Configurar a autenticação ativa do FDM (Portal cativo)

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Diagrama de Rede](#)
[Configurar](#)
[Verificar](#)
[Troubleshoot](#)

Introduction

Este documento descreve um exemplo de configuração para o Firepower Device Manager (FDM) com integração Ative Authentication (Captive-Portal). Esta configuração usa o Ative Diretory (AD) como a origem e os certificados autoassinados.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

As informações neste documento são baseadas na seguinte versão de software:

- Firepower Threat Defense 6.6.4
- Ative Diretory
- teste 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

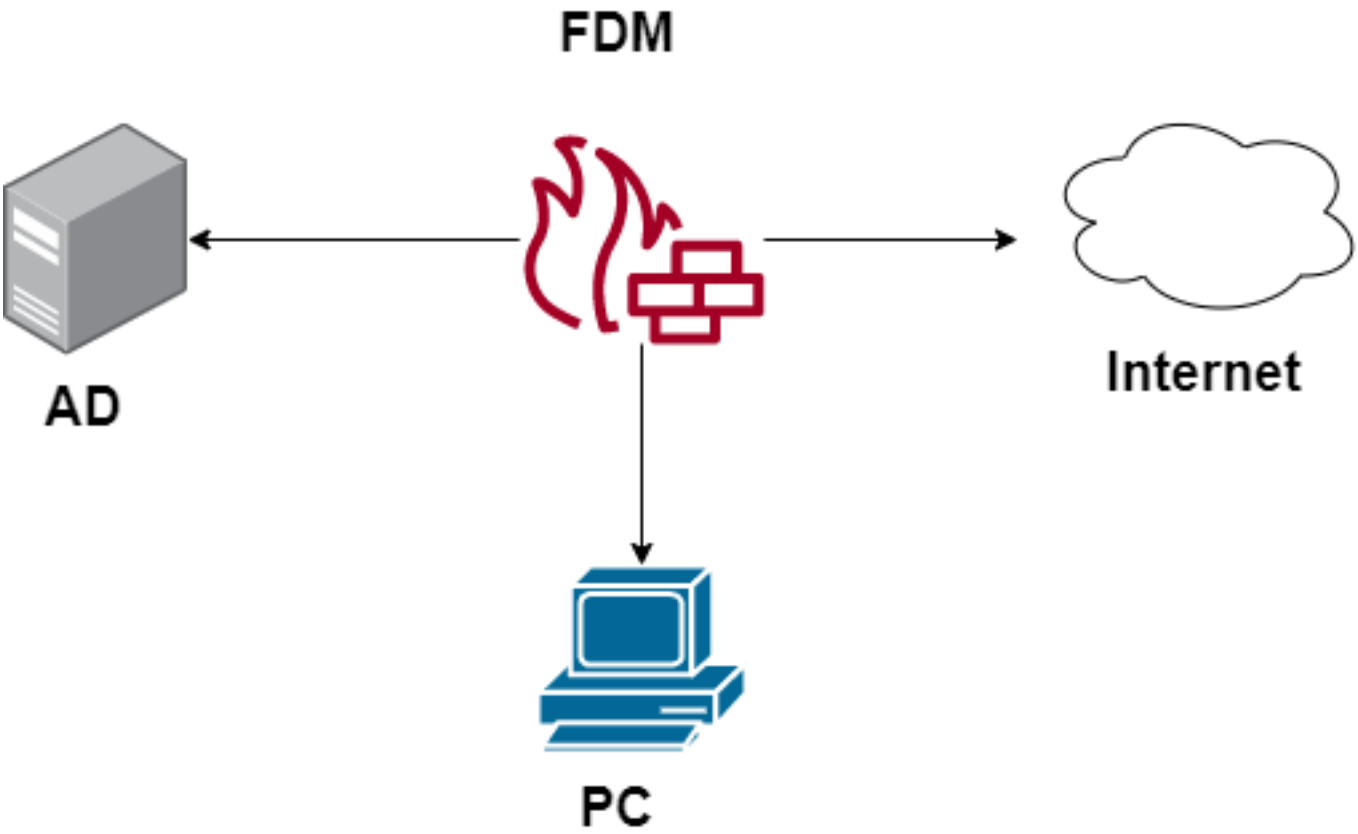
Informações de Apoio

Estabelecer a identidade do usuário por meio da autenticação ativa

A autenticação é o ato de confirmar a identidade de um usuário. Com a autenticação ativa, quando um fluxo de tráfego HTTP vem de um endereço IP para o qual o sistema não tem mapeamento de identidade de usuário, você pode decidir se deve autenticar o usuário que iniciou o fluxo de tráfego em relação ao diretório configurado para o sistema. Se o usuário autenticar com êxito, considera-se que o endereço IP tem a identidade do usuário autenticado.

A falha na autenticação não impede o acesso à rede para o usuário. Suas regras de acesso decidem, em última análise, qual acesso fornecer a esses usuários.

