AWS Documento técnico

# AWS Mejores prácticas para la DDoS resiliencia

# AWS Mejores prácticas para la DDoS resiliencia: AWS Documento técnico

# Table of Contents

# AWS Mejores prácticas para la DDoS resiliencia

Fecha de publicación: 9 de agosto de 2023 (Revisiones del documento)

Es importante proteger su empresa del impacto de los ataques de denegación de servicio distribuido (DDoS), así como de otros ciberataques. Mantener la confianza de los clientes en su servicio mediante el mantenimiento de la disponibilidad y la capacidad de respuesta de su aplicación es una prioridad absoluta. También querrá evitar costes directos innecesarios cuando su infraestructura deba ampliarse en respuesta a un ataque. Amazon Web Services (AWS) se compromete a proporcionarle las herramientas, las mejores prácticas y los servicios para defenderse de los malos actores en Internet. El uso de los servicios adecuados AWS ayuda a garantizar una alta disponibilidad, seguridad y resiliencia.

En este documento técnico, encontrará AWS una DDoS guía prescriptiva para mejorar la resiliencia de las aplicaciones en las que se ejecutan. AWS Incluye una arquitectura DDoS de referencia flexible que se puede utilizar como guía para ayudar a proteger la disponibilidad de las aplicaciones. Este documento técnico también describe diferentes tipos de ataques, como los ataques a la capa de infraestructura y los ataques a la capa de aplicación. AWS explica qué prácticas recomendadas son las más eficaces para gestionar cada tipo de ataque. Además, se describen los servicios y características que se integran en una estrategia de DDoS mitigación, así como la forma en que se puede utilizar cada uno de ellos para ayudar a proteger sus aplicaciones.

Este paper está dirigido a los responsables de la toma de decisiones de TI y a los ingenieros de seguridad que estén familiarizados con los conceptos básicos de redes, seguridad y AWS. Cada sección contiene enlaces a AWS la documentación que proporciona más detalles sobre las mejores prácticas o capacidades.

AWS detecta más de un millón de DDoS ataques al año y mitiga miles a diario contra nuestros clientes. Según nuestro equipo de Shield Response (SRT), la mayoría de los clientes que sufren un impacto empresarial a causa de DDoS los ataques no han implementado las recomendaciones de esta guía.

## ¿Usa Well-Architected?

El marco de AWS Well-Architected le ayuda a entender las ventajas y desventajas de las decisiones que toma al crear sistemas en la nube. Los seis pilares del marco le permitirán aprender las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes, rentables

y sostenibles. Con esta AWS Well-Architected Toolherramienta, disponible de forma gratuita en la página AWS Management Consoleweb (es necesario iniciar sesión), puede comparar sus cargas de trabajo con estas prácticas recomendadas respondiendo a una serie de preguntas para cada pilar.

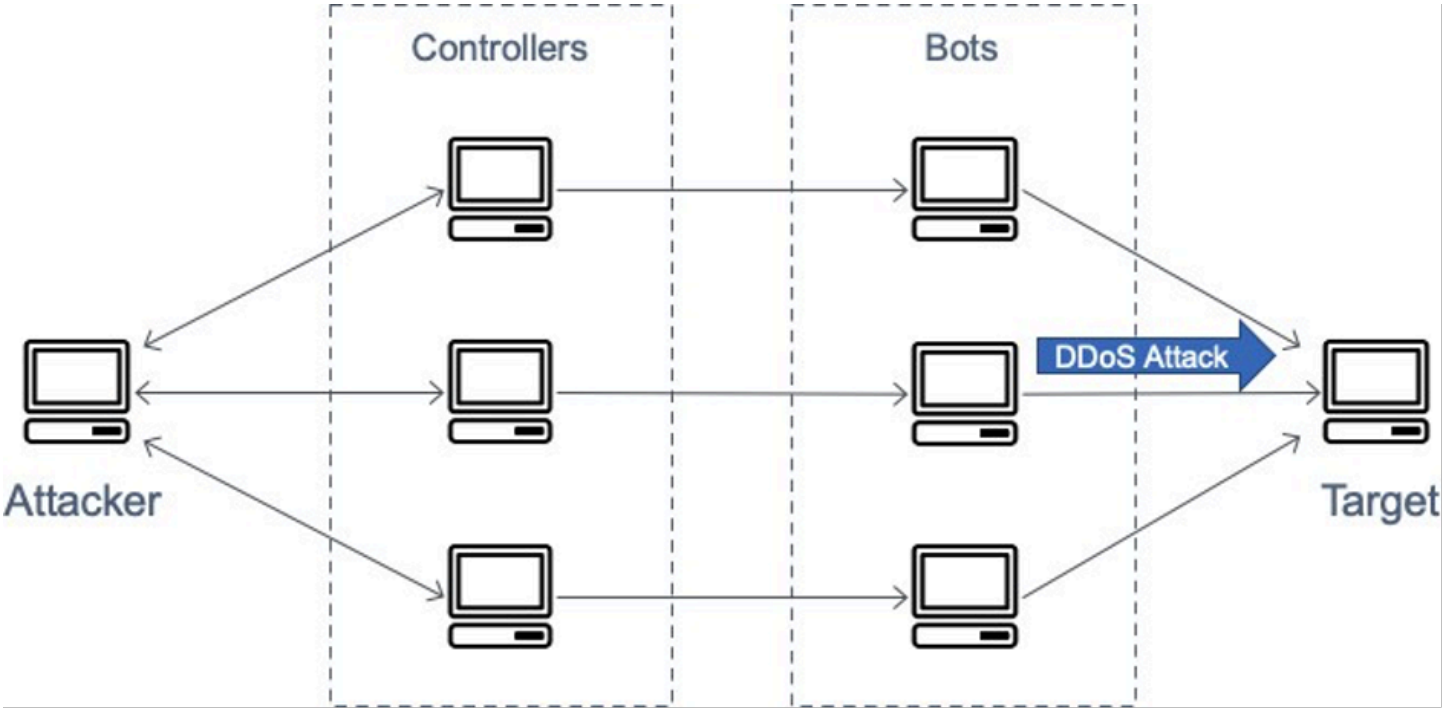
Para obtener más orientación experta y las mejores prácticas para su arquitectura de nube (consulte las implementaciones de la arquitectura, los diagramas y los documentos técnicos), consulte el Centro de Arquitectura.AWS

# Introducción a los ataques de denegación de servicio

Un ataque o evento de denegación de servicio (DoS) es un intento deliberado de hacer que un sitio web o una aplicación no estén disponibles para los usuarios, por ejemplo, inundándolos con tráfico de red. Los atacantes utilizan diversas técnicas que consumen grandes cantidades de ancho de banda de la red o inutilizan otros recursos del sistema, lo que interrumpe el acceso de los usuarios legítimos. En su forma más simple, un atacante solitario utiliza una única fuente para llevar a cabo un ataque DoS contra un objetivo, como se muestra en la siguiente figura.


Un diagrama que representa un ataque de DoS

En un ataque de denegación de servicio distribuido (DDoS), un atacante utiliza varias fuentes para organizar un ataque contra un objetivo. Estas fuentes pueden incluir grupos distribuidos de ordenadores, enrutadores, dispositivos de IoT y otros puntos finales infectados con malware. En la siguiente figura se muestra una red de hosts comprometidos que participan en el ataque y que generan una avalancha de paquetes o solicitudes que abruman al objetivo.



Un diagrama que representa un DDoS ataque

El modelo de interconexión de sistemas abiertos (OSI) consta de siete capas, que se describen en la siguiente tabla. DDoSlos ataques son más comunes en las capas 3, 4, 6 y 7.

- Los ataques de capa 3 y 4 corresponden a las capas de red y transporte del OSI modelo. En este documento técnico, los denominamos AWS colectivamente ataques a la capa de infraestructura.
- Los ataques de capa 6 y 7 corresponden a las capas de presentación y aplicación del OSI modelo. Este documento técnico los aborda juntos como ataques a la capa de aplicación.

Este paper analiza estos tipos de ataques en las secciones siguientes.

Tabla 1: OSI modelo

| # | Capa | Unidad | Descripción | Ejemplos vectoriales |
|---|---|---|---|---|
| 7 | Aplicación | Datos | Del proceso de red a la aplicación | HTTPinundaciones, inundaciones DNS de consultas |
| 6 | Presentación | Datos | Representación y cifrado de datos | Abuso de Transport Layer Security (TLS) |
| 5 | Sesión | Datos | Comunicación entre anfitriones | N/A |
| 4 | Transporte | Segmentos | nd-to-end Conexiones electrónicas y confiabilidad | Sincronizar (SYN) inundaciones |
| 3 | Network | Paquetes | Determinación de rutas y | Ataques de reflexión del |

| # | Capa | Unidad | Descripción | Ejemplos vectoriales |
|---|---|---|---|---|
| | | | direccionamiento lógico | User Datagram Protocol (UDP) |
| 2 | Enlace de datos | Fotogramas | Direccion amiento físico | N/A |
| 1 | Física | Bits | Transmisión multimedia, de señales y binaria | N/A |

# Ataques a la capa de infraestructura

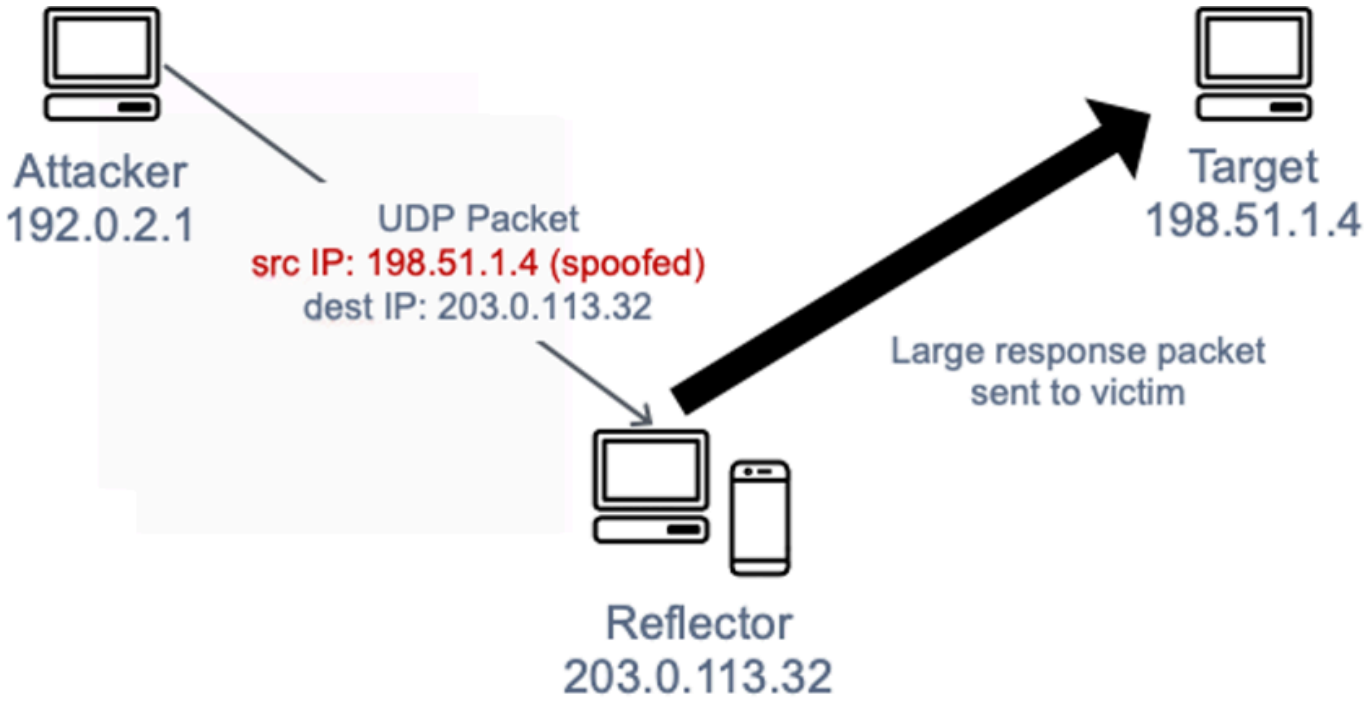
Los ataques más comunes, DDoS los ataques de reflexión y las SYN inundaciones del Protocolo de datagramas de usuario (User Datagram ProtocolUDP), son los ataques a la capa de infraestructura. Un atacante puede utilizar cualquiera de estos métodos para generar grandes volúmenes de tráfico que pueden inundar la capacidad de una red o agotar los recursos de sistemas como los servidores, los firewalls, el sistema de prevención de intrusiones (IPS) o el equilibrador de carga. Si bien estos ataques pueden ser fáciles de identificar, para mitigarlos de forma eficaz, es necesario disponer de una red o sistemas que amplíen la capacidad con mayor rapidez que la avalancha de tráfico entrante. Esta capacidad adicional es necesaria para filtrar o absorber el tráfico de los ataques y permitir que el sistema y la aplicación respondan al tráfico de clientes legítimos.

## UDPataques de reflexión

UDPlos ataques de reflexión explotan el hecho de que UDP se trata de un protocolo sin estado. Los atacantes pueden crear un paquete de UDP solicitud válido que incluya la dirección IP del objetivo del ataque como dirección IP de UDP origen. El atacante ahora ha falsificado (falsificado) la IP de origen del paquete de solicitud. UDP El UDP paquete contiene la IP de origen falsificada y el atacante lo envía a un servidor intermedio. Se engaña al servidor para que envíe sus paquetes de UDP respuesta a la IP de la víctima objetivo en lugar de devolverlos a la dirección IP del atacante. Se utiliza el servidor intermedio porque genera una respuesta varias veces mayor que el paquete de solicitud, lo que amplifica de forma efectiva la cantidad de tráfico de ataque que se envía a la dirección IP objetivo.

