SNA에서 텔레메트리 수집을 위한 NetFlow/IPFIX 구성

목차

소개

이 문서에서는 SNA(Secure Network Analytics)에서 텔레메트리 수집에 필요한 Netflow/IPFIX의 모범 사례 및 기본 컨피그레이션에 대해 설명합니다.

사전 요구 사항

- Cisco SNA 지식
- NetFlow/IPFIX 지식

요구 사항

- 7.2.1 이상의 보안 네트워크 분석
- 7.2.1 이상의 Flow Collector
- 플로우 컬렉터에 대한 루트로 CLI 액세스

사용되는 구성 요소

- 이는 네트워크 설계 및 NetFlow/IPFIX를 Secure Network Analytics에 전송하도록 선택한 디바이스에 따라 완전히 달라집니다. NetFlow/IPFIX 컨피그레이션은 각 익스포터에 따라 다릅니다. 자세한 컨피그레이션은 각 익스포터의 지원 팀에 문의하십시오.

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

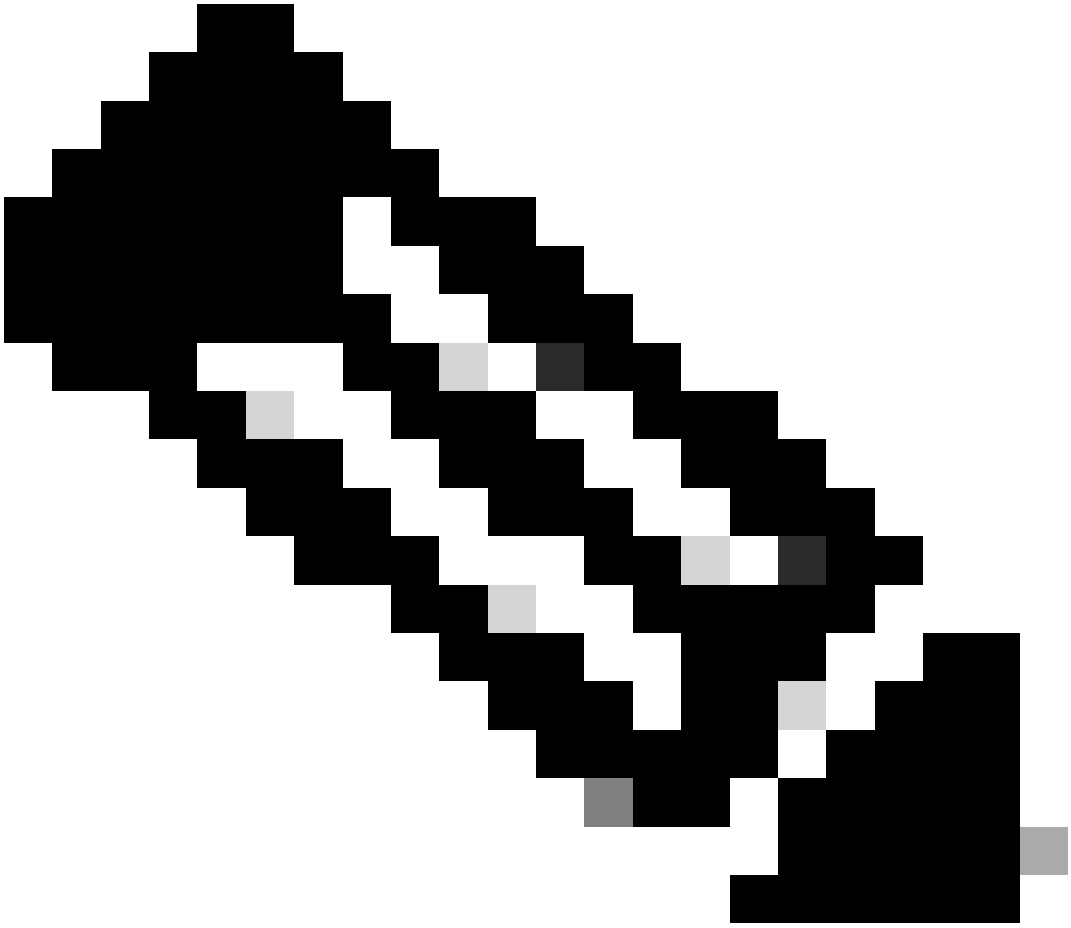
Flow Collector는 Secure Network Analytics로 전송되는 플로우를 수집, 처리 및 저장하는 SNA 어플라이언스입니다. NetFlow 버전 9 또는 IPFIX의 경우 네트워크 트래픽과 관련된 추가 정보를 추가하기 위해 NetFlow/IPFIX 템플릿에 여러 필드를 포함할 수 있지만, 플로우 컬렉터가 이러한 플로우를 처리하기 위해 NetFlow/IPFIX 템플릿에 포함해야 하는 9개의 특정 필드가 있습니다. Flow Collector는 유효하지 않은 템플릿을 포함하는 수신 플로우를 처리하지 않으므로, SNA는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

구성

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 텔레메트리 수집을 위한 Secure Network Analytics의 최소 요구 사항입니다.

