

20221223_아이디어스_AWS_WAF

내용 요약

: 아이디어스 서비스의 대부분은 웹기반으로 내부적으로 HTTP API를 사용

웹 기반 공격에 대한 보호방안으로 AWS WAF를 도입함

1) 어디에 WAF를 연동할까?

: AWS WAF는 CloudFront, ALB, APIGateway에 연동할 수 있다

: 정답은 없고, 경우에 따라 복합적으로 배치할 수 있는데 CF에 연동하는 경우 어느 정도 수준의 DDOS성 트래픽을 CF 엣지에서 처리하기 때문에 DDOS성 공격의 방어 측면에서 이점을 볼 수 있다.

2) WAF 적용시 어려운 점

1. AWS WAF가 사용하는 AWS managed rule의 경우 일부 경우 (XSS, SQL인젝션)를 제외하고는 룰에 의해 차단되었다는 것을 알려줄 뿐 구체적인 사유는 알려주지 않는다.
2. 때때로 오탐이 발생하기도 한다.
3. 로그를 조회할 수 있는 대시보드를 제공하지 않는다.

3) 해결책(?)

1. 안정적인 운영을 위해서는 일정 기간 모니터링 하면서 단계적으로 BLOCK으로 전환해가는 전략이 필요
2. WCU를 고려했을 때 WAS_WAF가 제공하는 룰을 모두 적용하기 어려워 수동으로 룰을 적용해야 할 때가 있다. 이 경우 수시로 로그를 살펴보고, 빈도수가 높은 패턴을 수동으로 룰셋을 생성해나가며 WAF의 룰셋을 발전시키는 과정이 필요하다. 룰을 설계할 때 정규식을 잘 쓰면 소모하는 WCU를 줄일 수 있다!
3. AWS WAF — FIREHOSE — OPENSEARCH 의 파이프라인을 사용하면 거의 실시간으로 트래픽 뷰를 확인할 수 있다. 또는 깃허브에서 AWS가 제공하는 대시보드들을 활용할 수도 있다. 이때, 연산의 부하 증가로 인한 오류 발생을 막기 위해서는 한 대시보드에 너무 많은 지표를 넣어서는 안된다
*이 과정에서 람다를 효과적으로 사용할 것!
4. 모든 로그들을 받기에는 로그의 양이 너무 많을 수 있으니 전략적으로 저장을 하는 것이 좋다

주요 어휘

- **WAF(=web application firewall, 웹 어플리케이션 방화벽)**

: 봇, 삽입, 애플리케이션 계층 서비스 거부(DoS)를 비롯한 악의적 공격과 원치 않는 인터넷 트래픽으로부터 웹 애플리케이션을 보호할 수 있도록 지원

: WAF를 사용하면 IP주소, HTTP헤더, HTTP본문, URI문자열, 교차 사이트 스크립팅(XSS), SQL 삽입 및 기타 OWASP정의 취약성을 비롯한 인터넷 위협을 방지하기 위한 규칙을 수립하고 관리할 수 있다.(출처. Oracle)

: 웹의 비정상 트래픽을 탐지하고 차단하기 위한 방화벽

*TCP/IP레벨에 포함된 정보들을 기반으로 차단 룰을 설정하는 단순 방화벽(FW)와는 다르게 WAF는 웹 프로토콜 HTTP 정보를 바탕으로 차단 룰을 서정

*OWASP(open web application security project)

: 오픈 소스 웹 애플리케이션 보안프로젝트

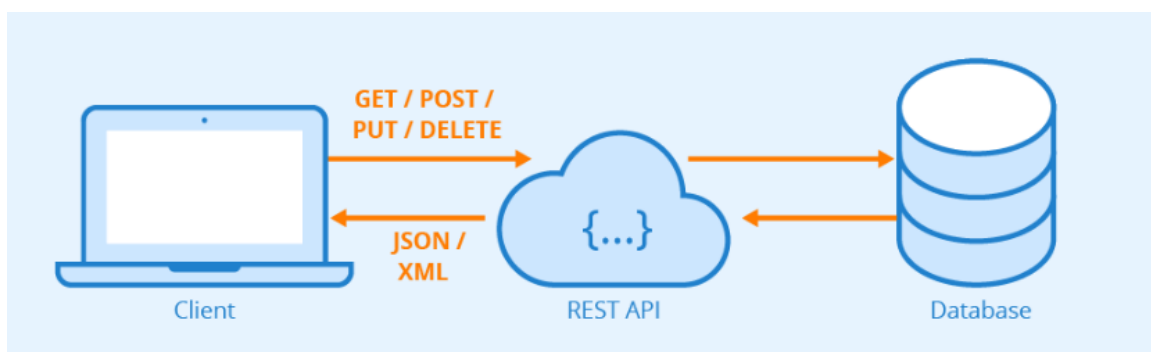
: 주로 웹에 대한 정보 노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며, 10대 웹 애플리케이션 취약점(OWASP TOP 10)을 발표

: injection, broken authentication and session management, cross-site scripting이 있다

- **HTTP API(application programming interface)**

: API란 애플리케이션이 어떤 프로그램이 제공하는 기능을 사용할 수 있게 만든 매개체로 컴퓨터나 소프트웨어를 서로 연결한다

: API의 목적은 서버 시스템이 동작하는 방식에 관한 내부의 프로세스를 숨기는 것, 추후 내부의 세세한 부분이 나중에 변경되더라도 프로그래머가 유용하게 사용할 수 있고 일정하게 관리할 수 있는 부분들만 노출시킴



: HTTP API는 HTTP를 사용하여 프로그램끼리 소통하는 API

- **CF(cloud front)**

: .html, .css, .js 및 이미지 파일과 같은 정적 및 동적 웹 콘텐츠를 사용자에게 더 빨리 배포하도록 지원하는 웹서비스 (출처. aws)


- WCU (웹 ACL 용량단위)

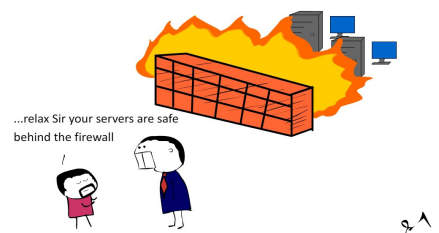
: WAF는 규칙을 정의하면서 WCU를 소모하게 되고 일정 한도 이상 규칙을 생성하기 위해서는 한도를 늘려야 한다

원본 글 링크

AWS WAF의 도입과 운영, 무엇을 고민해야할까?

최근 대부분의 서비스들이 그렇듯이, 아이디어스도 대부분의 서비스를 웹 기반으로 하고 있습니다. 앱이라고 하더라도 내부적으로는 HTTPS API를 사용하기 때문에 구조적으로는 웹 기반 공격에 대한 보

 <https://url.kr/f2liw9>



PS.

이 글을 읽기 전에 WAS WAF에 대한 배경지식이 부족하다면 우아한 형제들 기술블로그에 올라온 다음의 글을 먼저 읽어보면 도움이 될 것 같다.

[AWS WAF 운영에 대한 이야기 | 우아한형제들 기술블로그 \(woowahan.com\)](#)

참고자료

[API \(Application Programming Interface\), 그게 뭔가요? | Be Geeky_ \(assaeunji.github.io\)](#)

[Amazon CloudFront란 무엇입니까? - Amazon CloudFront](#)