Probleemoplossing recente melding 802.1X fout in Meraki-apparaat

Inhoud

Inleiding

In dit document wordt beschreven hoe de recente melding van 802.1X-fouten in het Meraki-apparaat moet worden opgelost.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Begrijp de basisoplossing van Meraki voor softwaregedefinieerde Wide Area Network (SDWAN)
- Basistoegangsbeleid en radiofrequentie-verificatie begrijpen

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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 levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

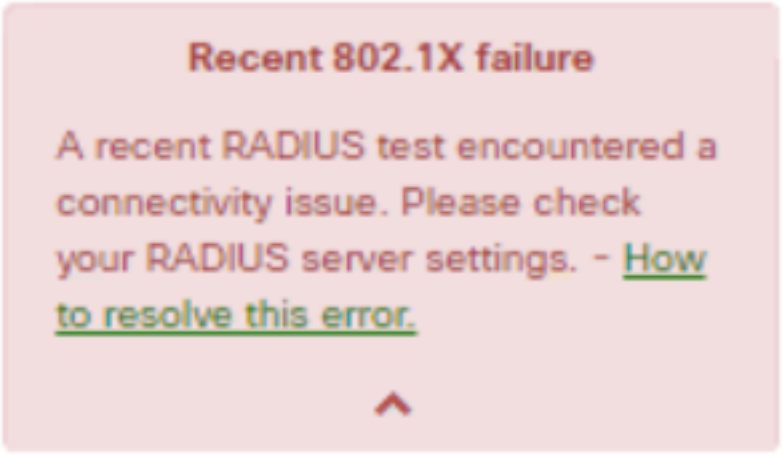
Probleem

Meraki-apparaten gebruiken de AAA-serverbeleidsconfiguratie om de eindgebruiker voor het eerst te authentiseren.

Wat is de RADIUS-test in Meraki-apparaten?

De recente melding van 802.1X is weergegeven. Als de periodieke berichten met een toegangsaanvraag die naar de geconfigureerde RADIUS-servers zijn verzonden, onbereikbaar zijn, moet u een tijdelijke periode van 10 seconden gebruiken.

Meraki-apparaten sturen regelmatig berichten met een toegangsaanvraag naar de geconfigureerde RADIUS-servers die een identiteit **meraki_8021x_test** gebruiken om er zeker van te zijn dat de RADIUS-servers bereikbaar zijn. Deze toegangsaanvragen hebben een onderbreking van 10 seconden en als de RADIUS-server niet reageert, worden de Straalservers onbereikbaar geacht en wordt de waarschuwing "Recent 802.1X fail" bericht gevraagd. Raadpleeg de screenshot van de waarschuwing op het apparaat:



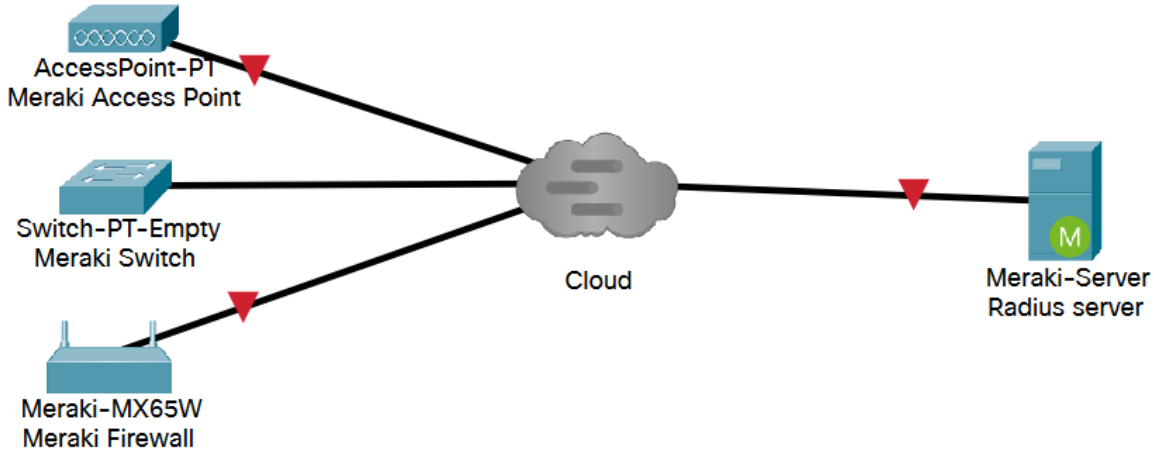
Een test wordt als succesvol beschouwd als het Meraki-apparaat een legitieme RADIUS-respons (Access-Accept/Afwerp/Challenge) van de server ontvangt.

