Citrix NetScaler: Una poderosa defensa contra los ataques de denegación de servicio

CITRIX®

Los dos últimos años han visto un marcado resurgimiento de los ataques denegación de servicio (DoS). No es solo este tipo de amenaza lo que preocupa a los equipos de seguridad de la red, también es el hecho de que ha cambiado la naturaleza de la amenaza. Las grandes compañías de Internet no son ya el objetivo principal. Ahora todas las empresas, sin importar su tamaño o segmento de la industria, están en riesgo. La detección de estos ataques es también mucho más difícil que en el pasado, a medida que distintas capas de aplicación de bajo ancho de banda centradas en agotar los recursos de backend se unen a los ya familiares ataques de alto volumen destinados a sobrecargar la red o derribar los dispositivos y servicios críticos de red.

Este white paper analiza el panorama actual de DoS y examina los enfoques comunes para hacer frente a las modernas amenaza DoS. En él se explica cómo el controlador de entrega de aplicaciones Citrix® NetScaler® (ADC) ofrece una robusta pero asequible base para las defensas de DoS de una organización. Los beneficios de la solución NetScaler incluyen:

- Un amplio conjunto de mecanismos de protección capaces de frustrar de forma efectiva ataques DoS en todas las capas informáticas.
- La inclusión de innovadoras y sensatas técnicas para hacer frente a las más insidiosas formas de ataques de denegación de servicio sin tener que afectar innecesariamente las transacciones legítimas.
- La capacidad de aprovechar la misma huella NetScaler para permitir también la transformación de los rígidos centros de datos heredados del pasado a las flexibles y adaptables redes cloud empresariales de hoy.

Entender el actual panorama DoS

Hoy en día se ha desvanecido la idea elemental de los hackers de desestabilizar a las grandes propiedades en Internet, dando paso a ataques DOS por motivos financieros. En general, estos ataques orientados al beneficio requieren técnicas no disruptivas y discretas para lograr su objetivo de robar datos valiosos. Durante este período, los ataques DOS fueron utilizados principalmente para la extorsión. En este escenario, el chico malo amenaza con ejecutar un ataque DoS a menos que se reciba un pago nominal en un determinado plazo. Pague y obtenga un correo electrónico de agradecimiento; no lo haga y sus negocios sufren las consecuencias.

El regreso de los ataques DOS

En los últimos años, sin embargo, los ataques han regresado con sed de venganza. Este desarrollo puede ser atribuido principalmente a que se han convertido en una técnica favorita para ataques por motivos políticos y sociales. Objetivamente hablando, van bien en estos casos. No es la información valiosa lo que importa a los atacantes, sino obtener la atención del objetivo y, aún más importante, la del público en general.

Un subproducto notable de este estilo de hacker fue la publicación gratuita o de bajo coste de kits de herramientas para la creación de los ataques DoS. Combinado con un fácil acceso a ordenadores en red con fines maliciosos, estos kit de herramientas cimentaron el retorno de los ataques DOS. También contribuyeron a una serie de características del panorama DoS actual y que son particularmente importantes de reconocer.

Para empezar, bajas barreras técnicas y financieras para acceder significa que prácticamente cualquier persona puede ejecutar un ataque DoS hoy en día. En segundo lugar, y por las mismas razones fundamentales, ahora es más fácil aprovechar las técnicas DoS para ataques por motivos financieros. Este tipo de ataques puede llevarse a cabo directamente interrumpiendo la actividad de un competidor o utilizando técnicas DoS como una cortina de humo para un ataque multi-vector diseñado en última instancia para robar datos valiosos. La clave aquí es que cada organización es ahora un potencial objetivo DoS, independientemente de su tamaño, sector vertical o programa.

La evolución de los ataques DoS

Mientras que la facilidad de ejecución ha facilitado el retorno de los ataques, otro cambio importante es tener un efecto igualmente profundo cuando se trata de defenderse ellos. Coherentemente con lo que ha ocurrido en general, en el panorama de las amenazas, los ataques DoS están migrando a niveles informáticos más altos. Porque "migrar" sugiere una salida de la zona de origen, sin embargo, es más exacto decir que están añadiendo nuevos trucos a su arsenal.

