태 점검을 사용한 상태 기반 탐지(을)를 참조하세요.

Shield Advanced에서 이벤트가 감지되면 SRT는 상태 확인 상태를 바탕으로 해당 이벤트에 대한 선제적 대응이 가능한지 여부를 판단합니다. 그럴 경우 SRT는 선제적 대응 구성에 제공된 연락처 지침에 따라 연락을 드릴 것입니다.

선제적 대응을 위해 연락처를 최대 10개까지 구성할 수 있으며 SRT가 연락하는 데 도움이 되는 참고 사항을 제공할 수 있습니다. 이벤트 동안 SRT와 소통할 수 있는 선제적 대응 담당자가 있어야 합니다. 고객에게 연중무휴 운영 센터가 없는 경우, 호출기 연락처를 제공하고 연락처 참고 사항에 해당 연락처 선호 사항을 기재할 수 있습니다.

선제적 대응이 가능하려면 고객이 다음을 수행해야 합니다.

- Business Support 플랜 또는 Enterprise Support 플랜을 구독해야 합니다.
- Amazon Route 53 상태 확인을 선제적 대응으로 보호하려는 모든 리소스와 연결해야 합니다. SRT는 상태 확인의 상태를 사용하여 이벤트에 선제적 대응이 필요한지 여부를 판단할 수 있으므로 상태 확인에서 보호 대상 리소스의 상태를 정확하게 반영하는 것이 중요합니다. 자세한 정보 및 지침은 상태 점검을 사용한 상태 기반 탐지(을)를 참조하세요.
- AWS WAF 웹 ACL이 연결된 리소스의 경우 의 최신 버전인 (v2) 를 사용하여 웹 ACL을 생성해야 합니다. AWS WAF AWS WAF
- SRT가 이벤트 동안 선제적 대응에 사용할 연락처를 한 곳 이상 제공해야 합니다. 연락처 정보를 완전하게 최신 상태로 유지하세요.

SRT 전향적 연계를 활성화하려면

1. AWS Shield 콘솔 개요 페이지의 사전 참여 및 연락처 아래에 있는 연락처 영역에서 편집을 선택합니다.

   연락처 편집 페이지에서 SRT가 전향적 연계를 위해 연락할 담당자의 연락처 정보를 입력합니다.

   둘 이상의 연락처를 제공하는 경우, 주에 각 연락처를 사용해야 하는 경우를 표시하십시오. 기본 및 보조 연락처 지정을 포함하고 각 연락처의 이용 가능 시간과 시간대를 제공하십시오.

   연락처 메모 예시:

   - 이 핫라인은 연중무휴 24시간 운영됩니다. 담당 분석가에게 문의하면 적절한 담당자를 통화 중에 연결해 드립니다.
   - 5분 이내에 핫라인이 응답하지 않으면 저에게 연락하십시오.
2. 저장을 선택합니다.

   개요 페이지에는 업데이트된 연락처 정보가 반영됩니다.
3. 전향적 연계 기능 편집을 선택하고 활성화를 선택한 다음 저장을 선택하여 전향적 연계를 활성화합니다.

Shield 대응 팀(SRT)에 문의하기

다음 방법 중 하나로 Shield 대응 팀(SRT)에 문의할 수 있습니다.

지원 사례

AWS 지원 센터 콘솔의 AWS Shield 아래에서 케이스를 시작할 수 있습니다.

지원 사례 생성에 대한 지침은 AWS Support 센터를 참조하세요.

상황에 적합한 심각도를 선택하고 연락처 세부 정보를 제공합니다. 설명에서 최대한 자세한 내용을 제공하십시오. 영향을 받을 수 있다고 생각되는 보호된 리소스 및 최종 사용자 환경의 현재 상태에 대한 정보를 제공합니다. 예를 들어 사용자 환경이 저하되거나 애플리케이션의 일부를 현재 사용할 수 없는 경우 해당 정보를 제공합니다.

- 의심되는 DDoS 공격의 경우 – 현재 발생 가능한 DDoS 공격으로 인해 애플리케이션의 가용성 또는 성능이 영향을 받는 경우, 다음의 심각도 및 연락처 옵션을 선택하십시오.
  - 심각도에 대해서는 지원 플랜에서 사용할 수 있는 가장 높은 심각도를 선택합니다.
    - 비즈니스 지원의 경우, 이 내용은 프로덕션 시스템 중단: 1시간 이내입니다.
    - 엔터프라이즈 지원의 경우, 이 내용은 비즈니스 크리티컬 시스템 중단: 15분 이내입니다.
  - 연락처 옵션의 경우, 전화 또는 채팅을 선택하고 세부 정보를 제공합니다. 실시간 연락 방법을 사용하면 가장 빠른 응답을 받을 수 있습니다.

선제적 대응

AWS Shield Advanced 사전 예방적 참여를 통해 이벤트 감지 중에 보호 대상 리소스와 관련된 Amazon Route 53 상태 확인이 비정상 상태가 되면 SRT에서 사용자에게 직접 연락을 취합니다. 이 옵션에 대한 자세한 내용은 선제적 대응 구성을 참조하세요.

Shield 대응 팀(SRT)을 통한 사용자 지정 완화 구성

엘라스틱 IP (EIP) 및 AWS Global Accelerator 표준 액셀러레이터의 경우 SRT (Shield Response Team) 와 협력하여 사용자 지정 완화 기능을 구성할 수 있습니다. 이는 완화 조치를 적용할 때 실행해야 하는 특정 로직을 알고 있는 경우에 유용합니다. 예를 들어 특정 국가에서 발송된 트래픽만 허용하거나, 특정 속도 제한을 적용하거나, 선택적 검증을 구성하거나, 조각을 허용하지 않거나, 패킷 페이로드의 특정 패턴과 일치하는 트래픽만 허용할 수 있습니다.

다음은 일반적인 사용자 지정 완화 조치의 예입니다.

- 패턴 매칭 — 클라이언트 측 애플리케이션과 상호 작용하는 서비스를 운영하는 경우 해당 애플리케이션 특유의 알려진 패턴을 기준으로 매칭하도록 선택할 수 있습니다. 예를 들어, 고객사에서 배포하는 특정 소프트웨어를 최종 사용자가 설치해야 하는 게임 또는 통신 서비스를 운영할 수 있습니다. 애플리케이션이 고객사의 서비스로 전송하는 모든 패킷에 매직 넘버를 포함할 수 있습니다. 최대 128바이트(분리 또는 연속)의 조각화되지 않은 TCP 또는 UDP 패킷 페이로드와 헤더를 기준으로 매칭할 수 있습니다. 일치는 16진수 표기법으로 패킷 페이로드 시작 부분으로부터의 특정 오프셋 또는 알려진 값 이후의 동적 오프셋으로 나타낼 수 있습니다. 예를 들어, 완화 기능은 바이트 `0x01`을(를) 찾은 후 `0x12345678`을(를) 다음 4바이트로 예상할 수 있습니다.
- DNS 관련 — Global Accelerator 또는 Amazon Elastic Compute Cloud(Amazon EC2)와 같은 서비스를 사용하여 신뢰할 수 있는 자체 DNS 서비스를 운영하는 경우, 패킷이 유효한 DNS 쿼리인지 확인하는 사용자 지정 완화 조치를 요청하고 DNS 트래픽과 관련된 속성을 평가하는 의심 점수를 적용할 수 있습니다.

SRT와 협력하여 사용자 지정 완화 조치를 구축하는 방법에 대해 문의하려면 AWS Shield아래에서 지원 케이스를 생성하십시오. AWS Support 사례 생성에 대해 자세히 알아보려면 시작하기를 참조하십시오. AWS Support

의 리소스 보호 AWS Shield Advanced

리소스에 대한 AWS Shield Advanced 보호를 추가하고 구성할 수 있습니다. 단일 리소스에 대한 보호를 관리하고 더 나은 이벤트 관리가 가능하도록 보호된 리소스를 논리적 모음으로 그룹화할 수 있습니다. 를 사용하여 AWS Config Shield Advanced 보호 기능의 변경 사항을 추적할 수도 있습니다.

주제

- AWS Shield Advanced 리소스 유형별 보호
- AWS Shield Advanced 애플리케이션 계층 (계층 7) 보호
- 상태 점검을 사용한 상태 기반 탐지
- 에서 리소스 보호 관리 AWS Shield Advanced
- AWS Shield Advanced 보호 그룹
- 에서 리소스 보호 변경 내용 추적 AWS Config

AWS Shield Advanced 리소스 유형별 보호

Shield Advanced는 네트워크 및 전송 계층 (계층 3 및 4) 과 애플리케이션 계층 (계층 7) 의 AWS 리소스를 보호합니다. 일부 리소스는 직접 보호하고 다른 리소스는 보호된 리소스와의 연결을 통해 보호할 수 있습니다. Shield Advanced는 IPv4를 지원하지만 IPv6는 지원하지 않습니다.

이 섹션에서는 각 리소스 유형에 대한 Shield Advanced 보호에 대한 정보를 제공합니다.

> **Note**
>
> Shield Advanced는 Shield Advanced를 통해 또는 AWS Firewall Manager Shield Advanced 정책을 통해 지정한 리소스만 보호합니다. 이 기능은 리소스를 자동으로 보호하지 않습니다.

다음 리소스 유형을 포함한 고급 모니터링 및 보호에 Shield Advanced를 사용할 수 있습니다.

- 아마존 CloudFront 배포판. CloudFront 지속적 배포의 경우 Shield Advanced는 보호된 기본 배포와 관련된 모든 스테이징 배포를 보호합니다.
- Amazon Route 53 호스팅 영역.
- AWS Global Accelerator 표준 액셀러레이터.
- Amazon EC2 탄력적 IP 주소. Shield Advanced는 보호된 탄력적 IP 주소와 연결된 리소스를 보호합니다.
- Amazon EC2 인스턴스, Amazon EC2 탄력적 IP 주소와의 연결을 통해.
- 다음 유형의 Elastic Load Balancing(ELB) 로드 밸런서:
  - Application Load Balancers.
  - Classic Load Balancer
  - Network Load Balancer, Amazon EC2 탄력적 IP 주소와의 연결을 통해.

그 외의 리소스 유형은 Shield Advanced를 사용하여 보호할 수 없습니다. 예를 들어 AWS Global Accelerator 사용자 지정 라우팅 액셀러레이터나 Gateway Load Balancer는 보호할 수 없습니다.

각 리소스 유형에 대해 AWS 계정당 최대 1,000개의 리소스를 모니터링하고 보호할 수 있습니다. 예를 들어 단일 계정으로 1,000개의 Amazon EC2 엘라스틱 IP 주소, 1,000개의 CloudFront 배포, 1,000개의 애플리케이션 로드 밸런서를 보호할 수 있습니다. https://console.aws.amazon.com/servicequotas/의 Service Quotas 콘솔을 통해 Shield Advanced로 보호할 수 있는 리소스 수를 늘려줄 것을 요청할 수 있습니다.

Shield Advanced로 Amazon EC2 인스턴스 및 Network Load Balancer 보호

먼저 이러한 리소스를 탄력적 IP 주소에 연결한 다음 Shield Advanced에서 탄력적 IP 주소를 보호함으로써 Amazon EC2 인스턴스와 Network Load Balancer를 보호할 수 있습니다.

탄력적 IP 주소를 보호하는 경우, Shield Advanced는 탄력적 IP 주소가 연결된 리소스를 식별하고 보호합니다. Shield Advanced는 탄력적 IP 주소에 연결된 리소스 유형을 자동으로 식별하고 해당 리소스에 적절한 탐지 및 완화 조치를 적용합니다. 여기에는 탄력적 IP 주소에 따라 네트워크 ACL을 구성하는 작업도 포함됩니다. AWS 리소스와 함께 탄력적 IP 주소를 사용하는 방법에 대한 자세한 내용은 다음 가이드를 참조하세요: Amazon Elastic Compute Cloud 설명서 또는 Elastic Load Balancing 설명서를 참조하세요.

공격 중에 Shield Advanced는 네트워크 ACL을 네트워크 경계에 자동으로 배포합니다 AWS . 네트워크 ACL이 네트워크의 경계에 있는 경우, Shield Advanced에서는 더 큰 DDoS 이벤트에 대한 보호를 제공할 수 있습니다. 일반적으로 네트워크 ACL은 Amazon VPC 내에서 근접한 Amazon EC2 인스턴스에 적용됩니다. 네트워크 ACL은 Amazon VPC와 인스턴스가 처리할 수 있을 정도의 큰 공격만 완화할 수 있습니다. 예를 들어, Amazon EC2 인스턴스에 연결된 네트워크 인터페이스가 최대 10Gbps를 처리할 수 있는 경우, 10Gbps를 초과하는 볼륨은 느려지며 해당 인스턴스에 대한 트래픽이 차단될 수 있습니다. 공격 시에 Shield Advanced는 네트워크 ACL을 AWS 경계로 승격시켜 다수 테라바이트의 트래픽을 처리할 수 있습니다. 네트워크 ACL은 네트워크의 일반적인 용량 이상으로 리소스에 대한 보호를 제공할 수 있습니다. 네트워크 ACL에 대한 자세한 내용은 네트워크 ACL을 참조하세요.

예를 들어 일부 확장 AWS Elastic Beanstalk도구에서는 Network Load Balancer에 엘라스틱 IP 주소를 자동으로 연결할 수 없습니다. 이러한 경우에는 탄력적 IP 주소를 수동으로 연결해야 합니다.

AWS Shield Advanced 애플리케이션 계층 (계층 7) 보호

Shield Advanced로 애플리케이션 계층 리소스를 보호하려면 먼저 AWS WAF 웹 ACL을 리소스에 연계하고 여기에 하나 이상의 속도 기반 규칙을 추가합니다. 또한 자동 애플리케이션 계층 DDoS 완화를 활성화하여 Shield Advanced가 DDoS 공격에 대응하여 사용자 대신 웹 ACL 규칙을 자동으로 생성하고 관리하도록 할 수 있습니다.

Shield Advanced로 애플리케이션 계층 리소스를 보호하는 경우, Shield Advanced는 시간 경과에 따른 트래픽을 분석하여 기준을 설정하고 유지합니다. Shield Advanced는 이러한 기준을 사용하여 DDoS 공격을 나타낼 수 있는 트래픽 패턴의 이상을 감지합니다. Shield Advanced가 공격을 감지하는 시점은 Shield Advanced가 공격 이전에 관찰할 수 있었던 트래픽과 웹 애플리케이션에 사용하는 아키텍처에 따라 달라집니다. Shield Advanced 동작에 영향을 줄 수 있는 아키텍처 변형에는 사용하는 인스턴스 타입, 인스턴스 크기, 인스턴스 타입이 향상된 네트워킹을 지원하는지 여부 등이 포함됩니다. 애플리케이션 계층 공격에 대한 완화 기능을 자동으로 배치하도록 Shield Advanced를 구성할 수도 있습니다.

쉴드 어드밴스드 구독 및 비용 AWS WAF

Shield Advanced를 구독하면 Shield Advanced로 보호하는 리소스의 표준 AWS WAF 기능을 사용하는 데 드는 비용이 포함됩니다. Shield Advanced 보호가 적용되는 표준 AWS WAF 요금은 웹 ACL당 비용, 규칙당 비용, 웹 요청 검사 요청 1백만 건당 기본 가격 (최대 1,500WCU 및 최대 기본 본체 크기) 입니다.

Shield Advanced 자동 애플리케이션 레이어 DDoS 완화를 활성화하면 150개의 웹 ACL 용량 단위 (WCU) 를 사용하는 규칙 그룹이 웹 ACL에 추가됩니다. 이러한 WCU는 웹 ACL의 WCU 사용량에 포함됩니다. 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화, Shield Advanced 규칙 그룹, AWS WAF 웹 ACL 용량 단위 (WCU) 단원을 참조하세요.

Shield Advanced를 구독해도 Shield Advanced를 사용하여 보호하지 않는 리소스에 AWS WAF 대한 사용은 포함되지 않습니다. 또한 보호 대상 리소스에 대한 추가 비표준 AWS WAF 비용도 포함되지 않습니다. 비표준 AWS WAF 비용의 예로는 Bot Control, CAPTCHA 규칙 작업, 1,500개 이상의 WCU를 사용하는 웹 ACL, 기본 본문 크기를 초과하여 요청 본문을 검사하는 비용 등이 있습니다. 전체 목록은 요금 페이지에 나와 있습니다. AWS WAF

전체 정보 및 요금 예는 Shield 요금 및 AWS WAF 요금을 참조하세요.

주제

- 감지 및 완화
- Shield Advanced 애플리케이션 레이어 AWS WAF 웹 ACL 및 요금 기반 규칙
- Shield Advanced 자동 애플리케이션 계층 DDoS 완화

감지 및 완화

이 섹션에서는 Shield Advanced의 애플리케이션 계층 이벤트 탐지 및 완화에 영향을 미치는 요인을 설명합니다.

상태 확인

애플리케이션의 전반적인 상태를 정확하게 보고하는 상태 점검은 Shield Advanced에 애플리케이션이 겪고 있는 트래픽 상황에 대한 정보를 제공합니다. Shield Advanced는 애플리케이션이 비정상이라고 보고할 때 잠재적 공격을 가리키는 정보가 덜 필요하고 애플리케이션이 정상이라고 보고하는 경우 공격의 증거가 더 많이 필요합니다.

애플리케이션 상태를 정확하게 보고하도록 상태 점검을 구성하는 것이 중요합니다. 자세한 정보 및 지침은 상태 점검을 사용한 상태 기반 탐지(을)를 참조하세요.

트래픽 베이스라인

트래픽 베이스라인은 Shield Advanced에 애플리케이션의 정상 트래픽 특성에 대한 정보를 제공합니다. Shield Advanced는 이러한 기준을 사용하여 애플리케이션이 정상적인 트래픽을 수신하지 않을 때를 인식하므로 사용자에게 이를 알리고 구성에 따라 잠재적 공격에 대응하기 위한 완화 옵션을 고안하고 테스트할 수 있습니다. Shield Advanced가 트래픽 기준을 사용하여 잠재적 이벤트를 탐지하는 방법에 대한 추가 정보는 개요 섹션을 참조하십시오. 애플리케이션 계층 위협에 대한 감지 로직

Shield Advanced는 보호된 리소스와 관련된 웹 ACL에서 제공하는 정보를 바탕으로 기준을 생성합니다. Shield Advanced가 애플리케이션의 기준을 안정적으로 결정할 수 있으려면 웹 ACL을 최소 24시간에서 최대 30일 동안 리소스에 연결해야 합니다. 필요한 시간은 Shield Advanced를 통해 또는 Shield Advanced를 통해 웹 ACL을 연결할 때 시작됩니다. AWS WAF

Shield Advanced 애플리케이션 계층 보호와 함께 웹 ACL을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오. Shield Advanced 애플리케이션 레이어 AWS WAF 웹 ACL 및 요금 기반 규칙

속도 기반 규칙

속도 기반 규칙은 공격을 완화하는 데 도움이 될 수 있습니다. 또한 정상적인 트래픽 기준이나 상태 점검 상태 보고에 나타날 정도로 큰 문제가 발생하기 전에 공격을 방어하여 공격을 모호하게 만들 수 있습니다.

Shield Advanced로 애플리케이션 리소스를 보호할 때는 웹 ACL에서 속도 기반 규칙을 사용하는 것이 좋습니다. 방어 기능이 잠재적 공격을 가릴 수 있기는 하지만 합법적 고객이 애플리케이션을 계속 사용할 수 있도록 하는 데 도움이 되는 중요한 1차 방어선입니다. 속도 기반 규칙이 탐지한 트래픽과 속도 제한은 지표에서 확인할 수 있습니다. AWS WAF

자체 속도 기반 규칙 외에도 자동 애플리케이션 레이어 DDoS 완화를 활성화하면 Shield Advanced는 공격을 완화하는 데 사용하는 규칙 그룹을 웹 ACL에 추가합니다. 이 규칙 그룹에서 Shield Advanced는 항상 DDoS 공격의 소스로 알려진 IP 주소의 요청 양을 제한하는 속도 기반 규칙을 적용합니다. Shield Advanced 규칙이 완화하는 트래픽에 대한 지표는 확인할 수 없습니다.

요금 기반 규칙에 대한 자세한 내용은 을 참조하십시오. 비율 기반 규칙 문 Shield Advanced가 자동 애플리케이션 계층 DDoS 완화에 사용하는 속도 기반 규칙에 대한 자세한 내용은 을 참조하십시오. Shield Advanced 규칙 그룹

Shield Advanced와 AWS WAF 지표에 대한 자세한 내용은 을 참조하십시오아마존을 통한 모니터링 CloudWatch.

Shield Advanced 애플리케이션 레이어 AWS WAF 웹 ACL 및 요금 기반 규칙

Shield Advanced로 애플리케이션 계층 리소스를 보호하려면 먼저 AWS WAF 웹 ACL을 리소스에 연결합니다. AWS WAF 애플리케이션 계층 리소스에 전달되는 HTTP 및 HTTPS 요청을 모니터링하고 요청의 특성에 따라 콘텐츠에 대한 액세스를 제어할 수 있게 해주는 웹 애플리케이션 방화벽입니다. 요청이 기원된 위치, 쿼리 문자열 및 쿠키의 내용, 단일 IP 주소에서 들어오는 요청의 비율과 같은 요소에 근거하여 요청을 모니터링하고 관리하도록 웹 ACL을 구성할 수 있습니다. Shield Advanced 보호를 사용하려면 최소한 웹 ACL을 속도 기반 규칙과 연계해야 합니다. 이 규칙은 각 IP 주소에 대한 요청 속도를 제한합니다.

연계된 웹 ACL에 속도 기반 규칙이 정의되어 있지 않은 경우, Shield Advanced는 하나 이상의 규칙을 정의하라는 메시지를 표시합니다. 속도 기반 규칙은 소스 IP가 정의된 임계값을 초과하는 경우, 소스 IP의 트래픽을 자동으로 차단합니다. 속도 기반 규칙은 웹 요청 홍수로부터 애플리케이션을 보호하는 데 도움이 되며, 잠재적인 DDoS 공격으로 이어질 수 있는 갑작스러운 트래픽 급증에 대한 알림을 제공할 수 있습니다.

> **Note**
>
> 속도 기반 규칙은 규칙이 모니터링하는 트래픽의 급증에 매우 빠르게 대응합니다. 따라서 속도 기반 규칙은 공격뿐만 아니라 Shield Advanced 탐지를 통한 잠재적 공격 탐지도 방지할 수 있습니다. 이러한 절충점은 공격 패턴에 대한 완전한 가시성보다 예방에 유리합니다. 공격에 대한 1차 방어선으로 속도 기반 규칙을 사용하는 것이 좋습니다.

웹 ACL을 사용하면 DDoS 공격이 발생할 경우, 웹 ACL에서 규칙을 추가하고 관리하여 완화를 적용할 수 있습니다. 이 작업은 Shield 대응팀(SRT)의 도움을 받아 직접 수행하거나 자동 애플리케이션 계층 DDoS 완화를 통해 자동으로 수행할 수 있습니다.

> **Important**
>
> 자동 애플리케이션 레이어 DDoS 완화 기능도 사용하는 경우 에서 웹 ACL 관리 모범 사례를 참조하십시오. 자동 완화 사용 모범 사례

기본 속도 기반 규칙 동작

속도 기반 규칙을 기본 구성과 함께 사용하는 경우 이전 5분 동안의 트래픽을 AWS WAF 주기적으로 평가합니다. AWS WAF 요청 비율이 허용 가능한 수준으로 떨어질 때까지 규칙의 임계값을 초과하는

모든 IP 주소의 요청을 차단합니다. Shield Advanced를 통해 속도 기반 규칙을 구성하는 경우 5분 내에 하나의 소스 IP에서 예상하는 일반 트래픽 속도보다 큰 값으로 속도 임계값을 구성하십시오.

웹 ACL에서 속도 기반 규칙을 두 개 이상 사용하고 싶을 수도 있습니다. 예컨대, 임계값이 높은 모든 트래픽에 대한 속도 기반 규칙 하나와 웹 애플리케이션의 특정 부분과 일치하도록 구성되고 임계값이 더 낮은 추가 규칙을 하나 이상 추가할 수 있습니다. 예를 들어, URI `/login.html`를 낮은 임계값으로 일치시켜 로그인 페이지에 대한 침해를 완화할 수 있습니다.

다른 평가 기간을 사용하고 헤더 값, 레이블, 쿼리 인수와 같은 여러 요청 구성 요소별로 요청을 집계하도록 속도 기반 규칙을 구성할 수 있습니다. 자세한 정보는 비율 기반 규칙 문을 참조하세요.

추가 정보 및 지침은 보안 블로그 게시물인 가장 중요한 AWS WAF 세 가지 속도 기반 규칙을 참조하십시오.

를 통해 구성 옵션을 확장했습니다. AWS WAF

Shield Advanced 콘솔에서는 속도 기반 규칙을 추가하고 기본 설정으로 구성할 수 있습니다. 를 통해 요금 기반 규칙을 관리하여 추가 구성 옵션을 정의할 수 있습니다. AWS WAF예를 들어 전달된 IP 주소, 쿼리 문자열, 레이블 등의 키를 기반으로 요청을 집계하도록 규칙을 구성할 수 있습니다. 규칙에 범위 축소 문을 추가하여 평가 및 속도 제한에서 일부 요청을 필터링할 수도 있습니다. 자세한 정보는 비율 기반 규칙 문을 참조하세요. 웹 요청 모니터링 및 관리 규칙을 관리하는 AWS WAF 데 사용하는 방법에 대한 자세한 내용은 을 참조하십시오. 웹 ACL 생성

Shield Advanced 자동 애플리케이션 계층 DDoS 완화

보호된 애플리케이션 계층 리소스에 대한 애플리케이션 계층(계층 7) 공격을 완화하도록 Shield Advanced를 구성하여 공격의 일부인 웹 요청을 세거나 차단함으로써 자동으로 대응하도록 구성할 수 있습니다. 이 옵션은 AWS WAF 웹 ACL 및 자체 속도 기반 규칙을 사용하여 Shield Advanced를 통해 추가하는 애플리케이션 계층 보호에 추가됩니다.

리소스에 대해 자동 완화가 활성화되면 Shield Advanced는 리소스를 대표하여 완화 규칙을 관리하는 리소스의 관련 웹 ACL에 규칙 그룹을 유지 관리합니다. 규칙 그룹에는 DDoS 공격의 소스로 알려진 IP 주소의 요청 양을 추적하는 속도 기반 규칙이 포함되어 있습니다.

또한, Shield Advanced는 현재 트래픽 패턴을 과거 트래픽 베이스라인과 비교하여 DDoS 공격을 표시할 수 있는 편차를 감지합니다. Shield Advanced는 규칙 그룹에 추가 사용자 지정 AWS WAF 규칙을 생성, 평가 및 배포하여 탐지된 DDoS 공격에 대응합니다.

목차

자동 완화 기능 사용 시 경고 사항

다음 목록은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화에 대한 경고 사항을 설명하고 이에 대응하여 취해야 할 조치를 설명합니다.

- 자동 애플리케이션 레이어 DDoS 완화는 최신 버전 AWS WAF (v2) 을 사용하여 만든 웹 ACL에서만 작동합니다.
- Shield Advanced는 애플리케이션의 정상 및 기록 트래픽의 기준을 설정하는 데 시간이 필요합니다. 이 기준을 활용하여 공격 트래픽을 탐지하고 정상 트래픽과 분리하여 공격 트래픽을 완화합니다. 기준을 설정하는 데 걸리는 시간은 웹 ACL을 보호된 애플리케이션 리소스에 연결한 시점으로부터 24시간에서 30일 사이입니다. 트래픽 기준에 대한 추가 정보는 을 참조하십시오. 감지 및 완화
- 자동 애플리케이션 레이어 DDoS 완화를 활성화하면 150개의 웹 ACL 용량 단위 (WCU) 를 사용하는 규칙 그룹이 웹 ACL에 추가됩니다. 이러한 WCU는 웹 ACL의 WCU 사용량에 포함됩니다. 자세한 정보는 Shield Advanced 규칙 그룹 및 AWS WAF 웹 ACL 용량 단위 (WCU) 섹션을 참조하세요.
- Shield Advanced 규칙 그룹은 AWS WAF 지표를 생성하지만 볼 수는 없습니다. 이는 웹 ACL에서 사용하지만 소유하지 않는 다른 규칙 그룹 (예: AWS 관리형 규칙 그룹) 의 경우와 동일합니다. AWS WAF 지표에 대한 자세한 내용은 을 참조하십시오AWS WAF 지표 및 차원. 이 Shield Advanced 보

호 옵션에 대한 자세한 내용은 을 참조하십시오Shield Advanced 자동 애플리케이션 계층 DDoS 완화.

- 여러 리소스를 보호하는 웹 ACL의 경우 자동 완화 기능은 보호된 리소스에 부정적인 영향을 미치지 않는 사용자 지정 완화 기능만 배포합니다.
- DDoS 공격이 시작된 시점부터 Shield Advanced가 사용자 지정 자동 완화 규칙을 적용하는 시점까지의 시간은 각 이벤트에 따라 다릅니다. 일부 DDoS 공격은 사용자 지정 규칙이 배포되기 전에 종료될 수 있습니다. 완화 조치가 이미 마련되어 있을 때 다른 공격이 발생할 수 있으며, 따라서 이벤트 시작부터 이러한 규칙에 의해 완화될 수 있습니다. 또한 웹 ACL 및 Shield Advanced 규칙 그룹의 속도 기반 규칙은 공격 트래픽이 가능한 이벤트로 탐지되기 전에 이를 완화할 수 있습니다.
- CloudFrontAmazon과 같은 CDN (콘텐츠 전송 네트워크) 을 통해 트래픽을 수신하는 애플리케이션 로드 밸런서의 경우, 해당 Application Load Balancer 리소스에 대한 Shield Advanced의 애플리케이션 계층 자동 완화 기능이 감소합니다. Shield Advanced는 클라이언트 트래픽 속성을 사용하여 애플리케이션으로 들어오는 일반 트래픽으로부터 공격 트래픽을 식별하고 분리하며, CDN은 원래 클라이언트 트래픽 속성을 보존하거나 전달하지 않을 수 있습니다. 를 사용하는 CloudFront 경우 배포 시 자동 완화 기능을 활성화하는 것이 좋습니다. CloudFront
- 자동 애플리케이션 계층 DDoS 완화는 보호 그룹과 상호 작용하지 않습니다. 보호 그룹에 있는 리소스에 대해 자동 완화를 활성화할 수 있지만 Shield Advanced는 보호 그룹 결과에 근거하여 공격 완화를 자동으로 적용하지 않습니다. Shield Advanced는 개별 리소스에 대한 자동 공격 완화 기능을 적용합니다.

자동 완화 사용 모범 사례

자동 완화를 사용할 때는 이 섹션에 제공된 지침을 준수하세요.

일반 보호 및 관리

자동 완화 보호를 계획하고 구현하려면 다음 지침을 따르십시오.

- 모든 자동 완화 보호 기능은 Shield Advanced를 통해 관리하거나, Shield Advanced 자동 방어 설정을 관리하는 AWS Firewall Manager 데 사용하는 경우 Firewall Manager를 통해 관리할 수 있습니다. Shield Advanced와 Firewall Manager를 혼용하여 이러한 보호 기능을 관리하지 마십시오.
- 동일한 웹 ACL과 보호 설정을 사용하여 유사한 리소스를 관리하고, 서로 다른 웹 ACL을 사용하여 서로 다른 리소스를 관리하세요. Shield Advanced는 보호된 리소스에 대한 DDoS 공격을 방어할 때 해당 리소스와 연계된 웹 ACL에 대한 규칙을 정의한 다음 웹 ACL과 연계된 모든 리소스의 트래픽에 대해 규칙을 테스트합니다. Shield Advanced는 관련 리소스에 부정적인 영향을 미치지 않는 경우에만 규칙을 적용합니다. 자세한 정보는 Shield Advanced가 자동 완화를 관리하는 방법을 참조하세요.

- Amazon CloudFront 배포를 통해 모든 인터넷 트래픽이 프록시되는 애플리케이션 로드 밸런서의 경우 배포에 대한 자동 완화 기능만 활성화하십시오. CloudFront CloudFront 배포에는 항상 원래 트래픽 속성이 가장 많으며, Shield Advanced는 이를 활용하여 공격을 완화합니다.

탐지 및 방어 최적화

다음 지침에 따라 자동 완화 기능이 보호된 리소스에 제공하는 보호를 최적화하십시오. 애플리케이션 계층 탐지 및 완화에 대한 개요는 를 참조하십시오. 감지 및 완화

- 보호되는 리소스에 대한 상태 확인을 구성하고 이를 사용하여 Shield Advanced 보호에서 상태 기반 탐지를 활성화하세요. 자세한 지침은 상태 점검을 사용한 상태 기반 탐지을 참조하세요.
- Shield Advanced가 정상적인 과거 트래픽에 대한 기준을 설정할 때까지 Count 모드에서 자동 완화 기능을 활성화합니다. Shield Advanced는 기준을 설정하는 데 24시간에서 30일이 소요됩니다.

  정상 트래픽 패턴의 기준을 설정하려면 다음이 필요합니다.
  - 웹 ACL과 보호된 리소스의 연결 를 사용하여 웹 ACL을 AWS WAF 직접 연결하거나 Shield Advanced 애플리케이션 계층 보호를 활성화하고 사용할 웹 ACL을 지정할 때 Shield Advanced가 이를 연결하도록 할 수 있습니다.
  - 보호된 애플리케이션으로의 정상적인 트래픽 흐름. 애플리케이션이 시작되기 전과 같이 애플리케이션에 정상적인 트래픽이 발생하지 않는 경우 또는 장기간 프로덕션 트래픽이 부족한 경우에는 기간별 데이터를 수집할 수 없습니다.

웹 ACL 관리

자동 완화 기능과 함께 사용하는 웹 ACL을 관리하려면 다음 지침을 따르십시오.

- 보호된 리소스와 연결된 웹 ACL을 교체해야 하는 경우 다음과 같이 순서대로 변경하십시오.
  1. Shield Advanced에서 자동 완화 기능을 비활성화합니다.
  2. 에서 AWS WAF기존 웹 ACL의 연결을 끊고 새 웹 ACL을 연결합니다.
  3. Shield Advanced에서 자동 완화 기능을 활성화합니다.

  Shield Advanced는 자동 완화 기능을 기존 웹 ACL에서 새 웹 ACL로 자동 이전하지 않습니다.
- 명칭이 `ShieldMitigationRuleGroup`으로 시작하는 웹 ACL에서 규칙 그룹 규칙을 삭제하지 마십시오. 이 규칙 그룹을 삭제하면 웹 ACL과 연결된 모든 리소스에 대해 Shield Advanced 자동 완화 기능이 제공하는 보호 기능을 비활성화합니다. 또한 Shield Advanced가 변경 알림을 받고 설정을 업데이트하는 데 다소 시간이 걸릴 수 있습니다. 이 기간 동안에는 Shield Advanced 콘솔 페이지에 올바르지 않은 정보가 표시됩니다.

규칙 그룹에 대한 자세한 내용은 Shield Advanced 규칙 그룹 섹션을 참조하세요.

- 명칭이 ShieldMitigationRuleGroup으로 시작하는 규칙 그룹 규칙의 명칭은 수정하지 마세요. 이렇게 하면 웹 ACL을 통한 Shield Advanced 자동 완화 기능이 제공하는 보호 기능에 방해가 될 수 있습니다.
- 규칙과 규칙 그룹을 생성할 때는 ShieldMitigationRuleGroup으로 시작하는 명칭을 사용하지 마세요. 이 문자열은 Shield Advanced에서 자동 완화 기능을 관리하는 데 사용됩니다.
- 웹 ACL 규칙을 관리할 때 우선 순위 설정을 10,000,000으로 지정하지 마세요. Shield Advanced는 자동 완화 규칙 그룹 규칙을 추가할 때 이 우선 순위 설정을 자동 완화 규칙 그룹 규칙에 할당합니다.
- ShieldMitigationRuleGroup 규칙의 우선 순위를 지정하여 웹 ACL의 다른 규칙과 관련하여 원하는 시간에 실행되도록 하세요. Shield Advanced는 우선 순위가 10,000,000인 규칙 그룹 규칙을 웹 ACL에 추가하여 다른 규칙 이후에 실행합니다. AWS WAF 콘솔 마법사를 사용하여 웹 ACL을 관리하는 경우 웹 ACL에 규칙을 추가한 후 필요에 따라 우선순위 설정을 조정하십시오.
- 를 AWS CloudFormation 사용하여 웹 ACL을 관리하는 경우 ShieldMitigationRuleGroup 규칙 그룹 규칙을 관리할 필요가 없습니다. 자동 애플리케이션 레이어 (DDoS) AWS CloudFormation 완화와 함께 사용의 지침을 따르십시오.

자동 완화를 활성화하려면 구성이 필요합니다.

Shield Advanced 자동 완화는 리소스에 대한 애플리케이션 계층 DDoS 보호의 일부로 활성화합니다. 콘솔을 통해 이를 수행하는 방법은 애플리케이션 계층 DDoS 보호 구성 섹션을 참조하세요.

자동 완화 기능을 사용하려면 다음을 수행해야 합니다.

- 웹 ACL을 리소스에 연계 - 이는 모든 Shield Advanced 애플리케이션 계층 보호에 필요합니다. 여러 리소스에 동일한 웹 ACL을 사용할 수 있습니다. 트래픽이 비슷한 리소스에만 이 방법을 사용하는 것이 좋습니다. 여러 리소스와 함께 사용하기 위한 요구 사항을 포함하여 웹 ACL에 대한 자세한 설명은 AWS WAF 작동 방식을 참조하세요.
- Shield Advanced의 자동 애플리케이션 레이어 DDoS 방어 활성화 및 구성 - 이 기능을 활성화하면 Shield Advanced에서 DDoS 공격의 일부로 판단되는 웹 요청을 자동으로 차단 또는 계수할지 여부를 지정합니다. Shield Advanced는 관련 웹 ACL에 규칙 그룹을 추가하고 이를 사용하여 리소스에 대한 DDoS 공격에 대한 대응을 동적으로 관리합니다. 규칙 작업 옵션에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.
- (선택 사항이지만 권장됨) 웹 ACL에 속도 기반 규칙 추가 - 기본적으로 속도 기반 규칙은 개별 IP 주소가 짧은 시간에 너무 많은 요청을 보내는 것을 방지하여 DDoS 공격에 대한 기본적인 리소스 보호

기능을 제공합니다. 맞춤 요청 집계 옵션 및 예를 비롯한 속도 기반 규칙에 대한 자세한 설명은 비율 기반 규칙 문을 참조하세요.

Shield Advanced가 자동 완화를 관리하는 방법

섹션의 주제에서는 Shield Advanced가 자동 애플리케이션 계층 DDoS 완화를 위한 구성 변경을 처리하는 방법과 자동 완화가 활성화된 경우, DDoS 공격을 처리하는 방법을 설명합니다.

주제

- 자동 완화 기능을 활성화하면 발생하는 상황
- Shield Advanced가 자동 방어 기능을 통해 DDoS 공격에 대응하는 방법
- Shield Advanced가 규칙 작업 설정을 관리하는 방법
- 공격이 감소할 때 Shield Advanced가 완화 기능을 관리하는 방법
- 자동 완화 기능을 비활성화하면 발생하는 상황

자동 완화 기능을 활성화하면 발생하는 상황

Shield Advanced는 자동 완화 기능을 활성화하면 다음과 같은 작업을 수행합니다.

- 필요에 따라 Shield Advanced 사용을 위한 규칙 그룹 추가 - 리소스에 연결한 AWS WAF 웹 ACL에 자동 애플리케이션 계층 DDoS 완화 전용 AWS WAF 규칙 그룹 규칙이 아직 없는 경우 Shield Advanced가 규칙을 추가합니다.

  규칙 그룹 규칙의 명칭은 `ShieldMitigationRuleGroup`으로 시작합니다. 규칙 그룹에는 `ShieldKnownOffenderIPRateBasedRule`으로 명명된 속도 기반 규칙이 항상 포함되어 있으며 이는 DDoS 공격의 소스로 알려진 IP 주소의 요청 양을 제한합니다. Shield Advanced 규칙 그룹 및 이를 참조하는 웹 ACL 규칙에 대한 자세한 설명은 Shield Advanced 규칙 그룹을 참조하세요.
- 리소스에 대한 DDoS 공격 대응 시작 - Shield Advanced는 보호된 리소스에 대한 DDoS 공격에 자동으로 대응합니다. Shield Advanced는 항상 존재하는 속도 기반 규칙 외에도 해당 규칙 그룹을 사용하여 DDoS 공격 완화를 위한 사용자 지정 AWS WAF 규칙을 배포합니다. Shield Advanced는 이러한 규칙을 애플리케이션과 애플리케이션에서 발생하는 공격에 맞게 조정하고 배포하기 전에 리소스의 과거 트래픽에 대해 테스트합니다.

Shield Advanced는 자동 완화에 사용하는 모든 웹 ACL에서 단일 규칙 그룹 규칙을 사용합니다. Shield Advanced가 다른 보호 리소스에 대한 규칙 그룹을 이미 추가한 경우 웹 ACL에 다른 규칙 그룹을 추가하지 않습니다.

자동 애플리케이션 계층 DDoS 완화는 공격을 완화하기 위한 규칙 그룹의 존재 여부에 따라 달라집니다. 어떤 이유로든 규칙 그룹이 AWS WAF 웹 ACL에서 제거되는 경우 제거를 통해 웹 ACL과 연결된 모든 리소스에 대한 자동 완화 기능이 비활성화됩니다.

Shield Advanced가 자동 방어 기능을 통해 DDoS 공격에 대응하는 방법

보호된 리소스에 자동 완화를 사용하도록 설정하면 Shield Advanced 규칙 그룹의 속도 기반 규칙 `ShieldKnownOffenderIPRateBasedRule`은(는) 알려진 DDoS 소스로부터 증가하는 트래픽 볼륨에 자동으로 응답합니다. 이 속도 제한은 신속하게 적용되며 공격에 대해 최전선 방어 역할을 합니다.

Shield Advanced는 공격을 탐지하면 다음과 같은 조치를 취합니다.

1. 애플리케이션으로 향하는 일반 트래픽으로부터 공격 트래픽을 분리하는 공격 시그니처를 식별하려고 시도합니다. 목표는 적용 시 공격 트래픽에만 영향을 미치고 애플리케이션에 대한 일반 트래픽에는 영향을 미치지 않는 고품질 DDoS 완화 규칙을 만드는 것입니다.
2. 공격을 받고 있는 리소스는 물론 동일한 웹 ACL과 연계된 다른 모든 리소스의 과거 트래픽 패턴을 기준으로 식별된 공격 시그니처를 평가합니다. Shield Advanced는 이벤트에 대한 응답으로 규칙을 배포하기 전에 이 작업을 수행합니다.

   평가 결과에 따라 Shield Advanced는 다음 중 하나를 수행합니다.

   - Shield Advanced는 공격 시그니처가 DDoS 공격과 관련된 트래픽만 격리한다고 판단하면 웹 ACL의 Shield Advanced 완화 AWS WAF 규칙 그룹에 속하는 규칙에 서명을 구현합니다. Shield Advanced는 리소스의 자동 완화를 위해 구성한 작업 설정(Count 또는 Block)을 이러한 규칙에 제공합니다.
   - 그렇지 않으면 Shield Advanced는 완화 조치를 취하지 않습니다.

공격 내내 Shield Advanced는 기본 Shield Advanced 애플리케이션 계층 보호와 동일한 알림을 보내고 동일한 이벤트 정보를 제공합니다. Shield Advanced 이벤트 콘솔에서 이벤트 및 DDoS 공격에 대한 정보와 공격에 대한 Shield Advanced 완화 조치에 대한 정보를 확인할 수 있습니다. 자세한 설명은 DDoS 이벤트에 대한 가시성을 참조하세요.

Block 규칙 동작을 사용하도록 자동 완화를 구성했는데 Shield Advanced가 배포한 완화 규칙에서 오감지가 발생하는 경우, 규칙 조치를 Count로 변경할 수 있습니다. 이를 위한 방법에 관한 정보는 자동 애플리케이션 계층 DDoS 완화에 사용되는 조치 변경 섹션을 참조하세요.

Shield Advanced가 규칙 작업 설정을 관리하는 방법

자동 완화에 대한 규칙 조치를 Block 또는 Count(으)로 설정할 수 있습니다.

보호된 리소스에 대한 자동 완화 규칙 작업 설정을 변경하면 Shield Advanced는 해당 리소스에 대한 모든 규칙 설정을 업데이트합니다. Shield Advanced 규칙 그룹의 리소스에 대해 현재 적용되는 모든 규칙을 업데이트하고 새 규칙을 생성할 때 새 작업 설정을 사용합니다.

동일한 웹 ACL을 사용하는 리소스의 경우 다른 작업을 지정하는 경우 Shield Advanced는 규칙 그룹의 속도 기반 규칙 `ShieldKnownOffenderIPRateBasedRule`에 대한 Block 작업 설정을 사용합니다. Shield Advanced는 특정 보호 리소스를 대표하여 규칙 그룹에서 다른 규칙을 생성 및 관리하고, 리소스에 대해 지정한 작업 설정을 사용합니다. 웹 ACL의 Shield Advanced 규칙 그룹에 있는 모든 규칙은 모든 관련 리소스의 웹 트래픽에 적용됩니다.

작업 설정 변경 내용이 전파되는 데 몇 초 가량 걸릴 수 있습니다. 이 시간 동안 규칙 그룹이 사용 중인 일부 위치에서는 이전 설정이 표시되고 다른 위치에서는 새 설정이 표시될 수 있습니다.

콘솔의 이벤트 페이지와 애플리케이션 계층 구성 페이지를 통해 자동 완화 구성에 대한 규칙 작업 설정을 변경할 수 있습니다. 이벤트 페이지에 대한 자세한 설명은 DDoS 이벤트에 대한 대응 섹션을 참조하세요. 구성 페이지에 대한 자세한 설명은 애플리케이션 계층 DDoS 보호 구성 섹션을 참조하세요.

공격이 감소할 때 Shield Advanced가 완화 기능을 관리하는 방법

Shield Advanced는 특정 공격에 배포된 완화 규칙이 더 이상 필요하지 않다고 판단되면 Shield Advanced 완화 규칙 그룹에서 해당 완화 규칙을 제거합니다.

완화 규칙이 제거된다고 해서 반드시 공격이 종료되는 시점은 아닙니다. Shield Advanced는 보호된 리소스에서 감지한 공격 패턴을 모니터링합니다. 공격의 초기 발생에 대비하여 배포한 규칙을 그대로 유지함으로써 특정 시그니처를 사용한 공격의 재발을 사전에 방지할 수 있습니다. Shield Advanced는 필요에 따라 규칙을 제자리에 유지하는 시간을 늘립니다. 이렇게 하면 Shield Advanced가 특정 시그니처를 사용한 반복적인 공격이 보호된 리소스에 영향을 미치기 전에 이를 완화할 수 있습니다.

Shield Advanced는 절대 속도 기반 규칙 `ShieldKnownOffenderIPRateBasedRule`을(를) 제거하지 않으며 이는 DDoS 공격의 소스로 알려진 IP 주소의 요청 양을 제한합니다.

자동 완화 기능을 비활성화하면 발생하는 상황

Shield Advanced는 리소스에 대한 자동 완화 기능을 비활성화하면 다음 작업을 수행합니다:

- DDoS 공격에 대한 자동 대응 중지 - Shield Advanced는 해당 리소스에 대한 자동 대응 활동을 중단합니다.
- Shield Advanced 규칙 그룹에서 불필요한 규칙 제거 - Shield Advanced가 보호된 리소스를 대신하여 관리형 규칙 그룹의 규칙을 유지 관리하는 경우, 해당 규칙을 제거합니다.

- 더 이상 사용하지 않는 경우, Shield Advanced 규칙 그룹 제거 - 리소스에 연계한 웹 ACL이 자동 완화가 활성화된 다른 리소스에 연계되지 않은 경우, Shield Advanced는 해당 규칙 그룹 규칙을 웹 ACL에서 제거합니다.

Shield Advanced 규칙 그룹

Shield Advanced는 사용자를 대신하여 소유하고 관리하는 규칙 그룹의 규칙을 사용하여 자동 완화 활동을 관리합니다. Shield Advanced는 보호된 리소스와 연결한 웹 ACL의 규칙을 사용하여 규칙 그룹을 참조합니다.

웹 ACL의 규칙 그룹 규칙

웹 ACL의 Shield Advanced 규칙 그룹 규칙에는 다음과 같은 속성이 있습니다.

- 명칭 – `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- 웹 ACL 용량 단위(WCU) – 150. 이러한 WCU는 웹 ACL의 WCU 사용량에 포함됩니다.

Shield Advanced는 우선순위 설정이 10,000,000인 웹 ACL에서 이 규칙을 생성하여 웹 ACL의 다른 규칙 및 규칙 그룹 이후에 실행되도록 합니다. AWS WAF 가장 낮은 숫자 우선 순위 설정부터 시작하여 웹 ACL의 규칙을 실행합니다. 웹 ACL을 관리하는 동안 이 우선순위 설정은 변경될 수 있습니다.

자동 완화 기능은 웹 ACL에 있는 규칙 그룹에서 사용되는 WCU 외의 계정에서 추가 AWS WAF 리소스를 소비하지 않습니다. 예컨대, Shield Advanced 규칙 그룹은 계정의 규칙 그룹 중 하나로 간주되지 않습니다. 의 계정 한도에 대한 자세한 내용은 AWS WAF을 참조하십시오. AWS WAF 할당량

규칙 그룹의 규칙

참조된 Shield Advanced 규칙 그룹 내에서 Shield Advanced는 속도 기반 규칙 `ShieldKnownOffenderIPRateBasedRule`을(를) 유지하며 이는 DDoS 공격의 소스로 알려진 IP 주소의 요청 양을 제한합니다. 이 규칙은 항상 규칙 그룹에 존재하며 공격을 억제하기 위해 트래픽 패턴 분석에 의존하지 않기 때문에 모든 공격에 대한 1차 방어선 역할을 합니다. 이 규칙의 작업은 규칙 그룹의 다른 규칙과 마찬가지로 자동 완화를 위해 선택한 작업으로 설정됩니다. 속도 기반 규칙에 대한 자세한 내용은 비율 기반 규칙 문 섹션을 참조하세요.

> **Note**
>
> 속도 기반 규칙은 Shield Advanced 이벤트 감지와 독립적으로 `ShieldKnownOffenderIPRateBasedRule` 작동합니다. 자동 완화 기능이 활성화되어 있는 경우 이 규칙 속도는 DDoS 공격의 소스로 알려진 IP 주소를 제한합니다. 이러한 IP 주소의 경

우 규칙의 속도 제한을 통해 공격을 방지하고 Shield Advanced 탐지 정보에 공격이 나타나지 않도록 할 수 있습니다. 이 절충안은 공격 패턴에 대한 완전한 가시성보다 예방에 유리합니다.

위에서 설명한 영구 속도 기반 규칙 외에도 규칙 그룹에는 Shield Advanced가 현재 DDoS 공격을 완화하는 데 사용하고 있는 모든 규칙이 포함되어 있습니다. Shield Advanced는 필요에 따라 이러한 규칙을 추가, 수정 및 제거합니다. 자세한 내용은 Shield Advanced가 자동 완화를 관리하는 방법을 참조하세요.

지표

규칙 그룹은 AWS WAF 지표를 생성하지만 이 규칙 그룹은 Shield Advanced의 소유이므로 이러한 지표를 볼 수 없습니다. 자세한 내용은 AWS WAF 지표 및 차원을(를) 참조하세요.

자동 애플리케이션 계층 DDoS 완화 관리

이 섹션의 지침을 사용하여 자동 애플리케이션 계층 DDoS 완화 구성을 관리하세요. 자동 완화 작동 방식에 대한 자세한 설명은 이전 항목을 참조하세요.

> **Note**
>
> 에 설명된 모범 사례를 따르십시오자동 완화 사용 모범 사례.

주제

- 리소스에 대한 자동 애플리케이션 계층 DDoS 완화 구성 보기
- 자동 애플리케이션 계층 DDoS 완화 활성화 및 비활성화
- 자동 애플리케이션 계층 DDoS 완화에 사용되는 조치 변경
- 자동 애플리케이션 레이어 (DDoS) AWS CloudFormation 완화와 함께 사용

리소스에 대한 자동 애플리케이션 계층 DDoS 완화 구성 보기

보호된 리소스 페이지 및 개별 보호 페이지에서 리소스에 대한 자동 애플리케이션 계층 DDoS 완화 구성을 볼 수 있습니다.

자동 애플리케이션 계층 DDoS 완화 구성을 보려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.

2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다. 보호된 리소스 목록에서 자동 애플리케이션 계층 DDoS 완화 열에는 자동 완화 기능이 활성화되어 있는지 여부와 Shield Advanced가 완화 기능에 사용할 조치가 표시됩니다.

   애플리케이션 계층 리소스를 선택하여 해당 리소스의 보호 페이지에 열거된 것과 동일한 정보를 볼 수도 있습니다.

자동 애플리케이션 계층 DDoS 완화 활성화 및 비활성화

다음 절차에서는 보호된 리소스에 대한 자동 대응을 활성화 또는 비활성화하는 방법을 보여 줍니다.

단일 리소스에 대한 자동 애플리케이션 계층 DDoS 완화를 활성화 또는 비활성화하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.
3. 보호 탭에서 자동 완화를 활성화하려는 애플리케이션 계층 리소스를 선택합니다. 해당 리소스에 대한 보호 페이지가 열립니다.
4. 리소스의 보호 페이지에서 편집을 선택합니다.
5. 글로벌 리소스에 대한 계층 7 DDoS 완화 구성 - 선택 사항 페이지에서 자동 애플리케이션 계층 DDoS 완화에 대해 자동 완화에 사용할 옵션을 선택합니다. 콘솔의 옵션은 다음과 같습니다:

   - 현재 설정 유지 - 보호된 리소스의 자동 완화 설정을 변경하지 않습니다.
   - 활성화 - 보호된 리소스에 대한 자동 완화를 활성화합니다. 이 옵션을 선택하는 경우, 웹 ACL 규칙에서 자동 완화 기능을 사용할 규칙 작업도 선택하십시오. 규칙 작업 설정에 대한 자세한 내용은 규칙 작업 섹션을 참조하세요.

     보호된 리소스에 아직 정상적인 애플리케이션 트래픽 기록이 없는 경우 Shield Advanced가 기준을 설정할 때까지 Count 모드에서 자동 완화 기능을 활성화하세요. Shield Advanced는 웹 ACL을 보호 대상 리소스에 연결할 때 해당 기준에 맞는 정보를 수집하기 시작하며 정상 트래픽의 적절한 기준을 설정하는 데 24시간에서 30일이 소요될 수 있습니다.
   - 비활성화 - 보호된 리소스에 대한 자동 완화를 비활성화합니다.
6. 구성을 완료하고 저장할 때까지 나머지 페이지를 계속 살펴보세요.

보호 페이지에서 리소스에 대한 자동 완화 설정이 업데이트됩니다.

자동 애플리케이션 계층 DDoS 완화에 사용되는 조치 변경

콘솔의 여러 위치에서 Shield Advanced가 애플리케이션 계층 자동 대응에 사용하는 작업을 변경할 수 있습니다.

- 자동 완화 구성 - 리소스에 대한 자동 완화를 구성할 때 조치를 변경하세요. 절차에 대해서는 이전 자동 애플리케이션 계층 DDoS 완화 활성화 및 비활성화 섹션을 참조하세요.
- 이벤트 세부 정보 페이지 - 콘솔에서 이벤트 정보를 볼 때 이벤트 세부 정보 페이지에서 작업을 변경하십시오. 자세한 설명은 AWS Shield Advanced 이벤트 세부 정보을 참조하세요.

웹 ACL을 공유하는 두 개의 보호된 리소스가 있고 둘 중 하나에 대해서는 Count(으)로 작업을 설정하고 다른 하나에 대해서는 Block(으)로 설정한 경우 Shield Advanced는 규칙 그룹의 속도 기반 규칙 `ShieldKnownOffenderIPRateBasedRule`에 대한 작업을 Block(으)로 설정합니다.

자동 애플리케이션 레이어 (DDoS) AWS CloudFormation 완화와 함께 사용

보호 및 웹 AWS CloudFormation ACL을 관리하는 데 사용하는 방법을 이해하세요. AWS WAF

자동 애플리케이션 계층 DDoS 완화 활성화 또는 비활성화

리소스를 사용하여 자동 애플리케이션 레이어 DDoS 완화를 활성화 및 비활성화할 수 있습니다. AWS CloudFormation`AWS::Shield::Protection` 콘솔이나 다른 인터페이스를 통해 기능을 활성화하거나 비활성화할 때와 같은 효과가 나타납니다. AWS CloudFormation 리소스에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 내용을 참조하십시오 AWS::Shield::Protection.

자동 완화 기능과 함께 사용되는 웹 ACL 관리

Shield Advanced는 보호된 리소스의 AWS WAF 웹 ACL에 있는 규칙 그룹 규칙을 사용하여 보호 리소스에 대한 자동 완화를 관리합니다. AWS WAF 콘솔과 API를 통해 웹 ACL 규칙에 규칙이 로 시작하는 이름으로 나열되어 있는 것을 확인할 수 있습니다. `ShieldMitigationRuleGroup` 이 규칙은 자동 애플리케이션 계층 DDoS 완화 전용이며 Shield Advanced 및 AWS WAF에서 관리합니다. 자세한 내용은 Shield Advanced 규칙 그룹 및 Shield Advanced가 자동 완화를 관리하는 방법 섹션을 참조하세요.

를 AWS CloudFormation 사용하여 웹 ACL을 관리하는 경우 Shield Advanced 규칙 그룹 규칙을 웹 ACL 템플릿에 추가하지 마세요. 자동 완화 보호와 함께 사용되는 웹 ACL을 업데이트하면 웹 ACL에서 규칙 그룹 규칙이 AWS WAF 자동으로 관리됩니다.

관리하는 다른 웹 ACL과 비교했을 때 다음과 같은 차이점을 확인할 수 있습니다. AWS CloudFormation

- AWS CloudFormation Shield Advanced 규칙 그룹 규칙을 사용하는 웹 ACL의 실제 구성과 규칙이 없는 웹 ACL 템플릿 사이의 스택 드리프트 상태에 어떠한 드리프트도 보고하지 않습니다. Shield Advanced 규칙은 드리프트 세부 정보의 리소스에 대한 실제 목록에 표시되지 않습니다.

  AWS WAF 콘솔이나 AWS WAF API 등을 통해 검색하는 웹 ACL 목록에서 Shield Advanced 규칙 그룹 규칙을 확인할 수 있습니다. AWS WAF
- 스택에서 웹 ACL 템플릿을 수정하면 Shield Advanced는 업데이트된 웹 ACL에서 Shield Advanced 자동 완화 규칙을 자동으로 유지 관리합니다. AWS WAF Shield Advanced에서 제공하는 자동 완화 보호 기능은 웹 ACL을 업데이트해도 중단되지 않습니다.

AWS CloudFormation 웹 ACL 템플릿에서 Shield Advanced 규칙을 관리하지 마세요. 웹 ACL 템플릿에는 Shield Advanced 규칙이 열거되어서는 안 됩니다. 자동 완화 사용 모범 사례 에서 웹 ACL 관리 모범 사례를 따르십시오.

상태 점검을 사용한 상태 기반 탐지

상태 기반 탐지를 사용하도록 Shield Advanced를 구성하여 공격 탐지 및 완화의 응답성과 정확성을 개선할 수 있습니다. Route 53 호스팅 영역을 제외한 모든 리소스 타입에서 이 옵션을 사용할 수 있습니다.

상태 기반 탐지를 구성하려면 Route 53에서 리소스의 상태 확인을 정의하고 정상으로 보고되는지 확인한 다음 Shield Advanced 보호와 연결합니다. Route 53 상태 확인에 대한 자세한 내용은 Amazon Route 53이 리소스 상태를 확인하는 방법 및 Amazon Route 53 개발자 안내서의 상태 확인 생성, 업데이트 및 삭제 섹션을 참조하세요.

> **Note**
>
> Shield 대응팀(SRT)의 전향적 연계 지원을 위해서는 상태 확인이 필요합니다. 전향적 연계에 대한 자세한 설명은 선제적 대응 구성을 참조하세요.

상태 확인은 사용자가 정의한 요구 사항을 기반으로 리소스의 상태를 측정합니다. 상태 점검 상태는 Shield Advanced 감지 메커니즘에 중요한 입력을 제공하여 특정 애플리케이션의 현재 상태에 대한 민감도를 높입니다.

Route 53 호스팅 영역을 제외한 모든 리소스 유형에 대해 상태 기반 탐지를 활성화할 수 있습니다.

- 네트워크 및 전송 계층(계층 3/계층 4) 리소스 – 상태 기반 탐지는 Network Load Balancer, 탄력적 IP 주소, Global Accelerator 표준 액셀러레이터에 대한 네트워크 계층 및 전송 계층 이벤트 탐지 및 완

화의 정확도를 개선합니다. Shield Advanced로 이러한 리소스 유형을 보호하면 Shield Advanced는 트래픽이 애플리케이션 용량 내에 있는 경우에도 소규모 공격에 대한 완화 기능과 더 빠른 공격 완화를 제공할 수 있습니다.

관련 상태 확인이 비정상인 기간 동안 상태 기반 탐지를 추가하면 Shield Advanced는 훨씬 더 빠르게 더 낮은 임계값으로 위험을 완화할 수 있습니다.

- 애플리케이션 계층 (계층 7) 리소스 — 상태 기반 탐지는 CloudFront 배포 및 애플리케이션 로드 밸런서에 대한 웹 요청 플러드 탐지의 정확도를 개선합니다. Shield Advanced로 이러한 리소스 유형을 보호하면 요청 특성에 따른 트래픽 패턴의 현저한 변화와 함께 트래픽 양에 통계적으로 유의한 편차가 있을 때 웹 요청 flood 감지 알림을 받게 됩니다.

  상태 기반 탐지를 사용하면 연결된 Route 53 상태 확인이 비정상인 기간 동안 Shield Advanced에서 경고에 대한 편차가 더 적어야 하며 이벤트를 더 빠르게 보고합니다. 연결된 Route 53 상태 확인이 정상인 경우 Shield Advanced에서는 경고에 대해 더 큰 편차가 필요합니다.

목차

Shield Advanced의 상태 확인 사용 모범 사례

Shield Advanced를 사용하여 상태 확인을 생성하고 사용할 때는 이 섹션의 모범 사례를 따르십시오.

- 모니터링하려는 인프라 구성 요소를 식별하여 상태 확인을 계획하십시오. 상태 확인을 위해 다음과 같은 리소스 유형을 고려해 보십시오.

  - 중요 리소스
  - Shield Advanced 탐지 및 완화에서 더 높은 민감도를 원하는 모든 리소스.
  - Shield Advanced가 사전에 연락하기를 원하는 리소스. 상태 확인은 상태 확인 상태를 기반으로 선제적 대응에 반영됩니다.

  모니터링할 수 있는 리소스의 예로는 Amazon CloudFront 배포, 인터넷 연결 로드 밸런서, Amazon EC2 인스턴스 등이 있습니다.
- 알림을 최대한 적게 하고 애플리케이션 오리진의 상태를 정확하게 반영하는 상태 확인을 정의하십시오.
  - 애플리케이션을 사용할 수 없거나 허용 가능한 파라미터 내에서 작동하지 않는 경우에만 상태가 좋지 않다고 표시하도록 상태 확인을 작성하십시오. 애플리케이션의 특정 요구 사항에 따라 상태 확인을 정의하고 유지 관리할 책임은 귀하에게 있습니다.
  - 애플리케이션 상태를 정확하게 보고하면서 상태 확인을 최대한 적게 사용하십시오. 예를 들어 애플리케이션의 여러 영역에서 발생하여 모두 동일한 문제를 보고하는 경보가 여러 개 있으면 정보 가치를 추가하지 않고도 대응 활동에 오버헤드가 가중될 수 있습니다.
  - 계산된 상태 확인을 사용하면 Amazon CloudWatch 지표의 조합을 사용하여 애플리케이션 상태를 모니터링할 수 있습니다. 예를 들어 애플리케이션 서버의 지연 시간과 5xx 오류율을 기반으로 종합 상태를 계산할 수 있습니다. 이는 오리진 서버가 요청을 이행하지 않았음을 나타냅니다.
  - 필요에 따라 자체 애플리케이션 상태 지표를 생성하여 CloudWatch 사용자 지정 지표에 게시하고 이를 계산된 상태 점검에 사용하십시오.
- 상태 확인을 구현하고 관리하여 탐지를 개선하고 불필요한 유지 관리 활동을 줄이십시오.
  - 상태 확인을 Shield Advanced 보호와 연결하기 전에 상태가 정상인지 확인하십시오. 비정상으로 보고된 상태 확인을 연결하면 보호 대상 리소스에 대한 Shield Advanced 탐지 메커니즘이 왜곡될 수 있습니다.
  - Shield Advanced에서 건강 검진을 계속 사용할 수 있도록 하십시오. Shield Advanced 보호를 위해 사용 중인 Route 53의 상태 확인을 삭제하지 마십시오.
  - 스테이징 및 테스트 환경은 상태 확인을 테스트하는 용도로만 사용하십시오. 프로덕션 수준의 성능과 가용성이 필요한 환경에 대해서만 상태 확인 연결을 유지하십시오. 스테이징 및 테스트 환경을 위해 Shield Advanced에서 상태 확인 연결을 유지하지 마십시오.

상태 확인에 일반적으로 사용되는 측정치

이 섹션에는 DDoS (분산 서비스 거부) 이벤트 중 애플리케이션 상태를 측정하기 위해 상태 확인에 일반적으로 사용되는 Amazon CloudWatch 지표가 나열되어 있습니다. 각 리소스 유형의 CloudWatch 지표에 대한 자세한 내용은 표 다음에 나오는 목록을 참조하십시오.

주제

- 애플리케이션 상태 모니터링에 사용하는 지표
- 각 리소스 유형에 대한 Amazon CloudWatch 메트릭

애플리케이션 상태 모니터링에 사용하는 지표

Resource	지표	설명
Route 53	`HealthCheckStatus`	상태 확인 엔드포인트의 상태입니다.
CloudFront	`5xxErrorRate`	HTTP 상태 코드가 5xx인 모든 요청의 백분율입니다. 이는 애플리케이션에 영향을 미치는 공격을 나타냅니다.
Application Load Balancer	`HTTPCode_ELB_5XX_Count`	로드 밸런서에서 생성된 HTTP 5xx 클라이언트 오류 코드 수입니다.
Application Load Balancer	`RejectedConnectionCount`	로드 밸런서가 최대 연결 수에 도달하여 거부된 연결 수.
Application Load Balancer	`TargetConnectionErrorCount`	로드 밸런서와 대상 사이에 성공적으로 구성되지 않은 연결 수.
Application Load Balancer	`TargetResponseTime`	로드 밸런서에서 요청 신호를 전송한 후 대상에서 응답 신호가 수신될 때까지 경과된 시간(초).

Resource	지표	설명
Application Load Balancer	`UnHealthyHostCount`	비정상 상태로 간주되는 대상 수.
Amazon EC2	`CPUUtilization`	현재 사용 중인 할당된 EC2 컴퓨팅 유닛(ECU)의 비율(%).

각 리소스 유형에 대한 Amazon CloudWatch 메트릭

보호 대상 리소스에 사용할 수 있는 지표에 대한 추가 정보는 리소스 가이드의 다음 섹션을 참조하세요.

- Amazon Route 53 — Amazon Route 53 개발자 안내서의 Amazon Route 53 상태 점검 및 Amazon을 사용하여 리소스를 모니터링합니다. CloudWatch
- Amazon CloudFront — Amazon CloudFront 개발자 안내서에서 CloudWatchAmazon을 CloudFront 통한 모니터링.
- 애플리케이션 로드 밸런서 — 애플리케이션 로드 밸런서 사용 설명서에 있는 애플리케이션 로드 밸런서에 대한 CloudWatch 메트릭입니다.
- Network Load Balancer — 네트워크 로드 밸런서 사용 설명서에 나와 있는 Network Load Balancer에 대한 CloudWatch 메트릭입니다.
- AWS Global Accelerator — AWS Global Accelerator 개발자 CloudWatch 안내서와 함께 AWS Global Accelerator Amazon 사용하기.
- Amazon Elastic Compute Cloud — https://docs.aws.amazon.com/ AWSEC UserGuide 2/latest/ /에 인스턴스에 사용할 수 있는 CloudWatch 메트릭을 나열하십시오.
- Amazon EC2 Auto Scaling — Amazon EC2 Auto Scaling 사용 설명서에서 Auto Scaling 그룹 및 인스턴스에 대한 CloudWatch 지표를 모니터링합니다.

상태 확인

애플리케이션이 허용 가능한 파라미터 내에서 실행될 때만 상태 확인이 정상이라고 보고하고, 그렇지 않을 때는 비정상이라고 보고하는 경우 Shield Advanced의 상태 확인을 사용하면 가장 큰 이점을 얻을 수 있습니다. 이 섹션의 지침을 사용하여 Shield Advanced에서 상태 확인 연결을 관리합니다.

> **Note**
>
> Shield Advanced는 상태 확인을 자동으로 관리하지 않습니다.

Shield Advanced에서 상태 확인을 사용하려면 다음이 필요합니다.

- 상태 확인을 Shield Advanced 보호와 연결하면 정상 상태로 보고되어야 합니다.
- 상태 확인은 보호 대상 리소스의 상태와 관련이 있어야 합니다. 애플리케이션의 특정 요구 사항에 따라 애플리케이션 상태를 정확하게 보고하는 상태 확인을 정의하고 유지 관리할 책임이 있습니다.
- 상태 확인은 Shield Advanced 보호 기능을 통해 계속 사용할 수 있어야 합니다. Shield Advanced 보호를 위해 사용 중인 Route 53의 상태 확인을 삭제하지 마십시오.

주제

상태 확인을 리소스와 연결하기

다음 절차에서는 Amazon Route 53 상태 확인을 보호된 리소스와 연결하는 방법을 보여줍니다.

> **Note**
>
> 상태 확인을 Shield Advanced 보호와 연결하기 전에 상태가 정상인지 확인하십시오. 자세한 내용은 Amazon Route 53 개발자 안내서의 상태 확인 상태 모니터링 및 알림 받기 섹션을 참조하세요.

상태 확인

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.
3. 보호 탭에서 상태 확인과 연결할 리소스를 선택합니다.

4. 보호 구성을 선택합니다.
5. 상태 확인 기반 DDoS 탐지 구성 - 선택 사항 페이지가 표시될 때까지 다음을 선택합니다.
6. 연계된 상태 체크에서 보호와 연계하려는 상태 체크의 ID를 선택합니다.

> **Note**
>
> 필요한 상태 체크가 보이지 않으면 Route 53 콘솔로 이동하여 상태 체크와 해당 ID를 확인하십시오. 자세한 내용은 상태 확인 생성 및 업데이트 섹션을 참조하세요.

7. 구성을 완료할 때까지 나머지 페이지를 살펴보십시오. 보호 페이지에는 리소스에 대한 업데이트된 상태 확인 연결이 나열되어 있습니다.
8. 보호 페이지에서 새로 연결된 상태 확인이 정상으로 보고되고 있는지 확인합니다.

   상태 확인이 비정상으로 보고되는 동안에는 Shield Advanced의 상태 확인 사용을 성공적으로 시작할 수 없습니다. 이렇게 하면 Shield Advanced가 매우 낮은 임계값에서 오탐지를 감지하고 Shield 대응 팀(SRT)이 리소스에 대한 선제적 대응을 제공하는 능력에도 부정적인 영향을 미칠 수 있습니다.

   새로 연결된 상태 확인이 비정상으로 보고되면 다음과 같이 하십시오.

   a. Shield Advanced의 상태 확인과 보호 기능을 분리하십시오.
   b. Amazon Route 53의 상태 확인 사양을 다시 살펴보고 전반적인 애플리케이션 성능 및 가용성을 확인하십시오.
   c. 애플리케이션이 정상 상태 파라미터 내에서 수행되고 상태 확인이 정상으로 보고되면 Shield Advanced에서 상태 확인을 다시 연결해 보십시오.

새 상태 확인 연결을 설정하고 Shield Advanced에서 정상 상태를 보고하면 상태 확인 연결 절차가 완료됩니다.

리소스에서 상태 확인 연결을 해제하기

다음 절차는 Amazon Route 53 상태 확인과 보호된 리소스의 연결을 해제하는 방법을 보여줍니다.

상태 확인 연결을 해제하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.

3. 보호 탭에서 상태 확인에서 연결을 해제할 리소스를 선택합니다.
4. 보호 구성을 선택합니다.
5. 상태 확인 기반 DDoS 탐지 구성 - 선택 사항 페이지가 표시될 때까지 다음을 선택합니다.
6. 연결된 상태 확인에서 -로 표시된 빈 옵션을 선택합니다.
7. 구성을 완료할 때까지 나머지 페이지를 살펴보십시오.

보호 페이지에서 리소스의 상태 확인 필드는 -로 설정되어 있으며, 이는 상태 확인 연결이 없음을 나타냅니다.

상태 확인 연결 상태

AWS WAF 및 Shield 콘솔 보호 리소스 페이지 및 각 리소스의 세부 정보 페이지에서 보호와 관련된 상태 확인 상태를 확인할 수 있습니다.

- 정상 – 상태 확인을 사용할 수 있으며 정상으로 보고됩니다.
- 비정상 – 상태 확인을 사용할 수 있으며 비정상으로 보고됩니다.
- 사용 불가 – Shield Advanced에서 상태 확인을 사용할 수 없습니다 .

사용 불가 상태 확인 문제를 해결하려면

새 상태 확인을 생성하여 사용하십시오. Shield Advanced에서 상태 확인을 사용할 수 없는 상태가 된 후에는 다시 연결을 시도하지 마십시오.

이러한 단계를 수행하는 방법에 대한 자세한 지침은 이전 항목을 참조하세요.

1. Shield Advanced에서, 리소스에서 상태 확인의 연결을 해제합니다.
2. Route 53에서, 리소스에 대한 새 상태 확인을 생성하고 해당 ID를 기록해 둡니다. 자세한 내용은 Amazon Route 53 개발자 안내서의 상태 확인 생성 및 업데이트 섹션을 참조하세요.
3. Shield Advanced에서, 새 상태 확인을 리소스에 연결합니다.

상태 확인 예시

이 섹션에서는 계산된 상태 확인에 사용할 수 있는 상태 확인의 예시를 보여줍니다. 계산된 상태 확인은 여러 개별 상태 확인을 사용하여 통합 상태를 결정합니다. 각 개별 상태 확인의 상태는 엔드포인트의 상태 또는 Amazon CloudWatch 지표의 상태를 기반으로 합니다. 상태 확인을 계산된 상태 확인으로 결합한 다음 개별 상태 확인의 통합 상태를 기반으로 상태를 보고하도록 계산된 상태 확인을 구성합

니다. 애플리케이션 성능 및 가용성에 대한 요구 사항에 따라 계산된 상태 확인의 민감도를 조정하십시오.

계산된 상태 확인에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 기타 상태 확인(계산된 상태 확인) 모니터링 섹션을 참조하세요. 자세한 내용은 블로그 게시물 Route 53 개선 사항 – 계산된 상태 확인 및 지연 시간 검사 섹션을 참조하세요.

주제

- 아마존 CloudFront 디스트리뷰션
- 로드 밸런서
- Amazon EC2 탄력적 IP 주소(EIP)

아마존 CloudFront 디스트리뷰션

다음 예는 CloudFront 배포의 계산된 상태 확인에 결합할 수 있는 상태 확인을 설명합니다.

- 동적 콘텐츠를 제공하는 배포의 경로에 도메인 이름을 지정하여 엔드포인트를 모니터링합니다. 정상 응답에는 HTTP 응답 코드 2xx 및 3xx가 포함됩니다.
- CloudFront 오리진의 상태를 측정하는 CloudWatch 알람 상태를 모니터링하세요. 예를 들어 Application Load Balancer `TargetResponseTime` 지표에서 CloudWatch 경보를 유지 관리하고 경보 상태를 반영하는 상태 점검을 생성할 수 있습니다. 요청이 로드 밸런서에서 나가는 시점부터 로드 밸런서가 대상으로부터 응답을 받을 때까지의 응답 시간이 경보에 구성된 임계값을 초과할 경우, 상태 확인이 비정상적일 수 있습니다.
- 응답의 HTTP 상태 코드가 5xx인 요청의 비율을 측정하는 CloudWatch 경보 상태를 모니터링합니다. CloudFront 배포의 5xx 오류율이 CloudWatch 경보에 정의된 임계값보다 높으면 이 상태 점검의 상태가 비정상으로 전환됩니다.

로드 밸런서

다음 예시에서는 Application Load Balancer, Network Load Balancer 또는 Global Accelerator 표준 액셀러레이터의 계산된 상태 확인에 사용할 수 있는 상태 확인에 사용할 수 있는 상태 확인에 대해 설명합니다.

- 클라이언트가 로드 밸런서에 설정한 새 연결 수를 측정하는 CloudWatch 경보 상태를 모니터링합니다. 평균 신규 연결 수에 대한 경보 임계값을 일일 평균보다 어느 정도 높게 설정할 수 있습니다. 각 리소스 유형의 지표는 다음과 같습니다.
  - Application Load Balancer: `NewConnectionCount`

  - Network Load Balancer: `ActiveFlowCount`
  - Global Accelerator: `NewFlowCount`
- Application Load Balancer 및 Network Load Balancer의 경우 CloudWatch 정상으로 간주되는 로드 밸런서의 수를 측정하는 경보 상태를 모니터링하십시오. 가용 영역 또는 로드 밸런서에 필요한 정상 호스트의 최소 수에 대해 경보 임계값을 설정할 수 있습니다. 로드 밸런서 리소스에 사용할 수 있는 지표는 다음과 같습니다.
  - Application Load Balancer: `HealthyHostCount`
  - Network Load Balancer: `HealthyHostCount`
- Application Load Balancer의 경우 로드 밸런서 대상에서 생성된 HTTP 5xx 응답 코드 수를 측정하는 CloudWatch 경보 상태를 모니터링합니다. Application Load Balancer의 경우 지표 `HTTPCode_Target_5XX_Count`을(를) 사용하고 로드 밸런서에 대한 모든 5xx 오류의 합계를 기준으로 경보 임계값을 설정할 수 있습니다.

Amazon EC2 탄력적 IP 주소(EIP)

다음 예시의 상태 확인을 Amazon EC2 탄력적 IP 주소의 계산된 상태 확인에 결합할 수 있습니다.

- 탄력적 IP 주소에 IP 주소를 지정하여 엔드포인트를 모니터링합니다. IP 주소를 기반으로 하는 리소스와 TCP 연결을 설정할 수 있는 한 상태 확인은 정상적으로 유지됩니다.
- 인스턴스에서 현재 사용 중인 할당된 Amazon EC2 컴퓨팅 유닛의 비율을 측정하는 CloudWatch 경보 상태를 모니터링합니다. Amazon EC2 지표 `CPUUtilization`을(를) 사용하고 애플리케이션의 CPU 사용률이 높다고 생각하는 비율(예: 90%)을 기준으로 경보 임계값을 설정할 수 있습니다.

에서 리소스 보호 관리 AWS Shield Advanced

이 섹션의 지침을 사용하여 리소스에 대한 Shield Advanced 보호를 관리하십시오.

> **Note**
>
> 쉴드 어드밴스드는 쉴드 어드밴스드 또는 쉴드 어드밴스드 정책을 통해 지정한 리소스만 보호합니다. AWS Firewall Manager 이 기능은 리소스를 자동으로 보호하지 않습니다.

AWS Firewall Manager Shield Advanced 정책을 사용하는 경우 정책 범위 내에 있는 리소스에 대한 보호를 관리할 필요가 없습니다. Firewall Manager는 정책 구성에 따라 정책 범위 내에 있는 계정 및 리소스에 대한 보호를 자동으로 관리합니다. 자세한 정보는 AWS Shield Advanced 정책을 참조하세요.

주제

리소스에 AWS Shield AdvancedAWS 보호 추가

이 섹션의 지침에 따라 하나 이상의 리소스에 Shield Advanced 보호를 추가하십시오.

AWS 리소스에 대한 보호를 추가하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. 탐색 창에서 보호된 리소스를 AWS Shield 선택합니다.
3. 보호할 리소스 추가를 선택합니다.
4. Shield Advanced로 보호할 리소스 선택 페이지의 지역 및 리소스 타입 지정에서 보호하려는 리소스에 대해 지역 및 리소스 타입 사양을 제공합니다. 모든 지역을 선택하여 여러 지역의 리소스를 보호할 수 있으며, 글로벌을 선택하여 글로벌 리소스로 선택 범위를 좁힐 수 있습니다. 보호하지 않으려는 모든 리소스 타입을 선택 취소할 수 있습니다. 리소스 타입의 보호에 대한 자세한 설명은 AWS Shield Advanced 리소스 유형별 보호을 참조하세요.
5. 리소스 로딩을 선택합니다. Shield Advanced는 리소스 선택 섹션을 기준에 맞는 AWS 리소스로 채웁니다.
6. 리소스 선택 섹션에서, 리소스 목록에서 검색할 문자열을 입력하여 리소스 목록을 필터링할 수 있습니다.