Als de RADIUS-test is ingeschakeld, worden alle RADIUS-servers minstens één keer per 24 uur op elk knooppunt uitgevoerd, ongeacht het testresultaat. Als een RADIUS-test voor een bepaald knooppunt mislukt, wordt elk uur opnieuw getest tot een resultaat dat doorgaat. Een volgende pas tekent de server bereikbaar, ontruimt de waakzaamheid en keert terug naar de testcyclus van 24 uur.

Configureren

Netwerkdiagram

Hier is een eenvoudig topologiediagram dat de instellingen beschrijft:



Probleemoplossing controleren

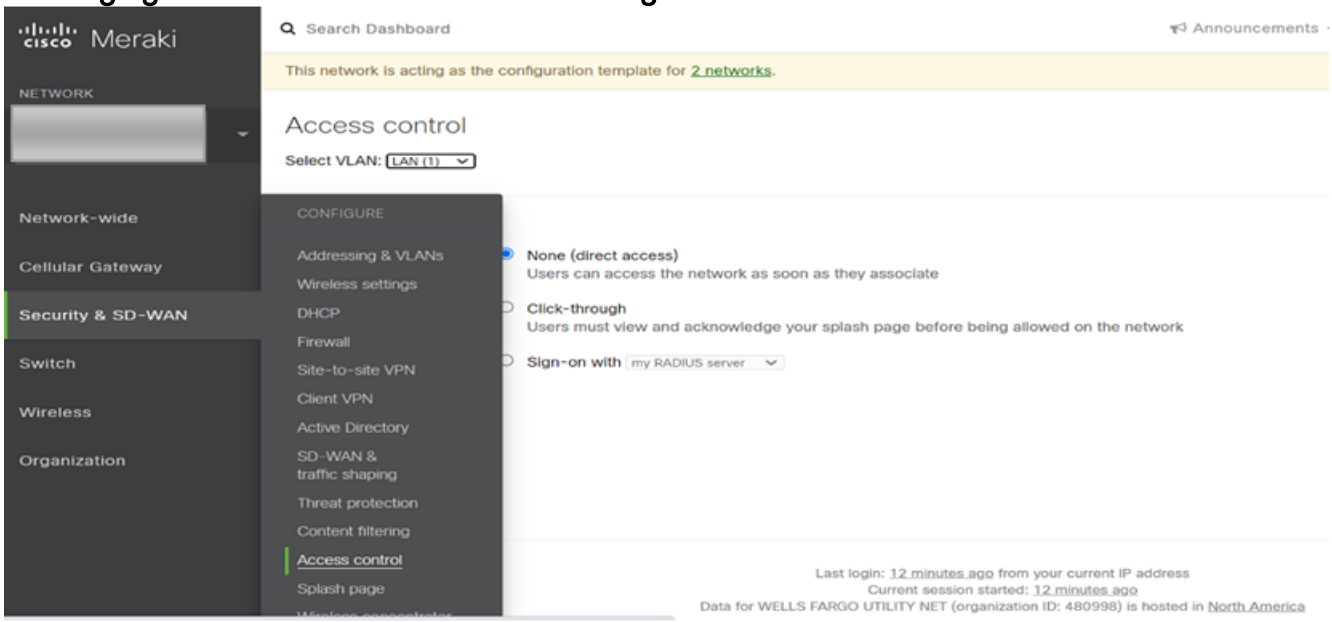
802.1x-configuratie

De configuratie van 802.1X RADIUS kan worden gevonden in het afgebeelde pad dat afhankelijk is van het Meraki-productmodel.

