& Active Directory-integratie configureren met FirePOWER-applicatie voor Single-Sign-On Captive Portal Verification

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Achtergrondinformatie
Configureren
Stap 1. De Firepower User Agent configureren voor eenmalige aanmelding
Stap 2. Het Firepower Management Center (FMC) integreren met User Agent
Stap 3. Integreer Firepower met Active Directory
Stap 3.1 Maak het rijk
Stap 3.2 Voeg de Directory Server toe
Stap 3.3 Wijzig de gebiedsconfiguratie
Stap 3.4 Downloaden Gebruikersdatabase
Stap 4. Het identiteitsbeleid configureren
Stap 4.1 Captive Portal (actieve verificatie)
Stap 4.2 Enkelvoudige aanmelding (passieve verificatie)
Stap 5. Het toegangscontrolebeleid configureren
Stap 6. Het toegangscontrolebeleid implementeren
Stap 7. Gebruikersgebeurtenissen en verbindingen bewaken
Verifiëren en probleemoplossing
Controleer de connectiviteit tussen VCC en User Agent (passieve verificatie)
Controleer de connectiviteit tussen VCC en Active Directory
Controleer de connectiviteit tussen Firepower Sensor en het eindsysteem (actieve verificatie)
Controleer de beleidsconfiguratie en -implementatie
De logboeken van de gebeurtenissen analyseren
Gerelateerde informatie

Inleiding

In dit document wordt de configuratie beschreven van Captive Portal Authentication (Actieve verificatie) en Single-Sign-On (Passieve verificatie).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Sourcefire-apparaten voor firewalls
- Modellen voor virtuele apparaten
- Lichtgewicht Directory Service (LDAP)
- Firepower User Agent

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center (FMC) versie 6.0.0 en hoger
- Firepower sensor versie 6.0.0 en hoger

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.

Achtergrondinformatie

Captive Portal Verification of Active Verification vraagt om een inlogpagina en gebruikersreferenties zijn vereist voor een host om de internettoegang te krijgen.

Single-Sign-On of Passive Verification biedt een gebruiker naadloze authenticatie voor netwerkbronnen en internettoegang zonder meerdere gebruikersreferenties. De Single-Sign-on verificatie kan worden bereikt door Firepower user agent of NTLM browser authenticatie.

Opmerking: voor Captive Portal-verificatie moet het apparaat in de routeringsmodus staan.

Configureren

Stap 1. De Firepower User Agent configureren voor eenmalige aanmelding

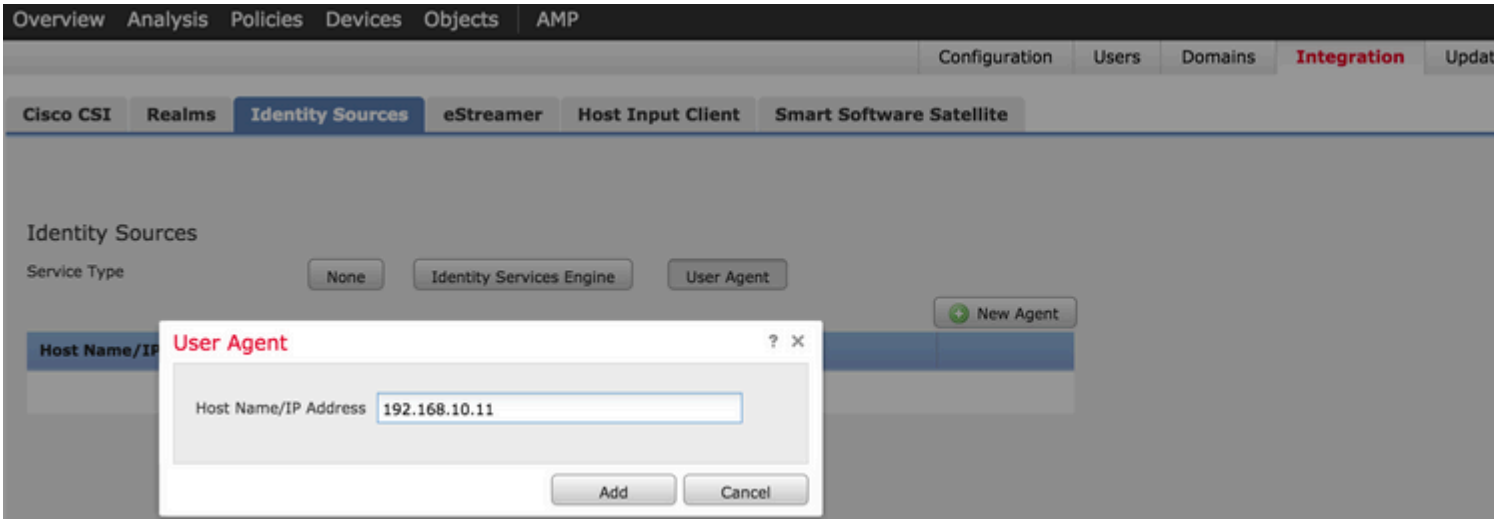
In dit artikel wordt uitgelegd hoe u Firepower User Agent kunt configureren in een Windows-machine:

Installatie en verwijdering van Sourcefire User Agent

Stap 2. Het Firepower Management Center (FMC) integreren met User Agent

Log in bij Firepower Management Center, navigeer naar **Systeem > Integratie > Identity Sources.** Klik op de optie **New Agent**. Configureer het IP-adres van het User Agent-systeem en klik op de knop **Toevoegen**.

Klik op de knop **Opslaan** om de wijzigingen op te slaan.



Stap 3. Integreer Firepower met Active Directory

Stap 3.1 Maak het rijk

Log in bij het VCC, navigeer naar **Systeem > Integratie > Realm.** Klik op de optie **Nieuw gebied toevoegen**.

Naam & Beschrijving: Geef een naam/beschrijving om het domein uniek te identificeren.

