Configurer la stratégie d'identité sur le Centre de gestion du pare-feu sécurisé (FMC)

Table des matières

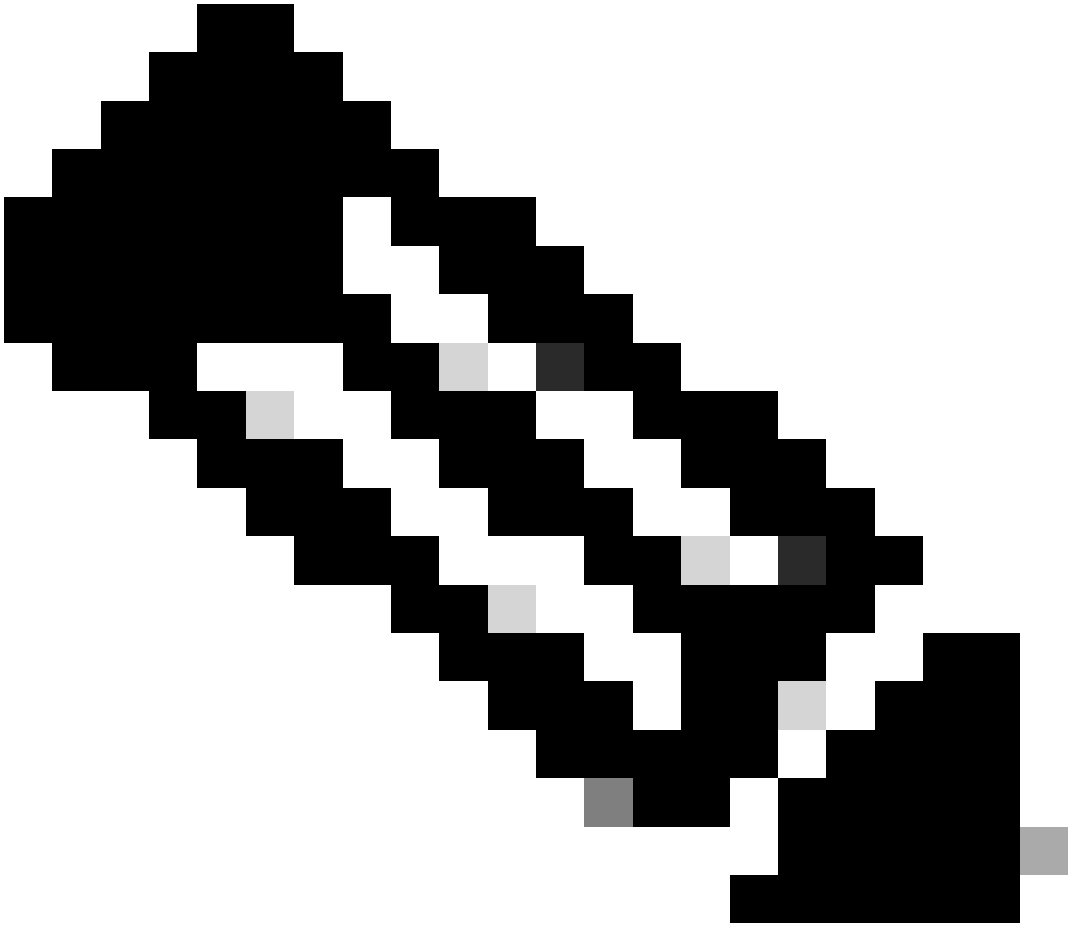
Introduction

Ce document décrit le processus de configuration et de déploiement d'une politique d'identité pour un trafic FTD sécurisé via Secure FMC.

Conditions préalables

1. Domaine déjà configuré dans FMC.

2. Source d'identité déjà configurée - ISE, ISE-PIC.



Remarque : les instructions de configuration ISE et de domaine (realm) sortent du cadre de ce document.

Exigences

Cisco recommande d'avoir connaissance de ces sujets :

- Centre de gestion du pare-feu sécurisé (FMC)
- Défense sécurisée contre les threads pare-feu (FTD)
- Cisco Identity Services Engine (ISE)
- Serveur(s) LDAP/AD
- Méthodes d'authentification

1. Authentification passive : utilisation d'une source utilisateur d'identité externe telle qu'ISE
2. Authentification active : utilisation du périphérique géré comme source d'authentification (portail captif ou accès VPN distant)

