Configurare una regola di controllo dell'accesso a tempo in FDM con API Rest

Sommario

Introduzione

In questo documento viene descritto come configurare e convalidare una regola di controllo dell'accesso a tempo sull'FTD gestito da FDM con API Rest.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Secure Firewall Threat Defense (FTD)
- FDM (Firepower Device Management)
- Conoscenza dell'API REST (Representative State Transfer Application Programming Interface)
- Access Control List (ACL)

Componenti usati

Le informazioni di questo documento si basano sulla versione 7.1.0 di FTD.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'API FTD versione 6.6.0 e successive supporta regole di controllo dell'accesso limitate in base al

tempo.

Utilizzando l'API FTD, è possibile creare oggetti intervallo di tempo, che specificano intervalli di tempo singoli o ricorrenti, e applicarli alle regole di controllo d'accesso. Utilizzando gli intervalli di tempo, è possibile applicare una regola di controllo di accesso al traffico in determinati orari del giorno o in determinati periodi di tempo, al fine di garantire flessibilità nell'utilizzo della rete. Non è possibile utilizzare FDM per creare o applicare intervalli di tempo, né viene visualizzato se a una regola di controllo di accesso è stato applicato un intervallo di tempo.

Configurazione

Passaggio 1. Fare clic sulle opzioni avanzate (menu Kebab) per aprire Esplora API di FDM.

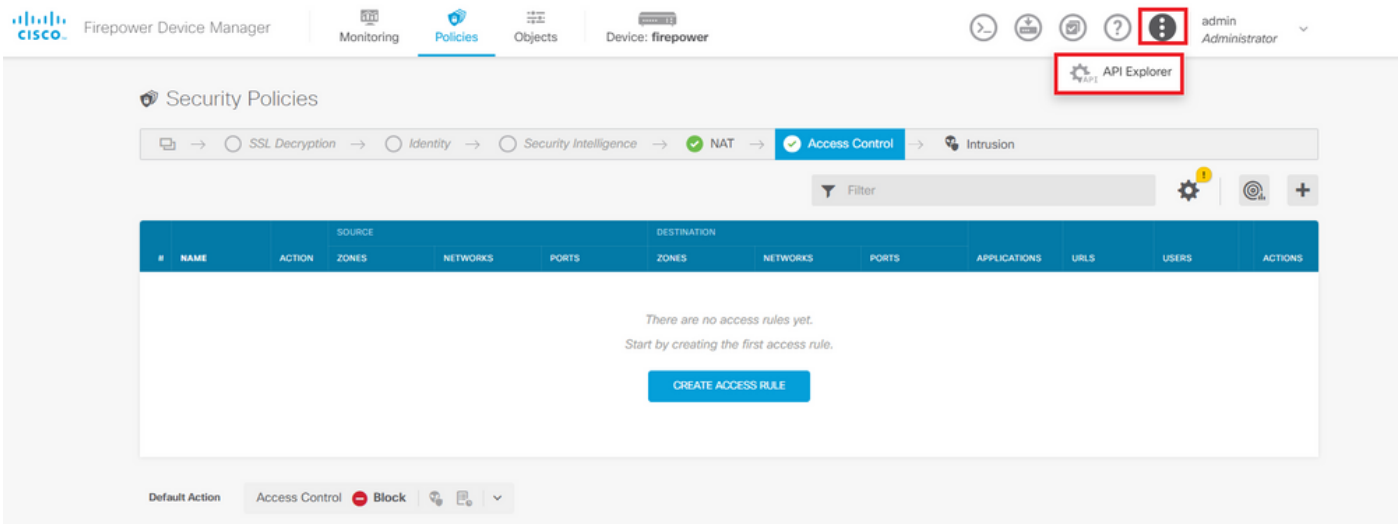

Immagine 1. Interfaccia utente Web di FDM.

Passaggio 2. Scegliere la categoria **AccessPolicy** per visualizzare le diverse chiamate API.

