Configureer en controleer NetFlow, AVC en ETA op Catalyst 9000 Series Switches

Inhoud

Inleiding

Dit document beschrijft hoe u NetFlow, Application Visibility and Control (AVC) en Encrypted Traffic Analytics (ETA) moet configureren en valideren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- NetFlow
- AVC
- ETA

Gebruikte componenten

De informatie in dit document is gebaseerd op een Catalyst 9300 switch met Cisco IOS XE-software 16.12.4.

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.

Verwante producten

Dit document kan ook worden gebruikt voor de volgende hardware- en softwareversies:

- 9200
- 9400
- 9500
- 9600
- Cisco IOS XE 16.12 en hoger

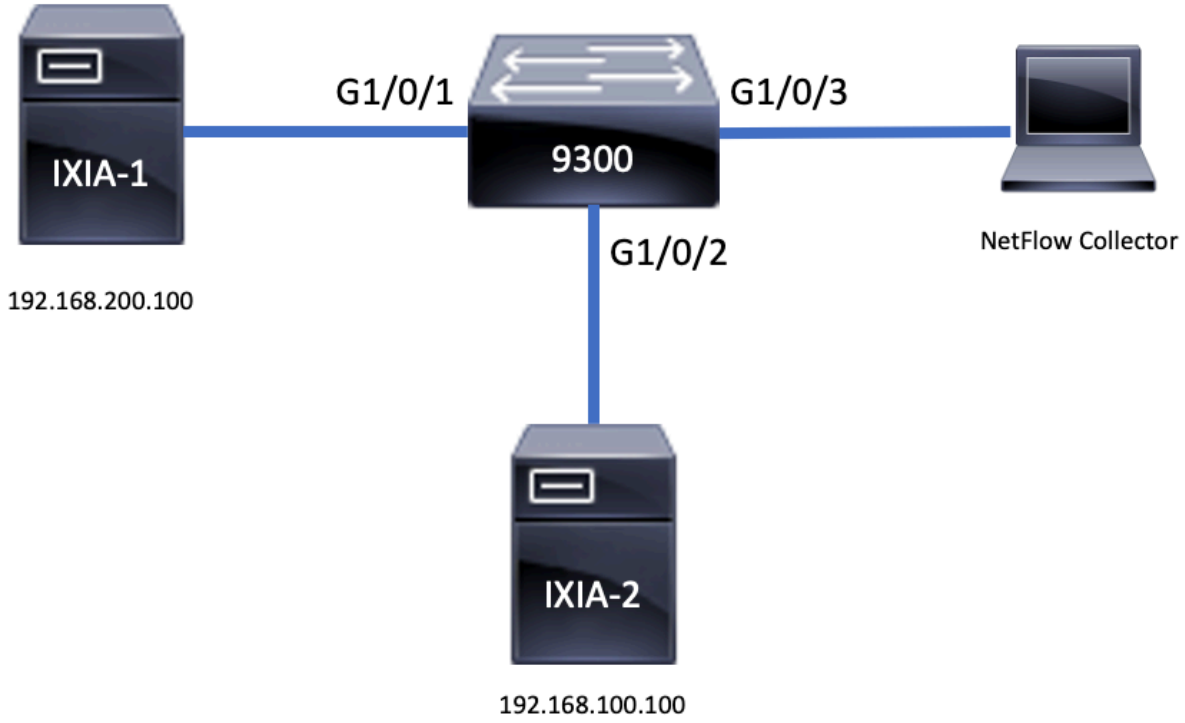
Achtergrondinformatie

- Flexible NetFlow is de next-generation in flow technologie die gegevens verzamelt en meet om alle switches in het netwerk een telemetriebron te laten worden.
- Flexibele NetFlow maakt extreem granulaire en nauwkeurige verkeersmetingen en hoogwaardige aggregatie van verkeer mogelijk.
- Flexibele NetFlow gebruikt stromen om statistieken te leveren voor accounting, netwerkbewaking en netwerkplanning.
- Een stroom is een unidirectionele stroom van pakketten die op een broninterface aankomt en dezelfde waarden heeft voor de toetsen. Een sleutel is een geïdentificeerde waarde voor een veld binnen het pakket. U maakt een flow via een flow record om de unieke toetsen voor uw flow te definiëren.

Opmerking: De opdrachten voor het platform (fed) kunnen verschillen. De opdracht kan zijn

"**show platform fed <active|standby>**" versus "**show platform fed switch <active|standby>**". Als de syntaxis die in de voorbeelden is genoteerd niet wordt geparseerd, probeer dan de variant.

Netwerkdiagram



Configureren

Componenten

De NetFlow-configuratie bestaat uit **drie hoofdcomponenten** die samen kunnen worden gebruikt, namelijk verschillende variaties om verkeersanalyse en gegevensexport uit te voeren.

Flow Record

- Een record is een combinatie van key- en nonkey-velden. Flexibele NetFlow-records worden toegewezen aan Flexibele NetFlow-monitoren om de cache te definiëren die wordt gebruikt voor de opslag van stroomgegevens.
- Flexibele NetFlow omvat verschillende vooraf gedefinieerde records die kunnen worden gebruikt om verkeer te bewaken.
- Flexibel NetFlow maakt het ook mogelijk om aangepaste records te definiëren voor een Flexible NetFlow-monitorcache door de specificatie van belangrijke en niet-sleutelvelden om de gegevensverzameling aan uw specifieke vereisten aan te passen.

Zoals in het voorbeeld, de configuratiedetails van het stroomverslag:

```
flow record TAC-RECORD-IN
match flow direction
match ipv4 source address
match interface input
match ipv4 destination address
match ipv4 protocol
collect counter packets long
collect counter bytes long
collect timestamp absolute last
collect transport tcp flags

flow record TAC-RECORD-OUT
match flow direction
match interface output
match ipv4 source address
match ipv4 destination address
match ipv4 protocol
collect counter packets long
collect counter bytes long
collect timestamp absolute last
collect transport tcp flags
```

Flow Exporteur

- Flow-exporteurs worden gebruikt om de gegevens in het Flow Monitor-cachegeheugen te exporteren naar een extern systeem (server die fungeert als NetFlow Collector), voor analyse en opslag.
- Flow-exporteurs worden toegewezen aan flow monitors om de data-export mogelijkheid voor de flow monitors te bieden.

Zoals in het voorbeeld, de configuratiedetails van de stroomexporteur:

```
flow exporter TAC-EXPORT
destination 192.168.69.2
source Vlan69
```

Flow Monitor

- Flow-monitoren zijn de Flexibele NetFlow-component die wordt toegepast op interfaces om netwerkverkeersbewaking uit te voeren.
- De gegevens van de stroom worden verzameld van het netwerkverkeer en aan het cachegeheugen van de stroommonitor toegevoegd terwijl het proces loopt. Het proces is gebaseerd op de belangrijkste en niet-belangrijkste velden in het stroomrecord.

Zoals in het voorbeeld, de configuratiedetails van de stroommonitor:

```
flow monitor TAC-MONITOR-IN
exporter TAC-EXPORT
record TAC-RECORD-IN

flow monitor TAC-MONITOR-OUT
exporter TAC-EXPORT
record TAC-RECORD-OUT

Switch#show run int g1/0/1
Building configuration...
```

```
Current configuration : 185 bytes
!
interface GigabitEthernet1/0/1
switchport access vlan 42
switchport mode access
ip flow monitor TAC-MONITOR-IN input
ip flow monitor TAC-MONITOR-OUT output
load-interval 30
end
```

Flow Sampler (optioneel)

- Flow samplers worden gecreëerd als afzonderlijke componenten in de configuratie van een router.
- Flow samplers beperken het aantal pakketten die worden geselecteerd voor analyse om de belasting op het apparaat dat Flexible NetFlow gebruikt te verminderen.
- Flow samplers worden gebruikt om de belasting op het apparaat dat Flexibele NetFlow gebruikt te verminderen die wordt bereikt door de limiet van het aantal pakketten dat voor analyse wordt geselecteerd.
- Flow samplers wisselen nauwkeurigheid uit voor routerprestaties. Als het aantal pakketten dat door de flowmonitor wordt geanalyseerd afneemt, kan de nauwkeurigheid van de informatie die in de cache van de flowmonitor is opgeslagen, worden beïnvloed.

Zoals in het voorbeeld, de configuratie van de voorbeeldstroom bemonsteraar:

```
sampler SAMPLE-TAC
description Sample at 50%
mode random 1 out-of 2

Switch(config)#interface GigabitEthernet1/0/1
Switch(config-if)#ip flow monitor TAC-MONITOR-IN sampler SAMPLE-TAC input
Switch(config-if)#end
```

Beperkingen

- DNA Addon-licentie is vereist voor volledige Flexible NetFlow, anders is Sampled NetFlow alleen beschikbaar.
- Flow-exporteurs kunnen de beheerpoort niet als bron gebruiken.

Dit is geen inclusieve lijst, raadpleeg de configuratiehandleiding voor het juiste platform en de juiste code.

