Configuración de la autenticación activa de FDM (portal cautivo)

Contenido

Introducción

Este documento describe un ejemplo de configuración para Firepower Device Manager (FDM) con integración de Active Authentication (Captive-Portal). Esta configuración utiliza Active Directory (AD) como el origen y los certificados autofirmados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Threat Defense (FTD)
- Active Directory (AD)
- Certificados autofirmados.
- Secure Socket Layer (SSL)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software:’

- Firepower Threat Defense 6.6.4
- Active Directory
- prueba de 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

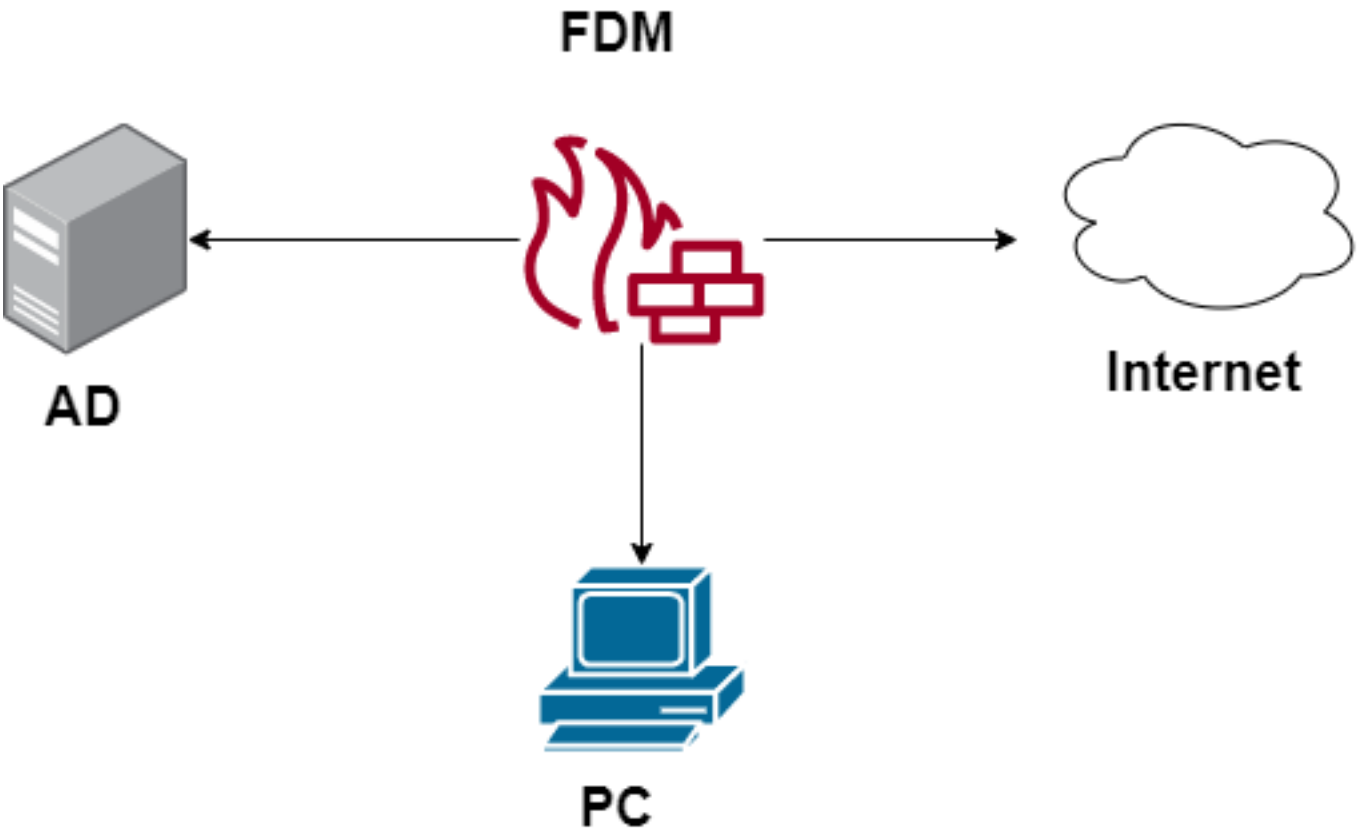
Antecedentes

Establecer identidad de usuario mediante autenticación activa

La autenticación es el acto de confirma la identidad de un usuario. Con la autenticación activa, cuando un flujo de tráfico HTTP proviene de una dirección IP para la que el sistema no tiene asignación de identidad de usuario, puede decidir si autenticar al usuario que inició el flujo de tráfico en el directorio configurado para el sistema. Si el usuario se autentica correctamente, se considera que la dirección IP tiene la identidad del usuario autenticado.

Si no se realiza la autenticación, no se impide el acceso a la red del usuario. En última instancia, las reglas de acceso deciden qué acceso se debe proporcionar a estos usuarios.

