Whitepaper zu AWS

AWS bewährte Methode für DDoS-Ausfallsicherheit

AWS bewährte Methode für DDoS-Ausfallsicherheit: Whitepaper zu AWS

Table of Contents

AWS Best Practices for DDoS Resiliency

Datum der Veröffentlichung: 21. September 2021 (Dokumentversionen)

Überblick

Es ist wichtig, Ihr Unternehmen vor den Auswirkungen von Distributed Denial of Service (DDoS) - Angriffen sowie anderen Cyberangriffen zu schützen. Das Vertrauen der Kunden in Ihren Service zu wahren, indem Sie die Verfügbarkeit und Reaktionsfähigkeit Ihrer Anwendung aufrechterhalten, hat hohe Priorität. Sie möchten auch unnötige direkte Kosten vermeiden, wenn Ihre Infrastruktur als Reaktion auf einen Angriff skaliert werden muss. Amazon Web Services (AWS) verpflichtet sich, Ihnen die Tools, bewährte Methoden und Services zur Verfügung zu stellen, mit denen Sie sich im Internet vor schlechten Akteuren schützen können. Durch die Verwendung der richtigen Services vonAWS können Sie Hochverfügbarkeit, Sicherheit und Ausfallsicherheit gewährleisten.

In diesem Whitepaper erhalten SieAWS eine präskriptive DDoS-Anleitung zur Verbesserung der Ausfallsicherheit von Anwendungen, die auf AWS ausgeführt werden. Dazu gehört eine DDoS-resistente Referenzarchitektur, die als Leitfaden zum Schutz der Anwendungsverfügbarkeit verwendet werden kann. In diesem Whitepaper werden auch verschiedene Angriffstypen beschrieben, z. B. Angriffe auf Infrastrukturebene und Angriffe auf Anwendungsebene. AWS erklärt, welche bewährten Methoden für die Verwaltung der einzelnen Angriffstypen am effektivsten sind. Darüber hinaus werden die Dienste und Funktionen beschrieben, die in eine DDoS-Abschwächungsstrategie passen, und es wird erläutert, wie jeder einzelne zum Schutz Ihrer Anwendungen verwendet werden kann.

Dieses Dokument richtet sich an IT-Entscheidungsträger und Sicherheitstechniker, die mit den grundlegenden Konzepten des Netzwerks, Sicherheit, und AWS vertraut sind. Jeder Abschnitt verfügt über Links zur AWS-Dokumentation, in der weitere Details zu den bewährten Methoden oder Funktionen zu finden sind.

Einführung: Denial-of-Service-Angriffe

Ein Denial of Service (DoS)-Angriff ist ein bewusster Versuch, eine Website oder Anwendung für Benutzer nicht verfügbar zu machen, z. B. indem sie mit Netzwerkverkehr überflutet wird. Angreifer verwenden eine Vielzahl von Techniken, die große Mengen an Netzwerkbandbreite verbrauchen oder andere Systemressourcen binden, wodurch der Zugriff für legitime Benutzer unterbrochen wird. In seiner einfachsten Form verwendet ein einzelner Angreifer eine einzige Quelle, um einen DoS-Angriff gegen ein Ziel durchzuführen, wie in der folgenden Abbildung gezeigt.

Tabelle 1: Diagramm eines DoS-Angriffs

Bei einem DDoS-Angriff verwendet ein Angreifer mehrere Quellen, um einen Angriff auf ein Ziel zu orchestrieren. Zu diesen Quellen können verteilte Gruppen von mit Malware infizierten Computern, Routern, IoT-Geräten und anderen Endpunkten gehören. Das folgende Diagramm zeigt ein Netzwerk kompromittierter Hosts, die an dem Angriff beteiligt sind und eine Flut von Paketen oder Anforderungen erzeugen, um das Ziel zu überfordern.

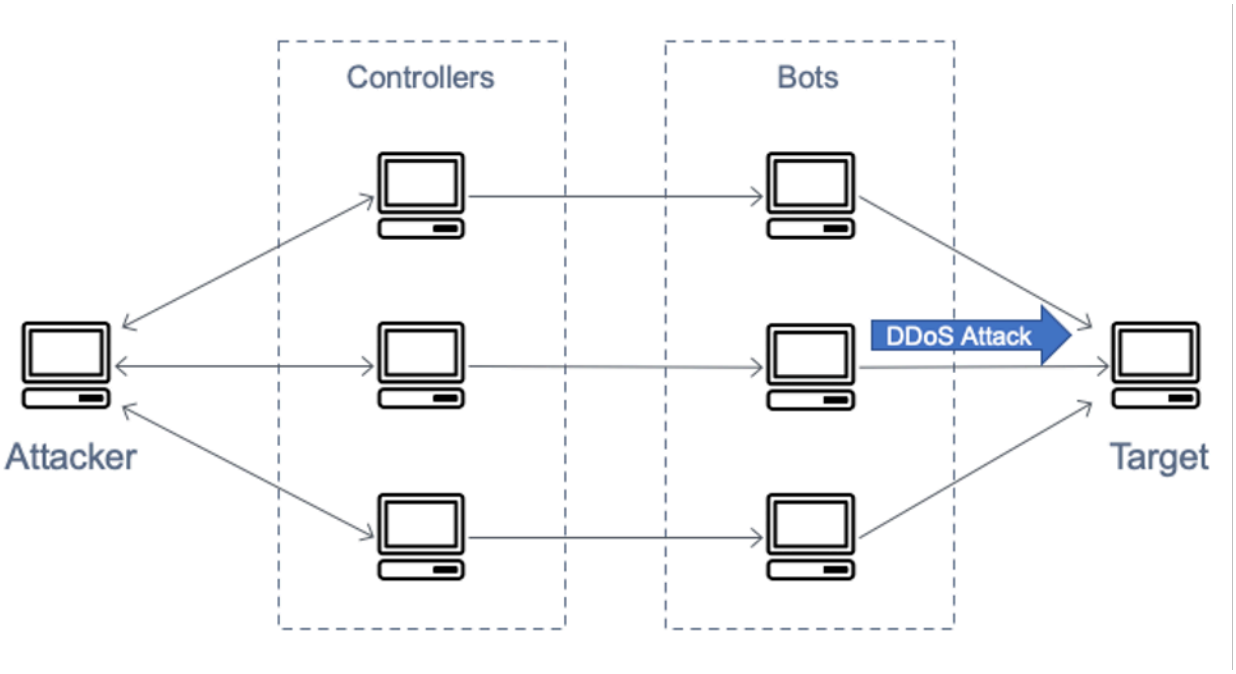

Diagramm eines DDoS-Angriffs

Das Open Systems Interconnection (OSI)-Modell besteht aus sieben Ebenen, die in der Tabelle des Open Systems Interconnection (OSI)-Modells beschrieben werden. DDoS-Angriffe treten am häufigsten auf den Ebenen drei, vier, sechs und sieben auf. Ebene-Drei- und Vier-Angriffe

entsprechen den Netzwerk- und Transportebenen des OSI-Modells. In diesem Dokument werden AWS zusammen als Angriffe auf Infrastrukturebene bezeichnet. Die Angriffe der Ebenen sechs und sieben entsprechen den Darstellungs- und Anwendungsebenen des OSI-Modells. AWSwird diese gemeinsam als Angriffe auf Anwendungsebene angehen. Beispiele für diese Angriffstypen werden in den folgenden Abschnitten erörtert.

OSI-Modell (Open Systems Interconnection)

#	Ebene	Einheit	Beschreibung	Vektorbeispiele
7	Anwendung	Daten	Netzwerkv erfahren zur Anwendung	HTTP-Floods, DNS-Abfrage-Floods
6	Darstellung	Daten	Darstellung und Verschlüsselung von Daten	TLS-Missbrauch
5	Sitzung	Daten	Kommunikation zwischen Hosts	k. A.
4	Transport	Segmente	Durchgängige Verbindungen und Zuverläss igkeit	SYN-Floods
3	Netzwerk	Pakete	Festlegung von Pfaden und logische Adresszuw eisung	UDP-Refle xionsangriffe
2	Data Link	Frames	Physische Adresszuw eisung	k. A.
1	Physisch	Bits	Medien-, Signal- und binäre Übertragung	k. A.

Themen

Angriffe auf die Infrastrukturebene

Die meisten DDoS-Angriffe – UDP-Reflexionsangriffe (User Datagram Protocol) und SYN-Floods (Synchronize-Floods) – erfolgen auf die Infrastrukturebene. Ein Angreifer kann eine dieser Methoden verwenden, um große Datenmengen zu generieren, die die Kapazität eines Netzwerks überschwemmen oder Ressourcen auf Systemen wie Servern, Firewalls, Intrusion Prevention System (IPS) oder Load Balancer binden können. Während diese Angriffe leicht zu identifizieren sind, müssen Sie über ein Netzwerk oder Systeme verfügen, die die Kapazität schneller als die Flut des eingehenden Datenverkehrs erhöhen, um sie effektiv abzuwehren. Diese zusätzliche Kapazität ist erforderlich, um den Angriffsverkehr herauszufiltern oder zu absorbieren, wodurch System und Anwendung auf legitimen Kundenverkehr reagieren können.

Themen

UDP-Reflexionsangriffe

Reflex-Angriffe des User Datagram Protocol (UDP) nutzen die Tatsache aus, dass UDP ein zustandsloses Protokoll ist. Angreifer können ein gültiges UDP-Anforderungspaket erstellen, in dem die IP-Adresse des Angriffsziels als UDP-Quell-IP-Adresse aufgeführt ist. Der Angreifer hat nun die Quell-IP des UDP-Anforderungspakets verfälscht oder 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 IP des Zielopfers 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 verstärkt wird.

