FMC(Secure Firewall Management Center)에서 ID 정책 구성

목차

소개

이 문서에서는 보안 FMC를 통해 보안 FTD 트래픽에 대한 ID 정책을 구성하고 구축하는 프로세스에 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

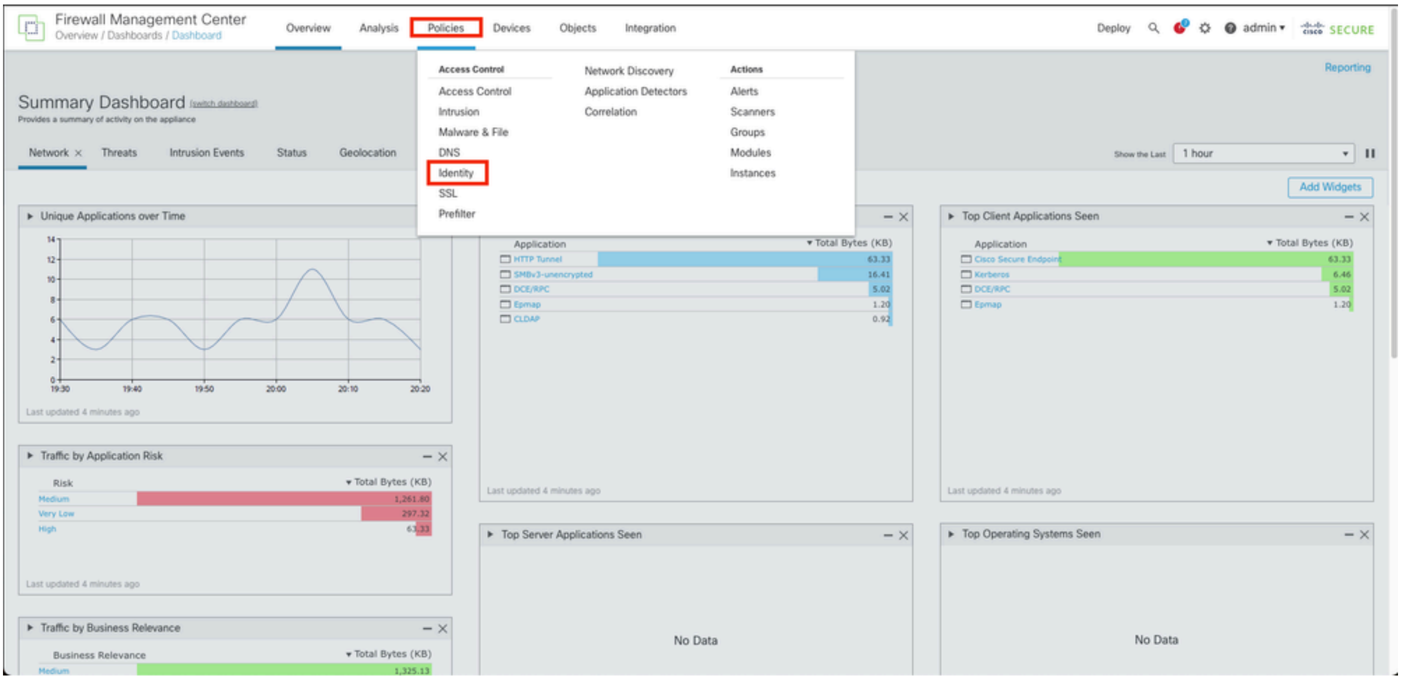
- Secure Firewall Management Center for VMWare v7.2.5
- Cisco Secure Firewall Threat Defense for VMWare v7.2.4
- Active Directory 서버
- Cisco ISE(Identity Services Engine) v3.2 패치 4
- 수동 인증 방법