Diagrama de la red



Configurar

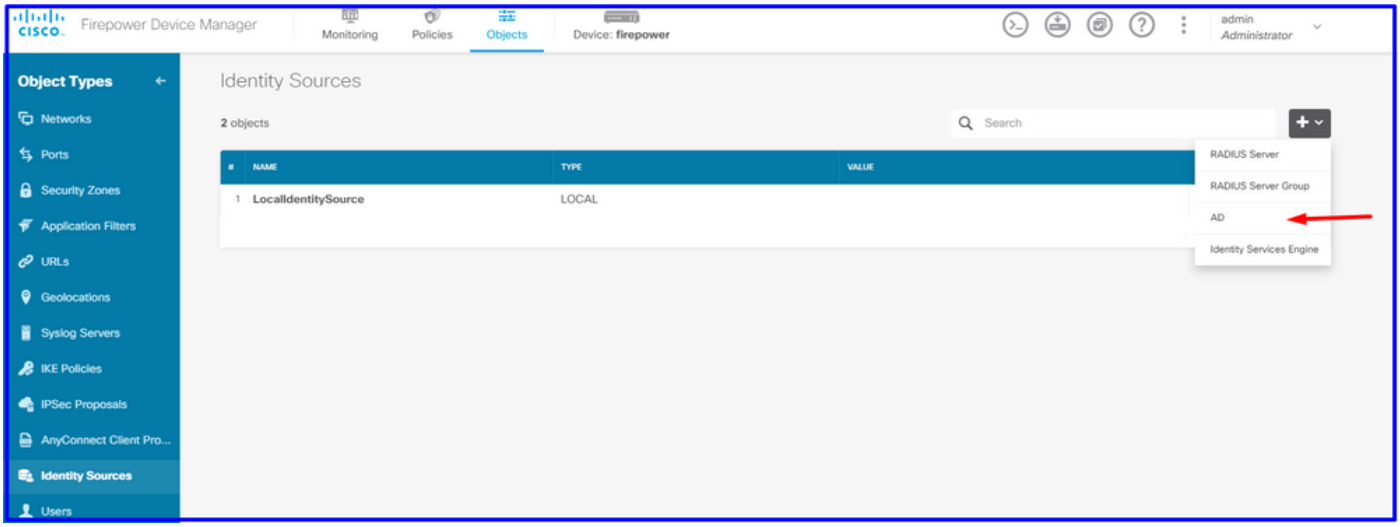
Implementar la política de identidad

Para habilitar la adquisición de identidad del usuario, de modo que se conozca al usuario asociado a una dirección IP, debe configurar varios elementos

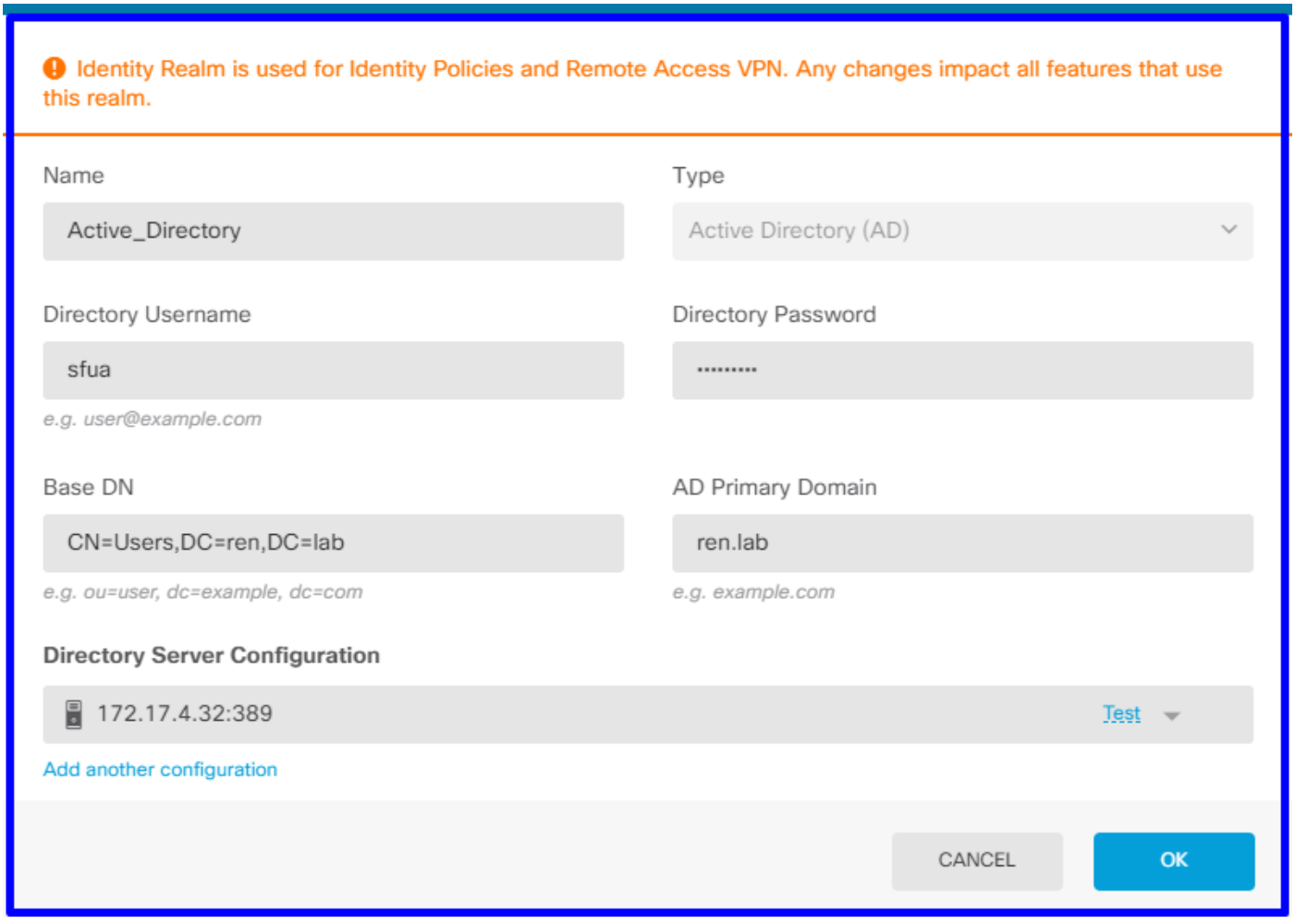
Paso 1. Configurar el rango de identidad AD

Tanto si recopila la identidad del usuario de forma activa (solicitando la autenticación del usuario) como pasiva, debe configurar el servidor de Active Directory (AD) que tiene la información de identidad del usuario.

