Konfigurieren einer zeitbasierten Zugriffskontrollregel für FDM mit REST-API

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie eine zeitbasierte Zugriffskontrollregel mit der REST-API in dem von FDM verwalteten FTD konfiguriert und validiert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Firepower Threat Defense (FTD)
- FirePOWER-Gerätemanagement (FDM)
- Kenntnisse der REST-API (Representational State Transfer Application Programming Interface)
- Zugriffskontrollliste (ACL)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf FTD-Version 7.1.0.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

FTD API Version 6.6.0 und höher unterstützt Zugriffskontrollregeln, die zeitlich begrenzt sind.

Mithilfe der FTD-API können Sie Zeitbereichsobjekte erstellen, die einmalige oder wiederkehrende Zeitbereiche angeben, und diese Objekte auf Zugriffskontrollregeln anwenden. Mithilfe von Zeiträumen können Sie eine Zugriffskontrollregel auf Datenverkehr anwenden, der zu bestimmten Tageszeiten oder für bestimmte Zeiträume generiert wird, um die Netzwerknutzung flexibel zu gestalten. Sie können FDM nicht zum Erstellen oder Anwenden von Zeitbereichen verwenden. FDM zeigt Ihnen auch nicht an, ob auf eine Zugriffskontrollregel ein Zeitbereich angewendet wurde.

Konfigurieren

Schritt 1: Klicken Sie auf die erweiterten Optionen (Kebab-Menü), um den FDM API Explorer zu öffnen.

