Configurazione avanzata API profili di sicurezza ad accesso sicuro

Sommario

Problema

Quando si cerca di configurare i profili di sicurezza ad accesso sicuro Cisco tramite l'API pubblica, gli utenti riscontrano limitazioni per le quali è possibile solo la creazione di profili di base con impostazioni predefinite. L'API non espone le opzioni di configurazione granulare per le funzionalità di sicurezza avanzate, tra cui:

- Impostazioni decrittografia TLS
- Controlli applicazione categoria di minaccia
- Blocco e ispezione dei tipi di file
- Impostazioni controllo malware

Gli utenti segnalano di aver ricevuto "403 messaggi di errore non consentiti" durante il tentativo di configurare le impostazioni di decrittografia tramite chiamate API standard. Gli endpoint API pubblici documentati sembrano non disporre dei parametri di configurazione dettagliati del profilo di sicurezza disponibili tramite l'interfaccia GUI, limitando le funzionalità di gestione programmatica.

Ambiente

- Piattaforma Cisco Secure Access
- Implementazione API profili di sicurezza
- Tutte le versioni software interessate
- Endpoint di documentazione API pubblici

Risoluzione

Le funzionalità avanzate di configurazione del profilo di sicurezza sono disponibili tramite l'API di Cisco Secure Access, ma richiedono approcci di implementazione specifici e convenzioni di denominazione dei campi che sono diversi dagli esempi di API pubblica documentati. Le seguenti procedure di risoluzione riguardano ogni area di configurazione:

Flusso di lavoro di creazione del profilo di sicurezza di base

Il flusso di lavoro appropriato per la creazione di profili di sicurezza con impostazioni avanzate è costituito da due passaggi:

Passaggio 1: Creare il profilo di sicurezza di base utilizzando POST.

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

Passaggio 2: Configurare le opzioni avanzate utilizzando PUT con l'ID profilo.

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

Ispezione dei file e configurazione del blocco del tipo di file

L'ispezione dei file e il blocco dei tipi di file possono essere configurati utilizzando i seguenti nomi di campo API all'interno della richiesta PUT:

- fileEngine - Controlla le funzionalità di ispezione dei file.
- fileTypeControlStatus: attiva o disattiva il blocco dei tipi di file.

Configurazione di esempio per le impostazioni dei file:

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

Configurazione decrittografia TLS

La configurazione della decrittografia TLS richiede l'utilizzo di un riferimento a un ID elenco da non decrittografare anziché l'utilizzo di un endpoint POST dedicato. La configurazione viene implementata tramite la richiesta API PUT utilizzando questo approccio:

Passaggio 1: Identificare l'ID dell'elenco Da non decrittografare dalla configurazione esistente.

Passaggio 2: Fare riferimento all'ID elenco nella richiesta API PUT.

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

In questo modo viene risolto l'errore "403 Forbidden" che si verifica quando si cerca di configurare la decrittografia tramite altri metodi API.

Configurazione categoria di minaccia

La configurazione delle categorie di minacce è disponibile tramite un endpoint API non documentato che diventa accessibile dopo la corretta decrittografia della configurazione. L'endpoint consente il controllo granulare della categoria di minaccia, ma richiede che il profilo di sicurezza sia configurato correttamente con le impostazioni di decrittografia.

Riferimento nome campo API

In questa tabella vengono mappate le funzionalità comuni dei profili di sicurezza ai nomi dei campi API corrispondenti:

Funzionalità	Nome campo API	Descrizione
Decrittografia TLS	impostazioneGroupBypassInspectionGroupID	ID elenco riferimenti non decrittografati
Ispezione file	fileEngine	Controlla le funzionalità di ispezione dei file
Blocco tipo di file	TipoFileStatoControllo	Abilita le restrizioni per i tipi di file

Causa

La limitazione è dovuta principalmente alla documentazione API incompleta e alle convenzioni di denominazione dei campi non intuitive, piuttosto che alle effettive restrizioni funzionali. Le funzionalità avanzate di configurazione del profilo di sicurezza sono disponibili nell'API, ma vengono implementate mediante:

- Nomi di campo non ovvi che differiscono dalla terminologia dell'interfaccia grafica
- Flusso di lavoro in due passaggi (POST per la creazione, PUT per la configurazione avanzata)
- Dipendenze dagli oggetti di configurazione esistenti, ad esempio gli elenchi Non decrittografare
- Endpoint API non documentati per alcune funzionalità

La documentazione pubblica dell'API non espone chiaramente questi dettagli di implementazione, portando alla percezione di limitazioni dell'API quando la funzionalità è effettivamente disponibile attraverso approcci alternativi.

Contenuto correlato

- Documentazione sull'API dei profili di sicurezza ad accesso sicuro Cisco

- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).