Cisco Secure Client VPN Connection Reset by Peer con interferenza decrittografia SSL/TLS zscaler

Sommario

Problema

Un utente rileva errori di connessione VPN durante il tentativo di stabilire una connessione utilizzando Cisco Secure Client.

Ambiente

- Tecnologia: Cisco Secure Access - Accesso remoto sicuro del client (VPN, postura, risorsa privata)
- Famiglia di prodotti: SECACS
- Sistema operativo: macOS (in base ai percorsi dei file di log che mostrano /Users/admin/workspace/secure-client-macos_Raccoon_MR15/)
- Software di terze parti: Zscaler installato sul sistema client
- Protocollo VPN: CSTP (Cisco SSL Tunnel Protocol)
- Versione TLS: TLS 1.3 con cifratura TLS_AES_256_GCM_SHA384

Risoluzione

La risoluzione implica l'identificazione e la risoluzione del conflitto tra Cisco Secure Client e la funzionalità di decrittografia SSL/TLS di Zscaler.

Passaggio 1: Analisi e diagnosi del registro

Acquisire e analizzare i log DART di Cisco Secure Client per identificare il modello di errore della connessione. Nei log verrà indicata la corretta attivazione della sessione TLS, seguita da una reimpostazione immediata della connessione.

Indicatori diagnostici chiave nei registri:

- Connessione TLS 1.3 stabilita con cifratura TLS_AES_256_GCM_SHA384
- Il calcolo dell'MTU e la negoziazione HTTP procedono normalmente
- Errore di reimpostazione connessione da peer (codice restituito: 54) durante l'operazione di lettura del socket

La sessione TLS 1.3 viene stabilita correttamente utilizzando la cifratura TLS_AES_256_GCM_SHA384, ma subito dopo la creazione della sessione, viene inviato un pacchetto di ripristino che termina la connessione, causando l'interruzione del tunnel VPN. L'errore specifico osservato nei log mostra "Connection reset by peer" con codice restituito 54 (0x0000036) durante l'operazione di lettura del socket.

Durante i tentativi di connessione si verifica la seguente sequenza di errori:

```
2026-03-11 10 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] A TLS 1.3 conne
2026-03-11 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function: calculat
2026-03-11 17:01:48. vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Function
2026-03-11 17:01:48.356 vpnagentd: (libvpncommon.dylib) [com.cisco.secureclient.vpn:csc_vpnagent] Funct
```

Passaggio 2: Identificazione software di terze parti

Verificare la presenza di software di sicurezza di terze parti che potrebbero eseguire l'ispezione o la decrittografia SSL/TLS sul sistema client. In questo caso, Zscaler è stato identificato come l'applicazione che interferisce.

Passaggio 3: Risoluzione dei conflitti di decrittografia SSL/TLS

Risolvere il conflitto tra il traffico VPN di Cisco Secure Client e la funzionalità di decrittografia SSL/TLS di Zscaler. Il traffico VPN sembra essere sottoposto alla decrittografia SSL/TLS da parte di Zscaler, che interferisce con la creazione del tunnel VPN e determina la reimpostazione della

connessione.

Gli approcci di risoluzione possibili includono:

- Configurare Zscaler per escludere il traffico VPN Cisco Secure Client dall'ispezione SSL/TLS
- Crea regole di bypass in Zscaler per gli endpoint del server VPN
- Disabilita temporaneamente Zscaler durante il test della connessione VPN per confermare il conflitto
- Coordinarsi con il team per la sicurezza della rete per stabilire le esclusioni corrette

Causa

La causa principale di questo problema è un conflitto tra il traffico VPN di Cisco Secure Client e la funzionalità di decrittografia SSL/TLS di Zscaler. Quando Zscaler tenta di decrittografare o ispezionare il traffico TLS della VPN, interferisce con il processo di definizione del tunnel sicuro. Questa interferenza si manifesta come una connessione reimpostata subito dopo la definizione della sessione TLS, impedendo al tunnel VPN di completare la fase di negoziazione. I tempi di ripristino del pacchetto (che si verificano subito dopo la corretta creazione del TLS ma prima del completamento del tunnel) sono caratteristici delle interferenze delle ispezioni SSL/TLS da parte delle appliance di sicurezza o del software.

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).