# Configurer l'authentification active FDM (portail captif)

## Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Diagramme du réseau Configuration Vérification Dépannage

## Introduction

Ce document décrit un exemple de configuration pour l'intégration de Firepower Device Manager (FDM) avec Active Authentication (Captive-Portal). Cette configuration utilise Active Directory (AD) comme certificats source et auto-signés.

## Conditions préalables

#### **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Threat Defense (FTD)
- Active Directory (AD)
- Certificats auto-signés.
- Secure Socket Layer (SSL)

#### **Components Used**

Les informations de ce document sont basées sur la version logicielle suivante :

- Firepower Threat Defense 6.6.4
- Active Directory
- Test PC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

#### Informations générales

#### Établir l'identité de l'utilisateur via l'authentification active

L'authentification est l'acte de confirmation de l'identité d'un utilisateur. Avec l'authentification active, lorsqu'un flux de trafic HTTP provient d'une adresse IP pour laquelle le système n'a pas de mappage d'identité utilisateur, vous pouvez décider d'authentifier l'utilisateur qui a initié le flux de trafic par rapport au répertoire configuré pour le système. Si l'utilisateur s'authentifie correctement, l'adresse IP est considérée comme ayant l'identité de l'utilisateur authentifié.

L'échec de l'authentification n'empêche pas l'accès au réseau de l'utilisateur. Vos règles d'accès déterminent en fin de compte quel accès fournir à ces utilisateurs.

#### Diagramme du réseau



## Configuration

#### Mettre en oeuvre la stratégie d'identité

Pour activer l'acquisition d'identité utilisateur, afin que l'utilisateur associé à une adresse IP soit connu, vous devez configurer plusieurs éléments

Étape 1. Configurer le domaine d'identité AD

Que vous collectiez l'identité de l'utilisateur de manière active (en demandant l'authentification de l'utilisateur) ou passive, vous devez configurer le serveur Active Directory (AD) qui possède les informations d'identité de l'utilisateur.

Accédez à **Objets > Services d'identité** et sélectionnez l'option **AD** pour ajouter Active Directory.

cisco. Firepower Devic	e Manager Monitoring Policies	Objects Device: firepower	> 🖨 @ ?	* admin * Administrator
Object Types 🗧 🗧	Identity Sources			
C Networks	2 objects		Q Search	+~
S Ports	* NAME	TIPE	VALUE	RADIUS Server
Security Zones	1 LocalidentitySource	LOCAL		RADIUS Server Group
Application Filters				AD
C <sup>9</sup> URLs				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
AnyConnect Client Pro				
State Identity Sources				
L Users				

Ajouter la configuration Active Directory :

Identity Realm is used for Identity Policies and Remot 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	

#### Étape 2. Créer des certificats auto-signés

Afin de créer une configuration de portail captif, vous avez besoin de deux certificats : un pour le portail captif et un pour le déchiffrement SSL.

Vous pouvez créer un certificat auto-signé comme dans cet exemple.

Accédez à Objets > Certificats

cisco. Firepower Devic	e 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	B NAME	туре		Add Internal Certificate
🐨 Application Filters	1 NGFW-Default-InternalCA	Internal CA		Add Trusted CA Certificate
<b>69</b> 1101 e	2 ssl_captive_portal	Internal CA		
OF URLS	3 DefaultInternalCertificate	Internal Certificate		
Geolocations	4 DefaultWebserverCertificate	Internal Certificate		

Certificat auto-signé du portail captif :

Add Internal Certificate	<b>e</b> ×
Name	
captive_portal	
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 ce	rtificate with remote access VPN.
	CANCEL SAVE

Certificat SSL autosigné :

# 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 Name		
ss_fdmcaptive		
You must specify a Common Name to use	e the cert	ificate with remote access VPN.
		CANCEL SAVE

Étape 3. Créer une règle d'identité

Accédez à **Politiques > Identité >** sélectionnez [+] bouton pour ajouter une nouvelle règle d'identité.

Vous devez créer la stratégie d'identité afin de configurer l'authentification active, la stratégie doit comporter les éléments suivants :

- Source de l'identité AD : Identique à l'étape numéro 1
- Action : AUTH ACTIVE
- certificat du serveur: Le même certificat auto-signé que vous avez créé avant [Dans ce scénario, captive\_portal]
- type : HTTP Basic (dans cet exemple de scénario)

Order Title	AD Identity Source	Action ACTIVE AUTHENTICATION	
1 v ad_captive	Active_Directory ~	Active Auth  Active Auth Activ	tor username and password and dentity source to obtain the user
Source / Destination Active authentication		PASSIVE AUTH Identity Sources are needed     h Server Certificate     Q cap	tive_portal:885
SOURCE		ACTIVE AUTH Captive Portal is needed	
Zones + Networks	+ Ports	NO AUTH	+ Ports/Protocols +
ANY ANY	ANY	ANY ANY	ANY

Une fois la stratégie d'identité créée en tant qu'authentification active, crée automatiquement une règle SSL, par défaut cette règle est configurée comme n'importe quelle règle avec **Decrypt-Resign**, ce qui signifie qu'il n'y a aucune modification SSL dans cette règle.

