

# REST APIを使用したFDMでの時間ベースのアクセス制御ルールの構成

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[確認](#)

---

## はじめに

このドキュメントでは、Rest APIを使用してFDMによって管理されるFTDで時間ベースのアクセス制御ルールを設定および検証する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール脅威対策(FTD)
- Firepowerデバイス管理(FDM)
- Representational State Transfer(REST)アプリケーションプログラミングインターフェイス(API)に関する知識
- Access Control List ( ACL; アクセス コントロール リスト )

### 使用するコンポーネント

このドキュメントの情報は、FTDバージョン7.1.0に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

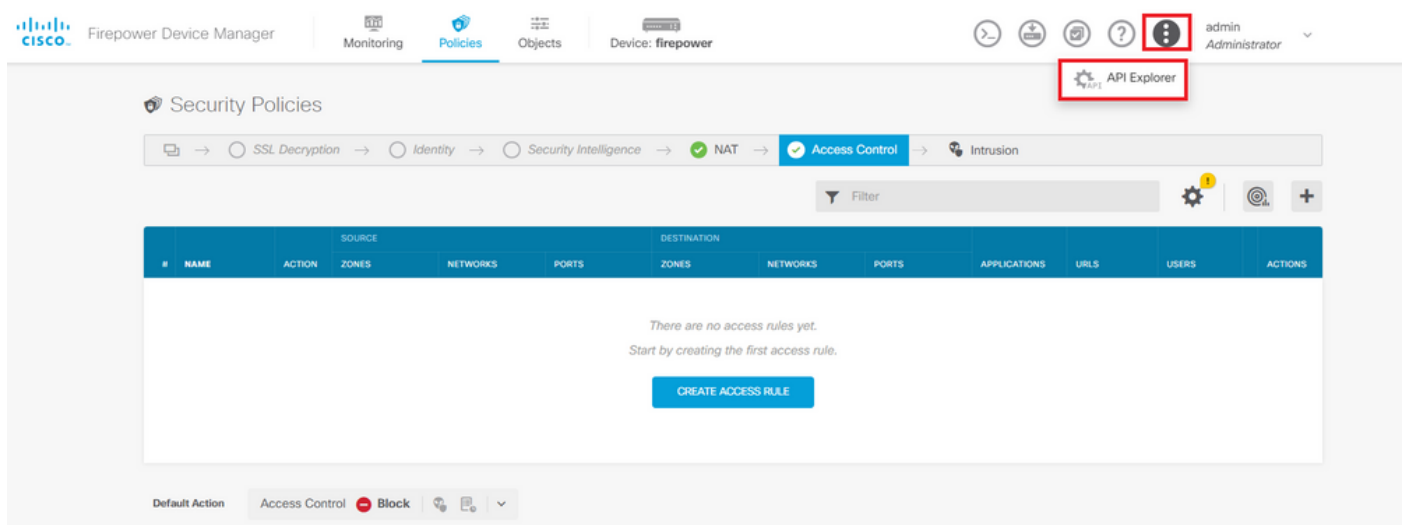
FTD APIバージョン6.6.0以降では、時間に基づいて制限されるアクセスコントロールルールがサ

ポートされています。

FTD APIを使用すると、一時間または反復する期間を指定する時間範囲オブジェクトを作成し、これらのオブジェクトをアクセス制御ルールに適用できます。時間範囲を使用すると、1日の特定の時間または特定の期間のトラフィックにアクセスコントロールルールを適用して、ネットワークの使用に柔軟性を提供できます。時間範囲の作成または適用にFDMを使用することはできません。また、アクセス制御ルールに時間範囲が適用されているかどうかはFDMに表示されません。

