AWS Livro branco

AWS Melhores práticas para DDoS resiliência

AWS Melhores práticas para DDoS resiliência: AWS Livro branco

Table of Contents

AWS Melhores práticas para DDoS resiliência

Data de publicação: 9 de agosto de 2023 (Revisões do documento)

É importante proteger sua empresa do impacto dos ataques distribuídos de negação de serviço (DDoS), bem como de outros ataques cibernéticos. Manter a confiança do cliente em seu serviço, mantendo a disponibilidade e a capacidade de resposta do seu aplicativo, é uma alta prioridade. Você também quer evitar custos diretos desnecessários quando sua infraestrutura precisa ser expandida em resposta a um ataque. A Amazon Web Services (AWS) tem o compromisso de fornecer a você as ferramentas, as melhores práticas e os serviços para se defender contra agentes mal-intencionados na Internet. Usar os serviços certos AWS ajuda a garantir alta disponibilidade, segurança e resiliência.

Neste whitepaper, AWS você encontrará DDoS orientações prescritivas para melhorar a resiliência dos aplicativos em execução. AWS Isso inclui uma arquitetura DDoS de referência resiliente que pode ser usada como guia para ajudar a proteger a disponibilidade dos aplicativos. Este whitepaper também descreve diferentes tipos de ataque, como ataques na camada de infraestrutura e ataques na camada de aplicativos. AWS explica quais práticas recomendadas são mais eficazes para gerenciar cada tipo de ataque. Além disso, os serviços e recursos que se encaixam em uma estratégia de DDoS mitigação são descritos, além de como cada um pode ser usado para ajudar a proteger seus aplicativos.

Este paper é destinado a tomadores de decisão de TI e engenheiros de segurança que estão familiarizados com os conceitos básicos de rede, segurança AWS e. Cada seção tem links para a AWS documentação que fornece mais detalhes sobre as melhores práticas ou capacidades.

AWS detecta mais de um milhão de DDoS ataques por ano e mitiga milhares diariamente contra nossos clientes. De acordo com nossa equipe Shield Response (SRT), a maioria dos clientes que sofrem o impacto dos DDoS ataques nos negócios não implementou as recomendações deste guia.

Sua arquitetura está bem planejada?

O Well-Architected Framework da AWS ajuda você a entender os prós e os contras das decisões que você toma ao criar sistemas na nuvem. Os seis pilares do framework permitem a você conhecer as melhores práticas de arquitetura para criar e operar sistemas confiáveis, seguros, econômicos e sustentáveis na nuvem. Usando o AWS Well-Architected Tool, disponível gratuitamente no AWS Management Console(é necessário fazer login), você pode analisar suas cargas de trabalho em relação a essas melhores práticas respondendo a um conjunto de perguntas para cada pilar.

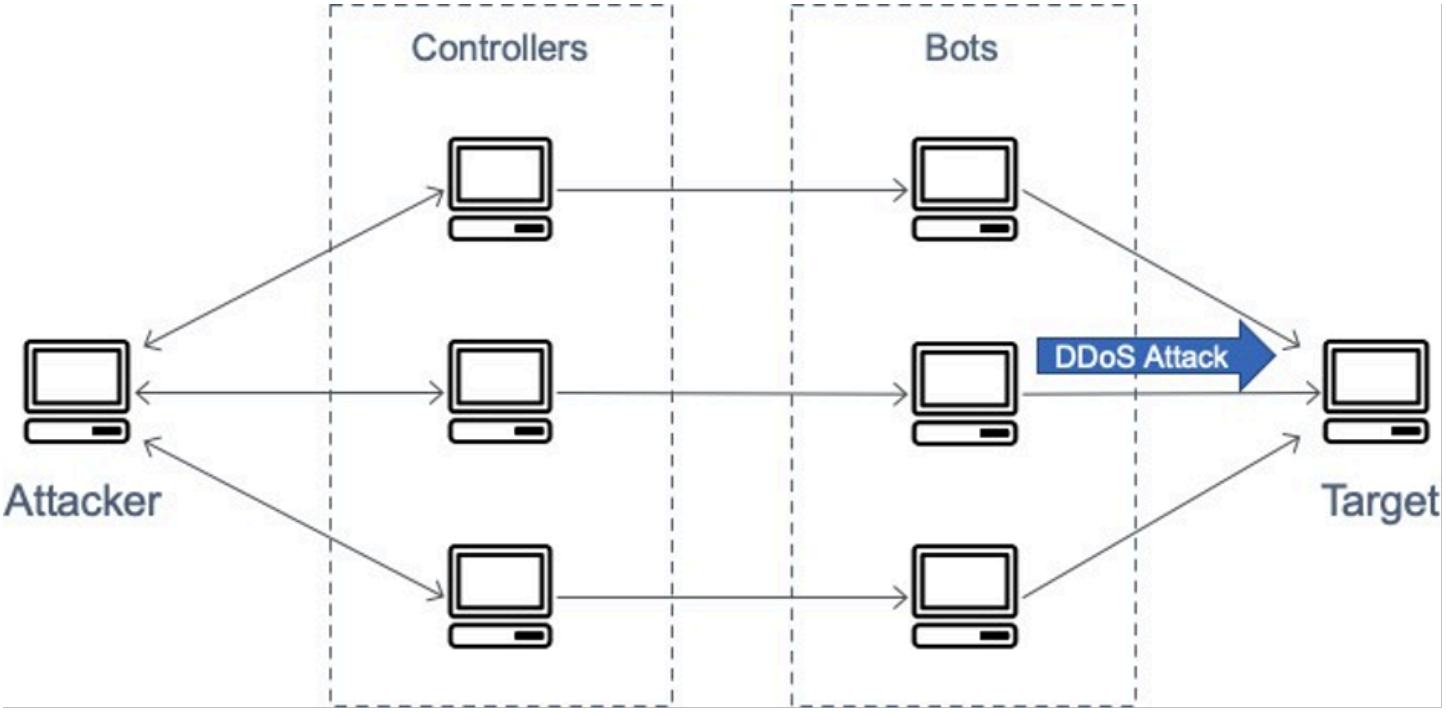
Para obter mais orientações de especialistas e melhores práticas para sua arquitetura de nuvem — implantações, diagramas e whitepapers de arquitetura de referência, consulte o Architecture Center.AWS

Introdução aos ataques de negação de serviço

Um ataque ou evento de negação de serviço (DoS) é uma tentativa deliberada de tornar um site ou aplicativo indisponível para os usuários, por exemplo, inundando-o com tráfego de rede. Os atacantes usam uma variedade de técnicas que consomem grandes quantidades de largura de banda da rede ou ocupam outros recursos do sistema, interrompendo o acesso de usuários legítimos. Em sua forma mais simples, um atacante solitário usa uma única fonte para realizar um ataque DoS contra um alvo, conforme mostrado na figura a seguir.

Um diagrama que descreve um ataque de DoS

Em um ataque distribuído de negação de serviço (DDoS), um atacante usa várias fontes para orquestrar um ataque contra um alvo. Essas fontes podem incluir grupos distribuídos de computadores, roteadores, dispositivos de IoT e outros terminais infectados por malware. A figura a seguir mostra uma rede de hosts comprometidos que participam do ataque, gerando uma enxurrada de pacotes ou solicitações para sobrecarregar o alvo.



Um diagrama que descreve um ataque DDoS

Há sete camadas no modelo de Interconexão de Sistemas Abertos (OSI) e elas estão descritas na tabela a seguir. DDoSos ataques são mais comuns nas camadas 3, 4, 6 e 7.

- Os ataques das camadas 3 e 4 correspondem às camadas de rede e transporte do OSI modelo. Neste whitepaper, AWS refere-se a eles coletivamente como ataques na camada de infraestrutura.
- Os ataques das camadas 6 e 7 correspondem às camadas de Apresentação e Aplicação do OSI modelo. Este whitepaper aborda esses ataques em conjunto como ataques à camada de aplicativos.

Este paper discute esses tipos de ataque nas seções a seguir.

Tabela 1 — OSI modelo

#	Camada	Unidade	Descrição	Exemplos de vetores
7	Aplicativo	Dados	Processo de rede até o aplicativo	HTTPinundações, inundações de DNS consultas
6	Apresentação	Dados	Representação e criptografia de dados	Abuso do Transport Layer Security (TLS)
5	Sessão	Dados	Comunicação entre anfitriões	N/D
4	Transporte	Segmentos	nd-to-end Conexões E e confiabilidade	Sincronizar (SYN) inundações
3	Rede	Pacotes	Determinação do caminho e endereçamento lógico	Ataques de reflexão do User Datagram Protocol (UDP)

#	Camada	Unidade	Descrição	Exemplos de vetores
2	Link de dados	Quadros	Endereçamento físico	N/D
1	Físico	Bits	Transmissão de mídia, sinal e binária	N/D

Ataques na camada de infraestrutura

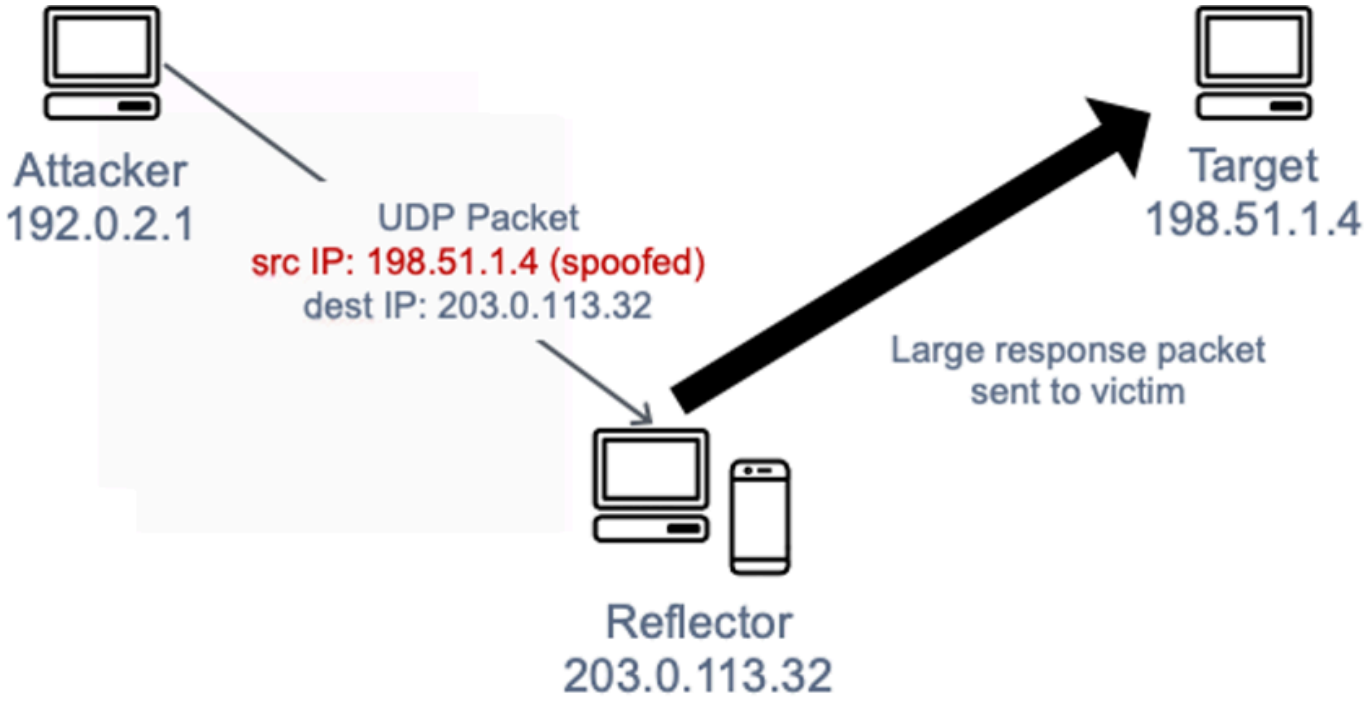
Os ataques mais comuns, DDoS ataques de reflexão e SYN inundações do User Datagram Protocol (UDP), são ataques à camada de infraestrutura. Um invasor pode usar qualquer um desses métodos para gerar grandes volumes de tráfego que podem inundar a capacidade de uma rede ou ocupar recursos em sistemas como servidores, firewalls, sistema de prevenção de intrusões (IPS) ou balanceador de carga. Embora esses ataques possam ser fáceis de identificar, para mitigá-los de forma eficaz, você deve ter uma rede ou sistemas que aumentem a capacidade mais rapidamente do que a inundação do tráfego de entrada. Essa capacidade extra é necessária para filtrar ou absorver o tráfego de ataque, liberando o sistema e o aplicativo para responder ao tráfego legítimo de clientes.

UDPataques de reflexão

UDPataques de reflexão exploram o fato de ser UDP um protocolo sem estado. Os atacantes podem criar um pacote de UDP solicitação válido listando o endereço IP do alvo do ataque como o endereço IP de UDP origem. O atacante agora falsificou — falsificou — o IP de origem do pacote de solicitaçãoUDP. O UDP pacote contém o IP de origem falsificado e é enviado pelo atacante para um servidor intermediário. O servidor é induzido a enviar seus pacotes de UDP resposta para o IP da vítima alvo, em vez de voltar para o endereço IP do atacante. O servidor intermediário é usado porque gera uma resposta várias vezes maior do que o pacote de solicitação, amplificando efetivamente a quantidade de tráfego de ataque enviado ao endereço IP de destino.

