在使用Rest API的FDM上配置基于时间的访问控制规则

目录

简介

本文档介绍如何在FDM使用Rest API管理的FTD上配置和验证基于时间的访问控制规则。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全防火墙威胁防御(FTD)
- Firepower设备管理(FDM)
- 具象状态传输应用编程接口(REST API)知识
- 访问控制列表(ACL)

使用的组件

本文档中的信息基于FTD 7.1.0版。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

FTD API版本6.6.0及更高版本支持基于时间限制的访问控制规则。

使用FTD API，您可以创建时间范围对象，指定一次性或循环时间范围，并将这些对象应用于访问控制规则。使用时间范围，您可以将访问控制规则应用于一天中的特定时间或特定时间段的流量，以便灵活使用网络。不能使用FDM创建或应用时间范围，如果访问控制规则应用了时间范围，FDM也不会显示您。

配置

步骤1:单击高级选项（“kebab”菜单）以打开FDM API资源管理器。

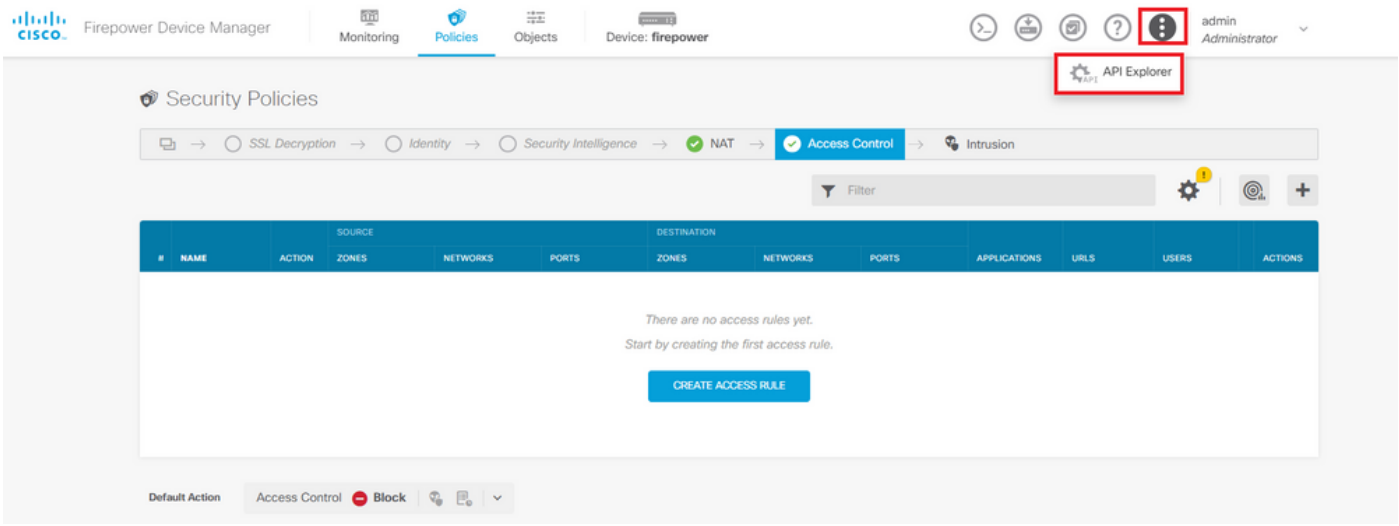

图 1.FDM Web用户界面。

第二步：选择类别AccessPolicy以显示不同的API调用。

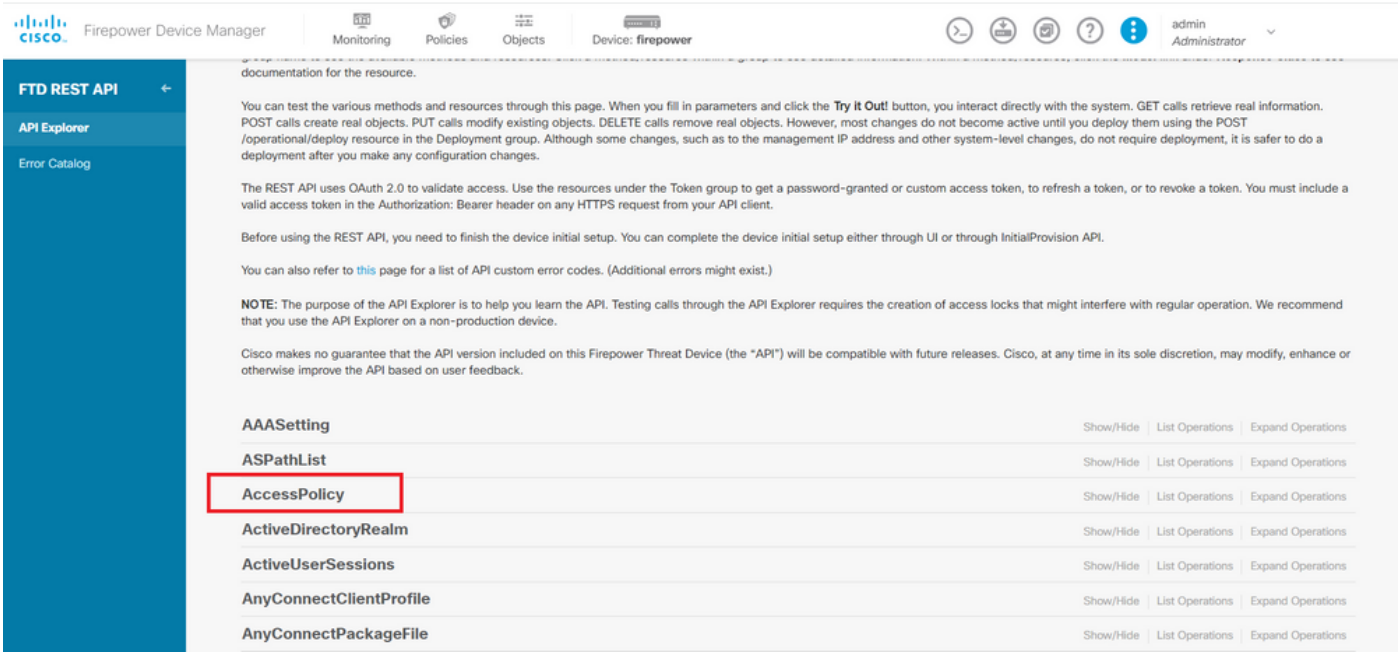

图 2.API Explorer Web用户界面。

第三步：运行GET调用以获取访问策略ID。

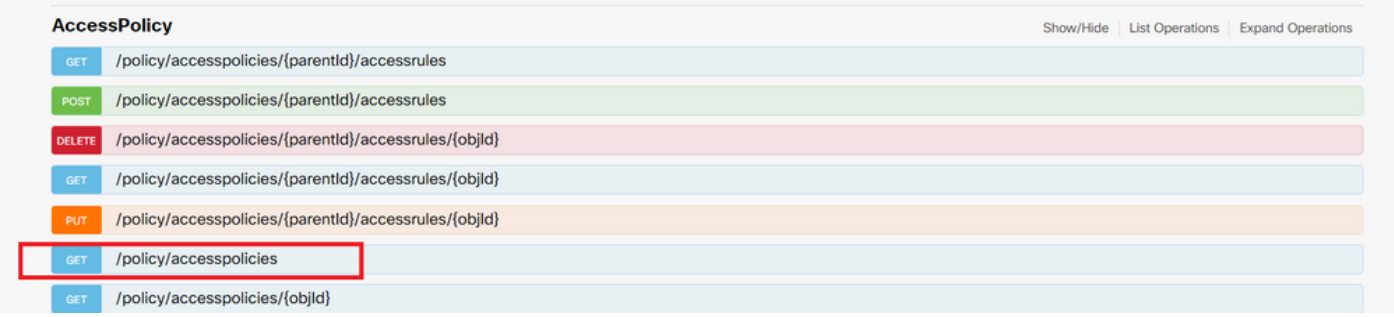

图 3.访问策略类别。

第四步：您必须点击TRY IT OUT!才能检索API响应。

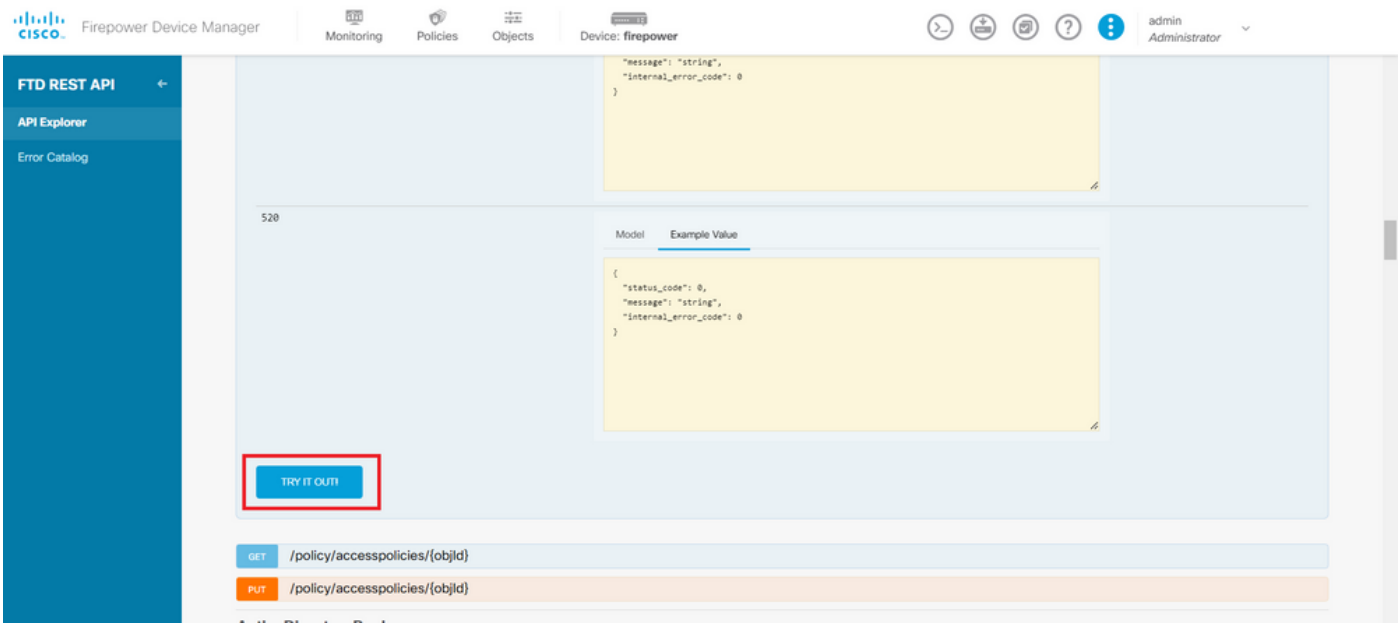

图 4.TRY IT OUT！运行API调用的按钮。

第五步：将数据从JSON响应正文复制到记事本。之后，您必须使用访问控制策略ID。

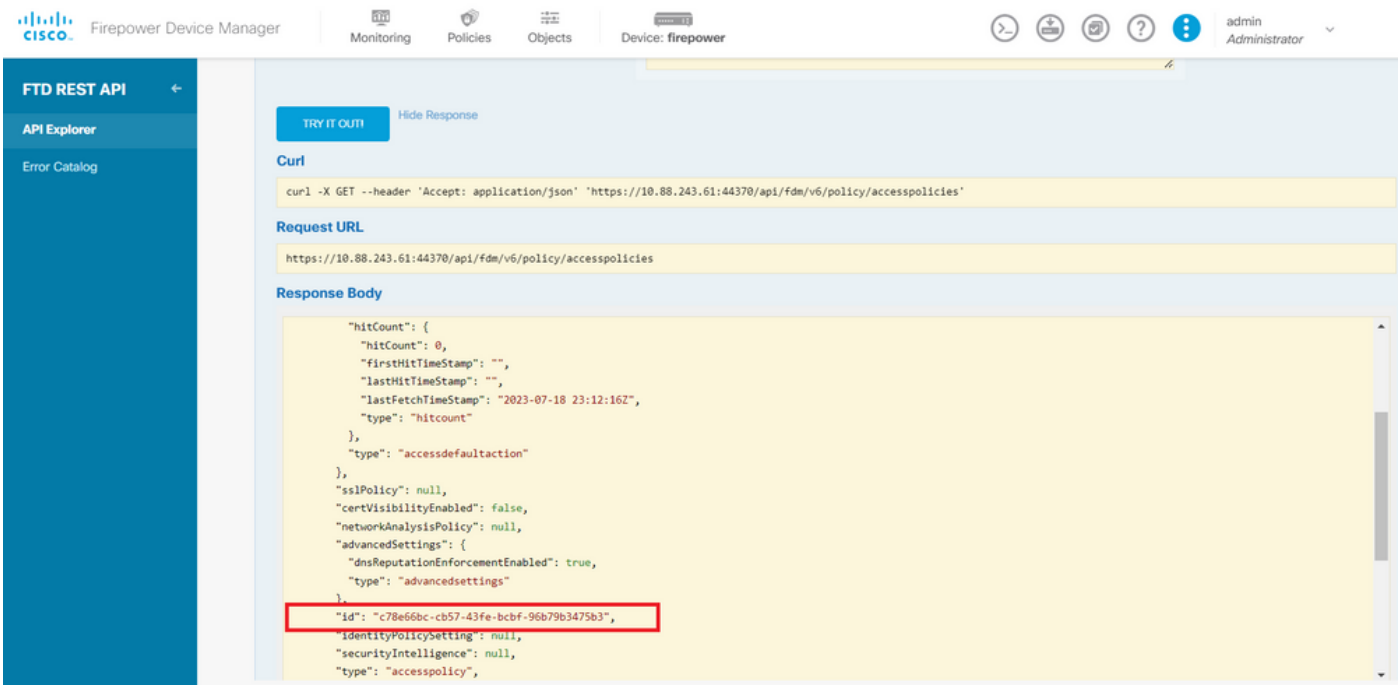