Type: AD

AD Primary Domain: Domeinnaam van Active Directory

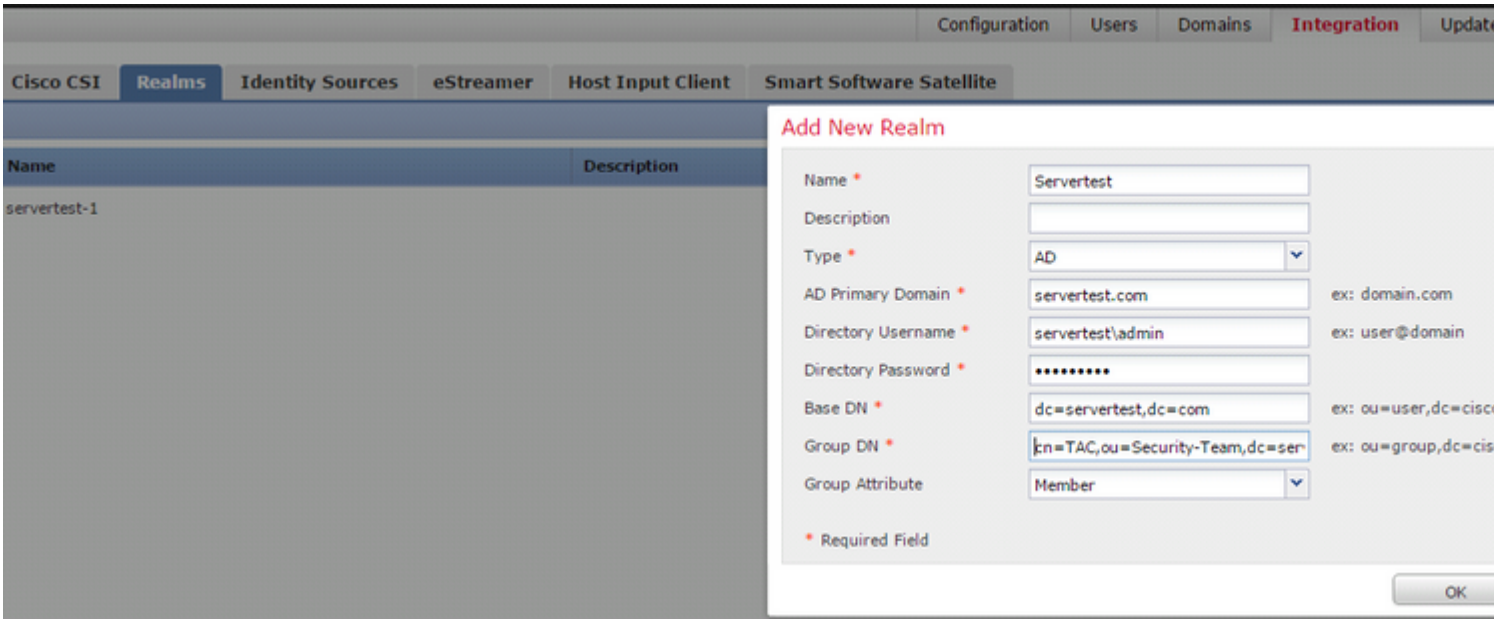
Gebruikersnaam: <gebruikersnaam>

Directory Wachtwoord: <password>

Base-DN: Domain of Specific OU DN waar het systeem een zoekactie start in de LDAP-database.

Groep DN: groep DN

Groepskenmerk: Member



Dit artikel helpt u om de waarden van de Basis DN en van de Groep DN te ontdekken.

[Identificeer actieve Directory LDAP-objectkenmerken]

Stap 3.2 Voeg de Directory Server toe

Klik op de knop **Toevoegen** om naar de volgende stap te gaan en klik vervolgens op de optie **Map toevoegen**.

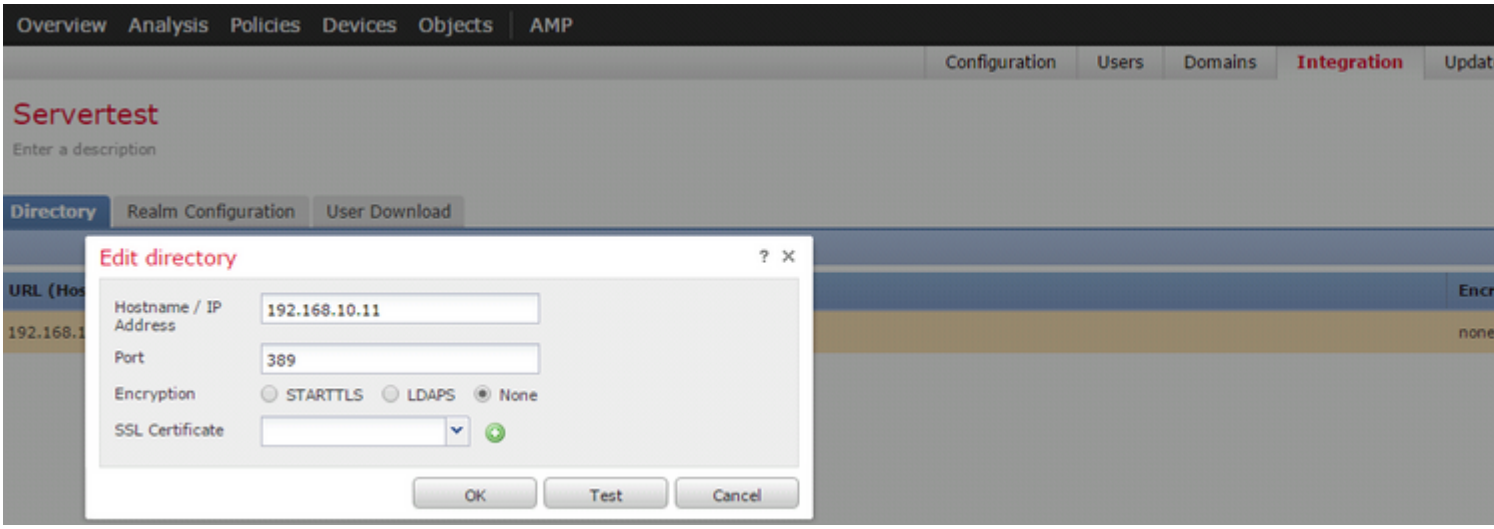
Hostnaam/IP-adres: configureer het IP-adres/hostnaam van de AD-server.

Poort: 389 (Active Directory LDAP-poortnummer)

Versleuteling/SSL-certificaat: (optioneel) Raadpleeg voor het versleutelen van de verbinding tussen FMC-

en AD-server het volgende

artikel: **Verificatie van verificatieobject op FireSIGHT-systeem voor Microsoft AD-verificatie via SSL/TLS**



Klik op de knop **Test** om te verifiëren of het VCC verbinding kan maken met de AD-server.

