AWS 백서

AWS DDoS레질리언스 모범 사례

AWS DDoS레질리언스 모범 사례: AWS 백서

Table of Contents

AWS DDoS레질리언스 모범 사례

발행일: 2023년 8월 9일 (문서 수정)

분산 서비스 거부 (DDoS) 공격과 기타 사이버 공격의 영향으로부터 비즈니스를 보호하는 것이 중요합니다. 애플리케이션의 가용성과 응답성을 유지하여 서비스에 대한 고객의 신뢰를 유지하는 것이 최우선 과제입니다. 또한 공격에 대응하여 인프라를 확장해야 하는 경우 불필요한 직접 비용을 피하는 것이 좋습니다. Amazon Web Services (AWS) 는 인터넷상의 악의적인 행위자로부터 보호할 수 있는 도구, 모범 사례 및 서비스를 제공하기 위해 최선을 다하고 있습니다. 에서 적합한 서비스를 사용하면 높은 가용성, 보안 및 탄력성을 보장하는 AWS 데 도움이 됩니다.

이 백서에서는 실행 중인 애플리케이션의 복원력을 개선하기 위한 규범적 DDoS 지침을 AWS 제공합니다. AWS여기에는 애플리케이션 가용성을 보호하는 데 도움이 되는 가이드로 사용할 수 있는 DDoS-Resilient 참조 아키텍처가 포함됩니다. 또한 이 백서에서는 인프라 계층 공격 및 애플리케이션 계층 공격과 같은 다양한 공격 유형에 대해서도 설명합니다. AWS 각 공격 유형을 관리하는 데 가장 효과적인 모범 사례를 설명합니다. 또한 DDoS 완화 전략에 맞는 서비스 및 기능과 각 서비스를 사용하여 애플리케이션을 보호하는 방법을 간략하게 설명합니다.

이 백서는 네트워킹, 보안 및 보안 등의 기본 개념을 잘 알고 있는 IT 의사 결정권자와 보안 엔지니어를 대상으로 AWS합니다. 각 섹션에는 모범 사례 또는 기능에 대한 자세한 내용을 제공하는 AWS 설명서 링크가 있습니다.

AWS 연간 100만 건 이상의 DDoS 공격을 탐지하고 매일 고객을 대상으로 한 수천 건의 공격을 방어합니다. Shield Response 팀 (SRT) 에 따르면 DDoS 공격으로 인한 비즈니스 영향을 경험하는 대다수의 고객은 이 가이드의 권장 사항을 구현하지 않았습니다.

귀사는 Well-Architected입니까?

AWS Well-Architected 프레임워크는 클라우드에서 시스템을 구축할 때 내리는 결정의 장단점을 이해하는 데 도움이 됩니다. 이 프레임워크를 사용하여 클라우드에서 안정적이고 안전하며 효율적이고 비용 효율적인 시스템을 설계하고 운영하기 위한 아키텍처 모범 사례를 살펴볼 수 있습니다. 에서 무료로 제공되는 AWS Management Console(로그인 필요) 를 사용하면 각 요소에 대한 일련의 질문에 답하여 이러한 모범 사례와 비교하여 워크로드를 검토할 수 있습니다. AWS Well-Architected Tool

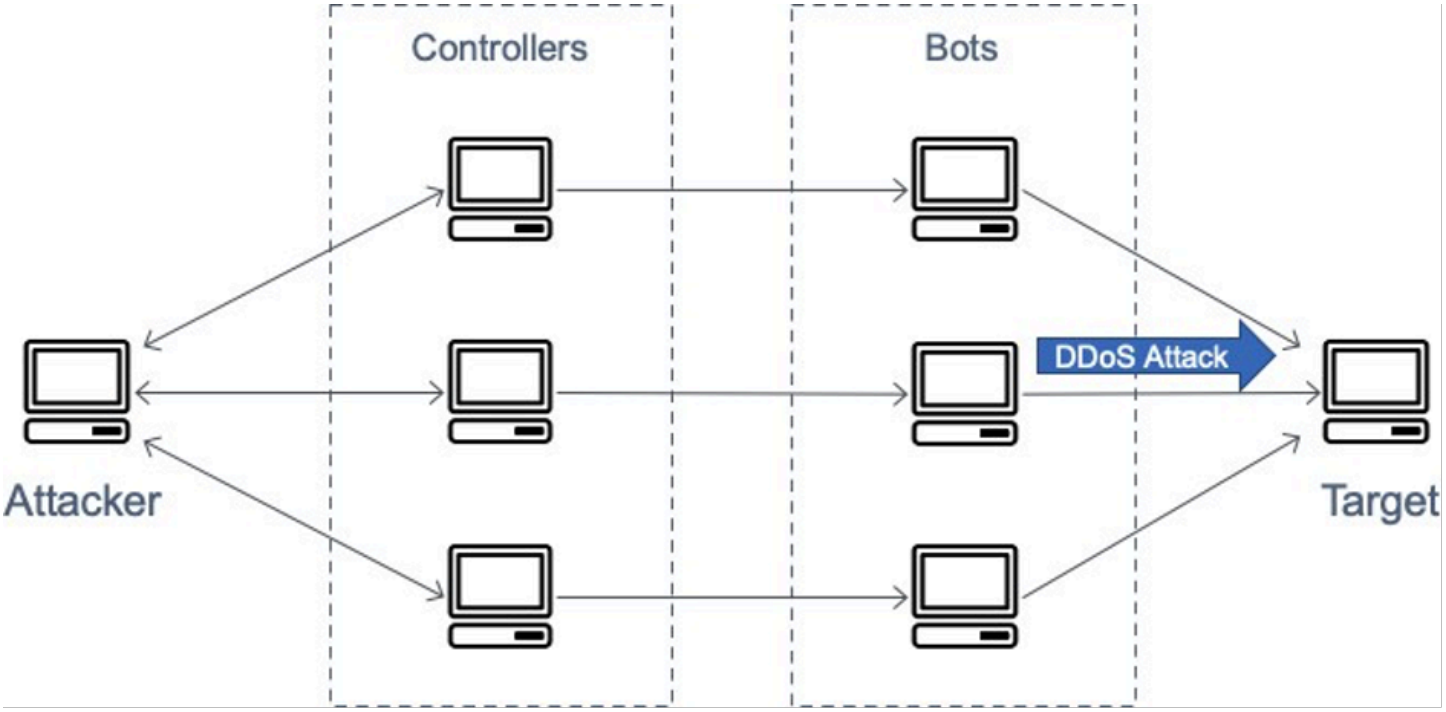
참조 아키텍처 배포, 다이어그램, 백서 등 클라우드 아키텍처에 대한 전문가 지침 및 모범 사례에 대한 자세한 내용은 아키텍처 센터를 참조하십시오.AWS

서비스 거부 공격 소개

DoS (DoS) 공격 또는 이벤트는 웹 사이트 또는 애플리케이션에 네트워크 트래픽이 폭주하는 등 사용자가 웹 사이트 또는 애플리케이션을 사용할 수 없게 만들려는 의도적인 시도입니다. 공격자는 많은 양의 네트워크 대역폭을 소비하거나 다른 시스템 리소스를 묶어 합법적인 사용자의 액세스를 방해하는 다양한 기법을 사용합니다. 가장 간단한 형태는 다음 그림과 같이 고독한 공격자가 단일 소스를 사용하여 표적에 대한 DoS 공격을 수행하는 것입니다.

DoS 공격을 나타내는 다이어그램

분산 서비스 거부 (DDoS) 공격에서 공격자는 여러 소스를 사용하여 표적에 대한 공격을 조직합니다. 이러한 소스에는 멀웨어에 감염된 컴퓨터, 라우터, IoT 장치 및 기타 엔드포인트의 분산된 그룹이 포함될 수 있습니다. 다음 그림은 공격에 가담하여 대량의 패킷 또는 요청을 생성하여 대상을 압도하는 손상된 호스트의 네트워크를 보여줍니다.



공격을 묘사한 다이어그램 DDoS

오픈 시스템 상호 연결 (OSI) 모델에는 7개의 계층이 있으며 다음 표에 설명되어 있습니다. DDoS공격은 계층 3, 4, 6, 7에서 가장 흔합니다.

- 계층 3 및 4 공격은 OSI 모델의 네트워크 및 전송 계층에 해당합니다. 이 백서에서는 이러한 공격을 AWS 총칭하여 인프라 계층 공격이라고 합니다.
- 계층 6 및 7 공격은 모델의 프레젠테이션 및 애플리케이션 계층에 OSI 해당합니다. 이 백서에서는 이러한 공격을 애플리케이션 계층 공격으로 통합하여 다룹니다.

이 백서에서는 다음 섹션에서 이러한 공격 유형에 대해 설명합니다.

표 1 — 모델 OSI

#	계층	단위	설명	벡터 예제
7	애플리케이션	데이터	애플리케이션으로의 네트워크 프로세스	HTTP플러드, DNS 쿼리 플러드
6	표시	데이터	데이터 표현 및 암호화	전송 계층 보안 (TLS) 남용
5	세션	데이터	호스트 간 통신	N/A
4	운송	세그먼트	E nd-to-end 연결 및 안정성	플러드 동기화 (SYN)
3	네트워크	패킷	경로 결정 및 논리적 주소 지정	사용자 데이터그램 프로토콜 (UDP) 리플렉션 공격
2	데이터 링크	Frames(프레임)	물리적 주소 지정	N/A
1	물리적	비트	미디어, 신호 및 바이너리 전송	N/A

인프라 계층 공격

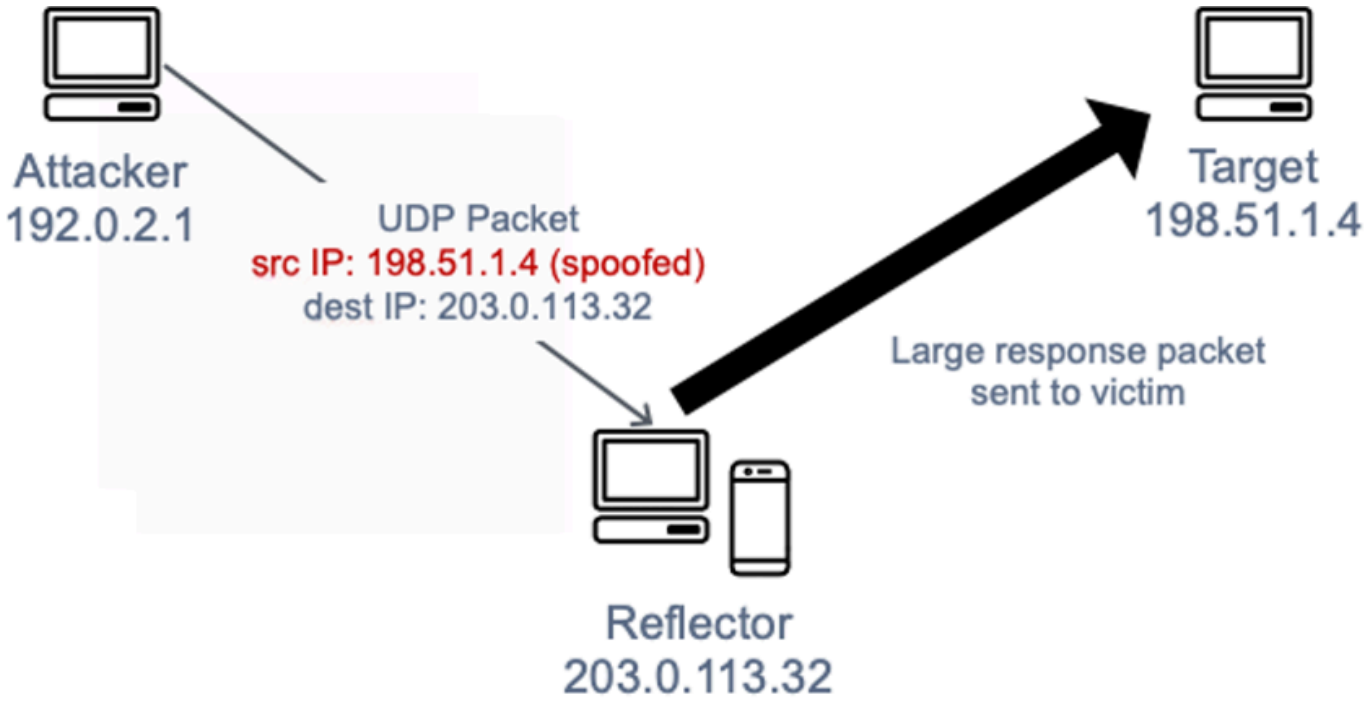
가장 일반적인 DDoS 공격인 사용자 데이터그램 프로토콜 (UDP) 반사 공격과 SYN 플러드는 인프라 계층 공격입니다. 공격자는 이러한 방법 중 하나를 사용하여 대량의 트래픽을 생성하여 네트워크 용량을 폭주시키거나 서버, 방화벽, 침입 방지 시스템 () 또는 로드 밸런서와 같은 시스템의 리소스를 제한할 수 있습니다. IPS 이러한 공격은 식별하기 쉽지만 효과적으로 방어하려면 인바운드 트래픽 플러드보다 더 빠르게 용량을 확장할 수 있는 네트워크나 시스템이 있어야 합니다. 이러한 추가 용량은 공격 트래픽을 필터링하거나 흡수하여 시스템과 애플리케이션이 합법적인 고객 트래픽에 대응할 수 있도록 하는 데 필요합니다.

UDP리플렉션 공격

UDP리플렉션 UDP 공격은 스테이트리스 프로토콜이라는 사실을 악용합니다. 공격자는 공격 대상의 IP 주소를 UDP 원본 IP 주소로 나열하는 유효한 UDP 요청 패킷을 만들 수 있습니다. 공격자는 이제 요청 패킷의 소스 IP를 위조하여 스푸핑했습니다UDP. UDP패킷에는 스푸핑된 소스 IP가 포함되어 있으며 공격자는 패킷을 중간 서버로 보냅니다. 서버는 속아 공격자의 IP 주소로 돌아가지 않고 표적이 된 피해자 IP로 UDP 응답 패킷을 보내도록 속입니다. 중간 서버가 사용되는 이유는 요청 패킷보다 몇 배 더 큰 응답을 생성하여 대상 IP 주소로 전송되는 공격 트래픽의 양을 효과적으로 증폭시키기 때문입니다.

증폭 요소는 요청 크기에 대한 응답 크기의 비율이며, 공격자가 사용하는 프로토콜 (), 네트워크 시간 프로토콜 ()DNS, 단순 서비스 디렉터리 프로토콜 (NTP), 무연결 경량 디렉터리 액세스 프로토콜 (SSDP), Memcached, Character Generator Protocol (CharGen) 또는 Quote of the day (QOTD) 에 따라 달라집니다. CLDAP

예를 들어 의 증폭 인자는 원래 바이트 수의 28~54배일 DNS 수 있습니다. 따라서 공격자가 64바이트의 요청 페이로드를 DNS 서버로 보내는 경우 공격 대상에게 3400바이트가 넘는 원치 않는 트래픽을 생성할 수 있습니다. UDP리플렉션 공격은 다른 공격에 비해 트래픽 양이 더 많습니다. 다음 그림은 반사 전략과 증폭 효과를 보여줍니다.

