Active Directory-integratie met ASDM configureren voor Single-aanmelding en Captive Portal verificatie (On-Box Management)

Inhoud

Inleiding

In dit document wordt de configuratie beschreven van Captive Portal Authentication (Active Accounting) en Single-Sign-On (Passive Verificatie) op Firepower Module met ASDM (Adaptieve Security Devices Manager).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van ASA (adaptieve security applicatie) firewall en ASDM
- Kennis van FirePOWER-module
- Lichtgewicht Map Service (LDAP)
- Firepower User Agent

Gebruikte componenten

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

- ASA FirePOWER-modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) met software versie 5.4.1 en hoger.
- ASA FirePOWER-module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) met software 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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Captive Portal Authentication or Active Verification leidt tot een inlogpagina en de gebruikersreferenties zijn vereist voor een host om de toegang tot internet te krijgen.

Single-aanmelding of Passive Verificatie biedt een gebruiker naadloze authenticatie voor netwerkbronnen en internettoegang zonder dat de gebruiker meerdere malen toegang heeft. De single-aanmelding-verificatie kan worden bereikt door een Firepower user agent of een NTLM browser verificatie.

> **Opmerking**: Captive Portal Authentication, ASA moet in routed Mode zijn.

> Opmerking: Opdracht Captive portal is beschikbaar in ASA versie 9.5(2) en later.

Configureren

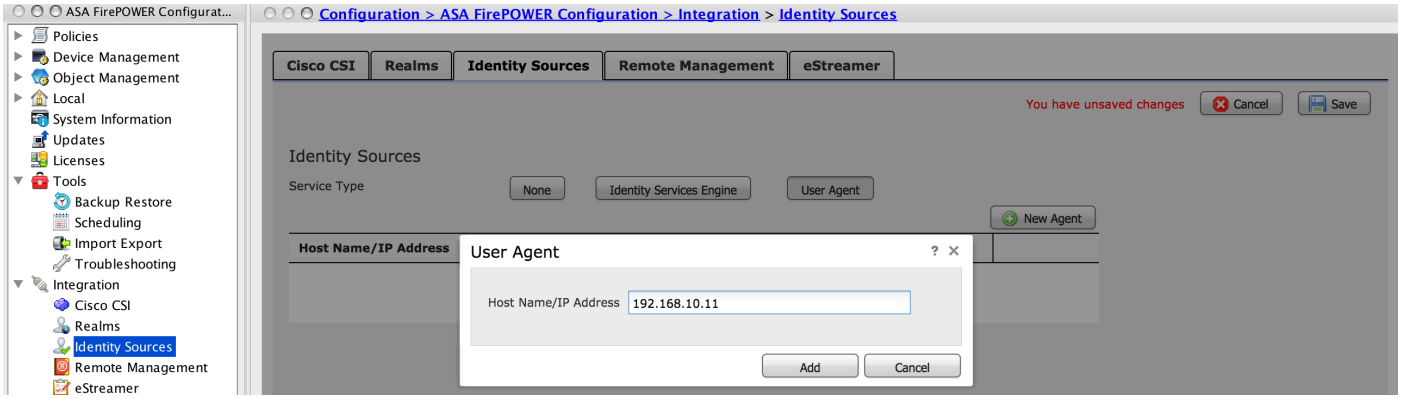
Stap 1. Configureer de FirePOWER User Agent voor Single-aanmelding.

Dit artikel legt uit hoe u Firepower User Agent in Windows machine kunt configureren:

[Installatie en uninstallatie van Sourcefire-gebruikersagent]

Stap 2. Integreer de Firepower Module (ASDM) met User Agent

Meld u aan bij ASDM, navigeer naar **Configuration > ASA FirePOWER Configuration > Integration > Identity Services** en klik op de optie **User Agent**. Nadat u op de optie **Gebruikersagent** klikt en het IP-adres van het systeem van Gebruikersagent configureren. klik op **Add**, zoals in de afbeelding:



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

Stap 3. Integreer Firepower met Active Directory.

Stap 3.1 Maak het antwoord.

Meld u aan bij ASDM, navigeer naar **Configuration > ASA FirePOWER Configuration > Integration > Realms.** Klik op **Toevoegen een nieuw voorbeeld**.

Naam en beschrijving: Geef een naam/beschrijving om het veld uniek te identificeren.

Type: AD

Primair domein: Domain Name of Active Directory (NETeuropa Name).