3. Aucune authentification

Composants utilisés

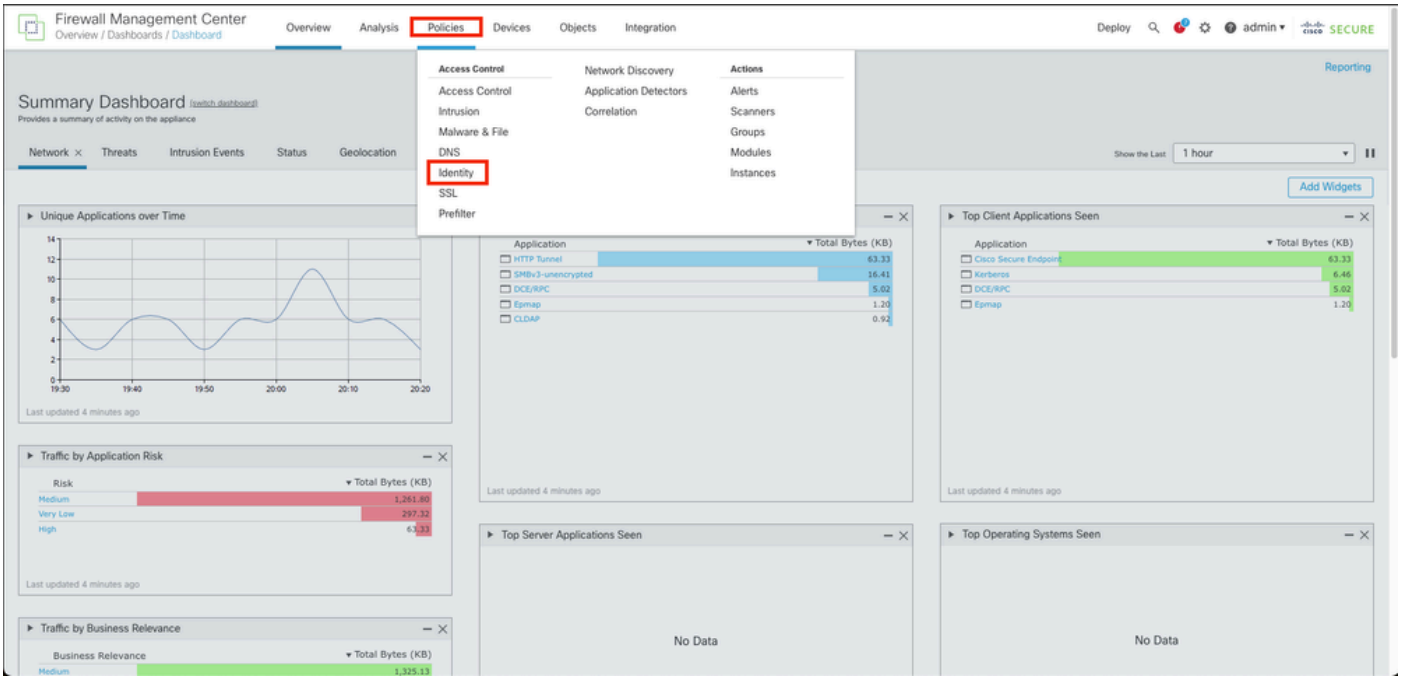
- Secure Firewall Management Center pour VMWare v7.2.5
- Cisco Secure Firewall Threat Defense pour VMWare v7.2.4
- Serveur Active Directory
- Correctif 4 de Cisco Identity Services Engine (ISE) v3.2
- Méthode d'authentification passive