Verifiëren

Platform onafhankelijke verificatie

Controleer de configuratie en bevestig dat de vereiste NetFlow-componenten aanwezig zijn:

1. **Flow Record**
2. **Flow Exporteur**
3. **Flow Monitor**
4. **Flow Sampler (optioneel)**

Tip: Om de flow record, flow exporteur, en flow monitor output in één opdracht te bekijken,

voer "**show in werking stellen-config flow monitor <flow monitor name> uit**"

Zoals in het voorbeeld wordt getoond, is de stroommonitor verbonden met de invoerrichting en de bijbehorende onderdelen:

```
Switch#show running-config flow monitor TAC-MONITOR-IN expand
Current configuration:
!
flow record TAC-RECORD-IN
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match interface input
 match flow direction
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute last
!
flow exporter TAC-EXPORT
 destination 192.168.69.2
 source Vlan69
!
flow monitor TAC-MONITOR-IN
 exporter TAC-EXPORT
 record TAC-RECORD-IN
!
```

Zoals in het voorbeeld wordt getoond, is de stroommonitor verbonden met de uitvoerrichting en de bijbehorende onderdelen:

```
Switch#show run flow monitor TAC-MONITOR-OUT expand
Current configuration:
!
flow record TAC-RECORD-OUT
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match interface output
 match flow direction
 collect transport tcp flags
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute last
!
flow exporter TAC-EXPORT
 destination 192.168.69.2
 source Vlan69
!
flow monitor TAC-MONITOR-OUT
 exporter TAC-EXPORT
 record TAC-RECORD-OUT
!
```

Voer de opdracht "**show flow monitor <flow monitor name>"-statistieken uit.** Deze output is nuttig om te bevestigen dat de gegevens worden geregistreerd:

```
Switch#show flow monitor TAC-MONITOR-IN statistics
  Cache type:                               Normal (Platform cache)
```

```
  Cache size:                             10000
  Current entries:                            1

  Flows added:                                1
  Flows aged:                                 0
```

Voer de opdracht **"show flow monitor <flow monitor name> cache uit** om te bevestigen dat het NetFlow cache output heeft:

```
Switch#show flow monitor TAC-MONITOR-IN cache
  Cache type:                           Normal (Platform cache)
  Cache size:                            10000
  Current entries:                            1

  Flows added:                                1
  Flows aged:                                 0

IPV4 SOURCE ADDRESS:       192.168.200.100
IPV4 DESTINATION ADDRESS:  192.168.100.100
INTERFACE INPUT:           Gi1/0/1
FLOW DIRECTION:            Input
IP PROTOCOL:               17
tcp flags:                 0x00
counter bytes long:        4606617470
counter packets long:      25311085
timestamp abs last:        22:44:48.579
```

Voer de opdracht **"toon flow exporteur <naam exporteur> statistieken"** om te bevestigen dat de exporteur pakketten verstuurde:

```
Switch#show flow exporter TAC-EXPORT statistics
Flow Exporter TAC-EXPORT:
  Packet send statistics (last cleared 00:08:38 ago):
    Successfully sent:         2                     (24 bytes)

  Client send statistics:
    Client: Flow Monitor TAC-MONITOR-IN
      Records added:           0
      Bytes added:             12
        - sent:                12

    Client: Flow Monitor TAC-MONITOR-OUT
      Records added:           0
      Bytes added:             12
        - sent:                12
```

Platform-afhankelijke verificatie

NetFlow Initialization - NFL partitietabel

- NetFlow-partities worden geïnitialiseerd voor verschillende functies met 16 partities per richting (Invoer vs Output).
- De configuratie van de NetFlow-verdelingstabel is verdeeld in de globale bankallocatie, die verder wordt onderverdeeld in de inkomende en uitgaande-stroombanken.

Belangrijke velden

- Aantal scheidingswanden

- Partitie inschakelen status
- Partitielimiet
- Huidig partitiegebruik

Om de NetFlow Partition Table te bekijken, kunt u de opdracht "**show platform software fed switch active|standby|member| fnf sw-table-size asic <asic number> schaduw 0"** uitvoeren

> **Opmerking:** Stromen die worden gecreëerd zijn specifiek voor de switch en basiskern wanneer ze worden gecreëerd. Het nummer van de switch (actief, stand-by, enzovoort) moet duidelijk worden aangegeven. Het ASIC-nummer dat wordt ingevoerd, is gekoppeld aan de respectieve interface. Gebruik "**show platform software fed switch active|standby|member information mappings"** om ASIC te bepalen die aan de interface beantwoordt. Gebruik voor de schaduwoptie altijd "0".

```
Switch#show platform software fed switch active fnf sw-table-sizes asic 0 shadow 0

---------------------------------
     Global Bank Allocation
---------------------------------
Ingress Banks : Bank 0 Bank 1
Egress Banks  : Bank 2 Bank 3
---------------------------------
    Global flow table Info                                  <--- Provides the number of entries
used per direction
INGRESS    usedBankEntry           0  usedOvfTcamEntry     0
 EGRESS    usedBankEntry           0  usedOvfTcamEntry     0
---------------------------------
    Flows Statistics
INGRESS    TotalSeen=0 MaxEntries=0 MaxOverflow=0
EGRESS     TotalSeen=0 MaxEntries=0 MaxOverflow=0

---------------------------------
       Partition Table
---------------------------------
## Dir  Limit  CurrFlowCount  OverFlowCount  MonitoringEnabled
 0 ING      0              0              0                 0
 1 ING  16640              0              0                 1          <-- Current flow count in hardware
 2 ING      0              0              0                 0
 3 ING  16640              0              0                 0
 4 ING      0              0              0                 0
 5 ING   8192              0              0                 1
 6 ING      0              0              0                 0
 7 ING      0              0              0                 0
 8 ING      0              0              0                 0
 9 ING      0              0              0                 0
10 ING      0              0              0                 0
11 ING      0              0              0                 0
12 ING      0              0              0                 0
13 ING      0              0              0                 0
14 ING      0              0              0                 0
15 ING      0              0              0                 0
 0 EGR      0              0              0                 0
 1 EGR  16640              0              0                 1          <-- Current flow count in hardware
 2 EGR      0              0              0                 0
 3 EGR  16640              0              0                 0
 4 EGR      0              0              0                 0
 5 EGR   8192              0              0                 1
 6 EGR      0              0              0                 0
```

```
 7 EGR       0           0                0           0
 8 EGR       0           0                0           0
 9 EGR       0           0                0           0
10 EGR       0           0                0           0
11 EGR       0           0                0           0
12 EGR       0           0                0           0
13 EGR       0           0                0           0
14 EGR       0           0                0           0
15 EGR       0           0                0           0
```

Flow Monitor

De configuratie van de stroommonitor omvat het volgende:

1. NetFlow ACL-configuratie, die resulteert in het maken van een vermelding binnen de ACL TCAM-tabel.

De ACL TCAM-vermelding bestaat uit:

- Lookup-overeenkomende toetsen
- Resultaatparameters die worden gebruikt voor NetFlow lookup, waaronder het volgende: Profiel IDNetFlow-id

2. Flow Mask Configuration, wat resulteert in het maken van een vermelding in NflLookupTable en NflFlowMaskTable.

- Geïndexeerd door NetFlow ACL-resultaatparameters om het stroommasker voor NetFlow lookup te vinden

NetFlow ACL

Om de NetFlow ACL-configuratie te bekijken, voert u de opdracht "**toon platform hardware fed switch active fwd-asic resource tcam table nfl_acl asic <asic number>**

> **Tip**: Als er een Port ACL (PACL) is, wordt het item gemaakt op de ASIC waarop de interface wordt toegewezen. In het geval van een Router ACL (RACL) is de vermelding aanwezig op alle ASIC(s).

