Umbrella DNS implementeren voor Aruba WLAN-beheerders

Inhoud

Inleiding

In dit document wordt beschreven hoe u de Umbrella DNS-service kunt implementeren voor Aruba WLAN-beheerders.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella.

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.

Overzicht

Aruba Networks heeft deze drie draadloze LAN (WLAN) productlijnen en besturingssystemen voor verschillende marktsegmenten en implementatiescenario's:

- ArubaOS: voor grote organisaties en implementaties met hoge dichtheid
- Aruba Instant / InstantOS: voor kleine tot middelgrote bedrijven en gedistribueerde bedrijven
- Aruba Instant On: voor thuisgebruikers en kleine kantoorgebruikers

Dit artikel biedt richtlijnen voor Aruba WLAN-beheerders om Umbrella DNS-service te gebruiken en te implementeren.

Implementatiemethoden

De implementatiemethoden zijn afhankelijk van uw Aruba-besturingssysteem en de manier waarop u Umbrella wilt gebruiken.

Als u een van de drie eerder genoemde Aruba-besturingssystemen uitvoert, kunt u Umbrella DNS implementeren door de Umbrella-gebruikershandleiding te raadplegen. Ook video tutorials zijn beschikbaar.

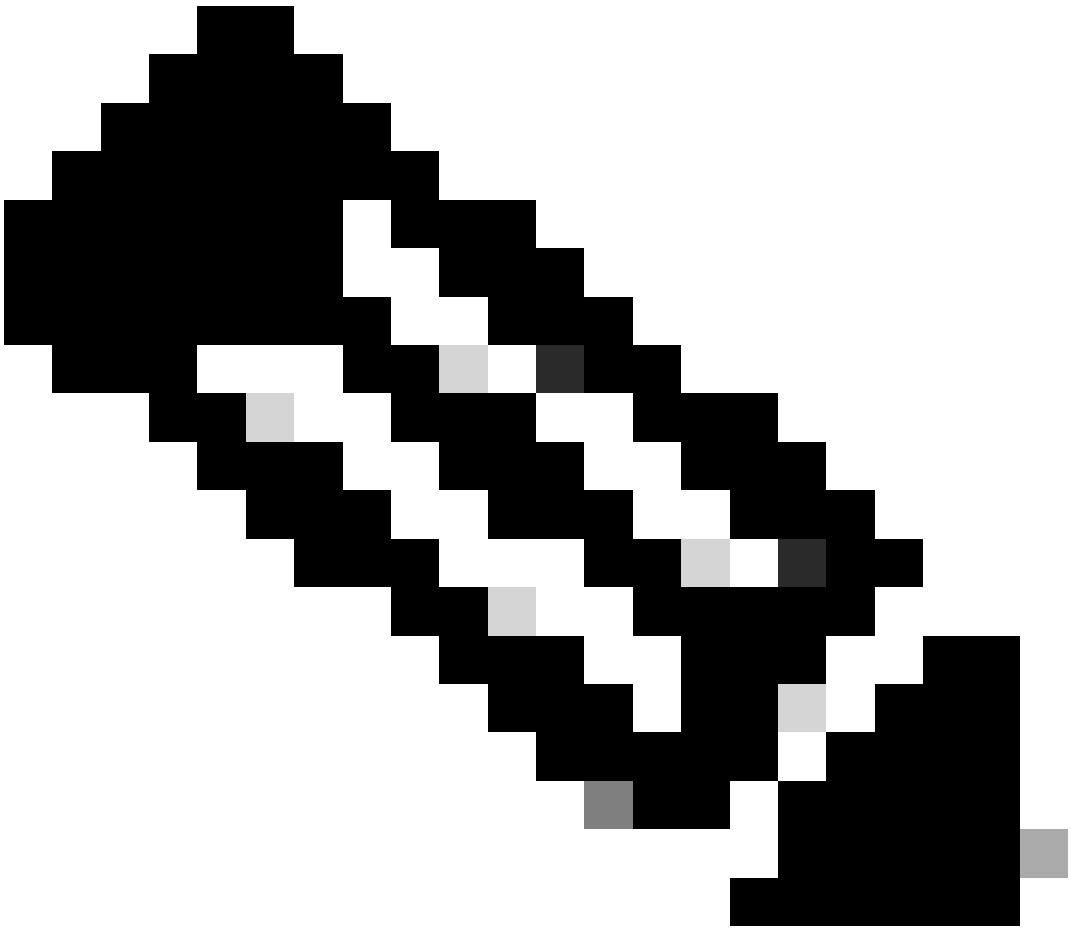
Als u Aruba Instant uitvoert, hebt u een extra optie om de Umbrella-netwerkapparaatintegratie te gebruiken die beschikbaar is in InstantOS. Houd er echter rekening mee dat als u deze optie kiest, u de interne/privé-IP-adressen van draadloze clients niet kunt zien op het WLAN in de overkoepelende rapportage, zoals het rapport Activiteit zoeken. DNS-query's van clients worden toegewezen aan de netwerkapparaatidentiteiten van Instant AP-clusters in Umbrella en informatie over de afzonderlijke clients is niet beschikbaar. Vanuit het perspectief van Umbrella cloud kunnen DNS-query's lijken te komen uit de Instant AP-clusters in plaats van de Wi-Fi-clients.

Als u de DNS-query's van individuele clients wilt traceren of het DNS-beleid voor individuele clients op een WLAN wilt afstemmen, kunt u Umbrella implementeren via standaardmethoden die worden beschreven in de Umbrella DNS-gebruikershandleiding (zonder de netwerkapparaatintegratie via Aruba Instant te gebruiken) en overwegen om Umbrella virtuele apparaten in hun implementatieplannen op te nemen.

Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

Aruba Instant Integration

Aruba Instant's Umbrella (OpenDNS) netwerkapparaatintegratie kan nuttig zijn in omgevingen waar alle Wi-Fi-clients die zijn verbonden met een Instant AP-cluster onderworpen zijn aan een enkelvoudig Umbrella DNS-beleid en waar het niet nodig is om de DNS-query's van individuele clients te bekijken in overkoepelende rapporten. In dit gedeelte wordt uitgelegd hoe u de integratie kunt instellen.



> Opmerking: De integratie maakt gebruik van een oudere versie van de netwerkapparaten API van Umbrella. De oudere versie vereist niet dat klanten API-tokens genereren vanuit hun Umbrella-dashboards, maar de nieuwere versies wel.

Umbrella legacy API's bereikten het einde van hun levensduur op 2023-09-01, waarna geen ondersteuning meer wordt geboden voor de integratie. Als u na 2023-09-01 problemen ondervindt met de integratie, vult u het gedeelte "Aan de slag" in de implementatiegids in om Umbrella te implementeren zonder de integratie te gebruiken.

Aan deze vereisten moet worden voldaan om de integratie te kunnen gebruiken:

- AP's moeten InstantOS versie 8.10.0.1 of nieuwer uitvoeren (vanaf mei 2022).
- De Umbrella dashboard-account die voor de integratie wordt gebruikt, moet de rol van Full Admin hebben.
- Het e-mailadres van het account kan niet aan meer dan één Umbrella-dashboard worden gekoppeld. Als u niet zeker weet of het e-mailadres slechts aan één dashboard is gekoppeld, kunt u contact opnemen met Cisco Umbrella Support om dit te controleren.
- Single sign-on (SSO) en two-factor authenticatie (2FA) kunnen niet worden ingeschakeld voor het account.
- Als er een netwerkbeveiligingstoestel (zoals een firewall) tussen toegangspunten en internet is, moet het toestel ongefilterde en niet-geïnspecteerde verbindingen toestaan naar 208.67.220.220, 208.67.222.222, 67.215.92.210 en 146.112.255.152/29 (.152 ~ .159).

Configuratie

Op hoog niveau zijn er vier configuratiestappen om de integratie mogelijk te maken:

1. Stel een naam in voor het AP-cluster

2. Voer accountgegevens in

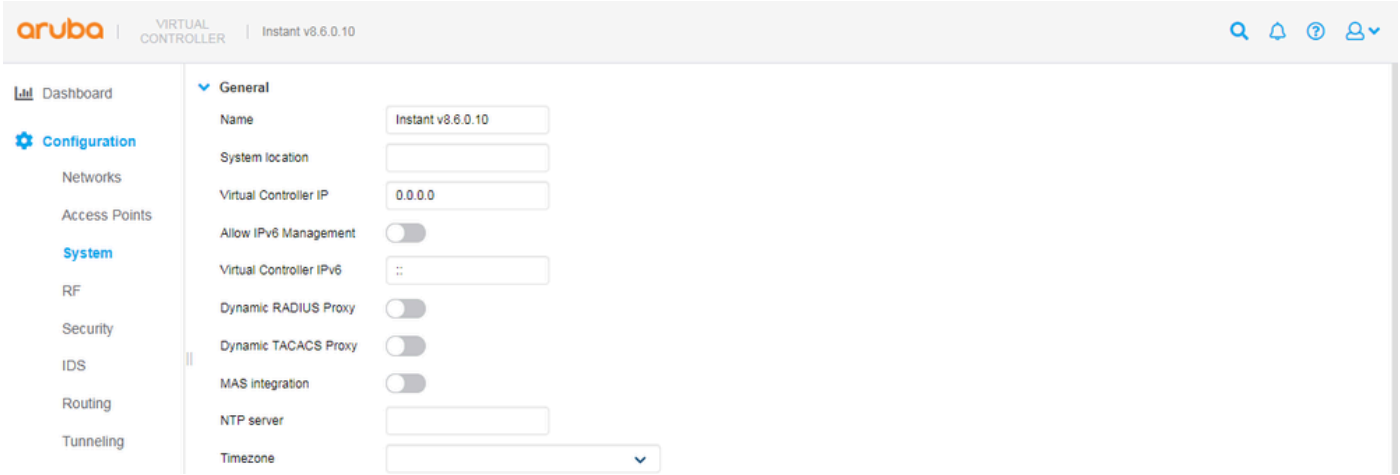
3. DNS-zoekopdrachten onderscheppen

4. DNS-beleid toepassen

Een naam instellen voor het AP-cluster

Wanneer een Instant-cluster zichzelf voor het eerst succesvol registreert op een Umbrella-dashboard, wordt een vermelding voor een netwerkapparaat toegevoegd aan het Umbrella-dashboard onder Implementaties > Netwerkapparaten. De apparaatnaam van een nieuw item is afkomstig van de systeemnaam die is geconfigureerd op de virtuele controller van een cluster.

Om de systeemnaam in te stellen op een Instant Virtual Controller, gaat u naar Configuratie > Systeem.



4404011628308

De waarde voor de naam wordt slechts eenmaal gekopieerd tijdens de eerste registratie. Als een systeem-/apparaatnaam achteraf aan de kant Instant of Umbrella wordt gewijzigd, moet u de naam aan de andere kant handmatig bijwerken.

