PROTECCIÓN CONTRA DDOS

PROTECCIÓN

Descubra cómo defiende Kaspersky Lab a las empresas contra los ataques de DDoS

LOS CIBERCRIMINALES CENTRAN SU ATENCIÓN EN LAS EMPRESAS

Si su empresa alguna vez ha sufrido un ataque de denegación de servicio distribuido (DDoS, del inglés "Distributed Denial of Service"), ya sabrá que los costes financieros y de reputación pueden ser devastadores. No obstante, incluso si su empresa ha tenido la suerte de escapar de la atención de los cibercriminales y los hackers que lanzan estos ataques, puede que las perspectivas para el futuro no sean tan positivas.

EL VOLUMEN Y LA GRAVEDAD DE LOS ATAQUES ES CADA VEZ MAYOR

Lamentablemente, durante los últimos años, el coste de lanzar un ataque de DDoS ha disminuido de forma significativa, lo que significa que se están poniendo en marcha más ataques que nunca. Al mismo tiempo, los ataques de hoy en día son más complejos y se lanzan a una escala que puede saturar el ancho de banda de comunicaciones de la empresa objetivo en solo unos segundos, debilitando casi al instante los procesos empresariales internos y esenciales, y desactivando totalmente la presencia online de la empresa víctima.

Las empresas de todos los tamaños confían en sus infraestructuras de IT y sus sitios web para sustentar casi todos sus procesos críticos, y el tiempo de inactividad prolongado que puede ocasionar un ataque de DDoS no es una opción. Es evidente que, con el volumen, la magnitud y la gravedad de los ataques modernos, ya no es viable para ningún tipo de empresa posponer cualquier planificación de protección y mitigación contra ataques de DDoS hasta que llegue el momento en el que la infraestructura ya sea víctima de un ataque. Por el contrario, las empresas y las organizaciones del sector público deben ser conscientes de las amenazas y asegurarse de que ya disponen de las medidas de defensa adecuadas contra los ataques de DDoS.

"MÁS VALE PREVENIR QUE CURAR"

Cada empresa debe disponer de una estrategia contra ataques de DDoS preparada para "ponerse en marcha" en cuanto se detecte un ataque. En ese caso, si se produce un ataque, la empresa podrá mitigar los efectos sin dilación para:

- Minimizar el tiempo de inactividad de las infraestructuras y los procesos empresariales críticos
- Garantizar que los clientes puedan continuar accediendo a los servicios online
- Mantener la productividad de los empleados
- Minimizar los daños a su reputación

MÉTODOS DE ATAQUE DE DDOS

Los cibercriminales y hackers utilizan varias técnicas diferentes para implementar ataques de DDoS que desactivan o sobrecargan la infraestructura de IT de la empresa objetivo.

ATAQUES VOLUMÉTRICOS

Estos ataques son cada vez más frecuentes. Mediante la generación de niveles de tráfico que superan el ancho de banda disponible de la empresa objetivo, el ataque satura la capacidad de la conexión a Internet empresarial de la víctima y así desactiva o retrasa todas las actividades online.

ATAQUES A NIVEL DE APLICACIONES

Los ataques a nivel de aplicaciones intentan bloquear los servidores en los que se ejecutan aplicaciones esenciales, como los servidores web de los cuales depende de presencia online de la víctima.

OTRAS ATAQUES A INFRAESTRUCTURAS

Los ataques que tienen como objetivo la desactivación de equipos de red o sistemas operativos del servidor pueden detener totalmente el funcionamiento de los procesos empresariales esenciales.

ATAQUES HÍBRIDOS

Los cibercriminales también lanzan ataques complejos que combinan varios métodos, incluidos las técnicas de ataques volumétricos, ataques a nivel de aplicaciones y ataques a infraestructuras.