Los ataques DoS ruidosos, de alto volumen, y centrados en la red no están desapareciendo necesariamente. Pero se juntan en la nueva generación de ataques DoS que operan en las capas altas de la informática. Un gran reto con estos nuevos ataques es que a menudo copian sesiones/transacciones legítimas, una característica que les permite pasar desapercibidos a través de una amplia gama de defensas, incluyendo cortafuegos y sistemas de prevención de intrusiones.

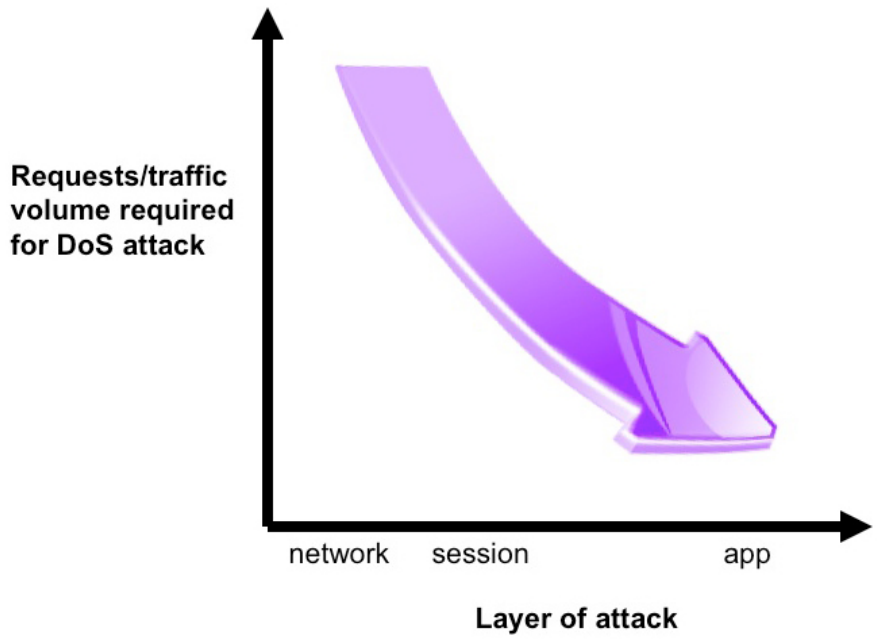


Imagen 1: Asimetría de los ataques DoS

Una segunda cuestión es su naturaleza cada vez más asimétrica [como se muestra en la figura 1]. Desde una perspectiva técnica, se refiere a que requieren solo un número relativamente pequeño de solicitudes de aplicación y/o una pequeña cantidad de ancho de banda para disparar un desproporcionado consumo de recursos de backend. Desde una perspectiva práctica, significa de nuevo que son más difíciles de detectar, ya que los picos inesperados en transacciones o el tráfico de red ya no son indicadores de su presencia.

A pesar de todos estos cambios, los ataques DoS permanecen enfocados a causar el agotamiento de los recursos en algún punto de extremo a extremo de la cadena informática, ya sea en los canales de la red, en el estado de los dispositivos de red y servidores o en la capacidad de procesamiento de los host de aplicaciones. Tener esto en cuenta es la clave para implementar con éxito una estrategia para mitigar los ataques DoS.

Estrategias de alto nivel para mitigar los ataques DoS

Las soluciones para mitigar los ataques DoS se dividen en dos clases: dispositivos ubicados en las instalaciones del cliente y servicios basados en cloud. Dentro de cada una de estas clases existen múltiples opciones, cada una con sus propios pros y contras.

Dispositivos localizados en casa del cliente

La primera opción para mitigar ataques DoS y que necesita ser descartada rápidamente ya que es una mala elección, es el firewall empresarial o sistema de prevención de intrusiones. Para ser justos, estos dispositivos a menudo incorporan una serie mecanismos de protección DoS (unos más que otros). Sin embargo, estos mecanismos son generalmente limitados para contrarrestar los ataques DoS de red y no proporcionan protección contra variantes de la capa superior. Además, estos dispositivos son inherentemente completos. La necesidad de seguir de cerca el estado de los paquetes y flujos que pasan a través de ellos, hacen a los dispositivos susceptibles de ser atacados.