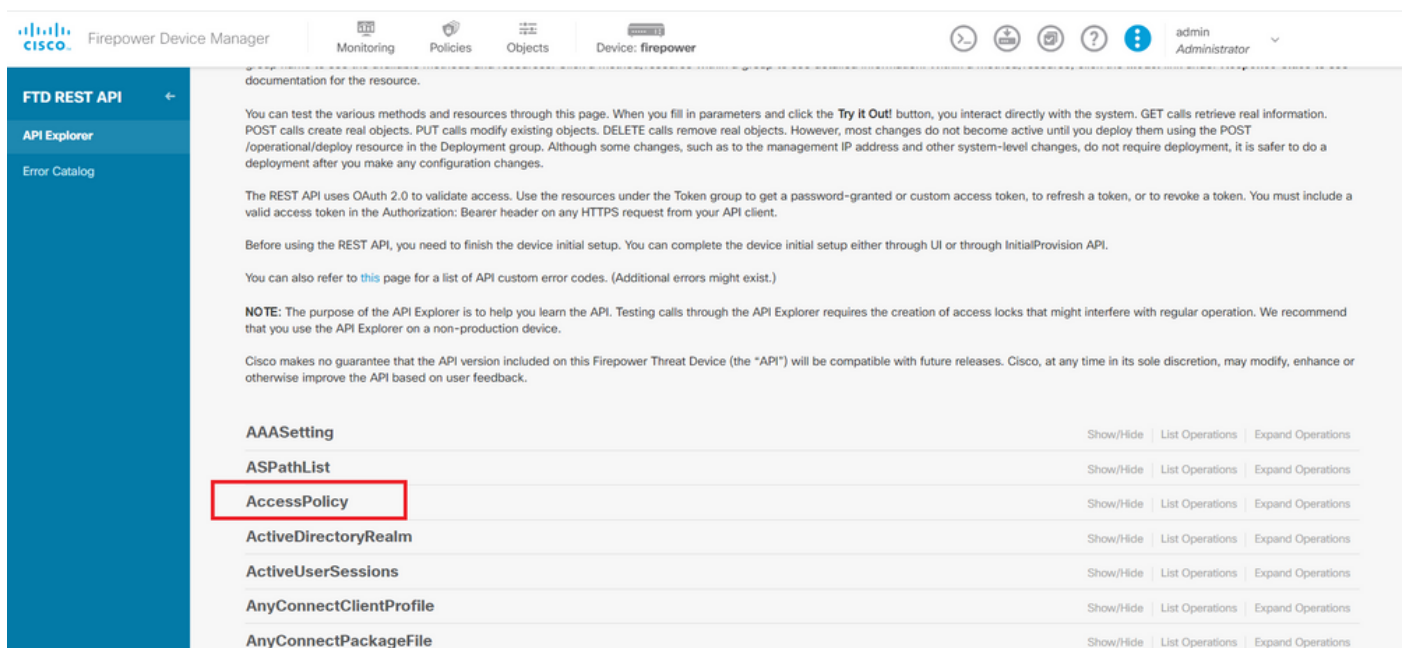
## 設定

ステップ 1：詳細オプション ( Kebabメニュー ) をクリックして、FDM APIエクスプローラを開きます。



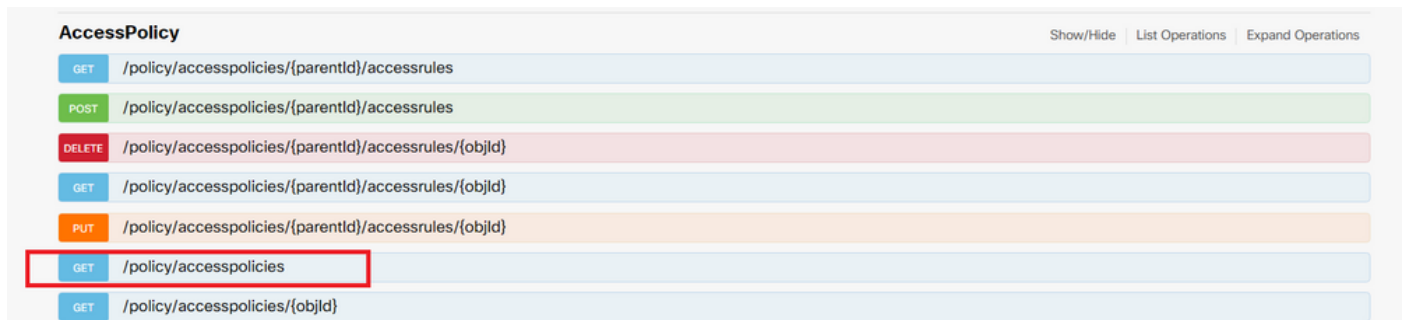
画像 1.FDM Webユーザー・ インタフエース。

ステップ 2：異なるAPIコールAccessPolicyを表示するには、カテゴリを選択します。



画像 2.API Explorer Webユーザインターフェイス。

ステップ 3 : コールを実行してGET、アクセスポリシーIDを取得します。



画像 3.アクセスポリシーカテゴリ。

