Tunnel All DNS for Secure Client with Umbrella Module 활성화

목차

소개

이 문서에서는 Umbrella 모듈을 사용하는 Cisco Secure Client에 대해 모든 DNS를 터널링하는 방법을 설명합니다.

배경 정보

Cisco는 2023년에 Cisco AnyConnect의 End-of-Life를, 2024년에 Umbrella Roaming Client를 발표했습니다. 많은 Cisco Umbrella 고객이 이미 Cisco Secure Client로의 마이그레이션을 통해 혜택을 누리고 있으며, 더 나은 로밍 경험을 얻으려면 최대한 빨리 마이그레이션을 시작하는 것이 좋습니다. 이 Knowledge Base 문서에서 자세히 읽기: Umbrella 모듈과 함께 Cisco Secure Client를 설치하려면 어떻게 해야 합니까?

Cisco Secure Client(CSC) with Umbrella(이전의 AnyConnect Roaming Security) 모듈은 추가 컨피그레이션 없이 거의 모든 CSC VPN 모드에서 작동하도록 설계되었습니다.

그러나 다음 두 조건이 모두 해당되는 경우 추가 고려 사항:

- 스플릿 터널링 사용
- "Tunnel All DNS" 기능이 활성화되어 있습니다.

문제 및 영향

"Tunnel All DNS(모든 DNS 터널링)"가 활성화되면 DNS 트래픽이 커널 레벨에서 인터셉트되고 올바른 VPN 인터페이스를 벗어나지 않는 경우 차단됩니다. 이 경우 Cisco Umbrella Resolver가 스플릿 터널(포함) 컨피그레이션의 일부가 아닌 경우 CSC 모듈에 문제가 발생합니다.

기본적으로 CSC 모듈은 "Tunnel All DNS(모든 DNS 터널링)"에 의해 차단되지 않은 암호화된 DNS(UDP 포트 443)를 사용하므로 이 문제의 영향은 미미합니다. 따라서 DNS 암호화를 사용할 수 없는 네트워크에서만 문제가 발생합니다.

시나리오는 다음과 같습니다.

- 로밍 모듈은 일반 LAN 인터페이스를 통해 Cisco Umbrella로 트래픽을 라우팅하려고 시도합

니다.
- 로컬 네트워크는 DNS 암호화를 허용하지 않으므로 표준 암호화되지 않은 DNS 쿼리를 보냅니다.
- 이 트래픽은 DNS가 VPN을 중단해야 하는 "Tunnel All DNS(모든 DNS 터널)" 기능에 의해 차단됩니다.

이 시나리오에서는 DNS가 예상대로 작동하지 않습니다.

권장 사항

이러한 상황이 발생하지 않도록 Cisco Umbrella는 다음 작업 중 하나를 권장합니다.

- VPN 그룹 정책에서 "Tunnel All DNS"를 비활성화합니다. CSC 모듈은 DNS 라우팅을 처리합니다.
  또는
- 다음 Cisco Umbrella DNS 리졸버를 Split Tunnel (Include) 컨피그레이션에 추가합니다.
  - 208.67.222.222
  - 208.67.220.220
  - 208.67.222.220
  - 208.67.220.222

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.