图 5.访问策略的GET响应。

第六步：在API资源管理器上查找并打开TimeRange类别以显示不同的API调用。

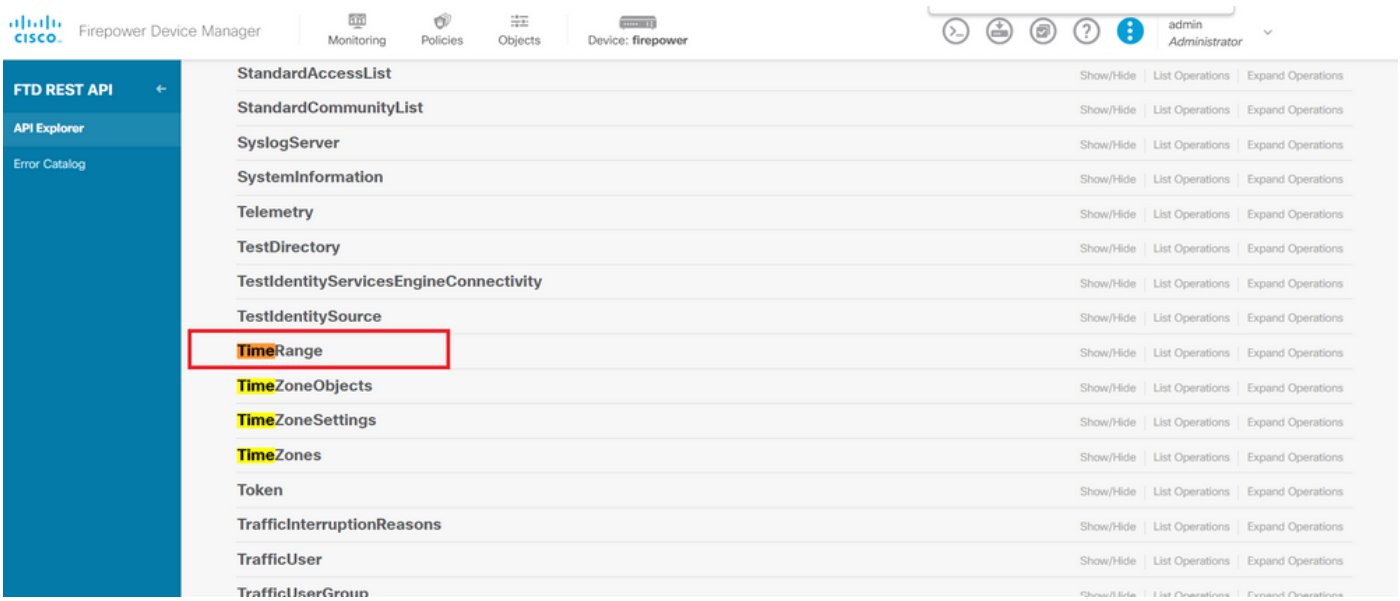

图 6.时间范围类别。

步骤 7.使用POST API调用，创建任意多个TimeRange对象。

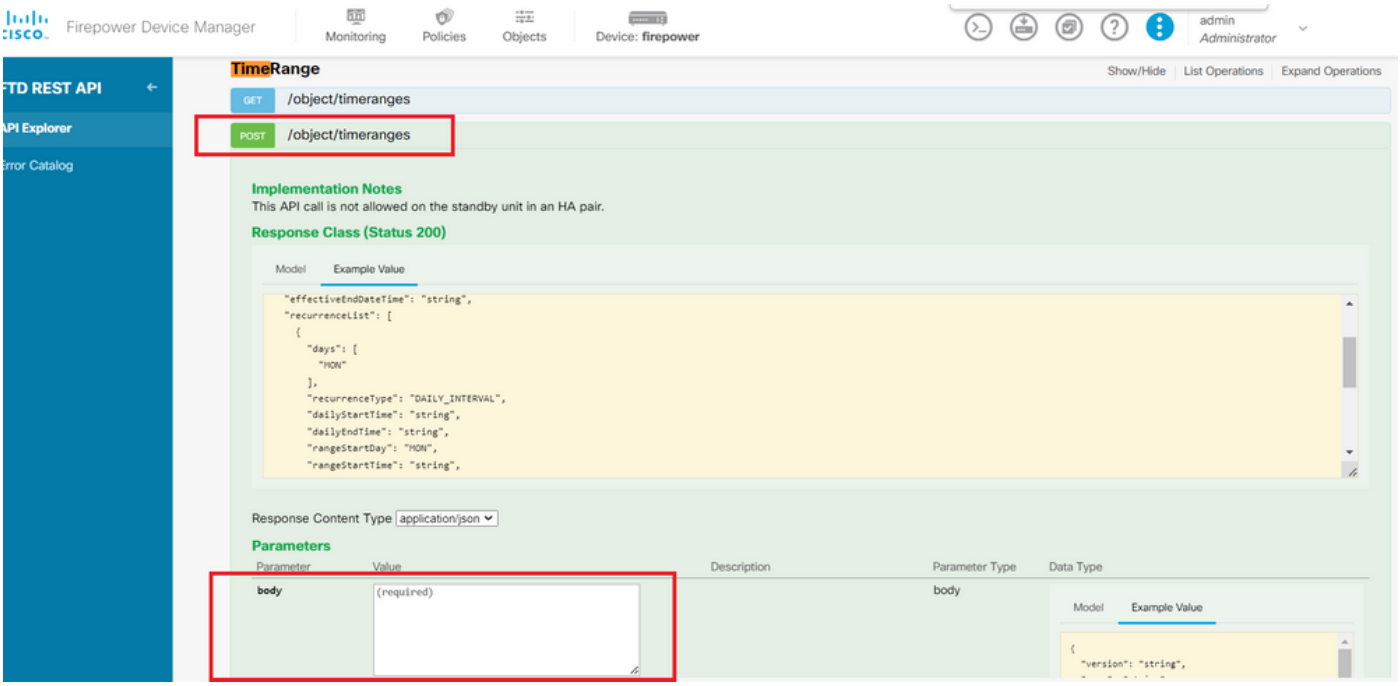

图 7.POST呼叫的时间范围。

在此处找到几个格式示JSON例，以创建两个不同的TimeRange对象。

对象1:

<#root>

{

```
  "name": "
```

range-obj-1

```
",
  "recurrenceList": [
    {
      "days": [
        "MON",
        "TUE",
        "WED",
        "THU",
        "FRI"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "
```

00:00

```
",
      "dailyEndTime": "
```

23:50

```
",
      "type": "recurrence"
    }
  ],
  "type": "timerangeobject"
}
```

対象2:

<#root>

```
{

  "name": "
```

range-obj-2

```
",
  "recurrenceList": [
    {
      "days": [
        "MON"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "
```

12:00

```
",
      "dailyEndTime": "
```

13:00

```
",
      "type": "recurrence"
    }
```

```
  ],
  "type": "timerangeobject",
}
```

