Cisco Umbrella op uw netwerk configureren via routers uit de RV34x-reeks

Inleiding

Vanaf firmware versie 1.0.0.2.16 ondersteunen de RV34x-routers nu Cisco Umbrella. Umbrella gebruikt DNS als verdedigingsvector of schild in verdediging tegen malware en data-inbraken.

Toepasselijke apparaten

- RV340x Series-router

Softwareversie

- 1.0.02.16

Vereisten

- Een actieve parapluaccount (geen account hebben? Offerte aanvragen of een gratis proefversie starten)

Doel

Dit hoe te leiden zal u de stappen tonen die betrokken zijn bij het integreren van het beveiligingsplatform van Umbrella in uw netwerk. Voordat we in de nitty gritty details gaan, zullen we een paar vragen beantwoorden die u misschien zelf stelt over Umbrella.

Wat is paraplu?

Umbrella is een eenvoudig maar zeer effectief cloud security platform van Cisco. Umbrella opereert in de cloud en voert veel security gerelateerde diensten uit. Van opkomende dreiging tot onderzoek na een gebeurtenis. Umbrella ontdekt en voorkomt aanvallen in alle havens en protocollen.

Hoe werkt het?

Umbrella gebruikt DNS als haar belangrijkste verdedigingsvector. Wanneer gebruikers een URL invoeren in hun browserbalk en op Enter klikken, neemt Umbrella deel aan de overdracht. Die URL gaat over naar Umbrella's DNS-oplosser en als een veiligheidswaarschuwing aan het domein gekoppeld is, wordt het verzoek geblokkeerd. Deze telemetriegegevens worden overgebracht en in microseconden geanalyseerd, toevoegend bijna geen latentie. Telemetriegegevens maken gebruik van logboeken en instrumenten om miljarden DNS-verzoeken wereldwijd te traceren. Als deze gegevens

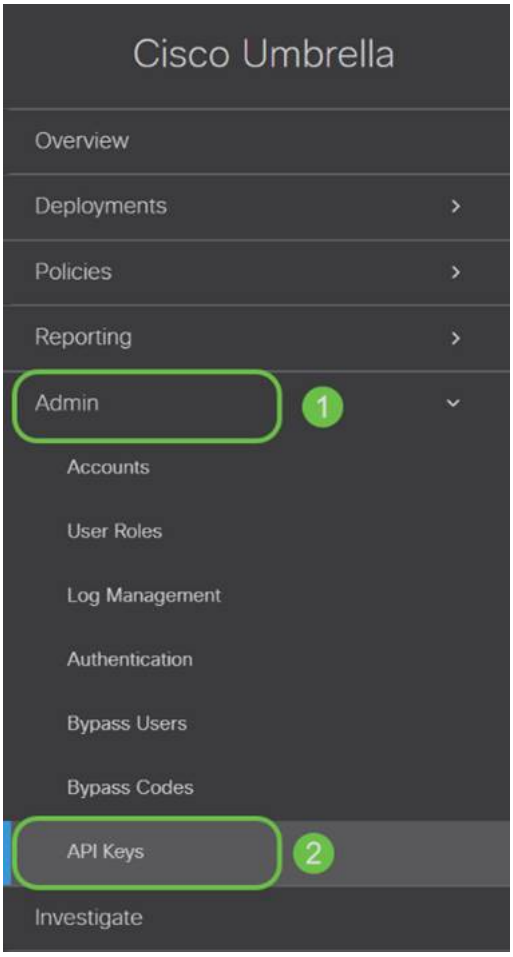
alomtegenwoordig zijn, maakt een wereldwijde correlatie een snelle reactie op aanvallen mogelijk zodra ze beginnen. Zie het privacybeleid van Cisco hier voor meer informatie - volledig beleid, overzichtsversie. Denk aan telemetriegegevens als gegevens die uit hulpmiddelen en logboeken worden afgeleid.

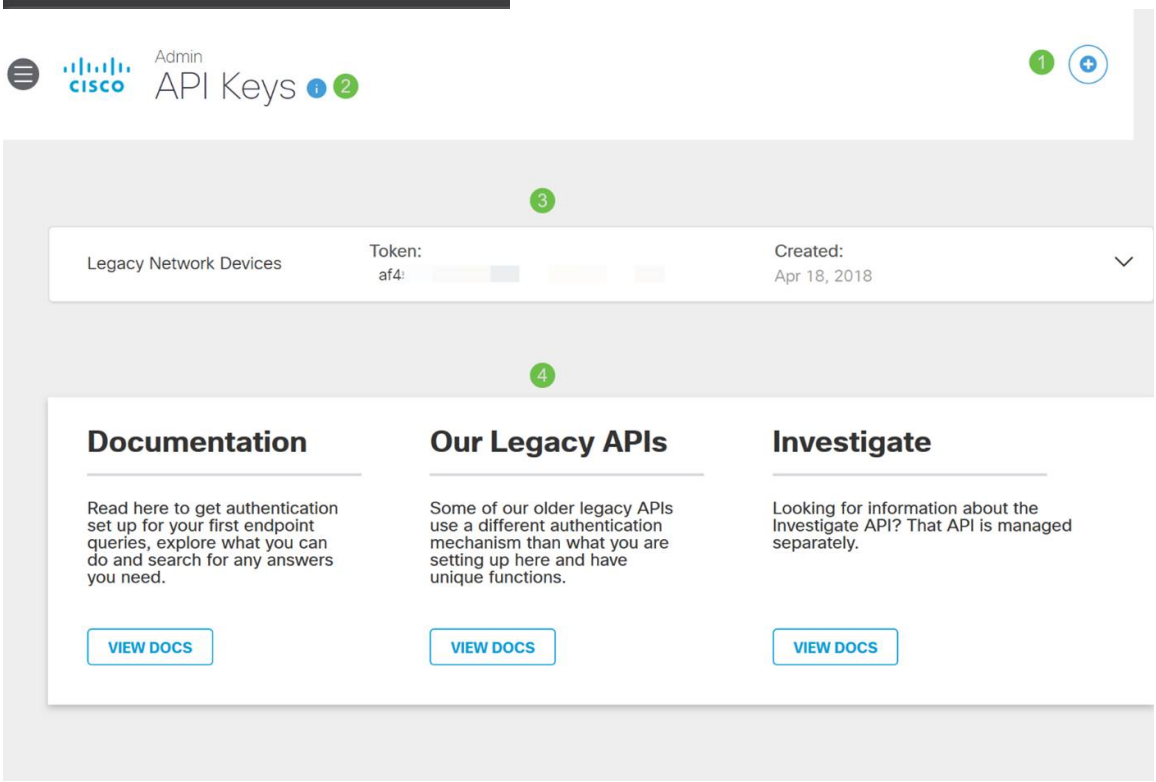
Samengevat in een metafoor: stel je voor dat je op een feestje bent. Op dit feestje is iedereen aan het surfen op het web. De stilte van de groep wordt getekend door de bezoekers van de feestjes die op hun schermen tikken. Het is geen groot feest, maar terwijl je op je eigen telefoon een hyperlink ziet naar een kitten GIF die onweerstaanbaar lijkt. De URL lijkt echter twijfelachtig, dus je weet niet zeker of je moet tikken of niet. Dus voordat je op de hyperlink tikt, roep je de rest van het feest "Is deze link slecht?" Als iemand van het feestje naar de link is geweest en ontdekt heeft dat het om oplichting ging, zouden ze roepen: "Ja, dat heb ik gedaan en het is oplichterij!" Je bedankt die persoon dat hij je heeft gered en dat hij je nobele zoektocht naar foto's van schattige dieren heeft voortgezet. Natuurlijk worden op de schaal van Cisco dit type verzoek- en terugbelbeveiligingscontroles miljoenen malen per seconde uitgevoerd, en dat is ten voordele van de beveiliging op uw netwerk.