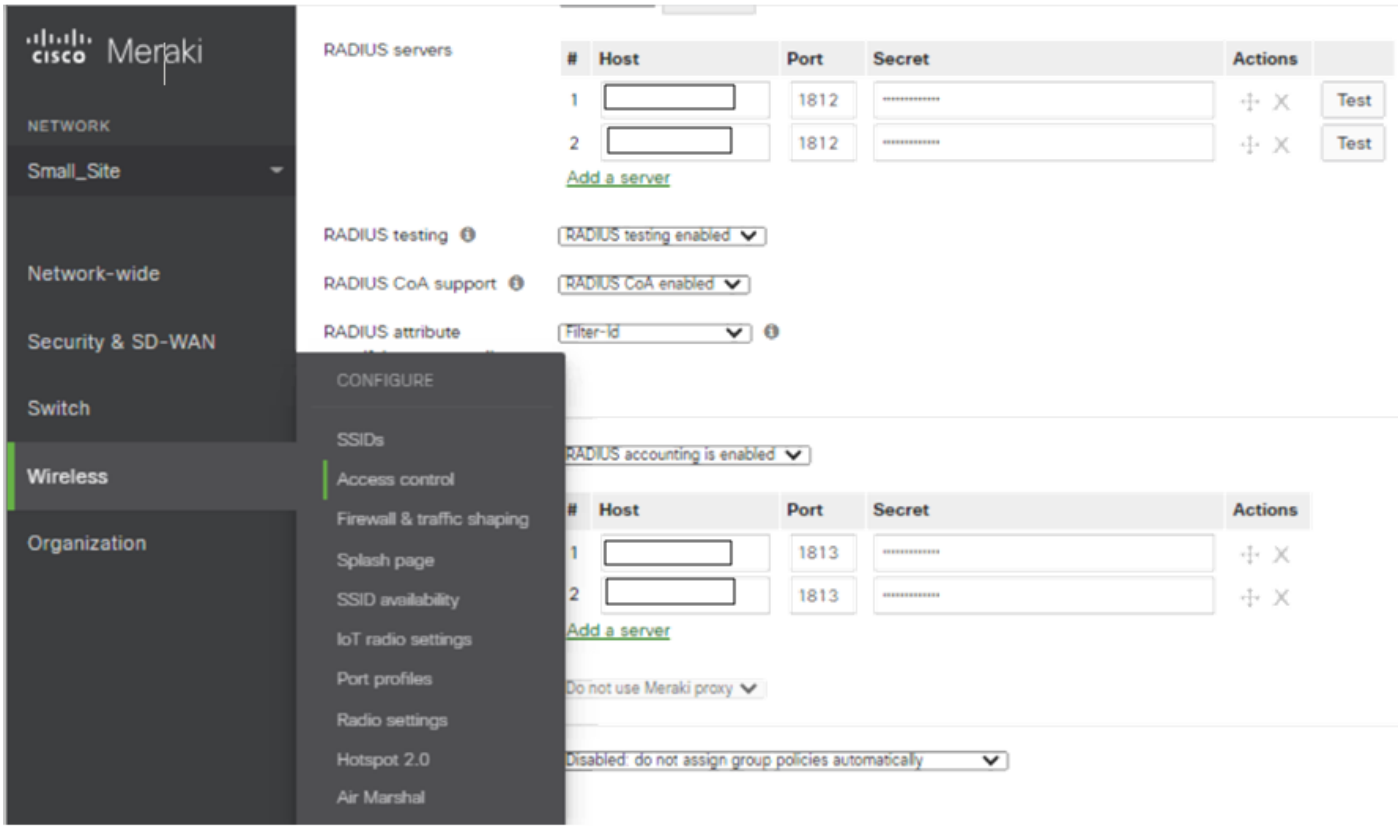
1. MGX-security applicatie (geconfigureerd voor ofwel toegangsporten ofwel draadloos)

