在具有Rest API的FDM上配置基於時間的訪問控制規則

目錄

簡介

本文描述如何在FDM使用Rest API管理的FTD上配置和驗證基於時間的訪問控制規則。

必要條件

需求

思科建議您瞭解以下主題：

- 安全防火牆威脅防禦(FTD)
- Firepower裝置管理(FDM)
- 具象狀態傳輸應用程式設計介面(REST API)知識
- 存取控制清單(ACL)

採用元件

本檔案中的資訊是根據FTD 7.1.0版。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

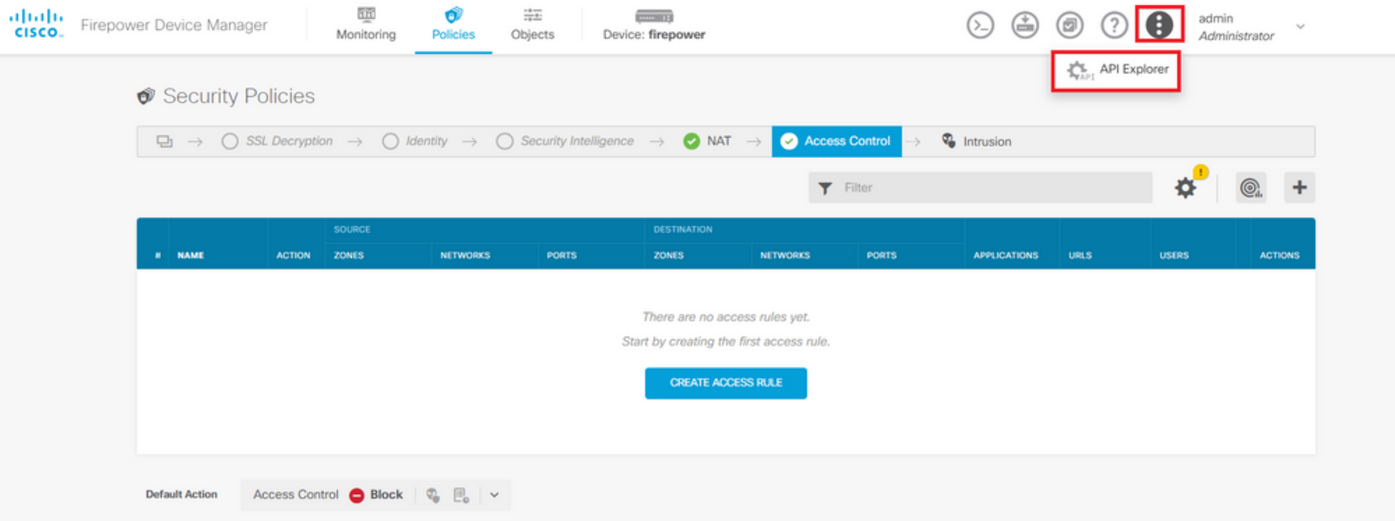
背景資訊

FTD API版本6.6.0和更新版本支援根據時間進行限制的訪問控制規則。

使用FTD API，您可以建立時間範圍對象（指定一次性或循環時間範圍），並將這些對象應用於訪問控制規則。使用時間範圍，您可以將訪問控制規則應用於一天中的某些時間或某些時間段的流量，以便為網路使用提供靈活性。不能使用FDM建立或應用時間範圍，FDM也不會顯示訪問控制規則是否應用了時間範圍。

設定

步驟 1.按一下高級選項（「kebab」選單）以開啟FDM API資源管理器。

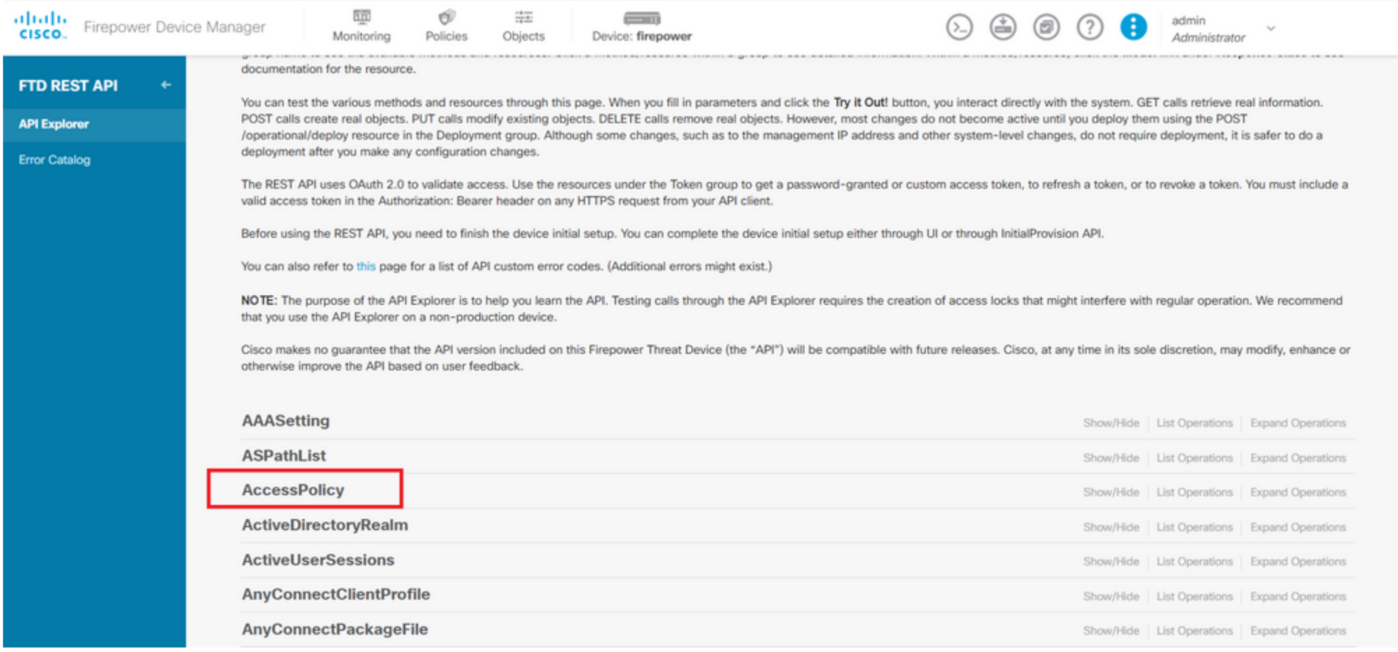


There are no access rules yet.

Start by creating the first access rule.

