ASA VPN-Benutzerauthentifizierung für Windows 2008 NPS-Server (Active Directory) mit RADIUS-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird erläutert, wie eine Adaptive Security Appliance (ASA) für die Kommunikation mit einem Microsoft Windows 2008 Network Policy Server (NPS) mit dem RADIUS-Protokoll konfiguriert wird, sodass die älteren Cisco VPN Client/AnyConnect/Clientless WebVPN-Benutzer mithilfe von Active Directory authentifiziert werden. NPS ist eine der Serverrollen, die von Windows 2008 Server angeboten werden. Sie entspricht Windows 2003 Server, IAS (Internet Authentication Service). Hierbei handelt es sich um die Implementierung eines RADIUS-Servers für die Remote-Einwahl-Benutzerauthentifizierung. Ebenso ist NPS in Windows 2008 Server die Implementierung eines RADIUS-Servers. Im Prinzip ist die ASA ein RADIUS-Client für einen NPS RADIUS-Server. ASA sendet RADIUS-Authentifizierungsanforderungen im Namen von VPN-Benutzern, und NPS authentifiziert diese über Active Directory.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

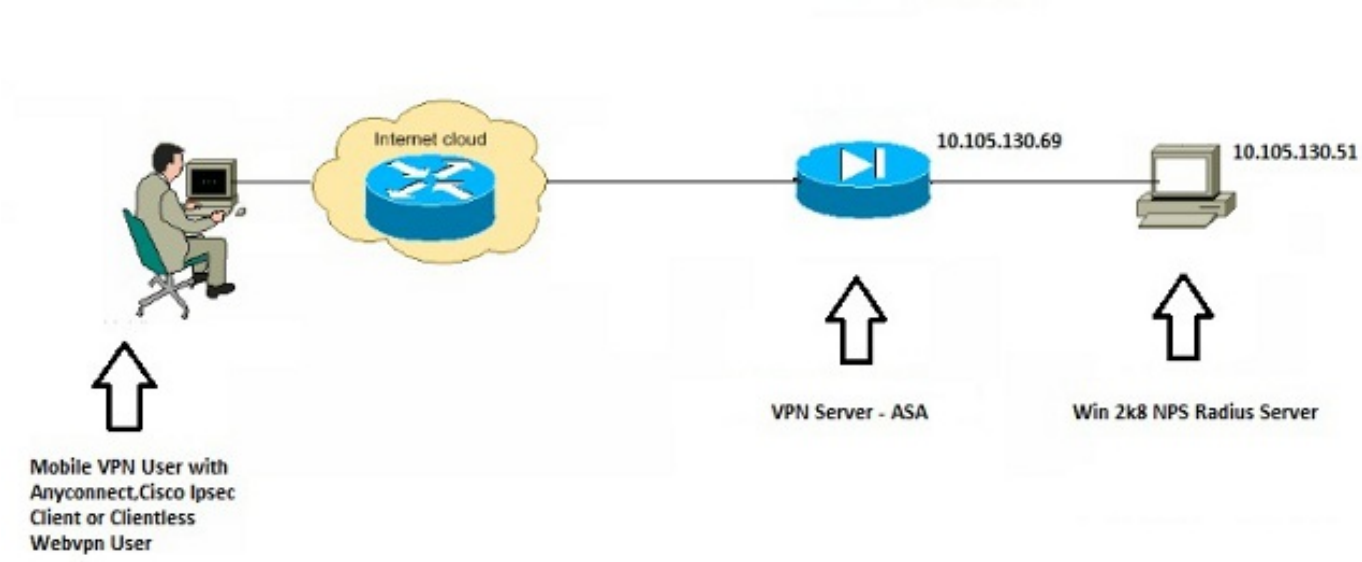
- ASA mit Ausführung von Version 9.1(4)
- Windows 2008 R2 Server mit installierten Active Directory-Diensten und NPS-Rolle

