

Configurer une règle de contrôle d'accès basée sur le temps sur FDM avec l'API Rest

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer et valider une règle de contrôle d'accès basée sur le temps avec l'API Rest dans le FTD géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Gestion des périphériques Firepower (FDM)
- Connaissance de l'interface de programmation REST (Representational State Transfer Application Programming Interface)
- Liste de contrôle d'accès (ACL)

Composants utilisés

Les informations contenues dans ce document sont basées sur la version FTD 7.1.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'API FTD version 6.6.0 et ultérieure prend en charge des règles de contrôle d'accès limitées dans le temps.

À l'aide de l'API FTD, vous pouvez créer des objets d'intervalle de temps qui spécifient des intervalles de temps uniques ou récurrents et appliquer ces objets aux règles de contrôle d'accès. À l'aide de plages horaires, vous pouvez appliquer une règle de contrôle d'accès au trafic à certains moments de la journée ou pendant certaines périodes, afin de fournir une certaine flexibilité à l'utilisation du réseau. Vous ne pouvez pas utiliser FDM afin de créer ou d'appliquer des intervalles de temps, et FDM ne vous indique pas si une plage de temps est appliquée à une règle de contrôle d'accès.

Configurer

Étape 1. Cliquez sur les options avancées (menu Kebab) afin d'ouvrir l'explorateur d'API FDM.

