FDMアクティブ認証の構成（キャプティブポータル）

内容

概要

このドキュメントでは、アクティブ認証（キャプティブポータル）統合を使用したFirepower Device Manager(FDM)の設定例について説明します。この設定では、ソースおよび自己署名証明書としてActive Directory(AD)を使用します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Firepower Threat Defense（FTD）
- Active Directory（AD）
- 自己署名証明書：
- Secure Socket Layer (SSL)

使用するコンポーネント

この文書の情報は、次のソフトウェアのバージョンに基づいています。

- Firepower Threat Defense 6.6.4
- Active Directory
- PCテスト

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

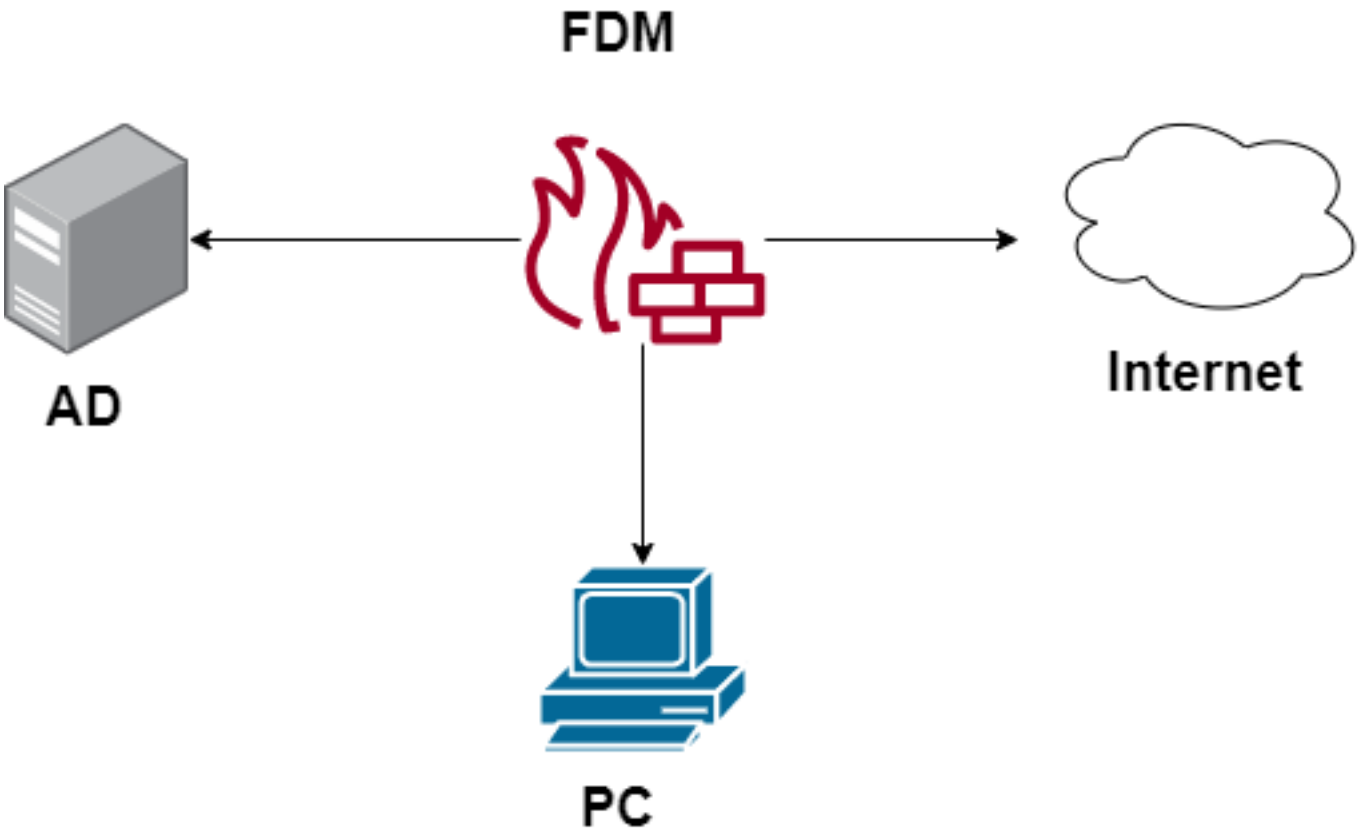
背景説明

アクティブ認証によるユーザIDの確立

認証は、ユーザのアイデンティティを確認する行為です。アクティブ認証では、システムにユーザIDマッピングがないIPアドレスからHTTPトラフィックフローが着信した場合、システムに設定されたディレクトリに対してトラフィックフローを開始したユーザを認証するかどうかを決定できます。ユーザが正常に認証されると、そのIPアドレスは認証されたユーザのアイデンティティを持つと見なされます。