   보호할 리소스를 선택합니다.
7. 태그 섹션에서 생성 중인 Shield Advanced 보호에 태그를 추가하려면 해당 태그를 지정하세요. AWS 리소스 태그 지정에 대한 자세한 설명은 태그 편집기 작업을 참조하세요.
8. Shield Advanced로 보호하기를 선택하세요. 이렇게 하면 리소스에 Shield Advanced 보호 기능이 추가됩니다.

AWS Shield Advanced 보호 구성

언제든지 AWS Shield Advanced 보호 설정을 변경할 수 있습니다. 이렇게 하려면 선택된 보호 옵션을 살펴본 후 변경해야 하는 설정을 수정합니다.

보호된 리소스를 관리하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.
3. 보호 탭에서 보호할 리소스를 선택합니다.
4. 보호 구성 및 원하는 리소스 사양 옵션을 선택합니다.
5. 각 리소스 보호 옵션을 살펴보면서 필요에 따라 변경하십시오.

애플리케이션 계층 DDoS 보호 구성

Amazon CloudFront 및 Application Load Balancer 리소스에 대한 공격으로부터 보호하기 위해 AWS WAF 웹 ACL을 추가하고 속도 기반 규칙을 추가할 수 있습니다. 이에 대한 자세한 내용은 Shield Advanced 애플리케이션 레이어 AWS WAF 웹 ACL 및 요금 기반 규칙 섹션을 참조하세요.

또한 Shield Advanced에 자동 애플리케이션 계층 DDoS 완화를 활성화할 수 있습니다. 작동 방식에 AWS WAF 대한 자세한 내용은 을 참조하십시오. AWS WAF 자동 완화 기능에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화을 참조하세요.

> **Important**
>
> Shield Advanced 정책을 AWS Firewall Manager 사용하여 Shield Advanced 보호를 관리하는 경우 여기에서 애플리케이션 계층 보호를 관리할 수 없습니다. 모든 다른 자원의 경우, 웹 ACL에 규칙이 포함되어 있지 않더라도 각 리소스에 웹 ACL을 적어도 하나 연결하는 것이 좋습니다.

> **Note**
>
> 리소스에 대한 자동 애플리케이션 계층 DDoS 완화를 활성화하면 필요한 경우 작업이 계정에 서비스 연결 역할을 자동으로 추가하여 Shield Advanced에 웹 ACL 보호를 관리하는 데 필요한 권한을 부여합니다. 자세한 내용은 Shield Advanced에 대한 서비스 연결 역할 사용을 참조하세요.

애플리케이션 계층 DDoS 보호를 구성하려면

1. 계층 7 DDoS 보호 구성 페이지에서 리소스가 아직 웹 ACL과 연결되어 있지 않은 경우 기존 웹 ACL을 선택하거나 직접 만들 수 있습니다.

   웹 ACL을 생성하려면 아래 단계를 따르십시오.

   a. Create web ACL(웹 ACL 생성)을 선택합니다.
   b. 명칭을 입력합니다. 웹 ACL을 생성한 후에는 명칭을 변경할 수 없습니다.
   c. 생성을 선택하세요.

   > **Note**
   >
   > 리소스가 이미 웹 ACL과 연결되어 있으면 다른 웹 ACL로 변경할 수 없습니다. 웹 ACL을 변경하려면 먼저 연결된 웹 ACL을 리소스에서 제거해야 합니다. 자세한 내용은 웹 ACL을 리소스와 연결 또는 연결 해제 AWS을 참조하세요.

2. 웹 ACL에 속도 기반 규칙이 정의되어 있지 않은 경우 속도 제한 규칙 추가를 선택하고 다음 단계를 수행하여 속도 기반 규칙을 추가할 수 있습니다.

   a. 명칭을 입력합니다.
   b. 비율 제한을 입력합니다. 이 값은 속도 기반 규칙 작업이 IP 주소에 적용되기 전, 단일 IP 주소에서 5분 동안 허용되는 최대 요청 수를 말합니다. IP 주소의 요청이 한도 아래로 떨어지면 작업이 중단됩니다.
   c. 요청 수가 제한을 초과하는 동안 IP 주소의 요청을 계산하거나 차단하도록 규칙 작업을 설정합니다. 규칙 적용 및 제거 조치는 IP 주소 요청 비율이 변경된 후 1~2분 후에 적용될 수 있습니다.
   d. 규칙 추가를 선택합니다.

3. 자동 애플리케이션 계층 DDoS 완화에 대해 다음과 같이 Shield Advanced가 사용자 대신 DDoS 공격을 자동으로 완화하도록 할지 여부를 선택합니다.

   - 자동 완화를 활성화하려면 [Enable] 을 선택한 다음 Shield Advanced가 사용자 지정 규칙에서 사용할 AWS WAF 규칙 작업을 선택합니다. 선택할 수 있는 옵션은 Count 및 Block입니다. 이러한 AWS WAF 규칙 조치에 대한 자세한 내용은 을 참조하십시오규칙 작업. Shield Advanced가 이 작업 설정을 관리하는 방법에 대한 자세한 내용은 Shield Advanced가 규칙 작업 설정을 관리하는 방법을(를) 참조하세요.
   - 자동 완화 기능을 비활성화하려면 비활성화를 선택합니다.

- 관리 중인 리소스의 자동 완화 설정을 변경하지 않고 그대로 두려면 기본 선택인 현재 설정 유지를 그대로 두십시오.

Shield Advanced 자동 애플리케이션 계층 DDoS 완화에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화을 참조하세요.

4. 다음을 선택합니다.

경보 및 알림 생성

다음 절차는 보호된 리소스에 대한 CloudWatch 경보를 관리하는 방법을 보여줍니다.

> **Note**
>
> CloudWatch 추가 비용이 발생합니다. CloudWatch 요금은 Amazon CloudWatch 요금을 참조하십시오.

경보 및 알림을 생성하려면

1. 경보 및 알림 생성 - 선택 사항 보호 페이지에서 수신할 경보 및 알림에 대한 SNS 주제를 구성합니다. 알림을 받지 않으려는 리소스의 경우 주제 없음을 선택합니다. Amazon SNS 주제를 추가하거나 새로운 주제를 생성할 수 있습니다.
2. Amazon SNS 주제를 생성하려면 아래 단계를 따르십시오.
   a. 드롭다운 목록에서 SNS 주제 생성을 선택합니다.
   b. 주제 이름을 입력합니다.
   c. 선택 사항으로 Amazon SNS 메시지를 수신할 이메일 주소를 입력한 후 이메일 추가를 선택합니다. 하나 이상을 입력할 수 있습니다.
   d. 생성을 선택하세요.
3. 다음을 선택합니다.

AWS 리소스에서 AWS Shield Advanced 보호 제거

언제든지 모든 AWS 리소스에서 AWS Shield Advanced 보호를 제거할 수 있습니다.

> **Important**
>
> 리소스를 삭제해도 AWS 리소스는 제거되지 않습니다 AWS Shield Advanced. 또한 이 절차에 설명된 대로 에서 AWS Shield Advanced리소스에 대한 보호를 제거해야 합니다.

AWS 리소스에서 AWS Shield Advanced 보호 제거

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.
3. 보호 탭에서 보호를 제거하려는 리소스를 선택합니다.
4. 삭제 보호를 선택합니다.
   - 보호를 위해 Amazon CloudWatch 경보가 구성된 경우 보호와 함께 경보를 삭제할 수 있는 옵션이 제공됩니다. 이때 경보를 삭제하지 않기로 선택한 경우 CloudWatch 콘솔을 사용하여 나중에 삭제할 수 있습니다.

> **Note**
>
> Amazon Route 53 상태 확인이 구성된 보호의 경우 나중에 보호를 다시 추가하면 보호에 상태 확인이 포함됩니다.

이전 단계는 특정 AWS 리소스의 AWS Shield Advanced 보호를 제거합니다. AWS Shield Advanced 구독을 취소하지는 않습니다. 서비스 요금은 계속 청구됩니다. AWS Shield Advanced 구독에 대한 자세한 내용은 AWS Support 센터에 문의하세요.

Shield Advanced 보호 기능에서 CloudWatch 알람 제거하기

Shield Advanced 보호 기능에서 CloudWatch 경보를 제거하려면 다음 중 하나를 수행하십시오.

- AWS 리소스에서 AWS Shield Advanced 보호 제거에서 설명하는 대로 보호를 삭제합니다. 이때 Also delete related DDoSDetection alarm(관련 DDoSDetection 경보도 삭제) 옆에 있는 확인란을 반드시 선택해야 합니다.
- CloudWatch 콘솔을 사용하여 알람을 삭제합니다. 삭제할 알람 이름은 DetectedAlarmForProtectionDDoS로 시작합니다.

AWS Shield Advanced 보호 그룹

보호 그룹을 사용하면 보호된 리소스의 논리적 컬렉션을 만들고 보호를 그룹으로 관리할 수 있습니다. 리소스 보호 관리에 대한 자세한 정보는 AWS Shield Advanced 보호 구성 섹션을 참조하세요.

> **Note**
>
> 자동 애플리케이션 계층 DDoS 완화는 보호 그룹과 상호 작용하지 않습니다. 보호 그룹에 있는 리소스에 대해 자동 완화를 활성화할 수 있지만 Shield Advanced는 보호 그룹 결과에 근거하여 공격 완화를 자동으로 적용하지 않습니다. Shield Advanced는 개별 리소스에 대한 자동 공격 완화 기능을 적용합니다.

AWS Shield Advanced 보호 그룹은 여러 개의 보호된 리소스를 단일 단위로 취급하여 탐지 및 완화 범위를 사용자 지정할 수 있는 셀프 서비스 방법을 제공합니다. 리소스 그룹화는 여러 가지 이점을 제공할 수 있습니다.

- 탐지 정확도를 개선하십시오.
- 실행 불가능한 이벤트 알림을 줄이십시오.
- 이벤트 중에 영향을 받을 수도 있는 보호 리소스를 포함하도록 완화 조치의 적용 범위를 늘리십시오.
- 유사한 표적이 여러 개 있는 공격을 완화하는 데 걸리는 시간을 단축하십시오.
- 새로 생성된 보호 리소스의 자동 보호를 촉진합니다.

보호 그룹은 리소스가 0에 가까운 부하와 완전히 로드된 상태 사이에서 번갈아 나타나는 블루/그린 스왑과 같은 상황에서 오탐지를 줄이는 데 도움이 될 수 있습니다. 또 다른 예로 그룹 구성원 간에 공유되는 부하 수준을 유지하면서 리소스를 자주 만들고 삭제하는 경우를 들 수 있습니다. 이러한 상황에서 개별 리소스를 모니터링하면 오탐지가 발생할 수 있지만 리소스 그룹의 상태를 모니터링하면 그렇지 않을 수 있습니다.

모든 보호된 리소스, 특정 리소스 유형의 모든 리소스 또는 개별적으로 지정된 리소스를 포함하도록 보호 그룹을 구성할 수 있습니다. 보호 그룹 기준을 충족하는 새로 보호된 리소스는 보호 그룹에 자동으로 포함됩니다. 보호된 리소스는 다중 보호 그룹에 속할 수 있습니다.

AWS Shield Advanced 보호 그룹 관리

이 섹션의 지침을 사용하여 보호 그룹 구성을 관리하십시오.

Shield Advanced 보호 그룹 생성

보호 그룹을 생성하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.
3. 보호 그룹 탭을 선택한 다음, 보호 그룹 만들기를 선택합니다.
4. 보호 그룹 만들기 페이지에서 그룹 이름을 입력합니다. 이 이름을 사용하여 보호된 리소스 목록에 있는 그룹을 식별할 수 있습니다. 보호 그룹을 생성한 후에는 해당 이름을 변경할 수 없습니다.
5. 보호 그룹화 기준의 경우, Shield Advanced가 그룹에 포함할 보호된 리소스를 식별하는 데 사용할 기준을 선택합니다. 선택한 기준에 따라 추가 항목을 선택합니다.
6. 집계의 경우, Shield Advanced가 그룹의 리소스 데이터를 결합하여 이벤트를 탐지, 완화 및 보고하는 방법을 선택합니다.
   - 합계 – 그룹 전체의 총 트래픽을 사용합니다. 대부분의 경우에서 이 방법을 선택하는 것이 좋습니다. 수동 또는 자동으로 확장되는 Amazon EC2 인스턴스의 탄력적 IP 주소를 예로 들 수 있습니다.
   - 평균 – 그룹 전체 트래픽의 평균을 사용합니다. 트래픽을 균일하게 공유하는 리소스에 적합합니다. 액셀러레이터와 로드 밸런서를 예로 들 수 있습니다.
   - 최대 – 각 리소스에서 가장 많은 트래픽을 사용합니다. 이는 트래픽을 공유하지 않는 리소스와 불균일한 방식으로 트래픽을 공유하는 리소스에 유용합니다. Amazon CloudFront 배포판 및 CloudFront 배포용 오리진 리소스를 예로 들 수 있습니다.
7. 저장을 선택하여 보호 그룹을 저장하고 보호된 리소스 페이지로 돌아가십시오.

Shield 이벤트 페이지에서 보호 그룹에 대한 이벤트를 보고 그룹에 있는 보호 리소스에 대한 추가 정보를 드릴다운하여 볼 수 있습니다.

Shield Advanced 보호 그룹 업데이트

보호 그룹을 업데이트하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.
3. 보호 그룹 탭에서 수정할 보호 그룹 옆의 확인란을 선택합니다.

4. 보호 그룹 페이지에서 편집을 선택합니다. 보호 그룹 설정을 변경합니다.
5. 저장을 선택하여 변경 사항을 저장합니다.

Shield Advanced 보호 그룹 삭제

보호 그룹을 삭제하려면

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 보호된 리소스를 선택합니다.
3. 보호 그룹 탭에서 제거할 보호 그룹 옆의 확인란을 선택합니다.
4. 보호 그룹 페이지에서 삭제를 선택하고 작업을 확인합니다.

에서 리소스 보호 변경 내용 추적 AWS Config

를 사용하여 리소스 AWS Shield Advanced 보호 변경 사항을 기록할 수 AWS Config있습니다. 그런 다음 감사 및 문제 해결을 목적으로 이 정보를 사용해 구성 변경 이력을 유지할 수 있습니다.

보호 변경 사항을 기록하려면 추적하려는 각 리소스에 AWS Config 대해 활성화하십시오. 자세한 내용은 AWS Config 개발자 안내서에서 AWS Config시작하기를 참조하세요.

추적된 리소스가 AWS 리전 포함된 각 리소스에 AWS Config 대해 활성화해야 합니다. AWS Config 수동으로 활성화하거나 사용 AWS CloudFormation 설명서의AWS CloudFormation StackSets 샘플 AWS CloudFormation 템플릿에서 “활성화 AWS Config" 템플릿을 사용할 수 있습니다.

AWS Config활성화하면 AWS Config 가격 페이지에 설명된 대로 요금이 부과됩니다.

> **Note**
>
> 필요한 지역 및 리소스를 이미 AWS Config 활성화한 경우 별도의 조치를 취하지 않아도 됩니다. AWS Config 리소스의 보호 변경과 관련된 로그가 자동으로 채워지기 시작합니다.

AWS Config활성화한 후에는 AWS Config 콘솔에서 미국 동부 (버지니아 북부) 지역을 사용하여 AWS Shield Advanced 글로벌 리소스의 구성 변경 기록을 볼 수 있습니다.

AWS Config 콘솔을 통해 미국 동부 (버지니아 북부), 미국 동부 (오하이오), 미국 서부 (오레곤), 미국 서부 (캘리포니아 북부), 유럽 (아일랜드), 유럽 (프랑크푸르트), 아시아 태평양 (시드니) 지역의 AWS Shield Advanced 지역 리소스 변경 기록을 볼 수 있습니다.

DDoS 이벤트에 대한 가시성

AWS Shield 다음과 같은 범주의 이벤트 및 이벤트 활동에 대한 가시성을 제공합니다.

- 글로벌 — 모든 고객이 지난 2주간의 글로벌 위협 활동을 집계하여 볼 수 있습니다. AWS Shield 콘솔의 시작하기 및 글로벌 위협 대시보드 페이지에서 이 정보를 확인할 수 있습니다. 자세한 정보는 AWS Shield 글로벌 및 계정 활동을 참조하세요.
- 계정 - 모든 고객은 해당 계정의 전년도 이벤트 요약에 액세스할 수 있습니다. AWS Shield 콘솔의 시작하기 페이지에서 이 정보를 확인할 수 있습니다. 자세한 정보는 AWS Shield 글로벌 및 계정 활동을 참조하세요.

Shield Advanced를 구독하고 리소스에 대한 보호를 추가하면 보호되는 리소스의 이벤트 및 DDoS 공격에 대한 추가 정보에 액세스할 수 있습니다.

- 보호된 리소스의 이벤트 — Shield Advanced는 AWS Shield 콘솔의 이벤트 페이지를 통해 각 이벤트에 대한 자세한 정보를 제공합니다. 자세한 정보는 AWS Shield Advanced 행사을 참조하세요.
- 보호 대상 리소스에 대한 이벤트 지표 — Shield Advanced는 보호하는 모든 리소스에 대한 탐지, 완화 및 상위 기여자 CloudWatch Amazon 지표를 게시합니다. 이러한 지표를 사용하여 CloudWatch 대시보드와 경보를 구성할 수 있습니다. 자세한 정보는 AWS Shield Advanced 측정 항목을 참조하세요.
- 보호된 리소스에 대한 계정 간 이벤트 가시성 — Shield Advanced 보호를 관리하는 AWS Firewall Manager 데 사용하는 경우 Firewall Manager와 함께 사용하면 여러 계정의 보호 기능을 가시적으로 파악할 수 있습니다. AWS Security Hub자세한 정보는 계정 전반에 걸친 이벤트 가시성을 참조하세요.

애플리케이션 계층 보호를 위해 자동 애플리케이션 계층 DDoS 완화를 활성화하는 경우

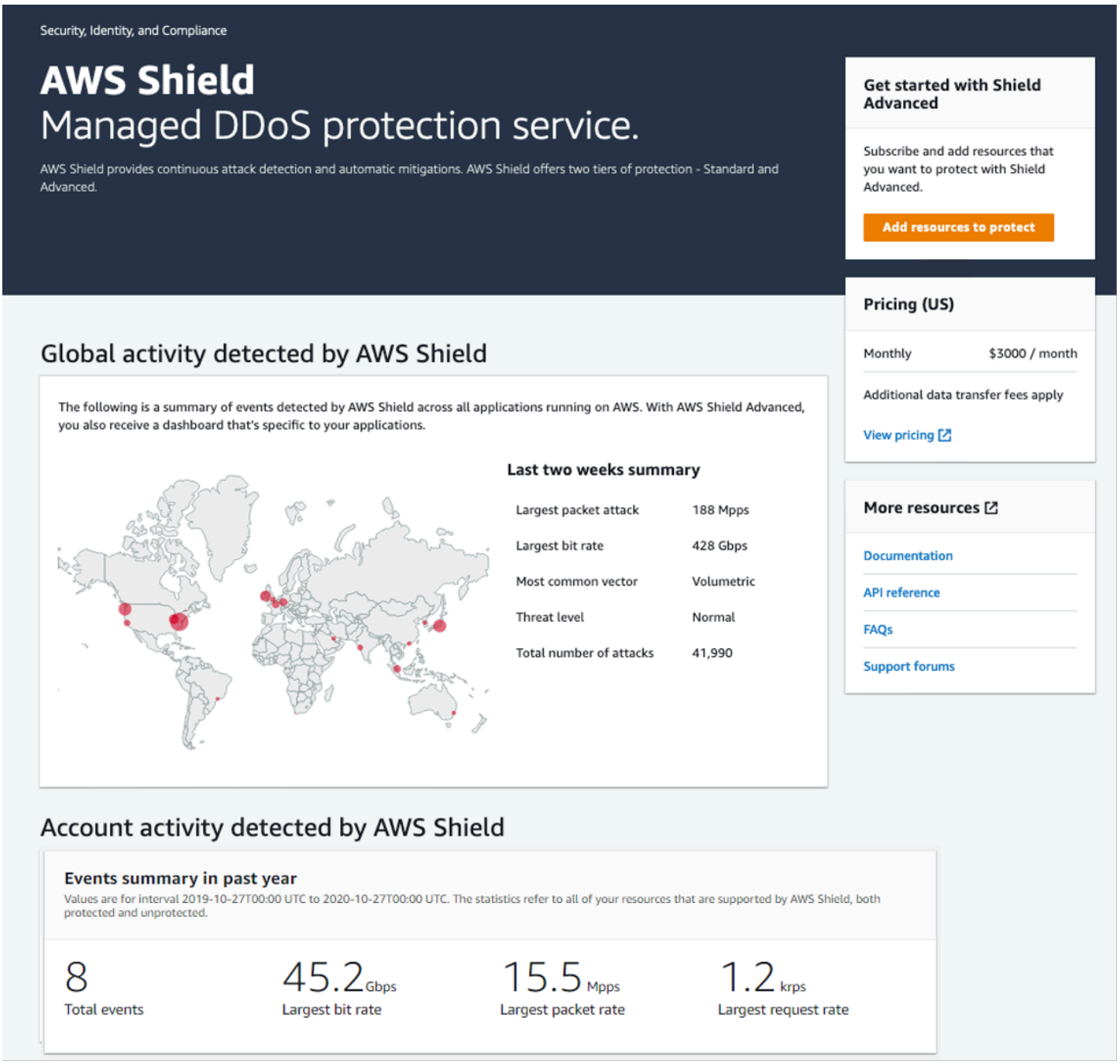
주제

- AWS Shield 글로벌 및 계정 활동
- AWS Shield Advanced 행사
- 계정 전반에 걸친 이벤트 가시성

AWS Shield 글로벌 및 계정 활동

AWS Shield 콘솔 시작하기 및 글로벌 위협 대시보드 페이지에서 글로벌 위협 활동에 대한 집계된 보기와 계정별 이벤트 요약에 액세스할 수 있습니다.

다음 스크린샷은 시작하기 페이지의 예를 보여줍니다.



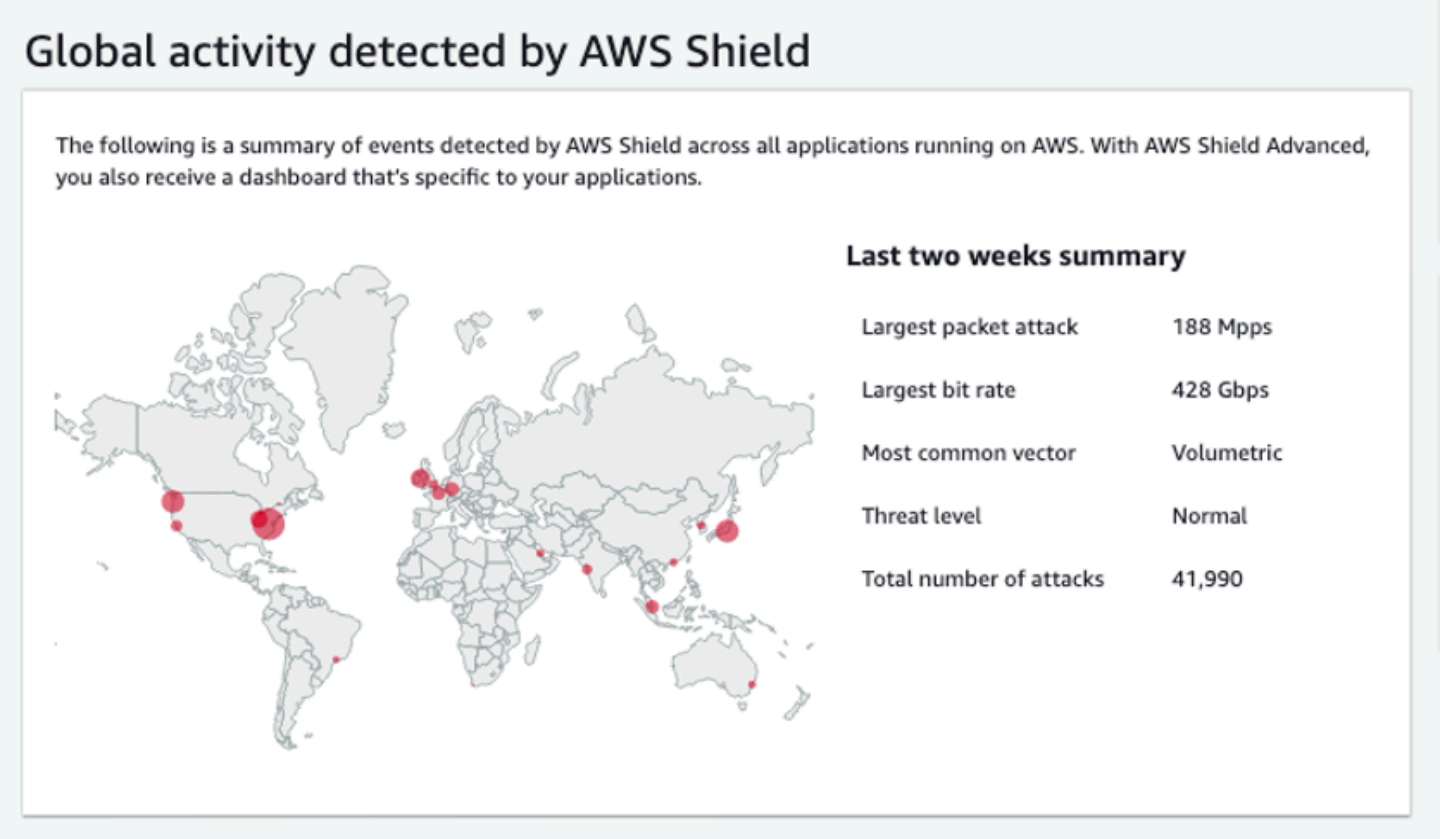
콘솔에 AWS Shield 액세스하려면

- AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.

Shield Advanced를 구독하지 않아도 글로벌 활동 및 계정 이벤트 요약 정보에 액세스할 수 있습니다.

글로벌 활동

이 정보는 AWS Shield 콘솔 글로벌 위협 대시보드 및 시작 페이지를 통해 확인할 수 있습니다. 다음 스크린샷은 글로벌 활동 창의 예를 보여줍니다.



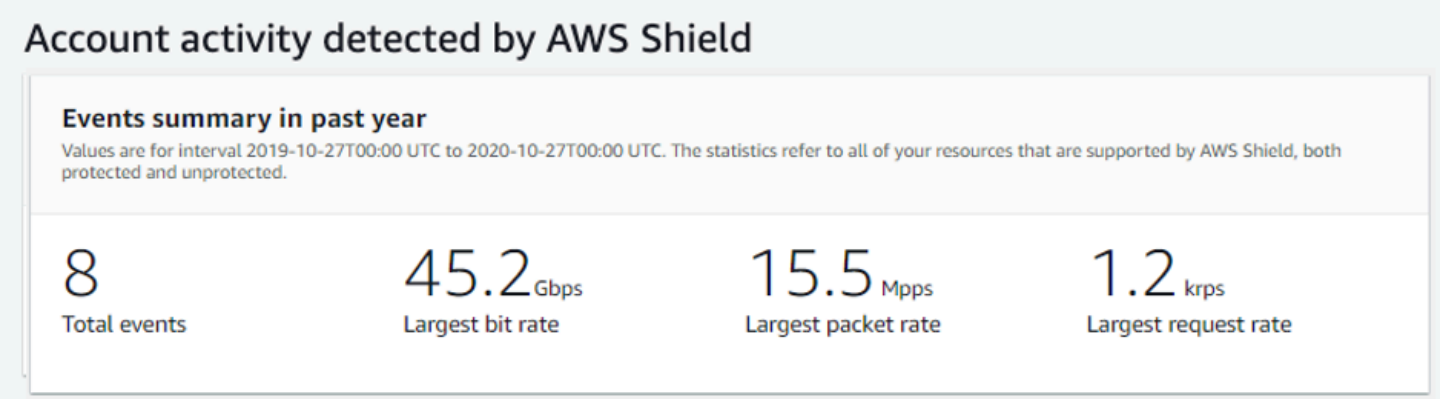
글로벌 활동은 모든 고객에서 관찰된 DDoS 이벤트를 나타냅니다. AWS 한 시간에 한 번씩 이전 2주 동안의 정보가 AWS 업데이트됩니다. 콘솔 창에서 AWS 지역별로 구분되고 세계 히트 맵에 표시된 결과를 볼 수 있습니다. Shield는 맵 옆에 최대 규모 패킷 공격, 최대 비트 전송률, 가장 일반적인 벡터, 총 공격 수, 위협 수준 등의 요약 정보를 표시합니다. 위협 수준은 현재의 글로벌 활동을 AWS 에서 일반적으로 관찰되는 활동과 비교한 평가입니다. 기본 위협 수준 값은 보통입니다. DDoS 활동이 증가하면 AWS 에서 높음으로 값이 자동으로 업데이트됩니다.

또한 글로벌 위협 대시보드는 시계열 지표를 제공하며 여러 기간 사이에서 변경할 수 기능을 사용자에게 제공합니다. 중요한 DDoS 공격의 기록을 보려면 마지막 날부터 지난 2주간의 뷰에 맞게 대시보드를 사용자 지정할 수 있습니다. 시계열 지표는 선택한 AWS 기간 동안 실행 중인 응용 프로그램에서 AWS Shield 감지한 모든 이벤트의 최대 비트 전송률, 패킷 속도 또는 요청 속도를 보여줍니다.

계정 활동

이 정보는 AWS Shield 콘솔 시작하기 페이지에서 확인할 수 있습니다.

다음 스크린샷은 계정 활동 창의 예를 보여줍니다.



계정 활동은 Shield Advanced의 보호를 받을 수 있는 사용자 리소스에 대해 Shield가 탐지한 DDoS 이벤트를 설명합니다. Shield는 매일 전날 00:00시(UTC)에 종료되는 연도의 요약 지표를 만든 다음 총 이벤트, 최대 비트 전송률, 최대 패킷 전송 속도 및 최대 요청률을 표시합니다.

- 총 이벤트 지표는 Shield가 애플리케이션으로 향하는 트래픽에서 의심스러운 속성을 관찰한 모든 이벤트를 반영합니다. 의심스러운 속성에는 볼륨이 정상보다 높은 트래픽, 애플리케이션의 기록 프로파일과 일치하지 않는 트래픽 또는 유효한 애플리케이션 트래픽에 대해 Shield에서 정의한 휴리스틱과 일치하지 않는 트래픽이 포함될 수 있습니다.
- 모든 리소스에 대해 최대 비트 전송률 및 최대 패킷 전송 속도 통계가 제공됩니다.
- 최대 요청률 통계는 연결된 AWS WAF 웹 ACL이 있는 Amazon CloudFront 배포와 애플리케이션 로드 밸런서에서만 사용할 수 있습니다.

> **Note**
>
> 또한 API 작업을 통해 계정 수준 이벤트 요약에 액세스할 수 있습니다. AWS Shield [DescribeAttackStatistics]

AWS Shield Advanced 행사

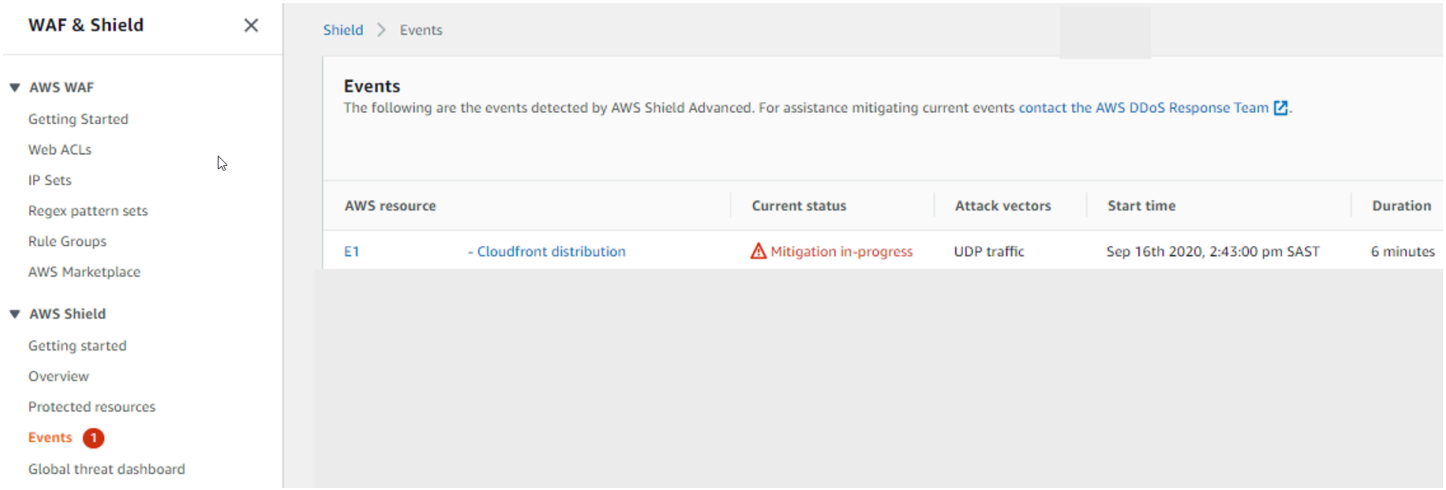
Shield Advanced를 구독하고 리소스를 보호하면 리소스에 대한 추가 가시성 기능을 이용할 수 있습니다. 여기에는 Shield Advanced가 탐지한 이벤트에 대한 거의 실시간에 가까운 알림과 탐지된 이벤트 및 완화 조치에 대한 추가 정보가 포함됩니다.

> **Note**
>
> Shield Advanced 콘솔의 이벤트 정보는 Shield Advanced 지표를 기반으로 합니다. Shield Advanced 지표에 대한 자세한 내용은 을 참조하십시오. AWS Shield Advanced 측정 항목

AWS Shield 보호 대상 리소스로 향하는 트래픽을 여러 차원에서 평가합니다. 이상 항목이 감지되는 경우 Shield Advanced는 영향을 받는 각 리소스에 대해 별도의 이벤트를 생성합니다.

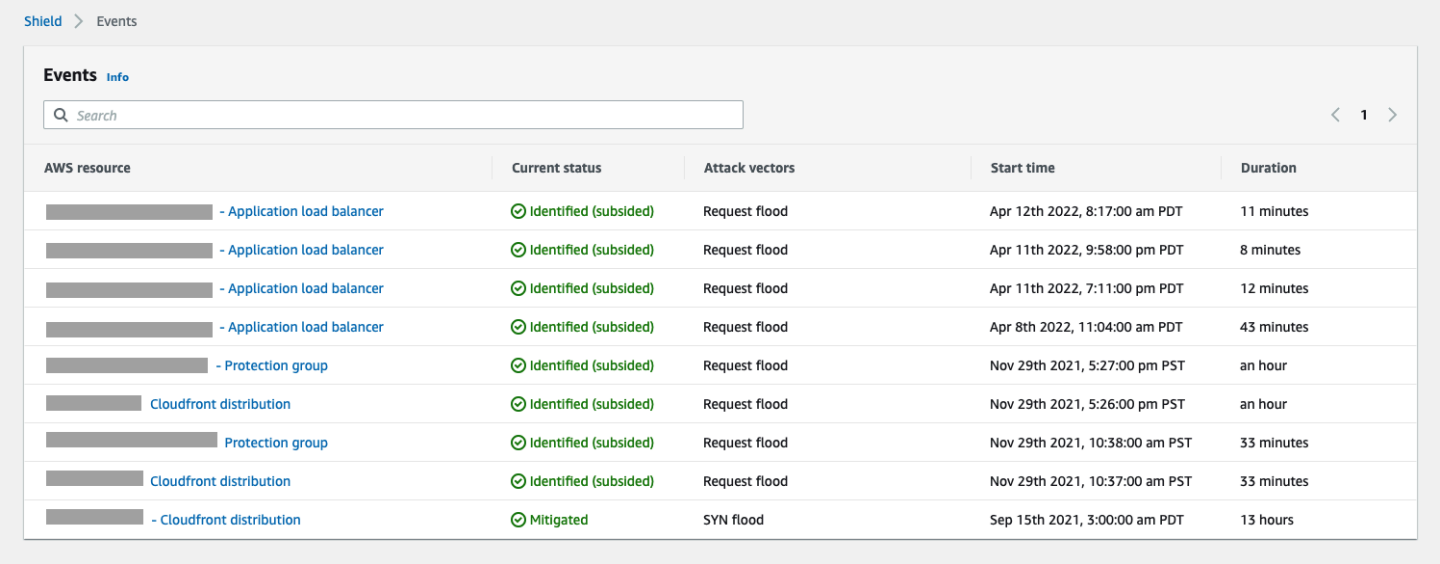
Shield 콘솔의 이벤트 페이지를 통해 이벤트 요약 및 세부 정보에 액세스할 수 있습니다. 최상위 수준 이벤트 페이지는 현재 및 과거 이벤트에 대한 개요를 제공합니다.

다음 스크린샷은 진행 중인 이벤트가 한 개인 이벤트 페이지의 예를 보여줍니다. 이 활성 이벤트는 왼쪽 탐색 창에도 플래그 지정되어 있습니다.



Shield Advanced는 트래픽 유형과 구성된 보호 기능에 따라 공격에 대한 완화 조치를 자동으로 적용할 수도 있습니다. 이러한 완화 조치는 리소스에서 알려진 DDoS 공격 시그니처와 일치하는 트래픽이나 초과 트래픽을 수신하지 않도록 보호할 수 있습니다.

다음 스크린샷은 Shield Advanced에 의해 모든 이벤트가 완화되었거나 저절로 진정된 이벤트 목록의 예를 보여줍니다.



이벤트 발생 전에 리소스 보호

리소스가 DDoS 공격을 받기 전에 정상적인 예상 트래픽을 수신하는 동안 Shield Advanced로 리소스를 보호하여 이벤트 탐지의 정확도를 개선하십시오.

보호된 리소스에 대한 이벤트를 정확하게 보고하려면 Shield Advanced는 먼저 해당 리소스에 대한 예상 트래픽 패턴의 기준을 설정해야 합니다.

- Shield Advanced는 리소스를 최소 15분 동안 보호한 후에 인프라 계층 이벤트를 보고합니다.
- Shield Advanced는 리소스를 최소 24시간 동안 보호한 후에 리소스에 대한 웹 애플리케이션 계층 이벤트를 보고합니다. 애플리케이션 계층 이벤트의 탐지는 Shield Advanced가 30일 동안 예상 트래픽을 관찰한 이후에 가장 정확합니다.

콘솔에서 이벤트 정보에 액세스하려면 AWS Shield

1. AWS Management Console 로그인하고 https://console.aws.amazon.com/wafv2/ 에서 AWS WAF & Shield 콘솔을 엽니다.
2. AWS Shield 탐색 창에서 [Events] 를 선택합니다. 콘솔이 이벤트 페이지를 보여줍니다.
3. 이벤트 페이지의 목록에 있는 이벤트를 선택하여 이벤트에 대한 추가 요약 정보 및 세부 정보를 볼 수 있습니다.

주제

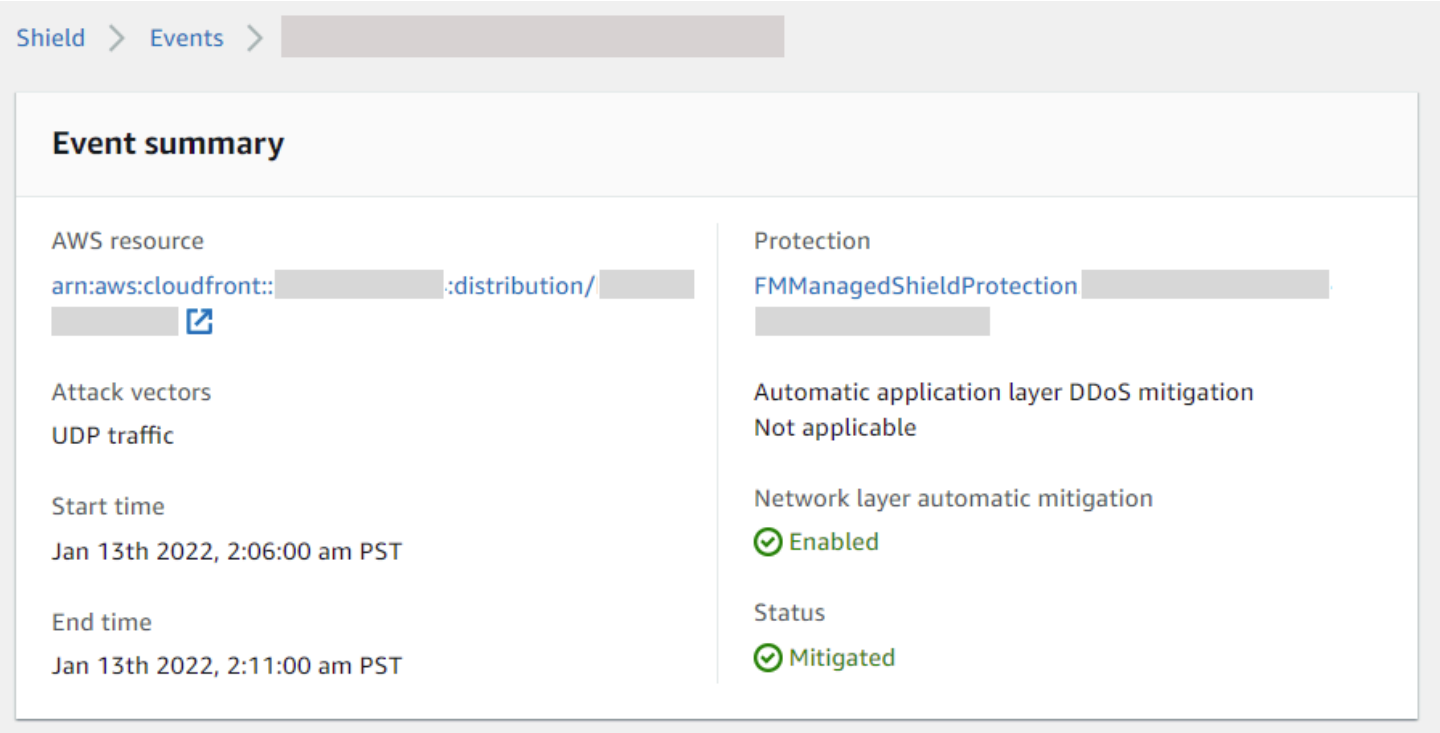
- AWS Shield Advanced 이벤트 요약

- AWS Shield Advanced 이벤트 세부 정보

AWS Shield Advanced 이벤트 요약

이벤트의 콘솔 페이지에서 이벤트에 대한 요약 및 세부 정보를 볼 수 있습니다. 이벤트 페이지를 열려면 이벤트 페이지 목록에서 해당 AWS 리소스 이름을 선택합니다.

다음 스크린샷은 네트워크 계층 이벤트에 대한 이벤트 요약의 예를 보여줍니다.



이벤트 페이지 요약 정보에는 다음 내용이 포함됩니다.

- 현재 상태 — 이벤트의 상태와 Shield Advanced가 이벤트에 대해 취한 조치를 나타내는 값입니다. 상태 값은 인프라 계층(계층 3 또는 4) 및 애플리케이션 계층(계층 7)이벤트에 적용됩니다.
  - 식별됨(진행 중) 및 식별됨(진정됨) — Shield Advanced가 이벤트를 감지했지만 지금까지 조치를 취하지 않았음을 나타냅니다. 식별됨(진정됨) — Shield가 감지한 의심스러운 트래픽이 개입 없이 중단되었음을 나타냅니다.
  - 완화 조치 진행 중 및 완화됨 — Shield Advanced가 이벤트를 감지하고 조치를 취했음을 나타냅니다. Melitigated는 대상 리소스가 자체 자동 인라인 완화 기능이 있는 Amazon CloudFront 배포 또는 Amazon Route 53 호스팅 영역인 경우에도 사용됩니다.
- 공격 벡터 — DDoS 공격 벡터(예: TCP SYN flood) 및 Shield Advanced 탐지 휴리스틱(예: 요청 플러드). 이는 DDoS 공격의 지표가 될 수 있습니다.

- 시작 시간 - 첫 번째 변칙적 트래픽 데이터 요소가 감지된 날짜 및 시간입니다.
- 지속 시간 또는 종료 시간 — 이벤트 시작 시간과 Shield Advanced가 마지막으로 관찰한 변칙적 데이터 요소 사이에 경과된 시간을 나타냅니다. 이벤트가 진행되는 동안 이 값은 계속 증가할 것입니다.
- 보호 - 리소스와 관련된 Shield Advanced 보호의 이름을 지정하고 보호 페이지로 연결되는 링크를 제공합니다. 이는 개별적인 이벤트 페이지에서 확인할 수 있습니다.
- 자동 애플리케이션 계층 DDoS 완화 — 애플리케이션 계층 보호에 사용되며, Shield Advanced 자동 애플리케이션 계층 DDoS 완화가 리소스에 대해 활성화되었는지 여부를 나타냅니다. 활성화된 경우 구성에 액세스하고 관리할 수 있는 링크가 제공됩니다. 이는 개별적인 이벤트 페이지에서 확인할 수 있습니다.
- 네트워크 계층 자동 완화 - 리소스에 네트워크 계층 자동 완화 기능이 있는지 여부를 나타냅니다. 리소스에 네트워크 계층 구성 요소가 있는 경우 이 구성 요소가 활성화됩니다. 이 정보는 개별적인 이벤트의 페이지에서 확인할 수 있습니다.

자주 표적이 되는 리소스의 경우, Shield는 초과 트래픽이 감소한 후에도 추가 재발을 방지하기 위해 완화 조치를 그대로 둘 수 있습니다.

> **Note**
>
> 또한 API 작업을 통해 보호된 리소스에 대한 이벤트 요약에 액세스할 수 있습니다. AWS Shield ListAttacks

AWS Shield Advanced 이벤트 세부 정보

콘솔 이벤트 페이지 하단 섹션에서 이벤트 탐지, 완화 조치 및 상위 기여자에 대한 세부 정보를 확인할 수 있습니다. 이 섹션에는 합법적인 트래픽과 잠재적으로 원치 않는 트래픽이 혼재되어 있을 수 있으며, 이 섹션은 보호된 리소스로 전달된 트래픽과 Shield 완화 조치로 차단된 트래픽 모두를 나타낼 수 있습니다.

- 탐지 및 완화 — 관찰된 이벤트와 이에 대해 적용된 모든 완화 조치에 대한 정보를 제공합니다. 완화 이벤트에 대한 자세한 내용은 DDoS 이벤트에 대한 대응(을)를 참조하세요.
- 상위 기여자 — 이벤트와 관련된 트래픽을 분류하고 Shield가 카테고리별로 식별한 트래픽의 기본 소스를 나열합니다. 애플리케이션 계층 이벤트의 경우 상위 기여자 정보를 사용하여 이벤트의 성격을 전반적으로 파악하되 보안 결정에는 AWS WAF 로그를 사용하십시오. 자세한 내용은 이어지는 섹션을 참조하세요.

Shield Advanced 콘솔의 이벤트 정보는 Shield Advanced 지표를 기반으로 합니다. Shield Advanced 지표에 대한 자세한 내용은 을 참조하십시오. AWS Shield Advanced 측정 항목

Amazon CloudFront 또는 Amazon Route 53 리소스에는 완화 지표가 포함되지 않습니다. 이러한 서비스는 항상 활성화되고 개별 리소스에 대한 완화 조치가 필요하지 않은 완화 시스템으로 보호되기 때문입니다.

세부 정보 섹션은 정보가 인프라 계층 이벤트 또는 애플리케이션 계층 이벤트에 대한 정보인지 여부에 따라 달라집니다.

애플리케이션 계층 이벤트 세부 정보

이벤트에 대한 콘솔 페이지 하단 섹션에서 애플리케이션 계층 이벤트 탐지, 완화 조치 및 상위 기여자에 대한 세부 정보를 확인할 수 있습니다. 이 섹션에는 합법적인 트래픽과 잠재적으로 원치 않는 트래픽이 혼합되어 포함될 수 있으며, 보호된 리소스로 전달된 트래픽과 Shield Advanced 완화 기능에 의해 차단된 트래픽을 모두 나타낼 수 있습니다.

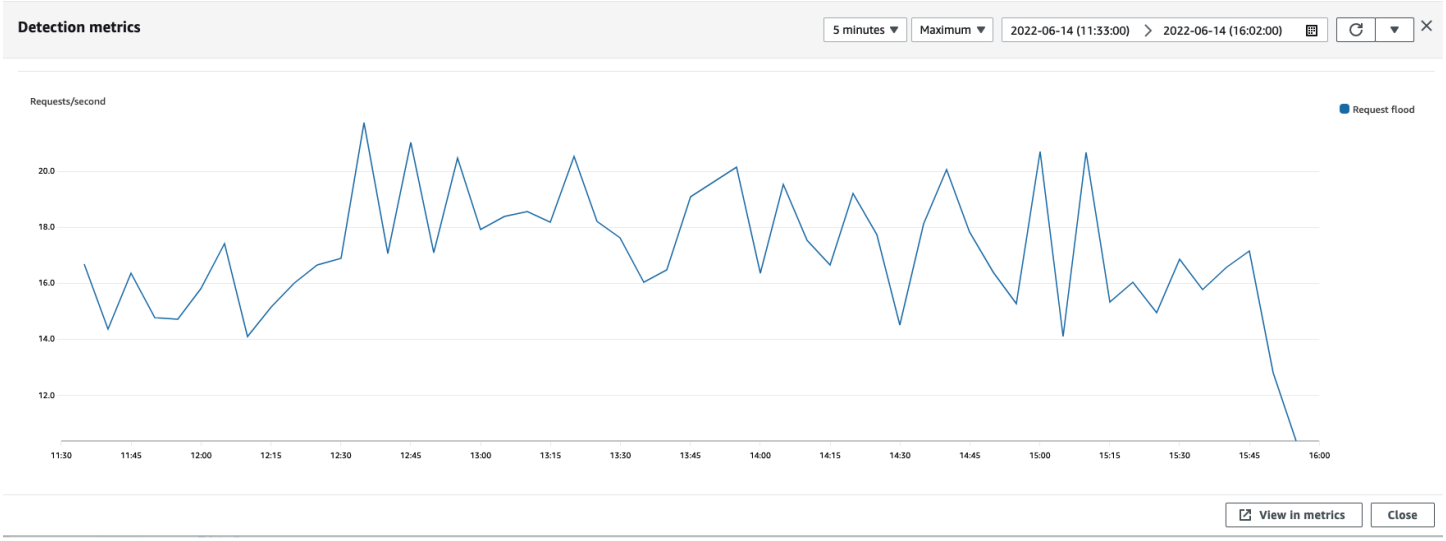
공격 대응으로 특별히 배포되는 규칙 및 웹 ACL에 정의된 속도 기반 규칙을 비롯하여 리소스와 관련된 웹 ACL의 모든 규칙에 대한 완화 세부 정보입니다. 애플리케이션에 대한 자동 애플리케이션 계층 DDoS 완화를 활성화하는 경우 완화 지표에는 해당 추가 규칙에 대한 지표가 포함됩니다. 이러한 애플리케이션 계층 보호에 대한 자세한 내용은 을 참조하십시오. AWS Shield Advanced 애플리케이션 계층 (계층 7) 보호

감지 및 완화

애플리케이션 계층 (계층 7) 이벤트의 경우 탐지 및 완화 탭에는 로그에서 얻은 정보를 기반으로 하는 탐지 지표가 표시됩니다. AWS WAF 완화 지표는 원치 않는 트래픽을 차단하도록 구성된, 연결된 웹 ACL의 AWS WAF 규칙을 기반으로 합니다.

Amazon CloudFront 배포의 경우 자동 완화 기능을 적용하도록 Shield Advanced를 구성할 수 있습니다. 모든 애플리케이션 계층 리소스를 사용하여 웹 ACL에서 자체 완화 규칙을 정의하도록 선택하고 Shield 대응 팀(SRT)에 도움을 요청할 수 있습니다. 이러한 옵션에 대한 자세한 내용은 DDoS 이벤트에 대한 대응 섹션을 참조하세요.

다음 스크린샷은 몇 시간 후에 진정된 애플리케이션 계층 이벤트에 대한 탐지 지표의 예를 보여줍니다.



완화 규칙이 적용되기 전에 감소하는 이벤트 트래픽은 완화 지표에 표시되지 않습니다. 이로 인해 탐지 그래프에 표시된 웹 요청 트래픽과 완화 그래프에 표시된 허용 및 차단 지표 간에 차이가 발생할 수 있습니다.

상위 기여자

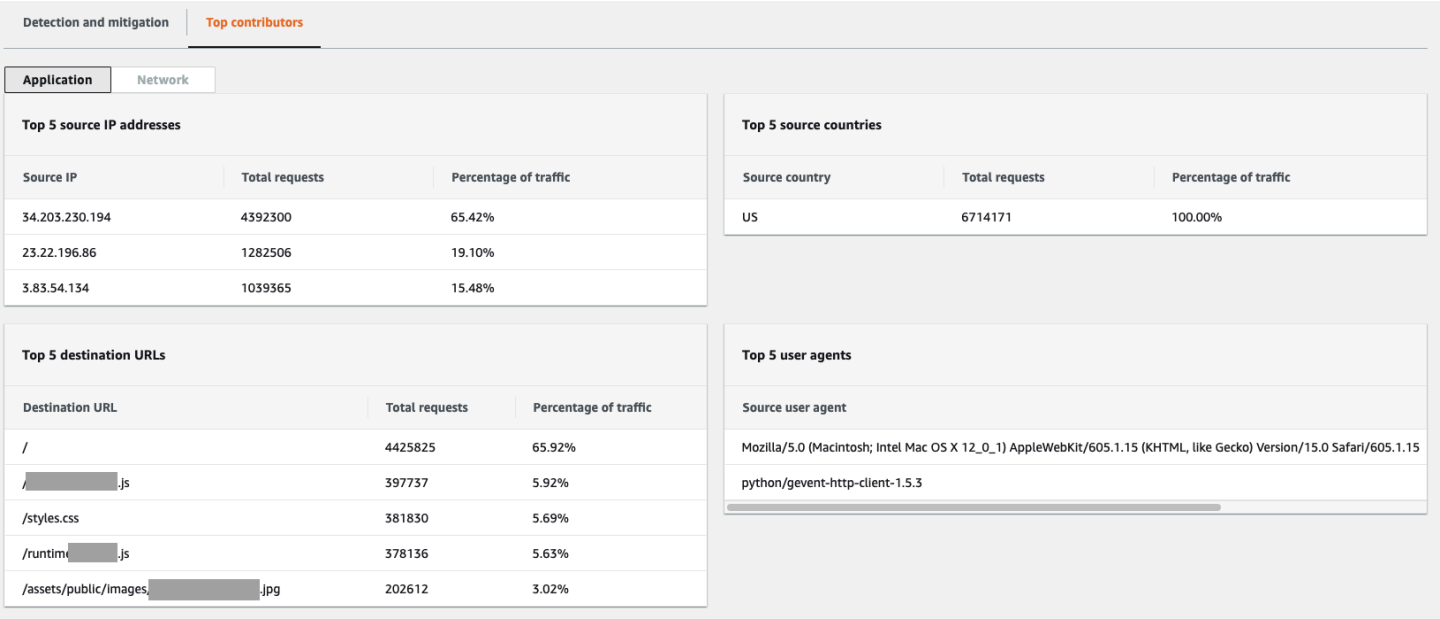
애플리케이션 계층 이벤트의 상위 기여자 탭에는 Shield가 검색한 AWS WAF 로그를 기반으로 해당 이벤트에 대해 식별한 상위 5명의 기여자가 표시됩니다. Shield는 소스 IP, 소스 국가, 대상 URL과 같은 측정기준별로 상위 기여자 정보를 분류합니다.

> **Note**
>
> 애플리케이션 레이어 이벤트에 기여하는 트래픽에 대한 가장 정확한 정보를 보려면 로그를 사용하세요. AWS WAF

Shield 애플리케이션 계층의 상위 기여자 정보는 공격의 성격을 전반적으로 파악하기 위한 용도로만 사용하고, 이를 기반으로 보안 결정을 내리지 마십시오. 애플리케이션 계층 이벤트의 경우 AWS WAF 로그는 공격의 원인을 파악하고 방어 전략을 수립하는 데 가장 좋은 정보 소스입니다.

Shield 상위 기여자 정보가 항상 AWS WAF 로그의 데이터를 완전히 반영하는 것은 아닙니다. Shield는 로그를 수집할 때 로그에서 전체 데이터 세트를 검색하는 것보다 시스템 성능에 미치는 영향을 줄이는 것을 우선시합니다. 이로 인해 Shield에서 분석에 사용할 수 있는 데이터의 세부 수준이 손실될 수 있습니다. 대부분의 경우 대부분의 정보를 사용할 수 있지만, 어떤 공격에서든 상위 기여자 데이터가 어느 정도 왜곡될 수 있습니다.

다음 스크린샷은 애플리케이션 계층 이벤트에 대한 상위 기여자 탭의 예를 보여줍니다.



기여자 정보는 합법적인 트래픽과 잠재적으로 원치 않는 트래픽 모두에 대한 요청을 기반으로 합니다. 볼륨이 큰 이벤트와 요청 소스가 크게 분산되지 않은 이벤트는 식별 가능한 상위 기여자가 있을 가능성이 더 큽니다. 상당한 정도의 분산형 공격은 소스의 수가 여러 개일 수 있어 공격의 상위 기여자를 식별하기 어렵습니다. Shield Advanced가 특정 카테고리의 주요 기여자를 식별하지 못하면 데이터가 사용할 수 없음으로 표시됩니다.

인프라 계층 이벤트 세부 정보

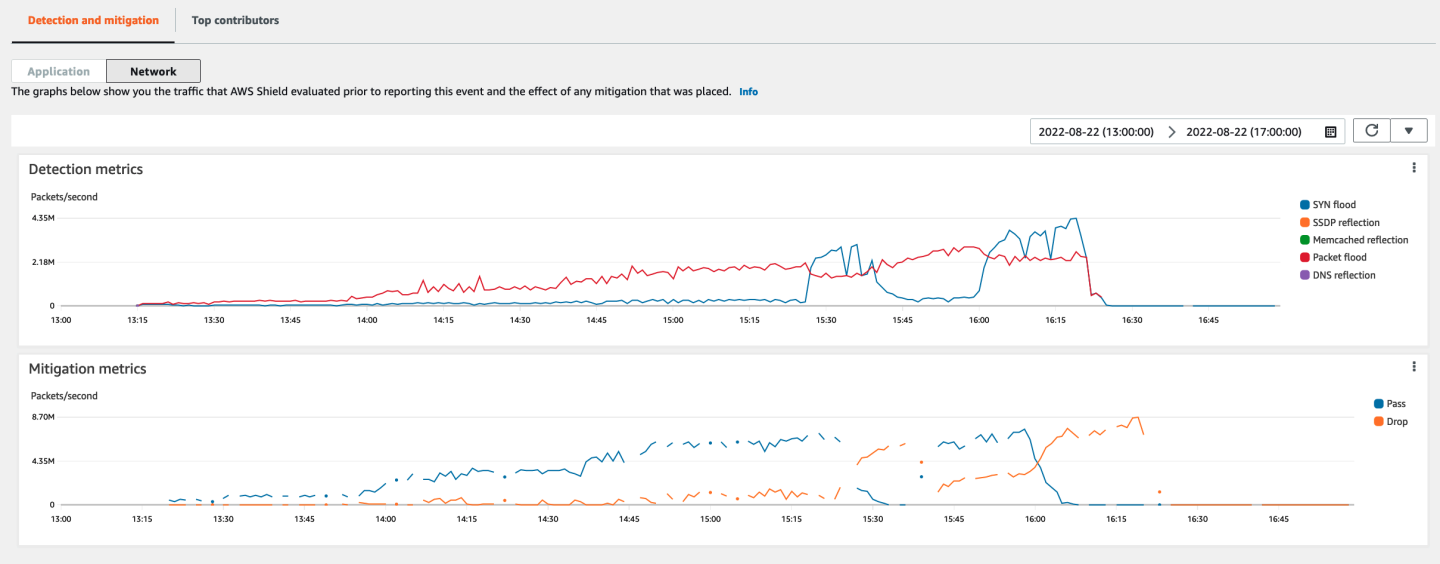
이벤트에 대한 콘솔 페이지 하단 섹션에서 인프라 계층 이벤트 탐지, 완화 조치 및 상위 기여자에 대한 세부 정보를 확인할 수 있습니다. 이 섹션에는 합법적인 트래픽과 잠재적으로 원치 않는 트래픽이 혼재되어 있을 수 있으며, 이 섹션은 보호된 리소스로 전달된 트래픽과 Shield 완화 조치로 차단된 트래픽 모두를 나타낼 수 있습니다.

감지 및 완화

인프라 계층(계층 3 또는 4)이벤트의 경우 감지 및 완화 탭에는 샘플링된 네트워크 흐름을 기반으로 하는 탐지 지표와 완화 시스템에서 관찰된 트래픽을 기반으로 하는 완화 지표가 표시됩니다. 완화 지표는 리소스로 유입되는 트래픽을 보다 정확하게 측정한 것입니다.

Shield는 보호되는 리소스 유형인 엘라스틱 IP (EIP), 클래식 로드 밸런서 (CLB), 애플리케이션 로드 밸런서 (ALB), 표준 가속기에 대한 완화 기능을 자동으로 생성합니다. AWS Global Accelerator EIP 주소 및 AWS Global Accelerator 표준 가속기에 대한 완화 지표는 통과 및 삭제된 패킷 수를 나타냅니다.

다음 스크린샷은 인프라 계층 이벤트에 대한 감지 및 완화 탭의 예를 보여줍니다.

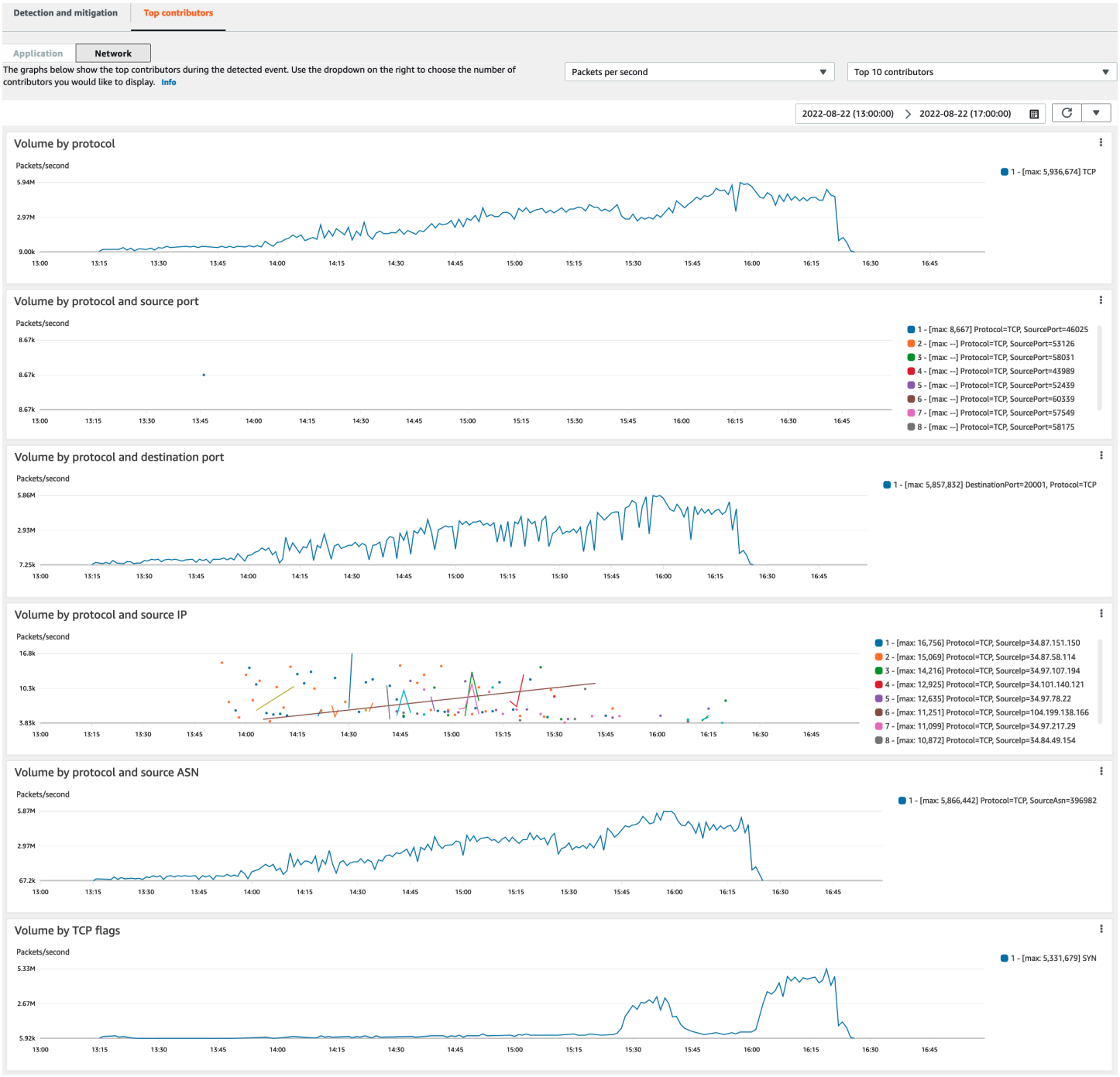


Shield가 완화를 적용하기 전에 감소하는 이벤트 트래픽은 완화 지표에 표시되지 않습니다. 이로 인해 탐지 그래프에 표시된 트래픽과 완화 그래프에 표시된 허용 및 차단 지표 간에 차이가 발생할 수 있습니다.

상위 기여자

인프라 계층 이벤트의 상위 기여자 탭에는 여러 트래픽 측정기준의 최대 100개의 상위 기여자에 대한 지표가 나열됩니다. 세부 정보에는 중요한 트래픽 소스를 5개 이상 식별할 수 있는 모든 측정기준에 대한 네트워크 계층 속성이 포함됩니다. 트래픽 소스의 예로는 소스 IP와 소스 ASN이 있습니다.

다음 스크린샷은 인프라 계층 이벤트에 대한 상위 기여자 탭의 예를 보여줍니다.



기여자 지표는 합법적인 트래픽과 잠재적으로 원치 않는 트래픽 모두에 대해 샘플링된 네트워크 흐름을 기반으로 합니다. 볼륨이 큰 이벤트와 트래픽 소스가 크게 분산되지 않은 이벤트는 식별 가능한 상위 기여자가 있을 가능성이 더 큽니다. 상당한 정도의 분산형 공격은 소스의 수가 여러 개일 수 있어 공격의 상위 기여자를 식별하기 어렵습니다. Shield가 특정 지표나 카테고리의 주요 기여자를 식별하지 못하면 해당 데이터를 사용할 수 없음으로 표시합니다.

인프라 계층 DDoS 공격에서는 트래픽 소스가 스푸핑되거나 반영될 수 있습니다. 스푸핑된 소스는 공격자가 의도적으로 위조한 것입니다. 반영된 소스는 탐지된 트래픽의 실제 소스이지만 공격에 기꺼이 참여하지는 않습니다. 예를 들어 공격자는 일반적으로 합법적인 인터넷 서비스 비활성화 공격을 반영하여 표적으로 대량의 증폭된 트래픽을 생성할 수 있습니다. 이 경우 소스 정보는 공격의 실제 소스는 아니지만 유효할 수 있습니다. 이러한 요인으로 인해 패킷 헤더를 기반으로 소스를 차단하는 완화 기술의 실행 가능성이 제한될 수 있습니다.

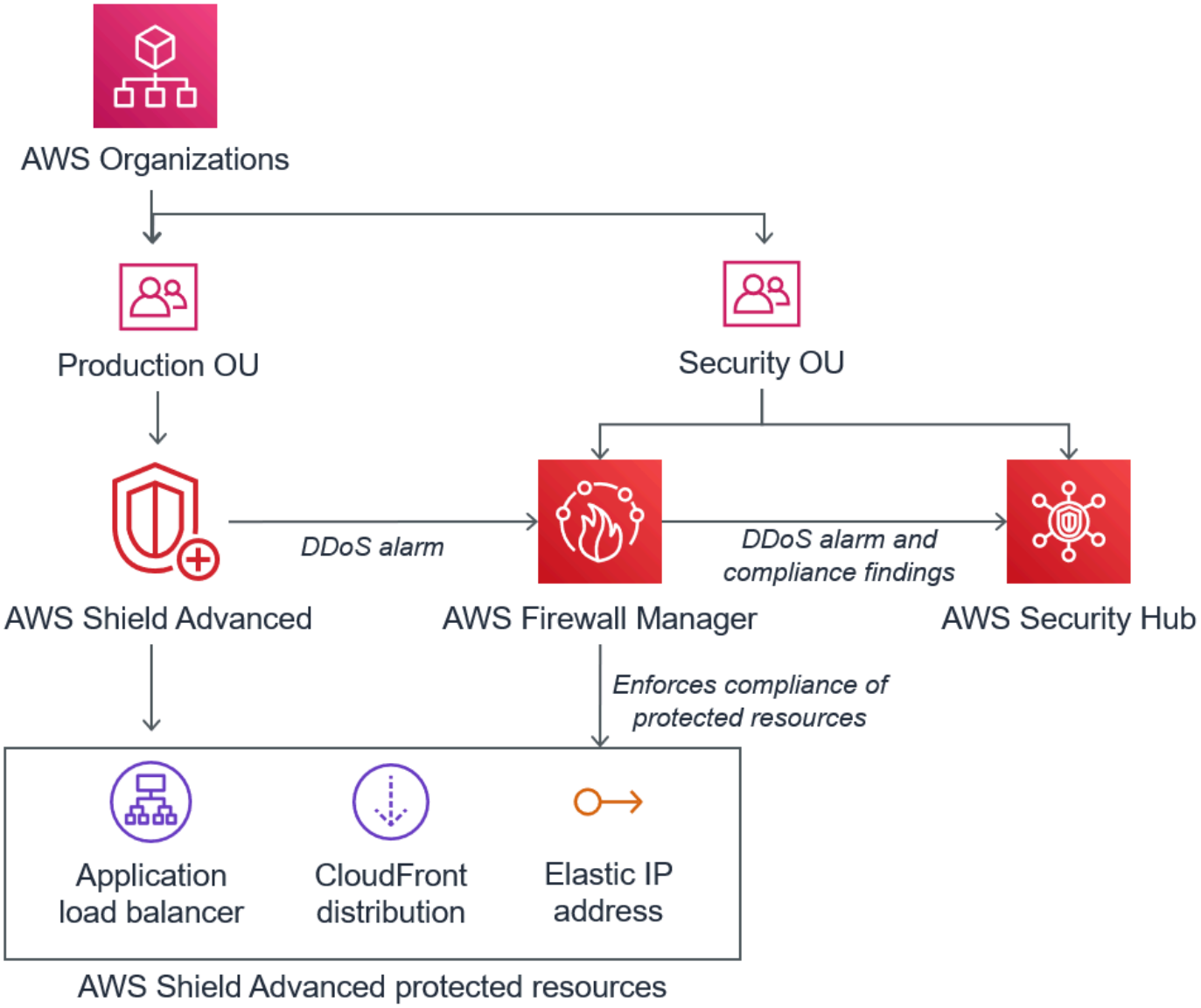
계정 전반에 걸친 이벤트 가시성

여러 AWS Security Hub 계정에서 AWS Shield Advanced 보호된 리소스를 사용하고 AWS Firewall Manager 관리하고 모니터링할 수 있습니다.

Firewall Manager를 사용하면 모든 계정에서 DDoS 보호 규정 준수를 보고하고 강제 적용하는 Shield Advanced 보안 정책을 생성할 수 있습니다. Firewall Manager는 Shield Advanced 정책 범위에 할당되는 새 리소스에 보호 기능을 추가하는 것을 포함하여 보호된 리소스를 모니터링합니다.

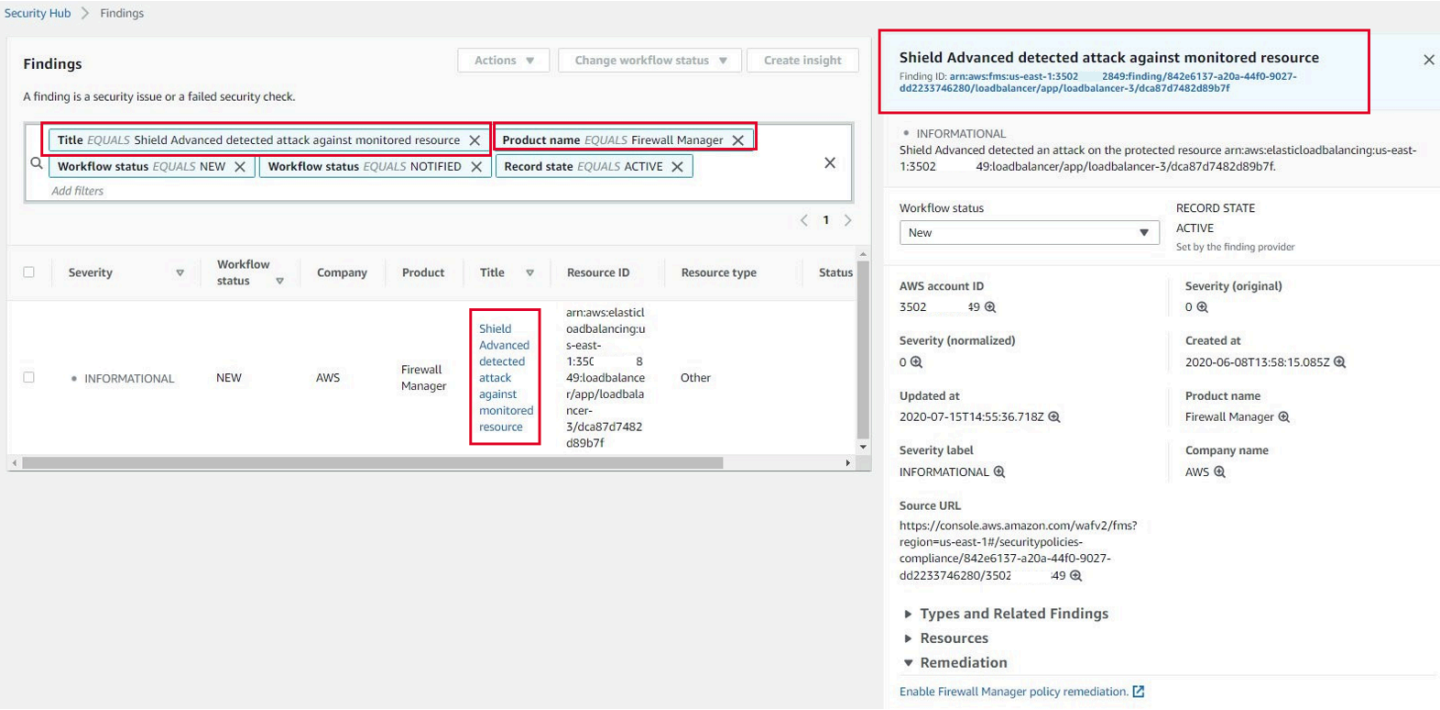
Firewall AWS Security Hub Manager를 와 통합하면, Firewall Manager가 Shield Advanced 보안 정책을 준수하지 않는 리소스를 식별할 때 Shield Advanced와 Firewall Manager 규정 준수 결과에 의해 탐지된 DDoS 이벤트를 보고하는 단일 대시보드를 만들 수 있습니다.

다음 그림은 Firewall Manager와 Security Hub를 사용하여 Shield Advanced 보호된 리소스를 모니터링하는 일반적인 아키텍처를 보여줍니다.



Firewall Manager를 Security Hub와 통합하면 AWS에서 실행하는 애플리케이션에 대한 다른 경보 및 규정 준수 상태 정보와 함께 보안 조사 결과를 한 곳에서 볼 수 있습니다.

다음 스크린샷은 이러한 유형의 통합이 있는 경우에 Security Hub 콘솔 내에서 Shield Advanced 이벤트에 대해 확인할 수 있는 정보를 보여줍니다.



Firewall Manager 및 Security Hub를 Shield Advanced와 통합하여 보호 대상 계정 전반의 이벤트 및 규정 준수 모니터링을 중앙 집중화하는 방법을 알아보려면 AWS 보안 블로그 DDoS 이벤트에 대한 중앙 집중식 모니터링 설정 및 비준수 리소스 자동 해결을 참조하십시오.

DDoS 이벤트에 대한 대응

AWS 네트워크 및 전송 계층 (계층 3 및 계층 4) DDoS (분산 서비스 거부) 공격을 자동으로 완화합니다. Shield Advanced를 사용하여 Amazon EC2 인스턴스를 보호하는 경우, 공격 중에 Shield Advanced는 Amazon VPC 네트워크 ACL을 AWS 네트워크 경계에 자동으로 배포합니다. 이를 통해 Shield Advanced는 대규모 DDoS 이벤트에 대한 보호 기능을 제공할 수 있습니다. 네트워크 ACL에 대한 자세한 내용은 네트워크 ACL을 참조하세요.

애플리케이션 계층 (계층 7) DDoS 공격의 경우 경보를 통해 탐지하고 고객에게 AWS AWS Shield Advanced 알리려고 시도합니다. CloudWatch 기본적으로, 유효한 사용자 트래픽이 실수로 차단되는 것을 방지하기 위해 완화 조치를 자동으로 적용하지 않습니다.

애플리케이션 계층(계층 7) 리소스의 경우, 공격에 대응하는 데 사용할 수 있는 옵션은 다음과 같습니다.

- 자체 완화 조치 제공 - 직접 공격을 조사하고 완화할 수 있습니다. 자세한 내용은 애플리케이션 계층 DDoS 공격을 수동으로 완화하기을 참조하세요.

- 지원팀에 문의 — Shield Advanced 고객인 경우, AWS Support 센터에 문의하여 완화 조치에 대한 도움을 받을 수 있습니다. 중요하고 긴급한 사례는 DDoS 전문가에게 직접 연결됩니다. 자세한 내용은 애플리케이션 계층 DDoS 공격 중에 지원 센터에 문의하기을 참조하세요.

또한 공격이 발생하기 전에 다음과 같은 완화 옵션을 사전에 활성화할 수 있습니다.

- Amazon CloudFront 배포의 자동 완화 — 이 옵션을 사용하면 Shield Advanced가 웹 ACL에서 완화 규칙을 정의하고 관리합니다. 자동 애플리케이션 계층 완화에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화(을)를 참조하세요.
- 사전 대응 — 애플리케이션 중 하나에 대한 대규모 애플리케이션 계층 공격이 AWS Shield Advanced 감지되면 SRT에서 사전에 연락을 취할 수 있습니다. SRT는 DDoS 이벤트를 분류하고 AWS WAF 완화를 생성합니다. SRT에서 고객에게 연락하여 고객의 동의 하에 AWS WAF 규칙을 적용할 수 있습니다. 이 옵션에 대한 자세한 내용은 선제적 대응 구성(을)를 참조하세요.

애플리케이션 계층 DDoS 공격 중에 지원 센터에 문의하기

AWS Shield Advanced 고객인 경우 AWS Support 센터에 문의하여 완화 조치에 대한 도움을 받을 수 있습니다. 중요하고 긴급한 사례는 DDoS 전문가에게 직접 연결됩니다. 를 사용하면 보호 분야에서 풍부한 경험을 갖춘 AWS Shield Advanced AWS Shield Response Team (SRT) AWS, Amazon.com 및 그 자회사에 복잡한 사례를 에스컬레이션할 수 있습니다. SRT에 대한 자세한 내용은 Shield 대응 팀 (SRT) 지원(을)를 참조하세요.

Shield 대응 팀(SRT)의 지원을 받으려면 AWS Support 센터에 문의하세요. 사례에 대한 응답 시간은 선택한 심각도 및 AWS Support 계획 페이지에 설명된 응답 시간에 따라 결정됩니다.

다음 옵션을 선택합니다.

- 사례 유형: 기술 지원
- 서비스: DDoS(분산 서비스 거부)
- 카테고리: 인바운드 AWS
- 보안: 적절한 옵션 선택

당사 담당자와 논의할 때는 귀사가 DDoS 공격을 받고 있을 가능성이 있는 AWS Shield Advanced 고객이라고 설명하십시오. 담당자가 적절한 DDoS 전문가에게 통화를 연결합니다. 분산 서비스 거부(DDoS) 서비스 유형을 사용하여 AWS Support 센터에서 사례를 개설하는 경우 채팅 또는 전화로

DDoS 전문가와 직접 이야기할 수 있습니다. DDoS 지원 엔지니어는 공격을 식별하고, AWS 아키텍처 개선을 권장하고, DDoS 공격 완화를 위한 AWS 서비스 사용에 대한 지침을 제공할 수 있습니다.