Navegue hasta **Objetos > Servicios de identidad** y seleccione la opción **AD** para agregar Active Directory.



Agregue la configuración de Active Directory:

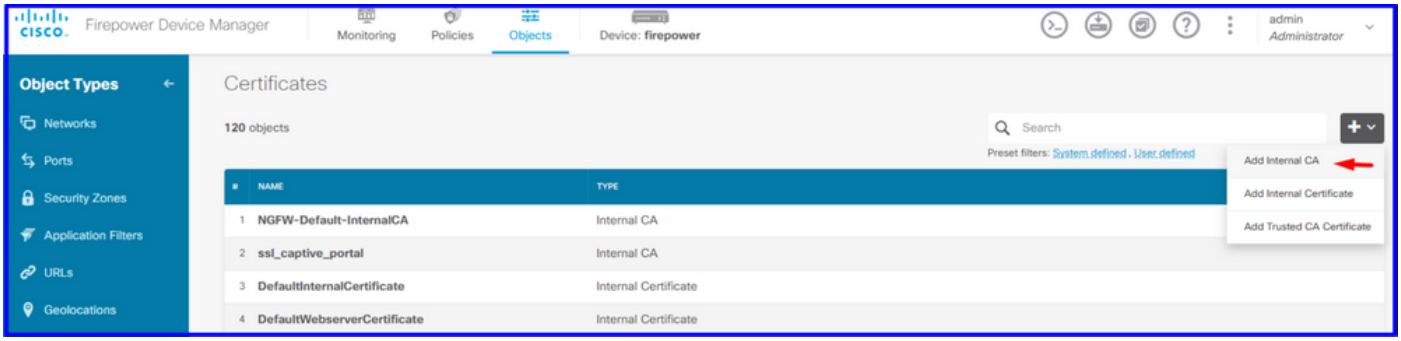


Paso 2. Crear certificados autofirmados

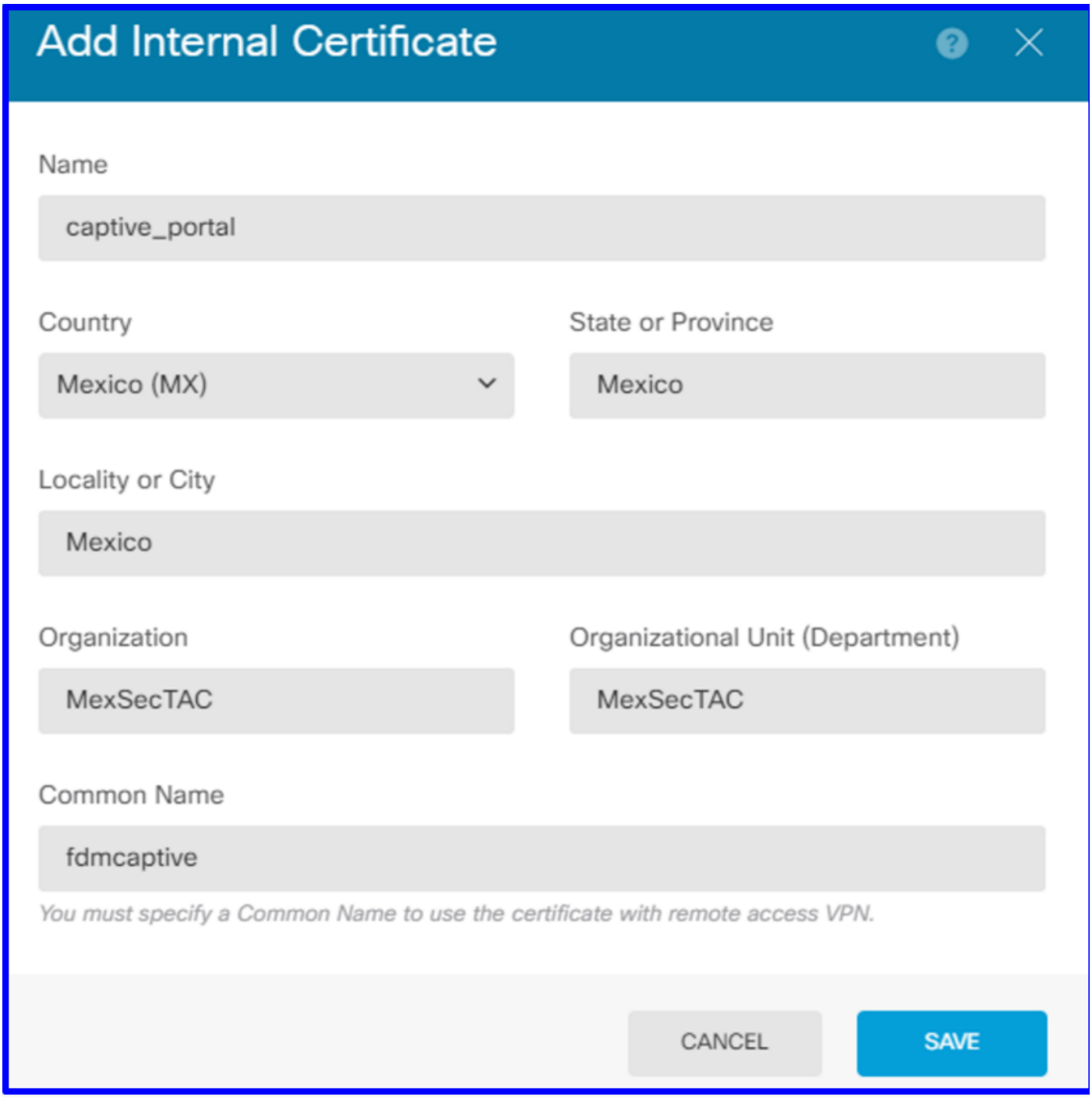
Para crear una configuración de Portal cautivo, necesita dos certificados uno para el portal cautivo y otro para el descifrado SSL.