認証に失敗しても、ユーザのネットワークアクセスは妨げられません。アクセスルールは、最終的に、これらのユーザに提供するアクセスを決定します。

ネットワーク図



設定

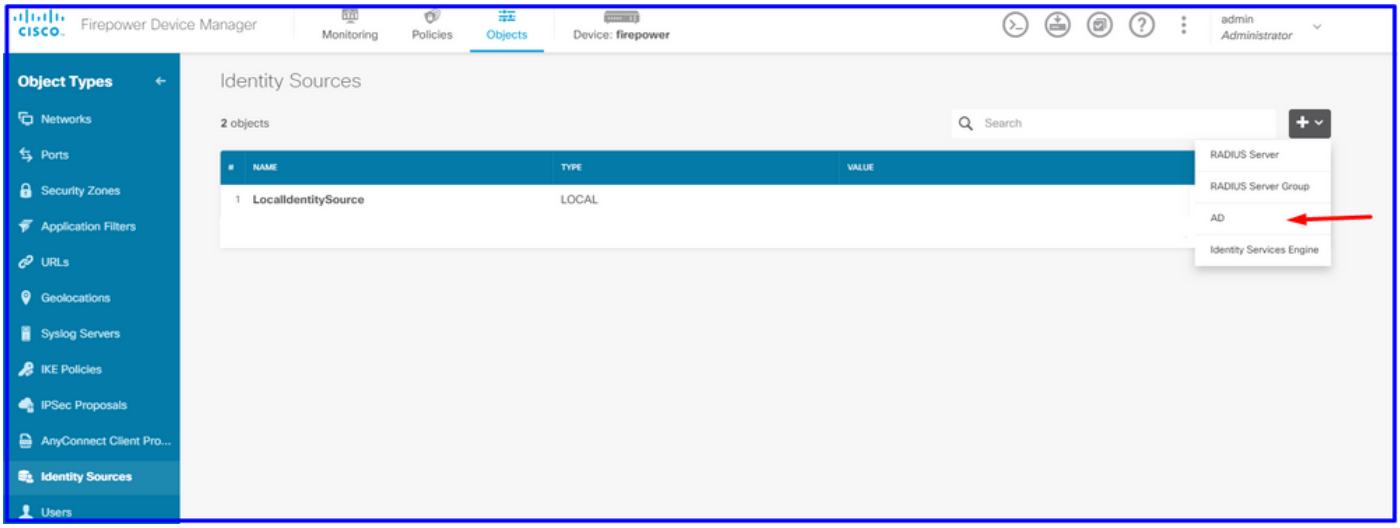
アイデンティティポリシーの実装

IPアドレスに関連付けられたユーザが認識されるようにユーザIDを取得できるようにするには、いくつかの項目を設定する必要があります

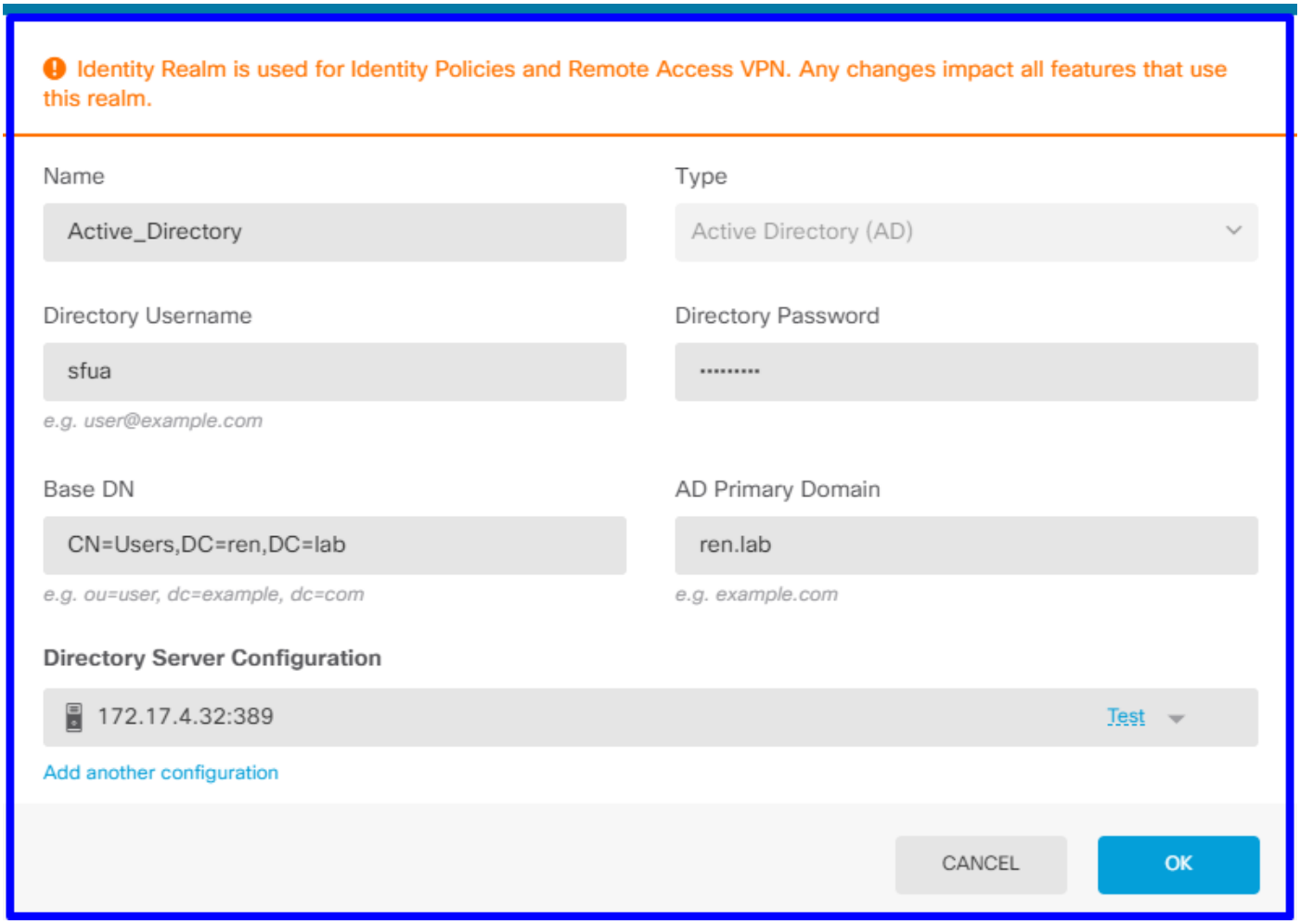
ステップ1:ADアイデンティティレルムの設定

ユーザIDをアクティブに（ユーザ認証のプロンプトで）収集するか、パッシブに収集するかにかかわらず、ユーザID情報を持つActive Directory(AD)サーバを設定する必要があります。