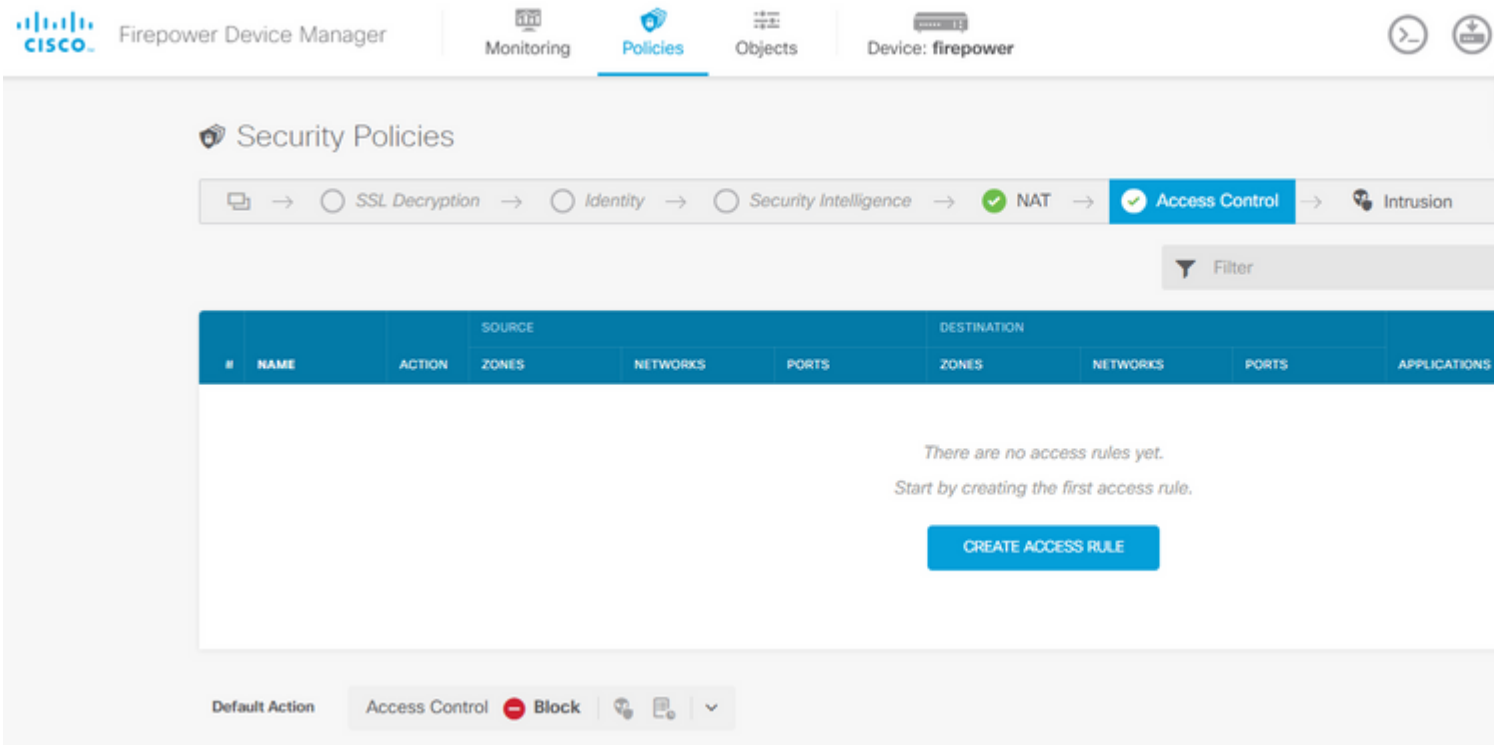


Bild 1. FDM-Web-Benutzeroberfläche.

Schritt 2: Wählen Sie die Kategorie **AccessPolicy** um