Klinkt goed, hoe maken we dit af?

Waar deze gids navigeert, begint door de API-sleutel en de Secret-sleutel van uw Umbrella account dashboard te grijpen. Daarna loggen we in op uw routerapparaat om de API en Secret-toets toe te voegen. Als u problemen ondervindt, raadpleegt u hier documentatie en hier Umbrella Support-opties.

Stap 1. Na het inloggen op uw Umbrella-account klik vanaf het scherm van het *Dashboard* op **Admin > API-toetsen**.



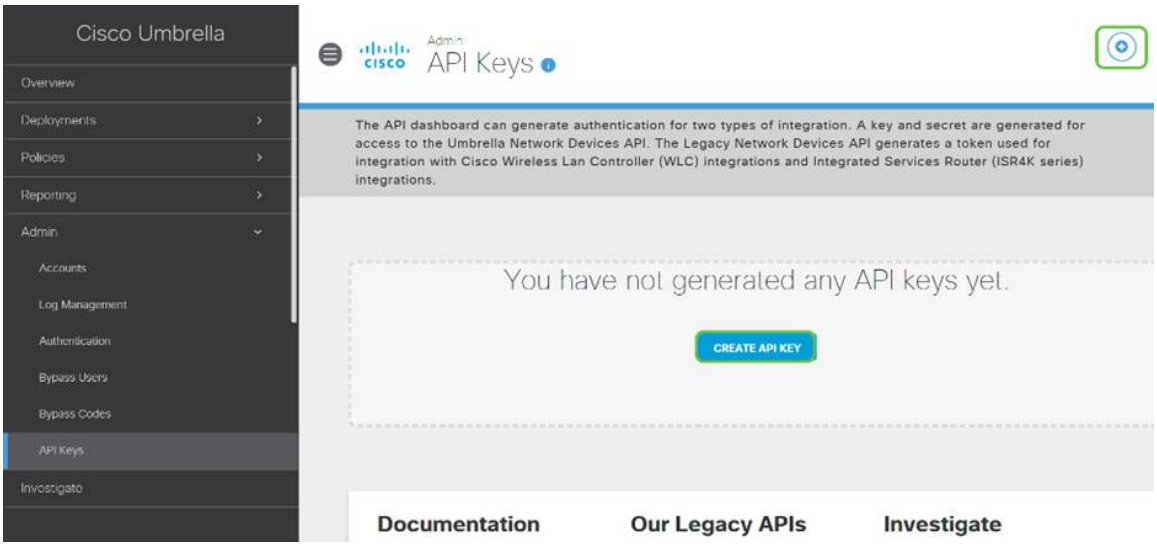


Anatomie van het scherm API-sleutels (met bestaande API-toets) -

1. Voeg API-sleutel toe - hiermee wordt de aanmaak van een nieuwe sleutel gestart voor gebruik met de Umbrella API.
2. Extra informatie - schuift neer/omhoog met een uitleg voor dit scherm.
3. Token Well - Bevat alle sleutels en tokens die door dit account zijn gemaakt. (Populeert zodra een sleutel is gemaakt)