Stap 3.3 Wijzig de gebiedsconfiguratie

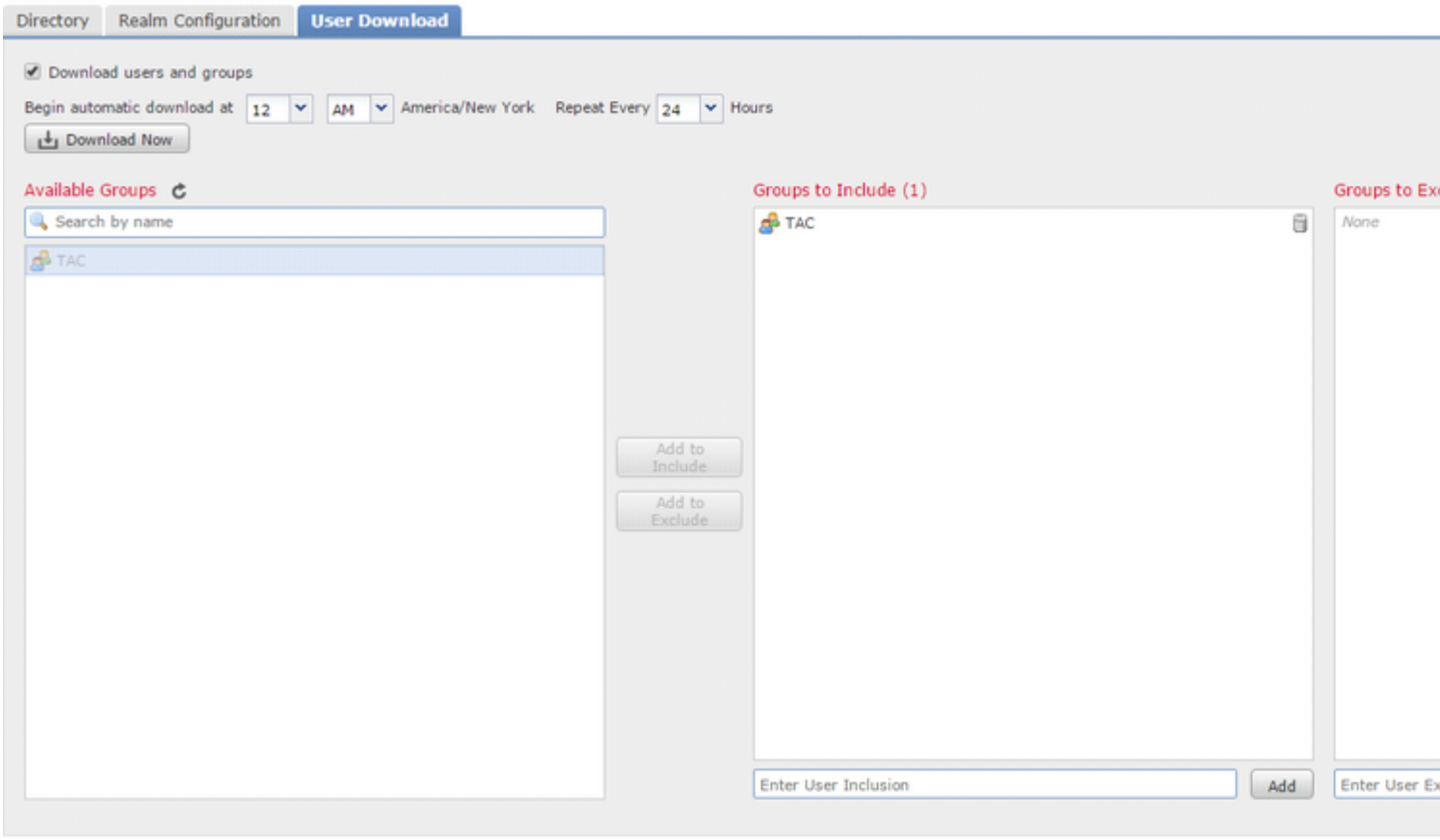
Ga naar **Realm Configuration** om de integratieconfiguratie van de AD-server te verifiëren en u kunt de AD-configuratie wijzigen.

Stap 3.4 Downloaden Gebruikersdatabase

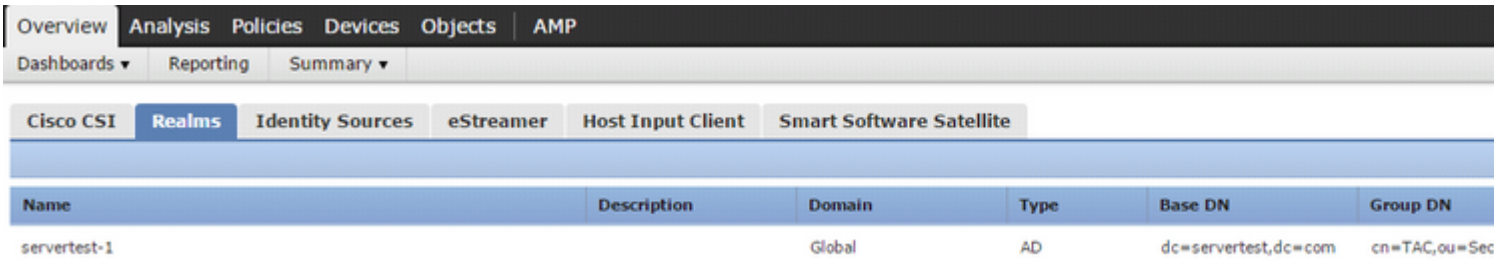
Navigeren naar **gebruiker Download** optie om de gebruikersdatabase te halen van de AD server.

Schakel het aanvinkvakje in om **gebruikers en groepen downloaden** te downloaden en het tijdsinterval te definiëren over hoe vaak FMC contact opneemt met AD om gebruikersdatabase te downloaden.

Selecteer de groep en plaats deze in de optie **Opnemen** waarvoor u de verificatie wilt configureren.



Schakel de AD-status in zoals in de afbeelding:



Stap 4. Het identiteitsbeleid configureren

Een identiteitsbeleid voert gebruikersverificatie uit. Als de gebruiker geen verificatie uitvoert, wordt toegang tot netwerkbronnen geweigerd. Dit dwingt Role-Based Access Control (RBAC) af op het netwerk en de resources van uw organisatie.

Stap 4.1 Captive Portal (actieve verificatie)

Actieve verificatie vraagt om gebruikersnaam/wachtwoord in de browser om een gebruikersidentiteit te identificeren om een verbinding mogelijk te maken. Browser authenticeert gebruiker met een verificatiepagina of authenticeert stilletjes met NTLM-verificatie. NTLM gebruikt de webbrowser om authenticatie-informatie te verzenden en ontvangen. Actieve verificatie maakt gebruik van verschillende typen om de identiteit van de gebruiker te verifiëren. Verschillende soorten verificatie zijn:

1. **HTTP Basic:** In deze methode vraagt de browser om gebruikersreferenties.
2. **NTLM:** NTLM gebruikt Windows werkstation referenties en bespreekt het met Active directory via een webbrowser. U moet de NTLM-verificatie in de browser inschakelen. Gebruikersverificatie

gebeurt transparant zonder aanwijzingen voor referenties. Het biedt een enkele aanmelding ervaring voor gebruikers.

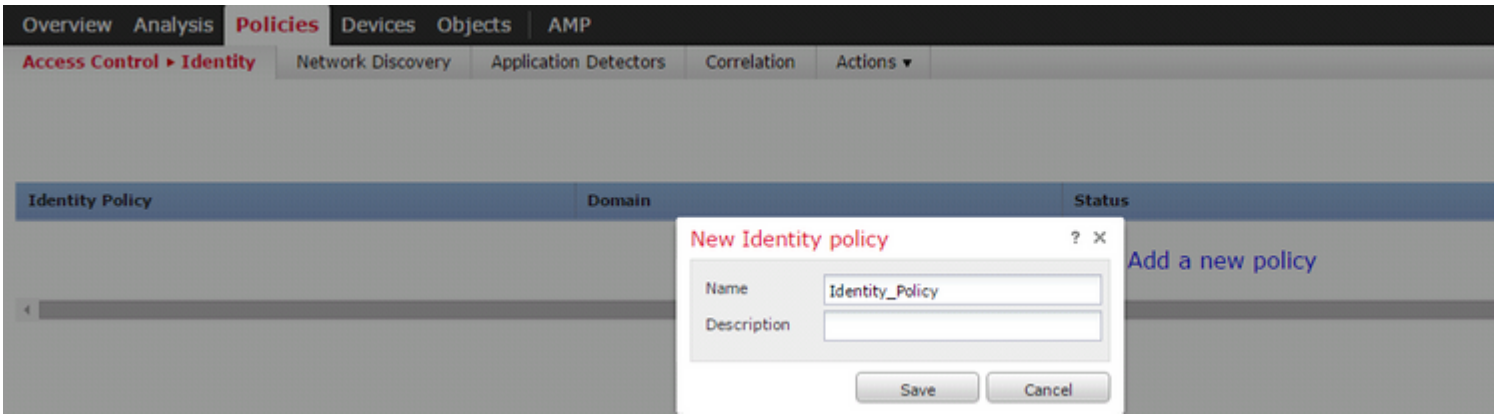
3. **HTTP Onderhandelen:**In dit type, probeert het systeem te verifiëren met NTLM. Als het mislukt, dan gebruikt de sensor HTTP Basic authenticatie type als een fallback methode en vraagt een dialoogvenster voor gebruikersreferenties.
4. **HTTP Response page:** Dit is vergelijkbaar met HTTP basis type, maar hier wordt de gebruiker gevraagd om de authenticatie in een HTML formulier dat kan worden aangepast.

