Soluciones ANTI DDoS existentes en el mercado

Autor: Graciela Martínez
Coordinación y revisión: Área de Comunicaciones
Edición: Área de Comunicaciones
Área: Área de Tecnología

Septiembre 2024

lacnic
www.lacnic.net

En el mercado existen diferentes soluciones anti-DDoS ofrecidas por proveedores y empresas. A continuación listamos una serie de esas herramientas disponibles.

Soluciones comerciales

La elección de la mejor solución para cada organización depende de diversos factores, como el presupuesto, el nivel de protección requerido y la infraestructura existente.

Cloudflare [1]:

Descripción: Cloudflare es una de las soluciones más populares para la mitigación de DDoS. Ofrece protección a nivel de red y aplicación, con una infraestructura global que dispersa el tráfico malicioso.

Características: Protección DDoS, CDN (Content Delivery Network),

WAF (Web Application Firewall), y DNS seguro.

Ventajas: Fácil de implementar, escalabilidad global, análisis en tiempo real, y coste efectivo para sitios de todos los tamaños.

Akamai:

Descripción: Esta empresa es conocida por su red de entrega de contenido aunque también ofrece robustas capacidades de mitigación de DDoS a través de su servicio Kona Site Defender.

Características: Protección a nivel de red y aplicación, distribución de tráfico a través de una red global, y herramientas avanzadas de análisis y monitoreo.

Ventajas: Amplia red de distribución, soporte para grandes volúmenes de tráfico, y alta fiabilidad.

https://www.akamai.com/

Amazon Web Services (AWS) Shield:

Descripción: AWS Shield es una solución de mitigación de DDoS integrada en la infraestructura de AWS. Disponible en dos niveles: Standard y Advanced.

Características: Protección contra ataques a nivel de red y aplicación, integración con otros servicios de AWS, y capacidades avanzadas de monitoreo y respuesta.

Ventajas: Integración nativa con AWS, protección automática y escalabilidad, opciones de informes detallados y soporte adicional con Shield Advanced. https://aws.amazon.com/es/shield/

Google Cloud Armor:

Descripción: Google Cloud Armor proporciona protección DDoS para aplicaciones alojadas en Google Cloud, utilizando la infraestructura global de Google.

Características: Políticas de seguridad basadas en reglas, mitigación de ataques a nivel de red y aplicación, y protección contra ataques volumétricos y de aplicación.

Ventajas: Integración nativa con Google Cloud, fácil de configurar y gestionar, y escalabilidad global.

https://cloud.google.com/armor/docs?hl=es-419

Imperva Incapsula:

Descripción: Imperva Incapsula ofrece protección DDoS para aplicaciones web y servicios basados en la nube.

Características: Mitigación de DDoS a nivel de red y aplicación, WAF, protección contra bots, y capacidades de monitoreo y análisis en tiempo real.

Ventajas: Protección integral contra diversos tipos de ataques, fácil implementación, y opciones avanzadas de configuración y personalización. https://www.imperva.com/

Arbor Networks (NETSCOUT):

Descripción: Arbor Networks es una solución de seguridad que se enfoca en la protección contra DDoS, utilizada tanto por proveedores de servicios como por empresas.

Características: Detección y mitigación de ataques en tiempo real, inteligencia basada en la red global, y análisis detallados.

Ventajas: Amplia experiencia y reputación en mitigación de DDoS, soporte para grandes infraestructuras, y herramientas avanzadas de

análisis.

https://www.netscout.com/solutions/service-provider-ddos-protection

F5 Networks:

Descripción: F5 Networks ofrece soluciones de mitigación de DDoS que protegen aplicaciones y redes mediante su sistema BIG-IP.

Características: Mitigación de DDoS a nivel de red y aplicación, WAF, balanceo de carga, y herramientas de monitoreo y análisis.

Ventajas: Enfoque híbrido de hardware y software, alta fiabilidad, y capacidad para manejar grandes volúmenes de tráfico.

https://www.f5.com/es_es

Las herramientas mencionadas son ampliamente utilizadas debido a su eficacia y capacidad para manejar grandes volúmenes de tráfico, así como su facilidad de integración y uso.

Las organizaciones pueden consultar a proveedores de soluciones de seguridad, así como también a sus ISPs que muchas veces ofrecen el servicio de mitigación de DDOS como un valor agregado a su servicio de conectividad.

Soluciones de código abierto

También existen herramientas open source (código abierto) con el mismo objetivo, mitigación de ataques de DDOS. Entre ellas vale la pena mencionar:

Haproxyr:

Descripción: HAProxy es un proxy inverso gratuito, muy rápido y confiable que ofrece alta disponibilidad, equilibrio de carga y proxy para aplicaciones basadas en TCP y HTTP.

Características: Es un balanceador de carga y proxy que puede ayudar a distribuir el tráfico de manera equitativa entre varios servidores.

Ventajas: lo que puede ser útil para manejar grandes volúmenes de tráfico durante un ataque DDoS

https://github.com/haproxy

Gatekeeper:

Descripción: Gatekeeper es el primer sistema de protección DDoS de código abierto, utilizado por operadores de redes de instituciones, proveedores de servicios y contenidos, redes empresariales, etc.

Características: Está diseñado para escalar a cualquier ancho de banda máximo. Su arquitectura está geográficamente distribuida mientras que la política de red que describe todas las decisiones que deben aplicarse al tráfico entrante está centralizada.

Ventajas: Su posibilidad de escalar a cualquier ancho de banda hace que pueda resistir ataques DDoS actuales y futuros. Y su política centralizada permite a los operadores de red aprovechar algoritmos distribuidos que no serían viables con una latencia muy alta (por ejemplo, bases de datos distribuidas) y combatir múltiples ataques DDoS multivectoriales a la vez.

https://github.com/AltraMayor/gatekeeper

FastNetMon:

Descripción: FastNetMon: un detector/sensor DDoS de alto rendimiento construido sobre múltiples motores de captura de paquetes: NetFlow, IPFIX, sFlow, AF_PACKET.

Características: Detecta hosts en la red que envían o reciben grandes volúmenes de tráfico, paquetes/bytes/flujos por segundo y realiza una acción configurable para manejar ese evento. Estas acciones configurables incluyen notificarle, llamar al script o realizar anuncios BGP.

Ventajas: Cuenta con múltiples ventajas como: detectar DoS/DDoS en tan solo 1-2 segundos, escalar hasta terabits en un solo servidor

(sFlow, Netflow, IPFIX) o hasta 40G + en modo espejo, permite configurar umbrales por subred, posee notificaciones por correo electrónico sobre ataques detectados y cuenta con soporte completo para IPv6.

https://github.com/pavel-odintsov/fastnetmon/

Finalmente debemos mencionar que algunos ISPs o proveedores de seguridad también ofrecen a sus clientes servicios de depuración de DDoS. Los mismos consisten en enviar a la organización el tráfico limpio después de absorber el ataque, porque se supone que tienen la inteligencia para detectar y descartar la mayoría de los tipos de ataques DDoS. Estos servicios deben complementarse con soluciones DNS y BGP para que sean eficaces.