ASA VPN-gebruikersverificatie met Windows 2008 NPS Server (Active Directory) met RADIUS-configuratievoorbeeld

Inhoud

Inleiding

Dit document legt uit hoe u een adaptieve security applicatie (ASA) kunt configureren om met een Microsoft Windows 2008 Network Policy Server (NPS) te communiceren met het RADIUS-protocol, zodat de bestaande Cisco VPN-gebruikers van client/AnyConnect/Clientloze WebVPN worden geauthentiseerd tegen Active Directory. NPS is een van de serverrollen die door Windows 2008 Server worden aangeboden. Het staat gelijk aan Windows 2003 Server, IAS (Internet Verificatieservice), die de implementatie van een RADIUS-server is om externe inbelgebruikersverificatie te leveren. Op dezelfde manier is NPS in Windows 2008 Server de implementatie van een RADIUS-server. De ASA is een RADIUS-client naar een NPS RADIUS-server. ASA stuurt RADIUS-verificatieverzoeken namens VPN-gebruikers en NPS authenticeert ze tegen Active Directory.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

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

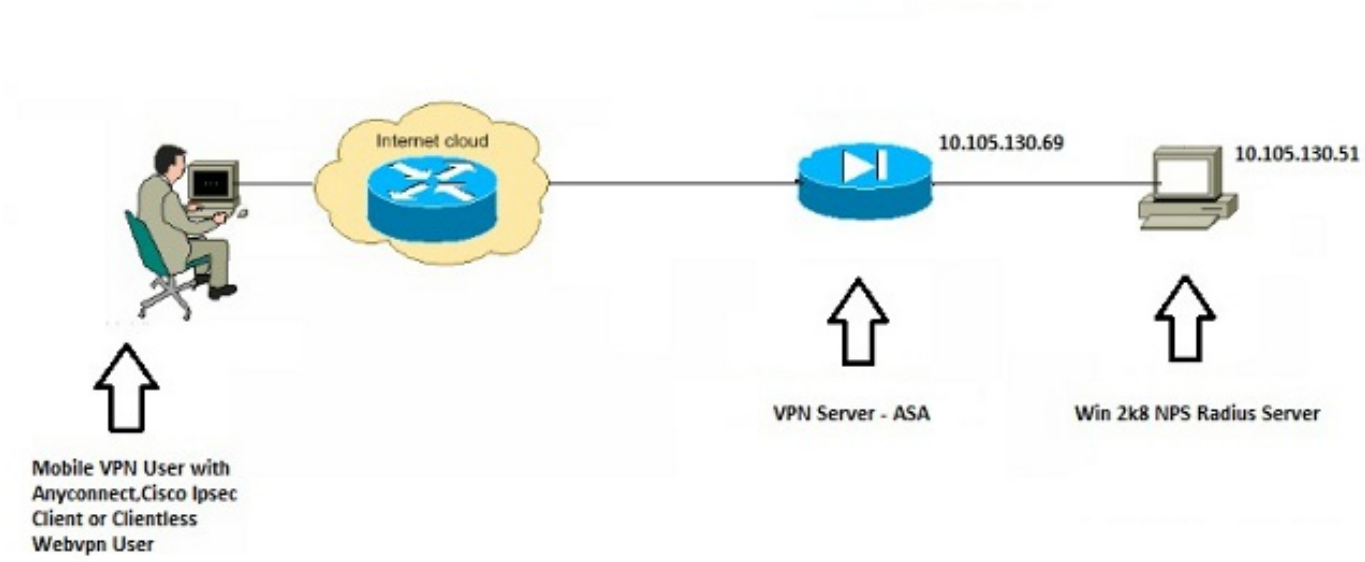
- ASA dat versie 9.1(4) draait
- Windows 2008 R2-server met geïntegreerde services en NPS-rol geïnstalleerd

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.