애플리케이션 계층 공격의 경우, SRT에서 의심스러운 활동을 분석하도록 지원합니다. 리소스에 대한 자동 완화 조치를 활성화한 경우, SRT는 Shield Advanced가 공격에 맞서 자동으로 적용하는 완화 조치를 검토할 수 있습니다. 어떤 경우든 SRT는 문제를 검토하고 완화하는 데 도움을 줄 수 있습니다. SRT가 권장하는 방어 조치를 취하려면 SRT가 사용자 계정에서 AWS WAF 웹 액세스 제어 목록 (웹 ACL) 을 만들거나 업데이트해야 하는 경우가 많습니다. SRT가 이 작업을 수행하려면 고객의 허락이 필요합니다.

> **Important**
>
> AWS Shield Advanced활성화의 일환으로 다음 단계에 따라 공격 중에 지원하는 Shield 대응 팀(SRT) 액세스 권한 구성 데 필요한 권한을 SRT에 사전에 제공하는 것이 좋습니다. 허가를 미리 제공하면 실제 공격이 발생할 경우 지연을 방지하는 데 도움이 됩니다.

SRT는 DDoS 공격을 분류하여 공격 서명 및 패턴을 식별하도록 지원합니다. SRT는 사용자의 동의 하에 공격을 완화하기 위한 AWS WAF 규칙을 만들고 배포합니다.

가능한 공격 이전 또는 공격 중에 SRT에 문의하여 완화를 검토하고 사용자 지정 완화를 개발 및 배포할 수 있습니다. 예를 들어, 웹 애플리케이션을 실행하고 있으며 포트 80과 443만 열어야 하는 경우 SRT와 협력하여 포트 80과 443만 "허용"하도록 웹 ACL을 미리 구성할 수 있습니다.

계정 레벨에서 SRT에게 권한을 부여하고 문의합니다. 즉, Firewall Manager Shield Advanced 정책 내에서 Shield Advanced를 사용하는 경우 계정 소유자(Firewall Manager 관리자가 아님)가 SRT에게 문의하여 지원을 요청해야 합니다. Firewall Manager 관리자는 자신이 소유하는 계정에 대해서만 SRT에게 문의할 수 있습니다.

애플리케이션 계층 DDoS 공격을 수동으로 완화하기

리소스에 대한 이벤트 페이지의 활동이 DDoS 공격이라고 판단되면 웹 ACL에 자체 AWS WAF 규칙을 만들어 공격을 완화할 수 있습니다. Shield Advanced 고객이 아닌 경우 사용할 수 있는 유일한 옵션입니다. AWS WAF 추가 비용 없이 AWS Shield Advanced 포함되어 있습니다. 웹 ACL의 규칙 생성에 대한 자세한 내용은 AWS WAF 웹 액세스 제어 목록 (웹 ACL)(을)를 참조하세요.

를 사용하는 AWS Firewall Manager경우 Firewall Manager AWS WAF 정책에 AWS WAF 규칙을 추가할 수 있습니다.

잠재적인 애플리케이션 계층 DDoS 공격을 수동으로 완화하려면

1. 웹 ACL에 비정상적인 동작과 일치하는 기준을 사용한 규칙 문을 생성하십시오. 먼저 일치하는 요청 수를 계수하도록 구성합니다. 웹 ACL 및 규칙 문 구성에 대한 자세한 내용은 웹 ACL 규칙 및 규칙 그룹 평가 및 AWS WAF 보호 기능 테스트 및 조정을(를) 참조하세요.

   > **Note**
   >
   > 처음에는 Block 대신 Count 규칙 작업을 사용하여 항상 규칙을 먼저 테스트하십시오. 새 규칙이 올바른 요청을 식별한다고 확신할 수 있으면 해당 요청을 차단하도록 새 규칙을 수정할 수 있습니다.

2. 요청 수를 모니터링하여 일치하는 요청을 차단할지 여부를 결정합니다. 요청 볼륨이 계속해서 비정상적으로 많은데 규칙을 통해 큰 볼륨의 원인이 되는 요청을 캡처하고 있다고 확신하는 경우, 요청을 차단하도록 웹 ACL의 규칙을 변경합니다.
3. 이벤트 페이지를 계속 모니터링하여 트래픽이 원하는 대로 처리되고 있는지 확인하십시오.

AWS 빠르게 시작할 수 있도록 미리 구성된 템플릿을 제공합니다. 템플릿에는 사용자 지정하여 일반적인 웹 기반 공격을 차단하는 데 사용할 수 있는 일련의 AWS WAF 규칙이 포함되어 있습니다. 자세한 내용은 AWS WAF 보안 자동화를 참조하세요.

크레딧 요청 AWS Shield Advanced

AWS Shield Advanced 구독하고 있는 상태에서 Shield Advanced로 보호되는 리소스의 활용도를 높이는 DDoS 공격을 경험하는 경우, Shield Advanced가 이를 완화할 수 없는 범위 내에서 사용률 증가와 관련된 비용에 대해 Shield Advanced 서비스 크레딧을 요청할 수 있습니다.

> **Note**
>
> 이 프로세스를 통해 받은 크레딧은 Shield Advanced 사용에만 적용할 수 있습니다. Shield Advanced 크레딧은 다른 서비스와 함께 사용할 수 없습니다.

크레딧은 다음 유형의 요금에만 사용할 수 있습니다.

- Shield Advanced 데이터 전송
- 아마존 CloudFront HTTP/HTTPS 요청

- CloudFront 데이터 송신
- Amazon Route 53 쿼리
- AWS Global Accelerator 표준 액셀러레이터 데이터 전송
- Application Load Balancer에 대한 로드 밸런서 용량 단위
- 공격에 대한 응답으로 자동 조정 정책을 통해 생성된 보호된 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 대한 인스턴스 비용

크레딧 요청을 위한 사전 요구 사항

크레딧을 받을 수 있는 자격이 되려면, 공격이 시작되기 전에 다음을 완료했어야만 합니다.

- 크레딧을 요청하려는 리소스에 Shield Advanced 보호를 추가했어야 합니다. 공격 중에 추가된 보호된 리소스는 비용 보호 자격에 해당되지 않습니다.

  > **Note**
  >
  > Shield Advanced를 활성화해도 개별 리소스에 대한 Shield Advanced 보호가 자동으로 활성화되지는 AWS 계정 않습니다.

  Shield Advanced를 사용하여 AWS 리소스를 보호하는 방법에 대한 자세한 내용은 을 참조하십시오리소스에 AWS Shield AdvancedAWS 보호 추가.
- 적용 CloudFront 가능하고 Application Load Balancer로 보호되는 리소스의 경우 AWS WAF 웹 ACL을 연결하고 웹 ACL 모드에서 속도 기반 규칙을 구현해야 합니다. Block AWS WAF 속도 기반 규칙에 대한 자세한 내용은 비율 기반 규칙 문 섹션을 참조하세요. 웹 ACL을 리소스와 연결하는 방법에 대한 자세한 내용은 을 참조하십시오. AWS AWS WAF 웹 액세스 제어 목록 (웹 ACL)
- DDoS 공격 중에 비용을 최소화하는 방식으로 애플리케이션을 구성하려면 DDoS 복원력AWS 모범 사례의 적절한 모범 사례를 구현했어야 합니다.

크레딧을 신청하는 방법

크레딧을 받을 자격이 되려면, 공격이 발생한 청구 월의 바로 다음 15일 이내에 크레딧 요청을 제출해야 합니다.

크레딧을 신청하려면, AWS Support 센터를 통해 청구 사례를 제출하십시오. 요청에서 다음 내용을 포함합니다.

- 제목 줄에 "DDoS 인정"이라는 단어
- 크레딧을 요청하고 있는 각 이벤트 또는 가용 중단의 날짜 및 시간
- 영향을 받은 AWS 서비스 및 특정 리소스

요청을 제출하면 AWS Shield Response Team (SRT) 이 DDoS 공격이 발생했는지 여부를 확인하고, 발생한 경우 DDoS 공격을 흡수할 수 있도록 확장된 보호 리소스가 있는지 확인합니다. 보호된 리소스가 DDoS 공격을 흡수하도록 확장되었다고 AWS 판단되면 DDoS 공격으로 인한 AWS 것으로 AWS 판단되는 트래픽의 해당 부분에 대한 크레딧을 발급합니다. 크레딧은 12개월 동안 유효합니다.

AWS Shield 서비스 사용 시 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

> **Note**
>
> 이 섹션에서는 Shield Advanced 보호와 같은 AWS Shield 서비스 및 AWS 리소스 사용에 대한 표준 AWS 보안 지침을 제공합니다.
> Shield and Shield Advanced를 사용하여 AWS 리소스를 보호하는 방법에 대한 자세한 내용은 AWS Shield 가이드의 나머지 부분을 참조하십시오.

보안은 두 사람 AWS 사이의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Shield에 적용되는 규정 준수 프로그램에 대한 자세한 설명은 규정 준수 프로그램을 통한AWS 범위 내 서비스 섹션을 참조하세요.
- 클라우드에서의 보안 — 사용하는 AWS 서비스에 따라 책임이 결정됩니다. 또한 데이터의 민감도, 조직의 요건 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Shield 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Shield를 구성하는 방법을 보여줍니다. 또한 Shield 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

Shield의 데이터 보호

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS Shield. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신하세요. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔 AWS CLI, API 또는 AWS 서비스 AWS SDK를 사용하여

Shield 또는 기타 기능을 사용하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

보호 등의 Shield 엔터티는 중국(베이징)과 중국(닝샤)를 포함하여 암호화를 사용할 수 없는 일부 지역을 제외하고 유휴 상태에서 암호화됩니다. 리전마다 고유한 암호화 키가 사용됩니다.

에 대한 ID 및 액세스 관리 AWS Shield

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 누가 Shield 리소스를 사용하도록 인증되고(로그인되고) 권한이 부여되는지(권한을 가지는지)를 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- AWS Shield IAM과의 작동 방식
- AWS Shield에 대한 자격 증명 기반 정책 예시
- AWS 에 대한 관리형 정책 AWS Shield
- AWS Shield ID 및 액세스 문제 해결
- Shield Advanced에 대한 서비스 연결 역할 사용

고객

사용 방법 AWS Identity and Access Management (IAM) 은 Shield에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 – Shield 서비스를 사용하여 작업을 수행하는 경우, 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Shield 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Shield의 기능에 액세스할 수 없는 경우 AWS Shield ID 및 액세스 문제 해결(을)를 참조하세요.

서비스 관리자 - 회사에서 Shield 리소스를 책임지고 있는 경우 Shield에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Shield 기능과 리소스를 결정합

니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Shield에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 AWS Shield IAM과의 작동 방식(을)를 참조하세요.

IAM 관리자 - IAM 관리자라면 Shield에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Shield 자격 증명 기반 정책 예제를 보려면 AWS Shield에 대한 자격 증명 기반 정책 예시(을)를 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역

할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은

사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.

- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련되어 있을 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

AWS Shield IAM과의 작동 방식

IAM을 사용하여 Shield에 대한 액세스를 관리하기 전에 Shield와 함께 사용할 수 있는 IAM 기능을 알아보세요.

함께 사용할 수 있는 IAM 기능 AWS Shield

IAM 특성	Shield 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요

IAM 특성	Shield 지원
ABAC(정책 내 태그)	부분
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

Shield 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서에서 IAM과 연동되는AWS 서비스를 참조하십시오.

Shield에 대한 자격 증명 기반 정책

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Shield 자격 증명 기반 정책의 예를 보려면 AWS Shield에 대한 자격 증명 기반 정책 예시(을)를 참조하세요.

Shield 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Shield에 대한 정책 작업

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

Shield 작업 목록을 보려면 서비스 권한 부여 참조의 AWS Shield에서 정의한 작업을 참조하세요.

Shield의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
shield
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
```

```
      "shield:action1",
      "shield:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, `List`(으)로 시작하는 Shield의 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "shield:List*"
```

Shield 자격 증명 기반 정책의 예를 보려면 AWS Shield에 대한 자격 증명 기반 정책 예시(을)를 참조하세요.

Shield에 대한 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Shield 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조의 AWS Shield에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Shield가 정의한 작업을 참조하십시오. Shield 리소스의 하위 집합에 대한 액세스를 허용하거나 거부하려면 리소스의 ARN을 정책의 `resource` 요소에 포함시킵니다.

에서 AWS Shield리소스는 보호 및 공격입니다. 다음 표에서처럼 이러한 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연계됩니다.

콘솔 내 AWS Shield 이름	AWS Shield SDK/CLI의 이름	ARN 형식
이벤트 또는 공격	AttackDetail	arn:aws:shield:: *account*:attack/*ID*
보호	Protection	arn:aws:shield:: *account*:protection/ *ID*

Shield 리소스의 하위 집합에 대한 액세스를 허용하거나 거부하려면 리소스의 ARN을 정책의 `resource` 요소에 포함시킵니다. Shield에 대한 ARN에는 다음과 같은 형식이 있습니다.

```
arn:partition:shield::account:resource/ID
```

account, *resource* 및 *ID* 변수를 유효한 값으로 대체합니다. 유효한 값은 다음과 같습니다.

- *##: ###* ID입니다. AWS 계정값을 지정해야 합니다.
- *###*: Shield 리소스의 유형으로, `attack` 또는 `protection`입니다.
- *ID*: 지정된 AWS 계정(와)과 연결되어 있는 지정된 유형의 모든 리소스를 나타내는 Shield 리소스의 ID 또는 와일드 카드(*)입니다.

예를 들어 다음 ARN은 계정 111122223333에 대한 모든 보호를 지정합니다.

```
arn:aws:shield::111122223333:protection/*
```

Shield 리소스에 대한 ARN의 형식은 다음과 같습니다.

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

ARN 사양에 대한 일반 정보는 Amazon Web Services 일반 참조의 Amazon 리소스 이름(ARN)을 참조하세요.

다음은 `wafv2` 리소스의 ARN과 관련된 요구 사항 목록입니다.

- *region*: Amazon CloudFront 배포판을 보호하는 데 사용하는 Shield 리소스의 경우 이 값을 로 `us-east-1` 설정하십시오. 그렇지 않으면 보호 대상 리전 리소스에서 사용하는 리전으로 설정합니다.

- *scope*: Amazon `global` CloudFront 배포판에서 사용하거나 AWS WAF 지원하는 모든 지역 리소스와 함께 `regional` 사용할 수 있도록 범위를 설정합니다. 리전 리소스는 Amazon API Gateway REST API, 애플리케이션 로드 밸런서, GraphQL API AWS AppSync , Amazon Cognito 사용자 풀, 서비스, 검증된 액세스 AWS App Runner 인스턴스입니다. AWS
- *resource-type*: 이벤트 또는 공격에 대해 `attack`, 보호 기능에 대해 `protection` 값을 지정합니다.
- *resource-name*: Shield 리소스에 지정한 이름을 지정하거나 와일드카드(*)를 지정하여 ARN의 나머지 사양을 충족하는 모든 리소스를 나타냅니다. 리소스 이름과 리소스 ID를 지정하거나 두 가지 모두에 대해 와일드카드를 지정해야 합니다.
- *resource-id*: Shield 리소스의 ID를 지정하거나 와일드카드(*)를 지정하여 ARN의 나머지 사양을 충족하는 모든 리소스를 나타냅니다. 리소스 이름과 리소스 ID를 지정하거나 두 가지 모두에 대해 와일드카드를 지정해야 합니다.

예를 들어 다음 ARN은 `us-west-1` 리전에서 계정 `111122223333`에 대한 리전 범위가 있는 모든 웹 ACL을 지정합니다.

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

다음 ARN은 `us-east-1` 리전의 `111122223333` 계정에 대해 글로벌 범위를 사용하는 `MyIPManagementRuleGroup`이라는 이름이 지정된 규칙 그룹을 지정합니다.

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Shield 자격 증명 기반 정책의 예를 보려면 AWS Shield에 대한 자격 증명 기반 정책 예시(을)를 참조하세요.

Shield에 대한 정책 조건 키

서비스별 정책 조건 키 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 AND 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 OR 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

Shield 조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS Shield을(를) 위한 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스에 대해 알아보려면 작업 정의 기준을 참조하십시오. AWS Shield

Shield 자격 증명 기반 정책의 예를 보려면 AWS Shield에 대한 자격 증명 기반 정책 예시(을)를 참조하세요.

Shield의 ACL

ACL 지원	아니요

ACL(액세스 통제 목록)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Shield를 사용한 ABAC

ABAC(정책 내 태그) 지원	부분

ABAC(속성 기반 액세스 통제)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부

할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Shield를 통한 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

Shield에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Shield에 대한 서비스 역할

서비스 역할 지원	예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Shield 기능이 중단될 수 있습니다. Shield가 그렇게 하도록 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Shield에 대한 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Shield 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 Shield Advanced에 대한 서비스 연결 역할 사용(을)를 참조하세요.

AWS Shield에 대한 자격 증명 기반 정책 예시

기본적으로 사용자 및 역할에는 Shield 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작

업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

각 리소스 유형에 대한 ARN 형식을 포함하여 Shield에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조에서 AWS Shield에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Shield 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- Shield Advanced 보호에 대한 읽기 권한 부여
- Shield에 대한 읽기 전용 액세스 권한 부여 CloudFront, CloudWatch
- Shield에 대한 전체 액세스 권한 부여 CloudFront, CloudWatch

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Shield 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르십시오.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한AWS 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하세요.
- Use conditions in IAM policies to further restrict access(IAM 정책의 조건을 사용하여 액세스 추가 제한) – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 생성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액

세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하십시오.

- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 MFA 보호 API 액세스 구성을 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하십시오.

Shield 콘솔 사용

AWS Shield 콘솔에 액세스하려면 최소한의 권한이 있어야 합니다. 이러한 권한을 통해 내 Shield 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

콘솔에 액세스하여 사용할 수 있는 사용자는 AWS 콘솔에도 액세스할 수 있습니다. AWS Shield 추가 권한은 필요하지 않습니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Shield Advanced 보호에 대한 읽기 권한 부여

AWS Shield 계정 간 리소스 액세스는 허용하지만 계정 간 리소스 보호를 생성할 수는 없습니다. 이러한 리소스를 소유한 계정 내에서만 리소스에 대한 보호를 생성할 수 있습니다.

다음은 모든 리소스의 `shield:ListProtections` 작업에 대한 권한을 부여하는 정책의 예시입니다. Shield는 일부 API 작업에 리소스 ARN(리소스 수준 권한이라고도 함)을 사용하여 특정 리소스를 식별하는 작업을 지원하지 않으므로 와일드카드 문자(*)를 지정합니다. 이렇게 하면 `ListProtections` 작업을 통해 검색할 수 있는 리소스에만 액세스할 수 있습니다.

```
{
    "Version": "2016-06-02",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
```

```
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

Shield에 대한 읽기 전용 액세스 권한 부여 CloudFront, CloudWatch

다음 정책은 사용자에게 Shield 및 Amazon 리소스, Amazon CloudFront CloudWatch 메트릭을 포함한 관련 리소스에 대한 읽기 전용 액세스 권한을 부여합니다. Shield 보호 및 공격의 설정을 보고 지표를 모니터링할 수 있는 권한이 필요한 사용자에게 유용합니다. CloudWatch 이러한 사용자는 Shield 리소스를 생성, 업데이트 또는 삭제할 수 없습니다.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
            {
```

```
                "Sid": "ShieldReadOnly",
                "Effect": "Allow",
                "Action": [
                    "shield:List*",
                    "shield:Describe*",
                    "shield:Get*"
                ],
                "Resource": "*"
            }
    ]
}
```

Shield에 대한 전체 액세스 권한 부여 CloudFront, CloudWatch

다음 정책을 통해 사용자는 모든 Shield 작업을 수행하고, CloudFront 웹 배포에서 모든 작업을 수행하고, 지표와 요청 샘플을 모니터링할 수 있습니다. CloudWatch 이 정책은 Shield 관리자인 사용자에게 유용합니다.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
```

```
                "arn:aws:globalaccelerator::*:*"
            ]
        },
        {
            "Sid": "ShieldFullAccess",
            "Effect": "Allow",
            "Action": [
                "shield:*"
            ],
            "Resource": "*"
        }
    ]
}
```

관리 권한이 있는 사용자에 대해 멀티 팩터 인증(MFA)을 구성하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS에서 멀티 팩터 인증(MFA) 기기 사용하기를 참조하세요.

AWS 에 대한 관리형 정책 AWS Shield

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하십시오.

AWS 관리형 정책: AWSShieldDRTAccessPolicy

AWS Shield Shield Response Team (SRT) 에 사용자를 대신하여 조치를 취할 수 있는 권한을 부여할 때 이 관리형 정책을 사용합니다. 이 정책은 SRT에 사용자 AWS 계정에 대한 제한된 액세스 권한을 부여하여 심각도가 높은 이벤트 발생 시 DDoS 공격을 완화하는 데 도움이 됩니다. 이 정책을 통해 SRT 는 AWS WAF 규칙 및 Shield Advanced 보호를 관리하고 로그에 액세스할 수 있습니다 AWS WAF .

SRT에게 대신 운영할 수 있는 권한을 부여하는 방법에 대한 자세한 내용은 Shield 대응 팀(SRT) 액세스 권한 구성을(를) 참조하세요.

이 정책에 대한 자세한 내용은 IAM 콘솔을 참조하십시오 AWSShieldDRTAccessPolicy.

AWS 관리형 정책: AWSShieldServiceRolePolicy

Shield Advanced는 자동 애플리케이션 계층 DDoS 완화를 활성화할 때 이 관리형 정책을 사용하여 계정의 리소스를 관리하는 데 필요한 권한을 설정합니다. 이 정책을 통해 Shield Advanced는 보호 대상 리소스에 연결한 웹 ACL에 AWS WAF 규칙 및 규칙 그룹을 생성하고 적용하여 DDoS 공격에 자동으로 대응할 수 있습니다.

IAM 엔티티에는 AWSShieldServiceRolePolicy 연결할 수 없습니다. Shield는 이 정책을 Shield에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할 `AWSServiceRoleForAWSShield`에 연결합니다.

Shield Advanced를 사용하면 자동 애플리케이션 계층 DDoS 완화를 활성화할 때 이 정책을 사용할 수 있습니다. 이 정책의 사용에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화(을)를 참조하세요.

이 정책을 사용하는 서비스 연결 역할에 대한 자세한 내용은 AWSServiceRoleForAWSShield 을 참조하십시오. Shield Advanced에 대한 서비스 연결 역할 사용

이 정책에 대한 자세한 내용은 IAM 콘솔을 참조하십시오 AWSShieldServiceRolePolicy.

AWS 관리형 정책에 대한 Shield 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Shield의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 문서 기록의 Shield 문서 기록 페이지에서 RSS 피드를 구독하세요.

정책	변경 내용 설명	날짜
`AWSShieldServiceRolePolicy` 이 정책을 통해 Shield는 사용자를 대신하여 애플리케이션	Shield Advanced에 자동 애플리케이션 계층 DDoS 완화 기능에 필요한 권한을 제공하기 위해 이 정책을 추가했습니다. 이 기능에 대한 자세한 내용은	2021년 12월 1일

정책	변경 내용 설명	날짜
레이어 DDoS 공격에 자동으로 대응하기 위해 AWS 리소스에 액세스하고 관리할 수 있습니다. IAM 콘솔의 세부 정보: AWSShieldServiceRolePolicy 서비스 연결 역할 `AWSServiceRoleForAWSShield` (이)가 이 정책을 사용합니다. 자세한 내용은 Shield Advanced에 대한 서비스 연결 역할 사용을 참조하세요.	Shield Advanced 자동 애플리케이션 계층 DDoS 완화(을)를 참조하세요.	
Shield가 변경 내용 추적을 시작함	Shield는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 3월 3일

AWS Shield ID 및 액세스 문제 해결

다음 정보를 사용하여 Shield 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Shield에서 작업을 수행할 권한이 없음
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 Shield 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

Shield에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `shield:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

이 경우 `shield:GetWidget` 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 `mateojackson` 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Shield에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 `marymajor`(이)라는 IAM 사용자가 콘솔을 사용하여 Shield에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 Shield 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- Shield에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS Shield IAM과의 작동 방식(을)를 참조하세요.

- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- 자격 증명 연동을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하십시오.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

Shield Advanced에 대한 서비스 연결 역할 사용

AWS Shield Advanced AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Shield Advanced에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Shield Advanced에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할은 Shield Advanced를 더 쉽게 설정할 수 있습니다. Shield Advanced에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Shield Advanced만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Shield Advanced 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하고 서비스 연결 역할 열에 예가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Shield Advanced에 대한 서비스 연결 역할 권한

Shield Advanced는 이름이 지정된 서비스 연결 역할을 사용합니다. AWSServiceRoleForAWSShield 이 역할을 통해 Shield Advanced는 사용자를 대신하여 애플리케이션 레이어 DDoS 공격에 자동으로 대응하기 위해 AWS 리소스에 액세스하고 관리할 수 있습니다. 이 기능에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화(을)를 참조하세요.

AWSServiceRoleForAWSShield 서비스 연결 역할은 다음 서비스를 신뢰하여 역할을 수임합니다.

- `shield.amazonaws.com`

이름이 지정된 역할 권한 정책을 AWSShieldServiceRolePolicy 통해 Shield Advanced는 모든 AWS 리소스에서 다음 작업을 완료할 수 있습니다.

- `wafv2:GetWebACL`
- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

모든 AWS 리소스에 대해 작업이 허용되는 경우 이는 정책에 다음과 같이 표시됩니다`"Resource": "*"`. 이는 서비스 연결 역할이 해당 작업이 지원하는 모든 AWS 리소스에 대해 표시된 각 작업을 수행할 수 있음을 의미할 뿐입니다. 예를 들어 `wafv2:GetWebACL` 작업은 `wafv2` 웹 ACL 리소스에 대해서만 지원됩니다.

Shield Advanced는 애플리케이션 계층 보호 기능을 활성화한 보호된 리소스 및 해당하는 보호된 리소스와 연결된 웹 ACL에 대해서만 리소스 수준 API 호출을 수행합니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 권한을 참조하세요.

Shield Advanced에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console AWS CLI, 또는 AWS API의 리소스에 대해 자동 애플리케이션 계층 DDoS 완화를 활성화하면 Shield Advanced가 서비스 연결 역할을 자동으로 생성합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 리소스에 대한 자동 애플리케이션 계층 DDoS 완화를 활성화한 경우 Shield Advanced가 자동으로 다시 서비스 연결 역할을 생성합니다.

Shield Advanced에 대한 서비스 연결 역할 편집

Shield Advanced에서는 AWSServiceRoleForAWSShield 서비스 연결 역할을 편집할 수 없습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 링크 역할 편집을 참조하세요.

Shield Advanced에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없어야 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제할 때 Shield Advanced가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

에서 사용하는 Shield Advanced 리소스를 삭제하려면 AWSServiceRoleForAWSShield

애플리케이션 계층 DDoS 보호가 구성된 모든 리소스에 대해 자동 애플리케이션 계층 DDoS 완화를 비활성화합니다. 콘솔 지침은 애플리케이션 계층 DDoS 보호 구성(을)를 참조하세요.

IAM을 사용하여 수동으로 서비스 링크 역할을 삭제하려면

IAM 콘솔 AWS CLI, 또는 AWS API를 사용하여 AWSServiceRoleForAWSShield 서비스 연결 역할을 삭제하십시오. 자세한 내용은 IAM 사용 설명서에서 서비스 연결 역할 삭제를 참조하세요.

Shield Advanced 서비스 연결 역할에 대해 지원되는 리전

Shield Advanced에서는 서비스를 사용할 수 있는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 Shield Advanced 엔드포인트 및 할당량을 참조하세요.

Shield에서의 로깅 및 모니터링

모니터링은 Shield 및 AWS 솔루션의 신뢰성, 가용성, 성능을 유지하는 데 있어 중요한 부분입니다. 다중 지점 장애가 발생할 경우 이를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 합니다. AWS Shield 리소스를 모니터링하고 잠재적 이벤트에 대응하기 위한 몇 가지 도구를 제공합니다.

아마존 CloudWatch 알람

CloudWatch 경보를 사용하면 지정한 기간 동안 단일 지표를 관찰할 수 있습니다. 지표가 지정된 임계값을 초과하는 경우 Amazon SNS 주제 또는 AWS Auto Scaling 정책에 알림을 CloudWatch 보냅니다. 자세한 정보는 아마존을 통한 모니터링 CloudWatch을 참조하세요.

AWS CloudTrail 로그

CloudTrail Shield에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공합니다. 에서 수집한 CloudTrail 정보를 사용하여 Shield에 요청한 내용, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다. 자세한 내용은 을 사용하여 AWS CloudTrail API 호출 로깅을(를) 참조하세요.

Shield의 규정 준수 검증

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수

프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.

- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Shield의 복원성

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다 AWS 리전 . AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS Shield에서 인프라 보안

관리형 서비스로서 AWS 글로벌 네트워크 보안으로 AWS Shield 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Shield에 액세스합니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증 정보를 생성하여 요청에 서명할 수 있습니다.

AWS Shield Advanced 할당량

AWS Shield Advanced 지역별 개체 수에 대한 기본 할당량이 있습니다. 이 할당량의 증가를 요청할 수 있습니다.

Resource	기본 할당량
계정당 보호를 AWS Shield Advanced 제공하는 각 리소스 유형의 최대 보호 리소스 수입니다.	1,000
계정당 보호 그룹의 최대수	100
보호 그룹에 구체적으로 포함할 수 있는 개별 보호 리소스의 최대수입니다. API에서 이는 보호 그룹 `Pattern`을 `ARBITRARY` 설정할 때 지정하는 `Members`에 적용됩니다. 콘솔에서 이는 보호된 리소스에서 선택 보호 그룹에 대해 선택한 리소스에 적용됩니다.	1,000

AWS Firewall Manager

AWS Firewall Manager AWS Shield Advanced Amazon VPC 보안 그룹 및 네트워크 ACL AWS WAF, Amazon Route 53 Resolver DNS 방화벽을 비롯한 다양한 보호를 위해 여러 계정 및 리소스에서 관리 AWS Network Firewall및 유지 관리 작업을 간소화합니다. Firewall Manager를 사용하여 보호 기능을 한 번만 설정하면 새로운 계정과 리소스를 추가할 때도 서비스가 자동으로 계정과 리소스 전체에 보호 기능을 적용합니다.

Firewall Manager는 다음과 같은 이점을 제공합니다.

- 계정의 리소스를 보호할 수 있습니다.
- 특정 유형의 모든 리소스 (예: 모든 Amazon CloudFront 배포판) 를 보호하는 데 도움이 됩니다.
- 특정한 태그를 가진 리소스를 모두 보호할 수 있습니다.
- 계정에 추가한 리소스에 자동으로 보호를 추가합니다.
- 조직의 모든 구성원 계정을 구독하고 AWS Organizations 조직에 가입하는 AWS Shield Advanced범위 내 새 계정을 자동으로 구독할 수 있습니다.
- 보안 그룹 규칙을 AWS Organizations 조직의 모든 구성원 계정 또는 계정의 특정 하위 집합에 적용하고 해당 규칙을 조직에 가입하는 범위 내 신규 계정에 자동으로 적용할 수 있습니다.
- 자체 규칙을 사용하거나 다음에서 관리형 규칙을 구입할 수 있습니다. AWS Marketplace

Firewall Manager는 소수의 특정 계정과 리소스보다는 전체 조직을 보호하려는 경우, 또는 보호할 새 리소스를 자주 추가하는 경우에 특히 유용합니다. 또한 Firewall Manager는 조직 전체에서 DDoS 공격에 대한 중앙 집중식 모니터링을 제공합니다.

주제

- AWS Firewall Manager 할당량

AWS Firewall Manager 가격 책정

에서 발생하는 AWS Firewall Manager 요금은 및 와 같은 AWS WAF 기본 서비스에 대한 요금입니다. AWS Config자세한 설명은 AWS Firewall Manager 요금을 참조하세요.

AWS Firewall Manager 전제 조건

이 항목에서는 관리 준비를 하는 방법을 보여줍니다. AWS Firewall Manager Firewall Manager 관리자 계정 하나를 사용하여 AWS Organizations의 조직에 대한 모든 Firewall Manager 보안 정책을 관리할 수 있습니다. 따로 언급된 경우를 제외하고, Firewall Manager 관리자로 사용할 계정을 사용하여 사전 요구 사항 단계를 수행하십시오.

처음으로 Firewall Manager를 사용하기 전에 다음 단계를 순차적으로 수행하십시오.

주제

- 1단계: 가입 및 구성 AWS Organizations
- 2단계: AWS Firewall Manager 기본 관리자 계정 생성
- 3단계: 활성화 AWS Config
- 4단계: 타사 정책의 경우 AWS Marketplace에서 구독하고 타사 설정을 구성하십시오.
- 5단계: 네트워크 방화벽 및 DNS 방화벽 정책에 대한 리소스 공유 활성화
- 6단계: 기본적으로 비활성화된 AWS Firewall Manager 지역에서 사용하려면

1단계: 가입 및 구성 AWS Organizations

Firewall Manager를 사용하려면, 사용자 계정이 Firewall Manager 정책을 사용하려는 AWS Organizations 서비스의 조직 구성원이어야 합니다.

> **Note**
>
> Organizations에 대한 자세한 내용은 AWS Organizations 사용 설명서 섹션을 참조하세요.

필요한 AWS Organizations 멤버십 및 구성을 설정하려면

1. Organizations에서 조직의 Firewall Manager 관리자로 사용할 계정을 선택합니다.

2. 선택한 계정이 아직 조직의 구성원이 아닌 경우 해당 계정을 가입하도록 하십시오. 조직에 AWS 계정 가입하도록 초대하기에 나와 있는 지침을 따르세요.
3. AWS Organizations 통합 결제 기능과 모든 기능이라는 두 가지 기능 세트를 사용할 수 있습니다. Firewall Manager를 사용하려면 조직에 대해 모든 기능이 활성화되어야 합니다. 조직에 통합 결제만 구성된 경우 조직 내 모든 기능 활성화 섹션을 참조하세요.

2단계: AWS Firewall Manager 기본 관리자 계정 생성

이 절차에서는 이전 단계에서 선택하고 구성한 계정과 조직을 사용합니다.

조직의 관리 계정만 Firewall Manager 기본 관리자 계정을 생성할 수 있습니다. 사용자가 만드는 첫 관리자 계정이 기본 관리자 계정입니다. 기본 관리자 계정은 타사 방화벽을 관리할 수 있고 전체 관리 범위를 가집니다. 기본 관리자 계정을 설정하면 Firewall Manager는 자동으로 해당 계정을 Firewall Manager의 AWS Organizations 위임 관리자로 설정합니다. 이렇게 하면 Firewall Manager에서 조직의 OU(조직 단위)에 대한 정보에 액세스할 수 있습니다. OU를 사용하여 Firewall Manager 정책의 범위를 지정할 수 있습니다. 정책 범위 설정에 대한 자세한 내용은 AWS Firewall Manager 정책 생성에서 개별 정책 유형에 대한 지침을 참조하세요. Organizations 및 관리 계정에 대한 자세한 내용은 조직의 AWS 계정 관리를 참조하십시오.

조직의 관리 계정에 대한 필수 설정

조직을 Firewall Manager에 온보딩하고 기본 관리자를 만들려면 조직의 관리 계정에 다음 설정이 있어야 합니다.

- Firewall Manager 정책을 AWS Organizations 적용하려는 조직의 구성원이어야 합니다.

기본 관리자 계정을 구성하려면

1. 기존 AWS Organizations 관리 계정을 AWS Management Console 사용하여 Firewall Manager에 로그인합니다.
2. https://console.aws.amazon.com/wafv2/fmsv2에서 Firewall Manager 콘솔을 엽니다.
3. 탐색 창에서 설정을 선택합니다.
4. Firewall Manager 관리자로 사용하도록 선택한 계정의 AWS 계정 ID를 입력합니다.

> **Note**
>
> 기본 관리자는 전체 관리 범위를 가집니다. 완전한 관리 범위란 이 계정이 조직 내 모든 계정 및 OU(조직 단위)에 정책을 적용하고, 모든 지역에서 조치를 취하고, 모든 Firewall Manager 정책 타입을 관리할 수 있음을 의미합니다.

5. 관리자 계정 생성을 선택하여 계정을 생성합니다.

Firewall Manager 관리자 계정 관리에 대한 자세한 내용은 AWS Firewall Manager 관리자와 함께 작업하기 섹션을 참조하세요.

3단계: 활성화 AWS Config

Firewall Manager를 사용하려면 AWS Config을 활성화해야 합니다.

> **Note**
>
> AWS Config 가격에 따라 AWS Config 설정 요금이 부과됩니다. 자세한 내용은 AWS Config시작하기를 참조하십시오.

> **Note**
>
> Firewall Manager에서 정책 준수를 모니터링하려면 보호된 리소스의 구성 변경 사항을 지속적으로 AWS Config 기록해야 합니다. AWS Config 구성에서는 녹화 빈도를 기본 설정인 연속으로 설정해야 합니다.

방화벽 관리자를 AWS Config 활성화하려면

1. Firewall Manager 관리자 계정을 포함하여 각 AWS Organizations 구성원 계정에 AWS Config 대해 활성화합니다. 자세한 내용은 시작하기를 참조하십시오 AWS Config.
2. 보호하려는 리소스가 AWS 리전 포함된 각 항목에 AWS Config 대해 활성화하십시오. AWS Config 수동으로 활성화하거나 AWS CloudFormation StackSets 샘플 AWS CloudFormation 템플릿의 “활성화 AWS Config" 템플릿을 사용할 수 있습니다.

모든 리소스에 AWS Config 대해 활성화하지 않으려면 사용하는 Firewall Manager 정책 유형에 따라 다음을 활성화해야 합니다.

- WAF 정책 — 리소스 CloudFront 유형 배포, 애플리케이션 로드 밸런서 ElasticLoadBalancing(목록에서 V2 선택), API Gateway, WAF WebACL, WAF 리전 WebACL 및 WAFv2 WebACL에 대해 Config를 활성화합니다. CloudFront 배포를 AWS Config 보호하려면 미국 동부 (버지니아 북부) 지역에 있어야 합니다. 다른 지역에는 CloudFront 옵션이 없습니다.
- 쉴드 정책 - 쉴드 보호, ShieldRegional 보호, 애플리케이션 로드 밸런서, EC2 EIP, WAF WebACL, WAF 리저널 WebACL 및 WAFv2 WebACL 리소스 유형에 대해 Config를 활성화합니다.
- 보안 그룹 정책 — 리소스 유형 EC2 SecurityGroup, EC2 인스턴스 및 EC2에 대해 Config를 활성화합니다. NetworkInterface
- 네트워크 ACL 정책 — Amazon EC2 서브넷 및 Amazon EC2 네트워크 ACL 리소스 유형에 대해 Config를 활성화합니다.
- 네트워크 방화벽 정책 — 리소스 유형 NetworkFirewall FirewallPolicy, EC2 VPC, EC2, EC2 NetworkFirewallRuleGroup, InternetGateway EC2 서브넷에 대해 Config를 활성화합니다. RouteTable
- DNS 방화벽 정책 – EC2 VPC 리소스 유형에 대해 Config를 활성화합니다.
- 타사 방화벽 정책 — Amazon EC2 VPC, 아마존 EC2, 아마존 EC2, 아마존 EC2 서브넷, 아마존 InternetGateway EC2 VPCendPoint 리소스 유형에 대해 Config를 활성화합니다. RouteTable

> **Note**
>
> 사용자 지정 IAM 역할을 사용하도록 AWS Config 레코더를 구성하는 경우, IAM 정책에 Firewall Manager 정책의 필수 리소스 유형을 기록할 수 있는 적절한 권한이 있는지 확인해야 합니다. 적절한 권한이 없으면 필요한 리소스가 기록되지 않아 Firewall Manager가 리소스를 제대로 보호하지 못할 수 있습니다. Firewall Manager는 이러한 권한 구성 오류를 파악할 수 없습니다. IAM과 함께 AWS Config사용하는 방법에 대한 자세한 내용은 IAM 용을 참조하십시오. AWS Config

4단계: 타사 정책의 경우 AWS Marketplace에서 구독하고 타사 설정을 구성하십시오.

Firewall Manager 타사 방화벽 정책을 시작하려면 다음 사전 요구 사항을 완료하십시오.

서비스로서의 Fortigate Cloud Native Firewall(CNF) 정책 사전 요구 사항

Firewall Manager용 Fortigate CNF를 사용하려면

1. 마켓플레이스에서 서비스형 Fortigate 클라우드 네이티브 방화벽 (CNF) 서비스를 구독하십시오. AWS
2. 먼저, Fortigate CNF 제품 포털에 테넌트를 등록하십시오. 그런 다음, Fortigate CNF 제품 포털의 테넌트 아래에 Firewall Manager 관리자 계정을 추가하십시오. 자세한 내용은 Fortigate CNF 설명서 섹션을 참조하세요.

Fortigate CNF 정책을 사용해 작업하기에 대한 자세한 내용은 서비스 정책형 Fortigate Cloud Native Firewall(CNF) 섹션을 참조하세요.

Palo Alto Networks Cloud Next Generation Firewall 정책 사전 요구 사항

Firewall Manager용 Palo Alto Networks Cloud NGFW를 사용하려면

1. Marketplace에서 팔로 알토 네트웍스 클라우드 차세대 방화벽 종량제 서비스를 구독하십시오. AWS
2. 팔로알토 네트웍스 클라우드 NGFW 배포 문서에 나와 있는 팔로알토 네트웍스 클라우드 NGFW 배포 단계에 나와 있는 팔로알토 네트웍스 클라우드 NGFW 배포 단계를 팔로알토 네트웍스 클라우드 차세대 배포용 AWS 방화벽 가이드의 항목과 함께 완료하십시오. AWS Firewall Manager AWS

Palo Alto Networks Cloud NGFW 정책을 사용해 작업하기에 대한 자세한 내용은 Palo Alto Networks Cloud NGFW 정책 섹션을 참조하세요.

5단계: 네트워크 방화벽 및 DNS 방화벽 정책에 대한 리소스 공유 활성화

Firewall Manager 네트워크 방화벽 및 DNS 방화벽 정책을 관리하려면 AWS Organizations 에서 공유를 활성화해야 합니다 AWS Resource Access Manager. 이렇게 하면 Firewall Manager에서 이러한 정책 유형을 생성할 때 계정 전체에 보호 기능을 배포할 수 있습니다.

In과의 AWS Organizations 공유를 활성화하려면 AWS Resource Access Manager

- AWS Resource Access Manager 사용 설명서의 AWS Organizations(으)로 공유 활성화에 있는 지침을 준수하십시오.

리소스 공유에 문제가 발생하는 경우 네트워크 방화벽 및 DNS 방화벽 정책에 대한 리소스 공유의 지침을 참조하세요.

6단계: 기본적으로 비활성화된 AWS Firewall Manager 지역에서 사용하려면

기본적으로 비활성화된 지역에서 Firewall Manager를 사용하려면 AWS 조직의 관리 계정과 Firewall Manager 기본 관리자 계정 모두에 대해 지역을 활성화해야 합니다. 기본적으로 비활성화되어 있는 리전과 이를 활성화하는 방법에 대한 자세한 내용은 AWS 일반 참조에서 AWS 리전관리 섹션을 참조하세요.

비활성화된 리전을 활성화하려면

- 조직 관리 계정과 Firewall Manager 기본 관리자 계정 모두에 대해서는 AWS 일반 참조의 리전 활성화의 지침을 준수하십시오.

이 단계들을 준수한 후에, 리소스 보호를 시작하도록 Firewall Manager를 구성할 수 있습니다. 자세한 내용은 AWS Firewall ManagerAWS WAF 정책 시작하기 섹션을 참조하세요.

AWS Firewall Manager 관리자와 함께 작업하기

함께 AWS Firewall Manager 조직의 방화벽 리소스를 관리할 수 있는 관리자를 한 명 또는 여러 명 둘 수 있습니다. 조직에서 Firewall Manager 관리자를 여러 명 사용하려는 경우, 각 관리자에게 관리 범위 조건을 적용하여 관리할 수 있는 리소스를 정의할 수 있습니다. 이렇게 하면 조직 내에서 다양한 관리자 역할을 유연하게 사용할 수 있으며, 최소 권한 액세스 담당자를 유지할 수 있습니다. 예컨대, 한 관리자는 조직의 OU(조직 단위) 집합을 관리하도록 하고 다른 관리자는 특정 Firewall Manager 정책 타입만 관리하도록 위임할 수 있습니다. Organizations 및 관리 계정에 대한 자세한 내용은 조직의 AWS 계정 관리를 참조하십시오.

조직당 지정할 수 있는 관리자의 최대수는 AWS Firewall Manager 할당량을 참조하세요.

Firewall Manager 관리자 사용 시작하기

Firewall Manager 관리자 사용을 시작하기 전에 AWS Firewall Manager 전제 조건에 열거된 사전 조건을 충족해야 합니다. 사전 요구 사항에서는 Firewall Manager에 AWS Organizations 조직을 온보딩하

고 Firewall Manager의 기본 관리자 계정을 생성해야 합니다. 기본 관리자 계정은 제3자 방화벽을 관리할 수 있고 완전한 관리 범위를 가집니다.

관리 범위

관리 범위는 Firewall Manager 관리자가 관리할 수 있는 리소스를 정의합니다. AWS Organizations 관리 계정이 조직을 Firewall Manager에 온보딩한 후 관리 계정은 관리 범위가 다른 추가 Firewall Manager 관리자를 만들 수 있습니다. AWS Organizations 관리 계정은 관리자에게 전체 관리 범위 또는 제한된 관리 범위를 부여할 수 있습니다. 완전 범위는 관리자에게 앞의 모든 리소스 타입에 대한 완전 액세스 권한을 부여합니다. 제약 범위란 앞의 리소스의 하위 집합에만 관리 권한을 부여하는 것을 말합니다. 관리자에게 자신의 역할을 수행하는 데 필요한 권한만 부여하는 것이 좋습니다. 이러한 관리 범위 조건은 어떤 조합으로든 관리자에게 적용할 수 있습니다.

- 관리자가 정책을 적용할 수 있는 조직의 계정 또는 OU입니다.
- 관리자가 작업을 수행할 수 있는 지역입니다.
- 관리자가 관리할 수 있는 Firewall Manager 정책 타입입니다.

관리자 역할

Firewall Manager에는 기본 관리자와 Firewall Manager 관리자라는 두 가지 타입의 관리자 역할이 있습니다.

- 기본 관리자 - 조직의 관리 계정은 AWS Firewall Manager 전제 조건을 완료하는 동안 Firewall Manager에 조직을 온보딩하는 과정에서 Firewall Manager 기본 관리자 계정을 생성합니다. 기본 관리자는 제3자 방화벽을 관리할 수 있고 완전한 관리 범위를 갖지만 관리자를 여러 명 둘 경우, 다른 관리자와 같은 동등 수준에 속합니다.
- Firewall Manager 관리자 - Firewall Manager 관리자는 AWS Organizations 관리 계정이 관리 범위 구성에서 자신에게 지정한 리소스를 관리할 수 있습니다. 조직당 지정할 수 있는 관리자의 최대수는 AWS Firewall Manager 할당량을 참조하세요. Firewall Manager 관리자 계정을 만들면 서비스가 해당 계정이 이미 조직 내 Firewall Manager의 위임된 관리자인지 확인합니다. AWS Organizations 그렇지 않은 경우, Firewall Manager는 Organizations를 호출하여 계정을 Firewall Manager의 위임된 관리자로 설정합니다. 조직의 위임된 관리자에 대한 자세한 설명은 AWS Organizations 사용자 가이드의 AWS Organizations 용어 및 개념을 참조하세요.

기존 관리자

기존 Firewall Manager 고객이고 이미 관리자를 설정한 경우, 이 기존 관리자는 Firewall Manager 기본 관리자가 됩니다. 기존 흐름에는 영향이 없어야 합니다. 관리자를 더 추가하려면 이 장의 절차에 따라 추가할 수 있습니다.

Firewall Manager 관리자 계정 생성, 업데이트 및 취소

다음 주제의 절차에서는 Firewall Manager 관리자 계정을 생성, 업데이트 및 취소하는 방법을 설명합니다. 조직의 관리 계정만 Firewall Manager 관리자 계정을 생성하고 업데이트할 수 있습니다. 개별 Firewall Manager 관리자만 자신의 관리자 계정을 취소할 수 있습니다.

Firewall Manager 관리자 계정 생성

다음 절차에서는 Firewall Manager 콘솔을 사용하여 Firewall Manager 관리자 계정을 생성하는 방법을 설명합니다.

Firewall Manager 관리자 계정을 생성하려면

1. 기존 AWS Organizations 관리 계정을 AWS Management Console 사용하여 Firewall Manager에 로그인합니다.
2. https://console.aws.amazon.com/wafv2/fmsv2에서 Firewall Manager 콘솔을 엽니다.
3. 탐색 창에서 설정을 선택합니다.
4. 관리자 계정 생성을 선택합니다.
5. 세부 정보 창에서 AWS 계정 ID에 Firewall Manager 관리자로 추가하려는 멤버 계정의 AWS ID를 입력합니다.
6. 관리 범위에서 다음 옵션 중 하나를 선택합니다.

   - 전체 - 이를 통해 관리자는 조직 내 모든 계정 및 OU(조직 단위)에 정책을 적용하고, 모든 지역에서 조치를 취하고, 제3자 방화벽을 제외한 모든 Firewall Manager 정책 타입을 적용할 수 있습니다. 기본 관리자만 제3자 방화벽을 생성하고 관리할 수 있습니다. 관리자에게 이 수준의 권한을 부여할 때는 주의해야 합니다. 최소 권한 원칙에 따라 관리자에게 자신의 역할을 수행하는 데 필요한 권한만 부여하는 것이 좋습니다.
   - 제약 - 제약 범위를 적용하는 경우, 관리 범위 구성에서 계정이 관리할 수 있는 계정 및 조직 단위, 지역 및 정책 타입을 구성합니다.

     계정 및 조직 단위의 경우, 다음과 같이 옵션을 선택합니다:

     - 조직의 모든 계정 또는 조직 단위에 정책을 적용하려면 내 AWS 조직의 모든 계정 포함을 선택합니다.

- 특정 계정이나 특정 OU (AWS Organizations 조직 단위) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
- 특정 계정 집합이나 AWS Organizations 조직 단위 (OU) 를 제외한 모든 계정에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 단위 포함을 선택한 다음 제외하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

지역에서 다음과 같이 옵션을 선택합니다:

- 관리자가 사용 가능한 모든 지역에서 작업을 수행하도록 허용하려면 모든 지역 포함을 선택합니다.
- 관리자가 특정 지역에서만 작업을 수행하도록 하려면 지정된 지역만 포함을 선택한 다음 포함하려는 지역을 지정합니다.

> **Note**
>
> 기본적으로 비활성화된 지역을 포함하려면 AWS Organizations 조직 관리 계정과 기본 관리 계정 모두에 대해 지역을 활성화해야 합니다. 계정에서 지역을 활성화하는 방법에 대한 자세한 설명은 Amazon Web Services 일반 참조의 지역 활성화를 참조하세요.

정책 타입의 경우, 다음과 같이 옵션을 선택합니다:

- 관리자가 모든 정책 타입을 관리하도록 허용하려면 모든 정책 타입 포함을 선택합니다.
- 관리자가 특정 정책 타입만 관리하도록 하려면 지정된 정책 타입만 포함을 선택한 다음 포함하려는 정책 타입을 지정합니다.

7. 관리자 계정 생성을 선택하여 관리자 계정을 생성합니다. Firewall Manager는 생성 시 관리자가 이미 조직의 위임 관리자인지 확인하기 AWS Organizations 위해 전화를 겁니다. 그렇지 않은 경우, Firewall Manager는 해당 계정을 위임된 관리자로 지정합니다. 조직의 위임된 관리자에 대한 자세한 설명은 AWS Organizations 사용자 가이드의 AWS Organizations 용어 및 개념을 참조하세요.

제한 관리 범위를 적용하면 Firewall Manager는 설정에 대해 새 리소스를 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU 또는 하위 OU에 계정을 추가하면 Firewall Manager가 관리 범위 내에서 계정을 자동으로 포함합니다.

Firewall Manager 관리자 계정 업데이트

다음 절차에서는 Firewall Manager 콘솔을 사용하여 Firewall Manager 관리자 계정을 업데이트하는 방법을 설명합니다.

> **Note**
>
> 기본적으로 비활성화된 지역을 포함하도록 관리자 범위를 업데이트하려면 AWS Organizations 조직 관리 계정과 기본 관리 계정 모두에 대해 지역을 활성화해야 합니다. 계정에서 지역을 활성화하는 방법에 대한 자세한 설명은 Amazon Web Services 일반 참조의 지역 활성화를 참조하세요.

관리자 계정을 업데이트하려면 (콘솔)

1. 기존 AWS Organizations 관리 계정을 AWS Management Console 사용하여 Firewall Manager에 로그인합니다.
2. https://console.aws.amazon.com/wafv2/fmsv2에서 Firewall Manager 콘솔을 엽니다.
3. 탐색 창에서 설정을 선택합니다.
4. Firewall Manager 관리자 테이블에서 업데이트하려는 계정을 선택합니다.
5. 편집을 선택하여 관리자 계정의 세부 정보를 변경합니다. 계정 ID는 변경할 수 없습니다.
6. 저장을 선택하여 변경 사항을 저장합니다.

관리자 계정 취소

다음 절차에서는 Firewall Manager 관리자 계정을 취소하는 방법을 설명합니다. 기본 관리자인 경우, 계정을 취소하려면 먼저 조직 내 모든 Firewall Manager 관리자 계정이 자신의 계정을 취소해야 합니다. 관리자 계정을 취소하려면 아래 절차를 따릅니다.

관리자 계정을 취소하려면 (콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 설명은 AWS Firewall Manager 전제 조건을 참조하세요.
2. 탐색 창에서 설정을 선택합니다.
3. 관리자 계정 창에서 관리자 계정 취소를 선택하여 계정을 취소합니다.

> **Important**
>
> 관리자 계정에서 관리자 권한을 취소하면 해당 계정으로 만든 모든 Firewall Manager 정책이 삭제됩니다.

기본 관리자 계정 변경

조직에서 하나의 계정만 기본 Firewall Manager 관리자 계정으로 지정할 수 있습니다. 기본 관리자 계정은 선입선출 원칙을 따릅니다. 다른 기본 관리자 계정을 지정하려면 먼저 각 개별 관리자 계정이 자신의 계정을 취소해야 합니다. 그러면 기존 기본 관리자가 자신의 계정을 취소할 수 있으며, 이 경우, Firewall Manager에서 조직이 오프보드됩니다. 관리자가 계정을 취소하면 해당 계정으로 만든 모든 Firewall Manager 정책이 삭제됩니다. 새 기본 관리자 계정을 지정하려면 AWS Organizations 관리 계정으로 Firewall Manager에 로그인하여 새 관리자 계정을 지정해야 합니다. 조직의 기본 관리자 계정을 변경하려면 다음 절차를 수행합니다.

기본 관리자 계정을 변경하려면

1. 기존 AWS Organizations 관리 계정을 AWS Management Console 사용하여 Firewall Manager에 로그인합니다.
2. https://console.aws.amazon.com/wafv2/fmsv2에서 Firewall Manager 콘솔을 엽니다.
3. 탐색 창에서 설정을 선택합니다.
4. Firewall Manager 관리자로 사용하도록 선택한 계정의 ID를 입력합니다.

   > **Note**
   >
   > 조직 내 모든 계정에서 Firewall Manager 정책을 생성하고 관리할 수 있는 권한이 이 계정에 부여됩니다.

5. 관리자 계정 생성을 선택합니다.
6. Firewall Manager 관리자로 사용하도록 선택한 계정의 AWS ID를 입력합니다.

> **Note**
>
> 이 계정에는 완전한 관리 범위가 부여됩니다. 완전한 관리 범위란 이 계정이 조직 내 모든 계정 및 OU(조직 단위)에 정책을 적용하고, 모든 지역에서 조치를 취하고, 모든 Firewall Manager 정책 타입을 관리할 수 있음을 의미합니다.

7. 관리자 계정 생성을 선택하여 기본 관리자 계정을 생성합니다.

관리자 계정에 대한 변경 자격 박탈

관리자 계정을 일부 변경하면 관리자 계정을 유지할 자격이 박탈될 수 있습니다.

이 섹션에서는 관리자 계정의 자격을 박탈할 수 있는 변경 사항과 Firewall Manager에서 이러한 변경을 처리하는 방법에 대해 AWS 설명합니다.

에서 조직에서 계정이 제거되었습니다. AWS Organizations

에서 조직에서 AWS Firewall Manager 관리자 계정을 제거하면 더 이상 조직에 대한 정책을 관리할 수 없습니다. AWS Organizations Firewall Manager는 다음 조치 중 하나를 취합니다:

- 정책이 없는 계정 - Firewall Manager 관리자 계정에 Firewall Manager 정책이 없는 경우, Firewall Manager는 관리자 계정을 취소합니다.
- Firewall Manager 정책이 있는 계정 - Firewall Manager 관리자 계정에 Firewall Manager 정책이 있는 경우 Firewall Manager는 AWS 영업 계정 담당자의 도움을 받아 상황을 알리고 사용자가 취할 수 있는 옵션을 제공하는 이메일을 보냅니다.

해지된 계정

AWS Firewall Manager 관리자로 사용 중인 계정을 폐쇄하는 경우 Firewall Manager는 다음과 같이 폐쇄를 처리합니다. AWS

- AWS Firewall Manager에서 계정의 관리자 액세스 권한을 취소하고 Firewall Manager는 관리자 계정으로 관리되던 정책을 모두 비활성화합니다. 이러한 정책에 의해 제공된 보호는 조직 전체에서 중지됩니다.
- AWS 관리자 계정 폐쇄의 발효일로부터 90일 동안 계정의 Firewall Manager 정책 데이터를 보존합니다. 이 90일 기간 동안 해지된 계정을 다시 열 수 있습니다.

- 90일 기간 동안 폐쇄된 계정을 다시 열면 계정을 Firewall Manager 관리자로 AWS 재할당하고 계정에 대한 Firewall Manager 정책 데이터를 복구합니다.
- 그렇지 않으면 90일이 지나면 계정에 대한 모든 Firewall Manager 정책 데이터가 AWS 영구적으로 삭제됩니다.

AWS Firewall Manager 정책 시작하기

를 AWS Firewall Manager 사용하여 다양한 유형의 보안 정책을 활성화할 수 있습니다. 설정하기 위한 단계는 각각의 경우에 약간 다릅니다.

주제

AWS Firewall ManagerAWS WAF 정책 시작하기

를 사용하여 조직 전체에서 AWS WAF 규칙을 AWS Firewall Manager 활성화하려면 다음 단계를 순서대로 수행하십시오.

주제

1단계: 필수 구성 요소 완성

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 2단계: AWS WAF 정책 생성 및 적용으로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: AWS WAF 정책 생성 및 적용

Firewall Manager AWS WAF 정책에는 리소스에 적용할 규칙 그룹이 포함되어 있습니다. Firewall Manager는 정책을 적용하는 각 계정에 Firewall Manager 웹 ACL을 생성합니다. 개별 계정 관리자는 여기에서 정의하는 규칙 그룹 외에도 결과 웹 ACL에 규칙 및 규칙 그룹을 추가할 수 있습니다. 방화벽 관리자 AWS WAF 정책에 대한 자세한 내용은 을 참조하십시오AWS WAF 정책.

방화벽 관리자 AWS WAF 정책을 만들려면 (콘솔)

Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

1. 탐색 창에서 보안 정책을 선택합니다.
2. 정책 생성을 선택합니다.
3. 정책 타입에서 AWS WAF를 선택합니다.
4. 지역의 경우 원하는 항목을 선택합니다 AWS 리전. Amazon CloudFront 배포를 보호하려면 글로벌을 선택하십시오.

   여러 지역 (CloudFront 배포 제외) 의 리소스를 보호하려면 각 지역에 대해 별도의 Firewall Manager 정책을 만들어야 합니다.
5. 다음을 선택합니다.
6. 정책 명칭에 서술적 명칭을 입력하십시오. Firewall Manager는 관리하는 웹 ACL의 명칭에 정책 명칭을 포함합니다. 웹 ACL 명칭에는 `FMManagedWebACLV2-` 뒤에 여기에 입력한 정책 명칭인 `-` 및 웹 ACL 생성 타임스탬프(UTC 밀리초)가 있습니다. 예를 들어 `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`입니다.

   > **Important**
   >
   > 웹 ACL 명칭은 생성 후에는 변경할 수 없습니다. 정책 명칭을 업데이트하는 경우, Firewall Manager는 관련 웹 ACL 명칭을 업데이트하지 않습니다. Firewall Manager에서 다른 명칭의 웹 ACL을 생성하도록 하려면 새 정책을 생성해야 합니다.

7. 정책 규칙의 첫 번째 규칙 그룹에서 규칙 그룹 추가를 선택합니다. AWS 관리형 규칙 그룹을 펼칩니다. 핵심 규칙 집합에서 웹 ACL에 추가를 전환합니다. AWS 알려진 악성 입력의 경우, 웹 ACL에 추가로 전환합니다. 규칙 추가를 선택합니다.

   마지막 규칙 그룹에서 규칙 그룹 추가를 선택합니다. AWS 관리형 규칙 그룹을 펼치고 Amazon IP 평판 목록에서 웹 ACL에 추가로 전환합니다. 규칙 추가를 선택합니다.

   첫 번째 규칙 그룹에서 핵심 규칙 세트를 선택하고 아래로 이동을 선택합니다. AWS WAF 웹 요청을 AWS 알려진 잘못된 입력 규칙 그룹과 비교하여 평가한 다음 핵심 규칙 세트를 기준으로 평가합니다.

   원하는 경우 콘솔을 사용하여 자체 AWS WAF 규칙 그룹을 만들 수도 있습니다. AWS WAF 생성한 모든 규칙 그룹은 정책 설명: 규칙 그룹 추가 페이지의 사용자 규칙 그룹 아래에 표시됩니다.

   Firewall Manager를 통해 관리하는 첫 번째 AWS WAF 규칙 그룹과 마지막 규칙 그룹의 이름은 각각 `PREFMManaged-` 또는 `POSTFMManaged-` 로 시작하고 그 뒤에 Firewall Manager 정책 이름과 규칙 그룹 생성 타임스탬프 (UTC 밀리초) 가 뒤따릅니다. 예를 들어 `PREFMManaged-MyWAFPolicyName-1621880555123`입니다.
8. 웹 ACL에 대한 기본 조치를 허용으로 그대로 둡니다.
9. 비준수 리소스의 문제를 자동으로 해결하지 않으려면 정책 작업을 기본값으로 그대로 둡니다. 나중에 옵션을 변경할 수 있습니다.
10. 다음을 선택합니다.
11. 정책 범위에서 정책을 적용할 리소스를 식별하는 계정, 리소스 타입 및 태그 지정에 대한 설정을 제공합니다. 이 자습서에서는 AWS 계정 및 리소스 설정을 그대로 두고 하나 이상의 리소스 타입을 선택합니다.
12. 리소스의 경우 지정한 태그에 리소스를 포함하거나 제외하여 태그 지정을 사용하여 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
13. 다음을 선택합니다.
14. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
15. 다음을 선택합니다.

16. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don't comply with the policy rules, but don't auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책 변경 내용을 검토할 수 있습니다.

17. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

3단계: 정리

관련 없는 요금이 발생하지 않도록 하려면 불필요한 정책과 리소스를 모두 삭제하십시오.

정책을 삭제하려면(콘솔)

1. AWS Firewall Manager 정책 페이지에서 정책 명칭 옆의 라디오 버튼을 선택한 다음 삭제를 선택합니다.
2. 삭제 확인 상자에서 모든 정책 리소스 삭제를 선택한 다음 삭제를 다시 선택합니다.

   AWS WAF 계정에서 생성한 정책 및 관련 리소스 (예: 웹 ACL) 를 제거합니다. 변경 사항이 모든 계정에 전파되려면 몇 분 정도 걸릴 수 있습니다.

AWS Firewall ManagerAWS Shield Advanced 정책 시작하기

를 사용하여 조직 전체에서 AWS Shield Advanced 보호 기능을 AWS Firewall Manager 활성화할 수 있습니다.

> **Important**
>
> Firewall Manager는 Amazon Route 53 또는 AWS Global Accelerator을 지원하지 않습니다. 이러한 리소스를 Shield Advanced로 보호해야 하는 경우 Firewall Manager 정책을 사용할 수 없습니다. 그 대신 리소스에 AWS Shield AdvancedAWS 보호 추가의 지시 사항을 따릅니다.

Firewall Manager를 사용하여 Shield Advanced 보호를 활성화하려면 다음 단계를 순서대로 수행합니다.

주제

1단계: 필수 구성 요소 완성

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 2단계: Shield Advanced 정책 생성 및 적용으로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: Shield Advanced 정책 생성 및 적용

사전 요구 사항을 완료한 후 AWS Firewall Manager Shield Advanced 정책을 생성합니다. Firewall Manager Shield Advanced 정책에는 Shield Advanced로 보호할 계정과 리소스가 포함되어 있습니다.

> **Important**
>
> Firewall Manager는 Amazon Route 53 또는 AWS Global Accelerator을 지원하지 않습니다. 이러한 리소스를 Shield Advanced로 보호해야 하는 경우 Firewall Manager 정책을 사용할 수 없습니다. 그 대신 리소스에 AWS Shield AdvancedAWS 보호 추가의 지시 사항을 따릅니다.

Firewall Manager Shield Advanced 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형으로는 Shield Advanced를 선택합니다.

   Shield Advanced 정책을 생성하려면 Firewall Manager 관리자 계정이 Shield Advanced를 구독한 상태여야 합니다. 가입되지 않은 경우 가입하라는 메시지가 나타납니다. 구독 비용에 관한 자세한 내용은 AWS Shield Advanced 가격을 참조하세요.

   > **Note**
   >
   > 각 회원 계정에서 수동으로 Shield Advanced를 구독할 필요가 없습니다. Firewall Manager는 정책을 생성할 때 이 작업을 수행합니다. 계정의 리소스를 계속해서 보호하려면 각 계정이 Firewall Manager 및 Shield Advanced를 계속 구독하고 있어야 합니다.

5. 지역의 경우 원하는 항목을 선택합니다 AWS 리전. Amazon CloudFront 리소스를 보호하려면 글로벌을 선택하십시오.

   여러 지역의 리소스 (CloudFront 리소스 제외) 를 보호하려면 각 지역에 대해 별도의 Firewall Manager 정책을 만들어야 합니다.
6. 다음을 선택합니다.
7. 이름에 설명하는 이름을 입력합니다.
8. (글로벌 리전 한정) 글로벌 리전 정책에 한해 Shield Advanced의 자동 애플리케이션 계층 DDoS 완화 관리 여부를 선택할 수 있습니다. 이 자습서에서는 이 옵션을 기본 설정인 무시로 그대로 두십시오.
9. 정책 작업에서 자동으로 문제를 해결하지 않는 옵션을 선택합니다.
10. 다음을 선택합니다.
11. AWS 계정 이 정책은 포함하거나 제외할 계정을 지정하여 정책 범위를 좁힐 수 있는 경우에 적용됩니다. 이 자습서에서는 내 조직에 있는 모든 계정 포함을 선택합니다.
12. 보호할 리소스 타입을 선택합니다.

    Firewall Manager는 Amazon Route 53 또는 AWS Global Accelerator을 지원하지 않습니다. 이러한 리소스를 Shield Advanced로 보호해야 하는 경우 Firewall Manager 정책을 사용할 수 없습니다. 대신 리소스에 AWS Shield AdvancedAWS 보호 추가의 Shield Advanced 지침을 따르십시오.
13. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

14. 다음을 선택합니다.
15. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
16. 다음을 선택합니다.
17. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don’t comply with the policy rules, but don’t auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책 변경 내용을 검토할 수 있습니다.
18. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

계속해서 3단계: (선택 사항) Shield 대응 팀(SRT)에 권한 부여로 이동하십시오.

3단계: (선택 사항) Shield 대응 팀(SRT)에 권한 부여

의 이점 중 AWS Shield Advanced 하나는 Shield 대응팀 (SRT) 의 지원입니다. 잠재적 DDoS 공격이 발생할 경우 AWS Support 센터에 문의할 수 있습니다. 필요한 경우 지원 센터는 문제를 SRT로 에스컬레이션합니다. SRT는 의심스러운 활동을 분석하고 문제를 완화하기 위한 지원을 제공합니다. 이 완화 조치를 취하려면 계정에서 AWS WAF 규칙과 웹 ACL을 만들거나 업데이트해야 하는 경우가 많습니다. SRT에서 AWS WAF 구성을 검사하고 AWS WAF 규칙과 웹 ACL을 생성 또는 업데이트할 수 있지만, 이를 위해서는 팀에서 승인이 필요합니다. 설정 AWS Shield Advanced과정에서 SRT에 필요한 승인을 사전에 제공하는 것이 좋습니다. 권한 부여를 미리 제공하면 실제 공격이 발생할 경우 완화 지연을 방지하는 데 도움이 됩니다.

계정 레벨에서 SRT에게 권한을 부여하고 문의합니다. 즉, 계정 소유자(Firewall Manager 관리자가 아님)가 다음 단계를 수행하여 SRT에게 공격을 완화할 수 있는 권한을 부여해야 합니다. Firewall

Manager 관리자는 자신이 소유하는 계정에 대해서만 SRT에게 권한을 부여할 수 있습니다. 마찬가지로, 계정 소유자만 SRT에게 문의하여 지원을 요청할 수 있습니다.

> **Note**
>
> SRT의 서비스를 사용하려면 Business Support 플랜 또는 Enterprise Support 플랜을 구독해야 합니다.

SRT에게 사용자를 대신하여 잠재적 공격을 완화할 수 있는 권한을 부여하려면 Shield 대응 팀(SRT) 지원의 지침을 따릅니다. 동일한 단계를 사용하여 언제든지 SRT 액세스 및 권한을 변경할 수 있습니다.

계속해서 4단계: Amazon SNS 알림 및 아마존 CloudWatch 경보를 구성합니다.로 이동하십시오.

4단계: Amazon SNS 알림 및 아마존 CloudWatch 경보를 구성합니다.

Amazon SNS 알림 또는 CloudWatch 경보를 구성하지 않고 이 단계를 계속할 수 있습니다. 하지만 이러한 경보 및 알림을 구성하면 발생 가능한 DDoS 이벤트에 대한 가시성이 크게 향상됩니다.

Amazon SNS를 사용하여 보호 리소스의 잠재적 DDoS 활동 여부를 모니터링할 수 있습니다. 가능한 공격에 대한 알림을 수신하려면 각 리전에 대해 Amazon SNS 주제를 생성합니다.

Firewall Manager에서 Amazon SNS 주제를 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창의 AWS FMS에서 설정을 선택합니다.
3. [Create new topic]을 선택합니다.
4. 주제 이름을 입력합니다.
5. Amazon SNS 메시지를 수신할 이메일 주소를 입력한 후 이메일 주소 추가를 선택합니다.

6. Update SNS configuration(SNS 구성 업데이트)을 선택합니다.

Amazon CloudWatch 알람 설정

Shield Advanced는 사용자가 모니터링할 수 CloudWatch 있는 탐지, 완화 및 상위 기여자 지표를 기록합니다. 자세한 내용은 을 참조하십시오. AWS Shield Advanced 측정 항목 CloudWatch 추가 비용이 발생합니다. CloudWatch 요금은 Amazon CloudWatch 요금을 참조하십시오.

CloudWatch 경보를 생성하려면 Amazon CloudWatch Alarms 사용의 지침을 따르십시오. 기본적으로 Shield Advanced는 잠재적 DDoS 이벤트를 단 한 번 표시한 후에 알림을 CloudWatch 보내도록 구성합니다. 필요한 경우 CloudWatch 콘솔을 사용하여 여러 지표가 탐지된 후에만 알림을 표시하도록 이 설정을 변경할 수 있습니다.

> **Note**
>
> 알람 외에도 CloudWatch 대시보드를 사용하여 잠재적 DDoS 활동을 모니터링할 수 있습니다. 대시보드는 Shield Advanced에서 원시 데이터를 수집한 후 판독이 가능한 지표로 실시간에 가깝게 처리합니다. CloudWatch Amazon의 통계를 사용하여 웹 애플리케이션 또는 서비스 성능에 대한 관점을 얻을 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 내용을 참조하십시오. CloudWatch
> CloudWatch 대시보드 생성에 대한 지침은 을 참조하십시오아마존을 통한 모니터링 CloudWatch. 대시보드에 추가할 수 있는 특정 Shield Advanced 지표에 대한 자세한 내용은 AWS Shield Advanced 측정 항목을 참조하세요.

Shield Advanced 구성을 완료했으면 DDoS 이벤트에 대한 가시성에서 이벤트를 볼 수 있는 옵션을 숙지하십시오.

AWS Firewall Manager Amazon VPC 보안 그룹 정책 시작하기

조직 전체에서 Amazon VPC 보안 그룹을 AWS Firewall Manager 활성화하는 데 사용하려면 다음 단계를 순서대로 수행하십시오.

주제

- 1단계: 필수 구성 요소 완성
- 2단계: 정책에 사용할 보안 그룹 만들기
- 3단계: 공통 보안 그룹 정책 생성 및 적용

1단계: 필수 구성 요소 완성

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 2단계: 정책에 사용할 보안 그룹 만들기으로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: 정책에 사용할 보안 그룹 만들기

이 단계에서는 Firewall Manager를 사용하여 조직 전체에 적용할 수 있는 보안 그룹을 만듭니다.

> **Note**
>
> 이 자습서에서는 보안 그룹 정책을 조직의 리소스에 적용하지 않습니다. 정책을 생성하고 정책의 보안 그룹을 리소스에 적용하면 어떻게 되는지 확인할 뿐입니다. 이렇게 하려면 정책에 대한 자동 문제 해결을 비활성화합니다.

일반 보안 그룹이 이미 정의되어 있는 경우 이 단계를 건너뛰고 3단계: 공통 보안 그룹 정책 생성 및 적용로 이동합니다.

Firewall Manager 공통 보안 그룹 정책에 사용할 보안 그룹을 만들려면

- Amazon VPC 사용 설명서의 VPC 보안 그룹 지침에 따라 조직의 모든 계정과 리소스에 적용할 수 있는 보안 그룹을 만드십시오.

  보안 그룹 규칙 옵션에 대한 자세한 내용은 보안 그룹 규칙 참조를 참조하세요.

이제 3단계: 공통 보안 그룹 정책 생성 및 적용으로 이동할 준비가 되었습니다.

3단계: 공통 보안 그룹 정책 생성 및 적용

사전 요구 사항을 완료한 후 AWS Firewall Manager 공통 보안 그룹 정책을 생성합니다. 공통 보안 그룹 정책은 전체 조직에 중앙에서 제어되는 보안 그룹을 제공합니다. AWS 또한 보안 그룹이 적용되는 리소스 AWS 계정 및 리소스를 정의합니다. Firewall Manager는 공통 보안 그룹 정책 외에도, 조직에서 사용 중인 보안 그룹 규칙을 관리하는 콘텐츠 감사 보안 그룹 정책, 사용되지 않는 보안 그룹 및 중복 보안 그룹을 관리하는 사용 감사 보안 그룹 정책을 지원합니다. 자세한 내용은 보안 그룹 정책을 참조하세요.

이 자습서에서는 공통 보안 그룹 정책을 만들고 자동으로 문제를 해결하지 않도록 작업을 설정합니다. 이렇게 하면 AWS 조직을 변경하지 않고도 정책이 어떤 영향을 미치는지 확인할 수 있습니다.

Firewall Manager 공통 보안 그룹 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 사전 조건을 충족하지 않으면 문제 해결 방법에 대한 지침이 콘솔에 표시됩니다. 지침을 따른 다음, 이 단계로 돌아와서 공통 보안 그룹 정책을 만듭니다.
4. 정책 생성(Create policy)을 선택합니다.
5. 정책 유형에서 보안 그룹을 선택합니다.
6. 보안 그룹 정책 유형에서 공통 보안 그룹을 선택합니다.
7. 지역의 경우 원하는 항목을 선택합니다 AWS 리전.
8. 다음을 선택합니다.
9. 정책 명칭에 서술적 명칭을 입력하십시오.
10. 정책 규칙에서 이 정책의 보안 그룹을 적용하고 유지 관리하는 방법을 선택할 수 있습니다. 이 자습서에서는 옵션을 선택하지 않은 상태로 두십시오.
11. 기본 보안 그룹 추가를 선택하고, 이 자습서용으로 생성한 보안 그룹을 선택한 다음, 보안 그룹 추가를 선택합니다.
12. 정책 작업에서 Identify resources that don't comply with the policy rules, but don't auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)을 선택합니다.
13. 다음을 선택합니다.
14. AWS 계정 이 정책의 영향을 받는 경우 포함하거나 제외할 계정을 지정하여 정책 범위를 좁힐 수 있습니다. 이 자습서에서는 내 조직에 있는 모든 계정 포함을 선택합니다.
15. 리소스 유형에서는 AWS 조직에 정의한 리소스에 따라 하나 이상의 유형을 선택합니다.
16. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

17. 다음을 선택합니다.
18. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
19. 다음을 선택합니다.
20. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don’t comply with the policy rules, but don’t auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책 변경 내용을 검토할 수 있습니다.
21. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.
22. 탐색이 끝나면 이 자습서용으로 생성한 정책을 유지하지 않으려는 경우 정책 이름을 선택하고, 삭제를 선택한 다음, 이 정책에서 생성한 리소스 정리를 선택하고, 마지막으로 삭제를 선택합니다.

Firewall Manager 보안 그룹 관리에 대한 자세한 내용은 보안 그룹 정책을 참조하세요.

AWS Firewall Manager Amazon VPC 네트워크 ACL 정책 시작하기

조직 전체에서 네트워크 ACL을 AWS Firewall Manager 활성화하는 데 사용하려면 이 섹션의 단계를 순서대로 수행하십시오.

네트워크 ACL에 대한 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL을 사용한 서브넷 트래픽 제어를 참조하십시오.

주제

- 1단계: 필수 구성 요소 완성
- 2단계: 네트워크 ACL 정책 생성

1단계: 필수 구성 요소 완성

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 2단계: 네트워크 ACL 정책 생성으로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: 네트워크 ACL 정책 생성

사전 요구 사항을 완료한 후 Firewall Manager 네트워크 ACL 정책을 생성합니다. 네트워크 ACL 정책은 전체 조직에 대해 중앙에서 제어되는 네트워크 ACL 정의를 제공합니다. AWS 또한 네트워크 ACL이 적용되는 AWS 계정 서브넷과 서브넷을 정의합니다.

Firewall Manager 네트워크 ACL 정책에 대한 자세한 내용은 을 참조하십시오네트워크 ACL 정책.

Firewall Manager 네트워크 ACL 정책에 대한 일반 정보는 을 참조하십시오네트워크 ACL 정책.

> **Note**
>
> 이 자습서에서는 네트워크 ACL 정책을 조직의 서브넷에 적용하지 않습니다. 정책을 생성하고 해당 정책의 네트워크 ACL을 서브넷에 적용한 경우 어떤 일이 발생하는지 확인하기만 하면 됩니다. 이렇게 하려면 정책에 대한 자동 문제 해결을 비활성화합니다.

Firewall Manager 네트워크 ACL 정책을 만들려면 (콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 사전 조건을 충족하지 않으면 문제 해결 방법에 대한 지침이 콘솔에 표시됩니다. 지침을 따른 다음 이 단계로 돌아가 네트워크 ACL 정책을 생성하십시오.
4. 정책 생성(Create policy)을 선택합니다.

5. 지역의 경우 원하는 항목을 선택합니다. AWS 리전
6. 정책 유형에서 네트워크 ACL을 선택합니다.
7. 다음을 선택합니다.
8. 정책 명칭에 서술적 명칭을 입력하십시오.
9. 네트워크 ACL 정책 규칙의 경우 인바운드 트래픽과 아웃바운드 트래픽 모두에 대한 첫 번째 규칙과 마지막 규칙을 정의합니다.

   Amazon VPC를 통해 정의하는 방법과 마찬가지로 Firewall Manager에서 네트워크 ACL 규칙을 정의합니다. 유일한 차이점은 규칙 번호를 직접 할당하는 대신 각 규칙 집합의 실행 순서를 할당하면 정책을 저장할 때 Firewall Manager에서 번호를 자동으로 할당한다는 것입니다. 첫 번째와 마지막 사이에 어떤 방식으로든 나누어 최대 5개의 인바운드 규칙을 정의할 수 있으며 최대 5개의 아웃바운드 규칙을 정의할 수 있습니다.

