Ataques DDoS en litespeed web server, cómo los maneja

Ataques DDoS en Litespeed web server, cómo los maneja. Hace unos días atrás en otro de nuestros blogs en español empezamos a reseñar algunas características de este tipo de servidores, tecnología que no solo ofrecemos en HostDime sino que los hemos probado en condiciones de **estrés y alto tráfico** con resultados estupendos.

Para entender a cabalidad esta nota sugiero leerlas, pues esta tecnología no es común que se use por físico desconocimiento por parte de los proveedores de Alojamiento web; los artículos previos fueron:

1. Prueba a nivel servidor Vps de Open Lite Speed, mediciones de velocidad
2. Litespeed vs Apache
3. Compresión Gzip en Litespeed web server

Regulación por Ip

Debido a su **arquitectura** impulsada por **eventos**, capaz de manejar todas las **conexiones con un solo proceso**, LiteSpeed recopila información rápidamente sobre la cantidad de conexiones o la cantidad de ancho de banda que usa una IP. Esto permite que el servidor imponga límites de manera eficiente.

Las aplicaciones basadas en procesos, como lo hace Apache, tienen problemas para afrontar este tipo de problemas porque deben recopilar información de muchas rutinas y subprocesos. Para cuando identifican una Ip a bloquear, ya es demasiado tarde.

Se detienen los ataques antes que invadan su servidor.

Escalabilidad

Al manejar mucho **más tráfico con menos recursos**, le permite sobrevivir a ataques muchos más grandes que las soluciones menos escalables. Cuando suceden ataques muy distribuidos, es capaz de aislar y bloquear a cada atacante.

Protección de renegociación SSL

Esta característica les permite a estos servidores **evitar sobrecargas** y congestiones innecesarias cada vez que sea precisa una conexión segura o https. Un servidor pequeño o con tecnología diferente, colapsa rápidamente.

Literalmente es capaz de **manejar mayor cantidad de peticiones** y además, limitar el número de veces que un cliente puede renegociar estos recursos.

¿Cómo configurarlo correctamente?

- **Limitando a lo usuarios o clientes**: Configuración-Servidor-configuraciones de seguridad-limitación de clientes. Allí hay varias opciones para el ancho de banda permitido y la velocidad de conexión por Ip remota.
- **Configurar la velocidad**, la compresión Gzip y la Broling respectivamente en el módulo respectivo.

- **Regulación del ancho de banda** para el tráfico saliente y entrante.
- **Regulación de la conexión**. Controlan conexiones concurrentes provenientes de una dirección Ip (de 4-10 conexiones resulta dentro de lo normal o aceptable).
- Puede usar el límite de conexión suave, el periodo de gracia y el periodo prohibido, para detectar y mitigar a los abusadores.

La configuración por defecto viene dada por:

- Peticiones estáticas 0
- Peticiones dinámicas 0
- Ancho de banda de salida 0
- Ancho de banda de entrada 0
- Conexión de límite suave 100.000
- Conexión de límite duro 150.000
- Periodo de Gracia 15 segundos
- Periodo de baneo 300 segundos

Una configuración idónea inicial pudiera ser:

- Peticiones estáticas / segundo 40
- Peticiones dinámicas / segundo 2
- Ancho de banda de salida (bytes / s) 0
- Ancho de banda de entrada (bytes / seg) 0
- Límite de conexión suave 15
- Límite de conexión dura 20
- Solicitud de bloqueo de bloque Sí
- Período de gracia (s) 15
- Período de exclusión (s) 60

¿Cual es el porqué de esta configuración recomendada? Una IP que ha establecido más de **20 conexiones** con el servidor web, o

ha establecido más de 15 conexiones de más de 15 segundos (el período de gracia), se trata como un DDoS-atacante. El servidor prohibirá la IP durante 60 segundos y registrará una entrada de registro en el archivo de registro de errores. Para excluir cualquier IP de los límites de aceleración del cliente (y eludir la detección de DDoS), agregue la IP con una 'T' final (también conocida como confiable) en Lista permitida (Consola WebAdmin> Servidor> Seguridad> Control de acceso).

Configuración máxima de solicitudes y respuestas

Se trata de fijar los valores como longitud de una url, la cantidad de solicitudes de un header, la cantidad de solicitudes máxima para un body, etc etc. Lograr estos valores ajustados, nos permiten determinar rápidamente a los atacantes y reducir el consumo de memoria de forma importante.

Establezca el tiempo de espera de conexión en alrededor de 30 segundos y el tiempo de espera en vivo en cerca de 15 segundos; la idea central es cerrar las conexiones muertas lo más pronto posible.

Aumente la configuración de conexión máxima

De 2.000-20.000, de 200 a 10.000 en SSL.

Y por supuesto el bloqueo manual de Ips sigue siendo funcional cuando se necesite.

¿Te ha gustado esta nota? ¿La compartes en tus redes sociales?

Leer también: Servidores web basados en procesos vs web server por eventos; Servidores para WordPress, Joomla, Magento, alto tráfico