Secure Network Analytics에서 NetFlow/IPFIX 텔레메트리 수집 문제 해결

목차

소개

이 문서에서는 SNA(Secure Network Analytics)에서 Netflow 텔레메트리 수집 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

- Cisco SNA 지식
- NetFlow/IPFIX 지식

요구 사항

- 7.5.0 이상의 보안 네트워크 분석
- Flow Collector in 7.5.0 이상
- 플로우 컬렉터에 대한 sysadmin으로서의 CLI 액세스
- 플로우 컬렉터에 대한 관리자 UI 액세스

컨피그레이션 가이드

- [보안 네트워크 분석에서 텔레메트리 수집을 위한 NetFlow/IPFIX 구성](#)

사용되는 구성 요소

- SNA Manager 및 Flow Collector on 7.5.0
- Wireshark 소프트웨어

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.

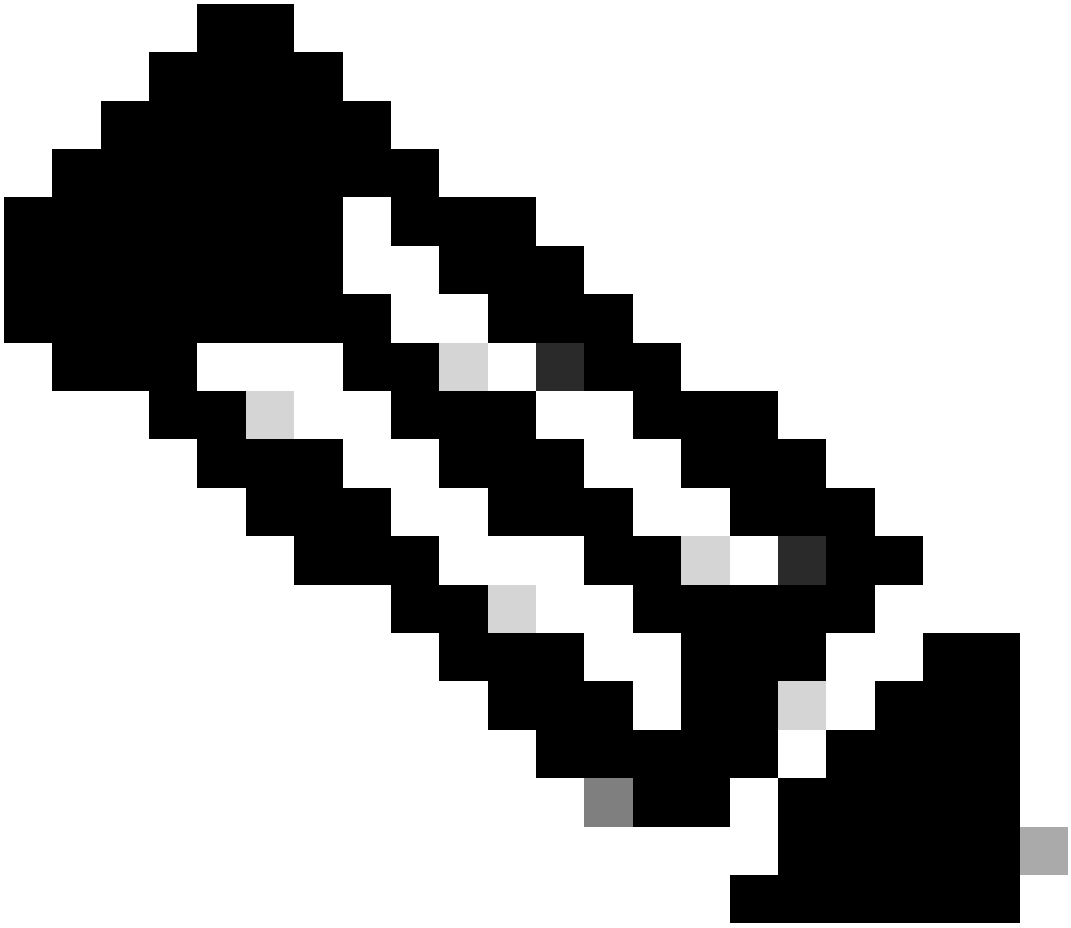
배경 정보

Flow Collector는 Secure Network Analytics로 전송되는 플로우를 수집, 처리 및 저장하는 SNA 어플라이언스입니다. NetFlow 버전 9 또는 IPFIX의 경우 네트워크 트래픽과 관련된 추가 정보를 추가하기 위해 NetFlow/IPFIX 템플릿에 여러 필드를 포함할 수 있지만, 플로우 컬렉터가 이러한 플로우를 처리하기 위해 NetFlow/IPFIX 템플릿에 포함해야 하는 9개의 특정 필드가 있습니다. Flow Collector는 유효하지 않은 템플릿을 포함하는 수신 플로우를 처리하지 않으므로, SNA는 웹 UI 또는 데스크톱 클라이언트 아래에 해당 내보내기의 플로우 정보를 표시하지 않습니다.

필수 필드

텔레메트리 수집을 위해 NetFlow/IPFIX 템플릿에 다음 필드를 포함해야 합니다. Secure Network Analytics에서 수신 흐름을 처리할 수 있도록 NetFlow/IPFIX 템플릿에 이 9개 필드가 포함되어 있는지 확인합니다.

