AWS 결정 가이드

AWS WAF 또는 AWS Shield?

AWS WAF 또는 AWS Shield?: AWS 결정 가이드

Table of Contents

결정 가이드 1
소개 1
차이 3
사용 7
문서 기록 9
..... x

AWS WAF 또는 AWS Shield?

차이점을 이해하고 자신에게 적합한 차이점을 선택합니다.

용도	AWS WAF 가 웹 애플리케이션 보안 서비스에 대한 요구 사항을 AWS Shield 충족하는지 확인하는 데 도움이 됩니다.
최종 업데이트 날짜	2024년 9월 17일
적용 대상 서비스	• AWS WAF • AWS Shield

소개

AWS WAF (웹 애플리케이션 방화벽) 및는 분산 서비스 거부(DDoS) 공격 및 기타 웹 애플리케이션 취약성과 같은 다양한 유형의 사이버 공격으로부터 웹 애플리케이션을 보호하는 데 도움이 될 AWS Shield 수 있습니다.

- AWS WAF는 일반적인 웹 악용으로부터 웹 애플리케이션을 보호하는 데 중점을 둡니다. AWS WAF 를 사용하여 사용자 지정 가능한 웹 보안 규칙을 생성하여 악성 트래픽을 필터링하고, SQL 삽입 및 교차 사이트 스크립팅(XSS)과 같은 공격으로부터 보호하고, 다른와 통합할 수 있습니다 AWS 서비스.
- AWS Shield는 관리형 DDoS 보호 서비스입니다. AWS Shield 를 사용하여 상시 탐지 및 자동 완화 기능을 켜고 네트워크 및 전송 계층에서 일반적인 DDoS 공격으로부터 보호합니다.

는 대규모 네트워크 수준 공격을 AWS Shield 방어하지만 AWS Shield 고급을 사용하면 AWS WAF 웹 ACL을 리소스와 연결하여 애플리케이션 계층에서 보호를 제공할 수 있습니다.는 애플리케이션별 취약성에 대해 보다 세분화된 보호를 AWS WAF 제공합니다. 다중 계층 방어 전략에 두 서비스를 함께 사용하여 다양한 네트워크 계층에서 광범위한 잠재적 위협으로부터 애플리케이션을 보호합니다.

다음은 이러한 서비스 간의 주요 차이점을 개괄적으로 나타낸 것입니다.

카테고리	 AWS WAF	 AWS Shield
기본 용도	웹 애플리케이션(예: SQL 명령어 삽입 또는 XSS)의 악용으로부터 보호	DDoS 공격(예: SYN 또는 UDP 플러드)으로부터 보호
보호 계층	애플리케이션 계층(L7)	네트워크, 전송 및 애플리케이션 계층(L3/L4/L7)
배포	명시적으로 설정해야 합니다.	AWS Shield 모든 고객 계정에 표준 보호 포함
사용자 지정	사용자 지정 규칙을 사용하여 고도로 사용자 지정 가능	애플리케이션 계층 DDoS 보호의 자동 완화를 켜는 옵션을 사용하여 AWS Shield 고급을 켜거나 비활성화합니다.
관리형 규칙	AWS 관리형 규칙 및 타사 규칙 포함	해당 사항 없음
요금 모델	규칙 및 요청 수에 따른 Pay-as-you-go 요금	AWS Shield 표준 포함, AWS Shield 고급에는 추가 비용이 발생합니다.
공격 대응 팀	해당 사항 없음	AWS Shield 고급(24/7 DDoS 대응 팀)에서 사용 가능
실시간 모니터링	예	예
트래픽 검사	요청 수준	패킷 수준

AWS WAF 와의 차이점 AWS Shield

보호 계층 AWS WAF, 배포, 사용자 지정, 관리형 규칙, 요금 모델, 공격 대응 팀, 실시간 모니터링 및 트래픽 검사를 포함하여 AWS Shield 와 간의 8가지 주요 차이점을 살펴봅니다.