Der Verstärkungsfaktor ist das Verhältnis von Antwortgröße zu Anforderungsgröße und hängt davon ab, welches Protokoll der Angreifer verwendet: DNS, NTP, SSDP, CLDAP, Memcached, CharGen oder QOTD. Beispielsweise kann der Verstärkungsfaktor für DNS das 28- bis 54-fache der ursprünglichen Byte-Anzahl betragen. Wenn ein Angreifer also eine Anforderungsnutzlast von

64 Byte an einen DNS-Server sendet, kann er über 3400 Byte unerwünschten Datenverkehr zu einem Angriffsziel generieren. UDP-Reflexionsangriffe sind im Vergleich zu anderen Angriffen für ein größeres Verkehrsaufkommen verantwortlich. Die Abbildung UDP Reflection Attack veranschaulicht die Reflexionstaktik und den Verstärkungseffekt.

UDP-Reflexionsangriff

SYN-Flood-Angriffe

Wenn ein Benutzer eine Verbindung zu einem TCP-Dienst (Transmission Control Protocol) herstellt, z. B. einem Webserver, sendet sein Client ein SYN-Synchronisationspaket. Der Server gibt ein SYN-ACK-Paket zur Bestätigung zurück, und schließlich antwortet der Client mit einem Bestätigungspaket (ACK), das den erwarteten Dreiwege-Handshake abschließt. Das folgende Bild veranschaulicht diesen typischen Handshake.

3-Way-Handshake (SYN)

Bei einem SYN-Flood-Angriff sendet ein böswilliger Client eine große Anzahl von SYN-Paketen, sendet jedoch niemals die endgültigen ACK-Pakete, um die Handshakes abzuschließen. Der Server wartet auf eine Antwort auf die halboffenen TCP-Verbindungen und hat schließlich keine Kapazität mehr, um neue TCP-Verbindungen zu akzeptieren. Dies kann verhindern, dass neue Benutzer eine Verbindung zum Server aufbauen. Der Angriff versucht, verfügbare Serververbindungen zu binden, sodass keine Ressourcen für legitime Verbindungen verfügbar sind. Während SYN-Floods bis zu Hunderte von Gbit/s erreichen können, besteht der Zweck des Angriffs nicht darin, das SYN-Traffic-Volumen zu erhöhen.

Angriffe auf die Anwendungsebene

Ein Angreifer kann auf die Anwendung selbst zielen, indem er einen Layer 7- oder Application-Layer-Angriff verwendet. Bei diesen Angriffen versucht der Angreifer, ähnlich wie bei Angriffen auf die SYN-Flood-Infrastruktur, bestimmte Funktionen einer Anwendung zu überlasten, damit die Anwendung nicht verfügbar ist oder für legitime Benutzer nicht mehr reagiert. Manchmal kann dies mit sehr geringen Anforderungsvolumina erreicht werden, die nur ein geringes Volumen an Netzwerkverkehr erzeugen. Damit wird der Angriff schwieriger zu erkennen und zu vermeiden. Beispiele für Angriffe auf die Anwendungsebene sind HTTP-Floods, Cache-Busting-Angriffe und XML-RPC-Floods in WordPress.

Bei einem HTTP-Flood-Angriff sendet der Angreifer HTTP-Anforderungen, die scheinbar von einem echten Benutzer der Webanwendung stammen. Einige HTTP-Floods zielen auf eine bestimmte Ressource ab, während komplexere HTTP-Floods versuchen, die menschliche Interaktion mit der Anwendung nachzuahmen. Damit kann es schwer werden, allgemeine Vermeidungstechniken wie die Einschränkung der Anforderungsrate einzusetzen.

Cache-Busting-Angriffe sind eine Art von HTTP-Flood, die Variationen in der Abfragezeichenfolge verwendet, um das Caching des Content Delivery Network (CDN) zu umgehen. Anstatt zwischengespeicherte Ergebnisse zurückgeben zu können, muss das CDN bei jeder Seitenanforderung den Original-Server kontaktieren, und diese Originalabrufe belasten den Anwendungswebserver zusätzlich.

Mit einem WordPress-XML-RPC-Flood-Angriff, auch als WordPress-Pingback-Flood bekannt, zielt ein Angreifer auf eine Website ab, die auf der WordPress-Content-Management-Software gehostet wird. Der Angreifer missbraucht die API-Funktion XML-RPC, um eine Flut von HTTP-Anfragen zu generieren. Mit der Pingback-Funktion kann eine auf WordPress gehostete Website (Website A) eine andere WordPress-Website (Website B) über einen Link benachrichtigen, dass Website A einen Link auf Website B erstellt hat. Daraufhin versucht Website B, Website A abzurufen, um das Vorhandensein des Links zu überprüfen. Bei einem Pingback-Flood missbraucht der Angreifer diese Funktion, damit Website B Website A angreift. Diese Art von Angriff hat eine eindeutige Signature: WordPress ist normalerweise im User-Agent des HTTP-Anforderungsheader vorhanden.

Es gibt andere Formen von bösartigem Datenverkehr, die sich auf die Verfügbarkeit einer Anwendung auswirken können. Scraper-Bots automatisieren Zugriffsversuche auf eine Webanwendung, um Inhalte zu stehlen oder Wettbewerbsinformationen wie die Preisgestaltung aufzuzeichnen. Brute-Force- und Credential Stuffing-Angriffe sind programmierte Maßnahmen, um unbefugten Zugriff auf sichere Bereiche einer Anwendung zu erhalten. Dies sind keine reinen DDoS-Angriffe; aber ihr automatisierter Charakter kann einem DDoS-Angriff ähneln und sie können durch die Implementierung einiger der gleichen Best Practices, die in diesem Dokument behandelt werden, abgewehrt werden.

Angriffe auf die Anwendungsebene können außerdem auf DNS-Services (Domain Name System) ausgerichtet sein. Bei den meisten Angriffen dieser Art handelt es sich um DNS-Abfrage-Floods, bei denen ein Angreifer viele wohlgeformte DNS-Abfragen nutzt, um die Ressourcen eines DNS-Servers zu überlasten. Solche Angriffe können auch eine Cache-Busting-Komponente enthalten, bei der der Angreifer die Zeichenfolge der Subdomain zufällig festlegt, um den lokalen DNS-Cache eines bestimmten Resolvers zu umgehen. Daher kann der Resolver die zwischengespeicherten

Domain-Abfragen nicht nutzen und muss stattdessen wiederholt den autorisierenden DNS-Server kontaktieren, was den Angriff verstärkt.

Wenn eine Webanwendung über Transport Layer Security (TLS) bereitgestellt wird, kann ein Angreifer auch den TLS-Verhandlungsprozess angreifen. TLS ist rechenaufwendig, sodass ein Angreifer, indem er zusätzliche Arbeitslast auf dem Server generiert, um unlesbare Daten (oder unverständliche (Geheimtext)) als legitimen Handshake zu verarbeiten, die Verfügbarkeit des Servers verringern kann. In einer Variante dieses Angriffs schließt ein Angreifer den TLS-Handshake ab, verhandelt jedoch ständig die Verschlüsselungsmethode neu. Ein Angreifer kann alternativ versuchen, Serverressourcen zu erschöpfen, indem er viele TLS-Sitzungen öffnet und schließt.

Techniken zur Risikovermeidung

Einige Formen der DDoS-Abwehr sind automatisch in den AWS-Diensten enthalten. Die DDoS-Ausfallsicherheit kann weiter verbessert werden, indem eineAWS-Architektur mit bestimmten 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.

Alle AWS-Kunden können ohne zusätzliche Kosten von den automatischen AWS Shield Standard-Schutzvorkehrungen profitieren. AWS Shield Standard schützt vor den häufigsten DDoS-Angriffen auf Netzwerk- und Transportebene, die auf Websites oder Anwendungen gerichtet sind. Dieser Schutz ist immer aktiviert, vorkonfiguriert, statisch und bietet keine Berichte oder Analysen. Es wird für alleAWS-Dienste und in jeder AWS-Region angeboten. In AWS-Regionen werden DDoS-Angriffe erkannt, und das Shield-Standard-System baut den Datenverkehr automatisch auf, erkennt Anomalien und sorgt bei Bedarf für Schutzmaßnahmen. Sie können AWS Shield Standard als Teil einer DDoS-resistenten Architektur verwenden, um sowohl Web- als auch Nicht-Webanwendungen zu schützen.

Sie können auch AWS-Services nutzen, die von Edge-Standorten aus betrieben werden, wie Amazon CloudFront, Global Accelerator und Route 53, um einen umfassenden Verfügbarkeitsschutz gegen alle bekannten Angriffe auf Infrastrukturebene aufzubauen. Diese Services sind Teil des AWS Global Edge Network und können die DDoS-Ausfallsicherheit Ihrer Anwendung verbessern, wenn sie jede Art von Anwendungsverkehr von Edge-Standorten auf der ganzen Welt bedienen. Sie können Ihre Anwendung in jeder AWS-Region ausführen und diese Services nutzen, um Ihre Anwendungsverfügbarkeit 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:

- Zugriff auf Internet und DDoS-Abwehrkapazitäten im gesamten AWS Global Edge Network. Dies ist nützlich, um Angriffe mit größerem Volumen abzuwehren, die die Terabit-Skala erreichen können.
- AWS Shield-DDoS-Abwehrsysteme sind inAWS-Edge-Dienste integriert, wodurch die Zeit bis zur Abwehr von Minuten auf Sekundenbruchteile reduziert wird.
- Zustandslose SYN-Flood-Abwehrtechniken arbeiten als Proxy und verifizieren eingehende Verbindungen, bevor sie an den geschützten Dienst weitergeleitet werden. Dadurch wird sichergestellt, dass nur gültige Verbindungen zu Ihrer Anwendung gelangen, während Ihre legitimen Endbenutzer vor Fehlalarmen geschützt werden.

- Automatische Traffic-Engineering-Systeme, die die Auswirkungen großer volumetrischer DDoS-Angriffe zerstreuen oder isolieren. Alle diese Dienste isolieren Angriffe an der Quelle, bevor sie Ihren Ursprung erreichen, was weniger Auswirkungen auf die durch diese Dienste geschützten Systeme bedeutet.
- Der Schutz auf der Anwendungsebene erfordert in Kombination mit AWS WAF keine Änderung der aktuellen Anwendungsarchitektur (z. B. in einer AWS-Region oder einem lokalen Rechenzentrum).

