Cisco Secure Client VPN Connection Reset by Peer with Zscaler SSL/TLS Decryption Interference

Contenido

Problema

Un usuario experimenta fallos de conexión VPN al intentar establecer una conexión mediante Cisco Secure Client.

Entorno

- Tecnología: Cisco Secure Access - Acceso remoto seguro del cliente (VPN, estado, recurso privado)
- Familia de productos: SECACCS
- Sistema operativo: macOS (basado en las rutas de archivo de registro que muestran /Users/admin/workspace/secure-client-macos_Raccoon_MR15/)
- Software de terceros: Zscaler instalado en el sistema cliente
- Protocolo VPN: CSTP (protocolo de túnel SSL de Cisco)
- Versión de TLS: TLS 1.3 con cifrado TLS_AES_256_GCM_SHA384

Resolución

La resolución implica identificar y resolver el conflicto entre Cisco Secure Client y la funcionalidad de descifrado SSL/TLS de Zscaler.

Paso 1: Análisis y diagnóstico de registros

Capture y analice los registros de DART de Cisco Secure Client para identificar el patrón de fallos de conexión. Los registros mostrarán el establecimiento correcto de la sesión TLS seguido de un restablecimiento inmediato de la conexión.

Indicadores de diagnóstico clave en los registros:

- Establecimiento de conexión de TLS 1.3 con cifrado TLS_AES_256_GCM_SHA384
- Cálculo de MTU y procedimiento de negociación HTTP normalmente
- Error al restablecer la conexión por el par (código devuelto: 54) durante la operación de lectura del socket

La sesión TLS 1.3 se establece correctamente mediante el cifrado TLS_AES_256_GCM_SHA384, pero inmediatamente después del establecimiento de la sesión, se envía un paquete de restablecimiento que finaliza la conexión, lo que da lugar a que se desconecte el túnel VPN. El error específico observado en los registros muestra "Connection reset by peer" con código de retorno 54 (0x00000036) durante la operación de lectura del socket.

La siguiente secuencia de error se produce durante los intentos de conexión:

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

Paso 2: Identificación de software de terceros

Investigue la presencia de software de seguridad de terceros que pueda estar realizando la inspección SSL/TLS o el descifrado en el sistema cliente. En este caso, se identificó a Zscaler como la aplicación que interfiere.

Paso 3: Resolución de conflictos de descifrado SSL/TLS

Solucione el conflicto entre el tráfico VPN de Cisco Secure Client y la funcionalidad de descifrado SSL/TLS de Zscaler. Parece que Zscaler está descifrando el tráfico VPN SSL/TLS, lo que interfiere con el establecimiento del túnel VPN y provoca el restablecimiento de la conexión.

Entre los posibles enfoques de resolución se incluyen:

- Configure Zscaler para excluir el tráfico VPN de Cisco Secure Client de la inspección SSL/TLS
- Cree reglas de omisión en Zscaler para los terminales del servidor VPN
- Deshabilite temporalmente Zscaler durante las pruebas de conexión VPN para confirmar el conflicto
- Coordine con el equipo de seguridad de la red para establecer las exclusiones adecuadas

Causa

La causa raíz de este problema es un conflicto entre el tráfico VPN de Cisco Secure Client y la funcionalidad de descifrado SSL/TLS de Zscaler. Cuando Zscaler intenta descifrar o inspeccionar el tráfico TLS de VPN, interfiere con el proceso de establecimiento de túnel seguro. Esta interferencia se manifiesta como un restablecimiento de la conexión inmediatamente después de establecer la sesión TLS, lo que impide que el túnel VPN complete su fase de negociación. La sincronización del paquete de restablecimiento (que ocurre justo después del establecimiento exitoso de TLS pero antes de la finalización del túnel) es característica de la interferencia de inspección SSL/TLS de los dispositivos de seguridad o el software.

Contenido relacionado

- 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).