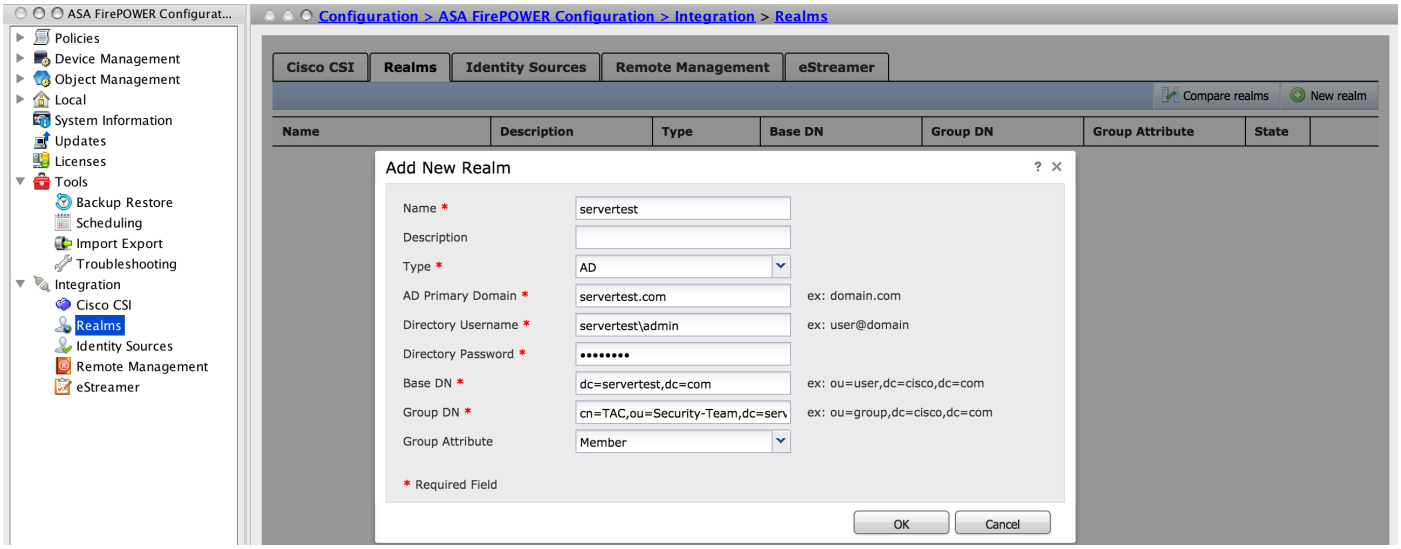
Gebruikersnaam map: Specificeer de <*gebruikersnaam*>.

Wachtwoord voor map: Specificeer het <*wachtwoord*>.

Base DN: Domain of Specific OU DN vanaf waar het systeem een zoekopdracht in LDAP database start.

Groep DN: Specificeer de groep DN.

Groepskenmerk: Specificeer het optie-lid in de vervolgkeuzelijst.



Klik op **OK** om de configuratie op te slaan.

Dit artikel kan u helpen om de waarden van de DN-basis en de groep te bepalen.

[Identificeer actieve bestandsindelingen voor map]

Stap 3.2 Voeg het IP-adres/hostname van de Map Server toe.

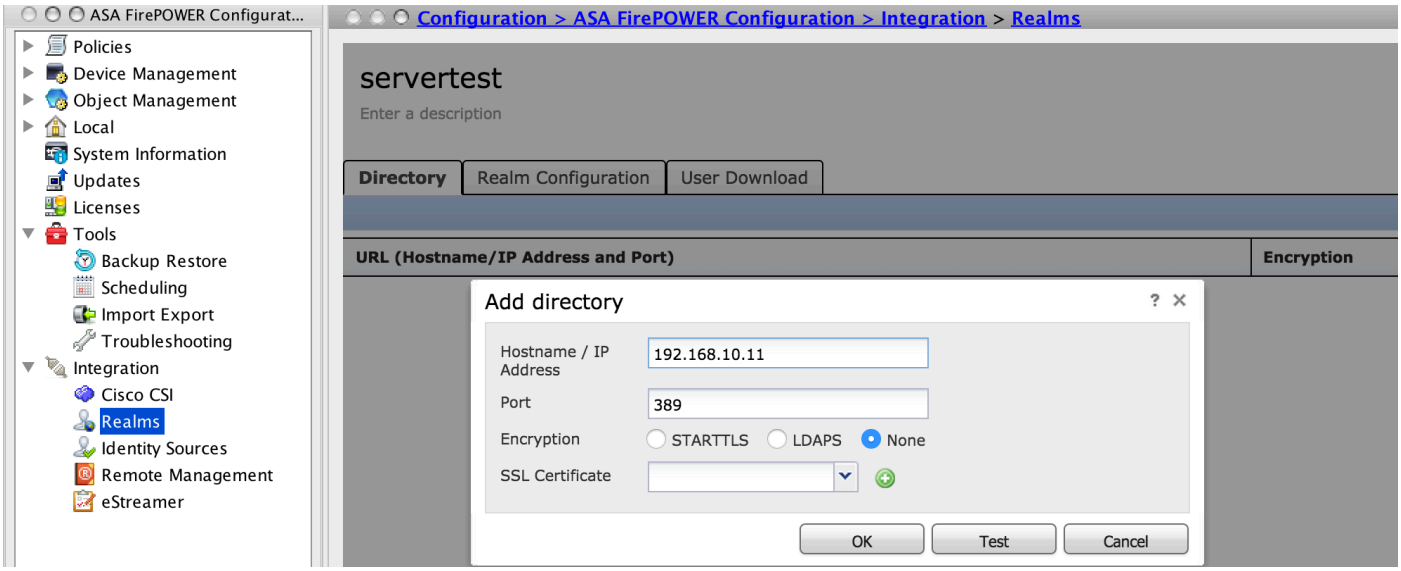
Om AD Server IP/hostname te specificeren, klik op **Add folder**.

Hostname/IP Adres: stel het IP adres/hostname van de AD server in.

Poorten: Specificeer het actieve LAN-poortnummer (standaard 389).

