ASA VPN User Authentication against Windows 2008 NPS Server (Active Directory) with RADIUS Configuration Example

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Network Diagram](#)
[Configurations](#)
[ASDM Configuration](#)
[CLI Configuration](#)
[Windows 2008 Server with NPS Configuration](#)
[Verify](#)
[ASA Debugs](#)
[Troubleshoot](#)

Introduction

This document explains how to configure an Adaptive Security Appliance (ASA) to communicate with a Microsoft Windows 2008 Network Policy Server (NPS) with the RADIUS protocol so that the legacy Cisco VPN Client/AnyConnect/Clientless WebVPN users are authenticated against Active Directory. NPS is one of the server roles offered by Windows 2008 Server. It is equivalent to Windows 2003 Server, IAS (Internet Authentication Service), which is the implementation of a RADIUS server to provide remote dial-in user authentication. Similarly, in Windows 2008 Server, NPS is the implementation of a RADIUS server. Basically, the ASA is a RADIUS client to an NPS RADIUS server. ASA sends RADIUS authentication requests on behalf of VPN users and NPS authenticates them against Active Directory.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

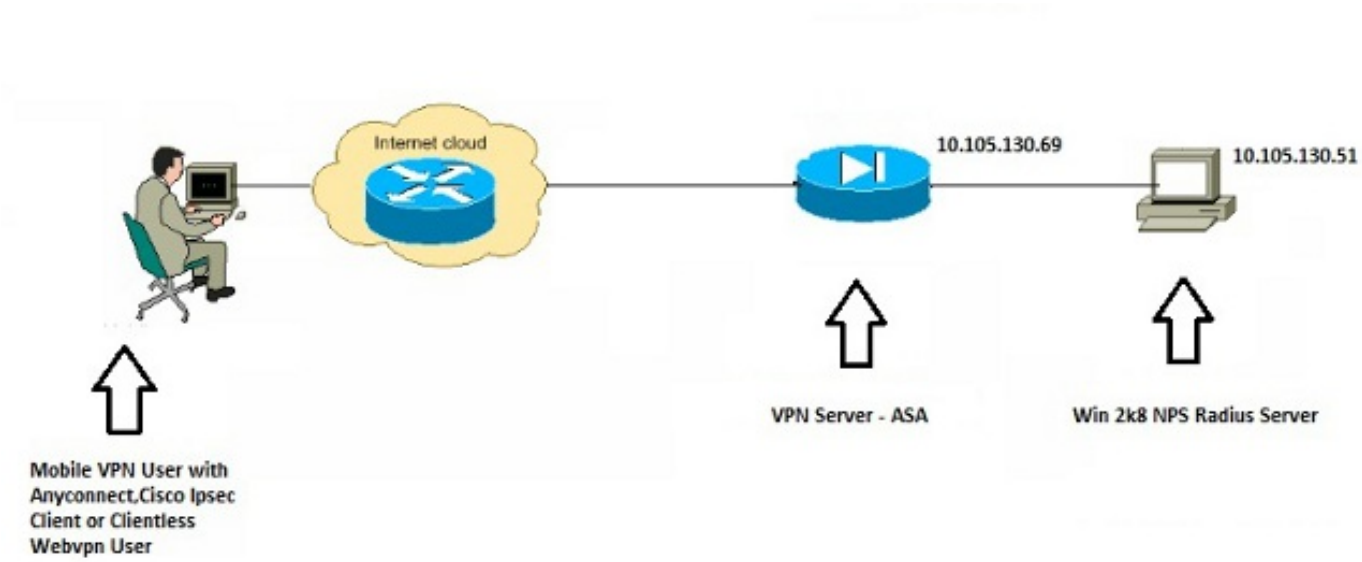
- ASA that runs Version 9.1(4)
- Windows 2008 R2 Server with Active Directory services and NPS role installed

