AWS Whitepaper

AWS Le migliori pratiche per la DDoS resilienza

AWS Le migliori pratiche per la DDoS resilienza: AWS Whitepaper

Table of Contents

AWS Le migliori pratiche per la DDoS resilienza

Data di pubblicazione: 9 agosto 2023 (Revisioni del documento)

È importante proteggere la propria azienda dall'impatto degli attacchi Distributed Denial of Service (DDoS) e da altri attacchi informatici. Mantenere la fiducia dei clienti nel vostro servizio mantenendo la disponibilità e la reattività dell'applicazione è una priorità assoluta. Volete anche evitare costi diretti non necessari quando l'infrastruttura deve scalare in risposta a un attacco. Amazon Web Services (AWS) si impegna a fornirti gli strumenti, le best practice e i servizi per difenderti dai malintenzionati su Internet. L'utilizzo dei servizi giusti AWS aiuta a garantire disponibilità, sicurezza e resilienza elevate.

In questo white paper, vengono AWS fornite DDoS linee guida prescrittive per migliorare la resilienza delle applicazioni in esecuzione. AWS Ciò include un'architettura di riferimento DDoS -resilient che può essere utilizzata come guida per proteggere la disponibilità delle applicazioni. Questo white paper descrive anche diversi tipi di attacco, come gli attacchi a livello di infrastruttura e gli attacchi a livello di applicazione. AWS spiega quali sono le best practice più efficaci per gestire ogni tipo di attacco. Inoltre, vengono descritti i servizi e le funzionalità che rientrano in una strategia di DDoS mitigazione, oltre a come ciascuno di essi può essere utilizzato per proteggere le applicazioni.

Questo paper è destinato ai responsabili delle decisioni IT e agli ingegneri della sicurezza che hanno familiarità con i concetti di base di rete, sicurezza e AWS. Ogni sezione contiene collegamenti alla AWS documentazione che fornisce maggiori dettagli sulle migliori pratiche o funzionalità.

AWS rileva oltre un milione di DDoS attacchi all'anno e ne mitiga migliaia su base giornaliera contro i nostri clienti. Secondo il nostro team Shield Response (SRT), la maggior parte dei clienti che subiscono l'impatto aziendale degli DDoS attacchi non ha implementato le raccomandazioni contenute in questa guida.

Sei Well-Architected?

Il AWS Well-Architected Framework ti aiuta a comprendere i pro e i contro delle decisioni che prendi quando crei sistemi nel cloud. I sei pilastri del Framework consentono di apprendere le migliori pratiche architettoniche per progettare e gestire sistemi affidabili, sicuri, efficienti, convenienti e sostenibili. Utilizzando AWS Well-Architected Tool, disponibile gratuitamente in AWS Management Console(è richiesto il login), puoi esaminare i tuoi carichi di lavoro rispetto a queste best practice rispondendo a una serie di domande per ogni pilastro.

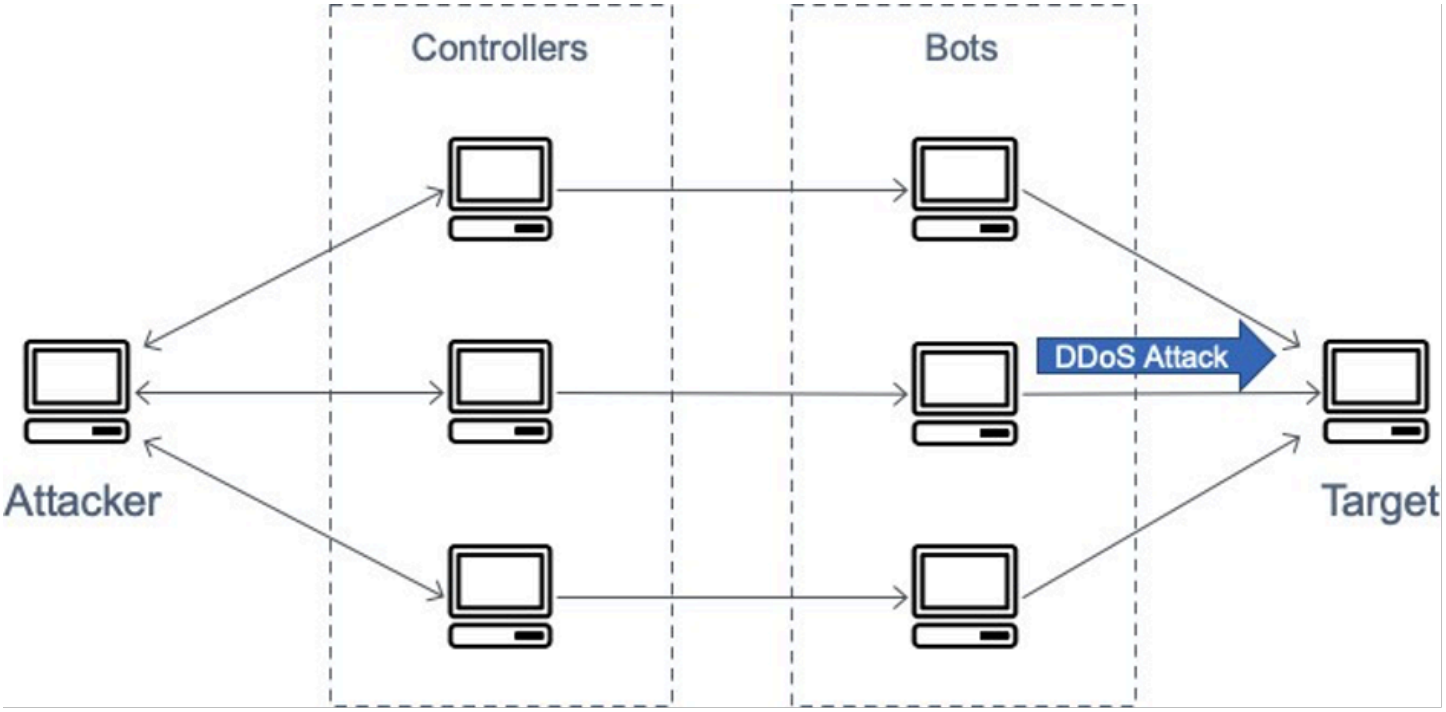
Per ulteriori indicazioni e best practice da parte di esperti per la tua architettura cloud (implementazioni dell'architettura di riferimento, diagrammi e white paper), consulta l'Architecture Center.AWS

Introduzione agli attacchi Denial of Service

Un attacco o evento Denial of Service (DoS) è un tentativo deliberato di rendere un sito Web o un'applicazione non disponibile agli utenti, ad esempio inondandoli di traffico di rete. Gli aggressori utilizzano una varietà di tecniche che consumano grandi quantità di larghezza di banda di rete o impegnano altre risorse di sistema, interrompendo l'accesso degli utenti legittimi. Nella sua forma più semplice, un aggressore solitario utilizza un'unica fonte per eseguire un attacco DoS contro un bersaglio, come illustrato nella figura seguente.

Un diagramma che illustra un attacco DoS

In un attacco Distributed Denial of Service (DDoS), un aggressore utilizza più fonti per orchestrare un attacco contro un obiettivo. Queste fonti possono includere gruppi distribuiti di computer, router, dispositivi IoT e altri endpoint infetti da malware. La figura seguente mostra una rete di host compromessi che partecipano all'attacco, generando una marea di pacchetti o richieste tali da sovraccaricare il bersaglio.



Un diagramma che mostra un attacco DDoS

Il modello Open Systems Interconnection (OSI) include sette livelli, descritti nella tabella seguente. DDoSgli attacchi sono più comuni ai livelli 3, 4, 6 e 7.

- Gli attacchi di livello 3 e 4 corrispondono ai livelli di rete e trasporto del OSI modello. In questo white paper, AWS si fa riferimento a questi attacchi collettivamente come attacchi a livello di infrastruttura.
- Gli attacchi di livello 6 e 7 corrispondono ai livelli Presentazione e Applicazione del modello. OSI Questo white paper li affronta insieme come attacchi a livello di applicazione.

Questo paper illustra questi tipi di attacco nelle sezioni che seguono.

Tabella 1 — modello OSI

#	Livello	Unità	Descrizione	Esempi vettoriali
7	Applicazione	Dati	Dal processo di rete all'appli cazione	HTTPinond azioni, DNS interroga inondazioni
6	Presentazione	Dati	Rappresen tazione e crittografia dei dati	Abuso di Transport Layer Security (TLS)
5	Sessione	Dati	Comunicazione tra host	N/D
4	Trasporto	Segmenti	nd-to-end Connessioni elettroniche e affidabilità	Sincronizza (SYN) alluvioni
3	Rete	Pacchetti	Determinazione del percorso e indirizzamento logico	Attacchi di riflessione del protocollo

#	Livello	Unità	Descrizione	Esempi vettoriali
				User Datagram Protocol (UDP)
2	Collegamento dati	Frames (Fotogrammi)	Indirizzamento fisico	N/D
1	Fisica	Bit	Trasmissione multimediale, di segnale e binaria	N/D

Attacchi a livello di infrastruttura

Gli attacchi più comuni, DDoS gli attacchi di riflessione e le inondazioni del protocollo User Datagram Protocol (UDP), sono attacchi a livello di infrastruttura. SYN Un utente malintenzionato può utilizzare uno di questi metodi per generare grandi volumi di traffico che possono inondare la capacità di una rete o bloccare risorse su sistemi come server, firewall, sistema di prevenzione delle intrusioni () o load balancer. IPS Sebbene questi attacchi possano essere facili da identificare, per mitigarli efficacemente è necessario disporre di una rete o di sistemi in grado di aumentare la capacità più rapidamente rispetto al flusso di traffico in entrata. Questa capacità aggiuntiva è necessaria per filtrare o assorbire il traffico di attacco, liberando il sistema e l'applicazione per rispondere al traffico legittimo dei clienti.

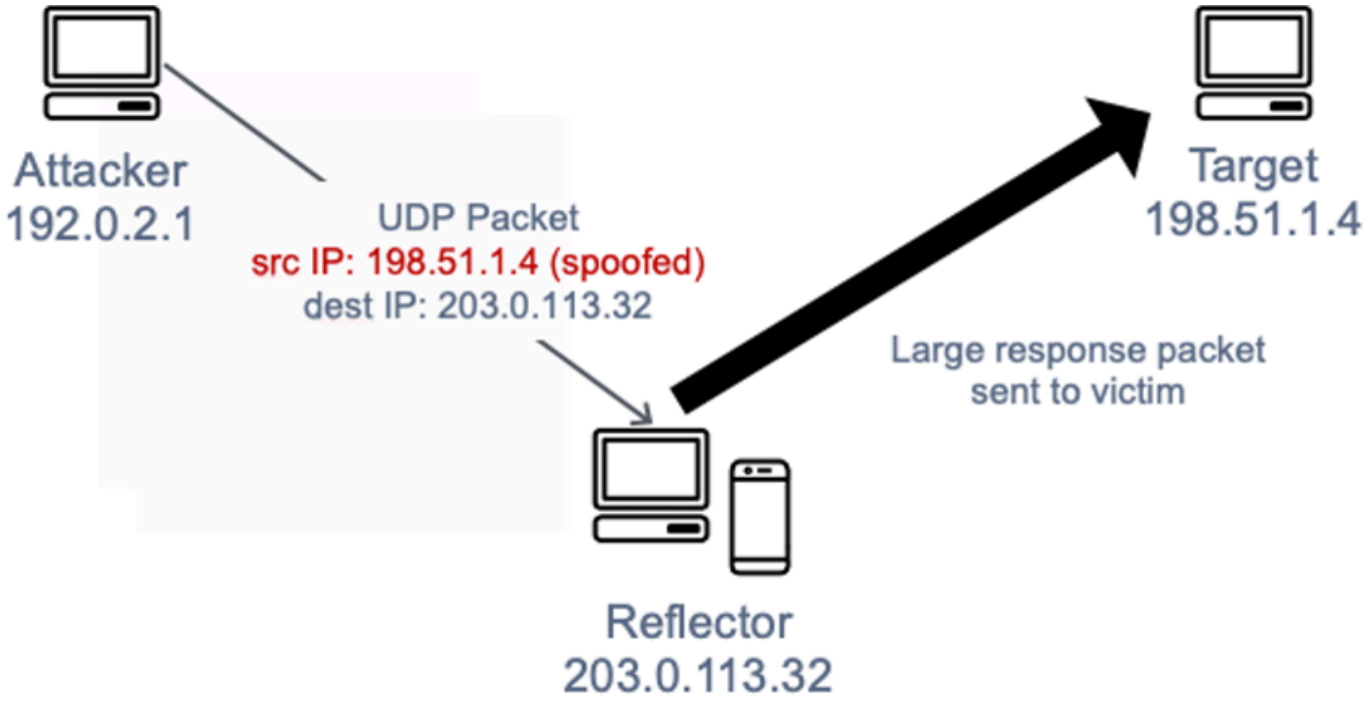
UDPattacchi di riflessione

UDPgli attacchi di riflessione sfruttano il fatto che UDP si tratta di un protocollo stateless. Gli aggressori possono creare un pacchetto di UDP richiesta valido che elenchi l'indirizzo IP del bersaglio dell'attacco come indirizzo IP di origine. UDP L'aggressore ha ora falsificato, o UDP falsificato, l'IP di origine del pacchetto di richiesta. Il UDP pacchetto contiene l'IP di origine contraffatto e viene inviato dall'aggressore a un server intermedio. Il server viene indotto con l'inganno a inviare i pacchetti di UDP risposta all'IP della vittima presa di mira anziché all'indirizzo IP dell'aggressore. Il server intermedio viene utilizzato perché genera una risposta molte volte più grande del pacchetto di richiesta, amplificando in modo efficace la quantità di traffico di attacco inviato all'indirizzo IP di destinazione.