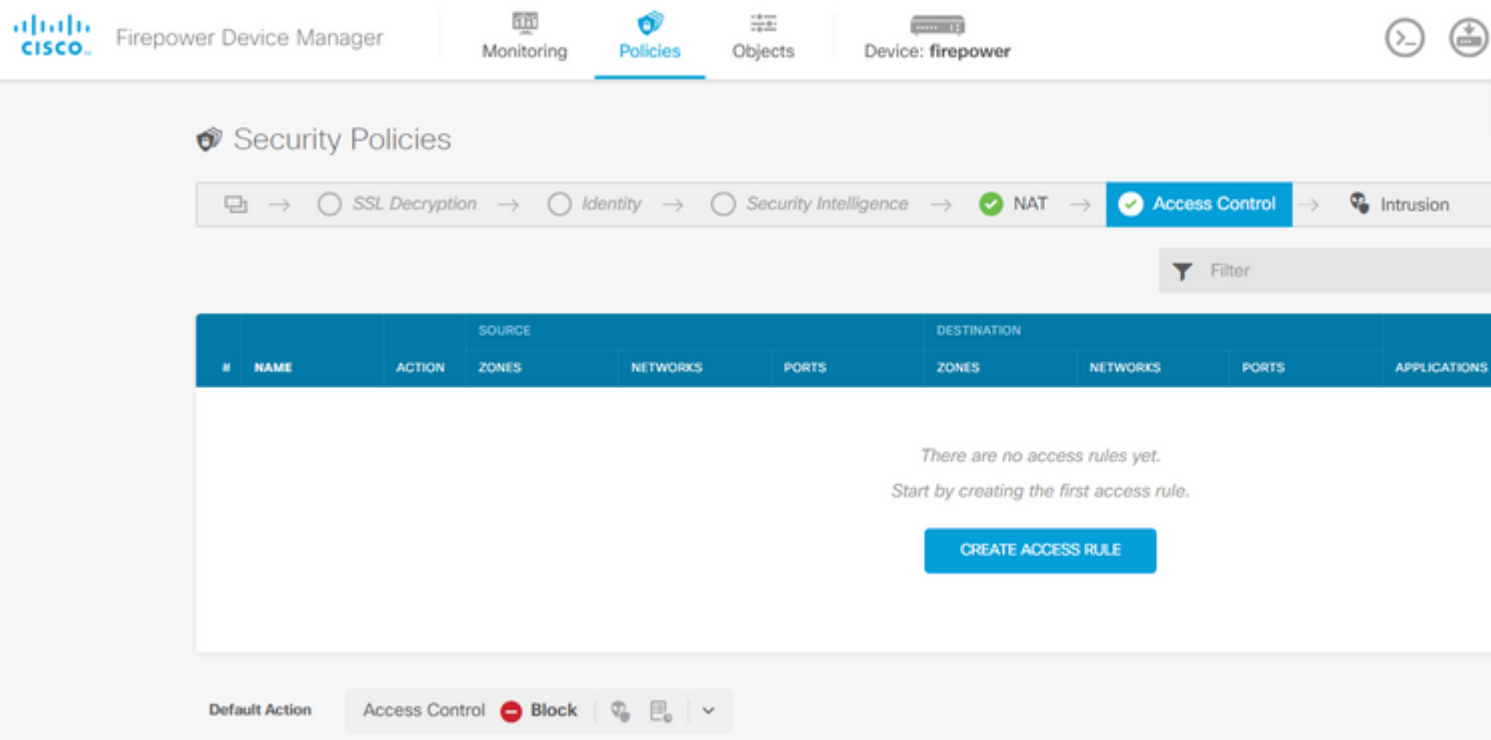


Image 1. Interface utilisateur Web FDM.

Étape 2. Sélectionnez la catégorie **AccessPolicy** afin d'afficher les différents appels API.

