تكوين المصادقة النشطة ل FDM (البوابة المقيدة)

المحتويات

المقدمة

يصف هذا المستند مثال لتكوين مدير أجهزة FirePOWER (FDM) باستخدام كامل المصادقة النشطة (Captive-Portal). يستخدم هذا التكوين خدمة Active Directory (AD) كشهادات المصدر والتوقيع الذاتي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الدفاع ضد تهديد FirePOWER (FTD) من Cisco
- خدمة Active Directory (AD)
- شهادات موقعة ذاتيا.
- طبقة مأخذ التوصيل الآمنة (SSL)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدار البرنامج التالي:

- الدفاع ضد تهديد Firepower 6.6.4
- خدمة Active Directory
- إختبار الكمبيوتر

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

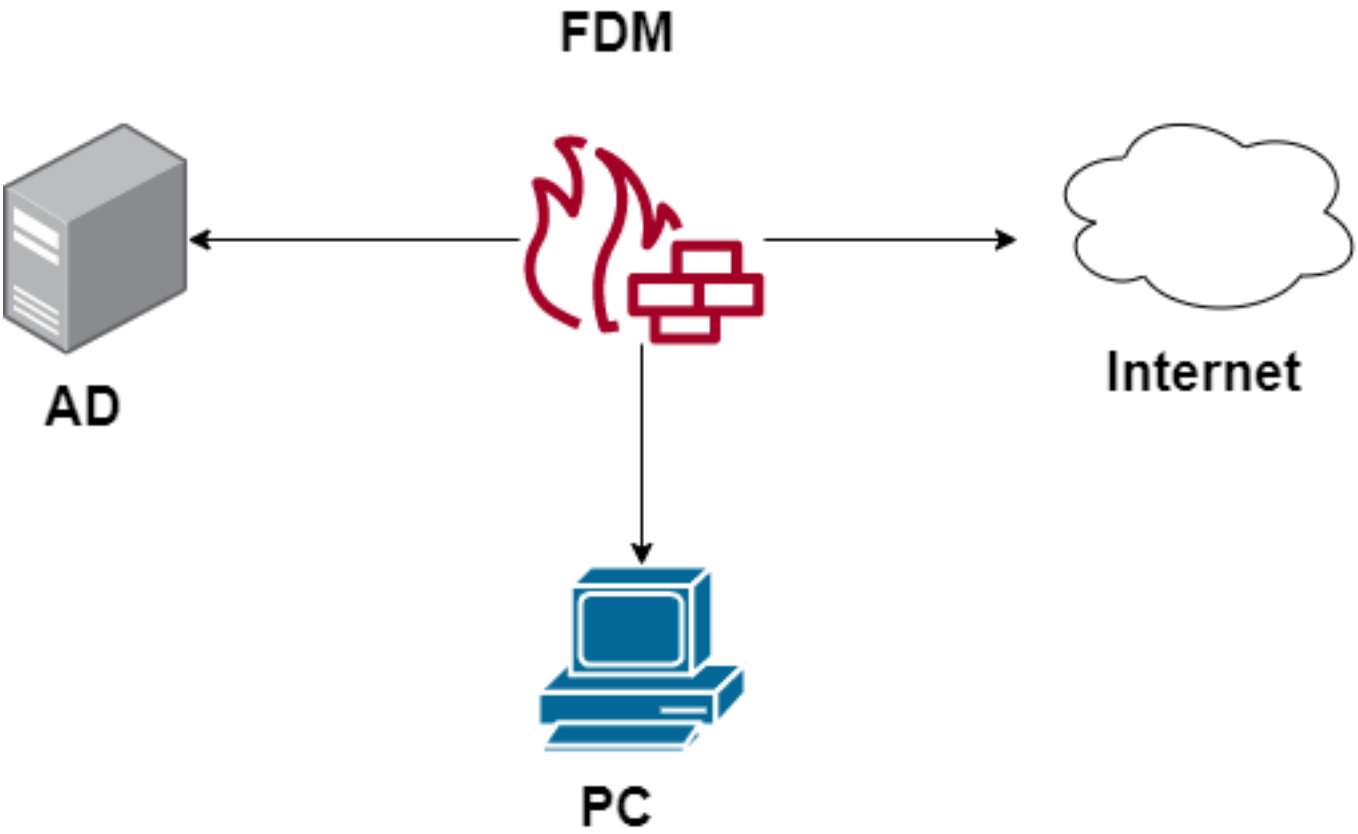
معلومات أساسية

إنشاء هوية مستخدم من خلال المصادقة النشطة

المصادقة هي إجراء لتأكيد هوية مستخدم ما. باستخدام المصادقة النشطة، عندما يأتي تدفق حركة مرور HTTP من عنوان IP ال يتضمن النظام تعيين هوية المستخدم له، يمكنك تحديد ما إذا كنت ستصادق المستخدم الذي بدأ تدفق حركة مرور البيانات مقابل الدليل الذي تم تكوينه للنظام أم ال. في حالة مصادقة المستخدم بنجاح، يتم إعتبار عنوان IP لديه هوية المستخدم الذي تمت مصادقته.

ال يمنع الفشل في المصادقة وصول المستخدم إلى الشبكة. تحدد قواعد الوصول الخاصة بك في نهاية المطاف الوصول الذي سيتم توفيره لهؤالء المستخدمين.