LA SOLUCIÓN COMPLETA DE DEFENSA Y MITIGACIÓN

La protección contra DDoS de Kaspersky ofrece una solución completa e integrada de protección y mitigación contra ataques DDoS que se ocupa de todas las fases necesarias para defender su empresa. La protección contra DDoS de Kaspersky incluye el análisis continuo de todo el tráfico online que le avisa de la posible presencia de un ataque; a continuación, recibe el tráfico redirigido, lo limpia y se lo devuelve "limpio". De esta forma, proporciona todo lo que su empresa necesita para defenderse de todos los tipos de ataque de DDoS y mitigar sus efectos.

LA PROTECCIÓN CONTRA DDOS DE KASPERSKY INCLUYE:

- Software del sensor de Kaspersky Lab que se ejecuta en su infraestructura de IT
- Servicios de nuestra red global de "centros de limpieza" del tráfico de datos
- Asesoramiento por parte de nuestro centro de operaciones de seguridad y expertos en protección contra DDoS
- Análisis e informes detallados posteriores al ataque

¿CÓMO FUNCIONA LA PROTECCIÓN CONTRA DDOS DE KASPERSKY?

El software del sensor de Kaspersky Lab recopila información sobre el tráfico de todas sus comunicaciones en cualquier momento durante todo el año. El sensor está instalado lo más cerca posible del recurso que desea proteger y recopila continuamente datos sobre su tráfico, incluidos los siguientes:

- Datos del encabezado
- Tipos de protocolo
- Número de bytes enviados y recibidos
- Número de paquetes enviados y recibidos
- Actividades y comportamiento de cada visitante de su sitio web
- Todos los metadatos acerca del tráfico

Toda esta información se envía a los servidores en la nube de Kaspersky Lab, donde se analiza para que podamos crear perfiles sobre cómo se comportan los visitantes habituales y perfiles de su tráfico normal, así como averiguar cómo puede variar este tráfico en función de la hora del día y el día de la semana, y determinar cómo pueden afectar los eventos especiales a sus patrones de tráfico. Con esta comprensión detallada de las "condiciones normales del tráfico" y los "comportamientos normales de los visitantes", nuestro servidores en la nube pueden evaluar con precisión las condiciones de su tráfico directo en tiempo real e identificar rápidamente las anomalías que pueden indicar que se ha lanzado un ataque contra su empresa.

Además, nuestros expertos en inteligencia sobre amenazas supervisan continuamente el panorama de amenazas de DDoS para identificar nuevos ataques. Esta inteligencia especializada ayuda a garantizar que los clientes de Kaspersky Lab se benefician de una respuesta rápida ante el lanzamiento de un ataque.

EVITAMOS LAS FALSAS ALARMAS... Y LUEGO LIMPIAMOS EL TRÁFICO

En cuanto nuestros servidores o expertos en inteligencia identifican un posible ataque contra su empresa, el Centro de operaciones de seguridad de Kaspersky Lab recibe una alerta. Para evitar falsas alarmas y trastornos innecesarios para su empresa, los ingenieros de Kaspersky Lab realizan las comprobaciones necesarias para confirmar si la anomalía o el comportamiento sospechoso del tráfico se debe a un ataque de DDoS. A continuación, nuestros ingenieros se ponen en contacto inmediatamente con su empresa para recomendarle que redirija su tráfico a nuestra red de centros de limpieza.

Durante el ataque, todo su tráfico pasa a través de uno de nuestros centros de limpieza, por lo que:

- La infraestructura ya no está saturada por el gran volumen de "tráfico basura".
- Nuestro proceso de limpieza descarta todo el tráfico basura.
- El tráfico legítimo se le devuelve desde nuestra red de centros de limpieza.

Además, todo el proceso es totalmente transparente para sus clientes y empleados.

