Errore interno del server del gruppo tunnel di rete ad accesso sicuro durante il ripristino dell'IP peer primario

Sommario

Problema

Quando si tenta di modificare l'indirizzo IP peer remoto in un gruppo di tunnel di rete (NTG) in Cisco Secure Access, gli utenti possono riscontrare un "errore interno del server" nell'interfaccia utente quando tentano di ripristinare l'indirizzo IP del tunnel primario su un valore configurato in precedenza. Lo scenario specifico prevede:

- Un NTG inizialmente configurato con un IP del tunnel primario e un IP secondario, con entrambi i tunnel che vengono stabiliti correttamente.
- L'indirizzo IP del tunnel primario viene modificato in un indirizzo IP diverso a scopo di test, che viene accettato senza problemi.
- Quando si tenta di ripristinare il valore originale dell'IP del tunnel primario, il sistema non riesce a salvare la configurazione e restituisce un "Errore interno del server" nell'interfaccia utente.
- Questo comportamento è riproducibile in modo coerente e viene visualizzato quando si cerca di riutilizzare un indirizzo IP configurato in precedenza.
- L'IP originale funzionava in precedenza e non ci sono conflitti con l'IP del tunnel secondario.

Ambiente

- Cisco Secure Access (in precedenza Cisco Umbrella per SSE)
- Configurazione di Network Tunnel Group per l'accesso privato
- Configurazione a doppio tunnel con IP peer primario e secondario

- Interfaccia di gestione basata su Web

Risoluzione

Questo problema è causato da un problema di stato/convalida back-end in cui l'IP peer originale rimane riservato o bloccato nel sistema back-end dopo le modifiche della configurazione. È necessario seguire le procedure di risoluzione dei problemi descritte nella sezione successiva:

Passaggio 1: Raccolta informazioni di diagnostica

Raccogliere le seguenti informazioni per la convalida back-end:

- ID organizzazione accesso sicuro
- Nome gruppo tunnel di rete
- ID tunnel per il tunnel primario interessato
- Area/centro dati selezionato per NTG
- Timestamp esatto di un tentativo di salvataggio non riuscito, incluso il fuso orario
- Conferma se l'indirizzo IP originale viene visualizzato in qualsiasi altro NTG, corrente o precedente
- Acquisizione HAR nel browser del tentativo di salvataggio non riuscito

Passaggio 2: Acquisisci file HAR del browser

Per raccogliere i dati di diagnostica per il tentativo di salvataggio non riuscito:

- Apri Strumenti di sviluppo browser
- Andare alla scheda Rete
- Abilita Mantieni registro

- Riproduzione dell'errore di salvataggio
- Esportare il file HAR e allegarlo alla richiesta di supporto

---


Nota: Eliminare i token di sessione o i cookie prima di caricare il file HAR.

Passaggio 3: Convalida e pulizia back-end

Questo problema richiede l'intervento del back-end e non può essere risolto solo dall'interfaccia utente. Il supporto tecnico Cisco deve eseguire le azioni seguenti:

- Coinvolgere il team backend/SSE della piattaforma Secure Access
- Convalida per prenotazione peer-IP non aggiornata
- Verifica oggetti tunnel orfani
- Identificare le chiavi back-end duplicate legate alla configurazione NTG specifica
- Cancella riferimento peer tunnel non aggiornato per l'IP originale
- Forza la risincronizzazione back-end degli oggetti NTG se necessario
- Rilascia allocazione peer-IP collegata all'UUID NTG

Passaggio 4: Metodo alternativo di risoluzione

Se la pulizia del back-end non è immediatamente disponibile, provare la seguente procedura:

- Elimina la configurazione primaria del gruppo di tunnel di rete
- Attendere 5 minuti
- Aggiungere nuovamente il file NTG con l'indirizzo IP richiesto

---


Attenzione: Possibile. I dettagli menzionati contengono procedure o comandi che potrebbero avere un impatto significativo se eseguiti. Prima di eseguire o consigliare le

---

procedure o i comandi descritti in precedenza, accertarsi che siano stati valutati da uno SME o da una Business Unit.

Passaggio 5: Soluzione temporanea

Se NTG è in produzione e non può essere rimosso:

- Continua a utilizzare il tunnel secondario per la connettività
- Ottenere una IP pubblica alternativa dal proprio fornitore/partner
- Aggiornare il file primario NTG per utilizzare l'indirizzo IP alternativo
- Riconoscere la riduzione della ridondanza fino alla risoluzione del problema di back-end

Causa

Questo problema è causato da un bug software nel sistema back-end Cisco Secure Access. Quando un IP peer primario viene modificato e ripristinato al valore originale, il sistema di convalida back-end considera erroneamente l'IP originale come ancora allocato o riservato, anche se dovrebbe essere disponibile per il riutilizzo. Ciò genera un errore di convalida back-end mascherato dall'interfaccia utente come un "errore interno del server" generico. Il sistema back-end non riesce a pulire o rilasciare correttamente la prenotazione IP durante il processo di modifica della configurazione, creando un problema persistente che impedisce il riutilizzo dell'IP nello stesso NTG.

Contenuto correlato

- Risoluzione dei problemi e raccolta di informazioni di base per Cisco Secure Access
- 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).