O fator de amplificação é a proporção entre o tamanho da resposta e o tamanho da solicitação e varia de acordo com o protocolo usado pelo atacante: Network Time Protocol ()DNS, Simple Service Directory Protocol (NTP), Connectionless Lightweight Directory Access Protocol (SSDPCLDAP), Memcached, Character Generator Protocol (CharGen) ou Quote of the Day (). QOTD

Por exemplo, o fator de amplificação para DNS pode ser de 28 a 54 vezes o número original de bytes. Portanto, se um invasor enviar uma carga de solicitação de 64 bytes para um DNS servidor, ele poderá gerar mais de 3400 bytes de tráfego indesejado para um alvo de ataque. UDPataques de reflexão são responsáveis por um maior volume de tráfego em comparação com outros ataques. A figura a seguir ilustra a tática de reflexão e o efeito de amplificação.

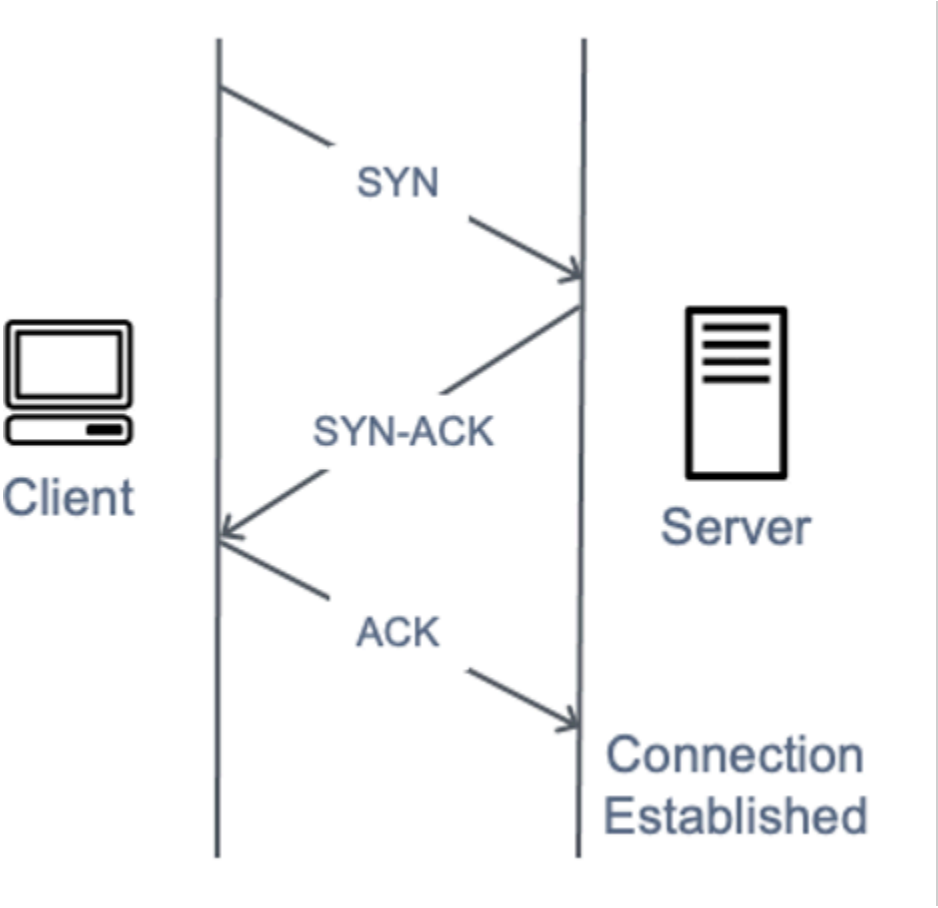


Um diagrama que descreve um ataque de UDP reflexão

Deve-se observar que os ataques de reflexão, embora forneçam aos atacantes uma amplificação “gratuita”, exigem a capacidade de falsificação de IP e, à medida que um número cada vez maior de provedores de rede adota a Validação de Endereço de Origem em Qualquer Lugar (SAVE) ou BCP38, essa capacidade é removida, exigindo que os provedores de DDoS serviços cessem os ataques de reflexão ou se mudem para data centers e provedores de rede que não implementam a validação do endereço de origem.

SYNataques de inundação

Quando um usuário se conecta a um serviço do Transmission Control Protocol (TCP), como um servidor web, o cliente envia um SYN pacote. O servidor retorna um pacote de confirmação de sincronização (SYN-ACK) e, finalmente, o cliente responde com um pacote de confirmação (ACK), que completa o handshake tridirecional esperado. A imagem a seguir ilustra esse aperto de mão típico.



Um diagrama que mostra um aperto de mão SYN tridirecional

Em um ataque de SYN inundação, um cliente mal-intencionado envia um grande número de SYN pacotes, mas nunca envia os ACK pacotes finais para concluir os apertos de mão. O servidor fica esperando por uma resposta às TCP conexões semiabertas e a ideia é que o alvo acabe sem capacidade para aceitar novas TCP conexões, o que impede que novos usuários se conectem ao servidor; no entanto, o impacto real é mais sutil. Todos os sistemas operacionais modernos implementam SYN cookies por padrão como um mecanismo para combater o esgotamento da tabela de estados devido a ataques de SYN inundação. Quando o comprimento da SYN fila atinge um limite predeterminado, o servidor responde com um SYN - ACK contendo um número de sequência inicial criado, sem criar uma entrada na fila. SYN Se o servidor receber um ACK contendo um número de confirmação incrementado corretamente, ele poderá adicionar a entrada à tabela de estados e continuar normalmente. O impacto real das SYN inundações nos dispositivos de destino tende a ser a capacidade e a CPU exaustão da rede, no entanto, dispositivos intermediários com estado, como firewalls (ou rastreamento de conexões de grupos de EC2 segurança), podem sofrer esgotamento da tabela de TCP estados e eliminar novas conexões.

TCPreflexão da caixa intermediária

Esse vetor de ataque relativamente novo foi divulgado pela primeira vez em um white paper acadêmico em agosto de 2021, que explicava como a TCP não conformidade nos firewalls disponíveis no estado nacional e no mercado poderia fazer com que eles fossem induzidos a se tornarem um vetor de amplificação. TCP Vimos esses ataques “na natureza” desde o início de 2022 e continuamos a vê-los até hoje. O fator de amplificação varia devido às diferentes maneiras pelas quais os fornecedores implementaram esse “recurso”, mas pode exceder a amplificação do UDP Memcached.

Ataques na camada de aplicação

Um invasor pode atacar o próprio aplicativo usando um ataque de camada 7 ou camada de aplicativo. Nesses ataques, semelhantes aos ataques à infraestrutura de SYN inundação, o atacante tenta sobrecarregar funções específicas de um aplicativo para tornar o aplicativo indisponível ou não responder aos usuários legítimos. Às vezes, isso pode ser obtido com volumes de solicitações muito baixos que geram apenas um pequeno volume de tráfego de rede. Isso pode dificultar a detecção e mitigação do ataque. Exemplos de ataques à camada de aplicação incluem HTTP inundações, ataques de destruição de cache e - inundações. WordPress XML RPC

- Em um ataque de HTTP inundação, um invasor envia HTTP solicitações que parecem ser de um usuário válido do aplicativo web. Algumas HTTP inundações têm como alvo um recurso específico, enquanto HTTP inundações mais complexas tentam emular a interação humana com o aplicativo. Isso pode aumentar a dificuldade de usar técnicas comuns de mitigação, como a limitação da taxa de solicitações.
- Os ataques de bloqueio de cache são um tipo de HTTP inundação que usa variações na sequência de caracteres de consulta para contornar o cache da rede de entrega de conteúdo (). CDN Em vez de serem capazes de retornar resultados em cache, eles CDN devem entrar em contato com o servidor de origem para cada solicitação de página, e essas buscas de origem causam pressão adicional no servidor web do aplicativo.
- Com um WordPress XMLataque de RPC inundação, também conhecido como inundação de WordPress pingback, um atacante tem como alvo um site hospedado no software de gerenciamento de conteúdo. WordPress O atacante usa indevidamente a RPC API função XML- para gerar uma enxurrada de solicitações. HTTP O recurso de pingback permite que um site hospedado no WordPress (Site A) notifique um WordPress site diferente (Site B) por meio de um link que o Site A criou para o Site B. O Site B então tenta acessar o Site A para verificar a existência do link. Em uma inundação de pingback, o atacante usa indevidamente esse recurso

para fazer com que o Site B ataque o Site A. Esse tipo de ataque tem uma assinatura clara: "`WordPress:`" normalmente está presente no User-Agent do cabeçalho da solicitação. HTTP

Há outras formas de tráfego malicioso que podem afetar a disponibilidade de um aplicativo. Os bots Scraper automatizam as tentativas de acessar um aplicativo da web para roubar conteúdo ou registrar informações da concorrência, como preços. Ataques de força bruta e preenchimento de credenciais são esforços programados para obter acesso não autorizado a áreas seguras de um aplicativo. Esses não são estritamente DDoS ataques, mas sua natureza automatizada pode ser semelhante a um DDoS ataque e pode ser mitigada com a implementação de algumas das mesmas melhores práticas abordadas neste paper.

Os ataques na camada de aplicativos também podem ter como alvo os serviços do Sistema de Nomes de Domínio (DNS). O mais comum desses ataques é uma inundação de DNS consultas, na qual um invasor usa muitas DNS consultas bem formadas para esgotar os recursos de um servidor. DNS Esses ataques também podem incluir um componente de bloqueio de cache em que o atacante randomiza a string do subdomínio para ignorar o cache local de qualquer resolvedor. DNS Como resultado, o resolvedor não pode tirar proveito das consultas de domínio em cache e, em vez disso, deve entrar em contato repetidamente com o DNS servidor autorizado, o que amplifica o ataque.

Se um aplicativo da web for entregue pelo Transport Layer Security (TLS), um invasor também poderá optar por atacar o TLS processo de negociação. TLSé computacionalmente caro, então um invasor, ao gerar carga de trabalho extra no servidor para processar dados ilegíveis (ou ininteligíveis (texto cifrado)) como um aperto de mão legítimo, pode reduzir a disponibilidade do servidor. Em uma variação desse ataque, um atacante conclui o TLS aperto de mão, mas renegocia perpetuamente o método de criptografia. Como alternativa, um invasor pode tentar esgotar os recursos do servidor abrindo e fechando várias TLS sessões.

Técnicas de mitigação

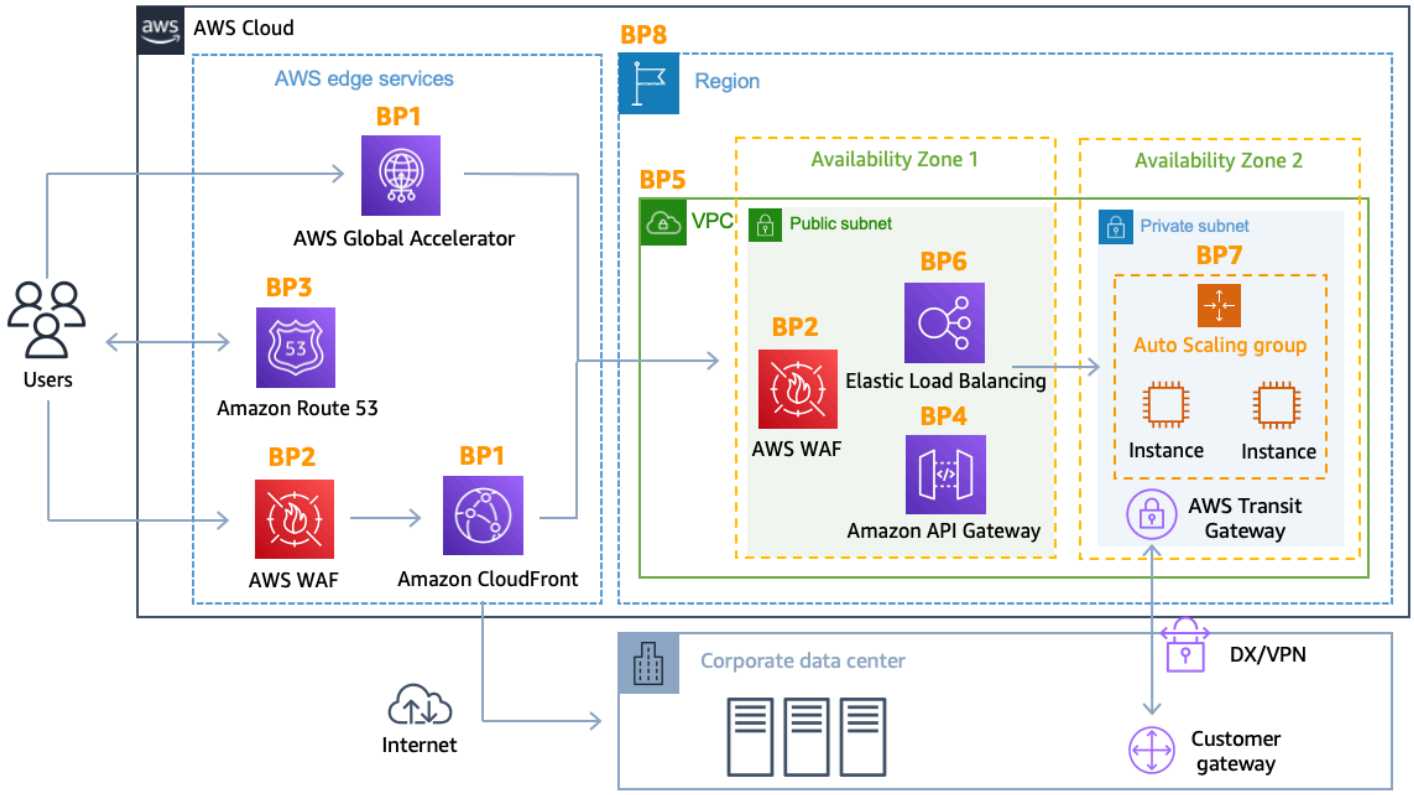
Algumas formas de DDoS mitigação são incluídas automaticamente nos serviços. AWS DDoSa resiliência pode ser aprimorada ainda mais usando uma AWS arquitetura com serviços específicos, abordados nas seções a seguir, e implementando práticas recomendadas adicionais para cada parte do fluxo de rede entre os usuários e seu aplicativo.