- In deze uitvoer zijn NFCMD0 en NFCMD1, die 4-bits waarden zijn. Om de profiel-ID te berekenen, converteert u de waarden naar binair getal.
- In deze uitvoer is NFCMD0 1, is NFCMD1 2. Bij conversie naar binair getal: 000100010
- In Cisco IOS-XE 16.12 en verder binnen de gecombineerde 8 bits zijn de eerste 4 bits de profielid en de 7e bit geeft aan dat de raadpleging is ingeschakeld. In het voorbeeld **0001**0010 is de profiel-ID 1.
- In Cisco IOS XE 16.11 en oudere versies van code, binnen de gecombineerde 8 bits, zijn de eerste 6 bits de profielid en de 7e bit geeft aan dat de raadpleging is ingeschakeld. In dit voorbeeld, **000100**10, is de profiel-ID 4.

```
Switch#show platform hardware fed switch active fwd-asic resource tcam table nfl_acl asic 0
```

```
Printing entries for region INGRESS_NFL_ACL_CONTROL (308) type 6 asic 0
=========================================================
Printing entries for region INGRESS_NFL_ACL_GACL (309) type 6 asic 0
=========================================================
Printing entries for region INGRESS_NFL_ACL_PACL (310) type 6 asic 0
=========================================================
TAQ-2 Index-32 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Input IPv4 NFL PACL

Labels  Port   Vlan   L3If   Group
M:      00ff   0000   0000   0000
V:      0001   0000   0000   0000

   vcuResults l3Len l3Pro l3Tos SrcAddr  DstAddr  mtrid vrfid  SH
M:  00000000   0000  00    00  00000000 00000000  00   0000   0000
V:  00000000   0000  00    00  00000000 00000000  00   0000   0000

   RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn  l3m
M:  0    0  0    0    0  0   0  0  0   0  0   0
V:  0    0  0    0    0  0   0  0  0   0  0   0

   SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S_P2P D_P2P
M:  0000    0000              00    00    0000    00       0     0     0
V:  0000    0000              00    00    0000    00       0     0     0

   SgEn SgLabel    AuthBehaviorTag  l2srcMiss  l2dstMiss ipTtl SgaclDeny
M:  0    000000    0  0   0 0     0
V:  0    000000    0  0   0 0     0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     1      2     0    1    0   0      0     0      0 0x0000f       0
Start/Skip Word: 0x00000003
Start Feature, Terminate

----------------------------------------
Printing entries for region INGRESS_NFL_ACL_VACL (311) type 6 asic 0
=========================================================
Printing entries for region INGRESS_NFL_ACL_RACL (312) type 6 asic 0
=========================================================
Printing entries for region INGRESS_NFL_ACL_SSID (313) type 6 asic 0
=========================================================
Printing entries for region INGRESS_NFL_CATCHALL (314) type 6 asic 0
=========================================================
TAQ-2 Index-224 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Input IPv4 NFL RACL

Labels  Port   Vlan   L3If   Group
M:      0000   0000   0000   0000
V:      0000   0000   0000   0000

   vcuResults l3Len l3Pro l3Tos SrcAddr  DstAddr  mtrid vrfid  SH
M:  00000000   0000  00    00  00000000 00000000  00   0000   0000
V:  00000000   0000  00    00  00000000 00000000  00   0000   0000

   RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn  l3m
M:  0    0  0    0    0  0   0  0  0   0  0   0
V:  0    0  0    0    0  0   0  0  0   0  0   0

   SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S_P2P D_P2P
M:  0000    0000              00    00    0000    00       0     0     0
V:  0000    0000              00    00    0000    00       0     0     0

   SgEn SgLabel    AuthBehaviorTag  l2srcMiss  l2dstMiss ipTtl SgaclDeny
M:  0    000000    0  0   0 0     0
```

```
V:  0    000000    0  0   0 0     0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000003
Start Feature, Terminate

----------------------------------------
TAQ-2 Index-225 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input IPv4 NFL PACL

Labels  Port   Vlan   L3If   Group
M:      0000   0000   0000   0000
V:      0000   0000   0000   0000

   vcuResults l3Len l3Pro l3Tos SrcAddr  DstAddr  mtrid vrfid  SH
M:  00000000   0000  00    00  00000000 00000000  00   0000   0000
V:  00000000   0000  00    00  00000000 00000000  00   0000   0000

   RMAC RA MEn IPOPT MF NFF DF SO DPT TM DSEn  l3m
M:  0    0  0    0    0  0   0  0  0   0  0   0
V:  0    0  0    0    0  0   0  0  0   0  0   0

   SrcPort DstPortIITypeCode TCPFlags TTL ISBM QosLabel ReQOS S_P2P D_P2P
M:  0000    0000              00     00    0000    00      0     0     0
V:  0000    0000              00     00    0000    00      0     0     0

   SgEn SgLabel    AuthBehaviorTag  l2srcMiss  l2dstMiss ipTtl SgaclDeny
M:  0    000000    0  0   0 0     0
V:  0    000000    0  0   0 0     0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000000
No Start, Terminate

----------------------------------------
TAQ-2 Index-226 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input IPv6 NFL PACL

Labels  Port   Vlan   L3If   Group
Mask    0x0000 0x0000 0x0000 0x0000
Value   0x0000 0x0000 0x0000 0x0000

vcuResult dstAddr0 dstAddr1 dstAddr2 dstAddr3 srcAddr0
00000000  00000000 00000000 00000000 00000000 00000000
00000000  00000000 00000000 00000000 00000000 00000000

srcAddr1 srcAddr2 srcAddr3 TC HL l3Len fLabel vrfId toUs
00000000 00000000 00000000 00 00  0000  00000  000   0
00000000 00000000 00000000 00 00  0000  00000  000   0

l3Pro mtrId AE FE RE HE MF NFF SO IPOPT RA MEn RMAC DPT TMP l3m
 00    00   0  0  0  0  0   0  0    0   0   0   0    0   0    0
 00    00   0  0  0  0  0   0  0    0   0   0   0    0   0    0

DSE srcPort dstPortIITypeCode tcpFlags IIPresent cZId dstZId
 0   0000    0000       00       00      00      00
 0   0000    0000       00       00      00      00

v6RT AH ESP mREn ReQOS QosLabel PRole VRole  AuthBehaviorTag
M: 0   0   0    0    0       00          0     0 0
V: 0   0   0    0    0       00          0     0 0
```

```
   SgEn SgLabel
M:  0    000000
V:  0    000000

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000000
No Start, Terminate

----------------------------------------
TAQ-2 Index-228 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
conversion to string vmr l2p not supported
----------------------------------------
TAQ-2 Index-230 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Input MAC NFL PACL

Labels  Port   Vlan   L3If   Group
M:      0000   0000   0000   0000
V:      0000   0000   0000   0000

   arpSrcHwAddr  arpDestHwAddr  arpSrcIpAddr  arpTargetIp  arpOperation
M: 000000000000  000000000000   00000000       00000000     0000
V: 000000000000  000000000000   00000000       00000000     0000


   TRUST  SNOOP  SVALID  DVALID
M:    0     0      0      0
V:    0     0      0      0


   arpHardwareLength  arpHardwareType  arpProtocolLength  arpProtocolType
M:   00000000          00000000            00000000          00000000
V:   00000000          00000000            00000000          00000000


   VlanId l2Encap l2Protocol cosCFI   srcMAC      dstMAC    ISBM  QosLabel
M:  000    0        0000     0     000000000000 000000000000 00     00
V:  000    0        0000     0     000000000000 000000000000 00     00


  ReQOS isSnap  isLLC  AuthBehaviorTag
M:  0     0      0       0
V:  0     0      0        0

NFCMD0 NFCMD1 SMPLR LKP1 LKP2 PID QOSPRI MQLBL MPLPRO LUT0PRI CPUCOPY
     0      0     0    0    0   0      0     0      0 0x00000       0
Start/Skip Word: 0x00000000
No Start, Terminate

----------------------------------------
```

Flow Mask

Voer de opdracht "**toon platform software fed switch active|standby|member fnf fmasker-entry asic <asic number> entry 1" uit** om te bekijken dat het flow mask in hardware is geïnstalleerd. Het aantal belangrijke velden vindt u hier ook.

```
Switch#show platform software fed switch active fnf fmask-entry asic 1 entry 1

---------------------------------
mask0_valid : 1
```

```
Mask hdl0   : 1
Profile ID  : 0
Feature 0   : 148
Fmsk0 RefCnt: 1
Mask M1     :
[511:256] => :00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
[255:000] => :FFFFFFFF 00000000 FFFFFFFF 03FF0000 00000000 00FF0000 00000000 C00000FF

Mask M2     :

Key Map     :

Source   Field-Id   Size   NumPFields   Pfields
 002       090       04        01       (0 1 1 1)
 002       091       04        01       (0 1 1 0)
 002       000       01        01       (0 1 0 7)
 000       056       08        01       (0 0 2 4)
 001       011       11        04       (0 0 0 1) (0 0 0 0) (0 1 0 6) (0 0 2 0)
 000       067       32        01       (0 1 12 0)
 000       068       32        01       (0 1 12 2)
```

Flow Stats en tijdstempel-offload gegevens

Voer de opdracht "**Toon platformsoftware gevoed switch actieve fnf flow-record asic <asic number> start-index <index number> num-flows <aantal stromen>** om netflow-statistieken en tijdstempels te bekijken

```
Switch#show platform software fed switch active fnf flow-record asic 1 start-index 1 num-flows 1
1 flows starting at 1 for asic 1:--------------------------------------------------
Idx 996 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
{11 PAD-UNK = 0x0000}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a86464}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a8c864}
FirstSeen = 0x4b2f, LastSeen = 0x4c59, sysUptime = 0x4c9d
PKT Count = 0x000000000102d5df, L2ByteCount = 0x00000000ca371638
```

```
Switch#show platform software fed switch active fnf flow-record asic 1 start-index 1 num-flows 1
1 flows starting at 1 for asic 1:--------------------------------------------------
Idx 996 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
{11 PAD-UNK = 0x0000}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a86464}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a8c864}
FirstSeen = 0x4b2f, LastSeen = 0x4c5b, sysUptime = 0x4c9f
PKT Count = 0x0000000001050682, L2ByteCount = 0x00000000cbed1590
```

Application Visibility and Control (AVC)

Achtergrondinformatie

- Application Visibility and Control (AVC) is een oplossing waarmee gebruik wordt gemaakt van

Network-Based Recognition versie 2 (**NBAR2**), **NetFlow V9** en verschillende rapport- en beheertools (**Cisco Prime**) om toepassingen te classificeren via deep packet inspection (DPI).
- AVC kan worden geconfigureerd op bekabelde toegangspoorten voor standalone switches of switch-stacks.
- AVC kan ook worden gebruikt op Cisco draadloze controllers om toepassingen te identificeren op basis van DPI en deze vervolgens te markeren met een specifieke DSCP-waarde. Het kan ook verschillende draadloze prestatiestatistieken verzamelen zoals bandbreedtegebruik in termen van toepassingen en clients.

