

Dépannage du contenu et des domaines desservis par Akamai après le passage à l'infrastructure

Table des matières

[Introduction](#)

[Qu'est-ce qu'Akamai et comment est-il utilisé ?](#)

[L'utilisation de Cisco Umbrella affecte-t-elle le contenu Akamai ? Pourquoi Umbrella me renvoie-t-il une adresse IP différente de celle de mon FAI ?](#)

[Cela affecte-t-il uniquement Akamai ?](#)

[Qu'est-ce qu'ECS et en quoi cela fait-il une différence ?](#)

[Quels sont les problèmes que cela peut provoquer lors de l'utilisation de Cisco Umbrella ?](#)

[Qui peut aider si cela se produit ?](#)

[Conseils de dépannage](#)

Introduction

Ce document décrit comment résoudre les problèmes liés au contenu et aux domaines desservis par Akamai après la commutation vers [Cisco Umbrella](#).

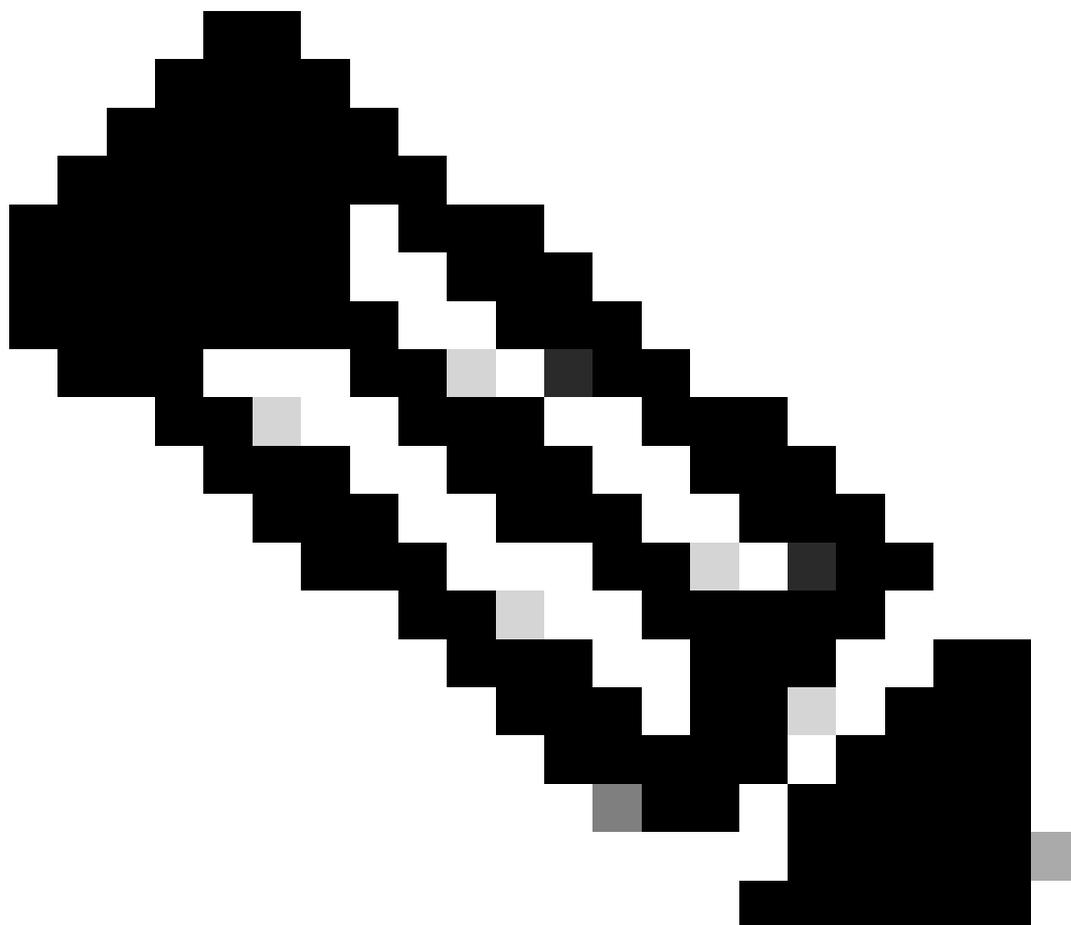
Qu'est-ce qu'Akamai et comment est-il utilisé ?

Akamai est un [réseau de diffusion de contenu \(CDN\)](#) qui stocke et fournit du contenu à de nombreux fournisseurs de contenu sur le Web. Cela inclut la diffusion de vidéos, d'images, de contenu de site, de scripts, de publicités, etc. Akamai est l'un des nombreux CDN, tels qu'Amazon CloudFront ou Limelight Networks, qui constituent l'épine dorsale de nombreux sites populaires.