Elke browser heeft een specifieke manier om de NTLM-verificatie in te schakelen en dus houden ze zich aan de browserrichtlijnen om de NTLM-verificatie mogelijk te maken.

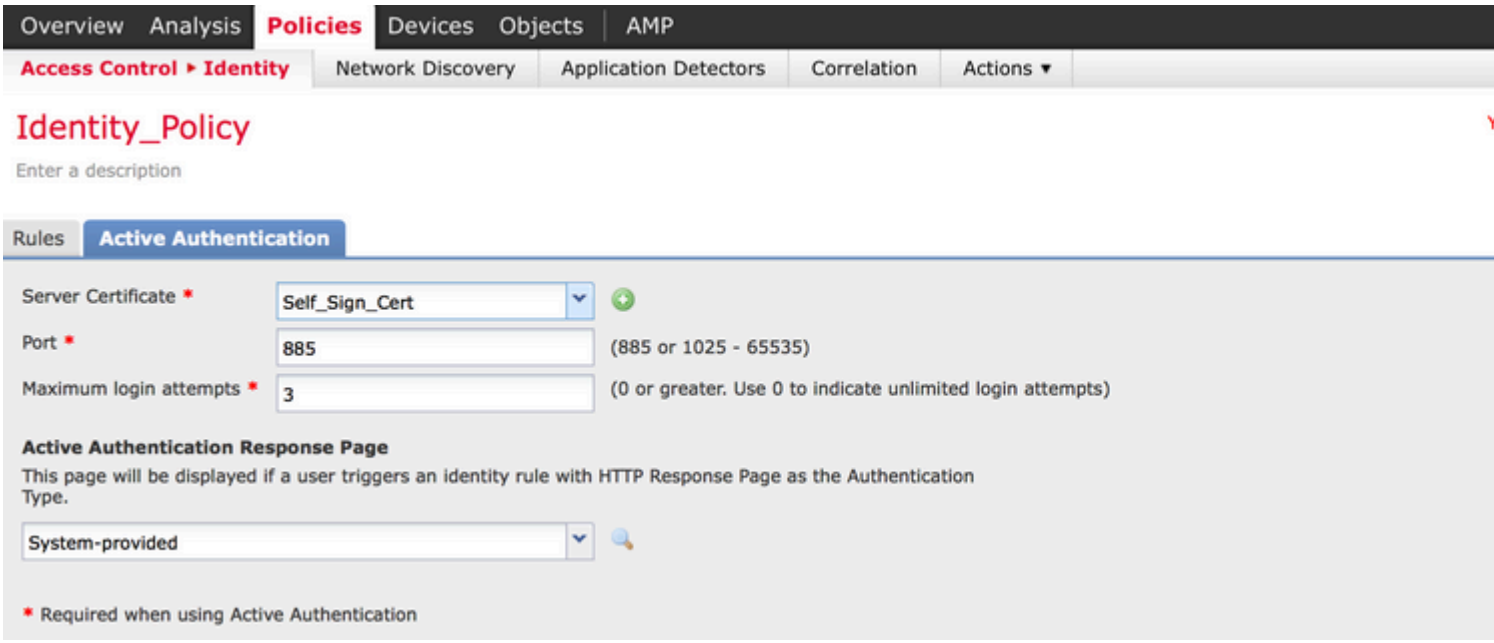
Om de referenties veilig te delen met de gerouteerde sensor, moet u ofwel zelf-ondertekende servercertificaat of openbaar-ondertekende servercertificaat installeren in het identiteitsbeleid.

```
Generate a simple self-signed certificate using openSSL -

Step 1.   Generate the Private key
               openssl genrsa -des3 -out server.key 2048

Step 2.   Generate Certificate Signing Request (CSR)
               openssl req -new -key server.key -out server.csr

Step 3.   Generate the self-signed Certificate.
               openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt
```

Ga naar **Beleid > Toegangsbeheer > Identiteit**. Klik op het **beleid toevoegen** & een naam geven aan het beleid en sla het op.

