AWS 백서

DDoS 복원성에 대한 AWS 모범 사례

DDoS 복원성에 대한 AWS 모범 사례: AWS 백서

Table of Contents

DDoS 복원력에 대한 AWS 모범 사례

게시 날짜: 2021년 9월 21일(문서 개정)

요약

분산 서비스 거부(DDoS) 공격 및 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 절감해야 합니다. Amazon Web Services(AWS)는 인터넷에서 악의적인 사용자로부터 방어하기 위한 도구, 모범 사례 및 서비스를 제공하기 위해 노력하고 있습니다. AWS의 올바른 서비스를 사용하면 고가용성, 보안 및 복원력을 보장할 수 있습니다.

본 백서에서는 AWS를 통해 AWS에서 실행되는 애플리케이션의 복원력을 향상시킬 수 있는 규범적인 DDoS 지침을 제공합니다. 여기에는 애플리케이션 가용성을 보호하는 지침으로 사용할 수 있는 DDoS 복원 참조 아키텍처가 포함됩니다. 또한 본 백서에서는 인프라 계층 공격 및 애플리케이션 계층 공격과 같은 다양한 공격 유형에 대해 설명합니다. AWS에서는 각 공격 유형을 관리하는 데 가장 효과적인 모범 사례를 설명합니다. 또한 DDoS 완화 전략에 적합한 서비스 및 기능에 대해 간략히 설명하고 각 서비스를 사용하여 애플리케이션을 보호하는 방법에 대해서도 설명합니다.

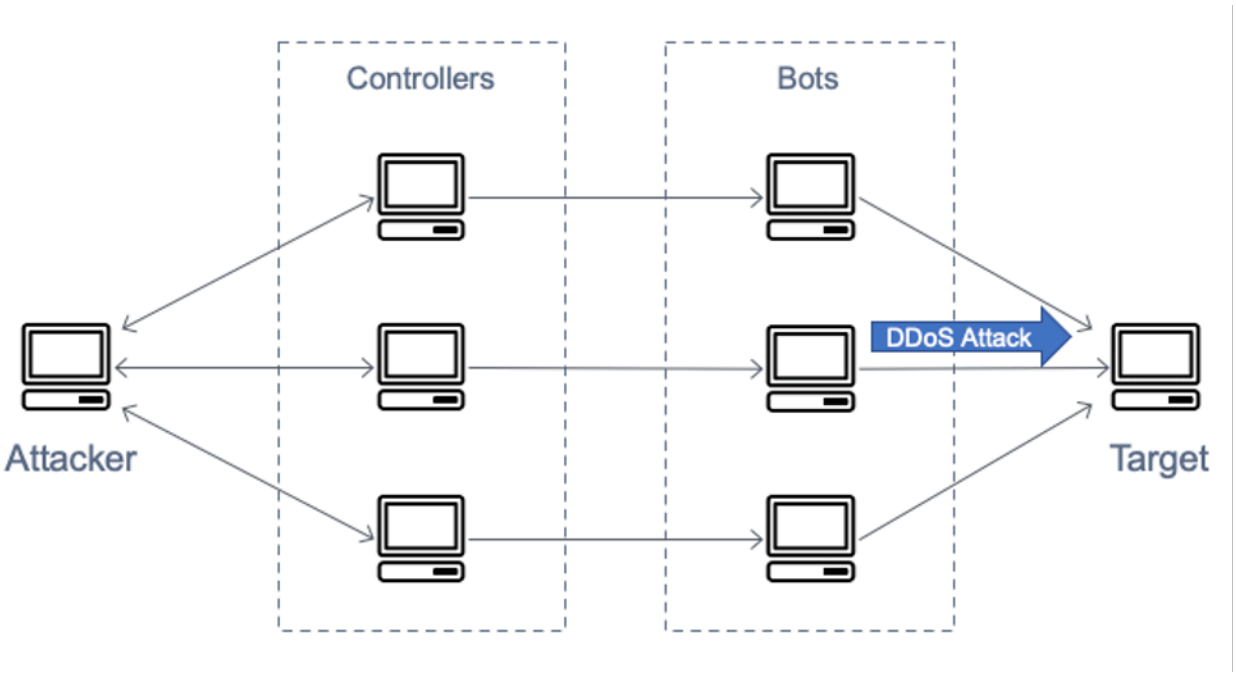
본 문서는 네트워킹, 보안 및 AWS의 기본 개념을 잘 알고 있는 IT 의사 결정권자 및 보안 엔지니어를 대상으로 작성되었습니다. 각 섹션에는 모범 사례 또는 기능에 대한 자세한 정보를 제공하는 AWS 설명서에 대한 링크가 있습니다.

소개: 서비스 거부 공격

서비스 거부(DoS) 공격은 네트워크 트래픽을 플러딩하는 것과 같이 사용자가 웹 사이트나 애플리케이션을 사용할 수 없도록 하려는 의도적인 시도입니다. 공격자는 많은 양의 네트워크 대역폭을 소비하거나 다른 시스템 리소스를 연결하여 합법적인 사용자의 액세스를 방해하는 다양한 기술을 사용합니다. 가장 간단한 형태의 단독 공격자는 다음 이미지와 같이 단일 소스를 사용하여 대상에 대해 DoS 공격을 수행합니다.

표 1: DoS 공격 다이어그램

DDoS 공격에서 공격자는 여러 소스를 사용하여 대상에 대한 공격을 오케스트레이션합니다. 이러한 소스에는 맬웨어에 감염된 컴퓨터, 라우터, IoT 디바이스 및 기타 엔드포인트의 분산 그룹이 포함될 수 있습니다. 다음 다이어그램은 손상된 호스트의 네트워크가 공격에 참여하여 대상을 압도하는 패킷 또는 요청 flood를 생성하는 것을 보여줍니다.



DDoS 공격 다이어그램

개방형 시스템 상호 연결(OSI) 모델에는 7개의 계층이 있으며 개방형 시스템 상호 연결(OSI) 모델 표에 설명되어 있습니다. DDoS 공격은 계층 3, 4, 6, 7에서 가장 일반적입니다. 계층 3 및 4 공격은 OSI 모델의 네트워크 및 전송 계층에 해당합니다. 본 문서에서 AWS는 이를 총칭하여 인프라 계층 공격이라고 합니다. 계층 6 및 7 공격은 OSI 모델의 프레젠테이션 및 애플리케이션 계층에 해당합니다. AWS는 애

플리케이션 계층 공격으로 이러한 문제를 함께 해결할 것입니다. 이러한 공격 유형의 예는 다음 섹션에서 설명합니다.

개방형 시스템 상호 연결(OSI) 모델

#	계층	단위	설명	벡터 예제
7	애플리케이션	데이터	애플리케이션에 대한 네트워크 프로세스	HTTP flood, DNS 쿼리 flood
6	프레젠테이션	데이터	데이터 표현 및 암호화	TLS 부정 사용
5	세션	데이터	호스트 간 통신	해당 없음
4	전송	세그먼트	엔드 투 엔드 연결 및 안정성	SYN flood
3	네트워크	패킷	경로 결정 및 논리적 주소 지정	UDP 반사 공격
2	데이터 링크	프레임	물리적 주소 지정	해당 없음
1	물리적	비트	미디어, 신호 및 바이너리 전송	해당 없음

주제

인프라 계층 공격

가장 일반적인 DDoS 공격인 UDP(User Datagram Protocol) 반사 공격과 SYN(동기화) flood는 인프라 계층 공격입니다. 공격자는 이러한 방법 중 하나를 사용하여 네트워크 용량을 넘치게 하거나 서버, 방화벽, 침입 방지 시스템(IPS) 또는 로드 밸런서와 같은 시스템의 리소스를 연결할 수 있는 대량의 트래픽을 생성할 수 있습니다. 이러한 공격을 쉽게 식별할 수 있지만 효과적으로 완화하려면 인바운드 트래

픽 flood보다 더 빠르게 용량을 확장하는 네트워크 또는 시스템이 있어야 합니다. 이 추가 용량은 공격 트래픽을 필터링하거나 흡수하여 시스템과 애플리케이션이 합법적인 고객 트래픽에 대응할 수 있도록 하는 데 필요합니다.

주제

UDP 반사 공격

UDP(User Datagram Protocol) 반사 공격은 UDP가 무상태 프로토콜이라는 사실을 악용합니다. 공격자는 공격 대상의 IP 주소를 UDP 소스 IP 주소로 나열하는 유효한 UDP 요청 패킷을 만들 수 있습니다. 공격자는 이제 UDP 요청 패킷의 소스 IP를 위조(스푸핑)합니다. UDP 패킷에는 스푸핑된 소스 IP가 포함되어 있으며 공격자가 중간 서버로 보냅니다. 서버는 UDP 응답 패킷을 공격자의 IP 주소로 되돌려 보내지 않고 대상 피해자 IP로 보내도록 속입니다. 중간 서버는 요청 패킷보다 몇 배 더 큰 응답을 생성하여 대상 IP 주소로 보내는 공격 트래픽의 양을 효과적으로 증폭하기 때문에 사용됩니다.

증폭 계수는 요청 크기에 대한 응답 크기의 비율이며 공격자가 사용하는 프로토콜(DNS, NTP, SSDP, CLDAP, Memcached, CharGen 또는 QOTD)에 따라 달라집니다. 예를 들어, DNS의 증폭 계수는 원래 바이트 수의 28~54배가 될 수 있습니다. 따라서 공격자가 64바이트의 요청 페이로드를 DNS 서버에 보내는 경우 공격 대상에 대해 3400바이트 이상의 원치 않는 트래픽을 생성할 수 있습니다. UDP 반사 공격은 다른 공격에 비해 더 많은 양의 트래픽을 담당합니다. UDP 반사 공격 그림은 반사 전술과 증폭 효과를 보여줍니다.

