Secure Firewall Management Center(FMC)でのアイデンティティポリシーの設定

内容

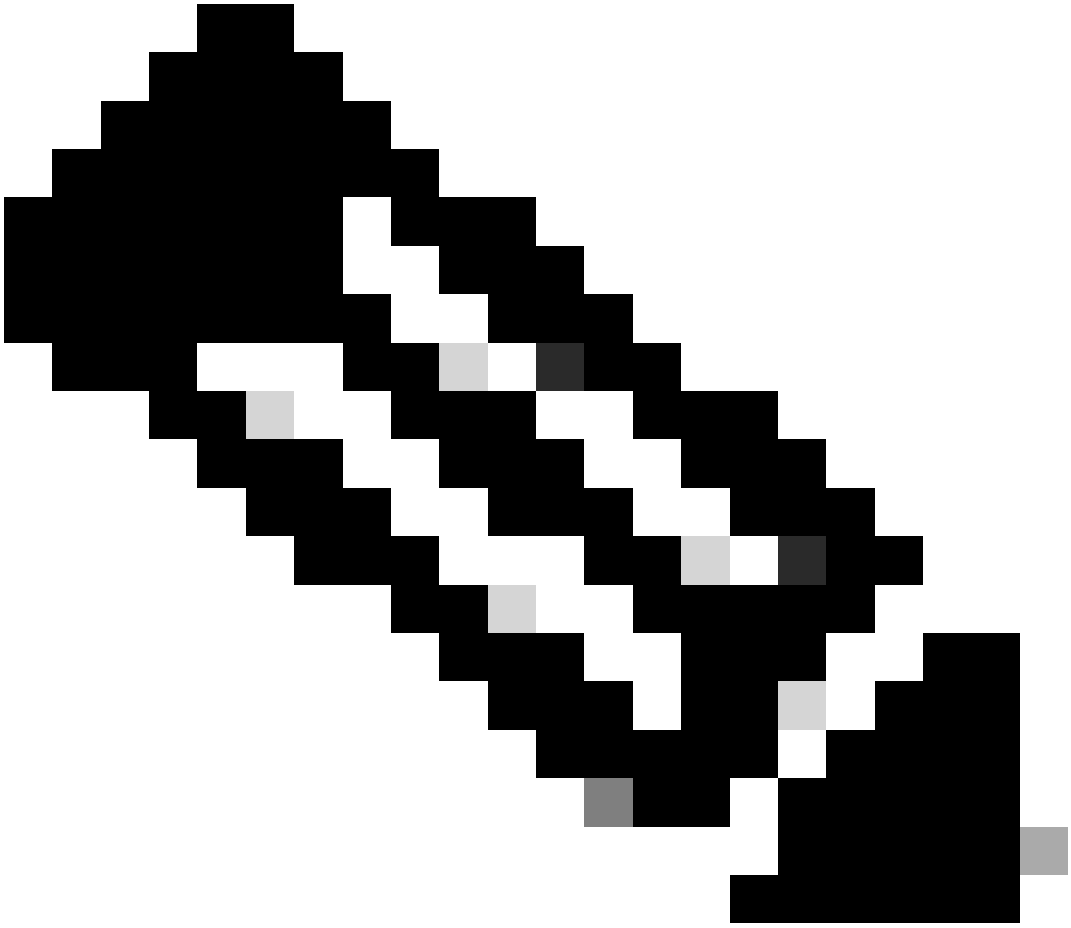
はじめに

このドキュメントでは、Secure FMCを介してSecure FTDトラフィックのアイデンティティポリシーを設定および展開する方法のプロセスについて説明します。

前提条件

1. FMCでレルムがすでに設定されている。

2. すでに設定されているアイデンティティ・ ソース：ISE、ISE-PIC



注:ISEおよびレルムの設定手順については、このドキュメントでは説明しません。

要件

次の項目に関する知識があることが推奨されます。

- セキュアファイアウォール管理センター(FMC)
- セキュアなファイアウォールスレッド防御(FTD)
- Cisco Identity Services Engine（ISE）
- LDAP/ADサーバ
- 認証方式

1. パッシブ認証：ISEなどの外部アイデンティティユーザソースの使用
2. アクティブ認証：認証元としての管理対象デバイスの使用（キャプティブポータルまたはリモートVPNアクセス）
3. 認証なし

