

Begrijp AVC op de Catalyst 9800 draadloze LAN-controller

Inhoud

[Inleiding](#)

[Voorwaarde](#)

[Informatie over Application Visibility and Control \(AVC\)](#)

[Hoe AVC werkt](#)

[Netwerkgebaseerde toepassingsherkenning \(NBAR\)](#)

[NBAR-protocol inzake beleidsprofiel inschakelen](#)

[NBAR upgraden op 9800 WLC](#)

[NetFlow](#)

[Flexibele NetFlow](#)

[Flow Monitor](#)

[AVC-ondersteunde access points](#)

[Ondersteuning voor verschillende 9800 implementatiemodi](#)

[Beperkingen bij implementatie van AVC op 9800](#)

[Netwerktopologie](#)

[AP in lokale modus](#)

[AP in flex modus](#)

[Configuratie van AVC op 9800 WLC](#)

[Lokale exporteur](#)

[Externe NetFlow Collector](#)

[Configuratie van AVC op 9800 WLC met Cisco Catalyst Center](#)

[Verificatie van AVC](#)

[Op 9800](#)

[Op DNAC](#)

[Over externe NetFlow Collector](#)

[Voorbeeld 1: Cisco Prime als NetFlow Collector](#)

[Voorbeeld 2: NetFlow Collector van derden](#)

[Verkeerscontrole](#)

[Probleemoplossing](#)

[Logbestanden verzamelen](#)

[WLC-logs](#)

[AP-logbestanden](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft Application Visibility and Control (AVC) op een Cisco Catalyst 9800 WLC die nauwkeurig beheer van toepassingsverkeer mogelijk maakt.

Voorwaarde

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco WLC 9800.
- Basiskennis van lokale en flex access mode AP.
- De toegangspunten moeten geschikt zijn voor AVC. (Niet van toepassing met Local Mode AP)
- Om het besturingspakket van AVC (QoS) te laten werken, moet de functie voor applicatiezichtbaarheid met FNF worden geconfigureerd.

Informatie over Application Visibility and Control (AVC)

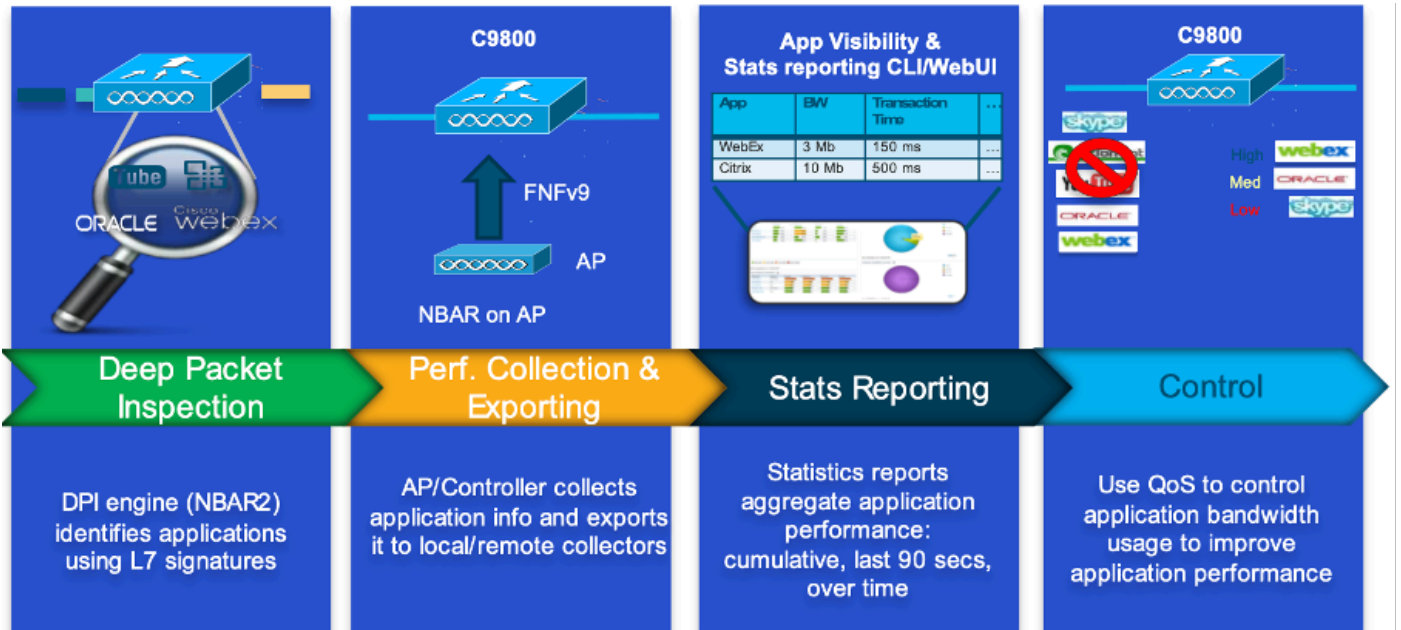
Application Visibility and Control (AVC) is de toonaangevende benadering van Cisco voor DPI-technologie (deep-packet inspection) voor zowel draadloze als bekabelde netwerken. Met AVC kunt u real-time analyses uitvoeren en beleid maken om netwerkcongestie effectief te reduceren, kostbaar netwerklinkgebruik te minimaliseren en onnodige infrastructuurupgrades te vermijden. Kortom, AVC stelt gebruikers in staat om een geheel nieuw niveau van verkeersherkenning en -vormgeving te bereiken via Network Based Application Recognition (NBAR). NBAR-pakketten die worden uitgevoerd op de 9800 WLC worden gebruikt voor DPI en de resultaten worden gerapporteerd met Flexible NetFlow (FNF).

Naast zichtbaarheid biedt AVC de mogelijkheid om verschillende soorten verkeer prioriteren, blokkeren of vertragen. Beheerders kunnen bijvoorbeeld beleid maken waarbij spraak- en videotoeepassingen prioriteit krijgen om Quality of Service (QoS) te waarborgen of de bandbreedte die beschikbaar is voor niet-essentiële toepassingen tijdens piekuren te beperken. Het programma kan ook worden geïntegreerd met andere Cisco-technologieën, zoals Cisco Identity Services Engine (ISE) voor op identiteit gebaseerde toepassingen en Cisco Catalyst Center voor gecentraliseerd beheer.

Hoe AVC werkt

AVC maakt gebruik van geavanceerde technologieën zoals FNF en NBAR2 engine voor DPI. Door verkeersstromen te analyseren en te identificeren met behulp van de NBAR2-motor, worden specifieke stromen gemarkeerd met het herkende protocol of de herkende toepassing. De controller verzamelt alle rapporten en presenteert ze via showcommando's, Web UI of extra NetFlow-exportberichten naar externe NetFlow-collectors zoals Prime.

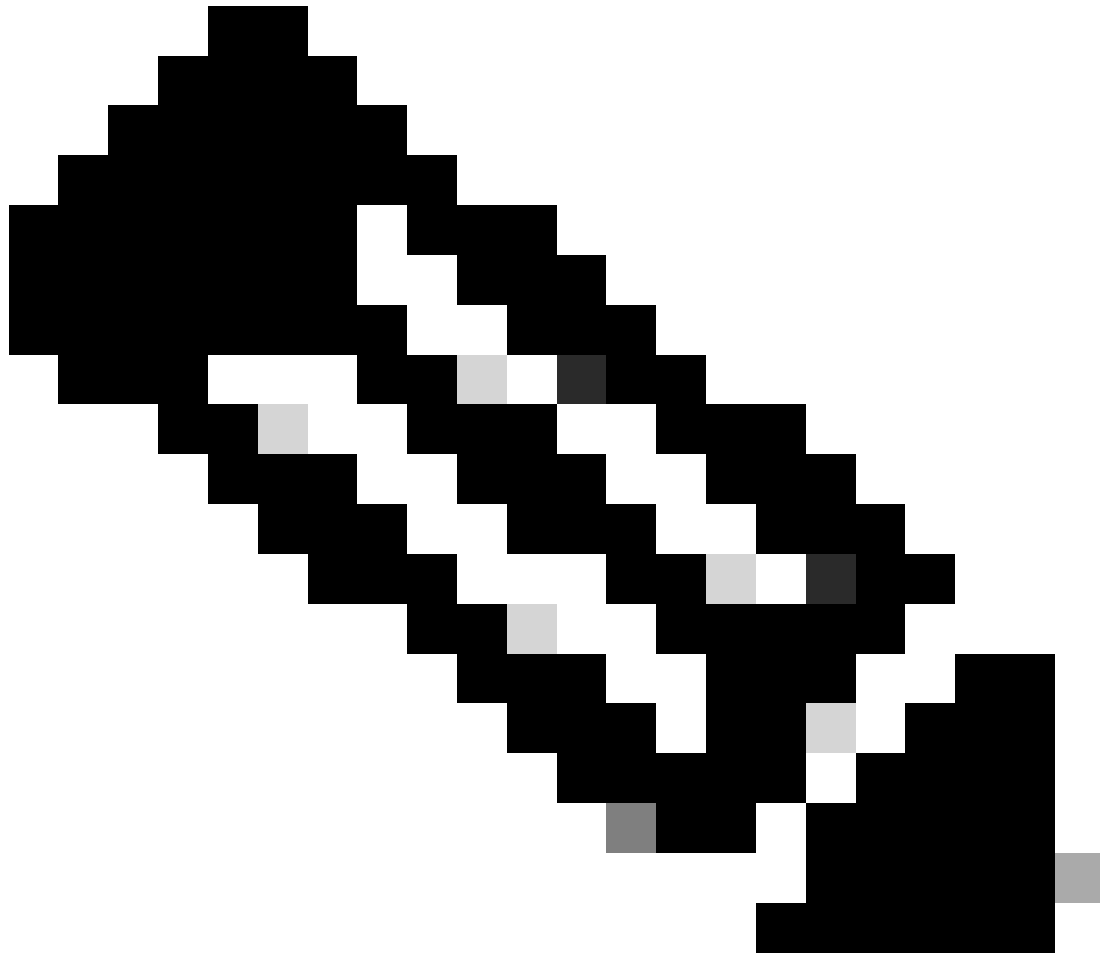
Wanneer Toepassingszichtbaarheid is vastgesteld, kunnen gebruikers besturingsregels maken met controlemechanismen voor clients door Quality of Service (QoS) te configureren.



Werkmechanisme van AVC

Netwerkgebaseerde toepassingsherkenning (NBAR)

NBAR is een mechanisme dat is geïntegreerd in de 9800 WLC, die wordt gebruikt om DPI uit te voeren voor het identificeren en classificeren van een grote verscheidenheid aan toepassingen die over een netwerk lopen. Het kan een groot aantal toepassingen herkennen en classificeren, inclusief versleutelde en dynamisch poorttoegewezen toepassingen, die vaak niet zichtbaar zijn voor traditionele pakketinspectietechnologieën.



Opmerking: om NBAR op de Catalyst 9800 WLC te kunnen gebruiken, is het nodig om deze correct in te schakelen en te configureren, vaak in combinatie met specifieke AVC-profielen die de juiste acties definiëren die moeten worden ondernomen op basis van de classificatie van het verkeer.

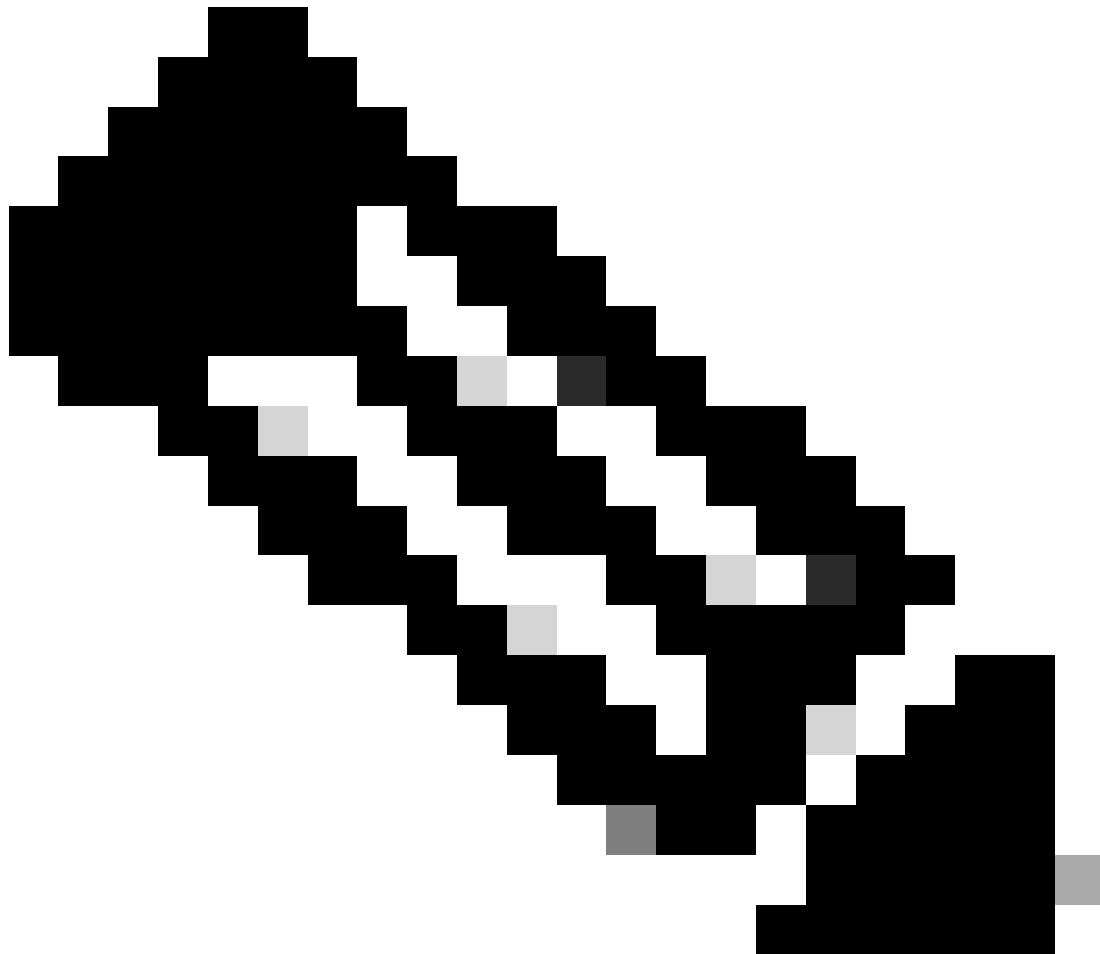
NBAR blijft periodiek worden bijgewerkt, en het is belangrijk om de software WLC bijgewerkt te houden om ervoor te zorgen dat de NBAR functieset huidig en effectief blijft.

Een volledige lijst van de protocollen die in de laatste releases worden ondersteund, is te vinden op https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

NBAR-protocol inzake beleidsprofiel inschakelen

```
9800WLC#configure terminal
9800WLC(config)#wireless profile policy AVC_testing
9800WLC(config-wireless-policy)#ip nbar protocol-discovery
```

```
9800WLC(config-wireless-policy)#end
```



Opmerking: % beleidsprofiel moet worden uitgeschakeld voordat deze handeling wordt uitgevoerd.