Il fattore di amplificazione è il rapporto tra la dimensione della risposta e la dimensione della richiesta e varia a seconda del protocollo utilizzato dall'aggressore: Network Time Protocol (NTP)DNS, Simple

Service Directory Protocol (SSDP), Connectionless Lightweight Directory Access Protocol (CLDAP), Memcached, Character Generator Protocol (CharGen) o Quote of the Day (QOTD).

Ad esempio, il fattore di amplificazione per DNS può essere compreso tra 28 e 54 volte il numero originale di byte. Pertanto, se un utente malintenzionato invia un payload di richiesta di 64 byte a un DNS server, può generare oltre 3400 byte di traffico indesiderato verso il bersaglio dell'attacco. UDPgli attacchi di riflessione sono responsabili di un volume di traffico maggiore rispetto ad altri attacchi. La figura seguente illustra la tattica di riflessione e l'effetto di amplificazione.

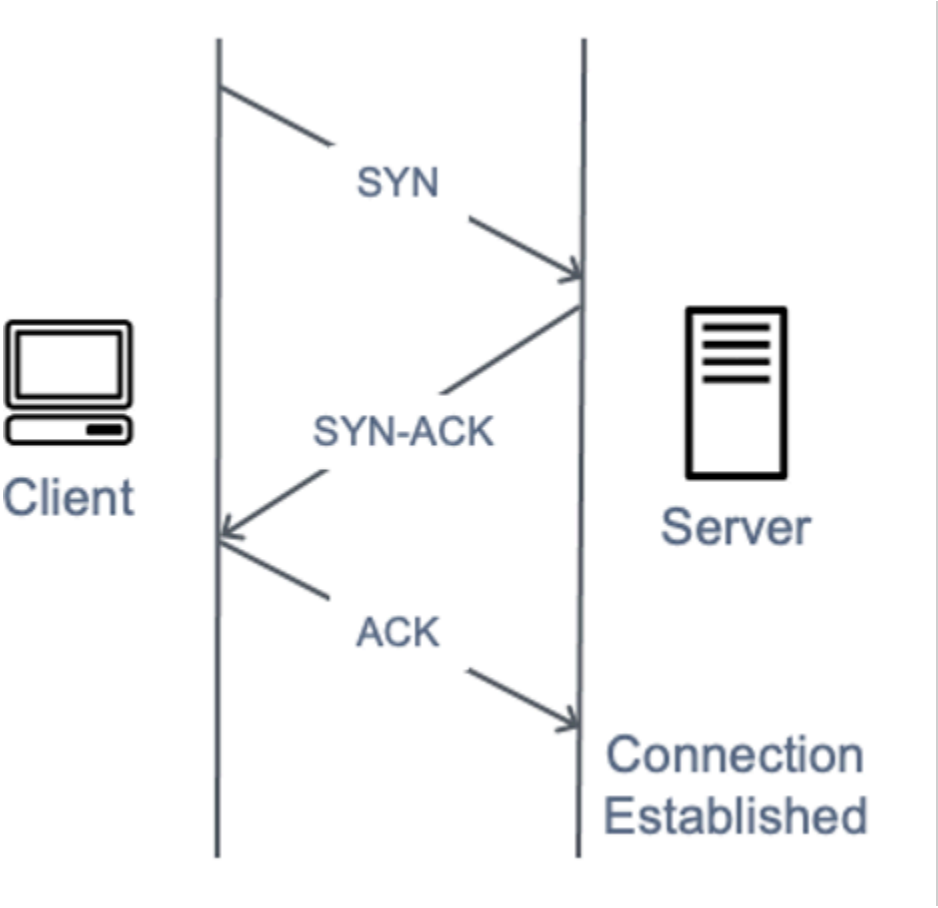


Un diagramma che mostra un attacco di riflessione UDP

Va notato che gli attacchi riflessi, sebbene forniscano agli aggressori un'amplificazione «gratuita», richiedono la capacità di spoofing dell'IP e poiché sempre più provider di rete adottano la funzionalità Source Address Validation Everywhere (SAVE) oppure BCP38, questa funzionalità viene rimossa, richiedendo ai provider di servizi di cessare gli attacchi di riflessione o di trasferirsi presso data center e DDoS provider di rete che non implementano la convalida dell'indirizzo sorgente.

SYNattacchi di alluvione

Quando un utente si connette a un servizio Transmission Control Protocol (TCP), ad esempio un server Web, il client invia un SYN pacchetto. Il server restituisce un pacchetto di conferma della sincronizzazione (SYN-ACK) e infine il client risponde con un pacchetto di conferma (), che completa l'handshake a tre vie previsto. ACK L'immagine seguente illustra questa tipica stretta di mano.



Un diagramma che mostra una stretta di mano a tre vie SYN

In un attacco SYN flood, un client malintenzionato invia un gran numero di SYN pacchetti, ma non invia mai i pacchetti finali ACK per completare le strette di mano. Il server resta in attesa di una risposta alle TCP connessioni semiaperte e l'idea è che l'obiettivo alla fine esaurisca la capacità di accettare nuove TCP connessioni, il che impedisce ai nuovi utenti di connettersi al server, tuttavia l'impatto effettivo è più sfumato. Tutti i sistemi operativi moderni implementano di default SYN i cookie come meccanismo per contrastare l'esaurimento delle tabelle di stato causato dagli SYN attacchi di inondazione. Quando la lunghezza della SYN coda raggiunge una soglia predeterminata, il server risponde con un SYN - ACK contenente un numero di sequenza iniziale preimpostato, senza creare una voce nella sua coda. SYN Se poi il server riceve un messaggio ACK contenente un numero di riconoscimento correttamente incrementato, è in grado di aggiungere la voce alla sua tabella degli stati e procedere normalmente. L'impatto effettivo delle SYN inondazioni sui dispositivi bersaglio tende a essere la capacità e l'CPUesaurimento della rete, tuttavia i dispositivi intermedi con stato come i firewall (o il tracciamento delle connessioni dei gruppi di EC2 sicurezza) possono risentire dell'esaurimento della tabella di stato e interrompere nuove connessioni. TCP

TCPriflesso del riquadro centrale

Questo vettore di attacco relativamente nuovo è stato divulgato per la prima volta in un white paper accademico nell'agosto 2021, che spiegava come la TCP mancata conformità dei firewall nazionali e di quelli disponibili in commercio potesse indurli a diventare un vettore di amplificazione. TCP Abbiamo visto questi attacchi «in natura» dall'inizio del 2022 e continuiamo a vederli ancora oggi. Il fattore di amplificazione varia a seconda dei diversi modi in cui i fornitori hanno implementato questa «funzionalità», ma può superare l'amplificazione UDP Memcached.

Attacchi a livello applicativo

Un utente malintenzionato può prendere di mira l'applicazione stessa utilizzando un attacco di livello 7 o di livello applicativo. In questi attacchi, simili agli attacchi di tipo SYN flood infrastructure, l'aggressore tenta di sovraccaricare funzioni specifiche di un'applicazione per renderla non disponibile o non rispondere agli utenti legittimi. A volte ciò può essere ottenuto con volumi di richieste molto bassi che generano solo un piccolo volume di traffico di rete. Ciò può rendere l'attacco difficile da rilevare e mitigare. Esempi di attacchi a livello di applicazione includono HTTP flood, attacchi di cache-busting e - floods. WordPress XML RPC

- In un attacco HTTP flood, un utente malintenzionato invia HTTP richieste che sembrano provenire da un utente valido dell'applicazione web. Alcune HTTP inondazioni hanno come obiettivo una risorsa specifica, mentre quelle più complesse HTTP tentano di emulare l'interazione umana con l'applicazione. Ciò può aumentare la difficoltà di utilizzare tecniche di mitigazione comuni come la limitazione della frequenza delle richieste.
- Gli attacchi di cache-busting sono un tipo di HTTP flood che utilizza variazioni nella stringa di query per aggirare la memorizzazione nella cache della rete di distribuzione dei contenuti (). CDN Invece di poter restituire i risultati memorizzati nella cache, CDN devono contattare il server di origine per ogni richiesta di pagina e questi recuperi dall'origine causano ulteriore stress sul server web dell'applicazione.
- Con un attacco WordPress XML - RPC flood, noto anche come WordPress pingback flood, un utente malintenzionato prende di mira un sito Web ospitato nel software di gestione dei contenuti. WordPress L'aggressore utilizza in modo improprio la RPC API funzione XML- per generare una marea di richieste. HTTP La funzionalità di pingback consente a un sito Web ospitato sul WordPress (Sito A) di notificare un altro WordPress sito (Sito B) tramite un collegamento che il Sito A ha creato al Sito B. Il Sito B tenta quindi di recuperare il Sito A per verificare l'esistenza del collegamento. In un flusso di pingback, l'aggressore sfrutta in modo improprio questa capacità per

indurre il Sito B ad attaccare il Sito A. Questo tipo di attacco ha una firma chiara: "`WordPress:`" è tipicamente presente nello User-Agent dell'intestazione della HTTP richiesta.

Esistono altre forme di traffico dannoso che possono influire sulla disponibilità di un'applicazione. I bot Scraper automatizzano i tentativi di accesso a un'applicazione Web per rubare contenuti o registrare informazioni sulla concorrenza, come i prezzi. Gli attacchi di forza bruta e di credential stuffing sono tentativi programmati per ottenere l'accesso non autorizzato alle aree sicure di un'applicazione. Non si tratta di DDoS attacchi in senso stretto, ma la loro natura automatizzata può sembrare simile a un DDoS attacco e possono essere mitigati implementando alcune delle stesse best practice trattate in questo paper.

Gli attacchi a livello di applicazione possono anche prendere di mira i servizi Domain Name System (DNS). Il più comune di questi attacchi è un flusso di DNS query in cui un utente malintenzionato utilizza molte DNS query ben formate per esaurire le risorse di un server. DNS Questi attacchi possono includere anche un componente di cache-busting in cui l'aggressore randomizza la stringa del sottodominio per aggirare la cache locale di un determinato resolver. DNS Di conseguenza, il resolver non può sfruttare le query di dominio memorizzate nella cache e deve invece contattare ripetutamente il server autorevole, il che amplifica l'attacco. DNS

Se un'applicazione Web viene distribuita tramite Transport Layer Security (TLS), un utente malintenzionato può anche scegliere di attaccare il processo di negoziazione. TLS TLSè costoso dal punto di vista computazionale, quindi un utente malintenzionato, generando un carico di lavoro aggiuntivo sul server per elaborare dati illeggibili (o incomprensibili (testo cifrato)) come una stretta di mano legittima, può ridurre la disponibilità del server. In una variante di questo attacco, un utente malintenzionato completa la stretta di mano ma rinegozia continuamente il metodo di crittografia. TLS In alternativa, un utente malintenzionato può tentare di esaurire le risorse del server aprendo e chiudendo molte sessioni. TLS

Tecniche di mitigazione

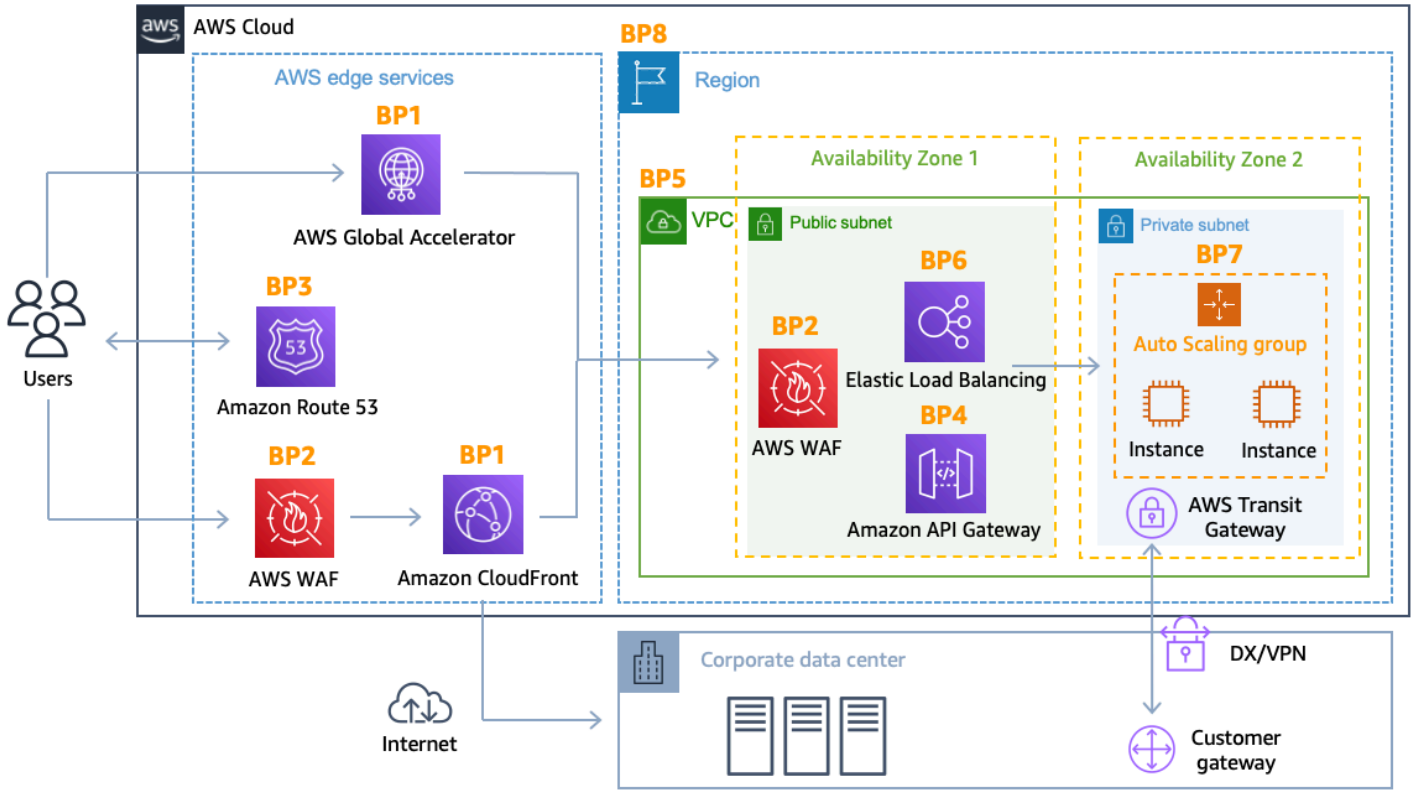
Alcune forme di DDoS mitigazione sono incluse automaticamente nei servizi. AWS DDoSla resilienza può essere ulteriormente migliorata utilizzando un' AWS architettura con servizi specifici, descritti nelle sezioni seguenti, e implementando best practice aggiuntive per ogni parte del flusso di rete tra gli utenti e l'applicazione.

