플로우 컬렉터의 목록 무시 기능 구성

목차

소개

이 문서에서는 Ignore List(목록 무시)를 사용하여 특정 내보내기에서 들어오는 netflow를 거부하도록 SNA 흐름 컬렉터를 구성하는 방법에 대해 설명합니다.

배경 정보

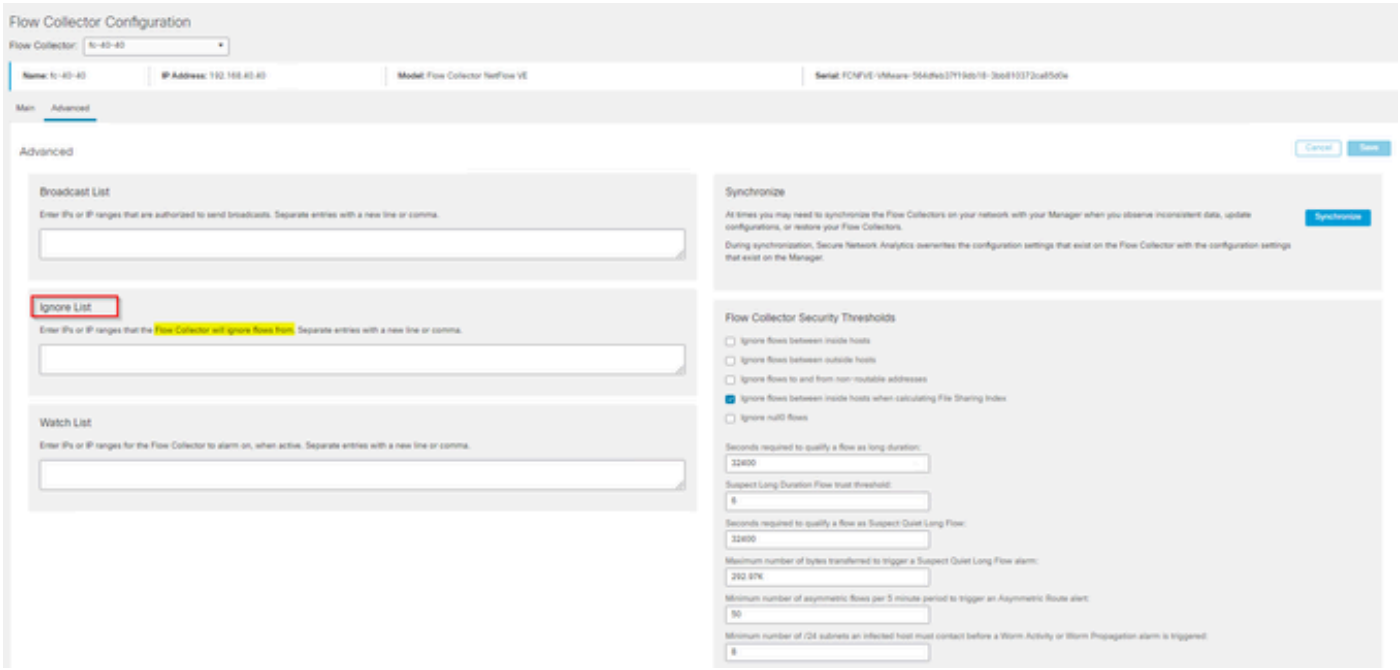
종종 문제가 제기됩니다. "SNA 플로우 컬렉터가 특정 내보내기의 수신 netflow를 거부하도록 할 방법이 있습니까?"

대답은 "예"입니다. 이 작업은 Flow Collector "Ignore List" 기능을 사용하여 수행됩니다.

구성

목록 무시 기능은 플로우 컬렉터에만 해당됩니다. SNA 7.x 이후 버전에서는 이 기능을 SNA Manager 웹 UI의 Flow Collector 컨피그레이션 페이지 내에서 사용할 수 있습니다.

이 페이지에서는 Flow Collectorcompletelyignorestraffic이 있는 호스트 또는 서브넷을 무제한 지정할 수 있습니다. Flow Collector에서 이러한 IP 주소로 인한 트래픽을 발견하면 해당 트래픽을 그래프 또는 테이블에서 제외합니다. 호스트에서 이동하는 모든 트래픽을 신뢰할 수 있는지 확인하십시오.보안 네트워크 분석이 트래픽을 분석하거나 이러한 호스트를 포함하도록 스푸핑된 트래픽은 분석하지 않습니다. 이러한 호스트/서브넷 중 하나를 포함하는 네트워크에서 공격이 시작된 경우 Flow Collector에서 이를 보고할 수 없습니다.



FAQ

Smart Licensing의 FPS(Flows Per Second) 계산에 대한 Ignore List의 효과는 무엇입니까?

대답: 호스트 IP 주소 또는 범위를 무시 목록에 추가하면 이러한 플로우가 SMC로 전송되어 Smart License 보고에 사용되는 계산된 FPS 속도를 기준으로 계산되지 않습니다. SMC 대시보드에 표시된 플로우 추세 그래프에서 더 이상 플로우가 표시/계산되지 않습니다.

클라이언트가 스플릿 터널 모드에 있을 때 NVM 흐름을 처리할 때 무시 목록 기능은 어떻게 사용됩니까?

고객은 AnyConnect를 구성하여 온네트워크 및 오프네트워크 트래픽(스플릿 터널이라고도 함)을 전송할 수 있습니다. 네트워크 외부 트래픽은 중복되는 IP를 포함할 가능성이 가장 높은 엔드포인트 로컬 IP 주소를 사용합니다. SNA는 중복 IP를 지원하지 않습니다.따라서 목록 무시 기능을 사용하여 스플릿 터널 문제를 우회하여 탐지에 대한 NVM 기반 흐름의 이점을 유지하는 것이 제안되었습니다.

이 활용 사례에서는 네트워크 외부 NVM 흐름이 flow cache, flow_stats, Flow Search, Custom Security Events에서 → 않도록 "Ignore List"를 구성합니다

1. IP 주소 및 네트워크 마스크를 Ignore List(무시 목록)에 추가합니다(예: 192.168.1.0/24, 127.0.0.1/24 추가).
2. nvm_flows가 여전히 NVM 플로우로 채워졌는지 확인합니다.
3. src 또는 dst IP 중 하나가 Ignore List(무시 목록)에 있는 경우 flow_stats에 NVM 흐름이 없는지 확인합니다

전체 내보내기의 플로우를 무시하려면 무시 목록을 사용할 수 있습니까? 아니요. 무시 목록은 내보내기 데이터가 아닌 플로우 데이터를 기반으로 하므로, 내보내기 IP 주소를 무시 목록에 추가하면 특정 내보내기의 모든 플로우 레코드를 무시하는 대신 내보내기 IP가 플로우의 소스 또는 대상으로 나열된 플로우 데이터를 효과적으로 무시합니다

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.