配置FDM主动身份验证（强制网络门户）

目录

简介

本文档介绍具有主动身份验证（强制网络门户）集成的Firepower设备管理器(FDM)的配置示例。此配置使用Active Directory(AD)作为源证书和自签名证书。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Firepower威胁防御(FTD)
- Active Directory (AD)
- 自签名证书。
- 安全套接字层 (SSL)

使用的组件

本文档中的信息基于以下软件版本：

- Firepower威胁防御6.6.4
- Active Directory
- PC测试

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

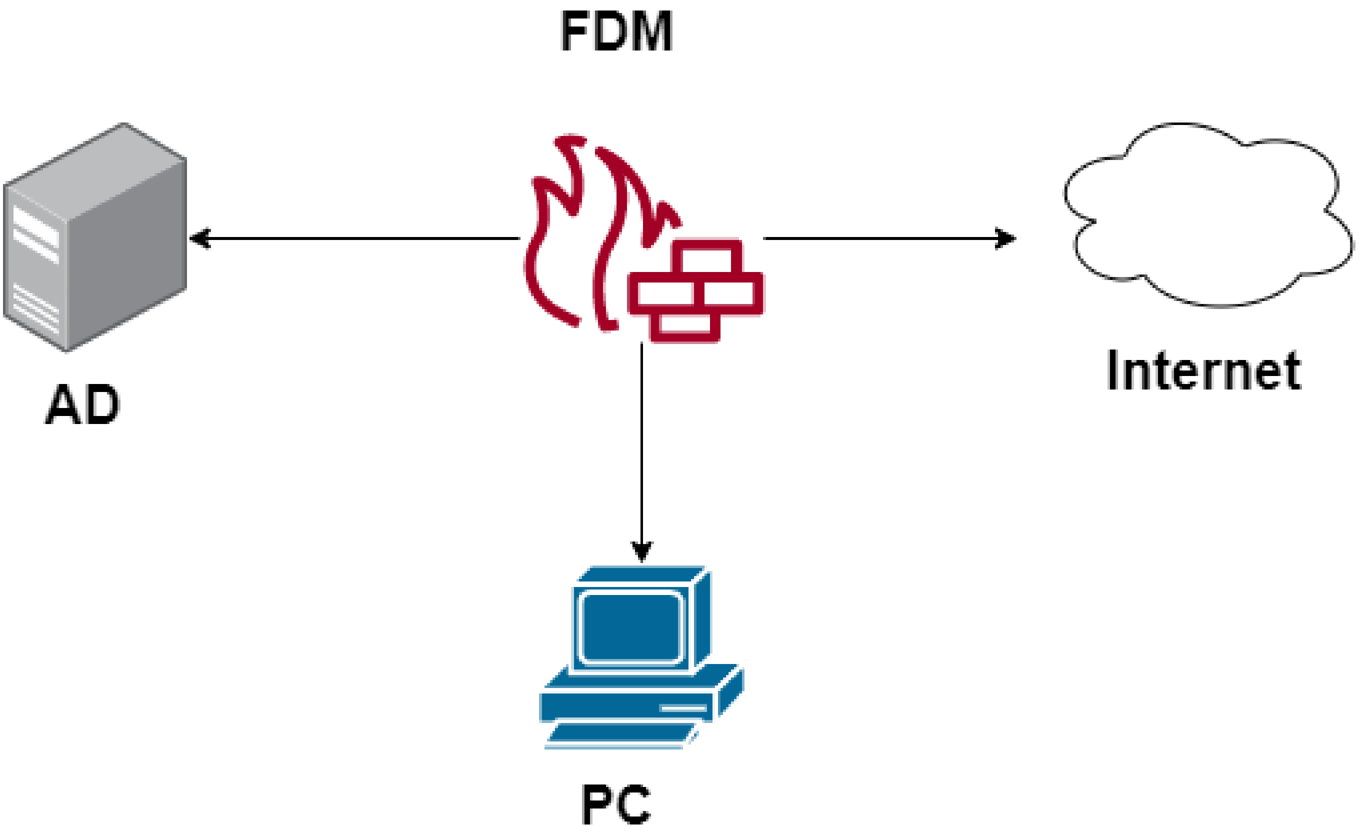
背景信息

通过主动身份验证建立用户身份

身份验证是确认用户身份的行为。使用主动身份验证时，当HTTP流量来自系统没有用户身份映射的IP地址时，您可以决定是否根据为系统配置的目录对发起流量的用户进行身份验证。如果用户成功进行身份验证，则IP地址被视为具有经过身份验证的用户的身份。

