Errore di connessione del client VPN di Azure con la sicurezza Web di accesso sicuro abilitata

Sommario

Problema

Dopo la migrazione da Umbrella a SSE e l'abilitazione della sicurezza Web con una licenza SIA appena assegnata, le connessioni client VPN di Azure non riescono a stabilire per gli utenti quando la sicurezza Web è abilitata. Il problema di connettività del client VPN di Azure influisce su tutti i client, impedendo loro di connettersi alla VPN. Quando Cisco Secure Access Client viene disinstallato dai computer client, la connettività VPN viene ripristinata, indicando che il client Secure Access blocca la connessione ai servizi VPN di Azure.

La disabilitazione di Web Security o la disinstallazione di Cisco Secure Access Client ripristina la connettività VPN, ma questo influisce sull'accesso degli utenti alle risorse tramite VPN di Azure quando è necessaria la protezione di Web Security.

Ambiente

- Cisco Secure Access (in precedenza SIA) con Web Security abilitato
- Client VPN di Azure
- Migrazione da Umbrella a SSE completata
- Nuova licenza SIA assegnata

Risoluzione

La risoluzione comporta l'aggiunta dell'indirizzo IP pubblico del gateway VPN di Azure all'elenco di eccezioni SSE/SWG per impedire l'intercettazione del traffico che blocca le connessioni VPN.

Passaggio 1: Identificare l'indirizzo IP del gateway VPN di Azure

Determinare l'indirizzo IP pubblico del gateway VPN di Azure.

Passaggio 2: Aggiungi eccezione basata su IP a SSE/SWG

1.- Aggiungere l'indirizzo IP pubblico del gateway virtuale di Azure all'elenco di eccezioni SSE/SWG nell'ambiente Cisco Secure Access.

2.- Accedere a Cisco Secure Access Dashboard - Fare clic su Connetti - Connettività utente finale - Sicurezza Internet - Aggiungi eccezione. In questo modo si impedisce al gateway Web sicuro di intercettare e controllare il traffico destinato al gateway VPN di Azure.

Passaggio 3: Test connettività VPN

Dopo aver applicato l'eccezione basata su IP, verificare la connessione VPN di Azure per verificare che i client siano in grado di stabilire connessioni VPN con la sicurezza Web abilitata.

Passaggio 4: Espandi test

Estendere il test dell'eccezione basata su IP ad altri utenti dell'ambiente per garantire funzionalità coerenti prima di considerare completata la risoluzione.

Causa

Il problema si verifica perché il meccanismo dell'eccezione Gateway Web sicuro (SWG) richiede una ricerca DNS di un dominio per creare una voce della cache da dominio a IP. Quando il client VPN di Azure si connette direttamente all'indirizzo IP senza eseguire una query DNS per l'URL VPN, il modulo SWG non può mappare il dominio all'indirizzo IP. Di conseguenza, il gruppo SWG continua a ispezionare e intercettare il traffico diretto all'indirizzo IP, impedendo alla connessione

VPN di stabilirsi.

L'analisi dell'acquisizione dei pacchetti ha mostrato che non sono state rilevate query DNS per l'URL VPN e nessun traffico di intercettazione SWG visibile per l'indirizzo IP del gateway di Azure, confermando che il file SWG stava bloccando la connessione a causa della mancanza di un mapping da dominio a IP appropriato nella cache.

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).