圖1.FDM Web使用者介面。

步驟 2.選擇類別AccessPolicy以顯示不同的API呼叫。



documentation for the resource.

You can test the various methods and resources through this page. When you fill in parameters and click the **Try it Out!** button, you interact directly with the system. GET calls retrieve real information. POST calls create real objects. PUT calls modify existing objects. DELETE calls remove real objects. However, most changes do not become active until you deploy them using the POST /operational/deploy resource in the Deployment group. Although some changes, such as to the management IP address and other system-level changes, do not require deployment, it is safer to do a deployment after you make any configuration changes.

The REST API uses OAuth 2.0 to validate access. Use the resources under the Token group to get a password-granted or custom access token, to refresh a token, or to revoke a token. You must include a valid access token in the Authorization: Bearer header on any HTTPS request from your API client.

Before using the REST API, you need to finish the device initial setup. You can complete the device initial setup either through UI or through InitialProvision API.

You can also refer to this page for a list of API custom error codes. (Additional errors might exist.)

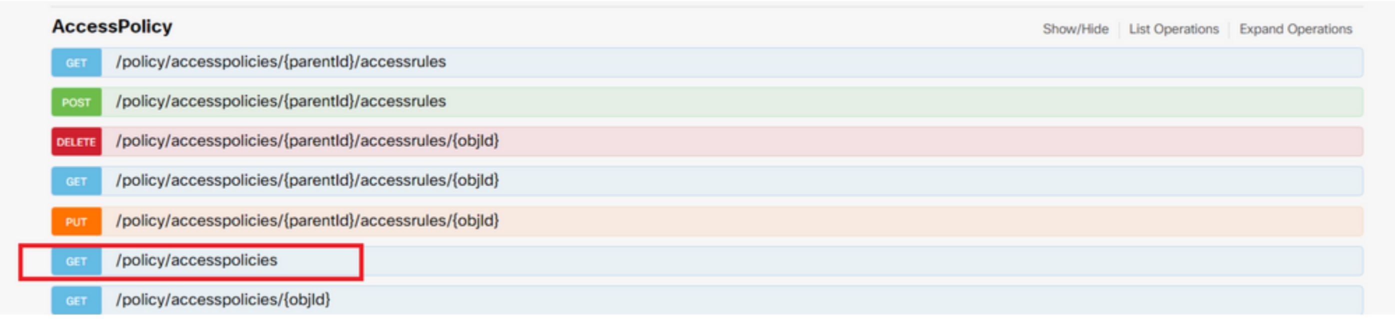
NOTE: The purpose of the API Explorer is to help you learn the API. Testing calls through the API Explorer requires the creation of access locks that might interfere with regular operation. We recommend that you use the API Explorer on a non-production device.

Cisco makes no guarantee that the API version included on this Firepower Threat Device (the "API") will be compatible with future releases. Cisco, at any time in its sole discretion, may modify, enhance or otherwise improve the API based on user feedback.

AAASetting Show/Hide | List Operations | Expand Operations
ASPathList Show/Hide | List Operations | Expand Operations
AccessPolicy Show/Hide | List Operations | Expand Operations
ActiveDirectoryRealm Show/Hide | List Operations | Expand Operations
ActiveUserSessions Show/Hide | List Operations | Expand Operations
AnyConnectClientProfile Show/Hide | List Operations | Expand Operations
AnyConnectPackageFile Show/Hide | List Operations | Expand Operations

圖2.API Explorer Web使用者介面。

步驟 3.運行GET呼叫以獲取訪問策略ID。



AccessPolicy

GET /policy/accesspolicies/{parentId}/accessrules

POST /policy/accesspolicies/{parentId}/accessrules

DELETE /policy/accesspolicies/{parentId}/accessrules/{objId}

GET /policy/accesspolicies/{parentId}/accessrules/{objId}

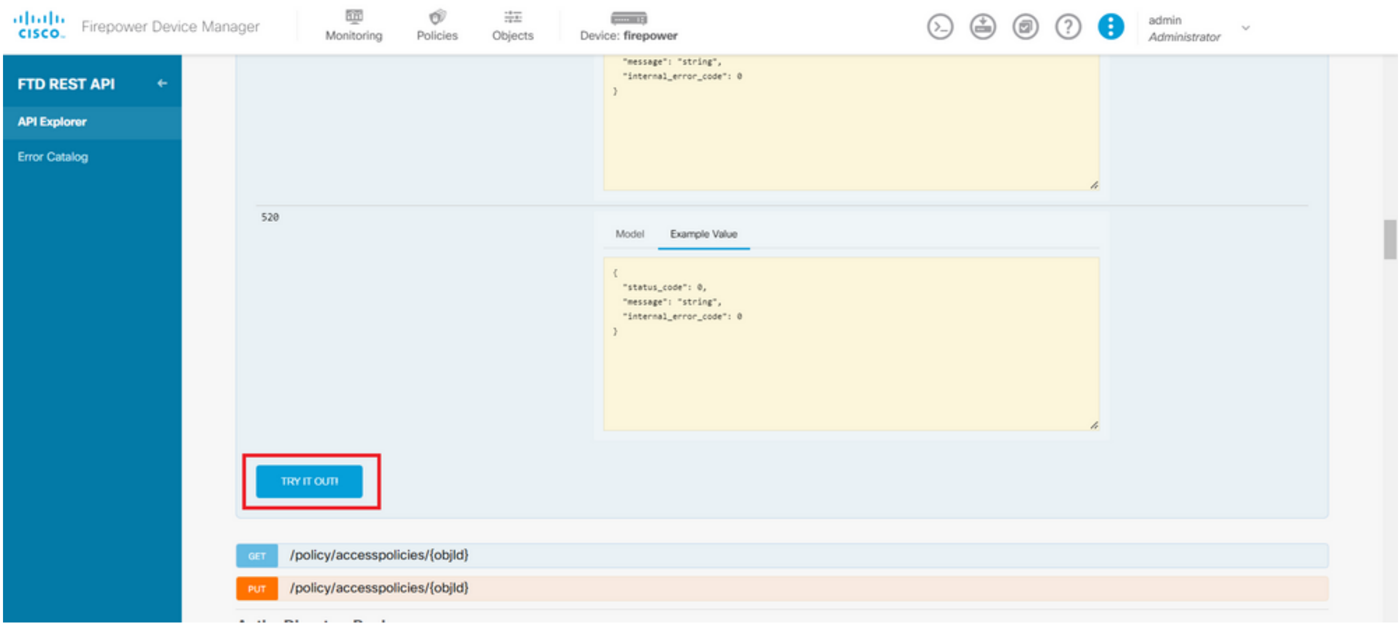
PUT /policy/accesspolicies/{parentId}/accessrules/{objId}

