Login a AnyConnect VPN negato a causa delle condizioni di postura dell'endpoint, tra cui Cortex

Sommario

Problema

Più utenti non sono in grado di connettersi in modo intermittente ad Accesso remoto client sicuro (RAVPN) e ricevono il messaggio di errore "Accesso VPN AnyConnect negato. L'ambiente non soddisfa i criteri di accesso definiti dall'amministratore." Il problema riguarda sia i MacBooks che i notebook Surface, con gli utenti che spesso richiedono più tentativi di connessione o il riavvio del sistema per stabilire una connessione riuscita. Gli errori di connessione sono correlati alle condizioni di convalida della postura dell'endpoint, in particolare ai requisiti di versione macOS e alla verifica dello stato di Cortex XDR.

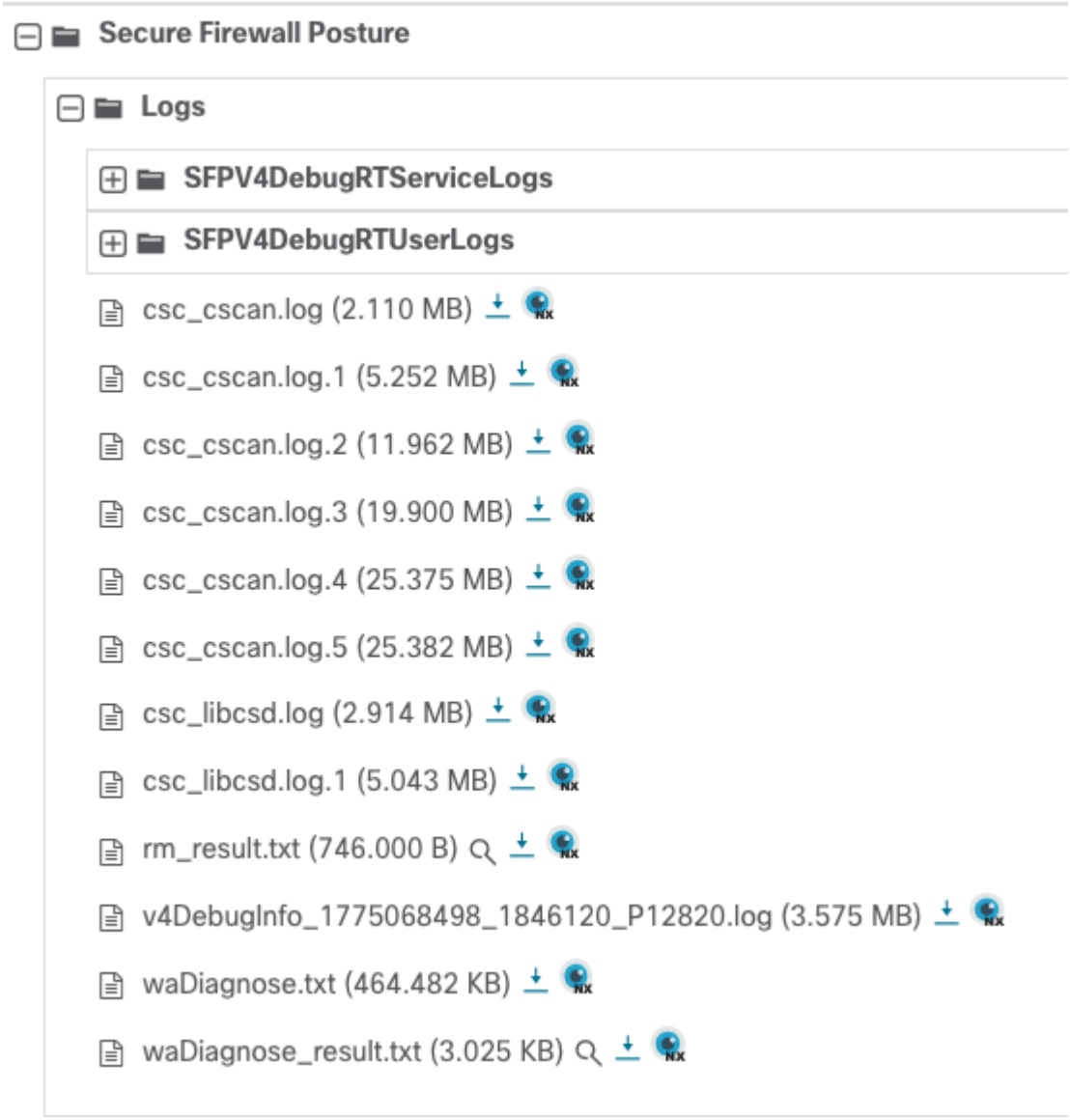
Ambiente

- Distribuzione RAVPN (Secure Client Remote Access) con valutazione della postura
- Ambiente endpoint misto, inclusi MacBook e notebook Surface
- Requisiti postura endpoint: macOS versione 26.2 o successiva e Cortex XDR in esecuzione
- Soluzione Secure Access con imposizione DAP (Device Access Policy)