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

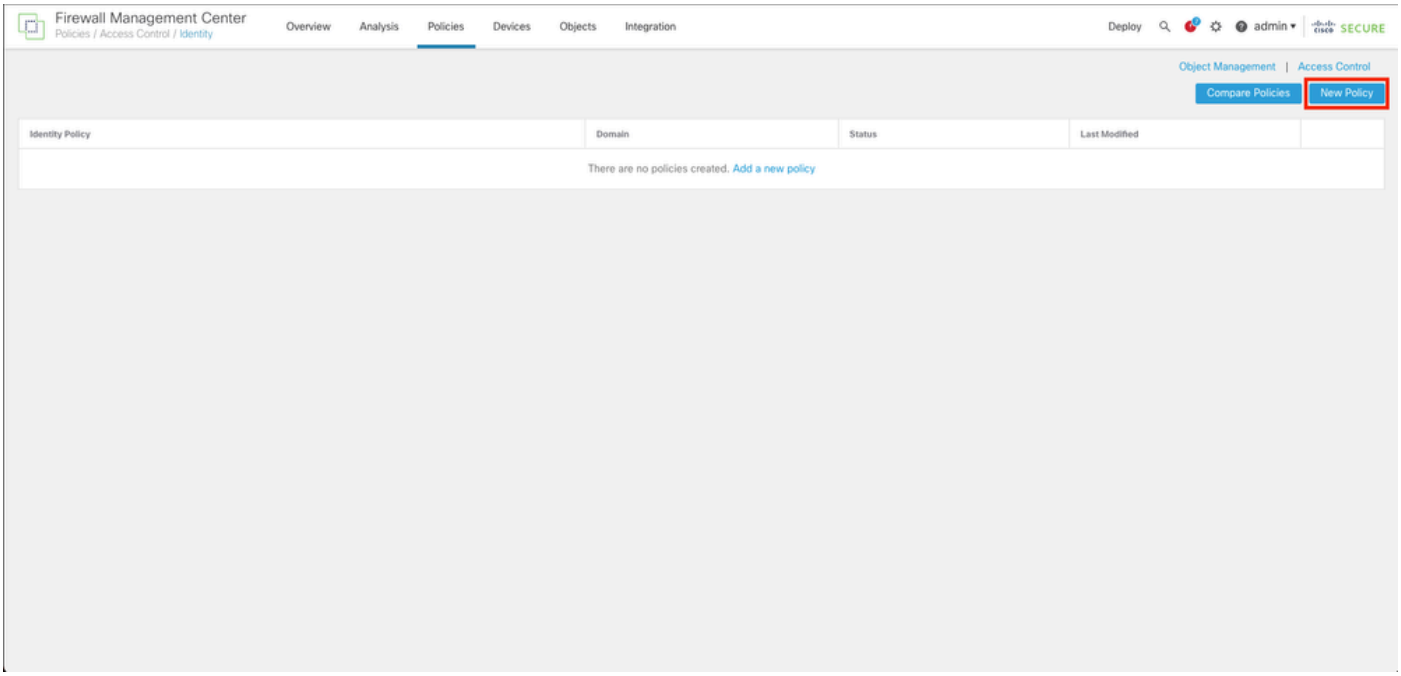
Configurer

Configurations

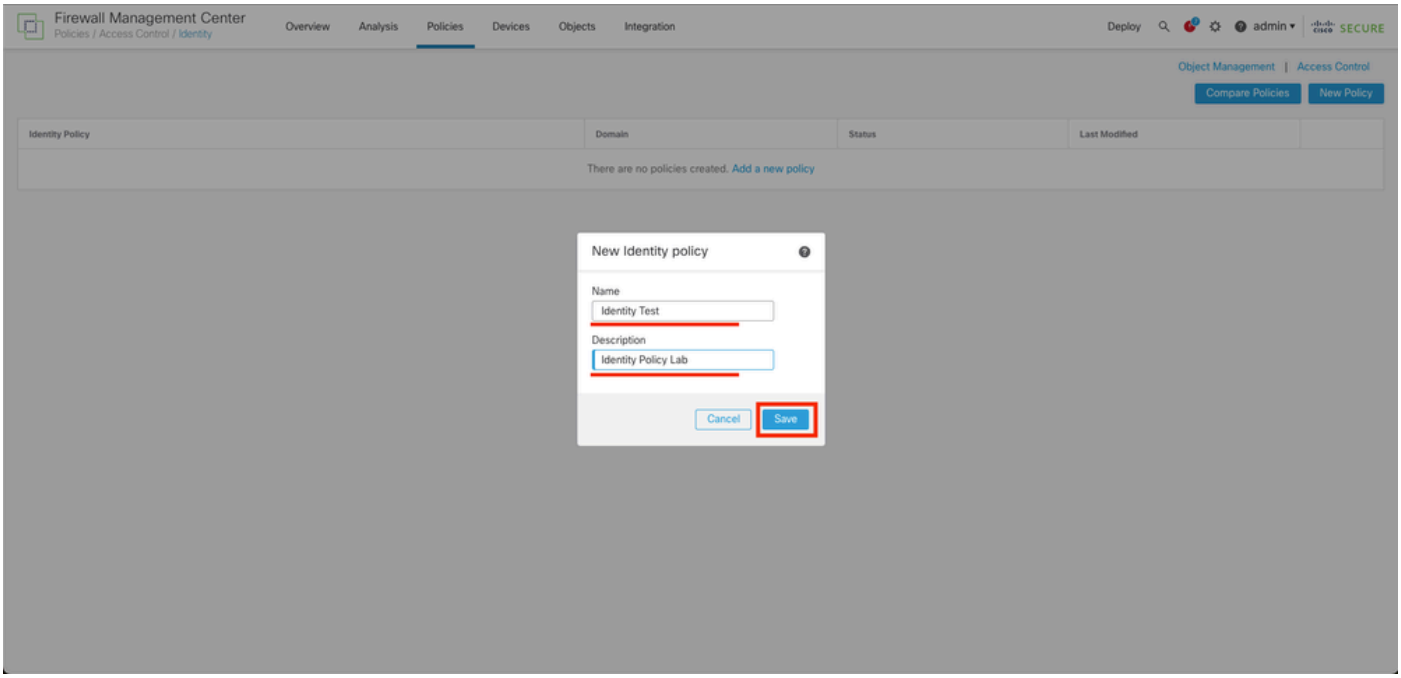
Étape 1. Dans l'interface utilisateur graphique de FMC , accédez à Policies > Access Control > Identity



Étape 2. Cliquez sur New Policy.

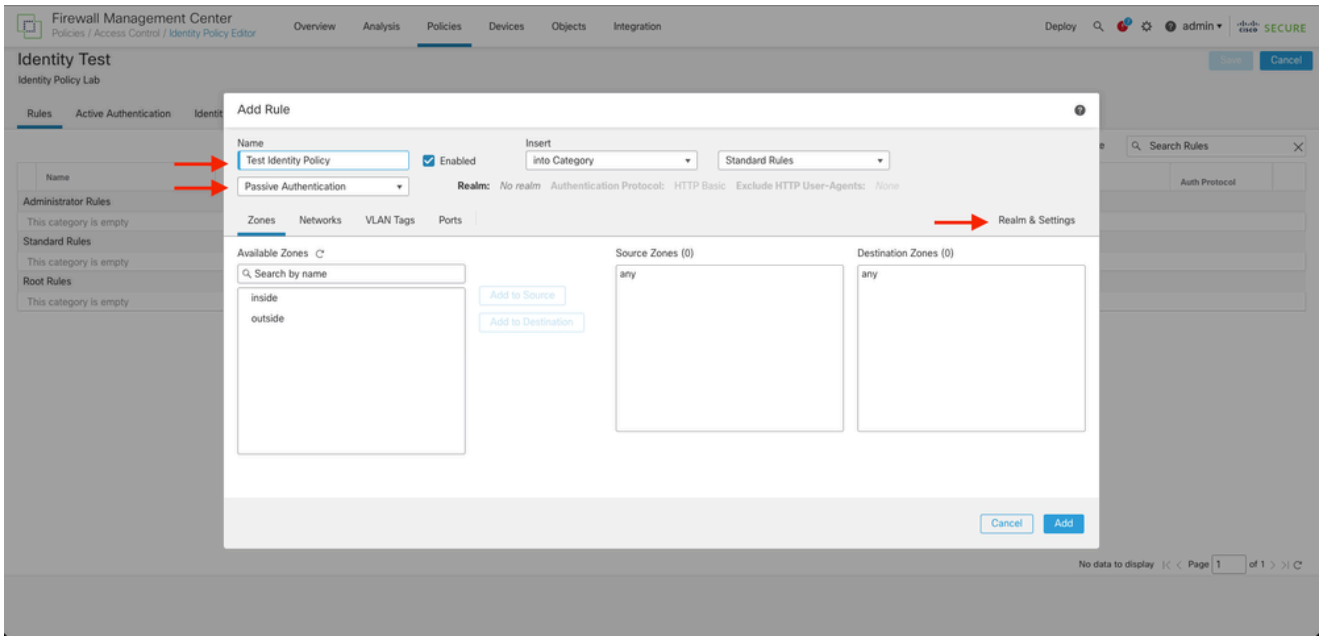


Étape 3. Attribuez un nom et une description à la nouvelle stratégie d'identité, puis cliquez sur Enregistrer.

