

Configurer une règle de contrôle d'accès basée sur le temps sur FDM avec l'API Rest

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Informations générales](#)
[Configurer](#)
[Vérifier](#)

Introduction

Ce document décrit comment configurer et valider une règle de contrôle d'accès basée sur le temps avec l'API Rest dans le FTD géré par FDM.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Threat Defense (FTD)
- Gestion des périphériques Firepower (FDM)
- Connaissance de l'interface de programmation REST (Representational State Transfer Application Programming Interface)
- Liste de contrôle d'accès (ACL)

Composants utilisés

Les informations contenues dans ce document sont basées sur la version FTD 7.1.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'API FTD version 6.6.0 et ultérieure prend en charge des règles de contrôle d'accès limitées dans le temps.

À l'aide de l'API FTD, vous pouvez créer des objets d'intervalle de temps qui spécifient des intervalles de temps uniques ou récurrents et appliquer ces objets aux règles de contrôle d'accès. À l'aide de plages horaires, vous pouvez appliquer une règle de contrôle d'accès au trafic à certains moments de la journée ou pendant certaines périodes, afin de fournir une certaine flexibilité à l'utilisation du réseau. Vous ne pouvez pas utiliser FDM afin de créer ou d'appliquer des intervalles de temps, et FDM ne vous indique pas si une plage de temps est appliquée à une règle de contrôle d'accès.

Configurer

Étape 1. Cliquez sur les options avancées (menu Kebab) afin d'ouvrir l'explorateur d'API FDM.

The screenshot shows the FDM web interface with the following navigation bar:

- Firepower Device Manager
- Monitoring
- Policies** (selected)
- Objects
- Device: firepower

The main content area is titled "Security Policies" and shows a flowchart: SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion.

The "Access Control" section has a table with the following columns:

| # | NAME | ACTION | SOURCE | DESTINATION | APPLICATIONS | | | | |
|--|------|--------|--------|-------------|--------------|-------|----------|-------|--------------|
| | | | ZONES | NETWORKS | PORTS | ZONES | NETWORKS | PORTS | APPLICATIONS |
| There are no access rules yet. Start by creating the first access rule. | | | | | | | | | |

A blue "CREATE ACCESS RULE" button is visible at the bottom of the table area.

Below the table, there are buttons for "Default Action" (Block), "Access Control" (Block), and other filtering options.

Image 1. Interface utilisateur Web FDM.

Étape 2. Sélectionnez la catégorie **AccessPolicy** afin d'afficher les différents appels API.

The screenshot shows the FTD REST API Explorer interface with the following navigation bar:

- Firepower Device Manager
- Monitoring
- Policies
- Objects
- Device: firepower

The main content area is titled "FTD REST API" and shows the following sidebar menu:

- FTD REST API
- API Explorer
- Error Catalog

The "AccessPolicy" item in the sidebar is highlighted with a red box.

The main content area contains the following text and links:

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 API. POST calls create real objects. PUT calls modify existing objects. DELETE calls remove real objects. However, most changes do not become active until you run /operational/deploy resource in the Deployment group. Although some changes, such as to the management IP address and other system-level changes, become active immediately 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 obtain 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 InitialProvisioning.

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 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 its discretion, may change, modify, or otherwise improve the API based on user feedback.

API categories listed in the sidebar:

- AAASetting
- ASPathList
- AccessPolicy**
- ActiveDirectoryRealm
- ActiveUserSessions
- AnyConnectClientProfile
- AnyConnectPackageFile

Image 2. Interface utilisateur Web de l'API Explorer.

Étape 3. Exécutez la commande GET afin d'obtenir l'ID de la stratégie d'accès.

AccessPolicy

GET /policy/accesspolicies/{parentId}/accessrules

données du corps de réponse vers un bloc-notes. Vous devez ensuite utiliser l'ID de stratégie de contrôle d'accès.

The screenshot shows the Firepower Device Manager interface with the FTD REST API selected. In the API Explorer section, a successful GET request for access policies is displayed. The response body includes a JSON object with various fields, and the 'id' field is highlighted with a red box.

```
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", }
```

Image 5. Réponse GET de la politique d'accès.

Étape 6. Recherchez et ouvrez la catégorie TimeRange dans l'Explorateur d'API afin d'afficher les différents appels d'API.