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

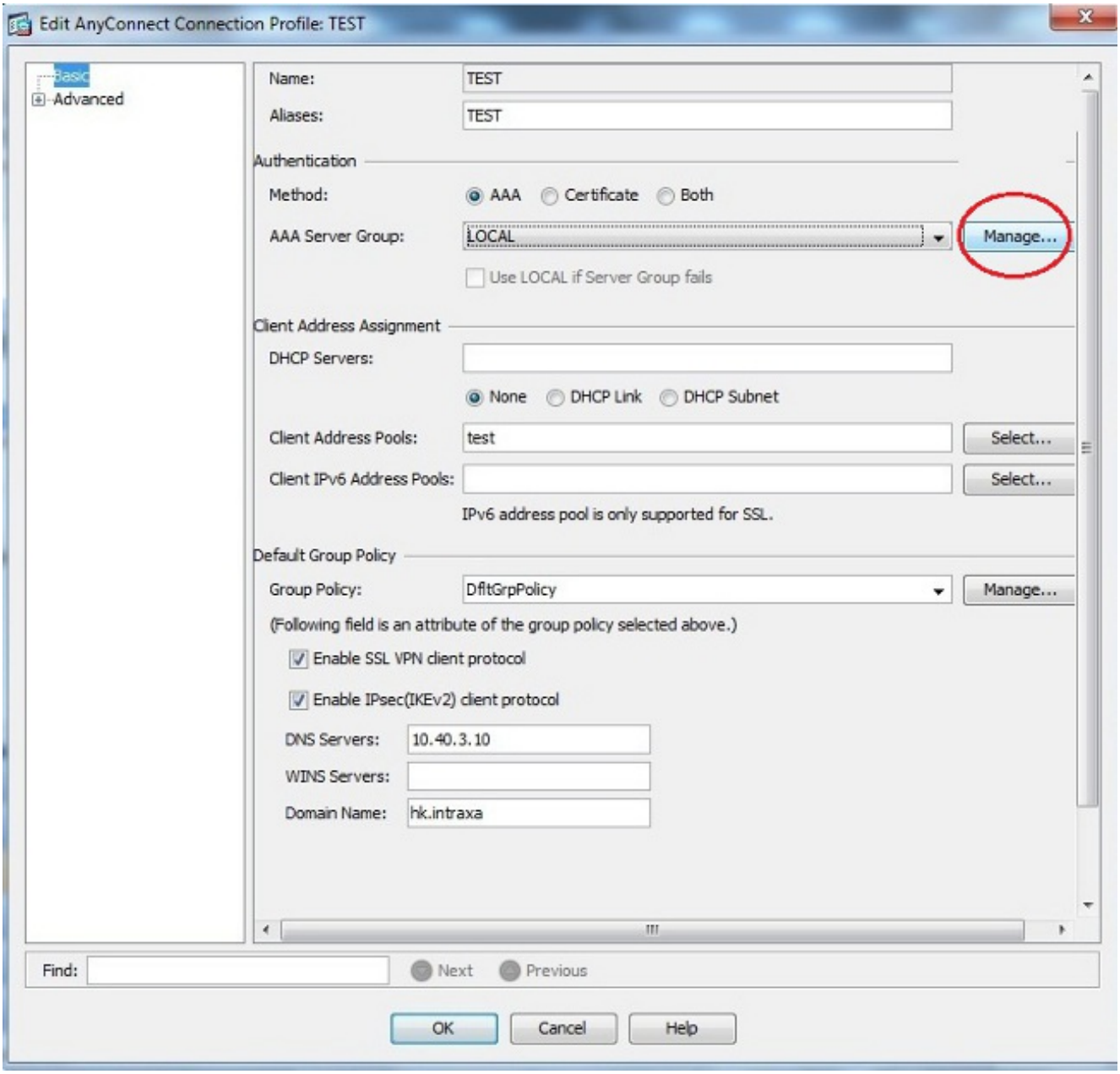
Network Diagram



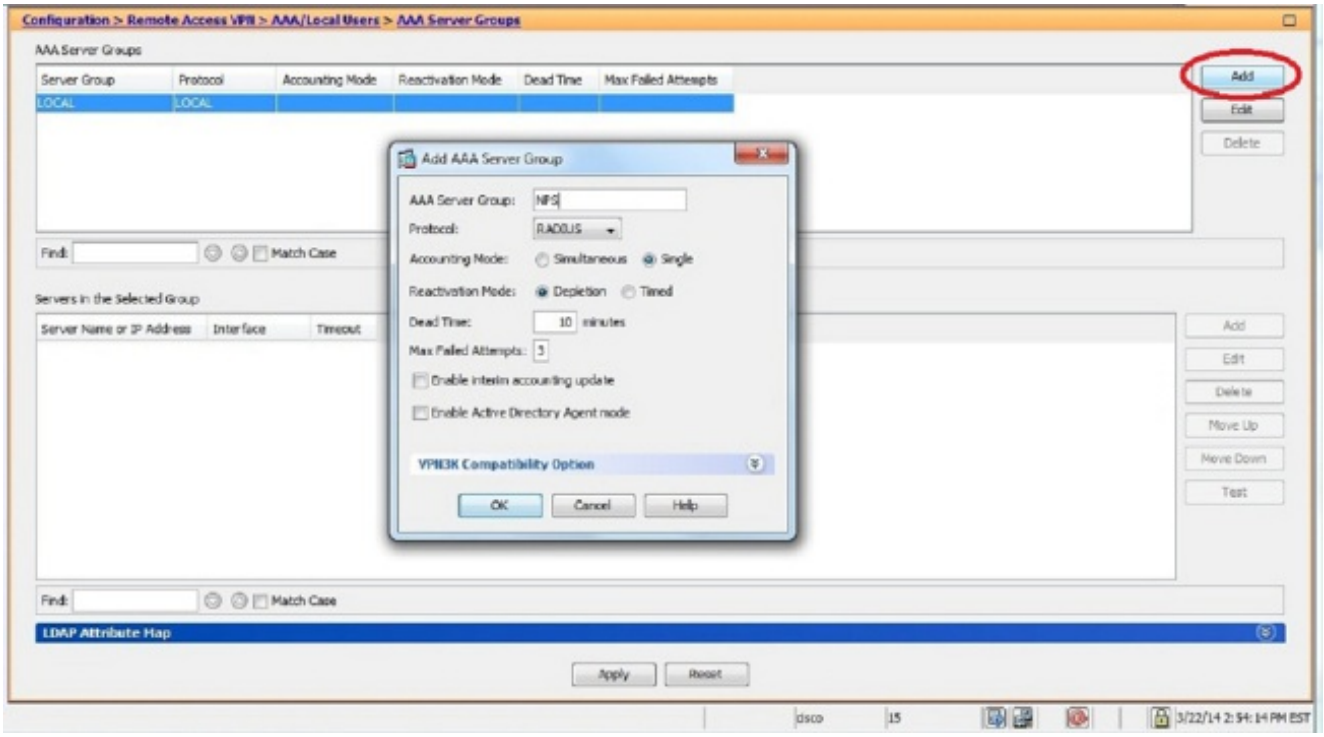
Configurations

ASDM Configuration

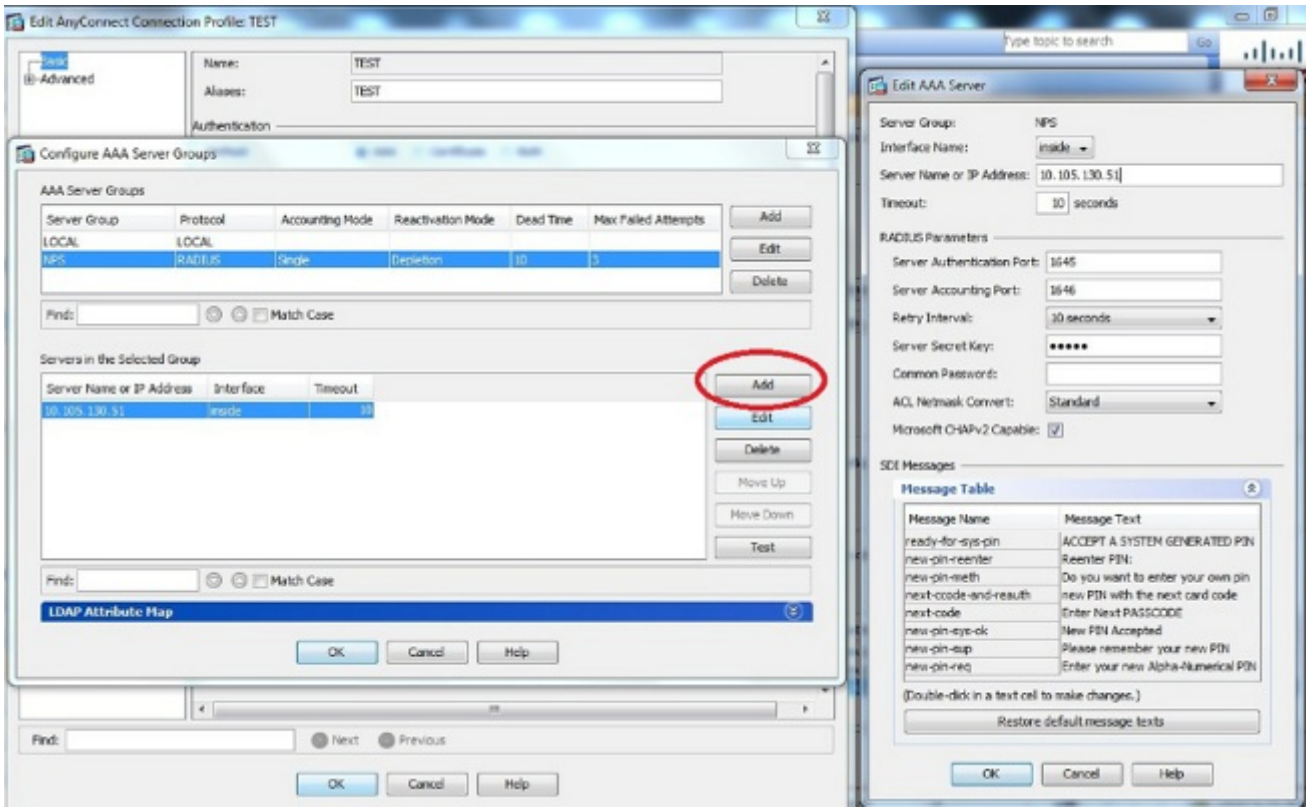
1. Choose the tunnel-group for which NPS authentication is required.
2. Click **Edit** and choose **Basic**.
3. In the Authentication section, click **Manage**.



4. In the AAA Server Groups section, click **Add**.
5. In the AAA Server Group field, enter the name of the server group (for example, NPS).
6. From the Protocol drop-down list, choose **RADIUS**.
7. Click
   OK.

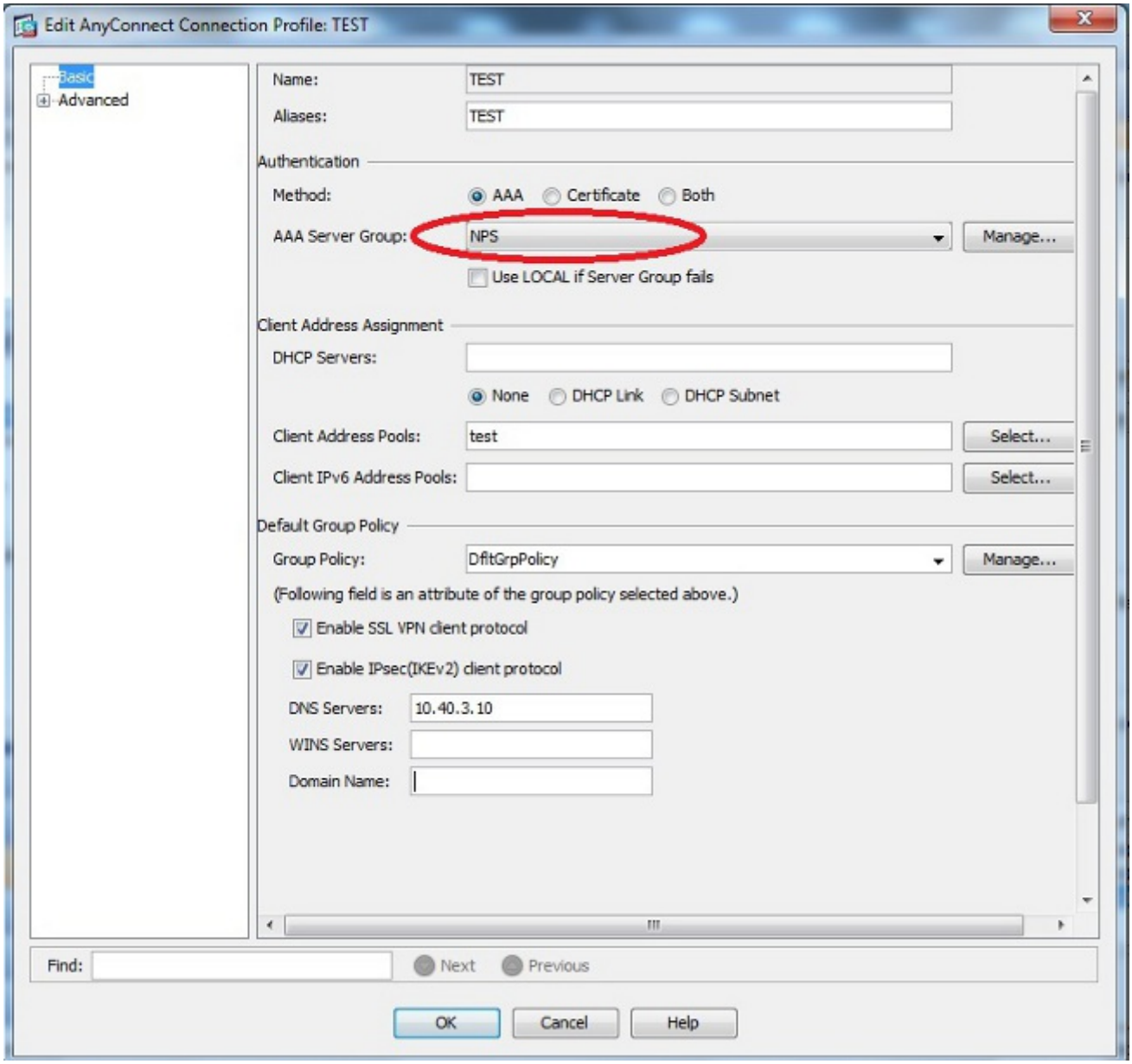


8. In the Servers in the Selected Group section, choose the AAA Server Group added and click **Add**.
9. In the Server Name or IP Address field, enter the server IP address.
10. In the Server Secret Key field, enter the secret key.
11. Leave the Server Authentication Port and the Server Accounting Port fields at the default value unless the server listens on a different port.
12. Click **OK**.
13. Click **OK**.



