Identiteitsbeleid configureren voor Secure Firewall Management Center (FMC)

Inhoud

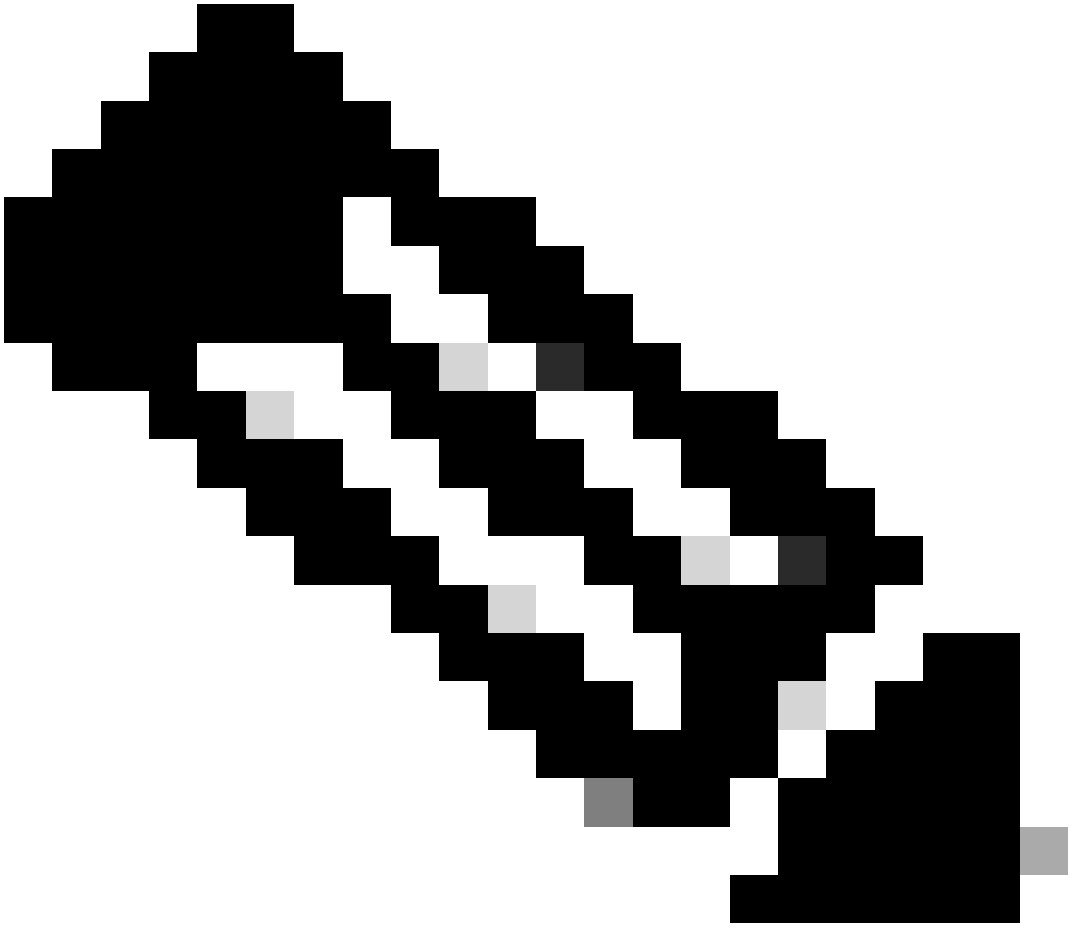
Inleiding

Dit document beschrijft het proces voor het configureren en implementeren van een identiteitsbeleid voor een beveiligd FTD-verkeer via een beveiligd FMC.

Voorwaarden

1. Realm al geconfigureerd in VCC.

2. Identiteitsbron reeds geconfigureerd - ISE, ISE-PIC.



Opmerking: instructies voor ISE- en Real-configuraties vallen buiten het bereik van dit document.

Vereisten

Cisco raadt aan kennis van deze onderwerpen te hebben:

- Secure Firewall Management Center (FMC)
- Secure Firewall Thread Defence (FTD)
- Cisco Identity Services Engine (ISE)
- LDAP/AD-servers
- Verificatiemethoden

1. Passieve verificatie: gebruik van externe identiteitsgebruikersbron zoals ISE
2. Actieve verificatie: gebruik van het beheerde apparaat als verificatiebron (captive portal of externe VPN-toegang)