- 소스 IP 주소
- 대상 IP 주소
- Source Port(소스 포트)
- Destination Port(대상 포트)
- 레이어 3 프로토콜
- 바이트 수
- 패킷 수
- 플로우 시작 시간
- 플로우 종료 시간



참고: NetFlow/IPFIX 컨피그레이션에는 더 많은 필드가 포함될 수 있지만, 이전 필드는 Secure Network Analytics for Telemetry Ingest의 최소 요구 사항입니다.

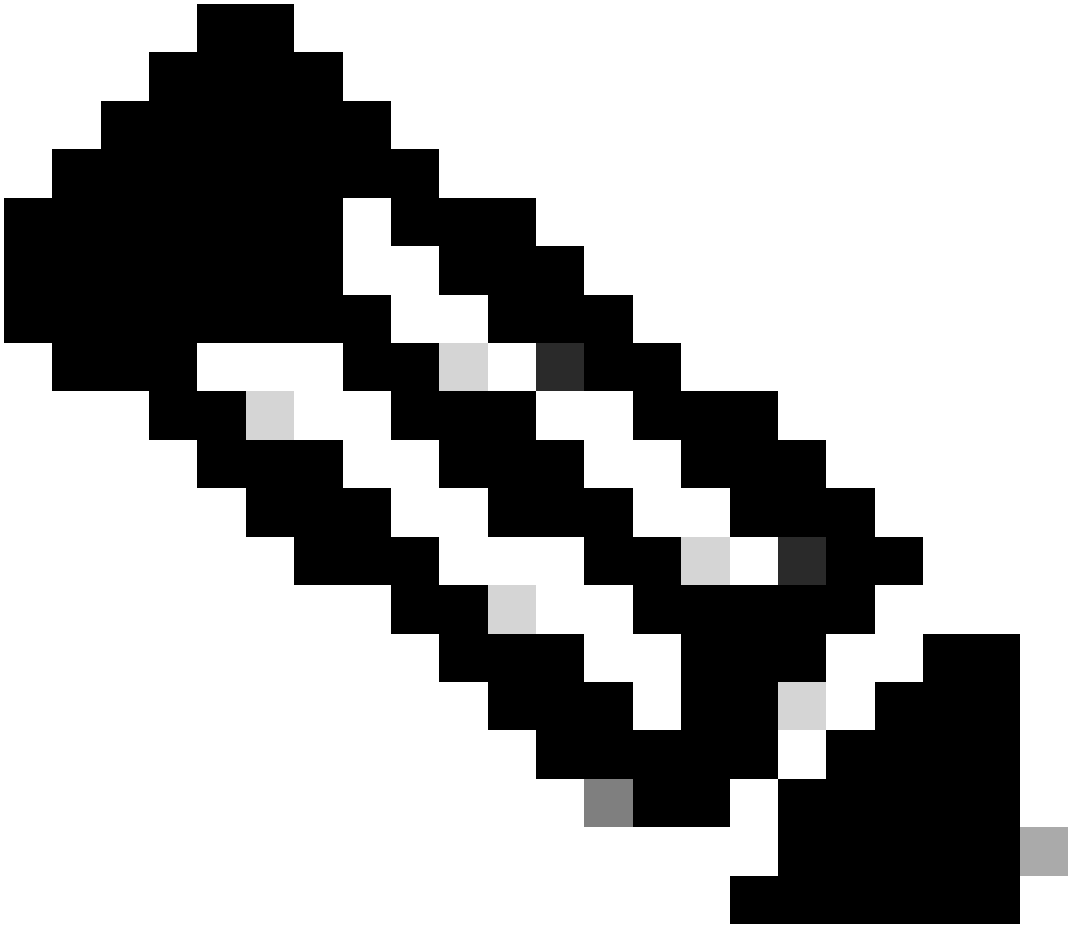
문제 해결 프로세스

NetFlow/IPFIX 텔레메트리 수집 확인

SNA Flow Collector가 엑스포터로부터 NetFlow/IPFIX 텔레메트리를 수신하여 삽입하는지 확인하려면 다음을 수행합니다.

1. 관리자 크리덴셜을 사용하여 SNA Flow Collector Admin UI에 로그인합니다. https://<Flow Collector IP Address>/swa/login.html
2. 왼쪽 패널에서 Support(지원) > Browse Files(파일 찾아보기)로 이동합니다
3. 다음 폴더로 이동합니다. sw > 오늘 > 로그
4. sw.log 파일을 클릭하여 로컬 시스템에 다운로드하고 텍스트 편집기에서 엽니다.
5. 로그 하단에서 이러한 행을 검색합니다. 이 요약은 5분마다 작성됩니다.

```
18:45:00 I-sch-t: process_5_min_period: begin
18:45:00 I-sch-t: process_5_min_period: periods(177)
18:45:00 S-per-t: Performance Period 177
18:45:00 S-per-t:     Engine status Status normal
18:45:00 S-per-t:     Processed 6948 flows at 24 fps this period
18:45:00 S-per-t:     Processed 4226 biflows at 15 fps this period
18:45:00 S-per-t:     Dropped 0 flows this period
18:45:00 S-per-t:     Discarded 4358 flows this period due to insufficient template data
18:45:00 S-per-t:     Processed 1838743 flows at 35 fps today
18:45:00 S-per-t:     Dropped 0 flows today
18:45:00 S-per-t:     Discarded 11069 flows today due to insufficient template data
18:45:00 S-per-t:     Process instance 0 processed 3372 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 0 processed 2066 biflows at 7 fps this period
18:45:00 S-per-t:     Process instance 1 processed 3576 flows at 12 fps this period
18:45:00 S-per-t:     Process instance 1 processed 2160 biflows at 8 fps this period
18:45:00 S-per-t:     Inserted 2048 flow stats at 7 fps this period
18:45:00 S-per-t:     Inserted 2013 interface stats at 7 fps this period
18:45:00 S-per-t:     Inserted 470932 flow stats at 9 fps today
18:45:00 S-per-t:     Inserted 678994 interface stats at 13 fps today
```



