MacOS에서 DNS 페널티 해결 및 내부 도메인의 액세스 문제

목차

소개

이 문서에서는 DNS 확인에 영향을 주는 최신 버전의 MacOS Big Sur를 사용하여 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

범위

- 네트워크의 AnyConnect 로밍 보안 모듈 또는 Umbrella(예: VA 또는 포워딩)
  - Umbrella 독립형 로밍 클라이언트는 영향을 받지 않습니다. 모든 DNS를 127.0.0.1로 덮어쓰는 단일 DNS 환경이 있습니다.
- 여러 네트워크 인터페이스가 있는 환경에서 발생하지만 내부 주소를 확인할 수 있는 인터페이스는 하나뿐입니다. 예를 들면 다음과 같습니다.
  - VPN 및 off-VPN
  - 다중 NIC - 기업 NIC 1개 및 비기업 NIC 1개

증상

- 공용 도메인에 액세스할 수 있는 기능은 그대로 유지하면서 로컬 도메인에 액세스할 수 없는 경우(또는 간헐적 기능)
  - nslookup은 특별히 영향을 받지 않으며 계속 작동합니다
    - ping, traceroute 등이 잘못 해결되거나 내부 도메인을 찾지 못함

문제

이 문제는 여러 DNS 서버가 있는 경우 DNS 확인 관리 방법을 처리하는 MacOS의 코드로 인해 발생합니다. 단일 네트워크 어댑터의 여러 리졸버 또는 서로 다른 네트워크 어댑터의 여러 리졸버일

수 있습니다. REJECTED(거부)로 응답하는 DNS 서버는 60초 동안 "페널티"됩니다. 이 경우 이 기간 동안 발생하는 모든 추가 DNS 쿼리는 페널티를 받지 않는 대체 DNS 서버에서 시도됩니다.

예를 들어 DHCP가 네트워크에 대해 두 개의 DNS 서버 A와 B를 광고하고 A가 REFUSED로 응답하면 B가 불이익을 받지 않는 한 60초 동안 A보다 B가 선호됩니다.

모든 DNS 서버가 페널티를 받는 경우 MacOS는 가장 최근에 페널티를 받지 않은 서버를 선호합니다. 예를 들어 A가 이미 페널티를 받은 상태에서 B가 페널티를 받는 경우 MacOS는 B보다 A를 선호합니다.

이는 MacOS 11 이상이 DoH(HTTPS를 통한 DNS)를 어설션하려고 시도하는 방식에 의해 누적됩니다. MacOS는 가능한 경우 사용자 집합 DoH 제공자를 선호하도록 프로그래밍됩니다. 이는 Umbrella DNS 보안을 우회합니다. 즉, MacOS가 DoH 요청을 시작할 때 RFC에 따라 거부된 응답을 반환합니다. DNS Penalization 때문에 내부 도메인이 올바르게 확인되지 않을 수 있습니다. 이 문제에 대한 자세한 내용은 다음 문서를 참조하십시오. iOS 14 및 macOS 11에서 DNS 확인자 선택

솔루션

우리는 Apple이 이 행동을 바꿀 계획인지 아니면 Umbrella가 이 문제를 해결하기 위해 그들의 행동을 바꿀 수 있는지 아직 알지 못합니다. 당분간은 다음 두 가지 방법을 통해 해결할 수 있습니다.

옵션 1

그룹 정책에서 스플릿 DNS를 활성화하고 스플릿 DNS 컨피그레이션에 내부 도메인을 구체적으로 추가하여 터널을 통해서만 확인할 수 있도록 합니다. 이렇게 하면 해당 도메인은 네이티브 OS 확인자에 의해 터널을 통해서만 확인 가능한 반면 다른 도메인은 터널 외부에서만 확인 가능합니다.

옵션 2

그룹 정책에서 tunnel-all-DNS를 활성화하여 모든 DNS 트래픽이 터널 외부로 나가지 않도록 합니다.

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.