# REST API를 사용하여 FDM에서 시간 기반 액세 스 제어 규칙 구성

## 목차

<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>배경 정보</u>
<u>구성</u>
<u>다음을 확인합니다.</u>

소개

이 문서에서는 FDM에서 Rest API를 사용하여 관리하는 FTD에서 시간 기반 액세스 제어 규칙을 구 성하고 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 디바 이스는 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 객체 를 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 적용 되는지 여부도 FDM에 표시되지 않습니다.

## 구성

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

	) SSL Decryption	$\rightarrow Ok$	dentity $\rightarrow$ $\bigcirc$	Security Intelligent	ce 🔶 🥑 NA	AT $ ightarrow$ Acces	is Control $\rightarrow$	Subscription			
						Ŧ	Filter			\$	<b>()</b> . +
		SOURCE			DESTINATION						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
					There are no s	accase allas vat					
					Start by creating t	the first access rule.					
					CREATE A	CCESS RULE					

이미지 1. FDM 웹 사용자 인터페이스.

### 2단계. 다른 API 호출AccessPolicy을 표시하려면 범주를 선택합니다.

cisco. Firep	ower Device Ma	nager	题 Monitoring	Ø Policies	.≑Ξ Objects	Device: firepower		6.		0	?	0	admin Administrator	~
FTD REST API	<del>~</del>	documenta	ation for the resource	9.										
API Explorer		POST calls	rou can test the vanous methods and resources through this page. When you hill in parameters and citics the <b>Try It Out!</b> button, you interact directly with the system. GET calls retrieve real information. POST calls create real objects. PUT calls modify existing objects. DELETE calls remove real objects. However, most changes do not become active unit you deploy them using the POST incorrectional divergence resources in the Deployment group. All the programment group. All the programment group. All the resource of the programment group. All they have be provided and the programment group. All they have be provided and the programment group. All they have be provided and the programment group. All they have be provided and they are the programment group. All they have be provided and they are the programment group. All they have be provided and they are the programment of the provided and they are the programment group. All they have be provided and they are the programment of the programment group. All they have be provided and they are the programment of the provided and they are the programment group. All they have be provided and they are the provided and the provid										al information.	
Error Catalog		deploymen	roperational report resource in the deployment group. Autoogn some changes, such as to the management of aduless and other system-level changes, do not require deployment, it is safer to do a deployment after you make any configuration changes.									5 38161 10 UV 8		
		The REST / valid acces	e 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 refresh a token, or to revoke a token. You must include a lid access token in the Authorization: Bearer header on any HTTPS request from your API client.											
		Before usin	ng the REST API, you	need to finis	h the device i	nitial setup. You can complete the devi	e initial setup either through UI	or throu	ugh Initia	IProvisio	on API.			
		You can also refer to this page for a list of API custom error codes. (Additional errors might exist.)												
		NOTE: The	e purpose of the API	Explorer is to	help you lear	n the API. Testing calls through the API	Explorer requires the creation o	of acces	is locks t	hat mig	ht interfe	re with r	egular operation	n. We recommend
		Cisco make otherwise i	es no guarantee that improve the API base	the API versi ed on user fe	on included o	n this Firepower Threat Device (the "Al	") will be compatible with futur	re releas	ses. Cisc	o, at an	y time in	its sole	discretion, may	modify, enhance or
		AAASet	ting								Show/	Hide	List Operations	Expand Operations
	_	ASPath	List								Show/	Hide	List Operations	Expand Operations
		Access	Policy								Show/	Hide	List Operations	Expand Operations
		ActiveD	irectoryRealm								Show/	Hide	List Operations	Expand Operations
		ActiveU	serSessions								Show/	Hide	List Operations	Expand Operations
		AnyCon	nectClientProf	file							Show/	Hide	List Operations	Expand Operations
		AnyCon	nectPackageF	ile							Show/	Hide	List Operations	Expand Operations

이미지 2. API Explorer 웹 사용자 인터페이스.

3단계. 액세스 정책 GET ID를 얻기 위해 통화를 실행합니다.

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}			

이미지 3. 액세스 정책 카테고리.