Diagrama de Rede



Configurar

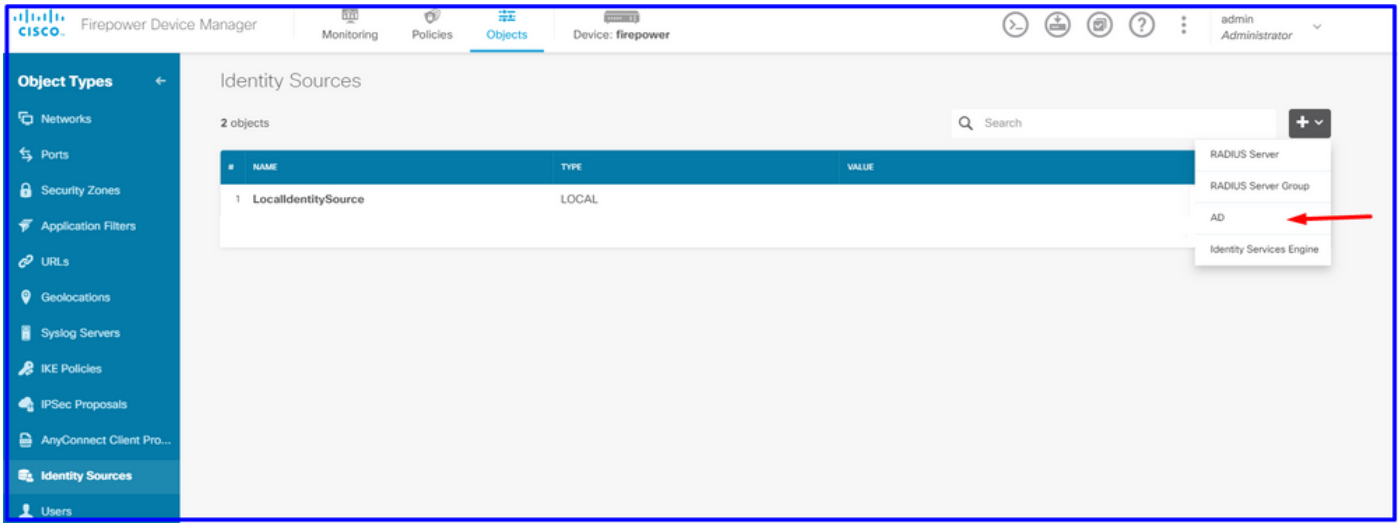
Implementar a política de identidade

Para ativar a aquisição de identidade do usuário, de modo que o usuário associado a um endereço IP seja conhecido, você precisa configurar vários itens

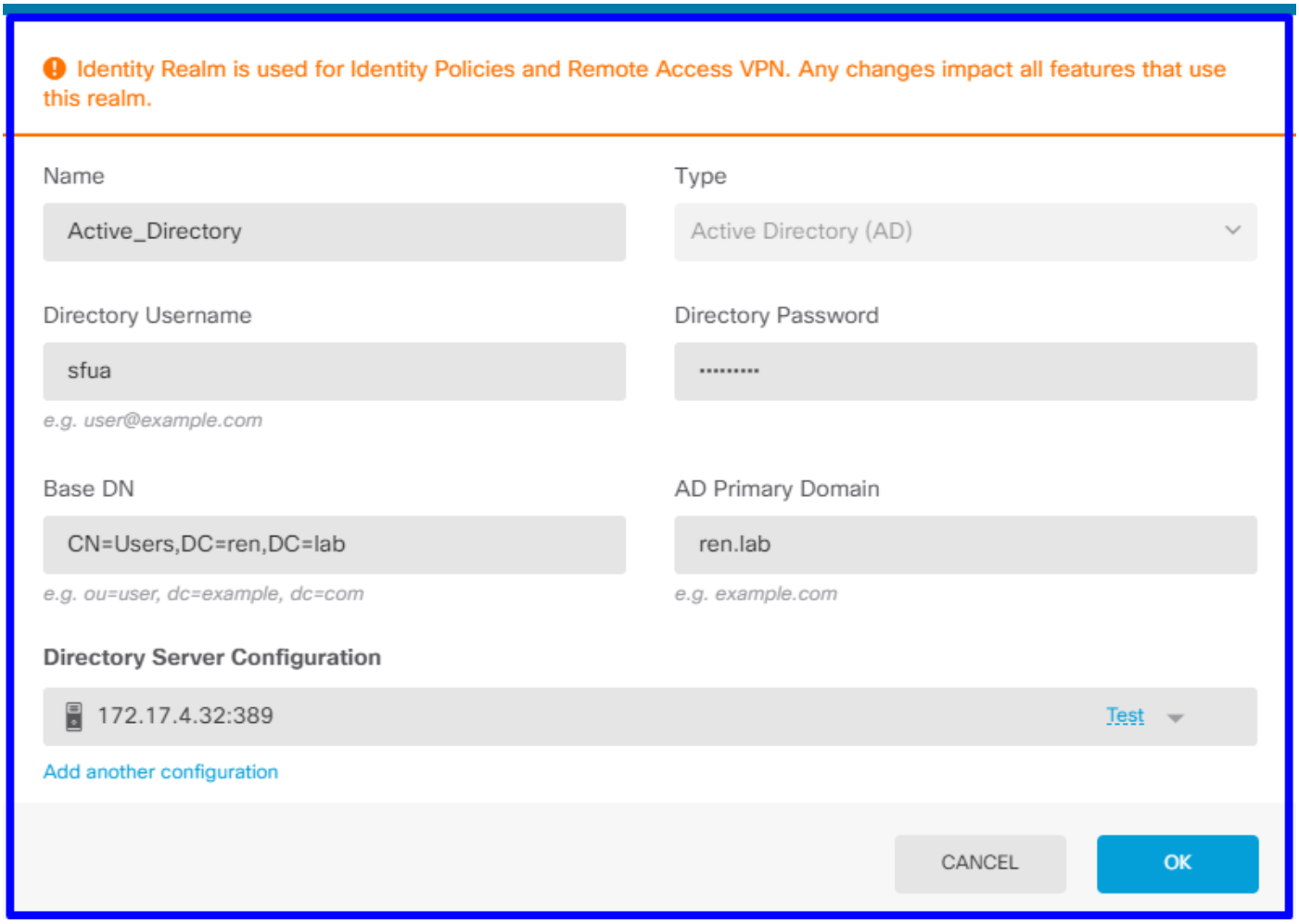
Etapa 1. Configurar o território de identidade do AD

Quer você colete a identidade do usuário ativamente (por prompt para autenticação do usuário) ou passivamente, você precisa configurar o servidor do Ative Diretory (AD) que tem as informações de identidade do usuário.