die verschiedenen API-Aufrufe anzuzeigen.

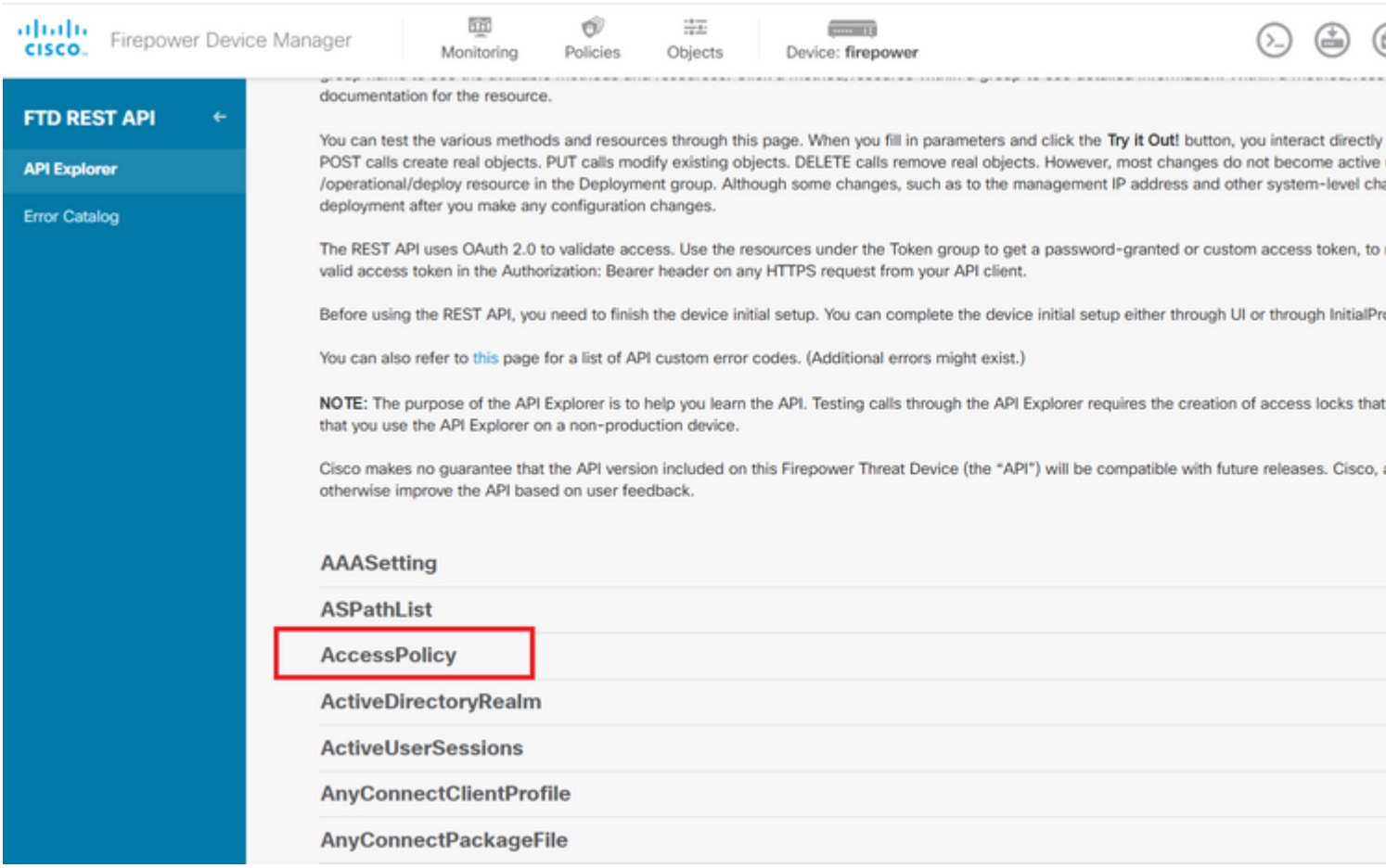
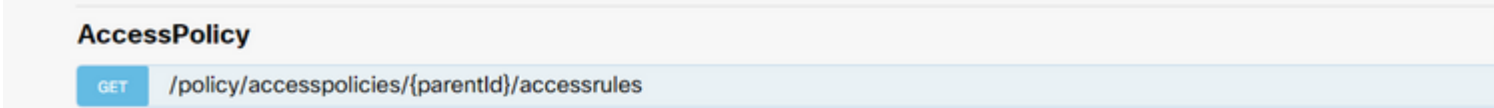


