Cumplimiento de exportaciones y restricciones geográficas para Cisco Secure Access

Contenido

Introducción

Este documento describe cómo exportar el cumplimiento y las restricciones geográficas para el acceso seguro de Cisco.

Antecedentes

De conformidad con la política general de cumplimiento de las exportaciones de Cisco y en respuesta a la guerra contra Ucrania, Cisco restringe la compra, el despliegue y el acceso seguro desde varios países y regiones, incluidos Rusia, Bielorrusia, Crimea, Luhansk, Donetsk, Siria, Cuba, Irán y Corea del Norte.

Servidor de nombres de dominio (DNS)

- El servicio DNS para consultas que se originan en direcciones IP identificadas como procedentes de Rusia, Bielorrusia, Crimea, Luhansk, Donetsk, Siria, Cuba, Irán, Corea del Norte y otras regiones sancionadas con bloqueo geográfico no tiene políticas de seguridad o filtrado de contenido aplicadas. Los informes también están deshabilitados. Las consultas de DNS siguen recibiendo una respuesta válida y se tratan con el mismo nivel de servicio que el tráfico del resto del mundo.
- Cuando se utiliza para DNS, el módulo de seguridad de roaming de Secure Client continúa resolviendo el tráfico DNS.

Seguridad web

- Los servidores de seguridad web no aceptan tráfico cuando la IP de origen proviene de uno de los países o regiones bloqueados.
- La configuración predeterminada del módulo de seguridad de roaming de Secure Client

hace que se conecte directamente a Internet cuando Secure Access no está disponible. Algunas configuraciones específicas del cliente funcionan en modo de "fallo-cierre", lo que puede provocar que los usuarios pierdan el acceso a Internet.
- El archivo predeterminado de credenciales de acceso seguro protegido (PAC) hace que se conecte directamente a Internet cuando Secure Access no está disponible. Algunas configuraciones específicas de los clientes (por ejemplo, aquellas sin una ruta predeterminada) pueden "fallar en el cierre", lo que hace que los usuarios pierdan el acceso a Internet.
- Los túneles IPsec se desconectan mediante el bloqueo de IP o la revocación de las credenciales de Intercambio de claves de Internet (IKE). El comportamiento y la experiencia del usuario dependen de la configuración específica del cliente. Algunas configuraciones vuelven a una conexión directa a Internet, otras vuelven a la conmutación de etiquetas multiprotocolo (MPLS) y otras pueden hacer que los usuarios pierdan el acceso a Internet.

Acceso de administrador y panel

El panel de acceso seguro y las API están bloqueados para los usuarios que se conectan desde una de las regiones de la lista.

Preguntas más Frecuentes

1. ¿Qué sucede si los usuarios se bloquean pero no se encuentran en una de las regiones afectadas?
   Póngase en contacto con el soporte técnico y estarán encantados de investigarlo.

2. ¿Qué precisión tienen sus datos de bloqueo geográfico?
   Los servicios de geolocalización líderes en el sector se utilizan para determinar el país de una dirección IP determinada.

3. ¿Qué se debe hacer si la ubicación asociada a la dirección IP es incorrecta?
   Se recomienda enviar una solicitud de corrección a estos servicios:

- 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/

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).