EVALUACIÓN Y PROTECCIÓN DDOS

Servicios Administrados de Ciber Seguridad **DDoS**

EVALUACIÓN Y PROTECCIÓN DE ATAQUES DDoS

En Shield Force ofrecemos dos servicios para apoyar a su estrategia de protección contra ataques de negación de servicios distribuidos (DDoS). Por un lado contamos con nuestro aliado **NimbusDDoS** y por el otro con **Cloudflare**. Estos servicios los ofrecemos porque entendemos el problema y hemos aprendido que es importante protegerse de dichas amenazas pero también es fundamental entender como se puede evaluar la infraestructura de nuestros clientes para llevarlos en un camino donde efectivamente se conozca que pasaría en un escenario de ataque.

Con **NimbusDDoS** podemos realizar simulaciones de ataques DDoS controlados, usando una plataforma de servicios de clase mundial acompañando a nuestros clientes en el proceso, desde la planeación, hasta la entrega de resultados de dicha simulación.

Con **Cloudflare** podemos implementar una estrategia de protección contra ataques de negación de servicios, utilizando una plataforma distribuida, que protegerá tu infraestructura de TI de manera efectiva.

El problema

Para la protección contra ataques DDoS es fundamental contar con mínimo dos componentes, uno es la evaluación de las capacidades mediante la simulación de ataques y por el otro lado usar una plataforma distribuida de protección contra ataques DDoS.

No uses "booters" o "stressers", donde no hay control del ancho de banda, al ejecutar una simulación, tampoco uses plataformas anti-DDoS "appliance on premise", que tienen su limitante en el ancho de banda que soportan sus interfases de red.

Ventajas de integrar ambos servicios:

Sobre **NimbusDDoS**

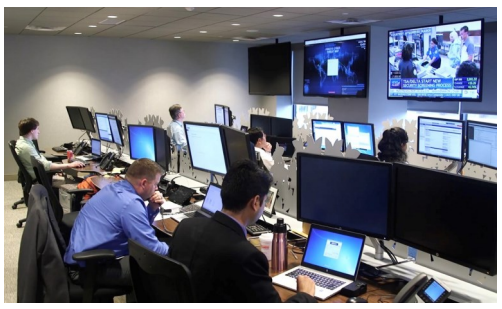
- Simulación de ataques de manera legal y controlados
- Evaluación de plataforma de protección, mecanismos de control y procesos de respuesta.
- Generación de Recomendaciones de mejora

Sobre **Cloudflare**:

- No dependencia de la capacidad de ancho de banda de interfases de red de appliances on Premise
- Protección de ataques DDoS volumétricos
- Protección contra ataques a nivel de aplicación

Servicio Administrado

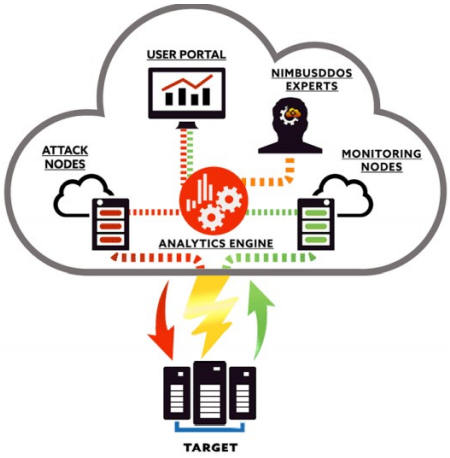
Desde nuestro "V-CSOC" Centro de Operaciones de Ciber Seguridad Virtual, podemos monitorear y administrar los servicios de **Cloudflare** en atendiendo los requerimientos y respondiendo ante cualquier incidente relacionado con la plataforma.



Simulación de Ataques de DDoS

Realizamos pruebas de ataques DDoS a fin de encontrar **debilidades** en su plataforma ejecutando **la simulación** de un ataque distribuido de negación de servicio. Con la plataforma en la nube se pueden realizar **pruebas y simulaciones** de ataques reales de una manera **legal y controlada.** Validamos los tiempos de respuesta de sus mecanismos de protección, así como sus planes de respuesta a incidentes y medidas de contingencia, identificando huecos, errores o fallas y localizar cuellos de botella.

Con nuestros servicios y usando la plataforma es posible ejecutar "juegos de guerra" o ejercicios "red teaming" emulando un incidente real usando técnicas que pueden usar los atacantes.



A diferencia del uso de "booters" o "stressers" que hacen uso de mecanismos ilegales y no autorizados (como una botnet), la plataforma de **NimbusDDoS** tiene **el control total de la simulación**, al grado de que si es necesario parar la simulación, esto se realiza de inmediato (usando el "Emergency Shutdown Switch"), y se cuentan con mecanismos (portal) de monitoreo y supervisión donde se ven las métricas en tiempo real y hay un control granular del tráfico que se simula y es enviado a los objetivos de evaluación; todo lo anterior con el acompañamiento de nuestros especialistas y expertos del fabricante.

Nuestro proceso es muy simple, revisamos los objetivos, se planea la simulación, se crea el escenario de prueba, se ejecuta la simulación acompañada y supervisada y entregamos los resultados de la simulación con recomendaciones.

Protección de Ataques DDoS

Cloudflare DDoS asegura sitios web, aplicaciones y el perímetro de la red de su infraestructura asegurando que el rendimiento y el tráfico legitimo no sea comprometido. Así mismo **Cloudflare WAF** (Web Application Firewall) trabaja en conjunto con la protección DDoS y el WAF protege las aplicaciones críticas de ataques maliciosos sin cambios a su infraestructura actual, mediante la construcción de reglas que permiten proteger de peticiones maliciosas que son bloqueadas y registradas para evaluación posterior. El WAF protege ataques de SQLi, XSS usando un conjunto de reglas OWASP.

Cloudflare Bot Management, protege su red de ataques de bots maliciosos en tiempo real usando métodos de detección como Análisis de Comportamiento para detectar anomalías, Aprendizaje de Máquina para crear un bot score y uso de "huellas digitales" para clasificar los bots.

Cloudflare Rate Limiting, protege contra intentos de ataques de fuerza bruta, así como otros tipos de ataque a nivel de capa de aplicación. Esta funcionalidad permite configurar umbrales, definir respuestas que pueden complementar el WAF y Bot Management para proteger de los ataques DDoS.

Es importante comentar, que este es un resumen de las capacidades de Cloudflare, hay más servicios que no se integran en este documento, para mas información contáctanos y podemos presentarte el portafolio completo de Cloudflare.