Configureren

> Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

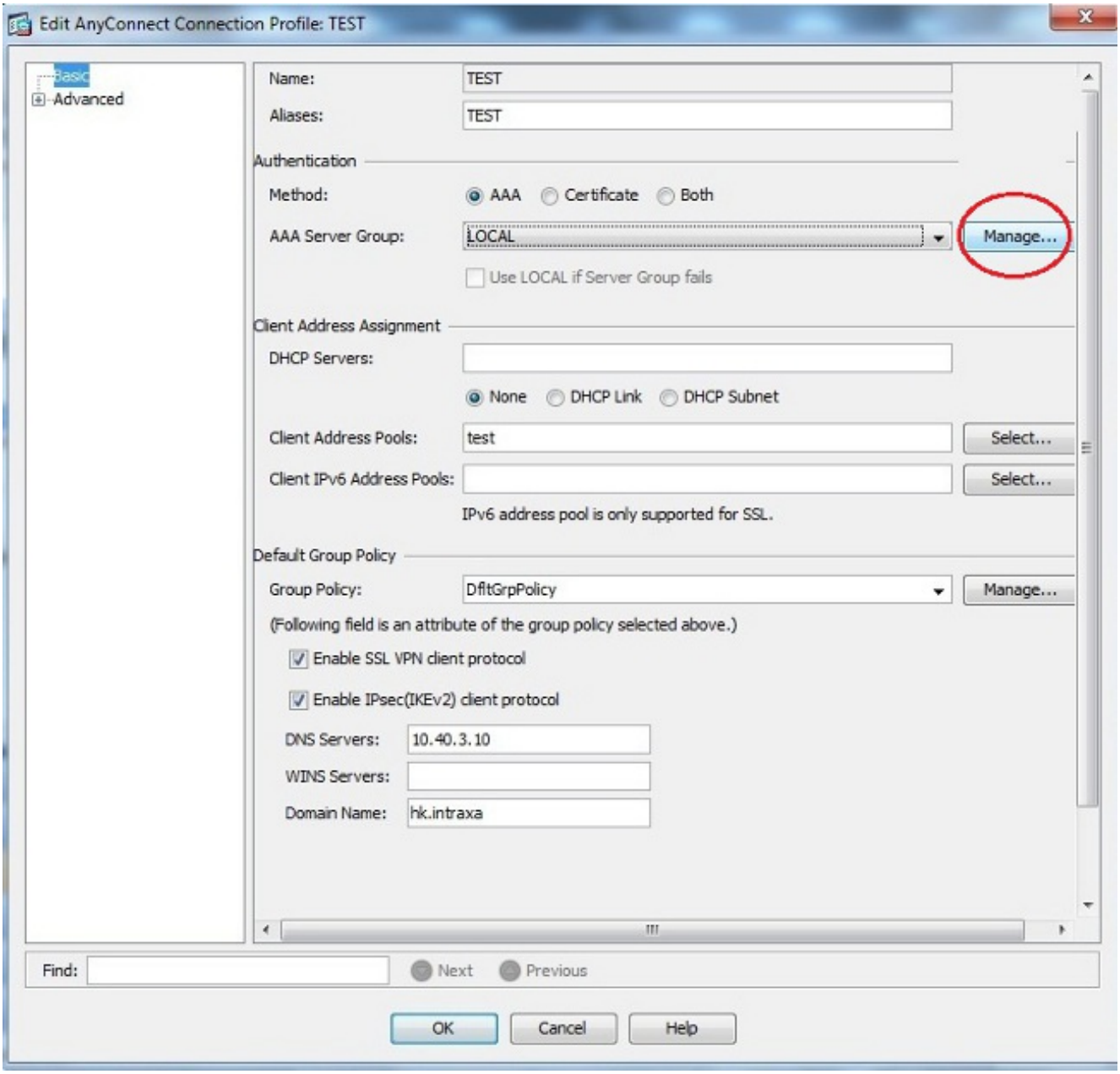
Netwerkdiagram



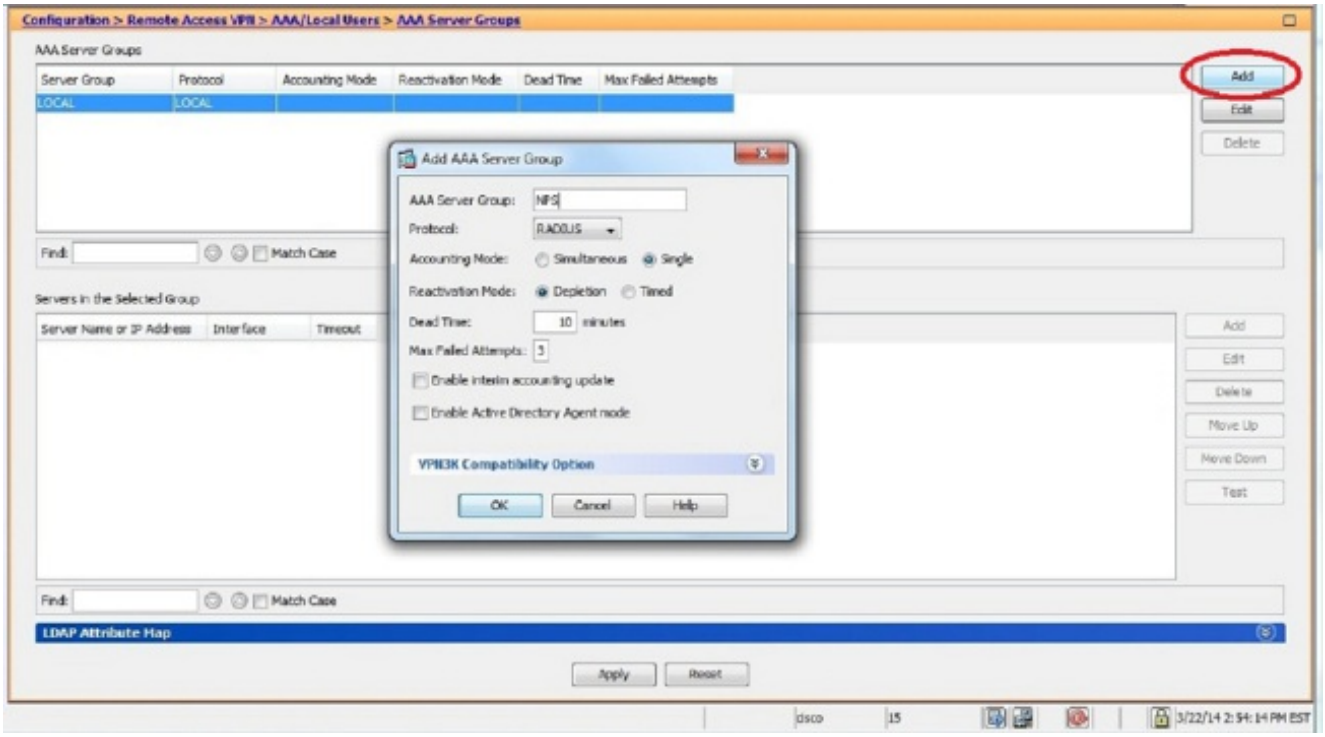
Configuraties

ASDM-configuratie

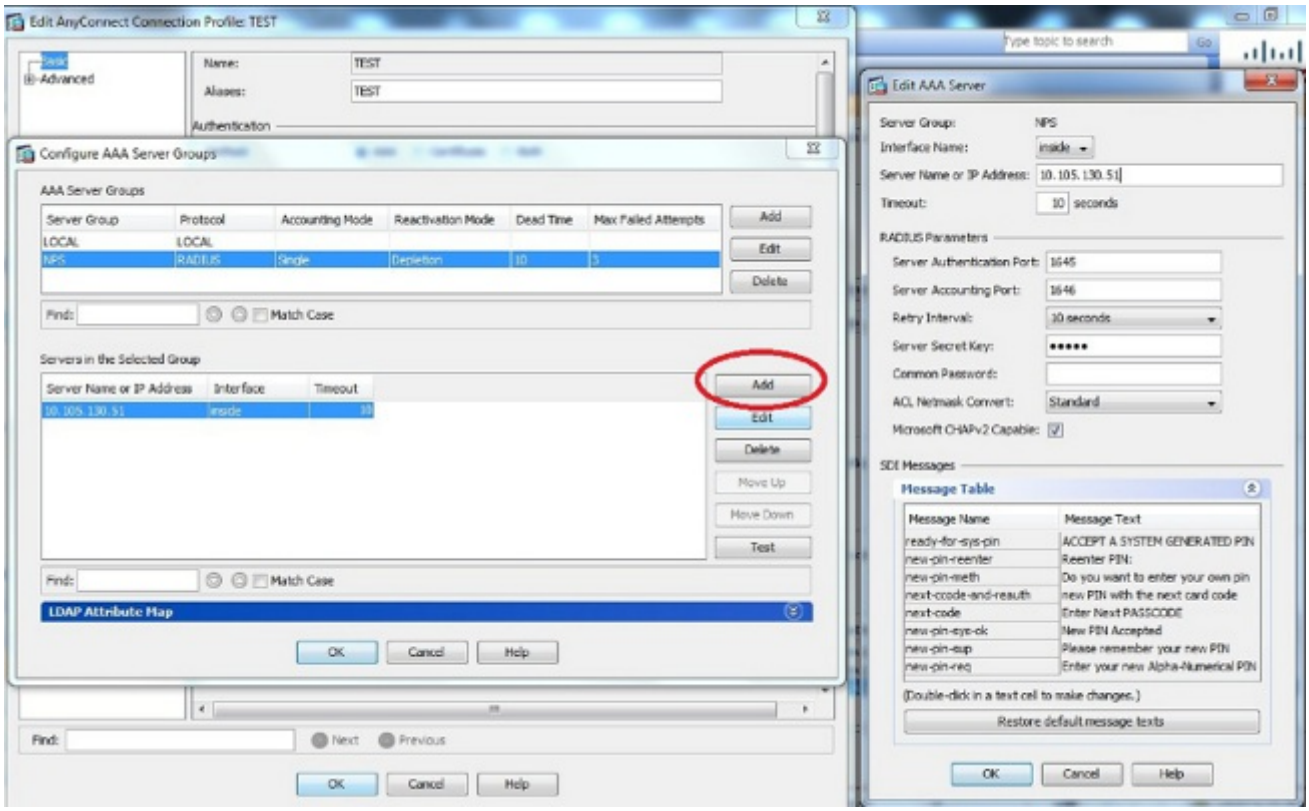
1. Kies de tunnelgroep waarvoor NPS-verificatie vereist is.
2. Klik op **Bewerken** en kies **basisstation**.
3. Klik in het gedeelte Verificatie op **beheren**.



4. Klik in het gedeelte AAA-servergroepen op **Toevoegen**.
5. Voer in het veld AAA-servergroep de naam van de servergroep in (bijvoorbeeld NPS).
6. Kies in de vervolgkeuzelijst Protocol de optie **RADIUS**.
7. Klik op
   OK.

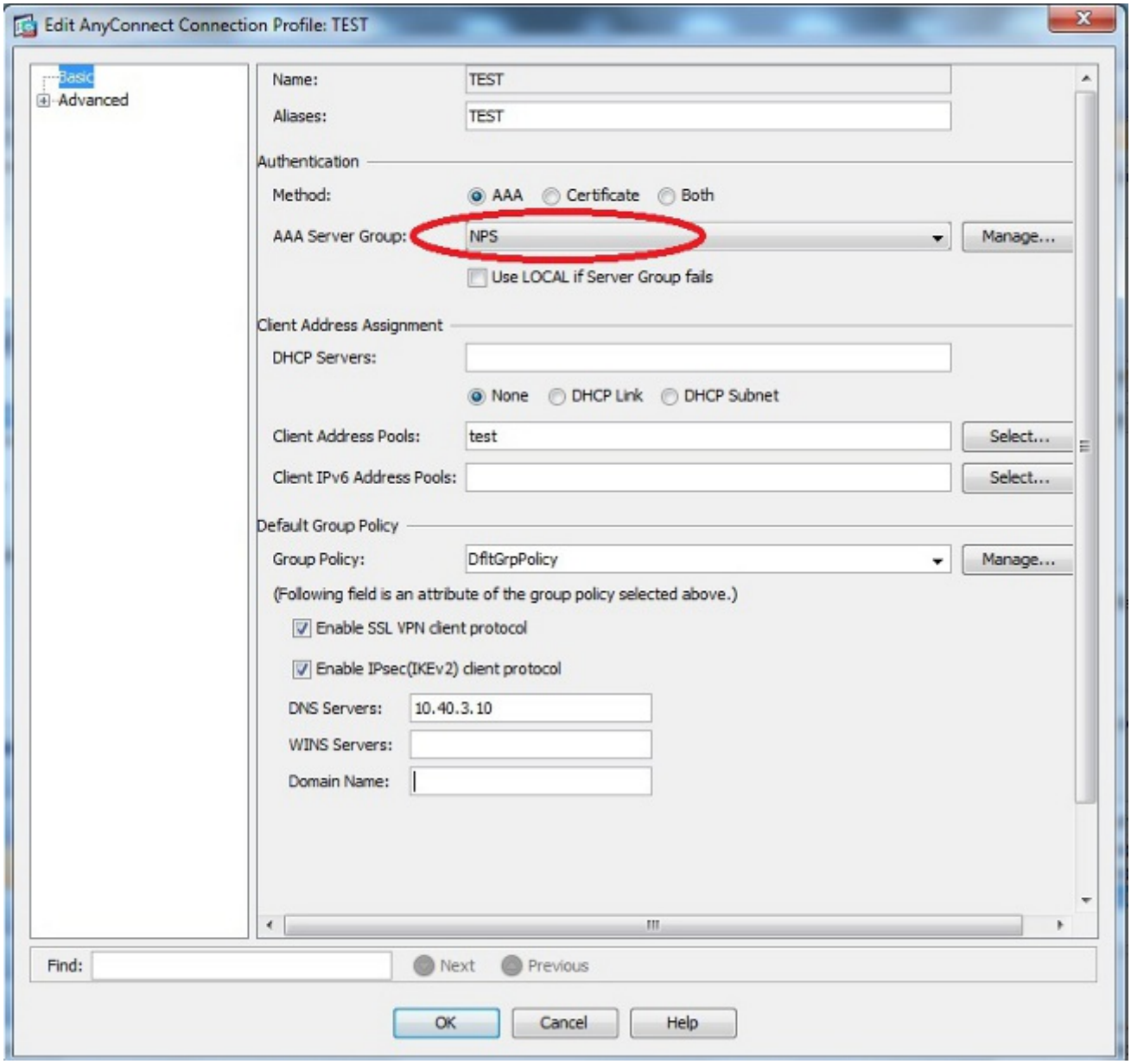


8. Kies in het gedeelte Geselecteerde groep de toegevoegde AAA-servergroep en klik op **Toevoegen**.
9. Voer in het veld Naam of IP-adres van de server het IP-adres in.
10. Voer in het veld Beveiligde sleutel van de server de geheime sleutel in.
11. Verlaat de Port voor serververificatie en de poortvelden voor serveraccounting bij de standaardwaarde tenzij de server op een andere poort luistert.
12. Klik op **OK**.
13. Klik op **OK**.



14. Kies in de vervolgkeuzelijst AAA-servergroep de groep (NPS in dit voorbeeld) die in de vorige stappen is toegevoegd.
15. Klik op

OK.



CLI-configuratie

```
aaa-server NPS protocol radius
aaa-server NPS (inside) host 10.105.130.51
 key *****

tunnel-group TEST type remote-access
tunnel-group TEST general-attributes
 address-pool test
 authentication-server-group (inside) NPS
tunnel-group TEST webvpn-attributes
 group-alias TEST enable

ip local pool test 192.168.1.1-192.168.1.10 mask 255.255.255.0
```

Standaard gebruikt de ASA het PAP-verificatietype (unencryptie Password Authentication Protocol). Dit betekent niet dat de ASA het wachtwoord in onbewerkte tekst verstuurt wanneer het de RADIUS-aanvraag verzonden wordt. Het wachtwoord voor het splitsen is eerder versleuteld met het gedeelde geheim van de RADIUS.

