Fehlerbehebung bei von Akamai bereitgestellten Inhalten und Domänen nach dem Wechsel zu Umbrella

Inhalt

Einleitung

Was ist Akamai und wie wird es angewendet?

Betrifft die Verwendung von Cisco Umbrella die Inhalte von Akamai? Warum erhalte ich von Umbrella eine andere IP-Adresse als mein ISP?

Betrifft dies nur Akamai?

Was ist ECS, und wie macht es einen Unterschied?

Welche Probleme können durch die Verwendung von Cisco Umbrella verursacht werden?

Wer kann helfen, wenn das geschieht?

Tipps zur Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie Sie nach dem Wechsel zu Cisco Umbrella Probleme mit von Akamai bereitgestellten Inhalten und Domänen beheben.

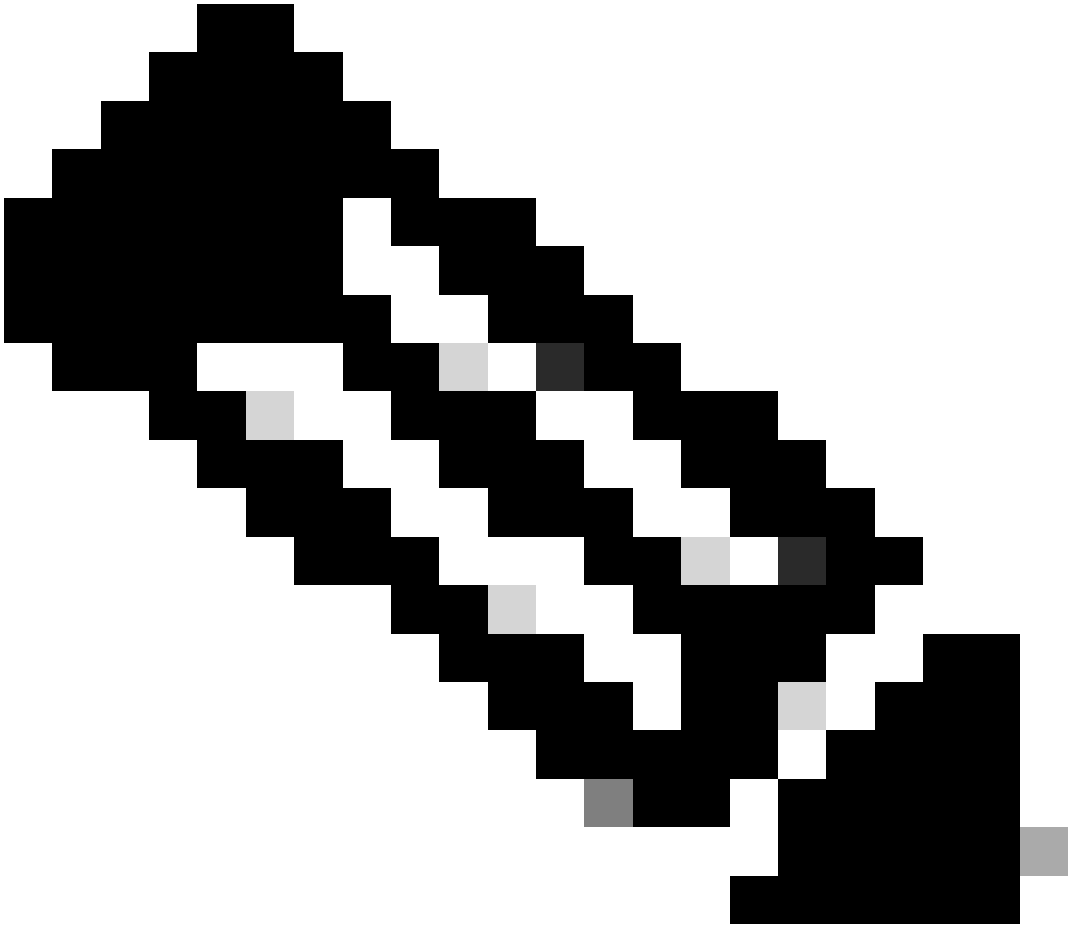
Was ist Akamai und wie wird es angewendet?