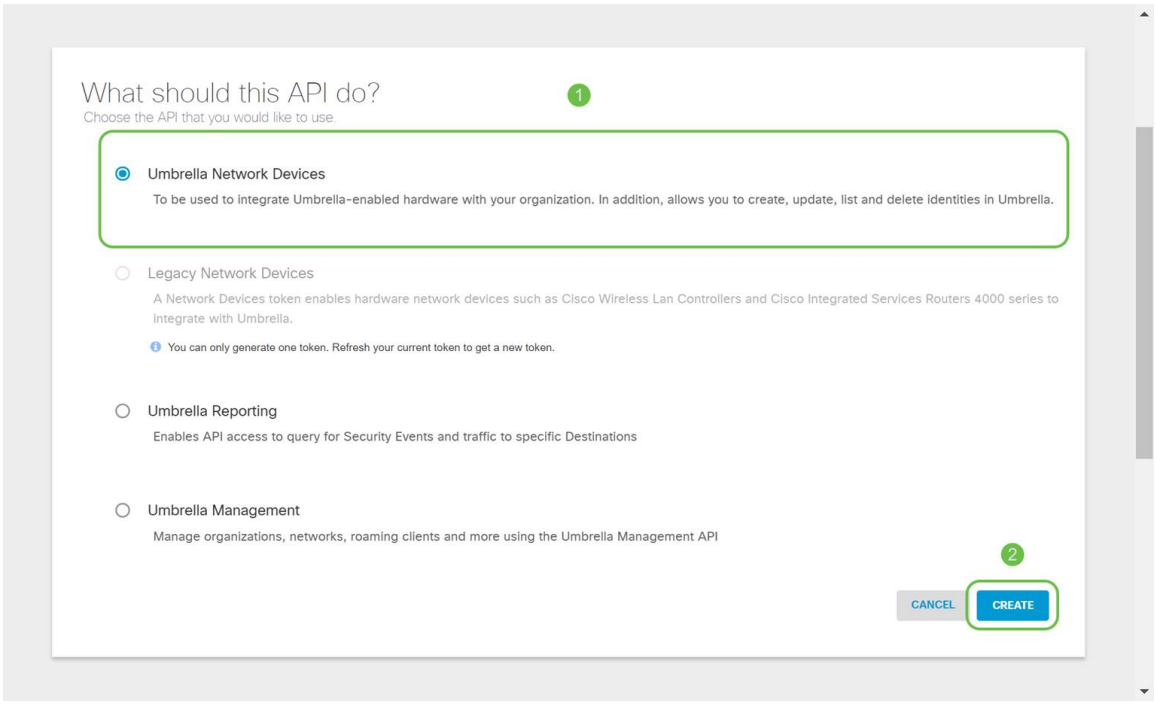
4. Ondersteunende documenten - Koppelingen naar documentatie op de Umbrella-site met betrekking tot de onderwerpen in elke sectie.

Stap 2. Klik op de knop **Add API Key** in de rechterbovenhoek of klik op de knop **Create API Key**. Ze werken allebei hetzelfde.

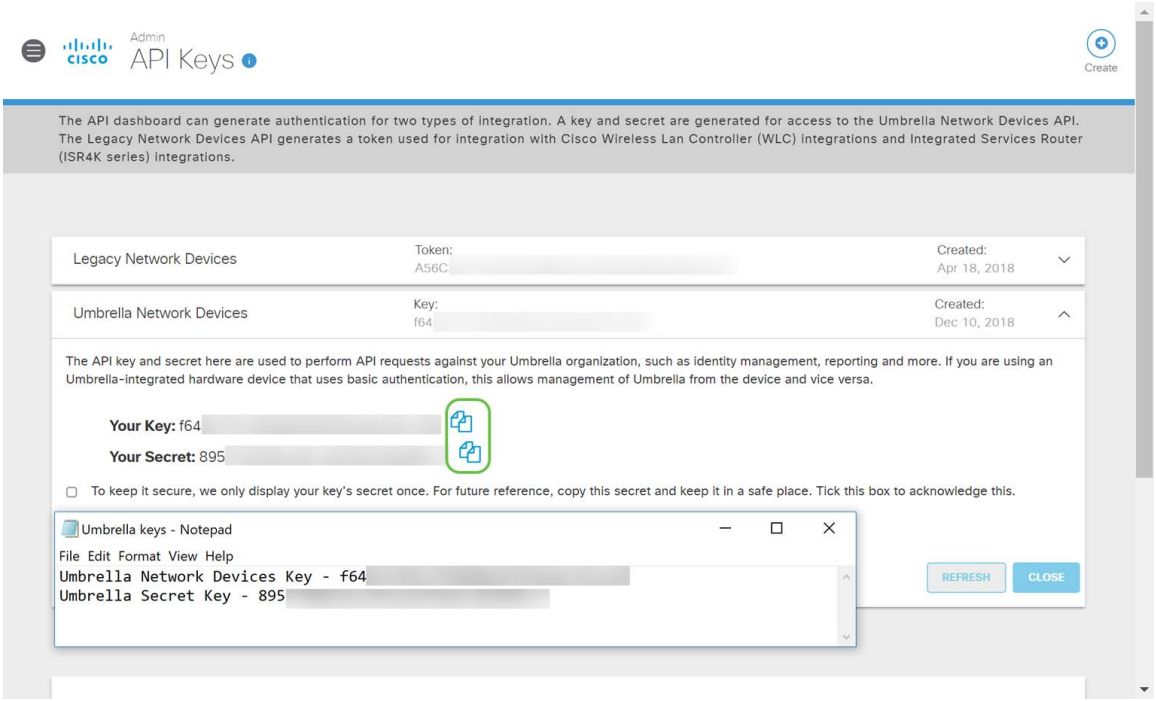


Opmerking: de bovenstaande screenshot zou gelijk zijn aan wat u ziet als u dit menu voor het eerst opent.

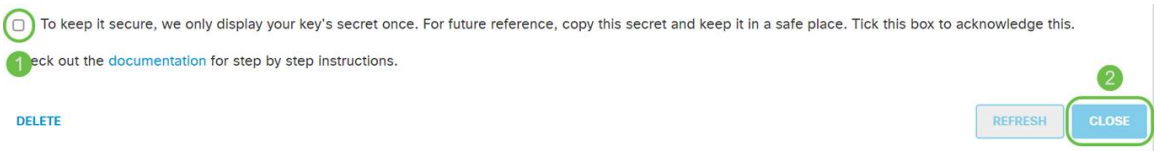
Stap 3. Selecteer **Umbrella Network Devices** en klik vervolgens op de knop **Create**.



Stap 4. Open een teksteditor zoals notitieblok en klik vervolgens op de knop **Kopiëren** rechts van uw API en API *Secret Key,* een pop-upmelding zal bevestigen dat de sleutel wordt gekopieerd naar uw klembord. Steek één voor één uw geheim en API-sleutel in het document, en plak deze voor later gebruik. In dit geval is het label "Umbrella network devices key". Sla het tekstbestand vervolgens op op een veilige locatie die later eenvoudig toegankelijk is.



Stap 5. Nadat u de sleutel en de geheime sleutel naar een veilige locatie hebt gekopieerd, klikt u vanaf het *scherm Umbrella API* op het **selectievakje** om te bevestigen dat u de tijdelijke weergave van de geheime sleutel bevestigt, en klikt u vervolgens op de knop **Sluiten**.