使用するコンポーネント

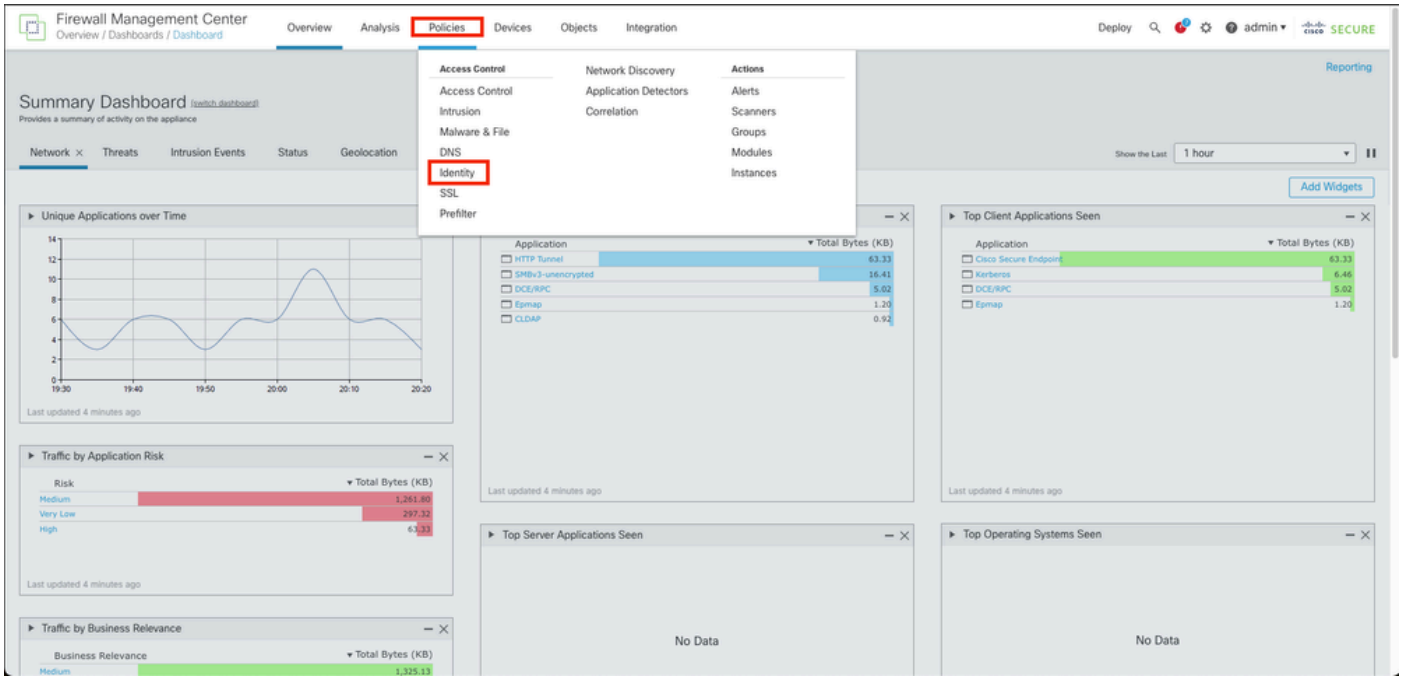
- VMWare v7.2.5向けセキュアファイアウォール管理センター
- VMWare v7.2.4向けシスコセキュアファイアウォール脅威対策
- Active Directory サーバ
- Cisco Identity Services Engine(ISE)v3.2パッチ4
- パッシブ認証方式

