# FDM 활성 인증 구성(종속 포털)

## 목차

<u>소개</u>
<u>사전 요구 사항</u>
<u>요구 사항</u>
<u>사용되는 구성 요소</u>
<u>배경 정보</u>
<u>네트워크 다이어그램</u>
<u>구성</u>
<u>다음을 확인합니다.</u>
문제 해결

## 소개

이 문서에서는 활성 인증(종속 포털) 통합을 사용하는 FDM(Firepower Device Manager)의 구성 예에 대해 설명합니다.이 구성에서는 AD(Active Directory)를 소스 및 자체 서명 인증서로 사용합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(Firepower Threat Defense)
- AD(Active Directory)
- 자체 서명 인증서.
- SSL(Secure Socket Layer)

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Firepower Threat Defense 6.6.4
- Active Directory
- PC 테스트

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

### 배경 정보

활성 인증을 통해 사용자 ID 설정

인증은 사용자의 ID를 확인하는 작업입니다.활성 인증을 사용하면 HTTP 트래픽 흐름이 시스템에 사용자 ID 매핑이 없는 IP 주소에서 오는 경우 시스템에 대해 구성된 디렉토리에 대해 트래픽 흐름 을 시작한 사용자를 인증할지 여부를 결정할 수 있습니다.사용자가 성공적으로 인증하면 IP 주소는 인증된 사용자의 ID를 가진 것으로 간주됩니다.

인증에 실패하더라도 사용자의 네트워크 액세스가 차단되지 않습니다.액세스 규칙은 이러한 사용 자에게 제공할 액세스 권한을 결정합니다.

#### 네트워크 다이어그램



## 구성

#### ID 정책 구현

IP 주소와 연결된 사용자를 알 수 있도록 사용자 ID 획득을 활성화하려면 여러 항목을 구성해야 합 니다

**1단계.** AD ID 영역 구성

사용자 ID를 능동적으로 수집(사용자 인증을 위해 프롬프트)하거나 수동적으로 수집(사용자 ID 정 보가 있는 Active Directory(AD) 서버를 구성)해야 합니다.

Objects(**개체) > Identity Services(ID 서비스**)로 이동하고 **AD** 옵션을 선택하여 Active Directory를 추 가합니다.

cisco. Firepower Device	Manager Monitoring Policies	Objects Device: firepower		2 admin Administrator
Object Types 🛛 🔶	Identity Sources			
C Networks	2 objects		Q Search	+~
S Ports	a NAME	TYPE	VALUE	RADIUS Server
Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
F Application Filters				AD
C <sup>9</sup> URLs				Identity Services Engine
Geolocations				
Syslog Servers				
🔎 IKE Policies				
🐴 IPSec Proposals				
AnyConnect Client Pro				
Lidentity Sources				
1 Users				

Active Directory 구성을 추가합니다.

Identity Realm is used for Identity Policies and Remote this realm.	e Access VPN. Any changes impact all features that use
Name	Туре
Active_Directory	Active Directory (AD) 🗸
Directory Username sfua	Directory Password
e.g. user@example.com	
Base DN	AD Primary Domain
CN=Users,DC=ren,DC=lab	ren.lab
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
172.17.4.32:389	<u>Test</u> –
Add another configuration	
	CANCEL

#### 2단계. 자체 서명 인증서 생성

종속 포털 컨피그레이션을 생성하려면 종속 포털용 인증서 2개와 SSL 암호 해독용 인증서가 필요 합니다.

이 예와 같이 자체 서명 인증서를 만들 수 있습니다.

Objects(개체) > Certificates(인증서)로 **이동합니다.** 

cisco. Firepower Devi	ce Manager Monitoring Policies Objects	Device: firepower		admin Administrator
Object Types ←	Certificates			
C Networks	120 objects		Q Search	+~
S Ports			Preset filters: System defined . User defined	Add Internal CA
Security Zones	H NAME	туре		Add Internal Certificate
🐨 Application Filters	1 NGFW-Default-InternalCA	Internal CA		Add Trusted CA Certificate
<b>6</b> 2 1101 o	2 ssl_captive_portal	Internal CA		
OF URLS	3 DefaultInternalCertificate	Internal Certificate		
Geolocations	4 DefaultWebserverCertificate	Internal Certificate		

종속 포털 자체 서명 인증서:

Add Internal Certificate	8 ×
Name	
captive_portai	
Country	State or Province
Mexico (MX)	Mexico
Locality or City	
Mexico	
Organization	Organizational Unit (Department)
MexSecTAC	MexSecTAC
Common Name	
fdmcaptive	
You must specify a Common Name to use the cer	tificate with remote access VPN.
	CANCEL SAVE

SSL 자체 서명 인증서:

## Add Internal CA

Name		
ssl_captive_portal		
Country		State or Province
Mexico (MX)	~	Mexico
Locality or City		
Mexico		
Organization		Organizational Unit (Department)
MexSecTAC		MexSecTAC
Common Namo		
Common Name		
ss_fdmcaptive		
You must specify a Common Name to us	e the cer	tificate with remote access VPN.
		CANCEL SAVE

#### **3단계.** ID 규칙 생성

Policies(정책) > Identity(ID) > select [+] 버튼을 선택하여 새 ID 규칙을 추가합니다.