Bild 2. API-Explorer-Webbenutzeroberfläche.

Schritt 3: Führen Sie **GET** um die Zugriffsrichtlinien-ID zu erhalten.



Daten vom Antworttext an ein Notizblock. Später müssen Sie die Richtlinien-ID für die Zugriffskontrolle verwenden.

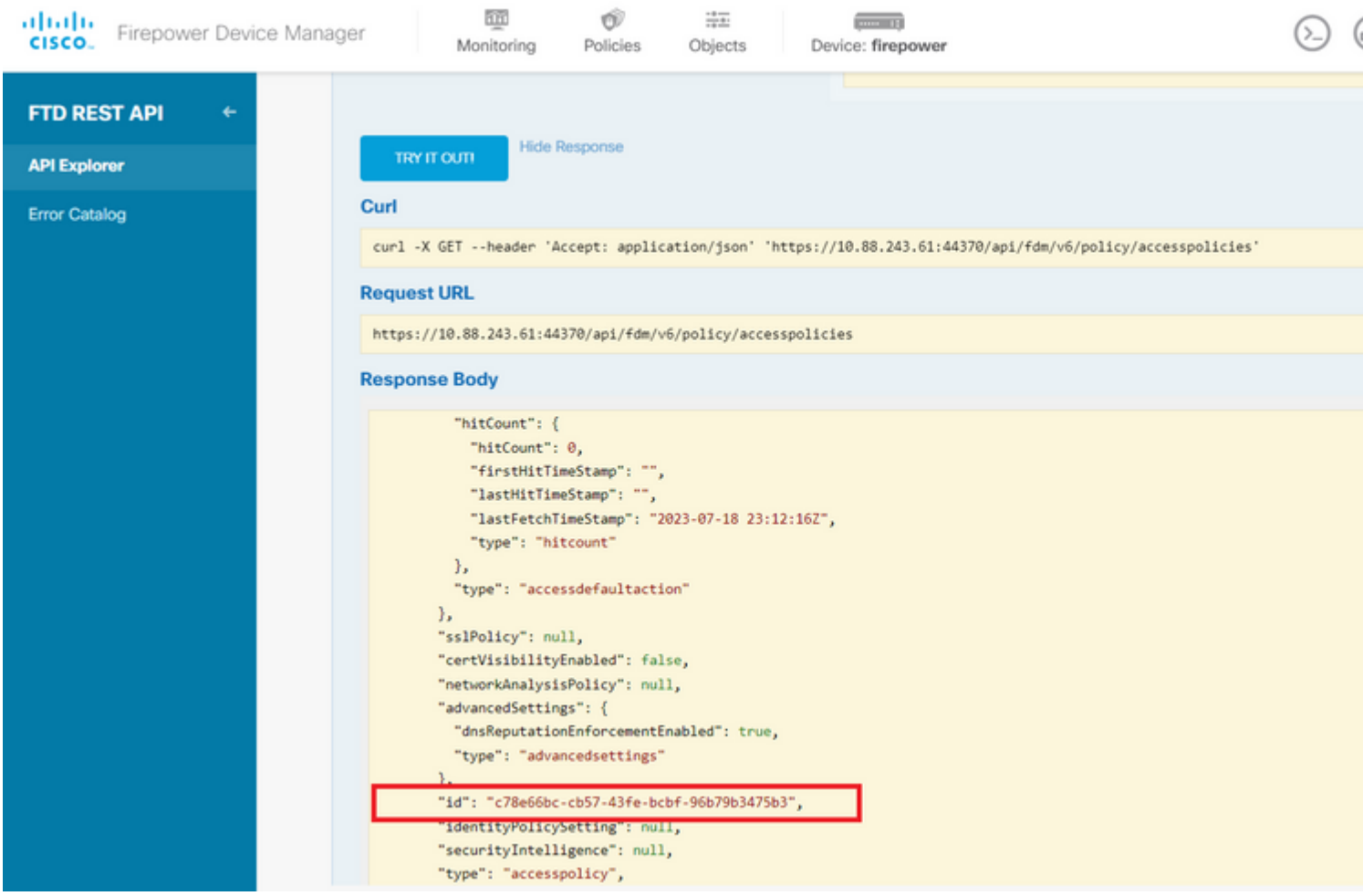


Bild 5. GET-Antwort von der Zugriffsrichtlinie.

Schritt 6: Suchen und öffnen Sie die Kategorie TimeRange im API-Explorer, um die verschiedenen API-Aufrufe anzuzeigen.

