PRÁCTICAS RECOMENDADAS

Diez pasos para combatir un ataque DDoS en tiempo real

Para los no iniciados, un ataque distribuido de denegación de servicio (distributed denial-of-service, DDoS) puede ser una experiencia estresante. Pero no se sienta pánico. Siga estos pasos para combatir exitosamente un ataque.

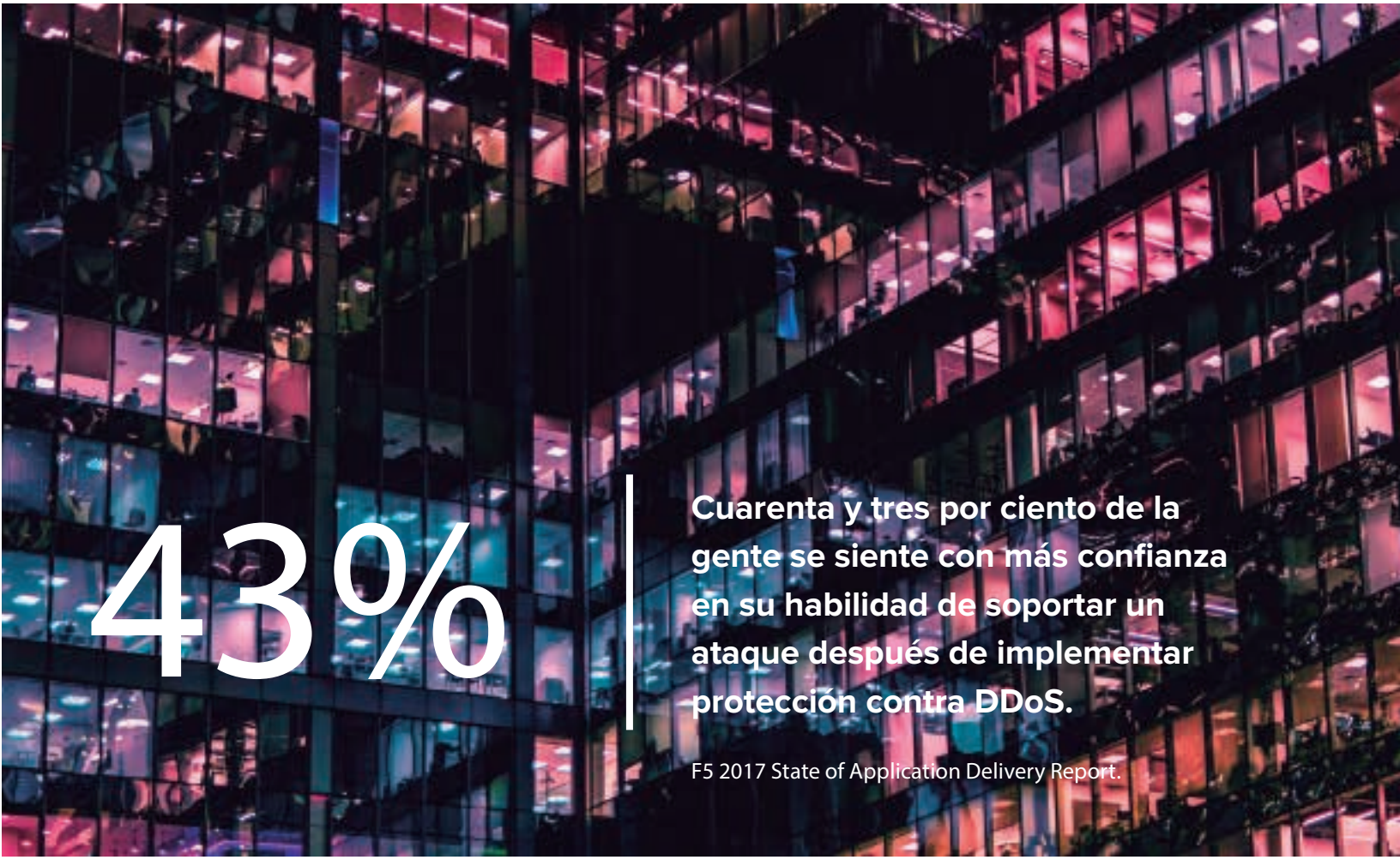
David Holmes
Senior Technical Marketing Manager, Security

Contenido

Introducción

Los ataques distribuidos de denegación de servicio (DDoS, en inglés) son una de las principales preocupaciones de muchas organizaciones hoy en día. Un ataque DDoS satura un sitio web, volviendo inoperables sus servicios, y evita que clientes legítimos puedan conectarse a él. Para los no iniciados, este tipo de ataques puede ser una experiencia estresante.

