FDM을 통해 AMP 파일 정책 구성 및 테스트

목차

소개

이 문서에서는 FDM(Firepower Device Manager)을 통해 AMP(Advanced Malware Protection) 파일 정책을 구성하고 테스트하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower 장치 관리자(FDM)
- FTD(Firepower Threat Defense)

사용되는 구성 요소

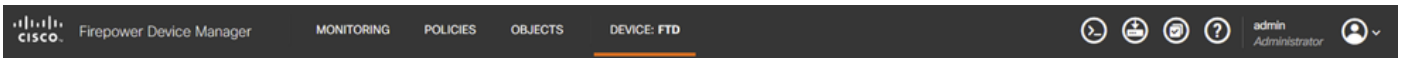
- FDM을 통해 관리되는 Cisco 가상 FTD 버전 7.0
- 평가판 라이센스(평가판 라이센스는 데모용으로 사용됩니다. Cisco의 권장 사항은 유효한 라이센스를 획득하여 활용하는 것입니다.)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

지침

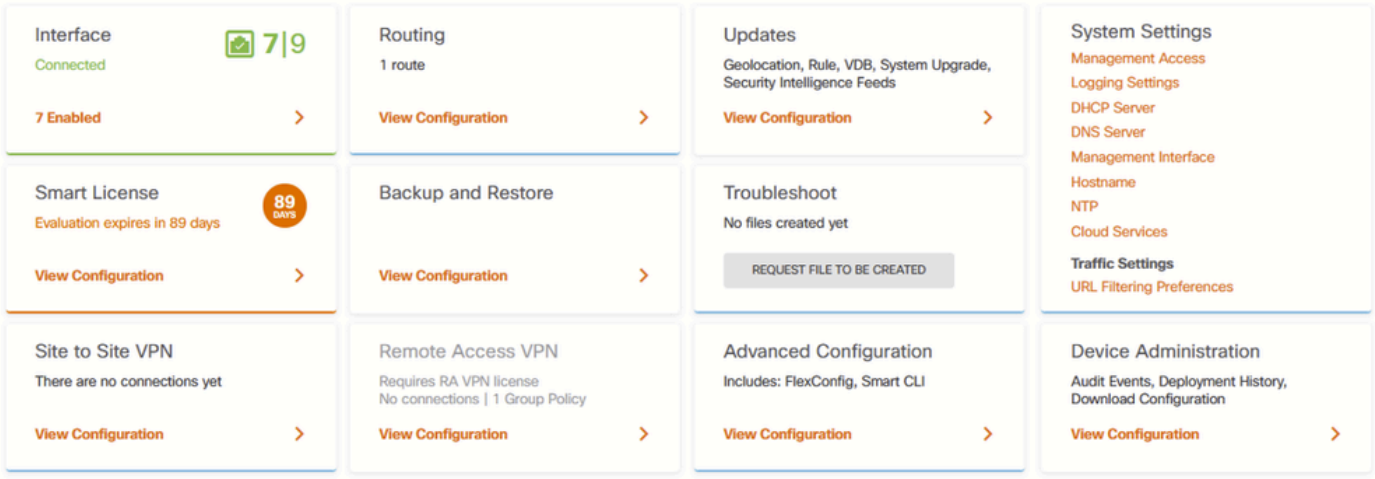
라이센싱

1. 악성코드 라이센스를 활성화하려면 FDM GUI의 DEVICE 페이지로 이동합니다.