Die eingehende Datenübertragung auf AWS ist kostenlos und Sie zahlen nicht für den DDoS-Angriffsverkehr, der durch AWS Shield abgewehrt wird. Das folgende Architekturdiagramm umfasst AWS Global Edge Network-Services.

Diese Architektur umfasst mehrere AWS-Dienste, mit denen Sie die Widerstandsfähigkeit Ihrer Webanwendung gegen DDoS-Angriffe verbessern können. Die Tabelle Zusammenfassung der bewährten Methoden enthält eine Zusammenfassung dieser Services und der Funktionen, die sie bereitstellen können. AWS hat jeden Dienst mit einem Best-Practice-Indikator (BP1, BP2) versehen, um in diesem Dokument leichter darauf zugreifen zu können. In einem nächsten Abschnitt werden beispielsweise die Funktionen von Amazon CloudFront und Global Accelerator erörtert, die den Best-Practice-Indikator BP1 enthalten.

Tabelle 2 - Zusammenfassung der bewährten Methoden

AWS Edge	AWS Region					
	Verwenden von Amazon CloudFront (BP1) mit AWS WAF (BP2)	Verwenden von Global Accelerator (BP1)	Verwenden von Amazon Route 53 (BP3)	Verwenden von Elastic Load Balancing (BP6) mitAWS WAF (BP2)	Verwenden von Sicherheitsgruppen und Netzwerk-ACLs in Amazon VPC (BP5)	Verwenden von Amazon EC2 Auto Scaling (BP7)
Abwehr von	✓	✓	✓	✓	✓	✓

AWS Edge	AWS Region					
Ebene-3-Angriffen (z. B. UDP-Reflexion)						
Abwehr von Ebene-4-Angriffen (z. B. SYN-Flood)	✓	✓	✓	✓		
Abwehr von Ebene-6-Angriffen (z. B. TLS)	✓	✓	✓	✓		
Verringern der Angriffsfläche	✓	✓	✓	✓	✓	
Skalierung zum Abwehren von Datenverkehr auf der Anwendungsebene	✓	✓	✓	✓	✓	✓

AWS Edge	AWS Region					
Abwehr von Ebene-7-Angriffen (Anwendungsebene)	✓	✓(*)	✓	✓	✓(*)	✓(*)
Geografische Isolierung und Streuung von übermäßigem Datenverkehr und größeren DDoS-Angriffen	✓	✓	✓			
✓ (*): bei Verwendung von 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.

Kunden erhalten eine maßgeschneiderte Erkennung basierend auf:

- Spezifischen Verkehrsmustern Ihrer Anwendung.
- Schutz vor Ebene-7-DDoS-Angriffen, einschließlich AWS WAF ohne zusätzliche Kosten.
- Zugriff auf spezialisierten Support rund um die Uhr über das AWS SRT.
- Zentralisierte Verwaltung von Sicherheitsrichtlinien durch AWS Firewall Manager.
- Kostenschutz zum Schutz vor Skalierungsgebühren aufgrund von DDOS-bezogenen Nutzungsspitzen.

Dieser optionale DDoS-Abwehrservice schützt Anwendungen, die in jeder beliebigen AWS-Region gehostet werden. Der Dienst ist global verfügbar für CloudFront, Route 53 und Global Accelerator. Durch die Verwendung von Shield Advanced mit Elastic IP-Adressen können Sie Network Load Balancer (NLBs) oder Amazon EC2-Instances schützen.

Zu den Vorteilen der Verwendung von AWS Shield Advanced gehören:

- Zugriff auf AWS SRT zur Unterstützung bei der Abwehr von DDoS-Angriffen, die sich auf die Anwendungsverfügbarkeit auswirken.
- Sichtbarkeit von DDoS-Angriffen mithilfe der AWS Management Console-, API- und Amazon CloudWatch-Metriken und -Alarme.
- Zugriff auf den Verlauf aller DDoS-Ereignisse der letzten 13 Monate.
- Zugriff auf die AWS-Webanwendungs-Firewall (AWS WAF) ohne zusätzliche Kosten zur Abwehr von DDoS-Angriffen auf Anwendungsebene (bei Verwendung mit Amazon CloudFront oder Application Load Balancer).
- Automatisches Baselining von Web-Traffic-Attributen bei Verwendung mit AWS WAF.
- Zugriff auf AWS Firewall Manager, ohne zusätzliche Kosten, für automatisierte Durchsetzung von Richtlinien.
- Sensible Erkennungsschwellenwerte, die den Datenverkehr früher in das DDoS-Abwehrsystem leiten und die Zeit bis zur Abwehr von Angriffen auf Amazon EC2 oder Network Load Balancer verkürzen können, wenn sie mit einer Elastic IP-Adresse verwendet werden.
- Kostenschutz, mit dem Sie eine begrenzte Rückerstattung der skalierungsbezogenen Kosten beantragen können, die sich aus einem DDoS-Angriff ergeben.
- Erweitertes Service Level Agreement, das speziell auf AWS Shield Advanced-Kunden zugeschnitten ist.
- Proaktives Engagement von AWS SRT, wenn ein Shield-Ereignis erkannt wird.

- Schutzgruppen, die es Ihnen ermöglichen, Ressourcen zu bündeln und so den Umfang der Erkennung und Abwehr für Ihre Anwendung anzupassen, indem mehrere Ressourcen als eine Einheit behandelt werden. Die Gruppierung von Ressourcen verbessert die Erkennungsgenauigkeit, minimiert Fehlalarme, erleichtert den automatischen Schutz neu erstellter Ressourcen und beschleunigt die Abwehr von Angriffen auf viele Ressourcen, die eine einzige Anwendung umfassen. Informationen zu Schutzgruppen finden Sie unter Shield Advanced-Schutzgruppen.

Eine vollständige Liste der AWS Shield Advanced-Funktionen und weitere Informationen zu AWS Shield finden Sie unterAWS Shield Funktionsweise.

Themen

Bewährte Methoden für die DDoS-Abwehr

In den folgenden Abschnitten werden die empfohlenen bewährten Methoden für die DDoS-Abwehr ausführlicher beschrieben. Eine schnelle und einfach zu implementierende Anleitung zum Aufbau einer DDoS-Schutzschicht für statische oder dynamische Webanwendungen finden Sie unter How to Help Protect Dynamic Web Applications Against DDoS-Angriffe (Schutz dynamischer Webanwendungen vor DDoS-Angriffen).

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

In einer herkömmlichen Rechenzentrumsumgebung können Sie DDoS-Angriffe auf die Infrastrukturebene mit Techniken, wie dem Überbereitstellung von Kapazität, der Bereitstellung von DDoS-Abwehrsystemen oder dem Scrubbing von Datenverkehr mithilfe von DDoS-Abwehrdiensten abwehren. In AWS werden DDoS-Abwehrfunktionen automatisch bereitgestellt. Sie können jedoch die DDoS-Ausfallsicherheit Ihrer Anwendung optimieren, indem Sie Architekturentscheidungen treffen, die diese Funktionen am besten nutzen und es Ihnen ermöglichen, für übermäßigen Datenverkehr zu skalieren.

Zu den wichtigsten Überlegungen zur Abwehr volumetrischer DDoS-Angriffe gehören die Sicherstellung einer ausreichenden Transitkapazität und Vielfalt sowie der Schutz vonAWS-Ressourcen wie Amazon EC2-Instances vor Angriffsverkehr.

Einige Amazon EC2-Instance-Typen unterstützen Funktionen, die große Datenmengen einfacher verarbeiten können, z. B. Netzwerkbandbreitenschnittstellen mit bis zu 100 Gbit/s und erweitertes Netzwerk. Damit wird die Überlastung von Schnittstellen für jeglichen Datenverkehr vermieden, der an der Amazon EC2-Instance ankommt. Instances, die Enhanced Networking unterstützen, bieten im Vergleich zu herkömmlichen Implementierungen eine höhere I/O-Leistung, eine größere Bandbreite und eine niedrigere CPU-Auslastung. Dies verbessert die Fähigkeit der Instance, große Datenmengen zu verarbeiten, und macht sie letztendlich sehr widerstandsfähig gegen Pakete-pro-Sekunde (pps) Last.

Um diese hohe Ausfallsicherheit zu ermöglichen, empfiehlt AWS die Verwendung von Amazon EC2 Dedicated Instances oder Amazon EC2-Instances mit höherem Netzwerkdurchsatz, die ein N-Suffix haben und Unterstützung für Enhanced Networking mit bis zu 100 Gbit/s Netzwerkbandbreite, z. B. c6gn.16xlarge und c5n.18xlarge oder Metal Instances (wie c5n.metal) bieten.

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

Das für Enhanced Networking erforderliche Modul und der erforderliche enaSupport-Attributsatz sind in Amazon Linux 2 und den neuesten Versionen des Amazon Linux AMI enthalten. Wenn Sie daher eine Instance mit einer HVM-Version von Amazon Linux auf einem unterstützten Instance-Typ starten, ist Enhanced Networking für Ihre Instance bereits aktiviert. Weitere Informationen finden Sie unter Testen, ob erweiterte Netzwerke aktiviert sind. Weitere Informationen zum Aktivieren erweiterter Netzwerke finden Sie unter Erweitertes Netzwerk unter Linux.

Amazon EC2 mit Auto Scaling (BP7)

Eine weitere Möglichkeit, sowohl Infrastruktur- als auch Angriffe auf Anwendungsebene abzuwehren, ist der skalierbare Betrieb. Wenn Sie über Webanwendungen verfügen, können Sie Load Balancer (Lastenverteilung) verwenden, um den Datenverkehr auf eine Reihe von Amazon EC2-Instances zu verteilen, die übermäßig bereitgestellt oder für die automatische Skalierung konfiguriert sind. Diese Instanzen können plötzliche Verkehrsspitzen bewältigen, die aus irgendeinem Grund auftreten, einschließlich einer Flash-Menge oder eines DDoS-Angriffs auf Anwendungsebene. Sie können Amazon CloudWatch-Alarme so einrichten, dass Auto Scaling initiiert wird, um die Größe Ihrer Amazon EC2-Flotte als Reaktion auf Ereignisse, die Sie definieren, wie CPU, RAM, 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-Aushandlung über die Verteilung (Amazon

CloudFront) oder den Load Balancer. Diese Funktionen schützen Ihre Instances vor TLS-basierten Angriffen, indem sie für legitime Anfragen und TLS-Missbrauchsangriffe skaliert werden.