LA CONFIGURACIÓN DE LA PROTECCIÓN ES RÁPIDA Y SENCILLA

Cuando elige la protección contra DDoS de Kaspersky, hay que realizar un número reducido de tareas de configuración antes de que se establezca la supervisión ininterrumpida y los canales de comunicaciones para los ataques "directos". Kaspersky Lab y sus partners pueden encargarse del proceso de configuración en la medida que usted necesite.

Si necesita una solución lista para usarse, Kaspersky Lab y sus partners pueden ayudarle a realizar la gran mayoría de los procesos de configuración, entre los que se incluyen los siguientes:

- Instalación del software y hardware del sensor en sus instalaciones
- Configuración de redirección del tráfico a nuestros centros de limpieza
- Configuración de la distribución del tráfico "limpio" a su empresa

A continuación, lo único que necesita es proporcionar un canal de Internet para el sensor con el fin de que la protección contra DDoS de Kaspersky pueda continuar recopilando datos cuando su principal canal de Internet haya sido desactivado debido a un ataque.

EL SENSOR: PERMITE LA SUPERVISIÓN ININTERRUMPIDA

El software del sensor de Kaspersky Lab se suministra completo con un sistema operativo Ubuntu de Linux estándar. Debido a que el software del sensor se ejecuta en un servidor x86 estándar (o en una máquina virtual*), no es necesario instalar hardware especial que deba mantener.

Debido a que el sensor se conecta al puerto SPAN (analizador de puerto conmutado, del inglés "Switched Port Analyzer"), puede obtener la mejor vista posible de todo el tráfico que fluye hacia dentro y fuera del recurso que protege.

En cuanto el sensor se conecta a la infraestructura, comienza a recopilar datos sobre el tráfico de entrada y de salida. Analiza los encabezados de cada paquete y envía información a los servidores en la nube de la protección contra DDoS de Kaspersky, en los que creamos perfiles estadísticos del "comportamiento normal del tráfico" y el "comportamiento normal de los visitantes" de su empresa.

Para mantener la privacidad de sus comunicaciones y ayudarle en el cumplimiento de las normativas, el sensor no captura el contenido de los mensajes que se generan en el ámbito de su tráfico de comunicaciones. El sensor solo recopila datos sobre el tráfico, por lo que la confidencialidad de sus mensajes jamás se verá perjudicada por ninguno de los procesos de la protección contra DDoS de Kaspersky.

*La máquina virtual debe cumplir o superar los requisitos mínimos de rendimiento especificados por Kaspersky Lab.

REDIRECCIÓN DEL TRÁFICO

En condiciones normales, mientras los servidores en la nube de protección contra DDoS de Kaspersky supervisan cualquier señal de un posible ataque de DDoS, el tráfico se distribuye directamente a su red corporativa. Su tráfico solo se redirige a nuestra red global de centros de limpieza cuando se ha detectado un ataque y su empresa ha confirmado que desea redirigir su tráfico.

La protección contra DDoS de Kaspersky le ofrece una amplia variedad de métodos de redireccionamiento:

- Protocolo de pasarela de borde (BGP, del inglés "Border Gateway Protocol")
- Sistema de nombres de dominio (DNS, del inglés "Domain Name System")

TÚNELES VIRTUALES DE ENCAPSULACIÓN DE ENRUTAMIENTO GENÉRICO (GRE)

Sea cual sea el mejor método de redireccionamiento para su empresa, los túneles virtuales de GRE se utilizan para permitir la comunicación entre la pasarela de borde (o router) y cada uno de los centros de limpieza de protección contra DDoS de Kaspersky correspondientes.

Si se lanza un ataque de DDoS contra su empresa, todo el tráfico se puede redirigir a uno de nuestros centros de limpieza. En ese caso, los túneles virtuales de GRE se utilizan para distribuir el tráfico limpio desde nuestros centros de limpieza a su empresa.