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

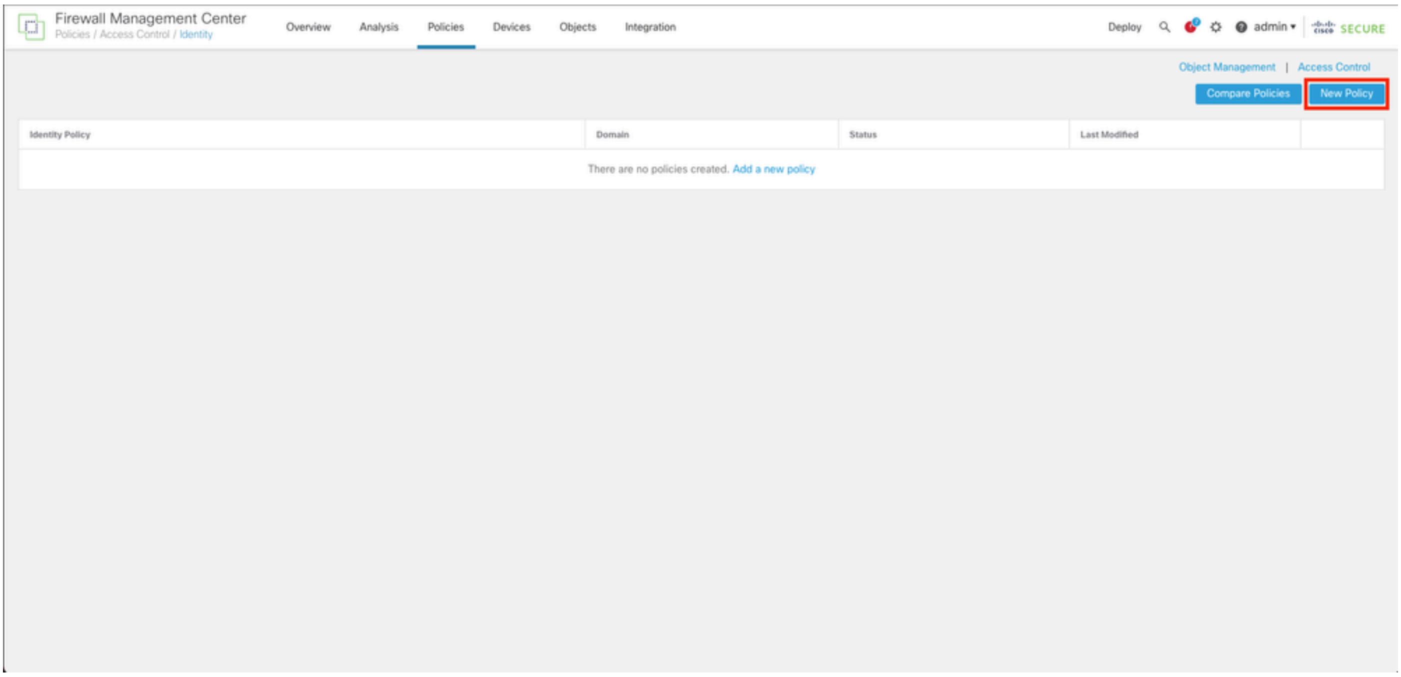
구성

설정

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

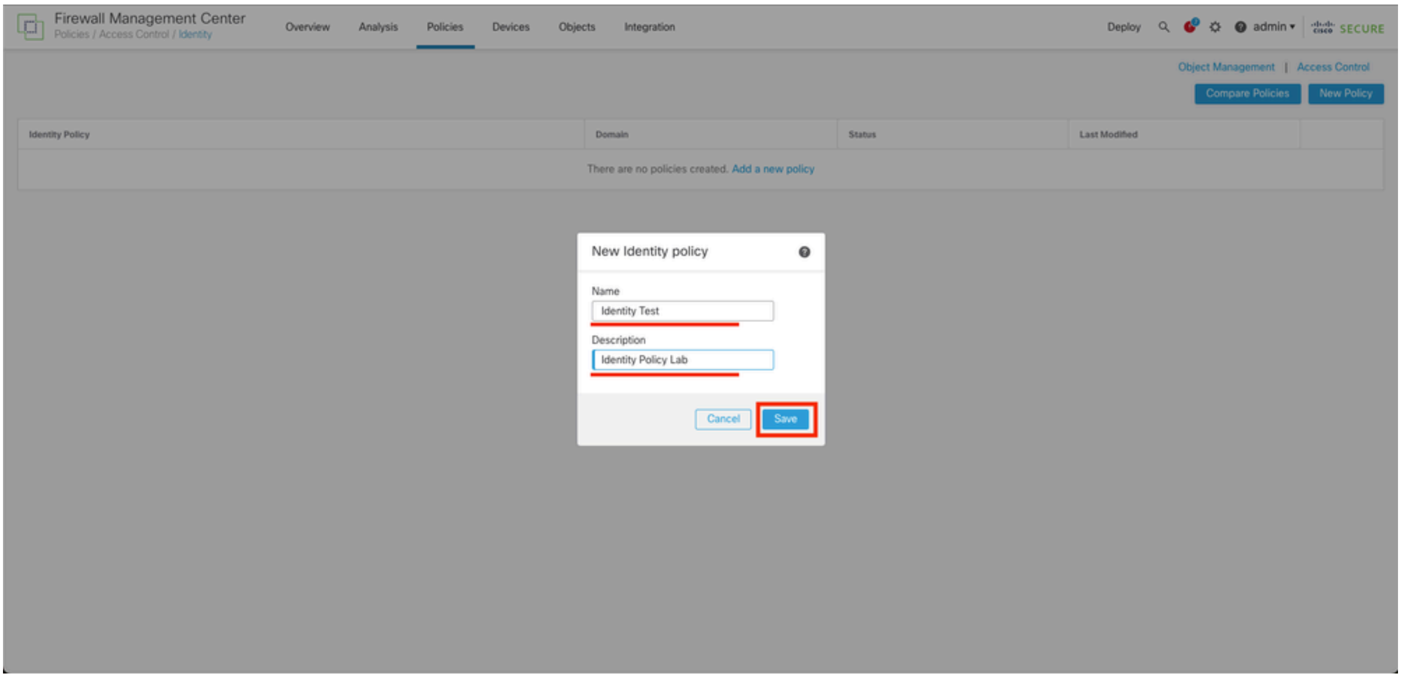


2단계. New Policy(새 정책)를 클릭합니다.


