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 | | |
|--------------------|--|--|
| <u>はじめに</u> | | |
| <u>前提条件</u> | | |
| <u>要件</u> | | |
| <u>使用するコンポーネント</u> | | |
| <u>背景説明</u> | | |
| <u>設定</u> | | |
| <u>確認</u> | | |

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、一時期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。

| | | | | | | | | API Explore | e . |
|------------|--------------------------------|--|-----------------------|------------------------|----------------------|--------------------------|--------------|-------------|--------------|
| 🛷 Security | / Policies | | | | | | | | - |
| ⊡ → C |) SSL Decryption \rightarrow | \bigcirc Identity \rightarrow \bigcirc |) Security Intelliger | nce $ ightarrow$ 📀 NAT | r $ ightarrow$ Acces | ss Control \rightarrow | Intrusion | | |
| | | | | | T | Filter | | | ¢' @. · |
| | SOURC | æ | | DESTINATION | | | | | |
| # NAME | ACTION ZONES | NETWORKS | PORTS | ZONES | NETWORKS | PORTS | APPLICATIONS | URLS U | ISERS ACTION |
| | | | | There are no ac | veges rules vot | | | | |
| | | | | Start by creating th | e first access rule. | | | | |
| | | | | CREATE AC | CESS RULE | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

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。

| cisco. Firepower Devic | ce Manager | 500 Monitoring | Ø Policies | Objects | Device: firepower | (Σ) | |) ? (| admin Administrato | or ~ |
|--|---|--|---|--|--|---|--|---|--|--|
| FTD REST API ← API Explorer Error Catalog | documenta You can tet POST calls /operations deploymen The REST / valid acces Before usin You can als | tion for the resource it the various method create real objects. I/deploy resource in t after you make any API uses OAuth 2.0 t is token in the Author ing the REST API, you to refer to this page | ds and resour PUT calls mo the Deploym configuration to validate acc rization: Beard need to finisi for a list of AP | ces through the dify existing of ent group. Alt in changes. bess. Use the er header on a h the device in a custom error | his page. When you fill in parami- bjects. DELETE calls remove rea- hough some changes, such as to resources under the Token grou my HTTPS request from your AP hitial setup. You can complete th r codes. (Additional errors migh | eters and click the Try it Out! button, you inte al objects. However, most changes do not bec o the management IP address and other syst p to get a password-granted or custom accer it client. e device initial setup either through UI or thro t exist.) | ract directly w come active ur em-level chan ss token, to re ugh InitialProv | ith the system ntil you deploy ges, do not re fresh a token, ision API. | GET calls retrieve r hem using the POS uuire deployment, it r to revoke a token | eal information. .T is safer to do a . You must include a |
| | NOTE: The that you us Cisco make otherwise i | purpose of the API i e the API Explorer or is no guarantee that mprove the API base ting | Explorer is to n a non-produ the API version ad on user fee | help you learn action device. on included or adback. | n the API. Testing calls through t | he API Explorer requires the creation of accer the "API") will be compatible with future relea | ss locks that n | night interfere any time in its Show/Hid | vith regular operations vith r | on. We recommend y modify, enhance or Expand Operations |
| | ASPathl Accessi ActiveD ActiveU AnyCon AnyCon | .ist Policy irectoryRealm serSessions nectClientProf nectPackageF | file ile | | | | | Show/Hic Show/Hic Show/Hic Show/Hic Show/Hic | List Operations | Expand Operations Expand Operations Expand Operations Expand Operations Expand Operations Expand Operations |

画像 1.FDM Webユーザー・インタフェース。

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。

| Acces | sPolicy | 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/{objld} | | | |

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TRYITOUT!するには、を押す必要があります。

| Monitoring Policies Objects | Device: firepower | () (admin admin administrator | |
|--------------------------------|--|---|---|
| | <pre>"message": "string", "internal_error_code": 0 }</pre> | | |
| | | | |
| | | h. | |
| 20 | Model Example Value ("status_code": 0, "status_error_code": 0) | | |
| /policy/accesspolicies/{objld} | | | |
| /policy/accesspolicies/{objld} | | | |
| | Monitoring Policies Objects Monitoring Policies Objects 20 IFR/ IT OUTI /policy/accesspolicies/(objid) /policy/accesspolicies/(objid) | Monitoring Policies Display Monitoring Policies Display Policies Display Image: Im | Monitoring Policies Monitoring Policies Policies |

