Aanmelding AnyConnect VPN geweigerd vanwege omstandigheden met betrekking tot eindpunthouding, waaronder cortex

Inhoud

uitgeven

Meerdere gebruikers kunnen met tussenpozen geen verbinding maken met Secure Client Remote Access (RAVPN) en krijgen de foutmelding "AnyConnect VPN-aanmelding geweigerd. Uw omgeving voldoet niet aan de toegangscriteria die door uw beheerder zijn gedefinieerd." Het probleem treft zowel MacBooks als Surface-laptops, waarbij gebruikers vaak meerdere verbindingspogingen of systeemreboots nodig hebben om een succesvolle verbinding tot stand te brengen. De verbindingsfouten lijken verband te houden met de validatievoorwaarden voor de eindpunthouding, met name de vereisten voor de macOS-versie en de verificatie van de XDR-status van Cortex.

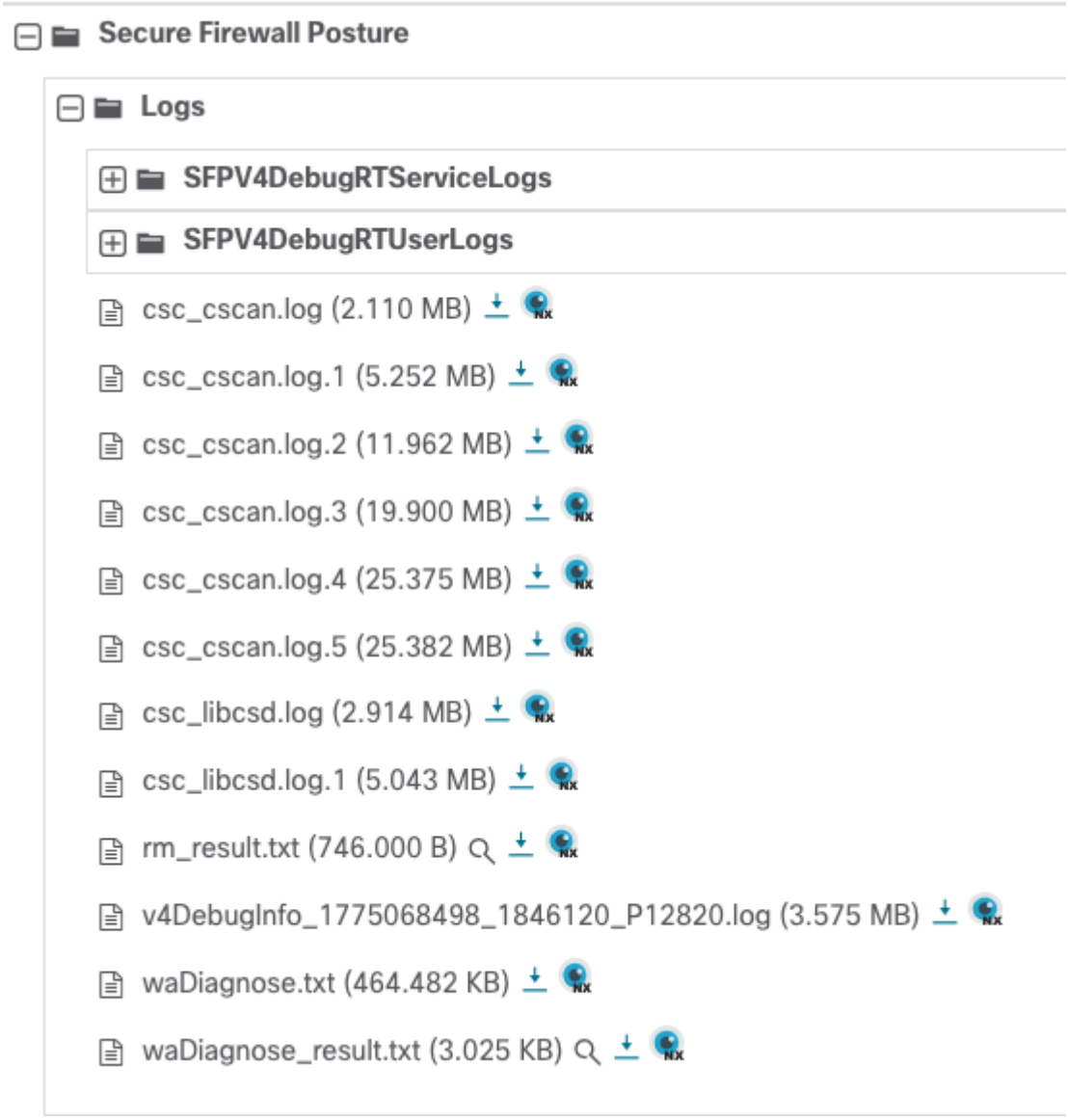
milieu

- Secure Client Remote Access (RAVPN)-implementatie met houdingsbeoordeling
- Gemengde eindpuntomgeving inclusief MacBooks en Surface-laptops
- Vereisten voor de eindpunthouding: macOS versie 26.2 of hoger en Cortex XDR actief
- Beveiligde toegangsoplossing met handhaving van het Device Access Policy (DAP)

resolutie

1: Verzamel DART.

2: Navigeer naar de map Secure Firewall Posture en download csc_scan.log:



inline_image_0.png

3: Kijk voor deze logs:

[vr mrt 27 13:53:10.419 2026] debug: Json in als {"input":{"methode":1000,"signature":}}

[Vr Mrt 27 13:53:10.420 2026] fout: Opswat keerde fout: -22 en omgezet naar: 6

[Vr Mrt 27 13:53:10.420 2026] fout: Mislukt in conditie: opSuccess!= status

[vr mrt 27 13:53:10.420 2026] debug:: Opswat Return status is ontzegd

[vr mrt 27 13:53:10.420 2026] debug: gebruik van de service om de RTP-status van antimalware te controleren.

[vr mrt 27 13:53:10.420 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:10.420 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:10.420 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:10.420 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:15.060 2026] fout: ontvangen van antwoord.

[Vr Mrt 27 13:53:15.060 2026] debug: Kan am check rtp niet uitvoeren.<<<--------

[vr mrt 27 13:53:15.060 2026] info:: de RTP-status is niet geretourneerd

