

Cisco Secure Access Migration으로 전환된 후 일관되지 않은 차단 페이지

목차

문제

마이그레이션 툴을 사용하여 Umbrella에서 Cisco SSE(Secure Access)로 마이그레이션한 후 차단된 웹 트래픽은 Cisco Secure Access 차단 페이지가 아닌 레거시 Umbrella 차단 페이지로 일관성 없이 리디렉션됩니다. 이 문제는 서로 다른 도메인이 차단 규칙을 트리거하여 스플래시 페이지와 차단 사유 문구가 서로 다른 경우 DNS Defense에서 발생합니다. 이로 인해 조직 전체에서 일관성 없는 최종 사용자 차단 알림이 생성됩니다.

관찰된 특정 증상은 다음과 같습니다.

- 차단 규칙은 사용자를 새로운 Cisco Secure Access 차단 페이지가 아닌 이전 Umbrella 차단 페이지로 리디렉션합니다.
- 차단 규칙을 트리거하는 서로 다른 도메인은 서로 다른 스플래시 페이지를 표시합니다
- 최종 사용자에게 일관성 없는 차단 사유 문구 제시
- 이러한 동작은 마이그레이션 후 DNS 방어 기능에 영향을 미칩니다

환경

- 기술: Cisco SSE(Secure Access)
- 마이그레이션: 마이그레이션 툴을 사용하여 SSE에 우산
- 서비스 유형: DNS 방어
- 구축: 마이그레이션 후 환경
- 웹 검사: 웹 스캐닝이 활성화된 FTD 디바이스

해결

FTD 디바이스의 웹 스캐닝은 Cisco Secure Access에 대한 맞춤형 랜딩 페이지의 올바른 렌더링을 방해합니다. 이 문제를 해결하려면 다음 세 도메인에 대해 FTD에서 웹 검사를 우회합니다.

- opendns.com
- cisco-secure.com
- sse.cisco.com

이 방법을 사용하면 기존 Umbrella 차단 페이지를 표시하는 대신 맞춤형 Cisco Secure Access 랜딩 페이지를 올바르게 렌더링할 수 있습니다.

확인 단계

해결 효과를 확인하려면

1단계: 이전에 일관되지 않은 동작을 보였던 도메인에 대해 정책 테스트 실행

2단계: 해결 방법을 구현한 후 페이지 동작 차단 확인

차단된 트래픽이 이제 레거시 Umbrella 페이지 대신 Cisco Secure Access blocking 페이지를 지속적으로 표시하는지 확인합니다.

3단계: 일관된 차단 이유 문구 확인

이제 차단된 모든 도메인에 Cisco Secure Access 표준에 맞는 균일한 차단 사유 메시징이 표시되는지 확인합니다.

원인

이 문제는 FTD 디바이스의 웹 검사 기능이 Cisco Secure Access 맞춤형 랜딩 페이지의 올바른 렌더링을 방해하여 발생합니다. FTD에서 웹 검사가 활성화되면 새 차단 페이지가 올바르게 표시되지 않으므로 시스템이 레거시 Umbrella 차단 페이지로 돌아갑니다. 이로 인해 서로 다른 도메인이 서로 다른 차단 페이지 형식을 트리거할 수 있는 일관되지 않은 사용자 환경이 생성됩니다.

엔지니어링 팀은 이를 Talos 관점에서 변경해야 하는 설계 차원의 문제로 파악했습니다. 현재 아키

텍처에서는 적절한 맞춤형 랜딩 페이지 기능을 보장하기 위해 특정 Cisco 도메인에 대해 웹 검사를 우회해야 합니다.

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.