Konfigurieren der API für sichere Zugriffsprofile Erweitert

Inhalt

Problem

Bei dem Versuch, Cisco Secure Access-Sicherheitsprofile über die öffentliche API zu konfigurieren, stoßen Benutzer auf Einschränkungen, bei denen nur die Erstellung von Basisprofilen mit Standardeinstellungen möglich ist. Die API bietet keine granularen Konfigurationsoptionen für erweiterte Sicherheitsfunktionen wie:

- TLS-Entschlüsselungseinstellungen
- Durchsetzungskontrollen für Bedrohungskategorien
- Dateityp-Blockierung und -überprüfung
- Einstellungen für Malware-Inspektion

Benutzer berichten von "403 Forbidden"-Fehlern, wenn sie versuchen, die Entschlüsselungseinstellungen über standardmäßige API-Aufrufe zu konfigurieren. Den dokumentierten öffentlichen API-Endpunkten fehlen anscheinend die detaillierten Konfigurationsparameter des Sicherheitsprofils, die über die GUI-Schnittstelle verfügbar sind, was die programmatischen Verwaltungsfunktionen einschränkt.

Umwelt

- Cisco Secure Access-Plattform
- API-Implementierung für Sicherheitsprofile
- Alle betroffenen Softwareversionen
- Öffentliche API-Dokumentationsendpunkte

Auflösung

Die erweiterten Konfigurationseinstellungen des Sicherheitsprofils sind über die Cisco Secure Access-API verfügbar, erfordern jedoch spezifische Implementierungsansätze und Feldbezeichnungskonventionen, die sich von den dokumentierten öffentlichen API-Beispielen unterscheiden. Diese Auflösungsschritte gelten für jeden Konfigurationsbereich:

Workflow zum Erstellen eines grundlegenden Sicherheitsprofils

Der richtige Workflow zum Erstellen von Sicherheitsprofilen mit erweiterten Einstellungen erfolgt in zwei Schritten:

Schritt 1: Erstellen Sie das grundlegende Sicherheitsprofil mithilfe des POST-Tests.

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

Phase 2: Konfigurieren Sie erweiterte Optionen mithilfe von PUT mit der Profil-ID.

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

Dateiprüfung und Konfiguration für die Blockierung von Dateitypen

Die Dateiprüfung und die Blockierung von Dateitypen können mithilfe der folgenden API-Feldnamen in der PUT-Anforderung konfiguriert werden:

- fileEngines - Steuert die Dateiprüfungsfunktionen.
- fileTypeControlStatus - Aktiviert oder deaktiviert die Blockierung von Dateitypen.

Beispielkonfiguration für Dateieinstellungen:

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

TLS-Entschlüsselungskonfiguration

Für die TLS-Entschlüsselungskonfiguration muss auf eine ID der Liste "Nicht entschlüsseln" verwiesen werden, anstatt einen dedizierten POST-Endpunkt zu verwenden. Die Konfiguration wird über die PUT-API-Anforderung nach folgendem Ansatz implementiert:

Schritt 1: Identifizieren Sie die Listen-ID "Nicht entschlüsseln" aus der vorhandenen Konfiguration.

Phase 2: Verweisen Sie auf die Listen-ID in der PUT-API-Anforderung.

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

Dadurch wird der Fehler "403 Forbidden" behoben, der beim Versuch auftritt, die Entschlüsselung über andere API-Methoden zu konfigurieren.

Konfiguration der Bedrohungskategorie

Die Konfiguration der Bedrohungskategorie ist über einen nicht dokumentierten API-Endpunkt verfügbar, auf den nach der erfolgreichen Entschlüsselungskonfiguration zugegriffen werden kann. Das Endgerät ermöglicht eine präzise Kontrolle der Bedrohungskategorie, es muss jedoch zuerst das Sicherheitsprofil korrekt mit den Entschlüsselungseinstellungen konfiguriert werden.

API-Feldnamensreferenz

Diese Tabelle ordnet den entsprechenden API-Feldnamen allgemeine Sicherheitsprofilfunktionen zu:

Funktion	API-Feldname	Beschreibung
TLS-Entschlüsselung	FestlegenGroupBypassInspectionGroupID	Verweise: Liste-ID nicht entschlüsseln
Dateiprüfung	DateiEngines	Kontrollfunktionen für Dateiinspektion
Dateityp-Blockierung	DateiTypSteuerungStatus	Aktiviert Einschränkungen für Dateitypen

Ursache

Die Einschränkung beruhte in erster Linie auf unvollständiger API-Dokumentation und nicht intuitiven Feldnamenskonventionen anstelle tatsächlicher funktionaler Einschränkungen. Die erweiterten Konfigurationsprofile für Sicherheitsprofile sind innerhalb der API verfügbar, werden jedoch mithilfe der folgenden Funktionen implementiert:

- Nicht eindeutige Feldnamen, die sich von der GUI-Terminologie unterscheiden
- Ein zweistufiger Workflow (POST für Erstellung, PUT für erweiterte Konfiguration)
- Abhängigkeiten von vorhandenen Konfigurationsobjekten (z. B. Listen nicht entschlüsseln)
- Nicht dokumentierte API-Endpunkte für bestimmte Funktionen

In der öffentlichen API-Dokumentation werden diese Implementierungsdetails nicht eindeutig beschrieben. Dies führt zu der Wahrnehmung von API-Einschränkungen, wenn die Funktionalität tatsächlich über alternative Ansätze verfügbar ist.

Verwandte Inhalte

- API-Dokumentation für Cisco Secure Access Security-Profile
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.