구현 안내서

AWS WAF의 보안 자동화

AWS WAF의 보안 자동화: 구현 안내서

Table of Contents

솔루션 개요 1
기능 및 이점 3
AWS 관리형 규칙 규칙 그룹으로 웹 애플리케이션 보호 3
사전 정의된 HTTP Flood 사용자 지정 규칙을 사용하여 계층 7 플러드 보호 제공 3
사전 정의된 스캐너 및 프로브 사용자 지정 규칙을 사용하여 취약성 악용 차단 3
사전 정의된 잘못된 봇 사용자 지정 규칙을 사용하여 침입 감지 및 편향 4
사전 정의된 IP 평판 목록 사용자 지정 규칙을 사용하여 악성 IP 주소 차단 4
사전 정의된 허용 및 거부 IP 목록 사용자 지정 규칙을 사용하여 수동 IP 구성 제공 4
자체 모니터링 대시보드 구축 4
사용 사례 4
개념 및 정의 5
아키텍처 개요 8
아키텍처 다이어그램 8
AWS Well-Architected 설계 고려 사항 11
운영 우수성 11
보안 12
신뢰성 12
성능 효율성 12
비용 최적화 13
지속 가능성 13
아키텍처 세부 정보 14
이 솔루션의 AWS 서비스 14
로그 구문 분석기 옵션 15
AWS WAF 속도 기반 규칙 15
Amazon Athena 로그 구문 분석기 15
AWS Lambda 로그 구문 분석기 16
구성 요소 세부 정보 16
로그 구문 분석기 - 애플리케이션 16
로그 구문 분석기 - AWS WAF 18
로그 구문 분석기 - 잘못된 봇 19
IP 목록 구문 분석기 20
배포 계획 21
지원되는 AWS 리전 21
비용 22

CloudWatch 로그의 비용 추정 24
Athena의 예상 비용 25
보안 26
IAM 역할 26
Data 26
보호 기능 26
할당량 27
이 솔루션의 AWS 서비스에 대한 할당량 27
AWS WAF 할당량 27
배포 고려 사항 28
AWS WAF 규칙 28
웹 ACL 트래픽 로깅 28
요청 구성 요소의 크기 초과 처리 28
다중 솔루션 배포 29
배포를 위한 최소 역할 권한(선택 사항) 29
솔루션 배포 37
배포 프로세스 개요 37
AWS CloudFormation 템플릿 38
기본 스택 38
WebACL 스택 38
Firehose Athena 스택 38
사전 조건 39
CloudFront 배포 구성 39
ALB 구성 39
1단계. 스택 시작 39
2단계. 웹 ACL을 웹 애플리케이션과 연결 67
3단계. 웹 액세스 로깅 구성 67
CloudFront 배포의 웹 액세스 로그 저장 67
Application Load Balancer의 웹 액세스 로그 저장 68
솔루션 업데이트 69
업데이트 고려 사항 70
리소스 유형 업데이트 70
WAFV2 업그레이드 70
스택 업데이트 시 사용자 지정 70
잘못된 봇 보호 업그레이드 70
CDK 업그레이드 71

솔루션 제거 72
솔루션 사용 73
허용 및 거부된 IP 세트 수정(선택 사항) 73
웹 애플리케이션에 Honeypot 링크 임베드(선택 사항) 73
Honeypot 엔드포인트에 대한 CloudFront 오리진 생성 74
Honeypot 엔드포인트를 외부 링크로 임베드 75
Lambda 로그 구문 분석기 JSON 파일 사용 76
HTTP 서비스 장애 방지에 Lambda 로그 구문 분석기 JSON 파일 사용 76
스캐너 및 프로브 보호에 Lambda 로그 구문 분석기 JSON 파일 사용 77
HTTP flood Athena 로그 구문 분석기에서 국가 및 URI 사용 78
Amazon Athena 쿼리 보기 79
WAF 로그 쿼리 보기 80
애플리케이션 액세스 로그 쿼리 보기 81
Athena 파티션 쿼리 추가 보기 81
허용 및 거부된 AWS WAF IP 세트에서 IP 보존 구성 82
작동 방법 82
IP 보존 켜기 83
모니터링 대시보드 구축 84
XSS 오탐 처리 85
문제 해결 87
Support에 문의하세요. 87
사례 생성 87
어떻게 도와드릴까요? 87
추가 정보 87
사례를 더 빠르게 해결할 수 있도록 지원 87
지금 해결하거나 문의하기 88
개발자 안내서 89
소스 코드 89
레퍼런스 90
익명화된 데이터 수집 90
관련 리소스 91
연결된 AWS 백서 91
연결된 AWS 보안 블로그 게시물 91
타사 IP 평판 목록 91
기여자 92
개정 93

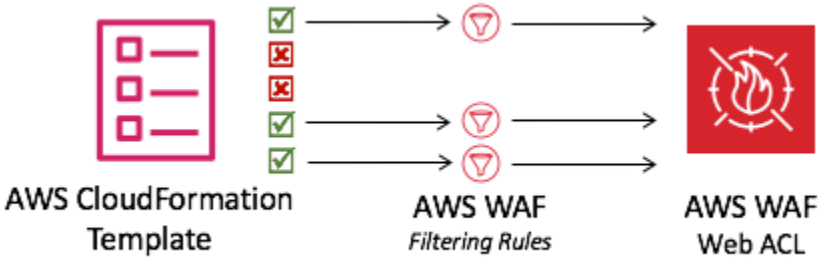
고지 사항 94
..... xcv

AWS WAF의 보안 자동화를 사용하여 웹 기반 공격을 필터링하는 단일 웹 액세스 제어 목록 자동 배포

AWS WAF용 보안 자동화 솔루션은 일반적인 웹 악용으로부터 애플리케이션을 보호하는 데 도움이 되는 사전 구성된 규칙 세트를 배포합니다. 이 솔루션의 핵심 서비스인 AWS WAF는 애플리케이션 가용성에 영향을 미치거나 보안을 손상시키거나 과도한 리소스를 소비할 수 있는 공격 기법으로부터 웹 애플리케이션을 보호하는 데 도움이 됩니다. AWS WAF를 사용하여 사용자 지정 가능한 웹 보안 규칙을 정의할 수 있습니다. 이러한 규칙은 Amazon CloudFront, Application Load Balancer(ALB)와 같은 AWS 리소스에 배포된 웹 애플리케이션 및 애플리케이션 프로그래밍 인터페이스(APIs)를 허용하거나 차단할 트래픽을 제어합니다. 지원되는 리소스 유형에 대한 자세한 내용은 AWS WAF, AWS Firewall Manager 및 AWS Shield Advanced 개발자 안내서의 AWS WAF를 참조하세요.

AWS WAF 규칙을 구성하는 것은 특히 전용 보안 팀이 없는 대규모 조직과 소규모 조직 모두에게 어렵고 부담스러울 수 있습니다. 이 프로세스를 간소화하기 위해 AWS WAF용 보안 자동화 솔루션은 일반적인 웹 기반 공격을 필터링하도록 설계된 일련의 AWS WAF 규칙과 함께 단일 웹 액세스 제어 목록(ACL)을 자동으로 배포합니다. 이 솔루션의 AWS CloudFormation 템플릿을 처음 구성하는 동안 포함할 보호 기능을 지정할 수 있습니다. 이 솔루션을 배포한 후 AWS WAF는 기존 CloudFront 배포(들) 또는 ALB(들)에 대한 웹 요청을 검사하고 해당하는 경우 차단합니다.

CloudFormation 템플릿은 AWS WAF 필터링 규칙을 사용하여 웹 ACL을 배포합니다.



이 구현 가이드에서는 Amazon Web Services(AWS) 클라우드에이 솔루션을 배포하기 위한 아키텍처 고려 사항, 구성 단계 및 운영 모범 사례를 설명합니다. 여기에는 보안 및 가용성에 대한 AWS 모범 사례를 사용하여 AWS에서이 솔루션을 배포하는 데 필요한 AWS 보안, 컴퓨팅, 스토리지 및 기타 서비스를 시작, 구성 및 실행하는 CloudFormation 템플릿에 대한 링크가 포함되어 있습니다.

이 설명서의 정보는 AWS WAF, CloudFront, ALBs. AWS Lambda 또한 일반적인 웹 기반 공격 및 완화 전략에 대한 기본 지식이 필요합니다.

> **Note**
>
> 버전 3.0.0부터이 솔루션은 최신 버전의 AWS WAF 서비스 API(AWS WAFV2)를 지원합니다.

이 가이드는 IT 관리자, 보안 엔지니어, DevOps 엔지니어, 개발자, 솔루션 아키텍트 및 웹 사이트 관리자를 대상으로 합니다.

> **Note**
>
> AWS WAF 규칙을 구현하기 위한 출발점으로이 솔루션을 사용하는 것이 좋습니다. 필요에 따라 소스 코드를 사용자 지정하고, 새 사용자 지정 규칙을 추가하고, 더 많은 AWS WAF 관리형 규칙을 활용할 수 있습니다.

이 탐색 테이블을 사용하여 다음 질문에 대한 답을 빠르게 찾을 수 있습니다.

다음을 수행하려는 경우 . . .	읽기 . . .
이 솔루션을 실행하는 데 드는 비용을 파악합니다. 이 솔루션을 실행하는 데 드는 총 비용은 활성화된 보호와 수집, 저장 및 처리된 데이터의 양에 따라 달라집니다.	비용
이 솔루션의 보안 고려 사항을 이해합니다.	보안
이 솔루션에서 지원되는 AWS 리전을 파악합니다.	지원되는 AWS 리전
이 솔루션에 포함된 CloudFormation 템플릿을 보거나 다운로드하여이 솔루션의 인프라 리소스("스택")를 자동으로 배포합니다.	AWS CloudFormation 템플릿
Support를 사용하면 솔루션을 배포, 사용 또는 문제 해결하는 데 도움이 됩니다.	지원
소스 코드에 액세스하고 선택적으로 AWS Cloud Development Kit(AWS CDK)를 사용하여 솔루션을 배포합니다.	GitHub 리포지토리

기능 및 이점

AWS WAF용 보안 자동화 솔루션은 다음과 같은 기능과 이점을 제공합니다.

AWS 관리형 규칙 규칙 그룹으로 웹 애플리케이션 보호

AWS WAF용 AWS 관리형 규칙은 일반적인 애플리케이션 취약성 또는 기타 원치 않는 트래픽에 대한 보호를 제공합니다. 이 솔루션에는 AWS 관리형 IP 평판 규칙 그룹, AWS 관리형 기준 규칙 그룹 및 AWS 관리형 사용 사례별 규칙 그룹이 포함됩니다. 최대 웹 ACL 용량 단위(WCU) 할당량까지 웹 ACL에 대해 하나 이상의 규칙 그룹을 선택할 수 있습니다.

사전 정의된 HTTP Flood 사용자 지정 규칙을 사용하여 계층 7 플러드 보호 제공

HTTP Flood 사용자 지정 규칙은 고객이 정의한 기간 동안 웹 계층 분산 Denial-of-Service(DDoS) 공격으로부터 보호합니다. 다음 옵션 중 하나를 선택하여이 규칙을 활성화할 수 있습니다.

- AWS WAF 속도 기반 규칙
- Lambda 로그 구문 분석기
- Amazon Athena 로그 구문 분석기

Lambda 로그 구문 분석기 또는 Athena 로그 구문 분석기 옵션을 사용하면 요청 할당량을 100 미만으로 정의할 수 있습니다. 이 접근 방식은 AWS WAF 속도 기반 규칙에 필요한 할당량에 도달하지 않는 데 도움이 될 수 있습니다. 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.

필터링 조건에 국가 및 URI(Uniform Resource Identifier)를 추가하여 Athena 로그 구문 분석기를 개선할 수도 있습니다. 이 접근 방식은 예측할 수 없는 URI 패턴이 있는 HTTP 플러드 공격을 식별하고 차단합니다. 자세한 내용은 HTTP Flood Athena 로그 구문 분석기에서 국가 및 URI 사용을 참조하세요.

사전 정의된 스캐너 및 프로브 사용자 지정 규칙을 사용하여 취약성 악용 차단

스캐너 및 프로브 사용자 지정 규칙은 오리진에서 생성된 비정상적인 양의 오류와 같은 의심스러운 동작을 검색하는 애플리케이션 액세스 로그를 구문 분석합니다. 그런 다음 고객이 정의한 기간 동안 의심스러운 소스 IP 주소를 차단합니다. Lambda 로그 구문 분석기 또는 Athena 로그 구문 분석기 중 하나를 선택하여이 규칙을 활성화할 수 있습니다. 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.

사전 정의된 잘못된 봇 사용자 지정 규칙을 사용하여 침입 감지 및 편향

잘못된 봇 사용자 지정 규칙은 허니팟 엔드포인트를 설정합니다. 허니팟 엔드포인트는 시도된 공격을 유추하고 방어하기 위한 보안 메커니즘입니다. 웹 사이트에 엔드포인트를 삽입하여 콘텐츠 스크레이퍼 및 잘못된 봇의 인바운드 요청을 감지할 수 있습니다. 감지되면 동일한 오리진의 모든 후속 요청이 차단됩니다. 자세한 내용은 웹 애플리케이션에 Honeypot 링크 임베드를 참조하세요.

사전 정의된 IP 평판 목록 사용자 지정 규칙을 사용하여 악성 IP 주소 차단

IP 신뢰도 목록 사용자 지정 규칙은 차단할 새 IP 범위에 대해 시간당 타사 IP 신뢰도 목록을 확인합니다. 이러한 목록에는 Spamhaus Don't Route Or Peer(DROP) 및 Extended DROP(EDROP) 목록, Proofpoint Emerging Threats IP 목록 및 Tor 출구 노드 목록이 포함됩니다.

사전 정의된 허용 및 거부 IP 목록 사용자 지정 규칙을 사용하여 수동 IP 구성 제공

허용 및 거부된 IP 목록 사용자 지정 규칙을 사용하면 허용 또는 거부하려는 IP 주소를 수동으로 삽입할 수 있습니다. 허용 및 거부 IP 목록에서 IP 보존을 구성하여 설정된 시간에 IPs를 만료시킬 수도 있습니다.

자체 모니터링 대시보드 구축

이 솔루션은 허용된 요청, 차단된 요청 및 기타 관련 지표와 같은 Amazon CloudWatch 지표를 내보냅니다. 사용자 지정 대시보드를 구축하여 이러한 지표를 시각화하고 AWS WAF에서 제공하는 공격 및 보호 패턴에 대한 인사이트를 얻을 수 있습니다. 자세한 내용은 빌드 모니터링 대시보드를 참조하세요.

사용 사례

다음은이 솔루션을 사용하는 사용 사례의 예입니다. 이 목록에 국한되지 않는 혁신적인 방식으로이 솔루션을 사용자 지정할 수 있습니다.

AWS WAF 규칙 설정 자동화

AWS WAF는 일반적인 공격으로부터 웹 애플리케이션을 보호하지만 AWS WAF 규칙 설정은 복잡하고 시간이 많이 걸릴 수 있습니다. 이 솔루션은 CloudFormation 템플릿을 사용하여 AWS WAF 규칙 세트를 계정에 자동으로 배포합니다. 이렇게 하면 AWS WAF 규칙을 직접 구성할 필요가 없으며 AWS WAF를 더 빠르게 시작할 수 있습니다.

계층 7 HTTP 서비스 장애 방지 사용자 지정

이 솔루션은 HTTP Flood 보호를 활성화하는 세 가지 옵션을 제공합니다. DDoS 공격으로부터 보호하는 데 필요한 옵션을 선택할 수 있습니다. 자세한 내용은 기능 및 이점의 사전 정의된 HTTP Flood 사용자 지정 규칙을 사용하여 계층 7 플러드 보호 제공을 참조하세요.

소스 코드를 활용하여 사용자 지정을 적용하거나 자체 보안 자동화를 구축합니다.

이 솔루션은 AWS WAF 및 기타 서비스를 사용하여 AWS 클라우드에서 보안 자동화를 구축하는 방법에 대한 예를 제공합니다. GitHub의 오픈 소스 코드를 사용하면 편리하게 사용자 지정을 적용하거나 필요에 맞는 자체 보안 자동화를 구축할 수 있습니다.

개념 및 정의

이 섹션에서는 주요 개념을 설명하고이 솔루션과 관련된 용어를 정의합니다.

ALB 로그

이 솔루션은 ALB 리소스에 대한 로그를 사용합니다. 이 솔루션의 스캐너 및 프로브 보호 규칙은 이러한 로그를 검사합니다.

Athena 로그 구문 분석기

Amazon Athena는 오픈 소스 프레임워크를 기반으로 구축된 서버리스 대화형 분석 서비스로, 오픈 테이블 및 파일 형식을 지원합니다. 이 솔루션은 사용자가 HTTP 서비스 장애 방지 규칙 또는 스캐너 및 프로브 보호 규칙을 활성화할 `yes - Amazon Athena log parser` 때를 선택하는 경우 예약된 Athena 쿼리를 실행하여 AWS WAF, CloudFront 또는 ALB 로그를 검사하며, 구조화된 로직 체인을 통해 작동하는 감지를 통해 잘못된 봇 보호 활성화에 사용할 수 있습니다.

AWS WAF 규칙

AWS WAF 규칙은 다음을 정의합니다.

- HTTP(S) 웹 요청을 검사하는 방법
- 검사 기준과 일치할 때 요청에 대해 수행할 작업

웹 ACL 또는 규칙 그룹의 컨텍스트에 있는 규칙만 정의합니다.

CloudFront 로그

이 솔루션은 CloudFront 리소스에 대한 로그를 사용합니다. 이 솔루션의 스캐너 및 프로브 보호 규칙은 이러한 로그를 검사합니다.

IP 세트

IP 세트는 사용하려는 IP 주소 및 IP 주소 범위 모음을 제공합니다.

규칙 문에서를 함께 사용합니다. IP 집합은 AWS 리소스입니다.

Lambda 로그 구문 분석기

이 솔루션은 Amazon Simple Storage Service(Amazon S3) 객체 생성 이벤트에 의해 호출되는 Lambda 함수를 실행합니다. 사용자가 HTTP 서비스 장애 방지 , 스캐너 및 프로브 보호를 활성화할 `yes - AWS Lambda log parser` 때를 선택하면 Lambda 함수가 AWS WAF, CloudFront 또는 ALB 로그 검사를 시작하며, 구조화된 로직 체인을 통해 작동하는 감지를 통해 잘못된 봇 보호 규칙에 사용할 수 있습니다.

관리형 규칙 그룹

관리형 규칙 그룹은 AWS 및 AWS Marketplace 판매자가 자동으로 작성하고 유지 관리하는 사전 정의되고 ready-to-use 수 있는 규칙 모음입니다. AWS WAF 요금은 관리형 규칙 그룹 사용에 적용됩니다.

리소스/엔드포인트 유형

AWS 리소스를 웹 ACLs과 연결하여 보호할 수 있습니다. 이러한 리소스는 CloudFront, ALB, AWS AppSync, Amazon Cognito, AWS App Runner 및 AWS Verified Access 리소스입니다. 현재이 솔루션 Amazon은 CloudFront 및 ALB를 지원합니다.

WAF 로그

이 솔루션은 웹 ACL과 연결된 리소스에 대해 AWS WAF에서 생성된 로그를 사용합니다. 이 솔루션에 대한 HTTP Flood Protection, Scanner & Probe Protection 및 Activate Bad Bot Protection 규칙은 이러한 로그를 검사합니다.

WCU

AWS WAF는 웹 액세스 제어 목록(ACL) 용량 단위(WCUs)를 사용하여 규칙, 규칙 그룹 및 웹 ACLs. AWS WAF는 규칙 그룹 및 웹 ACLs을 구성할 때 WCU 할당량을 적용합니다. WCUs AWS WAF가 웹 트래픽을 검사하는 방식에 영향을 주지 않습니다.

웹 ACL

웹 ACL을 사용하면 보호된 리소스가 응답하는 HTTP(S) 웹 요청을 세밀하게 제어할 수 있습니다.

