Configureer NetFlow/IPFIX voor telemetrie-ingest op SNA

Inhoud

Inleiding

In dit document worden de best practices en de basisconfiguratie beschreven van NetFlow/IPFIX die Secure Network Analytics (SNA) nodig heeft voor telemetrische invoer.

Voorwaarden

- Cisco SNA-kennis
- Kennis van NetFlow/IPFIX

Vereisten

- Secure Network Analytics in 7.2.1 of nieuwer
- Flow Collector in 7.2.1 of nieuwer
- CLI-toegang als root voor de Flow Collector

Gebruikte componenten

- Dit hangt volledig af van uw netwerkontwerp en de apparaten die u hebt geselecteerd om NetFlow/IPFIX naar Secure Network Analytics te verzenden. NetFlow/IPFIX configuratie is verschillend op elke exporteur, voor gedetailleerde configuratie gelieve het ondersteuningsteam van elke exporteur te contacteren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële

impact van elke opdracht begrijpt.

Achtergrondinformatie

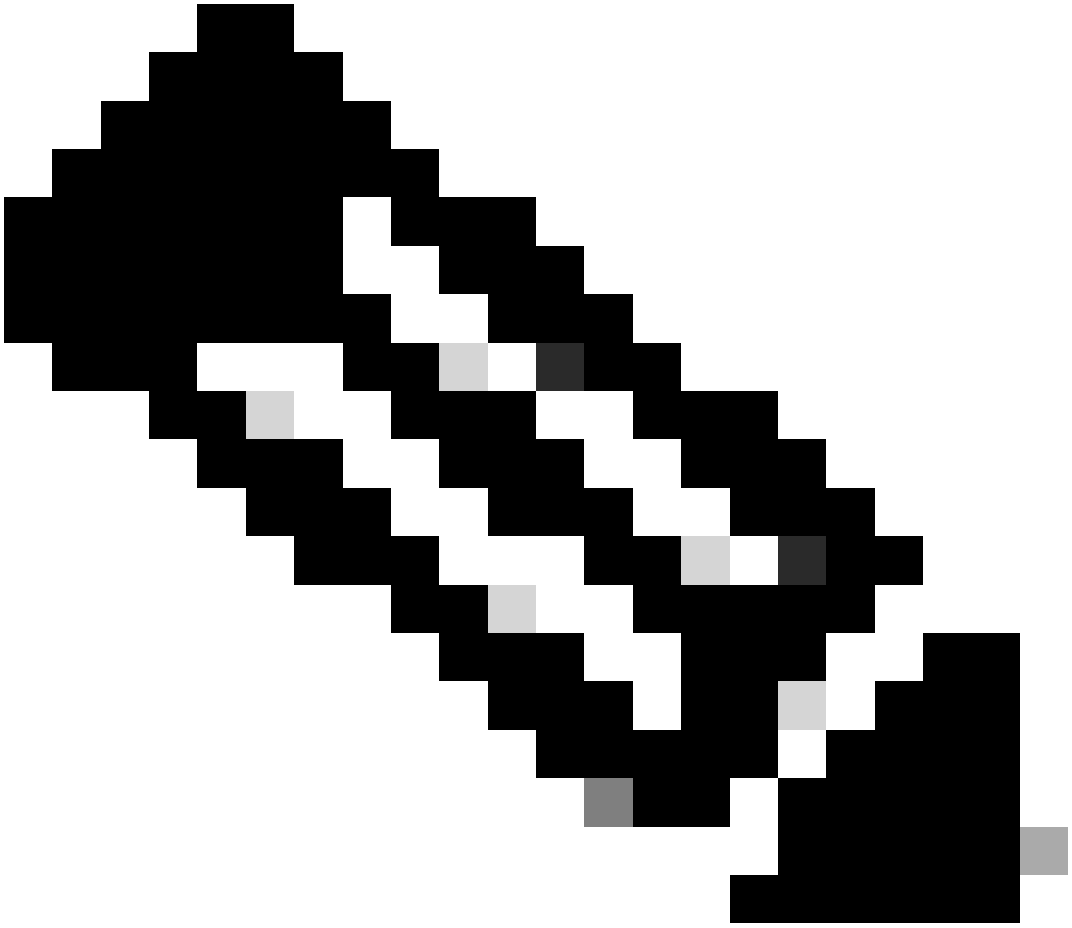
De Flow Collector is een SNA-apparaat dat verantwoordelijk is voor het verzamelen, verwerken en opslaan van stromen die naar Secure Network Analytics worden verzonden. Voor NetFlow versie 9 of IPFIX kunnen er verschillende velden worden opgenomen in NetFlow/IPFIX sjabloon om meer informatie toe te voegen met betrekking tot netwerkverkeer, maar er zijn 9 specifieke velden die moeten worden opgenomen in NetFlow/IPFIX sjabloon voor de Flow Collector om die stromen te verwerken. Flow Collector verwerkt geen inkomende stromen die een niet-geldige sjabloon omvatten, daarom geeft SNA geen stroominformatie weer van die exporteurs onder Web UI of Desktop Client.