ELECCIÓN ENTRE BGP Y DNS

La configuración del redireccionamiento del tráfico mediante BGP o DNS dependerá en gran medida de la naturaleza de la infraestructura de IT y comunicaciones de su empresa:

- Para BGP, necesitará disponer de lo siguiente:
  - Una red independiente de proveedores que incluya los recursos que desea proteger
  - Un sistema autónomo

  Y la mayoría de las grandes empresas pueden cumplir estos criterios.

- Para DNS, deberá poder:
  - Administrar su propia zona de dominio para los recursos que desea proteger
  - Establecer el tiempo de vida (TTL, del inglés "Time to Live") de los registros de DNS en 5 minutos

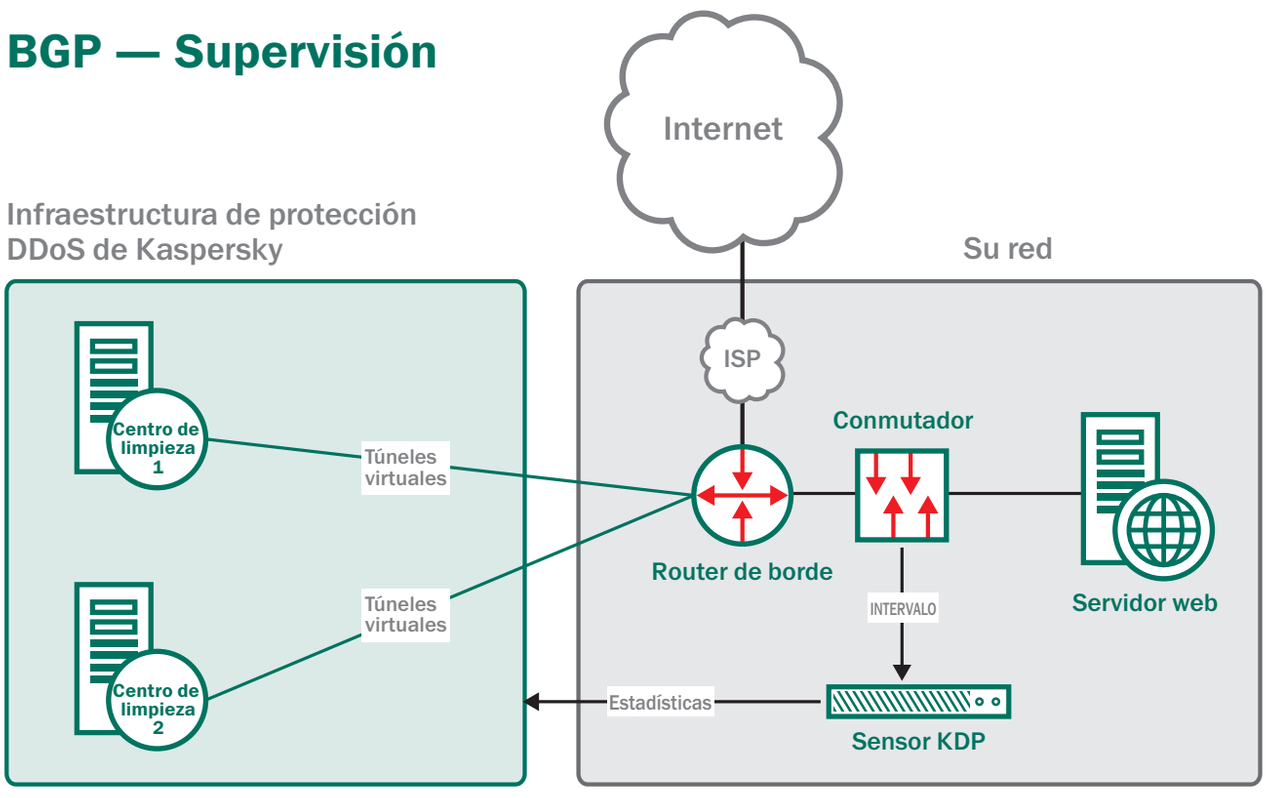
En general, durante un ataque, el método BGP consigue un redireccionamiento más rápido del tráfico, por lo que suele ser el método preferido para la mayoría de las empresas.

