SERVICIOS DE SEGURIDAD ADICIONALES

CONTENIDO

SERVICIOS DE SEGURIDAD ADICIONALES

Una seguridad sólida en el centro de una organización permite la transformación digital y la innovación. AWS ayuda a las organizaciones a desarrollar y convertir la seguridad, la identidad y el cumplimiento en facilitadores empresariales clave. En AWS, la seguridad es la máxima prioridad. AWS está diseñado para ser la infraestructura en la nube global más segura en la que crear, migrar y administrar aplicaciones y cargas de trabajo. Esto está respaldado por un amplio conjunto de más de 300 servicios y características de seguridad.

Continuando con los servicios de seguridad, vamos a hablar de Amazon Inspector, que ayuda a mejorar la seguridad y el cumplimiento de las aplicaciones implementadas en AWS mediante la ejecución de una evaluación de seguridad automatizada en su infraestructura. Específicamente, Amazon Inspector ayuda a comprobar las desviaciones de las prácticas recomendadas de seguridad, la exposición de instancias de EC2, las vulnerabilidades, etc. El servicio consta de tres partes: Una pieza de accesibilidad de configuración de red, un agente de Amazon, que se puede instalar en las instancias de EC2, y un servicio de evaluación de seguridad que las reúne a todas.
Para usarlo, configure las opciones de Inspector, ejecute el servicio y, a continuación, aparece una lista de posibles problemas de seguridad. Los hallazgos resultantes se muestran en la consola de Amazon Inspector y presentan una descripción detallada del problema de seguridad, y una recomendación sobre cómo solucionarlo.
Además, puede recuperar hallazgos a través de la API, con el objetivo de alinearse a las prácticas recomendadas y realizar corrección para solucionar sus problemas.

Otra oferta de AWS de servicio para la detección de amenazas es Amazon GuardDuty. Este servicio analiza flujos continuos de metadatos generados desde su cuenta y actividad de red encontrada en eventos de AWS CloudTrail, registros de flujo de Amazon VPC y registros de DNS.
Utiliza inteligencia integrada contra amenazas como: Direcciones IP maliciosas conocidas, detección de anomalías y machine learning para identificar amenazas con más precisión. La mejor parte es que se ejecuta independiente de los demás servicios de AWS, por lo que no afectará al rendimiento ni a la disponibilidad de la infraestructura existente y a las cargas de trabajo.

Hay muchos otros servicios de seguridad como AWS WAF, que permite proteger las aplicaciones web y las APIs de ataques y bots malintencionados y AWS Shield, que protege contra ataques de denegación de servicio distribuidos, los cuales abordaremos también en esta clase.

AWS WAF

AWS WAF es un firewall para aplicaciones web que ayuda a proteger aplicaciones web contra ataques al permitirle configurar reglas que habilitan, bloquean o monitorizan (cuentan) las solicitudes web a partir de las condiciones que usted defina. Las condiciones incluyen direcciones IP, encabezados HTTP, cadenas URI, inyección de código SQL y scripting entre sitios.

AWS WAF trabaja junto con Amazon CloudFront y un Application Load Balancer. Recuerde las listas de control de acceso a la red sobre las que aprendió en la clase de conectividad. AWS WAF funciona de forma similar para bloquear o permitir el tráfico, sin embargo, lo hace mediante una lista de control de acceso (ACL) web para proteger sus recursos de AWS.

AWS WAF le permite crear reglas de seguridad que controlan el tráfico de bots y bloquean los patrones de ataque comunes, como la inyección de código SQL o el scripting entre sitios (XSS).

A continuación, veamos un ejemplo del modo en que puede utilizar AWS WAF para permitir y bloquear solicitudes específicas: Imagine que su aplicación estuvo recibiendo solicitudes de red maliciosas de varias direcciones IP. Quiere evitar que estas solicitudes sigan accediendo a su aplicación, pero también quiere asegurarse de que los usuarios legítimos puedan seguir accediendo a ella. Configure la ACL web para permitir todas las solicitudes excepto las de las direcciones IP especificadas.

Cuando una solicitud llega a AWS WAF, se compara con la lista de reglas que ha configurado en la ACL web. Si una solicitud no proviene de una de las direcciones IP bloqueadas, entonces se permite el acceso a la aplicación.

Sin embargo, si una solicitud proviene de una de las direcciones IP bloqueadas que ha especificado en la ACL web, AWS WAF le deniega el acceso.

FUNCIONAMIENTO DE AWS WAF

AWS WAF lo ayuda a protegerse de los exploits y bots web comunes que podrían afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos.

CARACTERÍSTICAS DE AWS WAF

Filtrado del tráfico web: AWS WAF permite crear reglas para filtrar el tráfico web en función de condiciones como la dirección IP, los encabezados y cuerpos HTTP o los URI personalizados. Esto ofrece un nivel de protección adicional frente a ataques web que intenten aprovechar vulnerabilidades en aplicaciones web personalizadas o de terceros. Además, con AWS WAF es sencillo crear reglas que bloqueen ataques comunes como la inyección SQL o el scripting entre sitios.

AWS WAF permite crear un conjunto centralizado de reglas que puede implementar en varios sitios web. Esto significa que, en un entorno con muchos sitios y aplicaciones web, puede crear un único conjunto de reglas que es posible reutilizar entre aplicaciones, en vez de tener que volver a crear la regla en cada una de las aplicaciones que desea proteger.

AWS WAF Bot Control: AWS WAF Bot Control es un grupo de reglas administrado que brinda visibilidad y control sobre el tráfico de bot común y generalizado que puede consumir recursos en exceso, sesgar las métricas, generar tiempo de inactividad o realizar otras actividades no deseadas. Con solo unos pocos clics, puede bloquear o limitar fácilmente los bots generales, como raspadores, escáneres y rastreadores, o puede permitir bots comunes, como monitores de estado y motores de búsqueda.