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

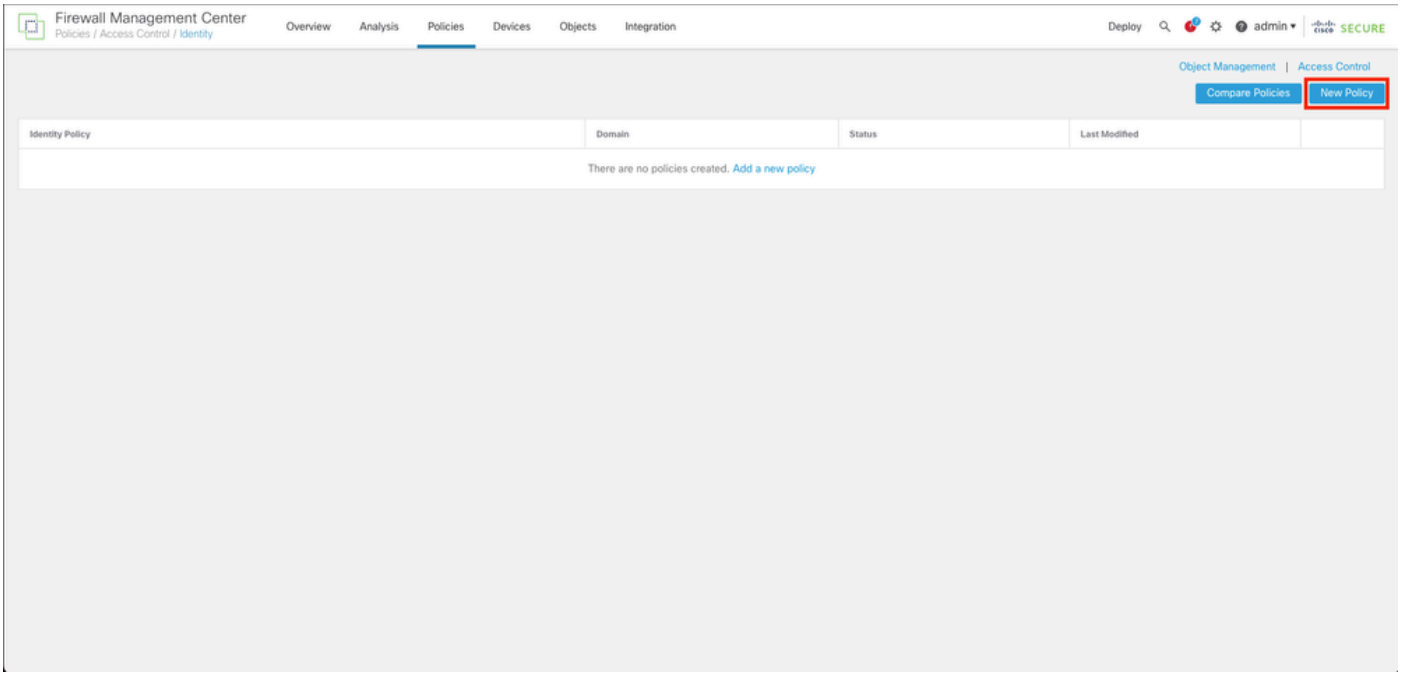
設定

コンフィギュレーション

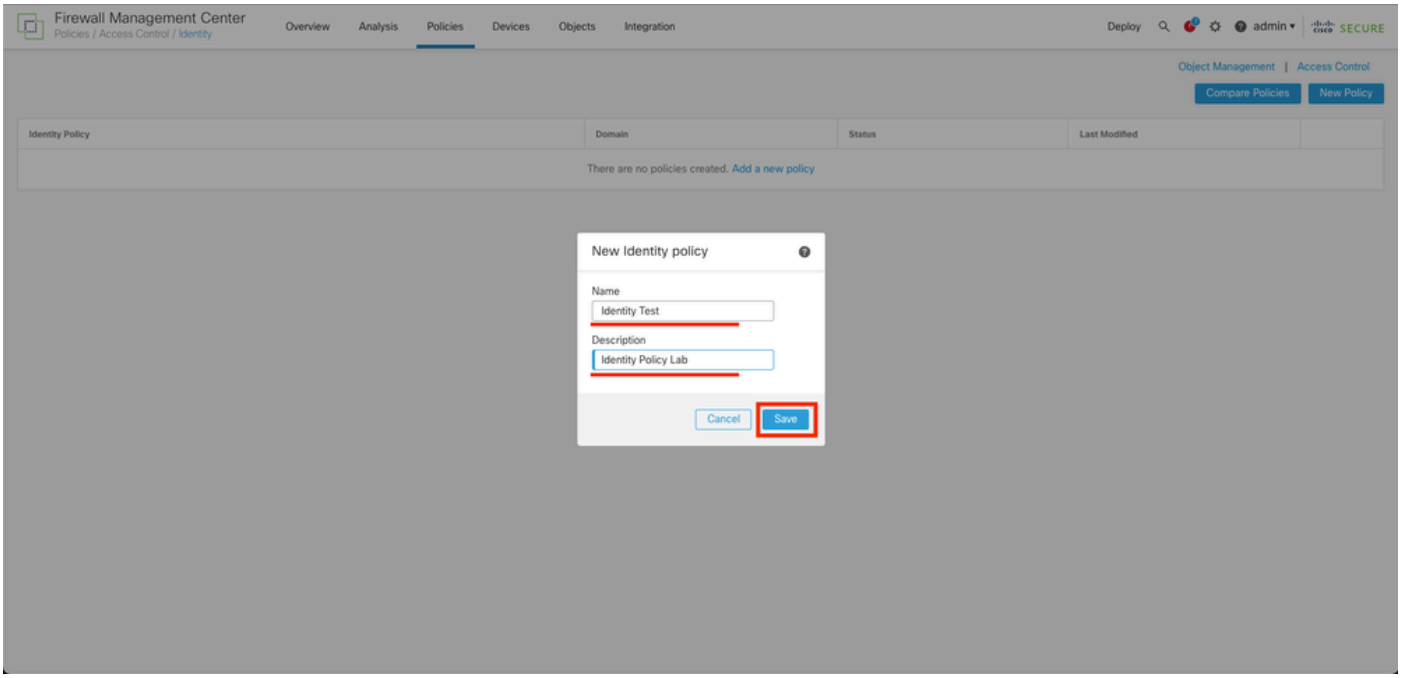
ステップ1:FMC GUIで、Policies > Access Control > Identityの順に移動します。



