在安全防火牆管理中心(FMC)上配置身份策略

目錄		
<u>簡介</u>		
<u>必要條件</u>		
<u>需求</u>		
<u>採用元件</u>		
<u>設定</u>		
<u>組態</u>		
<u>驗證</u>		

簡介

本檔案介紹如何透過安全FMC為安全FTD流量設定和部署辨識原則的程式。

必要條件

1. 已在FMC中配置領域。

2. 已配置身份源- ISE、ISE-PIC。



注意:ISE和領域配置說明不在本文檔的討論範圍之內。

需求

思科建議瞭解以下主題:

- 安全防火牆管理中心(FMC)
- 安全防火牆執行緒防禦(FTD)
- 思科身分辨識服務引擎(ISE)
- LDAP/AD伺服器
- 驗證方法
- 1. 被動身份驗證:使用外部身份使用者源,例如ISE
- 2. 主動身份驗證:將受管裝置用作身份驗證源(強制網路門戶或遠端VPN訪問)
- 3. 無身份驗證

採用元件

- 適用於VMWare v7.2.5的安全防火牆管理中心
- 適用於VMWare v7.2.4的思科安全防火牆威脅防禦
- Active Directory伺服器
- 思科身份服務引擎(ISE) v3.2修補4
- 被動驗證方法

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

組態

第1步:在FMC GUI中,導航到策略>訪問控制>身份

Firewall Management Center	luenciew Analysis Dulie	ins Devices Objects Integration		Danlay O	🖉 🗿 admin 🖌 deb accurr			
Overview / Dashboards / Dashboard	Pone Pone	overses overses mogration		nation of	CISCO SECORE			
Summary Dashboard /which deathoard/ Provides a summary of activity on the applance Network × Threats Intrusion Events Stat	tus Geolocation DN Iss	cess Control Network Discovery ccess Control Application Detectors rusion Correlation alware & File IS SL	Actions Alerts Scanners Groups Modules Instances	Show the Last	Reporting 1 hour •			
 Unique Applications over Time 	Pri	efilter	- :	➤ Top Client Applications Seen	- ×			
traffic by Application Risk Risk Medium Very Use	- × + Total Bytes (KB) 1,241.0 297.32	Application InTTP Turnal SHN-3-unencrypted CCLARC Campo CCLARC Last updated 4 minutes app	▼ Total Bytes (KB) 63.3 10.41 5.02 1.20 0.92	Application Crace Secure Response Crace Secure Response Craceses C	 ▼ Total Bytes (KB) 63.33 6.46 5.02 1.20 			
High	63 <mark>.33</mark>	 Top Server Applications Seen 	-	➤ Top Operating Systems Seen	- ×			
Last updated 4 minutes app Traffic by Business Relevance Business Relevance	– X • Total Bytes (KB)	No Data		No Da	a			
Business Relevance	▼ Total Bytes (KB)							

步驟2.按一下New Policy。

Firewall Management Center Policies / Access Control / Identity	Overview	Analysis	Policies	Devices	Obje	ts Integration		Deploy	۹.	¢ 🕫	🛛 admin •	disco SECURE
									o	bject M	anagement	Access Control
											iquite i oncies	income states
Identity Policy						Domain	Status	Last Modified				
						There are no policies created. Add a new policy						

第3步:為新Identity Policy分配名稱和說明,然後按一下Save。

Firewall Management Center Overview Anal Policies / Access Control / Identity Overview	lysis Policies Devices Obje	cts Integration		Deploy 🔍 💕 🌣 🎯 admin 🔻	cisco SECURE
				Object Management	Access Control New Policy
Identity Policy		Domain	Status	Last Modified	
		There are no policies created. Add a new policy			
		New Identity policy			
		Name			
		Description			
		Identity Policy Lab			
		Cancel			

步驟 4.點選+增加規則圖示。

- 1. 為新規則指定名稱。
- 2. 在name欄位下,選擇身份驗證方法,選擇Passive Authentication。
- 3. 在熒幕右邊選取範圍與設定。