참고: 행 8은 마지막 기간의 템플릿 데이터가 부족하여 삭제된 플로우가 있음을 나타냅니다 .

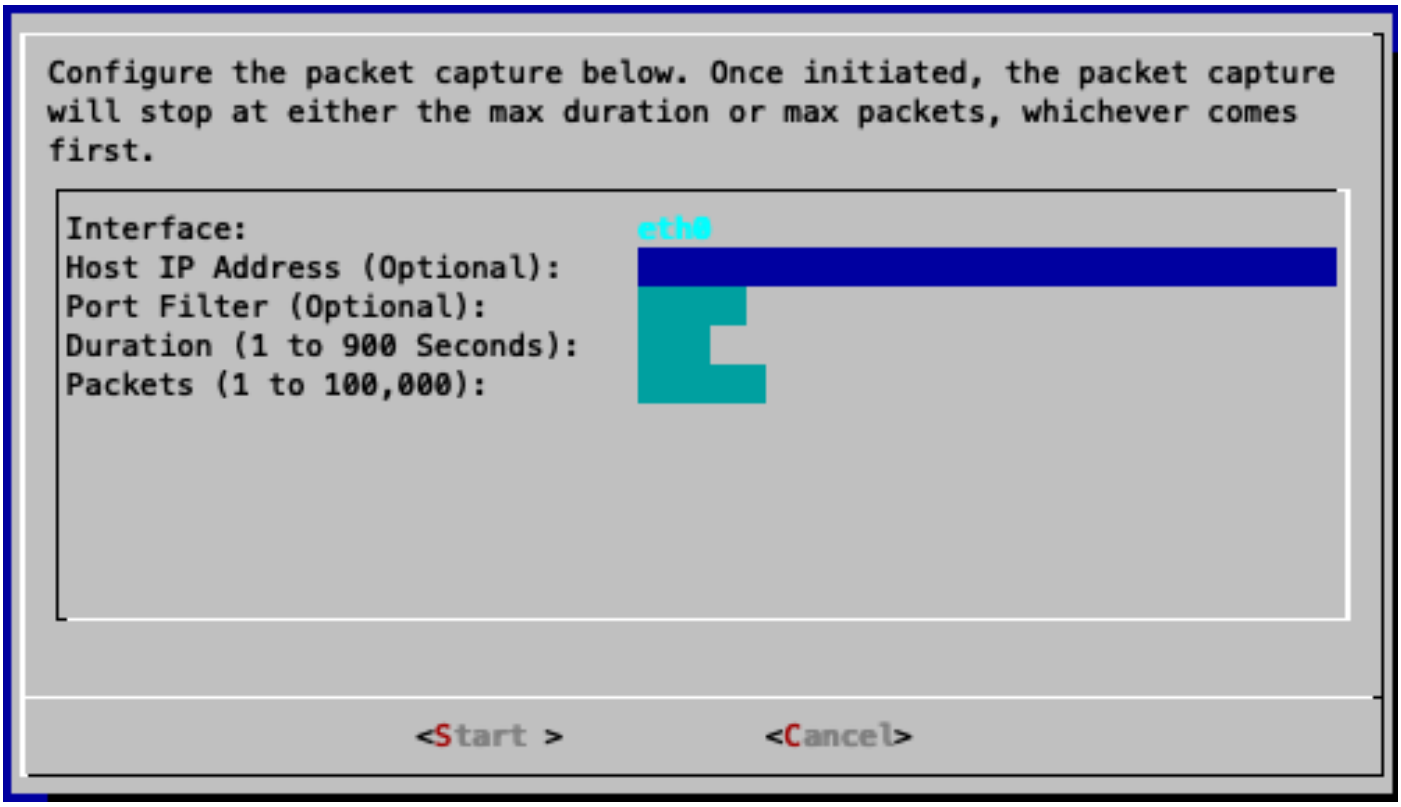
NetFlow/IPFIX 템플릿 확인

NetfFlow/IPFIX 템플릿에 포함된 필드를 확인하려면 다음을 수행합니다.

1. sysadmin 크리덴셜을 사용하여 SNA Flow Collector CLI에 로그인합니다.