El factor de amplificación es la relación entre el tamaño de la respuesta y el tamaño de la solicitud y varía según el protocolo que utilice el atacante: DNS Network Time Protocol (NTP), Simple Service Directory Protocol (SSDP), Connectionless Lightweight Directory Access Protocol (CLDAP), Memcached, Character Generator Protocol (CharGen) o Quote of the Day (QOTD).

Por ejemplo, el factor de amplificación DNS puede ser de 28 a 54 veces el número original de bytes. Por lo tanto, si un atacante envía una carga útil de solicitud de 64 bytes a un DNS servidor, puede generar más de 3400 bytes de tráfico no deseado hacia el objetivo del ataque. UDPLos ataques de reflexión generan un mayor volumen de tráfico en comparación con otros ataques. La siguiente figura ilustra la táctica de reflexión y el efecto de amplificación.

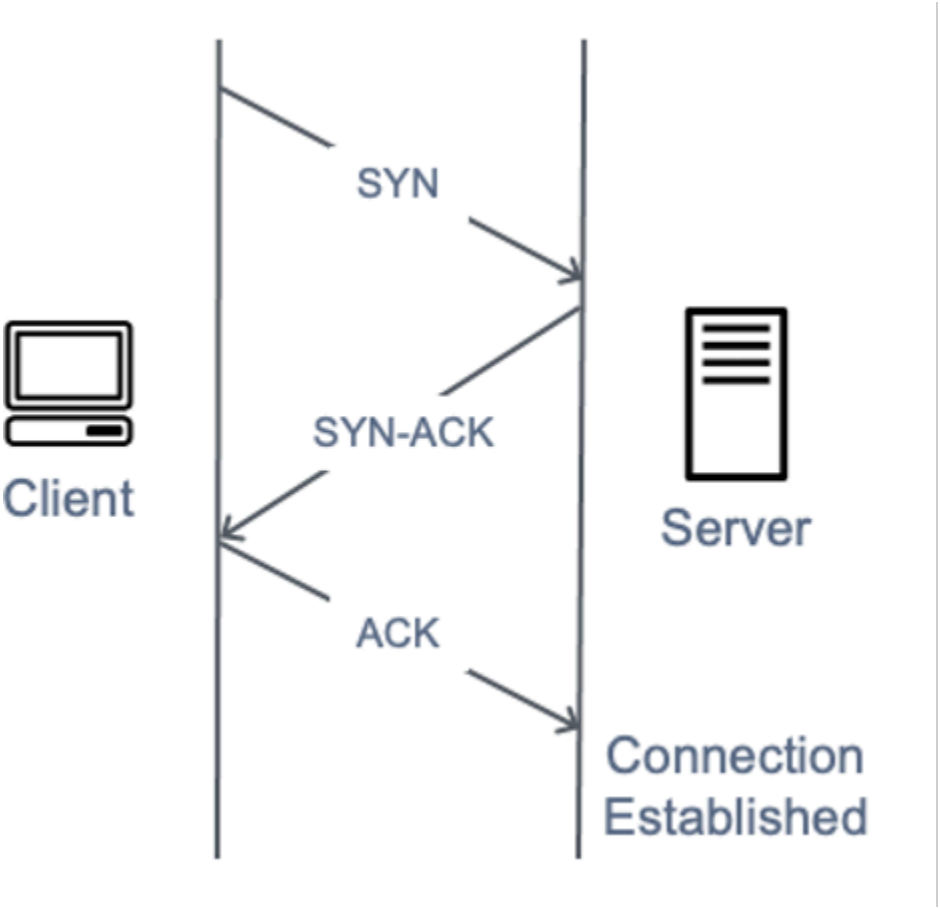



Un diagrama que representa un ataque de UDP reflexión

Cabe señalar que los ataques de reflexión, si bien proporcionan a los atacantes una amplificación «gratuita», requieren la capacidad de suplantación de IP y, a medida que un número cada vez mayor de proveedores de red adoptan la validación de direcciones de origen en todas partes (SAVE) o BCP38, se elimina esta capacidad, obligando a los proveedores de DDoS servicios a detener los ataques de reflexión o a trasladarse a centros de datos y proveedores de redes que no implementan la validación de direcciones de origen.

# SYNataques por inundación

Cuando un usuario se conecta a un servicio del Protocolo de Control de Transmisión (TCP), como un servidor web, su cliente envía un SYN paquete. El servidor devuelve un paquete de acuse de recibo de sincronización (SYN-ACK) y, finalmente, el cliente responde con un paquete de acuse de recibo (ACK), que completa el apretón de manos tridireccional esperado. La siguiente imagen ilustra este típico apretón de manos.




Un diagrama que representa un apretón de manos a tres SYN bandas

En un ataque de SYN inundación, un cliente malintencionado envía una gran cantidad de SYN paquetes, pero nunca envía los ACK paquetes finales para completar el apretón de manos. El servidor se queda esperando una respuesta a TCP las conexiones medio abiertas y la idea es que el objetivo acabe quedándose sin capacidad para aceptar nuevas TCP conexiones, lo que impide que nuevos usuarios se conecten al servidor. Sin embargo, el impacto real es más matizado. Todos los sistemas operativos modernos implementan SYN cookies de forma predeterminada como mecanismo para contrarrestar el agotamiento de la tabla de estados provocado por los ataques de SYN inundación. Una vez que la longitud de la SYN cola alcanza un umbral predeterminado, el

servidor responde con un SYN - ACK que contiene un número de secuencia inicial elaborado, sin crear una entrada en la colaSYN. Si, a continuación, el servidor recibe un número de confirmación ACK que contiene un número de confirmación incrementado correctamente, podrá añadir la entrada a su tabla de estados y continuar con normalidad. El impacto real de SYN las inundaciones en los dispositivos de destino suele ser el CPU agotamiento y la capacidad de la red. Sin embargo, los dispositivos con un estado intermedio, como los firewalls (o el seguimiento de conexiones de grupos de EC2 seguridad), pueden agotarse según la tabla de TCP estados e interrumpir las nuevas conexiones.

### TCPreflexión en el medio-caja

Este vector de ataque relativamente nuevo se dio a conocer por primera vez en un documento técnico académico publicado en agosto de 2021, en el que se explicaba cómo el TCP incumplimiento de los firewalls nacionales y los disponibles en el mercado podía provocar que se engañaran para que se convirtieran en un vector de amplificación. TCP Hemos visto estos ataques «de forma espontánea» desde principios de 2022 y los seguimos viendo en la actualidad. El factor de amplificación varía debido a las diferentes formas en que los proveedores han implementado esta «función», pero puede superar la amplificación de MemcachedUDP.

## Ataques a la capa de aplicación

Un atacante puede atacar la propia aplicación mediante un ataque de capa 7 o capa de aplicación. En estos ataques, similares a los ataques de infraestructura SYN inundada, el atacante intenta sobrecargar funciones específicas de una aplicación para hacer que la aplicación no esté disponible o no responda a los usuarios legítimos. A veces, esto se puede lograr con volúmenes de solicitudes muy bajos que generan solo un pequeño volumen de tráfico de red. Esto puede hacer que el ataque sea difícil de detectar y mitigar. Entre los ejemplos de ataques a la capa de aplicación se incluyen HTTP las inundaciones, los ataques que destruyen la memoria caché y las inundaciones. WordPress XML RPC

- En un ataque de HTTP inundación, un atacante envía HTTP solicitudes que parecen provenir de un usuario válido de la aplicación web. Algunas HTTP inundaciones se dirigen a un recurso específico, mientras que HTTP las inundaciones más complejas intentan emular la interacción humana con la aplicación. Esto puede aumentar la dificultad de utilizar técnicas de mitigación comunes, como la limitación de la tasa de solicitudes.
- Los ataques de destrucción de memoria caché son un tipo de HTTP inundación que utiliza variaciones en la cadena de consulta para evitar el almacenamiento en caché de la red de entrega

de contenido. CDN En lugar de poder devolver los resultados almacenados en caché, CDN deben ponerse en contacto con el servidor de origen para cada solicitud de página, y estas búsquedas de origen suponen una carga adicional para el servidor web de aplicaciones.

- En el caso de un WordPress XMLataque de RPC inundación, también conocido como «inundación de WordPress pingback», un atacante ataca un sitio web alojado en el software de gestión de WordPress contenido. El atacante hace un mal uso de la RPC API función XML- para generar una avalancha de HTTP solicitudes. La función pingback permite que un sitio web alojado en WordPress (Sitio A) notifique a otro WordPress sitio (Sitio B) a través de un enlace que el Sitio A ha creado al Sitio B. El Sitio B intenta entonces buscar el Sitio A para verificar la existencia del enlace. En una avalancha de pingbacks, el atacante hace un uso indebido de esta capacidad para provocar que el sitio B ataque el sitio A. Este tipo de ataque tiene una firma clara: «`WordPress:`» suele estar presente en el agente de usuario del encabezado de la solicitud. HTTP

Existen otras formas de tráfico malicioso que pueden afectar a la disponibilidad de una aplicación. Los robots rastreadores automatizan los intentos de acceder a una aplicación web para robar contenido o registrar información de la competencia, como los precios. Los ataques de fuerza bruta y de robo de credenciales son intentos programados para obtener acceso no autorizado a áreas seguras de una aplicación. No se trata estrictamente de DDoS ataques, pero su naturaleza automatizada puede parecerse a la de un DDoS ataque y pueden mitigarse mediante la implementación de algunas de las mismas prácticas recomendadas que se describen en este paper.

Los ataques a la capa de aplicación también pueden dirigirse a los servicios del Sistema de Nombres de Dominio (Domain Name SystemDNS). El más común de estos ataques es una inundación de DNS consultas en la que un atacante utiliza muchas DNS consultas bien formadas para agotar los recursos de un DNS servidor. Estos ataques también pueden incluir un componente de destrucción de caché en el que el atacante distribuye aleatoriamente la cadena del subdominio para evitar la caché local de cualquier solucionador determinado. DNS Como resultado, el solucionador no puede aprovechar las consultas de dominio almacenadas en caché y, en su lugar, debe ponerse en contacto repetidamente con el servidor autorizado, lo que amplifica el ataque. DNS

Si una aplicación web se entrega a través de Transport Layer Security (TLS), un atacante también puede optar por atacar el TLS proceso de negociación. TLSes caro desde el punto de vista computacional, por lo que un atacante, al generar una carga de trabajo adicional en el servidor para procesar datos ilegibles (o ininteligibles (texto cifrado)) como un apretón de manos legítimo, puede reducir la disponibilidad del servidor. En una variante de este ataque, un atacante completa el protocolo de enlace pero renegocia permanentemente el TLS método de cifrado. Como alternativa, un atacante puede intentar agotar los recursos del servidor abriendo y cerrando varias sesiones. TLS

# Técnicas de mitigación

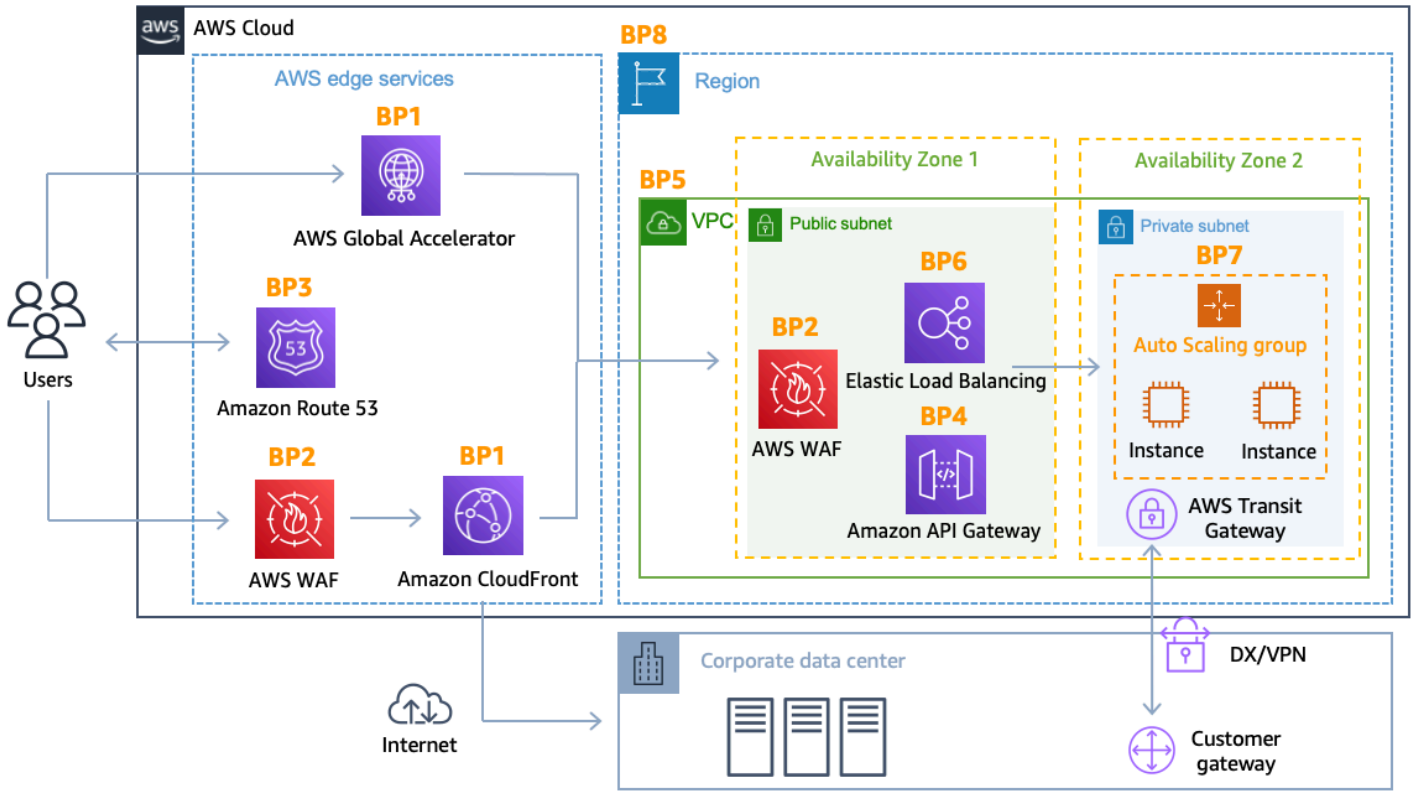
Algunas formas de DDoS mitigación se incluyen automáticamente en los AWS servicios. DDoSLa resiliencia se puede mejorar aún más mediante el uso de una AWS arquitectura con servicios específicos, que se describen en las siguientes secciones, y mediante la implementación de mejores prácticas adicionales para cada parte del flujo de red entre los usuarios y la aplicación.