الرسم التخطيطي للشبكة



التكوين

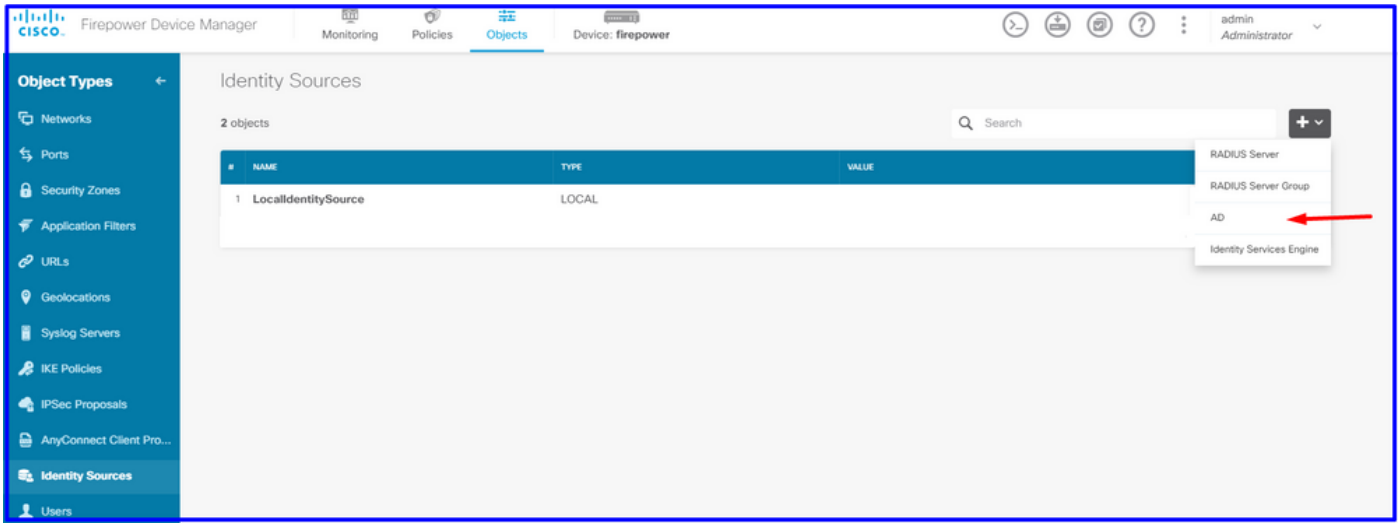
تنفيذ سياسة الهوية

لتمكين الحصول على هوية المستخدم، بحيث يكون المستخدم المقترن بعنوان IP معروف، تحتاج إلى تكوين عدة عناصر

