Problèmes de visibilité de l'identité du client sécurisé avec le tunnel réseau MX75 dans l'accès sécurisé

Table des matières

Problème

Lorsque des terminaux avec client sécurisé sont déployés derrière un tunnel réseau MX75 se connectant à Secure Access, les identités des clients et des utilisateurs itinérants ne sont pas correctement visibles dans le système. Les comportements spécifiques suivants sont observés :

- Les paramètres de désactivation configurés pour donner la priorité au client sécurisé sur les connexions de tunnel réseau ne fonctionnent pas comme prévu lorsque les terminaux sont derrière le MX75
- Les règles de direction du trafic basées sur les domaines ne s'appliquent pas, car le trafic est attribué uniquement à l'identité du tunnel réseau plutôt qu'au client d'itinérance
- La recherche d'activité affiche des informations d'emplacement source incomplètes, affichant uniquement l'identité du tunnel réseau tout en omettant les identités d'utilisateur et de client itinérant
- Les règles de direction du trafic basées sur l'identité (telles que celles basées sur les utilisateurs Active Directory ou l'identité du client itinérant) ne s'appliquent pas au trafic traversant le tunnel MX75

Ce comportement empêche la ségrégation d'identité et l'application de politiques appropriées pour les terminaux se connectant via l'infrastructure de tunnel réseau.

Environnement

- déploiement de Cisco Secure Access
- Appareil MX75 avec configuration de tunnel réseau pour un accès sécurisé
- Agents client sécurisés installés sur tous les terminaux
- Paramètres de réémission temporisée désactivés sur les clients itinérants pour donner la

priorité au client sécurisé sur les connexions de tunnel réseau
- Règles d'orientation du trafic configurées pour le routage basé sur le domaine
- Stratégies basées sur l'identité configurées pour les utilisateurs Active Directory et les clients itinérants

Résolution

Le problème a été résolu en implémentant une configuration de contournement à l'aide d'une approche de réseau enregistré au lieu de compter sur la visibilité des identités d'itinérance via le tunnel réseau MX75.

Implémentation de contournement

Étape 1: Configuration du module RSM (Roaming Security Module) avec le réseau enregistré

Remplacez la configuration de tunnel réseau existante par un déploiement RSM combiné à une configuration de réseau enregistré. Cette configuration permet d'attribuer correctement les identités et d'appliquer les politiques.

Étape 2: Valider la visibilité des identités

Après avoir implémenté la configuration du réseau enregistré, vérifiez que :

- Les identités utilisateur sont correctement affichées dans la recherche d'activité
- Les identités des clients itinérants sont visibles et attribuées correctement
- Règles de direction du trafic basées sur la fonction d'identité de l'utilisateur et du client

Étape 3: Tester la fonctionnalité de pilotage du trafic

Vérifiez que les règles de direction du trafic basées sur le domaine et les stratégies basées sur l'identité s'appliquent correctement avec la nouvelle configuration.

Approche alternative

Dans les environnements où la séparation des identités sur des réseaux privés n'est pas

nécessaire, envisagez de mettre en oeuvre la configuration RSM - Internet. Cette approche envoie le trafic RSM directement sur Internet plutôt que via le tunnel du réseau privé, ce qui peut fournir une visibilité correcte de l'identité tout en conservant les contrôles de sécurité.

Analyse technique

Lors du dépannage, les résultats du diagnostic ont été collectés à l'aide de policy.test.sse.cisco.com pour démontrer le comportement d'attribution d'identité lorsque les terminaux se trouvaient derrière le tunnel MX75. L'analyse a confirmé que bien que le routage des identités d'itinérance via un tunnel réseau soit techniquement possible, il ne s'agit pas d'un flux opérationnel recommandé ou pris en charge pour ce scénario de déploiement spécifique.

Motif

La cause principale est liée à la façon dont Secure Access gère l'attribution d'identité lorsque le trafic traverse l'infrastructure du tunnel réseau. Lorsque les points d'extrémité se connectent via le tunnel réseau MX75, le système attribue tout le trafic à l'identité du tunnel plutôt que de conserver les identités individuelles du client et de l'utilisateur en itinérance. Ce comportement est conçu pour les connexions de tunnel réseau, mais est en conflit avec les exigences de visibilité des identités individuelles et d'application de politiques.

Bien qu'il soit techniquement possible d'acheminer des identités d'itinérance via des tunnels réseau, cette configuration n'est pas recommandée ou prise en charge en tant que flux opérationnel standard en raison des limitations d'attribution d'identité décrites ci-dessus.

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.