使用RADIUS对Windows 2008 NPS服务器(Active Directory)进行ASA VPN用户身份验证配置示例

目录

简介

本文档介绍如何配置自适应安全设备(ASA)以使用RADIUS协议与Microsoft Windows 2008网络策略服务器(NPS)通信，以便对传统Cisco VPN客户端/AnyConnect/无客户端WebVPN用户进行Active Directory身份验证。NPS是Windows 2008 Server提供的服务器角色之一。它相当于Windows 2003 Server， IAS（Internet身份验证服务），即RADIUS服务器的实施，提供远程拨入用户身份验证。同样，在Windows 2008服务器中，NPS是RADIUS服务器的实施。基本上，ASA是NPS RADIUS服务器的RADIUS客户端。ASA代表VPN用户发送RADIUS身份验证请求，NPS根据Active Directory对其进行身份验证。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

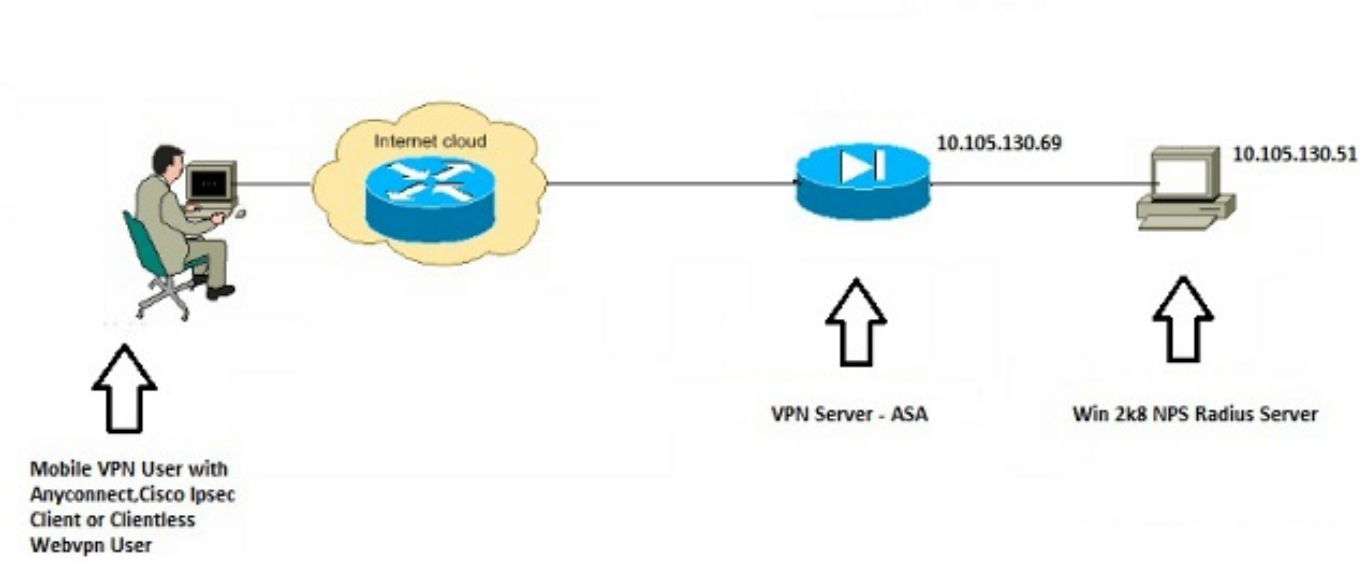
- 运行版本9.1(4)的ASA
- 安装了Active Directory服务和NPS角色的Windows 2008 R2服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