Prevención del fraude en la toma de control de cuenta: AWS WAF Fraud Control Account Takeover Prevention es un grupo de reglas administrado que supervisa la página de inicio de sesión de su aplicación para detectar el acceso no autorizado a las cuentas de usuario con credenciales comprometidas. Puede utilizar el grupo de reglas para protegerse contra ataques de relleno de credenciales, intentos de inicio de sesión por fuerza bruta y otras actividades de inicio de sesión anómalas. Con SDK opcionales de JavaScript e iOS o Android, puede recibir telemetría adicional en los dispositivos de usuarios que intentan iniciar sesión en su aplicación para protegerla mejor contra intentos de inicio de sesión automatizados por parte de bots.

Prevención del fraude en la creación de cuentas: La prevención del fraude en la creación de cuentas es un grupo de reglas administrado que supervisa el inicio de sesión en la aplicación o la página de registro para detectar la creación de cuentas falsas o fraudulentas. Puede usar el grupo de reglas para protegerse contra el abuso, como el abuso promocional o de inicio de sesión, el abuso por lealtad o recompensas y la suplantación de identidad.

API completa: AWS WAF puede administrarse por completo mediante API. Esto proporciona a las organizaciones la capacidad de crear y mantener reglas automáticamente e incorporarlas al proceso de desarrollo y diseño. Por ejemplo, un desarrollador que cuente con un conocimiento detallado de la aplicación web podría crear una regla de seguridad

como parte del proceso de implementación. Esta capacidad para incorporar seguridad al proceso de desarrollo evita complejas entregas entre la aplicación y los equipos de seguridad para asegurar que las reglas estén actualizadas.

AWS WAF también puede implementarse y aprovisionarse automáticamente con plantillas de muestra de AWS CloudFormation que permiten describir todas las reglas de seguridad que quiera implementar para sus aplicaciones web, entregadas por Amazon CloudFront.

Visibilidad en tiempo real: AWS WAF proporciona métricas en tiempo real y registra solicitudes sin procesar que incluyen detalles sobre direcciones IP, geolocalización, URI, agentes de usuario y recomendaciones. AWS WAF está plenamente integrado con Amazon CloudWatch, por lo que es sencillo configurar alarmas personalizadas cuando se excedan los umbrales o se produzcan ataques particulares. Se trata de información útil que puede emplearse para crear nuevas reglas que protejan mejor las aplicaciones.

AMAZON INSPECTOR

Amazon Inspector es un servicio de administración de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS en busca de vulnerabilidades de software y exposiciones involuntarias a la red. Con tan solo unos clics en la consola de administración de AWS, puede usar Amazon Inspector en todas las cuentas de su organización. Una vez que se inicia, detecta automáticamente las instancias de Amazon Elastic Compute Cloud (EC2) en ejecución, las imágenes de contenedor de Amazon Elastic Container Registry (Amazon ECR) y las funciones de AWS Lambda, a escala, y comienza de manera inmediata a evaluarlas en busca de vulnerabilidades conocidas.

Amazon Inspector calcula una puntuación de riesgo altamente contextualizada para cada resultado, ya que correlaciona informaciones de vulnerabilidades y exposiciones comunes (CVE) con factores como acceso a la red y explotabilidad. Esta puntuación se utiliza para dar prioridad a las vulnerabilidades más críticas y mejorar la eficiencia de la respuesta para solucionar dichas vulnerabilidades. Todos los resultados se agregan en la consola de Amazon Inspector y se transfieren a AWS Security Hub y a Amazon EventBridge para automatizar los flujos de trabajo. Las vulnerabilidades que se encuentran en imágenes de contenedores también se envían a Amazon ECR para que los propietarios de los recursos las visualicen y solucionen. Amazon Inspector permite a los equipos de seguridad y a los desarrolladores de cualquier tamaño lograr una seguridad y conformidad completas de la carga de trabajo de la infraestructura en sus entornos de AWS.

Supongamos que los desarrolladores de la cafetería están desarrollando y probando una nueva aplicación de pedidos. Quieren asegurarse de que están diseñando la aplicación de

acuerdo con las prácticas recomendadas de seguridad. Sin embargo, tienen que desarrollar otras aplicaciones, por lo que no pueden dedicar mucho tiempo a realizar evaluaciones manuales. Para realizar evaluaciones de seguridad automatizadas, deciden utilizar Amazon Inspector.

Amazon Inspector ayuda a mejorar la seguridad y el cumplimiento de las aplicaciones mediante la ejecución de evaluaciones de seguridad automatizadas. Comprueba las vulnerabilidades de seguridad y las desviaciones de las prácticas recomendadas de seguridad de las aplicaciones, como el acceso abierto a instancias de Amazon EC2 y las instalaciones de versiones de software vulnerables.

Una vez que Amazon Inspector realizó una evaluación, le proporciona una lista de los resultados de seguridad. La lista prioriza por nivel de gravedad, incluida una descripción detallada de cada problema de seguridad y una recomendación sobre cómo solucionarlo. Sin embargo, AWS no garantiza que, siguiendo las recomendaciones proporcionadas, se solucionen todos los posibles problemas de seguridad. Según el modelo de responsabilidad compartida, los clientes son responsables de la seguridad de sus aplicaciones, procesos y herramientas que se ejecutan en los servicios de AWS.

BENEFICIOS DE AMAZON INSPECTOR

Detecte las vulnerabilidades del software: Detecte las vulnerabilidades del software y la exposición involuntaria de la red en las cargas de trabajo de AWS, como Amazon EC2, las funciones de AWS Lambda y las imágenes de contenedores en Amazon ECR y en las herramientas de integración continua y entrega continua (CI/CD), prácticamente en tiempo real.