Als het wachtwoordbeheer onder de tunnelgroep is ingeschakeld, gebruikt ASA het MSCHAP-v2-authenticatietype om het Plaintext wachtwoord te versleutelen. Zorg er in dat geval voor dat het aanvinkvakje **Microsoft CHAPv2 Capable** is ingeschakeld in het venster AAA-server bewerken dat is geconfigureerd in het ASDM-configuratiescherm.

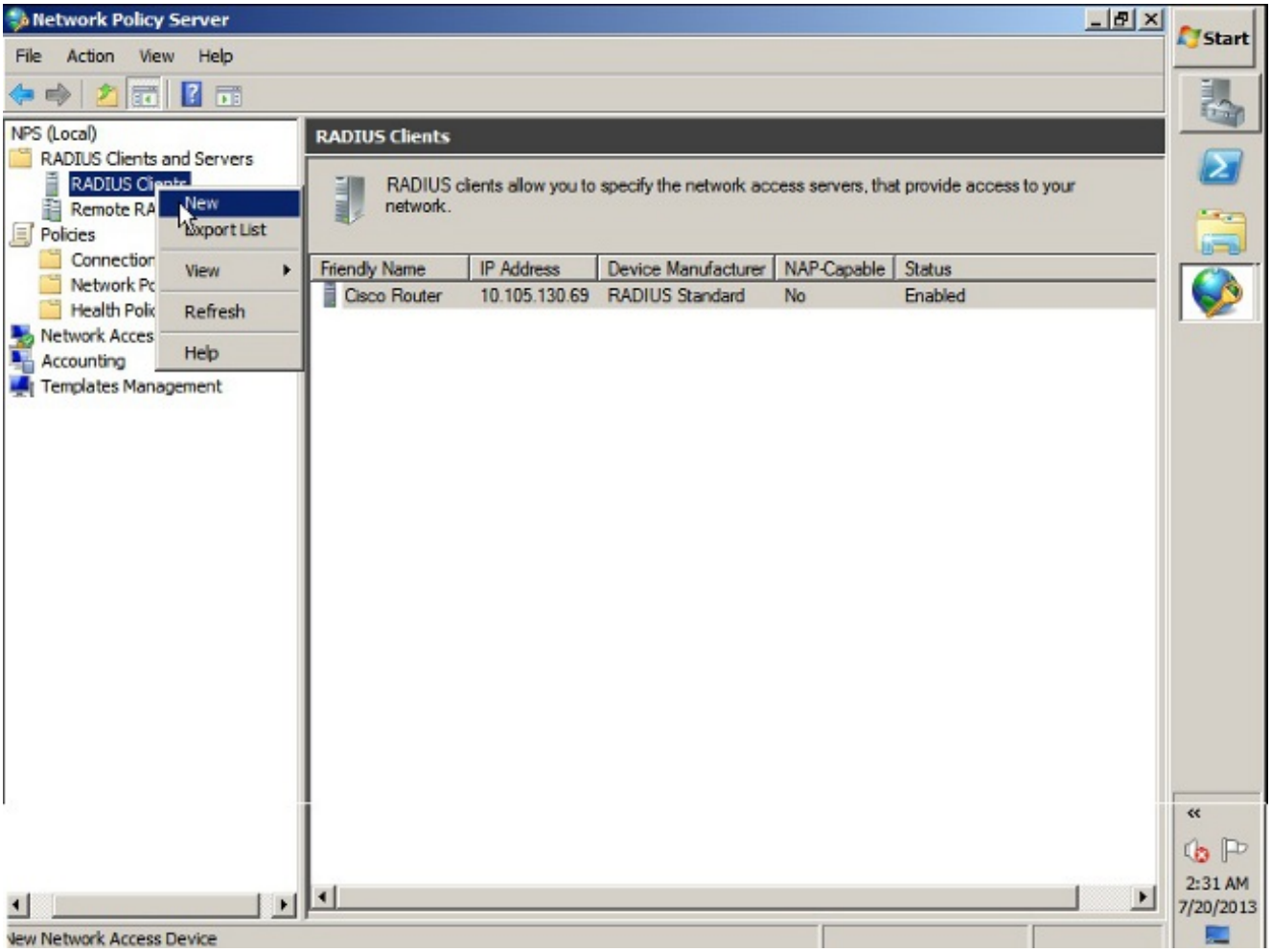
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> Opmerking: De opdracht **voor** de **verificatie van de testserver** gebruikt PP altijd. Alleen wanneer een gebruiker een verbinding naar tunnelgroep initieert met een wachtwoord-beheer dat is ingeschakeld, gebruikt de ASA MSCHAP-v2. Ook wordt de 'password-management [password-expo-in-dagen]' optie alleen ondersteund met Lichtgewicht Directory Access Protocol (LDAP). RADIUS biedt deze optie niet aan. U ziet dat het wachtwoord verloopt optie wanneer het wachtwoord al is verlopen in de actieve map.

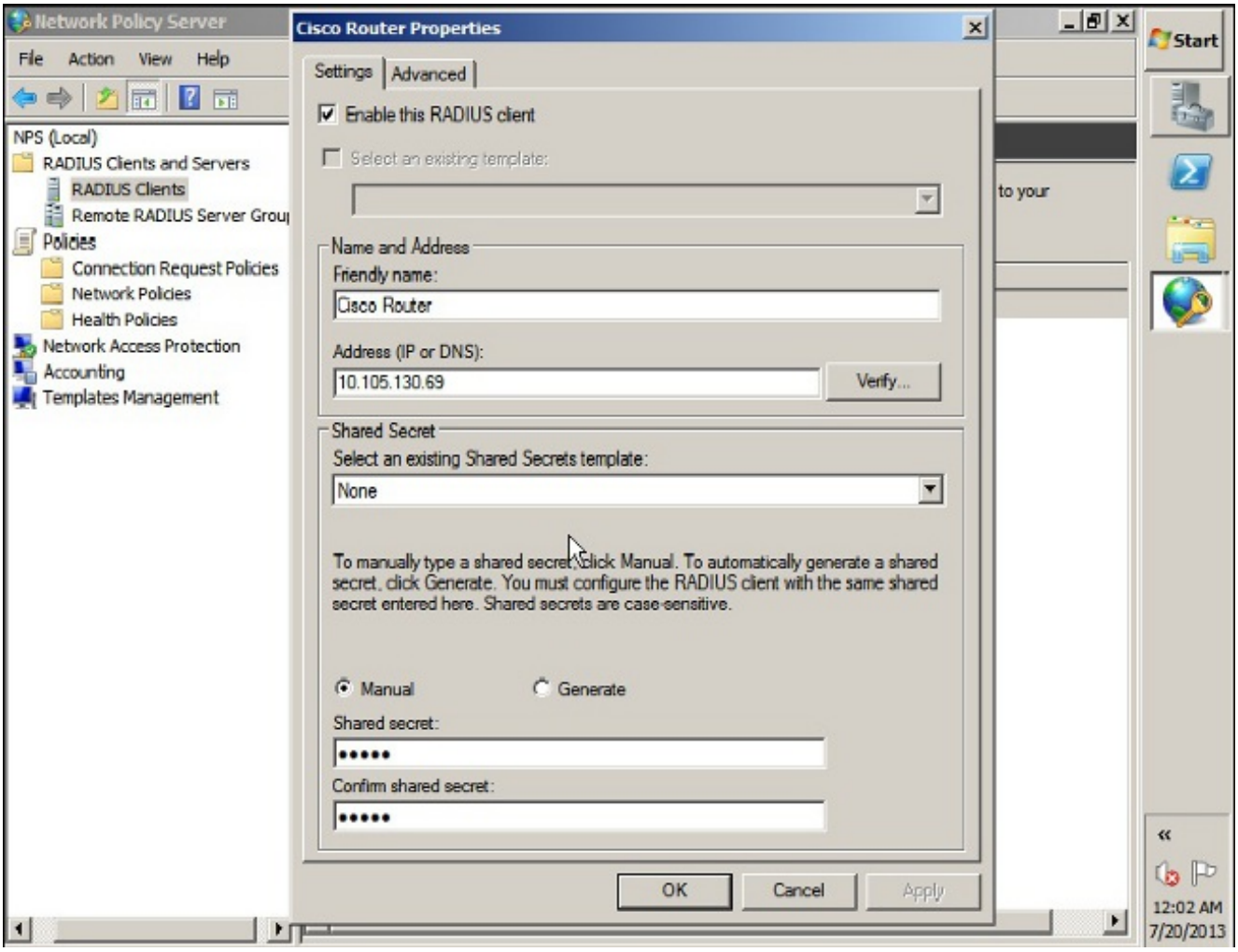
Windows 2008-server met NPS-configuratie

De NPS Server Rol moet op de Windows 2008 server geïnstalleerd en uitgevoerd worden. Als dit niet het geval is, kies **Start > Administratieve Gereedschappen > Server Rollen > Rol services toevoegen**. Kies de netwerkbeleidsserver en installeer de software. Nadat de NPS Server Rol is geïnstalleerd, voltooi deze stappen om NPS te vormen om de verzoeken van de ASA om de Verificatie van RADIUS te aanvaarden en te verwerken van de ASA te accepteren:

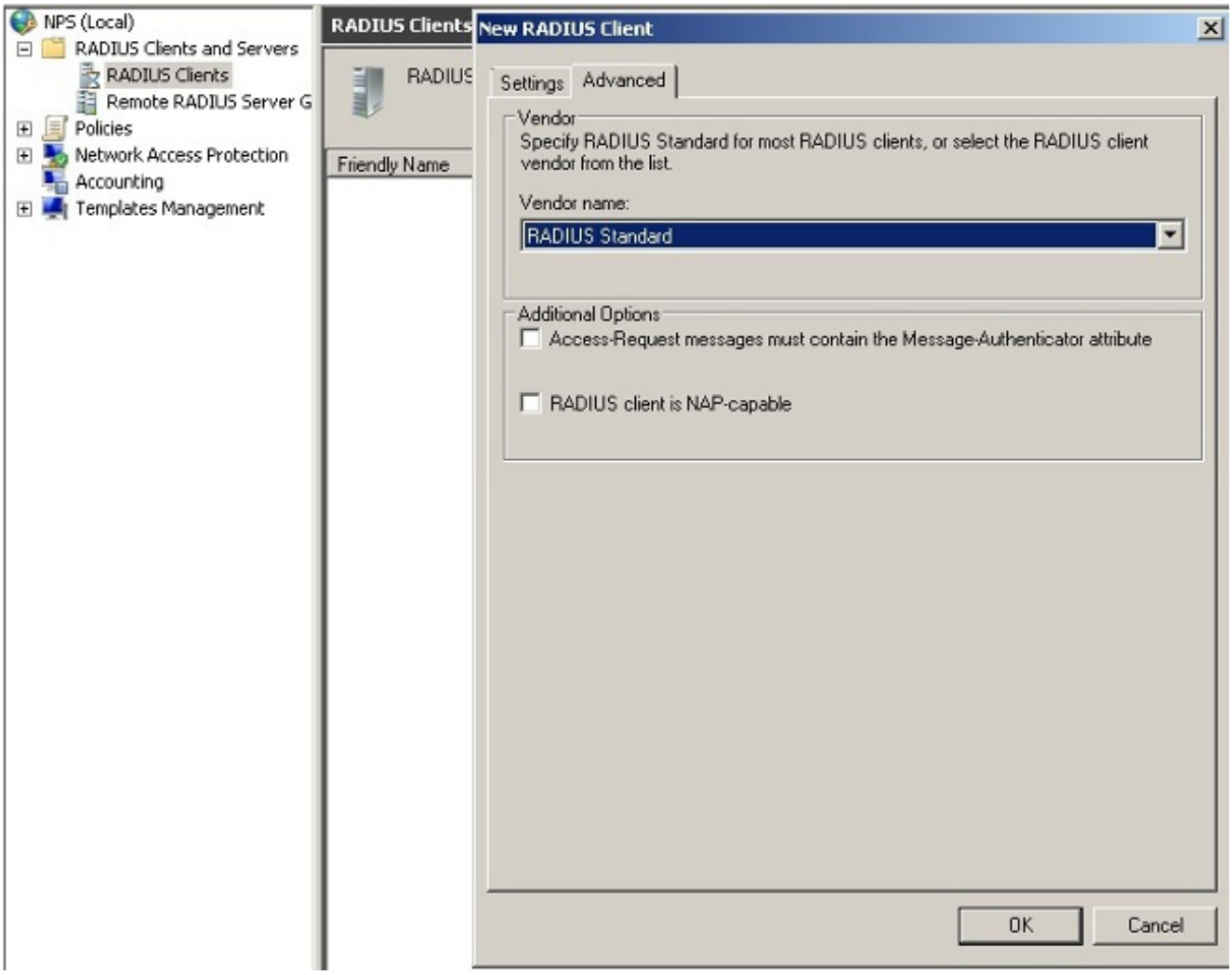
1. Voeg de ASA als een RADIUS-client toe in de NPS-server. Kies **Administratieve tools > Netwerkbeleidsserver.**Klik met de rechtermuisknop op **RADIUS-clients** en kies **Nieuw**.



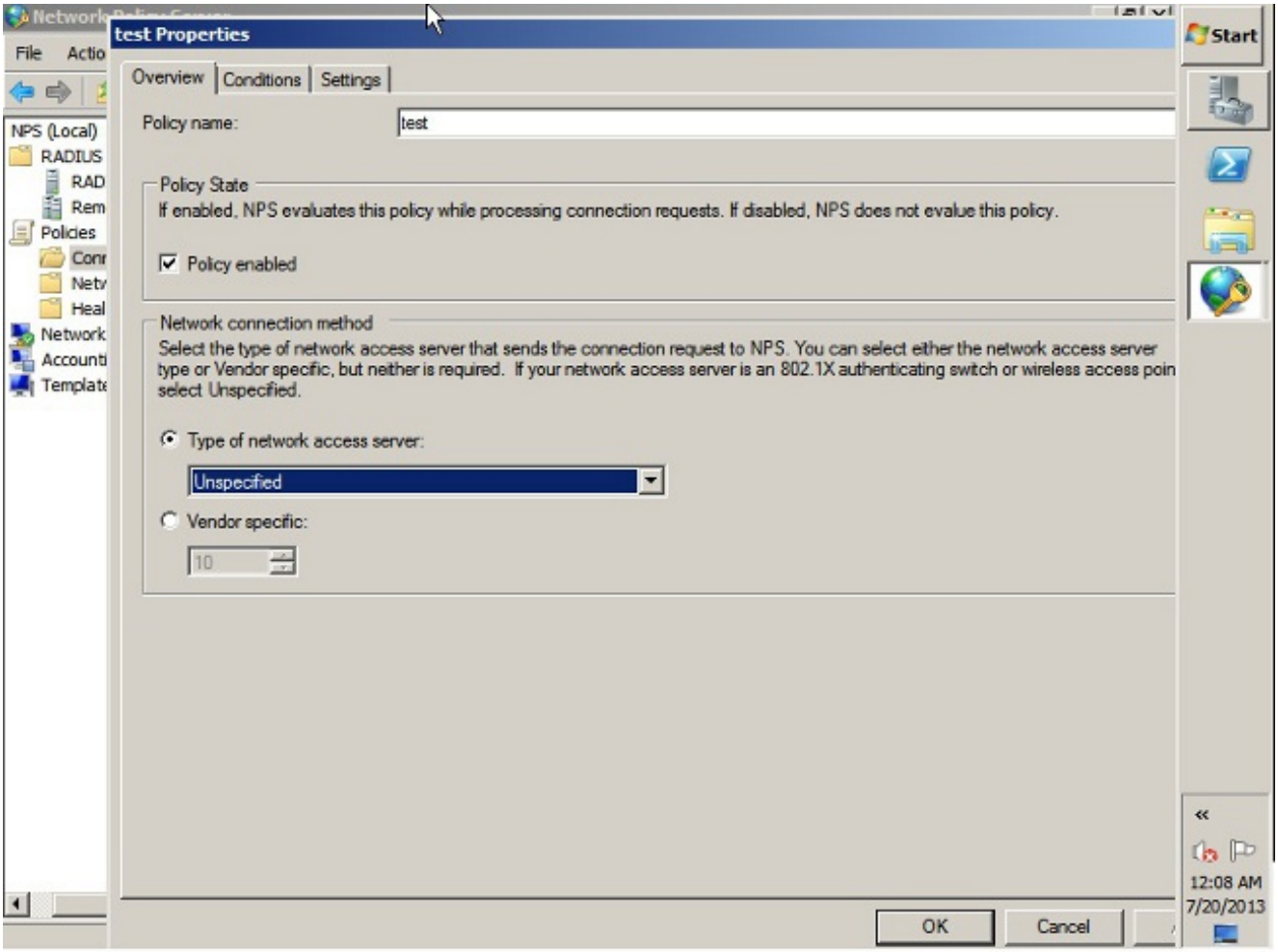
Voer een familienaam, een adres (IP of DNS) en een gedeeld geheim in die op de ASA is ingesteld.



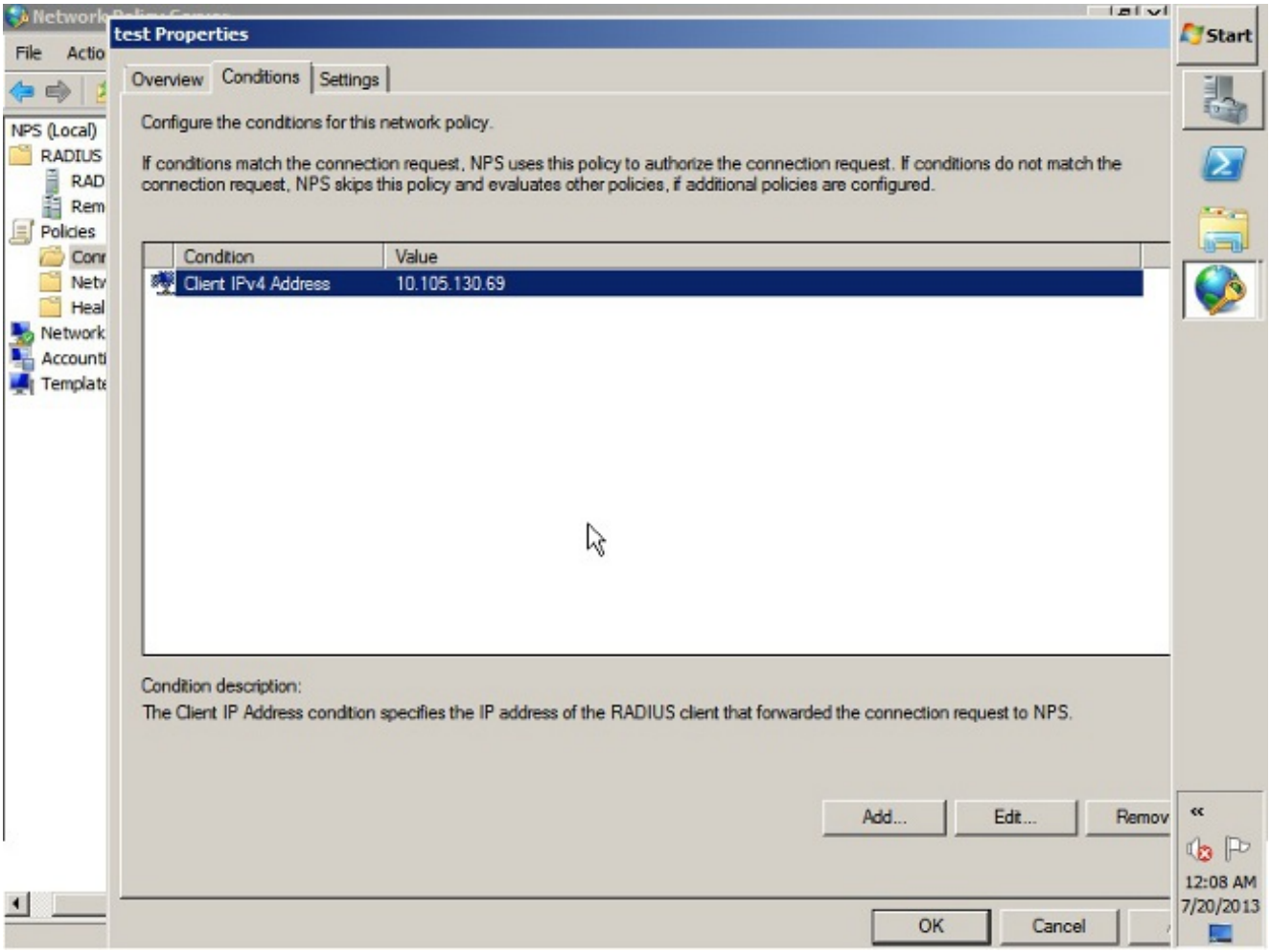
Klik op het tabblad **Geavanceerd**.Kies in de vervolgkeuzelijst Naam van verkoper de **RADIUS-standaard**.Klik op
OK.