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

Amazon EC2 bietet 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.

Elastic Load Balancing (BP6)

Große DDoS-Angriffe können die Kapazität einer einzelnen Amazon EC2-Instance überfordern. Mit Elastic Load Balancer (ELB) können Sie das Risiko einer Überlastung der Anwendung reduzieren, da der Datenverkehr über viele Backend-Instances verteilt wird. Elastic Load Balancing kann automatisch skaliert werden, sodass Sie größere Volumes verwalten können, wenn Sie unerwarteten zusätzlichen Datenverkehr haben, z. B. aufgrund von Flash-Crowds oder DDoS-Angriffen. Für Anwendungen, die in einer Amazon VPC erstellt wurden, sind je nach Anwendungstyp drei Arten von ELBs zu berücksichtigen: Application Load Balancer (ALB), Classic Load Balancer (CLB) und Network Load Balancer (NLB).

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

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

Für TCP-basierte Anwendungen können Sie den Network Load Balancer verwenden, um Datenverkehr mit extrem niedriger Latenz an Ziele (z. B. Amazon EC2-Instances) weiterzuleiten. Eine wichtige Überlegung beim Network Load Balancer ist, dass jeder Datenverkehr, der den Load Balancer auf einem gültigen Listener erreicht, an Ihre Ziele weitergeleitet und nicht absorbiert

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

Weitere Informationen zum Schutz von TCP-Anwendungen mit dem Network Load Balancer finden Sie unter Erste Schritte mit Network Load Balancers

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

Der Zugriff auf hoch skalierte, vielfältige Internetverbindungen kann Ihre Fähigkeit erheblich verbessern, Latenz und Durchsatz für Benutzer zu optimieren, DDoS-Angriffe zu absorbieren und Fehler zu isolieren und gleichzeitig die Auswirkungen auf die Verfügbarkeit Ihrer Anwendung zu minimieren. 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, die von AWS-Regionen aus ausgeführt werden, umfassend schützen.

Bereitstellung von Webanwendungen am Edge (BP1)

Amazon CloudFront ist ein CDN-Service (Content Delivery Network), der die Bereitstellung Ihrer gesamten Website, einschließlich statischer, dynamischer, gestreamter und interaktiver Inhalte ermöglicht. Persistente Verbindungen und variable Time-to-Live (TTL) -Einstellungen können verwendet werden, um den Datenverkehr von Ihrem Ursprung zu entladen, auch wenn Sie keine cachbaren Inhalte bereitstellen. Die Verwendung dieser CloudFront-Funktionen reduziert die Anzahl der Anfragen und TCP-Verbindungen zurück zu Ihrem Ursprung und schützt so Ihre Webanwendung vor HTTP-Floods. CloudFront akzeptiert nur wohlgeformte Verbindungen und hilft damit zu verhindern, dass viele häufig auftretende DDoS-Angriffe wie SYN-Floods und UDP-Reflexionsangriffe Ihren Ursprungs-Server erreichen. DDoS-Angriffe werden außerdem in der Nähe der Quelle geografisch isoliert, sodass vermieden wird, dass der Datenverkehr Auswirkungen auf andere Standorte hat. Mit diesen Fähigkeiten haben Sie deutlich bessere Möglichkeiten, den Endbenutzern während großer DDoS-Angriffen weiterhin Datenverkehr bereitzustellen. Mit CloudFront können Sie einen Ursprungs-Server auf AWS oder an anderer Stelle im Internet schützen.

Wenn Sie Amazon S3 verwenden, um statische Inhalte im Internet bereitzustellen, empfiehlt AWS die Verwendung von Amazon CloudFront zum Schutz Ihres Buckets. Sie können Origin Access Identify (OAI) verwenden, um sicherzustellen, dass Benutzer nur mithilfe von CloudFront-URLs auf Ihre Objekte zugreifen.

Weitere Informationen zu OAI finden Sie unter Beschränken des Zugriffs auf Amazon S3-Inhalte mithilfe einer ursprünglichen Zugriffsidentität.

Weitere Informationen zum Schützen und Optimieren der Leistung von Webanwendungen mit Amazon CloudFront finden Sie unter Erste Schritte mit CloudFront.

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

Global Accelerator ist ein Netzwerkdienst, der die Verfügbarkeit und Leistung des Datenverkehrs der Benutzer um bis zu 60 % verbessert. Dies wird erreicht, indem der Datenverkehr an dem Edge-Standort, der Ihren Benutzern am nächsten liegt, eingespeist und über die AWS globale Netzwerkinfrastruktur an Ihre Anwendung weitergeleitet wird, unabhängig davon, ob diese in einer oder mehreren AWS-Regionen ausgeführt wird.

Global Accelerator leitet TCP- und UDP-Verkehr basierend auf der Leistung in der dem Benutzer nächstgelegenen AWS-Region zum optimalen Endpunkt weiter. Bei einem Anwendungsausfall bietet Global Accelerator innerhalb von 30 Sekunden ein Failover zum nächstbesten Endpunkt. Global Accelerator nutzt die enorme Kapazität des AWS globalen Netzwerks und Integrationen mit Shield, wie z. B. eine zustandslose SYN-Proxy-Funktion, die neue Verbindungsversuche in Frage stellt und nur legitimen Endbenutzern dient, um Anwendungen zu schützen.

Sie können eine ausfallsichere DDoS-Architektur implementieren, die viele der gleichen Vorteile wie die bewährten Methoden der Web Application-Bereitstellung am Edge bietet, auch wenn Ihre Anwendung Protokolle verwendet, die nicht von CloudFront unterstützt werden oder Sie eine Webanwendung betreiben, die globale statische IP-Adressen erfordert. Beispielsweise benötigen Sie möglicherweise IP-Adressen, die Ihre Endbenutzer der Zulassungsliste in ihren Firewalls hinzufügen können und die von keinem 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 mit AWS WAF, um auch Anforderungs-Flooding auf Webanwendungsebene zu erkennen

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

Domänennamensauflösung am Edge (BP3)

Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Service (Domain Name System), mit dem Datenverkehr auf eine Webanwendung weitergeleitet werden kann. Er enthält viele erweiterte

Funktionen wie Datenverkehrsfluss, latenzbasiertes Routing, Geo DNS, Zustandsprüfungen und Überwachung. Mit diesen erweiterten Funktionen können Sie steuern, wie der Dienst auf DNS-Anforderungen reagiert, um die Leistung Ihrer Webanwendung zu verbessern und Site-Ausfälle zu vermeiden.

Amazon Route 53 verwendet Techniken wie Shuffle-Sharding und Anycast-Striping, mit denen Benutzer auf Ihre Anwendung zugreifen können, selbst wenn der DNS-Dienst von einem DDoS-Angriff angegriffen wird.

Mithilfe von Shuffle Sharding entsprechen alle Namenserver im Delegationssatz einem eindeutigen Satz von Edge-Standorten und Internetpfaden. Dies sorgt für größere Fehlertoleranz und minimiert Überlappungen zwischen Kunden. Wenn ein einzelner Namenserver im Delegationssatz nicht verfügbar ist, können Endbenutzer einen erneuten Versuch starten und eine Antwort von einem anderen Namenserver an einem anderen Edge-Standort erhalten.

Mit Anycast-Striping kann jede DNS-Anforderung vom optimalsten Standort bedient werden, wodurch die Netzwerklast verteilt und die DNS-Latenz reduziert wird. Dies ermöglicht eine schnellere Reaktion für Benutzer. Außerdem kann Amazon Route 53 Anomalien in der Quelle und im Volume der DNS-Abfragen erkennen und Anforderungen von Benutzern priorisieren, die als zuverlässig gelten.

Weitere Informationen zur Weiterleitung von Endbenutzern zur Anwendung mit Amazon Route 53 finden Sie unter Erste Schritte mit Amazon Route 53.

Abwehr der Anwendungsebene (BP1, BP2)

Viele der bisher in diesem Dokument behandelten Techniken schützen wirksam gegen die Auswirkungen von DDoS-Angriffen auf Infrastrukturebene auf die Verfügbarkeit Ihrer Anwendung. Um sich auch vor Angriffen auf Anwendungsebene zu schützen, müssen Sie eine Architektur implementieren, mit der Sie böswillige Anfragen gezielt erkennen, skalieren, absorbieren und blockieren können. Hierbei handelt es sich um einen sehr wichtigen Aspekt, denn netzwerkbasierte Systeme zur Vermeidung von DDoS-Angriffen sind in der Regel unwirksam, wenn es gilt, komplexe Angriffe auf die Anwendungsebene zu verhindern.

Erkennen und Filtern von bösartigen Webanforderungen (BP1, BP2)

Wenn Ihre Anwendung ausgeführt wirdAWS, können Sie sowohl Amazon CloudFront als auch AWS WAF zur Abwehr von DDoS-Angriffen auf Anwendungsebene nutzen.

Mit Amazon CloudFront können Sie statischen Inhalt in den Cache stellen und von AWS-Edge-Standorten aus bereitstellen, womit die Last auf dem Ursprungs-Server möglicherweise reduziert

werden kann. Es kann auch dazu beitragen, die Serverlast zu reduzieren, indem verhindert wird, dass Datenverkehr außerhalb des Webs Ihren Ursprung erreicht. Außerdem kann CloudFront Verbindungen für langsam lesende oder langsame schreibende Angreifer (z. B. Slowloris) schließen.

