Guida all'implementazione

Automazioni di sicurezza per AWS WAF

Automazioni di sicurezza per AWS WAF: Guida all'implementazione

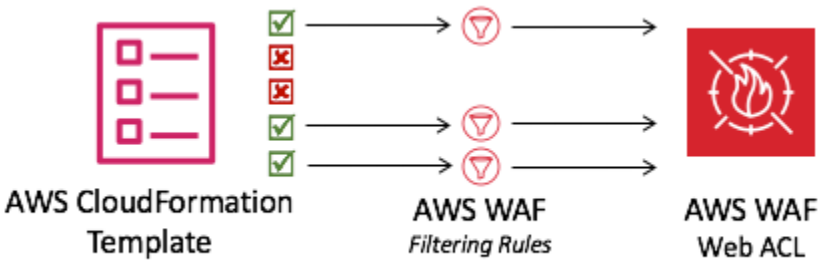
Table of Contents

Implementa automaticamente una singola lista di controllo degli accessi Web che filtra gli attacchi basati sul Web con Security Automations su AWS WAF

La soluzione Security Automations for AWS WAF implementa una serie di regole preconfigurate per aiutarti a proteggere le tue applicazioni dagli exploit web comuni. Il servizio principale di questa soluzione, AWS WAF, aiuta a proteggere le applicazioni Web dalle tecniche di attacco che possono influire sulla disponibilità delle applicazioni, compromettere la sicurezza o consumare risorse eccessive. Puoi usare AWS WAF per definire regole di sicurezza web personalizzabili. Queste regole controllano il traffico da consentire o bloccare verso le applicazioni Web e le interfacce di programmazione delle applicazioni (APIs) distribuite su risorse AWS come Amazon CloudFront, Application Load Balancer (ALB). Per altri tipi di risorse supportati, consulta AWS WAF nella AWS WAF, AWS Firewall Manager e AWS Shield Advanced Developer Guide.

La configurazione delle regole di AWS WAF può essere impegnativa e onerosa sia per le organizzazioni grandi che per quelle piccole, specialmente per quelle che non dispongono di team di sicurezza dedicati. Per semplificare questo processo, la soluzione Security Automations for AWS WAF implementa automaticamente una singola lista di controllo degli accessi Web (ACL) con un set di regole AWS WAF progettate per filtrare i comuni attacchi basati sul Web. Durante la configurazione iniziale del CloudFormation modello AWS di questa soluzione, puoi specificare quali funzionalità di protezione includere. Dopo aver distribuito questa soluzione, AWS WAF ispeziona le richieste Web alle distribuzioni o ALB CloudFront esistenti e le blocca quando applicabile.

Un CloudFormation modello implementa un ACL Web con regole di filtraggio AWS WAF.



Questa guida all'implementazione illustra considerazioni architettoniche, fasi di configurazione e best practice operative per la distribuzione di questa soluzione nel cloud Amazon Web Services (AWS). Include collegamenti a CloudFormation modelli che avviano, configurano ed eseguono i servizi di

sicurezza, calcolo, storage e altri servizi AWS necessari per distribuire questa soluzione su AWS, utilizzando le best practice di AWS per la sicurezza e la disponibilità.

Le informazioni contenute in questa guida presuppongono una conoscenza pratica dei servizi AWS come AWS WAF CloudFront e AWS Lambda. ALBs Richiede inoltre una conoscenza di base degli attacchi e delle strategie di mitigazione comuni basati sul Web.

> **Note**
>
> A partire dalla versione 3.0.0, questa soluzione supporta l'ultima versione dell'API del servizio AWS WAF (AWS). WAFV2

Questa guida è destinata a responsabili IT, ingegneri della sicurezza, DevOps ingegneri, sviluppatori, architetti di soluzioni e amministratori di siti Web.

> **Note**
>
> Consigliamo di utilizzare questa soluzione come punto di partenza per l'implementazione delle regole AWS WAF. Puoi personalizzare il codice sorgente, aggiungere nuove regole personalizzate e sfruttare altre regole gestite da AWS WAF in base alle tue esigenze.

Usa questa tabella di navigazione per trovare rapidamente le risposte a queste domande:

Se vuoi.	Leggi..
Conosci il costo di esecuzione di questa soluzione. Il costo totale per l'esecuzione di questa soluzione dipende dalla protezion e attivata e dalla quantità di dati acquisiti, archiviati ed elaborati.	Costo
Comprendi le considerazioni sulla sicurezza relative a questa soluzione.	Sicurezza
Scopri quali regioni AWS sono supportate per questa soluzione.	Regioni AWS supportate

Se vuoi.	Leggi..
Visualizza o scarica il CloudFormation modello incluso in questa soluzione per distribuire automaticamente le risorse dell'infrastruttura (lo «stack») per questa soluzione.	CloudFormation Modello AWS
Utilizza Support per aiutarti a implementare, utilizzare o risolvere i problemi della soluzione.	Support
Accedi al codice sorgente e, facoltativamente, utilizza l'AWS Cloud Development Kit (AWS CDK) per distribuire la soluzione	GitHub repository

Funzionalità e vantaggi

La soluzione Security Automations for AWS WAF offre le seguenti caratteristiche e vantaggi.

Proteggi le tue applicazioni Web con i gruppi di regole AWS Managed Rules

AWS Managed Rules per AWS WAF fornisce protezione contro le vulnerabilità comuni delle applicazioni o altro traffico indesiderato. Questa soluzione include gruppi di regole di reputazione AWS Managed IP, gruppi di regole di base AWS Managed e gruppi di regole AWS Managed specifici per casi d'uso. Hai la possibilità di selezionare uno o più gruppi di regole per il tuo ACL web, fino alla quota massima di unità di capacità Web ACL (WCU).

Fornisci una protezione dalle inondazioni di livello 7 con una regola personalizzata HTTP Flood predefinita

La regola personalizzata HTTP Flood protegge da un attacco Distributed Denial-of-Service (DDoS) a livello web per un periodo di tempo definito dal cliente. Puoi scegliere una di queste opzioni per attivare questa regola:

- Regola basata sulla tariffa AWS WAF
- Analizzatore di log Lambda
- Analizzatore di log Amazon Athena

Le opzioni Lambda log parser o Athena log parser consentono di definire una quota di richieste inferiore a 100. Questo approccio può aiutarti a non raggiungere la quota richiesta dalle regole basate sulle tariffe di AWS WAF. Per ulteriori informazioni, consulta Log parser options.

Puoi anche migliorare il parser di log Athena aggiungendo un paese e un URI (Uniform Resource Identifier) alle condizioni di filtraggio. Questo approccio identifica e blocca gli attacchi HTTP flood con pattern URI imprevedibili. Per ulteriori informazioni, consulta Usa paese e URI nel parser di log HTTP Flood Athena.

Blocca lo sfruttamento delle vulnerabilità con la regola personalizzata predefinita di Scanners & Probes

La regola personalizzata Scanners & Probes analizza i log di accesso alle applicazioni alla ricerca di comportamenti sospetti, come una quantità anomala di errori generati da un'origine. Blocca quindi quegli indirizzi IP di origine sospetti per un periodo di tempo definito dal cliente. Puoi scegliere una di queste opzioni per attivare questa regola: Lambda log parser o Athena log parser. Per ulteriori informazioni, consulta Opzioni del parser di log.

Rileva e devia le intrusioni con la regola personalizzata Bad Bot predefinita

La regola personalizzata Bad Bot imposta un endpoint honeypot, ovvero un meccanismo di sicurezza progettato per attirare e deviare un tentativo di attacco. Puoi inserire l'endpoint nel tuo sito Web per rilevare le richieste in entrata provenienti da content scraper e bot pericolosi. Una volta rilevate, tutte le richieste successive provenienti dalle stesse origini verranno bloccate. Per ulteriori informazioni, consulta Incorporare il link Honeypot nella tua applicazione web.

Blocca gli indirizzi IP dannosi con reputazioni IP predefinite, elenchi, regole personalizzate

La regola personalizzata degli elenchi di reputazione IP verifica ogni ora gli elenchi di reputazione IP di terze parti per individuare nuovi intervalli IP da bloccare. Questi elenchi includono gli elenchi Spamhaus Don't Route Or Peer (DROP) ed Extended DROP (EDROP), l'elenco IP di Proofpoint Emerging Threats e l'elenco dei nodi di uscita Tor.

Fornisci una configurazione IP manuale con elenchi di IP consentiti e negati predefiniti, regole personalizzate

Le regole personalizzate degli elenchi di IP consentiti e negati consentono di inserire manualmente gli indirizzi IP che si desidera consentire o negare. È inoltre possibile configurare la conservazione degli IP negli elenchi di IP consentiti e negati in modo che scada IPs a un orario prestabilito.

Crea la tua dashboard di monitoraggio

Questa soluzione emette CloudWatch parametri Amazon come richieste consentite, richieste bloccate e altri parametri pertinenti. Puoi creare una dashboard personalizzata per visualizzare queste metriche e ottenere informazioni sul modello di attacchi e protezione fornito da AWS WAF. Per ulteriori informazioni, consulta Build monitoring dashboard.

Casi d'uso

Di seguito sono riportati alcuni esempi di casi d'uso per l'utilizzo di questa soluzione. È possibile personalizzare questa soluzione in modi innovativi che non si limitano a questo elenco.

Automatizza la configurazione delle regole AWS WAF

AWS WAF protegge le tue applicazioni Web dagli attacchi più comuni; tuttavia, la configurazione delle regole di AWS WAF può essere complicata e richiedere molto tempo. Per aiutarti, questa soluzione distribuisce automaticamente un set di regole AWS WAF nel tuo account con CloudFormation un modello. In questo modo, non è necessario configurare personalmente le regole di AWS WAF e puoi iniziare a usare AWS WAF più velocemente.

Personalizza la protezione HTTP Flood di livello 7

Questa soluzione offre tre opzioni per attivare la protezione HTTP Flood. Puoi selezionare l'opzione più adatta alle tue esigenze per ottenere protezione dagli attacchi DDo S. Per ulteriori informazioni, consulta Fornire una protezione dalle inondazioni di livello 7 con la regola personalizzata HTTP Flood predefinita in Caratteristiche e vantaggi.

Sfrutta il codice sorgente per applicare la personalizzazione o creare automazioni di sicurezza personalizzate

Questa soluzione fornisce un esempio di come utilizzare AWS WAF e altri servizi per creare automazioni di sicurezza sul cloud AWS. Il suo codice open source GitHub semplifica l'applicazione

di personalizzazioni o la creazione di automazioni di sicurezza personalizzate adatte alle proprie esigenze.

Concetti e definizioni

Questa sezione descrive i concetti chiave e definisce la terminologia specifica di questa soluzione.

Registri ALB

Questa soluzione utilizza i log per la risorsa ALB. La regola Scanner & Probe Protection di questa soluzione analizza questi registri.

Analizzatore di log Athena

Amazon Athena è un servizio di analisi interattivo senza server basato su framework open source, che supporta tabelle aperte e formati di file. Questa soluzione esegue una query Athena pianificata per ispezionare i log AWS WAF o ALB se l'utente sceglie `yes - Amazon Athena log parser` quando attivare la regola HTTP Flood Protection o la regola Scanner & Probe Protection e può essere utilizzata per Activate Bad Bot Protection tramite un rilevamento che opera attraverso una catena logica strutturata. CloudFront

Regola AWS WAF

Una regola AWS WAF definisce:

- Come ispezionare le richieste web HTTP (S)
- L'azione da intraprendere su una richiesta quando corrisponde ai criteri di ispezione

Le regole vengono definite solo nel contesto di un gruppo di regole o di un ACL Web.

CloudFront logs

Questa soluzione utilizza i log per la CloudFront risorsa. La regola Scanner & Probe Protection di questa soluzione controlla questi registri.

IP impostato

Un set IP fornisce una raccolta di indirizzi IP e intervalli di indirizzi IP che si desidera utilizzare

insieme in una dichiarazione di regole. I set di IP sono risorse AWS.

Analizzatore di log Lambda

Questa soluzione esegue una funzione Lambda richiamata da un evento di creazione di oggetti Amazon Simple Storage Service (Amazon S3). La funzione Lambda avvia un'ispezione dei log di AWS WAF o ALB se l'utente `yes - AWS Lambda log parser` sceglie di attivare HTTP Flood Protection CloudFront, Scanner & Probe Protection e può essere utilizzata per la regola Bad Bot Protection tramite un rilevamento che opera attraverso una catena logica strutturata.

Gruppi di regole gestiti

I gruppi di regole gestiti sono raccolte di ready-to-use regole predefinite che i venditori di AWS e AWS Marketplace scrivono e gestiscono per te. I prezzi di AWS WAF si applicano all'uso di qualsiasi gruppo di regole gestito.

tipo di risorsa/endpoint

Puoi associare le risorse AWS al web ACLs per proteggerle. Queste risorse sono ALB CloudFront, AWS, Amazon Cognito AppSync, AWS App Runner e AWS Verified Access. Attualmente questa soluzione supporta Amazon CloudFront e ALB.

Registri WAF

Questa soluzione utilizza i log generati da AWS WAF per le risorse associate all'ACL Web. Le regole HTTP Flood Protection, Scanner & Probe Protection e Activate Bad Bot Protection per questa soluzione esaminano questi registri.

WCU

AWS WAF utilizza le unità di capacità () della Web Access Control List (ACLWCUs) per calcolare e controllare le risorse operative necessarie per eseguire regole, gruppi di regole e web. ACLs AWS WAF applica le quote WCU quando configuri i gruppi di regole e il web. ACLs WCUs non influiscono sul modo in cui AWS WAF ispeziona il traffico web.

ACL web

Un ACL web ti offre un controllo dettagliato sulle richieste web HTTP (S) a cui risponde la tua risorsa protetta.

> **Note**
>
> Per un riferimento generale ai termini di AWS, consulta il Glossario AWS.

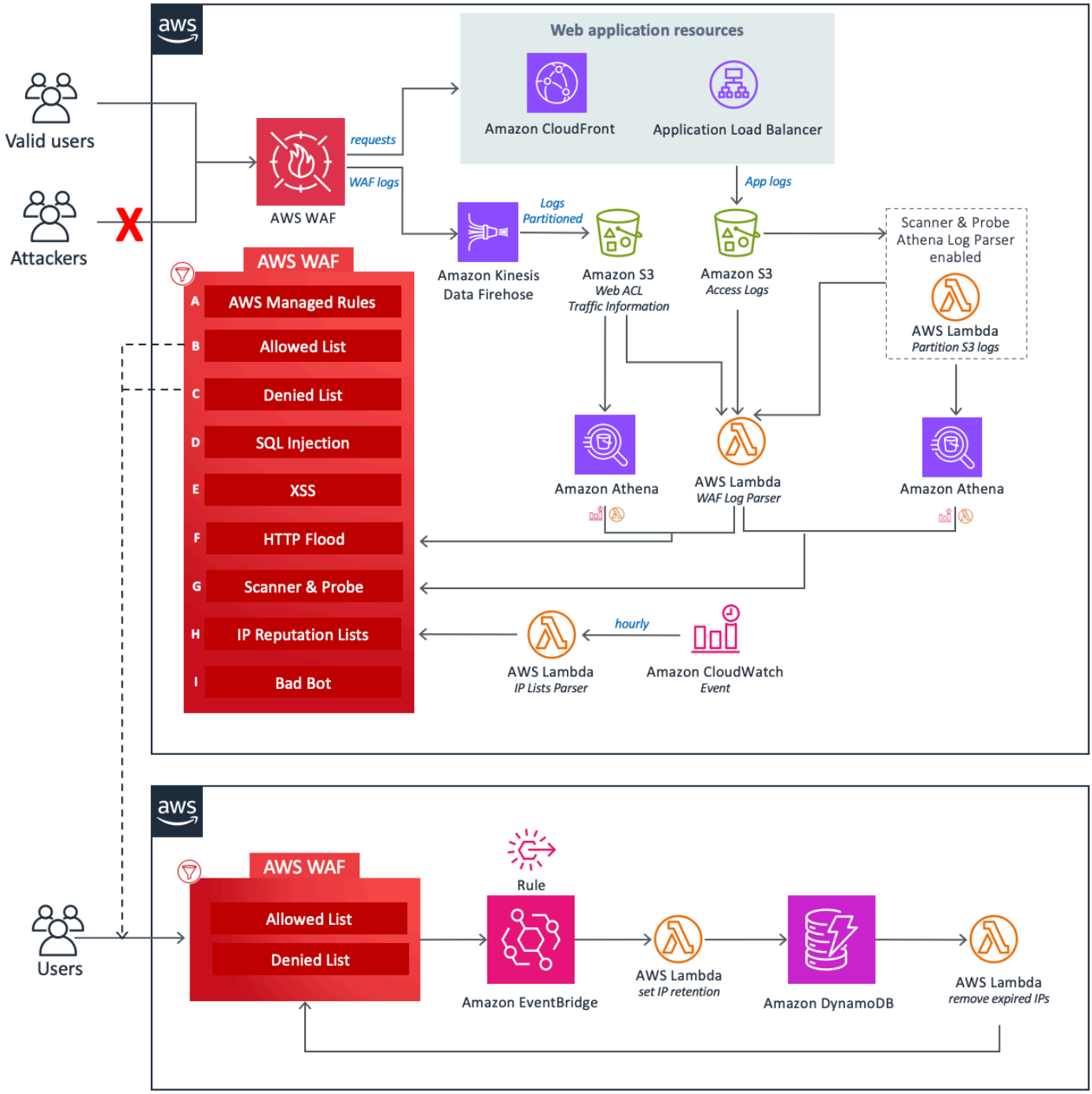
Panoramica dell'architettura

Questa sezione fornisce un diagramma dell'architettura di implementazione di riferimento per i componenti distribuiti con questa soluzione.

Diagramma architetturale

La distribuzione di questa soluzione con i parametri predefiniti distribuisce i seguenti componenti nel tuo account AWS.

CloudFormation template distribuisce AWS WAF e altre risorse AWS per proteggere la tua applicazione web dagli attacchi comuni.