身份验证失败不会阻止用户访问网络。您的访问规则最终决定为这些用户提供哪些访问权限。

网络图



配置

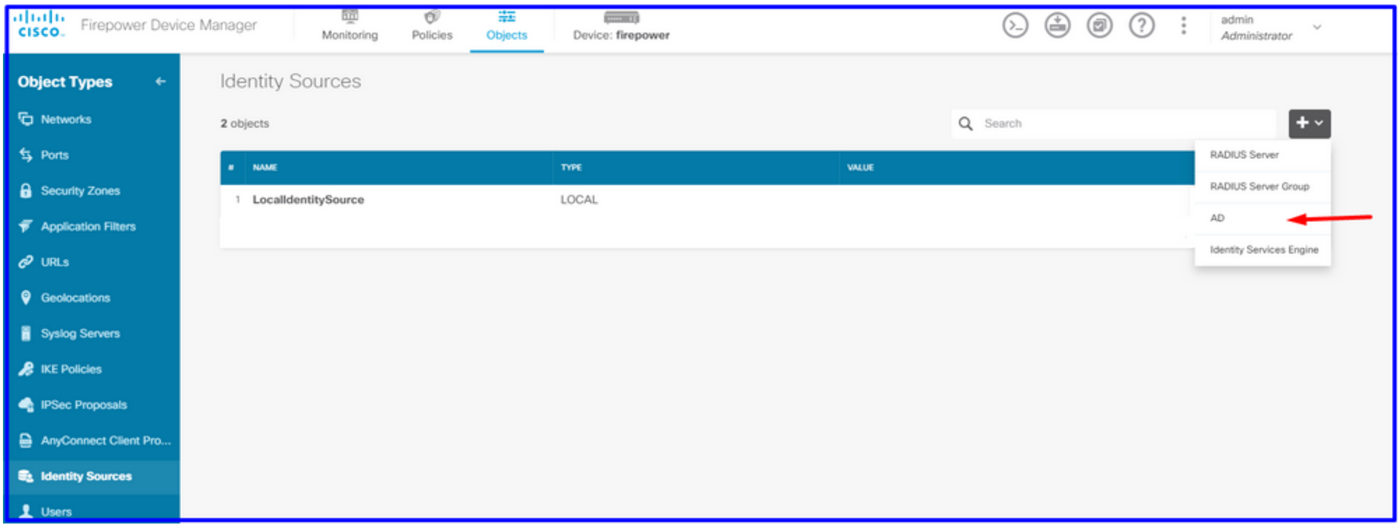
实施身份策略

要启用用户身份获取，以便与IP地址关联的用户已知，您需要配置多个项目

步骤1.配置AD身份领域

无论您主动（通过提示用户进行身份验证）还是被动收集用户身份，都需要配置具有用户身份信息的Active Directory(AD)服务器。

导航至**对象** > **身份服务**，然后选择**AD**以添加Active Directory。

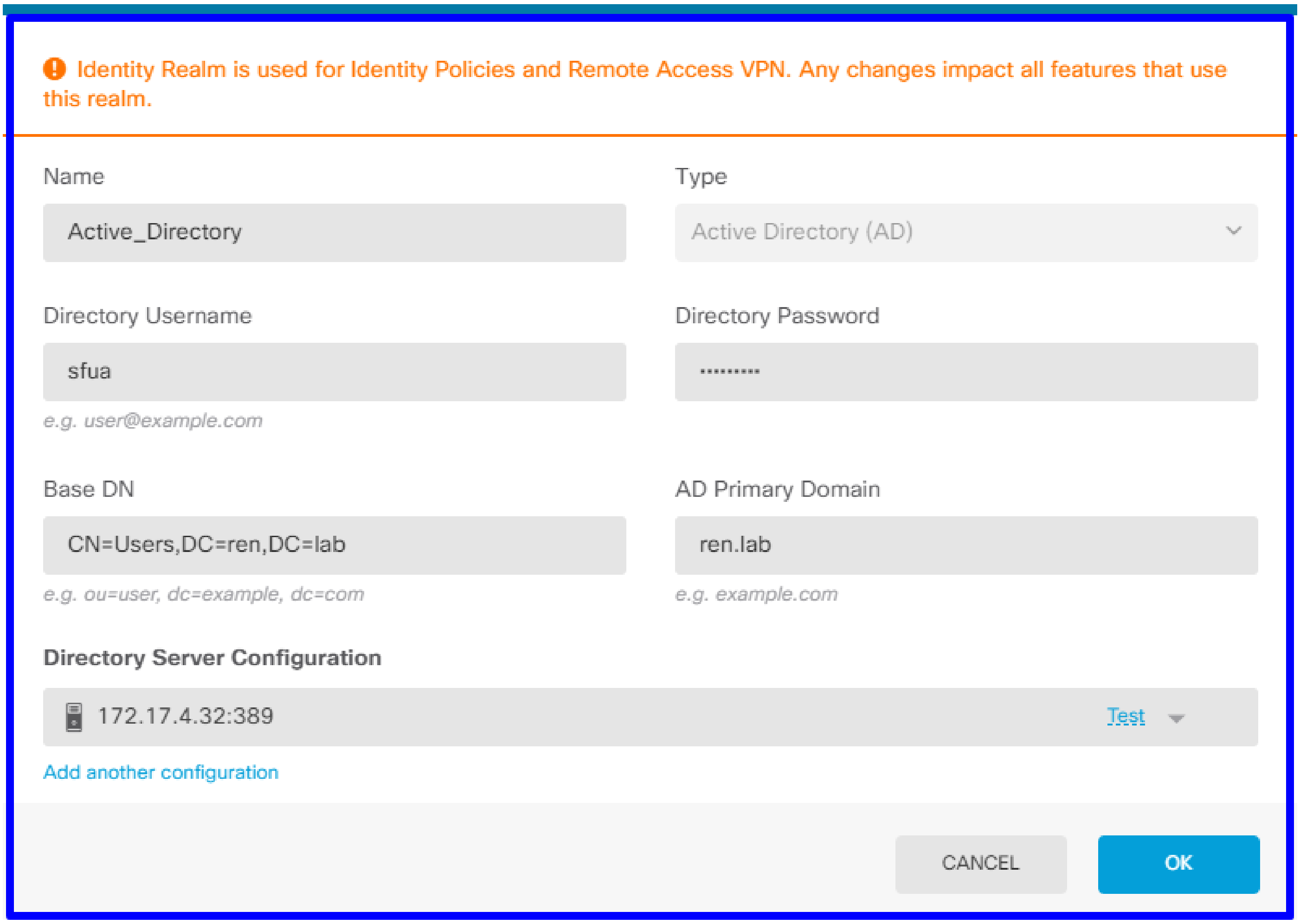


Identity Sources

2 objects

#	NAME	TYPE	VALUE
1	LocalIdentitySource	LOCAL	

添加Active Directory配置：



Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name: Active_Directory	Type: Active Directory (AD)
Directory Username: sfua e.g. user@example.com	Directory Password: *********
Base DN: CN=Users,DC=ren,DC=lab e.g. ou=user, dc=example, dc=com	AD Primary Domain: ren.lab e.g. example.com

