보안 네트워크 분석 가상 어플라이언스 네트워크 인터페이스 컨피그레이션 제한

목차

문제

플로우 컬렉터에 가상화 플랫폼을 통해 여러 네트워크 인터페이스가 할당된 비데이터 저장소의 SNA(Secure Network Analytics)에 대한 구축 시나리오를 평가하고 있었습니다.

발생한 구체적인 질문은 다음과 같습니다.

- 가상 Flow Collector가 SNA 내부 통신용 NIC와 NetFlow 수신용 NIC 2개로 작동할 수 있는지 여부
- 내부 통신 세그먼트가 인터넷에 액세스할 수 없을 때 위협 피드를 가져오기 위해 Virtual Manager 어플라이언스를 여러 NIC로 구성할 수 있는지 여부

환경

- Secure Network Analytics(Stealthwatch) 버전 최대 7.6.0
- 모든 SNA 구성 요소의 가상 어플라이언스 버전(Manager, Flow Collector)
- 내부 통신 및 NetFlow 수신 세그먼트가 분리된 네트워크 아키텍처

해결

Cisco SNA(Secure Network Analytics) Flow Collector는 2개의 NIC 인터페이스를 사용하여 구축할 수 있으며, 랩 환경에서 이 동작이 검증되었습니다.

1. 2개의 인터페이스 — 관리 액세스 및 NetFlow 수신

- Flow Collector는 관리 액세스를 위한 하나의 인터페이스와 NetFlow 수신 전용 두 번째 인터페이스로 구성할 수 있습니다.
- 그러나 관리 액세스는 인터페이스(management 또는 NetFlow)를 통해 연결 가능합니다. 현재 인터페이스를 의도한 목적에 엄격하게 제한하는 옵션은 없습니다.

2. 2개의 인터페이스 — NetFlow 수신 및 위협 피드 수신

- 위협 피드 업데이트는 Flow Collector에서 인터넷 액세스를 사용하여 검색됩니다.
- 관리 인터페이스 IP에 직접 인터넷 액세스가 없는 경우 Flow Collector에서 사용 가능한 프록시 옵션을 구성하여 이 요구 사항을 충족할 수 있으며, 두 번째 인터페이스에서는 계속해서 NetFlow를 수신합니다.

범위에 대한 중요 참고 사항
두 시나리오 모두 랩 설정에서만 검증되었으며 SNA 설계 가이드에 문서화되지 않았습니다. 따라서 공식적으로 발표된 설계 권장 사항이 아니라 관찰된 행동으로 취급해야 합니다. 이러한 구축을 계획하는 고객은 먼저 자체 테스트 환경에서 이를 검증하는 것이 좋습니다.

원인

이 동작은 Secure Network Analytics Flow Collector 어플라이언스 아키텍처의 설계에 따라 달라집니다. 어플라이언스는 추가 NIC 할당을 지원하며, 기본 인터페이스가 관리에 사용되는 동안 보조 인터페이스에서 텔레메트리(NetFlow)를 수신할 수 있습니다. 그러나 어플라이언스 소프트웨어는 구성된 모든 인터페이스와 주소가 지정된 인터페이스에 연결된 어플라이언스 관리 서비스(어플라이언스 관리 UI, SSH 및 SNA 어플라이언스 간 통신)를 실행하며, 인터페이스별 서비스 바인딩 또는 액세스 제어 옵션은 표시하지 않습니다. 따라서 관리 액세스는 두 NIC 중 하나에서 연결 가능한 상태로 유지되며 이를 위해 지정된 인터페이스로 제한할 수 없습니다.

마찬가지로, 위협 피드 검색은 특정 NIC에 연결되지 않습니다. 업데이트 프로세스는 어플라이언스 라우팅 테이블을 기반으로 아웃바운드 연결을 시작하므로 인터넷 서비스에 대한 유효한 경로를 가진 모든 인터페이스가 요청을 요청합니다. 관리 인터페이스에 직접 인터넷 연결이 없는 경우 어플라이언스 관리자 내의 프록시 컨피그레이션 옵션은 승인된 프록시 서버를 통해 아웃바운드 요청을 릴레이하므로 인터페이스 역할을 변경하지 않고 위협 피드를 성공적으로 업데이트할 수 있습니다.

다중 NIC Flow Collector 구축 및 인터페이스-역할 분리는 Secure Network Analytics Design Guide에서 다루지 않으므로, 이러한 동작은 지원되지 않는 것이 아니라 문서화되지 않으며, 조사 결과는 랩 검증만을 기반으로 합니다.

관련 콘텐츠

- Secure Network Analytics Virtual Edition Appliance 설치 설명서

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.