Prestaties en schaal

Prestaties: elk lid van de switch kan 500 verbindingen per seconde (CPS) aan bij minder dan 50% CPU-gebruik. Buiten dit tarief is AVC service niet gegarandeerd.

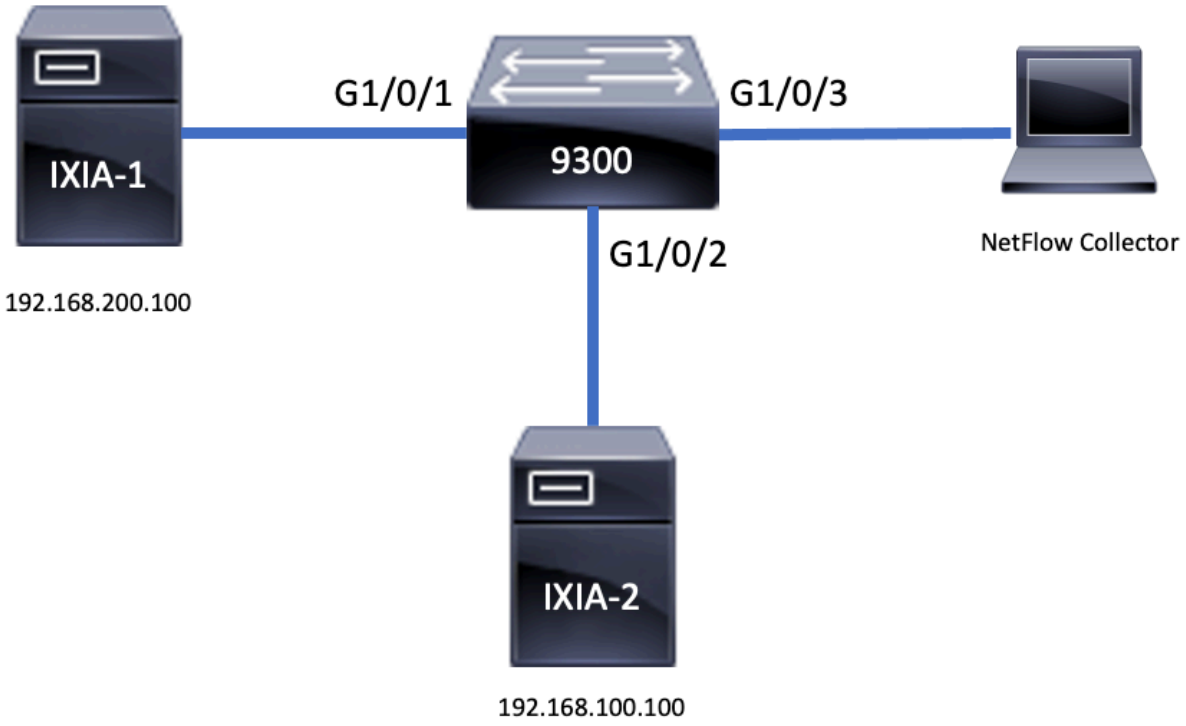
Schaal: Mogelijkheid om tot 5000 bidirectionele stromen per 24 access poorten (ongeveer 200 stromen per access poort) te verwerken.

Beperkingen van bekabelde AVC

- AVC en Encrypted Traffic Analytics (ETA) kunnen niet tegelijkertijd op dezelfde interface worden geconfigureerd.
- Packet classificatie wordt alleen ondersteund voor unicast IPv4 (TCP/UDP) verkeer.
- Op NBAR gebaseerde QoS-beleidsconfiguratie wordt alleen ondersteund op bekabelde fysieke poorten. Dit omvat Layer 2-toegangs- en trunkpoorten en Layer 3-routeringspoorten.
- Op NBAR gebaseerde QoS-beleidsconfiguratie wordt niet ondersteund op poortkanaals leden, Switch Virtual Interfaces (SVI's) of subinterfaces.
- Op NBAR2 gebaseerde classificators **(match protocol),** ondersteunen alleen QoS-acties van markering en toezicht.
- "Match protocol" is beperkt tot 255 verschillende protocollen in alle beleidsgebieden (8-bits hardwarebeperking)

Opmerking: Dit is geen uitputtende lijst van alle beperkingen, raadpleeg de aangewezen AVC configuratiegids voor uw platform en versie van code.

Netwerkdiagram



Componenten

AVC-configuratie bestaat uit **drie hoofdcomponenten** waaruit de oplossing bestaat:

Zichtbaarheid: Protocoldetectie

- Protocoldetectie wordt bereikt via NBAR, die per interface, richting en applicatie bytes/pakketten statistieken biedt.
- Protocoldetectie is ingeschakeld voor een specifieke interface via de interfaceconfiguratie: **ip nbar protocol-discovery**

Zoals in de uitvoer wordt getoond, hoe u protocoldetectie inschakelt:

```
Switch(config)#interface fi4/0/5
Switch(config-if)#ip nbar protocol-discovery
Switch(config-if)#exit

Switch#show run int fi4/0/5
Building configuration...

Current configuration : 70 bytes
!
interface FiveGigabitEthernet4/0/5
ip nbar protocol-discovery
end
```

Controle: Op toepassing gebaseerde QoS

In vergelijking met traditionele QoS die overeenkomt op IP-adres en UDP/TCP-poort, bereikt AVC een fijnere controle door op toepassingen gebaseerde QoS, waarmee u kunt matchen op toepassingen, en biedt meer granulaire controle door QoS-acties zoals markering en toezicht.

- Acties worden uitgevoerd op geaggregeerd verkeer (niet per-flow)
- Application Based QoS wordt bereikt door het maken van een class map, match van een protocol en vervolgens het maken van een policy map.
- Het op toepassing gebaseerde QoS-beleid is gekoppeld aan een interface.

Zoals getoond in de uitvoer, voorbeeldconfiguratie voor op toepassing gebaseerde QoS:

```
Switch(config)#class-map WEBEX
Switch(config-cmap)#match protocol webex-media
Switch(config)#end

Switch(config)#policy-map WEBEX
Switch(config-pmap)#class WEBEX
Switch(config-pmap-c)#set dscp af41
Switch(config)#end

Switch(config)#interface fi4/0/5
Switch(config-if)#service-policy input WEBEX
Switch(config)#end

Switch#show run int fi4/0/5
Building configuration...

Current configuration : 98 bytes
!
interface FiveGigabitEthernet4/0/5
service-policy input WEBEX
ip nbar protocol-discovery
end
```

Op toepassingen gebaseerde flexibele NetFlow

Wired AVC FNF ondersteunt twee typen vooraf gedefinieerde flow records: **oude bidirectionele stroomrecords** en nieuwe **directionele stroomrecords**.

De bidirectionele stroomverslagen houden spoor van de statistieken van de cliënt/servertoepassing.

Zoals getoond in de output, voorbeeldconfiguratie van een bidirectioneel stroomverslag.

```
Switch(config)#flow record BIDIR-1
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match application name
Switch(config-flow-record)#match connection client ipv4 address
Switch(config-flow-record)#match connection server ipv4 address
Switch(config-flow-record)#match connection server transport port
Switch(config-flow-record)#match flow observation point
Switch(config-flow-record)#collect flow direction
Switch(config-flow-record)#collect connection initiator
Switch(config-flow-record)#collect connection new-connections
Switch(config-flow-record)#collect connection client counter packets long
Switch(config-flow-record)#connection client counter bytes network long
Switch(config-flow-record)#collect connection server counter packets long
Switch(config-flow-record)#connection server counter bytes network long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end
```

```
Switch#show flow record BIDIR-1
flow record BIDIR-1:
Description: User defined
No. of users: 0
Total field space: 78 bytes
Fields:
match ipv4 version
match ipv4 protocol
match application name
match connection client ipv4 address
match connection server ipv4 address
match connection server transport port
match flow observation point
collect flow direction
collect timestamp absolute first
collect timestamp absolute last
collect connection initiator
collect connection new-connections
collect connection server counter packets long
collect connection client counter packets long
collect connection server counter bytes network long
collect connection client counter bytes network long
```

Directionele records zijn toepassingsstats voor invoer/uitvoer.