[Objects] > [Identity Services]の順に移動し、[AD]オプションを選択してActive Directoryを追加します。



Active Directory設定を追加します。

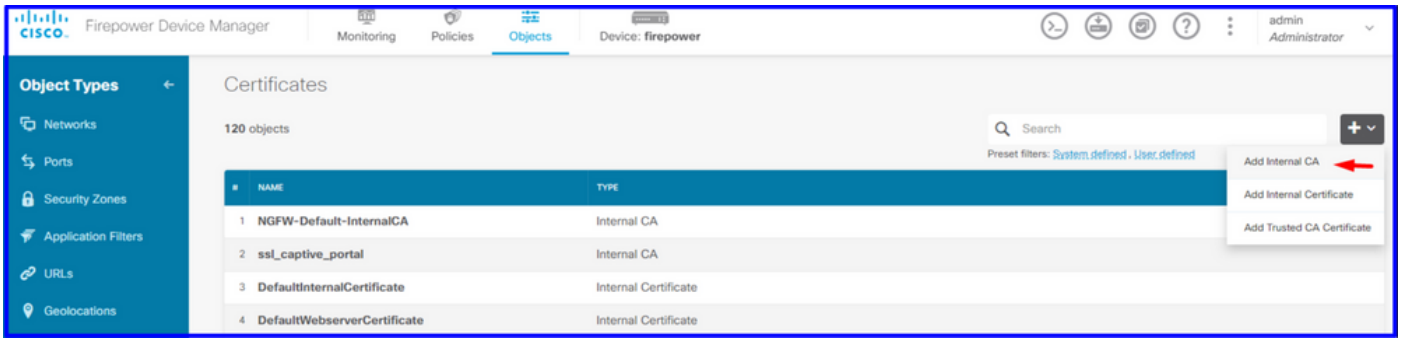


手順2：自己署名証明書の作成

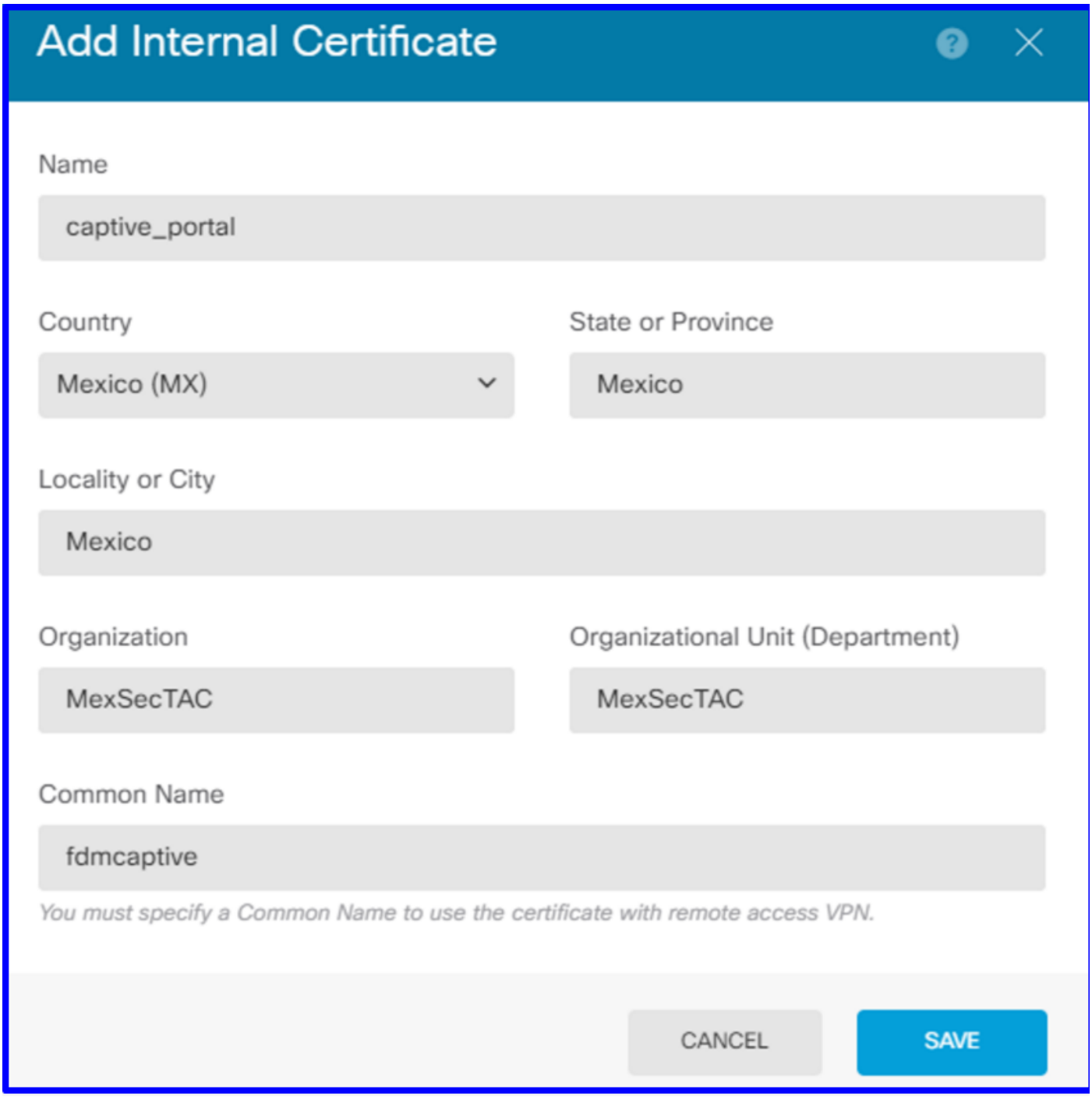
キャプティブポータル設定を作成するには、キャプティブポータル用とSSL復号化用の2つの証明書が必要です。