Belangrijke opmerking: als u de geheime sleutel kwijtraakt of per ongeluk verwijdert, is er geen functie of ondersteuningsnummer om te bellen om deze sleutel op te halen. Hou het geheim, hou het veilig. Indien verloren, moet u de sleutel verwijderen en opnieuw autoriseren van de nieuwe API-sleutel met elk apparaat dat u wilt beschermen met Umbrella.

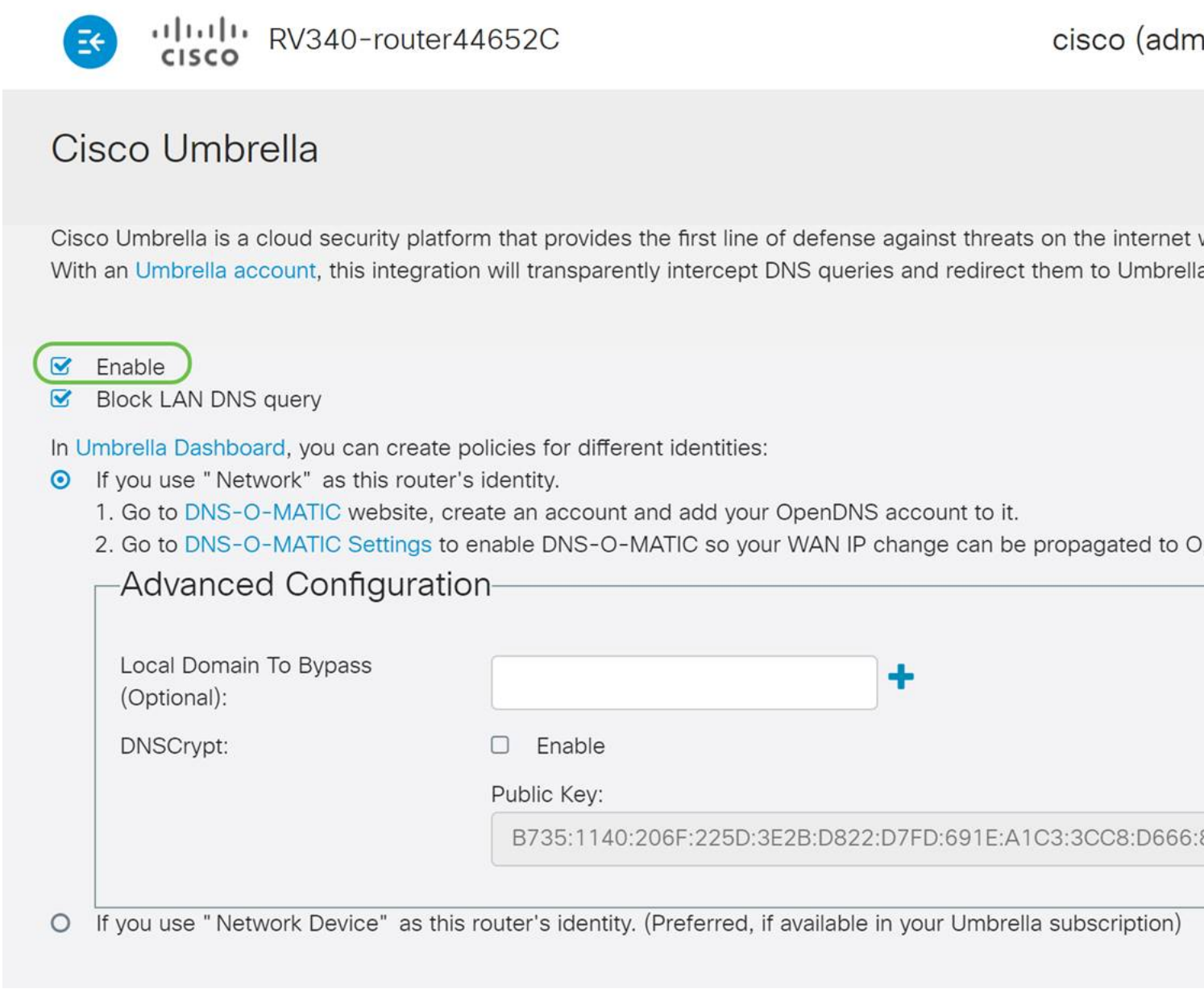
Best practices: Houd slechts één kopie van dit document op een apparaat, zoals een USB-thumbdrive, ontoegankelijk vanaf een netwerk.

Umbrella configureren op uw RV34x-apparaat

Nu we API-sleutels hebben gemaakt binnen Umbrella, nemen we deze sleutels en installeren ze op onze RV34x-apparaten. In ons geval gebruiken we een RV340.

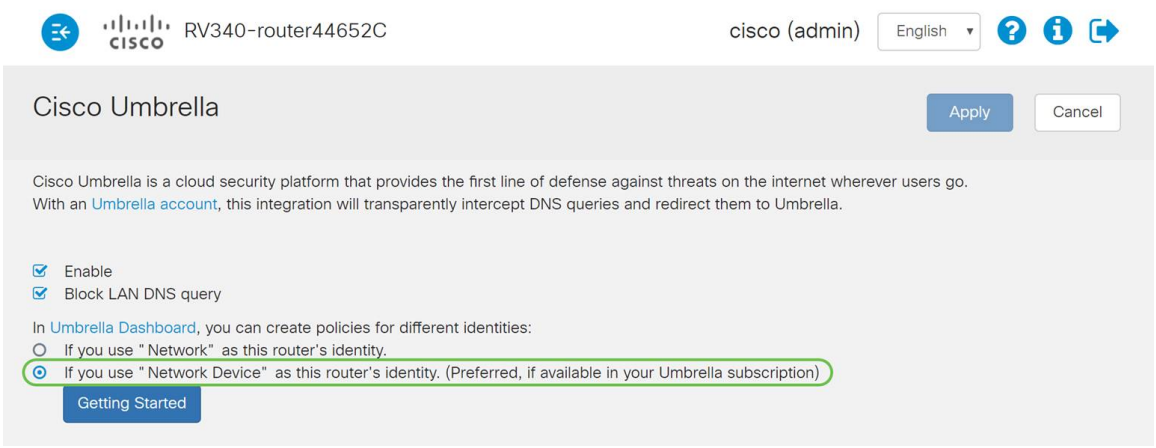
Stap 1. Na het inloggen op uw RV34x-apparaat, klik op **Security > Umbrella** in het knoppenmenu.