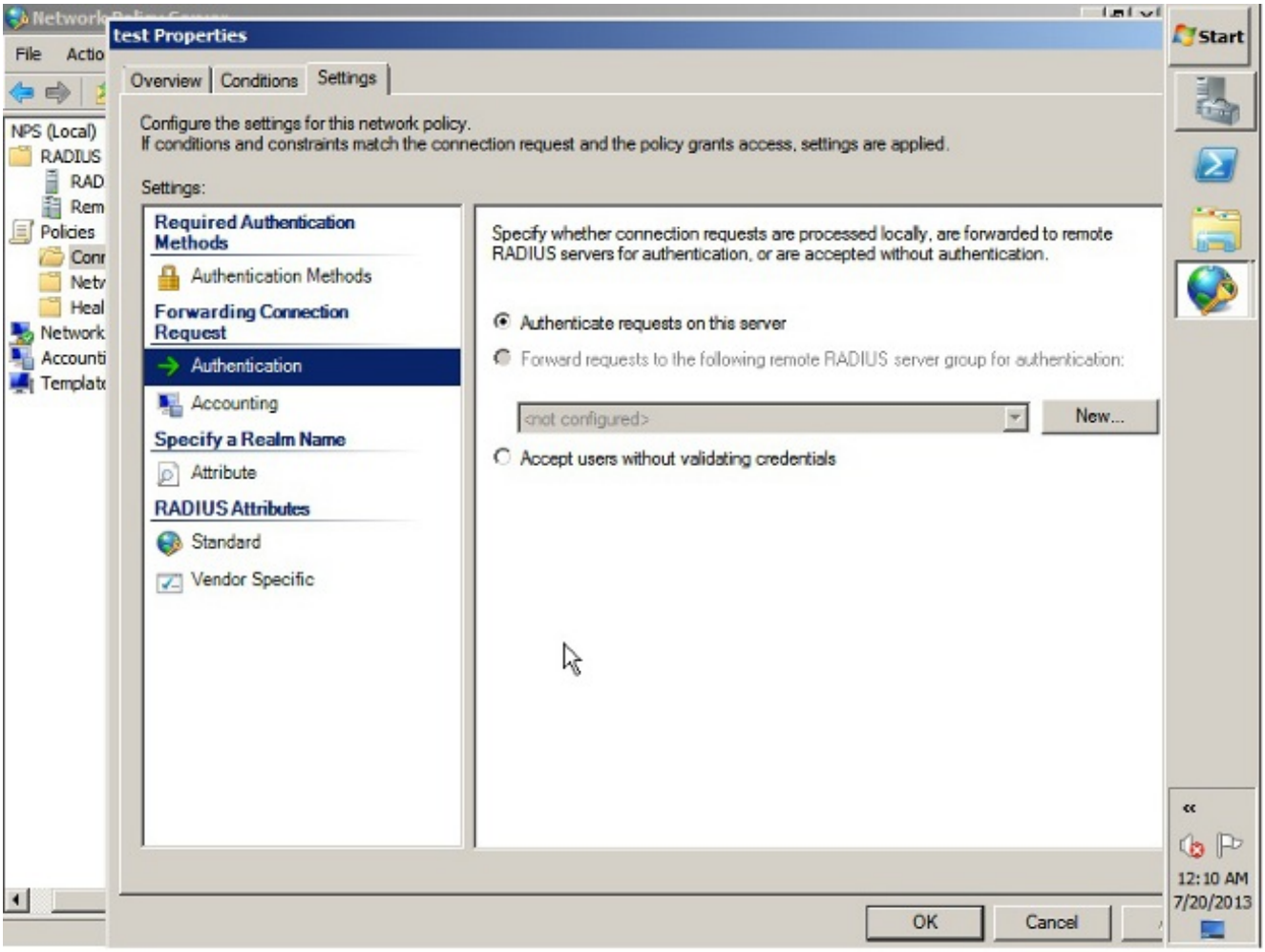
2. Maak een nieuw beleid van de verbindingsaanvraag voor VPN-gebruikers. Het doel van het beleid van de verbindingsaanvraag is om te specificeren of de verzoeken van RADIUS-klanten lokaal moeten worden verwerkt of naar externe RADIUS-servers moeten worden doorgestuurd. Onder NPS > Beleid, klikt u met de rechtermuisknop op **Aanvraagbeleid** en voert u een nieuw beleid.Kies in de vervolgkeuzelijst Type of Network Access Server de optie **Niet gespecificeerd**.



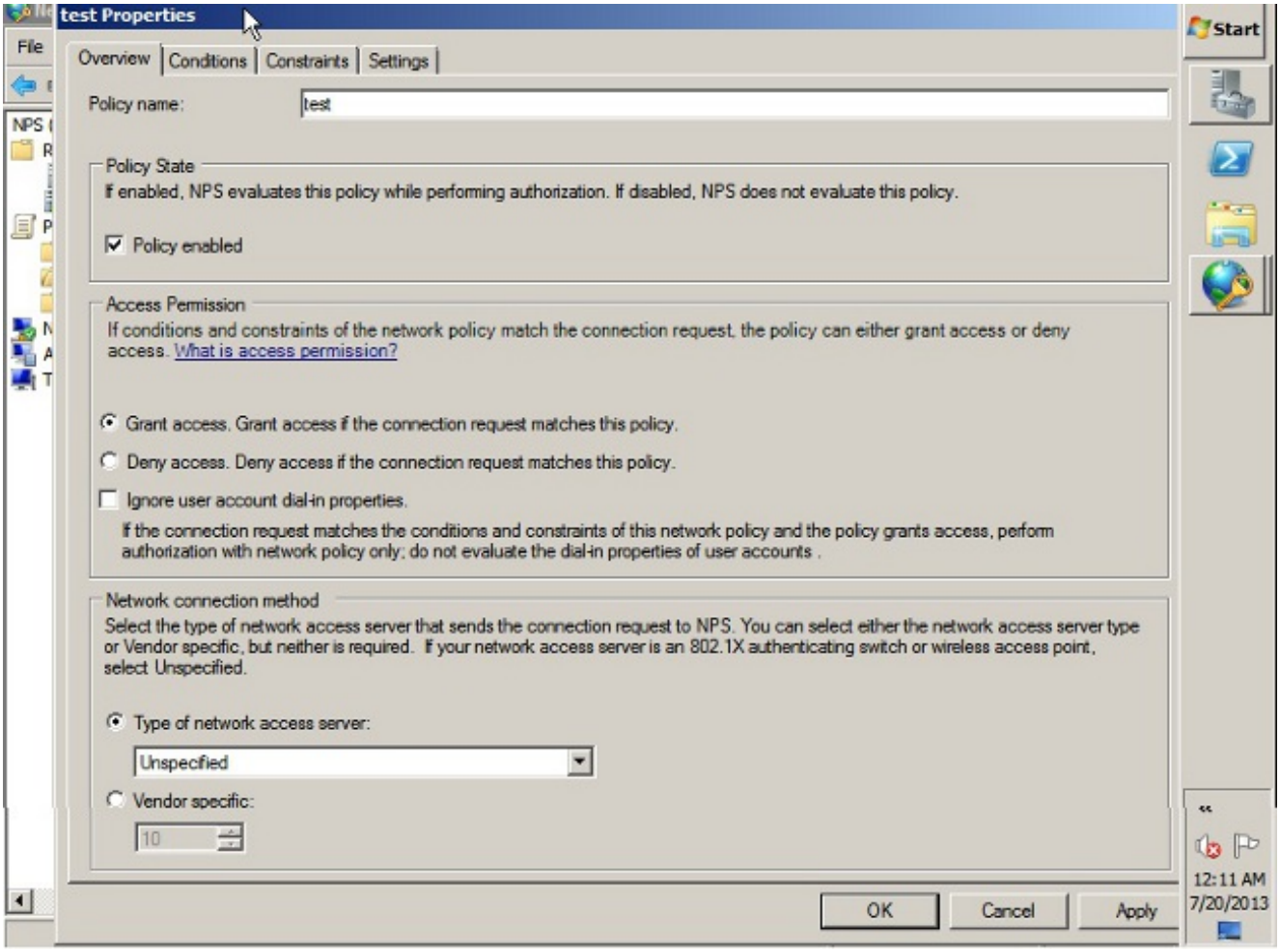
Klik op het tabblad **Voorwaarden**.Klik op **Toevoegen**.Voer het IP-adres van de ASA in als voorwaarde voor 'Client IPv4-
adres'.



