Cisco Umbrella FAQ Regarding IP-Based Geo-Blocking

Contents

Introduction

This document describes the behavior changes shown to customers of Cisco Umbrella and OpenDNS in Russia and Belarus starting on August 1. These behavior changes also apply to other regions for which Cisco Umbrella implements IP-based geo-blocking. This document was last updated on July 28, 2022.

DNS Customers:

- DNS service for queries originating from IP addresses identified as coming from Russia, Belarus, Crimea, Luhansk, Donetsk, Syria, Cuba, Iran, North Korea and other sanctioned regions with geo-blocking shall not have security or content filtering policies applied. The DNS queries still receive a valid response and are treated with the same service level as traffic from the rest of the world.
- When used for DNS, the Umbrella roaming security module and AnyConnect Umbrella roaming module continues to resolve DNS traffic.
- Roaming client sync and internal domains lists can continue to sync with the dashboard and provide the expected behavior (sending internal domains to the internal DNS server). This can change in the future.

SIG Customers:

- Umbrella secure web gateway servers is not accept traffic where the originating IP comes from Russia, Belarus, Crimea, Luhansk, Donetsk, Syria, Cuba, Iran, North Korea and other sanctioned regions with geo-blocking. The way this is implemented causes connections coming from these regions to see Cisco Umbrella servers as being offline or unavailable. Traffic is not accepted or processed.
- The default **AnyConnect Umbrella module** configuration causes it to connect directly to the internet when Umbrella is unavailable. Some specific customer configurations can operate in a 'fail closed' mode, which would cause users to lose internet access.
- The external domains list continue to sync, for now, to get updates from Umbrella. This can change in the future.
- The default Umbrella **PAC file** causes it to connect directly to the internet when Umbrella is unavailable. Some specific customer configurations (for example, those without a default route) can 'fail closed', causing users to lose internet access.
- IPsec tunnels are disconnected either by IP blocking or revocation of IKE credentials. The behavior and user experience is dependent on the specific customer configuration. Some configurations can revert to direct internet connection, others can revert to MPLS, and others can cause users to lose

internet access.

All Customers:

- Once IP-based geo-blocking is fully implemented for a country, Umbrella Dashboard and API access are also blocked.

What if my users in the affected regions connect to a corporate VPN outside of the affected regions, which in turn connects to Umbrella?

Our geo-blocking is IP-based, based on the source IP address seen by the Umbrella service.

Why is Cisco doing this?

Please visit The War in Ukraine: Supporting our Customers, Partners and Communities for more information.

What if my users are getting blocked but they aren’t in one of the affected regions?

Please contact support to have the issued investigated.

How accurate is your geo-blocking data?

We use industry leading geolocation services to determine the country for a given IP address.

What do I do if the location associated with my IP address is wrong?

We recommend submitting a correction request to these services:

- https://www.maxmind.com/en/geoip-location-correction (primary service used for Umbrella)
- https://support.google.com/websearch/contact/ip/
- https://ipinfo.io/corrections
- https://www.ip2location.com/contact/
- http://www.ipligence.com/contact/