AnyConnect VPN登录因终端安全评估条件（包括Cortex）而被拒绝

目录

问题

多个用户间歇性地无法连接到安全客户端远程访问(RAVPN)，并收到错误消息“AnyConnect VPN Login denied.您的环境不符合管理员定义的访问条件。" 此问题同时影响MacBooks和Surface笔记本电脑，用户通常需要多次尝试连接或系统重新启动才能成功建立连接。连接故障似乎与终端状态验证条件相关，具体而言是macOS版本要求和Cortex XDR状态验证。

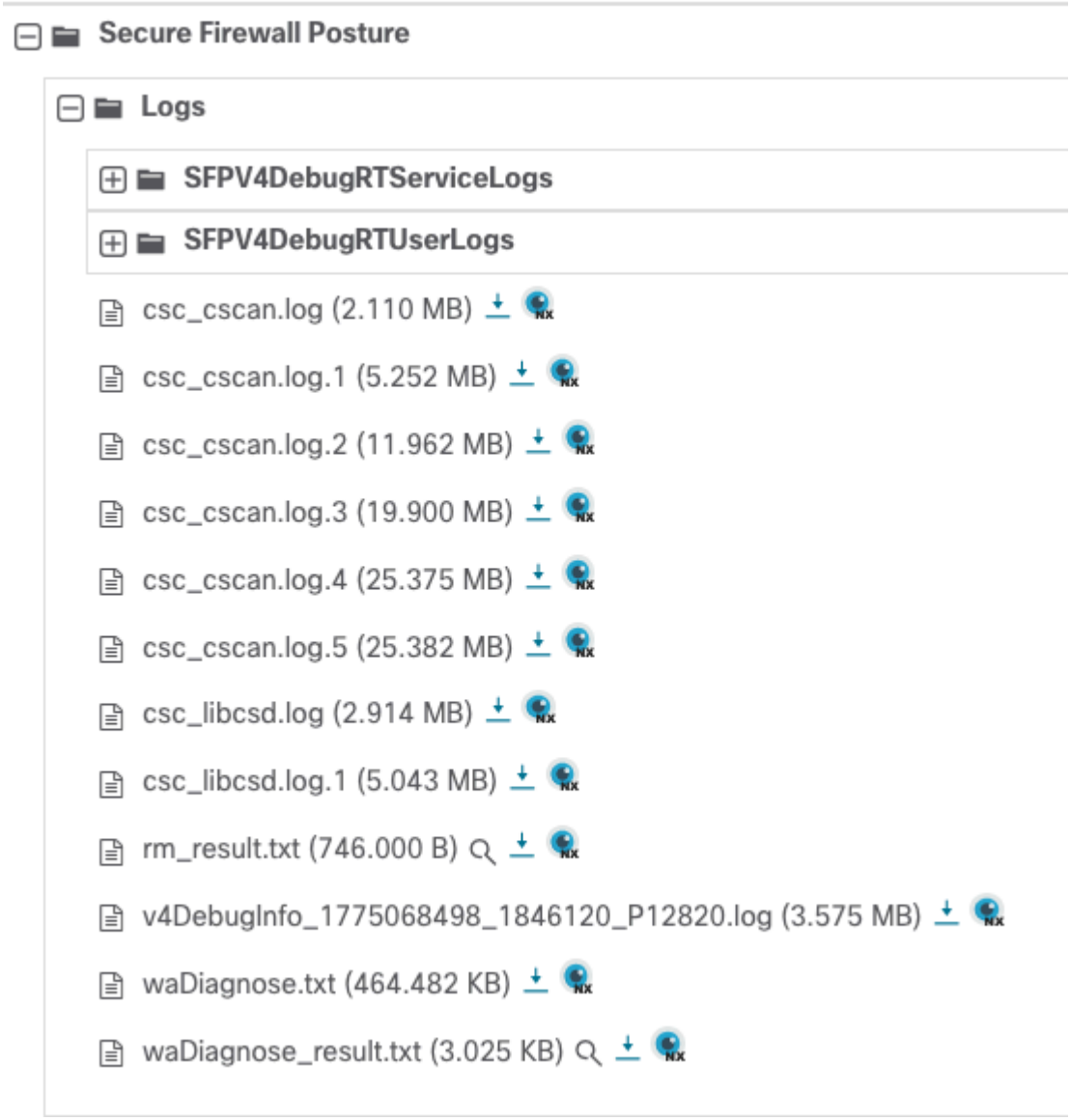
环境

- 安全客户端远程访问(RAVPN)部署，安全状态评估
- 混合终端环境，包括MacBooks和Surface笔记本电脑
- 终端安全评估要求：运行Cortex XDR的MacOS版本26.2或更高版本
- 实施设备访问策略(DAP)的安全访问解决方案

分辨率

1:收集 DART 信息.

2:导航到Secure Firewall Posture文件夹并下载csc_scan.log:



inline_image_0.png

3:查找以下日志：

[2026年3月27日星期五13:53:10.419] debug ::Json in as {"input":{"method":1000,"signature":}}

[Fri Mar 27 13:53:10.420 2026]错误：Opswat返回错误：-22并转换为：6

[Fri Mar 27 13:53:10.420 2026]错误：在以下情况下失败：opSuccess != status

[2026年3月27日星期五13:53:10.420] debug ::Opswat返回状态为访问被拒绝

[2026年3月27日星期五13:53:10.420] debug ::使用服务检查防恶意软件的rtp状态。

[2026年3月27日星期五13:53:10.420]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[2026年3月27日星期五13:53:10.420]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[2026年3月27日星期五13:53:10.420]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[2026年3月27日星期五13:53:10.420]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:15.060 2026]错误：接收响应。

[Fri Mar 27 13:53:15.060 2026]调试：无法执行am检查rtp。<<<<--------