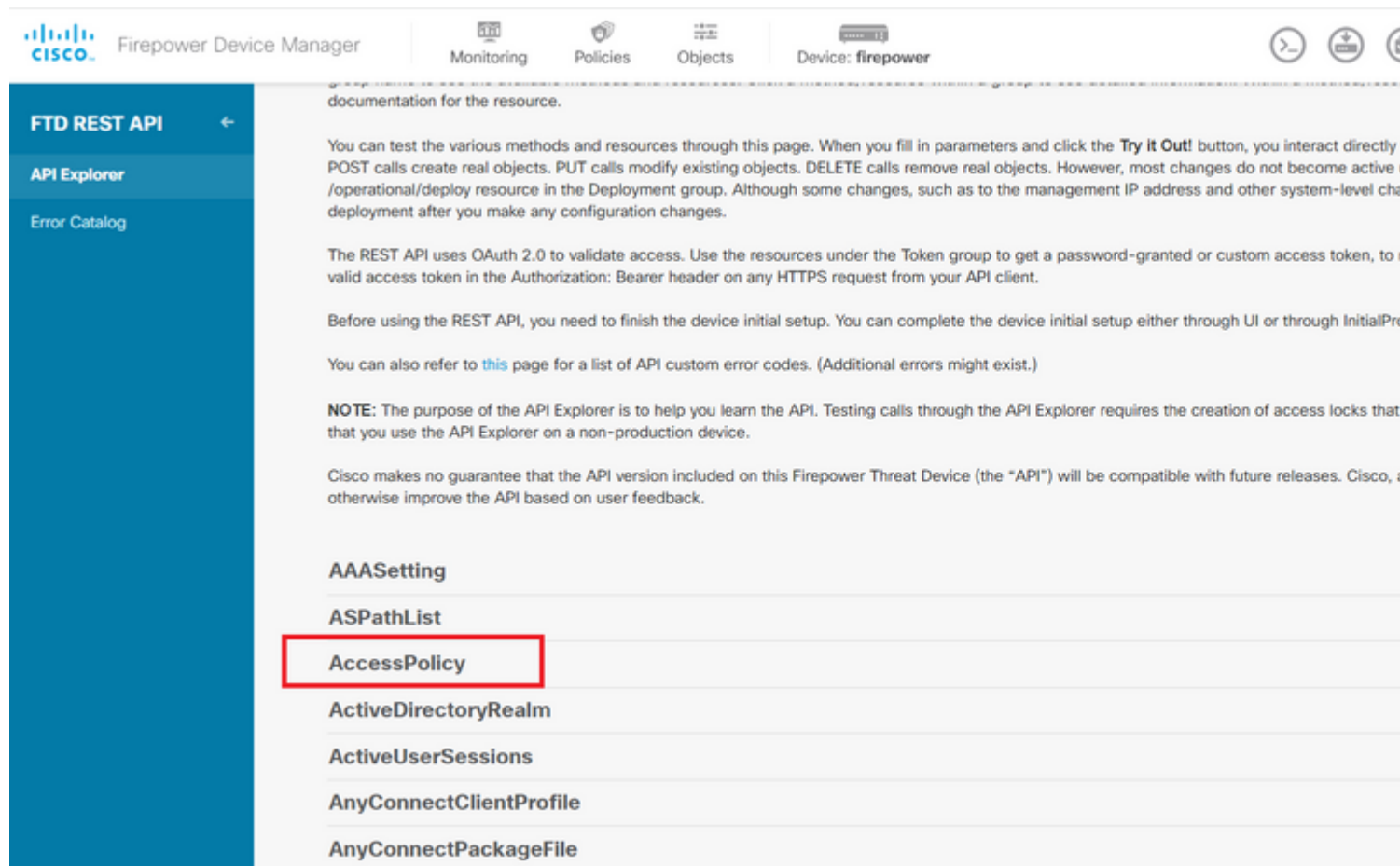


Image 2. Interface utilisateur Web de l'API Explorer.

Étape 3. Exécutez la commande **GET** afin d'obtenir l'ID de la stratégie d'accès.

AccessPolicy

GET /policy/accesspolicies/{parentId}/accessrules

données du corps de réponse vers un bloc-notes. Vous devez ensuite utiliser l'ID de stratégie de contrôle d'accès.