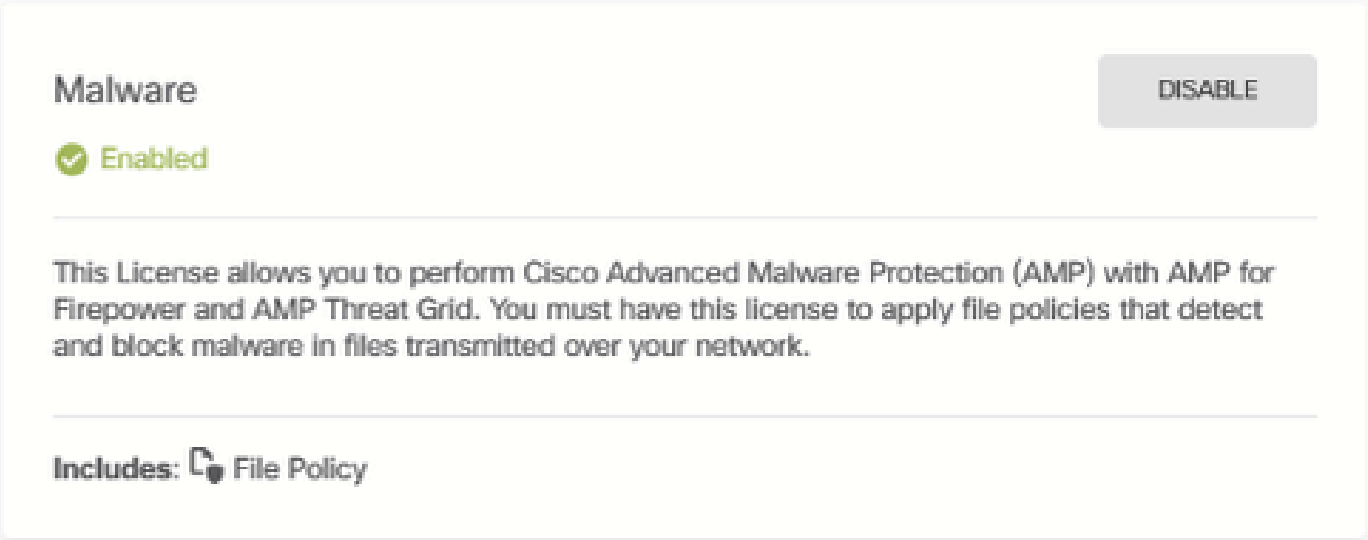
FDM 장치 탭

2. Smart License(Smart 라이센스)라는 상자를 찾고 View Configuration(컨피그레이션 보기)을 클릭합니다.



FDM 장치 페이지

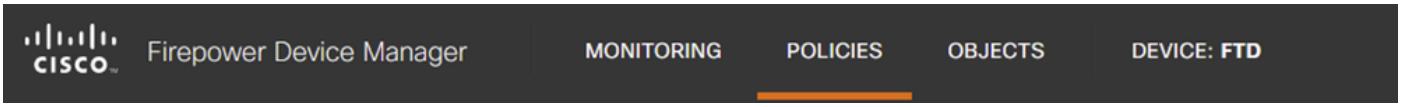
3. Malware라는 라이센스를 활성화합니다.



