Palo Alto 및 Secure Access NTG를 통한 RAVPNaaS의 PR 연결 문제 해결

목차

문제

사용자는 Cisco Secure Client를 사용하여 클라우드 VPN 연결을 설정했지만 연결 후 내부 프라이빗 리소스에 액세스할 수 없었습니다. 백엔드 확인 중에 보안 액세스 측에서 VPN 터널이 연결된 것처럼 보였지만 연결된 사용자가 내부 네트워크 서비스에 액세스할 수 없는 상태가 되었습니다. 이 연결 문제는 성공적인 VPN 인증 및 터널 설정에도 불구하고 내부 자산에 대한 사용자 액세스에 영향을 미쳤습니다.

환경

- Cisco 보안 클라이언트
- 보안 액세스의 네트워크 터널 그룹
- Palo Alto as Edge Firewall
- 내부 사설 네트워크 리소스 컨피그레이션
- 보안 액세스 원격 VPN

해결

연결 문제는 Palo Alto 방화벽 측에서 협업 트러블슈팅 세션 및 터널 재설정 절차를 통해 해결되었습니다.

수행된 트러블슈팅 단계

1단계: 초기 연결 검증

현재 연결 상태를 확인하고 백엔드 확인에서 Secure Access-side 터널이 연결된 것으로 표시되는지 확인합니다.

2단계: 터널 재설정 ID

트래픽이 Palo Alto에서 나가고 있는지 확인하려면 CNHE(Cloud Native Headend)에서 패킷을 가져옵니다.

3단계: Palo Alto 터널 재설정

Palo Alto 끝에는 트래픽이 관찰되지 않았습니다.

4단계: VPN 재연결

터널 재설정을 수행하는 것이 좋습니다. 터널이 재설정되면 사용자는 Secure Client를 사용하여 VPN에 다시 연결하여 재설정 인프라를 통해 새로운 터널 연결을 설정합니다.

5단계: 연결 확인

다시 연결한 후 내부 리소스 액세스가 복원되었으며 사용자가 VPN 연결을 통해 내부 네트워크 서비스에 성공적으로 연결할 수 있음을 확인했습니다.

원인

근본 원인은 Palo Alto 방화벽 측의 터널 상태 불일치로 인해 성공적인 VPN 인증에도 불구하고 내부 트래픽의 적절한 라우팅이 불가능했기 때문입니다. 터널 재설정 절차에서 이러한 상태 불일치를 지우고 내부 리소스 액세스를 위한 올바른 연결 경로를 복원했습니다.

관련 콘텐츠

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.