Los ataques DDoS usualmente están coordinados a través de un gran número de computadoras clientes (que pueden haber sido configuradas con ese propósito en mente). En muchas ocasiones, una computadora cliente puede haber sido infectada con un virus que le permite a un hacker controlar remotamente la computadora, haciéndola participar en el ataque.



Frecuencia de ataques de DDoS

Motivados tanto por razones financieras como políticas, los ataques DDoS se están volviendo más prevalentes. Aunque un primer ataque puede ocurrir de manera aleatoria, éstos ocurren frecuentemente cuando un atacante con conocimiento específico del alto valor de su servicio decide ponerlo fuera de línea. Esto puede causar pánico y provocar decisiones costosas, incluyendo el pago de un rescate, para priorizar y detener el ataque.

Un método objetivo de combate contra DDoS

Las organizaciones que han tenido que defenderse contra múltiples ataques DDoS entienden la importancia de tener un procedimiento metódico para asistirlos en su combate.

¿Cuál es su solución? Un plan de acción DDoS. Este documento puede ser la base para establecer un procedimiento que guíe al equipo operativo durante cualquier ataque DDoS, grande o pequeño, frecuente o infrecuente. Utilice las hojas de Referencia Rápida de F5 o cree uno propio. Complételo con anticipación para ayudarle a repeler un ataque DDoS.

Su modelo completado puede ser mantenido en su centro de datos y ser usado para documentación y mitigación en caso de ataque. Si no ha recopilado esta información previo a su primer ataque, hágalo a manera que la recolecta para prepararse mejor ante un futuro ataque.

Cumplimiento de regulaciones

Su organización puede estar sujeta a estatutos regulatorios que requieren un cierto nivel de presentación de informes en caso de ciberataques, filtraciones de seguridad, o ataques DDoS. Un registro de ataques puede serle de ayuda en esta situación dado que puede darle seguimiento y referirse a este registro posteriormente durante el proceso de presentación de informes.

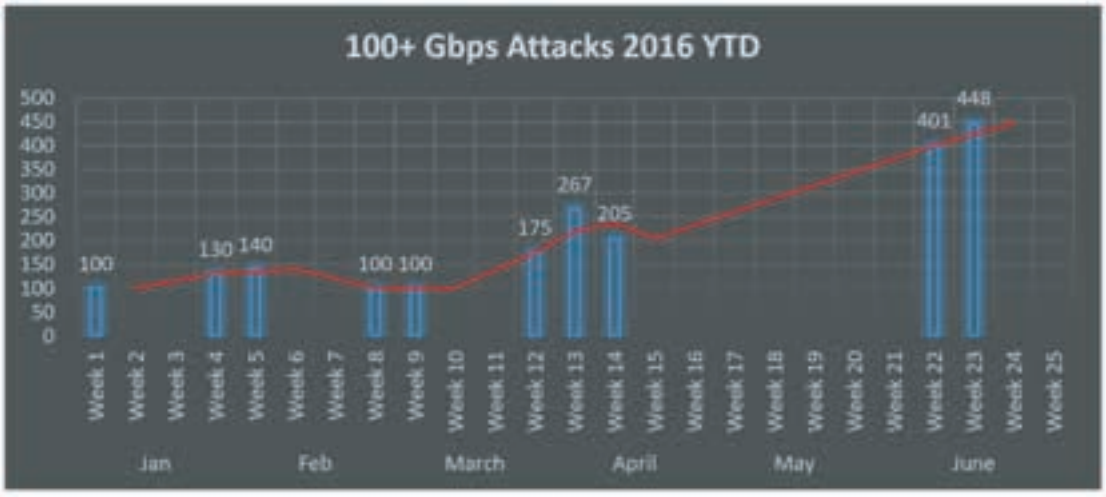


Figura1: Ancho de banda máximo de ataques en Gbps, 2016 hasta la fecha (no actualizado).