악성코드 라이센스

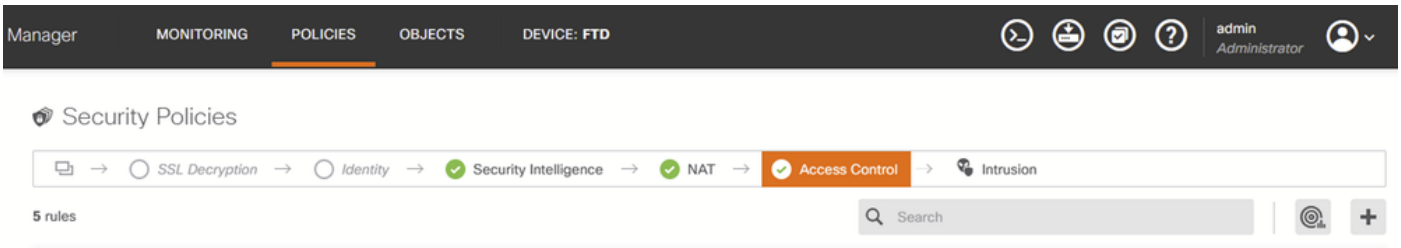
설정

1. FDM에서 정책 페이지로 이동합니다.



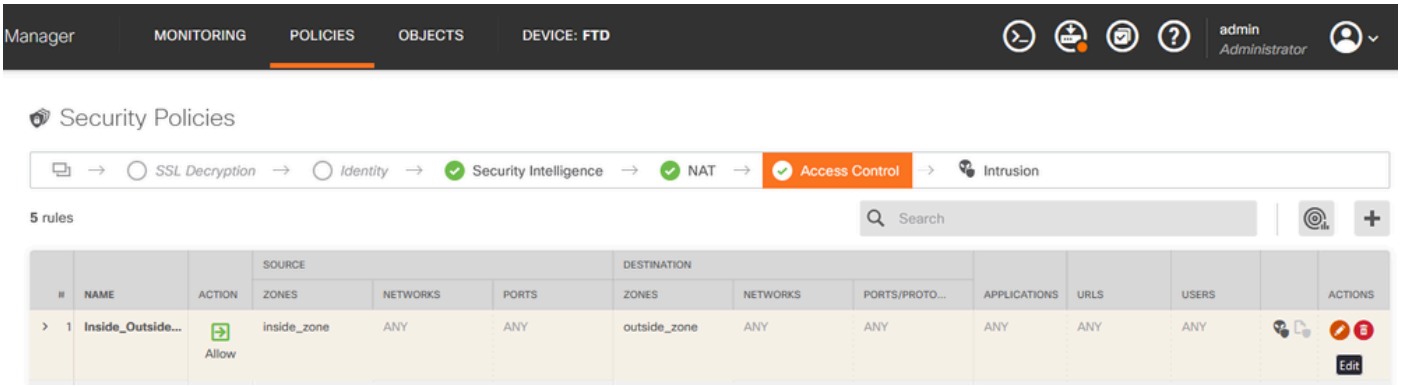
FDM 정책 탭

2. Security Policies(보안 정책) 아래에서 Access Control(액세스 제어) 섹션으로 이동합니다.



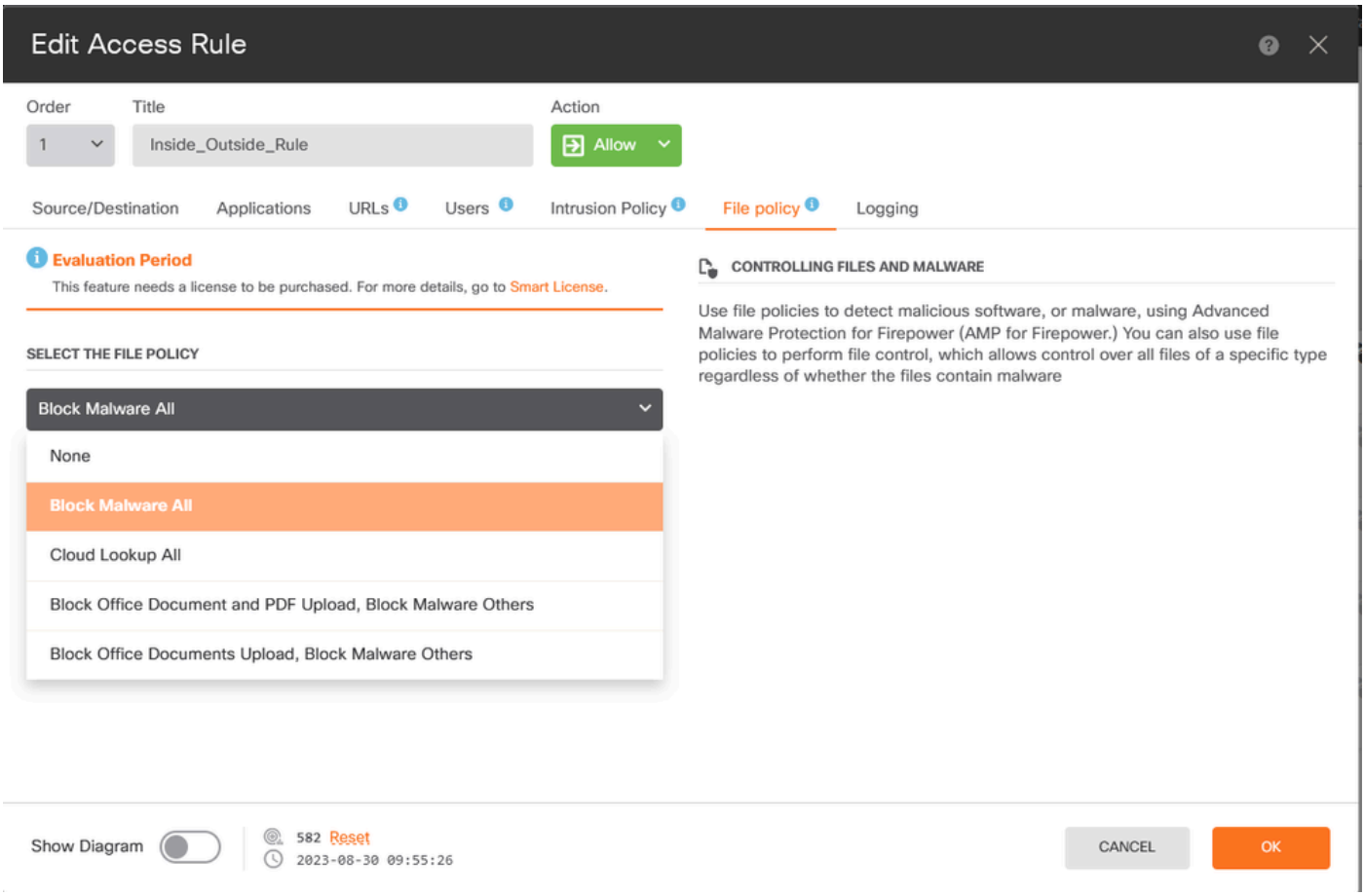
FDM 액세스 제어 탭

3. 액세스 규칙을 찾거나 생성하여 파일 정책을 구성합니다. Access Rule 편집기를 클릭합니다. 액세스 규칙을 생성하는 방법에 대한 지침은 이 링크를 참조하십시오.



FDM 액세스 제어 규칙

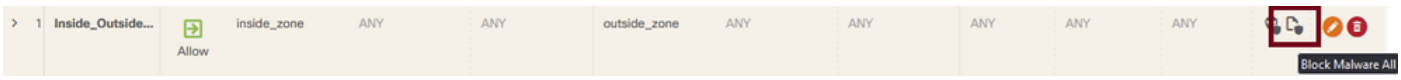
4. 액세스 규칙에서 파일 정책 섹션을 클릭하고 드롭다운에서 선호하는 파일 정책 옵션을 선택합니다. OK(확인)를 클릭하여 변경 사항을 규칙에 저장합니다.



FDM 액세스 제어 규칙 파일 정책 탭

5. 파일 정책 아이콘이 활성화되어 있는지 확인하여 파일 정책이 액세스 규칙에 적용되었는지 확인합니다.