GET /policy/accesspolicies

GET /policy/accesspolicies/{objId}

圖3.訪問策略類別。

步驟 4.您必須點選TRY IT OUT!才能檢索API響應。



```
  "message": "string",
  "internal_error_code": 0
}
```

520

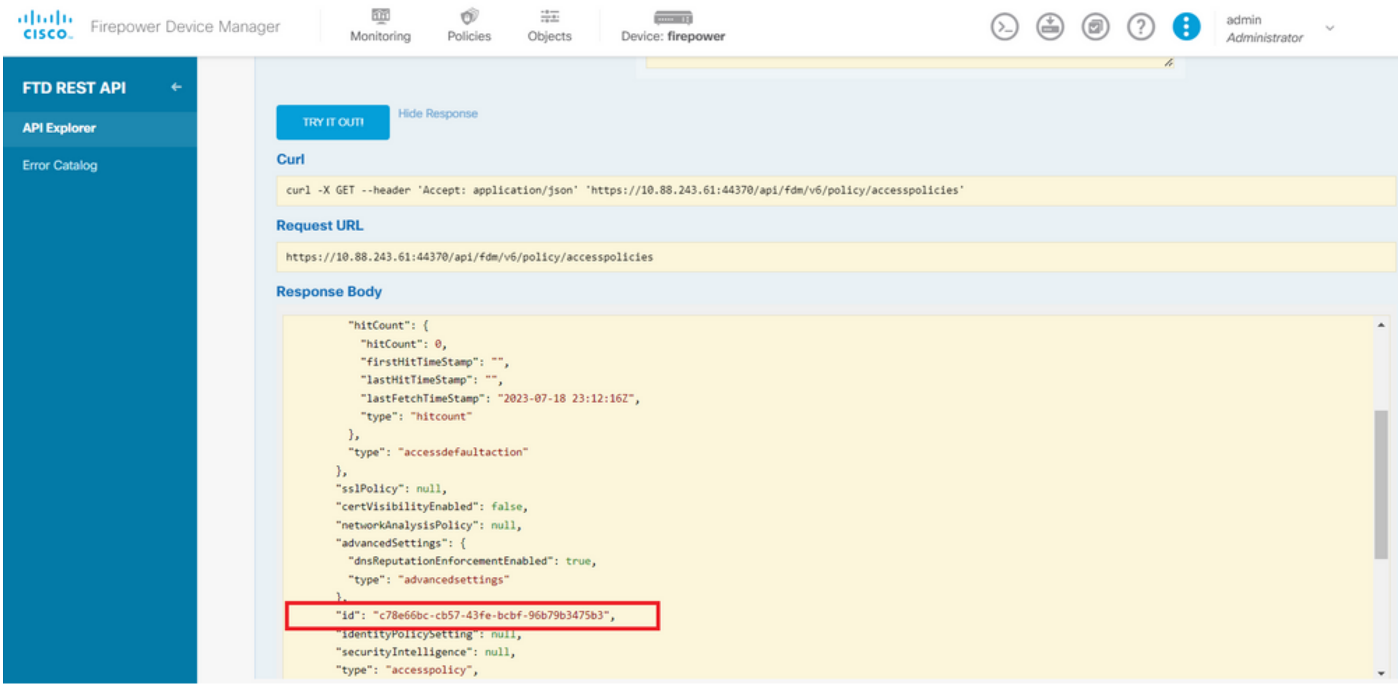
```
{
  "status_code": 0,
  "message": "string",
  "internal_error_code": 0
}
```

GET /policy/accesspolicies/{objId}

PUT /policy/accesspolicies/{objId}

圖4.TRY IT OUT！運行API呼叫的按鈕。

步驟 5.將資料從JSON響應正文複製到記事本。以後，您必須使用訪問控制策略ID。



Curl

```
curl -X GET --header 'Accept: application/json' 'https://10.88.243.61:44370/api/fdm/v6/policy/accesspolicies'
```

Request URL

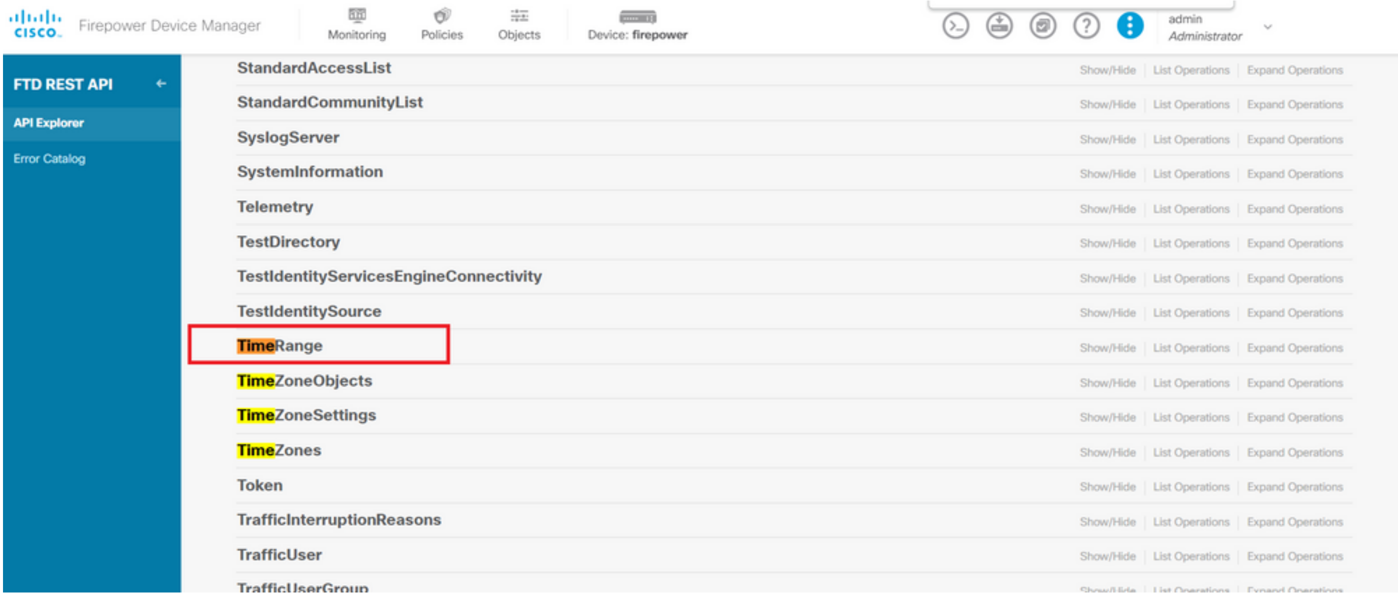
```
https://10.88.243.61:44370/api/fdm/v6/policy/accesspolicies
```