Puede crear un certificado autofirmado como en este ejemplo.

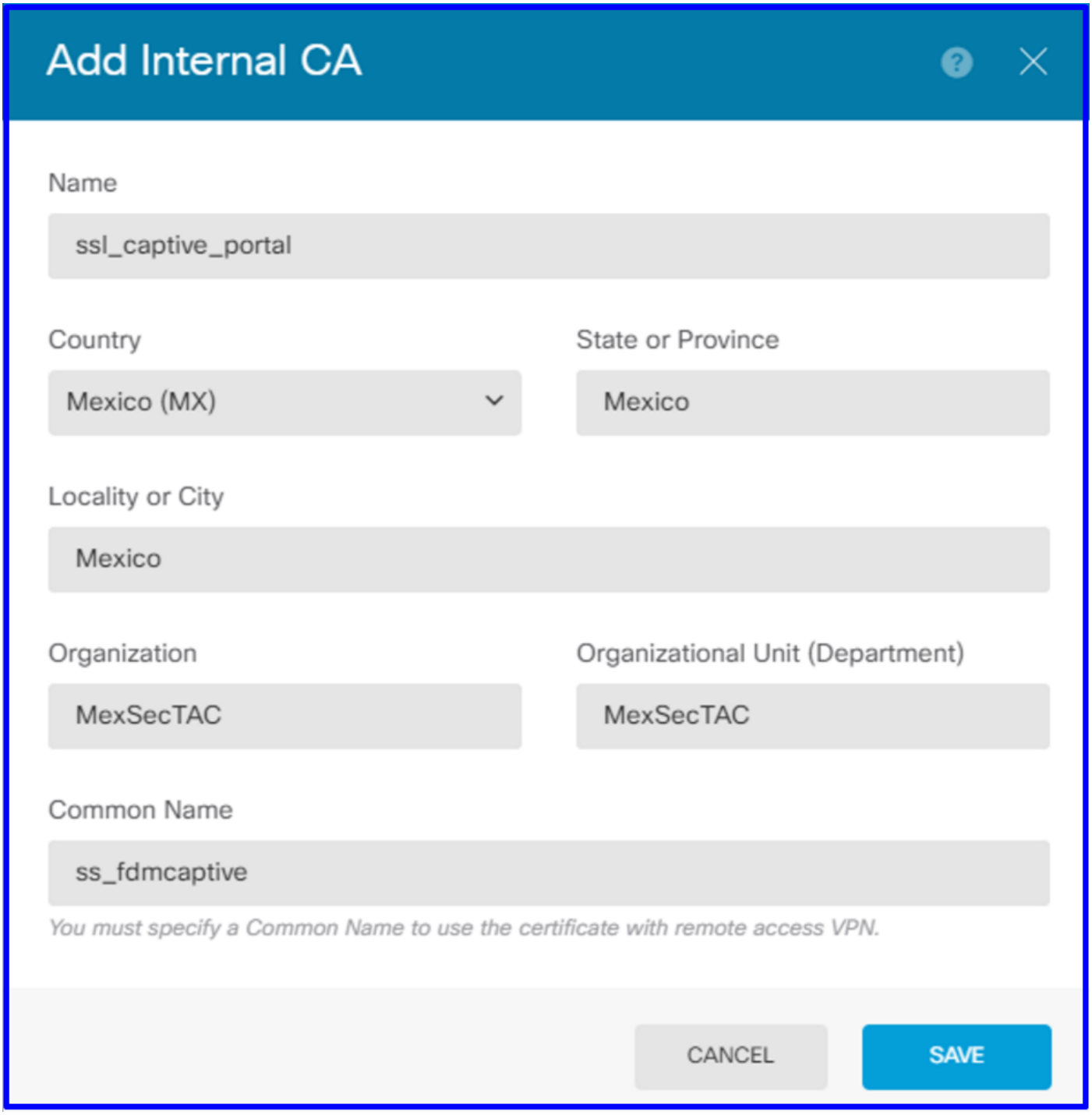
Vaya a **Objetos > Certificados**



Certificado de firma automática del portal cautivo:



Certificado con firma automática SSL:

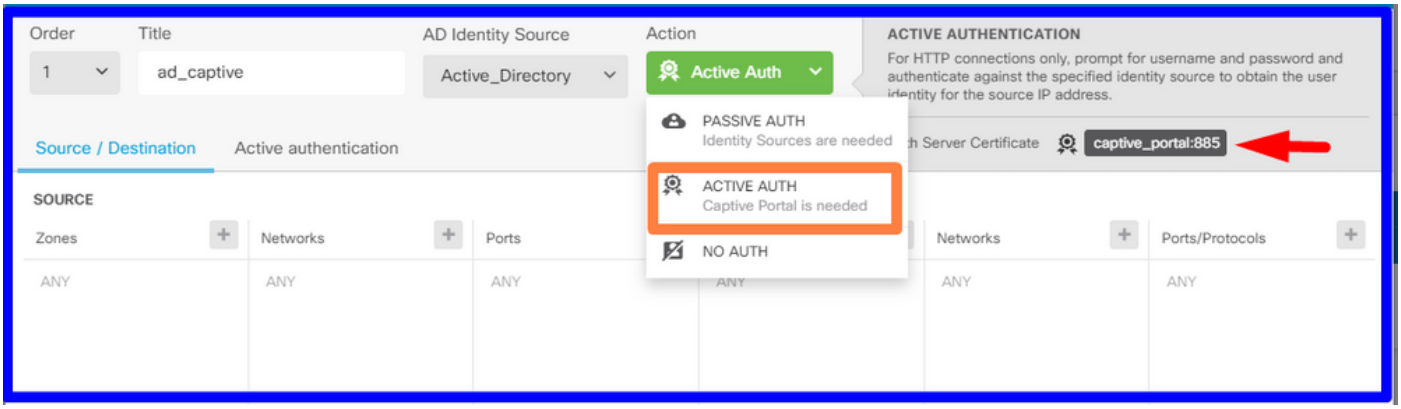


Paso 3. Crear regla de identidad

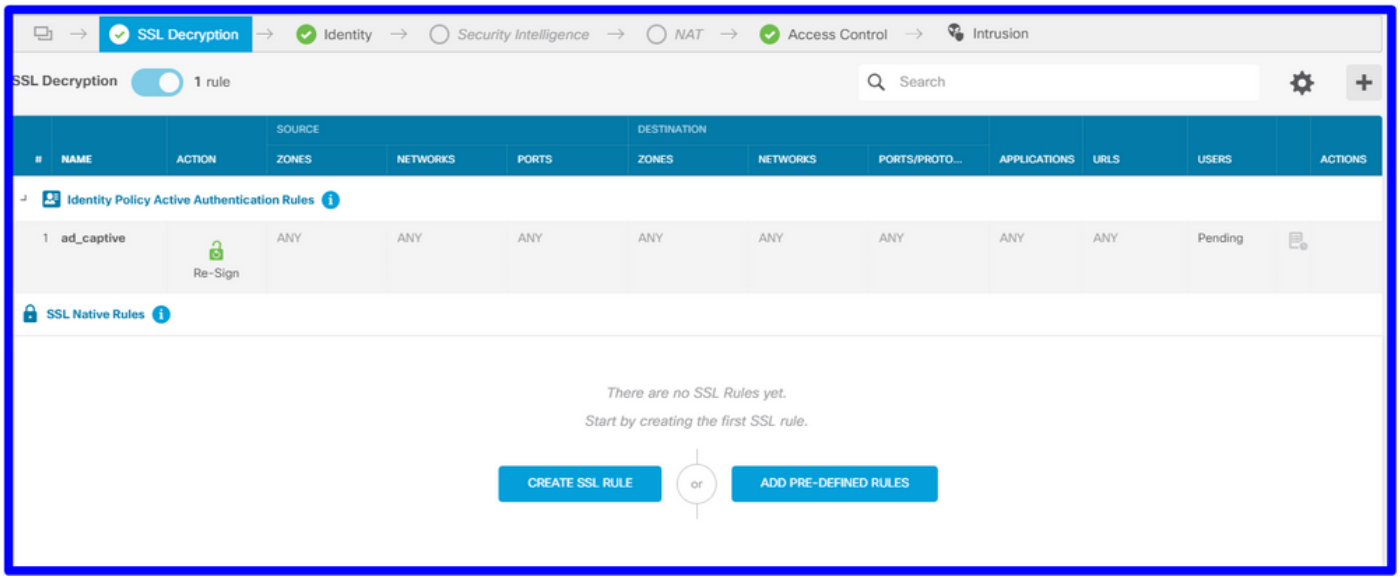
Navegue hasta **Políticas > Identidad >** seleccione el botón **[+]** para agregar una nueva regla de identidad.