Encryption/SSL-certificaat: (optioneel) Raadpleeg dit artikel om de verbinding tussen FMC en AD-server te versleutelen:

[Verificatie van verificatieobject via FireSIGHT System voor Microsoft AD-verificatie via SSL/T...]



Klik **Test** om de verbinding van FMC met de AD-server te verifiëren. Klik nu op **OK** om de configuratie op te slaan.

Stap 3.3 Wijzig de configuratie van het besturingssysteem.

Om de integratieconfiguratie van de AD-server te wijzigen en te controleren, navigeer dan naar **Realm Configuration**.

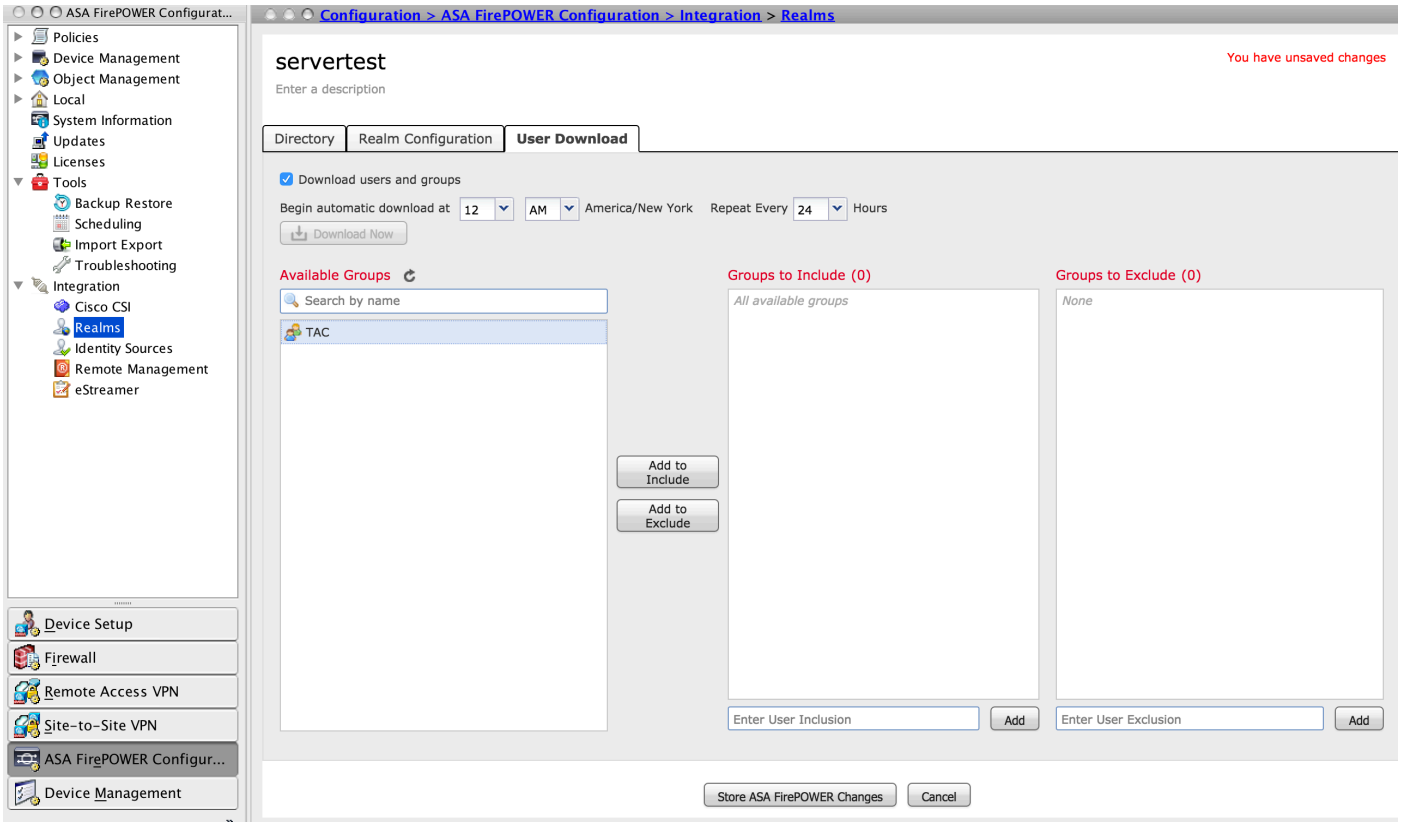
Stap 3.4 Downloadgebruikersdatabase.

Navigeer naar **User Download** om de gebruikersdatabase van de AD server te halen.

Schakel het aanvinkvakje in om **gebruikers en groepen van downloads** te downloaden en definieer het tijdsinterval over hoe vaak de Firepower module contact opneemt met AD server om gebruikersdatabase te downloaden.

