Dépannage des problèmes MS Teams avec la configuration du profil d'accès Zero Trust

Table des matières

Problème

Les utilisateurs inscrits à un profil ZTA (Zero Trust Access) pour un accès Internet sécurisé ont rencontré des problèmes de connectivité d'appel Microsoft Teams. Lorsque des utilisateurs sont ajoutés au profil ZTA, les appels Microsoft Teams se déconnectent de manière inattendue et les autres utilisateurs ne peuvent pas passer d'appels à l'utilisateur concerné. Cependant, les appels se connectent correctement lorsque l'utilisateur concerné initie l'appel de son côté.

Le problème est isolé pour les utilisateurs intégrés au profil ZTA, ce qui indique que les stratégies ZTA ou les configurations de routage ont un impact sur la connectivité des appels des équipes. Les journaux de trafic indiquent que le trafic de Microsoft Teams provenant de processus tels que ms-teams.exe vers des adresses IP comprises dans les plages requises (par exemple 52.115.245.30:3480, qui fait partie de 52.112.0.0/14) est intercepté par le client ZTA au lieu d'être directement dirigé vers Internet.

Environnement

- Configuration du profil Cisco Secure Access avec ZTA (Zero Trust Access)
- Profil ZTA configuré avec « Utiliser ZTA pour sécuriser toutes les destinations Internet »
- Application Microsoft Teams
- Cisco Secure Client avec fonctionnalités ZTA
- Utilisateurs inscrits au profil ZTA pour un accès Internet sécurisé

Résolution

Pour résoudre le problème, ajoutez des exceptions de trafic Microsoft Teams à la configuration du profil ZTA pour permettre au trafic Teams de contourner le tunnel ZTA et de se connecter directement à Internet :

1. Accédez à Dashboard > End User Connectivity > Zero Trust Access et localisez le profil ZTA affecté.

2. Sélectionnez le profil ZTA et choisissez Edit > Secure Internet Access.

3. Ajoutez ces plages d'adresses IP et ces noms de domaine complets à la liste d'exceptions de la documentation officielle de Microsoft :

Plages IP :

```
52.112.0.0/14
52.122.0.0/15
2603:1063::/38
2603:1027::/48
2603:1037::/48
2603:1047::/48
2603:1057::/48
2620:1ec:6::/48
2620:1ec:40::/42
```

FQDN :

```
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
teams.microsoft.com
*.keydelivery.mediaservices.windows.net
*.streaming.mediaservices.windows.net
aka.ms
```

4. Ajoutez une description des exceptions, par exemple :

```
MS Teams exception as per: https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-addre
```

5. Enregistrez les modifications de configuration. Attendez quelques minutes que les modifications soient appliquées.

6. Assurez-vous que la stratégie du client ZTA est resynchronisée sur les terminaux affectés. Cela peut nécessiter le redémarrage du service Zero Trust Access Agent ou le redémarrage du périphérique client.

7. Testez la fonctionnalité d'appel des équipes pour vérifier que :

- Les appels entrants destinés aux utilisateurs affectés se connectent désormais correctement
- Les appels d'équipe ne se déconnectent plus inopinément
- Le trafic des équipes contourne le tunnel ZTA et se connecte directement à Internet

---

Remarque : Une fois les exceptions implémentées, le trafic Teams n'apparaît pas dans les journaux d'activité Secure Access, car il contourne entièrement le tunnel ZTA.

Motif

Le problème est causé par le trafic Microsoft Teams acheminé via le tunnel ZTA Secure Internet Access au lieu de se connecter directement à Internet. Lorsque le profil ZTA est configuré avec l'option « Secure All Internet Destinations », il intercepte le trafic multimédia des équipes, y compris les flux UDP nécessaires à la communication en temps réel. Cela entraîne des problèmes de connectivité, en particulier pour les appels entrants et les flux multimédias.

Microsoft recommande de contourner le trafic Microsoft Teams des serveurs proxy et l'inspection SSL pour des performances et une qualité d'appel optimales. Lorsque la configuration ZTA ne comporte pas les exceptions nécessaires pour le trafic Teams, le flux de support d'application est traité via le client ZTA au lieu de prendre le chemin direct requis pour la communication en temps réel.

Autres informations utiles

- Plages d'adresses IP et d'URL Microsoft 365 - Microsoft Teams
- Recommandations de Microsoft Teams Proxy Server
- Dépannage et collecte des informations de base pour Cisco Secure Access

- 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.