ステップ2:New Policyをクリックします。

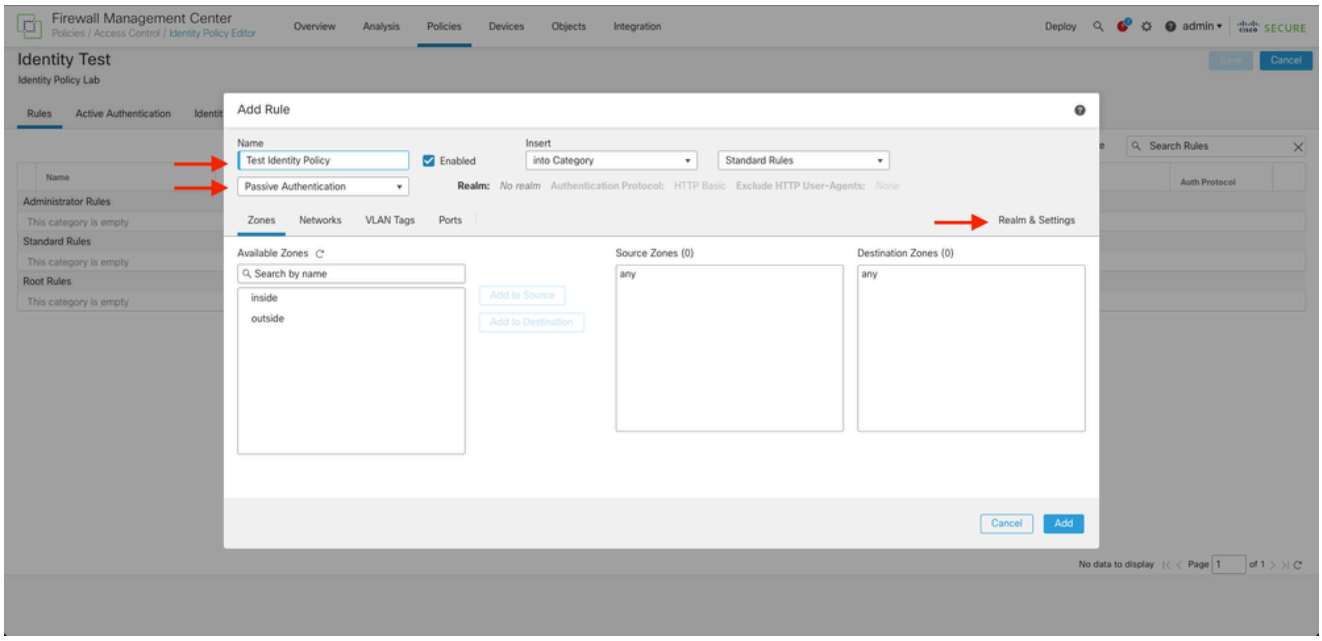


ステップ3:新しいアイデンティティポリシーに名前と説明を割り当ててから、保存をクリックします。

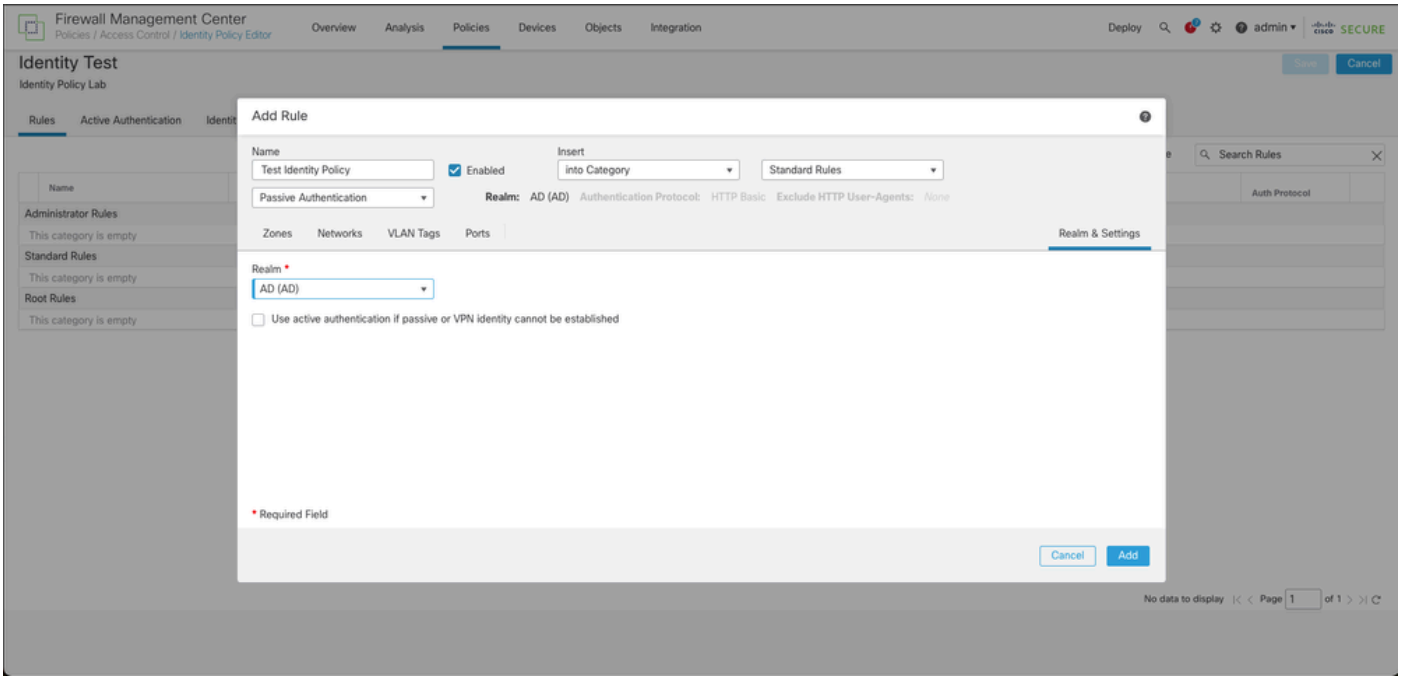


ステップ 4：+ Add Ruleアイコンをクリックします。

1. 新しいルールに名前を割り当てます。
2. nameフィールドで、認証方式を選択し、Passive Authenticationを選択します。
3. 画面の右側でRealm & Settingsを選択します。