> **Note**
>
> AWS 용어에 대한 일반적인 참조는 AWS 용어집을 참조하십시오.

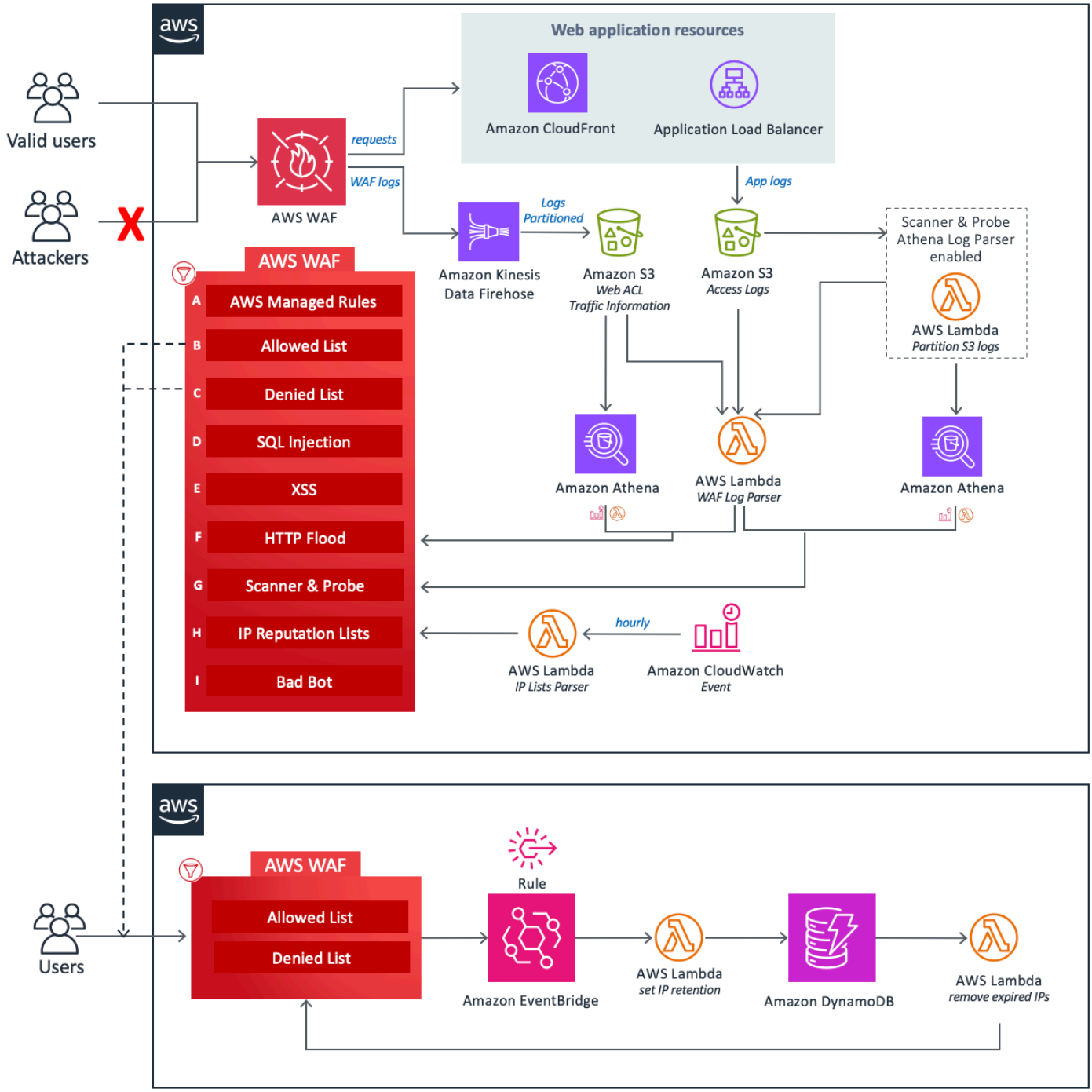
아키텍처 개요

이 섹션에서는 이 솔루션과 함께 배포된 구성 요소에 대한 참조 구현 아키텍처 다이어그램을 제공합니다.

아키텍처 다이어그램

기본 파라미터를 사용하여이 솔루션을 배포하면 AWS 계정에 다음 구성 요소가 배포됩니다.

CloudFormation 템플릿은 AWS WAF 및 기타 AWS 리소스를 배포하여 일반적인 공격으로부터 웹 애플리케이션을 보호합니다.



설계의 핵심은 웹 애플리케이션에 대한 모든 수신 요청에 대한 중앙 검사 및 결정 지점 역할을 하는 AWS WAF 웹 ACL입니다. CloudFormation 스택의 초기 구성 중에 사용자는 활성화할 보호 구성 요소를 정의합니다. 각 구성 요소는 독립적으로 작동하며 웹 ACL에 서로 다른 규칙을 추가합니다.

이 솔루션의 구성 요소는 다음과 같은 보호 영역으로 그룹화할 수 있습니다.

> **Note**
>
> 그룹 레이블은 WAF 규칙의 우선 순위 수준을 반영하지 않습니다.

- AWS 관리형 규칙(A) -이 구성 요소에는 AWS 관리형 규칙 IP 평판 규칙 그룹, 기준 규칙 그룹 및 사용 사례별 규칙 그룹이 포함되어 있습니다. 이러한 규칙 그룹은 자체 규칙을 작성할 필요 없이 OWASP 간행물에 설명된 트래픽을 포함하여 일반적인 애플리케이션 취약성 또는 기타 원치 않는 트래픽의 악용으로부터 보호합니다.
- 수동 IP 목록(B 및 C) - 이러한 구성 요소는 두 개의 AWS WAF 규칙을 생성합니다. 이러한 규칙을 사용하면 허용하거나 거부할 IP 주소를 수동으로 삽입할 수 있습니다. Amazon EventBridge 규칙 및 Amazon DynamoDB를 사용하여 허용되거나 거부된 IP 세트에서 IP 보존을 구성하고 만료된 IP 주소를 제거할 수 있습니다. https://docs.aws.amazon.com/eventbridge/latest/userguide/eb-rules.html 자세한 내용은 허용 및 거부된 AWS WAF IP 세트에서 IP 보존 구성을 참조하세요.
- SQL Injection(D) 및 XSS(E) - 이러한 구성 요소는 URI, 쿼리 문자열 또는 요청 본문의 일반적인 SQL 삽입 또는 교차 사이트 스크립팅(XSS) 패턴으로부터 보호하도록 설계된 두 가지 AWS WAF 규칙을 구성합니다.
- HTTP Flood(F) -이 구성 요소는 웹 계층 DDoS 공격 또는 무차별 대입 로그인 시도와 같은 특정 IP 주소의 많은 요청으로 구성된 공격으로부터 보호합니다. 이 규칙을 사용하면 기본 5분 기간 내에 단일 IP 주소에서 허용되는 최대 수신 요청 수를 정의하는 할당량을 설정합니다(Athena 쿼리 실행 시간 일정 파라미터로 구성 가능). 이 임계값을 위반하면 IP 주소의 추가 요청이 일시적으로 차단됩니다. AWS WAF 속도 기반 규칙을 사용하거나 Lambda 함수 또는 Athena 쿼리를 사용하여 AWS WAF 로그를 처리하여이 규칙을 구현할 수 있습니다. HTTP flood 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.
- 스캐너 및 프로브(G) -이 구성 요소는 오리진에서 생성된 비정상적인 양의 오류와 같은 의심스러운 동작을 검색하는 애플리케이션 액세스 로그를 구문 분석합니다. 그런 다음 고객이 정의한 기간 동안 의심스러운 소스 IP 주소를 차단합니다. Lambda 함수 또는 Athena 쿼리를 사용하여이 규칙을 구현할 수 있습니다. 스캐너 및 프로브 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.
- IP 평판 목록(H) -이 구성 요소는 차단할 새 범위에 대해 서드 파티 IP 평판 목록을 시간별로 확인하는 `IP Lists Parser` Lambda 함수입니다. 이러한 목록에는 Spamhaus Don't Route Or Peer(DROP) 및 Extended DROP(EDROP) 목록, Proofpoint Emerging Threats IP 목록 및 Tor 출구 노드 목록이 포함됩니다.
- 잘못된 봇(I) -이 구성 요소는 허니팟 메커니즘 외에도 Application Load Balancer(ALB) 또는 Amazon CloudFront에 대한 직접 연결을 모니터링하여 잘못된 봇 탐지를 개선합니다. 봇이 허니팟을 우회하

고 ALB 또는 CloudFront와 상호 작용하려고 하면 시스템은 요청 패턴 및 로그를 분석하여 악의적인 활동을 식별합니다. 잘못된 봇이 감지되면 IP 주소가 추출되어 AWS WAF 블록 목록에 추가되어 추가 액세스를 방지합니다. 잘못된 봇 탐지는 구조화된 로직 체인을 통해 작동하여 포괄적인 위협 범위를 보장합니다.

- HTTP Flood Protection Lambda 로그 파서 - 플러드 분석 중에 로그 항목에서 잘못된 봇 IPs를 수집합니다.
- 스캐너 및 프로브 보호 Lambda 로그 파서 - 스캐너 관련 로그 항목에서 잘못된 봇 IPs.
- HTTP Flood Protection Athena Log Parser - 쿼리 실행 전반의 파티션을 사용하여 Athena 로그에서 잘못된 봇 IPs를 추출합니다.
- 스캐너 및 프로브 보호 Athena 로그 파서 - 동일한 파티셔닝 전략을 사용하여 스캐너 관련 Athena 로그에서 잘못된 봇 IPs를 검색합니다.
- 폴백 감지 - HTTP Flood Protection과 스캐너 및 프로브 보호가 모두 비활성화된 경우 시스템은 WAF 레이블 필터를 기반으로 봇 활동을 기록하는 Log Lambda 구문 분석기를 사용합니다.

이 솔루션의 세 가지 사용자 지정 Lambda 함수는 각각 CloudWatch에 런타임 지표를 게시합니다. 이러한 Lambda 함수에 대한 자세한 내용은 구성 요소 세부 정보를 참조하세요.

AWS Well-Architected 설계 고려 사항

이 솔루션은 고객이 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 워크로드를 설계하고 운영할 수 있도록 지원하는 AWS Well-Architected Framework의 모범 사례를 사용합니다.

이 섹션에서는 Well-Architected Framework의 설계 원칙과 모범 사례가 이 솔루션에 어떤 이점을 제공하는지 설명합니다.

운영 우수성

이 섹션에서는 운영 우수성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 솔루션은 지표를 CloudWatch로 푸시하여 인프라, Lambda 함수, Amazon Data Firehose, Amazon S3 버킷 및 나머지 솔루션 구성 요소에 대한 관찰성을 제공합니다.
- AWS 지속적 통합 및 지속적 전달(CI/CD) 파이프라인을 통해 솔루션을 개발, 테스트 및 게시합니다. 이를 통해 개발자는 고품질 결과를 일관되게 달성할 수 있습니다.

- 계정에 필요한 모든 리소스를 프로비저닝하는 CloudFormation 템플릿을 사용하여 솔루션을 설치할 수 있습니다. 솔루션을 업데이트하거나 삭제하려면 템플릿을 업데이트하거나 삭제하기만 하면 됩니다.

보안

이 섹션에서는 보안 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 모든 서비스 간 통신은 AWS Identity and Access Management(IAM) 역할을 사용합니다.
- 솔루션에서 사용하는 모든 역할은 최소 권한 액세스를 따릅니다. 즉, 서비스가 제대로 작동하는 데 필요한 최소 권한만 포함됩니다.
- Amazon S3 버킷 및 DynamoDB를 포함한 모든 데이터 스토리지에는 저장 데이터 암호화가 있습니다.

신뢰성

이 섹션에서는 신뢰성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 가능한 경우 AWS 서버리스 서비스(예: Lambda, Firehose, Amazon S3, Athena)를 사용하여 서비스 장애로부터 고가용성과 복구를 보장합니다.
- 솔루션에 대한 자동 테스트를 수행하여 오류를 신속하게 감지하고 수정합니다.
- 이 솔루션은 데이터 처리에 Lambda 함수를 사용합니다. 솔루션은 Amazon S3 및 DynamoDB에 데이터를 저장하며 기본적으로 여러 가용 영역에 유지됩니다.

성능 효율성

이 섹션에서는 성능 효율성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 서버리스 아키텍처를 사용하여 저렴한 비용으로 높은 확장성과 가용성을 보장합니다.
- 이 솔루션은 데이터를 분할하고 쿼리를 최적화하여 데이터 스캔 양을 줄이고 더 빠른 결과를 달성하여 데이터베이스 성능을 향상시킵니다.
- 솔루션은 매일 자동으로 테스트되고 배포됩니다. 솔루션 아키텍트와 주제 전문가는 솔루션을 검토하여 실험하고 개선할 영역을 찾습니다.

비용 최적화

이 섹션에서는 비용 최적화 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 서버리스 아키텍처를 사용하며 고객은 사용한 만큼만 비용을 지불합니다.
- 솔루션의 컴퓨팅 계층은 기본적으로 pay-per-use 모델을 사용하는 Lambda로 설정됩니다.
- Athena 데이터베이스 및 쿼리는 데이터 스캔 양을 줄이도록 최적화되어 비용을 절감합니다.

지속 가능성

이 섹션에서는 지속 가능성 요소의 원칙과 모범 사례를 사용하여 이 솔루션을 설계한 방법을 설명합니다.

- 이 솔루션은 관리형 및 서버리스 서비스를 사용하여 백엔드 서비스의 환경 영향을 최소화합니다.
- 솔루션의 서버리스 설계는 지속적으로 운영되는 온프레미스 서버의 공간에 비해 탄소 발자국을 줄이는 것을 목표로 합니다.

아키텍처 세부 정보

이 섹션에서는이 솔루션을 구성하는 구성 요소 및 AWS 서비스와 이러한 구성 요소가 함께 작동하는 방식에 대한 아키텍처 세부 정보를 설명합니다.

이 솔루션의 AWS 서비스

AWS 서비스	설명
AWS WAF	Core. AWS WAF 웹 ACL, AWS 관리형 규칙 규칙 그룹, 사용자 지정 규칙 및 IP 세트를 배포합니다. AWS WAF API를 호출하여 일반적인 공격을 차단하고 웹 애플리케이션을 보호합니다.
Amazon Data Firehose	Core. Amazon S3 버킷에 AWS WAF 로그를 전송합니다.
Amazon S3	Core. AWS WAF, CloudFront 및 ALB 로그를 저장합니다.
Lambda	Core. 사용자 지정 규칙을 지원하기 위해 여러 Lambda 함수를 배포합니다.
Amazon EventBridge	Core. Lambda를 호출하는 이벤트 규칙을 생성합니다.
Amazon Athena	지원. Athena 로그 구문 분석기를 지원하는 Athena 쿼리 및 작업 그룹을 생성합니다.
AWS Glue	지원. Athena 로그 구문 분석기를 지원하는 데이터베이스와 테이블을 생성합니다.
Amazon SNS	지원. Amazon Simple Notification Service(Amazon SNS) 이메일 알림을 전송하여 허용 및 거부 목록에서 IP 보존을 지원합니다.

AWS 서비스	설명
AWS Systems Manager	지원. 리소스 운영 및 비용 데이터에 대한 애플리케이션 수준의 리소스 모니터링 및 시각화를 제공합니다.

로그 구문 분석기 옵션

아키텍처 개요에 설명된 대로 HTTP flood와 스캐너 및 프로브 보호를 처리하는 세 가지 옵션이 있습니다. 다음 섹션에서는 이러한 각 옵션에 대해 자세히 설명합니다.

AWS WAF 속도 기반 규칙

HTTP 플러드 보호에는 속도 기반 규칙을 사용할 수 있습니다. 기본적으로 속도 기반 규칙은 요청 IP 주소에 기반하여 요청을 집계하고 속도를 제한합니다. 이 솔루션을 사용하면 클라이언트 IP가 지속적으로 업데이트된 후행 5분 동안 허용하는 웹 요청 수를 지정할 수 있습니다. IP 주소가 구성된 할당량을 위반하면 AWS WAF는 요청 속도가 구성된 할당량보다 작을 때까지 차단된 새 요청을 차단합니다.

요청 할당량이 5분당 요청 2,000개를 초과하고 사용자 지정을 구현할 필요가 없는 경우 속도 기반 규칙 옵션을 선택하는 것이 좋습니다. 예를 들어 요청을 계산할 때 정적 리소스 액세스를 고려하지 않습니다.

다른 다양한 집계 키와 키 조합을 사용하도록 규칙을 추가로 구성할 수 있습니다. 자세한 내용은 집계 옵션 및 키를 참조하세요.

Amazon Athena 로그 구문 분석기

HTTP Flood Protection과 스캐너 및 프로브 보호 템플릿 파라미터 모두 Athena 로그 구문 분석기 옵션을 제공합니다. 활성화되면 CloudFormation은 Athena 쿼리와 Athena가 AWS WAF를 실행, 결과 출력 처리 및 업데이트하도록 오케스트레이션하는 예약된 Lambda 함수를 프로비저닝합니다. 이 Lambda 함수는 5분마다 실행되도록 구성된 CloudWatch 이벤트에 의해 호출됩니다. 이는 Athena 쿼리 실행 시간 일정 파라미터로 구성할 수 있습니다.

AWS WAF 속도 기반 규칙을 사용할 수 없고 SQL에 익숙하여 사용자 지정을 구현하는 경우이 옵션을 선택하는 것이 좋습니다. 기본 쿼리를 변경하는 방법에 대한 자세한 내용은 Amazon Athena 쿼리 보기를 참조하세요.

HTTP 플러드 보호는 AWS WAF 액세스 로그 처리를 기반으로 하며 WAF 로그 파일을 사용합니다. WAF 액세스 로그 유형은 지연 시간이 더 짧으므로 CloudFront 또는 ALB 로그 전송 시간에 비해 HTTP

플러드 오리진을 더 빠르게 식별하는 데 사용할 수 있습니다. 하지만 응답 상태 코드를 수신하려면 스캐너 및 프로브 보호 활성화 템플릿 파라미터에서 CloudFront 또는 ALB 로그 유형을 선택해야 합니다.

> **Note**
>
> 잘못된 봇이 허니팟을 우회하고 ALB 또는 CloudFront와 직접 상호 작용하는 경우 HTTP Flood Protection과 스캐너 및 프로브 보호가 모두 Lambda 로그 파서를 사용하지 않는 경우를 제외하고 시스템은 로그 분석을 통해 악의적인 동작을 감지합니다.

AWS Lambda 로그 구문 분석기

HTTP Flood Protection 및 스캐너 및 프로브 보호 템플릿 파라미터는 AWS Lambda 로그 구문 분석기 옵션을 제공합니다. AWS WAF 속도 기반 규칙 및 Amazon Athena 로그 구문 분석기 옵션을 사용할 수 없는 경우에만 Lambda 로그 구문 분석기를 사용합니다. 이 옵션의 알려진 제한 사항은 처리 중인 파일의 컨텍스트 내에서 정보가 처리된다는 것입니다. 예를 들어 IP는 정의된 할당량보다 더 많은 요청이나 오류를 생성할 수 있지만,이 정보는 서로 다른 파일로 분할되므로 각 파일은 할당량을 초과할 만큼 충분한 데이터를 저장하지 않습니다.

> **Note**
>
> 또한 잘못된 봇이 허니팟을 우회하고 ALB 또는 CloudFront와 직접 상호 작용하는 경우 탐지는 선택한 로그 파서 옵션을 사용하여 악의적인 활동을 효과적으로 식별하고 차단합니다.