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

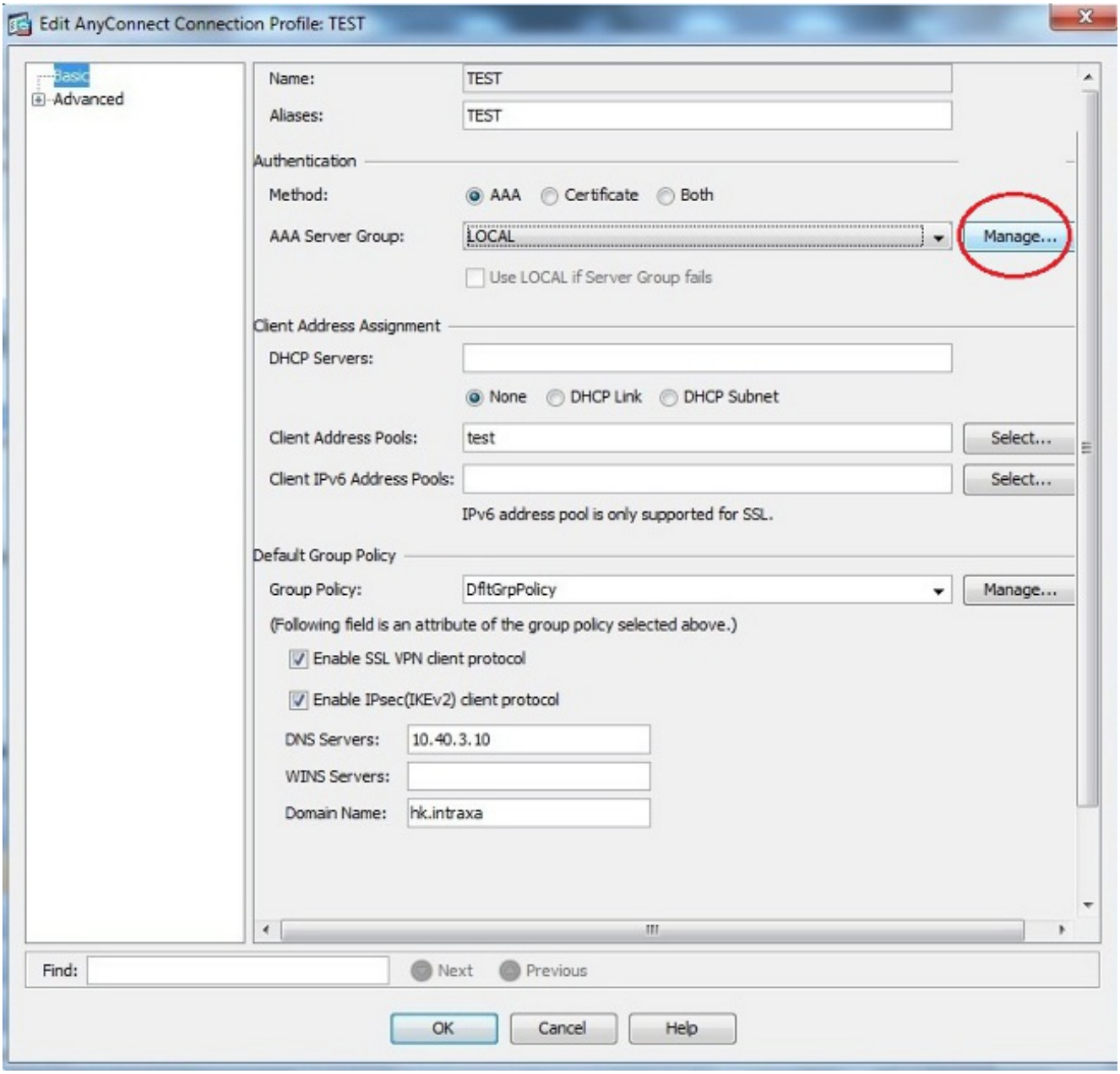
Netzwerkdiagramm



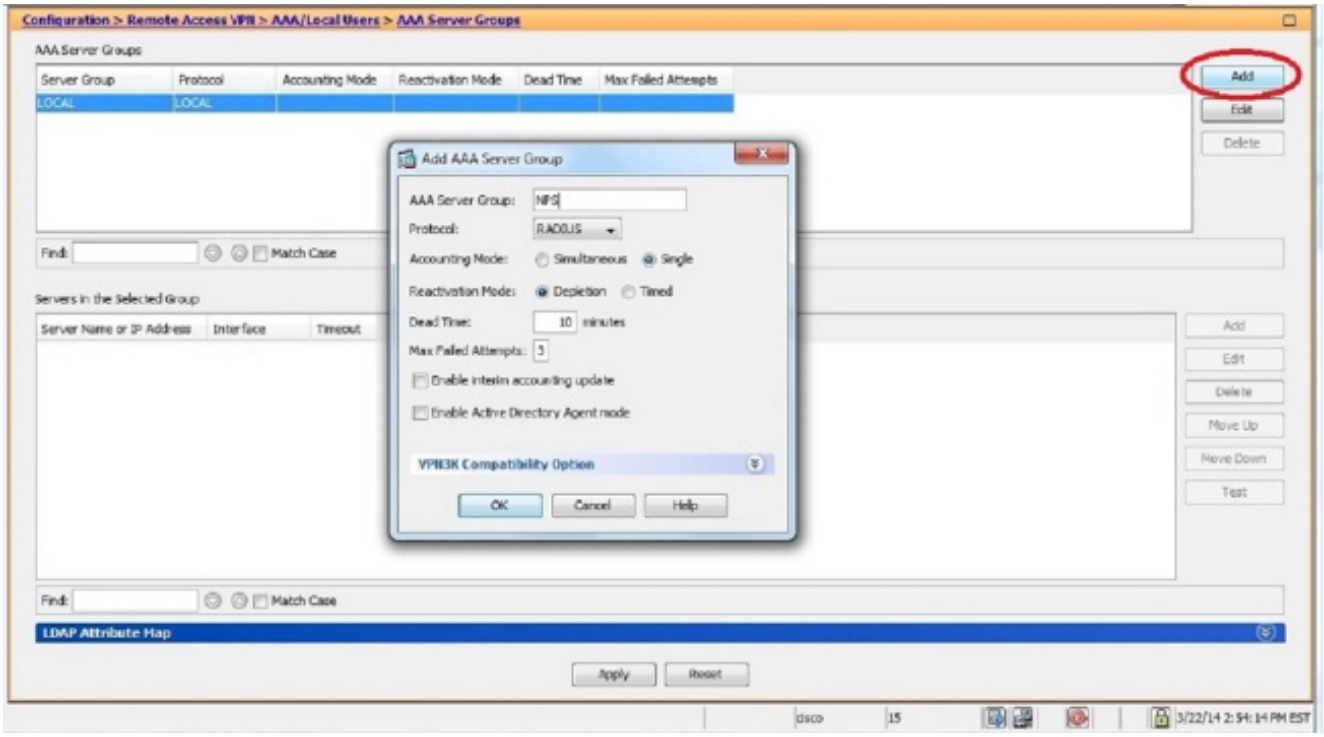
Konfigurationen

ASDM-Konfiguration

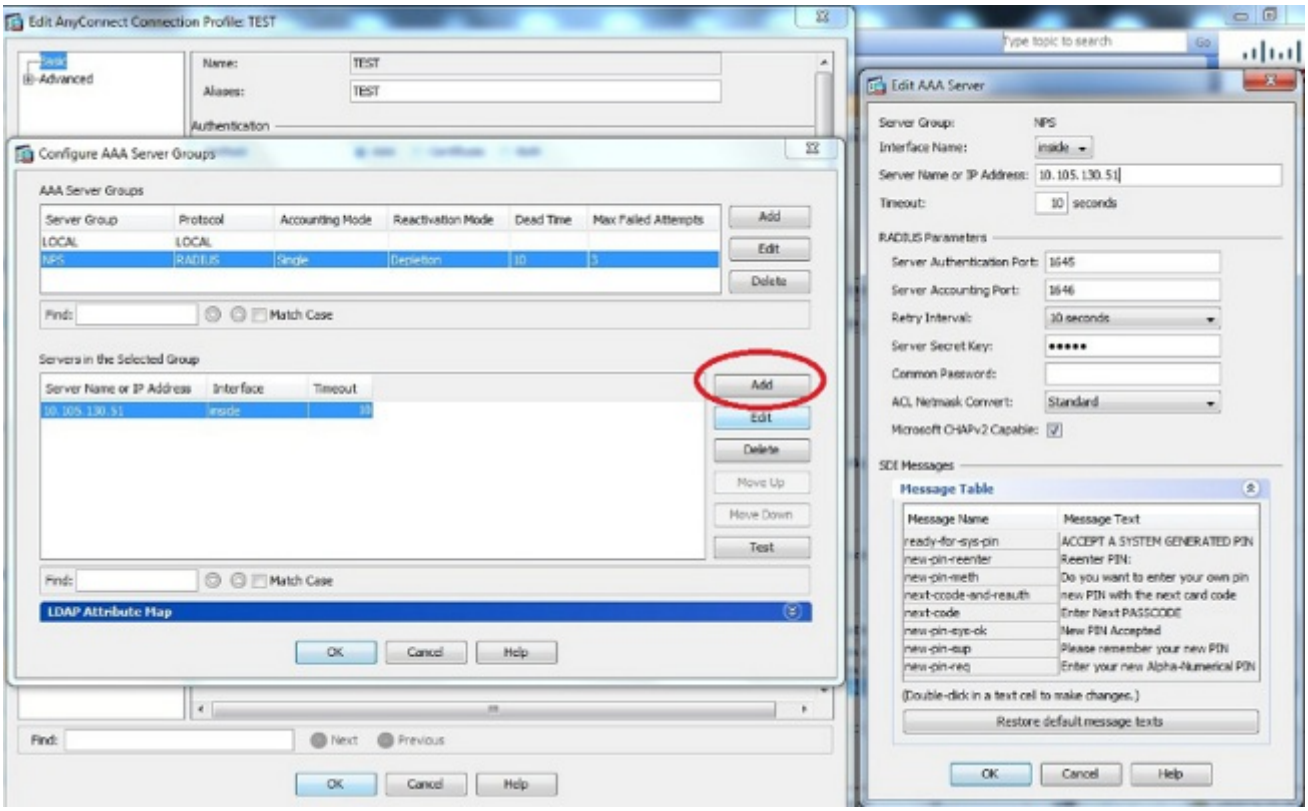
1. Wählen Sie die Tunnelgruppe aus, für die eine NPS-Authentifizierung erforderlich ist.
2. Klicken Sie auf **Bearbeiten** und wählen Sie **Grundlegend**.
3. Klicken Sie im Abschnitt Authentifizierung auf **Verwalten**.



4. Klicken Sie im Abschnitt AAA-Servergruppen auf **Hinzufügen**.
5. Geben Sie im Feld AAA Server Group (AAA-Servergruppe) den Namen der Servergruppe ein (z. B. NPS).
6. Wählen Sie in der Dropdown-Liste Protocol (Protokoll) die Option **RADIUS (RADIUS)** aus.
7. Klicken Sie auf **OK**.

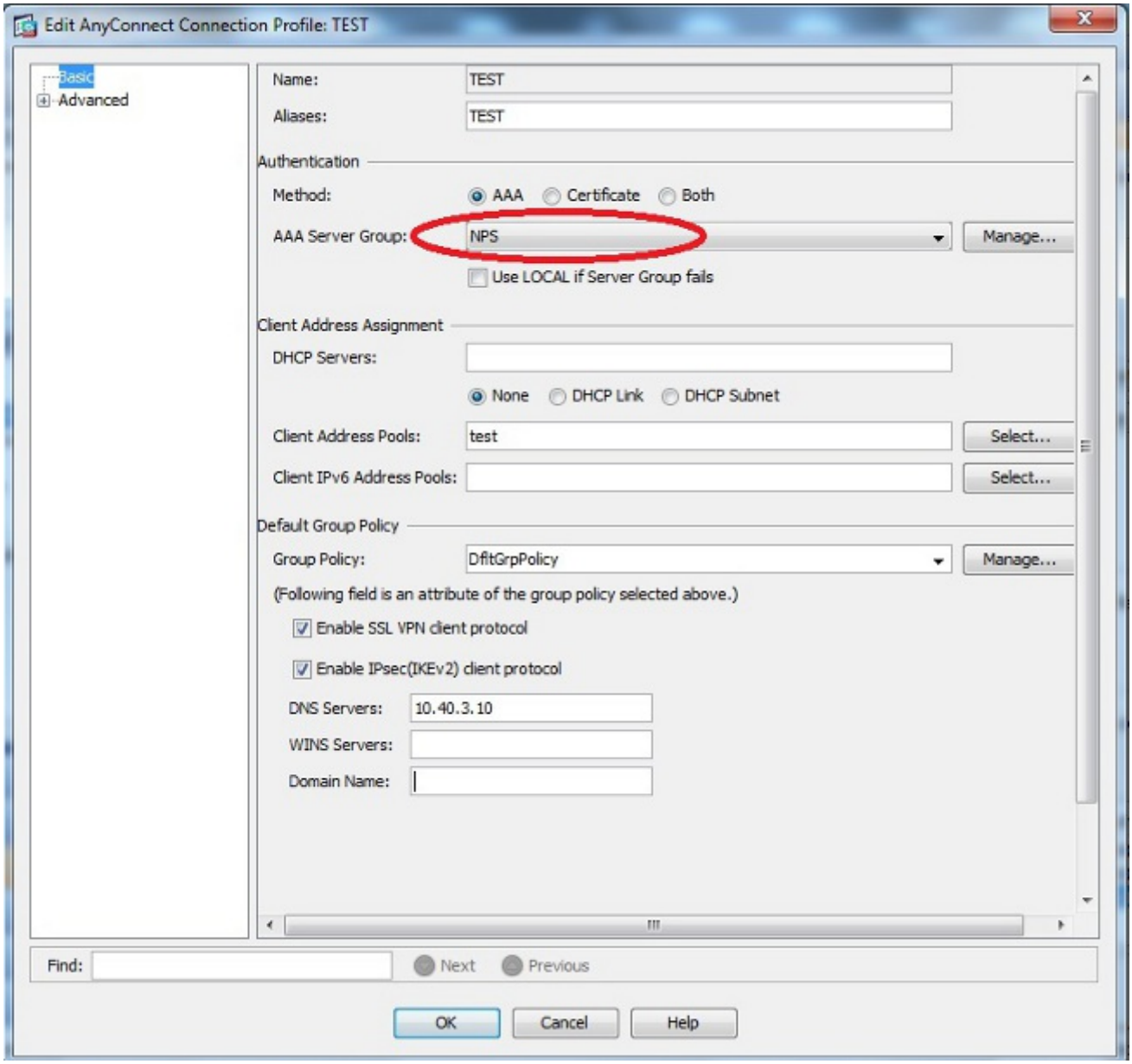


8. Wählen Sie im Abschnitt "Server" im Abschnitt "Ausgewählte Gruppe" die hinzugefügte AAA-Servergruppe aus, und klicken Sie auf **Hinzufügen**.
9. Geben Sie im Feld Servername oder IP-Adresse die IP-Adresse des Servers ein.
10. Geben Sie im Feld Server Secret Key (Servergeheimnis-Schlüssel) den geheimen Schlüssel ein.
11. Lassen Sie die Felder Server Authentication Port (Serverauthentifizierungsport) und Server Accounting Port den Standardwert, es sei denn, der Server hört auf einem anderen Port zu.
12. Klicken Sie auf **OK**.
13. Klicken Sie auf **OK**.