14. From the AAA Server Group drop-down list, choose the group (NPS in this example) added in the previous steps.
15. Click

OK.



CLI Configuration

```
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
```

By default, the ASA uses the unencrypted Password Authentication Protocol (PAP) authentication type. This does not mean that the ASA sends the password in plain text when it sends the RADIUS REQUEST packet. Rather, the plaintext password is encrypted with the RADIUS shared secret.

If password management is enabled under the tunnel-group, then ASA uses the MSCHAP-v2

authentication type in order to encrypt the plaintext password. In such a case, ensure that the **Microsoft CHAPv2 Capable** check box is checked in the Edit AAA Server window configured in the ASDM configuration section.

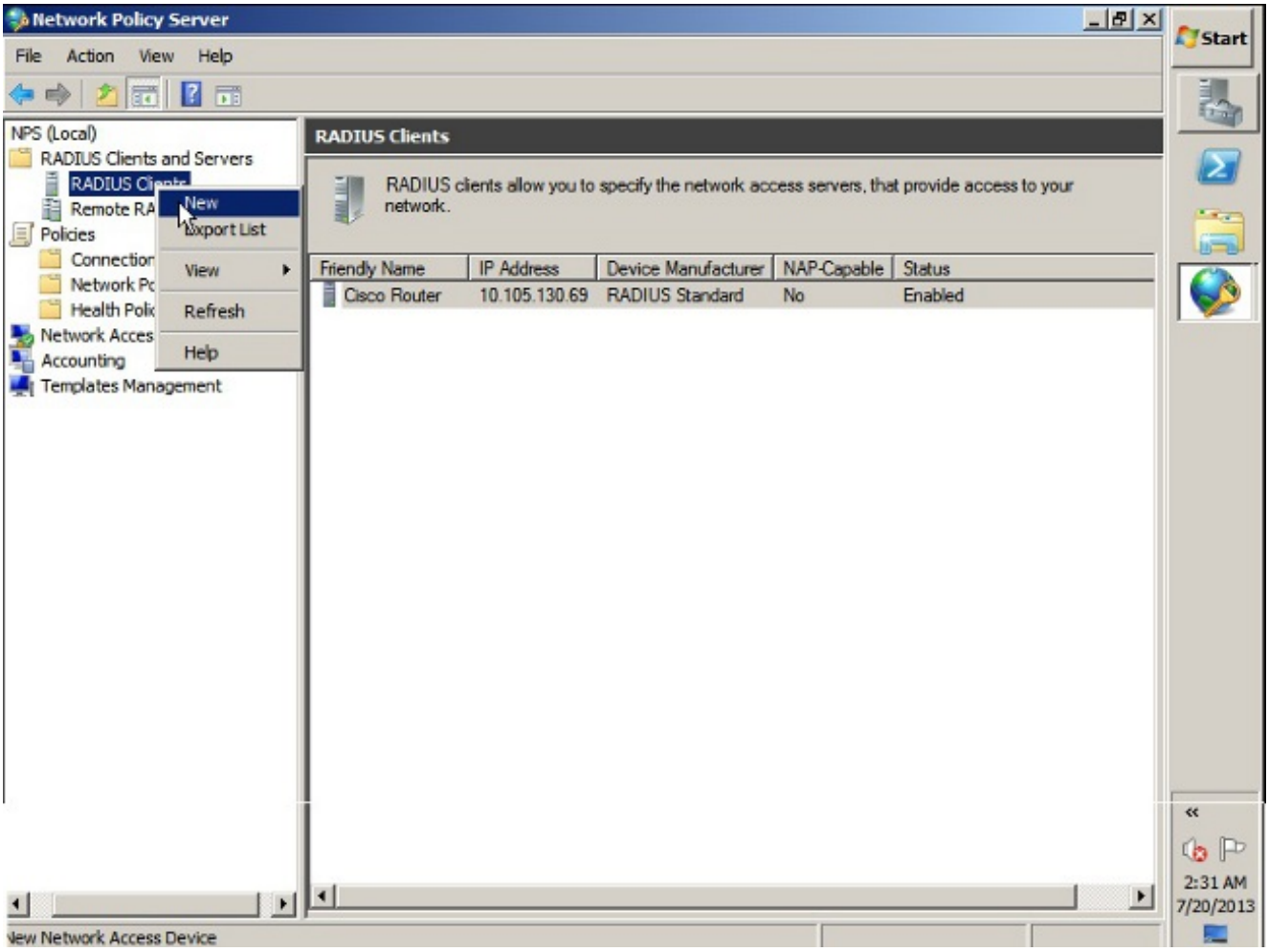
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **Note**: The **test aaa-server authentication** command always uses PAP. Only when a user initiates a connection to tunnel-group with password-management enabled does the ASA use MSCHAP-v2. Also, the 'password-management [password-expire-in-days days]' option is only supported with Lightweight Directory Access Protocol (LDAP). RADIUS does not provide this feature. You will see the password expire option when the password is already expired in Active Directory.

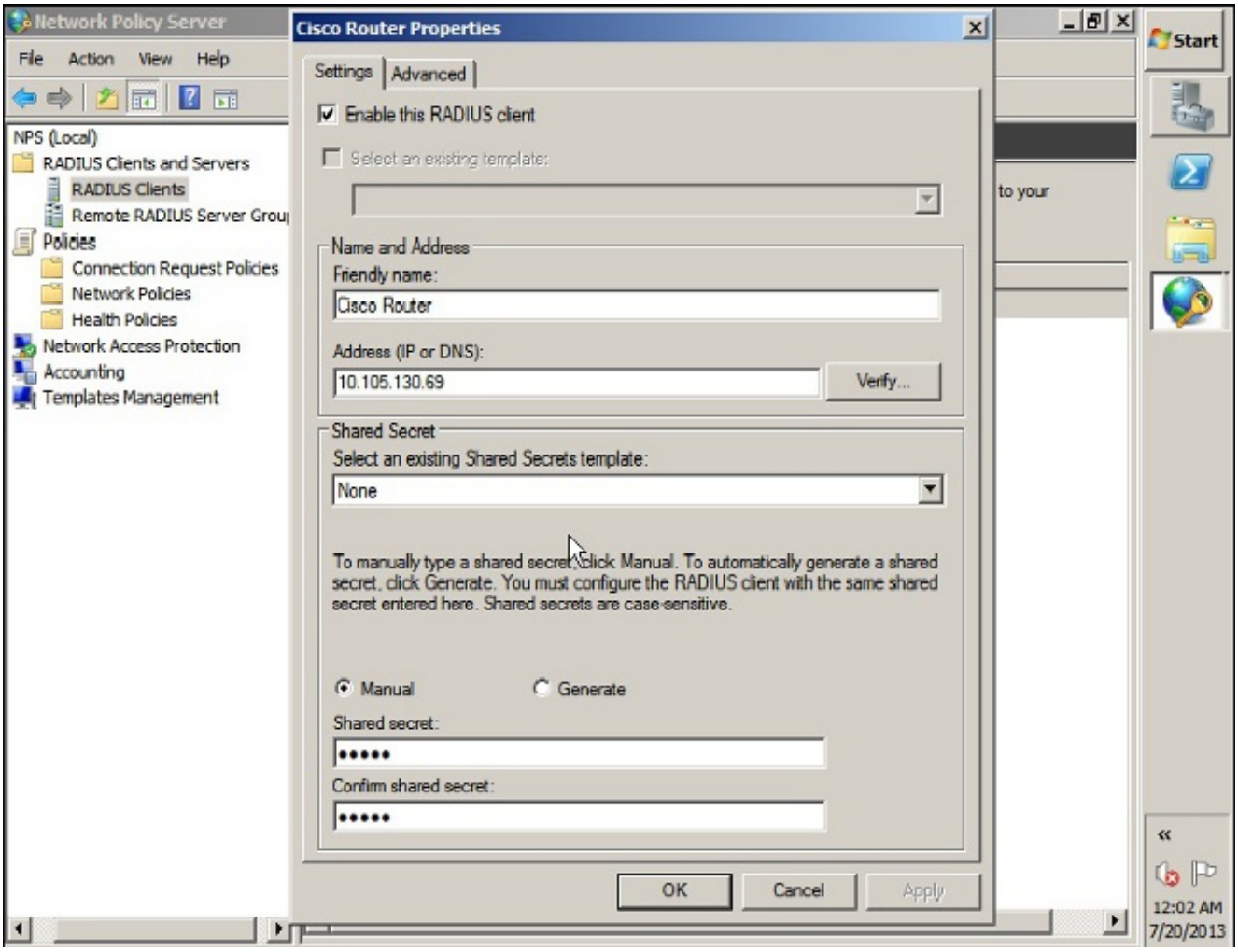
Windows 2008 Server with NPS Configuration