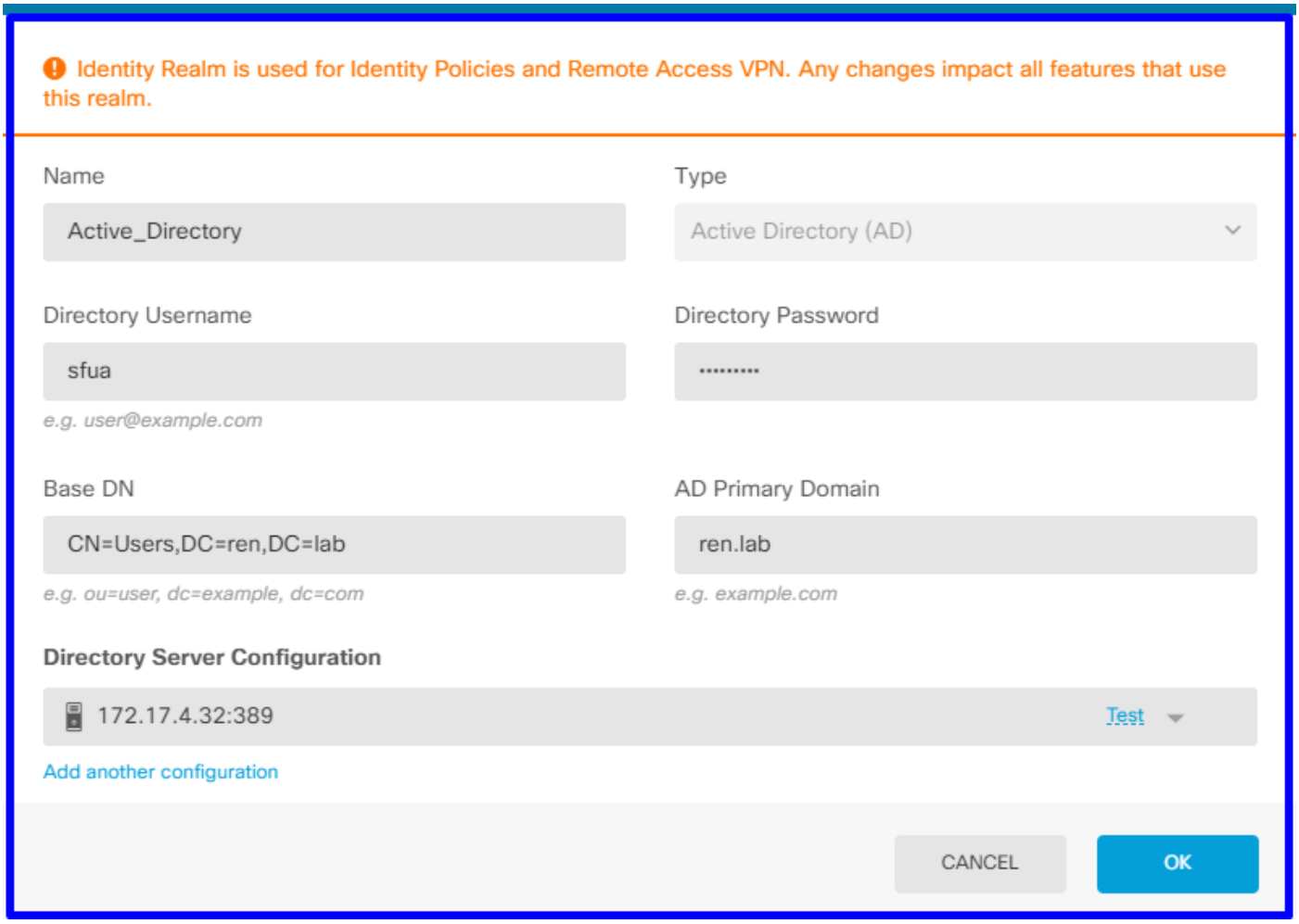
الخطوة 1. تكوين نطاق هوية AD

سواء قمت بجمع هوية المستخدم بشكل نشط (من خلال اإليعاز بمصادقة المستخدم) أو بشكل سلبي، تحتاج إلى تكوين خادم Active Directory (AD) الذي يحتوي على معلومات هوية المستخدم.

انتقل إلى **كائنات > خدمات الهوية** وحدد الخيار **AD** إلضافة Active Directory.



إضافة تكوين Active Directory:

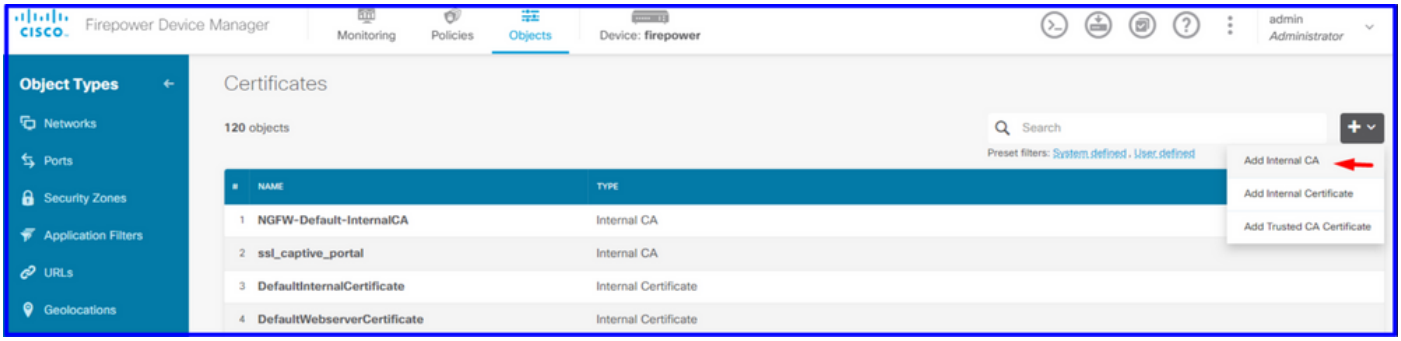


الخطوة 2. إنشاء شهادات موقعة ذاتيا

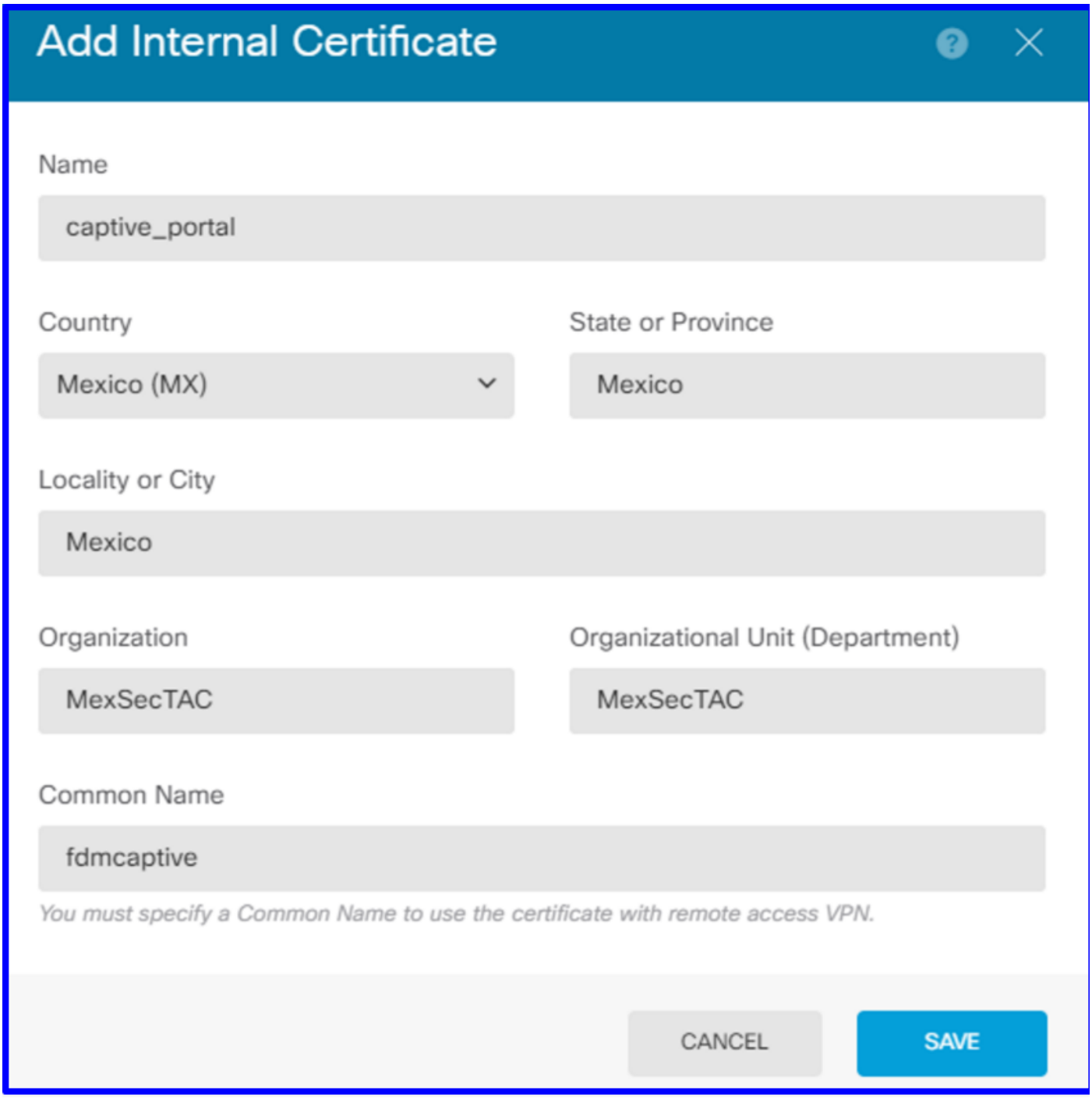
لإنشاء تكوين مدخل أسير، تحتاج إلى شهادتين، واحدة للمدخل الأسير والأخرى لفك تشفير SSL.