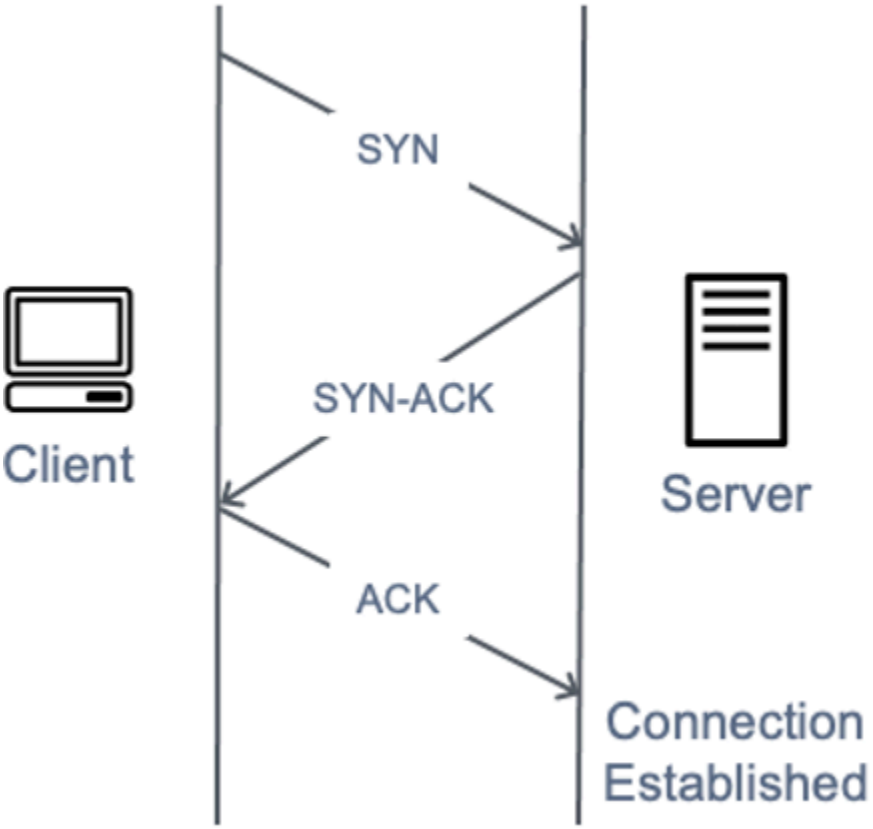


리플렉션 공격을 묘사한 UDP 다이어그램

참고로 리플렉션 공격은 공격자에게 “무료” 증폭을 제공하기는 하지만 IP 스푸핑 기능을 필요로 하고, Source Address Validation Everywhere (SAVE) 를 채택하는 네트워크 제공자의 수가 늘어남에 따라 이 기능이 제거되면서 DDoS 서비스 제공업체는 리플렉션 공격을 중단하거나 소스 주소 검증을 구현하지 않는 데이터 센터 및 네트워크 제공자로 재배치해야 합니다. BCP38

SYN플러드 공격

사용자가 웹 서버와 같은 전송 제어 프로토콜 (TCP) 서비스에 연결하면 클라이언트가 SYN 패킷을 보냅니다. 서버가 동기화 승인 (SYN-ACK) 패킷을 반환하고, 마지막으로 클라이언트는 확인 () 패킷으로 응답하여 예상된 3방향 핸드셰이크를 완료합니다. ACK 다음 이미지는 이러한 일반적인 핸드셰이크를 보여줍니다.



3방향 핸드셰이크를 묘사한 다이어그램 SYN

SYN플러드 공격에서 악의적인 클라이언트는 대량의 SYN 패킷을 보내지만 핸드셰이크를 완료하기 위해 최종 ACK 패킷을 보내지는 않습니다. 서버는 반쯤 열린 TCP 연결에 대한 응답을 기다리게 되며, 결국 타겟이 새 연결을 받아들일 수 있는 용량이 부족해져 새 TCP 사용자가 서버에 연결할 수 없게 된다는 것이 관건이지만, 실제 영향은 미미합니다. 최신 운영 체제는 모두 플러드 SYN 공격으로 인한 상태 테이블 고갈에 대응하기 위한 메커니즘으로 기본적으로 쿠키를 구현합니다. SYN SYN대기열 길이가 미리 정해진 임계값에 도달하면 서버는 대기열에 항목을 만들지 않고 조작된 초기 시퀀스 번호가 ACK 포함된 SYN -로 응답합니다. SYN 그러면 서버가 올바르게 증가된 확인 번호가 ACK 포함된 메시지를 수신하면 해당 항목을 상태 테이블에 추가하고 정상적으로 작업을 진행할 수 있습니다. SYN플러드가 대상 장치에 미치는 실제 영향은 네트워크 용량 및 CPU 고갈인 경향이 있지만 방화벽 (또는 EC2 보안 그룹 연결 추적) 과 같은 중간 상태 저장 장치는 상태 테이블을 고갈시키고 새 연결을 끊을 수 있습니다. TCP

TCP미들박스 리플렉션

비교적 새로운 공격 경로는 2021년 8월에 발표된 학술 백서에 처음 공개되었습니다. 이 백서에서는 국가 방화벽과 상용 방화벽 모두에서 TCP 규정을 준수하지 않을 경우 이러한 방화벽이 어떻게 이러한 방

화벽을 속여 증폭 매개체로 작용할 수 있는지를 설명했습니다. TCP 이러한 공격은 2022년 초부터 “야생에서” 발생했으며 오늘날에도 계속 목격되고 있습니다. 이 “기능”을 구현한 공급업체의 다양한 방식에 따라 증폭 요인은 다르지만 Memcached UDP 증폭을 넘어설 수 있습니다.

애플리케이션 계층 공격

공격자는 계층 7 또는 애플리케이션 계층 공격을 사용하여 애플리케이션 자체를 표적으로 삼을 수 있습니다. 이러한 공격에서 공격자는 SYN 플러드 인프라 공격과 마찬가지로 응용 프로그램의 특정 기능에 과부하를 일으켜 합법적인 사용자가 응용 프로그램을 사용할 수 없게 하거나 응답하지 못하게 하려고 합니다. 소량의 네트워크 트래픽만 생성하여 요청 양이 매우 적은 경우에도 이러한 문제가 발생할 수 있습니다. 이로 인해 공격을 탐지하고 완화하기 어려울 수 있습니다. 애플리케이션 계층 공격의 예로는 HTTP 플러드, 캐시 버스팅 공격, - 플러드 등이 있습니다. WordPress XML RPC

- HTTP플러드 공격에서 공격자는 웹 애플리케이션의 유효한 사용자가 보낸 것으로 보이는 HTTP 요청을 보냅니다. 일부 HTTP 플러드는 특정 리소스를 대상으로 하는 반면, 더 복잡한 HTTP 플러드는 애플리케이션과 사람의 상호 작용을 모방하려고 시도합니다. 이로 인해 요청 속도 제한과 같은 일반적인 완화 기법을 사용하기가 더 어려워질 수 있습니다.
- 캐시 무효화 공격은 쿼리 문자열의 변형을 사용하여 콘텐츠 전송 네트워크 () 캐싱을 우회하는 HTTP 플러드의 일종입니다. CDN 캐시된 결과를 반환하는 대신 모든 페이지 요청을 오리진 서버에 CDN 연결해야 하는데, 이러한 오리진 페치는 애플리케이션 웹 서버에 추가적인 부담을 줍니다.
- WordPress핑백 RPC플러드라고도 하는 WordPress XML - 플러드 공격을 사용하면 공격자는 콘텐츠 관리 소프트웨어에서 호스팅되는 웹 사이트를 표적으로 삼습니다. WordPress 공격자는 XML-RPC API 함수를 오용하여 많은 요청을 생성합니다. HTTP 핑백 기능을 사용하면 WordPress (사이트 A) 에서 호스팅되는 웹 사이트가 사이트 A가 WordPress 사이트 B로 연결한 링크를 통해 다른 사이트 (사이트 B) 에 알린 다음 사이트 A를 페치하여 링크의 존재 여부를 확인할 수 있습니다. 핑백 플러드에서 공격자는 이 기능을 악용하여 사이트 B가 사이트 A를 공격하도록 합니다. 이러한 유형의 공격에는 일반적으로 HTTP 요청 헤더의 User-Agent에 `WordPress: “"` 라는 명확한 서명이 있습니다.

애플리케이션의 가용성에 영향을 줄 수 있는 다른 형태의 악성 트래픽도 있습니다. 스크레이퍼 봇은 웹 애플리케이션에 액세스하여 콘텐츠를 훔치거나 가격과 같은 경쟁 정보를 기록하려는 시도를 자동화합니다. 무차별 대입 공격 및 크리덴셜 스터핑 공격은 애플리케이션의 보안 영역에 무단으로 액세스하기 위해 프로그래밍된 공격입니다. 엄밀히 말하면 이러한 DDoS 공격은 아니지만, 자동화된 특성은 DDoS 공격과 비슷해 보일 수 있으며 이 백서에서 다루는 것과 동일한 모범 사례를 구현하여 공격을 완화할 수 있습니다.

애플리케이션 계층 공격은 Domain Name System (DNS) 서비스를 대상으로 할 수도 있습니다. 이러한 공격 중 가장 흔한 것은 공격자가 여러 개의 올바른 형식의 DNS 쿼리를 사용하여 서버의 리소스를 고갈시키는 DNS쿼리 폭주입니다. DNS 이러한 공격에는 공격자가 하위 도메인 문자열을 무작위로 지정하여 특정 확인자의 로컬 캐시를 우회하는 캐시 무효화 구성 요소도 포함될 수 있습니다. DNS 따라서 확인자는 캐시된 도메인 쿼리를 이용할 수 없고 대신 신뢰할 수 있는 서버에 반복적으로 접속해야 하므로 공격이 증폭됩니다. DNS

전송 계층 보안 (TLS) 을 통해 웹 응용 프로그램을 제공하는 경우 공격자는 협상 프로세스를 공격할 수도 있습니다. TLS TLS계산 비용이 많이 들기 때문에 공격자는 읽을 수 없는 데이터 (또는 이해할 수 없는 데이터 (암호문)) 를 합법적인 핸드셰이크로 처리하기 위해 서버에 추가 워크로드를 생성하여 서버의 가용성을 떨어뜨릴 수 있습니다. 이 공격의 변형으로 공격자는 핸드셰이크를 완료하지만 암호화 방법을 계속 재협상합니다. TLS 또는 공격자는 여러 세션을 열고 닫아 서버 리소스를 고갈시키려 할 수도 있습니다. TLS

완화 기법

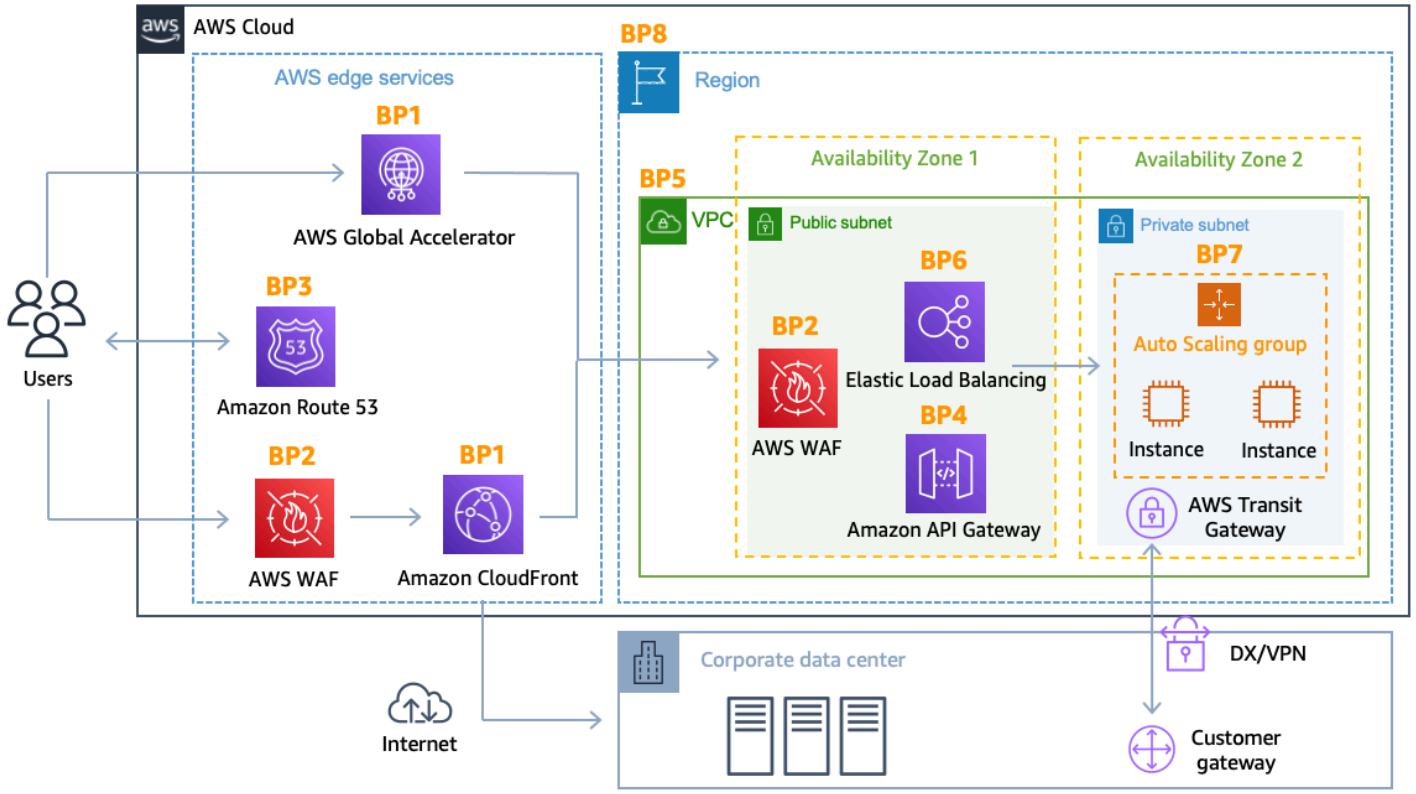
일부 형태의 DDoS 완화 기능은 서비스에 자동으로 포함됩니다. AWS DDoS다음 섹션에서 설명하는 특정 서비스가 포함된 AWS 아키텍처를 사용하고 사용자와 애플리케이션 간 네트워크 흐름의 각 부분에 대한 추가 모범 사례를 구현하면 복원력을 더욱 개선할 수 있습니다.