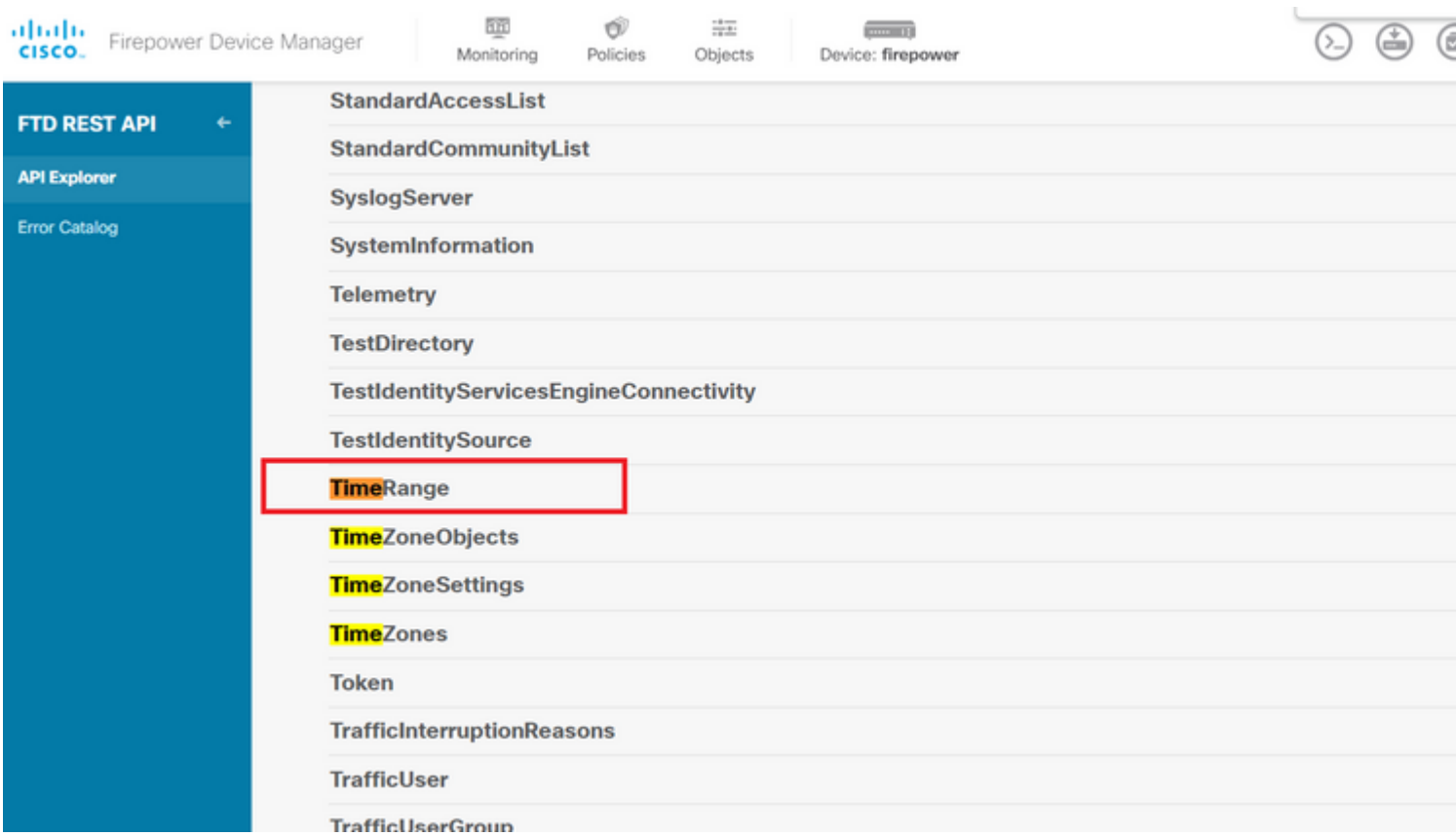


Bild 6. Kategorie "Zeitbereich".

-Formatbeispiel verwenden, um die zeitbasierte ACL zu erstellen, die den Datenverkehr von der Innen- zur Outside-Zone zulässt.

Stellen Sie sicher, dass Sie die richtige Objektkennung für den Zeitbereich verwenden.