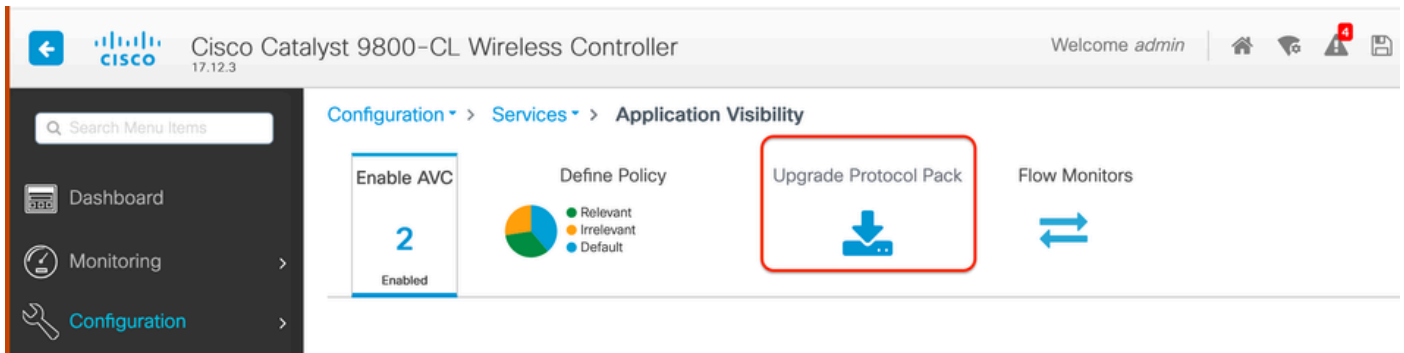
```
9800WLC#show wireless profile policy detailed AVC_testing | in NBAR  
NBAR Protocol Discovery : Enabled
```

NBAR upgraden op 9800 WLC

De 9800 WLC heeft al ~1500 herkenbare applicaties. In het geval dat een nieuwe toepassing wordt uitgebracht, wordt het protocol voor dezelfde toepassing bijgewerkt in de laatste NBAR die gedownload zou moeten worden van de Software Download pagina voor het specifieke model 9800.

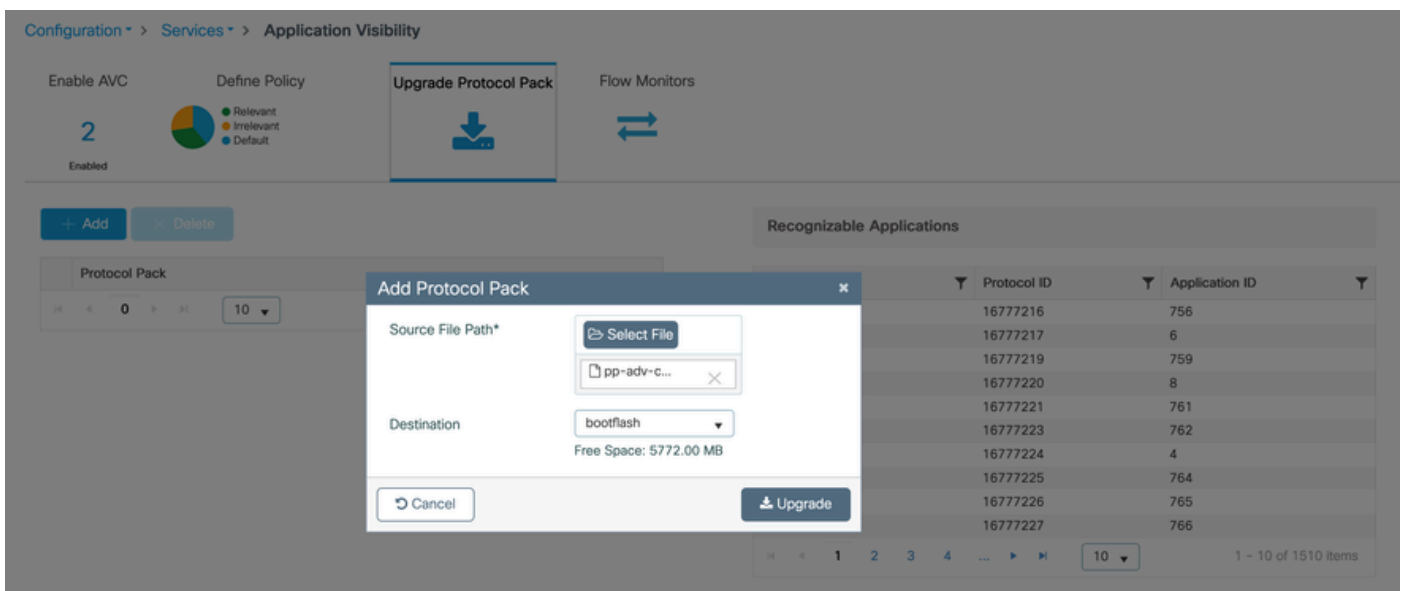
Via GUI

Ga naar Configuration > Services > Application Visibility. Klik op Upgradeprotocolpakket .



Sectie met uploadprotocol in 9800 WLC

Klik op Add, kies vervolgens het protocolpakket dat moet worden gedownload en klik op Upgrade .



NBAR-protocol toevoegen

Zodra de upgrade is uitgevoerd, wordt het protocolpakket toegevoegd.

Enable AVC 2 Enabled

Define Policy

- Relevant
- Irrelevant
- Default

Upgrade Protocol Pack

Flow Monitors

+ Add × Delete

Protocol Pack
<input type="checkbox"/> bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack

1 10 1 - 1 of 1 items

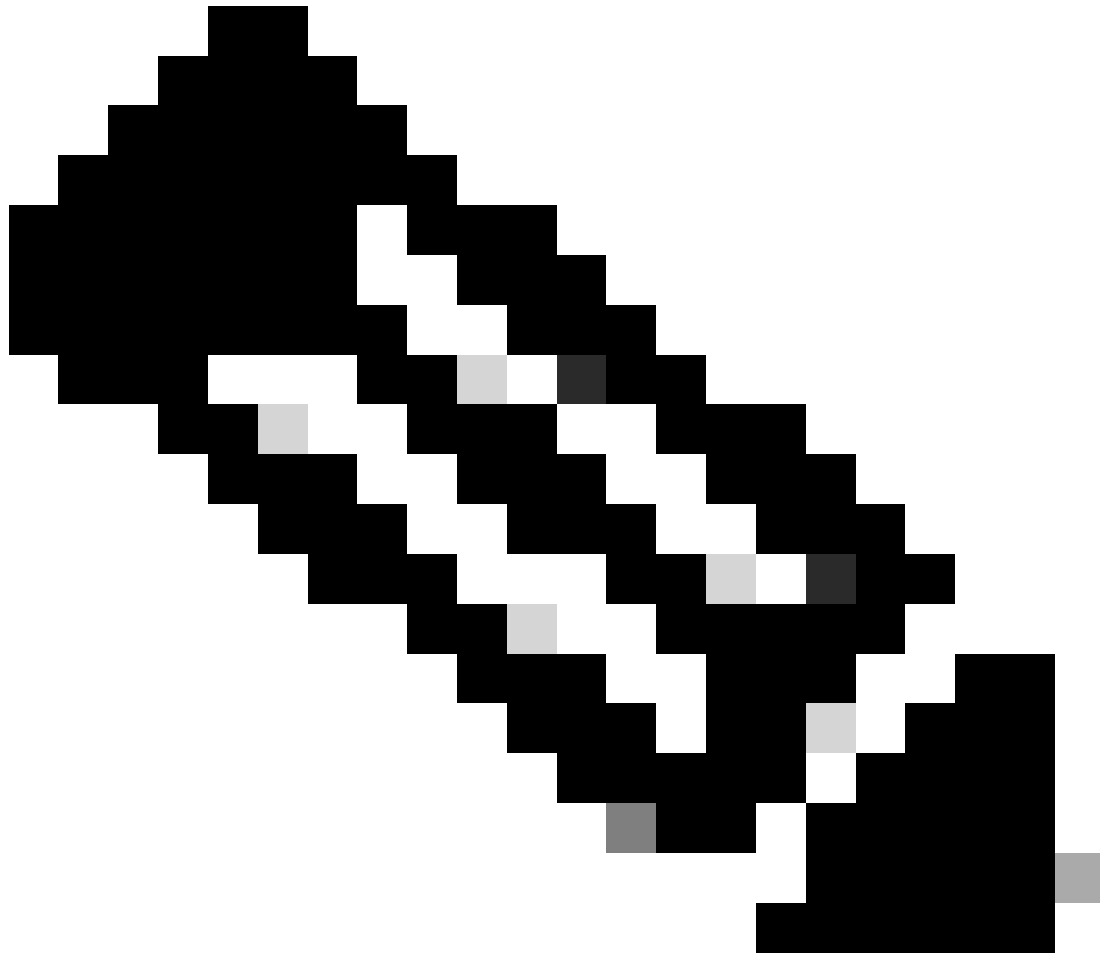
Verificatie van protocolpakket

Via CLI

```
9800WLC#copy tftp://10.10.10.1/pp-adv-c9800-1712.1-49-70.0.0.pack bootflash:
9800WLC#configure terminal
9800WLC(config)#ip nbar protocol-pack bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack
```

To verify NBAR protocol pack version

```
9800WLC#show ip nbar protocol-pack active
Active Protocol Pack:
Name: Advanced Protocol Pack
Version: 70.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 49
Creation time: Tue Jun 4 10:18:09 UTC 2024
File: bootflash:pp-adv-c9800-1712.1-49-70.0.0.pack
State: Active
```



Opmerking: tijdens de upgrade van NBAR-protocolpakket wordt de service niet verstoord.

NetFlow

NetFlow is een netwerkprotocol dat wordt gebruikt voor het verzamelen van IP-verkeersinformatie en het bewaken van netwerkstroomgegevens. Het wordt voornamelijk gebruikt voor netwerkverkeersanalyse en bandbreedtebewaking. Hier is een overzicht van hoe NetFlow werkt op de Cisco Catalyst 9800 Series controllers:

- Gegevensverzameling: 9800 WLC verzamelt gegevens over IP-verkeer dat door hen stroomt. Deze gegevens omvatten informatie zoals bron en bestemming IP adressen, bron en bestemmingshavens, gebruikte protocollen, klasse van de dienst, en de oorzaak van stroombeëindiging.
- Flow Records: De verzamelde gegevens worden georganiseerd in flow records. Een stroom wordt gedefinieerd als een unidirectionele opeenvolging van pakketten die een reeks gemeenschappelijke eigenschappen delen, zoals de zelfde bron/bestemming IP,

bron/bestemmingshavens, en protocoltype.

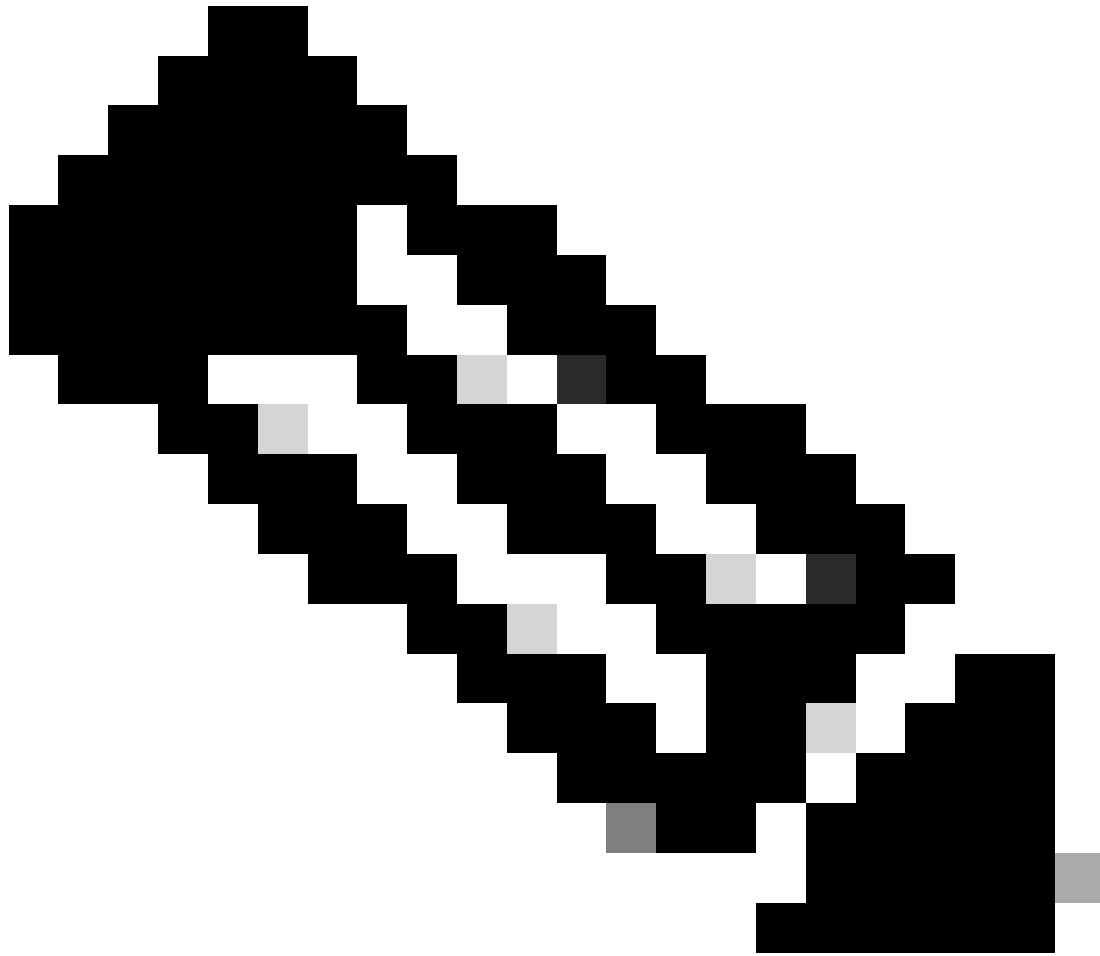
- Gegevens exporteren: De stroomrecords worden periodiek van het NetFlow-enabled apparaat geëxporteerd naar een NetFlow Collector. De collector kan lokale WLC zijn of een speciale server of softwaretoepassing die de stroomgegevens ontvangt, opslaat en verwerkt.
- Analyse: U kunt NetFlow-verzamelaars en analysetools gebruiken om verkeerspatronen te visualiseren, bandbreedte te identificeren, ongebruikelijke verkeersstromen te detecteren die duiden op veiligheidsbreuken, netwerkprestaties te optimaliseren en netwerkuitbreiding te plannen.
- Draadloze specifieke informatie: In de context van draadloze controllers kan NetFlow aanvullende informatie bevatten die specifiek is voor draadloze netwerken, zoals de SSID, AP-namen, client-MAC-adressen en andere details die relevant zijn voor Wi-Fi verkeer.

Flexibele NetFlow

Flexibele NetFlow (FNF) is een geavanceerde versie van traditionele NetFlow, en wordt ondersteund door Cisco Catalyst 9800 Series draadloze LAN-controllers (WLC's). Het verstrekt meer aanpassingsopties om, netwerkverkeerspatronen te volgen te controleren en te analyseren. De belangrijkste functies van Flexible NetFlow op Catalyst 9800 WLC zijn:

- Aanpassing: FNF stelt gebruikers in staat om te bepalen welke informatie ze willen verzamelen van het netwerkverkeer. Dit omvat een brede reeks verkeerskenmerken zoals IP-adressen, poortnummers, tijdstempels, pakket- en bytellingen, toepassingstypen en meer.
- Verbeterde zichtbaarheid: Door gebruik te maken van FNF, verkrijgen beheerders een gedetailleerd inzicht in de soorten verkeer die door het netwerk stromen, wat essentieel is voor capaciteitsplanning, op gebruik gebaseerde netwerkfacturering, netwerkanalyse en beveiligingsbewaking.
- Protocolafhankelijkheid: FNF is flexibel genoeg om verschillende protocollen buiten IP te ondersteunen, waardoor het aanpasbaar is aan verschillende soorten netwerkomgevingen.

