Login do AnyConnect VPN negado devido a condições de postura do endpoint, incluindo Cortex

Contents

Problema

Vários usuários são intermitentemente incapazes de se conectar ao acesso remoto de cliente seguro (RAVPN) e recebem a mensagem de erro "Login do AnyConnect VPN negado. Seu ambiente não atende aos critérios de acesso definidos pelo administrador." O problema afeta os laptops MacBooks e Surface, com os usuários frequentemente exigindo várias tentativas de conexão ou reinicializações do sistema para estabelecer uma conexão bem-sucedida. As falhas de conexão parecem estar relacionadas às condições de validação da postura do endpoint, especificamente aos requisitos da versão do macOS e à verificação de status do Cortex XDR.

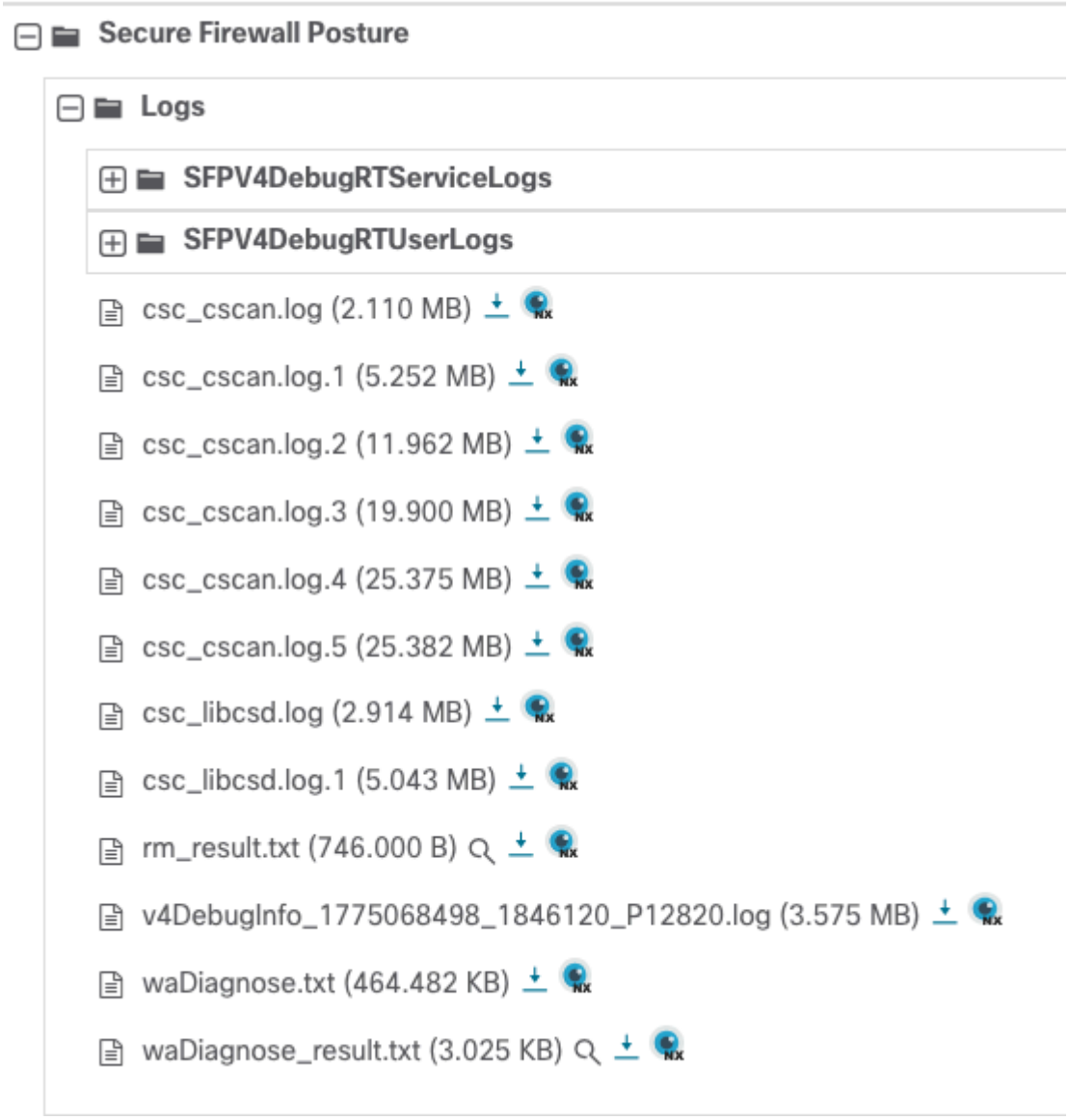
Ambiente

- Implantação de acesso remoto de cliente seguro (RAVPN) com avaliação de postura
- Ambiente de endpoint misto, incluindo MacBooks e notebooks Surface
- Requisitos de postura para endpoints: macOS versão 26.2 ou posterior e Cortex XDR em execução
- Solução de acesso seguro com aplicação de política de acesso a dispositivos (DAP)

Resolução

1: Coletar DART.

2: Navegue até a pasta Secure Firewall Posture e baixe csc_scan.log:



inline_image_0.png

3: Procure estes registros:

[Sex Mar 27 13:53:10.419 2026] debug :: Entrar como {"input":{"method":1000,"signature":}}

[Sex Mar 27 13:53:10.420 2026] erro :: O Opswat retornou um erro: -22 e convertido em: 6

[Sex Mar 27 13:53:10.420 2026] erro :: Falha na condição: status de != do opSuccess

[Sex Mar 27 13:53:10.420 2026] debug :: O status de retorno do Opswat é acessado negado

[Sex Mar 27 13:53:10.420 2026] debug :: usando o serviço para verificar o status rtp do antimalware.

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

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

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

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

[Sex Mar 27 13:53:15.060 2026] erro :: recebendo resposta.

[Sex Mar 27 13:53:15.060 2026] debug :: não é possível executar a verificação de am rtp.<<<<----
----

[Sex Mar 27 13:53:15.060 2026] info :: o status de RTP retornado falhou