The screenshot shows the Firepower Device Manager interface with the FTD REST API selected. In the API Explorer section, the 'TimeRange' category is highlighted with a red box. The list of categories includes StandardAccessList, StandardCommunityList, SyslogServer, SystemInformation, Telemetry, TestDirectory, TestIdentityServicesEngineConnectivity, TestIdentitySource, TimeRange, TimeZoneObjects, TimeZoneSettings, TimeZones, Token, TrafficInterruptionReasons, TrafficUser, and TrafficUserGroup.

Image 6. Catégorie Intervalle de temps.

exemple de format pour créer la liste de contrôle d'accès basée sur l'heure qui autorise le trafic de la zone Interne vers la zone Externe.

Assurez-vous d'utiliser l'ID d'objet Time Range correct.

```
<#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"
}
```

Remarque : eventLogAction doit être **LOG_FLOW_END** afin de consigner l'événement à la fin du flux, sinon il donne une erreur.

Étape 12. Déployez les modifications afin d'appliquer la nouvelle liste de contrôle d'accès basée sur le temps. L'invite Modifications en attente doit afficher l'objet de plage de temps utilisé à l'étape 10.

The screenshot shows the FDM Pending Changes interface. At the top, a green checkmark indicates "Last Deployment Completed Successfully" on "19 Jul 2023 07:05 PM". Below this, two tabs are visible: "Deployed Version (19 Jul 2023 07:05 PM)" and "Pending Version". A red box highlights the "Pending Version" tab, which displays a list of changes. The first change is "+ Access Rule Added: test_time_range", which includes fields for logFiles, eventLogAction, ruleId, name, timeRangeObjects, sourceZones, destinationZones, and logFile. The "timeRangeObjects" field contains "range-obj-2", which is also highlighted with a red box. Other changes listed include "- Access Policy Edited: NGFW-Access-Policy". At the bottom right are "CANCEL" and "DEPLOY NOW" buttons.

Image 12. La fenêtre Modifications en attente FDM affiche la nouvelle règle.

Étape 13 (facultatif). Si vous souhaitez modifier la liste de contrôle d'accès, vous pouvez utiliser la PUT appeler et modifiez l'ID de plage horaire.

The screenshot shows the FTD REST API Explorer. The top navigation bar includes "Cisco Firepower Device Manager", "Monitoring", "Policies", "Objects", and "Device: firepower". The left sidebar has sections for "FTD REST API", "API Explorer", and "Error Catalog". The main area shows a "GET /policy/accesspolicies/{parentId}/accessrules/{objId}" endpoint and a highlighted "PUT /policy/accesspolicies/{parentId}/accessrules/{objId}" endpoint. Below these, "Implementation Notes" state that the API call is not allowed on the standby unit in an HA pair. The "Response Class (Status 200)" section shows a table for "Model" and "Example Value" with JSON code. The "Parameters" section at the bottom lists "parentId" and "objId" as required parameters, both of which are highlighted with a red box.

Image 13. Stratégie d'accès Appel PUT.

exemple de format afin de modifier la plage horaire, ces ID de plage horaire peuvent être collectés à l'aide de la GET appel.

```
<#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"
}
```

Étape 14. Déployez et validez vos modifications.

The screenshot shows the 'Pending Changes' window in the FortiManager interface. At the top, a green checkmark indicates 'Last Deployment Completed Successfully' on '19 Jul 2023 07:19 PM'. Below this, a table lists pending changes:

| Deployed Version (19 Jul 2023 07:19 PM) | Pending Version |
|---|--|
| Access Rule Edited: test_time_range | |
| Access Rule Added: test_time_range_2 | <code>logFiles: false eventLogAction: LOG_FLOW_END ruleId: 268435461 name: test_time_range_2</code> <ul style="list-style-type: none"> - - - - timeRangeObjects: <ul style="list-style-type: none"> - range-obj-1 sourceZones: <ul style="list-style-type: none"> - inside_zone destinationZones: <ul style="list-style-type: none"> - outside_zone |
| Access Policy Edited: NGFW-Access-Policy | |

At the bottom right are 'MORE ACTIONS' and 'DEPLOY NOW' buttons.

Image 14. La fenêtre Modifications en attente FDM affiche la modification de l'objet.

Vérifier

- Exécutez la commande show time-range afin de valider l'état de vos objets d'intervalle de temps.

```
<#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
)[]
```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.