AWS Weißbuch

AWS Bewährte Methoden für DDoS Resilienz

AWS Bewährte Methoden für DDoS Resilienz: AWS Weißbuch

Table of Contents

AWS Bewährte Methoden für DDoS Resilienz

Datum der Veröffentlichung: 9. August 2023 (Dokumentversionen)

Es ist wichtig, Ihr Unternehmen vor den Auswirkungen von Distributed Denial of Service (DDoS) - Angriffen sowie anderen Cyberangriffen zu schützen. Es hat höchste Priorität, das Vertrauen der Kunden in Ihren Service aufrechtzuerhalten, indem Sie die Verfügbarkeit und Reaktionsfähigkeit Ihrer Anwendung aufrechterhalten. Außerdem möchten Sie unnötige direkte Kosten vermeiden, wenn Ihre Infrastruktur als Reaktion auf einen Angriff skaliert werden muss. Amazon Web Services (AWS) ist bestrebt, Ihnen die Tools, Best Practices und Services zur Verfügung zu stellen, mit denen Sie sich gegen böswillige Akteure im Internet schützen können. Die Verwendung der richtigen Dienste von AWS trägt dazu bei, hohe Verfügbarkeit, Sicherheit und Ausfallsicherheit zu gewährleisten.

In diesem Whitepaper finden Sie präskriptive DDoS Anleitungen AWS zur Verbesserung der Ausfallsicherheit von Anwendungen, die auf dem Computer ausgeführt werden. AWS Dazu gehört auch eine DDoS robuste Referenzarchitektur, die als Leitfaden zum Schutz der Anwendungsverfügbarkeit verwendet werden kann. In diesem Whitepaper werden auch verschiedene Angriffsarten beschrieben, z. B. Angriffe auf Infrastrukturebene und Angriffe auf Anwendungsebene. AWS erklärt, welche bewährten Methoden zur Bekämpfung der einzelnen Angriffsarten am effektivsten sind. Darüber hinaus werden die Dienste und Funktionen beschrieben, die in eine Strategie DDoS zur Schadensbegrenzung passen, und es wird erläutert, wie die einzelnen Dienste und Funktionen zum Schutz Ihrer Anwendungen eingesetzt werden können.

Dieses paper richtet sich an IT-Entscheidungsträger und Sicherheitsingenieure, die mit den grundlegenden Konzepten von Netzwerken, Sicherheit und vertraut sind AWS. Jeder Abschnitt enthält Links zu AWS Dokumentationen, die detailliertere Informationen zu den bewährten Verfahren oder Funktionen enthalten.

AWS erkennt über eine Million DDoS Angriffe pro Jahr und wehrt täglich Tausende von Angriffen gegen unsere Kunden ab. Laut unserem Shield Response-Team (SRT) hat die Mehrheit der Kunden, bei denen DDoS Angriffe Auswirkungen auf das Geschäft haben, die Empfehlungen in diesem Leitfaden nicht umgesetzt.

Sind Sie Well-Architected?

Das AWS Well-Architected Framework hilft Ihnen dabei, die Vor- und Nachteile der Entscheidungen zu verstehen, die Sie beim Aufbau von Systemen in der Cloud treffen. Die sechs Säulen des

Frameworks ermöglichen es Ihnen, bewährte Architekturpraktiken für den Entwurf und Betrieb zuverlässiger, sicherer, effizienter, kostengünstiger und nachhaltiger Systeme kennenzulernen. Mithilfe des AWS Well-Architected Tool, das kostenlos im Bereich verfügbar ist AWS Management Console(Anmeldung erforderlich), können Sie Ihre Workloads anhand dieser bewährten Methoden überprüfen, indem Sie für jede Säule eine Reihe von Fragen beantworten.

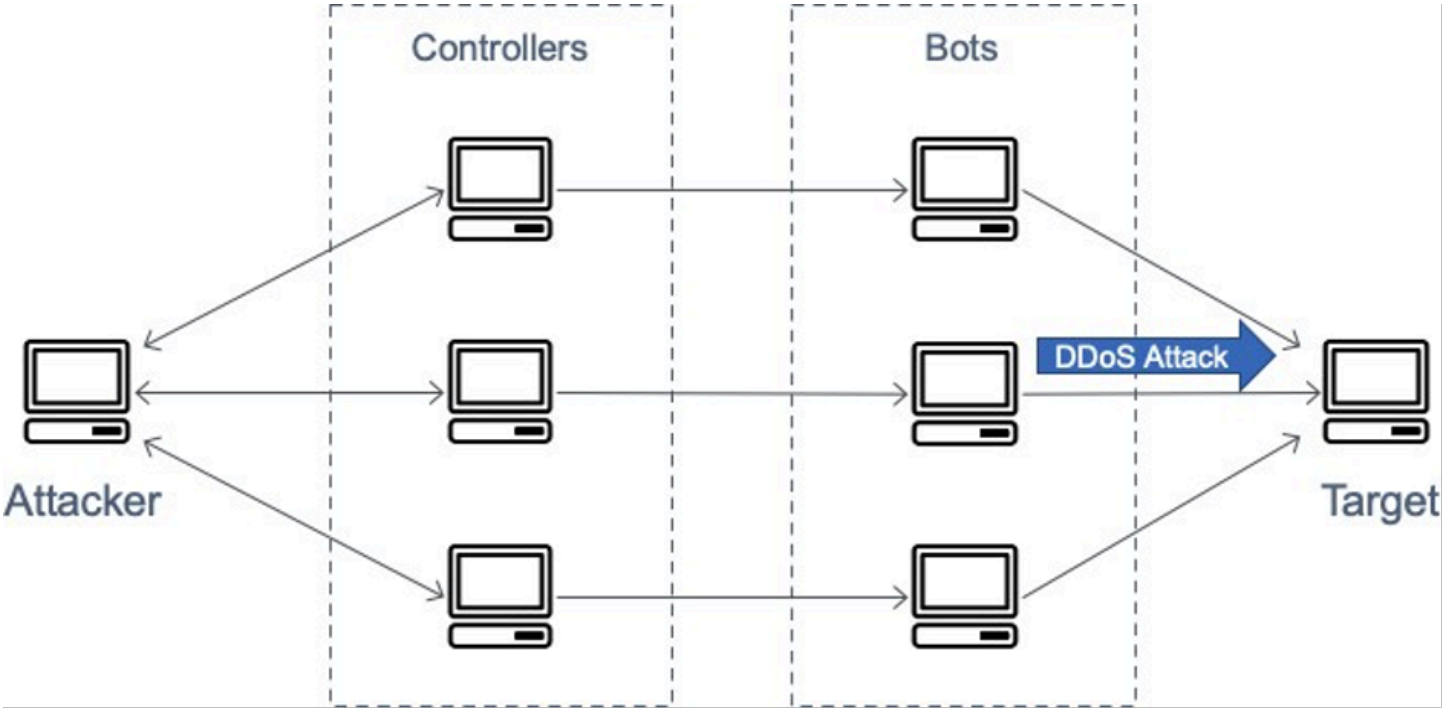
Weitere Expertentipps und bewährte Methoden für Ihre Cloud-Architektur — Referenzarchitekturbereitstellungen, Diagramme und Whitepapers — finden Sie im Architecture Center.AWS

Einführung in Denial-of-Service-Angriffe

Ein Denial of Service (DoS) -Angriff oder ein Ereignis ist ein vorsätzlicher Versuch, eine Website oder Anwendung für Benutzer nicht verfügbar zu machen, indem sie beispielsweise mit Netzwerkverkehr überflutet wird. Angreifer verwenden eine Vielzahl von Techniken, die große Mengen an Netzwerkbandbreite verbrauchen oder andere Systemressourcen beanspruchen und so den Zugriff für legitime Benutzer unterbrechen. In der einfachsten Form verwendet ein einsamer Angreifer eine einzige Quelle, um einen DoS-Angriff gegen ein Ziel auszuführen, wie in der folgenden Abbildung dargestellt.

Ein Diagramm, das einen DoS-Angriff darstellt

Bei einem Distributed-Denial-of-Service (DDoS) -Angriff verwendet ein Angreifer mehrere Quellen, um einen Angriff gegen ein Ziel zu orchestrieren. Zu diesen Quellen können verteilte Gruppen von mit Malware infizierten Computern, Routern, IoT-Geräten und anderen Endpunkten gehören. Die folgende Abbildung zeigt ein Netzwerk kompromittierter Hosts, die an dem Angriff beteiligt sind und eine Flut von Paketen oder Anfragen generieren, um das Ziel zu überfordern.



Ein Diagramm, das einen Angriff darstellt DDoS

Das Modell Open Systems Interconnection (OSI) besteht aus sieben Schichten, die in der folgenden Tabelle beschrieben werden. DDoSAngriffe treten am häufigsten auf den Ebenen 3, 4, 6 und 7 auf.

- Angriffe der Schichten 3 und 4 entsprechen den Netzwerk- und Transportebenen des OSI Modells. In diesem Whitepaper werden diese Angriffe zusammenfassend als Angriffe AWS auf die Infrastrukturebene bezeichnet.
- Angriffe der Schichten 6 und 7 entsprechen den Präsentations- und Anwendungsebenen des OSI Modells. In diesem Whitepaper werden diese zusammen als Angriffe auf Anwendungsebene behandelt.

In diesem paper werden diese Angriffsarten in den folgenden Abschnitten erörtert.

Tabelle 1 — OSI Modell

#	Ebene	Einheit	Beschreibung	Vektor-Beispiele
7	Anwendung	Daten	Vom Netzwerkprozess zur Anwendung	HTTPÜberschwemmung

#	Ebene	Einheit	Beschreibung	Vektor-Beispiele
				en, Fluten DNS abfragen
6	Darstellung	Daten	Datendarstellung und Verschlüs selung	Missbrauch von Transport Layer Security (TLS)
5	Sitzung	Daten	Kommunikation zwischen Hosts	N/A
4	Transport	Segmente	nd-to-end E-Verbindungen und Zuverläss igkeit	Synchroni sieren (SYN) Überschwe mmungen
3	Network (Netzwerk)	Pakete	Pfadbestimmung und logische Adressierung	Reflection-Angriffe mit dem User Datagram Protocol (UDP)
2	Datenverbindung	Frames (Frames)	Physikalische Adressierung	N/A
1	Physisch	Bits	Medien-, Signal- und Binärüber tragung	N/A

Angriffe auf Infrastrukturebene

Die häufigsten DDoS Angriffe, Reflection Attacks und SYN Floods mit User Datagram Protocol (UDP), sind Angriffe auf Infrastrukturebene. Ein Angreifer kann eine dieser Methoden verwenden, um große Datenverkehrsmengen zu erzeugen, die die Kapazität eines Netzwerks überfluten oder Ressourcen auf Systemen wie Servern, Firewalls, Intrusion Prevention System (IPS) oder Load Balancer beanspruchen können. Diese Angriffe sind zwar leicht zu erkennen, aber um sie wirksam abzuwehren, benötigen Sie ein Netzwerk oder Systeme, die die Kapazität schneller erhöhen als die Flut eingehenden Datenverkehrs. Diese zusätzliche Kapazität ist erforderlich, um den

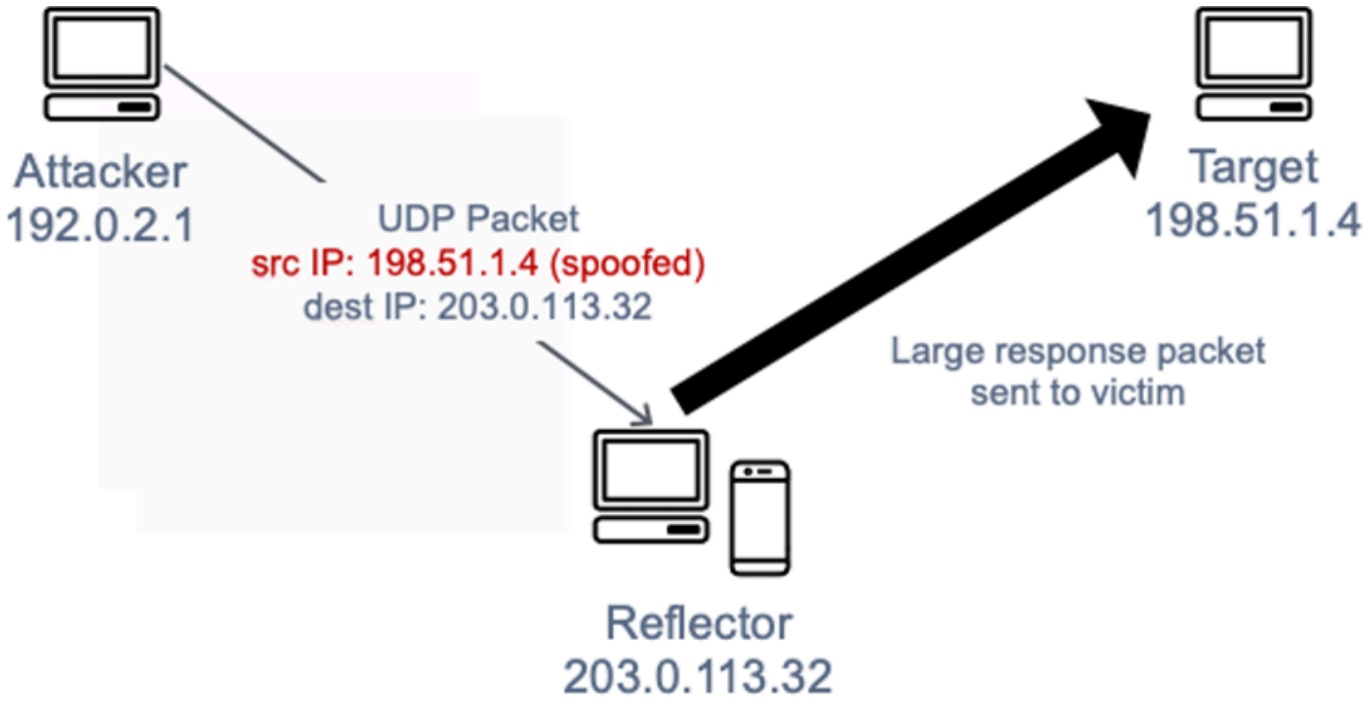
Angriffsdatenverkehr entweder herauszufiltern oder zu absorbieren, sodass das System und die Anwendung mehr Zeit haben, auf legitimen Kundenverkehr zu reagieren.

UDPReflection-Angriffe

UDPReflection-Angriffe nutzen die Tatsache aus, dass UDP es sich um ein zustandsloses Protokoll handelt. Angreifer können ein gültiges UDP Anforderungspaket erstellen, das die IP-Adresse des Angriffsziels als UDP Quell-IP-Adresse auflistet. Der Angreifer hat jetzt die Quell-IP des Anforderungspakets gefälscht — also UDP gefälscht. Das UDP Paket enthält die gefälschte Quell-IP und wird vom Angreifer an einen Zwischenserver gesendet. Der Server wird dazu verleitet, seine UDP Antwortpakete an die Ziel-IP des Opfers und nicht zurück an die IP-Adresse des Angreifers zu senden. Der Zwischenserver wird verwendet, weil er eine Antwort generiert, die um ein Vielfaches größer ist als das Anforderungspaket, wodurch die Menge des an die Ziel-IP-Adresse gesendeten Angriffsverkehrs effektiv erhöht wird.

Der Verstärkungsfaktor ist das Verhältnis von Antwortgröße zu Anforderungsgröße und hängt davon ab, welches Protokoll der Angreifer verwendet:DNS, Network Time Protocol (NTP), Simple Service Directory Protocol (SSDP), Connectionless Lightweight Directory Access Protocol (CLDAP), Memcached, Character Generator Protocol (CharGen) oder Quote of the Day (QOTD).

Der Verstärkungsfaktor für DNS kann beispielsweise das 28- bis 54-fache der ursprünglichen Bytezahl betragen. Wenn ein Angreifer also eine Anforderungs-Payload von 64 Byte an einen DNS Server sendet, kann er über 3400 Byte an unerwünschtem Traffic an ein Angriffsziel generieren. UDPReflection-Angriffe sind im Vergleich zu anderen Angriffen für ein größeres Datenverkehrsvolumen verantwortlich. Die folgende Abbildung veranschaulicht die Reflexionstaktik und den Verstärkungseffekt.