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。

| CISCO. Firepower Device Ma | Image Image | |
|----------------------------|---|--|
| FTD REST API 🔶 | | |
| API Explorer | TRY IT OUT | |
| Error Catalog | Curl | |
| | curl -X GETheader '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 | |
| | <pre>"hitCount": { "hitCount": 0, "firstHitTimeStamp": "", "lastHitTimeStamp": "", "lastFetchTimeStamp": "2023-07-18 23:12:162", "type": "hitcount" }, "type": "accessdefaultaction" }, "ssIPolicy": null, "certVisibilityEnabled": false, "networkAnalysisPolicy": null, "advancedsettings": { "davancedsettings": { "davancedsettings"; "id": "c78e66bc-cb57-d3fe-bcbf-96b79b3475bb", "dit": "c78e66bc-cb57-d3fe-bcbf-96b79b3475bb",</pre> | |
| | "scenityliteligence": null, "type": "accesspolicy", | |
| | | |

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。

| CISCO. Firepower Device Mar | nager 🐨 🛱 🗰 nager Monitoring Policies Objects Device: firepower | S admin Administrator |
|-----------------------------|---|--|
| FTD REST API ← | StandardAccessList | Show/Hide List Operations Expand Operations |
| | StandardCommunityList | Show/Hide List Operations Expand Operations |
| API Explorer | SyslogServer | Show/Hide List Operations Expand Operations |
| Error Catalog | SystemInformation | Show/Hilde List Operations Expand Operations |
| | Telemetry | Show/Hide List Operations Expand Operations |
| | TestDirectory | Show/Hide List Operations Expand Operations |
| | TestIdentityServicesEngineConnectivity | Show/Hide List Operations Expand Operations |
| | TestIdentitySource | Show/Hide List Operations Expand Operations |
| | TimeRange | Show/Hide List Operations Expand Operations |
| | TimeZoneObjects | Show/Hide List Operations Expand Operations |
| | TimeZoneSettings | Show/Hide List Operations Expand Operations |
| | TimeZones | Show/Hide List Operations Expand Operations |
| | Token | Show/Hide List Operations Expand Operations |
| | TrafficInterruptionReasons | Show/Hide List Operations Expand Operations |
| | TrafficUser | Show/Hide List Operations Expand Operations |
| | TrafficUserGroup | Show/Line List Onerations Evnand Onerations |

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。

| Firepower Device Manager | r Monitori | ng Policies | i≣≣ Objects | Device: firepo | wer | 6_ | ۵ (| 2 ? | admin Administrato | or ~ |
|--------------------------|--|--|-------------------|----------------|-------------|-----------------------|-------|------------------------|-----------------------|-------------------|
| TIN DEST ADI | <mark>ne</mark> Range | | | | | | | Show/Hid | e List Operations | Expand Operations |
| | er /object/timer | anges | | | | | | | | |
| API Explorer Pos | ost /object/timer | anges | | | | | | | | |
| irror Catalog | Implementation N This API call is not al Response Class (| otes lowed on the stand Status 200) | lby unit in an HA | A pair. | | | | | | |
| | "effectiveEndDa "recurrenceList { "days": ["NON"], "recurrence "dailyEtart "dailyEtart "rangeStart! "rangeStart! | <pre>tetime": "string", ': [fype": "DAILY_INTERV fime": "string", pay": "HON", fime": "string",</pre> | MAL", | | | | | | | • |
| | Response Content T Parameters Parameter body | ype application/json Value (required) | v | | Description | Parameter Tyj body | pe Da | ata Type Model Exam | ple Value | |
| | | | | 4 | | | | { "version": "str | ing", | Ê |

