Configureer een tijdgebaseerde toegangscontroleregel op FDM met rest-API

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Verifiëren

Inleiding

Dit document beschrijft hoe u een tijdgebaseerde toegangscontroleregel kunt configureren en valideren met Rest API in de FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defense (FTD)
- Firepower Device Management (FDM)
- Kennis van representatieve Overdracht van de Toepassingsprogrammeerinterface van de Staat (REST API)
- Toegangscontrolelijst (ACL)

Gebruikte componenten

De informatie in dit document is gebaseerd op FTD versie 7.1.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

FTD API versie 6.6.0 en hoger ondersteunen toegangscontroleregels die beperkt zijn op basis van tijd.

Met behulp van de FTD API kunt u tijdbereikobjecten maken, die eenmalige of terugkerende tijdbereiken specificeren, en deze objecten toepassen op toegangscontroleregels. Met behulp van tijdbereiken kunt u een toegangscontroleregel toepassen op verkeer tijdens bepaalde tijden van de dag of voor bepaalde periodes, om flexibiliteit te bieden aan netwerkgebruik. U kunt FDM niet gebruiken om tijdbereiken te maken of toe te passen, noch toont FDM u of een toegangscontroleregel een tijdbereik heeft toegepast op het.

Configureren

Stap 1. Klik op de geavanceerde opties (het menu Kebab) om de FDM API verkenner te openen.

cisco.	Firepov	ver Device Manage	er	Monitoring	Ø Policies	i#E Objects	Device: firepower			
		🔊 Security P	olicies							
			SL Decryptic	on \rightarrow \bigcirc k	dentity \rightarrow (Security Inte	lligence $ ightarrow$ 🔗 NA	r $ ightarrow$ Acce	ss Control \rightarrow	Intrusion
								Ŧ	Filter	
				SOURCE			DESTINATION			
		# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS
							There are no au Start by creating th	ccess rules yet. Ie first access rule. CESS RULE		
		Default Action /	Access Con	trol 😑 Block	₫, ₽, ×					

Afbeelding 1. FDM web gebruikersinterface.

Stap 2. Kies de categorie AccessPolicy om de verschillende API-oproepen weer te geven.

cisco. Firepow	ver Device Manager	题 Monitoring	Ø Policies		Device: firepower				
FTD REST API	documenta	tion for the resourc	e.	rces through thi	s nane. When you fill in naramet	ters and click the Try it Out! button, you interact directly			
API Explorer	POST calls /operationa	create real objects al/deploy resource i	PUT calls mo n the Deploym	dify existing ob nent group. Alth	jects. DELETE calls remove real ough some changes, such as to	objects. However, most changes do not become active the management IP address and other system-level cl	1		
Error Catalog	deploymen The REST / valid acces Before usin You can als NOTE: The that you use Cisco make otherwise in	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 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 InitialProvide and the term of ter							
	AAASet ASPathl Access ActiveD ActiveU AnyCon AnyCon	ting List Policy irectoryRealm serSessions nectClientPro nectPackagel	file						



Stap 3. Draai de GET bellen om de Access Policy ID te verkrijgen.

Acces	sPolicy
GET	/policy/accesspolicies/{parentld}/accessrules

formaat voorbeeld om de op tijd gebaseerde ACL te maken die verkeer van binnenuit naar de buitenzone toestaat.

Zorg ervoor dat u de juiste tijdbereik object-ID gebruikt.

```
<#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"
}
```

Opmerking: eventLogAction moet **LOG_FIOW_END** om de gebeurtenis aan het eind van de stroom te registreren, geeft het anders een fout.

Stap 12. Stel de veranderingen op om nieuwe op tijd-gebaseerde ACL toe te passen. De wachtende melding Wijzigingen moet het in Stap 10 gebruikte tijdbereikobject weergeven.

er .)	
https://10.	Pending Changes		0
Response E	Last Deployment Completed Successfully 19 Jul 2023 07:05 PM. See Deployment History		
{ "versio	Deployed Version (19 Jul 2023 07:05 PM)	Pending Version	O L
"name": "ruleId	Access Rule Added: test_time_range		7
"source { "ve		<pre>logFiles: false eventLogAction: LOG_FLOW_END ruleId: 268435460 name: test time range</pre>	
"id "ty	timeRangeObjects: -	nange-obj-2	
} }	sourceZones: -	inside_zone	
"destin {	destinationZones: -	outside_zone	
"ve "na "id	Access Policy Edited: NGFW-Access-Policy		
, }	MORE ACTIONS V	CANCEL	DEPLOY NOW
Response (
{ "ve "na "id "ty } Response (Access Policy Edited: NGFW-Access-Policy MORE ACTIONS ~	CANCEL	DEPLOY NOW

Afbeelding 12. FDM In afwachting van het venster van Veranderingen toont de nieuwe regel.

Stap 13 (optioneel). Als u ACL wilt bewerken, kunt u de PUT de tijdbereik-ID bellen en bewerken.

CISCO_ Firepower Device Manager	Monitoring	Policies Object	ts Device: firep	power	0	ê (
FTD REST API +	/policy/accesspolic	cies/{parentId}/acce	ssrules/{objid}			
API Explorer Error Catalog Res	lementation Notes API call is not allowed ponse Class (Status	on the standby unit in s 200)	an HA pair.			
	Model Example Value	_				
	<pre>], "sourceNetworks": [{ "id": "string", "type": "string", "version": "string" "name": "string" }],</pre>	r,				
Res	oonse Content Type a	pplication/json 👻				
Par	entId (requ	uired)		Description	Parameter Type path	Data Ty string
obj	Id (requ	uired)			path	string

Afbeelding 13. PUT call voor toegangsbeleid.

Vind hier de JSON Deze tijdbereik-ID's kunnen worden verzameld met behulp van deGET bellen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.