

Habilitación de todo el DNS del túnel para el cliente seguro con el módulo Umbrella

Contenido

[Introducción](#)

[Antecedentes](#)

[Problema e impacto](#)

[Recomendación](#)

Introducción

Este documento describe cómo habilitar el túnel de todos los DNS para el módulo Cisco Secure Client con Umbrella.

Antecedentes

Cisco anunció el fin del ciclo de vida de Cisco AnyConnect en 2023 y de Umbrella Roaming Client en 2024. Muchos clientes de Cisco Umbrella ya se están beneficiando de la migración a Cisco Secure Client, por lo que le animamos a que inicie la migración lo antes posible para disfrutar de una mejor experiencia de roaming. Obtenga más información en este artículo de Knowledge Base: ¿Cómo instalo Cisco Secure Client con el módulo Umbrella?

El módulo [Cisco Secure Client \(CSC\) con Umbrella \(anteriormente AnyConnect Roaming Security\)](#) está diseñado para funcionar con casi todos los modos de VPN CSC sin necesidad de configuración adicional.

Sin embargo, se debe tener en cuenta lo siguiente cuando ambas condiciones sean ciertas:

- La tunelización dividida está habilitada
- La función "Tunnel All DNS" está activada

Problema e impacto

Con "Tunnel All DNS" habilitado, el tráfico DNS se intercepta en el nivel del núcleo y se bloquea si no sale de la interfaz VPN correcta. Esto plantea un problema para el módulo CSC si los solucionadores de Cisco Umbrella no forman parte de la configuración de túnel dividido (Include).

El impacto de este problema es mínimo porque, de forma predeterminada, el módulo CSC utiliza DNS cifrado (puerto UDP 443) que no está bloqueado por "Tunnel All DNS". Por lo tanto, el problema sólo ocurre en redes donde el cifrado DNS no está disponible.

El escenario es el siguiente:

- El módulo de roaming intenta enrutar el tráfico a Cisco Umbrella a través de la interfaz LAN normal.
- La red local no permite el cifrado DNS y, por lo tanto, envía consultas DNS no cifradas estándar.
- Este tráfico se bloquea mediante la función "Tunnel All DNS", que requiere que DNS interrumpa la conexión VPN.

En esta situación, DNS no funciona como se esperaba.

Recomendación

Para garantizar que esta condición no sea posible, Cisco Umbrella recomienda una de estas acciones.

- Inhabilite "Tunnel All DNS" en la política de grupo VPN. El módulo CSC maneja el ruteo de DNS.
O
- Agregue estos resolvers de Cisco Umbrella DNS a la configuración de túnel dividido (Include):
 - 208.67.222.222
 - 208.67.220.220
 - 208.67.222.220
 - 208.67.220.222

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).