경고 규칙 작업 구성

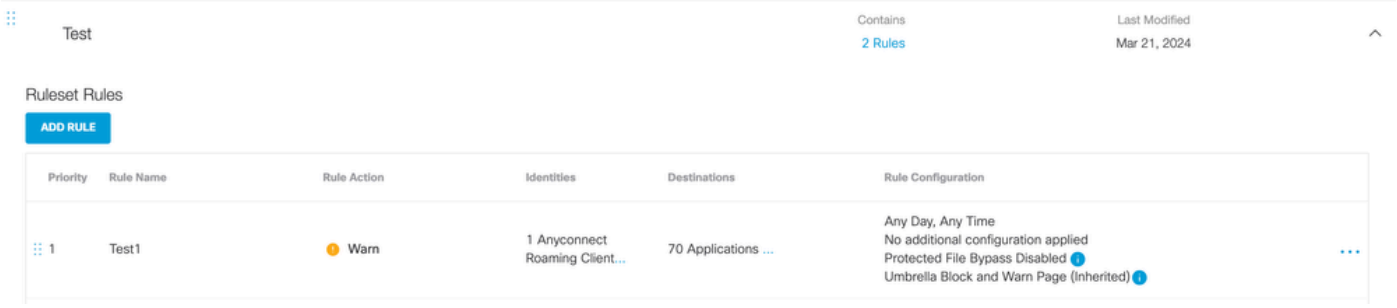
목차

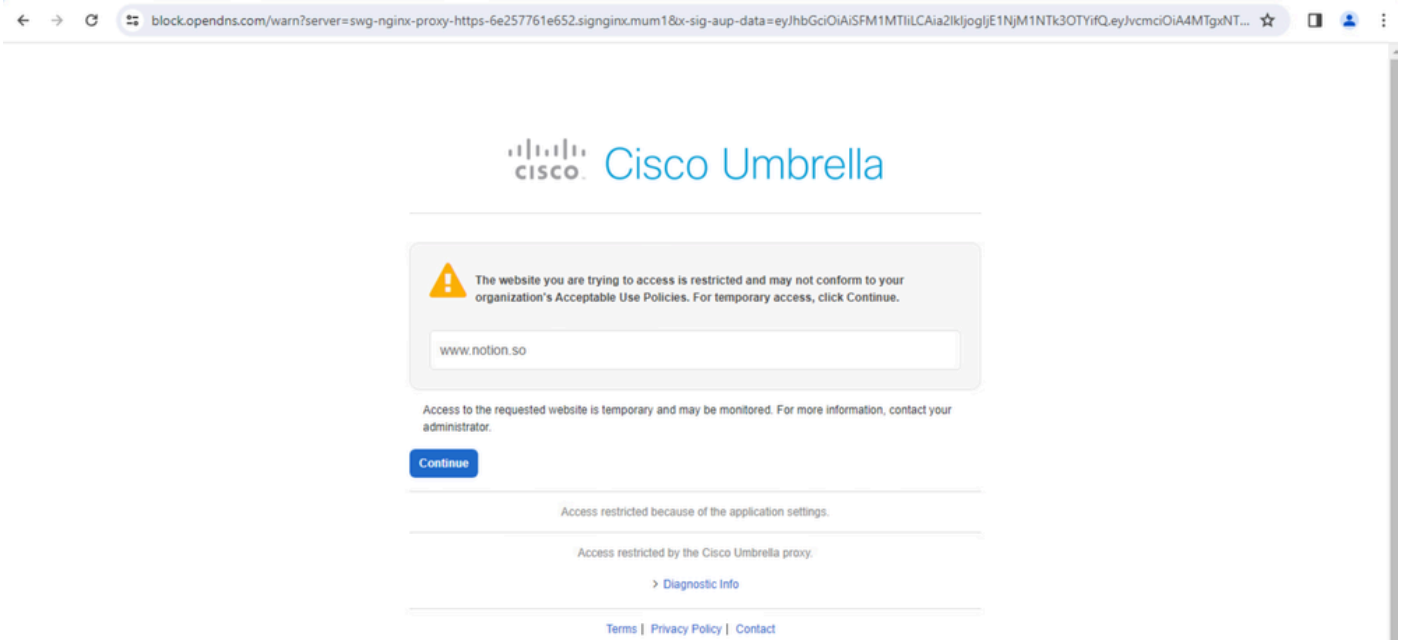
소개

이 문서에서는 Warn 규칙 작업 기능, 해당 컨피그레이션 및 Cisco Umbrella 내의 관련 제한에 대한 포괄적인 이해를 설명합니다.

개요

사용자가 Cisco Umbrella의 Warn(경고) 카테고리 아래에 분류된 웹 사이트에 액세스하려고 하면 Warn(경고) 페이지가 나타납니다. 계속하려면 사용자가 Warn(경고) 페이지를 클릭해야 합니다.