Amazon, AWS Global Accelerator CloudFront, Amazon Route 53과 같은 엣지 로케이션에서 운영되는 AWS 서비스를 사용하여 알려진 모든 인프라 계층 공격에 대한 포괄적인 가용성 보호를 구축할 수 있습니다. 이러한 서비스는 AWS 글로벌 에지 네트워크의 일부이며, 전 세계에 분산된 엣지 로케이션에서 모든 유형의 애플리케이션 트래픽을 처리할 때 애플리케이션의 DDoS 복원력을 개선할 수 있습니다. 어느 곳에서나 AWS 리전애플리케이션을 실행하고 이러한 서비스를 사용하여 애플리케이션 가용성을 보호하고 합법적인 최종 사용자를 위해 애플리케이션 성능을 최적화할 수 있습니다.

Amazon CloudFront, 글로벌 액셀러레이터, Amazon Route 53을 사용하면 다음과 같은 이점이 있습니다.

- AWS 글로벌 에지 네트워크 전반에서 인터넷 및 DDoS 완화 용량에 액세스할 수 있습니다. 이는 테라비트 규모에 이를 수 있는 대규모 공격을 완화하는 데 유용합니다.
- AWS Shield DDoS완화 시스템은 AWS 에지 서비스와 통합되어 몇 분에서 1초 미만으로 time-to-mitigate 단축됩니다.
- 스테이트리스 SYN 플러드 완화 기능은 들어오는 연결을 보호 서비스에 전달하기 전에 SYN 쿠키를 사용하여 들어오는 연결을 확인합니다. 이렇게 하면 유효한 연결만 애플리케이션에 도달할 수 있고 합법적인 최종 사용자는 오탐지가 발생하지 않도록 보호할 수 있습니다.
- 대규모 공격의 영향을 분산하거나 격리하는 자동 트래픽 엔지니어링 시스템. DDoS 이러한 모든 서비스는 공격이 오리진에 도달하기 전에 소스에서 공격을 격리하므로 이러한 서비스로 보호되는 시스템에 미치는 영향이 줄어듭니다.
- 애플리케이션 계층 방어와 함께 CloudFront 사용하면 AWS WAF현재 애플리케이션 아키텍처 (예: 온프레미스 데이터 센터) 를 AWS 리전 변경할 필요가 없습니다.

인바운드 데이터 전송에는 요금이 부과되지 않으며 이를 통해 AWS 차단되는 DDoS 공격 트래픽에 대해서는 비용을 지불하지 않습니다. AWS Shield다음 아키텍처 다이어그램에는 AWS 글로벌 에지 네트워크 서비스가 포함되어 있습니다.



DDoS-복원력이 뛰어난 레퍼런스 아키텍처

이 아키텍처에는 공격에 대한 웹 애플리케이션의 복원력을 향상시키는 데 도움이 되는 여러 AWS 서비스가 포함되어 있습니다. DDoS 다음 표에는 이러한 서비스와 해당 서비스가 제공할 수 있는 기능이 요약되어 있습니다. AWS 이 문서에서 쉽게 참조할 수 있도록 각 서비스에 모범 사례 지표 (BP1,BP2) 태그를 붙였습니다. 예를 들어 다음 섹션에서는 모범 사례 지표를 포함하여 CloudFront Amazon과 Global Accelerator에서 제공하는 기능에 대해 설명합니다. BP1

표 2 - 모범 사례 요약

	AWS 엣지			AWS 리전		
	Amazon CloudFront (BP1) 을 () 와 함께 AWS WAF 사용 BP2	글로벌 액셀러레이터 사용 () BP1	아마존 루트 53 사용 (BP3)	(BP6) 와 함께 Elastic Load Balancing AWS WAF (BP2) 사용	ACLsAmazon에서 보안 그룹 및 네트워크 사용 VPC (BP5)	아마존 엘라스틱 컴퓨트 클라우드 (AmazonEC2) Auto

	AWS 엣지			AWS 리전		
						Scaling (BP7) 사용
레이어 3 (예: UDP 리플렉션) 공격 완화	✓	✓	✓	✓	✓	✓
레이어 4 (예: SYN 플러드) 공격 완화	✓	✓	✓	✓		
레이어 6 (예:TLS) 공격 완화	✓	✓	✓	✓		
공격 표면 감소	✓	✓	✓	✓	✓	
애플리케이션 계층 트래픽을 흡수하도록 확장할 수 있습니다.	✓	✓	✓	✓	✓	✓
계층 7 (애플리케이션 계층) 공격 완화	✓	✓(*)	✓	✓	✓(*)	✓(*)

	AWS 엣지			AWS 리전		
과도한 트래픽과 대규모 공격의 지리적 격리 및 분산 DDoS	✓	✓	✓			

✓ (*): Application Load AWS WAF Balancer와 함께 사용하는 경우

DDoS공격에 대응하고 공격을 방어하기 위한 준비 상태를 개선하는 또 다른 방법은 구독하는 것입니다. AWS Shield Advanced사용의 이점은 다음과 같습니다. AWS Shield Advanced

- 애플리케이션 가용성에 영향을 미치는 DDoS 공격을 완화하는 데 필요한 지원을 위해 AWS Shield 대응팀 (AWS SRT) 의 연중무휴 전문 지원을 이용할 수 있으며, 여기에는 선택적 사전 참여 기능이 포함됩니다.
- 트래픽을 DDoS 완화 시스템으로 조기에 라우팅하고 엘라스틱 IP 주소와 함께 사용할 경우 Amazon EC2 (Elastic Load Balancer 포함) 또는 Network Load Balancer에 대한 time-to-mitigate 공격을 개선할 수 있는 민감한 탐지 임계값
- 다음과 함께 사용할 경우 애플리케이션의 기준 트래픽 패턴을 기반으로 하는 맞춤형 계층 7 탐지 AWS WAF
- Shield Advanced가 사용자 지정 규칙을 생성, 평가 및 배포하여 탐지된 DDoS 공격에 대응하는 자동 애플리케이션 계층 DDoS 완화 AWS WAF
- 애플리케이션 계층 DDoS 공격 완화를 위해 추가 비용 없이 액세스 가능 (Amazon CloudFront 또는 Application Load Balancer와 함께 사용하는 경우) AWS WAF
- 추가 비용 없이 보안 정책을 중앙 집중식으로 관리합니다. AWS Firewall Manager
- 공격으로 인한 규모 조정 관련 비용을 제한적으로 환불해 줄 수 있는 비용 보호. DDoS
- 고객별로 적용되는 AWS Shield Advanced 향상된 서비스 수준 계약.
- 보호 그룹을 사용하면 리소스를 묶을 수 있으며, 여러 리소스를 단일 단위로 취급하여 애플리케이션의 탐지 및 완화 범위를 사용자 지정하는 셀프 서비스 방식을 제공합니다. 보호 그룹에 대한 자세한 내용은 Shield Advanced 보호 그룹을 참조하십시오.
- DDoSAWS Management Console,API, Amazon CloudWatch 지표와 경보를 사용하여 공격을 파악할 수 있습니다.

이 선택적 DDoS 완화 서비스는 어느 곳에서나 호스팅되는 애플리케이션을 보호하는 데 도움이 됩니다. AWS 리전이 서비스는 Route 53 및 글로벌 액셀러레이터에서 전 세계적으로 사용할 수 있습니다. CloudFront 지역적으로는 Application Load Balancer, Classic Load Balancer 및 엘라스틱 IP 주소를 보호하여 Network Load Balancer () 또는 Amazon 인스턴스를 보호할 수 있습니다. NLBs EC2

전체 AWS Shield Advanced 기능 목록과 이에 AWS Shield대한 자세한 내용은 작동 방식을 참조하십시오. AWS Shield

DDoS완화 모범 사례

다음 섹션에서는 각 권장 DDoS 완화 모범 사례에 대해 자세히 설명합니다. 정적 또는 동적 웹 애플리케이션을 위한 DDoS 완화 계층을 구축하는 방법에 대한 간략한 easy-to-implement 지침은 Amazon CloudFront 및 Amazon Route 53을 사용하여 DDoS 공격으로부터 동적 웹 애플리케이션을 보호하는 방법을 참조하십시오.

인프라 계층 방어 (BP1,, BP3BP6,BP7)

기존 데이터 센터 환경에서는 용량 오버프로비저닝, 완화 시스템 배포 또는 DDoS 완화 서비스를 통한 트래픽 스크러빙과 같은 기술을 사용하여 인프라 계층 DDoS 공격을 완화할 수 있습니다. DDoS 활성화되면 DDoS 완화 기능이 자동으로 제공되지만 AWS, 이러한 기능을 가장 잘 활용하고 과도한 트래픽에 대비해 확장할 수 있는 아키텍처를 선택하여 애플리케이션의 DDoS 복원력을 최적화할 수 있습니다.

대량 DDoS 공격을 완화하는 데 도움이 되는 주요 고려 사항에는 충분한 전송 용량과 다양성을 확보하고 Amazon EC2 인스턴스와 같은 AWS 리소스를 공격 트래픽으로부터 보호하는 것이 포함됩니다.

일부 Amazon EC2 인스턴스 유형은 대용량 트래픽을 보다 쉽게 처리할 수 있는 기능 (예: 최대 100Gbps의 네트워크 대역폭 인터페이스 및 향상된 네트워킹) 을 지원합니다. 이를 통해 Amazon EC2 인스턴스에 도달한 트래픽의 인터페이스 혼잡을 방지할 수 있습니다. 향상된 네트워킹을 지원하는 인스턴스는 기존 구현에 비해 더 높은 입출력 (I/O) 성능, 더 높은 대역폭, 낮은 CPU 사용률을 제공합니다. 이를 통해 인스턴스의 대용량 트래픽 처리 능력이 향상되고 궁극적으로 초당 패킷 수 (pps) 부하에 대한 복원력이 높아집니다.

이러한 높은 수준의 복원력을 허용하려면 Amazon EC2 전용 인스턴스 또는 “N" 접미사가 있고 네트워크 대역폭이 최대 100Gbps인 향상된 네트워킹을 지원하는 네트워킹 처리량이 더 높은 Amazon EC2 인스턴스 `c5n.18xlarge` 또는 메탈 인스턴스 (예:) 를 사용하는 것이 좋습니다. AWS `c6gn.16xlarge` `c5n.metal`

100기가비트 네트워크 인터페이스와 향상된 네트워킹을 지원하는 Amazon EC2 인스턴스에 대한 자세한 내용은 Amazon EC2 인스턴스 유형을 참조하십시오.

향상된 네트워킹에 필요한 모듈과 필수 `enaSupport` 속성 세트는 Amazon Linux 2 및 최신 버전의 Amazon Linux에 포함되어 AMI 있습니다. 따라서 지원되는 인스턴스 유형에서 Amazon Linux의 하드웨어 가상 머신 (HVM) 버전으로 인스턴스를 시작하면 인스턴스에 향상된 네트워킹이 이미 활성화되어 있습니다. 자세한 내용은 향상된 네트워킹 활성화 여부 테스트 및 Linux에서의 향상된 네트워킹을 참조하십시오.

Auto EC2 Scaling을 지원하는 아마존 (BP7)

인프라 및 애플리케이션 계층 공격을 모두 완화하는 또 다른 방법은 대규모로 운영하는 것입니다. 웹 애플리케이션이 있는 경우 로드 밸런서를 사용하여 오버프로비저닝되거나 자동으로 확장되도록 구성된 여러 Amazon EC2 인스턴스로 트래픽을 분산할 수 있습니다. 이러한 인스턴스는 플래시 크라우드 또는 애플리케이션 계층 공격을 포함하여 어떤 이유로든 발생하는 갑작스러운 트래픽 급증을 처리할 수 있습니다. DDoS 사용자가 정의한 이벤트 (예: 네트워크 I/O 및 사용자 지정 지표) 에 따라 Amazon EC2 플릿 크기를 자동으로 조정하도록 Auto Scaling을 시작하도록 Amazon CloudWatch 경보를 설정할 수 있습니다. CPU RAM

이 접근 방식은 요청량이 예기치 않게 증가할 때 애플리케이션 가용성을 보호합니다. Amazon CloudFront, 애플리케이션 로드 밸런서, 클래식 로드 밸런서 또는 Network Load Balancer를 애플리케이션과 함께 사용하는 TLS 경우 협상은 배포 (CloudFrontAmazon) 또는 로드 밸런서에서 처리합니다. 이러한 기능은 합법적인 요청과 오용 공격을 처리하도록 확장하여 TLS 기반 공격의 영향을 받지 않도록 인스턴스를 보호하는 데 도움이 됩니다. TLS

Amazon을 사용하여 Auto CloudWatch Scaling을 호출하는 방법에 대한 자세한 내용은 Auto Scaling 그룹 및 인스턴스에 대한 Amazon CloudWatch 측정치 모니터링을 참조하십시오.

EC2Amazon은 크기 조정이 가능한 컴퓨팅 파워를 제공하므로 요구 사항의 변화에 따라 빠르게 규모를 확장하거나 축소할 수 있습니다. Amazon EC2 Auto Scaling 그룹의 크기를 조정하여 애플리케이션에 인스턴스를 자동으로 추가하여 수평적으로 확장할 수 있고, 더 큰 EC2 인스턴스 유형을 사용하여 수직으로 확장할 수 있습니다.

Amazon RDS Proxy를 사용하면 애플리케이션이 데이터베이스 연결을 풀링하고 공유하도록 허용하여 애플리케이션이 데이터베이스 트래픽의 예상치 못한 급증을 확장하고 처리하는 능력을 개선할 수 있습니다. Amazon RDS 데이터베이스 인스턴스에 대해 스토리지 자동 크기 조정을 활성화할 수도 있습니다. 자세한 내용은 Amazon RDS 스토리지 자동 확장을 통한 자동 용량 관리를 참조하십시오.

Elastic Load Balancing (BP6)

대규모 DDoS 공격은 단일 Amazon EC2 인스턴스의 용량을 압도할 수 있습니다. Elastic Load Balancing (ELB) 을 사용하면 많은 백엔드 인스턴스에 트래픽을 분산하여 애플리케이션 과부하 위험

을 줄일 수 있습니다. Elastic Load Balancing은 자동으로 확장할 수 있으므로, 예를 들어 플래시 크라우드나 공격으로 인해 예상치 못한 추가 트래픽이 발생할 경우 더 큰 볼륨을 관리할 수 있습니다. DDoS VPC아마존에서 빌드한 애플리케이션의 경우 애플리케이션 유형에 따라 애플리케이션 로드 밸런서 (), 네트워크 로드 밸런서 (ALB), 클래식 로드 밸런서 () 등 세 가지 유형을 고려해야 합니다. ELBs NLB CLB

웹 애플리케이션의 경우 Application Load Balancer를 사용하여 콘텐츠를 기반으로 트래픽을 라우팅하고 올바른 형식의 웹 요청만 수락할 수 있습니다. Application Load Balancer는 SYN 플러드 또는 UDP 리플렉션 공격과 같은 여러 가지 일반적인 DDoS 공격을 차단하여 애플리케이션을 공격으로부터 보호합니다. Application Load Balancer는 이러한 유형의 공격이 탐지되면 추가 트래픽을 흡수하도록 자동으로 확장됩니다. 인프라 계층 공격으로 인한 규모 조정 활동은 AWS 고객에게 투명하며 청구서에는 영향을 미치지 않습니다.