Alla base del design c'è un ACL web AWS WAF, che funge da punto centrale di ispezione e decisione per tutte le richieste in arrivo verso un'applicazione web. Durante la configurazione iniziale dello CloudFormation stack, l'utente definisce quali componenti protettivi attivare. Ogni componente funziona in modo indipendente e aggiunge regole diverse all'ACL Web.

I componenti di questa soluzione possono essere raggruppati nelle seguenti aree di protezione.

> **Note**
>
> Le etichette di gruppo non riflettono il livello di priorità delle regole WAF.

- AWS Managed Rules (A): questo componente contiene i gruppi di regole di reputazione IP di AWS Managed Rules, i gruppi di regole di base e i gruppi di regole specifici per i casi d'uso. Questi gruppi di regole proteggono dallo sfruttamento delle vulnerabilità più comuni delle applicazioni o di altro traffico indesiderato, inclusi quelli descritti nelle pubblicazioni OWASP, senza dover scrivere regole proprie.
- Elenchi IP manuali (B e C): questi componenti creano due regole AWS WAF. Con queste regole, puoi inserire manualmente gli indirizzi IP che desideri consentire o negare. Puoi configurare la conservazione degli IP e rimuovere gli indirizzi IP scaduti su set IP consentiti o negati utilizzando EventBridge le regole di Amazon e Amazon DynamoDB. Per ulteriori informazioni, consulta Configurare la conservazione degli IP sui set IP AWS WAF consentiti e negati.
- SQL Injection (D) e XSS (E): questi componenti configurano due regole AWS WAF progettate per proteggere dai comuni modelli di SQL injection o cross-site scripting (XSS) nell'URI, nella stringa di query o nel corpo di una richiesta.
- HTTP Flood (F): questo componente protegge dagli attacchi che consistono in un gran numero di richieste provenienti da un particolare indirizzo IP, come un attacco S a livello Web o un tentativo di accesso a forza DDo bruta. Con questa regola, si imposta una quota che definisce il numero massimo di richieste in entrata consentite da un singolo indirizzo IP entro un periodo predefinito di cinque minuti (configurabile con il parametro Athena Query Run Time Schedule). Una volta superata questa soglia, le richieste aggiuntive provenienti dall'indirizzo IP vengono temporaneamente bloccate. Puoi implementare questa regola utilizzando una regola basata sulla velocità di AWS WAF o elaborando i log di AWS WAF utilizzando una funzione Lambda o una query Athena. Per ulteriori informazioni sui compromessi relativi alle opzioni di mitigazione delle inondazioni HTTP, consulta le opzioni del parser di log.
- Scanner and Probe (G): questo componente analizza i log di accesso alle applicazioni alla ricerca di comportamenti sospetti, ad esempio una quantità anomala di errori generati da un'origine. Quindi blocca quegli indirizzi IP di origine sospetti per un periodo di tempo definito dal cliente. È possibile implementare questa regola utilizzando una funzione Lambda o una query Athena. Per ulteriori informazioni sui compromessi relativi alle opzioni di mitigazione dello scanner e della sonda, consulta le opzioni del parser di log.
- Elenchi di reputazione IP (H): questo componente è la funzione `IP Lists Parser` Lambda che controlla ogni ora gli elenchi di reputazione IP di terze parti per individuare nuovi intervalli

da bloccare. Questi elenchi includono gli elenchi Spamhaus Don't Route Or Peer (DROP) ed Extended DROP (EDROP), l'elenco IP di Proofpoint Emerging Threats e l'elenco dei nodi di uscita Tor.

- Bad Bot (I): questo componente migliora il rilevamento dei bot non validi monitorando le connessioni dirette a un Application Load Balancer (ALB) o CloudFront Amazon, oltre al meccanismo honeypot. Se un bot aggira l'honeypot e tenta di interagire con ALB or CloudFront, il sistema analizza gli schemi e i log delle richieste per identificare attività dannose. Quando viene rilevato un bot non valido, il relativo indirizzo IP viene estratto e aggiunto a una lista di blocchi AWS WAF per impedire ulteriori accessi. Il rilevamento dei bot non validi opera attraverso una catena logica strutturata, garantendo una copertura completa delle minacce:
  - HTTP Flood Protection Lambda Log Parser: raccoglie i IPs bot danneggiati dalle voci di registro durante l'analisi delle inondazioni.
  - Scanner & Probe Protection Lambda Log Parser: identifica i IPs bot non validi dalle voci di registro relative allo scanner.
  - HTTP Flood Protection Athena Log Parser: estrae il bot non valido IPs dai log di Athena, utilizzando le partizioni durante l'esecuzione delle query.
  - Scanner & Probe Protection Athena Log Parser: recupera i bot danneggiati IPs dai log Athena relativi allo scanner, utilizzando la stessa strategia di partizionamento.
  - Rilevamento fallback: se sia HTTP Flood Protection che Scanner & Probe Protection sono disabilitate, il sistema si basa sul parser Log Lambda, che registra l'attività dei bot in base ai filtri delle etichette WAF.

Ognuna delle tre funzioni Lambda personalizzate di questa soluzione pubblica le metriche di runtime su. CloudWatch Per ulteriori informazioni su queste funzioni Lambda, consulta i dettagli dei componenti.

Considerazioni sulla progettazione di AWS Well-Architected

Questa soluzione utilizza le best practice di AWS Well-Architected Framework, che aiuta i clienti a progettare e gestire carichi di lavoro affidabili, sicuri, efficienti ed economici nel cloud.

Questa sezione descrive in che modo i principi di progettazione e le migliori pratiche di Well-Architected Framework favoriscono questa soluzione.

Eccellenza operativa

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'eccellenza operativa.

- La soluzione utilizza parametri per CloudWatch fornire l'osservabilità dell'infrastruttura, delle funzioni Lambda, di Amazon Data Firehose, dei bucket Amazon S3 e del resto dei componenti della soluzione.
- Sviluppiamo, testiamo e pubblichiamo la soluzione tramite una pipeline di integrazione continua e distribuzione continua (CI/CD) di AWS. Questo aiuta gli sviluppatori a ottenere risultati di alta qualità in modo coerente.
- Puoi installare la soluzione con un CloudFormation modello che fornisca tutte le risorse necessarie nel tuo account. Per aggiornare o eliminare la soluzione, è sufficiente aggiornare o eliminare il modello.

Sicurezza

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sicurezza.

- Tutte le comunicazioni tra servizi utilizzano ruoli AWS Identity and Access Management (IAM).
- Tutti i ruoli utilizzati dalla soluzione seguono l'accesso con privilegi minimi. In altre parole, contengono solo le autorizzazioni minime necessarie per il corretto funzionamento del servizio.
- Tutti gli storage di dati, inclusi i bucket Amazon S3 e DynamoDB, dispongono di crittografia a riposo.

Affidabilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'affidabilità.

- La soluzione utilizza i servizi serverless AWS laddove possibile (ad esempio, Lambda, Firehose, Amazon S3 e Athena) per garantire un'elevata disponibilità e il ripristino in caso di guasto del servizio.
- Eseguiamo test automatici sulla soluzione per rilevare e correggere rapidamente gli errori.

- La soluzione utilizza le funzioni Lambda per l'elaborazione dei dati. La soluzione archivia i dati in Amazon S3 e DynamoDB e, per impostazione predefinita, persiste in più zone di disponibilità.

Efficienza delle prestazioni

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro prestazione-efficienza.

- La soluzione utilizza un'architettura serverless per garantire un'elevata scalabilità e disponibilità a un costo ridotto.
- La soluzione migliora le prestazioni del database partizionando i dati e ottimizzando le query per ridurre la quantità di dati da scansionare e ottenere risultati più rapidi.
- La soluzione viene testata e implementata automaticamente ogni giorno. I nostri architetti di soluzioni ed esperti in materia esaminano la soluzione per individuare le aree da sperimentare e migliorare.

Ottimizzazione dei costi

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'ottimizzazione dei costi.

- La soluzione utilizza un'architettura serverless e i clienti pagano solo per ciò che utilizzano.
- Il livello di calcolo della soluzione è impostato per impostazione predefinita su Lambda, che utilizza un modello. pay-per-use
- Il database e le query Athena sono ottimizzati per ridurre la quantità di scansione dei dati, riducendo così i costi.

Sostenibilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sostenibilità.

- La soluzione utilizza servizi gestiti e serverless per ridurre al minimo l'impatto ambientale dei servizi di backend.
- Il design serverless della soluzione mira a ridurre l'impronta di carbonio rispetto a quella dei server locali che operano continuamente.

Dettagli dell'architettura

Questa sezione descrive i componenti e i servizi AWS che compongono questa soluzione e i dettagli dell'architettura su come questi componenti interagiscono.

Servizi AWS in questa soluzione

Servizio AWS	Description
AWS WAF	Nucleo. Implementa un ACL web AWS WAF, gruppi di regole AWS Managed Rules, regole personalizzate e set IP. Effettua chiamate API AWS WAF per bloccare attacchi comuni e applicazioni Web sicure.
Amazon Data Firehose	Nucleo. Fornisce log AWS WAF ai bucket Amazon S3.
Amazon S3	Nucleo. Memorizza i log AWS WAF e ALB. CloudFront
AWS Lambda	Nucleo. Implementa più funzioni Lambda per supportare regole personalizzate.
Amazon EventBridge	Core. Crea regole di eventi per richiamare Lambda.
Amazon Athena	Supporto. Crea query e gruppi di lavoro Athena per supportare il parser di log Athena.
AWS Glue	Supporto. Crea database e tabelle per supportare il parser di log Athena.
Amazon SNS	Supporto. Invia notifiche e-mail di Amazon Simple Notification Service (Amazon SNS) per supportare la conservazione degli IP negli elenchi consentiti e negati.

Servizio AWS	Description
AWS Systems Manager	Supporto. Fornisce il monitoraggio delle risorse a livello di applicazione e la visualizzazione delle operazioni relative alle risorse e dei dati sui costi.

Opzioni del parser di registro

Come descritto nella panoramica dell'architettura, sono disponibili tre opzioni per gestire le protezioni HTTP flood e le protezioni da scanner e sonde. Le sezioni seguenti spiegano ognuna di queste opzioni in modo più dettagliato.

Regola basata sulla tariffa AWS WAF

Sono disponibili regole basate sulla tariffa per la protezione dalle inondazioni HTTP. Per impostazione predefinita, una regola basata sulla frequenza aggrega e limita la velocità delle richieste in base all'indirizzo IP della richiesta. Questa soluzione consente di specificare il numero di richieste Web consentite dall'IP di un client in un periodo finale di cinque minuti, aggiornato continuamente. Se un indirizzo IP viola la quota configurata, AWS WAF blocca le nuove richieste bloccate fino a quando la frequenza delle richieste non è inferiore alla quota configurata.

Ti consigliamo di selezionare l'opzione della regola basata sulla tariffa se la quota di richiesta è superiore a 2.000 richieste ogni cinque minuti e non è necessario implementare personalizzazioni. Ad esempio, non si considera l'accesso statico alle risorse nel conteggio delle richieste.

È possibile configurare ulteriormente la regola per utilizzare varie altre chiavi di aggregazione e combinazioni di tasti. Per ulteriori informazioni, consulta Opzioni e chiavi di aggregazione.

Analizzatore di log Amazon Athena

Entrambi i parametri del modello HTTP Flood Protection e Scanner & Probe Protection forniscono l'opzione Athena log parser. Se attivato, CloudFormation fornisce una query Athena e una funzione Lambda pianificata responsabile dell'orchestrazione di Athena per l'esecuzione, l'elaborazione dell'output dei risultati e l'aggiornamento di AWS WAF. Questa funzione Lambda viene richiamata da un CloudWatch evento configurato per essere eseguito ogni cinque minuti. Questo è configurabile con il parametro Athena Query Run Time Schedule.

Ti consigliamo di selezionare questa opzione quando non puoi utilizzare le regole basate sulla frequenza di AWS WAF e hai familiarità con SQL per implementare le personalizzazioni. Per ulteriori informazioni su come modificare la query predefinita, consulta Visualizza le query Amazon Athena.

La protezione dalle inondazioni HTTP si basa sull'elaborazione dei log di accesso AWS WAF e utilizza i file di registro WAF. Il tipo di log di accesso WAF ha un tempo di ritardo inferiore, che puoi utilizzare per identificare più rapidamente le origini del flood HTTP rispetto ai CloudFront nostri tempi di consegna dei log ALB. Tuttavia, è necessario selezionare il tipo di registro CloudFront o ALB nel parametro del modello Activate Scanner & Probe Protection per ricevere i codici di stato della risposta.

> **Note**
>
> Se un bot danneggiato aggira l'honeypot e interagisce direttamente con ALB or CloudFront, il sistema rileva un comportamento dannoso tramite l'analisi dei log, a meno che sia HTTP Flood Protection che Scanner & Probe Protection non utilizzino il parser di log Lambda.

Analizzatore di log AWS Lambda

I parametri del modello HTTP Flood Protection e Scanner & Probe Protection forniscono l'opzione AWS Lambda Log Parser. Utilizza il parser di log Lambda solo quando la regola basata sulla frequenza AWS WAF e le opzioni del parser di log di Amazon Athena non sono disponibili. Una limitazione nota di questa opzione è che le informazioni vengono elaborate nel contesto del file in fase di elaborazione. Ad esempio, un IP potrebbe generare più richieste o errori rispetto alla quota definita, ma poiché queste informazioni sono suddivise in diversi file, ogni file non memorizza dati sufficienti per superare la quota.

> **Note**
>
> Inoltre, se un bot malintenzionato aggira l'honeypot e interagisce direttamente con ALB or CloudFront, il rilevamento si basa sull'opzione di analisi dei log scelta per identificare e bloccare efficacemente le attività dannose.

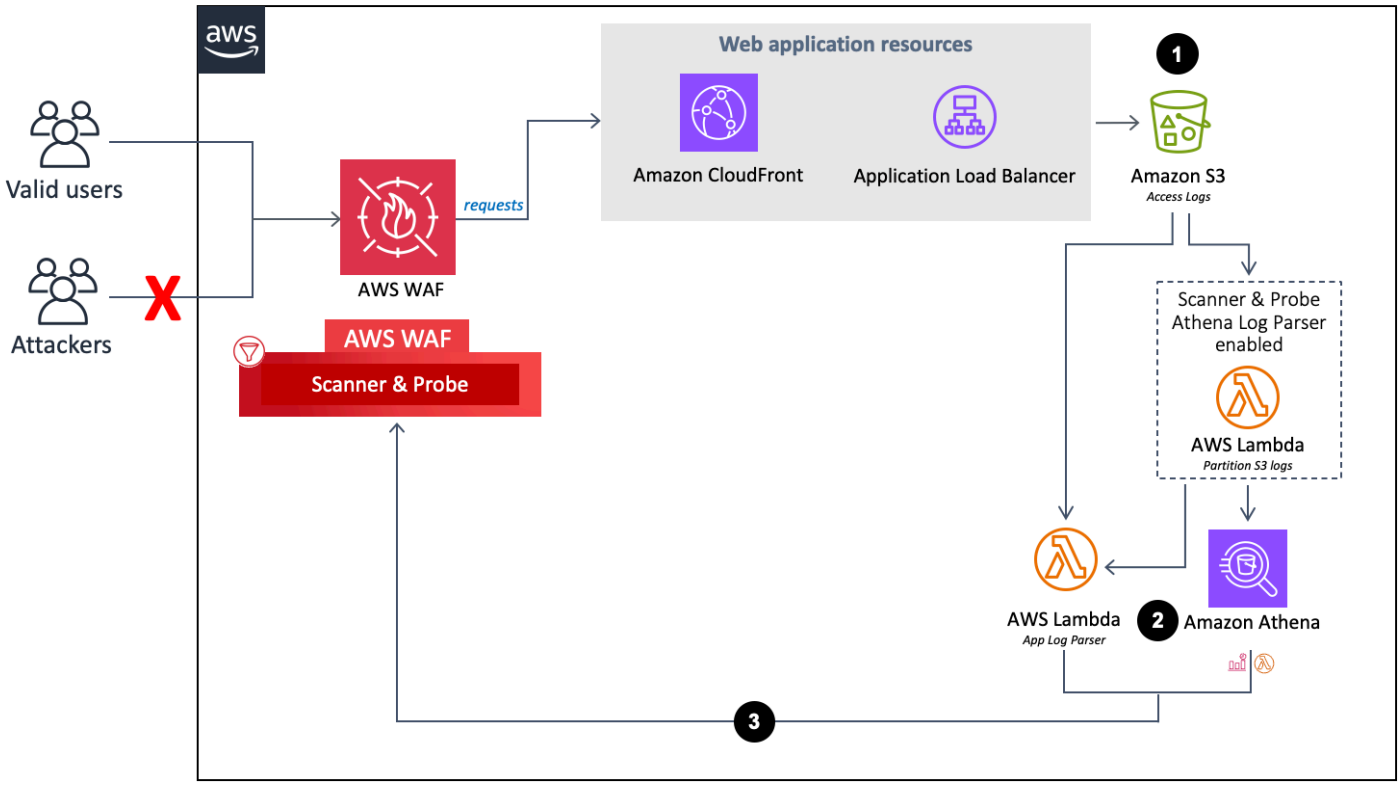
Dettagli dei componenti

Come descritto nel diagramma dell'architettura, quattro componenti di questa soluzione utilizzano automazioni per ispezionare gli indirizzi IP e aggiungerli alla lista di blocco di AWS WAF. Le seguenti sezioni spiegano ciascuno di questi componenti in modo più dettagliato.

Log parser - Applicazione

Il parser dei registri dell'applicazione aiuta a proteggere da scanner e sonde.

Flusso del parser del registro dell'applicazione.