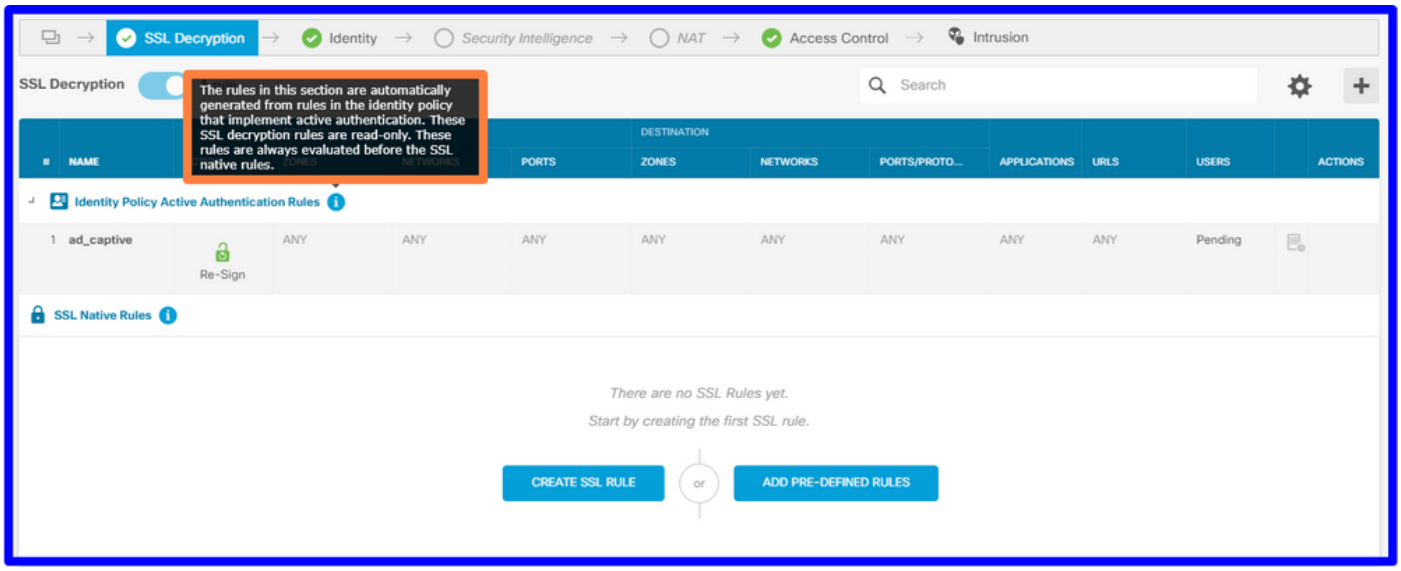
Debe crear la política de identidad para configurar la autenticación activa, la política debe tener los siguientes elementos:

- Origen de identidad de AD: Lo mismo que agrega en el paso número 1
- Acción: AUTH ACTIVE
- Certificado de servidor: El mismo certificado autofirmado que creó antes [En este escenario, captive_portal]
- Tipo: HTTP Basic (en este escenario de ejemplo)



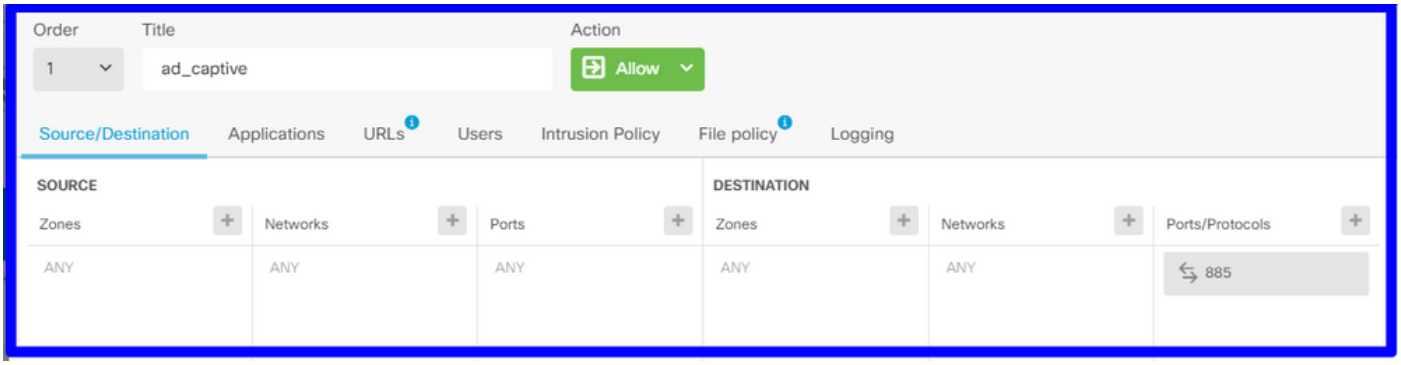
Una vez que se crea la política de identidad como autenticación activa, se crea automáticamente una regla SSL, de forma predeterminada esta regla se configura como cualquiera con **Decrypt-Resign**, lo que significa que no hay modificaciones SSL en esta regla.