Akamai ist ein Content Delivery Network (CDN), das Content für viele Content Provider im Web speichert und bereitstellt. Dies umfasst Video-Streaming, Bilder, Inhalte, Skripte, Werbung und mehr. Akamai ist eines von vielen CDNs wie Amazon CloudFront oder Limelight Networks, die das Rückgrat vieler beliebter Websites bilden.

Ein CDN wird von einer Website verwendet, da der Datenverkehr dort sehr hoch ist, einschließlich hoher Verkehrsspitzen (z. B. bei aktuellen Meldungen). Anstatt für ihre eigene Hosting-Infrastruktur zu bezahlen, um ihre Website zu hosten (die leistungsstark genug sein muss, um Spitzenzeiten zu bedienen und es teilweise ungenutzt lassen einen großen Teil der Zeit), verwenden Web-Administratoren CDNs, sodass sie nur für die Ressourcen bezahlen, die sie tatsächlich nutzen. In Zeiten mit geringer Auslastung werden Inhalte über weniger Ressourcen übertragen, und in Zeiten mit starker Auslastung kann das CDN seine Ressourcen erweitern, um alle Beteiligten zu erreichen, ohne dass eine Taktrate verpasst wird. Das Endergebnis ist eine Website, die viel bessere Betriebszeit hat und spart Geld für den Web-Administrator. Akamai ist einer der größten dieser Art von CDN.

Um zu überprüfen, ob eine Website Akamai verwendet, suchen Sie nach www.sitename.com, die auf Subdomains als CNAME verweisen, z. B. edgesuite.net, akamai.net, edgekey.net,

amakaiedge.net (in der Regel alle .net). Achten Sie darauf, www.domain.com statt domain.com zu suchen, um herauszufinden, ob es einen Akamai CNAME gibt.



Anmerkung: Einige Websites verwenden Akamai nur für Bilder oder Videoinhalte innerhalb der Website, und nur Bilder verweisen auf eine Domain, die Akamai über CNAME anbietet.

Betrifft die Verwendung von Cisco Umbrella die Inhalte von Akamai? Warum erhalte ich von Umbrella eine andere IP-Adresse als mein ISP?

Die Verwendung von Cisco Umbrella hat keinen Einfluss auf Akamai-Inhalte als solche, es sei denn, eine Akamai-Domäne wird durch eine Ihrer Domänenlisten blockiert. Denken Sie daran, dass alle hinzugefügten Domänen automatisch ein Platzhalter für alle Subdomänen sind (z. B.: *.domain), sodass die Eingabe "akamai.net" in Ihre Sperrliste bricht viele Websites im Web.

Es kann auch Unterschiede zwischen der Art und Weise geben, wie die DNS-Server Ihres ISP und Cisco Umbrella Akamai-Datenverkehr spezifisch behandeln. Es kann sogar sein, dass der DNS des ISP dazu führt, dass verschiedene Inhalte geladen werden. Es ist durchaus üblich, dass die IP-Adresse, die vom DNS-Server eines ISP zurückgegeben wird, sich von der IP-Adresse unterscheidet, die beim Abfragen von Cisco empfangen wurde. Dies bedeutet jedoch nicht, dass die Ergebnisse von Cisco falsch sind. Das Gegenteil ist der Fall. Die Ergebnisse weichen zwar voneinander ab, doch liegt dies daran, dass Cisco/OpenDNS und Akamai am Global Internet Speedup Project unter Verwendung von EDNS Client Subnet (ECS) teilnehmen. Lesen Sie diesen Artikel weiter, um zu erfahren, wie sich dies auf die IP auswirkt, die von der DNS-Anforderung zurückgegeben wird.

Betrifft dies nur Akamai?

Nein. Dies kann sich auf jeden CDN-Anbieter auswirken, der ECS verwendet. Akamai ist das häufigste Vorkommen.

Was ist ECS, und wie macht es einen Unterschied?

ECS steht für EDNS Client Subnet und ist Teil des Global Internet Speedup Project, das die Funktionalität und Geschwindigkeit verteilter Websites (insbesondere CDNs) weltweit verbessern soll.