Zoals getoond in de output, configuratie voorbeelden van input en output directionele verslagen:

> **Opmerking**: de opdracht "**match interface input**" specificeert een match met de input interface. Het commando "**match interface output**" specificeert een match met de output interface. De opdracht "**match application name**" is verplicht voor AVC ondersteuning.

```
Switch(config)#flow record APP-IN
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match ipv4 source address
Switch(config-flow-record)#match ipv4 destination address
Switch(config-flow-record)#match transport source-port
Switch(config-flow-record)#match transport destination-port
Switch(config-flow-record)#match interface input
Switch(config-flow-record)#match application name
Switch(config-flow-record)#collect interface output
Switch(config-flow-record)#collect counter bytes long
Switch(config-flow-record)#collect counter packets long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end

Switch#show flow record APP-IN
flow record APP-IN:
Description: User defined
No. of users: 0
Total field space: 58 bytes
Fields:
match ipv4 version
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface input
match application name
```

```
collect interface output
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last

Switch(config)#flow record APP-OUT
Switch(config-flow-record)#match ipv4 version
Switch(config-flow-record)#match ipv4 protocol
Switch(config-flow-record)#match ipv4 source address
Switch(config-flow-record)#match ipv4 destination address
Switch(config-flow-record)#match transport source-port
Switch(config-flow-record)#match transport destination-port
Switch(config-flow-record)#match interface output
Switch(config-flow-record)#match application name
Switch(config-flow-record)#collect interface input
Switch(config-flow-record)#collect counter bytes long
Switch(config-flow-record)#collect counter packets long
Switch(config-flow-record)#collect timestamp absolute first
Switch(config-flow-record)#collect timestamp absolute last
Switch(config-flow-record)#end

Switch#show flow record APP-OUT
flow record APP-OUT:
Description: User defined
No. of users: 0
Total field space: 58 bytes
Fields:
match ipv4 version
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match interface output
match application name
collect interface input
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
```

Flow Exporteur

Maak een flow-exporteur om exportparameters te definiëren.

Zoals getoond in de output, voorbeeldconfiguratie van de stroomexporteur:

```
Switch(config)#flow exporter AVC
Switch(config-flow-exporter)#destination 192.168.69.2
Switch(config-flow-exporter)#source vlan69
Switch(config-flow-exporter)#end

Switch#show run flow exporter AVC
Current configuration:
!
flow exporter AVC
destination 192.168.69.2
source Vlan69
!
```

Flow Monitor

Maak een flow monitor om deze aan een flow record te koppelen.

Zoals getoond in de output, voorbeeldconfiguratie van de stroommonitor:

```
Switch(config)#flow monitor AVC-MONITOR
Switch(config-flow-monitor)#record APP-OUT
Switch(config-flow-monitor)#exporter AVC
Switch(config-flow-monitor)#end

Switch#show run flow monitor AVC-MONITOR
Current configuration:
!
flow monitor AVC-MONITOR
exporter AVC
record APP-OUT
```

Associate Flow Monitor aan een interface

U kunt maximaal twee verschillende AVC monitoren met verschillende vooraf gedefinieerde records aan een interface **toevoegen**.

Zoals getoond in de output, voorbeeldconfiguratie van de stroommonitor:

```
Switch(config)#interface fi4/0/5
Switch(config-if)#ip flow monitor AVC-MONITOR out
Switch(config-if)#end

Switch#show run interface fi4/0/5
Building configuration...
Current configuration : 134 bytes
!
interface FiveGigabitEthernet4/0/5
ip flow monitor AVC-MONITOR output
service-policy input WEBEX
ip nbar protocol-discovery
end
```

NBAR2

NBAR2 dynamisch Hitless Protocol Pack upgrade

Protocolpakketten zijn softwarepakketten die de NBAR2-protocolondersteuning op een apparaat bijwerken zonder dat de Cisco-software op het apparaat wordt vervangen. Een protocolpakket bevat informatie over toepassingen die officieel door NBAR2 worden ondersteund en die samen worden gecompileerd en verpakt. Voor elke toepassing, omvat het protocol-pakket informatie over toepassingshandtekeningen en toepassingseigenschappen. Elke softwarerelease heeft een ingebouwde protocol-pack die bij het wordt gebundeld.

- NBAR2 biedt een manier om het protocolpakket bij te werken zonder verkeer of servicestoringen en zonder dat het softwarebeeld op het(de) apparaat(apparaten) hoeft te worden gewijzigd
- NBAR2-protocolpakketten kunnen via Cisco Software Center worden gedownload van deze URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

NBAR2-upgrade van protocolpack

Voordat u een nieuw protocolpakket installeert, moet u het protocolpakket naar de flitser op alle switch(s) kopiëren. Om het nieuwe protocolpakket te laden, gebruik de opdracht "**ip nbar protocol-pack flash:<Pack Name>**

U hoeft de switch(s) niet te herladen om de NBAR2-upgrade te moeten uitvoeren.

Zoals getoond in de uitvoer, voorbeeldconfiguratie van hoe het NBAR2-protocolpakket te laden:

```
Switch(config)#ip nbar protocol-pack flash:newProtocolPack
```

Om aan het ingebouwde protocolpakket terug te keren, gebruik het bevel "**standaard ip nbar protocol-pack**"

Zoals getoond in de output, voorbeeldconfiguratie van hoe terug te keren naar het ingebouwde protocolpakket:

```
Switch(config)#default ip nbar protocol-pack
```

Informatie over NBAR2-protocolpakketten weergeven

Om de informatie van het protocolpakket te tonen gebruik de vermelde bevelen:

- toon ip nbar versie
- toon ip nbar protocol-pack actief detail

Zoals in de uitvoer, voorbeeldoutput van die opdrachten:

```
Switch#show ip nbar version
NBAR software version: 37
NBAR minimum backward compatible version: 37
NBAR change ID: 293126

Loaded Protocol Pack(s):
Name: Advanced Protocol Pack
Version: 43.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 37
State: Active

Switch#show ip nbar protocol-pack active detail
Active Protocol Pack:
Name: Advanced Protocol Pack
Version: 43.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 37
State: Active
```

NBAR2 aangepaste toepassingen

NBAR2 ondersteunt het gebruik van aangepaste protocollen om aangepaste toepassingen te identificeren. Aangepaste protocollen ondersteunen protocollen en toepassingen die NBAR2 momenteel niet ondersteunt.

Deze kunnen het volgende omvatten:

- Specifieke toepassing op een organisatie
- Specifieke toepassingen voor een geografie

NBAR2 biedt een manier om toepassingen handmatig aan te passen via de opdrachtregel **ip nbar custom<*myappname*>**.

Opmerking: Aangepaste toepassingen hebben voorrang op ingebouwde protocollen

Er zijn verschillende soorten applicaties:

Aanpassing van generieke protocollen

- HTTP
- SSL
- DNS

Composite: Aanpassing op basis van meerdere protocollen -**server-naam**

Layer 3/Layer 4-aanpassing

- IPv4-adres
- DSCP-waarden
- TCP/UDP-poorten
- Stroombron of doelrichting

Byte Offset: Aanpassing op basis van specifieke byte-waarden in de payload

HTTP-aanpassing

HTTP-aanpassing kan worden gebaseerd op een combinatie van HTTP-velden van:

- **Cookies** - HTTP Cookie
- **host** - hostnaam van Origin Server die de bron bevat
- **methode** - HTTP-methode
- **referrer** - Adres het resourceverzoek is verkregen van
- **url** - Uniform Resource Locator-pad
- **user-agent** - Software die wordt gebruikt door de agent die het verzoek verstuurt
- **versie** - HTTP-versie
- **via** - HTTP via veld

Voorbeeld aangepaste toepassing genaamd MYHTTP die de HTTP-host "*mydomain.com" gebruikt met Selector ID 10.

```
Switch(config)#ip nbar custom MYHTTP http host *mydomain.com id 10
```

SSL-aanpassing

Aanpassing kan worden gedaan voor SSL-versleuteld verkeer via informatie die is afgeleid uit de SSL Server Name Indication (SNI) of Common Name (CN).

Voorbeeld aangepaste toepassing genaamd MYSSL die SSL unieke naam "mydomain.com"

gebruikt met selector ID 11.

```
Switch(config)#ip nbar custom MYSSL ssl unique-name *mydomain.com id 11
```

DNS-aanpassing

NBAR2 onderzoekt DNS verzoek en reactieverkeer, en kan de DNS reactie op een toepassing correleren. Het IP-adres dat afkomstig is van de DNS-respons wordt in de cachegeheugen opgeslagen en gebruikt voor latere pakketstromen die aan die specifieke toepassing zijn gekoppeld.

De commandip nbar *customapplication-namednsdomain-namedapplication*-idis wordt gebruikt voor DNS-aanpassing. Om een toepassing uit te breiden, gebruik de commandip nbar *customapplication*-names domain-*namedomain-name extends existing-application*.

Voorbeeld aangepaste toepassing genaamd MYDNS die de DNS domeinnaam "mydomain.com" gebruikt met selector ID 12.

```
Switch(config)#ip nbar custom MYDNS dns domain-name *mydomain.com id 12
```

Composite-aanpassing

NBAR2 biedt een manier om toepassingen aan te passen op basis van domeinnamen die worden weergegeven in HTTP, SSL of DNS.

Voorbeeld aangepaste toepassing genaamd MYDOMAIN die gebruikmaakt van HTTP, SSL of DNS domeinnaam "mydomain.com" met selector ID 13.

```
Switch(config)#ip nbar custom MYDOMAIN composite server-name *mydomain.com id 13
```

L3/L4-aanpassing

Layer 3/Layer 4-aanpassing is gebaseerd op de pakkettuple en wordt altijd afgestemd op het eerste pakket van een stroom.

