Configure Identity Policy on Secure Firewall Management Center (FMC)

Contents

Introduction	
<u>Prerequisites</u>	
Requirements	
Components Used	
Configure	
Configurations	
<u>Verify</u>	

Introduction

This document describes the process of how to configure and deploy an Identity Policy for a Secure FTD traffic through Secure FMC.

Prerequisites

- 1. Realm already configured in FMC.
- 2. Identity Source already Configured ISE, ISE-PIC.



Note: ISE and Realm configurations instructions are out of the scope of this document.

Requirements

Cisco recommends having knowledge of these topics:

- Secure Firewall Management Center (FMC)
- Secure Firewall Thread Defense (FTD)
- Cisco Identity Services Engine (ISE)
- LDAP/AD servers(s)
- Authentication Methods
- 1. Passive Authentication : Use of external identity user source such as ISE
- 2. Active authentication : Use of the managed device as Authenticate source (captive portal or remote vpn acess)
- 3. No Authentication

Components Used

- Secure Firewall Management Center for VMWare v7.2.5
- Cisco Secure Firewall Threat Defense for VMWare v7.2.4
- Active Directory Server
- Cisco Identity Services Engine (ISE) v3.2 patch 4
- Passive Authentication Method

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Configurations

Firewall Management Center Overview / Dashboards / Dashboard Overview Analysis	olicies Devices Objects Integration		Deploy Q 修 🔅 (admin • deade SECURE
Summary Dashboard (restin: dashboard) Provides a summary of activity on the appliance Network × Threats Intrusion Events Status Geolocation	Access Control Network Discovery Actions Access Control Application Detectors Alerts Intrusion Correlation Scanners Malware & File Groups Modules Identity Instances SSL Prefiter Frefiter Frefiter	- X	Show the Last 1 hour	Reporting II Add Widgets - ×
Last updated 4 minutes ago	Application Application Strip Basel Strip Control Strip Control Contro	 Total Bytes (KB) 43.33 16.41 5.02 1.70 0.52 	Application Cross Secure Endpoint Kontense Econop Control Econop	 Total Bytes (KB) 63.33 6.46 5.02 1.20
Risk Total Bytes (KB) Madum 1,345.80 Very Low 2297.22 High 6.33 Last updated 4 minutes app	Last updated 4 minutes age Top Server Applications Seen	- ×	Last updated 4 minutes ago Top Operating Systems Seen	- ×
Traffic by Business Relevance Business Relevance Votal Bytes (KB)	× No Data		No Data	

Step 1.In the FMC GUI, Navigate to Policies > Access Control > Identity

Step 2. Click New Policy.

Firewall Management Center Policies / Access Control / Identity	Overview	Analysis	Policies	Devices	Obje	cts Integration		Deploy	۹ (\$ \$ \$	admin •	tisce SECURE
									Ot	oject Mana	gement /	Access Control
										Compa	ire Policies	New Policy
Identity Policy						Domain	Status	Last Modified				
						There are no policies created. Add a new policy						

Step 3. Assign a name and description to the new Identity Policy, then click Save.

Firewall Management Center Overview	Analysis Policies Devices	Objects Integration		Deploy Q 💕 🌣 🎯 admin 🕶 🕬 SECU
				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		

Step 4. Click on + **Add Rule** Icon.

- 1. Assign a name to the new rule.
- 2. Under the name field, choose the authentication method, select : Passive Authentication.
- 3. At the right of the screen select **Realm & Settings.**

Firewall Management Center Policies / Access Control / Identity Policy	r Overview Analysis Editor	Policies Devices Objects	Integration	Deploy	Q 🚱 ✿ @ admin∙ 🕬 Secure
Identity Policy Lab					
Rules Active Authentication Identit	Add Rule			0	
	Name	Insert			e 🔍 Search Rules 🛛 🗙
Name	People Authority Policy	Enabled into Category	Standard Rules Standard Rules	•	Auth Protocol
Administrator Rules	Passive Authentication •	Ream: No ream Authenticatio		nis wore	
This category is empty	Zones Networks VLAN Tags	Ports		Realm & Settings	
Standard Rules	Available Zones C		Source Zones (0)	Destination Zones (0)	-
This category is empty	Q. Search by name		any	any	
This category is empty	inside				
	outside	Add to Destination			
				Cancel	
				No	o data to display $ \langle \langle Page 1 \rangle 0 \rangle$ of $1 > 0 \rangle$