يمكنك إنشاء شهادة موقعة ذاتيا مثل هذا المثال.

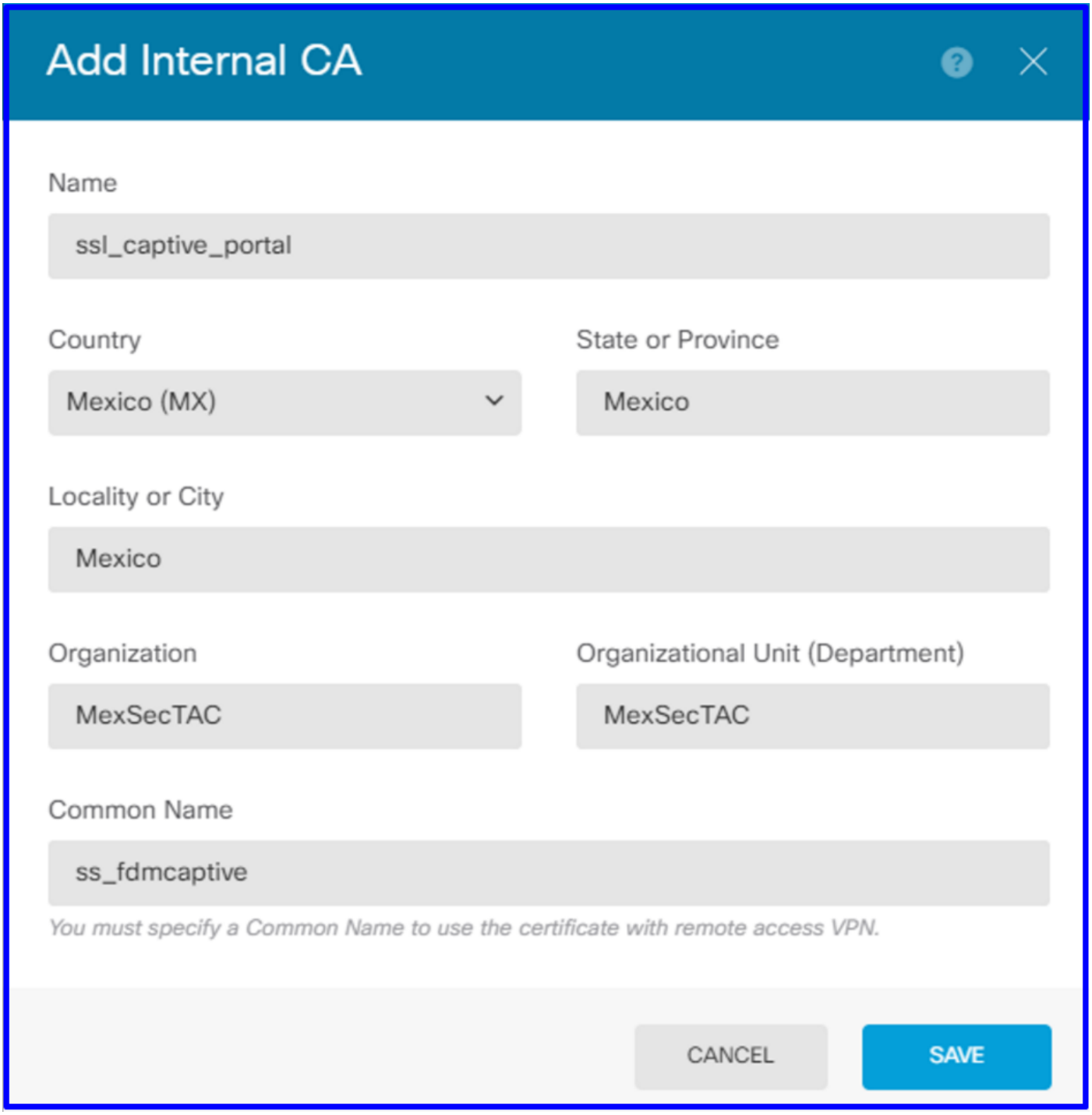
انتقل إلى **كائنات > شهادات**



شهادة الموقع الذاتي للمدخل المتنقل:



شهادة SSL ذاتية التوقيع:

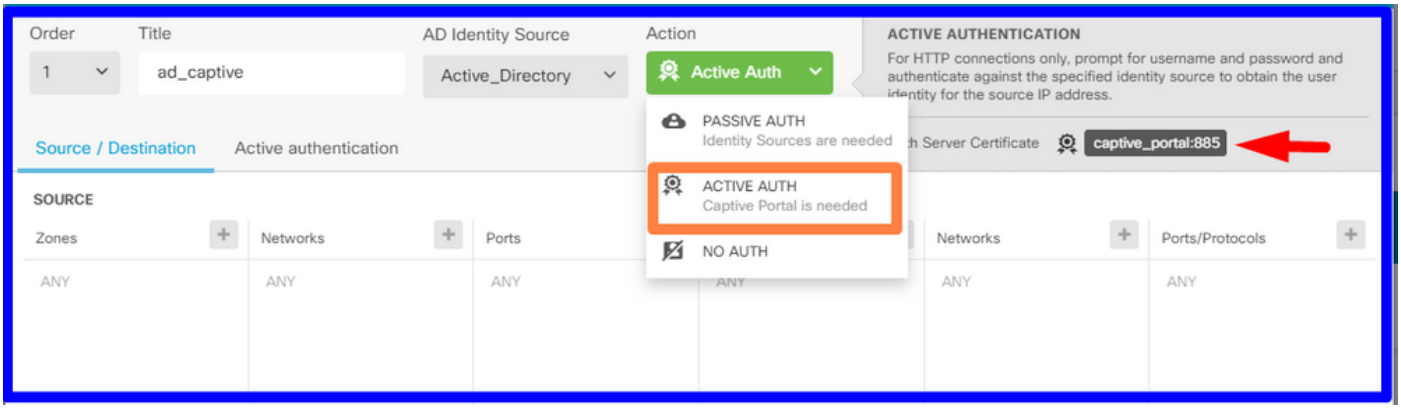


الخطوة 3. إنشاء قاعدة هوية

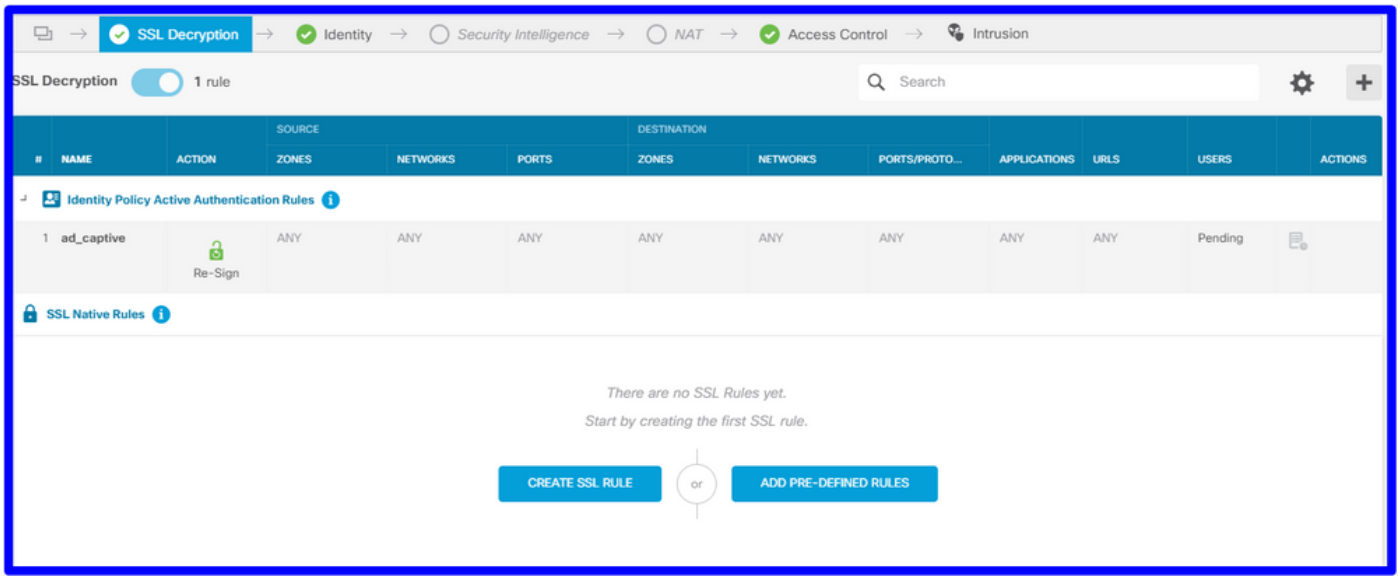
انتقل إلى **السياسات** > **الهوية** > حدد **[+]** زر لإضافة قاعدة هوية جديدة.