Stap 2. Het scherm van de Umbrella API heeft een reeks opties, begin het toelaten van Umbrella door checkbox te klikken **Enable**.

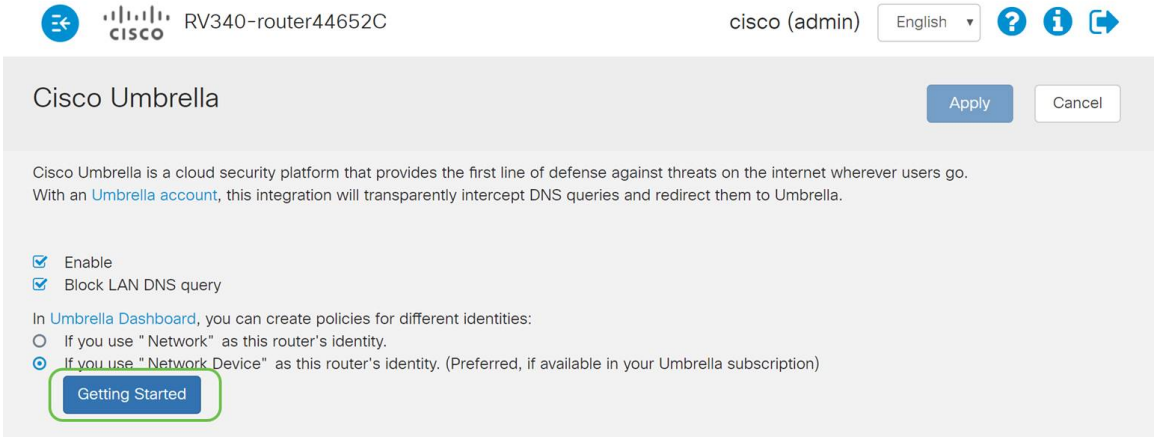


Stap 3. (Optioneel) Standaard is het vak Blok LAN DNS-vragen geselecteerd, deze nette functie maakt automatisch toegangscontrolelijsten op uw router die voorkomen dat DNS-verkeer naar het internet gaat. Deze functie dwingt alle domeinvertaalaanvragen om via de RV34x te worden geleid en is een goed idee voor de meeste gebruikers.

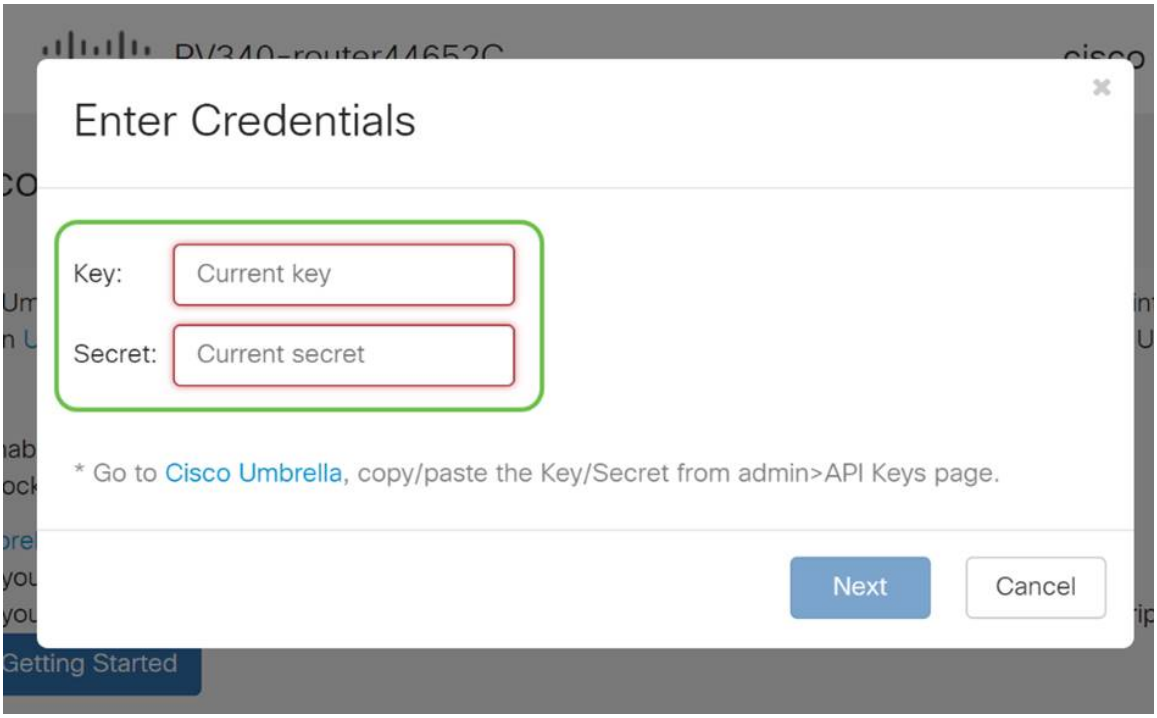
Stap 4. De volgende stap speelt zich op twee verschillende manieren uit. Ze zijn allebei afhankelijk van de installatie van uw netwerk. Als u een dienst zoals DynDNS of NoIP gebruikt, zou u het standaard naamgevingsschema van "Network" verlaten. Dan moet u inloggen op die account om Umbrella interfaces met die diensten te verzekeren, omdat het bescherming biedt. Voor onze doeleinden vertrouwen we op "Network Device", klik op de onderste radiale knop.