1. Quando CloudFront un ALB riceve richieste per conto della tua applicazione Web, invia i log di accesso a un bucket Amazon S3.
   a. (Facoltativo) Se si seleziona `Yes - Amazon Athena log parser` per i parametri del modello Activate HTTP Flood Protection e Activate Scanner & Probe Protection, una funzione Lambda sposta i log di accesso dalla cartella originale *`<customer-bucket>`* `/AWSLogs` a una cartella appena partizionata/al *`<customer-bucket>`* `/AWSLogs-partitioned/` *`<optional-prefix>`* `/year=` *`<YYYY>`* `/month=` *`<MM>`* `/day=` *`<DD>`* `/hour=` *`<HH>`* loro arrivo in Amazon S3.

b. (Facoltativo) Se si seleziona `yes` il parametro del modello di posizione Keep Data in Original S3, i log rimangono nella posizione originale e vengono copiati nella cartella partizionata, duplicando lo spazio di archiviazione dei log.

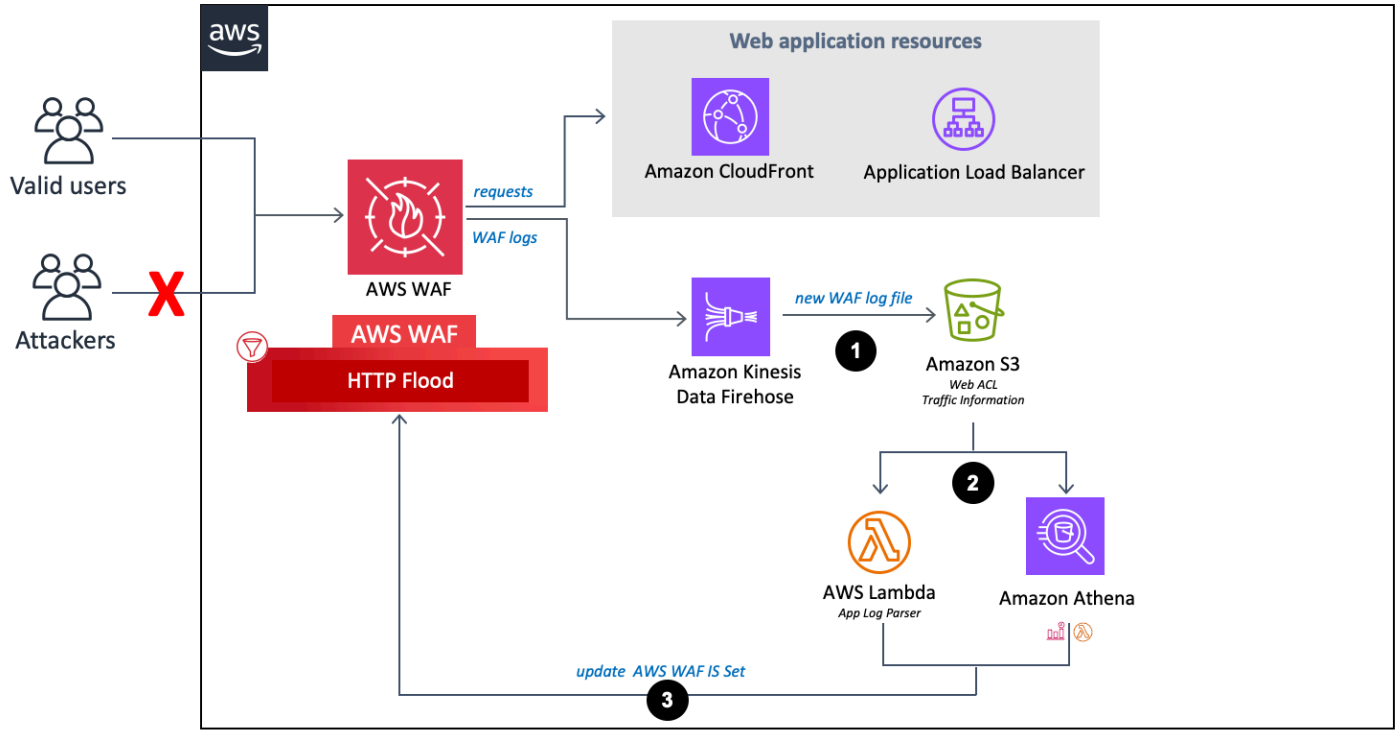
> **Note**
>
> Per il parser di log Athena, questa soluzione partiziona solo i nuovi log che arrivano nel bucket Amazon S3 dopo aver distribuito questa soluzione. Se disponi di log esistenti che desideri partizionare, devi caricarli manualmente su Amazon S3 dopo aver distribuito questa soluzione.

2. In base alla selezione dei parametri del modello Activate HTTP Flood Protection e Activate Scanner & Probe Protection, questa soluzione elabora i log utilizzando uno dei seguenti metodi:
   a. Lambda: ogni volta che un nuovo log di accesso viene archiviato nel bucket Amazon S3, viene avviata `Log Parser` la funzione Lambda.
   b. Athena - Per impostazione predefinita, ogni cinque minuti viene eseguita la query Athena di Scanner & Probe Protection e l'output viene inviato ad AWS WAF. Questo processo viene avviato da un CloudWatch evento che avvia la funzione Lambda responsabile dell'esecuzione della query Athena e invia il risultato in AWS WAF.
3. La soluzione analizza i dati di registro per identificare gli indirizzi IP che hanno generato più errori rispetto alla quota definita. La soluzione aggiorna quindi una condizione del set di IP AWS WAF per bloccare tali indirizzi IP per un periodo di tempo definito dal cliente.

Analizzatore di log - AWS WAF

Se selezioni `yes - AWS Lambda log parser` o `yes - Amazon Athena log parser` per Activate HTTP Flood Protection, questa soluzione fornisce i seguenti componenti, che analizzano i log di AWS WAF per identificare e bloccare le origini che inondano l'endpoint con una frequenza di richiesta superiore alla quota definita.

Flusso del parser di log AWS WAF.

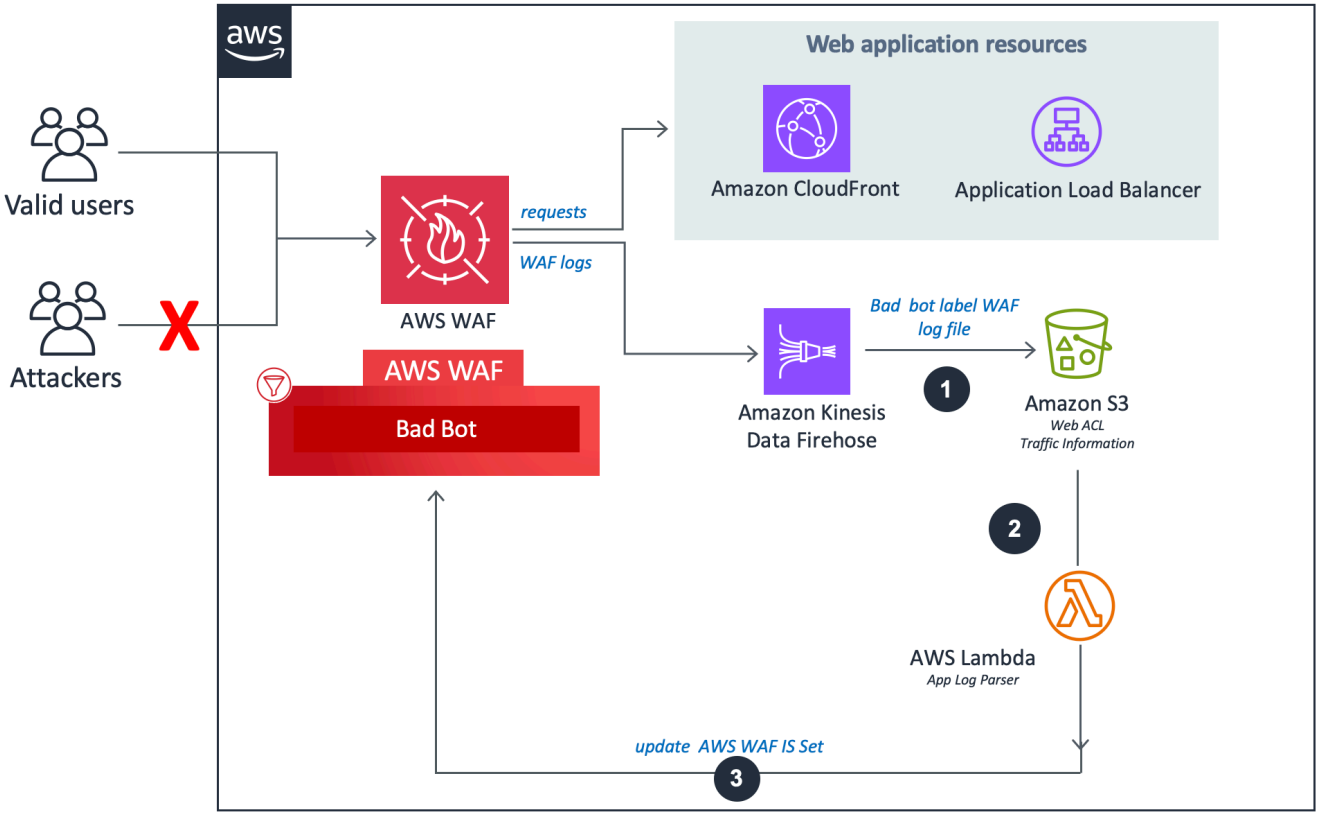


1. Quando AWS WAF riceve i log di accesso, li invia a un endpoint Firehose. Firehose invia quindi i log a un bucket partizionato in Amazon S3 denominato *<customer-bucket>* /AWSLogs/ *<optional-prefix>* /year= *<YYYY>* /month= *<MM>* /day= *<DD>* /hour= *<HH>* /
2. In base alla selezione effettuata per i parametri del modello Activate HTTP Flood Protection e Activate Scanner & Probe Protection, questa soluzione elabora i log utilizzando uno dei seguenti strumenti:
   a. Lambda: ogni volta che un nuovo log di accesso viene archiviato nel bucket Amazon S3, viene avviata `Log Parser` la funzione Lambda.
   b. Athena: per impostazione predefinita, ogni cinque minuti viene eseguita la query Athena dello scanner e della sonda e l'output viene inviato ad AWS WAF. Questo processo viene avviato da un CloudWatch evento Amazon, che avvia quindi la funzione Lambda responsabile dell'esecuzione della query Amazon Athena e invia il risultato in AWS WAF.
3. La soluzione analizza i dati di registro per identificare gli indirizzi IP che hanno inviato più richieste rispetto alla quota definita. La soluzione aggiorna quindi una condizione del set di IP AWS WAF per bloccare tali indirizzi IP per un periodo di tempo definito dal cliente.

Log parser - Bot non valido

Il parser di log Bad bot esamina le richieste all'endpoint honeypot per estrarne l'indirizzo IP di origine.

Flusso del parser del registro di avvio errato.

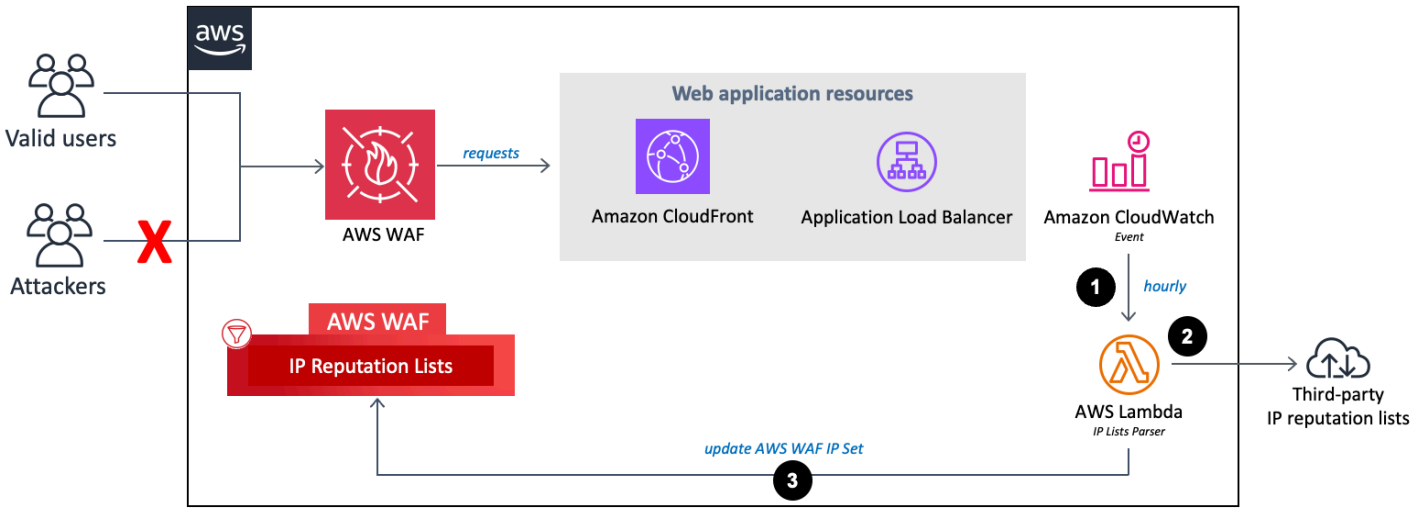


1. Se `Bad Bot Protection` è attivata e entrambe le funzionalità HTTP Flood Protection e Scanner & Probe Protection sono disabilitate: il sistema utilizzerà il parser Log Lambda, che registra solo le richieste bot non valide in base ai filtri di etichette WAF.
2. La funzione Lambda intercetta e ispeziona le intestazioni delle richieste per estrarre l'indirizzo IP della fonte che ha avuto accesso all'endpoint trap.
3. La soluzione analizza i dati di registro per identificare gli indirizzi IP che hanno inviato più richieste rispetto alla quota definita. La soluzione aggiorna quindi una condizione del set di IP AWS WAF per bloccare tali indirizzi IP per un periodo di tempo definito dal cliente.

Analizzatore di elenchi IP

La funzione `IP Lists Parser` Lambda aiuta a proteggere dagli aggressori noti identificati negli elenchi di reputazione IP di terze parti.

La reputazione IP elenca i flussi del parser.



1. Un CloudWatch evento Amazon ogni ora richiama la funzione `IP Lists Parser` Lambda.
2. La funzione Lambda raccoglie e analizza i dati da tre fonti:
   - Elenchi Spamhaus DROP e EDROP
   - Elenco IP Proofpoint Emerging Threats
   - Elenco dei nodi di uscita Tor
3. La funzione Lambda aggiorna l'elenco di blocchi di AWS WAF con gli indirizzi IP correnti.

Pianifica la tua implementazione

Questa sezione descrive i costi, la sicurezza, le quote e altre considerazioni prima di implementare la soluzione.

Regioni AWS supportate

A seconda dei valori dei parametri di input del modello definiti, questa soluzione richiede risorse diverse. Queste risorse (elencate nella tabella seguente) potrebbero non essere disponibili in tutte le regioni AWS. Pertanto, è necessario avviare questa soluzione in una regione AWS in cui questi servizi sono disponibili. Per la disponibilità più aggiornata dei servizi AWS per regione, consulta l'AWS Regional Services List.

	ACL Web AWS WAF	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Endpoint type (Tipo di endpoint)				
CloudFront	✓			
Application Load Balancer (ALB)	✓			
Attiva la protezione HTTP Flood				
sì - analizzatore di log AWS Lambda				✓
sì - Analizzatore di log Amazon Athena		✓	✓	✓

	ACL Web AWS WAF	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Attiva Scanner & Probe Protection				
sì - Analizzatore di log Amazon Athena		✓	✓	

> **Note**
>
> Se scegli `CloudFront` come endpoint, devi distribuire la soluzione nella regione Stati Uniti orientali (Virginia settentrionale) (). `us-east-1`

Costo

Sei responsabile del costo dei servizi AWS utilizzati durante l'esecuzione della soluzione Security Automations for AWS WAF. Il costo totale per l'esecuzione di questa soluzione dipende dalla protezione attivata e dalla quantità di dati acquisiti, archiviati ed elaborati.

Ti consigliamo di creare un budget tramite AWS Cost Explorer per gestire i costi. Per tutti i dettagli, consulta la pagina web dei prezzi per ogni servizio AWS utilizzato in questa soluzione.

Le tabelle seguenti sono esempi di suddivisione dei costi per l'esecuzione di questa soluzione nella regione Stati Uniti orientali (Virginia settentrionale) (escluso AWS Free Tier). I prezzi sono soggetti a modifiche.

Esempio 1: attivazione di Reputation List Protection, Bad Bot Protection, AWS Lambda Log Parser per HTTP Flood Protection e Scanner & Probe Protection

Servizio AWS	Dimensioni/mese	Costo [USD]
Amazon Data Firehose	100 GB	~$2,90
Simple Storage Service (Amazon S3)	100 GB	~2,30 $

Servizio AWS	Dimensioni/mese	Costo [USD]
AWS Lambda	128 MB: 3 funzioni, 1 milione di chiamate e una durata media di 500 millisecondi per esecuzione Lambda 512 MB: 2 funzioni, 1 milione di chiamate e una durata media di 500 millisecondi per esecuzione Lambda	~$5,40
ACL Web AWS WAF	1	$5,00
Regola AWS WAF	4	$4,00
Richiesta AWS WAF	1 milione	0,60 USD
Totale		~20,60 $ al mese

Esempio 2: attivazione di Reputation List Protection, Bad Bot Protection, Amazon Athena Log Parser per HTTP Flood Protection e Scanner & Probe Protection

Servizio AWS	Dimensioni/mese	Costo [USD]
Amazon Data Firehose	100 GB	~$2,90
Simple Storage Service (Amazon S3)	100 GB	~2,30 $
AWS Lambda	128 MB: 3 funzioni, 1 milione di chiamate e una durata media di 500 millisecondi per esecuzione Lambda 512 MB: 2 funzioni, 7560 chiamate e una durata	~$1,26

Servizio AWS	Dimensioni/mese	Costo [USD]
	media di 500 millisecondi per esecuzione Lambda	
Amazon Athena	1,2 milioni di accessi a CloudFront oggetti o 1,2 milioni di richieste ALB al giorno, con conseguente generazione di un record di log di ~500 byte per hit o richiesta	~$4,32
ACL Web AWS WAF	1	$5,00
Regola AWS WAF	4	$4,00
Richiesta AWS WAF	1 milione	0,60 USD
Totale		~20,38 $ al mese

Esempio 3: attivazione della conservazione degli IP per i set IP consentiti e negati

Servizio AWS	Dimensioni/mese	Costo [USD]
Amazon DynamoDB	1.000 scritture e 1 MB di spazio di archiviazione dati	~$0,00
AWS Lambda	128 MB: 1 funzione, 2.000 chiamate e durata media di 500 millisecondi per esecuzione Lambda 512 MB: 1 funzione, 2.000 chiamate e durata media di 500 millisecondi per esecuzione Lambda	~$0,01

Servizio AWS	Dimensioni/mese	Costo [USD]
Amazon CloudWatch	Eventi 2K	~$0,00
ACL Web AWS WAF	1	$5,00
Regola AWS WAF	2	$2,00
Richiesta WAS WAF	1 milione	$0,60
Totale		~7,61 $ al mese

Stima dei costi dei registri CloudWatch

Alcuni servizi AWS utilizzati in questa soluzione, come Lambda, generano CloudWatch log. Questi log sono a pagamento. Si consiglia di eliminare o archiviare i registri per ridurre i costi. Per informazioni dettagliate sull'archivio dei log, consulta Esportazione dei dati di log in Amazon S3 nella CloudWatch Amazon Logs User Guide.