Firewall Management Center
Policies / Access Control / Identity
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
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			

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


Firewall Management Center
Policies / Access Control / Identity
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
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
Cancel
Save

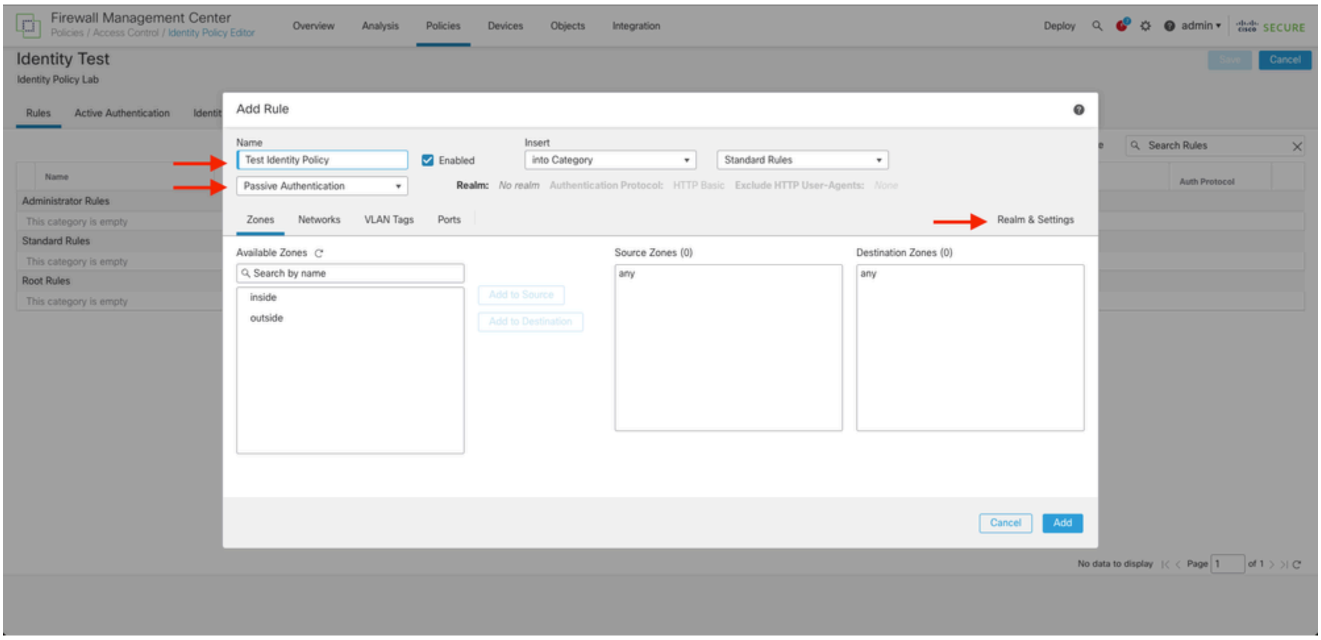
New Identity policy

Name: Identity Test

Description: Identity Policy Lab

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.