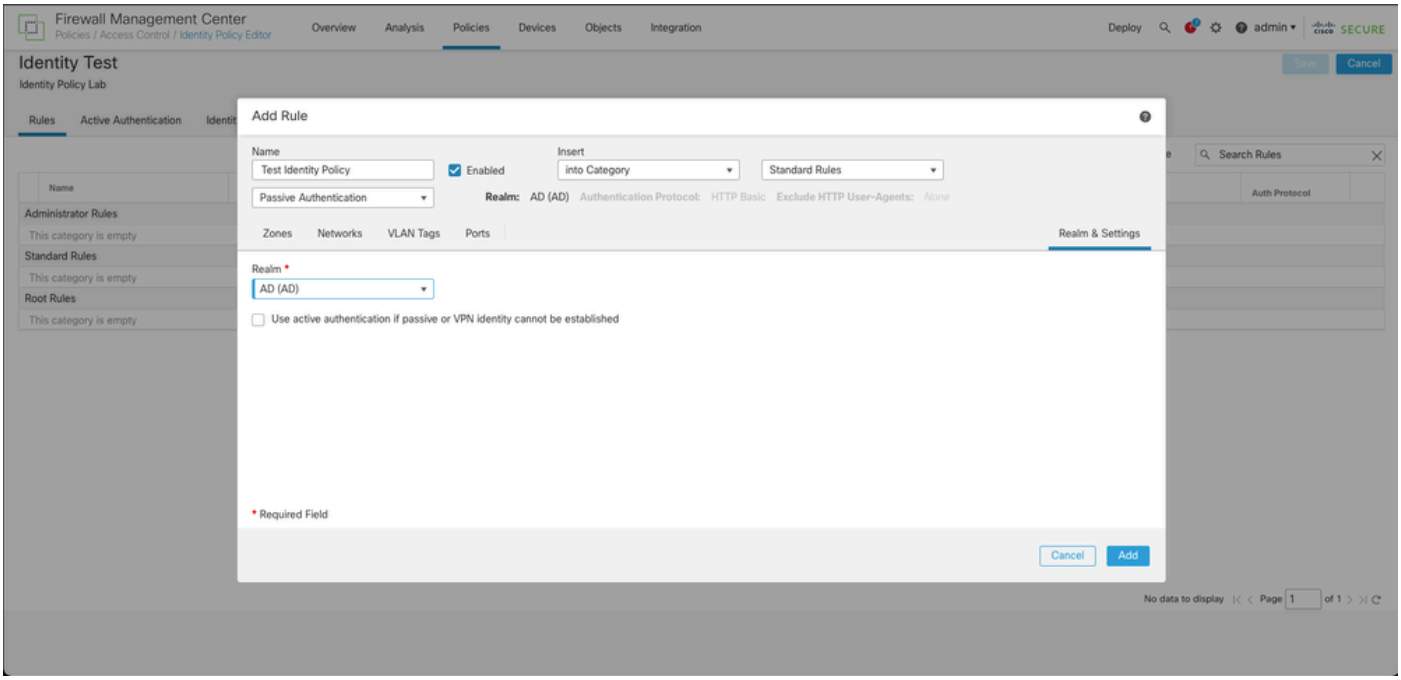


Étape 4. Cliquez sur + Icône Ajouter une règle.

1. Attribuez un nom à la nouvelle règle.
2. Dans le champ du nom, choisissez la méthode d'authentification, sélectionnez : Authentification passive.
3. À droite de l'écran, sélectionnez Domaine et paramètres.

