REST API를 사용하여 FDM에서 시간 기반 액세스 제어 규칙 구성

목차

소개

이 문서에서는 FDM에서 Rest API를 사용하여 관리하는 FTD에서 시간 기반 액세스 제어 규칙을 구성하고 검증하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(보안 방화벽 위협 방어)
- Firepower 장치 관리(FDM)
- REST API(Representational State Transfer Application Programming Interface)에 대한 지식
- ACL(Access Control List)

사용되는 구성 요소

이 문서의 정보는 FTD 버전 7.1.0을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

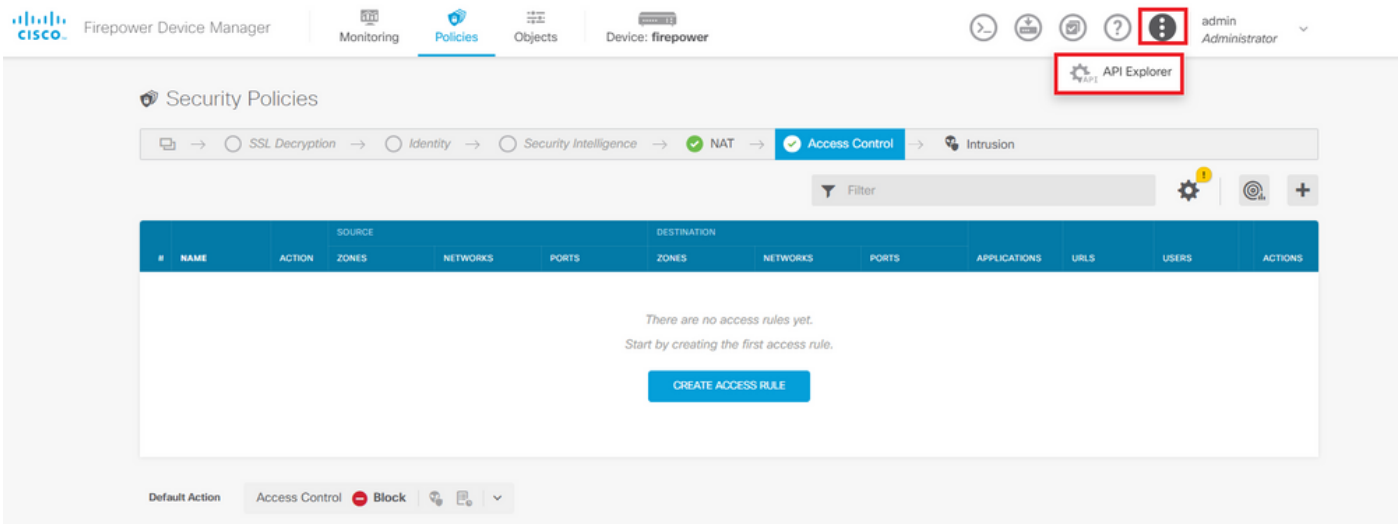
FTD API 버전 6.6.0 이상에서는 시간에 따라 제한되는 액세스 제어 규칙을 지원합니다.

FTD API를 사용하여 1회 또는 반복 시간 범위를 지정하는 시간 범위 객체를 생성하고 이러한 객체를 액세스 제어 규칙에 적용할 수 있습니다. 시간 범위를 사용하면 특정 시간 동안 또는 특정 시간

동안 트래픽에 액세스 제어 규칙을 적용하여 네트워크 사용에 유연성을 제공할 수 있습니다. FDM을 사용하여 시간 범위를 생성하거나 적용할 수 없으며, 액세스 제어 규칙에 시간 범위가 적용되는지 여부도 FDM에 표시되지 않습니다.