この例のように、自己署名証明書を作成できます。

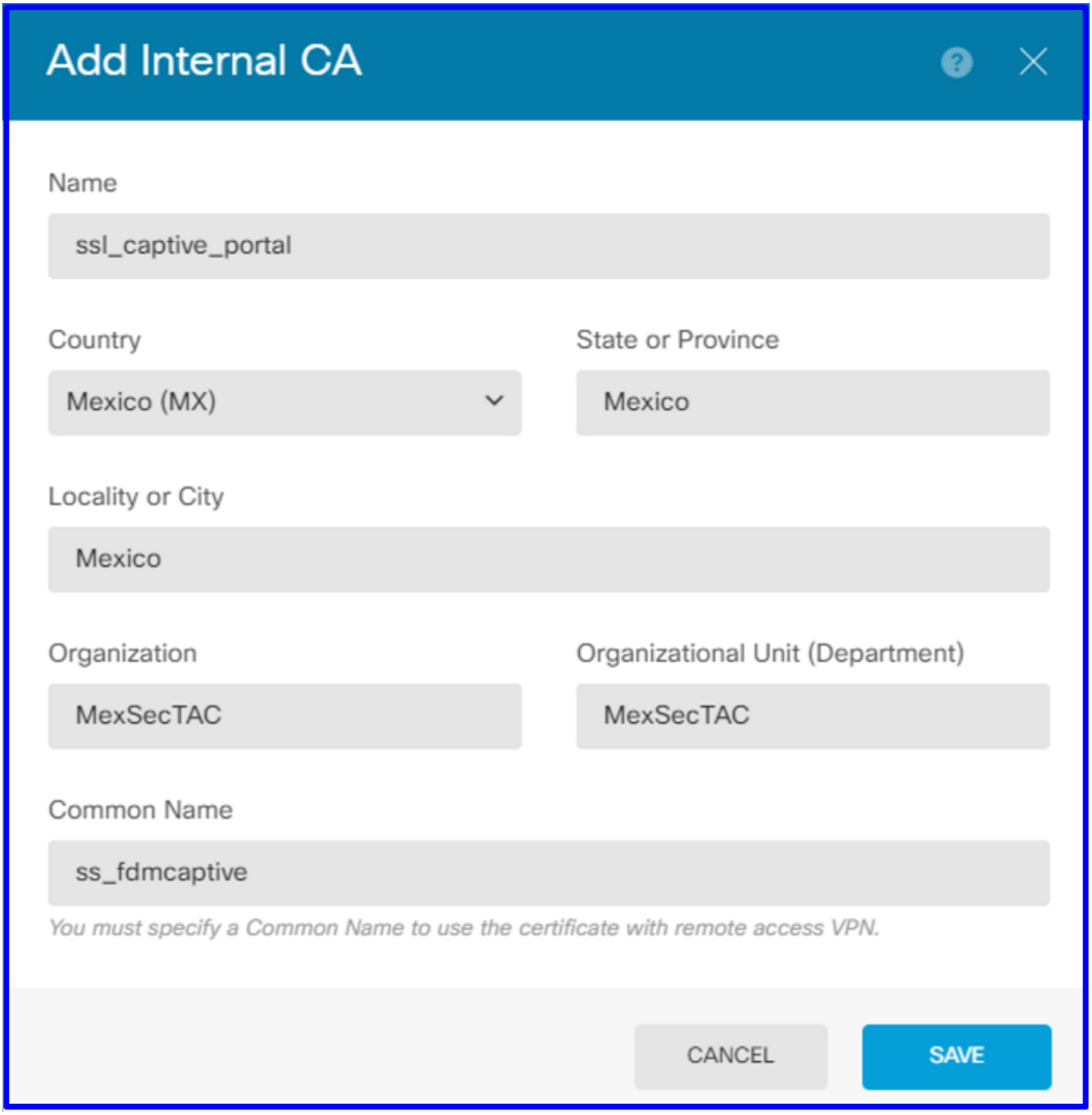
[Objects] > [**Certificates]に移動**します。



キャプティブポータル自己署名証明書：



SSL自己署名証明書：

