Tworzenie AWS Web Application Firewall

Uwaga: wszystkie zasoby należy utworzyć w regionie us-east-1

W tym przypadku skorzystasz z gotowego rozwiązania przygotowanego przez AWS - AWS WAF Security Automations

Link do dokumentacji

Szablon do pobrania

Kod

FAQ

Instrukcja

1. Utwórz foldery
   `waf/templates`
   `waf/commands`
   `waf/parameters`
2. Pobierz szablon i zapisz go w folderze `waf/templates`. Opcjonalnie - zamień rozszerzenie `.template` na `.yaml` - pozwoli to skorzystać ze znanych Ci wtyczek do Visual Studio Code.
3. Przejrzyj kod szablonu oraz kod szablonów do stacków podrzędnych
4. Wybierz parametry ochrony dla aplikacji

Modyfikacje

5. Dodaj parametry `Project`, `Stage`, `Component`
6. Zapisz do parametru SSM ID Web ACL. Ta wartość będzie potrzebna przy wdrożeniu Amazon CloudFront. Parametr powinien mieć nazwę wg konwencji: `${Project}/${Stage}${Component}/web-acl/id`
7. Utwórz plik JSON z parametrami
8. W razie potrzeby utwórz szablon, parametry oraz zestaw poleceń dotyczący bucketu na logi Amazon CloudFront. Może być potrzebne wskazanie tego bucketu jako miejsca przechowywania logów z Amazon CloudFront.
9. Utwórz zestaw poleceń AWS CLI tworzących stack z WAF
10. Utwórz stack z WAF (i innymi zasobami)

Komponenty

AWS Managed Rules

Zestaw reguł zapewniający ochronę przeciwko wykorzystywaniu popularnych podatności w aplikacjach

Manual IP lists

Pozwala tworzyć listy adresów IP z których ruch jest dozwolony lub zabroniony

SQL Injection

Ochrona przed atakami typu SQL Injection

XSS

Ochrona przed cross-site scripting

HTTP flood

Ochrona przed atakami DDoS, próbami przełamania hasła za pomocą brute-force

(Uwaga - jeśli robimy testy wydajnościowe, to należy czasowo wyłączyć tę regułę)

Scanners and Probes

Komponent wyszukuje podejrzane zdarzenia w logach (np. duża liczba błędów) i blokuje na określony czas ruch z podejrzanego adresu IP

IP Reputation Lists

Komponent zawiera funkcję lambda, która przeszukuje listy adresów IP i dodaje nowe zakresy do listy zablokowanych IP.

Bad Bots

Komponent zawierający `honeypot`, który ma zwabiać potencjalnych atakujących