Un CDN est utilisé par un site Web parce qu'il a un trafic très élevé, y compris des pics de trafic majeurs (comme lorsqu'il y a une actualité de dernière minute). Plutôt que de payer leur propre infrastructure d'hébergement pour héberger leur site (qui doit être suffisamment puissante pour répondre aux heures de pointe tout en le laissant partiellement inactif une grande partie du temps), les administrateurs Web utilisent des CDN pour ne payer que les ressources qu'ils utilisent réellement. Pendant les périodes de faible activité, le contenu circule en utilisant moins de ressources et pendant les périodes de pointe, le CDN augmente ses ressources pour servir tout le monde sans perdre de temps. Le résultat final est un site qui a beaucoup plus de temps de disponibilité et économise de l'argent pour l'administrateur Web. Akamai est l'un des plus grands de ce type de CDN.

Pour confirmer si un site Web utilise ou non Akamai, recherchez [www.sitename.com](#) pointant vers des sous-domaines en tant que CNAME tels que edgesuite.net, akamai.net, edgekey.net,

amakaiedge.net (généralement tous .net). Assurez-vous de rechercher www.domain.com plutôt que domain.com pour vérifier s'il y a un CNAME Akamai.



Remarque : Certains sites utilisent Akamai uniquement pour des images ou du contenu vidéo sur le site et seules les images font référence à un domaine desservi par Akamai via CNAME.

L'utilisation de Cisco Umbrella affecte-t-elle le contenu Akamai ? Pourquoi Umbrella me renvoie-t-il une adresse IP différente de celle de mon FAI ?

L'utilisation de Cisco Umbrella n'affecte pas le contenu d'Akamai seul, sauf si l'un de vos domaines Akamai est bloqué par l'une de vos listes de domaines. N'oubliez pas que tout domaine ajouté est automatiquement un caractère générique pour tous les sous-domaines (par exemple : *.domain), si vous entrez « akamai.net » dans votre liste de blocage, vous perdrez de nombreux

sites sur le web.

Il peut également y avoir des différences entre la façon dont les serveurs DNS de votre FAI et Cisco Umbrella gèrent spécifiquement le trafic Akamai. Il peut même arriver que le DNS du FAI entraîne le chargement d'un contenu différent. Il est assez courant que l'adresse IP renvoyée par le serveur DNS d'un FAI diffère de celle reçue lors de l'interrogation de Cisco, mais cela ne signifie pas que les résultats de Cisco sont incorrects. Le contraire est vrai. Bien que les résultats soient différents, c'est parce que Cisco/OpenDNS et Akamai participent au [projet Global Internet Speedup](#) en utilisant le sous-réseau client EDNS (ECS). Continuez à lire cet article pour savoir comment cela affecte l'IP retournée par la requête DNS.

Cela affecte-t-il uniquement Akamai ?

Non. Cela peut affecter n'importe quel fournisseur CDN qui utilise ECS. Akamai est l'occurrence la plus courante.

Qu'est-ce qu'ECS et en quoi cela fait-il une différence ?

ECS est l'acronyme de EDNS Client Subnet, et fait partie du [Global Internet Speedup Project](#) conçu pour améliorer la fonctionnalité et la vitesse des sites web distribués (notamment les CDN) à travers le monde.

Sans ECS : DNS est demandé à partir de votre serveur DNS actuel qui interroge ensuite le serveur DNS de référence du domaine et retourne une adresse IP du serveur auquel se connecter. Ce serveur est proche de celui du serveur DNS interrogé et peut être très éloigné de votre emplacement actuel. Le serveur DNS interrogé détermine le serveur de contenu de la région utilisé pour fournir une réponse. L'utilisateur final peut être très éloigné du serveur fournissant du contenu, ce qui entraîne des vitesses lentes. Exemple : L'utilisateur A au Brésil interroge le serveur DNS local qui se trouve être un serveur DNS à Miami. Le serveur DNS de Miami renvoie une adresse IP de réponse proche de Miami pour le domaine. L'utilisateur A est frustré par la lenteur du téléchargement et le fait qu'il provienne des États-Unis.

Avec ECS : Le sous-réseau source (généralement /24) du DNS vers un serveur DNS récursif est ajouté à sa requête DNS vers les serveurs DNS de référence. Le serveur faisant autorité pour le domaine répond avec une réponse personnalisée à ce qu'il croit être le meilleur serveur le plus proche pour répondre à la demande de l'utilisateur final. L'utilisateur peut interroger un serveur DNS n'importe où et obtenir un serveur local pour servir le contenu. Exemple : L'utilisateur A au Brésil interroge le serveur DNS local qui se trouve être un serveur DNS à Miami. ECS est activé sur le serveur DNS à Miami et passe sur le serveur DNS faisant autorité pour le domaine dont l'utilisateur provient d'un sous-réseau au Brésil. Il renvoie ensuite une adresse IP de réponse pour un centre de données de Sao Paulo, au Brésil, pour le domaine. L'utilisateur A est heureux que le serveur DNS de Miami prenne en charge ECS et propose un téléchargement rapide auprès du fournisseur de contenu.

Quels sont les problèmes que cela peut provoquer lors de

L'utilisation de Cisco Umbrella ?