[Sex Mar 27 13:53:15.060 2026] info :: A data de definição de devolução do Opswat é 1

[Sex Mar 27 13:53:15.060 2026] debug :: usar o serviço para obter a data de definição do antimalware.

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

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

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

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

[Sex Mar 27 13:53:20.079 2026] erro :: recebendo resposta.

[Sex Mar 27 13:53:20.079 2026] debug :: incapaz de executar operação de data de definição antimalware <<<<<—

[Sex Mar 27 13:53:20.079 2026] debug :: localizou antimalware ==> () (Cortex XDR (Mac)) (9.1.0) () () (falha) .

[Sex Mar 27 13:53:20.084 2026] debug :: Falha na correspondência: Os nomes dos processos são 'ciscod' e 'cscan'

[Sex Mar 27 13:53:20.084 2026] debug :: edr status de verificação de conexão com a internet (1)

Note: Com base nisso, parece ser uma restrição da Cortex aos nossos processos ou uma restrição ao acesso à Internet e a outra coisa que podemos verificar se Cortex não está interferindo no processo. Ele pode estar bloqueando a postura do firewall seguro, já que a varredura pode ser tratada como malware.

Lista de exclusões do AntiMalware

Cisco Secure Client (CSC): todos os 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 os módulos - usuário

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

Causa

O problema é causado por falhas intermitentes no processo de avaliação da postura do endpoint, especificamente relacionadas à validação dos requisitos da versão do macOS e ao status do Cortex XDR. O sistema de avaliação de postura está detectando ou validando de forma inconsistente as condições de segurança necessárias (macOS 26.2 ou superior e status de execução do Cortex XDR), levando a recusas de conexão mesmo quando os pontos de extremidade atendem aos critérios especificados. Isso faz com que os usuários precisem de várias tentativas de conexão ou reinicializações do sistema para obter uma avaliação de postura

bem-sucedida e uma conexão VPN.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.