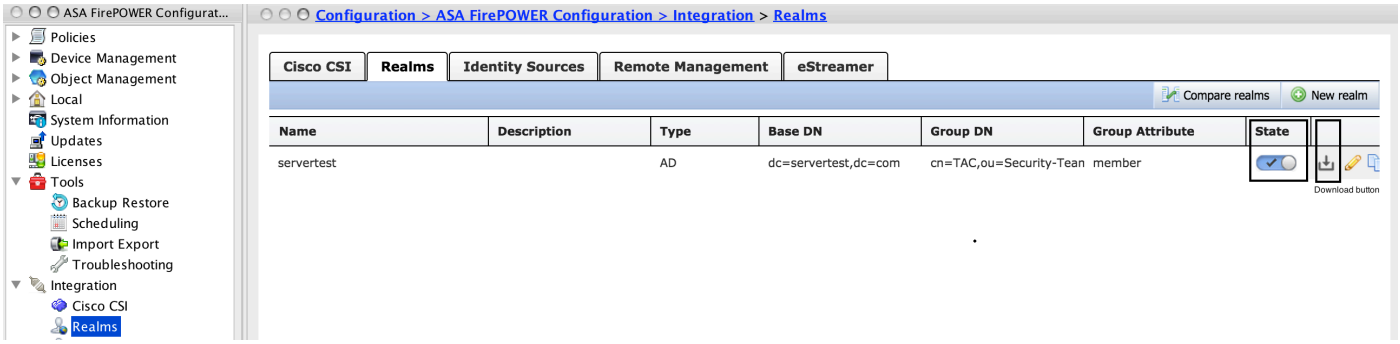
Selecteer de groep en voeg deze toe aan de optie **Inclusief** waarvoor u de Verificatie wilt

configureren. Standaard worden alle groepen geselecteerd als u er niet voor kiest om de groepen op te nemen.



Klik op **Store ASA Firepower Wijzigingen** om de realm-configuratie op te slaan.

Schakel de gebiedsstatus in en klik op de knop downloaden om de gebruikers en groepen te downloaden, zoals in de afbeelding.



Stap 4. Het identiteitsbeleid configureren.

Een identiteitsbeleid voert gebruikersauthenticatie uit. Als de gebruiker niet echt verklaart, wordt de toegang tot de netwerkbronnen geweigerd. Dit dwingt Rol-Based Access Control (RBAC) op het netwerk en de bronnen van uw organisatie.

Stap 4.1 Captive portal (actieve verificatie).

Actieve Verificatie vraagt om gebruikersnaam en wachtwoord in de browser om een gebruikersidentiteit te identificeren om een verbinding mogelijk te maken. browser authenticeert gebruiker door authenticatie pagina aan te bieden of authenticeert in stilte met NTLM authenticatie. NTLM gebruikt de webbrowser om verificatieinformatie te verzenden en ontvangen.

De actieve verificatie gebruikt verschillende typen om de identiteit van de gebruiker te controleren. Verschillende typen verificatie zijn:

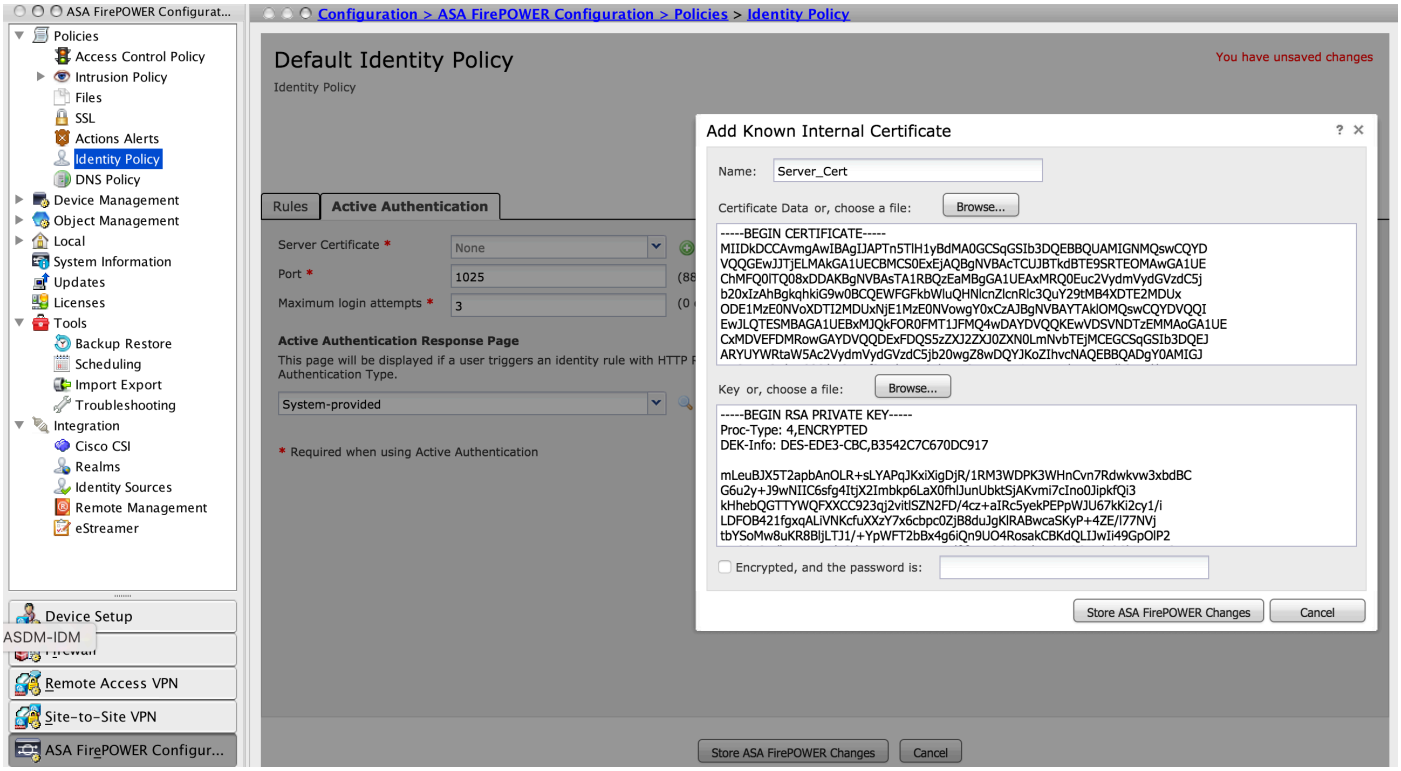
1. **HTTP Basic: In deze methode, vraagt de browser om gebruikersreferenties.**
2. **NTLM: NTLM gebruikt Windows-werkstationaanmeldingsgegevens en bespreekt dit met een actieve map op een webbrowser. U moet de NTLM-verificatie in de browser inschakelen. Gebruikersverificatie gebeurt op een transparante wijze zonder aanmeldingsgegevens te vragen. Het biedt één aanmelding ervaring voor gebruikers.**
3. **HTTP-onderhandeling:**In dit type probeert het systeem het gebruik van NTLM voor authenticatie te zorgen, als de sensor het HTTP Basic-verificatietype niet gebruikt als back-upmethode en een dialoogvenster voor gebruikersreferenties creëert.
4. **HTTP-responspagina: Dit is vergelijkbaar met het HTTP-basistype, maar hier wordt de gebruiker gevraagd de authenticatie in een HTML-formulier in te vullen dat kan worden aangepast.**