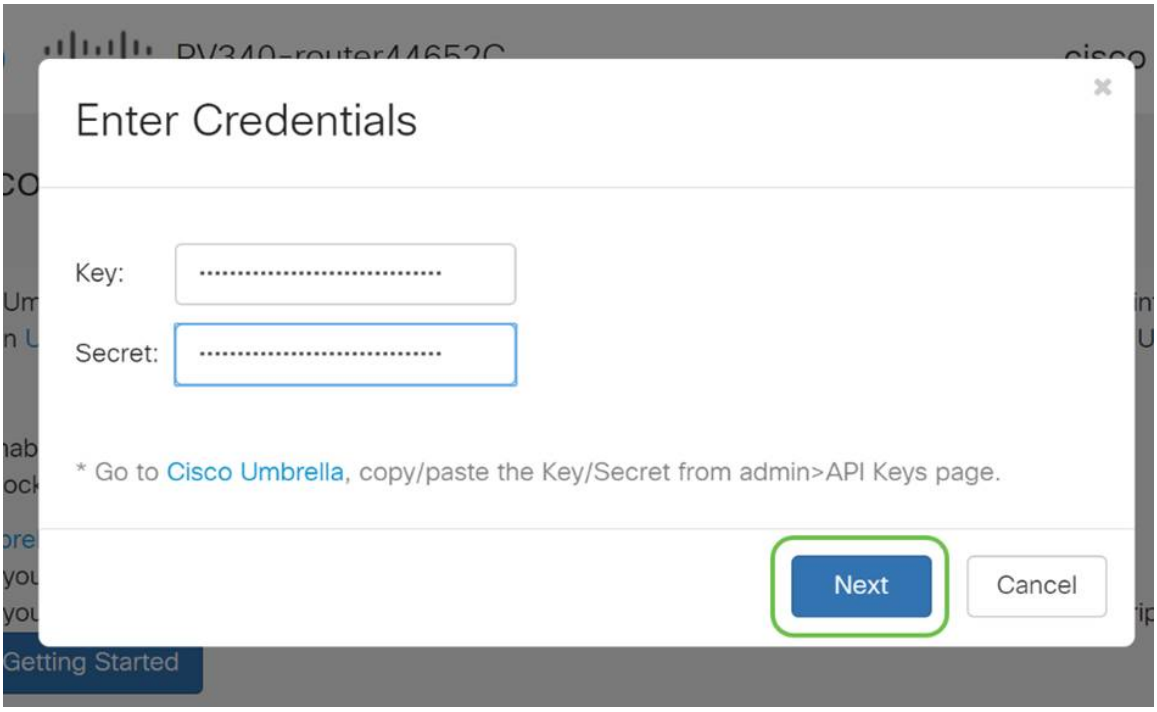
Stap 5. Klik nu op **Aan de slag** om de mini-wizard te starten.



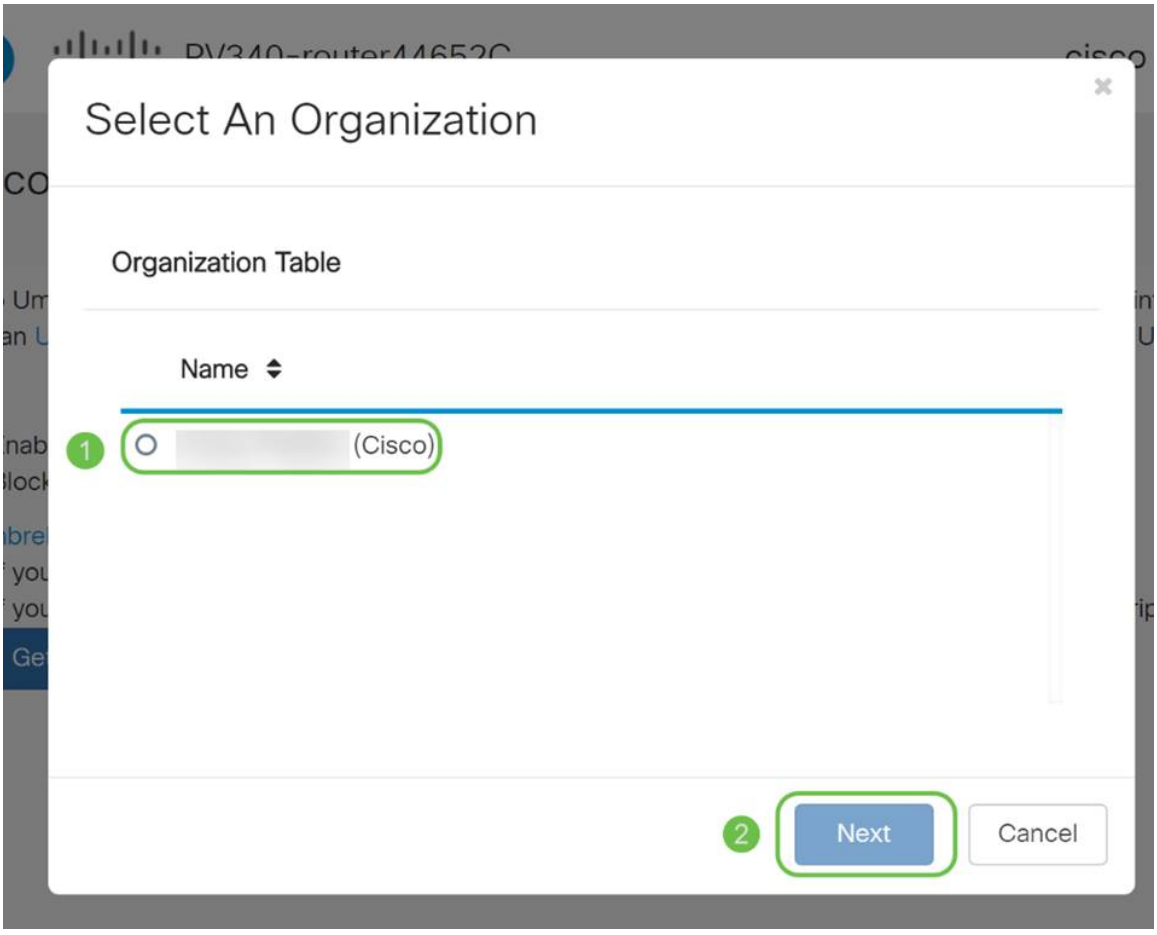
Stap 6. Voer nu de **API Key** en **Secret Key** in de tekstvakken.