2. SystemConfig 메뉴에서 다음으로 이동합니다. Advanced(고급) > Packet Capture(패킷 캡처)

3. SNA에 플로우를 표시하지 않는 익스포터 정보를 입력합니다.



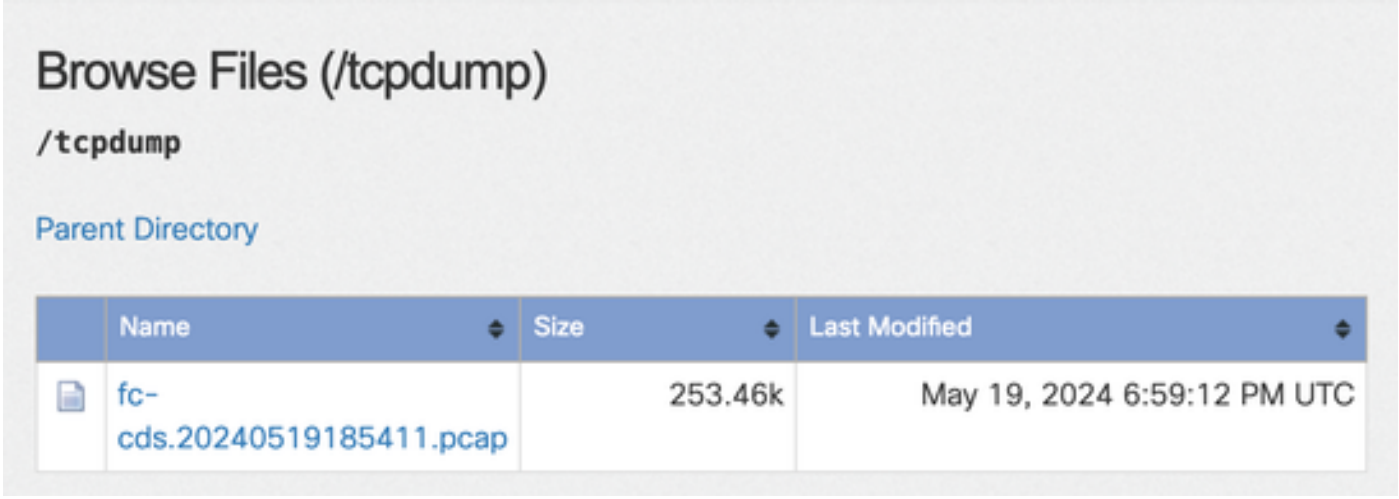
4. 프로세스가 완료될 때까지 기다립니다.

5. 파일을 다운로드하려면 관리자 자격 증명으로 SNA Flow Collector Admin UI에 로그인합니다. https://<Flow Collector IP Address>/swa/login.html