   네트워크 ACL 규칙을 지정하는 지침은 Amazon VPC 사용 설명서의 네트워크 ACL 규칙 추가 및 삭제를 참조하십시오.

   Firewall Manager 정책에서 정의하는 규칙은 네트워크 ACL이 네트워크 ACL 정책을 준수하기 위해 갖추어야 하는 최소 규칙 구성을 지정합니다. 예를 들어, 정책에 지정된 순서와 동일한 순서로 정책의 인바운드 우선 규칙으로 시작하지 않으면 네트워크 ACL의 인바운드 규칙은 정책을 준수할 수 없습니다. 자세한 정보는 네트워크 ACL 정책을 참조하세요.
10. 정책 작업에서 Identify resources that don't comply with the policy rules, but don't auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)을 선택합니다.
11. 다음을 선택합니다.
12. AWS 계정 이 정책의 영향을 받으면 포함하거나 제외할 계정을 지정하여 정책 범위를 좁힐 수 있습니다. 이 자습서에서는 내 조직에 있는 모든 계정 포함을 선택합니다.

    네트워크 ACL 정책의 리소스 유형은 항상 서브넷입니다.
13. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 "" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
14. 다음을 선택합니다.

15. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
16. 다음을 선택합니다.
17. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don't comply with the policy rules, but don't auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책 변경 내용을 검토할 수 있습니다.
18. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.
19. 탐색이 끝나면 이 자습서용으로 생성한 정책을 유지하지 않으려는 경우, 정책 명칭을 선택하고, 삭제를 선택한 다음, 이 정책에서 생성한 리소스 정리를 선택하고, 마지막으로 삭제를 선택합니다.

Firewall Manager 네트워크 ACL 정책에 대한 자세한 내용은 을 참조하십시오네트워크 ACL 정책.

AWS Firewall ManagerAWS Network Firewall 정책 시작하기

조직 전체에서 AWS Network Firewall 방화벽을 활성화하는 데 사용하려면 AWS Firewall Manager 다음 단계를 순서대로 수행하십시오. Firewall Manager 네트워크 방화벽 정책에 대한 자세한 설명은 AWS Network Firewall 정책을 참조하세요.

주제

- 1단계: 일반적인 사전 조건 완료
- 2단계: 정책에 사용할 Network 방화벽 규칙 그룹 생성
- 3단계: Network 방화벽 정책 생성 및 적용

1단계: 일반적인 사전 조건 완료

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: 정책에 사용할 Network 방화벽 규칙 그룹 생성

이 자습서를 따르려면 해당 규칙 그룹 AWS Network Firewall 및 방화벽 정책을 구성하는 방법을 잘 알고 있어야 합니다.

AWS Firewall Manager 정책에 사용될 규칙 그룹이 Network 방화벽에 하나 이상 있어야 합니다. Network 방화벽에서 규칙 그룹을 아직 생성하지 않았다면 지금 생성하십시오. 네트워크 방화벽 사용에 관한 자세한 내용은 AWS Network Firewall 개발자 안내서를 참조하세요.

3단계: Network 방화벽 정책 생성 및 적용

사전 조건을 완료한 후에는 AWS Firewall Manager Network 방화벽 정책을 생성할 수 있습니다. Network Firewall 정책은 전체 AWS 조직에 중앙에서 제어되는 AWS Network Firewall 방화벽을 제공합니다. 또한 방화벽이 적용되는 리소스 AWS 계정 및 리소스를 정의합니다.

Firewall Manager가 네트워크 방화벽 정책을 유지 관리하는 방법에 대한 자세한 설명은 AWS Network Firewall 정책을 참조하세요.

Firewall Manager 네트워크 방화벽 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 사전 조건을 충족하지 않으면 문제 해결 방법에 대한 지침이 콘솔에 표시됩니다. 지침을 따른 다음, 이 단계로 돌아와서 Network 방화벽 정책을 만듭니다.
4. 보안 정책 생성을 선택합니다.
5. 정책 타입에서 AWS Network Firewall를 선택합니다.
6. 지역의 경우 원하는 항목을 선택합니다 AWS 리전.
7. 다음을 선택합니다.
8. 정책 명칭에 서술적 명칭을 입력하십시오.

9. 정책 구성을 통해 방화벽 정책을 정의할 수 있습니다. 이 프로세스는 AWS Network Firewall 콘솔에서 사용하는 프로세스와 동일합니다. 정책에 사용하려는 규칙 그룹을 추가하고 기본 상태 비저장 작업을 제공합니다. 이 자습서에서는 네트워크 방화벽의 방화벽 정책과 마찬가지로 이 정책을 구성하십시오.

> **Note**
>
> AWS Firewall Manager Network Firewall 정책의 경우 자동 문제 해결이 자동으로 수행되므로 여기서는 자동 문제 해결을 선택하지 않도록 선택할 수 있는 옵션이 표시되지 않습니다.

10. 다음을 선택합니다.
11. 방화벽 엔드포인트의 경우 다중 방화벽 엔드포인트를 선택합니다. 이 옵션은 방화벽에 고가용성을 제공합니다. 정책을 만들 때 Firewall Manager는 보호할 퍼블릭 서브넷이 있는 각 가용 영역에 방화벽 서브넷을 생성합니다.
12. AWS Network Firewall 경로 구성의 경우, 모니터링을 선택하면 Firewall Manager가 VPC의 경로 구성 위반을 모니터링하고 경로를 준수하도록 도와주는 수정 제안 사항을 알려주도록 합니다. 필요에 따라 Firewall Manager에서 경로 구성을 모니터링하고 이러한 알림을 받지 않으려면 끄기를 선택합니다.

> **Note**
>
> 모니터링은 잘못된 경로 구성으로 인한 비준수 리소스에 대한 세부 정보를 제공하고 Firewall Manager `GetViolationDetails` API에서 수정 조치를 제안합니다. 예를 들어 네트워크 방화벽은 정책에 따라 생성된 방화벽 엔드포인트를 통해 트래픽이 라우팅되지 않는 경우 경고를 표시합니다.

> **Warning**
>
> 모니터링을 선택하면 향후 동일한 정책에 대해 이 설정을 끄기(Off)로 변경할 수 없습니다. 새 정책을 생성해야 합니다.

13. 트래픽 유형에서 방화벽 정책에 추가를 선택하여 인터넷 게이트웨이를 통해 트래픽을 라우팅합니다.
14. AWS 계정 이 정책의 영향을 받으면 포함하거나 제외할 계정을 지정하여 정책 범위를 좁힐 수 있습니다. 이 자습서에서는 내 조직에 있는 모든 계정 포함을 선택합니다.

Network 방화벽 정책의 리소스 유형은 항상 VPC입니다.

15. 리소스의 경우 지정한 태그가 있는 리소스를 포함하거나 제외하여 태그 지정을 사용하여 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
16. 다음을 선택합니다.
17. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
18. 다음을 선택합니다.
19. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don’t comply with the policy rules, but don’t auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책 변경 내용을 검토할 수 있습니다.
20. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.
21. 탐색이 끝나면 이 자습서용으로 생성한 정책을 유지하지 않으려는 경우, 정책 명칭을 선택하고, 삭제를 선택한 다음, 이 정책에서 생성한 리소스 정리를 선택하고, 마지막으로 삭제를 선택합니다.

Firewall Manager 네트워크 방화벽 정책에 대한 자세한 설명은 AWS Network Firewall 정책을 참조하세요.

AWS Firewall Manager DNS 방화벽 정책 시작하기

조직 전체에서 Amazon Route 53 Resolver DNS 방화벽을 활성화하는 데 사용하려면 AWS Firewall Manager 다음 단계를 순서대로 수행하십시오. Firewall Manager DNS 방화벽 정책에 대한 자세한 설명은 Amazon Route 53 Resolver DNS 방화벽 정책을 참조하세요.

주제

1단계: 일반적인 사전 조건 완료

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: 정책에 사용할 DNS 방화벽 규칙 그룹 생성

이 자습서를 따르려면 Amazon Route 53 Resolver DNS 방화벽에 대해 숙지하고 해당 규칙 그룹을 구성하는 방법을 알고 있어야 합니다.

AWS Firewall Manager 정책에 사용될 규칙 그룹이 DNS 방화벽에 하나 이상 있어야 합니다. DNS 방화벽에서 규칙 그룹을 아직 생성하지 않았다면 지금 생성하십시오. DNS 방화벽 사용에 대한 자세한 설명은 Amazon Route 53 개발자 가이드의 Amazon Route 53 Resolver DNS 방화벽을 참조하세요.

3단계: DNS 방화벽 정책 생성 및 적용

사전 요구 사항을 완료한 후 AWS Firewall Manager DNS 방화벽 정책을 생성합니다. DNS 방화벽 정책은 전체 조직에 대해 중앙에서 제어되는 DNS 방화벽 규칙 그룹 연결 세트를 제공합니다. AWS 또한 방화벽이 적용되는 AWS 계정 및 리소스도 정의합니다.

Firewall Manager가 DNS 방화벽 규칙 그룹 연계을 관리하는 방법에 대한 자세한 설명은 Amazon Route 53 Resolver DNS 방화벽 정책을 참조하세요.

Firewall Manager DNS 방화벽 정책을 생성하려면 (콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.
2. 탐색 창에서 보안 정책을 선택합니다.
3. 사전 조건을 충족하지 않으면 문제 해결 방법에 대한 지침이 콘솔에 표시됩니다. 지침을 따른 다음, 이 단계로 돌아와서 DNS 방화벽 정책을 만듭니다.
4. 보안 정책 생성을 선택합니다.

5. 정책 타입으로는 Amazon Route 53 Resolver DNS 방화벽을 선택합니다.
6. 지역의 경우 원하는 항목을 선택합니다 AWS 리전.
7. 다음을 선택합니다.
8. 정책 명칭에 서술적 명칭을 입력하십시오.
9. 정책 구성을 사용하면 Firewall Manager에서 관리하려는 DNS 방화벽 규칙 그룹 연계을 정의할 수 있습니다. 정책에 사용하려는 규칙 그룹을 추가합니다. VPC를 먼저 평가하고 마지막으로 평가하는 연계을 정의할 수 있습니다. 본 자습서에서는 필요에 따라 하나 또는 두 개의 규칙 그룹 연계을 추가합니다
10. 다음을 선택합니다.
11. AWS 계정 이 정책의 영향을 받는 경우 포함하거나 제외할 계정을 지정하여 정책 범위를 좁힐 수 있습니다. 이 자습서에서는 내 조직에 있는 모든 계정 포함을 선택합니다.

    DNS 방화벽 정책의 리소스 타입은 항상 VPC입니다.
12. 리소스의 경우 지정한 태그가 있는 리소스를 포함하거나 제외하여 태그 지정을 사용하여 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
13. 다음을 선택합니다.
14. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
15. 다음을 선택합니다.
16. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don’t comply with the policy rules, but don’t auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책에 적용되는 변경 내용을 검토할 수 있습니다.
17. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준

수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

18. 탐색이 끝나면 이 자습서용으로 생성한 정책을 유지하지 않으려는 경우, 정책 명칭을 선택하고, 삭제를 선택한 다음, 이 정책에서 생성한 리소스 정리를 선택하고, 마지막으로 삭제를 선택합니다.

Firewall Manager DNS 방화벽 정책에 대한 자세한 설명은 Amazon Route 53 Resolver DNS 방화벽 정책을 참조하세요.

AWS Firewall Manager팔로알토 네트웍스 클라우드 차세대 방화벽 정책 시작하기

AWS Firewall Manager 팔로알토 네트웍스 클라우드 차세대 방화벽 (NGFW) 정책을 활성화하는 데 사용하려면 다음 단계를 순서대로 수행하십시오. Palo Alto Networks 클라우드 NGFW 정책에 대한 자세한 설명은 Palo Alto Networks Cloud NGFW 정책을 참조하세요.

주제

- 1단계: 일반적인 사전 조건 완료
- 2단계: Palo Alto Networks 클라우드 NGFW 정책 사전 조건 완료
- 3단계: Palo Alto Networks 클라우드 NGFW 정책 생성 및 적용

1단계: 일반적인 사전 조건 완료

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: Palo Alto Networks 클라우드 NGFW 정책 사전 조건 완료

Palo Alto Networks 클라우드 NGFW 정책을 사용하려면 몇 가지 추가 필수 단계를 완료해야 합니다. 이 단계는 Palo Alto Networks Cloud Next Generation Firewall 정책 사전 요구 사항에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

3단계: Palo Alto Networks 클라우드 NGFW 정책 생성 및 적용

사전 요구 사항을 완료한 후 AWS Firewall Manager 팔로 알토 네트웍스 클라우드 NGFW 정책을 생성합니다.

Palo Alto Networks 클라우드 NGFW의 Firewall Manager 정책에 대한 자세한 설명은 Palo Alto Networks Cloud NGFW 정책을 참조하세요.

Palo Alto Networks Cloud NGFW에 대한 Firewall Manager 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형으로는 팔로 알토 네트웍스 클라우드 NGFW를 선택합니다. AWS 마켓플레이스에서 팔로 알토 네트웍스 클라우드 NGFW 서비스를 아직 구독하지 않았다면 먼저 구독해야 합니다. 마켓플레이스에서 구독하려면 AWS AWS 마켓플레이스 세부 정보 보기를 선택합니다.
5. 배포 모델의 경우, 분산 모델 또는 중앙 집중식 모델을 선택합니다. 배포 모델은 Firewall Manager가 정책의 엔드포인트를 관리하는 방법을 결정합니다. 분산 모델을 사용하면 Firewall Manager는 정책 범위 내에 있는 각 VPC에서 방화벽 엔드포인트를 유지 관리합니다. 중앙 집중식 모델을 사용하면 Firewall Manager는 검열 VPC에 단일 엔드포인트를 유지합니다.
6. 지역의 경우 원하는 항목을 선택합니다 AWS 리전. 여러 리전의 리소스를 보호하려면 각 리전에 대해 별도의 정책을 생성해야 합니다.
7. 다음을 선택합니다.
8. 정책 명칭에 서술적 명칭을 입력하십시오.
9. 정책 구성에서 이 정책과 연결할 Palo Alto Networks Cloud NGFW 방화벽 정책을 선택합니다. Palo Alto Networks Cloud NGFW 방화벽 정책 목록에는 Palo Alto Networks Cloud NGFW 테넌트와 관련된 모든 Palo Alto Networks Cloud NGFW 방화벽 정책이 포함되어 있습니다. 팔로알토 네트웍스 클라우드 NGFW 방화벽 정책의 생성 및 관리에 대한 자세한 내용은 팔로알토 네트웍스 클라우드 NGFW 배포 가이드의 AWSAWS Firewall Manager항목과 함께 팔로알토 네트웍스 클라우드 NGFW 배포를 참조하십시오. AWS
10. 팔로알토 네트웍스 클라우드 NGFW 로깅 (선택 사항) 의 경우 정책에 따라 기록할 팔로알토 네트웍스 클라우드 NGFW 로그 유형을 선택적으로 선택할 수 있습니다. 팔로알토 네트웍스 클라우드

NGFW 로그 유형에 대한 자세한 내용은 팔로알토 네트웍스 클라우드 NGFW 배포 가이드에서 팔로알토 네트웍스 클라우드 NGFW on에 대한 로깅 구성을 참조하십시오. AWS AWS

로그 대상의 경우, Firewall Manager에서 로그를 기록해야 하는 시기를 지정합니다.

11. 다음을 선택합니다.
12. 방화벽 엔드포인트를 생성할 때 분산 배포 모델을 사용하는지 아니면 중앙 집중식 배포 모델을 사용하는지에 따라 제3자 방화벽 엔드포인트 구성에서 다음 중 하나를 수행하십시오.
    - 이 정책에 분산 배포 모델을 사용하는 경우, 가용 영역에서 방화벽 엔드포인트를 만들 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
    - 이 정책에 중앙 집중식 배포 모델을 사용하는 경우, 검사 VPC 구성의 AWS Firewall Manager 엔드포인트 구성에서 검사 VPC 소유자의 AWS 계정 ID와 검사 VPC의 VPC ID를 입력합니다.
      - 가용 영역에서 방화벽 엔드포인트를 생성할 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
13. 다음을 선택합니다.
14. 정책 범위의 경우 이 정책이 적용되는AWS 계정 에서 다음과 같이 옵션을 선택합니다.
    - 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 조직의 모든 계정 포함을 그대로 두십시오. AWS
    - 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
    - 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

    옵션 중 하나만 선택할 수 있습니다.

    정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.

    Network Firewall 정책의 리소스 타입은 VPC입니다.

15. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 "" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

16. 크로스 계정 액세스 권한 부여에서 AWS CloudFormation 템플릿 다운로드를 선택합니다. 그러면 AWS CloudFormation 스택을 생성하는 데 사용할 수 있는 AWS CloudFormation 템플릿이 다운로드됩니다. 이 스택은 Firewall Manager에 팔로알토 네트웍스 클라우드 NGFW 리소스를 관리할 수 있는 계정 간 권한을 부여하는 AWS Identity and Access Management 역할을 생성합니다. 스택에 대한 자세한 설명은 AWS CloudFormation 사용자 가이드의 스택 작업을 참조하세요.
17. 다음을 선택합니다.
18. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
19. 다음을 선택합니다.
20. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don't comply with the policy rules, but don't auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책에 적용되는 변경 내용을 검토할 수 있습니다.

21. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

Firewall Manager Palo Alto Networks 클라우드 NGFW 정책에 대한 자세한 설명은 Palo Alto Networks Cloud NGFW 정책을 참조하세요.

AWS Firewall Manager포티게이트 CNF 정책 시작하기

서비스형 Fortigate 클라우드 네이티브 방화벽 (CNF) 은 정책에 사용할 수 있는 타사 방화벽 서비스입니다. AWS Firewall Manager Fortigate CNF for Firewall Manager를 사용하면 모든 계정에 Fortigate CNF 리소스 및 정책 세트를 생성하고 중앙에서 배포할 수 있습니다. AWS Fortigate AWS Firewall Manager CNF 정책을 활성화하는 데 사용하려면 다음 단계를 순서대로 수행하십시오. Fortigate CNF 정책에 대한 자세한 설명은 서비스 정책형 Fortigate Cloud Native Firewall(CNF) 섹션을 참조하세요.

주제

1단계: 일반적인 사전 조건 완료

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

2단계: Fortigate CNF 정책 사전 조건 완료

Fortigate CNF 정책을 사용하려면 추가로 완료해야 하는 필수 단계가 있습니다. 이 단계는 서비스로서의 Fortigate Cloud Native Firewall(CNF) 정책 사전 요구 사항에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

3단계: Fortigate CNF 정책 생성 및 적용

사전 요구 사항을 완료한 후 AWS Firewall Manager Fortigate CNF 정책을 생성합니다.

Fortigate CNF의 Firewall Manager 정책에 대한 자세한 설명은 서비스 정책형 Fortigate Cloud Native Firewall(CNF) 섹션을 참조하세요.

Fortigate CNF의 Firewall Manager 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

> **Note**
>
> Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 타입으로는 Fortigate CNF를 선택합니다. AWS 마켓플레이스에서 아직 Fortigate CNF 서비스를 구독하지 않았다면 먼저 가입해야 합니다. 마켓플레이스에서 구독하려면 AWS AWS 마켓플레이스 세부 정보 보기를 선택합니다.
5. 배포 모델의 경우, 분산 모델 또는 중앙 집중식 모델을 선택합니다. 배포 모델은 Firewall Manager가 정책의 엔드포인트를 관리하는 방법을 결정합니다. 분산 모델을 사용하면 Firewall Manager는 정책 범위 내에 있는 각 VPC에서 방화벽 엔드포인트를 유지 관리합니다. 중앙 집중식 모델을 사용하면 Firewall Manager는 검열 VPC에 단일 엔드포인트를 유지합니다.
6. 지역의 경우 원하는 항목을 선택합니다 AWS 리전. 여러 리전의 리소스를 보호하려면 각 리전에 대해 별도의 정책을 생성해야 합니다.
7. 다음을 선택합니다.
8.
9. 정책 구성에서 이 정책과 연계할 Fortigate CNF 방화벽 정책을 선택합니다. Fortigate CNF 방화벽 정책 목록에는 Fortigate CNF 테넌트와 관련된 모든 Fortigate CNF 방화벽 정책이 포함되어 있습니다. Fortigate CNF 방화벽 정책 생성 및 관리에 대한 자세한 설명은 Fortigate CNF 설명서를 참조하세요.
10. 다음을 선택합니다.
11. 방화벽 엔드포인트를 생성할 때 분산 배포 모델을 사용하는지 아니면 중앙 집중식 배포 모델을 사용하는지에 따라 제3자 방화벽 엔드포인트 구성에서 다음 중 하나를 수행하십시오.

    - 이 정책에 분산 배포 모델을 사용하는 경우, 가용 영역에서 방화벽 엔드포인트를 만들 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
    - 이 정책에 중앙 집중식 배포 모델을 사용하는 경우, 검사 VPC 구성의 AWS Firewall Manager 엔드포인트 구성에서 검사 VPC 소유자의 AWS 계정 ID와 검사 VPC의 VPC ID를 입력합니다.
      - 가용 영역에서 방화벽 엔드포인트를 생성할 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
12. 다음을 선택합니다.
13. 정책 범위의 경우 이 정책이 적용되는AWS 계정 에서 다음과 같이 옵션을 선택합니다.

- 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
- 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
- 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

옵션 중 하나만 선택할 수 있습니다.

정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.

포티게이트 CNF 정책의 리소스 유형은 VPC입니다.

14. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

15. 크로스 계정 액세스 권한 부여에서 AWS CloudFormation 템플릿 다운로드를 선택합니다. 그러면 AWS CloudFormation 스택을 생성하는 데 사용할 수 있는 AWS CloudFormation 템플릿이 다운로드됩니다. 이 스택은 Firewall Manager에 Fortigate CNF 리소스를 관리할 수 있는 계정 간 권한을 부여하는 AWS Identity and Access Management 역할을 생성합니다. 스택에 대한 자세한 설명은 AWS CloudFormation 사용자 가이드의 스택 작업을 참조하세요. 스택을 생성하려면 Fortigate CNF 포털의 계정 ID가 필요합니다.
16. 다음을 선택합니다.
17. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

18. 다음을 선택합니다.
19. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책 작업이 Identify resources that don't comply with the policy rules, but don't auto remediate(정책 규칙을 준수하지 않는 리소스를 식별하지만 자동으로 문제를 해결하지 않음)으로 설정되어 있는지 확인합니다. 이렇게 하면 정책을 활성화하기 전에 정책 변경 내용을 검토할 수 있습니다.
20. 정책이 마음에 들면 정책 생성를 선택합니다.

    AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

Fortigate CNF 정책의 Firewall Manager에 대한 자세한 설명은 서비스 정책형 Fortigate Cloud Native Firewall(CNF) 섹션을 참조하세요.

AWS Firewall Manager 정책 관련 작업

AWS Firewall Manager 는 다음과 같은 유형의 정책을 제공합니다. 각 정책 유형에 대해 다음을 정의합니다.

- AWS WAF정책 - Firewall Manager는 AWS WAF 클래식 정책을 지원합니다 AWS WAF . 두 버전 모두에 대해 정책으로 보호되는 리소스를 정의합니다.
  - AWS WAF 정책 유형에는 일련의 규칙 그룹이 웹 ACL에서 처음 실행되고 마지막에 실행됩니다. 그러면 웹 ACL을 적용하는 계정에서 계정 소유자는 두 세트 사이에서 실행할 규칙과 규칙 그룹을 추가할 수 있습니다.
  - AWS WAF 클래식 정책 유형은 단일 규칙 그룹을 사용하여 웹 ACL에서 실행합니다.
- Shield Advanced 정책 — 이 정책 유형은 지정한 리소스 유형에 대해 조직 전체에 Shield Advanced 보호를 적용합니다.
- Amazon VPC 보안 그룹 정책 — 이 정책 유형을 사용하면 조직 전체에서 사용되는 보안 그룹을 제어하고 조직 전체에 기본 규칙 세트를 적용할 수 있습니다.
- Amazon VPC 네트워크 액세스 제어 목록 (ACL) 정책 — 이 정책 유형을 사용하면 조직 전체에서 사용 중인 네트워크 ACL을 제어하고 조직 전체에 기본 네트워크 ACL 세트를 적용할 수 있습니다.
- Network Firewall 정책 - 이 정책 유형은 조직의 VPC에 AWS Network Firewall 보호를 적용합니다.

- Amazon Route 53 Resolver DNS 방화벽 정책 — 이 정책은 조직의 VPC에 DNS 방화벽 보호를 적용합니다.
- 타사 방화벽 정책 - 이 정책 유형은 타사 방화벽 보호를 적용합니다. 타사 방화벽은 AWS Marketplace의 Marketplace 콘솔을 통해 구독하여 사용할 수AWS 있습니다.
  - 팔로알토 네트웍스 클라우드 NGFW 정책 — 이 정책 유형은 팔로알토 네트웍스 클라우드 차세대 방화벽 (NGFW) 보호 및 팔로알토 네트웍스 클라우드 NGFW 규칙스택을 조직의 VPC에 적용합니다.
  - 서비스형 포티게이트 클라우드 네이티브 방화벽 (CNF) 정책 — 이 정책 유형은 Fortigate 클라우드 네이티브 방화벽 (CNF) 을 서비스 보호로 적용합니다. Fortigate CNF는 업계 최고의 고급 위협 방지, 스마트 웹 애플리케이션 방화벽(WAF) 및 API 보호를 통해 제로데이(Zero-Day) 위협을 차단하고 클라우드 인프라를 보호하는 클라우드 중심 솔루션입니다.

Firewall Manager 정책은 개별 정책 유형에 따라 상이합니다. 계정 전체에 여러 가지 정책 유형을 적용하려는 경우 여러 개의 정책을 생성할 수 있습니다. 각 유형에 대해 둘 이상의 정책을 생성할 수 있습니다.

로 AWS Organizations만든 조직에 새 계정을 추가하면 Firewall Manager는 정책 범위 내에 있는 해당 계정의 리소스에 정책을 자동으로 적용합니다.

AWS Firewall Manager 정책의 일반 설정

AWS Firewall Manager 관리형 정책에는 몇 가지 일반적인 설정과 동작이 있습니다. 모든 경우 이름을 지정하고 정책 범위를 정의하며 리소스 태깅을 사용하여 정책 범위를 제어할 수 있습니다. 수정 조치를 취하지 않고 규정을 위반하는 계정과 리소스를 보거나 규정 미준수 리소스를 자동으로 문제 해결하도록 선택할 수 있습니다.

정책 범위에 대한 자세한 내용은 AWS Firewall Manager 정책 범위을 참조하세요.

AWS Firewall Manager 정책 생성

정책을 생성하는 단계는 정책 유형에 따라 다릅니다. 필요한 정책 유형에 대한 절차를 사용해야 합니다.

> **Important**
>
> AWS Firewall Manager Amazon Route 53 또는 은 (는) 지원하지 않습니다 AWS Global Accelerator. 이러한 리소스를 Shield Advanced로 보호하려는 경우 Firewall Manager 정책을

사용할 수 없습니다. 그 대신 리소스에 AWS Shield AdvancedAWS 보호 추가의 지시 사항을 따릅니다.

주제

- 에 대한 AWS Firewall Manager 정책 생성 AWS WAF
- 클래식에 대한 AWS Firewall Manager 정책 생성 AWS WAF
- 에 대한 AWS Firewall Manager 정책 생성 AWS Shield Advanced
- AWS Firewall Manager 공통 보안 그룹 정책 생성
- AWS Firewall Manager 콘텐츠 감사 보안 그룹 정책 생성
- AWS Firewall Manager 사용 감사 보안 그룹 정책 생성
- AWS Firewall Manager 네트워크 ACL 정책 생성
- 에 대한 AWS Firewall Manager 정책 생성 AWS Network Firewall
- Amazon Route 53 리졸버 DNS 방화벽에 대한 AWS Firewall Manager 정책 생성
- 팔로알토 네트웍스 클라우드 NGFW에 대한 AWS Firewall Manager 정책 생성
- 서비스형 Fortigate 클라우드 네이티브 방화벽 (CNF) AWS Firewall Manager 정책 생성

에 대한 AWS Firewall Manager 정책 생성 AWS WAF

Firewall Manager AWS WAF 정책에서는 AWS Marketplace 셀러가 대신 생성하고 유지 관리하는 관리형 규칙 그룹을 사용할 수 있습니다. AWS 사용자 고유의 규칙 그룹을 생성하고 사용할 수도 있습니다. 규칙 그룹에 대한 자세한 내용은 AWS WAF 규칙 그룹을 참조하세요.

고유의 규칙 그룹을 사용하려는 경우 Firewall Manager AWS WAF 정책을 생성하기 전에 해당 규칙 그룹을 생성합니다. 자세한 지침은 자체 규칙 그룹 관리을 참조하세요. 개별 사용자 지정 규칙을 사용하려면 고유의 규칙 그룹을 정의하고, 해당 규칙 그룹 내에서 규칙을 정의한 다음, 정책에서 규칙 그룹을 사용해야 합니다.

방화벽 관리자 AWS WAF 정책에 대한 자세한 내용은 을 참조하십시오AWS WAF 정책.

AWS WAF (콘솔) 에 대한 방화벽 관리자 정책을 만들려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

> **Note**
>
> Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 타입에서 AWS WAF를 선택합니다.
5. [지역] 에서 원하는 항목을 선택합니다 AWS 리전. Amazon CloudFront 배포를 보호하려면 글로벌을 선택하십시오.

   여러 지역 (CloudFront 배포 제외) 의 리소스를 보호하려면 각 지역에 대해 별도의 Firewall Manager 정책을 만들어야 합니다.
6. 다음을 선택합니다.
7. 정책 명칭에 서술적 명칭을 입력하십시오. Firewall Manager는 관리하는 웹 ACL의 명칭에 정책 명칭을 포함합니다. 웹 ACL 명칭에는 `FMManagedWebACLV2-` 뒤에 여기에 입력한 정책 명칭인 - 및 웹 ACL 생성 타임스탬프(UTC 밀리초)가 있습니다. 예를 들어 `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`입니다.
8. 웹 요청 본문 검사의 경우 본문 크기 제한을 선택적으로 변경할 수 있습니다. 가격 고려 사항을 포함한 본문 검사 크기 제한에 대한 자세한 내용은 AWS WAF 개발자 안내서를 참조하세요신체 검사 크기 제한 관리.
9. 정책 규칙에서 웹 ACL에서 첫 번째와 마지막으로 AWS WAF 평가하려는 규칙 그룹을 추가합니다. AWS WAF 관리형 규칙 그룹 버전 관리를 사용하려면 버전 관리 활성화를 전환합니다. 개별 계정 관리자는 첫 번째 규칙 그룹과 마지막 규칙 그룹 사이에 규칙 및 규칙 그룹을 추가할 수 있습니다. Firewall Manager 정책의 AWS WAF 규칙 그룹 사용에 대한 AWS WAF자세한 내용은 을 참조하십시오AWS WAF 정책.

   (선택 사항) 웹 ACL에서 규칙 그룹을 사용하는 방식을 사용자 지정하려면 편집을 선택합니다. 다음은 일반적인 사용자 지정 설정입니다.

   - 관리형 규칙 그룹의 경우 일부 또는 모든 규칙에 대한 규칙 동작을 재정의하십시오. 규칙에 대한 재정의 작업을 정의하지 않는 경우 평가 시 규칙 그룹 내부에 정의된 규칙 작업이 사용됩니다. 이 옵션에 대한 자세한 내용은 AWS WAF 개발자 안내서의 규칙 그룹의 작업 재정의 옵션을 참조하세요.

- 일부 관리형 규칙 그룹에서는 추가 구성을 제공해야 합니다. 관리형 규칙 그룹 공급자가 제공한 설명서를 참조하세요. AWS 관리형 규칙 규칙 그룹과 관련된 자세한 내용은 AWS WAF 개발자 안내서의 내용을 참조하십시오AWS 에 대한 관리형 규칙 AWS WAF.

설정을 완료했으면 규칙 저장을 선택합니다.

10. 웹 ACL에 대한 기본 작업을 설정합니다. 이는 웹 요청이 웹 ACL의 어떤 규칙과도 일치하지 않을 때 AWS WAF가 취하는 조치입니다. 허용 작업을 사용하여 사용자 지정 헤더를 추가하거나 차단 작업에 대한 사용자 지정 응답을 추가할 수 있습니다. 기본 웹 ACL 작업에 대한 자세한 내용은 웹 ACL 기본 동작 섹션을 참조하세요. 웹 요청 및 응답을 사용자 지정하는 방법에 대한 자세한 내용은 AWS WAF의 사용자 지정된 웹 요청 및 응답을 참조하세요.
11. 로깅 구성의 경우 로깅 활성화를 선택하여 로깅을 활성화합니다. 로깅은 웹 ACL에서 분석한 트래픽에 대한 자세한 정보를 기록합니다. 로깅 대상 유형을 선택한 다음 구성한 로깅 대상을 선택합니다. 이름이 `aws-waf-logs-`로 시작하는 로깅 대상을 선택해야 합니다. AWS WAF 로깅 대상 구성에 대한 자세한 내용은 을 참조하십시오. AWS WAF 정책에 대한 로깅 구성
12. (선택 사항) 로그에 포함된 특정 필드와 그 값이 필요하지 않은 경우 해당 필드를 삭제합니다. 삭제할 필드를 선택한 후 추가를 선택합니다. 필요에 따라 이 작업을 반복하여 추가 필드를 삭제합니다. 삭제된 필드는 로그에서 `REDACTED`(으)로 표시됩니다. 예를 들어 URI 필드를 삭제한 경우 로그에서 URI 필드가 `REDACTED`로 나타납니다.
13. (선택 사항) 모든 요청을 로그로 전송하지 않으려면 필터링 기준과 동작을 추가합니다. 필터 로그에서 적용하려는 각 필터에 대해 필터 추가를 선택한 다음 기준과 일치하는 요청을 유지할지 아니면 삭제할지 여부를 지정합니다. 필터 추가를 완료할 때 필요 시 기본 로깅 동작을 수정합니다. 자세한 내용은 AWS WAF 개발자 안내서의 웹 ACL 로깅 구성을 참조하세요.
14. 토큰 도메인 목록을 정의하여 보호된 애플리케이션 간에 토큰을 공유하도록 할 수 있습니다. 토큰은 AWS WAF 사기 통제 계정 탈취 방지 (ATP) 및 봇 제어를 위해 AWS 관리형 규칙 규칙 그룹을 사용할 때 구현하는 애플리케이션 통합 SDK와 Challenge 작업 및 AWS WAF 작업에서 사용됩니다. CAPTCHA

    공개 접미사는 허용되지 않습니다. 예를 들면 `gov.au` 또는 `co.uk`를 토큰 도메인으로 사용할 수 없습니다.

    기본적으로 보호된 리소스의 도메인에 대한 토큰만 AWS WAF 허용합니다. 이 목록에 토큰 도메인을 추가하면 목록에 있는 모든 도메인과 관련 리소스의 도메인에 대해 토큰을 AWS WAF 수락합니다. 자세한 내용은 AWS WAF 개발자 안내서의 AWS WAF 웹 ACL 토큰 도메인 목록 구성을 참조하세요.

기존 웹 ACL을 편집할 때는 웹 ACL의 CAPTCHA와 챌린지 면제 시간만 변경할 수 있습니다. Firewall Manager 정책 세부 정보 페이지에서 이러한 설정을 찾을 수 있습니다. 이 설정에 대한 내용은 타임스탬프 만료: AWS WAF 토큰 면역 시간을 참조하세요. 기존 정책에서 연결 구성, CAPTCHA, 챌린지 또는 토큰 도메인 목록 설정을 업데이트하는 경우 Firewall Manager가 로컬 웹 ACL을 새 값으로 덮어씁니다. 하지만 정책의 연결 구성, CAPTCHA, 챌린지 또는 토큰 도메인 목록 설정을 업데이트하지 않는 경우 로컬 웹 ACL의 값은 변경되지 않습니다. 이 옵션에 대한 자세한 내용은 AWS WAF 개발자 안내서의 CAPTCHA그리고 Challenge 안에 AWS WAF을 참조하세요.

15. 웹 ACL 관리에서 Firewall Manager가 연결되지 않은 웹 ACL을 관리하도록 하려면 연결되지 않은 웹 ACL 관리를 활성화하십시오. 이 옵션을 사용하면 Firewall Manager는 하나 이상의 리소스에서 웹 ACL을 사용할 경우에만 정책 범위 내 계정에 웹 ACL을 생성합니다. 계정이 정책 범위에 포함되는 경우, 하나 이상의 리소스가 웹 ACL을 사용할 경우 Firewall Manager는 계정에 웹 ACL을 자동으로 생성합니다. 이 옵션을 활성화하면 Firewall Manager는 계정에서 연결되지 않은 웹 ACL을 한 번 정리합니다. 정리 프로세스에는 몇 시간이 걸릴 수 있습니다. Firewall Manager가 웹 ACL을 생성한 후 리소스가 정책 범위를 벗어나는 경우 Firewall Manager는 웹 ACL에서 리소스를 분리하지만 연결되지 않은 웹 ACL을 정리하지는 않습니다. Firewall Manager는 정책에서 연결되지 않은 웹 ACL의 관리를 처음 활성화한 경우에만 연결되지 않은 웹 ACL을 정리합니다.

16. 조직 내의 각 적용 가능 계정에서 웹 ACL을 생성하려고 하지만 아직 웹 ACL을 리소스에 적용하지 않으려는 경우 정책 작업에서 정책 규칙을 준수하지 않지만 자동 문제 해결을 수행하지 않는 리소스 식별을 선택합니다. 연결되지 않은 웹 ACL 관리를 선택하지 마세요. 나중에 옵션을 변경할 수 있습니다.

    그 대신 기존 범위 내 리소스에 정책을 자동으로 적용하려는 경우 비준수 리소스 자동 문제 해결을 선택합니다. Manage unassociated web ACLs를 사용하지 않도록 설정한 경우 비준수 리소스 자동 수정 옵션은 조직 내 각 해당 계정에 웹 ACL을 만들고 웹 ACL을 계정의 리소스와 연결합니다. Manage unassociated web ACLs를 사용하도록 설정한 경우 비준수 리소스 자동 수정 옵션은 웹 ACL에 연결할 수 있는 리소스가 있는 계정에서만 웹 ACL을 만들고 연결합니다.

    비준수 리소스 자동 문제 해결을 선택하면 다른 활성 Firewall Manager 정책에 의해 관리되지 않는 웹 ACL에 대해 범위 내 리소스에서 기존 웹 ACL 연결을 제거하도록 선택할 수도 있습니다. 이 옵션을 선택하면 Firewall Manager는 먼저 정책의 웹 ACL을 해당 리소스와 연결한 다음 이전 연결을 제거합니다. 리소스에 다른 활성 Firewall Manager 정책으로 관리되는 다른 웹 ACL과 연결되어 있는 경우 이 옵션은 해당 연결에 영향을 주지 않습니다.

17. 다음을 선택합니다.

18. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

- 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
- 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
- 특정 계정 집합 또는 AWS Organizations 조직 단위(OU)를 제외한 모든 항목에 정책을 적용하려는 경우, 지정된 계정과 조직 단위를 제외한 기타 모든 항목 포함을 선택한 다음 제외할 계정과 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

옵션 중 하나만 선택할 수 있습니다.

정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.

19. 리소스 유형에서 보호하려는 리소스 유형을 선택합니다.
20. 리소스의 경우 태그 지정을 사용하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
21. 다음을 선택합니다.
22. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
23. 다음을 선택합니다.
24. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책이 마음에 들면 정책 생성를 선택합니다. AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정

책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

클래식에 대한 AWS Firewall Manager 정책 생성 AWS WAF

AWS WAF 클래식용 방화벽 관리자 정책을 만들려면 (콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 타입에서 AWS WAF Classic을 선택합니다.
5. 정책에 추가하려는 AWS WAF 클래식 규칙 그룹을 이미 만든 경우 정책 생성 및 기존 규칙 그룹 추가를 선택합니다. AWS Firewall Manager 새 규칙 그룹을 생성하려면 Firewall Manager 정책 생성 및 새 규칙 그룹 추가를 선택합니다.
6. 지역의 경우 원하는 항목을 선택합니다 AWS 리전. Amazon CloudFront 리소스를 보호하려면 글로벌을 선택하십시오.

   여러 지역의 리소스 (CloudFront 리소스 제외) 를 보호하려면 각 지역에 대해 별도의 Firewall Manager 정책을 만들어야 합니다.
7. 다음을 선택합니다.
8. 규칙 그룹을 만들려면 AWS WAF 클래식 규칙 그룹 생성의 지침을 따릅니다. 규칙 그룹을 생성한 후 다음 단계를 계속 진행합니다.
9. 정책 이름을 입력합니다.
10. 기존 규칙 그룹을 추가하는 경우 드롭다운 메뉴를 사용하여 추가할 규칙 그룹을 선택한 다음 Add rule group(규칙 그룹 추가)을 선택합니다.
11. 정책에는 Action set by rule group(규칙 그룹에 설정된 작업) 및 Count(계산)라는 두 가지 가능한 작업이 있습니다. 정책과 규칙 그룹을 테스트하려면 작업을 Count(계산)로 설정합니다. 이 작업은 규칙 그룹 내 규칙으로 지정한 모든 차단 작업을 재정의합니다. 즉, 정책의 작업이 Count(계산)로

설정되면 요청이 계산되기만 하고 차단되지는 않습니다. 반대로 정책의 작업을 Action set by rule group(규칙 그룹에 설정된 작업)으로 설정하면 규칙 그룹 규칙의 작업이 사용됩니다. 적절한 작업을 선택합니다.

12. 다음을 선택합니다.
13. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

    - 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
    - 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
    - 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

    옵션 중 하나만 선택할 수 있습니다.

    정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.
14. 보호할 리소스 유형을 선택합니다.
15. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
16. 기존 리소스에 정책을 자동으로 적용하려면 Create and apply this policy to existing and new resources(이 정책을 생성하고 기존 리소스와 새 리소스에 적용)를 선택합니다.

이 옵션은 AWS 조직 내에 있는 각 적용 가능 계정에서 웹 ACL을 만들고 이 웹 ACL을 계정의 리소스와 연결합니다. 앞에서 설명한 기준(리소스 타입 및 태그)에 맞는 모든 새 리소스에 정책을 적용합니다. 그 대신 이 정책을 생성하지만 기존 리소스나 새로운 리소스에 적용 안 함을 선택하면 Firewall Manager에서는 조직 내의 각 적용 가능 계정에 웹 ACL이 생성되지만 리소스에 웹 ACL이 적용되지 않습니다. 나중에 정책을 리소스에 적용해야 합니다. 적절한 옵션을 선택합니다.

17. Replace existing associated web ACLs(기존 웹 ACL 연결 바꾸기)를 사용하면 현재 범위 내 리소스에 대해 정의된 모든 웹 ACL 연결을 제거한 다음 이 정책으로 생성 중인 웹 ACL과의 연결로 바꿀 수 있습니다. 기본적으로 Firewall Manager는 새 웹 ACL 연결을 추가하기 전에 기존 웹 ACL 연결을 제거하지 않습니다. 기존 연결을 제거하려면 이 옵션을 선택합니다.
18. 다음을 선택합니다.
19. 새 정책을 검토합니다. 변경하려면 Edit(편집)를 선택합니다. 정책이 마음에 들면 Create and apply policy(정책 생성 및 적용)를 선택합니다.

에 대한 AWS Firewall Manager 정책 생성 AWS Shield Advanced

Shield Advanced용 Firewall Manager 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형으로는 Shield Advanced를 선택합니다.

   Shield Advanced 정책을 생성하려면 Shield Advanced를 구독해야 합니다. 가입되지 않은 경우 가입하라는 메시지가 나타납니다. 구독 비용에 관한 자세한 내용은 AWS Shield Advanced 가격을 참조하세요.
5. [지역] 에서 원하는 항목을 선택합니다 AWS 리전. Amazon CloudFront 배포를 보호하려면 글로벌을 선택하십시오.

글로벌을 제외한 리전 선택의 경우 여러 리전에서 리소스를 보호하려면 각 리전에 대해 별도의 Firewall Manager 정책을 생성해야 합니다.

6. 다음을 선택합니다.
7. 이름에 설명하는 이름을 입력합니다.
8. 글로벌 리전 정책에 한해 Shield Advanced의 자동 애플리케이션 계층 DDoS 완화 관리 여부를 선택할 수 있습니다. 이 Shield Advanced 기능에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화을 참조하세요.

   자동 완화를 사용하거나 사용 중지하도록 선택하거나 무시하도록 선택할 수 있습니다. 이를 무시하도록 선택하면 Firewall Manager는 Shield Advanced 보호에 대한 자동 완화 기능을 전혀 관리하지 않습니다. 이러한 정책 옵션에 대한 자세한 내용은 자동 애플리케이션 계층 DDoS 완화을 참조하세요.
9. 웹 ACL 관리에서 Firewall Manager가 연결되지 않은 웹 ACL을 관리하도록 하려면 연결되지 않은 웹 ACL 관리를 활성화하십시오. 이 옵션을 사용하면 Firewall Manager는 하나 이상의 리소스에서 웹 ACL을 사용할 경우에만 정책 범위 내 계정에 웹 ACL을 생성합니다. 계정이 정책 범위에 포함되는 경우, 하나 이상의 리소스가 웹 ACL을 사용할 경우 Firewall Manager는 계정에 웹 ACL을 자동으로 생성합니다. 이 옵션을 활성화하면 Firewall Manager는 계정에서 연결되지 않은 웹 ACL을 한 번 정리합니다. 정리 프로세스에는 몇 시간이 걸릴 수 있습니다. Firewall Manager가 웹 ACL을 생성한 후 리소스가 정책 범위를 벗어나는 경우 Firewall Manager는 웹 ACL에서 리소스를 연결을 해제하지 않습니다. 일회성 정리에 웹 ACL을 포함하려면 먼저 웹 ACL에서 리소스를 수동으로 분리한 다음 연결되지 않은 웹 ACL 관리를 활성화해야 합니다.
10. 정책 작업에서 미준수 리소스의 문제를 자동으로 해결하지 않는 옵션을 사용하여 정책을 생성하는 것이 좋습니다. 자동 수정을 비활성화하면 새 정책을 적용하기 전에 그 효과를 평가할 수 있습니다. 변경 내용이 원하는 대로 만족스러우면 정책을 편집하고 정책 작업을 변경하여 자동 문제 해결을 활성화합니다.

    그 대신 기존 범위 내 리소스에 정책을 자동으로 적용하려는 경우 비준수 리소스 자동 문제 해결을 선택합니다. 이 옵션은 AWS 조직 내 각 해당 계정과 계정의 해당 리소스 각각에 대해 Shield Advanced 보호를 적용합니다.

    글로벌 지역 정책에 한해, 규정을 준수하지 않는 리소스에 대해 자동 수정 옵션을 선택하면 Firewall Manager가 기존 AWS WAF 클래식 웹 ACL 연결을 최신 버전 (v2) 을 사용하여 만든 웹 ACL에 대한 새 연결로 자동으로 바꾸도록 선택할 수도 있습니다. AWS WAF 이 옵션을 선택하면 Firewall Manager는 정책에 대한 웹 ACL이 아직 없는 범위 내 계정에 빈 웹 ACL을 새로 만든 후 이전 버전의 웹 ACL과의 연결을 제거하고 최신 버전 웹 ACL과의 연결을 새로 생성합니다. 이 옵션에 대한 자세한 내용은 AWS WAF 클래식 웹 ACL을 최신 버전의 웹 ACL로 교체을 참조하세요.

11. 다음을 선택합니다.
12. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

    - 조직의 모든 계정에 정책을 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 유지합니다.
    - 정책을 특정 계정이나 특정 OU (AWS Organizations 조직 구성 단위) 에 있는 계정에만 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
    - 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

    옵션 중 하나만 선택할 수 있습니다.

    정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.
13. 보호할 리소스 유형을 선택합니다.

    Firewall Manager는 Amazon Route 53 또는 AWS Global Accelerator을 지원하지 않습니다. Shield Advanced를 사용하여 이러한 서비스로부터 리소스를 보호해야 하는 경우 Firewall Manager 정책을 사용할 수 없습니다. 대신 리소스에 AWS Shield AdvancedAWS 보호 추가의 Shield Advanced 지침을 따르십시오.
14. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “” 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
15. 다음을 선택합니다.

16. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
17. 다음을 선택합니다.
18. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책이 마음에 들면 정책 생성를 선택합니다. AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

AWS Firewall Manager 공통 보안 그룹 정책 생성

공통 보안 그룹 정책의 작동 방식에 대한 자세한 내용은 공통 보안 그룹 정책을 참조하세요.

공통 보안 그룹 정책을 생성하려면 정책에 기본으로 사용할 보안 그룹을 Firewall Manager 관리자 계정에서 이미 생성한 상태여야 합니다. Amazon Virtual Private Cloud(Amazon VPC) 또는 Amazon Elastic Compute Cloud(Amazon EC2)를 통해 보안 그룹을 관리할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 작업을 참조하세요.

공통 보안 그룹 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형에서 보안 그룹을 선택합니다.
5. 보안 그룹 정책 유형에서 공통 보안 그룹을 선택합니다.
6. [지역] 에서 원하는 항목을 선택합니다 AWS 리전.
7. 다음을 선택합니다.

8. 정책 이름에 기억하기 쉬운 이름을 입력합니다.
9. 정책 규칙에서 다음을 수행합니다.

   a. 규칙 옵션에서 보안 그룹 규칙과 정책 범위 내에 있는 리소스에 적용할 제한을 선택합니다. 기본 보안 그룹의 태그를 이 정책으로 생성된 보안 그룹에 배포하도록 선택한 경우 이 정책에 따라 생성된 보안 그룹이 규정을 준수하지 않을 경우 식별 및 보고도 선택해야 합니다.

   > **Important**
   >
   > Firewall Manager는 AWS 서비스에서 추가한 시스템 태그를 복제본 보안 그룹에 배포하지 않습니다. 시스템 태그는 `aws:` 접두사로 시작합니다. 정책에 조직의 태그 정책과 충돌하는 태그가 있는 경우 Firewall Manager는 기존 보안 그룹의 태그를 업데이트하거나 새 보안 그룹을 만들지 않습니다. 태그 정책에 대한 자세한 내용은 AWS Organizations 사용 설명서의 태그 정책을 참조하십시오.

   기본 보안 그룹의 보안 그룹 참조를 이 정책에 따라 생성된 보안 그룹에 배포를 선택하면 Firewall Manager는 Amazon VPC에서 활성 피어링 연결이 있는 보안 그룹 참조만 배포합니다. 이 옵션에 대한 자세한 내용은 정책 규칙 설정을 참조하세요.

   b. 기본 보안 그룹의 경우 보안 그룹 추가를 선택한 다음 사용할 보안 그룹을 선택합니다. Firewall Manager는 Firewall Manager 관리자 계정에 있는 모든 Amazon VPC 인스턴스의 보안 그룹 목록을 채웁니다.

   기본적으로 정책당 기본 보안 그룹의 최대 수는 3개입니다. 이 설정에 대한 자세한 내용은 AWS Firewall Manager 할당량 섹션을 참조하세요.

   c. 정책 작업에서 자동으로 문제를 해결하지 않는 옵션을 사용하여 정책을 생성하는 것이 좋습니다. 이렇게 하면 정책을 적용하기 전에 새 정책의 효과를 평가할 수 있습니다. 변경 내용이 원하는 대로 만족스러우면 정책을 편집하고 정책 작업을 변경하여 규정 미준수 리소스의 자동 문제 해결을 활성화합니다.

10. 다음을 선택합니다.
11. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

    - 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
    - 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를

지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

- 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

옵션 중 하나만 선택할 수 있습니다.

정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.

12. 리소스 유형에서 보호하려는 리소스 유형을 선택합니다.

    EC2 인스턴스를 선택한 경우 각 인스턴스에 모든 탄력적 네트워크 인터페이스를 포함하거나 각 Amazon EC2 인스턴스에 기본 인터페이스만 포함하도록 선택할 수 있습니다. 범위 내 Amazon EC2 인스턴스에 두 개 이상의 탄력적 네트워크 인터페이스가 있는 경우 모든 인터페이스를 포함하는 옵션을 선택하면 Firewall Manager에서 모든 인터페이스에 정책을 적용할 수 있습니다. 자동 문제 해결을 사용하도록 설정하면 Firewall Manager에서 Amazon EC2 인스턴스의 모든 탄력적 네트워크 인터페이스에 정책을 적용할 수 없는 경우 인스턴스가 비호환으로 표시됩니다.

13. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

14. 공유 VPC 리소스의 경우 계정이 소유한 VPC 외에도 공유 VPC의 리소스에 정책을 적용하는 경우 공유 VPC의 리소스 포함을 선택합니다.
15. 다음을 선택합니다.
16. 정책 설정을 검토하여 원하는 대로 설정되었는지 확인한 다음 정책 생성을 선택합니다.

Firewall Manager는 범위 내 계정에 포함된 모든 Amazon VPC 인스턴스에서 계정당 지원되는 Amazon VPC 최대 할당량까지 기본 보안 그룹의 복제본을 생성합니다. Firewall Manager는 각 범위 내 계정의 정책 범위 내에 있는 리소스에 복제본 보안 그룹을 연결합니다. 이 정책의 작동 방식에 대한 자세한 내용은 공통 보안 그룹 정책을 참조하세요.

AWS Firewall Manager 콘텐츠 감사 보안 그룹 정책 생성

콘텐츠 감사 보안 그룹 정책의 작동 방식에 대한 자세한 내용은 콘텐츠 감사 보안 그룹 정책을 참조하세요.

일부 콘텐츠 감사 정책 설정의 경우 Firewall Manager가 템플릿으로 사용할 감사 보안 그룹을 제공해야 합니다. 예를 들어 어떤 보안 그룹에서도 허용하지 않는 모든 규칙을 포함하는 감사 보안 그룹이 있을 수 있습니다. 정책에서 사용할 수 있으려면 먼저 Firewall Manager 관리자 계정을 사용하여 이러한 감사 보안 그룹을 만들어야 합니다. Amazon Virtual Private Cloud(Amazon VPC) 또는 Amazon Elastic Compute Cloud(Amazon EC2)를 통해 보안 그룹을 관리할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 작업을 참조하세요.

콘텐츠 감사 보안 그룹 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형에서 보안 그룹을 선택합니다.
5. 보안 그룹 정책 유형에서 보안 그룹 규칙의 감사 및 적용을 선택합니다.
6. [지역] 에서 원하는 항목을 선택합니다 AWS 리전.
7. 다음을 선택합니다.
8. 정책 이름에 기억하기 쉬운 이름을 입력합니다.
9. 정책 규칙의 경우 사용하려는 관리형 또는 사용자 지정 정책 규칙 옵션을 선택합니다.

   a. 관리형 감사 정책 규칙 구성에 대해 다음을 수행합니다.

i. 감사할 보안 그룹 규칙 구성의 경우 감사 정책을 적용할 보안 그룹 규칙 유형을 선택합니다.

ii. 보안 그룹의 프로토콜, 포트 및 CIDR 범위 설정을 기반으로 하는 감사 규칙 등의 작업을 수행하려면 지나치게 허용적인 보안 그룹 규칙 감사를 선택하고 원하는 옵션을 선택하십시오.

모든 트래픽 규칙 허용을 선택하면 감사하려는 애플리케이션을 지정하는 사용자 지정 애플리케이션 목록을 제공할 수 있습니다. 사용자 정의 애플리케이션 목록 및 정책에서 이를 사용하는 방법에 대한 자세한 내용은 관리형 목록 및 관리형 목록 사용을 참조하세요.

프로토콜 목록을 사용하는 선택 항목의 경우 기존 목록을 사용하고 새 목록을 만들 수 있습니다. 프로토콜 목록 및 정책에서 이를 사용하는 방법에 대한 자세한 내용은 관리형 목록 및 관리형 목록 사용을 참조하세요.

iii. 예약된 CIDR 범위나 예약되지 않은 CIDR 범위에 대한 액세스를 기반으로 고위험 애플리케이션을 감사하려면 고위험 애플리케이션 감사를 선택하고 원하는 옵션을 선택합니다.

예약된 CIDR 범위에만 액세스할 수 있는 애플리케이션과 예약되지 않은 CIDR 범위에 액세스할 수 있는 애플리케이션은 상호 배타적입니다. 모든 정책에서 최대 한 개만 선택할 수 있습니다.

애플리케이션 목록을 사용하는 선택 항목의 경우 기존 목록을 사용하고 새 목록을 만들 수 있습니다. 애플리케이션 목록 및 정책에서 이를 사용하는 방법에 대한 자세한 내용은 관리형 목록 및 관리형 목록 사용을 참조하세요.

iv. 재정의 설정을 사용하면 정책의 다른 설정을 명시적으로 재정의할 수 있습니다. 정책에 설정한 다른 옵션을 준수하는지 여부에 관계없이 특정 보안 그룹 규칙을 항상 허용하거나 항상 거부하도록 선택할 수 있습니다.

이 옵션의 경우 감사 보안 그룹을 허용 규칙 또는 거부 규칙 템플릿으로 제공합니다. 감사 보안 그룹에서 감사 보안 그룹 추가를 선택하고 사용하려는 보안 그룹을 선택합니다. Firewall Manager는 Firewall Manager 관리자 계정에 있는 모든 Amazon VPC 인스턴스의 감사 보안 그룹 목록을 채웁니다. 정책의 감사 보안 그룹 수에 대한 기본 최대 할당량은 1입니다. 할당량 증가에 대한 자세한 내용은 AWS Firewall Manager 할당량을 참조하세요.

b. 사용자 지정 정책 규칙 설정에서 다음을 수행합니다.

i. 규칙 옵션에서 감사 보안 그룹에 정의된 규칙만 허용할지 또는 모든 규칙을 거부할지를 선택합니다. 이 옵션에 대한 자세한 내용은 콘텐츠 감사 보안 그룹 정책을 참조하세요.

ii. 감사 보안 그룹에서 감사 보안 그룹 추가를 선택하고 사용하려는 보안 그룹을 선택합니다. Firewall Manager는 Firewall Manager 관리자 계정에 있는 모든 Amazon VPC 인스턴스의 감사 보안 그룹 목록을 채웁니다. 정책의 감사 보안 그룹 수에 대한 기본 최대 할당량은 1입니다. 할당량 증가에 대한 자세한 내용은 AWS Firewall Manager 할당량을 참조하세요.

iii. 정책 작업에서 자동으로 문제를 해결하지 않는 옵션을 사용하여 정책을 생성해야 합니다. 이렇게 하면 정책을 적용하기 전에 새 정책의 효과를 평가할 수 있습니다. 변경 내용이 원하는 대로 만족스러우면 정책을 편집하고 정책 작업을 변경하여 규정 미준수 리소스의 자동 문제 해결을 활성화합니다.

10. 다음을 선택합니다.
11. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

    - 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
    - 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
    - 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

    옵션 중 하나만 선택할 수 있습니다.

    정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.
12. 리소스 유형에서 보호하려는 리소스 유형을 선택합니다.
13. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

14. 다음을 선택합니다.
15. 정책 설정을 검토하여 원하는 대로 설정되었는지 확인한 다음 정책 생성을 선택합니다.

Firewall Manager에서는 정책 규칙 설정에 따라 감사 보안 그룹을 AWS 조직의 범위 내 보안 그룹과 비교합니다. 정책 콘솔에서 정책 상태를 검토할 수 있습니다. AWS Firewall Manager 정책이 생성된 후 정책을 편집하고 자동 문제 해결을 활성화하여 감사 보안 그룹 정책을 시행할 수 있습니다. 이 정책의 작동 방식에 대한 자세한 내용은 콘텐츠 감사 보안 그룹 정책을 참조하세요.

AWS Firewall Manager 사용 감사 보안 그룹 정책 생성

사용 감사 보안 그룹 정책의 작동 방식에 대한 자세한 내용은 사용 감사 보안 그룹 정책을 참조하세요.

감사 감사 보안 그룹 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형에서 보안 그룹을 선택합니다.
5. 보안 그룹 정책 유형에서 연결되지 않은 보안 그룹 및 중복 보안 그룹의 감사 및 적용을 선택합니다.
6. [지역] 에서 원하는 항목을 선택합니다 AWS 리전.
7. 다음을 선택합니다.
8. 정책 이름에 기억하기 쉬운 이름을 입력합니다.
9. 정책 규칙에서 사용 가능한 옵션 중 하나 또는 둘 다를 선택합니다.

- 이 정책 범위 내의 보안 그룹은 최소한 하나 이상의 리소스에서 사용되어야 합니다를 선택하면 Firewall Manager가 사용되지 않는 것으로 판단한 보안 그룹을 모두 제거합니다. 이 규칙을 사용하도록 설정하면 Firewall Manager는 정책을 저장할 때 마지막으로 규칙을 실행합니다.

  Firewall Manager에서 사용량을 결정하는 방법과 수정 시기에 대한 자세한 내용은 을 참조하십시오사용 감사 보안 그룹 정책.

  > **Note**
  >
  > 이 사용 감사 보안 그룹 정책 유형을 사용할 때는 짧은 시간 내에 범위 내 보안 그룹의 연결 상태를 여러 번 변경하지 마십시오. 이렇게 하면 Firewall Manager에서 해당 이벤트를 놓칠 수 있습니다.

  기본적으로 Firewall Manager는 보안 그룹을 사용하지 않는 즉시 이 정책 규칙을 준수하지 않는 것으로 간주합니다. 선택적으로 보안 그룹이 비준수로 간주되기 전에 사용하지 않고 존재할 수 있는 시간 (분) 을 최대 525,600분 (365일) 까지 지정할 수 있습니다. 이 설정을 사용하여 새 보안 그룹을 리소스와 연결할 시간을 확보할 수 있습니다.

  > **Important**
  >
  > 기본값인 0이 아닌 시간 (분) 을 지정하는 경우 에서 간접 관계를 활성화해야 합니다 AWS Config. 그렇지 않으면 사용 감사 보안 그룹 정책이 의도한 대로 작동하지 않습니다. 의 간접 관계에 대한 자세한 내용은 AWS Config 개발자 안내서의 간접 관계를 참조하십시오. AWS Config AWS Config

- 이 정책 범위 내의 보안 그룹은 고유해야 합니다를 선택하면 Firewall Manager는 정책 하나만 모든 리소스와 연결되도록 중복 보안 그룹을 통합합니다. 이 항목을 선택하면 Firewall Manager는 정책을 저장할 때 이 규칙을 첫 번째로 실행합니다.

10. 정책 작업에서 자동으로 문제를 해결하지 않는 옵션을 사용하여 정책을 생성하는 것이 좋습니다. 이렇게 하면 정책을 적용하기 전에 새 정책의 효과를 평가할 수 있습니다. 변경 내용이 원하는 대로 만족스러우면 정책을 편집하고 정책 작업을 변경하여 규정 미준수 리소스의 자동 문제 해결을 활성화합니다.
11. 다음을 선택합니다.
12. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

- 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
- 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
- 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

옵션 중 하나만 선택할 수 있습니다.

정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.

13. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
14. 다음을 선택합니다.
15. 정책 범위에서 Firewall Manager 관리자 계정을 제외하지 않은 경우 Firewall Manager에서 이 작업을 수행하라는 메시지가 표시됩니다. 이렇게 하면 Firewall Manager 관리자 계정에서 어떤 보안 그룹을 공통 및 감사 보안 그룹 정책에 사용할지를 수동으로 제어할 수 있습니다. 이 대화 상자에서 원하는 옵션을 선택합니다.
16. 정책 설정을 검토하여 원하는 대로 설정되었는지 확인한 다음 정책 생성을 선택합니다.

보안 그룹이 고유해야 한다는 옵션을 선택한 경우 Firewall Manager에서는 각 범위 내 Amazon VPC 인스턴스에서 중복 보안 그룹을 검색합니다. 그런 다음 하나 이상의 리소스에서 각 보안 그룹을 사용하도록 선택한 경우 Firewall Manager가 규칙에 지정된 시간 동안 사용되지 않은 상태로 남아 있는 보안

그룹을 검색합니다. 정책 콘솔에서 정책 상태를 검토할 수 있습니다. AWS Firewall Manager 이 정책의 작동 방식에 대한 자세한 내용은 사용 감사 보안 그룹 정책을 참조하세요.

AWS Firewall Manager 네트워크 ACL 정책 생성

네트워크 ACL 정책의 작동 방식에 대한 자세한 내용은 을 참조하십시오. 네트워크 ACL 정책

네트워크 ACL 정책을 생성하려면 Amazon VPC 서브넷과 함께 사용할 네트워크 ACL을 정의하는 방법을 알아야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL을 사용한 서브넷 트래픽 제어 및 네트워크 ACL 사용을 참조하십시오.

네트워크 ACL 정책을 만들려면 (콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형에서 네트워크 ACL을 선택합니다.
5. 지역에서 하나를 선택합니다. AWS 리전
6. 다음을 선택합니다.
7. 정책 명칭에 서술적 명칭을 입력하십시오.
8. 정책 규칙의 경우 Firewall Manager에서 관리하는 네트워크 ACL에서 항상 실행할 규칙을 정의하십시오. 네트워크 ACL은 인바운드 및 아웃바운드 트래픽을 모니터링하고 처리하므로 정책에서 양방향에 대한 규칙을 정의합니다.

   어느 방향에서든 항상 먼저 실행할 규칙과 항상 마지막에 실행할 규칙을 정의합니다. Firewall Manager가 관리하는 네트워크 ACL에서 계정 소유자는 이러한 첫 번째 규칙과 마지막 규칙 사이에서 실행할 사용자 지정 규칙을 정의할 수 있습니다.
9. 정책 조치에서 비준수 서브넷과 네트워크 ACL을 식별하되 아직 수정 조치를 취하지 않으려는 경우 정책 규칙을 준수하지 않지만 자동 수정하지 않는 리소스 식별을 선택합니다. 나중에 옵션을 변경할 수 있습니다.

대신 기존 범위 내 서브넷에 정책을 자동으로 적용하려면 규정을 준수하지 않는 모든 리소스에 자동 수정 적용을 선택하십시오. 이 옵션을 사용하면 정책 규칙의 트래픽 처리 동작이 네트워크 ACL에 있는 사용자 지정 규칙과 충돌하는 경우 강제로 업데이트를 적용할지 여부도 지정할 수 있습니다. 수정 강제 적용 여부에 관계없이 Firewall Manager는 규정 준수 위반에서 충돌하는 규칙을 보고합니다.

10. 다음을 선택합니다.
11. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

    - 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 조직의 모든 계정 포함을 그대로 두십시오. AWS
    - 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
    - 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

    옵션 중 하나만 선택할 수 있습니다.

    정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예를 들어 특정 계정만 포함하는 경우 Firewall Manager는 다른 새 계정에 정책을 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.
12. 리소스 유형의 경우 설정이 서브넷으로 고정되어 있습니다.
13. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
14. 다음을 선택합니다.

15. 정책 설정을 검토하여 원하는 대로 설정되었는지 확인한 다음 정책 생성을 선택합니다.

Firewall Manager는 정책을 생성하고 설정에 따라 범위 내 네트워크 ACL을 모니터링하고 관리하기 시작합니다. 이 정책의 작동 방식에 대한 자세한 내용은 네트워크 ACL 정책을 참조하세요.

에 대한 AWS Firewall Manager 정책 생성 AWS Network Firewall

Firewall Manager 네트워크 방화벽 정책에서는 AWS Network Firewall에서 관리하는 규칙 그룹을 사용합니다. 규칙 그룹 관리에 대한 자세한 내용은 네트워크 방화벽 개발자 안내서의 AWS Network Firewall 규칙 그룹을 참조하세요.

Firewall Manager 네트워크 방화벽 정책에 대한 자세한 설명은 AWS Network Firewall 정책을 참조하세요.

AWS Network Firewall (콘솔) 에 대한 방화벽 관리자 정책을 만들려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 타입에서 AWS Network Firewall를 선택합니다.
5. 방화벽 관리 유형에서 Firewall Manager에서 정책의 방화벽을 관리하는 방법을 선택합니다. 다음 옵션 중 하나를 선택합니다.

   - 분산 - Firewall Manager는 정책 범위 내에 있는 각 VPC에서 방화벽 엔드포인트를 생성 및 유지 관리합니다.
   - 중앙 집중식 - Firewall Manager는 단일 검사 VPC에서 엔드포인트를 생성하고 유지 관리합니다.
   - 기존 방화벽 가져오기 - Firewall Manager는 리소스 세트를 사용하여 네트워크 방화벽에서 기존 방화벽을 가져옵니다. 리소스 세트에 대한 자세한 내용은 Firewall Manager에서 리소스 세트 관련 작업을 참조하세요.

6. [지역] 에서 원하는 항목을 선택합니다 AWS 리전. 여러 리전의 리소스를 보호하려면 각 리전에 대해 별도의 정책을 생성해야 합니다.
7. 다음을 선택합니다.
8. 정책 명칭에 서술적 명칭을 입력하십시오. Firewall Manager는 생성하는 네트워크 방화벽 방화벽 및 방화벽 정책의 이름에 정책 이름을 포함합니다.
9. AWS Network Firewall 정책 구성에서 네트워크 방화벽에서와 같이 방화벽 정책을 구성합니다. 상태 비저장 및 상태 저장 규칙 그룹을 추가하고 정책의 기본 동작을 지정합니다. 선택적으로 정책의 상태 저장 규칙 평가 순서와 기본 동작, 로깅 구성을 설정할 수 있습니다. 네트워크 방화벽 방화벽 정책 관리에 대한 자세한 내용은 AWS Network Firewall 개발자 안내서의 AWS Network Firewall 방화벽 정책을 참조하세요.

   Firewall Manager 네트워크 방화벽 정책을 생성하면 Firewall Manager는 범위 내에 있는 계정에 대한 방화벽 정책을 생성합니다. 개별 계정 관리자는 방화벽 정책에 규칙 그룹을 추가할 수 있지만 여기에서 제공하는 구성을 변경할 수는 없습니다.
10. 다음을 선택합니다.
11. 이전 단계에서 선택한 방화벽 관리 유형에 따라 다음 중 하나를 수행합니다.

    - 분산 방화벽 관리 유형을 사용하는 경우 방화벽 엔드포인트 위치의 AWS Firewall Manager 엔드포인트 구성에서 다음 옵션 중 하나를 선택합니다.
      - 사용자 지정 엔드포인트 구성 - Firewall Manager는 정책 범위 내 지정한 가용 영역에서 각 VPC에 대한 방화벽을 생성합니다. 각 방화벽에는 하나 이상의 방화벽 엔드포인트가 포함됩니다.
        - 가용 영역에서 방화벽 엔드포인트를 생성할 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
        - Firewall Manager가 VPC의 방화벽 서브넷에 사용할 CIDR 블록을 제공하려면 해당 블록은 모두 /28 CIDR 블록이어야 합니다. 줄마다 블록 하나를 입력합니다. 이를 생략하면 Firewall Manager가 VPC에서 사용할 수 있는 IP 주소 중에서 사용자를 대신하여 IP 주소를 선택합니다.

          > **Note**
          >
          > AWS Firewall Manager Network Firewall 정책의 경우 자동 문제 해결이 자동으로 수행되므로 여기서는 자동 문제 해결을 선택하지 않도록 선택할 수 있는 옵션이 표시되지 않습니다.

- 자동 엔드포인트 구성 - Firewall Manager는 VPC의 퍼블릭 서브넷이 있는 가용 영역에 방화벽 엔드포인트를 자동으로 생성합니다.
  - 방화벽 엔드포인트 구성의 경우 Firewall Manager에서 방화벽 엔드포인트를 관리하는 방법을 지정합니다. 고가용성을 위해 여러 엔드포인트를 사용하는 것이 좋습니다.
- 이 정책에 중앙 집중식 방화벽 관리 유형을 사용하는 경우 검사 VPC 구성의 AWS Firewall Manager 엔드포인트 구성에서 검사 VPC 소유자의 AWS 계정 ID와 검사 VPC의 VPC ID를 입력합니다.
  - 가용 영역에서 방화벽 엔드포인트를 생성할 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
  - Firewall Manager가 VPC의 방화벽 서브넷에 사용할 CIDR 블록을 제공하려면 해당 블록은 모두 /28 CIDR 블록이어야 합니다. 줄마다 블록 하나를 입력합니다. 이를 생략하면 Firewall Manager가 VPC에서 사용할 수 있는 IP 주소 중에서 사용자를 대신하여 IP 주소를 선택합니다.

  > **Note**
  >
  > AWS Firewall Manager Network Firewall 정책의 경우 자동 문제 해결이 자동으로 수행되므로 여기서는 자동 문제 해결을 선택하지 않도록 선택할 수 있는 옵션이 표시되지 않습니다.

- 기존 방화벽 가져오기 방화벽 관리 유형을 사용하는 경우 리소스 세트에 리소스 세트를 하나 이상 추가합니다. 리소스 세트는 이 정책에서 중앙에서 관리하려는 조직 계정이 소유한 기존 네트워크 방화벽 방화벽을 정의합니다. 정책에 리소스 세트를 추가하려면 먼저 콘솔이나 API를 사용하여 리소스 세트를 만들어야 합니다. PutResourceSet 리소스 세트에 대한 자세한 내용은 Firewall Manager에서 리소스 세트 관련 작업을 참조하세요. 네트워크 방화벽에서 기존 방화벽을 가져오는 방법에 대한 자세한 내용은 기존 방화벽 가져오기를 참조하세요.

12. 다음을 선택합니다.
13. 정책이 분산 방화벽 관리 유형을 사용하는 경우 경로 관리에서 Firewall Manager가 각 방화벽 엔드포인트를 통해 라우팅되어야 하는 트래픽을 모니터링하고 이에 대해 경고할지 여부를 선택합니다.

> **Note**
>
> 모니터링을 선택하면 나중에 설정을 끄기로 변경할 수 없습니다. 모니터링은 정책을 삭제할 때까지 계속됩니다.

14. 트래픽 유형에는 방화벽 검사를 위해 트래픽을 라우팅할 트래픽 엔드포인트를 선택적으로 추가할 수 있습니다.
15. 필수 AZ 간 트래픽 허용의 경우 이 옵션을 활성화하면 Firewall Manager는 자체 방화벽 엔드포인트가 없는 가용 영역에 대해 검사를 위해 가용 영역 밖으로 트래픽을 보내는 규정을 준수하는 라우팅으로 간주합니다. 엔드포인트가 있는 가용 영역은 항상 자체 트래픽을 검사해야 합니다.
16. 다음을 선택합니다.
17. 정책 범위의 경우 이 정책이 적용되는AWS 계정 에서 다음과 같이 옵션을 선택합니다.

    - 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
    - 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
    - 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

    옵션 중 하나만 선택할 수 있습니다.

    정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.
18. Network Firewall 정책의 리소스 타입은 VPC입니다.
19. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
20. 다음을 선택합니다.

21. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
22. 다음을 선택합니다.
23. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책이 마음에 들면 정책 생성를 선택합니다. AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

Amazon Route 53 리졸버 DNS 방화벽에 대한 AWS Firewall Manager 정책 생성

Firewall Manager DNS 방화벽 정책에서는 Amazon Route 53 Resolver DNS 방화벽에서 관리하는 규칙 그룹을 사용합니다. 규칙 그룹 관리에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 DNS 방화벽 규칙 그룹 및 규칙 관리를 참조하세요.

Firewall Manager DNS 방화벽 정책에 대한 자세한 설명은 Amazon Route 53 Resolver DNS 방화벽 정책을 참조하세요.

Amazon Route 53 Resolver DNS 방화벽용 Firewall Manager 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형으로는 Amazon Route 53 Resolver DNS Firewall을 선택합니다.
5. [지역] 에서 원하는 항목을 선택합니다 AWS 리전. 여러 리전의 리소스를 보호하려면 각 리전에 대해 별도의 정책을 생성해야 합니다.
6. 다음을 선택합니다.

7. 정책 명칭에 서술적 명칭을 입력하십시오.
8. 정책 구성에서 DNS Firewall이 VPC의 규칙 그룹 연결 중 첫 번째와 마지막으로 평가하도록 하려는 규칙 그룹을 추가합니다. 정책에는 최대 2개의 규칙 그룹을 추가할 수 있습니다.

   Firewall Manager DNS 방화벽 정책을 생성하면 Firewall Manager는 사용자가 제공한 연결 우선순위에 따라 범위 내에 있는 VPC와 계정에 대해 규칙 그룹 연결을 생성합니다. 개별 계정 관리자는 첫 번째 연결과 마지막 연결 사이에 규칙 그룹 연결을 추가할 수 있지만 여기서 정의한 연결을 변경할 수는 없습니다. 자세한 내용은 Amazon Route 53 Resolver DNS 방화벽 정책을 참조하세요.
9. 다음을 선택하세요.
10. 이 정책이 적용되는AWS 계정 의 경우 다음과 같이 옵션을 선택합니다.

    - 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
    - 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
    - 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

    옵션 중 하나만 선택할 수 있습니다.

    정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.
11. DNS 방화벽 정책의 리소스 유형은 VPC입니다.
12. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

13. 다음을 선택합니다.
14. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
15. 다음을 선택합니다.
16. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책이 마음에 들면 정책 생성를 선택합니다. AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

팔로알토 네트웍스 클라우드 NGFW에 대한 AWS Firewall Manager 정책 생성

팔로알토 네트웍스 클라우드 차세대 방화벽 (팔로알토 네트웍스 클라우드 NGFW) 에 대한 방화벽 관리자 정책에 따라 Firewall Manager를 사용하여 팔로알토 네트웍스 클라우드 NGFW 리소스를 배포하고 모든 계정에서 NGFW 룰스택을 중앙에서 관리할 수 있습니다. AWS

Firewall Manager Palo Alto Networks Cloud NGFW 정책에 대한 자세한 내용은 Palo Alto Networks Cloud NGFW 정책을 참조하세요. Firewall Manager에 대한 Palo Alto Networks Cloud NGFW를 구성하고 관리하는 방법에 대한 자세한 내용은 AWS설명서에서 Palo Alto Networks Palo Alto Networks Cloud NGFW를 참조하세요.

필수 조건

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

Palo Alto Networks Cloud NGFW에 대한 Firewall Manager 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

> **Note**
>
> Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형으로는 팔로 알토 네트웍스 클라우드 NGFW를 선택합니다. AWS 마켓플레이스에서 팔로 알토 네트웍스 클라우드 NGFW 서비스를 아직 구독하지 않았다면 먼저 구독해야 합니다. 마켓플레이스에서 구독하려면 AWS AWS 마켓플레이스 세부 정보 보기를 선택합니다.
5. 배포 모델의 경우, 분산 모델 또는 중앙 집중식 모델을 선택합니다. 배포 모델은 Firewall Manager가 정책의 엔드포인트를 관리하는 방법을 결정합니다. 분산 모델을 사용하면 Firewall Manager는 정책 범위 내에 있는 각 VPC에서 방화벽 엔드포인트를 유지 관리합니다. 중앙 집중식 모델을 사용하면 Firewall Manager는 검열 VPC에 단일 엔드포인트를 유지합니다.
6. 지역의 경우 원하는 항목을 선택합니다 AWS 리전. 여러 리전의 리소스를 보호하려면 각 리전에 대해 별도의 정책을 생성해야 합니다.
7. 다음을 선택합니다.
8. 정책 명칭에 서술적 명칭을 입력하십시오.
9. 정책 구성에서 이 정책과 연결할 Palo Alto Networks Cloud NGFW 방화벽 정책을 선택합니다. Palo Alto Networks Cloud NGFW 방화벽 정책 목록에는 Palo Alto Networks Cloud NGFW 테넌트와 관련된 모든 Palo Alto Networks Cloud NGFW 방화벽 정책이 포함되어 있습니다. 팔로알토 네트웍스 클라우드 NGFW 방화벽 정책의 생성 및 관리에 대한 자세한 내용은 팔로알토 네트웍스 클라우드 NGFW 배포 가이드의 AWSAWS Firewall Manager항목과 함께 팔로알토 네트웍스 클라우드 NGFW 배포를 참조하십시오. AWS
10. 팔로알토 네트웍스 클라우드 NGFW 로깅 (선택 사항) 의 경우 정책에 따라 기록할 팔로알토 네트웍스 클라우드 NGFW 로그 유형을 선택적으로 선택할 수 있습니다. 팔로알토 네트웍스 클라우드 NGFW 로그 유형에 대한 자세한 내용은 팔로알토 네트웍스 클라우드 NGFW 배포 가이드에서 팔로알토 네트웍스 클라우드 NGFW on에 대한 로깅 구성을 참조하십시오. AWS AWS

    로그 대상의 경우, Firewall Manager에서 로그를 기록해야 하는 시기를 지정합니다.
11. 다음을 선택합니다.
12. 방화벽 엔드포인트를 생성할 때 분산 배포 모델을 사용하는지 아니면 중앙 집중식 배포 모델을 사용하는지에 따라 제3자 방화벽 엔드포인트 구성에서 다음 중 하나를 수행하십시오.

