ESTRATEGIAS DE PROTECCIÓN CONTRA DDOS: ELIGIENDO EL MODELO CORRECTO

LA GUÍA DE UN PREVISOR PARA LOS ATAQUES DDoS

Al pensar proactivamente en una defensa DDoS, las organizaciones pueden construir una estrategia i ntegral para mitigar ataques. Elegir entre dispositivos de seguridad locales, servicios de depuración en la nube, y un enfoque híbrido hacia la protección DDoS permite a las organizaciones personalizar su estrategia de seguridad de acuerdo a su arquitectura de aplicaciones y las necesidades de su negocio.

Empresas de todo el mundo se encuentran en una constante lucha en contra de la amenaza – y realidad – de los ataques DDoS. Los ataques de denegación de servicio modernos no solamente interrumpen o deshabilitan sitios web y aplicaciones, también sirven para distraer a los equipos operativos de seguridad de amenazas aún más grandes. Los atacantes combinan una variedad de ataques de múltiples vectores, incluyendo inundaciones volumétricas, técnicas low-and-slow dirigidas a aplicaciones, y estrategias basadas en autenticación con la esperanza de identificar puntos débiles en la defensa de una organización.

Mientras que el propósito primario de los ataques DDoS es interrumpir el servicio a un sitio o aplicación web, las consecuencias de un ataque exitoso pueden tener un amplio alcance. Desde la simple pérdida de ganancias (debido a un sitio o servicio, como un VPN, deshabilitado), así como multas regulatorias y costos legales derivados de un ataque; a la pérdida de confianza por parte de los clientes y el daño a la reputación de su organización, las repercusiones de un solo ataque podrían afectar a su negocio por años.

Hasta hace poco, los equipos de seguridad de organizaciones en muchas industrias creían que no necesitaban preocuparse por los ataques DDoS, pero los últimos datos que arrojó el Data Breach Investigations Report 2016 de Verizon indican que empresas de todos los tamaños de todas las industrias corren el riesgo de ser atacadas. Casi la mitad de las organizaciones sufrieron de un ataque DDoS por lo menos una vez durante 2014, con un costo promedio de USD $200,000 - $500,000 por hora. Tome en cuenta también que muchos ataques DDoS no son siquiera reportados públicamente. Con estos preocupantes datos en mente, todas las organizaciones están comenzando a entender la necesidad de implementar una estrategia integral para mitigar los ataques DDoS.

Ya sea que su organización ya haya sido el blanco de un ataque DDoS o que haya visto a un socio o a otra organización luchar por mitigar uno, planificar es la clave para la supervivencia. Construir una arquitectura resistente a DDoS puede ayudar a su organización a mantener disponibles sus aplicaciones clave y mitigar ataques volumétricos, de red y aplicaciones. Con opciones como protección local, servicios de depuración en la nube y soluciones híbridas, la pregunta no es si debería prepararse para un ataque DDoS, sino cuál es la estrategia que mejor ayudará a su organización a asegurar la continuidad de sus servicios y limitar el daño al enfrentar un ataque.

verizonenterprise.com/verizon-insights-lab/dbir/2016/.

[2]"Understand the Business Impact and Cost of a Breach," Forrester, January 12, 2015, https://www.forrester.com/report/Understand+The+Business+Impact+And+Cost+Of+A+Breach/-/E-RES60563.

¿CUÁL MODELO DE MITIGACIÓN DDoS ES EL ADECUADO PARA MÍ?

Antes de pensar en cuál estrategia de protección DDoS tiene más sentido para su organización, aquí está un rápido curso de repaso sobre los tipos de ataques DDoS, los cuales están en cambio constante a medida que los atacantes se hacen más sofisticados.

TIPOS DE ATAQUES

Aunque el tipo de ataques que experimente no determinará por sí solo cuál modelo es el adecuado para usted, ayuda entender que un ataque DDoS puede tomar muchas formas. Los ataques modernos caen dentro de cuatro tipos: volumétricos, asimétricos, computacionales, y basados en vulnerabilidades.

Es posible, también, que un atacante utilice varios de estos tipos de ataques en conjunto, lo cual significa que las organizaciones deben desarrollar una estrategia integral – y flexible – de protección ante DDoS. Exploremos sus opciones, comenzando por las soluciones locales estándar.

Ataques VOLUMÉTRICOS basados en inundaciones que pueden ocurrir en las capas 3, 4 o 7.

Ataques COMPUTACIONALES diseñados para consumir CPU y memoria, como consultas de larga duración en inundaciones GET, y ataques SSL.

Ataques ASIMÉTRICOS diseñados para invocar expiraciones o cambios en el estado de sesión.

app

Ataques BASADOS EN VULNERABILIDADES que explotan vulnerabilidades en el software de aplicación.