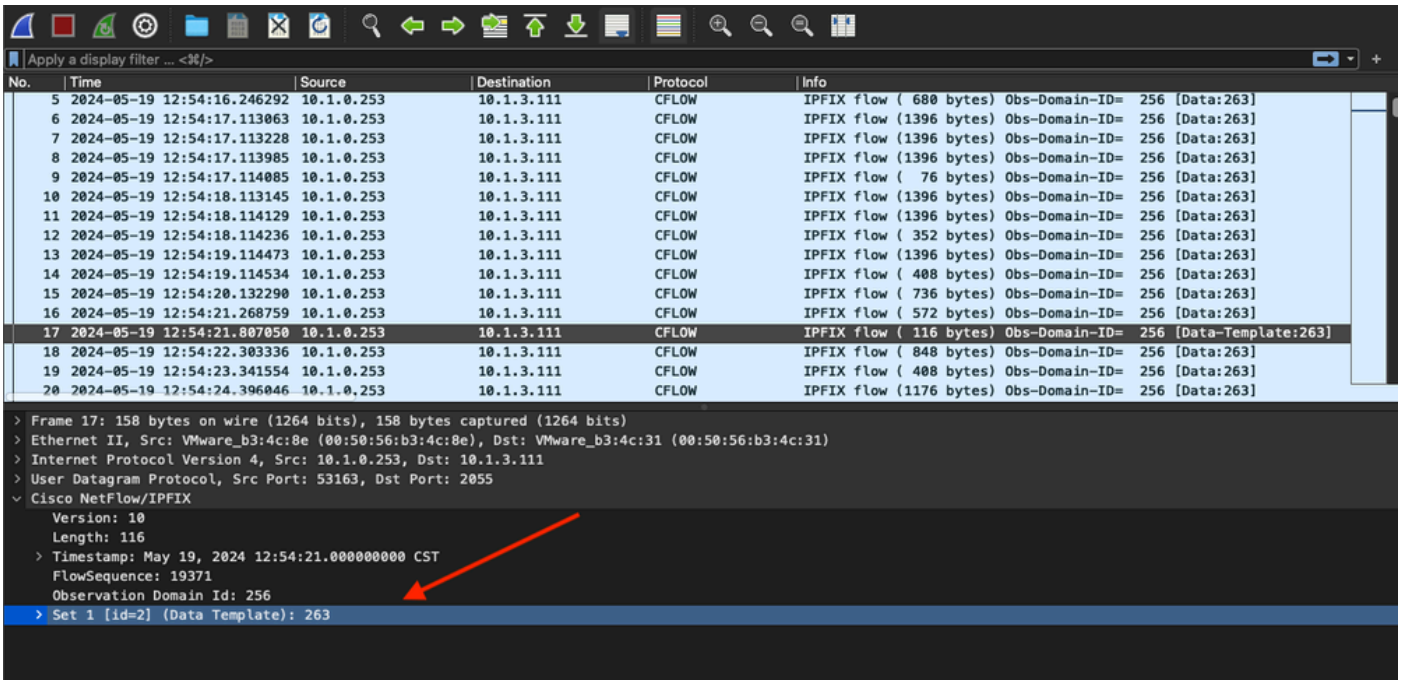
6.왼쪽 패널에서 Support > Browse Files로 이동합니다

7. 다음 폴더로 이동합니다. tcpdump

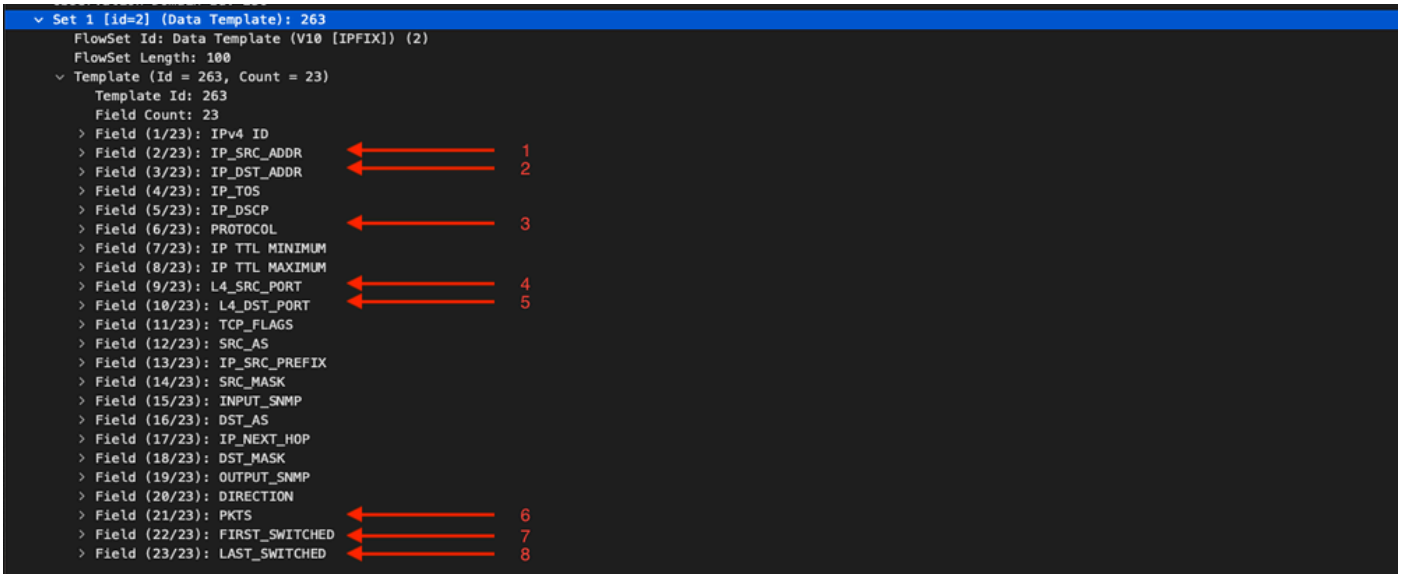
8. 패킷 캡처 파일을 클릭하여 로컬 시스템에 다운로드하고 Wireshark에서 엽니다.