Los dispositivos dedicados a mitigar los ataques DoS son una segunda opción. Aunque estos generalmente ofrecen un sólido conjunto de mecanismos de protección multicapas contra ataques DoS, también tienen algunas deficiencias. Para empezar, sufren la misma limitación que todas las demás soluciones localizadas en las instalaciones del cliente: son irrelevantes si el ataque sobrecarga sus conexiones de Internet evitando que el tráfico llegue hasta ellos en primer lugar. También es probable que sean susceptibles de ataques basados en SSL, que conllevan importantes multas, especialmente en ausencia de hardware dedicado para la terminación e inspección SSL. Otra desventaja a considerar es el grado en que cualquier capacidad de prevención DoS compensa la necesidad de adquirir, implementar y mantener "otro dispositivo" en cada conexión importante de Internet.

Los ADC modernos son ya un punto estratégico de control en la mayoría de las redes, y representan ya la tercera opción idónea a tener en cuenta. Los ADC líder del mercado como NetScaler combinan una gran cantidad de capacidades para mitigar ataques DoS que sirven para todas las capas informáticas. Incluso incluyen soporte ante ataques informáticos intensivos DoS a SSL. El resultado es una solución que proporciona una cobertura sustancial para amenazas DoS sin la necesidad de implementar otra serie de dispositivos dedicados.

Servicios basados en la nube

La principal ventaja de las opciones de mitigación DoS basadas en la nube es que, a diferencia de las soluciones basadas en las instalaciones del cliente, las primeras pueden dar cuenta de los ataques DoS dedicados a sobrecarga su ancho de banda de Internet. En términos generales, estas dos opciones, proveedores de servicios de entrega de contenidos de red y proveedores de servicios anti DoS, necesitan centros de datos aprovisionados con enormes cantidades de ancho de banda. Este enfoque permite que estas opciones hagan frente mejor a los ataques de estilo volumétrico. Además, ambos tipos de proveedores de soluciones han hecho inversiones sustanciales en una amplia variedad de tecnologías de mitigación DoS, ya que sus negocios dependen de ello. Sin embargo, hay algunas diferencias significativas a considerar, sin mencionar posibles defectos. Estas incluyen:

- Variabilidad significativa en cuanto a la cobertura proporcionada contra ataques DoS a las capas superiores. De alguna forma esto es inevitable, ya que nunca ningún proveedor externo entenderá las "características" de sus aplicaciones mejor que usted.
- Aunque los CDN son una solución siempre disponible, generalmente solo se usan para un subconjunto de los sitios más importantes de una organización, de cara al cliente y las aplicaciones. Aun así, hay formas en que los atacantes podrían "dar la vuelta" o "atravesar" el CDN, como por ejemplo, reventando las IP o enviando una avalancha de solicitudes que da lugar a errores de caché y que tienen que ser atendidos por su infraestructura fuente.
- En comparación, mientras todos los centros de limpieza anti-DoS proporcionan cobertura para todo el tráfico de una empresa, no están siempre en funcionamiento (porque sería un coste prohibitivo). En cambio, son involucrados de forma selectiva por el cliente cada vez que se detecta un ataque. Lo que les convierte en una mala opción para ataques DoS de la capa superior, ya que estos no siempre implican una fuerza bruta y, por lo tanto, no son fáciles de identificar cuando se producen.

La respuesta: Estrategia de una defensa en profundidad

No es de extrañar que el planteamiento ideal sea seguir una estrategia de defensa en profundidad que combine un servicio basado en cloud y un dispositivo que funcione de forma complementaria en las instalaciones del cliente. Dada la creciente prevalencia de ataques a la capa de aplicación, una solución basada en las instalaciones del cliente, en particular un ADC, proporcionaría el mayor impacto a su inversión. Por tanto, es un buen lugar de comienzo para la mayoría de las organizaciones. Dicho esto, hacer una inversión en un servicio de limpieza DoS capaz de frustrar ataques volumétricos a la red, no debería retrasarse, especialmente si usted es un objetivo prominente.