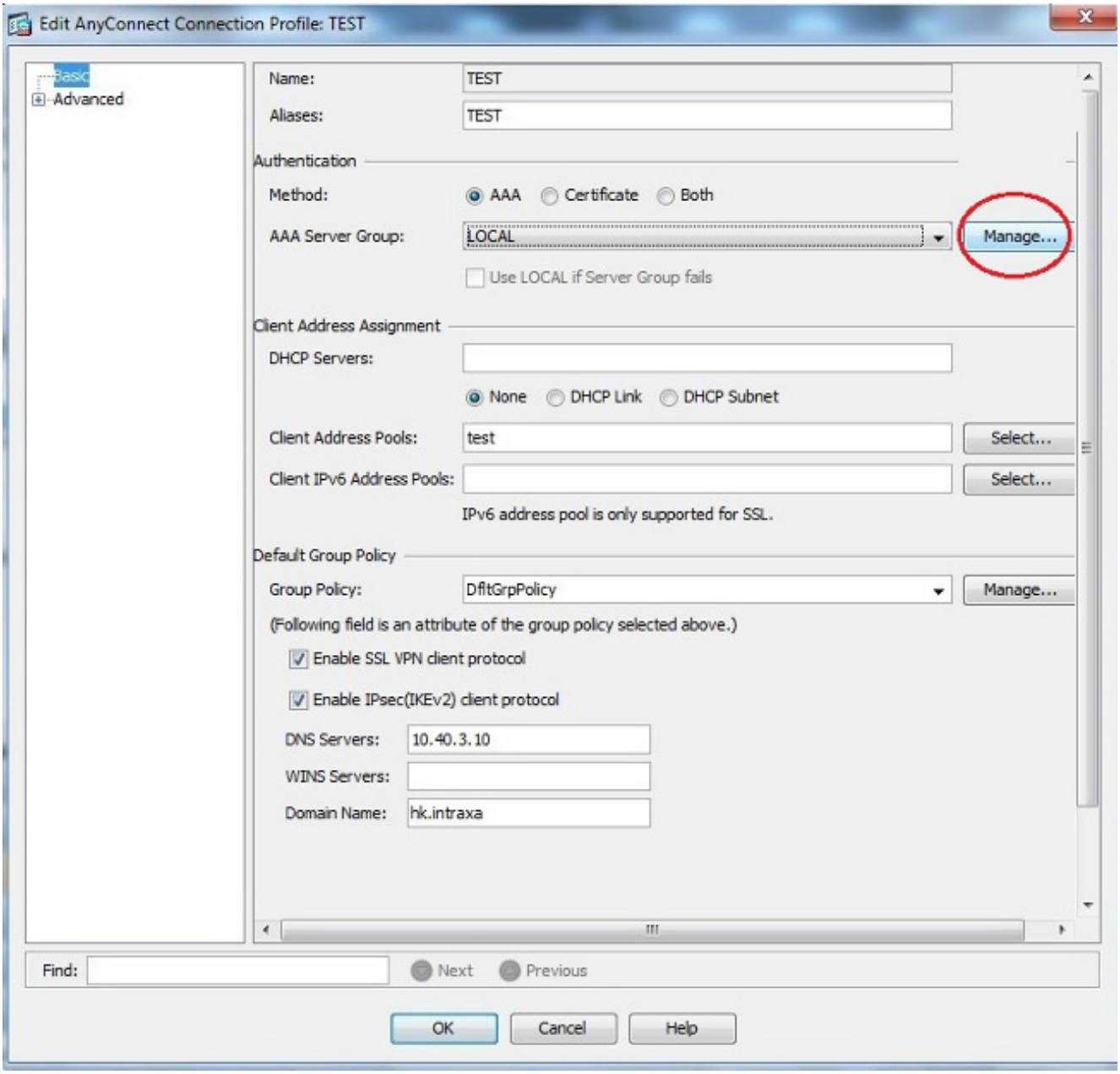
网络图



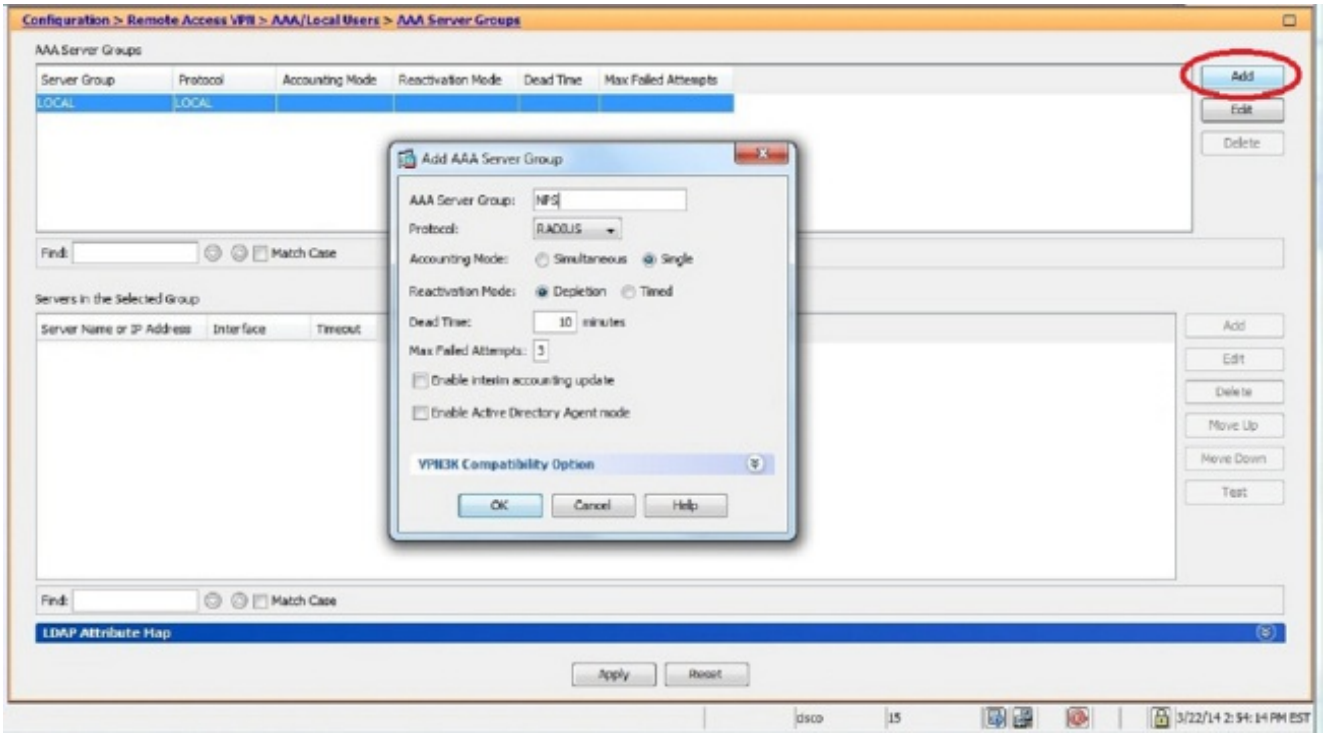
配置

ASDM 配置

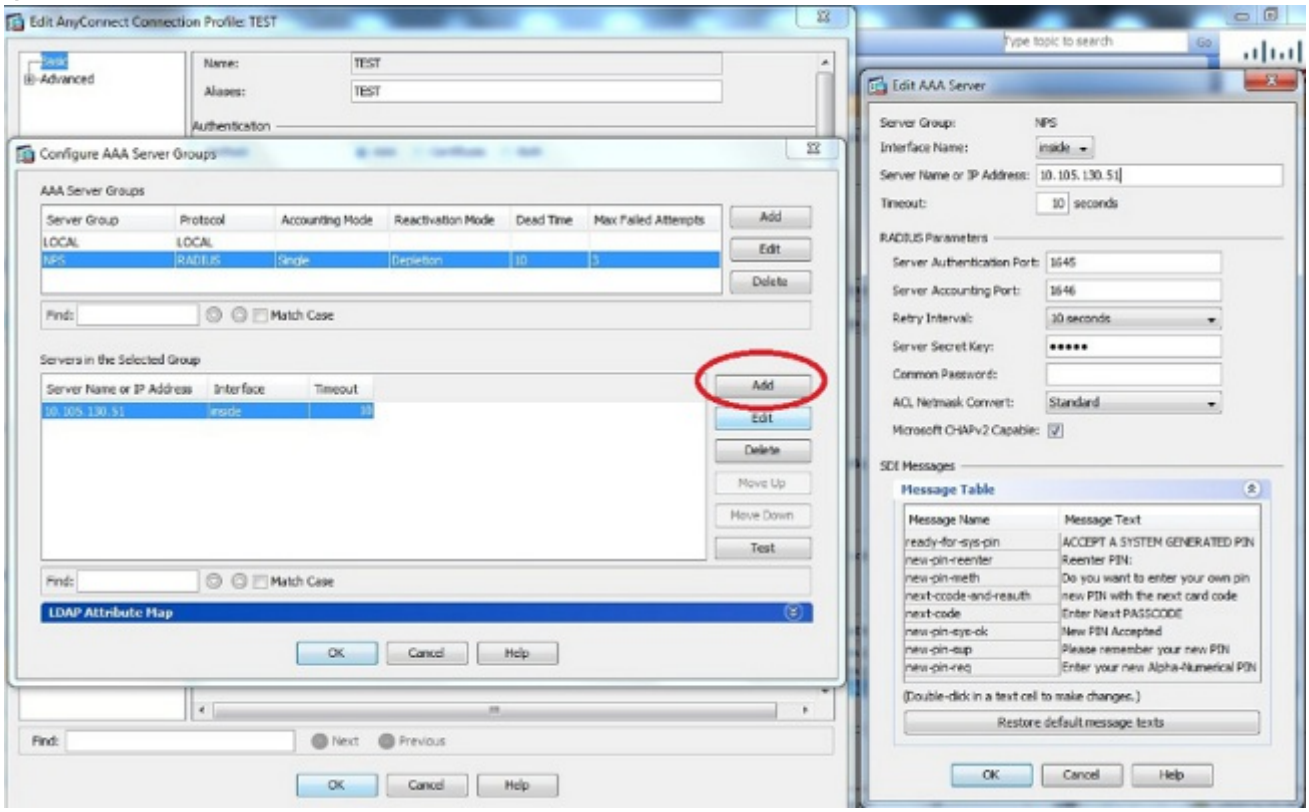
1. 选择需要NPS身份验证的隧道组。
2. 单击“**编辑**”，然后选**择“基本**”。
3. 在“身份验证”部分，单击**管理**。