Response Body

```
        "hitCount": {
          "hitCount": 0,
          "firstHitTimeStamp": "",
          "lastHitTimeStamp": "",
          "lastFetchTimeStamp": "2023-07-18 23:12:16Z",
          "type": "hitcount"
        },
        "type": "accessdefaultaction"
      },
      "sslPolicy": null,
      "certVisibilityEnabled": false,
      "networkAnalysisPolicy": null,
      "advancedSettings": {
        "dnsReputationEnforcementEnabled": true,
        "type": "advancedsettings"
      },
      "id": "c78e66bc-cb57-43fe-bcbf-96b79b3475b3",
      "identityPolicySetting": null,
      "securityIntelligence": null,
      "type": "accesspolicy",
```

圖5.從訪問策略獲取GET響應。

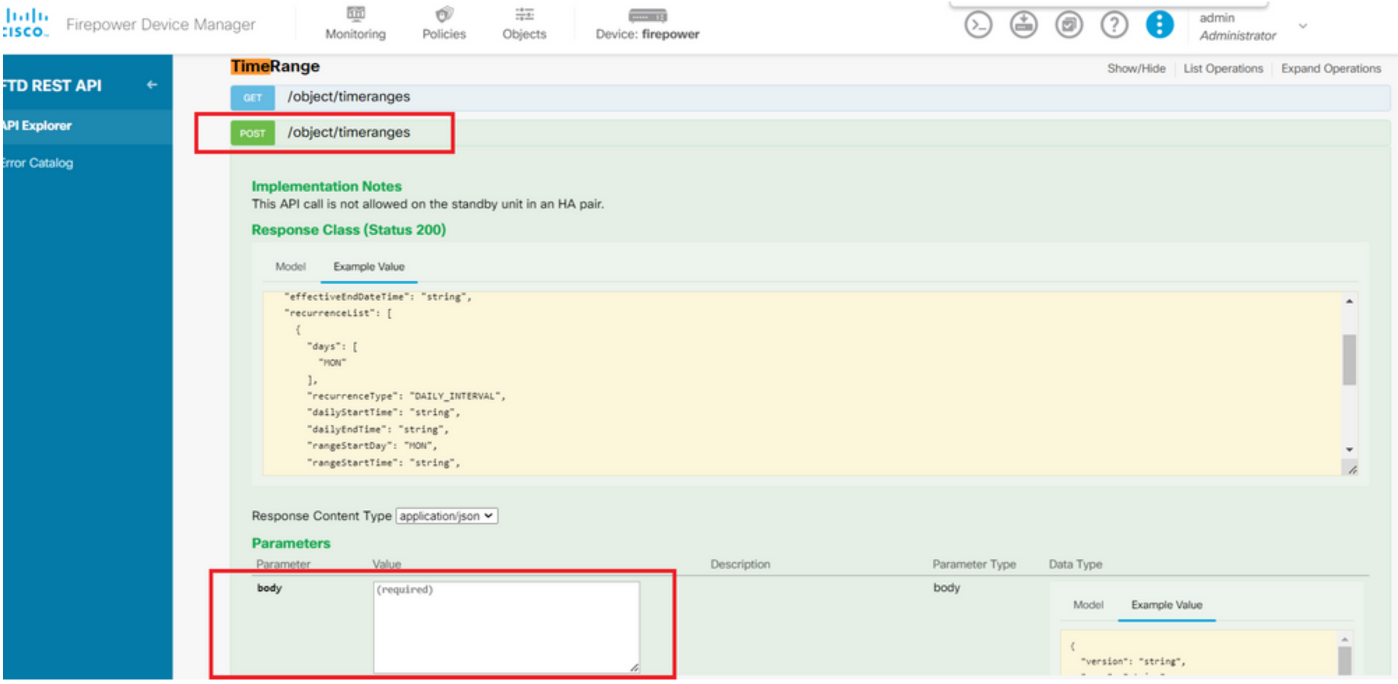
步驟 6.在API資源管理器上查詢並開啟TimeRange類別以顯示不同的API呼叫。



StandardAccessList
StandardCommunityList
SyslogServer
SystemInformation
Telemetry
TestDirectory
TestIdentityServicesEngineConnectivity
TestIdentitySource
TimeRange
TimeZoneObjects
TimeZoneSettings
TimeZones
Token
TrafficInterruptionReasons
TrafficUser
TrafficUserGroup

圖6.時間範圍類別。

步驟 7.使用POST API呼叫，建立任意多個TimeRange對象。



TimeRange

GET /object/timeranges

POST /object/timeranges

Implementation Notes

This API call is not allowed on the standby unit in an HA pair.

Response Class (Status 200)

```
  "effectiveEndDateTime": "string",
  "recurrenceList": [
    {
      "days": [
        "MON"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "string",
      "dailyEndTime": "string",
      "rangeStartDay": "MON",
      "rangeStartTime": "string",
```

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
body	(required)		body	{ "version": "string",