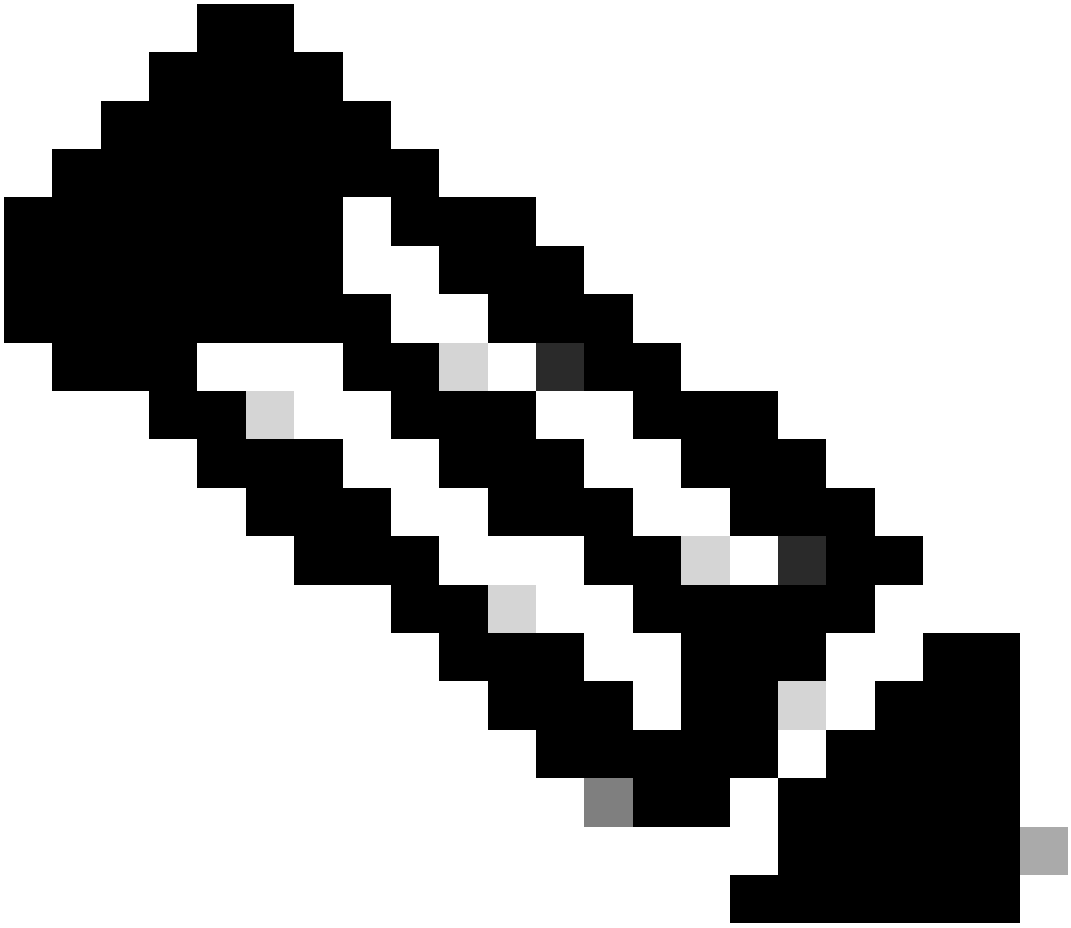


4. ドロップダウン・メニューからレルムを選択します。



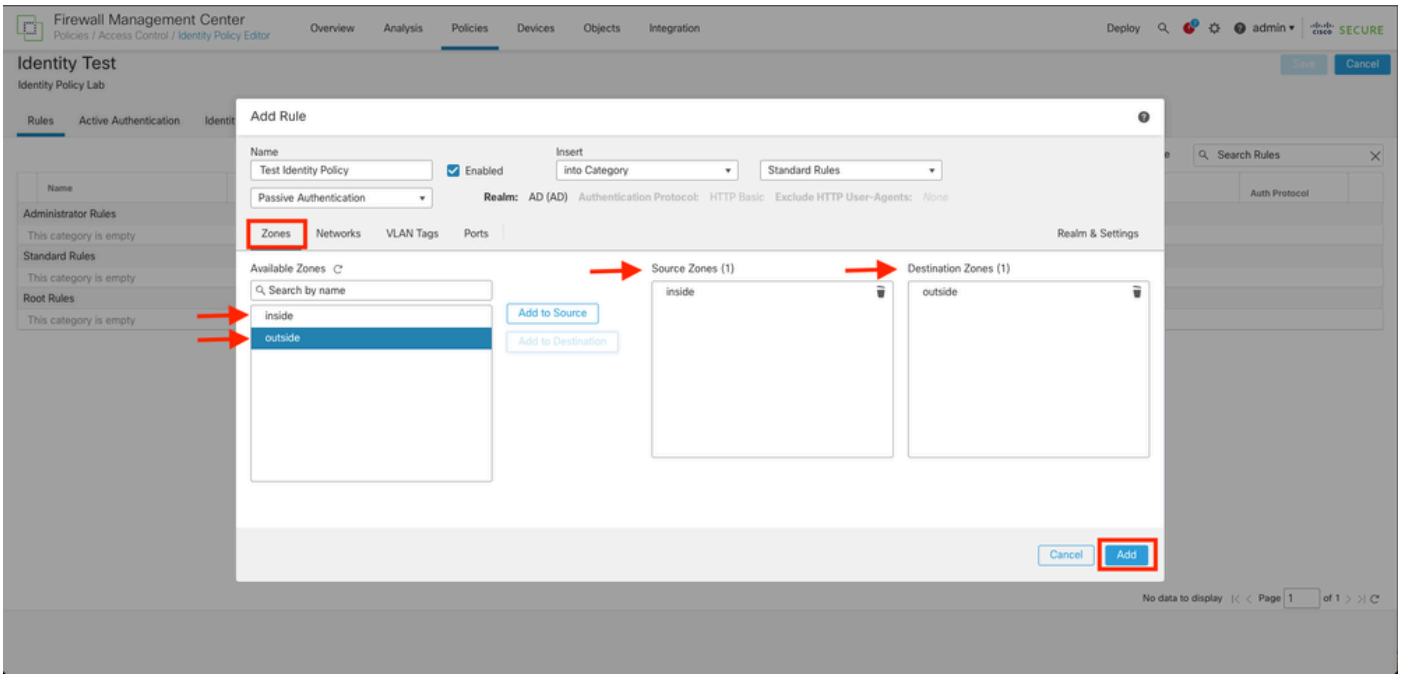
5. 画面の左側にあるZonesをクリックします。

6. [Avaliable Zones]メニューから、ユーザの検出に必要なトラフィックパスに基づいてsourceゾーンとdestinationゾーンを割り当てます。ゾーンを追加するには、ゾーンの名前をクリックし、Add to SourceまたはAdd to Destinationの場合に応じて選択します。