권장 필드

인터페이스 정보에 대한 정보를 수집하려면 NetFlow/IPFIX 템플릿에 다음 필드를 포함하는 것이 좋습니다. 이 컨피그레이션은 이름 및 속도와 같은 인터페이스 정보를 표시하는 데 필요합니다.

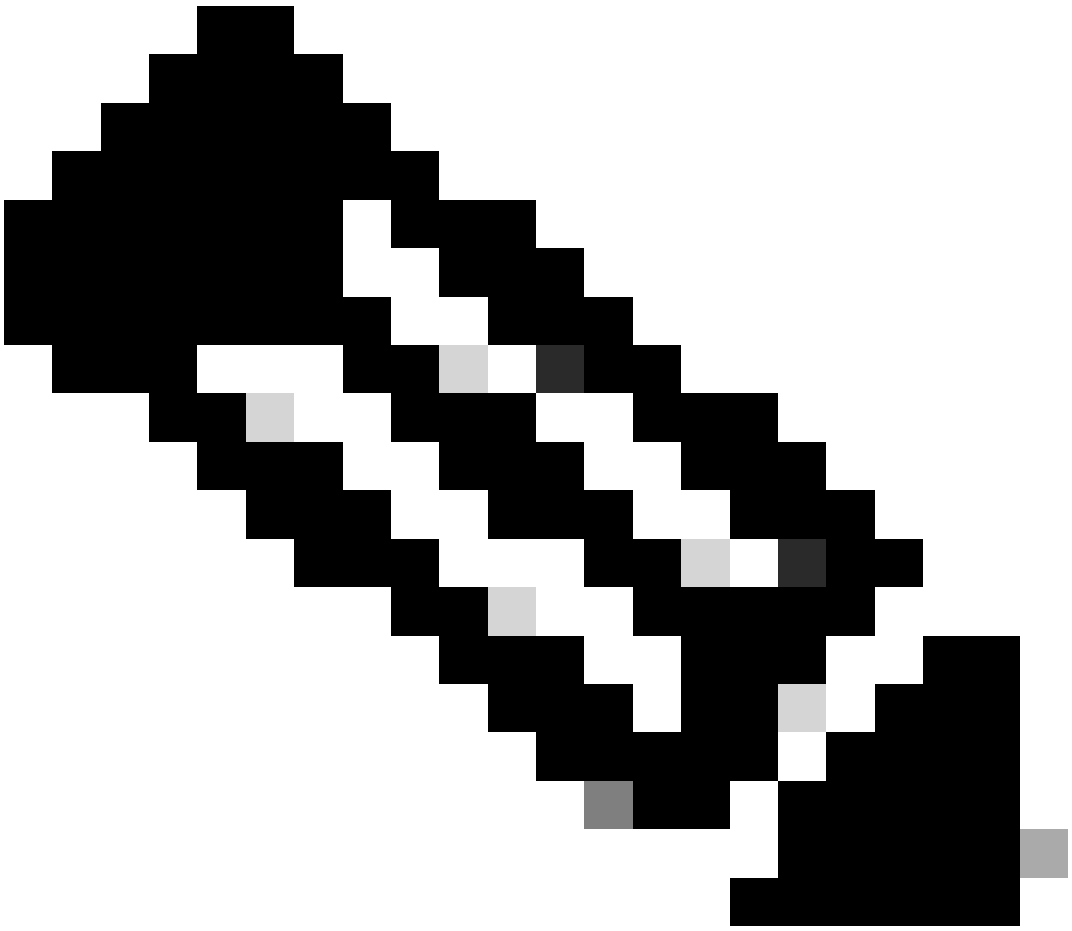
- 인터페이스 입력
- 인터페이스 출력

모범 사례

또한 Secure Network Analytics의 적절한 성능을 보장하기 위해 다음 설정이 모범 사례로 권장됩니다.

