Comportamento del protocollo VPN di Cisco Secure Access con TLS/DTLS e configurazione doppia IPsec(IKEv2)

Sommario

Problema

Quando entrambi i protocolli TLS/DTLS e IPsec(IKEv2) sono abilitati in Cisco Secure Access VPN con il protocollo primario impostato su IPsec(IKEv2), si verificano errori di connessione quando si tenta di stabilire la connettività VPN da reti in cui il traffico IPsec (porte UDP 500/4500) è bloccato. Il client sicuro utilizza per impostazione predefinita l'opzione IPsec nell'elenco a discesa dell'interfaccia utente del client e non esegue automaticamente il failover su TLS/DTLS quando la connettività IPsec non riesce, generando errori di connessione e impossibilità di stabilire la connettività RAVPN dagli ambienti di rete con restrizioni.

Ambiente

- Cisco Secure Access VPN con configurazione a doppio protocollo
- Protocolli TLS/DTLS e IPsec(IKEv2) entrambi abilitati
- Impostazione del protocollo primario configurata come IPsec(IKEv2)
- Secure Client con elenco a discesa per la selezione del protocollo contenente opzioni IPsec e TLS separate
- Ambiente di rete che blocca il traffico IPsec sulle porte UDP 500 e 4500

Risoluzione

Il comportamento osservato è previsto e previsto. Cisco Secure Access RAVPN non esegue il failover automatico del protocollo da IPsec(IKEv2) a TLS/DTLS quando entrambi i protocolli sono abilitati e il protocollo primario rileva problemi di connettività.

Selezione manuale protocollo richiesta

Quando ci si connette da reti che bloccano il traffico IPsec, gli utenti devono selezionare manualmente il protocollo appropriato nel client sicuro:

Passaggio 1: Aprire l'applicazione Secure Client

Passaggio 2: Individuare il menu a discesa per la selezione del protocollo nell'interfaccia client

Passaggio 3: Modificare manualmente la selezione dall'opzione IPSec all'opzione TLS

Passaggio 4: Avviare la connessione VPN utilizzando il protocollo TLS/DTLS

Chiarificazione del comportamento del protocollo

L'impostazione del protocollo primario in Cisco Secure Access RAVPN determina il protocollo predefinito presentato in Secure Client, ma non abilita la funzionalità di failover automatico. Quando sono abilitati sia TLS/DTLS che IPsec(IKEv2):

- Secure Client visualizza opzioni di protocollo separate nel menu a discesa
- Il client utilizza per impostazione predefinita l'impostazione del protocollo primario (in questo caso IPsec)
- Non si verifica alcun passaggio automatico tra i protocolli in base alle condizioni di connettività di rete
- Gli utenti devono selezionare manualmente il protocollo appropriato in base all'ambiente di rete

Causa

Cisco Secure Access VPN è progettato senza funzionalità di failover automatico del protocollo. Quando sono abilitati entrambi i protocolli TLS/DTLS e IPsec(IKEv2), il sistema richiede la selezione manuale del protocollo tramite l'interfaccia Secure Client. L'impostazione del protocollo primario determina solo la selezione predefinita nel menu a discesa del client e non implementa la logica di commutazione automatica quando si verificano problemi di connettività con il protocollo primario.

Contenuto correlato

- Documentazione di 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).