Op de Catalyst 9800 WLC kan FNF worden geconfigureerd om stroomrecords te exporteren naar een externe NetFlow Collector of analysetoepassing. Deze gegevens kunnen vervolgens worden gebruikt voor probleemoplossing, netwerkplanning en beveiligingsanalyse. De FNF-configuratie omvat het definiëren van een flow record (wat te verzamelen), een flow exporteur (waar de gegevens te verzenden) en het toevoegen van de flow monitor (die de record en de exporteur bindt) aan de juiste interfaces.



Opmerking: FNF kan 17 verschillende gegevensrecords (zoals gedefinieerd in RFC 3954) verzenden naar externe NetFlow Collector van derden, zoals Stealthwatch, Solarwinds en anderen die zijn: Application Tag, client Mac-adres, AP Mac-adres, WLANid, source IP, bestemming IP, bronpoort, bestemmingshaven, protocol, Flow Start Time, Flow End Time, directie, Packet out, byte count, VLAN ID (Local Mode) - Mgmt/client en TOS - DSCP Value

Flow Monitor

Een flowmonitor is een component die in combinatie met Flexible NetFlow (FNF) wordt gebruikt om netwerkverkeersgegevens op te nemen en te analyseren. Het speelt een cruciale rol in de bewaking en het begrip van verkeerspatronen voor netwerkbeheer, beveiliging en probleemoplossing. De flowmonitor is in wezen een toegepast exemplaar van FNF dat stroomgegevens verzamelt en bijhoudt op basis van gedefinieerde criteria. Het is verbonden met drie hoofdelementen:

- Flow Record: Dit definieert de gegevens die de Flow Monitor moet verzamelen van het netwerkverkeer. Het specificeert de sleutels (zoals bron en bestemming IP adressen,

poorten, protocoltypes) en niet-zeer belangrijke velden (zoals pakket en byte tellers, tijdstempels) die in de stroomgegevens zullen worden omvat.

- Flow Exporteur: Dit specificeert de bestemming waar de verzamelde stroomgegevens moeten worden verzonden. Het bevat details zoals het IP-adres van de NetFlow Collector, het transportprotocol (gewoonlijk UDP) en het bestemmingshaven nummer waar de collector luistert.
- Flow Monitor: De flow monitor zelf bindt de flow record en flow exporteur samen en past ze toe op een interface of WLAN om het monitoringproces daadwerkelijk te starten. Hij bepaalt hoe de stroomgegevens moeten worden verzameld en geëxporteerd op basis van de criteria die zijn vastgesteld in het stroomverslag en de bestemming die in de stroomexporteur is ingesteld.

AVC-ondersteunde access points

AVC wordt alleen ondersteund op deze access points:

- Cisco Catalyst 9100 Series access points
- Cisco Aironet 2800 Series access point
- Cisco Aironet 3800 Series access points
- Cisco Aironet 4800 Series access points

Ondersteuning voor verschillende 9800 implementatiemodi

Implementatiemodus	9800 WLC	Wave 1 access point	Wave 2 access point	WiFi 6 access point
Lokale modus (Central-switching)	IPV4-verkeer: AVC-ondersteunde producten FNF-ondersteunde producten IPV6-verkeer: AVC-ondersteunde producten FNF-ondersteunde producten	Verwerking op WLC-niveau	Verwerking op WLC-niveau	Verwerking op WLC-niveau
Flex-modus	IPV4-verkeer:	Verwerking	Verwerking	Verwerking

(Central-switching)	AVC- ondersteunde producten FNF- ondersteunde producten IPV6-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten	op WLC- niveau	op WLC- niveau	op WLC- niveau
Flex-modus (Lokale switching)	Verwerking op AP-niveau	IPV4-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten IPV6-verkeer: AVC- ondersteunde producten FNF niet ondersteund	IPV4-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten IPV6-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten	IPV4-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten IPV6-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten
Lokale modus (Materiaal)	Verwerking op AP-niveau	IPV4-verkeer: AVC niet ondersteund FNF niet ondersteund IPV6-verkeer: AVC niet ondersteund FNF niet ondersteund	IPV4-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten IPV6-verkeer: AVC- ondersteunde producten FNF- ondersteunde	IPV4-verkeer: AVC- ondersteunde producten FNF- ondersteunde producten IPV6-verkeer: AVC- ondersteunde producten FNF- ondersteunde

			producten	producten
--	--	--	-----------	-----------

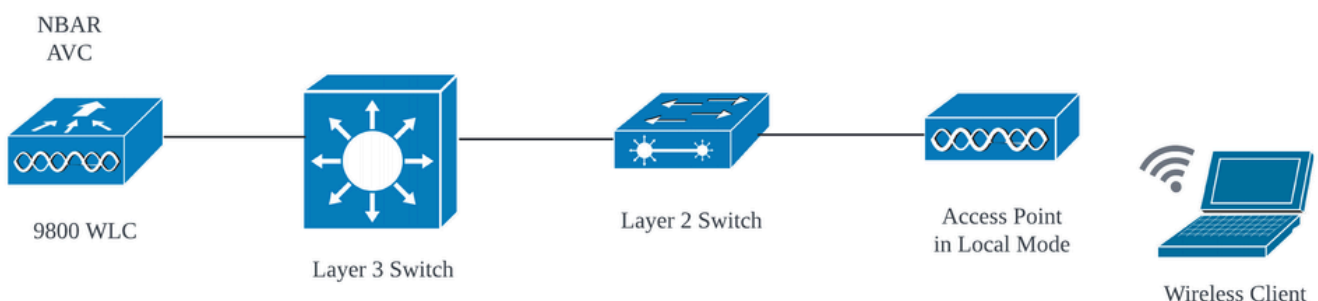
Beperkingen bij implementatie van AVC op 9800

Zowel Application Visibility and Control (AVC) als Flexible NetFlow (FNF) zijn krachtige functies op Cisco Catalyst 9800 Series draadloze LAN-controllers die de zichtbaarheid en controle van het netwerk verbeteren. Er zijn echter beperkingen en overwegingen die u in gedachten moet houden bij het gebruik van deze functies:

- Layer 2 roaming wordt niet ondersteund op meerdere controllers.
- Multicastverkeer wordt niet ondersteund.
- Alleen de toepassingen die met App-zichtbaarheid worden herkend, kunnen worden gebruikt voor het toepassen van QoS-besturing.
- Data link wordt niet ondersteund voor NetFlow-velden in AVC.
- U kunt hetzelfde WLAN-profiel niet toewijzen aan zowel het AVC-not-enabled-beleidsprofiel als het AVC-enabled-beleidsprofiel.
- U kunt het beleidsprofiel met ander switchingmechanisme niet gebruiken om hetzelfde WLAN te gebruiken om AVC te implementeren.
- AVC wordt niet ondersteund op de beheerpoort (Gig 0/0).
- Op NBAR gebaseerde QoS-beleidsconfiguratie is alleen toegestaan op bekabelde fysieke poorten. Beleidsconfiguratie wordt niet ondersteund op virtuele interfaces, bijvoorbeeld VLAN, poortkanaal en andere logische interfaces.
- Als AVC is ingeschakeld, ondersteunt het AVC-profiel alleen maximaal 23 regels, inclusief de standaard DSCP-regel. Het AVC-beleid wordt niet naar de AP geduwd, als de regels meer dan 23 zijn.

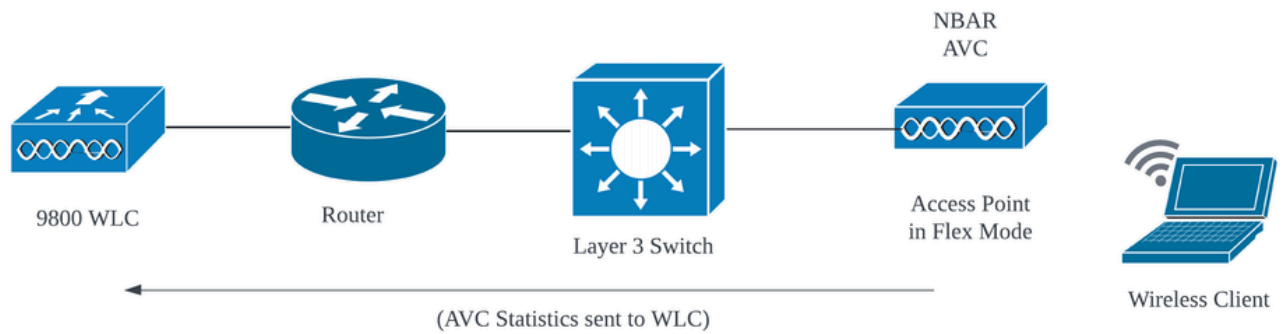
Netwerktopologie

AP in lokale modus



AVC in lokale modus AP (centrale switching)

AP in flex modus



AVC in Flex Mode AP

Configuratie van AVC op 9800 WLC

Tijdens het configureren van AVC op 9800 WLC, kunt u het gebruiken als NetFlow Collector of de NetFlow-gegevens exporteren naar Externe NetFlow Collector.

Lokale exporteur

Op een Cisco Catalyst 9800 draadloze LAN-controller (WLC) verwijst een lokale NetFlow-collector naar de ingesloten functie binnen de WLC waarmee NetFlow-gegevens kunnen worden verzameld en lokaal opgeslagen. Deze mogelijkheid stelt de WLC in staat om basisNetFlow-gegevensanalyse uit te voeren zonder de noodzaak om de stroomrecords naar een externe NetFlow-collector te exporteren.

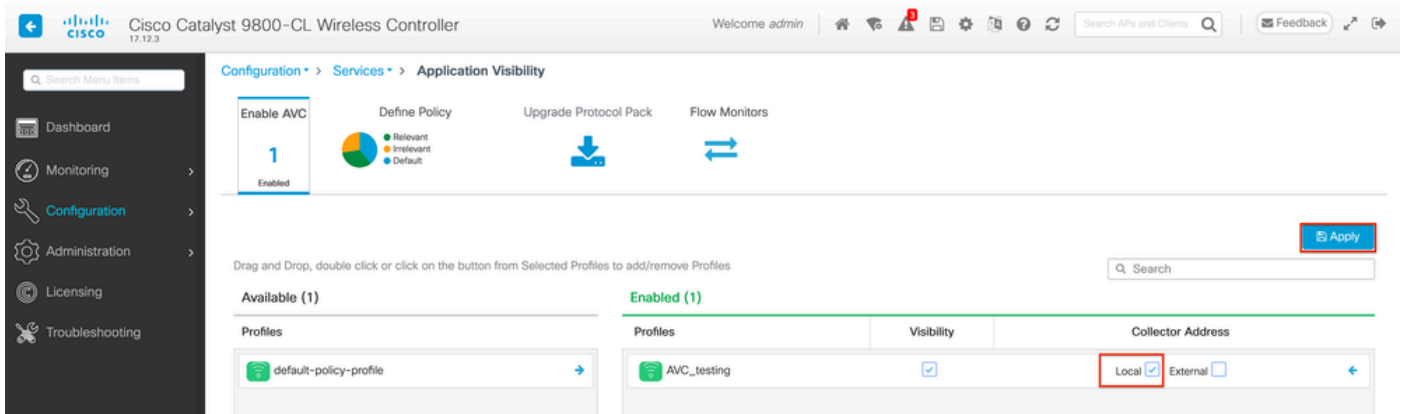
Via GUI

Stap 1: Om AVC op specifieke SSID in te schakelen, gaat u naar Configuration > Services > Application Visibility. Kies het specifieke beleidsprofiel waarvoor u AVC wilt activeren.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is 'Configuration > Services > Application Visibility'. The 'Enable AVC' section shows '1' and 'Enabled'. Below this, there are sections for 'Available (2)' and 'Enabled (0)'. The 'Available' section contains two profiles: 'AVC_testing' and 'default-policy-profile'. A red box highlights the right-pointing arrow next to the 'AVC_testing' profile. The 'Enabled' section is currently empty.

AVC inschakelen op beleidsprofiel

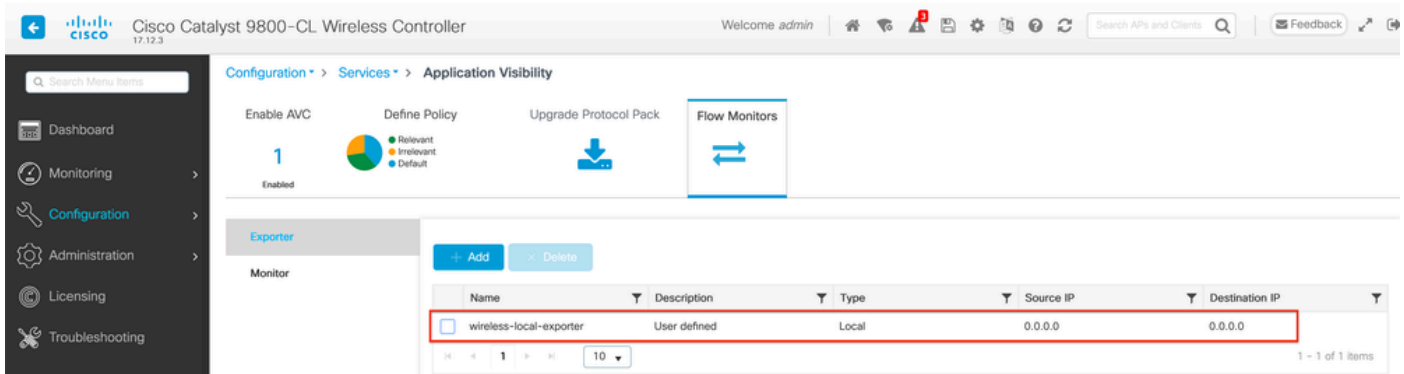
Stap 2: Selecteer Lokaal als NetFlow Collector en klik op Toepassen.