Directory Server Configuration

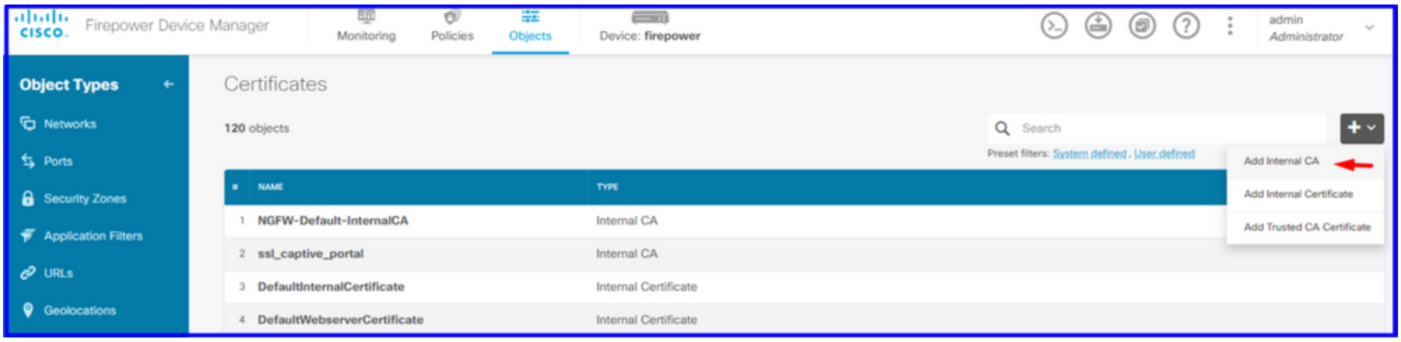
172.17.4.32:389

步骤2.创建自签名证书

要创建强制网络门户配置，您需要两个证书，一个用于强制网络门户，一个用于SSL解密。

您可以创建自签名证书，如本例所示。

导航至**对象**>**证书**



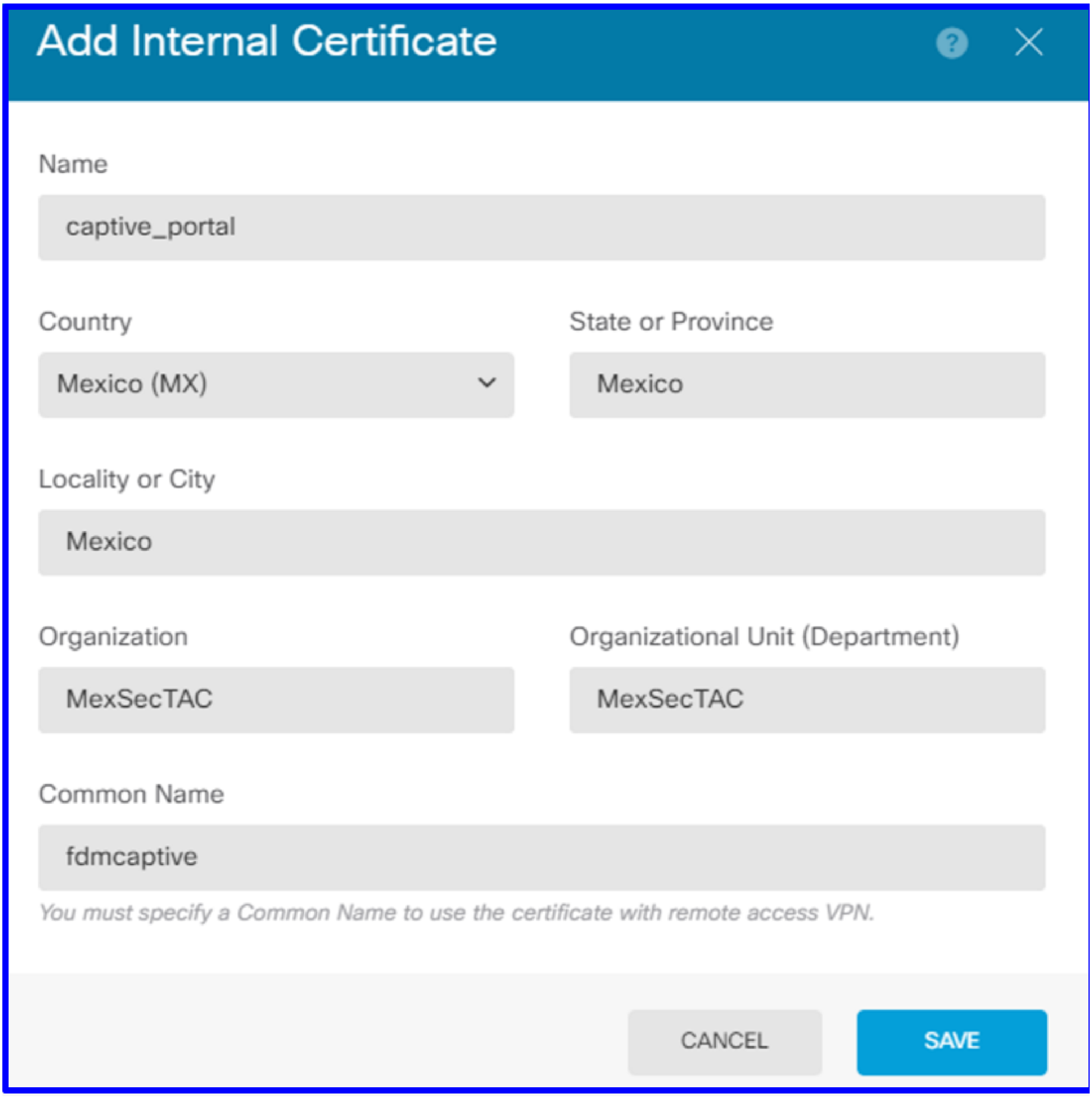
Certificates

120 objects

Preset filters: System defined, User defined

#	NAME	TYPE
1	NGFW-Default-InternalCA	Internal CA
2	ssl_captive_portal	Internal CA
3	DefaultInternalCertificate	Internal Certificate
4	DefaultWebserverCertificate	Internal Certificate

