Kennenlernen bekannter Softwarekonflikte für CSC

Inhalt

Einleitung

In diesem Dokument werden die bekannten Softwarekonflikte bei Cisco Security Connector (CSC) beschrieben.

Bekannte Softwarekonflikte bei Cisco Security Connector

Der Cisco Security Connector (CSC) funktioniert bekanntermaßen nicht ordnungsgemäß, wenn Software und bestimmte Szenarien vorhanden sind.

Unter diesen Bedingungen kann der CSC Geschützt melden, aber der Web-Datenverkehr wendet keine Richtlinie an:

- VPNs Gemäß dem Design von Apple kann der CSC keine DNS-Pakete für den Datenverkehr empfangen, der für ein VPN gebunden ist. Dies ist ein erwartungsgemäßes Verhalten.
- Mobiler Hotspot: Clients, die mit einem iPhone verbunden sind, auf dem ein Hotspot ausgeführt wird, werden vom CSC nicht abgedeckt. Das Telefon, das den Hotspot bedient, kann weiterhin abgedeckt sein.
- Wandera "Gateway": Apple erkennt den Wandera-Proxy als VPN-ähnliches Gateway. Daher kann jeder Datenverkehr, der über Wandera gesendet wird, keine CSC-Abdeckung erhalten. CSC kann viele DNS-Anfragen an *.proxy.wandera.com als ein Zeichen dafür sehen, dass Wandera aktiv ist.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.