- 이 정책에 분산 배포 모델을 사용하는 경우, 가용 영역에서 방화벽 엔드포인트를 만들 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
- 이 정책에 중앙 집중식 배포 모델을 사용하는 경우, 검사 VPC 구성의 AWS Firewall Manager 엔드포인트 구성에서 검사 VPC 소유자의 AWS 계정 ID와 검사 VPC의 VPC ID를 입력합니다.
  - 가용 영역에서 방화벽 엔드포인트를 생성할 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.

13. Firewall Manager가 VPC의 방화벽 서브넷에 사용할 CIDR 블록을 제공하려면 해당 블록은 모두 /28 CIDR 블록이어야 합니다. 줄마다 블록 하나를 입력합니다. 이를 생략하면 Firewall Manager가 VPC에서 사용할 수 있는 IP 주소 중에서 사용자를 대신하여 IP 주소를 선택합니다.

> **Note**
>
> AWS Firewall Manager Network Firewall 정책의 경우 자동 문제 해결이 자동으로 수행되므로 여기서는 자동 문제 해결을 선택하지 않도록 선택할 수 있는 옵션이 표시되지 않습니다.

14. 다음을 선택합니다.
15. 정책 범위의 경우 이 정책이 적용되는AWS 계정 에서 다음과 같이 옵션을 선택합니다.

- 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
- 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
- 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

옵션 중 하나만 선택할 수 있습니다.

정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용

하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.

16. Network Firewall 정책의 리소스 타입은 VPC입니다.
17. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
18. 크로스 계정 액세스 권한 부여에서 AWS CloudFormation 템플릿 다운로드를 선택합니다. 그러면 AWS CloudFormation 스택을 생성하는 데 사용할 수 있는 AWS CloudFormation 템플릿이 다운로드됩니다. 이 스택은 Firewall Manager에 팔로알토 네트웍스 클라우드 NGFW 리소스를 관리할 수 있는 계정 간 권한을 부여하는 AWS Identity and Access Management 역할을 생성합니다. 스택에 대한 자세한 설명은 AWS CloudFormation 사용자 가이드의 스택 작업을 참조하세요.
19. 다음을 선택합니다.
20. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
21. 다음을 선택합니다.
22. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책이 마음에 들면 정책 생성를 선택합니다. AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

서비스형 Fortigate 클라우드 네이티브 방화벽 (CNF) AWS Firewall Manager 정책 생성

Fortigate CNF에 대한 방화벽 관리자 정책을 사용하면 방화벽 관리자를 사용하여 모든 계정에 Fortigate CNF 리소스를 배포하고 관리할 수 있습니다. AWS

Fortigate CNF 정책의 Firewall Manager에 대한 자세한 설명은 서비스 정책형 Fortigate Cloud Native Firewall(CNF)을 참조하세요. Firewall Manager와 함께 사용하도록 Fortigate CNF를 구성하는 방법에 대한 자세한 내용은 Fortinet 설명서를 참조하세요.

필수 조건

AWS Firewall Manager의 계정을 준비하려면 몇 가지 필수 단계를 거쳐야 합니다. 이 단계는 AWS Firewall Manager 전제 조건에서 설명합니다. 그 다음 단계로 진행하기 전에 사전 조건을 모두 완료하십시오.

Fortigate CNF의 Firewall Manager 정책을 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책 생성을 선택합니다.
4. 정책 유형에서, 서비스형 Fortigate Cloud Native Firewall(CNF)를 선택하세요. AWS 마켓플레이스에서 아직 Fortigate CNF 서비스를 구독하지 않았다면 먼저 가입해야 합니다. 마켓플레이스에서 구독하려면 AWS AWS 마켓플레이스 세부 정보 보기를 선택합니다.
5. 배포 모델의 경우, 분산 모델 또는 중앙 집중식 모델을 선택합니다. 배포 모델은 Firewall Manager가 정책의 엔드포인트를 관리하는 방법을 결정합니다. 분산 모델을 사용하면 Firewall Manager는 정책 범위 내에 있는 각 VPC에서 방화벽 엔드포인트를 유지 관리합니다. 중앙 집중식 모델을 사용하면 Firewall Manager는 검열 VPC에 단일 엔드포인트를 유지합니다.
6. 지역의 경우 원하는 항목을 선택합니다 AWS 리전. 여러 리전의 리소스를 보호하려면 각 리전에 대해 별도의 정책을 생성해야 합니다.
7. 다음을 선택합니다.
8. 정책 명칭에 서술적 명칭을 입력하십시오.
9. 정책 구성에서 이 정책과 연계할 Fortigate CNF 방화벽 정책을 선택합니다. Fortigate CNF 방화벽 정책 목록에는 Fortigate CNF 테넌트와 관련된 모든 Fortigate CNF 방화벽 정책이 포함되어 있습니다. Fortigate CNF 테넌트 생성 및 관리에 대한 자세한 내용은 Fortigate 설명서를 참조하세요.
10. 다음을 선택합니다.
11. 방화벽 엔드포인트를 생성할 때 분산 배포 모델을 사용하는지 아니면 중앙 집중식 배포 모델을 사용하는지에 따라 제3자 방화벽 엔드포인트 구성에서 다음 중 하나를 수행하십시오.

- 이 정책에 분산 배포 모델을 사용하는 경우, 가용 영역에서 방화벽 엔드포인트를 만들 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.
- 이 정책에 중앙 집중식 배포 모델을 사용하는 경우, 검사 VPC 구성의 AWS Firewall Manager 엔드포인트 구성에서 검사 VPC 소유자의 AWS 계정 ID와 검사 VPC의 VPC ID를 입력합니다.
  - 가용 영역에서 방화벽 엔드포인트를 생성할 가용 영역을 선택합니다. 가용 영역 명칭 또는 가용 영역 ID별로 가용 영역을 선택할 수 있습니다.

12. Firewall Manager가 VPC의 방화벽 서브넷에 사용할 CIDR 블록을 제공하려면 해당 블록은 모두 /28 CIDR 블록이어야 합니다. 줄마다 블록 하나를 입력합니다. 이를 생략하면 Firewall Manager가 VPC에서 사용할 수 있는 IP 주소 중에서 사용자를 대신하여 IP 주소를 선택합니다.

> **Note**
>
> AWS Firewall Manager Network Firewall 정책의 경우 자동 문제 해결이 자동으로 수행되므로 여기서는 자동 문제 해결을 선택하지 않도록 선택할 수 있는 옵션이 표시되지 않습니다.

13. 다음을 선택합니다.
14. 정책 범위의 경우 이 정책이 적용되는AWS 계정 에서 다음과 같이 옵션을 선택합니다.

- 정책을 조직의 모든 계정에 적용하려면 기본 선택인 내 AWS 조직의 모든 계정 포함을 그대로 두십시오.
- 특정 계정이나 특정 AWS Organizations 조직 단위 (OU) 에 있는 계정에만 정책을 적용하려면 지정된 계정 및 조직 단위만 포함을 선택한 다음 포함하려는 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.
- 특정 계정 집합이나 OU (AWS Organizations 조직 구성 단위) 를 제외한 모든 항목에 정책을 적용하려면 지정된 계정 및 조직 단위 제외 및 다른 모든 구성 단위 포함을 선택한 다음 제외할 계정 및 OU를 추가합니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU 및 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 동등합니다.

옵션 중 하나만 선택할 수 있습니다.

정책을 적용하면 Firewall Manager가 새 계정을 귀하의 설정값에 대비하여 자동으로 평가합니다. 예컨대, 귀하가 특정 계정만 포함하는 경우, Firewall Manager는 해당 정책을 새 계정에 적용

하지 않습니다. 또 다른 예로 OU를 포함하는 경우, OU나 하위 OU에 계정을 추가하면 Firewall Manager는 새 계정에 정책을 자동으로 적용합니다.

15. Network Firewall 정책의 리소스 타입은 VPC입니다.
16. 리소스의 경우 태그를 지정하여 지정한 태그가 있는 리소스를 포함하거나 제외함으로써 정책 범위를 좁힐 수 있습니다. 포함 또는 제외를 사용할 수 있으며 둘 다 사용할 수는 없습니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.

    태그를 두 개 이상 입력하는 경우, 포함하거나 제외할 모든 태그가 리소스에 있어야 합니다.

    리소스 태그는 null이 아닌 값만 가질 수 있습니다. 태그 값을 생략하면 Firewall Manager는 빈 문자열 값 “" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.
17. 크로스 계정 액세스 권한 부여에서 AWS CloudFormation 템플릿 다운로드를 선택합니다. 그러면 AWS CloudFormation 스택을 생성하는 데 사용할 수 있는 AWS CloudFormation 템플릿이 다운로드됩니다. 이 스택은 Firewall Manager에 Fortigate CNF 리소스를 관리할 수 있는 계정 간 권한을 부여하는 AWS Identity and Access Management 역할을 생성합니다. 스택에 대한 자세한 설명은 AWS CloudFormation 사용자 가이드의 스택 작업을 참조하세요. 스택을 생성하려면 Fortigate CNF 포털의 계정 ID가 필요합니다.
18. 다음을 선택합니다.
19. 정책 태그의 경우 Firewall Manager 정책 리소스에 추가할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
20. 다음을 선택합니다.
21. 새 정책 설정을 검토하고 조정이 필요한 페이지로 돌아가십시오.

    정책이 마음에 들면 정책 생성를 선택합니다. AWS Firewall Manager 정책 창에 귀하의 정책이 등재되어야 합니다. 계정 제목 아래에 보류 중이라고 표시되고 자동 수정 설정의 상태가 표시될 수 있습니다. 정책을 만들려면 몇 분 정도 걸릴 수 있습니다. 보류 중 상태가 계정 수로 바뀐 후에는 정책 이름을 선택하여 계정과 리소스의 규정 준수 상태를 탐색할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

AWS Firewall Manager 정책 삭제

다음 단계를 수행하여 Firewall Manager 정책을 삭제할 수 있습니다.

정책을 삭제하려면(콘솔)

1. 탐색 창에서 보안 정책을 선택합니다.

2. 삭제할 정책 옆에 있는 옵션을 선택합니다.
3. 삭제를 선택합니다.

> **Note**
>
> Firewall Manager 공통 보안 그룹 정책을 삭제할 때 정책의 복제본 보안 그룹을 제거하려면 정책에서 생성한 리소스를 정리하는 옵션을 선택합니다. 그렇지 않으면 기본 정책이 삭제된 후 복제본이 그대로 유지되며 각 Amazon VPC 인스턴스에서 수동으로 관리해야 합니다.

> **Important**
>
> Firewall Manager Shield Advanced 정책을 삭제하면 정책이 삭제되지만 계정은 Shield Advanced를 구독하는 상태로 유지됩니다.

AWS Firewall Manager 정책 범위

정책 범위는 정책이 적용되는 위치를 정의합니다. 중앙 제어 정책을 조직 내 모든 계정 및 리소스 또는 일부 계정 및 리소스에 적용할 수 있습니다. AWS Organizations정책 범위 설정 방법에 대한 지침은 AWS Firewall Manager 정책 생성을 참조하세요.

정책 범위 옵션은 다음과 같습니다. AWS Firewall Manager

조직에 새 계정이나 리소스를 추가하면 Firewall Manager가 각 정책의 설정을 기준으로 이를 자동으로 평가하고 이러한 설정을 기반으로 정책을 적용합니다. 예를 들어 지정된 목록에 있는 계정 번호를 제외한 모든 계정에 정책을 적용하도록 선택할 수 있으며 목록에 모든 태그가 있는 리소스에만 정책을 적용하도록 선택할 수도 있습니다.

AWS 계정 범위 내

정책의 AWS 계정 영향을 받는 항목을 정의하기 위해 제공하는 설정에 따라 정책을 적용할 AWS 조직의 계정이 결정됩니다. 다음 중 한 가지 방법으로 정책을 적용하도록 선택할 수 있습니다.

- 조직의 모든 계정에 적용
- 포함된 계정 번호 및 AWS Organizations 조직 단위(OU)의 특정 목록만
- 제외된 계정 번호 및 AWS Organizations 조직 단위(OU)의 특정 목록을 제외한 모든 항목

에 대한 AWS Organizations자세한 내용은 AWS Organizations 사용 설명서를 참조하십시오.

범위 내 리소스

범위 내 계정 설정과 마찬가지로 리소스에 대해 제공하는 설정에 따라 정책을 적용할 범위 내 리소스 유형이 결정됩니다. 다음 중 하나를 선택할 수 있습니다.

- 모든 리소스
- 지정한 모든 태그가 있는 리소스
- 지정한 모든 태그가 있는 리소스를 제외한 모든 리소스

null이 아닌 값을 가진 리소스 태그만 지정할 수 있습니다. 값을 입력하지 않으면 Firewall Manager는 빈 문자열 값 "" 과 함께 태그를 저장합니다. 리소스 태그는 키와 값이 같은 태그와만 일치합니다.

리소스 태그 지정에 대한 자세한 내용은 태그 편집기 작업을 참조하세요.

의 정책 범위 관리 AWS Firewall Manager

정책이 수립되면 Firewall Manager는 정책을 지속적으로 관리하고 정책 범위에 따라 정책이 추가되는 대로 새 AWS 계정 리소스와 리소스에 적용합니다.

방화벽 관리자가 리소스를 AWS 계정 관리하는 방법

어떤 이유로든 계정 또는 리소스가 범위를 벗어나는 경우 정책 범위를 벗어나는 리소스에서 자동으로 보호 제거 확인란을 선택하지 않는 한 보호 기능이 자동으로 제거되거나 Firewall Manager에서 관리하는 리소스가 삭제되지 AWS Firewall Manager 않습니다.

> **Note**
>
> 정책 범위를 벗어나는 리소스에서 보호를 자동으로 제거하는 옵션은 또는 클래식 정책에는 사용할 수 없습니다. AWS Shield Advanced AWS WAF

이 확인란을 선택하면 계정이 정책 범위를 벗어날 때 Firewall Manager가 계정에 대해 관리하는 리소스를 자동으로 AWS Firewall Manager 정리하도록 지시합니다. 예를 들어 Firewall Manager는 고객 리소스가 정책 범위를 벗어날 때 보호된 고객 리소스에서 Firewall Manager 관리형 웹 ACL의 연결을 해제합니다.

고객 리소스가 정책 범위를 벗어나는 경우 보호에서 제거해야 하는 리소스를 결정하기 위해 Firewall Manager는 다음 지침을 따릅니다.

- 기본 동작:
  - 연결된 AWS Config 관리형 규칙이 삭제됩니다. 이 동작은 확인란과 무관합니다.
  - 리소스가 전혀 포함되지 않은 모든 관련 AWS WAF 웹 액세스 제어 목록 (웹 ACL) 은 삭제됩니다. 이 동작은 확인란과 무관합니다.
  - 범위를 벗어나는 보호된 리소스는 모두 연결되고 보호된 상태로 유지됩니다. 예를 들어 웹 ACL과 연결된 API Gateway의 Application Load Balancer 또는 API는 웹 ACL과 연결된 상태로 유지되며 보호 기능은 그대로 유지됩니다.
- 정책 범위를 벗어나는 리소스에서 보호 자동 제거 확인란을 선택한 경우:
  - 연결된 AWS Config 관리형 규칙이 삭제됩니다. 이 동작은 확인란과 무관합니다.
  - 리소스가 전혀 포함되지 않은 모든 관련 AWS WAF 웹 액세스 제어 목록 (웹 ACL) 은 삭제됩니다. 이 동작은 확인란과 무관합니다.
  - 범위를 벗어나는 보호된 리소스는 정책 범위를 벗어나면 자동으로 연결이 끊기고 Firewall Manager 보호에서 제거됩니다. 예를 들어 보안 그룹 정책의 경우 Elastic Inference 가속기 또는 Amazon EC2 인스턴스가 정책 범위를 벗어나면 복제된 보안 그룹과의 연결이 자동으로 끊깁니다. 복제된 보안 그룹과 해당 리소스는 보호에서 자동으로 제거됩니다.

관리형 목록

관리형 애플리케이션 및 프로토콜 목록을 사용하면 AWS Firewall Manager 콘텐츠 감사 보안 그룹 정책의 구성 및 관리를 간소화할 수 있습니다. 관리 목록을 사용하여 정책에서 허용하거나 허용하지 않는 프로토콜과 응용 프로그램을 정의합니다. 콘텐츠 감사 보안 그룹 정책에 대한 자세한 내용은 콘텐츠 감사 보안 그룹 정책을 참조하세요.

콘텐츠 감사 보안 그룹 정책에는 다음과 같은 유형의 관리 목록을 사용할 수 있습니다.

- Firewall Manager 애플리케이션 목록 및 프로토콜 목록 - Firewall Manager는 이러한 목록을 관리합니다.
  - 애플리케이션 목록에는 일반 대중에게 허용되거나 거부되어야 하는 일반적으로 사용되는 애플리케이션을 설명하는 `FMS-Default-Public-Access-Apps-Allowed` 및 `FMS-Default-Public-Access-Apps-Denied`가 포함됩니다.
  - 프로토콜 목록에는 일반 대중에게 허용되어야 하는 일반적으로 사용되는 프로토콜 목록 `FMS-Default-Protocols-Allowed`이 포함됩니다. Firewall Manager에서 관리하는 모든 목록을 사용할 수 있지만 편집하거나 삭제할 수는 없습니다.

- 사용자 지정 애플리케이션 목록 및 프로토콜 목록 — 사용자는 이러한 목록을 관리합니다. 필요한 설정을 사용하여 두 유형 중 하나의 목록을 만들 수 있습니다. 사용자 지정 관리 목록을 완전히 제어할 수 있으며 필요에 따라 생성, 편집, 삭제할 수 있습니다.

> **Note**
>
> 현재 Firewall Manager는 사용자 지정 관리 목록을 삭제할 때 해당 목록에 대한 참조를 확인하지 않습니다. 즉, 사용자 지정 관리 애플리케이션 목록 또는 프로토콜 목록을 활성 정책에서 사용 중인 경우에도 삭제할 수 있습니다. 이로 인해 정책이 작동하지 않을 수 있습니다. 애플리케이션 목록 또는 프로토콜 목록은 활성 정책에서 참조하지 않는지 확인한 후에만 삭제하십시오.

관리 목록은 AWS 리소스입니다. 사용자 지정 관리 목록에 태그를 지정할 수 있습니다. Firewall Manager 관리 목록에는 태그를 지정할 수 없습니다.

관리형 목록 버전 관리

사용자 지정 관리 목록에는 버전이 없습니다. 사용자 지정 목록을 수정하면 해당 목록을 참조하는 정책이 업데이트된 목록을 자동으로 사용합니다.

Firewall Manager 관리 목록에는 버전이 지정되어 있습니다. Firewall Manager 서비스 팀은 목록에 최상의 보안 사례를 적용하기 위해 필요에 따라 새 버전을 게시합니다.

정책에서 Firewall Manager 관리 목록을 사용할 때는 다음과 같이 버전 관리 전략을 선택합니다.

- 사용 가능한 최신 버전 - 목록에 명시적인 버전 설정을 지정하지 않으면 정책이 자동으로 최신 버전을 사용합니다. 콘솔을 통해 사용할 수 있는 유일한 옵션입니다.
- 명시적 버전 - 목록에 버전을 지정하면 정책에서 해당 버전을 사용합니다. 정책은 버전 설정을 수정할 때까지 지정한 버전에 고정된 상태로 유지됩니다. 버전을 지정하려면 콘솔 외부(예: CLI 또는 SDK 중 하나를 통해)에서 정책을 정의해야 합니다.

목록의 버전 설정 선택에 대한 자세한 내용은 콘텐츠 감사 보안 그룹 정책에 관리 목록 사용을 참조하세요.

콘텐츠 감사 보안 그룹 정책에 관리 목록 사용

콘텐츠 감사 보안 그룹 정책을 생성할 때 관리형 감사 정책 규칙을 사용하도록 선택할 수 있습니다. 이 옵션의 일부 설정에는 관리되는 애플리케이션 목록 또는 프로토콜 목록이 필요합니다. 이러한 설정의

예로는 보안 그룹 규칙에서 허용되는 프로토콜과 애플리케이션이 인터넷에 액세스할 수 있는 프로토콜이 있습니다.

관리 목록을 사용하는 각 정책 설정에는 다음과 같은 제한이 적용됩니다.

- 모든 설정에 대해 최대 1개의 Firewall Manager 관리 목록을 지정할 수 있습니다. 기본적으로 사용자 지정 목록을 최대 한 개만 지정할 수 있습니다. 사용자 지정 목록 한도는 소프트 할당량이므로 상향 조정을 요청할 수 있습니다. 자세한 내용은 AWS Firewall Manager 할당량을 참조하세요.
- 콘솔에서 Firewall Manager 관리 목록을 선택하면 버전을 지정할 수 없습니다. 정책은 항상 최신 버전의 목록을 사용합니다. 버전을 지정하려면 콘솔 외부(예: CLI 또는 SDK 중 하나를 통해)에서 정책을 정의해야 합니다. Firewall Manager 관리 목록의 버전 관리에 대한 자세한 내용은 관리형 목록 버전 관리을 참조하세요.

콘솔을 통해 콘텐츠 감사 보안 그룹 정책을 생성하는 방법에 대한 자세한 내용은 콘텐츠 감사 보안 그룹 정책 생성을 참조하세요.

사용자 지정 관리 애플리케이션 목록 생성

새 사용자 지정 관리 애플리케이션 목록을 생성하려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 애플리케이션 목록을 선택합니다.
3. 애플리케이션 목록 페이지에서 애플리케이션 목록 생성을 선택합니다.
4. 애플리케이션 목록 생성 페이지에서 목록에 이름을 지정합니다. 접두사 `fms-`은 Firewall Manager 용이므로 사용하지 마십시오.
5. 프로토콜 및 포트 번호를 제공하거나 유형 드롭다운에서 애플리케이션을 선택하여 애플리케이션을 지정합니다. 애플리케이션 사양에 이름을 지정하십시오.
6. 필요에 따라 다른 항목 추가를 선택하고 목록을 작성할 때까지 애플리케이션 정보를 입력합니다.
7. (선택 사항) 목록에 태그를 적용합니다.

8. 저장을 선택하여 목록을 저장하고 애플리케이션 목록 페이지로 돌아갑니다.

사용자 지정 관리 프로토콜 목록 생성

새 사용자 지정 관리 프로토콜 목록을 생성하려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 프로토콜 목록을 선택합니다.
3. 프로토콜 목록 페이지에서 프로토콜 목록 생성을 선택합니다.
4. 프로토콜 목록 생성 페이지에서 목록에 이름을 지정합니다. 접두사 `fms-`은 Firewall Manager용이므로 사용하지 마십시오.
5. 프로토콜을 지정합니다.
6. 필요에 따라 다른 항목 추가를 선택하고 목록을 완료할 때까지 프로토콜 정보를 입력합니다.
7. (선택 사항) 목록에 태그를 적용합니다.
8. 저장을 선택하여 목록을 저장하고 프로토콜 목록 페이지로 돌아갑니다.

관리 목록 보기

애플리케이션 목록 또는 프로토콜 목록을 보려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 애플리케이션 목록 또는 프로토콜 목록을 선택합니다.

   페이지에는 선택한 유형 중에서 사용할 수 있는 모든 목록이 표시됩니다. Firewall Manager에서 관리하는 목록의 ManagedList열에는 Y가 있습니다.

3. 목록의 세부 정보를 보려면 해당 이름을 선택합니다. 세부 정보 페이지에는 목록의 콘텐츠와 태그가 표시됩니다.

   Firewall Manager 관리 목록의 경우 버전 드롭다운을 선택하여 사용 가능한 버전을 확인할 수도 있습니다.

사용자 지정 관리 목록 삭제

사용자 지정 관리 목록을 삭제할 수 있습니다. Firewall Manager에서 관리하는 목록을 편집하거나 삭제할 수는 없습니다.

> **Note**
>
> 현재 Firewall Manager는 사용자 지정 관리 목록을 삭제할 때 해당 목록에 대한 참조를 확인하지 않습니다. 즉, 사용자 지정 관리 애플리케이션 목록 또는 프로토콜 목록을 활성 정책에서 사용 중인 경우에도 삭제할 수 있습니다. 이로 인해 정책이 작동하지 않을 수 있습니다. 애플리케이션 목록 또는 프로토콜 목록을 활성 정책에서 참조하지 않는지 확인한 후에만 삭제하십시오.

사용자 지정 관리 애플리케이션 또는 프로토콜 목록을 삭제하려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 다음을 수행하여 삭제하려는 목록이 감사 보안 그룹 정책에 사용되고 있지 않은지 확인하십시오.

   a. 탐색 창에서 보안 정책을 선택합니다.

b. AWS Firewall Manager 정책 페이지에서 감사 보안 그룹을 선택 및 편집하고, 삭제하려는 사용자 지정 목록에 대한 참조를 모두 제거합니다.

   감사 보안 그룹 정책에서 사용 중인 사용자 지정 관리 목록을 삭제하는 경우 해당 목록을 사용하는 정책이 작동하지 않을 수 있습니다.

3. 탐색 창에서 삭제하려는 삭제하려는 목록 유형에 따라 애플리케이션 목록 또는 프로토콜 목록을 선택합니다.
4. 목록 페이지에서 삭제할 사용자 지정 목록을 선택하고 삭제를 선택합니다.

AWS WAF 정책

Firewall Manager AWS WAF 정책에서는 리소스 전체에서 사용할 AWS WAF 규칙 그룹을 지정합니다. 정책을 적용하면 Firewall Manager는 정책에서 웹 ACL 관리를 구성하는 방법에 따라 정책 범위 내의 계정에 웹 ACL을 생성합니다. 정책으로 생성된 웹 ACL에서 개별 계정 관리자는 Firewall Manager를 통해 정의한 규칙 그룹 외에도 규칙 및 규칙 그룹을 추가할 수 있습니다.

Firewall Manager가 웹 ACL을 관리하는 방법

Firewall Manager는 정책에서 연결되지 않은 웹 ACL 관리 설정을 구성하거나 API의 SecurityServicePolicyData데이터 유형 **`optimizeUnassociatedWebACL`** 설정을 구성하는 방법에 따라 웹 ACL을 생성합니다.

연결되지 않은 웹 ACL의 관리를 활성화하면 Firewall Manager는 하나 이상의 리소스에서 웹 ACL을 사용할 경우에만 정책 범위 내의 계정에 웹 ACL을 생성합니다. 계정이 정책 범위에 포함되는 경우, 하나 이상의 리소스가 웹 ACL을 사용할 경우 Firewall Manager는 계정에 웹 ACL을 자동으로 생성합니다. 연결되지 않은 웹 ACL의 관리를 활성화하면 Firewall Manager는 계정에서 연결되지 않은 웹 ACL을 한 번 정리합니다. 정리 중에 Firewall Manager는 생성 후 수정한 웹 ACL을 건너뛰습니다(예: 웹 ACL에 규칙 그룹을 추가하거나 설정을 수정한 경우). 정리 프로세스에는 몇 시간이 걸릴 수 있습니다. Firewall Manager가 웹 ACL을 생성한 후 리소스가 정책 범위를 벗어나는 경우 Firewall Manager는 웹 ACL에서 리소스를 분리하지만 연결되지 않은 웹 ACL을 정리하지는 않습니다. Firewall Manager는 정책에서 연결되지 않은 웹 ACL의 관리를 처음 활성화한 경우에만 연결되지 않은 웹 ACL을 정리합니다.

이 옵션을 활성화하지 않는 경우 Firewall Manager는 연결되지 않은 웹 ACL을 관리하지 않으며 Firewall Manager는 정책 범위 내에 있는 각 계정에 웹 ACL을 자동으로 생성합니다.

샘플링 및 지표 CloudWatch

AWS Firewall Manager AWS WAF 정책용으로 생성한 웹 ACL 및 규칙 그룹에 대한 샘플링 및 Amazon CloudWatch 메트릭을 활성화합니다.

웹 ACL 이름 지정 구조

Firewall Manager는 정책에 대한 웹 ACL을 생성할 때 웹 ACL `FMManagedWebACLV2-`*`policy name`*`-`*`timestamp`*의 이름을 지정합니다. 타임스탬프는 UTC 밀리초 단위입니다. 예를 들어 `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`입니다.

> **Note**
>
> 고급 자동 애플리케이션 계층 DDoS 완화로 구성된 리소스가 정책 범위에 포함되는 경우 Firewall Manager는 AWS WAF 정책으로 생성된 웹 ACL을 리소스에 연결할 수 없습니다. AWS WAF

정책의 규칙 그룹 AWS WAF

Firewall Manager AWS WAF 정책으로 관리되는 웹 ACL에는 세 가지 규칙 세트가 포함되어 있습니다. 이러한 집합은 웹 ACL의 규칙 및 규칙 그룹에 대해 더 높은 수준의 우선 순위를 제공합니다.

- Firewall Manager AWS WAF 정책에서 사용자가 정의한 첫 번째 규칙 그룹 AWS WAF 이러한 규칙 그룹을 먼저 평가합니다.
- 웹 ACL에서 계정 관리자가 정의한 규칙 및 규칙 그룹입니다. AWS WAF 는 계정 관리형 규칙 또는 규칙 그룹을 다음에 평가합니다.
- Firewall Manager AWS WAF 정책에서 사용자가 정의한 마지막 규칙 그룹 AWS WAF 이러한 규칙 그룹을 마지막으로 평가합니다.

각 규칙 세트 내에서, 세트 내의 우선 순위 설정에 따라 평소와 같이 규칙과 규칙 그룹을 AWS WAF 평가합니다.

정책의 첫 번째 및 마지막 규칙 그룹 집합에서는 규칙 그룹만 추가할 수 있습니다. 관리형 규칙 및 AWS Marketplace 판매자가 대신 생성하고 유지 관리하는 AWS 관리형 규칙 그룹을 사용할 수 있습니다. 사용자 고유의 규칙 그룹을 관리하고 사용할 수도 있습니다. 이러한 옵션에 대한 자세한 내용은 AWS WAF 규칙 그룹을 참조하세요.

고유의 규칙 그룹을 사용하려는 경우 Firewall Manager AWS WAF 정책을 생성하기 전에 해당 규칙 그룹을 생성합니다. 자세한 지침은 자체 규칙 그룹 관리을 참조하세요. 개별 사용자 지정 규칙을 사용하려면 고유의 규칙 그룹을 정의하고, 해당 규칙 그룹 내에서 규칙을 정의한 다음, 정책에서 규칙 그룹을 사용해야 합니다.

Firewall Manager를 통해 관리하는 첫 번째 AWS WAF 규칙 그룹과 마지막 규칙 그룹의 이름은 각각 `PREFMManaged-` 또는 `POSTFMManaged-` 로 시작하고 그 뒤에 Firewall Manager 정책 이름과 규칙 그룹 생성 타임스탬프 (UTC 밀리초) 가 뒤따릅니다. 예를 들어 `PREFMManaged-MyWAFPolicyName-1621880555123`입니다.

웹 요청을 AWS WAF 평가하는 방법에 대한 자세한 내용은 을 참조하십시오. 웹 ACL 규칙 및 규칙 그룹 평가

Firewall Manager AWS WAF 정책을 만드는 절차는 을 참조하십시오에 대한 AWS Firewall Manager 정책 생성 AWS WAF.

Firewall Manager는 AWS WAF 정책에 정의한 규칙 그룹에 대한 샘플링 및 Amazon CloudWatch 지표를 활성화합니다.

개별 계정 소유자는 정책의 관리형 웹 ACL에 추가하는 모든 규칙 또는 규칙 그룹의 지표와 샘플링 구성을 완벽하게 제어할 수 있습니다.

AWS WAF 정책에 대한 로깅 구성

AWS WAF 정책에 대한 중앙 집중식 로깅을 활성화하여 조직 내 웹 ACL에서 분석한 트래픽에 대한 세부 정보를 얻을 수 있습니다. 로그의 정보에는 AWS 리소스로부터 요청을 AWS WAF 받은 시간, 요청에 대한 세부 정보, 범위 내 모든 계정에서 각 요청이 일치하는 규칙에 대한 조치 등이 포함됩니다. Amazon Data Firehose 데이터 스트림 또는 Amazon Simple Storage Service (S3) 버킷으로 로그를 보낼 수 있습니다. AWS WAF 로깅에 대한 자세한 내용은 AWS WAF 개발자 안내서를 참조하십시오AWS WAF 웹 ACL 트래픽 로깅.

> **Note**
>
> AWS Firewall Manager Classic에서는 이 옵션을 AWS WAFV2지원하지만 AWS WAF Classic에서는 지원하지 않습니다.

주제

- 로깅 대상
- 로깅 활성화
- 로깅 비활성화

로깅 대상

이 섹션에서는 AWS WAF 정책 로그를 전송하기 위해 선택할 수 있는 로깅 대상에 대해 설명합니다. 각 섹션에서는 대상 유형에 대한 로깅을 구성하기 위한 지침과 대상 유형과 관련된 모든 동작에 대한 정보를 제공합니다. 로깅 대상을 구성한 후 Firewall Manager AWS WAF 정책에 해당 사양을 제공하여 로깅을 시작할 수 있습니다.

Firewall Manager는 로깅 구성을 생성한 후 로그 실패를 확인할 수 없습니다. 로그 전달이 의도한 대로 작동하는지 확인하는 것은 사용자의 책임입니다.

> **Note**
>
> Firewall Manager는 조직 구성원 계정의 기존 로깅 구성을 수정하지 않습니다.

주제

- Amazon Data Firehose 데이터 스트림
- Amazon Simple Storage Service 버킷

Amazon Data Firehose 데이터 스트림

이 주제에서는 웹 ACL 트래픽 로그를 Amazon Data Firehose 데이터 스트림으로 전송하는 데 필요한 정보를 제공합니다.

Amazon Data Firehose 로깅을 활성화하면 Firewall Manager는 정책의 웹 ACL에서 사용자가 스토리지 대상을 구성한 Amazon Data Firehose로 로그를 전송합니다. 로깅을 활성화하면 Kinesis Data Firehose의 HTTPS 엔드포인트를 통해 구성된 각 웹 ACL에 대한 로그를 구성된 스토리지 대상으로 AWS WAF 전달합니다. 전송 스트림을 사용하기 전에 테스트하여 조직의 로그를 수용할 만큼 처리량이 충분한지 확인하십시오. Amazon Kinesis Data Firehose를 생성하고 저장된 로그를 검토하는 방법에 대한 자세한 내용은 Amazon Data Firehose란 무엇입니까? 를 참조하십시오.

Kinesis로 로깅을 활성화하려면 다음 권한이 있어야 합니다.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

AWS WAF 정책에 Amazon Data Firehose 로깅 대상을 구성하면 방화벽 관리자는 다음과 같이 방화벽 관리자 계정에 정책에 대한 웹 ACL을 생성합니다.

- Firewall Manager는 계정이 정책 범위 내에 있는지 여부와 상관없이 Firewall Manager 관리자 계정에 웹 ACL을 생성합니다.
- 웹 ACL에는 로그 이름 `FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`*과 함께 로깅이 활성화되어 있습니다. 여기서 타임스탬프는 로그가 웹 ACL에 대해 활성화된 UTC 시간(밀리초)입니다. 예를 들어 `FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`입니다. 웹 ACL에는 규칙 그룹과 관련 리소스가 없습니다.
- 가격 가이드라인에 따라 웹 ACL에 대한 요금이 부과됩니다. AWS WAF 자세한 내용은 AWS WAF 요금을 참조하세요.
- Firewall Manager는 정책을 삭제할 때 웹 ACL을 삭제합니다.

서비스 연결 역할 및 `iam:CreateServiceLinkedRole` 권한에 대한 자세한 내용은 서비스 연결 역할 사용 AWS WAF 섹션을 참조하세요.

전송 스트림 생성에 대한 자세한 내용은 Amazon Data Firehose 전송 스트림 생성을 참조하십시오.

Amazon Simple Storage Service 버킷

이 주제는 Amazon S3 버킷으로 웹 ACL 트래픽 로그를 전송하기 위한 정보를 제공합니다.

로깅 대상으로 선택한 버킷은 Firewall Manager 관리자 계정이 소유해야 합니다. 로깅을 위한 Amazon S3 버킷 생성 요구 사항 및 버킷 이름 지정 요구 사항에 대한 자세한 내용은 AWS WAF 개발자 안내서의 Amazon Simple Storage Service를 참조하세요.

최종 일관성

Amazon S3 로깅 대상으로 구성된 AWS WAF 정책을 변경하면 Firewall Manager가 버킷 정책을 업데이트하여 로깅에 필요한 권한을 추가합니다. 이 경우 Firewall Manager는 Amazon 심플 스토리지 서비스가 따르는 last-writer-wins 시맨틱 및 데이터 일관성 모델을 따릅니다. Firewall Manager 콘솔에서 또는 PutPolicyAPI를 통해 Amazon S3 대상에 여러 정책을 동시에 업데이트하는 경우 일부 권한이 저장되지 않을 수 있습니다. Amazon S3 데이터 일관성 모델에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 데이터 정합성 모델을 참조하세요.

Amazon S3 버킷에 로그를 게시하는 데 필요한 권한

AWS WAF 정책에서 Amazon S3 버킷에 대한 웹 ACL 트래픽 로깅을 구성하려면 다음 권한 설정이 필요합니다. Firewall Manager는 Amazon S3를 로깅 대상으로 구성하여 서비스에 로그를 버킷에 게시할 권한을 부여하는 경우 Amazon S3 버킷에 이러한 권한을 자동으로 연결합니다. 로깅 및 Firewall

Manager 리소스에 대한 보다 세분화된 액세스를 관리하려는 경우 이러한 권한을 직접 설정할 수 있습니다. 권한 관리에 관한 자세한 내용은 IAM 사용 설명서의 AWS 리소스에 대한 액세스 관리를 참조하세요. AWS WAF 관리형 정책에 대한 자세한 내용은 을 참조하십시오AWS 에 대한 관리형 정책 AWS WAF.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryForFirewallManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-DOC-EXAMPLE-BUCKET"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/
AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

서비스 간에 혼동되는 대리인 문제를 방지하려면 버킷 정책에서 aws:SourceArn 및 aws:SourceAccount 글로벌 조건 컨텍스트 키를 추가합니다. 이러한 키를 추가하려면 로깅 대상을 구성할 때 Firewall Manager가 생성하는 정책을 수정하거나, 세부적인 제어를 원하는 경우 자체 정책을 만들 수 있습니다. 로깅 대상 정책에 이러한 조건을 추가하는 경우 Firewall Manager는 혼동되는 보조 보호를 검증하거나 모니터링하지 않습니다. 혼동된 대리자 문제에 관한 일반적인 내용은 IAM 사용 설명서의 혼동된 대리자 문제를 참조하세요.

sourceAccount 추가 sourceArn 속성을 추가하면 버킷 정책 크기가 커집니다. sourceAccount 추가 sourceArn 속성의 긴 목록을 추가하는 경우 Amazon S3 버킷 정책 크기 할당량을 초과하지 않도록 주의하십시오.

다음 예는 버킷 정책에서 aws:SourceArn 및 aws:SourceAccount 글로벌 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다. 조직 구성원의 계정 *member-account-id*ID로 바꾸십시오.

```
{
   "Version":"2012-10-17",
   "Id":"AWSLogDeliveryForFirewallManager",
   "Statement":[
      {
         "Sid":"AWSLogDeliveryAclCheckFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:GetBucketAcl",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":[
                  "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id:*",
                  "arn:aws:logs:*:member-account-id:*"
               ]
            }
         }
      },
      {
         "Sid":"AWSLogDeliveryWriteFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
         },
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/AWSLogs/*",
```

```
         "Condition":{
            "StringEquals":{
               "s3:x-amz-acl":"bucket-owner-full-control",
               "aws:SourceAccount":[
                     "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id-1:*",
                  "arn:aws:logs:*:member-account-id-2:*"
               ]
            }
         }
      }
   ]
}
```

Amazon S3 버킷의 서버 측 암호화

Amazon S3 서버 측 암호화를 활성화하거나 S3 버킷에서 AWS Key Management Service 고객 관리 키를 사용할 수 있습니다. Amazon S3 버킷의 기본 Amazon S3 암호화를 AWS WAF 로그에 사용하기로 선택한 경우 특별한 조치를 취할 필요가 없습니다. 하지만 고객 제공 암호화 키를 사용하여 저장된 Amazon S3 데이터를 암호화하기로 선택한 경우 키 정책에 다음 권한 설명을 추가해야 합니다. AWS Key Management Service

```
{
            "Sid": "Allow Logs Delivery to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": "*"
}
```

Amazon S3와 고객 제공 암호화 키 사용에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 고객 제공 키(SSE-C)로 서버 측 암호화 사용을 참조하세요.

로깅 활성화

다음 절차는 Firewall Manager 콘솔에서 AWS WAF 정책에 대한 로깅을 활성화하는 방법을 설명합니다.

AWS WAF 정책에 대한 로깅을 활성화하려면

1. 로깅을 활성화하려면 먼저 로깅 대상 리소스를 다음과 같이 구성해야 합니다.

   - Amazon Kinesis 데이터 스트림 - Firewall Manager 관리자 계정을 사용하여 Amazon 데이터 파이어호스를 생성하십시오. 접두사 `aws-waf-logs-`로 시작하는 이름을 사용하십시오. 예를 들어 `aws-waf-logs-firewall-manager-central`입니다. 작업하려는 리전에서 PUT 소스를 사용하여 Data Firehose를 생성합니다. CloudFrontAmazon의 로그를 캡처하는 경우 미국 동부 (버지니아 북부) 에서 파이어호스를 생성하십시오. 전송 스트림을 사용하기 전에 테스트하여 조직의 로그를 수용할 만큼 처리량이 충분한지 확인하십시오. 자세한 내용은 Amazon Data Firehose 전송 스트림 생성을 참조하세요.
   - Amazon Simple Storage Service 버킷 - AWS WAF 개발자 안내서의 Amazon Simple Storage Service 주제에 있는 지침에 따라 Amazon S3 버킷을 생성합니다. 또한 Amazon S3 버킷에 로그를 게시하는 데 필요한 권한 에 나열된 권한으로 Amazon S3 버킷을 구성해야 합니다.

2. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

3. 탐색 창에서 보안 정책을 선택합니다.
4. 로깅을 활성화하려는 AWS WAF 정책을 선택합니다. AWS WAF 로깅에 대한 자세한 내용은 AWS WAF 웹 ACL 트래픽 로깅을 참조하세요.
5. 정책 규칙 섹션의 정책 세부 정보 탭에서 편집을 선택합니다.
6. 로깅 구성의 경우 로깅 활성화를 선택하여 로깅을 활성화합니다. 로깅은 웹 ACL에서 분석한 트래픽에 대한 자세한 정보를 기록합니다. 로깅 대상 유형을 선택한 다음 구성한 로깅 대상을 선택합니

다. 이름이 `aws-waf-logs-`로 시작하는 로깅 대상을 선택해야 합니다. AWS WAF 로깅 대상 구성에 대한 자세한 내용은 을 참조하십시오AWS WAF 정책에 대한 로깅 구성.

7. (선택 사항) 로그에 포함된 특정 필드와 그 값이 필요하지 않은 경우 해당 필드를 삭제합니다. 삭제할 필드를 선택한 후 추가를 선택합니다. 필요에 따라 이 작업을 반복하여 추가 필드를 삭제합니다. 삭제된 필드는 로그에서 `REDACTED`(으)로 표시됩니다. 예를 들어 URI 필드를 삭제한 경우 로그에서 URI 필드가 `REDACTED`로 나타납니다.
8. (선택 사항) 모든 요청을 로그로 전송하지 않으려면 필터링 기준과 동작을 추가합니다. 필터 로그에서 적용하려는 각 필터에 대해 필터 추가를 선택한 다음 기준과 일치하는 요청을 유지할지 아니면 삭제할지 여부를 지정합니다. 필터 추가를 완료할 때 필요 시 기본 로깅 동작을 수정합니다. 자세한 내용은 AWS WAF 개발자 안내서의 웹 ACL 로깅 구성을 참조하세요.
9. 다음을 선택합니다.
10. 설정을 검토한 다음 저장을 선택하여 변경 내용을 정책에 저장합니다.

로깅 비활성화

다음 절차는 Firewall Manager 콘솔에서 AWS WAF 정책에 대한 로깅을 비활성화하는 방법을 설명합니다.

AWS WAF 정책에 대한 로깅을 비활성화하려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 로깅을 비활성화하려는 AWS WAF 정책을 선택합니다.
4. 정책 규칙 섹션의 정책 세부 정보 탭에서 편집을 선택합니다.
5. 로깅 구성 상태에서 비활성화를 선택합니다.
6. 다음을 선택합니다.
7. 설정을 검토한 다음 저장을 선택하여 변경 내용을 정책에 저장합니다.

AWS Shield Advanced 정책

Firewall Manager AWS Shield 정책에서는 보호하려는 리소스를 선택합니다. 자동 수정이 활성화된 상태에서 정책을 적용하면 아직 웹 ACL과 연결되지 않은 범위 내 각 리소스에 대해 Firewall Manager가 빈 AWS WAF 웹 ACL을 연결합니다. AWS WAF 빈 웹 ACL은 Shield 모니터링 용도로 사용됩니다. 그런 다음 다른 웹 ACL을 리소스에 연결하면 Firewall Manager는 빈 웹 ACL 연결을 제거합니다.

> **Note**
>
> AWS WAF 정책 범위에 속하는 리소스가 자동 애플리케이션 레이어 DDoS 완화 기능으로 구성된 Shield Advanced 정책의 범위에 포함되는 경우 Firewall Manager는 정책에서 생성한 웹 ACL을 연결한 후에만 Shield Advanced 보호를 적용합니다. AWS WAF

Shield 정책에서 연결되지 않은 웹 ACL을 AWS Firewall Manager 관리하는 방법

정책의 연결되지 않은 웹 ACL 관리 설정 또는 API의 SecurityServicePolicyData데이터 유형 설정을 통해 Firewall Manager가 연결되지 않은 웹 ACL을 관리할지 여부를 구성할 수 있습니다. `optimizeUnassociatedWebACLs` 정책 내 연결되지 않은 웹 ACL의 관리를 활성화하면 Firewall Manager는 하나 이상의 리소스에서 웹 ACL을 사용할 경우에만 정책 범위 내의 계정에 웹 ACL을 생성합니다. 계정이 정책 범위에 포함되는 경우, 하나 이상의 리소스가 웹 ACL을 사용할 경우 Firewall Manager는 계정에 웹 ACL을 자동으로 생성합니다.

연결되지 않은 웹 ACL의 관리를 활성화하면 Firewall Manager는 계정에서 연결되지 않은 웹 ACL을 한 번 정리합니다. 정리 프로세스에는 몇 시간이 걸릴 수 있습니다. Firewall Manager가 웹 ACL을 생성한 후 리소스가 정책 범위를 벗어나는 경우 Firewall Manager는 웹 ACL에서 리소스를 연결하지 않습니다. Firewall Manager가 웹 ACL을 정리하도록 하려면 먼저 웹 ACL에서 리소스를 수동으로 분리한 다음 정책에서 연결되지 않은 웹 ACL 관리 옵션을 활성화해야 합니다.

이 옵션을 활성화하지 않는 경우 Firewall Manager는 연결되지 않은 웹 ACL을 관리하지 않으며 Firewall Manager는 정책 범위 내에 있는 각 계정에 웹 ACL을 자동으로 생성합니다.

Shield 정책의 범위 변경을 AWS Firewall Manager 관리하는 방법

정책 범위 설정 변경, 리소스의 태그 변경, 조직의 계정 제거 등 여러 가지 변경으로 인해 계정 및 리소스가 AWS Firewall Manager Shield Advanced 정책의 범위를 벗어날 수 있습니다. 정책 범위 설정에 대한 일반적인 내용은 AWS Firewall Manager 정책 범위을 참조하세요.

AWS Firewall Manager Shield Advanced 정책을 사용하면 계정 또는 리소스가 범위를 벗어나는 경우 Firewall Manager는 해당 계정 또는 리소스의 모니터링을 중지합니다.

조직에서 제거되어 계정이 범위를 벗어나는 경우에도 해당 계정은 Shield Advanced를 계속 구독합니다. 이 계정은 더 이상 통합 결제 패밀리의 일부가 아니기 때문에 계정에 비례 할당으로 계산된 Shield Advanced 가입 요금이 발생합니다. 반면, 범위를 벗어났지만 조직에 남아 있는 계정은 추가 요금이 발생하지 않습니다.

리소스가 범위를 벗어나도 해당 리소스는 Shield Advanced의 보호를 계속 받으며 Shield Advanced 데이터 전송 요금이 계속 발생합니다.

자동 애플리케이션 계층 DDoS 완화

Shield Advanced 정책을 Amazon CloudFront 배포판 또는 애플리케이션 로드 밸런서에 적용하는 경우 정책에서 Shield Advanced의 자동 애플리케이션 계층 DDoS 완화를 구성할 수 있습니다.

Shield Advanced 자동 완화에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화을 참조하세요.

Shield Advanced 자동 애플리케이션 계층 DDoS 완화에는 다음과 같은 요구 사항이 있습니다.

- 자동 애플리케이션 계층 DDoS 완화는 Amazon CloudFront 배포 및 애플리케이션 로드 밸런서에서만 작동합니다.

  아마존 CloudFront 배포에 Shield Advanced 정책을 적용하는 경우, 글로벌 지역에 대해 생성한 Shield Advanced 정책에 대해 이 옵션을 선택할 수 있습니다. Application Load Balancer에 보호를 적용하는 경우 Firewall Manager가 지원하는 모든 리전에 정책을 적용할 수 있습니다.
- 자동 애플리케이션 레이어 DDoS 완화는 최신 버전 (v2) 을 사용하여 생성된 웹 ACL에서만 작동합니다. AWS WAF

  따라서 AWS WAF 클래식 웹 ACL을 사용하는 정책이 있는 경우 정책을 새 정책으로 바꾸면 자동으로 최신 버전이 사용됩니다. 그렇지 않으면 Firewall Manager에서 기존 정책에 대한 새 버전의 웹 ACL을 만들고 이를 사용하도록 전환하도록 해야 합니다. AWS WAF이러한 옵션에 대한 자세한 내용은 AWS WAF 클래식 웹 ACL을 최신 버전의 웹 ACL로 교체을 참조하세요.

자동 완화 구성

Firewall Manager Shield Advanced 정책의 자동 애플리케이션 계층 DDoS 완화 옵션은 Shield Advanced 자동 완화 기능을 정책의 범위 내 계정 및 리소스에 적용합니다. 이 Shield Advanced 기능에 대한 자세한 내용은 Shield Advanced 자동 애플리케이션 계층 DDoS 완화을 참조하세요.

Firewall Manager가 정책 범위에 속하는 CloudFront 배포 또는 애플리케이션 로드 밸런서에 대한 자동 완화 기능을 활성화 또는 비활성화하도록 선택하거나, Shield Advanced 자동 완화 설정을 정책이 무시하도록 선택할 수 있습니다.

- 활성화 - 자동 완화를 활성화하도록 선택한 경우 Shield Advanced 규칙 완화 시 일치하는 웹 요청을 카운트할지 아니면 차단할지 여부도 지정합니다. Firewall Manager는 자동 완화 기능이 활성화되어 있지 않거나 정책에 지정한 것과 일치하지 않는 규칙 동작을 사용하는 경우 범위 내 리소스를 비준수로 표시합니다. 자동 수정을 위한 정책을 구성하면 Firewall Manager는 필요에 따라 비준수 리소스를 업데이트합니다.
- 비활성화 - 자동 완화를 사용하지 않도록 선택하면 Firewall Manager는 범위 내 리소스에 자동 완화 기능이 활성화되어 있는 경우 해당 리소스를 비준수로 표시합니다. 자동 수정을 위한 정책을 구성하면 Firewall Manager는 필요에 따라 비준수 리소스를 업데이트합니다.
- 무시 - 자동 완화를 무시하도록 선택하면 Firewall Manager는 정책에 대한 수정 작업을 수행할 때 Shield 정책의 자동 완화 설정을 고려하지 않습니다. 이 설정을 사용하면 Firewall Manager가 해당 설정을 덮어쓰지 않고도 Shield Advanced를 통해 자동 완화 기능을 제어할 수 있습니다. Shield Advanced를 통해 관리되는 Classic Load Balancer 또는 Elastic IP 리소스에는 이 설정이 적용되지 않습니다. Shield Advanced는 현재 해당 리소스에 대한 L7 자동 완화를 지원하지 않기 때문입니다.

AWS WAF 클래식 웹 ACL을 최신 버전의 웹 ACL로 교체

자동 애플리케이션 레이어 DDoS 완화는 최신 버전 AWS WAF (v2) 을 사용하여 생성된 웹 ACL에서만 작동합니다.

Shield Advanced 정책의 웹 ACL 버전을 확인하려면 Shield Advanced 정책에서 사용하는 버전 결정 AWS WAF을 참조하세요.

Shield Advanced 정책에서 현재 AWS WAF 클래식 웹 ACL을 사용하고 있는 경우 새 Shield Advanced 정책을 생성하여 현재 정책을 대체하거나 이 섹션에 설명된 옵션을 사용하여 이전 버전의 웹 ACL을 현재 Shield Advanced 정책 내에서 새 (v2) 웹 ACL로 교체할 수 있습니다. 새 정책은 항상 최신 버전의 웹 ACL을 생성합니다. AWS WAF전체 정책을 교체하는 경우 정책을 삭제할 때 Firewall Manager에서 이전 버전의 웹 ACL도 모두 삭제하도록 할 수 있습니다. 이 섹션의 나머지 부분에서는 기존 정책 내의 웹 ACL을 교체하기 위한 옵션에 대해 설명합니다.

Amazon CloudFront 리소스에 대한 기존 Shield Advanced 정책을 수정하면 Firewall Manager는 아직 v2 웹 ACL이 없는 범위 내 계정에서 정책에 대한 새로운 빈 AWS WAF (v2) 웹 ACL을 자동으로 생성할 수 있습니다. Firewall Manager가 새 웹 ACL을 생성할 때 정책에 이미 동일한 계정에 AWS WAF 클래식 웹 ACL이 있는 경우 Firewall Manager는 기존 웹 ACL과 동일한 기본 작업 설정으로 새 버전의 웹

ACL을 구성합니다. 기존 AWS WAF 클래식 웹 ACL이 없는 경우 Firewall Manager는 새 웹 Allow ACL에서 기본 동작을 로 설정합니다. Firewall Manager에서 새 웹 ACL을 생성한 후 AWS WAF 콘솔을 통해 필요에 따라 이를 사용자 지정할 수 있습니다.

다음 정책 구성 옵션 중 하나를 선택하면 Firewall Manager는 아직 해당 옵션이 없는 범위 내 계정에 대해 새 (v2) 웹 ACL을 생성합니다.

- 자동 애플리케이션 계층 DDoS 완화를 활성화 또는 비활성화하는 경우. 이 선택만 해도 Firewall Manager는 새 웹 ACL을 생성할 뿐 정책의 범위 내 리소스에 있는 기존 AWS WAF 클래식 웹 ACL 연결을 대체하지 않습니다.
- 자동 수정이라는 정책 조치를 선택하고 AWS WAF 클래식 웹 ACL을 AWS WAF (v2) 웹 ACL로 대체하는 옵션을 선택하는 경우 자동 애플리케이션 계층 DDoS 완화에 대한 구성 선택 사항과 상관없이 이전 버전의 웹 ACL을 교체하도록 선택할 수 있습니다.

  대체 옵션을 선택하면 Firewall Manager는 필요에 따라 새 버전의 웹 ACL을 생성한 다음 정책의 범위 내 리소스에 대해 다음을 수행합니다.
  - 리소스가 다른 활성 Firewall Manager 정책의 웹 ACL과 연결된 경우 Firewall Manager는 연결을 그대로 둡니다.
  - 다른 경우에는 Firewall Manager가 AWS WAF 클래식 웹 ACL과의 연결을 모두 제거하고 리소스를 정책의 AWS WAF (v2) 웹 ACL과 연결합니다.

원하는 경우 Firewall Manager에서 이전 버전의 웹 ACL을 새 버전의 웹 ACL로 교체하도록 선택할 수 있습니다. 이전에 정책의 AWS WAF 클래식 웹 ACL을 사용자 지정한 경우 Firewall Manager에서 대체 단계를 수행하도록 선택하기 전에 새 버전의 웹 ACL을 유사한 설정으로 업데이트할 수 있습니다.

동일한 버전의 콘솔 또는 Classic을 통해 정책에 대한 웹 ACL의 두 버전 중 하나에 액세스할 수 있습니다. AWS WAF AWS WAF

Firewall Manager는 정책 자체를 삭제할 때까지 교체된 AWS WAF 클래식 웹 ACL을 삭제하지 않습니다. 정책에서 AWS WAF 클래식 웹 ACL을 더 이상 사용하지 않는 경우 원하는 경우 삭제할 수 있습니다.

Shield Advanced 정책에서 사용하는 버전 결정 AWS WAF

정책의 AWS Config 서비스 연결 규칙에 있는 매개변수 키를 살펴보면 AWS WAF Firewall Manager Shield Advanced 정책의 어떤 버전을 사용하는지 확인할 수 있습니다. 사용 AWS WAF 중인 버전이 최신 버전인 경우 매개 변수 키에는 및 가 포함됩니다`policyId`. `webAclArn` 이전 버전인 AWS WAF Classic인 경우 매개 변수 키에는 `webAclId` 및 가 포함됩니다`resourceTypes`.

AWS Config 규칙에는 정책이 현재 범위 내 리소스와 함께 사용 중인 웹 ACL의 키만 나열됩니다.

방화벽 관리자 Shield Advanced 정책의 어떤 버전을 사용하는지 확인하려면 AWS WAF

1. Shield Advanced 정책의 정책 ID를 검색하십시오.

   a. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   b. 탐색 창에서 보안 정책을 선택합니다.

   c. 정책의 리전을 선택합니다. CloudFront 배포판의 경우 다음과 같습니다. `Global`

   d. 원하는 정책을 찾아 해당 정책 ID의 값을 복사하십시오.

      정책 ID 예제: `1111111-2222-3333-4444-a55aa5aaa555`.

2. 문자열에 정책 ID를 추가하여 정책의 AWS Config 규칙 이름을 생성합니다. `FMManagedShieldConfigRule`

   예제 AWS Config 규칙 이름:. `FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`

3. 관련 AWS Config 규칙의 매개 변수에서 이름이 지정된 `policyId` 키와 `webAclArn` 다음을 검색하십시오.

   a. https://console.aws.amazon.com/config/ 에서 AWS Config 콘솔을 엽니다.

   b. 탐색 창에서 규칙을 선택합니다.

   c. 목록에서 Firewall Manager 정책의 AWS Config 규칙 이름을 찾아 선택합니다. 역할 페이지가 열립니다.

   d. 파라미터 섹션의 규칙 세부 정보에서 키를 확인합니다. 이름이 `policyId` 및 `webAclArn`인 키를 찾은 경우 정책은 최신 버전의 AWS WAF을 사용하여 만든 웹 ACL을 사용합니다. 이름이 `webAclId` 및 `resourceTypes` 인 키를 찾은 경우 정책은 이전 버전인 AWS WAF Classic을 사용하여 만든 웹 ACL을 사용합니다.

보안 그룹 정책

에서 AWS Firewall Manager 보안 그룹 정책을 사용하여 조직의 Amazon Virtual Private Cloud 보안 그룹을 관리할 수 AWS Organizations있습니다. 중앙에서 제어하는 보안 그룹 정책을 전체 조직 또는 선

택한 계정 및 리소스 하위 집합에 적용할 수 있습니다. 또한 감사 및 사용 보안 그룹 정책을 사용하여 조직에서 사용 중인 보안 그룹 정책을 모니터링하고 관리할 수 있습니다.

Firewall Manager는 정책을 지속적으로 유지 관리하고 조직 전체에서 추가되거나 업데이트되는 계정과 리소스에 적용합니다. 에 대한 AWS Organizations자세한 내용은 AWS Organizations 사용 설명서를 참조하십시오.

Amazon Virtual Private Cloud 보안 그룹에 관한 자세한 내용은 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

Firewall Manager 보안 그룹 정책을 사용하여 AWS 조직 전체에서 다음을 수행할 수 있습니다.

- 지정된 계정과 리소스에 공통 보안 그룹을 적용합니다.
- 보안 그룹 규칙을 감사하여 규정 미준수 규칙을 찾고 문제를 해결합니다.
- 보안 그룹의 사용을 감사하여 사용되지 않는 보안 그룹과 중복 보안 그룹을 정리합니다.

이 단원에서는 Firewall Manager 보안 그룹 정책의 작동 방식을 다루고 정책 사용 지침을 제공합니다. 보안 그룹 정책을 생성하는 절차는 AWS Firewall Manager 정책 생성을 참조하세요.

공통 보안 그룹 정책

공통 보안 그룹 정책을 사용하면 Firewall Manager는 조직 전체에서 계정과 리소스에 대한 보안 그룹의 연결을 중앙에서 제어할 수 있습니다. 조직에서 정책을 적용할 위치와 방법을 지정합니다.

다음과 같은 리소스 유형에 공통 보안 그룹 정책을 적용할 수 있습니다.

- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스
- 탄력적 네트워크 인터페이스
- Application Load Balancer
- Classic Load Balancer

콘솔을 사용하여 공통 보안 그룹 정책을 생성하는 방법에 대한 지침은 공통 보안 그룹 정책 생성을 참조하세요.

공유 VPC

공통 보안 그룹 정책에 대한 정책 범위 설정에서 공유 VPC를 포함하도록 선택할 수 있습니다. 이 옵션에는 다른 계정이 소유하고 범위 내 계정과 공유되는 VPC가 포함됩니다. 범위 내 계정이 소유한 VPC

는 항상 포함됩니다. 공유 VPC에 대한 자세한 내용은 Amazon VPC 사용 설명서의 공유 VPC 작업을 참조하세요.

공유 VPC 포함에는 다음과 같은 주의 사항이 적용됩니다. 다음은 보안 그룹 정책 경고 및 제한에서 보안 그룹 정책에 대한 일반적인 주의 사항에 추가됩니다.

- Firewall Manager는 범위 내 각 계정에 대해 기본 보안 그룹을 VPC에 복제합니다. 공유 VPC의 경우, Firewall Manager는 VPC가 공유되는 범위 내 각 계정에 대해 기본 보안 그룹을 한 번 복제합니다. 이로 인해 단일 공유 VPC에 여러 개의 복제본이 생성될 수 있습니다.
- 새 공유 VPC를 생성하면 정책 범위 내에 있는 VPC에 리소스를 하나 이상 생성할 때까지 해당 공유 VPC가 Firewall Manager 보안 그룹 정책 세부 정보에 표시되지 않습니다.
- 공유 VPC가 활성화된 정책에서 공유 VPC를 비활성화하면 공유 VPC에서 Firewall Manager는 리소스와 연결되지 않은 복제본 보안 그룹을 삭제합니다. Firewall Manager는 나머지 복제본 보안 그룹을 그대로 두지만 관리를 중단합니다. 나머지 보안 그룹을 제거하려면 각 공유 VPC 인스턴스에서 수동으로 관리해야 합니다.

기본 보안 그룹

각 공통 보안 그룹 정책에 대해 하나 이상의 기본 보안 그룹을 제공합니다 AWS Firewall Manager .

- 기본 보안 그룹은 Firewall Manager 관리자 계정으로 생성해야 하며 계정의 모든 Amazon VPC 인스턴스에 상주할 수 있습니다.
- Amazon Virtual Private Cloud(Amazon VPC) 또는 Amazon Elastic Compute Cloud(Amazon EC2)를 통해 기본 보안 그룹을 관리할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 작업을 참조하세요.
- 하나 이상의 보안 그룹을 Firewall Manager 보안 그룹 정책의 기본 그룹으로 지정할 수 있습니다. 기본적으로 정책에 허용된 보안 그룹 수는 1이지만 요청을 제출하여 수를 증가시킬 수 있습니다. 자세한 내용은 AWS Firewall Manager 할당량을 참조하세요.

정책 규칙 설정

공통 보안 그룹 정책의 보안 그룹 및 리소스에 대해 다음 변경 제어 동작 중 하나 이상을 선택할 수 있습니다.

- 로컬 사용자가 변경한 내용을 식별하고 복제본 보안 그룹으로 되돌립니다.
- 정책 범위 내에 있는 AWS 리소스에서 다른 보안 그룹을 모두 분리하십시오.
- 기본 그룹의 태그를 복제본 보안 그룹에 배포합니다.

> **Important**
>
> Firewall Manager는 AWS 서비스에서 추가한 시스템 태그를 복제본 보안 그룹에 배포하지 않습니다. 시스템 태그는 `aws:` 접두사로 시작합니다. 정책에 조직의 태그 정책과 충돌하는 태그가 있는 경우 Firewall Manager는 기존 보안 그룹의 태그를 업데이트하거나 새 보안 그룹을 만들지 않습니다. 태그 정책에 대한 자세한 내용은 AWS Organizations 사용 설명서의 태그 정책을 참조하십시오.

- 기본 그룹에서 복제본 보안 그룹으로 보안 그룹을 배포합니다.

  이를 통해 모든 범위 내 리소스에서 지정된 보안 그룹의 VPC와 연결된 인스턴스에 대해 공통 보안 그룹 참조 규칙을 쉽게 설정할 수 있습니다. 이 옵션을 활성화하면 Firewall Manager는 보안 그룹이 Amazon Virtual Private Cloud의 피어 보안 그룹을 참조하는 경우에만 보안 그룹 참조를 전파합니다. 복제본 보안 그룹이 피어 보안 그룹을 올바르게 참조하지 않는 경우 Firewall Manager는 이러한 복제된 보안 그룹을 비준수로 표시합니다. Amazon VPC에서 피어 보안 그룹을 참조하는 방법에 대한 자세한 내용은 Amazon VPC 피어링 가이드의 피어 보안 그룹을 참조하도록 보안 그룹 업데이트를 참조하십시오.

  이 옵션을 활성화하지 않으면 Firewall Manager는 보안 그룹 참조를 복제본 보안 그룹에 전파하지 않습니다. Amazon VPC의 VPC 피어링에 대한 자세한 내용은 Amazon VPC 피어링 가이드를 참조하십시오.

정책 생성 및 관리

공통 보안 그룹 정책을 생성하면 Firewall Manager는 기본 보안 그룹을 정책 범위 내의 모든 Amazon VPC 인스턴스에 복제하고 복제된 보안 그룹을 정책 범위에 있는 계정과 리소스에 연결합니다. 기본 보안 그룹을 수정하면 Firewall Manager는 변경 사항을 복제본에 전파합니다.

공통 보안 그룹 정책을 삭제하면 정책에서 생성된 리소스를 정리할지 여부를 선택할 수 있습니다. Firewall Manager 공통 보안 그룹의 경우 이러한 리소스는 복제본 보안 그룹입니다. 정책을 삭제한 후 각 개별 복제본을 수동으로 관리하려는 경우가 아니면 정리 옵션을 선택합니다. 대부분의 경우 정리 옵션을 선택하는 것이 가장 간단한 접근 방식입니다.

복제본을 관리하는 방법

Amazon VPC 인스턴스의 복제본 보안 그룹은 다른 Amazon VPC 보안 그룹과 같은 방식으로 관리됩니다. 자세한 정보는 Amazon VPC 사용 설명서의 VPC의 보안 그룹을 참조하세요.

콘텐츠 감사 보안 그룹 정책

AWS Firewall Manager 콘텐츠 감사 보안 그룹 정책을 사용하여 조직의 보안 그룹에서 사용 중인 규칙을 감사하고 정책 조치를 적용할 수 있습니다. 콘텐츠 감사 보안 그룹 정책은 정책에 정의된 범위에 따라 AWS 조직에서 사용 중인 모든 고객 생성 보안 그룹에 적용됩니다.

콘솔을 사용한 콘텐츠 감사 보안 그룹 정책 생성에 대한 지침은 콘텐츠 감사 보안 그룹 정책 생성을 참조하세요.

정책 범위 리소스 유형

다음과 같은 리소스 유형에 콘텐츠 감사 보안 그룹 정책을 적용할 수 있습니다.

- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스
- 탄력적 네트워크 인터페이스
- Amazon VPC 보안 그룹

보안 그룹이 명시적으로 범위 내에 있거나 범위 내에 있는 리소스와 연결되어 있는 경우 보안 그룹은 정책 범위 내에서 고려됩니다.

정책 규칙 옵션

각 콘텐츠 감사 정책에는 관리형 정책 규칙 또는 사용자 지정 정책 규칙을 사용할 수 있지만 둘 다 사용할 수는 없습니다.

- 관리형 정책 규칙 - 관리형 규칙이 포함된 정책에서는 애플리케이션 및 프로토콜 목록을 사용하여 Firewall Manager가 감사하고 준수 또는 비준수로 표시하는 규칙을 제어할 수 있습니다. Firewall Manager에서 관리하는 목록을 사용할 수 있습니다. 자체 애플리케이션 및 프로토콜 목록을 만들어 사용할 수도 있습니다. 이러한 유형의 목록 및 사용자 지정 목록의 관리 옵션에 대한 자세한 내용은 관리형 목록을 참조하세요.
- 사용자 지정 정책 규칙 - 사용자 지정 정책 규칙이 포함된 정책에서는 기존 보안 그룹을 정책의 감사 보안 그룹으로 지정합니다. 감사 보안 그룹 규칙을 Firewall Manager가 감사하고 준수 또는 비준수로 표시하는 규칙을 정의하는 템플릿으로 사용할 수 있습니다.

감사 보안 그룹

정책에서 사용할 수 있으려면 먼저 Firewall Manager 관리자 계정을 사용하여 이러한 감사 보안 그룹을 만들어야 합니다. Amazon Virtual Private Cloud(Amazon VPC) 또는 Amazon Elastic Compute

Cloud(Amazon EC2)를 통해 보안 그룹을 관리할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 보안 그룹 작업을 참조하세요.

콘텐츠 감사 보안 그룹 정책에 사용하는 보안 그룹은 Firewall Manager에서 정책의 범위에 있는 보안 그룹에 대한 비교 참조로만 사용됩니다. Firewall Manager는 이를 조직의 어떤 리소스와도 연결하지 않습니다.

감사 보안 그룹에서 규칙을 정의하는 방법은 정책 규칙 설정에 따라 달라집니다.

- 관리형 정책 규칙 - 관리형 정책 규칙 설정의 경우 감사 보안 그룹을 사용하여 정책의 다른 설정을 재정의하고 다른 규정 준수 결과를 초래할 수 있는 규칙을 명시적으로 허용하거나 거부합니다.
  - 감사 보안 그룹에 정의된 규칙을 항상 허용하도록 선택하면 감사 보안 그룹에 정의된 규칙과 일치하는 모든 규칙이 다른 정책 설정과 상관없이 정책을 준수하는 것으로 간주됩니다.
  - 감사 보안 그룹에 정의된 규칙을 항상 거부하도록 선택하면 감사 보안 그룹에 정의된 규칙과 일치하는 모든 규칙이 다른 정책 설정과 상관없이 정책을 미준수하는 것으로 간주됩니다.
- 사용자 지정 정책 규칙 - 사용자 지정 정책 규칙 설정의 경우 감사 보안 그룹은 범위 내 보안 그룹 규칙에 허용되거나 허용되지 않는 항목의 예를 제공합니다.
  - 규칙 사용을 허용하도록 선택한 경우 범위 내 모든 보안 그룹에는 정책의 감사 보안 그룹 규칙의 허용 범위 내에 있는 규칙만 있어야 합니다. 이 경우 정책의 보안 그룹 규칙은 수행하도록 허용할 수 있는 작업의 예를 제공합니다.
  - 규칙 사용을 거부하도록 선택한 경우 범위 내 모든 보안 그룹에는 정책의 감사 보안 그룹 규칙의 허용 범위 내에 없는 규칙만 있어야 합니다. 이 경우 정책의 보안 그룹은 수행하도록 허용할 수 없는 작업의 예를 제공합니다.

정책 생성 및 관리

감사 보안 그룹 정책을 생성할 때 자동 문제 해결을 비활성화해야 합니다. 자동 문제 해결을 활성화하기 전에 정책 생성의 효과를 검토하는 것이 좋습니다. 예상되는 효과를 검토한 후 정책을 편집하고 자동 문제 해결을 활성화할 수 있습니다. 자동 문제 해결을 활성화하면 Firewall Manager는 범위 내 보안 그룹에서 규정을 준수하지 않는 규칙을 업데이트하거나 제거합니다.

감사 보안 그룹 정책의 영향을 받는 보안 그룹

조직에서 고객이 생성한 모든 보안 그룹은 감사 보안 그룹 정책의 범위에 속할 수 있습니다.

복제본 보안 그룹은 고객이 생성한 것이 아니므로 감사 보안 그룹 정책의 범위에 직접 포함될 수 없습니다. 하지만 복제본 보안 그룹은 정책의 자동 문제 해결 활동의 결과로 업데이트될 수 있습니다. 공통 보안 그룹 정책의 기본 보안 그룹은 고객이 생성하며 감사 보안 그룹 정책의 범위에 속할 수 있습니다.

감사 보안 그룹 정책에 따라 기본 보안 그룹이 변경되는 경우 Firewall Manager는 이러한 변경 사항을 복제본에 자동으로 전파합니다.

사용 감사 보안 그룹 정책

AWS Firewall Manager 사용 감사 보안 그룹 정책을 사용하여 조직에 사용되지 않고 중복된 보안 그룹이 있는지 모니터링하고 필요에 따라 정리를 수행할 수 있습니다. 이 정책에 대해 자동 문제 해결을 활성화하면 Firewall Manager에서 다음을 수행합니다.

1. 해당 옵션을 선택한 경우 중복 보안 그룹을 통합합니다.
2. 해당 옵션을 선택한 경우 사용하지 않는 보안 그룹을 제거합니다.

다음과 같은 리소스 유형에 사용 감사 보안 그룹 정책을 적용할 수 있습니다.

- Amazon VPC 보안 그룹

콘솔을 사용한 사용 감사 보안 그룹 정책 생성에 대한 지침은 사용 감사 보안 그룹 정책 생성을 참조하세요.

Firewall Manager가 중복 보안 그룹을 탐지하고 문제를 해결하는 방법

보안 그룹을 중복 보안 그룹으로 간주하려면 보안 그룹에 정확히 동일한 규칙이 설정된 상태여야 하며 보안 그룹이 동일한 Amazon VPC 인스턴스에 있어야 합니다.

중복 보안 그룹 세트의 문제를 해결하려면 Firewall Manager는 해당 세트의 보안 그룹 중에서 유지할 보안 그룹 하나를 선택한 다음, 해당 보안 그룹을 세트 내의 다른 보안 그룹과 연결된 모든 리소스에 연결합니다. 그런 다음 Firewall Manager는 연결된 리소스에서 다른 보안 그룹을 분리하여 사용하지 않게 합니다.

> **Note**
>
> 사용되지 않는 보안 그룹을 제거하도록 선택한 경우 Firewall Manager는 다음에 이 작업을 수행합니다. 그러면 중복 집합에 있는 보안 그룹이 제거될 수 있습니다.

Firewall Manager가 사용하지 않는 보안 그룹을 탐지하고 문제를 해결하는 방법

Firewall Manager는 다음 두 가지 조건에 모두 해당하는 경우 보안 그룹을 사용하지 않는 것으로 간주합니다.

- 보안 그룹은 Amazon EC2 인스턴스 또는 Amazon EC2 엘라스틱 네트워크 인터페이스에서 사용되지 않습니다.
- Firewall Manager가 정책 규칙 기간에 지정된 시간 (분) 내에 해당 구성 항목을 받지 못했습니다.

정책 규칙 기간의 기본 설정은 0분이지만 새 보안 그룹을 리소스와 연결할 시간을 확보하기 위해 시간을 최대 365일 (525,600분) 까지 늘릴 수 있습니다.

> **Important**
>
> 기본값인 0이 아닌 시간 (분) 을 지정하는 경우 에서 간접 관계를 활성화해야 합니다. AWS Config그렇지 않으면 사용 감사 보안 그룹 정책이 의도한 대로 작동하지 않습니다. 의 간접 관계에 대한 자세한 내용은 AWS Config 개발자 안내서의 간접 관계를 참조하십시오. AWS Config AWS Config

Firewall Manager는 가능한 경우 규칙 설정에 따라 계정에서 사용하지 않는 보안 그룹을 삭제하여 문제를 해결합니다. Firewall Manager에서 보안 그룹을 삭제할 수 없는 경우 정책을 준수하지 않는 것으로 표시합니다. Firewall Manager는 다른 보안 그룹에서 참조하는 보안 그룹을 삭제할 수 없습니다.

수정 시기는 기본 기간 설정을 사용하는지 사용자 지정 설정을 사용하는지에 따라 달라집니다.

- 기간은 0으로 설정, 기본값 — 이 설정을 사용하면 Amazon EC2 인스턴스 또는 Elastic network Interface에서 보안 그룹을 사용하지 않는 즉시 사용하지 않는 것으로 간주됩니다.

  이 제로 기간 설정의 경우 Firewall Manager는 보안 그룹을 즉시 수정합니다.
- 0보다 큰 기간 - 이 설정을 사용하면 Amazon EC2 인스턴스 또는 Elastic network 인터페이스에서 보안 그룹을 사용하지 않고 Firewall Manager가 지정된 시간 (분) 내에 보안 그룹에 대한 구성 항목을 받지 않으면 사용하지 않은 것으로 간주됩니다.

  0이 아닌 기간 설정의 경우 Firewall Manager는 보안 그룹이 24시간 동안 사용되지 않은 상태로 유지된 후에 보안 그룹을 수정합니다.

기본 계정 사양

콘솔을 통해 사용 감사 보안 그룹 정책을 생성할 때 Firewall Manager는 지정된 계정 제외 및 기타 모든 계정 포함을 자동으로 선택합니다. 그런 다음 이 서비스는 제외할 목록에 Firewall Manager 관리자 계정을 넣습니다. 이 방법이 권장되는 접근 방식이며 이렇게 하면 Firewall Manager 관리자 계정에 속한 보안 그룹을 수동으로 관리할 수 있습니다.

보안 그룹 정책의 모범 사례

이 단원에서는 AWS Firewall Manager를 사용하여 보안 그룹을 관리하기 위한 권장 사항을 설명합니다.

Firewall Manager 관리자 계정 제외

정책 범위를 설정할 때 Firewall Manager 관리자 계정을 제외합니다. 콘솔을 통해 사용 감사 보안 그룹 정책을 생성할 때는 이 작업이 기본 옵션입니다.

자동 문제 해결이 비활성화된 상태로 시작

콘텐츠 또는 사용 감사 보안 그룹 정책의 경우 자동 문제 해결이 비활성화된 상태로 시작합니다. 정책 세부 정보를 검토하여 자동 문제 해결이 미칠 수 있는 영향을 확인합니다. 변경 내용이 원하는 대로 만족스러우면 정책을 편집하여 자동 문제 해결을 활성화합니다.

외부 소스도 사용하여 보안 그룹을 관리하는 경우 충돌 방지

Firewall Manager 이외의 도구 또는 서비스를 사용하여 보안 그룹을 관리하는 경우 Firewall Manager의 설정과 외부 소스의 설정 간에 충돌이 발생하지 않도록 주의하십시오. 자동 문제 해결을 사용할 때 설정이 충돌하는 경우 충돌하는 문제 해결 주기가 생성되어 양쪽에서 리소스를 소비할 수 있습니다.

예를 들어 AWS 리소스 집합에 대한 보안 그룹을 유지 관리하도록 다른 서비스를 구성하고 동일한 리소스의 일부 또는 전체에 대해 또 다른 보안 그룹을 유지 관리하도록 Firewall Manager 정책을 구성한다고 가정합니다. 한 서비스를 다른 보안 그룹이 범위 내 리소스와 연결되지 않도록 구성하면 해당 서비스가 다른 서비스에서 유지 관리하는 보안 그룹 연결을 제거합니다. 양측 모두 이러한 방식으로 구성되면 충돌하는 연결 해제 및 연결 주기가 발생할 수 있습니다.

또한 Firewall Manager 감사 정책을 만들어 다른 서비스의 보안 그룹 구성과 충돌하는 보안 그룹 구성을 적용한다고 가정해 보겠습니다. Firewall Manager 감사 정책에 의해 적용된 문제 해결이 해당 보안 그룹을 업데이트하거나 삭제하여 다른 서비스가 규정 준수에서 벗어날 수 있습니다. 다른 서비스가 발견된 문제를 모니터링하고 자동으로 해결하도록 구성된 경우 이 서비스가 보안 그룹을 다시 생성하거나 업데이트하여 다시 Firewall Manager 감사 정책을 준수하지 않게 됩니다. Firewall Manager 감사 정책이 자동 문제 해결로 구성된 경우 이 정책이 다시 외부 보안 그룹을 업데이트하거나 삭제하는 식으로 계속 반복됩니다.

이와 같은 충돌을 피하려면 Firewall Manager와 외부 소스 간에 상호 배타적인 구성을 만들어야 합니다.