Se scegli di utilizzare il parser di log Athena durante l'installazione, questa soluzione pianifica l'esecuzione di una query sui log di accesso AWS WAF o alle applicazioni nei tuoi bucket Amazon S3 in base alla configurazione. I costi vengono addebitati in base alla quantità di dati analizzati da ciascuna query. La soluzione applica il partizionamento a log e query per ridurre al minimo i costi. Per impostazione predefinita, la soluzione sposta i log di accesso alle applicazioni dalla posizione originale di Amazon S3 a una struttura di cartelle partizionata. Puoi anche conservare l'originale, ma ti verrà addebitato un costo per l'archiviazione duplicata dei log. Questa soluzione utilizza gruppi di lavoro per segmentare i carichi di lavoro ed è possibile configurarli entrambi per gestire l'accesso alle query e i costi. Per un esempio di calcolo della stima dei costi, fare riferimento a Stima dei costi di Athena. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon Athena.

Stima dei costi di Athena

Se utilizzi l'opzione Athena log parser mentre esegui le regole HTTP Flood Protection, Scanner & Probe Protection o Bad Bot Protection, ti verrà addebitato l'utilizzo di Athena. Per impostazione predefinita, ogni query Athena viene eseguita ogni cinque minuti e analizza i dati delle ultime quattro ore. La soluzione applica il partizionamento ai log e alle query Athena per ridurre al minimo i costi. È possibile configurare il numero di ore di dati analizzate da una query modificando il valore del

parametro del modello WAF Block Period. Tuttavia, l'aumento della quantità di dati scansionati probabilmente aumenterà il costo di Athena.

> **Tip**
>
> Di seguito è riportato un esempio di calcolo del costo CloudFront dei log:
> In media, ogni CloudFront hit può generare circa 500 byte di dati.
> Se ogni giorno vengono visitati 1,2 milioni di CloudFront oggetti, si verificheranno 200.000 accessi (1,2 M/6) ogni quattro ore, supponendo che i dati vengano acquisiti a una velocità costante. Considerate i vostri modelli di traffico effettivi quando calcolate i costi.
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena addebita 5,00 USD per TB di dati scansionati.
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> La query Athena viene eseguita ogni cinque minuti, ovvero 12 esecuzioni all'ora.
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`
> I costi effettivi variano a seconda dei modelli di traffico dell'applicazione. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon Athena.

Sicurezza

Quando crei sistemi sull'infrastruttura AWS, le responsabilità di sicurezza vengono condivise tra te e AWS. Questo modello di responsabilità condivisa riduce il carico operativo perché AWS gestisce, gestisce e controlla i componenti, tra cui il sistema operativo host, il livello di virtualizzazione e la sicurezza fisica delle strutture in cui operano i servizi. Per ulteriori informazioni sulla sicurezza di AWS, visita AWS Cloud Security.

Ruoli IAM

Con i ruoli IAM, puoi assegnare accesso, policy e autorizzazioni granulari a servizi e utenti sul cloud AWS. Questa soluzione crea ruoli IAM con privilegi minimi e questi ruoli garantiscono alle risorse della soluzione le autorizzazioni necessarie.

Dati

Tutti i dati archiviati nei bucket Amazon S3 e nelle tabelle DynamoDB sono crittografati a riposo. Anche i dati in transito con Firehose sono crittografati.

Funzionalità di protezione

Le applicazioni Web sono vulnerabili a una varietà di attacchi. Questi attacchi includono richieste appositamente predisposte per sfruttare una vulnerabilità o assumere il controllo di un server, attacchi volumetrici progettati per disattivare un sito Web o bot e scraper dannosi programmati per acquisire e rubare contenuti Web.

Questa soluzione utilizza CloudFormation la configurazione delle regole AWS WAF, inclusi i gruppi di regole AWS Managed Rules e le regole personalizzate, per bloccare i seguenti attacchi comuni:

- AWS Managed Rules: questo servizio gestito fornisce protezione contro le vulnerabilità comuni delle applicazioni o altro traffico indesiderato. Questa soluzione include gruppi di regole di reputazione AWS Managed IP, gruppi di regole di base AWS Managed e gruppi di regole AWS Managed specifici per casi d'uso. Hai la possibilità di selezionare uno o più gruppi di regole per il tuo ACL web, fino alla quota massima di unità di capacità Web ACL (WCU).
- SQL injection: gli aggressori inseriscono codice SQL dannoso nelle richieste Web per estrarre dati dal database. Abbiamo progettato questa soluzione per bloccare le richieste web che contengono codice SQL potenzialmente dannoso.
- XSS - Gli aggressori sfruttano le vulnerabilità di un sito Web innocuo come veicolo per iniettare script dannosi del sito client nel browser Web di un utente legittimo. L'abbiamo progettato per esaminare gli elementi più comuni delle richieste in arrivo per identificare e bloccare gli attacchi XSS.
- Inondazioni HTTP: i server Web e altre risorse di backend sono a rischio di attacchi DDo S, come i flood HTTP. Questa soluzione richiama automaticamente una regola basata sulla velocità quando le richieste Web da un client superano una quota configurabile. In alternativa, puoi applicare questa quota elaborando i log di AWS WAF utilizzando una funzione Lambda o una query Athena.
- Scanner e sonde: fonti dannose scansionano e controllano le vulnerabilità delle applicazioni Web con accesso a Internet, inviando una serie di richieste che generano codici di errore HTTP 4xx. È possibile utilizzare questa cronologia per identificare e bloccare gli indirizzi IP di origine dannosi. Questa soluzione crea una funzione Lambda CloudFront o una query Athena che analizza automaticamente i log di accesso ALB, conta il numero di richieste errate provenienti da indirizzi IP

di origine univoci al minuto e aggiorna AWS WAF per bloccare ulteriori scansioni da indirizzi che hanno raggiunto la quota di errore definita.

- Origini note degli aggressori (elenchi di reputazione IP): molte organizzazioni mantengono elenchi di reputazione degli indirizzi IP gestiti da aggressori noti, come spammer, distributori di malware e botnet. Questa soluzione sfrutta le informazioni contenute in questi elenchi di reputazione per aiutarti a bloccare le richieste provenienti da indirizzi IP dannosi. Inoltre, questa soluzione blocca gli aggressori identificati da gruppi di regole di reputazione IP basati sull'intelligence interna delle minacce di Amazon.
- Bot e scraper: gli operatori di applicazioni Web accessibili al pubblico devono avere la certezza che i clienti che accedono ai loro contenuti si identifichino con precisione e utilizzino i servizi come previsto. Tuttavia, alcuni client automatizzati, come gli scraper di contenuti o i bot pericolosi, si presentano in modo errato per aggirare le restrizioni. Questa soluzione consente di identificare e bloccare bot e scraper dannosi.

Quote

Le quote di servizio, anche denominate limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l'account AWS.

Quote per i servizi AWS in questa soluzione

Assicurati di disporre di una quota sufficiente per ciascuno dei servizi implementati in questa soluzione. Per ulteriori informazioni, consulta le quote dei servizi AWS. Per visualizzare le quote di servizio per tutti i servizi AWS nella documentazione senza cambiare pagina, visualizza invece le informazioni nella pagina Endpoint e quote del servizio nel PDF.

Quote AWS WAF

AWS WAF può bloccare un massimo di 10.000 intervalli di indirizzi IP in notazione CIDR (Classless Inter-Domain Routing) per condizione di corrispondenza IP. Ogni elenco creato da questa soluzione è soggetto a questa quota. Per ulteriori informazioni, consulta le quote AWS WAF. A partire dalla versione 3.0, questa soluzione crea due set IP da allegare a ciascuna regola, uno per IPv4 e uno per. IPv6

AWS WAF consente un massimo di una richiesta al secondo, per account, per regione AWS per chiamate API a qualsiasi individuo `Create` o `Update` azione. `Put` Se effettui queste chiamate API al di fuori della soluzione, potresti riscontrare un problema di limitazione delle API. Per evitare il

problema, ti consigliamo di evitare di eseguire altre applicazioni che effettuano queste chiamate API nello stesso account e nella stessa regione in cui è implementata questa soluzione.

Considerazioni sull'implementazione

Le seguenti sezioni forniscono vincoli e considerazioni per l'implementazione di questa soluzione.

Regole AWS WAF

L'ACL Web generato da questa soluzione è progettato per offrire una protezione completa per le applicazioni Web. La soluzione fornisce un set di AWS Managed Rules e regole personalizzate che puoi aggiungere all'ACL Web. Per includere una regola, scegli `yes` i parametri pertinenti all'avvio dello CloudFormation stack. Vedi Fase 1. Avvia lo stack per l'elenco dei parametri.

> **Note**
>
> La out-of-box soluzione non supporta AWS Firewall Manager. Se desideri utilizzare le regole di Firewall Manager, ti consigliamo di applicare personalizzazioni al relativo codice sorgente.

Registrazione del traffico Web ACL

Se crei lo stack in una regione AWS diversa dagli Stati Uniti orientali (Virginia settentrionale) e imposti l'endpoint come`CloudFront`, devi impostare Activate HTTP Flood Protection su o. no `yes - AWS WAF rate based rule`

Le altre due opzioni (`yes - AWS Lambda log parser`e`yes - Amazon Athena log parser`) richiedono l'attivazione dei log AWS WAF su un ACL Web che viene eseguito in tutte le edge location AWS, e questa operazione non è supportata al di fuori degli Stati Uniti orientali (Virginia settentrionale). Per ulteriori informazioni sulla registrazione del traffico Web ACL, consulta la guida per sviluppatori AWS WAF.

Gestione sovradimensionata dei componenti della richiesta

AWS WAF non supporta l'ispezione di contenuti di grandi dimensioni per il corpo, le intestazioni o i cookie del componente di richiesta Web. Quando scrivi una dichiarazione di regola che esamina uno di questi tipi di componenti di richiesta, puoi scegliere una di queste opzioni per dire ad AWS WAF cosa fare con queste richieste:

- `yes`(continua) - Ispeziona normalmente il componente della richiesta in base ai criteri di ispezione delle regole. AWS WAF ispeziona i contenuti dei componenti della richiesta che rientrano nei limiti di dimensione. Questa è l'opzione predefinita utilizzata nella soluzione.
- `yes - MATCH`: considera la richiesta Web come corrispondente all'istruzione regola. AWS WAF applica l'azione della regola alla richiesta senza valutarla rispetto ai criteri di ispezione della regola. Per una regola con `Block` azione, questo blocca la richiesta con il componente sovradimensionato.
- `yes - NO_MATCH`- Considera la richiesta web come se non corrispondesse alla dichiarazione della regola, senza valutarla rispetto ai criteri di ispezione della regola. AWS WAF continua l'ispezione della richiesta Web utilizzando il resto delle regole nell'ACL Web, come farebbe per qualsiasi regola non corrispondente.

Per ulteriori informazioni, consulta Gestione di componenti di richieste Web di grandi dimensioni in AWS WAF.

Implementazioni di più soluzioni

È possibile distribuire la soluzione più volte nello stesso account e nella stessa regione. È necessario utilizzare un nome CloudFormation stack univoco e un nome di bucket Amazon S3 per ogni distribuzione. Ogni implementazione unica comporta costi aggiuntivi ed è soggetta alle quote AWS WAF per account e per regione.

Autorizzazioni minime di ruolo per la distribuzione (facoltative)

I clienti possono creare manualmente un ruolo IAM con le autorizzazioni minime richieste per la distribuzione:

- Autorizzazioni WAF

```
        {
            "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/*"
            ]
        }
```

- Autorizzazioni Lambda

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

- Autorizzazioni Firehose

```
        {
            "Effect": "Allow",
```

```
            "Action": [
                "firehose:CreateDeliveryStream",
                "firehose:DeleteDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "firehose:StartDeliveryStreamEncryption",
                "firehose:StopDeliveryStreamEncryption",
                "firehose:UpdateDestination"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*"
        }
```

- Autorizzazioni S3

```
        {
            "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:::*"
        }
```

- Autorizzazioni Athena

```
        {
            "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*"
        }
```

- Autorizzazioni Glue

```
        {
            "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 Registra le autorizzazioni

```
        {
            "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 Autorizzazioni

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

- Autorizzazioni SNS

```
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:Subscribe",
```

```
            "sns:Unsubscribe",
            "sns:SetTopicAttributes"
        ],
        "Resource": "arn:aws:sns:*:*:*"
    }
```

- Autorizzazioni DynamoDB

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

- CloudFormation Autorizzazioni

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

- Autorizzazioni del registro dell'app Service Catalog

```
    {
```

```
            "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:*:*:*"
        }
```

- Autorizzazioni X-Ray

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

- Autorizzazioni IAM

```
        {
            "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 Autorizzazioni