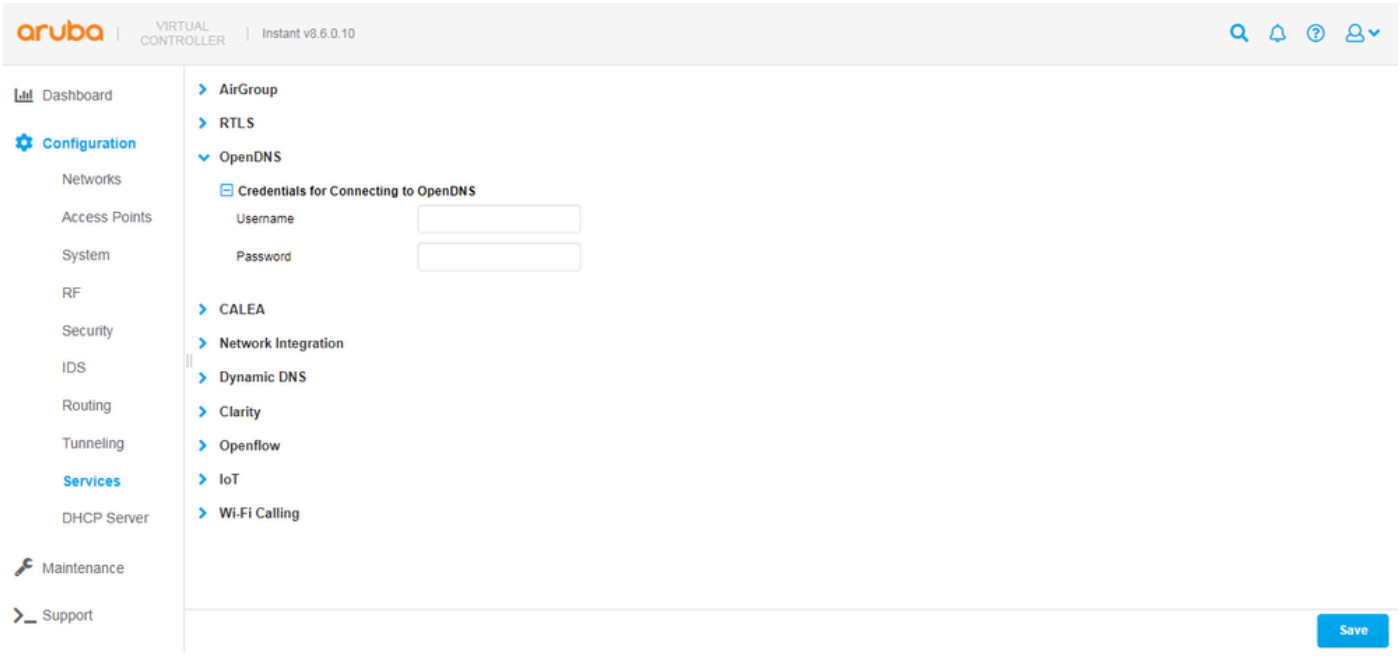
Accountreferenties invoeren

Als aan de vereisten in het gedeelte Vereisten wordt voldaan, kunt u een Instant-cluster als netwerkapparaat toevoegen aan uw Umbrella-dashboard. Dit doet u vanuit de virtuele controller van een cluster:

1. Ga naar Configuratie > Services > OpenDNS.

2. Voer de inloggegevens van een Umbrella-account in.

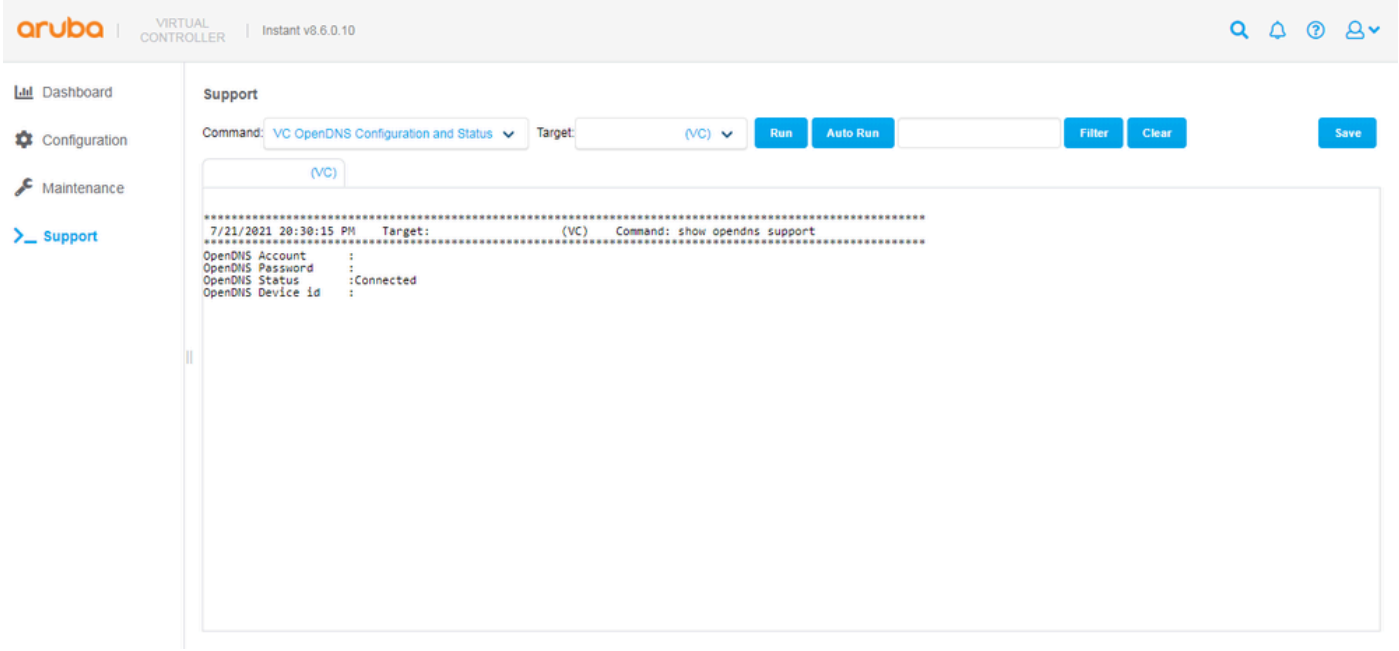
3. Selecteer Opslaan.



4404019266196

Als de virtuele controller (VC) succesvol verbinding maakt met Umbrella, kunt u een Connected-status zien wanneer u naar Support navigeert en de opdracht "VC OpenDNS Configuration and Status" (`openDNS-ondersteuning weergeven`) uitvoert.

