Configuración de una regla de control de acceso basado en tiempo en FDM con API de resto

Contenido

Introducción

Este documento describe cómo configurar y validar una regla de control de acceso basado en tiempo con API Rest en el FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense (FTD)
- Administración de dispositivos Firepower (FDM)
- Conocimiento de la interfaz de programación de aplicaciones de transferencia de estado representacional (API REST)
- Lista de control de acceso (ACL)

Componentes Utilizados

La información de este documento se basa en la versión 7.1.0 del FTD.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La versión 6.6.0 y posteriores de la API de FTD admiten reglas de control de acceso que están limitadas en función del tiempo.

Mediante la API de FTD, puede crear objetos de rango de tiempo, que especifican rangos de tiempo únicos o recurrentes, y aplicar estos objetos a las reglas de control de acceso. Mediante el uso de intervalos de tiempo, puede aplicar una regla de control de acceso al tráfico durante determinadas horas del día o durante determinados períodos de tiempo, con el fin de proporcionar flexibilidad al uso de la red. No puede utilizar FDM para crear o aplicar rangos de tiempo, ni FDM muestra si una regla de control de acceso tiene un rango

de tiempo aplicado.

Configurar

Paso 1. Haga clic en las opciones avanzadas (menú Kebab) para abrir el explorador de la API de FDM.