The NPS Server Role should be installed and running on the Windows 2008 server. If not, choose **Start > Administrative Tools > Server Roles > Add Role Services**. Choose the Network Policy Server and install the software. Once the NPS Server Role is installed, complete these steps in order to configure the NPS to accept and process RADIUS authentication requests from the ASA:

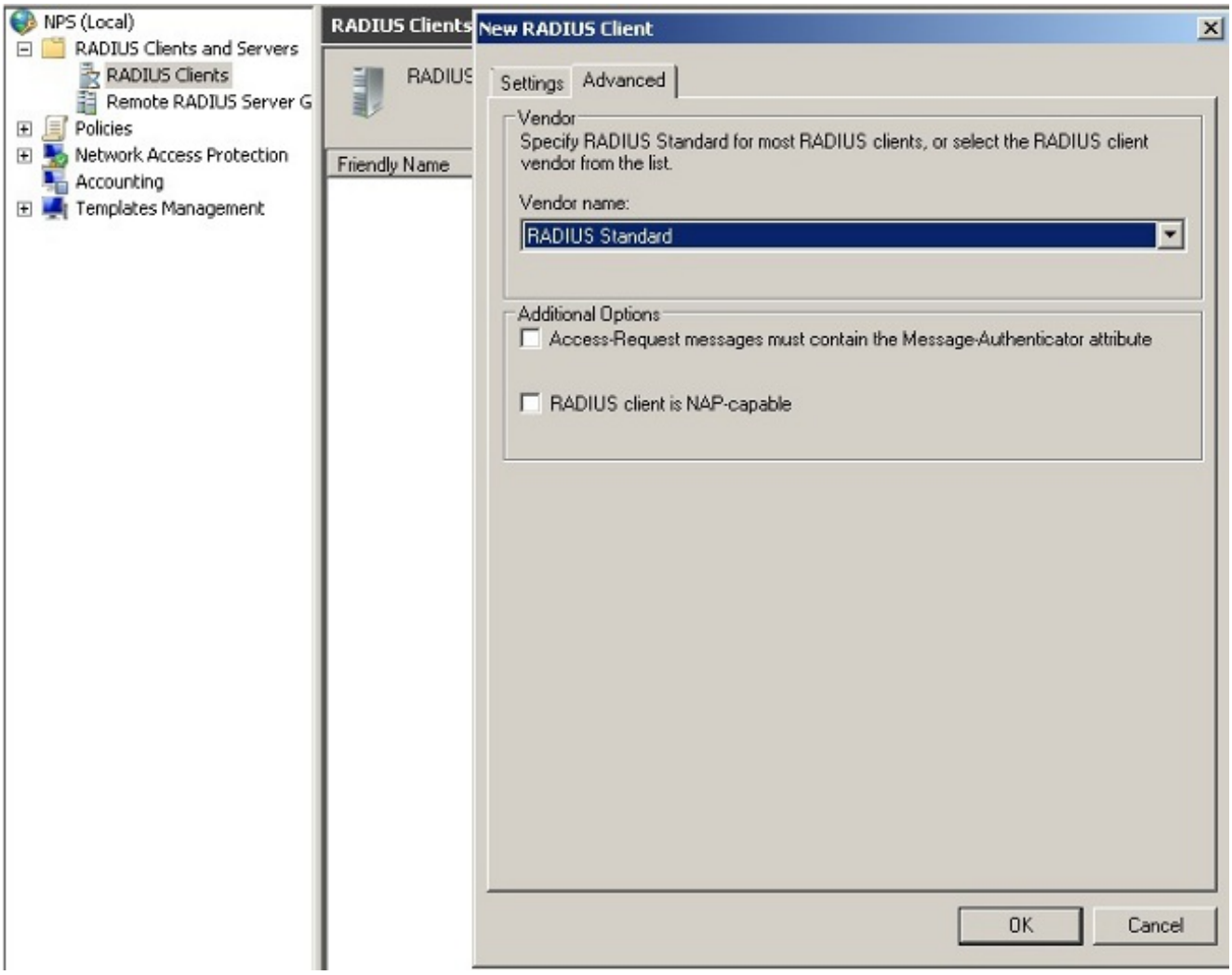
1. Add the ASA as a RADIUS client in the NPS server. Choose **Administrative Tools > Network Policy Server.**Right-click **RADIUS Clients** and choose **New**.



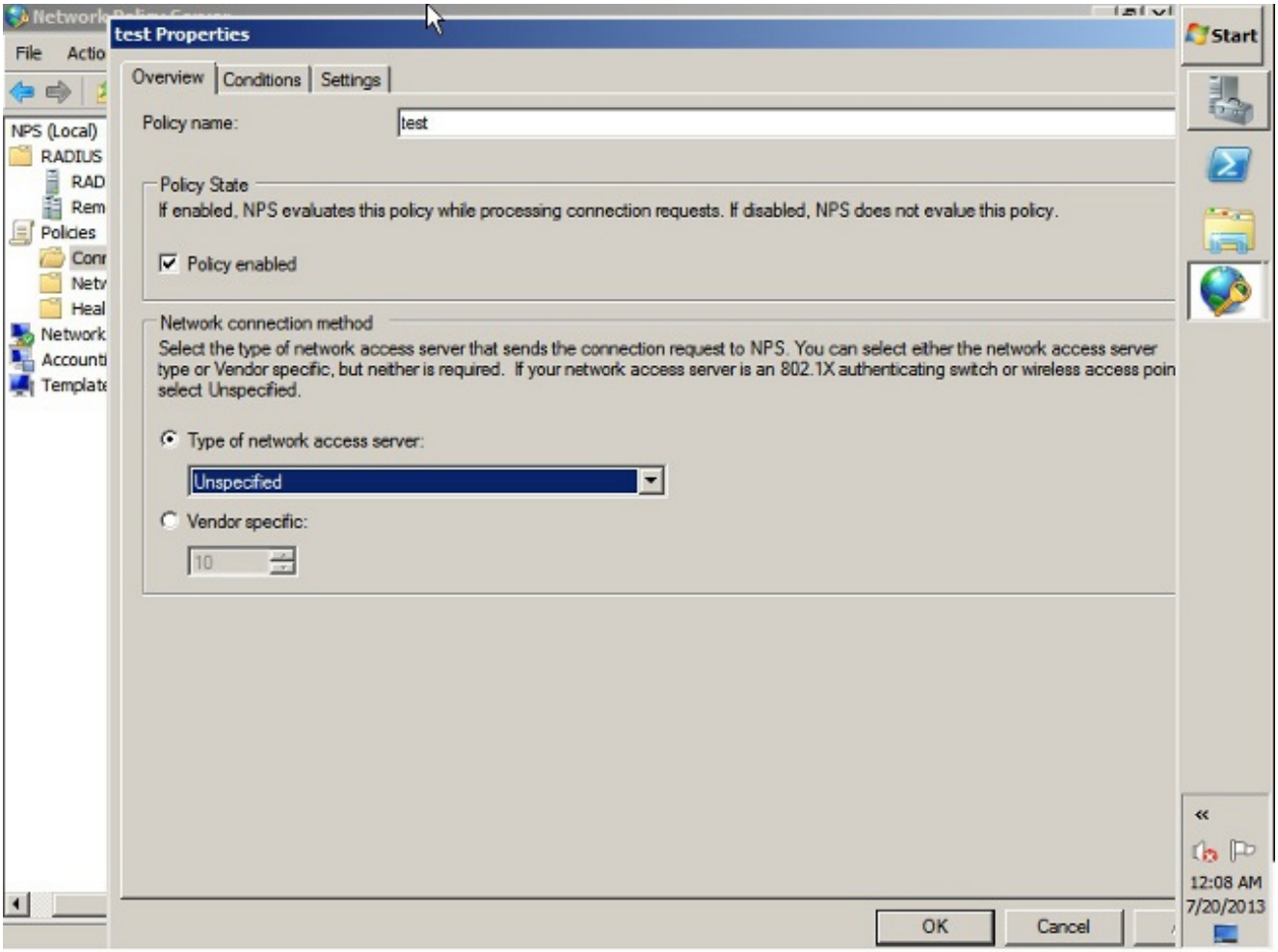
Enter a Friendly name, Address (IP or DNS), and Shared Secret configured on the ASA.