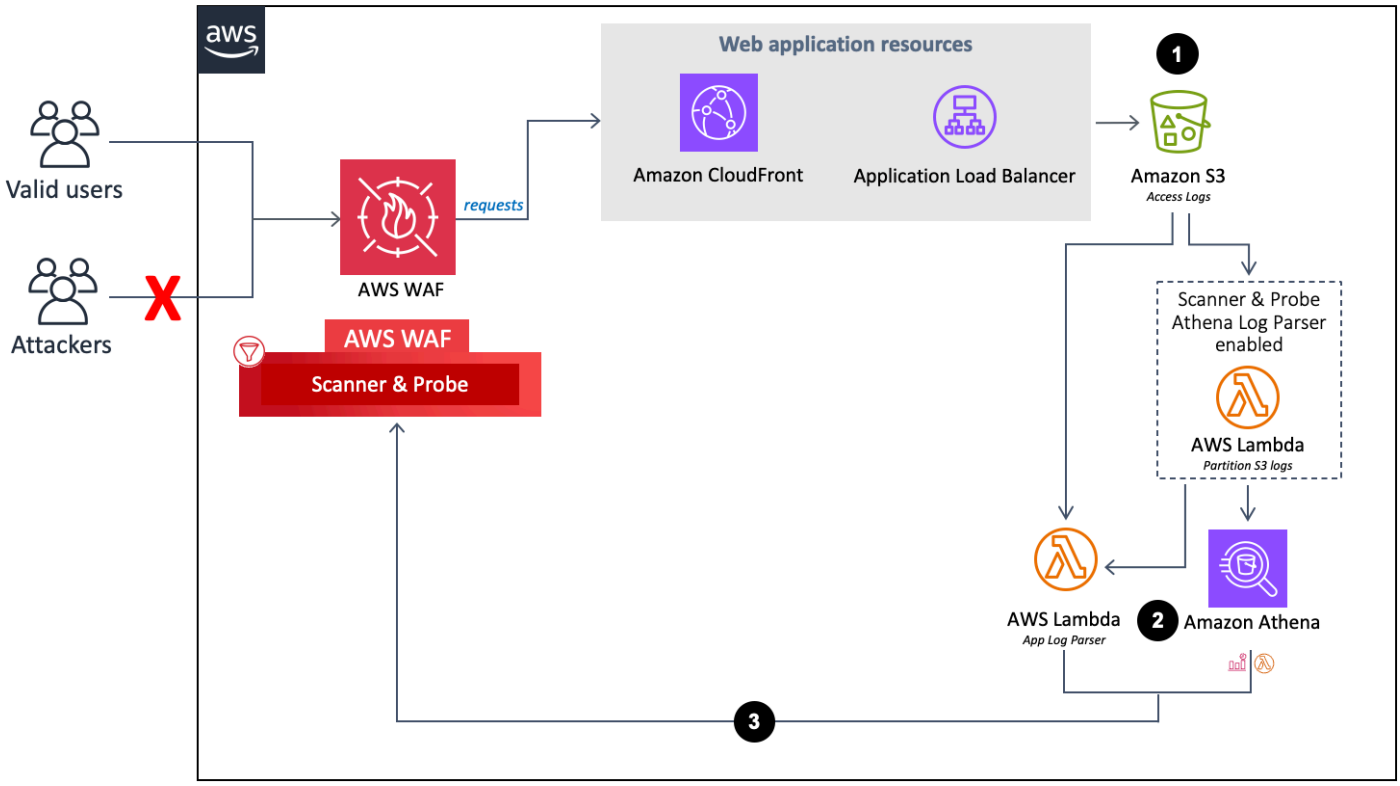
구성 요소 세부 정보

아키텍처 다이어그램에 설명된 대로이 솔루션의 구성 요소 중 4개는 자동화를 사용하여 IP 주소를 검사하고 이를 AWS WAF 블록 목록에 추가합니다. 다음 섹션에서는 이러한 각 구성 요소에 대해 자세히 설명합니다.

로그 구문 분석기 - 애플리케이션

애플리케이션 로그 구문 분석기는 스캐너 및 프로브로부터 보호하는 데 도움이 됩니다.

애플리케이션 로그 구문 분석기 흐름.



1. CloudFront 또는 ALB는 웹 애플리케이션을 대신하여 요청을 수신하면 액세스 로그를 Amazon S3 버킷으로 전송합니다.

   a. (선택 사항) 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해 HTTP 서비스 장애 방지 활성화 및 스캐너 및 프로브 보호 활성화를 선택하면 Lambda 함수는 Amazon S3에 도착하면 액세스 로그를 원래 폴더 *<customer-bucket>*에서 /AWSLogs 새로 분할된 폴더 *<customer-bucket>* /AWSLogs-partitioned/ *<optional-prefix>* /year= *<YYYY>* / month= *<MM>* /day= *<DD>* /hour= *<HH>*/로 이동합니다.

   b. (선택 사항) 원본 S3에 데이터 보관 위치 템플릿 파라미터yes로를 선택하면 로그가 원본 위치에 남아 분할된 폴더에 복사되어 로그 스토리지가 복제됩니다.

> **Note**
>
> Athena 로그 구문 분석기의 경우이 솔루션은이 솔루션을 배포한 후 Amazon S3 버킷에 도착하는 새 로그만 분할합니다. 분할하려는 기존 로그가 있는 경우이 솔루션을 배포한 후 해당 로그를 Amazon S3에 수동으로 업로드해야 합니다.

2. 템플릿 파라미터에 대한 선택에 따라 이 솔루션은 다음 중 하나를 사용하여 로그를 처리합니다.

a. Lambda - 새 액세스 로그가 Amazon S3 버킷에 저장될 때마다 `Log Parser` Lambda 함수가 시작됩니다.

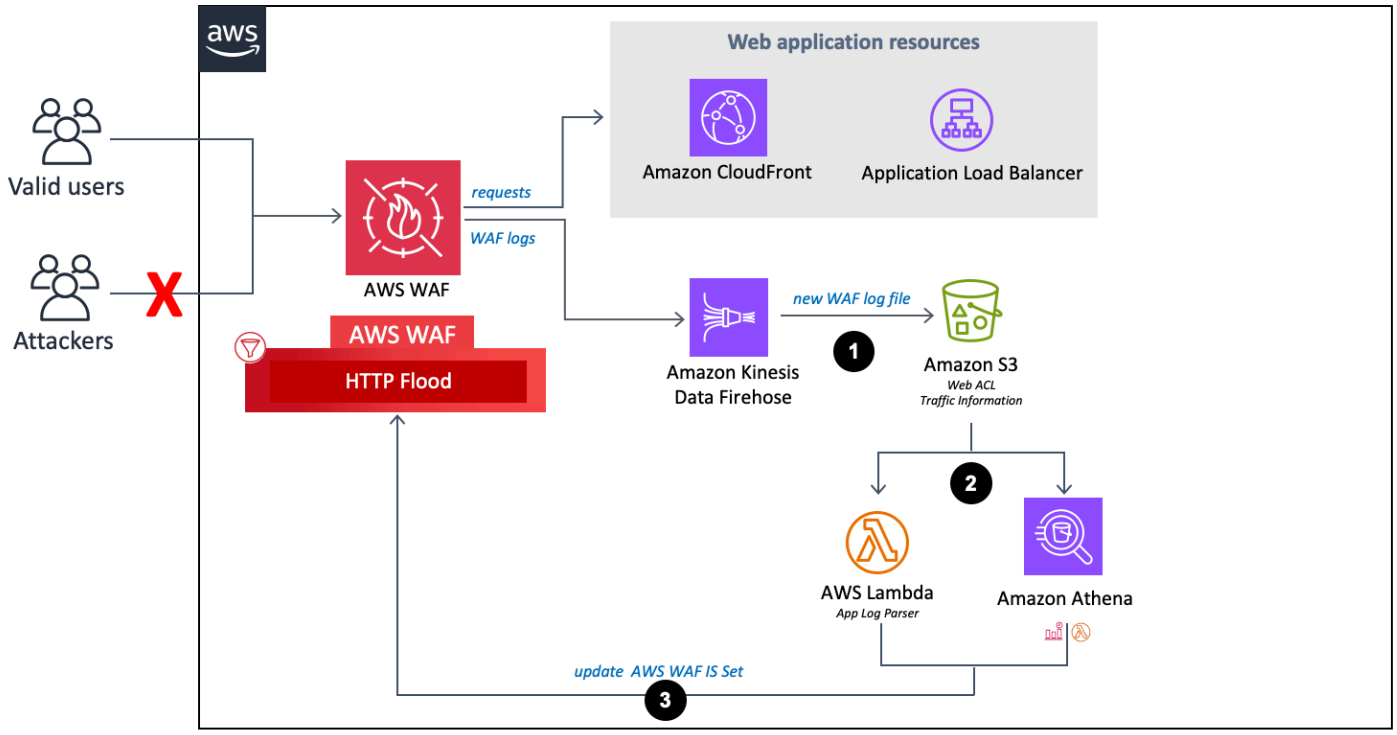
b. Athena - 기본적으로 5분마다 스캐너 및 프로브 보호 Athena 쿼리가 실행되고 출력이 AWS WAF로 푸시됩니다. 이 프로세스는 Athena 쿼리 실행을 담당하는 Lambda 함수를 시작하고 결과를 AWS WAF로 푸시하는 CloudWatch 이벤트에 의해 시작됩니다.

3. 이 솔루션은 로그 데이터를 분석하여 정의된 할당량보다 더 많은 오류를 생성한 IP 주소를 식별합니다. 그런 다음 솔루션은 AWS WAF IP 세트 조건을 업데이트하여 고객이 정의한 기간 동안 해당 IP 주소를 차단합니다.

로그 구문 분석기 - AWS WAF

HTTP Flood 보호 활성화`yes - Amazon Athena log parser`에서 `yes - AWS Lambda log parser` 또는를 선택하면이 솔루션은 AWS WAF 로그를 구문 분석하여 정의한 할당량보다 큰 요청 속도로 엔드포인트를 플러딩하는 오리진을 식별하고 차단하는 다음 구성 요소를 프로비저닝합니다.

AWS WAF 로그 구문 분석기 흐름.



1. AWS WAF는 액세스 로그를 수신하면 Firehose 엔드포인트로 로그를 전송합니다. 그런 다음 Firehose는 <*customer-bucket*> <optional-prefix> /AWSLogs/ <YYYY> /year= <MM> / month= </day=*DD*> /hour= <HH>라는 Amazon S3의 분할된 버킷에 로그를 전송합니다. /

2. 템플릿 파라미터인 HTTP 서비스 장애 방지 활성화 및 스캐너 및 프로브 보호 활성화에 대한 선택에 따라이 솔루션은 다음 중 하나를 사용하여 로그를 처리합니다.

   a. Lambda: 새 액세스 로그가 Amazon S3 버킷에 저장될 때마다 `Log Parser` Lambda 함수가 시작됩니다.

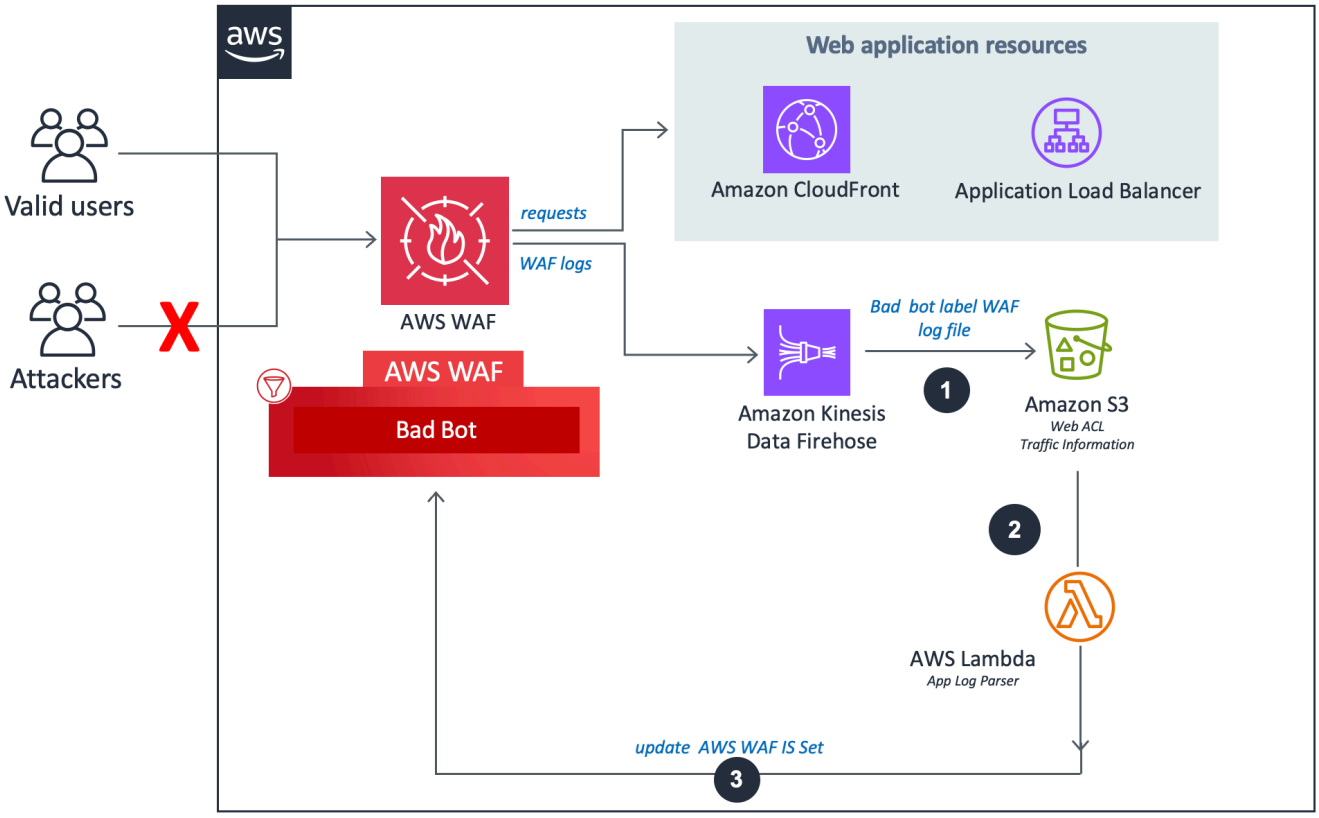
   b. Athena: 기본적으로 5분마다 스캐너 및 프로브 Athena 쿼리가 실행되고 출력이 AWS WAF로 푸시됩니다. 이 프로세스는 Amazon CloudWatch 이벤트에 의해 시작되며, Amazon Athena 쿼리 실행을 담당하는 Lambda 함수를 시작하고 결과를 AWS WAF로 푸시합니다.

3. 이 솔루션은 로그 데이터를 분석하여 정의된 할당량보다 많은 요청을 보낸 IP 주소를 식별합니다. 그런 다음 솔루션은 AWS WAF IP 세트 조건을 업데이트하여 고객이 정의한 기간 동안 해당 IP 주소를 차단합니다.

로그 구문 분석기 - 잘못된 봇

잘못된 봇 로그 구문 분석기는 허니팟 엔드포인트에 대한 요청을 검사하여 소스 IP 주소를 추출합니다.

봇 로그 구문 분석기 흐름이 잘못되었습니다.

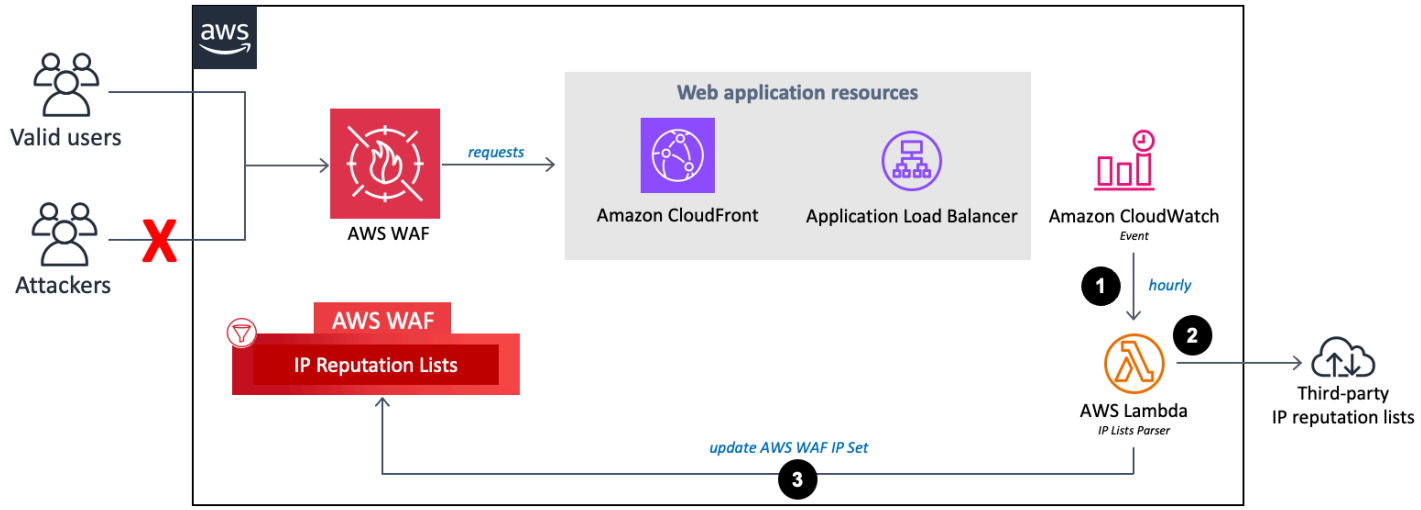


1. `Bad Bot Protection`가 활성화되고 HTTP Flood Protection 및 스캐너 및 프로브 보호 기능이 모두 비활성화된 경우: 시스템은 WAF 레이블 필터를 기반으로 잘못된 봇 요청만 로깅하는 로그 Lambda 구문 분석기를 사용합니다.
2. Lambda 함수는 요청 헤더를 가로채고 검사하여 트랩 엔드포인트에 액세스한 소스의 IP 주소를 추출합니다.
3. 이 솔루션은 로그 데이터를 분석하여 정의된 할당량보다 많은 요청을 보낸 IP 주소를 식별합니다. 그런 다음 솔루션은 AWS WAF IP 세트 조건을 업데이트하여 고객이 정의한 기간 동안 해당 IP 주소를 차단합니다.

IP 목록 구문 분석기

`IP Lists Parser` Lambda 함수는 타사 IP 평판 목록에서 식별된 알려진 공격자로부터 보호하는 데 도움이 됩니다.

IP 평가에는 구문 분석기 흐름이 나열됩니다.



1. 시간당 Amazon CloudWatch 이벤트는 `IP Lists Parser` Lambda 함수를 호출합니다.
2. Lambda 함수는 다음 세 가지 소스에서 데이터를 수집하고 구문 분석합니다.
   - Spamhaus DROP 및 EDROP 목록
   - Proofpoint 새로운 위협 IP 목록
   - Tor 종료 노드 목록
3. Lambda 함수는 AWS WAF 블록 목록을 현재 IP 주소로 업데이트합니다.

배포 계획

이 섹션에서는 솔루션을 배포하기 전에 발생하는 비용, 보안, 할당량 및 기타 고려 사항에 대해 설명합니다.

지원되는 AWS 리전

정의한 템플릿 입력 파라미터 값에 따라이 솔루션에는 다양한 리소스가 필요합니다. 일부 AWS 리전에서는 이러한 리소스(다음 표에 나와 있음)를 사용하지 못할 수 있습니다. 따라서 이러한 서비스를 사용할 수 있는 AWS 리전에서이 솔루션을 시작해야 합니다. 리전별 AWS 서비스의 최신 가용성은 AWS 리전 서비스 목록을 참조하세요.

	AWS WAF 웹 ACL	Glue	Amazon Athena	Amazon Kinesis Data Firehose
[엔드포인트 유형]				
CloudFront	✓			
Application Load Balancer(ALB)	✓			
HTTP 서비스 장애 방지 활성화				
예 - AWS Lambda 로그 구문 분석기				✓
예 - Amazon Athena 로그 구문 분석기		✓	✓	✓
스캐너 및 프로브 보호 활성화				

	AWS WAF 웹 ACL	Glue	Amazon Athena	Amazon Kinesis Data Firehose
예 - Amazon Athena 로그 구문 분석기		✓	✓	

> **Note**
>
> 엔드포인트CloudFront로를 선택하는 경우 미국 동부(버지니아 북부) 리전()에 솔루션을 배포해야 합니다.us-east-1

비용

AWS WAF용 보안 자동화 솔루션을 실행하는 동안 사용되는 AWS 서비스의 비용은 사용자의 책임입니다. 이 솔루션을 실행하는 데 드는 총 비용은 활성화된 보호와 수집, 저장 및 처리된 데이터의 양에 따라 달라집니다.