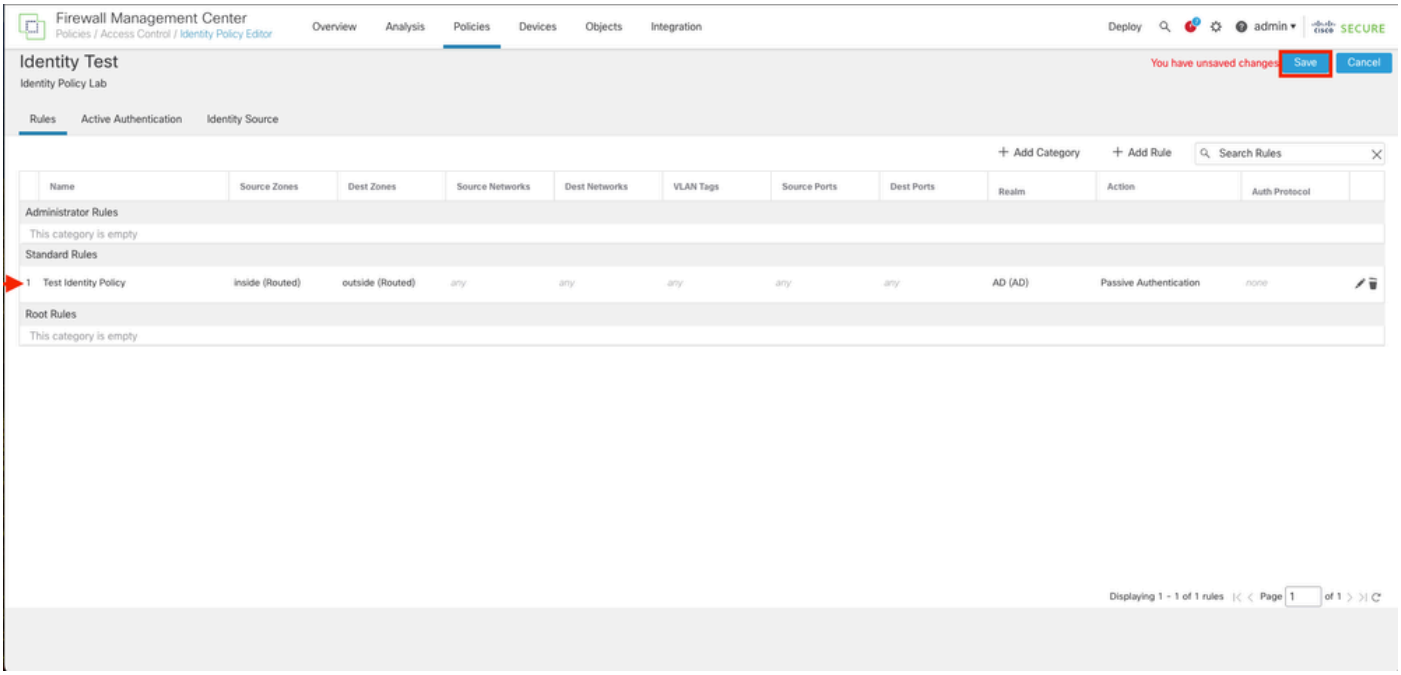


注：このドキュメントでは、ユーザ検出は内部ゾーンからのトラフィックのみに適用され、外部ゾーンに転送されます。

7. AddおよびSaveを選択します。

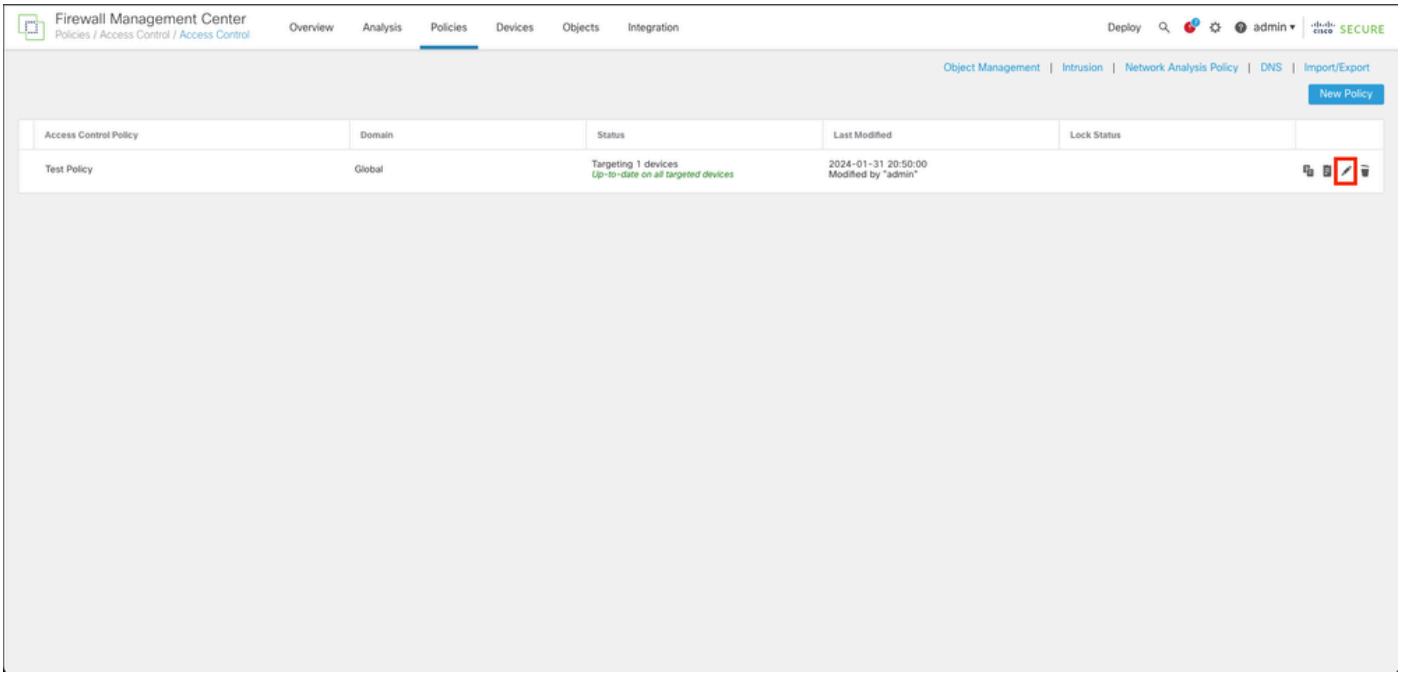


ステップ 5：新しいルールがアイデンティティポリシーに含まれていることを確認し、「保存」をクリックします。