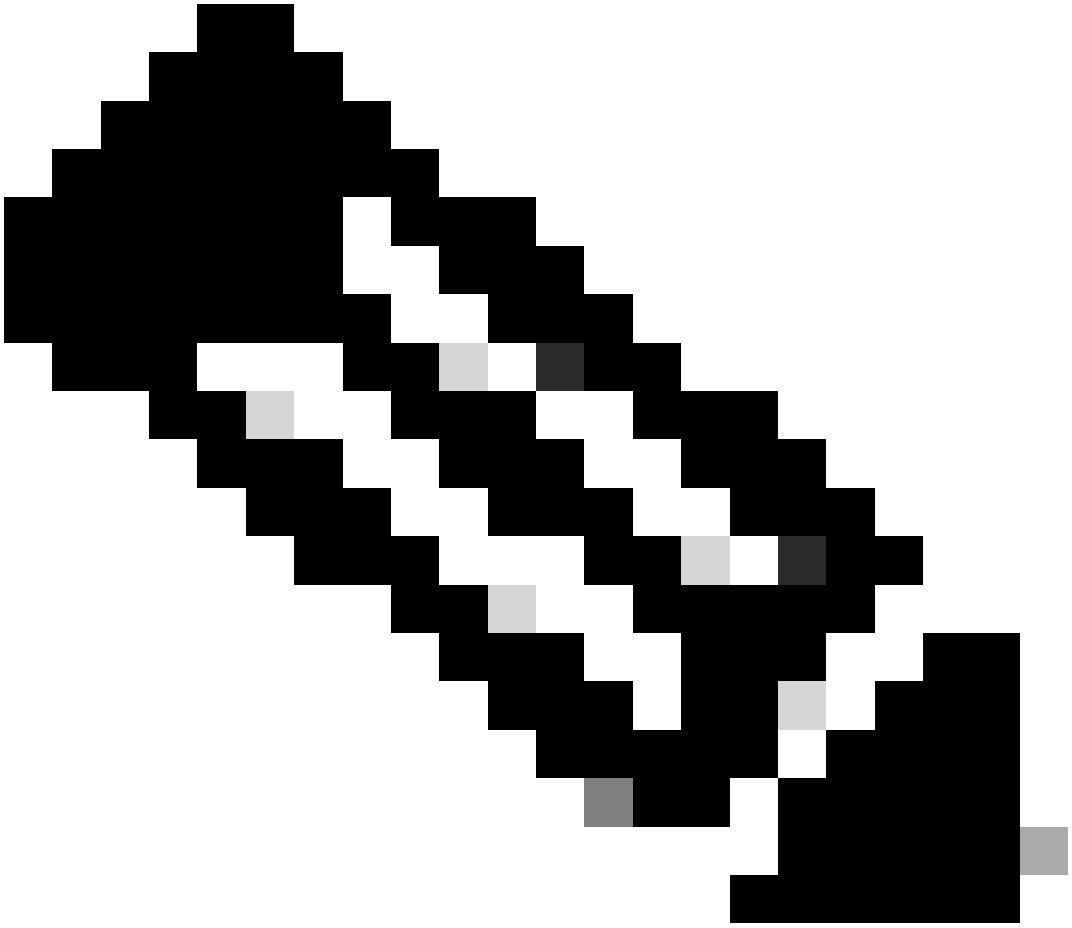


4. Sélectionnez un domaine dans le menu déroulant.



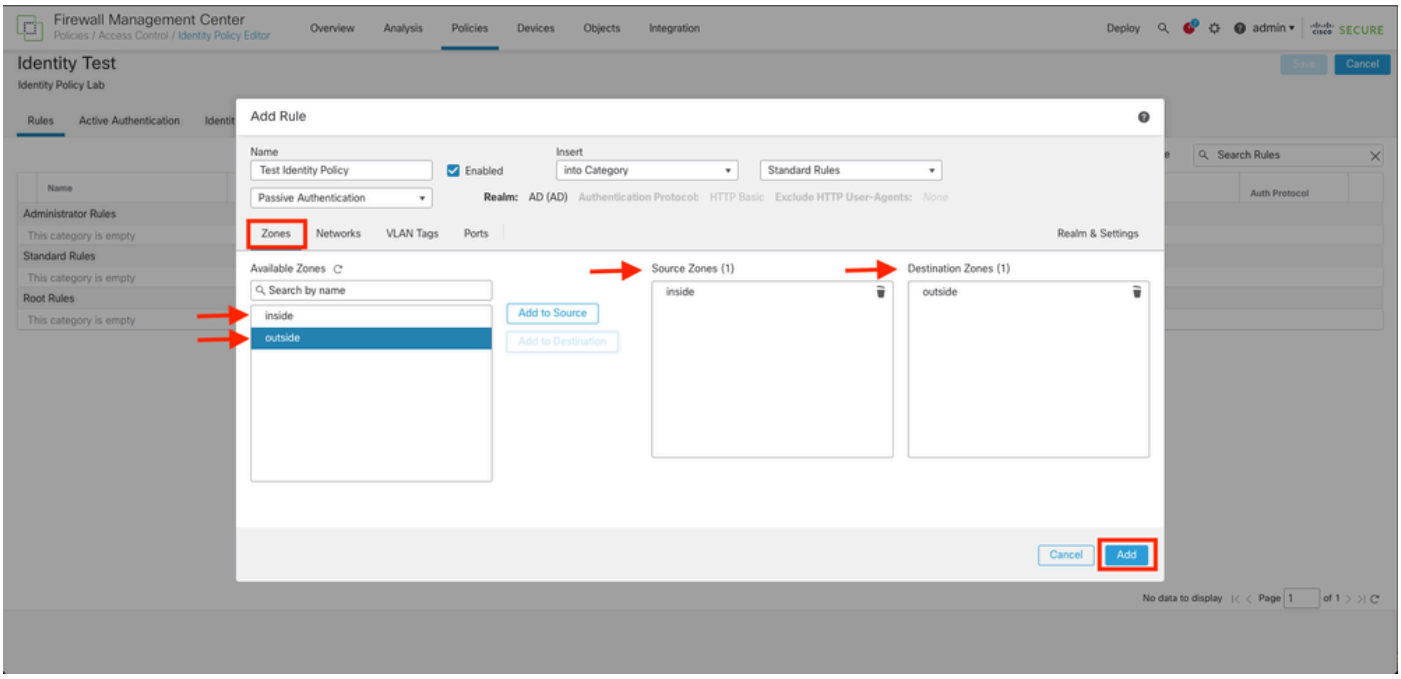
5. Cliquez sur Zones à gauche de l'écran.

6. Dans le menu Available Zones, affectez une zone source et une zone de destination en fonction du chemin de trafic nécessaire pour détecter les utilisateurs. Pour ajouter une zone, cliquez sur son nom, puis sélectionnez Ajouter à la source ou Ajouter à la destination selon le cas.