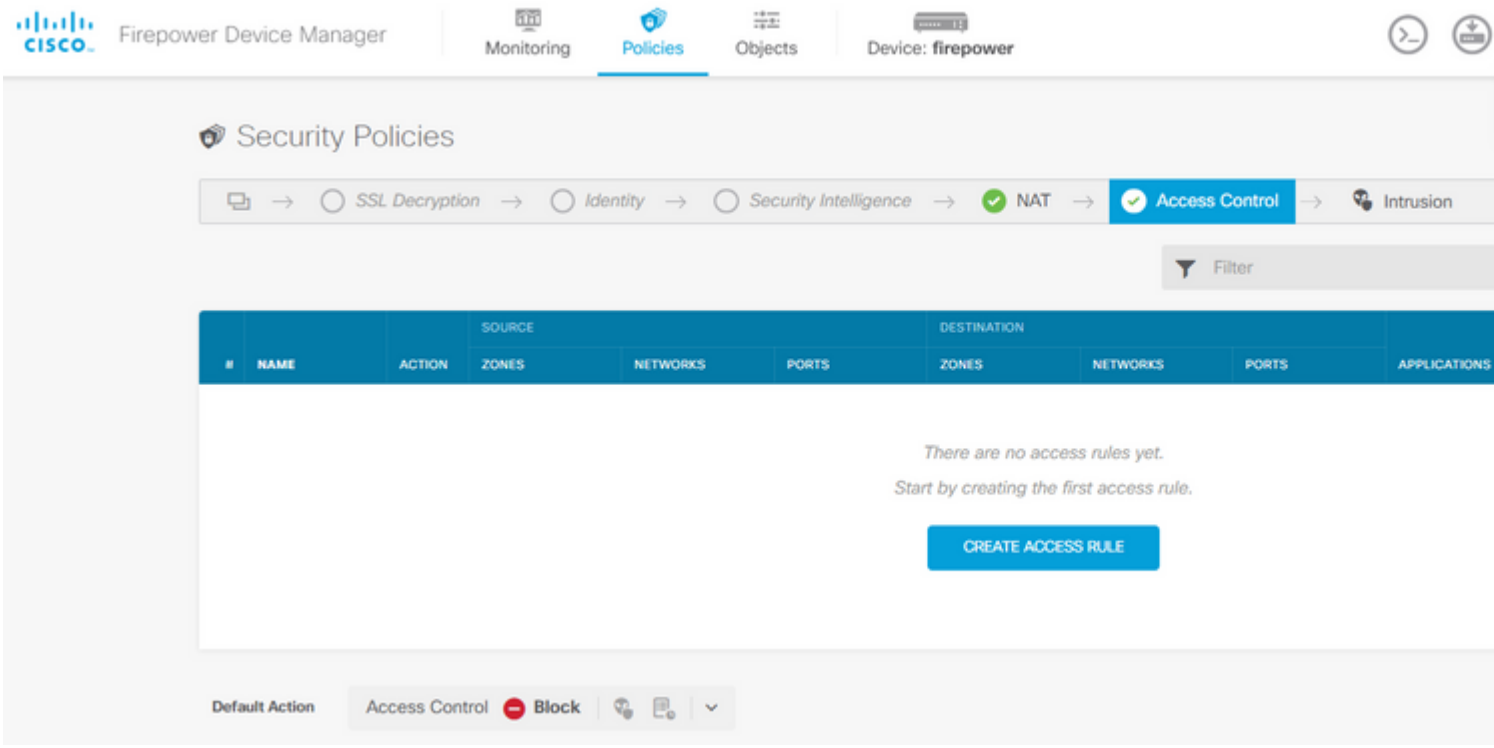


Imagen 1. Interfaz de usuario web de FDM.

Paso 2. Elija la categoría **AccessPolicy** para