Vérification de la fonctionnalité de comportement de contournement pour la compatibilité avec Secure Access Microsoft 365

Table des matières

Problème

Lors de la configuration de Cisco Secure Access avec la fonctionnalité de compatibilité Microsoft 365 activée, il existe une incertitude quant à savoir si des noms de domaine complets (FQDN) spécifiques liés à Microsoft sont automatiquement contournés par le traitement Secure Web Gateway (SWG) et le déchiffrement TLS. En particulier, des clarifications sont nécessaires concernant le comportement de contournement pour ces domaines :

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

La principale préoccupation est de savoir si ces domaines doivent être ajoutés manuellement à la liste Ne pas décrypter ou s'ils sont automatiquement exclus lorsque la compatibilité avec Microsoft 365 est activée. En outre, il existe une confusion au sujet de l'interaction entre les contournements de niveau SWG et les paramètres de déchiffrement de niveau IPS, en particulier pour manage.microsoft.com qui apparaît dans la documentation suggérant que la configuration manuelle de la liste de ne pas déchiffrer peut encore être requise.

Environnement

- Accès sécurisé Cisco
- Fonctionnalité de compatibilité Microsoft 365 activée
- Inspection Secure Web Gateway (SWG) et décryptage TLS configurés
- Stratégies de déchiffrement IPS utilisées
- Services de gestion et de mise à jour Microsoft nécessitant une connectivité

Résolution

Le comportement de la fonctionnalité de compatibilité de Microsoft 365 a été vérifié par des tests en laboratoire avec les résultats suivants :

Étendue des fonctionnalités de compatibilité Microsoft 365

La fonctionnalité de compatibilité Microsoft 365 exempte les domaines liés à Microsoft 365 marqués comme « Optimiser » et « Autoriser » dans les catégories de terminaux de Microsoft de l'inspection SWG et de l'application de la stratégie. Cela permet au trafic vers ces domaines de passer sans modification au niveau de la couche SWG.

Résultats des tests en laboratoire

Les tests ont été réalisés dans un environnement de laboratoire contrôlé avec la compatibilité Microsoft 365 activée. Ce comportement a été observé pour les noms de domaine complets spécifiés :

Étape 1: Activer la fonctionnalité de compatibilité Microsoft 365

La fonctionnalité de compatibilité Microsoft 365 a été activée dans la configuration d'accès sécurisé.

Étape 2: Tester le trafic vers les FQDN cibles

Le trafic Web a été généré vers chacun des trois FQDN à l'aide d'un navigateur Internet standard :

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Étape 3: Vérifier le comportement de contournement dans le tableau de bord

L'analyse du tableau de bord d'accès sécurisé a confirmé que l'inspection et le déchiffrement du trafic Web n'étaient pas effectués pour le trafic vers ces destinations spécifiques lorsque la fonctionnalité de compatibilité Microsoft 365 a été activée.

Étape 4: Confirmer le comportement de direction DNS

Le trafic DNS vers ces destinations a continué d'être dirigé via Secure Access, qui s'aligne sur le comportement documenté à moins qu'une exemption DNS spécifique ne soit configurée.

Principales conclusions comportementales

Sur la base des résultats des tests et de l'analyse de la documentation :

- Contournement SWG : Les trois noms de domaine complets spécifiés sont ignorés de l'inspection du trafic Web lorsque la compatibilité Microsoft 365 est activée.
- Déchiffrement TLS : Le déchiffrement est contourné au niveau de la couche SWG pour ces domaines.
- Pilotage DNS : Les requêtes DNS continuent d'être traitées via Secure Access, sauf en cas d'exemption explicite.
- Couverture du domaine : Bien que le domaine « *.microsoft.com » dans son ensemble ne soit pas entièrement contourné par la spécification, les URL spécifiques testées sont contournées dans la pratique.

Considérations relatives à la couche IPS

La fonctionnalité de compatibilité Microsoft 365 fonctionne au niveau de la couche SWG. Pour le contournement du déchiffrement au niveau IPS, une configuration manuelle peut toujours être requise :

- Si le contournement du décodage IPS est également souhaité pour ces domaines, l'ajout manuel à la liste Ne pas déchiffrer peut s'avérer nécessaire.
- La liste Ne pas déchiffrer affecte principalement le déchiffrement côté IPS plutôt que le traitement SWG.
- Ceci explique pourquoi la documentation peut faire référence à l'ajout de

manage.microsoft.com à la liste Ne pas déchiffrer même lorsque la compatibilité Microsoft 365 est activée.

Motif

La confusion provient de l'architecture en couches de Cisco Secure Access, où la compatibilité Microsoft 365 affecte le traitement au niveau SWG, tandis que le décryptage IPS fonctionne comme une couche séparée avec ses propres exigences de configuration. La fonctionnalité Compatibilité Microsoft 365 gère automatiquement le contournement SWG pour les domaines Microsoft qualifiés, mais les stratégies de décodage IPS peuvent nécessiter une configuration séparée via la liste Ne pas déchiffrer.

Autres informations utiles

- Documentation de compatibilité de Cisco Secure Access pour Microsoft 365
- Créer une liste de refus de déchiffrement efficace pour l'accès sécurisé Cisco
- 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.