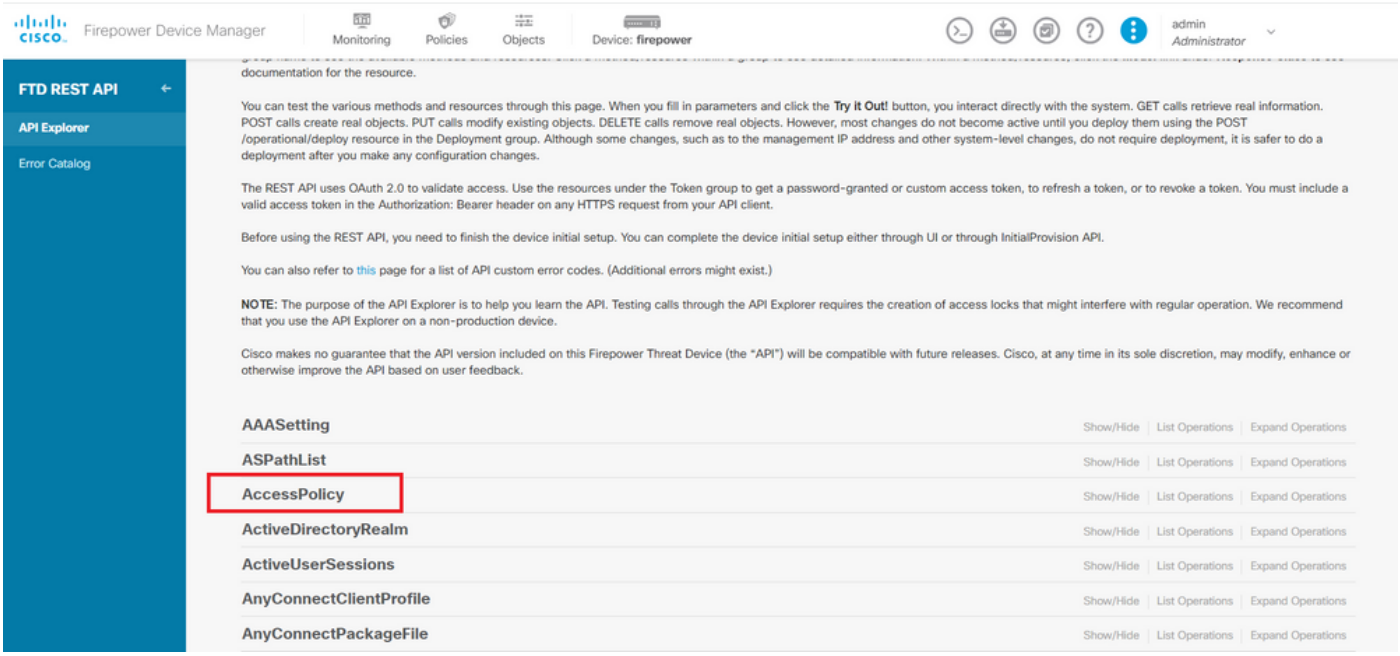

Immagine 2. Interfaccia utente Web di API Explorer.

Passaggio 3. Per ottenere l'ID dei criteri di accesso, eseguire la chiamata**GET**.

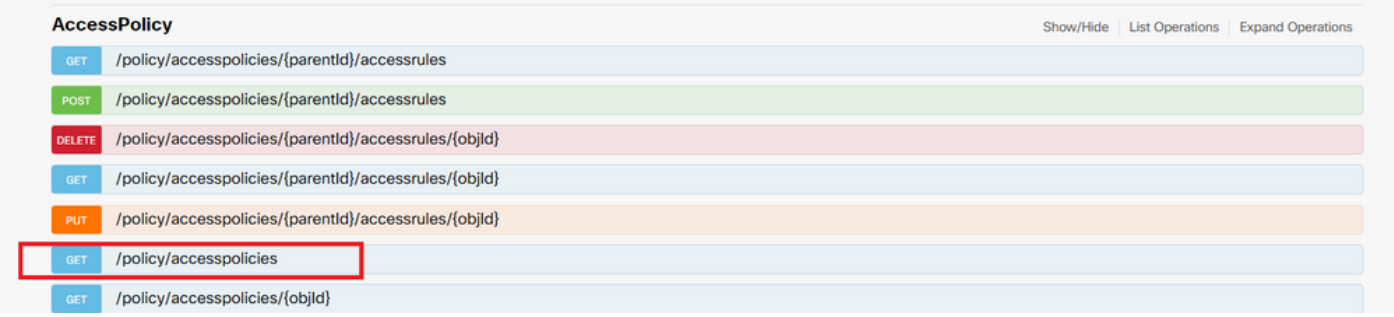

Immagine 3. Categoria Criteri di accesso.

Passaggio 4. Per recuperare la risposta**TRY IT OUT!**dell'API, è necessario premere.

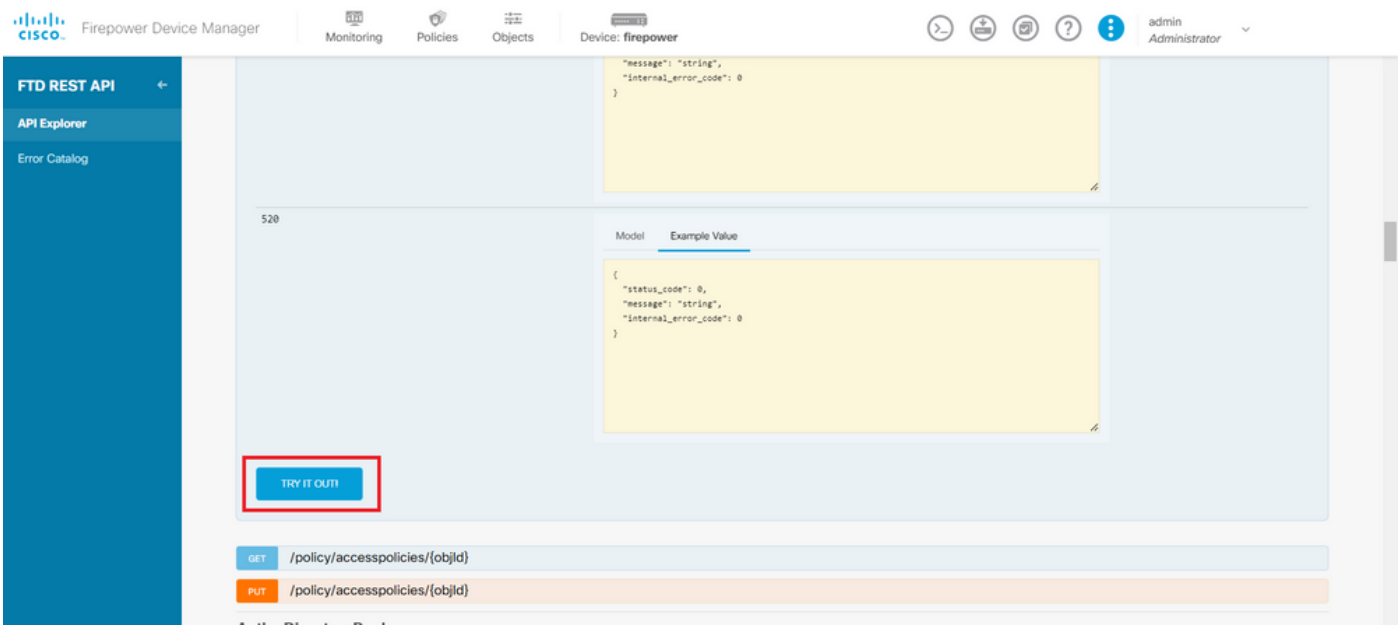

Immagine 4. Pulsante TRY IT OUT! che esegue la chiamata API.