3. Geen verificatie

Gebruikte componenten

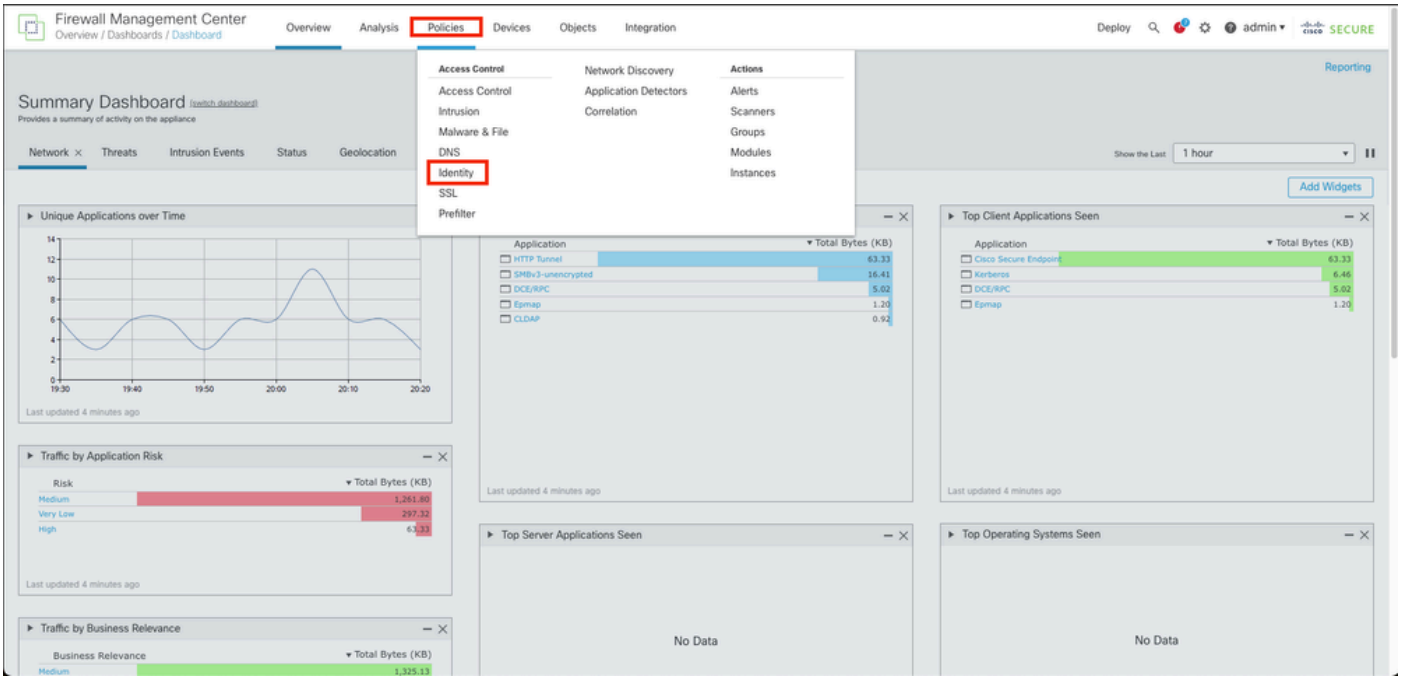
- Secure Firewall Management Center voor VMWare v7.2.5
- Cisco Secure Firewall Threat Defence voor VMWare v7.2.4
- Active Directory-server
- Cisco Identity Services Engine (ISE) v3.2-patch 4
- Passieve verificatiemethode

