Cisco Secure Access Traffic Steering 구성 및 클라이언트 동기화

목차

문제

Cisco Secure Access Traffic Steering 컨피그레이션을 검토할 때 VPN 프로필 설정 및 XML 파일에 트래픽 스티어링 제어를 위해 구성된 대상 IP 주소 또는 도메인이 표시되지 않습니다. 그러면 Secure Access 클라이언트에서 조정 결정을 위한 트래픽 대상을 결정하는 방법과 관리 포털에서 변경된 컨피그레이션이 클라이언트에 동기화되는 방법에 대한 혼란이 발생합니다.

특히, 관리자는 트래픽 조정 설정이 VPN 프로필 관리 인터페이스를 통해 구성되는 동안 해당 VPN 프로필 XML 파일에 트래픽 조정 제어의 대상이 되어야 하는 대상 주소 또는 도메인에 대한 표시되는 항목이 포함되어 있지 않음을 확인합니다.

환경

- Cisco Secure Access 솔루션
- 트래픽 스티어링이 활성화된 VPN 프로파일 컨피그레이션
- 보안 액세스 클라이언트 구축

해결

Cisco Secure Access의 트래픽 스티어링은 VPN 프로필 XML의 고정 항목이 아닌 동적 규칙 전달 메커니즘을 통해 작동합니다. 다음은 이 프로세스의 작동 방식과 컨피그레이션의 검증 방법에 대해 설명합니다.

트래픽 조정 규칙 전달 프로세스

트래픽 조정 규칙은 관리자가 볼 수 있는 VPN 프로필 XML 파일에 저장되지 않습니다. 대신, 이러한 규칙은 VPN 연결 설정 중에 Secure Access 헤드엔드에서 클라이언트로 동적으로 푸시됩니다. 이 프로세스는 다음과 같이 작동합니다.

1. VPN 연결이 설정되면 Secure Access 헤드엔드가 현재 트래픽 스티어링(스플릿 터널) 규칙을 연결 클라이언트에 푸시합니다
2. 클라이언트는 이러한 규칙을 수신하여 로컬 클라이언트 라우팅 테이블에 직접 기록합니다
3. 트래픽 조정 결정은 VPN 프로필 XML에 표시되는 정보가 아니라 클라이언트 라우팅 테이블의 항목을 기반으로 합니다

컨피그레이션 변경 동기화

관리 포털에서 Traffic Steering 설정을 변경하면 특정 동기화 패턴을 따릅니다.

- 관리 포털의 컨피그레이션 변경 사항은 활성 VPN 세션 중에는 적용되지 않습니다
- 다음 VPN 연결 설정에서는 새로운 트래픽 스티어링 규칙이 적용됩니다
- 트래픽 스티어링 컨피그레이션을 변경한 후 동작을 검증하려면 VPN 연결을 끊고 다시 연결해야 합니다

검증 단계

트래픽 스티어링 컨피그레이션 변경 사항을 검증하려면

1. 보안 액세스 관리 포털에서 트래픽 조정 설정을 원하는 대로 변경합니다
2. 클라이언트에서 기존 VPN 연결 끊기
3. 업데이트된 트래픽 스티어링 규칙을 수신하기 위해 VPN을 다시 연결합니다
4. 클라이언트 라우팅 테이블을 검사하여 새 규칙이 적용되었는지 확인합니다

원인

VPN 프로필 XML에 트래픽 조정 대상이 없는 것은 설계에 의한 것입니다. Cisco Secure Access는 트래픽 조정 규칙이 연결 시 클라이언트로 푸시되고 프로필 XML에 표시되는 컨피그레이션 요소로 저장되지 않고 라우팅 테이블 엔트리를 통해 구현되는 동적 규칙 전달 시스템을 사용합니다. 이 아키텍처에서는 보안과 성능을 유지하면서 실시간 정책 업데이트 및 중앙 집중식 제어가 가능합니다.

관련 콘텐츠

- ASA 스플릿 터널링 컨피그레이션 가이드
- 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.