强制网络门户自签名证书：



Add Internal Certificate

Name: captive_portal

Country: Mexico (MX)

State or Province: Mexico

Locality or City: Mexico

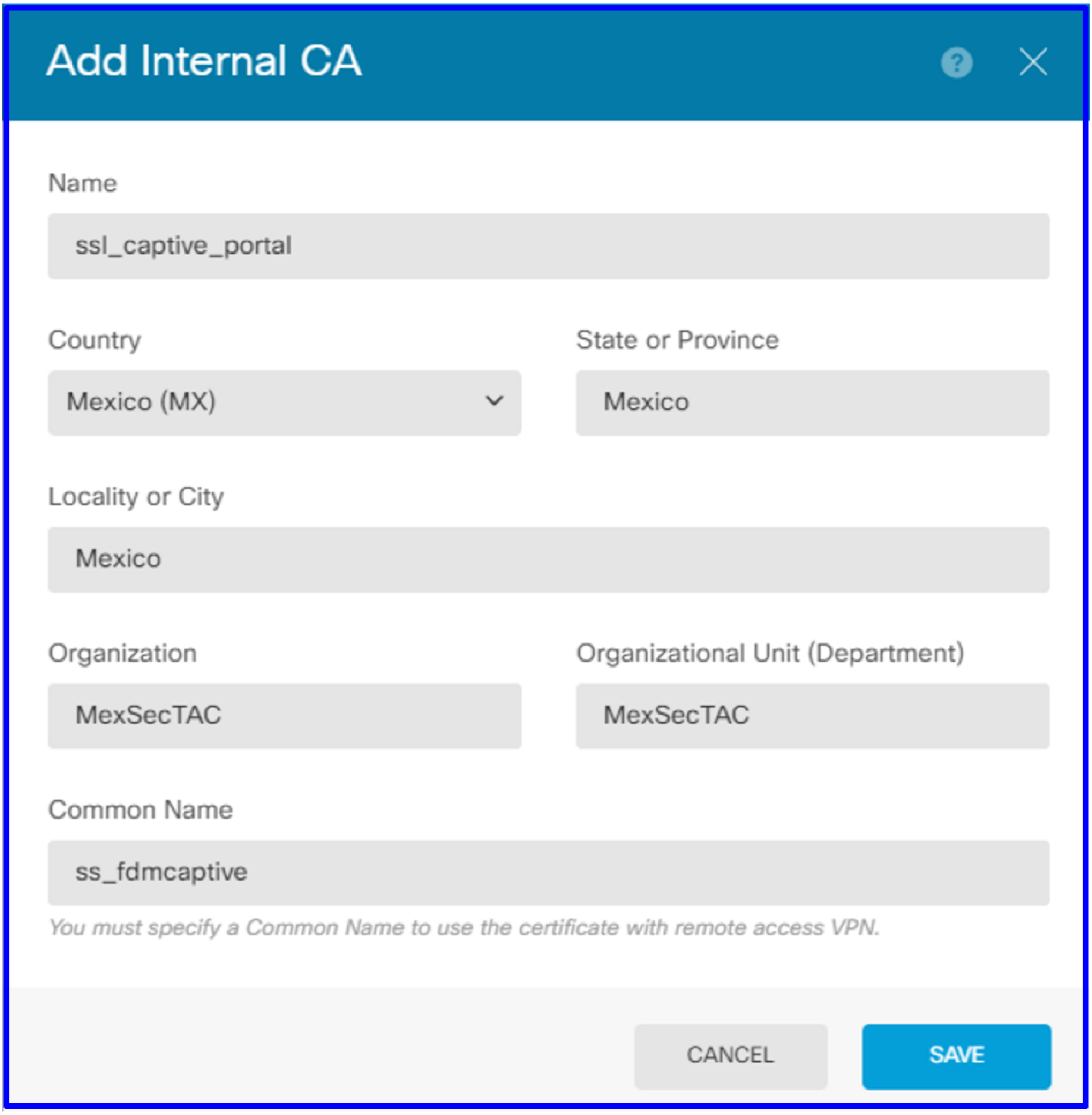
Organization: MexSecTAC

Organizational Unit (Department): MexSecTAC

Common Name: fdmcaptive

You must specify a Common Name to use the certificate with remote access VPN.

SSL自签名证书：



Name

ssl_captive_portal

Country

Mexico (MX)

State or Province

Mexico

Locality or City

Mexico

Organization

MexSecTAC

Organizational Unit (Department)

MexSecTAC

Common Name

ss_fdmcaptive

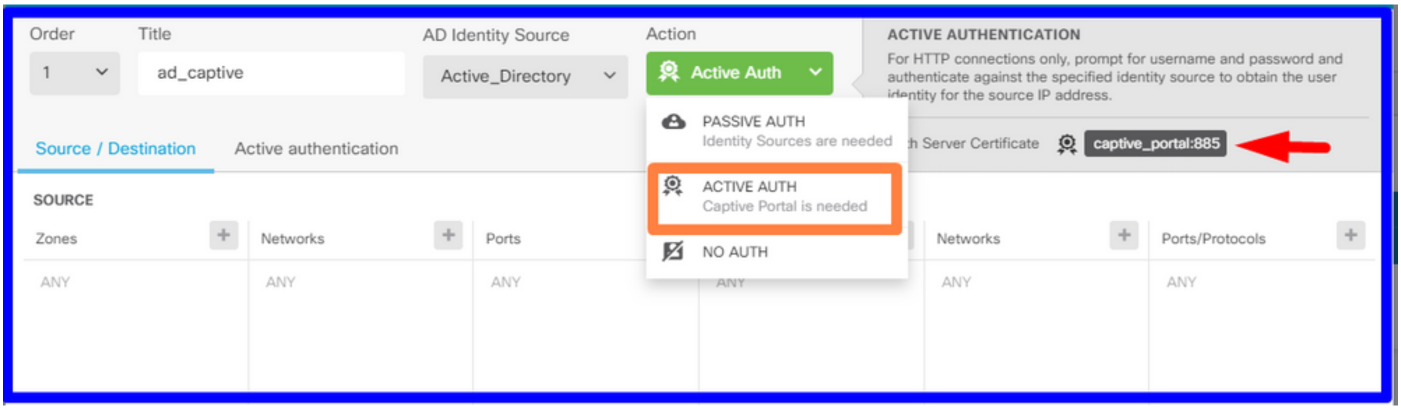
You must specify a Common Name to use the certificate with remote access VPN.

