# Resolución de problemas de contenido y dominios de Akamai tras el cambio a Umbrella

## Contenido



## Introducción

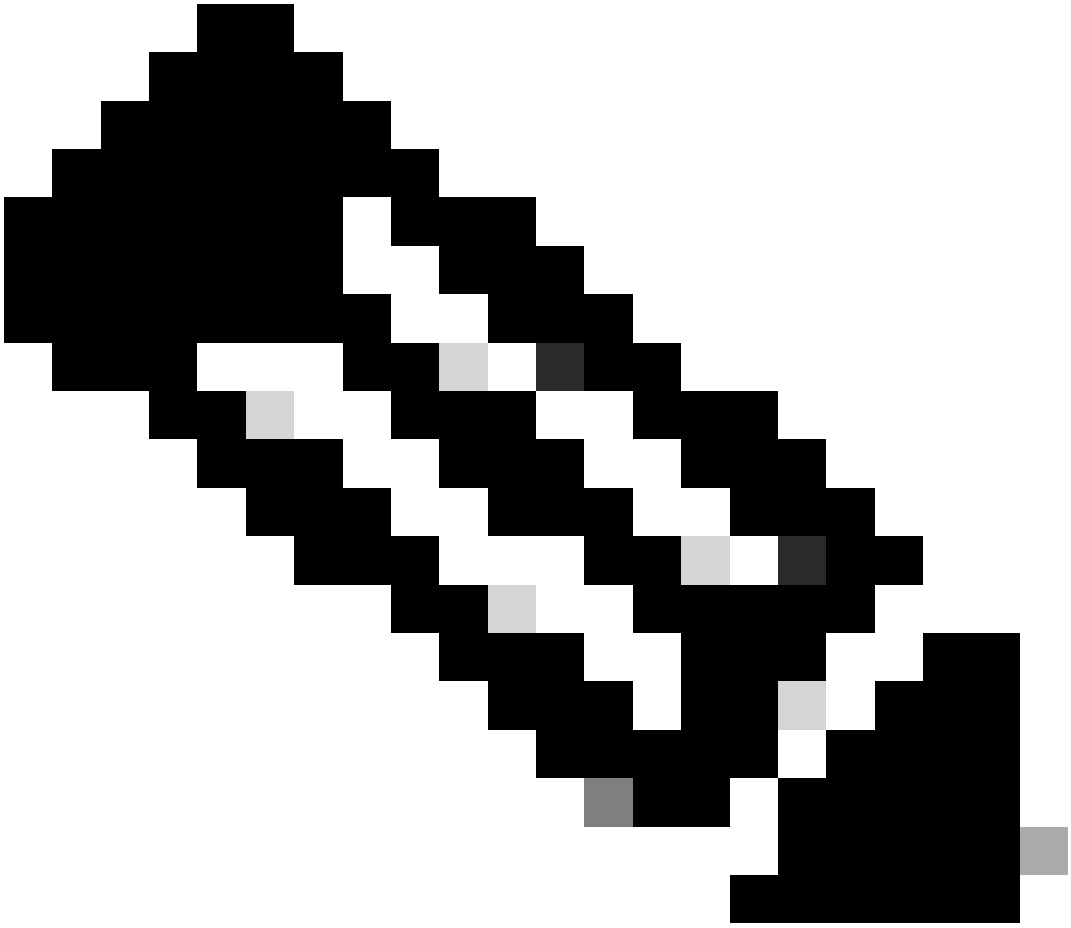
Este documento describe cómo resolver problemas con contenido y dominios servidos por Akamai después de cambiar a Cisco Umbrella.

## ¿Qué es Akamai y cómo se utiliza?

Akamai es una red de distribución de contenido (CDN) que almacena y suministra contenido a muchos proveedores de contenido de la Web. Esto incluye transmisión de vídeo, imágenes, contenido del sitio, guiones, publicidad y mucho más. Akamai es uno de los muchos CDN, como Amazon CloudFront o Limelight Networks, que constituyen la columna vertebral de muchos sitios populares.

Un CDN es utilizado por un sitio web porque tiene un tráfico muy alto, incluyendo picos de tráfico importantes (como cuando hay una noticia de último minuto). En lugar de pagar por su propia infraestructura de alojamiento para alojar su sitio (que debe ser lo suficientemente potente como para servir las horas punta, al tiempo que también lo deja parcialmente inactivo una gran parte del tiempo), los administradores web utilizan CDN, por lo que solo pagan por los recursos que realmente utilizan. Durante los tiempos lentos, el contenido se transmite utilizando menos recursos y, durante las horas punta, el CDN amplía sus recursos para servir a todos sin perder un solo compás. El resultado final es un sitio que tiene un tiempo de actividad mucho mejor y ahorra dinero para el administrador web. Akamai es uno de los más grandes de este tipo de CDN.

