AWS Direct Connect統合へのセキュアアクセスにおけるルートプレフィクス制限によるBGPセッションフラッピング

内容

お問い合わせ内容

BGPセッションで、Cisco Secure AccessとAWS Direct Connectの間のサイト間トンネルでフラッピングが発生しています。この不安定性は、セキュアアクセスからアドバタイズされたルートプレフィックスの数がAWS Direct Connectの制限を超えたために発生し、安定したルート交換が妨げられ、セキュアアクセスとAWSの間で一貫した接続を確立する機能に影響を与えます。

環境

- シスコセキュアアクセス(CSA)
- BGPルーティングを使用したAWS Direct Connect
- Secure AccessとAWS間のサイト間トンネル設定
- AWS Direct Connect BGPプレフィクス制限（100ルート）

解決策

この問題を解決するには、BGPプレフィクス制限の制約に対処する複数のアプローチが必要です。

ネットワークパケット分析により、プレフィックスの最大数に達したことを示すBGP NOTIFICATIONメッセージが明らかになります。

```
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)
```

迅速な回避策

オプション1: AWS側のルートフィルタリング

AWS側のオプションを評価して、セキュアアクセスからの着信ルートプレフィックスを無視またはフィルタして、AWS Direct Connectで課される100プレフィクスの制限内に収まるようにします。

オプション2: AWS Transit Gatewayの実装

別の接続モデルとして、AWS Transit Gatewayへの移行を検討してください。このアプローチにより、より柔軟なルーティングオプションが提供され、直接接続プレフィクスの制限を回避できます。

長期的なソリューション

機能要求の実装

セキュアアクセスでルートフィルタリングまたは集約機能を許可するための機能要求(CSE-I-4783)が提出されました。この機能拡張により、次のことが可能になります。

- アドバタイズされたプレフィックスの数を減らすルート集約
- AWS Direct Connectにアドバタイズされるプレフィックスを制御するルートフィルタリング

- セキュアアクセス側からのBGPアドバタイズメントに対する制御の向上

実装ステップ

1: AWS Direct Connectの制限を確認します。特定の制約については、AWS Direct Connectの制限に関するドキュメントを参照してください。

2：現在のルートアドバタイズメントを評価します。Secure Accessからアドバタイズされる現在のルート数を分析し、100プレフィクスのAWS制限をいくつ超えたかを判断します。

3：ただちに回避策を実施します。ネットワークアーキテクチャの要件とビジネスニーズに基づいて、AWS側のフィルタリングまたはトランジットゲートウェイの実装のいずれかを選択します。

4：機能要求の進行状況を監視します。該当するシスコアカウントチームと協力して、提案されたルートフィルタリング/集約機能要求の実現可能性と影響を確認します。

原因

根本原因は、BGPルートアドバタイズメントが最大100個のプレフィックスに制限されるAWS Direct Connectの基本的な制限です。Cisco Secure Accessは100を超えるルートプレフィックスをアドバタイズしているため、AWS Direct Connectは「Maximum Number of Prefixes Reached」というエラーコードのBGP NOTIFICATIONメッセージを送信し、BGPセッションを切断します。これにより、セッションの確立とティアダウンのサイクルが作成され、確認されたBGPセッションフラッピング動作が発生します。

関連コンテンツ

- AWS Direct Connect制限ドキュメント
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。