步骤3.创建身份规则

导航至**策略** > **身份>** 选择**[+]按钮以添加新的身份规则。**

您需要创建身份策略以配置主动身份验证，策略必须具有以下元素：

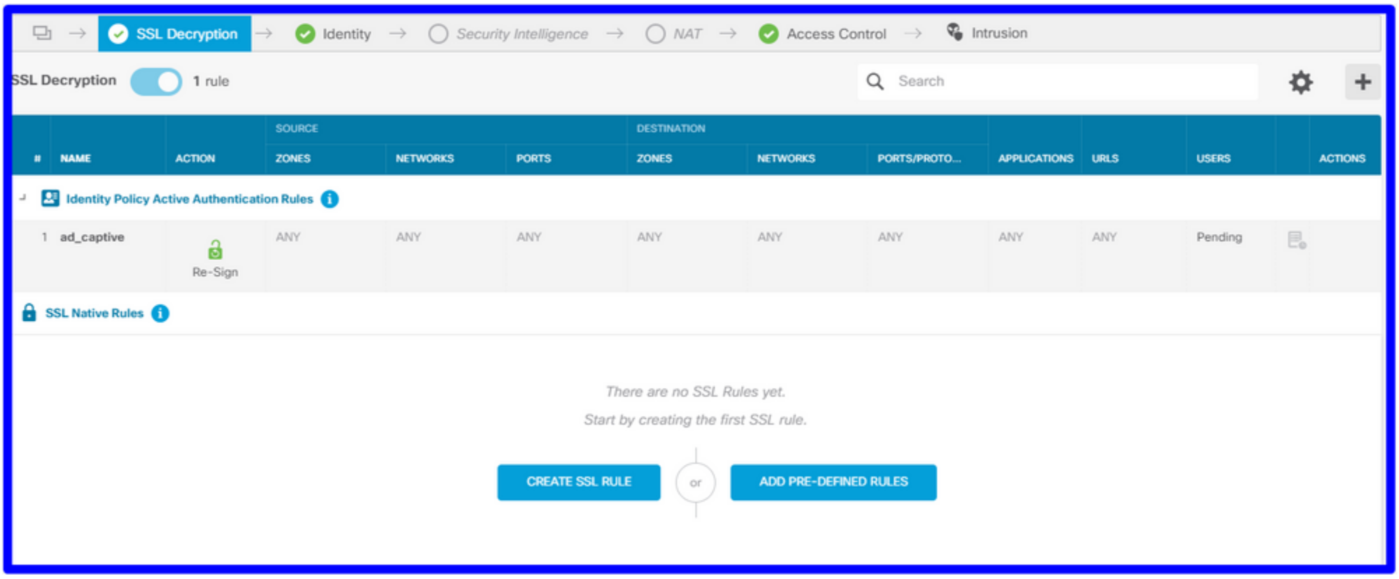
- AD身份源：步骤1中添加的相同
- 操作：活动身份验证
- 服务器证书:您在[在此场景中captive_portal]之前创建的自签名证书相同
- type：HTTP基本（在本示例场景中）



Order: 1
Title: ad_captive
AD Identity Source: Active_Directory
Action: Active Auth

ACTIVE AUTHENTICATION
For HTTP connections only, prompt for username and password and authenticate against the specified identity source to obtain the user identity for the source IP address.

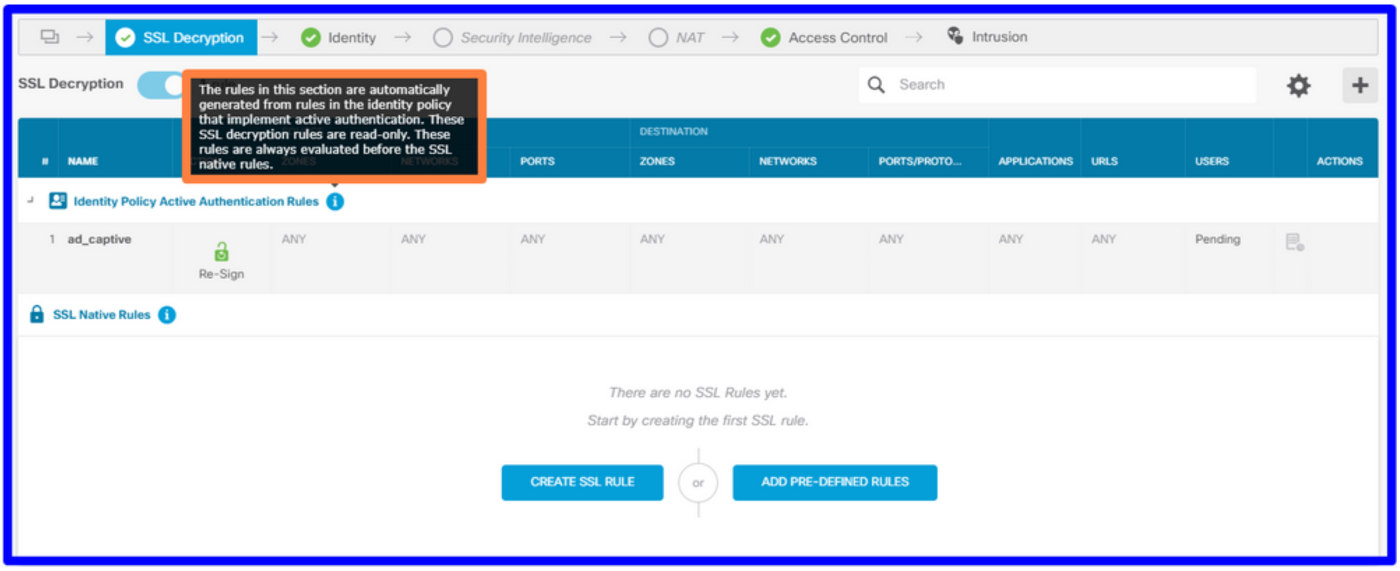
一旦身份策略创建为主动身份验证，将自动创建SSL规则，默认情况下，此规则设置为any any，并带有**Decrypt-Resign**，这意味着此规则没有SSL修改。