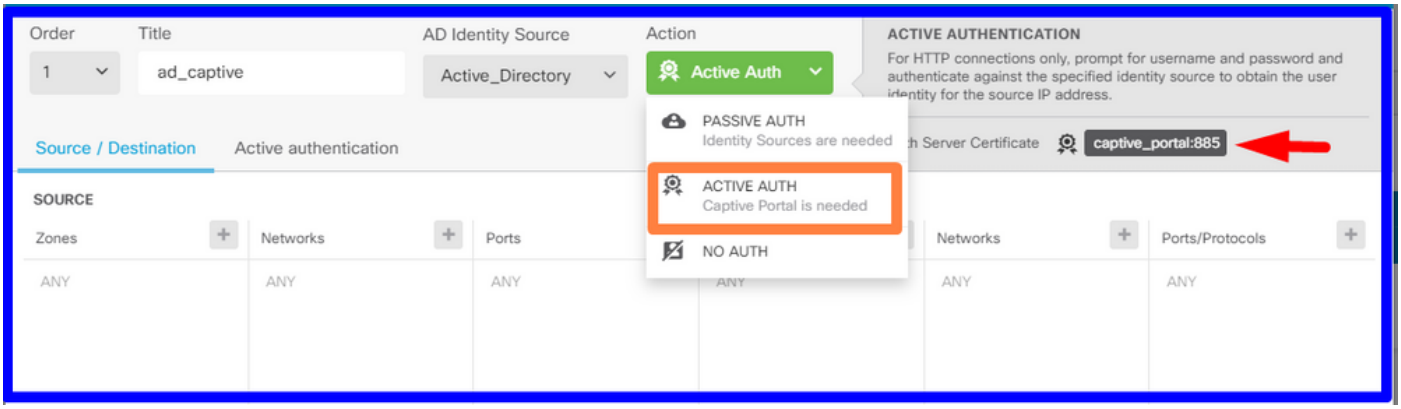


ステップ3:IDルールの作成

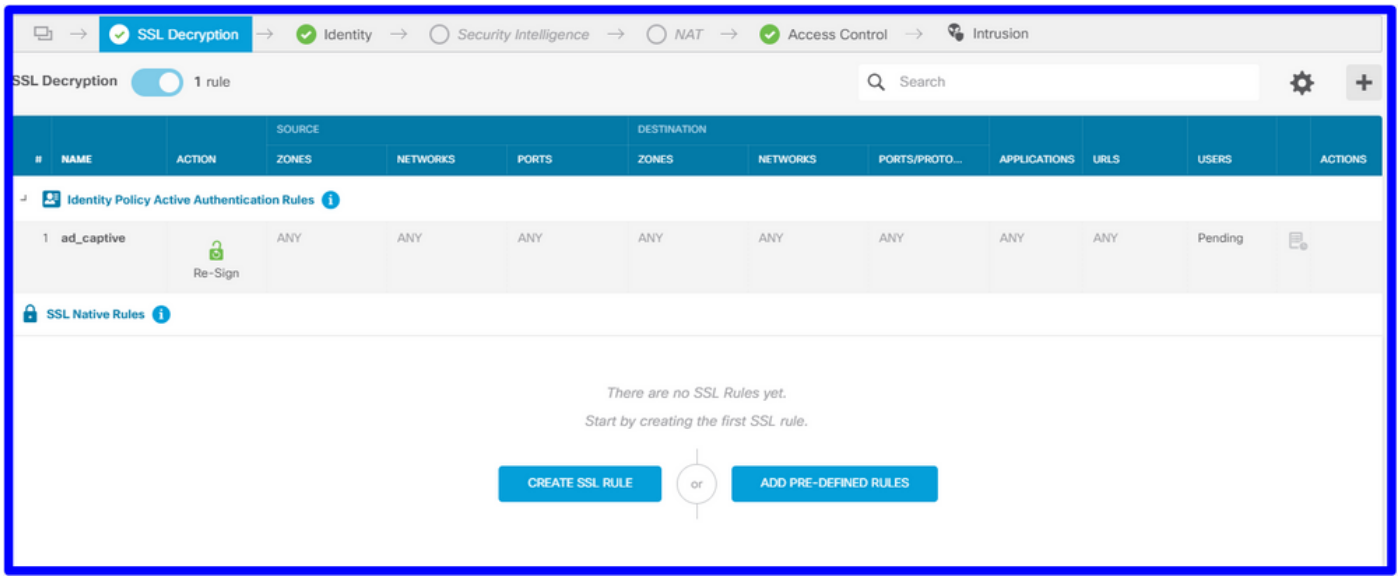
[Policies] > [Identity] > [select **[+]**ボタンに移動し、新しいアイデンティティルールを追加します。