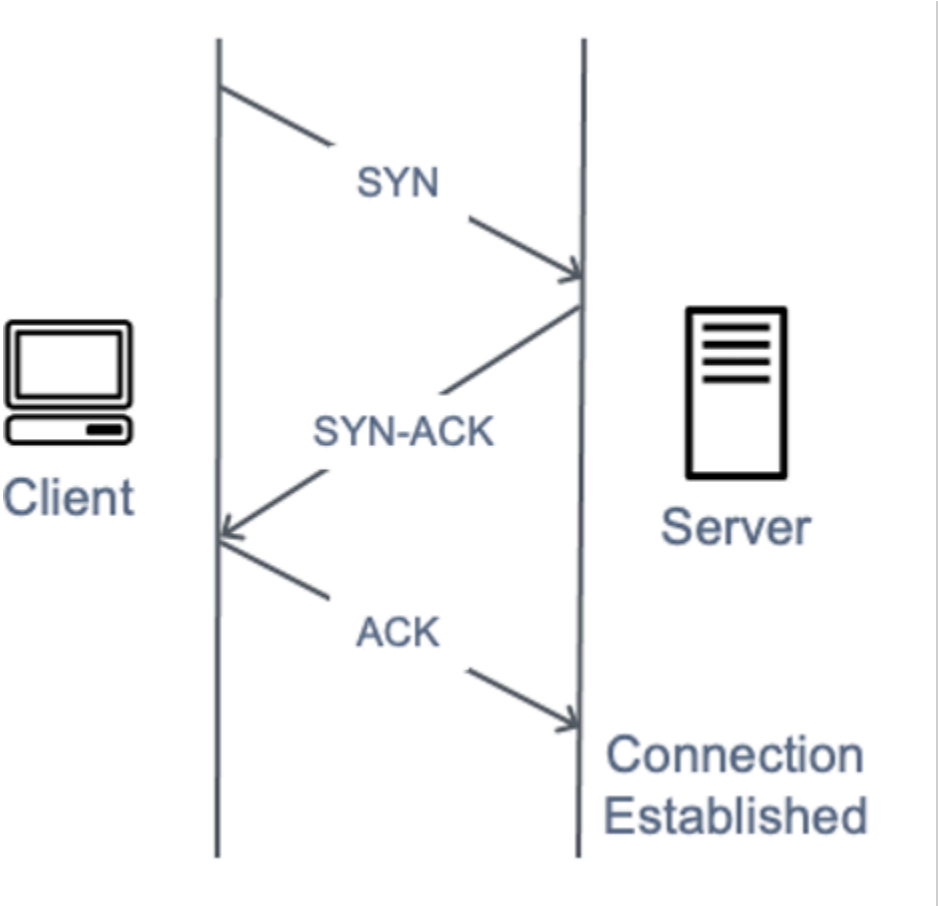


Ein Diagramm, das einen Reflection-Angriff darstellt UDP

Es sollte beachtet werden, dass Reflection-Angriffe den Angreifern zwar eine „kostenlose“ Verstärkung bieten, aber IP-Spoofing-Funktionen erfordern. Da immer mehr Netzwerkanbieter Source Address Validation Everywhere (SAVE) einführen oder diese Funktion abschaffen BCP38, werden DDoS Dienstanbieter gezwungen, Reflection-Angriffe einzustellen oder ihren Standort zu Rechenzentren und Netzwerkanbietern zu verlagern, die keine Quelladressvalidierung implementieren.

SYNHochwasserangriffe

Wenn ein Benutzer eine Verbindung zu einem Transmission Control Protocol (TCP) -Dienst, z. B. einem Webserver, herstellt, sendet sein Client ein SYN Paket. Der Server gibt ein Synchronisationsbestätigungspaket (SYN-ACK) zurück, und schließlich antwortet der Client mit einem Acknowledgement (ACK) -Paket, wodurch der erwartete Dreiwege-Handshake abgeschlossen wird. Die folgende Abbildung veranschaulicht diesen typischen Handshake.



Ein Diagramm, das einen Drei-Wege-Handschlag darstellt SYN

Bei einem SYN Hochwasserangriff sendet ein böswilliger Client eine große Anzahl von SYN Paketen, sendet aber nie die endgültigen ACK Pakete, um die Handshakes abzuschließen. Der Server wartet auf eine Antwort auf die halboffenen TCP Verbindungen. Die Idee ist, dass das Ziel irgendwann nicht mehr genug Kapazität hat, um neue TCP Verbindungen anzunehmen, wodurch neue Benutzer daran gehindert werden, sich mit dem Server zu verbinden. Die tatsächlichen Auswirkungen sind jedoch nuancierter. Moderne Betriebssysteme implementieren standardmäßig SYN Cookies als Mechanismus, um der Erschöpfung der State-Tabellen durch Hochwasserangriffe entgegenzuwirken. SYN Sobald die SYN Warteschlangenlänge einen vordefinierten Schwellenwert erreicht, antwortet der Server mit einem SYN -, das eine vordefinierte erste Sequenznummer ACK enthält, ohne einen Eintrag in der Warteschlange zu erstellen. SYN Wenn der Server dann eine Bestätigungsnummer erhält, ACK die eine korrekt inkrementierte Bestätigungsnummer enthält, kann er den Eintrag zu seiner Statustabelle hinzufügen und wie gewohnt fortfahren. Die tatsächlichen Auswirkungen von SYN Überschwemmungen auf Zielgeräte sind in der Regel Netzwerkkapazität und -auslastung. Bei Geräten mit Zwischenstatus wie Firewalls (oder Verbindungsverfolgung von EC2 Sicherheitsgruppen)

kann es jedoch vorkommen, dass die Statustabelle CPU erschöpft ist und neue Verbindungen TCP unterbrochen werden.

TCPMiddlebox-Spiegelung

Dieser relativ neue Angriffsvektor wurde erstmals im August 2021 in einem wissenschaftlichen Whitepaper veröffentlicht, in dem erklärt wurde, wie TCP Verstöße sowohl bei nationalstaatlichen als auch bei kommerziell verfügbaren Firewalls dazu führen können, dass diese per Täuschung zu einem Verstärkungsvektor werden. TCP Wir haben diese Angriffe seit Anfang 2022 „in freier Wildbahn“ gesehen und sehen sie auch heute noch. Der Verstärkungsfaktor variiert aufgrund der unterschiedlichen Art und Weise, wie Anbieter dieses „Feature“ implementiert haben, kann aber die UDP Memcached-Amplification übertreffen.

Angriffe auf Anwendungsebene

Ein Angreifer kann mithilfe eines Layer-7- oder Anwendungs-Layer-Angriffs die Anwendung selbst ins Visier nehmen. Bei diesen Angriffen, ähnlich wie bei Angriffen auf die SYN Hochwasserinfrastruktur, versucht der Angreifer, bestimmte Funktionen einer Anwendung zu überlasten, sodass die Anwendung für legitime Benutzer nicht verfügbar ist oder nicht mehr reagiert. Manchmal kann dies mit sehr geringem Anforderungsvolumen erreicht werden, das nur ein geringes Volumen an Netzwerkverkehr generiert. Dadurch kann es schwierig sein, den Angriff zu erkennen und abzuwehren. Beispiele für Angriffe auf Anwendungsebene sind HTTP Floods, Cache-Busting-Angriffe und — Floods. WordPress XML RPC

- Bei einem HTTPHochwasserangriff sendet ein Angreifer HTTP Anfragen, die anscheinend von einem gültigen Benutzer der Webanwendung stammen. Einige HTTP Überschwemmungen zielen auf eine bestimmte Ressource ab, während bei komplexeren HTTP Überschwemmungen versucht wird, die menschliche Interaktion mit der Anwendung nachzuahmen. Dies kann die Verwendung gängiger Abhilfemaßnahmen wie der Begrenzung der Anforderungsrate erschweren.
- Cache-Busting-Angriffe sind eine Art von HTTP Flut, bei der Variationen in der Abfragezeichenfolge verwendet werden, um das Caching von Content Delivery Network () zu umgehen. CDN Anstatt zwischengespeicherte Ergebnisse zurückgeben zu können, CDN müssen sie sich bei jeder Seitenanforderung an den Ursprungsserver wenden, und diese ursprünglichen Abrufe belasten den Anwendungswebserver zusätzlich.
- Bei einem WordPress XMLRPCFlood-Angriff, auch bekannt als WordPress Pingback-Flood, zielt ein Angreifer auf eine Website ab, die auf der WordPress Content-Management-Software gehostet wird. Der Angreifer missbraucht die RPC API Funktion XML-, um eine Flut von HTTP Anfragen

zu generieren. Die Pingback-Funktion ermöglicht es einer auf WordPress (Site A) gehosteten Website, eine andere WordPress Site (Site B) über einen von Site A erstellten Link zu Site B zu benachrichtigen. Site B versucht dann, Site A abzurufen, um das Vorhandensein des Links zu überprüfen. Bei einer Pingbackflut missbraucht der Angreifer diese Fähigkeit, um Site B zum Angriff auf Site A zu veranlassen. Diese Art von Angriff hat eine eindeutige Signatur: "`WordPress:`" ist normalerweise im User-Agent des Anforderungsheaders vorhanden. HTTP

Es gibt andere Formen von bösartigem Datenverkehr, die die Verfügbarkeit einer Anwendung beeinträchtigen können. Scraper-Bots automatisieren Versuche, auf eine Webanwendung zuzugreifen, um Inhalte zu stehlen oder Wettbewerbsinformationen wie Preise aufzuzeichnen. Brute-Force - und Credential-Stuffing-Angriffe sind programmierte Versuche, sich unbefugten Zugriff auf sichere Bereiche einer Anwendung zu verschaffen. Dabei handelt es sich nicht um DDoS Angriffe im eigentlichen Sinne, aber ihr automatisierter Charakter kann einem DDoS Angriff ähneln, und sie können durch die Implementierung einiger der gleichen bewährten Methoden, die in diesem paper behandelt werden, abgewehrt werden.

Angriffe auf Anwendungsebene können auch auf Domain Name System (DNS) -Dienste abzielen. Der häufigste dieser Angriffe ist eine DNSAbfrageflut, bei der ein Angreifer viele wohlgeformte DNS Abfragen verwendet, um die Ressourcen eines DNS Servers zu erschöpfen. Diese Angriffe können auch eine Cache-Busting-Komponente beinhalten, bei der der Angreifer die Subdomänenzeichenfolge nach dem Zufallsprinzip sortiert, um den lokalen DNS Cache eines beliebigen Resolvers zu umgehen. Aus diesem Grund kann der Resolver zwischengespeicherte Domainabfragen nicht nutzen und muss stattdessen wiederholt Kontakt mit dem autorisierenden Server aufnehmen, was den Angriff verstärkt. DNS

Wenn eine Webanwendung über Transport Layer Security (TLS) bereitgestellt wird, kann sich ein Angreifer auch dafür entscheiden, den Verhandlungsprozess anzugreifen. TLS TLSist rechenintensiv, sodass ein Angreifer die Verfügbarkeit des Servers verringern kann, indem er zusätzliche Arbeitslast auf dem Server generiert, um unlesbare Daten (oder unverständlichen Text) als legitimen Handshake zu verarbeiten. Bei einer Variante dieses Angriffs schließt ein Angreifer den Handshake ab, verhandelt aber ständig neu über die Verschlüsselungsmethode. TLS Ein Angreifer kann alternativ versuchen, Serverressourcen zu erschöpfen, indem er viele Sitzungen öffnet und schließt. TLS

Techniken zur Schadensbegrenzung

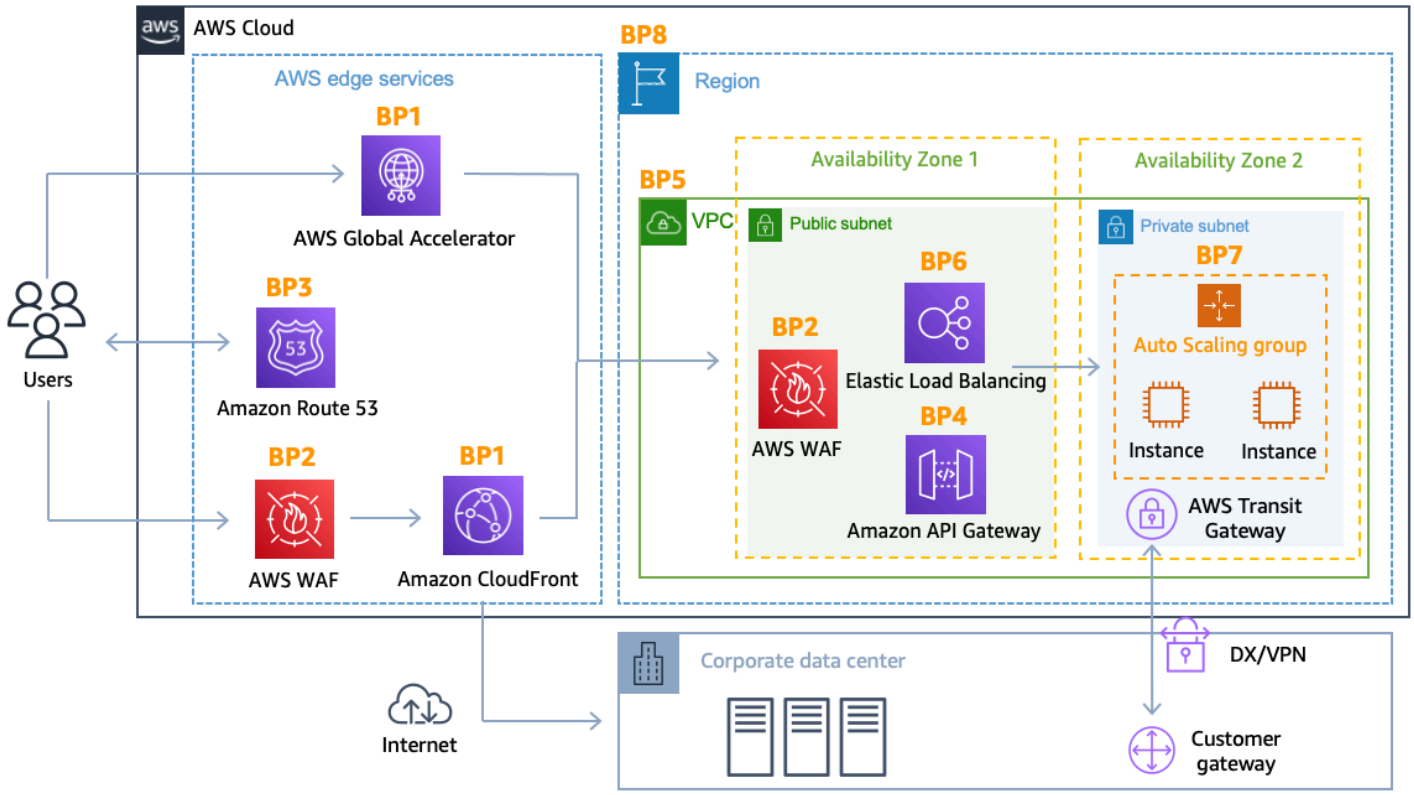
Einige Formen der DDoS Risikominderung sind automatisch in den AWS Diensten enthalten. DDoSDie Ausfallsicherheit kann weiter verbessert werden, indem eine AWS Architektur mit spezifischen Diensten verwendet wird, die in den folgenden Abschnitten behandelt werden, und indem zusätzliche bewährte Methoden für jeden Teil des Netzwerkflusses zwischen Benutzern und Ihrer Anwendung implementiert werden.

Sie können AWS Dienste verwenden, die von Edge-Standorten aus betrieben werden, wie Amazon CloudFront, AWS Global Accelerator und Amazon Route 53, um einen umfassenden Verfügbarkeitsschutz gegen alle bekannten Angriffe auf Infrastrukturebene aufzubauen. Diese Dienste sind Teil des AWS Global Edge-Netzwerks und können die DDoS Widerstandsfähigkeit Ihrer Anwendung verbessern, wenn sie jede Art von Anwendungsdatenverkehr von Edge-Standorten aus auf der ganzen Welt bedienen. Sie können Ihre Anwendung in jeder beliebigen Umgebung ausführen und diese Dienste verwenden AWS-Region, um die Verfügbarkeit Ihrer Anwendung zu schützen und die Leistung Ihrer Anwendung für legitime Endbenutzer zu optimieren.