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

Firepower Device Ma	anager Monitoring Policies Objects Device: firepower	
FTD REST API 🔶	"message": "string", "internal_error_code": 0 )	
API Explorer		
Error Catalog		h
	520 Model Example Value  ( "status_code": 0, "internal_error_code": 0 )	
	ТКУТГСИЛ	
	GET /policy/accesspolicies/{objid}	
	PUT /policy/accesspolicies/{objld}	

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

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

CISCO_ Firepower Device Mana	er Monitoring Policies Objects Device: firepower	(>)	Ť	0	?	•	admin Administrator	~
FTD REST API 🔶						le .		
API Explorer	TRY IT OUTI Hide Response							
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>ThitCount": {     "hitCount": 0,     "firstHitTimeStamp": "",     "lastHitTimeStamp": "",     "lastHitTimeStamp": "2023-07-18 23:12:162",     "type": "hitcount"     },     "type": "hitcount"     },     "sslPolicy": null,     "certVisibilityEnabled": false,     "networkAnalysisPolicy": null,     "advancedSettings" {         "dnsReputationEnforcementEnabled": true,         "type": "advancedSettings"     }.     "identityPolicySetting": null,     "advancedSetting:     hitcourtIolligence: null,     "securityIntelligence: null,     "type": "accesspolicy", </pre>							ĺ

이미지 5. 액세스 정책에서 응답을 가져옵니다.

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

CISCO. Firepower Device M	anager 🐨 🐨 🚎 📖 Monitoring Policies Objects Device: firepower	۵. (	1	?	admin Administrato	r
ETD REST API 6	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/Hide	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
	Time Range			Show/Hide	List Operations	Expand Operations
	TimeZoneObjects			Show/Hide	List Operations	Expand Operations
	Time Zone Settings			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/i lide	List Operations	Evnand Operations

이미지 6. 시간 범위 범주.

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

Firepower Device Manager	Monitoring Policies Objects Devi	(ce: firepower	>.	admin Administrator
Time	Range			Show/Hide   List Operations   Expand Operations
	/object/timeranges			
API Explorer POST	/object/timeranges			
Fror Catalog	plementation Notes s API call is not allowed on the standby unit in an HA pair. sponse Class (Status 200)			
	<pre>"effectiveEndDateTime": "string", "recurrenceList": [</pre>			
Re Pa	sponse Content Type [application/json 💙] rameters rameter Value	Description F	Parameter Type [	Data Type
be	dy (required)		body	Model Example Value

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
۳,
      "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
۳,
       "type": "recurrence"
    }
  ],
  "type": "timerangeobject",
}
```

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

8단계. 호출을GET 실행하여 TimeRange 개체 ID를 가져옵니다.

cisco. Firepower Device Manag	ger Monitoring Policies Objects Device: firepower	
FTD REST API 🔶	https://10.88.243.61:44370/api/fdm/v6/object/timeranges	
API Explorer	Response Body	
Error Catalog	<pre>"effectiveEndDateTime": "Newer End", "recurrenceList": [</pre>	
	Response Code	ł
	200 Response Headers	
	{ "accept-ranges": "bytes", "cache-control": "no-cache, no-store, max-age=0, must-revalidate",	

이미지 8. 시간 범위에서 응답을 가져옵니다.

## 9단계. 변경 사항을<sub>Deploy</sub>검증하고 적용하려면 버튼을 클릭합니다.

cisco. Fire	epower Devi	ce Manager	西 Monitoring	Ø Policies		Device: firepower		2 🔒	admin Administrator
FTD REST A	PI ←	Firepow	er Threat [	Defense I	REST API				
API Explorer		The following	g is a list of resou	rces you can u	se for programm	natic access to the device using th	Firepower Threat Defense REST API. The resources are or	anized into gro	ups of related resources. Click
Error Catalog		group name documentation	to see the availab on for the resourc	le methods an e.	d resources. Cli	ck a method/resource within a gro	p to see detailed information. Within a method/resource, cl	k the Model lin	nk under Response Class to see
		You can test POST calls c /operational/ deployment a	the various metho reate real objects deploy resource i after you make an	ods and resour . PUT calls mo in the Deploym ly configuration	ces through this dify existing obj ent group. Altho changes.	s page. When you fill in parameter: iects. DELETE calls remove real ob ough some changes, such as to th	and click the <b>Try It Out!</b> button, you interact directly with the cts. However, most changes do not become active until yo management IP address and other system-level changes, e	system. GET ca deploy them us o not require de	alls retrieve real information. Ising the POST eployment, it is safer to do a
		The DECT AP				· · · · · · · · · · · · · · · · · · ·			

이미지 9. API 탐색기에서 사용 가능한 배포 단추

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

	ending Changes			×	
)	Last Deployment Completed Successfully 19 Jul 2023 06:32 PM. <u>See Deployment History</u>				
	Deployed Version (19 Jul 2023 06:32 PM)	Pending Version	0		
5	timerangeobject Added: range-obj-1			4	•
	- - - - - -	recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 00:00 recurrenceList.dailyEndTime: 23:50 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 3 name: range-obj-1			
Ð	timerangeobject Added: range-obj-2		_	1	
		pocumpancalist pocumpancaTupa: DATLY INTEDVAL			
	- - - - - -	recurrenceList.dailyStartTime: 12:00 recurrenceList.dailyEndTime: 13:00 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2			

이미지 10. FDM 보류 중인 변경 사항 창

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

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
	cet /policy/accesspolicies/{parentld}/accessrules
	Post /policy/accesspolicies/{parentld}/accessrules
	DELETE /policy/accesspolicies/{parentld}/accessrules/{objld}
	/policy/accesspolicies/{parentid}/accessrules/{objid}
	pur /policy/accesspolicies/{parentId}/accessrules/{objId}
	set /policy/accesspolicies
	GET /policy/accesspolicies/{objid}
	<pre>put /policy/accesspolicies/{objid}</pre>
	ActiveDirectoryRealm Show/Hide List Operations Expand Operations
	ActiveUserSessions Show/Hide List Operations Expand Operations
	AnyConnectClientProfile List Operations Expand Operations

이미지 11. 액세스 정책 POST 통화.

내부 영역에서 외부 영역으로 이동하는 트래픽을 허용하는 시간 기반 ACL을 생성하는 JSON 형식 예 를 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