Mithilfe von AWS WAF können Sie Listen zur Steuerung des Webzugriffs (Web ACLs) auf Ihren CloudFront-Verteilungen oder Application Load Balancers konfigurieren, um Anforderungen basierend auf Anforderungssignaturen zu filtern und zu blockieren. Jede Web-ACL besteht aus Regeln, die Sie so konfigurieren können, dass Sie eine Zeichenfolgenübereinstimmung oder Regex-Übereinstimmung mit einem oder mehreren Anforderungsattributen wie dem Uniform Resource Identifier (URI), der Abfragezeichenfolge, der HTTP-Methode oder dem Headerschlüssel erhalten. Darüber hinaus können Sie mithilfe von AWS WAF der ratenbasierten Regeln die IP-Adressen fehlerhafter Akteure automatisch blockieren, wenn Anforderungen, die einer Regel entsprechen, einen von Ihnen definierten Schwellenwert überschreiten.

Anfragen von anstößigen Client-IP-Adressen erhalten 403 Verboten-Fehlerantworten und bleiben gesperrt, bis die Anforderungsrate unter den Schwellenwert fällt. Dies ist nützlich, um HTTP-Flood-Angriffe abzuwehren, die als regulärer Webverkehr getarnt sind. Um Angriffe basierend auf der Reputation von IP-Adressen zu blockieren, können Sie Regeln mithilfe von IP-Übereinstimmungsbedingungen erstellen oder verwaltete Regeln verwenden, die von Verkäufern im AWS MarketplaceAWS WAF angeboten werden. AWS WAF bietet AWS Managed Rules direkt als Managed Service an, bei dem Sie IP-Reputationsregelgruppen auswählen können. Die Regelgruppe „Amazon IP Reputation List“ enthält Regeln, die auf interner Threat Intelligence von Amazon basieren. Dies ist hilfreich, wenn Sie IP-Adressen blockieren möchten, die typischerweise mit Bots oder anderen Bedrohungen verbunden sind. Die Regelgruppe „Anonymous IP List“ enthält Regeln für das Blockieren von Anfragen über Services, die die Verschleierung der Betrachteridentität ermöglichen. Dazu gehören Anfragen von VPNs, Proxys, Tor-Knoten und Cloud-Plattformen (einschließlich AWS). Mit AWS WAF und CloudFront können Sie auch geografische Einschränkungen festlegen, um Anfragen aus ausgewählten Ländern zu blockieren oder zuzulassen. Dies kann dazu beitragen, Angriffe von geografischen Orten zu blockieren, an denen Sie nicht erwarten, dass sie Benutzern dienen.

Um böswillige Anfragen zu identifizieren, überprüfen Sie die Protokolle Ihres Webservers oder verwenden Sie die Funktionen von AWS WAF für Protokollierung und Stichprobenanfragen. Wenn Sie die AWS WAF-Protokollierung aktivieren, erhalten Sie detaillierte Informationen über den von der Web ACL analysierten Datenverkehr. AWS WAF unterstützt die Protokollfilterung, sodass Sie angeben können, welche Webanforderungen protokolliert werden und welche Anforderungen nach der Überprüfung aus dem Protokoll verworfen werden.

Zu den in den Protokollen aufgezeichneten Informationen gehören die Zeit, zu der AWS WAF die Anforderung von Ihrer AWS-Ressource empfangen hat, detaillierte Informationen über die Anforderung und die Übereinstimmungsaktion für jede angeforderte Regel. In die Stichprobe einbezogene Anfragen enthalten Details zu Anfragen innerhalb der letzten drei Stunden, die einer Ihrer AWS WAF-Regeln entsprachen. Sie können diese Informationen verwenden, um potenziell böswillige Verkehrssignaturen zu identifizieren und eine neue Regel zu erstellen, um diese Anforderungen abzulehnen. Wenn Sie eine Reihe von Anforderungen mit einer zufälligen Abfragezeichenfolge sehen, müssen Sie nur die Abfragezeichenfolgenparameter zulassen, die für den Cache für Ihre Anwendung relevant sind. Diese Methode ist bei der Abwehr eines Cache-Busting-Angriffs auf Ihren Ursprungs-Server hilfreich.

Wenn Sie ein AWS Shield Advanced-Abonnement haben, können Sie das AWS Shield Response Team (SRT) beauftragen, Regeln zu erstellen, um einen Angriff zu verhindern, der die Verfügbarkeit Ihrer Anwendung beeinträchtigt. Sie können AWS SRT eingeschränkten Zugriff auf Shield Advanced und AWS WAF-APIs Ihres Kontos gewähren. AWS SRT greift nur mit Ihrer ausdrücklichen Genehmigung auf diese APIs zu, um Schutzmaßnahmen für Ihr Konto vorzunehmen. Weitere Informationen finden Sie im Abschnitt Support dieses Dokuments.

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

Weitere Informationen zu:

- AWS Managed Rules for AWS WAF finden Sie unter AWS Managed Rules for AWS WAF.
- Weitere Informationen zur Einschränkung des Zugriffs auf die Amazon CloudFront-Verteilung mit Geo-Restriction finden Sie unter Einschränken der geografischen Verteilung von Inhalten.
- Verwenden Sie AWS WAF, um folgende Informationen zu erhalten:
  - Erste Schritte mit AWS WAF
  - Protokollieren von Web-ACL-Traffic-Informationen
  - Anzeigen einer Stichprobe von Webanforderungen
- Informationen zum Konfigurieren ratenbasierter Regeln finden Sie unter Schützen von Websites und Diensten mithilfe ratenbasierter Regeln für AWS WAF

- Wie Sie die Bereitstellung vonAWS WAF Regeln über IhreAWS Ressourcen hinweg mit Firewall Manager verwalten, finden Sie unter
  - Erste Schritte mit denAWS WAF Richtlinien von Firewall Manager.
  - Erste Schritte mit erweiterten Richtlinien von Firewall Manager Shield.

Verringern der Angriffsfläche

Ein weiterer wichtiger Aspekt, der bei der Entwicklung einer AWS-Lösung beachtet werden muss, ist die Einschränkung der Gelegenheiten, mit denen ein Angreifer auf Ihre Anwendung abzielen kann. Dieses Konzept wird als Verringern der Angriffsfläche bezeichnet. Ressourcen, die nicht mit dem Internet verbunden sind, sind schwerer anzugreifen. Damit reduzieren sich die Möglichkeiten, dass ein Angreifer auf die Verfügbarkeit Ihrer Anwendung abzielen kann.

Wenn Sie z. B. nicht erwarten, dass Benutzer direkt mit bestimmten Ressourcen interagieren, sollten Sie sicherstellen, dass nicht über das Internet auf diese Ressourcen zugegriffen werden kann. Akzeptieren Sie ebenfalls keinen Datenverkehr von Benutzern oder externen Anwendungen über Ports oder Protokolle, die für die Kommunikation nicht erforderlich sind.

Im folgenden Abschnitt stellt AWS bewährte Methoden bereit, die Sie bei der Reduzierung Ihrer Angriffsfläche und der Begrenzung der Internetpräsenz Ihrer Anwendung unterstützen.

Themen

Verschleiern von AWS-Ressourcen (BP1, BP4, BP5)

In der Regel können Benutzer eine Anwendung schnell und einfach verwenden, ohne dass AWS-Ressourcen vollständig dem Internet zugänglich sein müssen. Wenn Sie beispielsweise Amazon-EC2-Instances hinter einem Elastic Load Balancing haben, müssen die Instances selbst möglicherweise nicht öffentlich zugänglich sein. Stattdessen könnten Sie Benutzern Zugriff auf den Elastic Load Balancing an bestimmten TCP-Ports gewähren und nur Elastic Load Balancing mit den Instances kommunizieren lassen. Sie können das einrichten, indem Sie Sicherheitsgruppen und Netzwerk-Zugriffskontrolllisten (NACLs) innerhalb der Amazon Virtual Private Cloud (Amazon VPC) konfigurieren. Mit Amazon VPC können Sie einen logisch isolierten Abschnitt der AWS Cloud bereitstellen, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.

Sicherheitsgruppen und Netzwerk-ACLs sind insofern ähnlich, als dass Sie mit beiden den Zugriff auf AWS-Ressourcen innerhalb Ihrer VPC steuern können. Mit Sicherheitsgruppen können Sie jedoch den ein- und ausgehenden Datenverkehr auf Instance-Ebene steuern, während Netzwerk-ACLs ähnliche Funktionen auf der Ebene des VPC-Subnetzes bieten. Für die Verwendung von Sicherheitsgruppen oder Netzwerk-ACLs fallen keine zusätzlichen Gebühren an.

Sicherheitsgruppen und Netzwerk-Zugriffskontrolllisten (Netzwerk-ACLs) (BP5)

Sie können wählen, ob Sie beim Starten einer Instance Sicherheitsgruppen angeben oder die Instance zu einem späteren Zeitpunkt einer Sicherheitsgruppe zuordnen möchten. Wenn Sie keine Regel zum Erlauben erstellt haben, die den Datenverkehr zulässt, wird der gesamte Internetverkehr zu einer Sicherheitsgruppe implizit abgelehnt. Wenn Sie beispielsweise eine Webanwendung haben, die einen Elastic Load Balancing und mehrere Amazon-EC2-Instances verwendet, können Sie eine Sicherheitsgruppe für den Elastic Load Balancing (Sicherheitsgruppe Elastic Load Balancing) und eine für die Instances (Sicherheitsgruppe des Webanwendungsservers) erstellen. Dann können Sie eine Regel zum Erlauben des Internetverkehrs zur ELB-Sicherheitsgruppe und eine weitere Regel zum Erlauben des Verkehrs von der ELB-Sicherheitsgruppe zur Sicherheitsgruppe des Webanwendungsservers zuzulassen. Damit wird sichergestellt, dass Internetverkehr nicht direkt mit Ihren Amazon-E2-Instances kommunizieren kann; damit wird es für einen Angreifer schwieriger, Informationen über Ihre Anwendung zu erhalten und diese zu beinflussen.

Wenn Sie Netzwerk-ACLs erstellen, können Sie sowohl Regeln zum Erlauben als auch zum Ablehnen einrichten. Das ist hilfreich, wenn Sie bestimmte Arten von Datenverkehr zu Ihrer Anwendung explizit ablehnen möchten. So können Sie z. B. IP-Adressen (als CIDR-Bereich), Protokolle und Zielports definieren, die für das gesamte Subnetz abgelehnt werden. Wenn Ihre Anwendung nur für TCP-Datenverkehr verwendet wird, können Sie eine Regel zum Ablehnen des gesamten UDP-Datenverkehrs oder umgekehrt erstellen. Diese Option ist nützlich, wenn Sie auf DDoS-Angriffe reagieren, da Sie damit Ihre eigenen Regeln erstellen können, um den Angriff zu verhindern, wenn Sie die Quell-IPs oder andere Signaturen kennen.