Voorbeeld aangepaste toepassing LAYER4CUSTOMER die IP-adressen 10.56.1.10 en 10.56.1.11, TCP- en DSCP-ef aanpast met selector-ID 14.

```
Switch(config)#ip nbar custom LAYER4CUSTOM transport tcp id 14
Switch(config-custom)#ip address 10.56.1.10 10.56.1.11
Switch(config-custom)#dscp ef
Switch(config-custom)#end
```

Aangepaste toepassingen bewaken

Om aangepaste toepassingen te bewaken, gebruikt u de genoemde showopdrachten:

IP-nbar protocol-id tonen | inc Aangepast

```
Switch#show ip nbar protocol-id | inc Custom
LAYER4CUSTOM              14            Custom
MYDNS                     12            Custom
```

```
MYDOMAIN                 13            Custom
MYHTTP                   10            Custom
MYSSL                    11            Custom
```

IP-nbar protocol-id AANGEPASTE_APP tonen

```
Switch#show ip nbar protocol-id MYSSL
Protocol Name             id            type
-----------------------------------------------
MYSSL                    11            Custom
```

Controleer AVC

Er zijn meerdere stappen om de functionaliteit van AVC te valideren, deze sectie biedt opdrachten en voorbeelduitvoer.

Om te bevestigen dat NBAR actief is, kunt u de opdracht "toon ip nbar control-plane" uitvoeren

Belangrijke gebieden:

- De status NBAR moet in een correct scenario worden geactiveerd
- De NBAR-configuratiestatus moet in een correct scenario klaar zijn

```
Switch#show ip nbar control-plane
NGCP Status:
============

graph sender info:
NBAR state is ACTIVATED
NBAR config send mode is ASYNC
NBAR config state is READY

NBAR update ID 3
NBAR batch ID ACK 3
NBAR last batch ID ACK clients 1 (ID: 4)
Active clients 1 (ID: 4)
NBAR max protocol ID ever 1935
NBAR Control-Plane Version: 37

<snip>
```

Controleer dat elk switch lid een actief dataplatform heeft met de opdracht show platform software gevoed switch active|standby|member wdavc functie wdavc_stile_cp_show_info_ui:

Is DP geactiveerd moet TRUE zijn in een correct scenario

```
Switch#show platform software fed switch active wdavc function wdavc_stile_cp_show_info_ui

Is DP activated : TRUE
MSG ID : 3
Maximum number of flows: 262144
Current number of graphs: 1
Requests queue state : WDAVC_STILE_REQ_QUEUE_STATE_UP
Number of requests in queue : 0
Max number of requests in queue (TBD): 1
Counters:
activate_msgs_rcvd : 1
```

```
graph_download_begin_msgs_rcvd : 3
stile_config_msgs_rcvd : 1584
graph_download_end_msgs_rcvd : 3
deactivate_msgs_rcvd : 0
intf_proto_disc_msgs_rcvd : 1
intf_attach_msgs_rcvd : 2
cfg_response_msgs_sent : 1593
num_of_handle_msg_from_fmanfp_events : 1594
num_of_handle_request_from_queue : 1594
num_of_handle_process_requests_events : 1594
```

Gebruik de opdracht "**toon platform software fed switch active|standby|member wdavc flows** om belangrijke informatie weer te geven:

```
Switch#show platform software fed switch active wdavc flows

CurrFlows=1, Watermark=1

IX |IP1 |IP2 |PORT1|PORT2|L3 |L4 |VRF |TIMEOUT|APP |TUPLE|FLOW |IS FIF |BYPASS|FINAL |#PKTS
|BYPASS
  | | | | |PROTO|PROTO|VLAN|SEC |NAME |TYPE |TYPE |SWAPPED | | | |PKT
-------------------------------------------------------------------------------------
1 |192.168.100.2 |192.168.200.2 |68 |67 |1 |17 |0 |360 |unknown |Full |Real Flow|Yes |True |True
|40 |40
```

Belangrijkste velden:

CurrFlows: toont aan hoeveel actieve stromen door AVC worden bijgehouden

Watermerk: Toont het grootste aantal stromen aan dat historisch door AVC wordt bijgehouden

TIME-OUT SEC: Time-out voor inactiviteit op basis van de geïdentificeerde toepassing

APP-NAAM: Geïdentificeerde toepassing

STROOMTYPE: Real Flow geeft aan dat dit is gemaakt als resultaat van inkomende data. Pre Flow geeft aan dat deze flow wordt gecreëerd als resultaat van inkomende gegevens. Pre-flows worden gebruikt voor verwachte mediastromen

TUPLE TYPE: Echte stromen zijn altijd volledig tuple, Pre-flows zijn ofwel volledig tuple of half tuple

OMZEILEN: Indien ingesteld op TRUE, geeft aan dat er geen pakketten meer vereist zijn door de software om deze flow te kunnen identificeren

DEFINITIEF: Als dit item wordt ingesteld op TRUE, dan geeft dit aan dat de applicatie niet meer verandert voor deze stroom

OMZEILEN PKT: Hoeveel pakketten waren er nodig om tot de definitieve classificatie te komen

#PKTS: Hoeveel pakketten zijn eigenlijk gepunteerd aan software voor deze stroom

Bekijk aanvullende details over huidige stromen, u kunt de opdracht "**toon platformsoftware gevoed switch actieve wdavc functie wdavc_ft_show_all_flows_seg_ui" gebruiken**

```
Switch#show platform software fed switch active wdavc function wdavc_ft_show_all_flows_seg_ui
CurrFlows=1, Watermark=1

IX |IP1 |IP2 |PORT1|PORT2|L3 |L4 |VRF |TIMEOUT|APP |TUPLE |FLOW |IS FIF |BYPASS|FINAL |#PKTS
|BYPASS
| | | | |PROTO|PROTO|VLAN|SEC |NAME |TYPE |TYPE |SWAPPED | | | |PKT
-------------------------------------------------------------------------------------------
-------------------------------------------------------------------
1 |192.168.100.2 |192.168.200.2|68 |67 |1 |17 |0 |360 |unknown |Full |Real Flow|Yes |True |True
|40 |40

SEG IDX |I/F ID |OPST I/F |SEG DIR |FIF DIR |Is SET |DOP ID |NFL HDL |BPS PND |APP PND |FRST TS
|LAST TS |BYTES |PKTS |TCP FLGS
-------------------------------------------------------------------------------------------
-----------------------------------
0 |9 |---- |Ingress |True |True |0 |50331823 |0 |0 |177403000|191422000|24252524|70094 |0
```

Belangrijke velden

ID I/F: Specificeert de interface-ID

SEG DIR: Specificeert ingangen van uitgangsrichting

FIF DIR: bepaalt of dit de richting van de stroominitiator is

NFL HDL: Flow ID in hardware

Om het item in de hardware te bekijken, voert u de opdracht **"toon platform software gevoede switch actieve fnf flow-record asic <number> start-index <number> num-flows <aantal stromen>**

> **Opmerking:** Om de ASIC te kiezen, is het de ASIC-instantie waaraan de poort wordt toegewezen. Om de ASIC te identificeren, gebruik de opdracht **"show platform software fed switch active|standby|member ifm mappings"** De start-index kan op "0" worden ingesteld als u niet in een specifieke flow bent geïnteresseerd. Anders moet de start-index worden gespecificeerd. Voor num-stromen, die het aantal stromen specificeert dat kan worden bekeken, maximum 10.

```
Switch#show platform software fed switch active fnf flow-record asic 3 start-index 0 num-flows 1
1 flows starting at 0 for asic 3:-------------------------------------------------
Idx 175 :
{90, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE1 = 0x01}
{91, ALR_INGRESS_NET_FLOW_ACL_LOOKUP_TYPE2 = 0x01}
{0, ALR_INGRESS_NFL_SPECIAL1 = 0x00}
{11 PAD-UNK = 0x0000}
{94, PHF_INGRESS_DEST_PORT_OR_ICMP_OR_IGMP_OR_PIM_FIRST16B = 0x0043}
{93, PHF_INGRESS_SRC_PORT = 0x0044}
{67, PHF_INGRESS_IPV4_DEST_ADDRESS = 0xc0a8c802}
{68, PHF_INGRESS_IPV4_SRC_ADDRESS = 0xc0a86402}
{56, PHF_INGRESS_L3_PROTOCOL = 0x11}
FirstSeen = 0x2b4fb, LastSeen = 0x2eede, sysUptime = 0x2ef1c
PKT Count = 0x000000000001216f, L2ByteCount = 0x0000000001873006
```

