Formação AWS Cloud Foundations

Alexsandro Lechner

Arquiteto de Soluções AWS

linkedin.com/in/alexsandrolechner

Conteúdo Programático

❑ Módulo 9: Segurança na AWS

- ➢ Práticas recomendadas de segurança na nuvem
- ➢ Criptografia de dados na AWS
- ➢ **AWS WAF: firewall de aplicativos da web**

Segurança na AWS

AWS WAF: firewall de aplicativos da web

AWS WAF: firewall de aplicativos da web

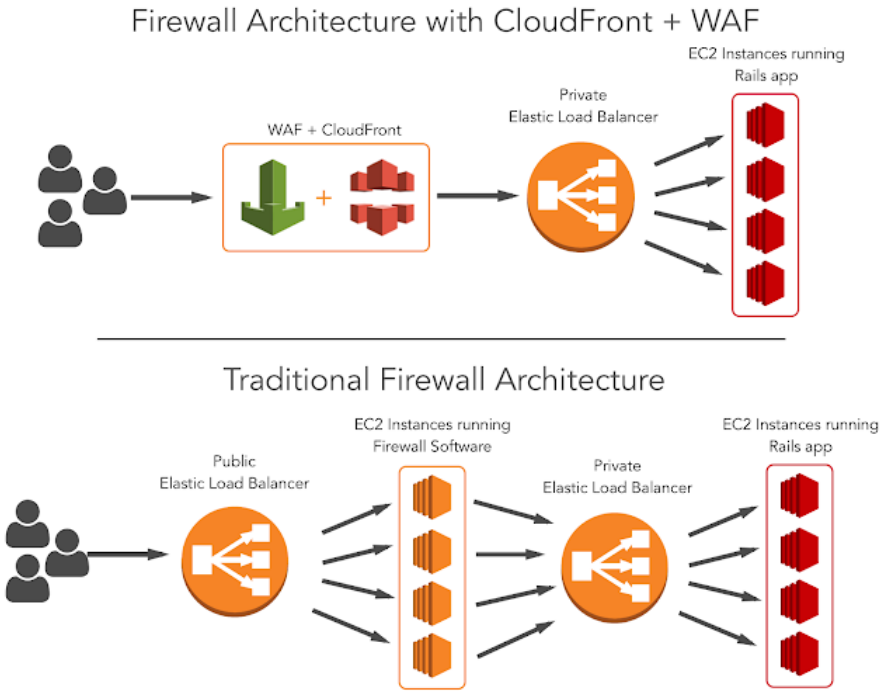
O AWS WAF (Web Application Firewall) é uma ferramenta que protege seus sites e aplicações na internet contra ataques maliciosos.

amazon WAF

E funciona como uma barreira de segurança, analisando o tráfego que chega ao seu site e bloqueando atividades suspeitas, como tentativas de invasão, ataques de força bruta ou exploração de vulnerabilidades.

[4]