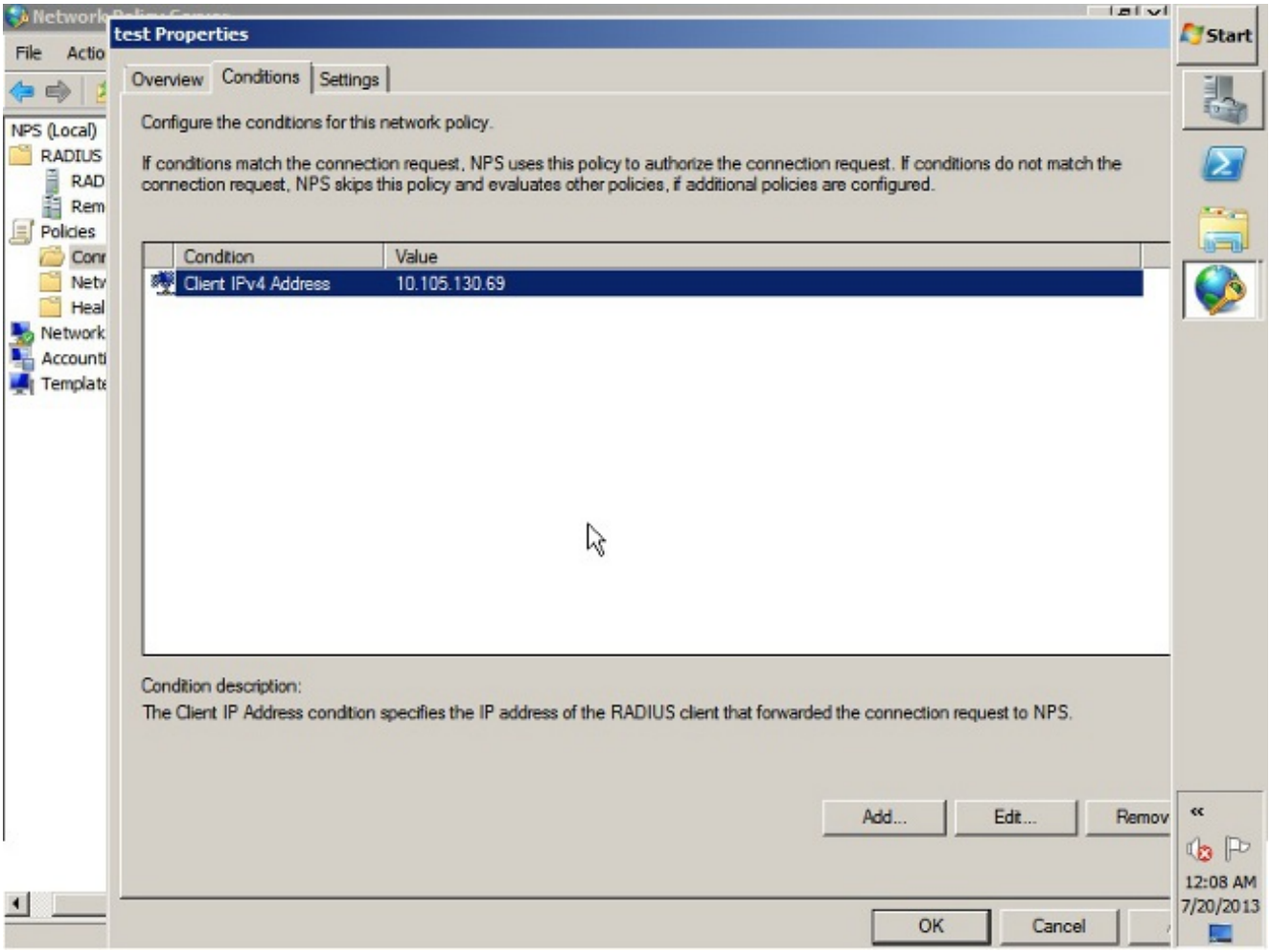
Click the **Advanced** tab.From the Vendor name drop-down list, choose **RADIUS Standard**.Click
OK.



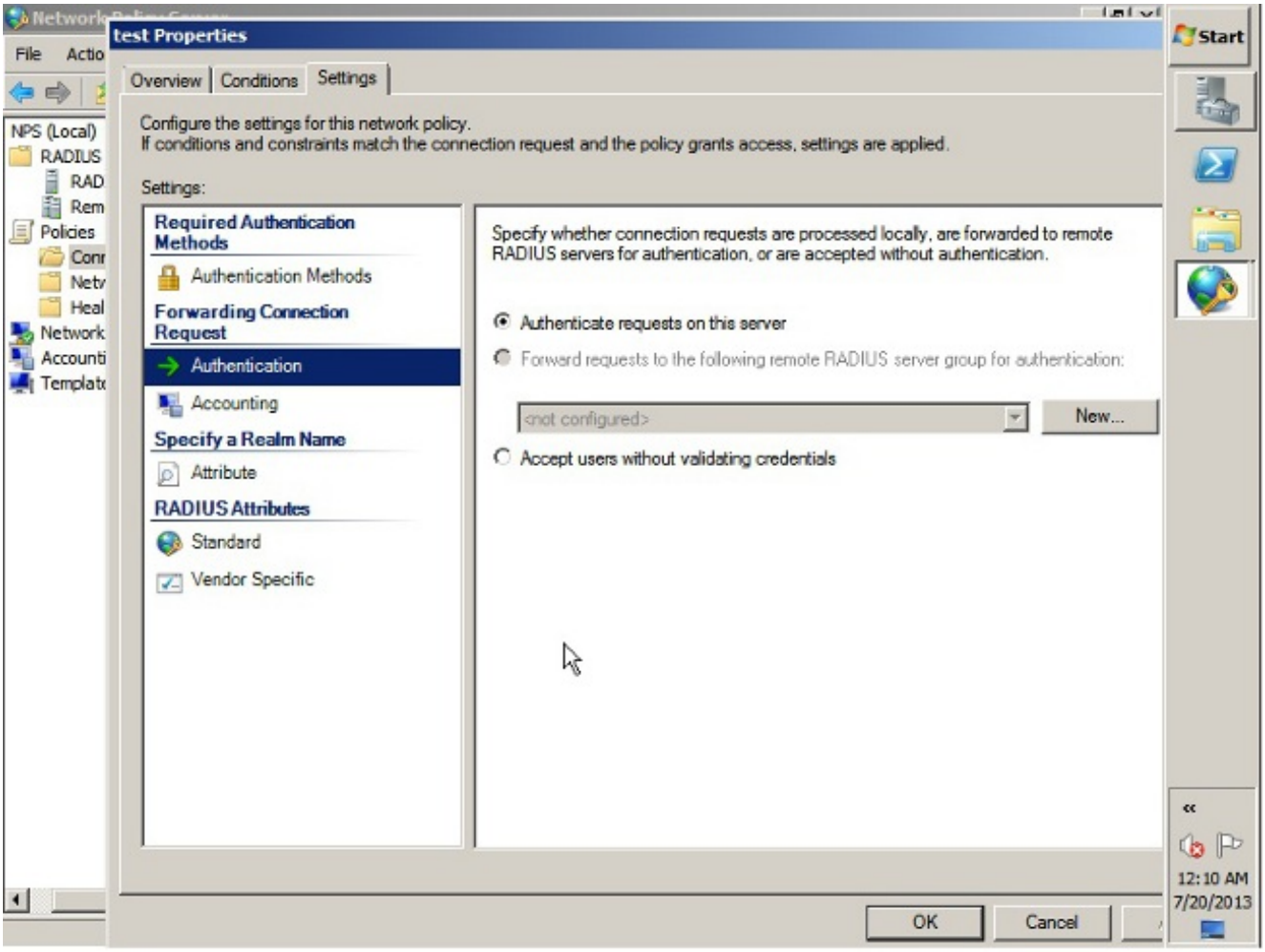
2. Create a new Connection Request Policy for VPN users. The purpose of the Connection Request Policy is to specify whether the requests from RADIUS clients are to be processed locally or forwarded to remote RADIUS servers. Under NPS > Policies, right-click **Connection Request Policies** and create a new policy.From the Type of network access server drop-down list, choose **Unspecified**.