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

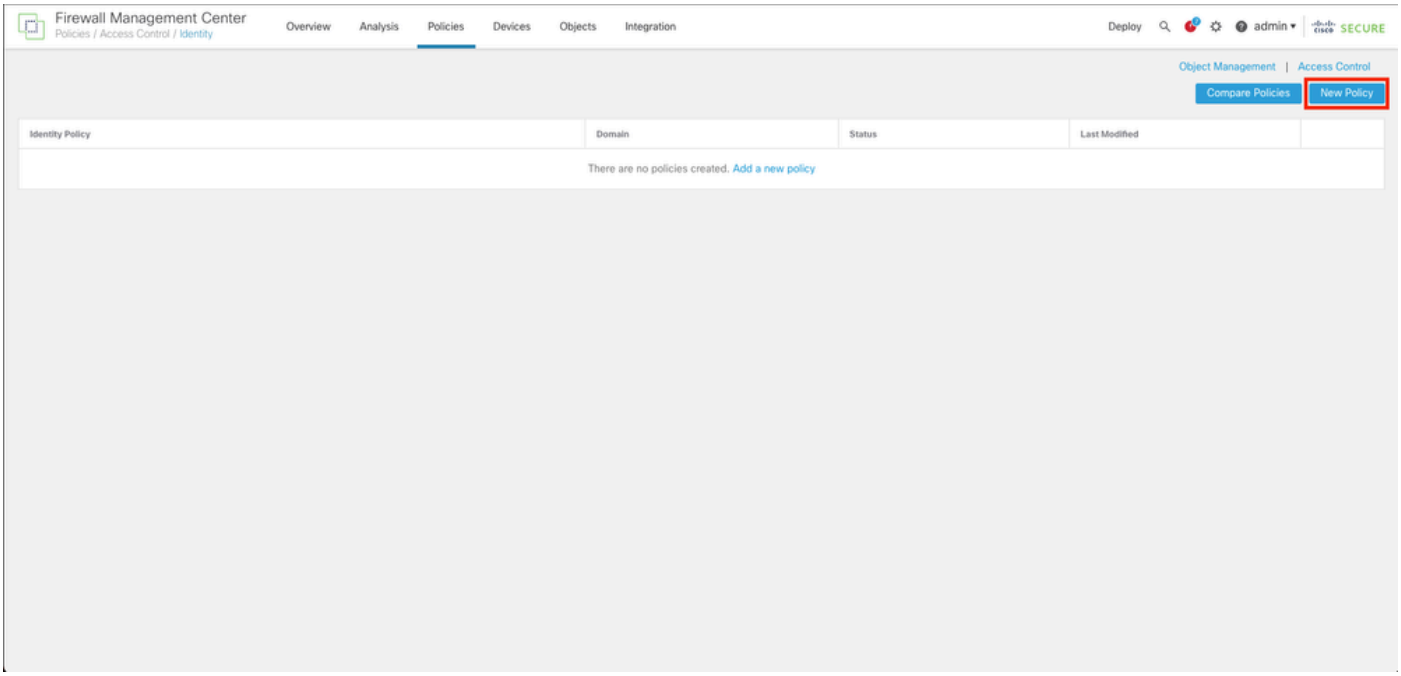
Configureren

Configuraties

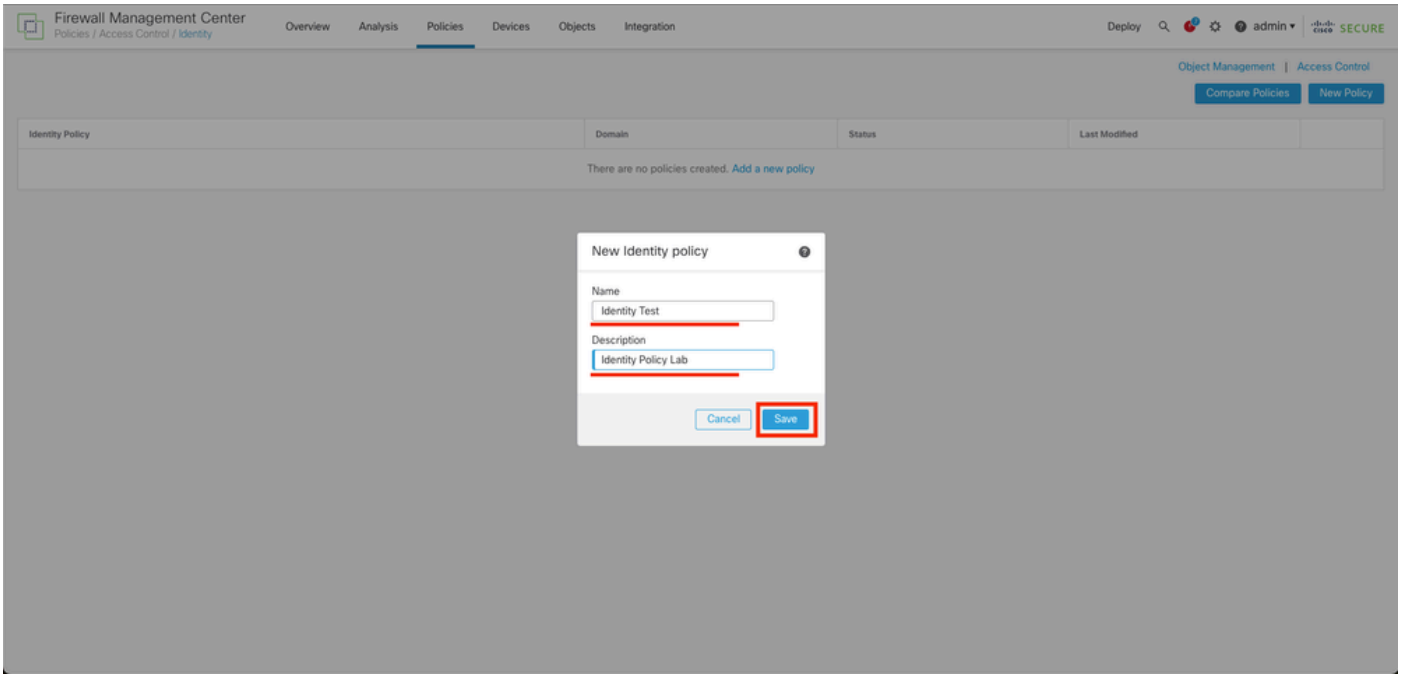
Stap 1.Ga in de FMC GUI naar Policy > Access Control > Identity



Stap 2. Klik op Nieuw beleid.

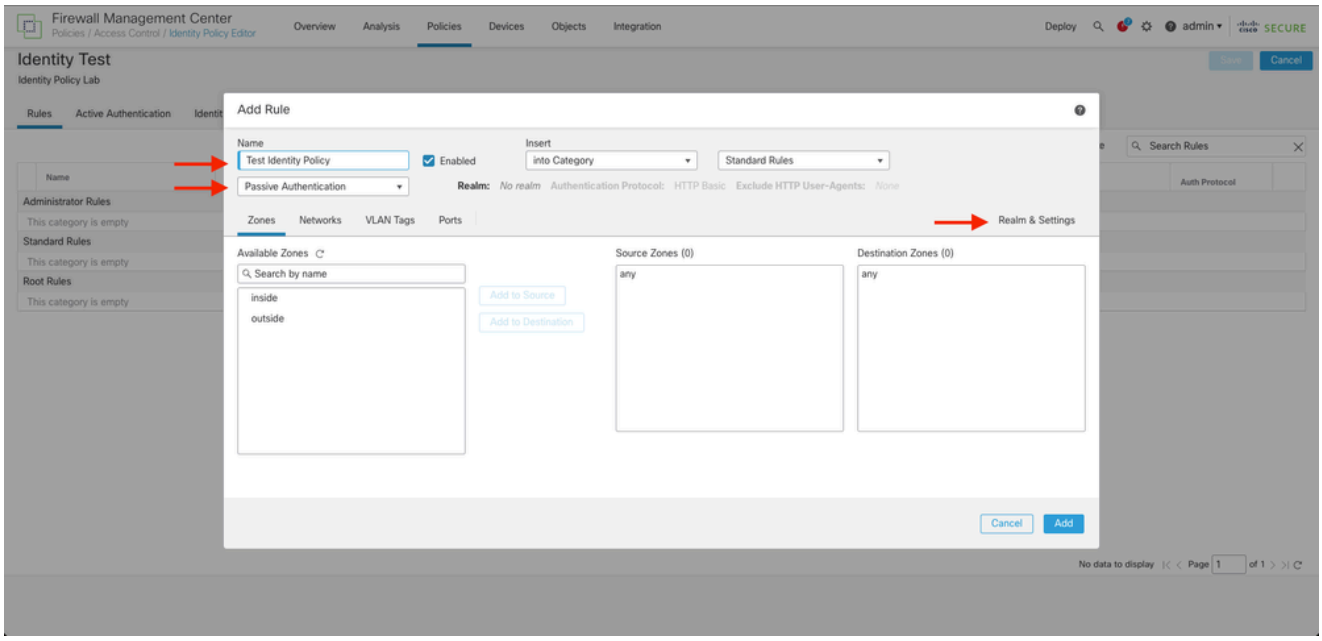


Stap 3. Wijs een naam en een beschrijving toe aan het nieuwe identiteitsbeleid en klik vervolgens op Opslaan.

