Konfigurieren einer zeitbasierten Zugriffskontrollregel für FDM mit REST-API

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Überprüfung

Einleitung

In diesem Dokument wird beschrieben, wie eine zeitbasierte Zugriffskontrollregel mit der REST-API in dem von FDM verwalteten FTD konfiguriert und validiert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Firepower Threat Defense (FTD)
- FirePOWER-Gerätemanagement (FDM)
- Kenntnisse der REST-API (Representational State Transfer Application Programming Interface)
- Zugriffskontrollliste (ACL)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf FTD-Version 7.1.0.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

FTD API Version 6.6.0 und höher unterstützt Zugriffskontrollregeln, die zeitlich begrenzt sind.

Mithilfe der FTD-API können Sie Zeitbereichsobjekte erstellen, die einmalige oder wiederkehrende Zeitbereiche angeben, und diese Objekte auf Zugriffskontrollregeln anwenden. Mithilfe von Zeiträumen können Sie eine Zugriffskontrollregel auf Datenverkehr anwenden, der zu bestimmten Tageszeiten oder für bestimmte Zeiträume generiert wird, um die Netzwerknutzung flexibel zu gestalten. Sie können FDM nicht zum Erstellen oder Anwenden von Zeitbereichen verwenden. FDM zeigt Ihnen auch nicht an, ob auf eine Zugriffskontrollregel ein Zeitbereich angewendet wurde.

Konfigurieren

Schritt 1: Klicken Sie auf die erweiterten Optionen (Kebab-Menü), um den FDM API Explorer zu öffnen.

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	₫, ₽, ×					

Bild 1. FDM-Web-Benutzeroberfläche.

Schritt 2: Wählen Sie die Kategorie AccessPolicy um die verschiedenen API-Aufrufe anzuzeigen.

Firepower Device	Manager	Monitoring	Ø Policies	∰⊒ Objects	Device: firepower				
FTD REST API ←	documental	tion for the resourc	e.	reas through this	e nana When unu fill in naramatare a	nd click the Try it Out! button, you interact directly			
API Explorer	POST calls create real objects. PUT calls modify existing objects. DELETE calls remove real objects. However, most changes do not become active //operational/deploy resource in the Deployment group. Although some changes, such as to the management IP address and other system-level cha deployment 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 i 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 InitialPro 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 that you use the API Explorer on a non-production device.								
Error Catalog									
	Cisco make otherwise in AAASett	is no guarantee tha mprove the API bas ting	t the API versi ed on user fe	ion included on edback.	this Firepower Threat Device (the "Af	PI") will be compatible with future releases. Cisco,			
	Access	Policy							
	ActiveDi	ActiveDirectoryRealm							
	ActiveU	serSessions							
	AnyCon	nectClientPro	file						
	AnyCon	nectPackagel	ile						



Schritt 3: Führen Sie GET um die Zugriffsrichtlinien-ID zu erhalten.

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

Daten vom Antworttext an ein Notizblock. Später müssen Sie die Richtlinien-ID für die Zugriffskontrolle verwenden.



Bild 5. GET-Antwort von der Zugriffsrichtlinie.

Schritt 6: Suchen und öffnen Sie die Kategorie TimeRange im API-Explorer, um die verschiedenen API-Aufrufe anzuzeigen.

cisco. Firepower Device Mar	anager Monitoring Policies Objects Device: firepower							
	StandardAccessList							
FID RESTAPT	StandardCommunityList							
API Explorer	SyslogServer							
Error Catalog	SystemInformation							
	Telemetry							
	TestDirectory							
	TestIdentityServicesEngineConnectivity							
	TestIdentitySource							
	TimeRange							
	TimeZoneObjects							
	TimeZoneSettings							
	TimeZones							
	Token							
	TrafficInterruptionReasons							
	TrafficUser							
	TrafficUserGroup							

-Formatbeispiel verwenden, um die zeitbasierte ACL zu erstellen, die den Datenverkehr von der Innen- zur Outside-Zone zulässt.

Stellen Sie sicher, dass Sie die richtige Objektkennung für den Zeitbereich verwenden.

```
<#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"
}
```

Anmerkung: eventLogAction muss LOG_FIOW_END um das Ereignis am Ende des Flusses zu protokollieren, andernfalls wird ein Fehler ausgegeben.

Schritt 12: Stellen Sie die Änderungen bereit, um die neue zeitbasierte Zugriffskontrollliste anzuwenden. An der Eingabeaufforderung Pending Changes (Ausstehende Änderungen) muss das in Schritt 10 verwendete Zeitbereichsobjekt angezeigt werden.

ager	- EE	Ø					
https://10	Pen	ding Char	iges				0
Response	E 🕑 Las 19-	st Deployment C Jul 2023 07:05 Pf	Completed Suco	cessfully ant History			
{ "versio	. D	eployed Vers	ion (19 Jul 202	3 07:05 PM)	Pending Vers	ion	O 1
"name" "ruleI	O Ac	cess Rule Added	: test_time_rang	je			
"source { "ve "ve	e -				logFiles: false eventLogAction: L ruleId: 268435466 name: test time r	LOG_FLOW_END	
"i	d t	imeRangeObjects:			maner cost_cint_	0.80	
"t; }	y -	- sourceZones :			range-obj-2		
Ъ					inside_zone		
"destin {	n -	estinationZones:			outside_zone		
"vi "n. "i("t;	Ac	cess Policy Edite	d: NGFW-Acces	s-Policy			
}	MORE	E ACTIONS V				CANCEL	DEPLOY NOW
Response	(
200							
Pospores	Hoodore						
Response	reducis						

Bild 12. Im Fenster "FDM - ausstehende Änderungen" wird die neue Regel angezeigt.

Schritt 13 (optional). Wenn Sie die ACL bearbeiten möchten, können Sie die PUT die ID des Zeitbereichs aufrufen und bearbeiten.

Firepower Device Manager	Monitoring	Policies	Objects	Device: firepo	wer	(Σ)	٩ (
GET	/policy/accessp	olicies/{parent	tld}/accessrule	s/{objld}			
FTD REST API +	/policy/accessp	olicies/{parent	tld}/accessrule	s/{objld}			
API Explorer							
Error Catalog Imp This Res	lementation Note API call is not allow ponse Class (Sta	ed on the stand tus 200)	dby unit in an H/	A pair.			
	Model Example Va	lue					
	<pre>"name": "string }], "sourceNetworks": [{ "id": "string", "type": "string "version": "str name": "string }],</pre>	- .,					
Resp Para	oonse Content Type ameters	application/json	•				
Para	meter Value				Description	Parameter Type	Data Ty
par	entId (r	equired)				path	string
obj	Id (r	equired)				path	string

Bild 13. Zugriffsrichtlinien-PUT-Anruf.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.