圖7.時間範圍POST呼叫。

在此處找到幾個格式示JSON例，以建立兩個不同的TimeRange對象。

對象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"
}
```

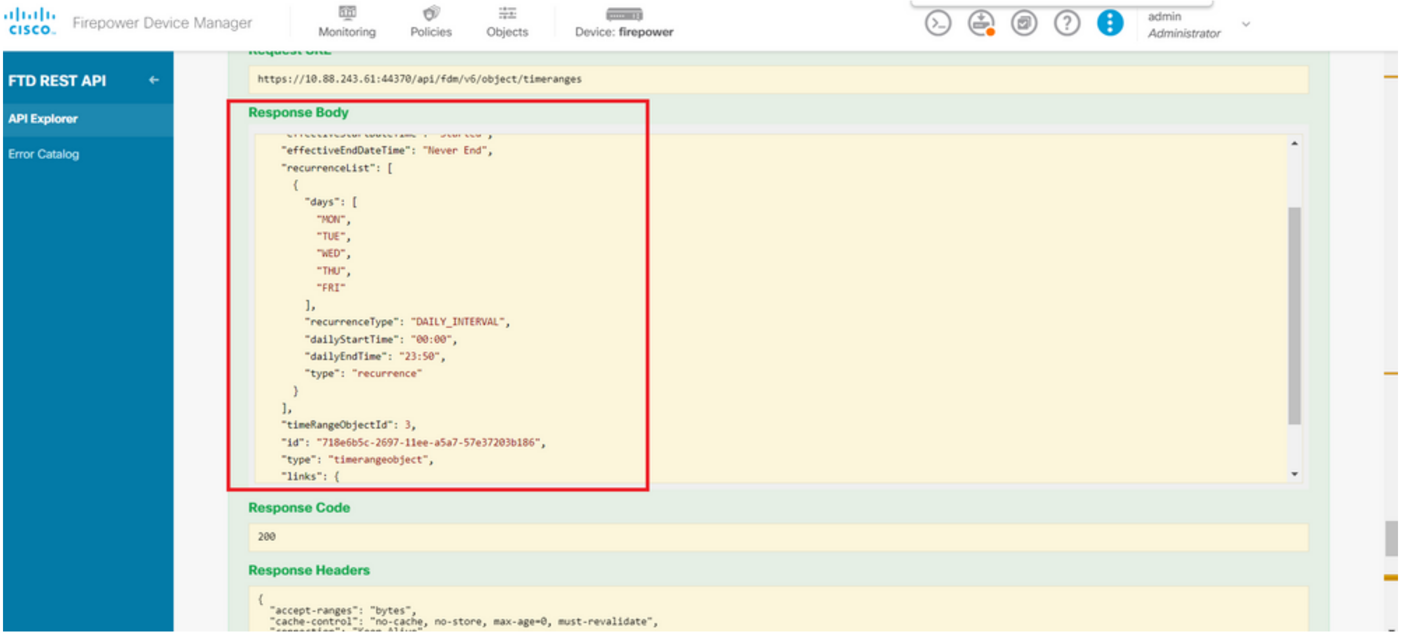
對象2:

<#root>

```
{

  "name": "

range-obj-2

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

12:00

",
      "dailyEndTime": "

13:00

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

注意：請記得按TRY IT OUT! 鍵以運行API呼叫。

步驟 8.運行調用GET ，以獲取TimeRange對象ID。



```
https://10.88.243.61:44370/api/fdm/v6/object/timeranges
```

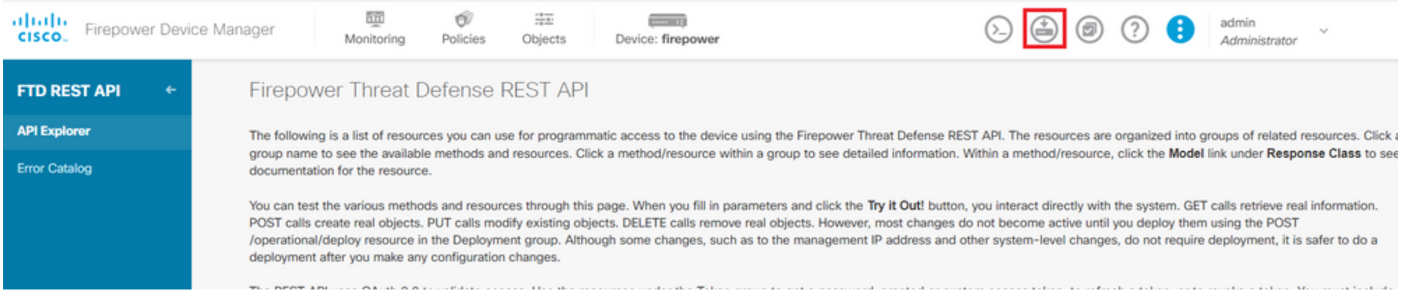
```
    "effectiveEndDateTime": "Never End",
    "recurrenceList": [
      {
        "days": [
          "MON",
          "TUE",
          "WED",
          "THU",
          "FRI"
        ],
        "recurrenceType": "DAILY_INTERVAL",
        "dailyStartTime": "00:00",
        "dailyEndTime": "23:50",
        "type": "recurrence"
      }
    ],
    "timeRangeObjectId": 3,
    "id": "718e6b5c-2697-11ee-a5a7-57e37203b186",
    "type": "timerangeobject",
    "links": {
```

```
200
```

```
{
  "accept-ranges": "bytes",
  "cache-control": "no-cache, no-store, max-age=0, must-revalidate",
```