Puede usar AWS servicios que funcionan desde ubicaciones periféricas, como Amazon CloudFront, AWS Global Accelerator y Amazon Route 53 para crear una protección de disponibilidad integral contra todos los ataques conocidos a la capa de infraestructura. Estos servicios forman parte de la red perimetral AWS global y pueden mejorar la DDoS resiliencia de su aplicación cuando atienden cualquier tipo de tráfico de aplicaciones desde ubicaciones periféricas distribuidas por todo el mundo. Puede ejecutar su aplicación en cualquier Región de AWS lugar y utilizar estos servicios para proteger su disponibilidad y optimizar su rendimiento para los usuarios finales legítimos.

Los beneficios de usar Amazon CloudFront, Global Accelerator y Amazon Route 53 incluyen:

- Acceso a Internet y capacidad de DDoS mitigación en toda la red AWS Global Edge. Esto resulta útil para mitigar los ataques volumétricos más grandes, que pueden alcanzar una escala de terabits.
- AWS Shield DDoSlos sistemas de mitigación están integrados con los servicios AWS perimetrales, lo que reduce la cantidad time-to-mitigate de minutos a menos de un segundo.
- Stateless SYN Flood Mitigation verifica las conexiones entrantes mediante SYN cookies antes de pasarlas al servicio protegido. Esto garantiza que solo las conexiones válidas lleguen a su aplicación y, al mismo tiempo, protege a sus usuarios finales legítimos contra las caídas de falsos positivos.
- Sistemas de ingeniería de tráfico automáticos que dispersan o aíslan el impacto de los grandes ataques volumétricosDDoS. Todos estos servicios aíslan los ataques en su origen antes de que lleguen a su origen, lo que se traduce en un menor impacto en los sistemas protegidos por estos servicios.
- La defensa de la capa de aplicación, CloudFront cuando se combina con AWS WAFeso, no requiere cambiar la arquitectura de la aplicación actual (por ejemplo, en un centro de datos local Región de AWS o en un centro de datos local).

La transferencia de datos entrantes es gratuita AWS y no se paga por el tráfico de DDoS ataque que se mitigue. AWS Shield El siguiente diagrama de arquitectura incluye los servicios de AWS Global Edge Network.




DDoS-arquitectura de referencia resiliente

Esta arquitectura incluye varios AWS servicios que pueden ayudarle a mejorar la resistencia de su aplicación web frente DDoS a los ataques. La siguiente tabla proporciona un resumen de estos servicios y las capacidades que pueden ofrecer. AWS ha etiquetado cada servicio con un indicador de mejores prácticas (BP1,BP2) para facilitar la consulta en este documento. Por ejemplo, en una próxima sección se analizarán las capacidades que ofrecen Amazon CloudFront y Global Accelerator, que incluye el indicador BP1 de mejores prácticas.

Tabla 2: Resumen de las mejores prácticas

| | AWS Edge | | | Región de AWS | | |
|---|---|---|---|---|---|---|
| | Uso de Amazon CloudFron | Uso de Global | Uso de Amazon | Uso de Elastic Load | Uso de grupos de seguridad | Uso de Amazon Elastic |

| | AWS Edge | | | Región de AWS | | |
|---|---|---|---|---|---|---|
| | t (BP1) con AWS WAF (BP2) | Accelerator () BP1 | Route 53 (BP3) | Balancing (BP6) con AWS WAF (BP2) | y redes ACLs en Amazon VPC (BP5) | Compute Cloud (AmazonEC2) Auto Scaling (BP7) |
| Mitigación de los ataques de capa 3 (por ejemplo, de UDP reflexión) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mitigación de ataques en la capa 4 (por ejemplo, SYN inundación) | ✓ | ✓ | ✓ | ✓ | | |
| Capa 6 (por ejemploTLS), mitigación de ataques | ✓ | ✓ | ✓ | ✓ | | |
| Reduzca la superficie de ataque | ✓ | ✓ | ✓ | ✓ | ✓ | |

| | AWS Edge | | | Región de AWS | | |
|---|---|---|---|---|---|---|
| Amplíe para absorber el tráfico de la capa de aplicación | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mitigación de ataques en la capa 7 (capa de aplicación) | ✓ | ✓(*) | ✓ | ✓ | ✓(*) | ✓(*) |
| Aislamiento geográfico y dispersión del exceso de tráfico y de DDoS los ataques de mayor envergadura | ✓ | ✓ | ✓ | | | |

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

Otra forma de mejorar su preparación para responder a los DDoS ataques y mitigarlos es suscribirse a. AWS Shield Advanced Los beneficios de su uso AWS Shield Advanced incluyen:

- Acceso al soporte especializado del equipo de AWS Shield respuesta las 24 horas del día, los 7 días de la semana AWS SRT, para ayudarlo a mitigar DDoS los ataques que afectan a la disponibilidad de las aplicaciones, incluida una función de participación proactiva opcional

- Umbrales de detección sensibles que redirigen el tráfico al sistema de DDoS mitigación antes y pueden mejorar time-to-mitigate los ataques contra Amazon EC2 (incluido el Elastic Load Balancer) o Network Load Balancer, cuando se utilizan con una dirección IP elástica
- Detección de nivel 7 personalizada basada en los patrones de tráfico de referencia de su aplicación cuando se utiliza con AWS WAF
- DDoSMitigación automática de la capa de aplicación, en la que Shield Advanced responde a DDoS los ataques detectados mediante la creación, la evaluación y el despliegue de AWS WAF reglas personalizadas
- Acceso sin AWS WAF coste adicional para mitigar los DDoS ataques a la capa de aplicaciones (cuando se utiliza con Amazon CloudFront o Application Load Balancer)
- Gestión centralizada de las políticas de seguridad sin AWS Firewall Managercoste adicional.
- Protección de costes que le permite solicitar un reembolso limitado de los costes relacionados con el escalamiento que se deriven de un DDoS ataque.
- Acuerdo de nivel de servicio mejorado específico para los AWS Shield Advanced clientes.
- Grupos de protección que le permiten agrupar los recursos, lo que proporciona una forma de autoservicio de personalizar el alcance de la detección y la mitigación de su aplicación al tratar varios recursos como una sola unidad. Para obtener información sobre los grupos de protección, consulte los grupos de protección Shield Advanced.
- DDoSatacar la visibilidad mediante el AWS Management Consoleuso de las CloudWatch métricas y alarmas de Amazon y Amazon. API

Este servicio de DDoS mitigación opcional ayuda a proteger las aplicaciones alojadas en cualquier sitio Región de AWS. El servicio está disponible en todo el mundo para CloudFront Route 53 y Global Accelerator. A nivel regional, puede proteger las direcciones IP de Application Load Balancer, Classic Load Balancer y Elastic, lo que le permite proteger las instancias de Network Load Balancer () o AmazonNLBs. EC2

Para obtener una lista completa de las AWS Shield Advanced funciones y obtener más información al respecto AWS Shield, consulta Cómo funciona. AWS Shield

## Mejores prácticas de DDoS mitigación

En las siguientes secciones, se describe con más detalle cada una de las mejores prácticas recomendadas para la DDoS mitigación. Para obtener una easy-to-implement guía rápida sobre cómo crear una capa de DDoS mitigación para aplicaciones web estáticas o dinámicas, consulte

Cómo ayudar a proteger las aplicaciones web dinámicas contra DDoS los ataques mediante Amazon CloudFront y Amazon Route 53.

## Defensa de la capa de infraestructura (BP1BP3,BP6,,BP7)

En un entorno de centro de datos tradicional, puede mitigar DDoS los ataques a la capa de infraestructura mediante técnicas como el sobreaprovisionamiento de capacidad, la implementación de sistemas de DDoS mitigación o la eliminación del tráfico con la ayuda de servicios de mitigación. DDoS Sí AWS, las capacidades de DDoS mitigación se proporcionan automáticamente, pero puede optimizar la DDoS resiliencia de su aplicación si elige la arquitectura que mejor aproveche esas capacidades y, además, le permita adaptarse al exceso de tráfico.

Las consideraciones clave para ayudar a mitigar DDoS los ataques volumétricos incluyen garantizar que haya suficiente capacidad y diversidad de tránsito disponibles y proteger AWS los recursos, como las EC2 instancias de Amazon, contra el tráfico de ataques.

Algunos tipos de EC2 instancias de Amazon admiten funciones que pueden gestionar con mayor facilidad grandes volúmenes de tráfico, por ejemplo, interfaces de ancho de banda de red de hasta 100 Gbps y redes mejoradas. Esto ayuda a evitar la congestión de la interfaz por el tráfico que ha llegado a la EC2 instancia de Amazon. Las instancias que admiten redes mejoradas ofrecen un mayor rendimiento de entrada/salida (E/S), un mayor ancho de banda y una menor CPU utilización en comparación con las implementaciones tradicionales. Esto mejora la capacidad de la instancia para gestionar grandes volúmenes de tráfico y, en última instancia, hace que sea muy resistente a la carga de paquetes por segundo (pps).

Para permitir este alto nivel de resiliencia, se AWS recomienda utilizar instancias EC2 dedicadas de Amazon o instancias de Amazon EC2 con un mayor rendimiento de red que tengan un sufijo `N` «» y que admitan redes mejoradas con un ancho de banda de red de hasta 100 Gbps, por ejemplo, `c6gn.16xlarge` `c5n.18xlarge` o instancias metálicas (como). `c5n.metal`

Para obtener más información sobre EC2 las instancias de Amazon que admiten interfaces de red de 100 Gigabit y redes mejoradas, consulte Tipos de EC2 instancias de Amazon.

El módulo necesario para mejorar las redes y el conjunto de `enaSupport` atributos necesarios se incluyen en Amazon Linux 2 y en las versiones más recientes de Amazon LinuxAMI. Por lo tanto, si lanza una instancia con una versión de máquina virtual (HVM) de hardware de Amazon Linux en un tipo de instancia compatible, la red mejorada ya está habilitada para su instancia. Para obtener más información, consulte Comprobar si las redes mejoradas están habilitadas y Redes mejoradas en Linux.

## Amazon EC2 con Auto Scaling (BP7)

Otra forma de mitigar los ataques tanto a la infraestructura como a la capa de aplicaciones es operar a escala. Si tienes aplicaciones web, puedes usar balanceadores de carga para distribuir el tráfico a varias EC2 instancias de Amazon que estén sobreaprovisionadas o configuradas para escalarse automáticamente. Estas instancias pueden gestionar picos de tráfico repentinos que se produzcan por cualquier motivo, como una aglomeración repentina o un ataque a la capa de aplicación. DDoS Puedes configurar CloudWatch las alarmas de Amazon para que inicien Auto Scaling para escalar automáticamente el tamaño de tu EC2 flota de Amazon en respuesta a los eventos que definas CPURAM, como las E/S de la red e incluso las métricas personalizadas.

Este enfoque protege la disponibilidad de las aplicaciones cuando se produce un aumento inesperado en el volumen de solicitudes. Si utilizas Amazon CloudFront, Application Load Balancer, Classic Load Balancers o Network Load Balancer con tu aplicaciónTLS, la negociación la gestiona la distribución ( CloudFrontAmazon) o el balanceador de cargas. Estas funciones ayudan a proteger sus instancias del impacto de los ataques TLS basados en bases, ya que se adaptan a las solicitudes legítimas y a los ataques abusivos. TLS

Para obtener más información sobre el uso de Amazon CloudWatch para invocar Auto Scaling, consulte Supervisión de CloudWatch las métricas de Amazon para sus grupos e instancias de Auto Scaling.

Amazon EC2 proporciona una capacidad de cómputo redimensionable para que puedas ampliarla o reducirla rápidamente a medida que cambien los requisitos. Puede escalar horizontalmente agregando instancias automáticamente a su aplicación escalando el tamaño de su grupo de Amazon EC2 Auto Scaling, y puede escalar verticalmente usando tipos de EC2 instancias más grandes.

Con Amazon RDS Proxy, puede permitir que sus aplicaciones agrupen y compartan conexiones de bases de datos para mejorar su capacidad de escalar y gestionar los picos impredecibles del tráfico de bases de datos. También puedes habilitar el autoscalamiento del almacenamiento para una instancia de RDS base de datos de Amazon. Consulte Administrar la capacidad automáticamente con el escalado automático del RDS almacenamiento de Amazon para obtener más información.

