Buenas prácticas y técnicas para mitigar ataques de DdoS

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

Septiembre 2024

lacnic
www.lacnic.net

Los ataques DDoS se producen por la explotación de vulnerabilidades en las distintas capas del Stack TCP/IP o por el abuso de la capacidad de la red para manejar grandes volúmenes de tráfico. Por ello es importante implementar una protección integral en la organización. Para tal fin compartimos con la comunidad distintas acciones que pueden complementar una solución DDoS y proteger servidores y redes.

En esta primera parte se describen las principales acciones que pueden llevarse a cabo desde la organización, con el fin de prevenir ataques de DDOS (bajar su probabilidad de ocurrencia y/o minimizar su impacto).

Respecto a la configuración de la red y servicios para reducir la probabilidad de ataques de DDOS y fortalecer la infraestructura frente a los mismos, es recomendable implementar (si es factible):

1. **Redundancia y Distribución de Carga**:

   Utilizar CDNs para proteger sitios WEB. Las CDN son redes distribuidas de servidores proxy que permiten reducir la latencia ya que almacenan contenido en caché y “acercan” el mismo a los usuarios finales. De esta forma los ataques de DDoS se mitigarán más cerca de la fuente sin impactar el rendimiento.

2. **Rate Limiting**:

   Limitar la cantidad de solicitudes que un usuario puede hacer en un período de tiempo específico para prevenir el abuso.

3. **Filtrado de Tráfico**:

   Configurar firewalls y sistemas de detección de intrusiones (IDS) para filtrar tráfico malicioso basados en patrones y firmas conocidas así como utilizando aprendizaje automático.

4. **Anycast Routing**:

   Utilizar enrutamiento Anycast para distribuir el tráfico en múltiples ubicaciones, haciendo más difícil para los atacantes concentrar el ataque en un solo punto.

5. **Capacidad de Sobrecarga**:

   Asegurarse de que la infraestructura pueda manejar una cantidad significativa de tráfico adicional mediante el uso de servidores y ancho de banda adicional.

6. **Protección a Nivel de Protocolo**:

   Configurar correctamente los protocolos de red para mitigar vulnerabilidades que den lugar a ataques de amplificación y así minimizar su impacto

Respecto al monitoreo y detección resultan buenas prácticas contar con:

7. **Sistemas de Detección y Respuesta Temprana**:

   Implementar soluciones de monitoreo que detecten patrones de tráfico inusuales y respondan automáticamente a posibles ataques.

8. **Implementar mecanismos para:**

   - Detectar bots maliciosos y bloquear su tráfico sin interrumpir el de usuarios legítimos.
   - Implementar mecanismos que permitan diferenciar entre tráfico de ataque y tráfico legítimo.

   Si bien diferenciar tráfico de ataque de tráfico legítimo no es trivial, hay distintas herramientas, proyectos e iniciativas que pueden colaborar en identificar posibles patrones de tráfico no deseado.[https://csirt.lacnic.net/honeynet].

Técnicas de mitigación

En nuestra segunda parte compartimos algunas técnicas reactivas ante ataques de DDoS, que son útiles para mitigar la afectación o el impacto cuando ésto ocurre.

Cuando la organización es víctima de un ataque de DDOS el impacto de este se minimizará si:

1) La organización cuenta con herramientas que detectan y controlan los ataques de DDoS.

2) La organización tiene un plan de mitigación para este tipo de ataques. Dicho plan debe definir cómo proceder para: estar preparados, identificar el ataque, contener, remediar y recuperar. Para cada una de esas etapas se recomienda definir procedimientos relacionados a realizar:

   a **Preparación** • contactos y procedimientos • ISP y soporte especializado • configuraciones de red e infraestructura

   b **Identificación** • detección y alerta • análisis del ataque • identificación de la motivación • adquisición/refinamiento de la mitigación • rastreo

   c **Contención** • modificaciones de la red • control de entrega de contenido • control de tráfico

   d **Remediación** • priorización y bloqueo del ancho de banda • depuración del tráfico (traffic scrubbing) • sinkholing

   e **Recuperación** • verificación del estado normal • reversión (rollback)

   f **Lecciones aprendidas** • revisión del incidente y divulgación de información • aplicación de la ley.