Redsys, error 403 usando Cloudflare

Introducción

Hoy me ha llamado la atención cuando un cliente me ha expuesto el problema, en el que su pasarela Redsys, le daba un error en el que tras un pogo, el retorno de Redsys, no se efectuaba, y por tanto el carrito quedaba pagado pero no figuraba como tal en la tienda. Sus pedidos quedaban pendientes de pago, pese a estar debidamente procesados en **Redsys.**

Al ir a buscar información me encuentro con post que dan mil vueltas, pero no llegan a la raíz y otros que dieron la apertura fácil (gracias, más abajo os enlazo)

Redsys como siempre, amables, pero poco operativos, le indicaron el que podía ser pero con escueta y difusa información. El cliente entendió un error de **java** y que tenía un error 403, que pudo ver en la intranet de cliente en redsys.

Error en pasarela intranet

Análisis

Lo primero que me vino a la cabeza fue ver los logs (lo primero que hay que hacer en cualquier análisis técnico) y allí descubrí que no había error 403. ¿Cómo es eso?

Viendo los logs de Apache, donde **no había** ningún error 403 asociado las path, algo extraño ocurría. Así que la siguiente prueba fue determinar su resolución DNS.

Todo quedó claro: el cliente usa CloudFlare como servicio de distribución, cacheado y seguridad de contenidos.

Y aquí estaba claro que la respuesta o callback que retorna la pasarela Redsys no llegaba al servidor y esto suele tener nombre proxy o firewall (tipo mod_security o desarrollo propio como el caso de Cloudflare)

Primera salida para solventarlo

Algunos lo primero y único que hacen es, desactivar el firewall, el camino más habitual en muchos técnicos (algunos intitulados como Especialista en CiberSeguridad) lo cual es un craso error.

Jamás debemos ir a lo fácil, por esto será difícil, tarde o temprano.

Análisis de logs de Cloudflare

En nuestro dashboard de Cloudflare, tenemos un área para el Firewall, y allí, tenemos un sistema de log de eventos llamado **Información general** donde podemos reviar el log, consultar por rangos de fechas.

Cloudflare > Firewall > Información General

Podemos crear una regla con esos datos, y tambien hacerlo directamente desde los botones que aparecen si ponemos el puntero del ratón encima de **Servicio** pero prefiero hacerlo desde el menú **Firewall > Reglas de firewall**

Añadir una regla en el firewall

Debemos pues añadir dos reglas con la condicional **Y**

ASN que es el número de Sistema Autónomo de la red que en este caso si es de apropiado ponerla porque es una red bancaria, y es confiable, y además es posible que nos cambien o modifiquen alguna vez la IP, que en este caso para la red de Redsys-Sermepa es el AS31627, pero solo usaremos la parte numérica. Y el identificador URI - Identificador de recursos uniforme del callback de nuestra aplicación de comercio electrónico.

Cloudflare > Firewall > Reglas de firewall

Por último nos queda añadir la acción a esta regla, que como vimos en el log, debería ser **Omitir > Comprobación de integridad del navegador**

Enlaces

- Ojo con Redsys y Cloudflare, revisa esto para que se registren los pagos
- Problemas con Redsys y Cloudflare (y como solucionarlos!)
- Cloudflare - Manage Rules in the Cloudflare dashboard

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Revision #2
Created 1 July 2021 20:47:50 by Abkrim
Updated 3 July 2021 06:30:24 by Abkrim