Passaggio 5. Copiare i dati dal corpo della **JSON** risposta in un blocco note. In seguito, sarà necessario utilizzare l'ID dei criteri di controllo di accesso.

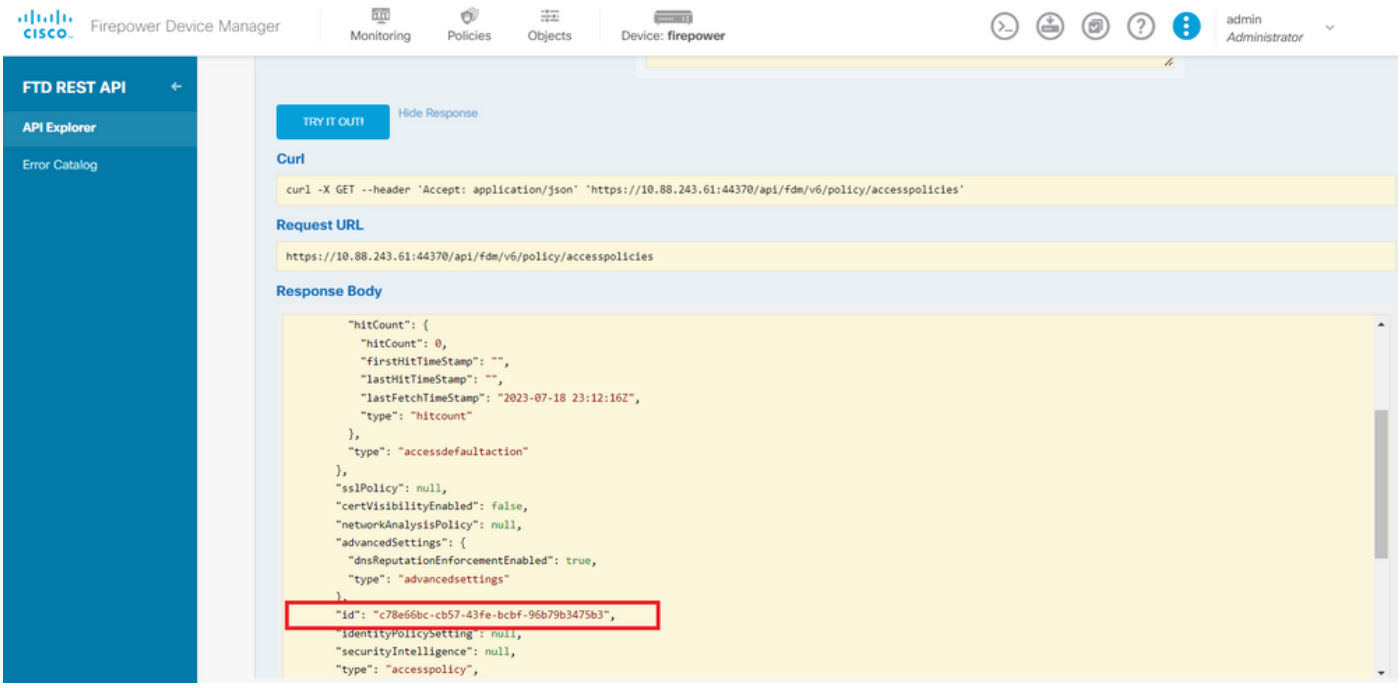

Immagine 5. Ottieni risposta dai criteri di accesso.

Passaggio 6. Individuare e aprire la categoria TimeRange in API Explorer per visualizzare le diverse chiamate API.