Layer of protection

AWS WAF

- 애플리케이션 계층(계층 7)에서 작동합니다. HTTP/S 트래픽을 필터링하고 모니터링하여 웹 애플리케이션을 보호합니다.는 SQL 삽입, 교차 사이트 스크립팅(XSS) 및 교차 사이트 요청 위조(CSRF)와 같은 일반적인 웹 악용으로부터 AWS WAF 보호합니다. 사용자 지정 규칙을 생성하여 IP 주소, 쿼리 문자열 및 헤더와 같은 다양한 기준에 따라 악성 요청을 차단할 수 있습니다.

AWS Shield

- 주로 네트워크(계층 3) 및 전송(계층 4) 계층에서 작동합니다. SYN/ACK 플러드, UDP 반사 공격 및 볼륨 공격과 같은 네트워크 리소스를 압도하는 것을 목표로 하는 분산 서비스 거부(DDoS) 공격을 완화하도록 설계되었습니다.는 공격 중에도 리소스에 도달 AWS 하는 네트워크 트래픽을 계속 사용할 수 AWS Shield 있도록 합니다. AWS Shield의 보호는 네트워크 트래픽 패턴을 분석하고 AWS 네트워크 엣지에서 식별된 위협을 자동으로 완화하여 작동합니다.

Deployment

AWS WAF

- 명시적 설정 및 구성이 필요합니다. Amazon CloudFront AWS 서비스, Application Load Balancer(ALB), Amazon API Gateway 및 AWS AppSync를 비롯한 여러에 배포할 수 있습니다. 웹 ACLs(액세스 제어 목록)을 생성하고 리소스와 연결하여 특정 웹 요청을 허용, 차단 또는 모니터링하는 규칙을 정의해야 합니다. AWS WAF 는 사용자 지정 가능한 배포 옵션을 제공하므로 특정 애플리케이션 요구 사항에 맞게 보안 정책을 조정할 수 있습니다.

AWS Shield

- AWS 서비스 및와 자동으로 통합되므로 기본 보호를 위한 추가 설정이 필요하지 않습니다. AWS Shield 표준은 모든에 자동으로 포함되어 Amazon EC2, Elastic Load Balancing(ELB), Amazon CloudFront 및 Route 53과 같은 리소스를 AWS 계정보호합니다. 고급으로 AWS Shield 보호를

강화하려면 특정 리소스에 대해 명시적으로 켜야 합니다. 배포가 원활하며가 켜져 있으면 추가 구성 AWS Shield 이 필요하지 않습니다.

Customization

AWS WAF

- 광범위한 사용자 지정 기능을 제공합니다. IP 주소, HTTP 헤더, 쿼리 문자열 파라미터 등을 기반으로 웹 요청을 허용, 차단 또는 계산하기 위한 특정 조건을 정의하는 규칙을 사용하여 사용자 지정 웹 ACLs(액세스 제어 목록)을 생성할 수 있습니다.는 특정 애플리케이션 요구 사항에 맞게 추가로 사용자 지정할 수 있는 AWS 또는 타사의 관리형 규칙 그룹을 AWS WAF 지원합니다. 또한 속도 기반 규칙을 설정하여 단일 IP 주소의 요청 수를 제한하고 고급 요청 검사 및 응답을 AWS Lambda 위해 AWS WAF 와 통합할 수 있습니다.

AWS Shield

- 제한된 사용자 지정 옵션을 제공합니다. AWS Shield Standard를 사용하면 보호가 자동으로 이루어지며 구성할 수 없습니다. AWS Shield 고급 기능을 사용하면 고급 지표 및 알림 활성화, 상태 확인 설정, 맞춤형 완화 지원을 위한 AWS DDoS 대응 팀(DRT) 액세스와 같은 일부 사용자 지정이 가능합니다. 그러나 사용자 정의 설정이 아닌 자동화된 DDoS 보호에 중점을 둡니다. AWS WAF 웹 ACL을 리소스와 연결하여 애플리케이션 계층 보호를 켤 수 있습니다.