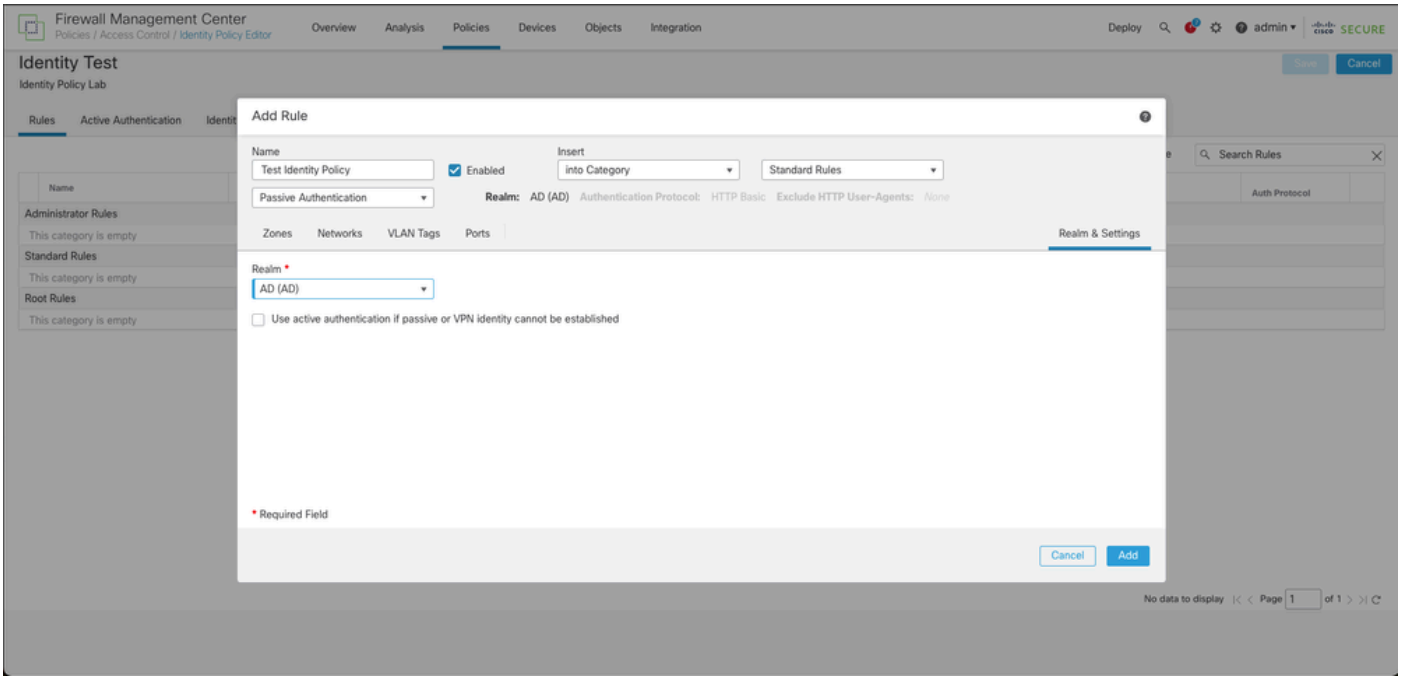


Stap 4. Klik op het pictogram + Regel toevoegen.

1. Wijs een naam toe aan de nieuwe regel.
2. Kies onder het veld Naam de verificatiemethode en selecteer: Passieve verificatie.
3. Selecteer Rechts van het scherm Realm & Settings.