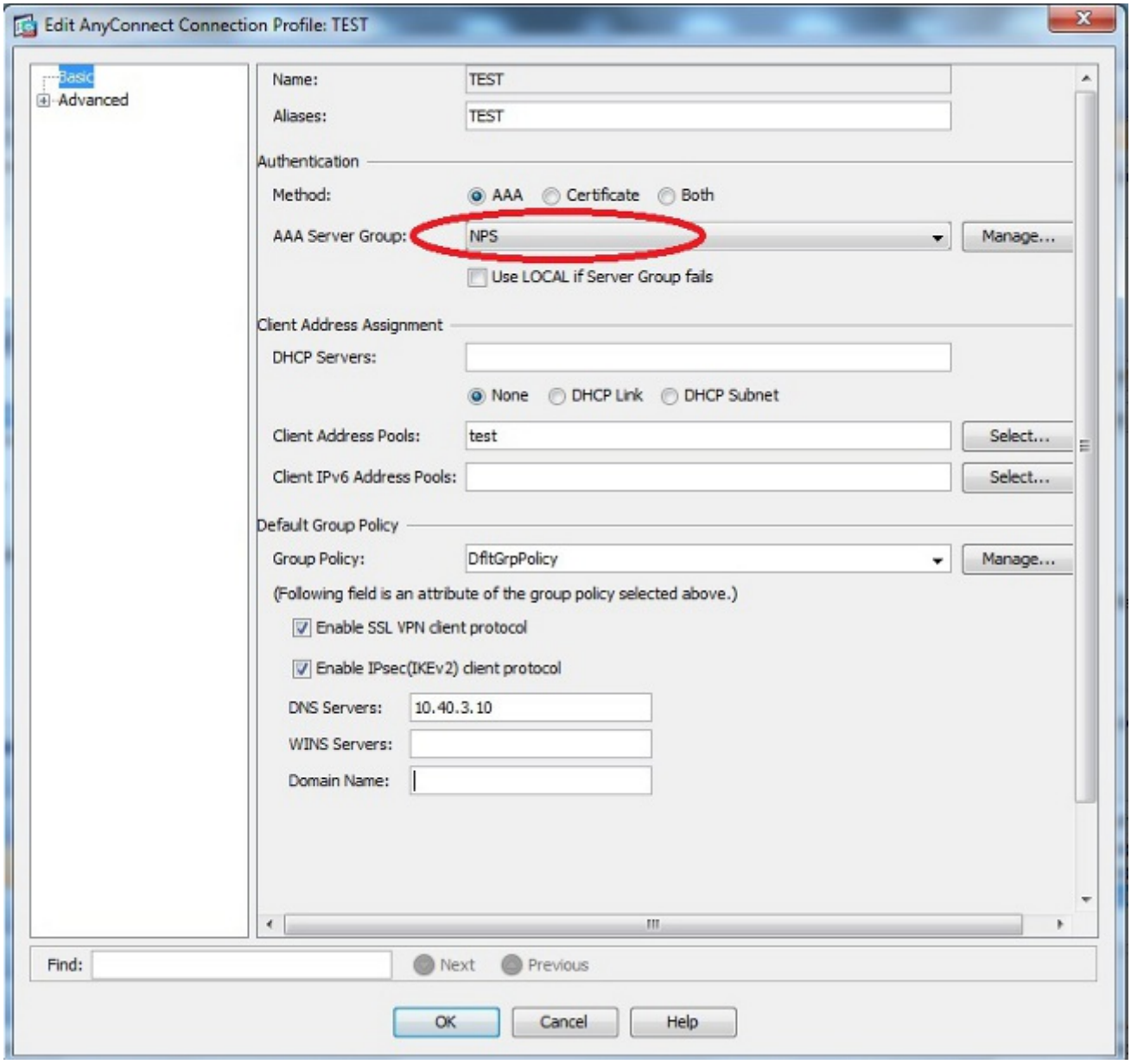
4. 在AAA Server Groups部分，单击**Add**。
5. 在AAA Server Group字段中，输入服务器组的名称（例如，NPS）。
6. 从Protocol下拉列表中，选择**RADIUS**。
7. Click
   OK.



8. 在Selected Group部分的Servers中，选择已添加的AAA Server Group，然后单击**Add**。
9. 在服务器名称或IP地址字段中，输入服务器IP地址。
10. 在Server Secret Key字段中，输入密钥。
11. 除非服务器侦听不同的端口，否则将服务器身份验证端口和服务器记帐端口字段保留为默认值。
12. Click **OK**.
13. Click **OK**.



14. 从AAA Server Group下拉列表中，选择在前面的步骤中添加的组（本例中为NPS）。
15. Click **OK**.