注：请记住，TRY IT OUT! 要执行API调用，请点击。

步骤 8运行调用GET ，以获取TimeRange对象ID。

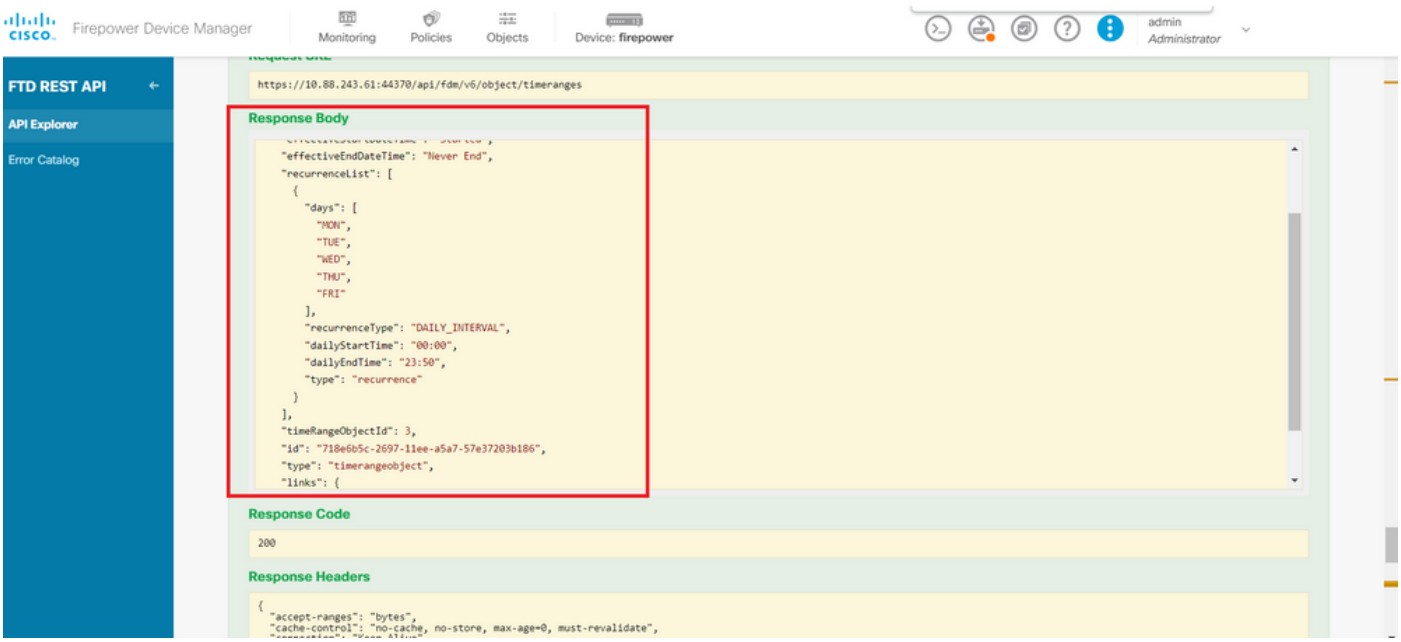

图 8.从时间范围获取GET响应。

步骤 9单击Deploy按钮以验证和应用更改。

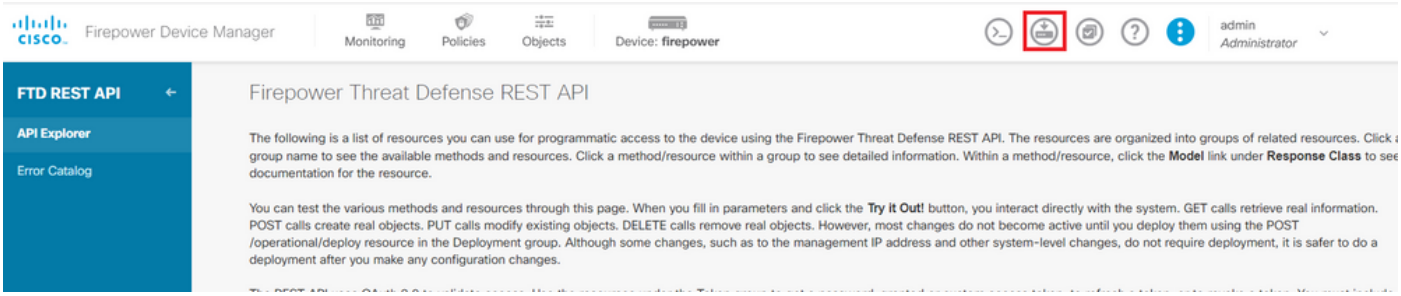

图 9.可从API资源管理器中使用部署按钮。

步骤 10验证您刚刚创建的配置，然后单击 DEPLOY NOW.

