

Meraki 통합을 통한 보안 액세스를 통한 Azure 호스팅 FQDN 연결 문제

목차

문제

사용자 트래픽이 Meraki를 통해 Cisco Secure Access로 라우팅될 경우, Secure Access 로그에서 트래픽을 "허용"으로 표시하더라도 특정 Azure 호스팅 FQDN에 연결할 수 없습니다. 이 문제는 주로 이러한 FQDN에 대한 비표준 포트를 사용하는 RDP 연결에 영향을 줍니다.

보안 액세스 포털에서 FQDN으로 로그를 검색할 때 DNS 보안 로그만 "허용" 상태를 보여 줍니다. 그러나 비표준 포트의 동일한 대상에 대한 RDP 연결이 실패합니다. FQDN이 IP 주소로 확인되고 Activity Search에서 대상 IP를 사용하면 트래픽을 차단하던 클라우드 방화벽 로그가 표시됩니다.

환경

- Meraki 통합을 통한 Cisco SSE(Secure Access)
- 로컬 브레이크아웃 기능이 있는 Meraki 대시보드
- 비표준 포트에서 RDP 액세스가 필요한 Azure 호스팅 개발 리소스
- Meraki 터널을 통해 보안 액세스로 트래픽 라우팅

해결

즉각적인 해결

영향받는 FQDN을 Meraki 로컬 분할 규칙에 추가하여 다음 섹션에 자세히 설명된 특정 대상에 대해 보안 액세스를 우회합니다.

1단계: Meraki 대시보드 액세스

Meraki Dashboard(Meraki 대시보드)로 이동하여 로컬 분할 구성 섹션을 찾습니다.

2단계: 로컬 분할 규칙 구성

보안 액세스 라우팅을 우회하려면 문제가 있는 FQDN을 로컬 분할 규칙에 추가합니다. 이 컨피그레이션 변경은 보안 액세스 터널을 우회하여 Meraki에서 인터넷으로 직접 트래픽을 라우팅함으로써 영향을 받는 사용자의 액세스를 즉시 복원합니다.

문제 해결 및 분석

1단계: FQDN별 로그 분석

FQDN을 사용하여 보안 액세스 활동 로그를 검색합니다. 이는 주로 DNS 보안 로그를 보여주며 포트 443에서 웹 트래픽에 대한 "허용" 상태를 표시할 수 있습니다.

2단계: 대상 IP별 로그 분석

FQDN을 IP 주소로 확인하고 FQDN 대신 대상 IP를 사용하여 활동 로그를 검색합니다. 이렇게 하면 차단된 트래픽을 보여주는 클라우드 방화벽 로그가 드러나 실제 트래픽 성향을 제공합니다.

3단계: 트래픽 흐름 확인

트래픽이 경로를 따르는 경우에만 문제가 발생하는지 확인합니다. 사용자 → Meraki → 터널 → 보안 액세스 → 인터넷. 로컬 브레이크아웃을 통해 우회하는 테스트로 연결 문제가 해결됩니다.

장기 결의

관찰된 동작은 현재 Secure Access 구현 내에서 예상된 기능으로 식별되었습니다. 다음과 관련된 가시성 및 기능 문제를 해결하기 위해 기능 요청(FR CSE-I-5543)이 열렸습니다.

- FQDN 기반 및 IP 기반 로그 검색 간의 불일치
- DNS 보안과 클라우드 방화벽 로그 간의 일관성 없는 트래픽 속성 보고
- 비표준 포트의 RDP 트래픽에 대한 가시성 향상

원인

이 문제는 비표준 포트에서 RDP를 통해 액세스할 때 Secure Access가 Azure 호스팅 FQDN에 대한 트래픽을 처리하고 보고하는 방법의 불일치로 인해 발생합니다. FQDN으로 로그를 검색할 때 시스템은 주로 웹 트래픽에 대해 "허용됨" 상태를 보여주는 DNS 보안 로그를 표시합니다(일반적으로 포트 443). 그러나 비표준 포트의 실제 RDP 트래픽은 클라우드 방화벽 규칙에 의해 처리됩니다. 클라우드 방화벽 규칙은 FQDN이 아닌 확인된 목적지 IP 주소로 검색할 때만 표시됩니다.

이로 인해 관리자는 FQDN 기반 검색에서 "허용됨" 트래픽을 볼 수 있는 반면, 실제 RDP 연결은 IP 기반 로그 검색에서만 나타나는 방화벽 정책에 의해 차단됩니다. 이 동작은 현재 예상 기능으로 간주되지만 여러 검색 방법 간에 트래픽 보고의 가시성과 일관성을 개선하기 위해 기능 요청이 제출되었습니다.

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.