圖8.從時間範圍獲取GET響應。

步驟 9.按一下Deploy「OK」按鈕以驗證並應用您的變更。



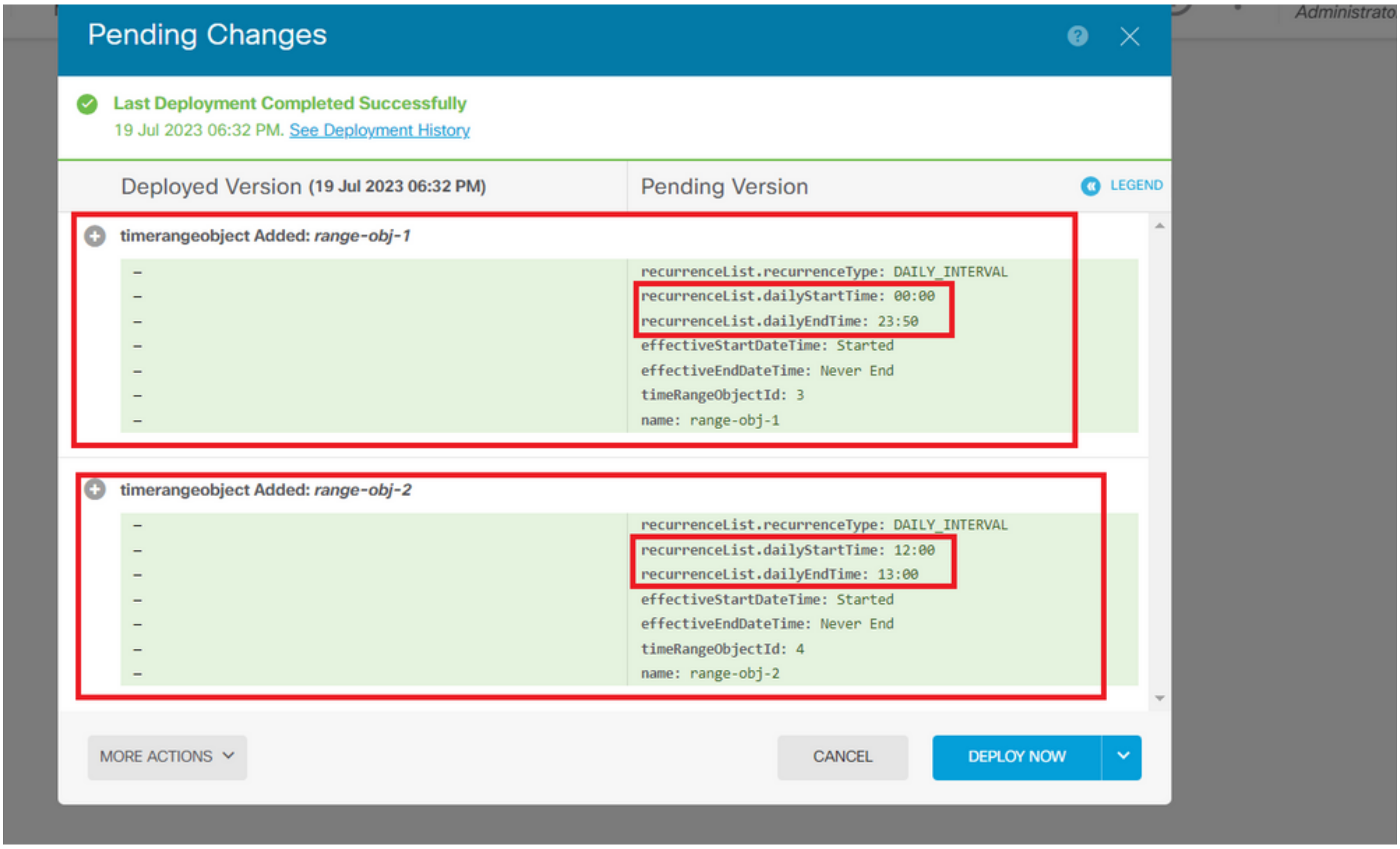
Firepower Threat Defense REST API

The following is a list of resources you can use for programmatic access to the device using the Firepower Threat Defense REST API. The resources are organized into groups of related resources. Click a group name to see the available methods and resources. Click a method/resource within a group to see detailed information. Within a method/resource, click the **Model** link under **Response Class** to see documentation for the resource.

You can test the various methods and resources through this page. When you fill in parameters and click the **Try it Out!** button, you interact directly with the system. GET calls retrieve real information. POST calls create real objects. PUT calls modify existing objects. DELETE calls remove real objects. However, most changes do not become active until you deploy them using the POST /operational/deploy resource in the Deployment group. Although some changes, such as to the management IP address and other system-level changes, do not require deployment, it is safer to do a deployment after you make any configuration changes.

圖9.API資源管理器中提供了「部署」按鈕。

步驟 10.驗證您剛剛建立的配置，然後按一下 DEPLOY NOW.



Pending Changes

Last Deployment Completed Successfully
19 Jul 2023 06:32 PM. See Deployment History

Deployed Version (19 Jul 2023 06:32 PM) | Pending Version

timerangeobject Added: *range-obj-1*

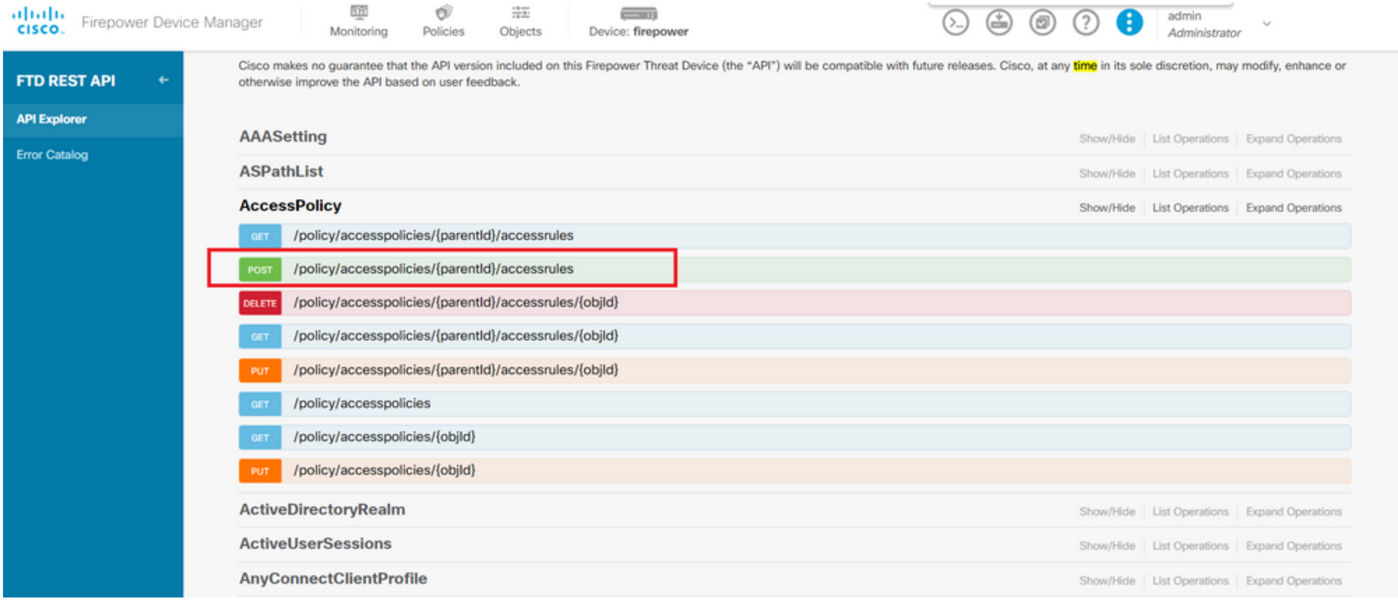
```
-    recurrenceList.recurrenceType: DAILY_INTERVAL
-    recurrenceList.dailyStartTime: 00:00
-    recurrenceList.dailyEndTime: 23:50
-    effectiveStartDateTime: Started
-    effectiveEndDateTime: Never End
-    timeRangeObjectId: 3
-    name: range-obj-1
```

timerangeobject Added: *range-obj-2*

```
-    recurrenceList.recurrenceType: DAILY_INTERVAL
-    recurrenceList.dailyStartTime: 12:00
-    recurrenceList.dailyEndTime: 13:00
-    effectiveStartDateTime: Started
-    effectiveEndDateTime: Never End
-    timeRangeObjectId: 4
-    name: range-obj-2
```

圖10.FDM掛起更改視窗。

步驟 11.查詢類AccessPolicy，然後開啟POST呼叫，以便建立基於時間的訪問控制規則。



Cisco makes no guarantee that the API version included on this Firepower Threat Device (the "API") will be compatible with future releases. Cisco, at any time in its sole discretion, may modify, enhance or otherwise improve the API based on user feedback.