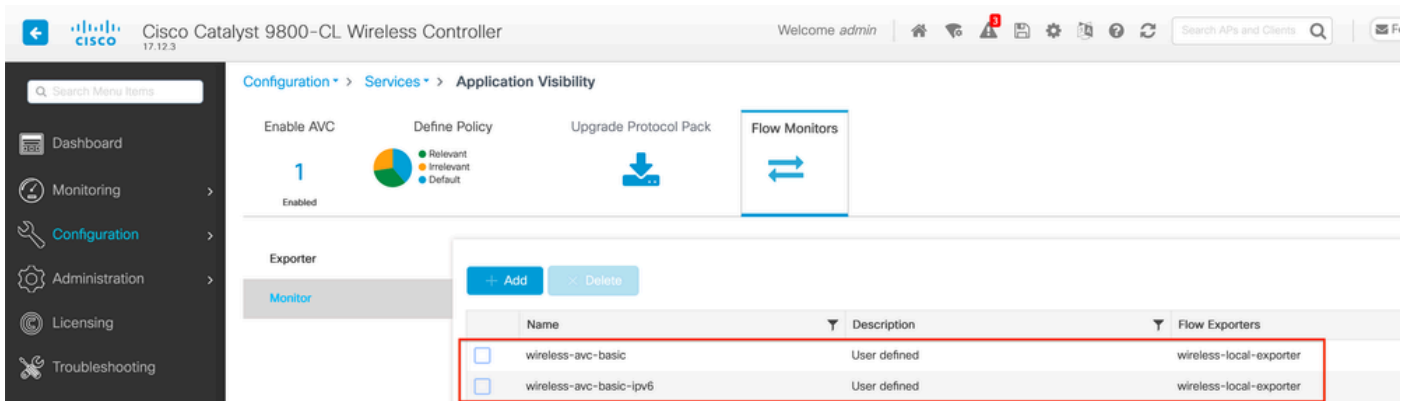
Lokale NetFlow Collector selecteren

Merk op dat de NetFlow Exporteur en NetFlow instellingen automatisch zijn geconfigureerd volgens de opgegeven voorkeuren zodra u de AVC-configuratie toepast.

U kunt het zelfde bevestigen door aan Configuratie > de Diensten > Toepassingszichtbaarheid > Flow Monitor > Exporter/Monitor te navigeren.

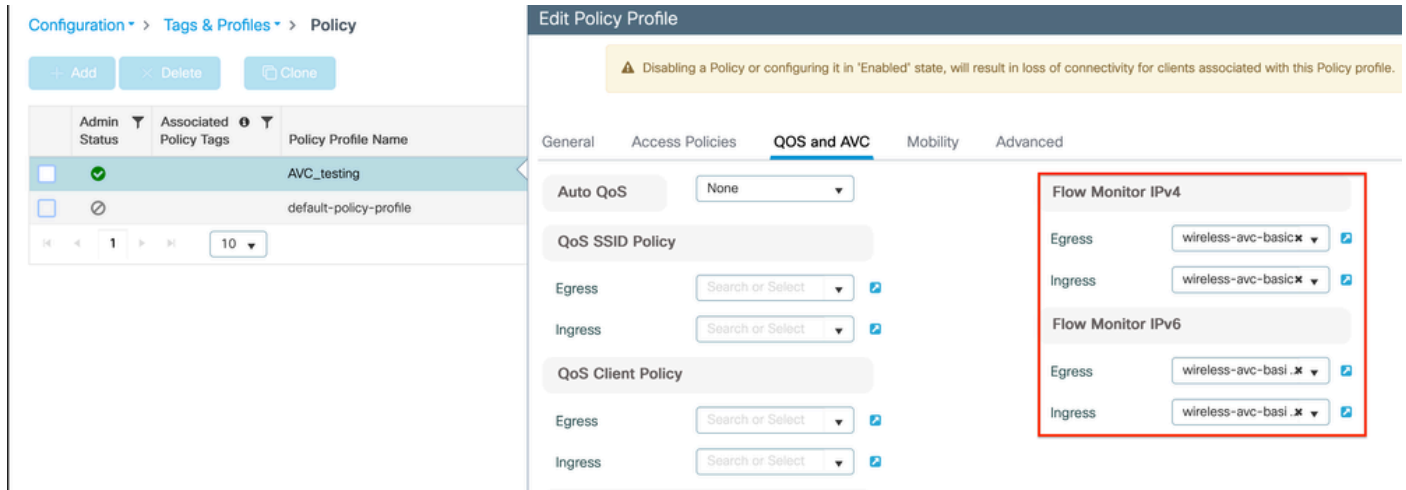


Local Flow Collector Configuration op 9800 WLC



Flow Monitor Configuration met Local NetFlow Collector

De IPv4- en IPv6 AVC Flow Monitors worden automatisch gekoppeld aan het beleidsprofiel. Navigeren naar Configuratie > Tags en profiel > Beleid . Klik op Beleidsprofiel > AVC en QOS.



Configuratie Flow Monitor in beleidsprofiel

Via CLI

Stap 1: Configureer 9800 WLC als lokale exporteur.

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter wireless-local-exporter
9800-C1-VM(config-flow-exporter)#destination local wlc
9800-C1-VM(config-flow-exporter)#exit
```

Stap 2: IPv4 en IPv6 Network Flow Monitor configureren om Local (WLC) te gebruiken als NetFlow Exporteur.

```
9800-C1-VM(config)#flow monitor wireless-avc-basic
9800-C1-VM(config-flow-monitor)#exporter wireless-local-exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor wireless-avc-basic-ipv6
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exit
```

Stap 3: Breng de IPv4 en IPv6 Flow Monitor in beleidsprofiel in kaart voor zowel toegang als uitgaand verkeer.

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin


```
9800-CL-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-CL-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
9800-CL-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 input
9800-CL-VM(config-wireless-policy)#ipv6 flow monitor wireless-avc-basic-ipv6 output
9800-CL-VM(config-wireless-policy)#no shutdown
9800-CL-VM(config-wireless-policy)#exit
```

Externe NetFlow Collector

Een externe NetFlow Collector, wanneer gebruikt in de context van Application Visibility and Control (AVC) op een Cisco Catalyst 9800 draadloze LAN-controller (WLC), is een speciaal systeem of service die NetFlow-gegevens ontvangt, aggregereert en analyseert die uit de WLC zijn geëxporteerd. U kunt ofwel alleen externe NetFlow Collector configureren om de zichtbaarheid van de toepassing te bewaken, ofwel u kunt deze ook gebruiken samen met Local Collector.

Via GUI

Stap 1: Om AVC op specifieke SSID in te schakelen, gaat u naar Configuration > Services > Application Visibility. Kies het specifieke beleidsprofiel waarvoor u AVC wilt activeren. Selecteer Collector als Extern en configureer het IP-adres van NetFlow Collector zoals Cisco Prime, SolarWind, StealthWatch en klik op Toepassen.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is Configuration > Services > Application Visibility. The 'Enable AVC' step is marked as 'Enabled'. Below this, there are sections for 'Available (1)' and 'Enabled (1)'. The 'Enabled (1)' section contains a table with the following data:

Profiles	Visibility	Collector Address
AVC_testing	<input checked="" type="checkbox"/>	Local <input checked="" type="checkbox"/> External <input checked="" type="checkbox"/> 10.106.36.22

AVC-configuratie voor externe NetFlow Collector

Merk op dat, zodra u de AVC-configuratie toepast, de NetFlow Exporter- en NetFlow-instellingen automatisch zijn geconfigureerd met het NetFlow Collector IP-adres als exporteur- en Exporter-adres als 9800 WLC met standaardinstellingen voor time-out en UDP-poort 9995. U kunt het zelfde bevestigen door aan Configuratie > de Diensten > Toepassingszichtbaarheid > Flow Monitor > Exporter/Monitor te navigeren.

Configuration > Services > Application Visibility

Enable AVC: 1 Enabled

Define Policy: Relevant, Irrelevant, Default

Upgrade Protocol Pack

Flow Monitors

Name	Description	Type	Source IP	Destination IP
export_-1638039067	User defined	External	10.197.234.75	10.106.36.22

Externe NetFlow Collector-configuratie op 9800 WLC

Configuration > Services > Application Visibility

Enable AVC: 1 Enabled

Define Policy: Relevant, Irrelevant, Default

Upgrade Protocol Pack

Flow Monitors

Exporter: Monitor

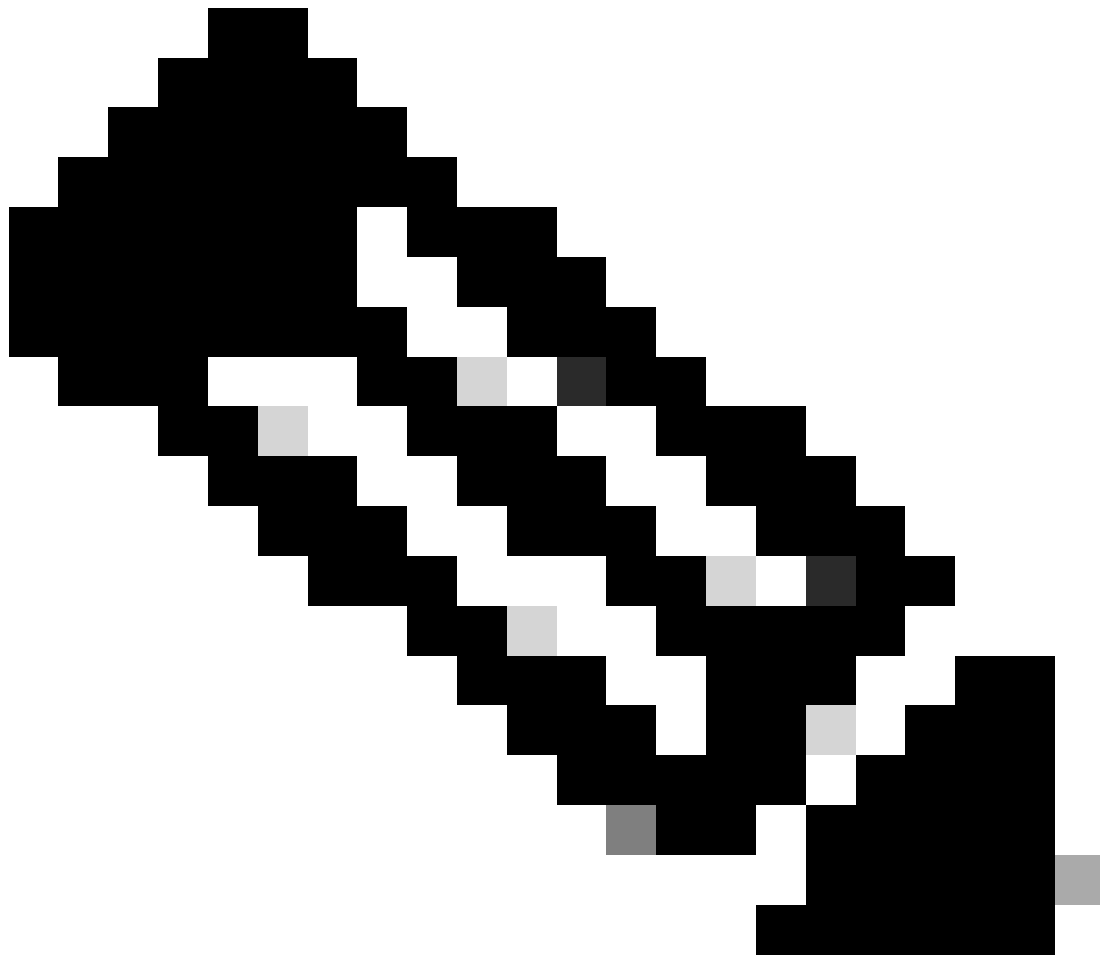
Name	Description	Flow Exporters
dwavc_-1638039067	User defined	export_-1638039067
dwavc_ipv6_-1638039067	User defined	export_-1638039067

Flow Monitor Configuration met externe NetFlow Collector

U kunt de poortconfiguratie van automatisch gegenereerde NetFlow Monitor controleren door te navigeren naar Configuration > Services > NetFlow .

Configuration > Services > NetFlow

Netflow Template	Interfaces/Profiles	Collector	Export Interface IP	Sampling Method	Sampling Range/ACL Name	Exporter Port
Wireless avc basic	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995
Wireless avc basic IPv6	AVC_testing	10.106.36.22	10.197.234.75	NA	NA	9995



Opmerking: als u AVC via GUI configureert, wordt de automatisch gegenereerde NetFlow Exporter geconfigureerd om UDP 995-poort te gebruiken. Zorg ervoor dat u het poortnummer valideert dat door uw NetFlow-collector wordt gebruikt.

Bijvoorbeeld: Als u Cisco Prime gebruikt als uw NetFlow Collector, is het essentieel om de Exporter-poort in te stellen op 9991, omdat dit de poort is waarop Cisco Prime op NetFlow-verkeer luistert. U kunt de Exporterpoort handmatig wijzigen in NetFlow Configuration.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The main navigation menu on the left includes Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main content area displays the 'Configuration > Services > NetFlow' section. A table lists NetFlow Templates:

NetFlow Template	Interfaces/Profiles	Collector	Export Inte
Wireless avc basic	Not Assigned	10.106.36.22	10.197.23
Wireless avc basic IPv6	Not Assigned	10.106.36.22	10.197.234
Wireless avc basic	AVC_testing		10.197.234
Wireless avc basic IPv6	AVC_testing		10.197.234

The 'Edit NetFlow' dialog is open, showing the following configuration:

- Netflow Template: Wireless avc basic
- Local Exporter:
- External Exporter:
- Collector Address*: 10.106.36.22
- Exporter Port*: 9991
- Available (1): Search
- Profiles: default-policy-profile
- Profiles: AVC_testing (Ingress: , Egress:)

A tooltip for the 'Exporter Port*' field states: 'Enter the port number on which your netflow collector configured above is listening.'

Poortnummer van exporteur in NetFlow-configuratie wijzigen

Via CLI

Stap 1: Configureer het IP-adres van de externe NetFlow Collector met de broninterface.

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter External_Exporter
9800-C1-VM(config-flow-exporter)#destination 10.106.36.22
9800-C1-VM(config-flow-exporter)#source $Source_Interface
9800-C1-VM(config-flow-exporter)#transport udp $Port_Numbet
9800-C1-VM(config-flow-exporter)#exit
```

Stap 2: IPv4 en IPv6 Network Flow Monitor configureren om Local (WLC) te gebruiken als NetFlow Exporteur.

```
9800-C1-VM(config)#flow monitor wireless-avc-basic
9800-C1-VM(config-flow-monitor)#exporter External_Exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 basic
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exporter External_Exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 basic
9800-C1-VM(config-flow-monitor)#exit
```

Stap 3: Breng de IPv4 en IPv6 Flow Monitor in beleidsprofiel in kaart voor zowel toegang als uitgaand verkeer.

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor wireless-avc-basic output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor wireless avc ipv6 basic output
9800-C1-VM(config-wireless-policy)#no shutdown
9800-C1-VM(config-wireless-policy)#exit
```

Configuratie van AVC op 9800 WLC met Cisco Catalyst Center

Alvorens te werk te gaan met de configuratie van Application Visibility and Control (AVC) op een Cisco Catalyst 9800 draadloze LAN-controller (WLC) via Cisco Catalyst Center, is het belangrijk om te verifiëren dat de telemetriecommunicatie tussen WLC en Cisco Catalyst Center met succes is tot stand gebracht. Zorg ervoor dat de WLC wordt weergegeven in een beheerde staat binnen de Cisco Catalyst Center-interface en dat de gezondheidsstatus actief wordt bijgewerkt. Bovendien is het voor een effectieve bewaking van de status van de gezondheid belangrijk om zowel de WLC als de Access points (AP's) op de juiste manier toe te wijzen aan hun respectievelijke locaties binnen Cisco Catalyst Center.

