Configuración de una regla de control de acceso basado en tiempo en FDM con API de resto

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Antecedentes Configurar Verificación

Introducción

Este documento describe cómo configurar y validar una regla de control de acceso basado en tiempo con API Rest en el FTD administrado por FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense (FTD)
- Administración de dispositivos Firepower (FDM)
- Conocimiento de la interfaz de programación de aplicaciones de transferencia de estado representacional (API REST)
- Lista de control de acceso (ACL)

Componentes Utilizados

La información de este documento se basa en la versión 7.1.0 del FTD.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La versión 6.6.0 y posteriores de la API de FTD admiten reglas de control de acceso que están limitadas en función del tiempo.

Mediante la API de FTD, puede crear objetos de rango de tiempo, que especifican rangos de tiempo únicos o recurrentes, y aplicar estos objetos a las reglas de control de acceso. Mediante el uso de intervalos de tiempo, puede aplicar una regla de control de acceso al tráfico durante determinadas horas del día o durante determinados períodos de tiempo, con el fin de proporcionar flexibilidad al uso de la red. No puede utilizar FDM para crear o aplicar rangos de tiempo, ni FDM muestra si una regla de control de acceso tiene un rango

de tiempo aplicado.

Configurar

Paso 1. Haga clic en las opciones avanzadas (menú Kebab) para abrir el explorador de la API de FDM.

cisco.	Firepov	ver Device Manag	er	Monitoring	Ø Policies	Objects	Device: firepower). 🏟
		🔊 Security F	Policies							
			SL Decrypti	on \rightarrow \bigcirc l	dentity \rightarrow (Security Intell	igence $ ightarrow$ 🥝 NAT	→ 🖌 Acce	ss Control \rightarrow	Intrusion
								T	Filter	
				SOURCE			DESTINATION			
		# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS
							There are no ac Start by creating the	cess rules yet. a first access rule.		
							CREATE ACC	ESS RULE		
		Default Action	Access Con	trol 😑 Block	₫ 8					

Imagen 1. Interfaz de usuario web de FDM.

Paso 2. Elija la categoría AccessPolicy para mostrar las diferentes llamadas de API.

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 /operationa	create real objects I/deploy resource i	. PUT calls mo n the Deploym	dify existing ob nent group. Alth	jects. DELETE calls remove real objection of the sector of	ts. However, most changes do not become active nanagement IP address and other system-level chi		
Error Catalog	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 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 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.							
	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	irectoryRealm	1					
	ActiveU	serSessions						
	AnyCon	nectClientPro	file					
	AnyCon	nectPackagel	ile					



Paso 3. Ejecute el GET para obtener el ID de política de acceso.

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

datos del cuerpo de la respuesta a un bloc de notas. Posteriormente, debe utilizar el ID de política de control de acceso.



Imagen 5. Respuesta GET de política de acceso.

Paso 6. Busque y abra la categoría TimeRange en el Explorador de API para mostrar las diferentes llamadas de API.

cisco. Firepower Device Mar	nager Monitoring Policies Objects Device: firepower							
	StandardAccessList							
FID REST APT	StandardCommunityList							
API Explorer	SyslogServer							
Error Catalog	SystemInformation							
	Telemetry							
	TestDirectory							
	TestIdentityServicesEngineConnectivity							
	TestIdentitySource							
	TimeRange							
	Time Zone Objects							
	TimeZoneSettings							
	TimeZones							
	Token							
	TrafficInterruptionReasons							
	TrafficUser							
	TrafficUserGroup							

ejemplo de formato para crear la ACL basada en tiempo que permite el tráfico desde la zona interna a la zona externa.

Asegúrese de utilizar el ID de objeto de intervalo de tiempo correcto.

```
<#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"
}
```

Nota: eventLogAction debe ser LOG_FIOW_END para registrar el evento al final del flujo; de lo contrario, genera un error.

Paso 12. Implemente los cambios para aplicar la nueva ACL basada en tiempo. El mensaje Cambios pendientes debe mostrar el objeto de intervalo de tiempo utilizado en el paso 10.

er	m	OV					$\bigcirc \bigcirc \bigcirc \bigcirc$	6	
https://10	Pe	ending Chan	ges				0		
Response I	Last Deployment Completed Successfully 19 Jul 2023 07:05 PM. See Deployment History								
{ "versio		Deployed Versi	on (19 Jul 20	23 07:05 PM)	Pending Vers	sion	C) (
"name": "ruleIo	0	Access Rule Added:	test_time_rar	nge					
"source { "ve		-			logFiles: false eventLogAction: ruleId: 26843546 name: test time	LOG_FLOW_END 0 range			
"id		timeRangeObjects:							
"ty }		- sourceZones:			range-obj-2				
Ъ		-			inside_zone				
"destin {		<pre>destinationZones: -</pre>			outside_zone				
"ve "na "io "to	0	Access Policy Edited	I: NGFW-Acce	ess-Policy					
}	MC	DRE ACTIONS V				CANCEL	DEPLOY NOW		
Response (_								

Imagen 12. La ventana Cambios pendientes de FDM muestra la nueva regla.

Paso 13 (opcional). Si desea editar la ACL, puede utilizar el PUT llame y edite el identificador del rango de tiempo.

CISCO. Firepower Device Manager	Monito	ring Policies	Objects	Device: firepo	ower	(Σ)	a
GET	/policy/acce	esspolicies/{parent	tld}/accessrule	s/{objld}			
FTD REST API 🔶	/policy/acce	sspolicies/{parent	tld}/accessrule	s/{objld}			
API Explorer							
Error Catalog Tr Rd	plementation l is API call is not a sponse Class	Notes allowed on the stand (Status 200)	dby unit in an H	A pair.			
	Model Examp	le Value					
	<pre>"name": "s }], "sourceNetwork { "id": "str "type": "s "version": "name": "s }],</pre>	tring" s": [ing", tring", "string", tring"					
Re	sponse Content	Type application/json	*				
Pi	rameters						
	arameter	Value			Description	Parameter Type	Data Ty
P	arentId	(required)				path	string
۰	ojId	(required)				path	string

Imagen 13. Política de acceso llamada PUT.

ejemplo de formato para editar el rango de tiempo, estos ID de rango de tiempo se pueden recopilar mediante el uso de laGET llamada.

<#root>

```
{
"version": "flya3jw7wvqq7",
"name": "test_time_range",
"ruleId": 268435460,
"sourceZones": [
ł
"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"
}
```

Paso 14. Implemente y valide los cambios.

si i "ve	Pending Changes							
"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 Vers	sion	0			
"type": "links" "self	0	Access Rule Edited: test_time_range						
}	0	Access Rule Added: test_time_range_2						
,		-	<pre>logFiles: false eventLogAction:</pre>	LOG_FLOW_END				
ponse (-	ruleId: 26843546 name: test time	1 range 2				
9		timeRangeObjects:						
onse k		-	range-obj-1					
onser		sourcezones:	inside zone					
accent-r		destinationZones:						
cache-cc		-	outside_zone					
"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-	tacti	ion": "1: modesblack"						
x-xss-pro	rect	1017 . 1, MODE-DIOCK						

Imagen 14. La ventana Cambios pendientes de FDM muestra el cambio del objeto.

Verificación

1. Ejecute el show time-range para validar el estado de sus objetos de rango de tiempo.

```
<#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
)□
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).