비용 관리에 도움이 되도록 AWS Cost Explorer를 통해 예산을 생성하는 것이 좋습니다. 자세한 내용은 이 솔루션에서 사용한 각 AWS 서비스의 요금 웹 페이지를 참조하세요.

다음 표는 미국 동부(버지니아 북부) 리전(AWS 프리 티어 제외)에서이 솔루션을 실행하기 위한 비용 분석의 예입니다. 요금은 변경될 수 있습니다.

예제 1: 평판 목록 보호 활성화, 잘못된 봇 보호, HTTP 플러드 보호를 위한 AWS Lambda 로그 파서, 스캐너 및 프로브 보호

AWS 서비스	차원/월	비용[USD]
Amazon Data Firehose	100GB	~$2.90
Amazon S3	100GB	~$2.30
AWS Lambda	128MB: Lambda 실행당 3개의 함수, 1M 간접 호출 및 평균 500밀리초 기간	~$5.40

AWS 서비스	차원/월	비용[USD]
	512MB: Lambda 실행당 2개의 함수, 1M 호출 및 평균 500밀리초 기간	
AWS WAF 웹 ACL	1	5.00 USD
AWS WAF 규칙	4	4.00 USD
AWS WAF 요청	100만	0.60 USD
합계		매월 ~$20.60

예제 2: 평판 목록 보호 활성화, 잘못된 봇 보호, HTTP 플러드 보호를 위한 Amazon Athena 로그 파서, 스캐너 및 프로브 보호

AWS 서비스	차원/월	비용[USD]
Amazon Data Firehose	100GB	~$2.90
Amazon S3	100GB	~$2.30
AWS Lambda	128MB: Lambda 실행당 함수 3개, 간접 호출 1M 및 평균 500밀리초 기간 512MB: Lambda 실행당 함수 2개, 간접 호출 7,560개, 평균 500밀리초 기간	~$1.26
Amazon Athena	적중 또는 요청당 약 500바이트 로그 레코드를 생성하는 하루에 120만 개의 CloudFront 객체 적중 또는 120만 개의 ALB 요청	~$4.32
AWS WAF 웹 ACL	1	5.00 USD

AWS 서비스	차원/월	비용[USD]
AWS WAF 규칙	4	4.00 USD
AWS WAF 요청	100만	0.60 USD
합계		매월 ~$20.38

예제 3: 허용 및 거부된 IP 세트에 대한 IP 보존 활성화

AWS 서비스	차원/월	비용[USD]
Amazon DynamoDB	1K 쓰기 및 1MB 데이터 스토리지	~$0.00
AWS Lambda	128MB: Lambda 실행당 함수 1개, 간접 호출 2K 및 평균 500밀리초 기간 512MB: Lambda 실행당 함수 1개, 간접 호출 2K 및 평균 500밀리초 기간	~$0.01
Amazon CloudWatch	2K 이벤트	~$0.00
AWS WAF 웹 ACL	1	5.00 USD
AWS WAF 규칙	2	2.00 USD
WAS WAF 요청	100만	0.60 USD
합계		매월 ~$7.61

CloudWatch 로그의 비용 추정

Lambda와 같이이 솔루션에 사용되는 일부 AWS 서비스는 CloudWatch 로그를 생성합니다. 이러한 로그에는 요금이 부과됩니다. 비용을 줄이려면 로그를 삭제하거나 보관하는 것이 좋습니다. 로그 아카이

브 세부 정보는 Amazon CloudWatch Logs 사용 설명서의 Amazon S3로 로그 데이터 내보내기를 참조하세요 Amazon CloudWatch.

설치 시 Athena 로그 파서를 사용하도록 선택한 경우이 솔루션은 구성된 대로 Amazon S3 버킷(들)의 AWS WAF 또는 애플리케이션 액세스 로그에 대해 실행되도록 쿼리를 예약합니다. 각 쿼리에서 스캔한 데이터의 양을 기준으로 요금이 부과됩니다. 이 솔루션은 로그 및 쿼리에 파티셔닝을 적용하여 비용을 최소화합니다. 기본적으로 솔루션은 애플리케이션 액세스 로그를 원래 Amazon S3 위치에서 분할된 폴더 구조로 이동합니다. 원본을 보존할 수도 있지만 중복된 로그 스토리지에 대한 요금이 부과됩니다. 이 솔루션은 작업 그룹을 사용하여 워크로드를 분할하며 쿼리 액세스와 비용을 모두 관리하도록 구성할 수 있습니다. 샘플 비용 견적 계산은 Athena의 비용 견적을 참조하세요. 자세한 내용은 Amazon Athena 요금을 참조하세요.

Athena의 예상 비용

HTTP 서비스 장애 방지, 스캐너 및 프로브 보호 또는 잘못된 봇 보호 규칙을 실행하는 동안 Athena 로그 구문 분석기 옵션을 사용하는 경우 Athena 사용에 대한 요금이 부과됩니다. 기본적으로 각 Athena 쿼리는 5분마다 실행되며 지난 4시간 동안의 데이터를 스캔합니다. 이 솔루션은 로그 및 Athena 쿼리에 파티셔닝을 적용하여 비용을 최소화합니다. WAF Block Period 템플릿 파라미터의 값을 변경하여 쿼리가 스캔하는 데이터 시간을 구성할 수 있습니다. 그러나 스캔되는 데이터의 양을 늘리면 Athena 비용이 증가할 수 있습니다.

> **Tip**
>
> 다음은 CloudFront 로그 비용 계산의 예입니다.
> 평균적으로 각 CloudFront 적중은 약 500바이트의 데이터를 생성할 수 있습니다.
> 하루에 120만 개의 CloudFront 객체 적중이 있는 경우 데이터가 일관된 속도로 수집된다고 가정하면 4시간당 200K(120만/6) 적중이 발생합니다. 비용을 계산할 때 실제 트래픽 패턴을 고려하세요.
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena는 스캔한 데이터의 TB당 5.00 USD를 청구합니다.
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> Athena 쿼리는 5분마다 실행되며, 시간당 12회 실행됩니다.
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`

실제 비용은 애플리케이션의 트래픽 패턴에 따라 달라집니다. 자세한 내용은 Amazon Athena 요금을 참조하세요.

보안

AWS 인프라에 시스템을 구축하면 사용자와 AWS 간에 보안 책임이 공유됩니다. AWS는 호스트 운영 체제, 가상화 계층, 서비스가 운영되는 시설의 물리적 보안을 포함한 구성 요소를 운영, 관리 및 제어하므로이 공동 책임 모델은 운영 부담을 줄입니다. AWS 보안에 대한 자세한 내용은 AWS Cloud Security를 참조하십시오.

IAM 역할

IAM 역할을 사용하면 AWS 클라우드의 서비스 및 사용자에게 세분화된 액세스, 정책 및 권한을 할당할 수 있습니다. 이 솔루션은 최소 권한을 가진 IAM 역할을 생성하며, 이러한 역할은 솔루션의 리소스에 필요한 권한을 부여합니다.

Data

Amazon S3 버킷 및 DynamoDB 테이블에 저장된 모든 데이터는 저장 시 암호화됩니다. Firehose를 통해 전송 중인 데이터도 암호화됩니다.

보호 기능

웹 애플리케이션은 다양한 공격에 취약합니다. 이러한 공격에는 취약성을 악용하거나 서버를 제어하도록 특별히 설계된 요청, 웹 사이트를 파괴하도록 설계된 볼륨 측정 공격, 웹 콘텐츠를 스크래핑하고 도용하도록 프로그래밍된 잘못된 봇 및 스크레이퍼가 포함됩니다.

이 솔루션은 CloudFormation을 사용하여 AWS 관리형 규칙 그룹 및 사용자 지정 규칙을 포함한 AWS WAF 규칙을 구성하여 다음과 같은 일반적인 공격을 차단합니다.

- AWS 관리형 규칙 -이 관리형 서비스는 일반적인 애플리케이션 취약성 또는 기타 원치 않는 트래픽에 대한 보호를 제공합니다. 이 솔루션에는 AWS 관리형 IP 평판 규칙 그룹, AWS 관리형 기준 규칙 그룹 및 AWS 관리형 사용 사례별 규칙 그룹이 포함됩니다. 최대 웹 ACL 용량 단위(WCU) 할당량까지 웹 ACL에 대해 하나 이상의 규칙 그룹을 선택할 수 있습니다.
- SQL 삽입 - 공격자는 악성 SQL 코드를 웹 요청에 삽입하여 데이터베이스에서 데이터를 추출합니다. 이 솔루션은 잠재적으로 악성 SQL 코드가 포함된 웹 요청을 차단하도록 설계되었습니다.

- XSS - 공격자는 양성 웹 사이트의 취약성을 차량으로 사용하여 악의적인 클라이언트 사이트 스크립트를 합법적인 사용자의 웹 브라우저에 삽입합니다. 일반적으로 탐색되는 수신 요청 요소를 검사하여 XSS 공격을 식별하고 차단하도록 설계되었습니다.
- HTTP 플러드 - 웹 서버 및 기타 백엔드 리소스는 HTTP 플러드와 같은 DDoS 공격의 위험이 있습니다. 이 솔루션은 클라이언트의 웹 요청이 구성 가능한 할당량을 초과할 때 속도 기반 규칙을 자동으로 호출합니다. 또는 Lambda 함수 또는 Athena 쿼리를 사용하여 AWS WAF 로그를 처리하여이 할당량을 적용할 수 있습니다.
- 스캐너 및 프로브 - 악성 소스는 HTTP 4xx 오류 코드를 생성하는 일련의 요청을 전송하여 인터넷 경계 웹 애플리케이션의 취약성을 스캔하고 프로브합니다. 이 기록을 사용하여 악성 소스 IP 주소를 식별하고 차단할 수 있습니다. 이 솔루션은 CloudFront 또는 ALB 액세스 로그를 자동으로 구문 분석하고, 분당 고유한 소스 IP 주소의 잘못된 요청 수를 계산하고, 정의된 오류 할당량에 도달한 주소의 추가 스캔을 차단하도록 AWS WAF를 업데이트하는 Lambda 함수 또는 Athena 쿼리를 생성합니다.
- 알려진 공격자 출처(IP 평판 목록) - 많은 조직이 스팸 메일, 멀웨어 배포자, 봇넷 등 알려진 공격자가 운영하는 IP 주소의 평판 목록을 유지합니다. 이 솔루션은 이러한 평판 목록의 정보를 활용하여 악성 IP 주소의 요청을 차단하는 데 도움이 됩니다. 또한이 솔루션은 Amazon 내부 위협 인텔리전스를 기반으로 IP 평판 규칙 그룹으로 식별된 공격자를 차단합니다.
- 봇 및 스크레이퍼 - 공개적으로 액세스할 수 있는 웹 애플리케이션 운영자는 콘텐츠에 액세스하는 클라이언트가 자신을 정확하게 식별하고 의도한 대로 서비스를 사용한다고 신뢰해야 합니다. 그러나 콘텐츠 스크레이퍼 또는 잘못된 봇과 같은 일부 자동화된 클라이언트는 제한을 우회하도록 잘못 표현됩니다. 이 솔루션은 잘못된 봇과 스크레이퍼를 식별하고 차단하는 데 도움이 됩니다.

할당량

서비스 할당량(제한이라고도 함)은 AWS 계정의 최대 서비스 리소스 또는 작업 수입니다.

이 솔루션의 AWS 서비스에 대한 할당량

이 솔루션에 구현된 각 서비스의 할당량이 충분한지 확인하세요. 자세한 내용은 AWS 서비스 할당량을 참조하세요. 페이지를 전환하지 않고 설명서에서 모든 AWS 서비스에 대한 서비스 할당량을 보려면 대신 PDF의 서비스 엔드포인트 및 할당량 페이지에서 정보를 확인합니다.

AWS WAF 할당량

AWS WAF는 IP 일치 조건당 Classless Inter-Domain Routing(CIDR) 표기법으로 최대 10,000개의 IP 주소 범위를 차단할 수 있습니다. 이 솔루션이 생성하는 각 목록에는이 할당량이 적용됩니다. 자세한 내용은 AWS WAF 할당량을 참조하세요. 버전 3.0부터이 솔루션은 각 규칙에 연결할 두 개의 IP 세트를 생성합니다. 하나는 IPv4용이고 다른 하나는 IPv6용입니다.

AWS WAF는 개별 , `Create` `Put`또는 `Update` 작업에 대한 API 호출에 대해 AWS 리전별로 계정당 초당 최대 1개의 요청을 허용합니다. 솔루션 외부에서 이러한 API를 호출하면 API 제한 문제가 발생할 수 있습니다. 문제를 방지하려면이 솔루션이 배포된 동일한 계정 및 리전에서 이러한 API 호출을 수행하는 다른 애플리케이션을 실행하지 않는 것이 좋습니다.

배포 고려 사항

다음 섹션에서는이 솔루션을 구현하기 위한 제약 조건과 고려 사항을 제공합니다.

AWS WAF 규칙

이 솔루션이 생성하는 웹 ACL은 웹 애플리케이션에 대한 포괄적인 보호를 제공하도록 설계되었습니다. 이 솔루션은 웹 ACL에 추가할 수 있는 AWS 관리형 규칙 및 사용자 지정 규칙 세트를 제공합니다. 규칙을 포함하려면 CloudFormation 스택을 시작할 때 관련 파라미터에 `yes` 대해를 선택합니다. 1단계를 참조하세요. 파라미터 목록에 대한 스택을 시작합니다.

> **Note**
>
> out-of-box 제공 솔루션은 AWS Firewall Manager를 지원하지 않습니다. Firewall Manager의 규칙을 사용하려면 소스 코드에 사용자 지정을 적용하는 것이 좋습니다.

웹 ACL 트래픽 로깅

미국 동부(버지니아 북부) 이외의 AWS 리전에서 스택을 생성하고 엔드포인트를 로 설정하는 경우 HTTP 서비스 장애 방지 활성화를 no 또는 로 설정해야 `CloudFront`합니다`yes - AWS WAF rate based rule`.

다른 두 옵션(`yes - AWS Lambda log parser` 및 `yes - Amazon Athena log parser`)은 모든 AWS 엣지 로케이션에서 실행되는 웹 ACL에서 AWS WAF 로그를 활성화해야 하며 미국 동부(버지니아 북부) 외부에서는 지원되지 않습니다. 웹 ACL 트래픽 로깅에 대한 자세한 내용은 AWS WAF 개발자 안내서를 참조하세요.

요청 구성 요소의 크기 초과 처리

AWS WAF는 웹 요청 구성 요소의 본문, 헤더 또는 쿠키에 대한 크기 초과 콘텐츠 검사를 지원하지 않습니다. 이러한 요청 구성 요소 유형 중 하나를 검사하는 규칙 문을 작성할 때 다음 옵션 중 하나를 선택하여 AWS WAF에 이러한 요청으로 수행할 작업을 지시할 수 있습니다.

- yes (계속) - 규칙 검사 기준에 따라 요청 구성 요소를 정상적으로 검사합니다. AWS WAF는 크기 제한 내에 있는 요청 구성 요소 콘텐츠를 검사합니다. 솔루션에 사용되는 기본 옵션입니다.
- yes - MATCH - 웹 요청을 규칙 문과 일치하는 것으로 처리합니다. AWS WAF는 규칙의 검사 기준에 따라 평가하지 않고 요청에 규칙 작업을 적용합니다. Block 작업이 있는 규칙의 경우 과대 구성 요소로 요청을 차단합니다.
- yes - NO_MATCH - 웹 요청을 규칙의 검사 기준에 따라 평가하지 않고 규칙 문과 일치하지 않는 것으로 취급합니다. AWS WAF는 일치하지 않는 규칙과 마찬가지로 웹 ACL의 나머지 규칙을 사용하여 웹 요청에 대한 검사를 계속합니다.

자세한 내용은 AWS WAF에서 과대 웹 요청 구성 요소 처리를 참조하세요.

다중 솔루션 배포

솔루션을 동일한 계정 및 리전에 여러 번 배포할 수 있습니다. 각 배포에 고유한 CloudFormation 스택 이름과 Amazon S3 버킷 이름을 사용해야 합니다. 각 고유 배포에는 추가 요금이 발생하며 리전별 계정당 AWS WAF 할당량이 적용됩니다.

배포를 위한 최소 역할 권한(선택 사항)

고객은 배포에 필요한 최소 권한으로 IAM 역할을 수동으로 생성할 수 있습니다.

- WAF 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:CreateWebACL",
                "wafv2:UpdateWebACL",
                "wafv2:DeleteWebACL",
                "wafv2:GetWebACL",
                "wafv2:ListWebACLs",
                "wafv2:CreateIPSet",
                "wafv2:UpdateIPSet",
                "wafv2:DeleteIPSet",
                "wafv2:GetIPSet",
                "wafv2:AssociateWebACL",
                "wafv2:DisassociateWebACL",
                "wafv2:PutLoggingConfiguration",
                "wafv2:DeleteLoggingConfiguration",
```

```
                "wafv2:ListWebACLs",
                "wafv2:ListIPSets",
                "wafv2:ListTagsForResource"
            ],
            "Resource": [
                "arn:aws:wafv2:*:*:regional/webacl/*",
                "arn:aws:wafv2:*:*:regional/ipset/*",
                "arn:aws:wafv2:*:*:global/webacl/*",
                "arn:aws:wafv2:*:*:global/ipset/*"
            ]
        }
```

- Lambda 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:InvokeFunction",
                "lambda:UpdateFunctionCode",
                "lambda:UpdateFunctionConfiguration",
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
            "Resource": "arn:aws:lambda:*:*:function:*"
        }
```

- Firehose 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "firehose:CreateDeliveryStream",
                "firehose:DeleteDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "firehose:StartDeliveryStreamEncryption",
                "firehose:StopDeliveryStreamEncryption",
                "firehose:UpdateDestination"
```

```
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*"
        }
```

- S3 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucketPolicy",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutLifecycleConfiguration",
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:ListMultipartUploadParts",
                "s3:PutBucketLogging",
                "s3:GetBucketLogging"
            ],
            "Resource": "arn:aws:s3:::*"
        }
```

- Athena 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "athena:CreateWorkGroup",
                "athena:DeleteWorkGroup",
```

```
                "athena:GetWorkGroup",
                "athena:UpdateWorkGroup",
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StopQueryExecution"
            ],
            "Resource": "arn:aws:athena:*:*:workgroup/WAF*"
        }
```

- Glue 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*",
                "arn:aws:glue:*:*:table/*/*",
                "arn:aws:glue:*:*:userDefinedFunction/*"
            ]
        }
```

- CloudWatch Logs 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
```

```
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DeleteLogGroup",
                "logs:DeleteLogStream",
                "logs:PutRetentionPolicy",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/lambda/*",
                "arn:aws:logs:*:*:log-group:*",
                "arn:aws:logs:*:*:log-group:/aws/kinesisfirehose/*"
            ]
        }
```

- CloudWatch 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DeleteDashboards",
                "cloudwatch:GetDashboard",
                "cloudwatch:ListDashboards",
                "cloudwatch:PutDashboard",
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*"
        }
```

- SNS 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:Subscribe",
                "sns:Unsubscribe",
                "sns:SetTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*"
```

```
        }
```

- DynamoDB 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:CreateTable",
                "dynamodb:DeleteTable",
                "dynamodb:DescribeTable",
                "dynamodb:PutItem",
                "dynamodb:GetItem",
                "dynamodb:UpdateItem",
                "dynamodb:DeleteItem"
            ],
            "Resource": "arn:aws:dynamodb:*:*:table/*"
        }
```

- CloudFormation 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:UpdateStack",
                "cloudformation:ListStacks"
            ],
            "Resource": "arn:aws:cloudformation:*:*:stack/*/*"
        }
```

- Service Catalog 앱 레지스트리 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:CreateApplication",
                "servicecatalog:DeleteApplication",
```

```
                "servicecatalog:GetApplication",
                "servicecatalog:TagResource",
                "servicecatalog:CreateAttributeGroup",
                "servicecatalog:DeleteAttributeGroup",
                "servicecatalog:GetAttributeGroup",
                "servicecatalog:AssociateAttributeGroup",
                "servicecatalog:DisassociateAttributeGroup",
                "servicecatalog:AssociateResource",
                "servicecatalog:DisassociateResource"
            ],
            "Resource": "arn:aws:servicecatalog:*:*:*"
        }
```

- X-Ray 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "xray:PutTraceSegments",
                "xray:PutTelemetryRecords"
            ],
            "Resource": "*"
        }
```

- IAM 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRoles",
                "iam:PassRole",
                "iam:PutRolePolicy"
```

```
            ],
            "Resource": "arn:aws:iam::*:role/*"
        }
```

- EventBridge 권한

```
        {
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:RemoveTargets",
                "events:DescribeRule",
                "events:EnableRule",
                "events:ListRules",
                "events:PutRule",
                "events:DeleteRule",
                "events:ListEventSources",
                "events:DescribeEventSource",
                "events:ActivateEventSource",
                "events:DeactivateEventSource"
            ],
            "Resource": "arn:aws:events:*:*:rule/*"
        }
```

솔루션 배포

이 솔루션은 AWS CloudFormation 템플릿 및 스택을 사용하여 배포를 자동화합니다. CloudFormation 템플릿은이 솔루션에 포함된 AWS 리소스와 해당 속성을 지정합니다. CloudFormation 스택은 템플릿에 설명된 리소스를 프로비저닝합니다.

