セキュアアクセスセキュリティプロファイルAPIの詳細設定

内容

問題

パブリックAPIを使用してCisco Secure Accessセキュリティプロファイルを設定しようとすると、デフォルト設定を使用した基本的なプロファイルの作成のみが可能であるという制限があります。このAPIは、次のような高度なセキュリティ機能に対する詳細な設定オプションを公開しません。

- TLS暗号化解除設定
- 脅威カテゴリの適用制御
- ファイルタイプのブロックと検査
- マルウェア検査の設定

標準API呼び出しを使用して復号化設定を構成しようとすると、「403 Forbidden」エラーが発生すると報告されます。文書化されているパブリックAPIエンドポイントには、GUIインターフェイスから使用できる詳細なセキュリティプロファイル設定パラメータがないため、プログラムによる管理機能が制限されているようです。

環境

- Cisco Secure Accessプラットフォーム
- セキュリティプロファイルAPIの実装
- すべてのソフトウェアバージョンが該当
- パブリックAPIドキュメントエンドポイント

解決方法

Cisco Secure Access APIを通じて高度なセキュリティプロファイル設定機能を使用できますが、その際には、文書化されているパブリックAPIの例とは異なる特定の実装方法とフィールド命名規則が必要です。これらの解決手順では、各設定領域に対処します。

基本的なセキュリティプロファイルの作成ワークフロー

詳細設定を使用してセキュリティプロファイルを作成するための適切なワークフローは、2段階のプロセスに従います。

ステップ1:POSTを使用して基本的なセキュリティプロファイルを作成します。

```
POST /api/v1/security-profiles
{
  "name": "profile_name",
  "description": "profile_description"
}
```

ステップ2：プロファイルIDを指定したPUTを使用して、詳細オプションを設定します。

```
PUT /api/v1/security-profiles/{profile_id}
{
  "advanced_settings": {
    "decryption_settings": {...},
    "file_settings": {...},
    "threat_settings": {...}
  }
}
```

ファイルインスペクションおよびファイルタイプブロッキングの設定

ファイルインスペクションとファイルタイプブロッキングは、PUT要求内で次のAPIフィールド名を使用して設定できます。

- fileEngines：ファイルインスペクション機能を制御します。
- fileTypeControlStatus：ファイルタイプブロッキングを有効または無効にします。

ファイル設定の設定例

```
{
  "fileEngines": "enabled",
  "fileTypeControlStatus": "active",
  "blockedFileTypes": ["exe", "zip", "rar"]
}
```

TLS復号化の設定

TLS復号化設定では、専用のPOSTエンドポイントを使用するのではなく、Do Not DecryptリストIDを参照する必要があります。設定は、次のアプローチを使用してPUT API要求を介して実装されます。

ステップ1：既存の設定から、復号化しないリストIDを特定します。

ステップ2:PUT APIリクエストでリストIDを参照します。

```
{
  "seetingGroupBypassInspectionGroupID": "do_not_decrypt_list_id",
  "decryptionEnabled": true
}
```

これにより、他のAPIメソッドを使用して復号化を設定しようとすると発生する「403 Forbidden」エラーが解決されます。

脅威カテゴリの設定

脅威カテゴリの設定は、ドキュメントに記載されていないAPIエンドポイントを通じて行うことができます。このAPIエンドポイントは、復号化の設定に成功するとアクセスできるようになります。このエンドポイントでは、脅威カテゴリのきめ細かい制御が可能ですが、最初に復号化の設定でセキュリティプロファイルを適切に設定する必要があります。

APIフィールド名のリファレンス

次の表は、共通のセキュリティプロファイル機能を、対応するAPIフィールド名にマッピングしたものです。

機能	APIフィールド名	説明
TLS復号化	GroupBypassInspectionGroupIDを設定しています	参照はリストIDを解読しません
ファイル検査	ファイルエンジン	ファイルインスペクション機能を制御
ファイルタイプブロッキング	fileTypeControlStatus	ファイルタイプの制限を有効にします。

原因

この制限は主に、実際の機能制限ではなく、不完全なAPIドキュメントと直感的でないフィールド命名規則が原因でした。高度なセキュリティプロファイルの設定機能はAPI内に存在しますが、次のものを使用して実装されます。

- GUIの用語とは異なる明白でないフィールド名
- 2段階のワークフロー（POSTによる作成、PUTによる高度な設定）
- 既存の設定オブジェクトへの依存関係（復号化しないリストなど）
- 特定の機能に関するドキュメント化されていないAPIエンドポイント

公開されているAPIドキュメントでは、これらの実装の詳細が明確に公開されていないため、別の方法で実際に機能を使用できる場合にAPIの制限が発生するという認識があります。

関連コンテンツ

- Cisco Secure Access Security Profiles APIに関するドキュメント
- 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。