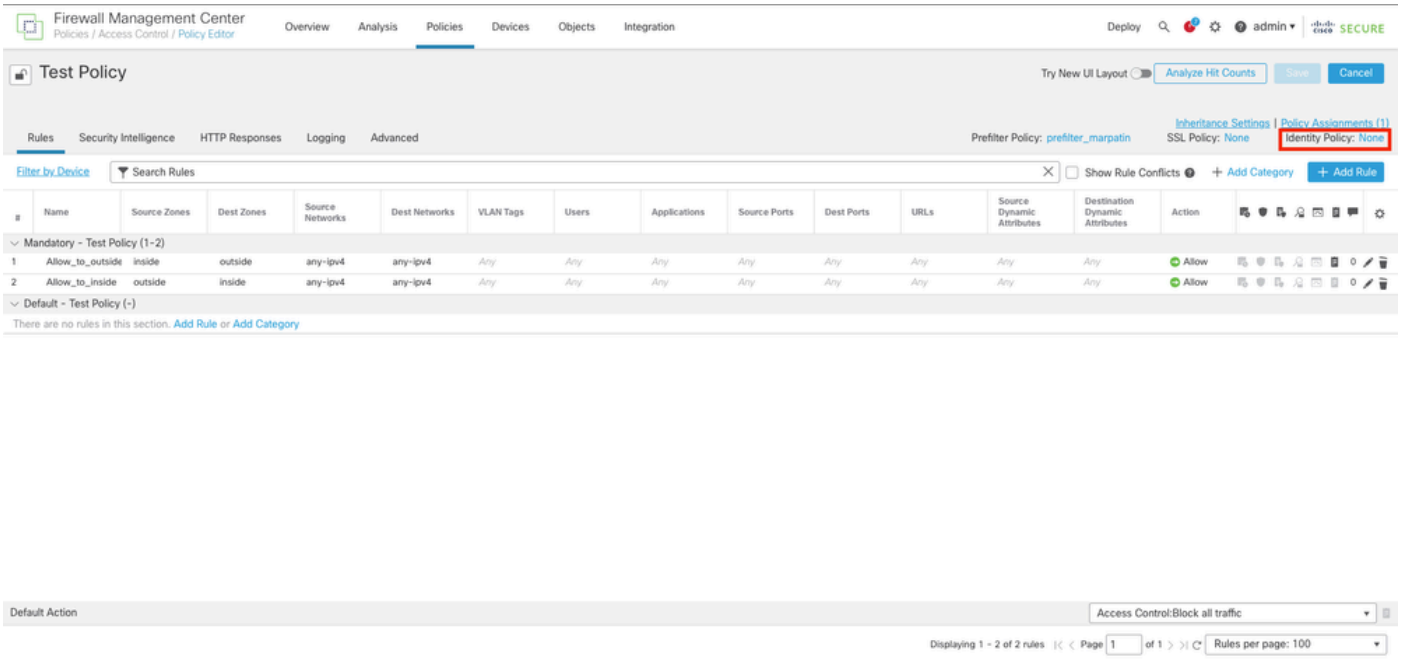


手順 6： Policies > Access Controlの順に移動します。

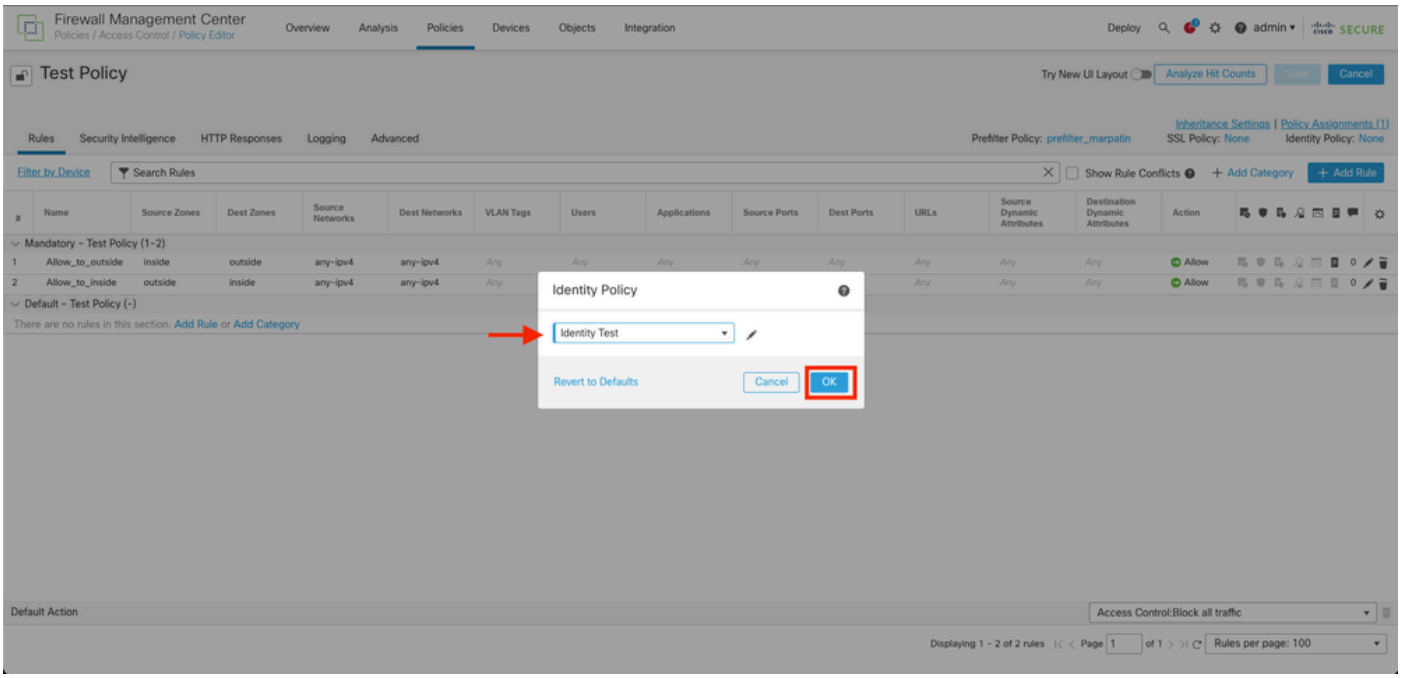
手順 7：ユーザトラフィックを処理するファイアウォールに導入されるアクセスコントロールポリシーを特定し、鉛筆アイコンをクリックして、ポリシーを編集します。