14. Wählen Sie aus der Dropdown-Liste AAA Server Group (AAA-Servergruppe) die Gruppe (in diesem Beispiel NPS) aus, die in den vorherigen Schritten hinzugefügt wurde.

15. Klicken Sie auf OK.



CLI-Konfiguration

```
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
```

Standardmäßig verwendet die ASA den Authentifizierungstyp PAP (Uncrypted Password Authentication Protocol). Dies bedeutet nicht, dass die ASA das Kennwort im Klartext sendet, wenn sie das RADIUS REQUEST-Paket sendet. Stattdessen wird das Klartext-Kennwort mit dem gemeinsamen geheimen RADIUS-Schlüssel verschlüsselt.

Wenn die Kennwortverwaltung unter der Tunnelgruppe aktiviert ist, verwendet ASA den Authentifizierungstyp MSCHAP-v2, um das Klartext-Kennwort zu verschlüsseln. Stellen Sie in diesem Fall sicher, dass das Kontrollkästchen **Microsoft CHAPv2 Capable** im Fenster Edit AAA Server (AAA-Server bearbeiten), das im ASDM-Konfigurationsabschnitt konfiguriert wurde, aktiviert ist.

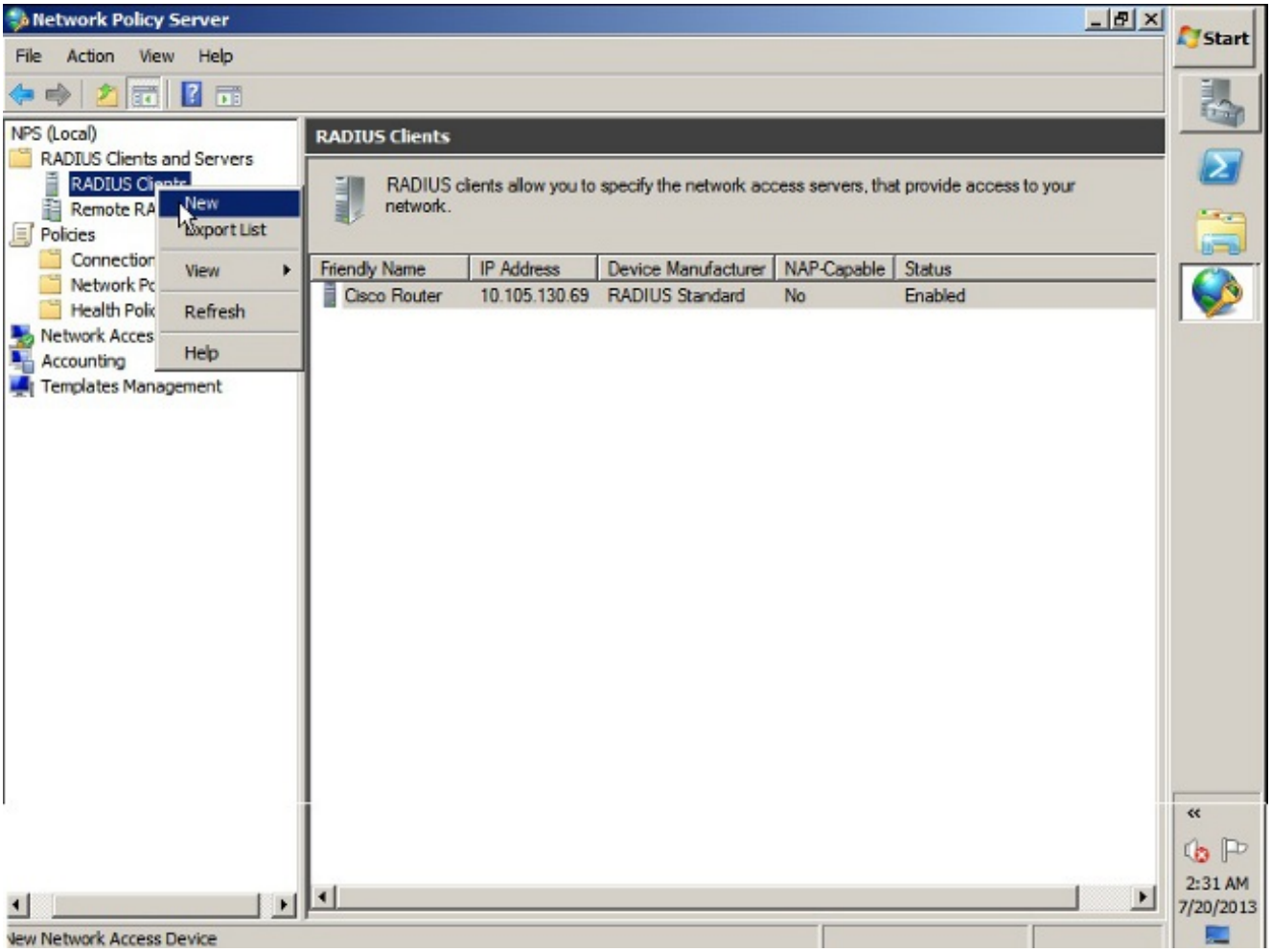
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **Hinweis**: Der **Test aaa-server authentication-**Befehl verwendet immer PAP. Die ASA verwendet MSCHAP-v2 nur dann, wenn ein Benutzer eine Verbindung zur Tunnelgruppe mit aktivierter Kennwortverwaltung initiiert. Außerdem wird die Option 'password-management [password-expire-in-days]' nur mit dem Lightweight Directory Access Protocol (LDAP) unterstützt. RADIUS bietet diese Funktion nicht. Wenn das Kennwort bereits in Active Directory abgelaufen ist, wird die Option Kennwort ablaufen angezeigt.

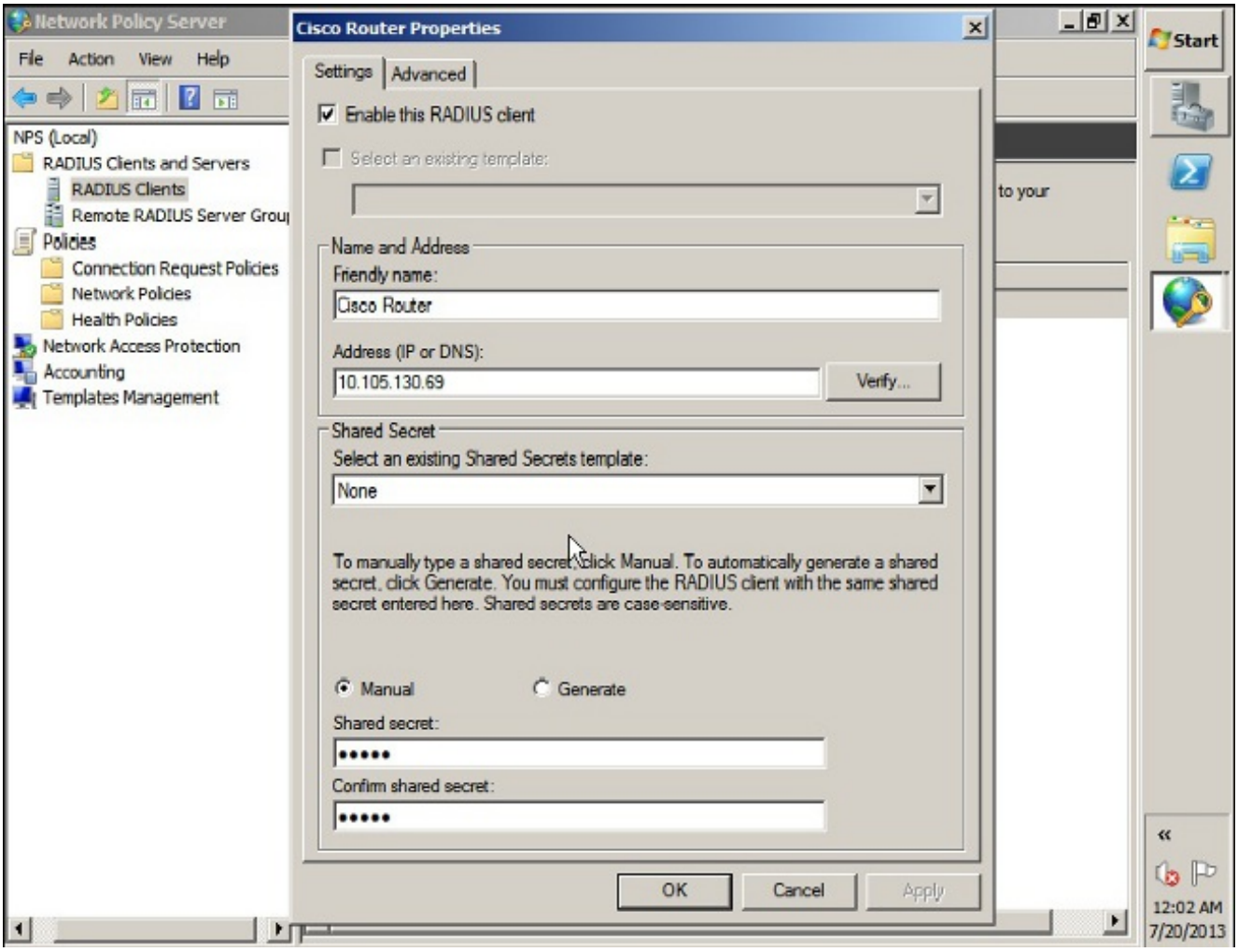
Windows 2008-Server mit NPS-Konfiguration