```
9800WLC#show telemetry connection all
Telemetry connections
```

Index	Peer Address	Port	VRF	Source Address	State	State Description
170	10.78.8.84	25103	0	10.105.193.156	Active	Connection up

Verificatie van telemetrieverbinding op 9800 WLC

The screenshot shows the 'Devices (5)' page in Cisco Catalyst Center. The 'Focus' is set to 'Inventory'. A search bar is present with the text 'Click here to apply basic or advanced filters or view recently applied filters'. Below the search bar, there are action buttons: '0 Selected', 'Tag', '+ Add Device', 'Edit Device', 'Delete Device', 'Actions', and an information icon. The main table lists three devices:

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability
	9800WLC.cisco.com	10.105.193.156	Cisco	Reachable	Not Scanned	Managed
	CW9164I-ROW1	10.105.193.152	NA	Reachable	Not Scanned	Managed
	CW9164I-ROW2	10.105.60.35	NA	Reachable	Not Scanned	Managed

The 'Manageability' column is highlighted with a red box, showing that all three devices are in a 'Managed' state.

WLC en AP zijn in beheerde staat

Network Devices

LATEST **67%** Healthy TOTAL: 3

No Devices



Router

No Devices



Core

No Devices



Distribution

No Devices



Access



1/1



Wireless Controller

1/2



Access Point

40%

7:30p

7:30p

[View Network Health](#)

Gezondheidsstatus van WLC en AP op Cisco Catalyst Center

Stap 1: Configureer Cisco Catalyst Center als NetFlow Collector en schakel draadloze telemetrie in de wereldwijde instelling in. Navigeer naar Design > Network Setting > Telemetry en schakel de gewenste configuratie in zoals aangegeven op de afbeelding.

Catalyst Center Design / Network Settings

Servers Device Credentials IP Address Pools Wireless **Telemetry** Security and Trust

Find Hierarchy Search Help

- Global
 - BGL TAC

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

Catalyst Center is your default SNMP collector. It polls network devices to gather telemetry data. [View details](#) on the metrics gathered and the frequency with which they are collected.

Application Visibility

Enable Netflow Application Telemetry and Controller Based Application Recognition (CBAR) by default upon network device site assignment ⓘ

Enable by default on supported wired access devices

Choose the destination collector for Netflow records sent from network devices.

Use Catalyst Center as the Netflow Collector

Use Cisco Telemetry Broker (CTB) or UDP director

Wired Endpoint Data Collection

The primary function of this feature is to track the presence, location, and movement of wired endpoints in the network. Traffic received from endpoints is used to extract and store their identity information (MAC address and IP address). Other features, such as IEEE 802.1X, web authentication, Cisco Security Groups (formerly TrustSec), SD-Access, and Assurance, depend on this identity information to operate properly.

Wired Endpoint Data Collection enables Device Tracking policies on devices assigned to the Access role in Inventory.

Enable Catalyst Center Wired Endpoint Data Collection At This Site

Disable Catalyst Center Wired Endpoint Data Collection At This Site ⓘ

Wireless Controller, Access Point and Wireless Clients Health

Enables Streaming Telemetry on your wireless controllers in order to determine the health of your wireless controller, access points and wireless clients.

Enable Wireless Telemetry

Configuratie draadloze telemetrie en AVC

Stap 2: Toepassingstelemetrie inschakelen op de gewenste 9800 WLC om de AVC-configuratie op 9800 WLC te drukken. Hiervoor navigeer je naar Provision > Network Device > Inventory. Kies de 9800 WLC waarop u Application Telemetry wilt activeren en navigeer vervolgens naar Action > Telemetry > Enable Application Telemetry .

Catalyst Center Provision / Inventory

Global

All Routers Switches Wireless Controllers Access Points Sensors

DEVICE WORK ITEMS

- Unreachable
- Unassigned
- Untagged
- Failed Provision
- Non Compliant
- Outdated Software Image
- No Golden Image
- Failed Image Prechecks
- Under Maintenance
- Security Advisories

Devices (5) Focus: Inventory

Click here to apply basic or advanced filters or view recently applied filters

1 Selected Tag Add Device Edit Device Delete Device Actions ⓘ

Tags	Device Name	IP Address	Inventory	EoX Status	Manageability
<input checked="" type="checkbox"/>	9800WLC.cisco.com	10.105.193.156	Inventory >	Not Scanned	Managed
<input type="checkbox"/>	CW9164I-ROW1	10.105.193.152	Software Image >		
<input type="checkbox"/>	CW9164I-ROW2	10.105.60.35	Provision >		
<input type="checkbox"/>	SDA_WLC.cisco.com	10.106.38.185	Telemetry >		
			Device Replacement >		
			Compliance >		
			More >		

Enable Application Telemetry

Disable Application Telemetry

Update Telemetry Settings

Toepassingstelemetrie inschakelen op 9800 WLC

Stap 3: Kies de implementatiemodus volgens de vereisten.

Lokaal: AVC inschakelen in profiel voor lokaal beleid (centrale switching)

Flex/Fabric: AVC inschakelen in Flex Policy Profile (Local Switching) of op Fabric gebaseerde SSID.

Enable Application Telemetry

You have chosen to enable Netflow with application telemetry on 1 wireless controllers.

By default, all non-guest WLANs on Wireless Controllers will be provisioned to send Netflow with Application telemetry. To override this default behavior, tag specific WLAN profile names with keyword "lan". Once specific WLANs are tagged, only those WLANs will be monitored.

For each wireless controller, select the AP modes where you would like to enable application telemetry.

- For Catalyst 9800 Series Wireless Controllers, the application telemetry source is always Netflow.
- For AireOS wireless controllers, the application telemetry source may be either Netflow or WSA (Wireless Service Assurance).

⚠ Enabling or disabling application telemetry on the selected SSID types will cause a disruption in network services.

⚠ Note: In order to update application telemetry configuration on the WLC, disable application telemetry first and then re-enable it. To do so, please use the Disable/Enable Application Telemetry buttons in the Actions menu.

9800WLC.cisco.com

Local Flex/Fabric

Include Guest SSIDs

ⓘ

Telemetry Source: **NetFlow**

Note: Devices require Catalyst Center Advantage license for this feature to be enabled.

Selectie van implementatiemodus op Cisco Catalyst Center

Stap 4: Het initieert een taak om de AVC-instellingen te activeren, en de bijbehorende configuratie wordt toegepast op de 9800 WLC. U kunt de status bekijken door te navigeren naar Activiteiten > Auditlogboek .

Jul 18, 2024 09:22 PM

3:37p

8/1 9/1 10/1 11/1 12/1 1/1 2/1 3/1 4/1 5/1

Filter

Time	Description
✓ Today	
Jul 18, 2024 20:52 PM (IST)	Compliance run completed for device 10.105.193.156[9800WLC.cisco.com] and compliance status is NON_COMPLIANT
Jul 18, 2024 20:36 PM (IST)	Executing command config t wireless profile policy default-policy-profile no shutdown exit wireless profile policy testpsk no shutdown exit wireless profile policy BGL14-4_WLANID_12 no shutdown exit wireless profile po...
Jul 18, 2024 20:36 PM (IST)	Executing command config t flow exporter avc_exporter destination 10.78.8.84 source Vlan1 transport udp 6007 export-protocol ipfix option vrf-table timeout 300 option ssid-table timeout 300 option application-table tim...
Jul 18, 2024 20:36 PM (IST)	Request received to enable telemetry on device(s) : [10.105.193.156]

Auditlogs na het inschakelen van telemetrie op 9800 WLC

Cisco Catalyst Center implementeert de configuraties van Flow Exporter en Flow Monitor, inclusief de gespecificeerde poort en andere instellingen, en activeert deze binnen het gekozen profiel voor modembeleid zoals hieronder wordt getoond:

Configure Cisco Catalyst Center as Flow Exporter:

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter avc_exporter
9800-C1-VM(config-flow-exporter)#destination 10.104.222.201
9800-C1-VM(config-flow-exporter)#source Vlan10
9800-C1-VM(config-flow-exporter)#transport udp 6007
9800-C1-VM(config-flow-exporter)#export-protocol ipfix
9800-C1-VM(config-flow-exporter)#option vrf-table timeout 300
9800-C1-VM(config-flow-exporter)#option ssid-table timeout 300
9800-C1-VM(config-flow-exporter)#option application-table timeout 300
9800-C1-VM(config-flow-exporter)#option application-attributes timeout 300
9800-C1-VM(config-flow-exporter)#exit
```

Configure 9800 WLC as Local Exporter

```
9800-C1-VM#config t
9800-C1-VM(config)#flow exporter avc_local_exporter
9800-C1-VM(config-flow-exporter)#destination local wlc
9800-C1-VM(config-flow-exporter)#exit
```

Configure Network Flow Monitor to use both Local(WLC) and Cisco Catalyst Center as Netflow Exporter:

```
9800-C1-VM(config)#flow monitor avc_ipv4_assurance
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 assurance
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv6_assurance
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#exporter avc_local_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 assurance
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv4_assurance_rtp
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv4 assurance-rtp
9800-C1-VM(config-flow-monitor)#exit
```

```
9800-C1-VM(config)#flow monitor avc_ipv6_assurance_rtp
```

```
9800-C1-VM(config-flow-monitor)#exporter avc_exporter
9800-C1-VM(config-flow-monitor)#cache timeout active 60
9800-C1-VM(config-flow-monitor)#default cache entries
9800-C1-VM(config-flow-monitor)#record wireless avc ipv6 assurance-rtp
9800-C1-VM(config-flow-monitor)#exit
```

Mapping the IPv4 and IPv6 Flow Monitor in Policy Profile

```
9800-C1-VM(config)#wireless profile policy AVC_Testing
9800-C1-VM(config-wireless-policy)#shutdown
```

Disabling policy profile will result in associated AP/Client rejoin

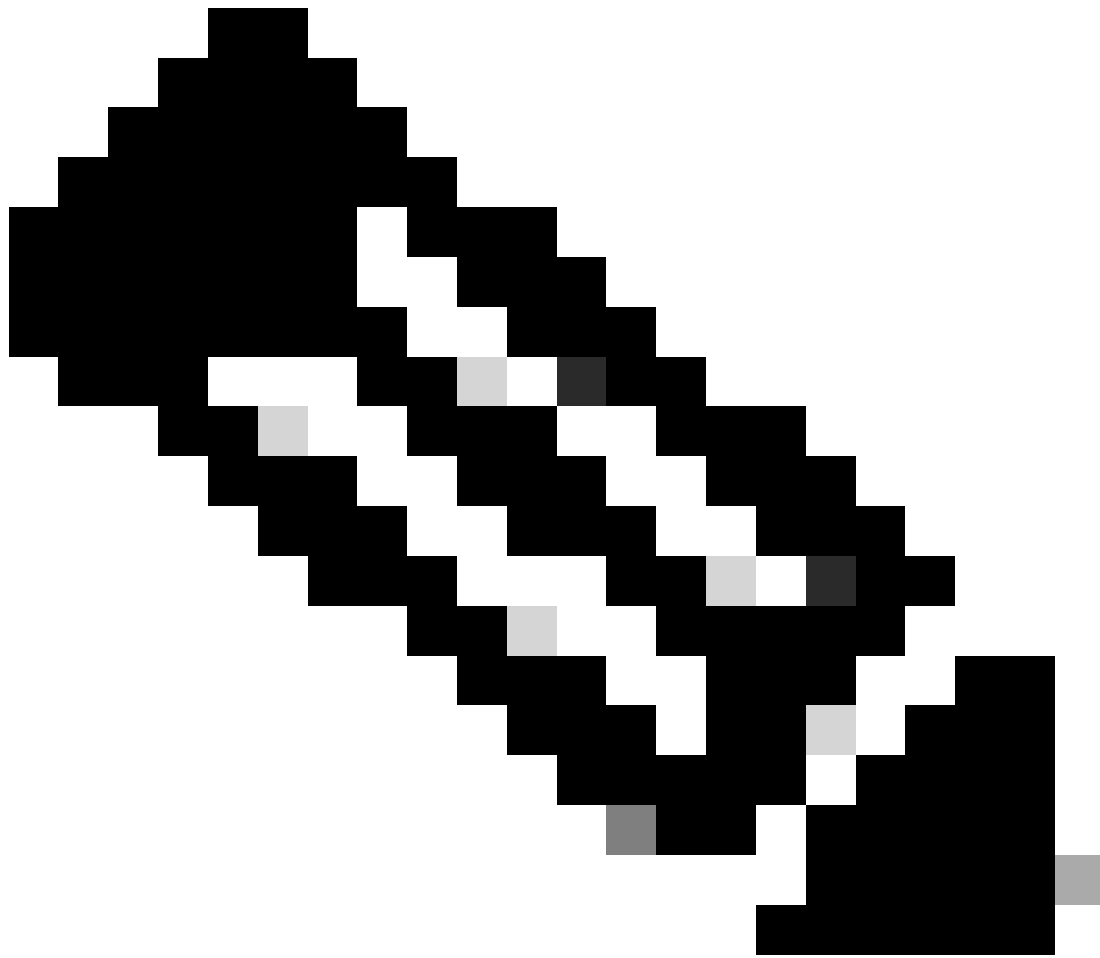
```
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance output
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv4 flow monitor avc_ipv4_assurance_rtp output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance output
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp input
9800-C1-VM(config-wireless-policy)#ipv6 flow monitor avc_ipv6_assurance_rtp output
9800-C1-VM(config-wireless-policy)#no shutdown
9800-C1-VM(config-wireless-policy)#exit
```

Verificatie van AVC

Op 9800

Wanneer de 9800 WLC wordt gebruikt als Flow-exporteur, kunnen deze AVC-statistieken worden waargenomen:

- Toepassingszichtbaarheid voor clients die op alle SID's zijn aangesloten.
- Individueel gebruik van de toepassing voor elke client.
- Specifiek gebruik van toepassingen op elke SSID afzonderlijk.



Opmerking: u hebt de optie om de gegevens te filteren op richting, zowel voor inkomend (toegang) als uitgaand (uitgaand) verkeer, en op tijdsinterval, met de mogelijkheid om een bereik van maximaal 48 uur te selecteren.

Via GUI

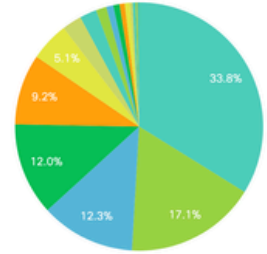
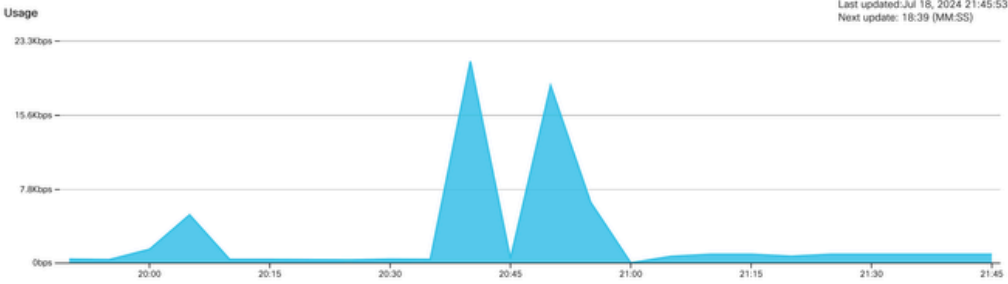
Navigeer naar Monitoring > Services > Application Visibility .