[Vr Mrt 27 13:53:15.060 2026] info: Opswat Return definitie datum is 1

[vr mrt 27 13:53:15.060 2026] debug: gebruik service om de definitiedatum van antimalware te krijgen.

[vr mrt 27 13:53:15.060 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:15.060 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:15.060 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:15.060 2026] trace: TCP/IP-status IPv4(1), IPv6(1)

[vr mrt 27 13:53:20.079 2026] fout: ontvangen van antwoord.

[Fri Mar 27 13:53:20.079 2026] debug: Kan antimalware definitie datum operatie niet uitvoeren <<<<<——

() () () [vr mrt 27 13:53:20.079 2026] debug: gevonden antimalware ==> (Cortex XDR (Mac)) (9.1.0)

[vr mrt 27 13:53:20.084 2026] debug: Match Failed: Procesnamen zijn 'ciscod' en 'cscan'

[vr mrt 27 13:53:20.084 2026] debug: edr internet verbinding check status (1)

Opmerking: Op basis hiervan lijkt het een beperking door Cortex te zijn van onze processen of een beperking van de internettoegang en het andere ding dat we kunnen controleren of Cortex het proces niet verstoort. Het zou kunnen blokkeren Secure Firewall Posture omdat de scan kan worden behandeld als een malware.

Uitsluitingslijst van AntiMalware

Cisco Secure Client (CSC): Alle modules - Systeem

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

Cisco Secure Client (CSC): alle modules - gebruiker

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

Oorzaak

Het probleem wordt veroorzaakt door intermitterende fouten in het beoordelingsproces van de eindpunthouding, specifiek gerelateerd aan de validatie van de vereisten voor de macOS-versie en de Cortex XDR-status. Het postuur-evaluatiesysteem detecteert of valideert inconsistent de vereiste beveiligingscondities (macOS 26.2 of hoger en de status van de Cortex XDR-uitvoering), wat leidt tot verbindingsontkenningen, zelfs wanneer eindpunten voldoen aan de opgegeven criteria. Dit resulteert in gebruikers die meerdere verbindingspogingen of systeemreboots nodig hebben om een succesvolle houdingsbeoordeling en VPN-verbinding te bereiken.

Verwante inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.