```
        {
            "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/*"
        }
```

Implementa la soluzione

Questa soluzione utilizza CloudFormation modelli e stack AWS per automatizzarne l'implementazione. I CloudFormation modelli specificano le risorse AWS incluse in questa soluzione e le relative proprietà. Lo CloudFormation stack fornisce le risorse descritte nei modelli.

Panoramica del processo di distribuzione

Prima di avviare il CloudFormation modello, esamina le considerazioni sull'architettura e sulla configurazione discusse in questa guida. Segui le step-by-step istruzioni in questa sezione per configurare e distribuire la soluzione nel tuo account.

Tempo di implementazione: circa 15 minuti.

> **Note**
>
> Se hai già distribuito questa soluzione, consulta Aggiornare la soluzione per le istruzioni di aggiornamento.

Prerequisiti

- Configurare una distribuzione CloudFront
- Configurare un ALB

Fase 1: Avvia lo stack

- Avvia il CloudFormation modello nel tuo account AWS.
- Inserisci i valori per i parametri richiesti: Stack Name e Application Access Log Bucket Name.
- Rivedete gli altri parametri del modello e modificateli se necessario.

Fase 2. Associa l'ACL Web alla tua applicazione Web

- Associate le vostre distribuzioni CloudFront Web o ALB all'ACL Web generato da questa soluzione. Puoi associare tutte le distribuzioni o i sistemi di bilanciamento del carico che desideri.

Fase 3. Configura la registrazione degli accessi al Web

- Attiva la registrazione degli accessi CloudFront Web per le tue distribuzioni Web o ALB e invia i file di registro al bucket Amazon S3 appropriato. Salva i log in una cartella corrispondente al prefisso definito dall'utente. Se non viene utilizzato alcun prefisso definito dall'utente, salva i log in (prefisso di registro predefinito). AWSLogs `AWSLogs/` Vedi il parametro Application Access Log Bucket Prefix nel passaggio 1. Avvia lo stack per ulteriori informazioni.

CloudFormation Modelli AWS

Questa soluzione include un CloudFormation modello AWS principale e due modelli annidati. Puoi scaricare i CloudFormation modelli prima di distribuire la soluzione.

Stack principale

aws-waf-security-automations.template: utilizza questo modello come punto di accesso per avviare la soluzione nel tuo account. La configurazione predefinita implementa un ACL web AWS WAF con regole preconfigurate. Puoi personalizzare il modello in base alle tue esigenze.

Stack WebACL

aws-waf-security-automations-webacl.template: questo modello annidato fornisce risorse AWS WAF tra cui un ACL Web, un IP, set e altre risorse associate.

Pila Firehose Athena

aws-waf-security-automations-firehose-athena.template: questo modello annidato fornisce risorse relative a AWS Glue, Athena e Firehose. Viene creato quando si sceglie il parser di log Scanner & Probe Athena o il parser di log HTTP Flood Lambda o Athena.

> **Note**
>
> Le CloudFormation risorse AWS vengono create a partire da costrutti di AWS Cloud Development Kit (AWS CDK).

Questo CloudFormation modello AWS distribuisce la soluzione Security Automations for AWS WAF nel cloud AWS.

Prerequisiti

Questa soluzione è progettata per funzionare con applicazioni Web distribuite con CloudFront o un ALB. Se non hai già configurato una di queste risorse, completa le attività applicabili prima di avviare questa soluzione.

Configura una CloudFront distribuzione

Completa i seguenti passaggi per configurare una CloudFront distribuzione per il contenuto statico e dinamico dell'applicazione Web. Consulta l'Amazon CloudFront Developer Guide per istruzioni dettagliate.

1. Crea una distribuzione di applicazioni CloudFront Web. Fare riferimento a Creazione di una distribuzione.
2. Configura origini statiche e dinamiche. Fare riferimento a Utilizzo di origini diverse con le CloudFront distribuzioni.
3. Specificate il comportamento della vostra distribuzione. Fai riferimento ai valori che specifichi quando crei o aggiorni una distribuzione.

   > **Note**
   >
   > Se scegli `CloudFront` come endpoint, devi creare WAFV2 le tue risorse nella regione Stati Uniti orientali (Virginia settentrionale).

Configura un ALB

Per configurare un ALB per distribuire il traffico in entrata verso la tua applicazione web, consulta Create an Application Load Balancer nella User Guide for Application Load Balancers.

Fase 1: Avvio dello stack

Questo CloudFormation modello AWS automatizzato distribuisce la soluzione sul cloud AWS.

1. Accedi alla Console di gestione AWS e seleziona il `waf-automation-on-aws.template` CloudFormation modello Launch Solution per avviare.

2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in un'altra regione AWS, utilizza il selettore della regione nella barra di navigazione della console. Se scegli `CloudFront` come endpoint, devi distribuire la soluzione nella regione Stati Uniti orientali (Virginia settentrionale) (). `us-east-1`

> **Note**
>
> A seconda dei valori dei parametri di input definiti, questa soluzione richiede risorse diverse. Queste risorse sono attualmente disponibili solo in regioni AWS specifiche. Pertanto, è necessario avviare questa soluzione in una regione AWS in cui questi servizi sono disponibili. Per ulteriori informazioni, consulta la sezione Regioni AWS supportate.

3. Nella pagina Specificare il modello, verifica di aver selezionato il modello corretto e scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome alla configurazione AWS WAF nel campo Stack name. Questo è anche il nome dell'ACL web creato dal modello.
5. In Parametri, esaminate i parametri del modello e modificateli se necessario. Per disattivare una particolare funzionalità, scegli none ono, se applicabile. Questa soluzione utilizza i seguenti valori predefiniti.

Parametro	Predefinito	Descrizione
Stack name (Nome stack)	`[.red]#<requires input>``	Il nome dello stack non può contenere spazi. Questo nome deve essere univoco all'interno del tuo account AWS ed è il nome dell'ACL web creato dal modello.

Parametro	Predefinito	Descrizione
Tipo di risorsa		
Endpoint	`CloudFront`	Scegli il tipo di risorsa da utilizzare. NOTA: se scegli `CloudFront` come endpoint, devi avviare la soluzione per creare risorse WAF nella regione Stati Uniti orientali (Virginia settentrionale) (). `us-east-1`
Gruppi di regole di reputazione IP gestita da AWS		

Parametro	Predefinito	Descrizione
Attiva Amazon IP Reputation List Managed Rule Group Protection	no	Scegli `yes` di attivare il componente progettato per aggiungere Amazon IP Reputation List Managed Rule Group all'ACL Web. Questo gruppo di regole si basa sull'intelligence interna delle minacce di Amazon. Ciò è utile se desideri bloccare gli indirizzi IP generalmente associati a bot o altre minacce. Il blocco di questi indirizzi IP consente di mitigare i bot e ridurre il rischio che un utente malintenzionato scopra un'applicazione vulnerabile. La WCU richiesta è 25. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuzione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi di regole di AWS Managed Rules.

Parametro	Predefinito	Descrizione
Attiva la protezione dei gruppi di regole gestite con elenco di IP anonimi	no	Scegli `yes` di attivare il componente progettato per aggiungere Anonymous IP List Managed Rule Group all'ACL web. Questo gruppo di regole blocca le richieste provenien ti da servizi che consenton o l'offuscamento dell'iden tità dello spettatore. Questi includono richieste provenien ti da proxy VPNs, nodi Tor e provider di hosting. Questo gruppo di regole è utile se si desidera filtrare i visualizz atori che potrebbero tentare di nascondere la propria identità dall'applicazione. Bloccare gli indirizzi IP di questi servizi può aiutare a mitigare i bot e l'evasione delle restrizioni geografiche. La WCU richiesta è 50. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuz ione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi

Parametro	Predefinito	Descrizione
		di regole di AWS Managed Rules.
Gruppi di regole AWS Managed Baseline		
Attiva Core Rule Set Managed Rule Group Protection	no	Scegli `yes` di attivare il componente progettato per aggiungere Core Rule Set Managed Rule Group all'ACL web. Questo gruppo di regole fornisce protezione contro lo sfruttamento di un'ampia gamma di vulnerabilità, incluse alcune delle vulnerabilità ad alto rischio e più comuni. Prendi in considerazione l'utilizzo di questo gruppo di regole per qualsiasi caso d'uso di AWS WAF. La WCU richiesta è 700. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuzione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi di regole di AWS Managed Rules.

Parametro	Predefinito	Descrizione
Attiva Admin Protection Managed Rule Group Protection	no	Scegli `yes` di attivare il componente progettato per aggiungere Admin Protection Managed Rule Group all'ACL web. Questo gruppo di regole blocca l'accesso esterno alle pagine amministrative esposte. Ciò potrebbe essere utile se esegui software di terza parte o se desideri ridurre il rischio che un utente malintenzionato ottenga l'accesso amministrativo all'applicazione. La WCU richiesta è 100. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuzione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi di regole di AWS Managed Rules.

Parametro	Predefinito	Descrizione
Attiva la protezione dei gruppi di regole gestite da Known Bad Input	no	Scegli `yes` di attivare il componente progettato per aggiungere Known Bad Inputs Managed Rule Group all'ACL web. Questo gruppo di regole blocca l'accesso esterno alle pagine amministrative esposte. Ciò potrebbe essere utile se esegui software di terza parte o se desideri ridurre il rischio che un utente malintenzionato ottenga l'accesso amministrativo all'applicazione. La WCU richiesta è 100. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuz ione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi di regole di AWS Managed Rules.
Gruppo di regole AWS Managed Use-Case specifico		

Parametro	Predefinito	Descrizione
Attiva la protezione dei gruppi di regole gestite del database SQL	no	Scegli `yes` di attivare il componente progettato per aggiungere SQL Database Managed Rule Group all'ACL Web. Questo gruppo di regole blocca i modelli di richiesta associati allo sfruttamento dei database SQL, come gli attacchi SQL injection . Ciò impedisce l'iniezione remota di query non autorizza te. Valuta l'uso di questo gruppo di regole se l'applica zione si interfaccia con un database SQL. L'utilizzo della regola personalizzata di SQL injection è facoltativo se hai già attivato il gruppo di regole SQL gestito da AWS. La WCU richiesta è 200. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuz ione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi di regole di AWS Managed Rules.

Parametro	Predefinito	Descrizione
Attiva la protezione dei gruppi di regole gestite dal sistema operativo Linux	no	Scegli `yes` di attivare il componente progettato per aggiungere Linux Operating System Managed Rule Group all'ACL web. Questo gruppo di regole blocca i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche di Linux, inclusi gli attacchi LFI (Local File Inclusion) specifici per Linux. Questo può aiutare a prevenire attacchi che espongono il contenuto dei file o eseguono codice a cui l'autore dell'attacco non avrebbe dovuto avere accesso. Valuta questo gruppo di regole se una parte dell'applicazione viene eseguita su Linux. È necessario utilizzare questo gruppo di regole insieme al gruppo di regole del sistema operativo POSIX. La WCU richiesta è 200. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuzione dello stack Web ACL dovuti al superamento del limite di capacità.

Parametro	Predefinito	Descrizione
		Per ulteriori informazioni, consulta l'elenco dei gruppi di regole di AWS Managed Rules.

Parametro	Predefinito	Descrizione
Attiva la protezione dei gruppi di regole gestite dal sistema operativo POSIX	no	Scegli `yes` di attivare il componente progettato per aggiungere Core Rule Set Managed Rule Group Protection all'ACL web. Questo gruppo di regole blocca i modelli di richiesta associati allo sfruttamento delle vulnerabilità specifiche dei sistemi operativi POSIX e simili a POSIX, inclusi gli attacchi LFI. Questo può aiutare a prevenire attacchi che espongono il contenuto dei file o eseguono codice a cui l'utente malintenzionato non avrebbe dovuto avere accesso. Valuta questo gruppo di regole se una parte dell'applicazione viene eseguita su un sistema operativo POSIX o simile a POSIX. La WCU richiesta è 100. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuzione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi

Parametro	Predefinito	Descrizione
		di regole di AWS Managed Rules.

Parametro	Predefinito	Descrizione
Attiva la protezione dei gruppi di regole gestite dal sistema operativo Windows	no	Scegli `yes` di attivare il componente progettato per aggiungere Windows Operating System Managed Rule Group all'ACL Web. Questo gruppo di regole blocca i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche di Windows, come l'esecuzi one remota di PowerShell comandi. Questo può aiutare a prevenire lo sfruttamento di vulnerabilità che consenton o a un utente malintenz ionato di eseguire comandi non autorizzati o eseguire codice dannoso. Valuta questo gruppo di regole se una parte dell'applicazione viene eseguita su un sistema operativo Windows. La WCU richiesta è 200. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuz ione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi

Parametro	Predefinito	Descrizione
		di regole di AWS Managed Rules.

Parametro	Predefinito	Descrizione
Attiva PHP Application Managed Rule Group Protection	no	Scegli `yes` di attivare il componente progettato per aggiungere PHP Application Managed Rule Group all'ACL web. Questo gruppo di regole blocca i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche all'uso del linguaggio di programma zione PHP, inclusa l'iniezio ne di funzioni PHP non sicure. Questo può aiutare a prevenire lo sfruttamento di vulnerabilità che consentono a un utente malintenzionato di eseguire in remoto codice o comandi per i quali non è autorizzato. Valuta questo gruppo di regole se PHP è installato su qualsiasi server che si interfaccia con l'applica zione. La WCU richiesta è 100. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuz ione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi

Parametro	Predefinito	Descrizione
		di regole di AWS Managed Rules.
Attiva WordPress Application Managed Rule Group Protection	no	Scegli `yes` di attivare il componente progettato per aggiungere WordPress Application Managed Rule Group all'ACL web. Questo gruppo di regole blocca i modelli di richiesta associati allo sfruttamento di vulnerabilità specifiche dei siti. WordPress Valuta questo gruppo di regole se stai correndo WordPress . Questo gruppo di regole deve essere usato insieme al database SQL e ai gruppi di regole delle applicazioni PHP. La WCU richiesta è 100. L'account deve disporre di una capacità WCU sufficiente per evitare errori di distribuzione dello stack Web ACL dovuti al superamento del limite di capacità. Per ulteriori informazioni, consulta l'elenco dei gruppi di regole di AWS Managed Rules.
Regola personalizzata: Scanner & Probes		

Parametro	Predefinito	Descrizione
Attiva la protezione di scanner e sonde	`yes - AWS Lambda log parser`	Scegli il componente utilizzato per bloccare scanner e sonde. Fate riferimento alle opzioni del parser di log per ulteriori informazioni sui compromessi relativi alle opzioni di mitigazione.

Parametro	Predefinito	Descrizione
Nome del bucket del log di accesso all'applicazione	`[.red]<requires input>`	Se hai scelto `yes` il parametro Activate Scanner & Probe Protection, inserisci il nome del bucket Amazon S3 (nuovo o esistente) in cui desideri archiviare i log di accesso per CloudFront le tue distribuzioni o ALB. Se utilizzi un bucket Amazon S3 esistente, deve trovarsi nella stessa regione AWS in cui stai distribuendo il modello. CloudFormation È necessari o utilizzare un bucket diverso per ogni implementazione della soluzione. Per disattivare questa protezione, ignora questo parametro. NOTA: attiva la registrazione degli accessi CloudFront Web per le tue distribuzioni Web o ALB per inviare file di registro a questo bucket Amazon S3. Salva i log con lo stesso prefisso definito nello stack (prefisso predefinito). `AWSLogs/` Per ulteriori informazioni, vedere il parametro Application Access Log Bucket Prefix.

Parametro	Predefinito	Descrizione
Prefisso Application Access Log Bucket	`AWSLogs/`	Se avete scelto `yes` il parametro Activate Scanner & Probe Protection, potete inserire un prefisso opzionale definito dall'utente per il bucket dei log di accesso alle applicazioni riportato sopra. Se avete scelto `CloudFront` il parametro Endpoint, potete inserire qualsiasi prefisso come. `yourprefix/` Se hai scelto `ALB` il parametro Endpoint, devi aggiungere `AWSLogs/` al prefisso come. `yourprefix/AWSLogs/` Utilizza `AWSLogs/` (impostazione predefinita) se non esiste un prefisso definito dall'utente. Per disattivare questa protezione, ignora questo parametro.

Parametro	Predefinito	Descrizione
La registrazione degli accessi al bucket è attivata?	no	Scegli `yes` se hai inserito un nome di bucket Amazon S3 esistente per il parametro Application Access Log Bucket Name e la registrazione degli accessi al server per il bucket è già attiva. Se lo desiderino, la soluzione attiva la registrazione degli accessi al server per il tuo bucket. Se avete scelto no il parametro Activate Scanner & Probe Protection, ignorate questo parametro.