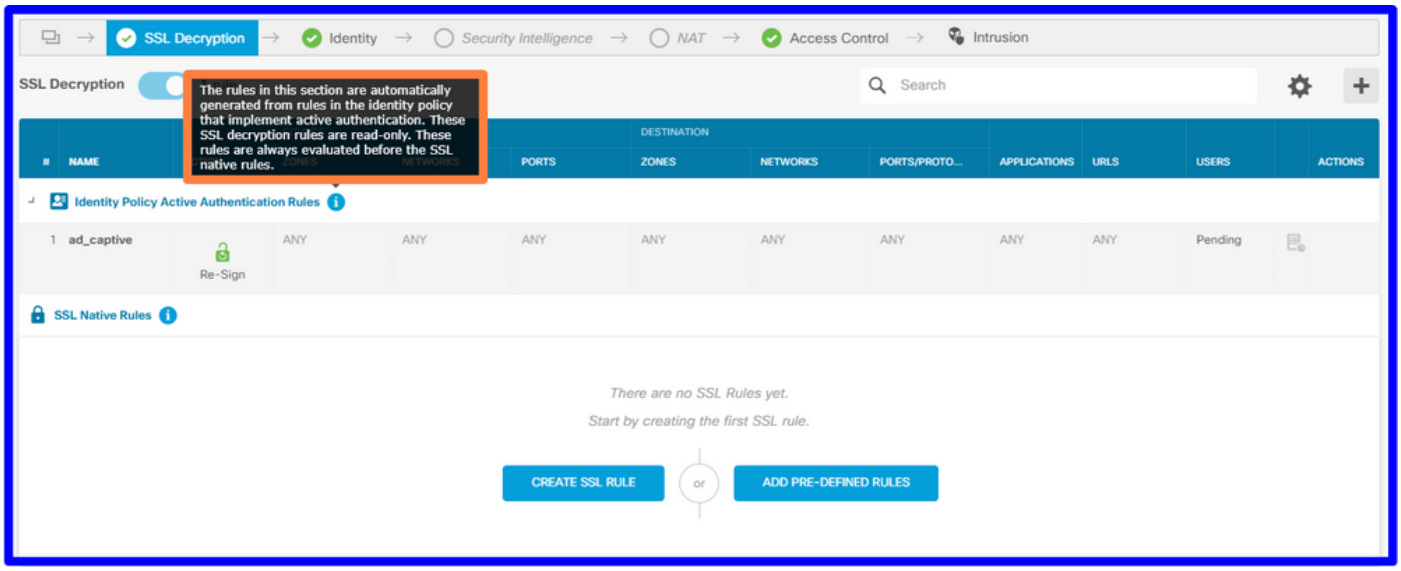
أنت تحتاج أن يخلق الهوية سياسة in order to شكلت صحة هوية نشطة، السياسة ينبغي أن يكون لها العناصر التالية:

- مصدر تعريف الإعلانات: نفس الشيء الذي تضيفه في الخطوة رقم 1
- الإجراء: المصادقة النشطة
- شهادة الخادم: نفس الشهادة الموقعة ذاتيا التي أنشأتها قبل [في هذا السيناريو captive_portal]
- النوع: HTTP Basic (في هذا المثال السيناريو)



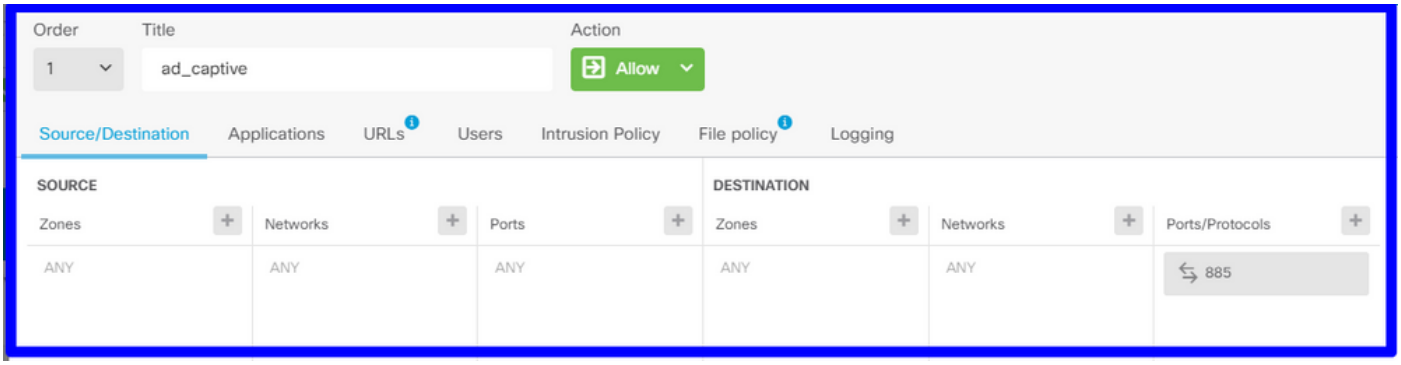
بمجرد إنشاء نهج الهوية كمصادقة نشطة، يتم إنشاء قاعدة SSL تلقائيا، ويتم إعداد هذه القاعدة بشكل افتراضي كأي قاعدة مع **إلغاء تشفير-Resign**، مما يعني عدم وجود تعديلات SSL في هذه القاعدة.



