パスワードで保護されたその他の悪意のないファイルを許可するためのファイルインスペクタの設定

内容

はじめに

問題

解決方法

代替ソリューション

はじめに

このドキュメントでは、悪意のないファイルがファイルインスペクションによってブロックされることを防ぐ方法について説明します。

問題

「ファイルインスペクション」を有効にすると、悪意のないファイルがブロックされる場合があります。次のようなファイルがあります。

- パスワードで保護されたファイル
- Potentially Unwanted Application(Corrupt)ファイル

これらのファイルは、ウイルス対策ツールで解凍およびスキャンできないため、Umbrellaによってブロックされます。パスワードで保護されたファイルは、「保護されたファイル」カテゴリでブロックされているように見える場合があります。破損したファイルには、暗号化されたコンテンツを含むファイル、アーカイブされたコンテンツを抽出できないファイル、圧縮されたデータが無効なファイル、アーカイブヘッダーが無効なファイル、サポートされていない形式で圧縮またはアーカイブされたファイルなどが含まれます。これらのファイルは悪意がない可能性がありますが、Umbrellaはファイルをスキャンできないため、予防策としてデフォルトでブロックします。

解決方法

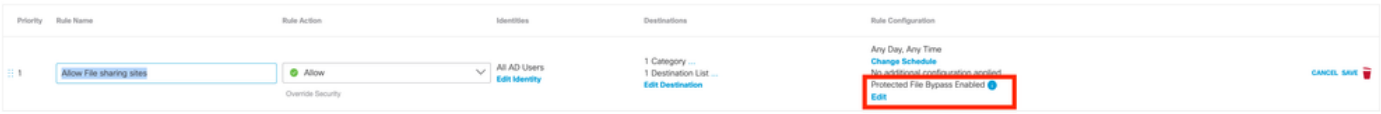
上記のいずれかの理由でブロックされた悪意のないファイルがわかっている場合は、保護されたファイルを許可することで、この問題を回避できます。 保護されたファイルをブロックする動作を、グローバルレベルまたは個々のWebルールで変更できるようになりました。

- 規則（推奨）- IDまたは宛先に対して保護されたファイルを許可します。 特定の宛先からの保護されたファイルを信頼する場合、または個々のユーザー/グループの動作を上書きする場合に、この操作を行います。

- Global：すべてのルール/ルールセット内のすべてのユーザに対して保護されたファイルを許可します。 保護されたファイルのダウンロードのリスクを受け入れ、より詳細な例外を作成するという管理上の負担よりも、このオプションの方が優先される場合に、この操作を行います。

ルール

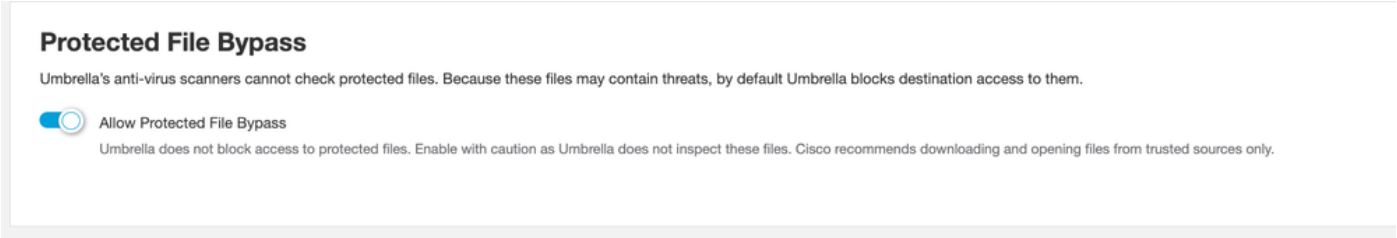
この機能を変更するには、Policies > Web PoliciesページでWebルールを編集します。



10588971481748

グローバル

この機能は、Policies > Web Policies > Global Settingsで変更できます。

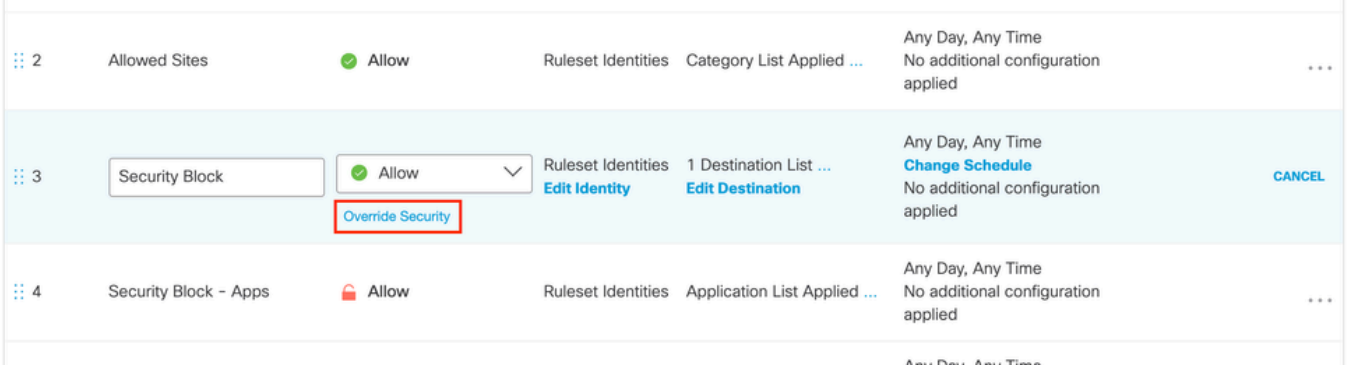


10589018672020

代替ソリューション

また、任意のWebポリシーでOverride Securityオプションを使用することにより、ファイルインスペクションの問題を回避することもできます。このオプションは、悪意のあるファイルのブロックを含む他のすべてのセキュリティ設定を無効にするため、注意して使用する必要があります。

- 保護されたファイルの場合は、代わりに、このドキュメントで説明するソリューションのいずれかを使用します。
- これは、宛先が絶対的に確実であると信頼でき、問題を回避する他のオプションがない状況でのみ使用してください。
- アンチウイルスの誤検出については、回避策を実行する前に、Cisco Talosからファイルがクリーンであることを確認します。



スクリーンショット_2021-10-07_at_2.59.04_PM.png

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。