Você pode usar AWS serviços que operam em pontos de presença, como Amazon CloudFront, AWS Global Accelerator e Amazon Route 53 para criar uma proteção de disponibilidade abrangente contra todos os ataques conhecidos na camada de infraestrutura. Esses serviços fazem parte da AWS Global Edge Network e podem melhorar a DDoS resiliência do seu aplicativo ao atender a qualquer tipo de tráfego de aplicativo a partir de pontos de presença distribuídos ao redor do mundo. Você pode executar seu aplicativo em qualquer Região da AWS um e usar esses serviços para proteger a disponibilidade do aplicativo e otimizar o desempenho do seu aplicativo para usuários finais legítimos.

Os benefícios de usar o Amazon CloudFront, o Global Accelerator e o Amazon Route 53 incluem:

- Acesso à internet e capacidade de DDoS mitigação em toda a AWS Global Edge Network. Isso é útil para mitigar ataques volumétricos maiores, que podem atingir a escala de terabits.
- AWS Shield DDoSos sistemas de mitigação são integrados aos serviços de AWS ponta, reduzindo time-to-mitigate de minutos para menos de um segundo.
- A mitigação de SYN inundação sem estado verifica as conexões de entrada usando SYN cookies antes de passá-las para o serviço protegido. Isso garante que somente conexões válidas cheguem ao seu aplicativo e, ao mesmo tempo, proteja seus usuários finais legítimos contra quedas de falsos positivos.
- Sistemas automáticos de engenharia de tráfego que dispersam ou isolam o impacto de grandes ataques volumétricosDDoS. Todos esses serviços isolam os ataques na origem antes que eles cheguem à sua origem, o que significa menos impacto nos sistemas protegidos por esses serviços.
- A defesa da camada de aplicativos, CloudFront quando combinada com AWS WAFisso, não exige a alteração da arquitetura atual do aplicativo (por exemplo, em um data center Região da AWS ou local).

Não há cobrança pela transferência de dados de entrada AWS e você não paga pelo tráfego de DDoS ataque que é mitigado por. AWS Shield O diagrama de arquitetura a seguir inclui os serviços da AWS Global Edge Network.



DDoS-arquitetura de referência resiliente

Essa arquitetura inclui vários AWS serviços que podem ajudá-lo a melhorar a resiliência do seu aplicativo web contra DDoS ataques. A tabela a seguir fornece um resumo desses serviços e dos recursos que eles podem fornecer. AWS marcou cada serviço com um indicador de melhores práticas (BP1,BP2) para facilitar a referência neste documento. Por exemplo, uma próxima seção discute os recursos fornecidos pela Amazon CloudFront e pelo Global Accelerator que incluem o indicador de melhores práticas. BP1

Tabela 2 - Resumo das melhores práticas

	AWS Edge			Região da AWS		
	Usando a Amazon CloudFront	Usando o Global	Usando o Amazon	Usando o Elastic Load	Usando grupos de segurança	Usando o Amazon Elastic

	AWS Edge			Região da AWS		
	(BP1) com AWS WAF (BP2)	Accelerator () BP1	Route 53 (BP3)	Balancing (BP6) com AWS WAF () BP2	e rede ACLs na Amazon VPC (BP5)	Compute Cloud (AmazonEC2) Auto BP7 Scaling ()
Mitigação de ataques na camada 3 (por exemplo, UDP reflexão)	✓	✓	✓	✓	✓	✓
Mitigação de ataques de camada 4 (por exemplo, SYN inundação)	✓	✓	✓	✓		
Mitigação de ataques na camada 6 (por exemploTLS)	✓	✓	✓	✓		
Reduza a superfície de ataque	✓	✓	✓	✓	✓	

	AWS Edge			Região da AWS		
Dimensione para absorver o tráfego da camada de aplicação	✓	✓	✓	✓	✓	✓
Mitigação de ataques na camada 7 (camada de aplicação)	✓	✓(*)	✓	✓	✓(*)	✓(*)
Isolamento geográfico e dispersão do excesso de tráfego e ataques maiores DDoS	✓	✓	✓			

✓ (*): Se usado AWS WAF com o Application Load Balancer

Outra forma de melhorar sua prontidão para responder e mitigar DDoS ataques é assinando. AWS Shield Advanced Os benefícios do uso AWS Shield Advanced incluem:

- Acesso ao suporte especializado 24 horas por dia, 7 dias por semana, da Equipe de AWS Shield Resposta (AWS SRT) para assistência na mitigação de DDoS ataques que afetam a disponibilidade dos aplicativos, incluindo um recurso opcional de engajamento proativo
- Limites de detecção confidenciais que direcionam o tráfego para o sistema de DDoS mitigação mais cedo e podem melhorar os ataques time-to-mitigate contra a Amazon EC2 (incluindo o Elastic Load Balancer) ou o Network Load Balancer, quando usados com um endereço IP elástico

- Detecção personalizada de camada 7 com base nos padrões de tráfego básicos do seu aplicativo quando usado com AWS WAF
- DDoSMitigação automática da camada de aplicativos, na qual o Shield Advanced responde aos DDoS ataques detectados criando, avaliando e implantando regras personalizadas AWS WAF
- Acesso sem AWS WAF custo adicional para a mitigação de DDoS ataques na camada de aplicação (quando usado com a Amazon CloudFront ou o Application Load Balancer)
- Gerenciamento centralizado de políticas de segurança sem AWS Firewall Managercusto adicional.
- Proteção de custos que permite que você solicite um reembolso limitado dos custos relacionados à escalabilidade resultantes de um DDoS ataque.
- Contrato de nível de serviço aprimorado que é específico para AWS Shield Advanced os clientes.
- Grupos de proteção que permitem agrupar recursos, fornecendo uma forma de autoatendimento de personalizar o escopo de detecção e mitigação do seu aplicativo, tratando vários recursos como uma única unidade. Para obter informações sobre grupos de proteção, consulte os grupos de proteção Shield Advanced.
- DDoSvisibilidade do ataque usando as AWS Management Console CloudWatch métricas API e alarmes da Amazon e,

Esse serviço opcional de DDoS mitigação ajuda a proteger aplicativos hospedados em qualquer um. Região da AWS O serviço está disponível globalmente para CloudFront Route 53 e Global Accelerator. Regionalmente, você pode proteger os endereços Application Load Balancer, Classic Load Balancer e Elastic IP, o que permite proteger instâncias do Network Load Balancer () ou da Amazon. NLBs EC2

Para obter uma lista completa de AWS Shield Advanced recursos e obter mais informações sobre AWS Shield, consulte Como AWS Shield funciona.

Melhores práticas para DDoS mitigação

Nas seções a seguir, cada uma das melhores práticas recomendadas para DDoS mitigação é descrita com mais detalhes. Para obter um easy-to-implement guia rápido sobre a criação de uma camada de DDoS mitigação para aplicativos web estáticos ou dinâmicos, consulte Como ajudar a proteger aplicativos web dinâmicos contra DDoS ataques usando a Amazon e o CloudFront Amazon Route 53.

Defesa da camada de infraestrutura (BP1BP3,,BP6,BP7)

Em um ambiente de datacenter tradicional, você pode mitigar DDoS ataques na camada de infraestrutura usando técnicas como superprovisionamento de capacidade, implantação de sistemas de mitigação ou eliminação de tráfego com a ajuda de serviços de DDoS mitigação. DDoS AWS Ativado, os recursos de DDoS mitigação são fornecidos automaticamente; mas você pode otimizar a DDoS resiliência do seu aplicativo fazendo escolhas de arquitetura que melhor aproveitem esses recursos e também permitam a escalabilidade para o excesso de tráfego.

As principais considerações para ajudar a mitigar DDoS ataques volumétricos incluem garantir que capacidade e diversidade de trânsito suficientes estejam disponíveis e proteger recursos AWS , como EC2 instâncias da Amazon, contra tráfego de ataques.

Alguns tipos de EC2 instância da Amazon oferecem suporte a recursos que podem lidar mais facilmente com grandes volumes de tráfego, por exemplo, interfaces de largura de banda de rede de até 100 Gbps e redes aprimoradas. Isso ajuda a evitar o congestionamento da interface para o tráfego que chegou à EC2 instância da Amazon. As instâncias que oferecem suporte a redes aprimoradas oferecem maior desempenho de entrada/saída (E/S), maior largura de banda e menor CPU utilização em comparação com as implementações tradicionais. Isso melhora a capacidade da instância de lidar com grandes volumes de tráfego e, em última análise, a torna altamente resiliente à carga de pacotes por segundo (pps).

Para permitir esse alto nível de resiliência, AWS recomenda o uso de instâncias EC2 dedicadas da Amazon ou EC2 instâncias da Amazon com maior taxa de transferência de rede que tenham um sufixo `N` "" e suporte para redes aprimoradas com até 100 Gbps de largura de banda de rede, por exemplo, `c6gn.16xlarge` `c5n.18xlarge` e/ou instâncias metálicas (como). `c5n.metal`

Para obter mais informações sobre EC2 instâncias da Amazon que oferecem suporte a interfaces de rede de 100 Gigabit e redes aprimoradas, consulte Tipos de EC2instância da Amazon.

O módulo necessário para redes aprimoradas e o conjunto de `enaSupport` atributos necessário estão incluídos no Amazon Linux 2 e nas versões mais recentes do Amazon LinuxAMI. Portanto, se você iniciar uma instância com uma versão de máquina virtual de hardware (HVM) do Amazon Linux em um tipo de instância compatível, a rede aprimorada já estará habilitada para sua instância. Para obter mais informações, consulte Testar se a rede avançada está habilitada e Rede aprimorada no Linux.

Amazon EC2 com Auto Scaling () BP7

Outra forma de mitigar os ataques à infraestrutura e à camada de aplicação é operar em grande escala. Se você tiver aplicativos web, poderá usar balanceadores de carga para distribuir o tráfego para várias EC2 instâncias da Amazon que estão superprovisionadas ou configuradas para escalar automaticamente. Essas instâncias podem lidar com picos repentinos de tráfego que ocorrem por qualquer motivo, incluindo uma multidão instantânea ou um DDoS ataque à camada de aplicativo. Você pode definir CloudWatch alarmes da Amazon para iniciar o Auto Scaling para escalar automaticamente o tamanho da sua frota da EC2 Amazon em resposta aos eventos que você define, CPU comoRAM, E/S de rede e até mesmo métricas personalizadas.

Essa abordagem protege a disponibilidade do aplicativo quando há um aumento inesperado no volume de solicitações. Ao usar Amazon CloudFront, Application Load Balancer, Classic Load Balancers ou Network Load Balancer com seu aplicativoTLS, a negociação é feita pela distribuição (CloudFrontAmazon) ou pelo balanceador de carga. Esses recursos ajudam a proteger suas instâncias contra o impacto de ataques TLS baseados, escalando para lidar com solicitações legítimas e ataques de TLS abuso.

Para obter mais informações sobre o uso da Amazon CloudWatch para invocar o Auto Scaling, consulte Monitoramento de métricas da CloudWatch Amazon para seus grupos e instâncias do Auto Scaling.

EC2A Amazon fornece capacidade computacional redimensionável para que você possa aumentar ou diminuir rapidamente a escala conforme os requisitos mudam. Você pode escalar horizontalmente adicionando automaticamente instâncias ao seu aplicativo, escalando o tamanho do seu grupo Amazon EC2 Auto Scaling, e você pode escalar verticalmente usando tipos de instância maiores. EC2

Ao usar o Amazon RDS Proxy, você pode permitir que seus aplicativos agrupem e compartilhem conexões de banco de dados para melhorar sua capacidade de escalar e lidar com picos imprevisíveis no tráfego do banco de dados. Você também pode ativar o auto-scaling de armazenamento para uma instância de banco de dados da AmazonRDS. Consulte Gerenciamento automático de capacidade com o RDS escalonamento automático de armazenamento da Amazon para obter mais informações.