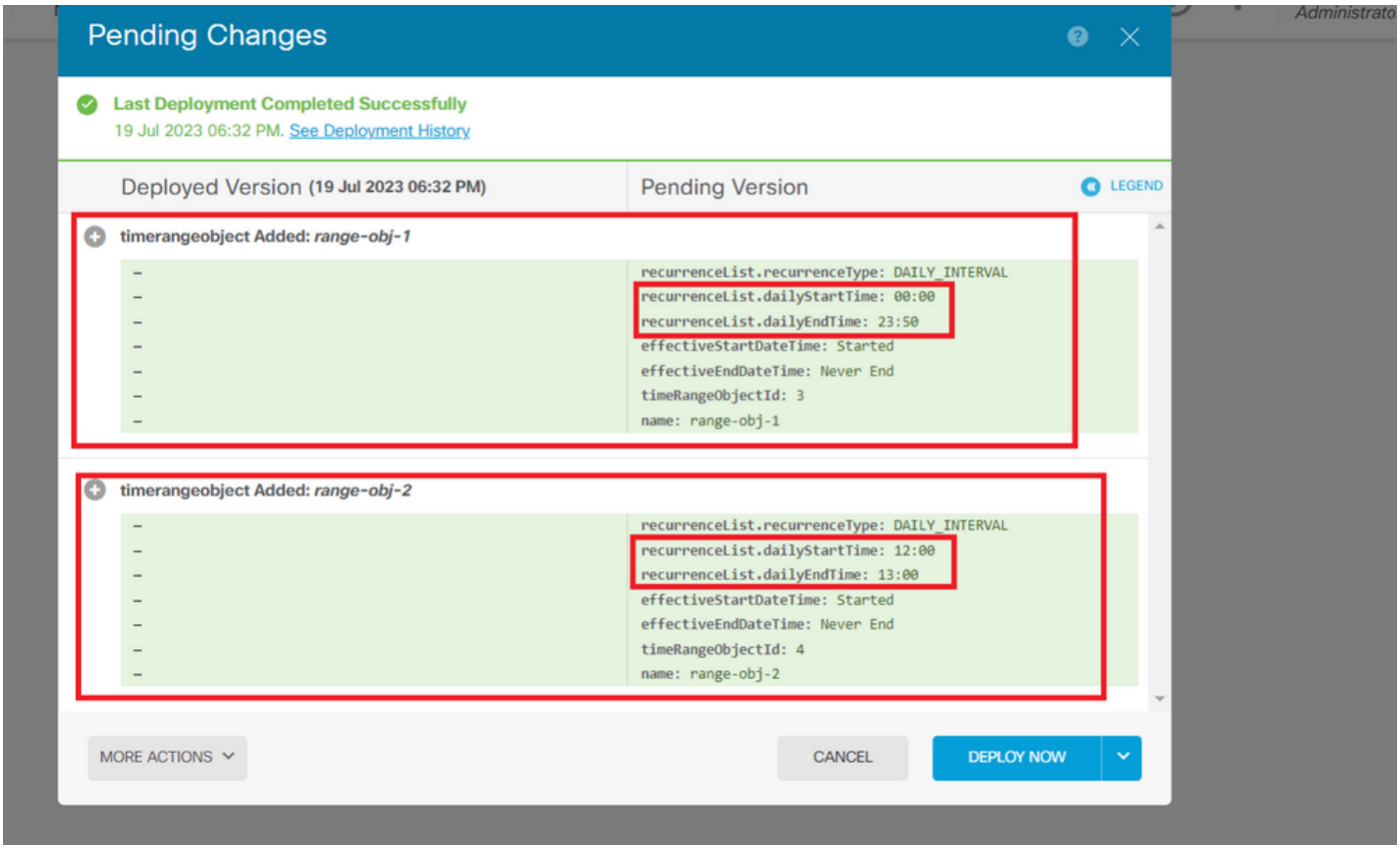

图 10.FDM挂起更改窗口。

步骤 11查找类别AccessPolicy，然后打开POST呼叫，以便创建基于时间的访问控制规则。

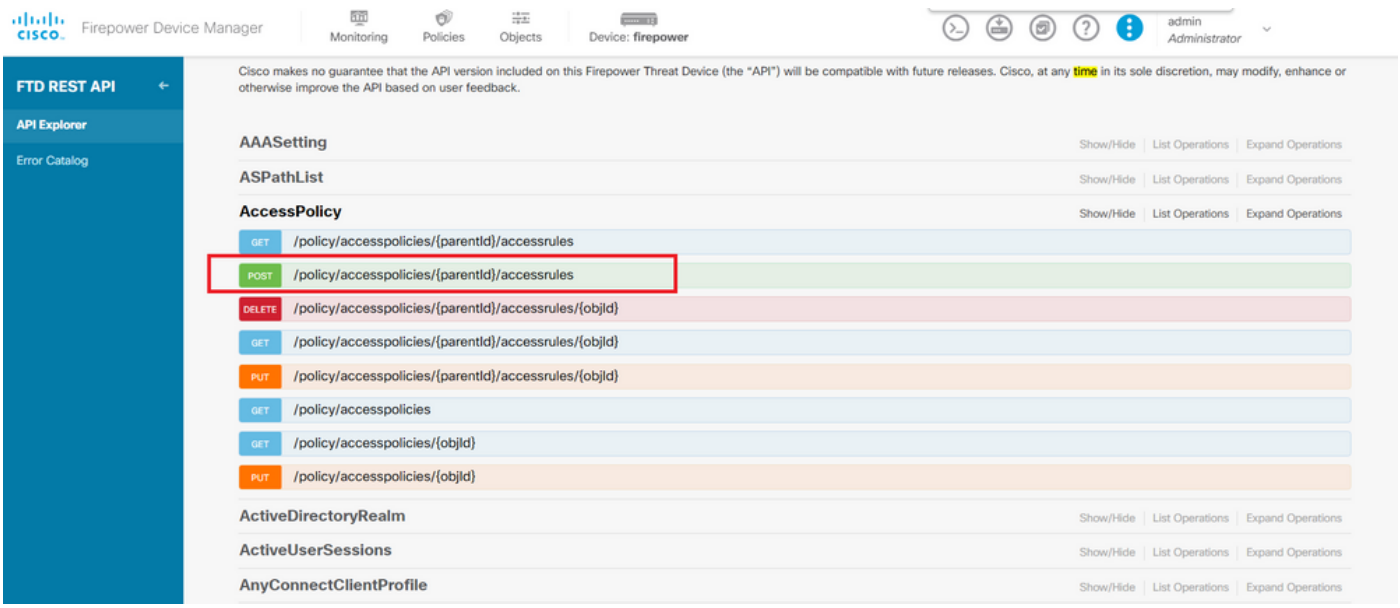

图 11.访问策略POST呼叫。

在此找到一JSON个格式示例，用于创建基于时间的ACL，允许流量从内部区域流向外部区域。

确保使用正确的时间范围对象ID。

<#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"
}
```

注意eventLogAction：必**LOG_FlOW_END**须在流程结束时记录事件，否则会出错。