태그 지정을 사용하여 Firewall Manager 정책에 따라 외부 보안 그룹을 자동 문제 해결에서 제외할 수 있습니다. 이렇게 하려면 보안 그룹 또는 외부 소스에서 관리하는 다른 리소스에 태그를 하나 이상 추

가합니다. 그런 다음 Firewall Manager 정책 범위를 정의할 때 리소스 사양에서 추가한 태그가 있는 리소스를 제외합니다.

마찬가지로 외부 도구 또는 서비스에서 Firewall Manager가 관리하는 보안 그룹을 관리 또는 감사 활동에서 제외합니다. Firewall Manager 리소스를 가져오거나 외부 관리에서 제외하기 위해 Firewall Manager 고유 태그를 지정하지 마십시오.

사용 감사 보안 그룹 정책의 모범 사례

사용 감사 보안 그룹 정책을 사용할 때는 이 가이드라인을 따르세요.

- 짧은 시간 (예: 15분 이내) 내에 보안 그룹의 연결 상태를 여러 번 변경하지 마십시오. 이렇게 하면 Firewall Manager에서 해당 이벤트 중 일부 또는 전체를 놓칠 수 있습니다. 예를 들어, Elastic Network Interface와 보안 그룹을 빠르게 연결하거나 연결 해제하지 마십시오.

보안 그룹 정책 경고 및 제한

이 섹션에는 Firewall Manager 보안 그룹 정책 사용에 대한 주의 사항 및 제한 사항이 나와 있습니다.

- Fargate 서비스 유형을 사용하여 생성한 Amazon EC2 탄력적 네트워크 인터페이스에 대한 보안 그룹 업데이트는 지원되지 않습니다. 하지만 Amazon ECS 서비스 유형을 사용하여 Amazon EC2 탄력적 네트워크 인터페이스에 대한 보안 그룹을 업데이트할 수 있습니다.
- Firewall Manager는 Amazon 관계형 데이터베이스 서비스에서 생성한 Amazon EC2 탄력적 네트워크 인터페이스의 보안 그룹을 지원하지 않습니다.
- Amazon ECS 탄력적 네트워크 인터페이스 업데이트는 롤링 업데이트(Amazon ECS) 배포 컨트롤러를 사용하는 Amazon ECS 서비스에 대해서만 가능합니다. CODE_DEPLOY 또는 외부 컨트롤러와 같은 다른 Amazon ECS 배포 컨트롤러의 경우 현재 Firewall Manager는 탄력적 네트워크 인터페이스를 업데이트할 수 없습니다.
- Amazon EC2 탄력적 네트워크 인터페이스에 대한 보안 그룹을 사용하는 경우, 보안 그룹에 대한 변경 사항은 Firewall Manager에 즉시 표시되지 않습니다. Firewall Manager는 일반적으로 몇 시간 내에 변경 사항을 탐지하지만 탐지는 최대 6시간까지 지연될 수 있습니다.
- Firewall Manager는 Network Load Balancer에 대한 탄력적 네트워크 인터페이스의 보안 그룹 업데이트를 지원하지 않습니다.
- 공통 보안 그룹 정책에서 공유 VPC가 나중에 계정과 공유되지 않는 경우 Firewall Manager는 계정의 복제본 보안 그룹을 삭제하지 않습니다.
- 사용 감사 보안 그룹 정책의 경우 범위가 모두 같은 사용자 지정 지연 시간 설정을 사용하여 정책을 여러 개 만들면 규정 준수 결과가 포함된 첫 번째 정책이 결과를 보고하는 정책이 됩니다.

보안 그룹 정책 사용 사례

AWS Firewall Manager 공통 보안 그룹 정책을 사용하여 Amazon VPC 인스턴스 간 통신을 위한 호스트 방화벽 구성을 자동화할 수 있습니다. 이 단원에서는 표준 Amazon VPC 아키텍처를 나열하고 Firewall Manager 공통 보안 그룹 정책을 사용하여 각 아키텍처를 보호하는 방법을 설명합니다. 이러한 보안 그룹 정책을 사용하면 통합된 규칙 세트를 적용하여 다양한 계정의 리소스를 선택하고 Amazon Elastic Compute Cloud 및 Amazon VPC에서 계정별 구성을 피할 수 있습니다.

Firewall Manager 공통 보안 그룹 정책을 사용하면 다른 Amazon VPC의 인스턴스와 통신하는 데 필요한 EC2 탄력적 네트워크 인터페이스에만 태그를 지정할 수 있습니다. 동일한 Amazon VPC의 다른 인스턴스는 더 안전하게 보호되고 격리됩니다.

사용 사례: Application Load Balancer 및 Classic Load Balancer에 대한 요청 모니터링 및 제어

Firewall Manager 공통 보안 그룹 정책을 사용하여 범위 내 로드 밸런서가 처리해야 하는 요청을 정의할 수 있습니다. Firewall Manager 콘솔을 통해 이를 구성할 수 있습니다. 보안 그룹의 인바운드 규칙을 준수하는 요청만 로드 밸런서에 도달할 수 있으며, 로드 밸런서는 아웃바운드 규칙을 충족하는 요청만 배포합니다.

사용 사례: 인터넷에 액세스할 수 있는 퍼블릭 Amazon VPC

Firewall Manager 공통 보안 그룹 정책을 사용하여 퍼블릭 Amazon VPC를 보호할 수 있습니다. 예를 들면, 인바운드 포트 443만 허용할 수 있습니다. 이렇게 하면 퍼블릭 VPC에 대한 인바운드 HTTPS 트래픽만 허용하는 것과 같습니다. VPC 내의 퍼블릭 리소스(예: “PublicVpc”)에 태그를 지정한 다음 Firewall Manager 정책 범위를 해당 태그가 있는 리소스만으로 설정할 수 있습니다. Firewall Manager는 해당 리소스에 정책을 자동으로 적용합니다.

사용 사례: 퍼블릭 및 프라이빗 Amazon VPC 인스턴스

인터넷에서 액세스할 수 있는 퍼블릭 Amazon VPC 인스턴스에 대한 이전 사용 사례에서 권장되는 것과 동일한 공통 보안 그룹 정책을 퍼블릭 리소스에 사용할 수 있습니다. 두 번째 공통 보안 그룹 정책을 사용하여 퍼블릭 리소스와 프라이빗 리소스 간의 통신을 제한할 수 있습니다. 퍼블릭 및 프라이빗 Amazon VPC 인스턴스의 리소스에 PublicPrivate ""와 같은 태그를 지정하여 두 번째 정책을 적용합니다. 세 번째 정책을 사용하여 프라이빗 리소스와 기타 기업 또는 프라이빗 Amazon VPC 인스턴스 간에 허용되는 통신을 정의할 수 있습니다. 이 정책의 경우 프라이빗 리소스에서 다른 식별 태그를 사용할 수 있습니다.

사용 사례: 허브 및 스포크 Amazon VPC 인스턴스

공통 보안 그룹 정책을 사용하여 허브 Amazon VPC 인스턴스와 스포크 Amazon VPC 인스턴스 간의 통신을 정의할 수 있습니다. 두 번째 정책을 사용하여 각 스포크 Amazon ECS 인스턴스에서 허브 Amazon ECS 인스턴스로 연결되는 통신을 정의할 수 있습니다.

사용 사례: Amazon EC2 인스턴스의 기본 네트워크 인터페이스

공통 보안 그룹 정책을 사용하여 내부 SSH 및 패치/OS 업데이트 서비스와 같은 표준 통신만 허용하고 다른 안전하지 않은 통신을 허용하지 않을 수 있습니다.

사용 사례: 공개 권한이 있는 리소스 식별

감사 보안 그룹 정책을 사용하여 퍼블릭 IP 주소와 통신할 권한이 있거나 타사 공급업체에 속한 IP 주소가 있는 조직 내의 모든 리소스를 식별할 수 있습니다.

Amazon VPC 네트워크 액세스 제어 목록 (ACL) 정책

이 섹션에서는 AWS Firewall Manager 네트워크 ACL 정책의 작동 방식을 다루고 이를 사용하기 위한 지침을 제공합니다. 콘솔을 사용하여 네트워크 ACL 정책을 생성하는 방법에 대한 지침은 을 참조하십시오. 네트워크 ACL 정책 생성

Amazon VPC 네트워크 액세스 제어 목록 (ACL) 에 대한 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL을 사용하여 서브넷으로의 트래픽 제어를 참조하십시오.

Firewall Manager 네트워크 ACL 정책을 사용하여 조직의 Amazon VPC (가상 사설 클라우드) 네트워크 액세스 제어 목록 (ACL) 을 관리할 수 있습니다. AWS Organizations정책의 네트워크 ACL 규칙 설정과 설정을 적용할 계정 및 서브넷을 정의합니다. Firewall Manager는 조직 전체에서 추가되거나 업데이트되는 계정 및 서브넷에 정책 설정을 지속적으로 적용합니다. 정책 범위 및 AWS Organizations에 대한 자세한 내용은 AWS Organizations 사용 설명서를 참조하십시오AWS Firewall Manager 정책 범위.

Firewall Manager 네트워크 ACL 정책을 정의할 때는 이름 및 범위와 같은 표준 Firewall Manager 정책 설정 외에도 다음을 제공합니다.

- 인바운드 및 아웃바운드 트래픽 처리에 대한 첫 번째 및 마지막 규칙. Firewall Manager는 정책 범위에 속하는 네트워크 ACL에서 이러한 ACL의 존재 및 순서를 적용하거나 규정 미준수를 보고합니다. 개별 계정은 정책의 첫 번째 규칙과 마지막 규칙 사이에서 실행할 사용자 지정 규칙을 만들 수 있습니다.
- 수정으로 인해 네트워크 ACL의 규칙 간에 트래픽 관리 충돌이 발생할 수 있는 경우 강제로 수정을 적용할지 여부 이는 정책에 대한 수정이 활성화된 경우에만 적용됩니다.

Firewall Manager 네트워크 ACL 규칙 및 태깅

이 섹션에서는 네트워크 ACL 정책 규칙 사양과 Firewall Manager에서 관리하는 네트워크 ACL에 대해 설명합니다.

관리형 네트워크 ACL에 태그 지정

Firewall Manager는 값이 인 태그로 관리형 네트워크 ACL에 FMManaged 태그를 지정합니다. true Firewall Manager는 이 태그 설정이 있는 네트워크 ACL에 대해서만 문제 해결을 수행합니다.

정책에서 정의하는 규칙

네트워크 ACL 정책 사양에서는 인바운드 트래픽에 대해 첫 번째 및 마지막으로 실행할 규칙과 아웃바운드 트래픽에 대해 처음 및 마지막으로 실행할 규칙을 정의합니다.

기본적으로 정책의 첫 번째 규칙과 마지막 규칙을 조합하여 사용할 인바운드 규칙을 최대 5개까지 정의할 수 있습니다. 마찬가지로 아웃바운드 규칙을 최대 5개까지 정의할 수 있습니다. 이러한 제한에 대한 자세한 내용은 을 참조하십시오소프트 할당량. 네트워크 ACL의 일반 한도에 대한 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL에 대한 Amazon VPC 할당량을 참조하십시오.

정책 규칙에 규칙 번호를 할당하지 마십시오. 대신 평가하려는 순서대로 규칙을 지정하면 Firewall Manager는 이 순서를 사용하여 관리하는 네트워크 ACL에 규칙 번호를 할당합니다.

이 외에는 Amazon VPC를 통해 네트워크 ACL에서 규칙을 관리하는 것처럼 정책의 네트워크 ACL 규칙 사양을 관리합니다. Amazon VPC의 네트워크 ACL 관리에 대한 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL을 사용한 서브넷 트래픽 제어 및 네트워크 ACL 사용을 참조하십시오.

관리형 네트워크 ACL의 규칙

Firewall Manager는 개별 계정 관리자가 정의하는 사용자 지정 규칙의 앞뒤에 정책의 첫 번째 규칙과 마지막 규칙을 배치하여 관리하는 네트워크 ACL에서 규칙을 구성합니다. Firewall Manager는 사용자 지정 규칙의 순서를 유지합니다. 네트워크 ACL은 번호가 가장 낮은 규칙부터 시작하여 평가됩니다.

Firewall Manager는 네트워크 ACL을 처음 생성할 때 다음과 같은 번호를 사용하여 규칙을 정의합니다.

- 첫 번째 규칙: 1, 2,... — Firewall Manager 네트워크 ACL 정책에서 사용자가 정의합니다.

  Firewall Manager는 정책 사양에서 순서에 따라 규칙을 정렬하여 1부터 시작하여 1씩 증가하는 규칙 번호를 할당합니다.
- 사용자 지정 규칙: 5,000, 5,100,... — Amazon VPC를 통해 개별 계정 관리자가 관리합니다.

Firewall Manager는 이러한 규칙에 5,000부터 시작하여 이후의 각 규칙에 대해 100씩 증가하는 번호를 할당합니다.

- 마지막 규칙:... 32,765, 32,766 — Firewall Manager 네트워크 ACL 정책에서 사용자가 정의합니다.

  Firewall Manager는 정책 사양에서 순서에 따라 규칙을 정렬하여 가능한 가장 높은 수인 32766에서 1씩 증가하는 규칙 번호를 할당합니다.

네트워크 ACL을 초기화한 후에는 Firewall Manager가 관리형 네트워크 ACL에서 개별 계정의 변경 내용을 제어하지 않습니다. 정책의 첫 번째 규칙과 마지막 규칙 사이에 번호가 매겨져 있고 첫 번째 규칙과 마지막 규칙이 지정된 순서를 유지한다면 개별 계정은 규정을 준수하지 않고도 네트워크 ACL을 변경할 수 있습니다. 사용자 지정 규칙을 관리할 때는 이 섹션에 설명된 번호 매기기를 준수하는 것이 가장 좋습니다.

Firewall Manager가 서브넷에 대한 네트워크 ACL 관리를 시작하는 방법

Firewall Manager는 Firewall Manager가 생성하고 태그가 설정된 네트워크 ACL에 서브넷을 연결할 때 서브넷에 대한 네트워크 ACL 관리를 시작합니다. `FMManaged true`

네트워크 ACL 정책을 준수하려면 서브넷의 네트워크 ACL이 정책의 첫 번째 규칙을 먼저 배치하고, 정책에 지정된 순서대로, 마지막 규칙을 마지막에 배치하고, 기타 사용자 지정 규칙을 중간에 배치해야 합니다. 서브넷이 이미 연결되어 있는 비관리형 네트워크 ACL이나 관리형 네트워크 ACL을 통해 이러한 요구 사항을 충족할 수 있습니다.

Firewall Manager가 비관리형 네트워크 ACL과 연결된 서브넷에 네트워크 ACL 정책을 적용하는 경우 Firewall Manager는 다음을 순서대로 확인하고 실행 가능한 옵션을 식별하면 중지합니다.

1. 연결된 네트워크 ACL이 이미 호환됨 - 현재 서브넷과 연결된 네트워크 ACL이 규정을 준수하는 경우 Firewall Manager는 해당 연결을 그대로 두고 서브넷에 대한 네트워크 ACL 관리를 시작하지 않습니다.

   Firewall Manager는 소유하지 않은 네트워크 ACL을 변경하거나 관리하지 않지만, 규정을 준수하는 한 Firewall Manager는 이를 그대로 두고 정책 준수 여부만 모니터링합니다.
2. 규정을 준수하는 관리형 네트워크 ACL을 사용할 수 있습니다. - Firewall Manager에서 필요한 구성을 준수하는 네트워크 ACL을 이미 관리하고 있는 경우 이 옵션을 사용할 수 있습니다. 수정이 활성화된 경우 Firewall Manager는 서브넷을 해당 수정에 연결합니다. 문제 해결을 사용하지 않도록 설정한 경우 Firewall Manager는 서브넷을 비준수로 표시하고 네트워크 ACL 연결 교체를 문제 해결 옵션으로 제공합니다.

3. 규정을 준수하는 새 관리형 네트워크 ACL 생성 - 문제 해결이 활성화된 경우 Firewall Manager는 새 네트워크 ACL을 생성하여 서브넷에 연결합니다. 그렇지 않으면 Firewall Manager는 서브넷을 비호환으로 표시하고 새 네트워크 ACL을 생성하고 네트워크 ACL 연결을 교체하는 수정 옵션을 제공합니다.

이러한 단계가 실패할 경우 Firewall Manager는 서브넷에 대한 비준수 사실을 보고합니다.

Firewall Manager는 서브넷이 처음으로 범위에 포함되고 서브넷의 비관리형 네트워크 ACL이 규정을 준수하지 않을 때 다음 단계를 따릅니다.

Firewall Manager가 규정을 준수하지 않는 관리형 네트워크 ACL을 해결하는 방법

이 섹션에서는 관리형 네트워크 ACL이 정책을 준수하지 않는 경우 Firewall Manager에서 관리형 네트워크 ACL을 수정하는 방법을 설명합니다. Firewall Manager는 태그가 로 설정된 관리형 네트워크 ACL만 수정합니다. `FMManaged` `true` Firewall Manager에서 관리하지 않는 네트워크 ACL에 대해서는 을 참조하십시오초기 네트워크 ACL 관리.

수정은 첫 번째 규칙, 사용자 지정 규칙, 마지막 규칙의 상대 위치를 복원하고 첫 번째 규칙과 마지막 규칙의 순서를 복원합니다. 문제 해결 중에 Firewall Manager가 반드시 규칙을 네트워크 ACL 초기화에 사용하는 규칙 번호로 이동하지는 않습니다. 이러한 규칙 범주의 초기 번호 설정 및 설명은 을 참조하십시오. 초기 네트워크 ACL 관리

규정을 준수하는 규칙과 규칙 순서를 설정하기 위해 Firewall Manager는 네트워크 ACL 내에서 규칙을 이동해야 할 수 있습니다. Firewall Manager는 기존의 규정 준수 규칙 순서를 유지함으로써 네트워크 ACL의 보호를 최대한 보존합니다. 예를 들어 규칙을 새 위치에 일시적으로 복제한 다음 원래 규칙을 순서대로 제거하여 프로세스 중에 상대적 위치를 보존할 수 있습니다.

이 방법을 사용하면 설정이 보호되지만 네트워크 ACL에 임시 규칙을 위한 공간도 필요합니다. Firewall Manager가 네트워크 ACL의 규칙 한도에 도달하면 문제 해결이 중단됩니다. 이 경우 네트워크 ACL은 규정을 준수하지 않는 상태로 유지되며 Firewall Manager가 그 이유를 보고합니다.

계정이 Firewall Manager에서 관리하는 네트워크 ACL에 사용자 지정 규칙을 추가했는데 이러한 규칙이 Firewall Manager 문제 해결을 방해하는 경우 Firewall Manager는 네트워크 ACL에서 모든 수정 작업을 중지하고 충돌을 보고합니다.

강제 수정

정책에 자동 수정을 선택하는 경우 첫 번째 규칙 또는 마지막 규칙에 강제로 수정을 적용할지 여부도 지정합니다.

Firewall Manager는 사용자 지정 규칙과 정책 규칙 간에 트래픽 처리 시 충돌이 발생하는 경우 해당하는 강제 수정 설정을 참조합니다. 강제 수정이 활성화된 경우 Firewall Manager는 충돌에도 불구하고 업데이트를 적용합니다. 이 옵션이 활성화되지 않은 경우 Firewall Manager는 문제 해결을 중단합니다. 어느 경우든 Firewall Manager는 규칙 충돌을 보고하고 수정 옵션을 제공합니다.

규칙 수 요구 사항 및 제한

문제 해결 중에 Firewall Manager는 규칙이 제공하는 보호 기능을 변경하지 않고 규칙을 이동하기 위해 규칙을 일시적으로 복제할 수 있습니다.

인바운드 규칙과 아웃바운드 규칙의 경우 Firewall Manager에서 문제 해결을 수행하는 데 필요할 수 있는 최대 규칙 수는 다음과 같습니다.

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

네트워크 ACL과 네트워크 ACL 정책에는 변경 가능한 규칙 제한이 적용됩니다. Firewall Manager는 수정 작업이 한계에 도달하면 수정 시도를 중단하고 규정 미준수를 보고합니다.

Firewall Manager가 수정 작업을 수행할 수 있는 공간을 확보하기 위해 한도 증가를 요청할 수 있습니다. 또는 정책 또는 네트워크 ACL의 구성을 변경하여 사용되는 규칙 수를 줄일 수 있습니다.

네트워크 ACL 한도에 대한 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL에 대한 Amazon VPC 할당량을 참조하십시오.

수정이 실패한 경우

네트워크 ACL을 업데이트하는 동안 어떤 이유로든 Firewall Manager를 중지해야 하는 경우 변경 내용을 롤백하지 않고 대신 네트워크 ACL을 중간 상태로 유지합니다. `FMManaged`태그가 로 설정된 네트워크 ACL에서 중복된 규칙이 발견되면 Firewall Manager에서 해결 중일 수 있습니다. `true` 일정 기간 동안 변경이 부분적으로 완료될 수 있지만 Firewall Manager에서 사용하는 수정 방식 때문에 트래픽이 중단되거나 관련 서브넷에 대한 보호 수준이 저하되지는 않습니다.

Firewall Manager는 규정을 준수하지 않는 네트워크 ACL을 완전히 수정하지 않을 경우 관련 서브넷의 비준수 사실을 보고하고 가능한 수정 옵션을 제안합니다.

수정이 실패한 후 재시도

대부분의 경우 Firewall Manager가 네트워크 ACL에 대한 수정 변경을 완료하지 못하면 결국 변경을 재시도합니다.

단, 수정이 네트워크 ACL 규칙 수 제한 또는 VPC 네트워크 ACL 수 한도에 도달하는 경우는 예외입니다. Firewall Manager는 AWS 리소스가 제한 설정을 초과하는 문제 해결 활동을 수행할 수 없습니다. 이러한 경우 계속하려면 개수를 줄이거나 제한을 늘려야 합니다. 한도에 대한 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL에 대한 Amazon VPC 할당량을 참조하십시오.

Firewall Manager 네트워크 ACL 규정 준수 보고

Firewall Manager는 범위 내 서브넷에 연결된 모든 네트워크 ACL의 규정 준수를 모니터링하고 보고합니다.

일반적으로 규칙 순서가 올바르지 않거나 정책 규칙과 사용자 지정 규칙 간의 트래픽 처리 동작이 충돌하는 등의 상황에서 규정 미준수가 발생합니다. 비준수 보고에는 규정 준수 위반 및 해결 옵션이 포함됩니다.

Firewall Manager는 다른 정책 유형과 동일한 방식으로 네트워크 ACL 정책에 대한 규정 준수 위반을 보고합니다. 규정 준수 보고에 대한 자세한 내용은 을 참조하십시오AWS Firewall Manager 정책에 대한 규정 준수 정보 보기.

정책 업데이트 중 규정 미준수

네트워크 ACL 정책을 수정한 후 Firewall Manager가 정책 범위에 속하는 네트워크 ACL을 업데이트할 때까지 Firewall Manager는 해당 네트워크 ACL을 비준수로 표시합니다. Firewall Manager는 네트워크 ACL이 엄밀히 말하면 규정을 준수할 수 있는 경우에도 이 작업을 수행합니다.

예를 들어 정책 사양에서 규칙을 제거해도 범위 내 네트워크 ACL에는 여전히 추가 규칙이 있지만 해당 규칙 정의는 정책을 준수할 수 있습니다. 하지만 추가 규칙은 Firewall Manager에서 관리하는 규칙의 일부이므로 Firewall Manager는 이러한 추가 규칙을 현재 정책 설정을 위반한 것으로 간주합니다. 이는 방화벽 관리자의 관리형 네트워크 ACL에 추가한 사용자 지정 규칙을 Firewall Manager에서 보는 방식과는 다릅니다.

Firewall Manager 네트워크 ACL 정책 사용 모범 사례

이 섹션에는 Firewall Manager 네트워크 ACL 정책 및 관리형 네트워크 ACL을 사용하기 위한 권장 사항이 나와 있습니다.

`FMManaged`태그를 참조하여 Firewall Manager에서 관리하는 네트워크 ACL을 식별하십시오.

Firewall Manager에서 관리하는 네트워크 ACL에는 `FMManaged` 태그가 로 `true` 설정되어 있습니다. 이 태그를 사용하면 사용자 지정 네트워크 ACL을 Firewall Manager를 통해 관리하는 사용자 지정 네트워크 ACL과 구별하는 데 도움이 됩니다.

네트워크 ACL의 **`FMManaged`** 태그 값을 수정하지 마세요.

Firewall Manager는 이 태그를 사용하여 네트워크 ACL을 통한 관리 상태를 설정하고 결정합니다.

Firewall Manager에서 관리하는 네트워크 ACL이 있는 서브넷의 연결을 수정하지 마십시오.

서브넷과 Firewall Manager에서 관리하는 네트워크 ACL 간의 연결을 수동으로 변경하지 마십시오. 이렇게 하면 Firewall Manager에서 해당 서브넷에 대한 보호를 관리하는 기능이 비활성화될 수 있습니다. 의 `FMManaged true` 태그 설정을 찾아 Firewall Manager에서 관리하는 네트워크 ACL을 식별할 수 있습니다.

Firewall Manager 정책 관리에서 서브넷을 제거하려면 Firewall Manager 정책 범위 설정을 사용하여 서브넷을 제외합니다. 예를 들어, 서브넷에 태그를 지정한 다음 해당 태그를 정책 범위에서 제외할 수 있습니다. 자세한 정보는 AWS Firewall Manager 정책 범위을 참조하세요.

관리형 네트워크 ACL을 업데이트할 때 Firewall Manager에서 관리하는 규칙을 수정하지 마세요.

Firewall Manager에서 관리하는 네트워크 ACL에서는 에 설명된 번호 지정 체계를 준수하여 사용자 지정 규칙을 정책 규칙과 분리하십시오. Firewall Manager 네트워크 ACL 규칙 및 태깅 5,000에서 32,000 사이의 숫자를 가진 규칙만 추가하거나 수정하십시오.

계정 한도에 규칙을 너무 많이 추가하지 마세요.

네트워크 ACL을 수정하는 동안 Firewall Manager는 일반적으로 네트워크 ACL 규칙 수를 일시적으로 늘립니다. 비준수 문제를 방지하려면 사용 중인 규칙을 위한 충분한 공간이 있어야 합니다. 자세한 정보는 Firewall Manager가 규정을 준수하지 않는 관리형 네트워크 ACL을 해결하는 방법을 참조하세요.

자동 문제 해결이 비활성화된 상태로 시작

자동 문제 해결을 사용하지 않도록 설정한 상태에서 시작한 다음 정책 세부 정보를 검토하여 자동 수정이 미치는 영향을 파악하십시오. 변경 내용이 원하는 대로 만족스러우면 정책을 편집하여 자동 문제 해결을 활성화합니다.

Firewall Manager 네트워크 ACL 정책 경고

이 섹션에는 Firewall Manager 네트워크 ACL 정책 사용에 대한 주의 사항 및 제한 사항이 나와 있습니다.

- 다른 정책보다 느린 업데이트 시간 — Amazon EC2 네트워크 ACL API가 요청을 처리할 수 있는 속도에 제한이 있기 때문에 Firewall Manager는 일반적으로 네트워크 ACL 정책 및 정책 변경을 다른 Firewall Manager 정책보다 느리게 적용합니다. 다른 Firewall Manager 정책의 유사한 변경 사항보다, 특히 정책을 처음 추가할 때 정책 변경이 더 오래 걸리는 것을 알 수 있습니다.
- 초기 서브넷 보호의 경우 Firewall Manager는 이전 정책을 선호합니다. 이 정책은 Firewall Manager 네트워크 ACL 정책으로 아직 보호되지 않은 서브넷에만 적용됩니다. 서브넷이 동시에 둘 이상의 네

트워크 ACL 정책 범위에 포함되는 경우 Firewall Manager는 가장 오래된 정책을 사용하여 서브넷을 보호합니다.

- 정책이 서브넷 보호를 중단해야 하는 이유 — 서브넷의 네트워크 ACL을 관리하는 정책은 다음 중 하나가 발생할 때까지 관리를 유지합니다.
  - 서브넷이 정책 범위를 벗어납니다.
  - 정책이 삭제됩니다.
  - 다른 Firewall Manager 정책으로 관리되고 서브넷이 범위 내에 있는 네트워크 ACL로 서브넷 연결을 수동으로 변경합니다.

방화벽 관리자 네트워크 ACL 정책 삭제

Firewall Manager 네트워크 ACL 정책을 삭제하면 Firewall Manager는 해당 정책에 대해 관리하고 있던 모든 네트워크 `false` ACL에서 `FMManaged` 태그 값을 로 변경합니다.

또한 정책으로 생성된 리소스를 정리할지 여부를 선택할 수 있습니다. 정리를 선택하면 Firewall Manager는 다음 단계를 순서대로 시도합니다.

1. 연결을 원래 상태로 되돌리기 — Firewall Manager는 서브넷을 Firewall Manager가 관리를 시작하기 전에 연결된 네트워크 ACL에 다시 연결하려고 합니다.
2. 네트워크 ACL에서 첫 번째 규칙과 마지막 규칙 제거 - 연결을 변경할 수 없는 경우 Firewall Manager는 정책의 첫 번째 규칙과 마지막 규칙을 제거하고 서브넷과 연결된 네트워크 ACL에는 사용자 지정 규칙만 남깁니다.
3. 규칙이나 연결에 아무 것도 하지 마십시오. — 위의 작업 중 하나를 수행할 수 없는 경우 Firewall Manager는 네트워크 ACL과 연결을 그대로 유지합니다.

정리 옵션을 선택하지 않으면 정책이 삭제된 후 각 네트워크 ACL을 수동으로 관리해야 합니다. 대부분의 경우 정리 옵션을 선택하는 것이 가장 간단한 접근 방식입니다.

AWS Network Firewall 정책

AWS Firewall Manager 네트워크 방화벽 정책을 사용하여 조직 전체의 Amazon Virtual Private Cloud VPC에 대한 AWS Network Firewall 방화벽을 관리할 수 있습니다. AWS Organizations중앙에서 제어하는 방화벽을 전체 조직 또는 선택한 계정 및 VPC 하위 집합에 적용할 수 있습니다.

네트워크 방화벽은 VPC의 퍼블릭 서브넷에 대한 네트워크 트래픽 필터링 보호를 제공합니다. Firewall Manager는 정책에 정의된 방화벽 관리 유형에 따라 방화벽을 생성하고 관리합니다. Firewall Manager는 다음과 같은 방화벽 관리 모델을 제공합니다.

- 분산 - 정책 범위 내에 있는 각 계정 및 VPC에 대해 Firewall Manager는 네트워크 방화벽 방화벽을 만들고 VPC 서브넷에 방화벽 엔드포인트를 배포하여 네트워크 트래픽을 필터링합니다.
- 중앙 집중식 - Firewall Manager는 단일 Amazon VPC에 단일 네트워크 방화벽을 생성합니다.
- 기존 방화벽 가져오기 - Firewall Manager는 단일 Firewall Manager 정책으로 기존 방화벽을 가져와서 관리합니다. 정책에 따라 관리되는 가져온 방화벽에 추가 규칙을 적용하여 방화벽이 보안 표준을 충족하는지 확인할 수 있습니다.

> **Note**
>
> Firewall Manager 네트워크 방화벽 정책은 조직 전체의 VPC에 대한 네트워크 방화벽 보호를 관리하는 데 사용하는 Firewall Manager 정책입니다.
> 네트워크 방화벽 보호는 방화벽 정책이라고 하는 네트워크 방화벽 서비스의 리소스에 지정됩니다.

네트워크 방화벽 사용에 관한 자세한 내용은 AWS Network Firewall 개발자 안내서를 참조하세요.

다음 섹션에서는 Firewall Manager 네트워크 방화벽 정책을 사용하기 위한 요구 사항을 다루고 정책의 작동 방식을 설명합니다. 정책을 생성하는 절차는 에 대한 AWS Firewall Manager 정책 생성 AWS Network Firewall을 참조하세요.

리소스 공유를 활성화해야 합니다

네트워크 방화벽 정책은 조직 내 계정 전체에서 네트워크 방화벽 규칙 그룹을 공유합니다. 이 기능을 사용하려면 AWS Organizations에 대한 리소스 공유를 사용하도록 설정해야 합니다. 리소스 공유를 활성화하는 방법에 대한 자세한 내용은 네트워크 방화벽 및 DNS 방화벽 정책에 대한 리소스 공유을 참조하세요.

네트워크 방화벽 규칙 그룹을 정의해야 합니다.

새 Network Firewall 정책을 지정할 때는 방화벽 정책을 AWS Network Firewall 직접 사용할 때와 동일하게 방화벽 정책을 정의합니다. 추가할 상태 비저장 규칙 그룹, 기본 상태 비저장 작업 및 상태 저장 규칙 그룹을 지정합니다. 규칙 그룹을 정책에 포함하려면 Firewall Manager 관리자 계정에 규칙 그룹이 이미 있어야 합니다. 네트워크 방화벽 규칙 그룹을 만드는 방법에 대한 자세한 내용은 AWS Network Firewall 규칙 그룹을 참조하세요.

Firewall Manager가 방화벽 엔드포인트를 생성하는 방법

정책의 방화벽 관리 유형에 따라 Firewall Manager가 방화벽을 생성하는 방법이 결정됩니다. 정책에 따라 분산 방화벽, 중앙 집중식 방화벽을 만들거나 기존 방화벽을 가져올 수 있습니다.

- 분산 - 분산 배포 모델을 사용하면 Firewall Manager는 정책 범위 내에 있는 각 VPC에 대한 엔드포인트를 생성합니다. 방화벽 엔드포인트를 생성할 가용 영역을 지정하여 엔드포인트 위치를 사용자 지정하거나, Firewall Manager가 퍼블릭 서브넷이 있는 가용 영역에 엔드포인트를 자동으로 생성할 수 있습니다. 가용 영역을 수동으로 선택하는 경우 가용 영역당 허용된 CIDR 세트를 제한할 수 있습니다. Firewall Manager에서 엔드포인트를 자동으로 생성하도록 하려면 서비스가 VPC 내에 단일 엔드포인트를 생성할지 아니면 여러 방화벽 엔드포인트를 생성할지도 지정해야 합니다.
  - 방화벽 엔드포인트가 여러 개인 경우, Firewall Manager는 라우팅 테이블에 인터넷 게이트웨이 또는 Firewall Manager가 생성한 방화벽 엔드포인트 경로가 있는 서브넷을 포함하는 각 가용 영역에 방화벽 엔드포인트를 배포합니다. 네트워크 방화벽 정책의 기본 옵션입니다.
  - 단일 방화벽 엔드포인트의 경우 Firewall Manager는 인터넷 게이트웨이 경로가 있는 모든 서브넷의 단일 가용 영역에 방화벽 엔드포인트를 배포합니다. 이 옵션을 사용할 경우 다른 영역의 트래픽이 방화벽으로 필터링되려면 영역 경계를 넘어야 합니다.

    > **Note**
    >
    > 이 두 옵션 모두 IPv4/prefixlist 경로가 포함된 라우팅 테이블에 연결된 서브넷이 있어야 합니다. Firewall Manager는 다른 리소스를 확인하지 않습니다.

- 중앙 집중식 - 중앙 집중식 배포 모델을 사용하면 Firewall Manager는 검사 VPC 내에 하나 이상의 방화벽 엔드포인트를 생성합니다. 검사 VPC는 Firewall Manager가 엔드포인트를 시작하는 중앙 VPC입니다. 중앙 집중식 배포 모델을 사용할 때는 방화벽 엔드포인트를 생성할 가용 영역도 지정합니다. 정책을 생성한 후에는 검사 VPC를 변경할 수 없습니다. 다른 검사 VPC를 사용하려면 새 정책을 생성해야 합니다.
- 기존 방화벽 가져오기 - 기존 방화벽을 가져올 때는 정책에 하나 이상의 리소스 세트를 추가하여 정책에서 관리할 방화벽을 선택합니다. 리소스 세트는 조직의 계정으로 관리되는 리소스(이 경우 네트워크 방화벽의 기존 방화벽)의 모음입니다. 정책에서 리소스 세트를 사용하기 전에 먼저 리소스 세트를 생성해야 합니다. Firewall Manager 리소스 세트에 대한 자세한 내용은 Firewall Manager에서 리소스 세트 관련 작업를 참조하세요.

  가져온 방화벽으로 작업할 때는 다음 고려 사항에 유의하십시오.

  - 가져온 방화벽이 규정을 준수하지 않는 경우 Firewall Manager는 다음과 같은 경우를 제외하고 위반 사항을 자동으로 해결하려고 시도합니다.
    - Firewall Manager와 네트워크 방화벽 정책의 상태 저장 또는 상태 비저장 기본 동작이 일치하지 않는 경우

  - 가져온 방화벽의 방화벽 정책에 있는 규칙 그룹이 Firewall Manager 정책의 규칙 그룹과 동일한 우선 순위를 갖는 경우
  - 가져온 방화벽이 정책의 리소스 세트에 속하지 않는 방화벽과 연결된 방화벽 정책을 사용하는 경우. 방화벽에는 정확히 하나의 방화벽 정책이 있을 수 있지만 단일 방화벽 정책이 여러 방화벽에 연결될 수 있기 때문에 이런 일이 발생할 수 있습니다.
  - 가져온 방화벽의 방화벽 정책에 속하며 Firewall Manager 정책에도 지정된 기존 규칙 그룹에 다른 우선 순위가 부여되는 경우
- 정책에서 리소스 정리를 활성화하면 Firewall Manager는 리소스 세트 범위 내의 방화벽에서 FMS 가져오기 정책에 포함된 규칙 그룹을 제거합니다.
- Firewall Manager에서 관리하는 방화벽 가져오기 기존 방화벽 관리 유형은 한 번에 하나의 정책으로만 관리할 수 있습니다. 여러 개의 네트워크 방화벽 가져오기 정책에 동일한 리소스 세트를 추가하면 리소스 세트에 추가된 첫 번째 정책에서 리소스 세트의 방화벽을 관리하고 두 번째 정책에서는 무시합니다.
- Firewall Manager는 현재 예외 정책 구성을 스트리밍하지 않습니다. 스트림 예외 정책에 대한 자세한 내용은 AWS Network Firewall 개발자 안내서의 스트림 예외 정책을 참조하세요.

분산 또는 중앙 집중식 방화벽 관리를 사용하여 정책의 가용 영역 목록을 변경하는 경우 Firewall Manager는 과거에 생성되었지만 현재 정책 범위에 포함되지 않은 엔드포인트를 정리하려고 시도합니다. Firewall Manager는 범위를 벗어난 엔드포인트를 참조하는 라우팅 테이블 경로가 없는 경우에만 엔드포인트를 제거합니다. Firewall Manager는 이러한 엔드포인트를 삭제할 수 없는 것으로 확인되면 방화벽 서브넷을 비준수로 표시하고 삭제해도 안전할 때까지 엔드포인트 제거를 계속 시도합니다.

Firewall Manager가 방화벽 서브넷을 관리하는 방법

방화벽 서브넷은 Firewall Manager가 네트워크 트래픽을 필터링하는 방화벽 엔드포인트에 대해 생성하는 VPC 서브넷입니다. 각 방화벽 엔드포인트는 전용 VPC 서브넷에 배포되어야 합니다. Firewall Manager는 정책 범위 내에 있는 각 VPC에 방화벽 서브넷을 하나 이상 생성합니다.

자동 엔드포인트 구성과 함께 분산 배포 모델을 사용하는 정책의 경우 Firewall Manager는 인터넷 게이트웨이 경로가 있는 서브넷 또는 Firewall Manager가 정책용으로 만든 방화벽 엔드포인트로 연결되는 경로가 있는 서브넷이 있는 가용 영역에만 방화벽 서브넷을 생성합니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC 및 서브넷을 참조하세요.

Firewall Manager가 방화벽 엔드포인트를 생성할 가용 영역을 지정하는 분산 또는 중앙 집중식 모델을 사용하는 정책의 경우, Firewall Manager는 가용 영역에 다른 리소스가 있는지 여부에 관계없이 특정 가용 영역에 엔드포인트를 생성합니다.

네트워크 방화벽 정책을 처음 정의할 때는 Firewall Manager가 범위 내에 있는 각 VPC의 방화벽 서브넷을 관리하는 방법을 지정합니다. 나중에 이 선택 항목을 변경할 수 없습니다.

자동 엔드포인트 구성과 함께 분산 배포 모델을 사용하는 정책의 경우 다음 옵션 중에서 선택할 수 있습니다.

- 퍼블릭 서브넷이 있는 모든 가용 영역에 방화벽 서브넷을 배포합니다. 이는 기본 설정 동작입니다. 이는 트래픽 필터링 보호의 고가용성을 제공합니다.
- 1개의 가용 영역에 단일 방화벽 서브넷을 배포합니다. 이 옵션을 선택하면 Firewall Manager는 VPC에서 퍼블릭 서브넷이 가장 많은 영역을 식별하고 해당 영역에 방화벽 서브넷을 생성합니다. 단일 방화벽 엔드포인트는 VPC의 모든 네트워크 트래픽을 필터링합니다. 이렇게 하면 방화벽 비용을 줄일 수 있지만 가용성이 높지는 않으며 필터링하려면 다른 영역의 트래픽이 영역 경계를 넘어야 합니다.

사용자 지정 엔드포인트가 구성된 분산 배포 모델 또는 중앙 집중식 배포 모델을 사용하는 정책의 경우 Firewall Manager는 정책 범위 내에 있는 지정된 가용 영역에 서브넷을 생성합니다.

Firewall Manager가 방화벽 서브넷에 사용할 VPC CIDR 블록을 제공하거나 방화벽 엔드포인트 주소의 선택은 Firewall Manager가 결정하도록 맡길 수 있습니다.

- CIDR 블록을 제공하지 않는 경우 Firewall Manager는 VPC를 쿼리하여 사용할 수 있는 IP 주소를 찾습니다.
- CIDR 블록 목록을 제공하는 경우 Firewall Manager는 사용자가 제공하는 CIDR 블록에서만 새 서브넷을 검색합니다. /28 CIDR 블록을 사용해야 합니다. Firewall Manager가 생성하는 각 방화벽 서브넷에 대해 CIDR 블록 목록을 검토하여 가용 영역 및 VPC에 적용되고 사용 가능한 주소가 있는 첫 번째 방화벽 서브넷을 사용합니다. Firewall Manager가 VPC에서 빈 공간을 찾을 수 없는 경우(제한이 있든 없든), 해당 서비스는 VPC에 방화벽을 만들지 않습니다.

Firewall Manager가 가용 영역에 필수 방화벽 서브넷을 만들 수 없는 경우 해당 서브넷을 정책을 준수하지 않는 것으로 표시합니다. 영역이 이 상태에 있는 동안 다른 영역의 엔드포인트에 의해 필터링되려면 해당 영역의 트래픽이 영역 경계를 넘어야 합니다. 이는 단일 방화벽 서브넷 시나리오와 유사합니다.

Firewall Manager가 네트워크 방화벽 리소스를 관리하는 방법

Firewall Manager에서 정책을 정의할 때는 표준 AWS Network Firewall 방화벽 정책의 네트워크 트래픽 필터링 동작을 제공합니다. 상태 비저장 및 상태 저장 네트워크 방화벽 규칙 그룹을 추가하고 상태 비저장 규칙과 일치하지 않는 패킷에 대한 기본 동작을 지정합니다. 에서 AWS Network Firewall방화벽 정책을 사용하는 방법에 대한 자세한 내용은 AWS Network Firewall 방화벽 정책을 참조하십시오.

분산 및 중앙 집중식 정책의 경우 네트워크 방화벽 정책을 저장하면 Firewall Manager는 정책 범위 내에 있는 각 VPC에 방화벽 및 방화벽 정책을 생성합니다. Firewall Manager는 다음 값을 연결하여 이러한 네트워크 방화벽 리소스의 이름을 지정합니다.

- 리소스 유형에 따라 고정 문자열(`FMManagedNetworkFirewall`또는`FMManagedNetworkFirewallPolicy`)이 달라집니다.
- Firewall Manager 정책 이름입니다. 정책을 생성할 때 할당하는 이름입니다.
- Firewall Manager 정책 이름. 방화벽 관리자 정책의 AWS 리소스 ID입니다.
- Amazon VPC ID입니다. Firewall Manager가 방화벽 및 방화벽 정책을 생성하는 VPC의 AWS 리소스 ID입니다.

다음은 Firewall Manager에서 관리하는 방화벽의 이름 예시입니다.

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

다음은 방화벽 정책 이름의 예입니다.

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

정책을 만든 후에는 VPC의 구성원 계정이 방화벽 정책 설정이나 규칙 그룹을 재정의할 수 없지만 Firewall Manager가 생성한 방화벽 정책에 규칙 그룹을 추가할 수는 있습니다.

Firewall Manager가 정책에 대한 VPC 라우팅 테이블을 관리하고 모니터링하는 방법

> **Note**
>
> 중앙 집중식 배포 모델을 사용하는 정책에는 현재 라우팅 테이블 관리가 지원되지 않습니다.

Firewall Manager는 방화벽 엔드포인트를 생성할 때 해당 엔드포인트에 대한 VPC 라우팅 테이블도 생성합니다. 하지만 Firewall Manager는 VPC 라우팅 테이블을 관리하지 않습니다. 네트워크 트래픽이 Firewall Manager에서 생성한 방화벽 엔드포인트로 전달되도록 VPC 라우팅 테이블을 구성해야 합니다. Amazon VPC 수신 라우팅 개선 기능을 사용하여 새 방화벽 엔드포인트를 통해 트래픽을 라우팅하도록 라우팅 테이블을 변경하십시오. 변경 시 보호하려는 서브넷과 외부 위치 사이에 방화벽 엔드포인트를 삽입해야 합니다. 필요로 하는 정확한 라우팅은 아키텍처와 해당 구성 요소에 따라 다릅니다.

현재 Firewall Manager를 사용하면 인터넷 게이트웨이로 향하는 모든 트래픽, 즉 방화벽을 우회하는 트래픽에 대한 VPC 라우팅 테이블 경로를 모니터링할 수 있습니다. Firewall Manager는 NAT 게이트웨이와 같은 다른 대상 게이트웨이를 지원하지 않습니다.

VPC의 라우팅 테이블 관리에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 VPC의 라우팅 테이블 관리를 참조하세요. 네트워크 방화벽의 라우팅 테이블 관리에 대한 자세한 내용은 AWS Network Firewall 개발자 안내서의 AWS Network Firewall에 대한 라우팅 테이블 구성을 참조하세요.

정책에 대한 모니터링을 활성화하면 Firewall Manager는 VPC 경로 구성을 지속적으로 모니터링하고 해당 VPC에 대한 방화벽 검사를 우회하는 트래픽에 대해 경고합니다. 서브넷에 방화벽 엔드포인트 경로가 있는 경우 Firewall Manager는 다음 경로를 찾습니다.

- 네트워크 방화벽 엔드포인트로 트래픽을 보내기 위한 경로입니다.
- 네트워크 방화벽 엔드포인트에서 인터넷 게이트웨이로 트래픽을 전달하는 경로입니다.
- 인터넷 게이트웨이에서 네트워크 방화벽 엔드포인트까지의 인바운드 경로입니다.
- 방화벽 서브넷의 경로.

서브넷에 네트워크 방화벽 경로가 있지만 네트워크 방화벽 및 인터넷 게이트웨이 라우팅 테이블에 비대칭 라우팅이 있는 경우 Firewall Manager는 해당 서브넷을 규정을 준수하지 않는 것으로 보고합니다. 또한 Firewall Manager는 Firewall Manager가 생성한 방화벽 라우팅 테이블과 서브넷의 라우팅 테이블에서 인터넷 게이트웨이로 가는 경로를 탐지하여 이를 비준수로 보고합니다. 네트워크 방화벽 서브넷 라우팅 테이블 및 인터넷 게이트웨이 라우팅 테이블의 추가 경로도 규정을 준수하지 않는 것으로 보고됩니다. Firewall Manager는 위반 유형에 따라 경로 구성을 준수하기 위한 수정 조치를 제안합니다. Firewall Manager는 모든 경우에 제안 사항을 제공하지는 않습니다. 예를 들어 고객 서브넷에 Firewall Manager 외부에서 생성된 방화벽 엔드포인트가 있는 경우 Firewall Manager는 수정 조치를 제안하지 않습니다.

기본적으로 Firewall Manager는 검사 대상 가용 영역 경계를 넘는 모든 트래픽을 비준수로 표시합니다. 하지만 VPC에 단일 엔드포인트를 자동으로 생성하도록 선택한 경우, Firewall Manager는 가용 영역 경계를 넘는 트래픽을 규정 비준수로 표시하지 않습니다.

사용자 지정 엔드포인트 구성과 함께 분산 배포 모델을 사용하는 정책의 경우 방화벽 엔드포인트가 없는 가용 영역에서 가용 영역 경계를 넘는 트래픽을 규정 준수로 표시할지 비준수로 표시할지 선택할 수 있습니다.

> **Note**
>
> - Firewall Manager는 IPv6 및 접두사 목록 경로와 같은 비 IPv4 경로에 대한 수정 조치를 제안하지 않습니다.
> - `DisassociateRouteTable` API 호출을 사용하여 이루어진 호출을 감지하는 데 최대 12시간이 걸릴 수 있습니다.
> - Firewall Manager는 방화벽 엔드포인트가 포함된 서브넷에 대해 네트워크 방화벽 라우팅 테이블을 생성합니다. Firewall Manager는 이 라우팅 테이블에 유효한 인터넷 게이트웨이와 VPC 기본 경로만 포함되어 있다고 가정합니다. 이 라우팅 테이블의 추가 경로나 유효하지 않은 경로는 규정을 준수하지 않는 것으로 간주됩니다.

Firewall Manager 정책을 구성할 때 모니터링 모드를 선택하면 Firewall Manager는 리소스 위반 및 리소스에 대한 수정 세부 정보를 제공합니다. 이렇게 제안된 수정 조치를 사용하여 라우팅 테이블의 경로 문제를 해결할 수 있습니다. 끄기 모드를 선택하면 Firewall Manager가 라우팅 테이블 콘텐츠를 모니터링하지 않습니다. 이 옵션을 사용하면 VPC 라우팅 테이블을 직접 관리할 수 있습니다. 이러한 리소스 위반에 대한 자세한 내용은 AWS Firewall Manager 정책에 대한 규정 준수 정보 보기을 참조하세요.

> **Warning**
>
> 정책을 생성할 때 AWS Network Firewall 경로 구성에서 Monitor를 선택하면 해당 정책에 대해 Monitor를 끌 수 없습니다. 하지만 끄기를 선택하면 나중에 활성화할 수 있습니다.

AWS Network Firewall 정책에 대한 로깅 구성

Network 방화벽 정책에 대한 중앙 집중식 로깅을 활성화하여 조직 내 트래픽에 대한 세부 정보를 얻을 수 있습니다. 흐름 로깅을 선택하여 네트워크 트래픽 흐름을 캡처하거나, 경고 로깅을 선택하여 규칙 동작이 `DROP` 또는 `ALERT`로 설정된 규칙과 일치하는 트래픽을 보고할 수 있습니다. AWS Network Firewall 로깅에 대한 자세한 내용은 AWS Network Firewall개발자 안내서AWS Network Firewall 의 에서 로깅 네트워크 트래픽 로깅 을 참조하세요.

정책의 네트워크 방화벽 방화벽에서 Amazon S3 버킷으로 로그를 전송합니다. 로깅을 활성화하면 예약된 AWS Firewall Manager 접두사 () 를 사용하여 선택한 Amazon S3 버킷에 로그를 전송하도록 방화벽 설정을 업데이트하여 구성된 각 Network Firewall에 대한 로그를 전송합니다. AWS Network Firewall `<policy-name>-<policy-id>`

> **Note**
>
> Firewall Manager는 이 접두사를 사용하여 Firewall Manager에서 로깅 구성을 추가했는지 아니면 계정 소유자가 추가했는지 여부를 결정합니다. 계정 소유자가 자신의 사용자 지정 로깅에 예약된 접두사를 사용하려고 하면 Firewall Manager 정책의 로깅 구성이 해당 접두사를 덮어씁니다.

Amazon S3 버킷을 생성하고 저장된 로그를 검토하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3이란 무엇인가요?를 참조하세요.

로깅을 활성화하려면 다음 요구 사항을 충족해야 합니다.

- Firewall Manager 정책에 지정된 Amazon S3가 존재해야 합니다.
- 이 경우 다음 권한이 있어야 합니다.
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- 로깅 대상인 Amazon S3 버킷이 키가 저장된 서버 측 암호화를 사용하는 경우 AWS Key Management Service, AWS KMS 고객 관리 키에 다음 정책을 추가하여 Firewall Manager가 Logs 로그 그룹에 기록할 수 CloudWatch 있도록 해야 합니다.

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

단, Firewall Manager 관리자 계정의 버킷만 AWS Network Firewall 중앙 로깅에 사용할 수 있습니다.

네트워크 방화벽 정책에서 중앙 집중식 로깅을 활성화하면 Firewall Manager는 사용자 계정에서 다음과 같은 작업을 수행합니다.

- Firewall Manager는 선택한 S3 버킷에 대한 권한을 업데이트하여 로그 전송을 허용합니다.
- Firewall Manager는 정책 범위 내의 각 구성원 계정에 대해 S3 버킷에 디렉토리를 생성합니다. 각 계정의 로그는 `<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`에서 찾을 수 있습니다.

네트워크 방화벽 정책에 대한 로깅을 활성화하려면

1. Firewall Manager 관리자 계정을 사용하여 Amazon S3 버킷을 생성합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 버킷 생성을 참조하세요.
2. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

3. 탐색 창에서 보안 정책을 선택합니다.
4. 로깅을 활성화하려는 네트워크 방화벽 정책을 선택합니다. AWS Network Firewall 로깅에 대한 자세한 내용은 AWS Network Firewall 개발자 안내서의 네트워크 트래픽 로깅을 참조하십시오. AWS Network Firewall
5. 정책 규칙 섹션의 정책 세부 정보 탭에서 편집을 선택합니다.
6. 로그를 활성화하고 집계하려면 로깅 구성에서 하나 이상의 옵션을 선택합니다.
   - 흐름 로그 활성화 및 집계
   - 알림 로그 활성화 및 집계
7. 로그를 전송할 Amazon S3 버킷을 선택합니다. 활성화한 각 로그 유형에 맞는 버킷을 선택해야 합니다. 두 로그 유형에 동일한 버킷을 사용할 수 있습니다.
8. (선택 사항) 사용자 지정 구성원 계정 생성 로깅을 정책의 로깅 구성으로 대체하려면 기존 로깅 구성 재정의를 선택합니다.

9. 다음을 선택합니다.
10. 설정을 검토한 다음 저장을 선택하여 변경 내용을 정책에 저장합니다.

Network 방화벽 정책에 대한 로깅을 비활성화하려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 로깅을 비활성화하려는 Network 방화벽 정책을 선택합니다.
4. 정책 규칙 섹션의 정책 세부 정보 탭에서 편집을 선택합니다.
5. 로깅 구성 상태에서 흐름 로그 활성화 및 집계와 알림 로그 활성화 및 집계가 선택되어 있는 경우 이를 선택 취소합니다.
6. 다음을 선택합니다.
7. 설정을 검토한 다음 저장을 선택하여 변경 내용을 정책에 저장합니다.

Amazon Route 53 Resolver DNS 방화벽 정책

AWS Firewall Manager DNS 방화벽 정책을 사용하여 조직 전체의 Amazon Route 53 Resolver DNS 방화벽 규칙 그룹과 Amazon Virtual Private Cloud VPC 간의 연결을 관리할 수 있습니다. AWS Organizations중앙에서 제어하는 규칙 그룹을 전체 조직 또는 선택한 계정 및 VPC 하위 집합에 적용할 수 있습니다.

DNS Firewall은 VPC의 아웃바운드 DNS 트래픽에 대한 필터링 및 규제를 제공합니다. DNS Firewall 규칙 그룹에 재사용 가능한 필터링 규칙 컬렉션을 생성하고 규칙 그룹을 VPC에 연결합니다. Firewall Manager 정책을 적용하면 정책 범위 내에 있는 각 계정 및 VPC에 대해 Firewall Manager는 Firewall Manager 정책에 지정된 연결 우선 순위 설정을 사용하여 정책의 각 DNS Firewall 규칙 그룹과 정책 범위 내에 있는 각 VPC 간의 연결을 생성합니다.

DNS 방화벽 사용에 대한 자세한 설명은 Amazon Route 53 개발자 가이드의 Amazon Route 53 Resolver DNS 방화벽을 참조하세요.

다음 섹션에서는 Firewall Manager DNS 방화벽 정책을 사용하기 위한 요구 사항을 다루고 정책의 작동 방식을 설명합니다. 정책을 생성하는 절차는 Amazon Route 53 리졸버 DNS 방화벽에 대한 AWS Firewall Manager 정책 생성을 참조하세요.

리소스 공유를 활성화해야 합니다

DNS 방화벽 정책은 조직 내 계정 전체에서 DNS 방화벽 규칙 그룹을 공유합니다. 이 기능을 사용하려면 를 사용하여 리소스 공유를 활성화해야 합니다. AWS Organizations리소스 공유를 활성화하는 방법에 대한 자세한 내용은 네트워크 방화벽 및 DNS 방화벽 정책에 대한 리소스 공유을 참조하세요.

DNS 방화벽 규칙 그룹을 정의해야 합니다

새 DNS 방화벽 정책을 지정할 때는 Amazon Route 53 Resolver DNS Firewall을 직접 사용할 때와 동일하게 규칙 그룹을 정의합니다. 규칙 그룹을 정책에 포함하려면 Firewall Manager 관리자 계정에 규칙 그룹이 이미 있어야 합니다. DNS 방화벽 규칙 그룹 생성에 대한 자세한 내용은 DNS 방화벽 규칙 그룹 및 규칙을 참조하세요.

가장 낮은 우선순위와 가장 높은 우선순위의 규칙 그룹 연결을 정의합니다

Firewall Manager DNS 방화벽 정책을 통해 관리하는 DNS Firewall 규칙 그룹 연결에는 VPC에 대한 가장 낮은 우선 순위의 연결과 가장 높은 우선 순위의 연결이 포함됩니다. 정책 구성에서 이들은 첫 번째 및 마지막 규칙 그룹으로 나타납니다.

DNS Firewall은 VPC의 DNS 트래픽을 다음 순서로 필터링합니다.

1. Firewall Manager DNS 방화벽 정책에 사용자가 정의한 첫 번째 규칙 그룹입니다. 유효한 값은 1~99입니다.
2. 개별 계정 관리자가 DNS Firewall을 통해 연결하는 DNS Firewall 규칙 그룹입니다.
3. Firewall Manager DNS 방화벽 정책에 사용자가 정의한 마지막 규칙 그룹입니다. 유효한 값은 9,901에서 10,000까지입니다.

규칙 그룹 삭제

Firewall Manager DNS 방화벽 정책에서 규칙 그룹을 삭제하려면 다음 단계를 수행해야 합니다.

1. Firewall Manager DNS 방화벽 정책에서 해당 규칙 그룹을 제거합니다.

2. 에서 규칙 그룹 공유를 취소하십시오. AWS Resource Access Manager소유하고 있는 규칙 그룹을 공유 해제하려면 리소스 공유에서 제거해야 합니다. AWS RAM 콘솔이나 AWS CLI를 사용하여 이 작업을 수행할 수 있습니다. 리소스 공유 해제에 대한 자세한 내용은 AWS RAM 사용 설명서의 AWS RAM리소스 공유 업데이트를 참조하세요.
3. DNS 방화벽 콘솔 또는 AWS CLI를 사용하여 규칙 그룹을 삭제합니다.

Firewall Manager가 생성한 규칙 그룹 연결의 이름을 지정하는 방법

DNS 방화벽 정책을 저장할 때 자동 수정을 활성화한 경우 Firewall Manager는 정책에 제공한 규칙 그룹과 정책 범위 내에 있는 VPC 간에 DNS Firewall 연결을 생성합니다. Firewall Manager는 다음 값을 연결하여 이러한 연결의 이름을 지정합니다.

- 고정 문자열 `FMManaged_`
- Firewall Manager 정책 이름. 방화벽 관리자 정책의 AWS 리소스 ID입니다.

다음은 Firewall Manager에서 관리하는 방화벽의 이름 예시입니다.

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

정책을 생성한 후 VPC의 계정 소유자가 방화벽 정책 설정이나 규칙 그룹 연결을 재정의하는 경우 Firewall Manager는 정책을 비준수로 표시하고 해결 조치를 제안하려고 합니다. 계정 소유자는 다른 DNS Firewall 규칙 그룹을 DNS 방화벽 정책 범위에 속하는 VPC에 연결할 수 있습니다. 개별 계정 소유자가 생성하는 모든 연결에는 첫 번째 규칙 그룹 연결과 마지막 규칙 그룹 연결 간의 우선 순위 설정이 있어야 합니다.

Palo Alto Networks Cloud NGFW 정책

팔로알토 네트웍스 클라우드 차세대 방화벽 (NGFW) 은 정책에 사용할 수 있는 타사 방화벽 서비스입니다. AWS Firewall Manager Firewall Manager용 팔로알토 네트웍스 클라우드 NGFW를 사용하면 모든 계정에서 팔로알토 네트웍스 클라우드 NGFW 리소스 및 룰스택을 생성하고 중앙에서 배포할 수 있습니다. AWS

Firewall Manager와 함께 팔로 알토 네트웍스 클라우드 NGFW를 사용하려면 먼저 마켓플레이스의 팔로알토 네트웍스 클라우드 NGFW 종량제 서비스에 가입해야 합니다. AWS 구독 후에는 Palo Alto Networks Cloud NGFW 서비스에서 일련의 단계를 수행하여 계정 및 Cloud NGFW 설정을 구성합니다. 그런 다음 Firewall Manager Cloud FMS 정책을 생성하여 조직의 모든 계정에 걸쳐 팔로알토 네트웍스 클라우드 NGFW 리소스 및 규칙을 중앙에서 배포하고 관리합니다. AWS

Firewall Manager 정책을 생성하는 절차는 팔로알토 네트웍스 클라우드 NGFW에 대한 AWS Firewall Manager 정책 생성을 참조하세요. Firewall Manager에 대한 Palo Alto Networks Cloud NGFW를 구성하고 관리하는 방법에 대한 자세한 내용은 AWS설명서에서 Palo Alto Networks Palo Alto Networks Cloud NGFW를 참조하세요.

서비스 정책형 Fortigate Cloud Native Firewall(CNF)

서비스형 Fortigate 클라우드 네이티브 방화벽 (CNF) 은 정책에 사용할 수 있는 타사 방화벽 서비스입니다. AWS Firewall Manager Fortigate CNF는 클라우드 네트워크를 보호하고 보안 정책을 쉽게 관리할 수 있게 해주는 차세대 방화벽 서비스입니다. Fortigate CNF for Firewall Manager를 사용하면 모든 계정에 Fortigate CNF 리소스 및 정책 세트를 생성하고 중앙에서 배포할 수 있습니다. AWS

Fortigate CNF를 Firewall Manager와 함께 사용하려면 먼저 마켓플레이스에서 서비스형 Fortigate 클라우드 네이티브 방화벽 (CNF) 을 구독해야 합니다. AWS 구독 후에는 Fortigate CNF 서비스에서 일련의 단계를 수행하여 글로벌 정책 세트 및 기타 설정을 구성합니다. 그런 다음 Firewall Manager 정책을 생성하여 조직의 모든 계정에서 Fortigate CNF 리소스를 중앙에서 배포하고 관리합니다. AWS

Fortigate CNF Firewall Manager 정책을 생성하는 절차는 서비스형 Fortigate 클라우드 네이티브 방화벽 (CNF) AWS Firewall Manager 정책 생성을 참조하세요. Firewall Manager와 함께 사용하도록 Fortigate CNF를 구성 및 관리하는 방법에 대한 자세한 내용은 Fortinet CNF 설명서를 참조하세요.

네트워크 방화벽 및 DNS 방화벽 정책에 대한 리소스 공유

Firewall Manager 네트워크 방화벽 및 DNS 방화벽 정책을 관리하려면 in을 사용하여 리소스 AWS Organizations 공유를 활성화해야 합니다 AWS Resource Access Manager. 이렇게 하면 Firewall Manager에서 이러한 정책 유형을 생성할 때 계정 전체에 보호 기능을 배포할 수 있습니다.

리소스 공유를 활성화하려면 AWS Resource Access Manager 사용 설명서의 AWS Organizations공유 활성화의 지침을 따르십시오.

리소스 공유 관련 문제

를 사용하여 사용하도록 설정하거나 이를 필요로 AWS RAM 하는 Firewall Manager 정책을 사용할 때 리소스 공유에 문제가 발생할 수 있습니다.

이러한 문제의 예는 다음과 같습니다.

- 지침에 따라 공유를 활성화하면 AWS RAM 콘솔에서 공유 활성화 옵션이 회색으로 표시되며 선택할 수 없습니다. AWS Organizations

- Firewall Manager에서 리소스 공유가 필요한 정책을 적용하면 정책이 비준수로 표시되고 리소스 공유 또는 AWS RAM 이 활성화되지 않았음을 나타내는 메시지가 표시됩니다.

리소스 공유에 문제가 발생하는 경우 다음 절차에 따라 활성화해 보십시오.

리소스 공유 활성화 재시도

- 다음 옵션 중 하나를 사용하여 공유를 다시 활성화합니다.
  - (옵션) AWS RAM 콘솔을 사용하여 사용 AWS Resource Access Manager 설명서의 공유 AWS Organizations활성화에 있는 지침을 따르십시오.
  - (옵션) AWS RAM API를 사용하여 `EnableSharingWithAwsOrganization` 호출합니다. 의 설명서를 참조하십시오 EnableSharingWithAwsOrganization.

Firewall Manager에서 리소스 세트 관련 작업

AWS Firewall Manager 리소스 세트는 방화벽과 같이 Firewall Manager 정책에서 그룹화하고 관리할 수 있는 리소스 모음입니다. 리소스 세트를 사용하면 조직 구성원이 정책에서 관리할 리소스를 세밀하게 제어할 수 있습니다. 리소스 세트를 사용하려면 콘솔에서 또는 PutResourceSetAPI를 사용하여 리소스 세트를 만든 다음 Firewall Manager 정책에 리소스 세트를 추가합니다.

다음 리소스 및 보안 정책 유형에 대한 리소스 세트를 생성하고 관리할 수 있습니다.

리소스 유형	Firewall Manager 보안 정책 유형
AWS Network Firewall - 방화벽	Network Firewall 정책 - 리소스 세트를 사용하여 Network Firewall의 기존 방화벽을 가져옵니다. Network Firewall 정책에서 리소스 세트를 사용하는 방법에 대한 자세한 내용은 에 대한 AWS Firewall Manager 정책 생성 AWS Network Firewall 절차의 기존 방화벽 가져오기 단계를 참조하세요.

다음 섹션에서는 리소스 세트를 만들고 삭제하기 위한 요건을 다룹니다.

주제

- Firewall Manager에서 리소스 세트 관련 작업을 할 때의 고려 사항
- 리소스 세트 생성
- 리소스 세트 삭제

Firewall Manager에서 리소스 세트 관련 작업을 할 때의 고려 사항

리소스 세트를 사용한 작업 시 다음 고려 사항에 유의하세요.

존재하지 않는 리소스에 대한 참조

리소스 세트에 리소스를 추가하는 경우 Amazon 리소스 이름(ARN)을 사용하여 리소스에 대한 참조를 생성합니다. Firewall Manager는 Amazon 리소스 이름(ARN)이 올바른 형식인지 확인하지만 Firewall Manager는 참조된 리소스의 존재 여부는 확인하지 않습니다. 리소스가 존재하지 않는데도 불구하고 ARN 검증을 통과하는 경우, Firewall Manager는 리소스 세트에 리소스 참조를 포함합니다. 나중에 같

은 ARN을 포함한 새 리소스가 생성되면 Firewall Manager는 리소스 세트의 연결된 정책에 있는 규칙 그룹을 새 리소스에 적용합니다.

삭제된 리소스

리소스 세트의 리소스를 삭제해도 해당 리소스에 대한 참조는 Firewall Manager 관리자가 해당 내용을 제거할 때까지 리소스 세트에 남아 있습니다.

조직을 떠나는 구성원 계정이 소유한 리소스 AWS Organizations

구성원이 조직을 떠나는 경우, 해당 구성원 계정이 소유한 리소스에 대한 모든 참조는 리소스 세트에 남아 있지만 더 이상 리소스 세트와 연결된 정책을 통해 관리되지 않습니다.

여러 정책에 대한 연결

리소스 세트를 여러 정책에 연결할 수 있지만 모든 정책 유형이 동일한 리소스를 관리하는 여러 정책을 지원하는 것은 아닙니다. 지원되지 않는 시나리오에 대한 자세한 내용은 특정 정책 유형에 대한 설명서를 참조하세요.

리소스 세트 생성

리소스 세트를 생성하려면(콘솔)

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 리소스 세트를 선택합니다.
3. 리소스 세트 생성을 선택합니다.
4. 리소스 세트 이름에 설명이 포함된 이름을 입력합니다.
5. (선택 사항) 리소스 세트에 대한 설명을 입력합니다.
6. 다음을 선택합니다.
7. 리소스 선택의 경우, AWS 계정 ID를 선택한 다음 리소스 선택을 선택하여 이 계정이 소유하고 관리하는 리소스를 리소스 세트에 추가합니다. 리소스를 선택한 후, 추가를 선택하여 리소스를 리소스 세트에 추가합니다.

8. 다음을 선택합니다.
9. 리소스 세트 태그의 경우, 리소스 세트에 사용할 식별 태그를 모두 추가합니다. 태그에 대한 자세한 내용은 Tag Editor 작업을 참조하세요.
10. 다음을 선택합니다.
11. 새 리소스 세트를 검토합니다. 변경하려면 변경할 영역에서 편집을 선택합니다. 그러면 생성 마법사의 해당 단계로 돌아갑니다. 리소스 세트에 만족하면, 리소스 세트 생성을 선택합니다.

리소스 세트 삭제

리소스 세트를 삭제하려면, 먼저 해당 리소스 세트를 사용하는 모든 정책으로부터 리소스 세트의 연결을 해제해야 합니다. 콘솔이나 PutPolicyAPI를 사용하여 정책 세부 정보 페이지에서 자원 그룹을 분리할 수 있습니다.

리소스 세트를 삭제하려면(콘솔)

1. 탐색 창에서 리소스 세트를 선택합니다.
2. 삭제하려는 리소스 세트 옆에 있는 옵션을 선택합니다.
3. 삭제를 선택합니다.

AWS Firewall Manager 정책에 대한 규정 준수 정보 보기

이 섹션에서는 AWS Firewall Manager 정책 범위에 속하는 계정 및 리소스의 규정 준수 상태를 확인하기 위한 지침을 제공합니다. 클라우드의 보안 및 규정 준수를 유지하기 AWS 위해 마련된 제어에 대한 자세한 내용은 을 참조하십시오Firewall Manager에 대한 규정 준수 확인.

> **Note**
>
> Firewall Manager에서 정책 준수를 모니터링하려면 보호된 리소스의 구성 변경 사항을 지속적으로 AWS Config 기록해야 합니다. AWS Config 구성에서는 녹화 빈도를 기본 설정인 연속으로 설정해야 합니다.

> **Note**
>
> 보호된 리소스에서 적절한 규정 준수 상태를 유지하려면 Firewall Manager 보호 상태를 자동 또는 수동으로 반복적으로 변경하지 마십시오. Firewall Manager는 의 AWS Config 정보를 사

용하여 리소스 구성의 변경 사항을 탐지합니다. 변경 사항이 충분히 빨리 적용되면 일부 변경 내용을 추적하지 못할 AWS Config 수 있으며, 이로 인해 Firewall Manager의 규정 준수 또는 수정 상태에 대한 정보가 손실될 수 있습니다.
Firewall Manager로 보호하고 있는 리소스의 규정 준수 또는 수정 상태가 잘못된 경우 먼저 Firewall Manager 보호를 변경하거나 재설정하는 프로세스를 실행하고 있지 않은지 확인한 다음 에서 관련 구성 규칙을 재평가하여 리소스에 대한 AWS Config 추적을 새로 고치십시오. AWS Config

모든 AWS Firewall Manager 정책에 대해 정책 범위에 속하는 계정 및 리소스의 규정 준수 상태를 볼 수 있습니다. 정책의 설정이 계정이나 자원의 설정에 반영되는 경우, 계정 또는 자원은 Firewall Manager 정책을 준수합니다. 각 정책 유형에는 고유한 규정 준수 요구 사항이 있으며, 사용자는 정책을 정의할 때 이러한 내용을 조정할 수 있습니다. 일부 정책의 경우, 범위 내 리소스에 대한 자세한 위반 정보를 볼 수도 있으므로 보안 위험을 더 잘 이해하고 관리하는 데 도움이 됩니다.

정책에 대한 규정 준수 정보를 보려면

1. Firewall Manager 관리자 계정을 AWS Management Console 사용하여 로그인한 다음 에서 Firewall Manager 콘솔을 엽니다https://console.aws.amazon.com/wafv2/fmsv2. Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

   > **Note**
   >
   > Firewall Manager 관리자 계정 설정에 대한 자세한 내용은 AWS Firewall Manager 전제 조건을 참조하세요.

2. 탐색 창에서 보안 정책을 선택합니다.
3. 정책을 선택합니다. 정책 페이지의 계정 및 리소스 탭에서 Firewall Manager는 조직의 계정을 정책 범위 내에 있는 계정과 범위 밖에 있는 계정별로 그룹화하여 나열합니다.

   정책 범위 내 계정 창에는 각 계정의 규정 준수 상태가 나열됩니다. 규정 준수 상태는 계정의 범위 내 리소스 모두에 정책이 성공적으로 적용되었음을 나타냅니다. 비준수 상태는 정책이 계정의 범위 내 리소스 중 하나 이상에 적용되지 않았음을 나타냅니다.
4. 규정을 준수하지 않는 계정을 선택하십시오. 계정 페이지에서 Firewall Manager는 각 비준수 리소스의 ID 및 유형과 해당 리소스가 정책을 위반하는 이유를 나열합니다.

> **Note**
>
> 리소스 유형 `AWS::EC2::NetworkInterface`(ENI) 및 `AWS::EC2::Instance`의 경우 Firewall Manager에 제한된 수의 비준수 리소스가 표시될 수 있습니다. 규정을 준수하지 않는 리소스를 추가로 나열하려면 계정에 대해 처음에 표시되는 리소스를 수정하십시오.

5. Firewall Manager 정책 유형이 콘텐츠 감사 보안 그룹 정책인 경우, 리소스에 대한 자세한 위반 정보에 액세스할 수 있습니다.

   위반 세부 정보를 보려면 리소스를 선택합니다.

   > **Note**
   >
   > Firewall Manager에서 리소스 위반에 대한 세부 정보 페이지를 추가하기 전에 규정을 준수하지 않는 것으로 확인된 리소스에는 위반 세부 정보가 없을 수 있습니다.

   리소스 페이지에서 Firewall Manager는 리소스 유형에 따라 위반에 대한 특정 세부 정보를 나열합니다.

   - **`AWS::EC2::NetworkInterface`**(ENI) - Firewall Manager는 리소스가 준수하지 않는 보안 그룹에 대한 정보를 표시합니다. 보안 그룹을 선택하면 보안 그룹에 대한 세부 정보를 볼 수 있습니다.
   - **`AWS::EC2::Instance`** – Firewall Manager는 규정을 준수하지 않는 EC2 인스턴스에 연결된 ENI를 표시합니다. 또한 리소스가 준수하지 않는 보안 그룹에 대한 정보도 표시합니다. 보안 그룹을 선택하면 보안 그룹에 대한 세부 정보를 볼 수 있습니다.
   - **`AWS::EC2::SecurityGroup`** – Firewall Manager는 다음과 같은 위반 세부 정보를 표시합니다.
     - 비준수 보안 그룹 규칙 - 프로토콜, 포트 범위, IP CIDR 범위 및 설명을 포함하여 위반된 규칙입니다.
     - 참조 규칙 - 비준수 보안 그룹 규칙이 위반하는 감사 보안 그룹 규칙(세부 정보 포함)
     - 위반 사유 – 규정 미준수 결과에 대한 설명.
     - 개선 조치 – 취해야 할 권장 조치. Firewall Manager에서 안전한 수정 조치를 결정할 수 없는 경우 이 필드는 비어 있습니다.
   - **`AWS::EC2::Subnet`**— 네트워크 ACL 및 네트워크 방화벽 정책에 사용됩니다.

Firewall Manager는 서브넷 ID, VPC ID, 가용 영역을 표시합니다. 해당하는 경우 Firewall Manager에는 위반에 대한 추가 정보가 포함됩니다. 위반 설명 구성 요소에는 리소스의 예상 상태, 현재 비준수 상태에 대한 설명과 가능한 경우 불일치의 원인에 대한 설명이 포함되어 있습니다.

Network Firewall 위반

- 라우팅 관리 위반 - 모니터링 모드를 사용하는 네트워크 방화벽 정책의 경우 Firewall Manager는 서브넷, 인터넷 게이트웨이 및 네트워크 방화벽 서브넷 라우팅 테이블의 예상 및 실제 경로뿐만 아니라 기본 서브넷 정보를 표시합니다. Firewall Manager는 실제 경로가 라우팅 테이블의 예상 경로와 일치하지 않는 경우 위반이 있음을 알려줍니다.
- 라우팅 관리 위반에 대한 수정 조치 - 모니터링 모드를 사용하는 네트워크 방화벽 정책의 경우 Firewall Manager는 위반이 있는 경로 구성에 대해 가능한 수정 조치를 제안합니다.

예를 들어 서브넷은 방화벽 엔드포인트를 통해 트래픽을 전송할 것으로 예상되지만 현재 서브넷은 트래픽을 인터넷 게이트웨이로 직접 전송한다고 가정해 보겠습니다. 이는 라우팅 관리 위반입니다. 이 경우 제안되는 해결 방법은 순서가 지정된 조치 목록일 수 있습니다. 첫 번째는 필요한 경로를 네트워크 방화벽 서브넷의 라우팅 테이블에 추가하여 나가는 트래픽을 인터넷 게이트웨이로 보내고 VPC 내부 목적지로 들어오는 트래픽은 `local`(으)로 보내도록 하는 것입니다. 두 번째 권장 사항은 서브넷의 라우팅 테이블에 있는 인터넷 게이트웨이 경로 또는 잘못된 네트워크 방화벽 경로를 대체하여 나가는 트래픽을 방화벽 엔드포인트로 보내는 것입니다. 세 번째 권장 사항은 인터넷 게이트웨이의 라우팅 테이블에 필수 경로를 추가하여 들어오는 트래픽을 방화벽 엔드포인트로 보내는 것입니다.

- **`AWS::EC2::InternetGateway`** - 모니터링 모드가 활성화된 네트워크 방화벽 정책에 사용됩니다.
  - 라우팅 관리 위반 - 인터넷 게이트웨이가 라우팅 테이블에 연결되어 있지 않거나 인터넷 게이트웨이 라우팅 테이블에 잘못된 경로가 있는 경우 인터넷 게이트웨이는 규정을 준수하지 않습니다.
  - 라우팅 관리 위반에 대한 해결 조치 - Firewall Manager는 라우팅 관리 위반을 해결하기 위한 가능한 수정 조치를 제안합니다.

Example 1 - 라우팅 관리 위반 및 개선 제안

인터넷 게이트웨이가 라우팅 테이블과 연결되어 있지 않습니다. 제안된 개선 조치는 순서가 지정된 조치 목록일 수 있습니다. 첫 번째 작업은 라우팅 테이블을 생성하는 것입니다. 두 번째 작업은 라우팅 테이블을 인터넷 게이트웨이와 연결하는 것입니다. 세 번째 작업은 인터넷 게이트웨이 라우팅 테이블에 필요한 경로를 추가하는 것입니다.

Example 2 - 라우팅 관리 위반 및 개선 제안

인터넷 게이트웨이가 유효한 라우팅 테이블과 연결되었지만 경로가 잘못 구성되었습니다. 제안된 해결 방법은 순서가 지정된 작업 목록일 수 있습니다. 첫 번째 제안은 잘못된 경로를 제거하는 것입니다. 두 번째는 인터넷 게이트웨이 라우팅 테이블에 필요한 경로를 추가하는 것입니다.

- **`AWS::NetworkFirewall::FirewallPolicy`** - 네트워크 방화벽 정책에 사용됩니다. Firewall Manager는 규정을 준수하지 않는 방식으로 수정된 네트워크 방화벽 방화벽 정책에 대한 정보를 표시합니다. 이 정보는 예상 방화벽 정책과 고객 계정에서 찾은 정책을 제공하므로 상태 비저장 및 상태 저장 규칙 그룹 이름과 우선 순위 설정, 사용자 지정 작업 이름, 기본 상태 비저장 작업 설정을 비교할 수 있습니다. 위반 설명 구성 요소에는 리소스의 예상 상태, 현재 비준수 상태에 대한 설명과 가능한 경우 불일치의 원인에 대한 설명이 포함되어 있습니다.
- **`AWS::EC2::VPC`** - DNS 방화벽 정책에 사용됩니다. Firewall Manager는 Firewall Manager DNS 방화벽 정책의 범위에 속하며 정책을 준수하지 않는 VPC에 대한 정보를 표시합니다. 제공된 정보에는 VPC와 연결될 것으로 예상되는 규칙 그룹과 실제 규칙 그룹이 포함됩니다. 위반 설명 구성 요소에는 리소스의 예상 상태, 현재 비준수 상태에 대한 설명과 가능한 경우 불일치의 원인에 대한 설명이 포함되어 있습니다.