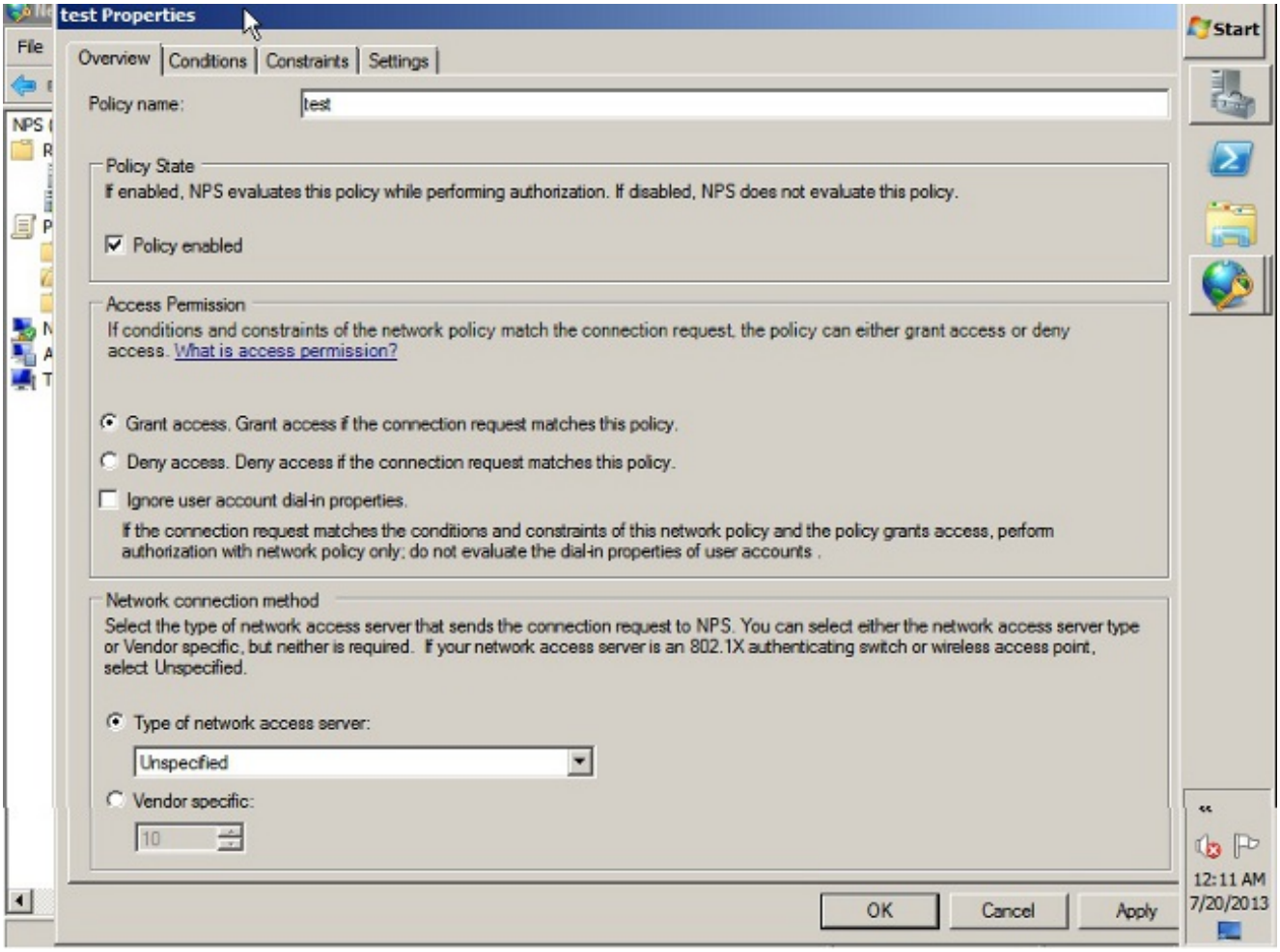
Click the **Conditions** tab.Click **Add**.Enter the ASA's IP address as a 'Client IPv4 Address' condition.



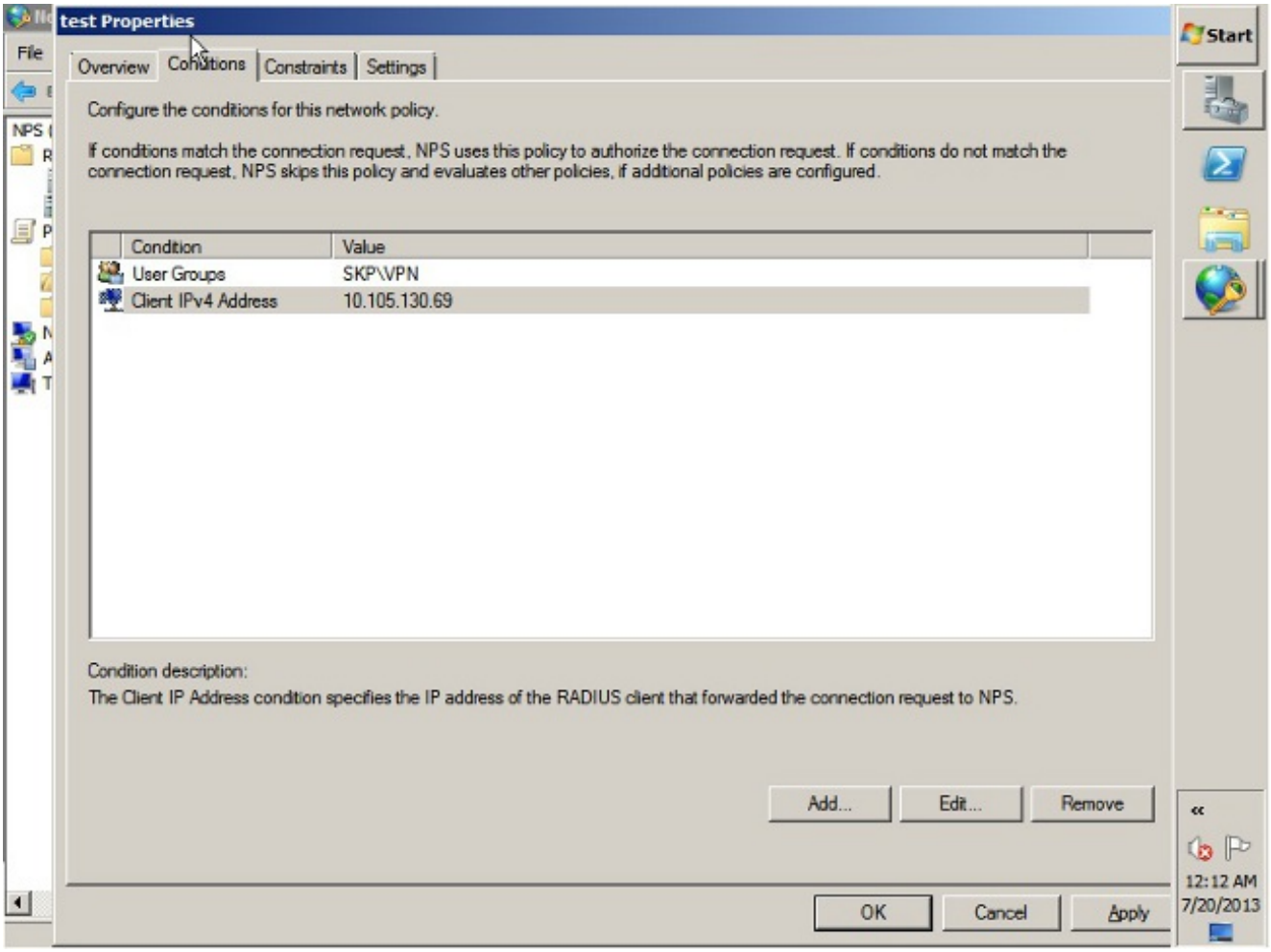
Click the **Settings** tab.Under Forwarding Connection Request, choose **Authentication**. Ensure the Authenticate requests on this server radio button is chosen.Click **OK**.



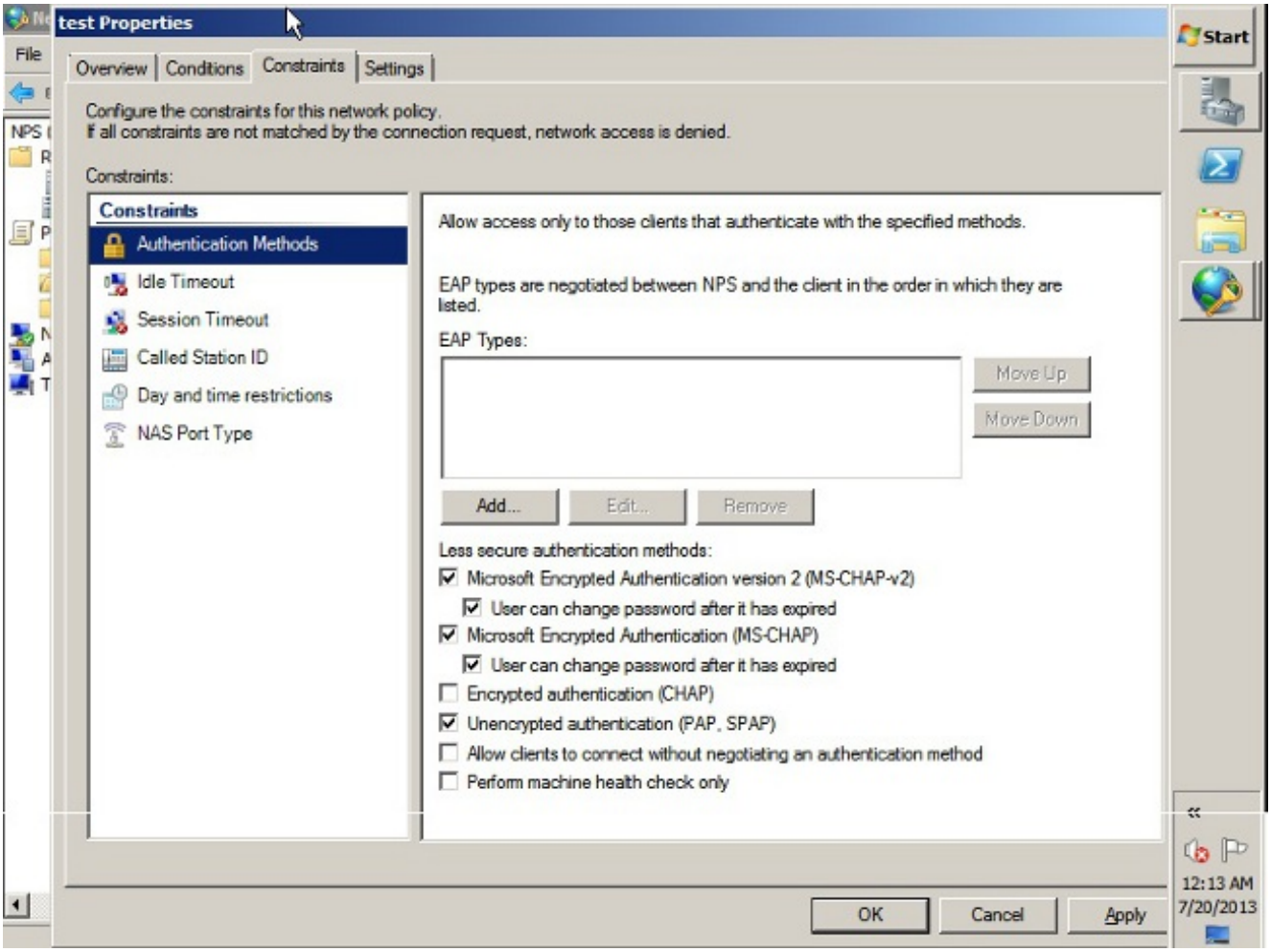
3. Add a Network Policy where you can specify which users are allowed to authenticate.For example, you can add Active Directory user groups as a condition. Only those users who belong to a specified Windows group are authenticated under this policy.Under NPS, choose **Policies**.Right-click **Network Policy** and create a new policy.Ensure the Grant access radio button is chosen.From the Type of network access server drop-down list, choose **Unspecified**.