Navegue até **Objetos > Serviços de identidade** e selecione a opção **AD** para adicionar o Ative Diretory.



Adicione a configuração do Ative Diretory:

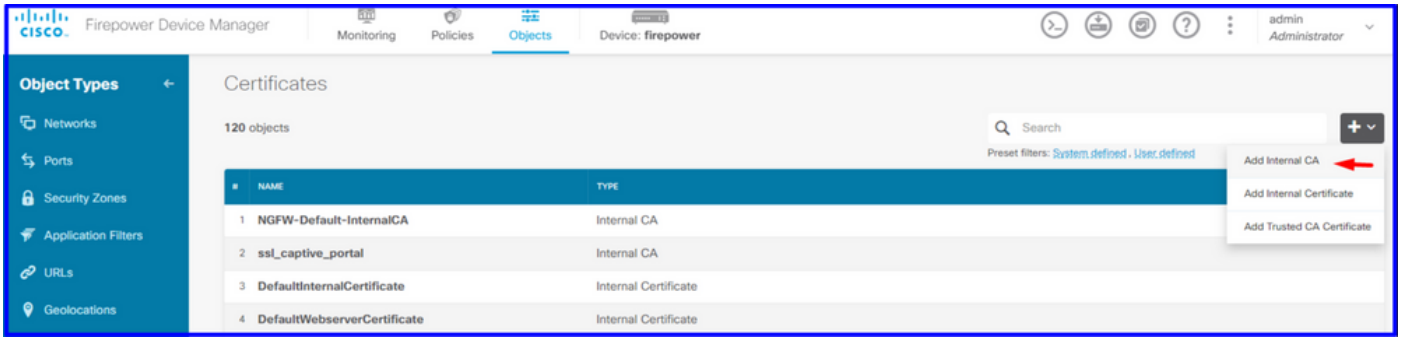


Etapa 2. Criar certificados autoassinados

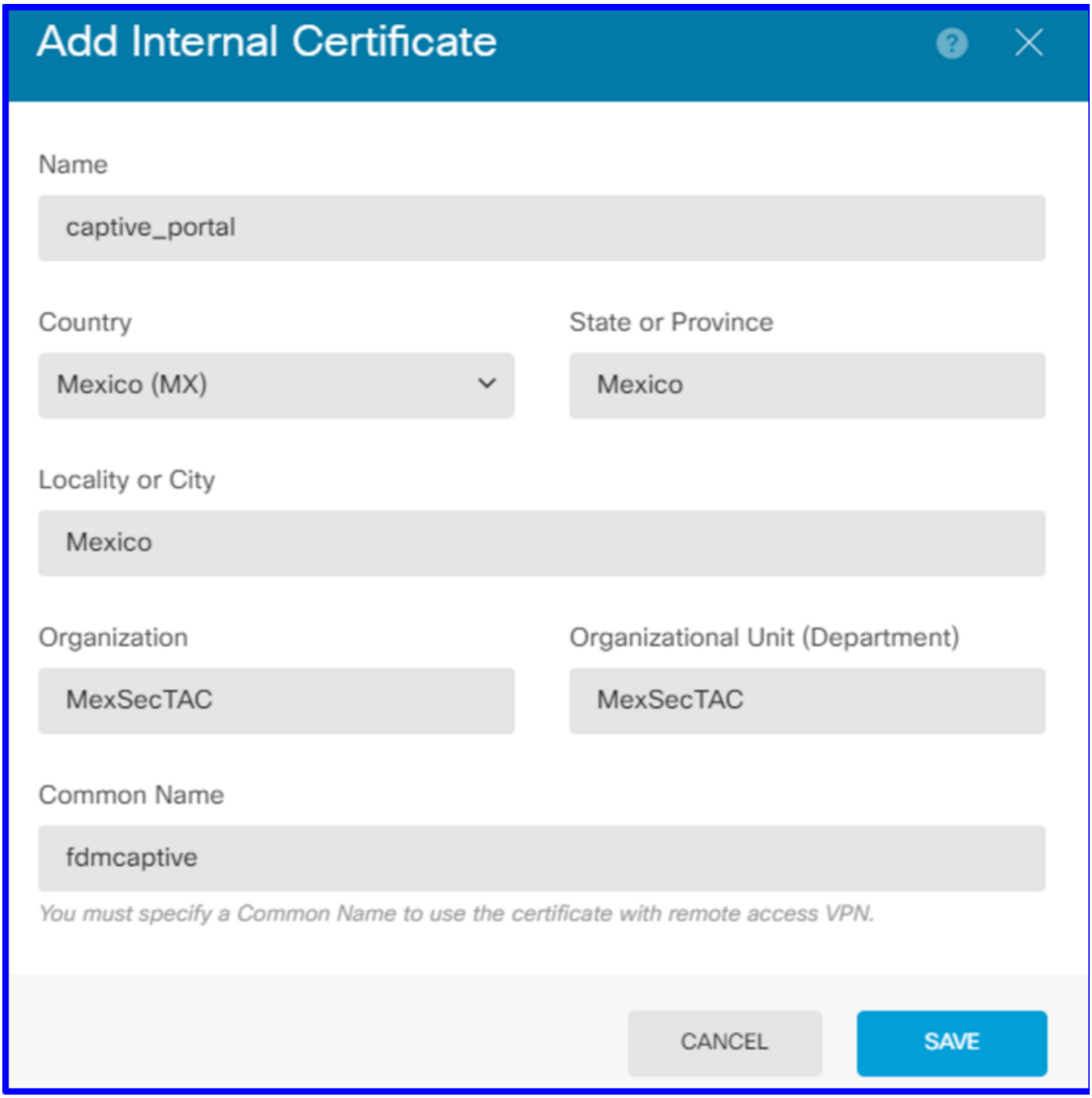
Para criar uma configuração do Portal cativo, você precisa de dois certificados, um para o portal cativo e um para a descriptografia de SSL.