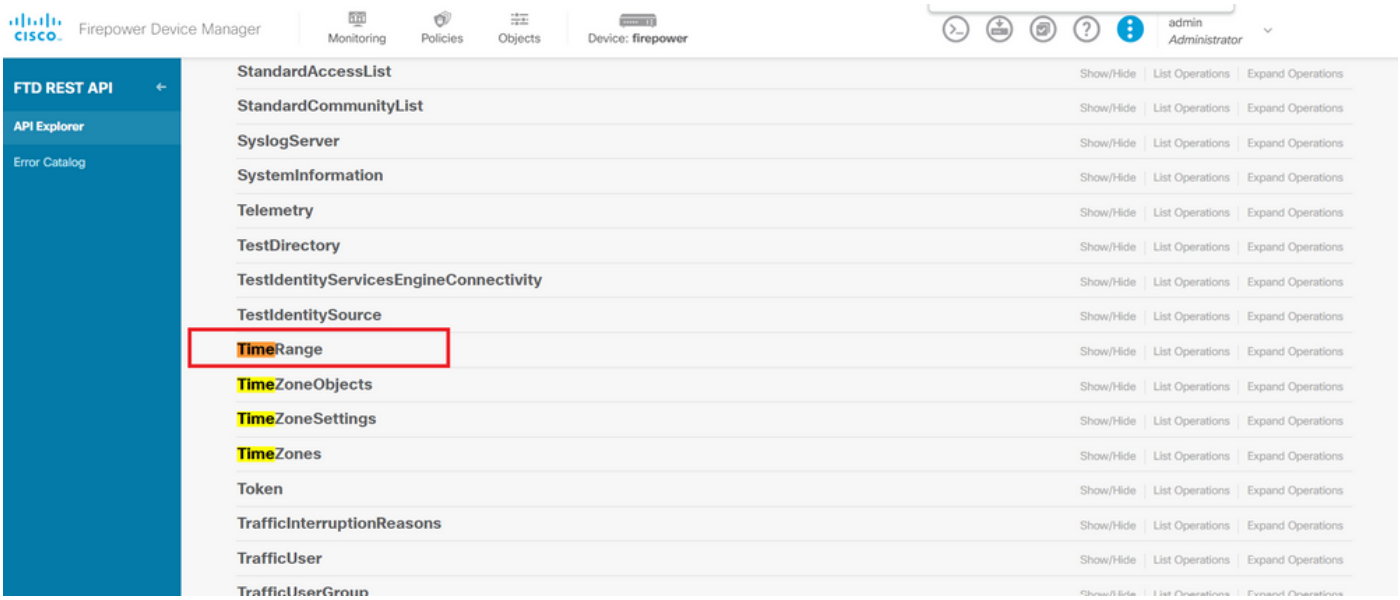

Immagine 6. Categoria Intervallo di tempo

Passaggio 7. Creare tutti gli oggetti TimeRange desiderati utilizzando la chiamata API POST.

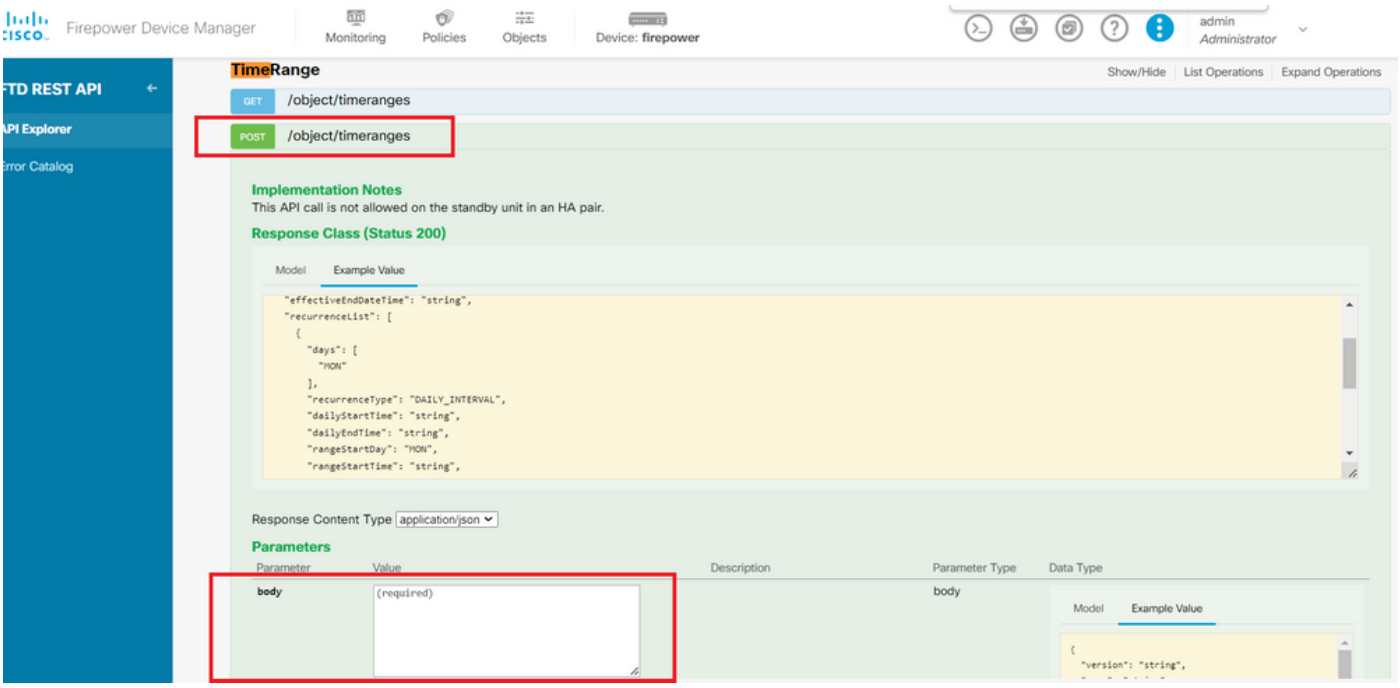

Immagine 7. Chiamata POST intervallo di tempo.

Di seguito sono riportati un paio di esempi di JSON formato per creare due diversi oggetti TimeRange.

Oggetto 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"
}
```

Oggetto 2:

<#root>

```
{

  "name": "

range-obj-2

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

12:00

",
      "dailyEndTime": "

13:00

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

Nota: ricordarsi di premere per **TRY IT OUT!** eseguire le chiamate API.

Passaggio 8. Eseguire la chiamata per GET ottenere gli ID dell'oggetto TimeRange.