Name: Test Identity Policy

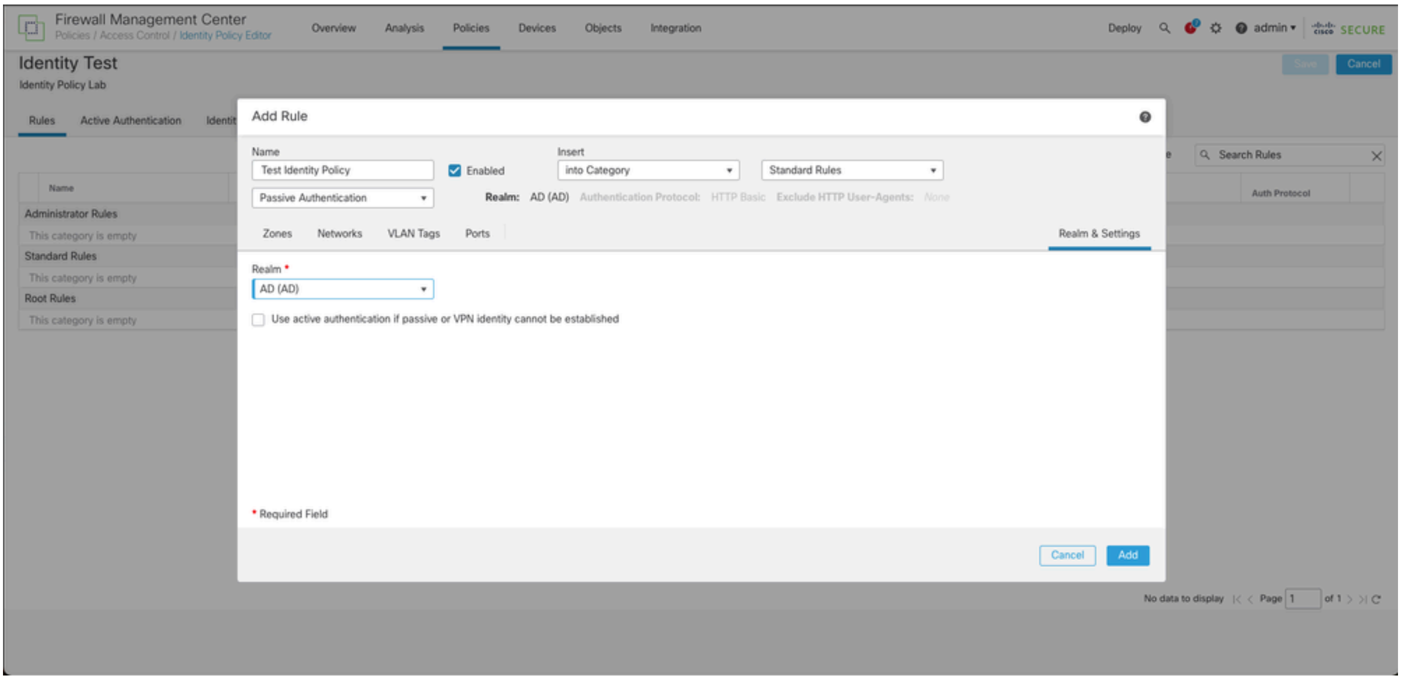
☑ Enabled

Insert: into Category | Standard Rules

Passive Authentication

Realm: No realm Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

4. 드롭다운 메뉴에서 영역을 선택합니다.



Name: Test Identity Policy

☑ Enabled

Insert: into Category | Standard Rules

Passive Authentication

Realm: AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Realm *: AD (AD)

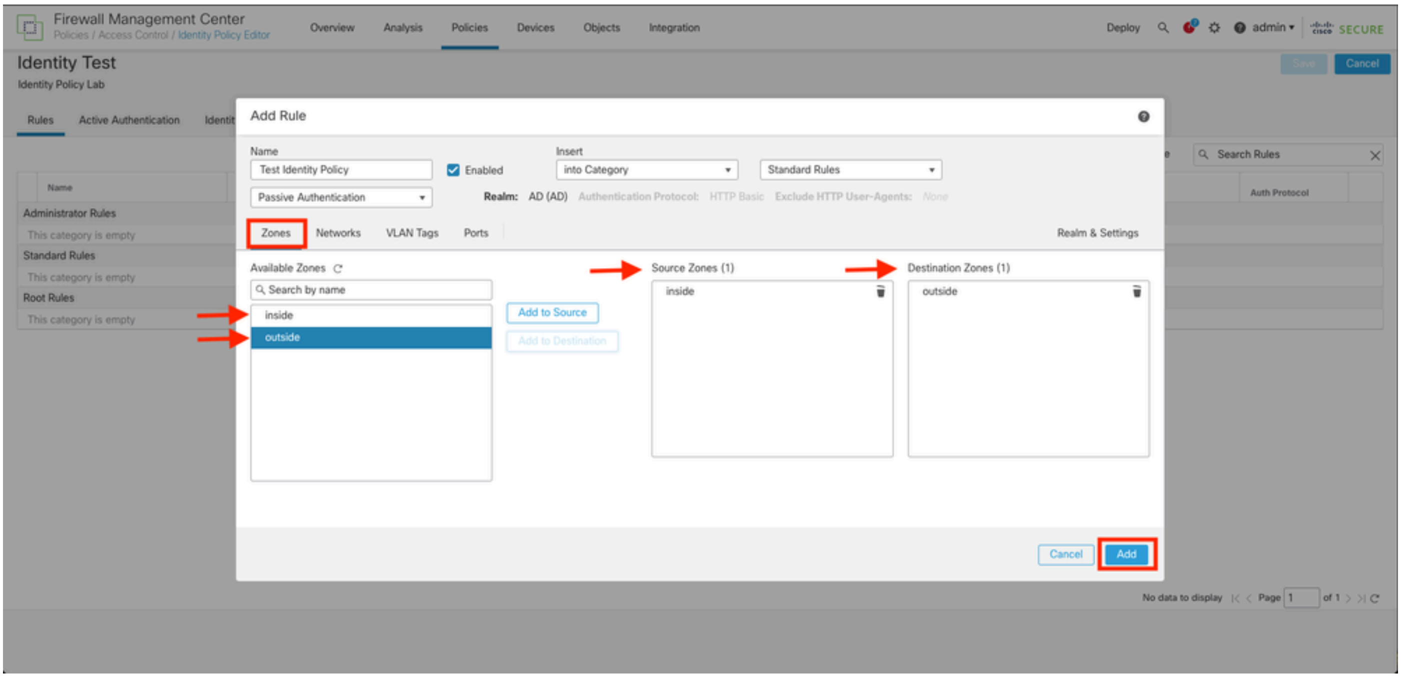
☐ Use active authentication if passive or VPN identity cannot be established