CÓMO FUNCIONA EL REDIRECCIONAMIENTO BGP

SUPERVISIÓN

En el modo de supervisión, todo el tráfico se distribuye directamente a su empresa. No obstante, los túneles virtuales de GRE están "en funcionamiento": sus routers y nuestros routers BGP intercambian con frecuencia información de estado, por lo que los centros de limpieza de protección contra DDoS de Kaspersky están preparados para recibir el tráfico redirigido cuando sea necesario.

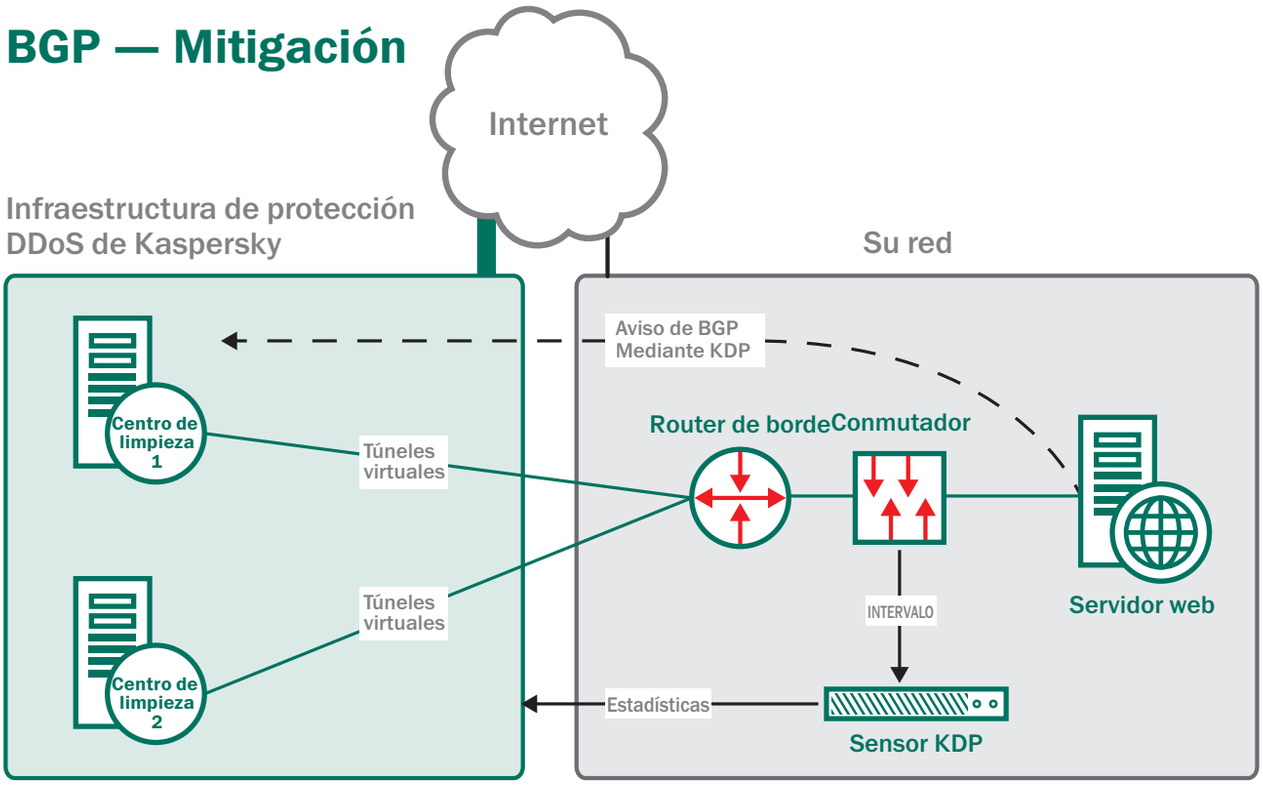
BGP — Supervisión



DURANTE UN ATAQUE

Cuando el sensor de Kaspersky Lab detecta una anomalía en el tráfico y los ingenieros de Kaspersky Lab confirman el inicio de un ataque, puede optar por redirigir todo el tráfico a un centro de limpieza de protección contra DDoS de Kaspersky.