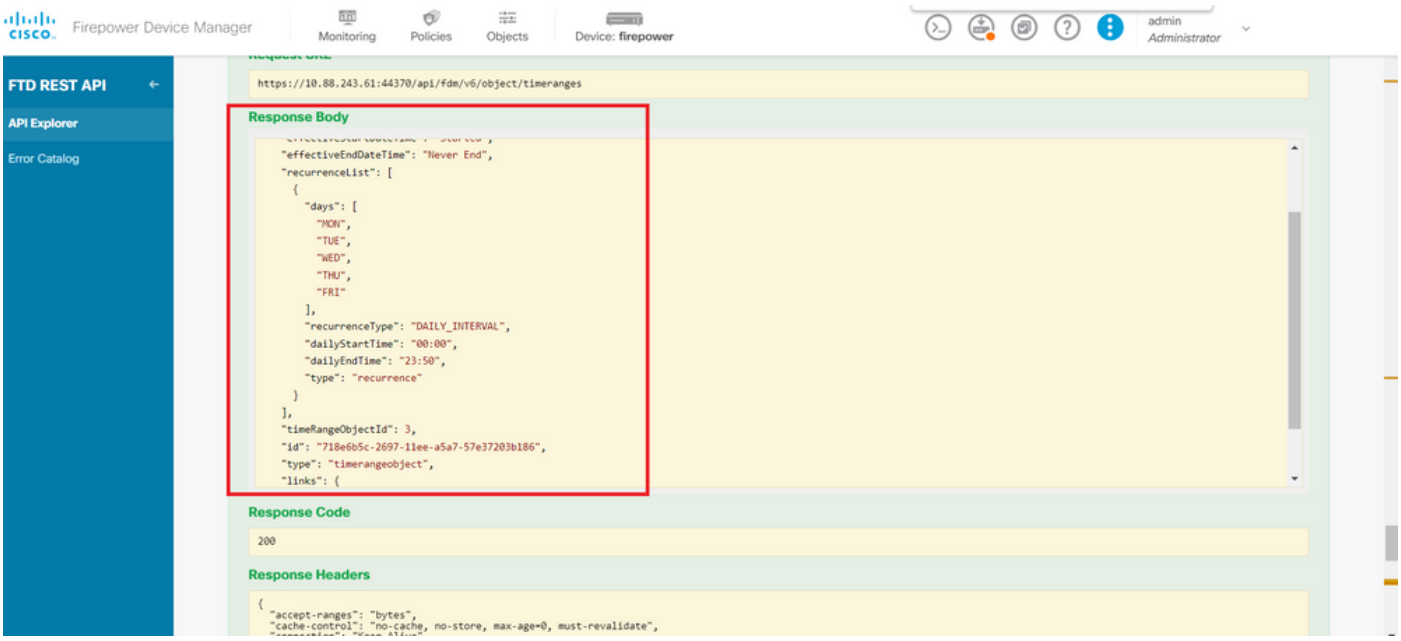

Immagine 8. Ottieni risposta dall'intervallo di tempo.

Passaggio 9. Fare clic sulDeploypulsante per convalidare e applicare le modifiche.

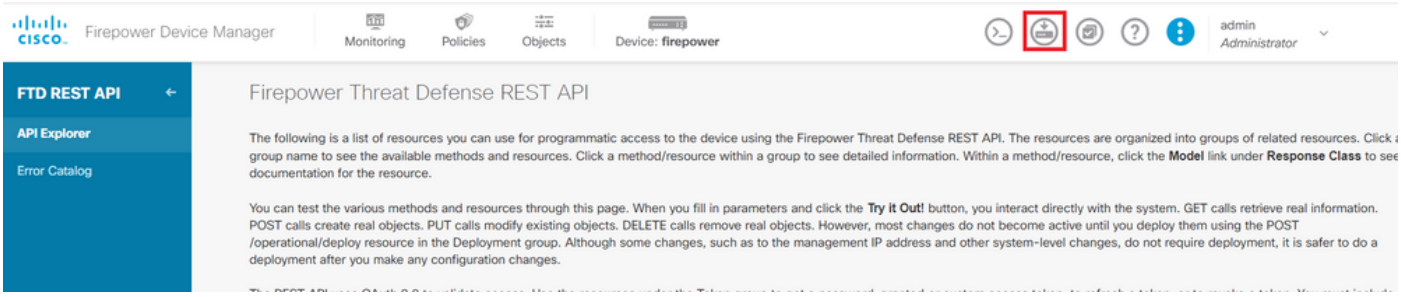

Immagine 9. Pulsante Distribuisci disponibile da Esplora API.

Passaggio 10. Verificare la configurazione appena creata e fare clic su DEPLOY NOW.