MODELO

01 PROTECCIÓN DDOS LOCAL

BENEFICIOS

EL valor de una solución local está claro para algunas organizaciones. Al desplegar productos específicos en sus centros de datos, usted puede mantener directamente el control sobre su infraestructura, permitiéndole actualizar, cambiar, agregar, o quitar cualquier componente en cualquier momento. También obtendrá los beneficios de la mitigación inmediata de un ataque gracias a la respuesta instantánea de sus dispositivos seguida de reportes con los detalles del ataque. Su equipo interno de TI puede crear soluciones a la medida que se escalen independientemente del resto.

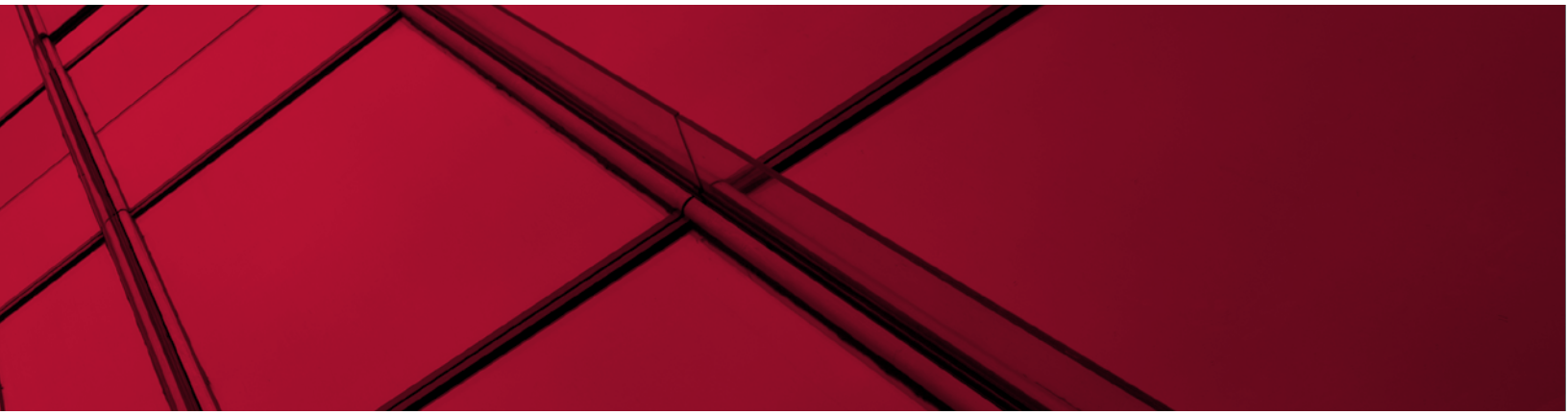
Además, ataques DDoS de bajo nivel como Slowloris, así como exploits que tienen como objetivo sus aplicaciones, son identificados y mitigados más eficientemente dentro de su centro de datos más cercano a la aplicación. Es más, muchas organizaciones – especialmente organizaciones financieras grandes – no están tan cómodas compartiendo sus claves privadas con proveedores externos, como un servicio DDoS de depuración en la nube.

Al mantener la mitigación de DDoS interna, las organizaciones logran tener siempre visibilidad y control óptimos sobre su estrategia de protección.

En resumidas cuentas, si su organización es un blanco en repetidas ocasiones, ahorrará tiempo y dinero teniendo una solución local que esté ajustada a la medida y lista para entrar en acción al primer indicio de un ataque.

CONSIDERACIONES

Las soluciones locales tienen algunas limitaciones. Por ejemplo, incluso la solución local DDoS más robusta puede verse superada por el tamaño de algunos de los ataques volumétricos modernos más grandes. Además, aunque hay muchos productos especializados en el mercado, hay muy pocas soluciones DDoS integrales, lo que significa que las organizaciones deben de trabajar con múltiples



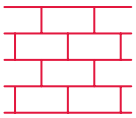
con múltiples proveedores para desarrollar una solución completa. Administrar varios productos de distintos proveedores requiere de cierto conocimiento técnico y puede ser un proceso tardado, lo cual disminuye la habilidad de su equipo operativo de seguridad para proteger sus sitios web y aplicaciones.

Muchas de estas soluciones individuales no pueden extenderse y tienen valor solamente cuando está siendo atacado, lo que significa que habrá gastado una gran cantidad de dinero en algo que tal vez utilizará una o dos veces (si tiene suerte). Finalmente, no todas las soluciones locales están diseñadas para funcionar con soluciones en la nube, este es un punto importante a considerar a medida que cambien las necesidades de su organización. Tener un proveedor que le pueda ofrecer una integración fluida al migrar de una defensa local a depuración en la nube (cuando sea necesario) le ayuda a simplificar su arquitectura de red, reducir el tiempo entre un ataque ysu mitigación, y evitar pasos manuales que puedan introducir errores.