Elke browser heeft een specifieke manier om NTLM-verificatie mogelijk te maken en daarom kunt u browser-richtlijnen volgen om NTLM-verificatie mogelijk te maken.

Om de geloofwaardigheid met de routesensor te delen, moet u een zelf-ondertekend servercertificaat of een door de overheid ondertekend servercertificaat in het identiteitsbeleid installeren.

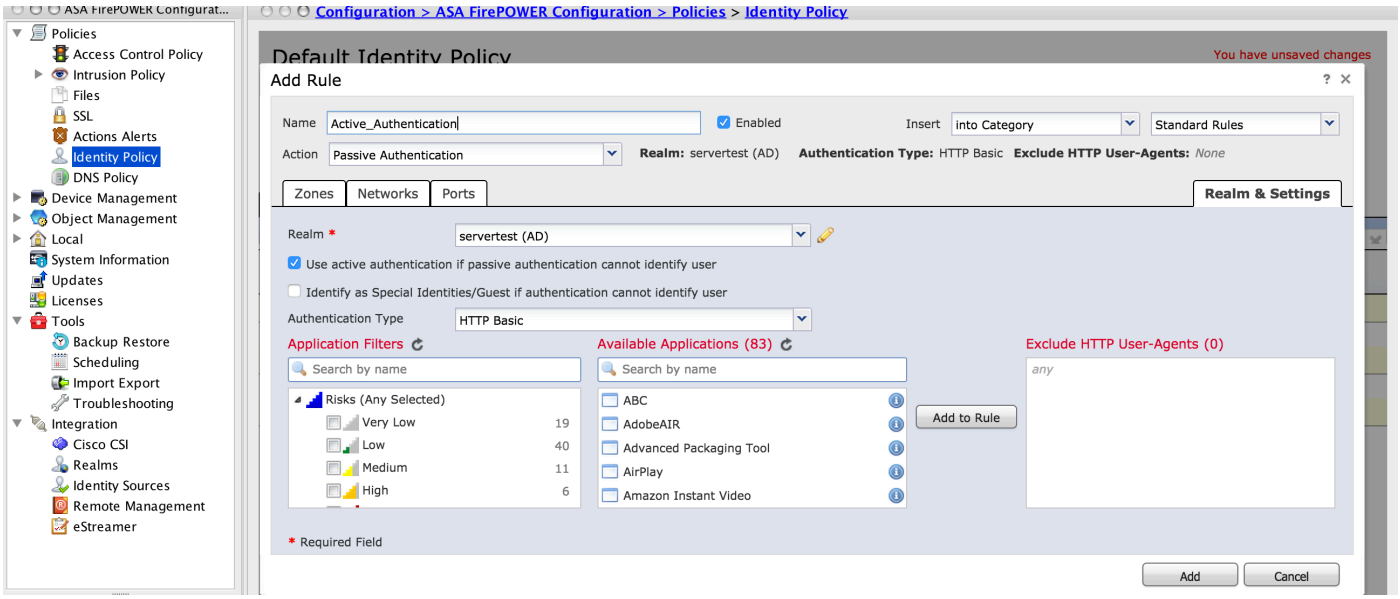
```
Generate a simple self-signed certificate using openSSL -

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
```

Navigatie in naar **configuratie > ASA FirePOWER-configuratie > Beleid > identiteitsbeleid**. Klik nu op het tabblad **Actieve verificatie** en klik in de optie **servercertificaat** op het **pictogram (+)** en uploadt u het certificaat en de privé-toets die u in de vorige stap hebt gegenereerd met behulp van openSSL, zoals in de afbeelding:



Klik nu op **Add Rule** om een naam aan de Regel te geven en de actie als **Actieve Verificatie** te kiezen. Defineer de bron/doelzone, bron/doelnetwerk waarvoor u de gebruikersverificatie wilt inschakelen.

navigeren naar het tabblad **Realm & Settings**. Selecteer het antwoord in de vervolgkeuzelijst die u in de vorige stap hebt ingesteld en selecteer het **verificatietype** in de vervolgkeuzelijst die het best past bij uw netwerkomgeving.