AAASetting — Show/Hide | List Operations | Expand Operations

ASPathList — Show/Hide | List Operations | Expand Operations

AccessPolicy — Show/Hide | List Operations | Expand Operations

```
GET     /policy/accesspolicies/{parentId}/accessrules
POST    /policy/accesspolicies/{parentId}/accessrules
DELETE  /policy/accesspolicies/{parentId}/accessrules/{objId}
GET     /policy/accesspolicies/{parentId}/accessrules/{objId}
PUT     /policy/accesspolicies/{parentId}/accessrules/{objId}
GET     /policy/accesspolicies
GET     /policy/accesspolicies/{objId}
PUT     /policy/accesspolicies/{objId}
```

ActiveDirectoryRealm — Show/Hide | List Operations | Expand Operations

ActiveUserSessions — Show/Hide | List Operations | Expand Operations

AnyConnectClientProfile — Show/Hide | List Operations | Expand Operations

圖11.訪問策略POST呼叫。

在此處找到JSON一個格式示例，以建立允許流量從內部區域流向外部區域的基於時間的ACL。

確保使用正確的時間範圍對象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

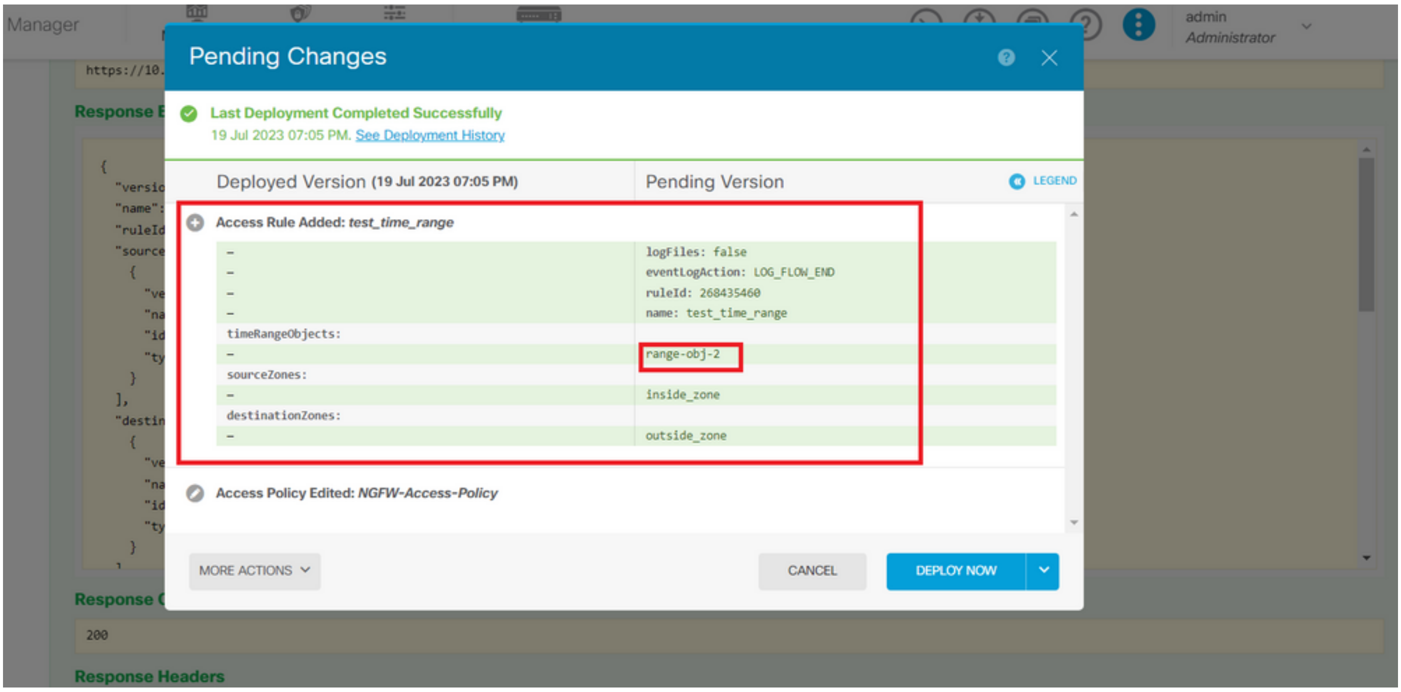
```
",
  "timeRangeObjects": [
    {
    "id": "
```

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

```
",
    "type": "timerangeobject",
    "name": "Time-test2"
    }
  ],
  "type": "accessrule"
}
```

注意eventLogAction：必**LOG_FlOW_END**須在流結束時記錄事件，否則會出錯。

步驟 12.部署更改以應用新的基於時間的ACL。Pending Changes提示必須顯示步驟10中所用的時間範圍對象。



Pending Changes

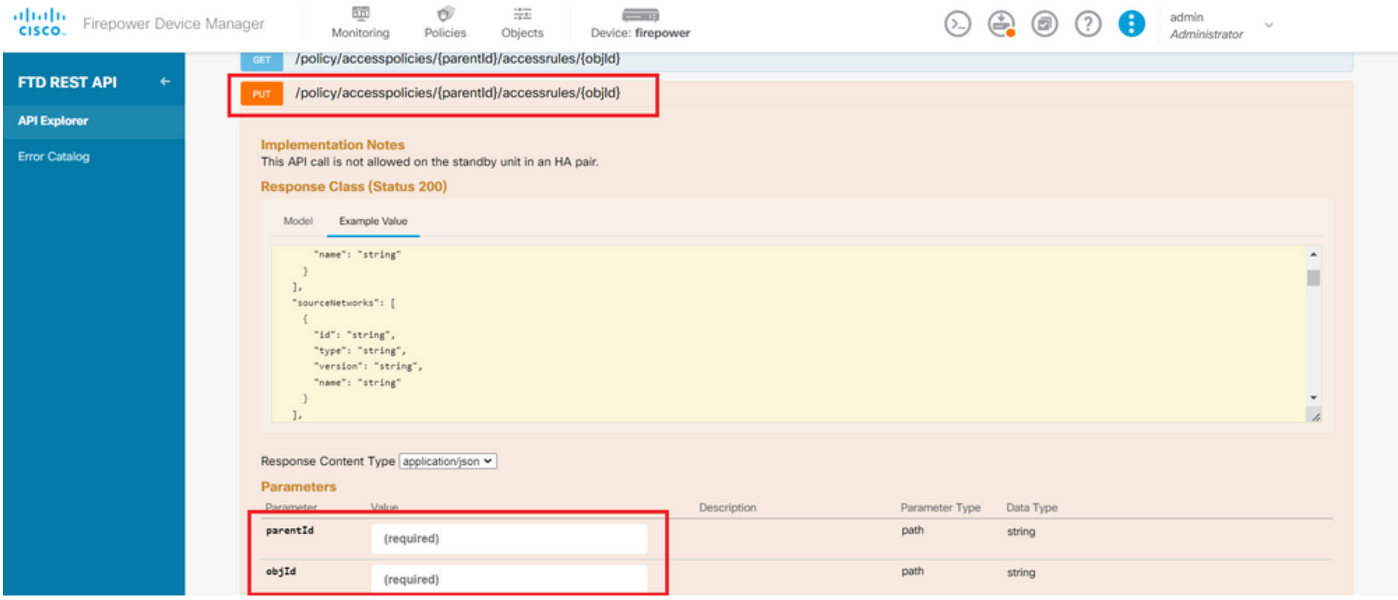
Last Deployment Completed Successfully
19 Jul 2023 07:05 PM. See Deployment History