CLI 配置

```
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
```

默认情况下，ASA使用未加密的密码身份验证协议(PAP)身份验证类型。这并不意味着ASA在发送RADIUS REQUEST数据包时以明文形式发送密码。相反，明文密码使用RADIUS共享密钥加密。

如果在隧道组下启用密码管理，则ASA使用MSCHAP-v2身份验证类型来加密明文密码。在这种情况下，请确保在ASDM配置部**分配置的"编辑AAA服**务器"窗口中选中"支持Microsoft CHAPv2"复选框。

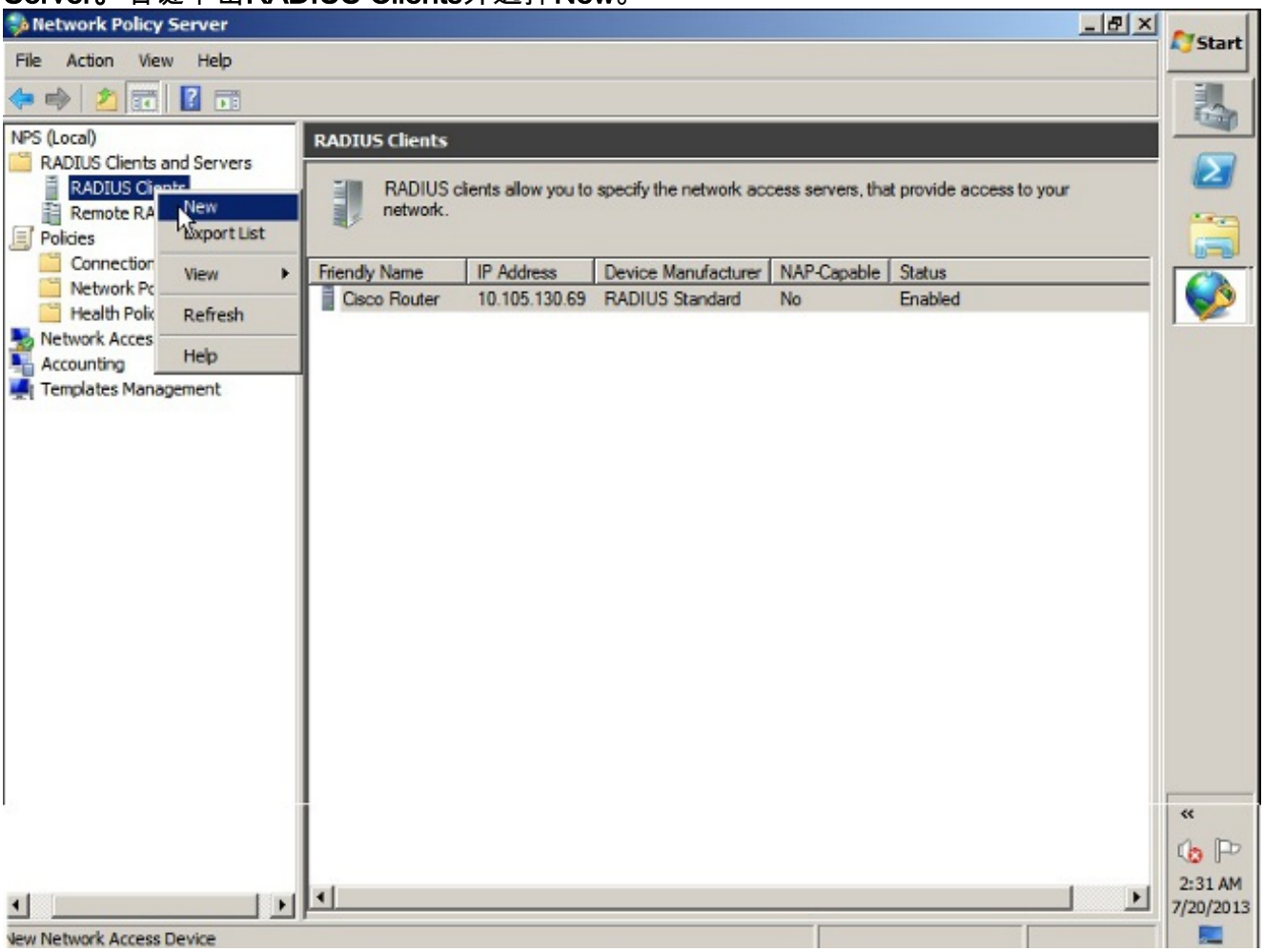
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

注意：test aaa-**server authentication命令始**终使用PAP。只有当用户启动与启用了密码管理的隧道组的连接时，ASA才使用MSCHAP-v2。此外，“密码管理[密码过期天数]”选项仅受轻量级目录访问协议(LDAP)支持。RADIUS不提供此功能。当密码在Active Directory中已过期时，您将看到密码过期选项。

