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

## Sommario

ntroduzione	
rerequisiti	
Requisiti	
Componenti usati	
remesse	
Configurazione	
<u>'erifica</u>	

## 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.

Securit	y Policies										
$\square \rightarrow ($	SSL Decryption	$\rightarrow OI$	dentity $\rightarrow$ $\bigcirc$	Security Intelliger	nce $ ightarrow$ 📀 NAT	$T \rightarrow \bigcirc$ Acces	is Control $\rightarrow$	Intrusion			
						T	Filter			¢	<b>.</b> +
		SOURCE			DESTINATION						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
					There are no ad Start by creating th	ccess rules yet. he first access rule.					
					clart by creating th						
					CREATE AC	CESS RULE					

Immagine 1. Interfaccia utente Web di FDM.

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

CISCO. Firepower	Device Manager	题 Monitoring	Ø Policies	Dbjects	Device: firepower		(>)		9	?	admin Administrato	r ×
FTD REST API API Explorer Error Catalog	← document You can th POST call /operation deployment The REST valid acce Before us You can a NOTE: Th that you u Cisco mal otherwise	ation for the resource est the various metho s create real objects. sal/deploy resource in nt after you make and API uses OAuth 2.0 s token in the Author ing the REST API, you loso refer to this page e purpose of the API se the API Explorer of kes no guarantee that improve the API bas	e. ds and resour pUT calls mo n the Deploym y configuration to validate accorrization: Bear u need to finis for a list of Al Explorer is to n a non-prod t the API versi ed on user fee	rces through the difly existing o nent group. Alt n changes. cess. Use the r header on a the the device in PI custom error help you lean uction device. ion included or edback.	his page. When you fill in parameter bjects. DELETE calls remove real of hough some changes, such as to the resources under the Token group to my HTTPS request from your API of hitial setup. You can complete the d r codes. (Additional errors might ex- the API. Testing calls through the n this Firepower Threat Device (the	s and click the <b>Try it Out!</b> buttor yiects. However, most changes of the management IP address and of the get a password-granted or cus- tent. evice initial setup either through ist.) API Explorer requires the creation "API") will be compatible with fur-	n, you inte do not bec other syste stom acces a UI or thro on of acces uture relea	ract directore action a	ctly with t ive until y changes to refres alProvisio that migh co, at any	the system. Gf rou deploy the , do not requir h a token, or t n API. t interfere with t interfere with time in its sol	ET calls retrieve n m using the POS e deployment, it o revoke a token. n regular operatio e discretion, may	eal information. T is safer to do a You must include a n. We recommend r modify, enhance or
	AAASe ASPath	tting List								Show/Hide Show/Hide	List Operations	Expand Operations Expand Operations
	Access	DirectoryRealm	I							Show/Hide	List Operations	Expand Operations
	AnyCo	nnectClientPro nnectPackageF	file							Show/Hide Show/Hide Show/Hide	List Operations List Operations List Operations	Expand Operations Expand Operations Expand Operations

Immagine 2. Interfaccia utente Web di API Explorer.

Passaggio 3. Per ottenere l'ID dei criteri di accesso, eseguire la chiamataGET.

Acces	ssPolicy	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/{objId}			

Immagine 3. Categoria Criteri di accesso.

Firepower Device Man	ager Monitoring Policies Objects Dr	evice: firepower	) 🖨 🔊 ?	admin Administrator	
FTD REST API 🔶		"message" "string", "internal_error_code": 0 }			
API Explorer					
Error Catalog					
	528			<i>A</i>	
		Model Example Value			
		( "statur_code": 0, "estage": "string", "internal_error_code": 0 )		<i>h</i>	
	TRY IT OUT				
	GET /policy/accesspolicies/{objld}				
	PUT /policy/accesspolicies/{objid}				

Passaggio 4. Per recuperare la rispostatry it outidell'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.

Firepower Device Ma	nager Monitoring Policies Objects Device: firepower	$\odot$	) ? 🚦	admin Administrato	r
	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
	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/Links	List Operations	Expand Operations

Immagine 6. Categoria Intervallo di tempo

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

Firepower Device Manager	Monitoring Policies Objects Device: firepower	$(\Sigma)$	admin Administrator
Time	Range		Show/Hide List Operations Expand Operations
	/object/timeranges		
API Explorer Post	/object/timeranges		
Fror Catalog	plementation Notes is API call is not allowed on the standby unit in an HA pair. asponse Class (Status 200)		
	<pre>Model Example Value "effectiveEndDateTime": "string", "recurrenceList": [</pre>		•
Ri P E	sponse Content Type [application/json 🗸] arameters arameter Value (required)	Description Parameter Typ body	pe Data Type Model Example Value ( "version": "string",

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
```

۳,

```
"dailyEndTime": "
```

#### 23:50

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