5. 화면 왼쪽의 Zones(영역)를 클릭합니다.

6. Available Zones 메뉴에서 사용자를 탐지하는 데 필요한 트래픽 경로에 따라 소스 및 목적지 영역을 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.



Name: Test Identity Policy

☑ Enabled

Insert: into Category — Standard Rules

Passive Authentication

Realm: AD (AD) Authentication Protocol: HTTP Basic Exclude HTTP User-Agents: None

Administrator Rules — This category is empty

Standard Rules — This category is empty

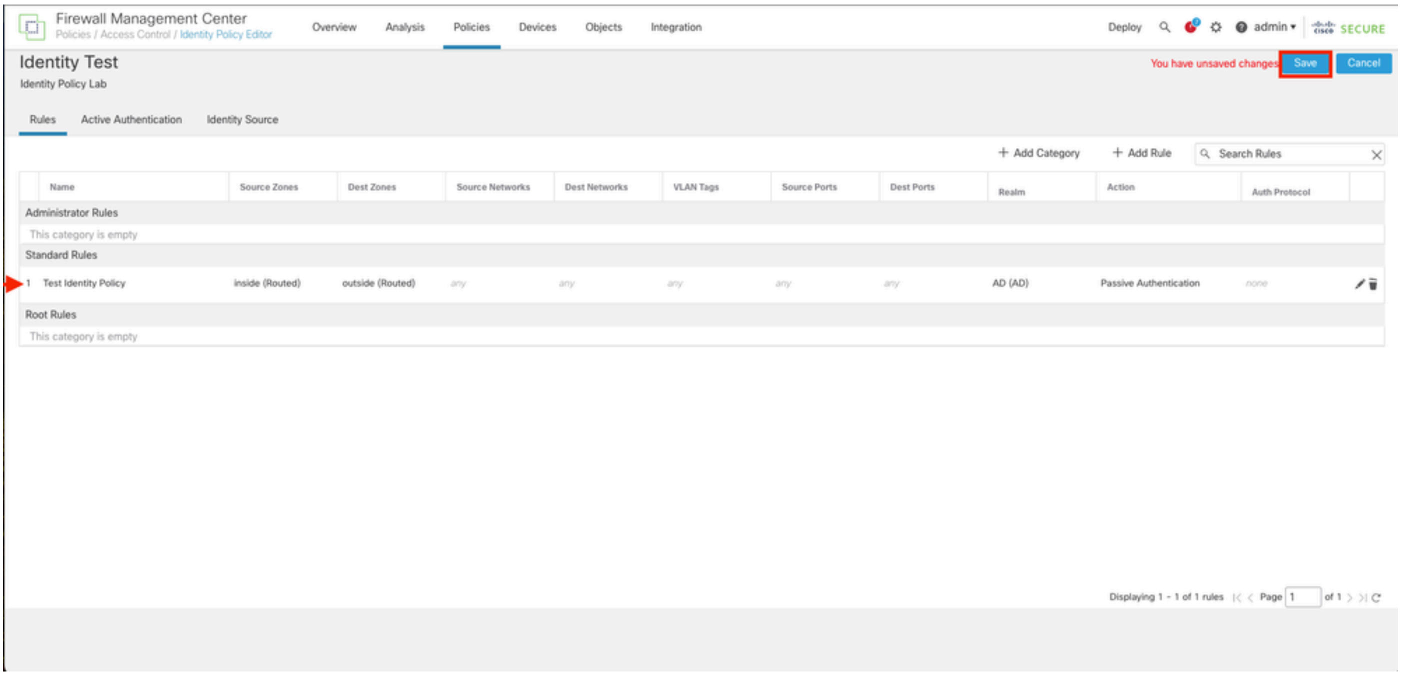