Wenn Sie AWS Shield Advanced abonniert haben, können Sie elastische IP-Adressen als geschützte Ressourcen registrieren. DDoS-Angriffe auf elastische 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 die Netzwerk-ACL, die der angestrebten elastischen IP entspricht, und setzen sie an der AWS-Netzwerkgrenze durch. Dies reduziert das Risiko einer Auswirkung durch eine Reihe von DDoS-Angriffen auf Infrastrukturebene erheblich.

Weitere Informationen zum Konfigurieren von Sicherheitsgruppen und Netzwerk-ACLs zur Optimierung der DDoS-Ausfallsicherheit finden Sie unter Wie Sie sich auf DDoS-Angriffe vorbereiten können, indem Sie Ihre Angriffsfläche verkleinern.

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

Schutz des Ursprungs-Servers (BP1, BP5)

Wenn Sie Amazon CloudFront mit einem Ursprung verwenden, der sich in Ihrer VPC befindet, sollten Sie sicherstellen, dass nur Ihre CloudFront-Verteilung Anforderungen an Ihren Ursprung weiterleiten kann. Mit Edge-to-Origin-Anforderungsheaders können Sie den Wert vorhandener Anforderungsheaders hinzufügen oder überschreiben, wenn CloudFront Anforderungen an Ihren Ursprungs-Server weiterleitet. Sie können die benutzerdefinierten Origin-Header verwenden, zum Beispiel den X-Shared-Secret-Header, um zu überprüfen, ob die an Ihren Ursprung gestellten Anforderungen von CloudFront gesendet wurden.

Weitere Informationen zum Schutz Ihres Ursprungs mit benutzerdefinierten Origin-Headern finden Sie unter Hinzufügen von benutzerdefinierten Headern zu Origin-Requests und Beschränken des Zugriffs auf Application Load Balancer.

Eine Anleitung zur Implementierung einer Beispiellösung, um den Wert von benutzerdefinierten Origin-Headern für die ursprüngliche Zugriffsbeschränkung automatisch zu rotieren, finden Sie unter So verbessern Sie die Amazon CloudFront-Ursprung-Sicherheit mit AWS WAF und Secrets Manager.

Alternativ können Sie eine AWS Lambda-Funktion verwenden, um Ihre Sicherheitsgruppenregeln automatisch zu aktualisieren, sodass nur CloudFront-Datenverkehr zulässig ist. Dies verbessert die Sicherheit Ihres AWS WAF Ursprungs, indem sichergestellt wird, dass böswillige Benutzer CloudFront und den Zugriff auf Ihre Webanwendung nicht umgehen können.

Weitere Informationen darüber, wie Sie Ihren Ursprung schützen können, indem Sie Ihre Sicherheitsgruppen automatisch aktualisieren, finden Sie unter X-Shared-Secret-Header, siehe Wie Sie Ihre Sicherheitsgruppen für Amazon CloudFront und AWS WAF mit AWS Lambda automatisch aktualisieren.

Schutz von API-Endpunkten (BP4)

Wenn Sie eine API der Öffentlichkeit zugänglich machen müssen, besteht normalerweise das Risiko, dass das API-Frontend von einem DDoS-Angriff angegriffen wird. Um das Risiko zu reduzieren, können Sie Amazon API Gateway als Zugang zu Anwendungen verwenden, die auf Amazon EC2, AWS Lambda oder anderswo ausgeführt werden. Wenn Sie Amazon API Gateway verwenden, 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 von einem DDoS-Angriff angegriffen werden.

Wenn Sie Amazon API Gateway verwenden, können Sie aus zwei Arten von API-Endpunkten wählen. Die erste ist die Standardoption: Edge-optimierte API-Endpunkte, auf die über eine Amazon CloudFront-Verteilung zugegriffen wird. Die Distribution 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 derselben AWS-Region aus zugegriffen wird, in der Ihre REST-API bereitgestellt wird. AWS empfiehlt, den zweiten Endpunkttyp zu verwenden und ihn Ihrer eigenen Amazon CloudFront-Verteilung zuzuordnen. Auf diese Weise haben Sie die Kontrolle über die Amazon CloudFront-Verteilung und Sie können AWS WAF für den Schutz der Anwendungsebene verwenden. Dieser Modus bietet Ihnen Zugriff auf skalierte DDoS-Abwehrkapazitäten imAWS globalen Edge-Netzwerk.

Konfigurieren Sie bei der Verwendung von Amazon CloudFront und AWS WAF mit Amazon API Gateway die folgenden Optionen:

- Konfigurieren Sie das Cache-Verhalten für Ihre Verteilungen, um alle Header an den regionalen Endpunkt des API Gateway weiterzuleiten. Auf diese Weise behandelt CloudFront den Inhalt dynamisch und überspringt das Zwischenspeichern des Inhalts.
- Schützen Sie Ihr API-Gateway vor direktem Zugriff, indem Sie die Verteilung so konfigurieren, dass sie den ursprünglichen benutzerdefinierten Header enthält`x-api-key`, indem Sie den API-Schlüsselwert in API Gateway festlegen.
- Schützen Sie Ihr Backend vor übermäßigem Datenverkehr, indem Sie dazu für alle Methoden in Ihren REST-APIs standardmäßige oder auf Durchsatzraten basierende Einschränkungen konfigurieren.

Weitere Informationen zum Erstellen von APIs mit Amazon API Gateway finden Sie unter Erste Schritte mit Amazon API Gateway.

Betriebliche Techniken

Mit den in diesem Artikel beschriebenen Schutzmaßnahmen können Sie Architekturen für Anwendungen erstellen, die grundsätzlich ausfallsicher gegen DDoS-Angriffe sind. In vielen Fällen ist es auch nützlich zu wissen, wann ein DDoS-Angriff auf Ihre Anwendung abzielt, damit Sie Schutzmaßnahmen ergreifen können. In diesem Abschnitt werden die bewährten Methoden für mehr Transparenz bei anormalem Verhalten, für Warnungen und Automatisierung, leistungsstarkem Schutz und für die Nutzung von AWS AWS für zusätzlichen Support erläutert.

Themen

Sichtbarkeit

Wenn eine wichtige Betriebsmetrik erheblich vom erwarteten Wert abweicht, versucht ein Angreifer möglicherweise, die Verfügbarkeit Ihrer Anwendung anzuvisieren. Wenn Sie mit dem normalen Verhalten Ihrer Anwendung vertraut sind, können Sie schneller Maßnahmen ergreifen, wenn Sie eine Anomalie feststellen. Amazon CloudWatch kann helfen, indem es Anwendungen überwacht, auf denen Sie ausgeführtAWS werden. Sie können z. B. mit Metriken erfassen und nachverfolgen, Protokolldateien sammeln und überwachen, Alarme festlegen und auf Änderungen in den AWS-Ressourcen automatisch reagieren.

Wenn Sie bei der Architektur Ihrer Anwendung der DDoS-resistenten Referenzarchitektur folgen, werden Angriffe auf die gesamte Infrastrukturebene blockiert, bevor Sie Ihre Anwendung erreichen. Wenn Sie AWS Shield Advanced abonniert haben, haben Sie Zugriff auf eine Reihe von CloudWatch-Metriken, die darauf hinweisen können, dass Ihre Anwendung als Ziel ausgewählt wird. Sie können beispielsweise Alarme konfigurieren, um Sie zu benachrichtigen, wenn ein DDoS-Angriff im Gange ist, sodass Sie den Zustand Ihrer Anwendung überprüfen und entscheiden können, ob Sie AWS SRT einsetzen möchten. Sie können die`DDoSDetected`Metrik so konfigurieren, dass Sie darüber informiert werden, ob ein Angriff erkannt wurde. Wenn Sie basierend auf dem Angriffsvolumen benachrichtigt werden möchten, können Sie auch die `DDoSAttackBitsPerSecond`-, `DDoSAttackPacketsPerSecond`- oder `DDoSAttackRequestsPerSecond`-Metriken verwenden. Sie können diese Metriken überwachen, indem Sie CloudWatch in Ihre eigenen Tools integrieren oder Tools verwenden, die von Dritten wie Slack oder PagerDuty bereitgestellt werden.

Ein Angriff auf Anwendungsebene kann viele Amazon CloudWatch-Metriken erhöhen. Wenn Sie AWS WAF verwenden, können Sie CloudWatch nutzen, um Alarme zu überwachen und zu aktivieren, wenn die Anforderungen, die Sie als zulässig, gezählt oder gesperrt festgelegt haben, zunehmen.AWS WAF Auf diese Weise erhalten Sie eine Benachrichtigung, wenn der Datenverkehr die Anforderungen Ihrer Anwendung übersteigt. Sie können auch Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, Amazon EC2 und Auto Scaling-Metriken verwenden, die in CloudWatch verfolgt werden, um Änderungen zu erkennen, die auf einen DDoS-Angriff hinweisen können.

In der Tabelle Empfohlene CloudWatch-Metriken werden Beschreibungen der CloudWatch-Metriken aufgeführt, die häufig zur Erkennung und Reaktion auf DDoS-Angriffe verwendet werden.

