

Problema de interoperabilidad de VPN de Umbrella y F5 BIG-IP Edge Client

Contenido

Problema

Los usuarios experimentan una completa pérdida de acceso a Internet cuando tanto Cisco Umbrella (Secure Client) como F5 BIG-IP Edge Client VPN están activados simultáneamente.

El problema se manifiesta de la siguiente manera:

- La conectividad a Internet no está disponible después de conectarse a la VPN de BIG-IP Edge Client cuando Cisco Umbrella está activo.
- El problema afecta a todos los recursos y sitios web de Internet, no solo a las URL específicas
- La conectividad VPN con aplicaciones internas relacionadas con el proyecto funciona según lo esperado
- El acceso a Internet funciona normalmente cuando Cisco Umbrella está desactivado
- El problema ocurre exclusivamente cuando ambos servicios se están ejecutando simultáneamente

Entorno

- Cisco Secure Client con el módulo Umbrella habilitado
- VPN de cliente de borde F5 BIG-IP configurada para tunelización dividida
- F5 Servicio de proxy de retransmisión DNS habilitado
- entorno de extremo de Windows

Resolución

Este problema de interoperabilidad requiere la implementación de una de las dos soluciones alternativas admitidas para resolver el conflicto de tráfico DNS entre Cisco Umbrella y la VPN del cliente de borde F5 BIG-IP.

Opción 1: Deshabilitar el servicio proxy de retransmisión DNS F5

El primer enfoque de resolución implica la inhabilitación del servicio proxy de retransmisión DNS F5 en la configuración del cliente de borde BIG-IP:

Paso 1: Acceso a la interfaz de configuración de F5 BIG-IP Edge Client

Paso 2: Vaya a la configuración del servicio proxy de retransmisión DNS

Paso 3: Deshabilitar el servicio proxy de retransmisión DNS



Nota: Este enfoque restaura la funcionalidad normal de Umbrella DNS, pero puede afectar al diseño de túnel dividido actual en función de los requisitos de configuración de F5.

Opción 2: Configuración de exclusiones de túnel dividido de VPN F5

La resolución recomendada implica la configuración del F5 BIG-IP Edge Client para excluir el tráfico de Umbrella de la tunelización VPN:

Paso 1: Póngase en contacto con el administrador de F5 para modificar la configuración de BIG-IP Edge Client

Paso 2: Configure la lista de tunelización dividida para excluir explícitamente todo el tráfico de red destinado a los rangos de IP de proxy y DNS de Umbrella

Paso 3: Aplique los cambios de configuración para garantizar las funciones de tráfico de



Consejo: Este cambio de configuración debe implementarlo el administrador F5 y requiere un conocimiento específico de los rangos de IP de proxy y DNS de Umbrella para garantizar una exclusión adecuada del túnel VPN.

Causa

Este problema es el resultado de una limitación de interoperabilidad conocida entre Cisco Secure Client (módulo Umbrella) y la VPN de F5 BIG-IP Edge Client cuando la VPN está configurada para la tunelización dividida con el Servicio de proxy de retransmisión de DNS F5 habilitado.

La causa raíz se produce porque tanto el cliente Umbrella como el cliente VPN F5 intentan interceptar y proxy el tráfico DNS en el nivel de terminal. Cuando ambos servicios están activos simultáneamente, esto crea un conflicto donde las solicitudes DNS no se reenvían correctamente, lo que resulta en una pérdida completa de la conectividad a Internet. El servicio proxy de retransmisión de DNS F5 interfiere con el mecanismo de interceptación de DNS de paraguas, lo que impide la resolución de DNS adecuada para los recursos de Internet.

Tanto Cisco como F5 documentan este comportamiento como una limitación conocida y no está relacionado con un defecto de software específico en ninguno de los productos.

Contenido relacionado

- [Problemas de DNS con BIG-IP Edge Client y Cisco Umbrella Client](#)
- [Comprender la compatibilidad de Umbrella Roaming Client y F5 VPN](#)
- [Soporte técnico y descargas de Cisco](#)

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).