Você pode criar um certificado autoassinado como neste exemplo.

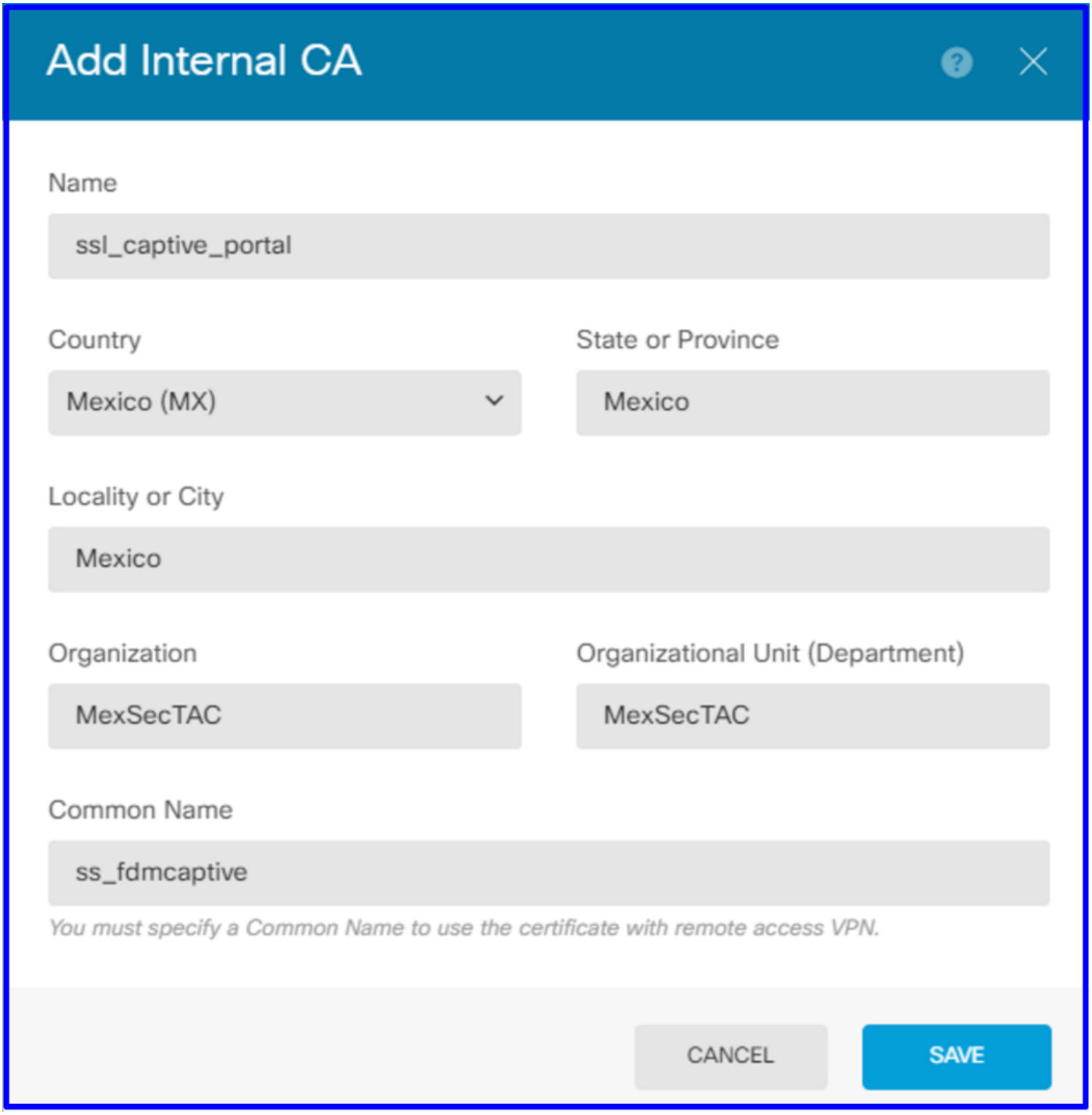
Navegue até **Objetos > Certificados**



Certificado autoassinado do portal cativo:



Certificado com assinatura automática SSL:

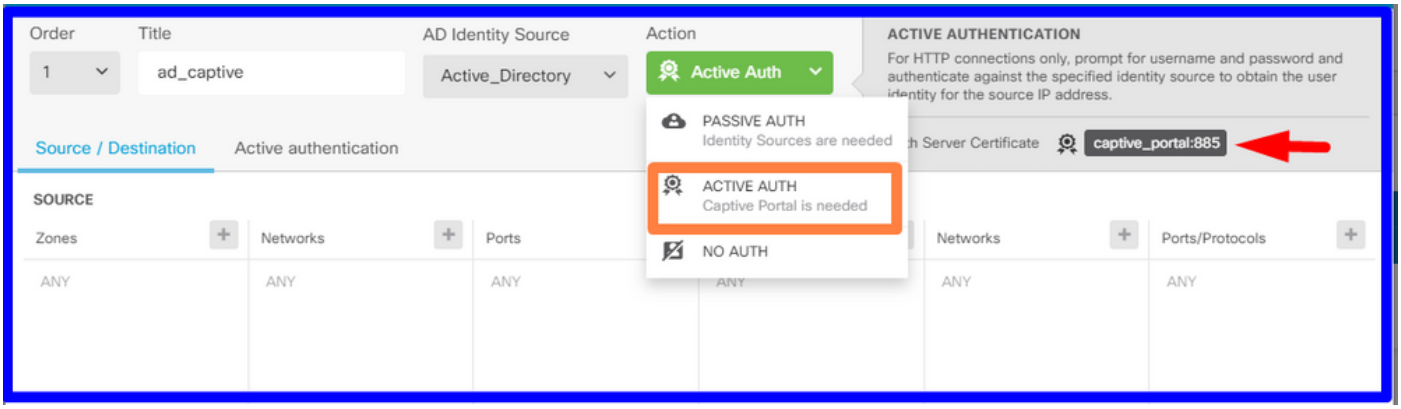


Etapa 3. Criar regra de identidade

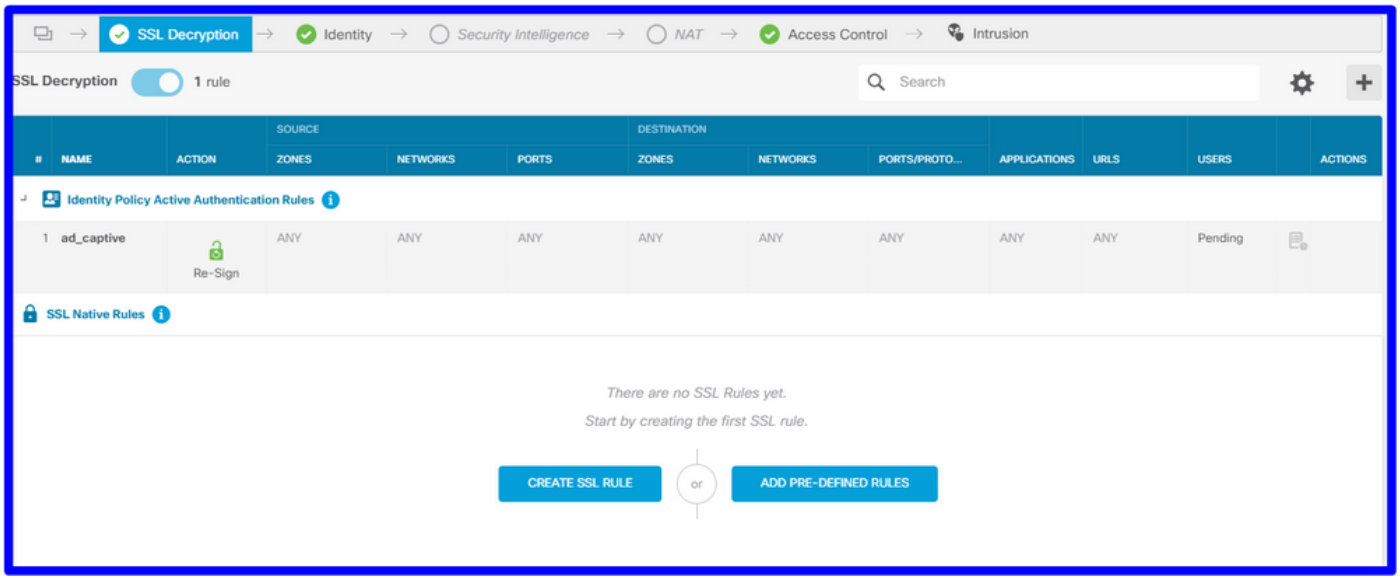
Navegue para **Políticas > Identidade >** selecione **[+]** o botão para adicionar uma nova regra de Identidade.