Elastic Load Balancing () BP6

Grandes DDoS ataques podem sobrecarregar a capacidade de uma única EC2 instância da Amazon. Com o Elastic Load Balancing (ELB), você pode reduzir o risco de sobrecarregar seu

aplicativo distribuindo o tráfego em várias instâncias de back-end. O Elastic Load Balancing pode ser escalado automaticamente, permitindo que você gerencie volumes maiores quando você tem tráfego extra imprevisto, por exemplo, devido a multidões ou ataques. DDoS Para aplicativos criados em uma AmazonVPC, há três tipos ELBs a serem considerados, dependendo do tipo de aplicativo: Application Load Balancer (ALB), Network Load Balancer () e Classic Load Balancer NLB (). CLB

Para aplicativos da web, você pode usar o Application Load Balancer para rotear o tráfego com base no conteúdo e aceitar somente solicitações da web bem formadas. O Application Load Balancer bloqueia muitos DDoS ataques comuns, como SYN inundações ou ataques de UDP reflexão, protegendo seu aplicativo do ataque. O Application Load Balancer é escalado automaticamente para absorver o tráfego adicional quando esses tipos de ataques são detectados. As atividades de escalonamento devido a ataques na camada de infraestrutura são transparentes para AWS os clientes e não afetam sua fatura.

Para obter mais informações sobre a proteção de aplicativos web com o Application Load Balancer, consulte Getting Started with Application Load Balancers.

Para HTTPS aplicativos que não HTTP sejam//, você pode usar o Network Load Balancer para rotear o tráfego para destinos (por exemplo, EC2 instâncias da Amazon) com latência ultrabaixa. Uma consideração importante com o Network Load Balancer é que qualquer TCP SYN UDP tráfego que chegue ao balanceador de carga em um ouvinte válido será roteado para seus destinos, não absorvido. No entanto, isso não se aplica aos TLS -listeners que encerram a conexão. TCP Para balanceadores de carga de rede com TCP ouvintes, recomendamos a implantação do Global Accelerator para se proteger contra inundações. SYN

Você pode usar o Shield Advanced para configurar a DDoS proteção para endereços IP elásticos. Quando um endereço IP elástico é atribuído por zona de disponibilidade ao Network Load Balancer, o Shield Advanced aplicará DDoS as proteções relevantes para o tráfego do Network Load Balancer.

Para obter mais informações sobre proteção TCP e UDP aplicativos com o Network Load Balancer, consulte Introdução aos Network Load Balancers.

> **Note**
>
> Dependendo da configuração do grupo de segurança, é necessário que o recurso que usa o grupo de segurança use o rastreamento de conexão para rastrear informações sobre o tráfego. Isso pode afetar a capacidade do balanceador de carga de processar novas conexões, pois o número de conexões rastreadas é limitado.

Uma configuração de grupo de segurança que contém uma regra de entrada que aceita tráfego de qualquer endereço IP (por exemplo, `0.0.0.0/0` ou `::/0`), mas não tem uma regra correspondente para permitir o tráfego de resposta, faz com que o grupo de segurança use informações de rastreamento de conexão para permitir que o tráfego de resposta seja enviado. No caso de um DDoS ataque, o número máximo de conexões rastreadas pode ser esgotado. Para melhorar a DDoS resiliência do seu Application Load Balancer ou Classic Load Balancer voltado para o público, certifique-se de que o grupo de segurança associado ao seu balanceador de carga esteja configurado para não usar rastreamento de conexão (conexões não rastreadas), para que o fluxo de tráfego não esteja sujeito aos limites de rastreamento de conexão.

Para isso, configure seu grupo de segurança com uma regra que permita que a regra de entrada aceite TCP fluxos de qualquer endereço IP (`0.0.0.0/0`ou`::/0`) e adicione uma regra correspondente na direção de saída, permitindo que esse recurso envie o tráfego de resposta (permita intervalo de saída para qualquer endereço IP `0.0.0.0/0` ou`::/0`) para todas as portas (0-65535), para que o tráfego de resposta seja permitido com base na regra do grupo de segurança e não nas informações de rastreamento. Com essa configuração, o Classic e o Application Load Balancer não estão sujeitos a limites de rastreamento de conexão de exaustão que podem afetar o estabelecimento de novas conexões com seus nós de balanceador de carga e permitem que ele seja escalado com base no aumento do tráfego no caso de um ataque. DDoS Mais informações sobre conexões não rastreadas podem ser encontradas em: Rastreamento de conexões de grupos de segurança: conexões não rastreadas.

Evitar o rastreamento de conexão do grupo de segurança só ajuda nos casos em que o DDoS tráfego se origina de uma fonte permitida pelo grupo de segurança — o DDoS tráfego de fontes que não são permitidas no grupo de segurança não afeta o rastreamento da conexão. Não é necessário reconfigurar seus grupos de segurança para evitar o rastreamento de conexão nesses casos, por exemplo, se sua lista de permissões de grupos de segurança consistir em intervalos de IP com os quais você tem um alto grau de confiança, como um firewall corporativo da empresa ou uma VPN saída IPs confiável ou. CDNs

Use localizações de AWS borda para escala (BP1,BP3)

O acesso a conexões de internet diversificadas e de alta escala pode aumentar significativamente sua capacidade de otimizar a latência e a taxa de transferência para os usuários, absorver DDoS ataques e isolar falhas, minimizando o impacto na disponibilidade do seu aplicativo. AWS Os pontos

de presença fornecem uma camada adicional de infraestrutura de rede que fornece esses benefícios a qualquer aplicativo web que use Amazon CloudFront, Global Accelerator e Amazon Route 53. Com esses serviços, você pode proteger de forma abrangente seus aplicativos em execução na borda. Regiões da AWS

Entrega de aplicativos web na borda (BP1)

CloudFront A Amazon é um serviço que pode ser usado para fornecer todo o seu site, incluindo conteúdo estático, dinâmico, de streaming e interativo. Conexões persistentes e configurações de variable time-to-live (TTL) podem ser usadas para descarregar o tráfego de sua origem, mesmo se você não estiver veiculando conteúdo armazenável em cache. O uso desses CloudFront recursos reduz o número de solicitações e TCP conexões de volta à sua origem, ajudando a proteger seu aplicativo web contra HTTP inundações.

CloudFront só aceita conexões bem formadas, o que ajuda a evitar que muitos DDoS ataques comuns, como SYN inundações e ataques de UDP reflexão, cheguem à sua origem. DDoSos ataques também são isolados geograficamente perto da origem, o que evita que o tráfego impacte outros locais. Esses recursos podem melhorar muito sua capacidade de continuar fornecendo tráfego aos usuários durante grandes DDoS ataques. Você pode usar CloudFront para proteger uma origem na Internet AWS ou em outro lugar.

Se você estiver usando o Amazon Simple Storage Service (Amazon S3) para veicular conteúdo estático na Internet, AWS recomenda que você use CloudFront a Amazon para proteger seu bucket, oferecendo os seguintes benefícios:

- Restringe o acesso ao bucket do Amazon S3 para que ele não seja acessível publicamente.
- Garante que os espectadores (usuários) possam acessar o conteúdo no bucket somente por meio da CloudFront distribuição especificada, ou seja, impede que eles acessem o conteúdo diretamente do bucket ou por meio de uma distribuição não intencional. CloudFront

Para conseguir isso, configure CloudFront para enviar solicitações autenticadas para o Amazon S3 e configure o Amazon S3 para permitir acesso somente às solicitações autenticadas do. CloudFront CloudFront fornece duas maneiras de enviar solicitações autenticadas para uma origem do Amazon S3: controle de acesso de origem OAC () e identidade OAI de acesso de origem (). Recomendamos o uso OAC porque ele suporta:

- Ao todo, todos os buckets do Amazon S3 Regiões da AWS, incluindo regiões opcionais lançadas após dezembro de 2022

- Criptografia do lado do servidor Amazon S3 com (-) AWS KMS SSE KMS
- Solicitações dinâmicas (PUT e DELETE) para o Amazon S3

Para obter mais informações sobre OAC eOAI, consulte Restringir o acesso à origem do Amazon S3.

Para obter mais informações sobre como proteger e otimizar o desempenho de aplicativos web com a Amazon CloudFront, consulte Getting Started with Amazon CloudFront.

Proteja o tráfego de rede mais longe de sua origem usando o AWS Global Accelerator () BP1

O Global Accelerator é um serviço de rede que melhora a disponibilidade e o desempenho do tráfego dos usuários em até 60%. Isso é feito inserindo tráfego no ponto de presença mais próximo de seus usuários e roteando-o pela infraestrutura de rede AWS global até seu aplicativo, seja ele executado de forma única ou múltipla. Regiões da AWS

O Global Accelerator TCP direciona o UDP tráfego para o endpoint ideal com base no desempenho mais próximo do Região da AWS usuário. Se houver uma falha no aplicativo, o Global Accelerator fornece failover para o próximo melhor endpoint em 30 segundos. O Global Accelerator usa a vasta capacidade da rede AWS global e as integrações com o Shield, como um recurso de SYN proxy sem estado que desafia novas tentativas de conexão e atende apenas a usuários finais legítimos, para proteger os aplicativos.

Você pode implementar uma arquitetura DDoS resiliente que ofereça muitos dos mesmos benefícios das melhores práticas do Web Application Delivery at the Edge, mesmo que seu aplicativo use protocolos não suportados CloudFront ou você esteja operando um aplicativo web que exija endereços IP estáticos globais.

Por exemplo, você pode exigir endereços IP que seus usuários finais possam adicionar à lista de permissões em seus firewalls e que não sejam usados por nenhum outro AWS cliente. Nesses cenários, você pode usar o Global Accelerator para proteger aplicativos web executados no Application Load Balancer e, em conjunto AWS WAF com, também, detectar e mitigar inundações de solicitações na camada de aplicativos web.

Para obter mais informações sobre como proteger e otimizar o desempenho do tráfego de rede usando o Global Accelerator, consulte Introdução ao Global Accelerator.

Resolução de nomes de domínio na borda (BP3)

Tópicos

Usando o Route 53 para DNS verificar a disponibilidade

O Amazon Route 53 é um serviço de Sistema de Nomes de Domínio (DNS) altamente disponível e escalável que pode ser usado para direcionar o tráfego para sua aplicação web. Ele inclui recursos avançados como fluxo de tráfego, Health Checks and Monitoring, roteamento baseado em latência e geolocalização. DNS Esses recursos avançados permitem que você controle como o serviço responde às DNS solicitações para melhorar o desempenho do seu aplicativo web e evitar interrupções no site. É o único AWS serviço que tem 100% de disponibilidade do plano de dadosSLA.

O Amazon Route 53 usa técnicas como shuffle sharding e anycast striping, que podem ajudar os usuários a acessar seu aplicativo mesmo que o DNS serviço seja alvo de um ataque. DDoS

Com a fragmentação aleatória, cada servidor de nomes em seu conjunto de delegação corresponde a um conjunto exclusivo de pontos de presença e caminhos da Internet. Isso proporciona maior tolerância a falhas e minimiza a sobreposição entre os clientes. Se um servidor de nomes no conjunto de delegação não estiver disponível, os usuários poderão tentar novamente e receber uma resposta de outro servidor de nomes em um ponto de presença diferente.

O striping Anycast permite que cada DNS solicitação seja atendida pelo local mais ideal, dispersando a carga da rede e reduzindo a latência. DNS Isso fornece uma resposta mais rápida para os usuários. Além disso, o Amazon Route 53 pode detectar anomalias na origem e no volume de DNS consultas e priorizar solicitações de usuários que são reconhecidamente confiáveis.

Para obter mais informações sobre o uso do Amazon Route 53 para direcionar usuários para seu aplicativo, consulte Getting Started with Amazon Route 53.

Configurando o Route 53 para proteção de custos contra ataques **NXDOMAIN**

`NXDOMAIN`os ataques ocorrem quando os atacantes enviam uma enxurrada de solicitações para uma zona hospedada para subdomínios inexistentes, geralmente por meio de resolvedores “bons” conhecidos. O objetivo desses ataques pode ser impactar o cache do resolvedor recursivo e/ou a disponibilidade do resolvedor autoritário, ou pode ser uma forma de DNS reconhecimento para tentar

descobrir registros da zona hospedada. Usar o Route 53 para seu resolvedor autorizado reduz o risco de impacto na disponibilidade/desempenho, no entanto, o resultado pode ser um aumento significativo nos custos mensais do Route 53. Para se proteger contra aumentos de custo, aproveite os preços do Route 53, nos quais DNS as consultas são gratuitas quando as duas condições a seguir são verdadeiras:

- O nome do domínio ou subdomínio (`example.comoustore.example.com`) e o tipo de registro (`A`) na consulta correspondem a um registro de alias.
- O destino do alias é um AWS recurso diferente de outro registro do Route 53.

