Problemi di visibilità dell'identità del client sicuro con il tunnel di rete MX75 in accesso sicuro

Sommario

Problema

Quando gli endpoint con Secure Client vengono distribuiti dietro un tunnel di rete MX75 che si connette a Secure Access, le identità utente e client in roaming non sono correttamente visibili nel sistema. Vengono osservati i seguenti comportamenti specifici:

- Le impostazioni di backoff configurate per assegnare priorità al client sicuro sulle connessioni del tunnel di rete non funzionano come previsto quando gli endpoint sono dietro al MX75
- Le regole di controllo del traffico basate sui domini non si applicano perché il traffico viene attribuito solo all'identità del tunnel di rete anziché al client di roaming
- Ricerca attività visualizza informazioni incomplete sul percorso di origine, mostrando solo l'identità del tunnel di rete omettendo le identità utente e client mobili
- Le regole di gestione del traffico basate sull'identità (ad esempio quelle basate sugli utenti di Active Directory o sull'identità di un client mobile) non vengono applicate al traffico che attraversa il tunnel MX75

Questo comportamento impedisce la corretta segregazione delle identità e l'applicazione dei criteri per gli endpoint che si connettono tramite l'infrastruttura del tunnel di rete.

Ambiente

- Distribuzione Cisco Secure Access
- Appliance MX75 con configurazione del tunnel di rete per l'accesso sicuro
- Agenti client sicuri installati su tutti gli endpoint
- Impostazioni di backoff disabilitate sui client mobili per assegnare priorità al client sicuro sulle connessioni del tunnel di rete
- Regole per la gestione del traffico configurate per il routing basato su dominio
- Criteri basati sulle identità configurati per gli utenti e i client mobili di Active Directory

Risoluzione

Il problema è stato risolto implementando una configurazione alternativa utilizzando un approccio basato sulla rete registrata invece di affidarsi alla visibilità dell'identità di roaming attraverso il tunnel di rete MX75.

Implementazione soluzione alternativa

Passaggio 1: Configurazione di RSM (Roaming Security Module) con la rete registrata

Sostituire la configurazione del tunnel di rete esistente con una distribuzione RSM combinata con un'installazione di una rete registrata. Questa configurazione consente l'applicazione corretta di criteri e attributi di identità.

Passaggio 2: Convalida visibilità identità

Dopo aver implementato la configurazione della rete registrata, verificare quanto segue:

- Le identità degli utenti vengono visualizzate correttamente in Ricerca attività
- Le identità dei client mobili sono visibili e attribuite correttamente
- Regole di controllo del traffico basate sulla funzione di identità di client e utente prevista

Passaggio 3: Verifica della funzionalità di controllo del traffico

Confermare che le regole di gestione del traffico e i criteri basati sull'identità basati sul dominio siano applicati correttamente con la nuova configurazione.

Approccio alternativo

Per gli ambienti in cui non è richiesta la separazione dell'identità sulle reti private, prendere in considerazione l'implementazione della configurazione RSM - Internet. Questo approccio permette di inviare il traffico RSM direttamente a Internet anziché attraverso il tunnel della rete privata, che può fornire un'adeguata visibilità dell'identità mantenendo al tempo stesso i controlli di sicurezza.

Analisi tecnica

Durante la risoluzione dei problemi, l'output di diagnostica è stato raccolto utilizzando policy.test.sse.cisco.com per dimostrare il comportamento di attribuzione dell'identità quando gli endpoint si trovavano dietro il tunnel MX75. L'analisi ha confermato che, sebbene sia tecnicamente possibile instradare le identità di roaming attraverso un tunnel di rete, non si tratta di un flusso operativo consigliato o supportato per questo specifico scenario di distribuzione.

Causa

La causa principale è correlata alla modalità con cui Secure Access gestisce l'attribuzione delle identità quando il traffico attraversa l'infrastruttura del tunnel di rete. Quando gli endpoint si connettono tramite il tunnel di rete MX75, il sistema attribuisce tutto il traffico all'identità del tunnel anziché conservare le singole identità utente e client in roaming. Questo comportamento è progettato per le connessioni del tunnel di rete, ma è in conflitto con i requisiti per la visibilità delle identità e l'applicazione dei criteri.

Sebbene sia tecnicamente possibile instradare le identità di roaming attraverso i tunnel di rete, questa configurazione non è consigliata né supportata come flusso operativo standard a causa delle limitazioni di attribuzione delle identità descritte in precedenza.

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).