手順 6： Identity PolicyフィールドでNoneをクリックします。



手順 7：ドロップダウンメニューから、ステップ3で作成したポリシーを選択し、OKをクリックして設定を終了します。

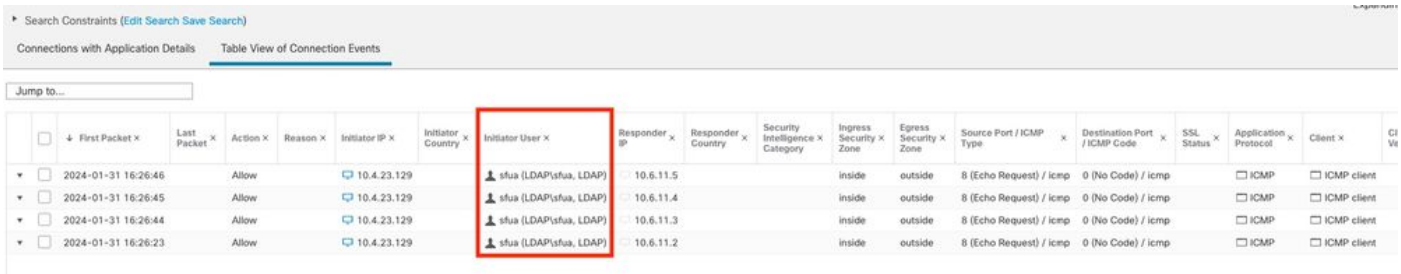


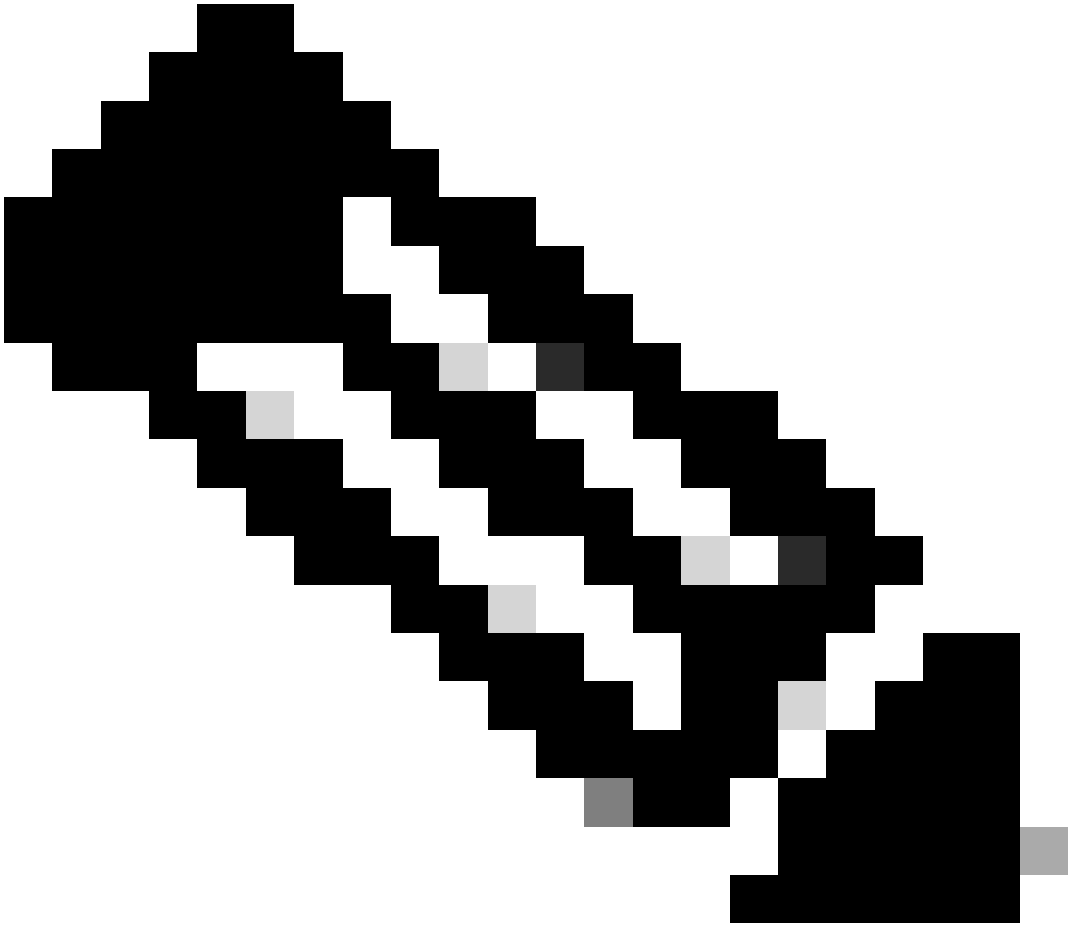
ステップ8：設定を保存し、FTDに展開します。

確認

1. FMC GUIで、[分析] > [ユーザ：アクティブセッション] に移動します。

3. 「分析」 > 「接続」 > 「イベント：接続イベントの表ビュー」の順に選択します。





注：アイデンティティポリシーおよびアクセスコントロールポリシーのトラフィック基準に一致するユーザは、そのユーザ名がUserフィールドに表示されます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。