

Restrição de acesso geográfico para acesso com confiança zero e conexões VPN

Contents

Problema

As organizações que exigem restrições de acesso geográfico para ZTA (Zero Trust Access) e conexões VPN podem descobrir que as políticas existentes de ZTA e VPN precisam ser desabilitadas ao tentar implementar controles de acesso baseados no país. Os usuários experimentam perda total de acesso aos recursos necessários quando as políticas são desativadas devido à incapacidade de localizar opções de restrição geográfica nativa na interface de produto Secure SSE. O requisito específico de restringir o acesso a conexões originárias apenas de um determinado país não pode ser configurado usando recursos de produto incorporados, resultando em um impacto generalizado do usuário quando as políticas existentes são desativadas em uma tentativa de implementar tais restrições.

Ambiente

- Produto Cisco Secure Access Service Edge (SASE) / Secure SSE
- Implementação do Zero Trust Access (ZTNA)
- Serviços VPN que exigem controle de acesso geográfico
- Políticas privadas de acesso a recursos
- Organização que exige restrições de acesso específicas do país

Resolução

O produto Cisco Secure SSE atualmente não fornece funcionalidade nativa para restringir o acesso a recursos privados com base na localização geográfica do usuário ou no país. As

abordagens descritas nas próximas seções podem ser consideradas para lidar com essa limitação.

Envio de solicitação de recurso

Uma solicitação de recurso deve ser enviada à Cisco para adicionar recursos de restrição geográfica para acesso ZTA e VPN. Essa solicitação de aprimoramento é avaliada pela equipe do produto para possível inclusão em versões futuras. As empresas podem trabalhar com seu Cisco Account Manager para ajudar a priorizar essas solicitações de recursos com base nos requisitos comerciais.

Consideração de solução manual

Uma possível solução manual envolve adicionar intervalos de endereços IP públicos específicos do país como grupos de objetos de rede nas políticas de acesso.

Passo 1: Obtenha os intervalos de endereços IP públicos dos países no Registro Internet Regional (RIR) apropriado.

Passo 2: Crie grupos de objetos de rede que contenham os intervalos IP identificados. Configure grupos de objetos de rede na configuração da política de acesso para incluir os intervalos de endereços IP específicos alocados ao país de destino.

Passo 3: Aplique os grupos de objetos de rede às políticas de acesso. Modifique as políticas de acesso existentes para fazer referência aos grupos de objetos de rede criados, limitando efetivamente o acesso às conexões originárias dos intervalos IP especificados.

Limitações importantes

Essa abordagem manual tem limitações significativas, pois se baseia em definições de intervalo de IP estático e não pode levar em conta alocações de IP dinâmico, usuários móveis ou serviços VPN que podem ignorar restrições geográficas. Além disso, esse método requer manutenção contínua para garantir a precisão do intervalo IP.

Gerenciamento de políticas temporárias

Até que uma solução permanente esteja disponível, as empresas devem evitar desativar todas as políticas de ZTA e VPN simultaneamente. Em vez disso, considere a implementação de uma abordagem em fases, em que as políticas críticas de acesso permaneçam ativas enquanto os requisitos de restrição geográfica estão sendo atendidos por meios alternativos ou aguardando melhorias no produto.

Causa

A arquitetura do produto Cisco Secure SSE não inclui recursos nativos de controle de acesso geográfico para acesso privado a recursos. A estrutura da política de acesso ao produto é projetada com base na identidade do usuário, na postura do dispositivo e nos controles baseados na rede, mas não incorpora a localização geográfica como um parâmetro de aplicação da política. Isso representa uma lacuna de capacidade do produto, e não um problema de configuração ou um defeito de software.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

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.