Clear AVC

NBAR Protocol Pack Version: 61.0
NBAR Version: 46

Source type: SSID | SSID: AVC_testing | Direction: Both | Interval: Last 2 hours

Clients
 Applications



Application	Usage (%)	Usage	Received	Sent
Unknown	33.83	796.0KB	300.0KB	496.0KB
Domain Name System	17.08	402.0KB	168.0KB	234.0KB
Ping	12.32	290.0KB	145.0KB	145.0KB
HyperText Transfer Protocol	12.03	283.0KB	117.0KB	166.0KB
ICMP for IPv6	9.22	217.0KB	169.0KB	48.0KB
Internet Control Message Protocol	5.10	120.0KB	84.0KB	36.0KB
Simple Service Discovery Protocol	2.55	60.0KB	47.0KB	13.0KB
Microsoft Services	2.21	52.0KB	44.0KB	8.0KB
mDNS	1.36	32.0KB	27.0KB	5.0KB
Binary over HTTP	0.93	22.0KB	9.0KB	13.0KB

Toepassingszichtbaarheid van gebruikers die zijn verbonden met AVC_testing SSID voor zowel Ingress- als uitgaand verkeer

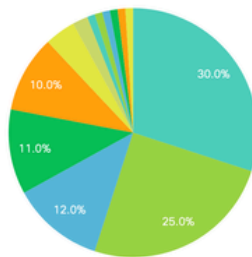
Om de statistieken van de Toepassingszichtbaarheid voor elke cliënt te bekijken, kunt u op het tabblad Clients klikken, een specifieke client kiezen en vervolgens op Toepassingsdetails weergeven klikken.

Clear AVC

NBAR Protocol Pack Version: 61.0
NBAR Version: 46

Source type: SSID | SSID: All | Direction: All | Interval: Last 90 seconds

Clients
 Applications



Total Clients: 1

View Application Details

Client MAC Address	AP Name	WLAN	State	Protocol
[Redacted]	CW9164I-ROW1	18	Run	11n(2,4)

Toepassingszichtbaarheid voor specifieke client - 1

[← Back to Client's](#)

Application Name	Avg Packet Size	Packet Count	Usage(%)	Usage	Sent	Received
ping	60	6662	29	390.4KB	195.2KB	195.2KB
unknown	693	572	29	387.2KB	122.4KB	264.8KB
dns	108	1511	12	160.4KB	23.3KB	137.1KB
ipv6-icmp	111	1313	10	142.6KB	115.4KB	27.2KB
http	300	427	9	125.4KB	52.1KB	73.3KB
icmp	147	333	4	47.8KB	44.1KB	3.7KB
ssdp	168	123	1	20.3KB	16.0KB	4.3KB
mdns	80	204	1	16.0KB	14.8KB	1.2KB
ms-services	64	231	1	14.6KB	10.9KB	3.7KB
llmnr	81	159	1	12.6KB	6.9KB	5.7KB

1 - 10 of 17 items

Toepassingszichtbaarheid voor specifieke client - 2

Via CLI

Controleer de AVC-status

```
9800WLC#show avc status wlan AVC_testing
WLAN profile name: AVC_testing
```

AVC configuration complete: YES

Statistieken van NetFlow (FNF Cache)

```
9800WLC#show flow monitor $Flow_Monitor_Name cache format table
```

```
9800WLC#show flow monitor wireless-avc-basic cache format table
Cache type: Normal (Platform cache)
Cache size: 200000
Current entries: 102
High Watermark: 102

Flows added: 102
Flows aged: 0
```

IPV4 SRC ADDR	IPV4 DST ADDR	TRNS SRC PORT	TRNS DST PORT	FLOW DIRN	WIRELESS SSID	IP PROT	APP NAME	bytes long
wireless client mac addr	mac addr							
10.105.193.170	10.105.193.195	5355	61746	Output	AVC_testing	17	layer7 llmnr	120
10.105.193.129	10.105.193.195	5355	61746	Output	AVC_testing	17	port dns	120
10.105.193.195	10.105.193.2	0	771	Input	AVC_testing	1	prot icmp	148
10.105.193.195	10.105.193.114	0	771	Input	AVC_testing	1	prot icmp	120
10.105.193.4	10.105.193.195	5355	64147	Output	AVC_testing	17	layer7 llmnr	120
10.105.193.169	10.105.193.195	5355	64147	Output	AVC_testing	17	port dns	120
10.105.193.195	10.105.193.52	0	771	Input	AVC_testing	1	prot icmp	148
10.105.193.59	10.105.193.195	5355	64147	Output	AVC_testing	17	port dns	120

Verificatie van AVC op 9800 CLI

U kunt als volgt het gebruik van de bovenste toepassing voor elk WLAN en de aangesloten clients afzonderlijk onderzoeken:

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
where n = <1-30> Enter the number of applications
```

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
where n = <1-10> Enter the number of clients
```

Controleer FNFv9 pakketellingen en decodeer de status die aan Control Plane (CP) is gepunteerd

```
9800WLC#show platform software wlavc status decoder
```

```
9800WLC#show platform software wlavc status decoder
AVC FNFv9 Decoder status:
```

Pkt Count	Pkt Decoded	Pkt Errors	Data Records	Last decoded time	Last error time
25703	25703	0	132480	07/20/2024 14:10:46	01/01/1970 05:30:00

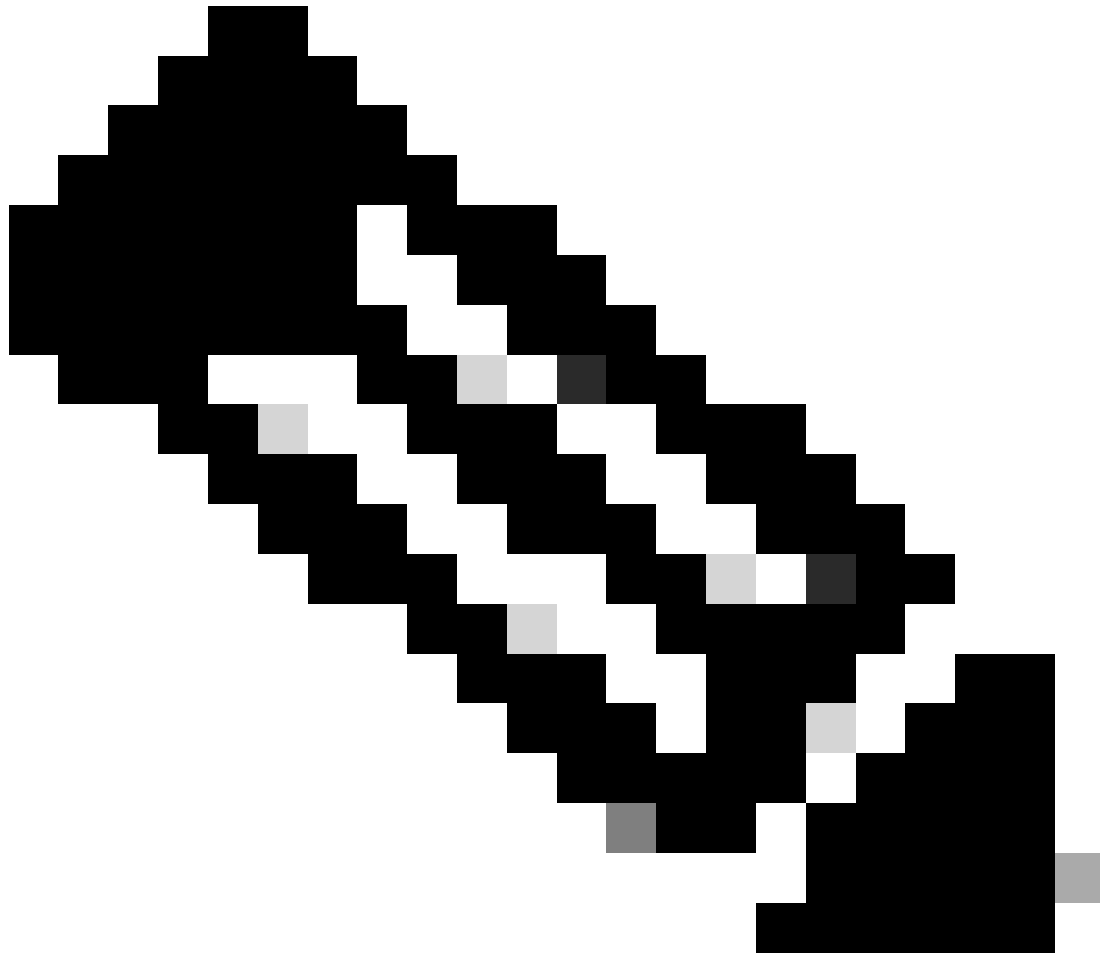
FNFv9 pakketrecord

U kunt ook direct de nbar statistieken controleren.

```
9800WLC#show ip nbar protocol-discovery
```

Op Fabric- en Flex-modi kunt u de NBAR-stats van AP verkrijgen via:

```
AP#show avc nbar statistics
Works on both IOS and ClickOS APs
```



Opmerking: In een buitenlands ankeropstelling, dient het anker WLC als Layer 3-aanwezigheid voor de client, terwijl de buitenlandse WLC werkt op Layer 2. Omdat Application Visibility and Control (AVC) werkt op Layer 3, zijn de relevante gegevens alleen waarneembaar op het anker WLC.

Op DNAC

Van de pakketopname die op 9800 WLC is genomen, kunnen we valideren dat er continu gegevens betreffende de toepassingen en het netwerkverkeer naar Cisco Catalyst Center worden verzonden.

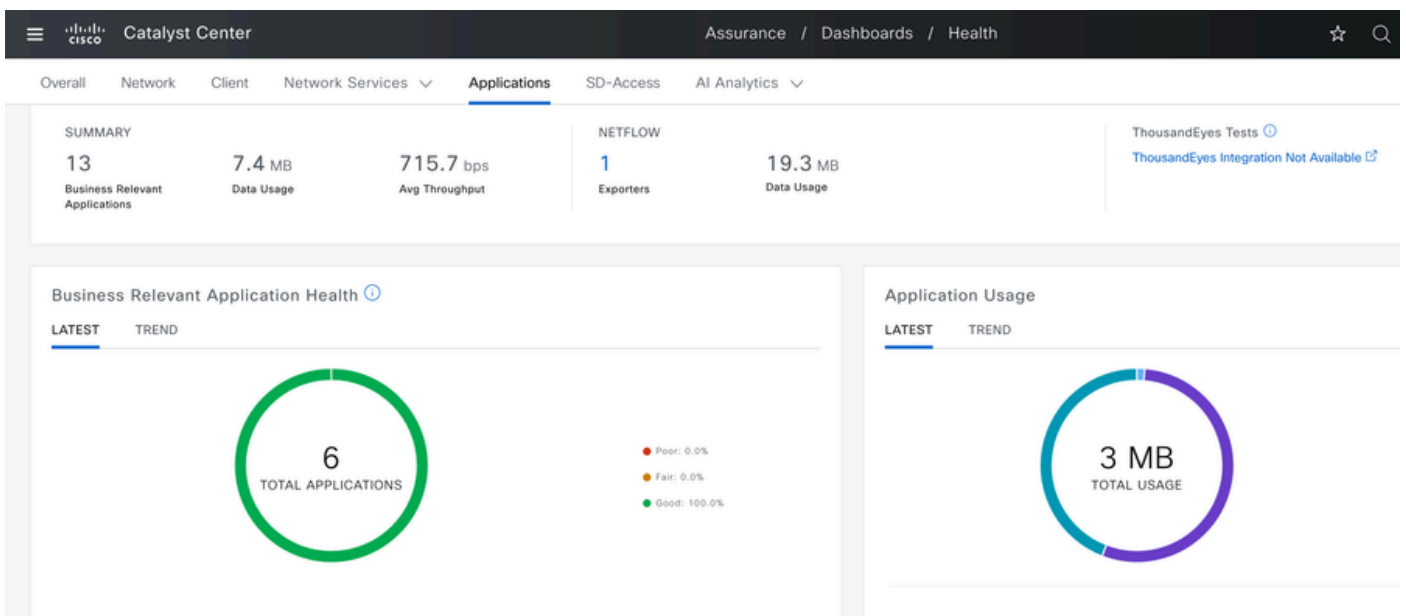
ip.addr == 10.78.8.84 and udp.port == 6007

No.	Time	Source	Destination	Protocol	Length	Info
74227	15:06:30.002990	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
74228	15:06:30.002990	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
76582	15:06:41.012984	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
76879	15:06:45.016997	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
79686	15:07:01.032987	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
85872	15:07:17.047986	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
93095	15:07:37.066982	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
94989	15:07:43.073986	10.105.193.156	10.78.8.84	UDP	178	55148 → 6007 Len=136
98292	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1434	55148 → 6007 Len=1392
98293	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1434	55148 → 6007 Len=1392
98294	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98295	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98296	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98297	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98298	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98299	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98300	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98301	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98302	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98303	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98304	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98305	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98306	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310
98307	15:08:02.784947	10.105.193.156	10.78.8.84	UDP	1352	55148 → 6007 Len=1310

> Frame 1332: 178 bytes on wire (1424 bits), 178 bytes captured (1424 bits)
 > Ethernet II, Src: [REDACTED]
 > Internet Protocol Version 4, Src: 10.105.193.156, Dst: 10.78.8.84
 > User Datagram Protocol, Src Port: 55148, Dst Port: 6007
 > Data (136 bytes)
 Data [truncated]: 000a00886698e17a00001fa700000100011800780a69c150080808080411003501242fd0daa7da00000002000000120d000309005
 [Length: 136]

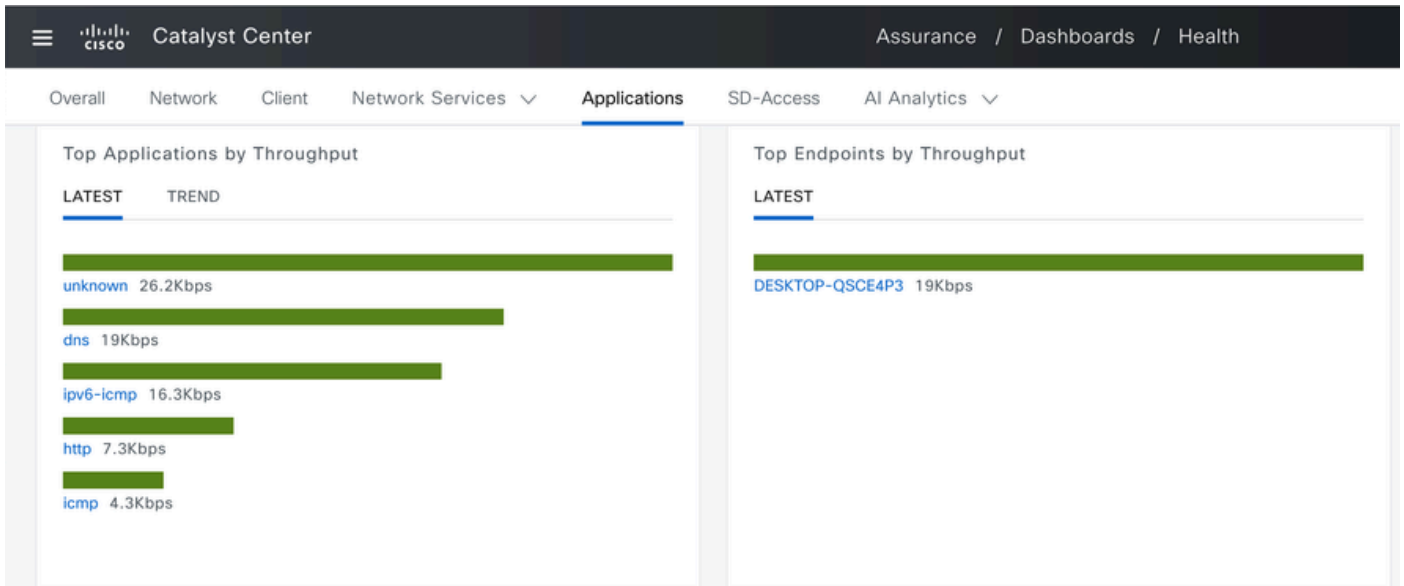
Packet Capture op 9800 WLC

Om de toepassingsgegevens te bekijken voor clients die zijn aangesloten op een specifieke WLC op Cisco Catalyst Center, navigeer je naar Assurance > Dashboards > Health > Application .