AWS WAF: firewall de aplicativos da web



AWS WAF: firewall de aplicativos da web

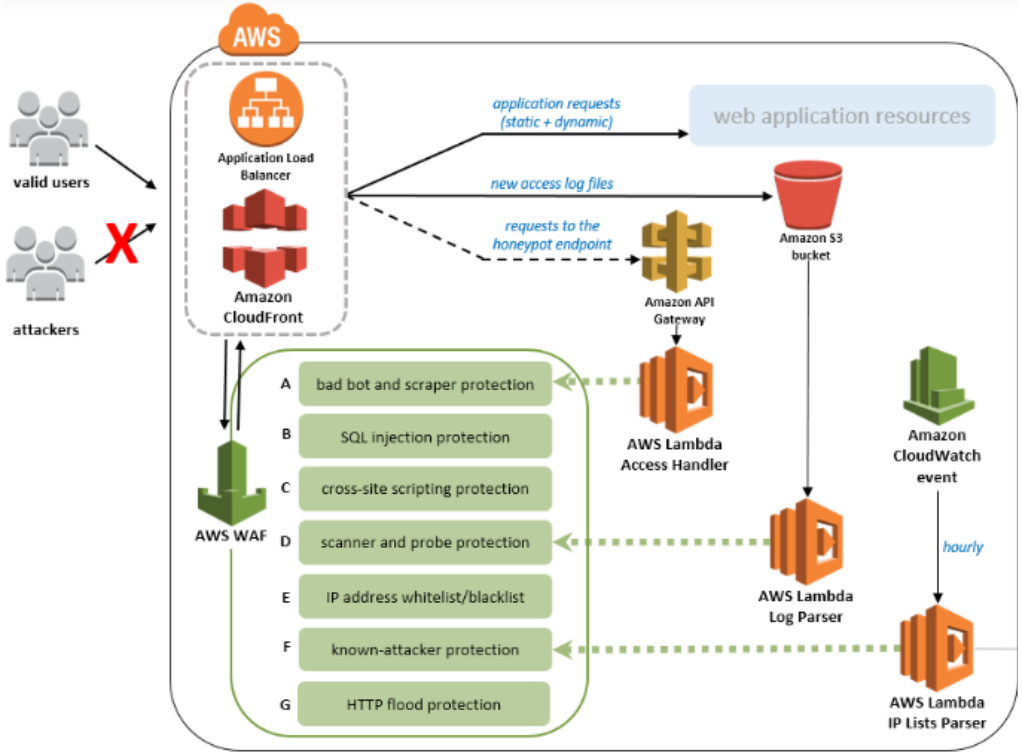
Com ele podemos criar regras personalizadas no WAF para decidir o que permitir ou bloquear.

Por exemplo, podemos impedir que hackers explorem falhas conhecidas, bloqueiem endereços IP suspeitos ou impeçam ataques comuns, como DDoS e injeções de SQL.

AWS WAF: firewall de aplicativos da web

O WAF é fácil de usar e funciona com outros serviços da AWS, como o Amazon CloudFront (para distribuir conteúdo na web) ou o Application Load Balancer. Ele ajuda a proteger suas aplicações, melhorar a segurança e manter os dados dos seus usuários seguros.

AWS WAF



1. Proteção contra bots maus e scrapers
2. Proteção contra injeção de SQL
3. Proteção contra scripts
4. Proteção do scanner
5. Lista branca e lista negra de Ips
6. Proteção contra atacantes conhecidos
7. Proteção contra inundações HTTP

AWS WAF: firewall de aplicativos da web

1. Proteção contra bots maus e scrapers
Quando o script AWS CloudFormation é iniciado, fornece ao utilizador um URL de honeypot na saída que é inserido em qualquer aplicação Web como uma ligação HTML oculta. Assim, se alguém tentar aceder a esse URL de forma anónima, esse IP específico será bloqueado e o utilizador não poderá continuar a aceder à aplicação Web.

2. Proteção contra injeção de SQL
A regra de injeção de SQL protege a aplicação web contra ataques de injeção de SQL. Analisa os URL, a cadeia de consulta, os cabeçalhos e o corpo do HTML.

3. Proteção contra scripts entre sítios
A proteção contra scripts entre sítios cria uma regra que protege a sua aplicação Web contra scripts XSS. Analisa os URLs, a cadeia de consulta, os cabeçalhos e o corpo HTML. É definido um conjunto de regras semelhante para os ataques XSS, tal como foi definido para a injeção de SQL

4. Proteção do scanner e da sonda
Uma função AWS Lambda personalizada analisa naturalmente os registos de acesso e, consequentemente, analisa a conduta duvidosa e adiciona esse IP a uma lista de endereços IP bloqueados.

AWS WAF: firewall de aplicativos da web

5. Lista branca e lista negra de IPs
Esta regra permite ao utilizador colocar manualmente na lista branca ou na lista negra os endereços IP da sua escolha.

6. Proteção contra atacantes conhecidos
Este componente é a função AWS Lambda do analisador de listas de IP, que verifica de hora a hora as listas de reputação de IPs de terceiros para obter novos intervalos a bloquear.

7. Proteção contra inundações HTTP
Este componente fornece proteção contra ataques de um determinado IP que consiste num grande número de pedidos. É definido um limiar com esta regra para definir o número máximo de pedidos.

AWS WAF: firewall de aplicativos da web

Dados para POC

WAF_TESTES.txt