Crie um registro curinga, por exemplo, `*.example.com` com um tipo `A` (Alias) apontando para um AWS recurso, como uma EC2 instância, Elastic Load Balancer CloudFront ou distribuição, `qwerty12345.example.com` para que, quando uma consulta for feita, o IP do recurso seja retornado e você não seja cobrado pela consulta.

Defesa da camada de aplicação (BP1,BP2)

Muitas das técnicas discutidas até agora neste paper são eficazes para mitigar o impacto que os DDoS ataques na camada de infraestrutura têm na disponibilidade do seu aplicativo. Para também se defender contra ataques na camada de aplicação, você precisa implementar uma arquitetura que permita detectar, escalar especificamente para absorver e bloquear solicitações maliciosas. Essa é uma consideração importante porque os sistemas de DDoS mitigação baseados em rede geralmente são ineficazes na mitigação de ataques complexos na camada de aplicativos.

Detecte e filtre solicitações maliciosas da web (BP1,BP2)

Quando seu aplicativo é executado AWS, você pode aproveitar a Amazon CloudFront (e sua capacidade de armazenamento em HTTP cache) e a proteção automática da camada de aplicativos Shield Advanced para ajudar a evitar que solicitações desnecessárias cheguem à sua origem durante DDoS ataques na camada de aplicação. AWS WAF

Amazon CloudFront

A Amazon CloudFront pode ajudar a reduzir a carga do servidor impedindo que o tráfego que não seja da web chegue à sua origem. Para enviar uma solicitação a um CloudFront aplicativo, a conexão deve ser estabelecida com um endereço IP válido por meio de um TCP handshake completo, que não pode ser falsificado. Além disso, CloudFront pode fechar automaticamente conexões de invasores de leitura lenta ou escrita lenta (por exemplo, Slowloris).

Armazenamento em cache do CDN

CloudFront permite que você forneça conteúdo dinâmico e conteúdo estático a partir de locais AWS periféricos. Ao fornecer conteúdo proxy armazenável em cache a partir do CDN cache, você evita que as solicitações cheguem à sua origem a partir de um determinado nó de cache de borda durante o armazenamento em cache. TTL Em conjunto com o colapso da solicitação de conteúdo expirado, mas que pode ser armazenado em cache, mesmo um número muito curto TTL significa que um número insignificante de solicitações chegará à sua origem durante a inundação de solicitações desse conteúdo. Além disso, ativar recursos como o CloudFront Origin Shield pode ajudar a reduzir ainda mais a carga em sua origem. Qualquer coisa que você possa fazer para melhorar a taxa de acerto do cache pode fazer a diferença entre um ataque de inundação de solicitações impactante e um não impactante.

AWS WAF

Usando AWS WAF, você pode configurar listas de controle de acesso à web (WebACLs) em suas CloudFront distribuições globais ou recursos regionais para filtrar, monitorar e bloquear solicitações com base nas assinaturas de solicitações. Para determinar se as solicitações devem ser permitidas ou bloqueadas, você pode considerar fatores como o endereço IP ou o país de origem, determinadas sequências de caracteres ou padrões na solicitação, o tamanho de partes específicas da solicitação e a presença de SQL códigos ou scripts maliciosos. Você também pode executar CAPTCHA quebra-cabeças e desafios silenciosos de sessões de clientes contra solicitações.

Ambos AWS WAF CloudFront também permitem que você defina restrições geográficas para bloquear ou permitir solicitações de países selecionados. Isso pode ajudar a bloquear ou limitar os ataques de localizações geográficas nas quais você não espera atender aos usuários. Com declarações refinadas de regras de correspondência geográfica AWS WAF, você pode controlar o acesso até o nível da região.

Você pode usar instruções Scope-down para restringir o escopo das solicitações que a regra avalia para economizar custos e “rótulos” nas solicitações da web para permitir que uma regra que corresponda à solicitação comunique os resultados da correspondência às regras que serão avaliadas posteriormente na mesma web. ACL Escolha essa opção para reutilizar a mesma lógica em várias regras.

Você também pode definir uma resposta personalizada completa, com código de resposta, cabeçalhos e corpo.

Para ajudar a identificar solicitações maliciosas, revise os registros do seu servidor web ou use AWS WAF o registro e a amostragem de solicitações. Ao ativar o AWS WAF registro, você obtém

informações detalhadas sobre o tráfego analisado pela Web. ACL AWS WAF oferece suporte à filtragem de registros, permitindo que você especifique quais solicitações da web são registradas e quais solicitações são descartadas do registro após a inspeção.

As informações registradas nos registros incluem a hora em que AWS WAF recebeu a solicitação do seu AWS recurso, informações detalhadas sobre a solicitação e a ação correspondente para cada regra solicitada.

As solicitações de amostra fornecem detalhes sobre as solicitações das últimas três horas que corresponderam a uma de suas AWS WAF regras. Você pode usar essas informações para identificar assinaturas de tráfego potencialmente maliciosas e criar uma nova regra para negar essas solicitações. Se você ver várias solicitações com uma sequência de caracteres de consulta aleatória, certifique-se de permitir somente os parâmetros da sequência de caracteres de consulta relevantes ao cache do seu aplicativo. Essa técnica é útil para mitigar um ataque de quebra de cache contra sua origem.

AWS WAF — Regras baseadas em tarifas

AWS recomenda fortemente a proteção contra inundações de HTTP solicitações usando as regras baseadas em taxas AWS WAF para bloquear automaticamente os endereços IP de agentes mal-intencionados quando o número de solicitações recebidas em uma janela deslizante de 5 minutos exceder um limite definido por você. Os endereços IP de clientes ofensivos receberão uma resposta 403 proibida (ou resposta de erro de bloco configurada) e permanecerão bloqueados até que as taxas de solicitação caiam abaixo do limite.

É recomendável colocar regras baseadas em taxas em camadas para fornecer proteção aprimorada para que você tenha:

- Uma regra geral baseada em taxas para proteger seu aplicativo contra grandes inundações. HTTP
- Uma ou mais regras baseadas em tarifas para proteger tarifas específicas e mais restritivas do que a regra geral baseada URIs em tarifas.

Por exemplo, você pode escolher uma regra geral baseada em taxa (sem declaração de escopo) com um limite de 500 solicitações em um período de 5 minutos e, em seguida, criar uma ou mais das seguintes regras baseadas em taxas com limites inferiores a 500 (tão baixos quanto 100 solicitações em um período de 5 minutos) usando instruções de escopo reduzido:

- Proteja suas páginas da Web com uma declaração de escopo reduzido, como "`if NOT uri_path contains '.'`", para que as solicitações de recursos sem uma extensão de arquivo

sejam ainda mais protegidas. Isso também protege sua página inicial (`/`), que é um URI caminho frequentemente direcionado.

- Proteja endpoints dinâmicos com uma declaração de redução de escopo como "" `if method exactly matches 'post' (convert lowercase)`
- Proteja solicitações pesadas que chegam ao seu banco de dados ou invoque uma senha de uso único (OTP) com um escopo reduzido como "" `if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

A base de tarifas no modo “Bloquear” é a base de sua defense-in-depth WAF configuração para se proteger contra inundações de solicitações e é um requisito para que as solicitações de proteção de AWS Shield Advanced custos sejam aprovadas. Examinaremos defense-in-depth WAF configurações adicionais nas seções a seguir.

AWS WAF — Reputação de IP

Para evitar ataques com base na reputação do endereço IP, você pode criar regras usando correspondência de IP ou usar Regras gerenciadas para AWS WAF.

O grupo de regras da lista de reputação de IP da Amazon inclui regras baseadas na inteligência interna de ameaças da Amazon. Essas regras buscam endereços IP que sejam bots, realizando reconhecimento de AWS recursos ou participando ativamente de atividades. DDoS A `AWSManagedIPDDoSList` regra foi observada bloqueando mais de 90% das inundações de solicitações maliciosas.

O grupo de regras da lista de IPs anônimos contém regras para bloquear solicitações de serviços que permitem a ofuscação da identidade do espectador. Isso inclui solicitações deVPNs, proxies, nós Tor e plataformas de nuvem (excluindo AWS).

Além disso, você pode usar listas de reputação de IP de terceiros usando o componente analisador de listas de IP da solução Security Automations for AWS WAF.

AWS WAF - Mitigação inteligente de ameaças

As redes de bots são uma séria ameaça à segurança e são comumente usadas para realizar atividades ilegais ou prejudiciais, como enviar spam, roubar dados confidenciais, iniciar ataques de ransomware, cometer fraudes publicitárias por meio de cliques fraudulentos ou lançar ataques distribuídos (). denial-of-service DDoS Para evitar ataques de bots, use o grupo de regras gerenciadas do AWS WAF Bot Control. Esse grupo de regras fornece um nível de proteção básico

“comum” que adiciona rótulos aos bots que se identificam automaticamente, verifica os bots geralmente desejáveis e detecta assinaturas de bots de alta confiança, e um nível de proteção “direcionado” que adiciona detecção para bots avançados que não se identificam.

As proteções direcionadas usam técnicas avançadas de detecção, como interrogação do navegador, impressão digital e heurística comportamental, para identificar tráfego incorreto de bots e, em seguida, aplicam controles de mitigação, como limitação de taxa e ações de regras de desafio. CAPTCHA O Targeted também fornece opções de limitação de taxa para impor padrões de acesso semelhantes aos humanos e aplicar limitação dinâmica de taxa por meio do uso de tokens de solicitação. Para obter detalhes adicionais, consulte Grupo de regras do AWS WAF Bot Control. Para detectar e gerenciar tentativas maliciosas de invasão na página de login do seu aplicativo, você pode usar o grupo de regras de prevenção de aquisição de contas (ATP) do AWS WAF Fraud Control. O grupo de regras faz isso inspecionando as tentativas de login que os clientes enviam para o endpoint de login do seu aplicativo e também inspeciona as respostas do seu aplicativo às tentativas de login, para monitorar a taxa de sucesso e falha.

A fraude na criação de conta é uma atividade ilegal online na qual um invasor tenta criar uma ou mais contas falsas. Os invasores usam contas falsas para executar atividades fraudulentas, como abusar de bônus promocionais e de inscrição, se passar por alguém e realizar ataques cibernéticos, como phishing. A presença de contas falsas pode impactar negativamente seus negócios, prejudicando sua reputação com os clientes e sua exposição a fraudes financeiras.

Você pode monitorar e controlar as tentativas de fraude na criação de contas implementando o AWS WAF recurso de prevenção de fraudes na criação de contas (ACFP). AWS WAF oferece esse recurso no grupo de AWS Managed Rules regras `AWS ManagedRulesACFPRuleSet` com integração de aplicativos complementaresSDKs.

Saiba mais sobre essas proteções na mitigação AWS WAF inteligente de ameaças.

Mitigue automaticamente os DDoS eventos da camada de aplicativo (,,) BP1 BP2 BP6

Se você estiver inscrito AWS Shield Advanced, poderá ativar a DDoSmitigação automática da camada de aplicação do Shield Advanced. Esse recurso cria, avalia e implanta automaticamente AWS WAF regras para mitigar os DDoS eventos da camada 7 em seu nome.

AWS Shield Advanced estabelece uma linha de base de tráfego para cada recurso protegido associado a uma WAF Web. ACL O tráfego que se desvia significativamente da linha de base estabelecida é sinalizado como um evento potencial. DDoS Depois que um evento é detectado, AWS

Shield Advanced tenta identificar uma assinatura das solicitações da web que constituem o evento e, se uma assinatura for identificada, AWS WAF regras serão criadas para mitigar o tráfego com essa assinatura.

Depois que as regras são avaliadas em relação à linha de base histórica e consideradas seguras, elas são adicionadas ao grupo de regras gerenciado pelo Shield e você pode escolher se as regras serão implantadas no modo de contagem ou bloqueio. O Shield Advanced remove automaticamente AWS WAF as regras depois de determinar que um evento foi totalmente encerrado.

Engage SRT (somente assinantes do Shield Advanced)

Além disso, ao assinar o Shield Advanced, você pode contratar o AWS SRT para ajudá-lo a criar regras para mitigar um ataque que está prejudicando a disponibilidade do seu aplicativo. Você pode conceder acesso AWS SRT limitado à sua conta AWS Shield Advanced AWS WAF APIs e. AWS SRTos acessa APIs para colocar mitigações em sua conta somente com sua autorização explícita. Para obter mais informações, consulte a Suporte seção deste documento.

Você pode usar AWS Firewall Manager para configurar e gerenciar centralmente as regras de segurança, como AWS Shield Advanced proteções e AWS WAF regras, em toda a sua organização. Sua conta AWS Organizations de gerenciamento pode designar uma conta de administrador, que está autorizada a criar políticas do Firewall Manager. Essas políticas permitem definir critérios, como tipo de recurso e tags, que determinam onde as regras são aplicadas. Isso é útil quando você tem várias contas e deseja padronizar sua proteção.

Para obter mais informações sobre:

- AWS Managed Rules para AWS WAF, consulte AWS Managed Rules para AWS WAF.
- Usando a restrição geográfica para limitar o acesso à sua CloudFront distribuição, consulte Restringir a distribuição geográfica do seu conteúdo.
- Usando AWS WAF, consulte:
  - Começando com AWS WAF
  - Registrando informações ACL de tráfego na web
  - Visualizando uma amostra de solicitações da web
- Configurando regras baseadas em taxas, consulte Proteger sites e serviços usando regras baseadas em taxas para. AWS WAF
- Como gerenciar a implantação de regras em seus AWS recursos com o Firewall Manager, consulte:

- Introdução às AWS WAF políticas do Firewall Manager.
- Introdução às políticas avançadas do Firewall Manager Shield.