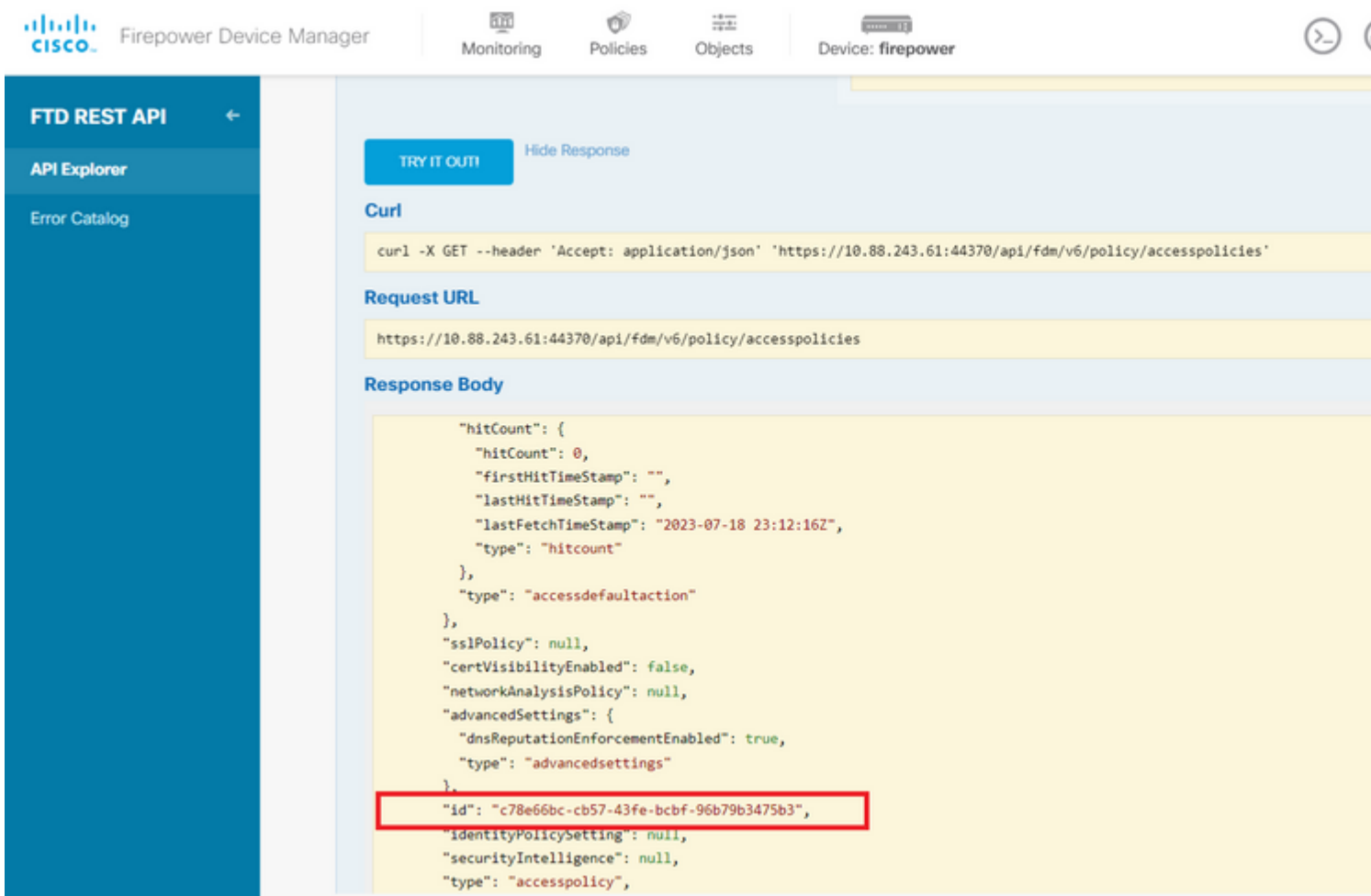


Image 5. Réponse GET de la politique d'accès.

Étape 6. Recherchez et ouvrez la catégorie TimeRange dans l'Explorateur d'API afin d'afficher les différents appels d'API.

