Secure Access Security Profiles API Advanced configureren

Inhoud

uitgifte

Wanneer gebruikers proberen Cisco Secure Access Security Profiles te configureren via de openbare API, ondervinden ze beperkingen waarbij alleen het maken van basisprofielen met standaardinstellingen mogelijk is. De API biedt geen granulaire configuratieopties voor geavanceerde beveiligingsfuncties, waaronder:

- TLS-decoderingsinstellingen
- Besturingselementen voor handhaving van dreigingscategorieën
- Bestandstype blokkeren en inspecteren
- Instellingen voor malware-inspectie

Gebruikers melden dat ze "403 Forbidden"-fouten ontvangen wanneer ze proberen decoderingsinstellingen te configureren via standaard API-oproepen. De gedocumenteerde openbare API-eindpunten lijken de gedetailleerde configuratieparameters van het beveiligingsprofiel te missen die beschikbaar zijn via de GUI-interface, waardoor de mogelijkheden voor programmatisch beheer worden beperkt.

milieu

- Cisco Secure Access-platform
- Implementatie van API voor beveiligingsprofielen
- Alle betrokken softwareversies
- Openbare API-documentatie-eindpunten

resolutie

De geavanceerde configuratiemogelijkheden voor het beveiligingsprofiel zijn beschikbaar via de Cisco Secure Access API, maar vereisen specifieke implementatiebenaderingen en conventies voor veldnamen die verschillen van de gedocumenteerde openbare API-voorbeelden. Deze resolutiestappen hebben betrekking op elk configuratiegebied:

Workflow voor het maken van basisbeveiligingsprofielen

De juiste workflow voor het maken van beveiligingsprofielen met geavanceerde instellingen volgt een proces in twee stappen:

Stap 1: Maak het basisbeveiligingsprofiel met POST.

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

Stap 2: Configureer geavanceerde opties met PUT met de profiel-ID.

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

Configuratie voor bestandsinspectie en blokkering van bestandstype

Bestandsinspectie en blokkering van bestandstypen kunnen worden geconfigureerd met behulp van de volgende API-veldnamen in het PUT-verzoek:

- fileEngines - Beheert mogelijkheden voor bestandsinspectie.
- fileTypeControlStatus - Hiermee wordt het blokkeren van bestandstypen in- of uitgeschakeld.

Voorbeeldconfiguratie voor bestandsinstellingen:

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

TLS-decoderingsconfiguratie

Voor de TLS-decoderingsconfiguratie moet worden verwezen naar een lijst-ID voor niet-decoderen in plaats van een speciaal POST-eindpunt te gebruiken. De configuratie wordt geïmplementeerd via het PUT API-verzoek met behulp van deze aanpak:

Stap 1: Identificeer de Do Not Decrypt lijst-ID van de bestaande configuratie.

Stap 2: Verwijs naar de lijst-ID in het PUT API-verzoek.

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

Hiermee wordt de "403 Forbidden" -fout opgelost die optreedt bij het configureren van decodering via andere API-methoden.

Configuratie dreigingscategorie

De configuratie van de dreigingscategorie is beschikbaar via een niet-gedocumenteerd API-eindpunt dat toegankelijk wordt na een succesvolle decoderingsconfiguratie. Het eindpunt maakt granulaire controle van de bedreigingscategorie mogelijk, maar vereist dat het beveiligingsprofiel eerst correct wordt geconfigureerd met decoderingsinstellingen.

API-veldnaamverwijzing

In deze tabel worden de algemene functies van het beveiligingsprofiel toegewezen aan de corresponderende API-veldnamen:

Feature	API-veldnaam	Beschrijving
TLS-decodering	settingGroupBypassInspectionGroupID	Referenties Niet-ontsleutelen lijst-ID
bestandsinspectie	fileEngines	Controleert de mogelijkheden voor bestandsinspectie
Bestandstype blokkeren	fileTypeControlStatus	Schakelt bestandstypebeperkingen in

Oorzaak

De beperking was voornamelijk te wijten aan onvolledige API-documentatie en niet-intuïtieve conventies voor veldnaamgeving in plaats van feitelijke functionele beperkingen. De geavanceerde configuratiemogelijkheden voor het beveiligingsprofiel bestaan binnen de API, maar worden geïmplementeerd met behulp van:

- Niet voor de hand liggende veldnamen die verschillen van GUI-terminologie
- Een werkstroom in twee stappen (POST voor creatie, PUT voor geavanceerde configuratie)
- Afhankelijkheden van bestaande configuratieobjecten (zoals lijsten niet decoderen)
- Niet-gedocumenteerde API-eindpunten voor bepaalde functies

De openbare API-documentatie legt deze implementatiedetails niet duidelijk bloot, wat leidt tot de perceptie van API-beperkingen wanneer de functionaliteit daadwerkelijk beschikbaar is via alternatieve benaderingen.

Gerelateerde inhoud

- Cisco Secure Access Security Profiles API-documentatie
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.