mostrar las diferentes llamadas de API.

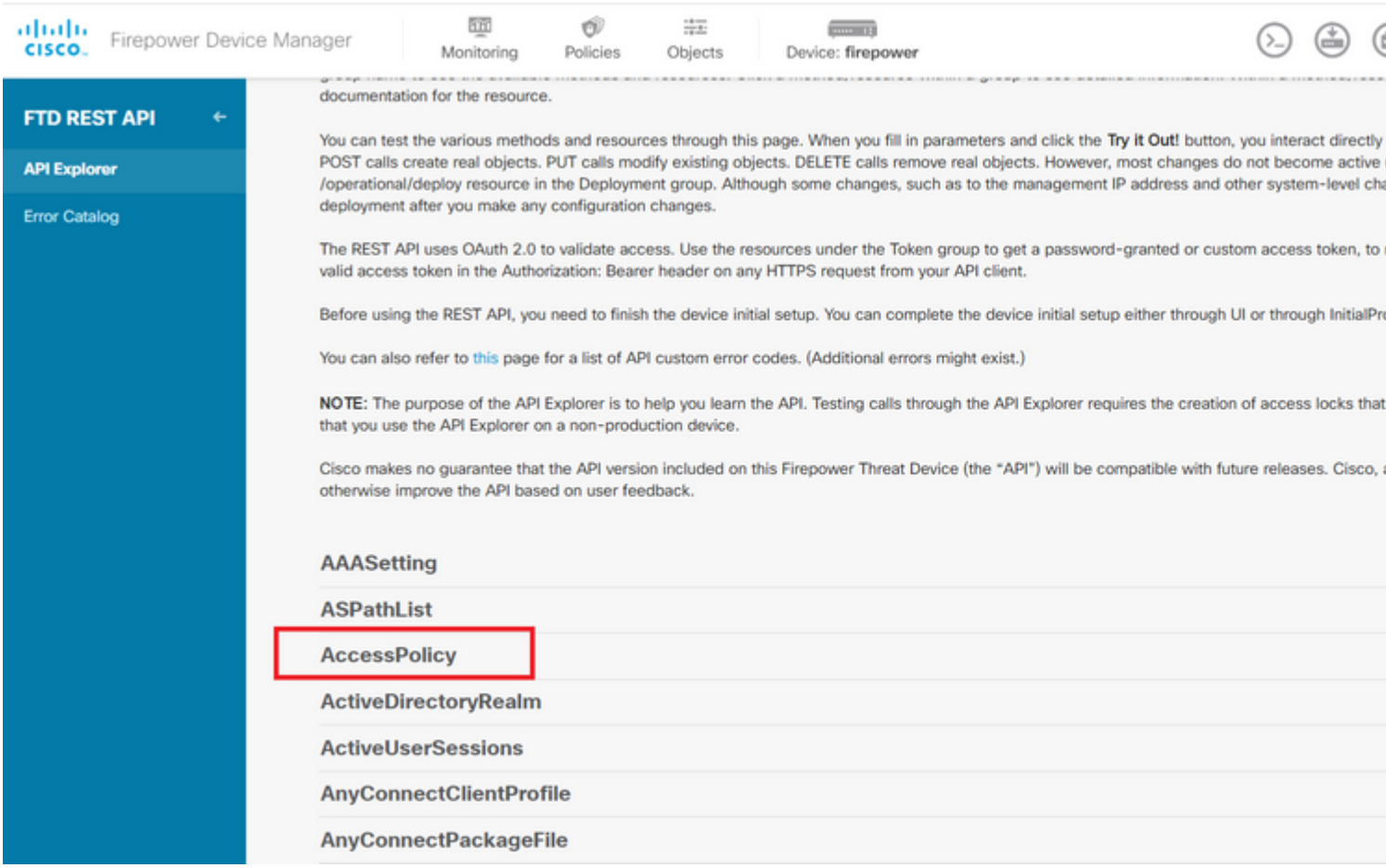
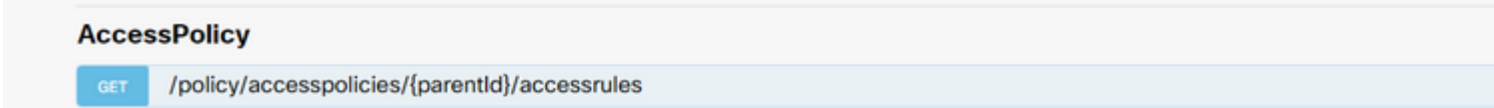