Preparándose para un ataque DDoS

Si usted tiene la fortuna de estar leyendo este documento antes de haber sido atacado, aquí le mostramos algunos pasos que puede tomar para hacer sus aplicaciones, redes y procesos resistentes ante ataques DDoS. Si se encuentra bajo ataque y necesita asistencia adicional, llame a alguno de los números gratuitos de F5 para comunicarse con expertos del Centro de Operaciones de Seguridad de F5 – disponible 24/7. Usando F5 Silverline, nuestro servicio basado en la nube de mitigación de DDoS, podemos ayudar a ponerlo nuevamente en línea.

Estudie una arquitectura resistente a DDoS

Después de haber llenado las hojas de referencia rápida en esta guía, obtenga el documento Prácticas Recomendadas para DDoS de F5 para que considere cómo alinear las defensas de su arquitectura de red.

F5 recomienda un enfoque multi nivel donde los ataques DDoS en las capas 3 y 4 sean mitigados al nivel de red con firewalls y bases de datos de reputación de IPs. Vea la figura 2.

- El nivel de aplicaciones está a cargo de funciones de seguridad de alto uso de CPU como terminación SSL y la funcionalidad del firewall para aplicaciones web.
- Para combatir DDoS, las organizaciones modernas necesitan de un nivel de depuración para DDoS. Estos servicios ofrecen depurar cientos de gigabytes por segundo y regresan tráfico “limpio” al centro de datos.
- DNS es manejado en la DMZ y protegido parcialmente por el nivel de red.

Este enfoque multi nivel puede:

- Frustrar inundaciones de conexiones TCP
- Sobreponerse al agotamiento de puertos SNAT
- Rechazar inundaciones SSL

Estas son solamente algunas de las prácticas y consideraciones recomendadas en el documento Prácticas Recomendadas para DDoS de F5.

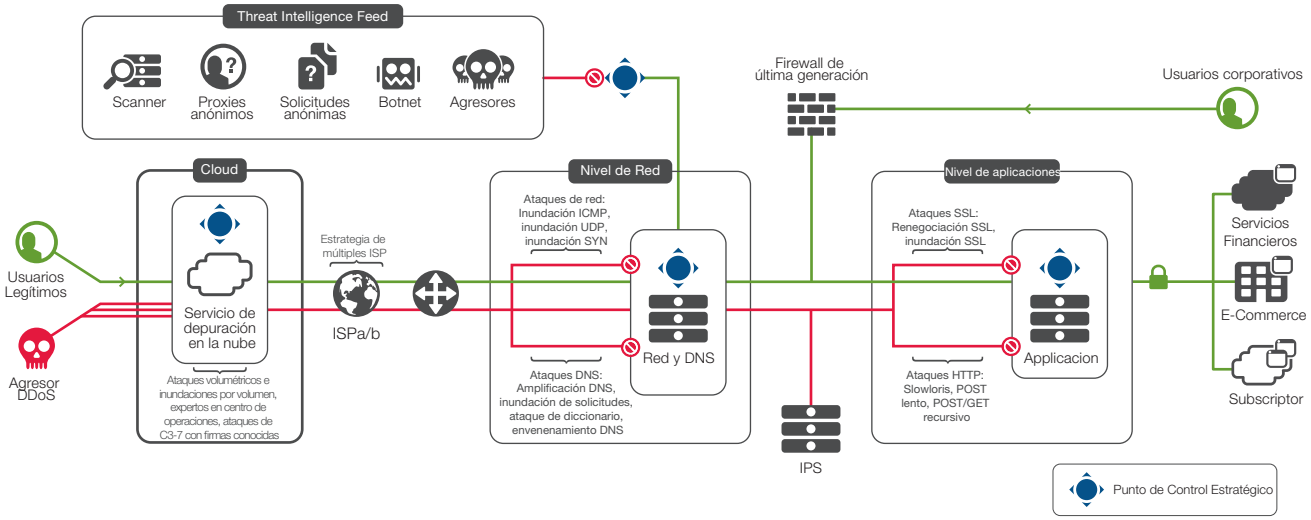


Figure 2: F5 recommends a multi-tiered DDoS protection approach to your architecture.