UDP 반사 공격

SYN flood 공격

사용자가 웹 서버와 같은 TCP(Transmission Control Protocol) 서비스에 연결하면 클라이언트가 SYN 동기화 패킷을 보냅니다. 서버는 확인 응답으로 SYN-ACK 패킷을 반환하고 마지막으로 클라이언트는 예상된 3방향 핸드셰이크를 완료하는 승인(ACK) 패킷으로 응답합니다. 다음 이미지는 이러한 일반적인 핸드셰이크를 보여줍니다.

SYN 3방향 핸드셰이크

SYN flood 공격에서 악의적인 클라이언트는 많은 수의 SYN 패킷을 전송하지만 핸드셰이크를 완료하기 위해 최종 ACK 패킷을 전송하지 않습니다. 서버는 반쯤 열린 TCP 연결에 대한 응답을 기다리며 결

국 새 TCP 연결을 수락할 수 있는 용량이 부족해집니다. 이로 인해 새 사용자가 서버에 연결하지 못할 수 있습니다. 이 공격은 사용 가능한 서버 연결을 연결하여 합법적인 연결에 리소스를 사용할 수 없도록 하려고 합니다. SYN flood는 최대 수백 Gbps에 도달할 수 있지만 공격의 목적은 SYN 트래픽 볼륨을 늘리는 것이 아닙니다.

애플리케이션 계층 공격

공격자는 계층 7 또는 애플리케이션 계층 공격을 사용하여 애플리케이션 자체를 대상으로 지정할 수 있습니다. 이러한 공격에서는 SYN flood 인프라 공격과 마찬가지로, 공격자가 애플리케이션의 특정 함수에 오버로드하여 애플리케이션을 사용할 수 없게 하거나 합법적인 사용자가 응답하지 않도록 합니다. 때때로 소량의 네트워크 트래픽만 생성하는 매우 낮은 요청 볼륨으로 이를 달성할 수 있습니다. 이로 인해 공격을 감지하고 완화하기가 어려울 수 있습니다. 애플리케이션 계층 공격의 예로는 HTTP flood, 캐시 버스팅 공격 및 WordPress XML-RPC flood가 있습니다.

HTTP flood 공격에서 공격자는 웹 애플리케이션의 유효한 사용자가 보낸 것처럼 보이는 HTTP 요청을 보냅니다. 일부 HTTP flood는 특정 리소스를 대상으로 하는 반면 더 복잡한 HTTP flood는 애플리케이션과 인간의 상호 작용을 에뮬레이트하려고 시도합니다. 이로 인해 요청 속도 제한과 같은 일반적인 완화 기술을 사용하는 데 어려움이 증가될 수 있습니다.

캐시 버스팅 공격은 쿼리 문자열의 변형을 사용하여 콘텐츠 전송 네트워크(CDN) 캐싱을 우회하는 HTTP flood 유형입니다. 캐시된 결과를 반환할 수 있는 대신 CDN은 모든 페이지 요청에 대해 원본 서버에 연결해야 하며 이러한 원본 가져오기는 애플리케이션 웹 서버에 추가적인 부담을 줍니다.

WordPress 핑백 flood라고도 하는 WordPress XML-RPC flood 공격에서는 공격자가 WordPress 콘텐츠 관리 소프트웨어에서 호스팅되는 웹 사이트를 대상으로 지정합니다. 공격자는 XML-RPC API 함수를 오용하여 대량의 HTTP 요청을 생성합니다. 핑백 기능을 사용하면 WordPress(사이트 A)에서 호스팅되는 웹 사이트가 사이트 A가 사이트 B에 대해 생성한 링크를 통해 다른 WordPress 사이트(사이트 B)에 알릴 수 있습니다. 그런 다음 사이트 B는 사이트 A를 가져와 링크가 있는지 확인합니다. 핑백 flood에서 공격자는 이 기능을 오용하여 사이트 B가 사이트 A를 공격하도록 합니다. 이러한 유형의 공격에는 명확한 서명이 있습니다. WordPress는 일반적으로 HTTP 요청 헤더의 User-Agent에 있습니다.

다른 형태의 악성 트래픽이 애플리케이션의 가용성에 영향을 줄 수도 있습니다. 스크레이퍼 봇은 콘텐츠를 훔치거나 가격과 같은 경쟁 정보를 기록하기 위해 웹 애플리케이션에 액세스하려는 시도를 자동화합니다. 무차별 대입 공격 및 크리덴셜 스터핑 공격은 애플리케이션의 보안 영역에 대한 무단 액세스를 얻기 위해 프로그래밍되는 작업입니다. 이는 엄밀히 말하면 DDoS 공격이 아닙니다. 그러나 자동화된 특성은 DDoS 공격과 유사하게 보일 수 있으며 본 백서에서 다룰 동일한 모범 사례를 구현하여 완화할 수 있습니다.

애플리케이션 계층 공격은 도메인 이름 시스템(DNS) 서비스도 대상으로 할 수 있습니다. 이러한 공격 중 가장 일반적인 것은 공격자가 잘 구성된 DNS 쿼리를 많이 사용하여 DNS 서버의 리소스를 고갈시키는 DNS 쿼리 flood입니다. 이러한 공격에는 공격자가 하위 도메인 문자열을 무작위로 지정하여 지정된 확인자의 로컬 DNS 캐시를 우회하는 캐시 버스트 구성 요소도 포함될 수 있습니다. 결과적으로 확인자는 캐시된 도메인 쿼리를 활용할 수 없으며 대신 권한 있는 DNS 서버에 반복적으로 연결해야 하므로 공격이 증폭됩니다.

웹 애플리케이션이 전송 계층 보안(TLS)을 통해 전달되는 경우 공격자는 TLS 협상 프로세스를 공격하도록 선택할 수도 있습니다. TLS는 계산 비용이 많이 들기 때문에 공격자는 읽을 수 없는 데이터(또는 이해할 수 없는(암호문))를 합법적인 핸드셰이크로 처리하기 위해 서버에 추가 워크로드를 생성하여 서버의 가용성을 줄일 수 있습니다. 이 공격의 변형에서 공격자는 TLS 핸드셰이크를 완료하지만 암호화 방법을 영구적으로 재협상합니다. 공격자는 대안으로 여러 TLS 세션을 열고 닫아 서버 리소스를 고갈시키려고 시도할 수 있습니다.

완화 기법

일부 형태의 DDoS 완화는 AWS 서비스에 자동으로 포함됩니다. 다음 섹션에서 설명하는 특정 서비스가 포함된 AWS 아키텍처를 사용하고 사용자와 애플리케이션 간의 네트워크 흐름의 각 부분에 대한 추가 모범 사례를 구현하여 DDoS 복원력을 더욱 향상시킬 수 있습니다.

모든 AWS 고객은 추가 비용 없이 AWS Shield Standard에 의한 자동 보호를 받을 수 있습니다. AWS Shield Standard는 웹 사이트나 애플리케이션을 대상으로 가장 흔하고, 자주 발생하는 네트워크 및 전송 계층 DDoS 공격을 방어합니다. 이 보호 기능은 항상 켜져 있고 사전 구성되어 있으며 정적이며 보고 또는 분석을 제공하지 않습니다. 모든 AWS 서비스와 모든 AWS 리전에서 제공됩니다. AWS 리전에서 DDoS 공격이 감지되면 Shield Standard 시스템이 자동으로 트래픽의 기준선을 설정하고 이상을 식별하며 필요에 따라 완화를 생성합니다. AWS Shield Standard를 DDoS 복원 아키텍처의 일부로 사용하여 웹 및 웹 이외의 애플리케이션을 모두 보호할 수 있습니다.

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

Amazon CloudFront, Global Accelerator 및 Amazon Route 53을 사용하면 다음과 같은 이점이 있습니다.

- AWS 글로벌 엣지 네트워크에서 인터넷 및 DDoS 완화 용량에 대한 액세스. 이는 테라비트 규모에 도달할 수 있는 더 큰 볼륨 공격을 완화하는 데 유용합니다.
- AWS Shield DDoS 완화 시스템은 AWS 엣지 서비스와 통합되어 완화 시간을 몇 분에서 1초 미만으로 단축합니다.
- 무상태 SYN flood 완화 기법은 들어오는 연결을 보호된 서비스에 전달하기 전에 프록시하고 확인합니다. 이렇게 하면 유효한 연결만 애플리케이션에 도달하는 동시에 합법적인 최종 사용자를 오탐지 삭제로부터 보호할 수 있습니다.
- 대규모 DDoS 공격의 영향을 분산하거나 격리하는 자동 트래픽 엔지니어링 시스템. 이러한 모든 서비스는 공격이 원본에 도달하기 전에 소스에서 공격을 격리하므로 이러한 서비스로 보호되는 시스템에 미치는 영향이 줄어듭니다.
- 현재 애플리케이션 아키텍처를 변경할 필요가 없는 AWS WAF와 결합된 애플리케이션 계층 방어(예: AWS 리전 또는 온프레미스 데이터 센터).

AWS의 인바운드 데이터 전송에는 요금이 부과되지 않으며 AWS Shield로 완화되는 DDoS 공격 트래픽에 대해서는 비용을 지불하지 않습니다. 다음 아키텍처 다이어그램에는 AWS 글로벌 엣지 네트워크 서비스가 포함되어 있습니다.

이 아키텍처에는 DDoS 공격에 대한 웹 애플리케이션의 복원력을 향상시키는 데 도움이 되는 여러 AWS 서비스가 포함되어 있습니다. 모범 사례 요약 표에는 이러한 서비스 및 해당 서비스가 제공할 수 있는 기능에 대한 요약이 제공됩니다. AWS는 본 문서 내에서 더 쉽게 참조할 수 있도록 각 서비스에 모범 사례 표시기(BP1, BP2)로 태그를 지정했습니다. 예를 들어, 다음 섹션에서는 모범 사례 표시기 BP1을 포함하는 Amazon CloudFront 및 Global Accelerator에서 제공하는 기능에 대해 설명합니다.