Stap 4.2 ASA Configuration voor Captive Portal.

Stap 1. Defineer het interessante verkeer dat voor inspectie naar Sourcefire zal worden omgeleid.

```
ASA(config)# access-list SFR_ACL extended permit ip 192.168.10.0 255.255.255.0 any
ASA(config)#
ASA(config)# class-map SFR_CMAP
```

```
ASA(config-cmap)# match access-list SFR_ACL


ASA(config)# policy-map global_policy
ASA(config-pmap)# class SFR_CMAP
ASA(config-pmap-c)# sfr fail-open
ASA(config)#service-policy global_policy global
```

Stap 2. Configureer deze opdracht in de ASA om het portaal in gevangenschap mogelijk te maken.

```
ASA(config)# captive-portal interface inside port 1025
```

> **Tip**: een portaal in gevangenschap kan mondiaal of per interface worden gebruikt.

> **Tip**: Zorg ervoor dat de serverpoort, TCP 1025 is ingesteld in de poortoptie van het tabblad Actieve Verificatie van het identiteitsbeleid.

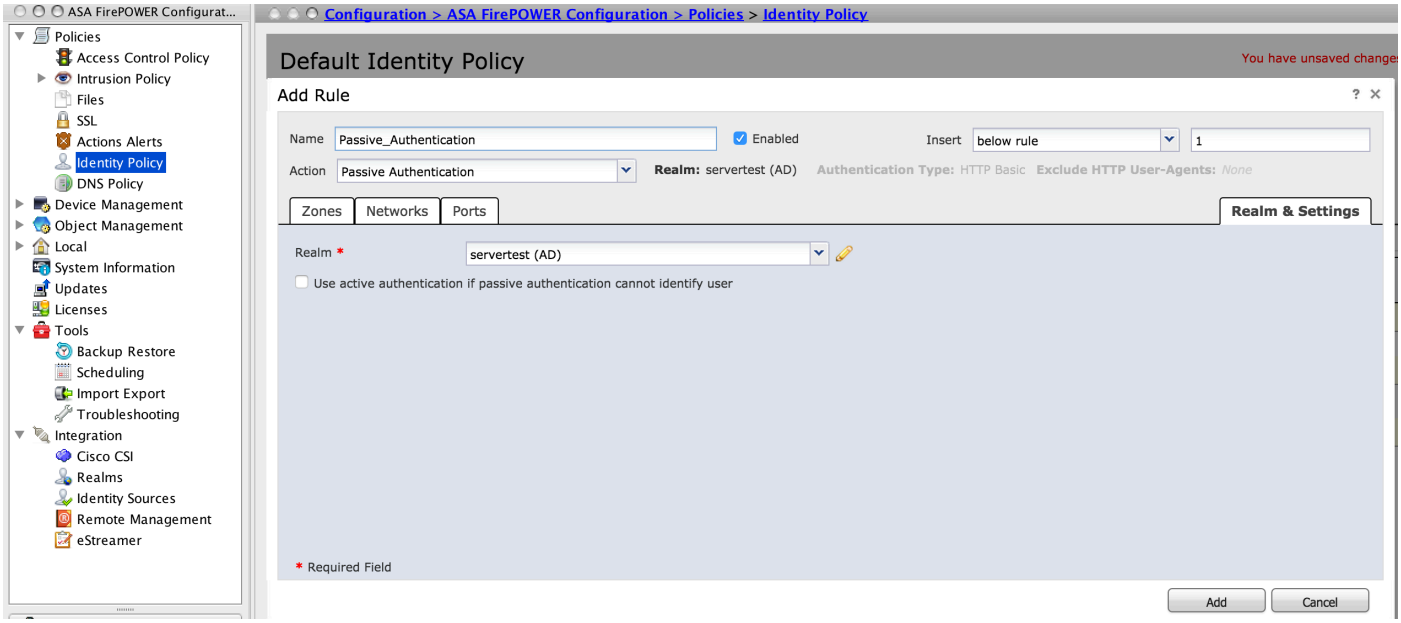
Stap 4.3 Eenvoudig aanmelding (passieve verificatie).

Bij passieve verificatie, wanneer een domeingebruiker logt en de AD voor authenticatie kan authenticeren, poilt de Firepower User Agent de User-IP mapping details van de veiligheidslogbestanden van AD en deelt deze informatie met Firepower Module. Firepower module gebruikt deze gegevens om de toegangscontrole af te dwingen.

Om de passieve authenticatieregel te configureren klikt u op **Toevoegen-regel** om een naam aan de regel te geven en vervolgens de **Actie** als **Passive Verificatie** te kiezen. Defineer de bron/doelzone, bron/doelnetwerk waarvoor u de gebruikersverificatie wilt inschakelen.