Managed rules

AWS WAF

- 일반적인 웹 위협으로부터 보호하기 위해 웹 애플리케이션에 적용할 수 있는 다양한 관리형 규칙을 제공합니다. 이러한 관리형 규칙은 AWS 또는 타사 보안 공급업체가 사전 구성하며 SQL 삽입, 교차 사이트 스크립팅(XSS) 및 알려진 잘못된 IP 주소와 같은 다양한 보안 시나리오를 다룹니다. 이러한 관리형 규칙 그룹을 구독하고 웹 ACLs에 적용하여 새로운 취약성과 위협을 해결하기 위해 정기적으로 업데이트되는 out-of-the-box 보호를 제공할 수 있습니다. 관리형 규칙을 사용자 지정하고 사용자 지정 규칙과 결합하여 특정 애플리케이션 요구 사항에 맞게 보안 정책을 조정할 수 있습니다. AWS WAF 또한는 관리형 지능형 위협 완화 기능을 제공합니다. 이러한 기능은 악성 봇 및 계정 탈취 시도와 같은 위협으로부터 보호하기 위해 구현할 수 있는 전문적인 고급 보호 기능입니다.

AWS Shield

- 주로 DDoS 보호에 중점을 두며 기존 관리형 규칙을 제공하지 않습니다. AWS Shield 표준은 일반적인 네트워크 및 전송 계층 DDoS 공격에 대해 미리 정의된 보호 세트를 자동으로 적용합니다. AWS Shield 고급 기능은 이러한 보호를 개선하지만 사용자 지정 가능한 관리형 규칙은 제공하지 않습니다. 대신 고급 완화 기술과 맞춤형 지원을 위해 DDoS 대응 팀에 대한 액세스를 제공합니다.

Pricing model

AWS WAF

- pay-as-you-go 요금 모델을 사용합니다. 생성한 웹 ACLs 수, 각 ACL 내에 배포한 규칙 수, 규칙에서 처리한 웹 요청 수를 기준으로 요금이 부과됩니다. 이 모델은 실제 사용량에 따라 확장 가능한 비용을 허용하므로 필요한 리소스에 대해서만 비용을 지불하면 됩니다. AWS 또는 타사 공급업체가 제공하는 관리형 규칙 그룹에는 추가 요금이 적용됩니다. AWS WAF 또한는 유사한 요청당 요금 모델을 사용하여 봇 제어 및 사기 제어에 대한 관리형 규칙을 제공합니다. AWS WAF 또한는 제공된 캡차 시도 및 챌린지 응답 수에 따라 요금이 부과되는 캡차/ 챌린지 기능을 제공합니다.

AWS Shield

- 계층형 요금 모델이 있습니다. AWS Shield 표준은 추가 비용 없이 포함되어 기본 DDoS 보호를 AWS 계정제공합니다. AWS Shield 고급는 월별 구독을 기준으로 요금이 발생하고 특정 임계값을 초과하는 데이터 전송 및 완화에 대한 추가 요금이 발생합니다. 이 구독에는 AWS DDoS 대응 팀(DRT), 고급 공격 진단 및 공격 중 비용 보호에 대한 연중무휴 액세스가 포함됩니다.

Attack response team

AWS WAF

- 서비스의 일부로 전용 공격 대응 팀을 포함하지 않습니다. 대신 보안 규칙을 직접 생성, 관리 및 조정할 수 있는 도구와 기능을 제공합니다. 트래픽을 모니터링하고 위협 환경에 따라 웹 ACLs을 실시간으로 변경할 수 있지만 공격 완화를 위해 전문 지원 팀에 직접 액세스할 수는 없습니다.

AWS Shield

- Advanced 서비스의 일부로 AWS DDoS 대응 팀(DRT)에 AWS Shield 대한 액세스를 제공합니다. DRT는 실시간 공격 완화 및 대응을 지원하는 연중무휴 전문가 팀입니다. DDoS 공격 시 DRT에 문의하여 위협을 효과적으로 관리하고 완화하기 위한 사용자 지정 조언과 지원을 받을 수 있습니

다. 여기에는 AWS 리소스에 미치는 영향을 최소화하기 위한 모범 사례, 인시던트 분석 및 조정된 대응에 대한 지침이 포함됩니다.