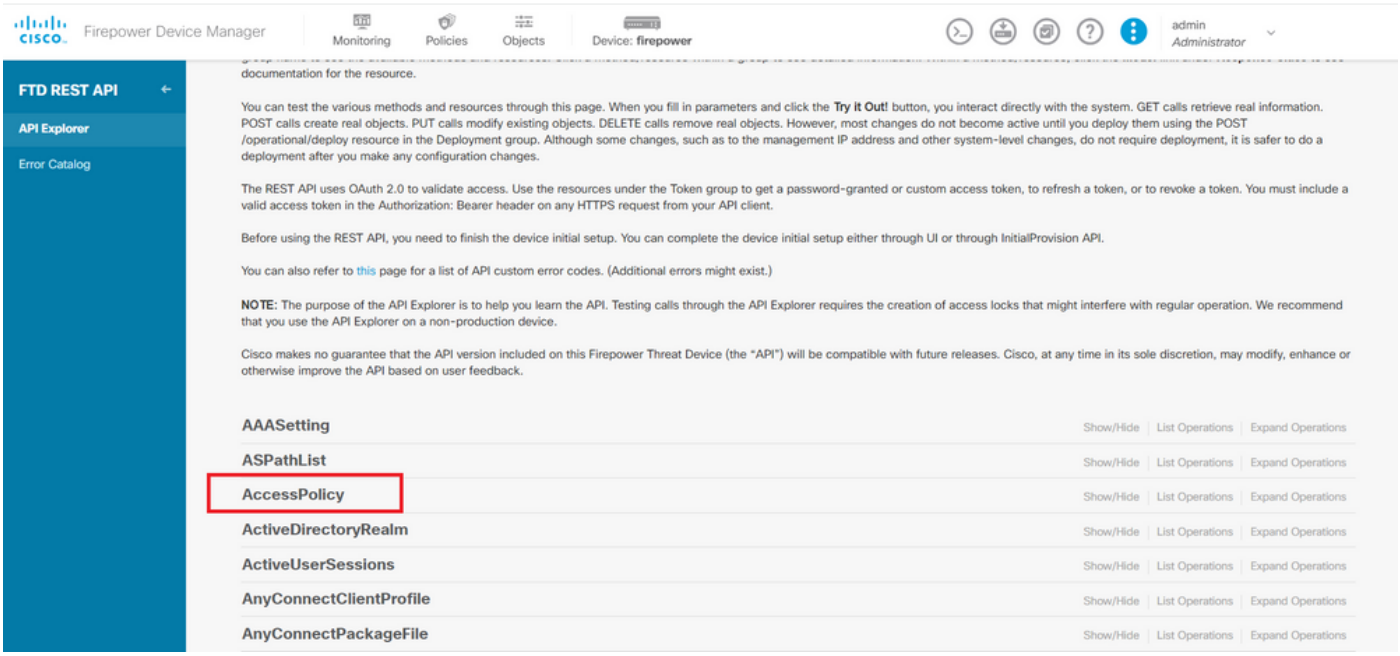
구성

1단계. FDM API 탐색기를 열려면 고급 옵션(Kebab 메뉴)을 클릭합니다.



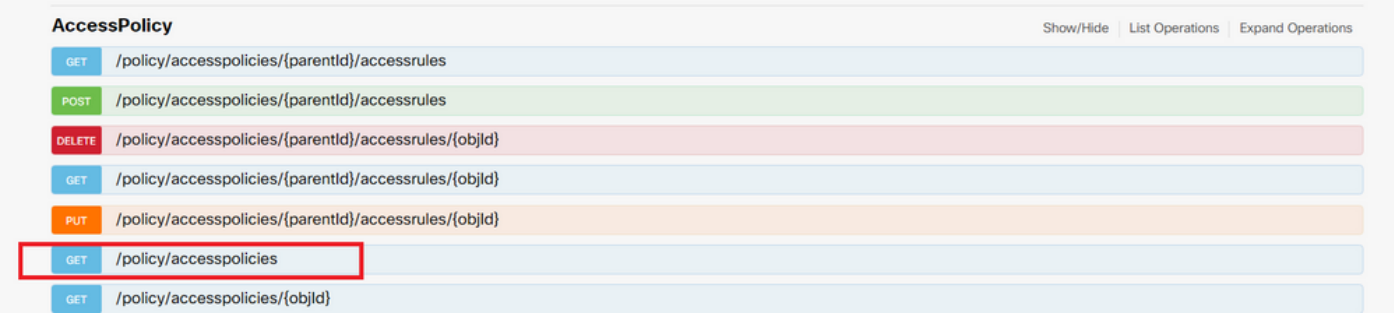
이미지 1. FDM 웹 사용자 인터페이스.

2단계. 다른 API 호출**AccessPolicy**을 표시하려면 범주를 선택합니다.



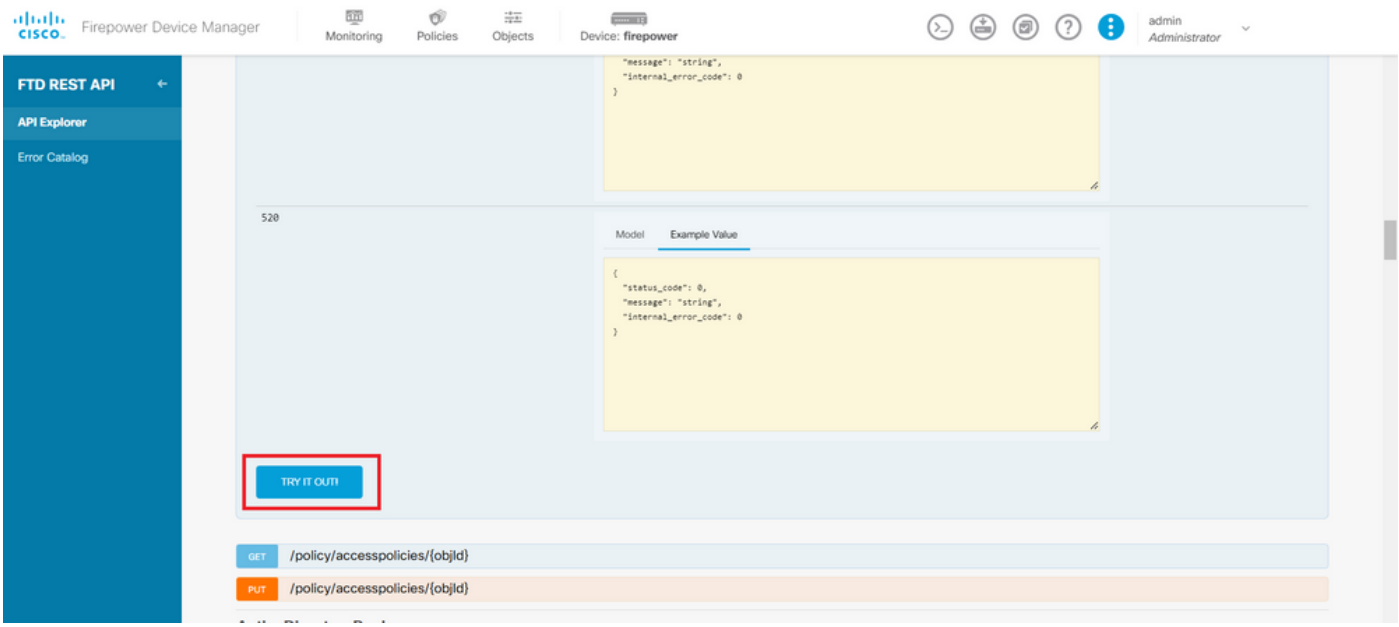
이미지 2. API Explorer 웹 사용자 인터페이스.