Soglia di errore	`50`	Se hai scelto `yes` il parametro Activate Scanner & Probe Protection, inserisci il numero massimo di richieste errate accettabili al minuto, per indirizzo IP. Se avete scelto no il parametro Activate Scanner & Probe Protection, ignorate questo parametro.

Parametro	Predefinito	Descrizione
Conserva i dati nella posizione originale di S3	no	Se si è scelto `yes - Amazon Athena log parser` il parametro Activate Scanner & Probe Protectio n, la soluzione applica il partizionamento ai file di registro degli accessi alle applicazioni e alle query Athena. Per impostazione predefinita, la soluzione sposta i file di log dalla loro posizione originale a una struttura di cartelle partizion ata in Amazon S3. Scegli `yes` se conservare anche una copia dei log nella loro posizione originale. Ciò duplicherà l'archiviazione dei registri. Se non hai scelto `yes - Amazon Athena log parser` il parametro Activate Scanner & Probe Protection, ignora questo parametro.
Regola personalizzata: HTTP Flood		

Parametro	Predefinito	Descrizione
Attiva la protezione HTTP Flood	`yes - AWS WAF rate-based rule`	Seleziona il componente utilizzato per bloccare gli attacchi HTTP Flood. Fai riferimento alle opzioni del parser di log per ulteriori informazioni sui compromessi relativi alle opzioni di mitigazione.
Soglia di richiesta predefinita	`100`	Se hai scelto `yes` il parametro Activate HTTP Flood Protection, inserisci il numero massimo di richieste accettabili per cinque minuti, per indirizzo IP. Se avete scelto `yes - AWS WAF rate-based rule` il parametro Activate HTTP Flood Protection, il valore minimo accettabile è. `10` Se hai scelto `yes - AWS Lambda log parser` o `yes - Amazon Athena log parser` per il parametro Activate HTTP Flood Protection, può avere qualsiasi valore. Per disattivare questa protezione, ignora questo parametro.

Parametro	Predefinito	Descrizione
Soglia di richiesta per Paese	<optional input>	Se hai scelto `yes - Amazon Athena log parser` il parametro Activate HTTP Flood Protection, puoi inserire una soglia per paese seguendo questo formato JSON. `{"TR":50, "ER":150}` La soluzione utilizza queste soglie per le richieste provenienti dai paesi specificati. La soluzione utilizza il parametro Default Request Threshold per le richieste rimanenti. NOTA: se si definisce questo parametro, il paese verrà automaticamente incluso nel gruppo di query Athena, insieme all'IP e ad altri campi facoltativi raggruppati per che è possibile seleziona re con il parametro Group By Requests in HTTP Flood Athena Query. + Se hai scelto di disattivare questa protezione, ignora questo parametro.

Parametro	Predefinito	Descrizione
Raggruppa per richieste in HTTP Flood Athena Query	`None`	Se hai scelto il parametro Activate HTTP Flood Protection, puoi scegliere un campo raggruppamento `yes - Amazon Athena log parser` per per per contare le richieste per IP e il campo raggruppato per selezionato. Ad esempio, se si sceglie`URI`, la soluzione conta le richieste per IP e URI. Se hai scelto di disattivare questa protezione, ignora questo parametro.
Periodo di blocco WAF	`240`	Se hai scelto `yes - AWS Lambda log parser` o `yes - Amazon Athena log parser` per i parametri Activate Scanner & Probe Protection o Activate HTTP Flood Protection, inserisci il periodo (in minuti) per bloccare gli indirizzi IP applicabili. Per disattivare l'analisi dei log, ignorate questo parametro.

Parametro	Predefinito	Descrizione
Pianificazione del tempo di esecuzione della query Athena (minuti)	5	Se hai scelto `yes - Amazon Athena log parser` i parametri Activate Scanner & Probe Protection o Activate HTTP Flood Protection, puoi inserire un intervallo di tempo (in minuti) durante il quale viene eseguita la query Athena. Per impostazione predefinita, la query Athena viene eseguita ogni 5 minuti. Se hai scelto di disattivare queste protezioni, ignora questo parametro.

Parametro	Predefinito	Descrizione
Regole e chiavi	`IP`	Se hai scelto `yes - AWS WAF rate-based rule` il parametro Activate HTTP Flood Protection, configura questa regola per utilizzar e varie altre combinazioni di chiavi di aggregazione. Opzioni disponibili: IP (predefinito) IP+Intestazione personali zzata (se questa opzione è selezionata, `Rule Keys Custom Header` è obbligato ria) IP+URI METODO IP+HTTP Per ulteriori informazioni, consulta Opzioni di aggregazi one basate sulla frequenza delle regole WAF.

Parametro	Predefinito	Descrizione
Intestazione personalizzata Rule Keys	no	Se hai scelto `IP+Custom Header` il parametro Rule Keys, inserisci il nome dell'intestazione personalizzata da utilizzare per l'aggregazione delle richieste. Per ulteriori informazioni, consulta Opzioni di aggregazione basate sul tipo di istruzione delle regole WAF.

Parametro	Predefinito	Descrizione
Soglia della finestra temporale (minuti)	5	Soglia temporale in minuti per la protezione dalle inondazioni HTTP. Si applica sia alla regola basata sulla frequenza che al parser di log lambda. Opzioni disponibili: [1, 2, 5, 10]. Se si sceglie `yes - AWS WAF rate-based rule` il parametro Activate HTTP Flood Protection, verrà utilizzato per le finestre temporali di valutazione. Per ulteriori informazioni, consulta l'informativa WAF web ACL rate based. Se si sceglie `yes - AWS Lambda log parser` Activate HTTP Flood Protection, il parametro Activate HTTP Flood Protection verrà utilizzato per il periodo di valutazione oltre al periodo di blocco.
Regola personalizzata: Bad Bot		
Attiva Bad Bot Protection	`yes`	Scegli `yes` di attivare il componente progettato per bloccare bot dannosi e raccoglitori di contenuti.

Parametro	Predefinito	Descrizione
ARN di un ruolo IAM con accesso in scrittura ai CloudWatch log del tuo account	<optional input>	Fornisci un ARN opzionale di un ruolo IAM con accesso in scrittura ai CloudWatch log del tuo account. Ad esempio: `ARN: arn:aws:iam::account_id:role/myrolename` . Se lasci vuoto questo parametro (impostazione predefinita), la soluzione crea un nuovo ruolo per te.
Regola personalizzata: elenchi di reputazione IP di terze parti		
Attiva la protezione dell'elenco di reputazione	`yes`	Scegli `yes` di bloccare le richieste provenienti da indirizzi IP su elenchi di reputazione di terze parti (gli elenchi supportati includono Spamhaus, Emerging Threats e Tor exit node).
Regole personalizzate precedenti		

Parametro	Predefinito	Descrizione
Attiva la protezione SQL Injection	`yes`	Scegli `yes` di attivare il componente progettato per bloccare i comuni attacchi di SQL injection. Valuta la possibilità di attivarlo se non utilizzi un set di regole di base gestito da AWS o un gruppo di regole del database SQL gestito da AWS. Puoi scegliere una delle opzioni (`yes`(continua) o`yes - NO_MATCH`) che desideri che AWS WAF gestisca richieste di grandi dimension i superiori a 8 KB (8192 byte). `yes - MATCH` Per impostazione predefinita, `yes` ispeziona i contenuti dei componenti della richiesta che rientrano nei limiti di dimensione in base ai criteri di ispezione delle regole. Per ulteriori informazioni, consulta Gestione dei componenti di richieste Web di grandi dimensioni. Scegli no di disattivare questa funzionalità. NOTA: lo CloudFormation stack aggiunge l'opzione di gestione delle sovradime nsionate selezionata alla regola di protezione SQL

Parametro	Predefinito	Descrizione
		injection predefinita e la distribuisce nel tuo account AWS. Se hai personali zzato la regola al di fuori di CloudFormation, le modifiche verranno sovrascritte dopo l'aggiornamento dello stack.

Parametro	Predefinito	Descrizione
Livello di sensibilità per SQL Injection Protection	`LOW`	Scegli il livello di sensibilità che desideri che AWS WAF utilizzi per ispezionare gli attacchi di SQL injection. `HIGH`rileva più attacchi, ma potrebbe generare più falsi positivi. `LOW` è generalmente una scelta migliore per le risorse che dispongono già di altre protezioni contro gli attacchi di iniezione SQL o che hanno una bassa tolleranza per i falsi positivi. Per ulteriori informazioni, consulta AWS WAF aggiunge livelli di sensibilità per le istruzioni e le SensitivityLevel proprietà delle regole di SQL injection nella AWS CloudFormation User Guide. Se scegli di disattivare la protezione SQL injection, ignora questo parametro. NOTA: lo CloudFormation stack aggiunge il livello di sensibilità selezionato alla regola di protezione SQL injection predefinita e lo distribuisce nel tuo account AWS. Se hai personali zzato la regola al di fuori di

Parametro	Predefinito	Descrizione
		CloudFormation, le modifiche verranno sovrascritte dopo l'aggiornamento dello stack.

Parametro	Predefinito	Descrizione
Attiva Cross-Site Scripting Protection	`yes`	Scegli `yes` di attivare il componente progettato per bloccare gli attacchi XSS comuni. Valuta la possibili tà di attivarlo se non utilizzi un set di regole di base gestito da AWS. Puoi anche selezionare una delle opzioni (`yes`(continua) o`yes - NO_MATCH`) che desideri che AWS WAF gestisca richieste di grandi dimension i superiori a 8 KB (8192 byte). `yes - MATCH` Per impostazione predefinita, `yes` utilizza l'`Continue`opzione, che controlla i contenuti dei componenti della richiesta che rientrano nei limiti di dimensione in base ai criteri di ispezione delle regole. Per ulteriori informazioni, consulta Gestione sovradimensionata dei componenti della richiesta . Scegliete no di disattiva re questa funzionalità. NOTA: lo CloudFormation stack aggiunge l'opzione di gestione oversize seleziona ta alla regola di cross-sit e scripting predefinita e la distribuisce nel tuo account AWS. Se hai personali

Parametro	Predefinito	Descrizione
		zzato la regola al di fuori di CloudFormation, le modifiche verranno sovrascritte dopo l'aggiornamento dello stack.
Impostazioni di conservazione degli IP consentite e negate		
Periodo di conservazione (minuti) per il set IP consentito	`-1`	Se si desidera attivare la conservazione degli IP per il set di IP consentiti, immettere un numero (`15`o superiore) come periodo di conservazione (minuti). Gli indirizzi IP che raggiungono il periodo di conservazione scadono e la soluzione li rimuove dal set IP. La soluzione supporta un periodo di conservazione minimo di 15 minuti. Se si immette un numero compreso tra `0` e`15`, la soluzione lo considera come`15`. Lasciala impostata `-1` (impostazione predefinita) per disattivare la conservazione degli IP.

Parametro	Predefinito	Descrizione
Periodo di conservazione (minuti) per il set di IP negato	`-1`	Se si desidera attivare la conservazione degli IP per il set di IP negati, immettere un numero (`15`o superiore) come periodo di conservazione (minuti). Gli indirizzi IP che raggiungono il periodo di conservazione scadono e la soluzione li rimuove dal set IP. La soluzione supporta un periodo di conservazione minimo di 15 minuti. Se si immette un numero compreso tra `0` e`15`, la soluzione lo considera come`15`. Lasciala impostata `-1` (impostazione predefinita) per disattivare la conservazione degli IP.

Parametro	Predefinito	Descrizione
E-mail per ricevere una notifica alla scadenza dei set di IP consentiti o negati	<optional input>	Se hai attivato i parametri del periodo di conservaz ione IP (vedi due parametri precedenti) e desideri ricevere una notifica e-mail quando gli indirizzi IP scadono, inserisci un indirizzo e-mail valido. Se non hai attivato la conservazione dell'IP o desideri disattivare le notifiche e-mail, lascialo vuoto (impostazione predefini ta).
Impostazioni avanzate		
Periodo di conservazione (giorni) per i gruppi di log	365	Se desideri attivare la conservazione per i gruppi di CloudWatch log, inserisci un numero (1o superiore) come periodo di conservazione (giorni). È possibile scegliere un periodo di conservaz ione compreso tra un giorno (1) e dieci anni (3650). Per impostazione predefinita, i log scadono dopo un anno. Impostalo per conservare i registri -1 a tempo indetermi nato.

6. Scegli Next (Successivo).

7. Nella pagina Configura le opzioni dello stack, puoi specificare i tag (coppie chiave-valore) per le risorse dello stack e impostare opzioni aggiuntive. Scegli Next (Successivo).
8. Nella pagina Rivedi e crea, rivedi e conferma le impostazioni. Seleziona le caselle che confermano che il modello creerà risorse IAM e tutte le funzionalità aggiuntive richieste.
9. Scegli Invia per distribuire lo stack.

   Visualizza lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo stato CREATE_COMPLETE in circa 15 minuti.

> **Note**
>
> Oltre alle funzioni `Log Parser` e `IP Lists Parser` AWS Lambda, questa soluzione include le funzioni e `helper` `custom-resource` Lambda, che vengono eseguite solo durante la configurazione iniziale o quando le risorse vengono aggiornate o eliminate. Quando usi questa soluzione, vedrai tutte le funzioni nella console AWS Lambda, ma solo le tre funzioni principali della soluzione sono regolarmente attive. Non eliminare le altre due funzioni; sono necessarie per gestire le risorse associate.

Per visualizzare i dettagli sulle risorse dello stack, scegli la scheda Output. Questo include il valore. BadBotHoneypotEndpoint Ricorda questo valore perché lo utilizzerai per incorporare il link Honeypot nella tua applicazione web.

Fase 2: Associa l'ACL web alla tua applicazione web

Aggiorna le tue CloudFront distribuzioni o ALB per attivare AWS WAF e la registrazione utilizzando le risorse generate nella fase 1. Avvia lo stack.

1. Accedi alla console AWS WAF.
2. Scegli l'ACL web che desideri utilizzare.
3. Nella scheda Associated AWS resources (Risorse AWS associate), scegliere Add AWS resources (Aggiungi risorse AWS).
4. In Tipo di risorsa, scegli la CloudFront distribuzione o ALB.
5. Seleziona una risorsa dall'elenco, quindi scegli Aggiungi per salvare le modifiche.

Fase 3. Configurazione della registrazione degli accessi Web

Configura CloudFront il tuo ALB per inviare i log di accesso Web al bucket Amazon S3 appropriato in modo che questi dati siano disponibili per la funzione Log Parser Lambda.

Memorizza i log di accesso al Web da una distribuzione CloudFront

1. Accedi alla CloudFront console Amazon.
2. Seleziona la distribuzione della tua applicazione web e scegli Impostazioni di distribuzione.
3. Nella scheda General (Generale), seleziona Edit (Modifica).
4. Per AWS WAF Web ACL, scegli la soluzione Web ACL creata (il parametro Stack name).
5. Per Logging, scegliere On (Abilitato).
6. Per Bucket for Logs, scegli il bucket S3 che desideri utilizzare per archiviare i log di accesso Web. Può trattarsi di un bucket S3 nuovo o esistente che viene utilizzato nello stack principale e dispone dell'autorizzazione per scrivere i log. CloudFront L'elenco a discesa enumera i bucket associati all'account AWS corrente. Per ulteriori informazioni, consulta la sezione Guida introduttiva a una CloudFront distribuzione di base nella Amazon CloudFront Developer Guide.
7. Imposta il prefisso del registro sul prefisso utilizzato per la distribuzione della soluzione. È possibile trovare il prefisso nello stack principale, scheda Parametri, (impostazione predefinita). AppAccessLogBucketPrefixParam`AWSLogs/`
8. Scegliere Sì, modifica per salvare le modifiche.

Per ulteriori informazioni, consulta Configurazione e utilizzo dei log standard (log di accesso) nella Amazon CloudFront Developer Guide.

Archivia i log di accesso al Web da un Application Load Balancer

1. Accedi alla console Amazon Elastic Compute Cloud (Amazon EC2).
2. Selezionare Sistemi di bilanciamento del carico nel riquadro di navigazione.
3. Seleziona ALB della tua applicazione web.
4. Nella scheda Descrizione scegli Modifica attributi.
5. Scegliere Enable access logs (Abilita log di accesso).
6. Per la posizione S3, digita il nome del bucket S3 che desideri utilizzare per archiviare i log di accesso al Web. Può trattarsi di un bucket S3 nuovo o esistente che viene utilizzato nello stack principale e che dispone dell'autorizzazione di Application Load Balancer per scrivere i log.

7. Imposta il prefisso del registro sul prefisso utilizzato per la distribuzione della soluzione. È possibile trovare il prefisso nello stack principale, scheda Parametri, (impostazione predefinita). AppAccessLogBucketPrefixParam`AWSLogs/`
8. Scegli Save (Salva).

Per ulteriori informazioni, consulta Access Logs for your Application Load Balancer nella Elastic Load Balancing User Guide.

Aggiorna la soluzione

Se hai già distribuito la soluzione, segui questa procedura per aggiornare lo CloudFormation stack della soluzione e ottenere la versione più recente del framework della soluzione. Prima di aggiornare lo stack, leggi attentamente le considerazioni sull'aggiornamento.

1. Accedi alla CloudFormation console AWS.
2. Seleziona Stacks nel menu di navigazione a sinistra.
3. Seleziona lo `aws-waf-security-automations` CloudFormation stack esistente.
4. Scegli Aggiorna.
5. Seleziona Sostituisci modello corrente.
6. In Specificare il modello:
   a. Seleziona l'URL di Amazon S3.
   b. Copia il link dell'`aws-waf-security-automations.template`AWS CloudFormation.
   c. Incolla il link nella casella dell'URL di Amazon S3.
   d. Verifica che l'URL del modello corretto sia visualizzato nella casella di testo dell'URL di Amazon S3.
