FMC(Secure Firewall Management Center)에서 ID 정책 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>구</u> <u>실정</u> <u>다음을 확인합니다.</u>

소개

이 문서에서는 보안 FMC를 통해 보안 FTD 트래픽에 대한 ID 정책을 구성하고 구축하는 프로세스 에 대해 설명합니다.

사전 요구 사항

1. FMC에 이미 구성된 영역

2. ID 소스가 이미 구성되었습니다. ISE, ISE-PIC



참고: ISE 및 Realm 컨피그레이션 지침은 이 문서의 범위에 포함되지 않습니다.

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- FMC(Secure Firewall Management Center)
- FTD(Secure Firewall Thread Defence)
- Cisco ISE(Identity Services Engine)
- LDAP/AD 서버
- 인증 방법
- 1. 수동 인증: ISE와 같은 외부 ID 사용자 소스 사용
- 2. 활성 인증: 관리되는 디바이스를 인증 소스로 사용(종속 포털 또는 원격 vpn 액세스)
- 3. 인증 없음

사용되는 구성 요소

- Secure Firewall Management Center for VMWare v7.2.5
- Cisco Secure Firewall Threat Defense for VMWare v7.2.4
- Active Directory 서버
- Cisco ISE(Identity Services Engine) v3.2 패치 4
- 수동 인증 방법

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

설정

1단계.FMC GUI에서 Policies(정책) > Access Control(액세스 제어) > Identity(ID)로 이동합니다

Firewall Management Center Overview / Dashboards / Dashboard Overview Analysis Policie	s Devices Objects Integration		Deploy 🔍 💕 🕻	admin • dade SECURE
Summary Dashboard (restricts distributed) Provides a summary of activity on the appliance Network × Threats Intrusion Events Status Geolocation Iden SSL	ss Control Network Discovery Actions Iss Control Application Detectors Alerts sion Correlation Scanners vare & File Groups Modules Ity Instances		Show the Last 1 hot	Reporting ar II Add Widgets
Unique Applications over Time	nor	- ×	 Top Client Applications Seen 	- ×
Last updated 4 minutes ago	Application TP Tunel Stitute Stitute Stitute Stitute CCUMP CLOMP CLOMP	total system (AB) (5.33) (5.4) (5.02) (1.20)	Application Cus Score Indepen Kerbers Cover Cove	* 10(34 Bytek (KB) 6.33 6.46 5.02 1.20
Risk violai Bytes (KB) Medium 1,261.80	Last updated 4 minutes ago		Last updated 4 minutes ago	
Very Low 227.32 High 6.33 Last updated 4 minutes app	Top Server Applications Seen	- ×	Top Operating Systems Seen	- ×
Traffic by Business Relevance - × Business Relevance * Total Bytes (KB) Hedum 1,225.33	No Data		No Data	

2단계. New Policy(새 정책)를 클릭합니다.

þ	Firewall Management Center Policies / Access Control / Identity	Overview	Analysis	Policies	Devices	Obje	ts Integration		Deploy	۹	¢ 🕹	@ admin	· cisco SECURE
										o	bject Ma Corr	nagement	Access Control New Policy
Ide	ntity Policy						Domain	Status	Last Modified				
							There are no policies created. Add a new policy						

3단계. 새 ID 정책에 이름 및 설명을 할당한 다음 Save를 클릭합니다.

Firewall Management Center Policies / Access Control / Identity	Overview An	alysis F	Policies D	Vevices 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			
					Identity Policy Lab			
					Cancel			

4단계. + Add Rule(규칙 추가) 아이콘을 클릭합니다.

- 1. 새 규칙에 이름을 할당합니다.
- 2. name(이름) 필드에서 authentication method(인증 방법)를 선택하고 : Passive Authentication(수동 인증)을 선택합니다.
- 3. 화면 오른쪽에서 Realm & Settings(영역 및 설정)를 선택합니다.

Firewall Management Center Policies / Access Control / Identity Policy	r Editor Overview Analysis Policies Devices	Objects Integration	Deploy Q	🔮 😂 👩 admin 🛛 🔤
Identity Test Identity Policy Lab				Save Cancel
Rules Active Authentication Identit	Add Rule		Θ	
Name	Name Enabled Enabled	nsert into Category	▼ Agents: None	Q. Search Rules X
This category is empty	Zones Networks VLAN Tags Ports		Realm & Settings	
Standard Rules This category is empty Root Rules This category is empty	Available Zones (2 Q. Search by name inside outside Add to 5 Add to 5 Add to 5	Source Zones (0) any estimation	Destination Zones (0) any	
			Cancel Add	
			No da	to display $ \langle \langle Page[1] $ of $1 > \rangle \subset$

4. 드롭다운 메뉴에서 영역을 선택합니다.