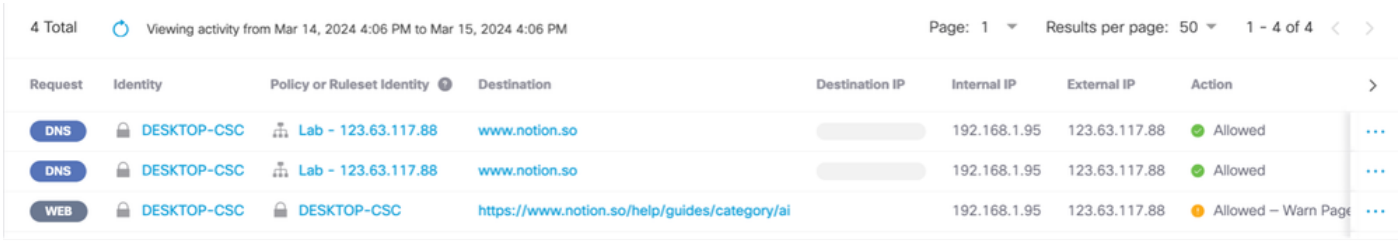


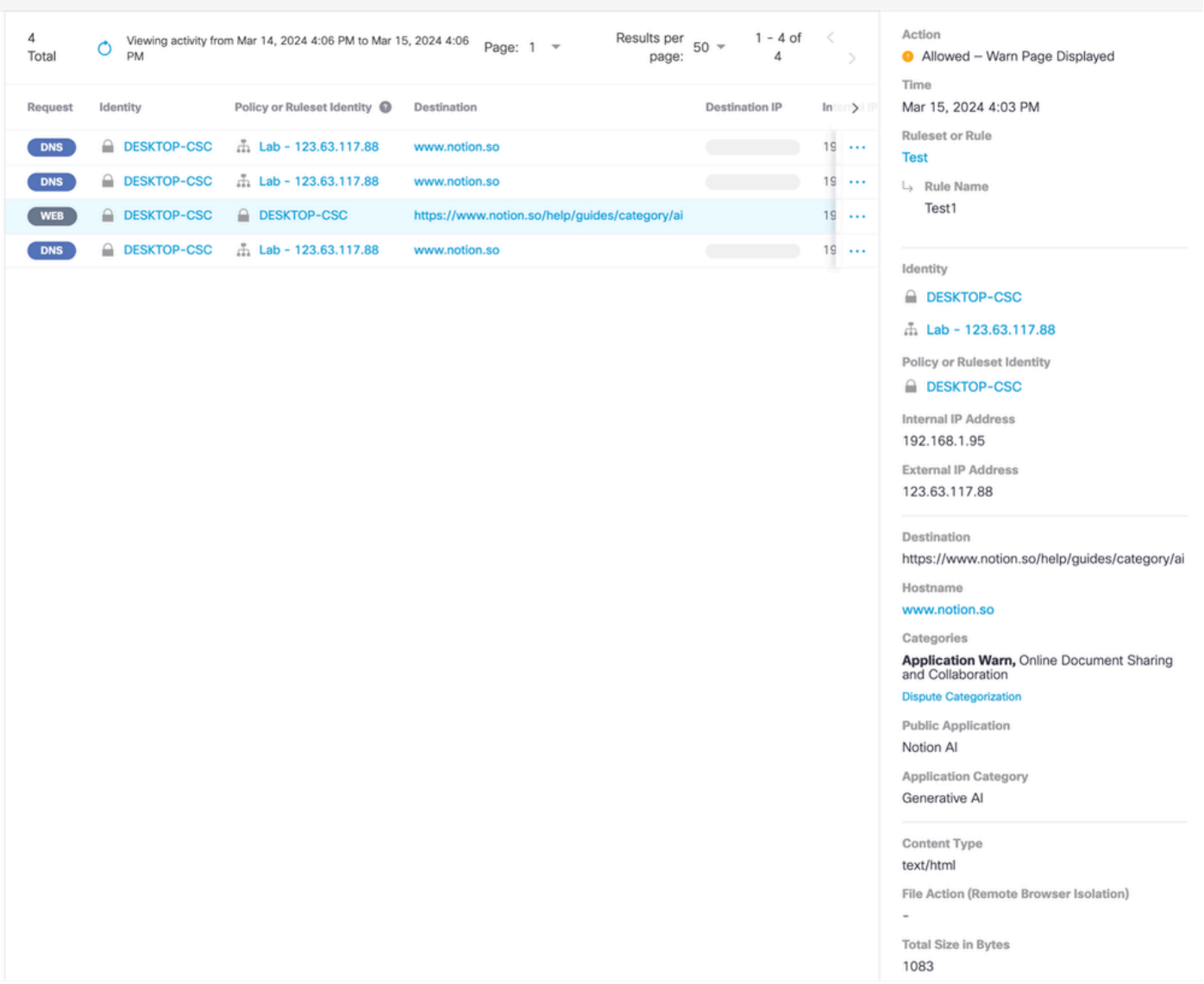
액세스 기간

Warn(경고) 페이지를 클릭하면 요청한 대상에 대한 액세스가 1시간의 제한된 기간 동안 부여됩니다. 이 기간이 지나면 Warn 페이지가 다시 나타나므로 사용자가 계속 액세스하려면 다시 클릭해야 합니다.

활동 보고서 개요

경고 페이지 상호 작용은 Umbrella의 활동 보고서 내에 기록되므로 관리자는 경고 규칙 작업 기능에 의해 트리거된 경고 및 사용자 상호 작용에 대한 정보를 볼 수 있습니다.





대상 목록 제한 사항

경고 페이지 기능을 활성화하면 대상 목록에 대한 액세스가 제한됩니다. 사용자는 경고에서 분류된 웹 사이트에 대해 Destination List 옵션을 선택할 수 없습니다.