   e. Scegli Next (Successivo).
   f. Scegliere Next (Successivo) di nuovo.
7. In Parametri, esamina i parametri del modello e modificali se necessario. Fate riferimento alla Fase 1. Avvia lo stack per i dettagli sui parametri.
8. Scegli Next (Successivo).
9. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
10. Nella pagina Rivedi, verifica e conferma le impostazioni.
11. Seleziona la casella riconoscendo che il modello potrebbe creare risorse IAM.
12. Scegli Visualizza set di modifiche e verifica le modifiche.
13. Scegli Aggiorna stack per distribuire lo stack.

Puoi vedere lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti vedere lo stato di UPDATE_COMPLETE tra circa 15 minuti.

Considerazioni sull'aggiornamento

Le seguenti sezioni forniscono vincoli e considerazioni per l'aggiornamento di questa soluzione.

Aggiornamento del tipo di risorsa

È necessario distribuire un nuovo stack per aggiornare il parametro Endpoint dopo aver creato lo stack. Non modificate il parametro Endpoint durante l'aggiornamento dello stack.

WAFV2 aggiornamento

A partire dalla versione 3.0, questa soluzione supporta AWS WAFV2. Abbiamo sostituito tutte le chiamate API AWS WAF Classic con chiamate API WAFV2 AWS. Ciò rimuove le dipendenze da Node.js e utilizza la maggior parte del runtime up-to-date Python. Per continuare a utilizzare questa soluzione con le funzionalità e i miglioramenti più recenti, è necessario distribuire la versione 3.0 o successiva come nuovo stack.

Personalizzazioni durante l'aggiornamento dello stack

La out-of-box soluzione implementa un set di regole AWS WAF con configurazioni predefinite nel tuo account AWS con lo stack. CloudFormation Non è consigliabile applicare personalizzazioni alle regole distribuite dalla soluzione. Gli aggiornamenti dello stack sovrascrivono queste modifiche. Se hai bisogno di regole personalizzate, ti consigliamo di creare regole separate all'esterno della soluzione.

Aggiornamento di Bad Bot Protection

Nella versione 4.1.0, l'Access Handler Lambda con API Gateway è stato obsoleto e sostituito con la funzionalità di registro avanzata della funzionalità. `Log parser - Bad bot` Invece di utilizzare richieste dirette tramite API Gateway, la soluzione ora riutilizza il flusso di log per rilevare bot dannosi.

Implementazione precedente:

1. Gestore di accesso richiesto Lambda e API Gateway.
2. Endpoint honeypot utilizzato per la gestione diretta delle richieste.
3. È necessario incorporare l'endpoint honeypot nei siti Web.

Nuova implementazione (4.1.0+): il parser di log di Bad Bot Protection ora:

1. Ispeziona le richieste all'endpoint honeypot tramite i log.
2. Elabora le richieste quando Bad Bot Protection è attivata.
3. Utilizza il filtro WAF BadBotRuleFilterper identificare le richieste di bot non valide.
4. Analizza i dati di registro per identificare gli indirizzi IP che superano le quote definite.
5. Aggiorna le condizioni IP di AWS WAF per bloccare gli indirizzi identificati.

Questa modifica semplifica l'architettura eliminando le funzionalità duplicate e sfruttando le funzionalità di elaborazione dei log esistenti.

Aggiornamento CDK

A partire dalla versione v4.1.0, questa soluzione è supportata da CDK. Se si esegue la migrazione da una versione precedente alla v4.1.0. Usa il nuovo modello e aggiorna la soluzione in Cloudformation. Quindi puoi iniziare ad aggiornare la soluzione localmente tramite il tuo terminale usando cdk deploy (vedi README per maggiori informazioni) Se provi a utilizzare cdk deploy direttamente, potresti vedere questo errore: Indentazione insufficiente nella raccolta dei flussi

L'altro modo per aggiornare la soluzione consiste nell'utilizzare il modello fornito dalla soluzione e accedere alla sezione Cloudformation della console AWS, fare clic su aggiorna la soluzione e incollare lì il nuovo modello.

> **Note**
>
> Se stai effettuando l'aggiornamento dalla versione 3.0 o 3.1 alla versione 3.2 o successiva di questa soluzione e hai inserito manualmente gli indirizzi IP nel set di IP consentito o negato, correrai il rischio di perderli. Per evitare che ciò accada, crea una copia degli indirizzi IP nel set IP consentito o negato prima di aggiornare la soluzione. Quindi, dopo aver completato l'aggiornamento, aggiungi nuovamente gli indirizzi IP al set IP, se necessario. Fare riferimento ai get-ip-setcomandi e update-ip-setCLI. Se stai già utilizzando la versione 3.2 o successiva, ignora questo passaggio.

Disinstalla la soluzione

Per disinstallare la soluzione, elimina gli CloudFormation stack:

1. Accedi alla CloudFormation console AWS.
2. Seleziona lo stack principale della soluzione. Tutti gli altri stack di soluzioni verranno eliminati automaticamente.
3. Scegliere Delete (Elimina).

> **Note**
>
> La disinstallazione della soluzione elimina tutte le risorse AWS utilizzate dalla soluzione ad eccezione dei bucket Amazon S3. Se alcuni set IP non riescono a essere eliminati a causa del problema di limitazione della velocità superata causato dalle quote delle API AWA WAF, elimina manualmente tali set IP e quindi elimina lo stack.

Usa la soluzione

Questa sezione fornisce istruzioni dettagliate per utilizzare la soluzione dopo averla distribuita.

Modifica i set IP consentiti e negati (opzionale)

Dopo aver distribuito lo CloudFormation stack di questa soluzione, puoi modificare manualmente i set IP consentiti e negati per aggiungere o rimuovere indirizzi IP, se necessario.

1. Accedi alla console AWS WAF.
2. Nel riquadro di navigazione a sinistra, scegli IP Sets.
3. Scegli IP set per Elenco consentito e aggiungi indirizzi IP da fonti attendibili.
4. Scegli IP set per Elenco negato e aggiungi gli indirizzi IP che desideri bloccare.

Incorpora il link Honeypot nella tua applicazione web (opzionale)

Se hai scelto il parametro `yes`Activate Bad Bot Protection nel passaggio 1. Avvia lo stack, il CloudFormation modello crea un endpoint trap verso un honeypot di produzione a bassa interazione. Questa trappola ha lo scopo di rilevare e deviare le richieste in entrata dagli scraper di contenuti e dai bot dannosi. Gli utenti validi non tenteranno di accedere a questo endpoint.

Questo componente migliora il rilevamento dei bot non validi monitorando le connessioni dirette a un Application Load Balancer (ALB) o CloudFront Amazon, oltre al meccanismo honeypot. Se un bot aggira l'honeypot e tenta di interagire con ALB oppure CloudFront, il sistema analizza gli schemi e i log delle richieste per identificare attività dannose. Quando viene rilevato un bot non valido, il relativo indirizzo IP viene estratto e aggiunto a una lista di blocchi AWS WAF per impedire ulteriori accessi. Il rilevamento dei bot non validi opera attraverso una catena logica strutturata, garantendo una copertura completa delle minacce:

- HTTP Flood Protection Lambda Log Parser: raccoglie i IPs bot danneggiati dalle voci di registro durante l'analisi delle inondazioni.
- Scanner & Probe Protection Lambda Log Parser: identifica i IPs bot non validi dalle voci di registro relative allo scanner.
- HTTP Flood Protection Athena Log Parser: estrae il bot non valido IPs dai log di Athena, utilizzando le partizioni durante l'esecuzione delle query.

- Scanner & Probe Protection Athena Log Parser: recupera i bot danneggiati IPs dai log Athena relativi allo scanner, utilizzando la stessa strategia di partizionamento.
- Rilevamento fallback: se sia HTTP Flood Protection che Scanner & Probe Protection sono disabilitate, il sistema si basa sul parser Log Lambda, che registra l'attività dei bot in base ai filtri delle etichette WAF.

Utilizzate una delle seguenti procedure per incorporare il collegamento honeypot per le richieste provenienti da entrambe le distribuzioni. CloudFront

Crea un' CloudFront origine per l'endpoint Honeypot

Utilizzare questa procedura per le applicazioni Web distribuite con una distribuzione. CloudFront Con CloudFront, puoi includere un `robots.txt` file per identificare gli scraper di contenuti e i bot che ignorano lo standard di esclusione dei robot. Completa i seguenti passaggi per incorporare il link nascosto e poi disabilitarlo esplicitamente nel file. `robots.txt`

1. Accedi alla CloudFormation console AWS.
2. Scegli lo stack che hai creato nella fase 1. Avvia lo stack
3. Seleziona la scheda Outputs (Output).
4. Dalla BadBotHoneypotEndpointchiave, copia l'URL dell'endpoint.
   - Il percorso del comportamento () `/ProdStage`
5. Incorpora questo link endpoint nei tuoi contenuti che puntano all'honeypot. Nascondi questo link ai tuoi utenti umani. Come esempio, esamina il seguente esempio di codice:`<a href="/behavior_path" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>`.
6. Modifica il `robots.txt` file nella radice del tuo sito Web per disabilitare esplicitamente il collegamento honeypot, come segue:

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

> **Important**
>
> Non CloudFront è richiesta la registrazione del percorso in quanto le richieste sono: Bloccate da WAF. BadBotRuleFilter Soluzione raccolta automaticamente nei log. Elaborato dal Log

parser lambda. Questo approccio semplificato utilizza direttamente i log WAF anziché richiedere una configurazione aggiuntiva degli endpoint, rendendo più efficiente il processo di rilevamento dei bot danneggiati attraverso l'analisi dei log

> **Note**
>
> È tua responsabilità verificare quali valori dei tag funzionano nell'ambiente del tuo sito web. Non utilizzarlo `rel="nofollow"` se l'ambiente non lo osserva. Per ulteriori informazioni sulla configurazione dei meta tag robots, consulta la guida per sviluppatori di Google. Modifica il `robots.txt` file nella cartella principale del tuo sito web per disabilitare esplicitamente il link honeypot, come segue:

Incorpora l'endpoint Honeypot come link esterno

> **Note**
>
> Queste regole utilizzano l'indirizzo IP di origine della richiesta Web. Se il traffico passa attraverso uno o più proxy o sistemi di bilanciamento del carico, l'origine della richiesta Web conterrà l'indirizzo dell'ultimo proxy e non l'indirizzo di origine del client.

Utilizzate questa procedura per le applicazioni Web.

1. Accedi alla CloudFormation console AWS.
2. Scegli lo stack che hai creato nella fase 1. Avvia lo stack.
3. Seleziona la scheda Outputs (Output).
4. Dalla BadBotHoneypotEndpointchiave, copia l'URL dell'endpoint.

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

> **Note**
>
> Questa procedura serve `rel=nofollow` per indicare ai robot di non accedere all'URL dell'honeypot. Tuttavia, poiché il collegamento è incorporato esternamente, non è possibile

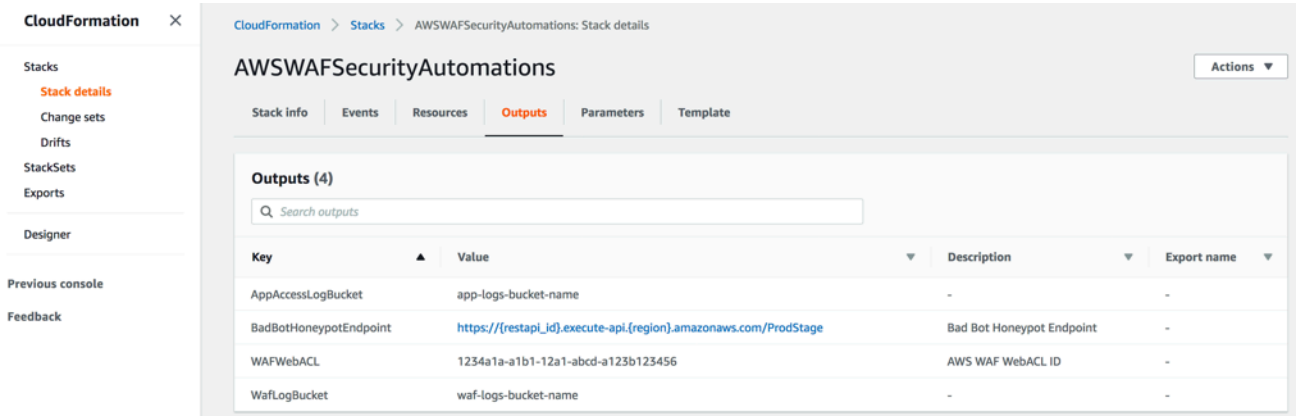
includere un `robots.txt` file per disabilitare esplicitamente il collegamento. È tua responsabilità verificare quali tag funzionano nell'ambiente del tuo sito web. Non utilizzarlo `rel="nofollow"` se l'ambiente non lo osserva.

Usa il file JSON del parser di log Lambda

Usa il file JSON del parser di log Lambda per la protezione da HTTP Flood

Se hai scelto `Yes - AWS Lambda log parser` il parametro del modello Activate HTTP Flood Protection, questa soluzione crea un file di configurazione denominato `<stack_name>-waf_log_conf.json` e lo carica nel bucket Amazon S3 utilizzato per archiviare i file di registro AWS WAF. Per trovare il nome del bucket, fai riferimento alla variabile nell'output. WafLogBucket CloudFormation La figura seguente mostra un esempio.

Schermata che mostra una schermata denominata AWSWAFSecurity Automazioni ed elenca quattro uscite



Se modifichi e sovrascrivi il `<stack_name>-waf_log_conf.json` file su Amazon S3, la funzione `Log Parser` Lambda considera i nuovi valori durante l'elaborazione di nuovi file di registro AWS WAF. Di seguito viene illustrato un esempio di file di configurazione:

Schermata di un file di configurazione di esempio

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

I parametri includono quanto segue:

- Generale:
  - Soglia di richiesta (obbligatoria): il numero massimo di richieste accettabili per cinque minuti, per indirizzo IP. Questa soluzione utilizza il valore definito durante il provisioning o l'aggiornamento dello CloudFormation stack.
  - Periodo di blocco (obbligatorio): il periodo (in minuti) per bloccare gli indirizzi IP applicabili. Questa soluzione utilizza il valore definito durante il provisioning o l'aggiornamento dello CloudFormation stack.
  - Suffissi ignorati: le richieste che accedono a questo tipo di risorsa non vengono conteggiate ai fini della soglia di richiesta. Per impostazione predefinita, questo elenco è vuoto.
- Elenco URI: utilizzalo per definire una soglia di richiesta e un periodo di blocco personalizzati per specifiche URLs. Per impostazione predefinita, questo elenco è vuoto.

Quando i log WAF arrivano in WafLogBucket, verranno elaborati dalla funzione Lambda log parser utilizzando le configurazioni nel file di configurazione. La soluzione scrive il risultato in un file di output denominato `<stack_name>-waf_log_out.json` nello stesso bucket. Se il file di output contiene un elenco di indirizzi IP identificati come aggressori, la soluzione li aggiunge all'IP WAF impostato per HTTP Flood e non possono accedere all'applicazione. Se i file di output non hanno indirizzi IP, controlla se il file di configurazione è valido o se il limite di velocità è stato superato in base al file di configurazione.

Usa il file JSON del parser di log Lambda per la protezione di scanner e sonde

Se hai scelto `Yes - AWS Lambda log parser` il parametro modello Activate Scanner & Probe Protection, questa soluzione crea un file di configurazione denominato `<stack_name>-app_log_conf.json` e lo carica nel bucket Amazon S3 definito utilizzato per archiviare i file di log di Application CloudFront Load Balancer.

Se modifichi e sovrascrivi `<stack_name>-app_log_conf.json` su Amazon S3, la funzione `Log Parser` Lambda considera i nuovi valori durante l'elaborazione di nuovi file di registro AWS WAF. Di seguito viene illustrato un esempio di file di configurazione:

Schermata del file di configurazione

I parametri includono quanto segue:

- Generale:
  - Soglia di errore (obbligatoria): il numero massimo di richieste non valide accettabili al minuto, per indirizzo IP. Questa soluzione utilizza il valore definito durante il provisioning o l'aggiornamento dello CloudFormation stack.
  - Periodo di blocco (obbligatorio): il periodo (in minuti) per bloccare gli indirizzi IP applicabili. Questa soluzione utilizza il valore definito durante il provisioning o l'aggiornamento dello CloudFormation stack.
  - Codici di errore: restituisce il codice di stato considerato errore. Per impostazione predefinita, l'elenco considera i seguenti codici di stato HTTP come errori: `400 (Bad Request)401 (Unauthorized)`,`403 (Forbidden)`,`404 (Not Found)`, `e405 (Method Not Allowed)`.

- Elenco URI: utilizzalo per definire una soglia di richiesta e un periodo di blocco personalizzati per specifiche. URLs Per impostazione predefinita, questo elenco è vuoto.

Quando i log di accesso alle applicazioni arrivano in AppAccessLogBucket, la funzione `Log Parser` Lambda li elabora utilizzando le configurazioni nel file di configurazione. La soluzione scrive il risultato in un file di output denominato `<stack_name>` -app_log_out.json` nello stesso bucket. Se il file di output contiene un elenco di indirizzi IP identificati come aggressori, la soluzione li aggiunge al set IP WAF per Scanner & Probe e impedisce loro di accedere all'applicazione. Se i file di output non hanno indirizzi IP, controllate se il file di configurazione è valido o se il limite di velocità è stato superato in base al file di configurazione.

Usa il paese e l'URI nel parser di log Athena HTTP flood

Puoi raggruppare in base IPs al paese e all'URI nella query Athena per rilevare e bloccare gli attacchi HTTP flood con pattern URI imprevedibili. A tale scopo, selezionate una delle opzioni (`Country`,`URI`,`Country and URI`) per il parametro Group By Requests in HTTP Flood Athena Query all'avvio dello stack.

Puoi anche inserire una soglia di richiesta per paese utilizzando il parametro Request Threshold by Country. Ad esempio, `{"TR": 50,"ER":150}`. La soluzione utilizza queste soglie sulle richieste provenienti da questi paesi specificati. La soluzione utilizza la soglia predefinita per le richieste provenienti da altri paesi.

> **Note**
>
> Se si definisce una soglia per paese, la soluzione include automaticamente il paese nella clausola group-by di Athena Query. Per ulteriori informazioni, consulta la tabella dei parametri nel passaggio 1. Avvia lo stack.

Per impostazione predefinita, la soluzione conta la soglia di richiesta in un periodo di cinque minuti. Questo è configurabile con il parametro Athena Query Run Time Schedule (Minute).

> **Note**
>
> La query Athena calcola la soglia al minuto dividendo la soglia della richiesta per il periodo di tempo. Esempio:
> Soglia di richiesta (soglia predefinita o soglia per paese): 100

Pianificazione del tempo di esecuzione della query Athena: 5
Soglia di richiesta al minuto: 20 = 100/5

Visualizza le query su Amazon Athena

Se hai selezionato `Yes - Amazon Athena log parser` i parametri del modello Activate HTTP Flood Protection o Activate Scanner & Probe Protection, questa soluzione crea ed esegue query Athena per CloudFront o ALB () o `ScannersProbesLogParser` AWS WAF logs (`HTTPFloodLogParser`), analizza l'output e aggiorna AWS WAF di conseguenza.