Durante el ataque, el sensor de Kaspersky Lab continuará recopilando información y enviándola para que los servidores en la nube de la protección contra DDoS de Kaspersky la analicen.



DESPUÉS DE UN ATAQUE

Cuando el ataque se ha detenido, el tráfico se envía de nuevo directamente a su empresa. El sensor continúa recopilando datos sobre el tráfico y envía estos datos a nuestros servidores en la nube de forma ininterrumpida para que podamos optimizar continuamente nuestros perfiles de comportamiento para sus condiciones normales del tráfico.

Los túneles virtuales siguen en funcionamiento, intercambiando información de estado entre sus routers y los routers de Kaspersky Lab, por lo que la protección contra DDoS de Kaspersky está lista para actuar si se lanza otro ataque contra su empresa y usted decide optar por redirigir de nuevo el tráfico.

Los expertos de Kaspersky Lab también le proporcionarán análisis e informes detallados posteriores al ataque sobre la siguiente información:

- Qué ha sucedido durante el ataque
- Cuánto tiempo ha durado el ataque
- Como ha gestionado la protección contra DDoS de Kaspersky el ataque

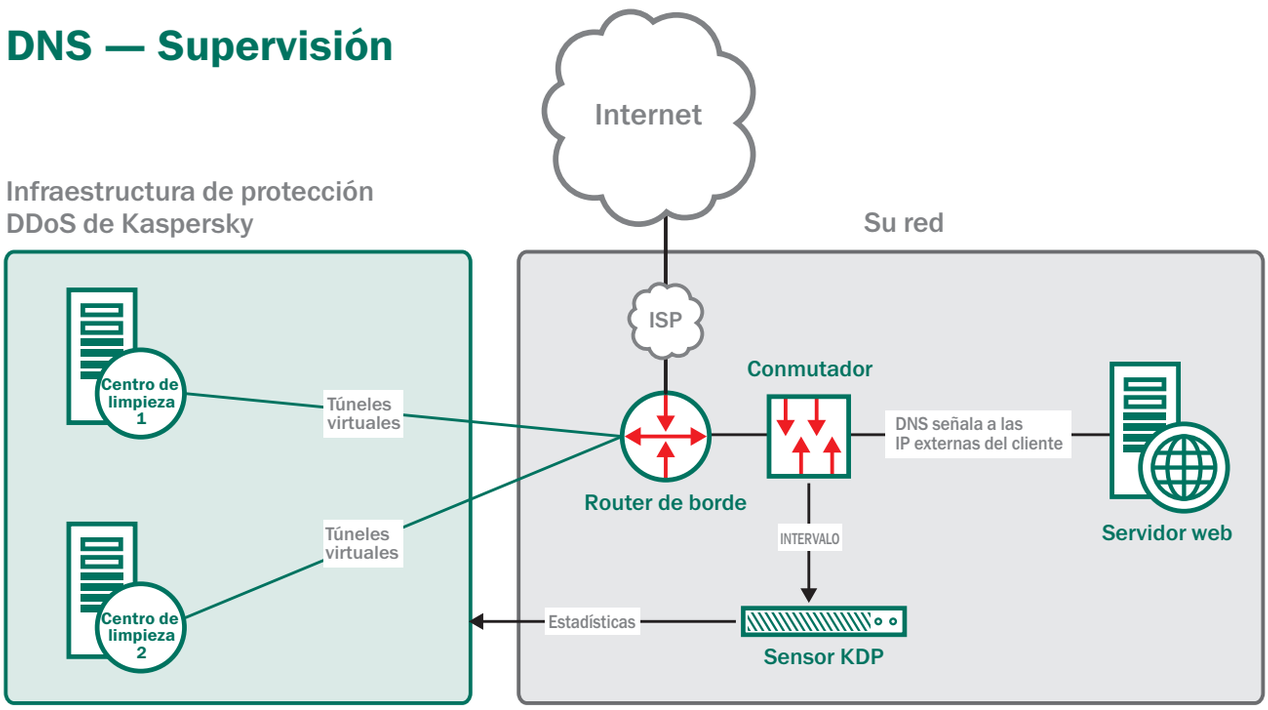
CÓMO FUNCIONA EL REDIRECCIONAMIENTO DNS

SUPERVISIÓN

Durante la configuración inicial, Kaspersky Lab asigna a su empresa una de las direcciones IP del grupo de protección contra DDoS de Kaspersky. Esta dirección se utilizará en el caso de que se produzca un ataque.

En el modo de supervisión, todo el tráfico se distribuye directamente en su empresa a través de su dirección o direcciones IP habituales. No obstante, los túneles virtuales de GRE están "en funcionamiento": sus routers y nuestros routers BGP intercambian con frecuencia información de estado, por lo que los centros de limpieza de protección contra DDoS de Kaspersky están preparados para recibir el tráfico redirigido cuando sea necesario.