3단계. 액세스 정책 **GET** ID를 얻기 위해 통화를 실행합니다.



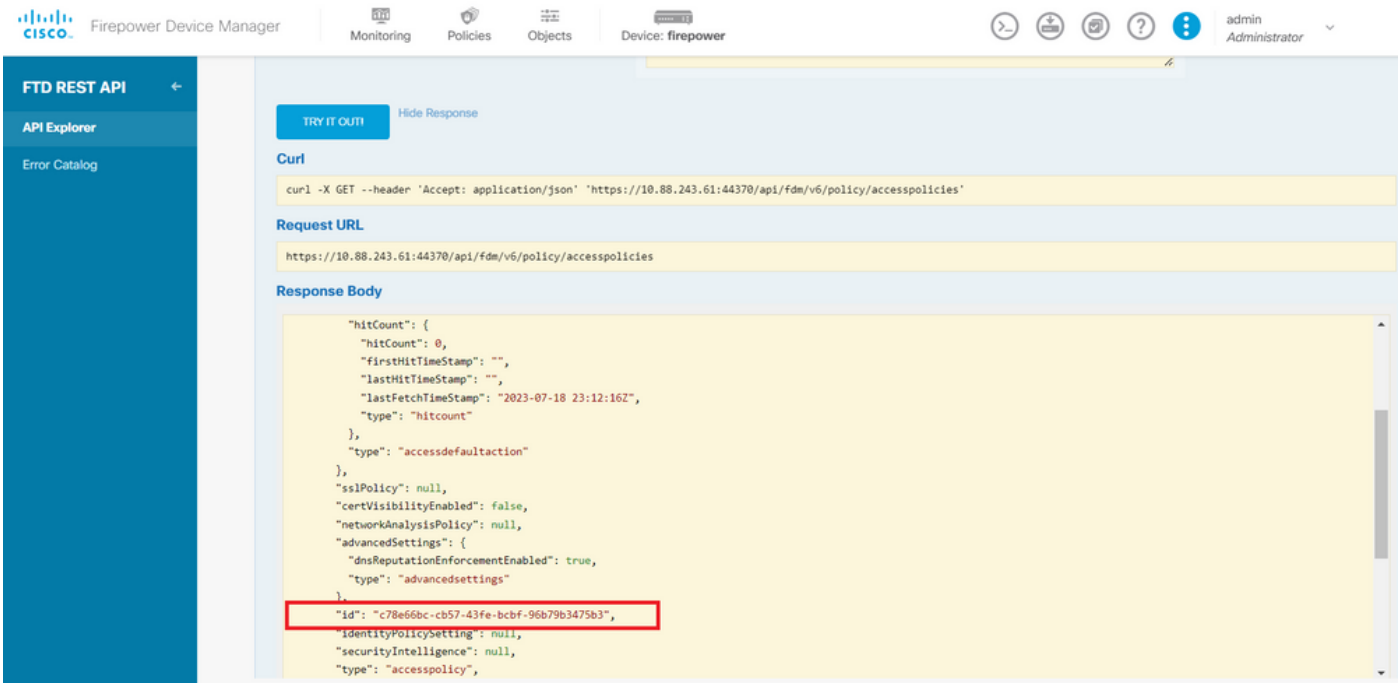
이미지 3. 액세스 정책 카테고리.

4단계. API 응답TRY IT OUT!을 검색하려면 키를 눌러야 합니다.



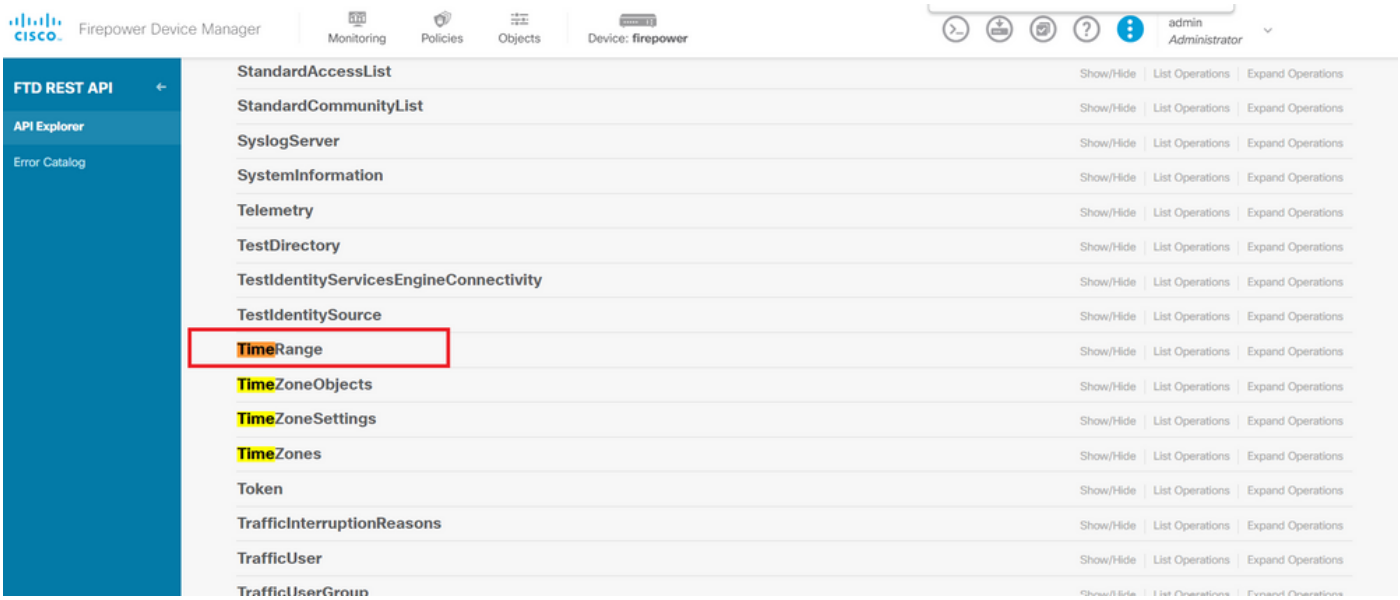
이미지 4. API 호출을 실행하는 TRY IT OUT! 버튼을 클릭합니다.