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 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 - 0 0 - 0 $

4.從下拉式功能表中選取範圍。

Firewall Management Center 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 ✓ Enabled Into Category ✓ Standard Rules ▼ Passive Authentication ▼ Realm: AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None	Q. Search Rules X Auth Protocol
This category is empty Standard Rules This category is empty Roof Rules This category is empty This category is empty	Zones Networks VLAN Tags Ports Realm • AD (AD) • O Use active authentication if passive or VPN identity cannot be established •	Ream & Settings
	* Required Field	
		Cancel Add
		No data to display $ < < Page 1 $ of $1 > > C$

5. 按一下螢幕左側的Zones。

6. 從可用區域選單中,根據檢測使用者所需的流量路徑分配源和目標區域。要增加區域,請點選區 域的名稱,然後根據具體情況,選擇Add to Source或Add to Destination。



注意:在本文檔中,使用者檢測僅應用於來自內部區域的流量,並且該流量被轉發到外部 區域。

7. 選擇增加和儲存。

Firewall Management Cente Policies / Access Control / Identity Policy	Glor Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🗘 🔕 admin v 📩 📩 SECURE
Identity Test Identity Policy Lab		Sine
Rules Active Authentication Identit	Add Rule	0
Name Artininistrator Bulas	Name Insert Test Identity Policy Enabled Into Category Passive Authentication • Realm: AD (AD) Authentication Protocol: HTTP	Standard Rules Standard Rules Auth Protocol
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	autside a
This category is empty	Inside Add to Source	
	Add to Destination	
		Cancel
		No data to display < < Page 1 of 1 > > C

步驟 5.驗證新規則是否在身份策略中,然後按一下Save。

l	irewall Management lolicies / Access Control / Identi	Center d ity Policy Editor	Overview Analysis	Policies D	Devices Objects I	ntegration				Deploy Q 💕 🕻	admin 🕶 🔤	SECURE
Ident	ity Test									You have unsa	ved changes Save	Cancel
Identity P	Policy Lab											
D. I. I.		11										
Rules	Active Authentication	identity Source										
									+ Add Category	+ Add Rule Q	Search Rules	\times
Na	me	Source Zones	Dest Zones	Source Network	us Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol	
Adminis	strator Rules											
This ca	stegory is empty											
Standar	d Rules											
1 Test	Identity Policy	inside (Routed)	outside (Routed)	any	any	any	any	any	AD (AD)	Passive Authentication	0000	11
Root Ru	les											
This ca	itegory is empty											
										Displaying 1 - 1 of 1 rule	s I< < Page 1 o	1>>IC

步驟 6. 導航到策略>訪問控制

步驟 7.確定它將在處理使用者流量的防火牆中部署的訪問控制策略,並按一下超過鉛筆圖示以編輯 策略。

Ę.	Policies / Access Control / Access Control Overvi	iew A	Analysis P	Policies Devices	Obje	cts Integration		Deploy 🔍 💕 🌣 🎯 admin 🕯	cisco SECURE
							Object Management	Intrusion Network Analysis Policy DNS	Import/Export
									New Policy
	Access Control Policy	D	Domain			Status	Last Modified	Lock Status	
	Test Policy	Gió	lobal			Targeting 1 devices Up-to-date on all targeted devices	2024-01-31 20:50:00 Modified by "admin"		% 8∕¥