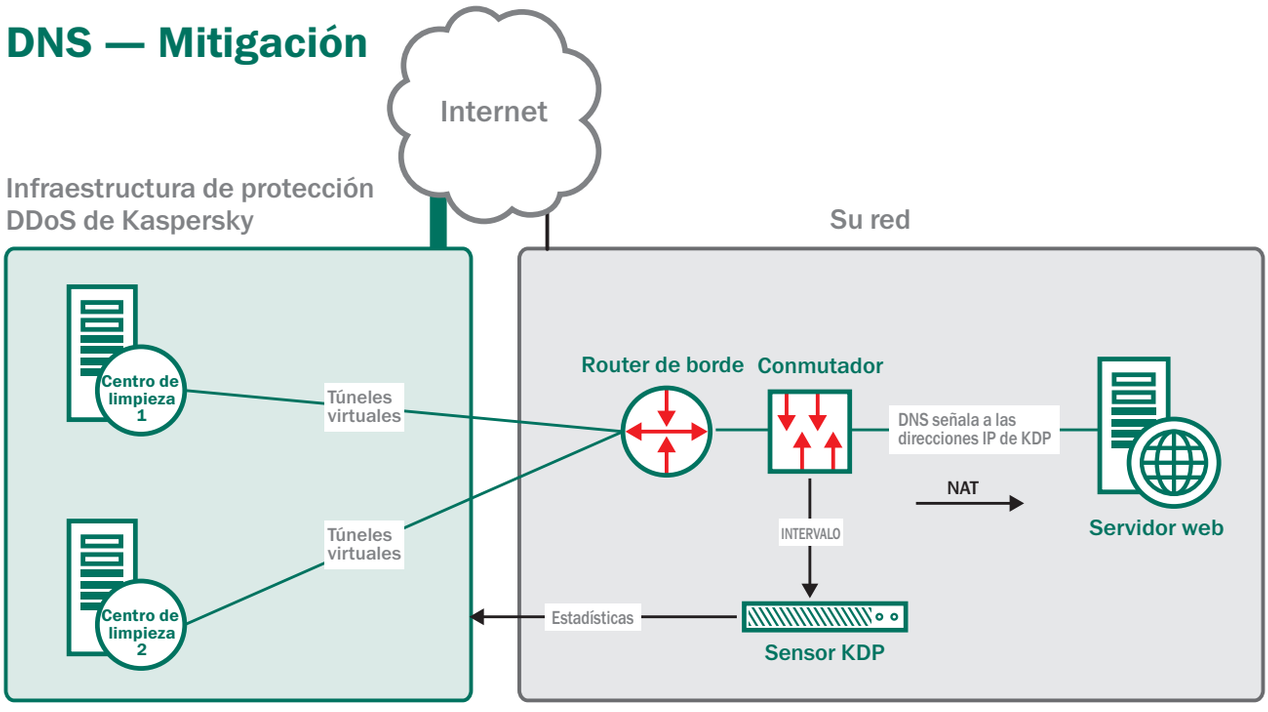
DNS — Supervisión



DURANTE UN ATAQUE

Cuando el sensor de Kaspersky Lab detecta una anomalía en el tráfico y los ingenieros de Kaspersky Lab confirman el inicio de un ataque, solo tiene que cambiar la dirección IP de la empresa en el registro DNS A para que su empresa utilice la dirección IP de la protección contra DDoS de Kaspersky que se le asignó durante la configuración inicial. Al mismo tiempo, como los hackers pueden atacar directamente su dirección IP, su ISP debe bloquear todo el tráfico a su dirección IP original, excepto las comunicaciones con la infraestructura de protección contra DDoS de Kaspersky Lab.

Al haber cambiado su dirección IP, todo el tráfico se redirige a los centros de limpieza de Kaspersky Lab. El tráfico "limpio" se vuelve a distribuir a su empresa desde nuestros centros de limpieza a través de los túneles virtuales de GRE.



DESPUÉS DE UN ATAQUE

Cuando el ataque se ha detenido, puede desbloquear su dirección IP original y cambiar el registro de DNS A para que el tráfico se envíe de nuevo directamente a su empresa.

El sensor de Kaspersky Lab continúa recopilando datos sobre el tráfico y envía estos datos a nuestros servidores en la nube de forma ininterrumpida para que podamos optimizar continuamente nuestros perfiles de comportamiento para sus condiciones normales del tráfico.

Los túneles virtuales siguen en funcionamiento, intercambiando información de estado entre sus routers y los routers de Kaspersky Lab, por lo que la protección contra DDoS de Kaspersky está lista para actuar si se lanza otro ataque contra su empresa y usted decide optar por redirigir de nuevo el tráfico.