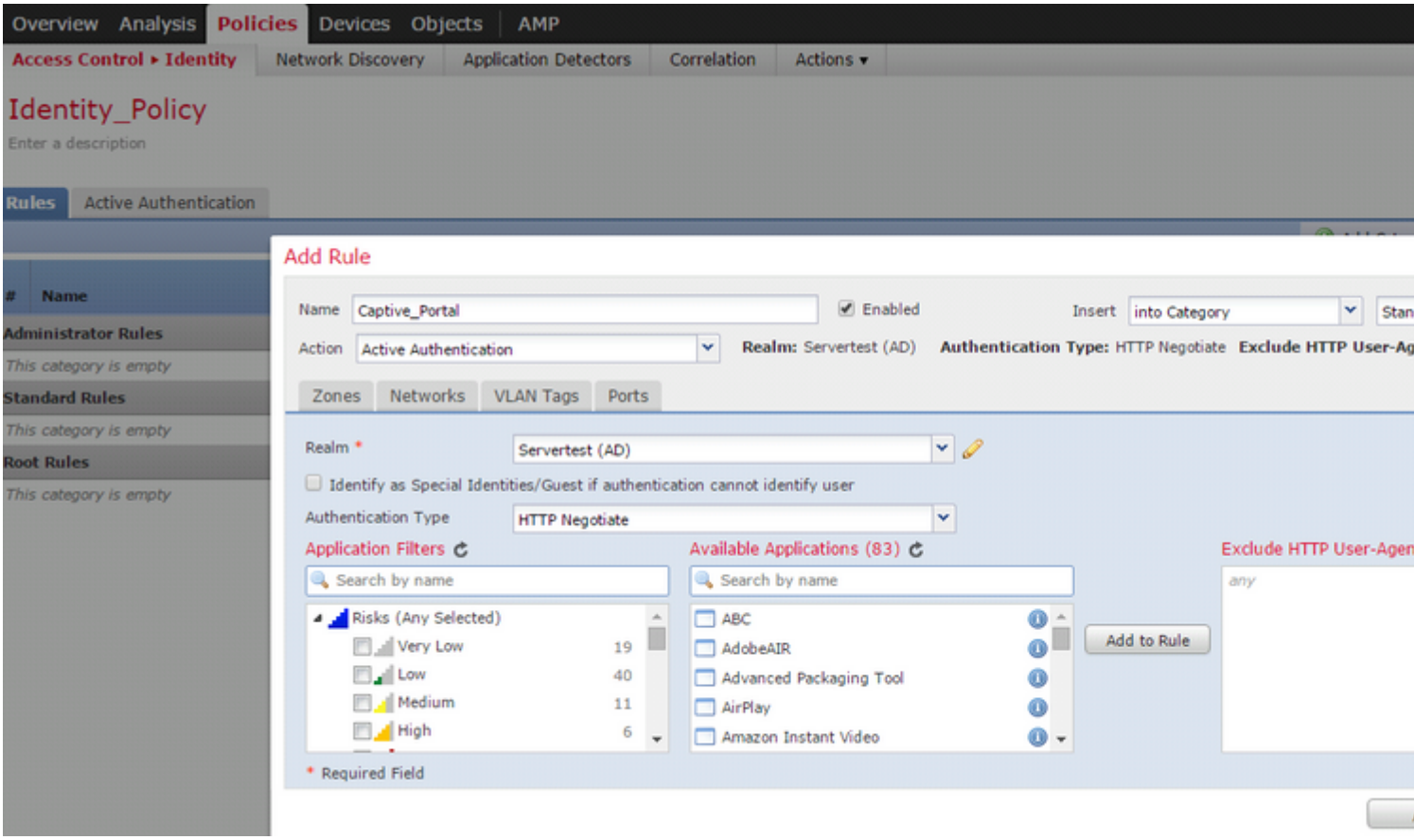


Navigeer naar het tabblad **Actieve verificatie** en klik in de optie **Servercertificaat** op het **pictogram (+)** en upload het certificaat en de privé-sleutel die u in de vorige stap met openSSL hebt gegenereerd.



Klik nu op de knop **Regel toevoegen** en geef een naam aan de regel en kies de actie als **actieve verificatie**. Definieer de bron/doelzone, het bron/doelnetwerk waarvoor u de gebruikersverificatie wilt inschakelen.

Selecteer het **domein,** dat u in de vorige stap hebt geconfigureerd, en een verificatietype dat het beste bij uw omgeving past.



ASA-configuratie voor Captive Portal

Voor ASA Firepower module, configureer deze opdrachten op de ASA om het captive portal te configureren.

```
ASA(config)# captive-portal global port 1055
```

Zorg ervoor dat de serverpoort, TCP 1055, is geconfigureerd in de **poortoptie** van het tabblad **Actieve verificatie** Identity Policy**.**

Om de actieve regels en hun klaptellingen te verifiëren, voer het bevel uit:

```
ASA# show asp table classify domain captive-portal
```

Opmerking: de opdracht Captive Portal is beschikbaar in ASA versie 9.5(2) en hoger.

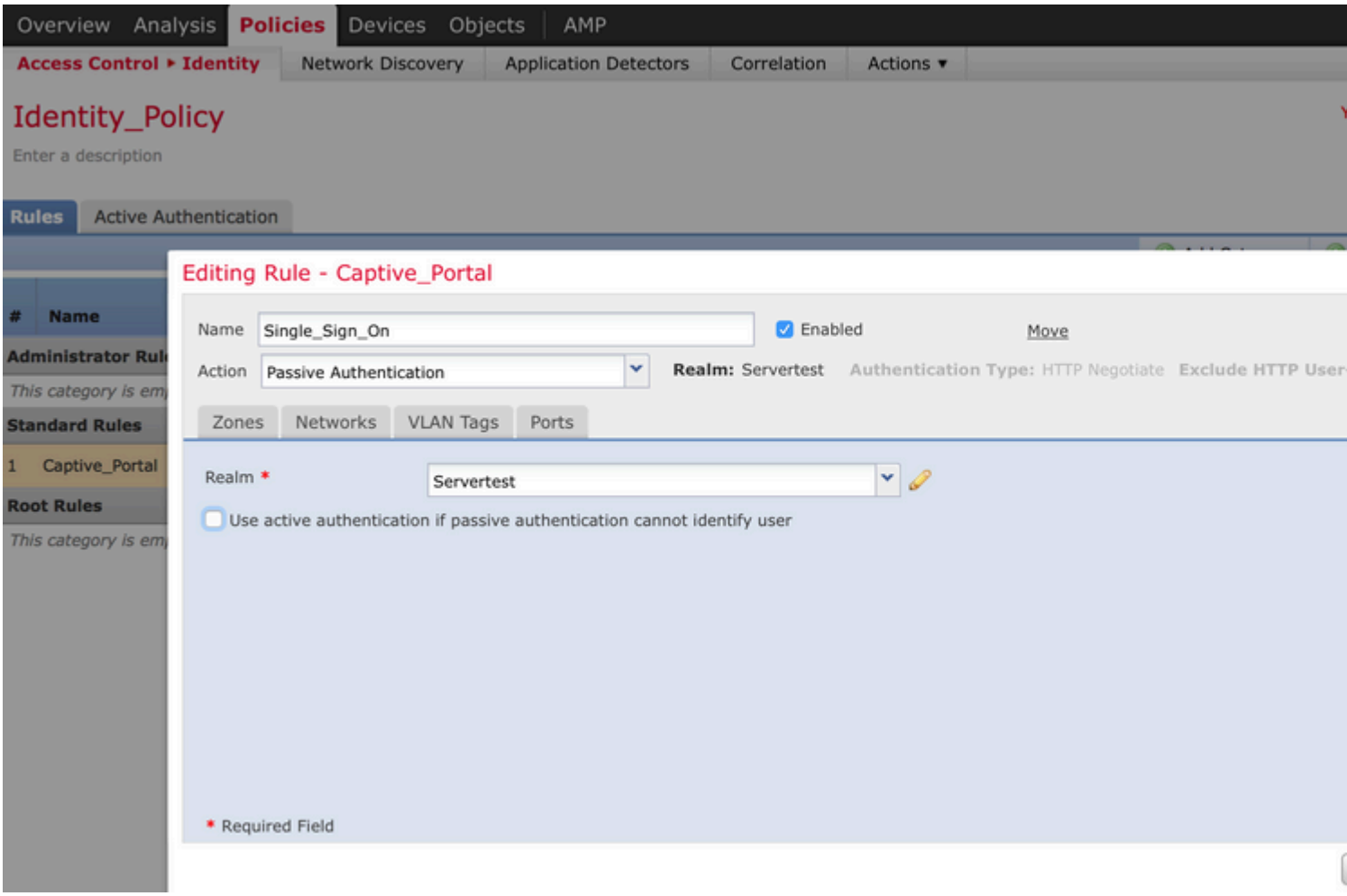
Stap 4.2 Enkelvoudige aanmelding (passieve verificatie)

Bij passieve authenticatie, wanneer een domeingebruiker inlogt en in staat is om de AD te authenticeren, de Firepower User Agent de User-IP-mapping details van de beveiligingslogbestanden van AD opvraagt en deze informatie deelt met Firepower Management Center (FMC). Het VCC stuurt deze gegevens naar de sensor om de toegangscontrole te handhaven.

Klik op de knop **Regel toevoegen** en geef een naam aan de regel en kies de **actie** als **passieve verificatie**. Definieer de bron/doelzone, het bron/doelnetwerk waarvoor u de gebruikersverificatie wilt inschakelen.

Selecteer het **gebied** dat u in de vorige stap hebt geconfigureerd en het verificatietype dat het best past bij uw omgeving, zoals in deze afbeelding.

