Cisco Umbrella FAQs zu IP-basiertem Geoblocking

Inhalt

[Einleitung](#)

[Was ist, wenn sich meine Benutzer in den betroffenen Regionen mit einem Unternehmens-VPN außerhalb der betroffenen Regionen verbinden, das wiederum eine Verbindung zu Umbrella herstellt?](#)

[Warum tut Cisco das?](#)

[Was geschieht, wenn meine Benutzer blockiert werden, sich aber nicht in einer der betroffenen Regionen befinden?](#)

[Wie genau sind Ihre Geoblocking-Daten?](#)

[Wie gehe ich vor, wenn der mit meiner IP-Adresse verknüpfte Standort falsch ist?](#)

Einleitung

Dieses Dokument beschreibt die Verhaltensänderungen, die Kunden von Cisco Umbrella und OpenDNS in Russland und Belarus ab dem 1. August gezeigt werden. Diese Verhaltensänderungen gelten auch für andere Regionen, in denen Cisco Umbrella IP-basiertes Geoblocking implementiert. Dieses Dokument wurde zuletzt am 28. Juli 2022 aktualisiert.

DNS-Kunden:

- Für den DNS-Dienst für Anfragen von IP-Adressen, die aus Russland, Belarus, der Krim, Luhansk, Donezk, Syrien, Kuba, dem Iran, Nordkorea und anderen sanktionierten Regionen mit Geoblocking stammen, dürfen keine Sicherheits- oder Content-Filterungsrichtlinien angewendet werden. Die DNS-Abfragen erhalten weiterhin eine gültige Antwort und werden mit derselben Servicestufe behandelt wie der Datenverkehr aus dem Rest der Welt.
- Bei Verwendung für DNS lösen das Umbrella Roaming Security-Modul und das AnyConnect Umbrella Roaming-Modul weiterhin den DNS-Datenverkehr auf.
- Die Synchronisierung von Roaming-Clients und Listen interner Domänen kann mit dem Dashboard fortgesetzt werden, um das erwartete Verhalten bereitzustellen (Senden interner Domänen an den internen DNS-Server). Das kann sich in Zukunft ändern.

SIG-Kunden:

- Umbrella Secure Web Gateway-Server akzeptieren keinen Datenverkehr, wenn die ursprüngliche IP aus Russland, Belarus, der Krim, Luhansk, Donezk, Syrien, Kuba, Iran, Nordkorea und anderen sanktionierten Regionen mit Geoblocking stammt. Bei der Implementierung werden Verbindungen aus diesen Regionen als offline oder nicht verfügbar eingestuft. Der Datenverkehr wird nicht akzeptiert oder verarbeitet.
- Die Standardkonfiguration des AnyConnect Umbrella-Moduls bewirkt, dass dieses eine direkte Verbindung mit dem Internet herstellt, wenn Umbrella nicht verfügbar ist. Einige spezifische Kundenkonfigurationen können in einem "Fail-Closed"-Modus betrieben werden,

was dazu führen würde, dass die Benutzer den Internetzugriff verlieren.

- Die Liste der externen Domänen wird weiterhin synchronisiert, um Aktualisierungen von Umbrella zu erhalten. Das kann sich in Zukunft ändern.
- Die Standard-Umbrella-PAC-Datei bewirkt, dass sie sich direkt mit dem Internet verbindet, wenn Umbrella nicht verfügbar ist. Einige spezifische Kundenkonfigurationen (z. B. solche ohne Standardroute) können "fehlschlagen" und dazu führen, dass Benutzer den Internetzugriff verlieren.
- IPsec-Tunnel werden entweder durch IP-Blockierung oder den Widerruf von IKE-Anmeldeinformationen getrennt. Das Verhalten und die Benutzerfreundlichkeit hängen von der jeweiligen Kundenkonfiguration ab. Einige Konfigurationen können auf eine direkte Internetverbindung zurücksetzen, andere auf MPLS, und wieder andere können dazu führen, dass Benutzer den Internetzugang verlieren.

Alle Kunden:

- Sobald die IP-basierte Geoblocking-Lösung für ein Land vollständig implementiert ist, werden auch der Umbrella Dashboard- und API-Zugriff blockiert.

Was ist, wenn sich meine Benutzer in den betroffenen Regionen mit einem Unternehmens-VPN außerhalb der betroffenen Regionen verbinden, das wiederum eine Verbindung zu Umbrella herstellt?

Unser Geoblocking ist IP-basiert und basiert auf der vom Umbrella-Service erkannten IP-Quelladresse.

Warum tut Cisco das?

Besuchen Sie [The War in Ukraine: Unterstützung unserer Kunden, Partner und Communities](#) für weitere Informationen

Was geschieht, wenn meine Benutzer blockiert werden, sich aber nicht in einer der betroffenen Regionen befinden?

Bitte [wenden](#) Sie [sich](#) an den [Support](#), um die Ausstellung untersuchen zu lassen.

Wie genau sind Ihre Geoblocking-Daten?

Wir verwenden branchenführende Geolokalisierungsdienste, um das Land für eine bestimmte IP-Adresse zu bestimmen.

Wie gehe ich vor, wenn der mit meiner IP-Adresse verknüpfte

Standort falsch ist?

Wir empfehlen, bei diesen Services einen Korrekturantrag zu stellen:

- <https://www.maxmind.com/en/geoip-location-correction> (Primärservice für Umbrella)
- <https://support.google.com/websearch/contact/ip/>
- <https://ipinfo.io/corrections>
- <https://www.ip2location.com/contact/>
- <http://www.ipligence.com/contact/>

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.