#	NAME	ACTION	SOURCE ZONES	SOURCE NETWORKS	SOURCE PORTS	DESTINATION ZONES	DESTINATION NETWORKS	DESTINATION PORTS/PROTO...	APPLICATIONS	URLS	USERS	ACTIONS
Identity Policy Active Authentication Rules												
1	ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	
SSL Native Rules												

There are no SSL Rules yet.
Start by creating the first SSL rule.

CREATE SSL RULE or ADD PRE-DEFINED RULES



The rules in this section are automatically generated from rules in the identity policy that implement active authentication. These SSL decryption rules are read-only. These rules are always evaluated before the SSL native rules.

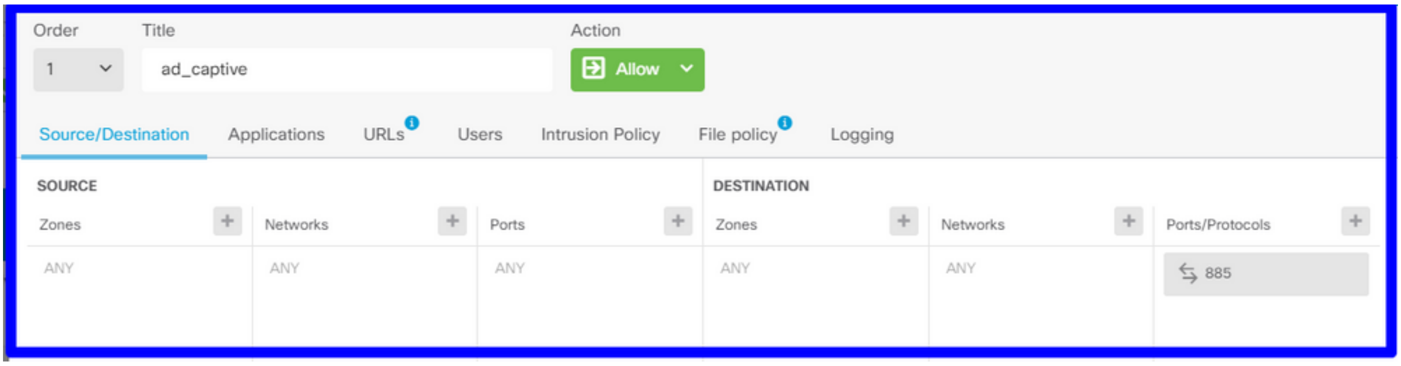
#	NAME	ACTION	SOURCE ZONES	SOURCE NETWORKS	SOURCE PORTS	DESTINATION ZONES	DESTINATION NETWORKS	DESTINATION PORTS/PROTO...	APPLICATIONS	URLS	USERS	ACTIONS
Identity Policy Active Authentication Rules												
1	ad_captive	Re-Sign	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Pending	
SSL Native Rules												

There are no SSL Rules yet.
Start by creating the first SSL rule.

CREATE SSL RULE or ADD PRE-DEFINED RULES

步骤4.在访问控制策略中创建访问规则

您需要允许将流**量重定向到强**制网络门户身份验证的端口885/tcp。导航至**Policies** > **Access Control**并添加访问规则。