NetScaler para la protección DoS

NetScaler, un ADC moderno en todos los sentidos, ofrece una protección robusta no solo contra los clásicos ataques DoS a la capa de red, sino también contra los más avanzados y cada vez más frecuentes ataques a la capa de sesión y de aplicación, incluyendo las variantes de bajo ancho de banda y asimétricas. Para la mitigación de ataques DoS, NetScaler realiza el mismo planteamiento aplicable a todos los demás aspectos de seguridad: un modelo de seguridad en capas. Esto permite a NetScaler destacar incluso cuando los ataques DoS evolucionan hacía los niveles informáticos más altos.

Incremento de la dificultad de detección

	Ataques ejemplo	Características de mitigación de NetScaler
Aplicación	Inundaciones maliciosas GET y POST; slowloris, slow POST, y otras variantes de bajo ancho de banda	Validación del Protocolo de aplicación, protección contra picos, colas de prioridad, protección contra inundaciones HTTP, protección de ataque HTTP de bajo ancho de banda protección contra ataques de bajo ancho de banda
Conexión y sesión	Inundaciones de conexión, inundaciones SSL, inundaciones DNS (udp, query, nxdomain)	Arquitectura proxy completa, diseño de alto rendimiento, gestión inteligente de memoria, amplia protección DNS
Red	Inundación Syn, UDP, ICMP, PUSH y ACK ; LAND, ataques smurf y teardrop	Defensas incorporadas, modelo de seguridad por denegación, protocolo de validación, limitación de velocidad.

Imagen 2: Características de NetScaler para mitigación de ataques DoS

Nota: Muchas de las tecnologías de mitigación que se indican en la imagen 2 en realidad ayudan a mitigar los ataques DoS a través de múltiples capas. El diseño de alto rendimiento de los ADC NetScaler, la adopción de denegación por defecto y la arquitectura basada en proxy son buenos ejemplos, ya que son aplicables a todas las capas informáticas. Solo se muestran en un lugar para ayudar a agilizar la discusión.

Protección de la capa de red contra DoS

Los ataques a la capa de red principalmente van a la infraestructura de red de una organización orientada al público con una avalancha de tráfico o paquetes especialmente diseñados para provocar que los dispositivos de red se comporten erráticamente. Las características de NetScaler que frustran los ataques en esta capa incluyen:

- **Defensas incorporadas**: NetScaler incorpora una informática de alto rendimiento normalizada con estándares TCP/IP que incluye mejoras específicamente destinadas a contrarrestar muchas formas de ataques DoS de bajo nivel. Un ejemplo es la implementación de cookies SYN, un mecanismo bien reconocido para la gestión de ataques por avalancha SYN, que está optimizado en cuanto al rendimiento (para maximizar el rendimiento de conexiones negociadas) y en la mejora de la seguridad (convirtiendo las antiguas técnicas de detección de conexiones falsas en obsoletas). Otras amenazas DoS similares, o configuradas por defecto, son LAND, ping of death, smurf y ataques fraggle.

- **Postura de seguridad por denegación predeterminada:** La denegación predeterminada podría ser un mecanismo de seguridad relativamente simple, por lo menos conceptualmente, pero también es muy poderoso. Eliminando automáticamente los paquetes que no estén expresamente permitidos por la política, o que no estén asociados a un flujo válido, NetScaler evita una gran variedad de ataques, incluyendo UDP, ACK, y avalanchas PUSH.
- **Validación de protocolos:** Una variedad particularmente problemática de ataque DoS se basa en el envío de datos con formato incorrecto, como por ejemplo paquetes con combinaciones no válidos de banderas, fragmentos incompletos o cabeceros cortados. Un buen ejemplo de la capa de red es el conocido como el ataque del "árbol de Navidad", que recibe su nombre por el hecho de que los paquetes malos son "iluminados" con todos los indicadores posibles TCP activados. NetScaler derrota esta subclase de ataques al asegurar que los protocolos de comunicación se utilizan de una manera estrictamente conforme a las especificaciones evitando las combinaciones que, aunque técnicamente están permitidas, podrían ser peligrosas. Con NetScaler, este mecanismo de mitigación abarca todas las capas, aplicándose a todos los protocolos soportados, incluyendo TCP, UDP, DNS, RADIUS, Diameter, HTTP, SSL, TFTP y SIP.
- **Limitación de velocidad:** Otra técnica general para mitigar los ataques DoS es evitar la sobrecarga por estrangulamiento de las conexiones de red y servidores o redirigir el tráfico que supere un límite específico. NetScaler proporciona una capacidad granular para realizar esto como controles de velocidad AppExpert. Con esta característica, los administradores pueden definir una amplia variedad de políticas de respuestas de NetScaler para que se activen cuando se superen los umbrales configurables del ancho de banda, conexión o las tasas de solicitudes desde un recurso determinado, incluyendo los servidores virtuales, dominios y las URL. Sin embargo se debe tener cuidado al utilizar este mecanismo, para no afectar involuntariamente a las comunicaciones legítimas.