Pasos de mitigación ante DDoS

Si parece que está sufriendo un ataque volumétrico, puede ayudarle tener un sentido histórico de sus patrones de tráfico propios. Mantenga una base de patrones normales de tráfico con la cual comparar.

Si ha determinado que se encuentra bajo un ataque DDoS, registre el tiempo estimado de inicio en su registro de ataques.

Monitoree ataques volumétricos. Recuerde siempre mantener una página web abierta para indicarle cuando el ataque pueda haber acabado (o haber sido mitigado).

Necesitará seguir (hasta) 10 pasos para lograr la mitigación de su ataque DDoS:

- Paso 1: Verifique el ataque
- Paso 2: Póngase en contacto con los líderes de equipo
- Paso 3: Jerarquice aplicaciones
- Paso 4: Proteja a sus asociados y usuarios remotos
- Paso 5: Identifique el ataque
- Paso 6: Evalúe opciones de mitigación por dirección de origen
- Paso 7: Mitigue ataques contra aplicaciones específicas
- Paso 8: Aumente la postura de seguridad a nivel de aplicaciones
- Paso 9: Limite recursos
- Paso 10: Maneje las relaciones públicas

Paso 1: Verifique el ataque

No todas las interrupciones son causadas por un ataque DDoS. Configuraciones erróneas de DNS, problemas de routing, y error humano son causas comunes de interrupciones de red. Primero debe descartar estos tipos de ataques no DDoS y distinguir un ataque de una interrupción común y corriente.

Descarte las interrupciones más comunes

Entre más rápido pueda verificar que la interrupción en el servicio es un ataque DDos, más rápido podrá responder a él. Aun si la interrupción no fue causada por una configuración errónea u otro tipo de error humanos, puede haber otras explicaciones que semejen a un ataque DDoS.

Por ejemplo, el Slashdot Effect ocurre cuando una página en particular dentro de su sitio es incluida en un foro o blog muy popular. Su investigación debe descartar este tipo de posibilidades.

Verifique la conectividad saliente.

¿Hay conectividad saliente? Si no, entonces el ataque es tan severo que está congestionando todo el tráfico entrante y saliente. Verifique con sus herramientas tradicionales de diagnóstico (como traceroute, ping, y dig) y descarte estas posibilidades.

Descarte posibles problemas globales

Revise los siguientes reportes del estado del Internet para determinar si el ataque es un problema global.

- Internet Health Report
- Internet Traffic Report

Revise el acceso externo a la red

Intente acceder a su aplicación desde una red externa. Servicios y productos que pueden realizar este tipo de monitoreo incluyen:

- Prueba y monitoreo de Keynote
- Monitoreo sin agentes de HP SiteScope
- SolarWinds NetFlow Traffic Analyzer
- Downforeveryoneorjustme.com

Confirme la respuesta de DNS

Verifique si el DNS está respondiendo para su sitio. El siguiente comando de UNIX resuelve un nombre contra el servidor del proyecto OpenDNS.

```
% dig @208.67.222.222 yourdomain.com
```

Paso 2: Póngase en contacto con los líderes de equipo

Una vez que el ataque ha sido verificado, contacte los líderes de los equipos relevantes. Si no ha llenado ninguna hoja de referencia rápida o lista de contactos, cree una ahora o utilice nuestras plantillas. Cuando una interrupción de servicio ocurra, puede que su organización convoque a una conferencia telefónica formal que incluya a varios de los equipos operativos y de aplicaciones. Si su organización tiene un procedimiento de este tipo, utilice esta reunión para confirmar oficialmente el ataque DDoS a los líderes de equipo.

Contacte a su proveedor de servicios de banda ancha

Una de las llamadas más importantes que puede hacer es a su proveedor de servicios de banda ancha. Agregue el número de su proveedor de servicios a su hoja de contactos. El proveedor probablemente le pueda confirmar el ataque, darle información acerca de otros clientes que puedan estar bajo ataque, y en algunas ocasiones ofrecerle asistencia.

Contacte a su equipo anti fraude

Es de especial importancia recurrir al equipo anti fraude tan pronto sea verificado el ataque. Lo ataques DDoS pueden ser usados como una pantalla para esconder una infiltración. Los registros que normalmente mostrarían una penetración pueden perderse durante un ataque DDoS. Por esta razón es que el registro independiente y de alta velocidad es tan importante.