표 2 - 모범 사례 요약

AWS 엣지	AWS 리전					
	Amazon CloudFront(BP1) 및 AWS WAF(BP2) 사용	Global Accelerator(BP1) 사용	Amazon Route 53(BP 사용	Elastic Load Balancing (BP6) 및 AWS WAF(BP2) 사용	Amazon VPC(BP5)에서 보안 그룹 및 네트워크 ACL 사용	Amazon EC2 Auto Scaling(BP7) 사용
계층 3(예: UDP 반사) 공격 완화	✓	✓	✓	✓	✓	✓
계층 4(예: SYN flood) 공격 완화	✓	✓	✓	✓		
계층 6(예: TLS) 공격 완화	✓	✓	✓	✓		
공격 대상 영역 축소	✓	✓	✓	✓	✓	

AWS 엣지	AWS 리전					
애플리케이션 계층 트래픽을 흡수하도록 확장	✓	✓	✓	✓	✓	✓
계층 7(애플리케이션 계층) 공격 완화	✓	✓(*)	✓	✓	✓(*)	✓(*)
과도한 트래픽 및 대규모 DDoS 공격의 지리적 격리 및 분산	✓	✓	✓			
✓(*): Application Load Balancer와 AWS WAF를 함께 사용하는 경우						

DDoS 공격에 대응하고 완화할 준비를 개선하는 또 다른 방법은 AWS Shield Advanced를 구독하는 것입니다.

고객은 다음을 기반으로 맞춤형 탐지를 받습니다.

- 애플리케이션의 특정 트래픽 패턴
- 추가 비용 없이 AWS WAF를 포함한 계층 7 DDoS 공격으로부터 보호
- AWS SRT의 연중무휴 전문 지원 액세스

- AWS Firewall Manager를 통한 보안 정책 중앙 집중식 관리
- DDoS 관련 사용량 급증으로 인한 확장 요금으로부터 보호하기 위한 비용 보호

이 선택적 DDoS 완화 서비스는 모든 AWS 리전에서 호스팅되는 애플리케이션을 보호하는 데 도움이 됩니다. 이 서비스는 CloudFront, Route 53, Global Accelerator에 대해 전 세계적으로 제공됩니다. 탄력적 IP 주소와 함께 Shield Advanced를 사용하면 Network Load Balancer(NLB) 또는 Amazon EC2 인스턴스를 보호할 수 있습니다.

AWS Shield Advanced 사용의 이점은 다음과 같습니다.

- 애플리케이션 가용성에 영향을 미치는 DDoS 공격 완화 지원을 위해 AWS SRT에 액세스
- AWS Management Console, API, Amazon CloudWatch 지표 및 경보를 사용한 DDoS 공격 가시성
- 지난 13개월 동안의 모든 DDoS 이벤트 기록에 대한 액세스
- 애플리케이션 계층 DDoS 공격 완화를 위한 추가 비용 없이 AWS 웹 애플리케이션 방화벽(AWS WAF) 액세스(Amazon CloudFront 또는 Application Load Balancer와 함께 사용하는 경우)
- AWS WAF와 함께 사용하는 경우 웹 트래픽 속성의 자동 기준 설정
- 자동화된 정책 시행을 위해 추가 비용 없이 AWS Firewall Manager 액세스
- 트래픽을 DDoS 완화 시스템으로 더 일찍 라우팅하고 탄력적 IP 주소와 함께 사용할 경우 Amazon EC2 또는 Network Load Balancer에 대한 공격 완화 시간을 개선할 수 있는 민감한 감지 임계값
- DDoS 공격으로 인한 확장 관련 비용의 제한된 환불을 요청할 수 있는 비용 보호
- AWS Shield Advanced 고객을 위한 향상된 서비스 수준 계약
- Shield 이벤트 감지 시 AWS SRT의 사전 참여
- 여러 리소스를 하나의 단위로 처리하여 애플리케이션에 대한 탐지 및 완화 범위를 사용자 지정하는 셀프 서비스 방식을 제공하여 리소스를 번들화할 수 있는 보호 그룹입니다. 리소스 그룹화는 탐지 정확도를 높이고 오탐지를 최소화하며 새로 생성된 리소스의 자동 보호를 용이하게 하고 단일 애플리케이션을 구성하는 많은 리소스에 대한 공격을 완화하는 시간을 단축합니다. 보호 그룹에 대한 정보는 Shield Advanced 보호 그룹을 참조하세요.

AWS Shield Advanced 기능의 전체 목록과 AWS Shield에 대한 자세한 내용은 AWS Shield작동 방식을 참조하세요.

주제

- DDoS 완화를 위한 모범 사례
- 크기 조정을 위해 AWS 엣지 로케이션 활용(BP1, BP3)

- 애플리케이션 계층 방어(BP1, BP2)

DDoS 완화를 위한 모범 사례

다음 섹션에서는 DDoS 완화에 권장되는 각 모범 사례에 대해 자세히 설명합니다. 정적 또는 동적 웹 애플리케이션을 위한 DDoS 완화 계층 구축에 대한 빠르고 구현하기 쉬운 가이드는 DDoS 공격으로부터 동적 웹 애플리케이션을 보호하는 방법을 참조하세요.

인프라 계층 방어(BP1, BP3, BP6, BP7)

기존 데이터 센터 환경에서는 용량 초과 프로비저닝, DDoS 완화 시스템 배포 또는 DDoS 완화 서비스의 도움으로 트래픽 스크러빙과 같은 기술을 사용하여 인프라 계층 DDoS 공격을 완화할 수 있습니다. AWS에서는 DDoS 완화 기능이 자동으로 제공됩니다. 그러나 이러한 기능을 가장 잘 활용하고 초과 트래픽에 맞게 확장할 수 있는 아키텍처를 선택하여 애플리케이션의 DDoS 복원력을 최적화할 수 있습니다.

볼륨 측정 DDoS 공격을 완화하는 데 도움이 되는 주요 고려 사항에는 충분한 전송 용량과 다양성을 사용할 수 있는지 확인하고 공격 트래픽으로부터 Amazon EC2 인스턴스와 같은 AWS 리소스를 보호하는 것이 포함됩니다.

일부 Amazon EC2 인스턴스 유형은 대용량 트래픽을 보다 쉽게 처리할 수 있는 기능(예: 최대 100Gbps 네트워크 대역폭 인터페이스 및 향상된 네트워킹)을 지원합니다. 이렇게 하면 Amazon EC2 인스턴스에 도달한 트래픽에 대한 인터페이스 정체를 방지하는 데 도움이 됩니다. 향상된 네트워킹을 지원하는 인스턴스는 기존 구현에 비해 더 높은 I/O 성능, 더 높은 대역폭 및 더 낮은 CPU 사용률을 제공합니다. 이렇게 하면 인스턴스가 대량의 트래픽을 처리할 수 있는 능력이 향상되고 궁극적으로 초당 패킷(pps) 로드에 대한 복원력이 높아집니다.

이러한 높은 수준의 복원력을 허용하기 위해 AWS는 접미사가 N이고 네트워크 대역폭이 최대 100Gbps인 향상된 네트워킹을 지원하는 네트워킹 처리량이 더 높은 Amazon EC2 전용 인스턴스 또는 Amazon EC2 인스턴스를 사용할 것을 권장합니다(예: c6gn.16xlarge 및 c5n.18xlarge 또는 메탈 인스턴스(예: c5n.metal)).

100기가비트 네트워크 인터페이스 및 향상된 네트워킹을 지원하는 Amazon EC2 인스턴스에 대한 자세한 내용은 Amazon EC2 인스턴스 유형을 참조하세요.

향상된 네트워킹에 필요한 모듈과 필수 enaSupport 속성 세트는 Amazon Linux 2 및 최신 버전의 Amazon Linux AMI에 포함되어 있습니다. 따라서 지원되는 인스턴스 유형에서 Amazon Linux의 HVM 버전을 사용하여 인스턴스를 시작하면, 향상된 네트워킹이 이미 해당 인스턴스에서 활성화된 상태입

니다. 자세한 내용은 향상된 네트워킹 기능 활성화 여부 테스트를 참조하세요. 향상된 네트워킹을 활성화하는 방법에 대한 자세한 내용은 Linux에서 향상된 네트워킹을 참조하세요.

Amazon EC2 및 Auto Scaling(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 인스턴스에 트래픽을 분산할 수 있습니다. 이러한 인스턴스는 플래시 크라우드 또는 애플리케이션 계층 DDoS 공격을 포함하여 어떤 이유로든 발생하는 갑작스러운 트래픽 급증을 처리할 수 있습니다. Auto Scaling을 시작하도록 Amazon CloudWatch 경보를 설정하여 CPU, RAM, 네트워크 I/O 및 사용자 지정 지표와 같이 정의한 이벤트에 대한 응답으로 Amazon EC2 플릿의 크기를 자동으로 조정할 수 있습니다. 이 접근 방식은 요청 볼륨이 예기치 않게 증가할 때 애플리케이션 가용성을 보호합니다. Amazon CloudFront, Application Load Balancer, Classic Load Balancer 또는 Network Load Balancer를 애플리케이션과 함께 사용할 때 TLS 협상은 배포(Amazon CloudFront) 또는 로드 밸런서에서 처리됩니다. 이러한 기능은 합법적인 요청 및 TLS 부정 사용 공격을 처리하도록 확장하여 인스턴스가 TLS 기반 공격의 영향을 받지 않도록 보호합니다.