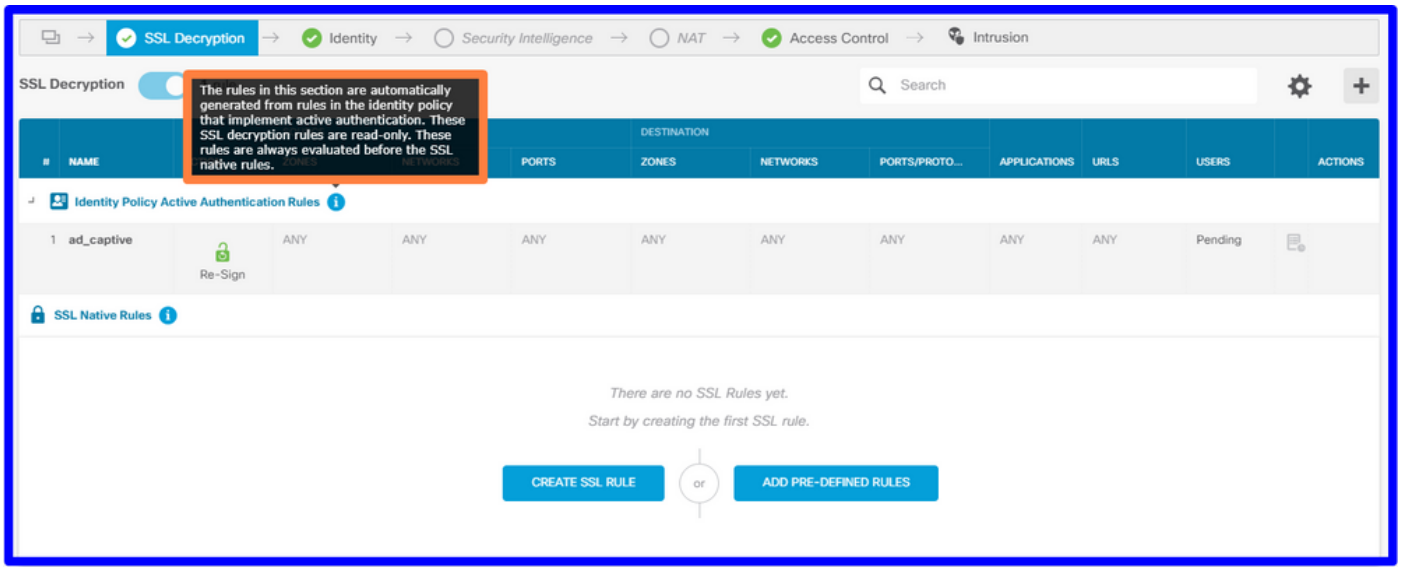
アクティブ認証を設定するには、アイデンティティポリシーを作成する必要があります。ポリシーには次の要素が含まれている必要があります。

- AD IDソース：手順1で追加したものと同じ
- Action:アクティブ認証
- サーバ証明書：前に作成したのと同じ自己署名証明書[このシナリオではcaptive_portal]
- Type:HTTP Basic（この例では）



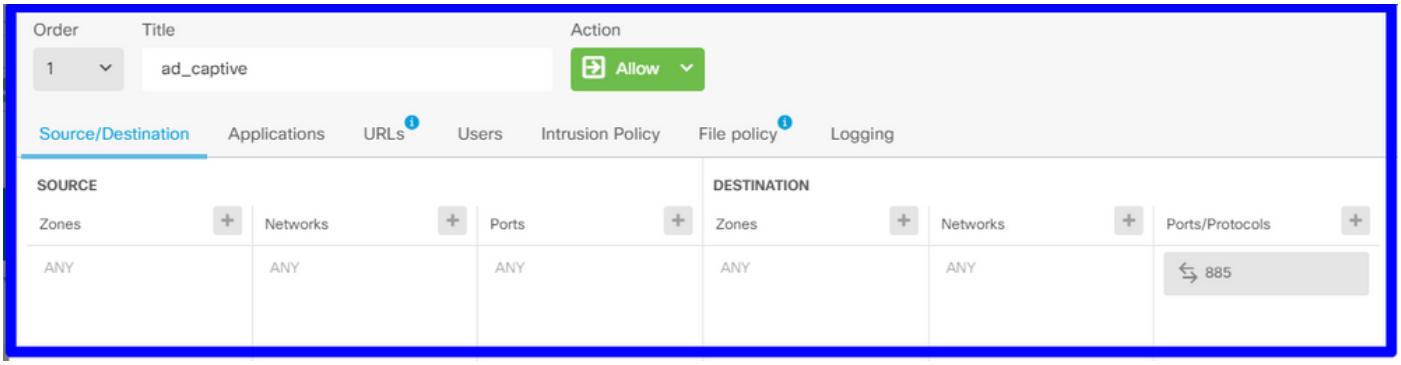
アイデンティティポリシーがアクティブ認証として作成されると、は自動的にSSLルールを作成します。デフォルトでは、このルールは**Decrypt-Resignを使用してanyとして設定されます。つまり、このルールに対するSSL変更はありません。**