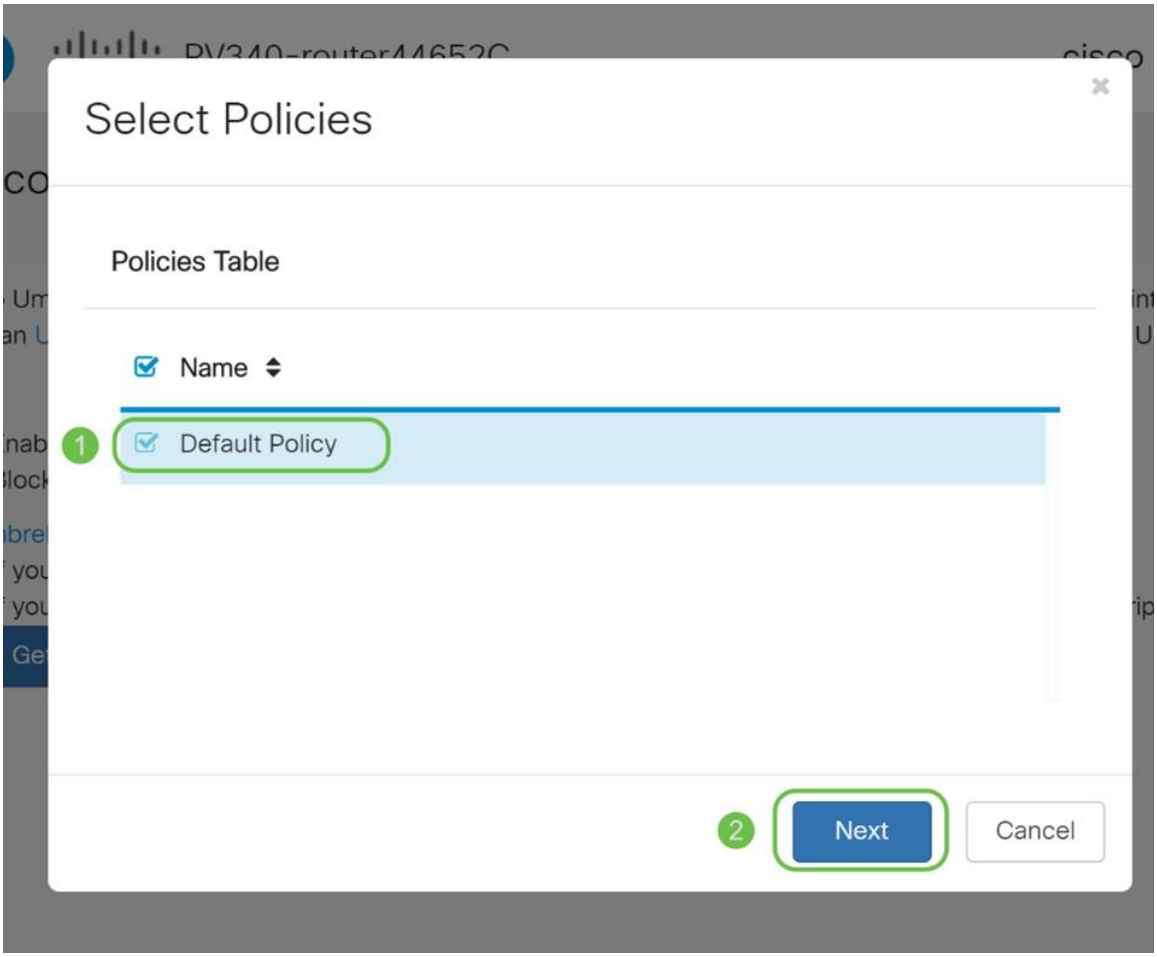
Stap 7. Na het invoeren van uw API en geheime sleutel klik op de **Volgende** knop.



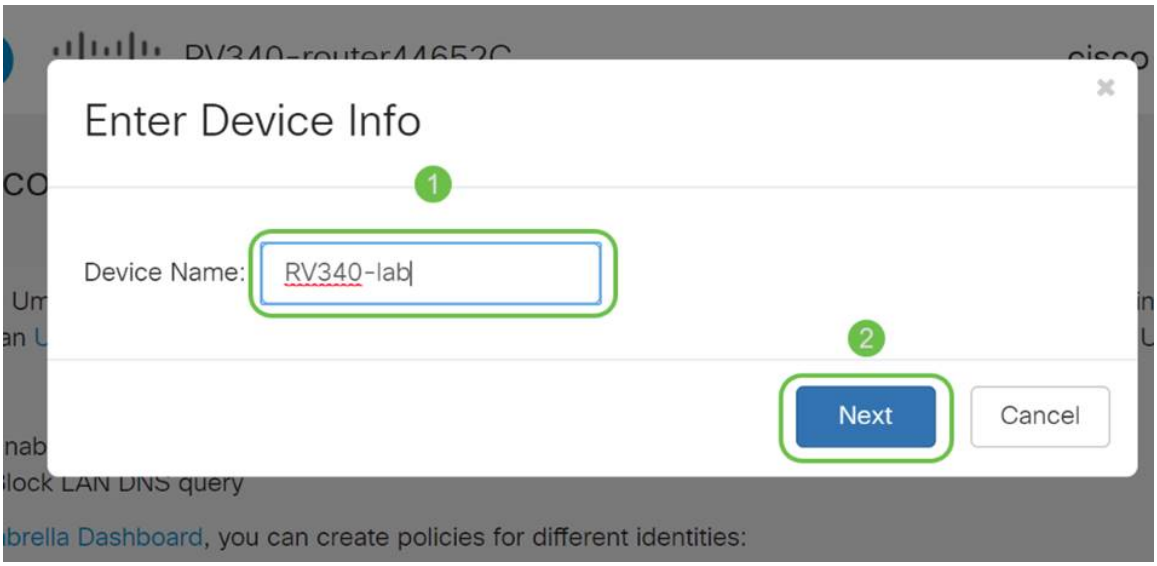
Stap 8. Selecteer in het volgende scherm de **organisatie** die u aan de router wilt koppelen en klik op **Volgende**.