Redução da superfície de ataque

Outra consideração importante ao arquitetar uma AWS solução é limitar as oportunidades que um invasor tem de atacar seu aplicativo. Esse conceito é conhecido como redução da superfície de ataque. Recursos que não estão expostos à Internet são mais difíceis de atacar, o que limita as opções que um invasor tem para atingir a disponibilidade do seu aplicativo.

Por exemplo, se você não espera que os usuários interajam diretamente com determinados recursos, certifique-se de que esses recursos não estejam acessíveis pela Internet. Da mesma forma, não aceite tráfego de usuários ou aplicativos externos em portas ou protocolos que não sejam necessários para comunicação.

Na seção a seguir, AWS fornece as melhores práticas para orientá-lo na redução da superfície de ataque e na limitação da exposição do seu aplicativo à Internet.

Ofuscando AWS recursos (,,) BP1 BP4 BP5

Normalmente, os usuários podem usar um aplicativo de forma rápida e fácil sem exigir que AWS os recursos sejam totalmente expostos à Internet.

Grupos de segurança e rede ACLs (BP5)

A Amazon Virtual Private Cloud (AmazonVPC) permite que você provisione uma seção logicamente isolada da Nuvem AWS qual você pode lançar AWS recursos em uma rede virtual que você define.

Os grupos de segurança e a rede ACLs são semelhantes, pois permitem que você controle o acesso aos AWS recursos dentro do seuVPC. Mas os grupos de segurança permitem que você controle o tráfego de entrada e saída no nível da instância, enquanto a rede ACLs oferece recursos semelhantes no nível da VPC sub-rede. Não há cobrança adicional pelo uso de grupos de segurança ou redeACLs.

Você pode escolher se deseja especificar grupos de segurança ao executar uma instância ou associar a instância a um grupo de segurança posteriormente. Todo o tráfego da Internet para um grupo de segurança é negado implicitamente, a menos que você crie uma regra de permissão para permitir o tráfego.

Por exemplo, quando você tem EC2 instâncias da Amazon por trás de um Elastic Load Balancer, as instâncias em si não precisam estar acessíveis ao público e devem ser apenas privadasIPs. Em

vez disso, você poderia fornecer ao Elastic Load Balancer acesso às portas necessárias do ouvinte de destino usando uma regra de grupo de segurança que permite acesso a 0.0.0.0/0 (para evitar problemas de rastreamento de conexão — veja a observação abaixo) em conjunto com uma Lista de Controle de Acesso à Rede (NACL) na sub-rede do grupo-alvo para permitir que somente os intervalos de IP do Elastic Load Balancing se comuniquem com as instâncias. Isso garante que o tráfego da Internet não possa se comunicar diretamente com suas EC2 instâncias da Amazon, o que torna mais difícil para um invasor conhecer e impactar seu aplicativo.

Ao criar uma redeACLs, você pode especificar as regras de permissão e negação. Isso é útil se você quiser negar explicitamente certos tipos de tráfego para seu aplicativo. Por exemplo, você pode definir endereços IP (como CIDR intervalos), protocolos e portas de destino aos quais o acesso à sub-rede inteira é negado. Se seu aplicativo for usado somente para TCP tráfego, você poderá criar uma regra para negar todo o UDP tráfego ou vice-versa. Essa opção é útil ao responder a DDoS ataques porque permite criar suas próprias regras para mitigar o ataque quando você conhece a origem IPs ou outra assinatura.

Se você estiver inscrito AWS Shield Advanced, poderá registrar endereços IP elásticos como recursos protegidos. DDoSataques contra endereços IP elásticos que foram registrados como recursos protegidos são detectados mais rapidamente, o que pode resultar em um tempo mais rápido de mitigação. Quando um ataque é detectado, os sistemas de DDoS mitigação lêem a rede ACL que corresponde ao endereço IP elástico de destino e a aplicam na borda da AWS rede, e não no nível da sub-rede. Isso reduz significativamente o risco de impacto de vários DDoS ataques na camada de infraestrutura.

Para obter mais informações sobre como configurar grupos de segurança e rede ACLs para otimizar a DDoS resiliência, consulte Como ajudar a se preparar para DDoS ataques reduzindo sua superfície de ataque.

Para obter mais informações sobre o uso do Shield Advanced com endereços IP elásticos como recursos protegidos, consulte as etapas para se inscrever AWS Shield Advanced.

Protegendo sua origem (BP1,BP5)

Se você estiver usando a Amazon CloudFront com uma origem dentro da suaVPC, convém garantir que somente sua CloudFront distribuição possa encaminhar solicitações para sua origem. Com os cabeçalhos de solicitação Edge-to-Origin, você pode adicionar ou substituir o valor dos cabeçalhos de solicitação existentes ao CloudFront encaminhar solicitações para sua origem. Você pode usar os cabeçalhos personalizados de origem, por exemplo, o `X-Shared-Secret` cabeçalho, para ajudar a validar se as solicitações feitas à sua origem foram enviadas de. CloudFront

Para obter mais informações sobre como proteger sua origem com cabeçalhos personalizados de origem, consulte Adicionar cabeçalhos personalizados às solicitações de origem e restringir o acesso aos Application Load Balancers.

Para obter um guia sobre a implementação de uma solução de amostra para alternar automaticamente o valor dos cabeçalhos personalizados de origem para a restrição de acesso à origem, consulte Como aprimorar a segurança de CloudFront origem da Amazon com o Secrets AWS WAF Manager.

Como alternativa, você pode usar uma AWS Lambdafunção para atualizar automaticamente as regras do seu grupo de segurança para permitir somente CloudFront tráfego. Isso melhora a segurança de sua origem, ajudando a garantir que usuários mal-intencionados não possam contornar CloudFront e AWS WAF acessar seu aplicativo web.

Para obter mais informações sobre como proteger sua origem atualizando automaticamente seus grupos de segurança e o `X-Shared-Secret` cabeçalho, consulte Como atualizar automaticamente seus grupos de segurança para a Amazon CloudFront e AWS WAF usando AWS Lambda.

No entanto, a solução envolve configuração adicional e o custo de execução das funções Lambda. Para simplificar isso, agora introduzimos uma lista AWS de prefixos gerenciada para CloudFront limitar o HTTPS tráfego de HTTP entrada/às suas origens a partir apenas dos endereços IP voltados para a CloudFront origem. AWS-as listas de prefixos gerenciadas são criadas e mantidas por AWS e estão disponíveis para uso sem custo adicional. Você pode referenciar a lista de prefixos gerenciados CloudFront em suas regras de grupo de segurança (AmazonVPC), tabelas de rotas de sub-rede, regras comuns de grupos de segurança com AWS Firewall Manager e quaisquer outros AWS recursos que possam usar uma lista de prefixos gerenciados.

Para obter mais informações sobre o uso da lista AWS de prefixos gerenciada para a Amazon CloudFront, consulte Limitar o acesso às suas origens usando a lista de prefixos AWS gerenciada para a Amazon. CloudFront

> **Note**
>
> Conforme discutido em outras seções deste documento, confiar em grupos de segurança para proteger sua origem pode adicionar o rastreamento de conexões de grupos de segurança como um possível gargalo durante uma inundação de solicitações. A menos que você consiga filtrar solicitações maliciosas CloudFront usando uma política de armazenamento em cache que permita o armazenamento em cache, talvez seja melhor confiar nos cabeçalhos personalizados de origem, discutidos anteriormente, para ajudar a

validar se as solicitações feitas à sua origem foram enviadas de CloudFront, em vez de usar grupos de segurança. O uso de um cabeçalho de solicitação personalizado com uma regra de ouvinte do Application Load Balancer evita a limitação devido aos limites de rastreamento que podem afetar o estabelecimento de novas conexões com um balanceador de carga, permitindo que o Application Load Balancer escale com base no aumento do tráfego em caso de ataque. DDoS

Protegendo API endpoints () BP4

Quando você precisa expor um API ao público, existe o risco de o API front-end ser alvo de um DDoS ataque. Para ajudar a reduzir o risco, você pode usar o Amazon API Gateway como porta de entrada para aplicativos executados na Amazon ou em EC2 outros AWS Lambda lugares. Ao usar o Amazon API Gateway, você não precisa de seus próprios servidores para o API front-end e pode ofuscar outros componentes do seu aplicativo. Ao dificultar a detecção dos componentes do seu aplicativo, você pode ajudar a evitar que esses AWS recursos sejam alvo de um DDoS ataque.

Ao usar o Amazon API Gateway, você pode escolher entre dois tipos de API endpoints. A primeira é a opção padrão: API endpoints otimizados para borda que são acessados por meio de uma distribuição da Amazon. CloudFront No entanto, a distribuição é criada e gerenciada pelo API Gateway, então você não tem controle sobre ela. A segunda opção é usar um API endpoint regional que seja acessado do mesmo Região da AWS em que o seu REST API está implantado. AWS recomenda que você use o segundo tipo de endpoint e o associe à sua própria CloudFront distribuição da Amazon. Isso lhe dá controle sobre a CloudFront distribuição da Amazon e a capacidade de uso AWS WAF para proteção da camada de aplicação. Esse modo fornece acesso à capacidade de DDoS mitigação escalonada em toda a rede de borda AWS global.

Ao usar a Amazon CloudFront e AWS WAF com o Amazon API Gateway, configure as seguintes opções:

- Configure o comportamento do cache de suas distribuições para encaminhar todos os cabeçalhos para o endpoint regional do API Gateway. Ao fazer isso, CloudFront tratará o conteúdo como dinâmico e ignorará o armazenamento em cache do conteúdo.
- Proteja seu API Gateway contra acesso direto configurando a distribuição para incluir o cabeçalho personalizado de origem x-api-key, definindo o valor da APIchave no API Gateway.
- Proteja o back-end do excesso de tráfego configurando limites padrão ou de taxa de intermitência para cada método em seu. REST APIs

Para obter mais informações sobre a criação APIs com o Amazon API Gateway, consulte Amazon API Gateway Getting Started.

Técnicas operacionais

As técnicas de mitigação neste paper ajudam você a arquitetar aplicativos que são inerentemente resilientes contra ataques. DDoS Em muitos casos, também é útil saber quando um DDoS ataque está atingindo seu aplicativo para que você possa tomar medidas de mitigação. Esta seção discute as melhores práticas para obter visibilidade sobre comportamentos anormais, alertas e automação, gerenciar a proteção em grande escala e solicitar suporte adicional AWS .

Testes de carga

Teste regularmente a carga de seu aplicativo usando as diretrizes em nosso whitepaper de aplicativos de teste de carga com níveis de tráfego esperados e acima do esperado, para que você possa ver a eficácia de sua arquitetura, como suas políticas de Auto Scaling funcionam e como funciona o tratamento de erros. Teste o aumento e a diminuição esperados do tráfego, mas também o comportamento do tipo “multidão instantânea”. Teste novamente periodicamente ou antes de qualquer versão importante. Para testes de DDoS simulação de camada 3 ou 4, como SYN inundação, siga nossa Política de testes de DDoS simulação.

Métricas e alarmes

Como prática recomendada, você deve usar ferramentas de monitoramento de infraestrutura e aplicativos para verificar a disponibilidade do seu aplicativo e garantir que seu aplicativo não seja afetado por um DDoS evento. Como opção, você pode configurar as verificações de integridade do aplicativo e da infraestrutura do Route 53 para os recursos para ajudar a melhorar a detecção de DDoS eventos. Para obter mais informações sobre verificações de integridade AWS WAF, consulte o Guia do Desenvolvedor do Firewall Manager and Shield Advanced.

Quando uma métrica operacional importante se desvia substancialmente do valor esperado, um invasor pode estar tentando atingir a disponibilidade do seu aplicativo. A familiaridade com o comportamento normal do seu aplicativo significa que você pode agir mais rapidamente ao detectar uma anomalia. A Amazon CloudWatch pode ajudar monitorando os aplicativos nos quais você executa AWS. Por exemplo, você pode coletar e monitorar métricas, coletar e monitorar arquivos de log, definir alarmes e responder automaticamente às mudanças em seus AWS recursos.

Se você seguir a arquitetura de referência DDoS -resilient ao arquitetar seu aplicativo, os ataques comuns da camada de infraestrutura serão bloqueados antes de chegar ao seu aplicativo. Se você

estiver inscrito AWS Shield Advanced, terá acesso a várias CloudWatch métricas que podem indicar que seu aplicativo está sendo direcionado.

