Configurer l'authentification active FDM (portail captif)

Contenu

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.

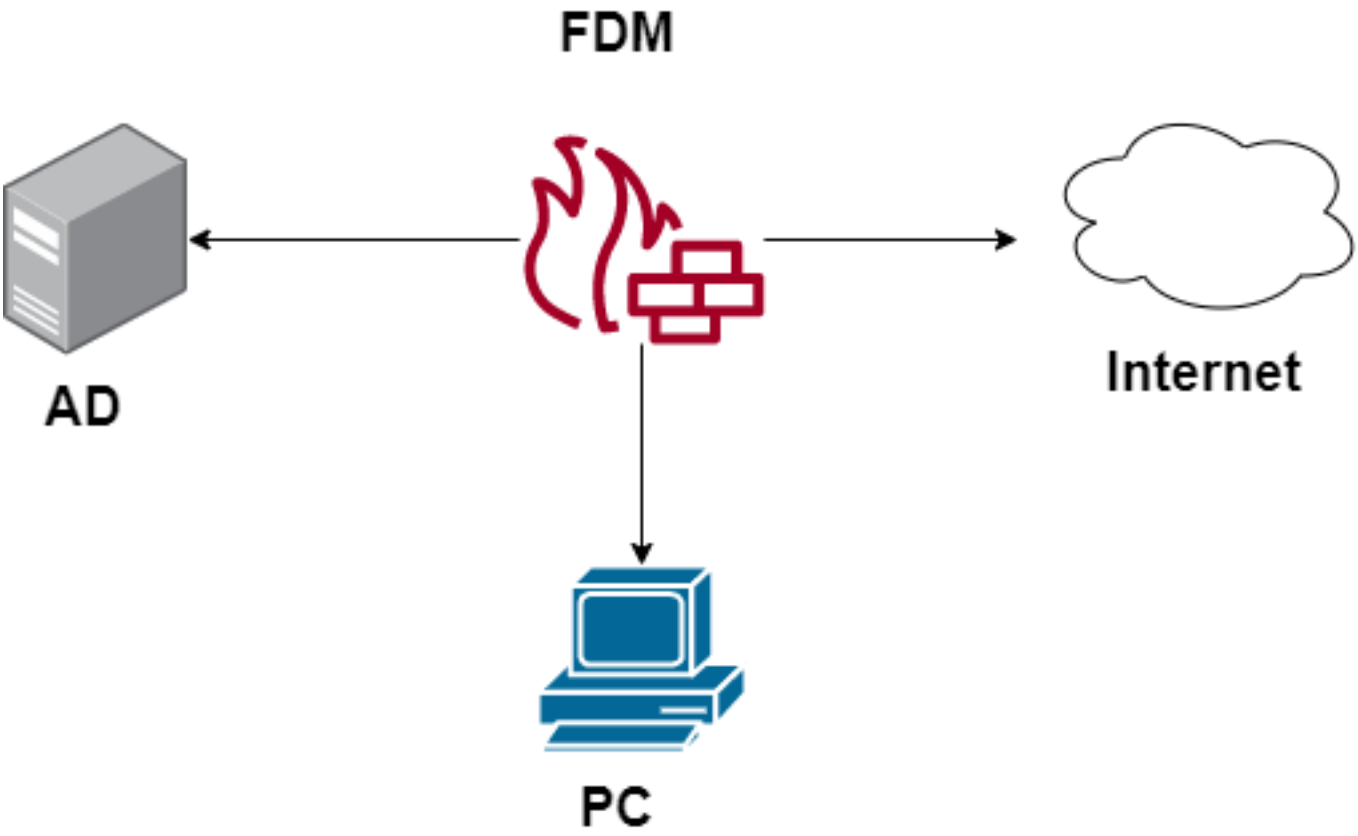
Informations générales

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

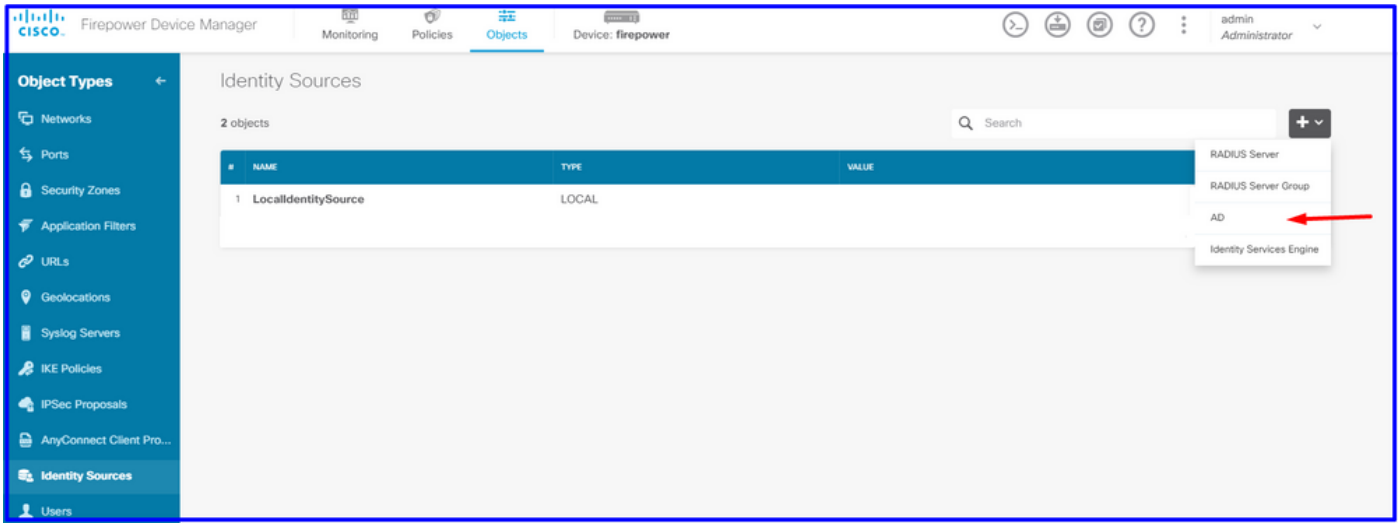
Mettre en oeuvre la stratégie d'identité