Navigeren in naar de **Instellingen lezen** tab. Selecteer het **Realm** uit de vervolgkeuzelijst die u in de vorige stap hebt ingesteld.

Hier kunt u de fall-back methode als **actieve authenticatie** kiezen **als passieve authenticatie de gebruikersidentiteit niet kan identificeren**, zoals getoond in het beeld:

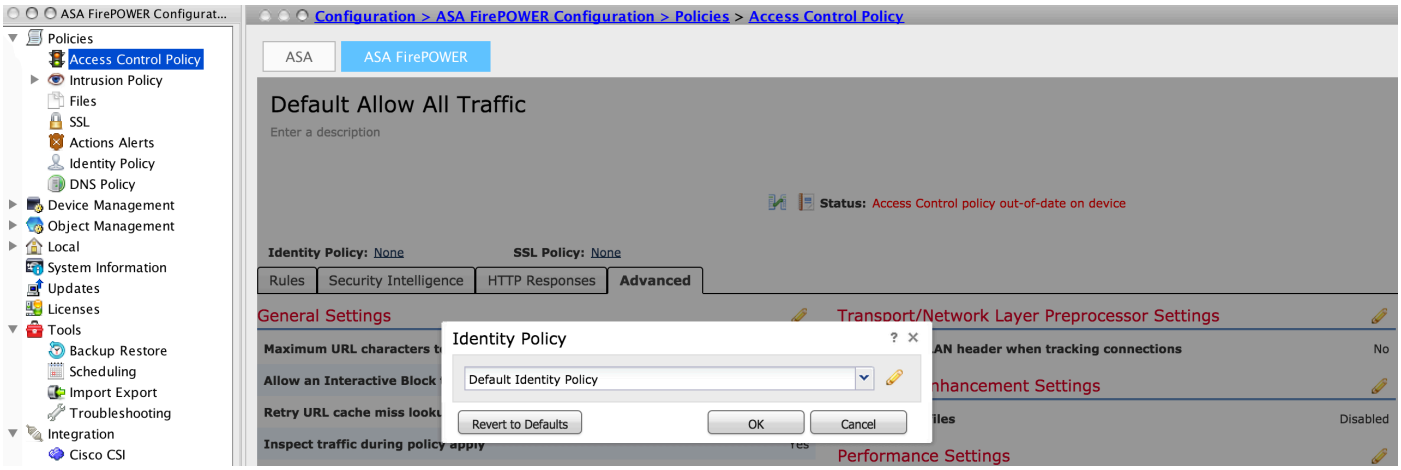


Klik nu op **Store ASA Firepower Wijzigingen** om de configuratie van het identiteitsbeleid op te slaan.

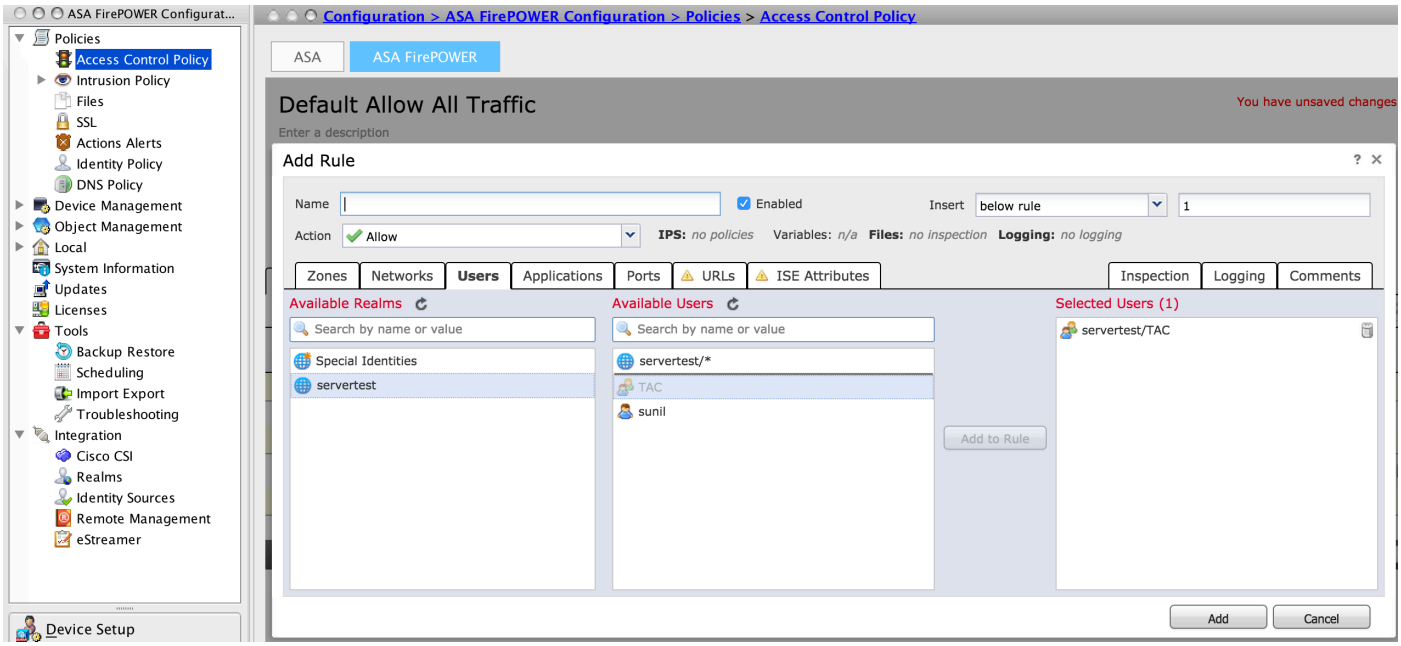
Stap 5. Configureer het toegangscontrolebeleid.

