Le blocage du protocole d'application d'accès sécurisé empêche la connectivité Internet

Table des matières

- Problème
- Environnement
- Résolution
  - Étape 1: Identifier la règle de blocage
  - Étape 2: Modifier les paramètres d'application
  - Étape 3: Application et vérification des modifications
- Motif
- Autres informations utiles

Problème

Après la migration vers Cisco Secure Access, les utilisateurs ont rencontré un blocage de la connectivité Internet lorsqu'ils tentaient d'accéder aux services Web. Le symptôme spécifique impliquait le blocage du trafic HTTP par la stratégie de sécurité, empêchant l'accès aux sites Web et applications légitimes.

Les détails de l'événement de blocage présentaient les caractéristiques suivantes :

- Action : Bloqué
- Motif du blocage des événements : BLOC_CORRESPONDANCE_RÈGLE_AC
- Destination : http://www.bing.com/api/shopping/v1/user/shoppingsettings

- Port de destination : 443
- Catégories : Non Classé
- Catégorie d'application : Rechercher
- Protocole d'application : Hypertext Transfer Protocol
- Protocole : TCP

Environnement

- déploiement de Cisco Secure Access
- Stratégie de sécurité active avec restrictions de protocole d'application

Résolution

La résolution implique de modifier la configuration de la règle de sécurité pour autoriser le trafic du protocole d'application HTTP tout en maintenant la position de sécurité pour les applications réellement non fiables.

Étape 1: Identifier la règle de blocage

Localisez la règle spécifique à l'origine du blocage dans l'interface de gestion d'accès sécurisé :

- Nom de la règle : Essai
- Configuration actuelle : Utilisation du bloc de paramètres d'application comme destination.

Étape 2: Modifier les paramètres d'application

Accédez à la configuration de la règle et vérifiez le nom des paramètres d'application dans

Destination :

- Accédez à Resources > Internet and SaaS resources > Application Lists. Cliquez ensuite sur l'application.
- Localisez les paramètres du protocole d'application.
- Décochez ou supprimez HTTP de la liste des protocoles d'application bloqués.
- S'assurer que d'autres contrôles de sécurité restent en place pour les applications réelles non fiables.

Étape 3: Application et vérification des modifications

Enregistrez les modifications de règle et testez la connectivité :

1.- Appliquez les modifications de configuration à la stratégie active.

2.- Testez la connectivité Internet vers des destinations précédemment bloquées.

3.- Surveillez les journaux de sécurité pour vous assurer que le trafic HTTP légitime est désormais autorisé.

4.- Vérifiez que les autres protections de sécurité restent efficaces.

Motif

La cause principale était une configuration de règle de sécurité trop restrictive dans Cisco Secure Access. La règle a été configurée pour bloquer tout le trafic du protocole d'application HTTP, ce qui a empêché la navigation légitime sur le Web et l'accès aux applications. L'application étendue du blocage du protocole HTTP a affecté la connectivité Internet normale pour les utilisateurs accédant à des services Web et applications légitimes qui utilisent les protocoles HTTP/HTTPS.

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.