Zoek naar verschillende fouten en waarschuwingen in het gegevenspad

Gebruik de opdracht **"toon platformsoftware gevoede switch active|standby|member wdavc function wdavc_ft_show_stats_ui | inc err|warn|fail** om mogelijke flow table fouten weer te geven:

```
Switch#show platform software fed switch active wdavc function wdavc_ft_show_stats_ui | inc
err|warn|fail
Bucket linked exceed max error : 0
extract_tuple_non_first_fragment_warn : 0
ft_client_err_alloc_fail : 0
ft_client_err_detach_fail : 0
ft_client_err_detach_fail_intf_attach : 0
ft_inst_nfl_clock_sync_err : 0
ft_ager_err_invalid_timeout : 0
ft_intf_err_alloc_fail : 0
ft_intf_err_detach_fail : 0
ft_inst_err_unreg_client_all : 0
ft_inst_err_inst_del_fail : 0
ft_flow_seg_sync_nfl_resp_pend_del_warn : 0
ager_sm_cb_bad_status_err : 0
ager_sm_cb_received_err : 0
ft_ager_to_time_no_mask_err : 0
ft_ager_to_time_latest_zero_ts_warn : 0
ft_ager_to_time_seg_zero_ts_warn : 0
ft_ager_to_time_ts_bigger_curr_warn : 0
ft_ager_to_ad_nfl_resp_error : 0
ft_ager_to_ad_req_all_recv_error : 0
ft_ager_to_ad_req_error : 0
ft_ager_to_ad_resp_error : 0
ft_ager_to_ad_req_restart_timer_due_err : 0
ft_ager_to_flow_del_nfl_resp_error : 0
ft_ager_to_flow_del_all_recv_error : 0
ft_ager_to_flow_del_req_error : 0
ft_ager_to_flow_del_resp_error : 0
ft_consumer_timer_start_error : 0
ft_consumer_tw_stop_error : 0
ft_consumer_memory_error : 0
ft_consumer_ad_resp_error : 0
ft_consumer_ad_resp_fc_error : 0
ft_consumer_cb_err : 0
ft_consumer_ad_resp_zero_ts_warn : 0
ft_consumer_ad_resp_zero_pkts_bytes_warn : 0
ft_consumer_remove_on_count_zero_err : 0
ft_ext_field_ref_cnt_zero_warn : 0
ft_ext_gen_ref_cnt_zero_warn : 0
```

Gebruik de opdracht **"toon platformsoftware gevoed switch actieve wdavc functie wdavc_stile_stats_show_ui | inc err"** om mogelijke NBAR-fouten te bekijken:

```
Switch#show platform software fed switch active wdavc function wdavc_stile_stats_show_ui | inc
err
find_flow_error : 0
add_flow_error : 0
remove_flow_error : 0
detach_fo_error : 0
is_forward_direction_error : 0
set_flow_aging_error : 0
ft_process_packet_error : 0
sys_meminfo_get_error : 0
```

Controleer of pakketten worden gekloond naar CPU

Gebruik de opdracht **"toon platformsoftware gevoed switch actief punt cpuq 21 | incl. ontvangen"** om te verifiëren dat pakketten naar de CPU worden gekloond voor verwerking van NBAR:

> **Opmerking:** In het lab is dit aantal niet toegenomen.

```
Switch#show platform software fed switch active punt cpuq 21 | inc received
Packets received from ASIC : 63
```

CPU-congestie identificeren

In tijden van stremming, kunnen de pakketten worden gelaten vallen alvorens naar proces WDAVC te verzenden. Gebruik de opdracht **"show platform software fed switch active wdavc function fed_wdavc_show_ots_stats_ui"** om te valideren:

```
Switch#show platform software fed switch active wdavc function fed_wdavc_show_ots_stats_ui
OTS Limits
-------------------------------------------
ots_queue_max : 20000
emer_bypass_ots_queue_stress : 4000
emer_bypass_ots_queue_normal : 200
OTS Statistics
-------------------------------------------
total_requests : 40
total_non_wdavc_requests : 0
request_empty_field_data_error : 0
request_invalid_di_error : 0
request_buf_coalesce_error : 0
request_invalid_format_error : 0
request_ip_version_error : 0
request_empty_packet_error : 0
memory_allocation_error : 0
emergency_bypass_requests_warn : 0
dropped_requests : 0
enqueued_requests : 40
max_ots_queue : 0
```

> **Tip**: Om de punt drop teller te wissen gebruik de opdracht "**toon platform software fed switch actieve wdavc functie fed_wdavc_clear_ots_stats_ui"**

Schaalproblemen identificeren

Als er geen gratis FNF-vermeldingen in de hardware zijn, is het verkeer niet onderhevig aan de NBAR2-classificatie. Gebruik de opdracht "**show platform software fed switch active fnf sw-table-size asic <number> schaduw 0"** om te bevestigen:

> **Opmerking:** Stromen die worden gecreëerd zijn specifiek voor de switch en basiskern wanneer ze worden gecreëerd. Het nummer van de switch (actief, stand-by, enzovoort) moet duidelijk worden aangegeven. Het ASIC-nummer dat wordt ingevoerd, is gekoppeld aan de respectieve interface. Gebruik "**show platform software fed switch active|standby|member information mappings"** om ASIC te bepalen die aan de interface beantwoordt. Gebruik voor de schaduwoptie altijd "0".

```
Switch#show platform software fed switch active fnf sw-table-sizes asic 3 shadow 0

---------------------------------
Global Bank Allocation
---------------------------------
Ingress Banks : Bank 0
Egress Banks : Bank 1
---------------------------------
```

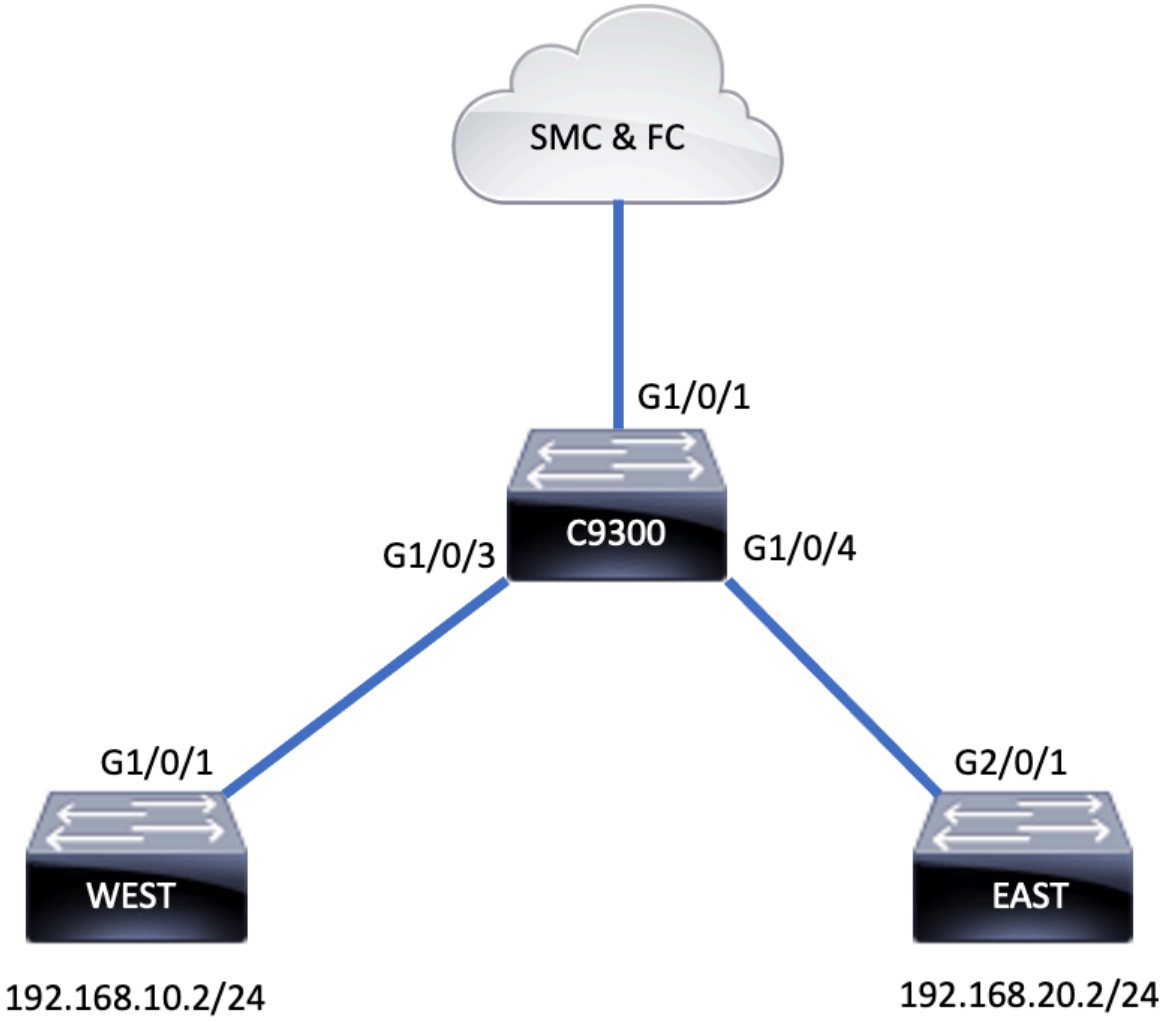
```
Global flow table Info
INGRESS usedBankEntry 1 usedOvfTcamEntry 0
EGRESS usedBankEntry 0 usedOvfTcamEntry 0 <-- 256 means TCAM entries are full
---------------------------------
Flows Statistics
INGRESS TotalSeen=1 MaxEntries=1 MaxOverflow=0
EGRESS TotalSeen=0 MaxEntries=0 MaxOverflow=0

---------------------------------
Partition Table
---------------------------------
## Dir Limit CurrFlowCount OverFlowCount MonitoringEnabled
0 ING 0 0 0 0
1 ING 16640 1 0 1
2 ING 0 0 0 0
3 ING 16640 0 0 0
4 ING 0 0 0 0
5 ING 8192 0 0 1
6 ING 0 0 0 0
7 ING 0 0 0 0
8 ING 0 0 0 0
9 ING 0 0 0 0
10 ING 0 0 0 0
11 ING 0 0 0 0
12 ING 0 0 0 0
13 ING 0 0 0 0
14 ING 0 0 0 0
15 ING 0 0 0 0
0 EGR 0 0 0 0
1 EGR 16640 0 0 1
2 EGR 0 0 0 0
3 EGR 16640 0 0 0
4 EGR 0 0 0 0
5 EGR 8192 0 0 1
6 EGR 0 0 0 0
7 EGR 0 0 0 0
8 EGR 0 0 0 0
9 EGR 0 0 0 0
10 EGR 0 0 0 0
11 EGR 0 0 0 0
12 EGR 0 0 0 0
13 EGR 0 0 0 0
14 EGR 0 0 0 0
15 EGR 0 0 0 0
```