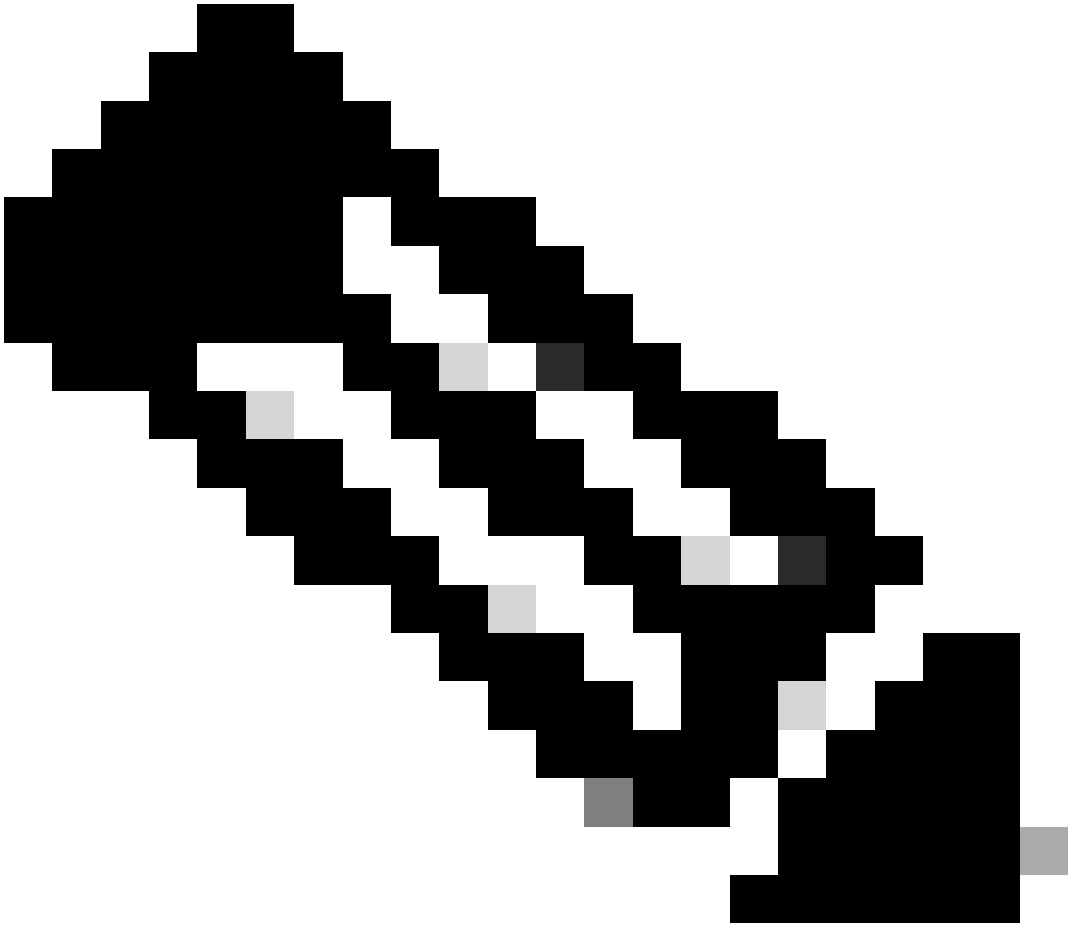


4. Selecteer een domein in het uitrolmenu.



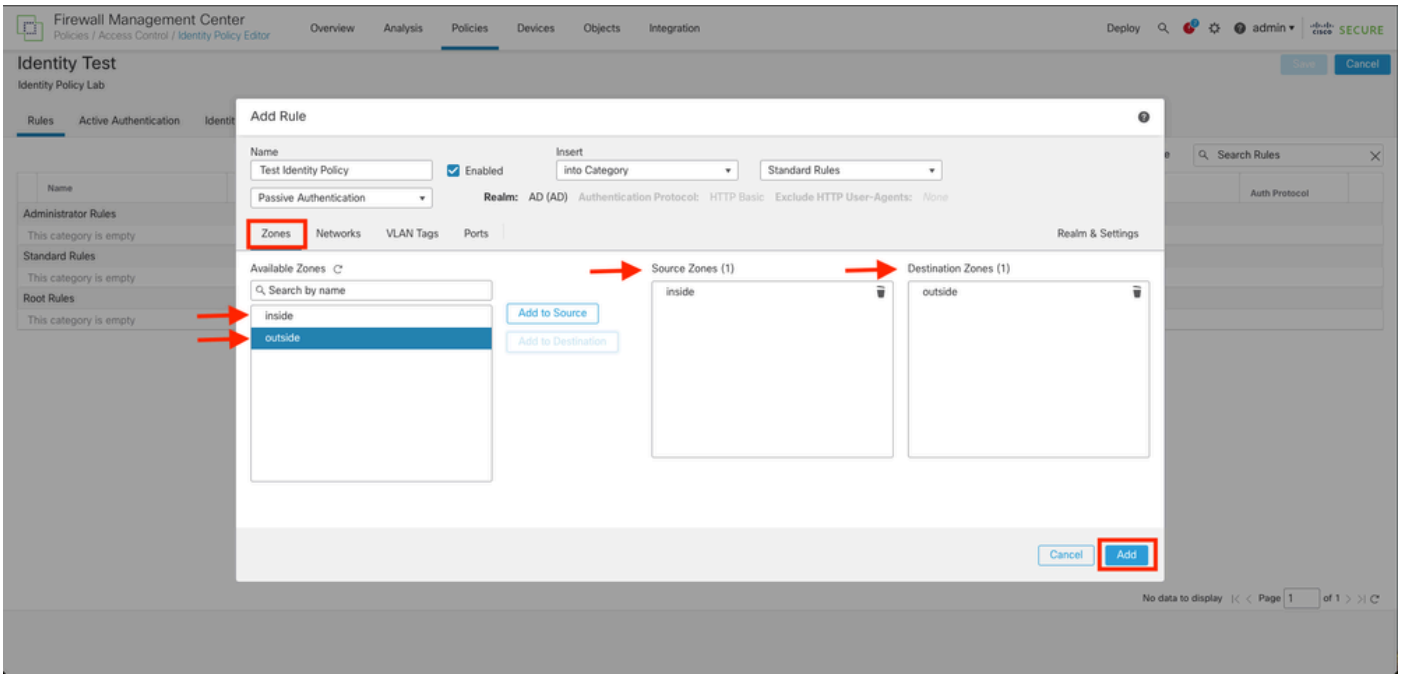
5. Klik op Zones links op het scherm.

6. Wijs in het menu Beschikbare zones een bron- en doelzone toe op basis van het verkeerspad dat nodig is om gebruikers te detecteren. Als u een zone wilt toevoegen, klikt u op de naam van de zone en selecteert u afhankelijk van de case Toevoegen aan bron of Toevoegen aan bestemming.