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

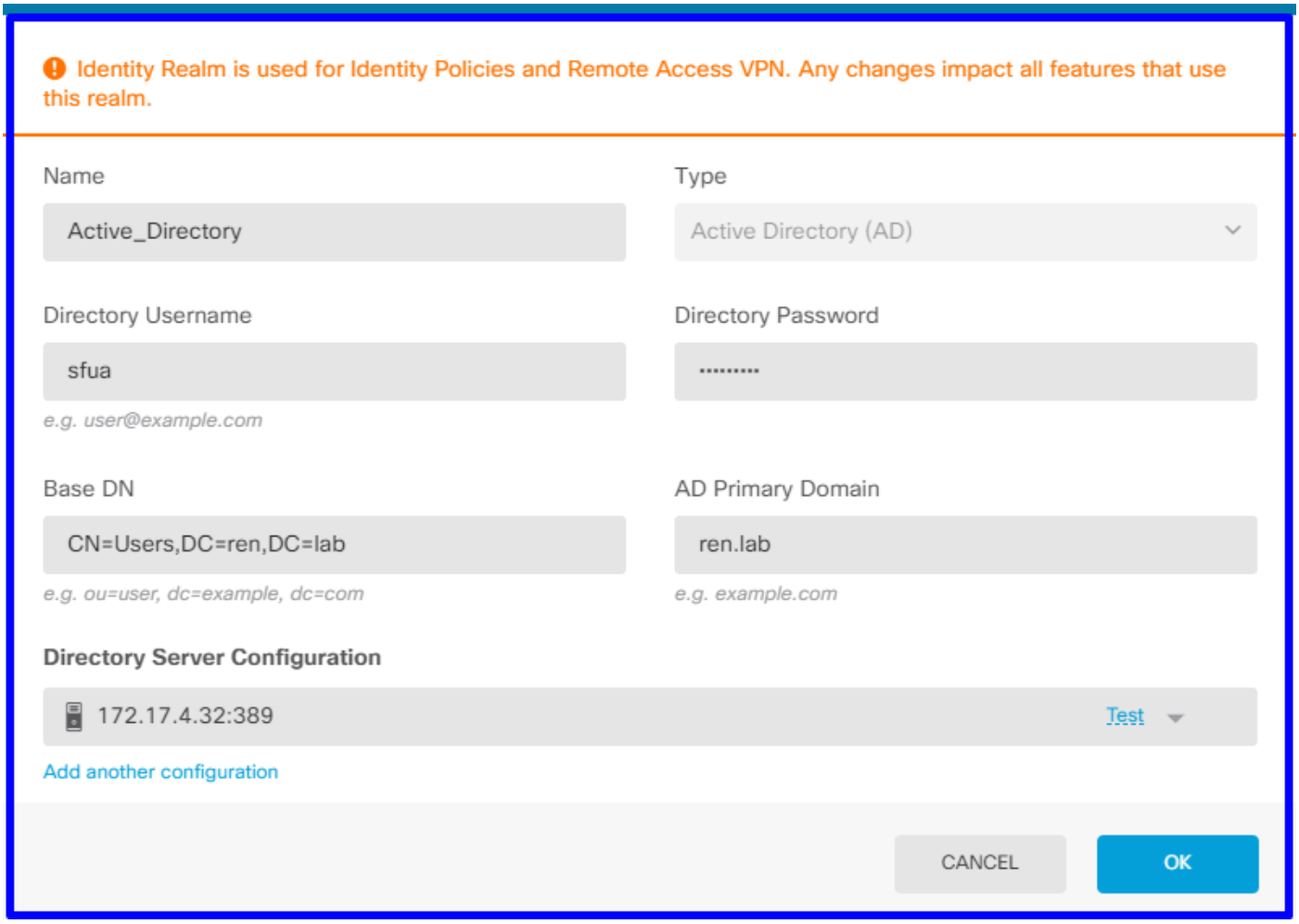
Étape 1. Configurer le domaine d'identité AD

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.