Real-time monitoring

AWS WAF

- AWS CloudWatch와 통합하여 실시간 모니터링을 제공하므로 차단되거나 허용된 요청, 요청 속도 및 특정 규칙의 효과와 같은 지표를 추적할 수 있습니다.는 AWS Management Console 또는 APIs를 통해 웹 트래픽 및 보안 이벤트에 대한 실시간에 가까운 가시성을 AWS WAF 제공합니다. AWS WAF 지표를 기반으로 사용자 지정 CloudWatch 경보를 설정하여 잠재적 위협 또는 비정상적인 트래픽 패턴에 신속하게 대응할 수 있습니다.

AWS Shield

- 주로 AWS Shield 고급을 통해 실시간 모니터링을 제공합니다. AWS CloudWatch와 통합되어 DDoS 공격과 관련된 거의 실시간에 가까운 지표 및 알림을 제공합니다. 공격 진단, 트래픽 패턴 및 완화 효과를 모니터링할 수 있습니다. AWS Shield 또한 고급는 공격 벡터에 대한 세부 보고서와 가시성을 제공하고 위협에 대응하여 자동으로 규모를 조정하여를 통해 인사이트를 제공합니다 AWS Management Console.

두 서비스 모두 공격 패턴 및 트래픽 추세를 시각화하기 위한 대시보드를 제공합니다. AWS Shield의 모니터링은 네트워크 수준 이상 및 볼륨 공격에 중점을 두는 반면,는 애플리케이션 계층 요청 및 규칙 효과에 대한 심층적인 인사이트를 AWS WAF 제공합니다.

Traffic inspection

AWS WAF

- 애플리케이션 계층(계층 7)의 트래픽을 검사하여 HTTP/S 요청의 내용을 분석합니다. 사용자 정의 규칙을 기준으로 웹 트래픽을 평가하여 SQL 삽입, 교차 사이트 스크립팅(XSS) 또는 요청 본문, 헤더 또는 URL 파라미터 내의 기타 악성 페이로드와 같은 특정 공격 패턴을 확인합니다.

AWS Shield

- 주로 네트워크(계층 3) 및 전송(계층 4) 계층의 트래픽을 검사하는 DDoS 공격으로부터 보호하는 데 중점을 둡니다. 애플리케이션 계층 트래픽(HTTP/S)의 내용을 검사하지 않고 비정상적으로 높은 트래픽 볼륨 또는 프로토콜 오용과 같은 DDoS 공격의 일반적인 패턴을 찾습니다. AWS

Shield 는 사용자 정의 규칙 또는 콘텐츠 기반 검사 없이 이러한 위협을 자동으로 완화하여 공격 AWS 서비스 중인의 가용성을 보장합니다.

사용

AWS WAF

- 란 무엇입니까 AWS WAF?

  AWS WAF 를 사용하여 일반적인 웹 악용으로부터 웹 애플리케이션을 모니터링하고 보호하는 방법을 알아봅니다.

  가이드 살펴보기

- Amazon CloudWatch AWS WAF Logs에서 로그 분석

  Amazon CloudWatch logs에 대한 기본 AWS WAF 로깅을 설정하고 로그의 데이터를 시각화하고 분석합니다.

  블로그 읽기

- Amazon CloudWatch 대시보드를 사용하여 AWS WAF 로그 시각화

  Amazon CloudWatch를 사용하여 CloudWatch 지표, Contributor Insights 및 Logs Insights를 사용하여 AWS WAF 활동을 모니터링하고 분석할 수 있습니다.

  블로그 읽기

AWS Shield

- 란 무엇입니까 AWS Shield?

  AWS Shield 를 사용하여 네트워크 및 전송 계층에서 일반적인 DDoS 공격으로부터 웹 애플리케이션을 보호하는 방법을 알아봅니다.

  가이드 살펴보기

- 고급 시작하기 AWS Shield

AWS Shield 고급 콘솔을 사용하여 AWS Shield 고급을 시작합니다.

가이드 살펴보기

- AWS Shield 고급 워크숍

  인터넷에 노출된 리소스를 DDoS 공격으로부터 보호하고, 인프라에 대한 DDoS 공격을 모니터링하고, 적절한 팀에 알립니다.

  워크숍 살펴보기

문서 이력

다음 표에서는이 결정 가이드의 중요한 변경 사항에 대해 설명합니다. 이 가이드의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
최초 게시	가이드가 처음 게시되었습니다.	2024년 9월 17일