DefensePro: Protección y mitigación de ataques DDoS

Proteja sus centros de datos y su red contra nuevas amenazas

En el panorama actual de la seguridad informática, los ataques de denegación de servicio (DoS) y los ataques de denegación de servicio distribuidos (DDoS) son una de las principales amenazas a la disponibilidad de las redes. Los ataques DDoS pueden provenir de hacktivistas que buscan dar visibilidad a una causa, defraudadores que intentan obtener ilegalmente datos o fondos, o incluso eventos geopolíticos. En cualquier caso, está claro que estos ataques pueden ser un arma de destrucción cibernética. Los gobiernos y las empresas de servicios públicos, servicios financieros y comercio sufren ataques a diario.

Los ataques se tornan cada vez más sofisticados y graves, al punto que burlan los servicios tradicionales de protección CDN y protección en la nube para atacar la infraestructura informática y las aplicaciones críticas de una organización. La siguiente gráfica del Informe global de seguridad de aplicaciones y seguridad de redes 2014-2015 de Radware resalta una nueva tendencia: el crecimiento de los ataques constantes contra las organizaciones.

La simplicidad con la que se lanzan estos ciberataques y la variedad de herramientas de ataque disponibles son algunos de los motivos por los cuales las organizaciones sufren más ataques, como los ataques DDoS. Ya no se trata de prevenir los ataques, sino de detectarlos y mitigarlos.

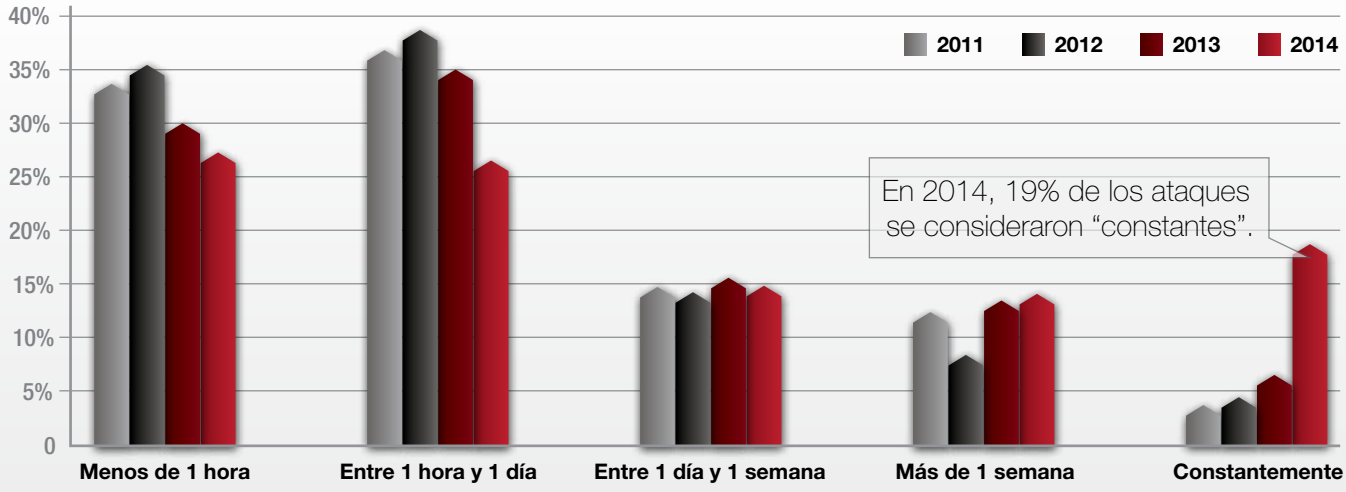

Figura 1: comparación interanual de la duración de los ataques

¿Qué hace DefensePro?

DefensePro es parte de la solución de mitigación de ataques de Radware y es un reconocido dispositivo perimetral de mitigación de ataques en tiempo real que protege a las organizaciones contra las nuevas amenazas a las redes y las aplicaciones. DefensePro protege la infraestructura contra la interrupción o la lentitud de las redes y las aplicaciones, la explotación de las vulnerabilidades de las aplicaciones, la diseminación de software malicioso, las anomalías en la red, el robo de información y otros tipos de ataques.

