在安全防火墙管理中心(FMC)上配置身份策略

目:	录	
<u>简介</u>		
<u>先决</u>		
要	<u>求</u>	
<u>使</u>	<u>用的组件</u>	
<u>配置</u>		
西		
验证		

简介

本文档介绍如何通过安全FMC为安全FTD流量配置和部署身份策略的流程。

先决条件

1. 已在FMC中配置领域。

2. 已配置身份源- ISE、ISE-PIC。



注意:ISE和领域配置说明不在本文档的讨论范围之内。

要求

思科建议了解以下主题:

- 安全防火墙管理中心(FMC)
- 安全防火墙线程防御(FTD)
- 思科身份服务引擎(ISE)
- LDAP/AD服务器
- 身份验证方法
- 1. 被动身份验证:使用外部身份用户源(例如ISE)
- 2. 主动身份验证:将受管设备用作身份验证源(强制网络门户或远程vpn访问)
- 3. 无身份验证

使用的组件

- 适用于VMWare v7.2.5的安全防火墙管理中心
- 适用于VMWare v7.2.4的思科安全防火墙威胁防御
- Active Directory 服务器
- 思科身份服务引擎(ISE) v3.2补丁4
- 被动身份验证方法

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

配置

第1步:在FMC GUI中,导航至策略>访问控制>身份

Firewall Management Center Overview Analysis	olicies Devices Objects Integration		Deploy Q 💕 🖏	admin •
Uverview / Dashboards / Dashboard				-
Summary Dashboard Issuith.disationed Provides a summary of activity on the applance Network × Network × Threats Intrusion Events Status Geolocation	Access Control Network Discovery Actions Access Control Application Detectors Alerts Intrusion Correlation Scanners Malware & File Groups DNS Modules Identity SSL		Show the Last 1 hou	Reporting r II Add Widgets
Unique Applications over Time	Prefilter	- ×	▶ Top Client Applications Seen	- ×
Image: state	Application IntTP Tunni Status Conservation Conservation Conservation Last updated 4 minutes app	▼Total Bytes (KB) 6.33 16.41 5.02 1.20 0.92	Application Gros Secure Independent Construction Construction Epresp Last updated 4 minutes ago	 ▼ Total Bytes (KB) €3.33 €.66 5.62 1.20
High 63,33	 Top Server Applications Seen 	- ×	▶ Top Operating Systems Seen	- ×
Last updated 4 minutes ago Traffic by Business Relevance Business Relevance Total Bytes (KB)	X No Data		No Data	

步骤2.点击New Policy。

Firewall Management Center Policies / Access Control / Identity	Overview	Analysis	Policies	Devices	Obje	ts Integration		Deploy	۹	¢ 🕹	admin •	disco SECURE
									c	bject M	lanagement	Access Control
											ingure r oncies	The first concy
Identity Policy						Domain	Status	Last Modified				
						There are no policies created. Add a new policy						

第3步:为新的身份策略分配名称和说明,然后点击保存。

Firewall Management Center Dverview Analysis Policies Dev	ices Objects Integration		Deploy Q 💕 🌣 🔕 admin 🕶 🕬 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	0	
	Name	_	
	Description		
	Identity Policy Lab		
	Cancel	Save	

第四步:点击+添加规则图标。

- 1. 为新规则指定名称。
- 2. 在name字段下,选择身份验证方法,选择:Passive Authentication。
- 3. 在屏幕右侧选择Realm & Settings。

Firewall Management Cente Policies / Access Control / Identity Policy	r Overview Analysis Policie:	es Devices Objects Integration		Deploy Q 💣 🌣 🛛 admin v 🔤
Identity Test Identity Policy Lab				Save Cancel
Rules Active Authentication Identit	Add Rule			0
Name	Name Test Identity Policy Passive Authentication	Insert ibled into Category • Realm: No realm Authentication Protocol: HTTP B	Standard Rules	e Q. Search Rules X
Administrator Rules This category is empty	Zones Networks VLAN Tags Port	ts		Realm & Settings
Standard Roles This category is empty Root Rules This category is empty This category is empty	Available Zones C Q. Search by name inside outside	Source Zones (0) Add to Source Add to Destination	Destination Zones (0) any	
			(Cancel
				No data to display $ < < Page 1 ext{ of } 1 > > C$

4. 从下拉菜单中选择领域。

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
Rules Active Authentication Identit	Add Rule	0
Name Administrator Rules	Name Insert Test Identity Policy Insert Passive Authentication • Realm: AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None	e Q. Search Rules X Auth Protocol
This category is empty Standard Rules	Zones Networks VLAN Tags Ports	Realm & Settings
This category is empty Root Rules This category is empty	AD (AD) Vise active authentication if passive or VPN identity cannot be established	
	* Required Field	
		Cancel
		No data to display $ \langle \langle Page \boxed{1} $ of $1 > C$