Configureren

Verplichte velden

Volgende velden moeten worden opgenomen in NetFlow/IPFIX sjabloon voor telemetrie inname. Zorg ervoor dat deze 9 velden zijn opgenomen in NetFlow/IPFIX-sjabloon, zodat Secure Network Analytics inkomende stromen kan verwerken.

- IP-bronadres
- IP-adres van bestemming
- Bronpoort
- Doelpoort
- Layer 3-protocol
- aantal bytes
- PacketCount
- Stroombegintijd
- Flow End-tijd



Opmerking: er kunnen meer velden worden opgenomen in NetFlow/IPFIX-configuratie, maar de vorige velden zijn de minimumvereisten van Secure Network Analytics voor Telemetry Ingest.

Aanbevolen velden

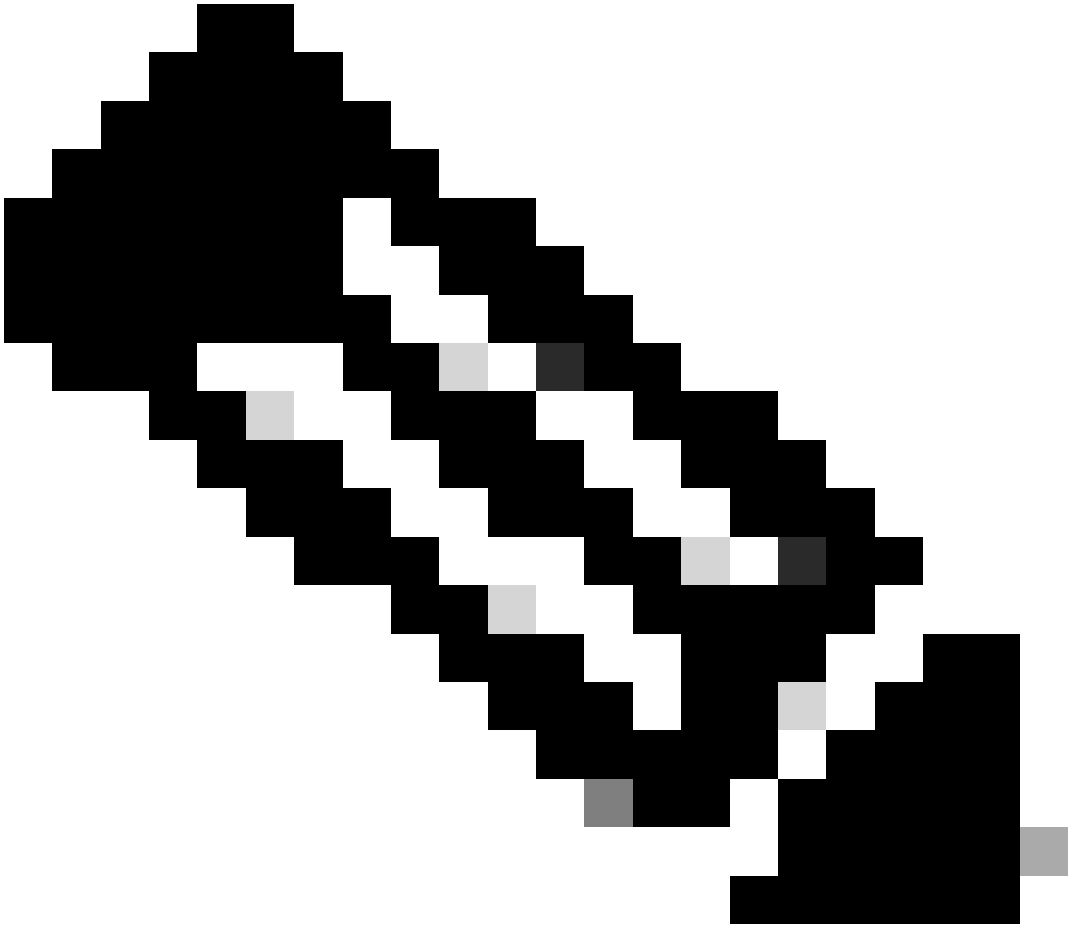
Het wordt aanbevolen de volgende velden op NetFlow/IPFIX-sjabloon op te nemen om informatie te verzamelen over interface-informatie. Deze configuratie is vereist om interface-informatie zoals naam en snelheid weer te geven:

- Interface-ingang
- Interface-uitgang

Best practices

Bovendien worden de volgende instellingen aanbevolen als best practices om een goede uitvoering van Secure Network Analytics te garanderen.

- Actieve timeout instellen op 60 seconden
- Inactieve timeout instellen op 15 seconden
- Time-out sjabloon instellen op 30 seconden



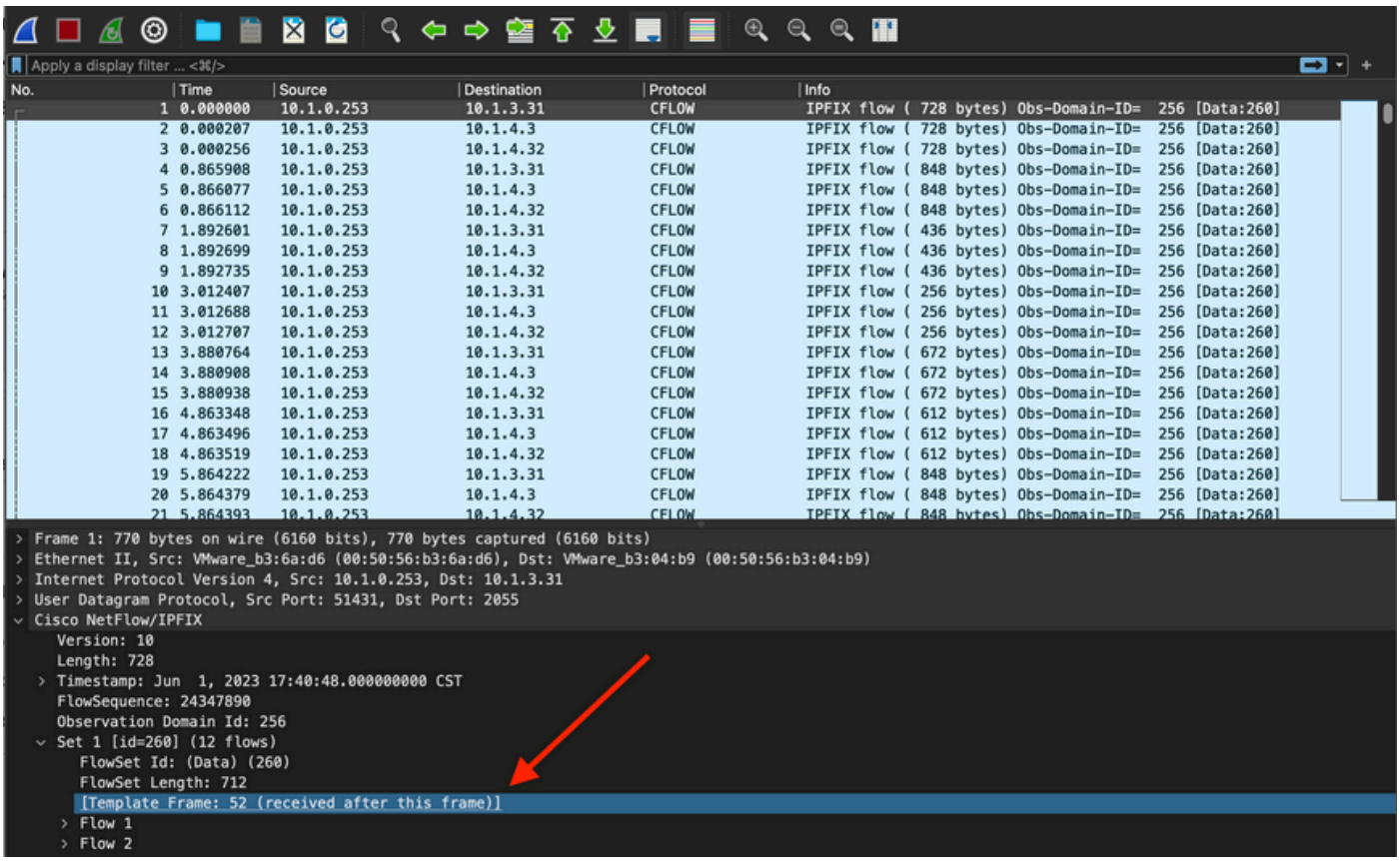
> Opmerking: de standaardpoort voor NetFlow is 2055. U kunt echter ook een andere poort selecteren. Zorg ervoor dat u dezelfde poort gebruikt tijdens het LC-astproces voor Flow Collector(s).