Root Rules — This category is empty

Available Zones: inside, outside

Source Zones (1): inside

Destination Zones (1): outside

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



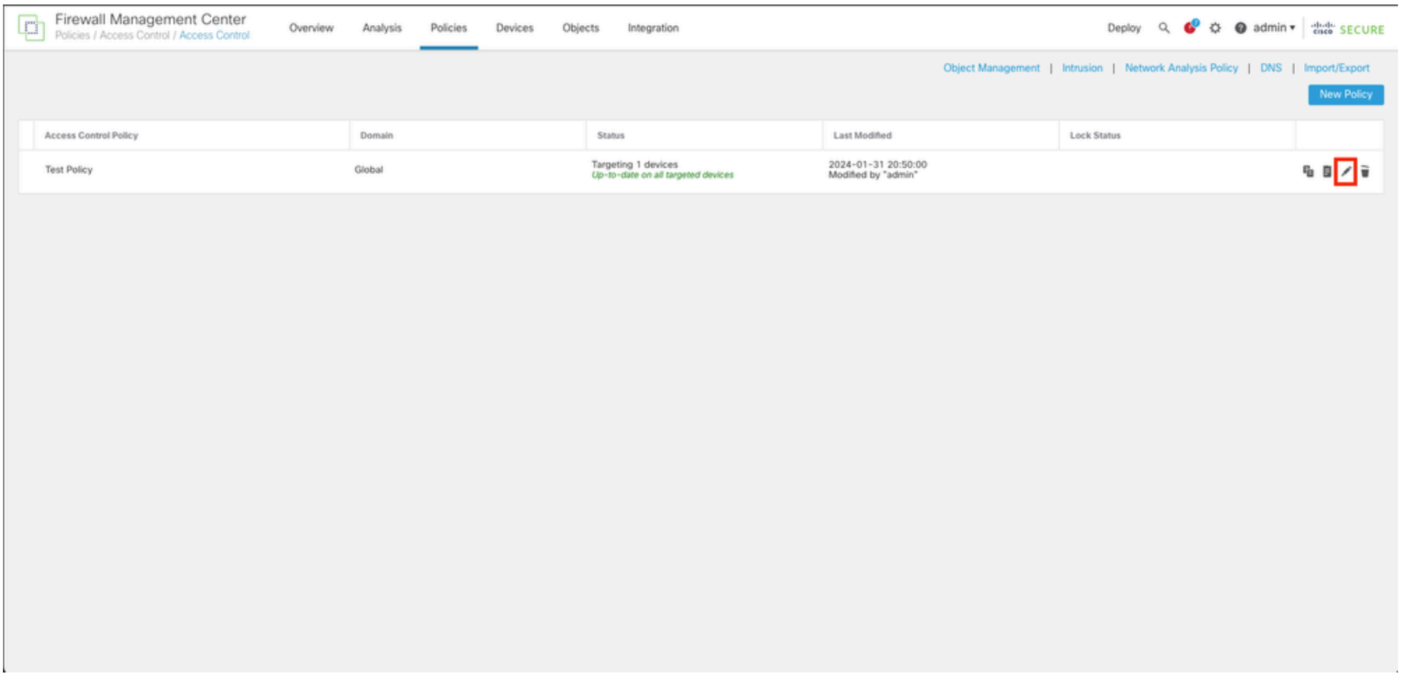
Identity Test

Identity Policy Lab

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
Root Rules										
This category is empty										

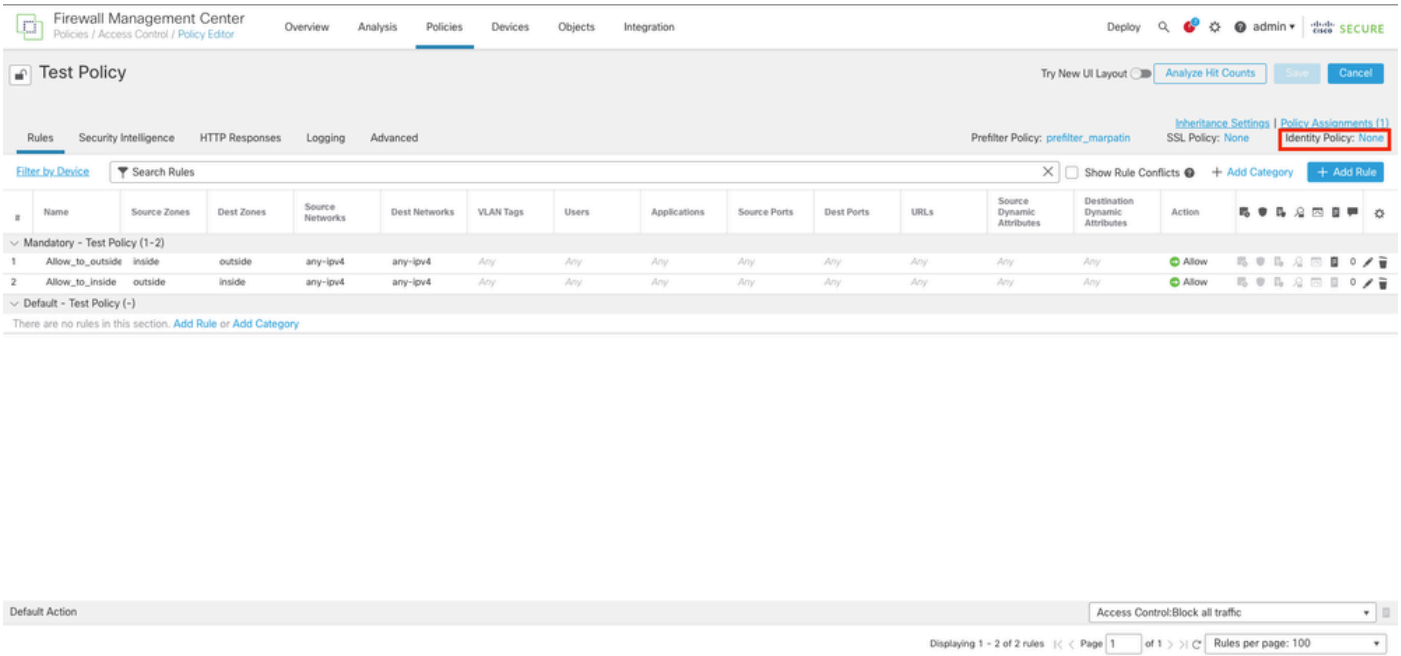
6단계. Policies(정책) > Access Control(액세스 제어)로 이동합니다