파일



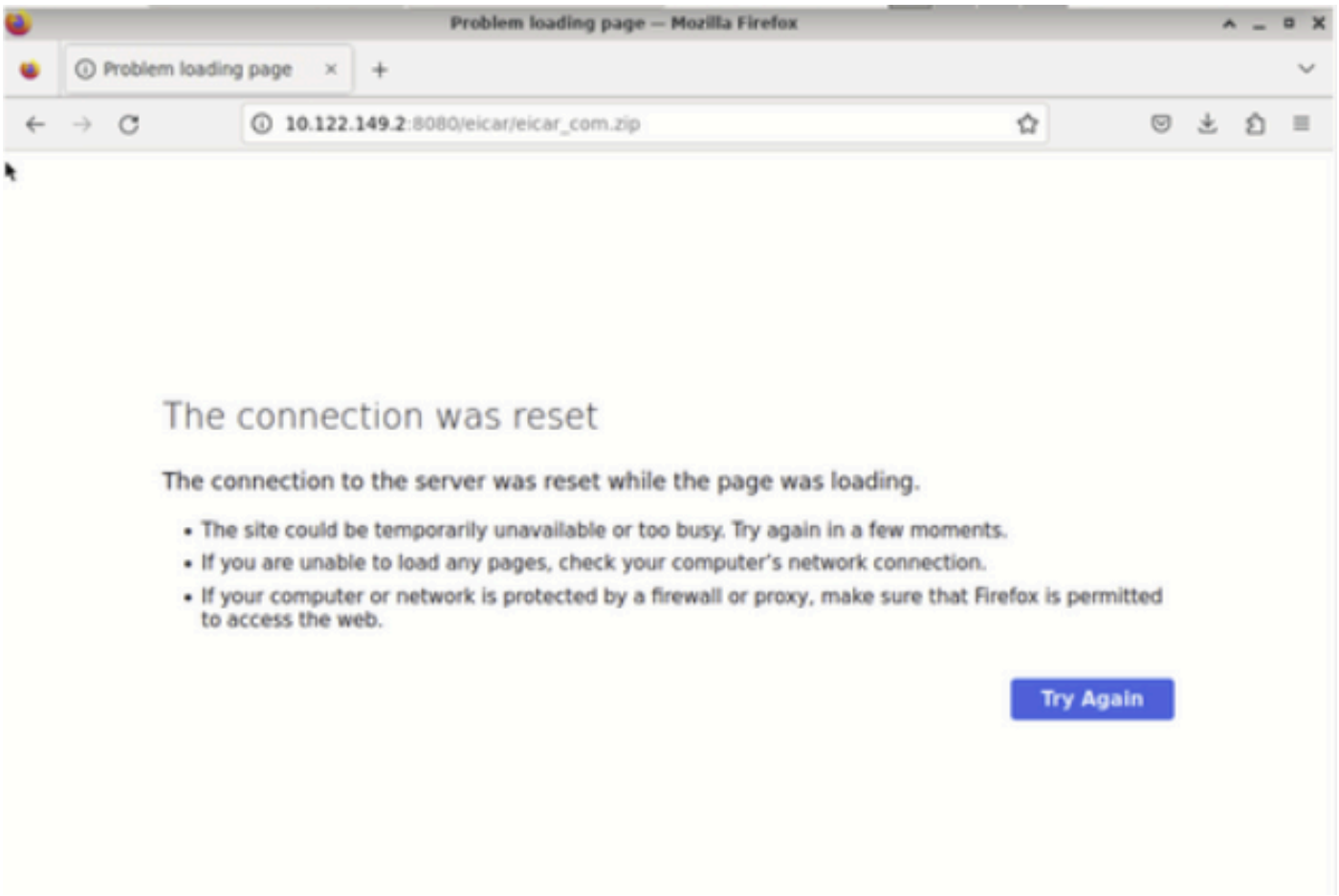
정책 아이콘 사용

6. 관리되는 장치에 대한 변경 사항을 저장하고 구축합니다.

테스트

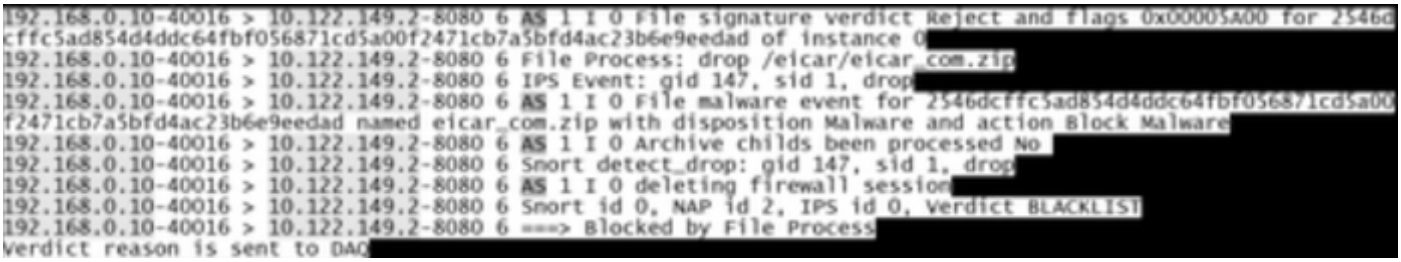
악성코드 차단을 위해 구성된 파일 정책이 작동하는지 확인하려면 이러한 테스트 시나리오를 사용하여 최종 호스트의 웹 브라우저에서 악성코드 테스트 파일을 다운로드합니다.

이 스크린샷에 표시된 대로 웹 브라우저에서 악성코드 테스트 파일을 다운로드하려는 시도가 성공하지 못했습니다.



브라우저 다운로드 테스트

FTD CLI에서 시스템 지원 추적은 파일 프로세스가 파일 다운로드를 차단했음을 보여줍니다. FTD CLI를 통해 시스템 지원 추적을 실행하는 방법에 대한 지침은 이 링크를 참조하십시오.



시스템 지원 추적 테스트

파일 정책 컨피그레이션이 악성코드를 성공적으로 차단했음을 확인합니다.

문제 해결

이전 컨피그레이션을 사용할 때 악성코드가 성공적으로 차단되지 않은 경우 다음 트러블슈팅 제안을 참조하십시오.

1. 악성코드 라이센스가 만료되지 않았는지 확인합니다.

2. 액세스 제어 규칙이 올바른 트래픽을 대상으로 하는지 확인합니다.

3. 선택한 파일 정책 옵션이 대상 트래픽과 원하는 악성코드 차단에 대해 올바른지 확인합니다.

여전히 문제를 해결할 수 없는 경우 Cisco TAC에 추가 지원을 문의하십시오.

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.