Zu den Vorteilen der Verwendung von Amazon CloudFront, Global Accelerator und Amazon Route 53 gehören:

- Zugang zum Internet und Kapazitäten DDoS zur Schadensbegrenzung im gesamten AWS Global Edge-Netzwerk. Dies ist nützlich bei der Abwehr größerer volumetrischer Angriffe, die Terabit-Ausmaße erreichen können.
- AWS Shield DDoSAbwehrsysteme sind in AWS Edge-Services integriert, sodass die Geschwindigkeit time-to-mitigate von Minuten auf weniger als eine Sekunde reduziert wird.
- Stateless SYN Flood Mitigation verifiziert eingehende Verbindungen mithilfe von SYN Cookies, bevor sie an den geschützten Dienst weitergeleitet werden. Dadurch wird sichergestellt, dass nur gültige Verbindungen zu Ihrer Anwendung gelangen, und gleichzeitig werden Ihre legitimen Endbenutzer vor Fehlalarmen geschützt.
- Automatische Traffic-Engineering-Systeme, die die Auswirkungen großer DDoS volumetrischer Angriffe verteilen oder isolieren. All diese Dienste isolieren Angriffe an der Quelle, bevor sie Ihren Ursprung erreichen, was bedeutet, dass weniger Auswirkungen auf die durch diese Dienste geschützten Systeme entstehen.
- Der Schutz auf Anwendungsebene erfordert in CloudFront Kombination AWS WAFdamit keine Änderung der aktuellen Anwendungsarchitektur (z. B. in einem AWS-Region oder einem lokalen Rechenzentrum).

Es fallen keine Gebühren für eingehende Datenübertragungen an AWS und Sie zahlen auch nicht für DDoS Angriffsdatenverkehr, der durch abgewehrt wird. AWS Shield Das folgende Architekturdiagramm umfasst die Dienste des AWS Global Edge Network.



DDoS-belastbare Referenzarchitektur

Diese Architektur umfasst mehrere AWS Dienste, mit denen Sie die Widerstandsfähigkeit Ihrer Webanwendung gegen DDoS Angriffe verbessern können. Die folgende Tabelle enthält eine Zusammenfassung dieser Dienste und der Funktionen, die sie bieten können. AWS hat jeden Dienst mit einem Best-Practice-Indikator (BP1,BP2) versehen, um in diesem Dokument leichter nachschlagen zu können. In einem kommenden Abschnitt werden beispielsweise die von Amazon CloudFront und Global Accelerator bereitgestellten Funktionen erörtert, einschließlich des Best-Practice-IndikatorsBP1.

Tabelle 2 — Zusammenfassung der bewährten Verfahren

	AWS Edge			AWS-Region		
	Amazon CloudFron	Verwenden von Global	Verwenden von	Elastic Load	Verwenden von	Verwenden von

	AWS Edge			AWS-Region		
	t (BP1) mit AWS WAF (BP2) verwenden	Accelerator (BP1)	Amazon Route 53 (BP3)	Balancing (BP6) mit AWS WAF (BP2) verwenden	Sicherheitsgruppen und Netzwerken ACLs in Amazon VPC (BP5)	Amazon Elastic Compute Cloud (AmazonEC2) Auto Scaling (BP7)
Abwehr von Angriffen auf Ebene 3 (z. B. UDP Reflection)	✓	✓	✓	✓	✓	✓
Abwehr von Angriffen auf Ebene 4 (z. B. SYN Überschwemmung)	✓	✓	✓	✓		
Abwehr von Angriffen auf Ebene 6 (z. B.TLS)	✓	✓	✓	✓		

	AWS Edge			AWS-Region		
Reduzieren Sie die Angriffsfläche	✓	✓	✓	✓	✓	
Skalieren Sie, um den Datenverkehr auf Anwendungsebene zu absorbieren	✓	✓	✓	✓	✓	✓
Abwehr von Angriffen auf Schicht 7 (Anwendungsebene)	✓	✓(*)	✓	✓	✓(*)	✓(*)

	AWS Edge			AWS-Region		
Geografische Isolierung und Verteilung von übermäßigem Datenverkehr und größeren Angriffen DDoS	✓	✓	✓			

✓ (*): Bei Verwendung AWS WAF mit Application Load Balancer

Eine weitere Möglichkeit, Ihre Bereitschaft zu verbessern, auf DDoS Angriffe zu reagieren und diese abzuwehren, ist das Abonnieren von. AWS Shield Advanced Zu den Vorteilen der Verwendung gehören AWS Shield Advanced :

- Rund um die Uhr verfügbarer, spezialisierter Support durch das AWS Shield Response Team (AWS SRT) für Unterstützung bei der Abwehr von DDoS Angriffen, die sich auf die Verfügbarkeit von Anwendungen auswirken, einschließlich einer optionalen Funktion für proaktives Engagement
- Sensitive Erkennungsschwellenwerte, die den Datenverkehr früher in das DDoS Mitigation-System weiterleiten und time-to-mitigate Angriffe gegen Amazon EC2 (einschließlich Elastic Load Balancer) oder Network Load Balancer verbessern können, wenn sie mit einer Elastic IP-Adresse verwendet werden
- Maßgeschneiderte Layer-7-Erkennung auf der Grundlage von Basisdatenverkehrsmustern Ihrer Anwendung bei Verwendung mit AWS WAF
- Automatische DDoS Abwehr auf Anwendungsebene, bei der Shield Advanced auf erkannte DDoS Angriffe reagiert, indem es benutzerdefinierte AWS WAF Regeln erstellt, auswertet und einsetzt
- Zugriff AWS WAF auf ohne zusätzliche Kosten zur Abwehr von DDoS Angriffen auf Anwendungsebene (bei Verwendung mit Amazon CloudFront oder Application Load Balancer)
- Zentralisierte Verwaltung der Sicherheitsrichtlinien ohne zusätzliche AWS Firewall ManagerKosten.

- Kostenschutz, der es Ihnen ermöglicht, eine begrenzte Rückerstattung der Kosten im Zusammenhang mit der Skalierung zu beantragen, die sich aus einem DDoS Angriff ergeben.
- Erweitertes Service Level Agreement, das speziell auf Kunden zugeschnitten AWS Shield Advanced ist.
- Schutzgruppen, die es Ihnen ermöglichen, Ressourcen zu bündeln, sodass Sie im Self-Service den Erkennungs- und Schutzbereich für Ihre Anwendung individuell anpassen können, indem mehrere Ressourcen als eine einzige Einheit behandelt werden. Informationen zu Schutzgruppen finden Sie unter Shield Advanced-Schutzgruppen.
- DDoSSichtbarkeit von Angriffen mithilfe der AWS Management Console API CloudWatch Metriken und Alarme von Amazon,, und

Dieser optionale DDoS Abhilfeservice trägt zum Schutz von Anwendungen bei, die auf beliebigen AWS-Region Geräten gehostet werden. Der Service ist weltweit für CloudFront Route 53 und Global Accelerator verfügbar. Regional können Sie die IP-Adressen Application Load Balancer, Classic Load Balancer und Elastic schützen, sodass Sie Network Load Balancer (NLBs) oder Amazon-Instances schützen können. EC2

Eine vollständige Liste der AWS Shield Advanced Funktionen und weitere Informationen dazu finden Sie unter So funktioniert AWS Shield es. AWS Shield

Bewährte Methoden zur DDoS Schadensbegrenzung

In den folgenden Abschnitten werden die empfohlenen bewährten Methoden zur DDoS Risikominderung ausführlicher beschrieben. Eine easy-to-implement Kurzanleitung zum Aufbau einer DDoS Abwehrschicht für statische oder dynamische Webanwendungen finden Sie unter How to Help Protect Dynamic Web Applications Against DDoS Attacks by Using Amazon CloudFront and Amazon Route 53.

Verteidigung auf Infrastrukturebene (BP1,BP3,BP6,BP7)

In einer herkömmlichen Rechenzentrumsumgebung können Sie DDoS Angriffe auf die Infrastrukturebene abwehren, indem Sie Techniken wie die Überbereitstellung von Kapazitäten, den Einsatz von Systemen DDoS zur Risikominderung oder die Bereinigung des Datenverkehrs mithilfe von Abwehrdiensten einsetzen. DDoS Bei Aktivierung AWS werden die DDoS Abwehrfunktionen automatisch bereitgestellt. Sie können jedoch die DDoS Widerstandsfähigkeit Ihrer Anwendung optimieren, indem Sie die Architektur so wählen, dass diese Funktionen optimal genutzt werden und Sie auch bei übermäßigem Datenverkehr skalieren können.

Zu den wichtigsten Überlegungen zur Abwehr volumetrischer DDoS Angriffe gehören die Sicherstellung, dass genügend Transitkapazität und -vielfalt verfügbar sind, und der Schutz von AWS Ressourcen wie EC2 Amazon-Instances vor Angriffsverkehr.

Einige EC2 Amazon-Instance-Typen unterstützen Funktionen, mit denen große Datenverkehrsmengen einfacher verarbeitet werden können, z. B. Netzwerkbandbreitenschnittstellen mit bis zu 100 Gbit/s und erweiterte Netzwerke. Dies trägt dazu bei, eine Überlastung der Schnittstelle für den Datenverkehr zu verhindern, der die EC2 Amazon-Instance erreicht hat. Instances, die Enhanced Networking unterstützen, bieten im Vergleich zu herkömmlichen Implementierungen eine höhere Eingabe-/Ausgangsleistung (I/O), eine höhere Bandbreite und eine geringere CPU Auslastung. Dies verbessert die Fähigkeit der Instance, große Datenverkehrsmengen zu verarbeiten, und macht sie letztlich äußerst widerstandsfähig gegenüber der Last von Paketen pro Sekunde (pps).

Um dieses hohe Maß an Ausfallsicherheit zu ermöglichen, AWS empfiehlt es sich, Amazon EC2 Dedicated EC2 Instances oder Amazon-Instances mit höherem Netzwerkdurchsatz zu verwenden, die ein `N` "" Suffix haben und Enhanced Networking mit beispielsweise bis zu 100 Gbit/s Netzwerkbandbreite unterstützen, `c6gn.16xlarge` `c5n.18xlarge` und/oder Metal-Instances (wie`c5n.metal`).

Weitere Informationen zu EC2 Amazon-Instances, die 100-Gigabit-Netzwerkschnittstellen und erweiterte Netzwerke unterstützen, finden Sie unter EC2Amazon-Instance-Typen.

Das für Enhanced Networking erforderliche Modul und der erforderliche `enaSupport` Attributsatz sind in Amazon Linux 2 und den neuesten Versionen von Amazon Linux enthaltenAMI. Wenn Sie also eine Instance mit einer Hardware-Version für virtuelle Maschinen (HVM) von Amazon Linux auf einem unterstützten Instance-Typ starten, ist Enhanced Networking für Ihre Instance bereits aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist und Enhanced Networking unter Linux.

Amazon EC2 mit Auto Scaling (BP7)

Eine weitere Möglichkeit, Angriffe sowohl auf die Infrastruktur als auch auf Anwendungsebene abzuwehren, besteht darin, in großem Maßstab zu operieren. Wenn Sie über Webanwendungen verfügen, können Sie Load Balancer verwenden, um den Traffic auf eine Reihe von EC2 Amazon-Instances zu verteilen, die überprovisioniert sind oder für die automatische Skalierung konfiguriert sind. Diese Instances können plötzliche Datenverkehrsspitzen bewältigen, die aus beliebigen Gründen auftreten, einschließlich eines Flash-Crowd-Angriffs oder eines Angriffs auf

Anwendungsebene. DDoS Sie können CloudWatch Amazon-Alarme so einrichten, dass Auto Scaling initiiert wird, um die Größe Ihrer EC2 Amazon-Flotte als Reaktion auf von Ihnen definierte EreignisseCPU, RAM wie Netzwerk-I/O und sogar benutzerdefinierte Metriken, automatisch zu skalieren.

Dieser Ansatz schützt die Anwendungsverfügbarkeit bei einem unerwarteten Anstieg des Anforderungsvolumens. Wenn Sie Amazon CloudFront, Application Load Balancer, Classic Load Balancer oder Network Load Balancer mit Ihrer Anwendung verwenden, erfolgt die TLS Verhandlung durch den Vertrieb (Amazon CloudFront) oder den Load Balancer. Diese Funktionen tragen dazu bei, Ihre Instances vor Angriffen zu schützen, indem sie auf legitime TLS Anfragen und missbräuchliche Angriffe skaliert werden. TLS

Weitere Informationen zur Verwendung von Amazon CloudWatch zum Aufrufen von Auto Scaling finden Sie unter Überwachen von CloudWatch Amazon-Metriken für Ihre Auto Scaling Scaling-Gruppen und -Instances.

Amazon EC2 bietet eine anpassbare Rechenkapazität, sodass Sie bei sich ändernden Anforderungen schnell nach oben oder unten skalieren können. Sie können horizontal skalieren, indem Sie Ihrer Anwendung automatisch Instances hinzufügen, indem Sie die Größe Ihrer Amazon EC2 Auto Scaling-Gruppe skalieren, und Sie können vertikal skalieren, indem Sie größere EC2 Instance-Typen verwenden.

Mithilfe von Amazon RDS Proxy können Sie es Ihren Anwendungen ermöglichen, Datenbankverbindungen zu bündeln und gemeinsam zu nutzen, um ihre Skalierbarkeit zu verbessern und unvorhersehbare Anstiege im Datenbankverkehr zu bewältigen. Sie können auch die automatische Speicherskalierung für eine RDS Amazon-Datenbank-Instance aktivieren. Weitere Informationen finden Sie unter Automatisches Kapazitätsmanagement mit Amazon RDS Storage Autoscaling.

Elastic Load Balancing (BP6)

Große DDoS Angriffe können die Kapazität einer einzelnen EC2 Amazon-Instance überfordern. Mit Elastic Load Balancing (ELB) können Sie das Risiko einer Überlastung Ihrer Anwendung reduzieren, indem Sie den Traffic auf viele Backend-Instances verteilen. Elastic Load Balancing kann automatisch skaliert werden, sodass Sie größere Volumen verwalten können, wenn Sie unerwartet zusätzlichen Traffic haben, z. B. aufgrund von Flash-Crowds oder DDoS Angriffen. Bei Anwendungen, die in einem Amazon erstellt wurdenVPC, sind je nach Anwendungstyp drei Typen ELBs zu berücksichtigen: Application Load Balancer (ALB), Network Load Balancer (NLB) und Classic Load Balancer (). CLB

Für Webanwendungen können Sie den Application Load Balancer verwenden, um den Datenverkehr auf der Grundlage von Inhalten weiterzuleiten und nur wohlgeformte Webanfragen anzunehmen. Application Load Balancer blockiert viele gängige DDoS Angriffe wie SYN Floods oder UDP Reflection-Angriffe und schützt so Ihre Anwendung vor dem Angriff. Application Load Balancer skaliert automatisch, um den zusätzlichen Datenverkehr zu absorbieren, wenn diese Art von Angriffen erkannt wird. Skalierungsaktivitäten aufgrund von Angriffen auf die Infrastrukturebene sind für AWS Kunden transparent und wirken sich nicht auf Ihre Rechnung aus.

Weitere Informationen zum Schutz von Webanwendungen mit Application Load Balancer finden Sie unter Erste Schritte mit Application Load Balancers.