Die NPS-Serverrolle sollte auf dem Windows 2008-Server installiert und ausgeführt werden. Wenn nicht, wählen Sie **Start > Verwaltung > Serverrollen > Rollendienste hinzufügen aus**. Wählen Sie den Network Policy Server aus, und installieren Sie die Software. Führen Sie nach der Installation der NPS-Serverrolle die folgenden Schritte aus, um das NPS so zu konfigurieren, dass es RADIUS-Authentifizierungsanforderungen von der ASA akzeptiert und verarbeitet:

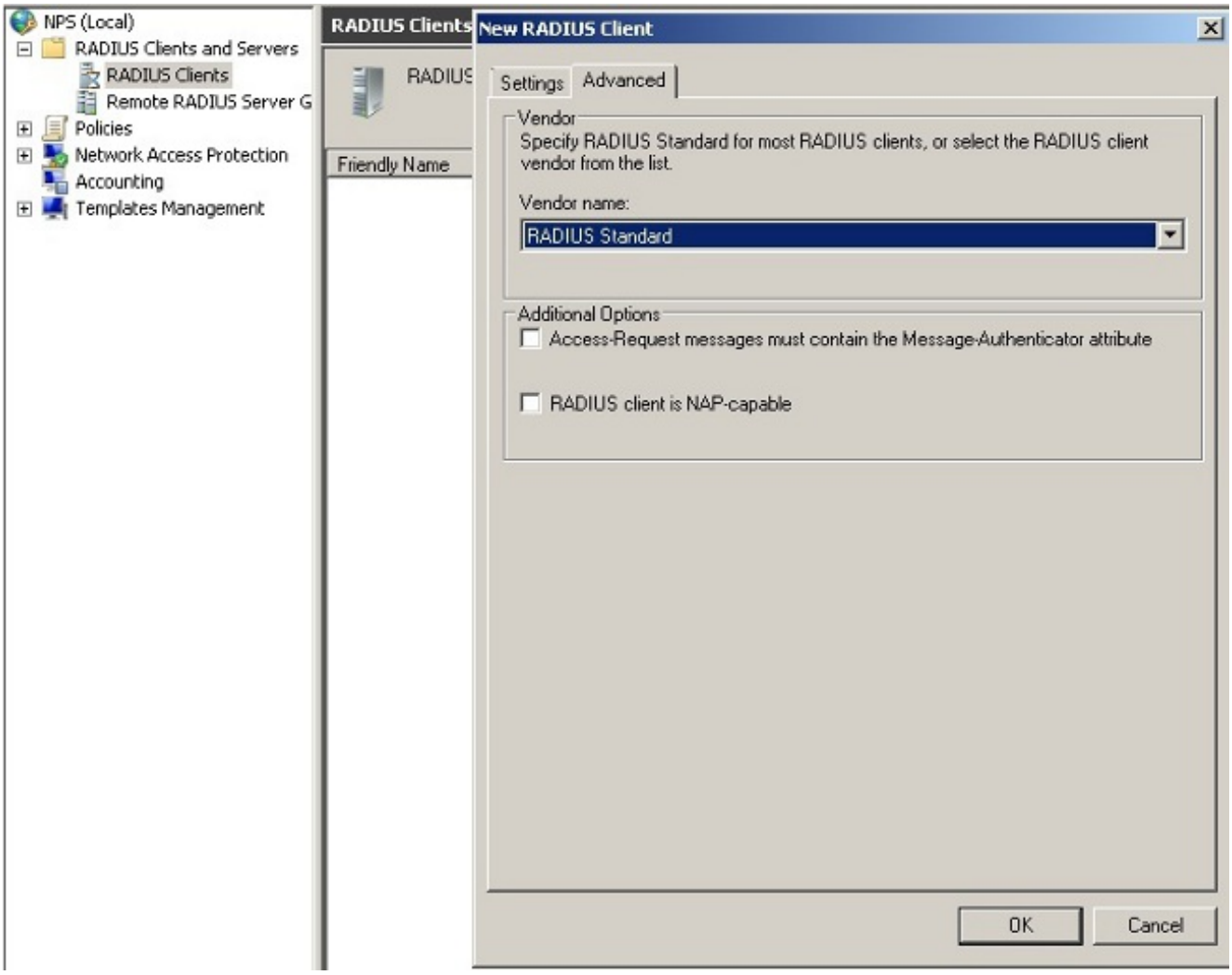
1. Fügen Sie die ASA als RADIUS-Client im NPS-Server hinzu. Wählen Sie **Verwaltung > Netzwerkrichtlinienserver aus.**Klicken Sie mit der rechten Maustaste auf **RADIUS-Clients**, und wählen Sie **Neu**
   aus.



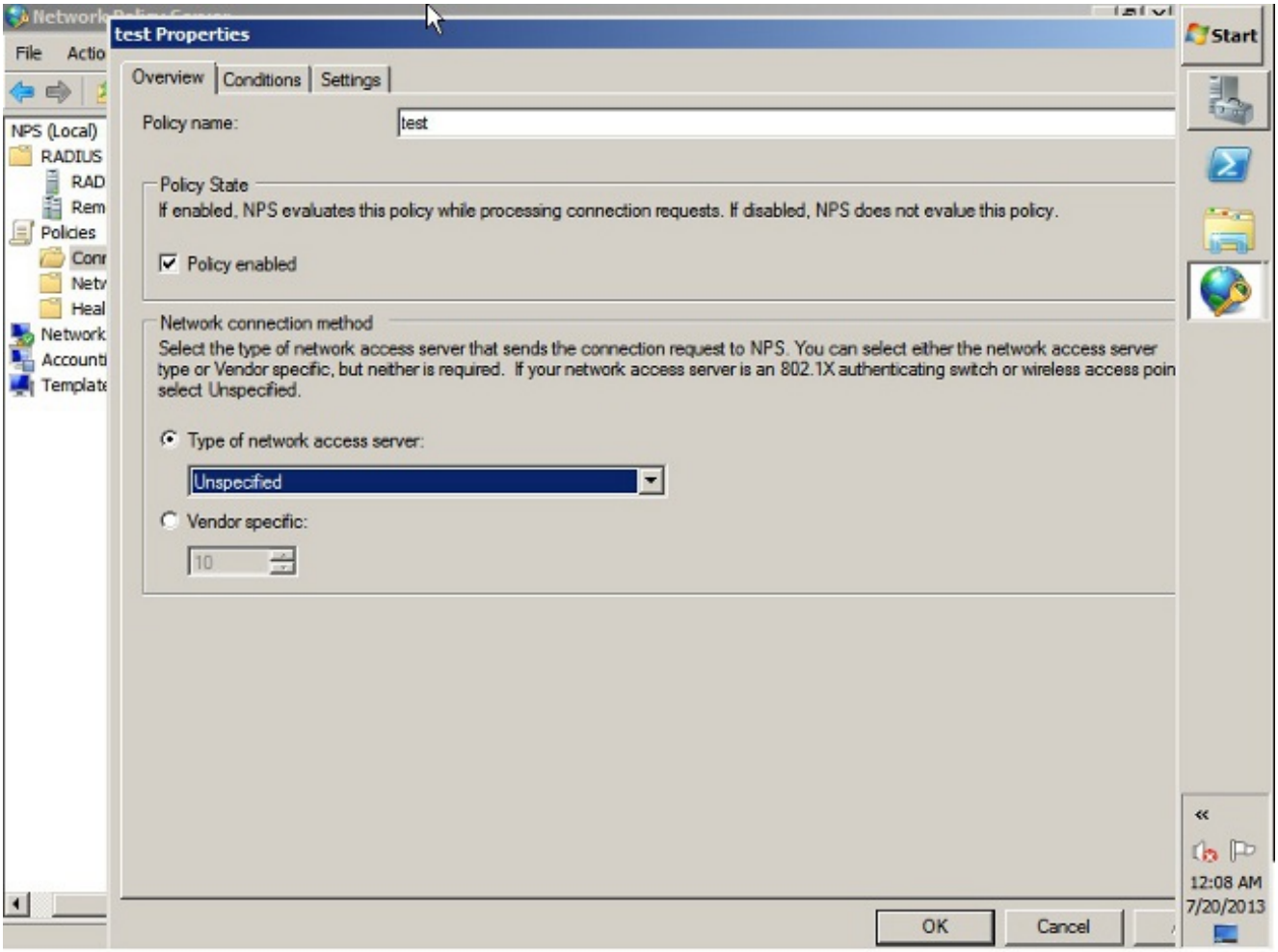
Geben Sie einen Namen, eine Adresse (IP oder DNS) und einen auf der ASA konfigurierten gemeinsamen geheimen Schlüssel
ein.