Ohne ECS: DNS wird von Ihrem aktuellen DNS-Server angefordert, der dann den Authoritative DNS-Server der Domäne abfragt und eine IP-Adresse des Servers zurückgibt, mit dem eine Verbindung hergestellt werden soll. Dieser Server befindet sich in der Nähe des abgefragten DNS-Servers und kann sich sehr weit von Ihrem aktuellen Standort entfernt befinden. Der abgefragte DNS-Server bestimmt, welcher Inhaltsserver der Region verwendet wird, um eine Antwort bereitzustellen. Der Endbenutzer kann sehr weit vom Server entfernt sein, der Inhalte bereitstellt, was zu langsamen Geschwindigkeiten führt. Beispiele: Benutzer A in Brasilien fragt den lokalen DNS-Server ab, der zufällig ein DNS-Server in Miami ist. Der DNS-Server in Miami gibt eine Antwort-IP-Adresse in der Nähe von Miami für die Domäne zurück. Benutzer A ist frustriert, dass der Download so langsam ist und aus den USA kommt.

Mit ECS: Bei DNS an einen rekursiven DNS-Server wird das Quell-Subnetz (in der Regel /24) an seine DNS-Anforderung an die autoritativen DNS-Server angefügt. Der autoritative Server für die Domäne antwortet mit einer benutzerdefinierten Antwort auf den Server, der seiner Meinung nach der nächstgelegene und beste Server ist, um die Anfrage des Endbenutzers zu erfüllen. Der Benutzer kann einen DNS-Server an einer beliebigen Stelle abfragen und trotzdem einen lokalen Server für den Inhalt erhalten. Beispiele: Benutzer A in Brasilien fragt den lokalen DNS-Server ab, der zufällig ein DNS-Server in Miami ist. Auf dem DNS-Server ist ECS in Miami aktiviert, und er wird an den autoritativen DNS-Server für die Domäne weitergeleitet, die der Benutzer von einem brasilianischen Subnetz bezieht. Anschließend wird eine Antwort-IP-Adresse für ein Rechenzentrum in Sao Paulo, Brasilien, für die Domäne zurückgegeben. Nutzer A freut sich, dass der DNS-Server in Miami ECS unterstützt und einen schnellen Download vom Content Provider hat.

Welche Probleme können durch die Verwendung von Cisco Umbrella verursacht werden?

Das globale DNS-Netzwerk von Cisco Umbrella und Akamai sind ECS-fähig und antworten daher mit der besten Server-IP-Adresse für Ihr aktuelles DNS-Ausgangs-Subnetz. Dies kann zu einem Problem werden, wenn der Lastenausgleich mit bestimmten ISPs erfolgt oder wenn ISPs auf ihrem Ende Routing-Probleme haben. Ein ISP kann beispielsweise einen internen Akamai-Server haben und jeden Benutzer, der seine ISP DNS-Server verwendet, an diesen lokalen Server weiterleiten. Anschließend blockieren sie die IPs anderer Akamai-Server, um alle Benutzer zu zwingen, ihren lokalen Akamai-Server zu verwenden, um Transitkosten zu sparen.

Beim Wechsel zu Cisco wird Akamai direkt gefragt, welcher Server am besten für das Endbenutzer-Subnetz geeignet ist, und Akamai antwortet direkt. Insbesondere bei Verbindungen mit Lastausgleich kann Akamai eine gültige IP-Adresse zurückgeben, an die der ISP nicht richtig routet.

In diesem Szenario wird der von Akamai bereitgestellte Inhalt nach dem Wechsel zu Cisco Umbrella gelegentlich nicht geladen. Die häufigste Manifestation ist mit Nachrichtenseiten wie das Laden als Wireframe von HTML ohne den reichen Inhalt. Die am häufigsten auftretenden Probleme betreffen das Zeitwarnkabel des ISP (RoadRunner).

Es ist wichtig zu beachten, dass die von Cisco Umbrella für Akamai-Inhalte zurückgegebene IP in diesen Fällen gültig ist und der ISP eine Zeitüberschreitung aufweist, da er die Verbindung nicht herstellt. Um zu bestätigen, dass es sich tatsächlich um diese Art von Problem handelt, testen Sie die exakt gleiche IP auf einem Gerät mit einem anderen Netzwerkverbindungstyp, z. B. einem Mobiltelefon mit mobilen Daten.