활성 인증을 구성하려면 ID 정책을 생성해야 하며, 정책에는 다음 요소가 있어야 합니다.

- AD ID 소스:1단계에서 추가한 것과 동일한
- 작업:활성 인증
- 서버 인증서:[이 시나리오에서 captive\_portal] 전에 생성한 것과 동일한 자체 서명 인증서
- 유형:HTTP Basic(이 예에서는)

Order Title	AD Identity Source	Action ACTIVE AUTHENTICATION For HTTP connections only, prompt for username and password an	d
1    ad_captive	Active_Directory ~	Active Auth authenticate against the specified identity source to obtain the user intentity for the source IP address.	r
Source / Destination Active authentication		PASSIVE AUTH Identity Sources are needed th Server Certificate	
SOURCE		ACTIVE AUTH Captive Portal is needed	
Zones + Networks	+ Ports	NO AUTH Networks + Ports/Protocols	+
ANY ANY	ANY	ANY ANY ANY	

ID 정책이 활성 인증으로 생성되면 는 자동으로 SSL 규칙을 생성합니다. 기본적으로 이 규칙은 Decrypt**-Resign**과 함께 any로 설정되며, 이는 이 규칙에 SSL 수정 사항이 없음을 의미합니다.

$\boxdot \rightarrow \bigcirc \text{SSL Decryption} \rightarrow \bigodot \text{Identity} \rightarrow \bigcirc \text{Security Intelligence} \rightarrow \bigcirc \text{NAT} \rightarrow \bigodot \text{Access Control} \rightarrow \And \text{Intrusion}$											
SSL Decryption	1 rule						Q Search				¢ +
		SOURCE			DESTINATION						
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
🧧 🔝 Identity Policy	y Active Authentica	tion Rules 🧻									
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	E.
SSL Native Rules	0										
SSL Native Rules  There are no SSL Rules yet.  Start by creating the first SSL rule.  CREATE SSL RULE  or  ADD PRE-DEFINED RULES											

🖳 → 🕑 ssi	$\square \rightarrow \bigcirc$ SSL Decryption $\rightarrow \bigotimes$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \bigcirc$ NAT $\rightarrow \bigotimes$ Access Control $\rightarrow \bigotimes$ Intrusion											
SSL Decryption The rules in this section are automatically generated from rules in the identity policy		Q Search							ф	+		
# NAME	SSL decry rules are a native rule	that implement active authentication. These SSL decryption rules are read-only. These rules are always evaluated before the SSL native rules.		PORTS	DESTINATION ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS		CTIONS
🕘 🔝 Identity Policy A	ctive Authentica	tion Rules 🐧										
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	E.	
SSL Native Rules	•											
SSL Native Rules ①          There are no SSL Rules yet.         Start by creating the first SSL rule.         CREATE SSL RULE         or         ADD PRE-DEFINED RULES												

4단계. 액세스 제어 정책에 액세스 규칙 생성

트래픽을 종속 포털 인증으로 리디렉션하는 **포트 885/tcp**를 허용해야 합니다.Policies(**정책**) > Access Control(**액세스 제어**)로 이동하고 액세스 규칙을 추가합니다.

Order Title		Action					
1 ∨ ad_ca	ptive	Allo	ow 🗸				
Source/Destination	Applications URLs	Users Intrusion Poli	licy File policy	Logging			
SOURCE			DESTINATION				
Zones	+ Networks	+ Ports	+ Zones	+ Networks	+	Ports/Protocols	+
ANY	ANY	ANY	ANY	ANY		⇔ 885	

#### 사용자가 AD에서 다운로드되었는지 확인해야 하는 경우 액세스 규칙을 편집하고 **사용자** 섹션으로 이동할 수 있으며, AVAILABLE USERS**에서 FDM**에 이미 있는 사용자 수를 확인할 수 있습니다.