Para confirmar si un sitio web utiliza o no Akamai, busque www.sitename.com que señala a los subdominios como CNAME, como edgesuite.net, akamai.net, edgekey.net, amakaiedge.net (generalmente todos .net). Asegúrese de consultar www.domain.com en lugar de domain.com para comprobar si hay un CNAME de Akamai.



Nota: Algunos sitios solo utilizan Akamai para imágenes o contenido de vídeo dentro del sitio y solo las imágenes hacen referencia a un dominio suministrado por Akamai a través de CNAME.

## ¿El uso de Cisco Umbrella afecta al contenido de Akamai? ¿Por qué Umbrella me devuelve una IP diferente a la de mi ISP?

El uso de Cisco Umbrella no afecta al contenido de Akamai por sí solo, a menos que alguno de los dominios de Akamai esté bloqueado por una de sus listas de dominios. Recuerde que cualquier dominio agregado es un comodín automáticamente para todos los subdominios (por ejemplo: *.domain), por lo que al introducir "akamai.net" en la lista de bloqueo se rompen muchos sitios de la Web.

También puede haber diferencias entre la forma en que los servidores DNS de su ISP y Cisco Umbrella gestionan el tráfico de Akamai específicamente. Incluso puede darse el caso de que el DNS del ISP provoque la carga de contenido diferente. Es bastante común que la dirección IP

devuelta por el servidor DNS de un ISP difiera de la recibida al consultar a Cisco, pero eso no significa que los resultados de Cisco sean incorrectos. Lo contrario es cierto. Si bien los resultados difieren, esto se debe a que Cisco/OpenDNS y Akamai participan en el Global Internet SpeedUp Project mediante EDNS Client Subnet (ECS). Continúe leyendo este artículo para aprender cómo esto afecta la IP devuelta de la solicitud DNS.

## ¿Esto sólo afecta a Akamai?

No. Esto puede afectar a cualquier proveedor de CDN que utilice ECS. Akamai es la incidencia más frecuente.

## ¿Qué es ECS y cómo marca la diferencia?

ECS significa EDNS Client Subnet y forma parte del Global Internet SpeedUp Project diseñado para mejorar la funcionalidad y velocidad de los sitios web distribuidos (especialmente CDN) en todo el mundo.

Sin ECS: DNS se solicita desde el servidor DNS actual que, a continuación, consulta el servidor DNS autorizado del dominio y devuelve una dirección IP del servidor al que se va a conectar. Este servidor está cerca del servidor DNS consultado y puede estar muy lejos de su ubicación actual. El servidor DNS consultado determina qué servidor de contenido de la región se utiliza para proporcionar una respuesta. El usuario final puede estar muy lejos del servidor que proporciona contenido, lo que se traduce en velocidades bajas. Por ejemplo: El usuario A de Brasil consulta el conjunto de servidores DNS local, que resulta ser un servidor DNS de Miami. El servidor DNS de Miami devuelve una dirección IP de respuesta cercana a Miami para el dominio. El usuario A está frustrado porque la descarga es tan lenta y viene de los EE.UU..

Con ECS: DNS a un servidor DNS recursivo tiene la subred de origen (normalmente un /24) anexada a su solicitud DNS a los servidores DNS autorizados. El servidor autorizado para el dominio responde con una respuesta personalizada a lo que considera el mejor y más cercano servidor para atender la solicitud del usuario final. El usuario puede consultar un servidor DNS en cualquier lugar y obtener un servidor local para servir el contenido. Por ejemplo: El usuario A de Brasil consulta el conjunto de servidores DNS local, que resulta ser un servidor DNS de Miami. El servidor DNS tiene habilitado ECS en Miami y pasa al servidor DNS autorizado para el dominio del que proviene el usuario desde una subred en Brasil. A continuación, devuelve una dirección IP de respuesta de un Data Center de Sao Paulo (Brasil) para el dominio. El usuario A está contento de que el servidor DNS de Miami admita ECS y tenga una descarga rápida del proveedor de contenido.

## ¿Qué problemas puede causar al utilizar Cisco Umbrella?

La red DNS global de Cisco Umbrella y Akamai tienen ECS habilitado y, por lo tanto, responden con la mejor IP de servidor para su subred de salida actual de DNS. Esto puede convertirse en un problema cuando el balanceo de carga con ciertos ISP o cuando los ISP tienen problemas de ruteo en su extremo. Por ejemplo, un ISP puede tener un servidor Akamai interno y dirige a

cualquier persona que utilice sus servidores DNS ISP a este servidor local. A continuación, bloquean las IP de otros servidores de Akamai para obligar a todos a utilizar su servidor Akamai local y ahorrar así en costes de tránsito.