Click the **Conditions** tab.Click **Add**.Enter the ASA's IP address as a Client IPv4 Address condition.Enter the Active Directory user group which contains VPN users.



Click the **Constraints** tab.Choose **Authentication Methods**.Ensure the Unencrypted authentication (PAP, SPAP) check box is checked.Click
OK.

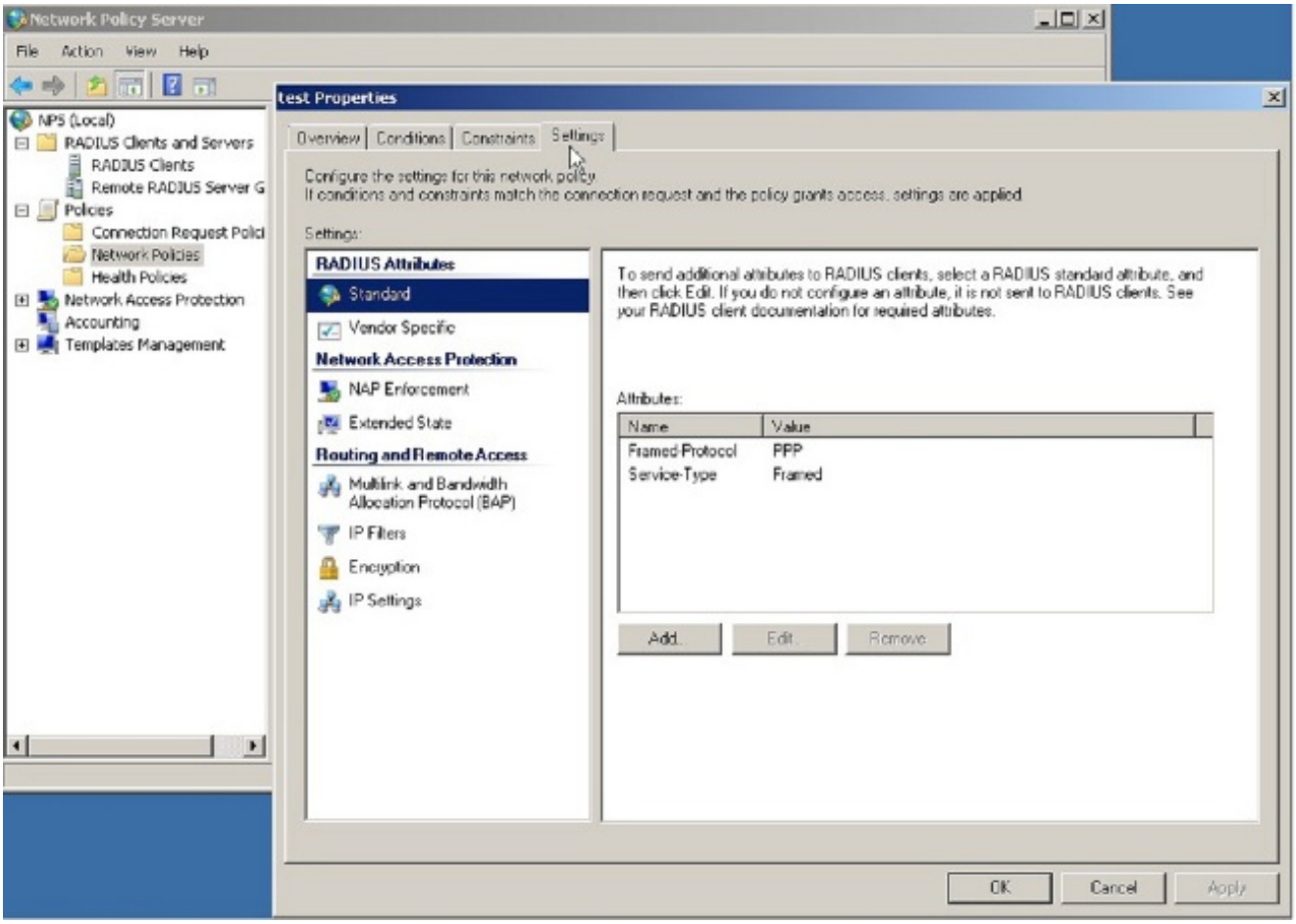


Pass Group-policy Attribute (Attribute 25) from the NPS RADIUS Server

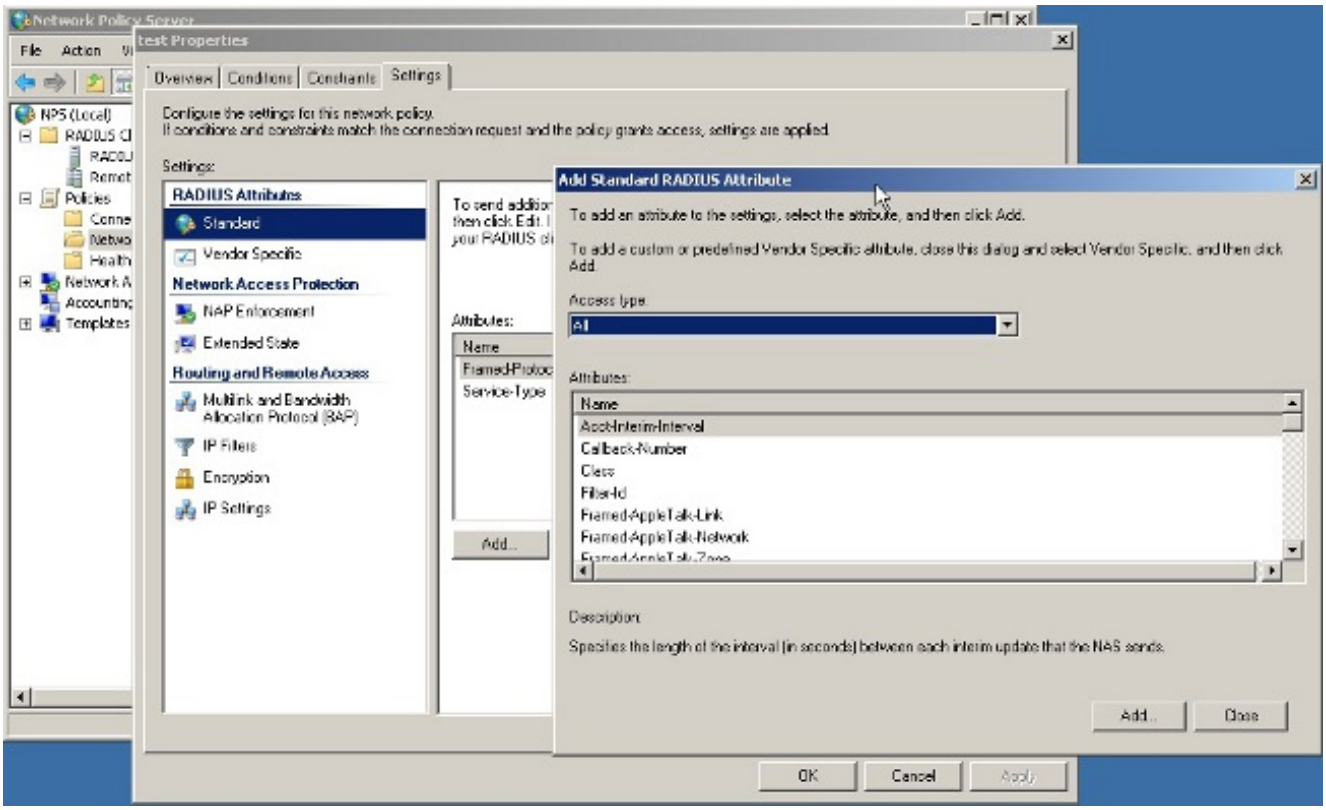
If the group-policy needs to be assigned to the user dynamically with the NPS RADIUS server, the group-policy RADIUS attribute (attribute 25) can be used.

