Export Compliance and Geographic Restrictions for Cisco Secure Access

Contents

Introduction

This document describes how to export compliance and geographic restrictions for Cisco secure access.

Background Information

In conformance with the general export compliance policy of Cisco and in response to the war on Ukraine, Cisco restricts purchase, deployment, and access to Secure Access from several countries and regions including Russia, Belarus, Crimea, Luhansk, Donetsk, Syria, Cuba, Iran, and North Korea.

Domain Name Server (DNS)

- 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 do not have security or content filtering policies applied. Reporting is also disabled. 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 Secure Client roaming security module continues to resolve the DNS traffic.

Web Security

- Web Security servers do not accept traffic where the originating IP comes from one of the blocked countries or regions.
- The default Secure Client roaming security module configuration causes it to connect directly to the internet when Secure Access is unavailable. Some specific customer configurations operate in a ‘fail closed’ mode, which can cause users to lose internet access.
- The default Secure Access Protected Access Credential (**PAC**) file causes it to connect directly to the internet when Secure Access 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 Internet Key Exchange (IKE) credentials. The behavior and user experience are dependent on the specific customer configuration.

Some configurations revert to a direct internet connection, others revert to Multiprotocol Label Switching (MPLS), and others can cause users to lose internet access.

VPN and Zero Trust Access

Connections to the VPN and zero trust access servers where the originating IP comes from one of these countries or regions is refused.

Dashboard and Admin Access

The Secure Access dashboard and APIs are blocked for users connecting from one of the listed regions.

FAQs

1. What if the users are getting blocked but they are not in one of the affected regions?
   Contact support and they are happy to investigate.

2. How accurate is your geo-blocking data?
   Industry-leading geolocation services are used in order to determine the country for a given IP address.

3. What must be done if the location associated with the IP address is wrong?
   It is recommended to submit a correction request to these services:

- https://www.maxmind.com/en/geoip-location-correction
- https://support.google.com/websearch/contact/ip/
- https://ipinfo.io/corrections
- https://www.ip2location.com/
- http://www.ipligence.com/