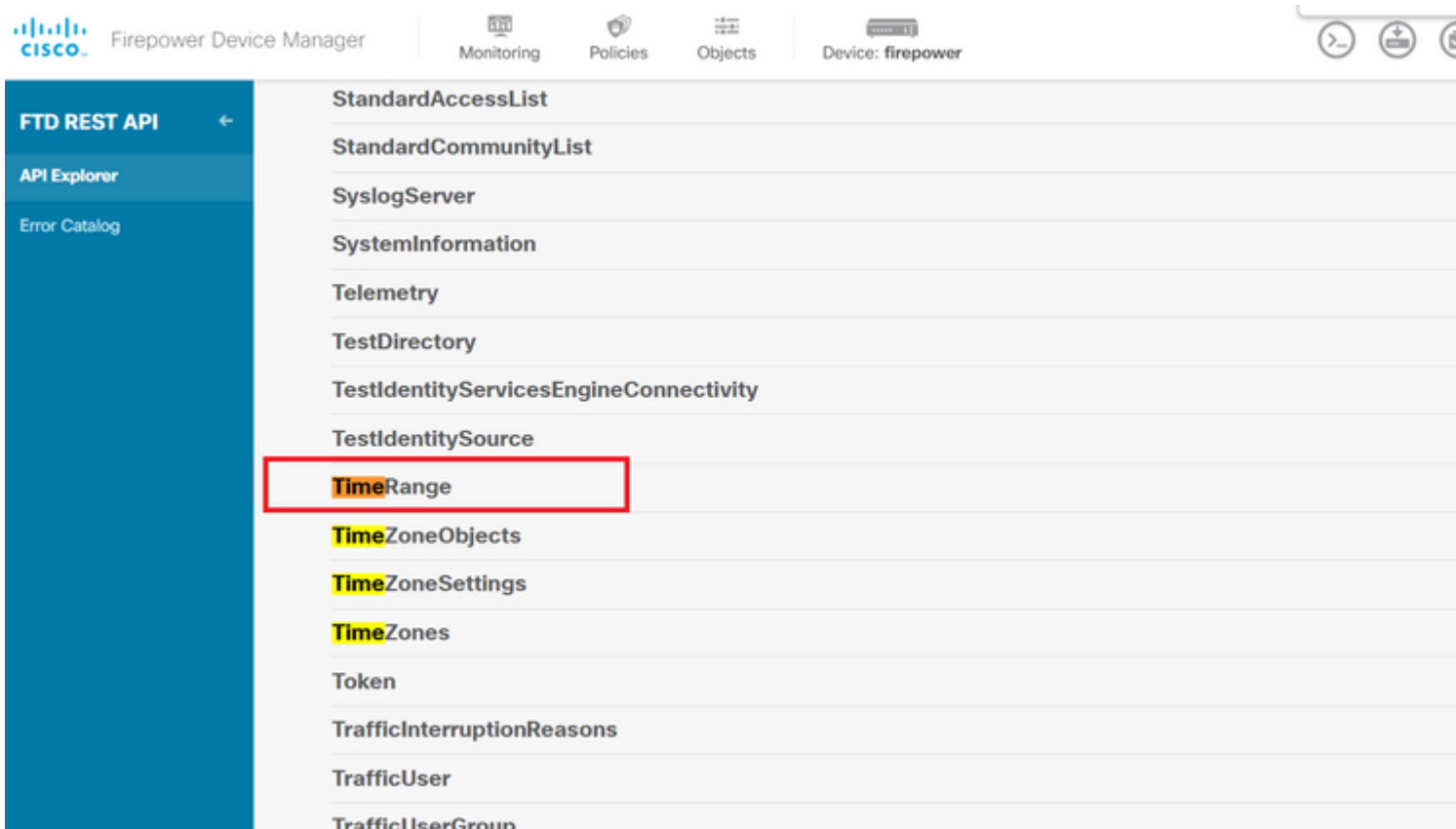


Image 6. Catégorie Intervalle de temps.

exemple de format pour créer la liste de contrôle d'accès basée sur l'heure qui autorise le trafic de la zone Interne vers la zone Externe.

Assurez-vous d'utiliser l'ID d'objet Time Range correct.

```
<#root>
{
  "name": "test_time_range_2",
  "sourceZones": [
    {
      "name": "inside_zone",
      "id": "90c377e0-b3e5-11e5-8db8-651556da7898",
      "type": "securityzone"
    }
  ],
  "destinationZones": [
    {
      "name": "outside_zone",
      "id": "b1af33e1-b3e5-11e5-8db8-afdc0be5453e",
      "type": "securityzone"
    }
  ],
  "ruleAction": "PERMIT",
  "eventLogAction": "
LOG_FLOW_END
",
  "timeRangeObjects": [
    {
      "id": "
718e6b5c-2697-11ee-a5a7-57e37203b186
",
      "type": "timerangeobject",
      "name": "Time-test2"
    }
  ],
  "type": "accessrule"
}
```

Remarque : eventLogAction doit être **LOG_FLOW_END** afin de consigner l'événement à la fin du flux, sinon il donne une erreur.

Étape 12. Déployez les modifications afin d'appliquer la nouvelle liste de contrôle d'accès basée sur le temps. L'invite Modifications en attente doit afficher l'objet de plage de temps utilisé à l'étape 10.