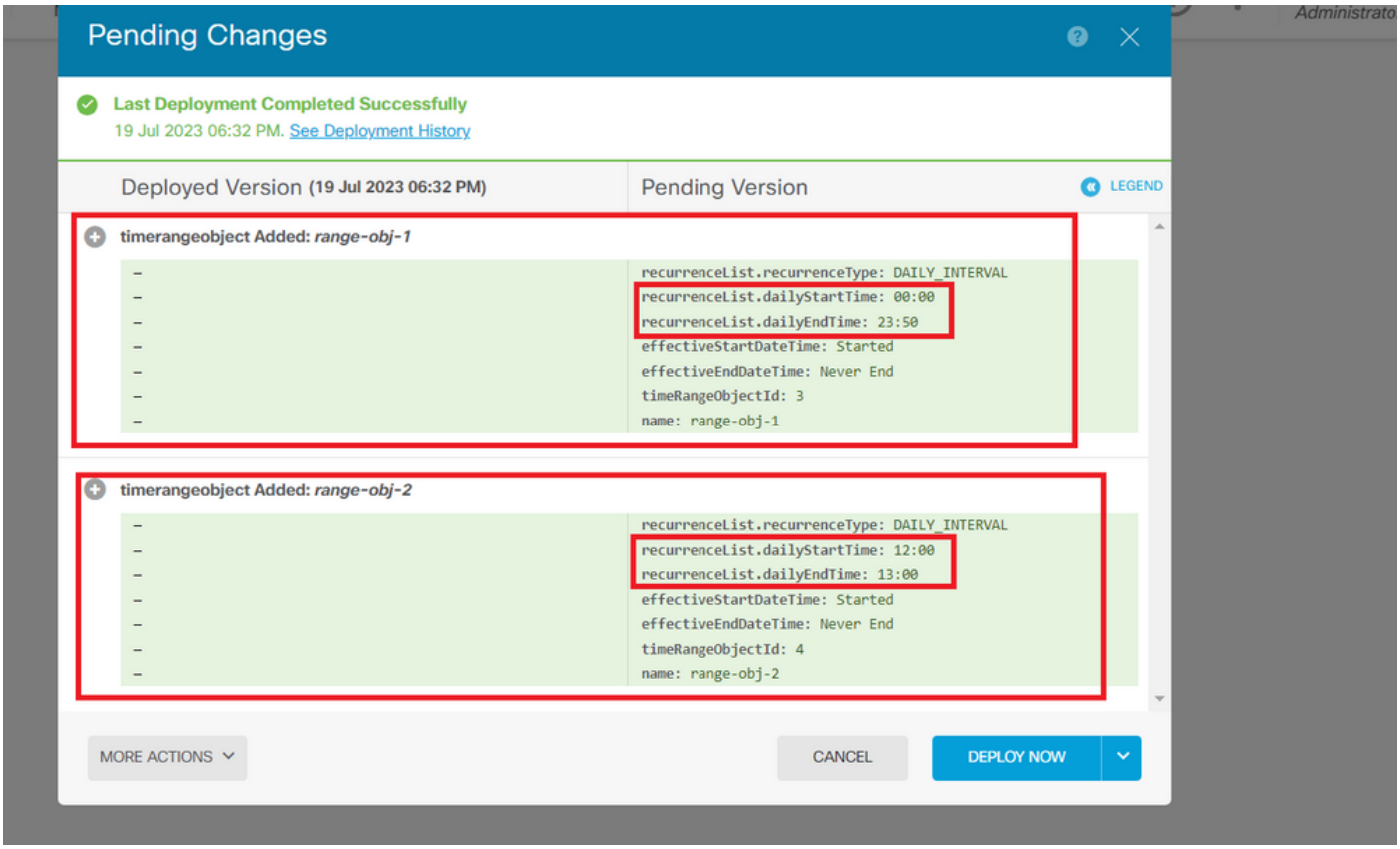

Immagine 10. Finestra Modifiche in sospeso FDM.

Passaggio 11. AccessPolicyIndividuare la categoria e aprire la chiamata POST per creare una regola di controllo dell'accesso basata sul tempo.

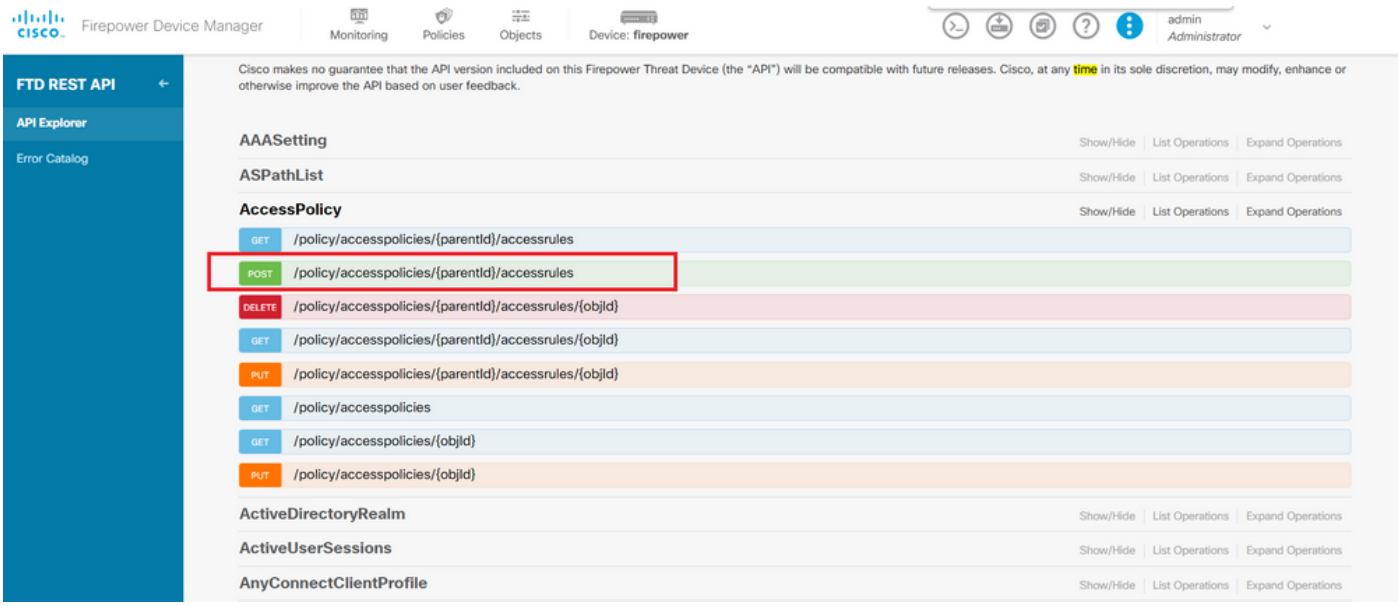

Immagine 11. Chiamata POST ai criteri di accesso.