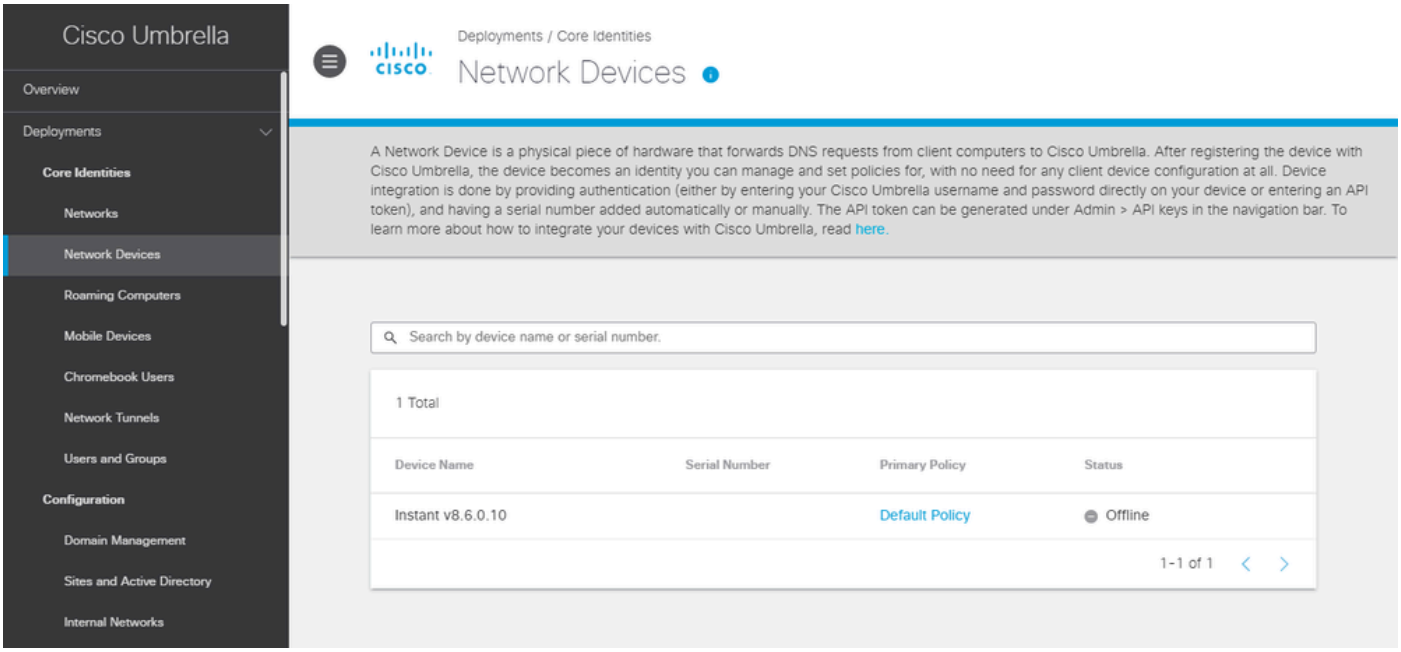
U kunt ook een apparaat-ID zien, die wordt gegenereerd door Umbrella wanneer een nieuw netwerkapparaat wordt gemaakt en opgeslagen in de Instant VC-configuratie. Het laatste deel is belangrijk. Aangezien elk Instant-cluster een unieke paraplu-netwerkapparaat-ID moet hebben, mag de apparaat-ID niet worden gekopieerd van de configuratie van het ene cluster naar het andere. Een geldige apparaat-ID heeft doorgaans 16 cijfers.



4404019268116

Als de opdrachtuitvoer een Niet-verbonden status toont, kunt u proberen uit te vinden waarom door de opdrachten "AP Tech Support Dump" (`toon technische ondersteuning`) en "AP Tech Support Dump Supplemental" (`toon technische ondersteuning`) uit te voeren en vervolgens te zoeken naar "opendns" in de logs. De commando-uitgangen kunnen ook worden gedeeld met Aruba TAC voor het oplossen van problemen.

Als alles correct werkt, kunt u een nieuw item in het dashboard van de paraplu bekijken onder Implementaties > Netwerkapparaten, waar u kunt zoeken naar een instant AP-cluster op basis van de naam of een bestaand item kunt verwijderen als u een nieuwe apparaat-ID wilt genereren.



4404011658516

DNS-zoekopdrachten onderscheppen

Nadat u hebt bevestigd dat een cluster als netwerkapparaat met succes aan uw Umbrella-dashboard is toegevoegd, kunt u het cluster zo instellen dat het begint met het onderscheppen van DNS-query's die zijn verzonden vanaf draadloze clients (die zijn verbonden met toegangspunten in het cluster). Zodra deze is ingesteld, ongeacht welke DNS-server-IP-adressen op de NIC's van draadloze clients zijn geconfigureerd, kunnen de DNS-query's van de clients door het cluster worden onderschept en worden doorgestuurd naar de anycastresolvers van Umbrella op 208.67.220.220 en 208.67.222.222.