Tabelle 3 - Empfohlene Amazon CloudWatch-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-Ereignisses für einen bestimmten ARN beobachtet wurden. Diese Metrik ist nur für Ebene-3/4-DDoS-Ereignisse verfügbar.
AWS Shield Advanced	DDoSAttackPacketsPerSecond	Die Anzahl der Pakete, die während eines DDoS-Ereignisses für einen bestimmten ARN beobachtet wurden. Diese Metrik ist nur für Ebene-3/4-DDoS-Ereignisse verfügbar.
AWS Shield Advanced	DDoSAttackRequestsPerSecond	Die Anzahl der Anforderungen, die während eines

Thema	Metrik	Beschreibung
		DDoS-Ereignisses für einen bestimmten ARN beobachte t wurden. Diese Metrik ist nur für Ebene-7-DDoS-Ereignisse verfügbar und wird nur für die wichtigsten Ebene-7-E reignisse 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.
AWS WAF	PassedRequests	Die Anzahl der übergebenen Anfragen. Dies wird nur für Anforderungen verwendet, die eine Regelgruppenauswer tung durchlaufen, ohne mit einer der Regelgruppenregeln übereinzustimmen.
Amazon CloudFront	Requests	Die Anzahl der HTTP/S-An forderungen
Amazon CloudFront	TotalErrorRate	Der Prozentsatz aller Anforderungen mit dem HTTP-Status code 4xx oder 5xx
Amazon Route 53	HealthCheckStatus	Der Status des Zustandsp rüfungs-Endpunkts.

Thema	Metrik	Beschreibung
Application Load Balancer	ActiveConnectionCount	Gesamtanzahl gleichzei tiger TCP-Verbindungen die zwischen Clients und Lastenverteilung sowie zwischen Lastenverteilung und Zielen aktiv sind.
Application Load Balancer	ConsumedLCUs	Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrer Lastenverteilung verwendet werden.
Application Load Balancer	HTTPCode_ELB_4XX_Count HTTPCode_ELB_5XX_Count	Die Anzahl der von der Lastenverteilung generiert en HTTP 4xx- oder 5xx-Clien tfehlercodes
Application Load Balancer	NewConnectionCount	Gesamtanzahl neuer TCP-Verbindungen, die zwischen Clients und Lastenverteilung und zwischen Lastenverteilung und Zielen hergestellt wurden.
Application Load Balancer	ProcessedBytes	Gesamtanzahl der von einer Lastenverteilung über IPv6 verarbeiteten Byte.
Application Load Balancer	RejectedConnectionCount	Anzahl der abgelehnten Verbindungen, weil die Lastenverteilung die maximale Anzahl an Verbindungen erreicht hat.
Application Load Balancer	RequestCount	Die Anzahl der Anfragen, die bearbeitet wurden.

Thema	Metrik	Beschreibung
Application Load Balancer	TargetConnectionErrorCount	Anzahl der Verbindungen, die zwischen der Lastenverteilung und dem Ziel nicht erfolgreich hergestellt wurden.
Application Load Balancer	TargetResponseTime	Die verstrichene Zeit in Sekunden bis zum Empfang einer Antwort vom Ziel, nachdem die Anforderung die Lastenverteilung verlassen hat.
Application Load Balancer	UnHealthyHostCount	Anzahl der als instabil betrachteten Ziele.
Network Load Balancer	ActiveFlowCount	Die Gesamtzahl der gleichzeitigen TCP-Datenflüsse (oder Verbindungen) von Clients zu Zielen.
Network Load Balancer	ConsumedLCUs	Anzahl von Load Balancer-Kapazitätseinheiten (LCU), die von Ihrer Lastenverteilung verwendet werden.
Network Load Balancer	NewFlowCount	Die Gesamtanzahl neuer TCP-Datenflüsse (oder Verbindungen), die zwischen Clients und Zielen in dem Zeitraum eingerichtet wurden.
Network Load Balancer	ProcessedBytes	Gesamtanzahl der von einer Lastenverteilung verarbeiteten Bytes, einschließlich der TCP/IP-Header.

Thema	Metrik	Beschreibung
Global Accelerator	NewFlowCount	Die Gesamtanzahl neuer TCP- und UDP-Datenflüsse (oder Verbindungen), die zwischen Clients und Endpunkten in dem Zeitraum eingerichtet wurden.
Global Accelerator	ProcessedBytesIn	Die Gesamtanzahl der vom Beschleuniger verarbeiteten eingehenden Byte, einschlie ßlich TCP/IP-Header.
Auto Scaling	GroupMaxSize	Die maximale Größe der Auto-Scaling-Gruppe.
Amazon EC2	CPUUtilization	Der Prozentsatz der zugewiesenen EC2-Reche neinheiten, die gegenwärtig in Gebrauch sind.
Amazon EC2	NetworkIn	Anzahl der von der Instance auf allen Netzwerkschnittste llen empfangenen Byte.

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

Ein Beispiel für ein Dashboard, das mit einigen der Metriken aus der vorherigen Tabelle erstellt wurde, finden Sie unter Ein benutzerdefiniertes Richtlinien-Überwachungssystem

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

Darüber hinaus bietet das Dashboard der globalen Bedrohungsumgebung zusammenfassende Informationen zu allen DDoS-Angriffen, die von AWS erkannt wurden. Diese Informationen können nützlich sein, um DDoS-Bedrohungen in einer größeren Population von Anwendungen besser zu verstehen, zusätzlich zu den Angriffstrends und zum Vergleich mit Angriffen, die Sie möglicherweise beobachtet haben.

Wenn Sie AWS Shield Advanced abonniert haben, zeigt das Service-Dashboard zusätzliche Erkennungs- und Schutzmetriken sowie Details zum Netzwerkverkehr für Ereignisse an, die auf geschützten Ressourcen erkannt wurden. AWS Shield wertet den Datenverkehr zu Ihrer geschützten Ressource in mehreren Dimensionen aus. Wenn eine Anomalie erkannt wird, erstellt AWS Shield wird ein Ereignis und meldet die Verkehrsdimension, in der die Anomalie beobachtet wurde. Mit einer platzierten Abwehr schützt dies Ihre Ressource vor übermäßigem Datenverkehr und Datenverkehr, der einer bekannten DDoS-Ereignissignatur entspricht.

Erkennungsmetriken basieren auf Stichproben von Netzwerkflüssen oder AWS WAF-Protokollen, wenn eine Web-ACL mit der geschützten Ressource verknüpft ist. Schutzmetriken basieren auf Datenverkehr, der von den DDoS-Abwehrsystemen von Shield beobachtet wird. Schutzmetriken sind eine genauere Messung des Datenverkehrs in Ihre Ressource.

Die Metrik für die wichtigsten Mitwirkenden des Netzwerks bietet Aufschluss darüber, woher der Datenverkehr während eines erkannten Ereignisses kommt. Sie können die meisten Volume-Mitwirkenden anzeigen und nach Aspekten wie Protokoll, Quellport und TCP-Flags sortieren.
Die Metrik der wichtigsten Mitwirkenden umfasst Metriken für den gesamten auf der Ressource beobachteten Datenverkehr in verschiedenen Dimensionen. Es bietet zusätzliche Metrikdimensionen, die Sie verwenden können, um den Netzwerkverkehr zu verstehen, der während eines Ereignisses an Ihre Ressource gesendet wird.

Dazu gehören auch Details zu den Maßnahmen, die automatisch ergriffen werden, um DDoS-Angriffe zu entschärfen. Diese Informationen erleichtern es, Anomalien zu untersuchen, die Dimensionen des Datenverkehrs zu erkunden und die Maßnahmen von Shield Advanced zum Schutz Ihrer Verfügbarkeit besser zu verstehen.

Ein weiteres Tool, mit dem Sie Einblick in den Datenverkehr erhalten, der auf Ihre Anwendung abzielt, sind VPC Flow-Protokolle. In einem herkömmlichen Netzwerk können Sie Netzwerk-Flow-Protokolle verwenden, um Konnektivitäts- und Sicherheitsprobleme zu beheben und sicherzustellen, dass die Netzwerkzugriffsregeln wie gewünscht funktionieren. Mit VPC Flow-Protokollen können Sie Informationen über den IP-Datenverkehr und von Netzwerkschnittstellen in Ihrer VPC erfassen.

Jeder Eintrag im Flow-Protokoll umfasst die Quell- und Ziel-IP-Adressen, die Quell- und Zielports, das Protokoll und die Anzahl der Pakete und Byte, die im Erfassungszeitfenster übertragen wurden. Anhand dieser Informationen können Sie Anomalien im Netzwerkdatenverkehr sowie den jeweiligen Angriffsvektor identifizieren. Die meisten UDP-Reflexionsangriffe haben z. B. bestimmte Quellports (z. B. Quellport 53 für DNS-Reflexion). Dies ist eine eindeutige Signatur, anhand derer Sie den Eintrag im Flow-Protokoll identifizieren können. Als Reaktion können Sie den jeweiligen Quellport auf Instance-Ebene blockieren oder eine Netzwerk-ACL-Regel erstellen, mit der das gesamte Protokoll blockiert wird, falls es für Ihre Anwendung nicht erforderlich ist.

Weitere Informationen zum Erkennen von Netzwerkanomalien und DDoS-Angriffsvektoren mit VPC Flow-Protokollen finden Sie unter VPC-Flow-Protokolle und VPC Flow-Protokolle – Protokollieren und Anzeigen von Flow im Netzwerkdatenverkehr.

Transparenz und Schutzmanagement über mehrere Konten

In Szenarien, in denen Sie über mehrereAWS Konten hinweg arbeiten und mehrere Komponenten schützen müssen, erhöhen Sie mithilfe von Techniken, die es Ihnen ermöglichen, skalierbar zu arbeiten und den betrieblichen Aufwand zu reduzieren, Ihre Abwehrfunktionen. Wenn SieAWS Shield Advanced geschützte Ressourcen in mehreren Konten verwalten, können Sie mithilfe vonAWS Firewall Manager und AWS Security Hub eine zentrale Überwachung einrichten. Mit Firewall Manager können Sie eine Sicherheitsrichtlinie erstellen, die die Einhaltung des DDoS-Schutzes für alle Ihre Konten durchsetzt. Sie können diese beiden Dienste zusammen verwenden, um Ihre geschützten Ressourcen über mehrere Konten hinweg zu verwalten und die Überwachung dieser Ressourcen zu zentralisieren.