4. Select a **Realm** from the drop down menu.

Firewall Management Center Policies / Access Control / Identity Policy	r Editor Overview Analysis Policies Devices Objects Integration	Deploy 🔍 💞 🌣 🎯 admin 🛛 🕬 SECURE
Identity Test Identity Policy Lab		Save Cancel
Rules Active Authentication Identit	Add Rule	0
Name	Name Insert Test Identity Policy Into Category Standard Rules Passive Authentication • 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 Rook Rules This category is empty	Realm * AD (AD) Use active authentication if passive or VPN identity cannot be established	
	* Required Field	
		Cancel
		No data to display $ <<$ Page 1 of 1 $>$ > C

5. Click on **Zones** at the left of the screen.

6. From the **Avaliable Zones** menu assign a **source** and **destination** zone based in the traffic path that is needed to detect users. To add a zone click on the name of the zone and then select depending on the case **Add to Source** or **Add to Destination**.



Note: In this documentation the user detection is going to be applied only for the traffic comes from the inside zone and it is forwarded to the outside zone.

7. Select Add and Save.

Firewall Management Center Policies / Access Control / Identity Policy	r Verview Analysis Policies Devices Objects Integration Deploy	역, 🚱 🌣 🔕 admin • 🔤 👯 SECURE
Identity Test Identity Policy Lab		Save Cancel
Rules Active Authentication Identit	Add Rule 🔮	
Name Administrator Rules	Name Insert Test Identity Policy ✓ Enabled Into Category ▼ Passive Authentication ▼ Realm: AD (AD) Authentication Protocot: HTTP Basic Exclude HTTP User-Agents: None	Q Search Rules X Auth Protocol
This category is empty Standard Pulse	Zones Networks VLAN Tags Ports Realm & Settings	
Standard Rules This category is empty Roof Rules This category is empty	Available Zones (2 Q: Search by name Inside Outside Add to Source Add to Destination Add to Destination	
	Cancel	data to display. 17 C. Page 1

Step 5. Validate the new Rule is in the Identity Policy and click on Save.

Ę	Firewall Management Cen Policies / Access Control / Identity Policies	nter Ov bicy Editor Ov	verview Analysis	Policies Device	es Objects I	ntegration				Deploy Q 🔮 🌣	@ admin • disce	SECURE
- 10	dentity Test									You have unsav	ed changes Save	Cancel
lo	lentity Policy Lab											
	Rules Active Authentication Iden	ntity Source										
									+ Add Category	+ Add Rule Q S	earch Rules	×
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol	
4	Administrator Rules											
	This category is empty											
3	Standard Rules											
	Test Identity Policy	inside (Routed)	outside (Routed)	any	any	any	any	any	AD (AD)	Passive Authentication	none	/1
1	Root Rules											
	This category is empty											
										Displaying 1 - 1 of 1 rules	I< < Page 1 of 1	1>>IC

Step 6. Navigate to Policies > Access Control

Step 7. Identify the **Access Control Policy** that it is going to be deployed in the Firewall handling the users traffic and **click** over the **pencil icon** in order to edit the policy.

Ę	Firewall Management Center Policies / Access Control / Access Control	verview	Analysis	Policies	Devices	Object	s Integration				Dep	loy Q 💰	🔅 🛛 admin 🕇	enco SECURE
										Object Management	Intrusion	Network Analy:	sis Policy DNS	Import/Export
														New Policy
	Access Control Policy		Domain				Status	Last Mo	dified		Lock Status			
	Test Policy		Global				Targeting 1 devices Up-to-date on all targeted devices	2024-01 Modified	-31 20:50:00 by "admin"					¶a 8 ∕¥

Step 6. Click on None in the Identity Policy field.