Protección contra DoS a la capa de conexión y de sesión

Los ataques DoS orientados a las conexiones, se centran en las tablas de estado de dispositivos agotados, mientras que los ataques DoS contra las capas intermedias implican típicamente la alteración de las funcionalidades DNS o SSL. Las características de NetScaler que contrarrestan estos tipos de ataques son las siguientes:

- **Arquitectura Full-proxy:** Como solución Full-proxy, NetScaler es una parte activa de la corriente del tráfico, no es un componente pasivo que se ve pero que no puede afectar a lo que pasa. Al terminar todas las sesiones entrantes, NetScaler no solo crea un "espacio" entre los recursos internos y externos, sino que también proporciona una valiosa oportunidad para inspeccionar y, si procede, manipular el tráfico antes de reenviarlo a su destino. Este planteamiento inherentemente detecta una variedad de elementos maliciosos mientras que simultáneamente proporciona una base para inspecciones avanzadas diseñadas para eliminar los restantes. También permite a NetScaler servir como un buffer de recursos de backend contra una variedad de amenazas, incluyendo muchos tipos de ataques DoS.
- **Diseño de alto rendimiento:** Sirviendo como un eficaz buffer de recursos de backend también requiere un diseño de alto rendimiento; de lo contrario, NetScaler simplemente podría suplantar los servidores individuales como el punto de fallo durante un ataque DoS. NetScaler emplea una plataforma creada ex profeso en la que tanto el software a nivel del sistema como de hardware están diseñados y optimizados explícitamente para cargas de trabajo NetScaler. Como características específicas incluye un sistema operativo modificado (para procesar la baja latencia), niveles optimizados de red, motor de análisis HTTP inteligente y uso selectivo de funciones específicas de aceleradores hardware. Aceleradores dedicados SSL, que operan en conjunto con un proxy completo capaz de identificar y descargar conexiones SSL vacías o maliciosas, son instrumentales cuando se trata de defenderse de los ataques de avalanchas SSL.

Clasificación por rendimiento de NetScaler (Serie MPX 22000)	
Conexiones TCP por segundo:	**8,5 millones**
Peticiones HTTP por segundo:	**4,7 millones**
Rendimiento de HTTP:	**120 Gbps**
Transacciones SSL por segundo	**560.000**
Ataques SYN por segundo	**38 millones**
Peticiones DNS por segundo	**35 millones**
Sesiones SSL concurrentes	**7,5 millones**
Sesiones TCP concurrentes	**75 millones**