步骤 12部署更改以应用新的基于时间的ACL。Pending Changes提示必须显示步骤10中所用的时间范围对象。

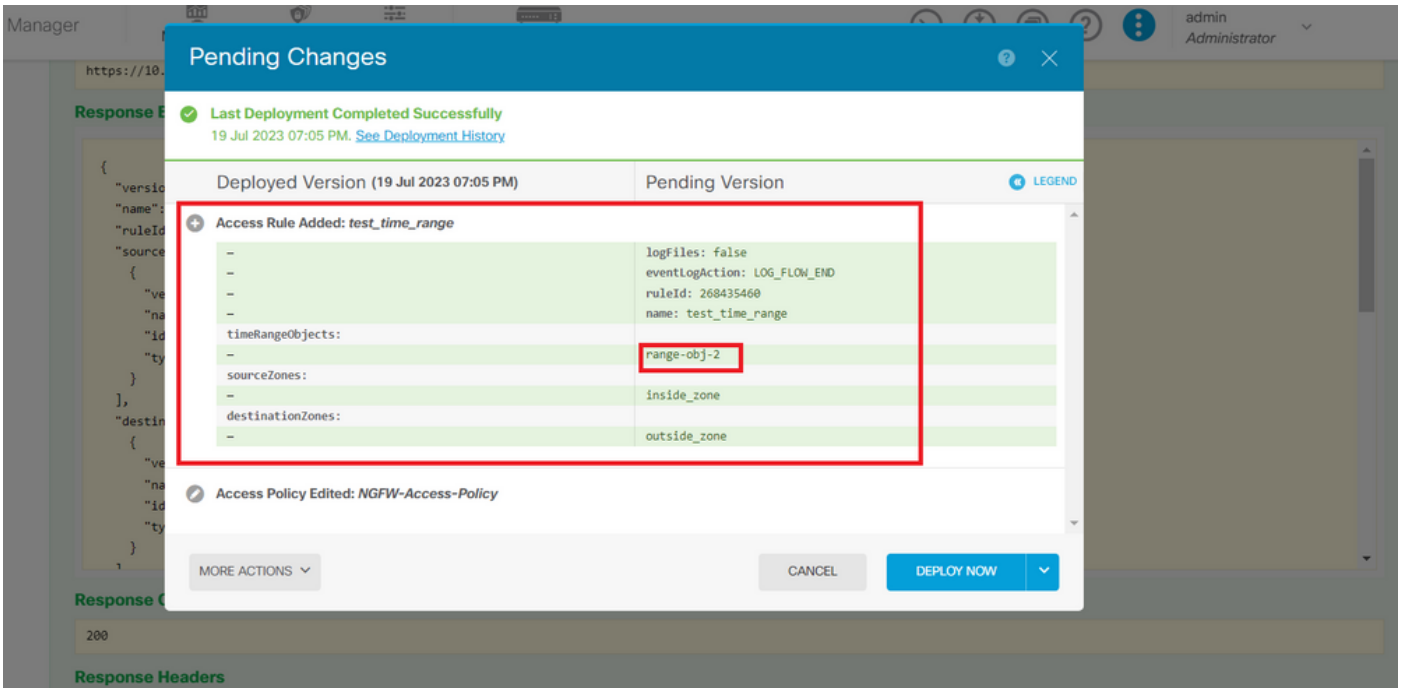

图 12.“FDM挂起更改”窗口将显示新规则。

第 13 步（可选）：如果要编辑ACL，可以使用呼叫并PUT编辑时间范围ID。

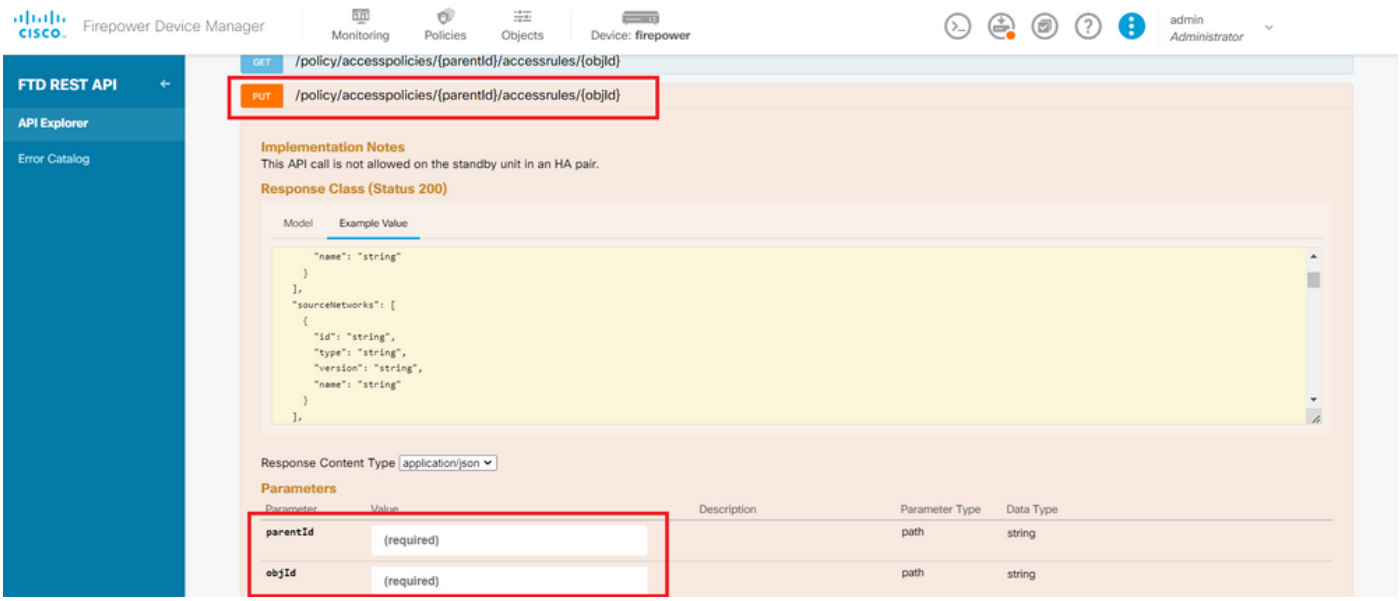

图 13.访问策略PUT呼叫。

在此找到格JSON式示例以编辑时间范围，这些时间范围ID可以通过使用调用进行收集GET。

<#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"
}
```