Wenn Sie als Antwort auf eine DNS-Anfrage an Cisco Umbrella keine IP-Adresse erhalten, handelt es sich um ein anderes Problem. Wenden Sie sich an support@umbrella.com, um Hilfe zu erhalten. Dieser Fall tritt nur ein, wenn Seiten nicht geladen werden, wenn Cisco Umbrella mit einer gültigen Akamai IP-Adresse antwortet.

Wer kann helfen, wenn das geschieht?

Ihr ISP ist die einzige Partei, die bei der Lösung dieses Problems helfen kann. Der Grund hierfür ist, dass die DNS-Anfrage eine IP-Adresse zurückgibt, an die der ISP eine Zeitüberschreitung sendet, während der Rest der Welt eine Verbindung mit genau dieser IP herstellen kann. Cisco Umbrella hat seinen Teil der Rückgabe einer gültigen IP-Adresse als Antwort auf die DNS-Anfrage abgeschlossen. Der ISP hat seine Aufgabe beim Routing der Daten zu dieser IP-Adresse noch nicht abgeschlossen. Ihr Abonnement beim ISP ermöglicht Ihnen den Zugriff auf Internetressourcen, was auf deren Seite nicht möglich ist.

Der ISP ist der einzige, der Routing-Probleme zwischen seinem Netzwerk und seinen Peers beheben kann. Cisco Umbrella bietet keine Transparenz und kann dieses Routing-Problem nicht beheben. Wir können nur anzeigen, dass wir eine gültige IP-Adresse zurückgeben, an die sie nicht weitergeleitet werden kann.

Beispiel: Domain.com ist ein CNAME für a1234.a.akamaiedge.net, der auf die IP 1.2.3.4 verweist. Verbindungen mit 1.2.3.4 Zeitüberschreitung. Bei der Ausführung einer Traceroute gehen wir acht Schritte vor den ISP, erhalten aber keine Rücksendungen mehr.

Beispiel für Problem und Lösung: Nach dem Gespräch mit dem ISP bestand das Problem darin, dass der IP-Bereich des ISP keine Rückroute von Akamai zurück zur IP des Benutzers innerhalb des Bereichs des ISP aufweist. Der ISP präsentierte zwei Optionen: 1) Warten Sie, bis Akamai eine Route zurück zu dieser IP hinzugefügt hat, oder 2) Ändern Sie die IPs innerhalb der Bereiche des ISP in eine IP-Adresse, für die die Rückroute von Akamai funktioniert.

Benötigen Sie Hilfe bei der Zusammenarbeit mit Ihrem ISP? Wir können helfen, zu erklären und Beweise mit der Bestätigung, dass die IP aus dem Akamai A-Datensatz zurückgegeben ist gültig von Akamai durch unsere Resolver.

Tipps zur Fehlerbehebung

Glauben Sie, dass Sie von diesem Problem betroffen sind, sind sich aber nicht sicher? Hier finden Sie einige hilfreiche Tipps zur Fehlerbehebung. Diese Schritte sind erforderlich, damit unser Support-Team Sie unterstützen kann. Wenn Sie diese Informationen erhalten haben, wenden Sie sich an support@umbrella.com.

1. Versuchen Sie, **nslookup queries** die problematische(n) Domäne(n) zu verwenden. In diesem Beispiel wird www.foxnews.com verwendet, eine von Akamai betriebene Website zum Zeitpunkt der Dokumenterstellung.
    - **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. Nutzung:**traceroutes** Je nach Betriebssystem kann dies **tracert** (Windows) oder **traceroute** (OS X) sein. In diesem Fall versuchen Sie, den FQDN sowie die IP-Adressen zu ermitteln, die Sie in Schritt 1 erhalten haben.
    - **tracert** www.foxnews.com
    - **tracert** <resultierende IP von **nslookup**www.foxnews.com>
    - **tracert** <resultierende IP von **nslookup**www.foxnews.com 8.8.8.8>
    - **tracert** <resultierende IP von **nslookup**www.foxnews.com 208.67.222.222>
3. Sammeln Sie eine Liste der Domänen und IPs, die Sie nicht erreichen können, sie können gemeinsame Akamai Host-Infrastruktur, die von Ihrem ISP blockiert wird teilen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.