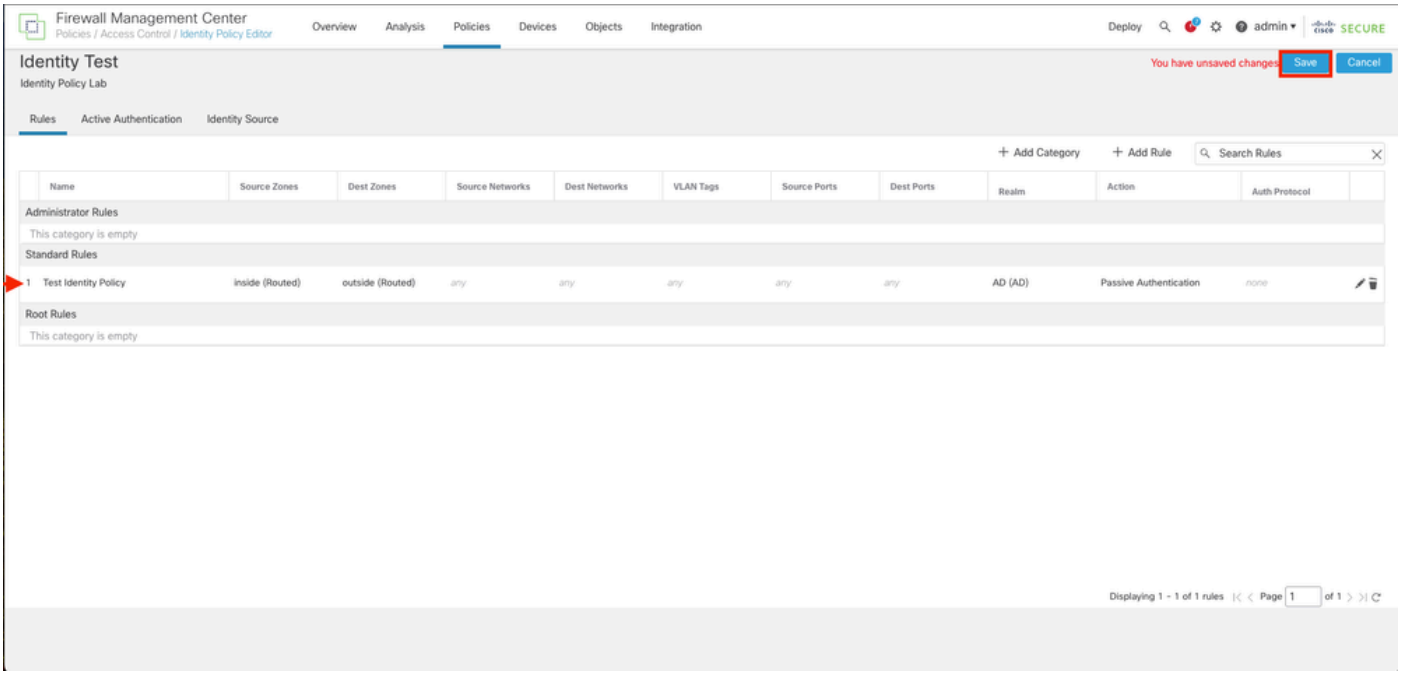


Remarque : dans cette documentation, la détection de l'utilisateur ne sera appliquée que pour le trafic provenant de la zone interne et transféré à la zone externe.

7. Sélectionnez Ajouter et Enregistrer.

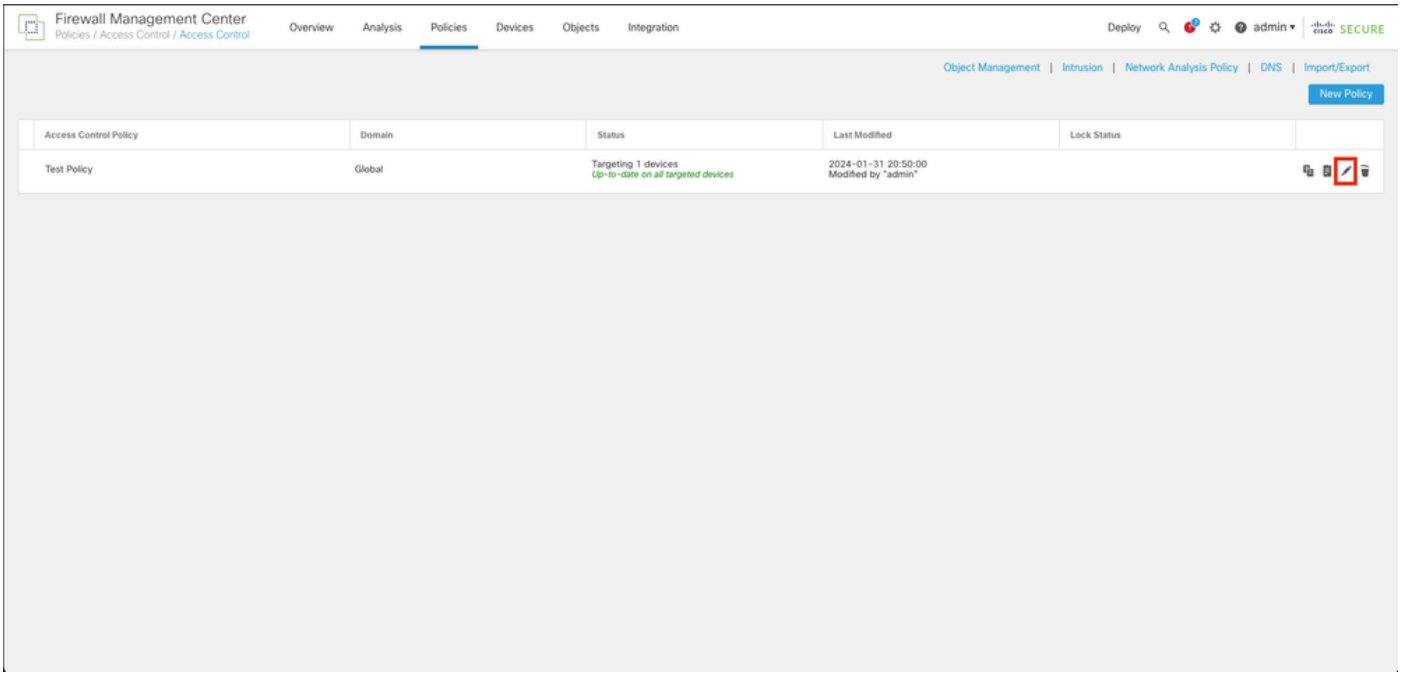


Étape 5. Vérifiez que la nouvelle règle se trouve dans la stratégie d'identité et cliquez sur Enregistrer.