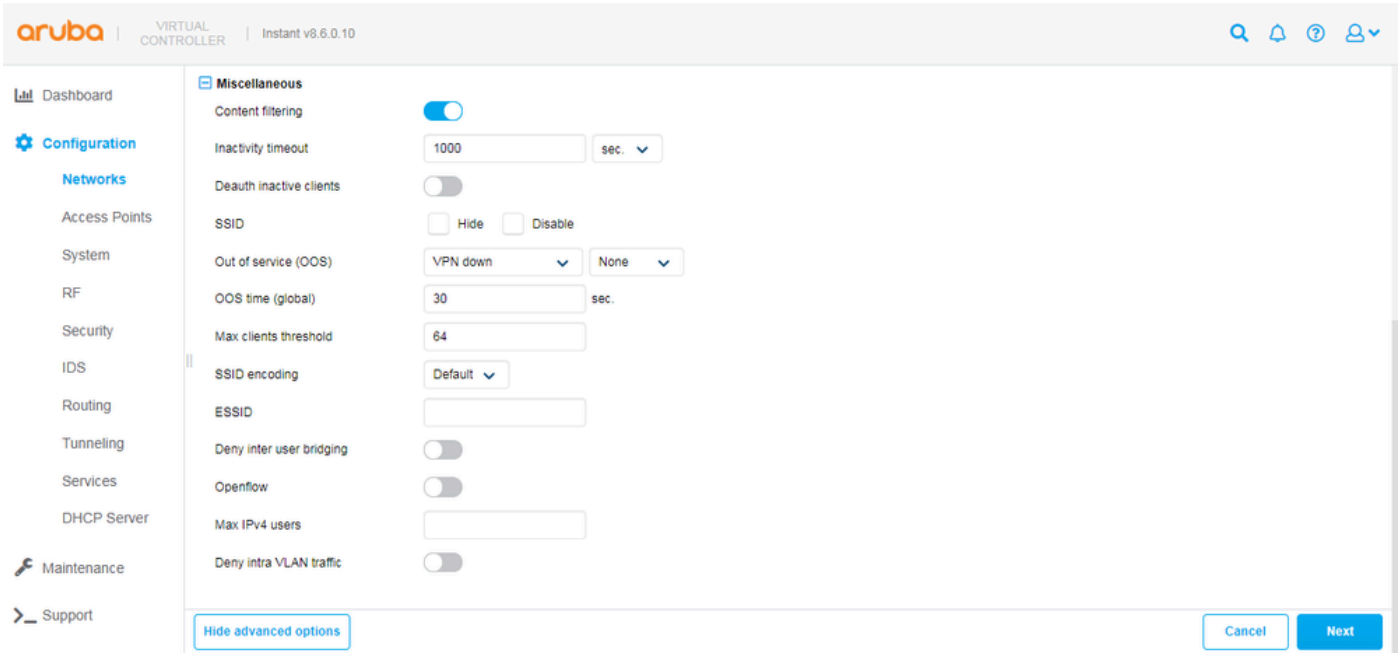
DNS-query's onderscheppen:

1. Navigeer naar de virtuele controller van een cluster onder Configuratie > Netwerken.

2. Selecteer een draadloos netwerk.

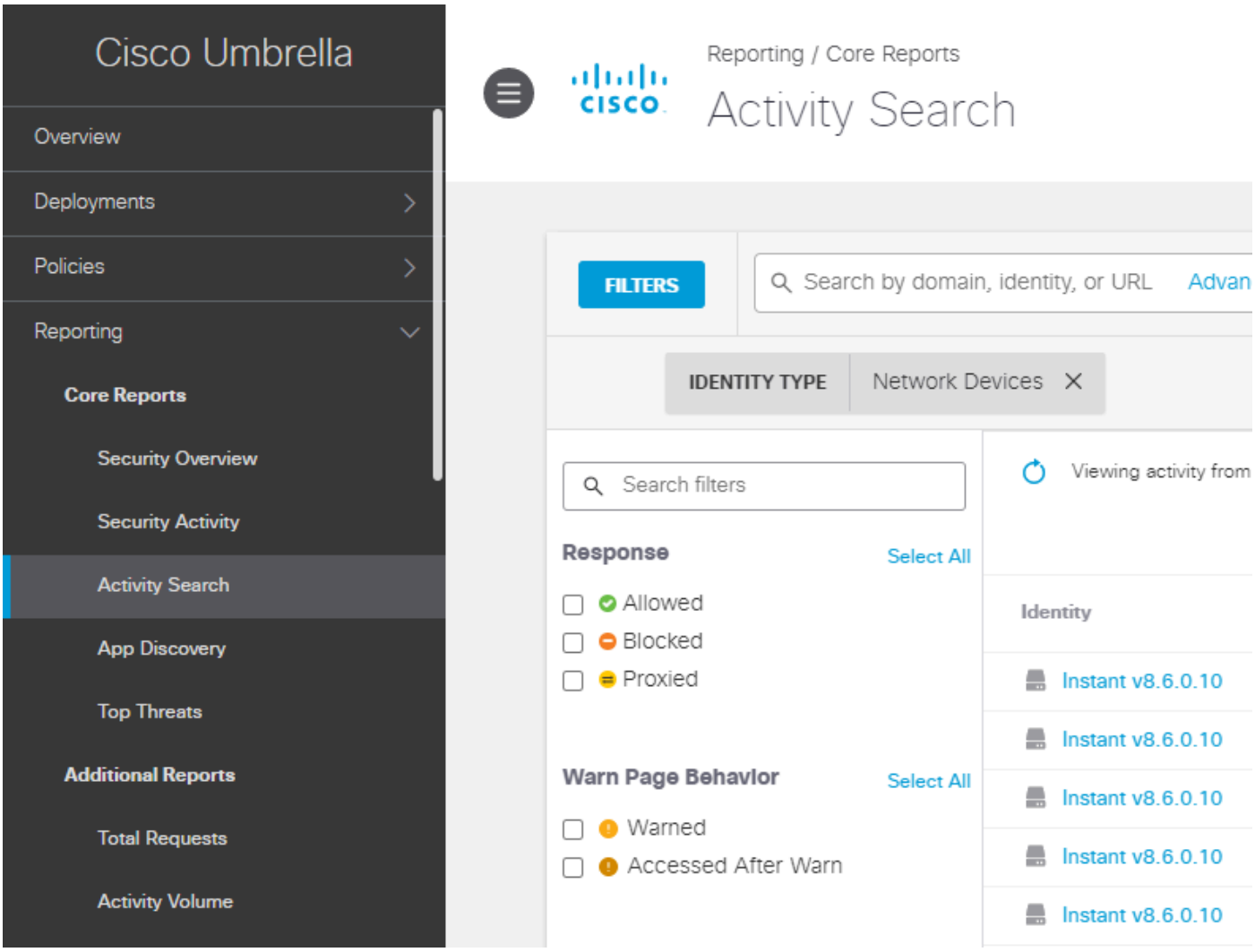
3. Bewerk het netwerk, selecteer Geavanceerde opties weergeven en blader naar de sectie Diversen.