Encrypted Traffic Analytics (ETA)

Achtergrondinformatie

- ETA richt zich op identificatie van malware communicatie in gecodeerd verkeer door middel van passieve monitoring, extractie van relevante data-elementen en een combinatie van gedragsmolering en machinaal leren met cloud-gebaseerde wereldwijde beveiliging.
- ETA maakt gebruik van telemetrie van NetFlow evenals versleutelde detectie van malware en naleving van cryptografische gegevens en stuurt deze gegevens naar Cisco Stealthwatch.
- ETA haalt twee belangrijke gegevenselementen uit: het Initial Data Packet (IDP) en de Sequence of Packet Length en Time (SPLT).

Netwerkdiagram



Componenten

ETA bestaat uit verschillende componenten die worden gebruikt in combinatie met de ETA-oplossing:

- NetFlow - Standaard die gegevenselementen definieert die worden geëxporteerd door netwerkapparaten die de stromen op het netwerk beschrijven.
- Cisco Stealthwatch - maakt gebruik van de kracht van netwerktelemetrie die NetFlow, IPFIX, proxy-logbestanden en diepe pakketinspectie van onbewerkte pakketten omvat - om geavanceerde netwerkzichtbaarheid, security intelligentie en analyses te bieden.
- Cisco Cognitive Intelligence - hiermee wordt kwaadaardige activiteit opgespoord die niet aan beveiligingscontroles is onderworpen of via ongecontroleerde kanalen en in de omgeving van een organisatie is ingevoerd.
- Encrypted Traffic Analytics - Cisco IOS XE-functie die geavanceerde gedragsalgoritmen gebruikt om kwaadaardige verkeerspatronen te identificeren door analyse van inftraflow-metagegevens van versleuteld verkeer, detecteert potentiële bedreigingen die verborgen zijn in versleuteld verkeer.

Opmerking: Dit deel van het document richt zich alleen op de configuratie en verificatie van ETA en NetFlow op de Catalyst 9000 Series switch en is niet van toepassing op de implementatie van Stealthwatch Management Console (SMC) en Flow Collector (FC) in de Cognitive Intelligence Cloud.

Beperkingen

- De toepassing van ETA vereist DNA-voordeel om te functioneren
- ETA en een zend (TX) switched Port Analyzer (SPAN) worden niet ondersteund op dezelfde interface.

Dit is geen inclusieve lijst. Raadpleeg de betreffende configuratiehandleiding voor de switch en versie van de code voor alle beperkingen.

Configuratie

Zoals in de output wordt getoond, laat ETA op de switch globaal toe en definieer de stroom exportbestemming:

```
C9300(config)#et-analytics
C9300(config-et-analytics)#ip flow-export destination 172.16.18.1 2055
```

Tip: U MOET poort 2055 gebruiken, gebruik geen ander poortnummer.

Configureer vervolgens Flexibel NetFlow zoals in de uitvoer wordt getoond:

Flow Record configureren

```
C9300(config)#flow record FNF-RECORD
C9300(config-flow-record)#match ipv4 protocol
C9300(config-flow-record)#match ipv4 source address
C9300(config-flow-record)#match ipv4 destination address
C9300(config-flow-record)#match transport source-port
C9300(config-flow-record)#match transport destination-port
C9300(config-flow-record)#collect counter bytes long
C9300(config-flow-record)#collect counter packets long
C9300(config-flow-record)#collect timestamp absolute first
C9300(config-flow-record)#collect timestamp absolute last
```

Flow Monitor configureren

```
C9300(config)#flow exporter FNF-EXPORTER
C9300(config-flow-exporter)#destination 172.16.18.1
C9300(config-flow-exporter)#transport udp 2055
C9300(config-flow-exporter)#template data timeout 30
C9300(config-flow-exporter)#option interface-table
C9300(config-flow-exporter)#option application-table timeout 10
C9300(config-flow-exporter)#exit
```

Flow Record configureren

```
C9300(config)#flow monitor FNF-MONITOR
C9300(config-flow-monitor)#exporter FNF-EXPORTER
C9300(config-flow-monitor)#record FNF-RECORD
C9300(config-flow-monitor)#end
```

Flow Monitor toepassen

```
C9300(config)#int range g1/0/3-4
C9300(config-if-range)#ip flow mon FNF-MONITOR in
C9300(config-if-range)#ip flow mon FNF-MONITOR out
C9300(config-if-range)#end
```

ETA op Switch-interface(s) inschakelen

```
C9300(config)#interface range g1/0/3-4
C9300(config-if-range)#et-analytics enable
```

Verifiëren

Controleer of de ETA-monitor "eta-mon" actief is. Bevestig dat de status is toegewezen via de opdracht "Toon flow monitor eta-mon"

```
C9300#show flow monitor eta-mon
Flow Monitor eta-mon:
Description: User defined
Flow Record: eta-rec
Flow Exporter: eta-exp
Cache:
Type: normal (Platform cache)
Status: allocated
Size: 10000 entries
Inactive Timeout: 15 secs
Active Timeout: 1800 secs
```

Controleer of de ETA-cache is ingevuld. Wanneer NetFlow en ETA op dezelfde interface zijn geconfigureerd, gebruik dan "show flow monitor <monitor name> cache" in plaats van "show flow monitor eta-mon cache" als de output van "show flow monitor eta-mon cache" leeg is:

```
C9300#show flow monitor FNF-MONITOR cache
Cache type: Normal (Platform cache)
Cache size: 10000
Current entries: 4

Flows added: 8
Flows aged: 4
- Inactive timeout ( 15 secs) 4

IPV4 SOURCE ADDRESS: 192.168.10.2
IPV4 DESTINATION ADDRESS: 192.168.20.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390

IPV4 SOURCE ADDRESS: 192.168.20.2
IPV4 DESTINATION ADDRESS: 192.168.10.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390
```

```
IPV4 SOURCE ADDRESS: 192.168.20.2
IPV4 DESTINATION ADDRESS: 192.168.10.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390

IPV4 SOURCE ADDRESS: 192.168.10.2
IPV4 DESTINATION ADDRESS: 192.168.20.2
TRNS SOURCE PORT: 0
TRNS DESTINATION PORT: 0
IP PROTOCOL: 1
counter bytes long: 500
counter packets long: 5
timestamp abs first: 21:53:23.390
timestamp abs last: 21:53:23.390
```

Valideren dat stromen worden geëxporteerd naar de SMC en FC met de opdracht "**toon flow exporteur eta-exp statistieken**"

```
C9300#show flow exporter eta-exp statistics
Flow Exporter eta-exp:
Packet send statistics (last cleared 03:05:32 ago):
Successfully sent: 3 (3266 bytes)

Client send statistics:
Client: Flow Monitor eta-mon
Records added: 4
- sent: 4
Bytes added: 3266
- sent: 3266
```

Bevestig dat SPLT en IDP naar de FC worden geëxporteerd met de opdracht "**Toon platformsoftware gevoede switch active fnf et-analytics-flows**"

```
C9300#show platform software fed switch active fnf et-analytics-flows

ET Analytics Flow dump

=================
Total packets received : 20
Excess packets received : 0
Excess syn received : 0
Total eta records added : 4
Current eta records : 0
Total eta splt exported : 2
Total eta IDP exported : 2
```

Valideren welke interfaces geconfigureerd zijn voor et-analytics met de opdracht "**toon platform software et-analytics interfaces**"

```
C9300#show platform software et-analytics interfaces
ET-Analytics interfaces
GigabitEthernet1/0/3
GigabitEthernet1/0/4

ET-Analytics VLANs
```

Gebruik de opdracht "toon platform software et-analytics global" om een wereldwijde status van ETA te bekijken:

```
C9300#show plat soft et-analytics global
ET-Analytics Global state
=========================
All Interfaces : Off
IP Flow-record Destination : 10.31.126.233 : 2055
Inactive timer : 15

ET-Analytics interfaces
GigabitEthernet1/0/3
GigabitEthernet1/0/4

ET-Analytics VLANs
```

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.