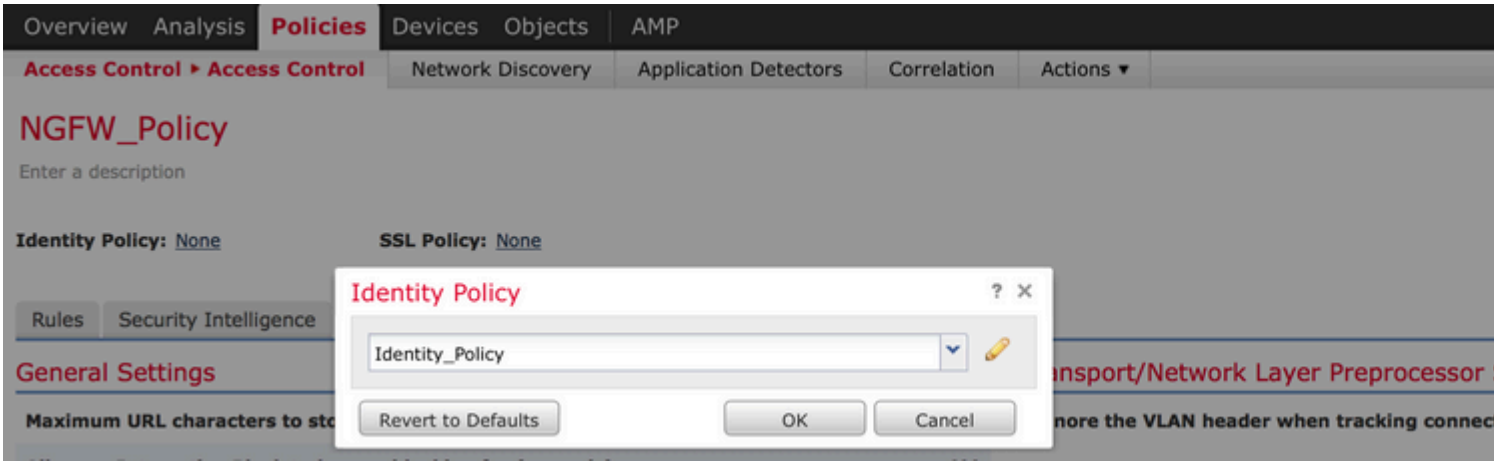
Hier kunt u een terugvalmethode als **actieve verificatie** kiezen **als passieve verificatie de gebruikersidentiteit niet kan identificeren**.



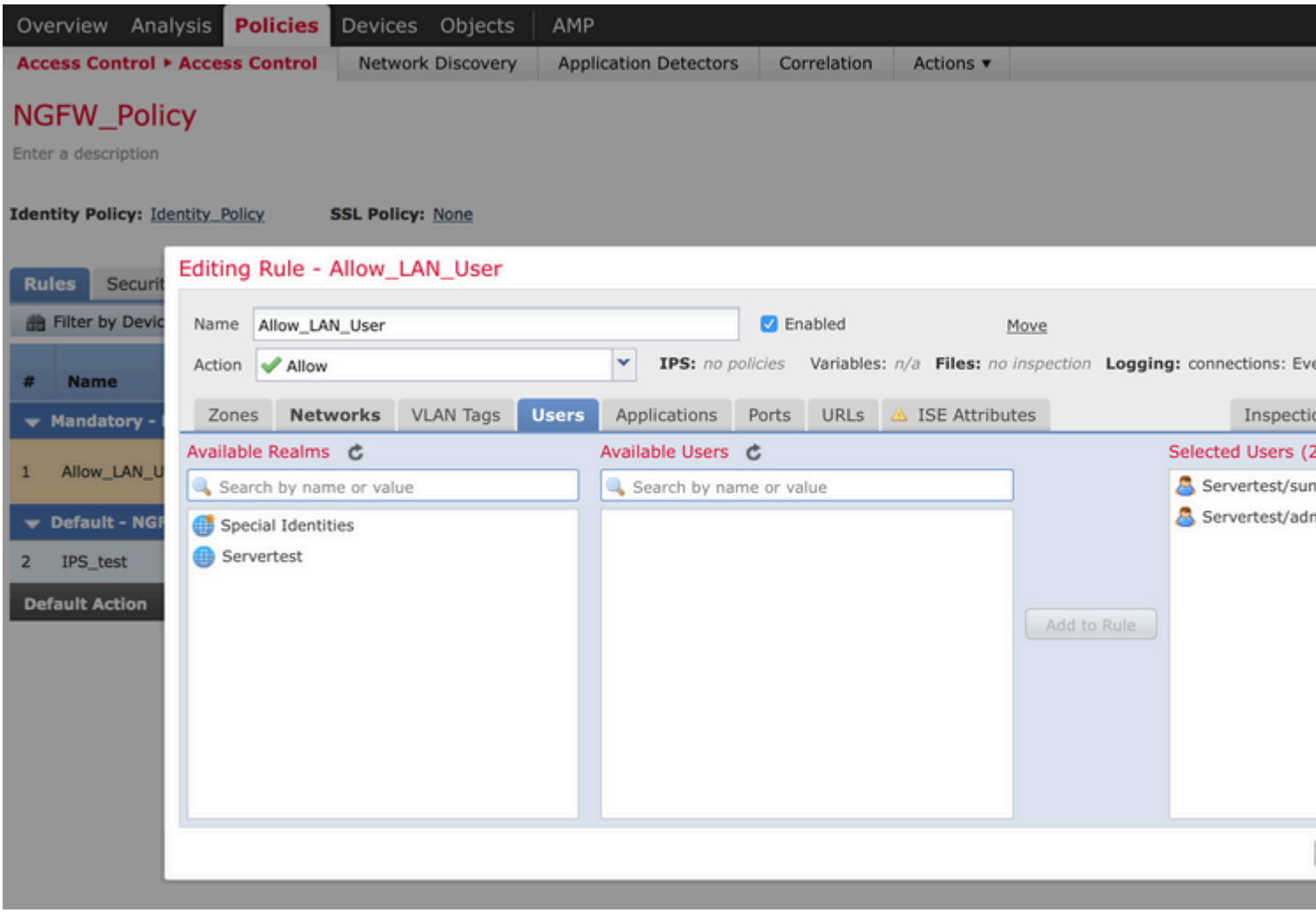
Stap 5. Configureer het toegangscontrolebeleid

Navigeer naar **Beleid > Toegangsbeheer > Een** beleid **maken/bewerken**.

Klik op het **identiteitsbeleid** (linkerbovenhoek), kies het identificatiebeleid dat u in de vorige stap hebt geconfigureerd en klik op de knop **OK**, zoals in deze afbeelding.