Los expertos de Kaspersky Lab también le proporcionarán análisis e informes detallados posteriores al ataque sobre la siguiente información:

- Qué ha sucedido durante el ataque
- Cuánto tiempo ha durado el ataque
- Como ha gestionado la protección contra DDoS de Kaspersky el ataque

INTELIGENCIA SOBRE AMENAZAS PARA CONSEGUIR UNA MEJOR DEFENSA

Existe otro importante componente de defensa en la protección contra DDoS de Kaspersky, y es un componente que otros proveedores no pueden igualar.

Kaspersky Lab es el primer proveedor antimalware que proporciona una solución de protección contra DDoS, y esto significa que no existe ningún otro proveedor de protección contra DDoS que pueda igualar la experiencia y magnitud de nuestro departamento e infraestructura internos de inteligencia sobre seguridad.

Como parte de su labor de diseño de seguridad de IT de vanguardia, nuestros expertos en inteligencia sobre amenazas supervisan continuamente el panorama de amenazas para identificar nuevo malware y amenazas emergentes en Internet. Estos mismos expertos, y los mismos métodos sofisticados, también se utilizan para supervisar el panorama de amenazas de DDoS. Esta inteligencia especializada nos ayuda a detectar antes los ataques de DDoS para que su empresa pueda beneficiarse de una protección más rápida.

PROTECCIÓN A VARIOS NIVELES

Con una combinación única de supervisión continua de tráfico, análisis estadísticos y análisis del comportamiento, además de nuestra inteligencia especializada y proactiva sobre ataques de DDoS, ofrecemos una protección de DDoS más rigurosa.

DataSheet_DDoS/August14/Global