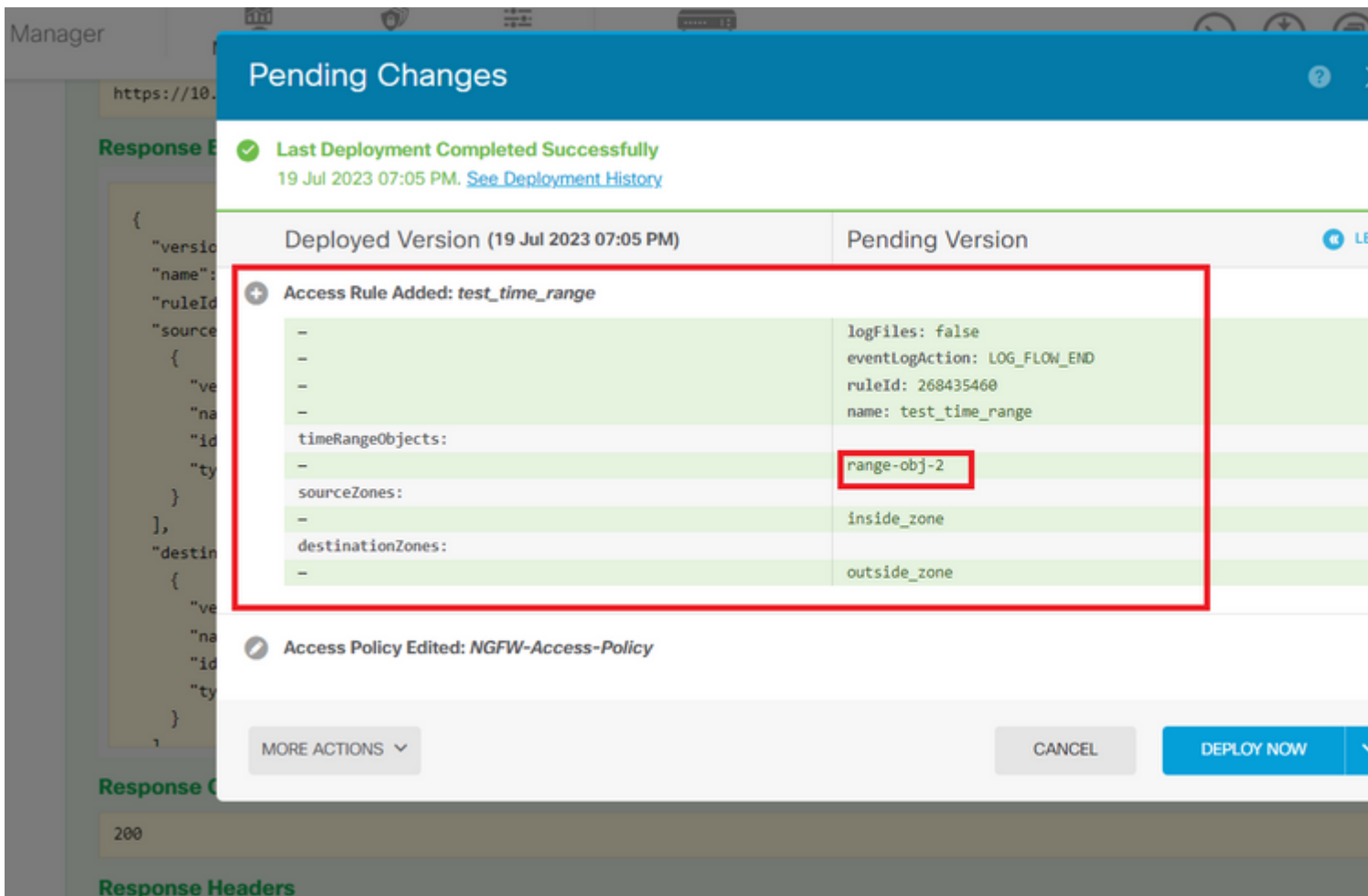


Image 12. La fenêtre Modifications en attente FDM affiche la nouvelle règle.

Étape 13 (facultatif). Si vous souhaitez modifier la liste de contrôle d'accès, vous pouvez utiliser la PUT appelez et modifiez l'ID de plage horaire.