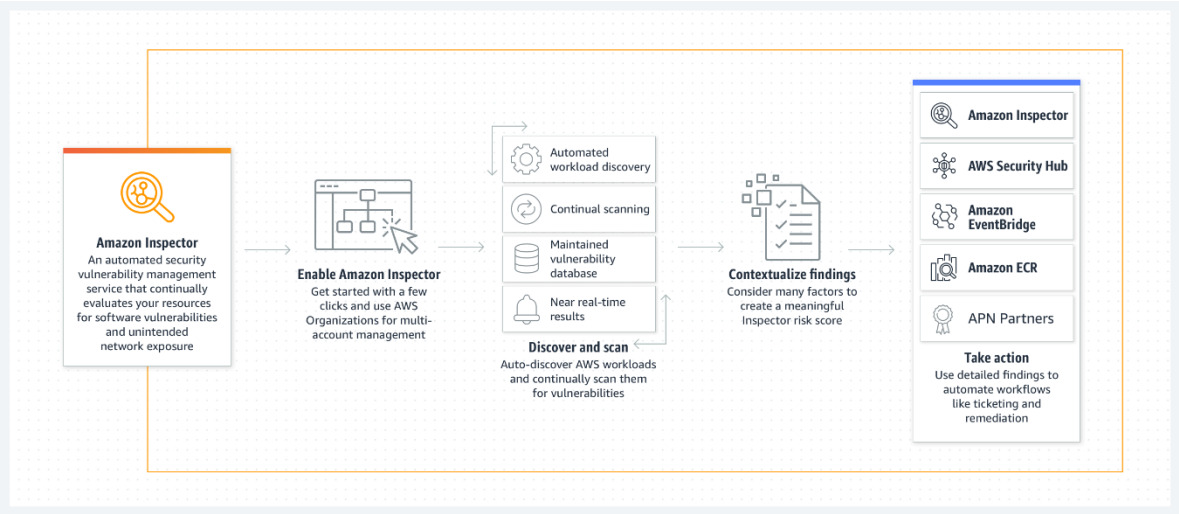
Administre las exportaciones de SBOM de forma centralizada: Incorpore la seguridad en las primeras etapas de los ciclos de desarrollo y administre de forma centralizada las exportaciones de listas de materiales del software (SBOM) para todos los recursos monitoreados.

Priorice la corrección: Utilice la puntuación de riesgo de Amazon Inspector para priorizar la corrección y reducir el tiempo medio de corrección (MTTR).

Maximice la cobertura de evaluación de vulnerabilidades: Escanee sin problemas las instancias EC2 y cambie entre el escaneo basado en agentes y sin agente.

FUNCIONAMIENTO DE AMAZON INSPECTOR

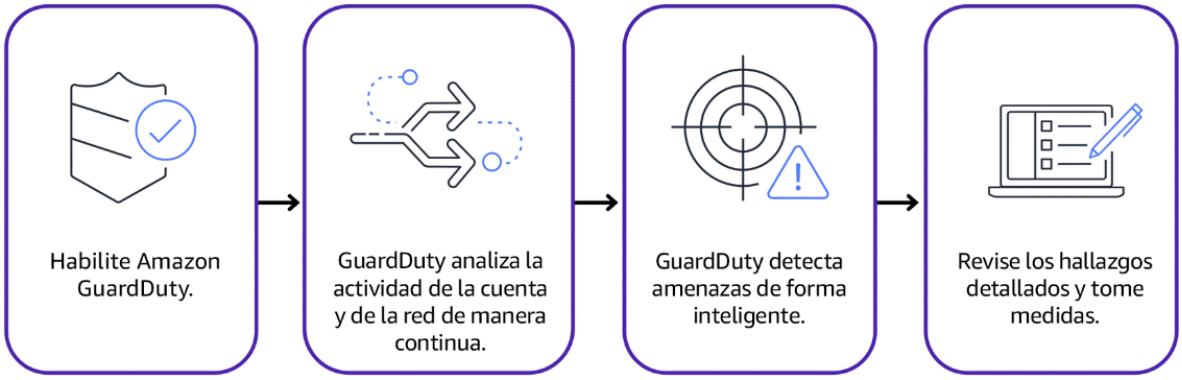
Amazon Inspector es un servicio de administración automatizada de vulnerabilidades que analiza continuamente las cargas de trabajo de AWS en busca de vulnerabilidades de software y exposición involuntaria a la red.



AMAZON GUARDUTY

Amazon GuardDuty es un servicio de detección de amenazas que supervisa continuamente la actividad maliciosa y el comportamiento no autorizado a lo largo de su entorno de AWS. Mediante el uso de orígenes de AWS y de terceros líderes del sector, GuardDuty combina machine learning, la detección de anomalías y la detección de archivos maliciosos para ayudar a proteger sus cuentas, las cargas de trabajo y los datos en AWS. GuardDuty analiza eventos a través de varios orígenes de datos de AWS, incluidos los registros de AWS CloudTrail, los registros de flujo de Amazon Virtual Private Cloud (Amazon VPC) y los registros de consultas de DNS. GuardDuty también supervisa los eventos de datos de Amazon Simple Storage Service (Amazon S3), los eventos de inicio de sesión de Amazon Aurora y la actividad de tiempo de ejecución de Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Compute Cloud (Amazon EC2) y Amazon Elastic Container Service (Amazon ECS), lo que incluye las cargas de trabajo de contenedores sin servidor en AWS Fargate.

Amazon GuardDuty es un servicio que proporciona la detección inteligente de amenazas para la infraestructura y los recursos de AWS. Identifica las amenazas mediante el monitoreo continuo de la actividad de la red y el comportamiento de la cuenta en el entorno de AWS.



Después de habilitar GuardDuty en su cuenta de AWS, GuardDuty comienza a supervisar la actividad de la red y de la cuenta. No es necesario desplegar ni administrar ningún software de seguridad adicional. GuardDuty analiza continuamente los datos de varias fuentes de AWS, incluidos los registros de flujo de VPC y los registros de DNS.

Si GuardDuty detecta amenazas, usted puede revisar los resultados detallados sobre ellas desde la consola de administración de AWS. Los hallazgos incluyen los pasos recomendados para la corrección. También puede configurar las funciones de AWS Lambda para que adopten medidas correctivas automáticamente en respuesta a los descubrimientos de seguridad de GuardDuty.