Für HTTPS Anwendungen ohneHTTP//können Sie den Network Load Balancer verwenden, um den Datenverkehr mit extrem niedriger Latenz an Ziele (z. B. EC2 Amazon-Instances) weiterzuleiten. Eine wichtige Überlegung bei Network Load Balancer ist, dass TCP SYN jeglicher UDP Datenverkehr, der den Load Balancer auf einem gültigen Listener erreicht, an Ihre Ziele weitergeleitet und nicht absorbiert wird. Dies gilt jedoch nicht für TLS -listener, die die Verbindung beenden. TCP Für Network Load Balancer mit TCP Listenern empfehlen wir den Einsatz von Global Accelerator zum Schutz vor Überschwemmungen. SYN

Sie können Shield Advanced verwenden, um den DDoS Schutz für Elastic IP-Adressen zu konfigurieren. Wenn dem Network Load Balancer pro Availability Zone eine Elastic IP-Adresse zugewiesen wird, wendet Shield Advanced die entsprechenden DDoS Schutzmaßnahmen für den Network Load Balancer Balancer-Verkehr an.

Weitere Informationen zum Schutz TCP von UDP Anwendungen mit Network Load Balancer finden Sie unter Erste Schritte mit Network Load Balancer.

> **Note**
>
> Je nach Konfiguration der Sicherheitsgruppe muss die Ressource, die die Sicherheit zur Gruppierung verwendet, die Verbindungsverfolgung verwenden, um Informationen über den Datenverkehr zu verfolgen. Dies kann die Fähigkeit des Load Balancers beeinträchtigen, neue Verbindungen zu verarbeiten, da die Anzahl der verfolgten Verbindungen begrenzt ist. Eine Sicherheitsgruppenkonfiguration, die eine Eingangsregel enthält, die Datenverkehr von einer beliebigen IP-Adresse akzeptiert (z. B. `0.0.0.0/0` oder `::/0`), aber keine entsprechende Regel hat, um den Antwortverkehr zuzulassen, veranlasst die Sicherheitsgruppe, Verbindungsverfolgungsinformationen zu verwenden, um das Senden des Antwortverkehrs zu ermöglichen. Im Falle eines DDoS Angriffs kann die maximale Anzahl nachverfolgter Verbindungen ausgeschöpft sein. Um die DDoS Resilienz Ihres öffentlich

zugänglichen Application Load Balancer oder Classic Load Balancer zu verbessern, stellen Sie sicher, dass die mit Ihrem Load Balancer verknüpfte Sicherheitsgruppe so konfiguriert ist, dass sie keine Verbindungsverfolgung (nicht verfolgte Verbindungen) verwendet, sodass der Verkehrsfluss keinen Beschränkungen für die Verbindungsverfolgung unterliegt. Konfigurieren Sie dazu Ihre Sicherheitsgruppe mit einer Regel, die es der eingehenden Regel ermöglicht, TCP Datenflüsse von einer beliebigen IP-Adresse (`0.0.0.0/0`oder`::/0`) zu akzeptieren, und fügen Sie eine entsprechende Regel in ausgehender Richtung hinzu, die es dieser Ressource ermöglicht, den Antwortverkehr zu senden (ausgehenden Bereich für jede IP-Adresse zulassen `0.0.0.0/0` oder`::/0`) für alle Ports (0-65535), sodass der Antwortverkehr auf der Grundlage der Sicherheitsgruppenregel und nicht auf der Grundlage von Tracking-Informationen zugelassen wird. Mit dieser Konfiguration unterliegen Classic und Application Load Balancer nicht den Grenzwerten für die vollständige Verbindungsverfolgung, die sich auf den Aufbau neuer Verbindungen zu seinen Load Balancer-Knoten auswirken können, und ermöglichen eine Skalierung auf der Grundlage der Zunahme des Datenverkehrs im Falle eines DDoS Angriffs. Weitere Informationen zu nicht verfolgten Verbindungen finden Sie unter: Verbindungsverfolgung von Sicherheitsgruppen: Unverfolgte Verbindungen.

Das Vermeiden der Verbindungsverfolgung von Sicherheitsgruppen hilft nur in Fällen, in denen der DDoS Datenverkehr von einer Quelle stammt, die von der Sicherheitsgruppe zugelassen ist. DDoS Datenverkehr von Quellen, die in der Sicherheitsgruppe nicht zulässig sind, hat keine Auswirkung auf die Verbindungsverfolgung. In diesen Fällen ist es nicht erforderlich, Ihre Sicherheitsgruppen neu zu konfigurieren, um die Verbindungsverfolgung zu vermeiden. Dies ist beispielsweise der Fall, wenn Ihre Sicherheitsgruppen-Zulassungsliste aus IP-Bereichen besteht, denen Sie ein hohes Maß an Vertrauen entgegenbringen, z. B. einer Unternehmensfirewall oder einem vertrauenswürdigen Ausgang oderVPN. IPs CDNs

Verwenden Sie AWS Edge-Standorte für die Skalierung (BP1,) BP3

Der Zugriff auf hoch skalierte, vielfältige Internetverbindungen kann Ihre Fähigkeit, Latenz und Durchsatz für Benutzer zu optimieren, DDoS Angriffe abzuwehren, Fehler zu isolieren und gleichzeitig die Auswirkungen auf die Verfügbarkeit Ihrer Anwendung zu minimieren, erheblich verbessern. AWS Edge-Standorte bieten eine zusätzliche Ebene der Netzwerkinfrastruktur, die diese Vorteile für jede Webanwendung bietet, die Amazon CloudFront, Global Accelerator und Amazon Route 53 verwendet. Mit diesen Services können Sie Ihre Anwendungen, von AWS-Regionen denen aus Sie laufen, umfassend am Edge schützen.

Bereitstellung von Webanwendungen am Edge () BP1

Amazon CloudFront ist ein Service, mit dem Sie Ihre gesamte Website einschließlich statischer, dynamischer, gestreamter und interaktiver Inhalte bereitstellen können. Dauerhafte Verbindungen und variable Einstellungen time-to-live (TTL) können verwendet werden, um Traffic von Ihrem Ursprung abzulagern, auch wenn Sie keine Inhalte bereitstellen, die zwischengespeichert werden können. Die Verwendung dieser CloudFront Funktionen reduziert die Anzahl der Anfragen und TCP Verbindungen zurück zu Ihrem Ursprung und trägt so dazu bei, Ihre Webanwendung vor Überschwemmungen zu schützen. HTTP

CloudFront akzeptiert nur wohlgeformte Verbindungen, wodurch verhindert wird, dass viele gängige DDoS Angriffe wie SYN Floods und UDP Reflection-Angriffe Ihren Ursprung erreichen. DDoSAngriffe werden außerdem geografisch in der Nähe der Quelle isoliert, wodurch verhindert wird, dass sich der Datenverkehr auf andere Standorte auswirkt. Diese Funktionen können Ihre Fähigkeit, Benutzern auch bei großen DDoS Angriffen weiterhin Traffic bereitzustellen, erheblich verbessern. Sie können CloudFront sie verwenden, um eine Quelle im AWS oder an anderer Stelle im Internet zu schützen.

Wenn Sie Amazon Simple Storage Service (Amazon S3) verwenden, um statische Inhalte im Internet bereitzustellen, AWS empfiehlt Ihnen Amazon CloudFront zum Schutz Ihres Buckets zu verwenden, was folgende Vorteile bietet:

- Schränkt den Zugriff auf den Amazon S3 S3-Bucket ein, sodass er nicht öffentlich zugänglich ist.
- Stellt sicher, dass Zuschauer (Benutzer) nur über die angegebene CloudFront Distribution auf die Inhalte im Bucket zugreifen können. Dadurch wird verhindert, dass sie direkt aus dem Bucket oder über eine unbeabsichtigte Verteilung auf die Inhalte zugreifen können. CloudFront

Um dies zu erreichen, konfigurieren Sie CloudFront es so, dass authentifizierte Anfragen an Amazon S3 gesendet werden, und konfigurieren Sie Amazon S3 so, dass nur der Zugriff auf authentifizierte Anfragen von möglich ist. CloudFront CloudFront bietet zwei Möglichkeiten, authentifizierte Anfragen an einen Amazon S3 S3-Ursprung zu senden: Origin Access Control (OAC) und Origin Access Identity (OAI). Wir empfehlen die VerwendungOAC, da sie Folgendes unterstützt:

- Alle Amazon S3 S3-Buckets insgesamt AWS-Regionen, einschließlich der Opt-in-Regionen, die nach Dezember 2022 eingeführt wurden
- Serverseitige Amazon S3 S3-Verschlüsselung mit AWS KMS (SSE-KMS)
- Dynamische Anforderungen (`PUT` und `DELETE`) an Amazon S3

Weitere Informationen zu OAC und OAI finden Sie unter Beschränken des Zugriffs auf Amazon S3 S3-Herkunft.

Weitere Informationen zum Schutz und zur Optimierung der Leistung von Webanwendungen mit Amazon CloudFront finden Sie unter Erste Schritte mit Amazon CloudFront.

Schützen Sie Netzwerkverkehr, der weiter von Ihrem Ursprung entfernt ist, mit AWS Global Accelerator (BP1)

Global Accelerator ist ein Netzwerkdienst, der die Verfügbarkeit und Leistung des Benutzerverkehrs um bis zu 60% verbessert. Dies wird erreicht, indem eingehender Datenverkehr an dem Edge-Standort, der Ihren Benutzern am nächsten ist, eingespeist und über die AWS globale Netzwerkinfrastruktur zu Ihrer Anwendung weitergeleitet wird, unabhängig davon, ob er einzeln oder mehrfach AWS-Regionen ausgeführt wird.

Global Accelerator leitet TCP den UDP Datenverkehr auf der Grundlage der Leistung in der Nähe des Benutzers AWS-Region zum optimalen Endpunkt weiter. Wenn eine Anwendung ausfällt, bietet Global Accelerator innerhalb von 30 Sekunden ein Failover zum nächstbesten Endpunkt. Global Accelerator nutzt die enorme Kapazität des AWS globalen Netzwerks und die Integrationen mit Shield, wie z. B. eine statusfreie SYN Proxyfunktion, die neue Verbindungsversuche abwehrt und nur legitimen Endbenutzern dient, um Anwendungen zu schützen.

Sie können eine DDoS robuste Architektur implementieren, die viele der gleichen Vorteile bietet wie die Best Practices für die Bereitstellung von Webanwendungen am Edge, auch wenn Ihre Anwendung Protokolle verwendet, die nicht unterstützt werden, CloudFront oder wenn Sie eine Webanwendung betreiben, die globale statische IP-Adressen erfordert.

Beispielsweise benötigen Sie möglicherweise IP-Adressen, die Ihre Endbenutzer zur Zulassungsliste in ihren Firewalls hinzufügen können und die nicht von anderen AWS Kunden verwendet werden. In diesen Szenarien können Sie Global Accelerator verwenden, um Webanwendungen zu schützen, die auf dem Application Load Balancer ausgeführt werden, und in Verbindung damit auch AWS WAF Fluten von Anfragen auf Webanwendungsebene zu erkennen und zu verhindern.

Weitere Informationen zum Schutz und zur Optimierung der Leistung des Netzwerkverkehrs mithilfe von Global Accelerator finden Sie unter Erste Schritte mit Global Accelerator.

Auflösung von Domainnamen am Rand (BP3)

Themen

- Für die DNS Verfügbarkeit wird Route 53 verwendet
- Konfiguration von Route 53 zum Kostenschutz vor NXDOMAIN Angriffen

Für die DNS Verfügbarkeit wird Route 53 verwendet

Amazon Route 53 ist ein hochverfügbarer und skalierbarer Domain Name System (DNS) -Service, mit dem Sie Traffic an Ihre Webanwendung weiterleiten können. Es umfasst erweiterte Funktionen wie Verkehrsfluss, Zustandsprüfungen und Überwachung, latenzbasiertes Routing und Geo. DNS Mit diesen erweiterten Funktionen können Sie steuern, wie der Dienst auf DNS Anfragen reagiert, um die Leistung Ihrer Webanwendung zu verbessern und Seitenausfälle zu vermeiden. Es ist der einzige AWS Dienst, der eine hundertprozentige Verfügbarkeit SLA der Datenebene bietet.

Amazon Route 53 verwendet Techniken wie Shuffle Sharding und Anycast Striping, mit denen Benutzer auf Ihre Anwendung zugreifen können, auch wenn der DNS Service Ziel eines Angriffs ist. DDoS

Beim Shuffle-Sharding entspricht jeder Nameserver in Ihrem Delegierungssatz einem eindeutigen Satz von Edge-Standorten und Internetpfaden. Dies sorgt für eine höhere Fehlertoleranz und minimiert Überschneidungen zwischen Kunden. Wenn ein Nameserver in der Delegierungsgruppe nicht verfügbar ist, können Benutzer es erneut versuchen und eine Antwort von einem anderen Nameserver an einem anderen Edge-Standort erhalten.

Mit Anycast-Striping kann jede DNS Anfrage vom optimalen Standort bedient werden, wodurch die Netzwerklast verteilt und die Latenz reduziert wird. DNS Dies ermöglicht eine schnellere Antwort für Benutzer. Darüber hinaus kann Amazon Route 53 Anomalien in der Quelle und dem Volumen von DNS Abfragen erkennen und Anfragen von Benutzern priorisieren, von denen bekannt ist, dass sie zuverlässig sind.

Weitere Informationen zur Verwendung von Amazon Route 53 zur Weiterleitung von Benutzern zu Ihrer Anwendung finden Sie unter Erste Schritte mit Amazon Route 53.

Konfiguration von Route 53 zum Kostenschutz vor **`NXDOMAIN`** Angriffen

`NXDOMAIN`Angriffe treten auf, wenn Angreifer eine Flut von Anfragen an eine Hosting-Zone für nicht existierende Subdomänen senden, oft über bekannte „gute“ Resolver. Der Zweck dieser Angriffe kann darin bestehen, den Cache des rekursiven Resolvers und/oder die Verfügbarkeit des autoritativen Resolvers zu beeinträchtigen, oder es kann sich um eine Form der DNS Erkundung handeln, um Datensätze in gehosteten Zonen zu finden. Durch die Verwendung von Route 53 für Ihren autoritativen Resolver wird das Risiko einer Beeinträchtigung der Verfügbarkeit/Leistung

gemindert. Dies kann jedoch zu einer erheblichen Erhöhung der monatlichen Kosten für Route 53 führen. Um sich vor Kostensteigerungen zu schützen, sollten Sie die Preisgestaltung für Route 53 nutzen, bei der DNS Abfragen kostenlos sind, wenn beide der folgenden Bedingungen zutreffen:

- Der Domain- oder Subdomainname (`example.comoderstore.example.com`) und der Datensatztyp (`A`) in der Abfrage stimmen mit einem Aliaseintrag überein.
- Das Alias-Ziel ist eine AWS Ressource, bei der es sich nicht um einen anderen Route 53-Datensatz handelt.

Erstellen Sie einen Platzhaltereintrag, z. B. `*.example.com` mit einem Typ `A` (Alias), der auf eine AWS Ressource wie eine EC2 Instance, Elastic Load Balancer oder CloudFront Distribution verweist, sodass bei einer Abfrage nach die IP der Ressource zurückgegeben wird und Ihnen die Abfrage nicht in Rechnung gestellt wird. `qwerty12345.example.com`

Verteidigung auf Anwendungsebene (BP1,) BP2

Viele der bisher in diesem paper erörterten Techniken sind wirksam, um die Auswirkungen von DDoS Angriffen auf die Infrastrukturebene auf die Verfügbarkeit Ihrer Anwendung zu mindern. Um sich auch vor Angriffen auf Anwendungsebene zu schützen, müssen Sie eine Architektur implementieren, die es Ihnen ermöglicht, bösartige Anfragen gezielt zu erkennen, zu skalieren, zu absorbieren und zu blockieren. Dies ist ein wichtiger Aspekt, da netzwerkbasierte DDoS Abwehrsysteme bei der Abwehr komplexer Angriffe auf Anwendungsebene im Allgemeinen nicht wirksam sind.

Erkennen und filtern Sie bösartige Webanfragen (,) BP1 BP2

Wenn Ihre Anwendung läuft AWS, können Sie Amazon CloudFront (und seine HTTP Caching-Funktion) und Shield Advanced Automatic Application Layer-Schutz nutzen AWS WAF, um zu verhindern, dass bei DDoS Angriffen auf Anwendungsebene unnötige Anfragen Ihren Ursprung erreichen.