DefensePro ayuda a las organizaciones a ganar la batalla constante contra los ataques que afectan la disponibilidad gracias a que detecta y mitiga los ataques DoS/DDoS (tanto conocidos como ataques de día cero) en tiempo real. Esta solución protege contra otras amenazas de seguridad que las herramientas tradicionales de mitigación de ataques DDoS no detectan, como los ataques de desbordamiento basados en SSL, los ataques contra las páginas de inicio y los ataques que se lanzan detrás de una CDN.

Gracias a DefensePro, la solución de mitigación de ataques de Radware ofrece protección con el menor tiempo de mitigación y la mayor cobertura contra ataques. Radware brinda una solución híbrida que combina herramientas de mitigación locales y en la nube en una única solución integrada diseñada para bloquear de manera óptima múltiples vectores de ataque que ocurren en paralelo.

¿Por qué DefensePro?

DefensePro ofrece un conjunto integral de cuatro módulos esenciales de seguridad –protección anti-DDoS, análisis de comportamiento de la red, sistema de prevención de intrusiones (IPS) y protección contra ataques SSL (DefenseSSL)– para proteger completamente la infraestructura contra ataques conocidos y nuevos que pongan en riesgo la seguridad de la red. DefensePro emplea múltiples módulos de detección y mitigación que incluyen un análisis de comportamiento adaptativo, tecnologías de desafío-respuesta y detección de firmas.

Ventajas de DefensePro

- Análisis de comportamiento de la red (NBA), sistema de prevención de intrusiones (IPS) y protección contra ataques SSL (DefenseSSL)
- Inspección de hasta 300 Gbps
- Mitiga hasta 230M PPS de tráfico de ataque a la vez que mantiene la mejor experiencia
- Hasta 25 millones de sesiones simultáneas

En comparación con las soluciones independientes, la sinergia de múltiples módulos de seguridad en una única plataforma acelerada por hardware ofrece una protección más efectiva contra los atacantes que buscan amenazar sistemáticamente los activos de una empresa, a la vez que permite generar informes, realizar estudios forenses y cumplir con las normas vigentes.

DefensePro consiste en una tecnología de firmas en tiempo real, adaptativas y basadas en el comportamiento que detecta y mitiga los ataques de red, los ataques de minuto cero, los ataques DoS/DDoS, los ataques de abuso de aplicaciones, las detecciones de red y la diseminación del software malicioso. Además, elimina la necesidad de intervención humana y no bloquea el tráfico legítimo.