Paso 3: Jerarquice aplicaciones

Una vez que el ataque ha sido confirmado, jerarquice sus aplicaciones.

Al enfrentarse a un ataque DDoS intenso con recursos limitados, las organizaciones deben de tomar decisiones de jerarquización. Los activos en línea de más alto valor normalmente generan también ganancias de alto valor. Estas son las aplicaciones que querrá mantener con vida.

Aplicaciones de menor valor, independientemente de su nivel de tráfico legítimo, deben ser deshabilitadas intencionalmente para que sus recursos de procesamiento y de red pueden ser puestos al servicio de aplicaciones de mayor valor. Es posible que necesite de la opinión de líderes de equipo para hacer esto.

Al final, estas son decisiones financieras. Tómelas debidamente.

Cree una lista de prioridad de aplicaciones – le tomará solamente unos minutos escribir una, y le será de gran ayuda al momento de tomar decisiones complicadas acerca de las aplicaciones cuando se encuentre combatiendo un evento DDoS de verdad.

Decida cuáles aplicaciones son de baja prioridad y pueden ser deshabilitadas durante un ataque. Esto puede incluir aplicaciones internas.

Paso 4: Proteja a sus asociados y usuarios remotos

Agregue las direcciones de sus asociados a una lista blanca

Es muy probable que usted tenga asociados de confianza que requieran de acceso a sus aplicaciones o redes. Si aún no lo ha hecho, recolecte las direcciones IP que siempre deben tener acceso y mantenga esa lista.

Es posible que la lista blanca tenga que ser distribuida a varios lugares dentro de la red, como en el firewall, el Controlador de Entrega de Aplicaciones (Application Delivery Controller, ADC), y posiblemente hasta con el proveedor de servicios, para garantizar que el tráfico desde y hacia esas direcciones no sea interrumpido.

Proteja a los usuarios de VPN

Las empresas actuales ponen a los usuarios de SSL VPN remotos en listas blancas o les proporcionan quality-of-service. Normalmente esto se logra en un servidor integrado firewall/VPN, el cual puede ser de gran importancia si usted tiene un número significativo de empleados remotos.

Paso 5: Identifique el ataque

Determine la naturaleza del ataque

Ahora es el momento para recolectar inteligencia técnica acerca del ataque. La primera pregunta que debe hacerse es: "¿Cuáles son los vectores del ataque?"

Cuatro tipos de ataque DDoS

Está tratando de determinar la naturaleza del ataque. ¿Es:

- **Volumétrico** – ataques basados en inundaciones que pueden ocurrir en las capas 3, 4, o 7?
- **Asimétrico** —diseñado para invocar límites de tiempo o cambios en el estado de sesión?
- **Computacional** – diseñado para consumir CPU y memoria?
- **Basado en vulnerabilidad** – diseñado para explotar vulnerabilidades en el software?

A esta altura ya debe de haber llamado a su proveedor de servicios de banda ancha con la información en su lista de contactos. Si el ataque es solamente volumétrico, el proveedor de servicios lo habrá informado y puede ser que ya haya tomado acciones para remediar el ataque DDoS.

Aunque organizaciones bien equipadas usan soluciones de monitoreo existentes (como NetScout) para capturas profundas de paquetes, podrá encontrarse con casos en los que tiene que utilizar capturas de paquetes de otros dispositivos, como el ADC, para asistirle en el diagnóstico del problema. Estos casos incluyen:

- **Vectores de ataque SSL.** Si el ataque es lanzado por medio de SSL, puede que no haya otra forma de diagnosticarlo más que por medio del ADC. Capture el flujo de paquetes ya sea en el ADC o en algún otro lugar, y luego use la utilidad ssldump para desencriptar el archivo.

- **FIPS-140.** Si su ADC está usando un módulo de seguridad de hardware (HSM) FIPS-140, en muchas ocasiones todavía puede usar ssldump para decodificar la captura de archivo. **Utilice un puerto espejo o una reserva de clones.** Una manera de capturar paquetes es copiarlos desde el ADC. Este método de alto rendimiento permite el flujo de datos a través del ADC y hacia un dispositivo externo sin interrupción.

