

Problemen oplossen met verbinding met hotspots via Captive Portal met AnyConnect SWG-module ingeschakeld

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossingen en aanbevelingen voor verdere probleemoplossing](#)

[Antivirustoepassingen configureren voor AnyConnect](#)

[Details](#)

[Versies vóór 4.10.05095](#)

Inleiding

In dit document wordt beschreven hoe verbindingen met hotspots kunnen worden opgelost via Captive Portal met AnyConnect SWG-module ingeschakeld.

Probleem

Gebruikers met de AnyConnect Secure Web Gateway (SWG)-module kunnen problemen ondervinden bij het aanmelden op bepaalde openbare hotspotlocaties.

Oplossingen en aanbevelingen voor verdere probleemoplossing

Controleer of u AnyConnect-versie 4.10.05095(4.10MR5) gebruikt. Problemen met betrekking tot het interne portaal worden in deze versie behandeld.

Als het probleem echter blijft bestaan, zelfs na een upgrade naar 4.10.05095, neemt u contact op met Umbrella Support.

Om het supportproces te versnellen, vragen we klanten om deze stappen te doorlopen en de gevraagde logs te verzamelen voordat ze contact opnemen met Umbrella Support.

1. We vragen klanten om alle beveiligingsagenten die op hun eindpunten zijn geïnstalleerd, zo te configureren dat AnyConnect-binaries en -verbindingen worden uitgesloten om beleidsconflicten te voorkomen. Daarom moeten TrendMicro en/of een andere beveiligingsagent dienovereenkomstig worden geconfigureerd.
Raadpleeg het betreffende fragment uit de [opmerkingen bij](#) de AnyConnect-[release](#) en zorg ervoor dat de uitzonderingen voor AnyConnect dienovereenkomstig worden gemaakt.
2. Bezoek zowel HTTP (bijvoorbeeld <http://www.portquiz.net>) als HTTPS (<https://www.google.com>) URL's in de browser en kijk of de omleiding naar de captive portal

gebeurt of niet.

3. Als het probleem zich blijft voordoen, verzamelt u een DART-bundel (max. debug ingeschakeld), een PCAP-bestand (inclusief loopback) en een schermopname (optioneel) om verder te onderzoeken.

Antivirustoepassingen configureren voor AnyConnect

Toepassingen zoals antivirus, antimalware en het Intrusion Prevention System (IPS) kunnen het gedrag van AnyConnect Secure Mobility Client-toepassingen verkeerd interpreteren als schadelijk. U kunt uitzonderingen configureren om een dergelijke verkeerde interpretatie te voorkomen. Nadat u de AnyConnect-modules of -pakketten hebt geïnstalleerd, configureert u de antivirussoftware om de AnyConnect-installatiemap toe te staan of uitzonderingen voor de AnyConnect-toepassingen te maken. De gemeenschappelijke directory's die moeten worden uitgesloten, worden vermeld, hoewel de lijst mogelijk niet volledig is:

- C:\Users<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program Files (x86)\Cisco

Details

Captive Portal-problemen kunnen worden veroorzaakt door [CSCwb39828](#) "Captive Portal page did not open when SWG is enabled for both fail open/fail close". Na een upgrade naar AnyConnect 4.10.05095 later is geen extra configuratie of gebruikersinteractie nodig.

Sommige draadloze hotspots en andere gastnetwerken onderbreken de internettoegang en leiden webverkeer door naar een portaal in gevangenschap (soms een ommuurde tuin genoemd). AnyConnect SWG-versies van vóór 4.10.05095 kunnen proberen dit webverkeer naar de Umbrella-cloud te verzenden, zelfs als er geen internettoegang beschikbaar is, waardoor het systeem niet lokaal kan communiceren met het interne portaal. Deze lokale interactie kan nodig zijn om toegang te verlenen via verificatie, betaling of een pagina met een doorklikovereenkomst.

Versies vóór 4.10.05095

Ondersteuning is beperkt voor captive portals met eerdere versies van AnyConnect bij het gebruik van SWG. Deze acties van een captive portal maken het waarschijnlijk onbereikbaar voor een SWG-client:

- Omleiden naar of laden van assets van een bestemming buiten de RFC-1918 privé-IP-adresruimte.
- Een TCP-handshake accepteren voor paraplu-proxy's op poort 80 of 443 en vervolgens de verbinding sluiten of een onverwachte reactie geven.

Voeg als tijdelijke oplossing uitzonderingen toe in het gedeelte Implementaties --> Domeinbeheer -> Externe domeinen en IP's van het overkoepelende dashboard voor elke bestemming die niet wordt geladen. Captive Portal-gedrag is implementatiespecifiek, dus de vereiste

omleidingsdomein(en) of IP-adressen verschillen per hotspot.

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.