Complete these steps in order to send the RADIUS attribute 25 for dynamic assignment of a group-policy to the user.

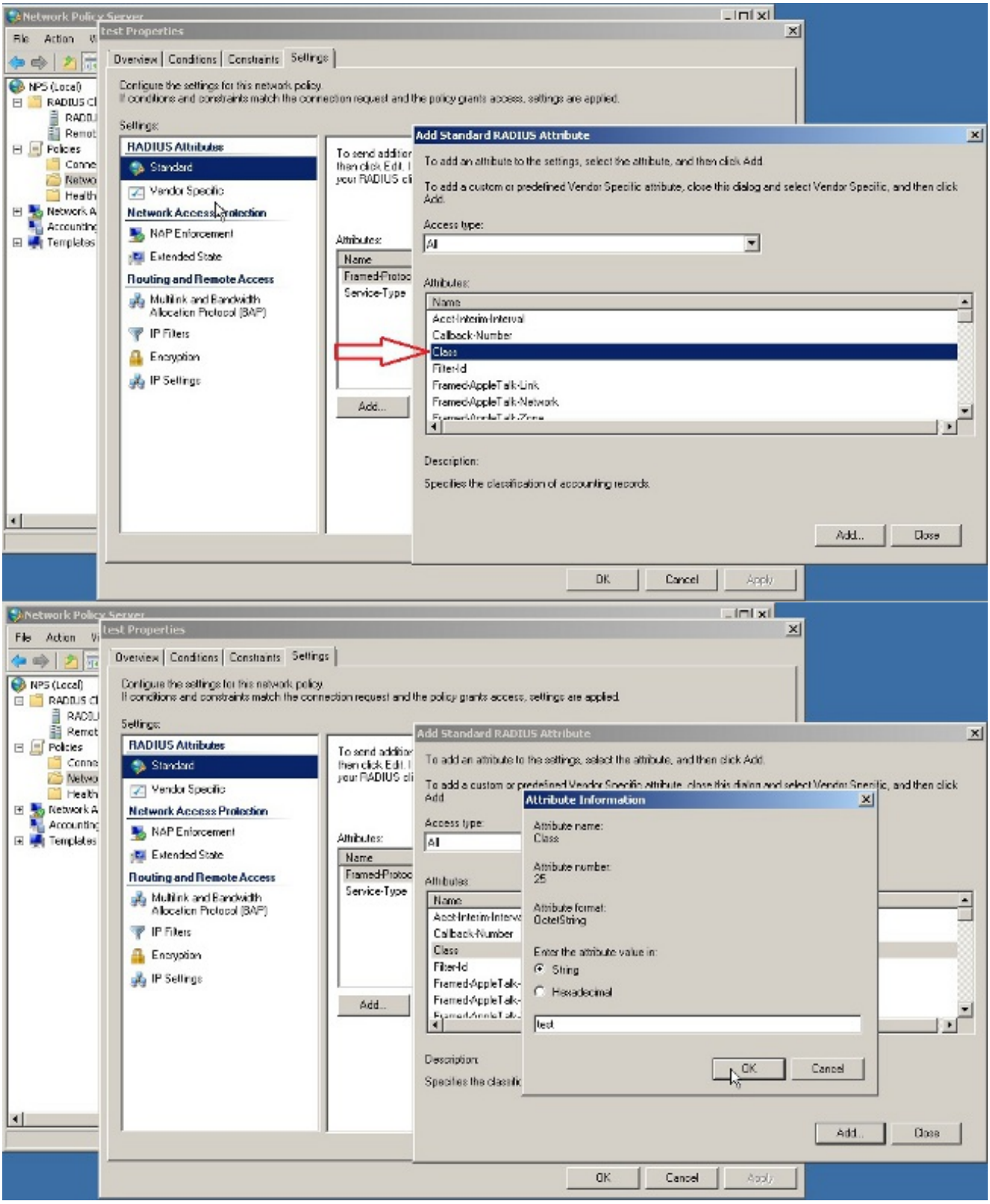
1. After the Network Policy is added, right -click the required Network Policy and click the **Settings**
   tab.



2. Choose **RADIUS Attributes > Standard**. Click **Add**. Leave the Access type as All.



3. In the Attributes box, choose **Class** and click **Add**. Enter the attribute value, that is, the name of the group-policy as a string. Remember that a group-policy with this name has to be configured in the ASA. This is so that the ASA assigns it to the VPN session after it receives this attribute in the RADIUS response.



Verify

Use this section to confirm that your configuration works properly.

> **Note**: Refer to Important Information on Debug Commands before you use **debug** commands.

ASA Debugs

Enable **debug radius all** on the ASA.

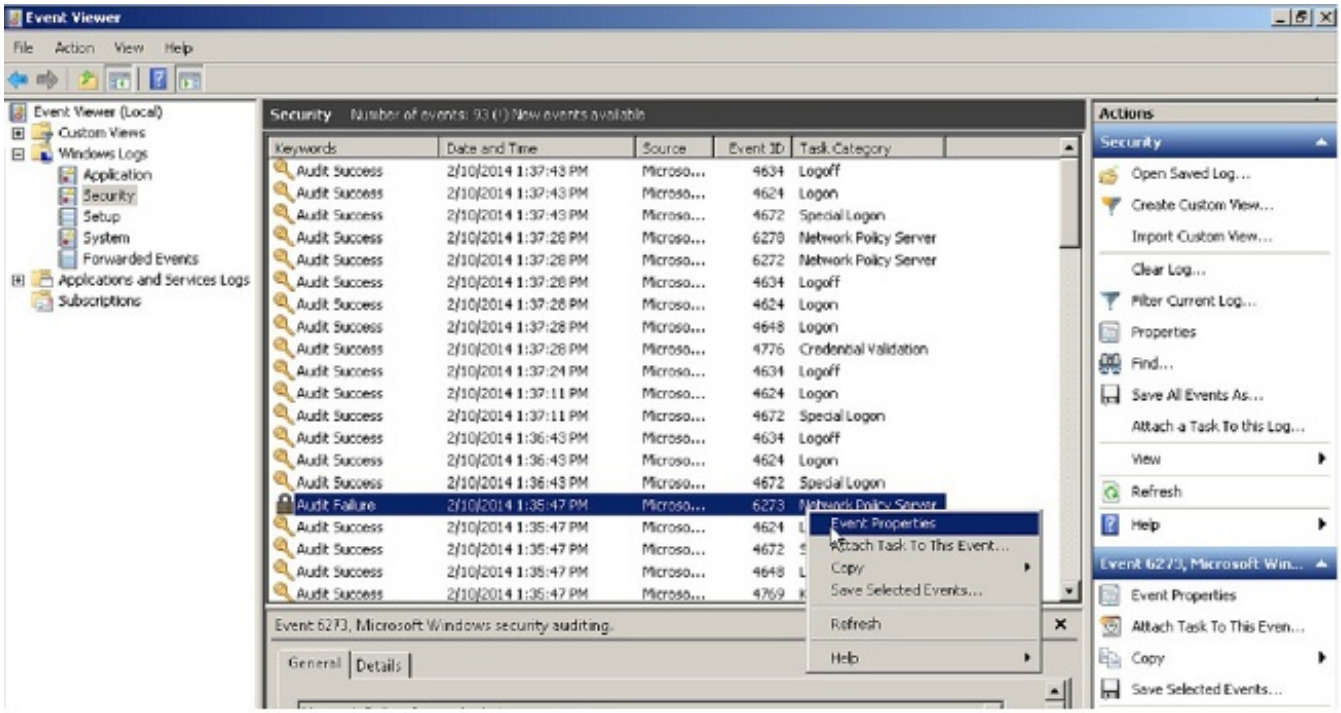
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- Ensure the connectivity between the ASA and the NPS server is good.Apply packet captures to ensure the authentication request leaves the ASA interface (from where the server is reachable). Confirm that the devices in the path do not block the UDP port 1645 (default RADIUS authentication port) in order to ensure it reaches the NPS server. More information on packet captures on the ASA can be found in ASA/PIX/FWSM: Packet Capturing using CLI and ASDM Configuration Example.
- If the authentication still fails, look in the event viewer on the windows NPS. Under Event Viewer > Windows Logs, choose **Security.** Look for events associated with NPS around the time of the authentication
  request.



Once you open Event Properties, you should be able to see the reason for failure as shown in the example. In this example, PAP was not chosen as the authentication type under Network policy. Hence, the authentication request fails.

```
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.
```