AVC-bewaking op Cisco Catalyst Center

We kunnen de meest gebruikte applicaties van klanten volgen en de hoogste data-consumenten identificeren, zoals hier wordt aangetoond.



Belangrijkste toepassing en Top Bandwidth Gebruikersstatistieken

U hebt de mogelijkheid om een filter in te stellen voor een bepaalde SSID, waarmee u de totale doorvoersnelheid en het toepassingsgebruik van clients die aan die SSID zijn gekoppeld kunt bewaken.

Deze functionaliteit stelt u in staat om de belangrijkste toepassingen en de hoogste bandbreedte verbruikende gebruikers binnen uw netwerk te identificeren.

Daarnaast kunt u gebruik maken van de Tijdfilter functie om deze gegevens te onderzoeken voor eerdere tijdsperioden, waardoor historische inzichten in het netwerkgebruik worden aangeboden.

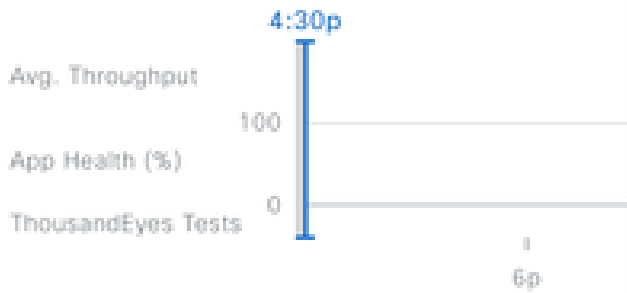
Global/BGL TAC/Shalini_AVC

24 Hours

Filter (1)



By default, hourly data is shown



Time Range

3 Hours

24 Hours

7 Days

Start Date

7 / 17 / 2024



4:23

PM



End Date

7 / 18 / 2024



4:23

PM



SSID: AVC_testing

SUMMARY

13

Business Relevant Applications

7.4 M

Data Usage

Cancel

Apply

Tijdfilter voor weergave van AVC-statistieken

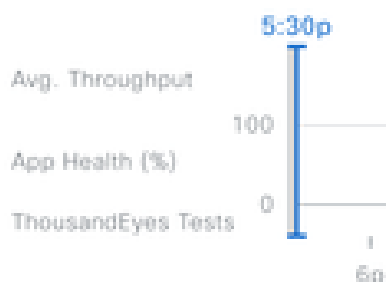


By default, hourly data is show

SSID (1/14)

Clear Filter

- CWA-test-321
- Session_timeout
- LM-INTERNAL
- AVC_testing
- testvritti
- CWA-test-2
- renjith
- Start-Stop
- ...



SSID: AVC_testing

Cancel

Apply

SID-filter voor weergave van AVC-statistieken

Over externe NetFlow Collector

Voorbeeld 1: Cisco Prime als NetFlow Collector

Wanneer u Cisco Prime als NetFlow Collector gebruikt, kunt u 9800 WLC als gegevensbron zien die NetFlow-gegevens verzenden. De NetFlow-sjabloon wordt automatisch gemaakt volgens de gegevens die door 9800 WLC worden verzonden.

Van het pakket dat op 9800 WLC is genomen, kunnen we valideren dat er continu gegevens betreffende de toepassingen en het netwerkverkeer naar Cisco Prime worden verzonden.

ip.addr == 10.106.36.22 && udp.port == 9991

No.	Time	Source	Destination	Protocol	Length	Info
87	20:50:23.855943	10.105.193.156	10.106.36.22	UDP	170	51154 → 9991 Len=128
1453	20:50:24.775945	10.105.193.156	10.106.36.22	UDP	458	51154 → 9991 Len=416
1465	20:50:24.856950	10.105.193.156	10.106.36.22	UDP	170	51154 → 9991 Len=128
1583	20:50:25.776952	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1584	20:50:25.776952	10.105.193.156	10.106.36.22	UDP	1082	51154 → 9991 Len=1040
1596	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1597	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1598	20:50:25.857942	10.105.193.156	10.106.36.22	UDP	474	51154 → 9991 Len=432
1779	20:50:26.777959	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1780	20:50:26.777959	10.105.193.156	10.106.36.22	UDP	1158	51154 → 9991 Len=1116
1857	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1858	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1859	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1860	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	270	51154 → 9991 Len=228
1861	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
1862	20:50:26.858949	10.105.193.156	10.106.36.22	UDP	678	51154 → 9991 Len=636
2086	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
2087	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352
2088	20:50:27.778951	10.105.193.156	10.106.36.22	UDP	534	51154 → 9991 Len=492
2113	20:50:27.859940	10.105.193.156	10.106.36.22	UDP	578	51154 → 9991 Len=536
2287	20:50:28.779958	10.105.193.156	10.106.36.22	UDP	378	51154 → 9991 Len=336
2295	20:50:28.859940	10.105.193.156	10.106.36.22	UDP	1394	51154 → 9991 Len=1352

> Frame 87: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits)
 > Ethernet II, Src: [REDACTED]
 > Internet Protocol Version 4, Src: 10.105.193.156, Dst: 10.106.36.22
 > User Datagram Protocol, Src Port: 51154, Dst Port: 9991
 > Data (128 bytes)
 Data [truncated]: 0009000120eb01e9669932b70000000400000400014f006c000000000000000000000000000000ff0200000000000000000001
 [Length: 128]

Packet Capture genomen op 9800 WLC

Prime Infrastructure

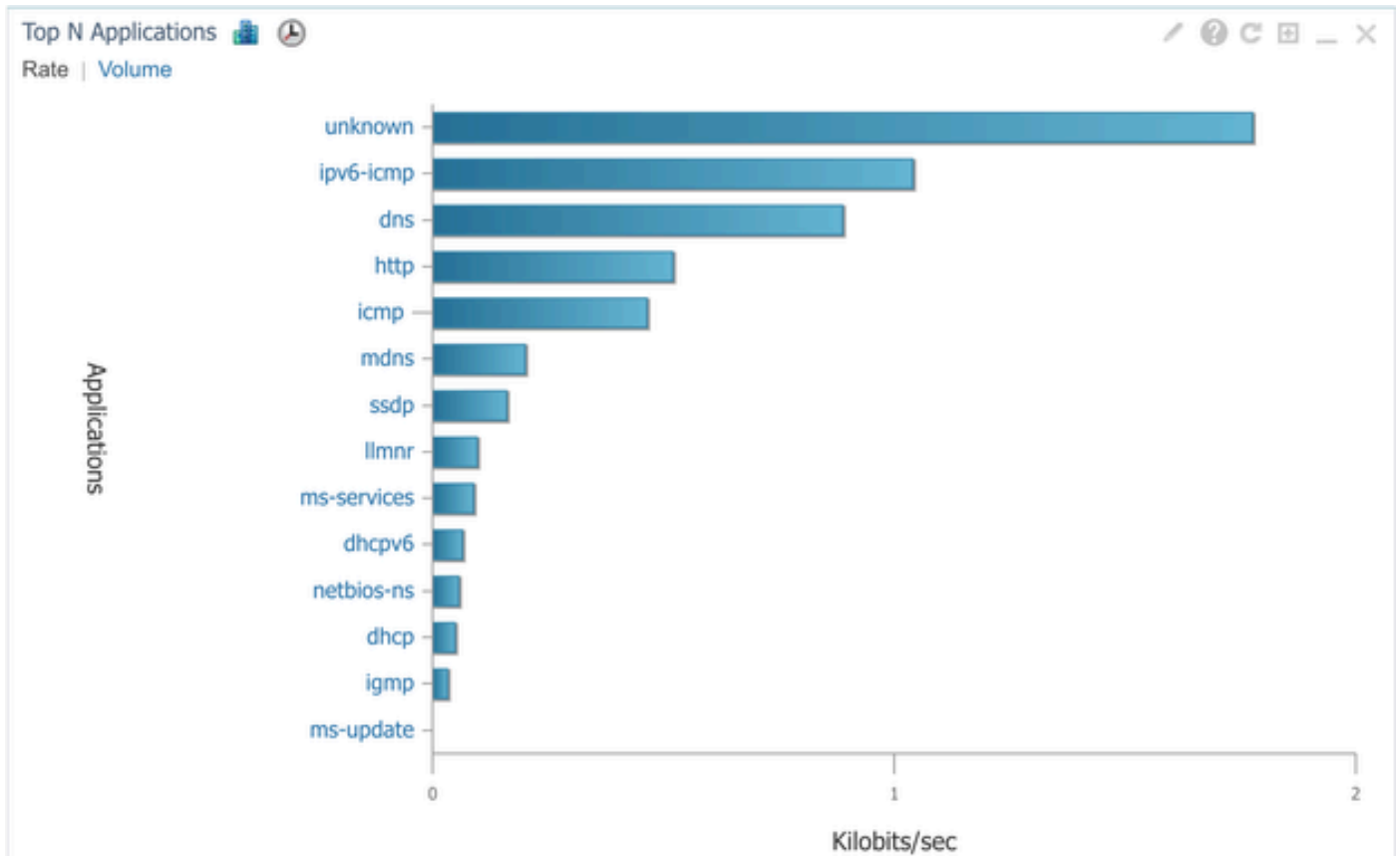
Services / Application Visibility & Control / Data Sources

Device Data Sources

Device Name	Data Source	Type	Exporting Device	Last 5 min Flow Record Rate	Last Active Time
<input type="checkbox"/> 9800WLC.cisco.com	10.105.193.156	NETFLOW	10.105.193.156	2	Friday, July 19 2024 at 04:50:18 AM India Standa...

Cisco Prime Detecting-applicatie 9800 WLC als NetFlow-gegevensbron

U kunt filters instellen op basis van Toepassing, Diensten en zelfs door Client, met behulp van het IP-adres voor meer gerichte gegevensanalyse.

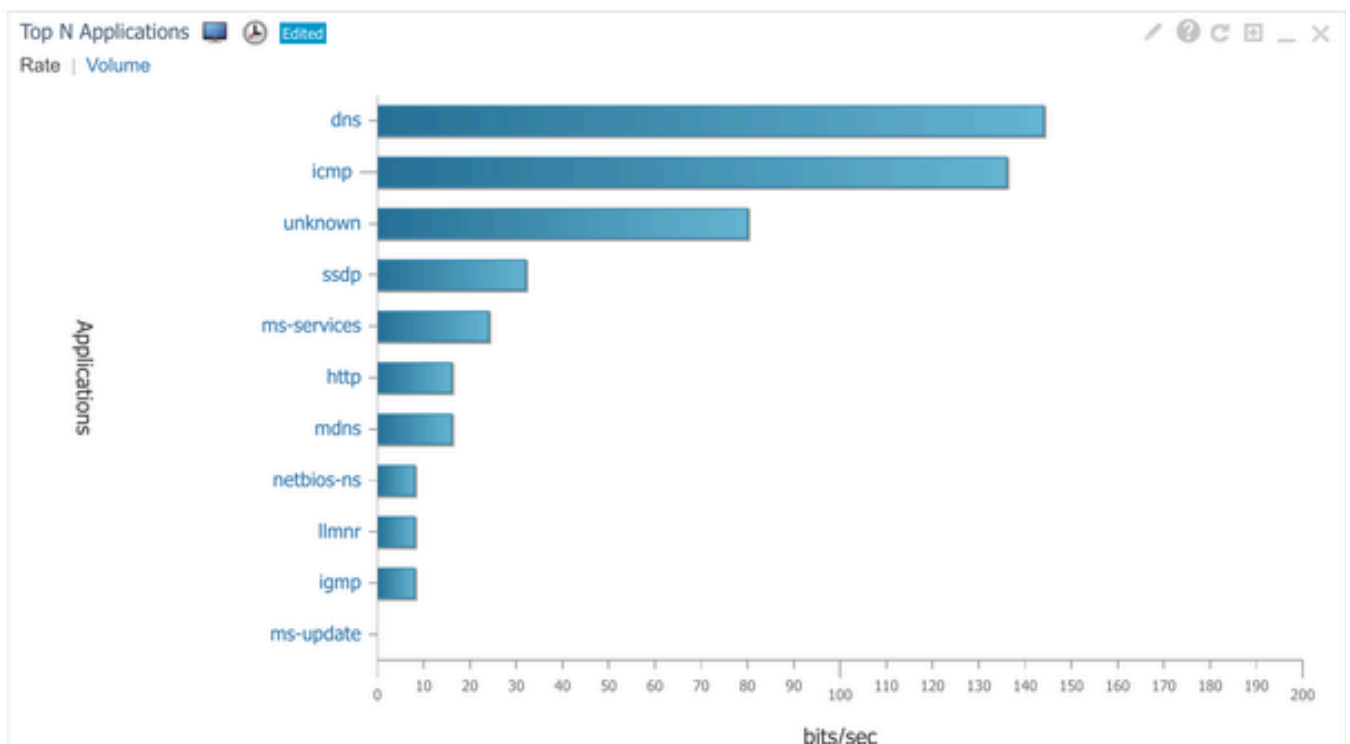


Toepassingszichtbaarheid voor alle clients

Dashboard / Performance

Site | Device | Access Point | Interface | Application | Voice/Video | End User Experience