ステップ 4 : API応答を取得TRY IT OUT!するには、を押す必要があります。

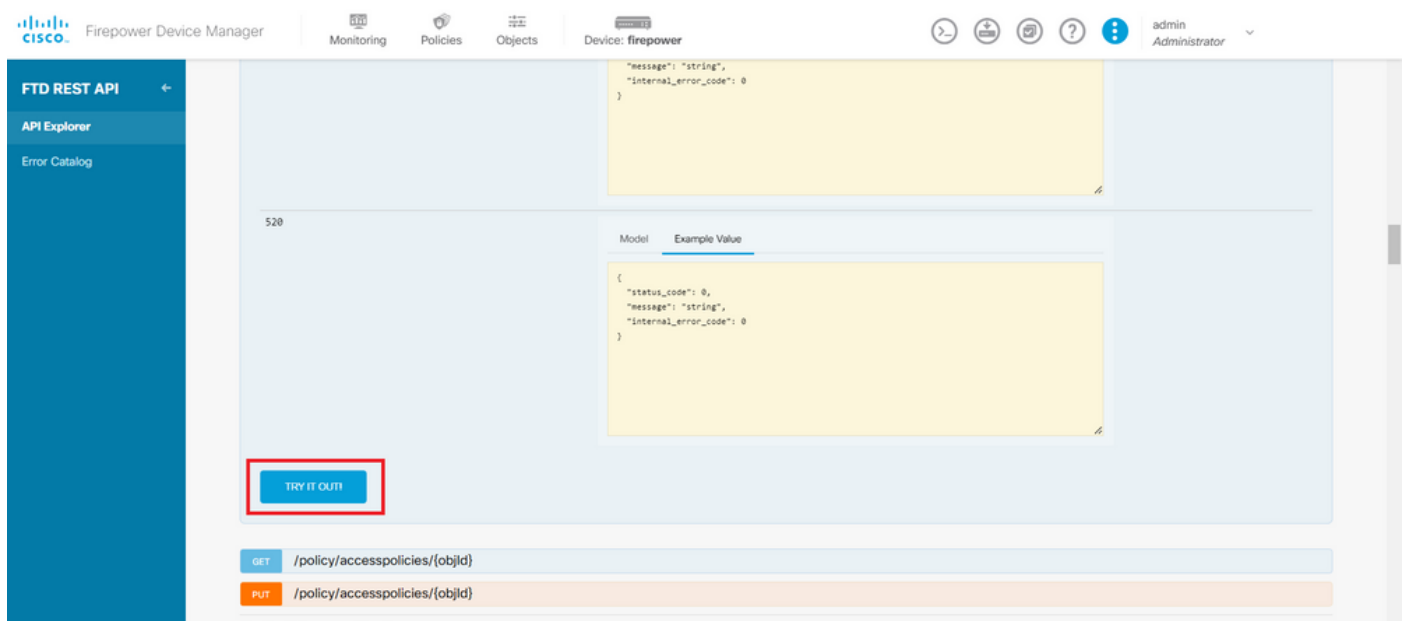


図 4.TRY IT OUT ! ボタンを押すと、API呼び出しが実行されます。

ステップ 5 : 応答本文のJSONデータをメモ帳にコピーします。後で、アクセスコントロールポリシーIDを使用する必要があります。

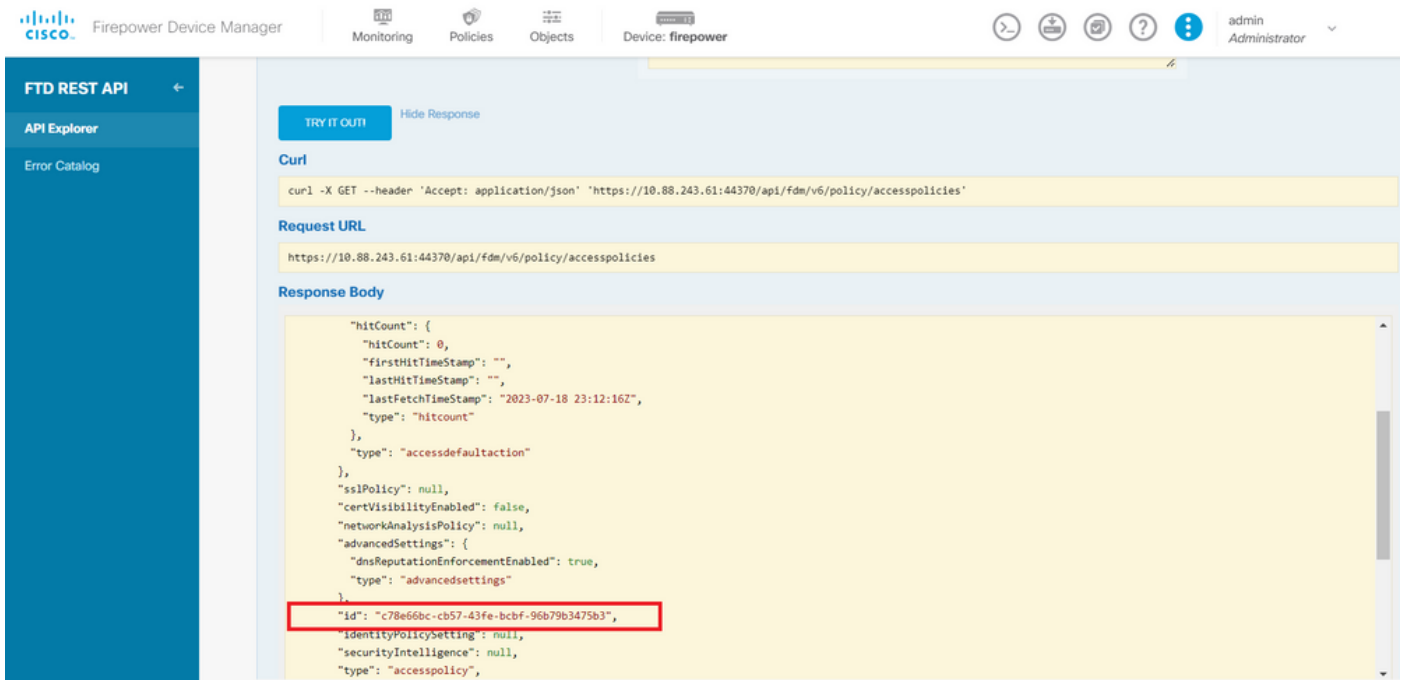


図 5. アクセスポリシーから応答を取得します。

手順 6 : さまざまなAPIコールを表示するには、API ExplorerでTimeRangeカテゴリを検索して開きます。