배포 프로세스 개요

CloudFormation 템플릿을 시작하기 전에이 가이드에서 설명하는 아키텍처 및 구성 고려 사항을 검토하세요. 이 섹션의 step-by-step 지침에 따라 솔루션을 구성하고 계정에 배포합니다.

배포 시간: 약 15분.

> **Note**
>
> 이전에이 솔루션을 배포한 경우 업데이트 지침은 솔루션 업데이트를 참조하세요.

사전 조건

- CloudFront 배포 구성
- ALB 구성

1단계. 스택 시작

- AWS 계정으로 CloudFormation 템플릿을 시작합니다.
- 필요한 파라미터의 값을 입력합니다. 스택 이름 및 애플리케이션 액세스 로그 버킷 이름.
- 다른 템플릿 파라미터를 검토하고 필요한 경우 조정합니다.

2단계. 웹 ACL을 웹 애플리케이션과 연결

- CloudFront 웹 배포(들) 또는 ALB(들)를이 솔루션이 생성하는 웹 ACL과 연결합니다. 원하는 만큼 배포 또는 로드 밸런서를 연결할 수 있습니다.

3단계. 웹 액세스 로깅 구성

- CloudFront 웹 배포(들) 또는 ALB(들)에 대한 웹 액세스 로깅을 활성화하고 로그 파일을 적절한 Amazon S3 버킷으로 전송합니다. 사용자 정의 접두사와 일치하는 폴더에 로그를 저장합니다. 사용자 정의 접두사를 사용하지 않는 경우 로그를 AWSLogs에 저장합니다(기본 로그 접두사 AWSLogs/). 1단계의 애플리케이션 액세스 로그 버킷 접두사 파라미터를 참조하세요. 자세한 내용을 보려면 스택을 시작합니다.

AWS CloudFormation 템플릿

이 솔루션에는 기본 AWS CloudFormation 템플릿 1개와 중첩 템플릿 2개가 포함되어 있습니다. 솔루션을 배포하기 전에 CloudFormation 템플릿을 다운로드할 수 있습니다.

기본 스택

View template

aws-waf-security-automations.template -이 템플릿을 진입점으로 사용하여 계정에서 솔루션을 시작합니다. 기본 구성은 사전 구성된 규칙이 있는 AWS WAF 웹 ACL을 배포합니다. 필요에 따라 템플릿을 사용자 지정할 수 있습니다.

WebACL 스택

View template

aws-waf-security-automations-webacl.template -이 중첩 템플릿은 웹 ACL, IP, 세트 및 기타 관련 리소스를 포함한 AWS WAF 리소스를 프로비저닝합니다.

Firehose Athena 스택

View template

aws-waf-security-automations-firehose-athena.template -이 중첩 템플릿은 AWS Glue, Athena 및 Firehose와 관련된 리소스를 프로비저닝합니다. 스캐너 및 프로브 Athena 로그 파서 또는 HTTP Flood Lambda 또는 Athena 로그 파서를 선택하면 생성됩니다.

> **Note**
>
> AWS CloudFormation 리소스는 AWS Cloud Development Kit(AWS CDK) 구문에서 생성됩니다.

이 AWS CloudFormation 템플릿은 AWS Cloud에 AWS WAF용 보안 자동화 솔루션을 배포합니다.

사전 조건

이 솔루션은 CloudFront 또는 ALB로 배포된 웹 애플리케이션에서 작동하도록 설계되었습니다. 이러한 리소스 중 하나가 아직 구성되지 않은 경우이 솔루션을 시작하기 전에 해당 작업을 완료합니다.

CloudFront 배포 구성

다음 단계를 완료하여 웹 애플리케이션의 정적 및 동적 콘텐츠에 대한 CloudFront 배포를 구성합니다. 자세한 지침은 Amazon CloudFront 개발자 안내서를 참조하세요.

1. CloudFront 웹 애플리케이션 배포를 생성합니다. 배포 생성을 참조하세요.
2. 정적 및 동적 오리진을 구성합니다. CloudFront 배포에서 다양한 오리진 사용을 참조하세요.
3. 배포의 동작을 지정합니다. 배포를 생성하거나 업데이트할 때 지정하는 값을 참조하세요.

> **Note**
>
> 엔드포인트`CloudFront`로를 선택하는 경우 미국 동부(버지니아 북부) 리전에서 WAFV2 리소스를 생성해야 합니다.

ALB 구성

수신 트래픽을 웹 애플리케이션에 배포하도록 ALB를 구성하려면 Application Load Balancer 사용 설명서의 Application Load Balancer 생성을 참조하세요.

1단계. 스택 시작

이 자동화된 AWS CloudFormation 템플릿은 AWS 클라우드에 솔루션을 배포합니다.

1. AWS Management Console에 로그인하고 솔루션 시작을 선택하여 `waf-automation-on-aws.template` CloudFormation 템플릿을 시작합니다.

2. 이 템플릿은 기본적으로 미국 동부(버지니아 북부) 리전에서 시작됩니다. 다른 AWS 리전에서이 솔루션을 시작하려면 콘솔 탐색 모음에서 리전 선택기를 사용합니다. 엔드포인트`CloudFront`로를 선택하는 경우 미국 동부(버지니아 북부)(`us-east-1`) 리전에 솔루션을 배포해야 합니다.

> **Note**
>
> 정의한 입력 파라미터 값에 따라이 솔루션에는 다양한 리소스가 필요합니다. 이러한 리소스는 현재 특정 AWS 리전에서만 사용할 수 있습니다. 따라서 이러한 서비스를 사용할 수 있는 AWS 리전에서이 솔루션을 시작해야 합니다. 자세한 내용은 지원되는 AWS 리전을 참조하세요.

3. 템플릿 지정 페이지에서 올바른 템플릿을 선택했는지 확인하고 다음을 선택합니다.
4. 스택 세부 정보 지정 페이지의 스택 이름 필드에서 AWS WAF 구성에 이름을 할당합니다. 템플릿이 생성하는 웹 ACL의 이름이기도 합니다.
5. 파라미터에서 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 특정 기능을 옵트아웃하려면 no 해당하는 경우 none 또는를 선택합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

파라미터	Default	설명
스택 이름	`[.red]#<입력 필요>`	스택 이름에는 공백을 사용할 수 없습니다. 이 이름은 AWS 계정 내에서 고유해야 하며 템플릿이 생성하는 웹 ACL의 이름입니다.
리소스 유형		
Endpoint	`CloudFront`	사용 중인 리소스 유형을 선택합니다. 참고: 엔드포인트`CloudFront` 로를 선택하는 경우 솔루션을 시작하여 미국 동부(버지니아 북부) 리전()

파라미터	Default	설명
		에서 WAF 리소스를 생성해야 합니다.us-east-1
AWS 관리형 IP 평판 규칙 그룹		
Amazon IP 평판 활성화 관리형 규칙 그룹 보호 나열	no	Amazon IP 신뢰도 목록 관리형 규칙 그룹을 웹 ACL에 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 Amazon 내부 위협 인텔리전스를 기반으로 합니다. 이는 일반적으로 봇 또는 기타 위협과 관련된 IP 주소를 차단하려는 경우에 유용합니다. 이러한 IP 주소를 차단하면 봇을 완화하고 악성 액터가 취약한 애플리케이션을 발견하는 위험을 줄일 수 있습니다. 필수 WCU는 25입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
익명 IP 목록 관리형 규칙 그룹 보호 활성화	no	웹 ACL에 익명 IP 목록 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 최종 사용자 자격 증명의 난독화를 허용하는 서비스의 요청을 차단합니다. 여기에는 VPN, 프록시, Tor 노드 및 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. 필수 WCU는 50입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.
AWS 관리형 기준 규칙 그룹		

파라미터	Default	설명
코어 규칙 세트 관리형 규칙 그룹 보호 활성화	no	코어 규칙 세트 관리형 규칙 그룹을 웹 ACL에 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 고위험 및 일반적으로 발생하는 취약성 중 일부를 포함하여 광범위한 취약성의 악용으로부터 보호합니다. AWS WAF 사용 사례에 이 규칙 그룹을 사용하는 것이 좋습니다. 필요한 WCU는 700입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
관리자 보호 관리형 규칙 그룹 보호 활성화	no	웹 ACL에 관리자 보호 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 노출된 관리 페이지에 대한 외부 액세스를 차단합니다. 서드 파티 소프트웨어를 실행 중이거나, 악성 액터가 애플리케이션에 대한 관리 액세스 권한을 얻게 되는 위험을 줄이려면 이 방법이 유용할 수 있습니다. 필요한 WCU는 100입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
알려진 잘못된 입력 활성화 관리형 규칙 그룹 보호	no	웹 ACL에 알려진 잘못된 입력 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 노출된 관리 페이지에 대한 외부 액세스를 차단합니다. 서드 파티 소프트웨어를 실행 중이거나, 악성 액터가 애플리케이션에 대한 관리 액세스 권한을 얻게 되는 위험을 줄이려면 이 방법이 유용할 수 있습니다. 필요한 WCU는 100입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.
AWS 관리형 사용 사례별 규칙 그룹		

파라미터	Default	설명
SQL 데이터베이스 관리형 규칙 그룹 보호 활성화	no	웹 ACL에 SQL 데이터베이스 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 SQL 삽입 공격과 같은 SQL 데이터베이스 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 승인되지 않은 쿼리가 원격으로 삽입되는 것을 방지할 수 있습니다. 애플리케이션이 SQL 데이터베이스와 접속하는 경우 이 규칙 그룹을 사용할 수 있는지 평가합니다. AWS 관리형 SQL 규칙 그룹이 이미 활성화된 경우 SQL 삽입 사용자 지정 규칙을 사용하는 것은 선택 사항입니다. 필요한 WCU는 200입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
Linux 운영 체제 관리형 규칙 그룹 보호 활성화	no	Linux 운영 체제 관리형 규칙 그룹을 웹 ACL에 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 Linux 관련 로컬 파일 포함(LFI) 공격을 포함하여 Linux 관련 취약성 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 파일 내용을 노출하거나 공격자가 액세스 권한을 가져서는 안 되는 코드를 실행하는 공격을 방지할 수 있습니다. 애플리케이션의 일부가 Linux에서 실행되는 경우이 규칙 그룹을 평가합니다. POSIX 운영 체제 규칙 그룹과 함께이 규칙 그룹을 사용해야 합니다. 필요한 WCU는 200입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
POSIX 운영 체제 관리형 규칙 그룹 보호 활성화	no	웹 ACL에 코어 규칙 세트 관리형 규칙 그룹 보호를 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 LFI 공격을 포함하여 POSIX 및 POSIX 유사 운영 체제와 관련된 취약성 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 파일 내용을 노출하거나 공격자가 액세스 권한을 가져서는 안 되는 코드를 실행하는 공격을 방지할 수 있습니다. 애플리케이션의 일부가 POSIX 또는 POSIX와 유사한 운영 체제에서 실행되는 경우이 규칙 그룹을 평가합니다. 필요한 WCU는 100입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
Windows 운영 체제 관리형 규칙 그룹 보호 활성화	no	웹 ACL에 Windows 운영 체제 관리형 규칙 그룹을 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 PowerShell 명령의 원격 실행과 같이 Windows 관련 취약성 악용과 관련된 요청 패턴을 차단합니다. 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. 필요한 WCU는 200입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
PHP 애플리케이션 관리형 규칙 그룹 보호 활성화	no	PHP 애플리케이션 관리형 규칙 그룹을 웹 ACL에 추가하도록 설계된 구성 요소를 켜yes려면 선택합니다. 이 규칙 그룹은 안전하지 않은 PHP 함수 주입을 포함하여 PHP 프로그래밍 언어 사용과 관련된 취약성 악용과 관련된 요청 패턴을 차단합니다. 이렇게 하면 공격자가 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. 필요한 WCU는 100입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.

파라미터	Default	설명
WordPress 애플리케이션 관리형 규칙 그룹 보호 활성화	no	WordPress 애플리케이션 관리형 규칙 그룹을 웹 ACL에 추가하도록 설계된 구성 요소를 켜yes도록 선택합니다. 이 규칙 그룹은 WordPress 사이트별 취약성 악용과 관련된 요청 패턴을 차단합니다. WordPress를 실행하는 경우 이 규칙 그룹을 평가합니다. 이 규칙 그룹은 SQL 데이터베이스 및 PHP 애플리케이션 규칙 그룹과 함께 사용해야 합니다. 필요한 WCU는 100입니다. 용량 제한을 초과하여 웹 ACL 스택 배포에 실패하지 않도록 계정에 충분한 WCU 용량이 있어야 합니다. 자세한 내용은 AWS 관리형 규칙 규칙 그룹 목록을 참조하세요.
사용자 지정 규칙 - 스캐너 및 프로브		
스캐너 및 프로브 보호 활성화	`yes - AWS Lambda log parser`	스캐너와 프로브를 차단하는 데 사용되는 구성 요소를 선택합니다. 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.

파라미터	Default	설명
애플리케이션 액세스 로그 버킷 이름	[.red]<requires input>	스캐너 및 프로브 보호 활성화 파라미터에 yes 대해를 선택한 경우 CloudFront 배포(들) 또는 ALB(들)에 대한 액세스 로그를 저장할 Amazon S3 버킷(신규 또는 기존)의 이름을 입력합니다. 기존 Amazon S3 버킷을 사용하는 경우 CloudFormation 템플릿을 배포하는 동일한 AWS 리전에 있어야 합니다. 솔루션 배포마다 다른 버킷을 사용해야 합니다. 이 보호를 비활성화하려면이 파라미터를 무시합니다. 참고: CloudFront 웹 배포(들) 또는 ALB(들)에 대한 웹 액세스 로깅을 활성화하여이 Amazon S3 버킷으로 로그 파일을 전송합니다. 스택에 정의된 것과 동일한 접두사(기본 접두사)에 로그를 저장합니다AWSLogs/. 자세한 내용은 애플리케이션 액세스 로그 버킷 접두사 파라미터를 참조하세요.

파라미터	Default	설명
애플리케이션 액세스 로그 버킷 접두사	AWSLogs/	스캐너 및 프로브 보호 활성화 파라미터에 yes 대해를 선택한 경우 위의 애플리케이션 액세스 로그 버킷에 대한 선택적 사용자 정의 접두사를 입력할 수 있습니다. 엔드포인트 파라미터CloudFront 로를 선택한 경우와 같은 접두사를 입력할 수 있습니다yourprefix/ . 엔드포인트 파라미터ALB로를 선택한 경우와 같은 접두사AWSLogs/에를 추가해야 합니다yourprefix/AWSLogs/ . 사용자 정의 접두사가 없는 경우 AWSLogs/ (기본값)을 사용합니다. 이 보호를 비활성화하려면이 파라미터를 무시합니다.

파라미터	Default	설명
버킷 액세스 로깅이 켜져 있습니까?	no	Application Access Log Bucket Name 파라미터에 기존 Amazon S3 버킷 이름을 입력했고 버킷에 대한 서버 액세스 로깅이 이미 켜져 yes 있는지 선택합니다. 를 선택하면 솔루션이 버킷no에 대한 서버 액세스 로깅을 켭니다. 스캐너 및 프로브 보호 활성화 파라미터에 no 대해를 선택한 경우이 파라미터를 무시합니다.
오류 임계값	50	스캐너 및 프로브 보호 활성화 파라미터에 yes 대해를 선택한 경우 IP 주소당 분당 허용되는 최대 잘못된 요청을 입력합니다. 스캐너 및 프로브 보호 활성화 파라미터에 no 대해를 선택한 경우이 파라미터를 무시합니다.

파라미터	Default	설명
원래 S3 위치에 데이터 유지	no	스캐너 및 프로브 보호 활성화 파라미터에 `yes - Amazon Athena log parser` 대해를 선택한 경우 솔루션은 애플리케이션 액세스 로그 파일 및 Athena 쿼리에 파티셔닝을 적용합니다. 기본적으로 솔루션은 로그 파일을 원래 위치에서 Amazon S3의 분할된 폴더 구조로 이동합니다. 로그 사본을 원래 위치에 보관할yes지 여부도 선택합니다. 그러면 로그 스토리지가 복제됩니다. 스캐너 및 프로브 보호 활성화 파라미터에 `yes - Amazon Athena log parser` 대해를 선택하지 않은 경우이 파라미터를 무시합니다.
사용자 지정 규칙 - HTTP 서비스 장애		
HTTP 서비스 장애 방지 활성화	`yes - AWS WAF rate-based rule`	HTTP flood 공격을 차단하는 데 사용되는 구성 요소를 선택합니다. 완화 옵션과 관련된 장단점에 대한 자세한 내용은 로그 구문 분석기 옵션을 참조하세요.

파라미터	Default	설명
기본 요청 임계값	`100`	HTTP 서비스 장애 방지 활성화 파라미터에 `yes` 대해를 선택한 경우 IP 주소당 5분당 허용되는 최대 요청을 입력합니다. HTTP 서비스 장애 방지 활성화 파라미터에 `yes - AWS WAF rate-based rule` 대해를 선택한 경우 허용되는 최소 값은 입니다`10`. HTTP 서비스 장애 방지 활성화 파라미터에 `yes - Amazon Athena log parser` 대해 `yes - AWS Lambda log parser` 또는 를 선택한 경우 모든 값이 될 수 있습니다. 이 보호를 비활성화하려면이 파라미터를 무시합니다.

파라미터	Default	설명
국가별 요청 임계값	<선택 사항 입력>	HTTP 서비스 장애 방지 활성화 파라미터yes - Amazon Athena log parser로를 선택한 경우이 JSON 형식에 따라 국가별 임계값을 입력할 수 있습니다{"TR":50, "ER":150} . 솔루션은 지정된 국가에서 시작된 요청에 대해 이러한 임계값을 사용합니다. 솔루션은 나머지 요청에 대해 기본 요청 임계값 파라미터를 사용합니다. 참고:이 파라미터를 정의하면 국가가 IP 및 HTTP Flood Athena 쿼리의 요청별 그룹화 파라미터를 사용하여 선택할 수 있는 기타 선택적 그룹화 필드와 함께 Athena 쿼리 그룹에 자동으로 포함됩니다. + 이 보호를 비활성화하기로 선택한 경우이 파라미터를 무시합니다.