Default Action

ę	Firewall Ma Policies / Acces	anagement (is Control / Policy	Center Editor	Overview An	nalysis Policies	Devices	Objects	Integration					Deploy	Q 🔮 :	🗘 🔞 adm	in • dudu	SECURE
•	Test Policy											Try N	iew UI Layout 🗇	Analyze H	lit Counts	Save	Cancel
R	les Security Ir	ntelligence H	ITTP Responses	Logging	Advanced							Prefilter Policy: pref	ilter_marpatin	Inherita SSL Polic	nce Settings y: None	Policy Assir Identity Po	ionments (1) olicy: None
Filte	by Device	Search Rules										×	Show Rule Co	onflicts Ø	+ Add Cates	jory +	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	R, 0	B_& ⊠	a = 0
$\sim M_{\rm f}$	ndatory - Test Poli	cy (1-2)															
1	Allow_to_outside	inside	outside	any-ipv4	any-ipv4	Any	Any	Any	Any'	Any	Any	Any	Any	C Allow	E 0	4 A 🗆 🖡	
2	Allow_to_inside	outside	inside	any-ipv4	any-ipv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow	15 O	4 A 🗆 I	0/1
$\sim \text{De}$	ault - Test Policy ((-)															
Ther	are no rules in thi	s section. Add R	ule or Add Categ	ory													

Step 7. From the Drop down menu, select the Policy created previously in step 3, then, click OK to finish the configuration.

•

Access Control:Block all traffic
 Access Controlitiock air trainc
 V

 Displaying 1 - 2 of 2 rules
 I

 I
 I

 I
 I

Try New II Larger () Analyze HI Con	nts Save Cancel
Rules Security Intelligence HTTP Responses Logging Advanced Prefilter_marpatin SSL Policy: Prefilter_marpatin SSL Policy: No	ettings Policy Assignments (1) lidentity Policy: None
Eller, by Device 🝸 Search Rules X	id Category + Add Rule
B Name Source Zones Dest Zones Dest Zones Dest Networks VLAN Tags Users Applications Source Ports Dest Ports URLs Source DestInation Dynamic Attributes Attributes	
Mandatory - Test Policy (1-2)	
1 Allow_to_outside inside outside any-ipv4 Any	5 @ 5 A B B O / P
2 Allow_to_inside outside inside any-ipv4 Any Identity Policy	5 @ B & B B B • / 🗑
v Default - Test Policy (-)	
There are no rules in this section. Add Rule or Add Category Mertily Test	
Revert to Defaults Cancel OK	
Default Action Access Control-Block all traffic	•
Displaying 1 - 2 of 2 rules < < Page 1 of 1 > > C Rules	per page: 100 🔹

Step 8. Save and deploy the configuration to the FTD.

Verify

1. In the FMC GUI navigate to Analysis > Users: Active Sessions

No Sea	rch Constraints (Edit Searc	h)												
Table	View of Active Sessions	Active Sessions												
Jump	to													
6	4 Login Time ×	Last Seen ×	User ×	Authentication Type ×	Current IP ×	Realm ×	Usemame X	First Name ×	Last Name ×	E-Mail ×	Department ×	Phone ×	Discovery Application ×	Device ×
• 0	2024-01-09 15:20:06	2024-01-31 16:21:08	💄 sfua (LDAP\sfua, LDAP)	Passive Authentication	0.4.23.129	LDAP	sfua	sfua		sfua@jorgeju.local	users (jorgeju)		🗆 LDAP	frepower

3. Validation from Analysis > Connection> Events: Table view of Connections events

																		E-April	
	Search	Constraints (Edit Sear	ch Save Si	Table View	of Connect	ion Functo													
	onneci	ions with Application L	Actails -	Table view	or connect	Jon Events													
J	ump to.	2																	
		4 First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	initiator x Country x	Initiator User ×	Responder _X	Responder × Country	Security Intelligence × Category	Ingress Security × Zone	Egress Security × Zone	Source Port / ICMP x Type	Destination Port x	SSL Status ×	Application x Protocol	Client ×	CI Ve
		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		I ICMP	ICMP client	
٠		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)	10.6.11.3			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client	
٠		2024-01-31 16:26:23		Allow		10.4.23.129)	🛦 stua (LDAP\stua, LDAP)	0 10,6.11.2			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp			CMP client	



Note: Users matching the traffic criteria for the Identity Policy and Access Control Policy are shown their username in the User field.