보안 액세스 IP 풀 서브넷 할당 및 BGP 경로 알림

목차

문제

/20 서브넷으로 구성된 IP 풀은 클라우드 경로에 설치된 두 개의 /22 서브넷을 예상된 두 개의 /21 서브넷 대신 표시합니다. 이 구성은 예상 주소 공간의 절반만 제공합니다.

환경

- 기술: 솔루션 지원(SSPT - 계약 필요)
- 하위 기술: 보안 액세스
- 제품군: 초
- 소프트웨어 버전: 모두
- 설정: /20 서브넷 구성을 사용하는 IP 풀
- 인프라: BGP 경로 알림이 포함된 활성 VPN 헤드엔드 2개

해결

사용자 VPN 풀 크기 조정 및 BGP 광고

Secure Access BGP는 /22보다 큰 접두사를 알리지 않습니다. Secure Access에서 RAVPN(원격 액세스 VPN)에 대한 사용자 VPN 풀을 구성하면 플랫폼에서 네트워크를 그에 따라 처리합니다.

- 제공된 네트워크가 /22보다 클 경우(예: /20), 플랫폼은 자동으로 네트워크를 여러 개의 /22 청크로 분할합니다.

예: /20 풀을 제공합니다. Secure Access는 이를 내부적으로 4×/22개의 서브넷으로 분할합니다. 각 /22는 해당 지역의 데이터 센터에서 온디맨드 방식으로 임대한 것입니다. 데이터 센터에서 /22를 임대하는 경우 /20 전체가 아닌 BGP를 통해 /22(또는 그보다 작음)만 광고합니다.

- 제공된 네트워크가 /22 이하(예: /24)인 경우, 플랫폼에서는 네트워크를 최소 2개의 더 작은 서브넷으로 분할하여 해당 지역의 최소 2개 데이터 센터에서 고가용성을 지원합니다.

예: /24 풀을 제공합니다. Secure Access는 이를 2×/25개의 서브넷으로 분할합니다. 각 /25는 지역의 다른 데이터 센터에 할당됩니다. 각 데이터 센터는 BGP를 통해 해당 /25를 광고합니다.

VPN 풀 서브넷이 모두 동시에 보급되는 것은 아닙니다. 대신 RAVPN 클라이언트 연결 수가 증가함에 따라 VPN 풀 서브넷이 온디맨드 방식으로 할당되고 보급됩니다.

- 처음에는 첫 번째 서브넷(예: /20의 첫 번째 /22)만 BGP를 통해 임대 및 광고됩니다.
- 수요가 증가함에 따라 데이터 센터에서 추가 서브넷을 임대한 다음 광고합니다.

- 이는 클라우드 리소스가 동적으로 확장되는 방식과 일치합니다.

예: /20 범위를 포함하도록 4 × /22 풀을 구성합니다. 낮은 연결 볼륨에서 BGP는 첫 번째 /22만 알립니다. RAVPN 연결이 증가하면 나머지 /22 풀이 활성화되며 점진적으로 광고됩니다.

중요: 구성된 풀 중 하나만 광고되는 경우 이는 예상된 동작입니다. 확장 요구가 있을 경우 추가 풀이 광고됩니다.

요약

제공된 풀 크기	내부 분할	BGP 광고	이유
/22보다 큼(예: /20)	여러 /22로 분할(예: 4 × /22)	온디맨드 방식으로 각 /22 이하	최대 알림 접두사는 /22입니다. 온디맨드 확장
/22	2개 이상의 더 작은 서브넷으로 분할	각 소규모 서브넷, 온디맨드	≥2 데이터 센터 전반의 고가용성
/22보다 작음(예: /24)	최소 2개의 서브넷(예: 2×/25)으로 분할합니다.	각 서브넷, 온디맨드	≥2 데이터 센터 전반의 고가용성

- Maximum BGP advertised prefix: /22 — Secure Access는 BGP를 통해 /22보다 큰 네트워크를 광고하지 않습니다.
- 자동 분할 — 고가용성(지역당 최소 2개의 데이터 센터) 및 확장성을 위해 네트워크가 내부적으로 분할됩니다.
- 온디맨드 알림 - 서브넷은 연결을 제공하기 위해 데이터 센터에서 활발하게 임대한 경우에만 BGP를 통해 광고됩니다. 모든 풀이 BGP에 동시에 나타나는 것은 아닙니다.
- 동적 확장 — 클라우드 네이티브 리소스 확장 원칙을 준수하여 RAVPN 클라이언트 연결 수가 증가하면 추가 풀 서브넷이 활성화됩니다.

원인

이는 Secure Access 시스템 서브넷 할당 알고리즘의 설계된 동작입니다. 시스템은 구성된 서브넷을 같은 크기의 더 작은 서브넷으로 자동으로 분할하고 사전 분류 방식을 사용하여 사용 가능한 VPN 헤드엔드에 배포하여 일관되고 예측 가능한 할당 패턴을 보장합니다.

관련 콘텐츠

- 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.