HTTPS 검사 활성화

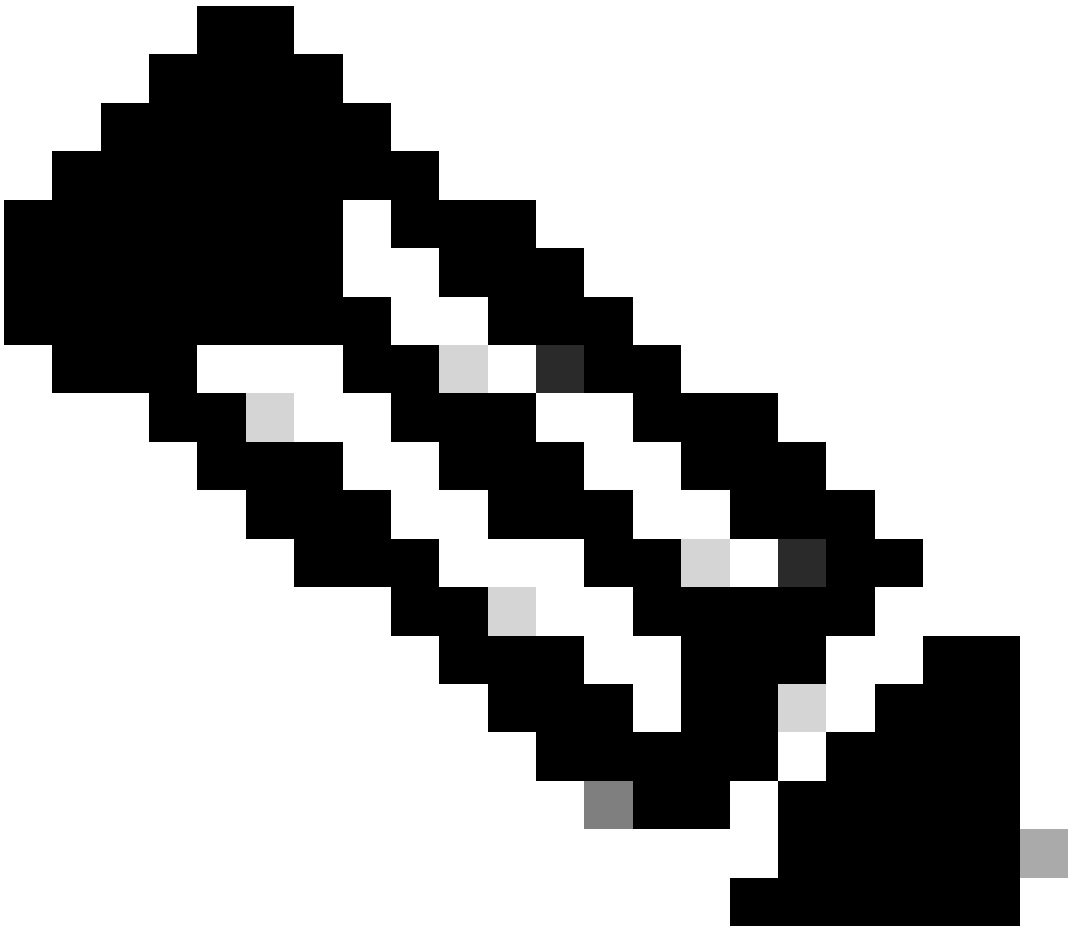
경고 페이지 기능을 효과적으로 적용하려면 Cisco Umbrella 내에서 HTTPS 검사를 활성화해야 합니다. HTTPS 검사는 HTTPS 트래픽을 해독 및 검사하여 Umbrella에서 암호화된 연결에 대해 경고 페이지를 적용할 수 있게 합니다.

사용자 지정 경고 페이지 만들기

관리자는 맞춤형 메시징이 포함된 맞춤형 경고 페이지를 만들 수 있습니다. 규칙 세트에 규칙을 추

가할 때 이 사용자 지정 경고 페이지를 선택하여 사용자에게 맞춤형 경고 경험을 제공할 수 있습니다.

맞춤형 경고 페이지를 생성하는 방법에 대한 자세한 지침과 경고 규칙 작업 컨피그레이션에 대한 자세한 내용은 공식 설명서를 참조하십시오. Create Custom Warn(사용자 지정 경고 생성) 페이지.



> 참고: 선택적인 암호 해독 목록 예외는 프록시의 특정 정책 및 기능 적용 기능에 영향을 미치며, 경고 페이지가 그중 하나입니다.

결론

Warn 규칙 작업 컨피그레이션 및 관련 제한을 이해하는 것은 Cisco Umbrella 내에서 효과적인 보안 정책을 구현하는 데 필수적입니다. 조직은 경고 페이지 및 HTTPS 검사를 활용하여 보안 상태를 강화하고 사용자에게 안전한 검색 환경을 제공할 수 있습니다.

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.