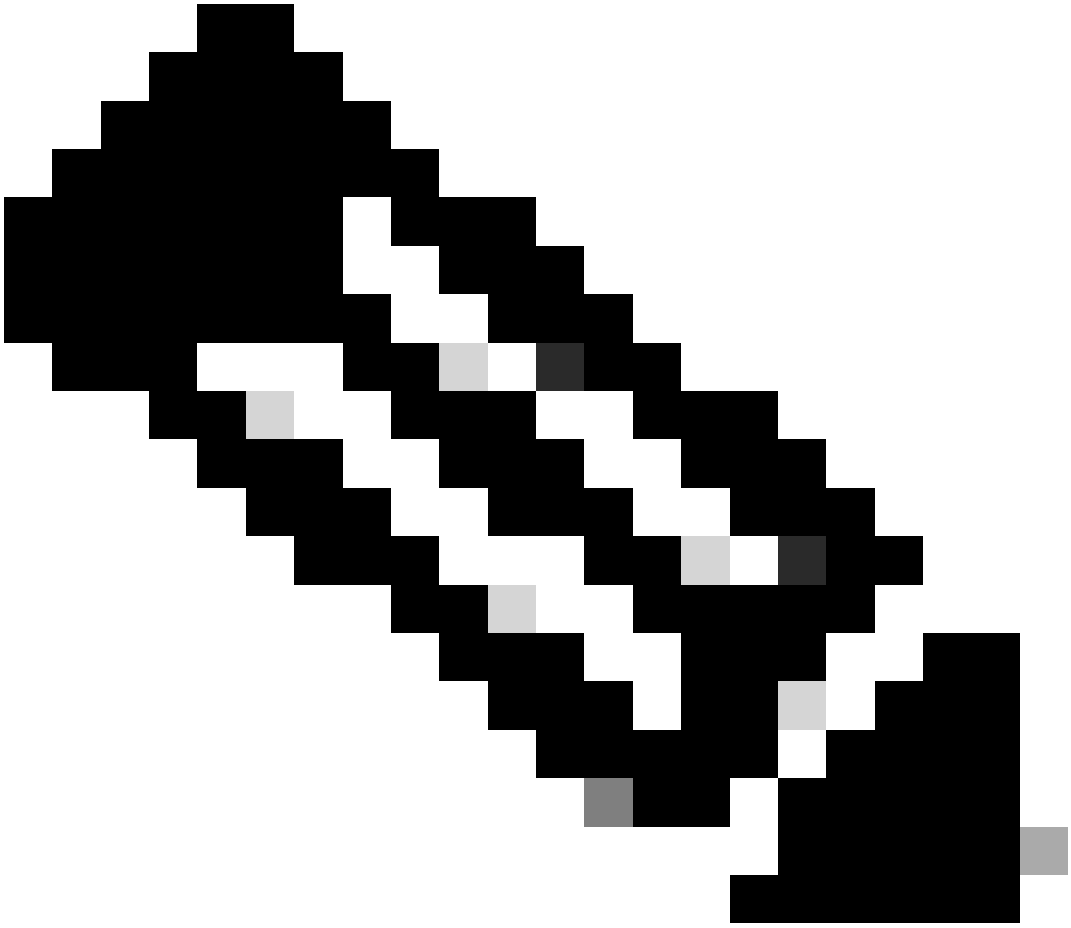


9 . NetFlow/IPFIX 템플릿이 수신된 프레임을 식별합니다.



10. 9개의 필수 필드가 템플리트에 표시되는지 검증합니다





참고: 템플릿에는 SNA에서 텔레메트리 수집에 필요한 필수 필드 9개 중 8개만 있습니다. 이 시나리오에서는 BYTES 필드가 없습니다.

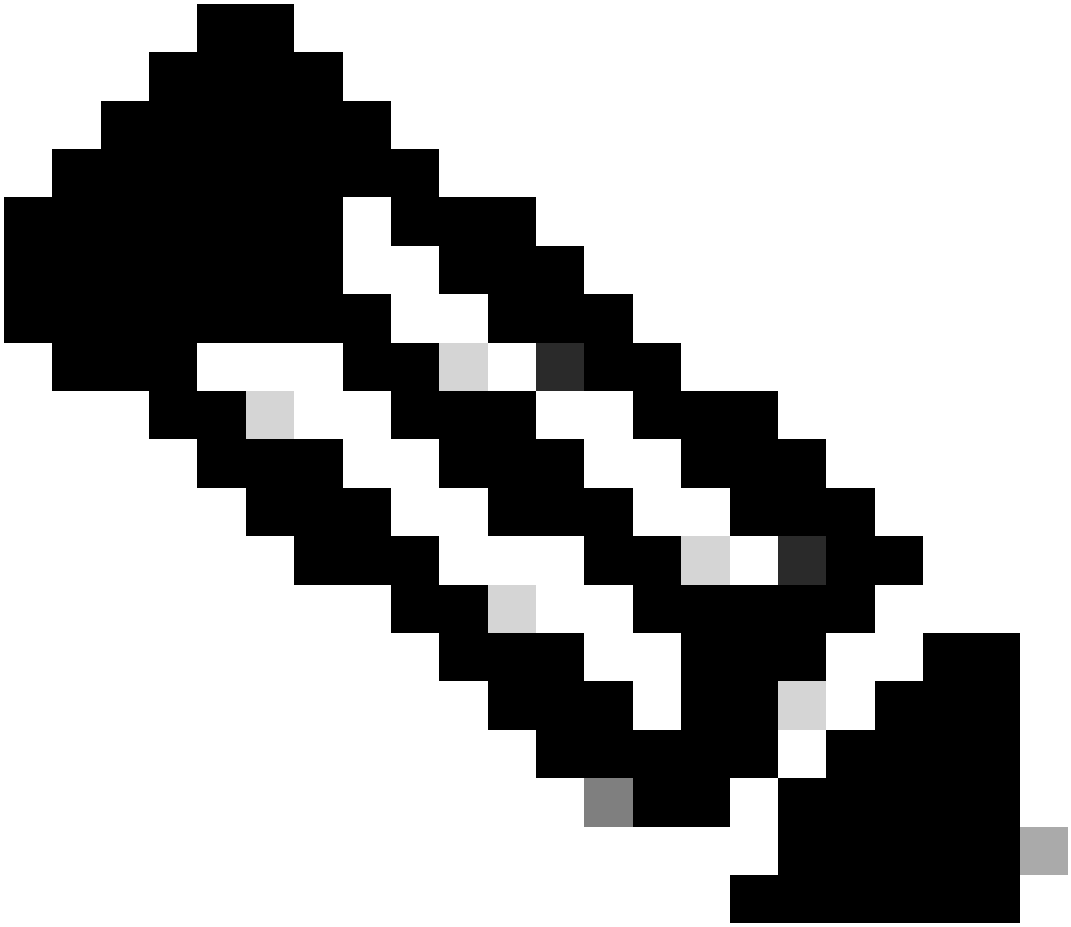
누락된 필드를 추가한 후 NetFlow/IPFIX 텔레메트리 수집 확인

변경 후 SNA Flow Collector가 NetFlow/IPFIX 텔레메트리를 내보내기에서 수신하여 삽입하는지 확인하려면 다음을 수행합니다.