- 활성 시간 제한을 60초로 설정
- 비활성 시간 제한을 15초로 설정

- 템플릿 시간 제한을 30초로 설정



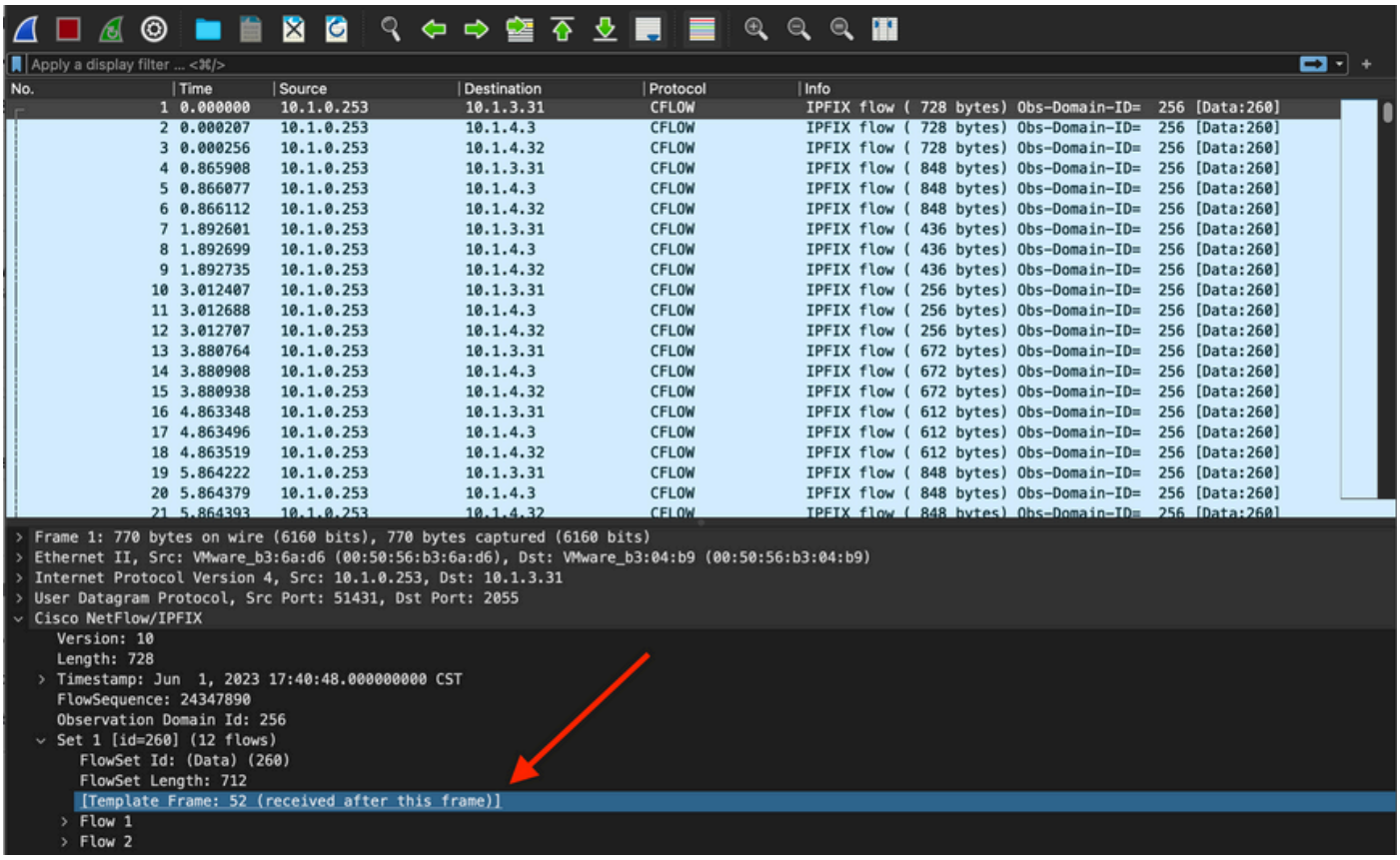
참고: NetFlow의 기본 포트는 2055이지만 다른 포트를 선택할 수 있습니다. 플로우 컬렉터에서 lc-ast 프로세스 중에 동일한 포트를 사용해야 합니다.

다음을 확인합니다.