Ajouter la configuration Active Directory :

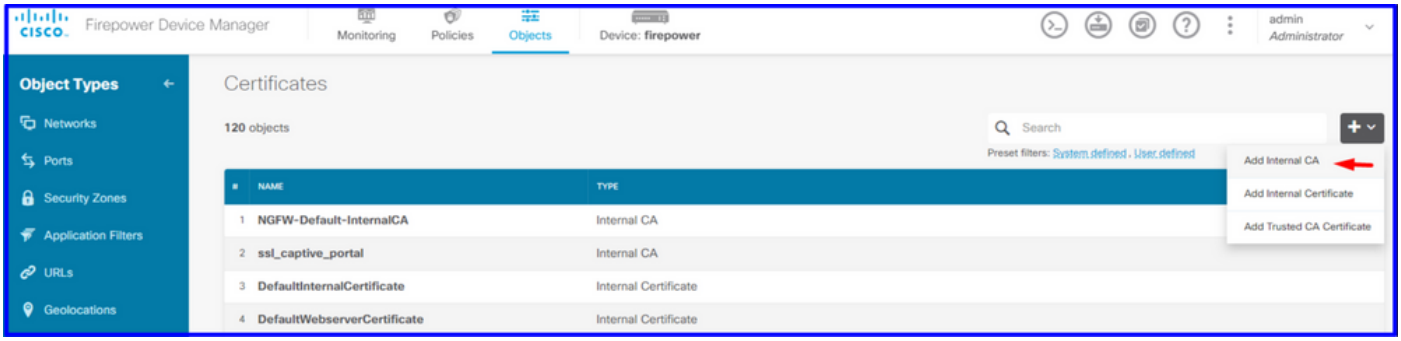


Étape 2. Créer des certificats auto-signés

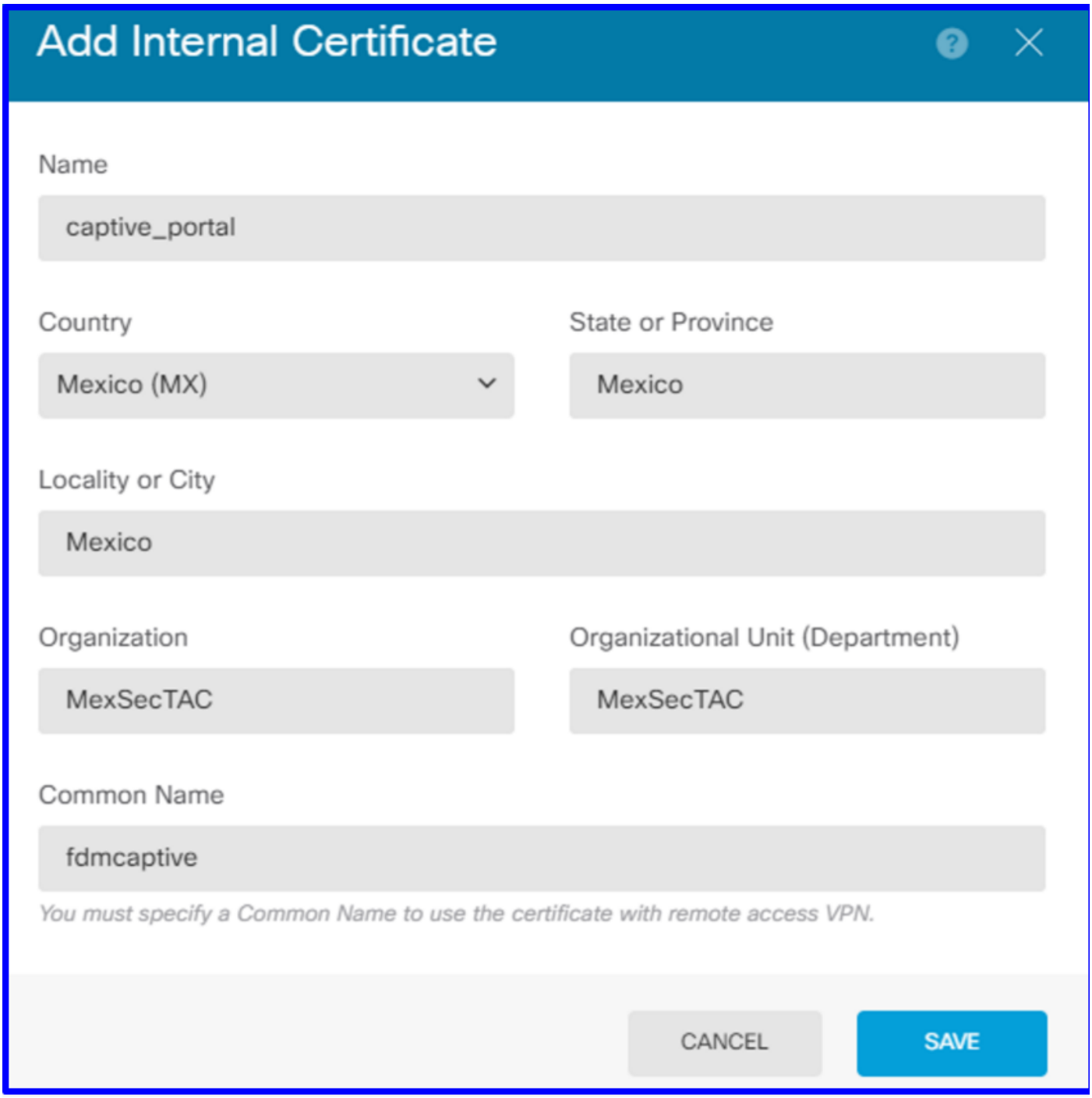
Afin de créer une configuration de portail captif, vous avez besoin de deux certificats : un pour le portail captif et un pour le déchiffrement SSL.