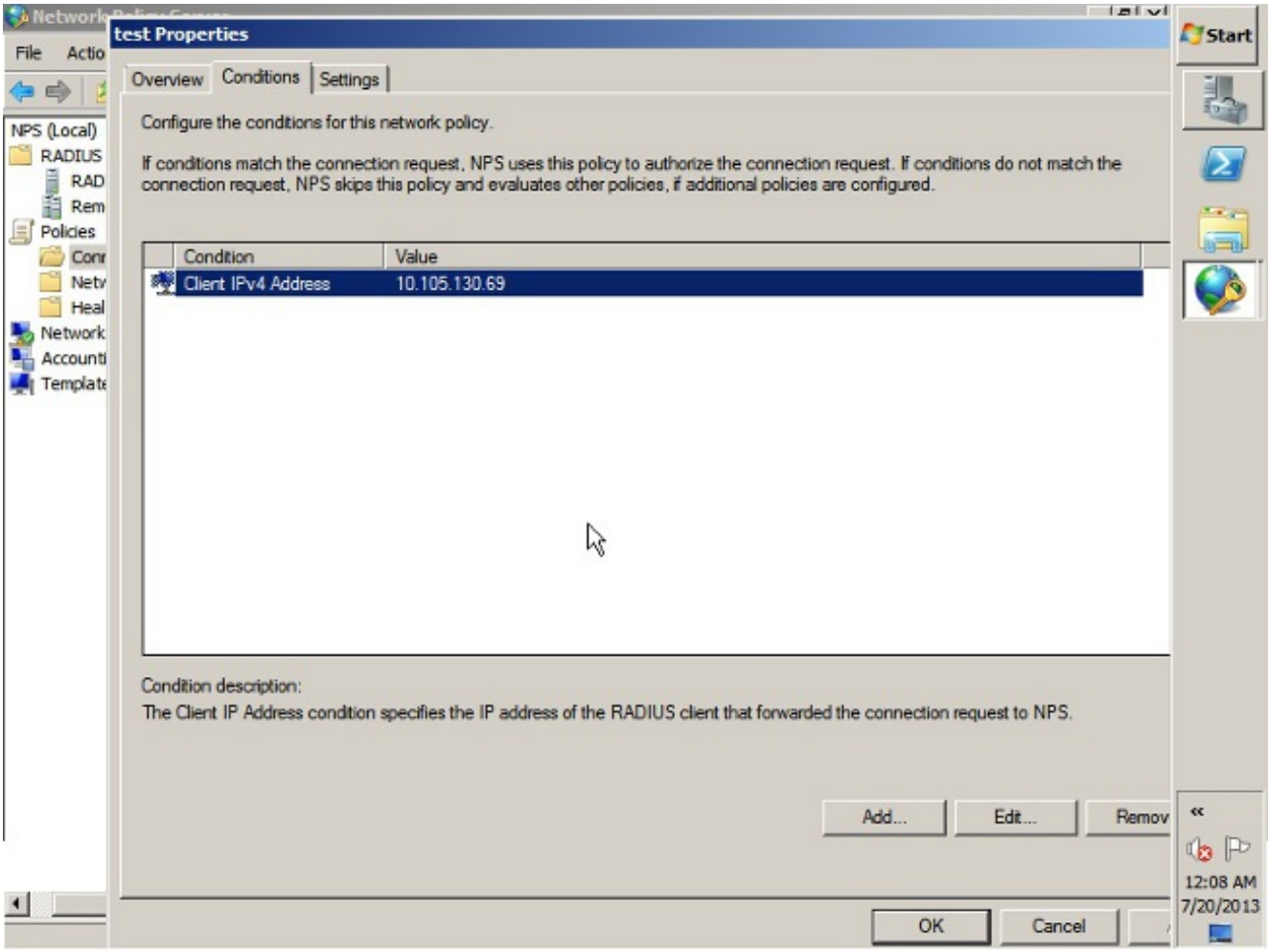
Klicken Sie auf die Registerkarte **Erweitert**.Wählen Sie in der Dropdown-Liste Vendor Name (Herstellername) die Option **RADIUS Standard (RADIUS-Standard)**.Klicken Sie auf **OK**.



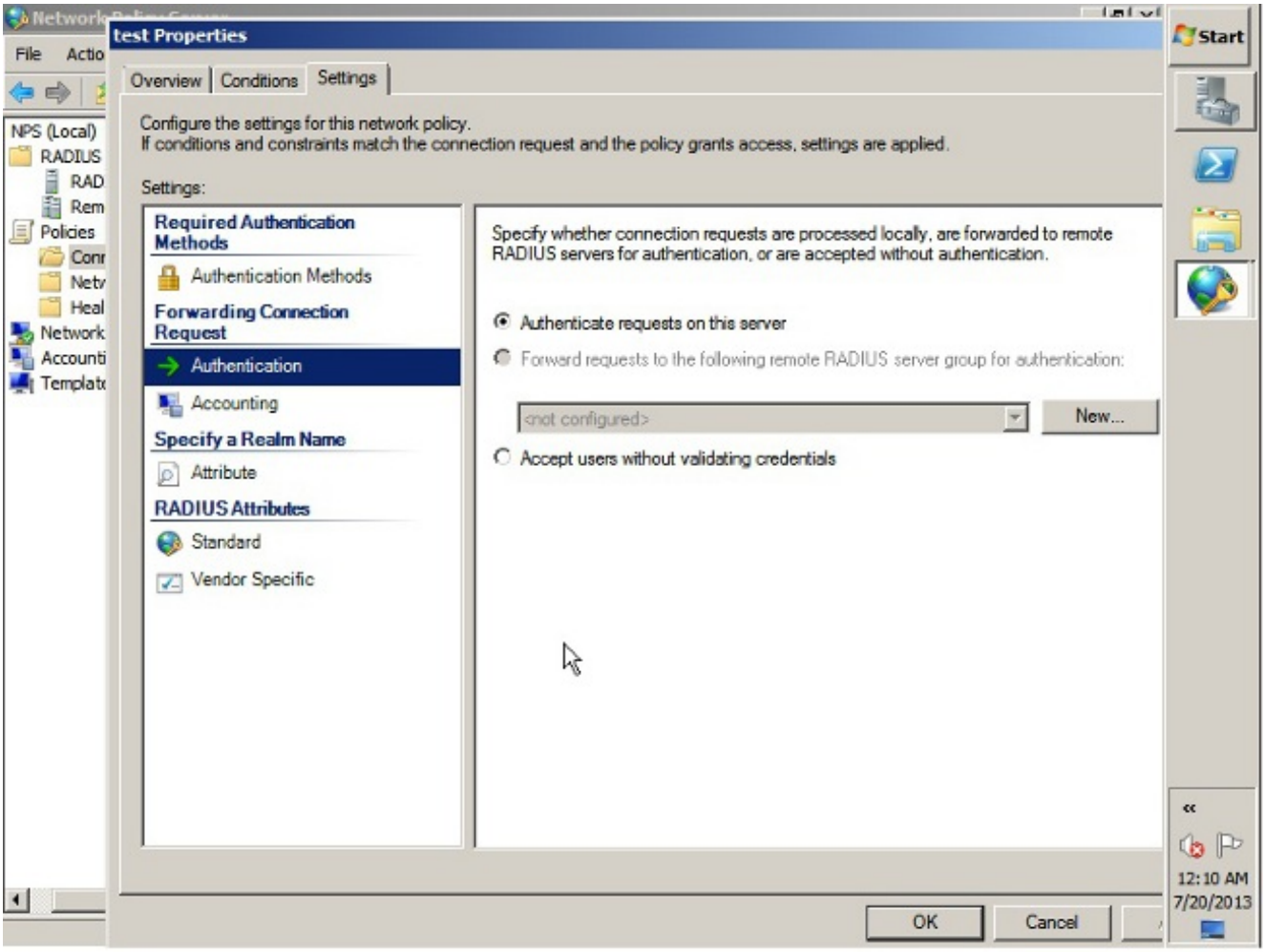
2. Erstellen Sie eine neue Verbindungsanforderungsrichtlinie für VPN-Benutzer. Die Richtlinie für Verbindungsanfragen legt fest, ob die Anfragen von RADIUS-Clients lokal verarbeitet oder an Remote-RADIUS-Server weitergeleitet werden sollen. Klicken Sie unter NPS > Policies (NPS > Richtlinien) mit der rechten Maustaste auf **Connection Request Policies (Verbindungsanforderungsrichtlinien)**, und erstellen Sie eine neue Richtlinie.Wählen Sie in der Dropdown-Liste Typ des Netzwerkzugriffsservers die Option **Unspecified (Nicht festgelegt)**
aus.