Puoi utilizzare AWS servizi che operano da edge location, come Amazon CloudFront, AWS Global Accelerator e Amazon Route 53 per creare una protezione completa della disponibilità contro tutti gli attacchi noti a livello di infrastruttura. Questi servizi fanno parte del AWS Global Edge Network e possono migliorare la DDoS resilienza dell'applicazione quando serve qualsiasi tipo di traffico applicativo da postazioni periferiche distribuite in tutto il mondo. È possibile eseguire l'applicazione in qualsiasi ambiente Regione AWS e utilizzare questi servizi per proteggere la disponibilità delle applicazioni e ottimizzarne le prestazioni per gli utenti finali legittimi.

I vantaggi dell'utilizzo di Amazon CloudFront, Global Accelerator e Amazon Route 53 includono:

- Accesso a Internet e capacità di DDoS mitigazione attraverso la rete AWS Global Edge. Ciò è utile per mitigare attacchi volumetrici di grandi dimensioni, che possono raggiungere una scala di terabit.
- AWS Shield DDoSi sistemi di mitigazione sono integrati con i servizi AWS edge e si riducono da pochi minuti a meno di un secondo. time-to-mitigate
- La mitigazione Stateless SYN Flood verifica le connessioni in entrata utilizzando i SYN cookie prima di passarle al servizio protetto. Ciò garantisce che solo le connessioni valide raggiungano l'applicazione, proteggendo al contempo gli utenti finali legittimi da cadute di falsi positivi.
- Sistemi automatici di ingegneria del traffico che disperdono o isolano l'impatto di attacchi volumetrici di grandi dimensioni. DDoS Tutti questi servizi isolano gli attacchi alla fonte prima che raggiungano l'origine, il che significa un minore impatto sui sistemi protetti da questi servizi.
- La difesa a livello di applicazione, CloudFront se combinata con AWS WAFquella, non richiede la modifica dell'architettura dell'applicazione corrente (ad esempio, in un data center Regione AWS o in sede).

Il trasferimento dei dati in entrata è gratuito AWS e non si paga per il traffico di DDoS attacco mitigato da. AWS Shield Il seguente diagramma di architettura include i servizi AWS Global Edge Network.



DDoS-architettura di riferimento resiliente

Questa architettura include diversi AWS servizi che possono aiutarti a migliorare la resilienza dell'applicazione web contro gli attacchi. DDoS La tabella seguente fornisce un riepilogo di questi servizi e delle funzionalità che possono offrire. AWS ha contrassegnato ogni servizio con un indicatore di best practice (BP1,BP2) per facilitare la consultazione all'interno di questo documento. Ad esempio, una prossima sezione illustra le funzionalità fornite da Amazon CloudFront e Global Accelerator che include l'indicatore delle migliori pratiche. BP1

Tabella 2 - Riepilogo delle migliori pratiche

	AWS Edge			Regione AWS		
	Usare Amazon CloudFront (BP1) con AWS WAF (BP2)	Utilizzo di Global Accelerator () BP1	Utilizzo di Amazon Route 53 (BP3)	Utilizzo di Elastic Load Balancing (BP6) con	Utilizzo di gruppi di sicurezza e rete ACLs in Amazon VPC (BP5)	Utilizzo di Amazon Elastic Compute Cloud (AmazonEC

	AWS Edge			Regione AWS		
				AWS WAF () BP2		2) Auto BP7 Scaling ()
Mitigazione degli attacchi di livello 3 (ad esempio, UDP riflessione)	✓	✓	✓	✓	✓	✓
Mitigazione degli attacchi di livello 4 (ad esempio, SYN alluvione)	✓	✓	✓	✓		
Mitigazione degli attacchi di livello 6 (ad esempioTLS)	✓	✓	✓	✓		
Ridurre la superficie di attacco	✓	✓	✓	✓	✓	

	AWS Edge			Regione AWS		
Scalabilità per assorbire il traffico a livello di applicazione	✓	✓	✓	✓	✓	✓
Mitigazione degli attacchi di livello 7 (livello applicativo)	✓	✓(*)	✓	✓	✓(*)	✓(*)
Isolamento geografico e dispersione del traffico in eccesso e degli attacchi più grandi DDoS	✓	✓	✓			

✓ (*): se utilizzato AWS WAF con Application Load Balancer

Un altro modo per migliorare la tua preparazione a rispondere e mitigare DDoS gli attacchi è abbonarti a. AWS Shield Advanced I vantaggi dell'utilizzo includono: AWS Shield Advanced

- Accesso al supporto specializzato 24 ore su 24, 7 giorni su 7 del AWS Shield Response Team (AWS SRT) per assistenza nella mitigazione DDoS degli attacchi che influiscono sulla disponibilità delle applicazioni, inclusa una funzione opzionale di coinvolgimento proattivo

- Soglie di rilevamento sensibili che indirizzano il traffico verso il sistema di DDoS mitigazione in anticipo e possono migliorare time-to-mitigate gli attacchi contro Amazon EC2 (incluso elastico Load Balancer) o Network Load Balancer, se utilizzate con un indirizzo IP elastico
- Rilevamento personalizzato di livello 7 basato sui modelli di traffico di base dell'applicazione se utilizzata con AWS WAF
- DDoSMitigazione automatica a livello di applicazione in cui Shield Advanced risponde agli DDoS attacchi rilevati creando, valutando e implementando regole personalizzate AWS WAF
- Accesso senza costi aggiuntivi per la mitigazione degli DDoS attacchi AWS WAF a livello di applicazione (se utilizzato con Amazon CloudFront o Application Load Balancer)
- Gestione centralizzata delle politiche di sicurezza senza costi AWS Firewall Manageraggiuntivi.
- Protezione dei costi che consente di richiedere un rimborso limitato dei costi relativi alla scalabilità derivanti da un attacco. DDoS
- Accordo sul livello di servizio avanzato specifico per AWS Shield Advanced i clienti.
- Gruppi di protezione che consentono di raggruppare le risorse, fornendo un modo self-service per personalizzare l'ambito di rilevamento e mitigazione dell'applicazione trattando più risorse come un'unica unità. Per informazioni sui gruppi di protezione, fare riferimento a Gruppi di protezione Shield Advanced.
- DDoSvisibilità degli attacchi utilizzando le AWS Management Console CloudWatch metriche e API gli allarmi di Amazon e Amazon.

Questo servizio di DDoS mitigazione opzionale aiuta a proteggere le applicazioni ospitate su qualsiasi piattaforma. Regione AWS Il servizio è disponibile a livello globale per CloudFront Route 53 e Global Accelerator. A livello regionale, puoi proteggere gli indirizzi IP di Application Load Balancer, Classic Load Balancer ed Elastic, il che ti consente di proteggere le istanze di Network Load Balancer () o AmazonNLBs. EC2

Per un elenco completo delle AWS Shield Advanced funzionalità e per ulteriori informazioni in merito AWS Shield, consulta How works. AWS Shield

Le migliori pratiche per la DDoS mitigazione

Nelle sezioni seguenti, ciascuna delle migliori pratiche consigliate per la DDoS mitigazione viene descritta in modo più approfondito. Per una easy-to-implement guida rapida sulla creazione di un livello di DDoS mitigazione per applicazioni Web statiche o dinamiche, consulta Come proteggere le applicazioni Web dinamiche dagli DDoS attacchi utilizzando Amazon CloudFront e Amazon Route 53.

Difesa a livello di infrastruttura (BP1,BP3,BP6,BP7)

In un ambiente di data center tradizionale, è possibile mitigare DDoS gli attacchi a livello di infrastruttura utilizzando tecniche come l'overprovisioning della capacità, l'implementazione di sistemi di DDoS mitigazione o la riduzione del traffico con l'aiuto di servizi di mitigazione. DDoS Sì AWS, le funzionalità di DDoS mitigazione vengono fornite automaticamente, ma è possibile ottimizzare la DDoS resilienza dell'applicazione effettuando scelte di architettura che sfruttino al meglio tali funzionalità e consentano inoltre di scalare in base al traffico in eccesso.

Le considerazioni chiave per contribuire a mitigare DDoS gli attacchi volumetrici includono la garanzia della disponibilità di capacità e diversità di transito sufficienti e la protezione delle risorse AWS , come le EC2 istanze Amazon, dal traffico di attacco.

Alcuni tipi di EC2 istanze Amazon supportano funzionalità in grado di gestire più facilmente grandi volumi di traffico, ad esempio interfacce con larghezza di banda di rete fino a 100 Gbps e reti avanzate. Questo aiuta a prevenire la congestione dell'interfaccia per il traffico che ha raggiunto l'EC2istanza Amazon. Le istanze che supportano una rete avanzata offrono prestazioni di input/output (I/O) più elevate, maggiore larghezza di banda e un utilizzo inferiore rispetto alle implementazioni tradizionali. CPU Ciò migliora la capacità dell'istanza di gestire grandi volumi di traffico e, in ultima analisi, la rende altamente resiliente al carico di pacchetti al secondo (pps).

Per consentire questo elevato livello di resilienza, AWS consiglia di utilizzare Amazon EC2 Dedicated Instances o istanze Amazon con un throughput di rete più elevato con un suffisso "N" e supporto per Enhanced Networking con larghezza di banda di rete fino a 100 Gbps, ad esempio, `c6gn.16xlarge` `c5n.18xlarge` e/o EC2 istanze metal (come). `c5n.metal`

Per ulteriori informazioni sulle EC2 istanze Amazon che supportano interfacce di rete da 100 Gigabit e reti avanzate, consulta i tipi di istanze Amazon EC2.

Il modulo richiesto per una rete avanzata e il set di `enaSupport` attributi richiesto sono inclusi in Amazon Linux 2 e nelle versioni più recenti di Amazon LinuxAMI. Pertanto, se avvii un'istanza con una versione hardware virtuale (HVM) di Amazon Linux su un tipo di istanza supportato, la rete avanzata è già abilitata per l'istanza. Per ulteriori informazioni, consulta Verifica se la rete avanzata è abilitata e Rete avanzata su Linux.

Amazon EC2 con Auto Scaling () BP7

Un altro modo per mitigare gli attacchi a livello di infrastruttura e applicazione consiste nell'operare su larga scala. Se disponi di applicazioni Web, puoi utilizzare i sistemi di bilanciamento del carico

per distribuire il traffico su una serie di EC2 istanze Amazon sovradimensionate o configurate per la scalabilità automatica. Queste istanze sono in grado di gestire picchi di traffico improvvisi che si verificano per qualsiasi motivo, tra cui un flash crowd o un attacco a livello di applicazione. DDoS Puoi impostare CloudWatch allarmi Amazon per avviare Auto Scaling per ridimensionare automaticamente le dimensioni della tua flotta EC2 Amazon in risposta a eventi da te definitiRAM, CPU come I/O di rete e persino metriche personalizzate.

Questo approccio protegge la disponibilità delle applicazioni in caso di aumento imprevisto del volume delle richieste. Quando utilizzi Amazon CloudFront, Application Load Balancer, Classic Load Balancers o Network Load Balancer con la tua applicazione, la TLS negoziazione viene gestita dalla distribuzione (Amazon) o dal load balancer. CloudFront Queste funzionalità aiutano a proteggere le istanze dall'impatto di attacchi TLS mirati grazie alla scalabilità necessaria per gestire richieste legittime e attacchi di abuso. TLS

Per ulteriori informazioni sull'utilizzo di Amazon per CloudWatch richiamare Auto Scaling, consulta Monitoraggio dei parametri CloudWatch Amazon per i gruppi e le istanze di Auto Scaling.

Amazon EC2 offre una capacità di elaborazione ridimensionabile in modo da poter scalare rapidamente verso l'alto o verso il basso man mano che i requisiti cambiano. Puoi scalare orizzontalmente aggiungendo automaticamente istanze alla tua applicazione scalando le dimensioni del tuo gruppo Amazon EC2 Auto Scaling e puoi scalare verticalmente utilizzando tipi di istanze più grandi. EC2

Utilizzando Amazon RDS Proxy, puoi consentire alle tue applicazioni di raggruppare e condividere connessioni al database per migliorare la loro capacità di scalare e gestire picchi imprevedibili del traffico del database. Puoi anche abilitare l'auto-scaling dello storage per un'istanza di database AmazonRDS. Per ulteriori informazioni, consulta Gestire la capacità automaticamente con Amazon RDS Storage Autoscaling.