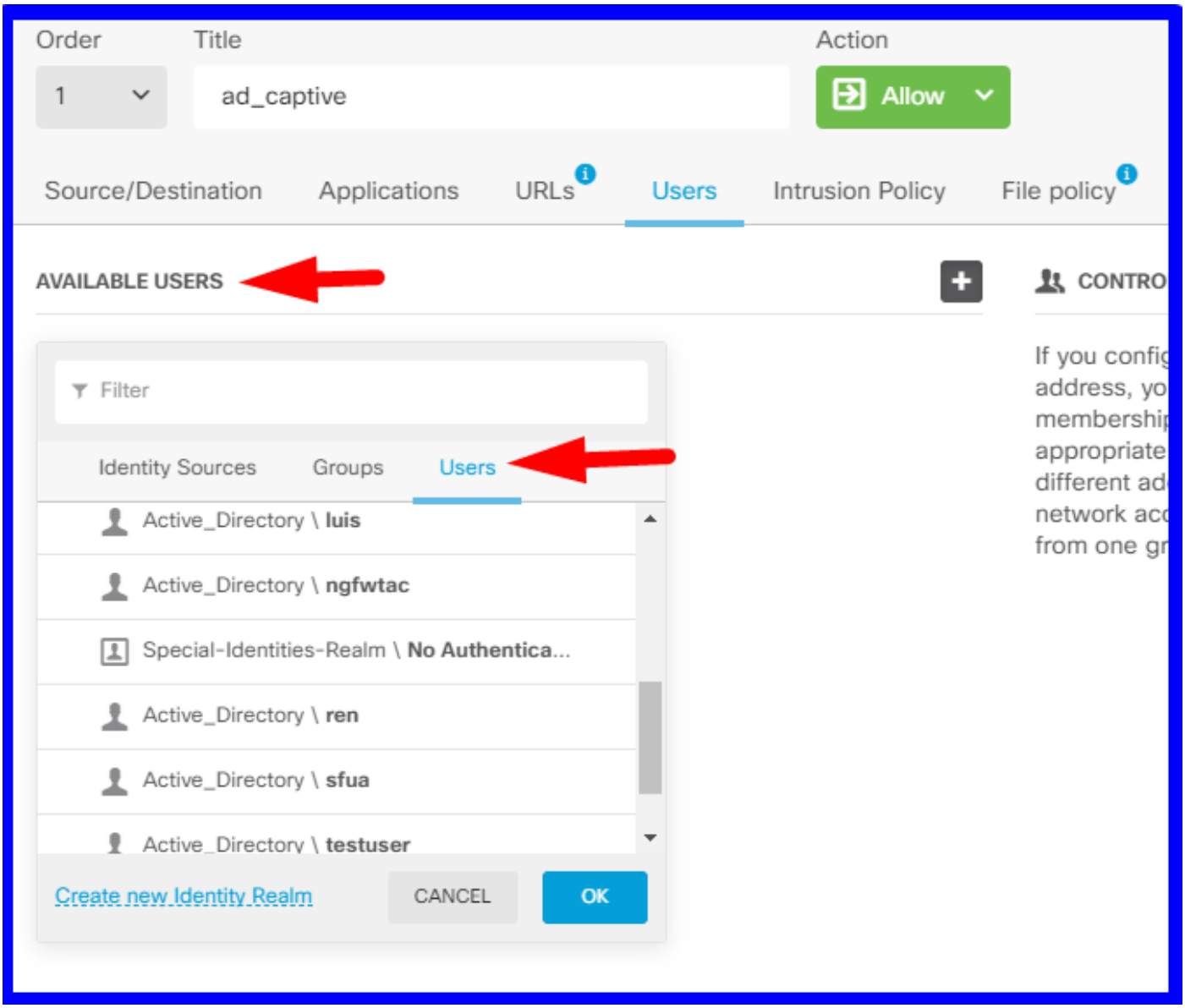


Paso 4. Crear regla de acceso en la política de control de acceso

Debe permitir el **puerto 885/tcp** que redirige el tráfico a la autenticación del portal cautivo. Navegue hasta **Políticas > Control de acceso** y agregue la regla de acceso.



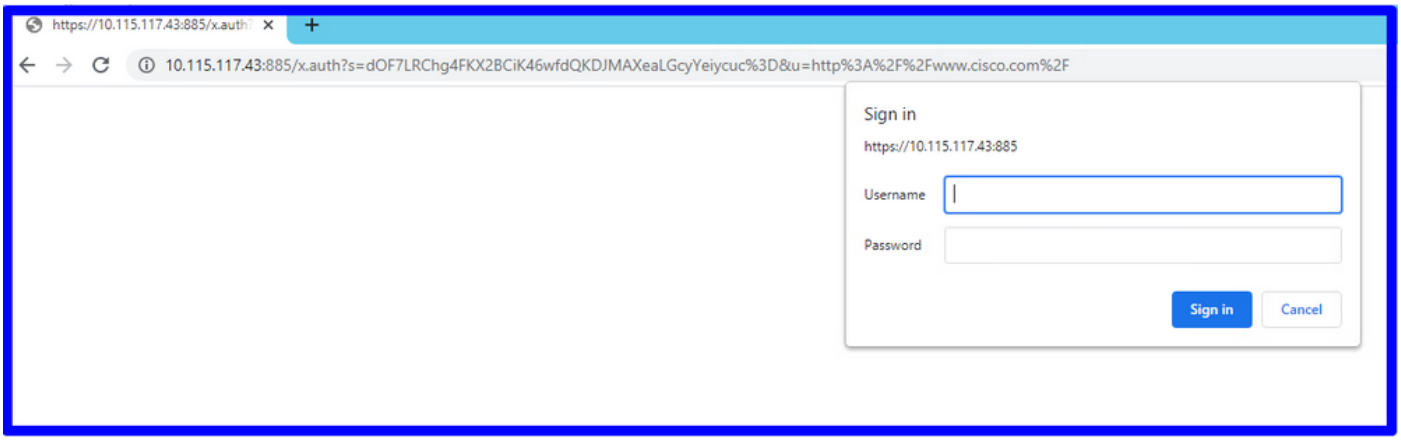
Si necesita verificar si los usuarios se descargaron de AD, puede editar la regla de acceso y navegar a la sección **Usuarios**, luego en **USUARIOS DISPONIBLES**, puede verificar cuántos usuarios tiene el FDM.