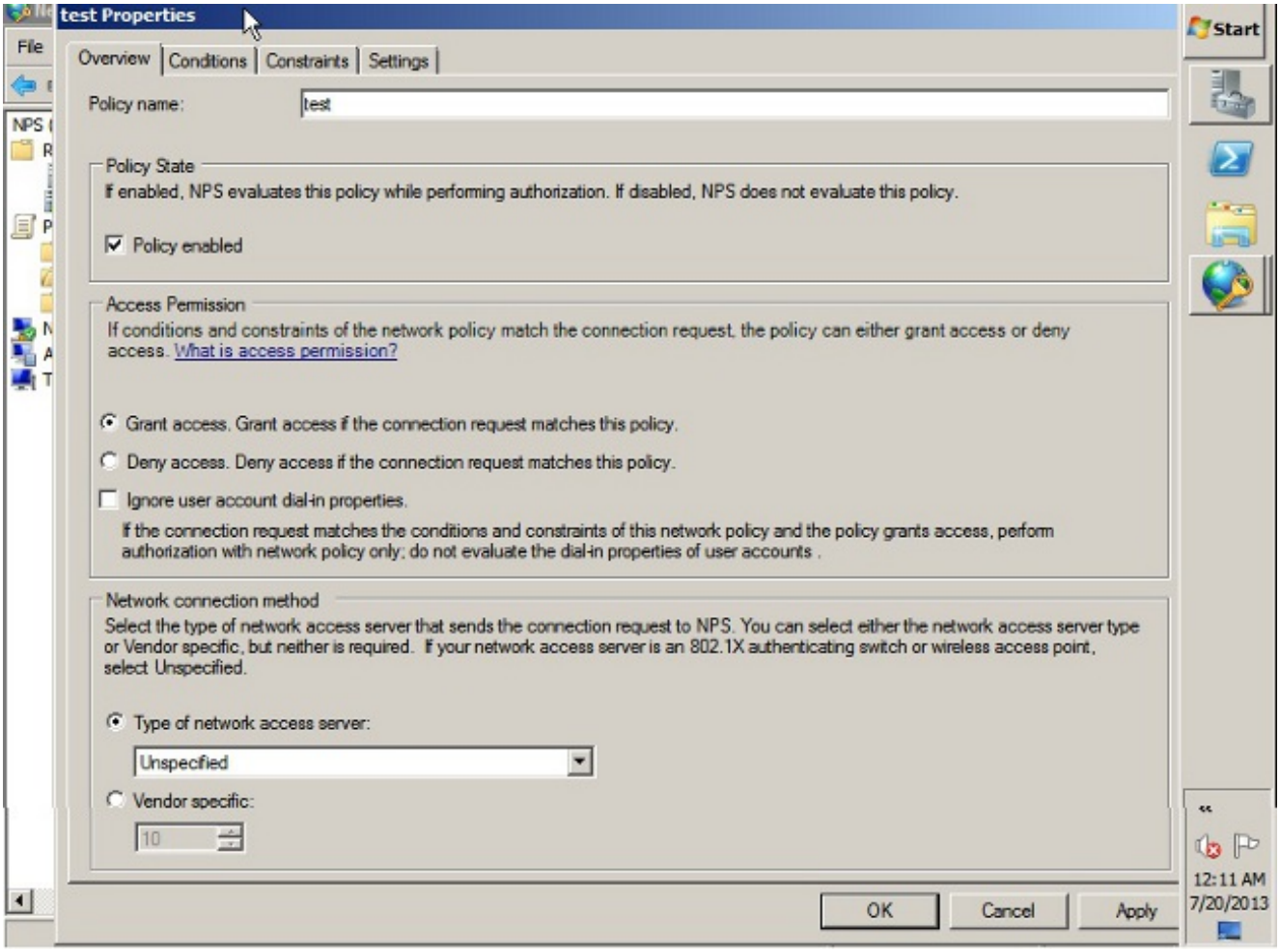
Klicken Sie auf die Registerkarte **Bedingungen**.Klicken Sie auf **Hinzufügen**.Geben Sie die IP-Adresse der ASA als 'Client IPv4 Address' (Client-IPv4-Adresse)
ein.



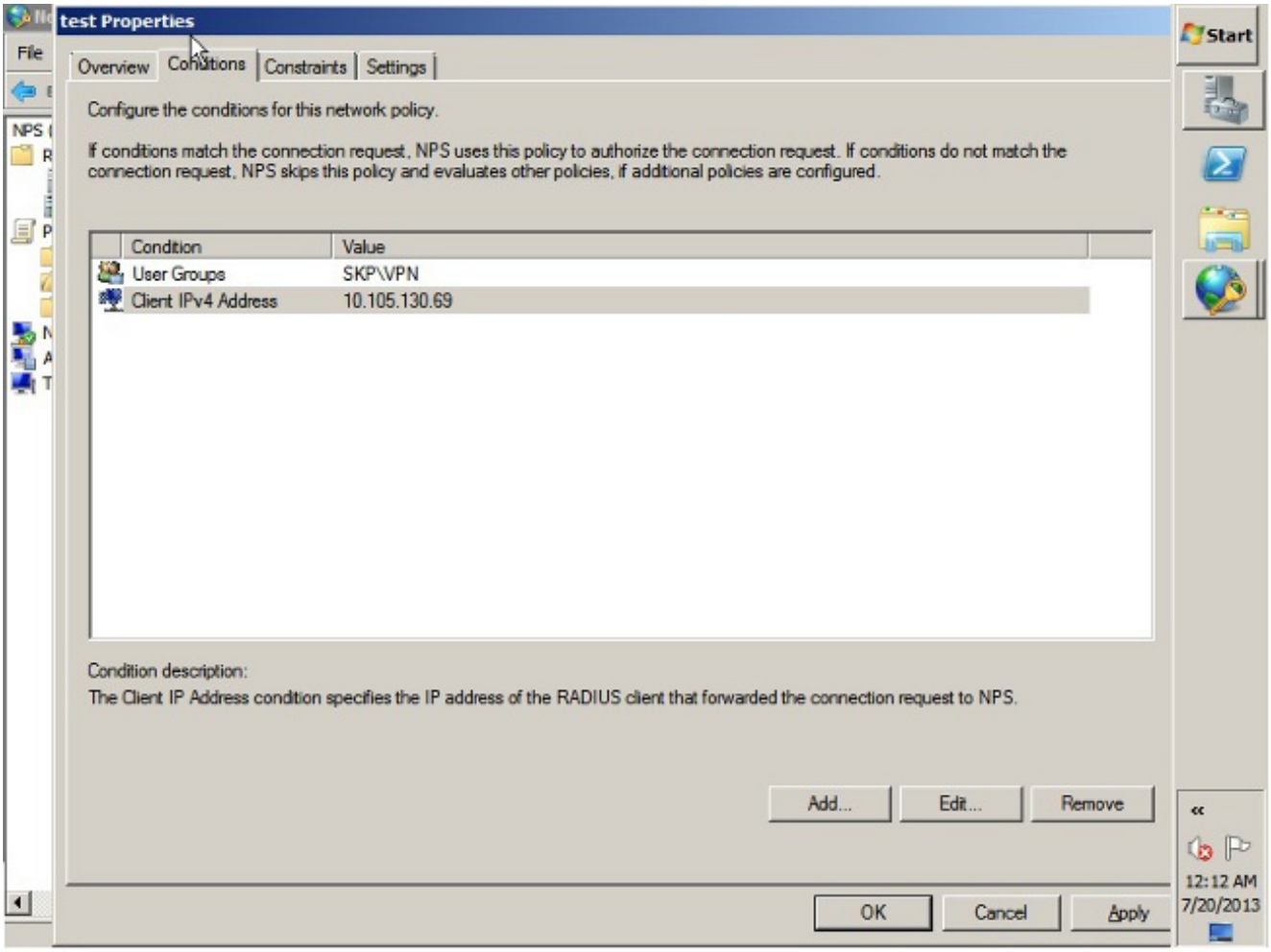
Klicken Sie auf die Registerkarte **Einstellungen**.Wählen Sie unter Forwarding Connection Request (Verbindungsanforderung weiterleiten) die Option **Authentication (Authentifizierung)**. Stellen Sie sicher, dass das Optionsfeld Authentifizierungsanforderungen auf diesem Server aktiviert ist.Klicken Sie auf
OK.



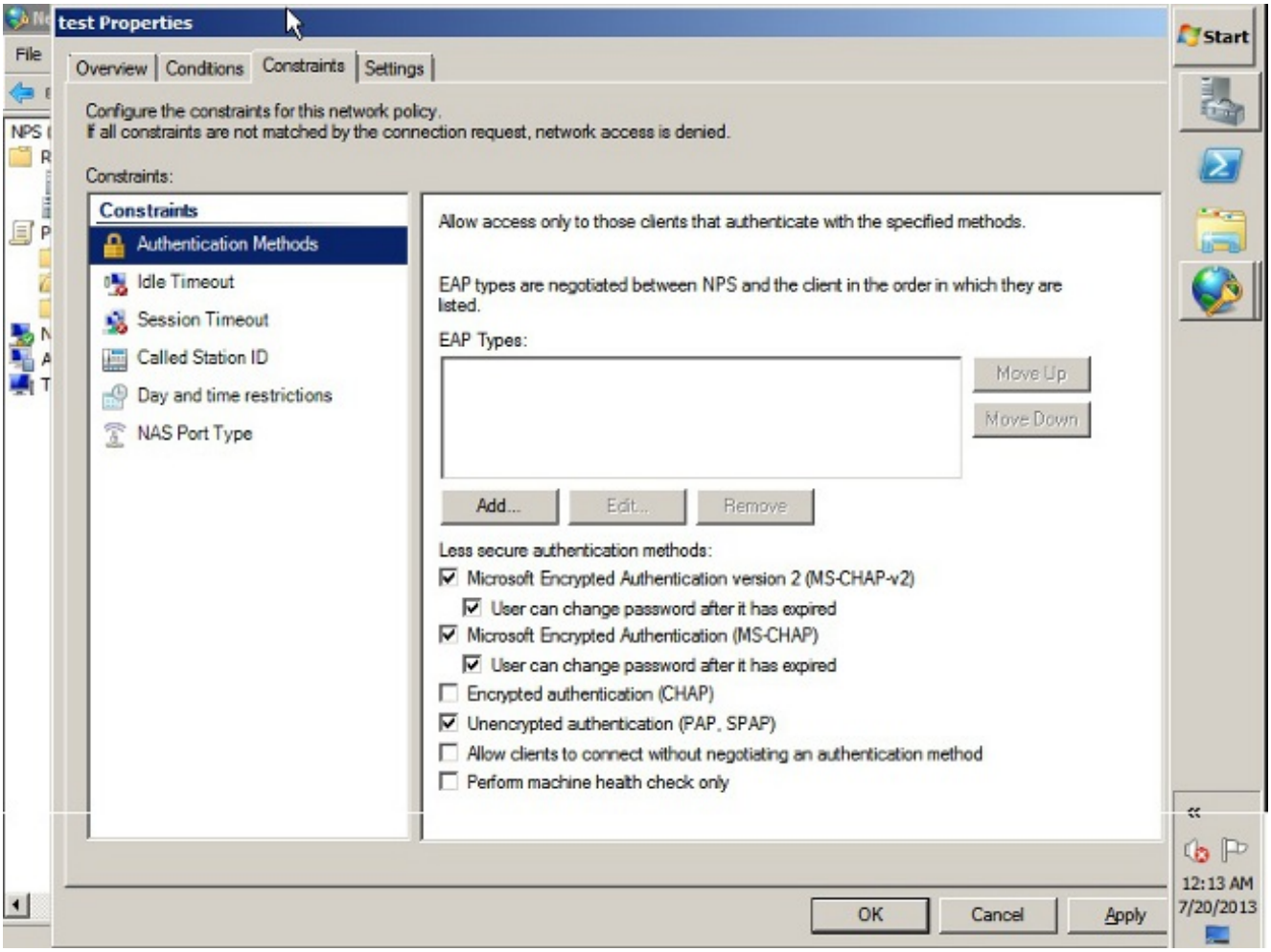
3. Fügen Sie eine Netzwerkrichtlinie hinzu, in der Sie angeben können, welche Benutzer authentifiziert werden dürfen.Beispielsweise können Sie Active Directory-Benutzergruppen als Bedingung hinzufügen. Nur die Benutzer, die einer angegebenen Windows-Gruppe angehören, werden unter dieser Richtlinie authentifiziert.Wählen Sie unter NPS die Option **Policies (Richtlinien)** aus.Klicken Sie mit der rechten Maustaste auf **Netzwerkrichtlinie**, und erstellen Sie eine neue Richtlinie.Stellen Sie sicher, dass das Optionsfeld Zugriff gewähren ausgewählt ist.Wählen Sie in der Dropdown-Liste Typ des Netzwerkzugriffsservers die Option **Unspecified (Nicht festgelegt)**
aus.