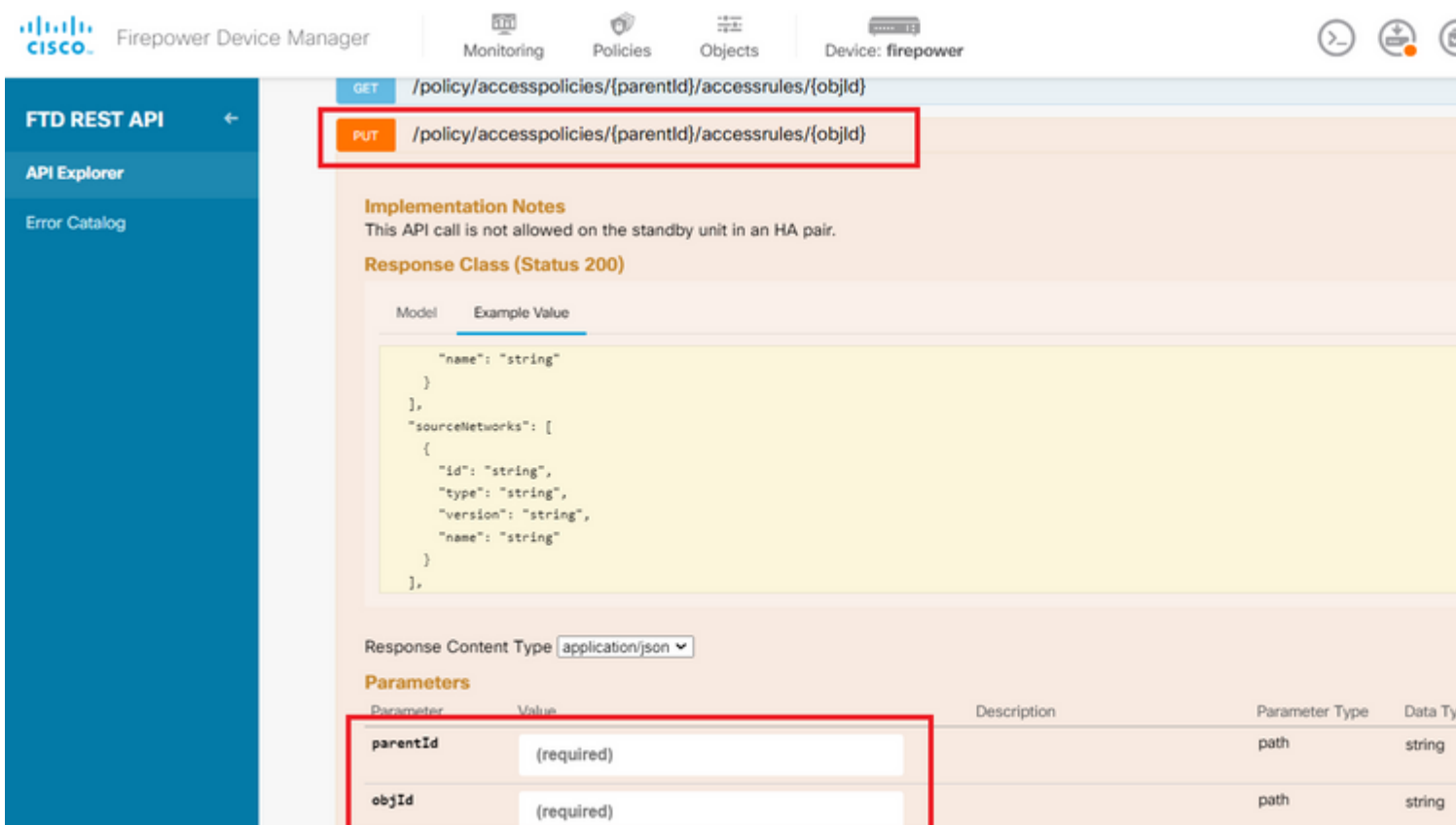


Image 13. Stratégie d'accès Appel PUT.

exemple de format afin de modifier la plage horaire, ces ID de plage horaire peuvent être collectés à l'aide de laGET appel.

```
<#root>

{
  "version": "flya3jw7wvqg7",
  "name": "test_time_range",
  "ruleId": 268435460,
  "sourceZones": [
    {
      "version": "lypkhscmwq4bq",
      "name": "inside_zone",
      "id": "90c377e0-b3e5-11e5-8db8-651556da7898",
      "type": "securityzone"
    }
  ],
  "destinationZones": [
    {
      "version": "pytctz6vvfb3i",
      "name": "outside_zone",
      "id": "b1af33e1-b3e5-11e5-8db8-afdc0be5453e",
      "type": "securityzone"
    }
  ],
  "sourceNetworks": [],
  "destinationNetworks": [],
  "sourcePorts": [],
  "destinationPorts": [],
  "ruleAction": "PERMIT",
  "eventLogAction": "LOG_FLOW_END",
  "identitySources": [],
  "users": [],
  "embeddedAppFilter": null,
  "urlFilter": null,
  "intrusionPolicy": null,
  "filePolicy": null,
  "logFiles": false,
  "syslogServer": null,
  "destinationDynamicObjects": [],
  "sourceDynamicObjects": [],
  "timeRangeObjects": [
    {
      "version": "i3iohbd5iufo1",
      "name": "range-obj-1",
      "id": "
718e6b5c-2697-11ee-a5a7-57e37203b186
",
      "type": "timerangeobject"
    }
  ],
  "id": "0f2e8f56-269b-11ee-a5a7-6f90451d6efd",
  "type": "accessrule"
}
```

Étape 14. Déployez et validez vos modifications.