Por exemplo, você pode configurar alarmes para notificá-lo quando houver um DDoS ataque em andamento, para que você possa verificar a integridade do seu aplicativo e decidir se deseja se AWS SRT engajar. Você pode configurar a `DDoSDetected` métrica para informar se um ataque foi detectado. Se você quiser ser alertado com base no volume do ataque, você também pode usar a `DDoSAttackRequestsPerSecond` métrica`DDoSAttackBitsPerSecond`,`DDoSAttackPacketsPerSecond`, ou. Você pode monitorar essas métricas integrando-as CloudWatch com suas próprias ferramentas ou usando ferramentas fornecidas por terceiros, como Slack ou. PagerDuty

Um ataque na camada de aplicação pode elevar muitas CloudWatch métricas da Amazon. Se estiver usando AWS WAF, você pode usar CloudWatch para monitorar e ativar alarmes sobre aumentos nas solicitações que você configurou AWS WAF para serem permitidas, contadas ou bloqueadas. Isso permite que você receba uma notificação se o nível de tráfego exceder o que seu aplicativo pode suportar. Você também pode usar as métricas Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, EC2 Amazon e Auto Scaling que são CloudWatch rastreadas para detectar alterações que podem indicar um ataque. DDoS

A tabela a seguir lista as descrições das CloudWatch métricas que são comumente usadas para detectar e reagir aos DDoS ataques.

Tabela 3 - CloudWatch Métricas recomendadas da Amazon

Tópico	Métrica	Descrição
AWS Shield Advanced	`DDoSDetected`	Indica um DDoS evento para um nome de recurso específico da Amazon (ARN).
AWS Shield Advanced	`DDoSAttackBitsPerSecond`	O número de bytes observados durante um DDoS evento específicoARN. Essa métrica está disponível somente para DDoS eventos de camada 3 ou 4.

Tópico	Métrica	Descrição
AWS Shield Advanced	`DDoSAttackPacketsPerSecond`	O número de pacotes observados durante um DDoS evento para um determina doARN. Essa métrica está disponível somente para DDoS eventos de camada 3 ou 4.
AWS Shield Advanced	`DDoSAttackRequestsPerSecond`	O número de solicitações observadas durante um DDoS evento para um evento específicoARN. Essa métrica está disponível somente para DDoS eventos da camada 7 e é relatada somente para os eventos mais significativos da camada 7.
AWS WAF	`AllowedRequests`	O número de solicitações da web permitidas.
AWS WAF	`BlockedRequests`	O número de solicitações da web bloqueadas.
AWS WAF	`CountedRequests`	O número de solicitações da web contadas.
AWS WAF	`PassedRequests`	O número de solicitações aprovadas. Isso é usado somente para solicitações que passam por uma avaliação de grupo de regras sem corresponder a nenhuma das regras do grupo de regras.

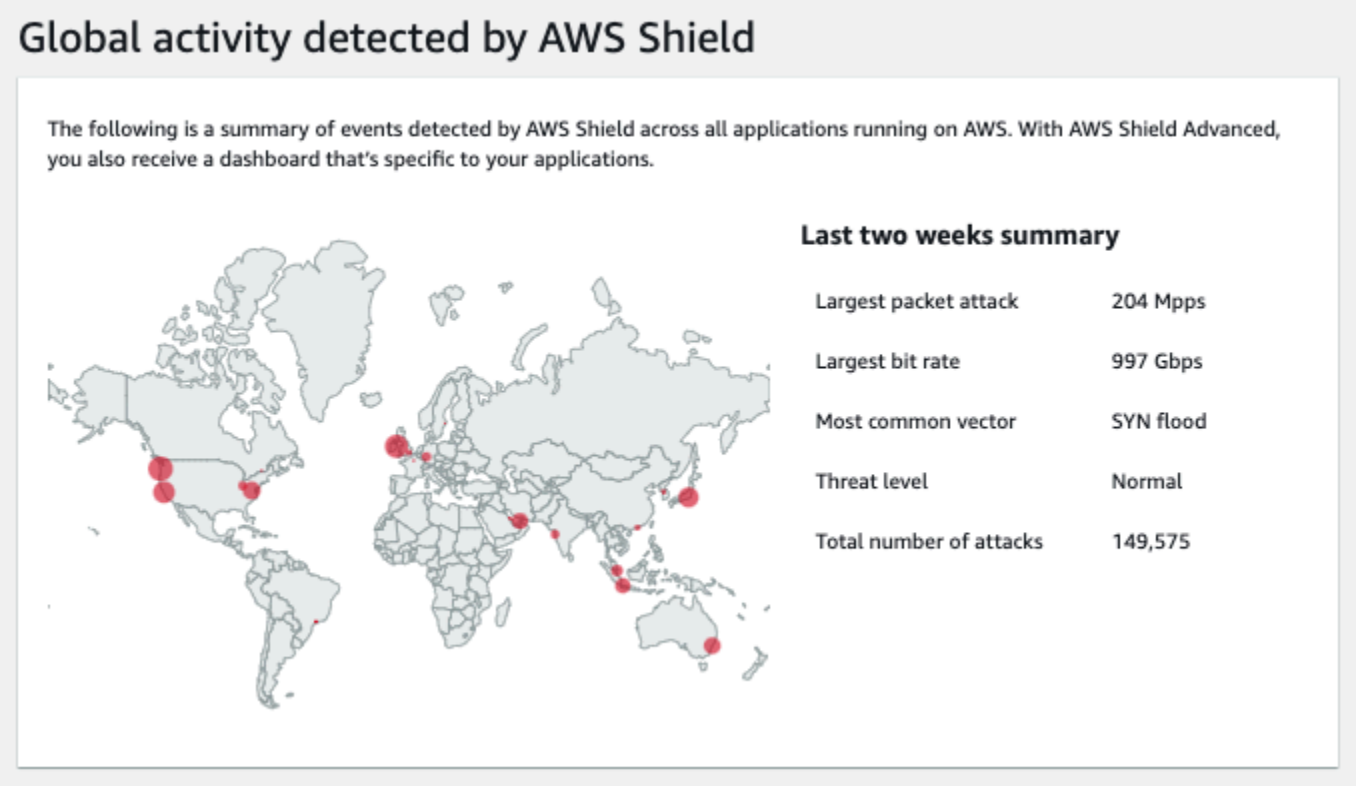
Tópico	Métrica	Descrição
Amazon CloudFront	`Requests`	O número de solicitações de HTTP /S.
Amazon CloudFront	`TotalErrorRate`	A porcentagem de todas as solicitações para as quais o código de HTTP status é `4xx` ou`5xx`.
Amazon Route 53	`HealthCheckStatus`	O status do endpoint da verificação de integridade.
Application Load Balancer	`ActiveConnectionCount`	O número total de TCP conexões simultâneas que estão ativas dos clientes ao balanceador de carga e do balanceador de carga aos destinos.
Application Load Balancer	`ConsumedLCUs`	O número de unidades de capacidade do balanceador de carga (LCU) usadas pelo balanceador de carga.
Application Load Balancer	`HTTPCode_ELB_4XX_Count` `HTTPCode_ELB_5XX_Count`	O número HTTP `4xx` ou os códigos de erro `5xx` do cliente gerados pelo balanceador de carga.
Application Load Balancer	`NewConnectionCount`	O número total de novas TCP conexões estabelecidas dos clientes com o balanceador de carga e do balanceador de carga com os destinos.

Tópico	Métrica	Descrição
Application Load Balancer	`ProcessedBytes`	O número total de bytes processados pelo load balancer.
Application Load Balancer	`RejectedConnectionCount`	O número de conexões que foram rejeitadas porque o load balancer atingiu o número máximo de conexões.
Application Load Balancer	`RequestCount`	O número de solicitações que foram processadas.
Application Load Balancer	`TargetConnectionErrorCount`	O número de conexões que não foram estabelecidas com êxito entre o balanceador de carga e o destino.
Application Load Balancer	`TargetResponseTime`	O tempo decorrido, em segundos, depois que a solicitação saiu do balancead or de carga até que uma resposta do destino fosse recebida.
Application Load Balancer	`UnHealthyHostCount`	O número de destinos considerados sem integridade.
Network Load Balancer	`ActiveFlowCount`	O número total de TCP fluxos simultâneos (ou conexões) de clientes para destinos.
Network Load Balancer	`ConsumedLCUs`	O número de unidades de capacidade do balanceador de carga (LCU) usadas pelo balanceador de carga.

Tópico	Métrica	Descrição
Network Load Balancer	`NewFlowCount`	O número total de novos TCP fluxos (ou conexões) estabelecidos de clientes para alvos no período.
Network Load Balancer	`ProcessedBytes`	O número total de bytes processados pelo balanceador de carga, incluindo cabeçalho s TCP /IP.
Global Accelerator	`NewFlowCount`	O número total de novos TCP UDP fluxos (ou conexões) estabelecidos de clientes para endpoints no período.
Global Accelerator	`ProcessedBytesIn`	O número total de bytes de entrada processados pelo acelerador, incluindo cabeçalhos TCP /IP.
Auto Scaling	`GroupMaxSize`	O tamanho máximo do grupo do Auto Scaling.
Amazon EC2	`CPUUtilization`	A porcentagem de unidades EC2 computacionais alocadas que estão atualmente em uso.
Amazon EC2	`NetworkIn`	A quantidade de bytes recebidos em todas as interfaces de rede pela instância.

Para obter mais informações sobre o uso da Amazon CloudWatch para detectar DDoS ataques ao seu aplicativo, consulte Getting Started with Amazon CloudWatch.

AWS inclui várias métricas e alarmes adicionais para notificá-lo sobre um ataque e ajudá-lo a monitorar os recursos do seu aplicativo. Use o AWS Shield console ou API forneça um resumo dos eventos por conta e detalhes sobre os ataques que foram detectados.



Atividade global detectada por AWS Shield

Além disso, o painel do ambiente global de ameaças fornece informações resumidas sobre todos os DDoS ataques que foram detectados pelo AWS. Essas informações podem ser úteis para entender melhor DDoS as ameaças em uma população maior de aplicativos, além das tendências de ataque e compará-las com os ataques que você possa ter observado.

Se você estiver inscrito AWS Shield Advanced, o painel de serviços exibirá métricas adicionais de detecção e mitigação e detalhes do tráfego de rede para eventos detectados em recursos protegidos. AWS Shield avalia o tráfego para seu recurso protegido em várias dimensões. Quando uma anomalia é detectada, AWS Shield cria um evento e relata a dimensão do tráfego em que a anomalia foi observada. Com uma mitigação posicionada, isso protege seu recurso de receber tráfego excessivo e tráfego que corresponda a uma assinatura de DDoS evento conhecida.

As métricas de detecção são baseadas em amostras de fluxos ou AWS WAF registros de rede quando uma web ACL está associada ao recurso protegido. As métricas de mitigação são baseadas

no tráfego observado pelos sistemas de DDoS mitigação da Shield. As métricas de mitigação são uma medida mais precisa do tráfego em seu recurso.

A métrica dos principais colaboradores da rede fornece informações sobre a origem do tráfego durante um evento detectado. Você pode visualizar os contribuidores de maior volume e classificar por aspectos como protocolo, porta de origem e TCP sinalizadores. A métrica dos principais colaboradores inclui métricas para todo o tráfego observado no recurso em várias dimensões. Ele fornece dimensões métricas adicionais que você pode usar para entender o tráfego de rede enviado ao seu recurso durante um evento. Lembre-se de que, para ataques de camada 3 ou 4 sem reflexão, os endereços IP de origem podem ter sido falsificados e não podem ser confiáveis.

O painel do serviço também inclui detalhes sobre as ações tomadas automaticamente para mitigar DDoS os ataques. Essas informações facilitam a investigação de anomalias, a exploração das dimensões do tráfego e a compreensão melhor das ações tomadas pelo Shield Advanced para proteger sua disponibilidade.

Registro em log

Ative o registro útil em todos os serviços de acordo com nosso guia de registro e monitoramento para proprietários de aplicativos para maximizar a visibilidade e ajudar na solução de problemas. Isso inclui, mas não está limitado a:

- AWS CloudTrail
- Registros do AWS WAF
- CloudFrontregistros de acesso
- VPCRegistros de fluxo (consulte Registrar e visualizar fluxos de tráfego de rede) — inclua um `tcp-flags` campo nos campos incluídos para maximizar a visibilidade
- ELBregistros de acesso (ALB, CLB, NLB)
- Registros de HTTP acesso ao servidor Web
- Registro de segurança do sistema operacional
- Registro de aplicativos

Gerenciamento de visibilidade e proteção em várias contas

Em cenários em que você opera em vários componentes Contas da AWS e tem vários componentes para proteger, o uso de técnicas que permitem operar em escala e reduzir a sobrecarga operacional

aumenta seus recursos de mitigação. Ao gerenciar recursos AWS Shield Advanced protegidos em várias contas, você pode configurar o monitoramento centralizado usando AWS Firewall Manager e. AWS Security Hub Com o Firewall Manager, você pode criar uma política de segurança que imponha a conformidade de DDoS proteção em todas as suas contas. Você pode usar esses dois serviços juntos para gerenciar seus recursos protegidos em várias contas e centralizar o monitoramento desses recursos.

O Security Hub se integra automaticamente ao Firewall Manager, permitindo que os clientes do Shield Advanced visualizem as descobertas de segurança em um único painel, junto com outros alertas de segurança de alta prioridade e status de conformidade.