Application Load Balancer를 사용하여 웹 애플리케이션을 보호하는 방법에 대한 자세한 내용은 애플리케이션 로드 밸런서 시작하기를 참조하십시오.

HTTP/이외의 HTTPS 애플리케이션의 경우 Network Load Balancer를 사용하여 매우 짧은 지연 시간으로 트래픽을 대상 (예: Amazon EC2 인스턴스) 으로 라우팅할 수 있습니다. Network Load Balancer의 주요 고려 사항 중 하나는 유효한 리스너의 로드 밸런서에 도달하는 모든 TCP SYN 또는 UDP 트래픽이 흡수되지 않고 대상으로 라우팅된다는 것입니다. 하지만 연결을 종료하는 TLS -listeners에는 적용되지 않습니다. TCP TCP리스너가 있는 네트워크 로드 밸런서의 경우 플러드를 방지하기 위해 글로벌 액셀러레이터를 배포하는 것이 좋습니다. SYN

Shield Advanced를 사용하여 엘라스틱 IP 주소에 대한 DDoS 보호를 구성할 수 있습니다. 가용 영역별로 엘라스틱 IP 주소를 Network Load Balancer에 할당하면 Shield Advanced는 Network Load Balancer DDoS 트래픽에 대한 관련 보호를 적용합니다.

Network Load Balancer를 사용한 보호 TCP 및 UDP 애플리케이션에 대한 자세한 내용은 네트워크 로드 밸런서 시작하기를 참조하십시오.

> **Note**
>
> 보안 그룹 구성에 따라 연결 추적을 사용하여 트래픽에 대한 정보를 추적하려면 보안을 사용하는 리소스가 필요합니다. 이 경우 추적되는 연결 수가 제한되므로 로드 밸런서가 새 연결을 처리하는 기능에 영향을 미칠 수 있습니다.
> IP 주소 (예: `0.0.0.0/0` 또는`::/0`) 의 트래픽을 수락하는 인그레스 규칙이 포함되어 있지만 응답 트래픽을 허용하는 해당 규칙이 없는 보안 그룹 구성은 보안 그룹이 연결 추적 정보를 사용하여 응답 트래픽이 전송되도록 허용합니다. DDoS공격이 발생할 경우 추적된 최대 연결 수가 소진될 수 있습니다. 공용 Application Load Balancer 또는 Classic Load Balancer의 DDoS

복원력을 개선하려면 로드 밸런서와 연결된 보안 그룹이 연결 추적 (추적되지 않은 연결) 을 사용하지 않도록 구성하여 트래픽 흐름에 연결 추적 제한이 적용되지 않도록 해야 합니다.
이를 위해 인바운드 규칙이 모든 IP 주소 (`0.0.0.0/0`또는`::/0`) 의 TCP 흐름을 받아들이도록 허용하는 규칙으로 보안 그룹을 구성하고, 이 리소스가 응답 트래픽 (모든 IP 주소에 대한 아웃바운드 범위 허용 `0.0.0.0/0` 또는 모든 포트 (0-65535`::/0`) 을 전송할 수 있도록 아웃바운드 방향에 해당 규칙을 추가하여 응답 트래픽이 추적 정보가 아닌 보안 그룹 규칙을 기반으로 허용되도록 합니다. 이 구성을 사용하면 Classic 및 Application Load Balancer에 로드 밸런서 노드에 대한 새 연결 설정에 영향을 미칠 수 있는 배기 연결 추적 제한이 적용되지 않으므로 공격 발생 시 트래픽 증가에 따라 확장할 수 있습니다. DDoS 추적되지 않은 연결에 대한 자세한 내용은 보안 그룹 연결 추적: 추적되지 않은 연결을 참조하십시오.
보안 그룹 연결 추적을 피하면 DDoS 트래픽이 보안 그룹에서 허용한 소스에서 발생하는 경우에만 도움이 됩니다. 보안 그룹에서 허용되지 않는 소스의 DDoS 트래픽은 연결 추적에 영향을 주지 않습니다. 이러한 경우에는 연결 추적을 피하도록 보안 그룹을 재구성할 필요가 없습니다. 예를 들어, 보안 그룹 허용 목록이 회사 방화벽이나 신뢰할 수 있는 VPN IPs 송신 등과 같이 신뢰도가 높은 IP 범위로 구성된 경우에는 더욱 그렇습니다. CDNs

확장 (BP1,) 에는 AWS 엣지 로케이션을 사용하십시오. BP3

확장성이 뛰어나고 다양한 인터넷 연결에 액세스하면 지연 시간과 사용자 처리량을 최적화하고, DDoS 공격을 흡수하고, 결함을 격리하는 동시에 애플리케이션 가용성에 미치는 영향을 최소화하는 능력이 크게 향상될 수 있습니다. AWS 엣지 로케이션은 Amazon CloudFront, 글로벌 액셀러레이터 및 Amazon Route 53을 사용하는 모든 웹 애플리케이션에 이러한 이점을 제공하는 네트워크 인프라의 추가 계층을 제공합니다. 이러한 서비스를 사용하면 애플리케이션을 실행하는 엣지에서 포괄적으로 보호할 수 있습니다. AWS 리전

엣지에서의 웹 애플리케이션 딜리버리 () BP1

CloudFront Amazon은 정적, 동적, 스트리밍 및 대화형 콘텐츠를 포함한 전체 웹 사이트를 전송하는 데 사용할 수 있는 서비스입니다. 캐시 가능한 콘텐츠를 제공하지 않는 경우에도 영구 연결 및 변수 time-to-live (TTL) 설정을 사용하여 오리진으로부터 트래픽을 오프로드할 수 있습니다. 이러한 CloudFront 기능을 사용하면 오리진에 다시 돌아가는 요청 및 TCP 연결 수가 줄어들어 웹 애플리케이션을 홍수로부터 보호하는 데 도움이 됩니다. HTTP

CloudFront 올바른 형식의 연결만 허용하므로 SYN 플러드 및 UDP 리플렉션 DDoS 공격과 같은 많은 일반적인 공격이 오리진에 도달하지 못하도록 방지할 수 있습니다. DDoS또한 공격은 소스 근처에서 지리적으로 격리되므로 트래픽이 다른 위치에 영향을 미치지 않습니다. 이러한 기능을 사용하면 대규

모 공격 중에도 사용자에게 트래픽을 계속 제공할 수 있는 능력이 크게 향상될 수 있습니다. DDoS 를 CloudFront 사용하여 인터넷상의 AWS 또는 다른 곳에서 오리진을 보호할 수 있습니다.

Amazon Simple Storage Service (Amazon S3) 를 사용하여 인터넷에서 정적 콘텐츠를 제공하는 경우 다음과 같은 이점을 제공하는 CloudFront Amazon을 사용하여 버킷을 보호할 AWS 것을 권장합니다.

- Amazon S3 버킷에 대한 액세스를 제한하여 공개적으로 액세스할 수 없도록 합니다.
- 최종 사용자 (사용자) 가 지정된 CloudFront 배포를 통해서만 버킷의 콘텐츠에 액세스할 수 있도록 합니다. 즉, 시청자가 버킷에서 직접 또는 의도하지 않은 배포를 통해 콘텐츠에 액세스하는 것을 방지합니다. CloudFront

이를 위해서는 Amazon S3에 인증된 요청을 CloudFront 전송하도록 구성하고 Amazon S3에서 인증된 요청에만 액세스를 허용하도록 구성하십시오. CloudFront CloudFront Amazon S3 오리진에 인증된 요청을 보내는 두 가지 방법, 즉 원본 액세스 제어 (OAC) 와 원본 액세스 ID (OAI) 를 제공합니다. 다음을 OAC 지원하므로 사용하는 것이 좋습니다.

- 2022년 12월 이후에 출시된 옵트인 지역을 AWS 리전포함한 모든 Amazon S3 버킷
- AWS KMS (SSE-) 를 사용한 Amazon S3 서버 측 암호화 KMS
- Amazon S3에 대한 동적 요청(PUT 및 DELETE)

OAC및 OAI 에 대한 자세한 내용은 Amazon S3 오리진에 대한 액세스 제한을 참조하십시오.

Amazon을 통한 웹 애플리케이션의 보호 및 성능 최적화에 대한 자세한 내용은 Amazon CloudFront 시작하기를 참조하십시오. CloudFront

AWS 글로벌 액셀러레이터 () 를 사용하여 오리진으로부터 멀리 떨어진 네트워크 트래픽을 보호하십시오. BP1

글로벌 액셀러레이터는 사용자 트래픽의 가용성과 성능을 최대 60% 향상시키는 네트워킹 서비스입니다. 이는 사용자와 가장 가까운 엣지 로케이션에서 트래픽을 수신하고 이를 AWS 글로벌 네트워크 인프라를 통해 애플리케이션으로 라우팅함으로써 가능합니다 (단일 또는 다중 실행). AWS 리전

Global Accelerator는 TCP 사용자와 가장 가까운 AWS 리전 위치에서의 성능을 기반으로 최적의 엔드포인트로 UDP 트래픽을 라우팅합니다. 애플리케이션에 장애가 발생하는 경우 Global Accelerator는 30초 내에 차상위 엔드포인트로 페일오버를 제공합니다. Global Accelerator는 AWS 글로벌 네트워크의 방대한 용량과 Shield와의 통합 (예: 새로운 연결 시도에 도전하고 합법적인 최종 사용자에게만 서비스를 제공하는 상태 비저장 SYN 프록시 기능) 을 사용하여 애플리케이션을 보호합니다.

애플리케이션이 지원되지 않는 프로토콜을 CloudFront 사용하거나 글로벌 고정 IP 주소가 필요한 웹 애플리케이션을 운영하는 경우에도 엣지에서의 웹 애플리케이션 딜리버리 모범 사례와 동일한 많은 이점을 제공하는 DDoS 탄력적인 아키텍처를 구현할 수 있습니다.

예를 들어 최종 사용자가 방화벽의 허용 목록에 추가할 수 있고 다른 AWS 고객은 사용하지 않는 IP 주소를 요구할 수 있습니다. 이러한 시나리오에서는 Global Accelerator를 사용하여 Application Load Balancer에서 실행되는 웹 애플리케이션을 보호하고 웹 애플리케이션 계층 요청 플러드를 탐지 및 완화할 수 있습니다. AWS WAF

글로벌 액셀러레이터를 사용하여 네트워크 트래픽을 보호하고 성능을 최적화하는 방법에 대한 자세한 내용은 글로벌 액셀러레이터 시작하기를 참조하십시오.

엣지에서의 도메인 이름 확인 () BP3

주제

- DNS가용성을 위해 Route 53 사용하기
- NXDOMAIN공격으로부터 비용을 보호할 수 있도록 Route 53 구성

DNS가용성을 위해 Route 53 사용하기

Amazon Route 53는 가용성과 확장성이 뛰어난 도메인 이름 시스템 (DNS) 서비스로서 트래픽을 웹 애플리케이션으로 전달하는 데 사용할 수 있습니다. 여기에는 트래픽 흐름, 건강 검사 및 모니터링, 지연 시간 기반 라우팅, 지역과 같은 고급 기능이 포함됩니다. DNS 이러한 고급 기능을 사용하면 서비스가 DNS 요청에 응답하는 방식을 제어하여 웹 애플리케이션의 성능을 개선하고 사이트 중단을 방지할 수 있습니다. 데이터 플레인 가용성이 100% 인 유일한 AWS 서비스입니다. SLA

Amazon Route 53은 셔플 샤딩 및 애니캐스트 스트라이핑과 같은 기술을 사용하므로 DNS 서비스가 공격의 대상이 되더라도 사용자가 애플리케이션에 액세스할 수 있습니다. DDoS

셔플 샤딩을 사용하면 위임 세트의 각 네임 서버가 고유한 엣지 로케이션 및 인터넷 경로 세트에 해당합니다. 따라서 내결함성이 향상되고 고객 간 중복이 최소화됩니다. 위임 세트의 한 이름 서버를 사용할 수 없는 경우 사용자는 다시 시도하여 다른 엣지에 있는 다른 이름 서버로부터 응답을 받을 수 있습니다.

애니캐스트 스트라이핑을 사용하면 최적의 위치에서 각 DNS 요청을 처리하여 네트워크 부하를 분산시키고 대기 시간을 줄일 수 있습니다. DNS 이를 통해 사용자는 더 빠르게 응답할 수 있습니다. 또한 Amazon Route 53는 DNS 쿼리 소스 및 볼륨에서 이상을 감지하고 신뢰할 수 있는 것으로 알려진 사용자의 요청에 우선 순위를 지정할 수 있습니다.

Amazon Route 53을 사용하여 사용자를 애플리케이션으로 라우팅하는 방법에 대한 자세한 내용은 Amazon Route 53 시작하기를 참조하십시오.

NXDOMAIN공격으로부터 비용을 보호할 수 있도록 Route 53 구성

NXDOMAIN공격자가 흔히 알려진 "정상" 확인자를 통해 존재하지 않는 하위 도메인에 대한 요청을 호스팅 영역에 대량으로 전송할 때 공격이 발생합니다. 이러한 공격의 목적은 재귀 확인자의 캐시 및/또는 신뢰할 수 있는 확인자의 가용성에 영향을 미치거나 호스팅 영역 레코드를 검색하기 위한 정찰의 한 형태일 수 있습니다. DNS Route 53을 신뢰할 수 있는 리졸버로 사용하면 가용성/성능에 미치는 영향을 줄일 수 있지만, 그 결과 월별 Route 53 비용이 크게 증가할 수 있습니다. 비용 증가를 방지하려면 다음 두 가지 조건에 모두 해당하는 경우 DNS 쿼리가 무료로 제공되는 Route 53 요금을 활용하십시오.

- 쿼리의 도메인 또는 하위 도메인 이름 (`example.com`또는`store.example.com`) 과 레코드 유형 (`A`) 은 별칭 레코드와 일치합니다.
- 별칭 대상은 다른 AWS Route 53 레코드가 아닌 리소스입니다.

