

Configuration du téléchargement du fichier ZIP protégé par mot de passe d'accès sécurisé

Table des matières

Problème

Après la migration vers Cisco Secure Access, les utilisateurs ne peuvent pas télécharger de fichiers ZIP protégés par mot de passe (chiffrés). Les téléchargements échouent systématiquement lors d'une tentative d'accès au contenu de fichiers chiffrés via le service d'accès sécurisé. Ce problème se produit malgré la configuration de stratégies de trafic liées à Internet sur un périphérique C8200 avec plusieurs règles de sécurité, notamment le blocage par catégorie, les contrôles d'inspection SSL et la fonctionnalité sandbox.

Les utilisateurs rencontrent des échecs de téléchargement complets lorsqu'ils tentent d'accéder à des fichiers ZIP protégés par mot de passe qui étaient auparavant accessibles avant la migration Secure Access. Le problème persiste sur plusieurs groupes de tunnels et affecte les 15 emplacements configurés.

Environnement

- Accès sécurisé Cisco (Secure Access OrgID : 8320925)
- Périphérique C8200 gérant les politiques de trafic liées à Internet
- Groupes de tunnels multiples sur 15 sites (TK-TG et autres)
- Stratégies d'inspection SSL avec configurations activées et désactivées
- Profils de sécurité Sandbox activés sur certaines stratégies
- Profils IPS configurés sur des règles d'accès spécifiques

Résolution

La résolution pour autoriser les téléchargements de fichiers ZIP protégés par mot de passe dans Cisco Secure Access implique la configuration du paramètre Autoriser l'accès aux fichiers chiffrés et la mise en oeuvre de solutions de contournement appropriées si nécessaire.

Méthode de configuration principale

Étape 1: Accéder à la configuration de la stratégie d'accès sécurisé Cisco

Accédez à la stratégie d'accès spécifique qui gère le trafic affecté dans votre tableau de bord Cisco Secure Access.

Étape 2: Activer l'accès aux fichiers chiffrés

Dans la stratégie Paramètres avancés, localisez et activez l'option Autoriser l'accès aux fichiers chiffrés. Ce paramètre est configuré par règle et contrôle si le contenu chiffré est accessible via cette stratégie spécifique.

Étape 3: Application de la configuration

Enregistrez et appliquez les modifications de stratégie pour les rendre actives pour le trafic utilisateur.

Méthode de contournement alternative

Si la méthode principale ne résout pas le problème, mettez en oeuvre la solution de contournement décrite dans les sections suivantes.

Étape 1: Identifier les URL affectées

Déterminez les URL ou les domaines spécifiques où les fichiers ZIP protégés par mot de passe sont hébergés et provoquent des échecs de téléchargement.

Étape 2: Configurer la liste Ne pas déchiffrer

Ajoutez les URL identifiées à la liste Do Not Decrypt dans votre configuration Cisco Secure Access. Cela empêche l'inspection SSL sur ces URL spécifiques.

Étape 3: Créer une stratégie de contournement d'inspection SSL

Assurez-vous qu'une stratégie d'accès avec l'inspection SSL désactivée est configurée pour gérer le trafic vers ces URL.

Cette politique doit comporter :

- Inspection SSL désactivée
- Tous les profils de sécurité désactivés
- Priorité supérieure aux stratégies SSL activées pour l'inspection

Référence de configuration de stratégie

L'ordre des politiques décrit dans les sous-sections suivantes et leurs configurations respectives peuvent être utilisés comme référence pour une gestion appropriée du trafic.

Politique 1 : Règle de blocage basée sur les catégories

- Nom de la stratégie : IA-To-InternetContentBlock
- Profil IPS : Aucune

- Objectif: Bloquer des catégories de contenu spécifiques
- Target (cible) : Tous les groupes de tunnels

Politique 2 : Règle d'inspection SSL désactivée

- Nom de la stratégie : IA-SSL-Inspection-MUKOU
- Profil IPS : Désactivé
- Profils de sécurité : Tous désactivés
- Target (cible) : Tous les groupes de tunnels

Politique 3 : Règle SSL activée pour l'inspection

- Nom de la stratégie : IA-SSL-Inspection
- Profil IPS : Activée
- Profils de sécurité : Fonctionnalité sandbox activée
- Target (cible) : Tous les groupes de tunnels

Notes de configuration importantes

Il n'existe aucun équivalent de paramètres globaux pour la fonctionnalité Autoriser l'accès aux fichiers chiffrés. Ce paramètre doit être configuré sur les stratégies d'accès individuelles, le cas échéant. Ce paramètre doit être explicitement activé dans la configuration des paramètres avancés de chaque stratégie nécessitant un accès chiffré aux fichiers.

Lorsque vous testez des modifications de configuration, laissez suffisamment de temps pour la propagation des politiques dans l'infrastructure d'accès sécurisé Cisco avant de valider la fonctionnalité. Les incidents de service ou les fenêtres de maintenance peuvent affecter les résultats des tests et doivent être pris en compte lors du dépannage.

Motif

Le problème se produit parce que Cisco Secure Access, par défaut, bloque l'accès aux fichiers chiffrés par mesure de sécurité. Lorsque l'inspection SSL est activée et rencontre du contenu protégé par mot de passe ou chiffré, le service empêche le téléchargement sauf s'il est explicitement configuré pour autoriser un tel accès. Le paramètre Autoriser l'accès aux fichiers chiffrés dans les paramètres avancés des stratégies d'accès contrôle ce comportement, et sans ce paramètre activé, les fichiers ZIP chiffrés et le contenu similaire sont bloqués pendant le processus de téléchargement.

En outre, les stratégies d'inspection SSL peuvent interférer avec les téléchargements de fichiers chiffrés lorsque le processus d'inspection ne peut pas traiter correctement le contenu chiffré, nécessitant soit le paramètre d'accès au fichier chiffré, soit le contournement de l'inspection SSL pour les URL affectées.

Autres informations utiles

- [Contrôles de sécurité avancés](#)
- [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.