1. 관리자 자격 증명으로 SNA Flow Collector Admin UI에 로그인합니다. https://<Flow Collector IP Address>/swa/login.html
2. 왼쪽 패널에서 Support(지원) > Browse Files(파일 찾아보기)로 이동합니다
3. 다음 폴더로 이동합니다. sw > 오늘 > 로그
4. sw.log 파일을 클릭하여 로컬 시스템에 다운로드하고 텍스트 편집기에서 엽니다.
5. 로그 하단에서 이러한 행을 검색합니다.

```
19:20:00 I-sch-t: process_5_min_period: begin
```

```
19:20:00 I-sch-t: process_5_min_period: periods(184)
19:20:00 S-per-t: Performance Period 184
19:20:00 S-per-t:     Engine status Status normal
19:20:00 S-per-t:     Processed 10992 flows at 37 fps this period
19:20:00 S-per-t:     Processed 4176 biflows at 14 fps this period
19:20:00 S-per-t:     Dropped 0 flows this period
19:20:00 S-per-t:     Discarded 0 flows this period due to insufficient template data
19:20:00 S-per-t:     Processed 1896017 flows at 35 fps today
19:20:00 S-per-t:     Dropped 0 flows today
19:20:00 S-per-t:     Discarded 36041 flows today due to insufficient template data
19:20:00 S-per-t:     Process instance 0 processed 5575 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 0 processed 2195 biflows at 8 fps this period
19:20:00 S-per-t:     Process instance 1 processed 5417 flows at 19 fps this period
19:20:00 S-per-t:     Process instance 1 processed 1981 biflows at 7 fps this period
19:20:00 S-per-t:     Inserted 2878 flow stats at 10 fps this period
19:20:00 S-per-t:     Inserted 4510 interface stats at 16 fps this period
19:20:00 S-per-t:     Inserted 486734 flow stats at 9 fps today
19:20:00 S-per-t:     Inserted 696260 interface stats at 13 fps today
```



참고: 행 8은 마지막 기간에 삭제된 흐름이 없음을 나타냅니다.