예를 들어 EC2 인스턴스, Elastic Load Balancer CloudFront 또는 `*.example.com` 배포와 같은 AWS 리소스를 가리키는 유형 `A` (Alias) 을 사용하여 와일드카드 레코드를 생성하면 쿼리가 수행될 때 리소스의 IP가 반환되고 쿼리 `qwerty12345.example.com` 요금이 청구되지 않습니다.

애플리케이션 계층 방어 (,) BP1 BP2

지금까지 이 백서에서 설명한 많은 기술은 인프라 계층 DDoS 공격이 애플리케이션 가용성에 미치는 영향을 완화하는 데 효과적입니다. 또한 애플리케이션 계층 공격을 방어하려면 악의적인 요청을 구체적으로 탐지하고 이를 흡수할 수 있도록 확장하고 차단할 수 있는 아키텍처를 구현해야 합니다. 네트워크 기반 DDoS 완화 시스템은 일반적으로 복잡한 애플리케이션 계층 공격을 방어하는 데 효과가 없기 때문에 이는 중요한 고려 사항입니다.

악성 웹 요청 탐지 및 필터링 (,) BP1 BP2

애플리케이션이 실행되면 Amazon CloudFront (및 해당 HTTP 캐싱 기능) AWS AWS WAF, Shield Advanced Automatic Application 계층 보호를 활용하여 애플리케이션 계층 DDoS 공격 중에 불필요한 요청이 오리진에 도달하는 것을 방지할 수 있습니다.

아마존 CloudFront

Amazon은 CloudFront 웹 이외의 트래픽이 오리진에 도달하는 것을 방지하여 서버 부하를 줄이는 데 도움을 줄 수 있습니다. CloudFront 애플리케이션에 요청을 보내려면 완료한 핸드셰이크를 통해 유효

한 IP 주소로 연결을 설정해야 합니다. TCP 핸드셰이크는 위조할 수 없습니다. 또한 읽기 속도가 느리거나 쓰기 속도가 느린 공격자 (예: Slowloris) 의 연결을 자동으로 닫을 CloudFront 수 있습니다.

CDN캐싱

CloudFront AWS 엣지 로케이션에서 동적 콘텐츠와 정적 콘텐츠를 모두 제공할 수 있습니다. 캐시 가능한 프록시 콘텐츠를 캐시에서 제공하면 CDN 캐싱 기간 동안 해당 엣지 캐시 노드에서 요청이 오리진에 도달하지 못하게 할 수 있습니다. TTL 만료되었지만 캐시 가능한 콘텐츠의 요청 축소와 함께 아주 TTL 짧더라도 해당 콘텐츠에 대한 요청이 폭주하는 동안 오리진에 도달하는 요청 수는 무시할 수 없을 정도입니다. 또한 CloudFront Origin Shield와 같은 기능을 활성화하면 오리진의 부하를 줄일 수 있습니다. 캐시 적중률을 개선하기 위해 할 수 있는 모든 조치가 강력한 요청 플러드 공격과 영향을 미치지 않는 요청 플러드 공격의 차이를 의미할 수 있습니다.

AWS WAF

를 사용하면 AWS WAF전 세계 CloudFront 배포판 또는 지역 리소스에 웹 액세스 제어 목록 (웹ACLs)을 구성하여 요청 서명을 기반으로 요청을 필터링, 모니터링 및 차단할 수 있습니다. 요청을 허용할지 차단할지를 결정하려면 IP 주소 또는 출처 국가, 요청의 특정 문자열이나 패턴, 요청의 특정 부분의 크기, 악성 SQL 코드나 스크립팅의 존재 여부 등의 요인을 고려할 수 있습니다. 요청에 대해 CAPTCHA 퍼즐을 실행하고 클라이언트 세션 챌린지를 무음으로 설정할 수도 있습니다.

CloudFront 또한 지역 제한을 설정하여 특정 국가의 요청을 차단하거나 허용할 수도 있습니다. AWS WAF 이렇게 하면 사용자에게 서비스를 제공할 것으로 예상되지 않는 지리적 위치에서의 공격을 차단하거나 공격률을 제한하는 데 도움이 될 수 있습니다. 세분화된 지리적 일치 규칙 명령문을 사용하면 지역 수준까지 액세스를 AWS WAF제어할 수 있습니다.

Scope-Down 문을 사용하여 비용 절감을 위해 규칙이 평가하는 요청의 범위를 좁히고, 웹 요청의 “레이블”을 지정하여 요청과 일치하는 규칙이 일치 결과를 동일한 웹에서 나중에 평가되는 규칙으로 전달하도록 허용할 수 있습니다. ACL 여러 규칙에서 동일한 로직을 재사용하려면 이 옵션을 선택하십시오.

응답 코드, 헤더, 본문이 포함된 완전한 사용자 지정 응답을 정의할 수도 있습니다.

악의적인 요청을 식별하는 데 도움이 되도록 웹 서버 로그를 검토하거나 AWS WAF사용자의 로깅 및 요청 샘플링을 검토하십시오. AWS WAF 로깅을 활성화하면 웹에서 분석한 트래픽에 대한 자세한 정보를 얻을 수 있습니다. ACL AWS WAF 로그 필터링을 지원하여 검사 후 로그할 웹 요청과 로그에서 삭제되는 요청을 지정할 수 있습니다.

로그에 기록되는 정보에는 AWS 리소스로부터 요청을 AWS WAF 받은 시간, 요청에 대한 세부 정보, 요청된 각 규칙에 대한 매칭 작업 등이 포함됩니다.

샘플링된 요청은 지난 3시간 이내에 규칙 중 하나와 일치하는 요청에 대한 세부 정보를 제공합니다. AWS WAF 이 정보를 사용하여 악의적일 수 있는 트래픽 시그니처를 식별하고 이러한 요청을 거부하는 새 규칙을 만들 수 있습니다. 무작위 쿼리 문자열이 포함된 요청이 여러 개 있는 경우 애플리케이션의 캐시와 관련된 쿼리 문자열 매개변수만 허용해야 합니다. 이 기법은 오리진에 대한 캐시 무효화 공격을 완화하는 데 유용합니다.

AWS WAF — 속도 기반 규칙

AWS 5분 슬라이딩 윈도우 내에 수신된 HTTP 요청 수가 사용자가 정의한 임계값을 AWS WAF 초과할 경우 속도 기반 규칙을 사용하여 악의적인 행위자의 IP 주소를 자동으로 차단하여 요청 폭주를 방지할 것을 강력히 권장합니다. 문제가 되는 클라이언트 IP 주소는 403 금지된 응답 (또는 구성된 블록 오류 응답) 을 받게 되며 요청 비율이 임계값 아래로 떨어질 때까지 차단된 상태를 유지합니다.

속도 기반 규칙을 계층화하여 향상된 보호 기능을 제공하여 다음과 같은 효과를 얻을 수 있도록 하는 것이 좋습니다.

- 대규모 홍수로부터 애플리케이션을 보호하기 위한 포괄적인 요금 기반 규칙. HTTP
- 총괄 요율 기반 규칙보다 더 제한적인 요율로 특정 항목을 보호하는 URIs 하나 이상의 요금 기반 규칙.

예를 들어 5분 내에 요청 500개로 제한하는 총괄 요금 기반 규칙 (범위 축소 설명 없음) 을 선택한 다음 범위 축소 명령문을 사용하여 500개 (5분 동안 최소 100개 요청) 보다 낮은 다음 속도 기반 규칙 중 하나 이상을 생성할 수 있습니다.

- 파일 확장자가 없는 리소스에 대한 요청도 추가로 보호되도록 `if NOT uri_path contains '.'` ""와 같은 범위 축소 명령문을 사용하여 웹 페이지를 보호하십시오. 이렇게 하면 자주 타겟팅되는 경로인 홈페이지 (/) 도 보호됩니다. URI
- "" 와 같은 범위 축소 명령문을 사용하여 동적 엔드포인트를 보호하십시오. `if method exactly matches 'post' (convert lowercase)`
- 데이터베이스에 도달하거나 ""와 같이 범위가 축소된 일회용 암호 (OTP) 를 호출하는 과도한 요청을 보호합니다. `if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

"차단" 모드의 속도 기반 모드는 요청 폭주로부터 보호하기 위한 defense-in-depth WAF 구성의 초석이며 비용 보호 요청을 승인하기 위한 요구 사항입니다. AWS Shield Advanced 다음 섹션에서 추가 defense-in-depth WAF 구성을 살펴보겠습니다.

AWS WAF — IP 평판

IP 주소 평판에 기반한 공격을 방지하려면 IP 매칭을 사용하여 규칙을 만들거나 관리형 규칙을 사용할 수 AWS WAF있습니다.

Amazon의 IP 평판 목록 규칙 그룹에는 Amazon의 내부 위협 인텔리전스에 기반한 규칙이 포함됩니다. 이 규칙은 AWS 리소스를 정찰하거나 활동에 적극적으로 참여하는 봇인 IP 주소를 찾습니다. DDoS 이 `AWSManagedIPDDoSList` 규칙은 악성 요청 플러드의 90% 이상을 차단하는 것으로 확인되었습니다.

익명 IP 목록 규칙 그룹에는 시청자 신원을 모호하게 만들 수 있는 서비스의 요청을 차단하는 규칙이 포함되어 있습니다. 여기에는VPNs, 프록시, Tor 노드 및 클라우드 플랫폼 (제외) 으로부터의 요청이 포함됩니다. AWS

또한 솔루션용 보안 자동화의 IP 목록 파서 구성 요소를 사용하여 타사 IP 평판 목록을 활용할 수 있습니다. AWS WAF

AWS WAF - 지능형 위협 완화

봇넷은 심각한 보안 위협이며 일반적으로 스팸 전송, 민감한 데이터 도용, 랜섬웨어 공격 시작, 부정 클릭을 통한 광고 사기 또는 분산 () 공격과 같은 불법적이거나 유해한 활동을 수행하는 데 사용됩니다. denial-of-service DDoS 봇 공격을 방지하려면 Bot Control 관리 규칙 그룹을 사용하십시오.AWS WAF 이 규칙 그룹은 자체 식별 봇에 레이블을 추가하고, 일반적으로 바람직한 봇을 확인하고, 신뢰도가 높은 봇 서명을 탐지하는 기본적인 “공통” 보호 수준과 자체 식별이 불가능한 고급 봇에 대한 탐지를 추가하는 “표적” 보호 수준을 제공합니다.

표적 보호는 브라우저 조사, 핑거프린팅, 행동 휴리스틱과 같은 고급 탐지 기술을 사용하여 잘못된 봇 트래픽을 식별한 다음 속도 제한 CAPTCHA 및 챌린지 규칙 조치와 같은 완화 제어를 적용합니다. 또한 Targeted는 사람과 유사한 액세스 패턴을 적용하고 요청 토큰을 사용하여 동적 속도 제한을 적용하는 속도 제한 옵션을 제공합니다. 자세한 내용은 AWS WAF 봇 제어 규칙 그룹을 참조하십시오. 애플리케이션의 로그인 페이지에서 악의적인 도용 시도를 탐지하고 관리하려면 AWS WAF Fraud Control 계정 도용 방지 (ATP) 규칙 그룹을 사용할 수 있습니다. 규칙 그룹은 클라이언트가 애플리케이션의 로그인 엔드포인트로 보내는 로그인 시도를 검사하고 로그인 시도에 대한 애플리케이션의 응답을 검사하여 성공률과 실패율을 추적함으로써 이를 수행합니다.

계정 생성 사기는 공격자가 하나 이상의 허위 계정을 만들려고 하는 온라인 불법 활동입니다. 공격자는 허위 계정을 사용하여 프로모션 및 가입 보너스를 남용하거나 누군가를 사칭하는 사기 활동과 피싱 등의 사이버 공격을 수행합니다. 허위 계정이 존재하면 고객에 대해 평판이 손상되고 금융 사기에 노출되어 비즈니스에 부정적인 영향이 미칠 수 있습니다.

Fraud Control 계정 생성 사기 방지 (ACFP) 기능을 구현하여 계정 생성 AWS WAF 사기 시도를 모니터링하고 제어할 수 있습니다. AWS WAF 이 기능을 컴패니언 애플리케이션 `AWSManagedRulesACFPRuleSet` 통합과 함께 AWS Managed Rules 규칙 그룹에서 제공합니다SDKs.

AWS WAF 지능형 위협 완화의 이러한 보호 기능에 대해 자세히 알아보십시오.

애플리케이션 계층 DDoS 이벤트를 자동으로 완화 (,,) BP1 BP2 BP6

에 AWS Shield Advanced가입한 경우 Shield Advanced 자동 애플리케이션 계층 DDoS 완화를 활성화할 수 있습니다. 이 기능은 사용자를 대신하여 계층 7 DDoS 이벤트를 완화하기 위한 AWS WAF 규칙을 자동으로 생성, 평가 및 배포합니다.

AWS Shield Advanced 웹과 관련된 각 보호 리소스에 대한 트래픽 기준을 설정합니다. WAF ACL 설정된 기준선을 크게 벗어나는 트래픽은 잠재적 이벤트로 플래그가 지정됩니다. DDoS 이벤트가 감지되면 이벤트를 구성하는 웹 요청의 시그니처를 AWS Shield Advanced 식별하려고 시도하고, 시그니처가 식별되면 해당 시그니처로 트래픽을 완화하기 위한 AWS WAF 규칙이 생성됩니다.

규칙이 이전 기준과 비교하여 평가되고 안전하다고 판단되면 해당 규칙은 Shield 관리 규칙 그룹에 추가되며 규칙을 카운트 모드로 배포할지 블록 모드로 배포할지 선택할 수 있습니다. Shield Advanced는 이벤트가 완전히 진정된 것으로 확인되면 AWS WAF 규칙을 자동으로 제거합니다.

참여 SRT (Shield 어드밴스드 구독자만 해당)

또한 Shield Advanced에 가입하면 애플리케이션 가용성을 저해하는 공격을 완화하는 규칙을 만드는 데 도움을 받을 수 있습니다. AWS SRT 계정 및 계정에 AWS SRT 제한된 액세스 권한을 부여할 수 있습니다. AWS Shield Advanced AWS WAF APIs AWS SRT사용자가 명시적으로 승인한 경우에만 이러한 APIs 기능에 액세스하여 사용자 계정에 완화 조치를 적용합니다. 자세한 내용은 이 문서의 지원 섹션을 참조하십시오.

를 AWS Firewall Manager 사용하여 조직 전체에서 AWS Shield Advanced 보호 및 규칙과 같은 보안 규칙을 중앙에서 구성하고 관리할 수 있습니다. AWS WAF AWS Organizations 관리 계정은 Firewall Manager 정책을 생성할 권한이 있는 관리자 계정을 지정할 수 있습니다. 이러한 정책을 통해 규칙 적용 위치를 결정하는 리소스 유형 및 태그와 같은 기준을 정의할 수 있습니다. 이는 계정이 여러 개이고 보호를 표준화하려는 경우에 유용합니다.