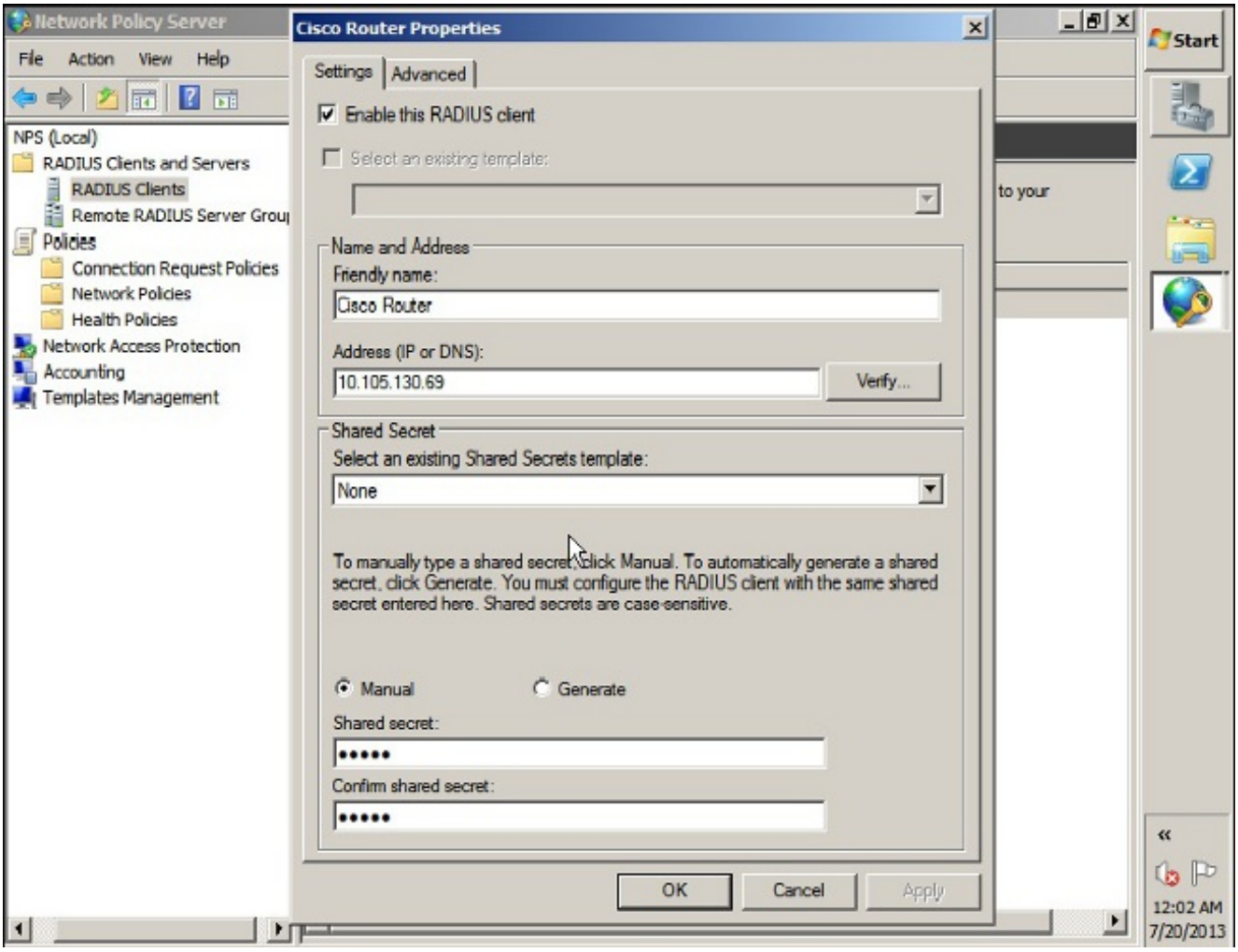
Windows 2008服务器，带NPS配置

NPS服务器角色应安装并运行在Windows 2008服务器上。否则，请选择开**始>管理工具>服务器角色>添加角色服务**。选择网络策略服务器并安装软件。安装NPS服务器角色后，请完成以下步骤，以便将NPS配置为接受和处理来自ASA的RADIUS身份验证请求：

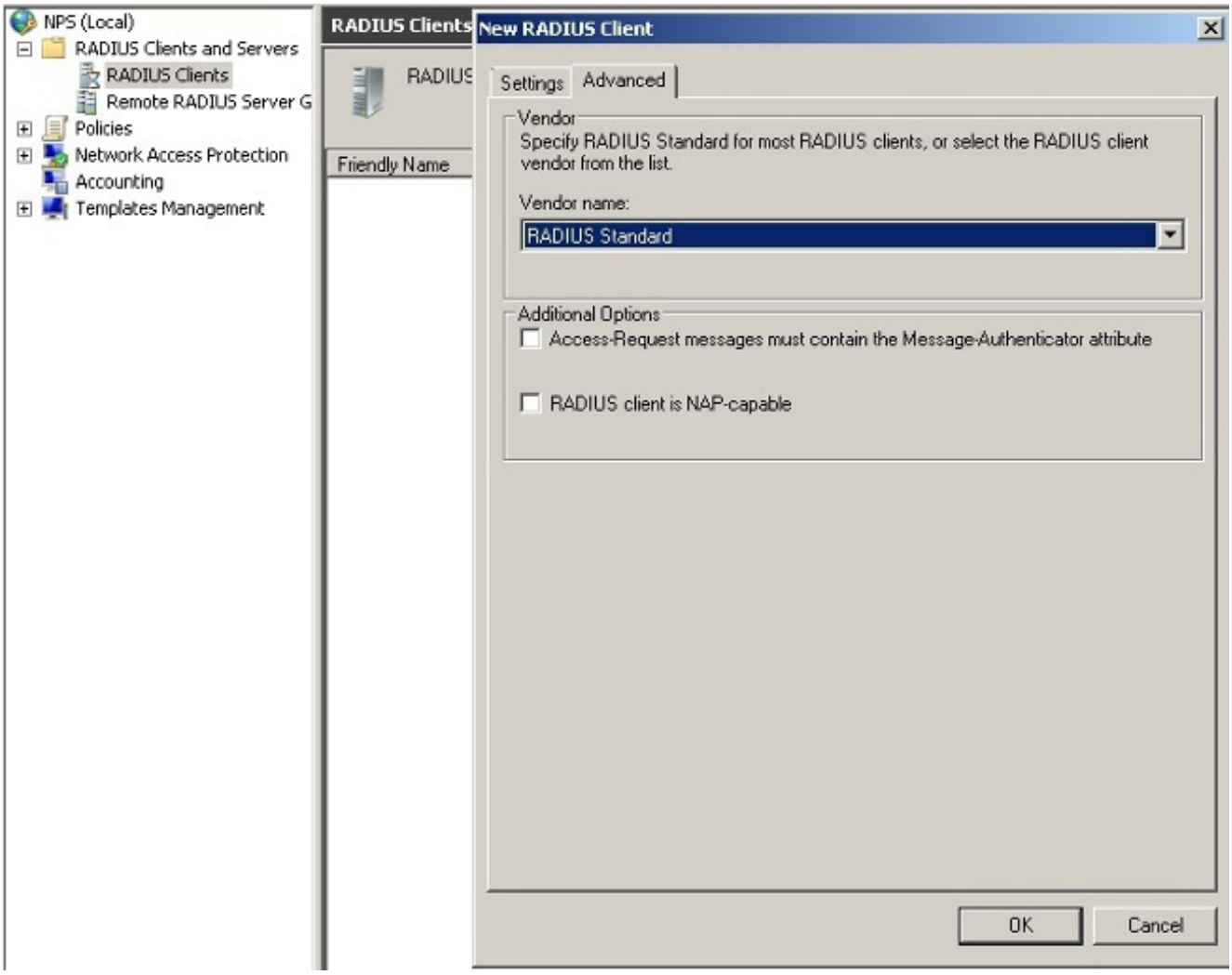
1. 将ASA添加为NPS服务器中的RADIUS客户端。 选择**Administrative Tools > Network Policy Server**。右键单击**RADIUS Clients**并选择**New**。