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	0
Name Administrator Rules This category is empty Standard Rules This category is empty Root Rules This category is empty	Name Inset Test Identity Policy Enabled into Category Standard Rules grassive Authentication Realm: AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None Zones Networks VLAN Tags Ports Realm: (AD (AD) Use active authentication if passive or VPN Identity cannot be established	Realm & Settings
	* Required Field	
		Cancel
		No data to display $ < < Page 1 ext{ of } 1 > > \mathbb{C}$

5. 화면 왼쪽의 Zones(영역)를 클릭합니다.

6. Available Zones 메뉴에서 사용자를 탐지하는 데 필요한 트래픽 경로에 따라 소스 및 목적지 영역 을 할당합니다. 영역을 추가하려면 영역의 이름을 클릭한 다음 Add to Source(소스에 추가) 또는 Add to Destination(대상에 추가)의 경우에 따라 선택합니다.



참고: 이 문서에서는 사용자 탐지가 내부 영역에서 오는 트래픽에 대해서만 적용되고 외부 영역으로 전달됩니다.

7. 추가 및 저장을 선택합니다.

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 Bules	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 Root Rules This category is empty	Available Zones C Source Zones (1) Destination Zones (1) Q. Search by name inside outside Add to Source Add to Source Add to Destination Add to Destination	
	Cancel	J
	Ne	data to display $ \langle \langle Page 1 0 0 1 \rangle > C$

5단계. 새 규칙이 ID 정책에 있는지 확인하고 Save(저장)를 클릭합니다.

Identity Test Identity Policy Lab Nume Ketrik Authentication Kentity Source + Add Rule Q. Search Rules × Name Source Zones Dest Zones Source Networks VLAN Tags Source Ports Realm Action Addh Protocol Image: Calced Rules × Administrator Rules	Firewall Management Center Policies / Access Control / Identity Policy Editor	Overview Analysis Policies I	evices Objects Integration		Deploy	२. 🧬 🌣 🔞 admin 🕶 🔤 🐯 SECURE
Rules Active Authentication Identity Source Rules Active Authentication Identity Source Name Source Zones Dest Zones Source Networks VLAN Tags Source Ports Realm Action Auth Protocol Add Initiatration Rules Addiministration Rules	Identity Test				Yo	u have unsaved changes Save Cancel
Rules Active Authentication Identify Source Image Source Zones Dest Networks VLAN Tags Source Ports Dest Ports Realm Action Auth. Protocol Image Administrator Rules	Identity Policy Lab					
Nume Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Source Ports Dest Ports Realm Action Auth Protecol Image: Control Con						
Image: Name Source Zones Dest Zones Source Networks Dest Networks VLNN Tage Source Ports Dest Ports Readm Action Auth Protected Concernance Administrator Rules	Rules Active Authentication Identity Source					
Name Source Zones Dest Zones Source Networks Dest Networks Dest Ports Dest Ports Dest Ports Action Auth Protect Administrator Rules					+ Add Category + Add Ru	le Q. Search Rules X
Administrator Rules This category is empty Standard Rules I field (Routed) outside (Routed) any any any any any any any AD (AD). Passive Authentication none Rot Rules This categories is assume to assume	Name Source Zor	nes Dest Zones Source Network	a Dest Networks VLAN Tags	Source Ports Dest Ports	Realm Action	Auth Protocol
This category is empty Standard Rules	Administrator Rules					
Standard Rules 1 Test Identity Policy inside (Routed) any	This category is empty					
	Standard Rules					
Root Rules	1 Test Identity Policy inside (Rout	ted) outside (Routed) any	any any	any any	AD (AD) Passive Authe	ntication none /T
This astronomy is somely	Root Rules					
Luis canadruk is ambrik.	This category is empty					
Displaying 1 - 1 of 1 rules < < Page 1 →) C					Displaying 1	- 1 of 1 rules $ \langle \langle Page 1 of 1 \rangle \rangle \subset C$

6단계. Policies(정책) > Access Control(액세스 제어)로 이동합니다

7단계. 사용자 트래픽을 처리하는 방화벽에 구축할 액세스 제어 정책을 식별하고 정책을 수정하려 면 연필 아이콘을 클릭합니다.