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

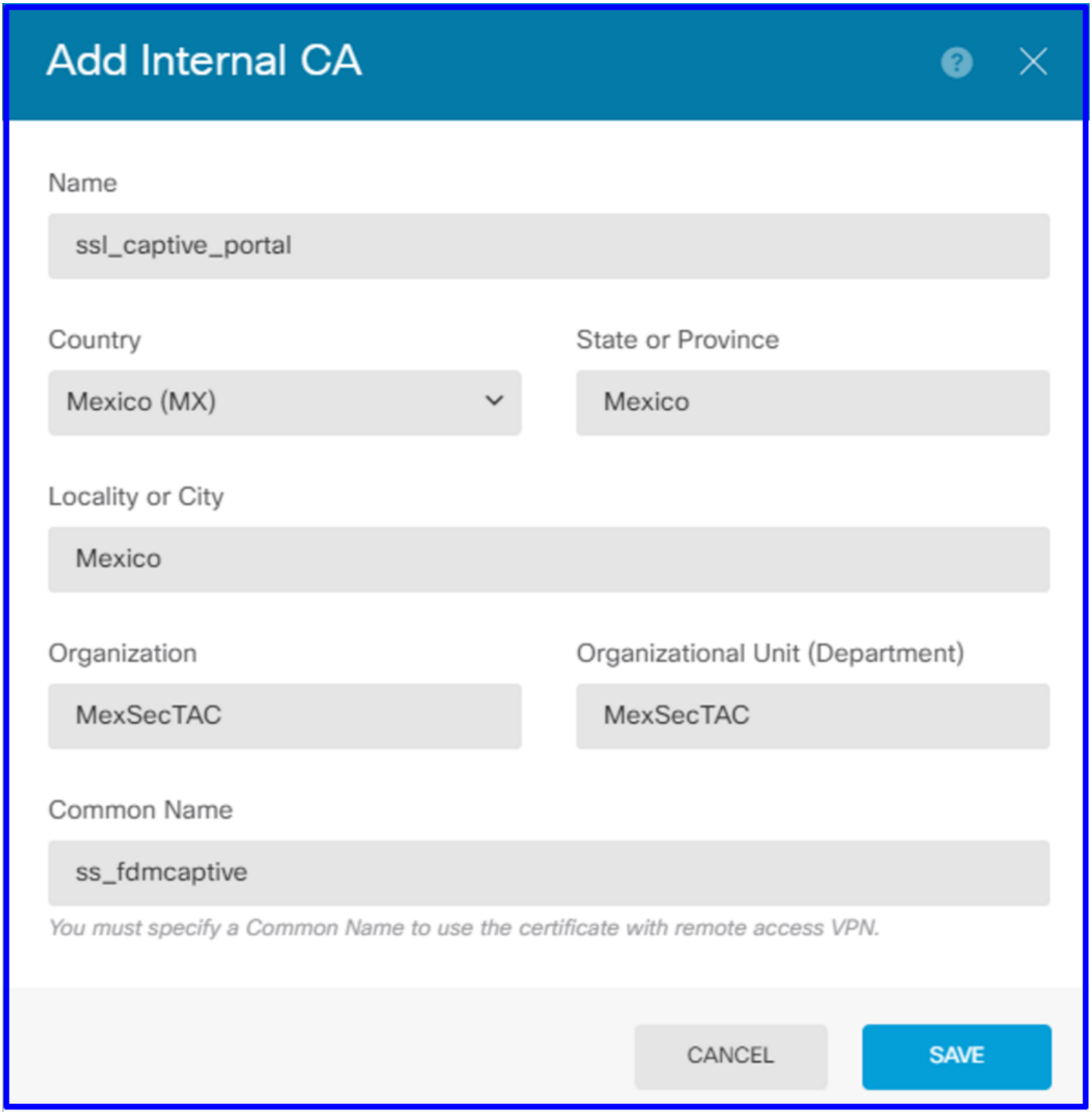
Accédez à **Objets** > **Certificats**



Certificat auto-signé du portail captif :



Certificat SSL autosigné :