Amazon CloudWatch를 사용하여 Auto Scaling을 호출하는 방법에 대한 자세한 내용은 Auto Scaling 그룹 및 인스턴스에 대한 Amazon CloudWatch 지표 모니터링을 참조하세요.

Amazon EC2는 요구 사항 변경에 따라 빠르게 확장 또는 축소할 수 있도록 크기 조정 가능한 컴퓨팅 용량을 제공합니다. Amazon EC2 Auto Scaling 그룹의 크기 조정을 통해 애플리케이션에 인스턴스를 자동으로 추가하여 수평으로 확장할 수 있고 더 큰 EC2 인스턴스 유형을 사용하여 수직으로 확장할 수 있습니다.

Elastic Load Balancing(BP6)

대규모 DDoS 공격은 단일 Amazon EC2 인스턴스의 용량을 압도할 수 있습니다. Elastic Load Balancing(ELB)을 사용하면 여러 백엔드 인스턴스에 트래픽을 분산하여 애플리케이션 과부하 위험을 줄일 수 있습니다. Elastic Load Balancing은 자동으로 확장할 수 있으므로, 예를 들어 플래시 크라우드 또는 DDoS 공격으로 인해 예상치 못한 추가 트래픽이 발생할 때 더 큰 볼륨을 관리할 수 있습니다. Amazon VPC 내에 구축된 애플리케이션의 경우 애플리케이션 유형에 따라 Application Load Balancer(ALB), Classic Load Balancer(CLB) 및 Network Load Balancer(NLB) 세 가지 유형의 ELB를 고려해야 합니다.

웹 애플리케이션의 경우 Application Load Balancer를 사용하여 콘텐츠를 기반으로 트래픽을 라우팅하고 올바른 형식의 웹 요청만 수락할 수 있습니다. Application Load Balancer는 SYN flood 또는 UDP 반사 공격과 같은 많은 일반적인 DDoS 공격을 차단하여 공격으로부터 애플리케이션을 보호합니다.

Application Load Balancer는 이러한 유형의 공격이 감지되면 추가 트래픽을 흡수하도록 자동으로 확장됩니다. 인프라 계층 공격으로 인한 크기 조정 활동은 AWS 고객에게 투명하며 청구서에 영향을 미치지 않습니다.

Application Load Balancer로 웹 애플리케이션을 보호하는 방법에 대한 자세한 내용은 Application Load Balancer 시작하기를 참조하세요.

TCP 기반 애플리케이션의 경우 Network Load Balancer를 사용하여 매우 짧은 대기 시간으로 트래픽을 대상(예: Amazon EC2 인스턴스)으로 라우팅할 수 있습니다. Network Load Balancer의 한 가지 주요 고려 사항은 유효한 리스너의 로드 밸런서에 도달하는 모든 트래픽이 흡수되지 않고 대상으로 라우팅된다는 것입니다. Shield Advanced를 사용하여 탄력적 IP 주소에 대한 DDoS 보호를 구성할 수 있습니다. 탄력적 IP 주소가 가용 영역별로 Network Load Balancer에 할당되면 Shield Advanced는 Network Load Balancer 트래픽에 관련 DDoS 보호를 적용합니다.

Network Load Balancer로 TCP 애플리케이션을 보호하는 방법에 대한 자세한 내용은 Network Load Balancer 시작하기를 참조하세요.

크기 조정을 위해 AWS 엣지 로케이션 활용(BP1, BP3)

대규모의 다양한 인터넷 연결에 대한 액세스는 대기 시간 및 사용자 처리량을 최적화하고, DDoS 공격을 흡수하고, 장애 지점을 격리하는 동시에 애플리케이션 가용성에 미치는 영향을 최소화하는 능력을 크게 향상시킬 수 있습니다. AWS 엣지 로케이션은 Amazon CloudFront, Global Accelerator 및 Amazon Route 53을 사용하는 모든 웹 애플리케이션에 이러한 이점을 제공하는 네트워크 인프라의 추가 계층을 제공합니다. 이러한 서비스를 사용하면 AWS 리전에서 실행되는 애플리케이션을 엣지에서 포괄적으로 보호할 수 있습니다.

엣지에서 웹 애플리케이션 제공(BP1)

Amazon CloudFront는 정적, 동적, 스트리밍 및 대화형 콘텐츠를 비롯한 전체 웹 사이트를 제공하는 데 사용할 수 있는 서비스입니다. 영구 연결 및 가변 유지 시간(TTL) 설정을 사용하여 캐시 가능한 콘텐츠를 제공하지 않는 경우에도 원본에서 트래픽을 오프로드할 수 있습니다. 이러한 CloudFront 기능을 사용하면 원본에 대한 요청 및 TCP 연결 수가 줄어들어 HTTP flood로부터 웹 애플리케이션을 보호하는 데 도움이 됩니다. CloudFront는 올바른 형식의 연결만 허용하므로 SYN flood 및 UDP 반사 공격과 같은 많은 일반적인 DDoS 공격이 원본에 도달하는 것을 방지할 수 있습니다. 또한 DDoS 공격이 소스와 지리적으로 가까운 곳에서 격리되므로 해당 트래픽이 다른 위치에 영향을 주는 것을 방지합니다. 이러한 기능을 통해 대규모 DDoS 공격 중에 사용자에게 계속해서 더욱 원활하게 트래픽을 제공할 수 있습니다. CloudFront를 사용하여 AWS 또는 인터넷의 다른 곳에서 원본을 보호할 수 있습니다.

Amazon S3을 사용하여 인터넷에서 정적 콘텐츠를 제공하는 경우 AWS는 Amazon CloudFront를 사용하여 버킷을 보호할 것을 권장합니다. 원본 액세스 ID(OAI)를 사용하여 사용자가 CloudFront URL을 통해서만 객체에 액세스하도록 할 수 있습니다.

OAI에 대한 자세한 내용은 원본 액세스 ID를 사용하여 Amazon S3 콘텐츠에 대한 액세스 제한을 참조하세요.

Amazon CloudFront를 사용하여 웹 애플리케이션의 성능을 보호하고 최적화하는 방법에 대한 자세한 내용은 CloudFront 시작하기를 참조하세요.

AWS Global Accelerator(BP1)를 사용하여 원본에서 멀리 떨어진 네트워크 트래픽 보호

Global Accelerator는 사용자 트래픽의 가용성과 성능을 최대 60%까지 향상시키는 네트워킹 서비스입니다. 이는 단일 AWS 리전에서 실행하든 여러 AWS 리전에서 실행하든 관계없이 사용자에게 가장 가까운 엣지 로케이션에서 트래픽을 수신하고 AWS 글로벌 네트워크 인프라를 통해 애플리케이션으로 라우팅하여 수행됩니다.

Global Accelerator는 사용자에게 가장 가까운 AWS 리전의 성능을 기반으로 TCP 및 UDP 트래픽을 최적의 엔드포인트로 라우팅합니다. 애플리케이션 장애 발생 시 Global Accelerator는 30초 내에 차선의 엔드포인트로 장애 조치를 수행합니다. Global Accelerator는 애플리케이션을 보호하기 위해 AWS 글로벌 네트워크의 방대한 용량과 Shield와의 통합(예: 새로운 연결 시도에 도전하고 합법적인 최종 사용자에게만 서비스를 제공하는 무상태 SYN 프록시 기능)을 사용합니다.

애플리케이션이 CloudFront에서 지원하지 않는 프로토콜을 사용하거나 글로벌 고정 IP 주소가 필요한 웹 애플리케이션을 운영하는 경우에도 엣지에서 웹 애플리케이션 제공 모범 사례와 동일한 많은 이점을 제공하는 DDoS 탄력적 아키텍처를 구현할 수 있습니다. 예를 들어 최종 사용자가 방화벽의 허용 목록에 추가할 수 있고 다른 AWS 고객이 사용하지 않는 IP 주소가 필요할 수 있습니다. 이러한 시나리오에서 Global Accelerator를 사용하여 Application Load Balancer에서 실행되는 웹 애플리케이션을 보호하고 AWS WAF과 함께 웹 애플리케이션 계층 요청 flood를 감지하고 완화할 수 있습니다.

Global Accelerator를 사용하여 네트워크 트래픽 성능을 보호하고 최적화하는 방법에 대한 자세한 내용은 Global Accelerator 시작하기를 참조하세요.

엣지에서 도메인 이름 확인(BP3)

Amazon Route 53은 트래픽을 웹 애플리케이션으로 전달하는 데 사용할 수 있는 가용성과 확장성이 뛰어난 도메인 이름 시스템(DNS) 서비스입니다. 여기에는 트래픽 흐름, 상태 확인 및 모니터링, 대기 시간 기반 라우팅, 지역 DNS와 같은 고급 기능이 포함됩니다. 이러한 고급 기능을 사용하면 서비스가

DNS 요청에 응답하는 방식을 제어하여 웹 애플리케이션의 성능을 개선하고 사이트 중단을 방지할 수 있습니다.

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

셔플 샤딩을 사용하면 위임 세트의 각 이름 서버가 고유한 엣지 로케이션 및 인터넷 경로 세트에 해당합니다. 이를 통해 내결함성이 향상하고 고객 간의 중복이 최소화됩니다. 위임 세트에 있는 하나의 이름 서버를 사용할 수 없는 경우 사용자는 다시 시도하고 다른 엣지 로케이션에 있는 다른 이름 서버의 응답을 받을 수 있습니다.

애니캐스트 스트라이핑을 사용하면 최적의 위치에서 각 DNS 요청을 처리할 수 있으므로 네트워크 부하를 분산시키고 DNS 대기 시간을 줄일 수 있습니다. 따라서 사용자에게 더 빠른 대응 속도를 제공합니다. 또한 Amazon Route 53은 DNS 쿼리의 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 참조하세요.