Di seguito viene riportato un esempio di JSON formato per creare l'ACL con limiti di tempo che permette il traffico dalla zona interna a quella esterna.

Assicurarsi di utilizzare l'ID oggetto Intervallo di tempo corretto.

<#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 è necessario **LOG_FlOW_END** eseguire questa operazione per registrare l'evento alla fine del flusso. In caso contrario, viene restituito un errore.

Passaggio 12. Distribuire le modifiche per applicare il nuovo ACL con limiti di tempo. Il prompt Modifiche in sospeso deve visualizzare l'oggetto intervallo di tempo utilizzato nel passaggio 10.

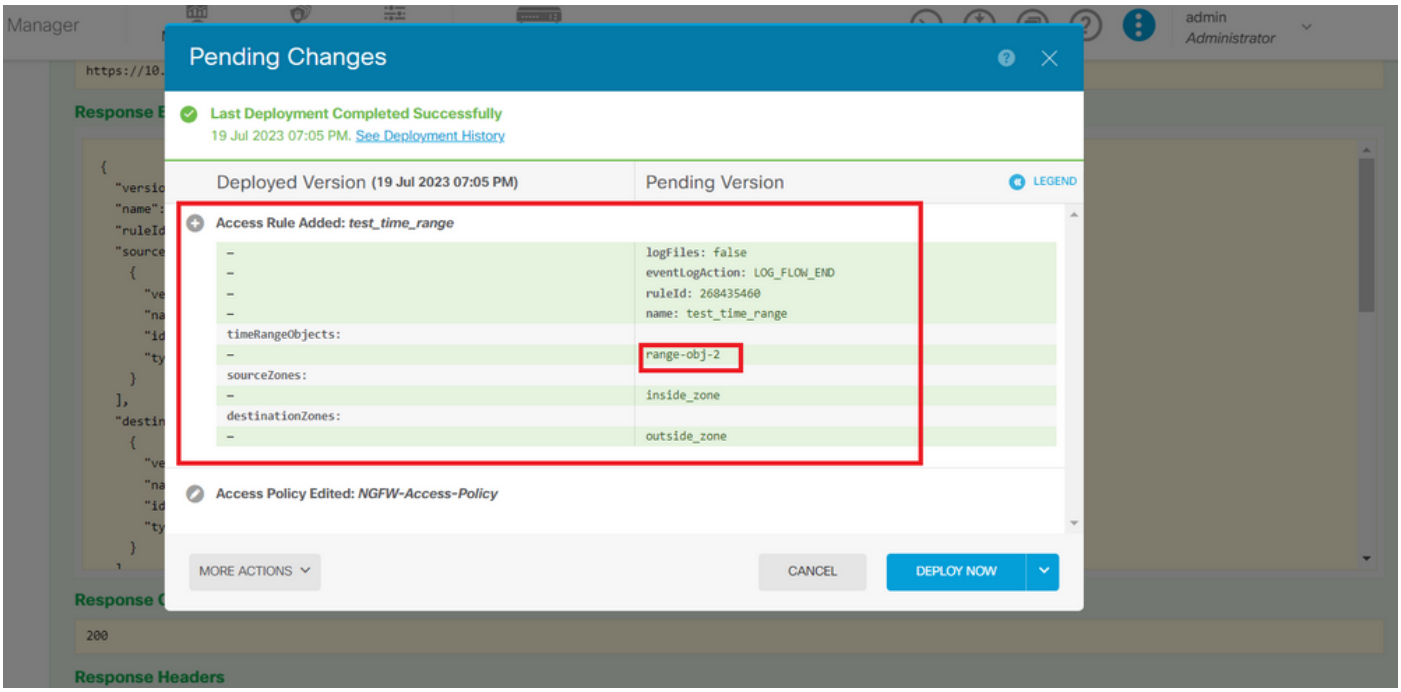

Immagine 12. Nella finestra Modifiche in sospeso di FDM viene visualizzata la nuova regola.

Passaggio 13 (facoltativo). Per modificare l'ACL, è possibile usare la chiamata e modificare l'ID dell'intervallo di tempo.PUT