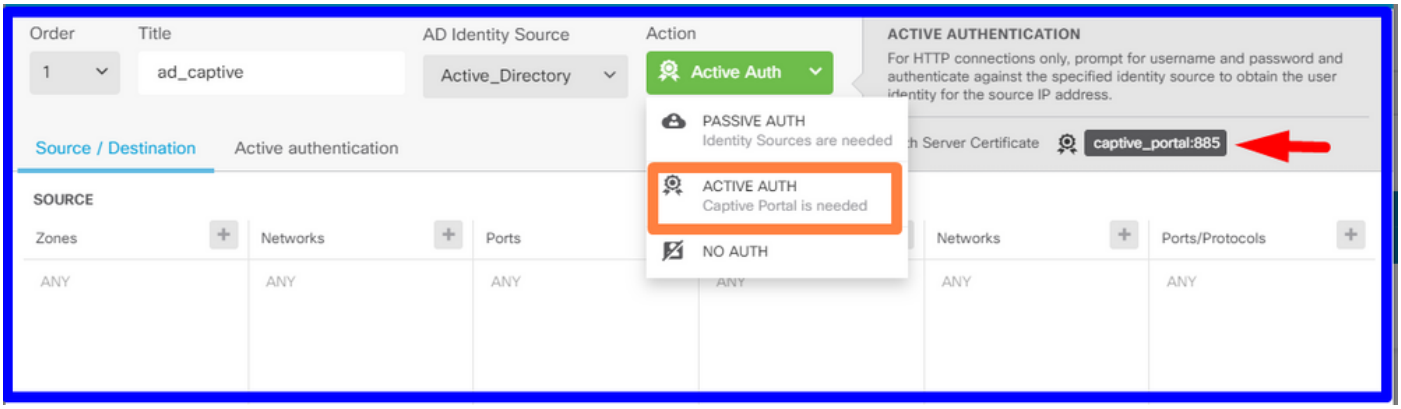


Étape 3. Créer une règle d'identité

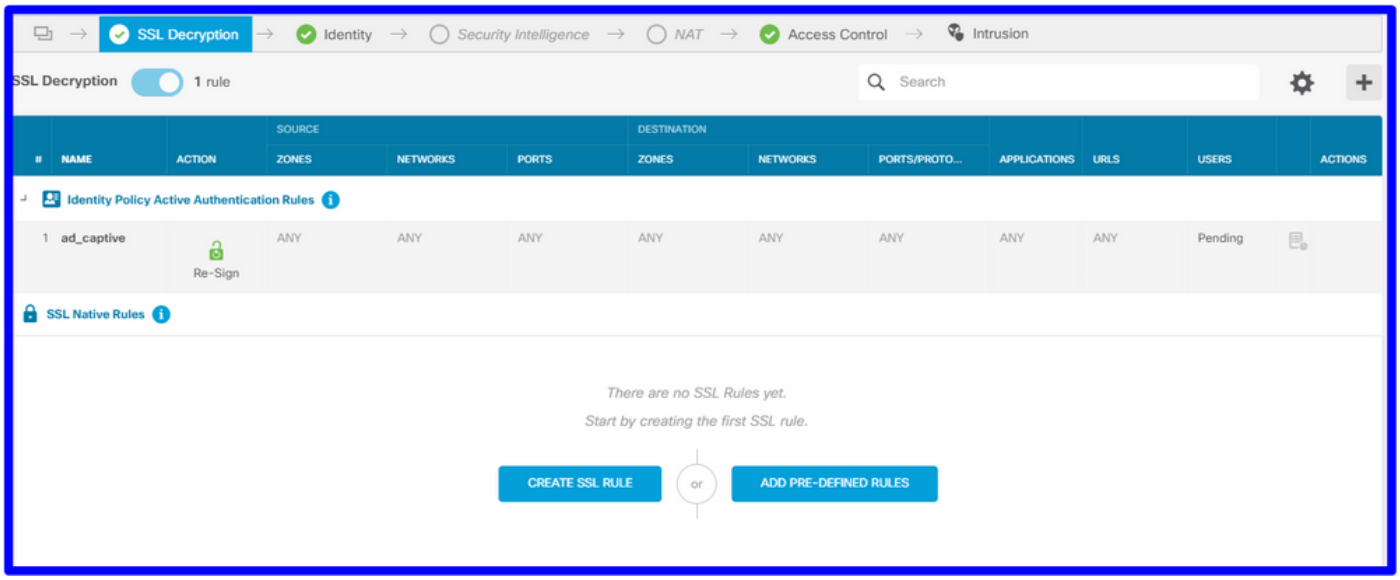
Accédez à **Politiques > Identité >** sélectionnez **[+]** bouton pour ajouter une nouvelle règle d'identité.