Elastic Load Balancing () BP6

DDoSGli attacchi di grandi dimensioni possono sovraccaricare la capacità di una singola EC2 istanza Amazon. Con Elastic Load Balancing (ELB), puoi ridurre il rischio di sovraccarico dell'applicazione distribuendo il traffico su molte istanze di backend. Elastic Load Balancing è in grado di scalare automaticamente, consentendoti di gestire volumi maggiori in caso di traffico extra imprevisto, ad esempio a causa di attacchi o affollamenti improvvisi. DDoS Per le applicazioni create all'interno di AmazonVPC, ci sono tre tipi ELBs da considerare, a seconda del tipo di applicazione: Application Load Balancer (ALB), Network Load Balancer () e Classic Load Balancer NLB (). CLB

Per le applicazioni Web, è possibile utilizzare Application Load Balancer per indirizzare il traffico in base ai contenuti e accettare solo richieste Web ben formate. Application Load Balancer blocca molti DDoS attacchi comuni, come SYN floods o attacchi di UDP riflessione, proteggendo l'applicazione dagli attacchi. Application Load Balancer si ridimensiona automaticamente per assorbire il traffico aggiuntivo quando vengono rilevati questi tipi di attacchi. Le attività di scalabilità dovute agli attacchi a livello di infrastruttura sono trasparenti per AWS i clienti e non influiscono sulla bolletta.

Per ulteriori informazioni sulla protezione delle applicazioni Web con Application Load Balancer, consulta Getting Started with Application Load Balancer.

Per HTTPS le applicazioni diverse daHTTP/, puoi utilizzare Network Load Balancer per indirizzare il traffico verso obiettivi (ad esempio, EC2 istanze Amazon) con una latenza estremamente bassa. Una considerazione fondamentale di Network Load Balancer è che tutto il UDP traffico che raggiunge il load balancer su un listener valido verrà indirizzato alle destinazioni, non assorbito, tuttavia ciò non si applica ai TLS -listener che interrompono la connessione. TCP SYN TCP Per i Network Load Balancer con TCP listener, consigliamo di implementare Global Accelerator per proteggersi dalle inondazioni. SYN

È possibile utilizzare Shield Advanced per configurare DDoS la protezione per gli indirizzi IP elastici. Quando viene assegnato un indirizzo IP elastico per zona di disponibilità al Network Load Balancer, Shield Advanced applicherà DDoS le protezioni pertinenti per il traffico Network Load Balancer.

Per ulteriori informazioni sulla protezione TCP e sulle UDP applicazioni con Network Load Balancer, consulta Guida introduttiva a Network Load Balancer.

> **Note**
>
> A seconda della configurazione del gruppo di sicurezza, è necessario che la risorsa che utilizza il gruppo security to group utilizzi il tracciamento delle connessioni per tenere traccia delle informazioni sul traffico. Ciò può influire sulla capacità del sistema di bilanciamento del carico di elaborare nuove connessioni, poiché il numero di connessioni tracciate è limitato. Una configurazione del gruppo di sicurezza che contiene una regola di ingresso che accetta il traffico da qualsiasi indirizzo IP (ad esempio, `0.0.0.0/0` o `::/0`) ma non dispone di una regola corrispondente per consentire il traffico di risposta, fa sì che il gruppo di sicurezza utilizzi le informazioni di tracciamento della connessione per consentire l'invio del traffico di risposta. In caso di DDoS attacco, il numero massimo di connessioni tracciate può essere esaurito. Per migliorare la DDoS resilienza del tuo Application Load Balancer o Classic Load Balancer rivolto al pubblico, assicurati che il gruppo di sicurezza associato al tuo sistema di bilanciamento del carico sia configurato per non utilizzare il tracciamento delle connessioni

(connessioni non tracciate), in modo che il flusso di traffico non sia soggetto ai limiti di tracciamento delle connessioni.
A tal fine, configura il tuo gruppo di sicurezza con una regola che consenta alla regola in entrata di accettare TCP flussi da qualsiasi indirizzo IP (`0.0.0.0/0`o`::/0`) e aggiungi una regola corrispondente nella direzione in uscita che consenta a questa risorsa di inviare il traffico di risposta (consenti l'intervallo in uscita per qualsiasi indirizzo IP `0.0.0.0/0` o`::/0`) per tutte le porte (0-65535), in modo che il traffico di risposta sia consentito in base alla regola del gruppo di sicurezza e non alle informazioni di tracciamento. Con questa configurazione, Classic e Application Load Balancer non sono soggetti ai limiti di tracciamento delle connessioni in uscita che possono influire sulla creazione di nuove connessioni ai relativi nodi di bilanciamento del carico e ne consente la scalabilità in base all'aumento del traffico in caso di attacco. DDoS Ulteriori informazioni sulle connessioni non tracciate sono disponibili all'indirizzo: Tracciamento delle connessioni del gruppo di sicurezza: connessioni non tracciate.
Evitare il tracciamento delle connessioni del gruppo di sicurezza è utile solo nei casi in cui il DDoS traffico proviene da una fonte consentita dal gruppo di sicurezza: il DDoS traffico proveniente da fonti non consentite nel gruppo di sicurezza non influisce sul tracciamento delle connessioni. La riconfigurazione dei gruppi di sicurezza per evitare il tracciamento delle connessioni non è necessaria in questi casi, ad esempio, se l'elenco dei gruppi di sicurezza consentiti è composto da intervalli di IP con i quali si ha un elevato grado di fiducia, ad esempio un firewall aziendale o un indirizzo di uscita affidabile VPN o. IPs CDNs

Utilizza le sedi AWS Edge per la scalabilità (,) BP1 BP3

L'accesso a connessioni Internet diversificate e altamente scalabili può aumentare in modo significativo la capacità di ottimizzare la latenza e la velocità effettiva per gli utenti, di assorbire gli DDoS attacchi e di isolare i guasti riducendo al minimo l'impatto sulla disponibilità dell'applicazione. AWS le edge location forniscono un ulteriore livello di infrastruttura di rete che offre questi vantaggi a qualsiasi applicazione Web che utilizza Amazon CloudFront, Global Accelerator e Amazon Route 53. Con questi servizi, puoi proteggere in modo completo sull'edge le tue applicazioni in esecuzione. Regioni AWS

Distribuzione di applicazioni Web all'edge () BP1

Amazon CloudFront è un servizio che può essere utilizzato per fornire l'intero sito Web, inclusi contenuti statici, dinamici, in streaming e interattivi. Le connessioni persistenti e le impostazioni

variabili time-to-live (TTL) possono essere utilizzate per scaricare il traffico dall'origine, anche se non offri contenuti memorizzabili nella cache. L'uso di queste CloudFront funzionalità riduce il numero di richieste e TCP connessioni di ritorno all'origine, contribuendo a proteggere l'applicazione Web dalle inondazioni. HTTP

CloudFront accetta solo connessioni ben formate, il che aiuta a prevenire che molti DDoS attacchi comuni, come SYN alluvioni e attacchi di UDP riflessione, raggiungano l'origine. DDoSgli attacchi sono inoltre isolati geograficamente vicino alla fonte, il che impedisce al traffico di influire su altre località. Queste funzionalità possono migliorare notevolmente la capacità di continuare a servire il traffico agli utenti durante attacchi di grandi dimensioni. DDoS Puoi utilizzarle CloudFront per proteggere un'origine su Internet AWS o altrove.

Se utilizzi Amazon Simple Storage Service (Amazon S3) per distribuire contenuti statici su Internet, ti consigliamo di AWS utilizzare Amazon CloudFront per proteggere il tuo bucket con i seguenti vantaggi:

- Limita l'accesso al bucket Amazon S3 in modo che non sia accessibile al pubblico.
- Garantisce che gli spettatori (utenti) possano accedere al contenuto del bucket solo attraverso la CloudFront distribuzione specificata, ovvero impedisce loro di accedere ai contenuti direttamente dal bucket o tramite una distribuzione involontaria. CloudFront

A tal fine, configura CloudFront l'invio di richieste autenticate ad Amazon S3 e configura Amazon S3 per consentire l'accesso solo alle richieste autenticate da. CloudFront CloudFront offre due modi per inviare richieste autenticate a un'origine Amazon S3: origin access control OAC () e origin access identity OAI (). Consigliamo di utilizzarlo OAC perché supporta:

- Tutti i bucket Amazon S3 in totale Regioni AWS, comprese le regioni opt-in lanciate dopo dicembre 2022
- Crittografia lato server Amazon S3 con (-) AWS KMS SSE KMS
- Richieste dinamiche (`PUT` e `DELETE`) su Amazon S3

Per ulteriori informazioni su OAC eOAI, consulta Limitazione dell'accesso all'origine di Amazon S3.

Per ulteriori informazioni sulla protezione e l'ottimizzazione delle prestazioni delle applicazioni Web con Amazon CloudFront, consulta Getting Started with Amazon CloudFront.

Proteggi ulteriormente il traffico di rete dalla tua origine utilizzando AWS Global Accelerator () BP1

Global Accelerator è un servizio di rete che migliora la disponibilità e le prestazioni del traffico degli utenti fino al 60%. Ciò si ottiene immettendo il traffico nella posizione periferica più vicina agli utenti e instradandolo attraverso l'infrastruttura di rete AWS globale verso l'applicazione, indipendentemente dal fatto che venga eseguita in una o più applicazioni. Regioni AWS

Global Accelerator indirizza TCP e UDP traffico verso l'endpoint ottimale in base alle prestazioni nel punto più vicino all'utente. Regione AWS In caso di errore dell'applicazione, Global Accelerator fornisce il failover all'endpoint migliore successivo entro 30 secondi. Global Accelerator utilizza la vasta capacità della rete AWS globale e le integrazioni con Shield, come una funzionalità SYN proxy stateless che sfida i nuovi tentativi di connessione e serve solo utenti finali legittimi, per proteggere le applicazioni.

È possibile implementare un'architettura DDoS resiliente che offra molti degli stessi vantaggi delle best practice di Web Application Delivery at the Edge, anche se l'applicazione utilizza protocolli non supportati da CloudFront o se si utilizza un'applicazione Web che richiede indirizzi IP statici globali.

Ad esempio, potreste richiedere indirizzi IP che gli utenti finali possano aggiungere all'elenco degli indirizzi consentiti nei loro firewall e che non vengano utilizzati da altri AWS clienti. In questi scenari è possibile utilizzare Global Accelerator per proteggere le applicazioni Web in esecuzione su Application Load Balancer e, in combinazione, anche per rilevare e mitigare AWS WAF i flood di richieste a livello di applicazione Web.

Per ulteriori informazioni sulla protezione e l'ottimizzazione delle prestazioni del traffico di rete utilizzando Global Accelerator, consulta Guida introduttiva a Global Accelerator.

Risoluzione dei nomi di dominio all'edge () BP3

Argomenti

- Utilizzo di Route 53 per DNS la disponibilità
- Configurazione di Route 53 per la protezione dei costi dagli attacchi NXDOMAIN

Utilizzo di Route 53 per DNS la disponibilità

Amazon Route 53 è un servizio Domain Name System (DNS) altamente disponibile e scalabile che può essere utilizzato per indirizzare il traffico verso la tua applicazione web. Include funzionalità

avanzate come Traffic Flow, Health Checks and Monitoring, Latency-Based Routing e Geo. DNS Queste funzionalità avanzate consentono di controllare il modo in cui il servizio risponde alle DNS richieste per migliorare le prestazioni dell'applicazione Web ed evitare interruzioni del sito. È l'unico AWS servizio con una disponibilità del piano dati del 100%. SLA

Amazon Route 53 utilizza tecniche come lo shuffle sharding e lo striping anycast, che possono aiutare gli utenti ad accedere alla tua applicazione anche se il DNS servizio è preso di mira da un attacco. DDoS

Con lo shuffle sharding, ogni name server del set di delega corrisponde a un set unico di edge location e percorsi Internet. Ciò offre una maggiore tolleranza agli errori e riduce al minimo la sovrapposizione tra i clienti. Se un name server del set di delega non è disponibile, gli utenti possono riprovare e ricevere una risposta da un altro name server in un'altra edge location.

Lo striping Anycast consente di DNS soddisfare ogni richiesta dalla posizione più ottimale, disperdendo il carico di rete e riducendo la latenza. DNS Ciò fornisce una risposta più rapida per gli utenti. Inoltre, Amazon Route 53 è in grado di rilevare anomalie nell'origine e nel volume delle DNS query e assegnare priorità alle richieste di utenti noti per la loro affidabilità.

Per ulteriori informazioni sull'uso di Amazon Route 53 per indirizzare gli utenti alla tua applicazione, consulta Getting Started with Amazon Route 53.

Configurazione di Route 53 per la protezione dei costi dagli attacchi **NXDOMAIN**

`NXDOMAIN`gli attacchi si verificano quando gli aggressori inviano una marea di richieste a una zona ospitata per sottodomini inesistenti, spesso tramite resolver «validi» noti. Lo scopo di questi attacchi può essere quello di influire sulla cache del resolver ricorsivo e/o sulla disponibilità del resolver autoritativo, oppure potrebbe essere una forma di ricognizione per cercare di scoprire i record delle zone ospitate. DNS L'utilizzo di Route 53 come resolver autoritativo riduce il rischio di impatto sulla disponibilità e sulle prestazioni, tuttavia il risultato può essere un aumento significativo dei costi mensili di Route 53. Per proteggerti dagli aumenti dei costi, approfitta dei prezzi di Route 53, in cui le DNS query sono gratuite quando sono soddisfatte entrambe le seguenti condizioni:

- Il nome di dominio o sottodominio (`example.comorstore.example.com`) e il tipo di record (`A`) nella query corrispondono a un record di alias.
- La destinazione dell'alias è una AWS risorsa diversa da un altro record della Route 53.