AWS Firewall Manager 조사 결과

AWS Firewall Manager 규정을 준수하지 않는 리소스와 탐지한 공격에 대한 검색 결과를 생성하여 AWS Security Hub전송합니다. Security Hub 조사 결과에 대한 자세한 내용은 AWS Security Hub의 조사 결과를 참조하세요.

Security Hub 및 Firewall Manager를 사용하면 Firewall Manager가 자동으로 검색 조사 결과를 Security Hub에 보냅니다. Security Hub를 시작하는 방법에 관한 자세한 내용은 AWS Security Hub 사용 설명서의 AWS Security Hub설정을 참조하세요.

> **Note**
>
> Firewall Manager는 관리 중인 정책과 모니터링 중인 리소스에 대한 결과만 업데이트합니다. Firewall Manager는 다음과 같은 문제를 해결하지 않습니다.
>
> - 정책이 삭제되었습니다.
> - 삭제된 리소스.
> - 태그 변경 또는 정책 정의 변경 등으로 인해 Firewall Manager 정책의 범위를 벗어난 리소스

Firewall Manager 조사사 조사 결과를 보려면 어떻게 해야 합니까?

Security Hub의 Firewall Manager 조사 결과를 보려면 Security Hub의 조사 결과로 작업에서 해당 지침을 따르고 다음 설정을 사용하여 필터를 만듭니다.

- 속성을 제품 이름으로 설정합니다.
- 연산자를 EQALS로 설정됩니다.
- 값을 `Firewall Manager`로 설정합니다. 이 설정은 대/소문자를 구분합니다.

이를 비활성화할 수 있습니까?

Security Hub 콘솔을 통해 AWS Firewall Manager 검색 결과를 Security Hub와 통합하지 않도록 설정할 수 있습니다. 탐색 모음에서 통합을 선택한 다음 Firewall Manager 창에서 통합 비활성화를 선택합니다. 자세한 정보는 AWS Security Hub 사용 설명서를 참조하세요.

AWS Firewall Manager 검색 유형

- AWS WAF 정책 조사 결과
- AWS Shield Advanced 정책 조사 결과
- 보안 그룹 공통 정책 결과
- 보안 그룹 콘텐츠 감사 정책 결과
- 보안 그룹 사용 감사 정책 결과
- Amazon Route 53 Resolver DNS 방화벽 정책 조사 결과

AWS WAF 정책 조사 결과

Firewall Manager AWS WAF 정책을 사용하여 AWS WAF 규칙 그룹을 의 리소스에 적용할 수 AWS Organizations있습니다. 자세한 정보는 AWS Firewall Manager 정책 관련 작업을 참조하세요.

리소스에 Firewall Manager에서 관리하는 웹 ACL이 없습니다.

AWS 리소스에는 Firewall Manager 정책에 따른 AWS Firewall Manager 관리형 웹 ACL 연결이 없습니다. 정책에 대해 Firewall Manager 수정을 활성화하여 이 문제를 해결할 수 있습니다.

- 심각도 – 80
- 상태 설정 – PASSED/FAILED

- 업데이트 - Firewall Manager가 수정 작업을 수행하면 조사 결과가 업데이트되고 심각도는 HIGH에서 INFORMATIONAL로 낮아집니다. 사용자가 수정을 수행하면 Firewall Manager는 조사 결과를 업데이트하지 않습니다.

Firewall Manager 관리형 웹 ACL에서 규칙 그룹이 잘못 구성되었습니다.

Firewall Manager에서 관리하는 웹 ACL의 규칙 그룹이 Firewall Manager 정책에 따라 올바르게 구성되지 않았습니다. 즉, 웹 ACL에 정책에서 필요로 하는 규칙 그룹이 누락되었습니다. 정책에 대해 Firewall Manager 수정을 활성화하여 이 문제를 해결할 수 있습니다.

- 심각도 – 80
- 상태 설정 – PASSED/FAILED
- 업데이트 - Firewall Manager가 수정 작업을 수행하면 조사 결과가 업데이트되고 심각도는 HIGH에서 INFORMATIONAL로 낮아집니다. 사용자가 수정을 수행하면 Firewall Manager는 조사 결과를 업데이트하지 않습니다.

AWS Shield Advanced 정책 조사 결과

AWS Shield Advanced 정책에 대한 자세한 내용은 을 참조하십시오보안 그룹 정책.

리소스에 Shield Advanced 보호 기능이 없습니다.

Firewall Manager 정책에 따라 Shield Advanced 보호 기능이 있어야 하는 AWS 리소스에는 해당 보호 기능이 없습니다. 정책에 대해 Firewall Manager 수정을 활성화하면 리소스에 대한 보호를 사용할 수 있습니다.

- 심각도 – 60
- 상태 설정 – PASSED/FAILED
- 업데이트 - Firewall Manager가 수정 작업을 수행하면 조사 결과가 업데이트되고 심각도는 HIGH에서 INFORMATIONAL로 낮아집니다. 사용자가 수정을 수행하면 Firewall Manager는 조사 결과를 업데이트하지 않습니다.

Shield Advanced가 모니터링되는 리소스에 대한 공격을 탐지했습니다.

Shield Advanced가 보호 대상 AWS 리소스에 대한 공격을 탐지했습니다. 정책에 대해 Firewall Manager 수정을 활성화할 수 있습니다.

- 심각도 – 70

- 상태 설정 – None
- 업데이트 - Firewall Manager는 이 조사 결과를 업데이트하지 않습니다.

보안 그룹 공통 정책 결과

보안 그룹 공통 정책에 대한 자세한 내용은 보안 그룹 정책을 참조하세요.

리소스에 보안 그룹이 잘못 구성되었습니다.

Firewall Manager가 Firewall Manager 정책에 따라 보유해야 하는 Firewall Manager 관리형 보안 그룹 연결이 누락된 리소스를 식별했습니다. 정책 설정에 따라 연결을 생성하는 정책에 대해 Firewall Manager 수정을 활성화할 수 있습니다.

- 심각도 – 70
- 상태 설정 – PASSED/FAILED
- 업데이트 - Firewall Manager가 이 조사사 조사 결과를 업데이트합니다.

Firewall Manager 복제본 보안 그룹이 기본 보안 그룹과 동기화되지 않았습니다.

Firewall Manager 복제본 보안 그룹이 공통 보안 그룹 정책에 따라 기본 보안 그룹과 동기화되지 않았습니다. 정책에 대해 Firewall Manager 수정을 활성화하여 복제본 보안 그룹을 기본 보안 그룹과 동기화할 수 있습니다.

- 심각도 – 80
- 상태 설정 – PASSED/FAILED
- 업데이트 - Firewall Manager가 이 조사사 조사 결과를 업데이트합니다.

보안 그룹 콘텐츠 감사 정책 결과

보안 그룹 콘텐츠 감사 정책에 대한 자세한 내용은 보안 그룹 정책을 참조하세요.

보안 그룹이 콘텐츠 감사 보안 그룹을 준수하고 있지 않습니다.

Firewall Manager 보안 그룹 콘텐츠 감사 정책에서 규정 미준수 보안 그룹을 식별했습니다. 이는 고객이 생성한 보안 그룹으로 콘텐츠 감사 정책의 범위 내에 있지만 정책 및 해당 감사 보안 그룹에서 정의한 설정을 준수하고 있지 않습니다. 정책에 대해 Firewall Manager 수정을 활성화하면 규정 미준수 보안 그룹을 수정하여 규정을 준수할 수 있습니다.

- 심각도 – 70
- 상태 설정 – PASSED/FAILED
- 업데이트 - Firewall Manager가 이 조사사 조사 결과를 업데이트합니다.

보안 그룹 사용 감사 정책 결과

보안 그룹 사용 감사 정책에 대한 자세한 내용은 보안 그룹 정책을 참조하세요.

Firewall Manager에서 중복된 보안 그룹을 찾았습니다.

Firewall Manager 보안 그룹 사용 감사에서 중복 보안 그룹을 식별했습니다. 이는 동일한 Amazon Virtual Private Cloud 인스턴스 내에서 다른 보안 그룹으로 설정된 동일한 규칙을 가진 보안 그룹입니다. 사용 감사 정책에 대해 Firewall Manager 자동 수정을 활성화하여 중복 보안 그룹을 단일 보안 그룹으로 바꿀 수 있습니다.

- 심각도 – 30
- 상태 설정 – None
- 업데이트 - Firewall Manager는 이 조사 결과를 업데이트하지 않습니다.

Firewall Manager에서 사용되지 않은 보안 그룹을 찾았습니다.

Firewall Manager 보안 그룹 사용 감사에서 사용되지 않은 보안 그룹을 식별했습니다. 이는 Firewall Manager 공통 보안 그룹 정책에서 참조하지 않는 보안 그룹입니다. 사용 감사 정책에 대해 Firewall Manager 자동 수정을 활성화하여 사용하지 않는 보안 그룹을 제거할 수 있습니다.

- 심각도 – 30
- 상태 설정 – None
- 업데이트 - Firewall Manager는 이 조사 결과를 업데이트하지 않습니다.

Amazon Route 53 Resolver DNS 방화벽 정책 조사 결과

DNS 방화벽 정책에 대한 자세한 설명은 Amazon Route 53 Resolver DNS 방화벽 정책을 참조하세요.

리소스에 DNS Firewall 보호가 없습니다.

VPC에 Firewall Manager DNS 방화벽 정책에 정의된 DNS Firewall 규칙 그룹 연결이 누락되었습니다. 조사 결과에는 정책에 지정된 규칙 그룹이 나열됩니다.

- 심각도 – 80

AWS Firewall Manager 서비스 사용 시 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

> **Note**
>
> 이 섹션에서는 Firewall Manager Network Firewall 정책 및 AWS 보안 그룹 정책과 같은 AWS Firewall Manager 서비스 및 해당 AWS 리소스 사용에 대한 표준 보안 지침을 제공합니다. Firewall Manager를 사용하여 AWS 리소스를 보호하는 방법에 대한 자세한 내용은 Firewall Manager 가이드의 나머지 부분을 참조하십시오.

보안은 사용자와 사용자 AWS 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 - AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호하는 역할을 합니다 AWS 클라우드. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사자는 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Firewall Manager에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램을 통한AWS 범위 내 서비스 섹션을 참조하세요.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 데이터의 민감도, 조직의 요건 및 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Firewall Manager 사용 시 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표를 충족하도록 Firewall Manager를 구성하는 방법을 보여줍니다. 또한 Firewall Manager 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- Firewall Manager의 데이터 보호
- Identity 및 Access Management에 대한 AWS Firewall Manager
- Firewall Manager에서의 로깅 및 모니터링
- Firewall Manager에 대한 규정 준수 확인

- Firewall Manager의 복원성
- AWS Firewall Manager에서 인프라 보안

Firewall Manager의 데이터 보호

AWS 공동 책임 모델 의 데이터 보호에 적용됩니다 AWS Firewall Manager. 이 모델에 설명된 대로 AWS 는 모든 데이터를 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 사용하는 AWS 서비스 의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS IAM Identity Center OR AWS Identity and Access Management (IAM) 을 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이 방식을 사용하면 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 리소스와 통신할 수 있습니다. AWS TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다. AWS CloudTrail
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하여 Amazon S3에 저장된 민감한 데이터를 검색하고 보호합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용하십시오. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하십시오.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔 AWS CLI, API 또는 AWS 서비스 AWS SDK를 사용하여 Firewall Manager 또는 기타 작업을 수행하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

정책 등의 Firewall Manager 엔터티는 중국(베이징)과 중국(닝샤)를 포함하여 암호화를 사용할 수 없는 일부 리전을 제외하고 유휴 상태에서 암호화됩니다. 리전마다 고유한 암호화 키가 사용됩니다.

Identity 및 Access Management에 대한 AWS Firewall Manager

AWS Identity and Access Management (IAM) 은 관리자가 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 AWS 도와줍니다. IAM 관리자는 어떤 사용자가 Firewall Manager 리소스를 사용할 수 있도록 인증(로그인)되고 권한이 부여(권한 있음)될 수 있는지 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

- 고객
- ID를 통한 인증
- 정책을 사용한 액세스 관리
- AWS Firewall Manager IAM과의 작동 방식
- 에 대한 ID 기반 정책 예제 AWS Firewall Manager
- AWS 에 대한 관리형 정책 AWS Firewall Manager
- AWS Firewall Manager ID 및 액세스 문제 해결
- Firewall Manager용 서비스 연결 역할 사용
- 교차 서비스 혼동된 대리인 방지

고객

AWS Identity and Access Management (IAM) 사용 방법은 Firewall Manager에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 – Firewall Manager 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증 정보와 권한을 관리자가 제공합니다. 더 많은 Firewall Manager 기능을 사용하여 작업을 수행한다면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Firewall Manager의 기능에 액세스할 수 없다면 AWS Shield ID 및 액세스 문제 해결(을)를 참조하세요.

서비스 관리자 – 회사에서 Firewall Manager 리소스를 책임지고 있다면 Firewall Manager에 대한 완전한 액세스 권한이 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Firewall Manager 기능과 리소스를 결정합니다. 그런 다음, IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하십시오. 회사가 Firewall

Manager에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 AWS Shield IAM과의 작동 방식(을)를 참조하세요.

IAM 관리자 - IAM 관리자라면 Firewall Manager에 대한 액세스 관리 정책 작성 방법을 자세히 알고 싶을 수도 있습니다. IAM에서 사용할 수 있는 Firewall Manager ID 기반 정책의 예제를 확인하려면 AWS Shield에 대한 자격 증명 기반 정책 예시(을)를 참조하세요.

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트 (SDK) 와 명령줄 인터페이스 (CLI) 를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하십시오.

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 태스크를 수행하는 데 사용하세요. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하십시오.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하십시오.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 보안 인증이 있는 IAM 사용자를 생성하는 대신 임시 보안 인증을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우 정기적으로 액세스 키 교체를 참조하십시오.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하십시오.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역

할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 IAM 역할 사용을 참조하십시오.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 서드 파티 ID 공급자의 역할 생성 단원을 참조하십시오. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하십시오.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 태스크에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스서비스의 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 태스크를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은

사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하십시오.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하십시오.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 가이드의 ACL(액세스 제어 목록) 개요를 참조하십시오.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 개체의 보안 인증 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 IAM 엔터티에 대한 권한 경계를 참조하십시오.

- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책 (SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 구성원 계정의 엔티티 (각 엔티티 포함) 에 대한 권한을 제한합니다. AWS 계정 루트 사용자조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서의 SCP 작동 방식을 참조하십시오.
- 세션 정책 - 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하십시오.

여러 정책 타입

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

AWS Firewall Manager IAM과의 작동 방식

IAM을 사용하여 Firewall Manager에 대한 액세스를 관리하기 전에 Firewall Manager와 함께 사용할 수 있는 IAM 기능을 알아보세요.

함께 사용할 수 있는 IAM 기능 AWS Firewall Manager

IAM 특성	Firewall Manager 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	아니요
ACL	아니요

IAM 특성	Firewall Manager 지원
ABAC(정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	부분
서비스 링크 역할	예

Firewall Manager 및 기타 AWS 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 연동되는AWS 서비스를 참조하십시오.

Firewall Manager에 대한 자격 증명 기반 정책

보안 인증 기반 정책 지원	예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하십시오.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

Firewall Manager 자격 증명 기반 정책의 예를 보려면 에 대한 ID 기반 정책 예제 AWS Firewall Manager(을)를 참조하세요.

Firewall Manager에 대한 자격 증명 기반 정책의 예

Firewall Manager 자격 증명 기반 정책의 예를 보려면 에 대한 ID 기반 정책 예제 AWS Firewall Manager(을)를 참조하세요.

Firewall Manager 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우, 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 태스크를 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하십시오.

Firewall Manager용 정책 작업

정책 작업 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 태스크를 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

Firewall Manager 작업 목록을 보려면 서비스 승인 참조의 AWS Firewall Manager에서 정의한 작업을 참조하세요.

Firewall Manager의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
fms
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

와일드카드(*)를 사용하여 여러 작업을 지정할 수 있습니다. 예를 들어, Describe라는 단어로 시작하는 모든 태스크를 지정하려면 다음 태스크를 포함합니다.

```
"Action": "fms:Describe*"
```

Firewall Manager 자격 증명 기반 정책의 예를 보려면 에 대한 ID 기반 정책 예제 AWS Firewall Manager(을)를 참조하세요.

Firewall Manager용 정책 리소스

정책 리소스 지원	예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 하나 이상의 개체를 지정합니다. 문장에는 Resource또는 NotResource요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Firewall Manager 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조에서 AWS Firewall Manager에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 AWS Firewall Manager가 정의한 작업을 참조하십시오.

Firewall Manager 자격 증명 기반 정책의 예를 보려면 에 대한 ID 기반 정책 예제 AWS Firewall Manager(을)를 참조하세요.

Firewall Manager에 대한 정책 조건 키

서비스별 정책 조건 키 지원	아니요

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예컨대, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

Firewall Manager 조건 키 목록을 보려면 서비스 승인 참조의 AWS Firewall Manager에 대한 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 작업 정의 기준을 참조하십시오.
AWS Firewall Manager

Firewall Manager 자격 증명 기반 정책의 예를 보려면 에 대한 ID 기반 정책 예제 AWS Firewall Manager(을)를 참조하세요.

Firewall Manager의 ACL

ACL 지원	아니요

ACL(액세스 통제 목록)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACLs는 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Firewall Manager과 관련된 ABAC

ABAC 지원(정책의 태그)	예

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 정보는 IAM 사용 설명서의 ABAC란 무엇입니까?를 참조하십시오. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하십시오.

Firewall Manager에서 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다

음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하십시오.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하십시오.

Firewall Manager에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Firewall Manager용 서비스 역할

서비스 역할 지원	부분

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 대한 권한을 위임할 역할 생성을 참조하십시오.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Firewall Manager 기능이 중단될 수 있습니다. Firewall Manager가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

Firewall Manager에서 IAM 역할 선택하기

Firewall Manager에서 *PutNotificationChannel*API 작업을 사용하려면 Firewall Manager가 Amazon SNS에 액세스할 수 있도록 허용하는 역할을 선택해야 합니다. 그러면 서비스에서 사용자

를 대신하여 Amazon SNS 메시지를 게시할 수 있습니다. 자세한 내용은 AWS Firewall Manager API PutNotificationChannel참조를 참조하십시오.

다음은 SNS 주제 권한 설정의 예를 보여줍니다. 자체 사용자 지정 역할에서 이 정책을 사용하려면 AWSServiceRoleForFMS Amazon 리소스 이름(ARN)을 SnsRoleName ARN으로 바꿉니다.

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

Firewall Manager 작업 및 리소스에 대한 자세한 내용은 AWS Identity and Access Management 가이드 항목 정의한 작업을 참조하십시오. AWS Firewall Manager

Firewall Manager용 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하십시오. 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

에 대한 ID 기반 정책 예제 AWS Firewall Manager

기본적으로 사용자 및 역할은 Firewall Manager 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Firewall Manager에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 권한 부여 참조의 AWS Firewall Manager에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Firewall Manager 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용
- Firewall Manager 보안 그룹에 읽기 액세스 권한 부여하기

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Firewall Manager 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 Policies and permissions in IAM(IAM의 정책 및 권한)을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여

안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하tpdy.

- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Firewall Manager 콘솔 사용

AWS Firewall Manager 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은 AWS 계정에서 Firewall Manager 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Firewall Manager 콘솔을 계속 사용할 수 있도록 하려면 Firewall Manager *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예시는 IAM 사용자가 자신의 사용자 자격 증명에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
```

```
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Firewall Manager 보안 그룹에 읽기 액세스 권한 부여하기

Firewall Manager에서는 교차 계정 리소스 액세스를 허용하지만 교차 계정 리소스 보호를 생성할 수 없습니다. 이러한 리소스를 소유한 계정 내에서만 리소스에 대한 보호를 생성할 수 있습니다.

다음은 모든 리소스에 대해 `fms:Get`,`fms:List` 및 `ec2:DescribeSecurityGroups` 작업 권한을 부여하는 정책의 예시입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

AWS 에 대한 관리형 정책 AWS Firewall Manager

AWS 관리형 정책은 에서 생성하고 관리하는 독립 실행형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하십시오.

AWS 관리형 정책: **`AWSFMAdminFullAccess`**

`AWSFMAdminFullAccess` AWS 관리형 정책을 사용하면 관리자가 모든 Firewall Manager 정책 유형을 비롯한 AWS Firewall Manager 리소스에 액세스할 수 있습니다. 이 정책에는 AWS Firewall Manager에서 Amazon Simple Notification Service 알림을 설정할 수 있는 권한이 포함되어 있지 않습니다. Amazon Simple Notification Service 액세스를 설정하는 방법에 대한 자세한 내용은 Amazon Simple Notification Service 액세스 설정을 참조하세요.

정책 목록 및 세부 정보는 의 IAM 콘솔을 참조하십시오. AWSFMAdminFullAccess 이 섹션의 나머지 부분에서는 정책 설정에 대한 개요를 제공합니다.

권한 설명

이 정책은 권한 세트에 기반하여 명령문으로 그룹화됩니다.

- AWS Firewall Manager 정책 리소스 - 모든 Firewall Manager 정책 유형을 AWS Firewall Manager포함하여 의 리소스에 대한 전체 관리 권한을 허용합니다.
- Amazon 심플 스토리지 서비스에 AWS WAF 로그 쓰기 - Firewall Manager가 Amazon S3에서 AWS WAF 로그를 쓰고 읽을 수 있도록 합니다.

- 서비스 연결 역할 생성 - 관리자가 서비스 연결 역할을 생성하여 Firewall Manager가 사용자를 대신하여 다른 서비스의 리소스에 액세스할 수 있도록 합니다. 이 권한은 Firewall Manager에서만 사용 가능한 서비스 연결 역할만 생성할 수 있습니다. Firewall Manager에서 서비스 연결 역할을 사용하는 방법에 대한 자세한 내용은 을 참조하십시오. Firewall Manager용 서비스 연결 역할 사용
- AWS Organizations - 관리자가 Firewall Manager를 AWS Organizations의 조직에 대해 사용하도록 허용합니다. 에서 AWS Organizations Firewall Manager에 대한 신뢰할 수 있는 액세스를 활성화한 후 관리자 계정 구성원은 조직 전체의 조사 결과를 볼 수 있습니다. 에서 사용하는 AWS Organizations 방법에 대한 자세한 내용은 사용 AWS Organizations 설명서의 다른 AWS 서비스와 AWS Organizations 함께 사용을 참조하십시오. AWS Firewall Manager

권한 카테고리

다음은 정책의 권한 유형과 해당 권한이 제공하는 권한을 나열합니다.

- `fms`— AWS Firewall Manager 리소스를 활용하세요.
- `waf`및 `waf-regional` — AWS WAF 클래식 정책을 사용하십시오.
- `elasticloadbalancing`— AWS WAF 웹 ACL을 엘라스틱 로드 밸런서에 연결합니다.
- `firehose`— 로그에 대한 정보를 볼 수 있습니다. AWS WAF
- `organizations`— AWS 조직 리소스를 활용하십시오.
- `shield`— AWS Shield 정책의 구독 상태를 볼 수 있습니다.
- `route53resolver`— VPC용 Route 53 프라이빗 DNS 정책에서 VPC용 Route 53 프라이빗 DNS 규칙 그룹을 사용하십시오.
- `wafv2`— 정책을 활용하십시오. AWS WAFV2
- `network-firewall`— AWS Network Firewall 정책 관련 작업.
- `ec2`— 정책 가용 영역 및 지역 보기.
- `s3`— AWS WAF 로그에 대한 정보를 볼 수 있습니다.

AWS 관리형 정책: **`FMSServiceRolePolicy`**

이 정책을 통해 AWS Firewall Manager Firewall Manager 및 통합 서비스에서 사용자를 대신하여 AWS 리소스를 관리할 수 있습니다. 이 정책은 `AWSServiceRoleForFMS` 서비스 역할에 연결됩니다. 서비스 링크 역할에 대한 자세한 내용은 Firewall Manager용 서비스 연결 역할 사용을(를) 참조하세요.

정책 세부 정보는 ServiceRolePolicyFMS의 IAM 콘솔을 참조하십시오.

AWS 관리형 정책: AWSFMAdminReadOnlyAccess

모든 AWS Firewall Manager 리소스에 대한 읽기 전용 액세스 권한을 부여합니다.

정책 목록 및 세부 정보는 의 IAM 콘솔을 참조하십시오. AWSFMAdminReadOnlyAccess 이 섹션의 나머지 부분에서는 정책 설정에 대한 개요를 제공합니다.

권한 카테고리

다음은 정책의 권한 유형과 해당 권한이 읽기 전용 액세스를 허용하는 정보를 나열합니다.

- `fms`— AWS Firewall Manager 리소스.
- `waf`및 `waf-regional` — AWS WAF 클래식 정책.
- `firehose`— AWS WAF 로그.
- `organizations`— AWS 조직 리소스.
- `shield`— AWS Shield 정책.
- `route53resolver`— VPC용 Route 53 프라이빗 DNS 규칙 그룹의 VPC용 Route 53 프라이빗 DNS 정책.
- `wafv2`— 에서 사용할 수 있는 사용자 AWS WAFV2 규칙 그룹 및 AWS 관리형 규칙 그룹. AWS WAFV2
- `network-firewall`— AWS Network Firewall 규칙 그룹 및 규칙 그룹 메타데이터.
- `ec2`— AWS Network Firewall 정책 가용 영역 및 지역.
- `s3`— AWS WAF 로그.

AWS 관리형 정책: AWSFMMemberReadOnlyAccess

AWS Firewall Manager 구성원 리소스에 대한 읽기 전용 액세스 권한을 부여합니다. 정책 목록 및 세부 정보는 의 IAM 콘솔을 참조하십시오. AWSFMMemberReadOnlyAccess

AWS 관리형 정책에 대한 방화벽 관리자 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Firewall Manager의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 문서 기록의 Firewall Manager 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
FMS ServiceRolePolicy — 업데이트된 정책	네트워크 ACL 관리를 위한 권한이 추가되었습니다. IAM 콘솔의 업데이트된 정책인 FMS를 참조하십시오. ServiceRolePolicy	2024-04-22
FMS — 업데이트된 정책 ServiceRolePolicy	Firewall Manager가 지정된 AWS Config 규칙의 준수 여부를 설명할 수 있는 권한이 추가되었습니다. IAM 콘솔의 업데이트된 정책인 FMS를 참조하십시오. ServiceRolePolicy	2023-04-21
FMS — 업데이트된 정책 ServiceRolePolicy	Firewall Manager가 Amazon EC2 인스턴스 및 네트워크 인터페이스 속성을 설명할 수 있도록 권한이 추가되었습니다. IAM 콘솔의 업데이트된 정책인 FMS를 참조하십시오. ServiceRolePolicy	2022-11-15
AWSFMAdminReadOnly Access - 정책 업데이트	Shield AWS WAFV2, 네트워크 방화벽, DNS 방화벽, Amazon VPC 보안 그룹, 정책을 지원하는 권한이 추가되었습니다. IAM 콘솔에서 업데이트된 정책을 참조하십시오. AWSFMAdminReadOnly Access	2022-11-02
AWSFMAdminFullAccess - 정책 업데이트	Shield AWS WAFV2, 네트워크 방화벽, DNS 방화벽, Amazon	2022-10-21

변경 사항	설명	날짜
	VPC 보안 그룹, 정책을 지원하는 권한이 추가되었습니다. Amazon SNS 권한이 삭제되었습니다. IAM 콘솔에서 업데이트된 정책을 참조하십시오. AWSFMAdminFullAccess	
`FMSServiceRolePolicy` — 타사 방화벽 정책에 대한 AWS Firewall Manager 새로운 권한	이 변경을 통해 Firewall Manager는 타사 방화벽 정책과 연결된 Amazon EC2 VPC 엔드포인트를 생성 및 삭제할 수 있습니다.	2022-03-30
`FMSServiceRolePolicy` — 정책에 대한 새로운 권한 AWS Network Firewall	Network Firewall 정책에 대한 방화벽 배포를 지원하는 새로운 권한이 추가되었습니다. 새로운 권한을 통해 정책 범위 내에 있는 계정의 가용 영역에 대한 정보를 검색할 수 있습니다.	2022-02-16
`FMSServiceRolePolicy` — 정책에 대한 새로운 권한 AWS Shield	AWS WAF 지역 및 AWS WAF 글로벌 리소스의 태그를 검색할 수 있는 새 권한이 추가되었습니다. 리소스 ARN을 사용하여 웹 ACL을 검색할 수 있는 AWS WAF 지역 권한이 추가되었습니다. Shield 자동 애플리케이션 계층 DDoS 완화를 지원할 수 있는 권한이 추가되었습니다.	2022-01-07
`FMSServiceRolePolicy` — 정책에 대한 새로운 권한 AWS Shield	Elastic Load Balancing 리소스의 태그를 검색할 수 있는 새로운 권한이 추가되었습니다.	2021-11-18

변경 사항	설명	날짜
`FMSServiceRolePolicy` — 보안 그룹 및 정책에 대한 새 권한 AWS Network Firewall	AWS Network Firewall 정책에 대한 중앙 집중식 로깅을 활성화할 수 있는 새 권한이 추가되었습니다. 또한 보안 그룹 정책에 대한 리소스 쿼리 AWS Firewall Manager 방식에 영향을 미치는 Config 서비스 변경을 지원하기 위해 읽기 전용 Amazon EC2 권한이 추가되었습니다.	2021-09-29
`FMSServiceRolePolicy` — 리소스용 ARN 형식 AWS WAF	AWS WAF 리소스용 ARN 형식을 표준화하도록 `FMSServiceRolePolicy` 이(가) 업데이트되었습니다. 업데이트된 ARN 형식은 `arn:aws:waf:*:*:*` 및 `arn:aws:waf-regional:*:*:*` 입니다.	2021-08-12
`FMSServiceRolePolicy` — 중국 내 추가 리전	AWS Firewall Manager 중국 내 BJS 및 `FMSServiceRolePolicy` ZHY 지역을 사용할 수 있게 되었습니다.	2021-08-12

변경 사항	설명	날짜
`FMSServiceRolePolicy` - 기존 정책에 대한 업데이트	DNS 방화벽을 관리할 수 있는 새 권한이 추가되었습니다 AWS Firewall Manager . Amazon Route 53 Resolver 이 변경을 통해 Firewall Manager는 Amazon Route 53 Resolver DNS 방화벽 연결을 구성할 수 있습니다. 이를 통해 AWS Organizations에서 Firewall Manager를 사용하여 조직 전체의 VPC에 대한 DNS 방화벽 보호를 제공할 수 있습니다.	2021-03-17
Firewall Manager가 변경 사항 추적을 시작함	Firewall Manager는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021-03-02

AWS Firewall Manager ID 및 액세스 문제 해결

다음 정보를 사용하여 Firewall Manager 및 IAM에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다.

주제

- Firewall Manager에서 작업을 수행할 권한이 없음
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 Firewall Manager AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

Firewall Manager에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `fms:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

이 경우 `fms:GetWidget` 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 `mateojackson` 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Firewall Manager에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예시 오류는 `marymajor`(이)라는 IAM 사용자가 콘솔을 사용하여 Firewall Manager에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우 Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 Firewall Manager AWS 계정 리소스에 액세스할 수 있도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하십시오.

- Firewall Manager에서 이러한 기능을 지원하는지 여부를 알아보려면 AWS Shield IAM과의 작동 방식(을)를 참조하세요.

- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- 자격 증명 연동을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(자격 증명 연동)을 참조하십시오.
- 교차 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하십시오.

Firewall Manager용 서비스 연결 역할 사용

AWS Firewall Manager AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Firewall Manager에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Firewall Manager에서 미리 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할로 Firewall Manager를 더 쉽게 설정할 수 있습니다. Firewall Manager에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Firewall Manager만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함됩니다. 이 권한 정책은 다른 어떤 IAM 엔터티에도 연결할 수 없습니다.

먼저 역할의 관련 리소스를 삭제해야 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 Firewall Manager 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조해 서비스 연결 역할 열이 예(Yes)인 서비스를 찾으세요. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 링크가 있는 예를 선택합니다.

Firewall Manager에 대한 서비스 연결 역할 권한 관리

AWS Firewall Manager 는 서비스에 연결된 역할 이름을 AWSServiceRoleForFMS 사용하여 Firewall Manager가 사용자 대신 AWS 서비스를 호출하여 방화벽 정책 및 AWS Organizations 계정 리소스를 관리할 수 있도록 합니다. 이 정책은 AWS 관리형 역할에 연결됩니다. `AWSServiceRoleForFMS` 관리형 역할에 대한 자세한 내용은 AWS 관리형 정책: `FMSServiceRolePolicy`(을)를 참조하세요.

AWSServiceRoleForFMS 서비스 연결 역할은 역할을 맡을 서비스를 신뢰합니다.
`fms.amazonaws.com`

역할 권한 정책은 Firewall Manager가 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- `waf`- 계정의 AWS WAF 클래식 웹 ACL, 규칙 그룹 권한 및 웹 ACL 연결을 관리합니다.
- `ec2` - 탄력적 네트워크 인터페이스 및 Amazon EC2 인스턴스 기반 보안 그룹을 관리합니다. Amazon VPC 서브넷의 네트워크 ACL을 관리합니다.
- `vpc` - Amazon VPC의 서브넷, 라우팅 테이블, 태그, 엔드포인트를 관리합니다.
- `wafv2`- 계정의 AWS WAF 웹 ACL, 규칙 그룹 권한 및 웹 ACL 연결을 관리합니다.
- `cloudfront`- 웹 ACL을 생성하여 배포를 보호하세요. CloudFront
- `config`- 계정에서 방화벽 관리자가 소유한 AWS Config 규칙을 관리합니다.
- `iam`- 이 서비스 연결 역할을 관리하고, 로깅 대상 및 AWS WAF Shield 정책을 구성하는 경우 필수 및 AWS WAF Shield 서비스 연결 역할을 생성합니다.
- `organization`- Firewall Manager가 소유하는 서비스 연결 역할을 생성하여 Firewall Manager에서 사용하는 AWS Organizations 리소스를 관리합니다.
- `shield`- 계정 내 리소스에 AWS Shield 대한 보호 및 L7 완화 구성을 관리합니다.
- `ram`- DNS 방화벽 규칙 그룹 및 Network Firewall 규칙 그룹의 AWS RAM 리소스 공유를 관리합니다.
- `network-firewall`- 방화벽 관리자가 소유한 AWS Network Firewall 리소스와 계정의 종속 Amazon VPC 리소스를 관리합니다.
- `route53resolver` - 계정에서 Firewall Manager 소유 DNS 방화벽 연결을 관리합니다.

IAM 콘솔: FMS에서 전체 정책을 참조하십시오. ServiceRolePolicy

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

Firewall Manager용 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. Firewall Manager 로그온을 활성화하거나 Firewall Manager CLI 또는 Firewall Manager API에서 `PutLoggingConfiguration` 요청을 하면 Firewall Manager가 서비스 연결 역할을 대신 생성합니다. AWS Management Console

로깅을 활성화하려면 `iam:CreateServiceLinkedRole` 권한이 있어야 합니다.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. Firewall Manager 로깅을 활성화하면, Firewall Manager가 사용자에 대한 서비스 연결 역할을 다시 생성합니다.

Firewall Manager용 서비스 연결 역할 편집

Firewall Manager에서는 AWSServiceRoleForFMS 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Firewall Manager용 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제하는 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 단, 서비스 링크 역할에 대한 리소스를 먼저 정리해야 수동으로 삭제할 수 있습니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Firewall Manager 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

IAM을 사용하여 서비스 연결 역할을 삭제하려면

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 서비스 연결 역할을 삭제합니다. AWSServiceRoleForFMS 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하세요.

Firewall Manager 서비스 연결 역할에 대해 지원되는 리전

Firewall Manager는 서비스가 제공되는 모든 리전에서 서비스 연결 역할을 사용하도록 지원합니다. 자세한 내용은 Firewall Manager 엔드포인트 및 할당량을 참조하세요.

교차 서비스 혼동된 대리인 방지

혼동된 대리인 문제는 작업을 수행할 권한이 없는 개체가 권한이 더 많은 개체에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS크로스 서비스 사칭으로 인해 대리인 문제가 발생할 수 있습니다. 교차 서비스 가장은 한 서비스(호출하는 서비스)가 다른 서비스(호출되는 서비스)를 호출할 때 발생할 수 있습니다. 직접적으로 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 보안 주체를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에 `aws:SourceArn`및 `aws:SourceAccount`글로벌 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스에 AWS Firewall Manager 부여하는 권한을 제한하는 것이 좋습니다. 하나의 리소스

만 교차 서비스 액세스와 연결되도록 허용하려는 경우 aws:SourceArn을(를) 사용하십시오. 해당 계정의 모든 리소스가 교차 서비스 사용과 연결되도록 허용하려는 경우 aws:SourceAccount을 사용하세요.

혼동된 대리자 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 aws:SourceArn 전역 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모르거나 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드 문자(*)를 포함한 aws:SourceArn 글로벌 조건 컨텍스트 키를 사용합니다. 예를 들어 arn:aws:fms:*:*account-id*:*입니다.

만약 aws:SourceArn 값에 Amazon S3 버킷 ARN과 같은 계정 ID가 포함되어 있지 않은 경우, 권한을 제한하려면 두 글로벌 조건 컨텍스트 키를 모두 사용해야 합니다.

의 값은 AWS Firewall Manager 관리자 aws:SourceArn AWS 계정이어야 합니다.

다음 예는 Firewall Manager에서 aws:SourceArn 글로벌 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다.

다음 예는 Firewall Manager 역할 신뢰 정책에서 aws:SourceArn 글로벌 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다. *##* 및 *account-id*를 자신의 정보로 바꿉니다.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "servicename.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fms:Region:account-id:${*}",
          "arn:aws:fms:Region:account-id:policy/*"]
      },
      "StringEquals": {
        "aws:SourceAccount": "account-id"
      }
    }
  }
```

```
}
```

Firewall Manager에서의 로깅 및 모니터링

모니터링은 Firewall Manager와 AWS 솔루션의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. 다중 지점 장애가 발생할 경우 이를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 합니다. AWS Firewall Manager 리소스를 모니터링하고 잠재적 이벤트에 대응하기 위한 몇 가지 도구를 제공합니다.

아마존 CloudWatch 알람

CloudWatch 경보를 사용하면 지정한 기간 동안 단일 지표를 관찰할 수 있습니다. 지표가 지정된 임계값을 초과하는 경우 Amazon SNS 주제 또는 AWS Auto Scaling 정책에 알림을 CloudWatch 보냅니다. 자세한 정보는 아마존을 통한 모니터링 CloudWatch을 참조하세요.

AWS CloudTrail 로그

CloudTrail Firewall Manager에서 사용자, 역할 또는 AWS 서비스가 수행한 작업의 기록을 제공합니다. 에서 수집한 CloudTrail 정보를 사용하여 Firewall Manager에 요청한 내용, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다. 자세한 내용은 을 사용하여 AWS CloudTrail API 호출 로깅을(를) 참조하세요.

Firewall Manager에 대한 규정 준수 확인

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.
- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수

프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.

- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Firewall Manager의 복원성

AWS 글로벌 인프라는 가용 영역을 중심으로 구축됩니다 AWS 리전 . AWS 리전 물리적으로 분리되고 격리된 여러 가용 영역을 제공합니다. 이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 가용 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

가용 영역에 대한 AWS 리전 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS Firewall Manager에서 인프라 보안

관리형 서비스로서 AWS 글로벌 네트워크 보안으로 AWS Firewall Manager 보호됩니다. AWS 보안 서비스 및 인프라 AWS 보호 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하십시오. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하십시오.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Firewall Manager에 액세스할 수 있습니다. 고객은 다음을 지원해야 합니다.

- 전송 계층 보안(TLS). TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 비밀 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증 정보를 생성하여 요청에 서명할 수 있습니다.

AWS Firewall Manager 할당량

AWS Firewall Manager 에는 다음과 같은 할당량 (이전에는 한도라고 함) 이 적용됩니다.

AWS Firewall Manager 늘릴 수 있는 기본 할당량과 고정된 할당량이 있습니다.

Firewall Manager에서 관리하는 보안 그룹 정책 및 네트워크 ACL 정책에는 표준 Amazon VPC 할당량이 적용됩니다. 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC 할당량 섹션을 참조하세요.

각 Firewall Manager 네트워크 방화벽 정책은 연결된 방화벽 정책 및 해당 규칙 그룹을 포함하는 네트워크 방화벽 방화벽을 생성합니다. 이러한 네트워크 방화벽 리소스에는 네트워크 방화벽 개발자 가이드의 AWS Network Firewall 할당량에 명시된 할당량이 적용됩니다.

소프트 할당량

AWS Firewall Manager 지역별 개체 수에 대한 기본 할당량이 있습니다. 이 할당량의 증가를 요청할 수 있습니다.

모든 정책 유형

Resource	리전별 기본 할당량
내 조직별 계정 AWS Organizations	다양. 계정으로 전송되는 초대 개수는 이 할당량을 기준으로 계산됩니다. 초대된 계정에서 초대를 거부하면 해당 카운트가 반환되고 관리 계정이 초대를 취소하거나 초대가 만료됩니다.
AWS Organizations에 속한 조직당 Firewall Manager 정책.	50 리전 사양 `Global` 및 `US East (N. Virginia) Region`은(는) 동일한 리전을 나타내며, 따라서 이 한도는 두 리전을 합친 모든 정책에 적용됩니다.
범위 내 조직당 Firewall Manager 정책당 조직 단위.	20

Resource	리전별 기본 할당량
개별 계정을 명시적으로 포함하거나 제외하는 경우 Firewall Manager 정책 범위에 속하는 계정.	200
개별 계정을 명시적으로 포함하거나 제외하지 않는 경우 Firewall Manager 정책 범위에 속하는 계정.	2,500
Firewall Manager 정책당 리소스를 포함하거나 제외하는 태그.	8
계정당 리소스 세트 수	20
리소스 세트당 리소스 수	100
방화벽 관리자 정책당 리소스 세트 수	5

AWS WAF 정책

Resource	리전별 기본 할당량
AWS WAF Firewall Manager 관리자 계정당 규칙 그룹 수	100
AWS WAF Firewall Manager 관리자 계정별 클래식 규칙 그룹	10
AWS WAF 정책별 규칙 그룹.	50

공통 보안 그룹 정책

Resource	리전별 기본 할당량.
정책당 기본 보안 그룹.	3
계정별 정책당 범위 내 Amazon VPC 인스턴스(공유 VPC 포함).	100

콘텐츠 감사 보안 그룹 정책

Resource	리전별 기본 할당량
정책당 보안 그룹 감사.	1

Resource	리전별 기본 할당량
애플리케이션별 애플리케이션 목록.	50
모든 트래픽을 허용하는 규칙에 대한 사용자 지정 관리 애플리케이션 목록.	1
정책 규칙별 사용자 지정 관리 애플리케이션 목록.	1
계정별 사용자 지정 관리 애플리케이션 목록.	10
프로토콜별 프로토콜 목록.	5
정책의 모든 설정에 대한 사용자 지정 관리 프로토콜 목록.	1
계정별 사용자 지정 관리 프로토콜 목록.	10

네트워크 ACL 정책

Resource	리전별 기본 할당량
첫 번째 또는 마지막 규칙에 사용된 네트워크 ACL 정책당 인바운드 규칙 수입니다. 예를 들어 최초 인바운드 규칙 5개와 마지막 인바운드 규칙 0개 또는 첫 번째 인바운드 규칙 2개와 마지막 규칙 3개를 사용할 수 있지만 처음 4개, 마지막 2개의 규칙을 둘 수는 없습니다.	5
첫 번째 또는 마지막 규칙에 사용된 네트워크 ACL 정책당 아웃바운드 규칙 수입니다. 예를 들어 최초 아웃바운드 규칙 5개와 마지막 아웃바운드 규칙 0개 또는 첫 번째 아웃바운드 규칙 2개와 마지막 3개의 마지막 아웃바운드 규칙을 만들 수 있지만 처음 4개, 마지막 2개의 규칙을 둘 수는 없습니다.	5

DNS 방화벽 정책

Resource	리전별 기본 할당량
DNS 방화벽 정책별 DNS 방화벽 규칙 그룹	2

하드 할당량

다음과 관련된 지역별 할당량은 변경할 AWS Firewall Manager 수 없습니다.

모든 정책 유형

Resource	리전별 할당량
한 AWS Organizations 조직에 둘 수 있는 최대 Firewall Manager 관리자 수입니다. 기본 관리자는 한 명이고 추가 Firewall Manager 관리자는 9명이어야 합니다.	10

AWS WAF 정책

Resource	리전별 할당량
AWS WAF 정책의 규칙 그룹에 대한 총 웹 ACL 용량 단위(WCU)입니다.	5,000

AWS WAF 클래식 정책

Resource	리전별 할당량
AWS WAF 정책별 클래식 규칙 그룹.	2:1 고객 생성 규칙 그룹과 1 AWS Marketplace 규칙 그룹
AWS WAF Firewall Manager AWS WAF 클래식 규칙 그룹별 클래식 규칙	10

보안 그룹 콘텐츠 감사 정책

Resource	리전별 할당량
정책의 모든 설정에 대한 Firewall Manager 관리형 애플리케이션 목록.	1
정책의 모든 설정에 대한 Firewall Manager 관리형 프로토콜 목록.	1

네트워크 방화벽 정책

Resource	리전별 할당량
단일 정책에 대해 자동으로 수정될 수 있는 VPC의 수.	1,000
단일 정책에 제공할 수 있는 IPV4 CIDR 수.	50

모니터링 AWS WAFAWS Firewall Manager, 및 AWS Shield Advanced

모니터링은 서비스의 안정성, 가용성 및 성능을 유지하는 데 중요한 부분입니다.

> **Note**
>
> Shield Advanced를 사용하여 Shield Advanced 리소스를 모니터링하고 발생 가능한 DDoS 이벤트를 식별하는 방법에 대한 자세한 내용은 AWS Shield을 참조하세요.

이러한 서비스를 모니터링하기 시작할 때 다음 질문에 대한 답변을 포함하는 모니터링 계획을 생성해야 합니다.

- 모니터링의 목표
- 모니터링할 리소스
- 이러한 리소스를 모니터링하는 빈도
- 사용할 모니터링 도구
- 모니터링 작업을 수행할 사람
- 문제 발생 시 알려야 할 대상

다음 단계에서는 다양한 시간과 다양한 부하 조건에서 성능을 측정하여 환경에서 일반 성능의 기준선을 설정합니다. 모니터링 AWS WAF시 Firewall Manager, Shield Advanced 및 관련 서비스는 과거 모니터링 데이터를 저장하여 현재 성능 데이터와 비교하고, 정상적인 성능 패턴 및 성능 이상을 식별하고, 문제 해결 방법을 고안할 수 있도록 합니다.

에 AWS WAF대해서는 최소한 다음 항목을 모니터링하여 기준을 설정해야 합니다.

- 허용된 웹 요청의 수
- 차단된 웹 요청의 수

주제

- 모니터링 도구
- 아마존을 통한 모니터링 CloudWatch

- 을 사용하여 AWS CloudTrail API 호출 로깅

모니터링 도구

AWS 모니터링 AWS WAF 및 모니터링에 사용할 수 있는 다양한 도구를 제공합니다 AWS Shield Advanced. 모니터링을 자동으로 수행하도록 구성할 수 있는 도구도 있지만, 수동 개입이 필요한 도구도 있습니다. 모니터링 작업은 최대한 자동화하는 것이 좋습니다.

자동 모니터링 도구

다음과 같은 자동 모니터링 도구를 사용하여 문제 발생 시 이를 AWS WAF AWS Shield Advanced 관찰하고 보고할 수 있습니다.

- 웹 ACL 트래픽 개요 대시보드 - AWS WAF 콘솔의 웹 ACL 페이지로 이동한 다음 트래픽 개요 탭을 열어 웹 ACL이 평가하는 웹 트래픽 요약에 액세스할 수 있습니다.

  트래픽 개요 대시보드는 애플리케이션 웹 트래픽을 평가할 때 AWS WAF 수집하는 Amazon CloudWatch 지표의 요약을 거의 실시간으로 제공합니다. 모든 웹 트래픽과 지능형 위협 완화 규칙 그룹에서 평가한 트래픽에 대한 요약을 볼 수 있습니다.

  자세한 내용은 웹 ACL 트래픽 개요 대시보드을 참조하거나 콘솔의 대시보드에서 확인하십시오.
- Amazon CloudWatch Alarms — 지정한 기간 동안 단일 지표를 관찰하고 일정 기간 동안 지정된 임계값을 기준으로 지표의 값을 기준으로 하나 이상의 작업을 수행합니다. 이 작업은 Amazon Simple Notification Service(Amazon SNS) 주제 또는 Amazon EC2 Auto Scaling 정책에 전송되는 알림입니다. 경보는 지속적인 상태 변경에 대한 작업만 호출합니다. CloudWatch 경보가 특정 상태에 있다는 이유만으로 경보가 작업을 호출하지는 않습니다. 경보는 지정된 기간 동안 변경되고 유지되어야 합니다. 자세한 내용은 다음을 사용하여 CloudFront활동 모니터링을 참조하십시오. CloudWatch

  > **Note**
  >
  > CloudWatch 에 대해서는 AWS Firewall Manager지표 및 경보가 활성화되지 않습니다.

  에 설명된 대로 Shield Advanced 지표를 AWS WAF 모니터링하고 보호하는 CloudWatch 데 사용할 수 있을 뿐만 아니라 보호된 리소스의 활동을 모니터링하는 데에도 사용해야 CloudWatch 합니다. 아마존을 통한 모니터링 CloudWatch 자세한 내용은 다음을 참조하십시오.

  - Amazon CloudFront 개발자 안내서를 사용하여 CloudFront CloudWatch 활동 모니터링

  - API Gateway 개발자 안내서 Amazon API Gateway에서의 로깅 및 모니터링
  - CloudWatch Elastic Load Balancing 사용 설명서의 애플리케이션 로드 밸런서에 대한 메트릭
  - AWS AppSync 개발자 안내서 모니터링 및 로깅
  - Amazon Cognito 개발자 안내서의 Amazon Cognito에서 로깅 및 모니터링
  - 로그로 스트리밍된 앱 러너 로그 보기 및 CloudWatch 개발자 가이드에 CloudWatch 보고된 앱 러너 서비스 지표 보기AWS App Runner
- Amazon CloudWatch Logs — AWS CloudTrail 또는 다른 소스에서 로그 파일을 모니터링, 저장 및 액세스합니다. 자세한 내용은 Amazon CloudWatch Logs란 무엇입니까? 를 참조하십시오. .
- Amazon CloudWatch Events — AWS 서비스를 자동화하고 시스템 이벤트에 자동으로 대응합니다. AWS 서비스의 이벤트는 거의 실시간으로 CloudWatch 이벤트로 전송되며, 이벤트가 작성한 규칙과 일치할 때 취할 자동 조치를 지정할 수 있습니다. 자세한 내용은 Amazon CloudWatch 이벤트란 무엇입니까? 를 참조하십시오.
- AWS CloudTrail 로그 모니터링 — 계정 간에 로그 파일을 공유하고, CloudTrail 로그 파일을 CloudWatch Logs로 전송하여 실시간으로 모니터링하고, Java로 로그 처리 애플리케이션을 작성하고, 전송 후 로그 파일이 변경되지 않았는지 확인합니다. CloudTrail 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 로그 파일 작업을 참조하십시오을 사용하여 AWS CloudTrail API 호출 로깅.
- AWS Config— AWS 리소스가 서로 어떻게 관련되어 있는지, 과거에 어떻게 구성되었는지를 포함하여 AWS 계정의 리소스 구성을 확인하여 시간이 지남에 따라 구성 및 관계가 어떻게 변하는지 확인할 수 있습니다.

수동 모니터링 도구

AWS WAF 모니터링의 또 다른 중요한 부분은 CloudWatch 경보에서 다루지 않는 항목을 수동으로 모니터링하는 것입니다. AWS Shield Advanced AWS WAF, Shield Advanced 및 기타 AWS Management Console 대시보드를 통해 AWS 환경 상태를 확인할 수 있습니다. CloudWatch 또한 웹 ACL 및 규칙에 대한 로그 파일도 확인하는 것이 좋습니다.

- 예를 들어 AWS WAF 대시보드를 보려면:
  - AWS WAF 웹 ACL 페이지의 요청 탭에서 총 요청 및 생성한 각 규칙과 일치하는 요청의 그래프를 볼 수 있습니다. 자세한 정보는 웹 요청 샘플 보기을 참조하세요.
- CloudWatch 홈 페이지에서 다음 내용을 확인하십시오.
  - 현재 경보 및 상태
  - 경보 및 리소스 그래프

- 서비스 상태

또한 를 CloudWatch 사용하여 다음 작업을 수행할 수 있습니다.

- 사용자 정의 대시보드를 생성하여 관심 있는 서비스를 모니터링
- 지표 데이터를 그래프로 작성하여 문제를 해결하고 추세 파악
- 모든 AWS 리소스 메트릭을 검색하고 찾아보십시오.
- 문제에 대해 알려주는 경보 생성 및 편집

아마존을 통한 모니터링 CloudWatch

Amazon을 사용하여 웹 요청과 웹 ACL 및 규칙을 모니터링할 수 있습니다. CloudWatch Amazon은 원시 데이터를 AWS WAF AWS Shield Advanced 수집하여 읽을 수 있는 거의 실시간 지표로 처리합니다. CloudWatch Amazon의 통계를 사용하여 웹 애플리케이션 또는 서비스 성능에 대한 관점을 얻을 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 내용을 참조하십시오. CloudWatch

> **Note**
>
> CloudWatch 지표 및 경보는 Firewall Manager에서 사용할 수 없습니다.

CloudWatch 알람 상태가 변경될 때 Amazon SNS 메시지를 보내는 Amazon 경보를 생성할 수 있습니다. 경보는 지정한 기간에 단일 메트릭을 감시하고 여러 기간에 지정된 임계값에 대한 메트릭 값을 기준으로 작업을 하나 이상 수행합니다. 이 작업은 Amazon SNS 주제 또는 Auto Scaling 정책으로 전송되는 알림입니다. 경보는 지속적인 상태 변경에 대한 조치만 호출합니다. CloudWatch 경보는 단순히 특정 상태에 있다는 이유만으로 조치를 호출하지 않습니다. 경보는 지정된 기간 동안 상태가 변경되고 유지되어야 합니다.

주제

- 지표 및 차원 보기
- AWS WAF 지표 및 차원
- AWS Shield Advanced 측정 항목
- AWS Firewall Manager 알림

지표 및 차원 보기

지표는 먼저 서비스 네임스페이스별로 그룹화된 다음 각 네임스페이스 내의 다양한 차원 조합별로 그룹화됩니다. AWS Firewall Manager 메트릭을 기록하지 않습니다.

- AWS WAF 네임스페이스는 `AWS/WAFV2`
- Shield Advanced의 네임스페이스는 `AWS/DDoSProtection`입니다

> **Note**
>
> AWS WAF 1분에 한 번 지표를 보고합니다.
> Shield Advanced는 이벤트 중에는 1분에 한 번 지표를 보고하고 다른 경우에는 덜 자주 보고합니다.

AWS WAF 및 에 대한 지표를 보려면 다음 절차를 사용하십시오 AWS Shield Advanced.

CloudWatch 콘솔을 사용하여 지표를 보려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 AWS Management Console 로그인하고 CloudWatch 콘솔을 엽니다.
2. 필요한 경우 해당 지역을 AWS 리소스가 위치한 지역으로 변경하십시오. 에서 미국 동부 (버지니아 북부) 지역을 선택합니다. CloudFront
3. 탐색 창의 지표에서 모든 지표를 선택한 다음 찾아보기 탭에서 서비스를 검색하십시오.

AWS CLI를 사용하여 지표를 보려면

- AWS/WAFV2의 경우 명령 프롬프트에서 다음 명령을 사용합니다.

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

Shield Advanced의 경우 명령 프롬프트에서 다음 명령을 사용합니다.

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF 지표 및 차원

AWS WAF 지표를 1분에 한 번 보고합니다. AWS WAF `AWS/WAFV2`네임스페이스에 지표와 차원을 제공합니다.

AWS WAF 콘솔의 웹 ACL의 트래픽 개요 탭에서 AWS WAF 지표에 대한 요약 정보를 볼 수 있습니다. 자세한 내용은 콘솔로 이동하거나 을 참조하십시오웹 ACL 트래픽 개요 대시보드.

웹 ACL, 규칙, 규칙 그룹 및 레이블에 대한 다음 지표를 볼 수 있습니다.

- 규칙 — 지표는 규칙 작업별로 그룹화됩니다. 예를 들어, Count 모드에서 규칙을 테스트하면 일치하는 규칙이 웹 ACL의 `Count` 지표로 나열됩니다.
- 규칙 그룹 — 규칙 그룹의 지표는 규칙 그룹 지표 아래에 나열됩니다.
- 다른 계정이 소유한 규칙 그룹 - 규칙 그룹 지표는 일반적으로 규칙 그룹 소유자만 볼 수 있습니다. 하지만 규칙에 대한 규칙 동작을 재정의하면 해당 규칙의 지표가 웹 ACL 지표 아래에 나열됩니다. 또한 모든 규칙 그룹에서 추가한 레이블은 웹 ACL 지표에 나열됩니다.

  이 범주의 규칙 그룹은 다른 계정에서 공유한 AWS 에 대한 관리형 규칙 AWS WAF AWS Marketplace 관리형 규칙 그룹다른 서비스에서 제공하는 규칙 그룹,, 및 규칙 그룹입니다.
- 레이블 - 평가 중에 웹 요청에 추가된 레이블은 웹 ACL 레이블 지표에 나열됩니다. 레이블이 자신의 규칙 및 규칙 그룹에 의해 추가되었는지 또는 다른 계정이 소유한 규칙 그룹의 규칙에 의해 추가되었는지에 관계없이 모든 레이블의 지표에 액세스할 수 있습니다.

주제

- 웹 ACL, 규칙 그룹, 규칙 지표 및 차원
- 레이블 지표 및 차원
- 무료 봇 가시성 지표 및 차원

웹 ACL, 규칙 그룹, 규칙 지표 및 차원

웹 ACL, 규칙 그룹, 규칙 지표

지표	설명
`AllowedRequests`	허용된 웹 요청의 수. 보고 기준: 0이 아닌 값이 있을 때.

지표	설명
	유효 통계: Sum
BlockedRequests	차단된 웹 요청의 수. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
CountedRequests	계수된 웹 요청의 수. 보고 기준: 0이 아닌 값이 있을 때. 계수된 웹 요청은 적어도 하나의 규칙과 일치하는 요청입니다. 요청 계수는 일반적으로 테스트에 사용됩니다. 유효 통계: Sum
CaptchaRequests	CAPTCHA 제어가 적용된 웹 요청 수입니다. 보고 기준: 0이 아닌 값이 있을 때. CAPTCHA 웹 요청은 CAPTCHA 작업 설정이 있는 규칙과 일치하는 요청입니다. 이 지표는 유효한 CAPTCHA 토큰이 있는지 여부에 관계없이 일치하는 모든 요청을 기록합니다. 유효 통계: Sum
RequestsWithValidCaptchaToken	CAPTCHA 제어가 적용되고 유효한 CAPTCHA 토큰이 있는 웹 요청 수. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum

지표	설명
CaptchasAttempted	CAPTCHA 퍼즐 챌린지에 대한 응답으로 최종 사용자가 제출한 솔루션 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
CaptchasSolved	제출된 CAPTCHA 퍼즐 솔루션 중 퍼즐을 성공적으로 해결한 횟수입니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
ChallengeRequests	챌린지 컨트롤이 적용된 웹 요청 수. 보고 기준: 0이 아닌 값이 있을 때. 챌린지 웹 요청은 Challenge 작업 설정이 있는 규칙과 일치하는 요청입니다. 이 지표는 유효한 챌린지 토큰이 있는지 여부에 관계없이 일치하는 모든 요청을 기록합니다. 유효 통계: Sum
RequestsWithValidChallengeToken	챌린지 제어가 적용되었고 유효한 챌린지 토큰이 있는 웹 요청의 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum

지표	설명
PassedRequests	전달된 요청의 수입니다. 규칙 그룹 규칙과 일치하지 않고 규칙 그룹 평가를 거치는 요청에만 사용됩니다. 보고 기준: 0이 아닌 값이 있을 때. 전달된 요청은 규칙 그룹에 포함된 어떠한 규칙과도 일치하지 않았던 요청입니다. 유효 통계: Sum

웹 ACL, 규칙 그룹, 규칙 차원

측정기준	설명
Region	Amazon CloudFront 배포를 제외한 모든 보호 리소스 유형에 필요합니다.
Rule	다음 중 하나입니다. • Rule의 지표 이름. • ALL: WebACL 또는 RuleGroup 내 모든 규칙을 나타냅니다. • Default_Action (WebACL차원과 결합한 경우에만)은 웹 ACL의 규칙 조치로 평가가 종료되지 않은 요청에 할당된 작업을 나타냅니다.
RuleGroup	RuleGroup 의 지표 이름.
WebACL	WebACL의 지표 이름.
Country	요청의 출처 국가. 이는 ISO(국제표준기구) 3166 표준에서 지정한 두 글자입니다. 예를 들어 US는 미국, UA는 우크라이나입니다. 요청에 X-Forwarded-For 헤더가 있는 경우 AWS WAF 는 해당 헤더를 사용하여 이 설정을 결정합니다. 그렇지 않으면 AWS WAF 이 클라이언트 IP의 국가를

측정기준	설명
	사용합니다. 이 결정은 원산지를 결정하기 위해 규칙에서 사용하는 모든 논리와 무관합니다. AWS WAF MaxMind GeoIP 데이터베이스를 사용하여 IP의 위치를 결정합니다.
`Attack`	웹 ACL에서 사용하는 규칙 및 규칙 그룹을 기반으로 요청에서 AWS WAF 식별된 공격 유형입니다. 규칙과 기준 AWS 관리 규칙 그룹의 규칙을 통해 공격 유형을 식별할 수 있습니다. 예를 들어 크로스 사이트 스크립팅(XSS) 규칙 매칭은 XSS 공격 유형을 식별하고 속도 기반 규칙은 대량 공격 유형을 식별합니다. 공격 유형은 일반적으로 웹 요청 평가를 종료한 규칙 유형을 나타냅니다.
`Device`	웹 요청의 `user-agent` 헤더에서 가져온 요청을 보낸 클라이언트의 장치 유형입니다.
`ManagedRuleGroup`	`ManagedRuleGroup` 의 지표 이름.
`ManagedRuleGroupRule`	해당 규칙 내의 `ManagedRuleGroup` 규칙이 일치했습니다.

레이블 지표 및 차원

웹 ACL에서 사용하는 규칙 및 관리형 규칙 그룹을 기준으로 평가하는 동안 요청에 추가된 레이블에 대한 지표입니다. 자세한 내용은 웹 요청의 레이블을 참조하세요.

단일 웹 요청의 경우 최대 100개의 레이블에 대한 지표를 AWS WAF 저장합니다. 웹 ACL 평가는 100개 이상의 레이블을 적용하고 100개 이상의 레이블과 일치시킬 수 있지만 지표에 처음 100개만 반영합니다.

라벨 지표

지표	설명
AllowedRequests	작업 설정 Allow이 적용된 웹 요청의 레이블 수입니다. 레이블은 웹 요청 평가 중 언제든지 추가될 수 있습니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
BlockedRequests	작업 설정 Block이 적용된 웹 요청의 레이블 수입니다. 레이블은 웹 요청 평가 중 언제든지 추가될 수 있습니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
CountedRequests	Count 작업 설정이 있는 규칙 그룹 규칙에 의해 웹 요청에 추가된 레이블 수입니다. 이 지표는 규칙 그룹 소유자, 즉 규칙 그룹 내 규칙에만 사용할 수 있습니다. 다른 경우에는 개수 레이블 지표가 요청에 적용된 종료 작업(예: Allow 또는 Block)으로 롤업됩니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
CaptchaRequests	종료 CAPTCHA 작업이 적용된 웹 요청의 레이블 수입니다. 레이블은 웹 요청 평가 중 언제든지 추가될 수 있습니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum

지표	설명
ChallengeRequests	종료 Challenge 작업이 적용된 웹 요청의 레이블 수입니다. 레이블은 웹 요청 평가 중 언제든지 추가될 수 있습니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
AllowRuleMatch	관련 레이블을 생성하고 Allow 작업을 통한 요청 평가를 종료한 일치하는 규칙의 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
BlockRuleMatch	관련 레이블을 생성하고 작업을 통한 요청 평가를 종료한 일치하는 규칙의 수. Block 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
CountRuleMatch	관련 레이블을 생성하고 Count 작업을 적용한 일치하는 규칙 수입니다. 동일한 레이블 및 작업으로 규칙이 여러 개 구성된 경우 요청 하나로 이 지표의 인스턴스가 여러 개 생성될 수 있습니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
CaptchaRuleMatch	관련 레이블을 생성하고 CAPTCHA 작업을 통한 요청 평가를 종료한 일치하는 규칙 수입니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum

지표	설명
ChallengeRuleMatch	관련 레이블을 생성하고 작업을 통한 요청 평가를 종료한 일치하는 규칙의 수입니다. Challenge 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
CaptchaRuleMatchWithValidToken	관련 레이블을 생성하고 비종료 CAPTCHA 작업을 적용한 일치하는 규칙의 수. 동일한 레이블 및 작업으로 규칙이 여러 개 구성된 경우 요청 하나로 이 지표의 인스턴스가 여러 개 생성될 수 있습니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
ChallengeRuleMatchWithValidToken	관련 레이블을 생성하고 비종료 작업을 Challenge 적용한 일치하는 규칙 수입니다. 동일한 레이블 및 작업으로 규칙이 여러 개 구성된 경우 요청 하나로 이 지표의 인스턴스가 여러 개 생성될 수 있습니다. 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum

라벨 차원

측정기준	설명
Region	Amazon CloudFront 배포를 제외한 모든 보호 리소스 유형에 필요합니다.
WebACL	WebACL의 지표 이름.

측정기준	설명
RuleGroup	RuleGroup 의 지표 이름. 지표 CountedRequests 에 사용됨.
LabelNamespace	요청에 추가된 레이블의 네임스페이스 접두사입니다.
Label	요청에 추가된 레이블의 이름입니다.
Context	레이블 추가의 컨텍스트로 사용된 관리형 규칙 그룹입니다. 예를 들어 토큰 관리 레이블의 awswaf:managed:token:accepted 컨텍스트는 요청 시 토큰 관리를 사용하는 AWS WAF 관리형 규칙 그룹(예: Bot Control 또는 ATP 관리 규칙 그룹) 입니다. 이 차원은 모든 레이블에 적용되는 것은 아닙니다.

무료 봇 가시성 지표 및 차원

웹 ACL에서 Bot Control을 사용하지 않는 경우 추가 비용 없이 Bot Control 관리 규칙 그룹을 웹 요청 샘플에 AWS WAF 적용합니다. 이를 통해 보호된 리소스로 들어오는 봇 트래픽을 파악할 수 있습니다. Bot Control에 대한 자세한 내용은 AWS WAF 봇 컨트롤 규칙 그룹을 참조하세요.

무료 봇 가시성 지표

지표	설명
SampleAllowedRequest	샘플링된 요청 중 작업이 수행된 요청 수. Allow 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
SampleBlockedRequest	작업이 있는 샘플 요청 수. Block 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
SampleCaptchaRequest	작업이 있는 샘플 요청 수. CAPTCHA

지표	설명
	보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
SampleChallengeRequest	작업이 있는 샘플 요청 수. Challenge 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum
SampleCountRequest	작업이 있는 샘플 요청 수. Count 보고 기준: 0이 아닌 값이 있을 때. 유효 통계: Sum

무료 봇 가시성 차원

측정기준	설명
Region	Amazon CloudFront 배포를 제외한 모든 보호 리소스 유형에 필요합니다.
WebACL	WebACL의 지표 이름.
BotCategory	웹 요청 레이블을 기반으로 탐지된 봇 카테고리의 이름입니다.
VerificationStatus	웹 요청 레이블을 기반으로 탐지된 봇 확인 상태의 이름입니다.
Signal	웹 요청 레이블을 기반으로 탐지된 봇 신호의 이름입니다.

AWS Shield Advanced 측정 항목

Shield Advanced는 보호하는 모든 리소스에 대한 Amazon CloudWatch 탐지, 완화 및 상위 기여자 지표를 게시합니다. 이러한 지표를 통해 리소스에 대한 CloudWatch 대시보드와 경보를 생성하고 구성할 수 있어 리소스 모니터링 능력이 향상됩니다.

Shield Advanced 콘솔은 기록되는 여러 지표에 대한 요약을 제공합니다. 자세한 내용은 DDoS 이벤트에 대한 가시성을 참조하세요.

애플리케이션 계층 보호를 위해 자동 애플리케이션 계층 DDoS 완화를 활성화하는 경우

지표 보고 위치

Shield Advanced는 다음에 대해 대해 미국 동부(버지니아 북부) 리전 `us-east-1`의 지표를 보고합니다.

- 글로벌 서비스 아마존 CloudFront 및 아마존 Route 53.
- 보호 그룹. 보호 그룹에 대한 자세한 내용은 AWS Shield Advanced 보호 그룹을 참조하세요.

다른 리소스 유형의 경우 Shield Advanced는 리소스 리전의 지표를 보고합니다.

메트릭 리포팅 타이밍

Shield Advanced는 진행 중인 이벤트가 없을 때보다 DDoS 이벤트가 발생하는 동안 더 자주 AWS 리소스에 CloudWatch 대한 지표를 Amazon에 보고합니다. Shield Advanced는 이벤트 중에는 1분에 한 번, 그리고 이벤트 종료 직후에 한 번 지표를 보고합니다.

진행 중인 이벤트가 없을 때 Shield Advanced는 지표를 하루에 한 번 리소스에 지정된 시간에 보고합니다. 이 정기 보고서는 지표를 활성 상태로 유지하고 사용자 지정 CloudWatch 알람 및 대시보드에서 사용할 수 있도록 합니다.

알람 권장 사항

주의가 필요한 상황임을 알려주는 경보를 생성하는 것이 좋습니다. 우선 보호 대상 리소스별로 `DDoSDetected` 탐지 지표가 0이 아닐 때 보고하는 경보를 만들 수 있습니다. 이 지표의 값이 0이 아니라고 해서 반드시 DDoS 공격이 진행 중임을 의미하지는 않지만, 지표가 이 상태일 때는 리소스 상태를 자세히 살펴보는 것이 좋습니다.

요청 폭주에 대비하여 애플리케이션 상태 및 웹 요청 볼륨 등의 요인도 고려하는 복합 검사에 대한 경보를 생성하는 것이 좋습니다. 다양한 공격 벡터 차원에 대한 트래픽 볼륨을 기반으로 보고하는 나머지

세 가지 지표에 대해 경보를 울리도록 선택할 수 있습니다. 애플리케이션의 용량을 고려하여 트래픽이 애플리케이션 한도에 근접할 때 경보를 보내게 하면 불필요한 잡음이 너무 심하지 않게 필요에 따라 알림을 보내는 규칙 세트를 만들 수 있습니다.

주제

탐지 지표

Shield Advanced는 `AWS/DDoSProtection` 네임스페이스의 지표와 차원을 제공합니다.

탐지 지표

지표	설명
`DDoSDetected`	DDoS 이벤트가 특정 Amazon 리소스 이름(ARN)에 진행 중인지 여부를 나타냅니다. 이 지표는 이벤트 중에 0이 아닌 값을 가집니다.
`DDoSAttackBitsPerSecond`	특정 Amazon 리소스 이름(ARN)에 대한 DDoS 이벤트에서 관찰되는 비트 수입니다. 이 지표는 네트워크 및 전송 계층(계층 3 또는 계층 4) DDoS 이벤트에 대해서만 사용할 수 있습니다. 이 지표는 이벤트 중에 0이 아닌 값을 가집니다. 단위: 비트
`DDoSAttackPacketsPerSecond`	특정 Amazon 리소스 이름(ARN)에 대한 DDoS 이벤트에서 관찰되는 패킷 수입니다. 이 지표는 네트워크 및 전송 계층(계층 3 또는 계층 4) DDoS 이벤트에 대해서만 사용할 수 있습니다. 이 지표는 이벤트 중에 0이 아닌 값을 가집니다. 단위: 패킷

지표	설명
DDoSAttackRequestsPerSecond	특정 Amazon 리소스 이름(ARN)에 대한 DDoS 이벤트에서 관찰되는 요청 수입니다. 이 지표는 계층 7 DDoS 이벤트에만 사용할 수 있습니다. 이 지표는 가장 중요한 계층 7 이벤트에 대해서만 보고됩니다. 이 지표는 이벤트 중에 0이 아닌 값을 가집니다. 단위: 요청

Shield Advanced는 다른 차원 없이 DDoSDetected 지표를 게시합니다. 나머지 탐지 지표에는 다음 목록의 공격 유형에 해당하는 AttackVector 차원이 포함됩니다.

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection
- SNMPReflection
- SSDPReflection
- SYNFlood
- UDPFragment
- UDPTraffic
- UDPReflection

완화 지표

Shield Advanced는 AWS/DDoSProtection 네임스페이스의 지표와 차원을 제공합니다.

완화 지표

지표	설명
VolumePacketsPerSecond	탐지된 이벤트에 대한 응답으로 배포된 완화 기능을 통해 삭제되거나 전달된 초당 패킷 수입니다. 단위: 패킷

완화 차원

측정기준	설명
ResourceArn	Amazon 리소스 이름(ARN)
MitigationAction	적용된 완화 조치의 결과입니다. 가능한 값은 Pass 또는 Drop입니다.

상위 기여자 지표

Shield Advanced는 AWS/DDoSProtection 네임스페이스에서 메트릭을 제공합니다.

상위 기여자 지표

지표	설명
VolumePacketsPerSecond	상위 기여자의 초당 패킷 수입니다. 단위: 패킷
VolumeBitsPerSecond	상위 기여자의 초당 비트 수입니다. 단위: 비트

Shield Advanced는 이벤트 기여자를 특징짓는 차원 조합별로 상위 기여자 지표를 게시합니다. 상위 기여자 지표에는 다음과 같은 차원 조합을 사용할 수 있습니다.

- `ResourceArn`, `Protocol`
- `ResourceArn`, `Protocol`, `SourcePort`
- `ResourceArn`, `Protocol`, `DestinationPort`
- `ResourceArn`, `Protocol`, `SourceIp`
- `ResourceArn`, `Protocol`, `SourceAsn`
- `ResourceArn`, `TcpFlags`

상위 기여자 차원

측정기준	설명
`ResourceArn`	Amazon 리소스 이름(ARN).
`Protocol`	IP 프로토콜 이름(`TCP` 또는 `UDP`)입니다.
`SourcePort`	소스 TCP 또는 UDP 포트입니다.
`DestinationPort`	대상 TCP 또는 UDP 포트입니다.
`SourceIp`	소스 IP 주소.
`SourceAsn`	소스 Autonomous System Number(ASN).
`TcpFlags`	TCP 패킷에 있는 플래그의 조합으로, 대시(`-`)로 구분됩니다. 모니터링되는 플래그는 `ACK`, `FIN`, `RST`, `SYN`입니다. 이 차원 값은 항상 알파벳순으로 정렬되어 표시됩니다. 예를 들면 `ACK-FIN-RST-SYN` , `ACK-SYN` 및 `FIN-RST`입니다.

AWS Firewall Manager 알림

AWS Firewall Manager 지표를 기록하지 않으므로 Firewall Manager 전용 Amazon CloudWatch 경보를 생성할 수 없습니다. 하지만 잠재적 공격을 알리도록 Amazon SNS 알림을 구성할 수 있습니

다. Firewall Manager에서 Amazon SNS 알림을 생성하려면 4단계: Amazon SNS 알림 및 아마존 CloudWatch 경보를 구성합니다.을 참조하세요.

을 사용하여 AWS CloudTrail API 호출 로깅

AWS WAF AWS Shield Advanced, 및 서비스와 AWS Firewall Manager 통합되어 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업의 기록을 제공하는 AWS 서비스입니다. CloudTrail Shield Advanced 또는 Firewall Manager 콘솔에서 오는 호출과 Shield Advanced 또는 Firewall Manager API에 대한 코드 호출에서 오는 호출을 포함하여 이러한 서비스에 대한 API 호출 중 일부를 이벤트로 캡처합니다. AWS WAF AWS WAF트레일을 생성하면, Shield Advanced 또는 Firewall Manager에 대한 AWS WAF이벤트를 포함하여 Amazon S3 버킷으로 이벤트를 지속적으로 전송할 수 있습니다. CloudTrail 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 가장 최근 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 이러한 서비스에 대한 요청, 요청한 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

구성 및 활성화 방법을 CloudTrail 포함하여 자세한 내용은 사용 AWS CloudTrail 설명서를 참조하십시오.

CloudTrail 계정을 만들 AWS 계정 때 활성화됩니다. 지원되는 이벤트 활동이 Shield Advanced 또는 Firewall Manager에서 AWS WAF발생하는 경우 해당 활동은 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. 에서 최근 이벤트를 보고, 검색하고, 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

AWS 계정, Shield Advanced 또는 Firewall Manager에 대한 AWS WAF이벤트를 포함하여 귀하의 이벤트에 대한 지속적인 기록을 보려면 트레일을 생성하십시오. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 리전에 추적이 적용됩니다. 트레일은 AWS 파티션에 있는 모든 지역의 이벤트를 기록하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

AWS WAF 에 있는 정보 AWS CloudTrail

모든 AWS WAF 작업은 AWS WAF API 참조에 의해 AWS CloudTrail 기록되고 문서화됩니다. 예를 들어 `ListWebACL`, `UpdateWebACL`, 를 호출하고 CloudTrail 로그 파일에 항목을 `DeleteWebACL` 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 신원 정보를 이용하면 다음을 쉽게 알아볼 수 있습니다.

- 요청을 루트 사용자 보안 인증으로 했는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부
- 요청이 다른 AWS 서비스에 의해 이루어졌는지 여부

자세한 내용은 CloudTrail사용자 ID 요소를 참조하십시오.

예: 로그 파일 항목 AWS WAF

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. AWS CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 추적이 아니므로 특정 순서로 표시되지 않습니다.

다음은 AWS WAF 웹 ACL 작업에 대한 CloudTrail 로그 항목의 예입니다.

예: 에 대한 CloudTrail 로그 입력 `CreateWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
```

```
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF",
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
```

```
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    }
  },
  "responseElements": {
    "summary": {
      "name": "foo",
      "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
      "description": "foo",
      "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

예: 에 대한 CloudTrail 로그 입력 GetWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AssumedRole",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AssumedRole",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
```

```
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:18:28Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "GetWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "webacl"
  },
  "responseElements": null,
  "requestID": "f2db4884-4eeb-490c-afe7-67cbb494ce3b",
  "eventID": "7d563cd6-4123-4082-8880-c2d1fda4d90b",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

예: 에 대한 CloudTrail 로그 입력 UpdateWebACL

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
```

```
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": ""us-east-1,
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
```

```
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```


예: 에 대한 CloudTrail 로그 입력 `DeleteWebACL`


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
```

```
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

예: AWS WAF 클래식 로그 파일 항목

AWS WAF 클래식은 의 이전 AWS WAF버전입니다. 자세한 내용은 AWS WAF 클래식을 참조하세요.

로그 항목은 `CreateRule`, `GetRule`, `UpdateRule` 및 `DeleteRule` 작업을 보여 줍니다.