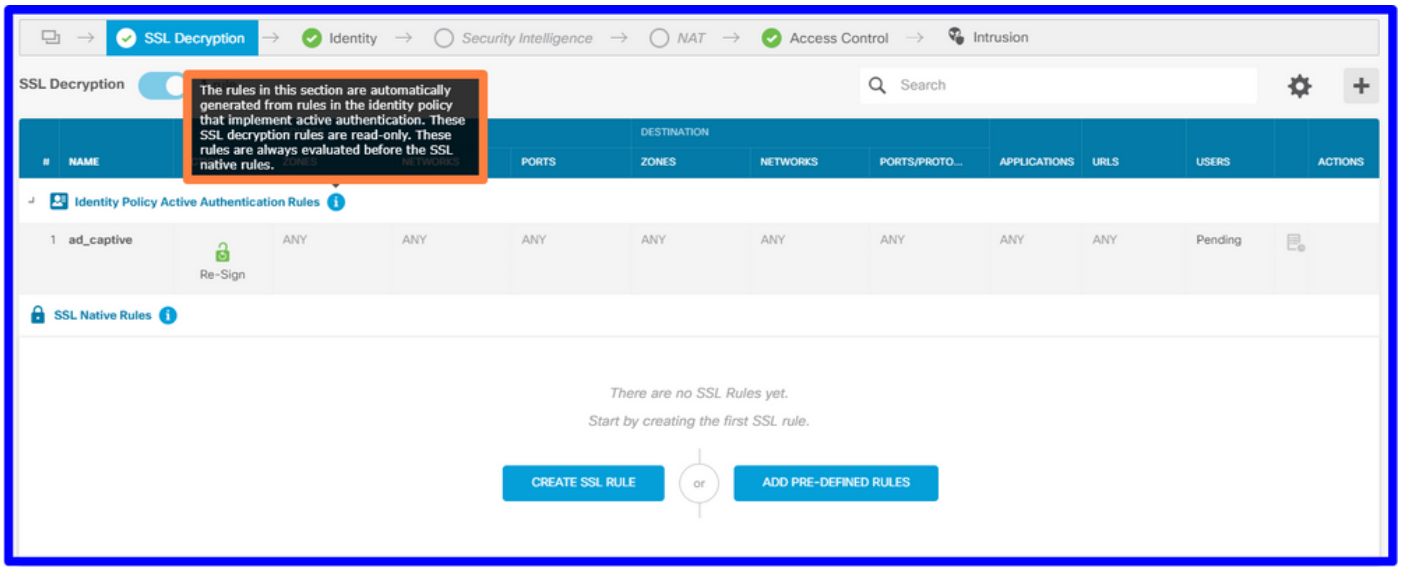
Vous devez créer la stratégie d'identité afin de configurer l'authentification active, la stratégie doit comporter les éléments suivants :

- 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)



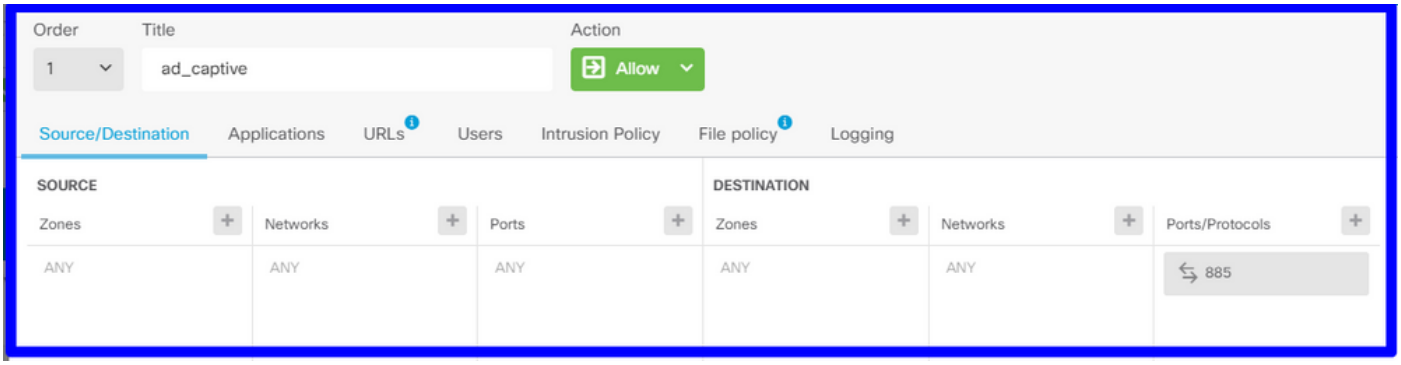
Une fois la stratégie d'identité créée en tant qu'authentification active, crée automatiquement une règle SSL, par défaut cette règle est configurée comme n'importe quelle règle avec **Decrypt-Resign**, ce qui signifie qu'il n'y a aucune modification SSL dans cette règle.