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


Firewall Management Center
Policies / Access Control / Access Control
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
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"	

6단계. ID 정책 필드에서 None(없음)을 클릭합니다.



Test Policy

Prefilter Policy: prefilter_marpatin SSL Policy: None Identity Policy: None

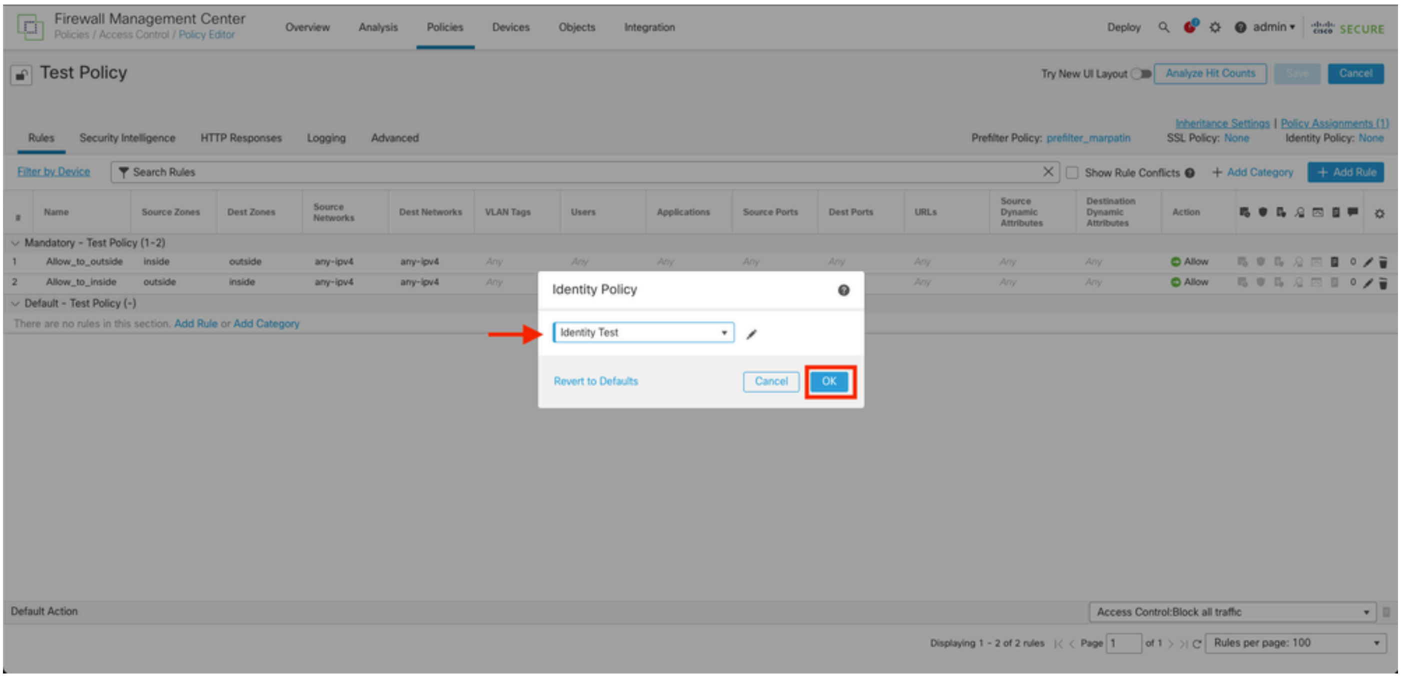
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destination Dynamic Attributes	Action
Mandatory - Test Policy (1-2)														
1	Allow_to_outside	inside	outside	any-ipv4	any-ipv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow
2	Allow_to_inside	outside	inside	any-ipv4	any-ipv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow
Default - Test Policy (-)														