## Elastic Load Balancing (BP6)

DDoSLos ataques de gran tamaño pueden sobrepasar la capacidad de una sola EC2 instancia de Amazon. Con Elastic Load Balancing (ELB), puede reducir el riesgo de sobrecargar la aplicación distribuyendo el tráfico entre muchas instancias de backend. Elastic Load Balancing se puede escalar automáticamente, lo que le permite gestionar volúmenes más grandes cuando hay tráfico

adicional imprevisto, por ejemplo, debido a aglomeraciones repentinas o DDoS ataques. En el caso de las aplicaciones creadas dentro de AmazonVPC, hay tres tipos ELBs a tener en cuenta, según el tipo de aplicación: Application Load Balancer (ALB), Network Load Balancer NLB () y Classic Load Balancer (). CLB

En el caso de las aplicaciones web, puede usar Application Load Balancer para enrutar el tráfico en función del contenido y aceptar únicamente solicitudes web bien estructuradas. Application Load Balancer bloquea muchos de DDoS los ataques más comunes, como SYN las inundaciones o los ataques de UDP reflexión, y protege la aplicación de dichos ataques. Application Load Balancer escala automáticamente para absorber el tráfico adicional cuando se detectan estos tipos de ataques. El escalamiento de las actividades debido a los ataques a la capa de infraestructura es transparente para AWS los clientes y no afecta a su factura.

Para obtener más información sobre cómo proteger las aplicaciones web con Application Load Balancer, consulte Introducción a Application Load Balancers.

Para HTTPS aplicaciones HTTP ajenas a/, puede usar Network Load Balancer para enrutar el tráfico a los destinos (por ejemplo, EC2 instancias de Amazon) con una latencia ultrabaja. Una consideración clave con Network Load Balancer es que todo el UDP tráfico que llegue al TCP SYN balanceador de cargas en un listener válido se enrutará a sus objetivos, no se absorberá; sin embargo, esto no se aplica a los TLS -listeners que finalizan la conexión. TCP En el caso de los balanceadores de carga de red con dispositivos de TCP escucha, recomendamos implementar Global Accelerator para protegerse de las inundaciones. SYN

Puede usar Shield Advanced para configurar la DDoS protección de las direcciones IP elásticas. Cuando se asigna una dirección IP elástica por zona de disponibilidad al Network Load Balancer, Shield Advanced aplicará DDoS las protecciones pertinentes al tráfico del Network Load Balancer.

Para obtener más información sobre la protección de TCP las UDP aplicaciones con Network Load Balancer, consulte Introducción a Network Load Balancers.

> **Note**
>
> Según la configuración del grupo de seguridad, es necesario que el recurso que utilice la seguridad para agrupar utilice el seguimiento de conexiones para rastrear la información sobre el tráfico, lo que puede afectar a la capacidad del equilibrador de cargas para procesar nuevas conexiones, ya que el número de conexiones rastreadas es limitado.
> Una configuración de grupo de seguridad que contiene una regla de entrada que acepta tráfico desde cualquier dirección IP (por ejemplo, `0.0.0.0/0` o `::/0`) pero no tiene una regla

correspondiente que permita el tráfico de respuesta, hace que el grupo de seguridad utilice la información de seguimiento de conexiones para permitir el envío del tráfico de respuesta. En caso de DDoS ataque, se puede agotar el número máximo de conexiones rastreadas. Para mejorar la DDoS resiliencia de su Application Load Balancer o Classic Load Balancer de acceso público, asegúrese de que el grupo de seguridad asociado a su balanceador de cargas esté configurado para no utilizar el seguimiento de conexiones (conexiones sin seguimiento), de modo que el flujo de tráfico no esté sujeto a los límites de seguimiento de conexiones.

Para ello, configure su grupo de seguridad con una regla que permita que la regla de entrada acepte TCP flujos desde cualquier dirección IP (`0.0.0.0/0`o`::/0`) y agregue la regla correspondiente en la dirección de salida que permita a este recurso enviar el tráfico de respuesta (permitir el rango de salida para cualquier dirección IP `0.0.0.0/0` o`::/0`) para todos los puertos (0-65535), de modo que el tráfico de respuesta se permita en función de la regla del grupo de seguridad y no de la información de seguimiento. Con esta configuración, Classic y Application Load Balancer no están sujetos a agotar los límites de seguimiento de conexiones que puedan afectar al establecimiento de nuevas conexiones con sus nodos de balanceador de carga, y le permiten escalar en función del aumento del tráfico en caso de un ataque. DDoS Puede encontrar más información sobre las conexiones no rastreadas en: Seguimiento de conexiones de grupos de seguridad: conexiones no rastreadas.

Evitar el seguimiento de las conexiones de los grupos de seguridad solo ayuda en los casos en que el DDoS tráfico se origina en una fuente permitida por el grupo de seguridad; el DDoS tráfico de fuentes que no están permitidas en el grupo de seguridad no afecta al seguimiento de las conexiones. En estos casos, no es necesario volver a configurar los grupos de seguridad para evitar el seguimiento de las conexiones, por ejemplo, si la lista de grupos de seguridad permitidos consta de rangos de IP en los que se tiene un alto grado de confianza, como el firewall corporativo de una empresa o una VPN salida IPs de confianza o. CDNs

## Utilice las ubicaciones de AWS Edge para escalar (BP1,) BP3

El acceso a conexiones de Internet diversas y de gran escala puede aumentar considerablemente su capacidad de optimizar la latencia y el rendimiento para los usuarios, absorber los DDoS ataques y aislar los fallos, al tiempo que minimiza el impacto en la disponibilidad de la aplicación. AWS las ubicaciones de borde proporcionan una capa adicional de infraestructura de red que proporciona estas ventajas a cualquier aplicación web que utilice Amazon CloudFront, Global Accelerator y

Amazon Route 53. Con estos servicios, puede proteger de forma integral las aplicaciones periféricas desde las que se ejecutan. Regiones de AWS

## Entrega de aplicaciones web en la periferia () BP1

Amazon CloudFront es un servicio que se puede utilizar para ofrecer todo tu sitio web, incluido contenido estático, dinámico, de streaming e interactivo. Las conexiones persistentes y la configuración variable time-to-live (TTL) se pueden usar para reducir el tráfico de tu sitio de origen, incluso si no publicas contenido que se pueda almacenar en caché. El uso de estas CloudFront funciones reduce el número de solicitudes y TCP conexiones que vuelven a su origen, lo que ayuda a proteger su aplicación web de las inundaciones. HTTP

CloudFront solo acepta conexiones bien formadas, lo que ayuda a evitar que muchos DDoS ataques comunes, como SYN las inundaciones y los ataques de UDP reflexión, lleguen a su origen. DDoSLos ataques también están aislados geográficamente cerca de la fuente, lo que evita que el tráfico afecte a otras ubicaciones. Estas funciones pueden mejorar considerablemente su capacidad de seguir proporcionando tráfico a los usuarios durante los ataques de gran DDoS envergadura. Se puede utilizar CloudFront para proteger un origen en Internet AWS o en cualquier otro lugar.

Si utilizas Amazon Simple Storage Service (Amazon S3) para publicar contenido estático en Internet, te AWS recomienda que utilices Amazon CloudFront para proteger tu depósito, ya que ofrece las siguientes ventajas:

- Restringe el acceso al bucket de Amazon S3 para que no sea de acceso público.
- Garantiza que los espectadores (usuarios) solo puedan acceder al contenido del bucket a través de la CloudFront distribución especificada, es decir, evita que accedan al contenido directamente desde el bucket o a través de una distribución no deseada. CloudFront

Para lograrlo, CloudFront configúrelo para enviar solicitudes autenticadas a Amazon S3 y configure Amazon S3 para que solo permita el acceso a las solicitudes autenticadas desde. CloudFront CloudFront proporciona dos formas de enviar solicitudes autenticadas a un origen de Amazon S3: control de acceso de origen (OAC) e identidad de acceso de origen (OAI). Recomendamos su uso OAC porque es compatible con:

- Todos los buckets de Amazon S3 en total Regiones de AWS, incluidas las regiones opcionales lanzadas después de diciembre de 2022
- Cifrado del lado del servidor de Amazon S3 con AWS KMS (SSE-) KMS
- Solicitudes dinámicas (`PUT` y `DELETE`) en Amazon S3

Para obtener más información OAC yOAI, consulte Restringir el acceso al origen de Amazon S3.

Para obtener más información sobre cómo proteger y optimizar el rendimiento de las aplicaciones web con Amazon CloudFront, consulta Cómo empezar con Amazon CloudFront.

## Proteja el tráfico de red más alejado de su origen con AWS Global Accelerator () BP1

Global Accelerator es un servicio de red que mejora la disponibilidad y el rendimiento del tráfico de los usuarios hasta en un 60%. Esto se logra ingresando el tráfico en la ubicación perimetral más cercana a los usuarios y enrutándolo a través de la infraestructura de red AWS global hasta su aplicación, ya sea que se ejecute de forma única o múltiple. Regiones de AWS

Global Accelerator enruta TCP y el UDP tráfico hacia el punto final óptimo en función del rendimiento en el punto más cercano Región de AWS al usuario. Si se produce un error en la aplicación, Global Accelerator proporciona una conmutación por error al siguiente mejor punto final en 30 segundos. Global Accelerator utiliza la amplia capacidad de la red AWS global y las integraciones con Shield, como una capacidad de SYN proxy sin estado que desafía los nuevos intentos de conexión y solo sirve a los usuarios finales legítimos, para proteger las aplicaciones.

Puede implementar una arquitectura DDoS flexible que ofrezca muchas de las mismas ventajas que las prácticas recomendadas de entrega de aplicaciones web en la periferia, incluso si su aplicación utiliza protocolos no compatibles CloudFront o si utiliza una aplicación web que requiere direcciones IP estáticas globales.

Por ejemplo, es posible que necesite direcciones IP que los usuarios finales puedan añadir a la lista de direcciones IP permitidas en sus firewalls y que ningún otro AWS cliente pueda utilizar. En estos escenarios, puede usar Global Accelerator para proteger las aplicaciones web que se ejecutan en Application Load Balancer y, además, para detectar y mitigar las inundaciones de solicitudes de la capa de aplicaciones web. AWS WAF

Para obtener más información sobre cómo proteger y optimizar el rendimiento del tráfico de red mediante Global Accelerator, consulte Introducción a Global Accelerator.

## Resolución de nombres de dominio en el borde () BP3

Temas

- Uso de Route 53 para determinar la DNS disponibilidad
- Configuración de Route 53 para protegerse de los costes frente a NXDOMAIN los ataques

## Uso de Route 53 para determinar la DNS disponibilidad

Amazon Route 53 es un servicio de sistema de nombres de dominio (DNS) escalable y de alta disponibilidad que se puede utilizar para dirigir el tráfico a su aplicación web. Incluye funciones avanzadas como Traffic Flow, Health Checks and Monitoring, Latency-Based Routing y Geo. DNS Estas funciones avanzadas le permiten controlar la forma en que el servicio responde a DNS las solicitudes para mejorar el rendimiento de su aplicación web y evitar interrupciones en el sitio. Es el único AWS servicio que tiene una disponibilidad SLA del plano de datos del 100%.

Amazon Route 53 utiliza técnicas como la fragmentación aleatoria y la segmentación anycast, que pueden ayudar a los usuarios a acceder a su aplicación incluso si el DNS servicio es blanco de un ataque. DDoS

Con la fragmentación aleatoria, cada servidor de nombres de su conjunto de delegación corresponde a un conjunto único de ubicaciones de borde y rutas de Internet. Esto proporciona una mayor tolerancia a los errores y minimiza la superposición entre los clientes. Si un servidor de nombres del conjunto de delegación no está disponible, los usuarios pueden volver a intentarlo y recibir una respuesta de otro servidor de nombres en una ubicación perimetral diferente.

La segmentación de Anycast permite atender cada DNS solicitud en la ubicación más óptima, lo que dispersa la carga de la red y reduce la latencia. DNS Esto proporciona una respuesta más rápida a los usuarios. Además, Amazon Route 53 puede detectar anomalías en el origen y el volumen de DNS las consultas y priorizar las solicitudes de los usuarios que se sabe que son confiables.

Para obtener más información sobre el uso de Amazon Route 53 para dirigir a los usuarios a su aplicación, consulte Introducción a Amazon Route 53.

## Configuración de Route 53 para protegerse de los costes frente a **`NXDOMAIN`** los ataques

`NXDOMAIN`los ataques se producen cuando los atacantes envían una avalancha de solicitudes a una zona alojada para subdominios inexistentes, a menudo a través de solucionadores conocidos como «buenos». El objetivo de estos ataques puede ser afectar a la memoria caché del solucionador recursivo o a la disponibilidad del solucionador autorizado, o pueden ser una forma de DNS reconocimiento para intentar descubrir los registros de la zona alojada. El uso de Route 53 como solucionador autorizado mitiga el riesgo de que se vea afectado la disponibilidad y el rendimiento; sin embargo, el resultado puede ser un aumento significativo de los costos mensuales de Route 53. Para protegerse de los aumentos de costos, aproveche los precios de Route 53, en los que DNS las consultas son gratuitas cuando se cumplen las siguientes condiciones:

- El nombre de dominio o subdominio (`example.comostore.example.com`) y el tipo de registro (`A`) de la consulta coinciden con un registro de alias.
- El destino del alias es un AWS recurso que no es otro registro de Route 53.

