

# Sessão BGP não sincronizada devido a Limites de Prefixo de Rota no Acesso Seguro à Integração do AWS Direct Connect

## Contents

---

---

## Problema

As sessões de BGP estão passando por oscilações em um túnel de site a site entre o Cisco Secure Access e o AWS Direct Connect. A instabilidade ocorre porque o número de prefixos de rota anunciados do Secure Access excede os limites do AWS Direct Connect, impedindo a troca de rota estável e afetando a capacidade de estabelecer conectividade consistente entre o Secure Access e o AWS.

## Ambiente

- Acesso seguro da Cisco (CSA)
- AWS Direct Connect com roteamento BGP
- Configuração de túnel de site a site entre Secure Access e AWS
- Limite de prefixo de BGP do AWS Direct Connect de 100 rotas

## Resolução

A resolução envolve várias abordagens para lidar com a restrição de limite de prefixo BGP.

A análise de pacote de rede revela mensagens BGP NOTIFICATION indicando que o número máximo de prefixos foi atingido:

Border Gateway Protocol - NOTIFICATION Message

Length: 28

Type: NOTIFICATION Message (3)

Major error Code: Cease (6)

Minor error Code (Cease): Maximum Number of Prefixes Reached (1)

## Soluções imediatas

### Opção 1: Filtragem de rota do lado AWS

Avalie as opções do lado do AWS para ignorar ou filtrar os prefixos de rota de entrada do Secure Access para ficar dentro do limite de 100 prefixos imposto pelo AWS Direct Connect.

### Opção 2: Implementação do AWS Transit Gateway

Considere migrar para um AWS Transit Gateway como um modelo de conectividade alternativo. Essa abordagem pode oferecer opções de roteamento mais flexíveis e pode ajudar a contornar as limitações do prefixo do Direct Connect.

## Solução de longo prazo

### Implementação da solicitação de recurso

Uma solicitação de recurso (CSE-I-4783) foi preenchida para permitir a filtragem de rota ou recursos de sumarização no Secure Access. Esse aprimoramento permitiria:

- Resumo de rotas para reduzir o número de prefixos anunciados
- Filtragem de rota para controlar quais prefixos são anunciados ao AWS Direct Connect
- Melhor controle sobre anúncios BGP do lado do acesso seguro

## Etapas de implementação

- 1: Analise as limitações do AWS Direct Connect. Consulte a documentação de [limites do AWS Direct Connect](#) para entender as restrições específicas.
- 2: Avalie os anúncios de rotas atuais. Analise o número atual de rotas que estão sendo anunciadas do Secure Access para determinar quantas excedem o limite de 100 prefixos do AWS.
- 3: Implemente uma solução imediata. Escolha entre a filtragem do lado AWS ou a implementação do Transit Gateway com base nos requisitos da arquitetura de rede e nas necessidades da empresa.
- 4: Monitorar o andamento da solicitação de recurso. Trabalhe com as equipes de conta da Cisco para analisar a viabilidade e o impacto da solicitação de recurso de filtragem/sumarização de rotas proposta.

## Causa

A causa raiz é uma limitação fundamental no AWS Direct Connect, que restringe os anúncios de rota BGP a um máximo de 100 prefixos. O Cisco Secure Access está anunciando mais de 100 prefixos de rota, fazendo com que o AWS Direct Connect envie mensagens de NOTIFICAÇÃO BGP com o código de erro "Número máximo de prefixos alcançados" e subsequentemente desmonte a sessão BGP. Isso cria um ciclo de estabelecimento e destruição de sessão, resultando no comportamento de oscilação de sessão BGP observado.

## Conteúdo relacionado

- [Documentação de Limites do AWS Direct Connect](#)
- [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.