Crea un record con caratteri jolly, ad esempio, `*.example.com` con un tipo `A` (Alias) che punti a una AWS risorsa come un'EC2istanza, Elastic Load Balancer CloudFront o una distribuzione, in modo

che quando viene effettuata una query `qwerty12345.example.com` per, venga restituito l'IP della risorsa e non ti venga addebitato alcun costo per la query.

Difesa a livello di applicazione (,) BP1 BP2

Molte delle tecniche discusse finora in questo paper sono efficaci nel mitigare l'impatto DDoS degli attacchi a livello di infrastruttura sulla disponibilità dell'applicazione. Per difendersi anche dagli attacchi a livello applicativo, è necessario implementare un'architettura che consenta di rilevare, scalare in modo specifico per assorbire e bloccare le richieste dannose. Questa è una considerazione importante perché i sistemi di DDoS mitigazione basati sulla rete sono generalmente inefficaci nel mitigare attacchi complessi a livello applicativo.

Rileva e filtra le richieste web dannose (,) BP1 BP2

Quando la tua applicazione è in esecuzione AWS, puoi sfruttare Amazon CloudFront (e la sua capacità di HTTP memorizzazione nella cache) e la protezione a livello di applicazione automatica Shield Advanced per evitare che richieste non necessarie raggiungano la tua origine durante gli attacchi a livello DDoS di applicazione. AWS WAF

Amazon CloudFront

Amazon CloudFront può aiutarti a ridurre il carico del server impedendo al traffico non Web di raggiungere la tua origine. Per inviare una richiesta a un' CloudFront applicazione, è necessario stabilire la connessione con un indirizzo IP valido tramite un TCP handshake completato, che non può essere falsificato. Inoltre, CloudFront può chiudere automaticamente le connessioni da aggressori che eseguono operazioni di lettura o scrittura lenta (ad esempio, Slowloris).

Caching CDN

CloudFront consente di fornire contenuti dinamici e contenuti statici da postazioni periferiche. AWS Fornendo contenuti memorizzabili CDN nella cache tramite proxy, si impedisce che le richieste arrivino all'origine da un determinato nodo di cache edge per tutta la durata della memorizzazione nella cache. TTL Oltre alla compressione delle richieste relative a contenuti scaduti ma inseribili nella cache, anche quelle molto brevi TTL significano che un numero trascurabile di richieste arriverà all'origine durante il flusso di richieste relative a quel contenuto. Inoltre, abilitare funzionalità come CloudFront Origin Shield può contribuire ulteriormente a ridurre il carico sull'origine: qualsiasi cosa tu possa fare per migliorare l'hit ratio della cache può fare la differenza tra un attacco di tipo Request Flood con impatto e uno senza impatto.

AWS WAF

Utilizzando AWS WAF, puoi configurare liste di controllo degli accessi Web (WebACLs) sulle tue CloudFront distribuzioni globali o sulle risorse regionali per filtrare, monitorare e bloccare le richieste in base alle firme delle richieste. Per determinare se consentire o bloccare le richieste, puoi prendere in considerazione fattori come l'indirizzo IP o il paese di origine, determinate stringhe o schemi nella richiesta, la dimensione di parti specifiche della richiesta e la presenza di SQL codice o script dannosi. Puoi anche eseguire CAPTCHA enigmi e sfidare sessioni client silenziose contro le richieste.

Entrambi AWS WAF consentono CloudFront anche di impostare restrizioni geografiche per bloccare o consentire le richieste provenienti da paesi selezionati. Questo può aiutare a bloccare o limitare la frequenza degli attacchi provenienti da aree geografiche in cui non si prevede di servire gli utenti. Inserendo istruzioni dettagliate sulle regole di corrispondenza geografica AWS WAF, puoi controllare l'accesso fino al livello di regione.

È possibile utilizzare le istruzioni Scope-down per restringere l'ambito delle richieste valutate dalla regola per ridurre i costi ed «etichettare» le richieste Web per consentire a una regola che corrisponde alla richiesta di comunicare i risultati delle corrispondenze alle regole che vengono valutate successivamente nello stesso Web. ACL Scegli questa opzione per riutilizzare la stessa logica su più regole.

Puoi anche definire una risposta personalizzata completa, con codice di risposta, intestazioni e corpo.

Per aiutare a identificare le richieste dannose, esaminate i log AWS WAF del server Web o utilizzate il logging e il campionamento delle richieste. AWS WAF Abilitando la registrazione, otterrete informazioni dettagliate sul traffico analizzato dal Web. ACL AWS WAF supporta il filtraggio dei log, che consente di specificare quali richieste Web vengono registrate e quali richieste vengono eliminate dal registro dopo l'ispezione.

Le informazioni registrate nei log includono l'ora in cui è AWS WAF stata ricevuta la richiesta dalla AWS risorsa, informazioni dettagliate sulla richiesta e l'azione corrispondente per ogni regola richiesta.

Le richieste campionate forniscono dettagli sulle richieste delle ultime tre ore che corrispondono a una delle tue regole. AWS WAF Puoi utilizzare queste informazioni per identificare le segnaletiche stradali potenzialmente dannose e creare una nuova regola per rifiutare tali richieste. Se vedi un certo numero di richieste con una stringa di query casuale, assicurati di consentire solo i parametri della stringa di query pertinenti alla cache dell'applicazione. Questa tecnica è utile per mitigare un attacco di cache busting contro l'origine.

AWS WAF — Regole basate sulla tariffa

AWS consiglia vivamente di proteggersi dal HTTP sovraffollamento di richieste utilizzando le regole basate sulla frequenza AWS WAF per bloccare automaticamente gli indirizzi IP dei malintenzionati quando il numero di richieste ricevute in una finestra scorrevole di 5 minuti supera una soglia definita dall'utente. Gli indirizzi IP dei client offensivi riceveranno una risposta proibita 403 (o una risposta di errore di blocco configurata) e rimarranno bloccati fino a quando la frequenza delle richieste non scenderà al di sotto della soglia.

Si consiglia di stratificare le regole basate sulla frequenza per fornire una protezione avanzata in modo da avere:

- Una regola generale basata sulla tariffa per proteggere l'applicazione da alluvioni di grandi dimensioni. HTTP
- Una o più regole basate sulle tariffe per proteggere aliquote specifiche e più restrittive rispetto URIs alla regola generale basata sulle tariffe.

Ad esempio, puoi scegliere una regola generica basata sulla tariffa (nessuna dichiarazione riduttiva) con un limite di 500 richieste in un periodo di 5 minuti e quindi creare una o più delle seguenti regole basate sulla tariffa con limiti inferiori a 500 (fino a 100 richieste in un periodo di 5 minuti) utilizzando istruzioni con ambito limitato:

- Proteggi le tue pagine Web con un'istruzione delimitata come ""`if NOT uri_path contains '.'`, in modo che le richieste di risorse senza estensione di file siano ulteriormente protette. In questo modo si protegge anche la home page (`/`), che è spesso un percorso mirato. URI
- Proteggi gli endpoint dinamici con un'istruzione «scope-down» come "» `if method exactly matches 'post' (convert lowercase)`
- Proteggi le richieste più complesse che raggiungono il tuo database o richiama una password monouso (OTP) con un ambito decrescente come "» `if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

I sistemi basati sulla tariffa in modalità «Block» sono alla base della defense-in-depth WAF configurazione per la protezione contro il sovraffollamento di richieste e sono un requisito fondamentale per l'approvazione delle richieste di protezione dei costi. AWS Shield Advanced Esamineremo le defense-in-depth WAF configurazioni aggiuntive nelle seguenti sezioni.

AWS WAF — Reputazione IP

Per prevenire attacchi basati sulla reputazione degli indirizzi IP, è possibile creare regole utilizzando IP matching o utilizzare Managed Rules for AWS WAF.

Il gruppo di regole dell'elenco di reputazione IP di Amazon include regole basate sull'intelligence interna di Amazon sulle minacce. Queste regole cercano indirizzi IP che siano bot, che eseguono ricognizioni AWS sulle risorse o che partecipano attivamente ad attività. DDoS È stato osservato che la `AWSManagedIPDDoSList` regola blocca oltre il 90% dei flussi di richieste dannose.

Il gruppo di regole dell'elenco di IP anonimi contiene regole per bloccare le richieste provenienti da servizi che consentono l'offuscamento dell'identità degli spettatori. Queste includono richieste provenienti daVPNs, proxy, nodi Tor e piattaforme cloud (escluse). AWS

Inoltre, puoi utilizzare elenchi di reputazione IP di terze parti utilizzando il componente parser IP Lists della soluzione Security Automations for. AWS WAF

AWS WAF - Mitigazione intelligente delle minacce

Le botnet rappresentano una grave minaccia alla sicurezza e vengono comunemente utilizzate per svolgere attività illegali o dannose come l'invio di spam, il furto di dati sensibili, l'avvio di attacchi ransomware, la commissione di frodi pubblicitarie tramite clic fraudolenti o il lancio di attacchi distribuiti (). denial-of-service DDoS Per prevenire gli attacchi dei bot, utilizzate il gruppo di regole gestito da Bot Control.AWS WAF Questo gruppo di regole fornisce un livello di protezione di base «Comune» che aggiunge etichette ai bot che si identificano automaticamente, verifica i bot generalmente desiderati e rileva le firme dei bot ad alta affidabilità e un livello di protezione «mirato» che aggiunge il rilevamento per i bot avanzati che non si identificano automaticamente.

Le protezioni mirate utilizzano tecniche di rilevamento avanzate come l'interrogazione del browser, l'impronta digitale e l'euristica del comportamento per identificare il traffico di bot non valido e quindi applicano controlli di mitigazione come la limitazione della velocità CAPTCHA e le azioni delle regole Challenge. Targeted offre anche opzioni di limitazione della velocità per imporre modelli di accesso simili a quelli umani e applicare una limitazione dinamica della velocità tramite l'uso di token di richiesta. Per ulteriori dettagli, consulta il gruppo di regole Bot Control.AWS WAF Per rilevare e gestire i tentativi di acquisizione malevoli sulla pagina di accesso dell'applicazione, puoi utilizzare il gruppo di regole AWS WAF Fraud Control account takeover prevention (ATP). Il gruppo di regole esegue questa operazione esaminando i tentativi di accesso che i client inviano all'endpoint di accesso dell'applicazione e controlla anche le risposte dell'applicazione ai tentativi di accesso, per monitorare il tasso di successo e di fallimento.

La frode nella creazione di account è un'attività illegale online in cui un utente malintenzionato tenta di creare uno o più account falsi. Gli aggressori utilizzano account falsi per attività fraudolente come l'abuso di bonus promozionali e di iscrizione, l'impersonificazione di qualcuno e attacchi informatici come il phishing. La presenza di account falsi può avere un impatto negativo sulla vostra attività, danneggiando la vostra reputazione presso i clienti ed esponendovi a frodi finanziarie.

Puoi monitorare e controllare i tentativi di frode nella creazione di account implementando la funzione di prevenzione delle AWS WAF frodi nella creazione di account Fraud Control (ACFP). AWS WAF offre questa funzionalità nel gruppo di Regole gestite da AWS regole `AWS ManagedRulesACFPRuleSet` con l'integrazione di applicazioni complementariSDKs.

Scopri di più su queste protezioni nella mitigazione AWS WAF intelligente delle minacce.

Mitiga automaticamente gli eventi a livello di applicazione (,,) DDoS BP1 BP2 BP6

Se sei abbonato AWS Shield Advanced, puoi abilitare la DDoSmitigazione automatica del livello di applicazione Shield Advanced. Questa funzionalità crea, valuta e implementa automaticamente AWS WAF regole per mitigare gli eventi di livello 7 DDoS per conto dell'utente.

AWS Shield Advanced stabilisce una linea di base del traffico per ogni risorsa protetta associata a un Web. WAF ACL Il traffico che si discosta in modo significativo dalla linea di base stabilita viene contrassegnato come evento potenziale. DDoS Dopo il rilevamento di un evento, AWS Shield Advanced tenta di identificare una firma delle richieste Web che costituiscono l'evento e, se viene identificata una firma, vengono create AWS WAF regole per mitigare il traffico con quella firma.

Una volta che le regole sono state valutate rispetto alla linea di base storica e ritenute sicure, vengono aggiunte al gruppo di regole gestito da Shield e puoi scegliere se implementarle in modalità conteggio o blocco. Shield Advanced rimuove automaticamente AWS WAF le regole dopo aver stabilito che un evento si è completamente attenuato.

Engage SRT (solo abbonati Shield Advanced)

Inoltre, se sei abbonato a Shield Advanced, puoi AWS SRT coinvolgerli per aiutarti a creare regole per mitigare un attacco che compromette la disponibilità dell'applicazione. Puoi concedere un accesso AWS SRT limitato al tuo account e. AWS Shield Advanced AWS WAF APIs AWS SRTaccede APIs a questi per applicare mitigazioni sul tuo account solo con la tua autorizzazione esplicita. Per ulteriori informazioni, consulta la Supporto sezione di questo documento.

È possibile utilizzarlo AWS Firewall Manager per configurare e gestire centralmente le regole di sicurezza, come AWS Shield Advanced protezioni e AWS WAF regole, in tutta l'organizzazione. L'account di AWS Organizations gestione può designare un account amministratore, che è autorizzato a creare politiche di Firewall Manager. Queste politiche consentono di definire criteri, come il tipo di risorsa e i tag, che determinano dove vengono applicate le regole. Ciò è utile quando si dispone di più account e si desidera standardizzare la protezione.