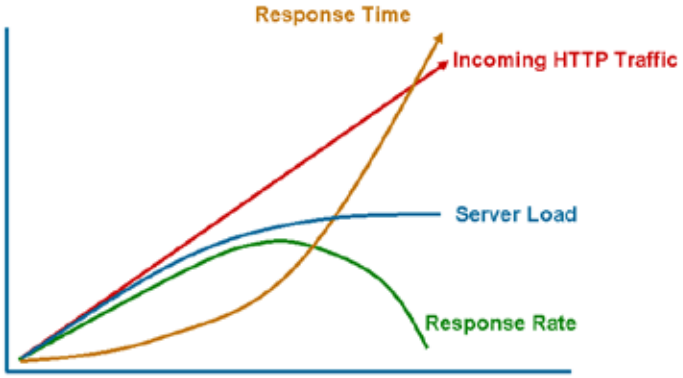
- **Gestión inteligente de la memoria:** Otra forma en la que NetScaler mitiga los ataques de sobrecarga de conexiones es mediante la incorporación de técnicas "memory-less" para la negociación de conexiones. Estas técnicas se utilizan en múltiples capas, incluso en la configuración de TCP y HTTP y evita que NetScaler tenga que destinar recursos hasta que una nueva conexión se haya validado totalmente, o hasta que se haya presentado una solicitud de aplicación real. Este enfoque reduce la dependencia de una tabla de conexión excesivamente grande y elimina la necesidad de numerosas rutinas de recogida. La recogida todavía se utiliza en otros escenarios para administrar memoria inteligentemente, por ejemplo, al dar prioridad a la eliminación de fragmentos en condiciones de poca memoria, y para ayudar a contrarrestar algunos de los ataques "lentos" a las capas de aplicación que veremos en secciones posteriores. El resultado final es el endurecimiento adicional de NetScaler contra los ataques DoS y un mejor almacenamiento en buffer de los sistemas de backend.
- **Amplias protecciones DNS:** Los ataques DoS contra DNS, un servicio de infraestructura esencial para el centro de datos moderno, no son nuevos ni poco frecuentes. Incluyen avalanchas UDP ordinarias, así como avalanchas basadas en consultas que utilizan numerosos trucos, tales como solicitar expedientes para los hosts inexistentes, para sobrecargar los servidores DNS. NetScaler hace frente a estas amenazas de dos formas: 1. Modo DNS proxy, donde equilibrar la carga de los servidores DNS internos de la organización; y 2. modo acreditado, donde sirve directamente como solución de la organización para solicitudes de nombre y resolución de IP. Características de mitigación que aplican a uno o ambos modos e incluyen la arquitectura NetScaler Full-proxy y el diseño de alto rendimiento, una implementación DNS endurecida, validación del protocolo DNS y capacidades de limitación del DNS específico. El soporte de NetScaler para DNSSEC permite neutralizar las amenazas falsas y los registros corruptos del host para su difusión a nuevos objetivos.

Protección de capa de aplicación contra DoS

La última innovación de ataques DoS de la capa de aplicación, es problemática por varias razones. Para empezar, los ataques a la capa de aplicación son más estrechos por definición, y a menudo no solo para un protocolo de la capa de aplicación (por ejemplo, HTTP), también para una aplicación individual. Para agravar la situación está el hecho de que el tráfico de ataque a menudo no se distingue en su contenido y volumen del tráfico normal. Un ejemplo clásico es un ataque de bajo ancho de banda que implica nada más que una serie constante de peticiones a una aplicación que se sabe que requieren procesamiento de backend sustancial (por ejemplo, un cálculo complejo u operación). Dispositivos de seguridad de bajo nivel, tales como los firewall de red, son en gran medida inútiles contra este tipo de ataques; e incluso dispositivos de nivel superior es probable que requieran sintonizarse periódicamente para mantenerse al día con nuevas tácticas y variables específicas de la aplicación.

Las características de NetScaler que abordan los ataques DoS de la capa de aplicación incluyen:

- **Validación del Protocolo de aplicaciones**; aplicar la normativa RFC y las mejores prácticas para el uso HTTP es una manera altamente efectiva por la que NetScaler elimina toda una franja de ataques basados en peticiones malformadas y comportamientos ilegales de protocolo HTTP. Pueden agregarse otros controles y protecciones personalizados a la política de seguridad aprovechando el filtrado de contenidos, acciones de respuestas personalizadas y capacidades de HTTP bidireccional.
- **Protección ante picos y prioridad de colas**; además de proteger a los servidores backend contra una carga más allá de su capacidad, una mitigación de ataque DoS de éxito necesita garantizar que los clientes reciben una respuesta y que el tráfico crítico del negocio no se vea impactado negativamente en condiciones de ataque. Las características de NetScaler que hacen frente a estos requisitos incluyen protección contra picos y prioridad de colas. NetScaler maneja las oleadas de tráfico intermitente basándose en la tasa en la que se presentan las nuevas conexiones a los servidores backend en su capacidad actual. Es significativo que ninguna conexión se ha caído con este mecanismo. Por el contrario, NetScaler las almacena y entrega en el orden recibido, una vez que los servidores de backend están preparados para gestionarlos. Una característica estrechamente relacionada, la prioridad de colas, proporciona un esquema de ponderación que puede utilizarse para controlar el orden en el que se procesan las solicitudes de cola. El orden se basa en la importancia relativa de las aplicaciones asociadas.



