Configurar API de perfiles de seguridad de acceso seguro avanzada

Contenido

Problema

Al intentar configurar los perfiles de seguridad de Cisco Secure Access a través de la API pública, los usuarios se enfrentan a limitaciones en las que solo es posible crear perfiles básicos con la configuración predeterminada. La API no expone opciones de configuración granular para las funciones de seguridad avanzada, entre las que se incluyen:

- configuración de descifrado TLS
- Controles de aplicación de categorías de amenazas
- Bloqueo e inspección de tipos de archivos
- Configuración de inspección de malware

Los usuarios informan de que reciben errores "403 Forbidden" al intentar configurar la configuración de descifrado a través de llamadas API estándar. Los terminales de API públicas documentados parecen carecer de los parámetros de configuración del perfil de seguridad detallados que están disponibles a través de la interfaz GUI, lo que limita las capacidades de gestión programáticas.

Entorno

- Plataforma Cisco Secure Access
- Implementación de API de perfiles de seguridad
- Todas las versiones de software afectadas
- Terminales de documentación de API públicas

Resolución

Las funciones de configuración avanzadas del perfil de seguridad están disponibles a través de la API de Cisco Secure Access, pero requieren enfoques de implementación específicos y convenciones de nomenclatura de campos que difieren de los ejemplos de API públicas documentadas. Estos pasos de resolución se dirigen a cada área de configuración:

Flujo de trabajo básico de creación de perfiles de seguridad

El flujo de trabajo adecuado para crear perfiles de seguridad con configuración avanzada sigue un proceso de dos pasos:

Paso 1: Cree el perfil de seguridad básico mediante POST.

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

Paso 2: Configure las opciones avanzadas mediante PUT con el ID de perfil.

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

Inspección de archivos y configuración de bloqueo de tipo de archivo

La inspección de archivos y el bloqueo de tipos de archivos se pueden configurar utilizando estos nombres de campo de API en la solicitud PUT:

- fileEngines - Controla las capacidades de inspección de archivos.
- fileTypeControlStatus: habilita o deshabilita el bloqueo de tipo de archivo.

Ejemplo de configuración para la configuración del archivo:

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

Configuración de descifrado de TLS

La configuración de descifrado de TLS requiere hacer referencia a un ID de lista de No descifrar en lugar de utilizar un terminal POST dedicado. La configuración se implementa a través de la solicitud de la API PUT mediante este enfoque:

Paso 1: Identifique el ID de la lista No descifrar de la configuración existente.

Paso 2: Haga referencia al ID de lista en la solicitud de API PUT.

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

Esto resuelve el error "403 Forbidden" que ocurre cuando se intenta configurar el descifrado a través de otros métodos de API.

Configuración de categorías de amenazas

La configuración de categorías de amenazas está disponible a través de un extremo de API no documentado al que se puede acceder después de una configuración de descifrado correcta. El terminal permite el control granular de categorías de amenazas, pero requiere que el perfil de seguridad se configure correctamente con los parámetros de descifrado en primer lugar.

Referencia de nombre de campo API

Esta tabla asigna las funciones comunes del perfil de seguridad a sus nombres de campo de API correspondientes:

Función	Nombre de campo de API	Descripción
Descifrado TLS	establecerIdGrupoDeInspecciónDeOmisiónDeGrupo	Las referencias no descifran la ID de lista
Inspección de archivos	fileEngines	Controla las funciones de inspección de archivos
Bloqueo de tipo de archivo	fileTypeControlStatus	Habilita las restricciones de tipo de archivo

Causa

La limitación se debió principalmente a la documentación incompleta de la API y a las convenciones de denominación de campos no intuitivas en lugar de a las restricciones funcionales reales. Las funciones de configuración avanzadas del perfil de seguridad existen en la API, pero se implementan mediante:

- Nombres de campo no obvios que difieren de la terminología GUI
- Un flujo de trabajo de dos pasos (POST para creación, PUT para configuración avanzada)
- Dependencias de los objetos de configuración existentes (como las listas No descifrar)
- Terminales API no documentados para determinadas funciones

La documentación de la API pública no expone claramente estos detalles de implementación, lo que da lugar a la percepción de las limitaciones de la API cuando la funcionalidad está realmente disponible a través de enfoques alternativos.

Contenido relacionado

- Documentación de la API de perfiles de seguridad de Cisco Secure Access
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).