5단계. 응답 본문의 JSON 데이터를 메모장에 복사합니다. 나중에 액세스 제어 정책 ID를 사용해야 합니다.



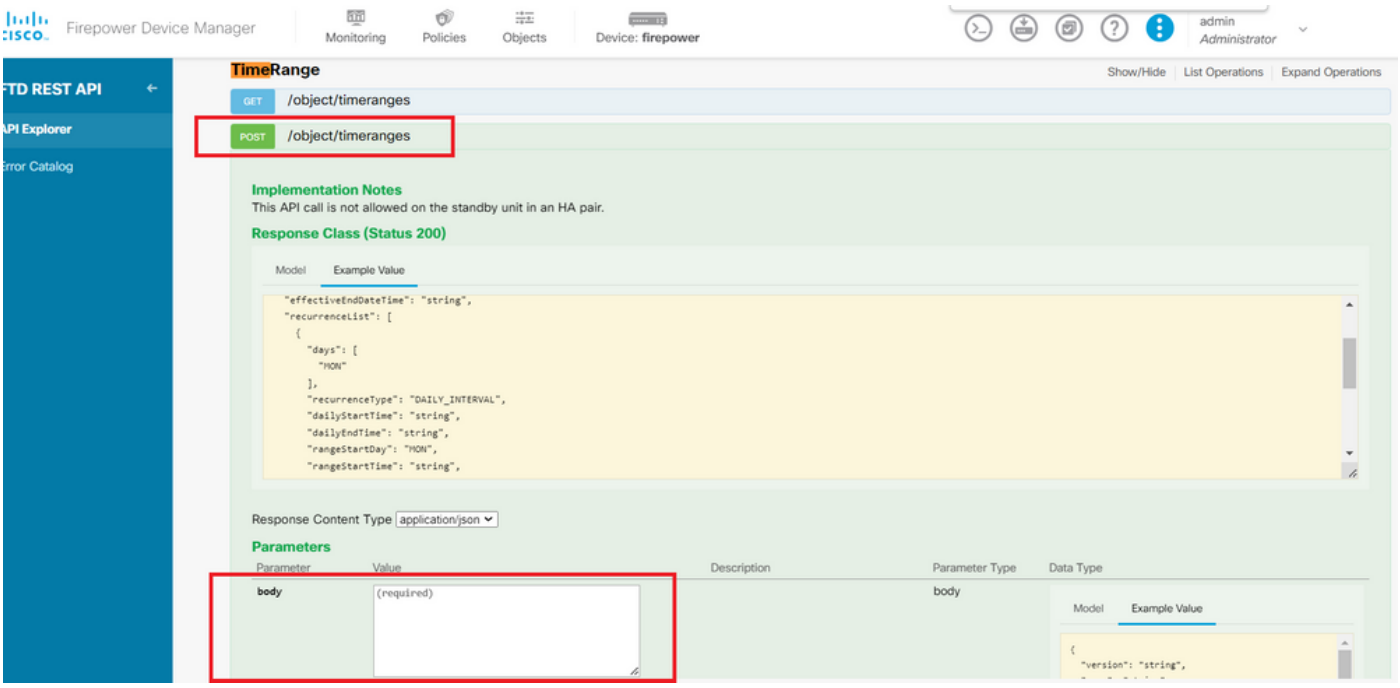
이미지 5. 액세스 정책에서 응답을 가져옵니다.

6단계. 다른 API 호출을 표시하기 위해 API 탐색기에서 TimeRange 범주를 찾아 엽니다.



이미지 6. 시간 범위 범주.

7단계. POST API 호출을 사용하여 원하는 만큼 TimeRange 개체를 만듭니다.



이미지 7. 시간 범위 POST 통화.

두 개의 서로 다른 TimeRange 개체를 만드는 몇 가지 JSON 형식 예제를 여기에서 찾을 수 있습니다.