Per ulteriori informazioni su:

- Regole gestite da AWS per AWS WAF, fare riferimento a Regole gestite da AWS for AWS WAF.
- Utilizzo della restrizione geografica per limitare l'accesso alla CloudFront distribuzione, consulta Limitazione della distribuzione geografica dei contenuti.
- Per quanto riguarda l'uso AWS WAF, fai riferimento a:
  - Guida introduttiva con AWS WAF
  - Registrazione delle informazioni sul ACL traffico web
  - Visualizzazione di un esempio di richieste Web
- Configurazione delle regole basate sulla tariffa, fare riferimento a Protezione di siti Web e servizi tramite regole basate sulla tariffa per. AWS WAF
- Come gestire l'implementazione delle regole tra le tue AWS risorse con Firewall Manager, vedi:
  - Guida introduttiva alle AWS WAF politiche di Firewall Manager.
  - Guida introduttiva alle policy di Firewall Manager Shield Advanced.

Riduzione della superficie di attacco

Un'altra considerazione importante quando si progetta una AWS soluzione è limitare le opportunità che un utente malintenzionato ha di prendere di mira l'applicazione. Questo concetto è noto come riduzione della superficie di attacco. Le risorse che non sono esposte a Internet sono più difficili da attaccare, il che limita le opzioni a disposizione di un utente malintenzionato per prendere di mira la disponibilità dell'applicazione.

Ad esempio, se non vi aspettate che gli utenti interagiscano direttamente con determinate risorse, assicuratevi che tali risorse non siano accessibili da Internet. Analogamente, non accettate il traffico proveniente da utenti o applicazioni esterne su porte o protocolli che non sono necessari per la comunicazione.

Nella sezione seguente, vengono AWS fornite le migliori pratiche per aiutarvi a ridurre la superficie di attacco e limitare l'esposizione dell'applicazione a Internet.

AWS Risorse offuscanti (,,) BP1 BP4 BP5

In genere, gli utenti possono utilizzare un'applicazione in modo rapido e semplice senza richiedere che AWS le risorse siano completamente esposte a Internet.

Gruppi di sicurezza e rete ACLs (BP5)

Amazon Virtual Private Cloud (AmazonVPC) consente di effettuare il provisioning di una sezione logicamente isolata della Cloud AWS quale è possibile avviare AWS risorse in una rete virtuale definita dall'utente.

I gruppi di sicurezza e la rete ACLs sono simili in quanto consentono di controllare l'accesso alle AWS risorse all'interno dell'aziendaVPC. Tuttavia, i gruppi di sicurezza consentono di controllare il traffico in entrata e in uscita a livello di istanza, mentre la rete ACLs offre funzionalità simili a livello di VPC sottorete. Non sono previsti costi aggiuntivi per l'utilizzo dei gruppi di sicurezza o della rete. ACLs

È possibile scegliere se specificare i gruppi di sicurezza all'avvio di un'istanza o associare l'istanza a un gruppo di sicurezza in un secondo momento. Tutto il traffico Internet verso un gruppo di sicurezza viene negato implicitamente a meno che non si crei una regola di autorizzazione per consentire il traffico.

Ad esempio, se hai EC2 istanze Amazon dietro un Elastic Load Balancer, non è necessario che le istanze stesse siano accessibili pubblicamente e dovrebbero essere solo private. IPs È possibile invece fornire a Elastic Load Balancer l'accesso alle porte listener di destinazione richieste utilizzando una regola del gruppo di sicurezza che consente l'accesso a 0.0.0.0/0 (per evitare problemi di tracciamento della connessione, vedere la nota seguente) insieme a una Network Access Control List (NACL) sulla sottorete del gruppo di destinazione per consentire solo agli intervalli IP di Elastic Load Balancing di comunicare con le istanze. Ciò garantisce che il traffico Internet non possa comunicare direttamente con le tue EC2 istanze Amazon, il che rende più difficile per un utente malintenzionato conoscere e influenzare la tua applicazione.

Quando crei una reteACLs, puoi specificare sia le regole di autorizzazione che quelle di rifiuto. Ciò è utile se desideri negare esplicitamente determinati tipi di traffico alla tua applicazione. Ad esempio, è possibile definire indirizzi IP (come CIDR intervalli), protocolli e porte di destinazione a cui viene negato l'accesso all'intera sottorete. Se l'applicazione viene utilizzata solo per il TCP traffico, è possibile creare una regola per negare tutto il UDP traffico o viceversa. Questa opzione è utile per rispondere agli DDoS attacchi perché consente di creare regole personalizzate per mitigare l'attacco quando si conosce l'origine IPs o un'altra firma.

Se sei abbonato AWS Shield Advanced, puoi registrare gli indirizzi IP elastici come risorse protette. DDoSgli attacchi contro gli indirizzi IP elastici che sono stati registrati come risorse protette vengono rilevati più rapidamente, il che può comportare tempi di mitigazione più rapidi. Quando viene rilevato un attacco, i sistemi di DDoS mitigazione leggono la rete ACL che corrisponde all'indirizzo IP elastico mirato e la applicano ai confini della AWS rete, anziché a livello di sottorete. Ciò riduce in modo significativo il rischio di impatto derivante da una serie di attacchi a livello di infrastruttura. DDoS

Per ulteriori informazioni sulla configurazione dei gruppi di sicurezza e della rete ACLs per ottimizzare DDoS la resilienza, consulta Come prepararsi DDoS agli attacchi riducendo la superficie di attacco.

Per ulteriori informazioni sull'utilizzo di Shield Advanced con indirizzi IP elastici come risorse protette, consulta la procedura di sottoscrizione a AWS Shield Advanced.

Proteggere la propria origine (BP1,BP5)

Se utilizzi Amazon CloudFront con un'origine interna alla tuaVPC, potresti voler assicurarti che solo la tua CloudFront distribuzione possa inoltrare le richieste alla tua origine. Con Edge-to-Origin Request Headers, puoi aggiungere o sostituire il valore delle intestazioni di richiesta esistenti quando inoltri le richieste all'origine. CloudFront Puoi utilizzare le Origin Custom Headers, ad esempio l'`X-Shared-Secret`intestazione, per verificare da che le richieste inviate all'origine siano state inviate. CloudFront

Per maggiori informazioni sulla protezione dell'origine con Origin Custom Headers, consulta Aggiungere intestazioni personalizzate alle richieste di origine e Limitazione dell'accesso agli Application Load Balancers.

Per una guida sull'implementazione di una soluzione di esempio per ruotare automaticamente il valore di Origin Custom Headers per la restrizione di accesso all'origine, consulta How to enhance Amazon CloudFront origin security with and Secrets AWS WAF Manager.

In alternativa, puoi utilizzare una AWS Lambdafunzione per aggiornare automaticamente le regole del tuo gruppo di sicurezza in modo da consentire solo il traffico. CloudFront Ciò migliora la sicurezza della tua origine contribuendo a garantire che gli utenti malintenzionati non possano aggirare CloudFront e AWS WAF accedere alla tua applicazione web.

Per ulteriori informazioni su come proteggere la tua origine aggiornando automaticamente i gruppi di sicurezza e l'`X-Shared-Secret`intestazione, consulta Come aggiornare automaticamente i tuoi gruppi di sicurezza per Amazon CloudFront e AWS WAF utilizzando AWS Lambda.

Tuttavia, la soluzione prevede una configurazione aggiuntiva e il costo di esecuzione delle funzioni Lambda. Per semplificare questa operazione, abbiamo ora introdotto un elenco AWS di prefissi gestiti per CloudFront limitare il HTTPS traffico in HTTP entrata/alle origini solo dagli indirizzi IP rivolti all' CloudFrontorigine. AWS-gli elenchi di prefissi gestiti vengono creati e gestiti da AWS e sono disponibili per l'uso senza costi aggiuntivi. Puoi fare riferimento all'elenco dei prefissi gestiti CloudFront nelle regole del gruppo di sicurezza (AmazonVPC), nelle tabelle di routing delle subnet, nelle regole comuni dei gruppi di sicurezza e in qualsiasi altra AWS risorsa che può utilizzare un elenco di prefissi gestiti. AWS Firewall Manager

Per ulteriori informazioni sull'utilizzo di AWS-managed prefix list per Amazon CloudFront, consulta Limita l'accesso alle tue origini utilizzando l'elenco di prefissi AWS-managed per Amazon. CloudFront

> **Note**
>
> Come discusso in altre sezioni di questo documento, affidarsi a gruppi di sicurezza per proteggere la propria origine può aggiungere il tracciamento delle connessioni dei gruppi di sicurezza come potenziale ostacolo durante un'ondata di richieste. A meno che non siate in grado di filtrare le richieste dannose CloudFront utilizzando una politica di memorizzazione nella cache che abiliti la memorizzazione nella cache, potrebbe essere meglio affidarsi alle Origin Custom Headers, discusse in precedenza, per verificare che le richieste inviate all'origine provengano da gruppi di sicurezza, anziché utilizzare gruppi di sicurezza. CloudFront L'utilizzo di un'intestazione di richiesta personalizzata con una regola del listener

Application Load Balancer impedisce la limitazione dovuta ai limiti di tracciamento che possono influire sulla creazione di nuove connessioni a un sistema di bilanciamento del carico, permettendo così ad Application Load Balancer di scalare in base all'aumento del traffico in caso di attacco. DDoS

Protezione degli endpoint () API BP4

Quando è necessario esporre un file API al pubblico, esiste il rischio che il API frontend venga preso di mira da un attacco. DDoS Per contribuire a ridurre il rischio, puoi utilizzare Amazon API Gateway come accesso alle applicazioni in esecuzione su Amazon EC2 o AWS Lambda altrove. Utilizzando Amazon API Gateway, non sono necessari server propri per il API frontend e si possono offuscare altri componenti dell'applicazione. Rendendo più difficile il rilevamento dei componenti dell'applicazione, puoi contribuire a evitare che tali AWS risorse vengano prese di mira da un attacco. DDoS

Quando usi Amazon API Gateway, puoi scegliere tra due tipi di API endpoint. La prima è l'opzione predefinita: API endpoint ottimizzati per i bordi a cui si accede tramite una distribuzione Amazon. CloudFront Tuttavia, la distribuzione viene creata e gestita da API Gateway, quindi non ne hai il controllo. La seconda opzione consiste nell'utilizzare un API endpoint regionale a cui si accede dallo stesso Regione AWS in cui REST API è distribuito il tuo. AWS consiglia di utilizzare il secondo tipo di endpoint e di associarlo alla propria CloudFront distribuzione Amazon. Questo ti dà il controllo sulla CloudFront distribuzione Amazon e la possibilità di utilizzarla AWS WAF per la protezione a livello di applicazione. Questa modalità fornisce l'accesso a una capacità di DDoS mitigazione scalabile su tutta la rete AWS perimetrale globale.

Quando usi Amazon CloudFront e AWS WAF con Amazon API Gateway, configura le seguenti opzioni:

- Configura il comportamento della cache per le tue distribuzioni per inoltrare tutte le intestazioni all'endpoint regionale API Gateway. In questo modo, CloudFront tratterà il contenuto come dinamico e salterà la memorizzazione nella cache del contenuto.
- Proteggi il tuo API gateway dall'accesso diretto configurando la distribuzione per includere l'intestazione personalizzata di origine x-api-key, impostando il valore della APIchiave in Gateway. API
- Proteggi il backend dal traffico in eccesso configurando limiti standard o di burst rate per ogni metodo utilizzato. REST APIs

Per ulteriori informazioni sulla creazione APIs con Amazon API Gateway, consulta Amazon API Gateway Getting Started.

Tecniche operative

Le tecniche di mitigazione illustrate in questo paper consentono di progettare applicazioni intrinsecamente resilienti agli attacchi. DDoS In molti casi, è anche utile sapere quando un DDoS attacco ha come obiettivo l'applicazione in modo da poter adottare misure di mitigazione. Questa sezione illustra le migliori pratiche per ottenere visibilità su comportamenti anomali, avvisi e automazione, gestire la protezione su larga scala e richiedere supporto aggiuntivo. AWS

Test di caricamento

Testa regolarmente la tua applicazione utilizzando le linee guida del nostro white paper sulle applicazioni di test di carico con livelli di traffico previsti e superiori a quelli previsti, in modo da poter vedere quanto sia efficace la tua architettura, come funzionano le tue politiche di Auto Scaling e come funzionano le tue funzioni di gestione degli errori. Esegui il test per verificare l'aumento e la riduzione del traffico previsto, ma anche per verificare il comportamento di tipo «flash-crowd». Ripeti il test periodicamente o prima di qualsiasi versione principale. Per i test di DDoS simulazione di livello 3 o 4, come SYN flood, segui la nostra politica sui test di DDoSsimulazione.

Parametri e allarmi

Come best practice, è consigliabile utilizzare strumenti di monitoraggio dell'infrastruttura e delle applicazioni per verificare la disponibilità dell'applicazione e garantire che l'applicazione non sia influenzata da un DDoS evento, come opzione è possibile configurare i controlli di integrità dell'applicazione e dell'infrastruttura Route 53 per le risorse per contribuire a migliorare il rilevamento degli DDoS eventi. Per ulteriori informazioni sui controlli di integrità AWS WAF, consulta Firewall Manager and Shield Advanced Developer Guide.

Quando una metrica operativa chiave si discosta in modo sostanziale dal valore previsto, è possibile che un utente malintenzionato stia tentando di prendere di mira la disponibilità dell'applicazione. La familiarità con il normale comportamento dell'applicazione significa che è possibile agire più rapidamente quando si rileva un'anomalia. Amazon CloudWatch può aiutarti monitorando le applicazioni su cui esegui AWS. Ad esempio, puoi raccogliere e tracciare metriche, raccogliere e monitorare file di registro, impostare allarmi e rispondere automaticamente ai cambiamenti nelle tue AWS risorse.