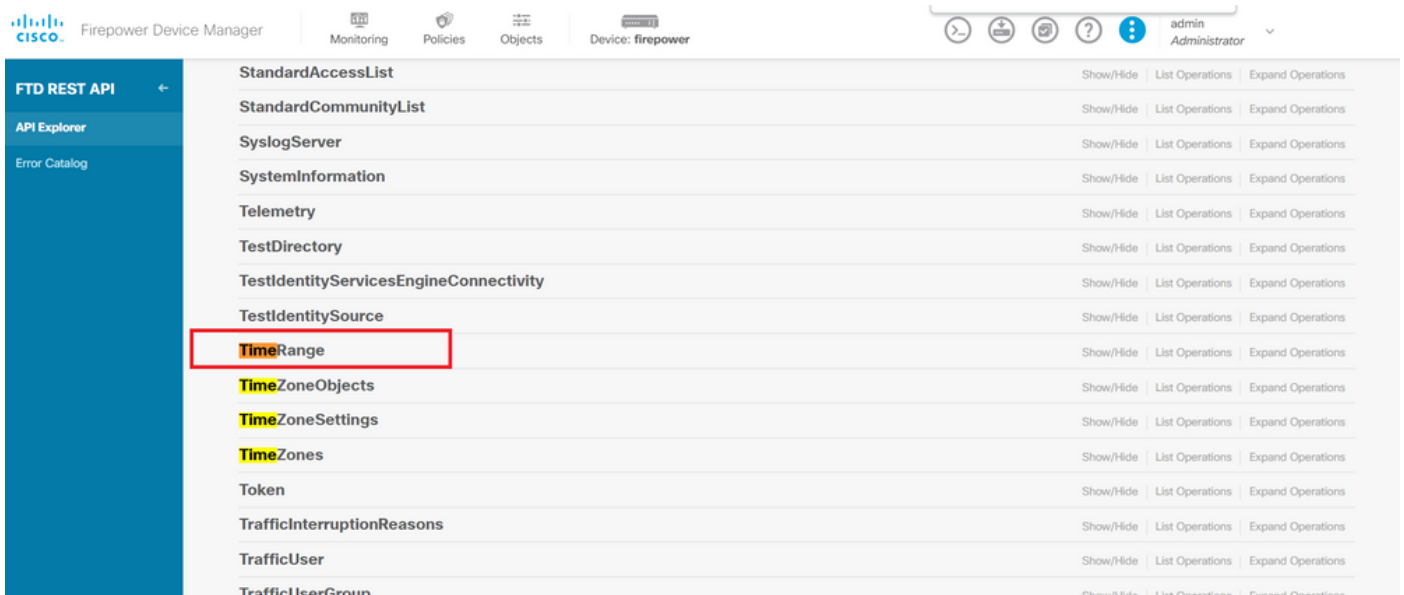


図 6. 時間範囲カテゴリ。

手順 7 : POST APIコールを使用して、必要な数のTimeRangeオブジェクトを作成します。

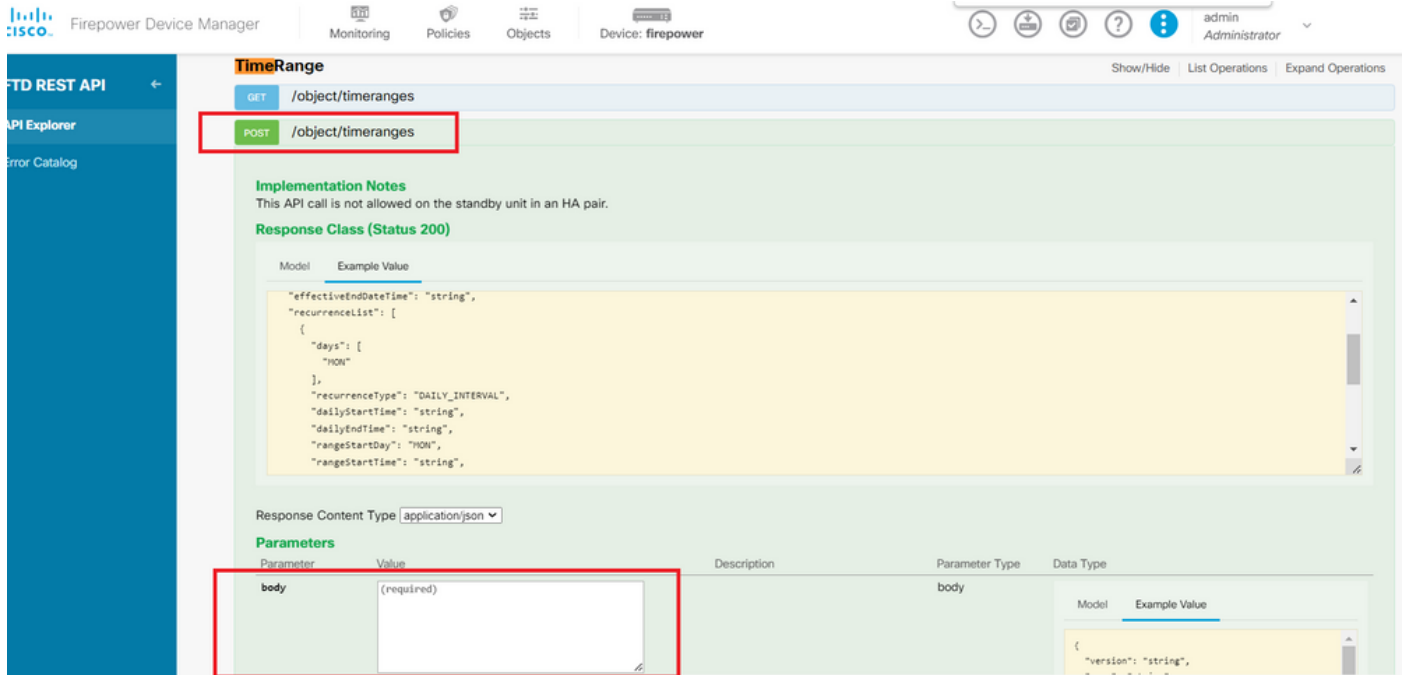


図 7.時間範囲POSTコール。

ここでは、2つの異なるTimeRangeオブジェクトを作成するJSON形式の例をいくつか紹介します。

オブジェクト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"
```

```
}
```

オブジェクト2:

```
<#root>
```

```
{
```

```
  "name": "
```

```
range-obj-2
```

```
",
```

```
  "recurrenceList": [
```

```
    {
```

```
      "days": [
```

```
        "MON"
```

```
      ],
```

```
      "recurrenceType": "DAILY_INTERVAL",
```

```
      "dailyStartTime": "
```

```
12:00
```

```
",
```

```
      "dailyEndTime": "
```

```
13:00
```

```
",
```

```
      "type": "recurrence"
```

```
    }
```

```
  ],
```

```
  "type": "timerangeobject",
```

```
}
```



注:APIコールを実行するには、必ずオンTRY IT OUT! にしてください。

---

ステップ 8 : コールを実行してGET、TimeRangeオブジェクトIDを取得します。

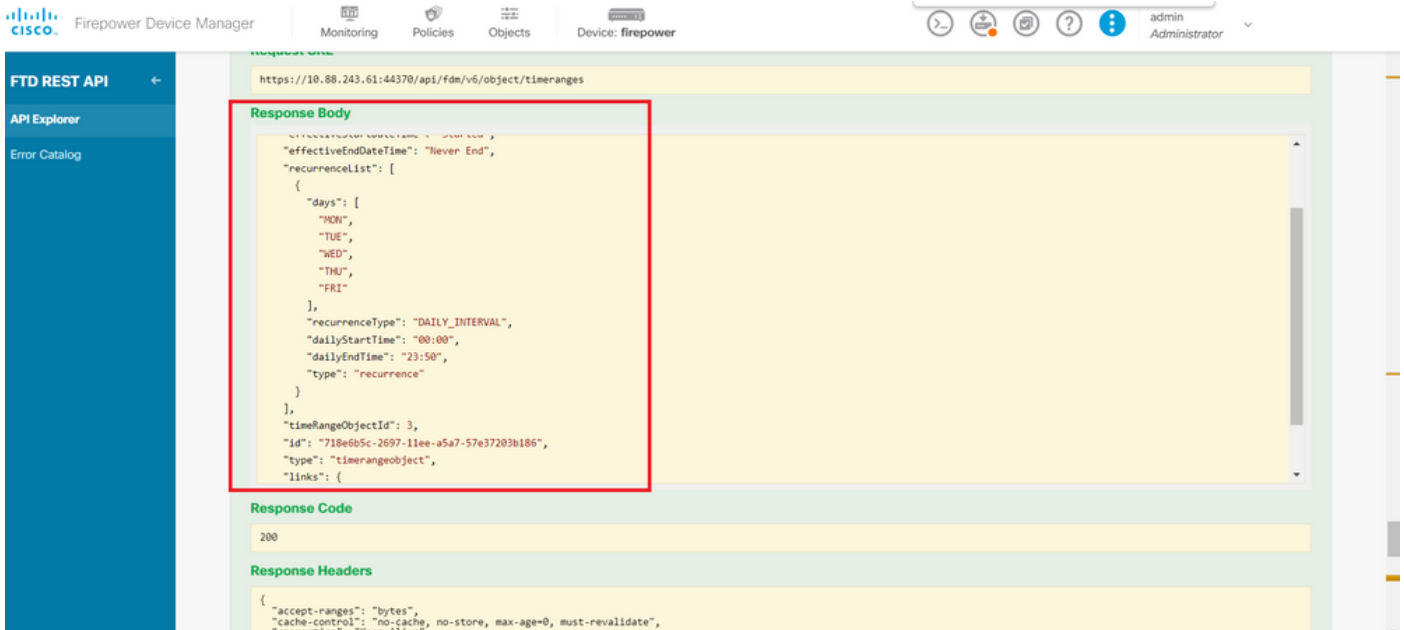


図 8.時間範囲から応答を取得します。

ステップ 9 : ボタンをクリックしDeploy、変更を検証して適用します。

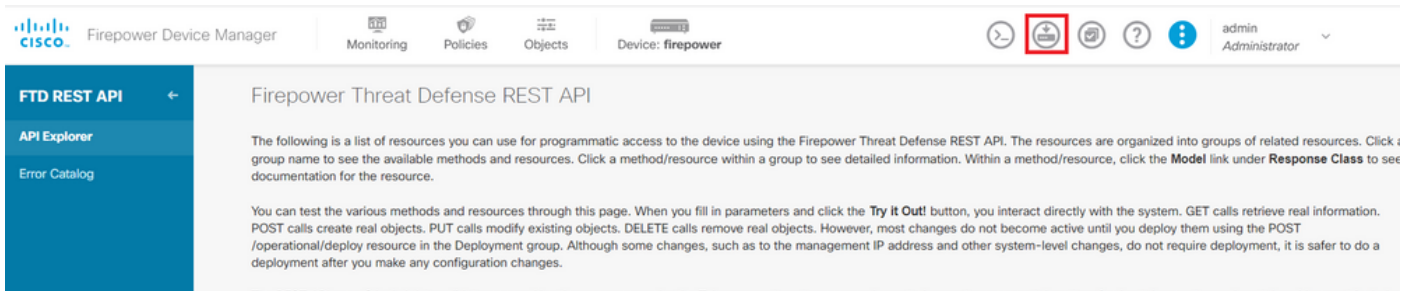


図 9. 「配備」 ボタンはAPIエクスプローラから使用できます。

ステップ 10 : 作成した設定を検証し、 **DEPLOY NOW**.

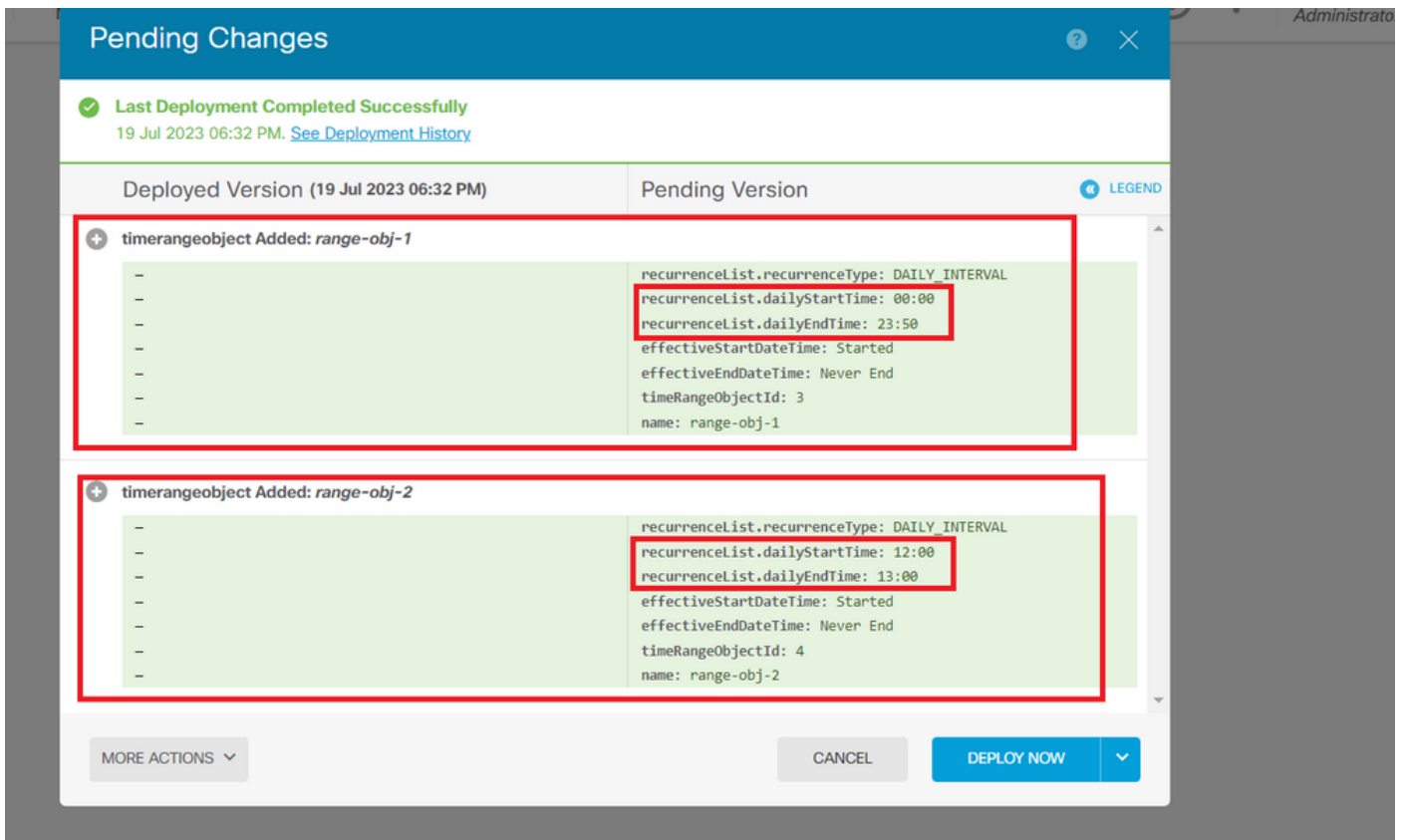


図 10.FDMの「保留中の変更」ウィンドウ

ステップ 11カテゴリを検索しAccessPolicy、POSTコールを開いて、時間ベースのアクセスコントロールルールを作成します。

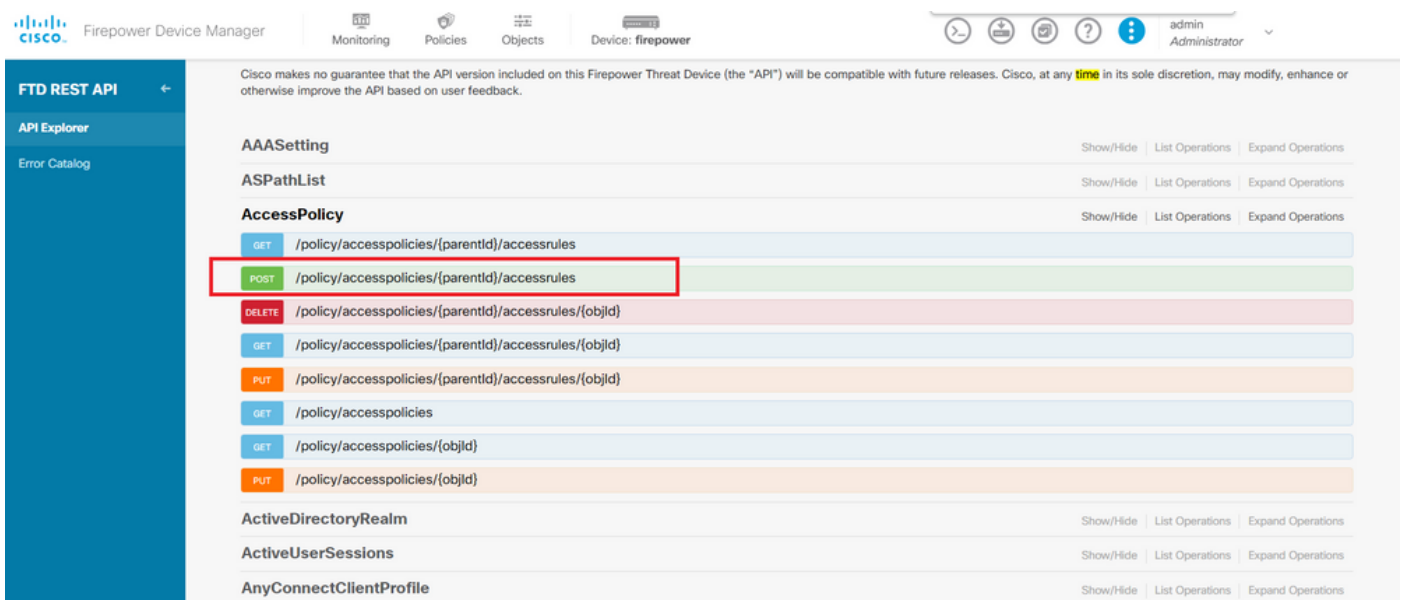


図 11.アクセスポリシーPOSTコール。

内部ゾーンから外部ゾーンへのトラフィックを許可する時間ベースACLを作成するJSONフォーマット例を次に示します。

正しい時間範囲オブジェクトIDを使用していることを確認します。