Amazon GuardDuty combina el machine learning y la inteligencia de amenazas integrada de AWS y de terceros líderes para ayudar a proteger las cuentas, las cargas de trabajo y los datos de AWS ante amenazas.

VENTAJAS DE AMAZON GUARDUTY

Monitoreo constante: Mantenga sus cuentas, cargas de trabajo y datos seguros mediante el monitoreo continuo de posibles amenazas en su entorno de AWS.

Detección de amenazas con tecnología de ML: Detecte las amenazas rápidamente mediante la detección de anomalías, el machine learning (ML), el modelado del comportamiento y la información sobre amenazas de AWS y de terceros líderes.

Responda más rápido a las amenazas: Detecte las amenazas con precisión y responda a ellas antes, lo que lo ayudará a detectarlas antes de que se conviertan en eventos más amplios que afecten al negocio.

Detección de amenazas escalable y totalmente administrada: Escale la detección de amenazas en todas las cuentas de su entorno de AWS sin necesidad de esfuerzo manual ni herramientas de terceros.

Visibilidad integral de las cargas de trabajo de computación de AWS: Proteja sus cuentas, datos y recursos en varios tipos de cómputo de AWS, que abarcan Amazon Elastic Compute Cloud (Amazon EC2), cargas de trabajo sin servidor y cargas de trabajo en contenedores, incluidas las de AWS Fargate.

FUNCIONAMIENTO DE AMAZON GUARDUTY

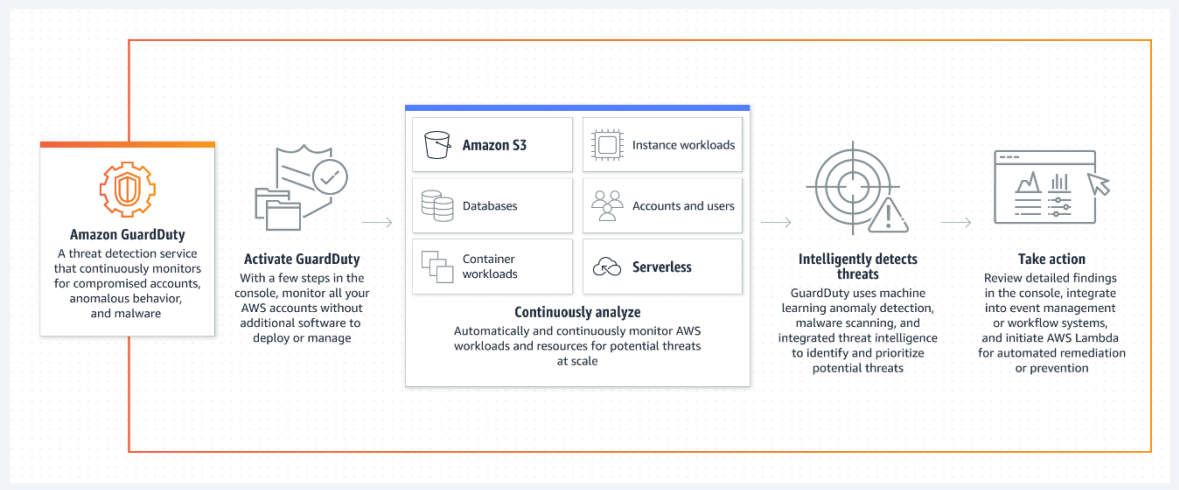
Este diagrama detalla las características y la integración de GuardDuty con diferentes tipos de recursos y cargas de trabajo de AWS. El diagrama está dividido en cinco secciones que se muestran de izquierda a derecha.

La primera sección se titula “Amazon GuardDuty” y dice: “Un servicio de detección de amenazas que supervisa continuamente las cuentas comprometidas, el comportamiento anómalo y el malware”.

La segunda sección se titula “Activar GuardDuty”. La segunda sección dice: “Con unos pocos pasos en la consola, monitoree todas sus cuentas de AWS sin necesidad de implementar o administrar software adicional”.

En la tercera sección se explican los diferentes tipos de cargas de trabajo y recursos que puede monitorear continuamente para detectar amenazas con Amazon GuardDuty. Los elementos descritos son: Amazon S3, bases de datos, cargas de trabajo de contenedores, cargas de trabajo de instancias, cuentas y usuarios, y sistemas sin servidor.
En la tercera sección, debajo de la carga de trabajo y los tipos de recursos, hay un cuadro titulado “Analizar continuamente”. Luego, el recuadro dice: “Monitoree de forma automática y continua las cargas de trabajo y los recursos de AWS para detectar posibles amenazas a gran escala”.

La cuarta sección tiene una ilustración que representa un punto de mira, con un ícono de alerta o advertencia. En esta sección se describe cómo GuardDuty detecta las amenazas de forma inteligente y se indica que “GuardDuty utiliza el machine learning, la detección de anomalías, el análisis de malware y la inteligencia de amenazas integrada para identificar y priorizar las posibles amenazas”.



ATAQUES DE DENEGACIÓN DE SERVICIO

Un ataque de denegación de servicio (DoS) es un intento deliberado de hacer que un sitio web o una aplicación no esté disponible para los usuarios.

Por ejemplo, un atacante podría inundar un sitio web o una aplicación con un tráfico de red excesivo hasta que el sitio web o la aplicación objetivo se sobrecarguen y ya no puedan responder. Si el sitio web o la aplicación dejan de estar disponibles, se deniega el servicio a los usuarios que intentan realizar solicitudes legítimas.

Los clientes pueden llamar a la cafetería para hacer sus pedidos. Después de contestar cada llamada, un cajero toma el pedido y se lo entrega al barista. Sin embargo, imagine que un bromista llama varias veces para realizar pedidos, pero nunca recoge las bebidas. Esto hace que el cajero no esté disponible para atender las llamadas de otros clientes.
La cafetería puede intentar detener las solicitudes falsas bloqueando el número de teléfono que usa el bromista. En esa situación, las acciones del bromista son similares a las de un ataque de denegación de servicio.