5. 单击屏幕左侧的Zones。

6. 从可用区域菜单中,根据检测用户所需的流量路径分配源和目标区域。要添加区域,请点击区域 的名称,然后根据情况选择添加到源或添加到目标。



注意:在本文档中,用户检测将仅应用于来自内部区域且被转发到外部区域的流量。

7. 选择添加和保存。

Firewall Management Center Policies / Access Control / Identity Policies	9F Overview Analysis Policies Devices Objects Integration Deploy	९ 💞 🌣 👩 admin - 🔤 अप्रिकार SECURE .
Identity Test Identity Policy Lab		Save Cancel
Rules Active Authentication Identit	Add Rule	4
Name Administrator Rules	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 Auth Protocol
This category is empty Standard Rules	Zones Networks VLAN Tags Ports Realm & Settings	-
This category is empty	Available Zones C Destination Zones (1)	
Root Rules	Q Search by name inside outside	
This category is empty	nsoe Restaure	
	N	o data to display $ <$ < Page 1 of 1 > > C

第五步:验证身份策略中的新规则并点击保存。

þ	Firewall Management Cen Policies / Access Control / Identity Po	iter Over	rview Analysis	Policies Device	es Objects Ir	tegration				Deploy Q 💕 🌣	admin • dada s	SECURE
lde	ntity Test									You have unsaved	I changes Save	Cancel
Ident	ty Policy Lab											
Rul	es Active Authentication Iden	tity Source										
									+ Add Category	+ Add Rule Q. See	arch Rules	×
	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol	
Adm	inistrator Rules											
Thi	s category is empty											
Star	dard Rules											
1 1	est Identity Policy	inside (Routed)	outside (Routed)	any	any	any	any	207	AD (AD)	Passive Authentication	0000	11
Roo	Rules											
Thi	a category is empty											
										Displaying 1 - 1 of 1 rules	< < Page 1 of 1	>>I C

第六步: 导航到策略>访问控制

步骤 7.确定要在处理用户流量的防火墙中部署的访问控制策略,然后单击铅笔图标上的以编辑策略 。

Ę	Firewall Management Center Policies / Access Control / Access Control	w Analysis	Policies Device	es Obje	cts Integration		Deploy 🔍 💕 🌣 🎯 admin 🔹	cisco 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"		% B∕¥

第六步: 在Identity Policy字段中单击None。

Fi Po	Firewall Management Center Policies / Access Control / Policy Editor																			
💣 Tes	Test Policy Try New UI Layout D Analyze Hit Counts Carcel																			
Rules	Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: prefilter Policy: prefilter Policy: prefilter Policy: prefilter Policy: None Identity Policy: None																			
Filter by D	Nevice T	Search Rules											×	Show Rule Con	flicts 🛛 + 🗚	dd Cat	egory	+	Add R	ule
# Nam	e	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, 5			o
\sim Mandato	ory - Test Polic	y (1-2)																		
1 Allor	w_to_outside	inside	outside	any-ipv4	any-	ipv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow	F5 0	16 12		0	11
2 Allos	w_to_inside	outside	inside	any-ipv4	any-	-lpv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow	F5 0	B . A		0	11
✓ Default -	- Test Policy (-)																		
There are r	on roles in this	eaction Add Do	In or Add Cate																	

 Default Action

 Access Control-Block all traffic
 Biplaying 1 - 2 of 2 rules
 C Page 1 of 1 >>I C Rules per page: 100
 C Rules per page: 100

步骤 7.从下拉菜单中选择之前在步骤3中创建的策略,然后单击OK以完成配置。

	Firewall Ma Policies / Acces	nagement C s Control / Policy I	Center Ov Editor	erview Analy	ysis Policies	Devices	Objects Inte	egration					Deploy	० 💞 🌣	👩 admin 🕶	diado SECU	JRE
	Test Policy											Try M	lew UI Layout 🗩	Analyze Hit	Counts Sav	Cance	8
	Rules Security In	telligence Hi	TTP Responses	Logging Ac	Ivanced							Prefilter Policy: pref	filter_marpatin	Inheritanc SSL Policy:	e Settings Polic None Ider	v Assignmen tity Policy: N	t <u>s (1)</u> Ione
E	Iter by Device	Search Rules										×	Show Rule Co	nflicts 🛛 🕂	Add Category	+ Add R	Je
	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 O IS /2		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 B A	S 0 0,	1
2	Allow_to_inside	outside	inside	any-ipv4	any-ipv4	Any	Identity Policy			0				C Allow	15 U IS A	⊠∎∘,	1
~	Default - Test Policy (.)								_							
Th	ere are no rules in this	section. Add Rul	le or Add Category			-	Identity Test										
										_							
							Revert to Defaults		Cancel	ОК							
Det	fault Action												Access Cor	troi:Block all tr	affic		
											Display	ing 1 - 2 of 2 rules	< Page 1 o	(1>>1C R	ules per page: 10	0	*

第8步:保存配置并部署到FTD。

验证

1. 在FMC GUI中,导航至分析>用户:活动会话

No Se	arch Constraints (Edit Searc	h)												
Tab	e View of Active Sessions	Active Sessions												
Jum	p to													
	4 Login Time ×	Last Seen ×	User X	Authentication Type ×	Current IP ×	Realm ×	Usemame ×	First Name ×	Last Name ×	E-Mail ×	Department ×	Phone ×	Discovery Application ×	Device ×
٠	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. 通过分析>连接>事件:连接事件表视图进行验证

Search Constraints (Edit Search Save Search)															r shares				
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		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	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:与身份策略和访问控制策略的流量条件匹配的用户在User字段中显示其用户名。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。