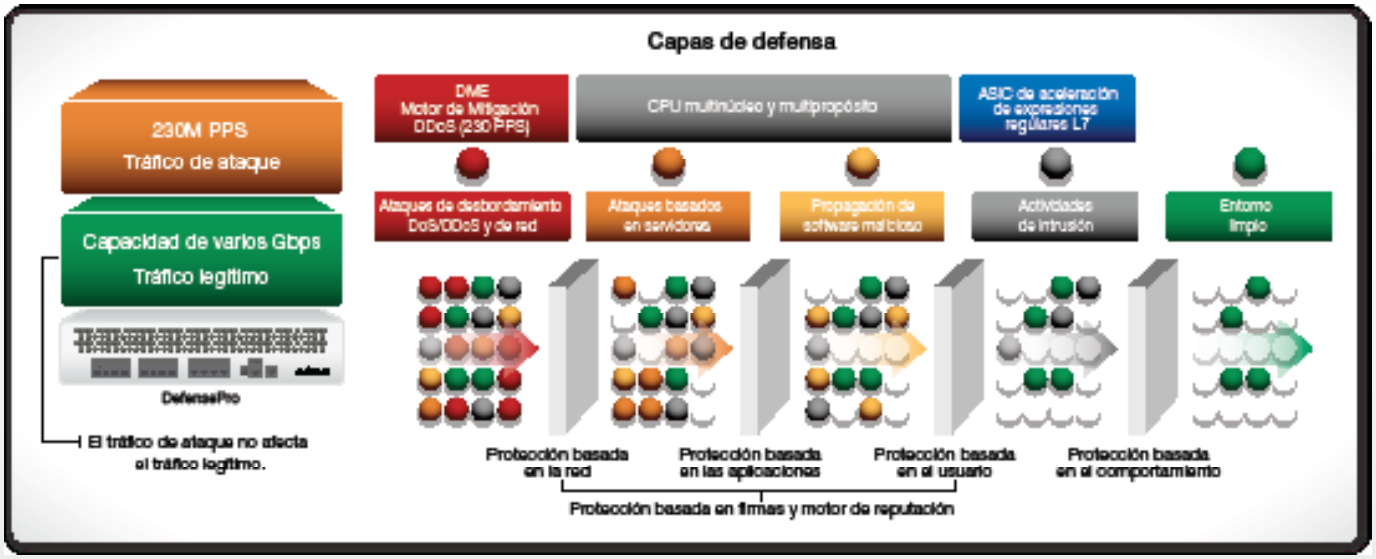

Figura 2: Arquitectura de DefensePro

Modos de implementación

Los dispositivos DefensePro se pueden implementar en serie, en derivación (*out-of-path*) o en un centro de depuración para maximizar la precisión de la mitigación y minimizar el tiempo de respuesta. Todos los modos de implementación ofrecen el mismo desempeño que un dispositivo en serie.

Si DefensePro se implementa en serie o en derivación y en un centro de depuración, los dispositivos se pueden comunicar entre ellos en tiempo real para obtener actualizaciones automáticas sobre los niveles de tráfico normales, detectar los patrones de comportamiento y obtener huellas digitales de los ataques. Este flujo constante en tiempo real de mensajes de defensa permite a DefensePro ofrecer una mitigación precisa e instantánea sin necesidad de aprender esta información cuando ocurre un ataque.

La implementación de los dispositivos DefensePro en derivación o en un centro de depuración es la solución más flexible o escalable, y se basa en la máxima capacidad de mitigación necesaria, sin verse limitada por la topología física real de la red.

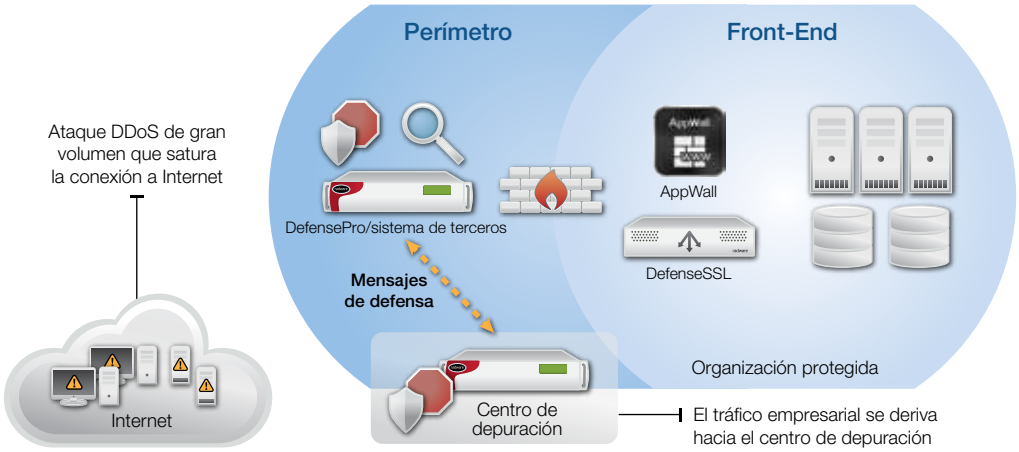

Figura 3: Dispositivo DefensePro instalado en serie en el perímetro empresarial para detectar y mitigar los ataques en tiempo real; el centro de depuración se invoca para mitigar los ataques de gran volumen que amenazan con saturar el enlace de Internet.

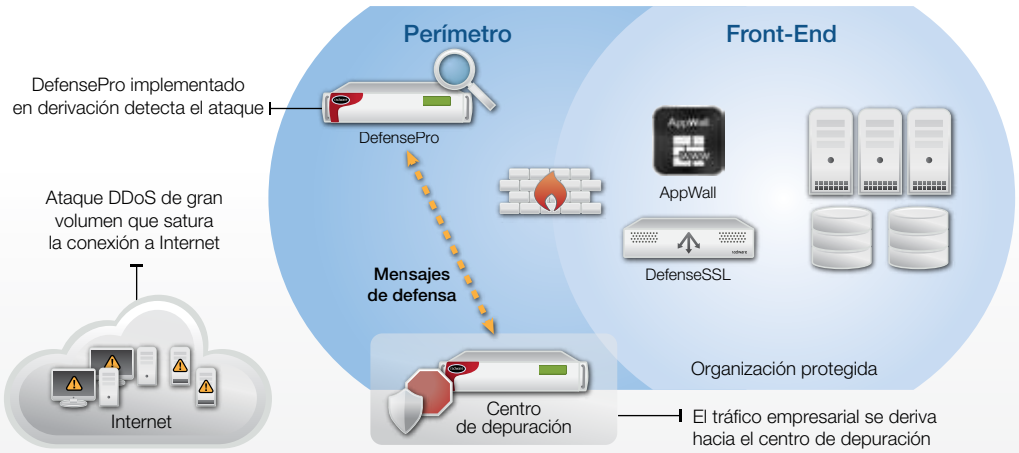

Figura 4: DefensePro implementado en derivación para la detección de ataques; el tráfico sospechoso se deriva al centro de depuración para la mitigación del ataque.