파라미터	Default	설명
HTTP Flood Athena 쿼리의 요청별 그룹화	None	HTTP 서비스 장애 방지 활성화 파라미터에 yes - Amazon Athena log parser 대해를 선택한 경우 그룹화 기준 필드를 선택하여 IP당 요청을 계산하고 선택한 그룹화 기준 필드를 선택할 수 있습니다. 예를 들어 URI를 선택하면 솔루션은 IP 및 URI당 요청을 계산합니다. 이 보호를 비활성화하기로 선택한 경우이 파라미터를 무시합니다.
WAF 블록 기간	240	스캐너 및 프로브 보호 활성화 또는 HTTP 서비스 장애 방지 활성화 파라미터yes - Amazon Athena log parser에 대해 yes - AWS Lambda log parser 또는 를 선택한 경우 기간(분)을 입력하여 해당 IP 주소를 차단합니다. 로그 구문 분석을 비활성화하려면이 파라미터를 무시합니다.

파라미터	Default	설명
Athena 쿼리 실행 시간 일정(분)	5	스캐너 및 프로브 보호 활성화 또는 HTTP 서비스 장애 방지 활성화 파라미터에 `yes - Amazon Athena log parser` 대해를 선택한 경우 Athena 쿼리가 실행되는 시간 간격(분)을 입력할 수 있습니다. 기본적으로 Athena 쿼리는 5분마다 실행됩니다. 이러한 보호를 비활성화하기로 선택한 경우이 파라미터를 무시합니다.
규칙 키	`IP`	HTTP Flood 보호 활성화 파라미터에 `yes - AWS WAF rate-based rule` 대해를 선택한 경우 집계 키의 다양한 다른 조합을 사용하도록이 규칙을 구성합니다. 사용 가능한 옵션: IP(기본값) IP+사용자 지정 헤더(이 옵션을 선택한 경우 `Rule Keys Custom Header` 필수) IP+URI IP+HTTP 메서드 자세한 내용은 WAF 규칙 속도 기반 집계 옵션을 참조하세요.

파라미터	Default	설명
규칙 키 사용자 지정 헤더	no	규칙 키 파라미터IP+Custom Header로를 선택한 경우 요청 집계에 사용할 사용자 지정 헤더의 이름을 입력합니다. 자세한 내용은 WAF 규칙 문 유형 속도 기반 집계 옵션을 참조하세요.
기간 임계값(분)	5	HTTP 플러드 보호를 위한 시간 범위 임계값입니다. 속도 기반 규칙과 Lambda 로그 구문 분석기 모두에 적용됩니다. 사용 가능한 옵션: [1, 2, 5, 10]. 에 yes - AWS WAF rate-based rule 대해 선택한 경우 HTTP 서비스 장애 방지 활성화 파라미터가 평가 기간에 사용됩니다. 자세한 내용은 WAF 웹 ACL 속도 기반 문을 참조하세요. 에 yes - AWS Lambda log parser 대해 선택한 경우 HTTP Flood 보호 활성화 파라미터는 차단 기간 외에도 평가 기간에 사용됩니다.
사용자 지정 규칙 - 잘못된 봇		
잘못된 봇 보호 활성화	yes	잘못된 봇과 콘텐츠 스크레이퍼를 차단하도록 설계된 구성 요소를 켜yes도록 선택합니다.

파라미터	Default	설명
계정의 CloudWatch 로그에 대한 쓰기 액세스 권한이 있는 IAM 역할의 ARN	<선택 사항 입력>	계정의 CloudWatch 로그에 대한 쓰기 액세스 권한이 있는 IAM 역할의 선택적 ARN을 제공합니다. 예를 들어 ARN: `arn:aws:iam::account_id:role/myrolename` 입니다. 이 파라미터를 비워 두면(기본값) 솔루션이 새 역할을 생성합니다.
사용자 지정 규칙 - 타사 IP 평판 목록		
평판 목록 보호 활성화	`yes`	타사 평판 목록에 있는 IP 주소의 요청을 차단`yes`하도록 선택합니다(지원되는 목록에는 Spamhaus, 새로운 위협 및 Tor 출구 노드가 포함됨).
레거시 사용자 지정 규칙		

파라미터	Default	설명
SQL 주입 보호 활성화	yes	일반적인 SQL 주입 공격을 차단하도록 설계된 구성 요소를 켜yes도록 선택합니다. AWS 관리형 코어 규칙 세트 또는 AWS 관리형 SQL 데이터베이스 규칙 그룹을 사용하지 않는 경우 활성화하는 것이 좋습니다. AWS WAF가 8KB(yes8yes - MATCH,192바이트yes - NO_MATCH)를 초과하는 크기 초과 요청을 처리하도록 하려는 옵션((계속), 또는) 중 하나를 선택할 수 있습니다. 기본적으로는 규칙 yes 검사 기준에 따라 크기 제한 내에 있는 요청 구성 요소 콘텐츠를 검사합니다. 자세한 내용은 과대 웹 요청 구성 요소 처리를 참조하세요. 이 기능을 비활성화no하려면를 선택합니다. 참고: CloudFormation 스택은 선택한 과대 처리 옵션을 기본 SQL 주입 보호 규칙에 추가하고 AWS 계정에 배포합니다. CloudFormation 외부에서 규칙을 사용자 지정한 경우 스택 업데이트 후 변경 사항을 덮어씁니다.

파라미터	Default	설명
SQL 주입 방지를 위한 민감도 수준	LOW	AWS WAF가 SQL 주입 공격을 검사하는 데 사용할 민감도 수준을 선택합니다. HIGH는 더 많은 공격을 탐지하지만 더 많은 거짓 긍정을 생성할 수 있습니다. LOW는 SQL 명령어 삽입 공격에 대한 다른 보호 기능이 이미 있거나 오탐에 대한 허용치가 낮은 리소스에 대체로 더 적합합니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 SQL 주입 규칙 문 및 SensitivityLevel 속성에 대한 AWS WAF 추가 민감도 수준을 참조하세요. SensitivityLevel AWS CloudFormation SQL 주입 보호를 비활성화하도록 선택한 경우이 파라미터를 무시합니다. 참고: CloudFormation 스택은 선택한 민감도 수준을 기본 SQL 주입 방지 규칙에 추가하고 AWS 계정에 배포합니다. CloudFormation 외부에서 규칙을 사용자 지정한 경우 스택 업데이트 후 변경 사항을 덮어씁니다.

파라미터	Default	설명
교차 사이트 스크립팅 보호 활성화	yes	일반적인 XSS 공격을 차단하도록 설계된 구성 요소를 켜yes도록 선택합니다. AWS 관리형 코어 규칙 세트를 사용하지 않는 경우 활성화하는 것이 좋습니다. AWS WAF가 8KB(yes8yes - MATCH,192 바이트yes - NO_MATCH)를 초과하는 크기 초과 요청을 처리하도록 하려는 옵션((계속), 또는) 중 하나를 선택할 수도 있습니다. 기본적으로는 규칙 검사 기준에 따라 크기 제한 내에 있는 요청 구성 요소 콘텐츠를 검사하는 Continue 옵션을 yes 사용합니다. 자세한 내용은 요청 구성 요소에 대한 과대 처리를 참조하세요. 이 기능을 비활성화no하려면를 선택합니다. 참고: CloudFormation 스택은 선택한 과대 처리 옵션을 기본 교차 사이트 스크립팅 규칙에 추가하고 AWS 계정에 배포합니다. CloudFormation 외부에서 규칙을 사용자 지정한 경우 스택 업데이트 후 변경 사항을 덮어씁니다.
허용 및 거부 IP 보존 설정		

파라미터	Default	설명
허용된 IP 세트의 보존 기간(분)	-1	허용된 IP 세트에 대해 IP 보존을 활성화하려면 보존 기간(15분)으로 숫자(이상)를 입력합니다. 보존 기간에 도달한 IP 주소는 만료되며 솔루션은 IP 세트에서 IP 주소를 제거합니다. 솔루션은 최소 15분의 보존 기간을 지원합니다. 0와 사이의 숫자를 입력하면 15솔루션은 이를 로 취급합니다15. IP 보존을 끄려면 -1 (기본값)으로 둡니다.
거부된 IP 세트의 보존 기간(분)	-1	거부된 IP 세트에 대해 IP 보존을 활성화하려면 보존 기간(15분)으로 숫자(이상)를 입력합니다. 보존 기간에 도달한 IP 주소는 만료되며 솔루션은 IP 세트에서 IP 주소를 제거합니다. 솔루션은 최소 15분의 보존 기간을 지원합니다. 0와 사이의 숫자를 입력하면 15솔루션은 이를 로 취급합니다15. IP 보존을 끄려면 -1 (기본값)으로 둡니다.

파라미터	Default	설명
허용 또는 거부 IP 세트 만료 시 알림을 수신하기 위한 이메일	<선택 사항 입력>	IP 보존 기간 파라미터(이전 파라미터 2개 참조)를 활성화하고 IP 주소가 만료될 때 이메일 알림을 받으려면 유효한 이메일 주소를 입력합니다. IP 보존을 활성화하지 않았거나 이메일 알림을 끄려면 비워 둡니다(기본값).
고급 설정		
로그 그룹의 보존 기간(일)	365	CloudWatch 로그 그룹에 대한 보존을 활성화하려면 보존 기간(1일)으로 숫자(이상)를 입력합니다. 1일(1)에서 10년() 사이의 보존 기간을 선택할 수 있습니다3650. 기본적으로 로그는 1년 후에 만료됩니다. 로그를 무기한 유지-1하려면 로 설정합니다.

6. 다음을 선택합니다.
7. 스택 옵션 구성 페이지에서 스택의 리소스에 대한 태그(키-값 페어)를 지정하고 추가 옵션을 설정할 수 있습니다. 다음을 선택합니다.
8. 검토 및 생성 페이지에서 설정을 검토하고 확인합니다. 템플릿이 IAM 리소스와 필요한 추가 기능을 생성할 것임을 확인하는 상자를 선택합니다.
9. 제출을 선택하여 스택을 배포합니다.

   AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 확인합니다. 약 15분 후에 CREATE_COMPLETE 상태를 받게 됩니다.

> **Note**
>
> `Log Parser` 및 `IP Lists Parser` AWS Lambda 함수 외에도이 솔루션에는 초기 구성 중에 또는 리소스가 업데이트되거나 삭제될 때만 실행되는 `helper` 및 `custom-resource` Lambda 함수가 포함되어 있습니다.
> 이 솔루션을 사용하면 AWS Lambda 콘솔에 모든 함수가 표시되지만 세 가지 기본 솔루션 함수만 정기적으로 활성화됩니다. 다른 두 함수는 삭제하지 마세요. 연결된 리소스를 관리하는 데 필요합니다.

스택 리소스에 대한 세부 정보를 보려면 출력 탭을 선택합니다. 여기에는 BadBotHoneypotEndpoint 값이 포함됩니다. 웹 애플리케이션의 Honeypot 링크 임베드에 사용되므로이 값을 기억하세요.

2단계. 웹 ACL을 웹 애플리케이션과 연결

CloudFront 배포(들) 또는 ALB(들)를 업데이트하여 1단계에서 생성한 리소스를 사용하여 AWS WAF 및 로깅을 활성화합니다. 스택 시작을 참조하세요.

1. AWS WAF 콘솔에 로그인합니다.
2. 사용할 웹 ACL을 선택합니다.
3. Associated AWS resources(연결된 AWS 리소스) 탭에서 Add AWS resources(AWS 리소스 추가)를 선택합니다.
4. 리소스 유형에서 CloudFront 배포 또는 ALB를 선택합니다.
5. 목록에서 리소스를 선택한 다음 추가를 선택하여 변경 사항을 저장합니다.

3단계. 웹 액세스 로깅 구성

이 데이터를 Log Parser Lambda 함수에 사용할 수 있도록 적절한 Amazon S3 버킷으로 웹 액세스 로그를 보내도록 CloudFront 또는 ALB를 구성합니다.

CloudFront 배포의 웹 액세스 로그 저장

1. Amazon CloudFront 콘솔에 로그인합니다.
2. 웹 애플리케이션의 배포를 선택하고 배포 설정을 선택합니다.
3. General 탭에서 Edit를 선택합니다.

4. AWS WAF 웹 ACL에서 생성된 웹 ACL 솔루션(스택 이름 파라미터)을 선택합니다.
5. [Logging]에서 [On]을 선택합니다.
6. 로그용 버킷에서 웹 액세스 로그를 저장하는 데 사용할 S3 버킷을 선택합니다. 이는 기본 스택에서 사용되고 CloudFront가 로그를 쓸 수 있는 권한이 있는 신규 또는 기존 S3 버킷일 수 있습니다. 드롭다운 목록에는 현재 AWS 계정과 연결된 버킷이 나열됩니다. 자세한 내용은 Amazon CloudFront 개발자 안내서의 기본 CloudFront 배포 시작하기를 참조하세요. Amazon CloudFront
7. 로그 접두사를 솔루션 배포에 사용되는 접두사로 설정합니다. 기본 스택, 파라미터 탭, AppAccessLogBucketPrefixParam(기본값)에서 접두사를 찾을 수 있습니다`AWSLogs/`.
8. [Yes, edit]를 선택하여 변경 사항을 저장합니다.

자세한 내용은 Amazon CloudFront 개발자 안내서의 표준 로그(액세스 로그) 구성 및 사용을 참조하세요.

Application Load Balancer의 웹 액세스 로그 저장

1. Amazon Elastic Compute Cloud(Amazon EC2) 콘솔에 로그인합니다.
2. 탐색 창에서 로드 밸런서를 선택합니다.
3. 웹 애플리케이션의 ALB를 선택합니다.
4. 설명 탭에서 속성 편집을 선택합니다.
5. [Enable access logs]를 선택합니다.
6. S3 위치에 웹 액세스 로그를 저장하는 데 사용할 S3 버킷의 이름을 입력합니다. 기본 스택에서 사용되고 Application Load Balancer가 로그를 작성할 수 있는 권한이 있는 신규 또는 기존 S3 버킷일 수 있습니다.
7. 로그 접두사를 솔루션 배포에 사용되는 접두사로 설정합니다. 기본 스택, 파라미터 탭, AppAccessLogBucketPrefixParam(기본값)에서 접두사를 찾을 수 있습니다`AWSLogs/`.
8. 저장을 선택합니다.

자세한 내용은 Elastic Load Balancing 사용 설명서의 Application Load Balancer에 대한 액세스 로그를 참조하세요.

솔루션 업데이트

이전에 솔루션을 배포한 경우 다음 절차에 따라 솔루션의 CloudFormation 스택을 업데이트하여 솔루션 프레임워크의 최신 버전을 가져옵니다. 스택을 업데이트하기 전에 업데이트 고려 사항을 주의 깊게 읽어보세요.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 왼쪽 탐색 메뉴에서 스택을 선택합니다.
3. 기존 `aws-waf-security-automations` CloudFormation 스택을 선택합니다.
4. 업데이트를 선택합니다.
5. 현재 템플릿 교체를 선택합니다.
6. 템플릿 지정에서 다음을 수행합니다.
   a. Amazon S3 URL을 선택합니다.
   b. `aws-waf-security-automations.template` AWS CloudFormation의 링크를 복사합니다.
   c. Amazon S3 URL 상자에 링크를 붙여넣습니다.
   d. Amazon S3 URL 텍스트 상자에 올바른 템플릿 URL이 표시되는지 확인합니다.
   e. 다음을 선택합니다.
   f. 다음을 다시 선택합니다.
7. 파라미터에서 템플릿의 파라미터를 검토하고 필요에 따라 수정합니다. 1단계. 스택 시작에서 파라미터에 대한 세부 정보를 참조할 수 있습니다.
8. 다음을 선택합니다.
9. Configure stack options(스택 옵션 구성) 페이지에서 Next(다음)를 선택합니다.
10. 검토 페이지에서 설정을 검토하고 확인합니다.
11. 템플릿이 IAM 리소스를 생성할 수 있음을 확인하는 상자를 선택합니다.
12. 변경 세트 보기를 선택하고 변경 사항을 확인합니다.
13. 스택 생성을 선택하여 스택을 배포합니다.

AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 확인할 수 있습니다. 약 15분 후에 UPDATE_COMPLETE 상태를 확인할 수 있습니다.

업데이트 고려 사항

다음 섹션에서는이 솔루션을 업데이트하기 위한 제약 조건과 고려 사항을 제공합니다.

리소스 유형 업데이트

스택을 생성한 후 엔드포인트 파라미터를 업데이트하려면 새 스택을 배포해야 합니다. 스택을 업데이트할 때 엔드포인트 파라미터를 변경하지 마십시오.

WAFV2 업그레이드

버전 3.0부터이 솔루션은 AWS WAFV2를 지원합니다. 모든 AWS WAF Classic API 호출을 AWS WAFV2 API 호출로 대체했습니다. 이렇게 하면 Node.js에 대한 종속성이 제거되고 up-to-date Python 런타임이 사용됩니다. 이 솔루션을 최신 기능 및 개선 사항과 함께 계속 사용하려면 버전 3.0 이상을 새 스택으로 배포해야 합니다.

스택 업데이트 시 사용자 지정

out-of-box 제공 솔루션은 기본 구성이 있는 AWS WAF 규칙 세트를 CloudFormation 스택이 있는 AWS 계정에 배포합니다. 솔루션에서 배포한 규칙에 사용자 지정을 적용하지 않는 것이 좋습니다. 스택 업데이트는 이러한 변경 사항을 덮어씁니다. 사용자 지정 규칙이 필요한 경우 솔루션 외부에서 별도의 규칙을 생성하는 것이 좋습니다.

잘못된 봇 보호 업그레이드

버전 4.1.0에서는 API Gateway가 포함된 액세스 핸들러 Lambda가 더 이상 사용되지 않으며 Log parser - Bad bot이 기능의 향상된 로그 기능으로 대체되었습니다. 이제 솔루션은 API Gateway를 통한 직접 요청을 사용하는 대신 로그 스트림을 재사용하여 잘못된 봇을 감지합니다.

이전 구현:

1. 필수 액세스 핸들러 Lambda 및 API Gateway.
2. 직접 요청 처리에 허니팟 엔드포인트를 사용했습니다.
3. 웹 사이트에 허니팟 엔드포인트를 포함해야 합니다.

새 구현(4.1.0 이상): 잘못된 봇 보호 로그 구문 분석기가 이제:

1. 로그를 통해 허니팟 엔드포인트에 대한 요청을 검사합니다.

2. 잘못된 봇 보호가 활성화되면 요청을 처리합니다.
3. WAF 필터 BadBotRuleFilter를 사용하여 잘못된 봇 요청을 식별합니다.
4. 로그 데이터를 분석하여 정의된 할당량을 초과하는 IP 주소를 식별합니다.
5. AWS WAF IP 세트 조건을 업데이트하여 식별된 주소를 차단합니다.

이 변경 사항은 중복 기능을 제거하고 기존 로그 처리 기능을 활용하여 아키텍처를 간소화합니다.

CDK 업그레이드

버전 v4.1.0부터이 솔루션은 CDK에서 지원됩니다. v4.1.0 미만의 버전에서 마이그레이션하는 경우. Cloudformation에서 새 템플릿을 사용하고 솔루션을 업데이트합니다. 그런 다음 cdk 배포를 사용하여 터미널을 통해 로컬에서 솔루션 업데이트를 시작할 수 있습니다(자세한 내용은 README 참조). cdk 배포를 직접 사용하려고 하면 흐름 컬렉션에 들여쓰기 부족 오류가 표시될 수 있습니다.

솔루션을 업데이트하는 또 다른 방법은 솔루션에서 제공하는 템플릿을 사용하고 AWS 콘솔의 Cloudformation 섹션으로 이동하여 솔루션 업데이트를 클릭하고 새 템플릿을 여기에 붙여넣는 것입니다.

> **Note**
>
> 버전 3.0 또는 3.1에서이 솔루션의 버전 3.2 이상으로 업그레이드하고 허용 또는 거부된 IP 세트에 IP 주소를 수동으로 삽입한 경우 해당 IP 주소가 손실될 위험이 있습니다. 이를 방지하려면 솔루션을 업그레이드하기 전에 허용 또는 거부된 IP 세트의 IP 주소를 복사합니다. 그런 다음 업그레이드를 완료한 후 필요에 따라 IP 주소를 IP 세트에 다시 추가합니다. get-ip-set 및 update-ip-set CLI 명령을 참조하세요. 이미 버전 3.2 이상을 사용하고 있는 경우이 단계를 무시하십시오.