Per migliorare le prestazioni e mantenere bassi i costi, la soluzione partiziona i log in base ai timestamp presenti nei nomi dei file. La soluzione genera dinamicamente query Athena per utilizzare le chiavi di partizione (anno, mese, giorno e ora). Per impostazione predefinita, le query vengono eseguite ogni cinque minuti. È possibile configurare le loro pianificazioni di esecuzione modificando il valore del parametro del modello Athena Query Run Time Schedule (Minute). Per impostazione predefinita, ogni esecuzione di query analizza le ultime quattro o cinque ore di dati. È possibile configurare la quantità di dati scansionati da una query modificando il valore del parametro del modello WAF Block Period. La soluzione colloca inoltre le interrogazioni in gruppi di lavoro separati per gestire l'accesso alle query e i relativi costi.

> **Note**
>
> Verifica che Athena sia configurata per accedere al catalogo dati di AWS Glue. Questa soluzione crea il catalogo dei dati dei log di accesso in AWS Glue e configura una query Athena per elaborare i dati. Se Athena non è configurata correttamente, la query non viene eseguita. Per ulteriori informazioni, consulta Aggiornamento alla versione più recente di AWSAWS Glue Data Catalog. step-by-step

Per visualizzare queste interrogazioni, utilizzare la procedura seguente:

Visualizza le interrogazioni di registro WAF

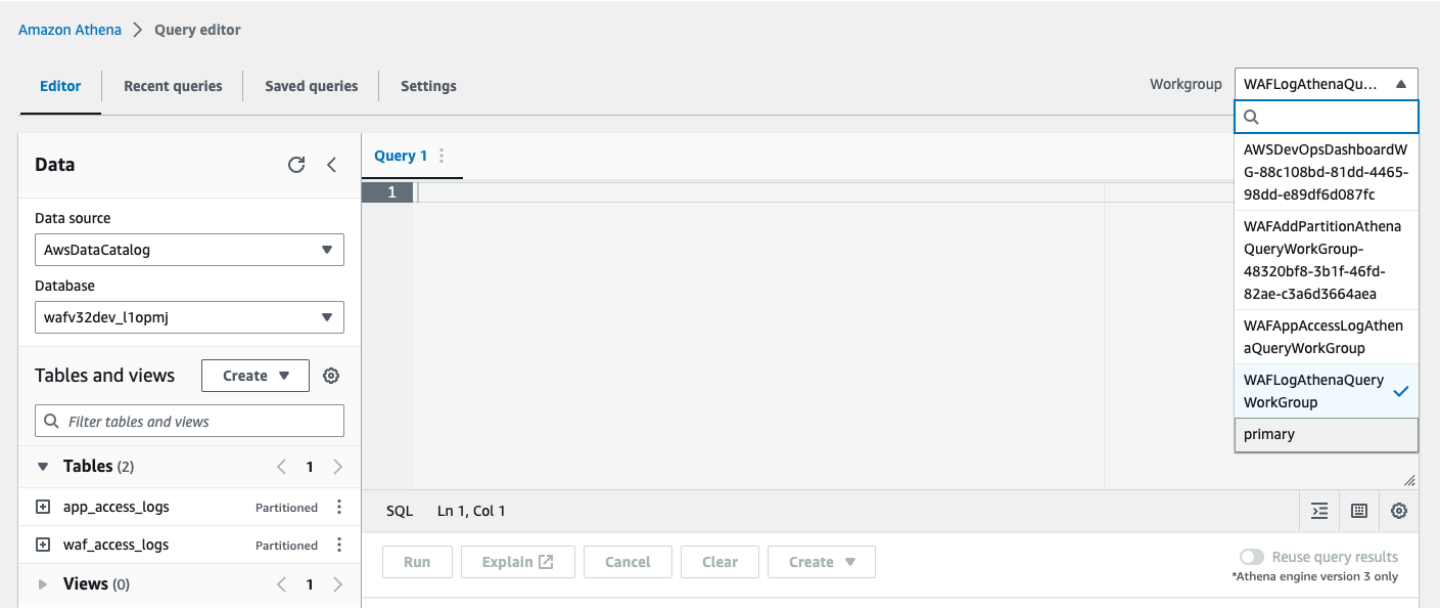
1. Accedi alla console Amazon Athena.
2. Scegliere Launch query editor.
3. Seleziona il database per questa soluzione.

4. Seleziona WAFLogAthenaQueryWorkGroupdall'elenco a discesa.

> **Note**
>
> Questo gruppo di lavoro esiste solo se è stato selezionato il parametro del `Yes - Amazon Athena log parser` modello Activate HTTP Flood Protection.

5. Scegli Switch per cambiare gruppo di lavoro.

Schermata dell'editor di query Athena che non mostra alcuna interrogazione



1. Seleziona la scheda Cronologia.
2. Seleziona e apri `SELECT` le interrogazioni dall'elenco.

Visualizza le interrogazioni relative ai registri di accesso alle applicazioni

1. Accedi alla console Amazon Athena.
2. Seleziona la scheda Workgroup.
3. Seleziona WAFAppAccessLogAthenaQueryWorkGroupdall'elenco.

> **Note**
>
> Questo gruppo di lavoro esiste solo se è stato selezionato `Yes - Amazon Athena log parser` il parametro del modello Activate Scanner & Probe Protection.

4. Scegliete Switch workgroup.
5. Seleziona la scheda Interrogazioni recenti.
6. Seleziona e apri `SELECT` le interrogazioni dall'elenco.

Visualizza l'aggiunta di interrogazioni sulle partizioni Athena

1. Accedi alla console Amazon Athena.
2. Seleziona la scheda Workgroup.
3. Seleziona WAFAddPartitionAthenaQueryWorkGroupdall'elenco.

> **Note**
>
> Questo gruppo di lavoro esiste solo se è stato selezionato il parametro del `Yes - Amazon Athena log parser` modello Activate HTTP Flood Protection and/or Activate Scanner & Probe Protection.

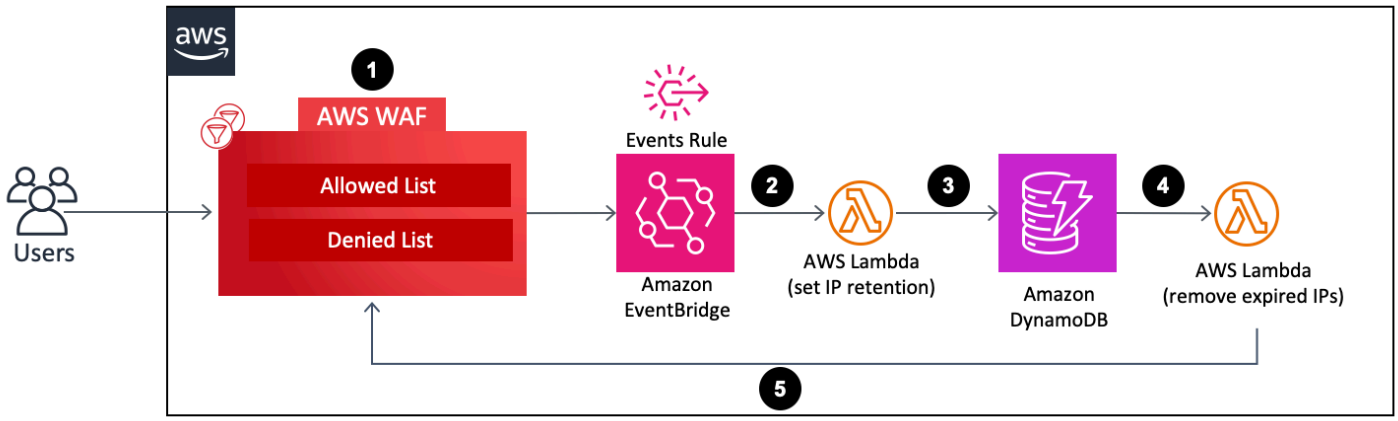
4. Seleziona Switch workgroup.
5. Seleziona la scheda Cronologia.
6. Seleziona e apri `ALTER TABLE` le interrogazioni dall'elenco. Queste query vengono eseguite ogni ora per aggiungere una nuova partizione oraria alla tabella Athena.

Configurazione della conservazione degli IP su set IP AWS WAF consentiti e negati

Puoi configurare la conservazione degli IP sui set IP AWS WAF consentiti e negati creati dalla soluzione. Le seguenti sezioni spiegano come funziona e forniscono i passaggi per configurarla.

Come funziona

Diagramma dell'architettura che illustra gli elenchi di dati consentiti e negati di AWS WAF e altre risorse AWS



1. Quando un utente aggiorna (aggiunge o elimina un indirizzo IP) il set di IP WAF consentito o negato, questa azione richiama una chiamata `UpdateIPSet` API AWS WAF e crea un evento.
2. Una regola di Amazon EventBridge Events rileva gli eventi in base a uno schema di eventi predefinito e richiama una funzione Lambda per impostare il periodo di conservazione per tutti gli indirizzi IP presenti nell'IP impostato dopo l'aggiornamento.
3. La funzione Lambda elabora gli eventi, estrae i dati rilevanti per la conservazione degli IP (come nome del set IP, ID, ambito, indirizzi IP) e li inserisce in una tabella DynamoDB. Inoltre inserisce un `ExpirationTime` attributo per ogni elemento di DynamoDB. La soluzione calcola il tempo di scadenza aggiungendo un periodo di conservazione definito dall'utente all'ora dell'evento. La tabella ha DynamoDB Streams and Time to Live (TTL) attivati. L'attributo TTL è. `ExpirationTime`
4. Quando un elemento raggiunge la scadenza, viene richiamato il TTL e DynamoDB elimina l'elemento dalla tabella dopo la scadenza. Dopo l'eliminazione dell'elemento, l'elemento eliminato viene aggiunto al flusso DynamoDB, che richiama una funzione Lambda per l'elaborazione a valle.
5. La funzione Lambda ottiene le informazioni sull'elemento eliminato dal flusso DynamoDB ed effettua una chiamata API AWS WAF per rimuovere gli indirizzi IP scaduti inclusi nell'elemento dal set IP AWS WAF di destinazione.

Attiva la conservazione degli IP

Segui questi passaggi per attivare la conservazione degli IP:

1. Nello stack Cloudformation che distribuisci o aggiorni, inserisci il Periodo di conservazione IP (minuti) per il set IP consentito e il Periodo di conservazione IP (minuti) per il set IP negato. Il periodo di conservazione minimo è di 15 minuti. La soluzione tratta qualsiasi numero compreso tra `0` e `15` come`15`. Per ulteriori informazioni sulla configurazione della distribuzione, fare riferimento alla Fase 1. Avvia lo stack.
2. Inserisci un indirizzo e-mail se desideri ricevere una notifica e-mail quando gli indirizzi IP scaduti vengono rimossi dal set IP AWS WAF. Se scegli di ricevere una notifica via e-mail, devi confermare l'iscrizione utilizzando il link contenuto nell'e-mail che ricevi dopo la corretta implementazione della soluzione. Per ulteriori informazioni sulla configurazione della distribuzione, fare riferimento alla Fase 1. Avvia lo stack.
3. Aggiorna il set di IP AWS WAF aggiungendo o eliminando indirizzi IP. Ciò avvia il processo di conservazione degli IP e crea un elemento DynamoDB, inclusa una lista di scadenza degli IP. Questa lista di scadenza è composta da indirizzi IP presenti nel set di IP AWS WAF dopo l'aggiornamento.
4. Una volta che l'elemento DynamoDB raggiunge la data di scadenza ed è stato eliminato dalla tabella, la soluzione elimina gli indirizzi IP inclusi nell'elenco di scadenza IP dell'elemento dal set IP WAF.

> **Note**
>
> A seconda del momento in cui DynamoDB elimina un elemento scaduto tramite TTL, l'operazione di eliminazione effettiva di un indirizzo IP scaduto dal set IP AWS WAF può variare. L'eliminazione TTL di DynamoDB dipende principalmente dalla dimensione e dal livello di attività di una tabella. Aspettatevi un ritardo nell'operazione di eliminazione di AWS WAF a causa del potenziale ritardo nell'operazione di eliminazione di DynamoDB. In generale, la soluzione elimina gli indirizzi IP scaduti dal set IP AWS WAF poco dopo l'eliminazione del TTL di DynamoDB. Per ulteriori informazioni, consulta DynamoDB Time to Live (TTL) nella Amazon DynamoDB Developer Guide.

Crea una dashboard di monitoraggio

AWS consiglia di configurare un sistema di monitoraggio di base personalizzato per ogni endpoint critico. Per informazioni sulla creazione e l'utilizzo di viste metriche personalizzate, consulta CloudWatch Dashboards - Create & Use Customized Metrics Views e Using Amazon Dashboards. CloudWatch

La seguente schermata della dashboard mostra un esempio di sistema di monitoraggio di base personalizzato.

Schermata della dashboard CloudFront

La dashboard mostra le seguenti metriche:

- Richieste consentite e richieste bloccate: mostra se si verifica un aumento degli accessi consentiti (il doppio del normale numero di accessi di picco) o degli accessi bloccati (qualsiasi periodo che identifica più di 1.000 richieste bloccate). CloudWatch invia un avviso a un canale Slack. Puoi utilizzare questa metrica per tenere traccia degli attacchi DDo S noti (quando aumentano le richieste bloccate) o una nuova versione di un attacco (quando alle richieste è consentito l'accesso al sistema).

  > **Note**
  >
  > Nota: la soluzione fornisce questa metrica.

- BytesDownloaded vs Uploaded: aiuta a identificare quando un attacco DDo S prende di mira un servizio che normalmente non riceve una grande quantità di accesso alle risorse esaurite (ad esempio, l'invio di informazioni da parte del motore di ricerca per uno specifico set MBs di parametri di richiesta).

- ELB Spillover e lunghezza della coda: aiuta a verificare se un attacco DDo S sta danneggiando l'infrastruttura e l'aggressore CloudFront sta aggirando il livello AWS WAF e attaccando direttamente risorse non protette.
- ELB Request Count: aiuta a identificare i danni all'infrastruttura. Questa metrica mostra se l'aggressore sta aggirando il livello di protezione o se è necessario rivedere una regola CloudFront della cache per aumentare la frequenza di accesso alla cache.
- ELB Healthy Host: puoi utilizzarla come un'altra metrica per il controllo dello stato del sistema.
- Utilizzo della CPU ASG: aiuta a identificare se l'aggressore sta bypassando AWS CloudFront WAF ed Elastic Load Balancing. Puoi utilizzare questa metrica anche per identificare i danni di un attacco.

Gestisci i falsi positivi XSS

Questa soluzione configura una regola AWS WAF che ispeziona gli elementi più comunemente esplorati delle richieste in entrata per identificare e bloccare gli attacchi XSS. Questo modello di rilevamento è meno efficace se il carico di lavoro consente agli utenti legittimi di comporre e inviare codice HTML, ad esempio utilizzando un rich text editor in un sistema di gestione dei contenuti. In questo scenario, prendete in considerazione la creazione di una regola di eccezione che aggiri la regola XSS predefinita per specifici modelli di URL che accettano l'immissione di testo RTF e implementate meccanismi alternativi per proteggere gli esclusi. URLs

Inoltre, alcuni formati di immagini o dati personalizzati possono causare falsi positivi perché contengono schemi che indicano un potenziale attacco XSS nei contenuti HTML. Ad esempio, un file SVG potrebbe contenere un tag. `<script>` Se ti aspetti questo tipo di contenuto da utenti legittimi, personalizza le regole XSS in modo restrittivo per consentire le richieste HTML che includono questi altri formati di dati.

Completa i seguenti passaggi per aggiornare la regola XSS in modo da escludere URLs che accetti HTML come input. Per istruzioni dettagliate, consulta la Amazon WAF Developer Guide.

1. Accedi alla console AWS WAF.
2. Crea una stringa di corrispondenza o una condizione regex.
3. Configura le impostazioni del filtro per controllare l'URI e elencare i valori che desideri accettare rispetto alla regola XSS.
4. Modifica la regola XSS di questa soluzione e aggiungi la nuova condizione che hai creato.

Ad esempio, per escludere tutto dall'elenco, scegli quanto segue URLs in Quando una richiesta:

- non
- corrisponde ad almeno uno dei filer nella condizione di corrispondenza delle stringhe
- Lista consentita XSS

Risoluzione dei problemi

Se hai bisogno di assistenza con questa soluzione, contatta il supporto tecnico per aprire una richiesta di supporto per questa soluzione.

Contattare AWS Support

Se disponi di AWS Business Support+, AWS Enterprise Support o Unified Operations, puoi utilizzare l'AWS Support Center per ottenere l'assistenza di esperti su questa soluzione. Le istruzioni per eseguire tali operazioni sono fornite nelle sezioni seguenti.

Crea un caso

1. Apri Support Center.
2. Scegli Crea caso.

Come possiamo aiutarti?

1. Scegli Tecnico.
2. Per Assistenza, seleziona Soluzioni.
3. Per Categoria, seleziona Automazioni di sicurezza per AWS WAF.
4. Per Severity, l'opzione più adatta al tuo caso d'uso.
5. Quando si inseriscono i campi Servizio, Categoria e Severità, l'interfaccia inserisce i collegamenti alle domande più comuni per la risoluzione dei problemi. Se non riesci a risolvere la tua domanda con questi link, scegli Passaggio successivo: Informazioni aggiuntive.

Informazioni aggiuntive

1. In Oggetto, inserisci il testo che riassume la domanda o il problema.
2. Per Descrizione, descrivi il problema in dettaglio, includendo il nome di questa soluzione e la versione che stai utilizzando, ad esempio: Security Automations for AWS WAF Vx.y.z.
3. Scegli Allega file.
4. Allega le informazioni necessarie a Support per elaborare la richiesta.

Aiutaci a risolvere il tuo caso più velocemente

1. Inserisci le informazioni richieste.
2. Scegli Passaggio successivo: risolvi ora o contattaci.

Risolvi subito o contattaci

1. Rivedi le soluzioni Solve now.
2. Se non riesci a risolvere il problema con queste soluzioni, scegli Contattaci, inserisci le informazioni richieste e scegli Invia.

Guida per sviluppatori

Questa sezione fornisce il codice sorgente della soluzione.

Codice sorgente

Visita il nostro GitHub repository per scaricare i modelli e gli script per questa soluzione e per condividere le tue personalizzazioni con altri.

I modelli di questa soluzione vengono generati utilizzando il CDK AWS. Per ulteriori informazioni, consulta il file README.md.

Riferimento

Questa sezione include informazioni su una funzionalità opzionale per la raccolta di metriche uniche per questa soluzione, riferimenti a risorse correlate e un elenco di sviluppatori che hanno contribuito a questa soluzione.

Raccolta di dati anonimizzata

Questa soluzione include un'opzione per inviare metriche operative ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. Quando è attivata, la soluzione raccoglie le seguenti informazioni e le invia ad AWS durante la distribuzione iniziale del CloudFormation modello:

- ID della soluzione: l'identificatore della soluzione AWS
- ID univoco (UUID): identificatore univoco generato casualmente per ogni implementazione di questa soluzione
- Timestamp: timestamp di raccolta dati
- Configurazione della soluzione: funzionalità attivate e parametri impostati durante l'avvio iniziale
- Ciclo di vita: per quanto tempo il cliente ha utilizzato questa soluzione (in base alla cancellazione dello stack)
- Dati del parser di registro:
  - Il numero di indirizzi IP nel set IP Scanner & Probe, nel set IP Bad Bot e nell'IP HTTP Flood impostato per bloccare
  - Il numero di richieste elaborate e bloccate
- IP elenca i dati del parser:
  - Il numero di indirizzi IP nel set di IP degli elenchi di reputazione
  - Il numero di richieste elaborate e bloccate
- Dati di conservazione IP: il numero di indirizzi IP scaduti rimossi dal set IP consentito o negato

AWS possiede i dati raccolti attraverso questo sondaggio. La raccolta dei dati è soggetta alla politica sulla privacy di AWS. Per disattivare questa funzionalità, completa i seguenti passaggi prima di avviare il CloudFormation modello AWS.

1. Scarica `aws-waf-security-automations.template` AWS CloudFormation sul tuo disco rigido locale.
2. Apri il CloudFormation modello con un editor di testo.
3. Modifica la sezione CloudFormation di mappatura dei modelli da:

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

   to:

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

4. Accedi alla CloudFormation console AWS.
5. Seleziona Create stack.
6. Nella pagina Crea stack, sezione Specificare il modello, seleziona Carica un file modello.
7. In Carica un file modello, scegli Scegli file e seleziona il modello modificato dall'unità locale.
8. Scegli Avanti e segui i passaggi del Passaggio 1. Avvia lo stack.

Risorse correlate

Whitepaper AWS associati

- Best practice AWS per la resilienza DDo S

Post associati al blog sulla sicurezza di AWS

- Come prevenire gli hotlinking utilizzando AWS WAF, CloudFront Amazon e Referer Checking

Elenchi di reputazione IP di terze parti

- Sito web Spamhaus DROP List
- Elenco IP Proofpoint Emerging Threats

- Elenco dei nodi di uscita Tor

Collaboratori

- Heitor Vital
- Lee Atkinson
- Ben Potter
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- Zitto Jackson
- William Quan
- Mikhail Markhain

Revisioni

Visita Changelog.md nel nostro GitHub repository per tenere traccia dei miglioramenti e delle correzioni specifici delle versioni.

Note

Questa guida all'implementazione viene fornita solo a scopo informativo. Rappresenta le attuali offerte e pratiche di prodotti AWS alla data di pubblicazione del presente documento, che sono soggette a modifiche senza preavviso. I clienti hanno la responsabilità di effettuare una valutazione indipendente delle informazioni contenute in questo documento e di qualsiasi uso dei prodotti o servizi AWS, ciascuno dei quali viene fornito «così com'è» senza garanzie di alcun tipo, esplicite o implicite. Questo documento non crea alcuna garanzia, dichiarazione, impegno contrattuale, condizione o assicurazione da parte di AWS, delle sue affiliate, fornitori o licenzianti. Le responsabilità di AWS nei confronti dei propri clienti sono definite dai contratti AWS e il presente documento non costituisce parte né modifica qualsivoglia contratto tra AWS e i suoi clienti.

La soluzione Security Automations for AWS WAF è concessa in licenza secondo i termini della licenza Apache versione 2.0.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.