```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
```

```
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [

          ],
          "name": "0923ab32-7229-49f0-a0e3-66c81example"
        },
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample"
      },
      "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
      "eventID": "923f4321-d378-4619-9b72-4605bexample",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:22Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "GetRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
      },
      "responseElements": null,
```

```
    "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
    "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAIEP4IT4TPDEXAMPLE",
      "arn": "arn:aws:iam::777777777777:user/nate",
      "accountId": "777777777777",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "nate"
    },
    "eventTime": "2016-04-25T21:35:13Z",
    "eventSource": "waf.amazonaws.com",
    "eventName": "UpdateRule",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
      "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
      "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
      "updates": [
        {
          "predicate": {
            "type": "SizeConstraint",
            "dataId": "9239c032-bbbe-4b80-909b-782c0example",
            "negated": false
          },
          "action": "INSERT"
        }
      ]
    },
    "responseElements": {
      "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
    },
    "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
    "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
```

```
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:28Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "DeleteRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example",
        "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
      },
      "responseElements": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example"
      },
      "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
      "eventID": "a3236565-1a1a-4475-978e-81c12example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    }
  ]
}
```


AWS Shield Advanced 에 있는 정보 CloudTrail

AWS Shield Advanced 는 다음 작업을 CloudTrail 로그 파일에 이벤트로 기록할 수 있습니다.

- ListAttacks
- DescribeAttack
- CreateProtection
- DescribeProtection

- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자 보안 인증으로 했는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증 정보를 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail 사용자 ID 요소를 참조하십시오.

예제: Shield Advanced 로그 파일 항목

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `DeleteProtection` 및 `ListProtections` 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123 1",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
     "accountId": "123456789012",
     "accessKeyId": "1AFGDT647FHU83JHFI81H",
     "userName": "SampleUser"
   },
   "eventTime": "2018-01-10T21:31:14Z",
```

```
    "eventSource": "shield.amazonaws.com",
    "eventName": "DeleteProtection",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": {
      "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
    },
    "responseElements": null,
    "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
    "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "12345678909876543212 3",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```

AWS Firewall Manager 에 있는 정보 CloudTrail

AWS Firewall Manager 는 다음 작업을 CloudTrail 로그 파일에 이벤트로 기록할 수 있습니다.

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy
- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트 사용자 보안 인증으로 했는지 여부
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증 정보를 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail 사용자 ID 요소를 참조하십시오.

예제: Firewall Manager 로그 파일 항목

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함되어 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 `GetAdminAccount --> 작업`을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
 {
                "eventVersion": "1.05",
                "userIdentity": {
                                "type": "AssumedRole",
                                "principalId": "123456789098765432123 1",
                                "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                                "accountId": "123456789012",
                                "accessKeyId": "1AFGDT647FHU83JHFI81H",
                                "sessionContext": {
                                                "attributes": {
                                                                "mfaAuthenticated":
 "false",
                                                                "creationDate":
 "2018-04-14T02:51:50Z"
                                                               },
                                                "sessionIssuer": {
                                                                "type": "Role",
                                                                "principalId":
 "123456789098765432123 1",
                                                                "arn":
 "arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
 "123456789012",
                                                                "userName": "Admin"
                                                                 }
                                                  }
                                },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "72.21.198.65",
                "userAgent": "console.amazonaws.com",
                "requestParameters": null,
                "responseElements": null,
                "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
                "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
                "eventType": "AwsApiCall",
                "apiVersion": "2018-01-01",
                "recipientAccountId": "123456789012"
    }
```

AWS WAF 및 AWS Shield Advanced API 사용

이 섹션에서는 Shield Advanced에서 매치 세트, 규칙, 웹 ACL을 생성하고 관리하기 위해 및 Shield Advanced API에 요청하는 방법과 Shield Advanced에서의 AWS WAF 구독 및 보호 기능을 설명하는 방법을 설명합니다. AWS WAF 이 단원에서는 요청의 구성 요소, 응답의 내용, 요청 인증 방법에 대해 알아봅니다.

주제

AWS SDK 사용

SDK를 AWS 제공하는 언어를 사용하는 경우 API를 통해 작업하려고 하지 말고 SDK를 사용하세요. SDK를 사용하면 인증이 더 간단하고, 개발 환경과 쉽게 통합되며, Shield Advanced 명령에 쉽게 액세스할 수 AWS WAF 있습니다. AWS SDK에 대한 자세한 내용은 주제를 참조하십시오도구 다운로드. 서비스를 사용하기 위한 계정 설정

AWS WAF 또는 Shield Advanced에 HTTPS 요청 보내기

AWS WAF Shield Advanced 요청은 RFC 2616에 정의된 HTTPS 요청입니다. 다른 HTTP 요청과 마찬가지로 Shield Advanced에 AWS WAF 대한 요청에는 요청 메서드, URI, 요청 헤더 및 요청 본문이 포함됩니다. 응답에는 HTTP 상태 코드, 응답 헤더, 그리고 때로는 응답 본문이 포함됩니다.

요청 URI

요청 URI는 항상 슬래시(/)입니다.

HTTP 헤더

AWS WAF Shield Advanced를 사용하려면 HTTP 요청 헤더에 다음 정보가 필요합니다.

호스트(필수)

리소스가 생성되는 위치를 지정하는 엔드포인트입니다. 엔드포인트에 대한 자세한 내용은 AWS 서비스 엔드포인트를 참조하세요. 예를 들어, CloudFront 배포의 Host 헤더 값은 다음과 같습니다waf.amazonaws.com:443. AWS WAF

x-amz-date 또는 날짜 (필수)

Authorization 헤더에 포함된 서명을 만드는 데 사용되는 날짜입니다. 다음 예와 같이 ISO 8601 표준 형식을 사용하여 UTC 시간으로 날짜를 지정합니다.

```
x-amz-date: 20151007T174952Z
```

x-amz-date 또는 Date를 포함시켜야 합니다. 일부 HTTP 클라이언트 라이브러리에서는 Date 헤더를 설정할 수 없습니다. x-amz-date헤더가 있는 경우 AWS WAF 요청을 인증할 때 Date 헤더를 모두 무시합니다.

타임스탬프는 요청을 받은 AWS 시스템 시간으로부터 15분 이내여야 합니다. 그렇지 않으면 다른 사람이 요청을 재생하는 것을 방지하기 위해 RequestExpired 오류 코드와 함께 요청이 실패합니다.

권한 부여(필수)

요청 인증에 필요한 정보. 이 헤더를 구성하는 방법에 대한 자세한 내용은 요청 인증(을)를 참조하세요.

X-Amz-Target(필수)

AWSWAF_ 또는 AWSShield_, 문장 부호 없는 API 버전, 마침표(.), 작업 이름을 연결합니다. 예를 들면 다음과 같습니다.

AWSWAF_20150824.CreateWebACL

Content-Type(조건부)

다음 예와 같이 콘텐츠 유형이 JSON 및 JSON의 버전임을 지정합니다.

```
Content-Type: application/x-amz-json-1.1
```

조건: POST 요청에 대해 필수 사항입니다.

Content-Length(조건부)

RFC 2616에 따른 메시지의 길이(헤더 제외).

조건: 요청 본문 자체에 정보가 포함되어 있는 경우에 필요합니다(대부분의 도구 키트는 이 헤더를 자동으로 추가함).

다음은 AWS WAF에서 웹 ACL을 생성하기 위한 HTTP 요청의 헤더 예제입니다.

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.CreateWebACL
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 231
Connection: Keep-Alive
```

HTTP 요청 본문

많은 AWS WAF Shield Advanced API 작업을 수행하려면 요청 본문에 JSON 형식의 데이터를 포함해야 합니다.

다음 예제 요청에서는 간단한 JSON 문을 사용하여 IP 주소 192.0.2.44(CIDR 표기법에서는 192.0.2.44/32로 표시됨)을 포함하도록 `IPSet`(을)를 업데이트합니다.

```
POST / HTTP/1.1
Host: waf.amazonaws.com:443
X-Amz-Date: 20151007T174952Z
Authorization: AWS4-HMAC-SHA256
               Credential=AccessKeyID/20151007/us-east-2/waf/aws4_request,
               SignedHeaders=host;x-amz-date;x-amz-target,

 Signature=145b1567ab3c50d929412f28f52c45dbf1e63ec5c66023d232a539a4afd11fd9
X-Amz-Target: AWSWAF_20150824.UpdateIPSet
Accept: */*
Content-Type: application/x-amz-json-1.1; charset=UTF-8
Content-Length: 283
Connection: Keep-Alive
```

```
{
   "ChangeToken": "d4c4f53b-9c7e-47ce-9140-0ee5ffffffff",
   "IPSetId": "69d4d072-170c-463d-ab82-0643ffffffff",
   "Updates": [
      {
         "Action": "INSERT",
         "IPSetDescriptor": {
            "Type": "IPV4",
            "Value": "192.0.2.44/32"
         }
      }
   ]
}
```

HTTP 응답

모든 AWS WAF 및 Shield Advanced API 작업은 응답에 JSON 형식의 데이터를 포함합니다.

다음은 HTTP 응답의 몇 가지 중요 헤더와 해당되는 경우 애플리케이션에서 이 헤더를 처리하는 방법입니다.

HTTP/1.1

이 헤더 다음에는 상태 코드가 이어집니다. 상태 코드 200은 작업 성공을 나타냅니다.

타입: 문자열

x-amzn- RequestId

요청을 고유하게 식별하는 값으로, AWS WAF 또는 Shield Advanced에서 생성한 값입니다 (예: K2QH8DN0U907N97FNA2GDLL80BVV4KQNS05AEMVJF66Q9ASUAAJG 에 문제가 있는 AWS WAF 경우 이 값을 사용하여 문제를 해결할 AWS 수 있습니다.

타입: 문자열

Content-Length

응답 본문의 길이(바이트)입니다.

타입: 문자열

날짜

Shield Advanced가 AWS WAF 응답한 날짜 및 시간 (예: 2015년 10월 7일 수요일 12:00:00 GMT)

타입: 문자열

오류 응답

요청에 오류가 발생할 경우 HTTP 응답에는 다음 값이 포함됩니다.

- JSON 오류 문서 - 응답의 본문
- Content-Type
- 적용되는 3xx, 4xx 또는 5xx HTTP 상태 코드

다음은 JSON 오류 문서의 예입니다.

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

요청 인증

SDK를 AWS 제공하는 언어를 사용하는 경우 SDK를 사용하는 것이 좋습니다. 모든 AWS SDK는 요청에 서명하는 프로세스를 크게 단순화하고 AWS WAF 또는 Shield Advanced API를 사용할 때와 비교할 때 상당한 시간을 절약합니다. 또한 SDK는 개발 환경에 쉽게 통합되며 관련 명령에 쉽게 액세스할 수 있습니다.

AWS WAF Shield Advanced에서는 요청에 서명하여 보내는 모든 요청을 인증해야 합니다. 요청에 서명하려면 입력을 바탕으로 해시 값을 반환하는 암호화 해시 함수를 사용하여 디지털 서명을 계산합니다. 입력에는 요청 텍스트와 보안 액세스 키가 포함됩니다. 해시 함수는 요청에 서명으로 포함하는 해시 값을 반환합니다. 서명은 요청에서 `Authorization` 헤더의 일부입니다.

요청을 받은 후, AWS WAF 또는 Shield Advanced는 요청에 서명할 때 사용한 것과 동일한 해시 함수 및 입력을 사용하여 서명을 재계산합니다. 결과 서명이 요청의 서명과 일치하면 Shield Advanced가 요청을 처리합니다. AWS WAF 그렇지 않으면 요청이 거부됩니다.

AWS WAF Shield Advanced는 AWS 시그니처 버전 4를 사용한 인증을 지원합니다. 서명을 계산하기 위한 프로세스는 다음 세 작업으로 나뉠 수 있습니다.

작업 1: 정식 요청 생성

https://docs.aws.amazon.com/general/latest/gr/sigv4-create-canonical-request.html의Amazon Web Services 일반 참조작업 1: Signature Version 4에 대한 정식 요청 생성에 설명되어 있는 대로 정규 형식으로 HTTP 요청을 생성합니다.

작업 2: 서명할 문자열 생성

암호화 해시 함수에 대한 입력 값 중 하나로 사용할 문자열을 만듭니다. 서명할 문자열은 다음 값을 연결한 문자열입니다.

- 해시 알고리즘의 이름
- 요청 날짜
- 자격 증명 범위 문자열
- 이전 작업에서 정규화된 요청

자격 증명 범위 문자열 자체는 날짜, 리전 및 서비스 정보를 연결한 것입니다.

`X-Amz-Credential` 파라미터에 대해 다음을 지정합니다.

- 요청 `us-east-2`을 전송할 엔드포인트에 대한 코드
- 서비스 약어에 대한 `waf`

예:

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

작업 3: 서명 생성

두 개의 입력 문자열을 허용하는 암호화 해시 함수를 사용하여 요청에 대한 서명을 생성합니다.

- 작업 2의 서명할 문자열.
- 파생된 키 파생된 키는 보안 액세스 키로 시작해서 자격 증명 범위 문자열을 사용하여 일련의 해시 기반 메시지 인증 코드(HMAC)를 만들어 계산됩니다.

관련 정보

다음의 관련 리소스는 이 서비스를 이용할 때 도움이 될 수 있습니다.

AWS WAF AWS Shield Advanced, 및 에 사용할 수 있는 리소스는 다음과 같습니다 AWS Firewall Manager.

- 구현 지침 AWS WAF — 기존 및 새 웹 애플리케이션을 AWS WAF 보호하기 위한 구현을 위한 최신 권장 사항이 포함된 기술 문서
- AWS 토론 포럼 — 이 서비스 및 기타 서비스와 관련된 기술적인 질문을 논의하기 위한 커뮤니티 기반 포럼입니다. AWS
- AWS WAF 토론 포럼 — 개발자가 관련된 기술적 질문에 대해 토론할 수 있는 커뮤니티 기반 포럼입니다. AWS WAF
- Shield Advanced 토론 포럼 – Shield Advanced에 관련된 기술적 질문을 논의할 수 있는 개발자를 위한 커뮤니티 기반 포럼입니다.
- AWS WAF 제품 정보 — 기능 AWS WAF, 가격 등 관련 정보를 제공하는 기본 웹 페이지입니다.
- Shield Advanced 제품 정보 – 기능, 요금 등 Shield Advanced에 대한 정보를 얻을 수 있는 기본 웹 페이지입니다.

Amazon Web Services에 사용할 수 있는 리소스는 다음과 같습니다.

- 수업 및 워크숍 — 역할 기반 및 전문 과정에 대한 링크와 함께 AWS 기술을 연마하고 실무 경험을 쌓는 데 도움이 되는 자습형 실습을 제공합니다.
- AWS 개발자 센터 — 튜토리얼을 탐색하고, 도구를 다운로드하고, 개발자 이벤트에 대해 알아보십시오. AWS
- AWS 개발자 도구 — 애플리케이션 개발 및 관리를 위한 개발자 도구, SDK, IDE 툴킷 및 명령줄 도구에 대한 링크입니다. AWS
- 시작하기 리소스 센터 — 애플리케이션을 설치하고, AWS 커뮤니티에 가입하고 AWS 계정, 첫 번째 애플리케이션을 시작하는 방법을 알아보세요.
- 실습 튜토리얼 — 튜토리얼을 따라 step-by-step 첫 번째 애플리케이션을 시작하세요. AWS
- AWS 백서 — 아키텍처, 보안, 경제 등의 주제를 다루고 솔루션스 아키텍트 또는 기타 기술 전문가가 작성한 포괄적인 기술 AWS 백서 목록에 대한 링크입니다. AWS
- AWS Support 센터 — 사례 작성 및 관리를 위한 허브. AWS Support 포럼, 기술 FAQ, 서비스 상태 등과 같은 기타 유용한 리소스에 대한 링크도 포함되어 있습니다. AWS Trusted Advisor

- AWS Support— 클라우드에서 애플리케이션을 구축하고 실행하는 데 도움이 되는 one-on-one 신속한 지원 채널에 대한 AWS Support정보를 제공하는 기본 웹 페이지입니다.
- Contact Us(문의처) - AWS 결제, 계정, 이벤트, 침해 및 기타 문제에 대해 문의할 수 있는 중앙 연락 창구입니다.
- AWS 사이트 약관 — 당사의 저작권 및 상표, 사용자 계정, 라이선스, 사이트 액세스, 기타 주제에 대한 자세한 정보.

문서 기록

이 페이지에는 이 설명서의 중요한 변경 사항이 나열되어 있습니다.

서비스를 사용할 수 있는 AWS 지역에 서비스 기능이 점진적으로 출시되는 경우가 있습니다. 이 문서는 첫 번째 릴리스에 대해서만 업데이트됩니다. 리전 가용성에 대한 정보를 제공하거나 후속 리전 롤아웃을 발표하지 않습니다. 서비스 기능의 지역 가용성에 대한 자세한 내용과 업데이트에 대한 알림을 구독하려면 무엇이 새로워졌나요? 를 AWS 참조하십시오. .

변경 사항	설명	날짜
JSON 본문 파싱의 작동 방식을 명확히 하세요.	구문 분석 및 본문 파싱 폴백 동작을 AWS WAF 처리하는 방법을 명확히 하기 위해 JSON 본문 검사 적용 범위를 업데이트했습니다.	2024년 6월 25일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	Linux 운영 체제 규칙 세트를 업데이트했습니다.	2024년 6월 6일
AWS WAF 관리형 정책 변경	권한 설정에 명령문 ID (SID) 를 `WAFV2LoggingServiceRolePolicy` 업데이트하고 `AWSServiceRoleForWAFV2Logging` 추가했습니다.	2024년 6월 3일
AWS WAF 관리형 정책 변경 추적	AWS WAF 관리형 정책 `WAFV2LoggingServiceRolePolicy` 및 서비스 연결 역할에 대한 변경 사항 추적을 시작했습니다. `AWSServiceRoleForWAFV2Logging`	2024년 6월 3일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	Bot Control, ATP 및 ACFP 관리 규칙 그룹은 이제 버전이 지정되었으며 다른 버전의 관리	2024년 5월 29일

	형 규칙과 마찬가지로 버전 업데이트에 대한 SNS 알림을 제공합니다. AWS	
AWS 에 대한 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 POSIX 운영 체제 규칙 그룹에 대한 관리형 규칙. `AWSManagedRulesUnixRuleSet`	2024년 5월 28일
CAPTCHA및 조치 Challenge	브라우저 클라이언트에서 CAPTCHA 퍼즐을 실행하고 자동 챌린지를 실행하려면 HTTPS가 필요하다는 설명이 추가되었습니다.	2024년 5월 24일
아마존 시큐리티 레이크와의 통합	이제 Security Lake를 사용하여 웹 ACL 트래픽 데이터를 수집할 수 있습니다. 자세한 내용은 Amazon Security Lake 사용 설명서의 AWS 서비스에서 데이터 수집을 참조하십시오.	2024년 5월 22일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2024년 5월 21일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 SQLi 데이터베이스 규칙 그룹에 대한 관리형 규칙.	2024년 5월 14일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS 알려진 잘못된 입력 및 POSIX 운영 체제 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙.	2024년 5월 8일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS Windows 운영 체제 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙	2024년 5월 3일

AWS WAF 모바일 SDK 안드로이드 코틀린 코드 샘플	Kotlin 기반 Android 통합을 위한 예제 코드를 추가했습니다.	2024년 5월 2일
AWS WAF 지표, 추가된 차원 및 새 지표	AWS WAF 규칙 `ManagedRuleSetRule` 내 지표에 대한 새 측정기준과 레이블 지표의 일치된 규칙 작업에 대한 새 측정항목을 추가했습니다.	2024년 5월 2일
AWS Firewall Manager 네트워크 ACL 정책 지원	방화벽 관리자는 이제 방화벽 관리자 네트워크 ACL 정책을 통해 Amazon VPC 네트워크 액세스 제어 목록 (ACL) 관리를 지원합니다.	2024년 4월 25일
AWS Firewall Manager 보안 정책 업데이트	네트워크 ACL 관리 권한을 `FMSServiceRolePolicy` 추가하기 위한 업데이트.	2024년 4월 22일
업데이트된 상태 점검 지표 목록	상태 확인에 일반적으로 사용되는 지표 목록에서 일부 지표를 제거했습니다.	2024년 4월 16일
방화벽 관리자 보안 그룹 정책 업데이트	사용 감사 보안 그룹 정책을 업데이트하고 설명서를 개선했습니다. 사용 감사 정책 섹션과 모범 사례 및 제한에 대한 섹션을 참조하십시오.	2024년 4월 2일
업데이트된 봇 컨트롤 예제	목표 검사 수준을 나타내는 예제를 추가하고 모범 사례를 반영하도록 기존 예제를 업데이트했습니다.	2024년 3월 27일
ATP 예제가 업데이트되었습니다.	응답 검사 구성을 설명하는 예제를 추가하고 모범 사례를 반영하도록 기존 예제를 업데이트했습니다.	2024년 3월 27일

ACFP 예제가 업데이트되었습니다.	응답 검사 구성을 설명하는 예제가 추가되었습니다.	2024년 3월 27일
Amazon CloudWatch Logs 로그 스트림 한도 업데이트	AWS WAF 로그 로그 스트림에 로그를 게시하는 데 CloudWatch 더 이상 웹별 ACL 제한이 없습니다.	2024년 3월 27일
AWS Shield Advanced 애플리케이션 계층 (계층 7) 보호	애플리케이션 계층 탐지 및 완화, 웹 ACL 사용, 속도 기반 규칙, 자동 애플리케이션 계층 DDoS 완화에 대한 일반 및 모범 사례 지침이 업데이트되었습니다.	2024년 3월 14일
AWS 에 대한 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 IP 평판 규칙 그룹에 대한 관리형 규칙.	2024년 3월 13일
신체 검사 크기 제한 변경	AWS WAF 이제 일부 지역 리소스에 대해 더 큰 신체 검사 크기 제한을 지원합니다.	2024년 3월 7일
AWS WAF 요율 기반 규칙을 위한 구성 가능한 평가 창	이제 속도 기반 규칙이 요청을 계산하는 데 사용하는 기간을 1, 2, 5 또는 10분으로 구성할 수 있습니다. 기본값은 5이며, 이 릴리스 이전에는 유일한 옵션이었습니다.	2024년 2월 28일
및 에 대한 CAPTCHA 확장된 로깅 정보 Challenge	이제 최상위 수준 `captchaResponse` 및 `challengeResponse` 필드는 종료 여부에 관계없이 요청에 적용할 마지막 작업으로 채워집니다. 이전에는 이러한 필드가 종료 작업에만 입력되었습니다.	2024년 2월 22일

JavaScript 캡차 API 키 관리	이제 API를 통해 캡차 JS API 키를 삭제할 수 있습니다. AWS WAF	2024년 2월 6일
AWS WAF 캡차 퍼즐 오디오	CAPTCHA 퍼즐의 오디오 버전은 이제 여러 언어를 지원합니다.	2024년 2월 6일
AWS WAF 챌린지 및 캡차 토큰 라벨링	토큰 관리는 이제 CAPTCHA 토큰에 대한 라벨을 추가하고 챌린지 토큰용 토큰 라벨링을 개선했습니다.	2023년 12월 20일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS 알려진 잘못된 입력 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙.	2023년 12월 16일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 알려진 잘못된 입력 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙.	2023년 12월 14일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2023년 12월 6일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: AWS WAF Bot Control.	2023년 12월 5일
업데이트된 방화벽 관리자 AWS Config 사전 요구 사항	Firewall Manager 관리 역할 대신 사용자 지정 IAM 역할을 사용하는 경우 AWS Config 레코더가 Firewall Manager 리소스를 기록할 수 있도록 권한 정책이 허용되는지 확인해야 합니다. AWS Config	2023년 11월 17일

AWS WAF 콘솔 대시보드	콘솔에서 웹 ACL에 대한 모든 규칙 및 샘플 요청을 보기 위한 지침을 수정했습니다. AWS WAF	2023년 11월 17일
에 대한 관리형 규칙이 업데이트되었습니다. AWSAWS WAF	AWS AWS WAF 업데이트된 봇 제어 규칙 그룹에 대한 관리형 규칙.	2023년 11월 14일
AWS WAF 콘솔에 새 웹 ACL 대시보드가 추가되었습니다.	AWS WAF 콘솔의 웹 ACL 페이지에는 새 웹 트래픽 개요 대시보드가 있습니다.	2023년 11월 14일
ATP 관리형 규칙 그룹이 업데이트됨	`VolumetricIpFailedLoginResponseHigh` 및 `VolumetricSessionFailedLoginResponseHigh` 규칙에 대한 레이블 정보가 수정됨	2023년 11월 13일
ACFP 관리형 규칙 그룹이 업데이트됨	`VolumetricIPSuccessfulResponse` 및 `VolumetricSessionSuccessfulResponse` 규칙에 대한 레이블 정보가 수정됨	2023년 11월 13일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2023년 11월 2일
Shield Advanced 자동 애플리케이션 계층 DDoS 완화	Shield Advanced는 이제 DDoS 공격의 원인으로 알려진 IP 주소의 요청 양을 제한하는 속도 기반 규칙을 자동 완화 규칙 그룹에 유지합니다.	2023년 10월 31일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2023년 10월 30일
Bot Control 관리형 규칙 그룹에서 요청 CSP 신호 레이블이 제거됨	Bot Control 관리형 규칙 그룹에서 클라우드 서비스 제공업체(CSP)를 나타내는 신호 라벨이 제거되었습니다.	2023년 10월 28일
요청 CSP에 대한 Bot Control 관리형 규칙 그룹 신호 레이블	Bot Control 관리형 규칙 그룹 신호 레이블에 클라우드 서비스 제공업체(CSP)를 나타내는 레이블이 포함됩니다.	2023년 10월 27일
AWS WAF IAM 권한 정보가 업데이트되었습니다.	웹 ACL 연결을 관리하는 AWS WAF 작업의 경우 이제 정책 작업 섹션에 각 웹 애플리케이션 리소스 유형에 대한 권한 요구 사항이 나열됩니다.	2023년 10월 25일
수정된 웹 ACL에 대한 Firewall Manager 관리	연결되지 않은 웹 ACL의 관리를 활성화하면, Firewall Manager는 사용되지 않는 리소스의 일회성 정리에서 수정된 웹 ACL을 포함하지 않습니다.	2023년 10월 19일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 POSIX 운영 체제 규칙 그룹에 대한 관리형 규칙. `AWSManagedRulesUnixRuleSet`	2023년 10월 12일
AWS WAF 메트릭, 추가, 차원	AWS WAF 웹 ACL 지표를 보기 위한 새 측정기준을 추가했습니다.	2023년 10월 12일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2023년 10월 11일
AWS WAF 모바일 SDK 사양 업데이트	`storeTokenInCookieStorage` 작업을 `WAFTokenProvider` 에 추가했습니다.	2023년 10월 11일
예외 배포 - 관리형 규칙: AWSAWS WAF	AWS Managed Rules for는 알려진 잘못된 입력 규칙 그룹의 두 가지 정적 버전을 AWS WAF 출시하고 최신 정적 버전을 가리키도록 기본 버전을 업데이트했습니다.	2023년 10월 4일
AWS WAF HTML 엔티티는 텍스트 변환을 디코딩합니다.	HTML 엔터티 디코드 텍스트 변환 기능을 확장했습니다.	2023년 10월 4일
Firewall Manager 보안 그룹 공통 정책에 새 옵션이 추가됨	Firewall Manager는 이제 보안 그룹 참조를 복제본 보안 그룹에 배포할 수 있습니다.	2023년 10월 3일
AWS WAF JA3 지문 검사 추가	이제 Amazon CloudFront 배포 및 애플리케이션 로드 밸런서에 대해 웹 요청의 JA3 핑거프린트와 정확히 일치하도록 수행할 수 있습니다.	2023년 9월 26일
Firewall Manager 보안 그룹 정책 규칙 설정에 대한 업데이트	Firewall Manager는 이제 기본 보안 그룹에서 복제본 보안 그룹으로의 보안 그룹 참조를 지원합니다.	2023년 9월 25일

업데이트된 Shield Advanced 자동 애플리케이션 계층 DDoS 완화	이제 Firewall Manager는 자동 애플리케이션 계층 DDoS 완화 기능으로 구성된 Shield Advanced 정책에 대한 Application Load Balancer 리소스를 지원합니다.	2023년 9월 14일
에 대한 관리형 규칙이 업데이트되었습니다 AWS . AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: AWS WAF Bot Control.	2023년 9월 6일
AWS WAF 봇 컨트롤	Bot Control 관리형 규칙 그룹의 대상 보호 수준이 이제 IP 주소 간의 토큰 재사용을 검사합니다. 또한 이제 일부 봇 관련 활동을 탐지하기 위한 트래픽 통계에 대해 선택적 기계 학습 분석이 제공됩니다.	2023년 9월 6일
AWS WAF 모바일 SDK 사양 업데이트	`tokenRefreshDelaySec` 의 최소값, 최대값 및 기본값을 최소 300, 최대 600, 기본값 300에서 최소 88, 최대 300, 기본값 88로 낮췄습니다.	2023년 9월 5일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS AWS WAF 업데이트된 AWS WAF 봇 제어 규칙 그룹에 대한 관리형 규칙.	2023년 8월 30일
Shield Advanced 자동 애플리케이션 계층 DDoS 완화	자동 애플리케이션 레이어 DDoS 완화와 함께 사용하는 웹 ACL을 관리하는 AWS CloudFormation 데 사용하기 위한 지침이 추가되었습니다.	2023년 8월 30일

새로운 Firewall Manager 콘텐츠 감사 보안 그룹 정책 옵션	지나치게 허용적인 규칙 그룹을 감사하기 위한 새 옵션을 추가하고 콘솔 절차 설명을 개선했습니다.	2023년 8월 29일
새로운 Firewall Manager Shield 및 AWS WAF 정책 옵션	and AWS WAF Shield에서 연결되지 않은 웹 ACL의 관리를 활성화하면 Firewall Manager는 하나 이상의 리소스에서 웹 ACL을 사용할 경우에만 정책 범위 내의 계정에 웹 ACL을 생성합니다.	2023년 8월 9일
에 대한 관리형 규칙이 업데이트되었습니다. AWSAWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2023년 7월 26일
URI 경로의 속도 기반 규칙 집계	이제 속도 기반 규칙에 대해 사용자 지정 집계 키에서 URI 경로를 지정할 수 있습니다.	2023년 7월 19일
의 새 AWS WAF정책 규칙 옵션 AWS Firewall Manager	AWS Firewall Manager AWS WAF 웹 요청 본문 검사 크기 제한을 구성하기 위한 지원을 추가합니다.	2023년 7월 18일
AWS WAF 관리형 정책 변경	`AWSWAFFullAccessPolicy` , `AWSWAFConsoleFullAccess` `AWSWAFReadOnlyAccess` , 를 `AWSWAFConsoleReadOnlyAccess` 업데이트하여 보호할 수 있는 리소스 유형에 AWS Verified Access를 추가했습니다 AWS WAF.	2023년 6월 17일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 추가된 규칙 그룹에 대한 관리형 규칙AWSManagedRulesACFPRuleSet .	2023년 6월 13일
AWS WAF 사기 방지 계정 탈취 방지 (ATP) 업데이트	이제 정규식을 사용하여 ATP 관리형 규칙 그룹의 로그인 엔드포인트를 지정할 수 있습니다.	2023년 6월 13일
CAPTCHA API에 대한 새로운 정보 JavaScript	새 섹션에서는 CAPTCHA로 AWS WAF 요청에 응답할 때 사용자 지정 CAPTCHA 퍼즐을 제공하는 방법을 설명합니다.	2023년 6월 13일
새 ACFP 관리형 규칙 그룹	새 규칙 그룹 AWSManagedRulesACFPRuleSet 을 사용하여 사기성 계정 생성 시도를 탐지하고 차단합니다.	2023년 6월 13일
새로운 AWS WAF 사기 방지 계정 생성 사기 방지 (ACFP)	새로운 AWS WAF 사기 통제 계정 생성 사기 방지 (ACFP) 관리 규칙 그룹을 사용하여 사기성 계정 생성 시도를 탐지하고 차단할 수 있습니다. AWSManagedRulesACFPRuleSet 보호 CloudFront 배포를 사용하면 ACFP를 사용하여 최근에 실패한 계정 생성 시도를 너무 많이 제출한 클라이언트의 새 계정 생성 시도를 차단할 수도 있습니다.	2023년 6월 13일

AWS WAF 관리형 정책 변경	AWSWAFFullAccessPolicy , AWSWAFConsoleFullAccess AWSWAFReadOnlyAccess , 및 AWS App Runner 서비스에 대한 액세스 설정을 AWSWAFConsoleReadOnlyAccess 수정하도록 업데이트되었습니다.	2023년 6월 6일
Firewall Manager 보안 그룹 정책에 대한 제한 사항이 추가됨	공유 VPC가 나중에 공유되지 않는 경우 Firewall Manager는 연결된 계정의 복제본 보안 그룹을 삭제하지 않습니다.	2023년 6월 2일
새 AWS WAF 요청 구성 요소: Header order	이제 요청 내 정렬된 헤더 이름 목록과 일치시킬 수 있습니다.	2023년 5월 30일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	Linux 운영 체제 규칙 세트를 업데이트했습니다.	2023년 5월 22일
AWS WAF 규칙 섹션의 구성을 업데이트했습니다.	이제 규칙 문 목록이 명령문 유형별로 그룹화됩니다.	2023년 5월 16일
주제 이동: 속도 제한이 적용되는 IP 주소 목록	속도 기반 규칙에 의해 속도 제한이 적용되는 IP 주소 나열에 대한 주제가 이제 속도 기반 규칙 주제 하단에 포함됩니다.	2023년 5월 16일
속도 기반 규칙 관련 옵션이 확장됨	이제 IP 주소 이외의 집계 키를 기반으로 웹 요청의 속도를 제한할 수 있으며 키 조합을 사용하여 집계할 수 있습니다. 추가 집계 없이 범위 축소 문과 일치하는 모든 요청의 속도를 제한할 수도 있습니다.	2023년 5월 16일

Firewall Manager 할당량 증가	조직당 Firewall Manager 정책 수를 AWS Organizations 20개에서 50개로 늘렸습니다. 정책당 기본 보안 그룹의 최대 수를 1개에서 3개로 늘렸습니다. 최대 WCU 수를 소프트 할당량에서 하드 할당량으로 변경했습니다.	2023년 5월 5일
규칙 그룹당 최대 WCU가 증가됨	이제 지원 팀에 증가를 요청하지 않고도 규칙 그룹당 최대 5,000개의 웹 ACL 용량 단위(WCU)를 사용할 수 있습니다. 이 새 한도는 늘릴 수 없습니다.	2023년 5월 1일
AWS WAF 접두사가 있는 Amazon S3 로그 버킷 위치	AWS WAF 이제 Amazon S3 로그 버킷 이름에 접두사를 사용할 수 있습니다.	2023년 5월 1일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2023년 4월 28일
AWS 검증된 액세스 인스턴스에 대한 지원을 에 추가했습니다. AWS WAF	이제 AWS WAF 웹 ACL을 검증된 액세스 인스턴스와 연결할 수 있습니다. 이 변경 사항은 최신 버전의 Classic에서만 사용할 수 AWS WAF 있으며 AWS WAF Classic에서는 사용할 수 없습니다.	2023년 4월 28일
여러 Firewall Manager 관리자 작업에 대한 장이 개정됨	조직의 방화벽 리소스를 생성하고 관리할 여러 Firewall Manager 관리자를 이제 지정할 수 있습니다.	2023년 4월 24일
AWS Firewall Manager 관리형 정책 업데이트	`FMSServiceRolePolicy` 업데이트됨	2023년 4월 21일

CAPTCHA를 위한 새로운 JavaScript 클라이언트 애플리케이션 통합	이제 클라이언트 애플리케이션에서 CAPTCHA 퍼즐의 배치와 특성을 사용자 정의할 수 있습니다. JavaScript	2023년 4월 20일
애플리케이션 통합이 지능형 위협 통합으로 이름이 변경됨	클라이언트 애플리케이션 통합을 위한 기존 기능의 이름을 지능형 위협 통합으로 변경하여 새로운 CAPTCHA 애플리케이션 통합과 구분할 수 있도록 했습니다. JavaScript	2023년 4월 20일
1,500개가 넘는 웹 ACL WCU에 대한 가변 가격	웹 ACL에서 1,500개가 넘는 웹 ACL 용량 단위(WCU)를 사용할 경우 추가 비용이 발생하며, 이 비용은 웹 ACL WCU 사용량이 증가하거나 감소함에 따라 자동으로 조정됩니다. 웹 ACL의 최대 용량은 5,000WCU입니다.	2023년 4월 11일
웹 ACL당 최대 WCU가 증가됨	이제 지원 팀에 증가를 요청하지 않고도 웹 ACL당 최대 5,000개의 웹 ACL 용량 단위(WCU)를 사용할 수 있습니다. 이 새 한도는 늘릴 수 없습니다.	2023년 4월 11일
웹 ACL의 본체 검사 크기 제한 CloudFront	Amazon CloudFront 배포를 보호하는 웹 ACL의 경우 웹 ACL 구성에서 본문 검사 크기 제한을 최대 64KB까지 늘릴 수 있습니다.	2023년 4월 11일

신체 검사 크기가 다음과 같이 증가합니다. CloudFront	Amazon CloudFront 배포판의 최대 AWS WAF 신체 검사 크기 제한이 8KB에서 64KB로 늘어났습니다. 기본 검사 크기 CloudFront 제한은 16KB입니다.	2023년 4월 11일
의 새 AWS WAF정책 규칙 옵션 AWS Firewall Manager	AWS Firewall Manager AWS WAF 사기 통제 계정 탈취 방지(ATP) 및 AWS WAF 봇 제어 AWS 관리 규칙 그룹, Amazon S3 로깅 대상, 규칙 조치 재정의, 규칙 조치, CAPTCHA 토큰 도메인 목록에 대한 지원을 추가합니다. Challenge	2023년 4월 7일
Firewall Manager는 Amazon S3 버킷을 로깅을 위한 AWS WAF 로깅 대상으로 지원합니다.	이제 Amazon S3 버킷을 AWS WAF 정책의 로깅 대상으로 사용할 수 있습니다.	2023년 4월 7일
AWS WAF 관리형 정책 변경	AWSWAFFullAccessPolicy , AWSWAFConsoleFullAccess AWSWAFReadOnlyAccess , 및 보호할 수 있는 리소스 유형에 AWS App Runner 서비스를 AWSWAFConsoleReadOnlyAccess 추가하도록 AWS WAF업데이트되었습니다.	2023년 3월 30일

보안 그룹 정책 내 태그 사용에 대한 경고가 추가됨	정책에 조직의 태그 정책과 충돌하는 태그가 있는 경우 Firewall Manager는 기존 보안 그룹의 태그를 업데이트하거나 새 보안 그룹을 만들지 않습니다.	2023년 3월 28일
서비스 역할 정보 업데이트	Firewall Manager를 통해 서비스 역할을 사용하는 방법을 업데이트했습니다.	2023년 3월 8일
속도 기반 규칙의 속도 제한 수행 방식에 대한 정보가 수정됨	범위 축소 문이 포함된 속도 기반 규칙은 규칙의 범위 축소 문과 일치하는 요청만 속도를 제한합니다. 이전에는 속도가 제한된 IP 주소에 대한 모든 요청에 제한이 적용되었다고 설명했습니다.	2023년 3월 1일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 PHP 응용 프로그램 규칙 그룹에 대한 관리형 규칙.	2023년 2월 27일
에 대한 AWS App Runner 지원이 추가되었습니다. AWS WAF	이제 AWS WAF 웹 ACL을 AWS App Runner 서비스와 연결할 수 있습니다. 이 변경 사항은 최신 버전의 Classic에서만 사용할 수 AWS WAF 있으며 AWS WAF Classic에서는 사용할 수 없습니다.	2023년 2월 23일
에 대한 IAM 지침이 업데이트되었습니다. AWS Firewall Manager	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 내용은 IAM의 보안 모범 사례 섹션을 참조하세요.	2023년 2월 16일

에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS Managed Rules의 경우 Amazon CloudFront 배포를 보호하는 웹 ACL에 로그인 응답 검사를 `AWSManagedRulesATPRuleSet` 추가하도록 규칙 그룹을 AWS WAF 업데이트했습니다.	2023년 2월 15일
AWS WAF 사기 방지 계정 탈취 방지 (ATP) 로그인 응답 검사	보호된 CloudFront 배포의 경우 이제 ATP를 사용하여 최근에 실패한 로그인 시도를 너무 많이 제출한 클라이언트의 새 로그인 시도를 차단할 수 있습니다.	2023년 2월 15일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	핵심 규칙 집합을 업데이트했습니다.	2023년 1월 25일
지능형 위협 완화 모범 사례	Bot Control, ATP 및 기타 지능형 위협 완화 기능을 구현하기 위한 모범 사례를 제공하는 섹션을 추가했습니다.	2023년 1월 22일
HTTP/2 의사 헤더를 검사하는 방법	HTTP/2 의사 헤더를 해당 웹 요청 구성 요소로 매핑하는 섹션을 추가했습니다.	2023년 1월 20일
클래식에 대한 AWS WAF IAM 지침이 업데이트되었습니다.	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 설명은 IAM의 보안 모범 사례를 참조하세요.	2023년 1월 3일
에 대한 IAM 지침이 업데이트되었습니다. AWS WAF	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 설명은 IAM의 보안 모범 사례를 참조하세요.	2023년 1월 3일

에 대한 IAM 지침이 업데이트 되었습니다. AWS Shield	IAM 모범 사례에 따라 가이드가 업데이트되었습니다. 자세한 설명은 IAM의 보안 모범 사례를 참조하세요.	2023년 1월 3일
Amazon Route 53 Resolver DNS 방화벽 정책 업데이트	Amazon Route 53 Resolver DNS 방화벽 규칙 그룹 삭제에 대한 정보가 추가되었습니다.	2022년 12월 29일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	Linux 운영 체제 규칙 세트를 업데이트했습니다.	2022년 12월 15일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	핵심 규칙 집합을 업데이트했습니다.	2022년 12월 5일
Firewall Manager는 서비스로서의 Fortigate Cloud Native Firewall(CNF) 정책에 대한 지원을 추가합니다.	Firewall Manager는 이제 Fortigate CNF 정책을 지원합니다.	2022년 12월 2일
DNS 방화벽 정책에 대한 AWS Config 요구 사항이 제거되었습니다.	DNS 방화벽 정책의 경우, 이제 리소스 유형 EC2 VPC에 대해 Config를 활성화하기만 하면 됩니다.	2022년 11월 17일
AWS Firewall Manager 관리형 정책 업데이트	`FMSServiceRolePolicy` 섹션을 업데이트했습니다.	2022년 11월 15일
AWS WAF CAPTCHA 퍼즐을 위한 언어 옵션 확장	CAPTCHA 퍼즐에 이제 여러 언어로 작성된 지침이 제공됩니다. 각 오디오 퍼즐의 지침은 여전히 영어로만 제공됩니다.	2022년 11월 11일
리소스 세트에 대한 새로운 Firewall Manager 할당량	리소스 세트에 대한 새 할당량을 추가했습니다.	2022년 11월 8일

리소스 세트에 대한 지원을 추가함	리소스를 그룹화하는 리소스 세트를 생성하여 Firewall Manager 정책으로 관리할 수 있습니다.	2022년 11월 8일
네트워크 방화벽에서 방화벽을 가져오기 위한 지원을 추가함	이제 리소스 세트를 사용하여 네트워크 방화벽 정책에서 기존 방화벽을 가져오고 관리할 수 있습니다.	2022년 11월 8일
AWS Firewall Manager 관리형 정책 업데이트	`AWSFMAdminReadOnlyAccess` 섹션을 업데이트했습니다.	2022년 11월 2일
이제 지역 일치 문이 국가 및 리전에 대한 요청에 레이블을 추가합니다.	이제 지역 일치와 레이블 일치를 결합하여 리전 수준에서 지리적 요청 오리진을 관리할 수 있습니다.	2022년 10월 31일
최상위 섹션의 이름이 변경됨: 관리형 보호	이 섹션은 이제 마케팅 페이지에 맞게 AWS WAF 지능형 위협 완화로 명명되었습니다.	2022년 10월 27일
Bot Control 관리형 규칙 그룹의 새로운 대상 보호 수준	Bot Control 관리형 규칙 그룹은 이제 정교한 봇의 탐지 및 완화를 위한 추가 대상 규칙을 제공합니다. 이 보호 수준은 추가 요금 지불 시 이용할 수 있습니다.	2022년 10월 27일
토큰에 대한 새 섹션 AWS WAF	지능형 위협 완화를 위해 토큰을 AWS WAF 사용하는 방법을 이해하십시오.	2022년 10월 27일

Firewall Manager 네트워크 방화벽 정책 업데이트에 대한 중요 정보가 추가됨	Firewall Manager 정책을 업데이트하면, 정책을 통해 생성된 모든 네트워크 방화벽 정책이 Firewall Manager 정책의 네트워크 방화벽 정책 구성으로 업데이트됩니다.	2022년 10월 27일
규칙 그룹의 작업 재정의	이제 규칙 그룹에 있는 규칙의 작업을 임의의 규칙 작업 설정으로 재정의할 수 있습니다. 이전 Count 작업 재정의와 마찬가지로, 규칙 그룹의 모든 규칙과 개별 규칙에 재정의를 적용할 수 있습니다.	2022년 10월 27일
AWS WAF 새 Challenge 규칙 조치 옵션	Challenge를 사용하도록 규칙을 구성하여 브라우저에서 요청을 보내고 있는지 확인할 수 있습니다.	2022년 10월 27일
AWS WAF 보호된 여러 애플리케이션 간에 토큰을 공유할 수 있습니다.	웹 ACL에 대한 토큰 도메인 목록을 구성하여 여러 보호되는 애플리케이션 간에 토큰을 사용할 수 있도록 할 수 있습니다.	2022년 10월 27일
모든 헤더 사양은 대소문자를 구분하지 않습니다.	대소문자를 구분하지 않도록 모든 헤더 사양을 변경했습니다. 이는 단일 헤더 동작과 일치합니다.	2022년 10월 26일
AWS Firewall Manager 관리형 정책 변경	`AWSFMAdminFullAccess` 에 대한 수정.	2022년 10월 21일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	알려진 잘못된 입력 규칙 그룹을 업데이트했습니다.	2022년 10월 20일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	알려진 잘못된 입력 규칙 그룹을 업데이트했습니다.	2022년 10월 5일

AWS WAF 모바일 SDK 사양 업데이트	`tokenRefreshDelaySec` 의 기본값을 600(10분)에서 300(5분)으로 낮췄습니다.	2022년 9월 30일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	POSIX 운영 체제, PHP 응용 프로그램, 응용 프로그램 등의 규칙 그룹에 대해 이 설명서에 제공된 레이블 이름을 수정했습니다. WordPress	2022년 9월 19일
의 새 AWS WAF정책 규칙 옵션 AWS Firewall Manager	AWS Firewall Manager 이제 AWS WAF 정책의 기본 웹 작업에 대한 사용자 지정된 웹 요청 및 응답을 지원합니다.	2022년 9월 9일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 규칙 그룹인 IP 평판에 대한 관리형 규칙.	2022년 8월 30일
AWS WAF 관리형 정책 변경	보호할 수 있는 리소스 유형에 Amazon Cognito 사용자 풀을 `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` `AWSWAFReadOnlyAccess` ,,, 추가하도록 업데이트되었습니다. `AWSWAFConsoleReadOnlyAccess` AWS WAF	2022년 8월 25일
AWS WAF 사기 통제 계정 탈취 방지 (ATP)	이제 Amazon CloudFront 배포에서 AWS WAF 사기 방지 계정 탈취 방지 (ATP) 기능을 사용할 수 있습니다.	2022년 8월 24일
에 대한 관리형 규칙이 업데이트되었습니다 AWS . AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: 알려진 잘못된 입력.	2022년 8월 22일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙:`AWSManagedRulesATPRuleSet` .	2022년 8월 11일
Amazon Cognito 사용자 풀에 대한 지원이 추가되었습니다. AWS WAF	이제 AWS WAF 웹 ACL을 Amazon Cognito 사용자 풀과 연결할 수 있습니다. 이 변경 사항은 최신 버전에서만 사용할 수 AWS WAF 있으며 Classic에서는 사용할 수 없습니다. AWS WAF	2022년 8월 11일
버전이 지정된 관리형 AWS 규칙 그룹 배포에 대한 섹션이 추가되었습니다.	버전이 지정된 관리형 규칙 그룹의 배포를 설명하는 새 섹션이 추가되었습니다. AWS 이 섹션에는 릴리스 후보 배포 시 기본 버전의 이름을 지정하는 방식에 대한 정보가 포함되어 있습니다.	2022년 7월 29일
네트워크 방화벽 정책에 대한 로깅 구성 요구 사항이 업데이트됨	암호화된 Amazon S3 버킷을 로그 대상으로 사용하는 네트워크 방화벽 정책에 대한 요구 사항을 추가했습니다.	2022년 7월 26일
SQLi 규칙 문의 민감도 수준 옵션	이제 SQL 명령어 삽입 규칙 문의 민감도를 높일 수 있습니다. 이렇게 해도 민감도 수준이 기본값인 LOW로 설정된 기존 명령문의 동작은 변경되지 않습니다.	2022년 7월 15일
네트워크 방화벽 정책 구성 옵션이 추가됨	Firewall Manager는 이제 네트워크 방화벽 방화벽 정책 구성에서 상태 저장 평가 순서와 기본 동작을 지원합니다.	2022년 7월 14일

Firewall Manager 보안 그룹 정책 규칙 설정에 대한 업데이트	Firewall Manager는 이제 기본 보안 그룹에서 복제본 보안 그룹으로의 태그 배포를 지원합니다.	2022년 7월 7일
가이드 업데이트 AWS Shield	Shield 가이드의 정보를 확장하여 Shield가 이벤트 완화를 수행하는 방법을 설명했습니다.	2022년 6월 24일
AWS WAF 보호 기능 테스트 및 튜닝에 대한 지침 업데이트	테스트 및 튜닝에 대한 일반 AWS WAF 지침이 업데이트되어 이제 최상위 항목입니다.	2022년 6월 20일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 규칙 그룹에 대한 관리형 규칙: 핵심 규칙 세트 (CRS).	2022년 6월 9일
새 Firewall Manager의 혼동된 보조 지침	Firewall Manager에 대해 혼동된 보조 문제를 방지하는 방법에 대한 지침을 추가했습니다.	2022년 6월 1일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS AWS WAF 업데이트된 규칙 그룹에 대한 관리형 규칙: 핵심 규칙 세트 (CRS).	2022년 5월 24일
새 AWS WAF 요청 구성 요소: Headers 및 Cookies	이제 웹 요청에서 쿠키를 검사할 수 있으며 단일 헤더 외에도 웹 요청의 모든 헤더를 검사할 수 있습니다.	2022년 4월 29일

AWS WAF 크기가 큰 본문, 헤더 및 쿠키 요청 구성 요소에 대한 처리	이제 이러한 구성 요소를 검사하는 규칙 내에서 크기 초과 요청 본문, 헤더 및 쿠키를 처리하는 방법을 AWS WAF 지정할 수 있습니다. 사용자가 이미 이러한 구성 요소를 검사하기 위해 생성한 규칙에는 과대 처리를 위한 새로운 Continue 옵션과 일치하는 동작이 있습니다.	2022년 4월 29일
AWS WAF Amazon S3 로그 정책 변경	Amazon S3 로그 권한 정책 및 예제를 업데이트했습니다.	2022년 4월 12일
이제 Application Load Balancer에서 자동 애플리케이션 계층 DDoS 완화 옵션을 사용할 수 있습니다. AWS Shield Advanced	Shield Advanced는 이제 Application Load Balancer에 대한 자동 애플리케이션 계층 DDoS 완화를 지원하여 모든 애플리케이션 계층 보호에 이 기능을 사용할 수 있습니다. Shield Advanced를 구성하여 보호된 리소스에 대한 애플리케이션 계층 DDoS 공격에 속한 웹 요청을 자동으로 계수 또는 차단할 수 있습니다.	2022년 4월 8일
관리형 규칙 그룹의 현재 기본 버전 설정 표시자가 추가됨	이제 관리형 규칙 그룹 버전 목록에 현재 기본 버전이 표시됩니다.	2022년 4월 8일
에 대한 관리형 규칙 업데이트 AWSAWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: AWS WAF Bot Control.	2022년 4월 6일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: 알려진 잘못된 입력.	2022년 3월 31일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: 알려진 잘못된 입력.	2022년 3월 30일
Firewall Manager는 Palo Alto Networks Cloud Next Generation Firewall(NGFW)에 대한 지원을 추가합니다.	이제 Firewall Manager는 Palo Alto Networks Cloud Next Generation Firewall(NGFW)를 지원합니다.	2022년 3월 30일
팔로 알토 네트웍스 클라우드 NGFW에 대한 지원 추가 AWS Firewall Manager	AWS Firewall Manager 이제 팔로알토 네트웍스 클라우드 차세대 방화벽 (NGFW) 정책을 지원합니다.	2022년 3월 30일
가이드 업데이트 AWS Shield	Shield 가이드의 정보를 확장하여 Shield가 이벤트 감지를 수행하는 방법을 설명하고 DDoS에 복원력 있는 아키텍처의 예를 제공했습니다.	2022년 3월 16일
AWS Shield 가이드 업데이트	Shield 가이드의 정보를 확장하고 다양한 섹션의 구성을 개선했습니다. 주요 변경 사항은 Shield 가이드 섹션 (SRT) 지원, 리소스 보호 및 DDoS 이벤트 가시성과 같은 Shield 가이드 섹션에 AWS Shield Advanced있습니다.	2022년 2월 28일
Firewall Manager는 이제 네트워크 방화벽 중앙 집중식 배포 모델을 지원합니다.	분산 및 중앙 집중식 배포 모델을 사용하는 정책을 구성하는 방법을 설명하는 새 절차가 추가되었습니다.	2022년 2월 24일

Firewall Manager는 AWS Network Firewall 중앙 집중식 배포 모델에 대한 지원을 추가합니다.	이제 분산 또는 중앙 배포 모델을 사용하도록 AWS Network Firewall 정책을 구성할 수 있습니다. 분산 배포 모델을 사용하면 Firewall Manager는 정책 범위 내에 있는 각 VPC에서 방화벽 엔드포인트를 생성 및 유지 관리합니다. 중앙 집중식 배포 모델을 사용하면 Firewall Manager는 단일 검사 VPC에서 방화벽 엔드포인트를 생성 및 유지 관리합니다.	2022년 2월 24일
AWS WAF 관리형 규칙 그룹 버전 관리에 대한 지원을 에 추가합니다. AWS Firewall Manager	AWS Firewall Manager 이제 Firewall Manager AWS WAF 정책에서 AWS WAF 관리형 규칙 그룹 버전 관리를 지원합니다.	2022년 2월 18일
AWS Firewall Manager 관리형 정책 변경	`FMSServiceRolePolicy` 에 대한 업데이트.	2022년 2월 16일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS AWS WAF 업데이트된 규칙 그룹인 IP 평판 목록에 대한 관리형 규칙.	2022년 2월 15일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS AWS WAF 사기 방지 계정 탈취 방지 (ATP) 규칙 그룹을 AWS WAF 추가하기 위한 관리형 규칙. `AWSManagedRulesATPRuleSet`	2022년 2월 11일

가이드 구성 변경 AWS WAF	관리형 보호에 대한 새로운 최상위 섹션을 추가했습니다. CAPTCHA 섹션을 규칙에서 새 관리형 보호 섹션으로 이동시켰습니다. 레이블 섹션을 규칙에서 자체 최상위 섹션으로 이동시켰습니다.	2022년 2월 11일
AWS WAF 클라이언트 애플리케이션 통합	AWS WAF JavaScript 및 모바일 클라이언트 API를 사용하여 클라이언트 애플리케이션을 지능형 위협 완화 AWS 관리 규칙 그룹과 통합하여 탐지 기능을 강화할 수 있습니다.	2022년 2월 11일
AWS WAF 사기 방지 계정 탈취 방지 (ATP)	새로운 AWS WAF 사기 통제 계정 탈취 방지 (ATP) 관리 규칙 그룹을 사용하여 계정 탈취 시도를 탐지하고 차단할 수 있습니다. `AWSManagedRulesATPRuleSet`	2022년 2월 11일
에 대한 관리형 규칙이 업데이트되었습니다 AWS . AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: 알려진 잘못된 입력.	2022년 1월 28일
AWS WAF 관리형 정책 변경	로깅 권한을 수정하도록 `AWSWAFFullAccessPolicy` 및 `AWSWAFConsoleFullAccess` 를 업데이트했습니다.	2022년 1월 11일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS 핵심 규칙 세트 (CRS), SQLi 데이터베이스와 같은 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙.	2022년 1월 10일

Firewall Manager가 Shield Advanced 자동 애플리케이션 계층 DDoS 완화를 지원합니다	Amazon CloudFront 리소스에 대한 Firewall Manager Shield Advanced 정책에는 이제 자동 애플리케이션 계층 DDoS 완화에 대한 지원이 포함됩니다.	2022년 1월 7일
AWS Firewall Manager 관리형 정책 변경	`FMSServiceRolePolicy` 에 대한 업데이트.	2022년 1월 7일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: 알려진 잘못된 입력.	2021년 12월 17일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: 알려진 잘못된 입력.	2021년 12월 11일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 다음 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙: 알려진 잘못된 입력.	2021년 12월 10일
새 AWS Shield Advanced 서비스 연결 역할	자동 애플리케이션 계층 DDoS 완화 기능을 지원하기 위해 `AWSServiceRoleForAWSShield` 이(가) 추가되었습니다.	2021년 12월 1일
새 AWS Shield 관리형 정책	자동 애플리케이션 계층 DDoS 완화 기능을 지원하기 위해 `AWSShieldServiceRolePolicy` 이(가) 추가되었습니다.	2021년 12월 1일

이제 다음과 함께 자동 애플리케이션 레이어 DDoS 완화 옵션을 사용할 수 있습니다. AWS Shield Advanced CloudFront	Shield Advanced는 이제 Amazon CloudFront 배포를 위한 자동 애플리케이션 계층 DDoS 완화를 지원합니다. CloudFront배포에 대한 애플리케이션 계층 DDoS 공격의 일부인 웹 요청을 자동으로 계산하거나 차단하도록 Shield Advanced를 구성할 수 있습니다.	2021년 12월 1일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 핵심 규칙 세트 (CRS), Windows 운영 체제, Linux 운영 체제, IP 평판 목록 등의 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙이 업데이트되었습니다.	2021년 11월 23일
AWS Firewall Manager 관리형 정책 변경	`FMSServiceRolePolicy` 에 대한 업데이트.	2021년 11월 18일
확장된 로깅 옵션 AWS WAF	이제 Amazon CloudWatch Logs 로그 그룹 또는 Amazon Simple Storage Service (Amazon S3) 버킷에 웹 ACL 트래픽을 로깅할 수 있습니다. 이러한 옵션은 Amazon Data Firehose 전송 스트림에 로그인하는 기존 옵션에 추가됩니다.	2021년 11월 15일
AWS WAF 관리형 정책 변경	추가 로깅 대상을 지원하도록 `AWSWAFFullAccessPolicy` 및 `AWSWAFConsoleFullAccess` 를 업데이트했습니다.	2021년 11월 15일

AWS WAF 새 CAPTCHA 규칙 조치 옵션	웹 요청에 대해 CAPTCHA를 실행하도록 규칙을 구성하고 필요에 따라 CAPTCHA 문제를 클라이언트에 전송할 수 있습니다.	2021년 11월 8일
에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS AWS WAF 업데이트된 핵심 규칙 세트 (CRS) 규칙 그룹에 대한 관리형 규칙.	2021년 10월 27일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	이제 모든 AWS 관리형 규칙 규칙 그룹이 레이블 지정을 지원합니다. 규칙 설명에는 레이블 사양이 포함됩니다.	2021년 10월 25일
Firewall Manager는 네트워크 방화벽 로그 필터링을 지원합니다	AWS Firewall Manager 이제 Network Firewall 정책에 대한 로그 필터링을 지원합니다.	2021년 10월 4일
AWS Firewall Manager 관리형 정책 변경	`FMSServiceRolePolicy` 에 대한 업데이트.	2021년 9월 29일
regex 일치 문이 추가됨	이제 웹 요청을 단일 정규식과 일치시킬 수 있습니다.	2021년 9월 22일
규칙 그룹 내 AWS WAF 속도 기반 규칙	이제 규칙 그룹 내에서 속도 기반 규칙을 정의할 수 있습니다. AWS WAF AWS Firewall Manager에서는 이 기능이 정책에 완전히 지원됩니다. AWS WAF	2021년 9월 13일
Firewall Manager는 AWS WAF 로그 필터링을 지원합니다.	AWS Firewall Manager 이제 AWS WAF 정책에 대한 로그 필터링이 지원됩니다.	2021년 8월 31일

에서 out-of-scope 리소스 보호를 자동으로 제거합니다. AWS Firewall Manager	AWS Firewall Manager 정책 범위를 벗어나는 리소스에서 보호를 자동으로 제거할 수 있습니다.	2021년 8월 25일
AWS Firewall Manager 관리형 정책 변경	`FMSServiceRolePolicy` 에 대한 업데이트.	2021년 8월 12일
관리형 규칙 그룹에 버전 관리가 추가됨	관리형 규칙 그룹 제공자는 이제 해당 규칙 그룹의 버전을 관리할 수 있습니다.	2021년 8월 9일
AWS Firewall Manager 관리자 요구 사항 수정	조직의 관리 계정을 Firewall Manager 관리자 계정으로 사용할 수 있습니다. 이는 허용되지 않았습니다.	2021년 8월 2일
Firewall Manager 할당량 증가	Firewall Manager 정책 범위 내에서 보유할 수 있는 Amazon VPC 인스턴스의 수를 10개에서 100개로 늘렸습니다.	2021년 7월 28일
AWS Firewall ManagerAWS Network Firewall 라우팅 테이블 모니터링 지원	AWS Firewall Manager 이제 라우팅 테이블 모니터링을 지원하고, 경로가 잘못 구성된 AWS Network Firewall 정책에 대해 보안 관리자에게 개선 조치 권장 사항을 제공합니다.	2021년 7월 8일
AWS WAF 추가 텍스트 변환 옵션	텍스트 변환 옵션을 확장했으며, 검사하기 전에 이러한 옵션을 웹 요청 구성 요소에 적용할 수 있습니다.	2021년 6월 24일
Firewall Manager AWS WAF 정책 리소스의 이름 지정 수정됨	Firewall Manager가 AWS WAF 정책에 따라 관리하는 웹 ACL, 규칙 그룹 및 로깅의 이름이 변경되었습니다.	2021년 5월 26일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS Amazon IP 평판 목록에 대한 레이블 지정 지원 AWS WAF 추가 및 Amazon IP 평판 목록의 규칙 이름 접미사 제거를 위한 관리형 규칙	2021년 5월 4일
위임 관리자에 대한 AWS Organizations 지원 추가	AWS Firewall Manager 관리자 계정을 설정하면 이제 Firewall Manager는 해당 계정을 Firewall Manager의 AWS Organizations 위임 관리자로 지정합니다. 이번 변경으로, Firewall Manager 관리자 계정을 설정할 때 조직의 관리 계정이 아닌 다른 구성원 계정을 제공해야 합니다. 이 변경은 기존 설정에는 영향을 주지 않습니다.	2021년 4월 30일
에 대한 관리형 규칙이 업데이트되었습니다 AWS . AWS WAF	AWS AWS WAF 추가된 AWS WAF 봇 제어 규칙 그룹에 대한 관리형 규칙.	2021년 4월 1일
규칙 그룹의 개별 규칙 동작을 Count로 설정함	이제 규칙 그룹의 개별 규칙 동작을 Count로 설정할 수 있습니다. 규칙 그룹 수준에 있는 기존 재정의 정보가 수정되었습니다.	2021년 4월 1일
관리형 규칙 그룹의 범위 축소 문	이제 속도 기반 문을 사용할 때와 동일한 방식으로 관리형 규칙 그룹에 범위 축소 문을 사용할 수 있습니다.	2021년 4월 1일
로그 필터링	이제 규칙 작업 및 레이블을 기반으로 기록하는 웹 ACL 트래픽을 필터링할 수 있습니다.	2021년 4월 1일

AWS WAF 웹 요청의 라벨	일치하는 웹 요청에 레이블을 추가하고 다른 규칙에 의해 추가되는 레이블과 일치하도록 규칙을 구성할 수 있습니다.	2021년 4월 1일
AWS WAF 봇 컨트롤	Bot Control 관리 규칙 그룹과 웹 요청 레이블 지정, 범위 축소 명령문 및 로그 필터링이 결합된 새로운 AWS WAF Bot Control 기능으로 봇 트래픽을 모니터링하고 제어할 수 있습니다.	2021년 4월 1일
Firewall Manager는 Amazon Route 53 Resolver DNS 방화벽 정책을 지원합니다.	AWS Firewall Manager VPC에 대한 Amazon Route 53 Resolver DNS 방화벽 아웃바운드 DNS 트래픽 필터링의 중앙 관리를 지원합니다.	2021년 3월 31일
사용자 지정 요청 및 응답 처리	AWS WAF 에서 차단하지 않는 웹 요청에 대해서는 사용자 지정 헤더를 포함할 수 있으며 AWS WAF 에서 차단하는 웹 요청에 대해서는 사용자 지정 응답을 보낼 수 있습니다. 이 기능은 웹 ACL 기본 작업 및 규칙 작업 설정에 대해 사용할 수 있습니다.	2021년 3월 29일
AWS Firewall Manager 관리형 정책 변경	`FMSServiceRolePolicy` 에 대한 업데이트.	2021년 3월 17일

에 대한 AWS 관리형 규칙 업데이트 AWS WAF	AWS 핵심 규칙 세트 (CRS), 관리자 보호, 알려진 잘못된 입력, Linux 운영 체제 등의 규칙 그룹을 AWS WAF 업데이트하기 위한 관리형 규칙이 업데이트되었습니다.	2021년 3월 3일
AWS Shield 관리형 정책 변경 추적	Shield는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 3월 3일
AWS Firewall Manager 관리형 정책 변경 추적	Firewall Manager는 AWS 관리형 정책의 변경 사항을 추적하기 시작했습니다.	2021년 3월 2일
AWS WAF 관리형 정책 변경 추적	AWS WAF AWS 관리형 정책의 변경 사항 추적을 시작했습니다.	2021년 3월 1일
웹 요청 본문을 구문 분석된 JSON으로 검사합니다.	웹 요청 본문을 구분 분석 및 필터링된 JSON으로 검사하는 옵션을 추가했습니다. 이 옵션은 웹 요청 본문을 일반 텍스트로 검사하는 기존 옵션에 추가됩니다.	2021년 2월 12일
Firewall Manager는 AWS Network Firewall 정책을 지원합니다.	AWS Firewall Manager VPC에 대한 AWS Network Firewall 네트워크 트래픽 필터링의 중앙 관리를 지원합니다.	2020년 11월 17일
AWS Shield Advanced 보호 그룹에 대한 지원 추가	이제 보호된 리소스를 논리적 그룹으로 그룹화하고 보호를 집합적으로 관리할 수 있습니다.	2020년 11월 13일

AWS AppSync 에 대한 지원 추가 AWS WAF	이제 AWS WAF 웹 ACL을 AWS AppSync GraphQL API와 연결할 수 있습니다. 이 변경 사항은 최신 버전의 Classic에서만 사용할 수 AWS WAF 있으며 Classic에서는 사용할 수 없습니다. AWS WAF	2020년 10월 1일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS Windows 운영 체제 규칙 세트를 AWS WAF 업데이트하기 위한 관리형 규칙.	2020년 9월 23일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 규칙 세트 PHP 응용 프로그램 및 POSIX 운영 체제에 대한 관리형 규칙.	2020년 9월 16일
콘솔이 업데이트되었습니다. AWS Shield	AWS Shield 사용자 경험이 개선된 새 콘솔 옵션을 제공합니다. 설명서의 콘솔 지침은 새 콘솔에 대한 지침입니다.	2020년 9월 1일
공통 보안 그룹 정책에 대한 Firewall Manager 업데이트	AWS Firewall Manager 이제 공통 보안 그룹 정책이 콘솔 구현을 통해 애플리케이션 로드 밸런서 및 클래식 로드 밸런서 리소스 유형을 지원합니다. 새 옵션은 공통 정책의 정책 범위 설정에서 사용할 수 있습니다.	2020년 8월 11일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 핵심 규칙 세트를 AWS WAF 업데이트하기 위한 관리형 규칙.	2020년 8월 7일
Firewall Manager는 AWS WAF 로깅 구성을 지원합니다.	AWS Firewall Manager 이제 AWS WAF 정책에 대한 중앙 집중식 로깅 구성을 지원합니다.	2020년 7월 30일

웹 요청에서 IP 주소 위치를 지정합니다.	웹 요청 오리진을 사용하는 대신 사용자가 지정하는 HTTP 헤더의 IP 주소를 사용하는 옵션을 추가했습니다. 대체 헤더는 일반적으로 `X-Forwarded-For`(XFF)지만 아무 헤더 이름이나 지정할 수 있습니다. 이 옵션은 IP 집합 매칭, 리전 매칭, 속도 기반 규칙 개수 집계에 사용할 수 있습니다.	2020년 7월 9일
콘텐츠 감사 보안 그룹 정책에 대한 Firewall Manager 업데이트	AWS Firewall Manager 관리되는 응용 프로그램 및 프로토콜 목록을 사용하는 관리형 규칙 옵션과 리소스 위반에 대한 세부 정보를 포함하여 콘텐츠 감사 보안 그룹 정책의 기능을 확장했습니다.	2020년 7월 7일
Firewall Manager 관리형 목록	AWS Firewall Manager 이제 관리형 응용 프로그램 및 프로토콜 목록을 지원합니다. Firewall Manager는 일부 목록을 관리하며 사용자가 사용자 자신의 목록을 직접 만들고 관리할 수 있습니다.	2020년 7월 7일
Firewall Manager는 공통 보안 그룹 정책에서 공유 VPC를 지원합니다.	AWS Firewall Manager 이제 공유 VPC에서 공통 보안 그룹 정책을 사용할 수 있습니다. 범위 내 계정이 소유한 VPC에서도 사용하는 것 외에도 이 작업을 수행할 수 있습니다.	2020년 5월 26일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 관리 규칙에 각 규칙에 대한 설명서가 추가되었습니다 AWS WAF.	2020년 5월 20일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 Linux 운영 체제 규칙 그룹에 대한 관리형 규칙	2020년 5월 19일
AWS WAF Classic 리소스를 AWS WAF (v2) 로 마이그레이션하기 위한 지원 추가	이제 콘솔 또는 API를 사용하여 AWS WAF Classic 리소스를 내보내 최신 버전으로 마이그레이션할 수 있습니다. AWS WAF	2020년 4월 27일
정책 범위에 AWS Organizations 조직 단위에 대한 지원을 추가합니다.	AWS Firewall Manager 이제 OU (AWS Organizations 조직 단위) 를 사용하여 정책 범위를 지정할 수 있습니다. OU를 사용하여 특정 계정을 포함하거나 제외할 뿐 아니라 범위의 계정을 포함하거나 제외할 수 있습니다. OU를 지정하는 것은 나중에 추가되는 모든 하위 OU와 계정을 포함하여 OU 및 하위 OU의 모든 계정을 지정하는 것과 같습니다.	2020년 4월 6일
AWS WAF (v2) 에 대한 지원 추가 AWS Firewall Manager	AWS Firewall Manager 이제 이전 AWS WAF버전인 AWS WAF Classic의 최신 버전도 지원합니다.	2020년 3월 31일
AWS Firewall Manager 공통 보안 그룹 정책 업데이트	AWS Firewall Manager 이제 공통 보안 그룹 정책에 범위 내 Amazon EC2 인스턴스의 모든 엘라스틱 네트워크 인터페이스에 정책을 적용할 수 있는 옵션이 있습니다. 기본 탄력적 네트워크 인터페이스에만 정책을 적용하도록 선택할 수도 있습니다.	2020년 3월 11일

에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 추가된 규칙 그룹에 대한 관리형 `AWSManagedRulesAnonymousIpList` 규칙.	2020년 3월 6일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS AWS WAF 업데이트된 WordPress 응용 프로그램 및 규칙 그룹에 대한 관리형 `AWSManagedRulesCommonRuleSet` 규칙.	2020년 3월 3일
AWS Shield Advanced 보호 옵션에 Amazon Route 53 상태 점검을 추가했습니다.	이제 Shield Advanced에서는 위협 탐지 및 완화의 정확성을 향상하기 위해 Amazon Route 53 상태 확인 연결 사용을 지원합니다.	2020년 2월 14일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 에 대한 AWS WAF 관리형 규칙이 SQL Database 규칙 그룹을 업데이트하여 메시지 URI 검사를 추가했습니다.	2020년 1월 23일
보안 그룹 사용 감사 정책에 대한 Firewall Manager 신규 옵션	Firewall Manager에 보안 그룹 사용 감사 정책에 대한 새로운 옵션이 추가되었습니다. 이제 보안 그룹이 미준수로 간주되기 전까지 사용되지 않은 상태로 유지되어야 하는 최소 시간(분)을 설정할 수 있습니다. 기본적으로 이 minutes(분) 설정은 0입니다.	2020년 1월 14일

Firewall Manager의 새 AWS WAF 정책 옵션	Firewall Manager에는 새로운 AWS WAF 정책 옵션이 있습니다. 이제 정책의 새 웹 ACL을 연결하기 전에 범위 내 리소스에서 기존 웹 ACL 연결을 모두 제거하도록 선택할 수 있습니다.	2020년 1월 14일
에 대한 AWS 관리형 규칙이 업데이트되었습니다. AWS WAF	AWS 관리형 규칙의 경우 핵심 규칙 세트 및 SQL Database 규칙 그룹의 규칙에 대한 텍스트 변환이 AWS WAF 업데이트되었습니다.	2019년 12월 20일
AWS Firewall Manager 다음과 통합되었습니다. AWS Security Hub	AWS Firewall Manager 이제 규정을 준수하지 않는 리소스와 공격에 대한 탐지 결과를 생성하여 AWS Security Hub전송합니다.	2019년 12월 18일

AWS WAF 버전 2 출시	AWS WAF 개발자 안내서의 새 버전. 웹 ACL 또는 규칙 그룹을 JSON 형식으로 관리할 수 있습니다. 확장된 기능에는 논리적 규칙 문, 규칙 문 중첩, IP 주소 및 주소 범위에 대한 완전한 CIDR 지원이 포함됩니다. 규칙은 더 이상 AWS 리소스가 아니며 웹 ACL 또는 규칙 그룹의 컨텍스트에서만 존재합니다. 기존 고객의 경우 이전 버전의 서비스를 이제 AWS WAF 클래식이라고 합니다. API, SDK 및 CLI에서 AWS WAF Classic은 이름 지정 체계를 유지하며 이 최신 버전은 컨텍스트에 따라 “V2" 또는 “v2"가 AWS WAF 추가되어 참조됩니다. AWS WAF Classic에서 만든 리소스에 액세스할 수 없습니다. AWS AWS WAF 에서 AWS WAF이러한 리소스를 사용하려면 마이그레이션해야 합니다.	2019년 11월 25일
AWS 관리형 규칙 규칙 그룹: AWS WAF	AWS 관리형 규칙 규칙 그룹을 추가했습니다. AWS WAF 고객에게는 무료로 제공됩니다.	2019년 11월 25일
AWS Firewall Manager Amazon Virtual Private Cloud 보안 그룹 지원	Amazon VPC 보안 그룹에 대한 지원이 Firewall Manager에 추가되었습니다.	2019년 10월 10일
AWS Firewall Manager 에 대한 지원 AWS Shield Advanced	Shield Advanced에 대한 지원이 Firewall Manager에 추가되었습니다.	2019년 3월 15일

자습서: 계층적 정책 생성	AWS Firewall Manager에서 계층적 정책을 생성하는 방법에 대한 자습서를 추가했습니다.	2019년 2월 11일
규칙 그룹의 규칙 레벨 제어	이제 규칙 그룹뿐만 아니라 자체 AWS Marketplace 규칙 그룹에서 개별 규칙을 제외할 수 있습니다.	2018년 12월 12일
AWS Shield AdvancedAWS Global Accelerator 표준 액셀러레이터 지원	Shield Advanced는 이제 AWS Global Accelerator 표준 액셀러레이터를 보호할 수 있습니다.	2018년 11월 26일
AWS WAF 아마존 API 게이트웨이 지원	AWS WAF 이제 Amazon API Gateway API를 보호합니다.	2018년 10월 25일
익스팬디드 AWS 쉴드 고급 시작 마법사	새 마법사는 요금 기반 규칙 및 Amazon CloudWatch Events를 생성할 수 있는 기회를 제공합니다.	2018년 8월 31일
AWS WAF logging	로깅을 활성화하여 웹 ACL에서 분석한 트래픽에 대한 자세한 정보를 기록합니다.	2018년 8월 31일
조건에서의 쿼리 파라미터 지원	조건을 만들면 이제 특정 파라미터에 대한 요청을 검색할 수 있습니다.	2018년 6월 5일
Shield Advanced 시작하기 마법사	AWS Shield Advanced를 구독하기 위한 새롭고 간소화된 프로세스를 소개합니다.	2018년 6월 5일
허용되는 CIDR 범위가 확장됨	AWS WAF 이제 IP 일치 조건을 생성할 때 IPv4 주소 범위 (/8) 및 /16에서 /32 사이의 모든 범위를 지원합니다.	2018년 6월 5일

2018년 이전의 업데이트

다음 표에서는 2018년 이전 발행된 AWS WAF 개발자 안내서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경 사항	API 버전	설명	릴리스 날짜
업데이트	2016-08-24	AWS Marketplace 규칙 그룹	2017년 11월
업데이트	2016-08-24	탄력적 IP 주소에 대한 Shield Advanced 지원	2017년 11월
업데이트	2016-08-24	글로벌 위협 대시보드	2017년 11월
업데이트	2016-08-24	DDoS 방지 웹 사이트 자습서	2017년 10월
업데이트	2016-08-24	지역 및 정규식 조건	2017년 10월
업데이트	2016-08-24	속도 기반 규칙	2017년 6월
업데이트	2016-08-24	재구성	2017년 4월
업데이트	2016-08-24	DDOS 보호 및 Application Load Balancer 지원에 대한 정보를 추가했습니다.	2016년 11월
새로운 기능	2015-08-24	이제 계정에 대한 API 호출을 기록하고 로그 파일을 S3 버킷으로 전달하는 AWS 서비스를 AWS WAF 통해 AWS CloudTrail모든 API 호출을 기록할 수 있습니다. CloudTrail 로그를 사용하여 보안 분석을 지원하고, AWS 리소스 변경 사항을 추적하고, 규정 준수 감사를 지원할 수 있습니다. 통합을 AWS WAF CloudTrail 통해 AWS WAF API에 대한 요청, 각 요청이 이루어진 소스 IP 주소, 요청한 사람, 요청 시기 등을 확인할 수 있습니다.	2016년 4월 28일

변경 사항	API 버전	설명	릴리스 날짜
		이미 사용하고 AWS CloudTrail있다면 CloudTrail 로그에 AWS WAF API 호출이 표시되기 시작할 것입니다. 계정을 CloudTrail 활성화하지 않은 경우 CloudTrail 에서 활성화할 수 AWS Management Console있습니다. CloudTrail활성화에 따른 추가 비용은 없지만 Amazon S3 및 Amazon SNS 사용에 대한 표준 요금이 적용됩니다.	
새로운 기능	2015-08-24	이제 크로스 사이트 스크립팅 또는 XSS라고 AWS WAF 하는 악성 스크립트가 포함된 것으로 보이는 웹 요청을 허용, 차단 또는 계산하는 데 사용할 수 있습니다. 때로 공격자는 웹 애플리케이션의 취약성을 악용하기 위해 악성 스크립트를 웹 요청에 삽입합니다. 자세한 내용은 교차 사이트 스크립팅 공격 규칙 문 섹션을 참조하세요.	2016년 3월 29일
새로운 기능	2015-08-24	이번 릴리스에는 AWS WAF 다음과 같은 기능이 추가되었습니다. • 요청의 지정된 부분 (예: 쿼리 문자열 또는 URI) 의 길이를 기준으로 웹 요청을 허용, 차단 또는 AWS WAF 계산하도록 구성할 수 있습니다. 자세한 정보는 크기 제약 조건 규칙 문을 참조하세요. • 요청 본문의 콘텐츠를 기반으로 웹 요청을 허용, 차단 또는 AWS WAF 계산하도록 구성할 수 있습니다. 이것은 HTTP 요청 본문으로 웹 서버에 전송할 추가 데이터(예: 양식 데이터)가 포함되어 있는 요청의 일부입니다. 이 기능은 문자열 일치 조건, SQL 명령어 주입 조건, 첫 번째 글머리표에 언급된 새로운 크기 제약 조건에 적용됩니다. 자세한 내용은 웹 요청 구성 요소 사양 및 처리 섹션을 참조하세요.	2016년 1월 27일

변경 사항	API 버전	설명	릴리스 날짜
새 기능	2015-08-24	이제 AWS WAF 콘솔을 사용하여 웹 ACL을 연결할 CloudFront 배포를 선택할 수 있습니다. 자세한 내용은 웹 ACL과 배포의 연결 또는 연결 해제를 참조하십시오. CloudFront	2015년 11월 16일
최초 릴리스	2015-08-24	이 문서는 첫 번째 AWS WAF 개발자 안내서 릴리스입니다.	2015년 10월 6일

AWS 용어집

최신 AWS 용어는 참조의 AWS 용어집을 참조하십시오.AWS 용어집

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.