Le réseau DNS global de Cisco Umbrella et Akamai sont activés pour ECS et répondent donc avec la meilleure adresse IP de serveur pour votre sous-réseau de sortie actuel de DNS. Cela peut devenir un problème lors de l'équilibrage de charge avec certains FAI ou lorsque les FAI ont des problèmes de routage à leur extrémité. Par exemple, un FAI peut avoir un serveur Akamai interne et dirige toute personne utilisant ses serveurs DNS FAI vers ce serveur local. Ils bloquent ensuite les adresses IP des autres serveurs Akamai pour forcer tout le monde à utiliser leur serveur local Akamai afin de réduire les coûts de transit.

Lorsque vous passez à Cisco, nous demandons directement à Akamai quel est le meilleur serveur à utiliser pour le sous-réseau de l'utilisateur final, et Akamai répond directement. En particulier sur les connexions à charge équilibrée, Akamai peut retourner une adresse IP valide vers laquelle le FAI ne se dirige pas correctement.

C'est dans ce scénario que, après la commutation vers Cisco Umbrella, le contenu desservi par Akamai ne se charge pas par intermittence. La manifestation la plus courante est avec les pages d'actualités telles que le chargement en tant que filaire de HTML sans le contenu riche. Les problèmes les plus courants concernent le câble Time Warner (RoadRunner) du FAI.

Il est important de noter que l'adresse IP renvoyée par Cisco Umbrella pour le contenu Akamai est valide dans ces cas et que le FAI expire car il n'établit pas la connexion. Pour confirmer qu'il s'agit bien de ce type de problème, testez exactement la même adresse IP sur un périphérique sur un autre type de connexion réseau, tel qu'un téléphone portable sur des données mobiles.

Si vous n'obtenez pas d'adresse IP en réponse à une requête DNS adressée à Cisco Umbrella, il s'agit d'un problème différent. Contactez support@umbrella.com pour obtenir de l'aide. Ce cas s'applique uniquement lorsque les pages ne sont pas chargées lorsque Cisco Umbrella répond avec une adresse IP Akamai valide.

Qui peut aider si cela se produit ?

Votre FAI est le seul à pouvoir vous aider à résoudre ce problème. En effet, la requête DNS renvoie une adresse IP à laquelle le FAI expire pendant que le reste du monde peut se connecter à cette même adresse IP. Cisco Umbrella a rempli sa part de travail en renvoyant une adresse IP valide en réponse à la requête DNS. Le FAI n'a pas terminé sa partie du routage des données vers cette adresse IP. Votre abonnement auprès du FAI vous permet d'accéder aux ressources Internet, ce qui n'est pas le cas de votre part.

Le FAI est le seul à pouvoir dépanner le routage entre son réseau et ses homologues ; Cisco Umbrella n'a aucune visibilité et ne peut pas résoudre ce problème de routage. Nous ne pouvons que montrer que nous retournons une adresse IP valide et qu'elle ne peut pas être routée vers.

Exemple : Domain.com est un CNAME pour a1234.a.akamaiedge.net qui pointe vers l'IP 1.2.3.4. Les connexions vers 1.2.3.4 dépassent le délai d'attente. Lors de l'exécution d'une commande traceroute, nous obtenons 8 étapes, après le FAI, mais cessons ensuite d'obtenir des retours.

Exemple de problème et de solution : Après avoir parlé au FAI, le problème était que la plage IP du FAI n'a pas de route de retour d'Akamai vers l'IP de l'utilisateur dans l'espace du FAI. Le FAI a présenté deux options : 1) Attendez qu'Akamai rajoute une route à cette adresse IP ou 2) Remplacez les adresses IP comprises dans les plages du FAI par une adresse IP dont la route de retour depuis Akamai fonctionne.

Besoin d'aide pour travailler avec votre FAI ? Nous pouvons vous aider à expliquer et à fournir des preuves confirmant que l'adresse IP renvoyée par l'enregistrement A d'Akamai est valide à partir d'Akamai via nos résolveurs.

Conseils de dépannage

Pensez-vous que ce problème vous affecte, mais vous n'en êtes pas sûr ? Voici quelques conseils utiles pour le dépannage. Ces étapes sont nécessaires pour que notre équipe d'assistance puisse vous aider. Une fois ces informations collectées, contactez support@umbrella.com pour obtenir de l'aide.

1. Essayez d'utiliser `nslookup` queries pour le ou les domaines qui posent problème. Cet exemple utilise www.foxnews.com, qui est un site alimenté par Akamai au moment de la rédaction de cet article.
 - `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. Utilisation: `tracert` / `tracert` Dépendant du système d'exploitation, il peut s'agir de `tracert` (Windows) ou `tracert` (OS X). Dans ce cas, vous tentez de suivre le nom de domaine complet (FQDN) ainsi que les adresses IP obtenues à l'étape 1.
 - `tracert www.foxnews.com`
 - `tracert <adresse IP résultante de nslookupwww.foxnews.com>`
 - `tracert <adresse IP résultante de nslookupwww.foxnews.com 8.8.8.8>`
 - `tracert <adresse IP résultante de nslookupwww.foxnews.com 208.67.222.222>`
3. Rassemblez une liste des domaines et des adresses IP que vous ne pouvez pas atteindre, ils peuvent partager l'infrastructure d'hôte Akamai commune bloquée par votre FAI.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.