솔루션 제거

솔루션을 제거하려면 CloudFormation 스택을 삭제합니다.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 솔루션의 상위 스택을 선택합니다. 다른 모든 솔루션 스택은 자동으로 삭제됩니다.
3. 삭제를 선택합니다.

> **Note**
>
> 솔루션을 제거하면 Amazon S3 버킷을 제외하고 솔루션에서 사용하는 모든 AWS 리소스가 삭제됩니다. AWA WAF API 할당량으로 인한 속도 초과 제한 문제로 인해 일부 IP 세트가 삭제되지 않는 경우 해당 IP 세트를 수동으로 삭제한 다음 스택을 삭제합니다.

솔루션 사용

이 섹션에서는 솔루션을 배포한 후 솔루션을 사용하는 방법에 대한 자세한 지침을 제공합니다.

허용 및 거부된 IP 세트 수정(선택 사항)

이 솔루션의 CloudFormation 스택을 배포한 후 허용 및 거부된 IP 세트를 수동으로 수정하여 필요에 따라 IP 주소를 추가하거나 제거할 수 있습니다.

1. AWS WAF 콘솔에 로그인합니다.
2. 왼쪽 탐색 창에서 IP 집합을 선택합니다.
3. 허용 목록에 IP 세트를 선택하고 신뢰할 수 있는 소스의 IP 주소를 추가합니다.
4. 거부 목록에서 IP 세트를 선택하고 차단하려는 IP 주소를 추가합니다.

웹 애플리케이션에 Honeypot 링크 임베드(선택 사항)

1단계에서 잘못된 봇 보호 활성화 파라미터yes로를 선택한 경우. 스택을 시작하면 CloudFormation 템플릿이 상호 작용이 적은 프로덕션 허니팟에 트랩 엔드포인트를 생성합니다. 이 트랩은 콘텐츠 스크레이퍼 및 잘못된 봇의 인바운드 요청을 감지하고 우회하기 위한 것입니다. 유효한 사용자는이 엔드포인트에 액세스하려고 시도하지 않습니다.

이 구성 요소는 허니팟 메커니즘 외에도 Application Load Balancer(ALB) 또는 Amazon CloudFront에 대한 직접 연결을 모니터링하여 잘못된 봇 탐지를 개선합니다. 봇이 허니팟을 우회하고 ALB 또는 CloudFront와 상호 작용하려고 하면 시스템은 요청 패턴 및 로그를 분석하여 악의적인 활동을 식별합니다. 잘못된 봇이 감지되면 IP 주소가 추출되어 AWS WAF 블록 목록에 추가되어 추가 액세스를 방지합니다. 잘못된 봇 탐지는 구조화된 로직 체인을 통해 작동하여 포괄적인 위협 범위를 보장합니다.

- HTTP Flood Protection Lambda 로그 파서 - 플러드 분석 중에 로그 항목에서 잘못된 봇 IPs를 수집합니다.
- 스캐너 및 프로브 보호 Lambda 로그 파서 - 스캐너 관련 로그 항목에서 잘못된 봇 IPs.
- HTTP Flood Protection Athena Log Parser - 쿼리 실행 전반의 파티션을 사용하여 Athena 로그에서 잘못된 봇 IPs를 추출합니다.
- 스캐너 및 프로브 보호 Athena 로그 파서 - 동일한 파티셔닝 전략을 사용하여 스캐너 관련 Athena 로그에서 잘못된 봇 IPs를 검색합니다.

- 폴백 감지 - HTTP Flood Protection과 스캐너 및 프로브 보호가 모두 비활성화된 경우 시스템은 WAF 레이블 필터를 기반으로 봇 활동을 로깅하는 Log Lambda 구문 분석기를 사용합니다.

다음 절차 중 하나를 사용하여 CloudFront 배포의 요청에 대한 허니팟 링크를 포함합니다.

Honeypot 엔드포인트에 대한 CloudFront 오리진 생성

CloudFront 배포와 함께 배포된 웹 애플리케이션에이 절차를 사용합니다. CloudFront를 사용하면 로봇 제외 표준을 무시하는 콘텐츠 스크레이퍼와 봇을 식별하는 데 도움이 되는 `robots.txt` 파일을 포함할 수 있습니다. 다음 단계를 완료하여 숨겨진 링크를 임베드한 다음 `robots.txt` 파일에 명시적으로 허용하지 않습니다.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 1단계에서 빌드한 스택을 선택합니다. 스택 시작
3. 출력 탭을 선택합니다.
4. BadBotHoneypotEndpoint 키에서 엔드포인트 URL을 복사합니다.
   - 동작 경로(`/ProdStage`)
5. 허니팟을 가리키는 콘텐츠에이 엔드포인트 링크를 포함합니다. 인간 사용자로부터이 링크를 숨깁니다. 예를 들어와 같은 코드 샘플을 검토합니다`<a href="/behavior_path" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>`.
6. 다음과 같이 허니팟 링크를 명시적으로 허용하지 않도록 웹 사이트 루트의 `robots.txt` 파일을 수정합니다.

```
User-agent: <*>
        Disallow: /<behavior_path>
```

> **Important**
>
> 요청은 WAF BadBotRuleFilter에서 차단되므로 CloudFront에서 경로 등록이 필요하지 않습니다. 로그에 자동으로 수집되는 솔루션. 로그 구문 분석기 Lambda로 처리됩니다. 이 간소화된 접근 방식은 추가 엔드포인트 구성이 필요한 대신 WAF 로그를 직접 사용하므로 로그 분석을 통해 잘못된 봇 감지 프로세스가 더 효율적입니다.

> **Note**
>
> 웹 사이트 환경에서 작동하는 태그 값을 확인하는 것은 사용자의 책임입니다. 환경이 이를 준수하지 않는 `rel="nofollow"` 경우를 사용하지 마십시오. 로봇 메타 태그 구성에 대한 자세한 내용은 Google 개발자 안내서를 참조하세요. 다음과 같이 허니팟 링크를 명시적으로 허용하지 않도록 웹 사이트 루트의 `robots.txt` 파일을 수정합니다.

Honeypot 엔드포인트를 외부 링크로 임베드

> **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.

웹 애플리케이션에이 절차를 사용합니다.

1. AWS CloudFormation 콘솔에 로그인합니다.
2. 1단계에서 빌드한 스택을 선택합니다. 스택 시작을 참조하세요.
3. 출력 탭을 선택합니다.
4. BadBotHoneypotEndpoint 키에서 엔드포인트 URL을 복사합니다.

```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-
hidden="true"><honeypot link></a>
```

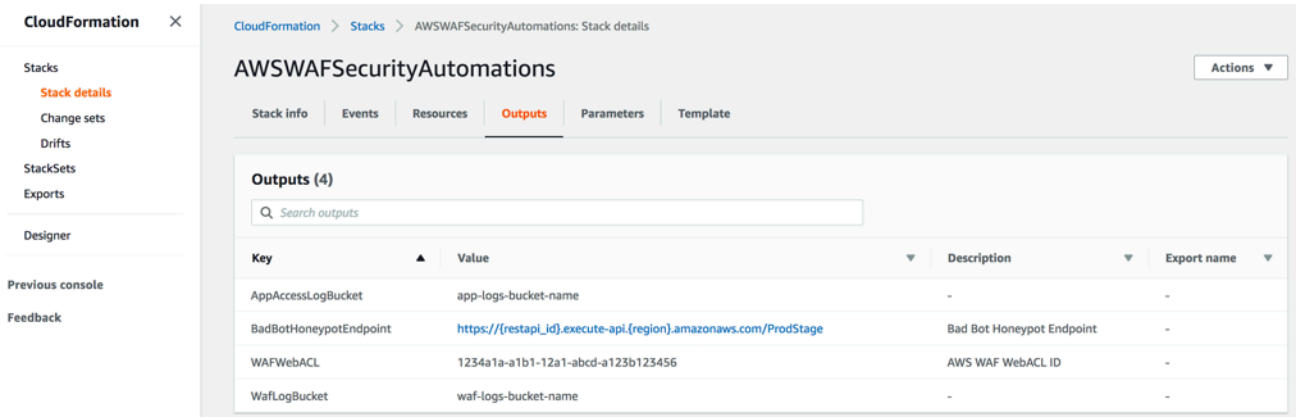
> **Note**
>
> 이 절차에서는 `rel=nofollow`를 사용하여 로봇이 허니팟 URL에 액세스하지 않도록 지시합니다. 그러나 링크는 외부에 포함되므로 링크를 명시적으로 허용하지 않는 `robots.txt` 파일을 포함할 수 없습니다. 웹 사이트 환경에서 작동하는 태그를 확인하는 것은 사용자의 책임입니다. 환경이 이를 준수하지 않는 `rel="nofollow"` 경우를 사용하지 마십시오.

Lambda 로그 구문 분석기 JSON 파일 사용

HTTP 서비스 장애 방지에 Lambda 로그 구문 분석기 JSON 파일 사용

HTTP 서비스 장애 방지 활성화 템플릿 파라미터Yes - AWS Lambda log parser로를 선택한 경우이 솔루션은 라는 구성 파일을 생성하여 AWS WAF 로그 파일을 저장하는 데 사용되는 Amazon S3 버킷에 `<stack_name>-waf_log_conf.json` 업로드합니다. 버킷 이름을 찾으려면 CloudFormation 출력에서 WafLogBucket 변수를 참조하세요. 다음 그림은 예를 보여줍니다.

AWSWAFSecurityAutomations 레이블이 지정된 화면을 보여주고 4개의 출력을 나열하는 스크린샷



Amazon S3에서 `<stack_name>-waf_log_conf.json` 파일을 편집하고 덮어쓰면 Log Parser Lambda 함수는 새 AWS WAF 로그 파일을 처리할 때 새 값을 고려합니다. 다음은 구성 파일 예제입니다.

샘플 구성 파일의 스크린샷

```
{
 "general": {
    "requestThreshold": 2000,
    "blockPeriod": 240,
    "ignoredSufixes": [".css", ".js", ".jpg", "png", ".gif"]
  },
 "uriList": {
    "/search": {
        "requestThreshold": 500,
        "blockPeriod": 600
    }
  }
}
```

파라미터에는 다음이 포함됩니다.

- 일반
  - 요청 임계값(필수) - IP 주소당 5분당 허용되는 최대 요청 수입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.
  - 차단 기간(필수) - 적용 가능한 IP 주소를 차단하는 기간(분)입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.
  - 무시된 접미사 -이 유형의 리소스에 액세스하는 요청은 임곗값을 요청하는 데 포함되지 않습니다. 기본적으로이 목록은 비어 있습니다.
- URI 목록 - 이를 사용하여 특정 URLs에 대한 사용자 지정 요청 임계값 및 차단 기간을 정의합니다. 기본적으로이 목록은 비어 있습니다.

WAF 로그가 WafLogBucket에 도착하면 구성 파일의 구성을 사용하여 Lambda 로그 구문 분석기 함수에 의해 처리됩니다. 솔루션은 `<stack_name>-waf_log_out.json` 동일한 버킷에 있는 라는 출력 파일에 결과를 기록합니다. 출력 파일에 공격자로 식별된 IP 주소 목록이 포함된 경우 솔루션은 이를 HTTP Flood용 WAF IP 세트에 추가하고 애플리케이션에 액세스할 수 없도록 차단합니다. 출력 파일에 IP 주소가 없는 경우 구성 파일이 유효한지 또는 구성 파일에 따라 속도 제한을 초과했는지 확인합니다.

스캐너 및 프로브 보호에 Lambda 로그 구문 분석기 JSON 파일 사용

스캐너 및 프로브 보호 활성화 템플릿 파라미터에 `Yes - AWS Lambda log parser` 대해를 선택한 경우이 솔루션은 라는 구성 파일을 생성하여 CloudFront 또는 Application Load Balancer 로그 파일을 저장하는 데 사용되는 정의된 Amazon S3 버킷에 `<stack_name>-app_log_conf.json` 업로드합니다.

Amazon S3에서 `<stack_name>-app_log_conf.json`를 편집하고 덮어쓰면 `Log Parser` Lambda 함수는 새 AWS WAF 로그 파일을 처리할 때 새 값을 고려합니다. 다음은 구성 파일 예제입니다.

구성 파일의 스크린샷

파라미터에는 다음이 포함됩니다.

- 일반
  - 오류 임계값(필수) - IP 주소당 분당 허용되는 최대 잘못된 요청 수입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.
  - 차단 기간(필수) - 적용 가능한 IP 주소를 차단하는 기간(분)입니다. 이 솔루션은 CloudFormation 스택을 프로비저닝하거나 업데이트할 때 정의한 값을 사용합니다.
  - 오류 코드 - 오류로 간주되는 상태 코드를 반환합니다. 기본적으로이 목록은 , , `400 (Bad Request)`, 및 HTTP 상태 코드를 오류로 간주합니다`401 (Unauthorized)403 (Forbidden)404 (Not Found)405 (Method Not Allowed)`.
- URI 목록 - 이를 사용하여 특정 URLs에 대한 사용자 지정 요청 임계값 및 차단 기간을 정의합니다. 기본적으로이 목록은 비어 있습니다.

애플리케이션 액세스 로그가 AppAccessLogBucket에 도착하면 `Log Parser` Lambda 함수는 구성 파일의 구성을 사용하여 이를 처리합니다. 솔루션은 동일한 버킷의 `<stack_name>`-app_log_out.json`이라는 출력 파일에 결과를 기록합니다. 출력 파일에 공격자로 식별된 IP 주소 목록이 포함된 경우 솔루션은 이를 스캐너 및 프로브용 WAF IP 세트에 추가하고 애플리케이션에 액세스하는 것을 차단합니다. 출력 파일에 IP 주소가 없는 경우 구성 파일이 유효한지 또는 구성 파일에 따라 속도 제한을 초과했는지 확인합니다.

HTTP flood Athena 로그 구문 분석기에서 국가 및 URI 사용

Athena 쿼리에서 국가 및 URI와 함께 IPs별로 그룹화하여 예측할 수 없는 URI 패턴이 있는 HTTP 플러드 공격을 탐지하고 차단할 수 있습니다. 이렇게 하려면 스택을 시작할 때 HTTP Flood Athena 쿼리의 요청별 그룹화 파라미터에 대한 옵션(`Country`, `URI`, `Country and URI`) 중 하나를 선택합니다.

국가별 요청 임계값 파라미터를 사용하여 국가별 요청 임계값을 입력할 수도 있습니다. 예를 들어 `{"TR": 50,"ER":150}`입니다. 솔루션은 이러한 지정된 국가에서 시작된 요청에 대해 이러한 임계값을 사용합니다. 솔루션은 다른 국가의 요청에 기본 임계값을 사용합니다.

> **Note**
>
> 국가별 임계값을 정의하면 솔루션은 Athena 쿼리 그룹화 기준 절에 국가를 자동으로 포함합니다. 자세한 내용은 1단계의 파라미터 표를 참조하세요. 스택 시작을 참조하세요.

솔루션은 기본적으로 5분 동안 요청 임계값을 계산합니다. 이는 Athena 쿼리 실행 시간 일정(분) 파라미터로 구성할 수 있습니다.

> **Note**
>
> Athena 쿼리는 요청 임계값을 기간으로 나누어 분당 임계값을 계산합니다. 예:
> 요청 임계값(기본 임계값 또는 국가별 임계값): 100
> Athena 쿼리 실행 시간 일정: 5
> 분당 요청 임계값: 20 = 100/5

Amazon Athena 쿼리 보기

HTTP Flood 보호 활성화 또는 스캐너 및 프로브 보호 활성화 템플릿 파라미터`Yes - Amazon Athena log parser`에 대해를 선택한 경우이 솔루션은 CloudFront 또는 ALB(`ScannersProbesLogParser`) 또는 AWS WAF 로그()에 대한 Athena 쿼리를 생성 및 실행하고`HTTPFloodLogParser`, 출력을 구문 분석하고, 그에 따라 AWS WAF를 업데이트합니다.

성능을 개선하고 비용을 낮게 유지하기 위해 솔루션은 파일 이름의 타임스탬프를 기반으로 로그를 분할합니다. 이 솔루션은 파티션 키(년, 월, 일 및 시간)를 사용하는 Athena 쿼리를 동적으로 생성합니다. 기본적으로 쿼리는 5분마다 실행됩니다. Athena 쿼리 실행 시간 일정(분) 템플릿 파라미터의 값을 변경하여 실행 일정을 구성할 수 있습니다. 각 쿼리 실행은 기본적으로 지난 4~5시간의 데이터를 스캔합니다. WAF Block Period 템플릿 파라미터의 값을 변경하여 쿼리가 스캔하는 데이터의 양을 구성할 수 있습니다. 또한이 솔루션은 쿼리 액세스 및 비용을 관리하기 위해 별도의 작업 그룹에 쿼리를 배치합니다.

> **Note**
>
> Athena가 AWS Glue 데이터 카탈로그에 액세스하도록 구성되어 있는지 확인합니다. 이 솔루션은 AWS Glue에서 액세스 로그 데이터 카탈로그를 생성하고 데이터를 처리하도록 Athena 쿼리를 구성합니다. Athena가 올바르게 구성되지 않으면 쿼리가 실행되지 않습니다. 자세한 내용은 AWS Glue 데이터 카탈로그를 최신 AWSAWS Glue 데이터 카탈로그로 단계별 업그레이드를 참조step-by-step.

다음 절차에 따라 이러한 쿼리를 봅니다.

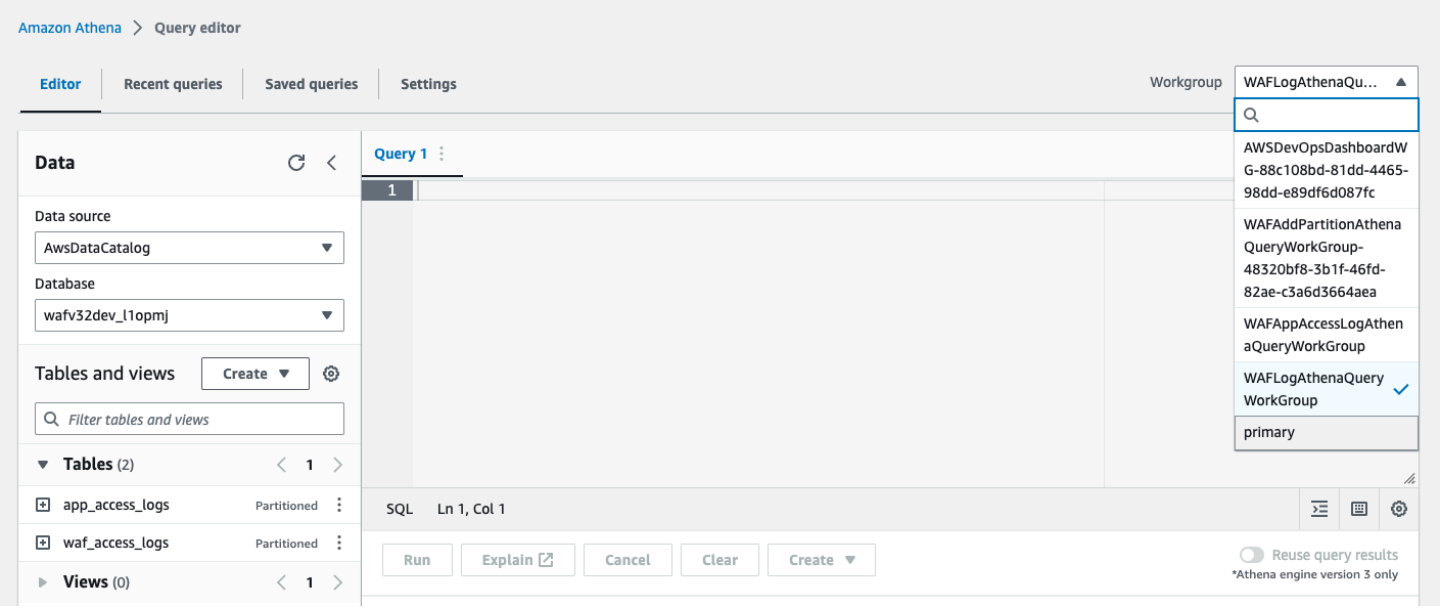
WAF 로그 쿼리 보기

1. Amazon Athena 콘솔에 로그인합니다.
2. 쿼리 편집기 시작을 선택합니다.
3. 이 솔루션의 데이터베이스를 선택합니다.
4. 드롭다운 목록에서 WAFLogAthenaQueryWorkGroup을 선택합니다.