Klicken Sie auf die Registerkarte **Bedingungen**.Klicken Sie auf **Hinzufügen**.Geben Sie die IP-Adresse der ASA als Client-IPv4-Adressbedingung ein.Geben Sie die Active Directory-Benutzergruppe ein, die VPN-Benutzer
enthält.



Klicken Sie auf die Registerkarte **Einschränkungen**.Wählen Sie **Authentifizierungsmethoden aus**.Stellen Sie sicher, dass das Kontrollkästchen Uncrypted Authentication (PAP, SPAP) aktiviert ist.Klicken Sie auf
OK.

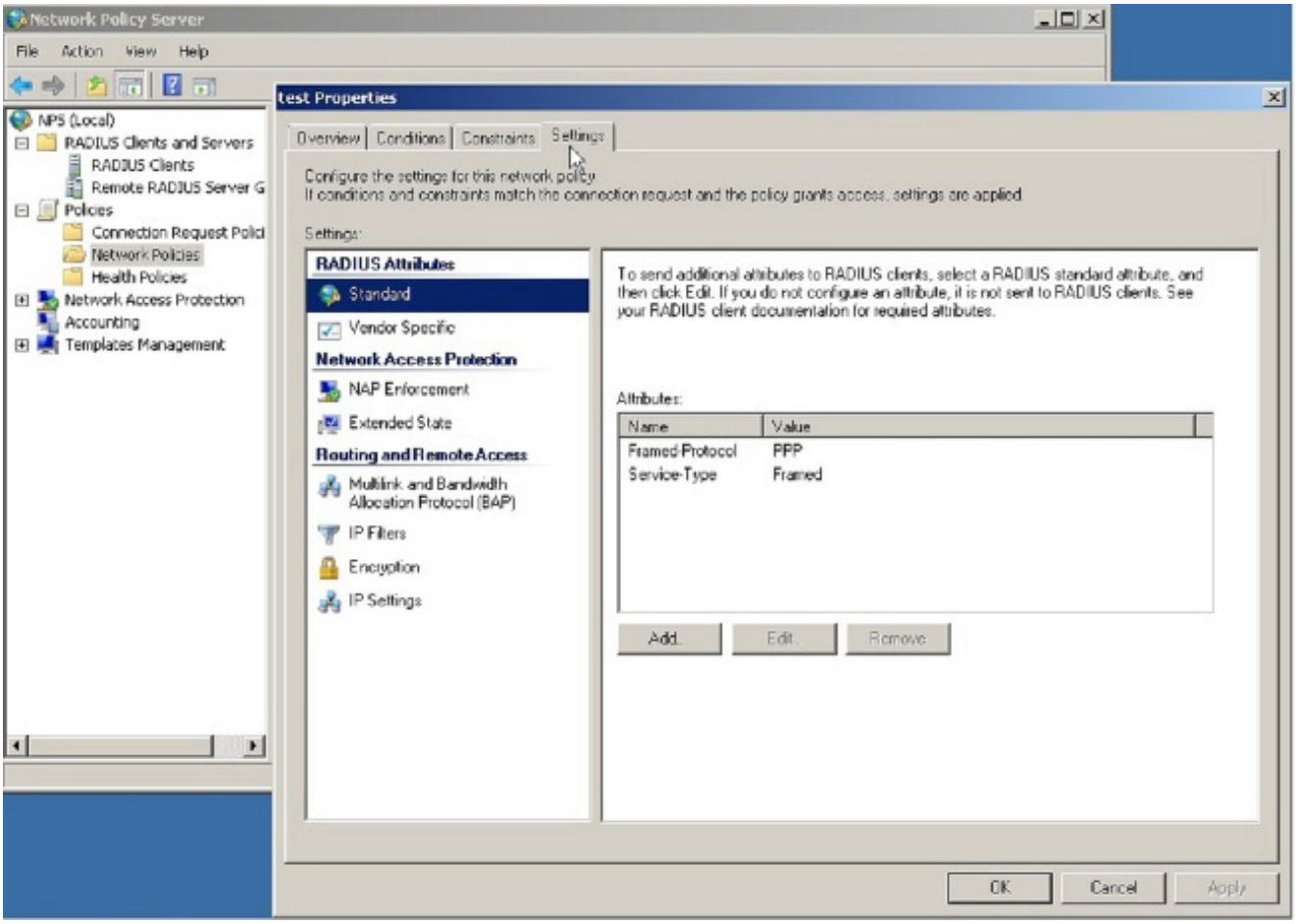


Gruppenrichtlinienattribut (Attribut 25) vom NPS RADIUS-Server übergeben

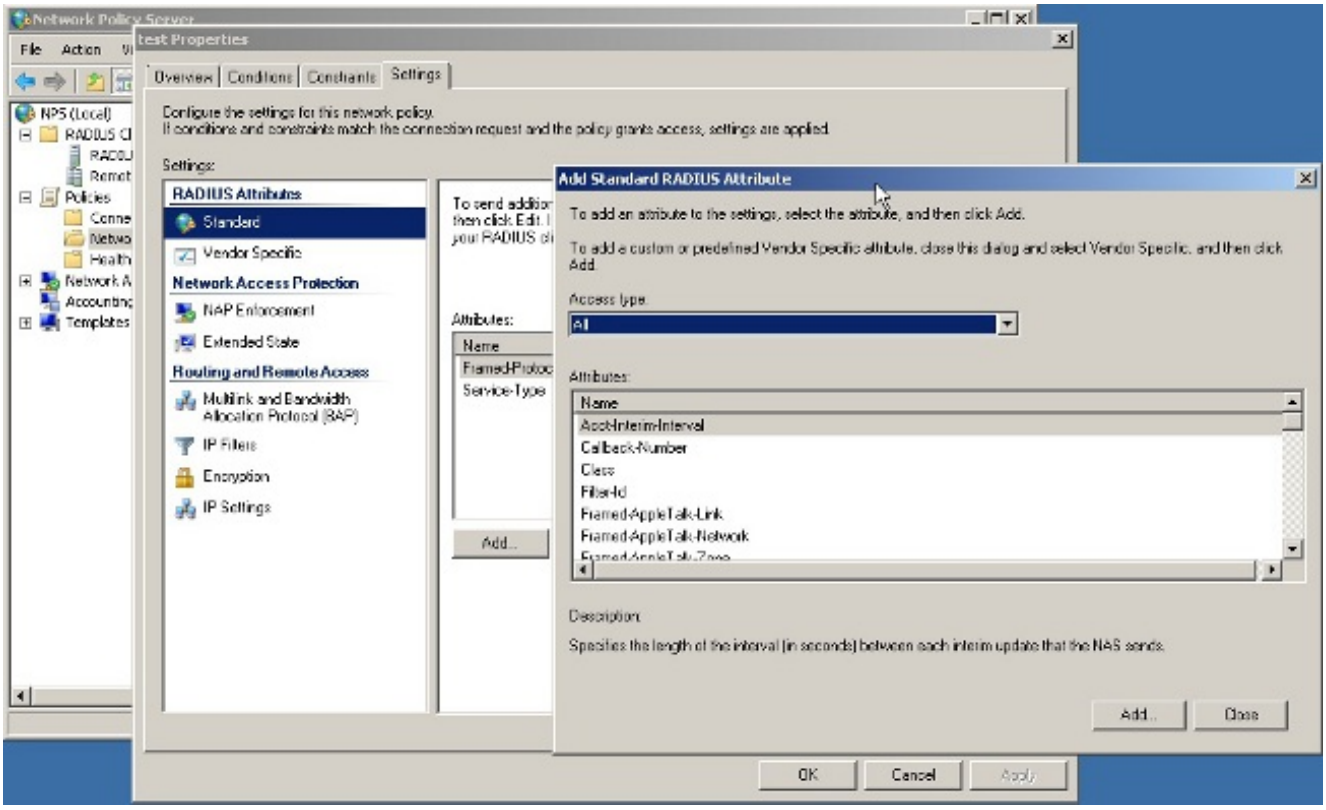
Wenn die Gruppenrichtlinie dem Benutzer dynamisch mit dem NPS RADIUS-Server zugewiesen werden muss, kann das Gruppenrichtlinien-RADIUS-Attribut (Attribut 25) verwendet werden.