Deployed Version (19 Jul 2023 07:05 PM)	Pending Version
Access Rule Added: *test_time_range*	
-	logFiles: false
-	eventLogAction: LOG_FLOW_END
-	ruleId: 268435460
-	name: test_time_range
timeRangeObjects:	
-	range-obj-2
sourceZones:	
-	inside_zone
destinationZones:	
-	outside_zone

Access Policy Edited: *NGFW-Access-Policy*

圖12.「FDM掛起更改」視窗顯示新規則。

第13步（可選）。如果要編輯ACL，可以使用調用PUT，並編輯時間範圍ID。



GET /policy/accesspolicies/{parentId}/accessrules/{objId}

PUT /policy/accesspolicies/{parentId}/accessrules/{objId}

Implementation Notes
This API call is not allowed on the standby unit in an HA pair.

Response Class (Status 200)

```
      "name": "string"
    }
  ],
  "sourceNetworks": [
    {
      "id": "string",
      "type": "string",
      "version": "string",
      "name": "string"
    }
  ],
```

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
parentId	(required)		path	string
objId	(required)		path	string

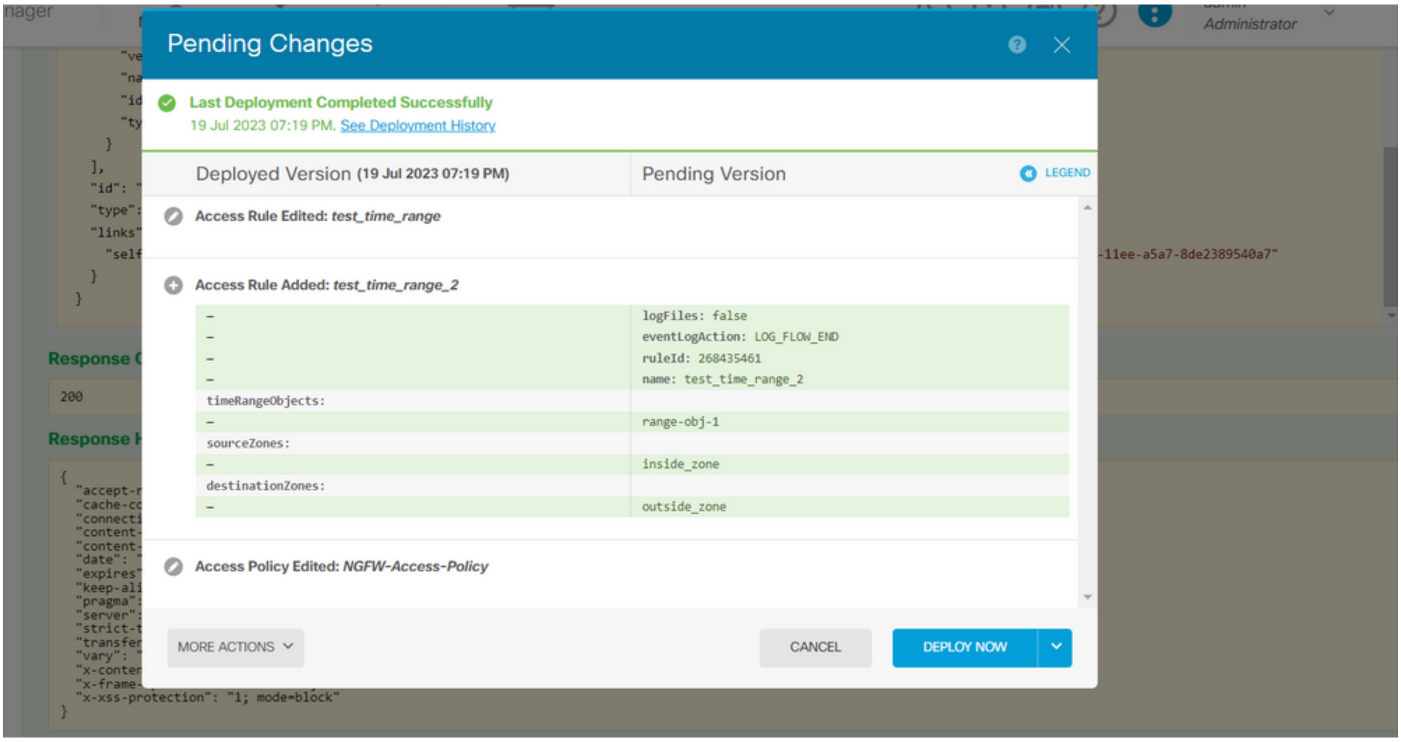
圖13.訪問策略PUT呼叫。

在此處查詢JSON「格式」示例為了編輯時間範圍，可以使用呼叫收集這些時間範圍IDGET。

<#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"
}
```

步驟 14.部署和驗證您的更改。



Pending Changes

Last Deployment Completed Successfully
19 Jul 2023 07:19 PM. See Deployment History

Deployed Version (19 Jul 2023 07:19 PM)	Pending Version
Access Rule Edited: *test_time_range*	
Access Rule Added: *test_time_range_2*	
–	logFiles: false
–	eventLogAction: LOG_FLOW_END
–	ruleId: 268435461
–	name: test_time_range_2
timeRangeObjects:	
–	range-obj-1
sourceZones:	
–	inside_zone
destinationZones:	
–	outside_zone
Access Policy Edited: *NGFW-Access-Policy*	

圖14.「FDM掛起更改」視窗顯示對象的更改。

驗證

1.運行命令show time-range，以驗證時間範圍對象的狀態。

<#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命令驗證訪問控制規則配置。

```
<#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.運行System Support Trace調試，以確認流量是否達到正確的規則。

<#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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。