

El módulo Secure Client Umbrella se vuelve inactivo debido a la tormenta DNS de la aplicación Codex

Contenido

Problema

Varios usuarios de macOS experimentan el módulo de roaming de Cisco Secure Client Umbrella que cambia intermitentemente a un estado inactivo (fallo-apertura). Durante estos períodos, las solicitudes DNS, incluidos los comandos nslookup iniciados por el terminal, no pueden alcanzar la capa de red, lo que afecta a la capacidad de los usuarios para resolver dominios y acceder a los recursos basados en Internet.

El problema se manifiesta con fallas de sondeo repetidas en los registros de Umbrella, que muestran mensajes como:

```
Transparent probe failed  
Encrypted probe failed  
Switching to basic probe  
DNS probe failed by timeout - going open
```

El análisis reveló que el controlador de memoria se bloquea durante la misma ventana de error cuando Umbrella se vuelve inactivo. El problema se observa con mayor frecuencia mientras los usuarios utilizan activamente aplicaciones Codex y AI Assistant, con un alto volumen de intentos de conexión a chatgpt.com inmediatamente después de los comandos enviados a CODEX.

Entorno

- Cisco Secure Client versiones 5.1.13, 5.1.16, 5.1.17
- macOS (se observaron varias versiones)

- Módulo Umbrella Roaming habilitado
- Módulo ZTNA/Secure Internet Access (SIA) activado
- Aplicación Codex en uso
- Usuarios que trabajan desde varias redes (domésticas, de oficina, diferentes ISP)

Resolución

El problema se resolvió implementando configuraciones de omisión de dominio para evitar la duplicación de solicitudes DNS. Se validaron los enfoques descritos en las siguientes secciones.

Resolución principal: Omisión de dominio

- Paso 1: Agregue chatgpt.com a la lista de desvío de la configuración de Cisco Secure Access. Esto evita que Secure Client duplique las solicitudes DNS generadas por la aplicación Codex, eliminando la tormenta DNS que causa la inestabilidad del controlador.
- Paso 2: Verifique la configuración del desvío. Pruebe la funcionalidad del Codex para confirmar que el problema ya no se reproduce con el bypass en su lugar.

Resolución alternativa: Solución alternativa Codex Configuration

Aplique los cambios de configuración de Codex a los que se hace referencia en el problema de GitHub para reducir el volumen de solicitudes DNS generadas por la aplicación.

<https://github.com/openai/codex/issues/21218>

Pasos avanzados de resolución de problemas utilizados

Estos pasos de diagnóstico se realizaron para identificar la causa raíz.

1.- Activar el registro detallado de acsock:

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -sdf 0x830801F2
```

2.- Reproducir el problema y recoger el paquete DART inmediatamente después de la falla.

3.- Deshabilitar el registro detallado:

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -cdf
```

4.- Activar registro de depuración máximo para SWG. Cree el archivo SWGConfigOverride.json con contenido:

```
{"logLevel": "1"}
```

Guarde en /opt/cisco/secureclient/umbrella/swg/SWGConfigOverride.json.

5.- Activar los registros de seguimiento de RSM para DNS. Cree el archivo force_log_level.plist con contenido:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>logLevel</key>
<string>trace</string>
</dict>
</plist>
```

Guarde en /opt/cisco/secureclient/umbrella/data.

Causa

El problema principal está relacionado con el comportamiento de la aplicación Codex, que genera un volumen muy alto de solicitudes DNS. Cuando no se omite chatgpt.com, estas solicitudes son duplicadas efectivamente por Cisco Secure Client, lo que crea una tormenta de DNS que conduce

a un alto uso de la CPU y a la inestabilidad del controlador de núcleo de acsock.

El problema ocurre porque:

- Codex genera numerosas consultas DNS a chatgpt.com durante la operación.
- Sin la configuración de desvío, Secure Client intercepta y duplica estas solicitudes.
- El alto volumen de solicitudes DNS duplicadas hace que el controlador de memoria se bloquee.
- La inestabilidad del controlador provoca errores de sondeo de Umbrella y la transición al estado fallo-apertura.

Cuando se omite chatgpt.com o se aplica la solución alternativa del Codex, no se produce esta duplicación y el problema deja de reproducirse. El problema afecta a las configuraciones Umbrella-only y ZTNA SIA, lo que indica que el problema se encuentra en el mecanismo de control de tráfico en lugar de en un módulo específico.

Contenido relacionado

- [Troubleshooting del módulo Secure Access Roaming](#)
- [Solucionar problemas y recopilar información básica](#)
- [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).

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).