해당 내용은 다음을 참조하세요.

- AWS Managed Rules 에 대해서는 AWS WAF for를 참조하십시오.AWS Managed RulesAWS WAF
- 지리적 제한을 사용하여 CloudFront 배포에 대한 액세스를 제한하려면 콘텐츠의 지리적 배포 제한을 참조하십시오.

- 사용 시 AWS WAF다음을 참조하십시오.
  - 시작하기 AWS WAF
  - 웹 ACL 트래픽 정보 로깅
  - 웹 요청 샘플 보기
- 속도 기반 규칙 구성은 속도 기반 규칙을 사용하여 웹 사이트 및 서비스 보호를 참조하십시오. AWS WAF
- Firewall Manager를 사용하여 AWS 리소스 전반의 규칙 배포를 관리하는 방법은 다음을 참조하십시오.
  - 방화벽 관리자 AWS WAF 정책 시작하기
  - 방화벽 관리자 쉴드 고급 정책 시작하기

공격 표면 감소

AWS 솔루션을 설계할 때 고려해야 할 또 다른 중요한 사항은 공격자가 애플리케이션을 표적으로 삼을 기회를 제한하는 것입니다. 이 개념을 공격 표면 감소라고 합니다. 인터넷에 노출되지 않은 리소스는 공격하기가 더 어려우므로 공격자가 애플리케이션의 가용성을 목표로 삼을 수 있는 옵션이 제한됩니다.

예를 들어 사용자가 특정 리소스와 직접 상호 작용할 것으로 예상되지 않는 경우 인터넷에서 해당 리소스에 액세스할 수 없도록 하세요. 마찬가지로 통신에 필요하지 않은 포트나 프로토콜을 통해 사용자나 외부 애플리케이션이 보내는 트래픽을 수락하지 마세요.

다음 섹션에서는 공격 표면을 줄이고 애플리케이션의 인터넷 노출을 제한하는 방법을 안내하는 모범 사례를 AWS 제공합니다.

AWS 리소스 난독화 (,,) BP1 BP4 BP5

일반적으로 사용자는 AWS 리소스를 인터넷에 완전히 노출하지 않고도 애플리케이션을 빠르고 쉽게 사용할 수 있습니다.

보안 그룹 및 네트워크 ACLs (BP5)

Amazon Virtual Private Cloud (AmazonVPC) 를 사용하면 정의한 가상 네트워크에서 AWS 리소스를 시작할 수 AWS 클라우드 있는 논리적으로 격리된 구역을 프로비저닝할 수 있습니다.

보안 그룹과 ACLs 네트워크는 조직 내 AWS 리소스에 대한 액세스를 제어할 수 있다는 점에서 비슷합니다VPC. 그러나 보안 그룹을 사용하면 인스턴스 수준에서 인바운드 및 아웃바운드 트래픽을 제어할 수 있는 반면, 네트워크는 VPC 서브넷 수준에서 유사한 기능을 ACLs 제공합니다. 보안 그룹 또는 네트워크 사용에 따른 추가 요금은 없습니다. ACLs

인스턴스를 시작할 때 보안 그룹을 지정할지 또는 나중에 인스턴스를 보안 그룹과 연결할 것인지 선택할 수 있습니다. 트래픽을 허용하는 허용 규칙을 만들지 않는 한 보안 그룹에 대한 모든 인터넷 트래픽은 암시적으로 거부됩니다.

예를 들어, Elastic Load Balancer 뒤에 Amazon EC2 인스턴스가 있는 경우 인스턴스 자체는 공개적으로 액세스할 수 없고 IPs 비공개로만 가능해야 합니다. 대신, 대상 그룹 서브넷의 네트워크 액세스 제어 목록 () 과 함께 0.0.0.0/0에 대한 액세스를 허용하는 보안 그룹 규칙 (아래 참고 참조) 을 사용하여 Elastic Load Balancer IP 범위만 인스턴스와 통신하도록 허용하는 보안 그룹 규칙을 사용하여 Elastic Load Balancer에 필요한 대상 수신기 포트에 대한 액세스 권한을 제공할 수 있습니다. NACL 이렇게 하

면 인터넷 트래픽이 Amazon EC2 인스턴스와 직접 통신할 수 없으므로 공격자가 애플리케이션에 대해 알아내고 애플리케이션에 영향을 미치기가 더 어려워집니다.

네트워크를 ACLs 생성할 때 허용 및 거부 규칙을 모두 지정할 수 있습니다. 이는 애플리케이션에 대한 특정 유형의 트래픽을 명시적으로 거부하려는 경우에 유용합니다. 예를 들어 전체 서브넷에 대한 액세스가 거부되는 IP 주소 (CIDR범위), 프로토콜 및 대상 포트를 정의할 수 있습니다. 애플리케이션이 트래픽에만 사용되는 경우 모든 TCP UDP 트래픽을 거부하거나 그 반대의 규칙을 만들 수 있습니다. 이 옵션을 사용하면 소스 IPs 또는 기타 시그니처를 알면 DDoS 공격을 완화하는 규칙을 직접 만들 수 있으므로 공격에 대응할 때 유용합니다.

를 구독하는 AWS Shield Advanced경우 엘라스틱 IP 주소를 보호된 리소스로 등록할 수 있습니다. DDoS보호 리소스로 등록된 엘라스틱 IP 주소에 대한 공격은 더 빠르게 탐지되므로 방어 시간이 더 빨라질 수 있습니다. 공격이 탐지되면 DDoS 방어 시스템은 대상 엘라스틱 IP 주소에 ACL 해당하는 네트워크를 읽고 서브넷 수준이 아닌 AWS 네트워크 경계에서 적용합니다. 이렇게 하면 여러 인프라 계층 공격으로 인한 영향을 받을 위험이 크게 줄어듭니다. DDoS

DDoS복원력을 ACLs 최적화하도록 보안 그룹과 네트워크를 구성하는 방법에 대한 자세한 내용은 공격 표면을 줄여 DDoS 공격에 대비하는 방법을 참조하십시오.

엘라스틱 IP 주소가 포함된 Shield Advanced를 보호 리소스로 사용하는 방법에 대한 자세한 내용은 구독 단계를 참조하십시오 AWS Shield Advanced.

오리진 보호 (BP1,BP5)

오리진이 내부에 CloudFront 있는 Amazon을 사용하는 경우 CloudFront 배포에서만 오리진에 요청을 전달할 수 있도록 하는 것이 좋습니다. VPC Edge-to-Origin 요청 헤더를 사용하면 요청을 오리진에 전달할 때 CloudFront 기존 요청 헤더의 값을 추가하거나 재정의할 수 있습니다. Origin 사용자 지정 헤더 (예: `X-Shared-Secret` 헤더) 를 사용하여 오리진에 보낸 요청이 보낸 것인지 확인하는 데 도움이 될 수 있습니다. CloudFront

오리진 커스텀 헤더로 오리진을 보호하는 방법에 대한 자세한 내용은 오리진 요청에 커스텀 헤더 추가 및 애플리케이션 로드 밸런서에 대한 액세스 제한을 참조하십시오.

오리진 액세스 제한을 위한 Origin 사용자 지정 헤더의 값을 자동으로 교체하는 샘플 솔루션을 구현하는 방법에 대한 지침은 Secrets Manager를 사용하여 AWS WAF Amazon CloudFront 오리진 보안을 강화하는 방법을 참조하십시오.

또는 AWS Lambda함수를 사용하여 CloudFront 트래픽만 허용하도록 보안 그룹 규칙을 자동으로 업데이트할 수도 있습니다. 이렇게 하면 악의적인 사용자가 웹 애플리케이션을 우회하거나 웹 애플리케이션에 액세스할 AWS WAF 때 이를 방지할 CloudFront 수 있어 오리진의 보안이 향상됩니다.

보안 그룹과 X-Shared-Secret 헤더를 자동으로 업데이트하여 오리진을 보호하는 방법에 대한 자세한 내용은 Amazon CloudFront 및 AWS WAF Us를 사용하여 보안 그룹을 자동으로 업데이트하는 방법을 참조하십시오 AWS Lambda.

그러나 솔루션에는 추가 구성 및 Lambda 함수 실행 비용이 포함됩니다. 이를 단순화하기 위해 이제 오리진 연결 IP 주소에서만 오리진으로 CloudFront 향하는 HTTP HTTPS 인바운드/트래픽을 제한하는 AWS-managed 접두사 목록을 도입했습니다. CloudFront AWS-관리형 접두사 목록은 에서 생성 및 유지 관리하며 추가 비용 없이 사용할 AWS 수 있습니다. (AmazonVPC) 보안 그룹 규칙, 서브넷 라우팅 테이블, 공통 보안 그룹 규칙 및 관리형 접두사 목록을 사용할 수 있는 AWS Firewall Manager기타 AWS 리소스에서 관리형 접두사 목록을 참조할 수 있습니다. CloudFront

Amazon용 AWS-managed 접두사 목록 사용에 대한 자세한 내용은 CloudFront Amazon용 AWS-managed 접두사 목록을 사용하여 원본에 대한 액세스 제한을 참조하십시오. CloudFront

> **Note**
>
> 이 문서의 다른 섹션에서 설명한 것처럼 보안 그룹을 사용하여 오리진을 보호하면 요청이 폭주하는 동안 보안 그룹 연결 추적을 병목 현상으로 만들 수 있습니다. 캐싱을 활성화하는 캐싱 정책을 CloudFront 사용하여 악의적인 요청을 필터링할 수 없다면 보안 그룹을 사용하는 것보다 앞서 설명한 Origin 사용자 지정 헤더를 사용하여 오리진에 대한 요청이 보낸 것인지 확인하는 것이 더 나을 수 있습니다. CloudFront Application Load Balancer 리스너 규칙과 함께 사용자 지정 요청 헤더를 사용하면 로드 밸런서에 대한 새 연결 설정에 영향을 미칠 수 있는 추적 제한으로 인한 병목 현상이 방지되므로 Application Load Balancer는 공격 발생 시 트래픽 증가에 따라 규모를 조정할 수 있습니다. DDoS

API엔드포인트 보호 () BP4

일반에 공개해야 API 하는 경우 API 프론트엔드가 공격의 표적이 될 위험이 있습니다. DDoS 위험을 줄이기 위해 Amazon API Gateway를 Amazon 또는 다른 곳에서 실행되는 애플리케이션으로 들어가는 진입로로 사용할 수 있습니다. EC2 AWS Lambda Amazon API Gateway를 사용하면 API 프런트엔드에 자체 서버가 필요하지 않으며 애플리케이션의 다른 구성 요소를 난독화할 수 있습니다. 애플리케이션 구성 요소를 탐지하기 어렵게 만들면 해당 AWS 리소스가 공격의 표적이 되는 것을 방지할 수 있습니다. DDoS

Amazon API Gateway를 사용하면 두 가지 유형의 API 엔드포인트 중에서 선택할 수 있습니다. 첫 번째는 기본 옵션입니다. Amazon 배포를 통해 액세스하는 엣지 최적화 API 엔드포인트입니다. CloudFront 하지만 배포는 API Gateway에서 생성하고 관리하므로 사용자가 이를 제어할 수 없습니다. 두 번째

REST API 옵션은 배포된 지역과 동일한 AWS 리전 지역에서 액세스할 수 있는 리전 API 엔드포인트를 사용하는 것입니다. AWS 두 번째 유형의 엔드포인트를 사용하고 이를 자체 Amazon CloudFront 배포와 연결할 것을 권장합니다. 이를 통해 Amazon CloudFront 배포를 제어하고 애플리케이션 계층 보호에 AWS WAF 사용할 수 있습니다. 이 모드를 사용하면 AWS 글로벌 엣지 네트워크 전반에서 확장된 DDoS 완화 용량에 액세스할 수 있습니다.

Amazon CloudFront 및 AWS WAF Amazon API Gateway를 사용하는 경우 다음 옵션을 구성하십시오.

- 모든 헤더를 API 게이트웨이 리전 엔드포인트로 전달하도록 배포의 캐시 동작을 구성하십시오. 이렇게 하면 콘텐츠를 동적인 CloudFront 것으로 취급하고 콘텐츠 캐싱을 건너뛰게 됩니다.
- Gateway에서 APIAPI키 값을 설정하여 원본 사용자 지정 헤더를 x-api-key 포함하도록 배포를 구성하여 API 게이트웨이를 직접 액세스로부터 보호하십시오.
- 각 메서드에 대해 표준 또는 버스트 속도 제한을 구성하여 초과 트래픽으로부터 백엔드를 보호하십시오. REST APIs

Amazon API Gateway를 APIs 사용하여 생성하는 방법에 대한 자세한 내용은 Amazon API Gateway 시작하기를 참조하십시오.

운영 기법

이 백서의 완화 기법은 공격에 대해 본질적으로 복원력이 있는 애플리케이션을 설계하는 데 도움이 됩니다. DDoS 대부분의 경우 DDoS 공격이 애플리케이션을 대상으로 하는 시점을 파악하여 방어 조치를 취하는 것도 유용합니다. 이 섹션에서는 비정상 동작에 대한 가시성 확보, 경고 및 자동화, 대규모 보호 관리, 추가 지원 참여 AWS 등을 위한 모범 사례를 설명합니다.

로드 테스트.

예상 트래픽 수준과 예상 초과 트래픽 수준을 모두 포함하는 부하 테스트 애플리케이션 백서의 지침을 사용하여 애플리케이션을 정기적으로 로드 테스트하여 아키텍처가 얼마나 효과적인지, Auto Scaling 정책이 어떻게 작동하는지, 오류 처리 기능이 어떻게 작동하는지 확인할 수 있습니다. 예상되는 트래픽 규모 확대 및 축소뿐 아니라 '플래시 크라우드' 유형의 동작도 테스트해 보세요. 주기적으로 또는 메이저 릴리스 전에 다시 테스트하십시오. SYN플러드와 같은 레이어 3 또는 4 DDoS 시뮬레이션 테스트의 경우 DDoS시뮬레이션 테스트 정책을 따르십시오.

지표 및 경보

가장 좋은 방법은 인프라 및 애플리케이션 모니터링 도구를 사용하여 애플리케이션의 가용성을 확인하여 애플리케이션이 이벤트의 영향을 받지 않도록 하는 것입니다. 옵션으로, DDoS 이벤트 감지를 개선하는 데 도움이 되도록 리소스에 대한 애플리케이션 및 인프라 Route 53 상태 검사를 구성할 수 있습니다. DDoS 상태 확인에 대한 자세한 내용은 Firewall Manager 및 Shield 고급 개발자 가이드를 참조하십시오AWS WAF.

