

Limites de la stratégie DLP avec WhatsApp dans l'accès sécurisé

Table des matières

Problème

Les politiques DLP de Cisco Secure Access ne détectent pas ou ne bloquent pas les fichiers sensibles lorsqu'ils sont partagés via WhatsApp (navigateur ou application de bureau), malgré l'activation du déchiffrement HTTPS. Le moteur DLP ne parvient pas à déclencher ou à détecter les téléchargements de fichiers via ces plates-formes, tandis que les mêmes stratégies DLP bloquent avec succès les fichiers identiques lorsqu'ils sont téléchargés via d'autres outils de téléchargement en ligne. Lors du test du blocage de base des téléchargements pour WhatsApp, la fonctionnalité fonctionne correctement sur les versions de navigateur et de bureau, mais le problème est spécifiquement isolé pour l'application de la politique DLP.

Environnement

- Accès sécurisé Cisco
- Stratégies DLP configurées
- Décryptage HTTPS activé
- Applications WhatsApp Web et WhatsApp Desktop

Résolution

Le comportement observé est une limitation attendue de WhatsApp et des plates-formes similaires en raison de leur mise en oeuvre de cryptage de bout en bout (E2EE) et de la gestion du trafic non standard. Les étapes de dépannage décrites dans les sections suivantes et la solution de contournement peuvent être mises en oeuvre.

Dépannage des étapes de vérification

Avant d'implémenter la solution de contournement, vérifiez les éléments de configuration suivants :

- Assurez-vous que l'identité/l'ID d'origine SWG est correctement configuré.
- Vérifiez que l'inspection/le déchiffrement HTTPS est activé et n'est pas contourné de manière sélective pour les plates-formes cibles.
- Vérifiez que les paramètres Isolation/RBI et Allow-Override sont correctement configurés.
- Confirmez l'appartenance au groupe AD si les stratégies DLP sont basées sur un groupe.
- Vérifiez les listes de contournement de Traffic Steering pour toute exclusion.
- Vérifiez que le protocole QUIC est désactivé dans les navigateurs.
- Recherchez les effets du trafic IPv6 qui pourraient contourner l'inspection.

Solution recommandée

Pour activer l'application DLP pour le trafic Web WhatsApp, implémentez l'isolation du navigateur distant (RBI) pour le trafic destiné à WhatsApp Web. Cette solution de contournement permet d'appliquer les politiques DLP en isolant la session du navigateur et en activant l'inspection du contenu dans l'environnement isolé.

Configurez l'application RBI spécifiquement pour les domaines Web WhatsApp pour garantir que les téléchargements de fichiers et le partage de contenu via l'interface Web sont soumis à l'évaluation de la stratégie DLP.

Additional Information

Une demande d'amélioration de produit a été documentée pour cette limitation - CSE-I-1249.

Motif

WhatsApp (y compris WhatsApp Web) et les plates-formes de collaboration similaires implémentent un chiffrement de bout en bout (E2EE) qui empêche l'inspection complète du contenu et l'analyse du texte des messages et des téléchargements de fichiers. En outre, le trafic WhatsApp n'utilise pas les ports HTTP/HTTPS standard de la même manière que les téléchargements Web classiques, ce qui signifie que la passerelle Web sécurisée (SWG) ne peut pas intercepter et inspecter le trafic via le chemin d'inspection HTTPS normal. Cette méthode de cryptage et de gestion du trafic est conçue de manière à limiter les capacités d'inspection DLP actuelles pour ces plates-formes spécifiques.

Autres informations utiles

- [Demande d'amélioration du produit CSE-I-1249](#)
- [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.