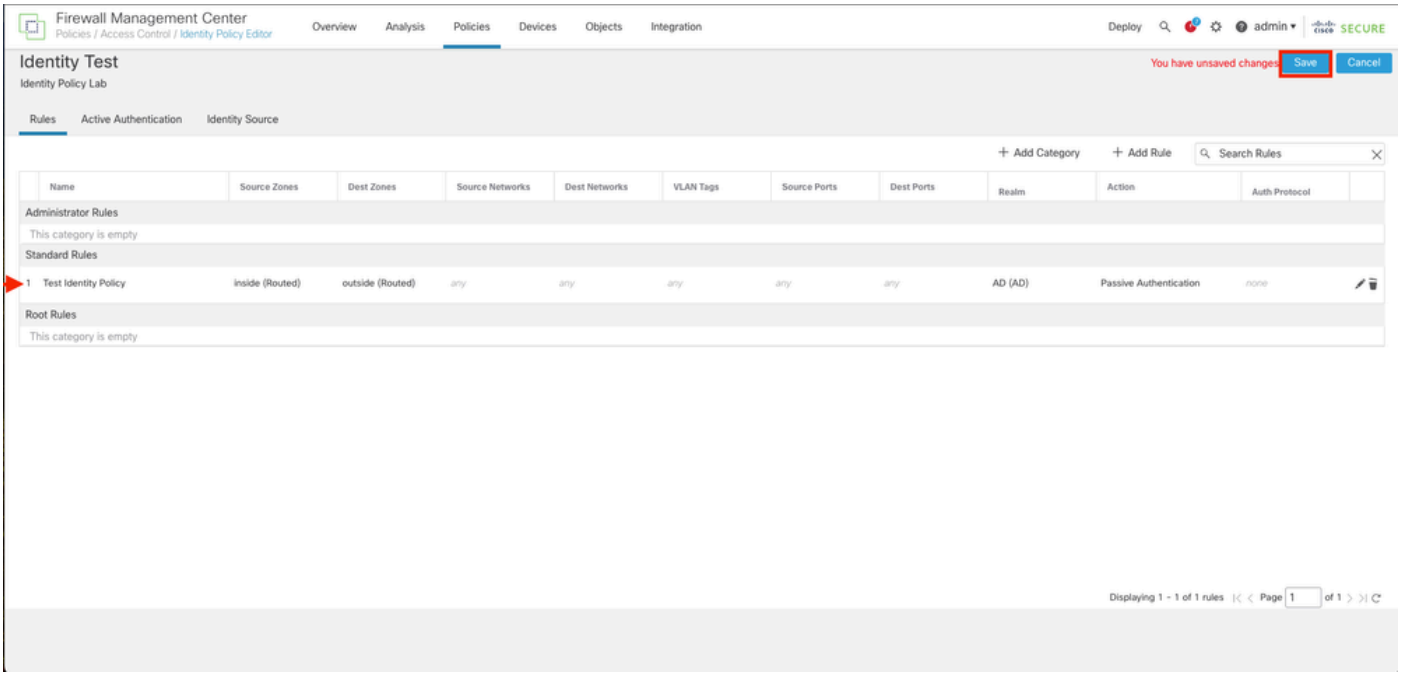


Opmerking: in deze documentatie wordt de gebruikersdetectie alleen toegepast voor het verkeer komt van de binnenzone en wordt doorgestuurd naar de buitenzone.

7. Selecteer Add en Save.

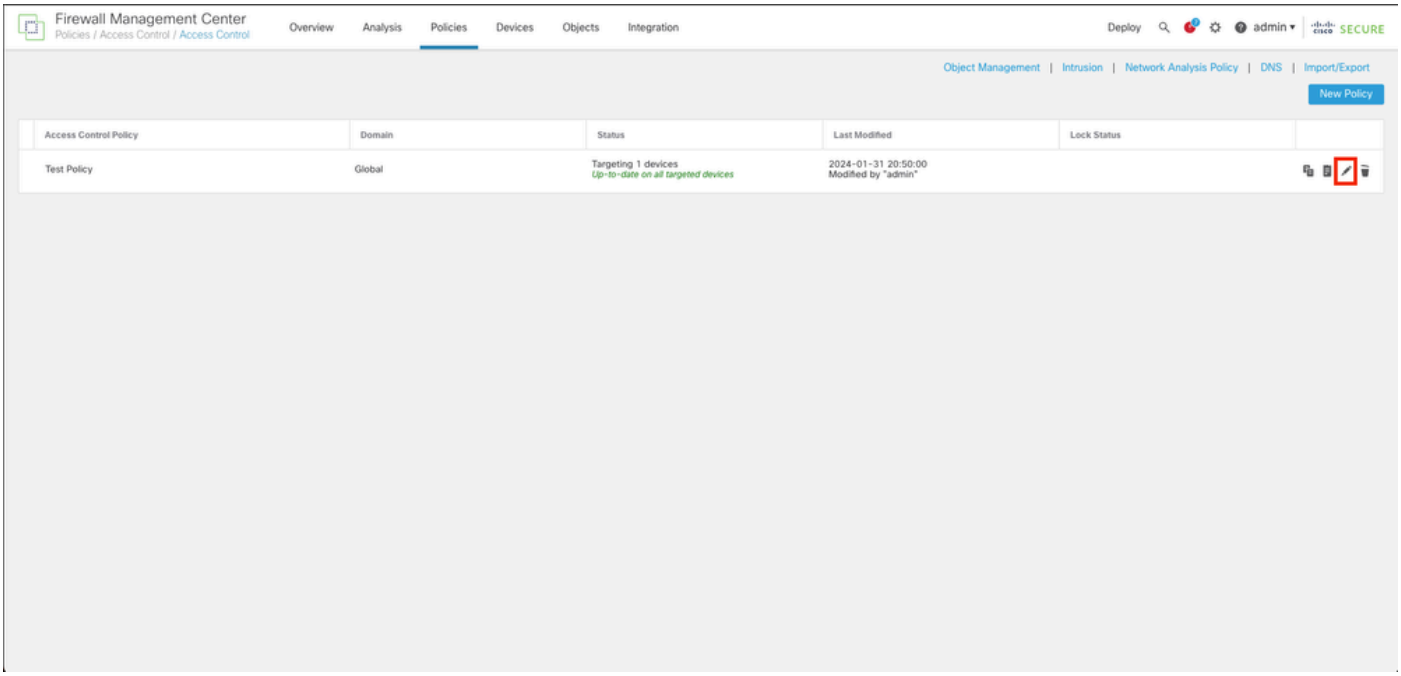


Stap 5. Controleer of de nieuwe regel in het identiteitsbeleid staat en klik op Opslaan.