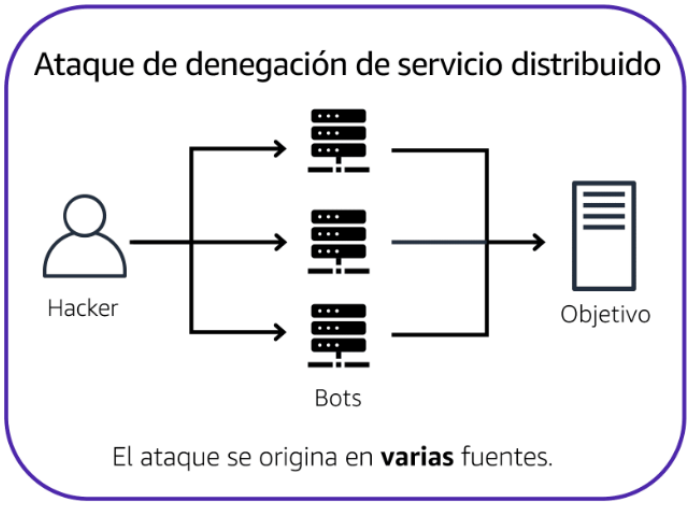
El objetivo de un ataque de denegación de servicio es apagar la capacidad de funcionamiento de la aplicación saturando el sistema hasta el punto de que ya no pueda funcionar.

ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDOS

D-D-o-S, DDoS, son las siglas en inglés para denegación de servicio distribuido. Es un ataque a la infraestructura de su empresa.

Ahora, supongamos que el bromista ha conseguido la ayuda de amigos. El bromista y sus amigos llaman repetidamente a la cafetería con solicitudes para realizar pedidos, a pesar de que no tengan la intención de recogerlos. Estas solicitudes vienen de diferentes números de teléfono, y es imposible que la cafetería los bloquee todos. Además, la afluencia de llamadas ha dificultado cada vez más que los clientes puedan realizar sus llamadas. Eso es similar a un ataque de denegación de servicio distribuido.

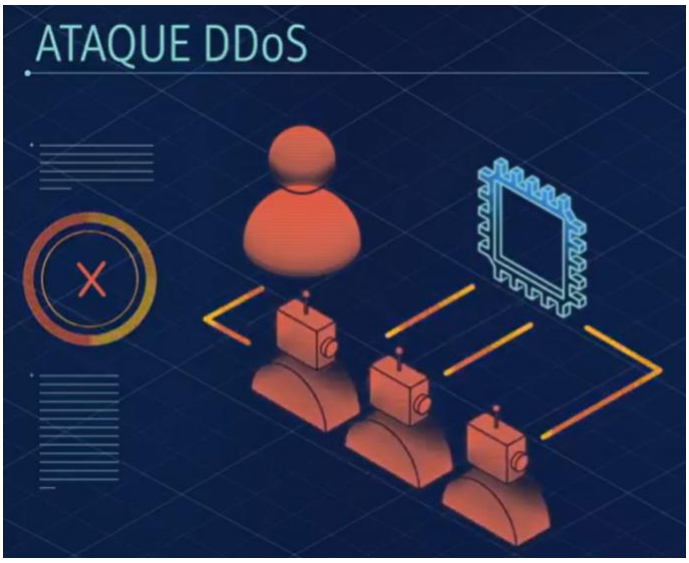
En un ataque de denegación de servicio distribuido (DDoS), se utilizan varias fuentes para iniciar un ataque cuyo objetivo es hacer que un sitio web o una aplicación no estén disponibles. Esto puede provenir de un grupo de atacantes o incluso de un solo atacante. El único atacante puede utilizar varios equipos infectados (también conocidos como “bots”) para enviar tráfico excesivo a un sitio web o una aplicación.



En operaciones normales, tu aplicación recibe solicitudes de clientes y devuelve resultados.

En un ataque de denegación de servicios, el actor malicioso intenta abrumar la capacidad de tu aplicación, básicamente para denegar sus servicios a cualquiera que intente consumirlos.

Pero una sola máquina que ataca a tu aplicación no tiene esperanza de realmente atacar fuertemente por sí misma, por lo que busca apoyo en la parte distribuida, lo cual es que el ataque aprovecha otras máquinas en Internet para atacar tu infraestructura sin tu saberlo. El actor malicioso crea un ejército de bots zombies sin cerebro que atacan a tu empresa. La clave para un ataque potente, es que el comando de asalto haga la menor cantidad de trabajo posible y que la víctima objetivo reciba como resultado una carga insoportable de trabajo que deba procesar.



Veamos algunos ejemplos de ataques específicos:

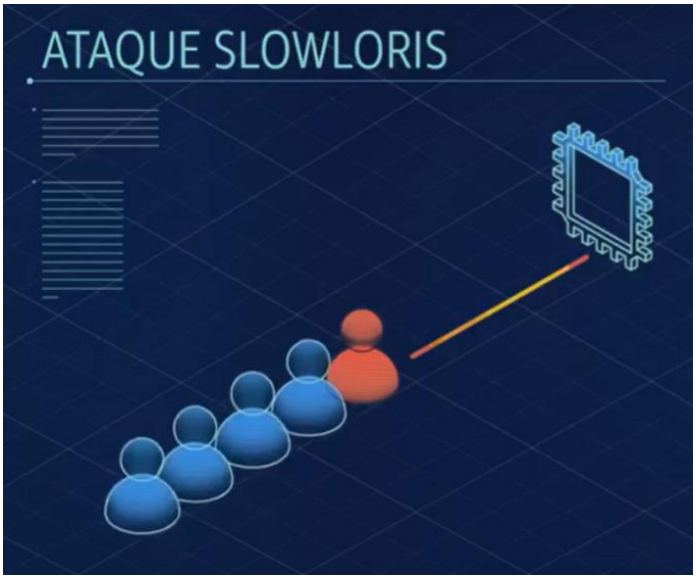
La inundación UDP se basa en las partes útiles de internet, como por ejemplo el Servicio Meteorológico Nacional. Ahora, cualquiera puede enviar una pequeña solicitud al Servicio Meteorológico y preguntar "Cuál es el estado del tiempo" y a cambio, la flota de máquinas del Servicio Meteorológico enviará una gran cantidad de telemetría meteorológica, pronósticos, actualizaciones, muchas cosas.