COMPONENTES LOCALES

FIREWALL DE RED DE ALTA CAPACIDAD CON DETECCIÓN DDOS

- Soporta millones de conexiones simultáneas
- Repele inundaciones SYN mientras admite tráfico legítimo



FIREWALL DE APLICACIONES WEB
con protección DDoS integrada

BASE DE DATOS DE REPUTACIÓN IP

MODELO

02 SERVICIOS DE DEPURACIÓN EN LA NUBE

BENEFICIOS

Para algunas organizaciones, emplear un servicio de depuración en la nube para externalizar (o simplemente mejorar) su protección contra DDoS es la mejor estrategia. Si está administrando aplicaciones “nacidas en la nube,” puede ser que no esté operando un centro de datos tradicional donde los dispositivos locales de seguridad pueden ser colocados. Además, una organización puede no tener el personal técnico necesario para desplegar y administrar una solución local de protección contra DDoS. Por último, para las organizaciones que sí operan un centro de datos local, un servicio de depuración en la nube puede ofrecerles un conjunto de centros de datos con un ancho de banda alto que pueden depurar su tráfico antes de pasarlo de forma segura hacia su centro de datos.

El principal atractivo comercial de algunos de estos servicios de depuración en la nube es que están localizados completamente en el exterior, así que los ataques DDoS pueden nunca llegar a su red dependiendo del nivel de la suscripción que elija. La detección y mitigación en tiempo real de ataques DDoS volumétricos en la nube puede mantener el tráfico malo fuera de su red, al mismo tiempo que permite a los usuarios legítimos continuar usando su sitio y servicios.

Los múltiples centros de datos operados por dichos servicios de depuración en la nube significan que su organización tiene una protección extra contra ataques a nivel mundial. Utilizar DNS Anycast para distribuir los ataques hacia varios centros de datos globales significa que los atacantes no podrán enfocar todo su arsenal en un solo sitio, aun si todos tienen la misma dirección IP como objetivo. Además, tener múltiples centros de datos reduce la latencia y garantiza de mejor manera la alta disponibilidad de sus servicios y sitios.

Los servicios de depuración en la nube muchas veces pueden mejorar la eficiencia operacional y reducir los gastos operativos de TI ya que pueden

ser desplegados en minutos y con mínima experiencia técnica. Además, los mejores servicios ofrecen soporte 24x7 por parte de expertos en seguridad, lo cual puede liberar a su equipo de seguridad para enfocarse en otros problemas. Finalmente, estos servicios protegen a muchos clientes, así que el costo total del equipo es compartido por un grupo de clientes. Y dado que su organización solamente tiene que pagar por los servicios que usa, es posible que pueda lograr grandes ahorros en su CapEx.

CONSIDERACIONES

Si todo su tráfico de red está siendo depurado – y se encuentra atado por los términos del acuerdo de servicio firmado con el servicio de depuración en la nube – tendrá menos flexibilidad para personalizar su solución.

Finalmente, la mayoría de estos servicios se concentran en las capas 3 y 4 y no son los óptimos para combatir ciertos tipos de ataques, como ataques a aplicaciones de la capa 7 y ataques pesados de recursos URL, incluyendo peticiones complejas de bases de datos, que rápidamente abruman su red. Si está considerando un servicio de depuración en la red, busque uno que también ofrezca una opción con firewall para aplicaciones web (WAF en inglés) para contrarrestar ataques contra aplicaciones.

MODELO

03 ESTRATEGIA DE PROTECCIÓN HÍBRIDA CONTRA DDoS

BENEFICIOS

A pesar de que tanto las soluciones locales como los servicios de depuración en la nube ofrecen protección contra ataques DDoS, muchas organizaciones podrían verse beneficiadas por una estrategia híbrida que emplee protección local y en la nube combinadas para detener todas las variedades de ataques DDoS. Una vez diseñada, una solución híbrida ofrece un ciclo de retroalimentación cerrado entre componentes locales y en la nube, lo cual permite una mitigación afinada, así como reportes granulares de los detalles de los ataques.