Verifiëren

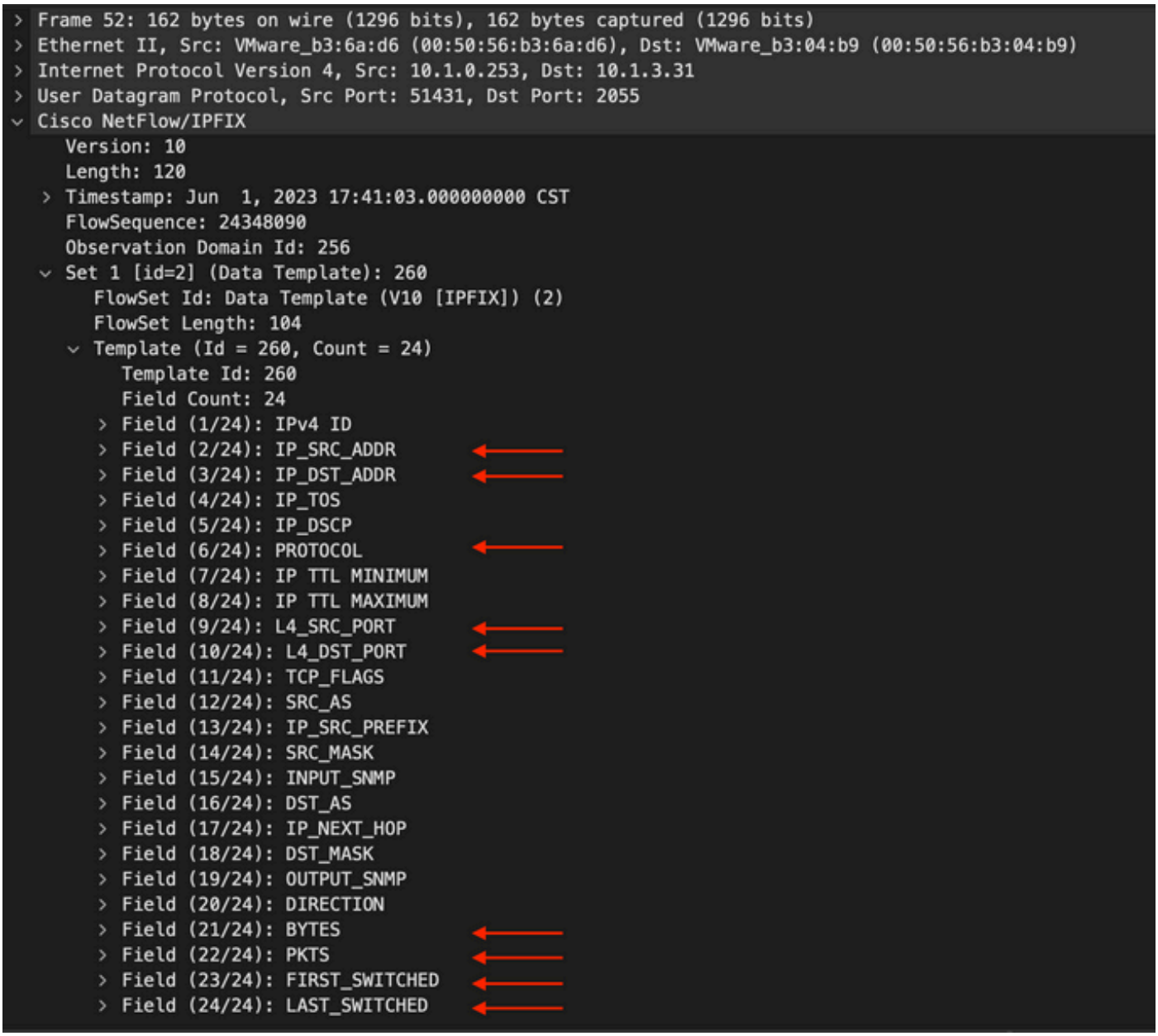
Om de configuratie van NetFlow/IPFIX-sjabloon te valideren, kunt u een pakketopname uitvoeren tussen de exporteur en Flow Collector. Log in de Flow Collector met root-gebruiker via SSH en voer de opdracht uit:

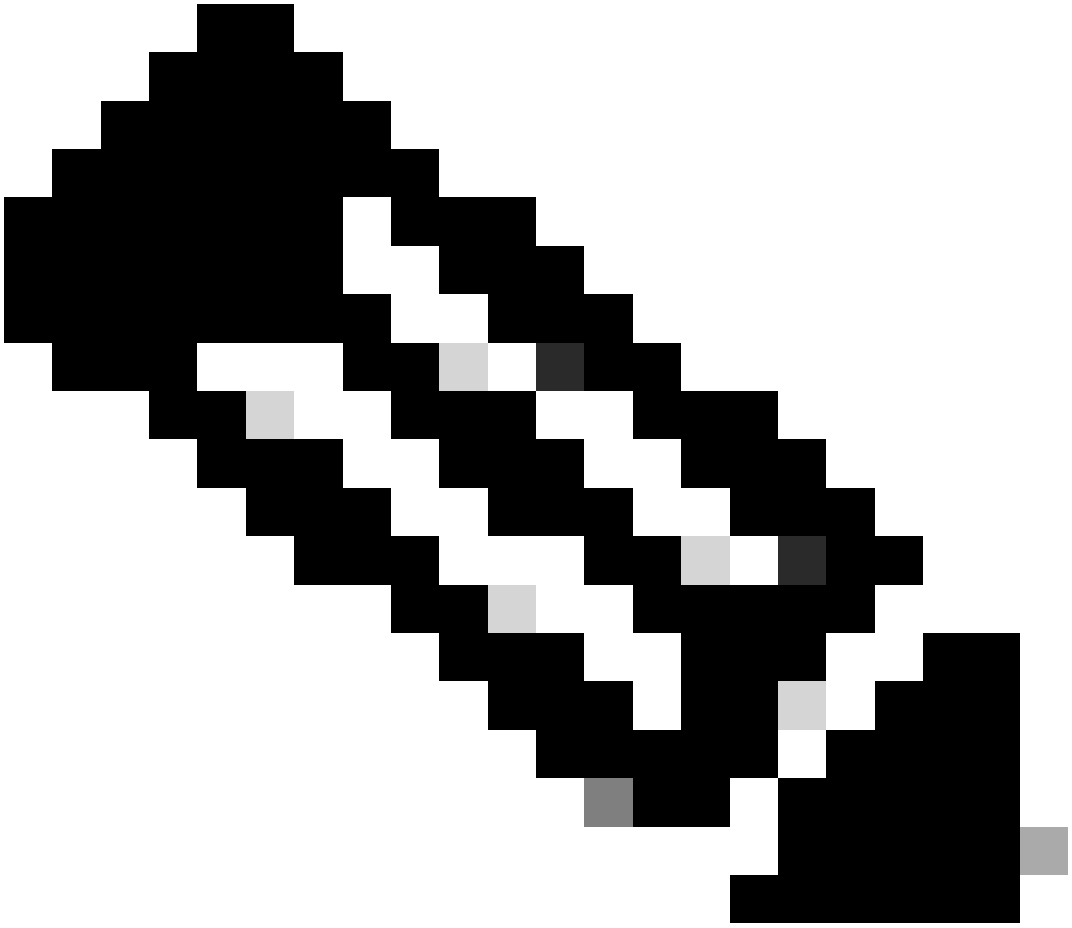
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- Gebruik een SCP-gereedschap om de pakketopname van de Flow Collector (bevindt zich in /lancope/var/tcpdump) naar uw lokale machine te exporteren en open deze vervolgens op Wireshark



- Identificeer het kader waarin het NetFlow/IPFIX-sjabloon is ontvangen en open het om de velden die het sjabloon bevat te valideren


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



Opmerking: de weergegeven veldnamen kunnen er per exporteur anders uitzien. Dit is slechts een verwijzing naar hoe u deze velden kunt valideren.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.