Cree un registro comodín, por ejemplo, `*.example.com` con un tipo `A` (Alias) que apunte a un AWS recurso, como una EC2 instancia, Elastic Load Balancer CloudFront o una distribución, de modo que cuando se realice una consulta`qwerty12345.example.com`, se devuelva la IP del recurso y no se le cobre por la consulta.

# Defensa de la capa de aplicación (BP1,) BP2

Muchas de las técnicas analizadas hasta ahora en este paper son eficaces para mitigar el impacto que los DDoS ataques a la capa de infraestructura tienen en la disponibilidad de la aplicación. Para defenderse también de los ataques en la capa de aplicación, debe implementar una arquitectura que le permita detectar, escalar para absorber y bloquear específicamente las solicitudes maliciosas. Esta es una consideración importante porque los sistemas de DDoS mitigación basados en la red suelen ser ineficaces a la hora de mitigar los ataques complejos a la capa de aplicaciones.

## Detecte y filtre las solicitudes web maliciosas (BP1,) BP2

Cuando su aplicación se ejecute AWS, podrá aprovechar Amazon CloudFront (y su capacidad de almacenamiento en HTTP caché) y la protección automática de la capa de aplicaciones Shield Advanced para evitar que las solicitudes innecesarias lleguen a su origen durante DDoS los ataques a la capa de aplicaciones. AWS WAF

### Amazon CloudFront

Amazon CloudFront puede ayudar a reducir la carga del servidor impidiendo que el tráfico no web llegue a tu origen. Para enviar una solicitud a una CloudFront aplicación, la conexión debe establecerse con una dirección IP válida mediante un TCP apretón de manos completo, que no se puede falsificar. Además, CloudFront puede cerrar automáticamente las conexiones causadas por atacantes que leen o escriben con lentitud (por ejemplo, Slowloris).

Almacenamiento en caché de CDN

CloudFront permite ofrecer tanto contenido dinámico como contenido estático desde ubicaciones AWS periféricas. Al servir contenido almacenado en caché mediante proxy desde la CDN memoria

caché, evita que las solicitudes lleguen a su origen desde un nodo de caché perimetral determinado mientras dure el almacenamiento en caché. TTL Además de reducir las solicitudes por contenido caducado pero que se puede almacenar en caché, incluso si son muy cortasTTL, un número insignificante de solicitudes llegará a tu origen durante una avalancha de solicitudes relacionadas con ese contenido. Además, habilitar funciones como CloudFront Origin Shield puede ayudar a reducir aún más la carga en tu Origin: cualquier cosa que puedas hacer para mejorar la ratio de aciertos de la caché puede marcar la diferencia entre un ataque de inundación de solicitudes impactante y no impactante.

## AWS WAF

Si lo utilizas AWS WAF, puedes configurar listas de control de acceso web (webACLs) en tus CloudFront distribuciones globales o recursos regionales para filtrar, supervisar y bloquear las solicitudes en función de sus firmas. Para determinar si se deben permitir o bloquear las solicitudes, se pueden tener en cuenta factores como la dirección IP o el país de origen, determinadas cadenas o patrones de la solicitud, el tamaño de partes específicas de la solicitud y la presencia de SQL códigos o secuencias de comandos malintencionados. También puede CAPTCHA resolver acertijos y resolver silenciosamente las sesiones de los clientes en función de las solicitudes.

Ambas AWS WAF opciones CloudFront también te permiten establecer restricciones geográficas para bloquear o permitir solicitudes de países seleccionados. Esto puede ayudar a bloquear o limitar la velocidad de los ataques desde ubicaciones geográficas en las que no se espera que sirvan a los usuarios. Con las detalladas reglas de coincidencia geográfica AWS WAF, puede controlar el acceso hasta el nivel de la región.

Puedes usar declaraciones de alcance reducido para limitar el alcance de las solicitudes que evalúa la regla para ahorrar costos y «etiquetas» en las solicitudes web para permitir que una regla que coincida con la solicitud comunique los resultados de las coincidencias a las reglas que se evalúan más adelante en la misma web. ACL Elija esta opción para reutilizar la misma lógica en varias reglas.

También puede definir una respuesta personalizada completa, con código de respuesta, encabezados y cuerpo.

Para ayudar a identificar las solicitudes maliciosas, revise los registros del servidor web o utilice AWS WAF los registros y solicite un muestreo. Al habilitar el AWS WAF registro, obtendrá información detallada sobre el tráfico que analiza la Web. ACL AWS WAF admite el filtrado de registros, lo que le permite especificar qué solicitudes web se registran y qué solicitudes se descartan del registro tras la inspección.

La información registrada en los registros incluye la hora en que se AWS WAF recibió la solicitud de su AWS recurso, información detallada sobre la solicitud y la acción coincidente para cada regla solicitada.

Las solicitudes incluidas en los ejemplos proporcionan detalles sobre las solicitudes de las últimas tres horas que se ajustaron a una de tus AWS WAF reglas. Puedes usar esta información para identificar señales de tráfico potencialmente maliciosas y crear una nueva regla para denegar esas solicitudes. Si ve varias solicitudes con una cadena de consulta aleatoria, asegúrese de permitir solo los parámetros de la cadena de consulta que sean relevantes para almacenar en la memoria caché de su aplicación. Esta técnica es útil para mitigar un ataque de robo de caché contra tu origen.

AWS WAF — Reglas basadas en tarifas

AWS recomienda encarecidamente protegerse contra la HTTP avalancha de solicitudes mediante el uso de reglas basadas en tarifas AWS WAF para bloquear automáticamente las direcciones IP de los delincuentes cuando el número de solicitudes recibidas en un período deslizante de 5 minutos supere el umbral que usted defina. Las direcciones IP de los clientes infractoras recibirán una respuesta prohibida de 403 puntos (o una respuesta de error de bloqueo configurada) y permanecerán bloqueadas hasta que el porcentaje de solicitudes caiga por debajo del umbral.

Se recomienda establecer capas de reglas basadas en tasas para ofrecer una protección mejorada, de forma que pueda:

- Una regla general basada en tarifas para proteger su aplicación de grandes HTTP inundaciones.
- Una o más reglas basadas en tarifas para proteger a personas específicas URIs a tarifas más restrictivas que la regla general basada en tarifas.

Por ejemplo, puede elegir una regla general basada en una tarifa (sin una declaración de alcance) con un límite de 500 solicitudes en un período de 5 minutos y, a continuación, crear una o más de las siguientes reglas basadas en tarifas con límites inferiores a 500 (tan solo 100 solicitudes en un período de 5 minutos) utilizando declaraciones de alcance reducido:

- Proteja sus páginas web con una declaración de alcance reducido, como «`if NOT uri_path contains '.'`», para proteger aún más las solicitudes de recursos sin una extensión de archivo. Esto también protege tu página de inicio (`/`), que es una ruta a la que se dirige con frecuencia. URI
- Proteja los puntos finales dinámicos con una declaración de alcance reducido, como "» `if method exactly matches 'post' (convert lowercase)`

- Proteja las solicitudes pesadas que llegan a su base de datos o invoque una contraseña de un solo uso (OTP) con un alcance reducido como "» `if uri_path starts_with '/login' OR uri_path starts_with '/signup' OR uri_path starts_with '/forgotpassword'`

Las tarifas basadas en el modo «Bloquear» son la piedra angular de la defense-in-depth WAF configuración para protegerse contra la avalancha de solicitudes y son un requisito para poder aprobar las solicitudes de protección de AWS Shield Advanced costes. Examinaremos las defense-in-depth WAF configuraciones adicionales en las siguientes secciones.

AWS WAF — Reputación IP

Para evitar ataques basados en la reputación de la dirección IP, puede crear reglas mediante la coincidencia de IP o utilizar reglas administradas para ello AWS WAF.

El grupo de reglas de la lista de reputación IP de Amazon incluye reglas basadas en la inteligencia de amenazas interna de Amazon. Estas reglas buscan direcciones IP que son bots, que realizan reconocimientos de AWS recursos o que participan activamente en DDoS actividades. Se ha observado que esta `AWSManagedIPDDoSList` regla bloquea más del 90% de las oleadas de solicitudes maliciosas.

El grupo de reglas de la lista de direcciones IP anónimas contiene reglas para bloquear las solicitudes de los servicios que permiten ocultar la identidad del espectador. Estas incluyen solicitudes desde proxiesVPNs, nodos Tor y plataformas en la nube (excluidas). AWS

Además, puedes utilizar listas de reputación de IP de terceros mediante el componente analizador de listas de IP de la solución Security Automations for. AWS WAF

AWS WAF - Mitigación inteligente de amenazas

Las botnets son una grave amenaza para la seguridad y se suelen utilizar para llevar a cabo actividades ilegales o dañinas, como enviar spam, robar datos confidenciales, iniciar ataques de ransomware, cometer fraudes publicitarios mediante clics fraudulentos o lanzar ataques distribuidos denial-of-service (DDoS). Para evitar los ataques de bots, usa el grupo de reglas gestionado por AWS WAF Bot Control. Este grupo de reglas proporciona un nivel de protección básico, «común», que añade etiquetas a los bots que se identifican a sí mismos, verifica los bots más habituales y detecta las firmas de bots más fiables, y un nivel de protección «segmentado» que añade la detección de los bots avanzados que no se identifican a sí mismos.

Las protecciones específicas utilizan técnicas de detección avanzadas, como la interrogación del navegador, la toma de huellas digitales y la heurística del comportamiento, para identificar el

tráfico de bots inadecuados y, a continuación, aplican controles de mitigación, como la limitación de velocidad y las reglas de impugnación. CAPTCHA Targeted también ofrece opciones de limitación de velocidad para hacer cumplir patrones de acceso similares a los humanos y aplicar una limitación de velocidad dinámica mediante el uso de tokens de solicitud. Para obtener más información, consulta el grupo de reglas de control de AWS WAF bots. Para detectar y gestionar los intentos de apropiación maliciosos en la página de inicio de sesión de tu aplicación, puedes usar el grupo de reglas de prevención de apropiación de cuentas (ATP) de AWS WAF Fraud Control. Para ello, el grupo de reglas inspecciona los intentos de inicio de sesión que los clientes envían al punto final de inicio de sesión de la aplicación y también inspecciona las respuestas de la aplicación a los intentos de inicio de sesión para hacer un seguimiento de la tasa de aciertos y fracasos.

El fraude en la creación de cuentas es una actividad ilegal en línea en la que un atacante intenta crear una o más cuentas falsas. Los atacantes utilizan cuentas falsas para realizar actividades fraudulentas, como abusar de las bonificaciones promocionales y de registro, hacerse pasar por alguien y los ciberataques, como la suplantación de identidad. La presencia de cuentas falsas puede afectar negativamente a su empresa, ya que perjudica su reputación ante los clientes y la expone al fraude financiero.

Puedes supervisar y controlar los intentos de fraude en la creación de cuentas mediante la implementación de la función Control de AWS WAF Fraude y Prevención del Fraude en la creación de cuentas (ACFP). AWS WAF ofrece esta función en el grupo de Reglas administradas de AWS reglas `AWS ManagedRulesACFPRuleSet` con la integración de aplicaciones complementariasSDKs.

Obtenga más información sobre estas protecciones en la mitigación AWS WAF inteligente de amenazas.

## Mitigue automáticamente los DDoS eventos de la capa de aplicación (BP1,,BP2) BP6

Si está suscrito AWS Shield Advanced, puede activar la DDoSmitigación automática de la capa de aplicación Shield Advanced. Esta función crea, evalúa e implementa automáticamente AWS WAF reglas para mitigar los DDoS eventos de la capa 7 en su nombre.

AWS Shield Advanced establece una línea base de tráfico para cada recurso protegido asociado a una WAF Web. ACL El tráfico que se desvía significativamente de la línea base establecida se marca como un evento potencialDDoS. Tras detectar un evento, AWS Shield Advanced intenta identificar una firma de las solicitudes web que constituyen el evento y, si se identifica una firma, se crean AWS WAF reglas para mitigar el tráfico con esa firma.

Una vez que las reglas se evalúan con respecto a la línea base histórica y se consideran seguras, se agregan al grupo de reglas administrado por Shield y puede elegir si las reglas se implementan en modo de recuento o de bloque. Shield Advanced elimina automáticamente AWS WAF las reglas cuando determina que un evento ha desaparecido por completo.

## Engage SRT (solo para suscriptores de Shield Advanced)

Además, al suscribirse a Shield Advanced, puede utilizar el AWS SRT para que le ayude a crear reglas que mitiguen un ataque que perjudique la disponibilidad de su aplicación. Puede conceder acceso AWS SRT limitado a su cuenta AWS Shield Advanced y AWS WAF APIs. AWS SRTaccede APIs a ellos para aplicar mitigaciones a tu cuenta solo con tu autorización explícita. Para obtener más información, consulte la Soporte sección de este documento.

Se puede utilizar AWS Firewall Manager para configurar y gestionar de forma centralizada las reglas de seguridad, como AWS Shield Advanced las protecciones y AWS WAF las reglas, en toda la organización. Su cuenta AWS Organizations de administración puede designar una cuenta de administrador, que está autorizada a crear políticas de Firewall Manager. Estas políticas le permiten definir criterios, como el tipo de recurso y las etiquetas, que determinan dónde se aplican las reglas. Esto resulta útil cuando tiene varias cuentas y desea estandarizar la protección.