Der Security Hub lässt sich automatisch in den Firewall Manager integrieren, sodass Shield Advanced-Kunden neben anderen Sicherheitswarnungen und Compliance-Status auch Sicherheitswarnungen mit hoher Priorität in einem einzigen Dashboard anzeigen können. Wenn Shield Advanced beispielsweise in einem AWS-Konto innerhalb des Bereichs anomalen Datenverkehr erkennt, der für eine geschützte Ressource bestimmt ist, ist dieser Befund in der Security Hub-Konsole sichtbar. Falls konfiguriert, kann Firewall Manager die Ressource automatisch zur Einhaltung bringen, indem er sie als Shield Advanced-geschützte Ressource erstellt und dann den Security Hub aktualisiert, wenn sich die Ressource in einem konformen Zustand befindet.

Weitere Informationen zur zentralen Überwachung von Shield-geschützten Ressourcen finden Sie unter Einrichten der zentralen Überwachung für DDoS-Ereignisse und automatische Behebung nicht konformer Ressourcen.

Support

Wenn Sie einen Angriff erleben, können Sie auch vom Support von AWS bei der Bewertung der Bedrohung und der Überprüfung der Architektur Ihrer Anwendung profitieren, oder Sie können andere Unterstützung anfordern. Es ist wichtig, einen Plan für DDoS-Angriffe zu erstellen, bevor diese wirklich auftreten. Bei den in diesem Dokument beschriebenen bewährten Methoden handelt es sich um proaktive Maßnahmen, die Sie vor dem Start einer Anwendung implementieren. DDoS-Angriffe auf Ihre Anwendung können jedoch weiterhin auftreten. Lesen Sie die Optionen in diesem Abschnitt, um die Supportressourcen zu ermitteln, die für Ihr Szenario am besten geeignet sind. Ihr Kundenbetreuungsteam kann Ihren Anwendungsfall und Ihre Anwendung bewerten und Ihnen bei spezifischen Fragen oder Herausforderungen behilflich sein.

Wenn Sie Produktionsworkloads auf AWS ausführen, sollten Sie den Business Support abonnieren, der Ihnen rund um die Uhr Zugriff auf Cloud Support-Techniker bietet, die Sie bei Problemen mit DDoS-Angriffen unterstützen können. Wenn Sie geschäftskritische Workloads ausführen, sollten Sie den Enterprise Support in Betracht ziehen, der Ihnen die Möglichkeit bietet, kritische Fälle zu öffnen und die schnellste Antwort von einem Senior Cloud Support-Techniker zu erhalten.

Wenn Sie Business Support oder Enterprise Support und auch AWS Shield Advanced abonniert haben, können Sie das proaktive Shield-Engagement konfigurieren. Sie können damit Integritätsprüfungen konfigurieren, Ihren Ressourcen zuordnen und rund um die Uhr Kontaktinformationen für den Betrieb bereitstellen. Wenn Shield Anzeichen von DDoS erkennt und Ihre Anwendungszustandsprüfungen Anzeichen einer Verschlechterung zeigen, wird AWS SRT Sie proaktiv kontaktieren. Dies ist unser empfohlenes Engagement-Modell, da es die schnellsten AWS-SRT-Reaktionszeiten ermöglicht und AWS SRT in die Lage versetzt, mit der Fehlerbehebung zu beginnen, noch bevor ein Kontakt mit Ihnen hergestellt wurde.

Für die Funktion des proaktiven Engagements müssen Sie eine Route 53-Integritätsprüfung konfigurieren, die den Zustand Ihrer Anwendung genau misst und mit der durch Shield Advanced geschützten Ressource verknüpft ist. Sobald eine Route 53-Zustandsprüfung in der Shield-Konsole zugeordnet ist, verwendet das Shield Advanced-Erkennungssystem den Status der Integritätsprüfung als Indikator für den Zustand Ihrer Anwendung. Die zustandsbasierte Erkennungsfunktion von Shield Advanced stellt sicher, dass Sie benachrichtigt werden und dass Abhilfemaßnahmen schneller durchgeführt werden, wenn Ihre Anwendung fehlerhaft ist. AWS SRT wird sich mit Ihnen in Verbindung setzen, um zu untersuchen, ob die fehlerhafte Anwendung von einem DDoS-Angriff betroffen ist und bei Bedarf zusätzliche Abhilfemaßnahmen vornehmen.

Der Abschluss der Konfiguration des proaktiven Engagements umfasst das Hinzufügen von Kontaktdaten in der Shield-Konsole. AWS SRT verwendet diese Informationen, um Sie zu kontaktieren. Sie können bis zu 10 Kontakte konfigurieren und zusätzliche Hinweise geben, wenn Sie spezielle Kontaktanforderungen oder -präferenzen haben. Proaktive Kontakte sollten rund um die Uhr eine Rolle innehaben, z. B. ein Sicherheitszentrum oder eine Person, die sofort verfügbar ist.

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

Sie können auch an AWS SRT eskalieren, indem Sie mithilfe der AWS Support-Konsole oder der Support-API einen AWS Support-Fall erstellen, wenn Sie ein DDOS-bezogenes Ereignis haben, das sich auf die Verfügbarkeit Ihrer Anwendung auswirkt.

Fazit

Die in diesem Dokument beschriebenen bewährten Methoden können Ihnen helfen, eine ausfallsichere DDoS-Architektur zu entwickeln, die die Verfügbarkeit Ihrer Anwendung schützt, indem sie viele gängige Infrastruktur- und DDoS-Angriffe auf Anwendungsebene verhindert. Inwieweit Sie diese bewährten Methoden bei der Entwicklung Ihrer Anwendung befolgen, wirkt sich auf Art, Vektor und Volumen der DDoS-Angriffe aus, die Sie abwehren können. Sie können Ausfallsicherheit integrieren, ohne einen DDoS-Abwehrdienst zu abonnieren. Wenn Sie sich für ein Abonnement entscheiden, erhaltenAWS Shield Advanced Sie zusätzliche Funktionen für Support, Transparenz, Minderung und Kostenschutz, die eine bereits robuste Anwendungsarchitektur weiter schützen.

Mitwirkende

An diesem Dokument haben folgende Personen mitgewirkt:

- Jeffrey Lyon, AWS-Perimeterschutz
- Rodrigo Ferroni, AWS-Sicherheitsexperte TAM
- Dmitriy Novikov, AWS-Lösungsarchitekt
- Achraf Souk, AWS-Lösungsarchitekt
- Yoshihisa Nakatani, AWS-Lösungsarchitekt

Ressourcen

Weitere Informationen:

- Bewährte Methoden für DDoS-Mitigation auf AWS
- Leitfaden für die Implementierung AWS WAF
- SID324 — re:Invent 2017: Automating DDoS Response in the Cloud (Automatisierung der DDoS-Reaktion in der Cloud)
- CTD304 — re:Invent 2017: Dow Jones & Wall Street Journal's Journey to Manage Traffic Spikes While Mitigating DDoS & Application Layer Threats (Die Reise von Dow Jones und Wall Street Journal zur Verwaltung von Verkehrsspitzen bei gleichzeitiger Minderung von DDoS und Bedrohungen auf Anwendungsebene)
- AWS re:Invent 2017: Living on the Edge, It's Safer Than You Think! (Arbeiten mit Edge ist sicherer, als Sie denken!) Building Strong with Amazon CloudFront (Starker Aufbau mit Amazon CloudFront) AWS Shield und AWS WAF
- SEC407 - re:Invent 2019: A defense-in-depth approach to building web applications (Ein vertiefter Ansatz zur Entwicklung von Webanwendungen)
- SEC321 - re:Invent 2020: Get ahead of the curve with DDoS Response Team escalations (Mit Eskalationen des DDoS-Response-Teams der Kurve einen Schritt voraus)
- William Hill: High-performance DDOS Protection with (Leistungsstarker DDoS-Schutz mit) AWS

Dokumentversionen

Abonnieren Sie den RSS-Feed, um über Aktualisierungen des Whitepapers benachrichtigt zu werden.

Update-Historie-Änderung	Update-Historie-Beschreibung	Update-Historie-Datum
Whitepaper-Aktualisierung	Aktualisiert mit den neuesten Empfehlungen und Funktione n. AWS Global Acceleratorwird als Teil eines umfassenden Schutzes zu Edge hinzugefü gt. AWS Firewall Manager zur zentralen Überwachung von DDoS-Ereignissen und zur automatischen Behebung nicht konformer Ressourcen.	21. September 2021
Whitepaper-Aktualisierung	Aktualisiert, um das Cache-Busting im Abschnitt Erkennung und Filter bösartige r Webanforderungen (BP1, BP2) und die ELB- und ALB-Nutzung im Abschnitt Scale-to-Absorb (BP6) zu verdeutli chen. Aktualisierte Diagramme und Tabelle 2, gekennzeichnet als „Wahl der Region“ als BP8. BP7-Abschnitt mit weiteren Details aktualisiert.	18. Dezember 2019
Whitepaper-Aktualisierung	Aktualisiert, um AWS WAF-Protokollierung als bewährte Methode aufzunehmen.	1. Dezember 2018
Whitepaper-Aktualisierung	Aktualisiert mit AWS ShieldAWS WAF-Funkt	1. Juni 2018

	ionen, AWS Firewall Manager und verwandten bewährten Methoden.	
Whitepaper-Aktualisierung	Es wurden Richtlinien für die präskriptive Architektur hinzugefügt und um AWS WAF aktualisiert.	1. Juni 2016
Erste Veröffentlichung	Whitepaper veröffentlicht.	1. Juni 2015

Hinweise

Kunden sind eigenverantwortlich für die unabhängige Bewertung der Informationen in diesem Dokument zuständig. Dieses Dokument: (a) dient rein zu Informationszwecken, (b) spiegelt die aktuellen Produktangebote und Verfahren von AWS wider, die sich ohne vorherige Mitteilung ändern können, und (c) impliziert keinerlei Verpflichtungen oder Zusicherungen seitens AWS und dessen Tochtergesellschaften, Lieferanten oder Lizenzgebern. AWS-Produkte oder -Services werden im vorliegenden Zustand und ohne ausdrückliche oder stillschweigende Gewährleistungen, Zusicherungen oder Bedingungen bereitgestellt. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden wird durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen zwischen AWS und seinen Kunden und ändert diese Vereinbarungen auch nicht.