> **Note**
>
> 이 작업 그룹은 HTTP 서비스 장애 방지 활성화 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해를 선택한 경우에만 존재합니다.

5. 전환을 선택하여 작업 그룹을 전환합니다.

쿼리가 없는 Athena 쿼리 편집기 스크린샷



1. 기록 탭을 선택합니다.
2. 목록에서 SELECT 쿼리를 선택하고 엽니다.

애플리케이션 액세스 로그 쿼리 보기

1. Amazon Athena 콘솔에 로그인합니다.
2. 작업 그룹 탭을 선택합니다.
3. 목록에서 WAFAppAccessLogAthenaQueryWorkGroup을 선택합니다.

> **Note**
>
> 이 작업 그룹은 스캐너 및 프로브 보호 활성화 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해를 선택한 경우에만 존재합니다.

4. 작업 그룹 전환을 선택합니다.
5. 최근 쿼리 탭을 선택합니다.
6. 목록에서 SELECT 쿼리를 선택하고 엽니다.

Athena 파티션 쿼리 추가 보기

1. Amazon Athena 콘솔에 로그인합니다.

2. 작업 그룹 탭을 선택합니다.
3. 목록에서 WAFAddPartitionAthenaQueryWorkGroup을 선택합니다.

> **Note**
>
> 이 작업 그룹은 HTTP 서비스 장애 방지 활성화 및/또는 스캐너 및 프로브 보호 활성화 템플릿 파라미터에 `Yes - Amazon Athena log parser` 대해를 선택한 경우에만 존재합니다.

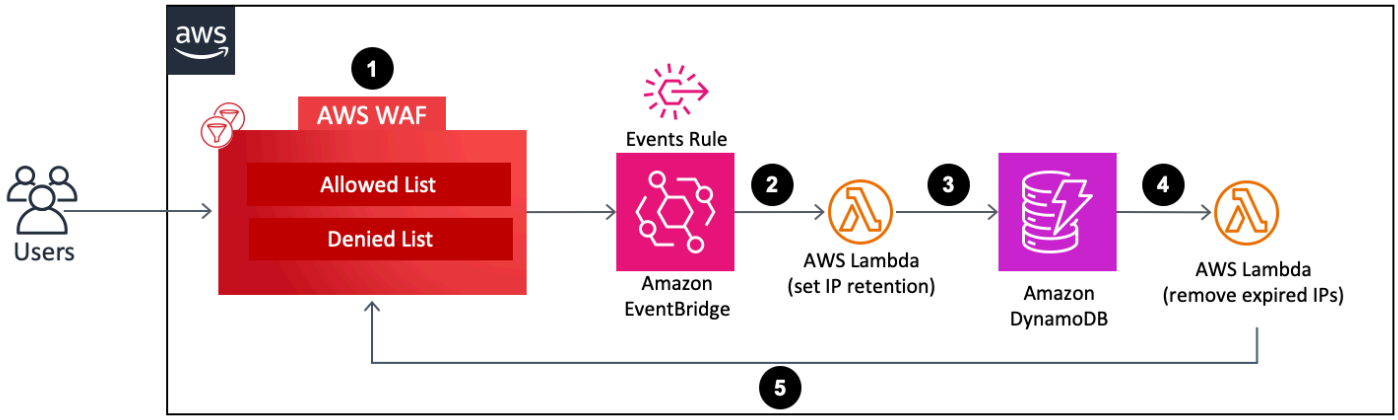
4. 작업 그룹 전환을 선택합니다.
5. 기록 탭을 선택합니다.
6. 목록에서 `ALTER TABLE` 쿼리를 선택하고 엽니다. 이러한 쿼리는 매시간 실행되어 Athena 테이블에 새 시간당 파티션을 추가합니다.

허용 및 거부된 AWS WAF IP 세트에서 IP 보존 구성

솔루션이 생성하는 허용 및 거부 AWS WAF IP 세트에서 IP 보존을 구성할 수 있습니다. 다음 섹션에서는 작동 방식을 설명하고 설정 단계를 제공합니다.

작동 방법

AWS WAF 허용 및 거부 목록과 기타 AWS 리소스를 보여주는 아키텍처 다이어그램



1. 사용자가 허용 또는 거부된 WAF IP 세트를 업데이트(IP 주소 추가 또는 삭제)하면이 작업은 AWS WAF `UpdateIPSet` API 호출을 호출하고 이벤트를 생성합니다.
2. Amazon EventBridge 이벤트 규칙은 사전 정의된 이벤트 패턴을 기반으로 이벤트를 감지하고 Lambda 함수를 호출하여 업데이트 후 IP 세트에 있는 모든 IP 주소의 보존 기간을 설정합니다.

3. Lambda 함수는 이벤트를 처리하고 관련 데이터를 IP 보존(예: IP 세트 이름, ID, 범위, IP 주소)에 추출하여 DynamoDB 테이블에 삽입합니다. 또한 각 DynamoDB 항목에 대한 `ExpirationTime` 속성을 삽입합니다. 솔루션은 이벤트 시간에 사용자 정의 보존 기간을 추가하여 만료 시간을 계산합니다. 테이블에는 DynamoDB Streams 및 TTL(Time to Live)이 켜져 있습니다. TTL 속성은 입니다`ExpirationTime`.
4. 항목이 만료 시간에 도달하면 TTL이 호출되고 DynamoDB는 만료 시간 이후에 테이블에서 항목을 삭제합니다. 항목이 삭제되면 삭제된 항목이 DynamoDB 스트림에 추가되어 다운스트림 처리를 위해 Lambda 함수를 호출합니다.
5. Lambda 함수는 DynamoDB 스트림에서 삭제된 항목에 대한 정보를 가져오고 AWS WAF API 호출을 수행하여 대상 AWS WAF IP 세트에서 항목에 포함된 만료된 IP 주소를 제거합니다.

IP 보존 켜기

다음 단계에 따라 IP 보존을 켭니다.

1. 배포하거나 업데이트하는 Cloudformation 스택에서 허용된 IP 세트의 IP 보존 기간(분)과 거부된 IP 세트의 IP 보존 기간(분)을 입력합니다. 최소 보존 기간은 15분입니다. 솔루션은 `0` ~ 사이의 숫자를 15로 처리합니다15. 배포 구성에 대한 자세한 내용은 1단계를 참조하세요. 스택 시작을 참조하세요.
2. 만료된 IP 주소가 AWS WAF IP 세트에서 제거될 때 이메일 알림을 받으려면 이메일 주소를 입력합니다. 이메일 알림을 받기로 선택한 경우 솔루션이 성공적으로 배포된 후 받은 이메일의 링크를 사용하여 구독을 확인해야 합니다. 배포 구성에 대한 자세한 내용은 1단계를 참조하세요. 스택 시작을 참조하세요.
3. IP 주소를 추가하거나 삭제하여 AWS WAF IP 세트를 업데이트합니다. 이렇게 하면 IP 보존 프로세스가 시작되고 IP 만료 목록을 포함한 DynamoDB 항목이 생성됩니다. 이 만료 목록은 업데이트 후 AWS WAF IP 세트에 있는 IP 주소로 구성됩니다.
4. DynamoDB 항목이 만료 시간에 도달하고 테이블에서 삭제되면 솔루션은 항목의 IP 만료 목록에 포함된 IP 주소를 WAF IP 세트에서 삭제합니다.

> **Note**
>
> DynamoDB가 TTL에서 만료된 항목을 삭제하는 시간에 따라 AWS WAF IP 세트에서 만료된 IP 주소의 실제 삭제 작업이 달라질 수 있습니다. DynamoDB TTL 삭제는 주로 테이블의 크기 및 활동 수준에 따라 달라집니다. DynamoDB 삭제 작업의 잠재적 지연으로 인해 AWS WAF 삭제 작업이 지연될 수 있습니다. 일반적으로 솔루션은 DynamoDB TTL 삭제 직후 AWS WAF IP

세트에서 만료된 IP 주소를 삭제합니다. 자세한 내용은 Amazon DynamoDB 개발자 안내서의 DynamoDB TTL(Time to Live)을 참조하세요. DynamoDB

모니터링 대시보드 구축

AWS는 각 중요 엔드포인트에 대해 사용자 지정 기준 모니터링 시스템을 구성할 것을 권장합니다. 사용자 지정 지표 보기 생성 및 사용에 대한 자세한 내용은 CloudWatch 대시보드 - 사용자 지정 지표 보기 생성 및 사용 및 Amazon CloudWatch 대시보드 사용을 참조하세요.

다음 대시보드 스크린샷은 사용자 지정 기준 모니터링 시스템의 예를 보여줍니다.

CloudFront 대시보드 스크린샷

대시보드에는 다음 지표가 표시됩니다.

- 허용된 요청과 차단된 요청 비교 - 허용된 액세스(정상 피크 액세스의 2배) 또는 차단된 액세스(차단된 요청이 1K000개를 초과하는 것을 식별하는 기간)의 급증을 받는 경우 표시됩니다. CloudWatch는 Slack 채널에 알림을 보냅니다. 이 지표를 사용하여 알려진 DDoS 공격(차단된 요청이 증가할 때) 또는 공격의 새 버전(요청이 시스템에 액세스할 수 있는 경우)을 추적할 수 있습니다.

> **Note**
>
> 참고: 솔루션은이 지표를 제공합니다.

- BytesDownloaded vs Uploaded - DDoS 공격이 일반적으로 소진 리소스에 대한 대량의 액세스를 수신하지 않는 서비스를 대상으로 하는 시기를 식별하는 데 도움이 됩니다(예: 검색 엔진 구성 요소에서 하나의 특정 요청 파라미터 세트에 대해 MBs의 정보를 전송).
- ELB 스필오버 및 대기열 길이 - DDoS 공격으로 인해 인프라가 손상되고 공격자가 CloudFront 또는 AWS WAF 계층을 우회하고 보호되지 않는 리소스를 직접 공격하는지 확인하는 데 도움이 됩니다.
- ELB 요청 수 - 인프라 손상을 식별하는 데 도움이 됩니다. 이 지표는 공격자가 보호 계층을 우회하는지 또는 캐시 적중률을 높이기 위해 CloudFront 캐시 규칙을 검토해야 하는지를 보여줍니다.
- ELB 정상 호스트 - 다른 시스템 상태 확인 지표로 사용할 수 있습니다.
- ASG CPU 사용률 - 공격자가 CloudFront, AWS WAF 및 Elastic Load Balancing을 우회하고 있는지 식별하는 데 도움이 됩니다. 이 지표를 사용하여 공격의 피해를 식별할 수도 있습니다.

XSS 오탐 처리

이 솔루션은 일반적으로 탐색되는 수신 요청 요소를 검사하여 XSS 공격을 식별하고 차단하는 AWS WAF 규칙을 구성합니다. 이 감지 패턴은 합법적인 사용자가 콘텐츠 관리 시스템에서 서식 있는 텍스트 편집기를 사용하여 HTML을 작성하고 제출하도록 허용하는 워크로드의 경우 덜 효과적입니다. 이 시나리오에서는 서식 있는 텍스트 입력을 허용하는 특정 URL 패턴에 대한 기본 XSS 규칙을 우회하는 예외 규칙을 생성하고 제외된 URLs을 보호하는 대체 메커니즘을 구현하는 것이 좋습니다.

또한 일부 이미지 또는 사용자 지정 데이터 형식은 HTML 콘텐츠에서 잠재적 XSS 공격을 나타내는 패턴을 포함하므로 오탐지가 발생할 수 있습니다. 예를 들어 SVG 파일에는 `<script>` 태그가 포함될 수 있습니다. 합법적인 사용자로부터 이러한 유형의 콘텐츠를 기대하는 경우 이러한 다른 데이터 형식을 포함하는 HTML 요청을 허용하도록 XSS 규칙을 좁히십시오.

다음 단계를 완료하여 입력으로 HTML을 허용하는 URLs을 제외하도록 XSS 규칙을 업데이트합니다. 자세한 지침은 Amazon WAF 개발자 안내서를 참조하세요.

1. AWS WAF 콘솔에 로그인합니다.
2. 문자열 일치 또는 정규식 조건을 생성합니다.
3. URI를 검사하고 XSS 규칙에 대해 수락하려는 값을 나열하도록 필터 설정을 구성합니다.
4. 이 솔루션의 XSS 규칙을 편집하고 생성한 새 조건을 추가합니다.

예를 들어 목록의 모든 URLs 제외하려면 요청 시에서 다음을 선택합니다.

- 는
- 문자열 일치 조건에서 하나 이상의 파일러와 일치
- XSS 허용 목록

문제 해결

이 솔루션에 도움이 필요한 경우 Support에 문의하여이 솔루션에 대한 지원 사례를 개설하세요.

Support에 문의하세요.

AWS 개발자 지원, AWS 비즈니스 지원 또는 AWS 엔터프라이즈 지원이 있는 경우 지원 센터를 사용하여이 솔루션에 대한 전문가 지원을 받을 수 있습니다. 이후 단원에서는 그 방법에 대해서 설명합니다.

사례 생성

1. 지원 센터를 엽니다.
2. 사례 생성을 선택합니다.

어떻게 도와드릴까요?

1. 기술을 선택합니다.
2. 서비스에서 WAF 또는 AWS WAF를 선택합니다.
3. 범주에서 WAF 보안 자동화 또는 AWS WAF용 보안 자동화를 선택합니다.
4. 심각도의 경우 사용 사례와 가장 일치하는 옵션입니다.
5. 서비스, 범주 및 심각도를 입력하면 인터페이스가 일반적인 문제 해결 질문에 대한 링크를 채웁니다. 이러한 링크로 질문을 해결할 수 없는 경우 다음 단계: 추가 정보를 선택합니다.

추가 정보

1. 제목에 질문 또는 문제를 요약하는 텍스트를 입력합니다.
2. 설명에서 문제를 자세히 설명합니다.
3. 파일 연결을 선택합니다.
4. Support에서 요청을 처리하는 데 필요한 정보를 첨부합니다.

사례를 더 빠르게 해결할 수 있도록 지원

1. 요청된 정보를 입력합니다.

2. 다음 단계: 지금 해결하거나 문의하기를 선택합니다.

지금 해결하거나 문의하기

1. 지금 해결 솔루션을 검토합니다.
2. 이러한 솔루션의 문제를 해결할 수 없는 경우 문의하기를 선택하고 요청된 정보를 입력한 다음 제출을 선택합니다.

개발자 안내서

이 섹션에서는 솔루션의 소스 코드를 제공합니다.

소스 코드

GitHub 리포지토리를 방문하여이 솔루션의 템플릿과 스크립트를 다운로드하고 사용자 지정을 다른 사용자와 공유합니다.

이 솔루션의 템플릿은 AWS CDK를 사용하여 생성됩니다. 자세한 내용은 README.md 파일을 참조하세요.

레퍼런스

이 섹션에는이 솔루션에 대한 고유한 지표를 수집하기 위한 선택적 기능, 관련 리소스에 대한 포인터, 이 솔루션에 기여한 빌더 목록에 대한 정보가 포함되어 있습니다.

익명화된 데이터 수집

이 솔루션에는 운영 지표를 AWS로 전송하는 옵션이 포함되어 있습니다. 당사는 이 데이터를 사용하여 고객이 이 솔루션과 관련 서비스 및 제품을 어떻게 사용하는지 더 잘 이해합니다. 이 기능을 켜면 솔루션은 CloudFormation 템플릿을 처음 배포하는 동안 다음과 같은 정보를 수집하여 AWS로 전송합니다.

- 솔루션 ID - AWS 솔루션 식별자
- 고유 ID(UUID) -이 솔루션의 각 배포에 대해 무작위로 생성된 고유 식별자
- 타임스탬프 - 데이터 수집 타임스탬프
- 솔루션 구성 - 초기 시작 시 설정된 기능 및 파라미터
- 수명 주기 - 고객이이 솔루션을 사용한 기간(스택 삭제 기준)
- 로그 구문 분석기 데이터:
  - 스캐너 및 프로브 IP 세트, 잘못된 봇 IP 세트 및 HTTP Flood IP 세트의 IP 주소 수를 차단으로 설정
  - 처리 및 차단된 요청 수
- IP 목록 구문 분석기 데이터:
  - 평판 목록 IP 세트의 IP 주소 수
  - 처리 및 차단된 요청 수
- IP 보존 데이터 - 허용 또는 거부 IP 세트에서 제거되는 만료된 IP 주소 수

AWS는이 설문 조사를 통해 수집된 데이터를 소유합니다. 데이터 수집에는 AWS 개인정보 취급방침이 적용됩니다. 이 기능을 옵트아웃하려면 AWS CloudFormation 템플릿을 시작하기 전에 다음 단계를 완료하세요.

1. `aws-waf-security-automations.template` AWS CloudFormation을 로컬 하드 드라이브에 다운로드합니다.
2. 텍스트 편집기를 사용하여 CloudFormation 템플릿을 엽니다.
3. CloudFormation 템플릿 매핑 섹션을 다음에서 수정합니다.

```
Solution:
  Data:
   SendAnonymizedUsageData: "Yes"
```

변경 후:

```
Solution:
  Data:
   SendAnonymizedUsageData: "No"
```

4. AWS CloudFormation 콘솔에 로그인합니다.
5. 스택 생성을 선택합니다.
6. 스택 생성 페이지, 템플릿 지정 섹션에서 템플릿 파일 업로드를 선택합니다.
7. 템플릿 파일 업로드에서 파일 선택을 선택하고 로컬 드라이브에서 편집한 템플릿을 선택합니다.
8. 다음을 선택하고 1단계의 단계를 따릅니다. 스택 시작을 참조하세요.

관련 리소스

연결된 AWS 백서

- DDoS 복원력에 대한 AWS 모범 사례

연결된 AWS 보안 블로그 게시물

- AWS WAF, Amazon CloudFront 및 Referer Checking을 사용하여 핫 링크 연결을 방지하는 방법

타사 IP 평판 목록

- Spamhaus DROP 목록 웹 사이트
- Proofpoint 새로운 위협 IP 목록
- Tor 종료 노드 목록

기여자

- 하이터 바이탈
- Lee Atkinson
- 벤 포터
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- 쇼 잭슨
- William Quan
- Mykhailo Markhain

개정

GitHub 리포지토리의 CHANGELOG.md 방문하여 버전별 개선 사항 및 수정 사항을 추적하세요.

고지 사항

이 구현 가이드는 정보 제공 목적으로만 제공됩니다. 이 문서는이 문서의 발행일을 기준으로 현재 AWS 제품 제공 및 관행을 나타내며, 예고 없이 변경될 수 있습니다. 고객은 본 문서의 정보를 독립적으로 평가하고 AWS 제품 또는 서비스를 사용할 책임이 있으며, 각 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증도 없이 "있는 그대로" 제공됩니다. 이 문서는 AWS, 그 계열사, 공급업체 또는 라이선스 제공자로부터 어떠한 보증, 진술, 계약 약정, 조건 또는 보증도 생성하지 않습니다. 고객에 대한 AWS의 책임 및 채무는 AWS 계약에 준거합니다. 본 문서는 AWS와 고객 간의 어떠한 계약도 구성하지 않으며 이를 변경하지도 않습니다.

AWS WAF용 보안 자동화 솔루션은 Apache 라이선스 버전 2.0의 약관에 따라 라이선스가 부여됩니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.