Al cambiar a Cisco, preguntamos directamente a Akamai cuál es el mejor servidor para la subred del usuario final, y Akamai responde directamente. Especialmente en conexiones con carga equilibrada, Akamai puede devolver una IP válida a la que el ISP no enruta correctamente.

Es en esta situación donde, después de cambiar a Cisco Umbrella, el contenido suministrado por Akamai no se carga de forma intermitente. La manifestación más común es con las páginas de noticias, tales como la carga como una estructura alámbrica de HTML sin el contenido rico. Los problemas más frecuentes son con el cable de Time Warner del ISP (RoadRunner).

Es importante tener en cuenta que la IP devuelta por Cisco Umbrella para el contenido de Akamai es válida en estos casos y que el ISP agota el tiempo de espera, ya que no realiza la conexión. Para confirmar que se trata realmente de este tipo de problema, pruebe exactamente la misma IP en un dispositivo con un tipo diferente de conexión de red, como un teléfono móvil con datos móviles.

Si no obtiene una dirección IP en respuesta a una solicitud de DNS a Cisco Umbrella, se trata de un problema diferente. Póngase en contacto con support@umbrella.com para obtener ayuda. Este caso solo se aplica cuando las páginas no se cargan cuando Cisco Umbrella responde con una dirección IP de Akamai válida.

## ¿Quién puede ayudar si esto está sucediendo?

El ISP es la única parte que puede ayudar a resolver este problema. Esto se debe a que la solicitud DNS devuelve una dirección IP a la que el ISP agota el tiempo de espera mientras el resto del mundo puede conectarse a esa misma IP. Cisco Umbrella ha completado su parte en la devolución de una dirección IP válida en respuesta a la solicitud DNS. El ISP no ha completado su parte en el enrutamiento de datos a esta dirección IP. Su suscripción al ISP es para permitir el acceso a los recursos de Internet y esto es una falla al hacerlo de su lado.

El ISP es el único capaz de resolver problemas de ruteo entre su red y sus pares; Cisco Umbrella no tiene visibilidad y no puede solucionar este problema de routing. Solo podemos mostrar que estamos devolviendo una IP válida y a la que no se puede enrutar.

Ejemplo: Domain.com es un CNAME para a1234.a.akamaiedge.net que apunta a la IP 1.2.3.4. Conexiones a 1.2.3.4 tiempo de espera. Al ejecutar un traceroute, obtenemos 8 pasos, más allá del ISP pero luego dejamos de obtener devoluciones.

Ejemplo de problema y solución: Después de hablar con el ISP, el problema era que el rango de IP del ISP no tiene una ruta de retorno de Akamai a la IP del usuario dentro del espacio del ISP. El ISP presentó dos opciones: 1) Espere a que Akamai vuelva a agregar una ruta a esta IP o 2) Cambie las IP dentro de los intervalos del ISP por una IP que tenga una ruta de retorno de Akamai que funcione.

¿Necesita ayuda para trabajar con su ISP? Podemos ayudar a explicar y proporcionar evidencia

con la confirmación de que la IP devuelta del registro A de Akamai es válida de Akamai a través de nuestros resolvers.

## Consejos de Troubleshooting

¿Cree que este problema le afecta, pero no está seguro? A continuación, se ofrecen algunas sugerencias útiles para la solución de problemas. Estos pasos son necesarios para que nuestro equipo de soporte pueda ayudarle. Una vez recopilada esta información, póngase en contacto con support@umbrella.com para obtener ayuda.

1. Intente utilizar **nslookup queries** para los dominios que están siendo problemáticos. En este ejemplo se utiliza www.foxnews.com, que es un sitio de Akamai en el momento de escribir este documento.
    - **nslookup** www.foxnews.com
    - **nslookup** www.foxnews.com 8.8.8.8
    - **nslookup** www.foxnews.com 208.67.222.222
    - **nslookup** www.foxnews.com 208.67.220.220
2. Uso:**traceroutes** Depende del sistema operativo, puede ser **tracert** (Windows) o **traceroute** (OS X). En este caso, está intentando realizar un seguimiento del FQDN, así como de las direcciones IP obtenidas en el paso 1.
    - **tracert** www.foxnews.com
    - **tracert** <IP resultante de **nslookup**www.foxnews.com>
    - **tracert** <IP resultante de **nslookup**www.foxnews.com 8.8.8.8>
    - **tracert** <IP resultante de **nslookup**www.foxnews.com 208.67.222.222>
3. Recopile una lista de los dominios e IP a los que no puede acceder; pueden compartir una infraestructura de host de Akamai común que está bloqueando el ISP.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).