Navigeer naar **Configuratie > ASA FirePOWER Configuration > Policy > Access Control Policy.**

Klik op de **hoek** van het **identiteitsbeleid** (linker kant boven), selecteer het beleid identificeren dat u in de vorige stap hebt ingesteld in de vervolgkeuzelijst en klik op **OK**, zoals in deze afbeelding.



Klik op **Regels toevoegen** om een nieuwe regel toe te voegen, navigeer om **Gebruikers** en selecteer de gebruikers waarvoor de toegangscontroleregel wordt afgedwongen, zoals in deze afbeelding wordt weergegeven en klik op **Toevoegen**.



Klik op **ASA FireSIGHT-wijzigingen opslaan** om de configuratie van het beleid voor toegangscontrole op te slaan.

Stap 6. Voer het beleid voor toegangscontrole in.

U moet het beleid voor toegangscontrole implementeren. Voordat u het beleid toepast, ziet u een bijgewerkte indicatie Toegangsbeheer beleid in de module. Om de veranderingen in de sensor in te stellen, klikt u op **Uitvoeren** en kiest u **optie FirePOWER Veranderingen implementeren** en klikt

u vervolgens op **Uitvoeren** in het pop-upvenster.

> Opmerking: In versie 5.4.x, om het toegangsbeleid op de sensor toe te passen, moet u ASA FirePOWER Wijzigingen toepassen

> Opmerking: Navigeer naar bewaking > ASA Firepower Monitoring > Task Status. Zorg ervoor dat deze taak de toepassing van de configuratieverandering moet voltooien.

Stap 7. Controleer gebruikersgebeurtenissen.

Navigeer naar **bewaking > ASA FirePOWER-bewaking > Real-Time Eventing**, om het type verkeer te controleren dat door de gebruiker wordt gebruikt.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Navigeer naar **Analyse > Gebruikers** om de gebruikersverificatie/Verificatietype/User-IP mapping/Access-regel die aan de verkeersstroom is gekoppeld te controleren.

Connectiviteit tussen Firepower Module en User Agent (passieve verificatie)

Firepower Module gebruikt TCP poort 3306 om gebruikersactiviteitsloggegevens van de gebruikersagent te ontvangen.

Gebruik deze opdracht in het VCC om de servicestatus van de Firepower Module te controleren.

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

Start pakketvastlegging op het FMC om de connectiviteit met de gebruikersagent te controleren.

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

Connectiviteit tussen FMC en actieve map

Firepower module gebruikt TCP poort 389 om de gebruikersdatabase van de actieve map op te halen.

Voer pakketvastlegging in op de Firepower Module om connectiviteit met de Active Directory te controleren.

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

Zorg ervoor dat de gebruikersinterface die in de configuratie van Realm wordt gebruikt voldoende voorrecht heeft om de gebruikersdatabase van de AD te halen.

Controleer de configuratie van het programma en zorg ervoor dat de gebruikers/groepen worden gedownload en de tijd voor de gebruikerssessie correct wordt ingesteld.

Navigeren in om ASA FirePOWER Monitoring Task Status te controleren en ervoor zorgen dat de download van taakgebruikers/groepen met succes wordt voltooid, zoals in deze afbeelding wordt getoond.

Connectiviteit tussen ASA en het end systeem (actieve verificatie)

actieve authenticatie, zorg ervoor dat het certificaat en de poort correct zijn ingesteld in Firepower Module Identity Policy en ASA (commando van een portal). Standaard luisteren ASA en Firepower module op TCP poort 885 voor actieve verificatie.

Om de actieve regels en hun hit tellingen te verifiëren, voer deze opdracht op de ASA uit.

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

Input Table
in  id=0x2aaadf516030, priority=121, domain=captive-portal, deny=false
   hits=10, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
   src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
   dst ip/id=19.19.19.130, mask=255.255.255.255, port=1025, tag=any, dscp=0x0
   input_ifc=inside, output_ifc=identity

Output Table:

L2 - Output Table:

L2 - Input Table:

Last clearing of hits counters: Never
```

Beleidsconfiguratie en -implementatie

Zorg ervoor dat de velden Realm, Verificatie, Gebruiker en Actie correct zijn ingesteld in Identity Policy.

Zorg ervoor dat het identiteitsbeleid correct in verband wordt gebracht met het toegangscontrolebeleid.

Navigeren in om > ASA FirePOWER Monitoring > Taakstatus te controleren en ervoor zorgen dat de Beleidsinstelling voltooid is.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems
- Active Directory-integratie met FirePOWER-applicatie voor Single Sign-On en Captive Portal verificatie