Paso 6: Evalúe opciones de mitigación por dirección de origen

Si el paso 5 ha identificado que la campaña utiliza vectores de ataque avanzados que su proveedor de servicios no puede mitigar (como ataques slow-and-low, ataques a aplicaciones, o ataques SSL), entonces el próximo paso hacerse la siguiente pregunta: "¿Cuántas fuentes existen?"

Si la lista de direcciones IP agresoras es pequeña, puede bloquearlas todas con su firewall. Otra opción sería pedirle a su proveedor de servicios de banda ancha que bloquee esas direcciones por usted.

Bloqueo geográfico

La lista de direcciones IP agresoras puede ser demasiado grande para ser bloqueadas en el firewall. Cada dirección que agrega a la lista de bloqueo alentará el procesamiento y aumentará el CPU. Pero es posible aún bloquear a los atacantes si todos se encuentran en la misma región geográfica o dentro de unas cuantas regiones que pueda bloquear temporalmente.

Por ejemplo, si la mayoría de los ataques parecen provenir del sureste de Asia, evalúe la pérdida de ganancias al bloquear todo el tráfico de esa región. Sea prudente al bloquear geográficamente.

La decisión de bloquear regiones enteras por medio de localización geográfica debe de tomarse como una decisión de negocios.

Finalmente, si hay muchos atacantes en muchas regiones, pero no le importa ninguna región más que la suya, también puede utilizar la localización geográfica como defensa para bloquear todo el tráfico excepto aquél que se origine desde su región.

Mitigue múltiples vectores de ataque

Si hay demasiados agresores como para poderlos bloquear por dirección IP o región, puede que tenga que desarrollar un plan para desarmar el ataque mitigándolo "al revés" – es decir, defendiendo su sitio desde el nivel de bases de datos hasta el de aplicaciones, y luego al de servidores web, balanceadores de carga, y finalmente los firewalls.

Puede que se encuentre bajo presión para encontrar un remedio en la dirección opuesta – por ejemplo, mitigar en la capa 4 para poner en funcionamiento de nuevo la capa 4. Sin embargo, tome en cuenta que al hacer esto, los ataques comenzarán a llegar más profundo dentro del centro de datos.

A medida que puede identificar la mezcla de diferentes vectores de ataque, revise la tabla siguiente para encontrar remedios específicos para cada ataque individual.

Vector de ataque	Firewall	DDoS Local	Controlador de Entrega de Aplicaciones	Depurador en la nube
Inundación SYN	×	×	×	×
Inundación ICMP	×	×	×	×
Inundación UDP	×	×	×	×
Inundación TCP			×	×
Inundación DNS		×	×	×
Apache Killer		×	×	
Slowloris		×	×	
Keep Dead		×	×	
HTTP Recursivo GET		×	×	

Paso 7: Mitigue ataques contra aplicaciones específicas

Si ha alcanzado este paso, entonces el ataque DDoS es suficientemente sofisticado para hacer de la mitigación por dirección de origen inefectiva. Los ataques que caen dentro de esta categoría pueden haber sido generados por herramientas como el Low Orbit Ion Cannon, Apache Killer, o el Brobot. Estos ataques se ven como tráfico normal en la capa 4, pero tienen anomalías que alteran los servicios al nivel de servidor, aplicación, o base de datos. (Para conocer más acerca de herramientas comunes de ataque y estrategias de mitigación, vea "La Taxonomía de los Ataques a Aplicaciones" en el documento Prácticas Recomendadas para DDoS de F5 .)

Para combatir estos ataques, debe de habilitar o construir defensas al nivel de gestión de aplicaciones.

Mitigando herramientas de ataque específicas

Una vez que ha analizado el tráfico en el Paso 4, si el ataque parece ser un ataque al nivel de aplicaciones, las preguntas importantes son:

- ¿Puede identificar el tráfico malicioso?
- ¿Parece haber sido generado por una herramienta de ataque conocida?

Ataques específicos al nivel de aplicaciones pueden ser mitigados dependiendo del caso por medidas compensatorias específicas de F5. Los agresores de hoy en día utilizan varios tipos de vectores de ataque DDoS, pero la mayoría de esos vectores están entre las capas 3 y 4, con solo uno o dos ataques a nivel de aplicaciones. Esperamos que este sea el caso para usted, lo cual significaría que ya casi ha terminado con su ataque DDoS.