- Voor toegangspoorten
  Security en SD-WAN > adressering en VLAN's

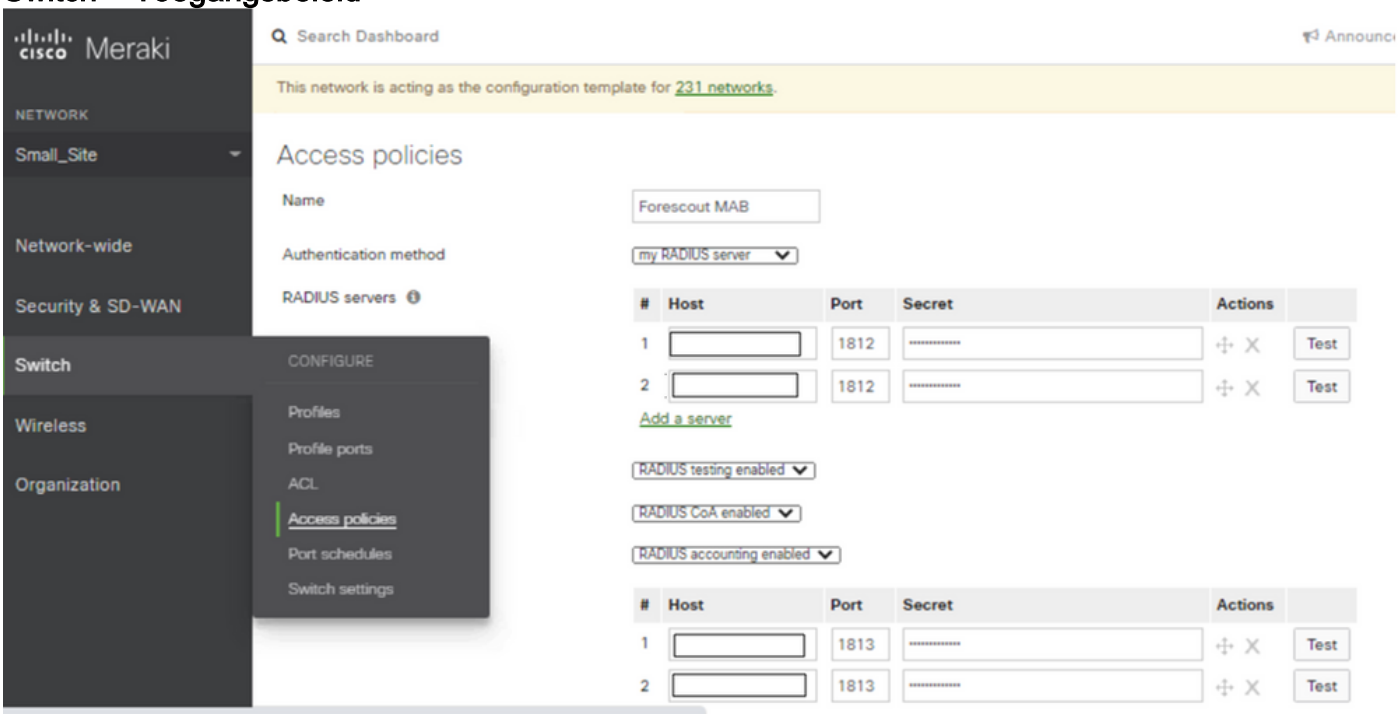
- Voor draadloos
  Beveiliging en SD-WAN > Draadloze instellingen



