Umbrella Proxy bloque la connectivité des applications Ninja

Table des matières

Problème

Les utilisateurs ne peuvent pas exécuter un système distant à l'aide d'un fichier d'installation téléchargé lorsqu'ils sont connectés via Cisco Umbrella. L'application ne fonctionne pas sous la protection Umbrella, ce qui affecte particulièrement l'accès au système distant. Le même système distant fonctionne parfaitement sans aucun problème lorsque le proxy Cisco Umbrella est désactivé.

Les tentatives de dépannage comprenaient un test avec une stratégie distincte où la sécurité et la destination du système étaient définies sur ANY, mais le problème persistait. En outre, le routage du trafic via ZTA (Zero Trust Access) a été tenté, mais le problème est resté inchangé. Le trafic était autorisé via l'accès sécurisé sur TCP/443, mais les connexions étaient toujours bloquées sur le terminal.

Environnement

- Cisco Umbrella avec fonctionnalité de proxy activée
- Configuration ZTA (Zero Trust Access)
- Stratégies d'accès sécurisé configurées pour le trafic TCP/443

Résolution

La résolution implique l'exclusion de domaines spécifiques liés à NinjaOne du proxy Umbrella pour permettre une connectivité directe pour l'application d'accès à distance.

Étape 1: Identifier les domaines affectés

L'analyse de la capture de paquets et des fichiers HAR révèle que ces domaines liés à NinjaOne sont affectés par le proxy Umbrella :

- ninjarmm.net
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

Étape 2: Configurer les exemptions de domaine

Excluez les domaines identifiés des stratégies de sécurité Internet Secure Web Gateway (SWG) et du pilotage du trafic Internet ZTA. Ce changement de configuration permet à ces domaines de contourner le proxy Umbrella et d'établir des connexions directes.

Remarque : Une configuration de liste Ne pas déchiffrer (NPD) a été considérée comme inefficace pour résoudre ce problème. L'orientation du trafic et l'exemption sont l'approche recommandée.

Étape 3: Appliquer les modifications de configuration

Implémentez les exemptions de domaine dans la configuration Umbrella pour exclure le trafic lié à NinjaOne du traitement proxy. Cela permet à l'application d'accès à distance d'établir des connexions directes aux services requis.

Étape 4: Valider la résolution

Testez la fonctionnalité de l'application d'accès à distance après l'application des exemptions pour vous assurer que la connectivité est rétablie tout en maintenant la protection Umbrella pour le reste du trafic.

Motif

Le problème se produit parce que les applications d'accès à distance NinjaOne rejettent les connexions proxy lorsque le trafic est acheminé via le proxy Cisco Umbrella. L'application nécessite une connectivité directe à des domaines NinjaOne spécifiques pour fonctionner correctement. Lorsque ces connexions sont mises en proxy via Umbrella, le service d'accès à distance ne peut pas établir les canaux de communication nécessaires, ce qui entraîne une défaillance de l'application même lorsque les stratégies de sécurité sont configurées pour autoriser le trafic.

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.