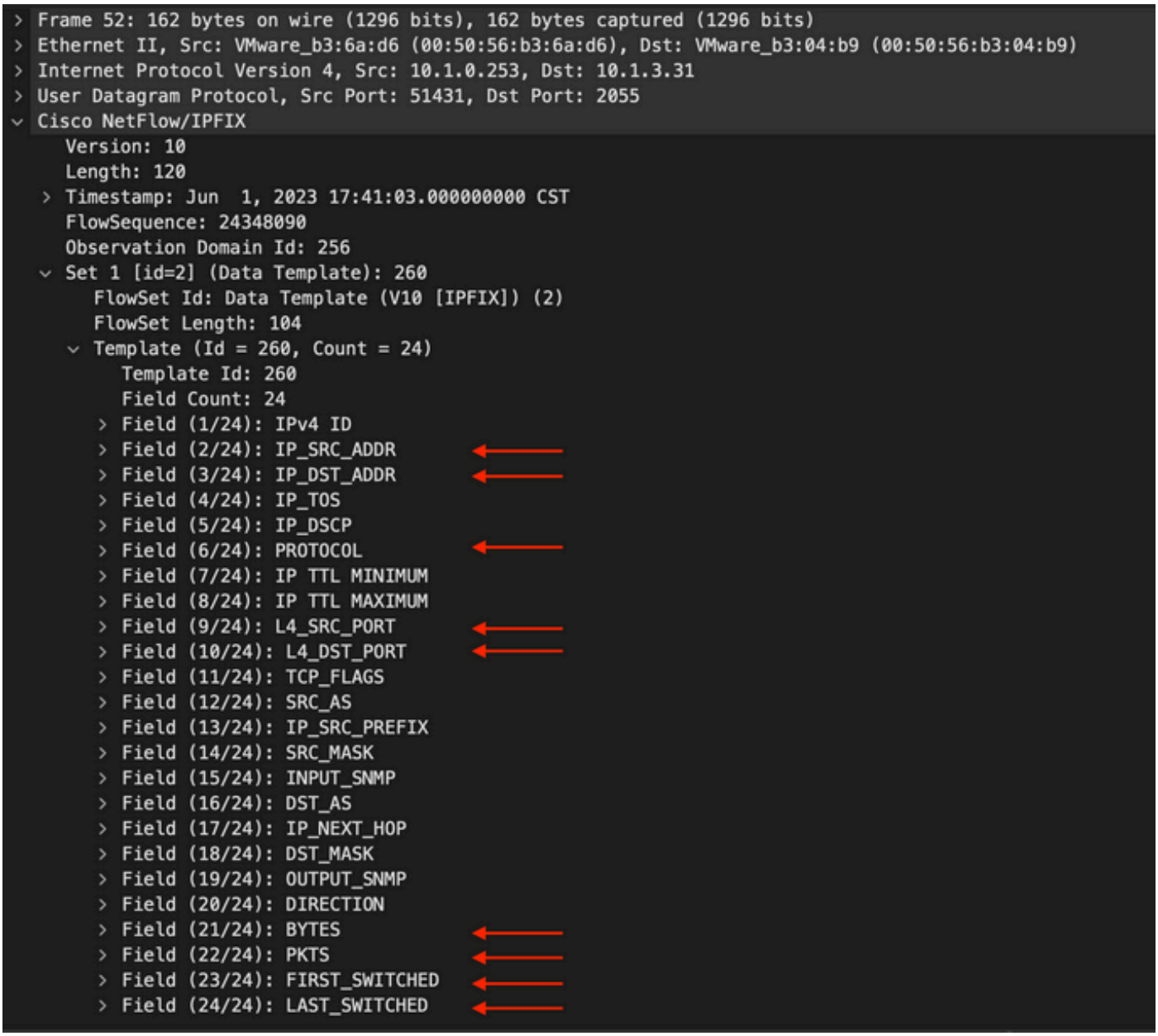
NetFlow/IPFIX 템플릿 컨피그레이션을 검증하기 위해 내보내기와 플로우 컬렉터 간에 패킷 캡처를 실행할 수 있습니다. SSH를 통해 루트 사용자로 Flow Collector에 로그인하고 다음 명령을 실행합니다.