2. MR-access points (ingeschakeld op basis van een SSID (Service Set Identifier)):
Draadloos > toegangscontrole



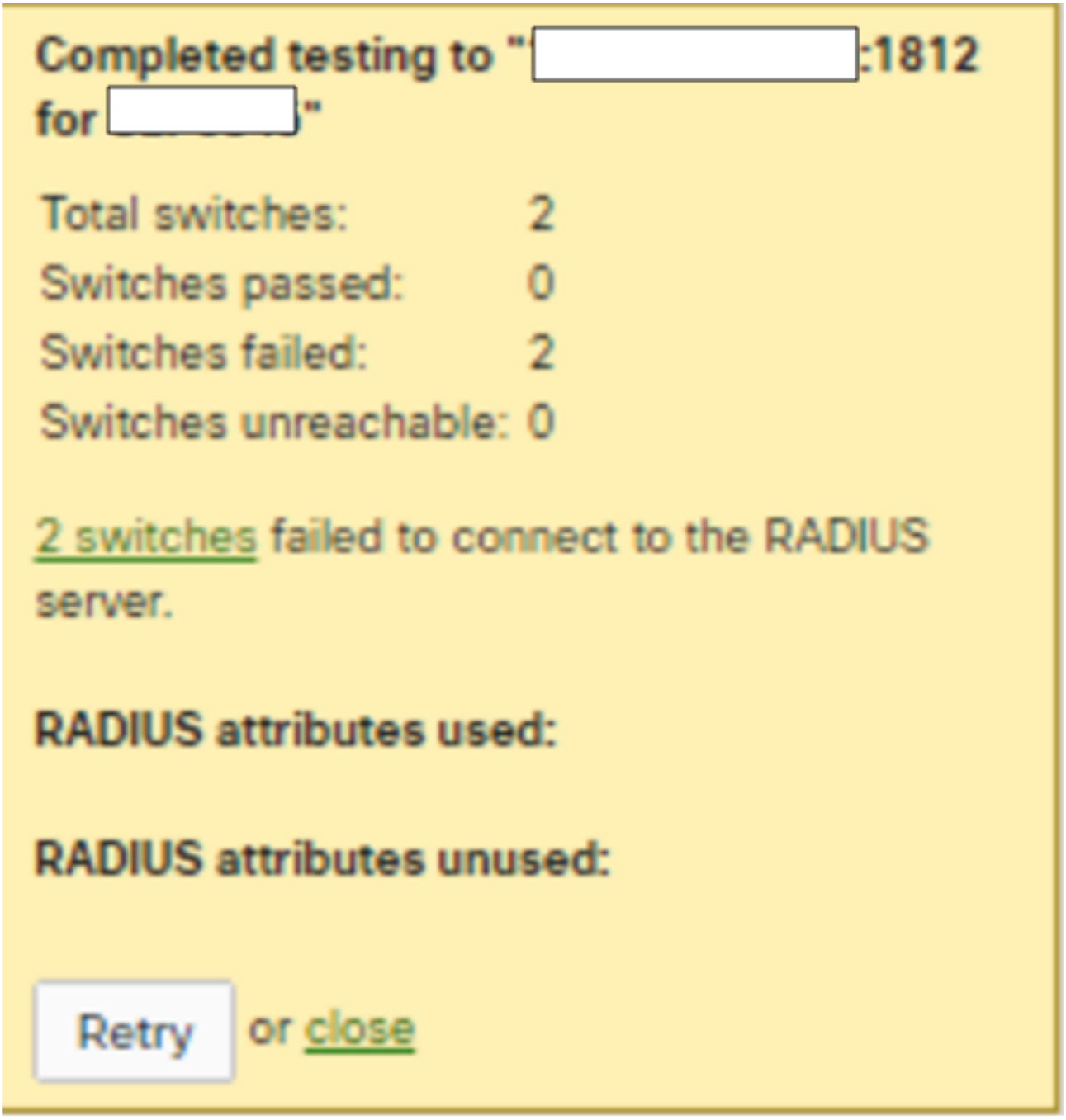
3. MS-Switches
Switch > Toegangsbeleid



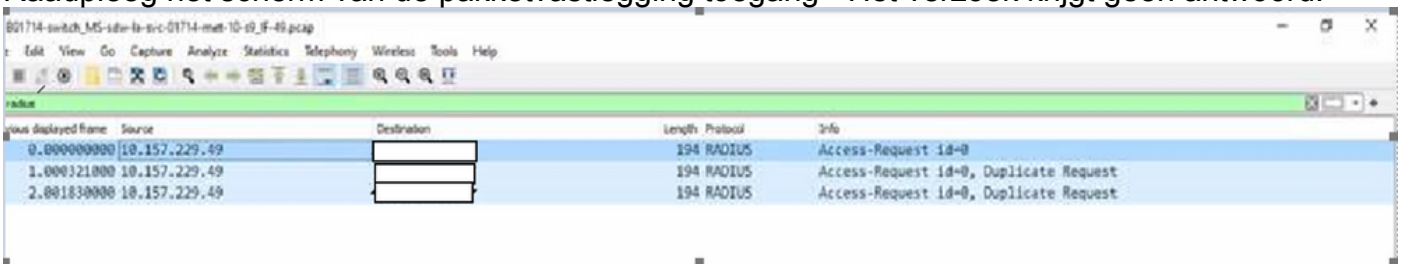
802.1X controletest voor de configuratie

- **Meraki dashboard > Netwerksjabloon > Switch > Toegangsbeleid > RADIUS-servers > Test**
- **Meraki Dashboard > Netwerksjabloon > Draadloos > Toegangsbeheer > Straalservers > Test**