Imagen 2. Interfaz de usuario web del Explorador de API.

Paso 3. Ejecute el **GET** para obtener el ID de política de acceso.



datos del cuerpo de la respuesta a un bloc de notas. Posteriormente, debe utilizar el ID de política de control de acceso.

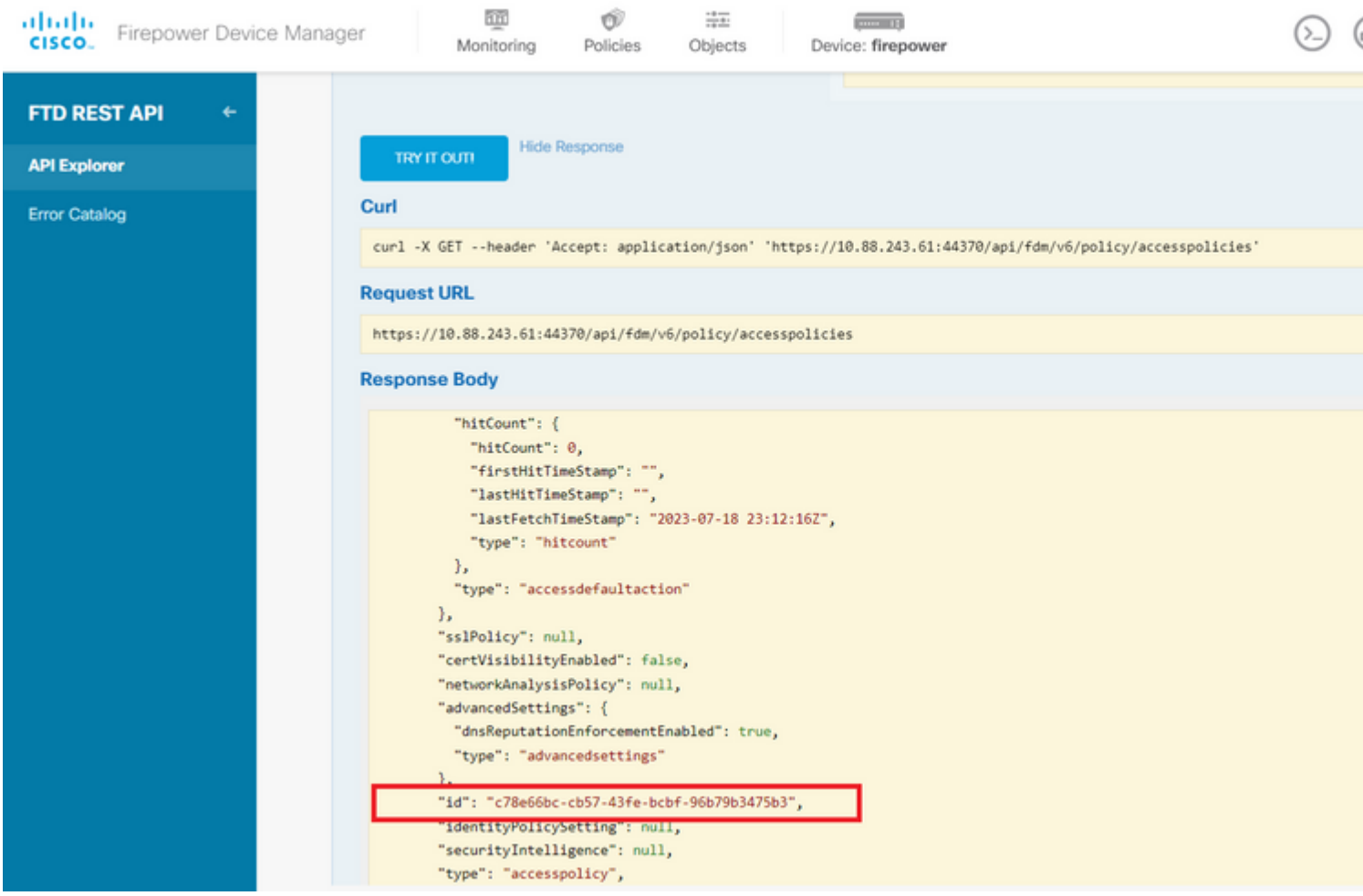


Imagen 5. Respuesta GET de política de acceso.

Paso 6. Busque y abra la categoría TimeRange en el Explorador de API para mostrar las diferentes llamadas de API.