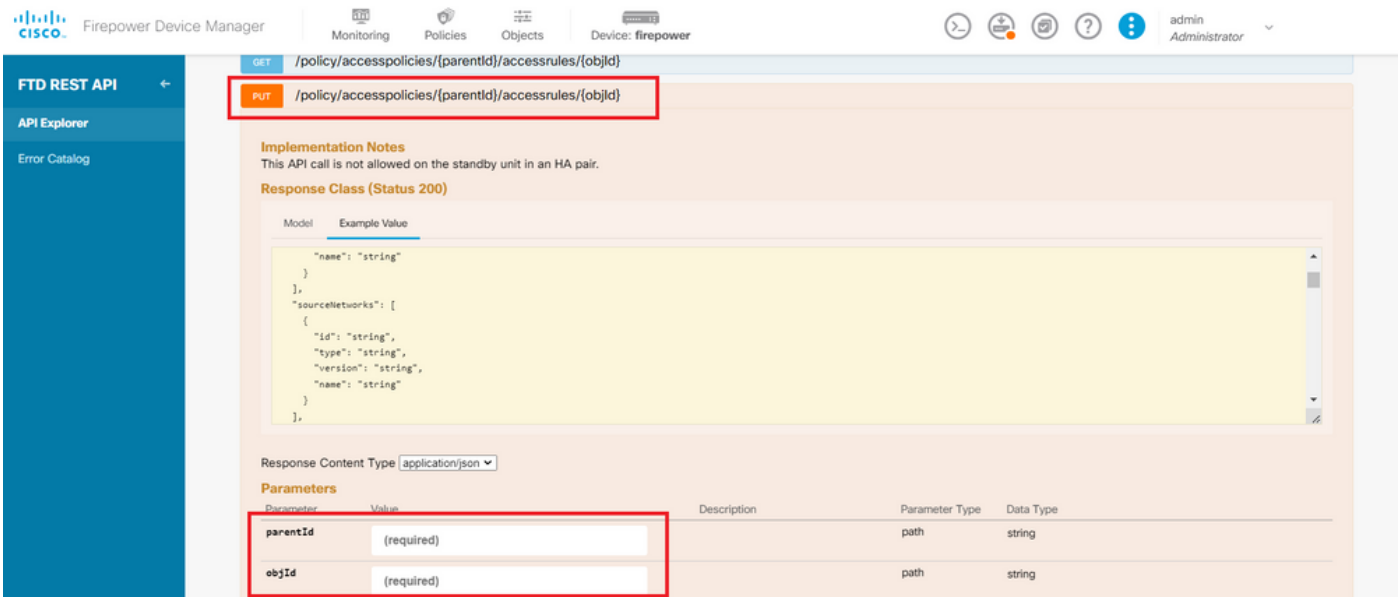

Immagine 13. Chiamata PUT criteri di accesso.

Fare clic qui per visualizzare l'esempio del formato. Gli ID degli intervalli di tempo possono essere raccolti tramite la chiamata perJSON modificare l'intervallo di tempo.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"
}
```


Passaggio 14. Distribuire e convalidare le modifiche.

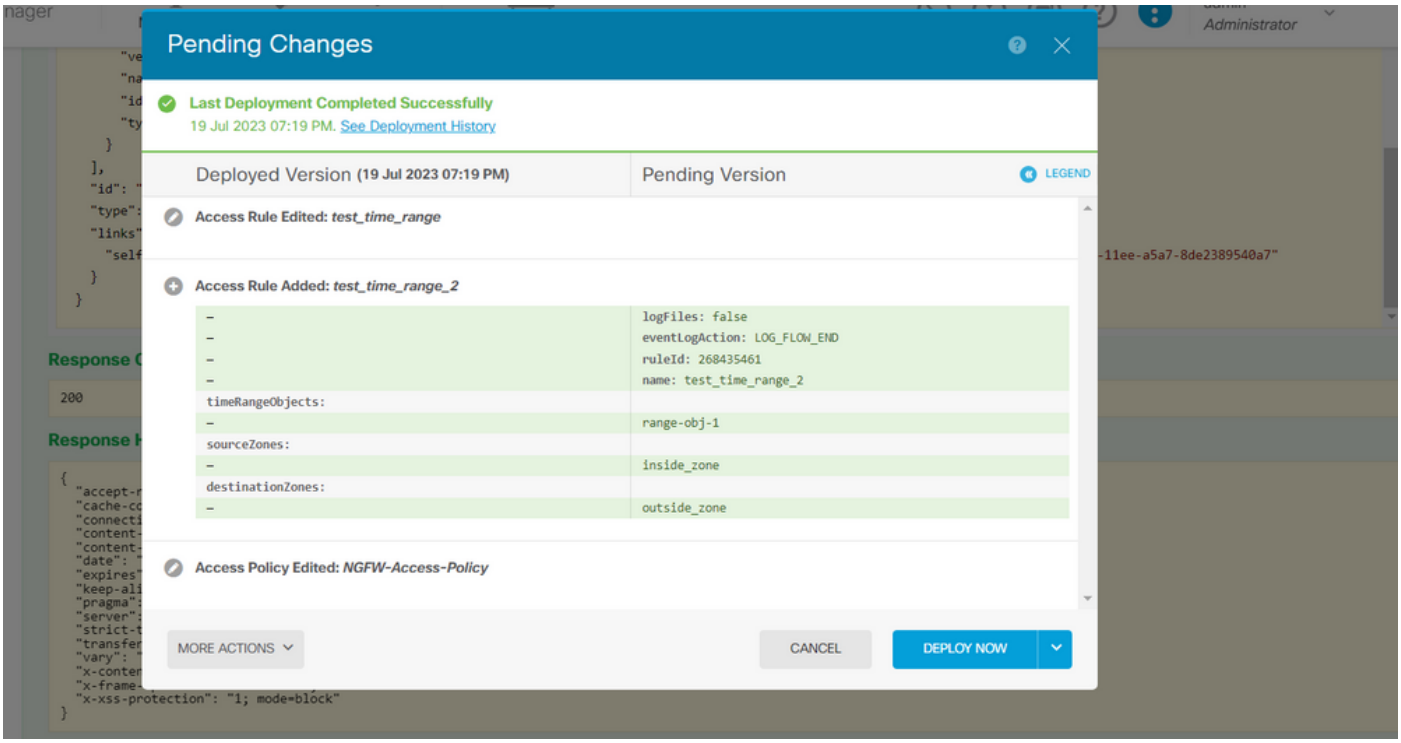

Immagine 14. Nella finestra Modifiche in sospeso di FDM viene visualizzata la modifica dell'oggetto.

Verifica

1. Eseguire il comando`show time-range`per convalidare lo stato degli oggetti dell'intervallo di tempo.

```
<#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. Usare il comando`show access-control-config`per convalidare la configurazione della regola di controllo di

accesso.

<#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. Eseguire un debug perSystem Support Traceverificare che il traffico stia rispettando la regola corretta.

<#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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).