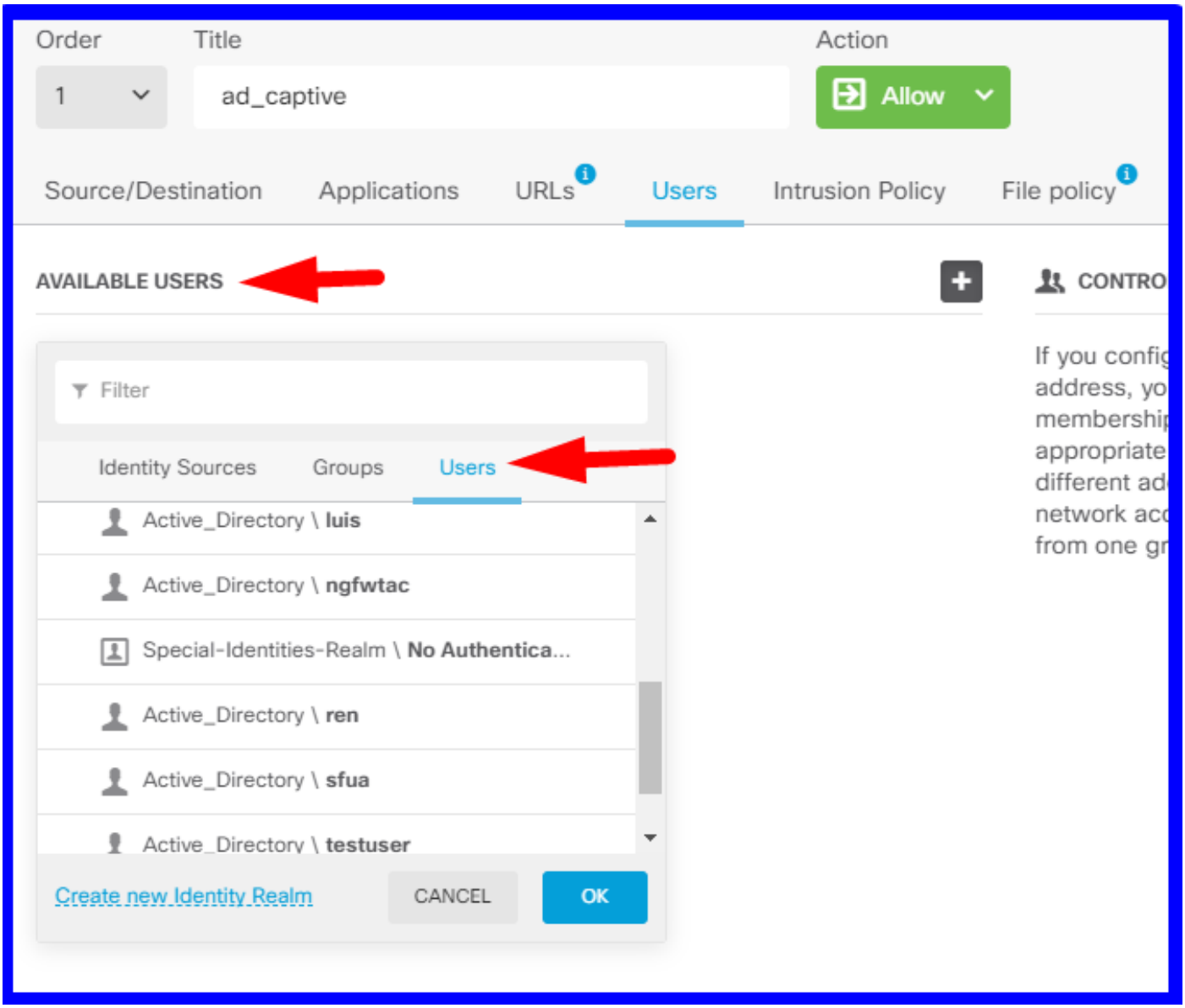


الخطوة 4. إنشاء قاعدة الوصول في نهج التحكم بالوصول

أنت تحتاج إلى السماح **للمنفذ 885/tcp** الذي يعيد توجيه حركة مرور البيانات إلى مصادقة البوابة المقيدة. انتقل إلى **السياسات > التحكم في الوصول** وأضف قاعدة الوصول.



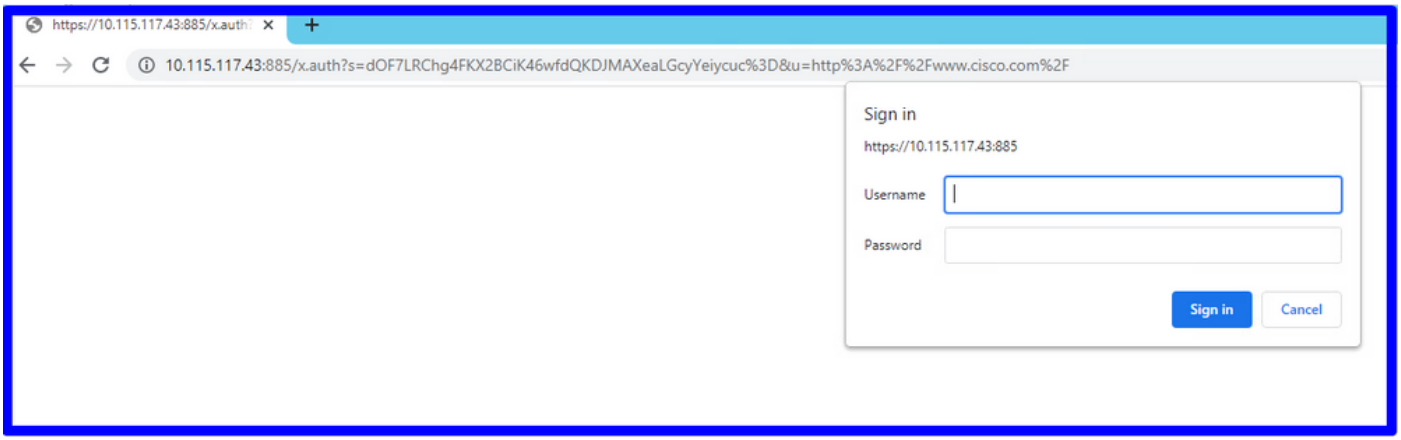
إذا كنت بحاجة إلى التحقق من تنزيل المستخدمين من AD، فيمكنك تحرير قاعدة الوصول والتنقل إلى قسم **المستخدمون**، ثم على **المستخدمين المتاحين**، فيمكنك التحقق من عدد المستخدمين الذين لديهم FDM بالفعل.