4. Schakel de optie Inhoudsfiltering in en blijf Volgende selecteren totdat u de knop Voltooien kunt selecteren om de wijziging op te slaan.



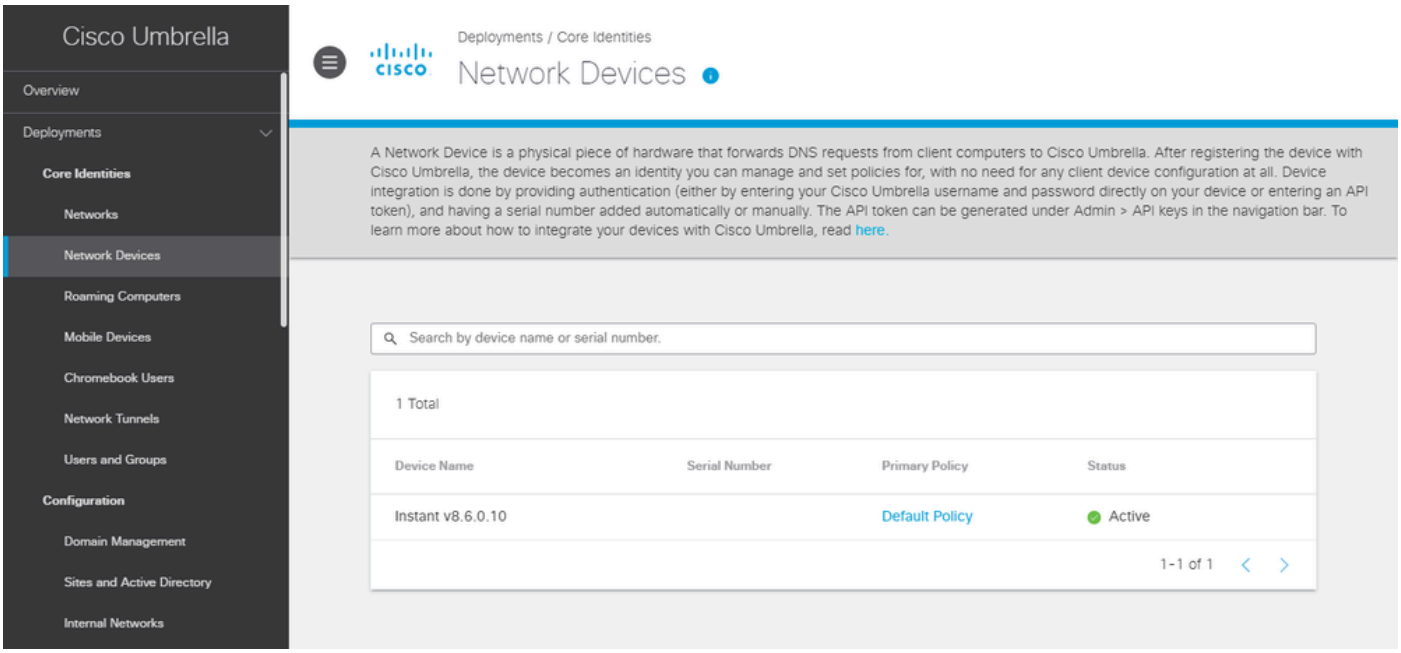
4404011668500

Nadat de optie is ingeschakeld, kunt u DNS-query's bekijken in het overkoepelende dashboard onder Rapportage > Activiteit zoeken.De identiteit van de query's kan worden toegewezen aan een netwerkapparaatnaam, die meestal de systeemnaam is die is geconfigureerd op de virtuele controller van een AP-cluster. Merk op dat het enige tijd (ongeveer 15 minuten) kan duren voordat vragen worden verwerkt en weergegeven in de GUI van het dashboard.



4404011721620

In het Umbrella-dashboard onder Implementaties > Netwerkapparaten kan het tot 24 uur duren voordat een apparaat de status Actief/Online heeft gekregen. De status van een netwerkapparaat geeft alleen aan of DNS-query's door het apparaat zijn onderschept en in de 24 uur daarvoor naar Umbrella zijn doorgestuurd, en heeft geen invloed op de manier waarop een apparaat communiceert met Umbrella. Een offline/inactieve status kan eenvoudig betekenen dat er de afgelopen 24 uur geen draadloze client is verbonden met een AP-cluster en kan niet voorkomen dat het cluster de Umbrella-service gebruikt.