步骤 14部署和验证更改。

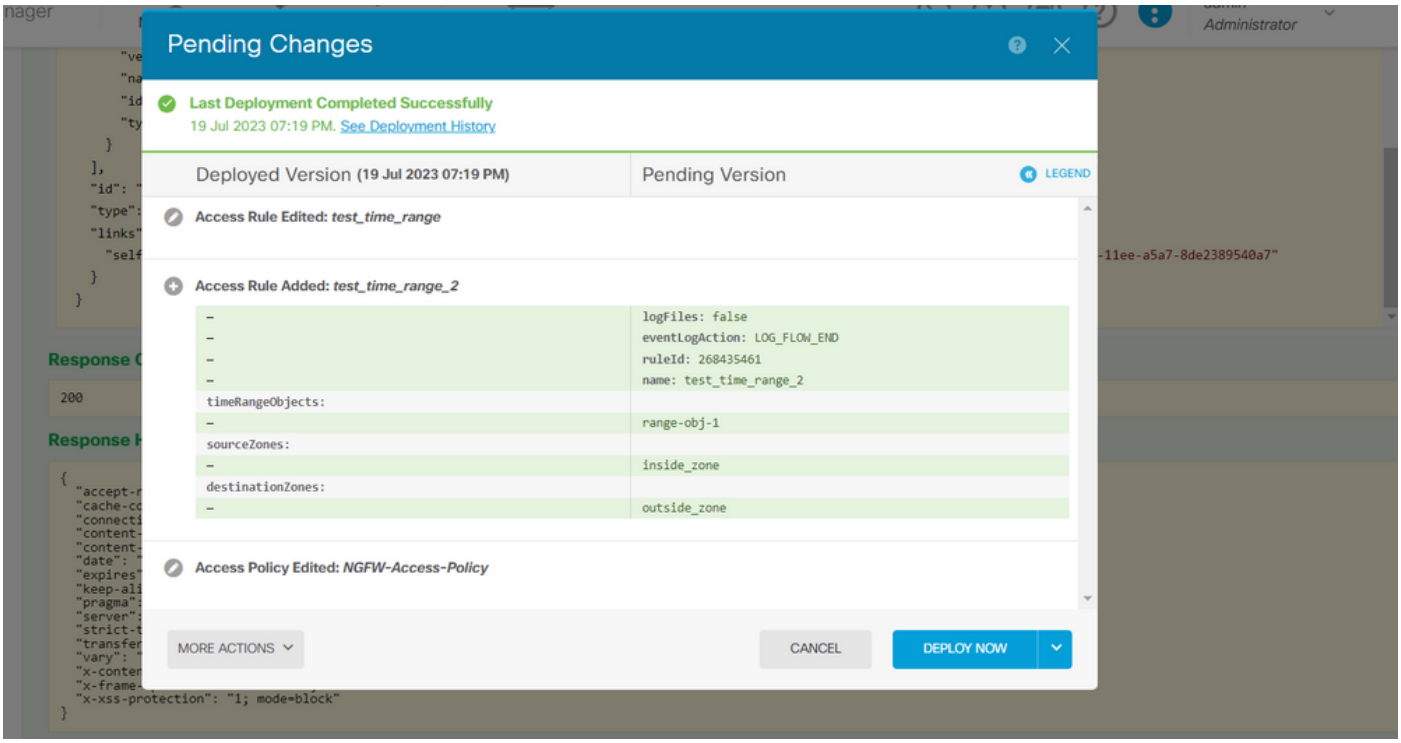

图 14.“FDM挂起更改”(FDM Pending Changes)窗口显示对象的更改。

验证

1.运行命令show time-range，以验证时间范围对象的状态。

```
<#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

)
   periodic Monday 12:00 to 13:00
```

2.使用show access-control-config命令验证访问控制规则配置。

<#root>

>

show access-control-config

```
===============[ NGFW-Access-Policy ]===============
Description :
=================[ Default Action ]=================
Default Action : Block
Logging Configuration
DC : Enabled
Beginning : Disabled
End : Disabled
Rule Hits : 0
Variable Set : Object missing: 76fa83ea-c972-11e2-8be8-8e45bb1343c0

===[ Security Intelligence - Network Whitelist ]====
===[ Security Intelligence - Network Blacklist ]====
Logging Configuration : Disabled
DC : Disabled

=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
Logging Configuration : Disabled
DC : Disabled


======[ Rule Set: admin_category (Built-in) ]=======

=====[ Rule Set: standard_category (Built-in) ]=====

-------------[ Rule: test_time_range ]--------------
Action :
```

Allow

```
Source ISE Metadata :


Source Zones : inside_zone
Destination Zones : outside_zone
Users
URLs
Logging Configuration
DC : Enabled
Beginning : Disabled
End : Enabled
Files : Disabled
Safe Search : No
Rule Hits : 0
Variable Set : Object missing: 76fa83ea-c972-11e2-8be8-8e45bb1343c0
Time Range :
```

range-obj-1

```
Daily Interval
StartTime : 00:00
EndTime : 23:50
Days : Monday,Tuesday,Wednesday,Thursday,Friday
```

3.运行调试System Support Trace，以确认流量符合正确的规则。

<#root>

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:
Please specify a server port: 443
Monitoring packet tracer and firewall debug messages


10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 New firewall session
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 app event with app id no change, url no chang
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Starting with minimum 1, 'test_time_range', a
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1

match rule order 1, 'test_time_range', action Allow

10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 MidRecovery data sent for rule id: 268435460,
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1

allow action


10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Packet 1930048: TCP ******S*, 07/20-18:05:06.
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Session: new snort session
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 AppID: service: (0), client: (0), payload: (0
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Firewall: starting rule matching, zone 2 -> 1
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1

Firewall: allow rule, 'test_time_range', allow

10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Policies: Network 0, Inspection 0, Detection
10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Verdict:

pass
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。