There are no rules in this section. Add Rule or Add Category

Default Action: Access Control:Block all traffic

Displaying 1 - 2 of 2 rules Page 1 of 1 Rules per page: 100

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



Test Policy

Prefilter Policy: prefilter_marpatin SSL Policy: None Identity Policy: None

#	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
Mandatory - Test Policy (1-2)														
1	Allow_to_outside	inside	outside	any-ipv4	any-ipv4	Any	Any	Any	Any	Any	Any	Any	Any	Allow
2	Allow_to_inside	outside	inside	any-ipv4	any-ipv4	Any					Any	Any	Any	Allow
Default - Test Policy (-)														

There are no rules in this section. Add Rule or Add Category

Identity Policy

Identity Test ▾

Revert to Defaults Cancel OK

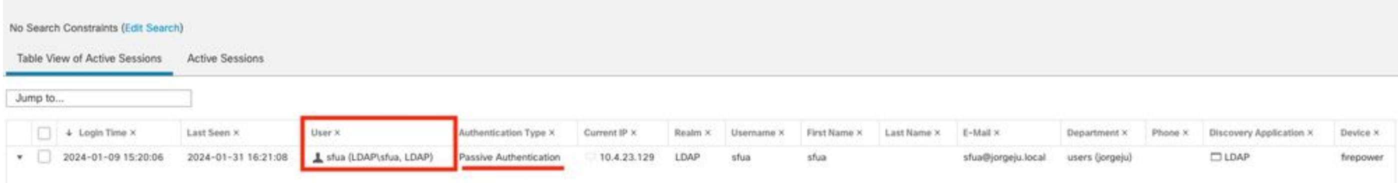
Default Action Access Control:Block all traffic

Displaying 1 - 2 of 2 rules Page 1 of 1 Rules per page: 100

8단계. 컨피그레이션을 저장하고 FTD에 구축합니다.

다음을 확인합니다.

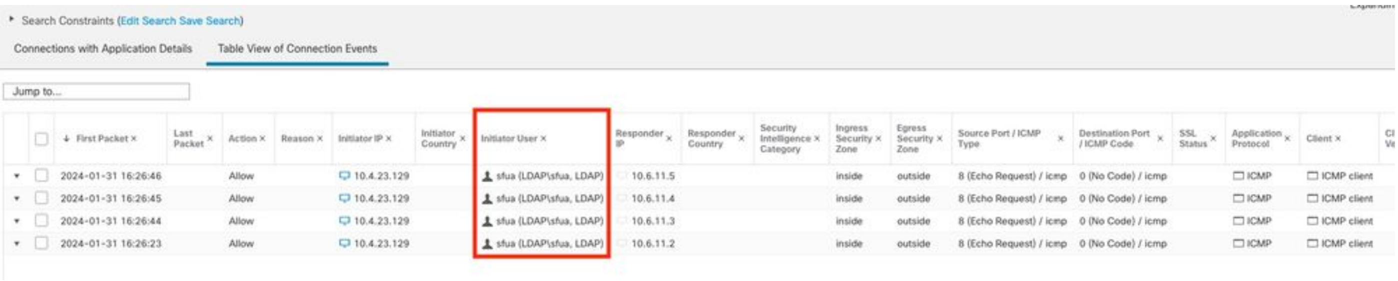
1. FMC GUI에서 Analysis > Users: Active Sessions로 이동합니다



No Search Constraints (Edit Search)

	☐	↓ Login Time ×	Last Seen ×	User ×	Authentication Type ×	Current IP ×	Realm ×	Username ×	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. Analysis(분석) > Connection(연결) > Events(이벤트)에서 검증: 연결 이벤트의 테이블 보기



Search Constraints (Edit Search Save Search)

Connections with Application Details
Table View of Connection Events
Jump to...

	☐	↓ First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	Initiator Country ×	Initiator User ×	Responder IP ×	Responder Country ×	Security Intelligence Category ×	Ingress Security Zone ×	Egress Security Zone ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	SSL Status ×	Application Protocol ×	Client ×
▾	☐	2024-01-31 16:26:46		Allow		10.4.23.129		sfua (LDAP\sfua, LDAP)	10.6.11.5			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client
▾	☐	2024-01-31 16:26:45		Allow		10.4.23.129		sfua (LDAP\sfua, LDAP)	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		sfua (LDAP\sfua, LDAP)	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		sfua (LDAP\sfua, LDAP)	10.6.11.2			inside	outside	8 (Echo Request) / icmp	0 (No Code) / icmp		ICMP	ICMP client

참고: ID 정책 및 액세스 제어 정책의 트래픽 기준과 일치하는 사용자는 User 필드에 사용자 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 번역 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.