Comportement de journalisation DNS et d'enregistrement de périphérique avec Cisco Secure Client sur iOS pour VPN d'accès à distance

Table des matières

Problème

Lors de l'utilisation de Cisco Secure Client sur iOS (iPad) pour établir un VPN d'accès à distance avec Cisco Secure Access à l'aide de l'authentification SAML via Microsoft Entra ID, les journaux DNS ne sont pas affichés dans Secure Access après une connexion VPN réussie, même si les journaux Web et de pare-feu sont générés correctement. En outre, l'iPad n'apparaît pas sous Périphériques itinérants > Périphériques mobiles dans le tableau de bord d'accès sécurisé après l'établissement de la connexion VPN.

Les symptômes spécifiques observés sont les suivants :

- Les journaux d'accès à distance affichent les événements de connexion réussis dans Secure Access
- Les journaux Web et de pare-feu sont générés et affichent l'identité utilisateur authentifiée SAML
- Les journaux DNS sont complètement absents de la journalisation d'accès sécurisé
- Les informations relatives au périphérique iPad ne sont pas renseignées dans la section Périphériques d'itinérance d'accès sécurisé
- Tout le trafic passe par le tunnel VPN (pas de split tunneling configuré)

Environnement

- iPad exécutant iOS 26.2
- Client sécurisé Cisco
- Fournisseur d'identité : ID d'entrée Microsoft
- Connecteur de sécurité : Non installé
- Accès sécurisé Cisco avec authentification SSO configurée
- Implémentation d'authentification SAML
- Profil VPN configuré avec le mode DNS défini par défaut
- Aucune tunnellisation partagée configurée (tout le trafic est acheminé via le VPN)
- Gestion des appareils mobiles (MDM) utilisée pour la distribution des profils

Résolution

Le comportement observé est attendu pour la configuration documentée. Cisco Secure Client sur iOS fonctionne comme un client VPN (équivalent AnyConnect) et n'inclut pas de fonctionnalité équivalente RSM par défaut. Security Connector est le composant équivalent RSM sur iOS qui est requis pour le remplissage d'identité de point d'extrémité et le contrôle DNS de type Umbrella.

Comprendre l'architecture

L'absence de journaux DNS et d'enregistrement de périphérique se produit pour les raisons suivantes :

- Cisco Secure Client fournit à lui seul la connectivité VPN, mais ne dispose pas de la fonctionnalité d'agent de point de terminaison nécessaire à la visibilité DNS
- Le connecteur de sécurité (équivalent à RSM sous Windows) est requis pour le contrôle DNS et l'enregistrement des périphériques dans Secure Access
- Sans Security Connector, les requêtes DNS sont traitées par les serveurs DNS obtenus par VPN sans visibilité sur Umbrella/Secure Access

Solution de journalisation DNS via le pilotage du trafic

Pour activer la journalisation DNS sans installer Security Connector, configurez l'orientation du trafic pour diriger les requêtes DNS vers les serveurs DNS Umbrella :

Étape 1: Configurer le pilotage du trafic dans Secure Access

Accédez à Traffic Steering > Add > Add a source et spécifiez l'adresse IP du serveur DNS comme source.

Étape 2: Trafic DNS direct vers les serveurs parapluies

Configurez le profil VPN pour utiliser les serveurs DNS Umbrella (208.67.222.222 et 208.67.220.220) afin de garantir que les requêtes DNS sont visibles par l'accès sécurisé.

Étape 3: Valider la journalisation DNS

Après la mise en oeuvre de la configuration du pilotage du trafic, les journaux DNS doivent devenir visibles dans le tableau de bord Secure Access pour les sessions VPN.

Paramètre du mode DNS du profil VPN

Le paramètre « DNS Mode » du profil VPN n'est pas lié à l'absence de journaux DNS dans cette configuration. Les sessions RAVPN (Remote Access VPN) utilisent les serveurs DNS obtenus par VPN indépendamment de ce paramètre, et la visibilité de la journalisation dépend du fait que le trafic DNS est dirigé ou non vers l'infrastructure DNS surveillée.

Option d'installation du connecteur de sécurité

L'installation de Security Connector sur iOS permettra :

- Visibilité de la journalisation DNS dans Secure Access
- Fonctionnalités améliorées d'identification des terminaux et d'enregistrement des périphériques

- Contrôle et protection DNS de type parapluie

Le connecteur de sécurité peut être utilisé avec le client sécurisé, mais des considérations d'exclusion de trafic et de conception appropriées sont nécessaires pour éviter les conflits entre les deux composants.

Motif

La cause principale est architecturale : Cisco Secure Client sur iOS fournit une connectivité VPN, mais n'inclut pas la fonctionnalité d'agent de point d'extrémité requise pour la visibilité DNS et l'enregistrement de périphérique dans Secure Access. Cette fonctionnalité nécessite l'installation du connecteur de sécurité ou la configuration du pilotage du trafic pour diriger les requêtes DNS via l'infrastructure surveillée. Sans ces composants, les requêtes DNS contournent la surveillance d'accès sécurisé et les informations d'identité des périphériques ne sont pas renseignées dans la section des périphériques itinérants.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.