AnyConnect VPN Login Denied Due to Endpoint Posture Conditions including Cortex

Contents

Issue

Multiple users are intermittently unable to connect to Secure Client Remote Access (RAVPN) and receive the error message "AnyConnect VPN Login denied. Your environment does not meet the access criteria defined by your administrator." The issue affects both MacBooks and Surface laptops, with users often requiring multiple connection attempts or system reboots to establish a successful connection. The connection failures appear to be related to endpoint posture validation conditions, specifically macOS version requirements and Cortex XDR status verification.

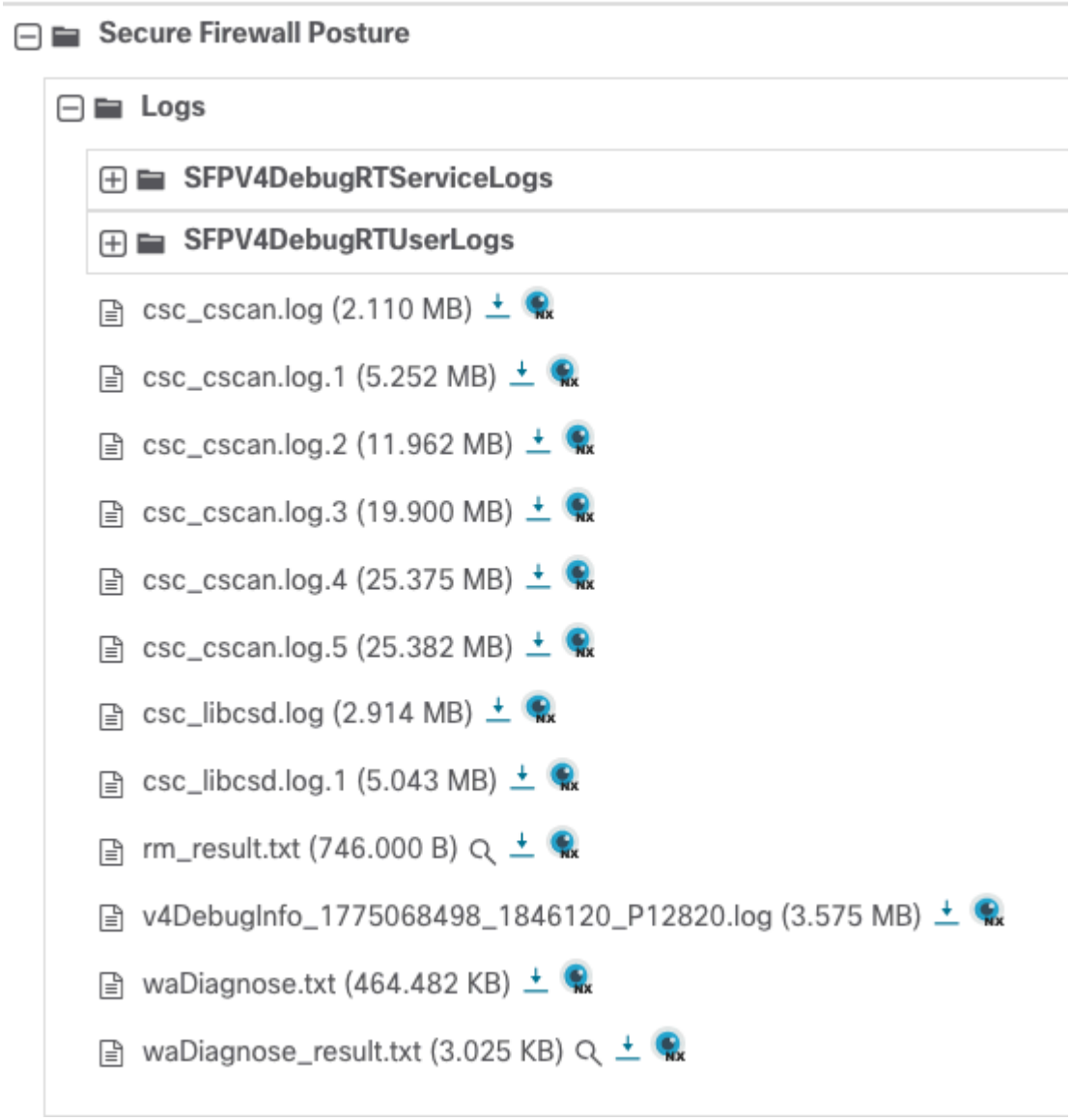
Environment

- Secure Client Remote Access (RAVPN) deployment with posture assessment
- Mixed endpoint environment including MacBooks and Surface laptops
- Endpoint posture requirements: macOS version 26.2 or greater and Cortex XDR running
- Secure Access solution with Device Access Policy (DAP) enforcement

Resolution

1: Collect DART.

2: Navigate to the **Secure Firewall Posture** folder and **download csc_scan.log**:



inline_image_0.png

3: Look for these logs:

[Fri Mar 27 13:53:10.419 2026] debug :: Json in as {"input":{"method":1000,"signature":}}

[Fri Mar 27 13:53:10.420 2026] error :: Opswat returned error: -22 and converted to: 6

[Fri Mar 27 13:53:10.420 2026] error :: Failed in condition: opSuccess != status

[Fri Mar 27 13:53:10.420 2026] debug :: Opswat Return status is accessdenied

[Fri Mar 27 13:53:10.420 2026] debug :: using service to check rtp status of antimalware.

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

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

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

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

[Fri Mar 27 13:53:15.060 2026] error :: receiving response.

[Fri Mar 27 13:53:15.060 2026] debug :: unable to perform am check rtp.<<<<<--------

[Fri Mar 27 13:53:15.060 2026] info :: the RTP status returned is failed

[Fri Mar 27 13:53:15.060 2026] info :: Opswat Return definition date is 1

[Fri Mar 27 13:53:15.060 2026] debug :: using service to get the definition date of antimalware.

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

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

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

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

[Fri Mar 27 13:53:20.079 2026] error :: receiving response.

[Fri Mar 27 13:53:20.079 2026] debug :: unable to perform antimalware definition date operation <<<<<<<———

[Fri Mar 27 13:53:20.079 2026] debug :: **found antimalware ==> () (Cortex XDR (Mac)) (9.1.0) () () (failed) .**

[Fri Mar 27 13:53:20.084 2026] debug :: Match Failed : Process names are 'ciscod' and 'cscan'

[Fri Mar 27 13:53:20.084 2026] debug :: edr internet connection check status (1)

Note: Based on this, it seems to be either a restriction by Cortex to our processes or restriction to the internet access and the other thing we can check if Cortex is not interfering with the process. It could be blocking Secure Firewall Posture since the scan could be treated as a malware.

Exclusion List from AntiMalware

Cisco Secure Client (CSC): All Modules - System

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

Cisco Secure Client (CSC): All Modules - User

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

Cause

The issue is caused by intermittent failures in the endpoint posture assessment process, specifically related to the validation of macOS version requirements and Cortex XDR status. The posture evaluation system is inconsistently detecting or validating the required security conditions (macOS 26.2 or greater and Cortex XDR running status), leading to connection denials even when endpoints meet the specified criteria. This results in users needing multiple connection attempts or system reboots to achieve a successful posture assessment and VPN connection.

Related Content

- Cisco Technical Support & Downloads