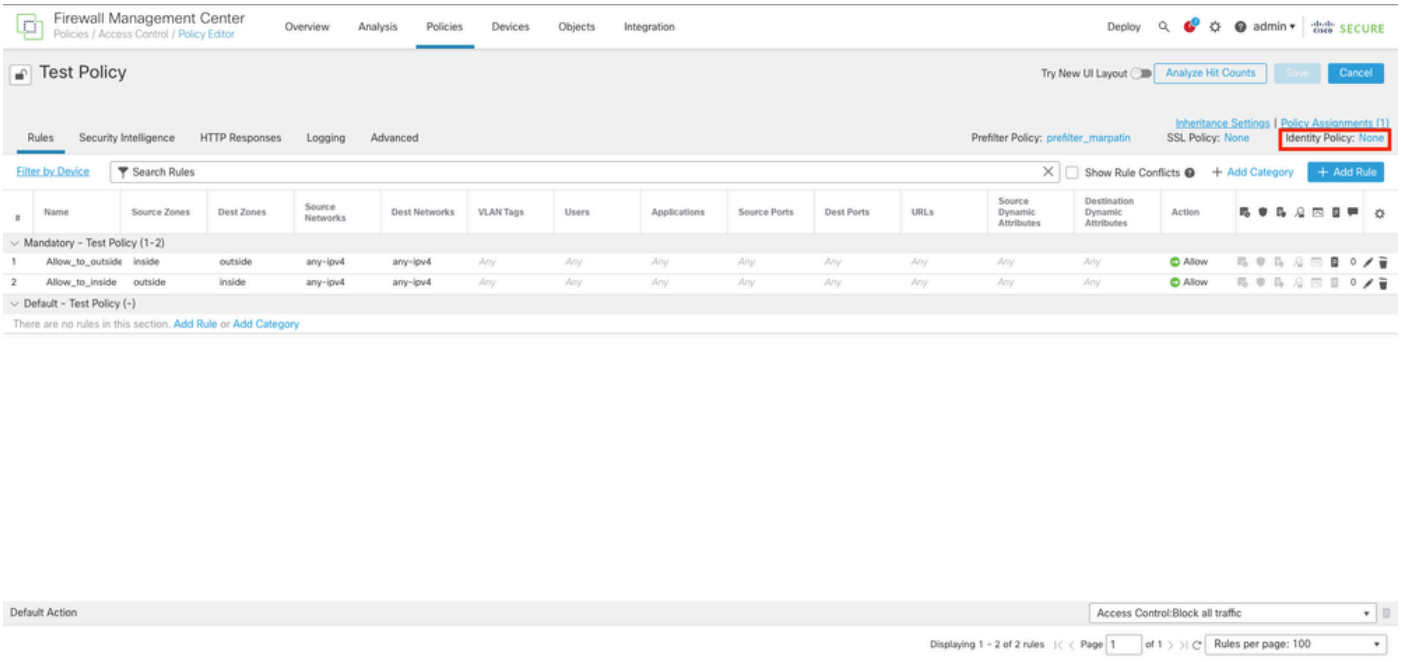


Étape 6. Accédez à Politiques > Contrôle d'accès

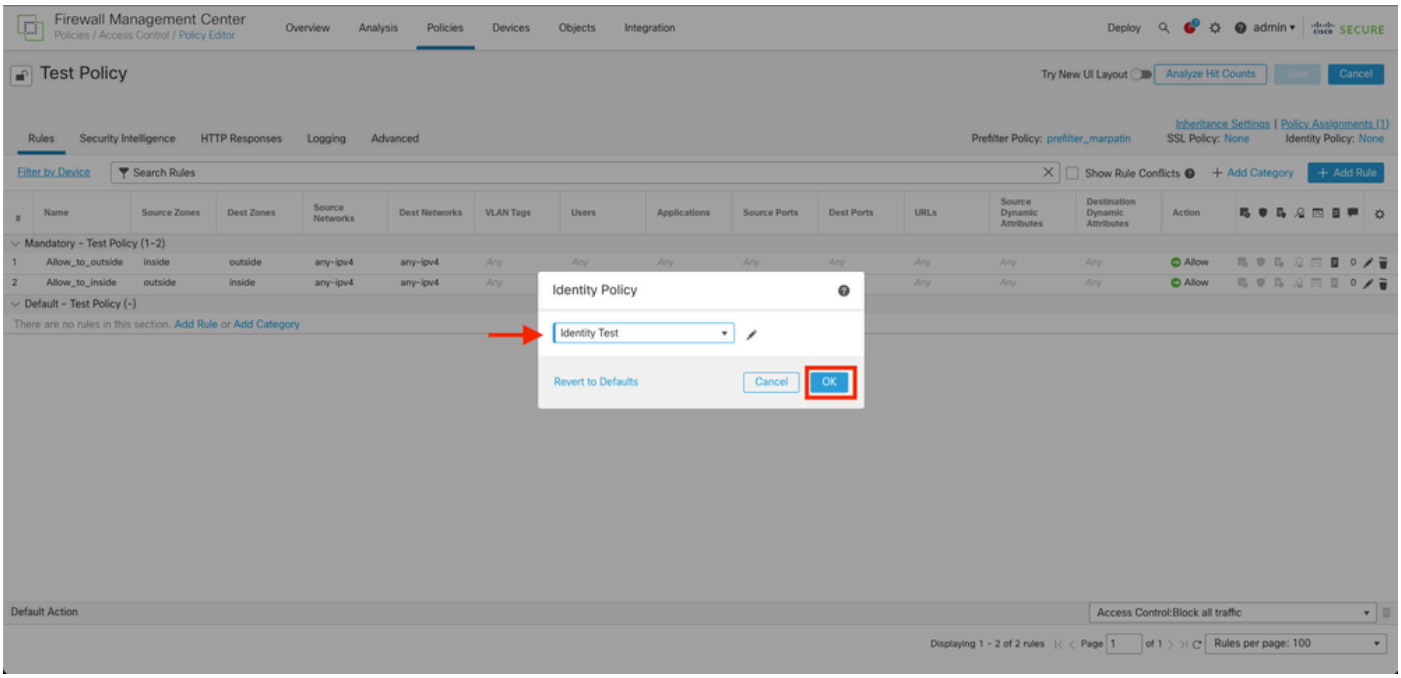
Étape 7. Identifiez la stratégie de contrôle d'accès qu'il va déployer dans le pare-feu traitant le trafic des utilisateurs et cliquez sur l'icône crayon afin de modifier la stratégie.