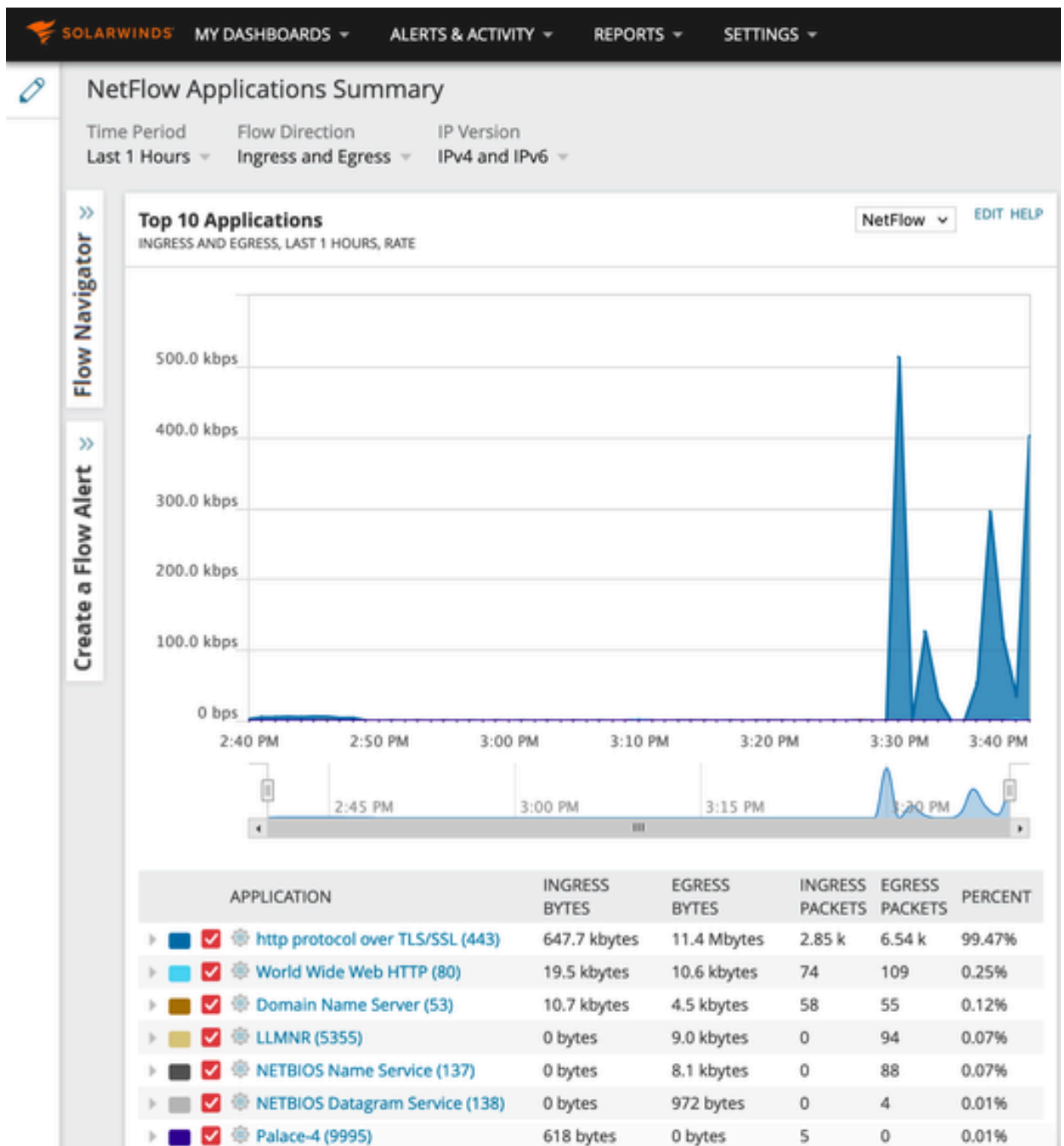
Filters *Client 10.105.193.80,Una... *Time Frame Past 1 Hour Application All Network Aware



Toepassing van specifieke client met IP-adres

Voorbeeld 2: NetFlow Collector van derden

In dit voorbeeld, wordt de derde partij NetFlow Collector [SolarWinds] gebruikt om toepassingsstatistieken te verzamelen. De 9800 WLC maakt gebruik van Flexible NetFlow (FNF) om uitgebreide gegevens te verzenden over de toepassingen en het netwerkverkeer, die vervolgens door SolarWinds worden verzameld.



NetFlow Application Statistics op SolarWind

Verkeerscontrole

Traffic control verwijst naar een reeks functies en mechanismen die worden gebruikt om de stroom van netwerkverkeer te beheren en te reguleren. Traffic policing of snelheidsbeperking zijn mechanismen die in draadloze controller worden gebruikt om de hoeveelheid verkeer te controleren die van de client wordt verzonden. Het controleert het gegevenstarief voor netwerkverkeer en neemt onmiddellijk actie wanneer een vooraf bepaalde snelheidsgrens wordt overschreden. Wanneer het verkeer het opgegeven tarief overschrijdt, kan snelheidsbeperking de overtollige pakketten laten vallen of ze markeren door hun CoS-waarden (Class of Service) of DSCP-waarden (Differentiated Services Code Point) te wijzigen. Dit kan worden bereikt door QOS in 9800 WLC te configureren. U kunt naar

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/215441-configure-qos-rate-limiting-on-catalyst.html> verwijzen om een overzicht te krijgen van hoe deze componenten werken en hoe ze kunnen worden geconfigureerd om verschillende resultaten te bereiken.

Probleemoplossing

Problemen met AVC oplossen houdt in dat problemen worden geïdentificeerd en opgelost die mogelijk van invloed zijn op het vermogen van AVC om toepassingsverkeer op uw draadloze netwerk nauwkeurig te identificeren, classificeren en beheren. Gemeenschappelijke kwesties kunnen problemen met verkeersclassificatie, beleidshandhaving, of rapportering omvatten. Hier zijn enkele stappen en overwegingen bij het oplossen van problemen met AVC op een Catalyst 9800 WLC:

- Controleer AVC Configuration: zorg ervoor dat AVC correct op de WLC is geconfigureerd en aan de juiste WLAN's en profielen is gekoppeld.
- Wanneer u AVC instelt via de GUI, wordt automatisch poort 995 als de standaardpoort toegewezen. Als u echter een Externe Collector gebruikt, controleert u welke poort is ingesteld om te luisteren op NetFlow-verkeer. Het is van cruciaal belang om dit poortnummer nauwkeurig te configureren zodat het overeenkomt met de instellingen van uw verzamelaar.
- Controleer het AP-model en de ondersteuning voor de implementatiemodus.
- Raadpleeg beperkingen op de 9800 WLC bij implementatie van AVC in uw draadloze netwerk.

Logbestanden verzamelen

WLC-logs

1. Laat timestamp toe om tijdverwijzing voor alle bevelen te hebben.

```
9800WLC#term exec prompt timestamp
```

2. De configuratie bekijken

```
9800WLC#show tech-support wireless
```

3. U kunt de avc-status en netflow-statistieken verifiëren.

Controleer de AVC-configuratiestatus.

```
9800WLC#show avc status wlan <wlan_name>
```

Controleer FNFv9 pakkettellingen en decodeer de status gepunteerd aan Control Plane (CP).

```
9800WLC#show platform software wlavc status decoder
```

Controleer de statistieken van NetFlow (FNF Cache).

```
9800WLC#show flow monitor <Flow_Monitor_Name>
```

Controleer het gebruik van de toepassing voor elk WLAN, waarbij n = <1-30> Het aantal toepassingen invoert.

```
9800WLC#show avc wlan <SSID> top <n> applications <aggregate|downstream|upstream>
```

Controleer het toepassingsgebruik voor elke client, waarbij n = <1-30> Het aantal toepassingen invoert.

```
9800WLC#show avc client <mac> top <n> applications <aggregate|downstream|upstream>
```

Controleer de top-n-clients die met specifieke WLAN zijn verbonden met behulp van de specifieke toepassing, waarbij n=<1-10> het aantal clients invoert.

```
9800WLC#show avc wlan <SSID> application <app> top <n> <aggregate|downstream|upstream>
```


Controleer de nbar-statistieken.

```
9800WLC#show ip nbar protocol-discovery
```

4. Stel het registratieniveau in op debug/verbose.

```
9800WLC#set platform software trace all debug/verbose
```

!! To View the collected logs

```
9800WLC#show logging profile wireless internal start last clear to-file bootflash:<File_Name>
```

!!Set logging level back to notice post troubleshooting

```
9800WLC#set platform software trace wireless all debug/verbose
```

5. Schakel Radioactive (RA) Trace voor client-MAC-adres in om de AVC-stats te valideren.

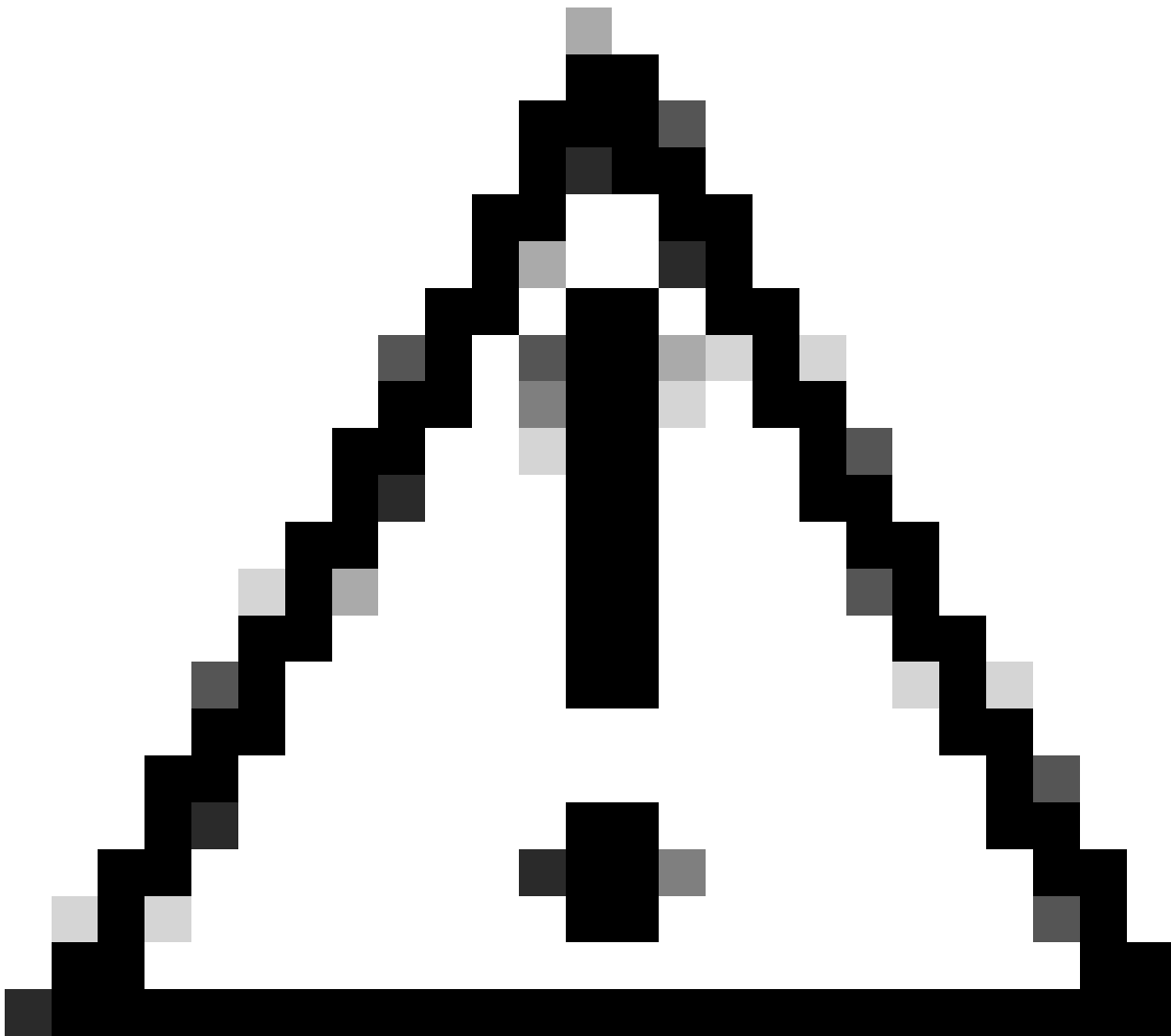
Via CLI

```
9800WLC#debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting ti
```

```
9800WLC#no debug wireless mac <Client_MAC>
```

!!WLC generates a debug trace file with Client_info, command to check for debug trace file generated.

```
9800WLC#dir bootflash: | i debug
```



Waarschuwing: het voorwaardelijke debuggen maakt debug-level logging mogelijk, waardoor het volume van de gegenereerde logs toeneemt. Als u dit programma laat draaien, vermindert u hoe ver u terug in de tijd kunt kijken naar logbestanden van. Daarom wordt aangeraden om debugging altijd uit te schakelen aan het eind van de probleemplossing sessie.

```
# clear platform condition all  
# undebug all
```

Via GUI

Stap 1. Ga naar Problemen oplossen > Radioactief spoor.

Stap 2. Klik op Add en voer een client-Mac-adres in dat u wilt oplossen. U kunt meerdere Mac-adressen aan de track toevoegen.

Stap 3. Wanneer u klaar bent om de radioactieve tracersing te starten, klikt u op Start. Zodra begonnen, debug het registreren wordt geschreven aan schijf over om het even welke verwerking

van het controlevliegtuig met betrekking tot de gevolgde adressen van MAC.

Stap 4. Wanneer u het probleem reproduceert dat u wilt oplossen, klikt u op Stoppen .

Stap 5. Voor elk gedebuggeerd mac-adres kunt u een logbestand genereren door te klikken op Generate om alle logbestanden met betrekking tot dat mac-adres te verzamelen.

Stap 6. Kies hoe lang u wilt dat uw gecollationeerde logbestand gaat en klik op Toepassen op apparaat.

Stap 7. U kunt het bestand nu downloaden door op het kleine pictogram naast de bestandsnaam te klikken. Dit bestand is aanwezig in de boot flash drive van de controller en kan ook uit het vak worden gekopieerd via CLI.

Hier is een glimp van AVC debugs in RA-sporen

```
2024/07/20 20:15:24.514842337 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514865665 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:24.514875837 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
2024/07/20 20:15:40.530177442 {wstatsd_R0-0}{2}: [avc-stats] [15736]: (debug): Received stats record fo
```

6. Ingesloten Captures gefilterd op client MAC-adres in beide richtingen, client binnenkant MAC-filter beschikbaar na 17.1.

Het is bijzonder nuttig wanneer het gebruiken van een externe collector, aangezien het helpt bevestigen of WLC NetFlow gegevens aan de voorgenomen haven zoals verwacht overbrengt.

Via CLI

```
monitor capture MYCAP clear
monitor capture MYCAP interface <Interface> both
monitor capture MYCAP buffer size 100
monitor capture MYCAP match any
monitor capture MYCAP inner mac CLIENT_MAC@
monitor capture MYCAP start
!! Initiate different application traffic from user
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:../filename.pcap
```

Via GUI

Stap 1. Ga naar Problemen oplossen > Packet Capture > +Add.

Stap 2. Bepaal de naam van de pakketopname. U mag maximaal 8 tekens gebruiken.

Stap 3. Definieer eventuele filters.

Stap 4. Schakel het vakje Monitor Control Traffic in als u wilt zien dat verkeer wordt gestraft naar de systeem CPU en opnieuw wordt ingespoten in het dataplatform.

Stap 5. Definieer de buffergrootte. Een maximum van 100 MB is toegestaan.

Stap 6. Definieer de limiet, hetzij door de duur die een bereik van 1 - 1000000 seconden toestaat, hetzij door het aantal pakketten dat een bereik van 1 - 100000 pakketten toestaat, zoals gewenst.

Stap 7. Kies de interface uit de lijst met interfaces in de linkerkolom en selecteer de pijl om deze naar de rechterkolom te verplaatsen.

Stap 8. Klik op Toepassen op apparaat.

Stap 9. Om de opname te starten, selecteert u Start .

Stap 10. U kunt de opname tot de gedefinieerde limiet laten lopen. Selecteer Stop om de opname handmatig te stoppen.

Stap 11. Zodra gestopt, een Export knop beschikbaar om te klikken met de optie om het opnamebestand (.pcap) op de lokale desktop te downloaden via HTTP of TFTP server of FTP server of lokale systeem harde schijf of flash.

AP-logbestanden

Op fabric en Flex-modi

1. toon technologie om alle configuratie details en client stats voor de AP te hebben.
2. toon avc nbar statistieken nbar stats van AP
3. AVC-debug

```
AP#term mon
```

```
AP#debug capwap client avc <all/detail/error/event>
```

```
AP#debug capwap client avc netflow <all/detail/error/event/packet>
```

Gerelateerde informatie

[AVC-configuratiehandleiding](#)

[Snelheidsbeperking op 9800 WLC](#)

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.