Para obtener más información acerca de:

- Reglas administradas de AWS para AWS WAF, consulte Reglas administradas de AWS para AWS WAF.
- Si utiliza la restricción geográfica para limitar el acceso a su CloudFront distribución, consulte Restringir la distribución geográfica de su contenido.
- Si utiliza AWS WAF, consulte:
  - Cómo empezar con AWS WAF
  - Registrar la información ACL del tráfico web
  - Visualización de una muestra de solicitudes web
- Para configurar reglas basadas en tarifas, consulte Proteja los sitios y servicios web mediante reglas basadas en tarifas para. AWS WAF
- Para gestionar el despliegue de reglas en sus AWS recursos con Firewall Manager, consulte:
  - Introducción a las AWS WAF políticas de Firewall Manager.
  - Introducción a las políticas avanzadas de Firewall Manager Shield.

# Reducción de la superficie de ataque

Otra consideración importante a la hora de diseñar una AWS solución es limitar las oportunidades que tiene un atacante de atacar su aplicación. Este concepto se conoce como reducción de la superficie de ataque. Los recursos que no están expuestos a Internet son más difíciles de atacar, lo que limita las opciones de las que dispone un atacante para atacar la disponibilidad de la aplicación.

Por ejemplo, si no espera que los usuarios interactúen directamente con determinados recursos, asegúrese de que no se pueda acceder a esos recursos desde Internet. Del mismo modo, no aceptes tráfico de usuarios o aplicaciones externas en puertos o protocolos que no sean necesarios para la comunicación.

En la siguiente sección, AWS se describen las prácticas recomendadas que le servirán de guía para reducir la superficie de ataque y limitar la exposición de su aplicación a Internet.

# AWS Recursos ofuscados (,,) BP1 BP4 BP5

Por lo general, los usuarios pueden utilizar una aplicación de forma rápida y sencilla sin necesidad de que AWS los recursos estén completamente expuestos a Internet.

## Grupos de seguridad y red ACLs (BP5)

Amazon Virtual Private Cloud (AmazonVPC) le permite aprovisionar una sección aislada de forma lógica desde la Nube de AWS que puede lanzar AWS los recursos en una red virtual que usted defina.

Los grupos de seguridad y la red ACLs son similares en el sentido de que le permiten controlar el acceso a AWS los recursos de su VPC red. Sin embargo, los grupos de seguridad le permiten controlar el tráfico entrante y saliente a nivel de instancia, mientras que la red ACLs ofrece capacidades similares a nivel de VPC subred. El uso de grupos de seguridad o redes no conlleva ningún cargo adicional. ACLs

Puede elegir si desea especificar los grupos de seguridad al lanzar una instancia o asociar la instancia a un grupo de seguridad más adelante. Se deniega implícitamente todo el tráfico de Internet a un grupo de seguridad, a menos que cree una regla de autorización para permitir el tráfico.

Por ejemplo, si tienes EC2 instancias de Amazon detrás de un Elastic Load Balancer, las instancias en sí mismas no deberían ser de acceso público y solo deberían ser privadasIPs. En su lugar,

puede proporcionar al Elastic Load Balancer acceso a los puertos de escucha de destino necesarios mediante una regla de grupo de seguridad que permita el acceso a 0.0.0.0/0 (para evitar problemas de seguimiento de conexiones, consulte la nota siguiente) junto con una lista de control de acceso a la red (NACL) en la subred del grupo de destino para permitir que solo los rangos de IP de Elastic Load Balancing se comuniquen con las instancias. Esto garantiza que el tráfico de Internet no pueda comunicarse directamente con tus EC2 instancias de Amazon, lo que dificulta que un atacante conozca tu aplicación e impacte en ella.

Al crear una redACLs, puede especificar tanto las reglas de autorización como las de denegación. Esto resulta útil si quiere denegar de forma explícita ciertos tipos de tráfico a su aplicación. Por ejemplo, puede definir direcciones IP (como CIDR rangos), protocolos y puertos de destino a los que se deniega el acceso a toda la subred. Si la aplicación se usa solo para TCP el tráfico, puede crear una regla para denegar todo UDP el tráfico o viceversa. Esta opción resulta útil a la hora de responder a DDoS los ataques porque te permite crear tus propias reglas para mitigar el ataque cuando conoces el origen IPs u otra firma.

Si está suscrito AWS Shield Advanced, puede registrar las direcciones IP elásticas como recursos protegidos. DDoSlos ataques contra las direcciones IP de Elastic que se han registrado como recursos protegidos se detectan más rápidamente, lo que puede reducir el tiempo de mitigación. Cuando se detecta un ataque, los sistemas de DDoS mitigación leen la red ACL que corresponde a la dirección IP de Elastic objetivo y la utilizan en el borde de la AWS red, en lugar de hacerlo a nivel de subred. Esto reduce considerablemente el riesgo de que se vean afectados por varios ataques a la capa DDoS de infraestructura.

Para obtener más información sobre cómo configurar los grupos de seguridad y la red ACLs para optimizar DDoS la resiliencia, consulte Cómo prepararse para DDoS los ataques reduciendo su superficie de ataque.

Para obtener más información sobre el uso de Shield Advanced con direcciones IP elásticas como recursos protegidos, consulte los pasos para suscribirse AWS Shield Advanced.

## Protegiendo su origen (BP1,BP5)

Si utilizas Amazon CloudFront con un origen que está dentro del tuyoVPC, asegúrate de que solo tu CloudFront distribuidor pueda reenviar las solicitudes a tu origen. Con los encabezados de solicitud de extremo a origen, puedes añadir o anular el valor de los encabezados de solicitud existentes al reenviar las solicitudes a tu origen. CloudFront Puedes usar los encabezados personalizados de Origin, por ejemplo, el `X-Shared-Secret` encabezado, para comprobar desde dónde se enviaron las solicitudes realizadas a tu origen. CloudFront

Para obtener más información sobre cómo proteger tu origen con encabezados personalizados de Origin, consulta Cómo añadir encabezados personalizados a las solicitudes de origen y Restringir el acceso a los balanceadores de carga de aplicaciones.

Para obtener una guía sobre cómo implementar una solución de muestra para rotar automáticamente el valor de los encabezados personalizados de Origin para la restricción de acceso a origen, consulta Cómo mejorar la seguridad de CloudFront origen de Amazon con AWS WAF Secrets Manager.

Como alternativa, puedes usar una AWS Lambdafunción para actualizar automáticamente las reglas de tu grupo de seguridad y permitir solo CloudFront el tráfico. Esto mejora la seguridad de tu sitio de origen, ya que ayuda a garantizar que los usuarios malintencionados no puedan eludir CloudFront tu aplicación web ni AWS WAF acceder a ella.

Para obtener más información sobre cómo proteger tu origen mediante la actualización automática de tus grupos de seguridad y del `X-Shared-Secret` encabezado, consulta Cómo actualizar automáticamente tus grupos de seguridad para Amazon CloudFront y AWS WAF mediante el uso AWS Lambda.

Sin embargo, la solución implica una configuración adicional y el costo de ejecutar las funciones de Lambda. Para simplificarlo, ahora hemos introducido una lista de AWS prefijos gestionados para limitar el HTTPS tráfico entrante HTTP o que llega CloudFront a sus orígenes únicamente desde las direcciones IP orientadas al CloudFront origen. AWS-Las listas de prefijos gestionadas las crea y mantiene, AWS y están disponibles para su uso sin coste adicional. Puede hacer referencia a la lista de prefijos gestionados CloudFront en las reglas de su grupo de seguridad (AmazonVPC), en las tablas de enrutamiento de subred, en las reglas comunes de los grupos de seguridad y en cualquier otro AWS recurso que pueda utilizar una lista de prefijos gestionada. AWS Firewall Manager

Para obtener más información sobre el uso AWS de la lista de prefijos gestionada por Amazon CloudFront, consulta Limita el acceso a tus orígenes mediante la lista de prefijos AWS gestionada por Amazon. CloudFront

> **Note**
>
> Como se explica en otras secciones de este documento, confiar en los grupos de seguridad para proteger tu origen puede añadir el seguimiento de las conexiones de los grupos de seguridad como un posible cuello de botella durante una avalancha de solicitudes. A menos que seas capaz de filtrar las solicitudes malintencionadas CloudFront con una política de almacenamiento en caché que permita el almacenamiento en caché, puede ser mejor utilizar los encabezados personalizados de Origin, descritos anteriormente, para validar

que las solicitudes hechas a tu origen provienen de grupos de CloudFront seguridad. El uso de un encabezado de solicitud personalizado con una regla de escucha de Application Load Balancer evita la limitación debido a los límites de seguimiento que pueden afectar al establecimiento de nuevas conexiones a un balanceador de cargas, lo que permite que Application Load Balancer escale en función del aumento del tráfico en caso de un ataque. DDoS

## Proteger los puntos finales () API BP4

Cuando se debe exponer un API mensaje al público, existe el riesgo de que la API interfaz sea blanco de un DDoS ataque. Para ayudar a reducir el riesgo, puede utilizar Amazon API Gateway como puerta de entrada a las aplicaciones que se ejecutan en Amazon o en EC2 cualquier otro AWS Lambda lugar. Al utilizar Amazon API Gateway, no necesita sus propios servidores para la API interfaz y puede ocultar otros componentes de la aplicación. Al dificultar la detección de los componentes de su aplicación, puede evitar que esos AWS recursos sean blanco de un ataque. DDoS

Cuando utiliza Amazon API Gateway, puede elegir entre dos tipos de API puntos de enlace. La primera es la opción predeterminada: API puntos de enlace optimizados para periferia a los que se accede a través de una distribución de Amazon. CloudFront Sin embargo, API Gateway crea y administra la distribución, por lo que no tienes control sobre ella. La segunda opción consiste en utilizar un API punto final regional al que se acceda desde el mismo punto Región de AWS en el que REST API está desplegado el suyo. AWS recomienda que utilices el segundo tipo de punto final y lo asocies a tu propia CloudFront distribución de Amazon. Esto te da el control sobre la CloudFront distribución de Amazon y la posibilidad de utilizarla AWS WAF para la protección de la capa de aplicaciones. Este modo le proporciona acceso a una capacidad de DDoS mitigación escalable en toda la red perimetral AWS global.

Cuando utilice Amazon CloudFront y AWS WAF con Amazon API Gateway, configure las siguientes opciones:

- Configure el comportamiento de la caché de sus distribuciones para reenviar todos los encabezados al punto de API enlace regional de Gateway. De este modo, CloudFront tratará el contenido como dinámico y omitirá el almacenamiento en caché del contenido.
- Proteja su API Gateway contra el acceso directo configurando la distribución para que incluya el encabezado personalizado de origen; para ello x-api-key, establezca el valor de la APIclave en API Gateway.

- Proteja el backend del exceso de tráfico configurando límites de velocidad estándar o de ráfaga para cada método de su REST APIs dispositivo.

Para obtener más información sobre cómo crear APIs con Amazon API Gateway, consulte Introducción a Amazon API Gateway.

# Técnicas operativas

Las técnicas de mitigación de este paper le ayudan a diseñar aplicaciones que son intrínsecamente resistentes a DDoS los ataques. En muchos casos, también es útil saber cuándo un DDoS ataque está dirigido a tu aplicación para poder tomar medidas de mitigación. En esta sección, se analizan las mejores prácticas para obtener visibilidad sobre el comportamiento anormal, las alertas y la automatización, la gestión de la protección a escala y la contratación AWS de asistencia adicional.

## Prueba de carga

Realice pruebas de carga de su aplicación con regularidad siguiendo las pautas de nuestro documento técnico sobre aplicaciones de pruebas de carga con los niveles de tráfico esperados y superiores a los esperados para que pueda ver qué tan efectiva es su arquitectura, cómo funcionan sus políticas de Auto Scaling y cómo funciona su gestión de errores. Compruebe el aumento y la reducción esperados del tráfico, así como el comportamiento de tipo «aglomerado». Vuelva a realizar la prueba periódicamente o antes de cualquier versión importante. Para las pruebas de DDoS simulación de nivel 3 o 4, como las de SYN inundación, siga nuestra Política de pruebas de DDoS simulación.

## Métricas y alarmas

Como práctica recomendada, debe utilizar herramientas de monitoreo de infraestructura y aplicaciones para comprobar la disponibilidad de su aplicación y garantizar que su aplicación no se vea afectada por un DDoS evento. Como opción, puede configurar las comprobaciones de estado de la aplicación y la infraestructura de Route 53 para los recursos a fin de ayudar a mejorar la detección de DDoS eventos. Para obtener más información sobre las comprobaciones de estado AWS WAF, consulte la Guía avanzada para desarrolladores de Firewall Manager and Shield.

Cuando una métrica operativa clave se desvía sustancialmente del valor esperado, es posible que un atacante esté intentando atacar la disponibilidad de la aplicación. Si está familiarizado con el comportamiento normal de la aplicación, podrá actuar con mayor rapidez cuando detecte una anomalía. Amazon CloudWatch puede ayudarte supervisando las aplicaciones en las que ejecutas AWS. Por ejemplo, puede recopilar y realizar un seguimiento de las métricas, recopilar y supervisar los archivos de registro, configurar alarmas y responder automáticamente a los cambios en sus AWS recursos.

Si sigue la arquitectura DDoS de referencia flexible al diseñar la arquitectura de su aplicación, los ataques comunes a la capa de infraestructura se bloquearán antes de que lleguen a su aplicación. Si está suscrito AWS Shield Advanced, tiene acceso a una serie de CloudWatch métricas que pueden indicar que su aplicación está siendo atacada.