Así que el ataque aquí es sencillo. El actor malicioso envía una simple solicitud, ¿cuál es el estado del tiempo? Pero da una dirección de respuesta falsa en la solicitud, tu dirección de respuesta. Entonces ahora el Servicio Meteorológico inunda felizmente tu servidor con megabytes de pronósticos de lluvia y tu sistema podría paralizarse, simplemente ordenando la información que nunca quiso tener en primer lugar.

Eso es un ejemplo de media docena de ataques de fuerza bruta de bajo nivel, todos diseñados para agotar tu red.

Algunos ataques son mucho más sofisticados, como los ataques de nivel HTTP, que parecen clientes normales que piden cosas normales, como búsquedas de productos complicados una y otra vez, todas provenientes de un ejército de máquinas bot similares a zombies. Piden tanta atención que los clientes habituales no pueden entrar.

Incluso intentan trucos horribles como el ataque Slowloris. Imagínense en la fila de la cafetería cuando alguien frente a usted tarda siete minutos en pedir lo que sea que esté pidiendo y usted no puede pedir hasta que termine y salga de su camino. Bueno, el ataque Slowloris es exactamente lo mismo. En lugar de una conexión normal, me gustaría hacer un pedido, el atacante pretende tener una conexión terriblemente lenta. Mientras tanto, sus servidores de producción están parados esperando que el cliente termine su solicitud para que pueda salir y devolver el resultado. Pero hasta que obtengan el paquete completo, no pueden pasar al siguiente subproceso, el próximo cliente. Unos pocos atacantes Slowloris pueden agotar la capacidad de todo su front end con casi ningún esfuerzo.



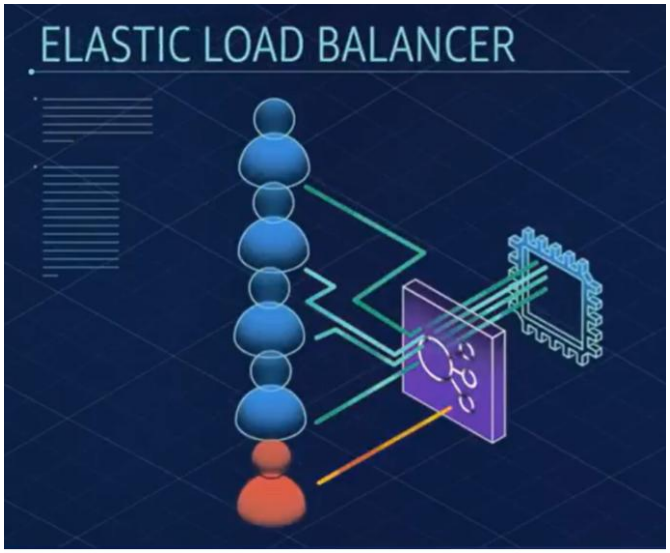
Ahora es momento de hablar de cómo detener estos ataques en frío y la solución ya la conocemos, todo lo que hemos estado hablando durante todo este curso no es solo una buena arquitectura, sino que también ayuda a resolver casi todas las alternativas de ataques de denegación de servicio sin esfuerzo ni costo adicional.

Primer ataque, los ataques de red de bajo nivel, como las inundaciones UDP. Solución, grupos de seguridad. Los grupos de seguridad solo permiten el tráfico de solicitudes adecuado. Cosas como los informes meteorológicos usan un protocolo completamente diferente que los que usan sus clientes. No está en la lista, no puede hablar con el servidor.

Además, los grupos de seguridad operan a nivel de red de AWS, no a nivel de instancia de EC2, como lo podría hacer un firewall de sistema operativo. Ataques masivos como inundaciones UDP o los ataques de reflexión implemente se ignoran por la escala de toda la capacidad de las regiones de AWS, no la capacidad individual de EC2. Este es un caso donde nuestro tamaño es una gran ventaja en su protección.

No diría que es imposible abrumar a AWS, pero la escala que tomaría sería demasiado cara para estos actores maliciosos.

¿Ataques Slowloris? Tenemos AWS Elastic Load Balancer. Debido a que ELB maneja primero la solicitud de tráfico http y entonces espera hasta que esté todo el mensaje, no importa cuán rápido o lento se complete antes de enviarlo al servidor web front end.
Es decir, claro, puede intentar abrumarlo, pero ¿recuerda cómo ELB es escalable y cómo se ejecuta a nivel regional? Para abrumar a ELB, tendría que abrumar una vez más a toda la región de AWS. Teóricamente no es imposible, pero es demasiado caro para que alguien lo haga.



Para los ataques más agudos y sofisticados, AWS también ofrece herramientas de defensa especializadas llamadas AWS Shield con AWS WAF. AWS WAF utiliza un firewall de aplicaciones web para filtrar el tráfico entrante para las firmas de los actores maliciosos. Tiene amplias capacidades de machine learning y puede reconocer nuevas amenazas a medida que evolucionan y puede ayudar de forma proactiva a defender su sistema contra una lista cada vez mayor de vectores destructivos.