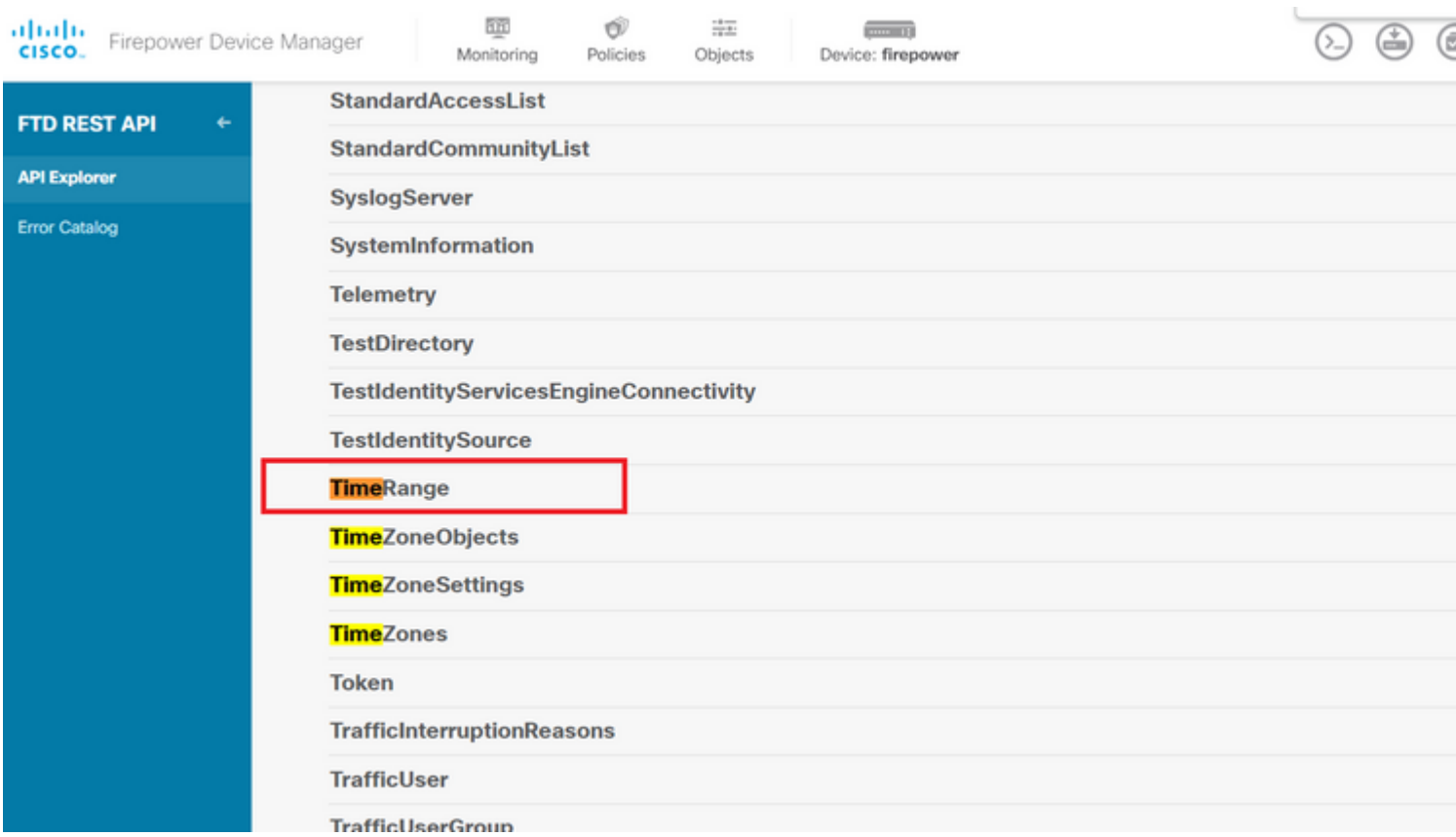


Imagen 6. Categoría Intervalo de tiempo.

ejemplo de formato para crear la ACL basada en tiempo que permite el tráfico desde la zona interna a la zona externa.

Asegúrese de utilizar el ID de objeto de intervalo de tiempo correcto.