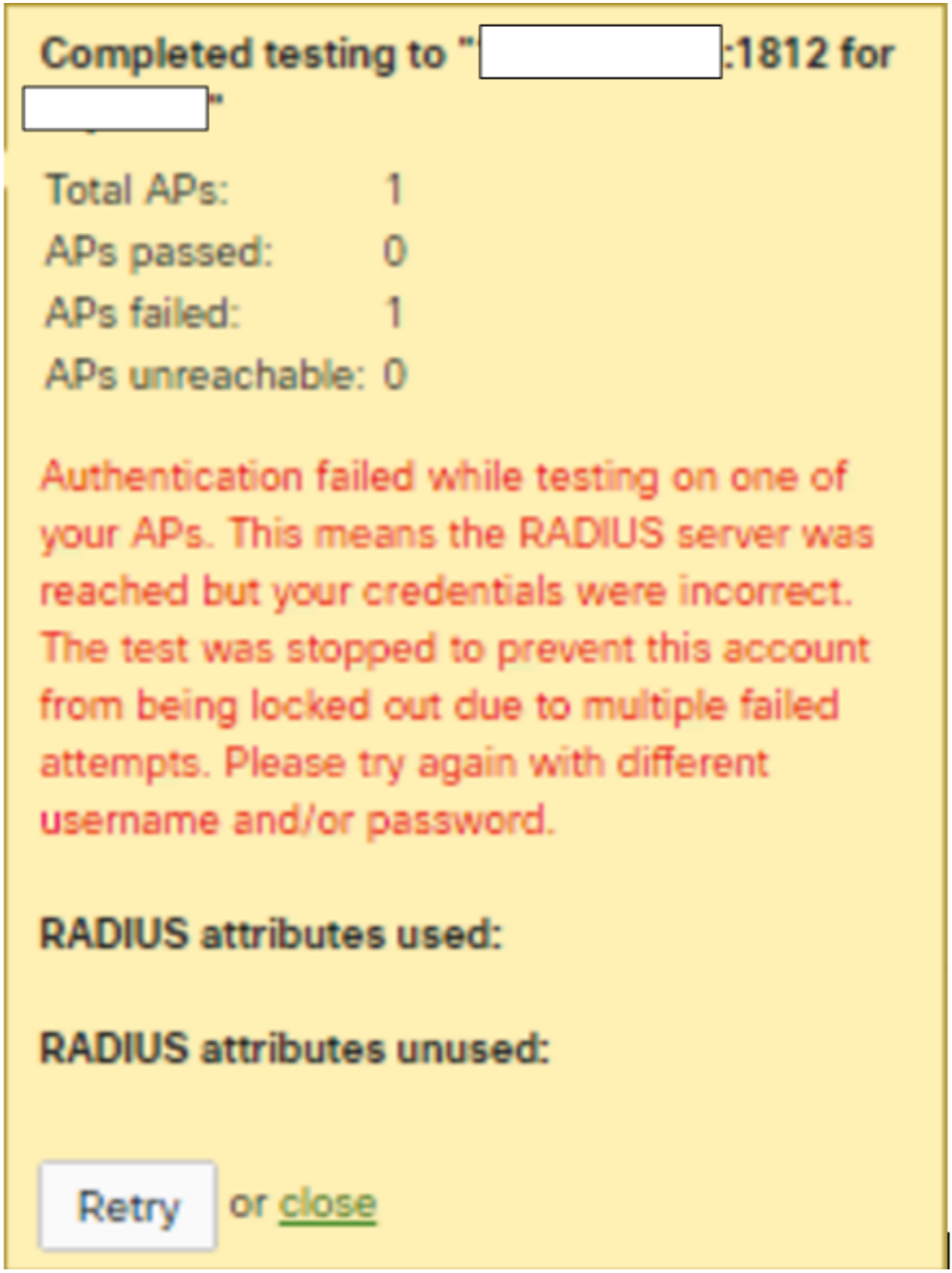
1. Als het testresultaat wordt opgemerkt aangezien **Alle AP er niet in slaagde om de radiogateway aan te sluiten**, moet u controleren waar het toegangs-verzoek is gevallen.



