Configuration avancée de l'API des profils de sécurité Secure Access

Table des matières

Problème

Lorsque vous essayez de configurer des profils de sécurité Cisco Secure Access via l'API publique, les utilisateurs rencontrent des limitations où seule la création de profil de base avec les paramètres par défaut est possible. L'API n'offre pas d'options de configuration granulaires pour les fonctions de sécurité avancées, notamment :

- Paramètres de décodage TLS
- Contrôles d'application des catégories de menaces
- Blocage et inspection du type de fichier
- Paramètres d'inspection des programmes malveillants

Les utilisateurs signalent la réception d'erreurs « 403 Forbidden » lors de la configuration des paramètres de décodage via des appels API standard. Les terminaux API publics documentés semblent ne pas disposer des paramètres de configuration détaillés du profil de sécurité disponibles via l'interface utilisateur graphique, ce qui limite les capacités de gestion de la programmation.

Environnement

- Plate-forme Cisco Secure Access
- Implémentation de l'API Security Profiles
- Toutes les versions du logiciel concernées
- Terminaux de documentation API publique

Résolution

Les fonctionnalités avancées de configuration des profils de sécurité sont disponibles via l'API d'accès sécurisé Cisco, mais nécessitent des approches de mise en oeuvre spécifiques et des conventions d'attribution de noms de champ qui diffèrent des exemples d'API publiques documentés. Ces étapes de résolution concernent chaque zone de configuration :

Workflow de création de profil de sécurité de base

Le workflow approprié pour créer des profils de sécurité avec des paramètres avancés suit un processus en deux étapes :

Étape 1: Créez le profil de sécurité de base à l'aide de POST.

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

Étape 2: Configurez les options avancées à l'aide de PUT avec l'ID de profil.

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

Inspection de fichier et configuration du blocage de type de fichier

L'inspection de fichier et le blocage de type de fichier peuvent être configurés à l'aide des noms de champ API suivants dans la demande PUT :

- fileEngines - Contrôle les fonctionnalités d'inspection des fichiers.
- fileTypeControlStatus : active ou désactive le blocage des types de fichiers.

Exemple de configuration des paramètres de fichier :

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

Configuration du décodage TLS

La configuration du déchiffrement TLS nécessite de référencer un ID de liste Ne pas déchiffrer plutôt que d'utiliser un point de terminaison POST dédié. La configuration est mise en oeuvre via la demande d'API PUT en utilisant cette approche :

Étape 1: Identifiez l'ID de liste Ne pas déchiffrer à partir de la configuration existante.

Étape 2: Référencez l'ID de liste dans la requête API PUT.

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

Cela résout l'erreur « 403 Forbidden » qui se produit lors d'une tentative de configuration du déchiffrement via d'autres méthodes API.

Configuration des catégories de menaces

La configuration de la catégorie de menace est disponible via un point de terminaison API non documenté qui devient accessible après une configuration de déchiffrement réussie. Le point d'extrémité permet un contrôle granulaire des catégories de menaces, mais nécessite que le profil de sécurité soit configuré correctement avec des paramètres de déchiffrement au préalable.

Référence du nom du champ API

Ce tableau mappe les fonctions de profil de sécurité communes à leurs noms de champs d'API correspondants :

Fonctionnalité	Nom du champ API	Description
Déchiffrement TLS	DéfinitionGroupBypassInspectionGroupID	Références Ne pas déchiffrer ID liste
Inspection des fichiers	FileEngines	Contrôle les fonctionnalités d'inspection des fichiers
Blocage de type de fichier	ÉtatContrôleTypeFichier	Active les restrictions de type de fichier

Motif

La limitation était principalement due à une documentation API incomplète et à des conventions de noms de champs non intuitives plutôt qu'à des restrictions fonctionnelles réelles. Les fonctionnalités avancées de configuration des profils de sécurité existent dans l'API, mais sont implémentées à l'aide des éléments suivants :

- Noms de champ non évidents qui diffèrent de la terminologie de l'interface utilisateur graphique
- Un workflow en deux étapes (POST pour la création, PUT pour la configuration avancée)
- Dépendances d'objets de configuration existants (tels que les listes à ne pas déchiffrer)
- Terminaux API non documentés pour certaines fonctionnalités

La documentation de l'API publique n'expose pas clairement ces détails d'implémentation, ce qui conduit à la perception de limitations de l'API lorsque la fonctionnalité est réellement disponible via d'autres approches.

Autres informations utiles

- Documentation de l'API des profils de sécurité Cisco Secure Access
- 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.