

Se ha denegado el inicio de sesión de VPN AnyConnect debido a condiciones de estado del terminal, incluido Cortex

Contenido

Problema

Varios usuarios no pueden conectarse de forma intermitente a Secure Client Remote Access (RAVPN) y reciben el mensaje de error "AnyConnect VPN Login denied. Su entorno no cumple los criterios de acceso definidos por el administrador." El problema afecta tanto a los portátiles MacBooks como a los de Surface, ya que los usuarios suelen necesitar varios intentos de conexión o reinicios del sistema para establecer una conexión correcta. Los fallos de conexión parecen estar relacionados con las condiciones de validación de estado del terminal, en concreto los requisitos de la versión de macOS y la verificación de estado de Cortex XDR.

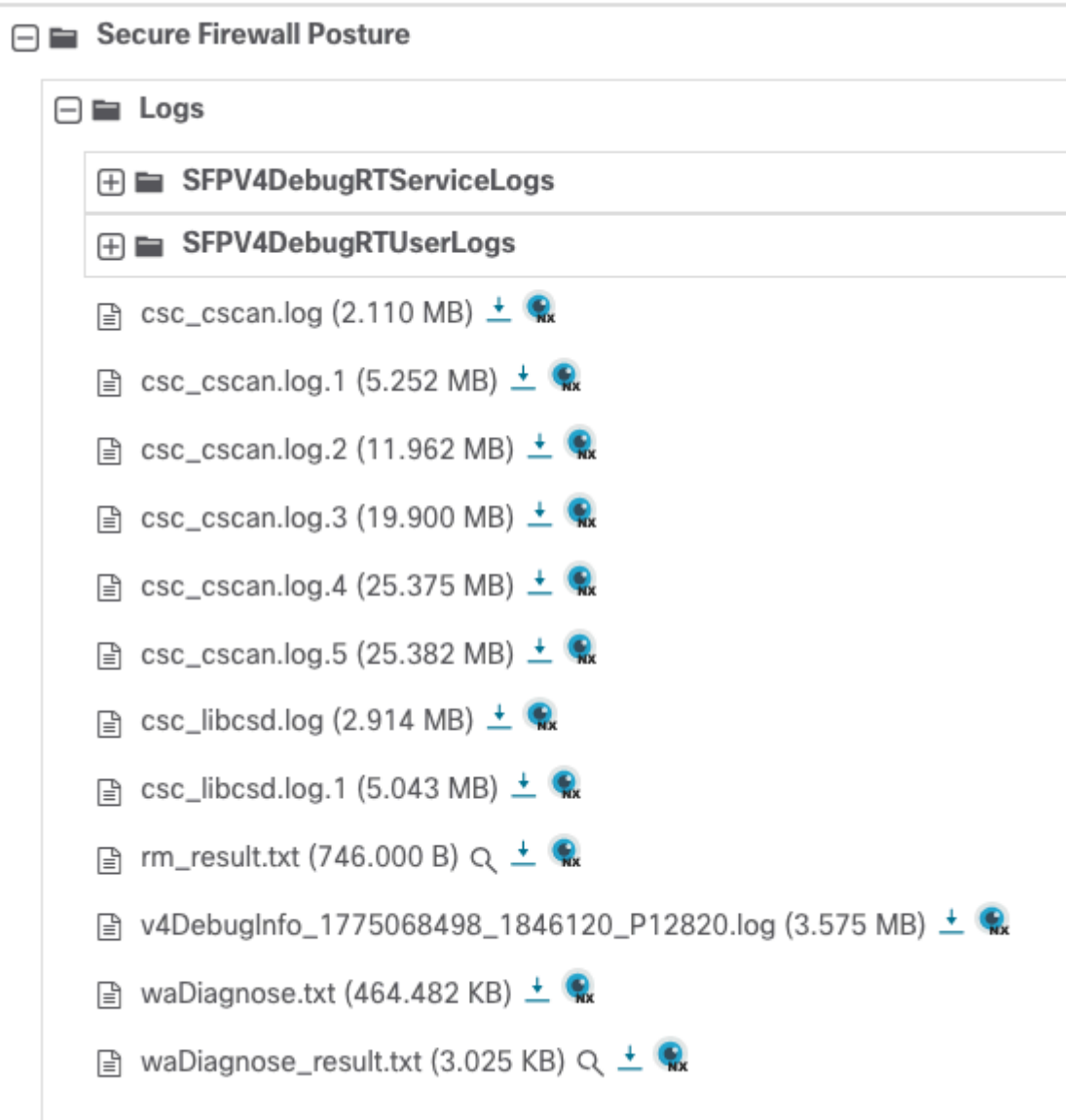
Entorno

- Implementación de acceso remoto de cliente seguro (RAVPN) con evaluación de estado
- Entorno mixto de terminales, incluidos portátiles MacBooks y Surface
- Requisitos de estado del terminal: macOS versión 26.2 o superior y Cortex XDR en ejecución
- Solución de acceso seguro con aplicación de políticas de acceso de dispositivos (DAP)

Resolución

1: Recopile DART.