Por ejemplo, puedes configurar alarmas para que te avisen cuando se esté produciendo un DDoS ataque, de forma que puedas comprobar el estado de tu aplicación y decidir si quieres AWS SRT activarla. Puede configurar la `DDoSDetected` métrica para que le indique si se ha detectado un ataque. Si quieres recibir alertas en función del volumen de ataques, también puedes usar las `DDoSAttackRequestsPerSecond` métricas `DDoSAttackBitsPerSecondDDoSAttackPacketsPerSecond`, o. Puedes monitorizar estas métricas integrándolas CloudWatch con tus propias herramientas o utilizando herramientas proporcionadas por terceros, como Slack o. PagerDuty

Un ataque a la capa de aplicación puede mejorar muchas CloudWatch métricas de Amazon. Si lo usas AWS WAF, puedes usarlo CloudWatch para monitorear y activar alarmas cuando aumente el número de solicitudes que hayas configurado para que se AWS WAF permitan, se cuenten o se bloqueen. Esto te permite recibir una notificación si el nivel de tráfico supera lo que puede gestionar tu aplicación. También puede utilizar las métricas de Amazon CloudFront, Amazon Route 53, Application Load Balancer, Network Load Balancer, EC2 Amazon y Auto Scaling, a las que se CloudWatch hace un seguimiento para detectar cambios que puedan DDoS indicar un ataque.

En la siguiente tabla se enumeran las descripciones de CloudWatch las métricas que se utilizan habitualmente para detectar los ataques y reaccionar ante DDoS ellos.

Tabla 3: CloudWatch Métricas recomendadas de Amazon

| Tema | Métrica | Descripción |
| --- | --- | --- |
| AWS Shield Advanced | `DDoSDetected` | Indica un DDoS evento para un nombre de recurso de Amazon específico (ARN). |
| AWS Shield Advanced | `DDoSAttackBitsPerSecond` | El número de bytes observados durante un DDoS evento específicoARN. Esta métrica solo está disponible para los DDoS eventos de capa 3 o 4. |

| Tema | Métrica | Descripción |
| --- | --- | --- |
| AWS Shield Advanced | `DDoSAttackPacketsPerSecond` | El número de paquetes observados durante un DDoS evento específicoARN. Esta métrica solo está disponible para los DDoS eventos de nivel 3 o 4. |
| AWS Shield Advanced | `DDoSAttackRequestsPerSecond` | El número de solicitudes observadas durante un DDoS evento específicoARN. Esta métrica solo está disponible para los DDoS eventos de la capa 7 y solo se informa para los eventos de la capa 7 más importantes. |
| AWS WAF | `AllowedRequests` | El número de solicitudes web permitidas. |
| AWS WAF | `BlockedRequests` | El número de solicitudes web bloqueadas. |
| AWS WAF | `CountedRequests` | El número de solicitudes web contabilizadas. |
| AWS WAF | `PassedRequests` | El número de solicitudes aprobadas. Solo se usa para las solicitudes que se someten a una evaluación de un grupo de reglas sin coincidir con ninguna de las reglas del grupo de reglas. |
| Amazon CloudFront | `Requests` | El número de solicitudes HTTP de /S. |

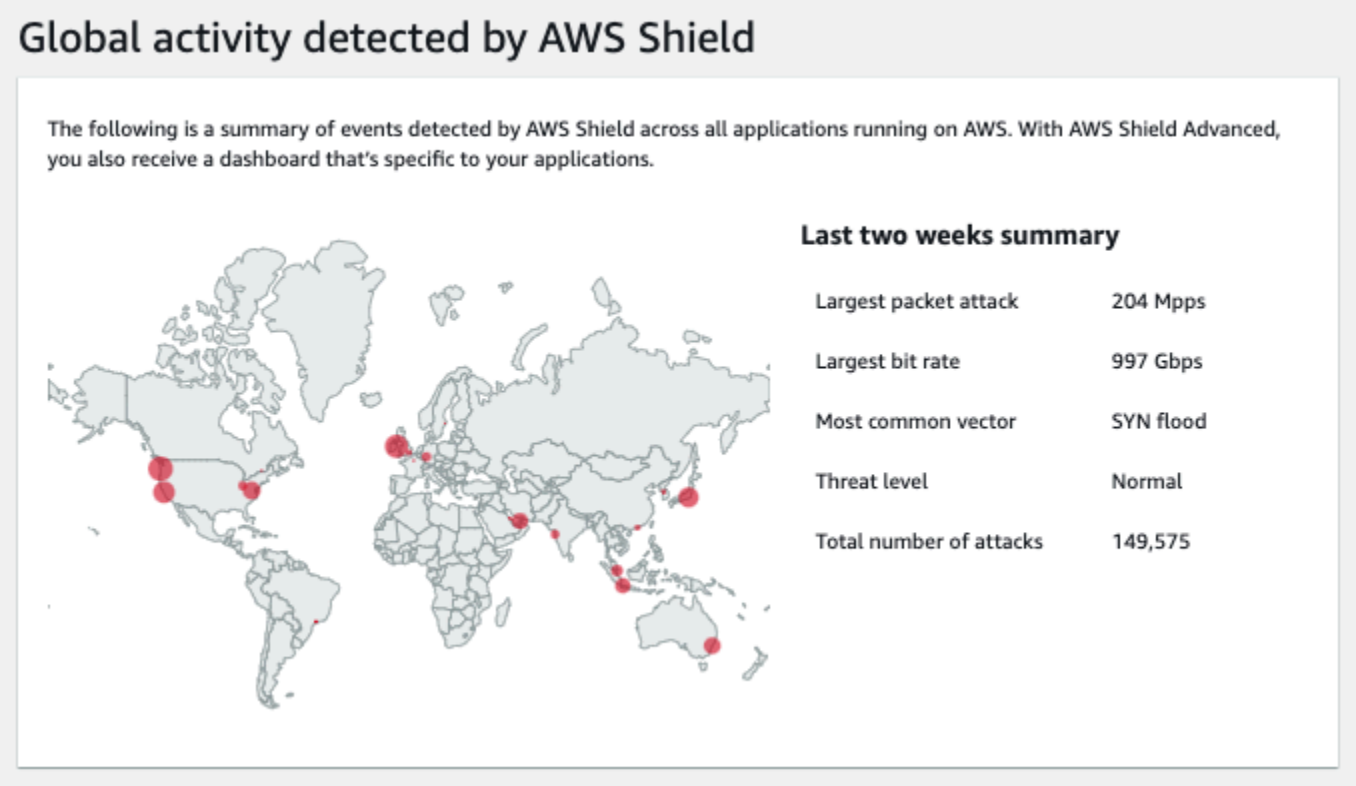
| Tema | Métrica | Descripción |
| --- | --- | --- |
| Amazon CloudFront | `TotalErrorRate` | El porcentaje de todas las solicitudes para las que el código de HTTP estado es `4xx` o`5xx`. |
| Amazon Route 53 | `HealthCheckStatus` | El estado del punto de conexión de comprobación de estado. |
| Equilibrador de carga de aplicación | `ActiveConnectionCount` | El número total de TCP conexiones simultáneas activas desde los clientes al balanceador de cargas y desde el balanceador de cargas a los destinos. |
| Equilibrador de carga de aplicación | `ConsumedLCUs` | El número de unidades de capacidad del balanceador de cargas (LCU) utilizadas por el balanceador de cargas. |
| Equilibrador de carga de aplicación | `HTTPCode_ELB_4XX_Count` `HTTPCode_ELB_5XX_Count` | El número de códigos de HTTP `4xx` error del `5xx` cliente generados por el balanceador de cargas. |
| Equilibrador de carga de aplicación | `NewConnectionCount` | El número total de TCP conexiones nuevas establecidas desde los clientes al balanceador de cargas y desde el balanceador de cargas a los destinos. |
| Equilibrador de carga de aplicación | `ProcessedBytes` | El número total de bytes procesados por el equilibrador de carga. |

| Tema | Métrica | Descripción |
| --- | --- | --- |
| Equilibrador de carga de aplicación | `RejectedConnectionCount` | El número de conexiones que se rechazaron porque el equilibrador de carga alcanzó el número máximo de conexiones. |
| Equilibrador de carga de aplicación | `RequestCount` | El número de solicitudes que se procesaron. |
| Equilibrador de carga de aplicación | `TargetConnectionErrorCount` | El número de conexiones que no se establecieron correctamente entre el equilibrador de carga y el destino. |
| Equilibrador de carga de aplicación | `TargetResponseTime` | El tiempo transcurrido, en segundos, desde que la solicitud salió del balanceador de cargas hasta que se recibió una respuesta del objetivo. |
| Equilibrador de carga de aplicación | `UnHealthyHostCount` | El número de destinos que se considera que no están en buen estado. |
| Equilibrador de carga de red | `ActiveFlowCount` | El número total de TCP flujos (o conexiones) simultáneos de los clientes a los destinos. |
| Equilibrador de carga de red | `ConsumedLCUs` | El número de unidades de capacidad del balanceador de cargas (LCU) utilizadas por el balanceador de cargas. |

| Tema | Métrica | Descripción |
| --- | --- | --- |
| Equilibrador de carga de red | `NewFlowCount` | El número total de TCP flujos (o conexiones) nuevos establecidos desde los clientes hasta los destinos en un período de tiempo. |
| Equilibrador de carga de red | `ProcessedBytes` | El número total de bytes procesados por el balancead or de cargas, incluidos los encabezados TCP /IP. |
| Global Accelerator | `NewFlowCount` | El número total de UDP flujos (o conexiones) nuevos TCP y establecidos desde los clientes hasta los puntos finales en el período de tiempo. |
| Global Accelerator | `ProcessedBytesIn` | El número total de bytes entrantes procesados por el acelerador, incluidos los encabezados TCP /IP. |
| Auto Scaling | `GroupMaxSize` | El tamaño máximo del grupo de Auto Scaling. |
| Amazon EC2 | `CPUUtilization` | El porcentaje de unidades de EC2 cómputo asignadas que están actualmente en uso. |
| Amazon EC2 | `NetworkIn` | El número de bytes recibidos por la instancia en todas las interfaces de red. |

Para obtener más información sobre el uso de Amazon CloudWatch para detectar DDoS ataques a tu aplicación, consulta Cómo empezar con Amazon CloudWatch.

AWS incluye varias métricas y alarmas adicionales para avisarle de un ataque y ayudarle a supervisar los recursos de su aplicación. La AWS Shield consola o API proporcione un resumen de los eventos por cuenta y detalles sobre los ataques que se hayan detectado.




Actividad global detectada por AWS Shield

Además, el panel del entorno de amenazas global proporciona información resumida sobre todos DDoS los ataques detectados por AWS. Esta información puede resultar útil para comprender mejor DDoS las amenazas en un mayor número de aplicaciones, además de las tendencias de los ataques, y compararlas con los ataques que pueda haber observado.

Si está suscrito AWS Shield Advanced, el panel de servicio muestra métricas adicionales de detección y mitigación y detalles del tráfico de red de los eventos detectados en los recursos protegidos. AWS Shield evalúa el tráfico hacia su recurso protegido en varias dimensiones. Cuando se detecta una anomalía, AWS Shield crea un evento e informa de la dimensión de tráfico en la que se observó la anomalía. Si se aplica una mitigación, se protege el recurso de recibir tráfico excesivo y tráfico que coincida con la firma de un DDoS evento conocido.

Las métricas de detección se basan en flujos de red o AWS WAF registros muestreados cuando una web ACL está asociada al recurso protegido. Las métricas de mitigación se basan en el tráfico

observado por los sistemas de DDoS mitigación de Shield. Las métricas de mitigación son una medida más precisa del tráfico que llega a su recurso.

La métrica de los principales contribuyentes de la red proporciona información sobre la procedencia del tráfico durante un evento detectado. Puedes ver los contribuyentes con mayor volumen y ordenarlos por aspectos como el protocolo, el puerto de origen y los TCP indicadores. La métrica de los principales contribuyentes incluye métricas de todo el tráfico observado en el recurso en varias dimensiones. Proporciona dimensiones métricas adicionales que puede utilizar para comprender el tráfico de red que se envía a su recurso durante un evento. Tenga en cuenta que, en el caso de los ataques de capa 3 o 4 que no reflejan el reflejo, es posible que las direcciones IP de origen hayan sido falsificadas y no se pueda confiar en ellas.

El panel de servicio también incluye detalles sobre las acciones que se toman automáticamente para mitigar los ataques. DDoS Esta información facilita la investigación de anomalías, la exploración de las dimensiones del tráfico y la mejor comprensión de las medidas adoptadas por Shield Advanced para proteger su disponibilidad.

## Registro

Habilite un registro útil en todos los servicios de acuerdo con nuestra guía de registro y monitoreo para propietarios de aplicaciones a fin de maximizar la visibilidad y ayudar a solucionar problemas. Esto incluye, pero no se limita a:

- AWS CloudTrail
- Registros de AWS WAF
- CloudFrontregistros de acceso
- VPCRegistros de flujo (consulte Registrar y ver los flujos de tráfico de red): incluya un `tcp-flags` campo en los campos incluidos para maximizar la visibilidad
- ELBregistros de acceso (ALB, CLB, NLB)
- registros de HTTP acceso al servidor web
- Registro de seguridad del sistema operativo
- Registro de aplicaciones

# Gestión de la visibilidad y la protección en varias cuentas

En situaciones en las que opera con varios componentes Cuentas de AWS y tiene varios componentes que proteger, el uso de técnicas que le permitan operar a escala y reducir la sobrecarga operativa aumenta sus capacidades de mitigación. Al administrar los recursos AWS Shield Advanced protegidos en varias cuentas, puede configurar la supervisión centralizada mediante AWS Firewall Manager y AWS Security Hub. Con Firewall Manager, puede crear una política de seguridad que imponga el cumplimiento de las normas de DDoS protección en todas sus cuentas. Puede usar estos dos servicios juntos para administrar sus recursos protegidos en varias cuentas y centralizar la supervisión de esos recursos.

