Bekende softwareconflicten voor CSC begrijpen

Inhoud

Inleiding

Dit document beschrijft de bekende softwareconflicten voor Cisco Security Connector (CSC).

Wat zijn de bekende softwareconflicten voor Cisco Security Connector?

Het is bekend dat de Cisco Security Connector (CSC) niet correct functioneert in de aanwezigheid van bepaalde software en bepaalde scenario's.

Onder deze voorwaarden kan de CSC Beveiligd rapporteren, maar het webverkeer is niet van toepassing op het beleid:

- VPN's: volgens het ontwerp van Apple kan de CSC geen DNS-pakketten ontvangen voor verkeer dat is gebonden aan een VPN. Dit is verwacht gedrag.
- Mobiele hotspot: Klanten die zijn verbonden met een iPhone met een hotspot vallen niet onder de CSC. De telefoon die de hotspot beheert, kan dekking blijven hebben.
- Wandera "Gateway": Apple herkent de Wandera-proxy als een VPN-achtige gateway. Daarom kan elk verkeer dat via Wandera wordt verzonden geen CSC-dekking ontvangen. CSC kan veel DNS-verzoeken naar *.proxy.wandera.com zien als een teken dat Wandera actief is.

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.