Problèmes de connectivité FQDN hébergée par Azure grâce à l'accès sécurisé avec l'intégration Meraki

Table des matières

Problème

Des FQDN spécifiques hébergés sur Azure deviennent inaccessibles lorsque le trafic utilisateur est acheminé via Meraki vers Cisco Secure Access, malgré les journaux d'accès sécurisé indiquant que le trafic est « autorisé ». Le problème affecte principalement la connectivité RDP à ces FQDN à l'aide de ports non standard.

Lors de la recherche de journaux par FQDN dans le portail d'accès sécurisé, seuls les journaux de sécurité DNS affichent l'état « autorisé ». Cependant, la connectivité RDP aux mêmes destinations sur les ports non standard échoue. Lorsque le nom de domaine complet est résolu en adresse IP et que la recherche d'activité utilise l'adresse IP de destination, les journaux du pare-feu cloud qui bloquaient le trafic sont révélés.

Environnement

- Cisco Secure Access (SSE) avec intégration Meraki
- Tableau de bord Meraki avec fonction de séparation locale
- Ressources de développement hébergées Azure nécessitant un accès RDP sur des ports non standard
- Routage du trafic via le tunnel Meraki vers un accès sécurisé

Résolution

Solution de contournement immédiate

Ajoutez les FQDN concernés aux règles de séparation locales de Meraki pour contourner l'accès sécurisé pour les destinations spécifiques détaillées dans les sections suivantes.

Étape 1: Accéder au tableau de bord Meraki

Accédez au tableau de bord Meraki et localisez la section de configuration séparée locale.

Étape 2: Configurer les règles de répartition locale

Ajoutez les noms de domaine complets problématiques aux règles de séparation locales pour contourner le routage d'accès sécurisé. Cette modification de configuration restaure immédiatement l'accès des utilisateurs concernés en acheminant le trafic directement de Meraki vers Internet, en contournant le tunnel d'accès sécurisé.

Dépannage et analyse

Étape 1: Analyse des journaux par FQDN

Recherchez les journaux d'activité Secure Access en utilisant le FQDN. Cette option affiche principalement les journaux de sécurité DNS et peut afficher l'état « autorisé » pour le trafic Web sur le port 443.

Étape 2: Analyse du journal par adresse IP de destination

Résolvez le nom de domaine complet à son adresse IP et recherchez les journaux d'activité en utilisant l'adresse IP de destination au lieu du nom de domaine complet. Cela permet d'afficher les

journaux du pare-feu cloud qui affichent le trafic bloqué, en indiquant la disposition réelle du trafic.

Étape 3: Vérification du flux de trafic

Vérifiez que le problème se produit uniquement lorsque le trafic suit le chemin : Utilisateur → Meraki → Tunnel → Accès sécurisé → Internet. Testez que le contournement via la séparation locale résout le problème de connectivité.

Résolution à long terme

Le comportement observé a été identifié comme une fonctionnalité attendue dans la mise en oeuvre d'accès sécurisé actuelle. Une demande de fonctionnalités (FR CSE-I-5543) a été ouverte pour répondre aux préoccupations de visibilité et de fonctionnalité liées à :

- Différence entre les recherches de journaux basées sur FQDN et sur IP
- Rapports de disposition de trafic incohérents entre les journaux de sécurité DNS et de pare-feu cloud
- Meilleure visibilité du trafic RDP sur les ports non standard

Motif

Le problème provient d'une différence dans la façon dont Secure Access traite et signale le trafic pour les FQDN hébergés Azure lorsqu'ils sont accessibles via RDP sur des ports non standard. Lors de la recherche de journaux par FQDN, le système affiche principalement les journaux de sécurité DNS indiquant l'état « autorisé » pour le trafic Web (généralement le port 443). Cependant, le trafic RDP réel sur les ports non standard est traité par les règles du pare-feu cloud, qui ne sont visibles que lors de la recherche par l'adresse IP de destination résolue plutôt que par le nom de domaine complet.

Cela crée un écart de visibilité où les administrateurs voient le trafic « autorisé » dans les recherches basées sur FQDN alors que les connexions RDP réelles sont bloquées par des stratégies de pare-feu qui ne sont apparentes que dans les recherches de journaux basées sur IP. Le comportement est actuellement considéré comme une fonctionnalité attendue, mais une

demande de fonctionnalité a été soumise pour améliorer la visibilité et la cohérence des rapports de trafic entre les différentes méthodes de recherche.

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.