애플리케이션 계층 방어(BP1, BP2)

지금까지 본 백서에서 논의된 많은 기술은 인프라 계층 DDoS 공격이 애플리케이션의 가용성에 미치는 영향을 완화하는 데 효과적입니다. 또한 애플리케이션 계층 공격으로부터 방어하려면 악의적인 요청을 구체적으로 감지하고 흡수하도록 확장하고 차단할 수 있는 아키텍처를 구현해야 합니다. 네트워크 기반 DDoS 완화 시스템은 일반적으로 복잡한 애플리케이션 계층 공격을 완화하는 데 효과적이지 않기 때문에 이는 중요한 고려 사항입니다.

악성 웹 요청 감지 및 필터링(BP1, BP2)

애플리케이션이 AWS에서 실행될 때 Amazon CloudFront와 AWS WAF를 모두 활용하여 애플리케이션 계층 DDoS 공격을 방어할 수 있습니다.

Amazon CloudFront를 사용하면 정적 콘텐츠를 캐시하고 AWS 엣지 로케이션에서 제공할 수 있으므로 원본의 로드를 줄이는 데 도움이 됩니다. 또한 웹 이외의 트래픽이 원본에 도달하는 것을 방지하여 서버 로드를 줄이는 데 도움이 될 수 있습니다. 또한 CloudFront는 읽기 속도가 느리거나 쓰기 속도가 느린 공격자(예: Slowloris)의 연결을 자동으로 닫을 수 있습니다.

AWS WAF를 사용하면 CloudFront 배포 또는 Application Load Balancer에서 웹 액세스 제어 목록(ACL)을 구성하여 요청 서명을 기반으로 요청을 필터링하고 차단할 수 있습니다. 각 웹 ACL은 Uniform

Resource Identifier(URI), 쿼리 문자열, HTTP 메서드 또는 헤더 키와 같은 하나 이상의 요청 속성과 문자열 일치 또는 정규식이 일치하도록 구성할 수 있는 규칙으로 구성됩니다. 또한 AWS WAF의 비율 기반 규칙을 사용하여 규칙과 일치하는 요청이 사용자가 정의한 임계값을 초과할 경우 악의적인 행위자의 IP 주소를 자동으로 차단할 수 있습니다.

문제가 되는 클라이언트 IP 주소의 요청은 403 Forbidden 오류 응답을 수신하고 요청 빈도가 임계값 아래로 떨어질 때까지 차단된 상태로 유지됩니다. 이는 일반 웹 트래픽으로 위장한 HTTP flood 공격을 완화하는 데 유용합니다. IP 주소 평판을 기반으로 공격을 차단하려면 IP 일치 조건을 사용하여 규칙을 생성하거나 AWS Marketplace에서 판매자가 제공하는 AWS WAF에 대한 관리형 규칙을 사용할 수 있습니다. AWS WAF는 IP 평판 규칙 그룹을 선택할 수 있는 관리형 서비스로 AWS 관리형 규칙을 직접 제공합니다. Amazon IP 평판 목록 규칙 그룹에는 Amazon 내부 위협 인텔리전스를 기반으로 하는 규칙이 포함되어 있습니다. 이는 일반적으로 봇이나 다른 위협과 연결된 IP 주소를 차단하려는 경우에 유용합니다. 익명 IP 목록 규칙 그룹에는 뷰어 ID 난독화를 허용하는 서비스의 요청을 차단하는 규칙이 포함되어 있습니다. 여기에는 VPN, 프록시, Tor 노드 및 클라우드 플랫폼(AWS 포함)의 요청이 포함됩니다. AWS WAF 및 CloudFront에서는 지역 제한을 설정하여 선택한 국가의 요청을 차단하거나 허용할 수도 있습니다. 이렇게 하면 사용자에게 서비스를 제공할 것으로 예상되지 않는 지리적 위치의 공격을 차단하는 데 도움이 될 수 있습니다.

악의적인 요청을 식별하는 데 도움이 되도록 웹 서버 로그를 검토하거나 AWS WAF의 로깅 및 샘플링된 요청 기능을 사용하세요. AWS WAF 로깅을 활성화하면 웹 ACL에서 분석한 트래픽에 대한 자세한 정보를 얻을 수 있습니다. AWS WAF는 로그 필터링을 지원하므로 어떤 웹 요청이 기록되고 어떤 요청이 검사 후 로그에서 삭제되는지 지정할 수 있습니다.

로그에 기록되는 정보에는 AWS WAF가 AWS 리소스로부터 요청을 받은 시간, 요청에 대한 세부 정보, 요청된 각 규칙에 대한 일치 작업이 포함됩니다. 샘플링된 요청은 지난 3시간 동안 AWS WAF 규칙 중 하나와 일치하는 요청에 대한 세부 정보를 제공합니다. 이 정보를 사용하여 잠재적으로 악의적인 트래픽 서명을 식별하고 이러한 요청을 거부하는 새 규칙을 만들 수 있습니다. 임의의 쿼리 문자열이 포함된 여러 요청이 표시되면 애플리케이션의 캐시와 관련된 쿼리 문자열 파라미터만 허용해야 합니다. 이 기술은 원본에 대한 캐시 버스팅 공격을 완화하는 데 유용합니다.

AWS Shield Advanced를 구독하면 AWS Shield 대응 팀(SRT)과 협력하여 애플리케이션 가용성을 저해하는 공격을 완화하는 규칙을 생성할 수 있습니다. 계정의 Shield Advanced 및 AWS WAF API에 대한 제한된 액세스 권한을 AWS SRT에 부여할 수 있습니다. AWS SRT는 이러한 API에 액세스하여 명시적 권한 부여가 있는 경우에만 계정에 완화 조치를 취합니다. 자세한 내용은 본 문서의 지원 섹션을 참조하세요.

AWS Firewall Manager를 사용하여 조직 전체에서 Shield Advanced 보호 및 AWS WAF 규칙과 같은 보안 규칙을 중앙에서 구성하고 관리할 수 있습니다. AWS Organizations 관리 계정은 Firewall Manager 정책을 생성할 권한이 있는 관리자 계정을 지정할 수 있습니다. 이러한 정책을 사용하면 리소

스 유형 및 태그와 같은 기준을 정의하여 규칙이 적용되는 위치를 결정할 수 있습니다. 이는 여러 계정이 있고 보호를 표준화하려는 경우에 유용합니다.

또한

- AWS WAF용 AWS 관리형 규칙에 대한 자세한 내용은 AWS WAF용 AWS 관리형 규칙을 참조하세요.
- 지리적 제한을 사용하여 CloudFront 배포에 대한 액세스를 제한하는 방법은 콘텐츠의 지리적 배포 제한을 참조하세요.
- AWS WAF 사용 방법에 대해서는 다음을 참조하세요.
  - AWS WAF 시작하기
  - 웹 ACL 트래픽 정보 로깅
  - 웹 요청 샘플 보기
- 비율 기반 규칙 구성은 AWS WAF에 대해 비율 기반 규칙을 사용하여 웹 사이트 및 서비스 보호를 참조하세요.
- Firewall Manager를 사용하여 AWS 리소스 전반에 걸쳐 AWS WAF 규칙 배포를 관리하는 방법은 다음을 참조하세요.
  - Firewall Manager AWS WAF 정책 시작하기
  - Firewall Manager Shield Advanced 정책 시작하기

공격 대상 영역 감소

AWS 솔루션을 설계할 때 또 다른 중요한 고려 사항은 공격자가 애플리케이션을 대상으로 할 수 있는 기회를 제한하는 것입니다. 이 개념을 공격 대상 영역 감소라고 합니다. 인터넷에 노출되지 않은 리소스는 공격하기가 더 어렵기 때문에 공격자가 애플리케이션의 가용성을 목표로 삼을 수 있는 옵션이 제한됩니다.

예를 들어 사용자가 특정 리소스와 직접 상호 작용할 것으로 예상하지 않는 경우 인터넷에서 해당 리소스에 액세스할 수 없도록 합니다. 마찬가지로, 통신에 필요하지 않은 포트 또는 프로토콜에서 사용자 또는 외부 애플리케이션의 트래픽을 수락하지 마세요.

다음 섹션에서 AWS는 공격 대상 영역을 줄이고 애플리케이션의 인터넷 노출을 제한하는 데 도움이 되는 모범 사례를 제공합니다.

주제

AWS 리소스 난독화(BP1, BP4, BP5)

일반적으로 사용자는 AWS 리소스를 인터넷에 완전히 노출하지 않고도 애플리케이션을 빠르고 쉽게 사용할 수 있습니다. 예를 들어 Elastic Load Balancing 뒤에 Amazon EC2 인스턴스가 있는 경우 인스턴스 자체에 공개적으로 액세스할 필요가 없을 수 있습니다. 대신 특정 TCP 포트에서 Elastic Load Balancing에 대한 액세스 권한을 사용자에게 제공하고 Elastic Load Balancing만 인스턴스와 통신하도록 허용할 수 있습니다. Amazon Virtual Private Cloud(Amazon VPC) 내에서 보안 그룹 및 네트워크 액세스 제어 목록(NACL)을 구성하여 이를 설정할 수 있습니다. Amazon VPC를 통해 정의한 가상 네트워크에서 AWS 리소스를 실행할 수 있는 AWS 클라우드의 논리적으로 격리된 영역을 프로비저닝할 수 있습니다.

보안 그룹과 네트워크 ACL은 사용자가 VPC 내의 AWS 리소스에 대한 액세스를 제어할 수 있다는 점에서 유사합니다. 그러나 보안 그룹을 사용하면 인스턴스 수준에서 인바운드 및 아웃바운드 트래픽을 제어할 수 있으며 네트워크 ACL은 VPC 서브넷 수준에서 유사한 기능을 제공합니다. 보안 그룹 또는 네트워크 ACL 사용에 대한 추가 비용은 없습니다.

