Configurar uma Regra de Controle de Acesso com Limite de Tempo no FDM com API Rest

Contents

Introdução Pré-requisitos Requisitos Componentes Utilizados Informações de Apoio Configurar Verificar

Introdução

Este documento descreve como configurar e validar uma regra de controle de acesso com base no tempo com API Rest no FTD gerenciado pelo FDM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Threat Defense (FTD)
- FDM (Firepower Device Management, Gerenciamento de dispositivos do Firepower)
- Conhecimento da interface de programação de aplicativo de transferência de estado representacional (REST API)
- Lista de controle de acesso (ACL)

Componentes Utilizados

As informações neste documento são baseadas no FTD versão 7.1.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A API do FTD versão 6.6.0 e posterior suporta regras de controle de acesso que são limitadas com base no tempo.

Usando a API do FTD, você pode criar objetos de intervalo de tempo, que especificam intervalos de tempo únicos ou recorrentes, e aplicar esses objetos às regras de controle de acesso. Usando intervalos de tempo, você pode aplicar uma regra de controle de acesso ao tráfego durante determinados horários do dia ou por determinados períodos de tempo, a fim de fornecer flexibilidade ao uso da rede. Não é possível usar o FDM para criar ou aplicar intervalos de tempo, nem o FDM mostrará se uma regra de controle de acesso tem um

intervalo de tempo aplicado a ela.

Configurar

Etapa 1. Clique nas opções avançadas (menu Kebab) para abrir o FDM API explorer.

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	₫, ₽, ×					

Imagem 1. Interface do usuário da Web do FDM.

Etapa 2. Escolha a categoria AccessPolicy para exibir as diferentes chamadas de API.

ahaha cisco.	Firepower Device N	lanager	题 Monitoring	Ø Policies	∰E Objects	Device: firepower				
FTD RE	STAPI ←	documentatio	on for the resourc	e.	reas through this	s page When you fill in paramete	are and allak the Tay it Out! button you interact directly			
API Explo	pror	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 c								
Error Cat	alog	deployment a The REST AP valid access to Before using You can also NOTE: The p that you use to Cisco makes otherwise imp	 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 InitialProt 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 makes no guarantee that the API version included on this Firepower Threat Device (the "API") will be compatible with future releases. Cisco, a otherwise improve the API based on user feedback. 							
	[AAASettin ASPathLin AccessPon ActiveDim ActiveUse AnyConn AnyConn	ng st olicy ectoryRealm erSessions ectClientPro ectPackagef	file						



Etapa 3. Execute o comando GET para obter a ID da política de acesso.

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

dados do corpo da resposta para um bloco de notas. Posteriormente, você deverá usar a ID da Política de Controle de Acesso.



Imagem 5. Resposta GET da Política de Acesso.

Etapa 6. Localize e abra a categoria TimeRange no API Explorer para exibir as diferentes chamadas de API.

Firepower Device Ma	anager Monitoring Policies Objects Device: firepower							
	StandardAccessList							
	StandardCommunityList							
API Explorer	SyslogServer							
Error Catalog	SystemInformation							
	Telemetry							
	TestDirectory							
	TestIdentityServicesEngineConnectivity							
	TestIdentitySource							
	Time Range							
	Time Zone Objects							
	Time Zone Settings							
	TimeZones							
	Token							
	TrafficInterruptionReasons							
	TrafficUser							
	TrafficUserGroup							

Imagem 6. Categoria de intervalo de tempo.

Passo 7. Crie quantos obietos TimeRange desejar usando a chamada à API **POST**.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.