Amazon CloudFront

Amazon CloudFront kann dazu beitragen, die Serverlast zu reduzieren, indem verhindert wird, dass Datenverkehr, der nicht aus dem Internet stammt, Ihren Ursprung erreicht. Um eine Anfrage an eine CloudFront Anwendung zu senden, muss die Verbindung mit einer gültigen IP-Adresse über einen abgeschlossenen TCP Handshake hergestellt werden, der nicht gefälscht werden kann. CloudFront Kann außerdem Verbindungen vor langsam lesenden oder langsam schreibenden Angreifern (z. B. Slowloris) automatisch schließen.

CDN-Caching

CloudFront ermöglicht es Ihnen, sowohl dynamische als auch statische Inhalte von AWS Edge-Standorten aus bereitzustellen. Indem Sie Proxyinhalte aus dem CDN Cache bereitstellen, verhindern Sie, dass Anfragen für die Dauer des Cachings von einem bestimmten Edge-Cache-Knoten aus Ihren Ursprung erreichen. TTL In Verbindung mit dem Kollabieren von Anfragen für abgelaufene, aber zwischenspeicherbare Inhalte TTL bedeuten selbst sehr kurze Anfragen, dass während einer Flut von Anfragen für diesen Inhalt nur eine geringe Anzahl von Anfragen Ihren Ursprung erreicht. Darüber hinaus kann die Aktivierung von Funktionen wie CloudFront Origin Shield dazu beitragen, die Belastung Ihres Origins weiter zu reduzieren. Alles, was Sie tun können, um Ihre Cache-Trefferquote zu verbessern, kann den Unterschied zwischen einem effektiven und einem nicht wirksamen Request-Flood-Angriff ausmachen.

AWS WAF

Mithilfe AWS WAF von können Sie Web-Zugriffskontrolllisten (WebACLs) für Ihre globalen CloudFront Distributionen oder regionalen Ressourcen konfigurieren, um Anfragen auf der Grundlage von Anforderungssignaturen zu filtern, zu überwachen und zu blockieren. Um zu bestimmen, ob Anfragen zugelassen oder blockiert werden sollen, können Sie Faktoren wie die IP-Adresse oder das Herkunftsland, bestimmte Zeichenfolgen oder Muster in der Anfrage, die Größe bestimmter Teile der Anfrage und das Vorhandensein von bösartigem SQL Code oder Skripting berücksichtigen. Sie können auch CAPTCHA Puzzles und automatische Client-Sitzungen gegen Anfragen ausführen.

AWS WAF Beides ermöglicht es dir CloudFront außerdem, geografische Einschränkungen festzulegen, um Anfragen aus ausgewählten Ländern zu blockieren oder zuzulassen. Dies kann dazu beitragen, Angriffe von geografischen Standorten aus zu blockieren oder ihre Geschwindigkeit zu begrenzen, von denen Sie nicht erwarten, dass sie Benutzern zugutekommen. Wenn detaillierte Anweisungen für geografische Vergleichsregeln enthalten sind AWS WAF, können Sie den Zugriff bis auf Regionsebene kontrollieren.

Mithilfe von Scope-down-Anweisungen können Sie den Umfang der Anfragen einschränken, die von der Regel ausgewertet werden, um Kosten zu sparen. Außerdem können Sie Webanfragen mit „Labels“ versehen, damit eine Regel, die der Anfrage entspricht, die Vergleichsergebnisse an Regeln weitergeben kann, die später im selben Web ausgewertet werden. ACL Wählen Sie diese Option, um dieselbe Logik für mehrere Regeln wiederzuverwenden.

Sie können auch eine vollständige benutzerdefinierte Antwort mit Antwortcode, Headern und Text definieren.

Um böswillige Anfragen zu identifizieren, überprüfen Sie Ihre Webserverprotokolle oder verwenden Sie AWS WAF die Protokollierung und Anforderungssampling. Wenn Sie die AWS WAF Protokollierung aktivieren, erhalten Sie detaillierte Informationen über den vom Web analysierten Datenverkehr. ACL AWS WAF unterstützt die Protokollfilterung, sodass Sie angeben können, welche Webanfragen protokolliert werden und welche Anfragen nach der Überprüfung aus dem Protokoll gelöscht werden.

Zu den in den Protokollen aufgezeichneten Informationen gehören die Uhrzeit, zu der die Anfrage von Ihrer AWS Ressource AWS WAF eingegangen ist, detaillierte Informationen zu der Anfrage und die entsprechende Aktion für jede angeforderte Regel.

Stichprobenanfragen enthalten Details zu Anfragen innerhalb der letzten drei Stunden, die einer Ihrer AWS WAF Regeln entsprachen. Sie können diese Informationen verwenden, um potenziell bösartige Datenverkehrssignaturen zu identifizieren und eine neue Regel zu erstellen, um diese Anfragen abzulehnen. Wenn Sie eine Reihe von Anfragen mit einer zufälligen Abfragezeichenfolge sehen, stellen Sie sicher, dass Sie nur die Abfragezeichenfolgenparameter zulassen, die für den Cache Ihrer Anwendung relevant sind. Diese Technik ist hilfreich, um einen Cache-Busting-Angriff gegen Ihren Ursprung abzuwehren.

AWS WAF — Ratenbasierte Regeln

AWS empfiehlt dringend, sich vor einer Flut von HTTP Anfragen zu schützen, indem die ratenbasierten Regeln verwendet werden AWS WAF , um IP-Adressen böswilliger Akteure automatisch zu blockieren, wenn die Anzahl der Anfragen, die in einem 5-minütigen gleitenden Fenster eingehen, einen von Ihnen definierten Schwellenwert überschreitet. IP-Adressen von Clients, bei denen ein Verstoß vorliegt, erhalten eine verbotene 403-Antwort (oder eine konfigurierte Blockfehlerantwort) und bleiben blockiert, bis die Anforderungsraten unter den Schwellenwert fallen.

Es wird empfohlen, ratenbasierte Regeln zu kombinieren, um einen besseren Schutz zu bieten, sodass Sie:

- Eine pauschale ratenbasierte Regel zum Schutz Ihrer Anwendung vor großen Fluten. HTTP
- Eine oder mehrere ratenbasierte Regeln zum Schutz bestimmter URIs Regeln zu restriktiveren Tarifen als die pauschale ratenbasierte Regel.

Sie können beispielsweise eine pauschale, ratenbasierte Regel (keine Angabe zum Umfang) mit einer Obergrenze von 500 Anfragen innerhalb von 5 Minuten wählen und dann mithilfe von Scope-down-Aussagen eine oder mehrere der folgenden ratenbasierten Regeln mit niedrigeren Grenzwerten als 500 (bis zu 100 Anfragen innerhalb von 5 Minuten) erstellen:

- Schützen Sie Ihre Webseiten mit einer Scopedown-Anweisung wie "`if NOT uri_path contains '.'`", sodass Anfragen nach Ressourcen ohne Dateierweiterung weiter geschützt sind. Dadurch wird auch Ihre Homepage (`/`) geschützt, die häufig als URI Zielpfad angesehen wird.
- Schützen Sie dynamische Endpunkte mit einer Scopedown-Anweisung wie "“ `if method exactly matches 'post' (convert lowercase)`
- Schützen Sie umfangreiche Anfragen, die Ihre Datenbank erreichen oder ein Einmalkennwort (OTP) aufrufen, mit einem Scopedown wie "“ `if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

Ratenbasierte Lösungen im Blockmodus bilden den Eckpfeiler Ihrer defense-in-depth WAF Konfiguration zum Schutz vor einer Flut von Anfragen und sind Voraussetzung für die Genehmigung von AWS Shield Advanced Kostenschutzanfragen. In den folgenden Abschnitten werden wir weitere defense-in-depth WAF Konfigurationen untersuchen.

AWS WAF — IP-Reputation

Um Angriffe zu verhindern, die auf der Reputation von IP-Adressen basieren, können Sie Regeln mithilfe von IP-Abgleich erstellen oder verwaltete Regeln für verwenden AWS WAF.

Die Regelgruppe der IP-Reputationsliste von Amazon umfasst Regeln, die auf den internen Bedrohungsinformationen von Amazon basieren. Diese Regeln suchen nach IP-Adressen, bei denen es sich um Bots handelt, die AWS Ressourcen ausspionieren oder aktiv an Aktivitäten teilnehmen. DDoS Es wurde beobachtet, dass die `AWSManagedIPDDoSList` Regel mehr als 90% der Fluten bösartiger Anfragen blockiert.

Die Regelgruppe „Liste anonymer IP-Adressen“ enthält Regeln zum Blockieren von Anfragen von Diensten, die die Verschleierung der Identität von Zuschauern ermöglichen. Dazu gehören Anfragen von ProxysVPNs, Tor-Knoten und Cloud-Plattformen (ausgenommen). AWS

Darüber hinaus können Sie IP-Reputationslisten von Drittanbietern verwenden, indem Sie die IP-Listen-Parser-Komponente der Security Automations for Solution verwenden. AWS WAF

AWS WAF - Intelligente Abwehr von Bedrohungen

Botnetze stellen eine ernste Sicherheitsbedrohung dar und werden häufig für illegale oder schädliche Aktivitäten wie das Versenden von Spam, das Stehlen vertraulicher Daten, das Auslösen von Ransomware-Angriffen, das Begehen von Werbebetrug durch betrügerische Klicks oder das Starten von Distributed () -Angriffen eingesetzt. denial-of-service DDoS Verwenden Sie die verwaltete

Regelgruppe Bot Control, um AWS WAF Bot-Angriffe zu verhindern. Diese Regelgruppe bietet eine grundlegende, „allgemeine“ Schutzstufe, mit der selbstidentifizierende Bots gekennzeichnet werden, allgemein wünschenswerte Bots verifiziert und Bot-Signaturen mit hoher Zuverlässigkeit erkannt werden. Außerdem bietet sie eine „gezielte“ Schutzstufe, die auch fortgeschrittene Bots erkennt, die sich nicht selbst identifizieren.

Gezielte Schutzmaßnahmen verwenden fortschrittliche Erkennungstechniken wie Browserabfragen, Fingerabdrücke und Verhaltensheuristiken, um bösartigen Bot-Traffic zu identifizieren, und wenden dann Gegenmaßnahmen wie Ratenbegrenzung und Challenge-Regelaktionen an. CAPTCHA Targeted bietet auch Optionen zur Ratenbegrenzung, um menschenähnliche Zugriffsmuster durchzusetzen und dynamische Ratenbegrenzungen mithilfe von Anforderungstoken anzuwenden. Weitere Informationen finden Sie unter Regelgruppe AWS WAF Bot Control. Um böswillige Übernahmeversuche auf der Anmeldeseite Ihrer Anwendung zu erkennen und zu verwalten, können Sie die Regelgruppe AWS WAF Fraud Control Account Takeover Prevention (ATP) verwenden. Zu diesem Zweck untersucht die Regelgruppe Anmeldeversuche, die Kunden an den Anmeldeendpunkt Ihrer Anwendung senden, und untersucht auch die Antworten Ihrer Anwendung auf Anmeldeversuche, um die Erfolgs- und Fehlschlagrate nachzuverfolgen.

Betrug bei der Kontoerstellung ist eine illegale Online-Aktivität, bei der ein Angreifer versucht, ein oder mehrere gefälschte Konten zu erstellen. Angreifer verwenden gefälschte Konten für betrügerische Aktivitäten wie den Missbrauch von Werbe- und Anmeldeboni, das Ausgeben einer anderen Person und für Cyberangriffe wie Phishing. Das Vorhandensein gefälschter Konten kann sich negativ auf Ihr Unternehmen auswirken, da es Ihren Ruf bei Kunden schädigt und der Gefahr von Finanzbetrug ausgesetzt ist.

Sie können Betrugsversuche bei der Kontoerstellung überwachen und kontrollieren, indem Sie die Funktion AWS WAF Fraud Control zur Betrugsprävention bei der Kontoerstellung (ACFP) implementieren. AWS WAF bietet diese Funktion in der Von AWS verwaltete Regeln Regelgruppe `AWS ManagedRulesACFPRuleSet` mit integrierter Begleitanwendung anSDKs.

Weitere Informationen zu diesen Schutzmaßnahmen finden Sie unter AWS WAF Intelligent Threat Mitigation.

Automatisches Abmildern von Ereignissen auf Anwendungsebene DDoS (,,) BP1 BP2 BP6

Wenn Sie ein Abonnement haben AWS Shield Advanced, können Sie die automatische DDoSAbwehr auf Anwendungsebene von Shield Advanced aktivieren. Diese Funktion erstellt, bewertet und

implementiert automatisch AWS WAF Regeln zur Abwehr von DDoS Layer-7-Ereignissen in Ihrem Namen.

AWS Shield Advanced richtet eine Datenverkehrsbasis für jede geschützte Ressource ein, die einem Web zugeordnet ist. WAF ACL Datenverkehr, der erheblich von der festgelegten Ausgangsbasis abweicht, wird als DDoS potenzielles Ereignis gekennzeichnet. Nachdem ein Ereignis erkannt wurde, wird AWS Shield Advanced versucht, eine Signatur der Webanfragen zu identifizieren, die das Ereignis ausmachen. Wenn eine Signatur identifiziert wird, werden AWS WAF Regeln erstellt, um den Datenverkehr mit dieser Signatur einzudämmen.

Sobald Regeln anhand der historischen Baseline bewertet und als sicher eingestuft wurden, werden sie der von Shield verwalteten Regelgruppe hinzugefügt, und Sie können wählen, ob die Regeln im Zähl- oder Blockmodus bereitgestellt werden sollen. Shield Advanced entfernt automatisch AWS WAF Regeln, nachdem festgestellt wurde, dass ein Ereignis vollständig abgeklungen ist.

Engage SRT (nur für Shield Advanced-Abonnenten)

Wenn Sie Shield Advanced abonniert haben, können Sie den außerdem beauftragen, Regeln AWS SRT zur Abwehr eines Angriffs zu erstellen, der die Verfügbarkeit Ihrer Anwendung beeinträchtigt. Sie können AWS SRT eingeschränkten Zugriff auf Ihr Konto gewähren und. AWS Shield Advanced AWS WAF APIs AWS SRTgreift nur mit Ihrer ausdrücklichen Genehmigung auf diese APIs zu, um Abhilfemaßnahmen auf Ihrem Konto vorzunehmen. Weitere Informationen finden Sie im Support Abschnitt dieses Dokuments.

Sie können AWS Firewall Manager es verwenden, um Sicherheitsregeln wie AWS Shield Advanced Schutzmaßnahmen und Regeln in Ihrer gesamten Organisation zentral zu konfigurieren und AWS WAF zu verwalten. Ihr AWS Organizations Verwaltungskonto kann ein Administratorkonto festlegen, das berechtigt ist, Firewall Manager Manager-Richtlinien zu erstellen. Mit diesen Richtlinien können Sie Kriterien wie Ressourcentyp und Tags definieren, die bestimmen, wo Regeln angewendet werden. Dies ist nützlich, wenn Sie mehrere Konten haben und Ihren Schutz standardisieren möchten.

Weitere Informationen über:

- Von AWS verwaltete Regeln für AWS WAF, siehe Von AWS verwaltete Regeln für AWS WAF.
- Informationen zur Beschränkung des Zugriffs auf Ihre CloudFront Distribution mithilfe geografischer Beschränkungen finden Sie unter Beschränkung der geografischen Verbreitung Ihrer Inhalte.
- Informationen zur Verwendung AWS WAF finden Sie unter:

  - Erste Schritte mit AWS WAF
  - Protokollierung von ACL Web-Traffic-Informationen
  - Ein Beispiel für Webanfragen anzeigen
- Konfiguration ratenbasierter Regeln finden Sie unter Schützen von Websites und Diensten mithilfe von ratenbasierten Regeln für. AWS WAF
- Informationen zur Verwaltung der Bereitstellung von Regeln auf Ihren AWS Ressourcen mit Firewall Manager finden Sie unter:
  - Erste Schritte mit Firewall Manager AWS WAF Manager-Richtlinien.
  - Erste Schritte mit den erweiterten Richtlinien von Firewall Manager Shield.