보안 그룹 및 네트워크 액세스 제어 목록(네트워크 ACL)(BP5)

인스턴스를 시작할 때 또는 나중에 인스턴스를 보안 그룹에 연결할 때 보안 그룹을 지정할 수 있습니다. 트래픽을 허용하는 허용 규칙을 생성하지 않는 한 보안 그룹에 대한 모든 인터넷 트래픽은 암시적으로 거부됩니다. 예를 들어 Elastic Load Balancing과 여러 Amazon EC2 인스턴스를 사용하는 웹 애

플리케이션이 있는 경우 Elastic Load Balancing(Elastic Load Balancing 보안 그룹)과 인스턴스(웹 애플리케이션 서버 보안 그룹)에 대해 하나씩 보안 그룹을 생성할 수 있습니다. 그런 다음 ELB 보안 그룹에 대한 인터넷 트래픽을 허용하는 허용 규칙과 ELB 보안 그룹에서 웹 애플리케이션 서버 보안 그룹으로의 트래픽을 허용하는 다른 규칙을 생성할 수 있습니다. 이렇게 하면 인터넷 트래픽이 Amazon EC2 인스턴스와 직접 통신할 수 없으므로 공격자가 애플리케이션에 대해 알아보고 영향을 받기가 더 어려워집니다.

네트워크 ACL을 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(CIDR 범위), 프로토콜 및 대상 포트를 정의할 수 있습니다. 애플리케이션이 TCP 트래픽에만 사용되는 경우, 모든 UDP 트래픽을 거부하는 규칙 또는 그 반대의 규칙을 만들 수 있습니다. 이 옵션은 소스 IP 또는 기타 서명을 알고 있을 때 공격을 완화하는 고유한 규칙을 생성할 수 있기 때문에 DDoS 공격에 대응할 때 유용합니다.

AWS Shield Advanced를 구독하면 탄력적 IP 주소를 보호 리소스로 등록할 수 있습니다. 보호 리소스로 등록된 탄력적 IP 주소에 대한 DDoS 공격은 더 빨리 탐지되므로 완화 시간이 더 빨라질 수 있습니다. 공격이 감지되면 DDoS 완화 시스템이 대상 탄력적 IP에 해당하는 네트워크 ACL을 읽고 AWS 네트워크 경계에서 적용합니다. 이를 통해 여러 인프라 계층 DDoS 공격으로 인한 영향의 위험을 크게 줄일 수 있습니다.

DDoS 복원력을 최적화하도록 보안 그룹 및 네트워크 ACL을 구성하는 방법에 대한 자세한 내용은 공격 대상 영역을 줄여 DDoS 공격에 대한 대비를 돕는 방법을 참조하세요.

탄력적 IP 주소와 함께 Shield Advanced를 보호 리소스로 사용하는 방법에 대한 자세한 내용은 AWS Shield Advanced 구독 단계를 참조하세요.

원본 보호(BP1, BP5)

VPC 내부에 있는 원본과 함께 Amazon CloudFront를 사용하는 경우 CloudFront 배포만 원본에 요청을 전달할 수 있도록 할 수 있습니다. Edge-to-Origin 요청 헤더를 사용하면 CloudFront에서 원본으로 요청을 전달할 때 기존 요청 헤더 값을 추가하거나 재정의할 수 있습니다. 원본 사용자 지정 헤더(예: X-Shared-Secret 헤더)를 사용하여 원본에 대한 요청이 CloudFront에서 전송되었는지 확인할 수 있습니다.

원본 사용자 지정 헤더로 원본을 보호하는 방법에 대한 자세한 내용은 사용자 지정 헤더를 원본 요청에 추가 및 Application Load Balancer에 대한 액세스 제한을 참조하세요.

원본 액세스 제한에 대해 원본 사용자 지정 헤더 값을 자동으로 교체하는 샘플 솔루션 구현에 대한 지침은 AWS WAF 및 Secrets Manager를 사용하여 Amazon CloudFront 원본 보안을 강화하는 방법을 참조하세요.

또는 AWS Lambda 함수를 사용하여 CloudFront 트래픽만 허용하도록 보안 그룹 규칙을 자동으로 업데이트할 수 있습니다. 이렇게 하면 악의적인 사용자가 웹 애플리케이션에 액세스할 때 CloudFront 및 AWS WAF를 우회할 수 없어 원본의 보안이 향상됩니다.

보안 그룹을 자동으로 업데이트하여 원본을 보호하는 방법에 대한 자세한 내용은 X-Shared-Secret 헤더, AWS Lambda를 이용하여 Amazon CloudFront 및 AWS WAF용 보안 그룹을 자동 업데이트하는 방법을 참조하세요.

API 엔드포인트 보호(BP4)

일반적으로 API를 공개해야 하는 경우 API 프런트 엔드가 DDoS 공격의 대상이 될 위험이 있습니다. 위험을 줄이기 위해 Amazon API Gateway를 Amazon EC2, AWS Lambda 또는 다른 곳에서 실행되는 애플리케이션의 진입로로 사용할 수 있습니다. Amazon API Gateway를 사용하면 API 프런트 엔드에 자체 서버가 필요하지 않으며 애플리케이션의 다른 구성 요소를 난독화할 수 있습니다. 애플리케이션의 구성 요소를 감지하기 어렵게 함으로써 해당 AWS 리소스가 DDoS 공격의 표적이 되는 것을 방지할 수 있습니다.

Amazon API Gateway를 사용할 때 두 가지 유형의 API 엔드포인트 중에서 선택할 수 있습니다. 첫 번째는 기본 옵션인 Amazon CloudFront 배포를 통해 액세스되는 엣지 최적화 API 엔드포인트입니다. 그러나 배포는 API Gateway에서 생성 및 관리하므로 사용자가 제어할 수 없습니다. 두 번째 옵션은 REST API가 배포된 동일한 AWS 리전에서 액세스하는 리전 API 엔드포인트를 사용하는 것입니다. AWS는 두 번째 유형의 엔드포인트를 사용하고 이를 자체 Amazon CloudFront 배포와 연결할 것을 권장합니다. 이를 통해 Amazon CloudFront 배포를 제어하고 애플리케이션 계층 보호를 위해 AWS WAF를 사용할 수 있습니다. 이 모드는 AWS 글로벌 엣지 네트워크에서 확장된 DDoS 완화 용량에 대한 액세스를 제공합니다.

Amazon CloudFront 및 AWS WAF를 Amazon API Gateway와 함께 사용하는 경우 다음 옵션을 구성합니다.

- 모든 헤더를 API Gateway 리전 엔드포인트로 전달하도록 배포에 대한 캐시 동작을 구성합니다. 이렇게 하면 CloudFront에서 콘텐츠를 동적으로 처리하고 콘텐츠 캐싱을 건너뜁니다.
- API Gateway에서 API 키 값을 설정하여 원본 사용자 지정 헤더 `x-api-key`를 포함하도록 배포를 구성하여 직접 액세스로부터 API Gateway를 보호합니다.
- REST API의 각 방법에 대한 표준 또는 버스트 속도 제한을 구성하여 과도한 트래픽으로부터 백엔드를 보호합니다.

Amazon API Gateway로 API를 생성하는 방법에 대한 자세한 내용은 Amazon API Gateway 시작하기를 참조하세요.

운영 기술

본 문서의 완화 기술은 DDoS 공격에 대해 기본적으로 복원력이 뛰어난 애플리케이션을 설계하는 데 도움이 됩니다. 대부분의 경우 DDoS 공격이 애플리케이션을 대상으로 삼는 시기를 파악하면 완화 단계를 취하는 데 도움이 됩니다. 이 섹션에서는 비정상 동작, 알림 및 자동화에 대한 가시성을 확보하고 대규모 보호를 관리하며 추가 지원을 위해 AWS에 참여하기 위한 모범 사례에 대해 설명합니다.

주제

가시성

주요 운영 지표가 예상 값을 크게 벗어나면 공격자가 애플리케이션의 가용성을 목표로 할 수 있습니다. 애플리케이션의 정상적인 동작에 익숙하다는 것은 이상을 감지했을 때 보다 신속하게 조치를 취할 수 있다는 것을 의미합니다. Amazon CloudWatch는 AWS에서 실행되는 애플리케이션을 모니터링하여 도움을 줄 수 있습니다. 예를 들어 지표를 수집 및 추적하고, 로그 파일을 수집 및 모니터링하며, 경보를 설정하고, AWS 리소스의 변경에 자동으로 대응할 수 있습니다.

애플리케이션을 설계할 때 DDoS 복원 참조 아키텍처를 따르는 경우 애플리케이션에 도달하기 전에 일반적인 인프라 계층 공격이 차단됩니다. AWS Shield Advanced를 구독하면 애플리케이션이 대상으로 지정되었음을 나타내는 여러 CloudWatch 지표에 액세스할 수 있습니다. 예를 들어, DDoS 공격이 진행 중일 때 알리도록 경보를 구성하여 애플리케이션 상태를 확인하고 AWS SRT에 참여할지 여부를 결정할 수 있습니다. 공격이 탐지되었는지 여부를 알려 주는 `DDoSDetected` 지표를 구성할 수 있습니다. 공격 볼륨을 기준으로 알림을 받으려면 `DDoSAttackBitsPerSecond`, `DDoSAttackPacketsPerSecond` 또는 `DDoSAttackRequestsPerSecond` 지표를 사용할 수도 있습니다. CloudWatch를 자체 도구와 통합하거나 Slack 또는 PagerDuty와 같은 서드 파티 도구를 사용하여 이러한 지표를 모니터링할 수 있습니다.