```

<#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:**eventLogAction フローの最後でイベントを記録するLOG\_FLOW\_ENDには、このコマンドを使用する必要があります。そうでない場合はエラーが発生します。

---

ステップ 12 新しい時間ベースのACLを適用するために変更を展開します。Pending Changesプロンプトに、ステップ10で使用した時間範囲オブジェクトを表示する必要があります。

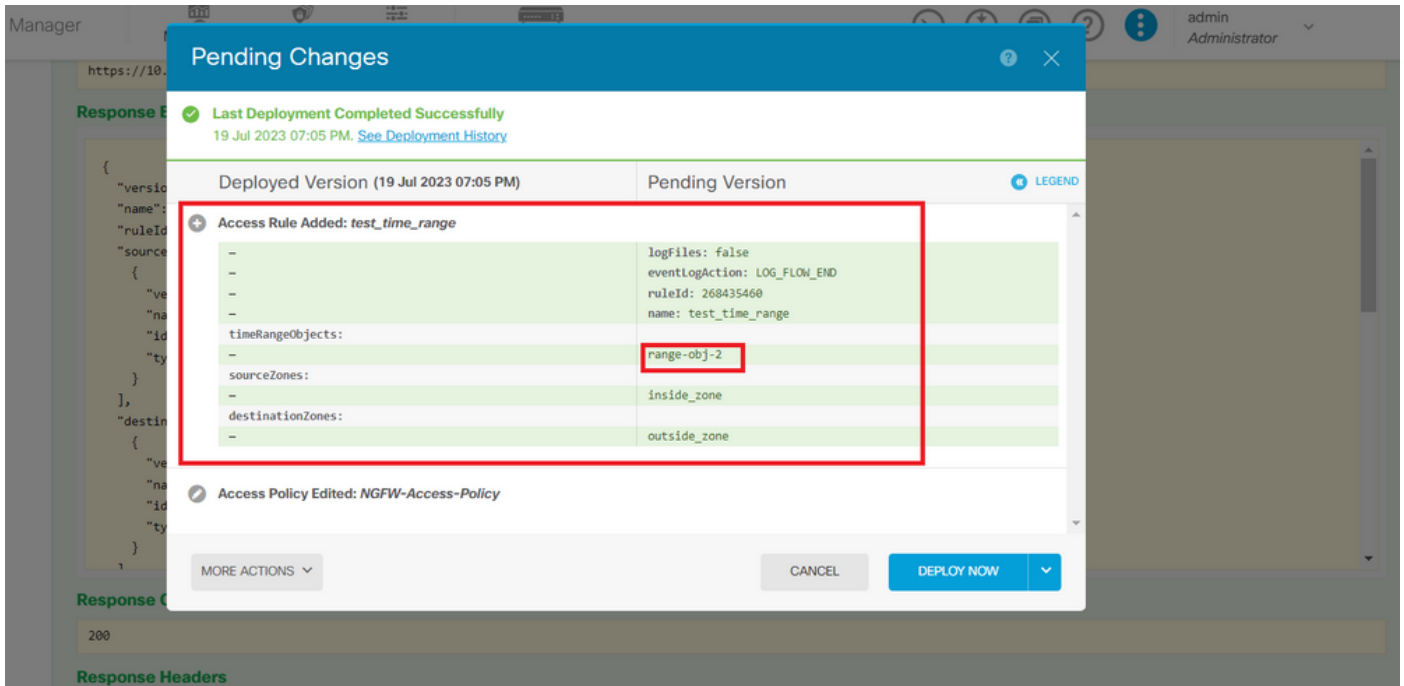


図 12.FDMの「保留中の変更」ウィンドウに新しいルールが表示されます。

ステップ 13 ( オプション ) : ACLを編集する場合は、コールを使用してPUT、時間範囲IDを編集できます。

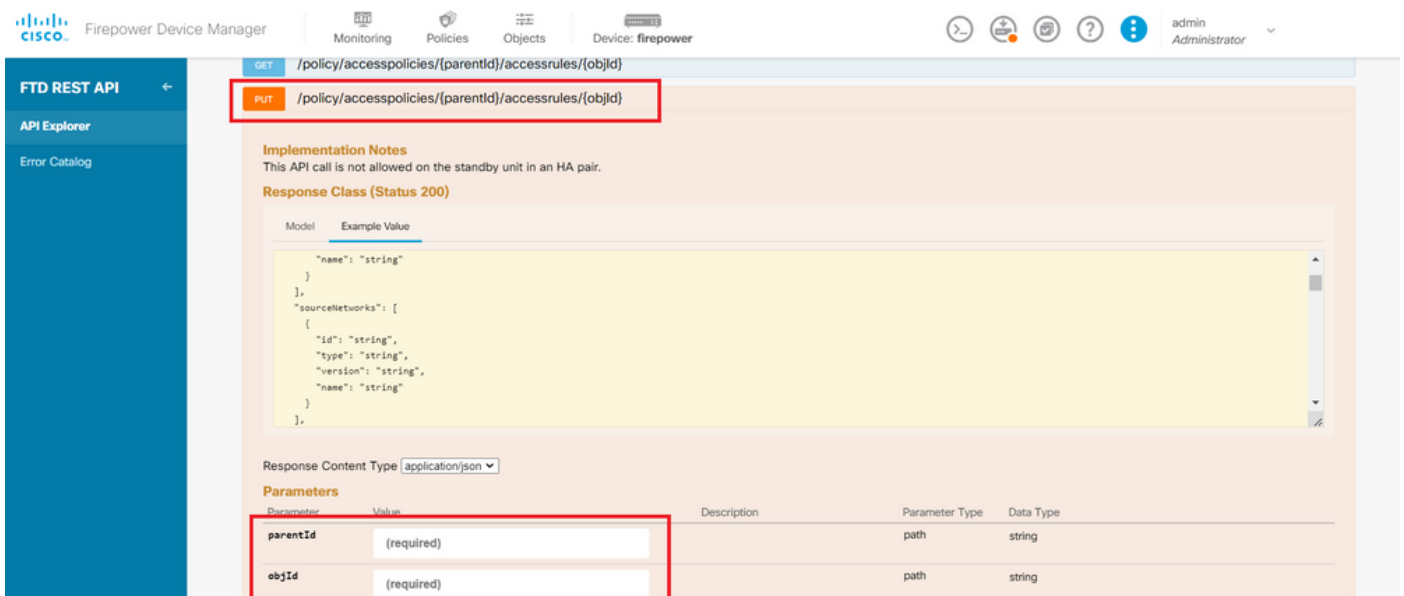


図 13.アクセスポリシーPUTコール。

時間範囲を編集するためにJSON、フォーマットの例を見つけてください。これらの時間範囲IDはGET、コールを使用して収集できます。

<#root>

```
{
  "version": "f1ya3jw7wvqg7",
  "name": "test_time_range",
  "ruleId": 268435460,
  "sourceZones": [
```

```

{
  "version": "1ypkhscmq4bq",
  "name": "inside_zone",
  "id": "90c377e0-b3e5-11e5-8db8-651556da7898",