Por exemplo, quando o Shield Advanced detecta tráfego anômalo destinado a um recurso protegido em qualquer parte do Conta da AWS escopo, essa descoberta será visível no console do Security Hub. Se configurado, o Firewall Manager pode automaticamente colocar o recurso em conformidade, criando-o como um recurso protegido pelo Shield Advanced e, em seguida, atualizando o Security Hub quando o recurso estiver em um estado compatível.

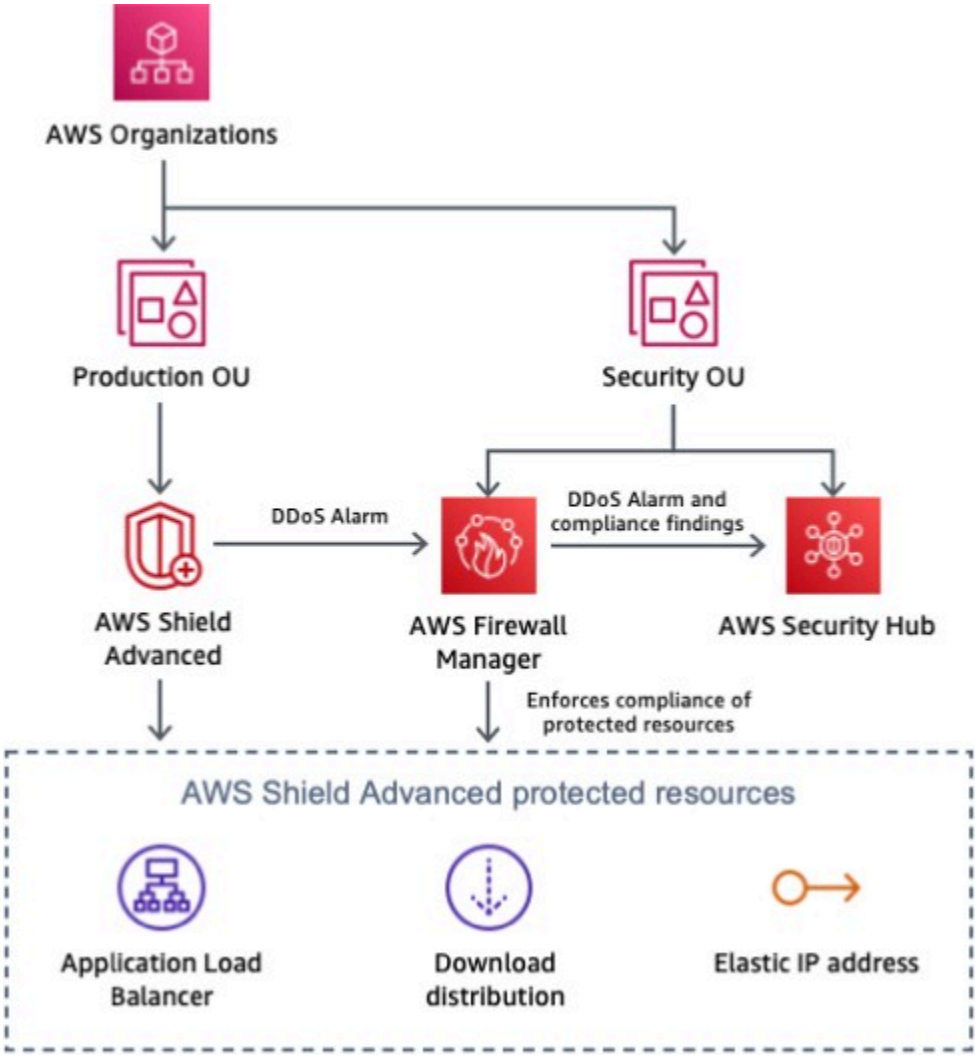


Diagrama de arquitetura mostrando recursos AWS Shield protegidos pelo monitoramento com o Firewall Manager e o Security Hub

Para obter mais informações sobre o monitoramento central dos recursos protegidos do Shield, consulte Configurar o monitoramento centralizado para DDoS eventos e remediar automaticamente recursos não compatíveis.

Estratégia de resposta a incidentes e runbooks

Desenvolver uma estratégia de resposta a incidentes de DDoS ataque e criar um processo de resposta a incidentes de segurança em torno dela é crucial para todas as organizações. Uma abordagem recomendada é modelar seu manual de resposta com base nas NIST etapas sugeridas, como coleta de evidências, mitigação, recuperação e realização de análises pós-incidentes. Por exemplo, um manual de resposta para DoS ou DDoS ataques de aplicativos web é fornecido

como exemplo. Recursos adicionais estão disponíveis no Guia de Resposta a Incidentes de AWS Segurança.

Suporte

Se você sofrer um ataque, também poderá se beneficiar do AWS suporte para avaliar a ameaça e revisar a arquitetura do seu aplicativo, ou talvez queira solicitar outra assistência. É importante criar um plano de resposta para DDoS ataques antes de um evento real. As melhores práticas descritas neste paper pretendem ser medidas proativas que você implementa antes de iniciar um aplicativo, mas DDoS ataques contra seu aplicativo ainda podem ocorrer. Analise as opções nesta seção para determinar os recursos de suporte mais adequados ao seu cenário. Sua equipe de contas pode avaliar seu caso de uso e aplicação e ajudar com suas perguntas ou desafios específicos.

Se você estiver executando cargas de trabalho de produção AWS, considere assinar o Business Support, que fornece acesso 24 horas por dia, 7 dias por semana, aos engenheiros de suporte de nuvem que podem ajudar com DDoS problemas de ataque. Se você estiver executando cargas de trabalho de missão crítica, considere o Enterprise Support, que oferece a capacidade de abrir casos críticos e receber a resposta mais rápida de um engenheiro sênior de suporte de nuvem.

Se você está inscrito AWS Shield Advanced e também está inscrito no Business Support ou no Enterprise Support, você pode configurar o engajamento proativo do Shield. Ele permite que você configure verificações de saúde, associe seus recursos e forneça informações de contato operacionais 24 horas por dia, 7 dias por semana. Quando o Shield detectar sinais de degradação DDoS e as verificações de integridade de seu aplicativo mostrarem sinais de degradação, AWS SRT entrará em contato com você de forma proativa. Esse é nosso modelo de engajamento recomendado, pois permite tempos de AWS SRT resposta mais rápidos e permite iniciar AWS SRT a solução de problemas antes mesmo de o contato ser estabelecido com você.

Para obter mais informações, consulte Comparar AWS Support planos.

O recurso de engajamento proativo exige que você configure uma verificação de integridade do Route 53 que meça com precisão a integridade do seu aplicativo e esteja associada ao recurso protegido pelo Shield Advanced. Depois que uma verificação de integridade do Route 53 é associada ao console Shield, o sistema de detecção Shield Advanced usa o status da verificação de saúde como um indicador da integridade do seu aplicativo. O recurso de detecção com base na integridade do Shield Advanced garantirá que você seja notificado e que as mitigações sejam aplicadas mais rapidamente quando seu aplicativo não estiver íntegro. AWS SRTentraremos em contato com você para solucionar se o aplicativo não íntegro está sendo alvo de um DDoS ataque e implementará atenuações adicionais conforme necessário.

A conclusão da configuração do engajamento proativo inclui a adição de detalhes de contato no console Shield. AWS SRTusaremos essas informações para entrar em contato com você. Você pode configurar até dez contatos e fornecer notas adicionais se tiver requisitos ou preferências de contato específicos. Proativo

os contatos de engajamento devem ter uma função 24 horas por dia, 7 dias por semana, como um centro de operações de segurança ou um indivíduo que esteja imediatamente disponível.

Você pode habilitar o engajamento proativo para todos os recursos ou para selecionar os principais recursos de produção em que o tempo de resposta é fundamental. Isso é feito atribuindo verificações de saúde somente a esses recursos.

Você também pode escalar AWS SRT criando um AWS Support caso usando o AWS Support console (é necessário fazer login) ou o Support API se tiver um evento DDoS relacionado que afete a disponibilidade do seu aplicativo.

Conclusão

As melhores práticas descritas neste paper podem ajudá-lo a criar uma arquitetura DDoS resiliente que proteja a disponibilidade do seu aplicativo, evitando muitos ataques comuns à infraestrutura e à camada DDoS de aplicativos. A extensão em que você segue essas melhores práticas ao arquitetar seu aplicativo influenciará o tipo, o vetor e o volume de DDoS ataques que você pode mitigar. Você pode incorporar resiliência sem assinar um serviço de DDoS mitigação. Ao optar por assinar, AWS Shield Advanced você obtém recursos adicionais de suporte, visibilidade, mitigação e proteção de custos que protegem ainda mais uma arquitetura de aplicativos já resiliente.

Colaboradores

Os colaboradores deste documento incluem:

- Rodrigo Ferroni, especialista em segurança AWS TAM
- Dmitriy Novikov, arquiteto de soluções AWS
- Achraf Souk, arquiteto de soluções AWS
- Joanna Knox, Engenharia AWS Support
- Anuj Butail, AWS arquiteto de soluções
- Harith Gaddamanugu, especialista em Edge SA AWS

Outras fontes de leitura

Para obter informações adicionais, consulte:

- Diretrizes para implementação AWS WAF (AWS whitepaper)
- NIS301 — Re:inForce 2023: Como a inteligência AWS contra ameaças se torna regras gerenciadas de firewall (vídeo) YouTube
- NET314- RE: Invent 2022: Construindo aplicativos DDoS resilientes usando (vídeo) AWS Shield YouTube
- SEC321- re:Invent 2020: fique à frente da curva com os escalonamentos da equipe de DDoS resposta (vídeo) YouTube
- William Hill: DDoS Proteção de alto desempenho com AWS - 2020 (YouTubevídeo)
- SEC407 - re:Invent 2019: Uma defense-in-depth abordagem para criar aplicativos web (vídeo) YouTube
- Melhores práticas para DDoS mitigação em AWS — 2018 (vídeo) YouTube
- SID324— re:Invent 2017: Automatizando a DDoS resposta na nuvem (vídeo) YouTube
- CTD304 — Re:Invent 2017: a jornada da Dow Jones e do Wall Street Journal para gerenciar picos de tráfego enquanto (vídeo) YouTube
- Mitigação DDoS e ameaças na camada de aplicação (vídeo) YouTube
- CTD310 — re:Invent 2017: Viver no limite é mais seguro do que você pensa! Construindo forte com a Amazon (YouTube vídeo)
- CloudFront, AWS Shield, e AWS WAF (YouTube vídeo)

Revisões do documento

Para ser notificado sobre as atualizações deste whitepaper, assine o RSS feed.

Alteração	Descrição	Data
Atualização do whitepaper	Adicionado OAC para proteção de custos CloudFront e DNS curinga. Discussão ampliada sobre técnicas operacionais, armazenamento em cache, regras baseadas em taxas e grupos de regras gerenciados. Foi adicionado local ao diagrama de arquitetura, removeu a duplicação e esclareceu o texto para remover a ambigüidade.	9 de agosto de 2023
Atualização do whitepaper	Revisado para maior clareza; atualizado para incluir as recomendações e os recursos mais recentes: rastreamento de conexão de grupos de segurança e DDoS mitigação automática da camada de aplicação Shield Advanced.	13 de abril de 2022
Atualização do whitepaper	Atualizado para incluir as recomendações e os recursos mais recentes. AWS Global Accelerator é adicionado como parte de uma proteção abrangente na borda. AWS Firewall Manager para monitoramento centralizado de DDoS eventos e correção	21 de setembro de 2021

	automática de recursos não compatíveis.	
Atualização do whitepaper	Atualizado para esclarecer a interrupção do cache na seção Detectar e filtrar solicitações maliciosas da Web (BP1,BP2) ELB e o ALB uso na seção Escalar para absorver (BP6). Diagramas atualizados e a Tabela 2, marcada como “Escolha da região”. comoBP8. BP7Seção atualizada com mais detalhes.	18 de dezembro de 2019
Atualização do whitepaper	Atualizado para incluir o AWS WAF registro como uma prática recomendada.	1º. de dezembro de 2018
Atualização do whitepaper	Atualizado para incluir AWS Shield AWS WAF recursos AWS Firewall Manager e melhores práticas relacionadas.	1º de junho de 2018
Atualização do whitepaper	Orientação de arquitetura prescritiva adicionada e atualizada para incluir. AWS WAF	1 de junho de 2016
Publicação inicial	Publicação do whitepaper.	1.º de junho de 2015

Avisos

Os clientes são responsáveis por fazer a própria avaliação independente das informações contidas neste documento. Este documento: (a) é apenas para fins informativos, (b) representa ofertas e práticas atuais de AWS produtos, que estão sujeitas a alterações sem aviso prévio, e (c) não cria nenhum compromisso ou garantia de AWS suas afiliadas, fornecedores ou licenciadores. AWS os produtos ou serviços são fornecidos “como estão” sem garantias, representações ou condições de qualquer tipo, expressas ou implícitas. As responsabilidades e obrigações de AWS seus clientes são controladas por AWS contratos, e este documento não faz parte nem modifica nenhum contrato entre AWS e seus clientes.

AWS Glossário

Para obter a AWS terminologia mais recente, consulte o AWS glossário na Glossário da AWS Referência.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.