Comprender los conflictos de software conocidos de CSC

Contenido

Introducción

Este documento describe los conflictos de software conocidos para Cisco Security Connector (CSC).

¿Cuáles son los conflictos de software conocidos de Cisco Security Connector?

Se sabe que el conector de seguridad de Cisco (CSC) no funciona correctamente en presencia de software y de determinados escenarios.

En estas condiciones, el CSC puede informar de Protected, pero el tráfico web no aplica la política:

- VPN: Según el diseño de Apple, el CSC no puede recibir paquetes DNS para el tráfico destinado a una VPN. Debe ocurrir lo siguiente.
- Hotspot móvil: Los clientes conectados a un iPhone que ejecuta un hotspot no están cubiertos por el CSC. El teléfono que funciona en el punto de conexión puede seguir teniendo cobertura.
- Wandera "Gateway": Apple reconoce el proxy de Wandera como un gateway similar a una VPN. Por lo tanto, cualquier tráfico enviado a través de Wandera no puede recibir cobertura CSC. CSC puede ver muchas solicitudes DNS a *.proxy.wandera.com como una señal de que Wandera está activo.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).