Se si segue l'architettura di riferimento DDoS -resilient durante l'architettura dell'applicazione, gli attacchi comuni a livello di infrastruttura verranno bloccati prima di raggiungere l'applicazione. Se

sei abbonato AWS Shield Advanced, hai accesso a una serie di CloudWatch metriche che possono indicare che la tua applicazione è presa di mira.

Ad esempio, puoi configurare allarmi per avvisarti quando è in corso un DDoS attacco, in modo da poter controllare lo stato dell'applicazione e decidere se attivarla. AWS SRT Puoi configurare la `DDoSDetected` metrica per dirti se è stato rilevato un attacco. Se desideri essere avvisato in base al volume dell'attacco, puoi anche utilizzare le metriche `DDoSAttackBitsPerSecond`DDoSAttackPacketsPerSecond, o`DDoSAttackRequestsPerSecond`. Puoi monitorare queste metriche integrandole CloudWatch con i tuoi strumenti o utilizzando strumenti forniti da terze parti, come Slack o. PagerDuty

Un attacco a livello di applicazione può elevare molti CloudWatch parametri di Amazon. Se lo utilizzi AWS WAF, puoi utilizzarlo CloudWatch per monitorare e attivare allarmi in caso di aumento delle richieste che hai impostato AWS WAF per consentire, conteggiare o bloccare. Ciò ti consente di ricevere una notifica se il livello di traffico supera quello che l'applicazione è in grado di gestire. Puoi anche utilizzare i parametri di Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, EC2 Amazon e Auto Scaling di cui viene CloudWatch tenuta traccia per rilevare le modifiche che possono indicare un attacco. DDoS

La tabella seguente elenca le descrizioni delle CloudWatch metriche comunemente utilizzate per rilevare e reagire agli attacchi. DDoS

Tabella 3 - CloudWatch Metriche Amazon consigliate

Argomento	Parametro	Descrizione
AWS Shield Advanced	`DDoSDetected`	Indica un DDoS evento per uno specifico Amazon Resource Name (ARN).
AWS Shield Advanced	`DDoSAttackBitsPerSecond`	Il numero di byte osservati durante un DDoS evento per uno specificoARN. Questa metrica è disponibile solo per gli eventi di livello 3 o 4DDoS.
AWS Shield Advanced	`DDoSAttackPacketsPerSecond`	Il numero di pacchetti osservati durante un DDoS evento per un determinato

Argomento	Parametro	Descrizione
		evento. ARN Questa metrica è disponibile solo per gli eventi di livello 3 o 4DDoS.
AWS Shield Advanced	`DDoSAttackRequests PerSecond`	Il numero di richieste osservate durante un DDoS evento per uno specificoARN. Questa metrica è disponibi le solo per DDoS gli eventi di livello 7 e viene riportata solo per gli eventi di livello 7 più significativi.
AWS WAF	`AllowedRequests`	Il numero di richieste Web consentite.
AWS WAF	`BlockedRequests`	Il numero di richieste Web bloccate.
AWS WAF	`CountedRequests`	Il numero di richieste Web contate.
AWS WAF	`PassedRequests`	Il numero di richieste passate. Viene utilizzato solo per le richieste che vengono sottoposte a una valutazione del gruppo di regole senza corrispondere a nessuna delle regole del gruppo di regole.
Amazon CloudFront	`Requests`	Il numero di richieste HTTP /S.
Amazon CloudFront	`TotalErrorRate`	La percentuale di tutte le richieste per le quali il codice di HTTP stato è `4xx` o`5xx`.

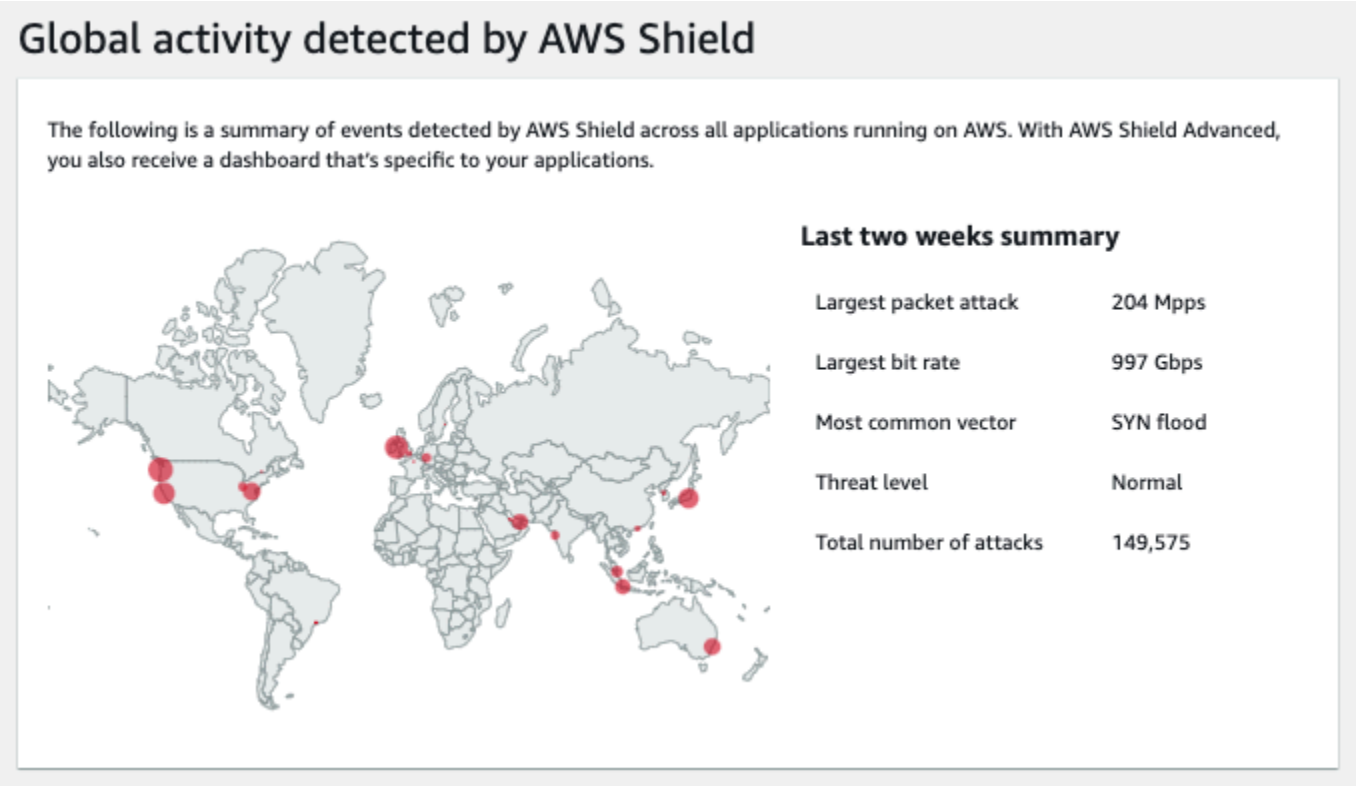
Argomento	Parametro	Descrizione
Amazon Route 53	`HealthCheckStatus`	Lo stato dell'endpoint per il controllo dello stato di salute.
Application Load Balancer	`ActiveConnectionCount`	Il numero totale di TCP connessioni simultanee attive dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico alle destinazioni.
Application Load Balancer	`ConsumedLCUs`	Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal sistema di bilanciamento del carico.
Application Load Balancer	`HTTPCode_ELB_4XX_Count` `HTTPCode_ELB_5XX_Count`	Il numero di codici HTTP `4xx` di errore `5xx` del client generati dal load balancer.
Application Load Balancer	`NewConnectionCount`	Il numero totale di nuove TCP connessioni stabilite dai client al sistema di bilanciamento del carico e dal sistema di bilanciamento del carico alle destinazioni.
Application Load Balancer	`ProcessedBytes`	Il numero totale di byte elaborati dal sistema di bilanciamento del carico.
Application Load Balancer	`RejectedConnectionCount`	Il numero di connessioni respinte perché il sistema di bilanciamento del carico ha raggiunto il numero massimo di connessioni.

Argomento	Parametro	Descrizione
Application Load Balancer	`RequestCount`	Il numero di richieste che sono state elaborate.
Application Load Balancer	`TargetConnectionErrorCount`	Il numero di connessioni che non sono state stabilite correttamente tra il load balancer e la destinazione.
Application Load Balancer	`TargetResponseTime`	Il tempo trascorso, in secondi, dal momento in cui la richiesta ha lasciato il sistema di bilanciamento del carico fino alla ricezione di una risposta dalla destinazione.
Application Load Balancer	`UnHealthyHostCount`	Il numero di target considerati non integri.
Network Load Balancer	`ActiveFlowCount`	Il numero totale di TCP flussi (o connessioni) simultanei dai client alle destinazioni.
Network Load Balancer	`ConsumedLCUs`	Il numero di unità di capacità del sistema di bilanciamento del carico (LCU) utilizzate dal sistema di bilanciamento del carico.
Network Load Balancer	`NewFlowCount`	Il numero totale di nuovi TCP flussi (o connessioni) stabiliti dai client alle destinazioni nel periodo di tempo.

Argomento	Parametro	Descrizione
Network Load Balancer	`ProcessedBytes`	Il numero totale di byte elaborati dal sistema di bilanciamento del carico, incluse le intestazioni TCP /IP.
Global Accelerator	`NewFlowCount`	Il numero totale di UDP flussi (o connessioni) nuovi TCP e stabiliti dai client agli endpoint nel periodo di tempo.
Global Accelerator	`ProcessedBytesIn`	Il numero totale di byte in entrata elaborati dall'acce leratore, incluse le intestazi oni /IP. TCP
Auto Scaling	`GroupMaxSize`	Dimensione massima del gruppo con scalabilità automatica.
Amazon EC2	`CPUUtilization`	La percentuale di unità di EC2 calcolo allocate attualmente in uso.
Amazon EC2	`NetworkIn`	Il numero di byte ricevuti dall'istanza su tutte le interfacc e di rete.

Per ulteriori informazioni sull'utilizzo di Amazon CloudWatch per rilevare DDoS gli attacchi alla tua applicazione, consulta Getting Started with Amazon CloudWatch.

AWS include diverse metriche e allarmi aggiuntivi per avvisarti di un attacco e aiutarti a monitorare le risorse della tua applicazione. AWS Shield Console o API fornisci un riepilogo degli eventi per account e dettagli sugli attacchi rilevati.



Attività globale rilevata da AWS Shield

Inoltre, la dashboard sull'ambiente globale delle minacce fornisce informazioni di riepilogo su tutti DDoS gli attacchi rilevati da AWS. Queste informazioni possono essere utili per comprendere meglio DDoS le minacce su una popolazione più ampia di applicazioni, oltre alle tendenze degli attacchi e al confronto con gli attacchi che potresti aver osservato.

Se sei abbonato AWS Shield Advanced, la dashboard del servizio mostra ulteriori metriche di rilevamento e mitigazione e dettagli sul traffico di rete per gli eventi rilevati sulle risorse protette. AWS Shield valuta il traffico verso la risorsa protetta secondo più dimensioni. Quando viene rilevata un'anomalia, AWS Shield crea un evento e segnala la dimensione del traffico in cui è stata osservata l'anomalia. Con una mitigazione applicata, questo protegge la risorsa dalla ricezione di traffico in eccesso e di traffico corrispondente a un evento notoDDoS.

Le metriche di rilevamento si basano su flussi o AWS WAF registri di rete campionati quando un Web ACL è associato alla risorsa protetta. Le metriche di mitigazione si basano sul traffico osservato dai sistemi di mitigazione di Shield. DDoS Le metriche di mitigazione sono una misurazione più precisa del traffico verso la risorsa.

La metrica dei principali contributori della rete fornisce informazioni sulla provenienza del traffico durante un evento rilevato. Puoi visualizzare i contributori con il maggior volume di contributi e

ordinarli per aspetti come protocollo, porta di origine e flag. TCP La metrica dei principali contributori include metriche per tutto il traffico osservato sulla risorsa in varie dimensioni. Fornisce dimensioni metriche aggiuntive che puoi utilizzare per comprendere il traffico di rete inviato alla tua risorsa durante un evento. Tieni presente che per gli attacchi non riflettenti di livello 3 o 4, è possibile che gli indirizzi IP di origine siano stati falsificati e non siano affidabili.

La dashboard del servizio include anche dettagli sulle azioni intraprese automaticamente per mitigare gli attacchi. DDoS Queste informazioni facilitano l'indagine sulle anomalie, l'esplorazione delle dimensioni del traffico e una migliore comprensione delle azioni intraprese da Shield Advanced per proteggere la disponibilità.

Registrazione

Abilita la registrazione utile su tutti i servizi secondo la nostra guida alla registrazione e al monitoraggio per i proprietari delle applicazioni per massimizzare la visibilità e assistere nella risoluzione dei problemi. Ciò include, a titolo esemplificativo ma non esaustivo:

- AWS CloudTrail
- File di log AWS WAF
- CloudFrontregistri di accesso
- VPCRegistri di flusso (vedi Registra e visualizza i flussi di traffico di rete): includi il `tcp-flags` campo nei campi inclusi per massimizzare la visibilità
- ELBregistri di accesso (,,) ALBCLBNLB
- registri di HTTP accesso al server Web
- Registrazione della sicurezza del sistema operativo
- Registrazione delle applicazioni

Gestione della visibilità e della protezione su più account

Negli scenari in cui si opera su più componenti Account AWS e si hanno più componenti da proteggere, l'utilizzo di tecniche che consentono di operare su larga scala e ridurre il sovraccarico operativo aumenta le capacità di mitigazione. Quando si gestiscono risorse AWS Shield Advanced protette in più account, è possibile impostare un monitoraggio centralizzato utilizzando and. AWS Firewall Manager AWS Security Hub Con Firewall Manager, puoi creare una politica di sicurezza che impone la conformità alla DDoS protezione in tutti i tuoi account. È possibile utilizzare questi

due servizi insieme per gestire le risorse protette su più account e centralizzare il monitoraggio di tali risorse.

