

원격 액세스 사용자가 RAVPN을 통해 내부 서비스에 연결할 수 없음

목차

문제

Secure Access를 사용하는 원격 액세스 사용자는 본사의 Domain Controller를 비롯한 내부 서비스에 연결할 수 없는 반면, 인터넷 액세스는 계속 정상적으로 작동합니다. 사용자는 인터넷을 성공적으로 탐색할 수 있었지만 RAVPN(Remote Access VPN)을 통해 도메인 컨트롤러와 같은 내부 리소스에 액세스할 수 없었습니다.

환경

- Cisco Secure Access - 보안 클라이언트 원격 액세스(VPN, 보안 상태, 개인 리소스)
- RAVPN(Remote Access VPN) 터널이 작동 및 정상으로 보고됨
- 사용 중인 SD-WAN 인프라
- 본사의 내부 DNS 서버
- 본사 위치의 도메인 컨트롤러 서비스
- 인프라를 통해 연결된 여러 브랜치 네트워크

해결

원격 액세스 연결 문제를 해결하기 위해 다음 트러블슈팅 및 해결 단계를 수행했습니다.

1단계: 패킷 캡처 분석

클라이언트 및 엣지 디바이스(양방향)에서 Simultaneous Packet Capture를 수집하여 트래픽 흐름 패턴을 분석합니다.

흐름:

RA VPN 클라이언트-----Cisco Secure Access-----Ipsec 터널 ----- 엣지 디바이스-----
전용 리소스

- 클라이언트의 DNS 쿼리가 엣지 디바이스에 성공적으로 도달하여 DNS 서버로 전송되었는지 확인합니다.
- 로컬 DNS 서버에서 클라이언트로 반환되는 DNS 회신이 관찰되지 않았는지 확인
- 로컬 DNS 서버가 응답을 보냈지만 터널 인터페이스로 응답이 돌아가지 않았습니다.

2단계: 근본 원인 식별

패킷 캡처 분석을 기반으로, 이 문제는 반환 경로 라우팅 문제로 식별되었습니다. 트래픽 분석에 따르면 DNS 쿼리가 Cisco Secure Access 인프라를 통해 로컬 DNS 서버에 성공적으로 도달했지만 인프라의 라우팅 또는 컨피그레이션 문제로 인해 DNS 응답을 포함하는 반환 트래픽이 원격 액세스 클라이언트에 도달하지 못했습니다.

3단계: 컨피그레이션 검토 및 교정

내부 네트워크 컨피그레이션 및 내부 네트워크 컨피그레이션을 검토하고 수정합니다. 특히 다음 사항에 중점을 둡니다.

- DNS 컨피그레이션 및 반환 트래픽 라우팅
- VPN 반환 트래픽을 위한 내부 라우팅 정책
- 내부 네트워크 라우팅 컨피그레이션
- 엣지 장치 쪽에 구성 요소가 없습니다.

4단계: 서비스 복원 확인

컨피그레이션 검토 및 수정 이후 Secure Access 기능이 크게 복원되었습니다. 대부분의 원격 액세스 사용자는 본사의 도메인 컨트롤러를 비롯한 내부 서비스에 다시 액세스했습니다.

원인

근본 원인은 내부 네트워크 인프라 내에서 반환 경로 라우팅 문제로 확인되었습니다. 원격 액세스 클라이언트의 DNS 쿼리가 Cisco Secure Access Infrastructure를 통해 로컬 DNS 서버에 도달하는 동안 DNS 응답이 포함된 반환 트래픽이 클라이언트에 제대로 라우팅되지 않았습니다. 이는 내부 네트워크 인프라 측에서 구성이 누락되었거나 잘못되어 DNS 회신 및 TCP 응답이 VPN 연결을 통해 원격 액세스 클라이언트에 도달하지 못하게 되었기 때문입니다.

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.