Ę	Policies / Access Control / Access Control Over	view Ar	Analysis Polic	cies Devices	Obje	cts Integration			Deploy 🔍 💕 🌣 🚳 admin	diade SECURE
								Object Management	Intrusion Network Analysis Policy DNS	Import/Export
										New Policy
	Access Control Policy	Do	omain			Status	Last Modified		Lock Status	
	Test Policy	Glot	bal			Targeting 1 devices Up-to-date on all targeted devices	2024-01-31 20:50:00 Modified by "admin"			% 8 ∕ ¥

6단계. ID 정책 필드에서 None(없음)을 클릭합니다.

Firewall N Policies / Acc	Management (less Control / Policy	Center Editor	Overview	Analysis	Policies	Devices	Objects	Integration					Deploy	९ 🔮 🌣	🛛 admin 🔻	idude S	SECURE
Test Polic	ÿ											Try Ne	w UI Layout 🍞	Analyze Hit Co	unts S:	ve C	Cancel
Rules Security	Intelligence	ITTP Responses	Logging	Advance	ed						Pre	filter Policy: prefilt	er_marpatin	Inheritance S SSL Policy: No	Settings Pol	cv Assign entity Polic	ments (1) cy: None
Filter by Device	ilter by Device 🝸 Search Rules X 🗋 Show Rule Conflicts 🕢 + Add Category + Add Rule																
# 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	15 O Is	8 🗆 🖬	• •
V Mandatory - Test P	olicy (1-2)																
1 Allow_to_outsid	6e inside	outside	any-ipv4	any	-ipv4	Any	Any	Any	Any	Any	Any	Any	Any	C Allow	R 0 R .	ê 🖂 🛢	0/1
2 Allow_to_inside	outside	inside	any-ipv4	any	-lpv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow	15 O Iz :	2 🖂 🖬	∘⁄≣
✓ Default - Test Polic	y (-)																
There are no rules in	this section. Add R	ule or Add Cate	gory														

Default Action	Access Control:Block all traffic	٠	8
	Displaying 1 - 2 of 2 rules < < Page 1 of 1 >> C Rules per page: 100		î.

7단계. 드롭다운 메뉴에서 이전에 3단계에서 생성한 정책을 선택한 다음 확인을 클릭하여 컨피그레 이션을 완료합니다.

	Firewall Man	nagement C Control / Policy I	enter Ov Editor	erview Analy	rsis Policies	Devices	Objects In	tegration					Deploy	ې 😵 ک	😝 admin 🔻	cisco SECU	RE
	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	ter by Device	Search Rules										×	Show Rule Co	nflicts 🛛 🕂	Add Category	+ Add Rul	•
	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		• /								
									_	_							
							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		*

8단계. 컨피그레이션을 저장하고 FTD에 구축합니다.

다음을 확인합니다.

1. FMC GUI에서 Analysis > Users: Active Sessions로 이동합니다

No Se	arch Constraints (Edit Searc	n)												
Tabl	e View of Active Sessions	Active Sessions												
Jum	p to													
	4 Login Time X	Last Seen ×	User ×	Authentication Type ×	Current IP ×	$\operatorname{Realm}\times$	Usemame x	First Name ×	Last Name ×	II-Mail ×	Department ×	Phone ×	Discovery Application ×	Device ×
٠	2024-01-09 15:20:06	2024-01-31 16:21:08	🛓 stua (LDAP\stua, LDAP)	Passive Authentication	0 10.4.23.129	LDAP	sfua	sfua		sfua@jorgeju.local	users (jorgeju)		🗆 LDAP	frepower

3. Analysis(분석) > Connection(연결) > Events(이벤트)에서 검증: 연결 이벤트의 테이블 보기

* Search Constraints (Edit Search Save Search)															L'April Ann				
Co	nnecti	ions with Application	Details	Table View	of Connect	ion Events													
Jun	np to.																		
		↓ First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	Initiator x Country x	Initiator User ×	Responder _×	Responder ×	Security Intelligence X Category	Ingress Security × Zone	Egress Security × Zone	Source Port / ICMP x	Destination Port x	SSL Status ×	Application x Protocol	Client ×	CI Ve
		2024-01-31 16:26:46	í.	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	CMP client	
٠		2024-01-31 16:26:45	5	Allow		10.4.23.129		1 sfua (LDAP\sfua, LDAP)	0 10.6.11.4			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	CMP 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	CMP client	
٠		2024-01-31 16:26:23	i.	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	



참고: ID 정책 및 액세스 제어 정책의 트래픽 기준과 일치하는 사용자는 User 필드에 사용 자 이름이 표시됩니다. 이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.