Risoluzione

1: Raccogli DART.

2: Passare alla cartella Secure Firewall Posture e scaricare csc_scan.log:



inline_image_0.png

3: Cerca i seguenti log:

[venerdì 27 marzo 13:53:10.419 2026] debug :: Json in come {"input":{"method":1000,"signature":}}

[venerdì 27 marzo 13:53:10.420 2026] errore :: Opswat ha restituito l'errore: -22 e convertito in: 6

[venerdì 27 marzo 13:53:10.420 2026] errore :: Non riuscito nella condizione: opSuccess != stato

[venerdì 27 marzo 13:53:10.420 2026] debug :: Stato di ritorno Opswat negato

[venerdì 27 marzo 13:53:10.420 2026] debug :: utilizzo del servizio per controllare lo stato rtp dell'antimalware.

[venerdì 27 marzo 13:53:10.420 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[venerdì 27 marzo 13:53:10.420 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[venerdì 27 marzo 13:53:10.420 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[venerdì 27 marzo 13:53:10.420 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[Venerdì 27 marzo 13:53:15.060 2026] errore :: ricezione della risposta.

[venerdì 27 marzo 13:53:15.060 2026] debug :: impossibile eseguire il comando rtp di controllo am.<<<—

[Venerdì 27 marzo 13:53:15.060 2026] Informazioni :: lo stato RTP restituito non è riuscito

[Venerdì 27 marzo 13:53:15.060 2026] Informazioni :: La data di definizione della restituzione Opswat è 1

[venerdì 27 marzo 13:53:15.060 2026] debug :: utilizzo del servizio per ottenere la data di definizione dell'antimalware.

[venerdì 27 marzo 13:53:15.060 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[venerdì 27 marzo 13:53:15.060 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[venerdì 27 marzo 13:53:15.060 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[venerdì 27 marzo 13:53:15.060 2026] traccia :: Stato TCP/IP Ipv4(1),Ipv6(1)

[venerdì 27 marzo 13:53:20.079 2026] errore :: ricezione della risposta.

[venerdì 27 marzo 13:53:20.079 2026] debug :: impossibile eseguire l'operazione antimalware definition date <<<<<—

[venerdì 27 marzo 13:53:20.079 2026] debug :: antimalware trovato ==> () (Cortex XDR (Mac)) (9.1.0) () () (non riuscito).

[venerdì 27 marzo 13:53:20.084 2026] debug :: Corrispondenza non riuscita: I nomi dei processi

sono 'ciscod' e 'cscan'

[venerdì 27 marzo 13:53:20.084 2026] debug :: stato controllo connessione internet edr (1)

Nota: In base a ciò, sembra essere o una restrizione da parte di Cortex ai nostri processi o una restrizione all'accesso a Internet e l'altra cosa che possiamo controllare se Cortex non sta interferendo con il processo. Potrebbe bloccare la postura di Secure Firewall poiché la scansione potrebbe essere trattata come un malware.

Elenco di esclusione da AntiMalware

Cisco Secure Client (CSC): Tutti i moduli - 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): Tutti i moduli - Utente

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

Causa

Il problema è causato da errori intermittenti nel processo di valutazione della postura dell'endpoint, correlati in modo specifico alla convalida dei requisiti della versione macOS e allo stato di Cortex XDR. Il sistema di valutazione della postura rileva o convalida in modo incoerente le condizioni di sicurezza richieste (macOS 26.2 o versione successiva e stato di esecuzione Cortex XDR), determinando il rifiuto della connessione anche quando gli endpoint soddisfano i criteri specificati.

In questo modo, gli utenti hanno bisogno di più tentativi di connessione o riavvii del sistema per ottenere una corretta valutazione della postura e una connessione VPN.

Contenuto correlato

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).