步驟 6. 在Identity Policy欄位中按一下None。

Ę	Firewall Ma Policies / Acces	inagement C s Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	¢ 🔮	🕜 adı	nin 🕶	obide S	ECUR	£
•	Test Policy												Try Ne	w UI Layout 🍽	Analyze Hit Co	ounts		0	Cancel	1
R	Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: prefilter_marpatin SSL Policy: None Identity Policy: None																			
Filt	er by Device	Search Rules											×	Show Rule Cor	flicts 🛛 🕂 🖊	dd Cate	gory	+ Ad	id Rule	L
	Name	Source Zones	Dest Zones	Source Networks	Des	t Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action	r, e	6 , <u>2</u>			0
$\sim M$	andatory - Test Poli	cy (1-2)																		
1	Allow_to_outside	inside	outside	any-ipv4	any	-ipv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow	$\Pi_0^- = 0$	B .2	I	0 /	Ŷ.
2	Allow_to_inside	outside	inside	any-ipv4	any	-lpv4	Any	Any	Any	Any	Any	Any	Any	Any	C Allow	F5 0	B . A	•	0/	¥
$\sim \mathrm{D}$	efault - Test Policy (-)																		
The	n an na ndas is thi	s section Add D	in or Add Cate	000																

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

步驟 7.從下拉選單中選擇之前在步驟3中建立的「Policy」,然後按一下OK以完成配置。

	Firewall Management Center Policies / Access Control / Policy Editor Dverview Analysis Policies Devices Objects Integration Deploy Q 🥩 🌣 🕢 admin v 🖏 SECURE																
	Test Policy											Try №	New UI Layout	Analyze Hit	Counts Save	Cancel	
	Rules Security In	elligence H	TTP Responses	Logging Ad	lvanced							Prefilter Policy: pre	filter_marpatin	Inheritanc SSL Policy:	e Settings Policy None Identi	Assignments ity Policy: No	.(1) ine
E	Eller by Device 🛛 Show Rule Conflicts 🕢 + 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 V I5 A		0
~1	Mandatory - Test Polic	y (1-2)															
1	Allow_to_outside	inside	outside	any-ipv4	any-ipv4	Any	Acty	Any	Any	Any				C Allow	5.05.2	S 🛛 • 🖊	T
2	Allow_to_inside outside inside any-ipv4 any-ipv4 Any						Identity Policy	/		0				C Allow	15 W IS AL		1
~ [Default - Test Policy (-)															
Th		section. Add Rul	le or Add Category			\rightarrow	Identity Test	Identity Test									
							Revert to Default	5	Cancel	ОК							
										_							
Def	ault Action												Access Cor	trol:Block all tr	affic	*	10
											Displayi	ng 1 - 2 of 2 rules <	< Page 1 o	R	ules per page: 100		*

步驟8.儲存並部署組態至FTD。

驗證

1. 在FMC GUI中,導航至分析>使用者:活動會話

No Sean	ch Constraints (Edit Searc	h)												
Table View of Active Sessions		Active Sessions												
Jump t	0													
	4 Login Time ×	Last Seen ×	User X	Authentication Type ×	Current IP ×	Realm ×	Usemame X	First Name ×	Last Name ×	E-Mail ×	Department ×	Phone x	Discovery Application ×	Device ×
•	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. 從分析>連線>事件:連線事件的表格檢視進行驗證

Search Constraints (Edit Search Save Search)														C.Agran Auto					
Conn	ections v	with Application D	Details	Table View	of Connect	ion Events													
Jump	to																		
) + R	irst Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	Initiator x Country x	Initiator User ×	Responder _×	Responder ×	Security Intelligence × Category	Ingress Security × Zone	Egress Security × Zone	Source Port / ICMP x Type	Destination Port x	SSL × Status	Application x Protocol	Client ×	C V
• 0	2024	-01-31 16:26:46		Allow		口 10.4.23.129		1 stua (LDAP\stua, LDAP)	10.6.11.5			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	CMP client	
• [2024	-01-31 16:26:45		Allow		C 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	CMP client	
• 0	2024	-01-31 16:26:44		Allow		10.4.23.129		🌲 stua (LDAP\stua, LDAP)	0 10.6.11.3			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	CMP client	
• [2024	1-01-31 16:26:23		Allow		10.4.23.129		👗 sfua (LDAP\sfua, LDAP)	0 10.6.11.2			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	CMP client	



注意:與「身份策略」和「訪問控制策略」的流量條件匹配的使用者在其使用者名稱欄位 中顯示。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。