Configuración de Umbrella y BlueCoat Webfilter/K9

Contenido

Introducción

Este documento describe cómo configurar la compatibilidad entre el cliente de roaming de Umbrella y BlueCoat Webfilter/K9.

Overview

Este artículo hace referencia a los equipos en los que están instalados Umbrella roaming Client y BlueCoat. Este artículo se refiere al uso de un agente de filtrado de BlueCoat instalado en el equipo. Esto puede coincidir con una configuración PAC o proxy.

El cliente de roaming de Umbrella y el módulo de seguridad de roaming de Umbrella en AnyConnect no son compatibles con el filtrado basado en software de BlueCoat que intenta controlar DNS.

Software afectado:

- Módulo de seguridad Cisco AnyConnect Umbrella Roaming
- Cliente de roaming de Umbrella

Síntomas

AnyConnect Roaming Module y cliente de roaming anterior a 2.2.150

Cuando el cliente móvil o el módulo móvil están activos, parece que todos los DNS fallan. Esto provoca una pérdida aparente de capacidad de uso en la máquina y una pérdida de la capacidad de acceder a los recursos web. Más específicamente, cualquier solicitud DNS a un registro A falla; sin embargo, otros tipos de registro como AAAA o TXT tienen éxito.

Cuando el cliente de roaming se desinstala o detiene temporalmente, el comportamiento normal

de la red regresa.

El cliente de roaming no reconoce que el DNS está fallando porque solo fallan los registros A y, por lo tanto, el cliente permanece activo y cifrado.

Cliente de roaming 2.2.150 y posterior

Cuando el cliente de roaming está activo, el cliente conmuta por error a un estado abierto con el mensaje

"hemos detectado una posible interferencia con las consultas de DNS A o AAAA; puede haber algún software en el sistema que esté causando problemas"

Se trata de un nuevo método de detección para el software que reemplaza los registros A pero no modifica los registros TXT. Marcamos este comportamiento y lo desactivamos para evitar la pérdida de DNS.

Resolución de problemas

Para validar si actualmente está observando este problema, confirme que son verdaderos:

- Estos escenarios dan lugar a la falla de DNS (o a la desactivación del modo de registro A)
    - BlueCoat activa y:
        - Módulo o cliente de roaming protegido y cifrado
        - Módulo o cliente de roaming protegido y sin cifrar
    - Proceso de BlueCoat eliminado manualmente (no desinstalado). La redirección está activa, pero el proxy subyacente está desconectado.
        - Cliente de roaming o módulo protegido
        - Cliente de roaming desinstalado o detenido
- Estos resultados no generan ningún problema
    - El cliente o módulo de itinerancia activo con BlueCoat desinstalado (después de un reinicio)
    - El filtro web de BlueCoat está instalado y no se está ejecutando ningún cliente de roaming

Cuando DNS falla, todos los registros A fallan, pero los registros TXT siguen sin ser redirigidos por BlueCoat y la función.

Causa raíz y solución

La causa principal de este problema de compatibilidad es doble.

1. El software BlueCoat redirige las consultas de registro A (los registros DNS más comunes para ver páginas web) de modo que solo él pueda responder a estas consultas. Este DNS puede salir de la red, pero no responde al sistema. El cliente de roaming no tiene forma de invalidar esto.

2. El cliente de roaming determina la disponibilidad de DNS al verificar las respuestas del registro TXT que son únicas para los resolvers de Umbrella. Dado que BlueCoat no exige los registros TXT, las pruebas del cliente de roaming continúan teniendo éxito incluso después de que todos los registros A comiencen a fallar. Este error en el registro A y el éxito en el registro TXT hacen que el cliente de roaming permanezca cifrado, perpetuando de manera efectiva un estado roto con el software BlueCoat.

La aplicación selectiva del proxy DNS de BlueCoat en un nivel bajo en el sistema causa un problema de compatibilidad directa con el cliente de roaming. El impacto en el usuario es una pérdida de DNS y de la capacidad de navegación web basada en DNS.

La única solución en este momento es dejar de usar el software de estación de trabajo BlueCoat que redirige DNS y en su lugar utilizar restricciones de contenido basadas en Umbrella. BlueCoat puede agregar la capacidad de deshabilitar la aplicación de DNS en el futuro.

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).