[2026年3月27日星期五13:53:15.060]信息：返回的RTP状态失败

[2026年3月27日星期五13:53:15.060]信息：Opswat退货定义日期为1

[Fri Mar 27 13:53:15.060 2026]调试：使用服务获取反恶意软件的定义日期。

[2026年3月27日星期五13:53:15.060]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[2026年3月27日星期五13:53:15.060]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[2026年3月27日星期五13:53:15.060]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[2026年3月27日星期五13:53:15.060]跟踪：TCP/IP状态Ipv4(1),Ipv6(1)

[Fri Mar 27 13:53:20.079 2026]错误：接收响应。

[Fri Mar 27 13:53:20.079 2026]调试：无法执行反恶意软件定义日期操作<<<<<—

[Fri Mar 27 13:53:20.079 2026]调试：找到反恶意软件==>()(Cortex XDR(Mac))(9.1.0)()()（失败）。

[Fri Mar 27 13:53:20.084 2026]调试：匹配失败：进程名称是'ciscod'和'cscan'

[Fri Mar 27 13:53:20.084 2026]调试：edr internet连接检查状态(1)

注意：基于此，这似乎是Cortex对我们流程的限制或互联网接入的限制，以及我们可以检查

的Cortex是否没有干扰流程。它可能正在阻止安全防火墙状态，因为扫描可能被视为恶意软件。

防恶意软件排除列表

思科安全客户端(CSC)：所有模块 — 系统

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

思科安全客户端(CSC)：所有模块 — 用户

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

原因

此问题由终端状态评估过程中的间歇性故障引起，具体与macOS版本要求和Cortex XDR状态的验证有关。安全状态评估系统无法持续检测或验证所需的安全条件（macOS 26.2或更高版本和Cortex XDR运行状态），导致连接拒绝，即使终端满足指定的标准也是如此。这会导致用户需要多次连接尝试或系统重新启动才能成功进行状态评估和VPN连接。

相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。