Configuración de la política de identidad en el Secure Firewall Management Center (FMC)

Contenido

troducción	
rerequisites	
Requirements	
Componentes Utilizados	
onfigurar	
Configuraciones	
erificación	

Introducción

Este documento describe el proceso de configuración e implementación de una política de identidad para un tráfico FTD seguro a través de FMC seguro.

Prerequisites

- 1. Rango ya configurado en FMC.
- 2. Origen de identidad ya configurado: ISE, ISE-PIC.



Nota: las instrucciones de configuración de ISE y de rango no están incluidas en este documento.

Requirements

Cisco recomienda tener conocimiento de estos temas:

- Centro de gestión de firewall seguro (FMC)
- Firewall seguro Thread Defense (FTD)
- Cisco Identity Services Engine (ISE)
- Servidores LDAP/AD
- Métodos de autenticación
- 1. Autenticación pasiva: uso de una fuente de usuario de identidad externa, como ISE
- 2. Autenticación activa: uso del dispositivo administrado como fuente de autenticación (portal cautivo o acceso VPN remoto)

3. Sin autenticación

Componentes Utilizados

- Secure Firewall Management Center para VMWare v7.2.5
- Cisco Secure Firewall Threat Defence para VMWare v7.2.4
- Servidor de directorio activo
- Cisco Identity Services Engine (ISE) v3.2, parche 4
- Método de autenticación pasiva

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.

Configurar

Configuraciones

Firewall Management Center Overview / Dashboards / Dashboard ०, 🔮 🌣 🚳 admin 🔹 👶 SECURE Analysis Policie Devices Overview Objects Integration Access Co ork Dise Access Contro Application Dete Summary Dashboard Intrusion Scanner Malware & File DNS • II Identity Add Widgets Prefilte - × - × ► Traffic by Ann - × Traffic by Busin No Data No Data

Paso 1.En la GUI de FMC , vaya a Políticas > Control de acceso > Identidad

Paso 2. Haga clic en Nueva directiva.

Firewall Management Center Policies / Access Control / Identity	Overview	Analysis	Policies	Devices	Obje	cts Integration		Deploy	۹ (ہ 😢	🕢 admin	cisco SECURE
									0	bject Ma	nagement	Access Control
										Com	quare Policies	New Policy
Identity Policy						Domain	Status	Last Modified				
						There are no policies created. Add a new policy						

Paso 3. Asigne un nombre y una descripción a la nueva política de identidad y, a continuación, haga clic en Guardar.

Firewall Management Center Policies / Access Control / Identity Overview A	nalysis Policies Devices Obje	icts Integration		Deploy 🔍 💕 🌣 🔞 admin	cisco SECURE
				Object Management	Access Control
				Compare Policies	New Policy
Identity Policy		Domain	Status	Last Modified	
		There are no policies created. Add a new policy			
		New Identity policy			
		Name Identity Test			
		Description			
		Identity Policy Lab			
		Cancel			

Paso 4. Haga clic en el icono + Agregar regla.

- 1. Asigne un nombre a la nueva regla.
- 2. En el campo name (nombre), elija el método de autenticación y seleccione : Passive Authentication (Autenticación pasiva).
- 3. A la derecha de la pantalla, seleccione Realm & Settings (Dominio y parámetros).

Firewall Management Center Policies / Access Control / Identity Policy	Editor Overview Analysis Policies Devices Objects Integ	gration	Deploy	९. 💕 🌣 🕘 admin 🛛 🔤 🐝 SECURE
Identity Test Identity Policy Lab				Save Cancel
Rules Active Authentication Identit	Add Rule		Θ	
Name Administrator Rules	Name Insert Test Identity Policy Insert Passive Authentication • •	Standard Rules totocol: HTTP Basic Exclude HTTP User-Agent	a: None	e Q. Search Rules X Auth Protocol
This category is empty Standard Pules	Zones Networks VLAN Tags Ports		Realm & Settings	
This category is empty	Available Zones C Sour	arce Zones (0)	Destination Zones (0)	
Root Rules	Q. Search by name any	У	any	
This category is empty	inside Add to Source			
	outside Add to Destination			
			Cancel Add	
			No	data to display $ \langle \langle Page 1 0 0 1 \rangle \rangle \subset C$

4. Seleccione un rango en el menú desplegable.

Firewall Management Cente Policies / Access Control / Identity Policy	r Editor Overview Analysis Policies Devices Objects Integration	Deploy Q 💞 🌣 🛛 admin 🔹 🕬 SECURE
Identity Test Identity Policy Lab		Save Cancel
Rules Active Authentication Identit	Add Rule	•
Name Administrator Rules	Name Insert Test Identity Policy Insert Into Category Into Category Standard Rules Into Category Into	e Q. Search Rules X Auth Protocol
Standard Rules This category is empty Root Rules This category is empty	Realm • AD (AD) Use active authentication if passive or VPN identity cannot be established	
	* Required Field	
		Cancel Add
		No data to display $ < < Page 1$ of $1 > > C$

5. Haga clic en Zones a la izquierda de la pantalla.

6. En el menú Zonas disponibles, asigne una zona de origen y de destino basada en la ruta de tráfico necesaria para detectar usuarios. Para agregar una zona, haga clic en el nombre de la zona y, a continuación, seleccione en función del caso Add to Source o Add to Destination.