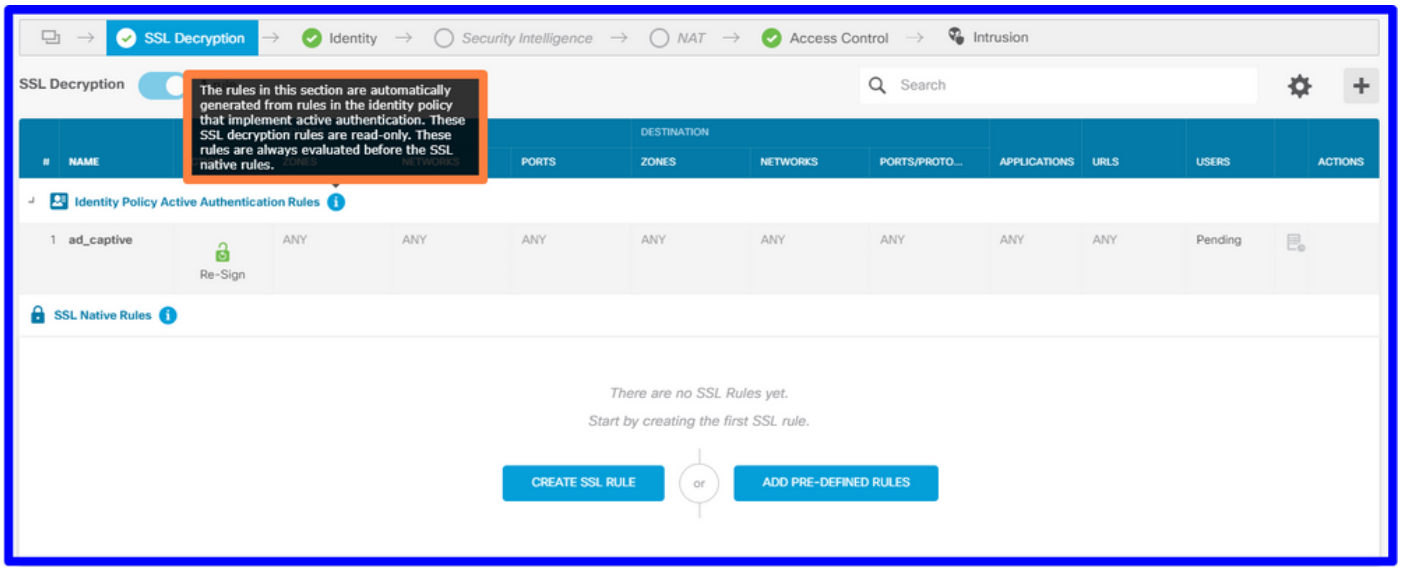
Você precisa criar a política de identidade para configurar a autenticação ativa, a política deve ter os seguintes elementos:

- Fonte de identidade do AD: O mesmo que você adiciona na etapa número 1
- Ação: AUTH ATIVO
- Server Certificate: O mesmo certificado autoassinado que você criou antes de [Neste cenário, portal cativo]
- Digite: HTTP Basic (neste cenário de exemplo)



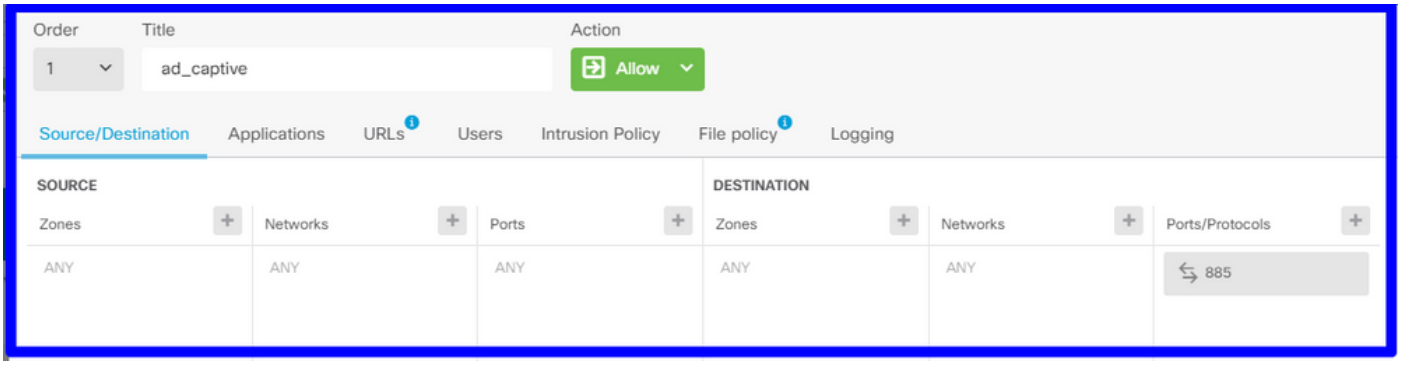
Uma vez que a política de Identidade é criada como autenticação ativa, cria automaticamente uma regra SSL, por padrão, esta regra é configurada como qualquer uma com **Decrypt-Resign**, o que significa que não há modificações SSL nesta regra.