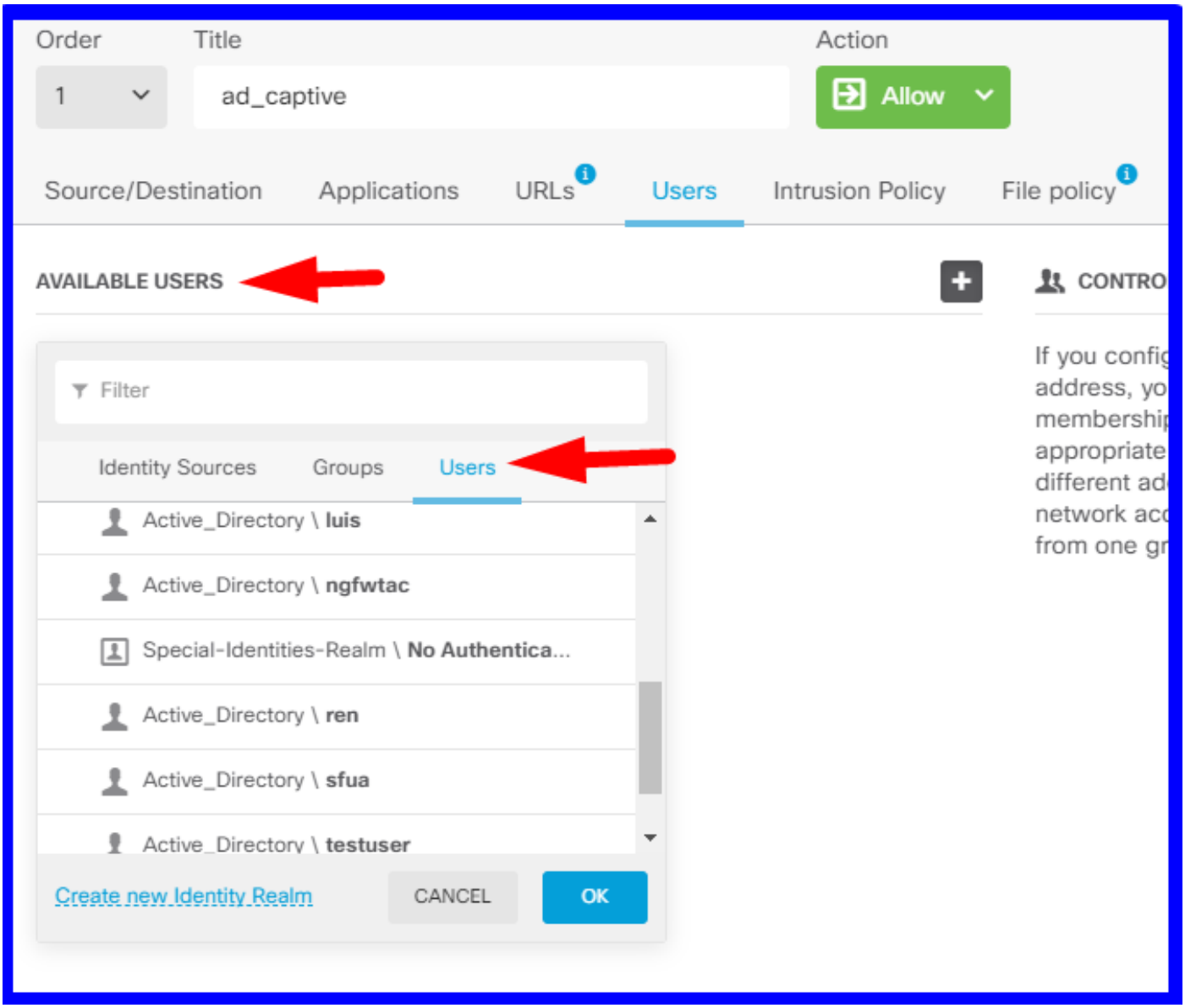


ステップ4：アクセスコントロールポリシーへのアクセスルールの作成

ポート885/tcpを許可して、**キャプティブポータル**認証にトラフィックをリダイレクトする必要があります。[Policies] > [Access Control] に移動し、アクセスルールを追加します。



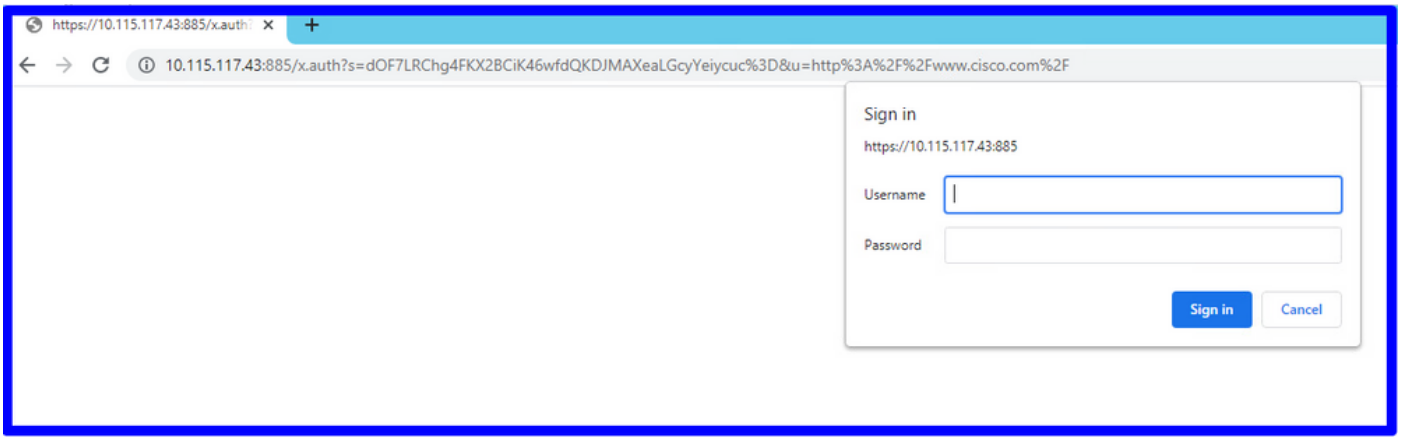
ユーザーがADからダウンロードされたかどうか確認する必要がある場合、アクセス・ルールを編集して「ユーザー」セクションに移動し、「AVAILABLE USERS」で、FDMがすでに持っているユーザー数を確認できます。