Order: 1
Title: ad_captive
Action: Allow

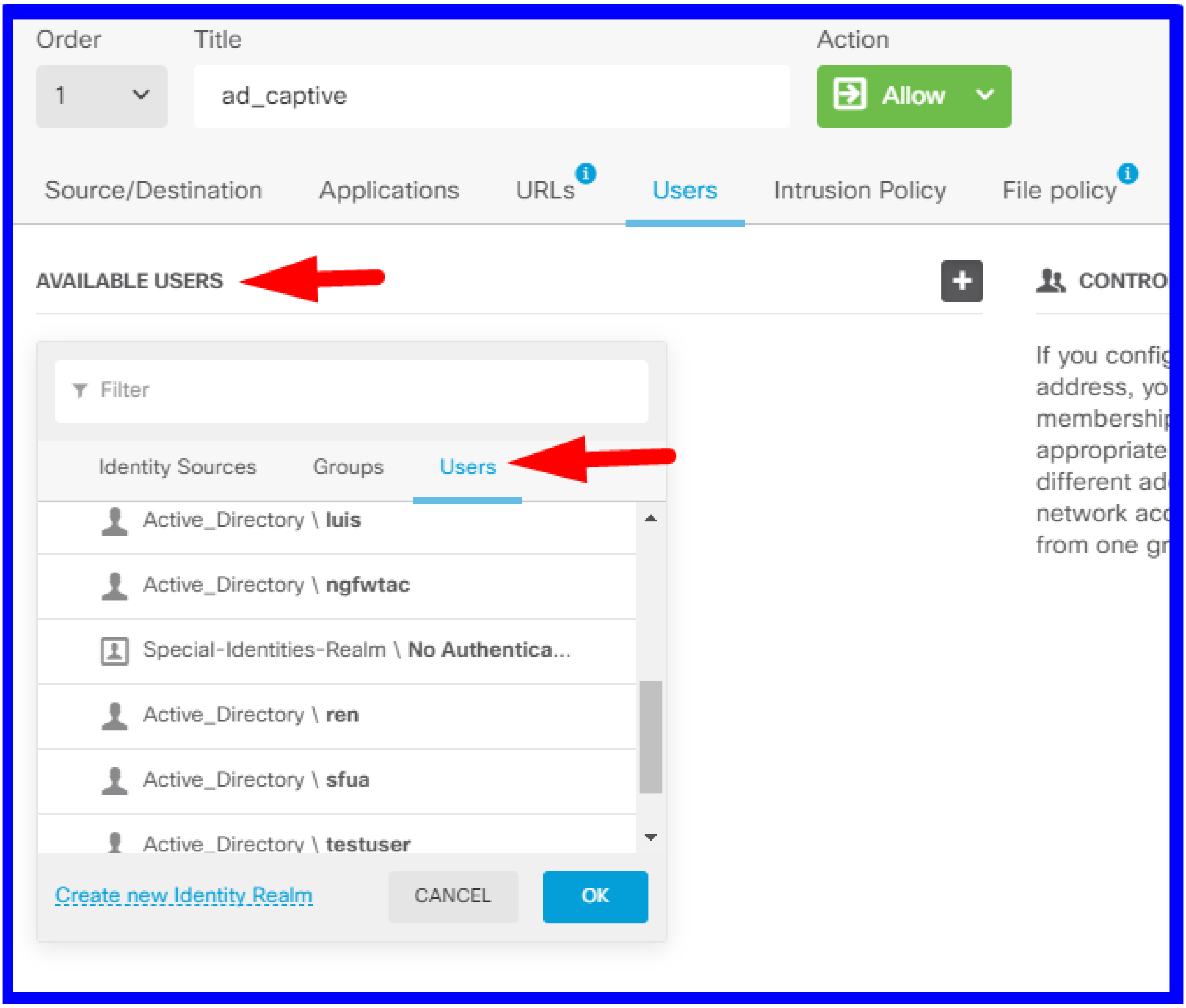
SOURCE

Zones	Networks	Ports
ANY	ANY	ANY

DESTINATION

Zones	Networks	Ports/Protocols
ANY	ANY	885

如果需要检查用户是否从AD下载，可以编辑访问规则并导航至**用户**部分，然后在可用用户**上**，可以验证FDM已有多少用户。



Order: 1
Title: ad_captive
Action: Allow

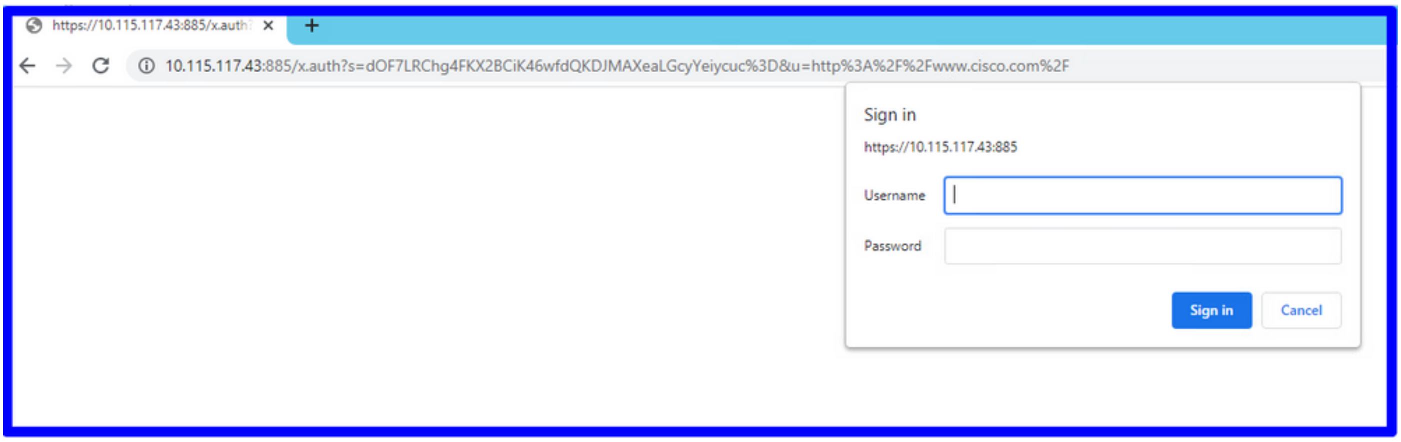
- Active_Directory \ **luis**
- Active_Directory \ **ngfwtac**
- Special-Identities-Realm \ **No Authentica...**
- Active_Directory \ **ren**
- Active_Directory \ **sfua**
- Active_Directory \ **testuser**

If you config
address, yo
membershi
appropriate
different ad
network acc
from one gr

切记部署配置更改。

验证

检验用户设备在导航到HTTPS站点时是否收到复选框。



https://10.115.117.43:885/x.auth?s=dOF7LRChg4FKX2BCiK46wfdQKDJMAXeaLGcyYeiycuc%3D&u=http%3A%2F%2Fwww.cisco.com%2F