Étape 6. Cliquez sur None dans le champ Identity Policy.



Étape 7. Dans le menu déroulant, sélectionnez la politique créée précédemment à l'étape 3, puis cliquez sur OK pour terminer la configuration.

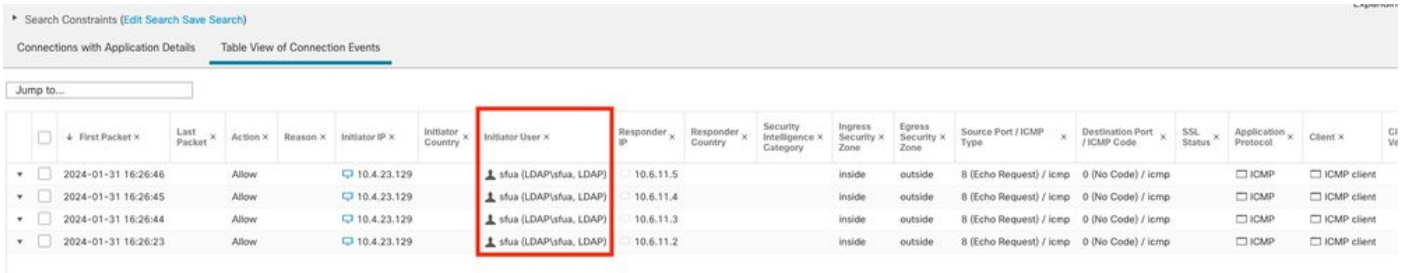


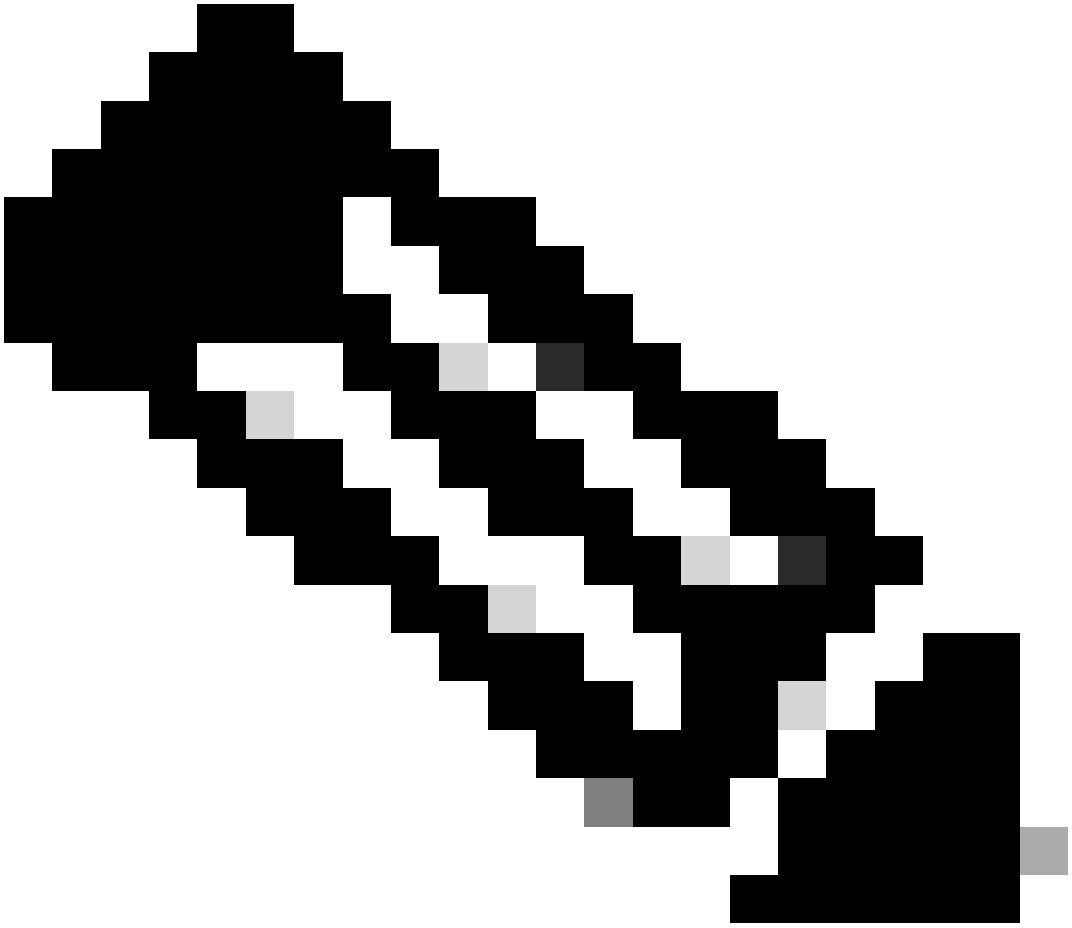
Étape 8 : enregistrement et déploiement de la configuration sur le FTD

Vérifier

1. Dans l'interface graphique FMC, accédez à Analysis > Users : Active Sessions

3. Validation à partir d'Analysis > Connection > Events : Tableau des événements Connections





Remarque : les utilisateurs correspondant aux critères de trafic de la politique d'identité et de la politique de contrôle d'accès affichent leur nom d'utilisateur dans le champ Utilisateur.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.