묘 → 🖌	SL Decryption	→ 📀 Identity	$\rightarrow$ $\bigcirc$ Secu	ity Intelligence $ ightarrow$	$\rightarrow$ $\bigcirc$ NAT $\rightarrow$	📀 Access Co	ntrol $ ightarrow$ 🖓 Ir	ntrusion				
SSL Decryption	1 rule						Q Search				\$	÷
		SOURCE			DESTINATION							
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIO	NS
2 🛃 Identity Polic	y Active Authenticat	ion Rules 🚺										
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	E.	
SSL Native Rules	0											
				Th Start i CREATE SSL RUI	ere are no SSL Ru by creating the firs	les yet. t SSL rule. ADD PRE-DEFINE	D RULES					
	SSL Decryption	ightarrow Identity	ightarrow $ ightarrow$ Secu	rity Intelligence —	$\rightarrow$ () NAT $\rightarrow$	Access Co	introl $ ightarrow$ 😵 Ir	ntrusion				

SSL Decryption	The rules generated	in this section a I from rules in th	re automatically le identity policy				Q Search				ф	+
	SSL decry	ption rules are r	hentication. These ead-only. These		DESTINATION							
# NAME	native rule	aiways evaluated es.	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS		ACTIONS
a 🛃 Identity Policy A	ctive Authentica	ation Rules 🧴										
1 ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	E.	
SSL Native Rules	3											
					There are no SSL	Rules yet.						
				S	tart by creating the	first SSL rule.						
				CREATE SS	L RULE Or	ADD PRE-DEFI	INED RULES					

Étape 4. Créer une règle d'accès dans la stratégie de contrôle d'accès

Vous devez autoriser le **port 885/tcp** qui redirige le trafic vers l'authentification du portail captif. Accédez à **Policies > Access Control** et ajoutez la règle d'accès.

Order Tit	tle				Action	_					
1 ~	ad_captive				🔁 Allow 🗸						
Source/Destina	ation Ap	plications URLs	U	sers Intr	usion Policy	File policy	Logging				
SOURCE						DESTINATION	ı				
Zones	+	Networks	+	Ports	+	Zones	+	Networks	+	Ports/Protocols	+
ANY		ANY		ANY		ANY		ANY		\$ 885	

Si vous devez vérifier si les utilisateurs ont été téléchargés à partir d'AD, vous pouvez modifier la règle d'accès et accéder à la section **Utilisateurs**, puis sur **UTILISATEURS DISPONIBLES**, vous pouvez vérifier combien d'utilisateurs le FDM a déjà.

Order Title				Action	
1 ∨ ad_ca	ptive			Allow	<b>~</b>
Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy
AVAILABLE USERS	-			+	L CONTRO
▼ Filter					lf you config address, yo membership
Identity Sources	Groups Users		-		appropriate different ad
Active_Director	y \ <b>luis</b>		*		network acc from one gr
Active_Director	y \ <b>ngfwtac</b>				
Special-Identitie	es-Realm \ No Auth	entica			
Active_Director	y \ ren				
Active_Director	y ∖ sfua				
Active_Director	v \ testuser		-		
Create new Identity Real	m CANCEL	ОК			

N'oubliez pas de déployer les modifications de configuration.

## Vérification

Vérifiez que le périphérique de l'utilisateur reçoit la case à cocher lorsqu'il accède à un site HTTPS.

https://10.115.117.43:885/x.auth: × +										
- > C 🛈 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									

Saisissez les informations d'identification Active Directory de l'utilisateur.

https://10.115.117.43:885/x.auth? ×	F				
← → C ① 10.115.117.43:885/x.	auth?s=dOF7LRChg4FKX2BCiK46	wfdQKDJMAXeaLGcyYeiycu	c%3D&u=http%3A%2F%2Fv	www.cisco.com%2F	
			Sign in https://10.11 Username Password	15.117.43:885	Sign in Cancel
the Cisco - Networking, Cloud, and ⊂ x +	Support & Learn Partners Events	s Videos			Q L ⊕ <sup>us</sup>
Kiva and Cisco retail o	Active	e exploit of Kaseya VSA in supply-	chain attack. Read the Talos blo		time to take the lead
De	E A+ sign Guides Find Training	క్షిస్తే Learning & Certifications	() Software Downloads	දුරිය Cisco Community	Activate Windows Tech Support Cases

# Dépannage

Vous pouvez utiliser le script user\_map\_query.pl pour valider le mappage IP utilisateur de FDM

user_map_query.pl	-u username	> fc	or use	users	
user_map_query.pl	-i x.x.x.x	> fc	or ip	addresses	
root@firepower:~#	user_map_que	ery.pl -	u ngi	wtac	

```
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)]
En mode clish, vous pouvez configurer :
```

le système prend en charge identity-debug pour vérifier si la redirection a réussi.

```
> 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
```

```
Référence:
```

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