Tal vez la estrategia más sólida de protección híbrida contra DDoS involucra una arquitectura de múltiples niveles donde los ataques DDoS de capa 3 y capa 4 sean mitigados a nivel de red con firewalls y bases de datos de reputación IP. EL nivel de aplicaciones se encarga de funciones de seguridad de alta demanda de CPU como terminación SSL y funcionalidades del firewall de aplicaciones web. Y un nivel de depuración basado en la nube protege en contra de grandes ataques volumétricos filtrando el tráfico generado por el atacante al tiempo que permite el tráfico legítimo hacia su centro de datos. Esta solución verdaderamente híbrida proporciona defensa contra DDoS a todos los niveles, protegiendo los protocolos (incluyendo aquellos que emplean encripción SSL y TLS) así como deteniendo ráfagas de DDoS, inundaciones HTTP aleatorizadas, bypass de caché, y otros ataques que puedan intervenir con el comportamiento de sus aplicaciones.

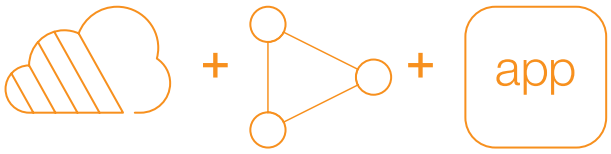
Una estrategia híbrida para la protección DDoS también puede llevar a ahorros en costos y una mayor eficiencia. Trasladar automáticamente ataques grandes hacia la nube requiere menor cantidad de recursos técnicos locales, pero aumenta la velocidad de mitigación, lo cual resulta en menos tiempo de inactividad. También está el beneficio de pagar por el servicio de depuración en la nube solamente cuando lo usa en vez de mantenerlo prendido todo el tiempo. E, idealmente, ambas partes de su solución híbrida pueden compartir una estructura combinada que controle si los ataques son manejados localmente o en la nube – permitiendo así el balance óptimo para cualquier ataque o series de ataques.

Tal vez el más grande beneficio del modelo híbrido es que prepara a su organización para un futuro en el cual pueda usar un tablero visual para administrar el rango de sus soluciones tanto locales como externas. A manera que esta visión se convierte en una realidad, usted podrá enfocarse menos en dónde debería ser mitigado y más en garantizar la alta disponibilidad de sus sitios y servicios, así como del continuo crecimiento del negocio.

CONSIDERACIONES

Administrar una solución híbrida requiere algo de recursos locales, mientras que externalizar por completo sus necesidades de protección contra DDoS hacia un servicio de depuración en la nube es la forma más sencilla de lograr un grado de protección bastante alto. Por otro lado, algunos negocios han gastado cantidades considerables de tiempo y dinero estableciendo soluciones volumétricas locales sólidas, lo cual funciona bien mientras sus dispositivos locales no se vean sobrepasados por el creciente tamaño de los ataques DDoS. El último detalle acerca de una solución híbrida es que su organización puede necesitar emplear múltiples administradores de incidentes para abordar ataques localmente y en la nube.

CÓMO FUNCIONA UNA SOLUCIÓN HÍBRIDA



NUBE

Depuración de tráfico de alto volumen, basada en la nube

Detección y mitigación en tiempo real de ataques DDoS volumétricos

Servicios con soporte 24x7x365 de expertos en seguridad

RED

Servicios de firewall de red en capas 3 y 4

Mitigación de ataques transitorios y de bajo volumen

Balanceo de cargas simple a un segundo nivel

IP reputation database *

APP

Mecanismos de defensa conscientes de aplicaciones y de uso intensivo de CPU

Mitigación de ataques asimétricos y basados en SSL

Terminación SSL

Firewall para aplicaciones web (WAF)

¿EXISTE UNA SOLUCIÓN IDEAL?

En el clima actual de ataques DDoS en constante evolución, está cada vez más claro que cada organización necesita considerar y adoptar una estrategia de protección contra DDoS. Soluciones locales integradas ofrecen un estricto control y flexibilidad, pero pueden verse rápidamente sobrepasadas por ataques volumétricos grandes. Servicios administrados de depuración en la nube ofrecen protección contra estos grandes ataques, pero pueden ser caros si son de uso exclusivo. Al usar una combinación de dispositivos de seguridad locales y un servicio de depuración en la nube para manejar ataques volumétricos, las organizaciones pueden mantener el control, al mismo tiempo que ponen en funcionamiento servicios de protección en la nube a manera que son necesarios para manejar las inundaciones volumétricas más grandes.

Al elegir cómo proteger de la mejor manera a su organización de ataques DDoS, debe tomar en cuenta la probabilidad de experimentar un ataque contra la habilidad de su organización para mitigarlo efectivamente. Tener proveedor único que le ofrezca servicios de protección constantes dentro de todos estos modelos para satisfacer sus necesidades hoy y a manera que éstas evolucionan puede ser una ventaja clave. Sea lo que sea que decida, sea proactivo en su defensa contra DDoS. Garantice la continuidad de su sitio y sus servicios estableciendo su solución – antes de que sufra un ataque.

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com

RPRT-DDOS MYTHS