Security Hub se integra automáticamente con Firewall Manager, lo que permite a los clientes de Shield Advanced ver los hallazgos de seguridad en un único panel de control, junto con otras alertas de seguridad y estados de cumplimiento de alta prioridad.

Por ejemplo, cuando Shield Advanced detecte tráfico anómalo destinado a un recurso protegido en cualquier lugar del Cuenta de AWS ámbito, este hallazgo estará visible en la consola de Security Hub. Si está configurado, Firewall Manager puede hacer que el recurso cumpla automáticamente las normas al crearlo como un recurso protegido por Shield Advanced y, a continuación, actualizar Security Hub cuando el recurso esté en un estado compatible.

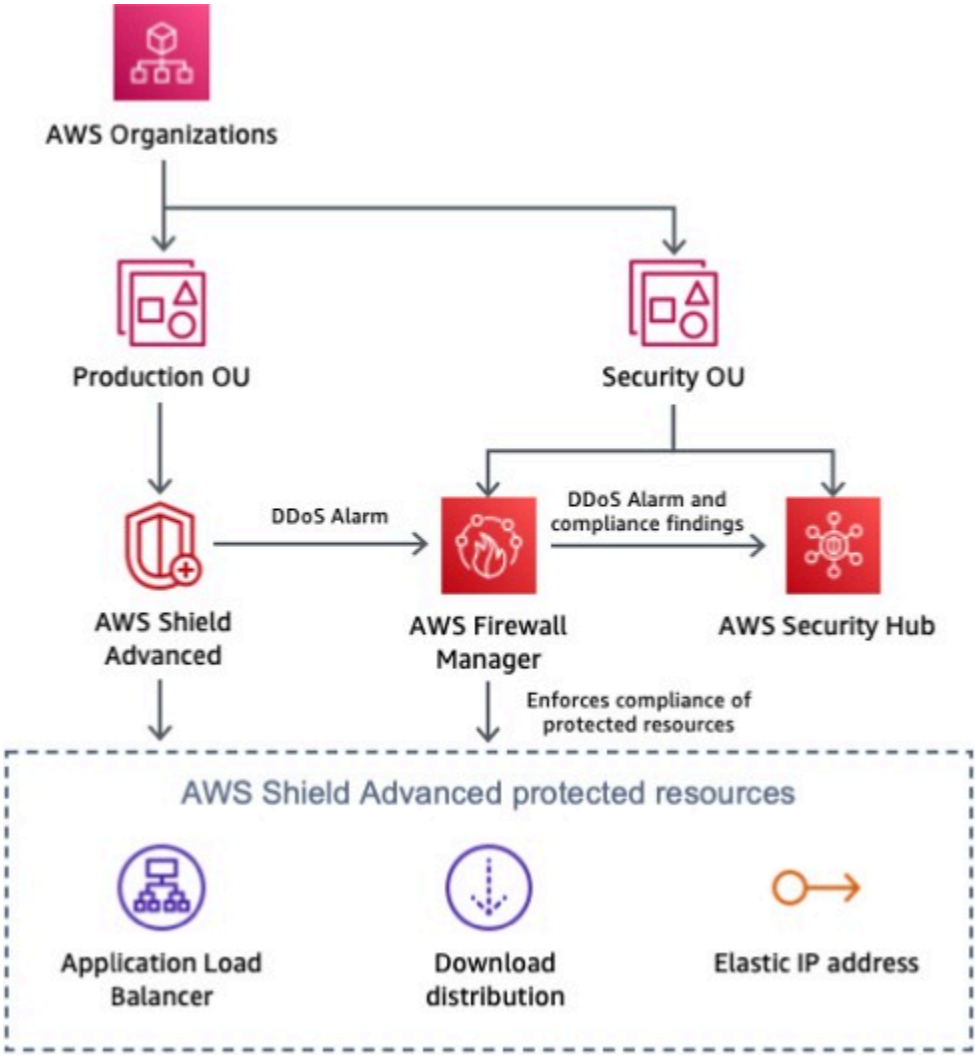



Diagrama de arquitectura que muestra la supervisión AWS Shield de recursos protegidos con Firewall Manager y Security Hub

Para obtener más información sobre la supervisión central de los recursos protegidos por Shield, consulte Configurar la supervisión centralizada de DDoS eventos y corregir automáticamente los recursos no conformes.

## Estrategia y manuales de respuesta a incidentes

Desarrollar una estrategia de respuesta a los DDoS ataques y crear un proceso de respuesta a los incidentes de seguridad en torno a ella es crucial para todas las organizaciones. Un enfoque recomendado consiste en modelar el manual de respuesta en función de los pasos sugeridos, como NIST la recopilación de pruebas, la mitigación, la recuperación y la realización de un análisis posterior al incidente. Por ejemplo, se proporciona como ejemplo un manual de respuesta para DoS

o DDoS ataques de aplicaciones web. Hay recursos adicionales disponibles en la Guía de respuesta a incidentes de AWS seguridad.

# Soporte

Si sufre un ataque, también puede solicitar ayuda para evaluar AWS la amenaza y revisar la arquitectura de su aplicación, o bien solicitar otro tipo de asistencia. Es importante crear un plan de respuesta a DDoS los ataques antes de que se produzca un suceso real. Las mejores prácticas descritas en este paper pretenden ser medidas proactivas que se implementen antes de lanzar una aplicación, pero es posible que aún se produzcan DDoS ataques contra la aplicación. Revise las opciones de esta sección para determinar los recursos de soporte que mejor se adapten a su situación. Su equipo de cuentas puede evaluar su caso de uso y su solicitud, y ayudarlo con las preguntas o desafíos específicos que tenga.

Si está ejecutando cargas de trabajo de producción AWS, considere la posibilidad de suscribirse a Business Support, que le proporciona acceso ininterrumpido a ingenieros de soporte en la nube que pueden ayudarlo con los problemas de DDoS ataque. Si está ejecutando cargas de trabajo de misión crítica, considere Enterprise Support, que ofrece la posibilidad de abrir casos críticos y recibir la respuesta más rápida de un ingeniero sénior de soporte en la nube.

Si está suscrito AWS Shield Advanced y también está suscrito a Business Support o Enterprise Support, puede configurar la participación proactiva de Shield. Le permite configurar los controles de estado, asociarlos a sus recursos y proporcionar información de contacto operativa ininterrumpida. Cuando Shield detecte señales de degradación DDoS y las comprobaciones de estado de la aplicación muestren señales de degradación, AWS SRT se pondrá en contacto contigo de forma proactiva. Este es nuestro modelo de colaboración recomendado porque permite tiempos de AWS SRT respuesta más rápidos y permite empezar AWS SRT a solucionar problemas incluso antes de que se haya establecido contacto con usted.

Para obtener más información, consulta Comparar AWS Support planes.

La función de participación proactiva requiere que configure una comprobación de estado de Route 53 que mida con precisión el estado de su aplicación y esté asociada al recurso protegido por Shield Advanced. Una vez que se asocia una comprobación de estado de Route 53 a la consola Shield, el sistema de detección Shield Advanced utiliza el estado de la comprobación de estado como indicador del estado de la aplicación. La función de detección basada en el estado de Shield Advanced garantizará que se le notifique y que las mitigaciones se apliquen más rápidamente cuando la aplicación no esté en buen estado. AWS SRTse pondrá en contacto con usted para

determinar si la aplicación en mal estado está siendo objeto de un DDoS ataque y aplicar las medidas de mitigación adicionales que sean necesarias.

Para completar la configuración de la interacción proactiva, se incluyen los detalles de contacto en la consola Shield. AWS SRTutilizará esta información para ponerse en contacto con usted. Puede configurar hasta diez contactos y proporcionar notas adicionales si tiene requisitos o preferencias de contacto específicos. Proactiva

Los contactos de interacción deben desempeñar una función ininterrumpida, como un centro de operaciones de seguridad o una persona que esté disponible de inmediato.

Puede habilitar la participación proactiva de todos los recursos o de algunos recursos de producción clave en los que el tiempo de respuesta es fundamental. Esto se logra mediante la asignación de controles de estado únicamente a estos recursos.

También puede escalar un AWS Support caso AWS SRT mediante la AWS Support consola (es necesario iniciar sesión) o Support API si tiene un evento DDoS relacionado que afecte a la disponibilidad de su aplicación.

# Conclusión

Las mejores prácticas descritas en este paper pueden ayudarlo a crear una arquitectura DDoS resiliente que proteja la disponibilidad de su aplicación al evitar muchos DDoS ataques comunes a la infraestructura y la capa de aplicaciones. La medida en que siga estas mejores prácticas al diseñar su aplicación influirá en el tipo, el vector y el volumen de DDoS los ataques que pueda mitigar. Puede incorporar la resiliencia sin tener que suscribirse a un servicio de DDoS mitigación. Si opta por suscribirse, AWS Shield Advanced obtiene funciones adicionales de soporte, visibilidad, mitigación y protección de costos que protegen aún más una arquitectura de aplicaciones que ya es flexible.

# Colaboradores

Los colaboradores de este documento son:

- Rodrigo Ferroni, AWS especialista en seguridad TAM
- Dmitriy Novikov, arquitecto de soluciones AWS
- Achraf Souk, arquitecto de soluciones AWS
- Joanna Knox, ingeniería AWS Support
- Anuj Butail, arquitecto de soluciones AWS
- Harith Gaddamanugu, Edge Specialist SA AWS

# Documentación adicional

Para obtener información adicional, consulte los siguientes recursos:

- Directrices para la implementación AWS WAF (AWS documento técnico)
- NIS301 — Re:inForce 2023: cómo la inteligencia de AWS amenazas se convierte en reglas de firewall gestionadas (vídeo) YouTube
- NET314- Re:Invent 2022: Creación de aplicaciones resilientes mediante DDoS (vídeo) AWS Shield YouTube
- SEC321- Re:Invent 2020: póngase a la vanguardia con las ampliaciones del equipo de DDoS respuesta (vídeo) YouTube
- William Hill: DDoS Protección de alto rendimiento con AWS - 2020 (vídeo) YouTube
- SEC407 - Re:Invent 2019: un defense-in-depth enfoque para la creación de aplicaciones web (vídeo) YouTube
- Mejores prácticas de DDoS mitigación en AWS 2018 (vídeo) YouTube
- SID324— re:Invent 2017: Automatizar la DDoS respuesta en la nube (vídeo) YouTube
- CTD304 — Re:Invent 2017: La trayectoria de Dow Jones y Wall Street Journal para gestionar los picos de tráfico (vídeo) YouTube
- Mitigación de las amenazas DDoS y de la capa de aplicación (vídeo) YouTube
- CTD310 — Re:Invent 2017: Vivir al límite, ¡es más seguro de lo que cree! Fortaleciendo con Amazon (YouTube vídeo)
- CloudFront AWS Shield, y AWS WAF (YouTube vídeo)

# Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase al feed. RSS

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Actualización del documento técnico | Se agregó OAC una protección CloudFront de DNS costos estándar. Análisis ampliado sobre las técnicas operativas, el almacenamiento en caché, las reglas basadas en tasas y los grupos de reglas gestionados. Se agregó la tecnología local al diagrama de arquitectura, se eliminó la duplicación y se aclaró el texto para eliminar la ambigüedad. | 9 de agosto de 2023 |
| Actualización del documento técnico | Revisado para mayor claridad; actualizado para incluir las recomendaciones y funciones más recientes: seguimiento de conexiones de grupos de seguridad y DDoS mitigación automática de la capa de aplicación Shield Advanced. | 13 de abril de 2022 |
| Actualización del documento técnico | Se ha actualizado para incluir las recomendaciones y funciones más recientes. AWS Global Accelerator se añade como parte de una protección integral en la periferia. AWS Firewall Manager para la supervisión centralizada de | 21 de septiembre de 2021 |

| | | |
|---|---|---|
| | DDoS eventos y la corrección automática de los recursos no conformes. | |
| Actualización del documento técnico | Se actualizó para aclarar la acumulación de caché en la sección Detectar y filtrar solicitudes web maliciosas (BP1,BP2) ELB y su ALB uso en la sección Scale to Absorb (BP6). Se actualizaron los diagramas y la tabla 2, marcados como «Selección de región». comoBP8. BP7Sección actualizada con más detalles. | 18 de diciembre de 2019 |
| Actualización del documento técnico | Se ha actualizado para incluir el AWS WAF registro como práctica recomendada. | 1 de diciembre de 2018 |
| Actualización del documento técnico | Se actualizó para incluir AWS Shield AWS WAF funciones y mejores prácticas relacionadas. AWS Firewall Manager | 1 de junio de 2018 |
| Actualización del documento técnico | Se agregó una guía de arquitectura prescriptiva y se actualizó para incluirla. AWS WAF | 1 de junio de 2016 |
| Publicación inicial | Documento técnico publicado. | 1 de junio de 2015 |

# Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas de AWS productos actuales, que están sujetas a cambios sin previo aviso, y (c) no crea ningún compromiso ni garantía por parte de AWS sus filiales, proveedores o licenciantes. AWS los productos o servicios se proporcionan «tal cual» sin garantías, representaciones o condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS sus clientes están reguladas por AWS acuerdos, y este documento no forma parte de ningún acuerdo entre sus clientes AWS y sus clientes ni lo modifica.

# AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.