Funzionamento della registrazione DNS e della registrazione del dispositivo con Cisco Secure Client su iOS per VPN ad accesso remoto

Sommario

Problema

Quando si utilizza Cisco Secure Client su iOS (iPad) per stabilire una VPN ad accesso remoto con Cisco Secure Access utilizzando l'autenticazione SAML tramite Microsoft Entra ID, i registri DNS non vengono visualizzati in Secure Access dopo la connessione VPN riuscita, anche se il firewall e i registri Web vengono generati correttamente. Inoltre, l'iPad non viene visualizzato in Dispositivi mobili > Dispositivi mobili nel dashboard Secure Access dopo aver stabilito la connessione VPN.

I sintomi specifici osservati includono:

- I registri di accesso remoto mostrano gli eventi di connessione riusciti in Accesso sicuro
- Vengono generati i registri Web e del firewall e viene visualizzata l'identità utente autenticata SAML
- I registri DNS sono completamente assenti dalla registrazione di accesso protetto
- Le informazioni sul dispositivo iPad non vengono inserite nella sezione Dispositivi mobili di accesso sicuro
- Tutti i flussi di traffico attraverso il tunnel VPN (non è configurato alcun tunneling suddiviso)

Ambiente

- iPad con iOS 26.2
- Cisco Secure Client
- Provider di identità: ID Entra Microsoft

- Security Connector: Non installato
- Cisco Secure Access con autenticazione SSO configurata
- Implementazione autenticazione SAML
- Profilo VPN configurato con la modalità DNS impostata sui valori predefiniti
- Nessun tunneling suddiviso configurato (tutto il traffico instradato tramite VPN)
- MDM (Mobile Device Management) utilizzato per la distribuzione dei profili

Risoluzione

Il comportamento osservato è previsto per la configurazione documentata. Cisco Secure Client su iOS funziona come client VPN (AnyConnect equivalente) e non include per impostazione predefinita funzionalità equivalenti a RSM. Security Connector è il componente equivalente a RSM su iOS necessario per il popolamento delle identità degli endpoint e il controllo DNS di tipo Umbrella.

Informazioni sull'architettura

L'assenza di registri DNS e di registrazione del dispositivo si verifica per i motivi seguenti:

- Cisco Secure Client da solo fornisce la connettività VPN, ma non dispone della funzionalità dell'agente endpoint necessaria per la visibilità DNS
- Security Connector (equivalente a RSM in Windows) è necessario per il controllo DNS e la registrazione dei dispositivi in Secure Access
- Senza Security Connector, le query DNS vengono gestite dai server DNS ottenuti tramite VPN senza visibilità per Umbrella/Secure Access

Soluzione di registrazione DNS tramite Traffic Steering

Per abilitare la registrazione DNS senza installare Security Connector, configurare la direzione del traffico per indirizzare le query DNS ai server DNS Umbrella:

Passaggio 1: Configurazione del controllo del traffico in modalità di accesso sicuro

Passare a Traffic Steering > Aggiungi > Aggiungi origine e specificare l'indirizzo IP del server DNS come origine.

Passaggio 2: Traffico DNS diretto verso i server Umbrella

Configurare il profilo VPN in modo che utilizzi i server DNS Umbrella (208.67.222.222 e 208.67.220.220) per garantire che le query DNS siano visibili per l'accesso protetto.

Passaggio 3: Convalida registrazione DNS

Dopo aver implementato la configurazione di gestione del traffico, i registri DNS dovrebbero diventare visibili nel dashboard di accesso sicuro per le sessioni VPN.

Impostazione modalità DNS profilo VPN

L'impostazione "Modalità DNS" nel profilo VPN non è correlata all'assenza di registri DNS in questa configurazione. Le sessioni RAVPN (Remote Access VPN) utilizzano i server DNS ottenuti dalla VPN indipendentemente da questa impostazione e la visibilità della registrazione dipende dal fatto che il traffico DNS venga indirizzato o meno all'infrastruttura DNS monitorata.

Opzione di installazione di Security Connector

L'installazione di Security Connector su iOS consentirà:

- Visibilità della registrazione DNS in Accesso sicuro
- Funzionalità avanzate di registrazione di dispositivi e identità degli endpoint
- Controllo e protezione DNS di tipo Umbrella

Security Connector può essere utilizzato in combinazione con Secure Client, ma per evitare conflitti tra i due componenti sono necessarie considerazioni sulla progettazione e sull'esclusione del traffico.

Causa

La causa principale è l'architettura: Cisco Secure Client su iOS fornisce la connettività VPN, ma non include la funzionalità dell'agente endpoint necessaria per la visibilità DNS e la registrazione del dispositivo in Secure Access. Questa funzionalità richiede l'installazione di Security Connector o la configurazione del controllo del traffico per indirizzare le query DNS attraverso l'infrastruttura monitorata. Senza questi componenti, le query DNS ignorano il monitoraggio dell'accesso sicuro e le informazioni sull'identità dei dispositivi non vengono popolate nella sezione dei dispositivi mobili.

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).