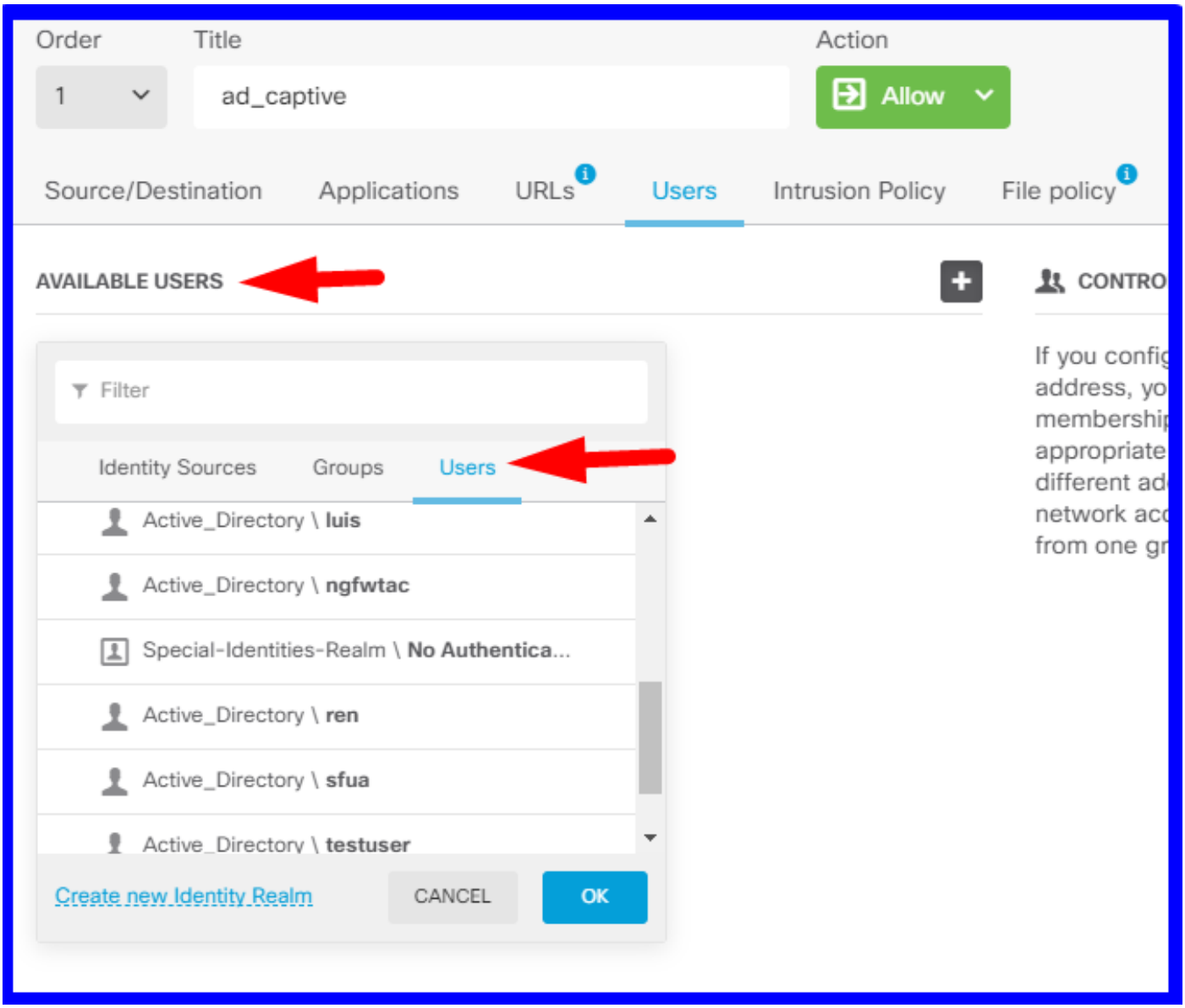


Étape 4. Créer une règle d'accès dans la stratégie de contrôle d'accès

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.



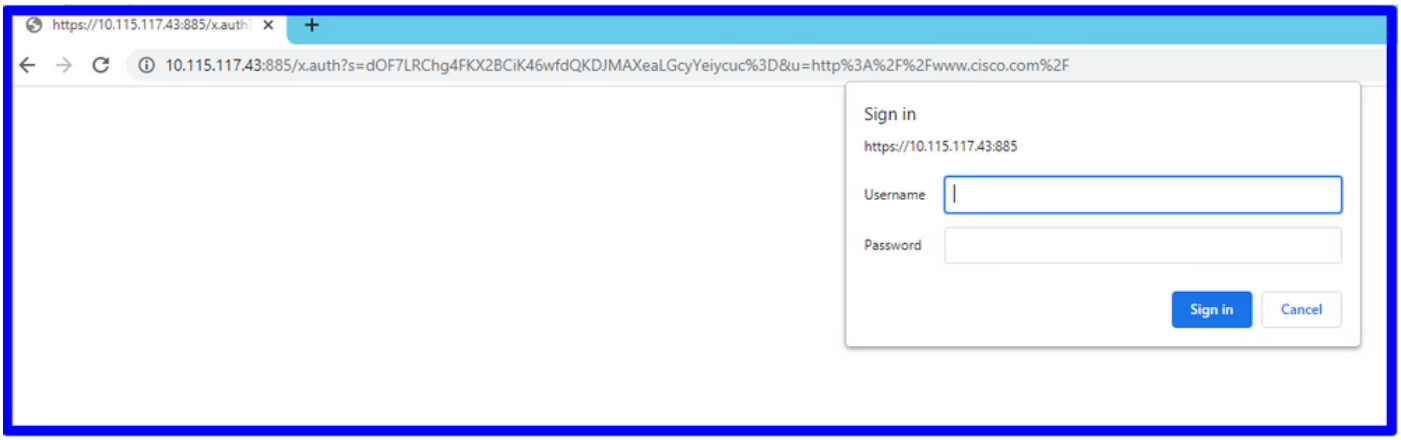
Si vous devez vérifier si les utilisateurs ont été téléchargés à partir d'AD, vous pouvez modifier la règle d'accès et accéder à la section **Utilisateurs**, puis sur **UTILISATEURS DISPONIBLES**, vous pouvez vérifier combien d'utilisateurs le FDM a déjà.