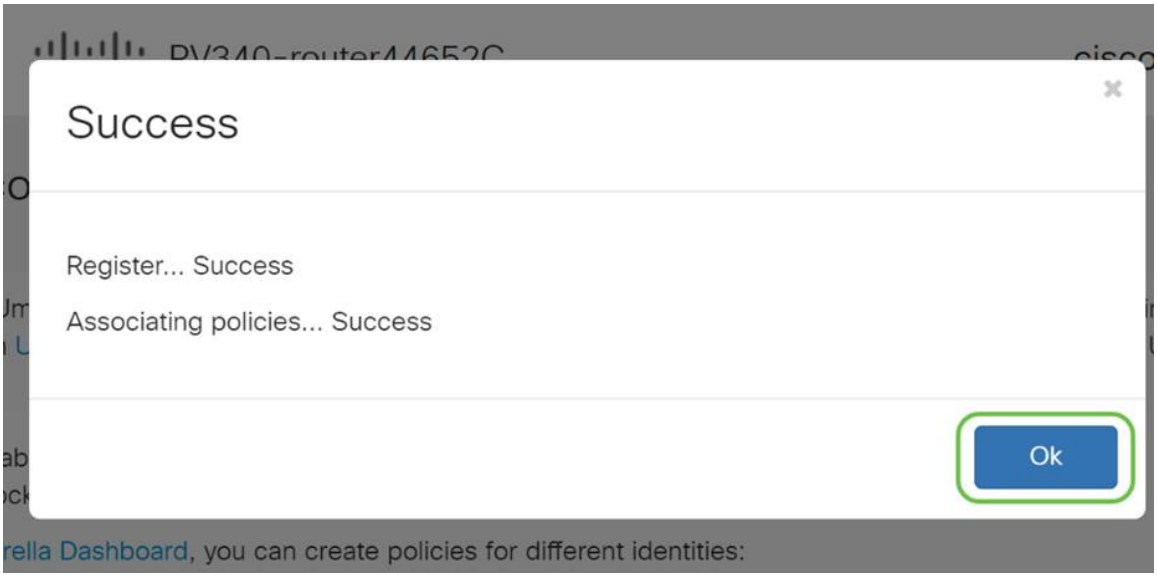
Stap 9. Selecteer nu het beleid dat op verkeer moet worden toegepast dat door de RV34x wordt gerouteerd. Voor de meeste gebruikers zal het standaardbeleid voldoende dekking bieden.



Stap 10. **Geef een naam** aan het hulpmiddel zodat dit in de Umbrella-rapportage kan worden aangeduid. In onze installatie hebben we "RV340-lab" toegewezen.



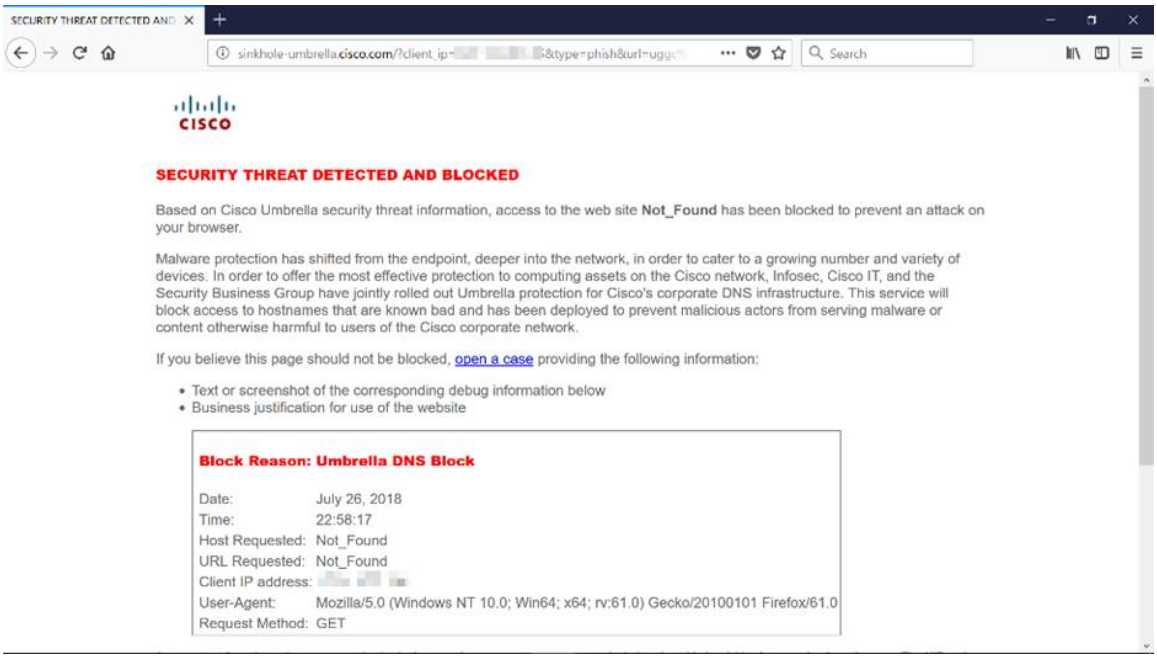
Stap 11. Het volgende scherm zal uw gekozen instellingen valideren en een update geven, wanneer de koppeling met succes op **OK** wordt gekoppeld.



Bevestigen dat alles op zijn plaats is

Gefeliciteerd, u bent nu beschermd door Cisco's Umbrella. Of wel? Laten we zeker zijn door te dubbelcontroleren met een live voorbeeld. Cisco heeft een website gemaakt die erop gericht is dit zo snel als de pagina wordt geladen te bepalen. Klik hier of typ https://InternetBadGuys.com in de browser balk.

Als Umbrella goed is geconfigureerd, wordt u verwelkomd door een scherm vergelijkbaar met dit!



Bekijk een video met betrekking tot dit artikel...

Klik hier om andere Tech Talks van Cisco te bekijken

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.