Naleving van exportregels en geografische beperkingen voor Cisco Secure Access

Inhoud

Inleiding

Dit document beschrijft hoe u naleving en geografische beperkingen voor beveiligde Cisco-toegang kunt exporteren.

Achtergrondinformatie

In overeenstemming met het algemene beleid van Cisco op het gebied van exportnaleving en in reactie op de oorlog tegen Oekraïne, beperkt Cisco de aankoop, implementatie en toegang tot beveiligde toegang van meerdere landen en regio's, waaronder Rusland, Belarus, de Krim, Loehansk, Donetsk, Syrië, Cuba, Iran en Noord-Korea.

Domain Name Server (DNS)

- DNS-service voor vragen afkomstig van IP-adressen die zijn geïdentificeerd als afkomstig van Rusland, Wit-Rusland, de Krim, Loehansk, Donetsk, Syrië, Cuba, Iran, Noord-Korea en andere gesanctioneerde regio's met geoblocking hebben geen beleid voor beveiliging of contentfiltering. De rapportage is eveneens uitgeschakeld. De DNS-vragen ontvangen nog steeds een geldig antwoord en worden behandeld met hetzelfde serviceniveau als verkeer uit de rest van de wereld.
- Wanneer gebruikt voor DNS, blijft de Secure Client roaming security module het DNS-verkeer oplossen.

Web security

- Web security servers accepteren geen verkeer waarbij het oorspronkelijke IP afkomstig is uit een van de geblokkeerde landen of regio's.
- De standaard beveiligde client roaming security module configuratie zorgt ervoor dat het

direct verbinding met het internet wanneer Secure Access niet beschikbaar is. Sommige specifieke klantconfiguraties werken in een ‘fail closed’-modus, waardoor gebruikers internettoegang verliezen.
- Het standaard Secure Access Protected Access Credential (PAC) bestand zorgt ervoor dat het direct verbinding maakt met het internet wanneer Secure Access niet beschikbaar is. Sommige specifieke klantenconfiguraties (bijvoorbeeld die zonder standaardroute) kunnen "dicht mislukken", waardoor gebruikers internettoegang verliezen.
- IPsec-tunnels worden losgekoppeld door IP-blokkering of herroeping van Internet Key Exchange (IKE)-referenties. Het gedrag en de gebruikerservaring zijn afhankelijk van de specifieke klantconfiguratie. Sommige configuraties keren terug naar een directe internetverbinding, andere keren terug naar Multiprotocol Label Switching (MPLS) en andere kunnen ervoor zorgen dat gebruikers hun internettoegang verliezen.

Dashboard en toegang tot beheer

Het Secure Access-dashboard en de API's zijn geblokkeerd voor gebruikers die verbinding maken vanuit een van de vermelde gebieden.

Veelgestelde vragen

1. Wat als de gebruikers worden geblokkeerd, maar ze niet in een van de getroffen regio's zijn?
   Neem contact op met ondersteuning en ze zijn blij om te onderzoeken.

2. Hoe accuraat zijn je geoblocking data?
   Voor het bepalen van het land voor een bepaald IP-adres worden industrieel toonaangevende geolocatiediensten gebruikt.

3. Wat moet er worden gedaan als de locatie die gekoppeld is aan het IP-adres onjuist is?
   Aanbevolen wordt om bij deze diensten een correctieverzoek in te dienen:

- 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/

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.