개체 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"
```

```
}
```

개체 2:

<#root>

```
{

  "name": "
```

range-obj-2

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

12:00

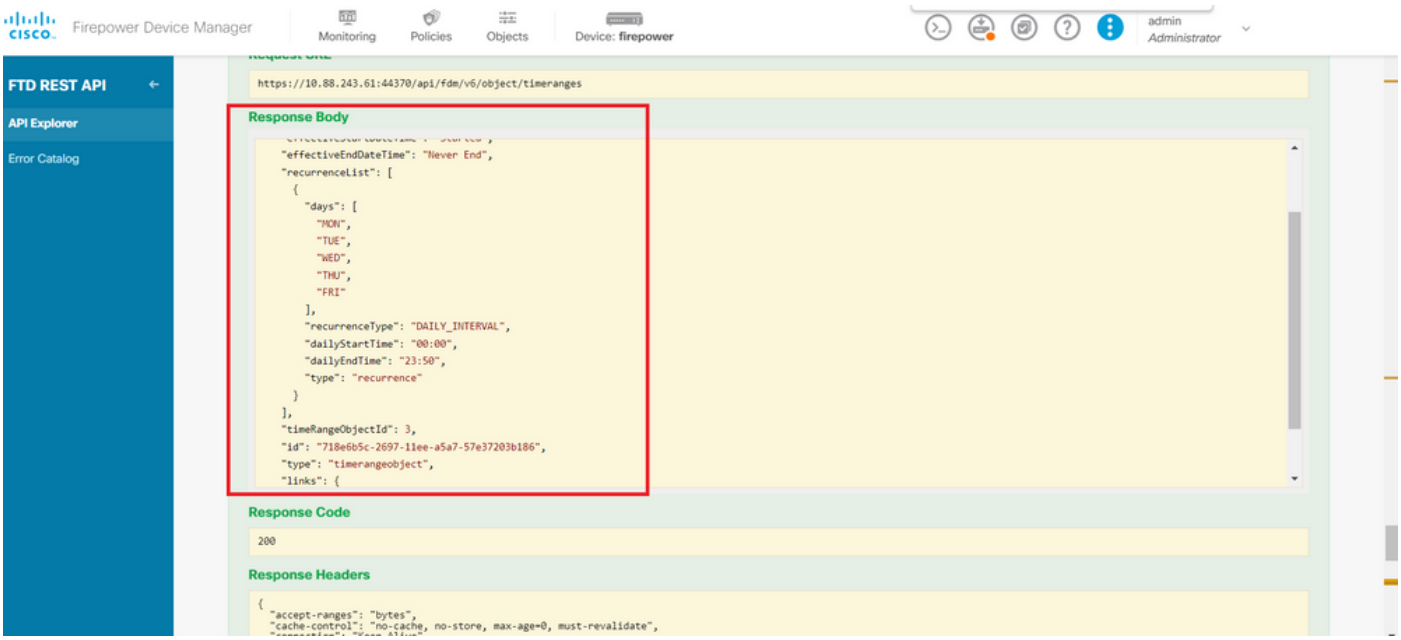
```
",
      "dailyEndTime": "
```

13:00

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

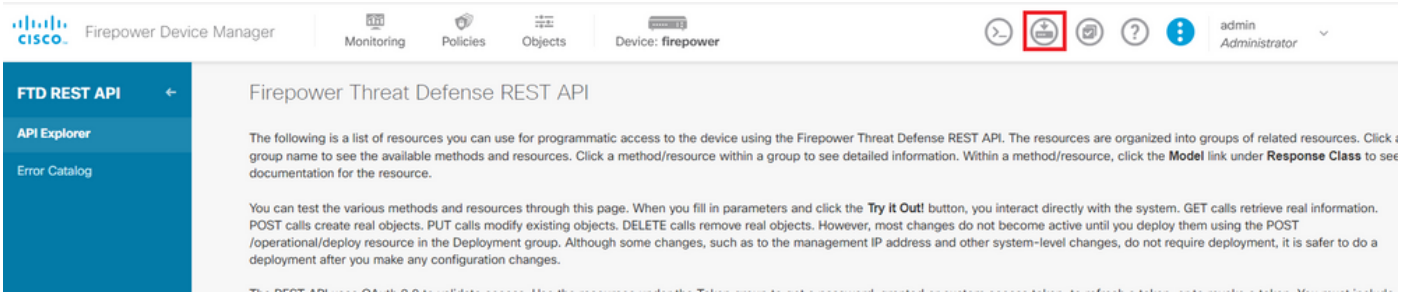
참고: API 호출을 실행하기 **TRY IT OUT!** 위해서는 키를 눌러야 합니다.

8단계. 호출을GET 실행하여 TimeRange 개체 ID를 가져옵니다.



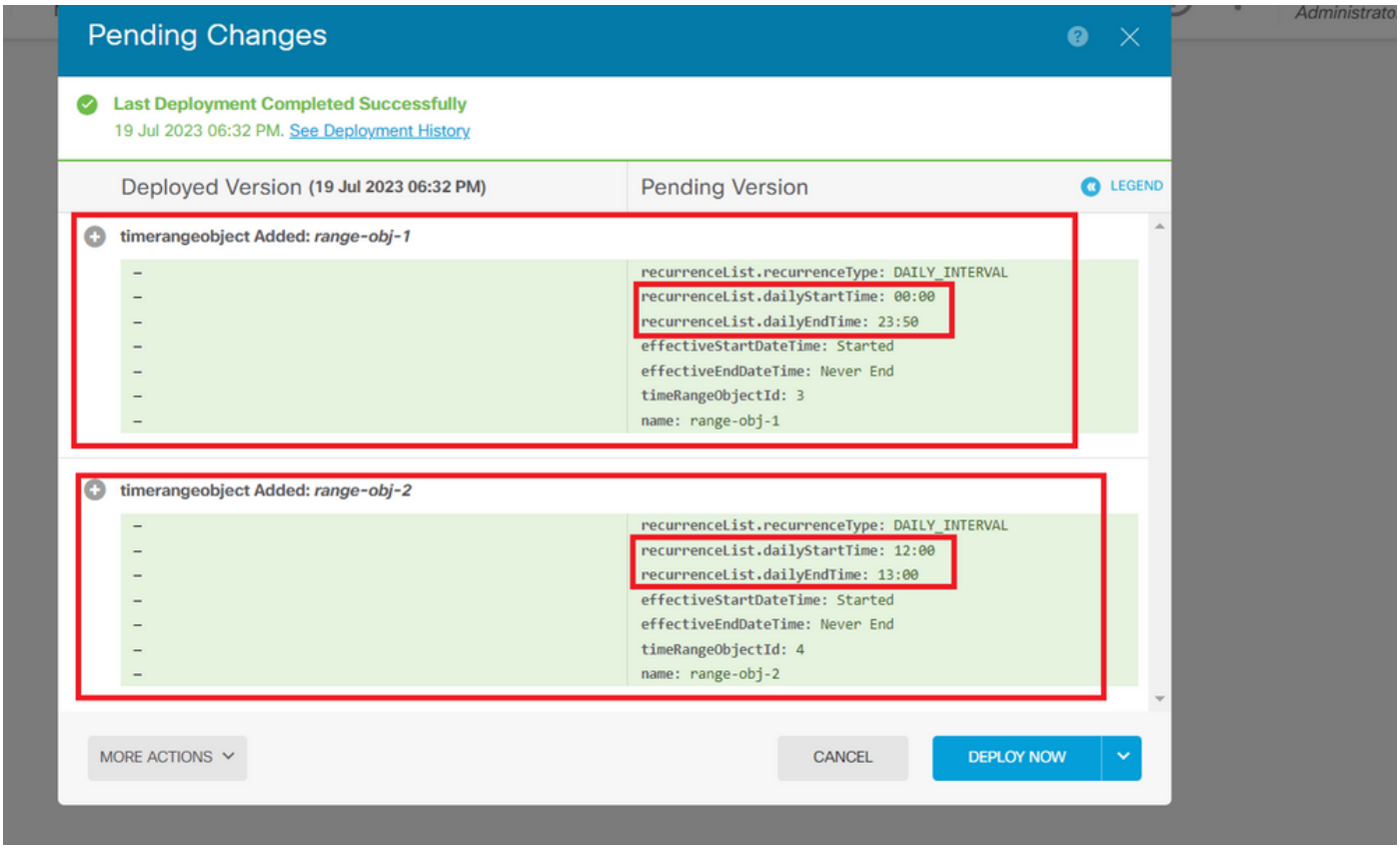
이미지 8. 시간 범위에서 응답을 가져옵니다.

9단계. 변경 사항을Deploy검증하고 적용하려면 버튼을 클릭합니다.