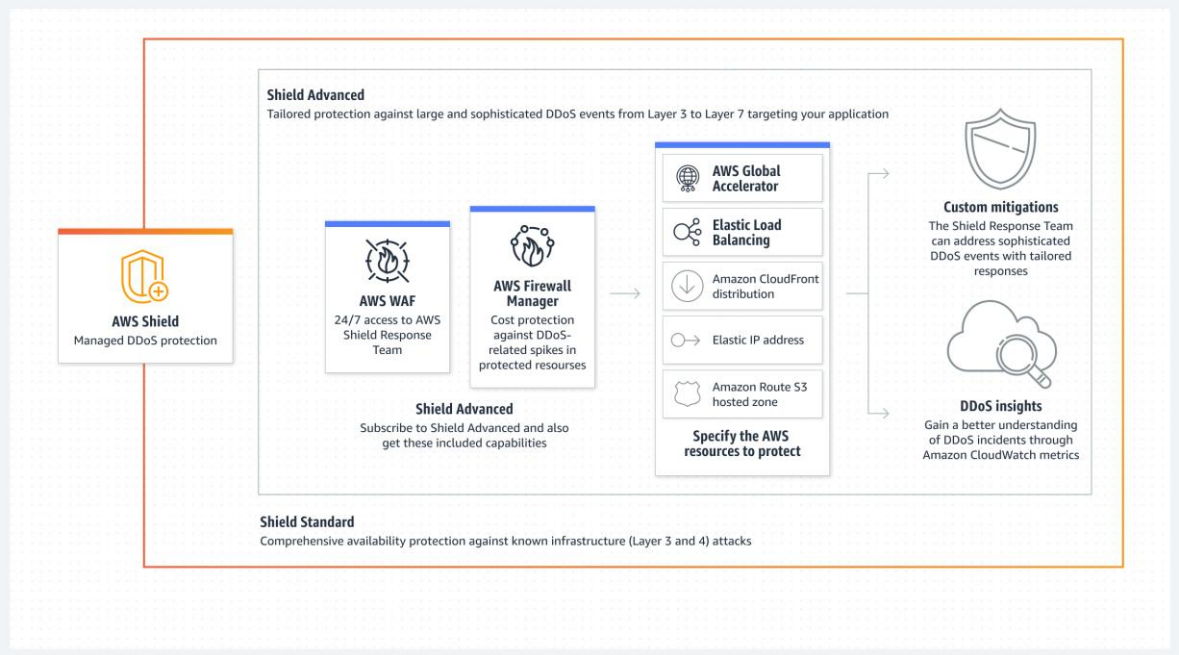
AWS SHIELD

Para ayudar a minimizar el efecto de los ataques DoS y DDoS en las aplicaciones, puede utilizar AWS Shield.

AWS Shield es un servicio de protección administrado contra ataques de denegación de servicio distribuidos (DDoS) que protege las aplicaciones ejecutadas en AWS. Proporciona una detección dinámica y mitigaciones en línea automáticas que minimizan el tiempo de inactividad y la latencia de la aplicación, por lo que no es necesario disponer de AWS Support para beneficiarse de la protección contra DDoS.

AWS Shield ofrece dos niveles de protección: Standard y Advanced.
AWS Shield Standard se habilita automáticamente para todos los clientes de AWS sin costo adicional.
AWS Shield Advanced es un servicio de pago opcional que ofrece protecciones adicionales ante los ataques más grandes y sofisticados para las aplicaciones que se ejecutan en Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator y Route 53.

FUNCIONAMIENTO DE AWS SHIELD



AWS SHIELD STANDARD

AWS Shield Standard protege a todos los clientes de AWS sin costo y de forma automática. Protege sus recursos de AWS de los tipos de ataques DDoS más comunes y frecuentes.

A medida que el tráfico de red entra en sus aplicaciones, AWS Shield Standard utiliza diversas técnicas de análisis para detectar el tráfico malicioso en tiempo real y mitigarlo de manera automática.

Todos los clientes de AWS se benefician de la protección automática de AWS Shield Standard sin cargo adicional. AWS Shield Standard ofrece protección ante los ataques DDoS más comunes, que normalmente ocurren en la capa de red y transporte, y que están dirigidos a su aplicación o sitio web. Si utiliza AWS Shield Standard con Amazon CloudFront y Amazon Route 53, recibirá protección de disponibilidad integral contra todos los ataques conocidos a la infraestructura (capa 3 y 4).

CARACTERÍSTICAS AWS SHIELD STANDARD

Protección frente ataques DDoS de límite estático para los servicios de AWS subyacentes: AWS Shield Standard proporciona monitoreo del flujo de red de funcionamiento continuo que inspecciona el tráfico entrante en los servicios de AWS y aplica una combinación de firmas del tráfico, algoritmos de anomalías y otras técnicas de análisis para detectar el tráfico malicioso en tiempo real. Shield Standard establece límites estáticos para cada tipo de recurso de AWS, pero no proporciona ninguna protección personalizada para sus aplicaciones.

Mitigación de ataques en línea: AWS Shield Standard cuenta con técnicas de mitigación automatizadas integradas, lo que aporta a los servicios subyacentes de AWS protección contra los ataques más comunes que suelen ocurrir en la infraestructura. Las mitigaciones automáticas se implementan en línea para proteger los servicios de AWS y no afectar la latencia. Shield Standard utiliza técnicas como el filtrado de paquetes determinista y la configuración de tráfico basada en prioridades, para mitigar automáticamente ataques a la capa de red básica.

AWS SHIELD ADVANCED

AWS Shield Advanced es un servicio pago que proporciona diagnósticos detallados de ataques y la capacidad de detectar y mitigar ataques DDoS sofisticados.

También se integra a otros servicios, como Amazon CloudFront, Amazon Route 53 y Elastic Load Balancing. Además, puede integrar AWS Shield con AWS WAF escribiendo reglas personalizadas para mitigar los ataques DDoS complejos.