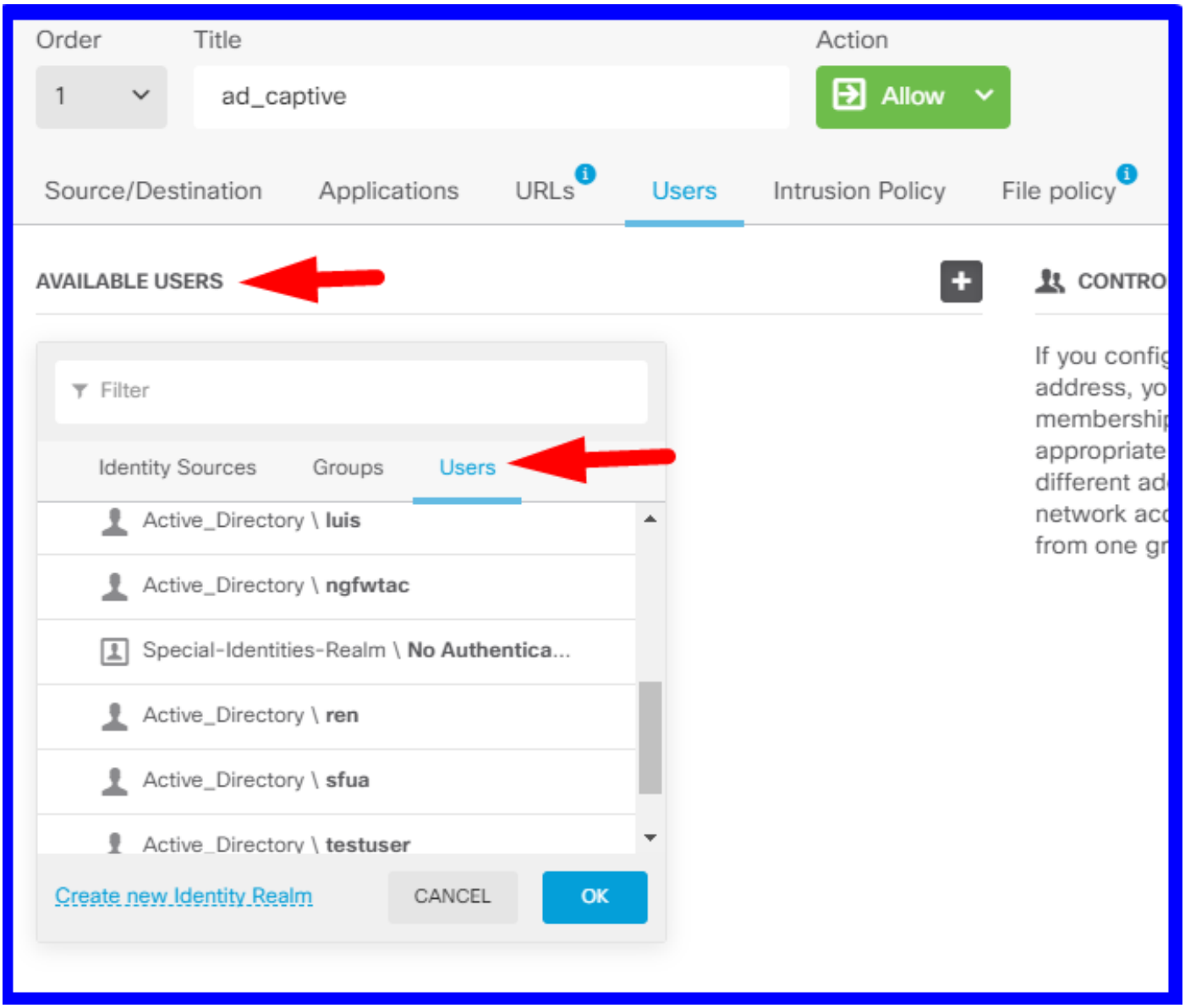


Etapa 4. Criar regra de acesso à política de controle de acesso

Você precisa permitir a **porta 885/tcp** que redireciona o tráfego para a autenticação do portal cativo. Navegue para **Políticas > Controle de acesso** e adicione a regra de acesso.



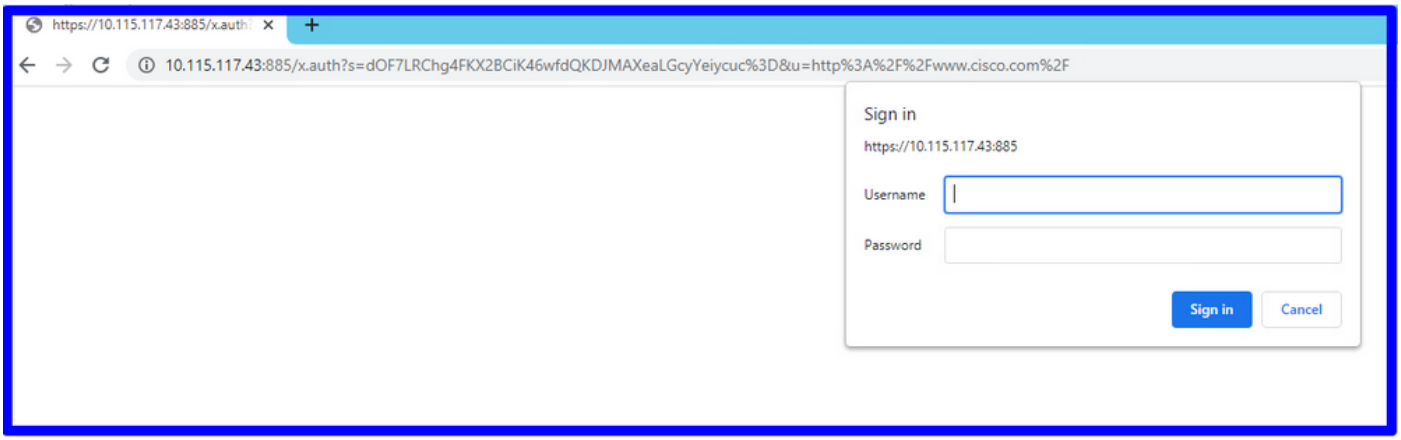
Se precisar verificar se os usuários foram baixados do AD, você pode editar a regra de acesso e navegar até a seção **Usuários** e, em **USUÁRIOS DISPONÍVEIS**, você pode verificar quantos usuários o FDM já possui.



