BGP Session Flapping Due to Route Prefix Limits in Secure Access to AWS Direct Connect Integration

Contents

Issue

BGP sessions are experiencing flapping on a site-to-site tunnel between Cisco Secure Access and AWS Direct Connect. The instability occurs because the number of route prefixes advertised from Secure Access exceeds AWS Direct Connect limits, preventing stable route exchange and impacting the ability to establish consistent connectivity between Secure Access and AWS.

Environment

- Cisco Secure Access (CSA)
- AWS Direct Connect with BGP routing
- Site-to-site tunnel configuration between Secure Access and AWS
- AWS Direct Connect BGP prefix limit of 100 routes

Resolution

The resolution involves multiple approaches to address the BGP prefix limit constraint.

Network packet analysis reveals BGP NOTIFICATION messages indicating that the maximum number of prefixes has been reached:

```
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)
```

Immediate Workarounds

Option 1: AWS-Side Route Filtering

Evaluate AWS-side options to ignore or filter incoming route prefixes from Secure Access to stay within the 100-prefix limit imposed by AWS Direct Connect.

Option 2: AWS Transit Gateway Implementation

Consider migrating to an AWS Transit Gateway as an alternative connectivity model. This approach can provide more flexible routing options and can help circumvent the Direct Connect prefix limitations.

Long-Term Solution

Feature Request Implementation

A feature request (CSE-I-4783) has been filed to allow route filtering or summarization capabilities on Secure Access. This enhancement would enable:

- Route summarization to reduce the number of advertised prefixes
- Route filtering to control which prefixes are advertised to AWS Direct Connect
- Better control over BGP advertisements from the Secure Access side

Implementation Steps

1: Review AWS Direct Connect limitations. Reference the AWS Direct Connect limits documentation to understand the specific constraints.

2: Evaluate current route advertisements. Analyze the current number of routes being advertised from Secure Access to determine how many exceed the 100-prefix AWS limit.

3: Implement immediate workaround. Choose between AWS-side filtering or Transit Gateway implementation based on network architecture requirements and business needs.

4: Monitor feature request progress. Work with applicable Cisco account teams to review the feasibility and impact of the proposed route filtering/summarization feature request.

Cause

The root cause is a fundamental limitation in AWS Direct Connect, which restricts BGP route advertisements to a maximum of 100 prefixes. Cisco Secure Access is advertising more than 100 route prefixes, causing AWS Direct Connect to send BGP NOTIFICATION messages with error code "Maximum Number of Prefixes Reached" and subsequently tear down the BGP session. This creates a cycle of session establishment and teardown, resulting in the observed BGP session flapping behavior.

Related Content

- AWS Direct Connect Limits Documentation
- Cisco Technical Support & Downloads