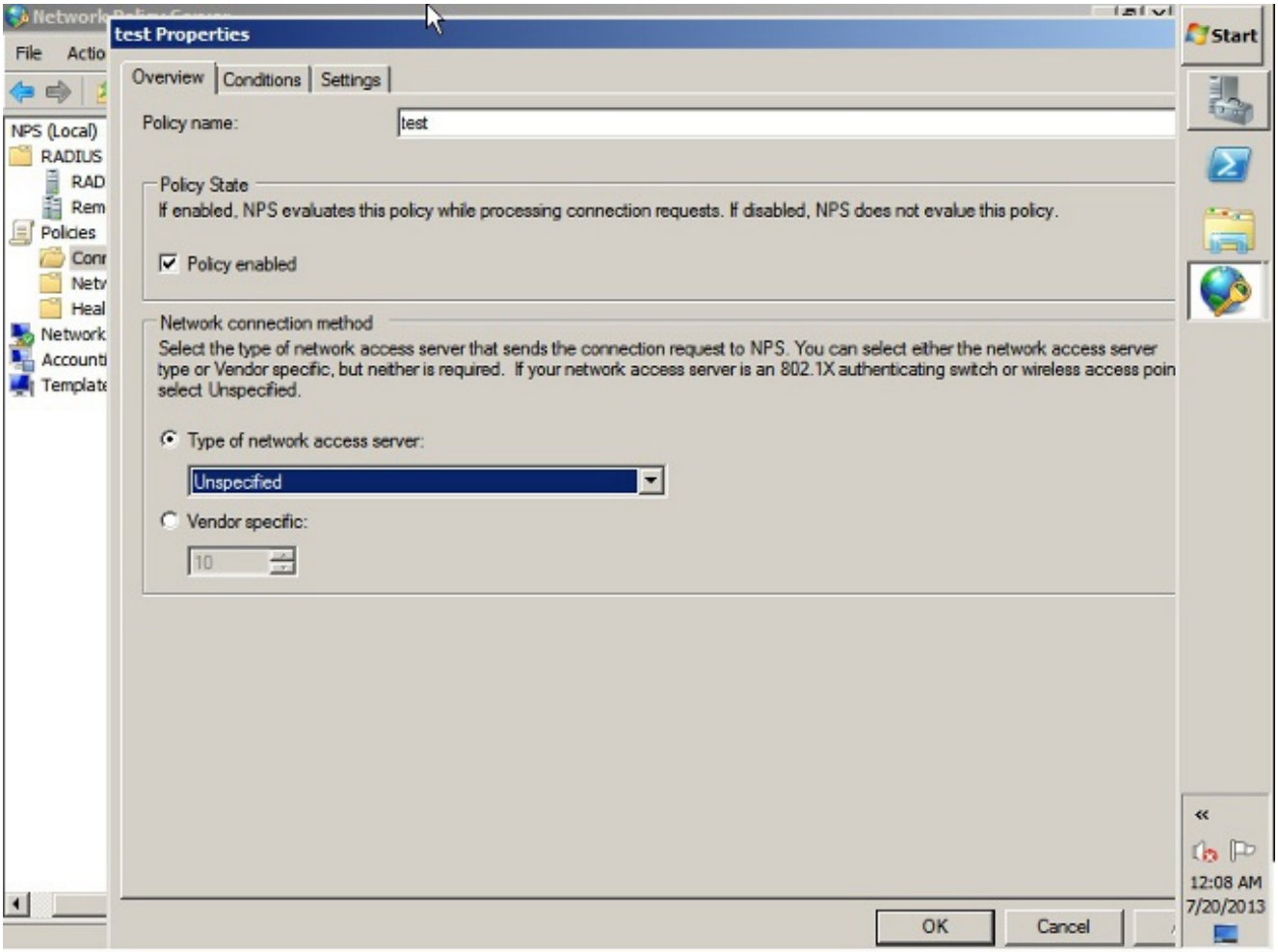
输入在ASA上配置的友好名称、地址（IP或DNS）和共享密钥。



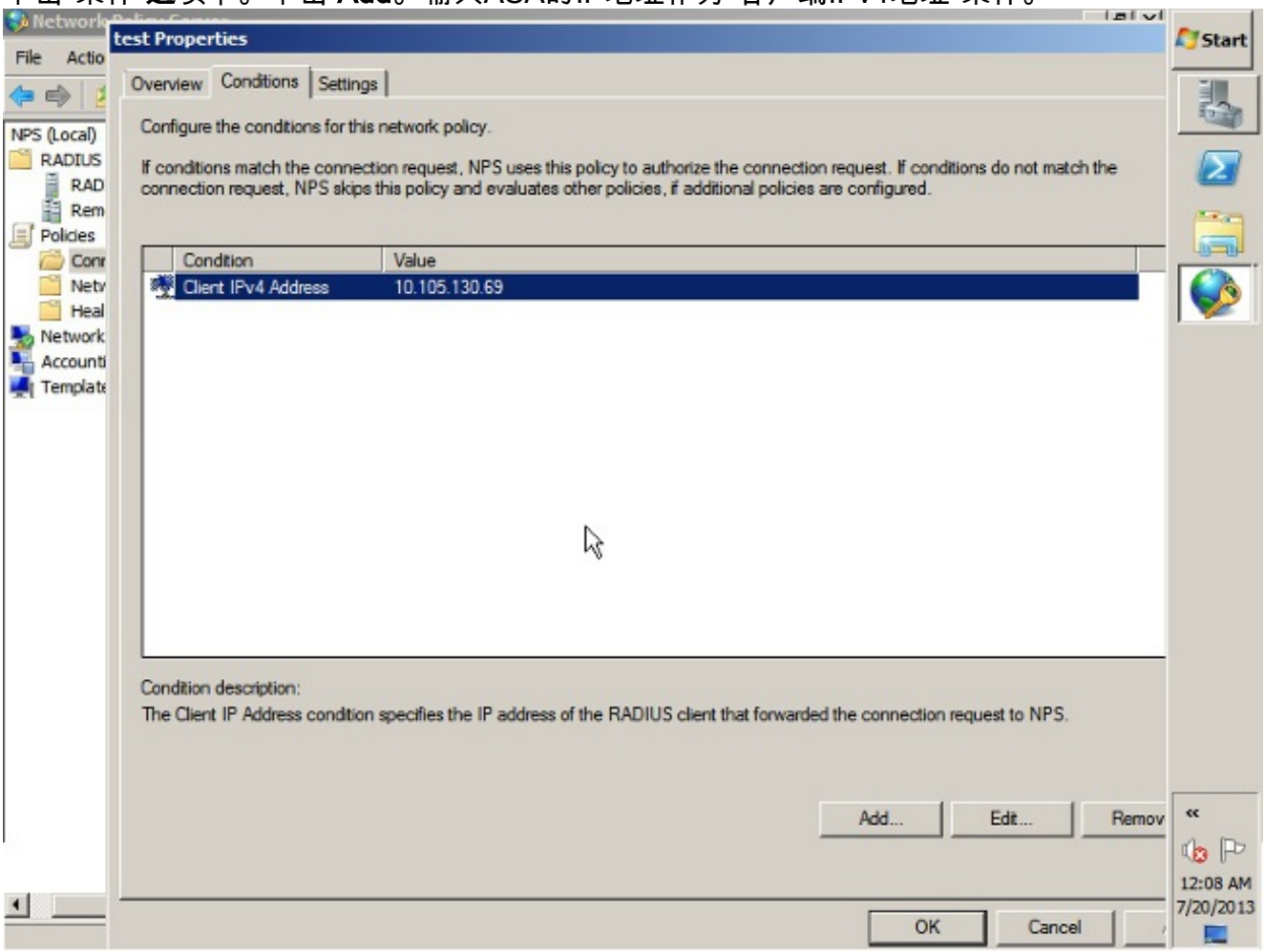
单击 **Advanced 选项卡。**从供应商名称下拉列表中，选择**RADIUS标准。**Click **OK**.