Security Hub si integra automaticamente con Firewall Manager, consentendo ai clienti di Shield Advanced di visualizzare i risultati di sicurezza in un'unica dashboard, insieme ad altri avvisi di sicurezza e stati di conformità ad alta priorità.

Ad esempio, quando Shield Advanced rileva traffico anomalo destinato a una risorsa protetta Account AWS all'interno dell'ambito, questo risultato sarà visibile nella console Security Hub. Se configurato, Firewall Manager può rendere automaticamente conforme la risorsa creandola come risorsa protetta da Shield Advanced e quindi aggiornare Security Hub quando la risorsa è in uno stato conforme.

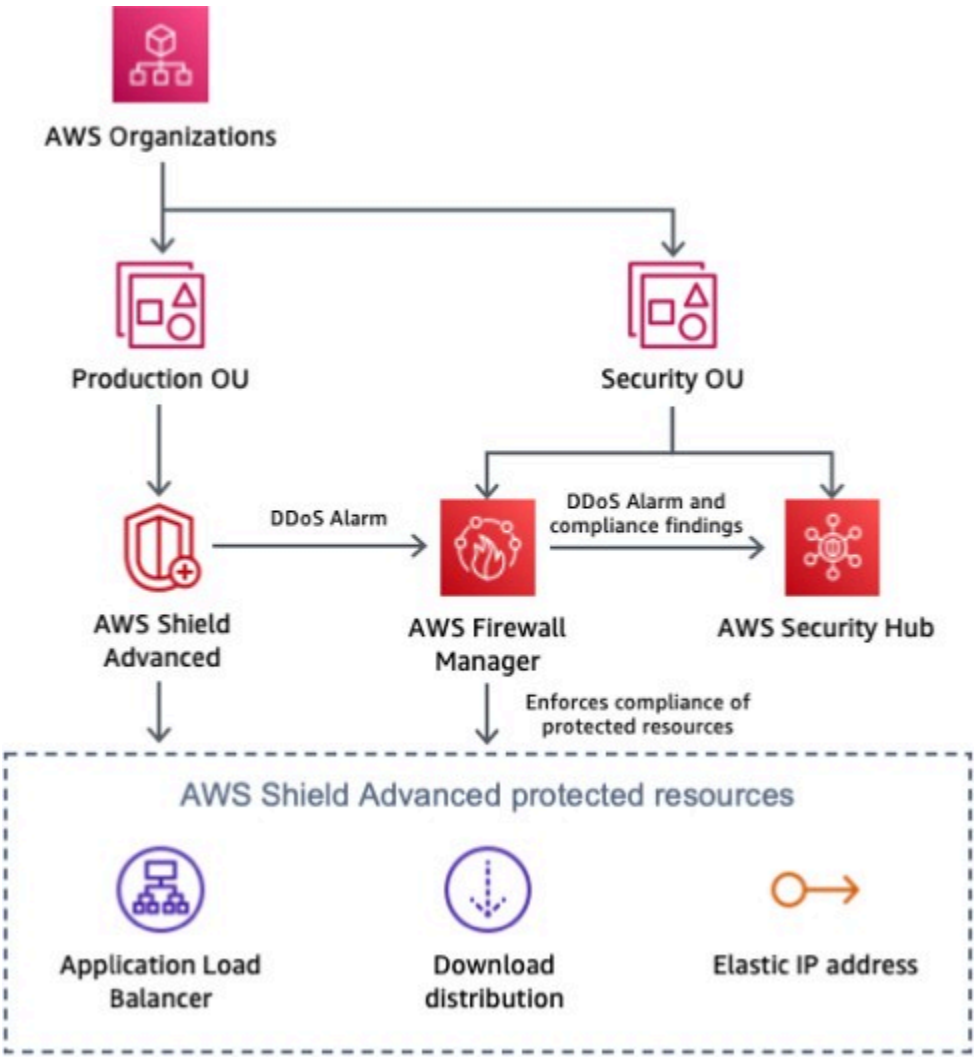


Diagramma dell'architettura che mostra il monitoraggio delle risorse AWS Shield protette con Firewall Manager e Security Hub

Per ulteriori informazioni sul monitoraggio centralizzato delle risorse protette da Shield, consulta Configurare il monitoraggio centralizzato DDoS degli eventi e correggere automaticamente le risorse non conformi.

Strategia e runbook di risposta agli incidenti

Lo sviluppo di una strategia di risposta agli DDoS attacchi e la creazione di un processo di risposta agli incidenti di sicurezza sulla base di tale strategia sono fondamentali per tutte le organizzazioni. Un approccio consigliato consiste nel modellare il proprio playbook di risposta in NIST base ai passaggi suggeriti, come la raccolta di prove, la mitigazione, il ripristino e l'esecuzione di analisi post-incidente. Ad esempio, viene fornito un playbook di risposta per DoS o DDoS attacchi di applicazioni Web. Risorse aggiuntive sono disponibili nella AWS Security Incident Response Guide.

Supporto

Se subite un attacco, potete anche avvalervi del AWS supporto necessario per valutare la minaccia e rivedere l'architettura dell'applicazione, oppure potete richiedere altra assistenza. È importante creare un piano di risposta agli DDoS attacchi prima di un evento effettivo. Le best practice descritte in questo paper sono intese come misure proattive da implementare prima del lancio di un'applicazione, ma potrebbero comunque verificarsi DDoS attacchi contro l'applicazione. Esamina le opzioni in questa sezione per determinare le risorse di supporto più adatte al tuo scenario. Il team addetto all'account può valutare il caso d'uso e l'applicazione e fornire assistenza in caso di domande o problemi specifici.

Se esegui carichi di lavoro di produzione AWS, prendi in considerazione la possibilità di abbonarti a Business Support, che ti offre accesso 24 ore su 24, 7 giorni su 7 ai tecnici del supporto cloud che possono aiutarti in caso di problemi DDoS di attacco. Se esegui carichi di lavoro mission critical, prendi in considerazione Enterprise Support, che offre la possibilità di aprire casi critici e ricevere la risposta più rapida da un Senior Cloud Support Engineer.

Se sei abbonato AWS Shield Advanced e sei anche abbonato a Business Support o Enterprise Support, puoi configurare il coinvolgimento proattivo di Shield. Ti consente di configurare i controlli sanitari, associarti alle tue risorse e fornire informazioni di contatto operative 24 ore su 24, 7 giorni su 7. Quando Shield rileva segni di degrado DDoS e i controlli dello stato dell'applicazione mostrano segni di deterioramento, AWS SRT ti contatterà in modo proattivo. Questo è il nostro modello di coinvolgimento consigliato perché consente i tempi di AWS SRT risposta più rapidi e consente di iniziare la risoluzione dei problemi anche prima di AWS SRT stabilire un contatto con l'utente.

Per ulteriori informazioni, consulta la sezione Confronta AWS Support i piani.

La funzionalità di coinvolgimento proattivo richiede la configurazione di un controllo dello stato di Route 53 che misuri accuratamente lo stato dell'applicazione e sia associato alla risorsa protetta da Shield Advanced. Una volta associato un controllo dello stato di Route 53 nella console Shield, il sistema di rilevamento Shield Advanced utilizza lo stato del controllo di integrità come indicatore dello stato dell'applicazione. La funzionalità di rilevamento basata sullo stato di salute di Shield Advanced garantirà che l'utente riceva notifiche e che le misure di mitigazione vengano applicate più rapidamente quando l'applicazione non è integra. AWS SRTti contatterà per stabilire se l'applicazione non integra è oggetto di un DDoS attacco e per adottare misure di mitigazione aggiuntive, se necessario.

Il completamento della configurazione del coinvolgimento proattivo include l'aggiunta dei dettagli di contatto nella console Shield. AWS SRTutilizzerà queste informazioni per contattarti. Puoi configurare fino a dieci contatti e fornire note aggiuntive se hai requisiti o preferenze di contatto specifici. Proattiva

i contatti di contatto devono ricoprire un ruolo 24 ore su 24, 7 giorni su 7, ad esempio un centro operativo di sicurezza o una persona immediatamente disponibile.

È possibile abilitare un coinvolgimento proattivo per tutte le risorse o per alcune risorse di produzione chiave in cui i tempi di risposta sono fondamentali. Ciò si ottiene assegnando controlli sanitari solo a queste risorse.

Puoi anche passare a AWS SRT creando un AWS Support caso utilizzando la AWS Support console (è richiesto l'accesso) o Support API se hai un evento DDoS correlato che influisce sulla disponibilità dell'applicazione.

Conclusioni

Le best practice illustrate in questo paper possono aiutarvi a creare un'architettura DDoS resiliente che protegga la disponibilità delle applicazioni prevenendo molti attacchi comuni a livello DDoS di infrastruttura e applicazione. La misura in cui seguirete queste best practice durante la progettazione dell'applicazione influenzerà il tipo, il vettore e il volume degli DDoS attacchi che potete mitigare. È possibile incorporare la resilienza senza sottoscrivere un servizio di mitigazione. DDoS Scegliendo di AWS Shield Advanced abbonarvi otterrete ulteriori funzionalità di supporto, visibilità, mitigazione e protezione dei costi che proteggono ulteriormente un'architettura applicativa già resiliente.

Collaboratori

Hanno collaborato alla stesura del presente documento:

- Rodrigo Ferroni, specialista della sicurezza AWS TAM
- Dmitriy Novikov, architetto delle soluzioni AWS
- Achraf Souk, architetto delle soluzioni AWS
- Joanna Knox, Ingegneria AWS Support
- Anuj Butail, architetto delle soluzioni AWS
- Harith Gaddamanugu, Edge Specialist SA AWS

Approfondimenti

Per ulteriori informazioni, fare riferimento a:

- Linee guida per l'implementazione AWS WAF (AWS white paper)
- NIS301 — Re:INforce 2023: In che modo l'intelligence AWS sulle minacce diventa regole di firewall gestite (video) YouTube
- NET314- re:Invent 2022: DDoS Creazione di applicazioni resilienti utilizzando (video) AWS Shield YouTube
- SEC321- re:Invent 2020: anticipa i tempi con le escalation del Response Team (video) DDoS YouTube
- William Hill: DDoS protezione ad alte prestazioni con - 2020 (video) AWS YouTube
- SEC407 - re:Invent 2019: un defense-in-depth approccio alla creazione di applicazioni web (video) YouTube
- Migliori pratiche per la DDoS mitigazione nel 2018 AWS(video) YouTube
- SID324— re:Invent 2017: Automatizzazione della DDoS risposta nel cloud (video) YouTube
- CTD304 — re:Invent 2017: Il percorso di Dow Jones e del Wall Street Journal per gestire i picchi di traffico While (video) YouTube
- Attenuazione delle minacce a livello applicativo DDoS e di mitigazione (video) YouTube
- CTD310 — re:Invent 2017: Vivere ai margini è più sicuro di quanto si pensi! Creiamo solidi con Amazon (YouTube video)
- CloudFront AWS Shield, e AWS WAF (YouTube video)

Revisioni del documento

Per ricevere notifiche sugli aggiornamenti di questo white paper, iscriviti al feed. RSS

Modifica	Descrizione	Data
Aggiornamento del white paper	Aggiunto OAC per la protezion e CloudFront dei costi aggiuntiviDNS. Discussione estesa sulle tecniche operative , la memorizzazione nella cache, le regole basate sulla frequenza e i gruppi di regole gestiti. Aggiunto in locale al diagramma di architettura, rimossa la duplicazione e chiarito il testo per eliminare le ambiguità.	9 agosto 2023
Aggiornamento del white paper	Rivisto per maggiore chiarezza ; aggiornato per includere i consigli e le funzionalità più recenti: tracciamento delle connessioni dei gruppi di sicurezza e DDoS mitigazio ne automatica del livello di applicazione Shield Advanced.	13 aprile 2022
Aggiornamento del white paper	Aggiornato per includere i consigli e le funzionalità più recenti. AWS Global Accelerat or viene aggiunto come parte di una protezione completa ai margini. AWS Firewall Manager per il monitorag gio centralizzato degli DDoS eventi e la riparazione	21 settembre 2021

	automatica delle risorse non conformi.	
Aggiornamento del white paper	Aggiornato per chiarire l'interruzione della cache nella sezione Detect and Filter Malicious Web Requests (BP1,BP2) ELB e l'ALButilizzo nella sezione Scale to Absorb (). BP6 Diagrammi aggiornati e Tabella 2, contrassegnata con «Scelta della regione». come. BP8 BP7Sezione aggiornata con maggiori dettagli.	18 dicembre 2019
Aggiornamento del white paper	Aggiornato per includere la AWS WAF registrazione come best practice.	1 dicembre 2018
Aggiornamento del white paper	Aggiornato per includere AWS Shield AWS WAF funzionalità e best AWS Firewall Manager practice correlate.	1 giugno 2018
Aggiornamento del white paper	Sono state aggiunte linee guida sull'architettura prescrittiva e sono state aggiornate per includere. AWS WAF	1 giugno 2016
Pubblicazione iniziale	Whitepaper pubblicato.	1 giugno 2015

Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute in questo documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le offerte e le pratiche attuali di AWS prodotti, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte dei suoi affiliati, AWS fornitori o licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.