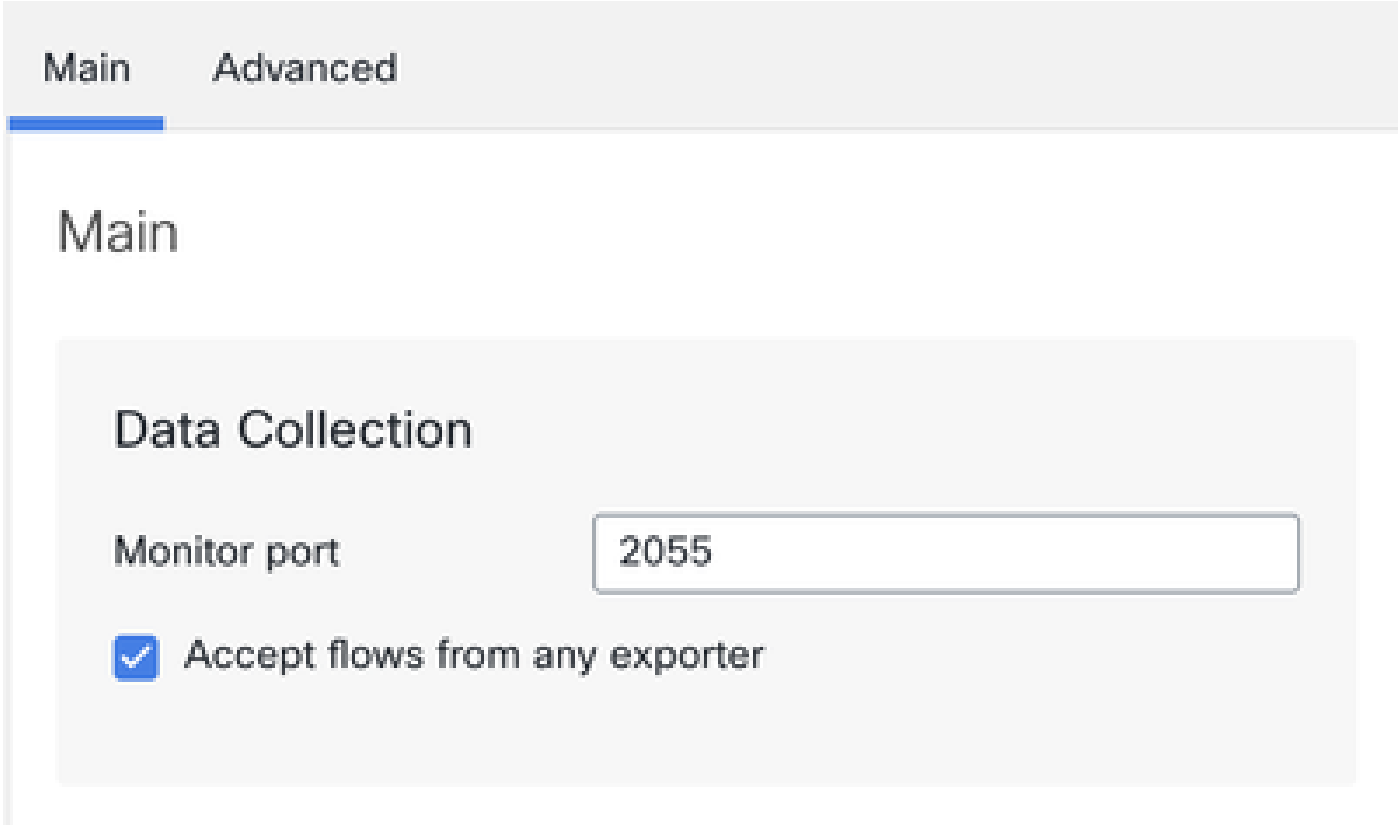
NetFlow/IPFIX 텔레메트리 수집 포트 확인

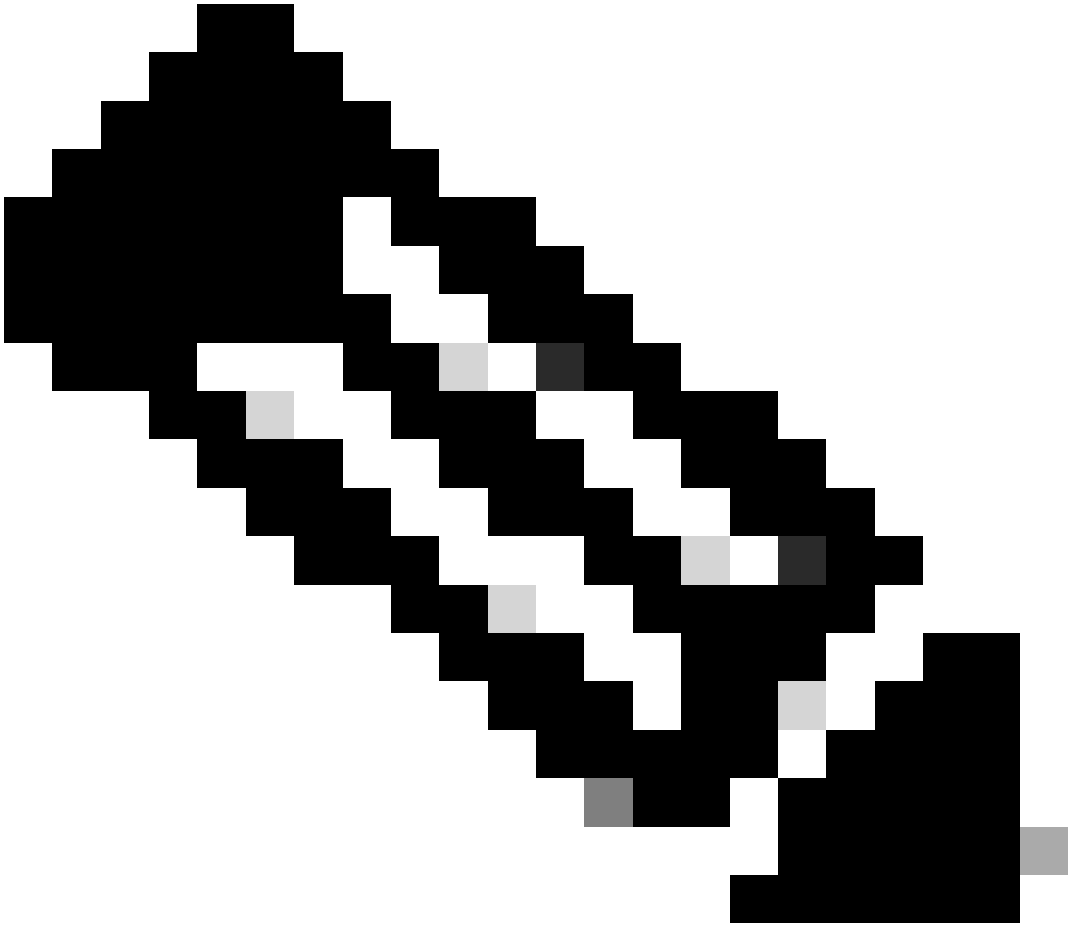
SNA Flow Collector가 올바른 포트의 Exporter로부터 NetFlow/IPFIX 텔레메트리를 수신하는지 확인하려면 다음을 수행합니다.

1. 관리자 권한이 있는 사용자로 SNA 웹 UI에 로그인합니다.

2. 상단 메뉴에서 Configure(구성)로 이동하여 Flow Collectors(Flow Collectors)를 선택합니다

3. SNA Flow Collector에서 NetFlow/IPFIX를 전송하도록 내보내기가 구성한 포트를 사용하는지 확인합니다





참고: NetFlow의 기본 포트는 2055이지만 다른 포트를 선택할 수 있습니다. Flow Collector에서 처음 설정하는 동안 동일한 포트를 사용해야 합니다.

NetFlow/IPFIX Telemetry Ingest NetFlow 옵션이 활성화되었는지 확인

NetFlow/IPFIX의 텔레메트리 수집에 대한 SNA Flow Collector 옵션이 활성화되었는지 확인하려면 다음을 수행합니다.

1. 관리자 자격 증명으로 SNA Flow Collector Admin UI에 로그인합니다. https://<Flow Collector IP Address>/swa/login.html
2. 왼쪽 패널에서 Support(지원) > Advanced Settings(고급 설정)로 이동합니다
3. enable_netflow 옵션이 1로 설정되어 있는지 확인합니다.

관련 정보

- 추가 지원이 필요한 경우 TAC(Technical Assistance Center)에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco Worldwide Support 연락처
- 여기서 Cisco Security Analytics Community를 방문할 수도 있습니다.
- 기술 지원 및 문서 – Cisco Systems

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.