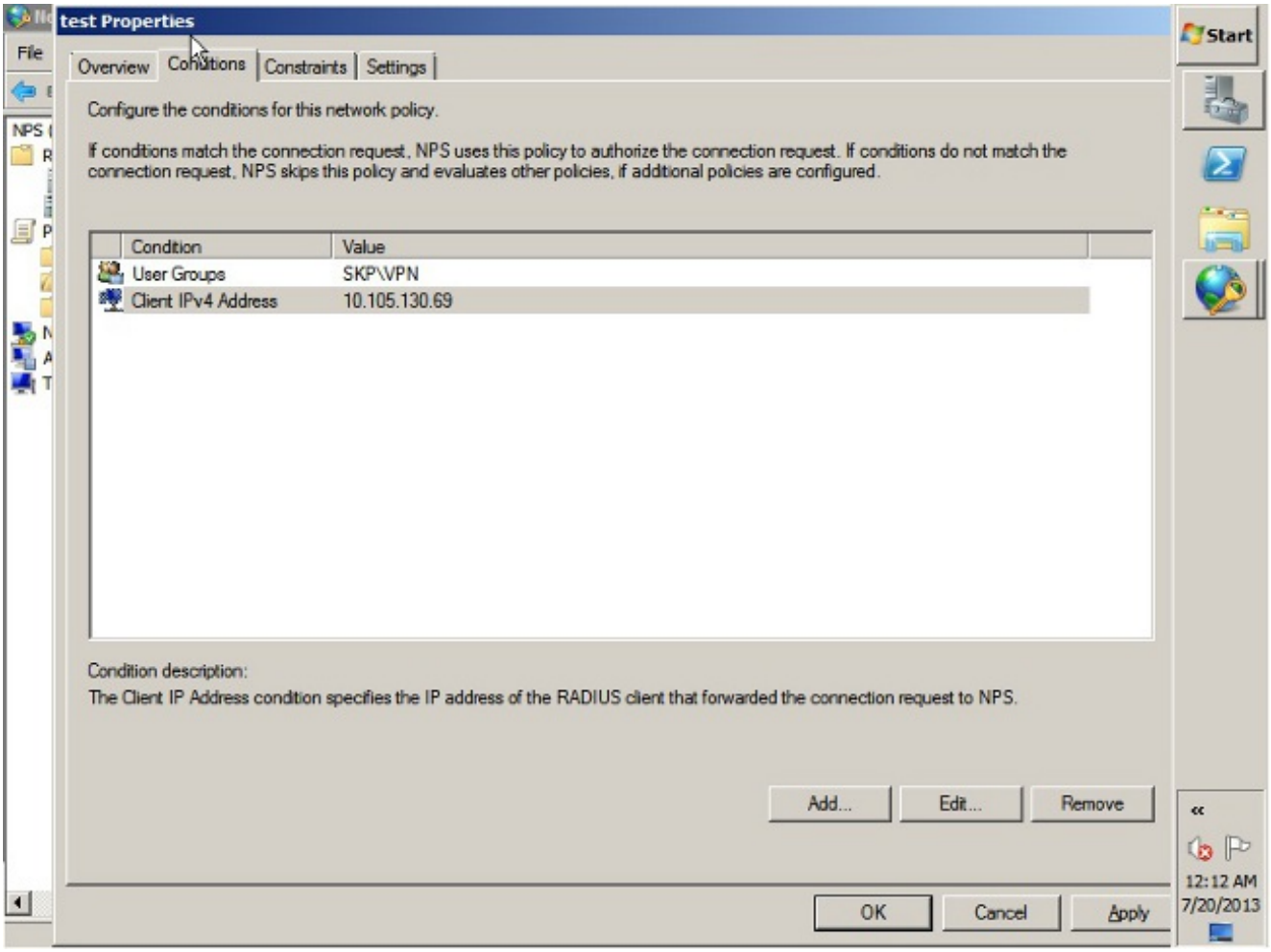
Klik op het tabblad **Instellingen**.Selecteer onder Doorsturen van een verbindingsaanvraag de optie **Verificatie**. Verzeker u dat de Authenticate aanvragen op deze server radioknop geselecteerd is.Klik op
OK.



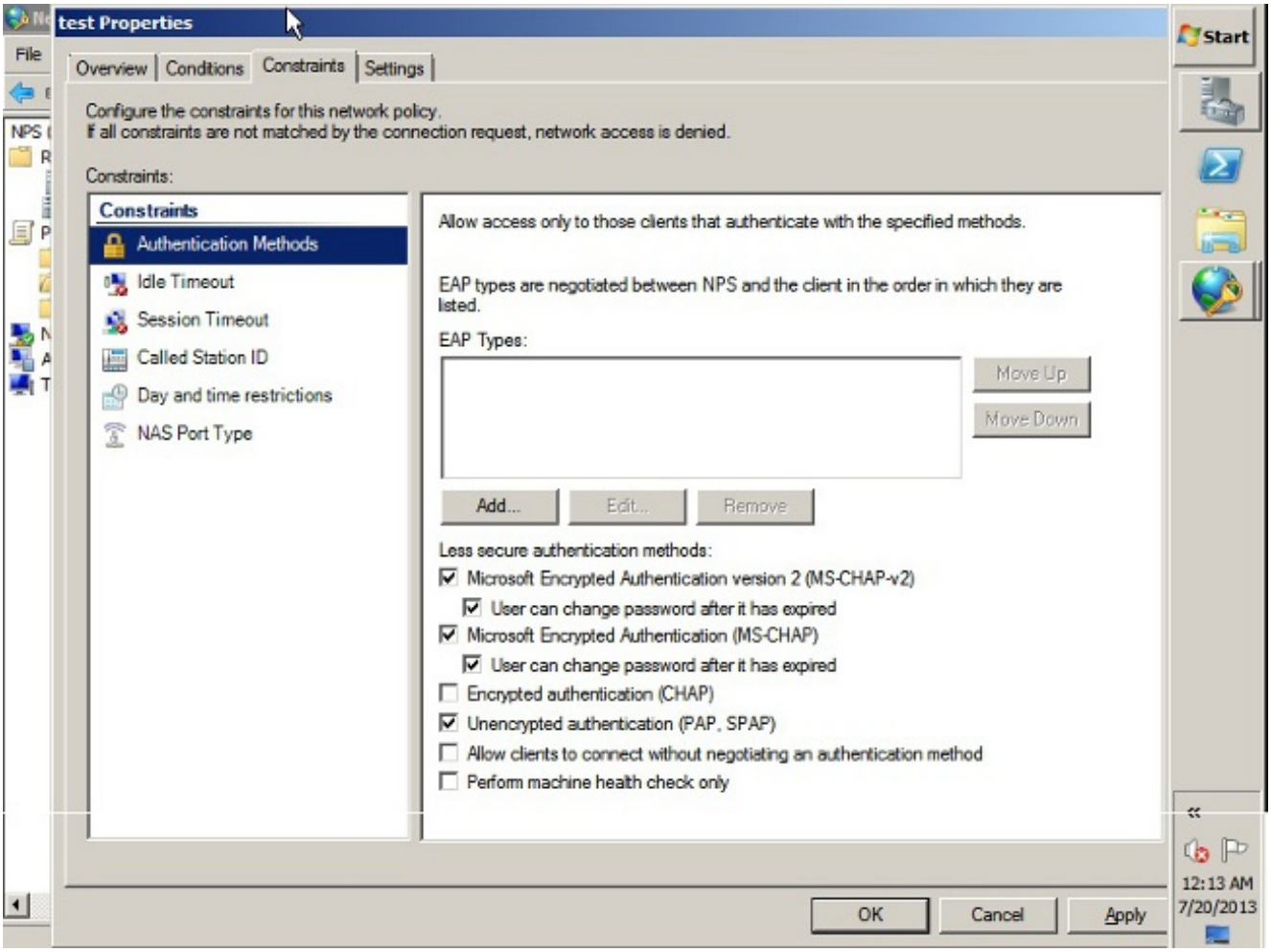
3. Voeg een Netwerkbeleid toe waar u kunt specificeren welke gebruikers mogen authenticeren.U kunt bijvoorbeeld actieve gebruikersgroepen van de map als voorwaarde toevoegen. Alleen gebruikers die tot een bepaalde groep van Windows behoren, zijn onder dit beleid voor authentiek verklaard.Kies onder NPS **beleid**.Klik met de rechtermuisknop op **Netwerkbeleid** en maak een nieuw beleid.Zorg ervoor dat de selectieknop voor Grant Access is geselecteerd.Kies in de vervolgkeuzelijst Type of Network Access Server de optie **Niet gespecificeerd**.



Klik op het tabblad **Voorwaarden**.Klik op **Toevoegen**.Voer het IP-adres van de ASA in als voorwaarde voor IPv4-adres van de client.Voer de gebruikersgroep Active Directory in die VPN-gebruikers
bevat.



Klik op het tabblad **Beperkingen**.Kies **verificatiemethoden**.Verzeker u dat het vakje UnEncryption (PAP, SPAP) is ingeschakeld.Klik op
OK.