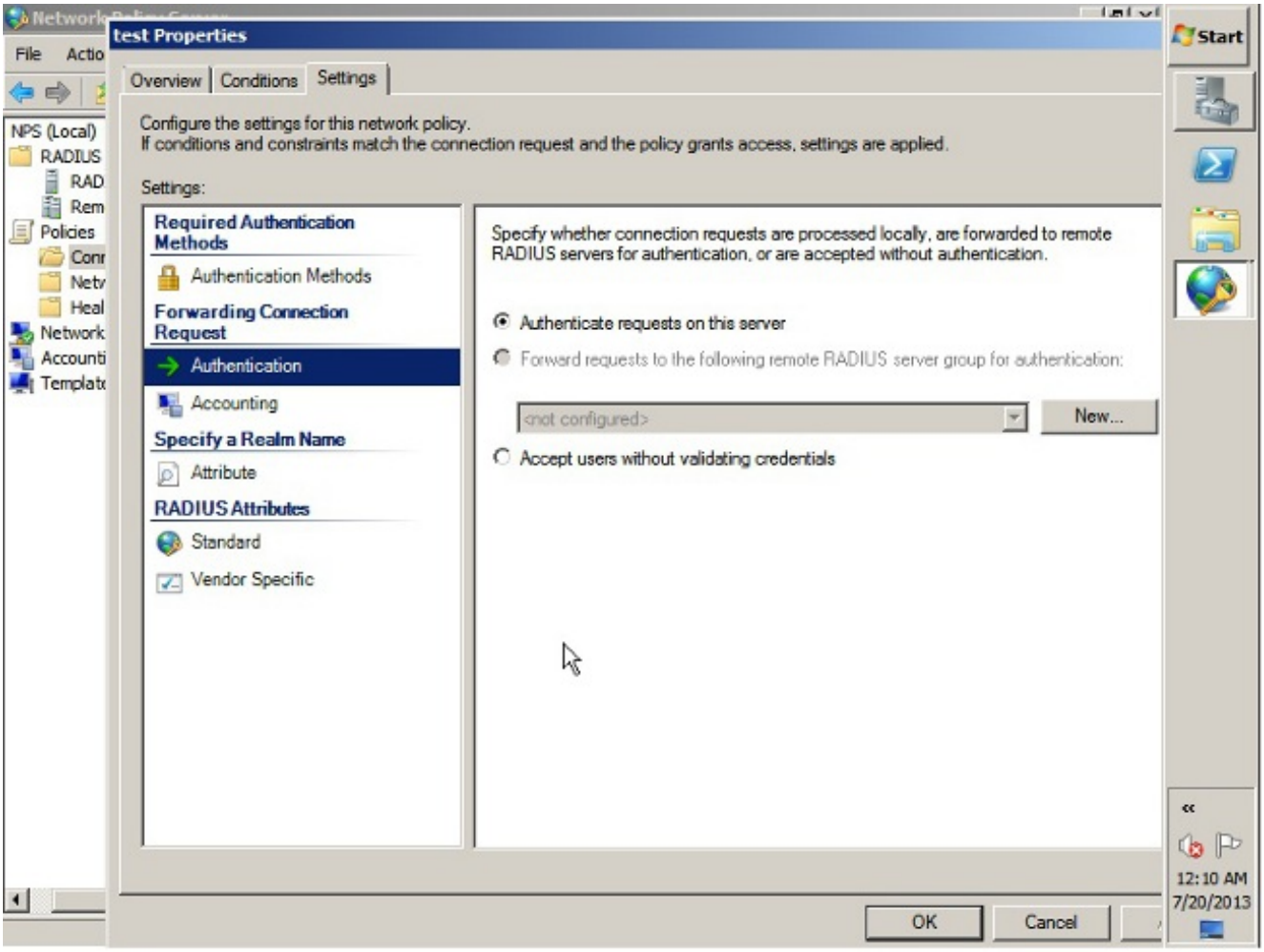
2. 为VPN用户创建新的连接请求策略。连接请求策略的用途是指定是本地处理来自RADIUS客户端的请求还是转发到远程RADIUS服务器。 在NPS > Policies下，右键单击**Connection Request Policies**并创建新策略。从Type of network access server下拉列表中，选择**Unspecified**。