주요 운영 지표가 예상 값에서 크게 벗어나는 경우 공격자는 애플리케이션의 가용성을 목표로 삼으려고 할 수 있습니다. 애플리케이션의 정상적인 동작을 잘 알고 있으면 이상 징후를 감지했을 때 더 빠르게 조치를 취할 수 있습니다. Amazon은 실행 중인 애플리케이션을 모니터링하여 도움을 줄 CloudWatch 수 AWS있습니다. 예를 들어, 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하고, 경보를 설정하고, AWS 리소스 변경에 자동으로 대응할 수 있습니다.

애플리케이션을 설계할 때 DDoS -resilient 참조 아키텍처를 따르는 경우 일반적인 인프라 계층 공격이 애플리케이션에 도달하기 전에 차단됩니다. 를 AWS Shield Advanced구독하면 애플리케이션이 표적이 되고 있음을 나타내는 여러 CloudWatch 메트릭에 액세스할 수 있습니다.

예를 들어 DDoS 공격이 진행 중일 때 알림을 받도록 경보를 구성하여 애플리케이션의 상태를 확인하고 참여 여부를 결정할 수 있습니다. AWS SRT 공격이 탐지되었는지 여부를 알려주도록 `DDoSDetected` 메트릭을 구성할 수 있습니다. 공격 볼륨에 따라 알림

을 받으려면 DDoSAttackBitsPerSecondDDoSAttackPacketsPerSecond, 또는 DDoSAttackRequestsPerSecond 지표를 사용할 수도 있습니다. 자체 CloudWatch 도구와 통합하거나 타사에서 제공하는 도구 (예: Slack 또는) 를 사용하여 이러한 지표를 모니터링할 수 있습니다. PagerDuty

애플리케이션 계층 공격은 많은 Amazon CloudWatch 지표를 높일 수 있습니다. 를 사용하는 경우 허용 AWS WAF, 계산 또는 CloudWatch 차단하도록 설정한 요청 증가에 대한 경보를 모니터링하고 AWS WAF 활성화하는 데 사용할 수 있습니다. 이렇게 하면 트래픽 수준이 애플리케이션이 처리할 수 있는 수준을 초과할 경우 알림을 받을 수 있습니다. 또한 CloudWatch 추적되는 Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, EC2 Amazon 및 Auto Scaling 지표를 사용하여 공격을 나타낼 수 있는 변경 사항을 탐지할 수 있습니다. DDoS

다음 표에는 공격을 탐지하고 이에 대응하는 데 일반적으로 사용되는 CloudWatch 지표에 대한 설명이 나와 있습니다. DDoS

표 3 - 아마존 권장 CloudWatch 측정치

주제	지표	설명
AWS Shield Advanced	DDoSDetected	특정 Amazon 리소스 이름 (ARN) 에 대한 DDoS 이벤트를 나타냅니다.
AWS Shield Advanced	DDoSAttackBitsPerSecond	특정 DDoS ARN 이벤트에서 관찰된 바이트 수입니다. 이 지표는 레이어 3 또는 4 DDoS 이벤트에만 사용할 수 있습니다.
AWS Shield Advanced	DDoSAttackPacketsPerSecond	특정 DDoS ARN 이벤트에서 관찰된 패킷 수입니다. 이 지표는 레이어 3 또는 4 DDoS 이벤트에만 사용할 수 있습니다.
AWS Shield Advanced	DDoSAttackRequestsPerSecond	특정 DDoS 이벤트에서 관찰된 요청 수입니다ARN. 이 지표는 계층 7 DDoS 이벤트에만 사용할 수 있으며 가장 중요한 계층 7 이벤트에 대해서만 보고됩니다.

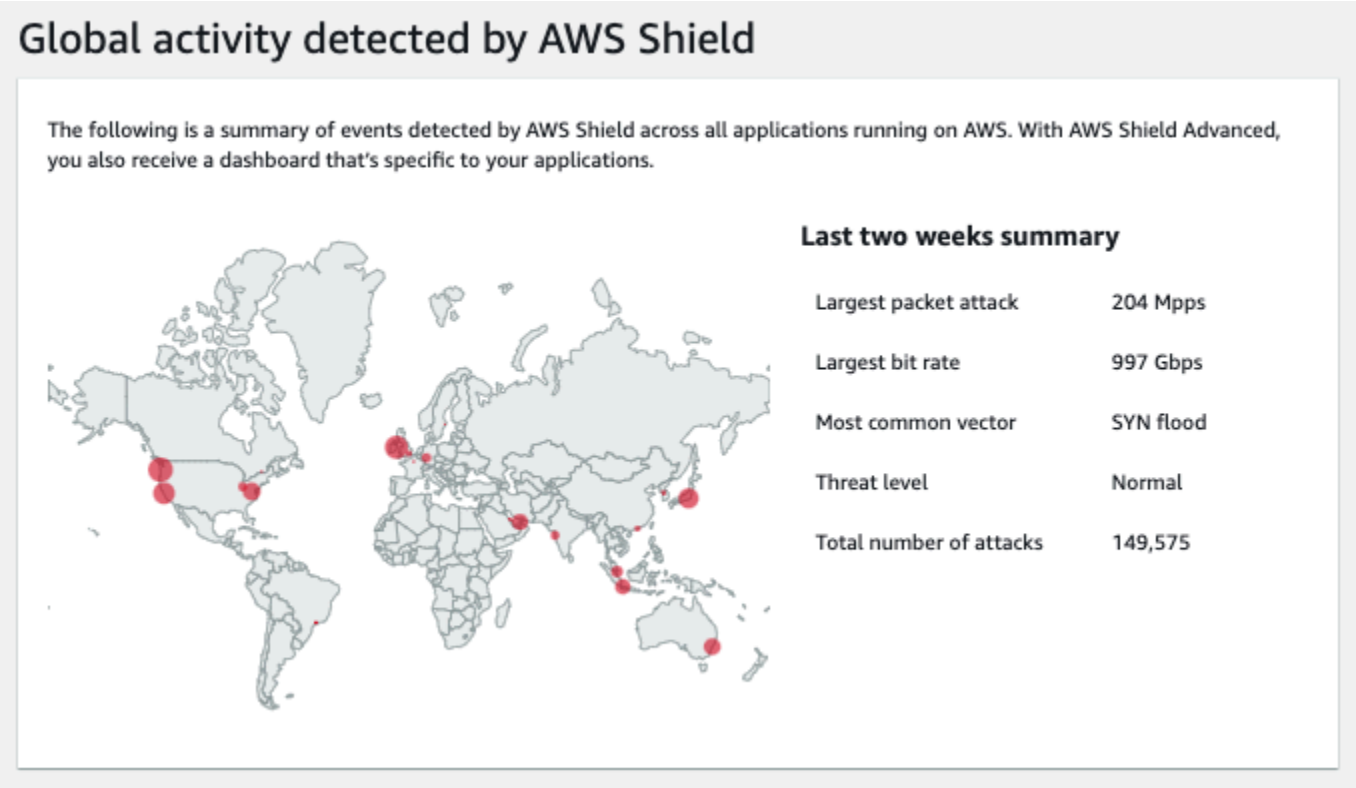
주제	지표	설명
AWS WAF	AllowedRequests	허용된 웹 요청의 수.
AWS WAF	BlockedRequests	차단된 웹 요청의 수.
AWS WAF	CountedRequests	계수된 웹 요청의 수.
AWS WAF	PassedRequests	전달된 요청의 수입니다. 규칙 그룹 규칙과 일치하지 않고 규칙 그룹 평가를 거치는 요청에만 사용됩니다.
아마존 CloudFront	Requests	HTTPA/S 요청 수.
아마존 CloudFront	TotalErrorRate	HTTP상태 코드가 4xx OR인 모든 요청의 백분율5xx.
Amazon Route 53	HealthCheckStatus	상태 확인 엔드포인트의 상태입니다.
Application Load Balancer	ActiveConnectionCount	클라이언트에서 로드 밸런서로, 로드 밸런서에서 타겟으로 활성 상태인 총 동시 TCP 연결 수입니다.
Application Load Balancer	ConsumedLCUs	로드 밸런서에서 사용하는 로드 밸런서 용량 단위 수 (LCU).
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	로드 밸런서에서 생성된 HTTP 4xx 또는 5xx 클라이언트 오류 코드의 수
Application Load Balancer	NewConnectionCount	클라이언트에서 로드 밸런서로, 로드 밸런서에서 타겟으로 설정된 총 새 TCP 연결 수입니다.

주제	지표	설명
Application Load Balancer	ProcessedBytes	로드 밸런서에서 처리된 총 바이트 수.
Application Load Balancer	RejectedConnectionCount	로드 밸런서가 최대 연결 수에 도달하여 거부된 연결 수
Application Load Balancer	RequestCount	처리된 요청 수입니다.
Application Load Balancer	TargetConnectionErrorCount	로드 밸런서와 대상 사이에 성공적으로 구성되지 않은 연결 수.
Application Load Balancer	TargetResponseTime	요청이 로드 밸런서를 떠난 후 대상으로부터 응답을 받을 때까지 경과된 시간 (초) 입니다.
Application Load Balancer	UnHealthyHostCount	비정상 상태로 간주되는 대상 수.
Network Load Balancer	ActiveFlowCount	클라이언트에서 타겟까지의 총 동시 TCP 흐름 (또는 연결) 수입니다.
Network Load Balancer	ConsumedLCUs	로드 밸런서에서 사용하는 로드 밸런서 용량 단위 수 (LCU).
Network Load Balancer	NewFlowCount	일정 기간 동안 클라이언트에서 대상까지 설정된 새 TCP 흐름 (또는 연결) 의 총 수입니다.
Network Load Balancer	ProcessedBytes	TCP/IP 헤더를 포함하여 로드 밸런서에서 처리한 총 바이트 수입니다.

주제	지표	설명
Global Accelerator	NewFlowCount	일정 기간 동안 클라이언트에서 엔드포인트로 설정된 새 TCP UDP 플로우 (또는 연결)의 총 수입니다.
Global Accelerator	ProcessedBytesIn	/IP 헤더를 포함하여 TCP 액셀러레이터에서 처리된 총 수신 바이트 수입니다.
Auto Scaling	GroupMaxSize	Auto Scaling 그룹 의 최대 크기입니다.
아마존 EC2	CPUUtilization	할당된 EC2 컴퓨팅 유닛 중 현재 사용 중인 컴퓨팅 유닛의 비율.
아마존 EC2	NetworkIn	모든 네트워크 인터페이스에서 인스턴스가 받은 바이트 수입니다.

CloudWatch Amazon을 사용하여 애플리케이션에 대한 DDoS 공격을 탐지하는 방법에 대한 자세한 내용은 Amazon 시작하기를 참조하십시오 CloudWatch.

AWS 공격에 대해 알리고 애플리케이션 리소스를 모니터링하는 데 도움이 되는 몇 가지 추가 지표 및 경보가 포함되어 있습니다. AWS Shield 콘솔 또는 계정별 이벤트 요약 및 탐지된 공격에 대한 세부 정보를 API 제공합니다.



글로벌 활동은 다음을 통해 탐지되었습니다. AWS Shield

또한 글로벌 위협 환경 대시보드는 에서 탐지된 모든 DDoS 공격에 대한 요약 정보를 제공합니다 AWS. 이 정보는 공격 경향 외에도 많은 응용 프로그램에 걸친 DDoS 위협을 더 잘 이해하고 관찰했을 수 있는 공격과 비교하는 데 유용할 수 있습니다.

에 AWS Shield Advanced가입한 경우 서비스 대시보드에는 보호된 리소스에서 탐지된 이벤트에 대한 추가 탐지 및 완화 지표와 네트워크 트래픽 세부 정보가 표시됩니다. AWS Shield 보호 대상 리소스로 향하는 트래픽을 여러 차원에서 평가합니다. 예외가 감지되면 이벤트를 AWS Shield 생성하고 이상이 관찰된 트래픽 차원을 보고합니다. 적절한 완화 기능을 사용하면 알려진 이벤트 시그니처와 일치하는 과도한 트래픽 및 트래픽이 리소스에 수신되지 않도록 보호할 수 있습니다. DDoS

탐지 ACL 지표는 웹이 보호된 리소스와 연결된 경우 샘플링된 네트워크 흐름 또는 AWS WAF 로그를 기반으로 합니다. 완화 지표는 Shield의 DDoS 완화 시스템에서 관찰한 트래픽을 기반으로 합니다. 완화 지표는 리소스로 유입되는 트래픽을 보다 정확하게 측정한 것입니다.

네트워크 상위 기여자 지표는 감지된 이벤트 중에 트래픽이 어디서 오는지에 대한 통찰력을 제공합니다. 볼륨 기여도가 가장 높은 요인을 확인하고 프로토콜, 소스 포트, 플래그와 같은 항목별로 정렬할 수 있습니다. TCP 상위 기여자 지표에는 다양한 차원을 기준으로 리소스에서 관찰된 모든 트래픽에 대한 지표가 포함됩니다. 이벤트 중에 리소스로 전송되는 네트워크 트래픽을 이해하는 데 사용할 수 있는 추

가 지표 측정기준을 제공합니다. 비반사 계층 3 또는 4 공격의 경우 소스 IP 주소가 스푸핑되어 신뢰할 수 없다는 점을 염두에 두십시오.

서비스 대시보드에는 공격을 완화하기 위해 자동으로 취해진 조치에 대한 세부 정보도 포함되어 있습니다. DDoS 이 정보를 통해 더 쉽게 이상 현상을 조사하고, 트래픽의 차원을 탐색하고, Shield Advanced가 가용성을 보호하기 위해 취한 조치를 더 잘 이해할 수 있습니다.

로깅

애플리케이션 소유자를 위한 로깅 및 모니터링 가이드에 따라 모든 서비스에 유용한 로깅을 활성화하여 가시성을 극대화하고 문제 해결을 지원할 수 있습니다. 여기에는 다음이 포함되며 이에 국한되지는 않습니다.