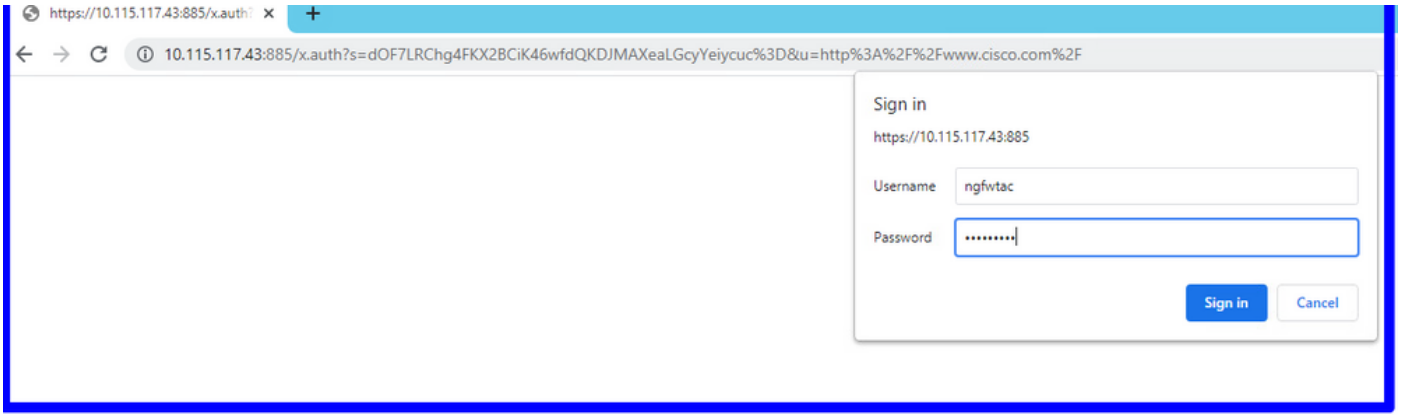
N'oubliez pas de déployer les modifications de configuration.

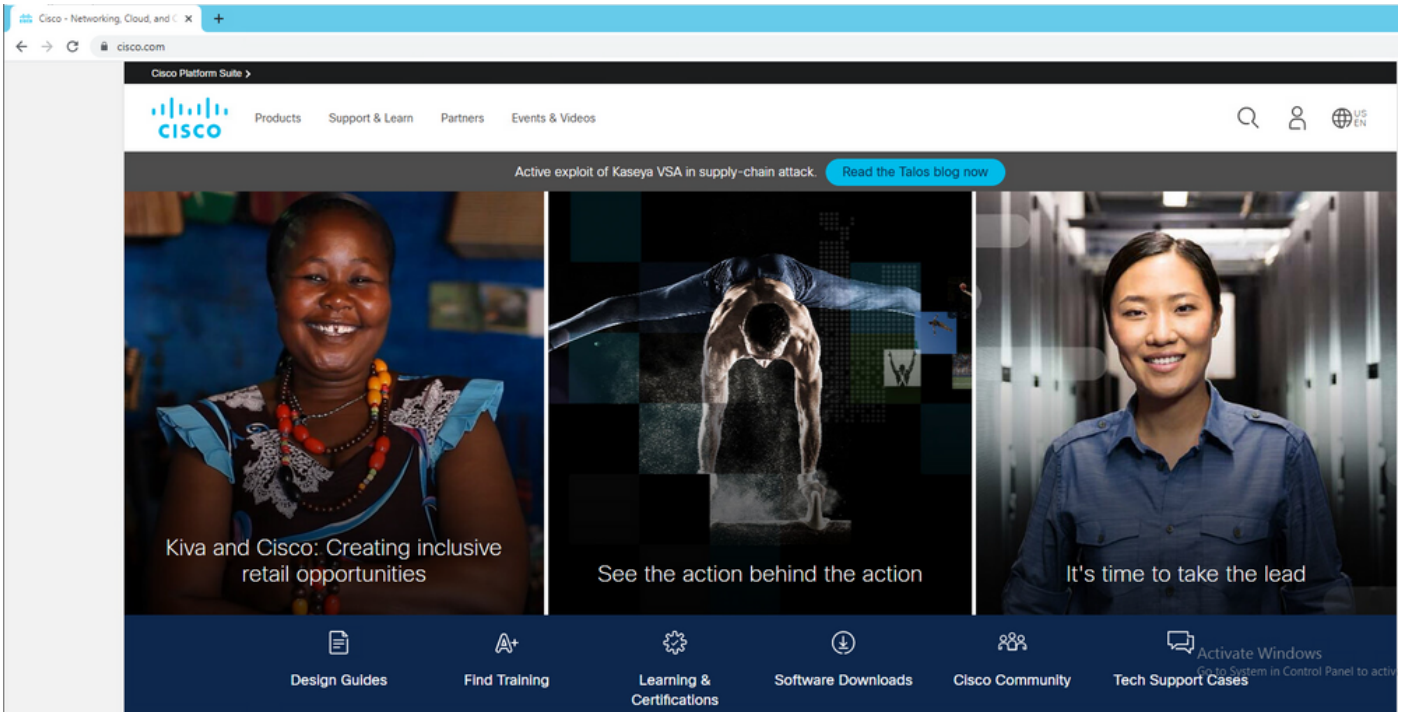
Vérification

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



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





Dépannage

Vous pouvez utiliser le script **user_map_query.pl** pour valider le mappage IP utilisateur de FDM

```
user_map_query.pl -u username ---> for users
user_map_query.pl -i x.x.x.x  ---> for ip addresses
root@firepower:~# user_map_query.pl -u ngfwtac
```

```
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
---
ID:         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 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 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/fptd-fdm-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