<#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"
}
```

> **Nota:** eventLogAction debe ser **LOG_FlOW_END** para registrar el evento al final del flujo; de lo contrario, genera un error.

Paso 12. Implemente los cambios para aplicar la nueva ACL basada en tiempo. El mensaje Cambios pendientes debe mostrar el objeto de intervalo de tiempo utilizado en el paso 10.

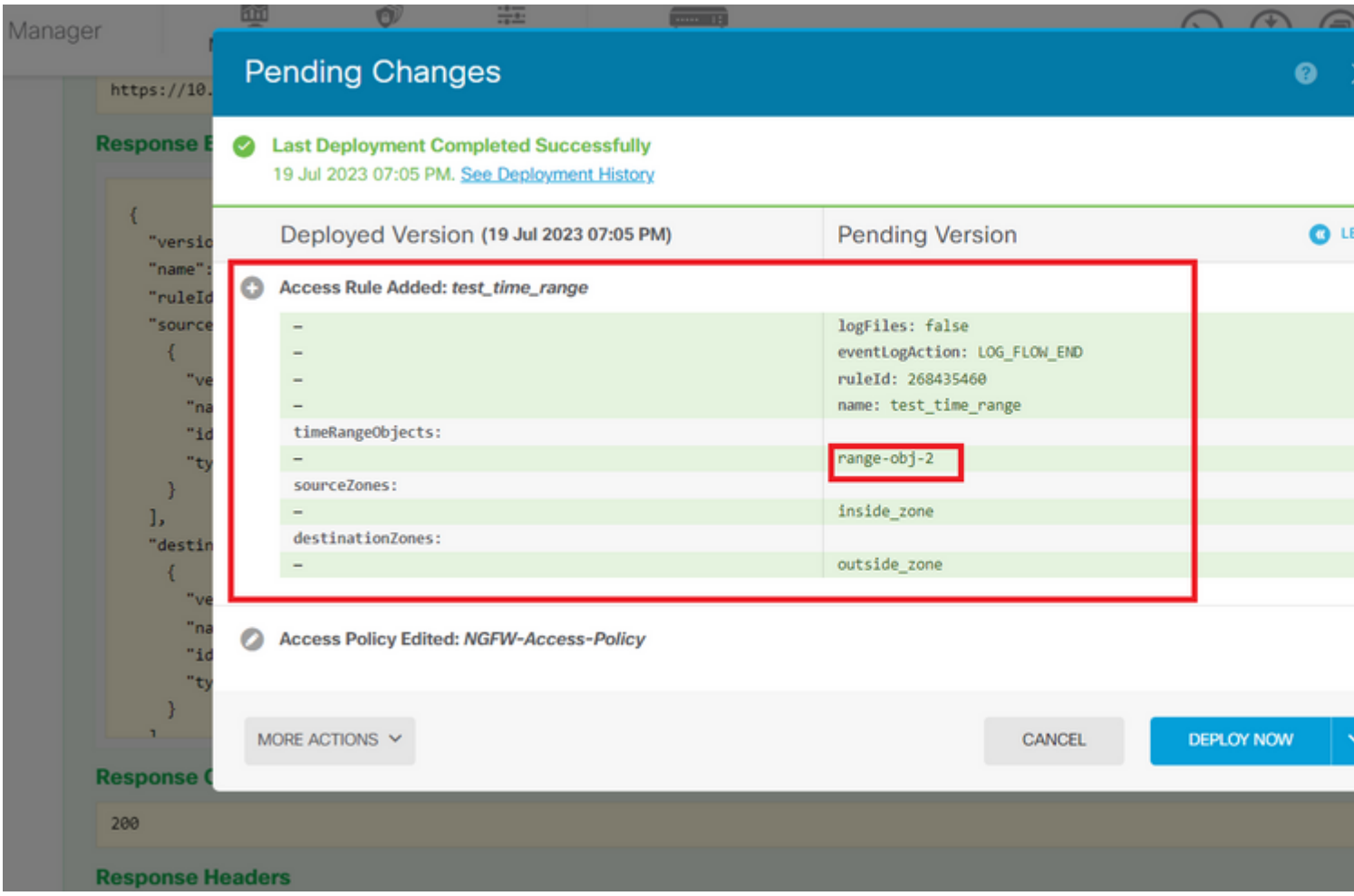


Imagen 12. La ventana Cambios pendientes de FDM muestra la nueva regla.

