Configurer File Inspector pour autoriser les fichiers protégés par mot de passe et les autres fichiers non malveillants

Table des matières

Introduction

Problème

Solution

- Solution alternative

Introduction

Ce document décrit comment empêcher un fichier non malveillant d'être bloqué par l'inspection de fichier.

Problème

L'activation de l'inspection des fichiers dans certains cas bloque les fichiers non malveillants. Ces types de fichiers sont les suivants :

- Fichiers protégés par mot de passe
- Fichiers d'application potentiellement indésirables (corrompus)

Ces fichiers sont bloqués par Umbrella car ils ne peuvent pas être décompressés et analysés par notre outil antivirus. Les fichiers protégés par mot de passe peuvent apparaître bloqués dans la catégorie « Fichier protégé ». Les fichiers corrompus peuvent inclure des fichiers dont le contenu est chiffré, dont le contenu archivé ne peut pas être extrait, dont les données compressées ou l'en-tête d'archive ne sont pas valides, ou qui sont simplement compressés ou archivés dans un format non pris en charge. Bien que ces fichiers puissent être non malveillants, Umbrella les bloque par défaut par précaution car les fichiers ne peuvent pas être analysés.

Solution

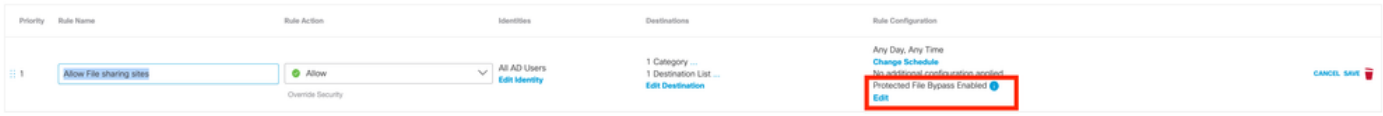
Si vous connaissez un fichier non malveillant qui a été bloqué pour l'une des raisons ci-dessus, vous pouvez contourner ce problème en autorisant les fichiers protégés. Le comportement de blocage des fichiers protégés peut désormais être modifié au niveau global ou dans une règle Web individuelle.

- Règle (recommandée) - Autoriser les fichiers protégés pour une identité et/ou une destination. Procédez de la sorte si vous souhaitez faire confiance aux fichiers protégés d'une destination particulière ou si vous souhaitez remplacer le comportement d'un

utilisateur/groupe individuel.
- Global - Autoriser les fichiers protégés pour tous les utilisateurs dans toutes les règles/ensembles de règles. Procédez ainsi si vous acceptez le risque de téléchargement de fichiers protégés et préférez cette option à la charge administrative liée à la création d'exceptions plus granulaires.

Règle

Vous pouvez modifier la fonctionnalité en modifiant une règle Web sur la page Stratégies > Stratégies Web.



10588971481748

Global

La fonctionnalité peut être modifiée dans Stratégies > Stratégies Web > Paramètres globaux.

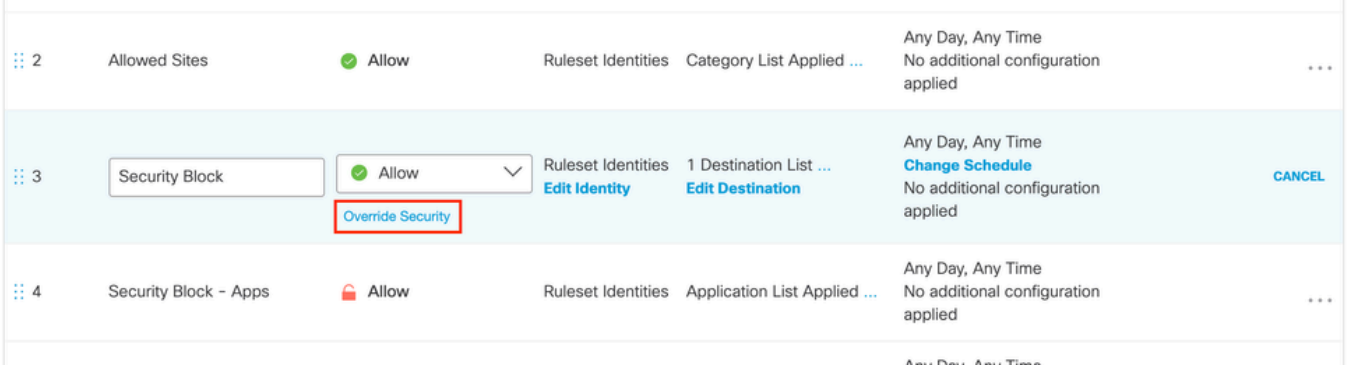


10589018672020

Solution alternative

Il est également possible de contourner les problèmes avec l'inspection de fichier en utilisant l'option Override Security dans n'importe quelle stratégie web. Cette option doit être utilisée avec prudence car elle désactive tous les autres paramètres de sécurité, y compris le blocage des fichiers malveillants.

- Pour les fichiers protégés, utilisez plutôt l'une des solutions décrites dans ce document.
- Utilisez cette option uniquement lorsque vous faites confiance à la destination avec une certitude absolue et que vous n'avez aucune autre option pour contourner le problème.
- Pour les faux positifs antivirus, obtenez confirmation que le fichier est sain auprès de Cisco Talos avant d'implémenter une solution de contournement. Si nécessaire, voir Envoyer des demandes d'examen de sécurité sans réponse rapide.



Capture d'écran_2021-10-07_at_2.59.04_PM.png

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.