Solución híbrida e integrada

Además de los módulos de seguridad incorporados en DefensePro, la solución de mitigación de ataques de Radware incluye un motor de cifrado y descifrado SSL, un módulo WAF y un servicio de depuración para mitigación de ataques basado en la nube que se sincroniza con la solución local. Sin afectar el desempeño ni presentar riesgos, la solución de mitigación de ataques de Radware garantiza la continuidad comercial incluso durante un ataque.

La solución se complementa con un sistema centralizado de Gestión de Eventos de Seguridad Informática (SIEM), que ofrece una perspectiva unificada de la situación, y con el Equipo de Respuesta a Emergencias (ERT) de Radware, que ofrece atención 24x7 de expertos en seguridad para que los clientes que sufren ataques puedan mitigarlos en tiempo real y restablecer el funcionamiento normal.

El intercambio de mensajes específicos garantiza que cada uno de los módulos proporcione información sobre los niveles de tráfico normales y firmas en tiempo real a los otros, de manera que todos los componentes del sistema tienen visibilidad plena de toda la información.

Gracias a estos mensajes, la solución de mitigación de ataques de Radware puede detectar los ataques donde corresponde y mitigarlos en el punto ideal. Por ejemplo, el sistema puede detectar un ataque de gran volumen en el perímetro de la red pero mitigarlo en la nube. Esta característica automática en tiempo real permite a las organizaciones trasladar la mitigación tan lejos de la infraestructura como sea posible y así ampliar la capacidad de mitigación.

Beneficios comerciales

Mantenga la continuidad de las operaciones comerciales incluso cuando la red está bajo ataque

- Obtenga protección plena de las aplicaciones de los centros de datos contra nuevas amenazas de red
- Mantenga el desempeño de la red incluso ante ataques con muchos paquetes por segundo (PPS)
- Brinde al usuario un excelente tiempo de respuesta incluso cuando el sistema está bajo ataque

La mejor solución de seguridad para centros de datos en un paquete unificado

- DefensePro combina un sistema de prevención de intrusiones (IPS), análisis de comportamiento de la red (NBA), protección contra ataques de denegación de servicio (DoS) y DefenseSSL
- Detecte y prevenga los ataques con precisión sin bloquear el tráfico legítimo

Reduzca el costo total de propiedad (TCO) de la gestión de su sistema de seguridad

- Un arsenal de herramientas de seguridad en un único paquete
- Una única aplicación de gestión permite administrar múltiples unidades DefensePro en distintos centros de datos
- Plena protección de la inversión y mayor vida útil de la plataforma gracias al sistema de actualización progresiva de licencias que maximiza el retorno de la inversión y protege el capital