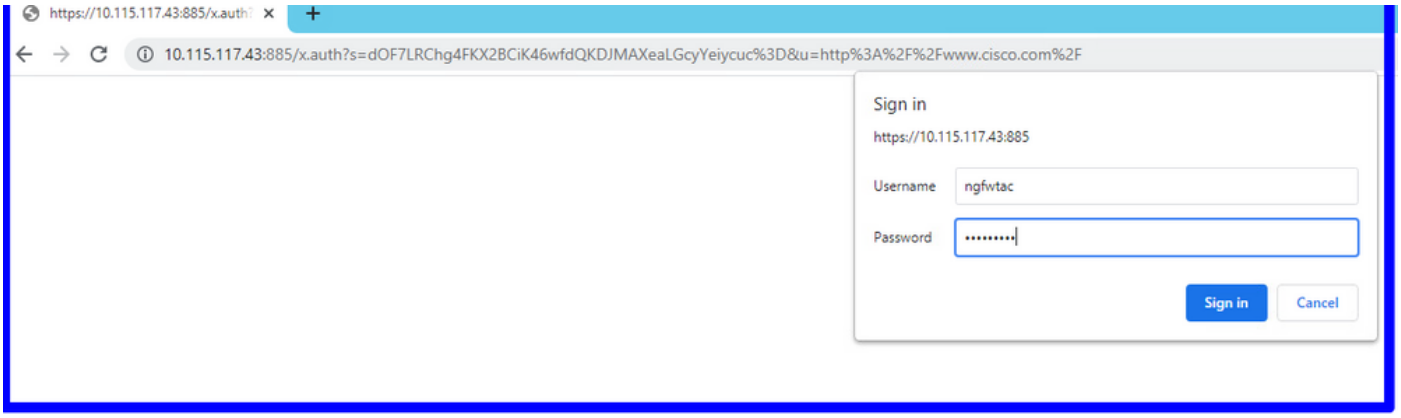
تذكر لنشر تغييرات التكوين.

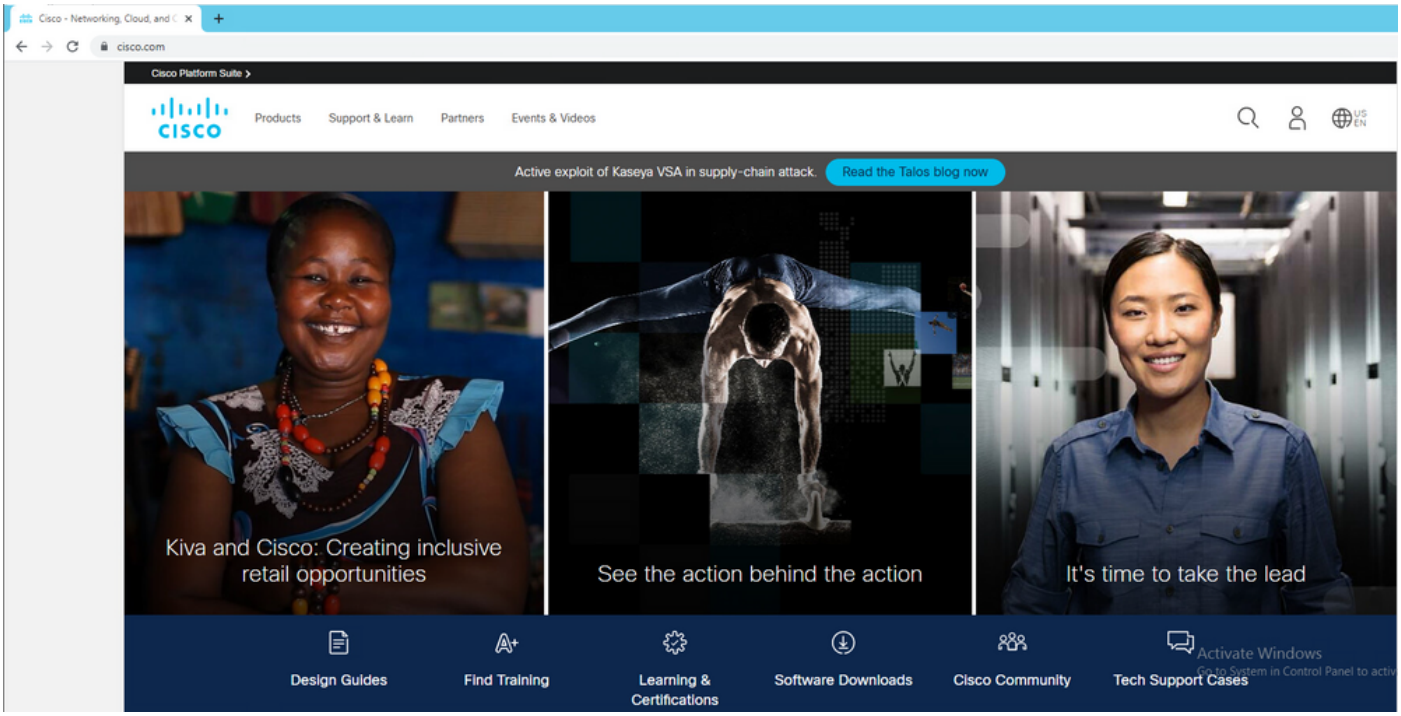
التحقق من الصحة

تحقق من تلقي جهاز المستخدم لمربع الاختيار عند الانتقال إلى موقع HTTPS.



أدخل مسوغات AD للمستخدم.





استكشاف الأخطاء وإصلاحها

يمكنك إستخدام البرنامج النصي **user_map_query.pl** للتحقق من أن FDM به تعيين IP للمستخدم

```
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)]

في وضع التحكم يمكنك تكوين:

يدعم النظام تصحيح أخطاء الهوية للتحقق من نجاح إعادة التوجيه.

> 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
```

المرجع:

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).