  "type": "securityzone"
},
{
  "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"
}

```

ステップ 14 : 変更を導入して検証します。

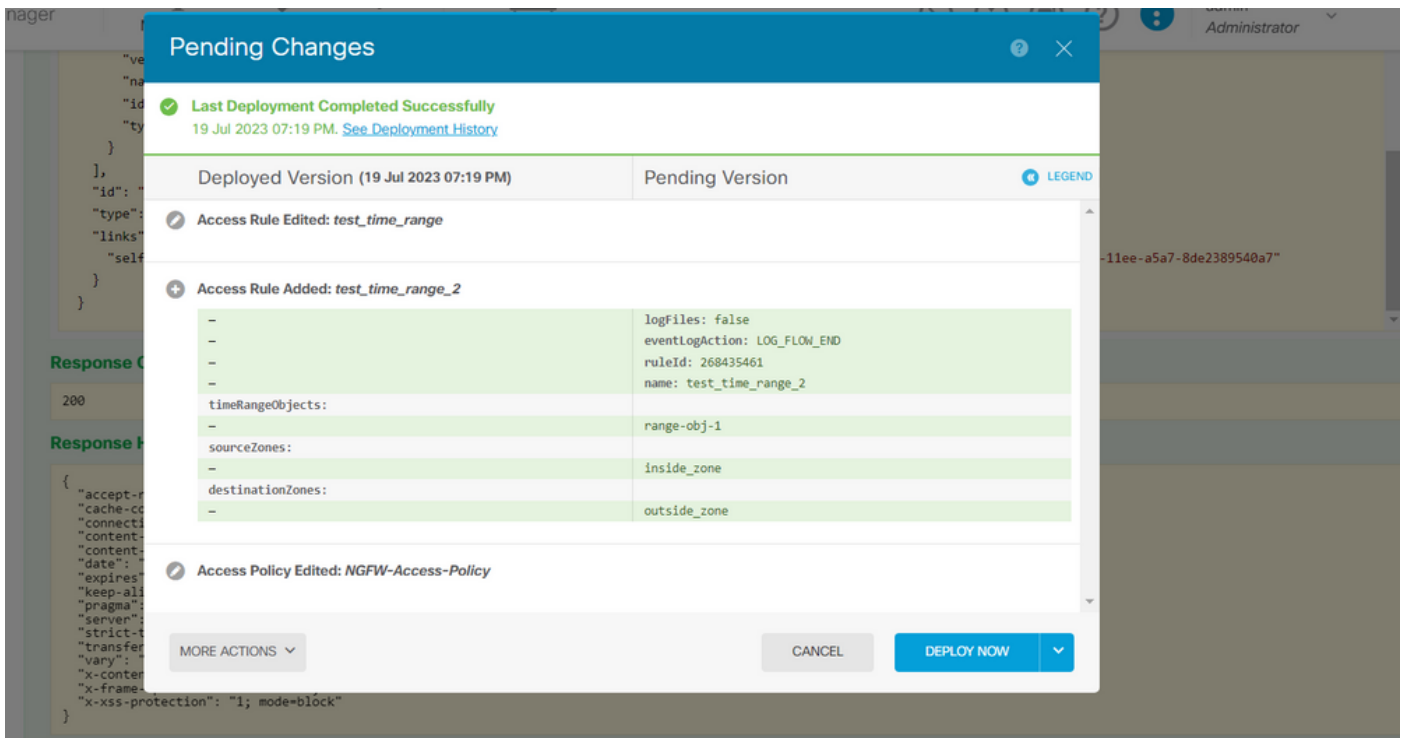


図 14.FDMの「保留中の変更」ウィンドウに、オブジェクトの変更が表示されます。

## 確認

1.コマンドを実行してshow time-range、時間範囲オブジェクトのステータスを検証します。

```
<#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.コマンドを使用してshow access-control-config、アクセスコントロールルールの設定を検証します。

<#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.System Support Trace debugを実行して、トラフィックが正しいルールに一致していることを確認します。

<#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 change

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 0

10.10.10.3 62360 -> Destination IP 443 6 AS=0 ID=3 GR=1-1 Verdict:

pass

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。