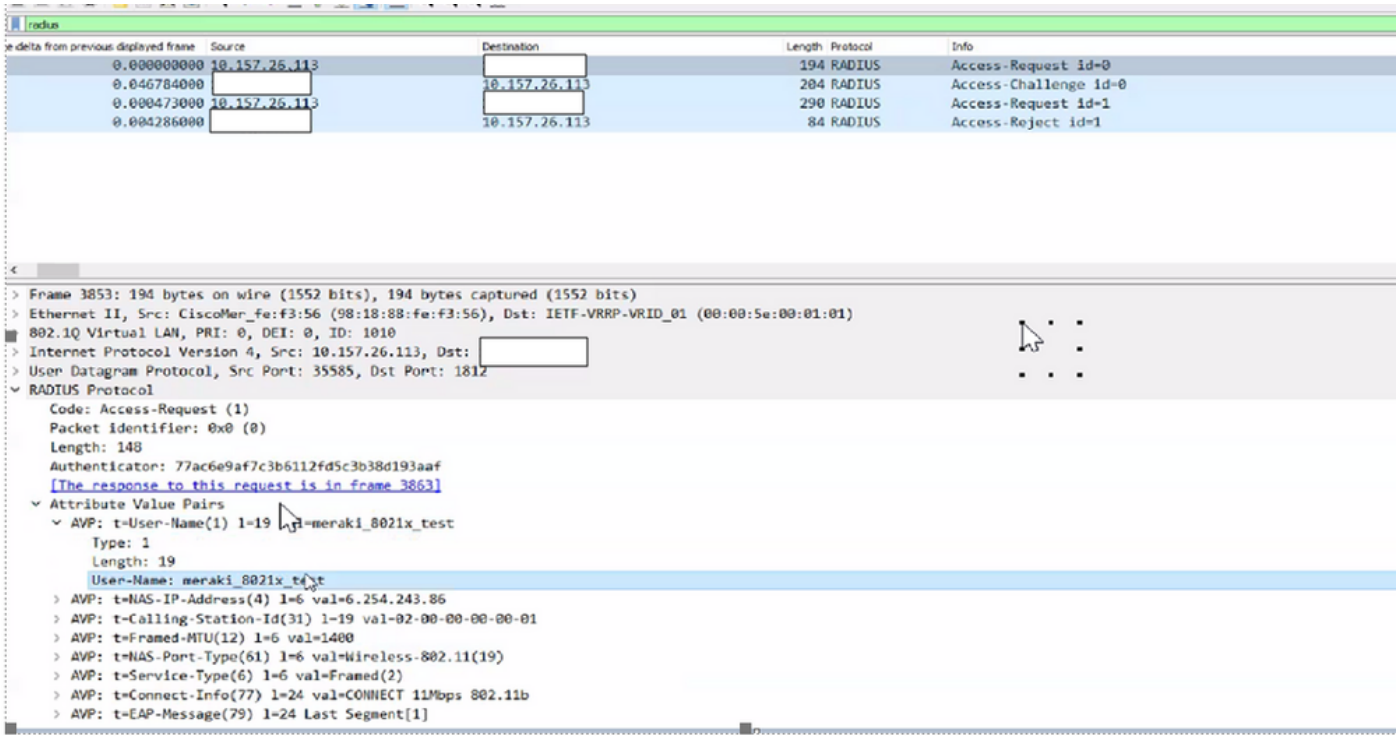
2. Start de pakketvastlegging op de uplinks-poort en controleer de toegangsaanvraag-stroom. Raadpleeg het scherm van de pakketvastlegging toegang - Het verzoek krijgt geen antwoord.



3. Als het opvallende testresultaat wordt beantwoord als aanvaarden/afwijzen/antwoorden/onjuiste geloofsbrieven, betekent dit dat de straal server leeft.

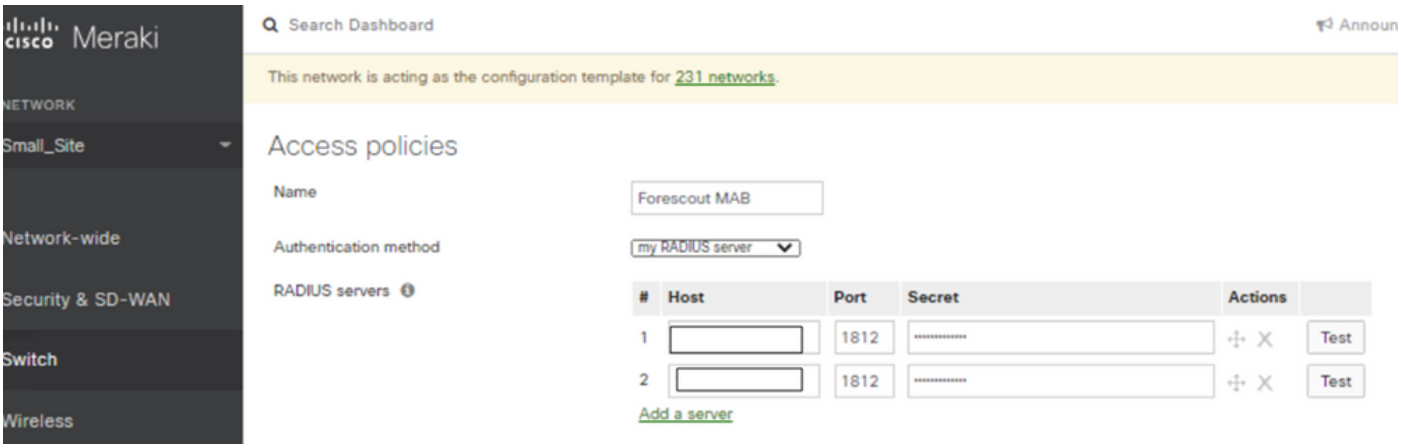


4. Start de pakketvastlegging op de uplinks-poort en controleer de toegangsaanvraag-stroom. Raadpleeg het screenshot van de pakketvastlegging toegang - het verzoek kreeg een antwoord.