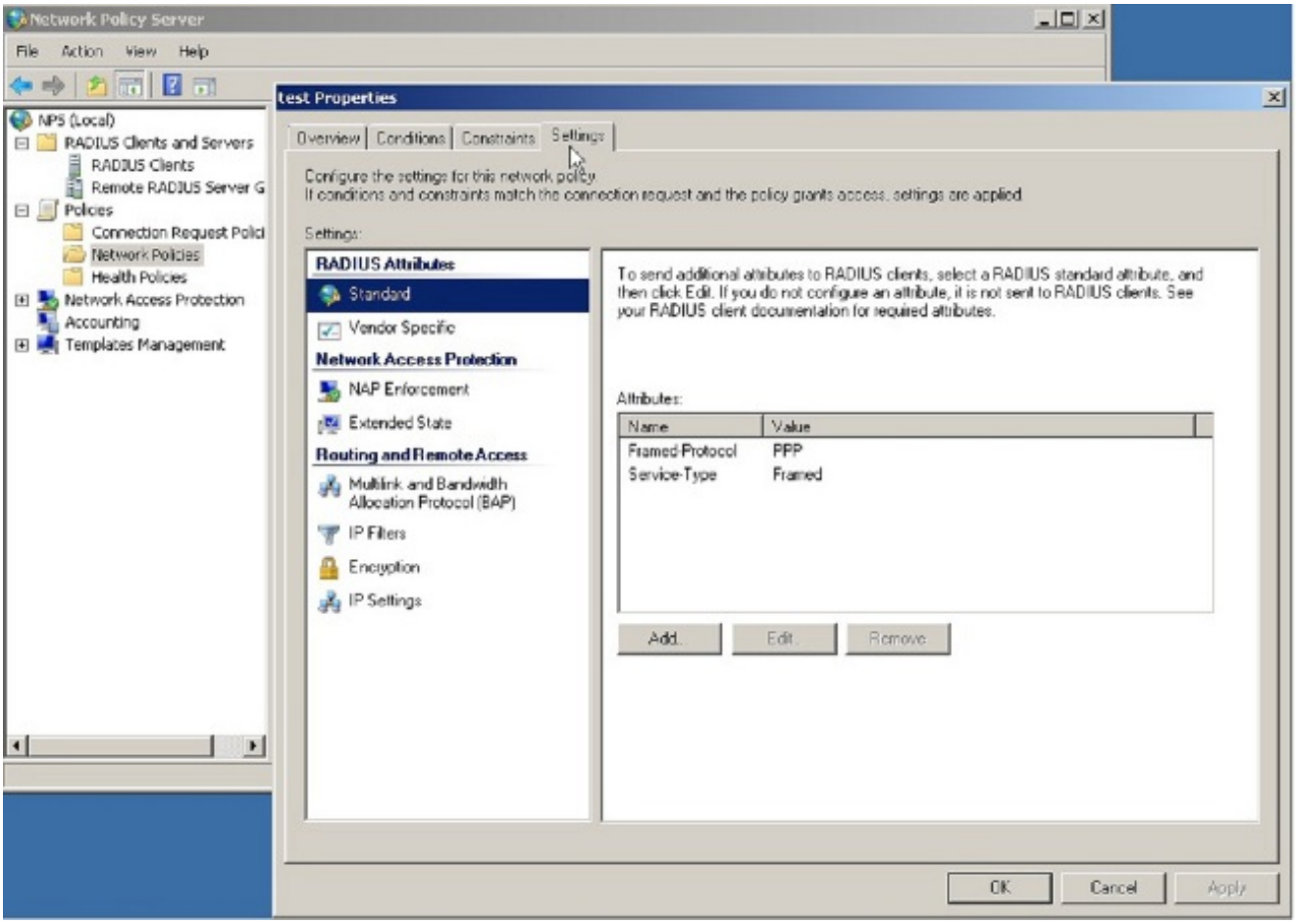


Pass Group-beleidskenmerk (kenmerk 25) van de NPS RADIUS-server

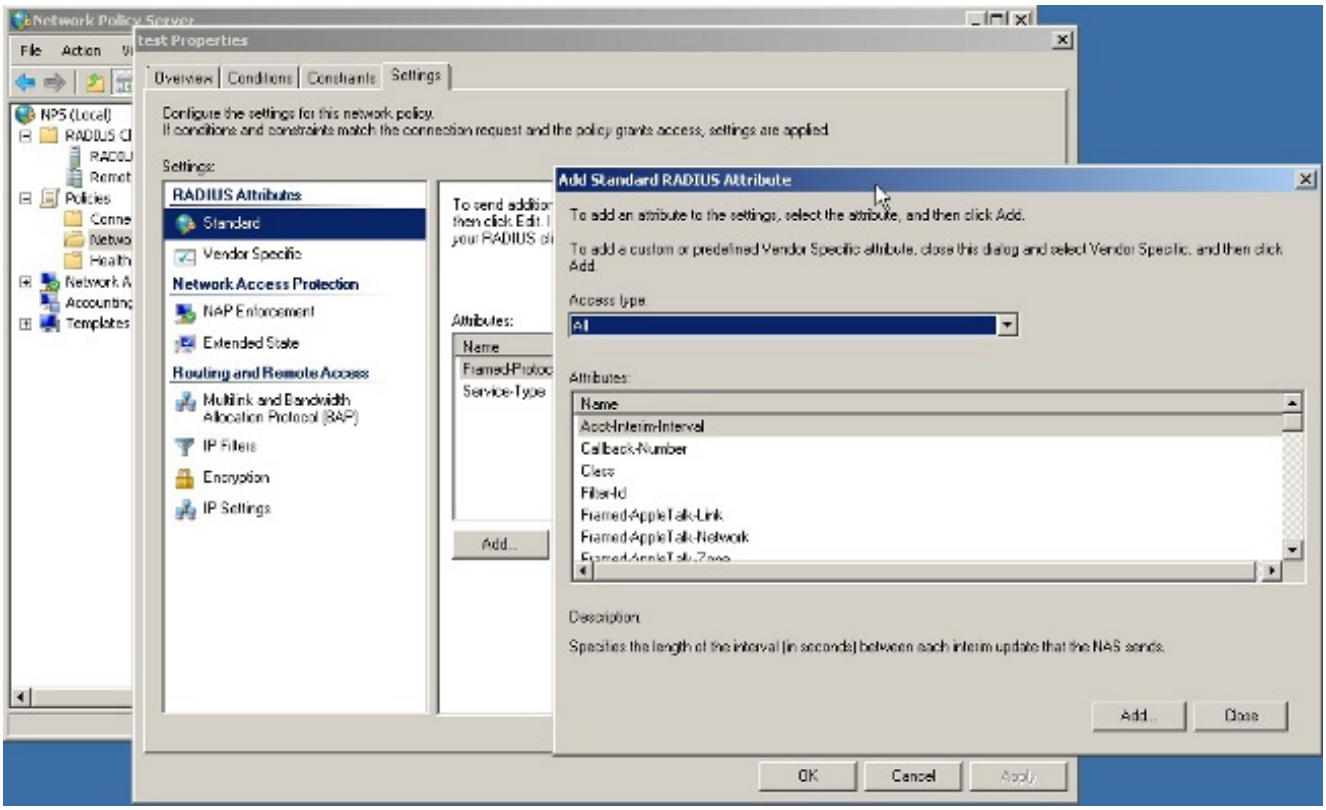
Als het groepsbeleid dynamisch met de NPS RADIUS-server aan de gebruiker moet worden toegewezen, kan de RADIUS-eigenschap (eigenschap 25) van het groepsbeleid worden gebruikt.

Voltooi deze stappen om de RADIUS-eigenschap 25 voor dynamische toewijzing van een groepsbeleid naar de gebruiker te sturen.

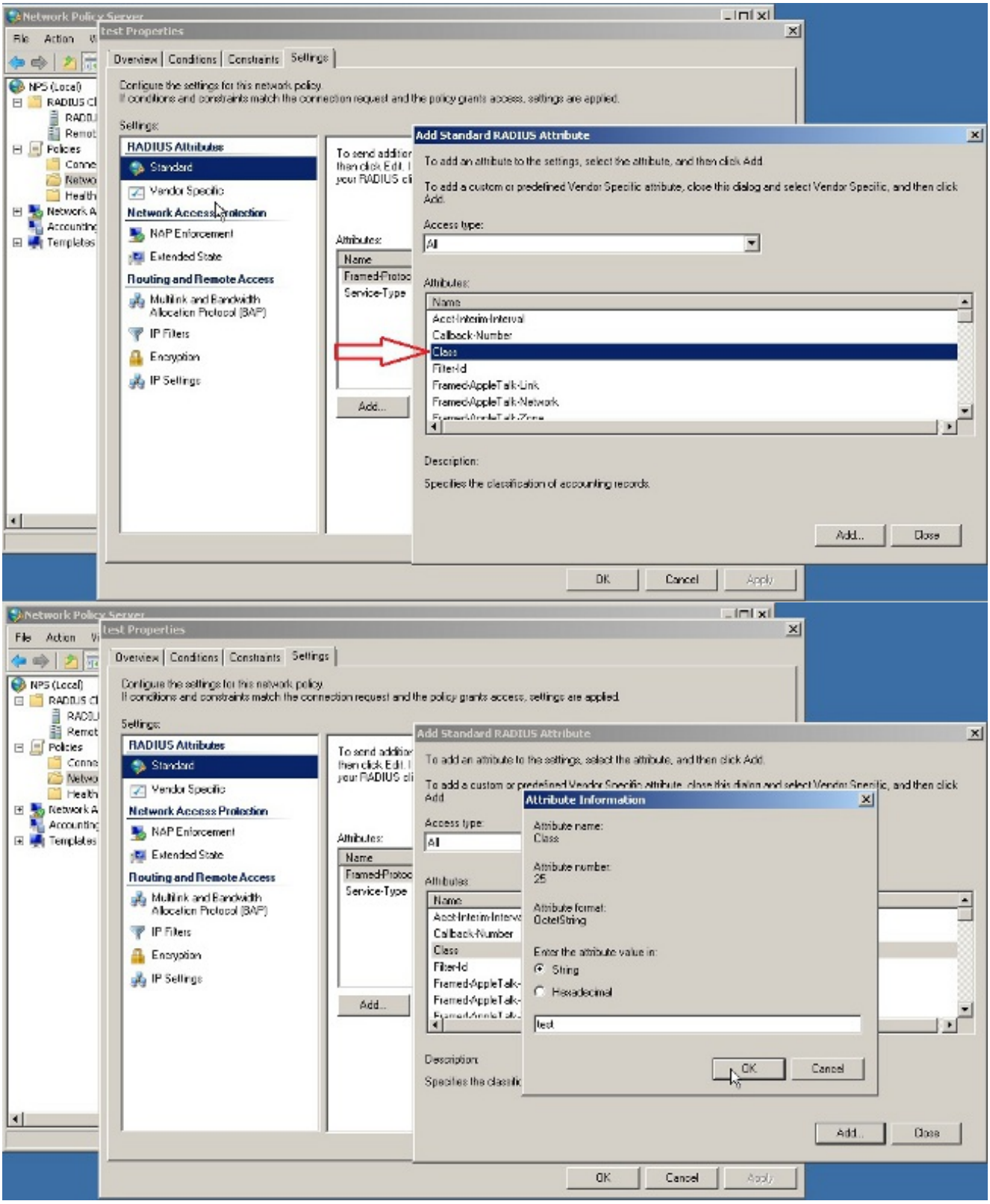
1. Klik na het toevoegen van het netwerkbeleid met de rechtermuisknop op het gewenste netwerkbeleid en klik vervolgens op het tabblad **Instellingen**.