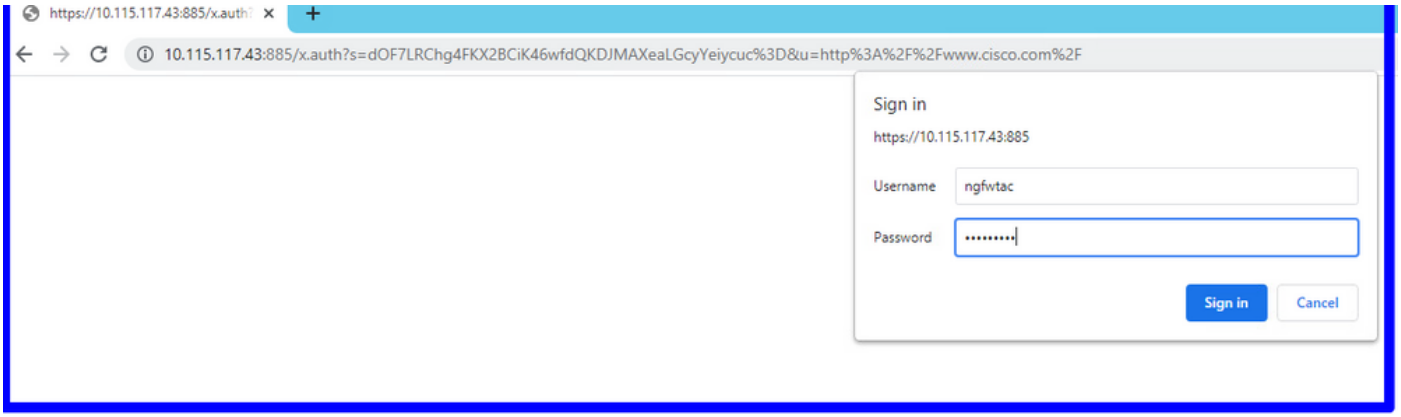
設定変更を必ず導入してください。

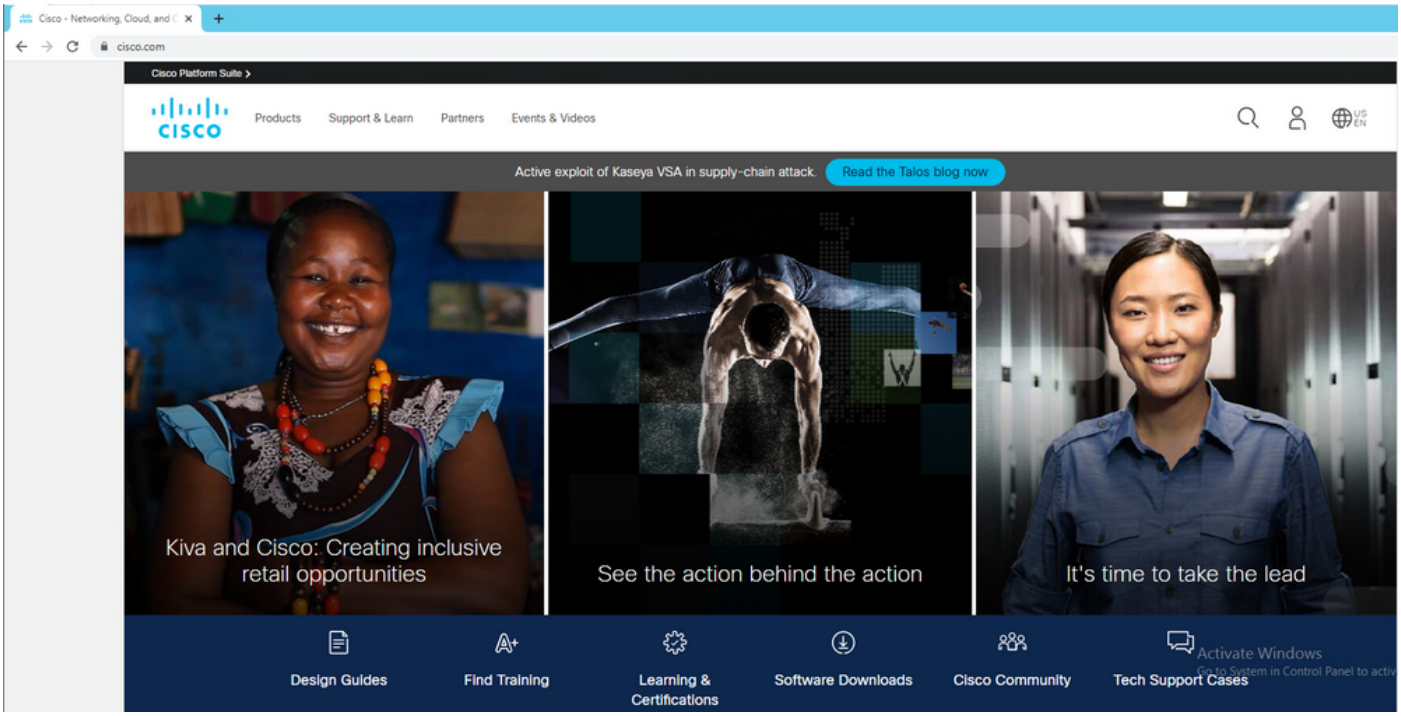
確認

HTTPSサイトに移動するときに、ユーザのデバイスがチェックボックスをオンになっていることを確認します。



ユーザADクレデンシャルを入力します。





トラブルシュート

user_map_query.plスクリプトを使用して、FDMにユーザipマッピングがあることを検証できます

```
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)]
```

clishモードでは、次のように設定できます。

system support identity-debug」を参照してください。

```
> 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
```

参考資料

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