```
۳,
    "type": "timerangeobject",
    "name": "Time-test2"
    }
  ],
  "type": "accessrule"
}
```



 참고: eventLogAction 흐름LOG\_FIOW\_END이 끝날 때 이벤트를 기록하려면 이(가) 되어야 합니다. 그 렇지 않으면 오류가 발생합니다.

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

https://10	P	ending Changes		3 X Adminis	rator
Response I	0	Last Deployment Completed Successfully 19 Jul 2023 07:05 PM. <u>See Deployment History</u>			
{ "versid		Deployed Version (19 Jul 2023 07:05 PM)	Pending Version	C LEGEND	
"name" "ruleIo	0	Access Rule Added: test_time_range		A	
"source { "vi	e	-	<pre>logFiles: false eventLogAction: LOG_FLOW_END ruleId: 268435460 name: test time range</pre>		
"io "ty	d Y	timeRangeObjects: -	range-obj-2		
} ],		<pre>sourceZones: - destinationZones:</pre>	inside_zone		
destin		-	outside_zone		
"vi "ni "io "ty	0	Access Policy Edited: NGFW-Access-Policy		· .	
}	N	IORE ACTIONS V	CANCEL	DEPLOY NOW Y	
Response					
200					

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

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

CISCO. Firepower Device Mana	ger Monitoring Policies Objects Device: firep	ower (>	) 🚱 🞯 🕐 🚯 admin - Administrator					
	GET /policy/accesspolicies/{parentId}/accessrules/{objId}							
FTD REST API ←	/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)								
	<pre>"name": "string" } ], "sourceletworks": [ {     'id": "string",     "type": "string",     "version": "string",     "name": "string" } ],</pre>		* * #					
	Response Content Type application/json							
	Parameter Value	Description Parameter Ty	pe Data Type					
	parentId (required)	path	string					
	objId (required)	path	string					

이미지 13. 액세스 정책 PUT 호출

시간 범위를 JSON 수정하려면 통화를 사용하여 이러한 시간 범위 ID를 수집할 수 있는 형식 예를 여 기에서GET 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
۳,
"type": "timerangeobject"
}
],
"id": "0f2e8f56-269b-11ee-a5a7-6f90451d6efd",
"type": "accessrule"
}
```

14단계. 변경 내용을 배포하고 검증합니다.

901 "ve	P	ending Changes			Administrator	
"na "id "ty }	0	Last Deployment Completed Successfully     19 Jul 2023 07:19 PM. See Deployment History				
], "id": "		Deployed Version (19 Jul 2023 07:19 PM)	Pending Version	C LEGEND		
"type": "links"	0	Access Rule Edited: test_time_range				
}	0	Access Rule Added: test_time_range_2			-11ee-aba/-00e2303540a/	
Ĺ		-	<pre>logFiles: false eventLogAction: LOG_FLOW_END</pre>			
Response (		1	<pre>ruleId: 268435461 name: test_time_range_2</pre>			
200		timeRangeObjects:	and the second s			
Response H		- sourceZones:	range-obj-1			
1		-	inside_zone			
accept-r "cache-cc		<pre>destinationZones: _</pre>	outside zone			
"connecti "content-						
"content- "date": " "expires" "keep-ali "pragma":	0	Access Policy Edited: NGFW-Access-Policy				
"server": "strict-t "transfer "vary":	N	MORE ACTIONS V	CANCEL	DEPLOY NOW		
"x-frame- "x-xss-pro	otecti	ion": "1; mode=blóck"				

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

#### <#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

10.10.3 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

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 번 역 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.