Reduzierung der Angriffsfläche

Ein weiterer wichtiger Aspekt bei der Entwicklung einer AWS Lösung ist die Begrenzung der Möglichkeiten, die ein Angreifer hat, Ihre Anwendung ins Visier zu nehmen. Dieses Konzept wird als Reduzierung der Angriffsfläche bezeichnet. Ressourcen, die nicht dem Internet ausgesetzt sind, sind schwieriger anzugreifen, wodurch die Möglichkeiten, die Angreifer haben, die Verfügbarkeit Ihrer Anwendung ins Visier zu nehmen, eingeschränkt sind.

Wenn Sie beispielsweise nicht erwarten, dass Benutzer direkt mit bestimmten Ressourcen interagieren, stellen Sie sicher, dass diese Ressourcen nicht über das Internet zugänglich sind. Ebenso sollten Sie keinen Datenverkehr von Benutzern oder externen Anwendungen über Ports oder Protokolle akzeptieren, die für die Kommunikation nicht erforderlich sind.

Im folgenden Abschnitt finden Sie AWS bewährte Methoden, mit denen Sie Ihre Angriffsfläche reduzieren und die Internetgefährdung Ihrer Anwendung einschränken können.

Verschleierung von AWS Ressourcen (BP1,,) BP4 BP5

In der Regel können Benutzer eine Anwendung schnell und einfach verwenden, ohne dass die AWS Ressourcen vollständig im Internet verfügbar sein müssen.

Sicherheitsgruppen und Netzwerk ACLs (BP5)

Mit Amazon Virtual Private Cloud (AmazonVPC) können Sie einen logisch isolierten Bereich bereitstellen, in AWS Cloud dem Sie AWS Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.

Sicherheitsgruppen und Netzwerke ACLs sind sich insofern ähnlich, als sie es Ihnen ermöglichen, den Zugriff auf AWS Ressourcen innerhalb Ihres VPC Netzwerks zu kontrollieren. Sicherheitsgruppen ermöglichen es Ihnen jedoch, eingehenden und ausgehenden Datenverkehr auf Instanzebene zu kontrollieren, während Netzwerke ähnliche Funktionen auf VPC Subnetzebene ACLs bieten. Für die Nutzung von Sicherheitsgruppen oder Netzwerken fallen keine zusätzlichen Gebühren an. ACLs

Sie können wählen, ob Sie beim Starten einer Instance Sicherheitsgruppen angeben oder die Instance zu einem späteren Zeitpunkt einer Sicherheitsgruppe zuordnen möchten. Jeglicher Internetverkehr zu einer Sicherheitsgruppe wird implizit verweigert, es sei denn, Sie erstellen eine Zulassungsregel, die den Datenverkehr zulässt.

Wenn Sie beispielsweise EC2 Amazon-Instances hinter einem Elastic Load Balancer haben, sollten die Instances selbst nicht öffentlich zugänglich sein müssen und sollten IPs nur privat sein. Stattdessen könnten Sie dem Elastic Load Balancer Zugriff auf die erforderlichen Ziel-Listener-Ports gewähren, indem Sie eine Sicherheitsgruppenregel verwenden, die den Zugriff auf 0.0.0.0/0 erlaubt (um Probleme mit der Verbindungsverfolgung zu vermeiden — siehe Hinweis unten) in Verbindung mit einer Network Access Control List (NACL) im Zielgruppen-Subnetz, sodass nur die Elastic Load Balancing Balancing-IP-Bereiche mit den Instances kommunizieren können. Dadurch wird sichergestellt, dass der Internetverkehr nicht direkt mit Ihren EC2 Amazon-Instances kommunizieren kann, was es für einen Angreifer schwieriger macht, etwas über Ihre Anwendung zu erfahren und sie zu beeinflussen.

Wenn Sie ein Netzwerk erstellenACLs, können Sie sowohl Regeln zum Zulassen als auch zum Ablehnen angeben. Dies ist nützlich, wenn Sie bestimmte Arten von Datenverkehr für Ihre Anwendung explizit verweigern möchten. Sie können beispielsweise IP-Adressen (als CIDR Bereiche), Protokolle und Zielports definieren, denen der Zugriff auf das gesamte Subnetz verweigert wird. Wenn Ihre Anwendung nur für den TCP Datenverkehr verwendet wird, können Sie eine Regel erstellen, um den gesamten UDP Datenverkehr zu verweigern oder umgekehrt. Diese Option ist nützlich, wenn Sie auf DDoS Angriffe reagieren, da Sie damit Ihre eigenen Regeln zur Abwehr des Angriffs erstellen können, wenn Sie die Quelle IPs oder eine andere Signatur kennen.

Wenn Sie ein Abonnement haben AWS Shield Advanced, können Sie Elastic IP-Adressen als geschützte Ressourcen registrieren. DDoSAngriffe auf Elastic IP-Adressen, die als geschützte Ressourcen registriert wurden, werden schneller erkannt, was zu einer schnelleren Abwehr führen kann. Wenn ein Angriff erkannt wird, lesen die DDoS Abwehrsysteme das NetzwerkACL, das der gewünschten Elastic IP-Adresse entspricht, und erzwingt es an der AWS Netzwerkgrenze und nicht auf Subnetzebene. Dadurch wird Ihr Risiko, dass eine Reihe von Angriffen auf die Infrastrukturebene Auswirkungen haben, erheblich reduziert. DDoS

Weitere Informationen zur Konfiguration von Sicherheitsgruppen und Netzwerken ACLs zur Optimierung der DDoS Ausfallsicherheit finden Sie unter How to Help Prepare for DDoS Attacks by Reducing Your Attack Surface.

Weitere Informationen zur Verwendung von Shield Advanced mit Elastic IP-Adressen als geschützte Ressourcen finden Sie in den Schritten zum Abonnieren AWS Shield Advanced.

Schützen Sie Ihre Herkunft (BP1,BP5)

Wenn Sie Amazon CloudFront mit einer Herkunft verwenden, die innerhalb Ihres liegtVPC, sollten Sie sicherstellen, dass nur Ihr CloudFront Vertrieb Anfragen an Ihren Ursprung weiterleiten kann.

Mit Edge-to-Origin-Anforderungsheadern können Sie den Wert vorhandener Anforderungsheader hinzufügen oder deren Wert überschreiben, wenn Anfragen an Ihren Absender weitergeleitet werden CloudFront . Du kannst die benutzerdefinierten Origin-Header verwenden, zum Beispiel den `X-Shared-Secret` Header, um zu überprüfen, ob die Anfragen an deinen Absender gesendet wurden. CloudFront

Weitere Informationen zum Schutz Ihres Ursprungs mit benutzerdefinierten Origin-Headern finden Sie unter Benutzerdefinierte Header zu ursprünglichen Anfragen hinzufügen und Zugriff auf Application Load Balancers einschränken.

Eine Anleitung zur Implementierung einer Musterlösung zur automatischen Rotation des Werts von Origin Custom Headers für die Ursprungszugriffsbeschränkung finden Sie unter How to enhance Amazon CloudFront Origin Security with AWS WAF and Secrets Manager.

Alternativ können Sie eine AWS LambdaFunktion verwenden, um Ihre Sicherheitsgruppenregeln automatisch so zu aktualisieren, dass nur CloudFront Datenverkehr zugelassen wird. Auf diese Weise wird die Sicherheit Ihres Ursprungs verbessert, indem sichergestellt wird, dass böswillige Benutzer den Zugriff auf Ihre Webanwendung nicht umgehen CloudFront können. AWS WAF

Weitere Informationen darüber, wie Sie Ihren Ursprung schützen können, indem Sie Ihre Sicherheitsgruppen und den `X-Shared-Secret` Header automatisch aktualisieren, finden Sie unter So aktualisieren Sie Ihre Sicherheitsgruppen für Amazon CloudFront und mithilfe AWS WAFAWS Lambda von

Die Lösung erfordert jedoch zusätzliche Konfiguration und die Kosten für die Ausführung von Lambda-Funktionen. Um dies zu vereinfachen, haben wir jetzt eine von AWS-verwaltete Präfixliste eingeführt, mit der Sie den eingehenden HTTP HTTPS /-Traffic CloudFront auf Ihre Ursprünge beschränken können, und zwar nur von den IP-Adressen, an die der Absender gerichtet CloudFront ist. AWS-verwaltete Präfixlisten werden von erstellt und verwaltet AWS und können ohne zusätzliche Kosten verwendet werden. Sie können CloudFront in Ihren (Amazon-VPC) Sicherheitsgruppenregeln, Subnetz-Routing-Tabellen, allgemeinen Sicherheitsgruppenregeln für und allen anderen AWS Ressourcen, die eine verwaltete Präfixliste verwenden können AWS Firewall Manager, auf die Liste der verwalteten Präfixe verweisen.

Weitere Informationen zur Verwendung der AWS-managed prefix list für Amazon CloudFront finden Sie unter Beschränken Sie den Zugriff auf Ihre Ursprünge mithilfe der AWS-managed prefix list für Amazon. CloudFront

> **Note**
>
> Wie bereits in anderen Abschnitten dieses Dokuments beschrieben, kann der Einsatz von Sicherheitsgruppen zum Schutz Ihrer Herkunft die Verbindungsverfolgung von Sicherheitsgruppen als potenzieller Engpass bei einer Flut von Anfragen mit sich bringen. Sofern Sie nicht in der Lage sind, bösartige Anfragen CloudFront mithilfe einer Caching-Richtlinie zu filtern, die das Zwischenspeichern ermöglicht, ist es möglicherweise besser, sich auf die zuvor erläuterten benutzerdefinierten Origin-Header zu verlassen, um zu überprüfen, ob die Anfragen an Ihren Ursprung gesendet wurden, anstatt Sicherheitsgruppen zu verwenden. CloudFront Die Verwendung eines benutzerdefinierten Anforderungsheaders mit einer Application Load Balancer-Listener-Regel verhindert Drosselungen aufgrund von Tracking-Limits, die sich auf den Aufbau neuer Verbindungen zu einem Load Balancer auswirken können, sodass Application Load Balancer im Falle eines Angriffs auf die Zunahme des Datenverkehrs skalieren kann. DDoS

APIEndgeräte schützen () BP4

Wenn Sie eine API der Öffentlichkeit zugänglich machen müssen, besteht die Gefahr, dass das API Frontend Ziel eines DDoS Angriffs wird. Um das Risiko zu verringern, können Sie Amazon API Gateway als Zugang zu Anwendungen verwenden EC2 AWS Lambda, die auf Amazon oder anderswo ausgeführt werden. Durch die Verwendung von Amazon API Gateway benötigen Sie keine eigenen Server für das API Frontend und können andere Komponenten Ihrer Anwendung verschleiern. Indem Sie es schwieriger machen, die Komponenten Ihrer Anwendung zu erkennen, können Sie verhindern, dass diese AWS Ressourcen Ziel eines Angriffs werden. DDoS

Wenn Sie Amazon API Gateway verwenden, können Sie zwischen zwei Arten von API Endpunkten wählen. Die erste ist die Standardoption: Edge-optimierte API Endgeräte, auf die über eine Amazon-Distribution zugegriffen wird. CloudFront Die Verteilung wird jedoch von API Gateway erstellt und verwaltet, sodass Sie keine Kontrolle darüber haben. Die zweite Option besteht darin, einen regionalen API Endpunkt zu verwenden, auf den von demselben AWS-Region Endpunkt aus zugegriffen REST API wird, auf dem Ihr bereitgestellt wurde. AWS empfiehlt, den zweiten Endpunkttyp zu verwenden und ihn mit Ihrer eigenen CloudFront Amazon-Distribution zu verknüpfen. Auf diese Weise haben Sie die Kontrolle über den CloudFront Amazon-Vertrieb und können ihn AWS WAF für den Schutz auf Anwendungsebene verwenden. Dieser Modus bietet Ihnen Zugriff auf skalierte DDoS Minderungskapazitäten im gesamten AWS globalen Edge-Netzwerk.

Wenn Sie Amazon CloudFront und AWS WAF Amazon API Gateway verwenden, konfigurieren Sie die folgenden Optionen:

- Konfigurieren Sie das Cache-Verhalten für Ihre Distributionen so, dass alle Header an den regionalen API Gateway-Endpunkt weitergeleitet werden. Auf diese Weise CloudFront wird der Inhalt als dynamisch behandelt und das Zwischenspeichern des Inhalts übersprungen.
- Schützen Sie Ihr API Gateway vor direktem Zugriff, indem Sie die Distribution so konfigurieren, dass sie den benutzerdefinierten Origin-Header enthält x-api-key, indem Sie den APISchlüsselwert in API Gateway festlegen.
- Schützen Sie das Backend vor übermäßigem Datenverkehr, indem Sie Standard- oder Burst-Rate-Limits für jede Methode in Ihrem REST APIs konfigurieren.

Weitere Informationen zur Erstellung APIs mit Amazon API Gateway finden Sie unter Erste Schritte mit Amazon API Gateway.

Operative Techniken

Die Techniken zur Risikominderung in diesem paper helfen Ihnen dabei, Anwendungen zu entwickeln, die von Natur aus widerstandsfähig gegen DDoS Angriffe sind. In vielen Fällen ist es auch nützlich zu wissen, wann ein DDoS Angriff auf Ihre Anwendung abzielt, damit Sie Gegenmaßnahmen ergreifen können. In diesem Abschnitt werden bewährte Methoden beschrieben, um Einblick in abnormales Verhalten zu erhalten, Warnmeldungen und Automatisierung zu erhalten, den Schutz in großem Umfang zu verwalten und zusätzlichen Support in Anspruch AWS zu nehmen.

Lasttest

Testen Sie Ihre Anwendung regelmäßig anhand der Richtlinien in unserem Whitepaper Load Testing Applications mit erwartetem und höherem Traffic, damit Sie sehen können, wie effektiv Ihre Architektur ist, wie Ihre Auto Scaling Scaling-Richtlinien funktionieren und wie Ihre Fehlerbehandlung funktioniert. Testen Sie den erwarteten Anstieg und Rückgang des Datenverkehrs, aber auch das Verhalten vom Typ „Flash-Crowd“. Testen Sie entweder regelmäßig oder vor jeder Hauptversion erneut. Halten Sie sich bei Layer-3- oder DDoS Layer-4-Simulationstests, z. B. bei SYN Hochwasser, an unsere Richtlinien für DDoS Simulationstests.

Metriken und Alarme

Als bewährte Methode sollten Sie Tools zur Infrastruktur- und Anwendungsüberwachung verwenden, um die Verfügbarkeit Ihrer Anwendung zu überprüfen und sicherzustellen, dass Ihre Anwendung nicht durch ein DDoS Ereignis beeinträchtigt wird. Optional können Sie Route 53-Zustandsprüfungen für Anwendungen und Infrastruktur für die Ressourcen konfigurieren, um die Erkennung von DDoS Ereignissen zu verbessern. Weitere Informationen zu Integritätsprüfungen finden Sie AWS WAF im Entwicklerhandbuch für Firewall Manager und Shield Advanced.

Wenn eine wichtige Betriebskennzahl erheblich vom erwarteten Wert abweicht, versucht ein Angreifer möglicherweise, die Verfügbarkeit Ihrer Anwendung ins Visier zu nehmen. Wenn Sie mit dem normalen Verhalten Ihrer Anwendung vertraut sind, können Sie schneller Maßnahmen ergreifen, wenn Sie eine Anomalie entdecken. Amazon CloudWatch kann Ihnen helfen, indem es die Anwendungen überwacht, auf denen Sie laufen AWS. Sie können beispielsweise Kennzahlen sammeln und verfolgen, Protokolldateien sammeln und überwachen, Alarme einrichten und automatisch auf Änderungen in Ihren AWS Ressourcen reagieren.

Wenn Sie sich bei der DDoS Architektur Ihrer Anwendung an die Referenzarchitektur für Stabilität halten, werden gängige Angriffe auf die Infrastrukturebene blockiert, bevor sie Ihre Anwendung erreichen. Wenn Sie ein Abonnement haben AWS Shield Advanced, haben Sie Zugriff auf eine Reihe von CloudWatch Kennzahlen, die darauf hinweisen können, dass Ihre Anwendung ins Visier genommen wird.