Paso 8: Aumente la postura de seguridad a nivel de aplicaciones

Si ha alcanzado este paso en un ataque DDoS, ya ha mitigado al nivel de capas 3 y 4, y ha evaluado mitigaciones para ataques específicos a aplicaciones, y sigue experimentando problemas. Esto significa que el ataque es relativamente sofisticado, y su habilidad para mitigarlo dependerá en parte de sus aplicaciones.

Ataque asimétrico a aplicaciones

Es muy probable que se esté enfrentando a uno de los ataques modernos más difíciles: el ataque asimétrico a aplicaciones. Este tipo de ataque puede ser:

- Una inundación de GETs recursivos de la aplicación completa.
- Una solicitud repetida de un objeto público de gran tamaño (como un MP3 o PDF).
- Una invocación repetida de una petición de bases de datos costosa.

Si usted ha implementado algunas de las recomendaciones de arquitectura mencionadas en la introducción, puede hacer uso de esas defensas ahora.

Aproveche su perímetro de seguridad

La mejor defensa contra estos ataques asimétricos depende de su aplicación. Por ejemplo, organizaciones financieras conocen a sus clientes y son capaces de usar barreras de inicio de sesión para rechazar solicitudes anónimas. Aplicaciones de la industria del entretenimiento como sitios web de hoteles, por otro lado, muchas veces no conocen al usuario hasta que éste accede a hacer una reservación. Para ellos, un CAPTCHA puede ser una mejor disuasión.

Escoja la defensa a nivel de aplicación que tenga mayor sentido para su aplicación:

- Una barrera de inicio de sesión
- Detección de humanos
- Cumplimiento de navegadores reales

Barreras de inicio de sesión

Una barrera de inicio de sesión es una defensa lógica que requiere que un cliente haya iniciado una sesión como un usuario conocido antes de que ese cliente pueda acceder a algún activo de alto valor o ejecute una petición de base de datos. Las barreras de inicio de sesión pueden ser implementadas al nivel del proveedor de servicios, un firewall de aplicación web, o un ADC.

La desventaja de esta solución, que de otra forma sería perfecta, es que no cualquier aplicación tiene una integración cercana con los usuarios conocidos. Por ejemplo, los hoteleros deben dar servicio con aplicaciones de disponibilidad de cuartos que no requieren que el usuario inicie una sesión.

Detección de humanos

La detección de humanos es el segundo mejor enfoque. Validar que la conexión del cliente esté siendo controlada por un humano (en lugar de un bot malicioso) puede hacer mucho para rechazar un ataque DDoS de capa 7. Usualmente esto se hace con un CAPTCHA.

CAPTCHA es un acrónimo en inglés para Prueba de Turing Pública Completamente Automatizada para diferenciar Computadoras de Humanos. Es una prueba usada en computación para determinar si la entidad realizando la solicitud es humana, al requerir una respuesta específica. La desventaja de las CAPTCHAs (y la razón por la cual no pueden proteger todos los recursos en todo momento) es que rechazarán a un porcentaje de usuarios legítimos. Aplicaciones flexibles pueden permitir que las CAPTCHAS puedan ser activadas durante un ataque y desactivadas después.

Figura 3: Una CAPTCHA típica puede ayudar a repeler un ataque en capa 7.

Cumplimiento de navegadores reales

Algunos firewalls de aplicaciones web ofrecen esta funcionalidad insertando un redireccionamiento JavaScript en conexiones nuevas y luego poniéndolas en una lista negra si no siguen el redireccionamiento. Este es un enfoque útil dado que irrumpe con la mayoría de los bots sin interferir con los usuarios reales usando navegadores reales.

Paso 9: Limite recursos

Si todos los pasos previos fallan al detener el ataque DDoS, puede verse forzado a simplemente limitar recursos para sobrevivir el ataque.

Esta técnica rechaza tanto tráfico bueno como malo. De hecho, limitar la capacidad en muchos casos rechaza del 90 al 99 por ciento del tráfico deseable al mismo tiempo que permite que el agresor aumente los costos en su centro de datos. Para muchas organizaciones es mejor deshabilitar una aplicación que limitar su capacidad.