Nota: En esta documentación, la detección de usuarios se aplicará solo para el tráfico que proviene de la zona interna y se reenvía a la zona externa.

7. Seleccione Agregar y Guardar.

Firewall Management Center Policies / Access Control / Identity Policies	If Overview Analysis Policies Devices Objects Integration Deploy	Q 🚱 🌣 🙆 admin∙ 🔤 🖏 SECURE
Identity Test Identity Policy Lab		Save Cancel
Rules Active Authentication Identit	Add Rule	
Name Administrator Rules	Name Insert Test Identity Policy Into Category Insert Passive Aurthentication • Realm: AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None	e Q. Search Rules X
This category is empty	Zones Networks VLAN Tags Ports Realm & Settings	
Standard Rules This category is empty	Available Zones C Source Zones (1) Destination Zones (1)	
Root Rules	Q. Search by name inside outside Inside Add to Source	
This category is empty	outside Add to Destination Cancel Add	
	Ne	data to display $ \langle \langle Page 1 \rangle $ of $1 > C$

Paso 5. Valide que la nueva regla está en la política de identidad y haga clic en Guardar.

Firewall Management O Policies / Access Control / Identity	Center a y Policy Editor	Verview Analysis	Policies Device	es Objects	Integration				Deploy Q 🗳 🌣	admin deater SE	CURE
Identity Test									You have unsaver	changes Save C	ancel
Identity Policy Lab											
Rules Active Authentication	Identity Source										
								+ Add Category	+ Add Rule Q. Se	arch Rules	×
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol	
Administrator Rules											
This category is empty											
Standard Rules											
1 Test Identity Policy	inside (Routed)	outside (Routed)	any	any	any	any	any	AD (AD)	Passive Authentication	none	11
Root Rules											
This category is empty											
									Displaying 1 - 1 of 1 rules	I< < Page 1 of 1 >	NC

Paso 6. Vaya a Políticas > Control de acceso

Paso 7. Identifique la política de control de acceso que se va a implementar en el firewall que administra el tráfico de usuarios y haga clic sobre el icono del lápiz para editar la política.

þ	Firewall Management Center Policies / Access Control / Access Control	ew Analysis	Policies C	Devices Obje	cts Integration		Deploy 🔍 🍪 🔅 🕲 admin	enco SECURE
						Object Management	Intrusion Network Analysis Policy DNS	Import/Export
								New Policy
	Access Control Policy	Domain			Status	Last Modified	Lock Status	
	Test Policy	Global			Targeting 1 devices Up-to-date on all targeted devices	2024-01-31 20:50:00 Modified by "admin"		% 0 ∕ ¥

Paso 6. Haga clic en None en el campo Identity Policy.

In the second secon	Ę	Firewall M Policies / Acce	anagement rss Control / Polic	Center y Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	¢ 🔮 م	🕜 adm	iin • 🕴	nde SEC	URE
Rules Security Intelligence HTTP Responses Loggin Advanced Philip Assignments (1) Rules Security Intelligence HTTP Responses Loggin Advanced * Name SSL Policy: None SSL Policy: None Identify Policy: Assignments (1) Elter.by.Denice * Secure 2 nones Dest Zones Source 2 + Add Category	n î	Test Polic	y											Try Ne	w UI Layout 🍞	Analyze Hit	Counts		Can	cel
Ellere by: Derice Y Search Rules X Source Add Category + Add Cate	F	Rules Security	Intelligence	HTTP Responses	Logging	Advanced	đ						F	Prefilter Policy: prefil	er_marpatin	Inheritanc SSL Policy:	e Settings None	Policy A	y Policy:	nts (1) None
Name Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applications Source Ports Dest Ports URLs Source Dynamics Destination Dynamics Action R • R • R • R • R • R • R • R • R • R •	Filt	er by Device	Y Search Rules											×	Show Rule Cor	nflicts 🛛 +	Add Cate	pory	+ Add i	Rule
✓ Mandatory - Test Policy (1-2) 1 Allow, to_outside inside outside any-ipv4 any-ipv4 Any	,	Name	Source Zones	Dest Zones	Source Networks	Dest	Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	n, e	ធុ∠ខ្		o
1 Allow_to_outside inside outside any-lov4 any-lov4 Any	$\sim N$	fandatory - Test Po	licy (1-2)																	
2 Allow_to_inside outside inside any-ipv4 any-ipv4 Any	1	Allow_to_outside	inside	outside	any-ipv4	any-i	ipv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow	F5 0	6 A 0	0	11
Default - Test Policy (-) There are no rules in this section. Add Rule or Add Category	2	Allow_to_inside	outside	inside	any-ipv4	any-i	pv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow	15 0	4 A 5	3 [] 0	11
There are no rules in this section. Add Rule or Add Category	∨ D	efault - Test Policy	(-)																	
	The	re are no rules in th	his section. Add R	Rule or Add Categ	pory															

