# AWS Direct Connect 통합에 대한 보안 액세스에서 경로 접두사 제한으로 인한 BGP 세션 플랩

## 목차

## 문제

BGP 세션에서 Cisco Secure Access와 AWS Direct Connect 간의 사이트 간 터널에서 플래핑이 발생합니다. 이러한 불안정한 상황은 Secure Access에서 광고된 경로 접두사의 수가 AWS Direct Connect 제한을 초과하여 안정적인 경로 교환을 방해하고 Secure Access와 AWS 간의 일관된 연결을 설정하는 기능에 영향을 주기 때문에 발생합니다.

## 환경

- CSA(Cisco Secure Access)
- BGP 라우팅을 사용하는 AWS Direct Connect
- Secure Access와 AWS 간의 Site-to-Site 터널 구성
- AWS Direct Connect BGP 접두사 제한(경로 100개)

## 해결

이 확인에는 BGP 접두사 제한 제약 조건을 해결하기 위한 여러 접근 방식이 포함됩니다.

네트워크 패킷 분석을 통해 접두사의 최대 수에 도달했음을 나타내는 BGP NOTIFICATION 메시지가 나타납니다.

```
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)
```

## 즉각적인 해결 방법

### 옵션 1: AWS측 경로 필터링

AWS Direct Connect에서 지정한 100개의 접두사 제한 내에서 유지되도록 수신 경로 접두사를 무시하거나 Secure Access에서 필터링하도록 AWS측 옵션을 평가합니다.

### 옵션 2: AWS Transit Gateway 구현

대체 연결 모델로 AWS Transit Gateway로 마이그레이션하는 것을 고려해 보십시오. 이 접근 방식은 보다 유연한 라우팅 옵션을 제공할 수 있으며 Direct Connect 접두사 제한을 피할 수 있습니다.

## 장기적인 솔루션

### 기능 요청 구현

Secure Access에서 경로 필터링 또는 요약 기능을 허용하기 위한 기능 요청(CSE-I-4783)이 제출되었습니다. 이러한 개선을 통해 다음을 수행할 수 있습니다.

- 알려진 접두사 수를 줄이기 위한 경로 요약
- AWS Direct Connect에 광고되는 접두사를 제어하는 경로 필터링
- 보안 액세스 측에서 BGP 광고를 더 효과적으로 제어

### 구현 단계

1: AWS Direct Connect 제한 사항을 검토합니다. 특정 제약 조건을 이해하려면 AWS Direct Connect 제한 설명서를 참조하십시오.

2: 현재 경로 알림을 평가합니다. Secure Access에서 광고되는 현재 경로 수를 분석하여 접두사 100개 AWS 제한을 초과하는 경로 수를 확인합니다.

3: 즉각적인 해결 방법 구현 네트워크 아키텍처 요구 사항 및 비즈니스 요구 사항에 따라 AWS측 필터링 또는 트랜짓 게이트웨이 구현 중에서 선택할 수 있습니다.

4: 기능 요청 진행률 모니터링 해당 Cisco 어카운트 팀과 함께 제안된 경로 필터링/요약 기능 요청의 실행 가능성 및 영향을 검토합니다.

## 원인

근본 원인은 BGP 경로 알림을 최대 100개의 접두사로 제한하는 AWS Direct Connect의 근본적인 제한입니다. Cisco Secure Access는 100개가 넘는 경로 접두사를 광고하므로 AWS Direct Connect가 "Maximum Number of Prefixes Reached(최대 접두사 수에 도달함)" 오류 코드와 함께 BGP 알림 메시지를 보낸 다음 BGP 세션을 해제합니다. 이렇게 하면 세션 설정 및 해체의 주기가 생성되므로, BGP 세션 플래핑 동작이 관찰됩니다.

## 관련 콘텐츠

- AWS Direct Connect 제한 문서
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.