보안 액세스를 위한 F5 로드 밸런서 DNS 포워딩 컨피그레이션

목차

문제

Umbrella to Secure Access 마이그레이션 중에 F5 로드 밸런서를 클라이언트 DNS 서버로 사용할 때 DNS 확인이 작동하지 않았습니다. DNS 요청이 VIP(가상 IP)에 도달할 때 F5 로드 밸런서가 백엔드 DNS 전달자로 패킷을 전달했지만 엔드포인트 컴퓨터에서 호스트 이름이 확인되지 않았습니다. 가상 어플라이언스를 클라이언트 DNS 서버로 직접 사용할 경우 DNS 확인이 올바르게 수행되었으며, F5 로드 밸런서 컨피그레이션에 문제가 있음을 나타냅니다.

패킷 캡처에서 DNS 회신이 예상 F5 VIP 주소 대신 가상 어플라이언스 IP 주소를 사용한다는 것을 확인했습니다. 클라이언트 컴퓨터는 F5 VIP 주소에서 DNS 회신이 올 것으로 예상했지만 대신 백엔드 가상 어플라이언스 IP 주소에서 회신을 받았습니다.

환경

- Cisco Umbrella to Secure Access 마이그레이션 환경
- DNS 부하 균형 VIP가 구성된 F5 부하 분산 장치
- 여러 DNS 전달자를 백엔드 서버로 사용
- DNS 서버 역할을 하는 가상 어플라이언스
- 로드 밸런서를 통한 DNS 확인이 필요한 클라이언트 엔드포인트

해결

클라이언트 컴퓨터와 가상 어플라이언스 간의 프록시 역할을 제대로 수행하도록 F5 로드 밸런서를

구성하여 문제를 해결했습니다. 주요 컨피그레이션 변경에는 자동 맵 기능을 사용하여 SNAT(Source Network Address Translation)를 활성화하는 작업이 포함되었습니다.

진단 단계 수행

1단계: DNS 확인 동작 확인

문제를 격리하기 위해 F5 로드 밸런서 VIP 및 직접 가상 어플라이언스 연결을 모두 사용하여 DNS 확인을 테스트했습니다.

2단계: DNS 트래픽 캡처 및 분석

F5 로드 밸런서를 통한 DNS 요청 및 응답 흐름을 분석하기 위해 패킷 캡처를 수행했습니다.

3단계: 소스 주소 불일치 확인

분석 결과 DNS 회신에 F5 VIP 주소 대신 가상 어플라이언스 IP 주소가 포함되어 있어 클라이언트 혼란이 발생했습니다.

컨피그레이션 변경

1단계: 액세스 F5 로드 밸런서 컨피그레이션

F5 로드 밸런서 관리 인터페이스로 이동하여 DNS VIP 컨피그레이션을 수정합니다.

2단계: SNAT 자동 매핑 활성화

F5 로드 밸런서에서 자동 매핑하도록 SNAT(Source Network Address Translation)를 구성합니다. 이렇게 하면 F5 디바이스가 클라이언트와 백엔드 DNS 서버 간에 DNS 요청 및 응답을 올바르게 프록시합니다.

3단계: 컨피그레이션 확인

SNAT 자동 맵 컨피그레이션을 구현한 후 DNS 확인이 F5 로드 밸런서를 통해 올바르게 작동하기 시작했습니다.

원인

근본 원인은 F5 로드 밸런서에서 잘못된 SNAT(Source Network Address Translation) 컨피그레이션이었습니다. SNAT 자동 맵이 활성화되지 않으면 F5 디바이스가 DNS 트래픽에 대한 프록시 역할을 제대로 수행하지 못했습니다. 이로 인해 필요한 F5 VIP 주소 대신 가상 어플라이언스 IP 주소를 소스로 사용하여 백엔드 가상 어플라이언스에서 클라이언트 컴퓨터로 DNS 응답이 직접 전송되었습니다. 클라이언트 컴퓨터는 요청을 보낸 동일한 IP 주소(F5 VIP)에서 DNS 응답이 시작되어야 한다고 예상했지만 다른 IP 주소(백엔드 서버)에서 응답을 받아 DNS 확인 오류가 발생했습니다.

관련 콘텐츠

- F5 GTM 로드 밸런싱 구성
- 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.