애플리케이션 계층 공격은 많은 Amazon CloudWatch 지표를 상승시킬 수 있습니다. AWS WAF를 사용하는 경우 CloudWatch를 사용하여 AWS WAF에서 허용, 계산 또는 차단하도록 설정한 요청의 증가에 대한 경보를 모니터링하고 활성화할 수 있습니다. 이렇게 하면 트래픽 수준이 애플리케이션에서 처리할 수 있는 수준을 초과할 경우 알림을 받을 수 있습니다. CloudWatch에서 추적되는 Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, Amazon EC2 및 Auto Scaling 지표를 사용하여 DDoS 공격을 나타낼 수 있는 변경 사항을 감지할 수도 있습니다.

권장되는 CloudWatch 지표 표에는 DDoS 공격을 감지하고 대응하는 데 일반적으로 사용되는 CloudWatch 지표에 대한 설명이 나와 있습니다.

표 3 - 권장되는 Amazon CloudWatch 지표

주제	지표	설명
AWS Shield Advanced	DDoSDetected	특정 Amazon 리소스 이름(ARN)에 대한 DDoS 이벤트를 나타냅니다.
AWS Shield Advanced	DDoSAttackBitsPerSecond	특정 ARN에 대한 DDoS 이벤트에서 관찰되는 바이트 수입니다. 이 지표는 계층 3/4 DDoS 이벤트에서만 제공됩니다.
AWS Shield Advanced	DDoSAttackPacketsPerSecond	특정 ARN에 대한 DDoS 이벤트에서 관찰되는 패킷 수입니다. 이 지표는 계층 3/4 DDoS 이벤트에서만 제공됩니다.
AWS Shield Advanced	DDoSAttackRequestsPerSecond	특정 ARN에 대한 DDoS 이벤트에서 관찰되는 요청 수입니다. 이 지표는 계층 7 DDoS 이벤트에서만 제공되며, 가장 중요한 계층 7 이벤트일 때만 보고됩니다.
AWS WAF	AllowedRequests	허용된 웹 요청 수입니다.
AWS WAF	BlockedRequests	차단된 웹 요청 수입니다.
AWS WAF	CountedRequests	계수된 웹 요청 수입니다.
AWS WAF	PassedRequests	전달된 요청 수입니다. 규칙 그룹 규칙과 일치하지 않고 규칙 그룹 평가를 통과하는 요청에만 사용됩니다.

주제	지표	설명
Amazon CloudFront	Requests	HTTP/S 요청 수입니다.
Amazon CloudFront	TotalErrorRate	HTTP 상태 코드가 4xx 또는 5xx인 모든 요청의 백분율입니다.
Amazon Route 53	HealthCheckStatus	상태 확인 엔드포인트의 상태입니다.
Application Load Balancer	ActiveConnectionCount	클라이언트에서 로드 밸런서로, 그리고 로드 밸런서에서 대상으로 동시에 연결되는 활성 TCP 연결 총 수입니다.
Application Load Balancer	ConsumedLCUs	로드 밸런서에서 사용하는 로드 밸런서 용량 단위(LCU) 수입니다.
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	로드 밸런서에서 생성된 HTTP 4xx 또는 5xx 클라이언트 오류 코드 수입니다.
Application Load Balancer	NewConnectionCount	클라이언트에서 로드 밸런서로, 그리고 로드 밸런서에서 대상으로 새롭게 구성된 총 TCP 연결 수입니다.
Application Load Balancer	ProcessedBytes	로드 밸런서에서 처리된 총 바이트 수입니다.
Application Load Balancer	RejectedConnectionCount	로드 밸런서가 최대 연결 수에 도달하여 거부된 연결 수입니다.
Application Load Balancer	RequestCount	처리된 요청 수입니다.

주제	지표	설명
Application Load Balancer	TargetConnectionErrorCount	로드 밸런서와 대상 사이에 성공적으로 구성되지 않은 연결 수입니다.
Application Load Balancer	TargetResponseTime	로드 밸런서에서 요청 신호를 전송한 후 대상에서 응답 신호가 수신될 때까지 결과된 시간(초)입니다.
Application Load Balancer	UnHealthyHostCount	비정상 상태로 간주되는 대상 수입니다.
Network Load Balancer	ActiveFlowCount	클라이언트에서 대상까지의 동시 TCP 흐름(또는 연결)의 총 수입니다.
Network Load Balancer	ConsumedLCUs	로드 밸런서에서 사용하는 로드 밸런서 용량 단위(LCU) 수입니다.
Network Load Balancer	NewFlowCount	해당 기간 동안 클라이언트에서 대상까지 설정되는 새로운 TCP 흐름(또는 연결)의 총 수입니다.
Network Load Balancer	ProcessedBytes	TCP/IP 헤더를 포함하여 로드 밸런서가 처리하는 총 바이트 수입니다.
Global Accelerator	NewFlowCount	해당 기간 동안 클라이언트에서 엔드포인트까지 설정되는 새로운 TCP 및 UDP 흐름(또는 연결)의 총 수입니다.
Global Accelerator	ProcessedBytesIn	TCP/IP 헤더를 포함하여 액셀러레이터에 의해 처리된 수신 바이트의 총 수입니다.

주제	지표	설명
Auto Scaling	GroupMaxSize	Auto Scaling 그룹의 최대 크기입니다.
Amazon EC2	CPUUtilization	현재 사용 중인 할당된 EC2 컴퓨팅 유닛(ECU)의 비율(%)입니다.
Amazon EC2	NetworkIn	모든 네트워크 인터페이스에서 인스턴스가 받은 바이트 수입니다.

Amazon CloudWatch를 사용하여 애플리케이션에 대한 DDoS 공격을 탐지하는 방법에 대한 자세한 내용은 Amazon CloudWatch 시작하기를 참조하세요.

이전 표의 일부 지표를 사용하여 구축된 대시보드의 예를 탐색하려면 사용자 정의 기준 모니터링 시스템을 참조하세요.

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

또한 글로벌 위협 환경 대시보드에서는 AWS에서 탐지된 모든 DDoS 공격에 대한 요약 정보를 제공합니다. 이 정보는 공격 경향뿐만 아니라 더 많은 애플리케이션에서 발생하는 DDoS 위협을 더 잘 이해하고 관찰된 공격과 비교하는 데 유용할 수 있습니다.

AWS Shield Advanced를 구독하면 서비스 대시보드는 보호된 리소스에서 탐지된 이벤트에 대한 추가 탐지 및 완화 지표와 네트워크 트래픽 세부 정보를 표시합니다. AWS Shield는 여러 차원에서 보호된 리소스에 대한 트래픽을 평가합니다. 이상이 감지된 경우 AWS Shield는 이벤트를 생성하고 이상이 관찰된 트래픽 차원을 보고합니다. 완화 기능을 사용하면 리소스가 과도한 트래픽과 알려진 DDoS 이벤트 서명과 일치하는 트래픽을 수신하지 않도록 보호할 수 있습니다.

탐지 지표는 웹 ACL이 보호된 리소스와 연결될 때 샘플링된 네트워크 흐름 또는 AWS WAF 로그를 기반으로 합니다. 완화 지표는 Shield의 DDoS 완화 시스템에서 관찰된 트래픽을 기반으로 합니다. 완화 지표는 리소스로 유입되는 트래픽을 보다 정확하게 측정합니다.

네트워크 상위 기여자 지표는 탐지된 이벤트 동안 트래픽이 어디에서 오는지 파악할 수 있는 인사이트를 제공합니다. 가장 높은 볼륨 기여자를 보고 프로토콜, 소스 포트 및 TCP 플래그 등을 기준으로 정렬할 수 있습니다. 상위 기여자 지표에는 다양한 차원의 리소스에서 관찰된 모든 트래픽에 대한 지표가 포함됩니다. 이벤트 중에 리소스로 전송되는 네트워크 트래픽을 이해하는 데 사용할 수 있는 추가 지표 차원을 제공합니다.

서비스 대시보드에는 DDoS 공격을 완화하기 위해 자동으로 수행된 작업에 대한 세부 정보도 포함됩니다. 이 정보를 사용하면 이상을 쉽게 조사하고 트래픽 차원을 탐색하며 Shield Advanced에서 취한 조치를 더 잘 이해하여 가용성을 보호할 수 있습니다.

애플리케이션을 대상으로 하는 트래픽을 파악하는 데 도움이 되는 또 다른 도구는 VPC 흐름 로그입니다. 기존 네트워크에서는 네트워크 흐름 로그를 사용하여 연결 및 보안 문제를 해결하고 네트워크 액세스 규칙이 예상대로 작동하는지 확인할 수 있습니다. VPC 흐름 로그를 사용하면 VPC의 네트워크 인터페이스에서 송수신되는 IP 트래픽에 대한 정보를 수집할 수 있습니다.

각 흐름 로그 레코드에는 소스 및 대상 IP 주소, 소스 및 대상 포트, 프로토콜, 캡처 창에서 전송된 패킷 및 바이트 수가 포함됩니다. 이 정보를 사용하여 네트워크 트래픽의 이상을 파악하고 특정 공격 벡터를 식별할 수 있습니다. 예를 들어 대부분의 UDP 반사 공격에는 DNS 반사용 소스 포트 53과 같은 특정 소스 포트가 있습니다. 이는 흐름 로그 레코드에서 식별할 수 있는 명확한 공격 서명입니다. 이에 대한 응답으로 특정 소스 포트를 인스턴스 수준에서 차단하거나 애플리케이션에 필요하지 않은 경우 전체 프로토콜을 차단하는 네트워크 ACL 규칙을 생성할 수 있습니다.

VPC 흐름 로그를 사용하여 네트워크 이상 및 DDoS 공격 벡터를 식별하는 방법에 대한 자세한 내용은 VPC 흐름 로그 및 VPC 흐름 로그 - 네트워크 트래픽 흐름 기록 및 보기를 참조하세요.

