

보안 액세스 트래픽 조정 동작 및 예외 목록 컨피그레이션

목차

문제

사용자는 Use ZTA to secure all internet destinations(ZTA를 사용하여 모든 인터넷 대상을 보호하며 기본 예외 컨피그레이션을 사용하는 경우 Cisco Secure Access Traffic Steering 동작을 명확하게 지정해야 합니다. 다음과 관련된 구체적인 질문이 제기됩니다.

- 트래픽 조정 결정이 사후 DNS 확인 대상 IP 주소를 기반으로 하는지 여부.
- 조정 프로세스에서 DNS 트래픽 자체가 처리되는 방식.
- 추가 로컬 도메인 항목을 예외 목록의 기본 .local 도메인 항목 이상으로 구성해야 하는지 여부.

해당 컨피그레이션은 다음 위치에 있습니다. Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(제로 트러스트 액세스) > (Zero Trust Access Profiles(제로 트러스트 액세스 프로필)) > Secure Internet Access(보안 인터넷 액세스) > Traffic Steering(트래픽 스티어링) > Use ZTA to secure all internet destinations(ZTA를 사용하여 모든 인터넷 대상 보호)

기본 예외 목록에는 개인 IP 주소 범위(클래스 A, B, C) 및 .local 도메인이 포함되며, 사용자는 이러한 설정의 작동 동작을 이해해야 합니다.

환경

- Cisco 보안 액세스
- ZTA(Zero Trust Access) 컨피그레이션
- 트래픽 조정 기능 활성화됨
- 개인 IP 범위 및 .local 도메인을 포함하는 기본 예외 목록

해결

Cisco Secure Access Traffic Steering 동작은 다음과 같이 작동합니다.

트래픽 조정 결정 프로세스

트래픽 조정 결정은 DNS 확인 후 목적지 IP 주소를 기반으로 합니다. 시스템은 DNS 이름 확인에서 얻은 실제 목적지 IP를 평가하여 트래픽이 Zero Trust Access 보안 스택을 통해 조정되어야 하는지 여부를 결정합니다.

DNS 트래픽 처리

DNS 쿼리 자체는 트래픽 스티어링의 대상이 아닙니다. 엔드포인트가 내부 DNS 서버를 가리키는 DHCP를 통해 DNS 서버 할당을 수신할 경우(일반적으로 프라이빗 IP 주소 사용) 이러한 DNS 통신은 트래픽 조정 메커니즘을 건너뛰고 로컬에서 처리됩니다.

예외 목록 구성

기본 예외 목록에는 다음이 포함됩니다.

- 프라이빗 IP 주소 범위(클래스 A: 10.0.0.0/8, 클래스 B: 172.16.0.0/12, 클래스 C: 192.168.0.0/16)
- .local 도메인

사용자 지정 로컬 도메인(내부 도메인 이름)을 사용하는 조직의 경우, 내부 트래픽이 보안 스택을 통해 불필요하게 조정되지 않도록 예외 목록에 추가 도메인 항목을 추가해야 합니다. 기본 .local 항목은 표준 로컬 네트워크 검색 프로토콜을 포함하지만 모든 조직 내부 도메인을 포함하지는 않습니다.

컨피그레이션 확인

올바른 컨피그레이션을 확인하려면

Connect(연결) > End User Connectivity(최종 사용자 연결) > Zero Trust Access(Zero Trust 액세스)
> Secure Internet Access(보안 인터넷 액세스) > Traffic Steering(트래픽 조정)으로 이동합니다.

예외 목록을 검토하여 필요한 모든 개인 IP 범위 및 조직의 내부 인프라에 특정한 로컬 도메인 이름을 포함하는지 확인합니다.

원인

Cisco Secure Access Traffic Steering 기능의 작동 동작과 관련된 정보 요청입니다. 트래픽 조정 로직의 복잡성과 DNS 확인, IP 기반 라우팅 결정, 예외 처리 메커니즘 간의 상호 작용으로 인해 명확화가 필요합니다.

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.