Conformación de capacidad

Si llega a la conclusión de que debe limitar su capacidad, puede establecer limitaciones en diferentes puntos en una arquitectura DDDoS de múltiples niveles. Al nivel de red, donde los servicios de seguridad de capa 3 y 4, utilice la conformación de capacidad para evitar que inundaciones TCP sobrecarguen sus firewalls y otros dispositivos de capa 4.

Límites de conexión

Los límites de conexión pueden ser una técnica efectiva de mitigación, pero no funcionan bien con funcionalidades de múltiplex de conexiones. Los límites de conexión al nivel de aplicaciones deben de ofrecer la mejor protección para evitar que demasiado flujo de salida sobrecargue sus servidores web y middleware de aplicaciones.

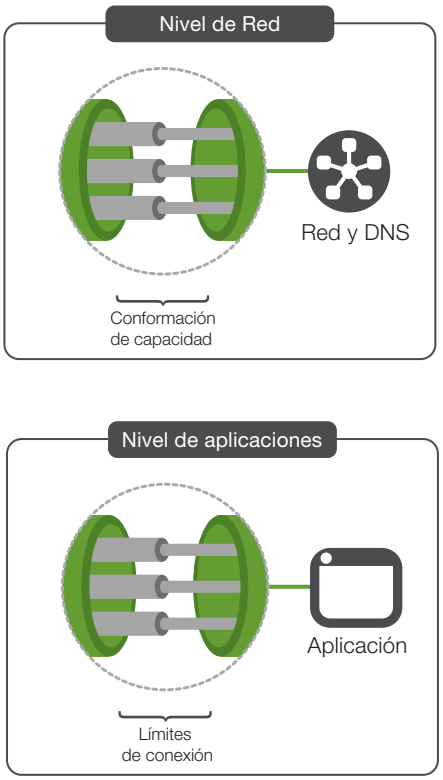


Figura 4: Los límites de recursos le pueden ayudar a sobrevivir el ataque.

Paso 10: Maneje las relaciones públicas

Las organizaciones hacktivistas de hoy en día utilizan a los medios para llamar atención hacia sus causas. Muchos hacktivistas informan a los medios cuando un ataque está sucediendo y pueden contactar también a la compañía blanco durante el ataque.

Las organizaciones financieras, en particular, pueden tener políticas relacionadas con responsabilidad legal que les impiden admitir cuando un ataque está sucediendo. Esto puede convertirse en una situación complicada para el responsable de las relaciones públicas. El responsable puede decir algo como, "En estos momentos estamos experimentando algunas dificultades técnicas, pero estamos optimistas en que nuestros clientes podrán tener acceso completo a nuestros servicios en línea pronto."

Lidiando con los reporteros

Los reporteros, sin embargo, pueden no aceptar este tipo de evasivas, especialmente si el sitio parece estar completamente fuera de servicio En un caso reciente, un reportero llamó al gerente de una sucursal local de un banco y le preguntó cómo estaba transcurriendo el ataque. El gerente de la sucursal, que no había recibido entrenamiento para medios, respondió, "Es horrible, ¡nos están matando!"

Si el ataque DDoS parece ser un ataque de hacktivismo de alto perfil, prepare dos comunicados:

1. Para la prensa. Si las políticas de su industria le permiten admitir cuando ha sido atacado desde el exterior, hágalo y sea franco al respecto. Si una política dicta que debe desviar los cuestionamientos, argumente dificultades técnicas, pero asegúrese de preparar su próximo comunicado.
2. Para el personal interno, *incluyendo a cualquiera que pueda ser contactado por la prensa*. Su comunicado interno debe de dar direcciones acerca de qué decir y qué no decir a los medios, o mejor aún, indique a su personal que dirija todas las preguntas relacionadas con el evento al responsable de RP. Incluya un número telefónico.

Conclusión

Si esta información le ha sido de utilidad, cree un plan de acción personalizado para su organización. Utilice nuestras hojas de referencia o cree las suyas. Imprímalas, llénelas, y enmíquelas. Úselas para iniciar un plan de acción físico o colóquelas en la pared en su centro de datos.

A manera que se defienda de ataques DDoS, podrá refinar su plan de acción y mejorar la resistencia de sus aplicaciones.