- AWS CloudTrail
- AWS WAF 로그
- CloudFront액세스 로그
- VPC흐름 로그 (네트워크 트래픽 흐름 기록 및 보기 참조) - 포함된 `tcp-flags` 필드에 필드를 포함하여 가시성을 극대화합니다.
- ELB액세스 로그 (ALB, CLB, NLB)
- 웹 서버 HTTP 액세스 로그
- 운영 체제 보안 로깅
- 애플리케이션 로깅

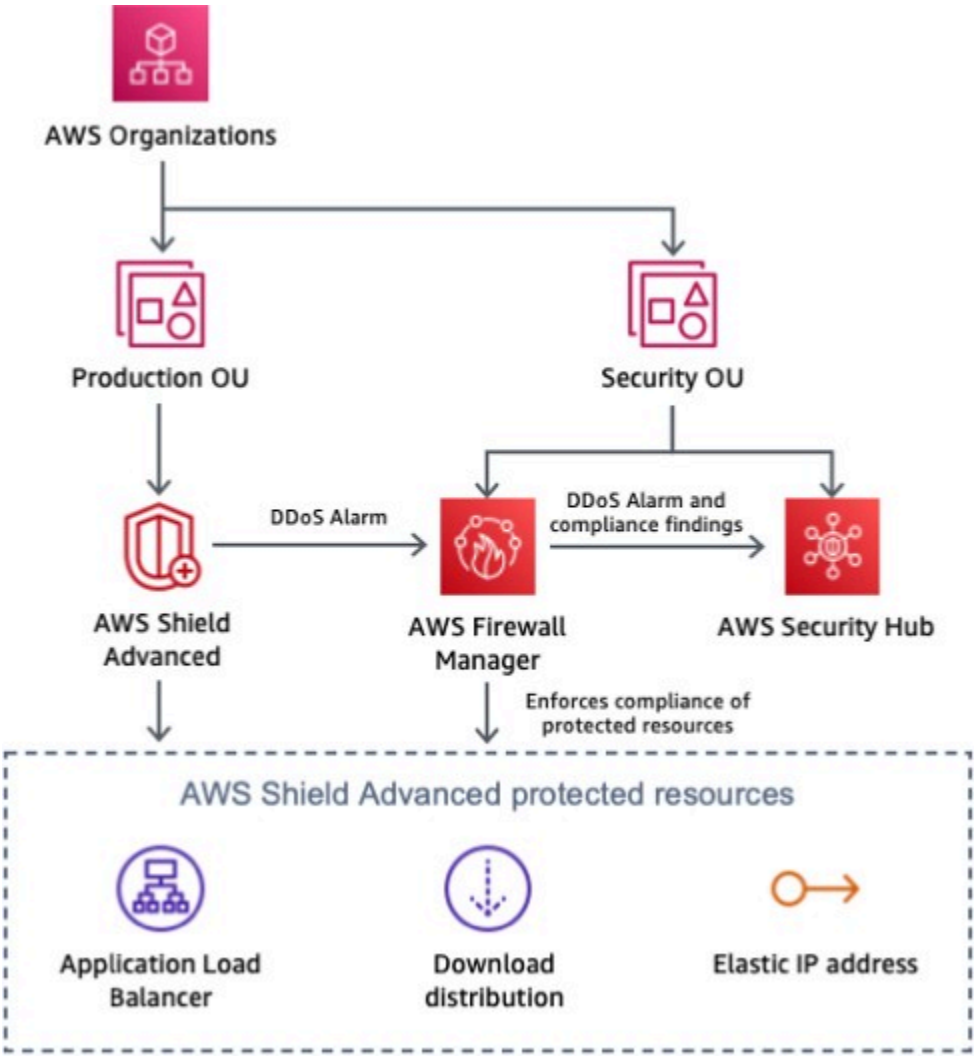
여러 계정에 대한 가시성 및 보호 관리

여러 AWS 계정 구성 요소를 대상으로 운영하고 보호해야 할 구성 요소가 여러 개 있는 경우 대규모로 운영하고 운영 오버헤드를 줄일 수 있는 기술을 사용하면 완화 기능을 높일 수 있습니다. 여러 계정에서 AWS Shield Advanced 보호된 리소스를 관리하는 경우 및 를 사용하여 AWS Firewall Manager 중앙 모니터링을 설정할 수 있습니다. AWS Security Hub Firewall Manager를 사용하면 모든 계정에 DDoS 보호 규정 준수를 적용하는 보안 정책을 만들 수 있습니다. 이 두 서비스를 함께 사용하여 여러 계정의 보호된 리소스를 관리하고 해당 리소스에 대한 모니터링을 중앙 집중화할 수 있습니다.

Security Hub는 Firewall Manager와 자동으로 통합되므로 Shield Advanced 고객은 단일 대시보드에서 보안 결과와 함께 우선 순위가 높은 다른 보안 경고 및 규정 준수 상태를 볼 수 있습니다.

예를 들어 Shield Advanced가 범위 AWS 계정 내의 보호 대상 리소스로 향하는 비정상적인 트래픽을 탐지하면 Security Hub 콘솔에서 이 탐지 결과를 볼 수 있습니다. Firewall Manager를 구성하면

Firewall Manager를 Shield Advanced 보호 리소스로 생성하여 리소스를 자동으로 규정 준수 상태로 만든 다음 리소스가 규정 준수 상태에 있을 때 Security Hub를 업데이트할 수 있습니다.



Firewall Manager 및 AWS Shield Security Hub를 통한 모니터링 보호 리소스를 보여 주는 아키텍처 다이어그램

Shield 보호 리소스의 중앙 모니터링에 대한 자세한 내용은 DDoS이벤트에 대한 중앙 모니터링 설정 및 비준수 리소스 자동 개선을 참조하십시오.

사고 대응 전략 및 런북

DDoS공격 사고 대응 전략을 개발하고 이를 중심으로 보안 사고 대응 프로세스를 구축하는 것은 모든 조직에 매우 중요합니다. 권장되는 접근 방식은 증거 수집, 완화, 복구, 사고 후 분석 수행과 같은 제안된 단계를 기반으로 NIST 대응 플레이북을 모델링하는 것입니다. 예를 들어, 웹 애플리케이션 DoS 또

는 DDoS 공격에 대한 대응 플레이북이 예로 제공됩니다. 추가 리소스는 AWS 보안 사고 대응 가이드에서 확인할 수 있습니다.

지원

공격이 발생한 경우 위협을 평가하고 애플리케이션 아키텍처를 검토하여 지원을 받을 수도 있고 다른 지원을 요청할 수도 있습니다. AWS 실제 사건이 발생하기 전에 DDoS 공격에 대한 대응 계획을 세우는 것이 중요합니다. 이 백서에 설명된 모범 사례는 애플리케이션을 시작하기 전에 구현하는 사전 조치를 취하기 위한 것이지만 애플리케이션에 대한 DDoS 공격은 여전히 발생할 수 있습니다. 이 섹션의 옵션을 검토하여 시나리오에 가장 적합한 지원 리소스를 결정하십시오. 계정 팀이 사용 사례 및 애플리케이션을 평가하고 특정 질문이나 문제에 대해 도움을 줄 수 있습니다.

프로덕션 워크로드를 실행하는 경우 공격 문제를 지원할 수 있는 Cloud Support 엔지니어를 연중무휴 이용할 수 있는 Business Support에 가입하는 것이 좋습니다DDoS. AWS업무상 중요한 워크로드를 실행하는 경우 중요한 사례를 접수하고 선임 클라우드 지원 엔지니어로부터 가장 빠른 응답을 받을 수 있는 기능을 제공하는 Enterprise Support를 고려해 보십시오.

비즈니스 지원 또는 엔터프라이즈 지원에 가입되어 AWS Shield Advanced 있고 구독하고 있는 경우 Shield 사전 참여를 구성할 수 있습니다. 이를 통해 상태 점검을 구성하고, 리소스에 연결하고, 연중무휴 운영 연락처 정보를 제공할 수 있습니다. Shield가 징후를 DDoS 감지하고 애플리케이션 상태 점검에 성능 저하 징후가 AWS SRT 보이면 사전에 연락을 드릴 것입니다. 이는 가장 빠른 AWS SRT 응답 시간을 제공하고 고객과 연락하기 전에도 문제 해결을 시작할 수 있기 때문에 AWS SRT 권장되는 참여 모델입니다.

자세한 내용은 플랜 AWS Support 비교를 참조하십시오.

사전 참여 기능을 사용하려면 애플리케이션의 상태를 정확하게 측정하고 Shield Advanced에 의해 보호되는 리소스와 연결되는 Route 53 상태 점검을 구성해야 합니다. Route 53 상태 점검이 Shield 콘솔에 연결되면 Shield Advanced 탐지 시스템은 상태 점검 상태를 애플리케이션 상태의 지표로 사용합니다. Shield Advanced의 상태 기반 탐지 기능을 사용하면 애플리케이션이 비정상일 때 알림을 받고 완화 조치를 더 신속하게 적용할 수 있습니다. AWS SRT비정상 애플리케이션이 DDoS 공격의 표적이 되고 있는지 여부를 해결하기 위해 연락을 드리고 필요에 따라 추가 완화 조치를 취합니다.

사전 예방적 참여 구성을 완료하려면 Shield 콘솔에 연락처 세부 정보를 추가하는 작업이 포함됩니다. AWS SRT이 정보를 사용하여 연락을 드릴 것입니다. 연락처를 10개까지 구성할 수 있으며, 특정 연락처 요구 사항이나 기본 설정이 있는 경우 추가 메모를 제공할 수 있습니다. 사전

업무 담당자는 보안 운영 센터 또는 즉시 연락할 수 있는 개인과 같이 연중무휴 역할을 수행해야 합니다.

모든 리소스 또는 응답 시간이 중요한 일부 주요 프로덕션 리소스에 대해 사전 예방적 참여를 유도할 수 있습니다. 이를 위해서는 이러한 리소스에만 상태 점검을 할당하면 됩니다.

또한 AWS Support 콘솔을 AWS SRT 사용하여 AWS Support 사례를 생성하거나 (로그인 필요) 애플리케이션 가용성에 영향을 미치는 DDoS 관련 이벤트가 있는 API 경우 Support로 에스컬레이션할 수 있습니다.

결론

이 백서에 설명된 모범 사례는 많은 일반적인 인프라 및 애플리케이션 계층 DDoS 공격을 방지하여 애플리케이션의 가용성을 보호하는 DDoS 복원력 있는 아키텍처를 구축하는 데 도움이 될 수 있습니다. 애플리케이션을 설계할 때 이러한 모범 사례를 따르는 정도는 방어할 수 있는 DDoS 공격의 유형, 벡터 및 볼륨에 영향을 미칩니다. 완화 서비스에 가입하지 않고도 복원력을 통합할 수 있습니다DDoS. 구독을 AWS Shield Advanced 선택하면 이미 복원력이 뛰어난 애플리케이션 아키텍처를 더욱 보호하는 추가 지원, 가시성, 완화 및 비용 보호 기능을 얻을 수 있습니다.

기여자

다음은 이 문서의 기여자입니다.

- 로드리고 페로니, 보안 전문가 AWS TAM
- 드미트리 노비코프, 솔루션 아키텍트 AWS
- 아흐라프 수크, AWS 솔루션스 아키텍트
- 조안나 녹스, 엔지니어링 AWS Support
- 아누 부테일, 솔루션 아키텍트 AWS
- 해리스 가다마누구, 엣지 스페셜리스트 SA AWS

참조 자료

추가 정보는 다음을 참조하세요.

- 구현 지침 AWS WAF (AWS 백서)
- NIS301 — Re:Inforce 2023: AWS 위협 인텔리전스가 관리형 방화벽 규칙이 되는 방법 (비디오) YouTube
- NET314- re:Invent 2022: (비디오) 를 사용하여 복원력이 뛰어난 애플리케이션 구축 DDoS AWS Shield YouTube
- SEC321- re:Invent 2020: 대응팀 에스컬레이션으로 시대를 앞서가세요 (비디오) DDoS YouTube
- 윌리엄 힐: 고성능 DDoS 보호 기능 AWS- 2020 (비디오) YouTube
- SEC407 - re:Invent 2019: 웹 애플리케이션 구축을 위한 defense-in-depth 접근 방식 (비디오) YouTube
- 2018년 DDoS완화 모범 사례 (비디오) AWS YouTube
- SID324— re:Invent 2017: 클라우드에서의 DDoS 대응 자동화 (비디오) YouTube
- CTD304 — re:Invent 2017: 다우 존스와 월스트리트 저널의 트래픽 급증 관리를 위한 여정 (동영상) YouTube
- 애플리케이션 계층 위협 완화 DDoS 및 애플리케이션 계층 위협 (비디오) YouTube
- CTD310 — re:Invent 2017: 엣지에서의 생활은 생각보다 안전합니다! Amazon과 함께 강력하게 구축하기 (YouTube 동영상)
- CloudFront, AWS Shield, AWS WAF (YouTube 동영상)

문서 수정

이 백서 업데이트에 대한 알림을 받으려면 피드를 구독하십시오. RSS

변경 사항	설명	날짜
백서 업데이트	양식 CloudFront 및 DNS 와일드카드 비용 보호 기능이 추가되었습니다OAC. 운영 기법, 캐싱, 속도 기반 규칙 및 관리형 규칙 그룹에 대한 확장된 논의. 아키텍처 다이어그램에 온프레미스를 추가하고, 중복을 제거하고, 텍스트를 명확히 하여 모호성을 제거했습니다.	2023년 8월 9일
백서 업데이트	명확성을 위해 수정되었습니다. 보안 그룹 연결 추적 및 Shield Advanced 자동 애플리케이션 계층 DDoS 완화와 같은 최신 권장 사항 및 기능을 포함하도록 업데이트되었습니다.	2022년 4월 13일
백서 업데이트	최신 권장 사항 및 기능을 포함하도록 업데이트되었습니다. AWS Global Accelerator 엣지에 대한 포괄적인 보호의 일환으로 추가되었습니다. AWS Firewall Manager DDoS이벤트에 대한 중앙 집중식 모니터링 및 비준수 리소스 자동 수정	2021년 9월 21일
백서 업데이트	악성 웹 요청 탐지 및 필터링 (BP1,BP2) 섹션의 캐시 버스팅 및 Scale to Abswor () 섹션의 ALB 사용을 명확히 설명하도록 업데이트되었습니다. ELB	2019년 12월 18일

	BP6 다이어그램과 표 2 (“지역 선택”) 가 업데이트되었습니다. 와 같습니다. BP8 자세한 내용이 포함된 BP7 섹션이 업데이트되었습니다.	
백서 업데이트	AWS WAF 로깅을 모범 사례로 포함하도록 업데이트되었습니다.	2018년 12월 1일
백서 업데이트	AWS WAF 기능 AWS Shield AWS Firewall Manager, 관련 모범 사례를 포함하도록 업데이트되었습니다.	2018년 6월 1일
백서 업데이트	규범적 아키텍처 지침을 추가하고 포함하도록 업데이트되었습니다. AWS WAF	2016년 6월 1일
최초 게시	백서가 게시되었습니다.	2015년 6월 1일

고지 사항

고객은 본 문서의 정보를 독립적으로 평가할 책임이 있습니다. 이 문서는 (a) 정보 제공만을 목적으로 하고, (b) 사전 통지 없이 변경될 수 있는 현재의 AWS 제품 제안 및 관행을 나타내며, (c) 계열사, 공급업체 또는 라이선스 제공자로부터 AWS 어떠한 약정이나 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 “있는 그대로” 제공됩니다. AWS 고객에 대한 책임과 책임은 AWS 계약에 의해 통제되며, 본 문서는 고객과 체결한 계약의 일부가 아니며 수정하지도 않습니다. AWS

AWS 용어집

최신 AWS 용어는 참조의 AWS 용어집을 참조하십시오.AWS 용어집

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.