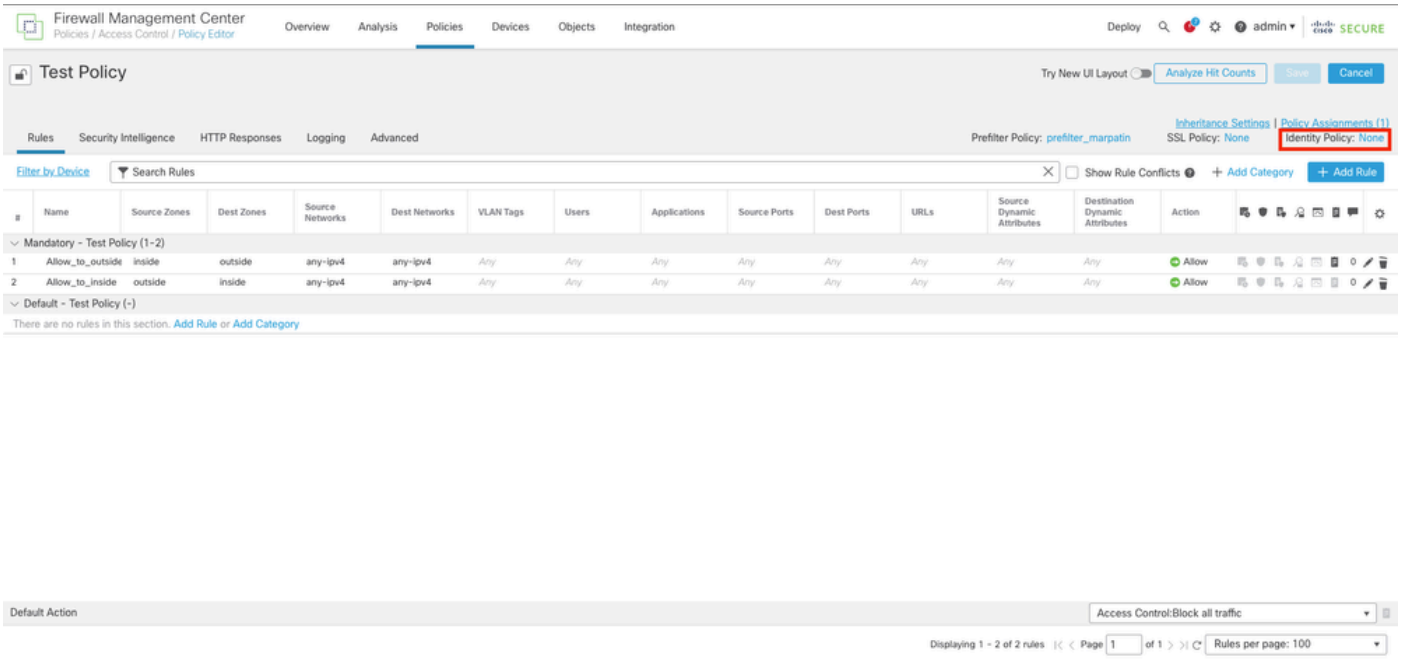


Stap 6. Naar beleid > Toegangsbeheer navigeren

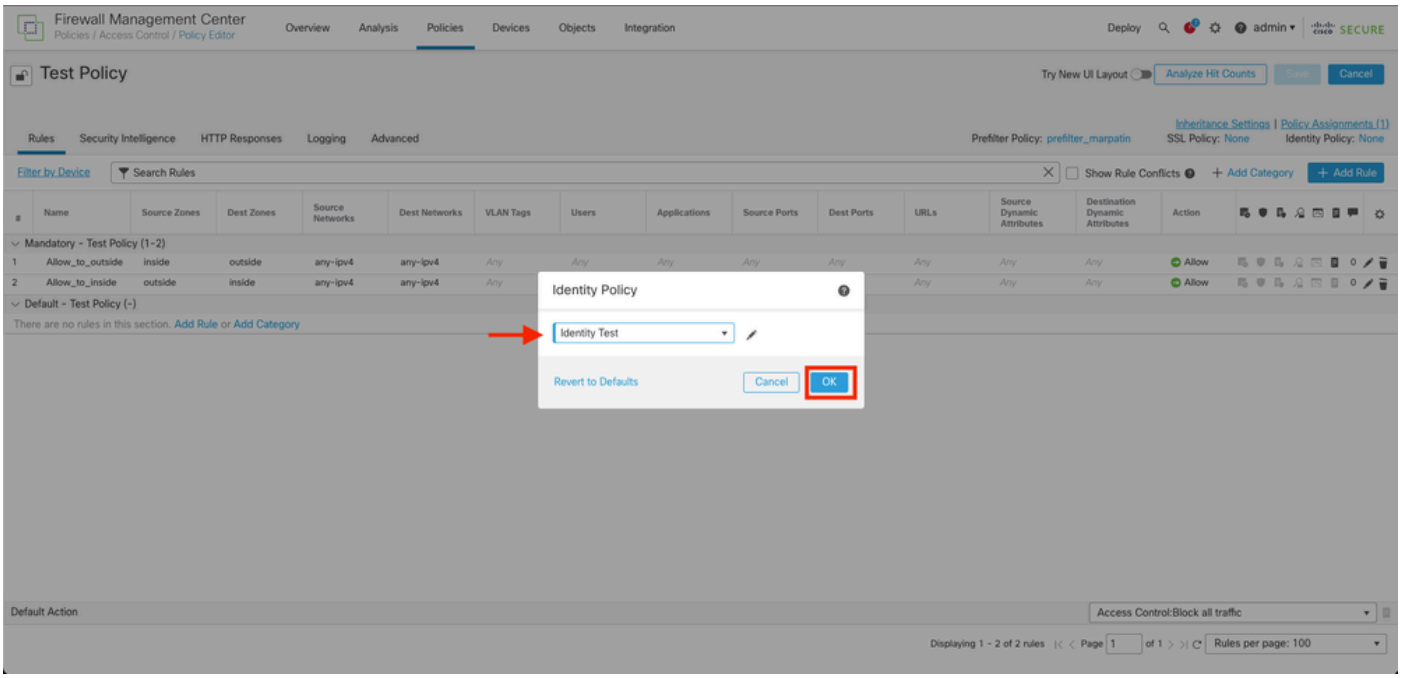
Stap 7. Identificeer het Toegangsbeheerbeleid dat in de Firewall zal worden geïmplementeerd die het gebruikersverkeer verwerkt en klik op het potlood-pictogram om het beleid te bewerken.