Order Title				Action	
1 ∨ ad_c	aptive			Allow	<b>~</b>
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy
AVAILABLE USERS	-			E	👢 CONTRO
<ul> <li>Filter</li> <li>Identity Sources</li> </ul>	Groups User				If you config address, yo membership appropriate
Active_Directo	ory \ luis		•		different ad network acc
Active_Directo	ory \ ngfwtac				nom one gr
Special-Identi	ties-Realm \ No Auth	entica			
Active_Directo	ory \ ren				
Active_Directo	ory \ sfua				
Active_Directo	ory \ testuser		-		
Create new Identity Re	alm CANCEL	ок			

구성 변경 사항을 구축해야 합니다.

## 다음을 확인합니다.

HTTPS 사이트로 이동할 때 사용자의 디바이스가 확인란을 수신하는지 확인합니다.

Shttps://10.115.117.43:885/x.authi: x +								
C 0 10.115.117.43:885/x.auth?s=dOF7LRChg4FKX2BCiK46wfdQKDJMAXeaLGcyYeiycuc%3D&u=http%3A%2F%2Fwww.cisco.com%2F								
	Sign in https://10.115.117.43:885 Username   Password Sign in Cancel							

#### 사용자 AD 자격 증명을 입력합니다.

S https://10.115.117.43:885/x.auth	× +					
← → C ③ 10.115.117.4	13:885/x.auth?s=dOF7LRC	hg4FKX2BCiK46wfd	IQKDJMAXeaLGcyYeiycu	c%3D&u=http%3A%2F%2F\	www.cisco.com%2F	
				Sign in https://10.1 Username Password	15.117.43:885	Sign in Cancel
Cisco - Networking, Cloud, and ⊂ x + → C a cisco.com Cisco Platform Skite > 1   1 + 1   1 + CISCO	Products Support & Learn	Partners Events & Vic	deos			ଦ
Kiva and	Cisco: Creating in etail opportunities	Active exp inclusive	ploit of Kaseya VSA in supply-of	chain attack. Read the Talos bet	bg now	s time to take the lead
	Design Guides	A+ Find Training	र््र्ट्रे Learning & Certifications	(1) Software Downloads	දිරිදි Cisco Community	Activate Windows Tech Support Cases

## 문제 해결

user\_map\_query.pl 스크립트를 사용하여 FDM에 사용자 IP 매핑이 있는지 검증할 수 있습니다.

WARNING: This script was not tested on this major version (6.6.0)! The results may be unexpected. Current Time: 06/24/2021 20:45:54 UTC Getting information on username(s)... \_\_\_ User #1: ngfwtac \_ \_ \_ TD: 8 Last Seen: 06/24/2021 20:44:03 UTC for\_policy: 1 Realm ID: 4 Database ------##) IP Address [Realm ID] 1) ::ffff:10.115.117.46 [4] ##) Group Name (ID) [realm: Realm Name (ID)] 1) Domain Users (12) [realm: Active\_Directory (4)] 통화 모드에서는 다음을 구성할 수 있습니다.

리디렉션이 성공했는지 확인하기 위해 시스템에서 identity-debug를 지원합니다.

```
> system support identity-debug
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address: 10.115.117.46
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring identity and firewall debug messages
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-55809 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 2
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 Logging EOF for event from hardware with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 : Received EOF, deleting the snort
session.
10.115.117.46-50611 > 142.250.138.94-443 6 AS 1-1 I 0 deleting firewall session flags = 0x10003,
fwFlags = 0x114
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-65489 > 173.36.131.10-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 deleting firewall session flags = 0x10001,
fwFlags = 0x100
10.115.117.46-53417 > 72.163.47.11-53 17 AS 1-1 I 0 Logging EOF as part of session delete with
rule_id = 1 ruleAction = 2 ruleReason = 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 63784 -> 53, geo 16671760 -> 16671778
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 looked for user_id with realm_id 4 auth_type
```

```
2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 found active binding for user_id 8 in realm
4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 2023803385 user_id =
8 \text{ realm_id} = 4
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 1,
10.115.117.46-63784 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 3, port 50619 -> 443, geo 16671760 -> 16671778
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 looked for user_id with realm_id 4
auth_type 2, returning realm_id 4 auth_type 2 user_id 8
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 found active binding for user_id 8 in
realm 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 matched auth rule id = 2023803385 user_id
= 8 \text{ realm_id} = 4
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 new firewall session
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Action', action Allow and prefilter rule 0
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 HitCount data sent for rule id: 1,
10.115.117.46-50619 > 142.250.138.94-443 6 AS 1-1 I 0 allow action
참조:
```

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptdfdm-identity.html#id\_71535

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-identity-sources.html#task\_83008ECD0DBF4E388B28B6247CB2E64B