Conformidade de exportação e restrições geográficas para Cisco Secure Access

Contents

Introdução

Este documento descreve como exportar as restrições geográficas e de conformidade para acesso seguro da Cisco.

Informações de Apoio

De acordo com a política geral de conformidade para exportação da Cisco e em resposta à guerra contra a Ucrânia, a Cisco restringe a compra, a implantação e o acesso ao Secure Access de vários países e regiões, incluindo Rússia, Belarus, Crimeia, Luhansk, Donetsk, Síria, Cuba, Irã e Coreia do Norte.

Servidor de Nomes de Domínio (DNS)

- O serviço DNS para consultas originadas de endereços IP identificados como provenientes da Rússia, Belarus, Crimeia, Luhansk, Donetsk, Síria, Cuba, Irã, Coreia do Norte e outras regiões sancionadas com bloqueio geográfico não possuem políticas de segurança ou filtragem de conteúdo aplicadas. Os relatórios também são desativados. As consultas DNS ainda recebem uma resposta válida e são tratadas com o mesmo nível de serviço que o tráfego do resto do mundo.
- Quando usado para DNS, o módulo de segurança de roaming do cliente seguro continua a resolver o tráfego DNS.

Segurança da Web

- Os servidores de segurança da Web não aceitam o tráfego em que o IP de origem vem de um dos países ou regiões bloqueados.
- A configuração padrão do módulo de segurança de roaming do Secure Client faz com que

ele se conecte diretamente à Internet quando o Secure Access não estiver disponível. Algumas configurações específicas do cliente operam em um modo "fail closed", o que pode fazer com que os usuários percam o acesso à Internet.
- O arquivo padrão PAC (Secure Access Protected Access Credential) faz com que ele se conecte diretamente à Internet quando o Secure Access não está disponível. Algumas configurações específicas do cliente (por exemplo, aquelas sem uma rota padrão) podem "falhar ao fechar", fazendo com que os usuários percam o acesso à Internet.
- Os túneis IPsec são desconectados por bloqueio de IP ou revogação de credenciais de Internet Key Exchange (IKE). O comportamento e a experiência do usuário dependem da configuração específica do cliente. Algumas configurações revertem para uma conexão direta com a Internet, outras revertem para Multiprotocol Label Switching (MPLS) e outras podem fazer com que os usuários percam o acesso à Internet.

Painel e Acesso de Administrador

O painel e as APIs do Secure Access estão bloqueados para usuários que se conectam de uma das regiões listadas.

Perguntas freqüentes

1. E se os usuários estiverem sendo bloqueados, mas não estiverem em uma das regiões afetadas?
   Entre em contato com o suporte e eles ficarão felizes em investigar.

2. Qual é a precisão de seus dados de bloqueio geográfico?
   Serviços de geolocalização líderes de mercado são usados para determinar o país para um determinado endereço IP.

3. O que deve ser feito se o local associado ao endereço IP estiver errado?
   Recomenda-se enviar uma solicitação de correção para estes serviços:

- 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/

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.