Sie können beispielsweise Alarme so konfigurieren, dass sie Sie benachrichtigen, wenn ein DDoS Angriff im Gange ist, sodass Sie den Zustand Ihrer Anwendung überprüfen und entscheiden können, ob Sie aktiv AWS SRT werden möchten. Sie können die `DDoSDetected` Metrik so konfigurieren, dass Sie darüber informiert werden, ob ein Angriff erkannt wurde. Wenn Sie anhand des Angriffsvolumens gewarnt werden möchten, können Sie auch die `DDoSAttackRequestsPerSecond` Metriken `DDoSAttackBitsPerSecondDDoSAttackPacketsPerSecond`, oder verwenden. Sie können diese Metriken überwachen, indem Sie sie in Ihre eigenen Tools integrieren CloudWatch oder Tools von Drittanbietern wie Slack oder verwenden. PagerDuty

Ein Angriff auf Anwendungsebene kann viele CloudWatch Amazon-Kennzahlen erhöhen. Wenn Sie dies verwenden AWS WAF, können Sie es CloudWatch zur Überwachung und Aktivierung von Alarmen verwenden, wenn die Anzahl der Anfragen zunimmt, für die Sie festgelegt haben, dass AWS WAF sie zugelassen, gezählt oder blockiert werden. Auf diese Weise können Sie eine Benachrichtigung erhalten, wenn der Datenverkehr das Datenvolumen übersteigt, das Ihre Anwendung verarbeiten kann. Sie können auch Amazon- CloudFront, Amazon Route 53-, Application Load Balancer-, Network Load Balancer-, Amazon- und Auto Scaling-Metriken verwendenEC2, die nachverfolgt werden, um Änderungen CloudWatch zu erkennen, die auf einen DDoS Angriff hinweisen können.

In der folgenden Tabelle werden die CloudWatch Kennzahlen beschrieben, die häufig zur Erkennung und Reaktion auf DDoS Angriffe verwendet werden.

Tabelle 3 — Empfohlene CloudWatch Amazon-Metriken

Thema	Metrik	Beschreibung
AWS Shield Advanced	`DDoSDetected`	Zeigt ein DDoS Ereignis für einen bestimmten Amazon-Ressourcennamen (ARN) an.
AWS Shield Advanced	`DDoSAttackBitsPerSecond`	Die Anzahl der Byte, die während eines DDoS

Thema	Metrik	Beschreibung
		Ereignisses für ein bestimmtes Ereignis beobachtet wurdenARN. Diese Metrik ist nur für Layer-3- oder DDoS Layer-4-Ereignisse verfügbar.
AWS Shield Advanced	`DDoSAttackPacketsPerSecond`	Die Anzahl der Pakete, die während eines DDoS Ereignisses für ein bestimmtes Ereignis beobachtet wurdenARN. Diese Metrik ist nur für Layer-3- oder DDoS Layer-4-Ereignisse verfügbar.
AWS Shield Advanced	`DDoSAttackRequestsPerSecond`	Die Anzahl der Anfragen, die während eines DDoS Ereignisses für ein bestimmtes Ereignis beobachtet wurdenARN. Diese Metrik ist nur für DDoS Layer-7-Ereignisse verfügbar und wird nur für die signifikantesten Layer-7-Ereignisse gemeldet.
AWS WAF	`AllowedRequests`	Die Anzahl der zulässigen Webanforderungen.
AWS WAF	`BlockedRequests`	Die Anzahl der blockierten Webanforderungen.
AWS WAF	`CountedRequests`	Die Anzahl der gezählten Webanforderungen.

Thema	Metrik	Beschreibung
AWS WAF	`PassedRequests`	Die Anzahl der übergeben en Anfragen. Dies wird nur für Anfragen verwendet, die einer Regelgruppenbewert ung unterzogen werden, ohne einer der Regelgruppenregeln zu entsprechen.
Amazon CloudFront	`Requests`	Die Anzahl der HTTP /S-Anfragen.
Amazon CloudFront	`TotalErrorRate`	Der Prozentsatz aller Anfragen, für die der HTTP Statuscode `4xx` oder lautet`5xx`.
Amazon Route 53	`HealthCheckStatus`	Der Status des Endpunkts für die Integritätsprüfung.
Application Load Balancer	`ActiveConnectionCo unt`	Die Gesamtzahl der gleichzei tigen TCP Verbindungen, die von Clients zum Load Balancer und vom Load Balancer zu Zielen aktiv sind.
Application Load Balancer	`ConsumedLCUs`	Die Anzahl der Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer verwendet werden.
Application Load Balancer	`HTTPCode_ELB_4XX_C ount HTTPCode_ ELB_5XX_Count`	Die Anzahl der vom HTTP `4xx` Load Balancer generierten `5xx` Client-Fehlercodes.

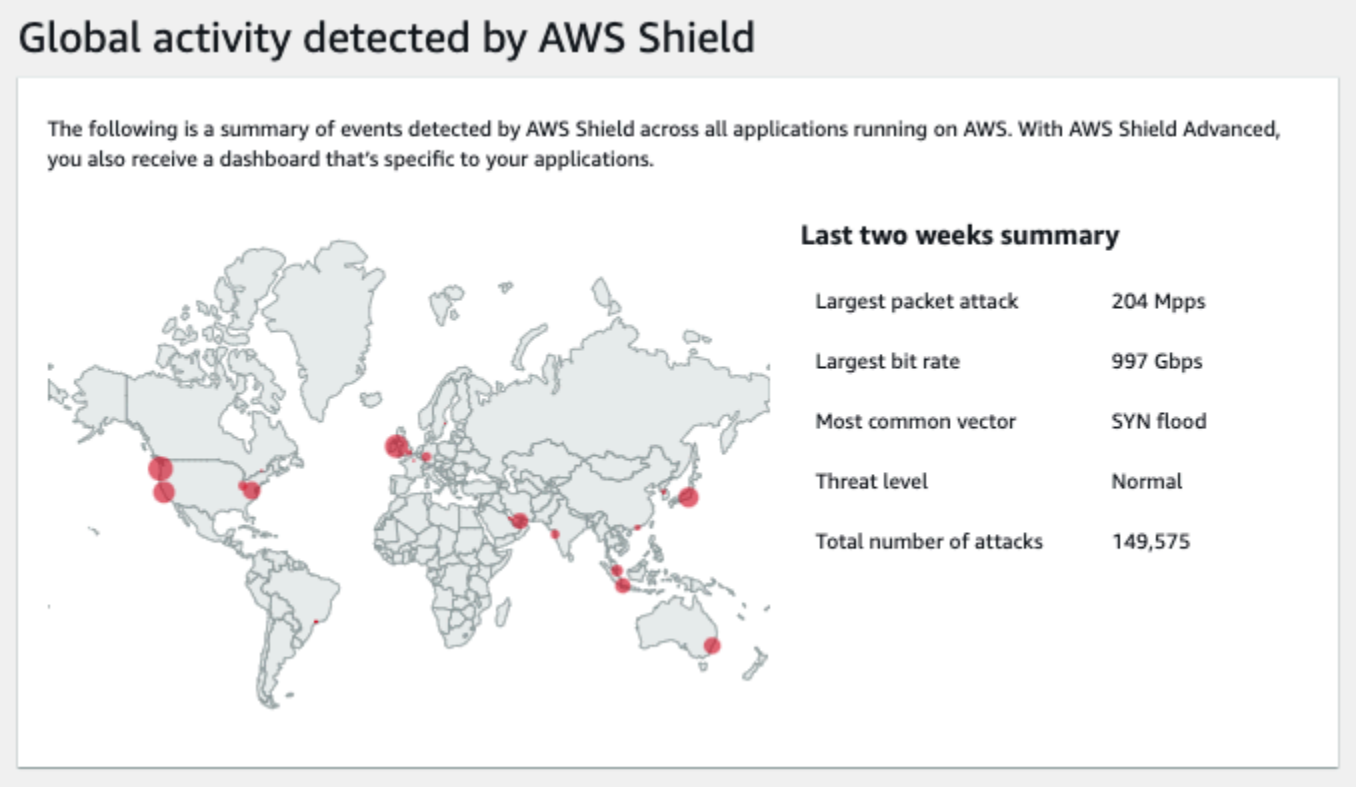
Thema	Metrik	Beschreibung
Application Load Balancer	`NewConnectionCount`	Die Gesamtzahl der neuen TCP Verbindungen, die von Clients zum Load Balancer und vom Load Balancer zu Zielen hergestellt wurden.
Application Load Balancer	`ProcessedBytes`	Die Gesamtzahl der vom Load Balancer verarbeiteten Bytes.
Application Load Balancer	`RejectedConnectionCount`	Anzahl der abgelehnten Verbindungen, weil der Load Balancer die maximale Anzahl an Verbindungen erreicht hat.
Application Load Balancer	`RequestCount`	Die Anzahl der Anfragen, die verarbeitet wurden.
Application Load Balancer	`TargetConnectionErrorCount`	Die Anzahl der Verbindungen, die zwischen dem Load Balancer und dem Ziel nicht erfolgreich hergestellt wurden.
Application Load Balancer	`TargetResponseTime`	Die verstrichene Zeit in Sekunden, nachdem die Anfrage den Load Balancer verlassen hat, bis eine Antwort vom Ziel eingeht.
Application Load Balancer	`UnHealthyHostCount`	Die Anzahl der als instabil betrachteten Ziele.
Network Load Balancer	`ActiveFlowCount`	Die Gesamtzahl der gleichzeitigen TCP Datenflüsse (oder Verbindungen) von Clients zu Zielen.

Thema	Metrik	Beschreibung
Network Load Balancer	`ConsumedLCUs`	Die Anzahl der Load Balancer-Kapazitätseinheiten (LCU), die von Ihrem Load Balancer verwendet werden.
Network Load Balancer	`NewFlowCount`	Die Gesamtzahl der neuen TCP Datenflüsse (oder Verbindungen), die innerhalb des Zeitraums von Clients zu Zielen hergestellt wurden.
Network Load Balancer	`ProcessedBytes`	Die Gesamtzahl der vom Load Balancer verarbeiteten Byte, einschließlich TCP /IP-Heade rn.
Global Accelerator	`NewFlowCount`	Die Gesamtzahl der neuen TCP UDP Datenflüsse (oder Verbindungen), die innerhalb des Zeitraums von Clients zu Endpunkten hergestellt wurden.
Global Accelerator	`ProcessedBytesIn`	Die Gesamtzahl der vom Accelerator verarbeiteten eingehenden Byte, einschlie ßlich TCP /IP-Headern.
Auto Scaling	`GroupMaxSize`	Die maximale Größe der Auto-Scaling-Gruppe.
Amazon EC2	`CPUUtilization`	Der Prozentsatz der zugewiesenen EC2 Rechenein heiten, die derzeit verwendet werden.

Thema	Metrik	Beschreibung
Amazon EC2	`NetworkIn`	Anzahl der von der Instance auf allen Netzwerkschnittstellen empfangenen Byte.

Weitere Informationen zur Verwendung von Amazon CloudWatch zur Erkennung von DDoS Angriffen auf Ihre Anwendung finden Sie unter Erste Schritte mit Amazon CloudWatch.

AWS enthält mehrere zusätzliche Metriken und Alarme, um Sie über einen Angriff zu informieren und Ihnen zu helfen, die Ressourcen Ihrer Anwendung zu überwachen. Die AWS Shield Konsole oder API bietet eine Zusammenfassung der Ereignisse pro Konto und Details zu den erkannten Angriffen.



Globale Aktivität erkannt von AWS Shield

Darüber hinaus bietet das Dashboard zur globalen Bedrohungsumgebung zusammenfassende Informationen über alle DDoS Angriffe, die von erkannt wurden AWS. Diese Informationen können nützlich sein, um die DDoS Bedrohungen für eine größere Anzahl von Anwendungen besser zu verstehen und um Angriffstrends zu ermitteln und sie mit Angriffen zu vergleichen, die Sie möglicherweise beobachtet haben.

Wenn Sie ein Abonnement abgeschlossen haben AWS Shield Advanced, zeigt das Service-Dashboard zusätzliche Erkennungs- und Abhilfemetriken sowie Details zum Netzwerkverkehr für Ereignisse an, die auf geschützten Ressourcen erkannt wurden. AWS Shield bewertet den Datenverkehr zu Ihrer geschützten Ressource anhand mehrerer Dimensionen. Wenn eine Anomalie erkannt wird, wird ein Ereignis AWS Shield erstellt und die Verkehrsdimension gemeldet, in der die Anomalie beobachtet wurde. Durch eine platzierte Risikominderung wird Ihre Ressource vor übermäßigem Datenverkehr und Datenverkehr geschützt, der einer bekannten DDoS Ereignissignatur entspricht.

Erkennungsmetriken basieren auf Stichproben von Netzwerkströmen oder AWS WAF Protokollen, wenn ein Web mit der geschützten Ressource verknüpft ACL ist. Die Messwerte zur Schadensbegrenzung basieren auf dem Datenverkehr, der von den Schutzsystemen von DDoS Shield beobachtet wird. Messwerte zur Schadensbegrenzung sind eine genauere Messung des Datenverkehrs in Ihre Ressource.

Die Metrik der wichtigsten Mitwirkenden im Netzwerk gibt Aufschluss darüber, woher der Verkehr während eines erkannten Ereignisses kommt. Sie können die Mitwirkenden mit dem höchsten Volumen anzeigen und nach Aspekten wie Protokoll, Quellport und TCP Flags sortieren. Die Metrik mit den meisten Mitwirkenden umfasst Metriken für den gesamten auf der Ressource beobachteten Traffic in verschiedenen Dimensionen. Sie bietet zusätzliche Metrikdimensionen, anhand derer Sie den Netzwerkverkehr verstehen können, der während eines Ereignisses an Ihre Ressource gesendet wird. Denken Sie daran, dass bei Angriffen auf Layer 3 oder 4 ohne Reflection die Quell-IP-Adressen möglicherweise gefälscht wurden und man sich nicht darauf verlassen kann.

Das Service-Dashboard enthält auch Details zu den Maßnahmen, die automatisch zur Abwehr von Angriffen ergriffen werden. DDoS Diese Informationen erleichtern es, Anomalien zu untersuchen, die Dimensionen des Datenverkehrs zu untersuchen und die Maßnahmen, die Shield Advanced zum Schutz Ihrer Verfügbarkeit ergriffen hat, besser zu verstehen.