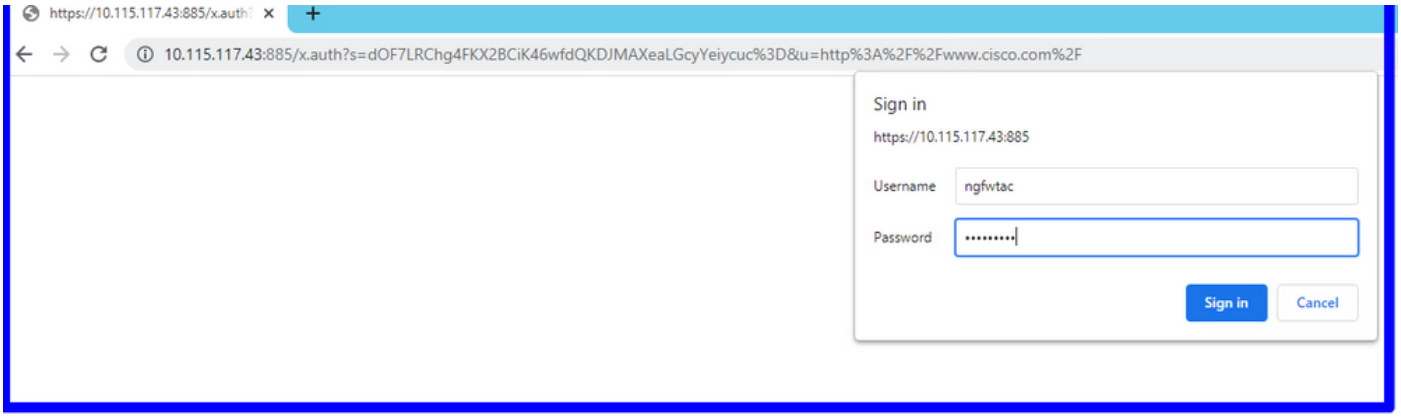
Recuerde implementar los cambios de configuración.

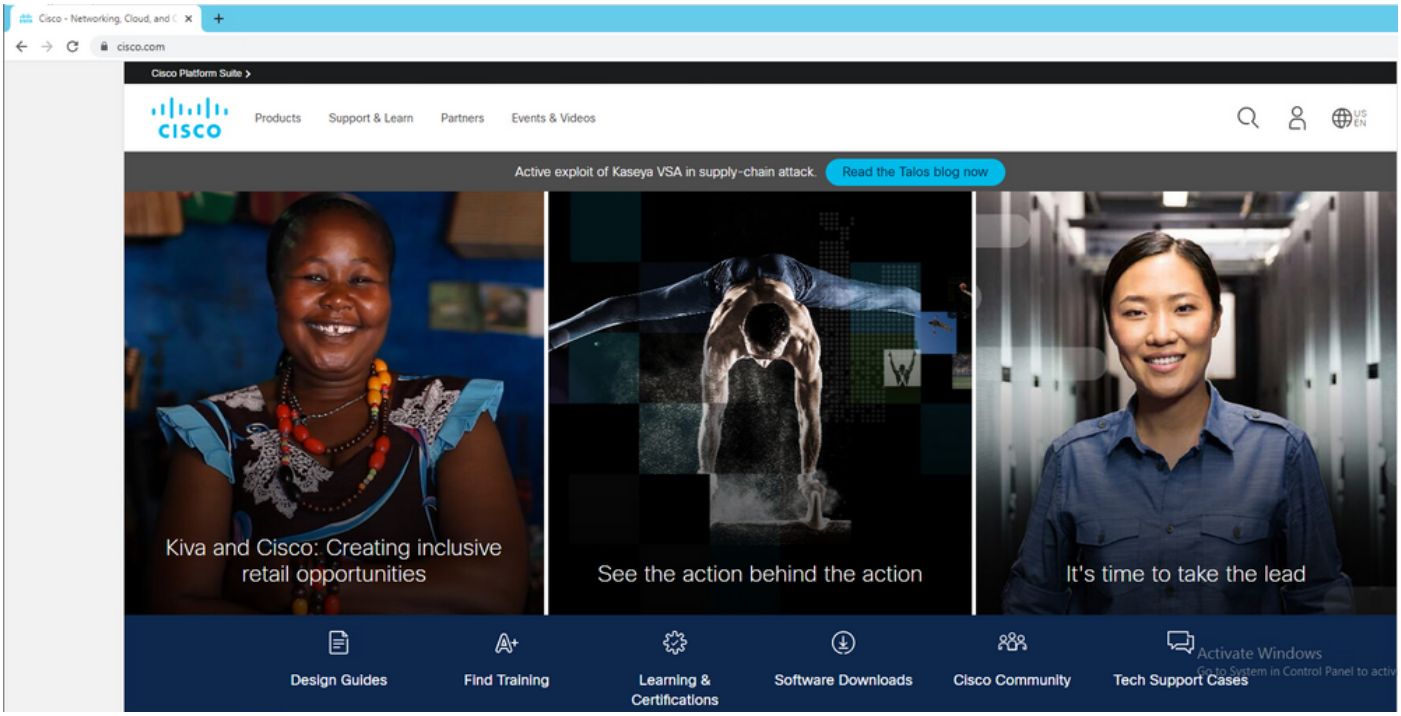
Verificación

Verifique que el dispositivo del usuario recibe la casilla de verificación cuando se desplaza a un sitio HTTPS.



Introduzca las credenciales de AD del usuario.





Troubleshoot

Puede utilizar la secuencia de comandos **user_map_query.pl** para validar FDM tiene la asignación ip de usuario

```
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 el modo clish puede configurar:

system support identity-debug para verificar si la redirección es exitosa.

```
> 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
```

Referencia:

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