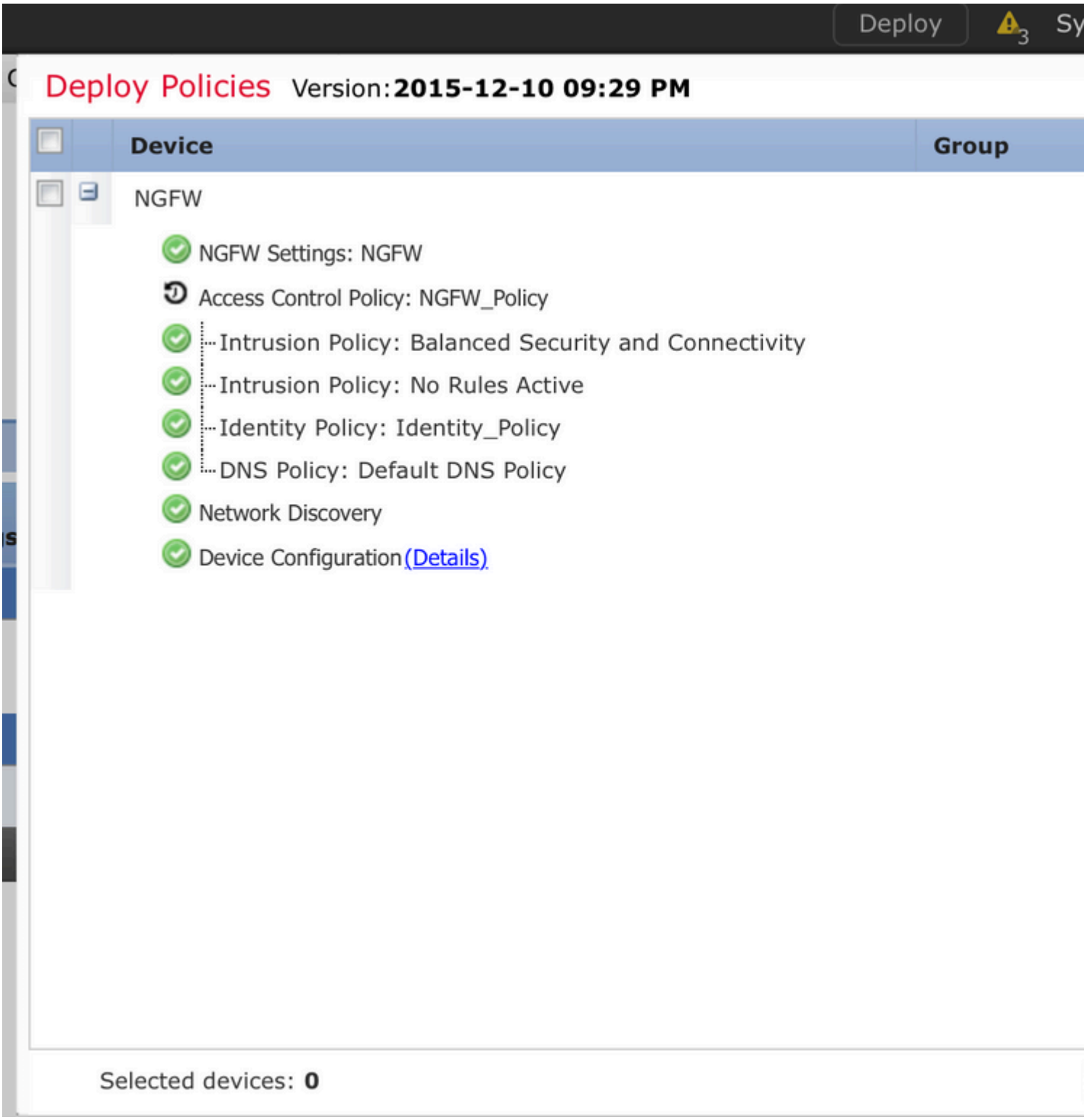


Klik op de knop **Regel toevoegen** om een nieuwe regel toe te voegen. Navigeer naar **Gebruikers** en selecteer de gebruikers waarvoor toegangscontroleregel afdwingt, zoals in deze afbeelding. Klik op **OK** en klik op **Opslaan** om de wijzigingen op te slaan.



Stap 6. Implementeer het toegangscontrolebeleid

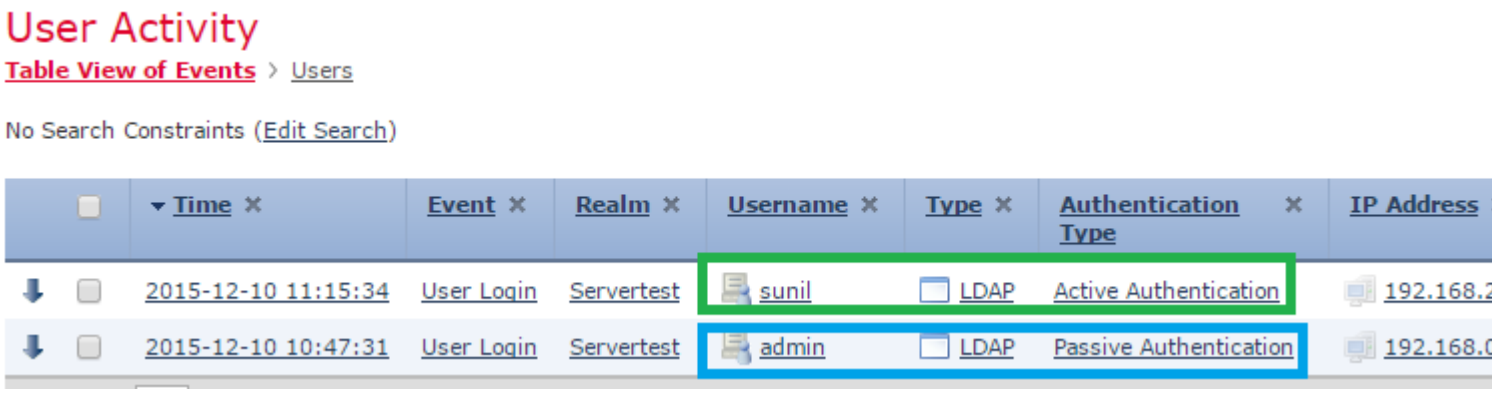
Navigeer om optie **op** te **stellen**, kies het **apparaat** en klik op de optie **op te stellen** om de configuratie te veranderen in de sensor. Controleer de implementatie van beleid vanaf de optie **Berichtencentrum** (pictogram tussen implementatie en systeemoptie) en zorg ervoor dat het beleid succesvol moet worden toegepast, zoals in deze afbeelding wordt getoond.



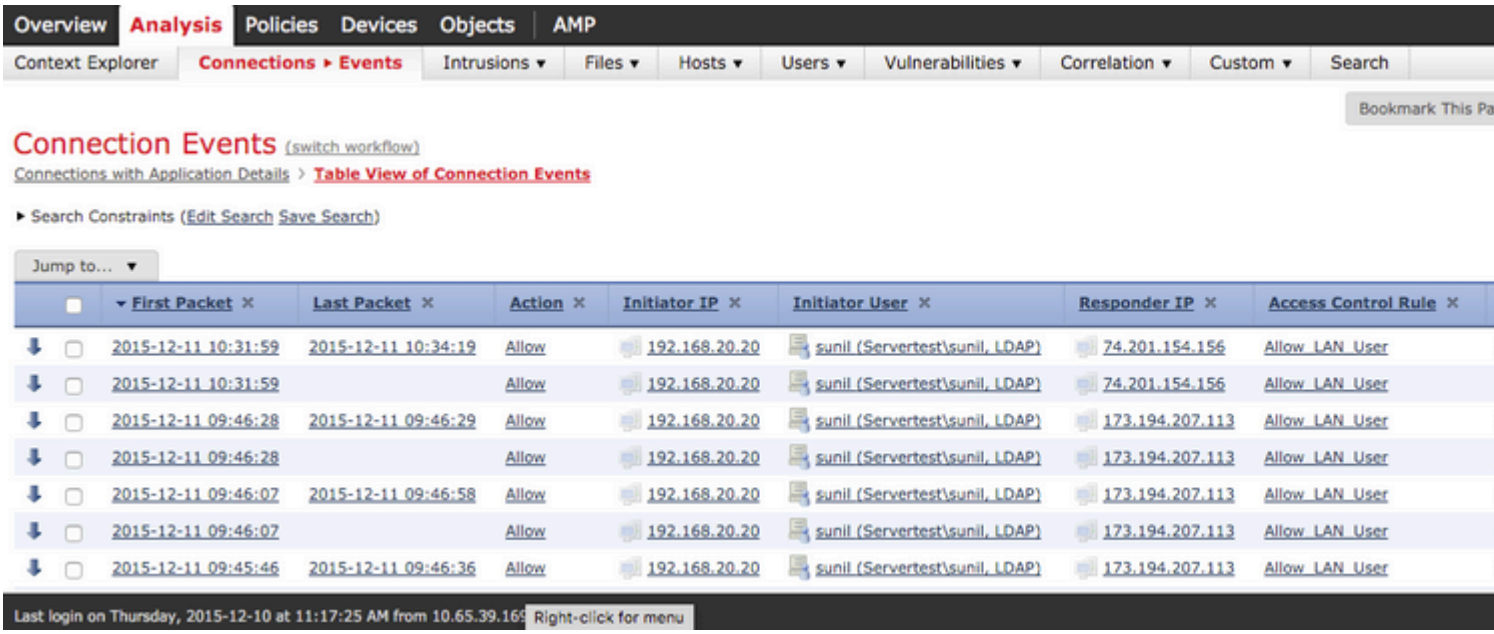
Stap 7. Controleer de gebeurtenissen van de gebruikers en van de verbindingen