2. Kies **RADIUS-kenmerken > Standaard**. Klik op **Toevoegen**. Laat het Access-type als alles achter.



3. Kies in het vak Eigenschappen **Class** en klik op **Add**. Voer de waarde van de eigenschap in, dat wil zeggen, de naam van het groepsbeleid als string. Onthoud dat een groepsbeleid met deze naam in de ASA moet worden geconfigureerd. Dit is zo dat de ASA deze aan de VPN sessie toewijst nadat deze eigenschap in de RADIUS-respons wordt ontvangen.



Verifiëren

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

> Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

ASA Debugs

Schakel **de straal** op de ASA in.

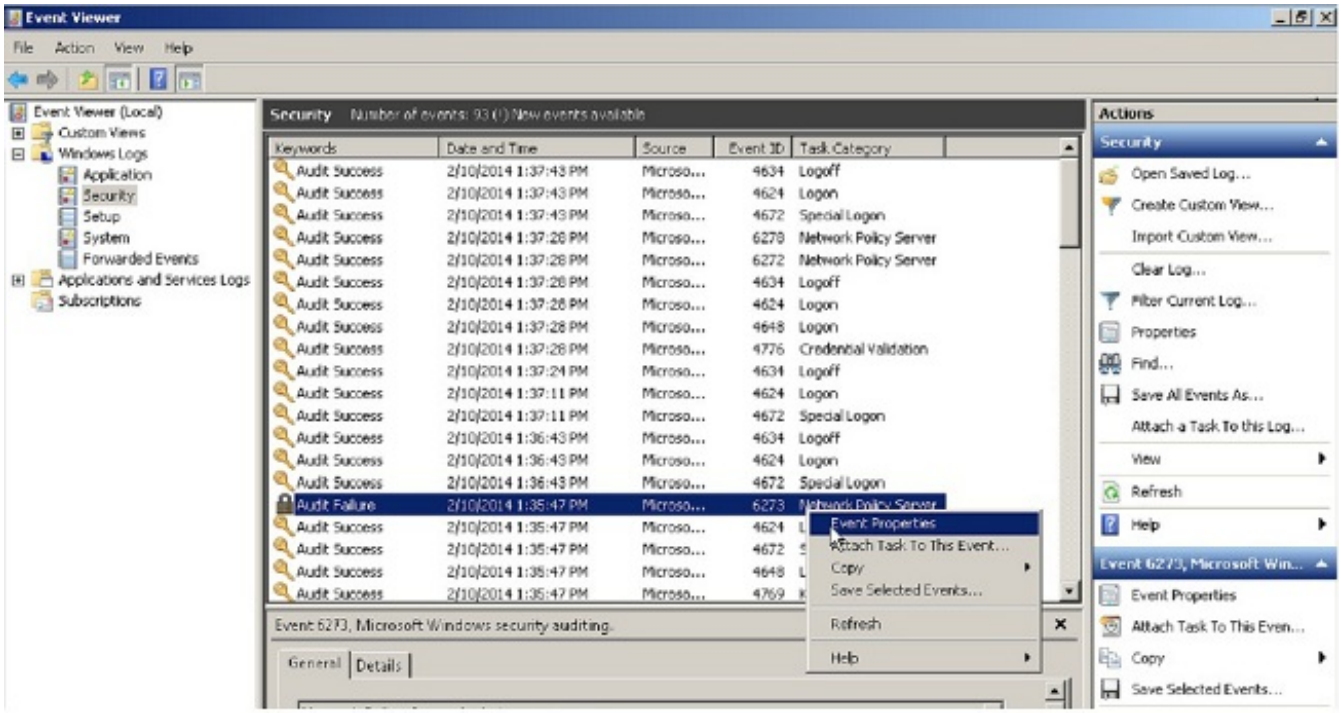
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password
add_req 0x787a6424 session 0x80000001 id 8
RADIUS_REQUEST
radius.c: rad_mkpkt

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 65).....
01 08 00 41 c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f    |  ...A.....~m...
40 50 a8 36 01 09 76 70 6e 75 73 65 72 02 12 28    |  @P.6..vpnuser..(
c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04    |  .h.........Z.oC.
06 0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00    |  ..i........=....
05                                                 |  .

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 8 (0x08)
Radius: Length = 65 (0x0041)
Radius: Vector: C41BAB1AE37E6D12DA876F7F4050A836
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
76 70 6e 75 73 65 72                               |  vpnuser
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
28 c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43    |  (.h.........Z.oC
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.105.130.52 (0x0A6982DE)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
send pkt 10.105.130.51/1645
rip 0x787a6424 state 7 id 8
rad_vrfy() : response message verified
rip 0x787a6424
 : chall_state ''
 : state 0x7
 : reqauth:
    c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f 40 50 a8 36
 : info 0x787a655c
    session_id 0x80000001
    request_id 0x8
    user 'vpnuser'
    response '***'
    app 0
```

```
    reason 0
    skey 'cisco'
    sip 10.105.130.51
    type 1

RADIUS packet decode (response)

--------------------------------------
Raw packet data (length = 78).....
02 08 00 4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37    |  ...N..Kv ....+.7
bf 9a 6c 4c 07 06 00 00 00 01 06 06 00 00 00 02    |  ..lL............
19 2e 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a    |  .........7.....j
2c bf 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf    |  ,.....<..n...@..
1e 3a 18 6f 05 81 00 00 00 00 00 00 00 03          |  .:.o..........

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 8 (0x08)
Radius: Length = 78 (0x004E)
Radius: Vector: E8884B7620B6AAD30D2B9437BF9A6C4C
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 25 (0x19) Class
Radius: Length = 46 (0x2E)
Radius: Value (String) =
9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a 2c bf    |  .......7.....j,.
00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a    |  ....<..n...@...:
18 6f 05 81 00 00 00 00 00 00 00 03                |  .o..........
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x787a6424 session 0x80000001 id 8
free_rip 0x787a6424
radius: send queue empty
INFO: Authentication Successful
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

- Zorg ervoor dat de connectiviteit tussen de ASA en de NPS server goed is.Pas pakketvastlegging toe om te verzekeren de authenticatieaanvraag de ASA interface verlaat (van waar de server bereikbaar is). Bevestig dat de apparaten in het pad de UDP-poort 1645 (standaard RADIUS-verificatiepoort) niet blokkeren om er zeker van te zijn dat deze de NPS-server bereikt. Meer informatie over pakketvastlegging in de ASA is te vinden in ASA/PIX/FWSM: Packet Capture met CLI en ASDM Configuration Voorbeeld.
- Als de authenticatie nog steeds faalt, kijk dan in de evenement viewer op de windows NPS. Selecteer onder Event Viewer > Windows Logs **Security.** Zoek op het tijdstip van de authenticatieaanvraag naar gebeurtenissen die geassocieerd zijn met NPS.



Zodra u de eigenschappen van een gebeurtenis opent, dient u de reden voor de mislukking te kunnen zien zoals in het voorbeeld wordt getoond. In dit voorbeeld werd PAP niet gekozen als het authenticatietype onder Netwerkbeleid. Het verzoek om echtheidscontrole is dan ook mislukt.

```
 Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Date:          2/10/2014 1:35:47 PM
Event ID:      6273
Task Category: Network Policy Server
Level:         Information
Keywords:      Audit Failure
User:          N/A
Computer:      win2k8.skp.com
Description:
Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:
   Security ID:            SKP\vpnuser
   Account Name:            vpnuser
   Account Domain:            SKP
   Fully Qualified Account Name:    skp.com/Users/vpnuser

Client Machine:
   Security ID:            NULL SID
   Account Name:            -
   Fully Qualified Account Name:    -
   OS-Version:            -
   Called Station Identifier:        -
   Calling Station Identifier:        -

NAS:
   NAS IPv4 Address:        10.105.130.69
   NAS IPv6 Address:        -
   NAS Identifier:            -
   NAS Port-Type:            Virtual
   NAS Port:           0

RADIUS Client:
```

```
   Client Friendly Name:        vpn
   Client IP Address:            10.105.130.69

Authentication Details:
   Connection Request Policy Name:    vpn
   Network Policy Name:        vpn
   Authentication Provider:        Windows
   Authentication Server:        win2k8.skp.com
    Authentication Type:        PAP
   EAP Type:            -
   Account Session Identifier:        -
   Logging Results:            Accounting information was written to the local log file.
   Reason Code:            66
   Reason:                The user attempted to use an authentication method that is
not enabled on the matching network policy.
```