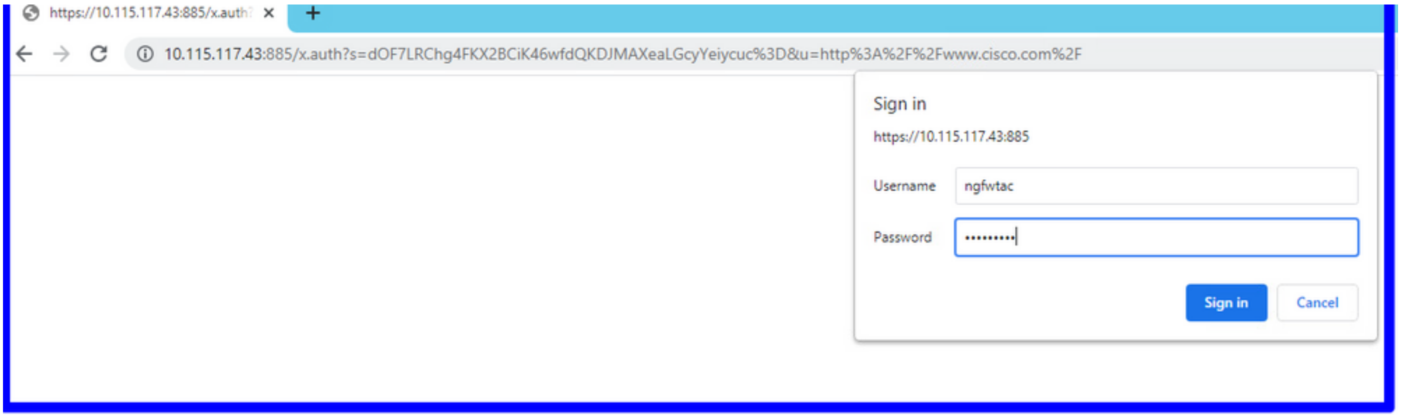
Sign in

https://10.115.117.43:885

Username

Password

输入用户AD凭证。



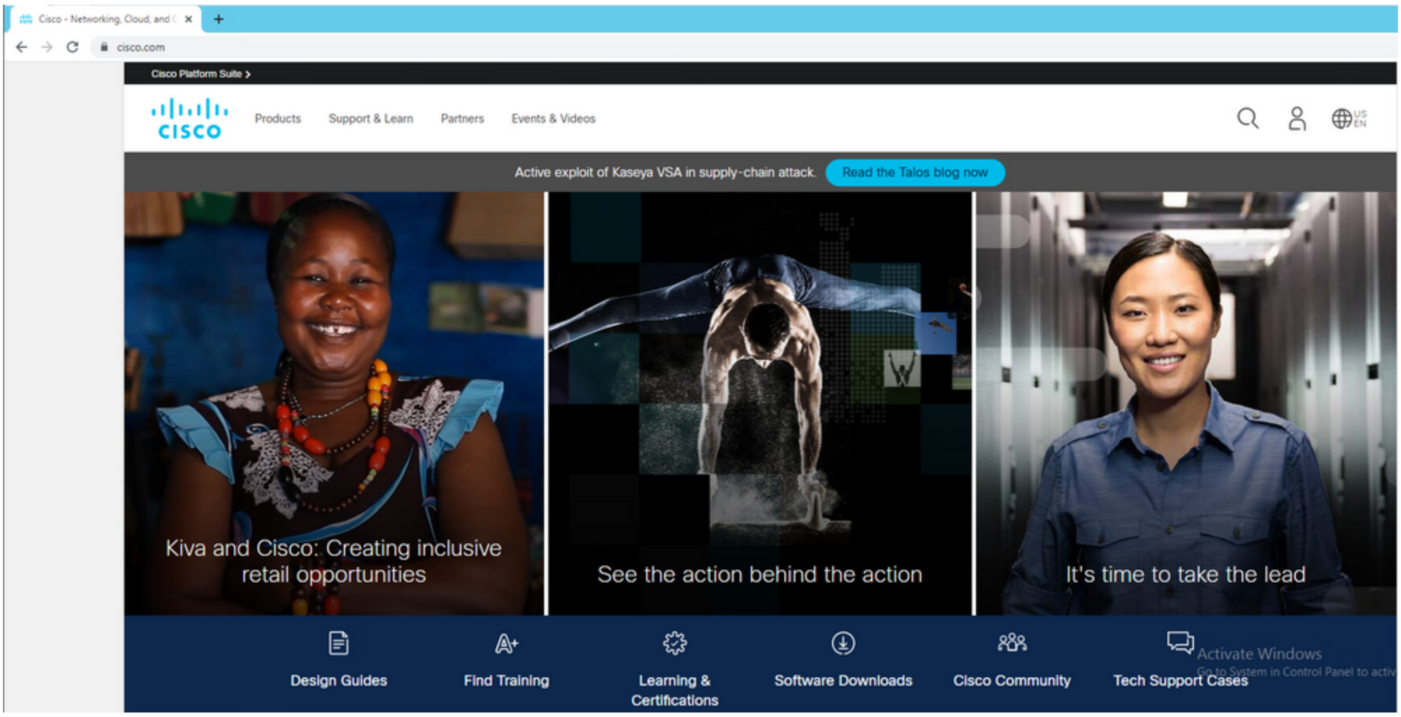
https://10.115.117.43:885/x.auth?s=dOF7LRChg4FKX2BCiK46wfdQKDJMAXeaLGcyYeiycuc%3D&u=http%3A%2F%2Fwww.cisco.com%2F

Sign in

https://10.115.117.43:885

Username ngfwtac

Password •••••••••



cisco.com

Cisco - Networking, Cloud, and C
Cisco Platform Suite >
CISCO
Products
Support & Learn
Partners
Events & Videos
Active exploit of Kaseya VSA in supply-chain attack.
Read the Talos blog now
Kiva and Cisco: Creating inclusive retail opportunities
See the action behind the action
It's time to take the lead
Design Guides
Find Training
Learning & Certifications
Software Downloads
Cisco Community
Tech Support Cases
Activate Windows
Go to System in Control Panel to activ

故障排除

可以使用**user_map_query.pl**脚本验证FDM具有用户IP映射

```
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)]
```

在clish模式下，您可以配置：

系统支持identity-debug以验证重定向是否成功。

```
> 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:

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