Default Action	Access Control:Block all traffic	•	8
	Displaying 1 - 2 of 2 rules < < Page 1 of 1 > > ♂ Rules per page: 100		ì.

Paso 7. En el menú desplegable, seleccione la política creada anteriormente en el paso 3 y, a continuación, haga clic en Aceptar para finalizar la configuración.

	Firewall Management Center Policies / Access Control / Policy Editor Devices Devices Objects Integration Devices Objects Integration Device Access Control / Policy Editor																
	Test Policy											Try №	lew UI Layout 🗩	Analyze Hit	Counts Save	Cancel	
	Rules Security In	elligence Hi	TTP Responses	Logging Ad	vanced							Prefilter Policy: pre	filter_marpatin	Inheritanc SSL Policy:	e Settings Policy / None Identif	Assignments ty Policy: Nor	(1) ne
E	Iter by Device	Search Rules										×	Show Rule Co	nflicts 🛛 🕂	Add Category	+ Add Rule	
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	15 0 15 A		0
~ 1	Mandatory - Test Polic	y (1-2)															
1	Allow_to_outside	inside	outside	any-ipv4	any-ipv4	Any	Any	Any	Any	Any				C Allow	5 0 G A C	S 🖬 o 🖊	1
2	Allow_to_inside	outside	inside	any-ipv4	any-ipv4	Any	Identity Policy	/		0				C Allow	5 0 5 2 1	a 🛛 o 🖊	1
~	Default - Test Policy (-)								_							
Th	ere are no rules in this	section. Add Rul	le or Add Category			\rightarrow	Identity Test		• •								
										_							
							Revert to Default:	5	Cancel	ок							
							_	_		_							
Def	ault Action												Access Cor	ntrol:Block all tr	affic	*	
											Disate				ulas pas pages 100		5
											Display	ing t = 2 of 2 rules <	CPage 1 0	C N	uies per page: 100		

Paso 8. Guardar e implementar la configuración en el FTD.

Verificación

1. En la GUI de FMC, navegue hasta Análisis > Usuarios: Sesiones activas

No Search Constraints (Edit Sea	rch)												
Table View of Active Sessions	Active Sessions												
Jump to													
4 Login Time ×	Last Seen ×	User ×	Authentication Type ×	Current IP ×	Realm ×	Usemame x	First Name ×	Last Name ×	E-Mail ×	Department ×	Phone ×	Discovery Application ×	Device ×
· 2024-01-09 15:20:06	2024-01-31 16:21:08	🛓 sfua (LDAP\sfua, LDAP)	Passive Authentication	10.4.23.129	LDAP	sfua	sfua		sfua@jorgeju.local	users (jorgeju)		🗆 LDAP	firepower

3. Validación de Análisis > Conexión> Eventos: Vista de tabla de los eventos de Conexiones

 Sea 	arch	Constraints (Edit Sear	rch Save Se	earch)														
Conr	necti	ons with Application D	Details	Table View	of Connect	ion Events												
Jump	p to																	
		4 First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	Initiator x Country x	Initiator User ×	Responder _×	Responder x Country	Security Intelligence × Category	Ingress Security × Zone	Egress Security × Zone	Source Port / ICMP x	Destination Port x	SSL ×	Application x Protocol	Client ×
• 1	0	2024-01-31 16:26:46		Allow		10.4.23.129		1 stua (LDAP(stua, LDAP)	0 10.6.11.5			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	CMP client
•		2024-01-31 16:26:45		Allow		10.4.23.129		1 stua (LDAP\stua, LDAP)	0 10.6.11.4			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client
•		2024-01-31 16:26:44		Allow		10.4.23.129		1 stua (LDAP\stua, LDAP)	0 10.6.11.3			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client
*		2024-01-31 16:26:23		Allow		10.4.23.129		1 stua (LDAP\stua, LDAP)	10.6.11.2			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client



Nota: Los usuarios que coinciden con los criterios de tráfico de la política de identidad y la política de control de acceso muestran su nombre de usuario en el campo Usuario.

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).