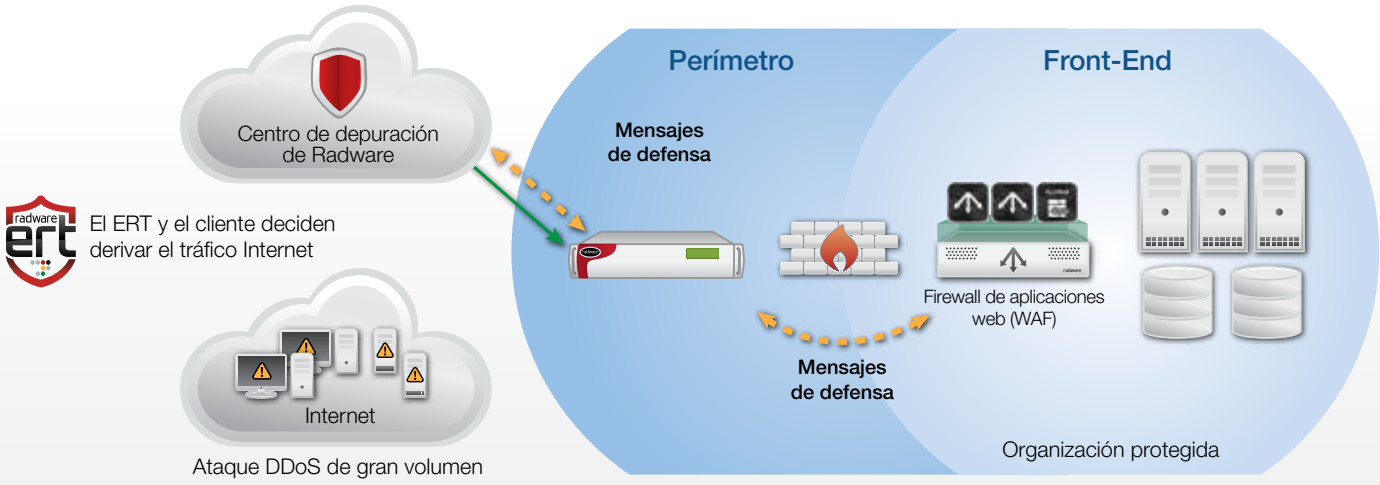

Figura 5: Implementación de una solución completa de mitigación de ataques

Ventajas

La **más amplia cobertura contra ataques**, que incluye detección y mitigación de los siguientes tipos de ataques:

- Ataques de desbordamiento DoS/DDoS conocidos y de día cero que desaprovechan el ancho de banda de la red
- Ataques DoS que desaprovechan los recursos de los servidores y las aplicaciones, tales como:
  - Ataques de desbordamiento DNS y HTTP/HTTPS
  - Barridos y ataques de desbordamiento SIP
  - Ataques web silenciosos (p. ej. ataques de fuerza bruta contra páginas de inicio, ataques basados en SSL)
  - Robo de información, barrido de aplicaciones
- Ataques que explotan las vulnerabilidades de los servidores de aplicaciones, como los servidores web, de correo, DNS, FTP y SQL

Alto rendimiento

- Inspección de hasta 300 Gbps
- Bloqueo de ataques con muchos paquetes por segundo (PPS), que sobrecargan los recursos de los equipos de red y seguridad (hasta 230M PPS)
- Solución de mitigación de ataques que se puede implementar tanto en serie como en derivación, lo cual maximiza la flexibilidad y la escalabilidad
- Tecnología de desafío-respuesta granular para la detección de redes de robots (botnets) avanzadas que imitan a los usuarios legítimos; mantiene un excelente tiempo de respuesta para los usuarios legítimos

Especificaciones y requisitos técnicos

Para obtener más información sobre las especificaciones o los requisitos técnicos, consulte las Especificaciones técnicas de los siguientes productos de Radware:

DefensePro Serie x4420
DefensePro Serie x420
DefensePro Serie x412
DefensePro Serie x06

Acerca de Radware

Radware® (NASDAQ: RDWR), es un líder global de entrega de aplicaciones y soluciones de seguridad cibernética para centros de datos virtuales, en la nube y definidos por software. Su galardonada cartera de soluciones ofrece un nivel de servicio garantizado para aplicaciones críticas para el negocio, al tiempo que maximiza la eficiencia informática. Las soluciones de Radware permiten que más de 10.000 clientes de todo el mundo, que incluyen empresas y proveedores, se adapten rápidamente a los desafíos del mercado, mantengan la continuidad de sus negocios y maximicen la productividad a la vez que minimizan los costos. Para obtener más información, visite www.radware.com.

Radware le recomienda que se una a nuestra comunidad y nos siga en: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, la aplicación Radware Connect para iPhone® y nuestro centro de seguridad DDoSWarriors.com, que proporciona un análisis completo sobre las herramientas, tendencias y amenazas relacionadas con los ataques DDoS.

Certainty Support

Radware ofrece asistencia técnica para todos sus productos a través del programa Certainty Support. Cada nivel del programa Certainty Support consiste en cuatro elementos: asistencia telefónica, actualizaciones de software, mantenimiento de hardware y asistencia en el lugar. Radware también tiene personal de ingeniería dedicado que puede ayudar a los clientes a implementar proyectos avanzados bajo la modalidad de servicios profesionales.

Más información

Para descubrir cómo las soluciones integradas de provisión y seguridad de aplicaciones de Radware pueden ayudarlo a aprovechar al máximo sus inversiones informáticas y comerciales, envíenos un correo electrónico a info@radware.com o visite www.radware.com.