Stap 6. Klik op Geen in het veld Identity Policy.



Stap 7. Selecteer in het vervolgkeuzemenu het beleid dat eerder in stap 3 is gemaakt en klik vervolgens op OK om de configuratie te voltooien.

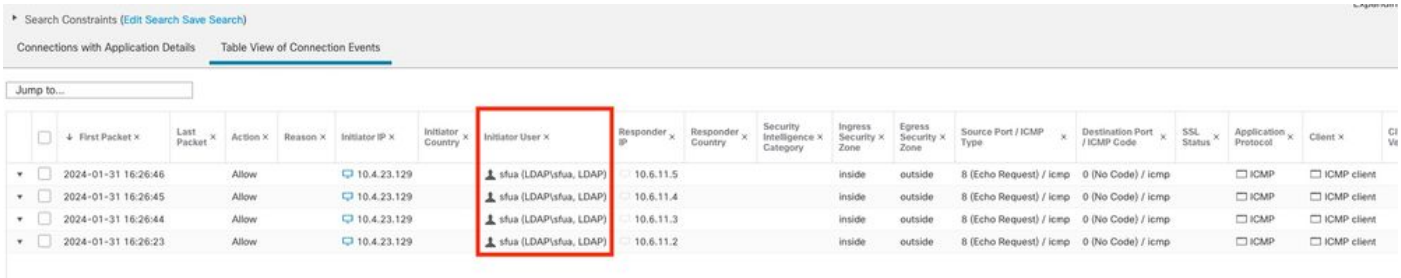


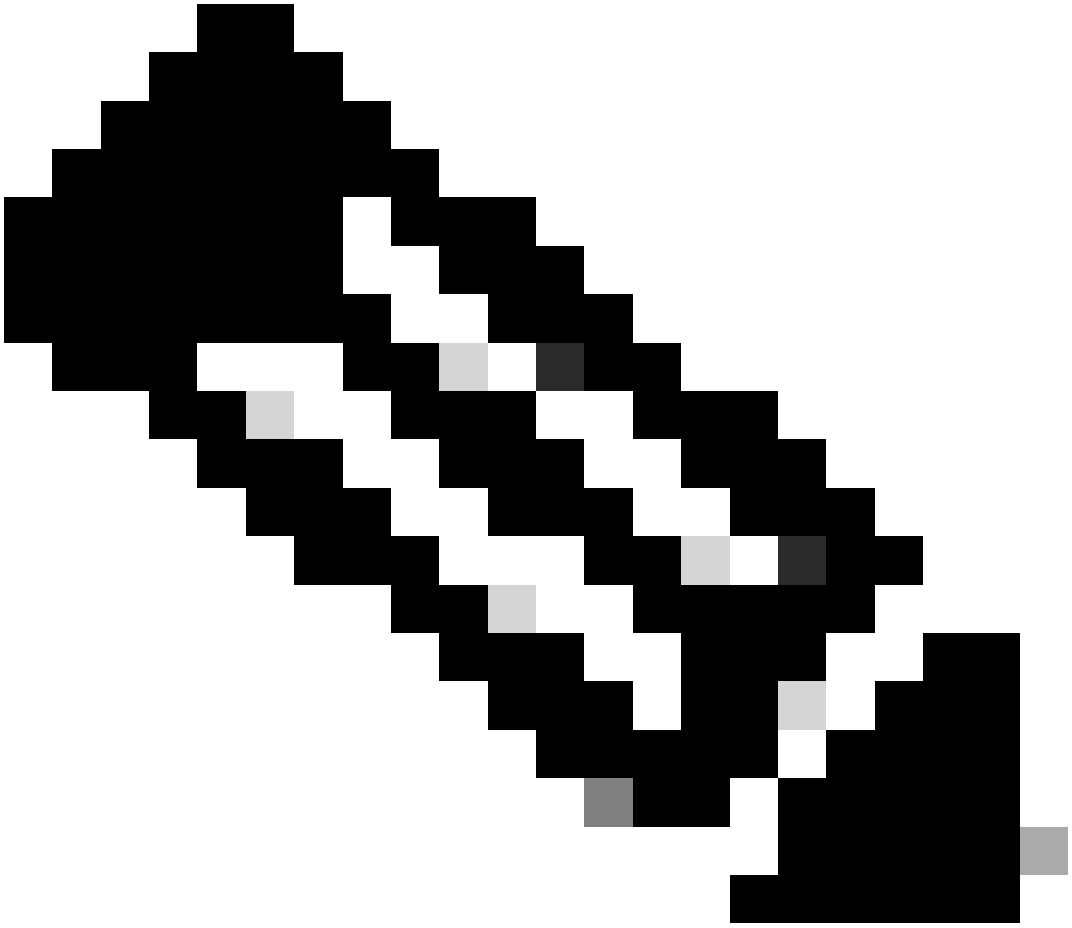
Stap 8. Opslaan en implementeren van de configuratie in de FTD.

Verifiëren

1. In de FMC GUI navigeren naar Analysis > Gebruikers: Actieve sessies

3. Validering van analyse > verbinding> Evenementen: Tabelweergave van Connecties gebeurtenissen





Opmerking: Gebruikers die voldoen aan de verkeerscriteria voor het identiteitsbeleid en het toegangscontrolebeleid, krijgen hun gebruikersnaam in het veld Gebruiker te zien.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.