<#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"
}
```

> **Anmerkung:** eventLogAction muss **LOG_FlOW_END** um das Ereignis am Ende des Flusses zu protokollieren, andernfalls wird ein Fehler ausgegeben.

Schritt 12: Stellen Sie die Änderungen bereit, um die neue zeitbasierte Zugriffskontrollliste anzuwenden. An der Eingabeaufforderung Pending Changes (Ausstehende Änderungen) muss das in Schritt 10 verwendete Zeitbereichsobjekt angezeigt werden.

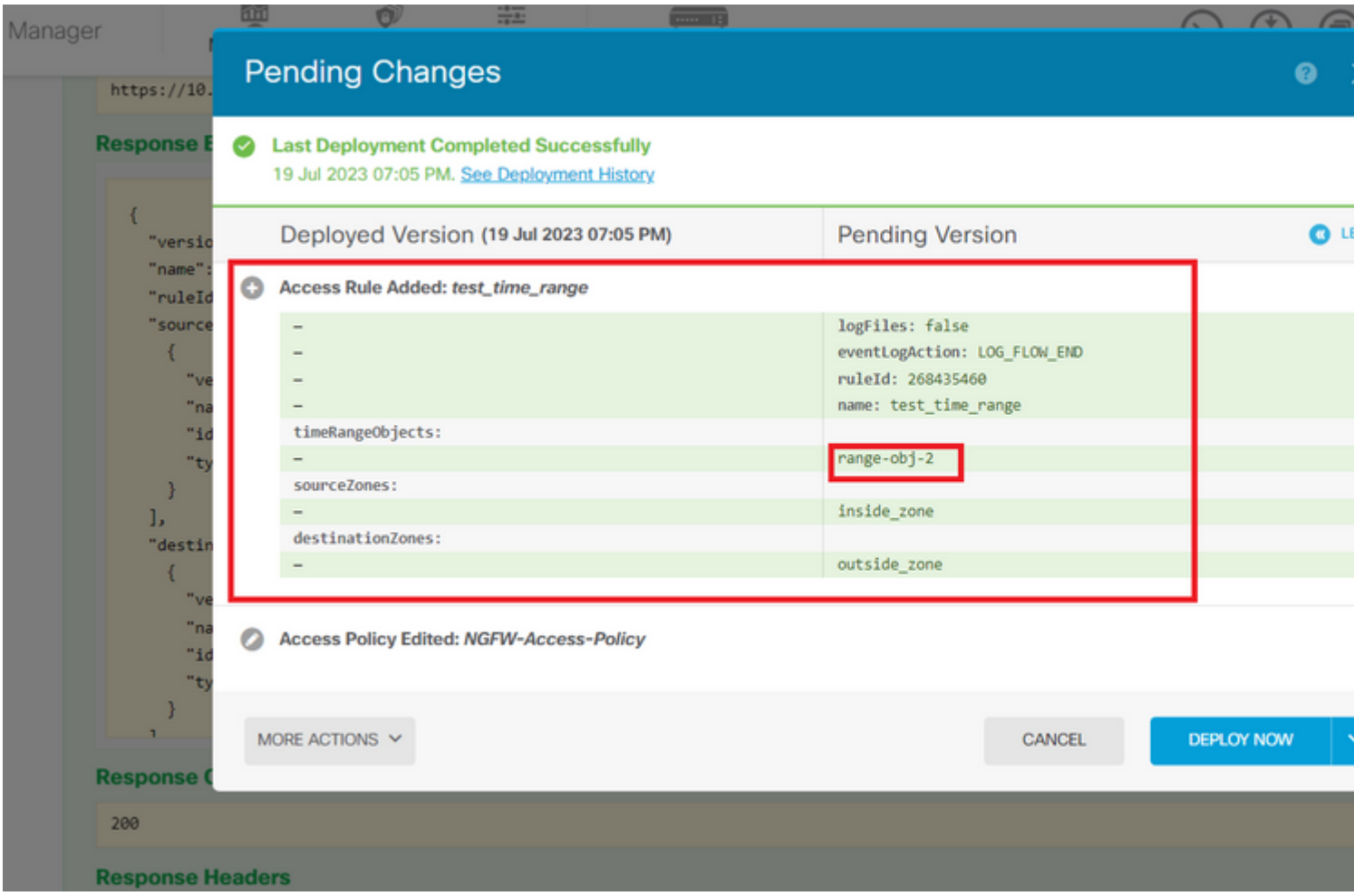


Bild 12. Im Fenster "FDM - ausstehende Änderungen" wird die neue Regel angezeigt.

Schritt 13 (optional). Wenn Sie die ACL bearbeiten möchten, können Sie die PUT die ID des Zeitbereichs aufrufen und bearbeiten.

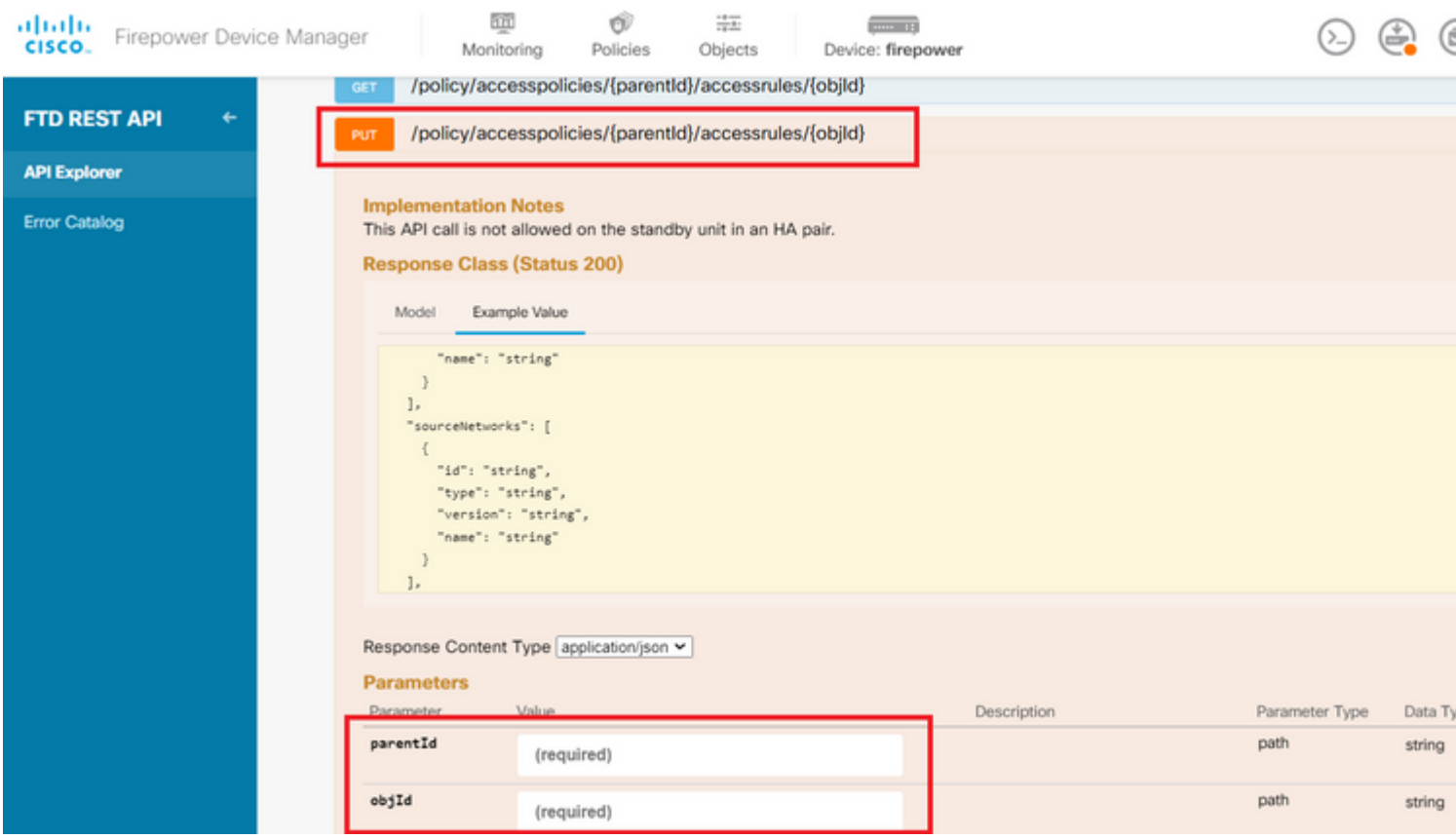


Bild 13. Zugriffsrichtlinien-PUT-Anruf.

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.