Paso 13 (opcional). Si desea editar la ACL, puede utilizar el PUT llame y edite el identificador del rango de tiempo.

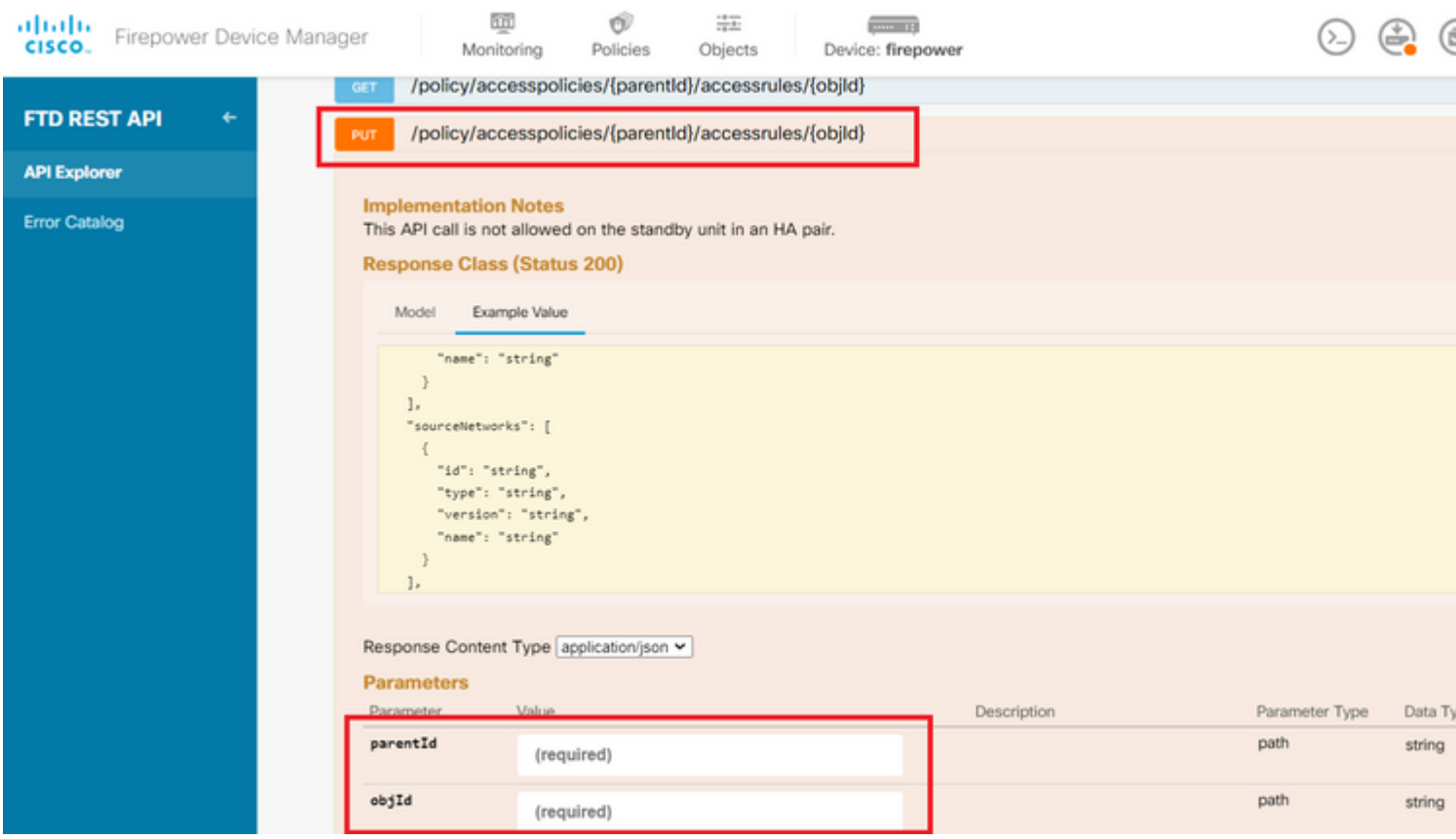


Imagen 13. Política de acceso llamada PUT.

ejemplo de formato para editar el rango de tiempo, estos ID de rango de tiempo se pueden recopilar mediante el uso de la**GET** llamada.

<#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": "i3iohbd5iufol",
"name": "range-obj-1",
"id": "
```