Comportamiento del servidor sin protección ante avalanchas

Comportamiento del servidor con protección ante avalanchas

- Protección contra avalanchas HTTP; un método innovador que se utiliza para mitigar avalanchas HTTP GET. Cuando se detecta una condición de ataque (basándose en un umbral configurable para solicitudes de cola), NetScaler envía un desafío de bajo impacto a un número de clientes asociados. El desafío está diseñado de tal forma que los clientes legítimos pueden responder correcta y fácilmente, pero los "dumb" DoS no pueden. Esta información permite a NetScaler distinguir e ignorar las solicitudes falsas manteniendo aquellas enviadas por los usuarios de aplicaciones legítimas. Se utilizan técnicas similares combinadas con limitación de velocidad de nivel de aplicación, para frustrar avalanchas HTTP POST y GET.
- Protección contra ataques Http de bajo ancho de banda: NetScaler derrota automáticamente ataques Slowloris, que entregan cabeceras HTTP fragmentadas justo por debajo del límite del tiempo de espera para el servidor de destino, por no reconocer la configuración de una conexión válida. En contraste, derrotar los lentos ataques POST, que alimentan muy lentamente los datos HTTP al servidor, es un poco más difícil, pero también posible. En estos casos, NetScaler utiliza algoritmos especializados para monitorizar las condiciones indicadoras del nivel de petición de la aplicación, modera el número de conexiones lentas que están siendo servidas en cualquier momento y proactivamente recoge las conexiones excesivamente lentas de la memoria. La supervisión del estado de salud de las anomalías del funcionamiento de un servidor y las reglas de limitación, pueden utilizarse también para frustrar otras variantes que surgen de ataques DoS de bajo ancho de banda.

Conclusión

La disponibilidad de ataques DoS ha crecido en frecuencia y sofisticación en los últimos años. Para la mayoría de las organizaciones, defenderse completamente contra esta clase de amenazas, significará una combinación de servicios de limpieza complementarios basados en la nube y tecnologías de mitigación de ataques DoS en el entorno del cliente. En la parte del cliente, Citrix NetScaler representa una solución ideal. Con NetScaler, las empresas pueden aprovechar la misma plataforma que les permite pasar del rígido entorno informático de ayer a los altamente adaptables centros cloud para establecer una sólida defensa multicapa contra los potencialmente devastadores ataques DoS a los negocios.

Sede central corporativa
Fort Lauderdale, FL (EE.UU.)

Sede central de Silicon Valley
Santa Clara, CA (EE.UU.)

Sede central de EMEA
Schaffhausen (Suiza)

Centro de Desarrollo de la India
Bangalore (India)

Sede central de la División Online
Santa Bárbara, CA (EE.UU.)

Sede central del Pacífico
Hong Kong (China)

Sede central de América Latina
Coral Gables, FL (EE.UU.)

Centro de Desarrollo del Reino Unido
Chalfont (Reino Unido)

CITRIX®

Acerca de Citrix
Citrix (NASDAQ: CTX) es un líder en espacios de trabajo móviles, que proporciona virtualización, gestión de la movilidad, networking y servicios cloud para habilitar nuevas formas para trabajar mejor. Las soluciones de Citrix impulsan la movilidad empresarial a través de espacios de trabajo seguros y personales que proporcionan a los usuarios un acceso instantáneo a las aplicaciones, puestos de trabajo, datos y comunicaciones en cualquier dispositivo, sobre cualquier red y cloud. Este año, Citrix celebra 25 años de innovación, logrando que las TI sean más sencillas y los trabajadores sean más productivos. Con unos ingresos anuales de 2900 millones de dólares en 2013, las soluciones de Citrix son utilizadas en más de 330 000 organizaciones y por más de 100 millones de personas en todo el mundo. Para más información, visite www.citrix.es.