Protokollierung

Aktivieren Sie die nützliche Protokollierung aller Dienste gemäß unserem Leitfaden zur Protokollierung und Überwachung für Anwendungsbesitzer, um die Transparenz zu maximieren und bei der Fehlerbehebung zu helfen. Dies beinhaltet, ist aber nicht beschränkt auf:

- AWS CloudTrail
- AWS WAF Protokolle
- CloudFrontZugriffsprotokolle

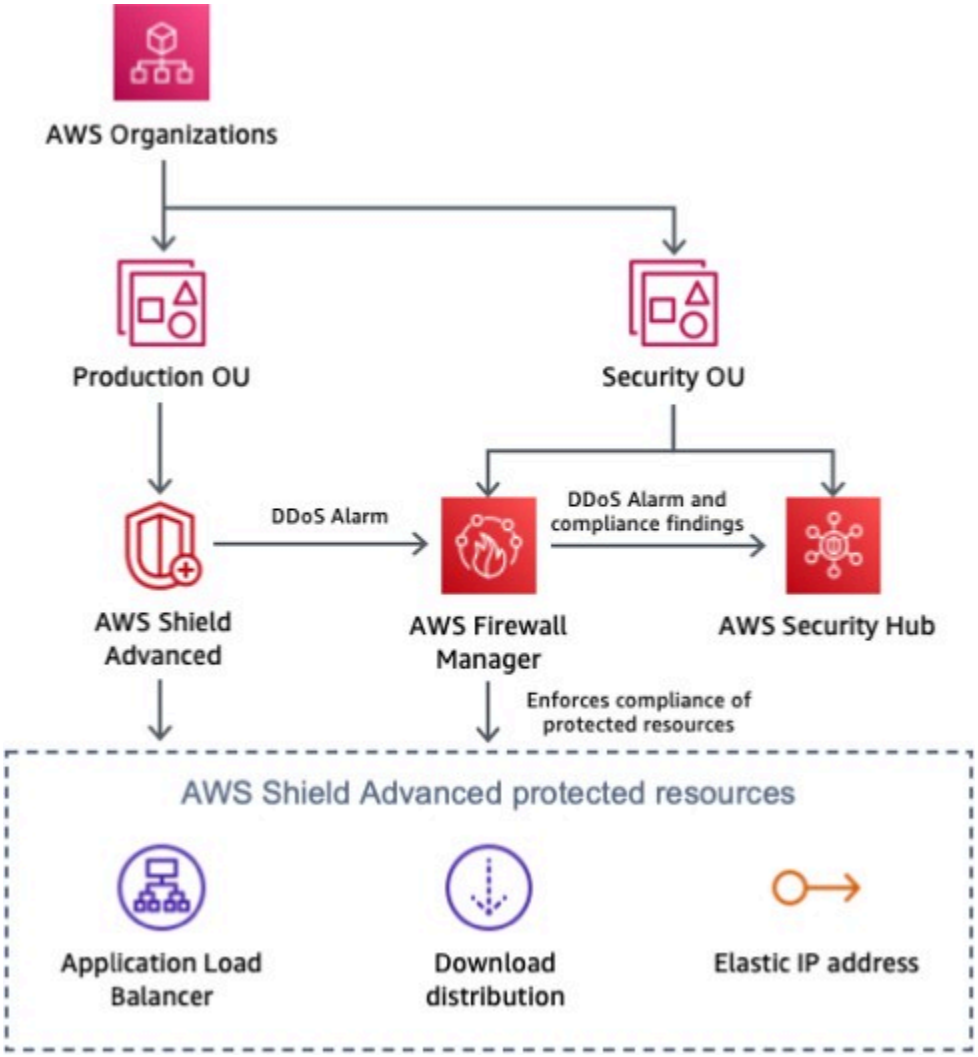
- VPCDatenflussprotokolle (siehe Netzwerkdatenverkehrsflüsse protokollieren und anzeigen) — Fügen Sie `tcp-flags` Felder in die enthaltenen Felder ein, um die Sichtbarkeit zu maximieren
- ELBZugriffsprotokolle (ALB, CLB, NLB)
- HTTPZugriffsprotokolle für Webserver
- Sicherheitsprotokollierung des Betriebssystems
- Protokollierung von Anwendungen

Verwaltung von Transparenz und Schutz für mehrere Konten

In Szenarien, in denen Sie mit mehreren Komponenten arbeiten AWS-Konten und mehrere Komponenten schützen müssen, erhöhen Sie Ihre Möglichkeiten zur Schadensbegrenzung durch den Einsatz von Techniken, die es Ihnen ermöglichen, in großem Umfang zu arbeiten und die Betriebskosten zu reduzieren. Wenn Sie AWS Shield Advanced geschützte Ressourcen in mehreren Konten verwalten, können Sie mithilfe von AWS Firewall Manager und AWS Security Hub eine zentrale Überwachung einrichten. Mit Firewall Manager können Sie eine Sicherheitsrichtlinie erstellen, die die Einhaltung der DDoS Schutzbestimmungen für alle Ihre Konten durchsetzt. Sie können diese beiden Dienste zusammen verwenden, um Ihre geschützten Ressourcen für mehrere Konten zu verwalten und die Überwachung dieser Ressourcen zu zentralisieren.

Security Hub lässt sich automatisch in Firewall Manager integrieren, sodass Shield Advanced-Kunden Sicherheitsergebnisse zusammen mit anderen Sicherheitswarnungen und Compliance-Status mit hoher Priorität in einem einzigen Dashboard einsehen können.

Wenn Shield Advanced beispielsweise anomalen Datenverkehr erkennt, der für eine geschützte Ressource AWS-Konto innerhalb des Bereichs bestimmt ist, wird dieser Befund in der Security Hub Hub-Konsole sichtbar. Falls konfiguriert, kann Firewall Manager die Ressource automatisch richtlinientreu machen, indem er sie als durch Shield Advanced geschützte Ressource erstellt und Security Hub aktualisiert, wenn sich die Ressource in einem konformen Zustand befindet.



Architekturdiagramm, das die Überwachung AWS Shield geschützter Ressourcen mit Firewall Manager und Security Hub zeigt

Weitere Informationen zur zentralen Überwachung von durch Shield geschützten Ressourcen finden Sie unter Zentrale Überwachung für DDoS Ereignisse einrichten und nicht konforme Ressourcen automatisch korrigieren.

Strategie und Runbooks zur Reaktion auf Vorfälle

Die Entwicklung einer Strategie zur Reaktion auf DDoS Angriffsvorfälle und der Aufbau eines darauf basierenden Prozesses zur Reaktion auf Sicherheitsvorfälle sind für alle Unternehmen von entscheidender Bedeutung. Ein empfohlener Ansatz besteht darin, Ihr Reaktionsprogramm auf der Grundlage der vorgeschlagenen Schritte wie dem Sammeln NIST von Beweisen, der Schadensbegrenzung, der Wiederherstellung und der Durchführung von Analysen nach einem

Vorfall zu erstellen. Als Beispiel wird ein Response-Playbook für DoS- oder DDoS Angriffe von Webanwendungen bereitgestellt. Zusätzliche Ressourcen sind im AWS Security Incident Response Guide verfügbar.

Support

Wenn Sie von einem Angriff betroffen sind, können Sie auch Unterstützung AWS bei der Bewertung der Bedrohung und der Überprüfung der Architektur Ihrer Anwendung in Anspruch nehmen oder weitere Unterstützung anfordern. Es ist wichtig, vor einem tatsächlichen Ereignis einen Reaktionsplan für DDoS Angriffe zu erstellen. Bei den in diesem paper beschriebenen bewährten Methoden handelt es sich um proaktive Maßnahmen, die Sie implementieren, bevor Sie eine Anwendung starten. DDoS Angriffe auf Ihre Anwendung können jedoch dennoch auftreten. Sehen Sie sich die Optionen in diesem Abschnitt an, um herauszufinden, welche Supportressourcen für Ihr Szenario am besten geeignet sind. Ihr Kundenbetreuungsteam kann Ihren Anwendungsfall und Ihre Anwendung bewerten und Ihnen bei spezifischen Fragen oder Problemen weiterhelfen.

Wenn Sie Produktionsworkloads ausführen, sollten Sie erwägen AWS, Business Support zu abonnieren, der Ihnen rund um die Uhr Zugriff auf Cloud-Supporttechniker bietet, die Ihnen bei DDoS Angriffsproblemen weiterhelfen können. Wenn Sie geschäftskritische Workloads ausführen, sollten Sie Enterprise Support in Betracht ziehen, der die Möglichkeit bietet, kritische Fälle zu öffnen und die schnellste Antwort von einem Senior Cloud Support Engineer zu erhalten.

Wenn Sie Business Support oder Enterprise Support abonniert haben AWS Shield Advanced und auch abonniert haben, können Sie Shield Proactive Engagement konfigurieren. Es ermöglicht Ihnen, Integritätsprüfungen zu konfigurieren, sie Ihren Ressourcen zuzuordnen und Kontaktinformationen für den Betrieb rund um die Uhr bereitzustellen. Wenn Shield Anzeichen einer Beeinträchtigung feststellt DDoS und die Integritätsprüfungen Ihrer Anwendung Anzeichen einer Verschlechterung aufweisen, AWS SRT wird es sich proaktiv mit Ihnen in Verbindung setzen. Dies ist unser empfohlenes Kooperationsmodell, da es die schnellsten AWS SRT Reaktionszeiten ermöglicht und es ermöglicht, mit der Fehlerbehebung AWS SRT zu beginnen, noch bevor Kontakt mit Ihnen aufgenommen wurde.

Weitere Informationen finden Sie unter Tarife vergleichen Support.

Für die proaktive Interaktion müssen Sie eine Route 53-Zustandsprüfung konfigurieren, die den Zustand Ihrer Anwendung genau misst und der durch Shield Advanced geschützten Ressource zugeordnet ist. Sobald eine Route 53-Zustandsprüfung in der Shield-Konsole verknüpft ist, verwendet das Shield Advanced-Erkennungssystem den Status der Integritätsprüfung als Indikator für den Zustand Ihrer Anwendung. Die zustandsbasierte Erkennungsfunktion in Shield Advanced stellt

sicher, dass Sie benachrichtigt werden und dass Schutzmaßnahmen schneller ergriffen werden, wenn Ihre Anwendung fehlerhaft ist. AWS SRTwird sich mit Ihnen in Verbindung setzen, um herauszufinden, ob die fehlerhafte Anwendung Ziel eines DDoS Angriffs ist, und um bei Bedarf zusätzliche Abhilfemaßnahmen zu ergreifen.

Der Abschluss der Konfiguration des proaktiven Engagements umfasst das Hinzufügen von Kontaktdaten in der Shield-Konsole. AWS SRTwird diese Informationen verwenden, um Sie zu kontaktieren. Sie können bis zu zehn Kontakte konfigurieren und zusätzliche Hinweise angeben, falls Sie spezielle Kontaktanforderungen oder -präferenzen haben. Proaktiv

Kontaktpersonen sollten rund um die Uhr besetzt sein, z. B. ein Security Operations Center oder eine Person, die sofort verfügbar ist.

Sie können proaktives Engagement für alle Ressourcen oder für ausgewählte wichtige Produktionsressourcen aktivieren, bei denen die Reaktionszeit entscheidend ist. Dies wird erreicht, indem nur diesen Ressourcen Zustandsprüfungen zugewiesen werden.

Sie können auch eskalieren, AWS SRT indem Sie über die Support Konsole (Anmeldung erforderlich) oder über den Support einen Support Fall erstellen, API wenn Sie ein DDoS verwandtes Ereignis haben, das die Verfügbarkeit Ihrer Anwendung beeinträchtigt.

Schlussfolgerung

Die in diesem paper beschriebenen Best Practices können Ihnen helfen, eine DDoS robuste Architektur aufzubauen, die die Verfügbarkeit Ihrer Anwendung schützt, indem sie viele gängige DDoS Angriffe auf Infrastruktur- und Anwendungsebene verhindert. Inwieweit Sie diese bewährten Methoden bei der Architektur Ihrer Anwendung befolgen, hat Einfluss auf die Art, den Vektor und das Volumen der DDoS Angriffe, die Sie abwehren können. Sie können Resilienz integrieren, ohne einen DDoS Abwehrservice abonnieren zu müssen. Wenn Sie sich für ein Abonnement entscheiden, erhalten AWS Shield Advanced Sie zusätzliche Funktionen für Support, Transparenz, Risikominderung und Kostenschutz, die eine bereits belastbare Anwendungsarchitektur weiter schützen.

Mitwirkende

Zu den Mitwirkenden an diesem Dokument gehören:

- Rodrigo Ferroni, Sicherheitsspezialist AWS TAM
- Dmitriy Novikov, Lösungsarchitekt AWS
- Achraf Souk, Lösungsarchitekt AWS
- Joanna Knox, Ingenieurwesen Support
- Anuj Butail, Lösungsarchitekt AWS
- Harith Gaddamanugu, Edge-Spezialist SA AWS

Weitere Informationen

Weitere Informationen finden Sie unter:

- Richtlinien für die Implementierung AWS WAF (AWS Whitepaper)
- NIS301 — Re:inForce 2023: Wie aus AWS Bedrohungsinformationen verwaltete Firewall-Regeln werden (Video) YouTube
- NET314- re:Invent 2022: Aufbau DDoS robuster Anwendungen mithilfe von (Video) AWS Shield YouTube
- SEC321- re:Invent 2020: Seien Sie mit den Eskalationen des DDoS Response Teams Ihrer Zeit immer einen Schritt voraus (Video) YouTube
- William Hill: Leistungsstarker DDoS Schutz mit AWS — 2020 (Video) YouTube
- SEC407 - re:Invent 2019: Ein defense-in-depth Ansatz zur Erstellung von Webanwendungen (Video) YouTube
- Bewährte Methoden zur DDoS Risikominderung am AWS — 2018 (Video) YouTube
- SID324— re:Invent 2017: Automatisierung der DDoS Reaktion in der Cloud (Video) YouTube
- CTD304 — re:Invent 2017: Die Reise von Dow Jones und dem Wall Street Journal zur Bewältigung von Verkehrsspitzen während der Fahrt (Video) YouTube
- Abwehr von Bedrohungen DDoS und Bedrohungen auf Anwendungsebene (Video) YouTube
- CTD310 — re:Invent 2017: Ein Leben am Netzwerkrand ist sicherer als Sie denken! Mit Amazon stark werden (YouTube Video)
- CloudFront AWS Shield, und AWS WAF (YouTube Video)

Dokumentversionen

Abonnieren Sie den Feed, um über Aktualisierungen dieses Whitepapers informiert zu werden. RSS

Änderung	Beschreibung	Datum
Aktualisierung des Whitepapers	OACFür Kostenschutz CloudFront und DNS Platzhalterschutz hinzugefügt. Ausführliche Erläuterung von Betriebstechniken, Caching, ratenbasierten Regeln und verwalteten Regelgruppen. Dem Architekturdiagramm wurden lokale Strukturen hinzugefügt, Duplikate wurden entfernt und der Text wurde klarer gefasst, um Unklarheiten zu beseitigen.	9. August 2023
Aktualisierung des Whitepapers	Aus Gründen der Übersichtlichkeit überarbeitet; aktualisiert mit den neuesten Empfehlungen und Funktionen: Verbindungsverfolgung von Sicherheitsgruppen und automatische DDoS Abwehr auf Anwendungsebene mit Shield Advanced.	13. April 2022
Aktualisierung des Whitepapers	Mit den neuesten Empfehlungen und Funktionen aktualisiert. AWS Global Accelerator wurde als Teil eines umfassenden Schutzes am Netzwerkrand hinzugefügt. AWS Firewall Manager für die zentrale Überwachung	21. September 2021

	von DDoS Ereignissen und die automatische Behebung nicht richtlinienkonformer Ressourcen.	
Aktualisierung des Whitepapers	Das Update wurde aktualisiert, um das Cache-Busting im Abschnitt Erkennung und Filterung bösartiger Webanfragen (BP1,BP2) ELB und die ALB Verwendung im Abschnitt Scale to Absorb (BP6) zu verdeutlichen. Die Diagramme und Tabelle 2 mit dem Vermerk „Wahl der Region“ wurden aktualisiert. alsBP8. Der BP7 Abschnitt wurde mit weiteren Details aktualisiert.	18. Dezember 2019
Aktualisierung des Whitepapers	Es wurde aktualisiert und beinhaltet nun auch die AWS WAF Protokollierung als bewährte Methode.	1. Dezember 2018
Aktualisierung des Whitepapers	Es wurde aktualisiert und umfasst AWS Shield nun AWS WAF AWS Firewall Manager Funktionen und verwandte bewährte Methoden.	1. Juni 2018
Aktualisierung des Whitepapers	Präskriptive Architekturrichtlinien wurden hinzugefügt und um weitere Informationen aktualisiert. AWS WAF	1. Juni 2016
Erste Veröffentlichung	Whitepaper veröffentlicht.	01. Juni 2015

Hinweise

Kunden sind dafür verantwortlich, Ihre eigene unabhängige Bewertung der Informationen in diesem Dokument vorzunehmen. Dieses Dokument: (a) dient nur zu Informationszwecken, (b) stellt aktuelle AWS Produktangebote und Praktiken dar, die ohne vorherige Ankündigung geändert werden können, und (c) stellt keine Verpflichtungen oder Zusicherungen von AWS und seinen verbundenen Unternehmen, Lieferanten oder Lizenzgebern dar. AWS Produkte oder Dienstleistungen werden „wie sie sind“ ohne ausdrückliche oder stillschweigende Garantien, Zusicherungen oder Bedingungen jeglicher Art bereitgestellt. Die Verantwortlichkeiten und Verbindlichkeiten AWS gegenüber seinen Kunden werden durch AWS Vereinbarungen geregelt, und dieses Dokument ist weder Teil einer Vereinbarung zwischen AWS und seinen Kunden noch ändert es diese.

AWS Glossar

Die neueste AWS Terminologie finden Sie im AWS Glossar in der AWS-Glossar Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.