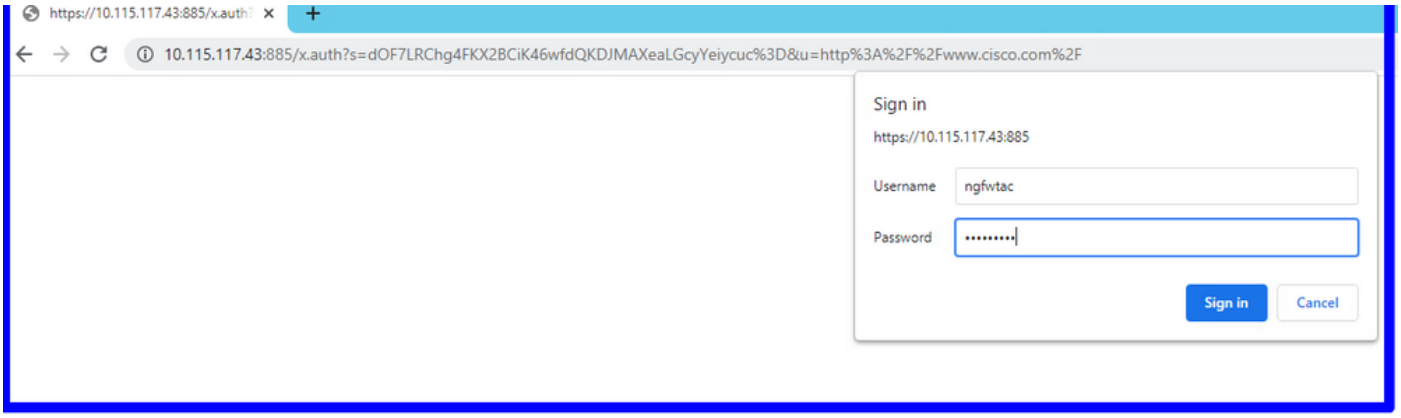
Lembre-se de implantar as alterações de configuração.

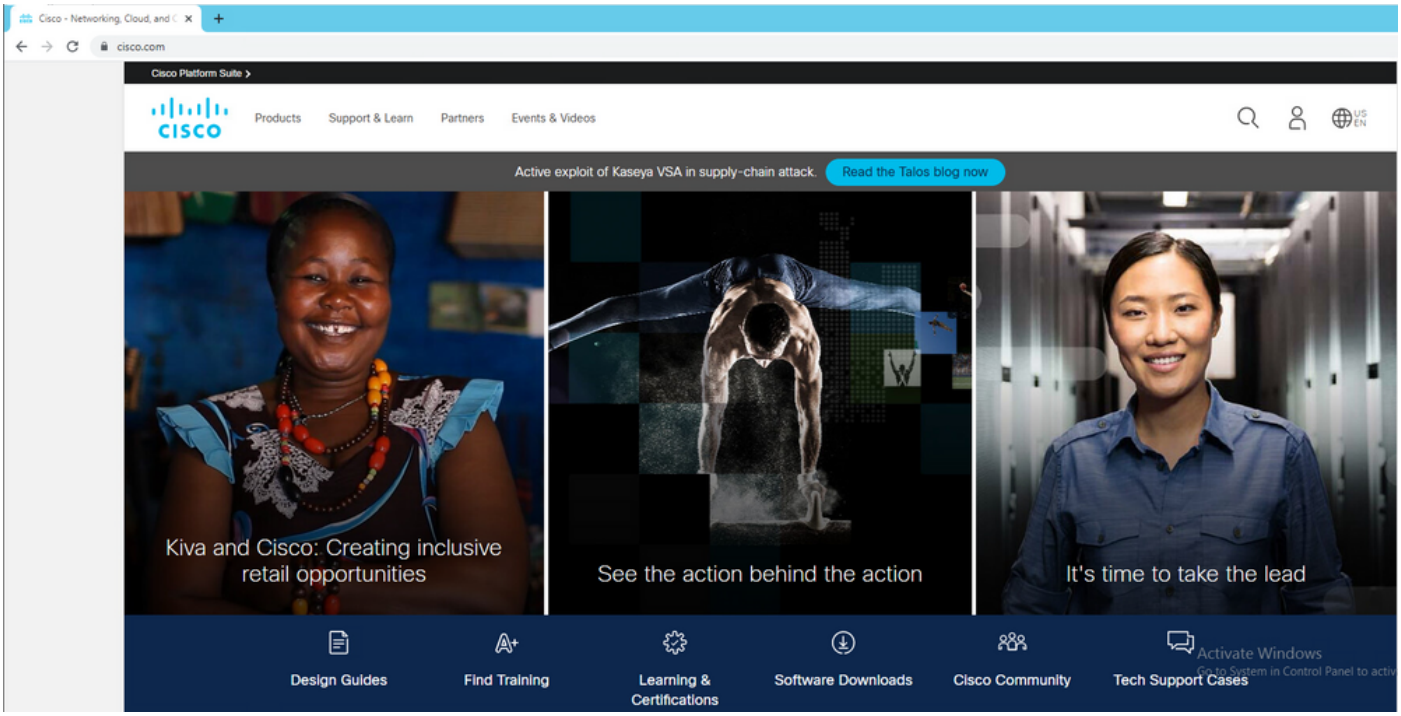
Verificar

Verifique se o dispositivo do usuário recebe a caixa de seleção ao navegar para um site HTTPS.



Insira as credenciais do AD do usuário.





Troubleshoot

Você pode usar o script **user_map_query.pl** para validar se o FDM tem o mapeamento ip do usuário

```
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)]
```

No modo de silêncio, você pode configurar:

o sistema oferece suporte à identificação-depuração para verificar se o redirecionamento foi bem-sucedido.

```
> 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
```

Referência:

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