2: Vaya a la carpeta Secure Firewall Posture y descargue csc_scan.log:



inline_image_0.png

3: Busque estos registros:

[Viernes 27 de marzo 13:53:10.419 2026] debug :: Participe como {"input":{"method":1000,"signature":{}}

[Viernes 27 de marzo 13:53:10.420 2026] error :: Opswat devolvió un error: -22 y convertido a: 6

[Viernes 27 de marzo 13:53:10.420 2026] error :: Error en la condición: estado de opSuccess !=

[Viernes 27 de marzo 13:53:10.420 2026] debug :: El estado de devolución de Opswat es accedenied

[Viernes 27 de marzo 13:53:10.420 2026] debug :: uso del servicio para comprobar el estado de rtp de antimalware.

[Vie Mar 27 13:53:10.420 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Vie Mar 27 13:53:10.420 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Vie Mar 27 13:53:10.420 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Vie Mar 27 13:53:10.420 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Viernes 27 de marzo 13:53:15.060 2026] error :: recibir respuesta.

[Viernes 27 de marzo 13:53:15.060 2026] debug :: no se puede realizar la comprobación am rtp.<<<<-----

[Viernes 27 de marzo 13:53:15.060 2026] info :: el estado de RTP devuelto es erróneo

[Viernes 27 de marzo 13:53:15.060 2026] info :: Opswat La fecha de definición de devolución es 1

[Viernes 27 de marzo 13:53:15.060 2026] debug :: utilizar el servicio para obtener la fecha de definición de antimalware.

[Vie Mar 27 13:53:15.060 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Vie Mar 27 13:53:15.060 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Vie Mar 27 13:53:15.060 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Vie Mar 27 13:53:15.060 2026] trace :: Estado TCP/IP Ipv4(1), Ipv6(1)

[Viernes 27 de marzo 13:53:20.079 2026] error :: recibir respuesta.

[Viernes 27 de marzo 13:53:20.079 2026] debug :: no se puede realizar la operación antimalware definition date <<<<<<—

[Viernes 27 de marzo 13:53:20.079 2026] debug :: antimalware encontrado ==> () (Cortex XDR (Mac)) (9.1.0) () (error) .

[Viernes 27 de marzo 13:53:20.084 2026] debug :: Error de coincidencia: Los nombres de los procesos son 'ciscod' y 'cscan'

[Viernes 27 de marzo 13:53:20.084 2026] debug :: estado de comprobación de la conexión a internet edr (1)



Nota: Basado en esto, parece ser una restricción de Cortex a nuestros procesos o restricción al acceso a Internet y la otra cosa que podemos comprobar si Cortex no está interfiriendo con el proceso. Podría estar bloqueando la condición de firewall seguro, ya que el análisis podría tratarse como malware.

Lista de exclusión de AntiMalware

Cisco Secure Client (CSC): todos los módulos - Sistema

1. Windows: C:\Program Files (x86)\Cisco\Cisco Secure Client*
2. macOS: /opt/cisco/secureclient/*
3. Linux: /opt/cisco/secureclient/*

Cisco Secure Client (CSC): todos los módulos - Usuario

1. Windows: %localappdata%\Cisco\Cisco Secure Client*
2. macOS: ~/.cisco/secureclient/*
3. Linux: ~/.cisco/secureclient/*

Causa

El problema se debe a fallos intermitentes en el proceso de evaluación de la postura del terminal, relacionados específicamente con la validación de los requisitos de la versión de macOS y el estado de Cortex XDR. El sistema de evaluación de estado detecta o valida de forma incoherente

las condiciones de seguridad necesarias (macOS 26.2 o superior y estado de ejecución de Cortex XDR), lo que provoca denegaciones de conexión incluso cuando los terminales cumplen los criterios especificados. Esto hace que los usuarios necesiten varios intentos de conexión o reinicios del sistema para lograr una evaluación de estado y una conexión VPN satisfactorias.

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).