Führen Sie diese Schritte aus, um das RADIUS-Attribut 25 für die dynamische Zuweisung einer Gruppenrichtlinie an den Benutzer zu senden.

1. Klicken Sie nach dem Hinzufügen der Netzwerkrichtlinie mit der rechten Maustaste auf die gewünschte Netzwerkrichtlinie, und klicken Sie auf die Registerkarte **Einstellungen**.

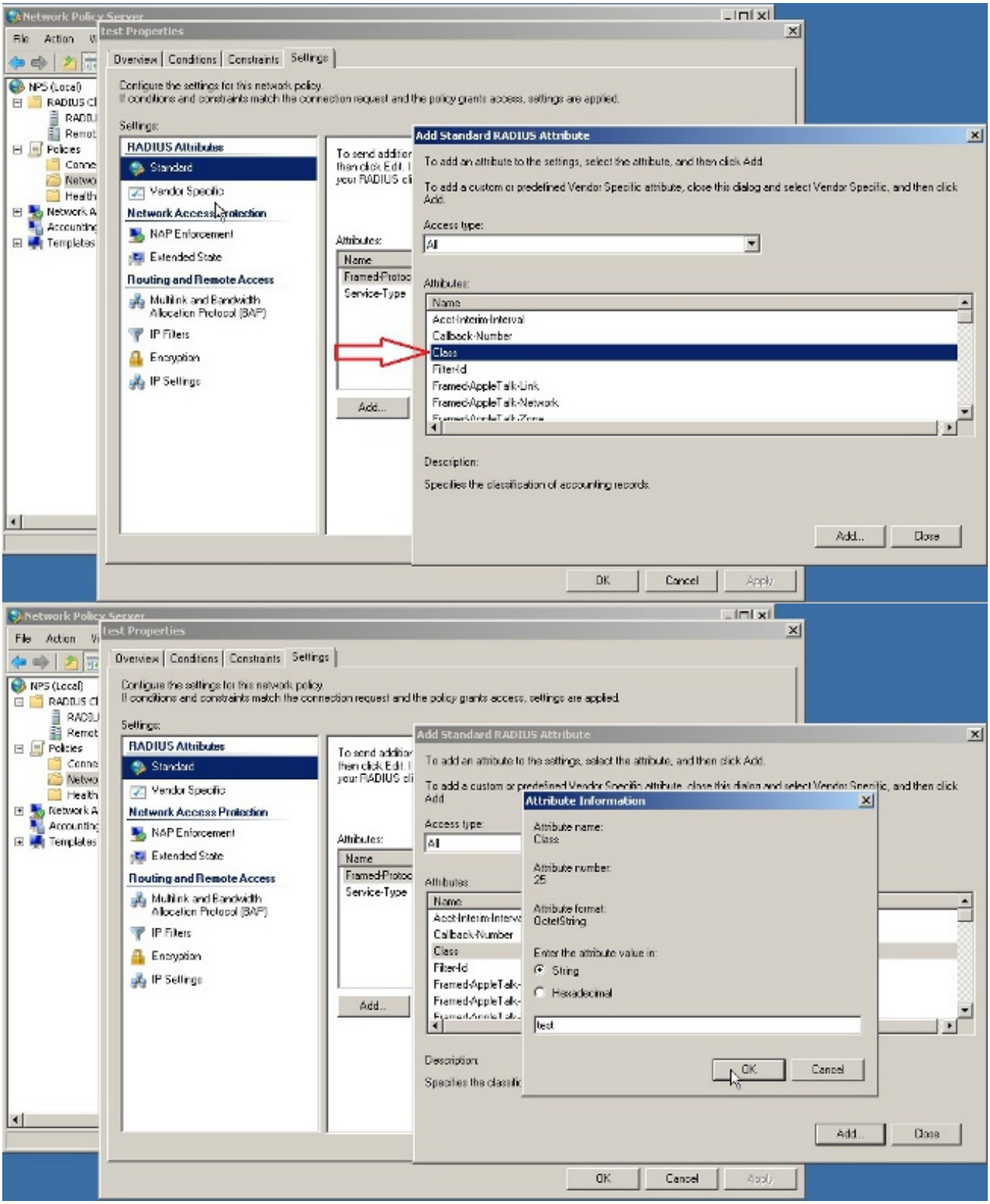


2. Wählen Sie **RADIUS Attributes > Standard aus**. Klicken Sie auf **Hinzufügen**. Lassen Sie den Zugriffstyp
Alle.



3. Wählen Sie im Feld Attribute die Option **Klasse aus**, und klicken Sie auf **Hinzufügen**. Geben Sie den Attributwert ein, d. h. den Namen der Gruppenrichtlinie als Zeichenfolge. Denken Sie daran, dass eine Gruppenrichtlinie mit diesem Namen in der ASA konfiguriert werden muss. Dies bedeutet, dass die ASA diese der VPN-Sitzung zuweist, nachdem sie dieses Attribut in

der RADIUS-Antwort erhalten hat.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Hinweis: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug**-Befehlen finden Sie unter Wichtige Informationen.

ASA-Debugger

Aktivieren Sie **den Debugradius alle** auf der ASA.

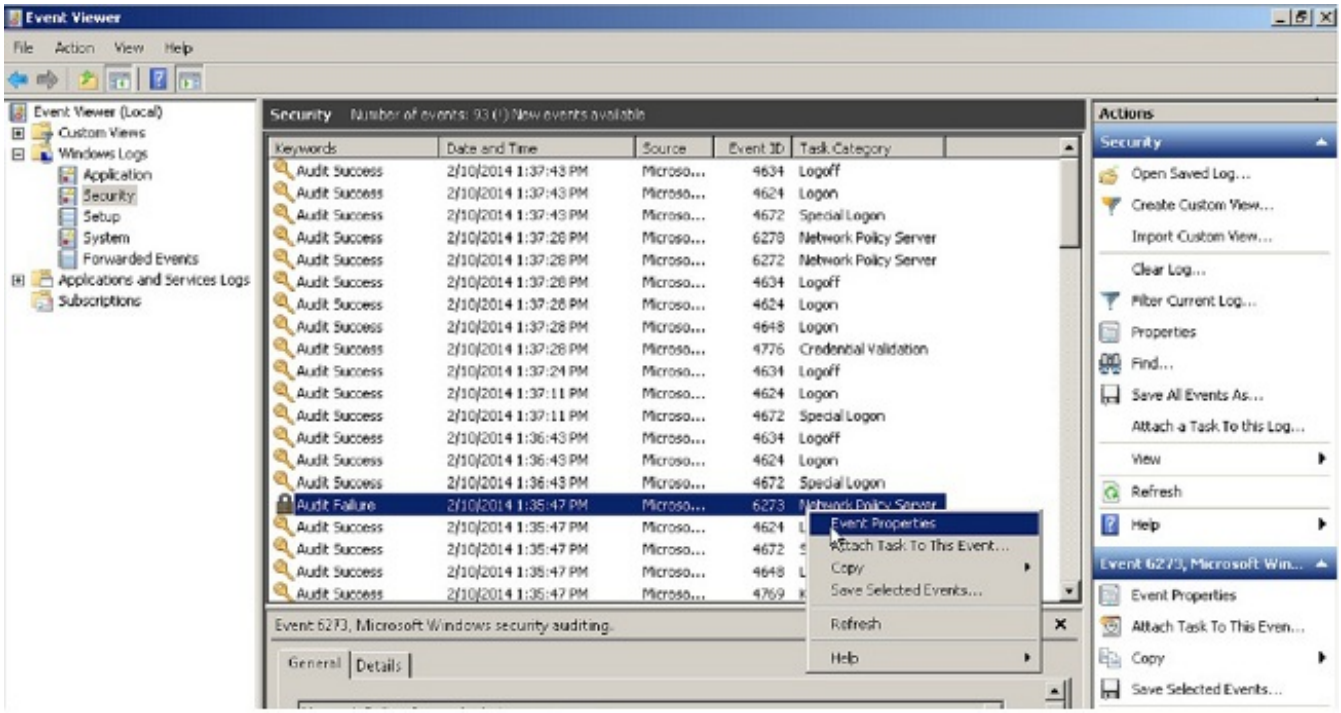
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Stellen Sie sicher, dass die Verbindung zwischen ASA und NPS-Server gut ist.Wenden Sie Paketerfassungen an, um sicherzustellen, dass die Authentifizierungsanfrage die ASA-Schnittstelle verlässt (von der aus der Server erreichbar ist). Vergewissern Sie sich, dass die Geräte im Pfad den UDP-Port 1645 (RADIUS-Standardauthentifizierungsport) nicht blockieren, um sicherzustellen, dass er den NPS-Server erreicht. Weitere Informationen zur Paketerfassung auf der ASA finden Sie in ASA/PIX/FWSM: Paketerfassung mithilfe von CLI- und ASDM-Konfigurationsbeispiel.
- Wenn die Authentifizierung immer noch fehlschlägt, sehen Sie in der Ereignisanzeige in den Fenstern NPS nach. Wählen Sie unter Ereignisanzeige > Windows-Protokolle die Option **Sicherheit aus.** Suchen Sie zum Zeitpunkt der Authentifizierungsanfrage nach Ereignissen, die NPS zugeordnet
  sind.



Wenn Sie Ereigniseigenschaften öffnen, sollten Sie die Fehlerursache sehen können, wie im Beispiel gezeigt. In diesem Beispiel wurde PAP nicht als Authentifizierungstyp unter Netzwerkrichtlinie ausgewählt. Daher schlägt die Authentifizierungsanforderung fehl.

```
 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.**