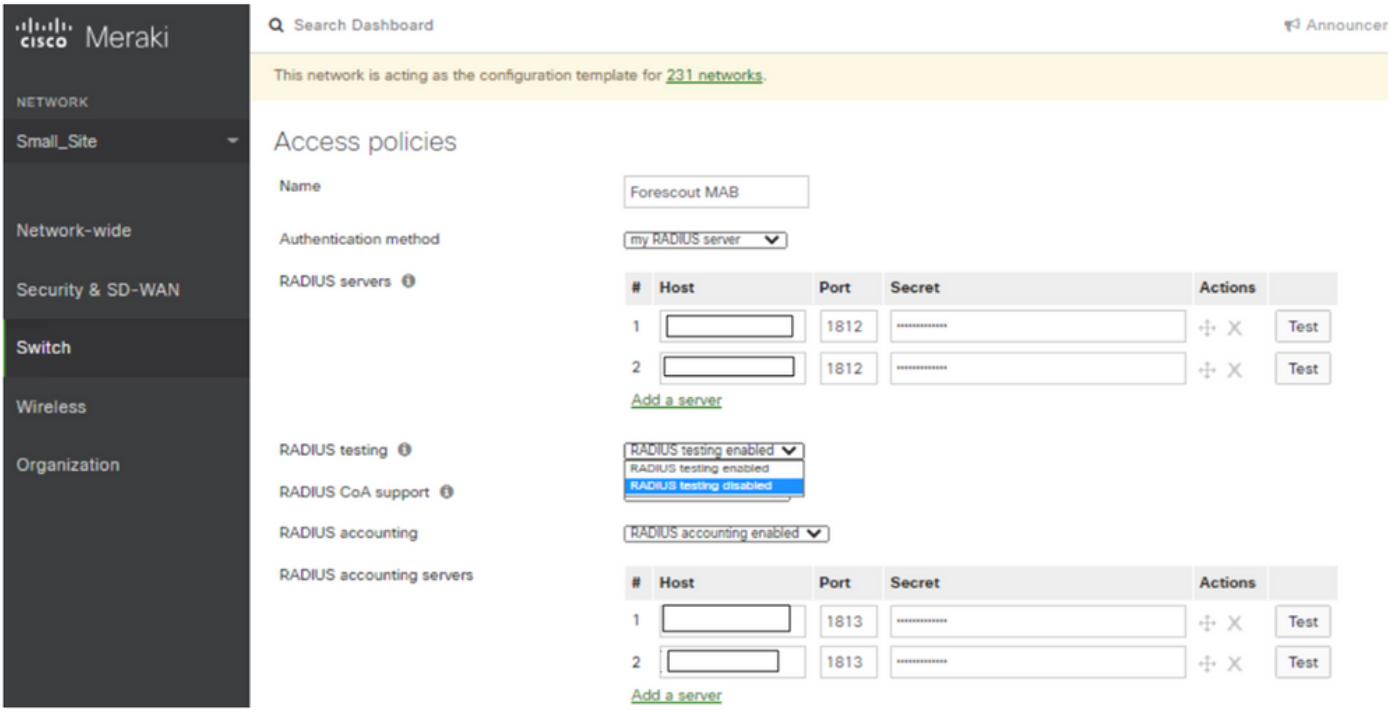


Verificatie van toegangsbeleid

1. De noodzaak om de in het toegangsbeleid vermelde parameter te controleren is correct en omvat Host IP, Port Number en Secret Key.



2. De IP's die zijn geconfigureerd, zijn dummy of worden niet gebruikt in het productiebeleid of het toegangsbeleid is niet in gebruik. Aanbevolen wordt het toegangsbeleid te schrappen. Als u dit wilt behouden, kunt u de **instelling** voor het **testen van straal** uitschakelen.



Gerelateerde informatie

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- Technische ondersteuning en documentatie – Cisco Systems

Opmerking

- Wanneer de sleuven Meraki-apparaten hebben gevraagd om de LAN IP- en standaardgebruikersnaam voor "meraki_8021x_test", werd het Meraki-dashboard als bron gebruikt.
- Meraki heeft deze waarschuwingen sinds oktober 2021 zichtbaar gemaakt.