Si desea un nivel de protección superior contra ataques dirigidos a sus aplicaciones que se ejecutan en recursos de Amazon Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator y Amazon Route 53, puede suscribirse a AWS Shield Advanced. Además de las protecciones de la capa de transporte y red que Standard incluye, Shield Advanced proporciona detección y mitigación adicionales contra ataques DDoS sofisticados y a gran escala, visibilidad de los ataques casi en tiempo real e integración con AWS WAF, un firewall para aplicaciones web. AWS Shield Advanced también le proporciona acceso las 24 horas del día, los 7 días de la semana al equipo de respuesta de AWS (DRT) y protección contra incrementos en los cargos de EC2, ELB, CloudFront, Global Accelerator y Route 53 relacionados con ataques DDoS.

CARACTERÍSTICAS AWS SHIELD ADVANCED

Detección personalizada basada en los patrones de tráfico de la aplicación: AWS Shield Advanced proporciona detección personalizada basada en los patrones de tráfico de la dirección IP elástica, Elastic Load Balancing (ELB), CloudFront, Global Accelerator y recursos de Route 53. Mediante técnicas de monitoreo específicas de recursos y región adicional, Shield Advanced detecta y le informa de ataques DDoS de menor escala. Shield Advanced crea una base de referencia del tráfico de sus recursos con la que detecta también ataques en la capa de la aplicación, como inundaciones HTTP o de consultas DNS, e identifica las anomalías.

Detección basada en el estado: AWS Shield Advanced utiliza el estado de sus aplicaciones para mejorar la respuesta y la precisión para la detección y la mitigación de los ataques. Puede definir una verificación de estado en Route 53 y asociarla con un recurso que esté protegido por Shield Advanced a través de la consola o API. Esto permite que Shield Advanced detecte ataques que afectan el estado de la aplicación con mayor velocidad y en límites de tráfico inferiores, lo que mejora la resiliencia ante DDoS de la aplicación y evita notificaciones falsas positivas.

Mitigación avanzada de ataques: AWS Shield Advanced ofrece un nivel de mitigación automática más sofisticado para los ataques dirigidos a las aplicaciones que se ejecutan en recursos protegidos de Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), CloudFront, Global Accelerator y Route 53. Mediante técnicas avanzadas de enrutamiento, Shield Advanced implementa automáticamente capacidad de mitigación adicional para proteger la aplicación ante ataques DDoS.

Mitigación automática de ataques DDoS en la capa de aplicaciones: AWS Shield Advanced puede proteger automáticamente las aplicaciones web a través de la mitigación de los eventos DDoS de la capa de aplicación (Capa 7) sin que sea necesaria una intervención manual por su parte o por parte de AWS SRT. Shield Advanced puede crear reglas WAF en su WebACL para mitigar automáticamente un ataque o usted puede activarlas en modo solo recuento. Esto le permite responder rápidamente a eventos DDoS para evitar la inactividad de una aplicación causada por un ataque DDoS en la capa de la aplicación.

Respuesta proactiva a eventos: AWS Shield Advanced permite la interacción proactiva del equipo de respuesta de Shield SRT cuando se detecta un evento DDoS. Cuando activa la interacción proactiva, el SRT le contactará directamente si una comprobación de estado de Route 53 asociada al recurso protegido muestra un estado anómalo durante un evento de DDoS. Esto le permite interactuar con los expertos con mayor rapidez cuando la disponibilidad de la aplicación se ve afectada por un ataque sospechoso. Puede recibir interacción proactiva para eventos de capa de transporte y de capa de red en direcciones IP elásticas y aceleradores de Global Accelerator y para los ataques de la capa de la aplicación en distribuciones de CloudFront y balanceadores de carga de aplicaciones.

Grupos de protección: AWS Shield Advanced permite agrupar recursos en grupos de protección, lo que representa una forma de autoservicio de personalizar el alcance de la detección y la mitigación para la aplicación al gestionar varios recursos como una sola unidad. La agrupación de recursos mejora la precisión de la detección, reduce los falsos positivos, facilita la protección automática de recursos recién creados y acelera el tiempo para mitigar ataques en contra de varios recursos. Por ejemplo, si una aplicación está compuesta por cuatro distribuciones de CloudFront, puede agruparlas en un grupo de protección para recibir detección y protección para el conjunto de recursos como un todo.

Visibilidad y notificación de ataques: AWS Shield Advanced le ofrece una visibilidad completa de los ataques DDoS con notificación casi en tiempo real mediante Amazon CloudWatch y un diagnóstico detallado en la consola de AWS WAF y AWS Shield o las API. También puede ver un resumen de ataques previos desde la consola.

Protección de costos en ataques DDoS: AWS Shield Advanced incorpora protección de costos en DDoS, una característica que evita los cargos de escalado generados por picos de uso relacionados con DDoS en recursos de Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), CloudFront, Global Accelerator y Route 53. Si cualquiera de estos recursos protegidos se escala como respuesta a un ataque DDoS, puede solicitar créditos del servicio Shield Advanced a través del canal habitual de AWS Support.

Disponibilidad global: AWS Shield Advanced está disponible a nivel mundial en todas las ubicaciones de borde de CloudFront, Global Accelerator y Route 53. Puede proteger sus

aplicaciones web hospedadas en cualquier lugar del mundo mediante la implementación de CloudFront por delante de su aplicación.

CONCLUSIONES

- AWS WAF es un firewall para aplicaciones web que le permite supervisar las solicitudes de red que entran en sus aplicaciones web.

- Amazon Inspector descubre automáticamente cargas de trabajo, como las instancias de Amazon EC2, contenedores y funciones de Lambda, y los escanea para encontrar vulnerabilidades de software y exposición involuntaria de red.

- Amazon GuardDuty es un servicio de detección de amenazas que supervisa de manera continua sus cargas de trabajo y cuentas de AWS para detectar actividades maliciosas y envía hallazgos detallados de seguridad para su visibilidad y corrección.

- Un sistema que está bien diseñado ya tiene defensa contra la mayoría de los ataques y con AWS Shield Advanced, puede convertir a AWS en su socio frente a los ataques de denegación de servicio DDoS.

- AWS Shield es un servicio de protección administrado que protege a aplicaciones web que se ejecutan en AWS contra ataques de denegación distribuida de servicio (DDoS).