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
۳,
      "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
",
```



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

注:APIコールを実行するには、必ずオンтку ит о∪т! 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。

| Firepower Device Manag | Jer Monitoring Policies Objects Device: firepower | |
|------------------------|---|---|
| FTD REST API 🛛 ← | https://10.88.243.61:44370/ap1/fdm/v6/object/timeranges | |
| API Explorer | Response Body | |
| Error Catalog | <pre>""""""""""""""""""""""""""""""""""""</pre> | |
| | Response Code | ł |
| | Response Headers | |
| | { "accept-ranges": "bytes", "cache-control": "no-cache, no-store, max-age=0, must-revalidate", "cache-control": "no-cache, no-store, max-age=0, must-revalidate", | |

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.

| Last Deployment Completed Suc | cessfully | | | | |
|---|--------------|--|----|--------|--|
| 19 Jul 2023 06:32 PM. See Deploym | nent History | | | | |
| Deployed Version (19 Jul 20 | 23 06:32 PM) | Pending Version | ((| LEGEND | |
| timerangeobject Added: range-ob | oj-1 | | | - | |
| - | | recurrenceList.recurrenceType: DAILY_INTERVAL | | | |
| - | | recurrenceList.dailyStartTime: 00:00 | | | |
| - | | recurrenceList.dailyEndTime: 23:50 | | | |
| - | | effectiveStartDateTime: Started | | | |
| - | | effectiveEndDateTime: Never End | | | |
| | | timeDepareObjectId. 3 | | | |
| - | | timeKangeoDjectid: 3 | | | |
| - | | name: range-obj-1 | | | |
| 1 | | name: range-obj-1 | | | |
| - - • • timerangeobject Added: range-ob | ∋j−2 | name: range-obj-1 | | - | |
| timerangeobject Added: range-ob | <i>ij-2</i> | <pre>range-obj-1 recurrenceList.recurrenceType: DAILY INTERVAL</pre> | | | |
| - - timerangeobject Added: range-ob - - | j−2 | recurrenceList.recurrenceType: DAILY_INTERVAL | _ | | |
| - - timerangeobject Added: range-ob - - - | j−2 | recurrenceList.dailyEndTime: 13:00 | _ | | |
| - - timerangeobject Added: range-ob - - - - | ij-2 | recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:00 effectiveStartDateTime: Started | _ | | |
| timerangeobject Added: range-ob | -j-2 | recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:80 effectiveStartDateTime: Started effectiveEndDateTime: Never End | | | |
| timerangeobject Added: range-ob | ıj−2 | recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:80 effectiveEndDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 | | | |
| - - timerangeobject Added: range-ob - - - - - - - - - - - - - | j−2 | recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:80 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2 | | | |
| - - timerangeobject Added: range-ob - - - - - - - - - - - - - | nj-2 | recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:80 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2 | | | |
| timerangeobject Added: range-ob - -<td>-j-2</td><td>recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:80 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2</td><td></td><td></td><td></td> | -j-2 | recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:80 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2 | | | |

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。

| cisco. Firepower Devic | ce Manager Monitoring Policies Objects Device: firepower Objects Device: firepower |
|------------------------|---|
| FTD REST API + | 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. |
| API Explorer | AAASetting Show//Hide List Operations Expand Operations |
| Error Catalog | ASPathList Show/Hide List Operations Expand Operations |
| | AccessPolicy Show/Hide List Operations Expand Operations |
| | aer /policy/accesspolicies/(parentid)/accessrules post /policy/accesspolicies/(parentid)/accessrules |
| | DELET /policy/accesspolicies/{parentid}/accessrules/(objid} |
| | /policy/accesspolicies/{parentid}/accessrules/{objid} |
| | put /policy/accesspolicies/{parentid}/accessrules/{objid} |
| | ort /policy/accesspolicies |
| | vit /policy/accesspolicies/(objid) |
| | ActiveDirectoryRealm Show/Hide List Operations Expand Operations |