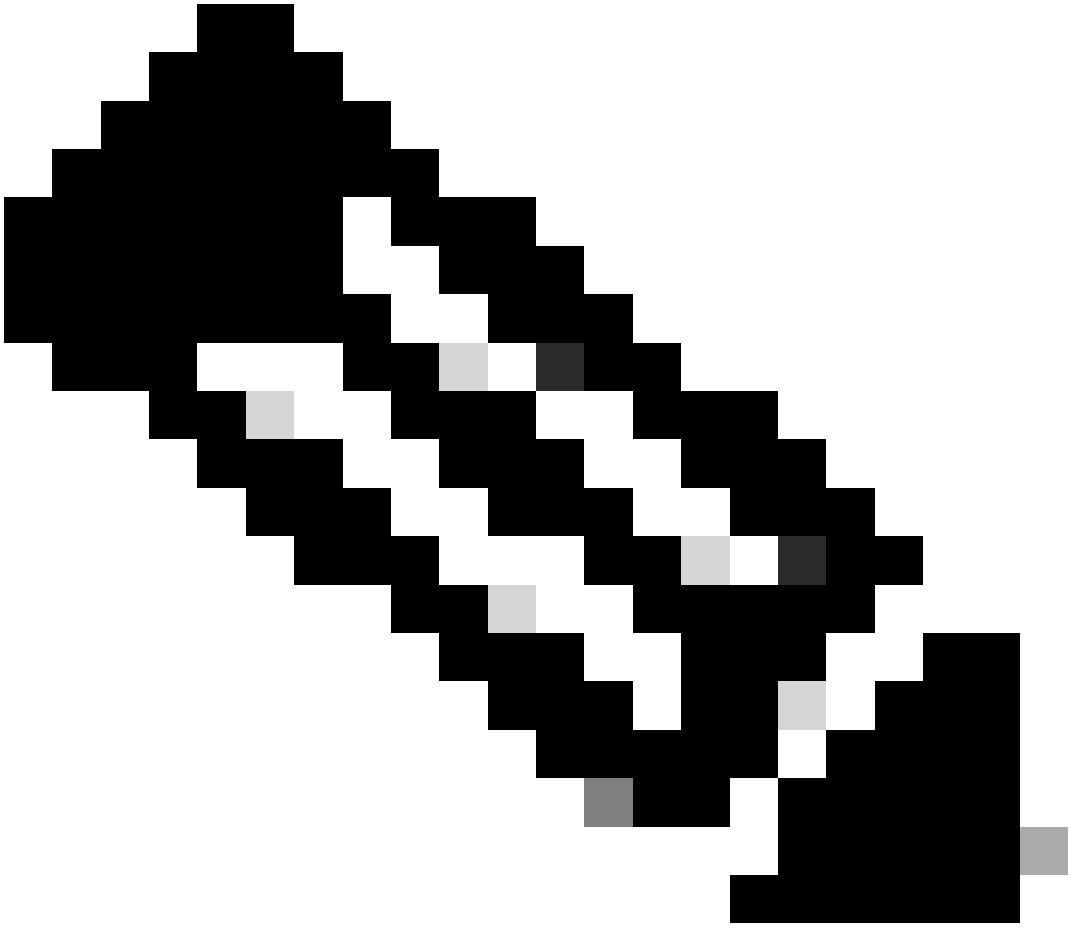
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- SCP 툴을 사용하여 Flow Collector(/lancope/var/tcpdump에 위치)에서 패킷 캡처를 로컬 시스템으로 내보낸 다음 Wireshark에서 엽니다



- NetFlow/IPFIX 템플릿이 수신된 프레임을 식별하고 열어 템플릿에 포함된 필드를 검증합니다


Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
User Datagram Protocol, Src Port: 51431, Dst Port: 2055
Cisco NetFlow/IPFIX
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 CST
FlowSequence: 24348090
Observation Domain Id: 256
Set 1 [id=2] (Data Template): 260
FlowSet Id: Data Template (V10 [IPFIX]) (2)
FlowSet Length: 104
Template (Id = 260, Count = 24)
Template Id: 260
Field Count: 24
Field (1/24): IPv4 ID
Field (2/24): IP_SRC_ADDR
Field (3/24): IP_DST_ADDR
Field (4/24): IP_TOS
Field (5/24): IP_DSCP
Field (6/24): PROTOCOL
Field (7/24): IP TTL MINIMUM
Field (8/24): IP TTL MAXIMUM
Field (9/24): L4_SRC_PORT
Field (10/24): L4_DST_PORT
Field (11/24): TCP_FLAGS
Field (12/24): SRC_AS
Field (13/24): IP_SRC_PREFIX
Field (14/24): SRC_MASK
Field (15/24): INPUT_SNMP
Field (16/24): DST_AS
Field (17/24): IP_NEXT_HOP
Field (18/24): DST_MASK
Field (19/24): OUTPUT_SNMP
Field (20/24): DIRECTION
Field (21/24): BYTES
Field (22/24): PKTS
Field (23/24): FIRST_SWITCHED
Field (24/24): LAST_SWITCHED



참고: 표시된 필드 이름은 내보내기마다 다를 수 있습니다. 이는 해당 필드를 검증하는 방법에 대한 참조일 뿐입니다.

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.