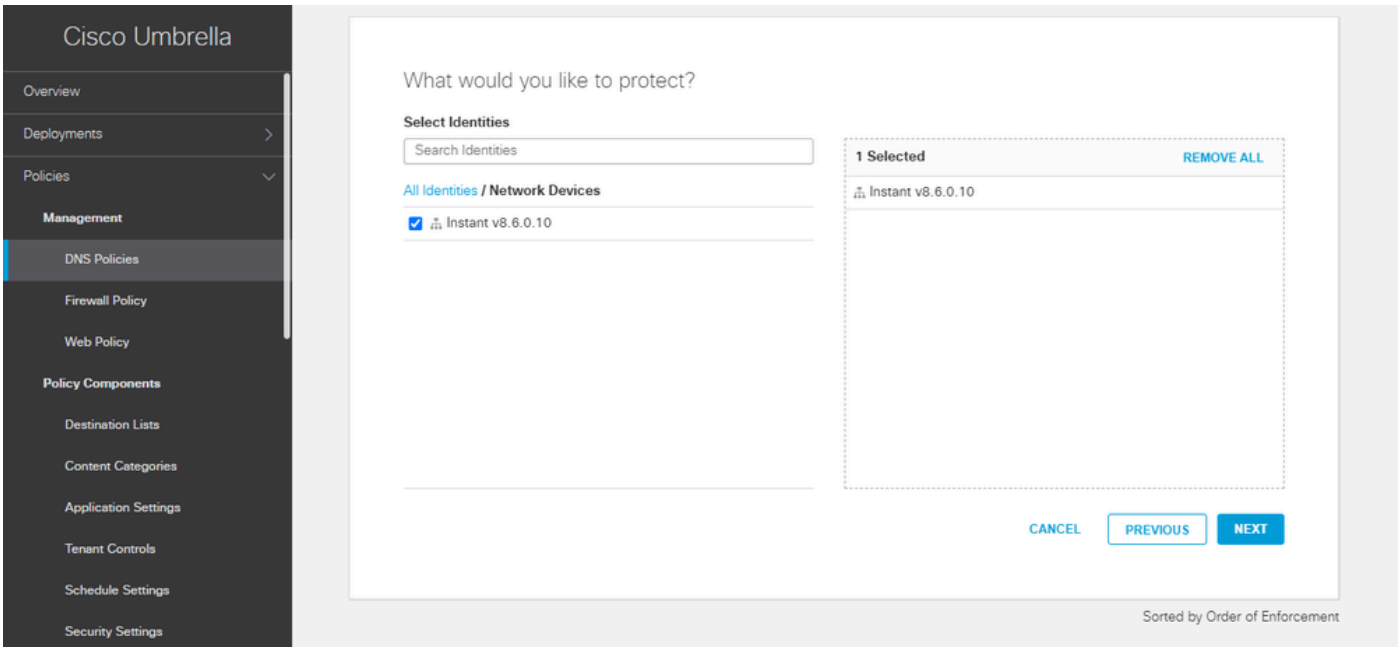


4404011756308

DNS-beleid toepassen

In Umbrella bevat het "Standaardbeleid" automatisch alle identiteiten (zoals netwerkapparaten) die aan een dashboard zijn toegevoegd. Het is niet nodig om extra DNS-beleid te maken als alle AP-clusters in uw implementatie aan hetzelfde beleid kunnen worden onderworpen. Als dit voor u het geval is, gaat u naar de volgende sectie.

Als u een aangepast beleid wilt toepassen op een specifiek netwerkapparaat, moet u een nieuw beleid toevoegen in het overkoepelende dashboard onder Beleid > Alle beleidsregels (DNS-beleid) en het netwerkapparaat selecteren in het beleid.



4404011773588

Wanneer er meer dan één beleid op de pagina DNS-beleid (Alle beleidsregels) staat, wordt het

beleid van boven naar beneden geëvalueerd op basis van een eerste overeenkomst. Zie de documentatie over beleidsprioriteiten en de beste praktijken voor het definiëren van beleidsdocumentatie voor meer informatie.

Interne DNS

In een omgeving waar interne DNS-servers bestaan en u DNS-query's voor bepaalde (interne) domeinen wilt doorsturen naar de interne DNS-servers, kunt u de functie Enterprise Domains in Instant gebruiken.

DNS-query's kunnen worden onderschept door een AP-cluster nadat de functie is ingeschakeld, behalve dat query's voor de opgegeven domeinen niet langer kunnen worden doorgestuurd naar Umbrella. In plaats daarvan kunnen ze worden doorgestuurd naar de IP-adressen van de DNS-server die oorspronkelijk zijn geconfigureerd op de NIC's van de draadloze clients (zoals via DHCP). De functie is vergelijkbaar met de functionaliteit Interne domeinen die beschikbaar is in standaard Umbrella-implementatiemethoden (met virtuele apparaten), waarbij de Aruba Instant-integratie niet wordt gebruikt.

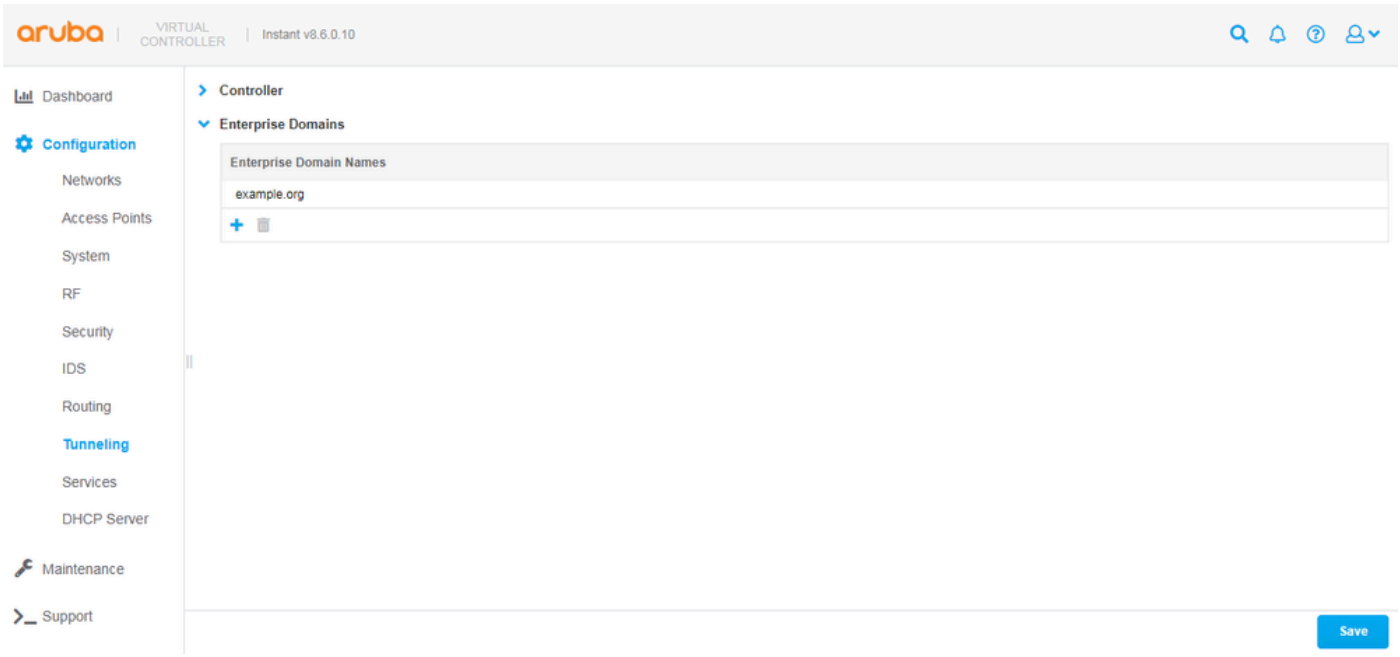
U configureert de functie als volgt op een Instant Virtual Controller:

1. Navigeer naar Configuratie > Tunneling > Enterprise Domains.

2. Domeinnamen toevoegen aan of verwijderen uit de lijst Enterprise Domain Names.

3. Selecteer Opslaan.

Er is een impliciete wildcard voor elk domein toegevoegd aan de lijst, dus example.org impliceert *.example.org.



4404238114452

Verificatie

Of u Umbrella op uw WLAN hebt geïmplementeerd met behulp van de standaardmethoden waarnaar wordt verwezen in het gedeelte "Implementatieoverzicht" van deze handleiding, of de integratie die wordt beschreven in het gedeelte "Aruba Instant Integration", u kunt controleren of draadloze clients Umbrella DNS gebruiken door van een van de clients naar https://welcome.umbrella.com/ te bladeren. U ziet dan een groene controle vergelijkbaar met de schermafbeelding weergegeven in de Umbrella documentatie.

4404011960212

U kunt dit ook controleren door deze opdracht uit te voeren in de opdrachtprompt van een draadloze client.

```
nslookup -type=txt debug.opendns.com.
```

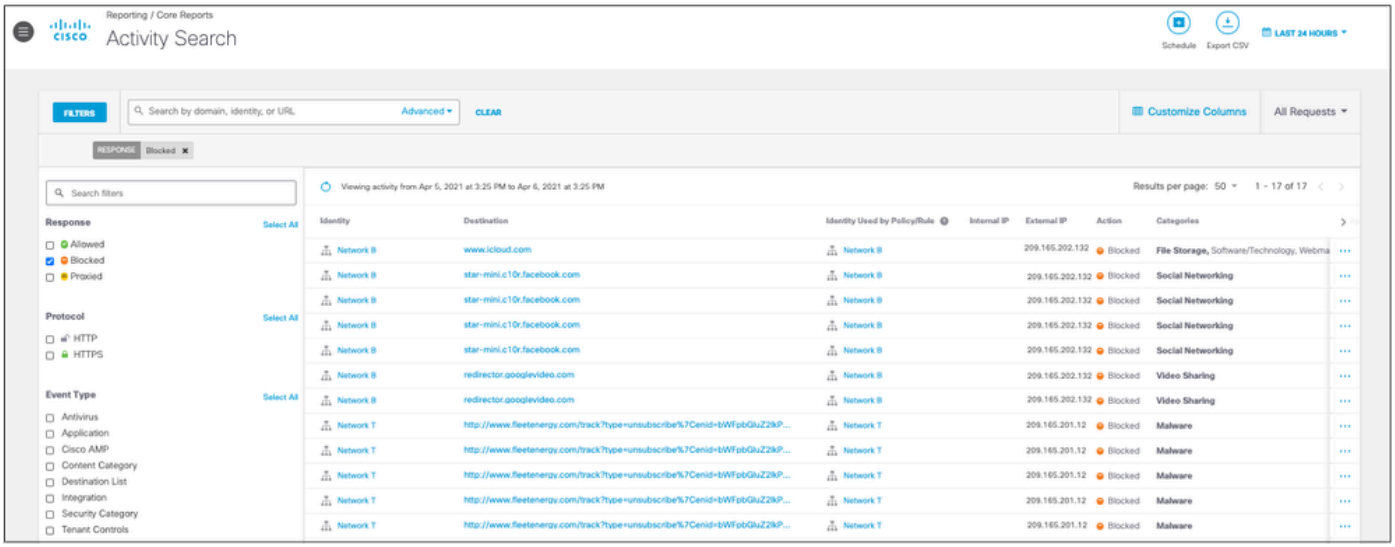
U kunt een uitvoer zien met een aantal tekstregels, vergelijkbaar met deze schermafbeelding:

```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id
debug.opendns.com       text = "appliance id
debug.opendns.com       text = "host id
debug.opendns.com       text = "user id
debug.opendns.com       text = "remoteip
debug.opendns.com       text = "flags
debug.opendns.com       text = "id
debug.opendns.com       text = "source
debug.opendns.com       text = "fw: flags
debug.opendns.com       text = "fw: id
debug.opendns.com       text = "fw: source

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

Vanuit de opdrachtuitvoer kunt u de org-ID van uw Umbrella-dashboard zien in de regel "orgid" of "organisatie-id" en als u de Instant-integratie gebruikt, kunt u de extra regel "apparaat" zien die een apparaat-ID bevat.

Als u DNS-query's in uw Umbrella-dashboard wilt bekijken, gaat u naar Rapportage > Zoeken naar activiteiten. Merk op dat het enige tijd (ongeveer 15 minuten) kan duren voordat vragen worden weergegeven in de GUI van het dashboard. Instructies voor het gebruik van Activity Search zijn beschikbaar op in de overkoepelende documentatie.



4404019393044

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.