| | ActiveUserSessions Show/Hide List Operations Expand Operations |
| | AnyConnectClientProfile Show/Hide List Operations Expand Operations |

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_FIOW_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。

| ager | 100 | Ø | | (| | | | | ? | 8 | admin Administrator | ~ |
|---------------------|-----------------------|---------------------------------|-------------------------------|------------------------|---|--|-------|--------|----|---|------------------------|---|
| https://10. | Pendin | ig Chang | es | | | | | | | | Hammilton | |
| Response E | S Last De | ployment Com 023 07:05 PM. S | npleted Succ See Deploymen | essfully nt History | | | | | | | | |
| { "versic | Deplo | oyed Versior | ר (19 Jul 2023 | 07:05 PM) | Pending | Version | | C LEGE | ND | | | |
| "name": "ruleId | Access | Rule Added: te | st_time_range | e | | | | | ^ | | | |
| "source { "ve | - | | | | logFiles: f eventLogAct ruleId: 268 name: test | false tion: LOG_FLOW_END 3435460 time cange | | | | | | |
| "id "ty } | timeRa - source | angeObjects: eZones: | | | range-obj-2 | | | | | | | |
|], "destin | - destin - | nationZones: | | | inside_zone outside_zon | e e | | | | | | |
| "ve "na "id | Access | Policy Edited: / | NGFW-Access | s-Policy | | | | | | | | |
| "ty } | MORE ACT | ions ~ | | | | CANCEL | DEPLO | | | | | |
| Response (| | _ | | | | | | | | | | |
| 200 | | | | | | | | | | | | |
| Response He | eaders | | | | | | | | | | | |

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。

| CISCO. Firepower Devic | ce Manager Monitoring Policies Objects Device: firepower 🕑 🍪 🎯 ? <table-cell> admin</table-cell> | | | | | | |
|--|---|--|--|--|--|--|--|
| GT /policy/accesspolicies/(parentid)/accessrules/(objid) | | | | | | | |
| FTD REST API 🔶 | Fur /policy/accesspolicies/{parentld}/accessrules/{objld} | | | | | | |
| API Explorer | | | | | | | |
| Error Catalog | Implementation Notes This API call is not allowed on the standby unit in an HA pair. Response Class (Status 200) | | | | | | |
| | Model Example Value | | | | | | |
| | "name": "string" } /, "sourceletworks": [(| | | | | | |
| | <pre>'id': 'string', 'type': "string', "wersion': 'string' } }</pre> | | | | | | |
| Response Content Type application/json 👻 | | | | | | | |
| | Parameters Personners | | | | | | |
| | parentid (required) path string | | | | | | |
| | ebjId (required) path string | | | | | | |

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": "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
۳,
"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。

| ager I | P | ending Changes | | 0 × | Administrator | | |
|---|-------|--|---|------------|-------------------------------|--|--|
| "ve "na "id "ty } | 0 | ast Deployment Completed Successfully 9 Jul 2023 07:19 PM. See Deployment History | | | | | |
|], | | Deployed Version (19 Jul 2023 07:19 PM) | Pending Version | C LEGEND | | | |
| "type": "links" "self | 0 | Access Rule Edited: test_time_range | | A | ^ -11ee-a5a7-8de2389540a7* | | |
| } | 0 | Access Rule Added: test_time_range_2 | | | | | |
| , | | - | <pre>logFiles: false eventLogAction: LOG_FLOW_END</pre> | | | | |
| Response (| | 1 | ruleId: 268435461 name: test time range 2 | | | | |
| 200 | | timeRangeObjects: | Hand, conclosuel, ouBels | | | | |
| Deserves | | - | range-obj-1 | | | | |
| Response P | | sourceZones: | lacida zona | | | | |
| { | | - destinationZones: | Inside_zone | | | | |
| "cache-co | | - | outside_zone | | | | |
| "content- | | | | | | | |
| "date": " "expires" "keep-ali "pragma": | 0 | Access Policy Edited: NGFW-Access-Policy | | ~ | | | |
| "server": "strict-t "transfer "vary": " "x-conter | N | NORE ACTIONS V | CANCEL | DEPLOY NOW | | | |
| "x-frame- "x-xss-pro } | tect: | ion": "1; mode=blóck" | | | | | |

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

10.10.3 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

10.10.3 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

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。