718e6b5c-2697-11ee-a5a7-57e37203b186


```
",
"type": "timerangeobject"
}
],
"id": "0f2e8f56-269b-11ee-a5a7-6f90451d6efd",
"type": "accessrule"
}
```


Paso 14. Implemente y valide los cambios.

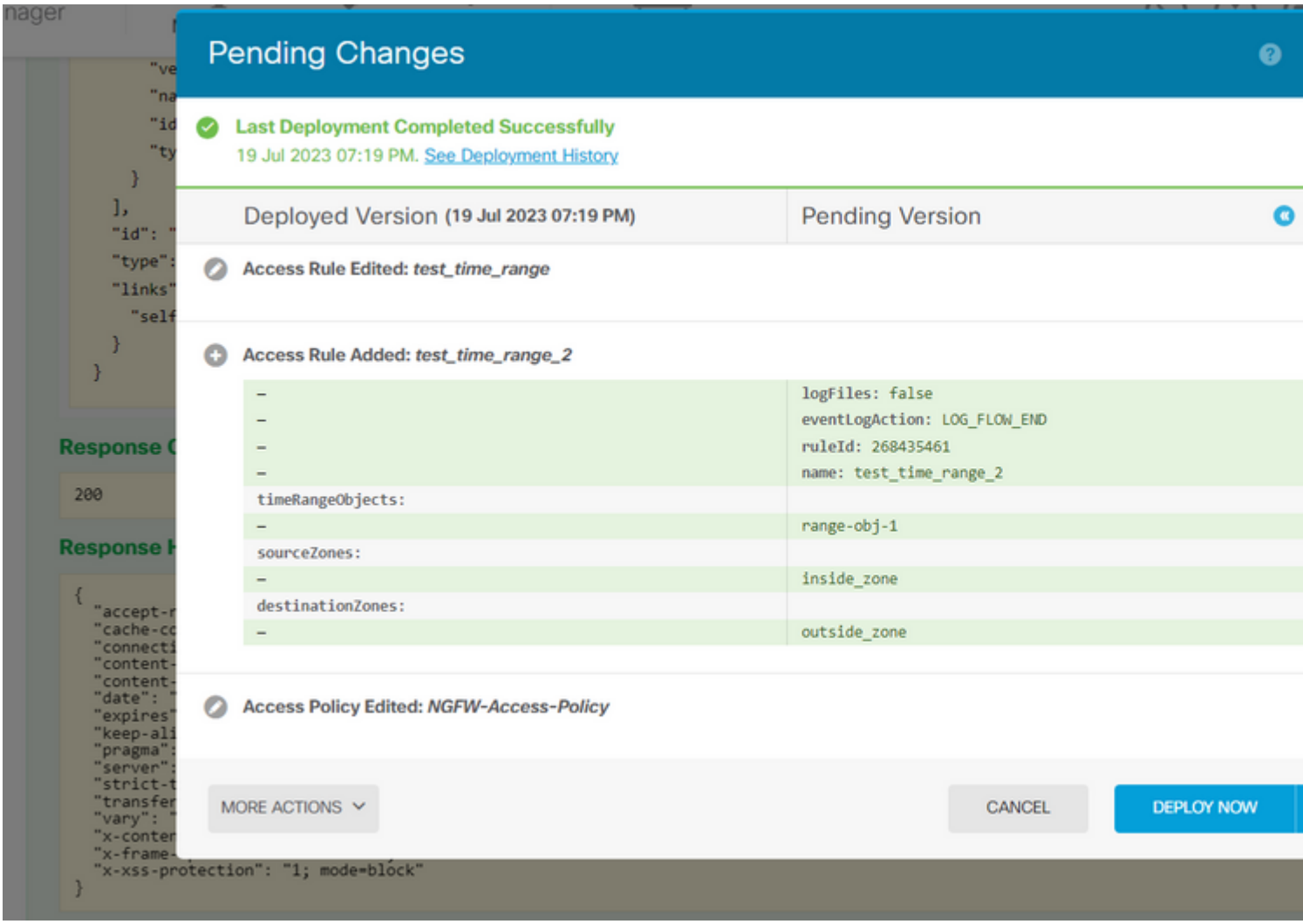


Imagen 14. La ventana Cambios pendientes de FDM muestra el cambio del objeto.

Verificación

1. Ejecute el show time-range para validar el estado de sus objetos de rango de tiempo.

```
<#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
)
```

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).