Momenteel zijn actieve gebruikerssessies beschikbaar in de sectie **Analyse > Gebruikers > Gebruikers**.

Met de bewaking van gebruikersactiviteit kunt u uitzoeken welke gebruiker aan welk IP-adres is gekoppeld en hoe de gebruiker door het systeem wordt gedetecteerd door actieve of passieve verificatie. **Analyse > Gebruikers > Gebruikersactiviteit**



Navigeer naar **Analyse > Verbindingen > Gebeurtenissen**, om het type verkeer te bewaken dat door de gebruiker wordt gebruikt.



Verifiëren en probleemoplossing

Navigeer naar **Analyse** > **Gebruikers** om het type Gebruikersverificatie/verificatie/Gebruiker-IP-koppeling/toegangsregel die aan de verkeersstroom is gekoppeld, te verifiëren.

Controleer de connectiviteit tussen VCC en User Agent (passieve verificatie)

Firepower Management Center (FMC) maakt gebruik van TCP-poort 3306 om loggegevens van gebruikersactiviteit te ontvangen van de User Agent.

Gebruik deze opdracht in het VCC om de status van de dienst van het VCC te verifiëren.

```
admin@firepower:~$ netstat -tan | grep 3306
```

Voer pakketvastlegging uit op het VCC om de connectiviteit met de User Agent te verifiëren.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 3306
```

Ga naar **Analyse > Gebruikers > Gebruikersactiviteit** om te controleren of het VCC gebruikersaanmeldingsgegevens ontvangt van de User Agent.

Controleer de connectiviteit tussen VCC en Active Directory

FMC gebruikt TCP-poort 389 om de gebruikersdatabase op te halen uit de Actieve map.

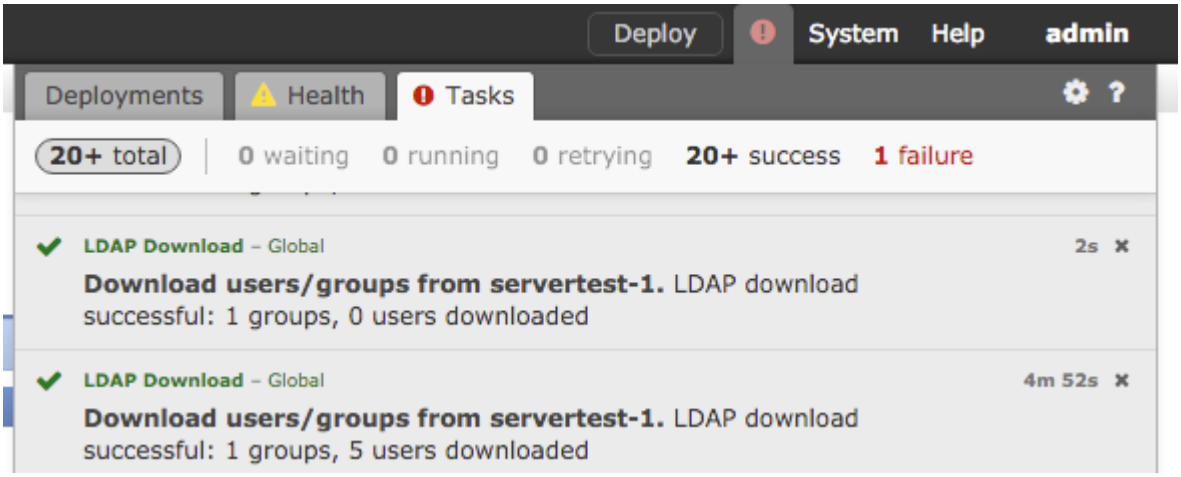
Voer pakketvastlegging uit op het VCC om de connectiviteit met de Active Directory te verifiëren.

```
admin@firepower:~$ sudo tcpdump -i eth0 -n port 389
```

Zorg ervoor dat de gebruikersreferenties die worden gebruikt in de configuratie van het FMC Real voldoende rechten hebben om de AD User-database op te halen.

Controleer de configuratie van het VCC-gebied en zorg ervoor dat de gebruikers/groepen worden gedownload en de time-out van de gebruikerssessie correct wordt geconfigureerd.

Navigeer naar **Berichtencentrum > Taken** en zorg ervoor dat de taak van de **gebruikers/groepen** succesvol wordt voltooid, zoals in deze afbeelding wordt getoond.



Controleer de connectiviteit tussen Firepower Sensor en het eindsysteem (actieve verificatie)

Voor actieve verificatie, zorg ervoor dat het certificaat en de poort correct zijn geconfigureerd in FMC Identity beleid.Standaard luistert Firepower sensor op TCP poort 885 voor actieve verificatie.

Controleer de beleidsconfiguratie en -implementatie

Zorg ervoor dat de velden Realm, Verificatietype, Gebruikersagent en Actie correct zijn geconfigureerd in Identity Policy.

Zorg ervoor dat het identiteitsbeleid correct aan het toegangscontrolebeleid wordt gekoppeld.

Navigeer naar **Berichtencentrum > Taken** en zorg ervoor dat de beleidsimplementatie met succes wordt voltooid.

De logboeken van de gebeurtenissen analyseren

De verbinding en de gebeurtenissen van de Activiteit van de Gebruiker kunnen worden gebruikt om te diagnosticeren of de gebruikerslogin of niet succesvol is. Deze gebeurtenissen

U kunt ook controleren welke toegangscontroleregel op de stroom wordt toegepast.

Navigeer naar **Analyse > Gebruiker** om de logboeken met gebruikersgebeurtenissen te controleren.

Navigeer naar **Analyse > Verbindingsgebeurtenissen** om de verbindingsgebeurtenissen te controleren.

Gerelateerde informatie

- **Technische ondersteuning en documentatie â€“ Cisco Systems**

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.