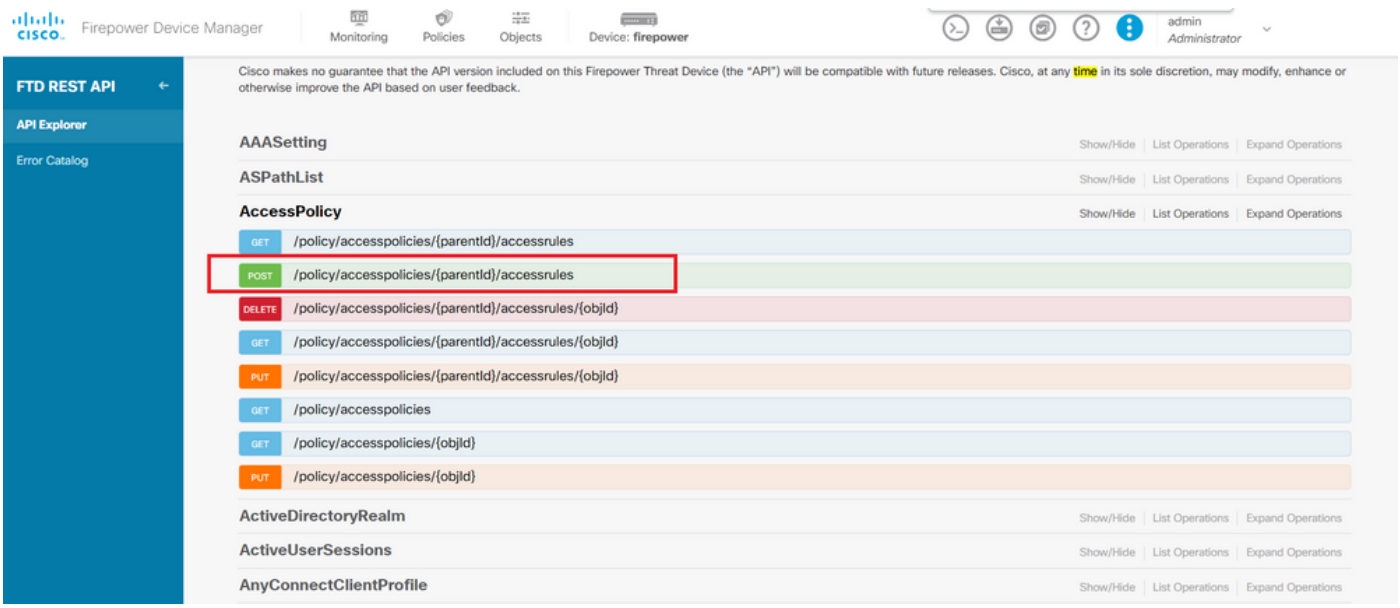
이미지 9. API 탐색기에서 사용 가능한 배포 단추

10단계. 방금 생성한 컨피그레이션을 확인하고 **DEPLOY NOW**.



이미지 10. FDM 보류 중인 변경 사항 창

11단계. 시간 기반 액세스 제어 규칙을 생성하기 위해 AccessPolicy카테고리를 찾고 POST 호출을 엽니다.



이미지 11. 액세스 정책 POST 통화.

내부 영역에서 외부 영역으로 이동하는 트래픽을 허용하는 시간 기반 ACL을 생성하는 JSON 형식 예를 여기에서 찾을 수 있습니다.

올바른 시간 범위 개체 ID를 사용해야 합니다.

<#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

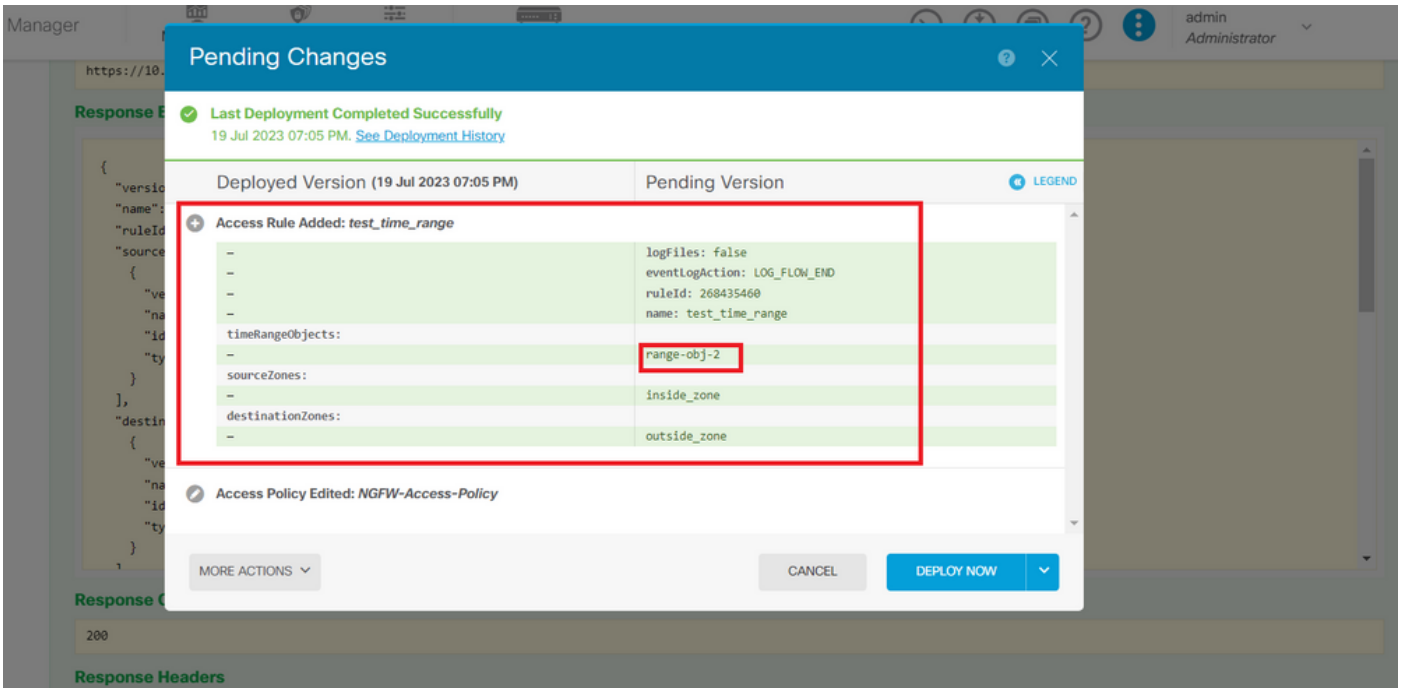
```
",
  "timeRangeObjects": [
    {
    "id": "
```

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

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