```
"type": "timerangeobject"
}
```

Oggetto 2:

<#root>

{

```
"name": "
range-obj-2
```

```
",
"recurrenceList": [
    {
      "days": [
        "MON"
      ],
      "recurrenceType": "DAILY_INTERVAL",
      "dailyStartTime": "
12:00
۳,
      "dailyEndTime": "
13:00
",
      "type": "recurrence"
    }
  ],
  "type": "timerangeobject",
}
```

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

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

Firepower Device Man	ager Monitoring Policies Objects Device: firepower Objects @ ? : admin
FTD REST API ←	https://10.88.243.61:44370/api/fdm/v6/object/timeranges
API Explorer	Response Body
Error Catalog	<pre>Contention: "New End", "effectiveEndDateTime: "New End", "recurrenceIst": [ ( "days": [ "DU", "TUU", "TUU", "TBU",</pre>
	Response Code
	Response Headers
	{     "accept-ranges": "bytes",     "cache-control": "no-cache, no-store, max-age=0, must-revalidate",     """"""""""""""""""""""""""""""""

Immagine 8. Ottieni risposta dall'intervallo di tempo.

#### Passaggio 9. Fare clic sul<sub>Deploy</sub>pulsante 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.

	Last Deployment Completed Successfully 19 Jul 2023 06:32 PM. See Deployment History					
	Deployed Version (19 Jul 2023 06:32 PM)	Pending Version	(	LEGE	END	
Ð	timerangeobject Added: range-obj-1				^	
	- - - - - - - -	recurrenceList.recurrenceType: DAILY_INTERVAL recurrenceList.dailyStartTime: 00:00 recurrenceList.dailyEndTime: 23:50 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 3 name: range-obj-1				
_	timerangeobject Added: range-obj-2			1		
Ð	-	recurrenceList.recurrenceType: DAILY_INTERVAL				
•	- - - - -	recurrenceList.dailyEndTime: 12:00 effectiveStartDateTime: Started effectiveEndDateTime: Never End timeRangeObjectId: 4 name: range-obj-2				

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.

CISCO_ Firepower Devic	e Manager Monitoring Policies Objects Device: firepower	admin Administrator
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 tim otherwise improve the API based on user feedback.	ne in its sole discretion, may modify, enhance or
API Explorer	AAASetting	Show/Hide   List Operations   Expand Operations
Error Catalog	ASPathList s	how/Hide   List Operations   Expand Operations
	AccessPolicy	how/Hide   List Operations   Expand Operations
	cet /policy/accesspolicies/{parentid}/accessrules	
	POST /policy/accesspolicies/{parentld}/accessrules	
	Velete /policy/accesspolicies/{parentid}/accessrules/{objid}	
	cer /policy/accesspolicies/{parentid}/accessrules/{objid}	
	/policy/accesspolicies/{parentid}/accessrules/{objid}	
	art /policy/accesspolicies	
	art /policy/accesspolicies/{objid}	
	рит /policy/accesspolicies/{objid}	
	ActiveDirectoryRealm	ihow/Hide List Operations Expand Operations
	ActiveUserSessions	how/Hide List Operations Expand Operations
	AnyConnectClientProfile	how/Hide List Operations Expand Operations

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": [
    Ł
    "id": "
718e6b5c-2697-11ee-a5a7-57e37203b186
...
    "type": "timerangeobject",
    "name": "Time-test2"
    }
  ],
   'type": "accessrule"
}
```



Nota: eventLogAction è necessario LOG\_FIOW\_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.

yei https://10.	Pending Changes		Adminis	rator
Response E	Last Deployment Completed Successfully 19 Jul 2023 07:05 PM. See Deployment History			
{ "versic	Deployed Version (19 Jul 2023 07:05 PM)	Pending Version	C LEGEND	
"name": "ruleId	Access Rule Added: test_time_range		A	
"source { "ve		logFiles: false eventlogAction: LOG_FLOM_END rulEd: 260435460 name: test time range		
"id "ty	timeRangeObjects: -	range-obj-2	_	
) }	sourceZones:	inside_zone	_	
"destin	destinationZones: -	outside_zone		
"ve "na "id "ty }	Access Policy Edited: NGFW-Access-Policy		•	
1 Decemence (	MORE ACTIONS V	CANCEL	EPLOY NOW Y	
Response (				
200				

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<sup>PUT</sup> intervallo di tempo.

CISCO. Firepower Devic	ice Manager Devices Objects Device: firepower Device: firepower	
	/policy/accesspolicies/{parentld}/accessrules/{objld}	
FTD REST API 🗧 🗧	/policy/accesspolicies/{parentld}/accessrules/{objid}	
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": "strine"	
	"sourceletworks": [ (	
	"id": "string", "www.s. "string".	
	"version": "string", "name": "string"	
	neme : string	
	A definition of the second sec	
	Response Content Type application/json 🗸	
	Parameters	
	Parameter Value Description Parameter Type Data Type	
	parentId (required) path string	
	objId         path         string	

Immagine 13. Chiamata PUT criteri di accesso.

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

#### <#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"
}
```

Passaggio 14. Distribuire e convalidare le modifiche.

nager	P	ending Changes	K	0 ×	2 Commission Administrator	
"na "id "ty }	0	ast Deployment Completed Successfully 9 Jul 2023 07:19 PM. See Deployment History				
], "14", "		Deployed Version (19 Jul 2023 07:19 PM)	Pending Version	C LEGEND		
"type": "links" "self	0	Access Rule Edited: test_time_range		-11ee-a5a7-8de2389540a7"		
}	0	Access Rule Added: test_time_range_2				
J Posponso (		1	<pre>logFiles: false eventLogAction: LOG_FLOW_END mulad: 269/35/61</pre>			
200		- - timePanne/biosts:	name: test_time_range_2			
Response F		-	range-obj-1			
		sourceZones:	incida zono			
{ "accent_r		- destinationZones:	Inside_zone			
"cache-co "connecti		-	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	EPLOY NOW 🗸		
"x-trame- "x-xss-pro }	tecti	lon": "1; mode+blóck"				

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

## Verifica

1. Eseguire il comandoshow time-rangeper 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
```

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 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).