여러 계정에 대한 가시성 및 보호 관리

여러 AWS 계정에 걸쳐 운영하고 보호할 여러 구성 요소가 있는 시나리오에서 대규모로 운영되고 운영 오버헤드를 줄일 수 있는 기술을 사용하면 완화 기능이 향상됩니다. 여러 계정의 AWS Shield Advanced 보호 리소스를 관리하는 경우 AWS Firewall Manager 및 AWS Security Hub를 사용하여 중앙 집중식 모니터링을 설정할 수 있습니다. Firewall Manager를 사용하면 모든 계정에서 DDoS 보호 규정 준수를 시행하는 보안 정책을 만들 수 있습니다. 이 두 서비스를 함께 사용하여 여러 계정의 보호된 리소스를 관리하고 이러한 리소스를 중앙 집중식으로 모니터링할 수 있습니다.

Security Hub는 Firewall Manager와 자동으로 통합되어 있으므로 Shield Advanced 고객이 우선 순위가 높은 다른 보안 경고 및 규정 준수 상태와 함께 단일 대시보드에서 보안 결과를 볼 수 있습니다. 예를 들어 Shield Advanced가 범위 내의 모든 AWS 계정에서 보호된 리소스로 향하는 비정상적인 트래픽을 감지하면 이 결과가 Security Hub 콘솔에 표시됩니다. 구성된 경우 Firewall Manager는 리소스를

Shield Advanced로 보호되는 리소스로 생성하여 자동으로 규정 준수 상태로 전환한 다음 리소스가 규정 준수 상태에 있을 때 Security Hub를 업데이트할 수 있습니다.

Shield 보호 리소스의 중앙 집중식 모니터링에 대한 자세한 내용은 DDoS 이벤트에 대한 중앙 집중식 모니터링 설정 및 비준수 리소스 자동 해결을 참조하세요.

지원

공격이 발생하면 위협 평가 및 애플리케이션 아키텍처 검토 시 AWS 지원의 이점을 얻거나 다른 지원을 요청할 수도 있습니다. 실제 이벤트가 발생하기 전에 DDoS 공격에 대한 대응 계획을 세우는 것이 중요합니다. 본 문서에서 설명하는 모범 사례는 애플리케이션을 시작하기 전에 미리 구현하는 사전 예방 조치이지만 애플리케이션에 대한 DDoS 공격은 여전히 발생할 수 있습니다. 이 섹션의 옵션을 검토하여 시나리오에 가장 적합한 지원 리소스를 결정합니다. 귀사의 계정 팀이 귀사의 사용 사례 및 애플리케이션을 평가하고 구체적인 질문이나 당면 과제를 해결할 수 있습니다.

AWS에서 프로덕션 워크로드를 실행하는 경우 Business Support 서비스에 가입하면 24시간 연중무휴로 클라우드 지원 엔지니어를 통해 DDoS 공격 문제에 대해 지원을 받을 수 있습니다. 미션 크리티컬 워크로드를 실행하는 경우 중요한 사례를 열고 수석 클라우드 지원 엔지니어로부터 가장 빠른 응답을 받을 수 있는 Enterprise Support를 고려해 보세요.

AWS Shield Advanced를 구독하고 Business Support 또는 Enterprise Support도 구독 중인 경우 Shield 사전 참여를 구성할 수 있습니다. 이를 통해 상태 확인을 구성하고 리소스에 연결하며 연중무휴 24시간 작업 연락처 정보를 제공할 수 있습니다. Shield가 DDoS 징후를 감지하고 애플리케이션 상태 확인에서 성능 저하 징후를 보이면 AWS SRT가 적극적으로 연락을 취할 것입니다. 이는 AWS SRT 응답 시간이 가장 빠르고 귀사와 연락이 닿기도 전에 AWS SRT가 문제 해결을 시작할 수 있도록 지원하는 권장 참여 모델입니다.

사전 예방적 참여 기능을 사용하려면 애플리케이션 상태를 정확하게 측정하고 Shield Advanced에서 보호하는 리소스와 연결된 Route 53 상태 확인을 구성해야 합니다. Shield 콘솔에 Route 53 상태 확인이 연결되면 Shield Advanced 탐지 시스템은 상태 확인 상태를 애플리케이션 상태의 지표로 사용합니다. Shield Advanced의 상태 기반 탐지 기능을 사용하면 애플리케이션이 비정상 상태일 때 알림을 받고 완화 조치를 보다 신속하게 수행할 수 있습니다. AWS SRT는 비정상 애플리케이션이 DDoS 공격의 대상인지 여부를 확인하고 필요에 따라 추가 완화 조치를 취하기 위해 연락을 드릴 것입니다.

사전 예방적 참여 구성을 완료하려면 Shield 콘솔에 연락처 세부 정보를 추가해야 합니다. AWS SRT는 이 정보를 사용하여 연락을 드립니다. 연락처 요구 사항이나 기본 설정이 있는 경우 최대 10개의 연락처를 구성하고 추가 메모를 제공할 수 있습니다. 사전 예방적 참여 담당자는 보안 운영 센터 또는 즉시 사용 가능한 개인과 같이 연중무휴 24시간 역할을 담당해야 합니다.

모든 리소스 또는 응답 시간이 중요한 주요 프로덕션 리소스에 대해 사전 예방적 참여를 지원할 수 있습니다. 이 작업은 이러한 리소스에만 상태 확인을 할당하는 방식으로 수행됩니다.

애플리케이션 가용성에 영향을 미치는 DDoS 관련 이벤트가 있는 경우 AWS Support 콘솔 또는 Support API를 사용하여 AWS Support 사례를 생성하여 AWS SRT로 에스컬레이션할 수도 있습니다.

결론

본 백서에 설명된 모범 사례를 통해 많은 일반적인 인프라 및 애플리케이션 계층 DDoS 공격을 방지하여 애플리케이션의 가용성을 보호하는 복원력 있는 DDoS 아키텍처를 구축할 수 있습니다. 애플리케이션을 설계할 때 이러한 모범 사례를 따르는 정도는 완화할 수 있는 DDoS 공격의 유형, 벡터 및 양에 영향을 미칩니다. DDoS 완화 서비스에 가입하지 않고도 복원력을 통합할 수 있습니다. AWS Shield Advanced를 구독하면 이미 복원력이 뛰어난 애플리케이션 아키텍처를 추가로 보호하는 추가 지원, 가시성, 완화 및 비용 보호 기능을 얻을 수 있습니다.

기여자

본 문서를 작성하는 데 도움을 주신 분들입니다.

- Jeffrey Lyon, AWS 경계 보호
- Rodrigo Ferroni, AWS 보안 전문가 TAM
- Dmitriy Novikov, AWS 솔루션스 아키텍트
- Achraf Souk, AWS 솔루션스 아키텍트
- Yoshihisa Nakatani, AWS 솔루션스 아키텍트

리소스

참고 문헌:

- Best Practices for DDoS Mitigation on AWS
- Guidelines for Implementing AWS WAF
- SID324 – re:Invent 2017: Automating DDoS Response in the Cloud
- CTD304 – re:Invent 2017: Dow Jones & Wall Street Journal's Journey to Manage Traffic Spikes While Mitigating DDoS & Application Layer Threats
- CTD310 – re:Invent 2017: Living on the Edge, It's Safer Than You Think! Building Strong with Amazon CloudFront, AWS Shield, and AWS WAF
- SEC407 - re:Invent 2019: A defense-in-depth approach to building web applications
- SEC321 - re:Invent 2020: Get ahead of the curve with DDoS Response Team escalations
- William Hill: High-performance DDOS Protection with AWS

문서 개정

본 백서의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하세요.

update-history-change	update-history-description	update-history-date
백서 업데이트	최신 권장 사항 및 기능을 포함하도록 업데이트되었습니다. AWS Global Accelerator는 엣지에서 포괄적인 보호의 일부로 추가됩니다. DDoS 이벤트에 대한 중앙 집중식 모니터링 및 비준수 리소스 자동 해결을 위한 AWS Firewall Manager.	2021년 9월 21일
백서 업데이트	악성 웹 요청 탐지 및 필터링(BP1, BP2) 섹션의 캐시 버스팅과 흡수 규모(BP6) 섹션의 ELB 및 ALB 사용을 명확히 하기 위해 업데이트되었습니다. '리전 선택'으로 표시된 다이어그램 및 표 2를 BP8로 업데이트했습니다. BP7 섹션을 추가 세부 정보로 업데이트했습니다.	2019년 12월 18일
백서 업데이트	AWS WAF 로깅을 모범 사례로 포함하도록 업데이트되었습니다.	2018년 12월 1일
백서 업데이트	AWS Shield, AWS WAF 기능, AWS Firewall Manager 및 관련 모범 사례를 포함하도록 업데이트되었습니다.	2018년 6월 1일

백서 업데이트	규범적 아키텍처 지침을 추가하고 AWS WAF를 포함하도록 업데이트했습니다.	2016년 6월 1일
최초 게시	백서를 게시했습니다.	2015년 6월 1일

고지 사항

고객은 본 문서에 포함된 정보를 독자적으로 평가할 책임이 있습니다. 본 문서는 (a) 정보 제공만을 위한 것이며, (b) 사전 고지 없이 변경될 수 있는 현재의 AWS 제품 제공 서비스 및 사례를 보여 주며, (c) AWS 및 자회사, 공급업체 또는 라이선스 제공자로부터 어떠한 약정 또는 보증도 하지 않습니다. AWS 제품 또는 서비스는 명시적이든 묵시적이든 어떠한 종류의 보증, 진술 또는 조건 없이 '있는 그대로' 제공됩니다. 고객에 대한 AWS의 책임과 법적 책임은 AWS 계약서에 준하며 본 문서는 AWS와 고객 간의 계약에 포함되지 않고 계약을 변경하지도 않습니다.