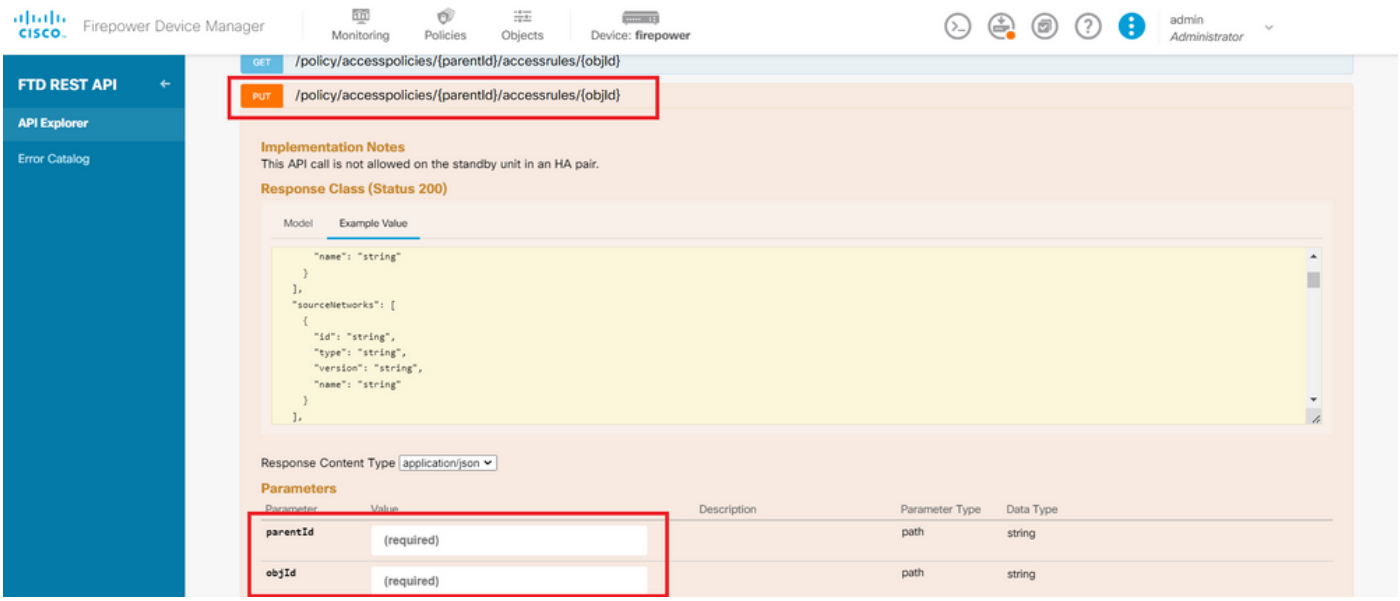
참고: eventLogAction 흐름**LOG_FlOW_END**이 끝날 때 이벤트를 기록하려면 이(가) 되어야 합니다. 그렇지 않으면 오류가 발생합니다.

12단계. 새 시간 기반 ACL을 적용하기 위해 변경 사항을 구축합니다. Pending Changes 프롬프트는 10단계에서 사용된 시간 범위 객체를 표시해야 합니다.



이미지 12. FDM 보류 중인 변경 사항 창에 새 규칙이 표시됩니다.

13단계(선택 사항) ACL을 수정하려면 통화를 사용하고 시간 범위 ID를PUT수정할 수 있습니다.



이미지 13. 액세스 정책 PUT 호출

시간 범위를 JSON 수정하려면 통화를 사용하여 이러한 시간 범위 ID를 수집할 수 있는 형식 예를 여기에서GET 확인하십시오.

<#root>

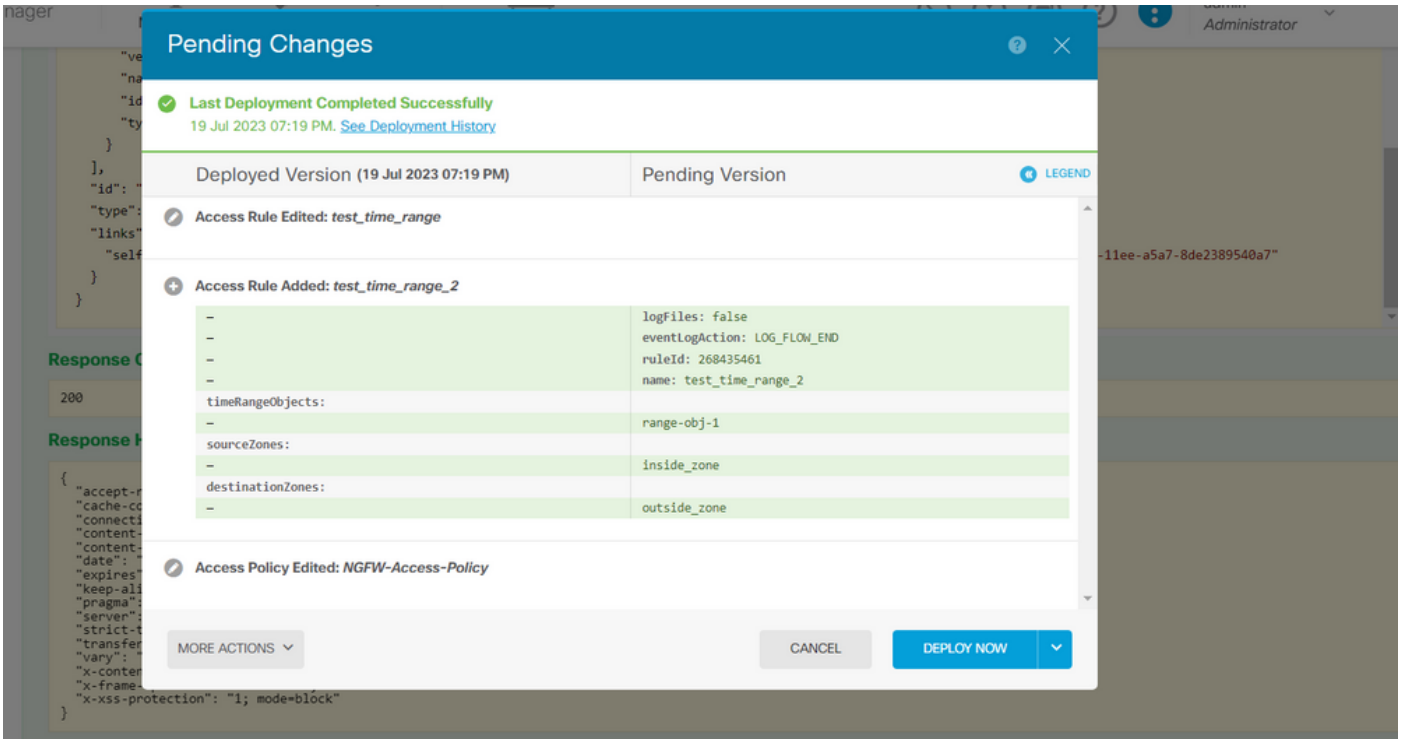
```
{
"version": "flya3jw7wvqg7",
"name": "test_time_range",
"ruleId": 268435460,
"sourceZones": [
{
```

```
"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"
}
```


14단계. 변경 내용을 배포하고 검증합니다.



이미지 14. [FDM 보류 중인 변경 사항] 창에는 객체의 변경 사항이 표시됩니다.

다음을 확인합니다.

1.show time-range시간 범위 객체의 상태를 검증하려면 명령을 실행합니다.

```
<#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.show access-control-config액세스 제어 규칙 컨피그레이션을 검증하려면 명령을 사용합니다.

<#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. 트래픽이System Support Trace올바른 규칙에 도달하고 있는지 확인하기 위해 디버그를 실행합니다.

<#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
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.