Secure Accessセキュリティプロファイルの警告操作の暗号化解除要件

内容

お問い合わせ内容

アクセスポリシーアクションが警告に設定されている場合、セキュリティプロファイル設定で復号を有効にする必要があるかどうかに関する、Cisco Secure Accessの設定ガイダンスがユーザに必要です。固有の質問は、次のセキュリティプロファイル機能に適用されます。

- 脅威のカテゴリ
- ファイル検査
- Cisco SecureX Malware Analytics
- ファイルタイプブロッキング
- セーフサーチ

この質問は、アクセスポリシーの警告アクションとセキュリティプロファイルの復号化の要件の関係を理解することに重点を置いており、これらのセキュリティ機能が正しく機能するために必要です。

環境

- 製品：Cisco Secure Internet Access Advantage
- テクノロジー：セキュアなアクセス
- ソフトウェアバージョン：すべて
- 設定：さまざまなセキュリティ機能を備えたセキュリティプロファイル
- ポリシーの構成：警告アクションの設定を含むアクセスポリシー

解決策

ラボ検証では、セキュリティプロファイルで復号化だけが有効になっていて、他のすべての機能が無効になっている場合でも、アクセスポリシーの警告操作が正常に機能することが確認されています。つまり、次のセキュリティプロファイル機能では、警告アクションの使用時に、個々の機能に対して復号化を明示的に有効にする必要はありません。

- 脅威のカテゴリ
- ファイル検査
- Cisco SecureX Malware Analytics
- ファイルタイプブロッキング
- セーフサーチ

設定ガイダンス

警告アクションを使用してアクセスポリシーを設定する場合：

ステップ1：目的のポリシールールのアクセスポリシーアクションを警告に設定します。

ステップ2:セキュリティプロファイル設定で、復号がプロファイルレベルで有効になっていることを確認します。

ステップ3：個々のセキュリティ機能（脅威カテゴリ、ファイルインスペクション、Cisco Secure Malware Analytics、ファイルタイプブロッキング、およびセーフサーチ）は、警告アクションを使用して適切に機能している間は、特定の復号化設定で無効のままにすることができます。

この設定方法では、セキュリティプロファイル機能の管理の柔軟性を維持しながら、警告アクションを正しく機能させることができます。

原因

アクセスポリシーの警告アクションは、個々のセキュリティプロファイル機能の復号化要件とは異なるレベルで動作します。警告アクションは、セキュリティプロファイルレベルで有効になっているメインの復号設定でのみ機能し、特定のセキュリティ機能ごとに個別の復号を有効にする必要はありません。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

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。