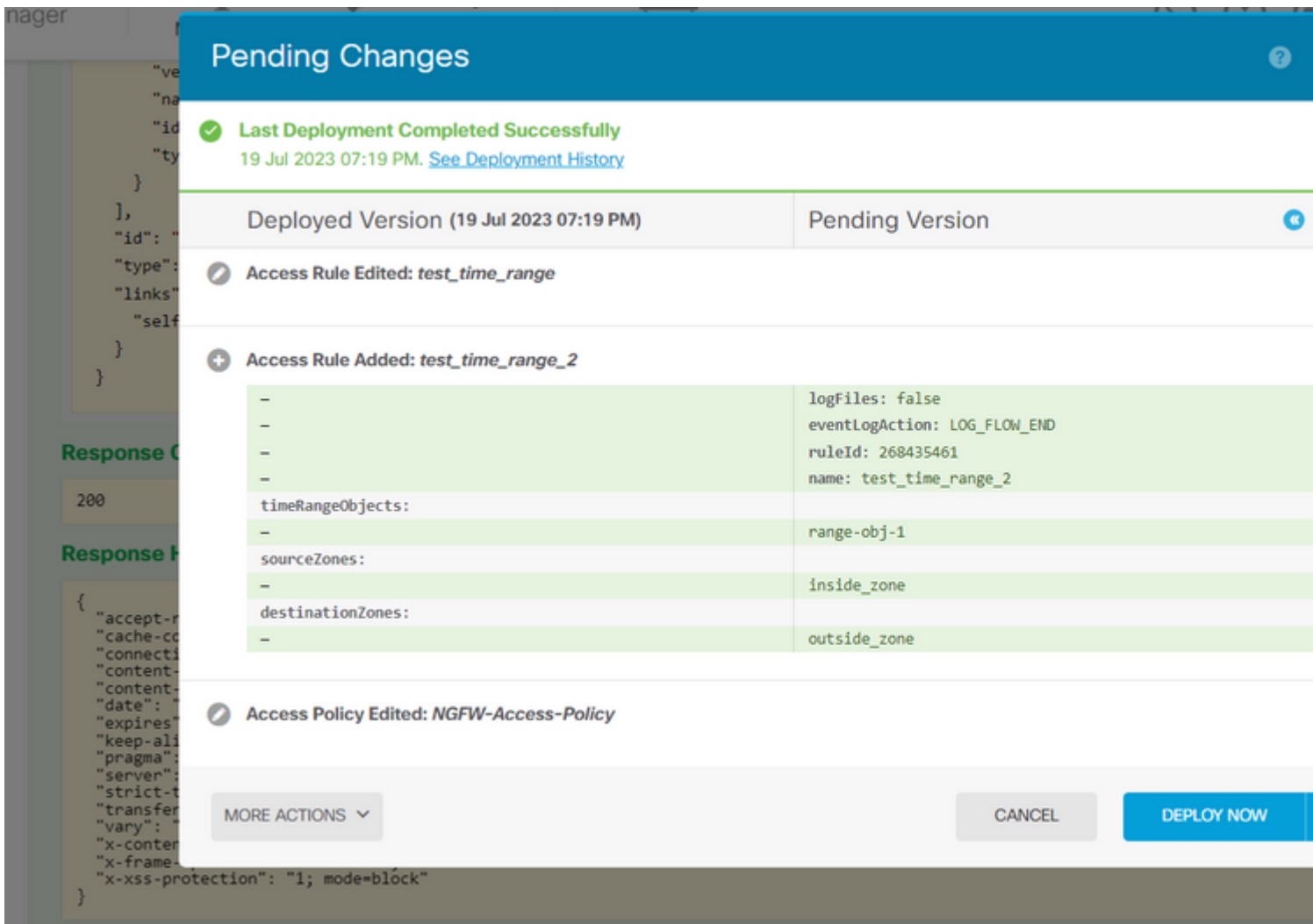


Image 14. La fenêtre Modifications en attente FDM affiche la modification de l'objet.

Vérifier

1. Exécutez la commande `show time-range` afin de valider l'état de vos objets d'intervalle de temps.

```
<#root>
```

```
>
```

```
show time-range
```

```
time-range entry:
```

```
range-obj-1
```

```
(
active
```

```
)
periodic weekdays 0:00 to 23:50
```

```
time-range entry:
```

```
range-obj-2
```

```
(
inactive
)[]
```

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.