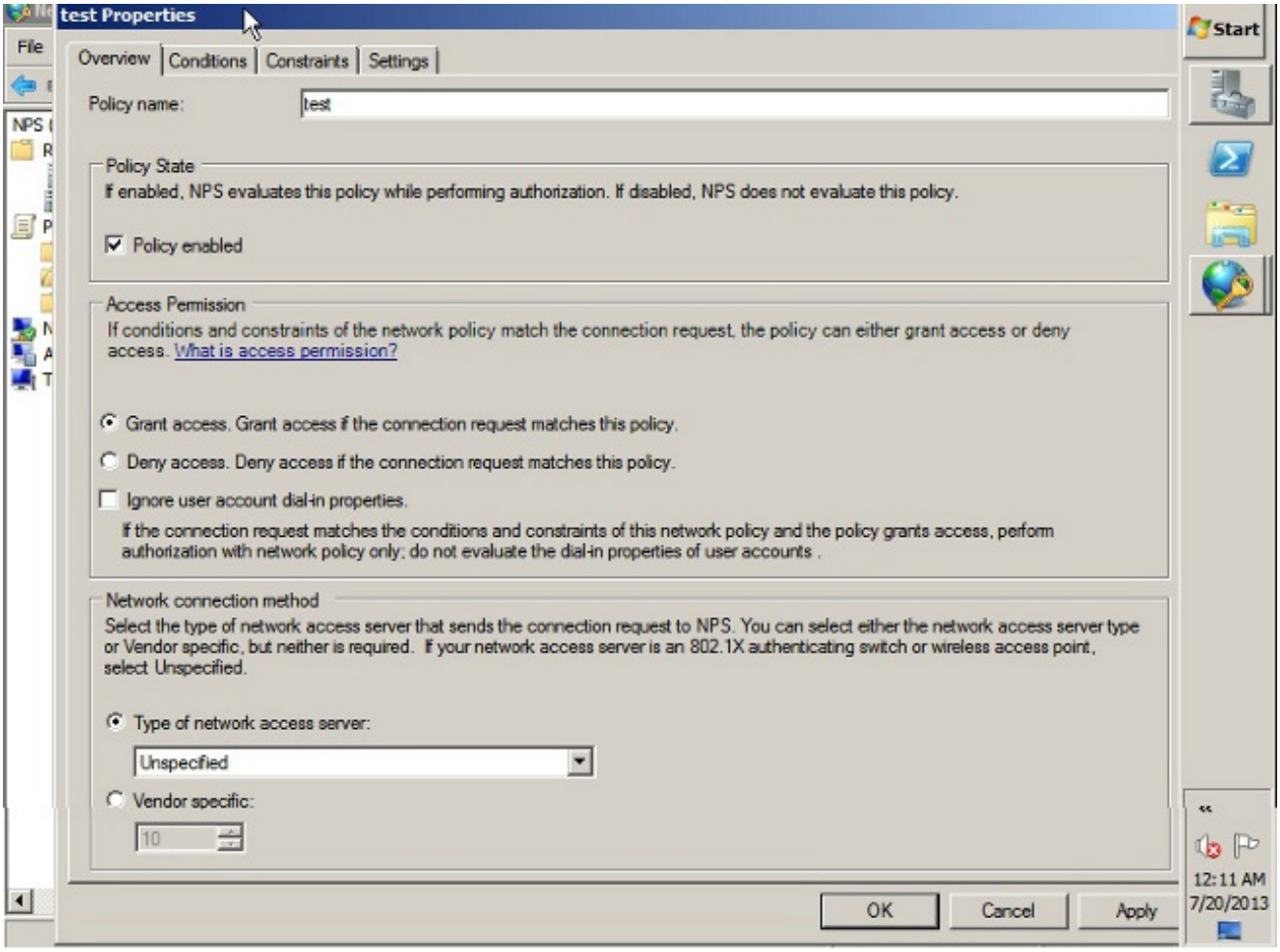
单击“条件”选项卡。单击 Add。输入ASA的IP地址作为“客户端IPv4地址”条件。



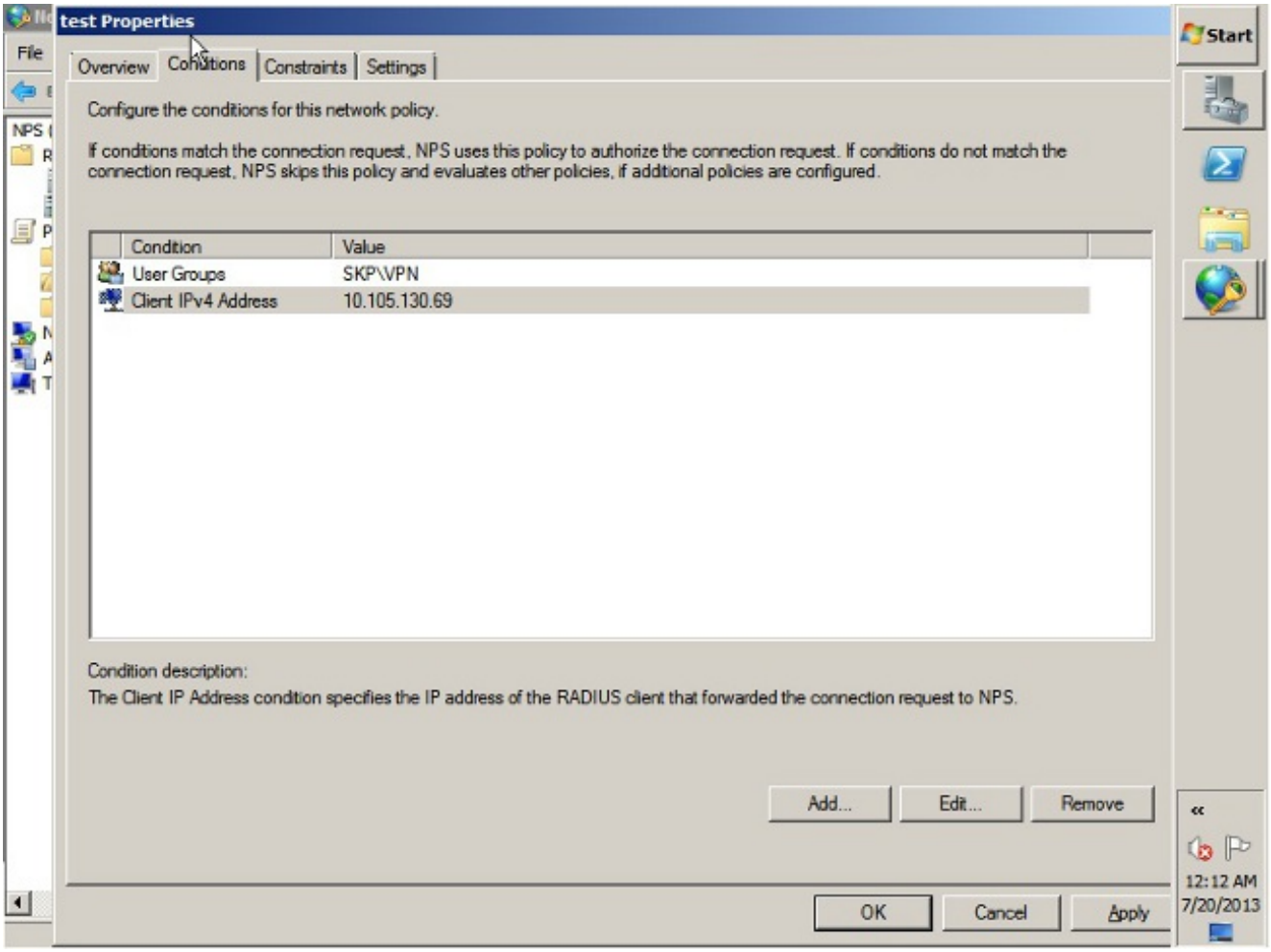
单击“设置”选项卡。在Forwarding Connection Request（转发连接请求）下，选择**Authentication**。确保选择Authenticate requests on this server单选按钮。Click **OK**.



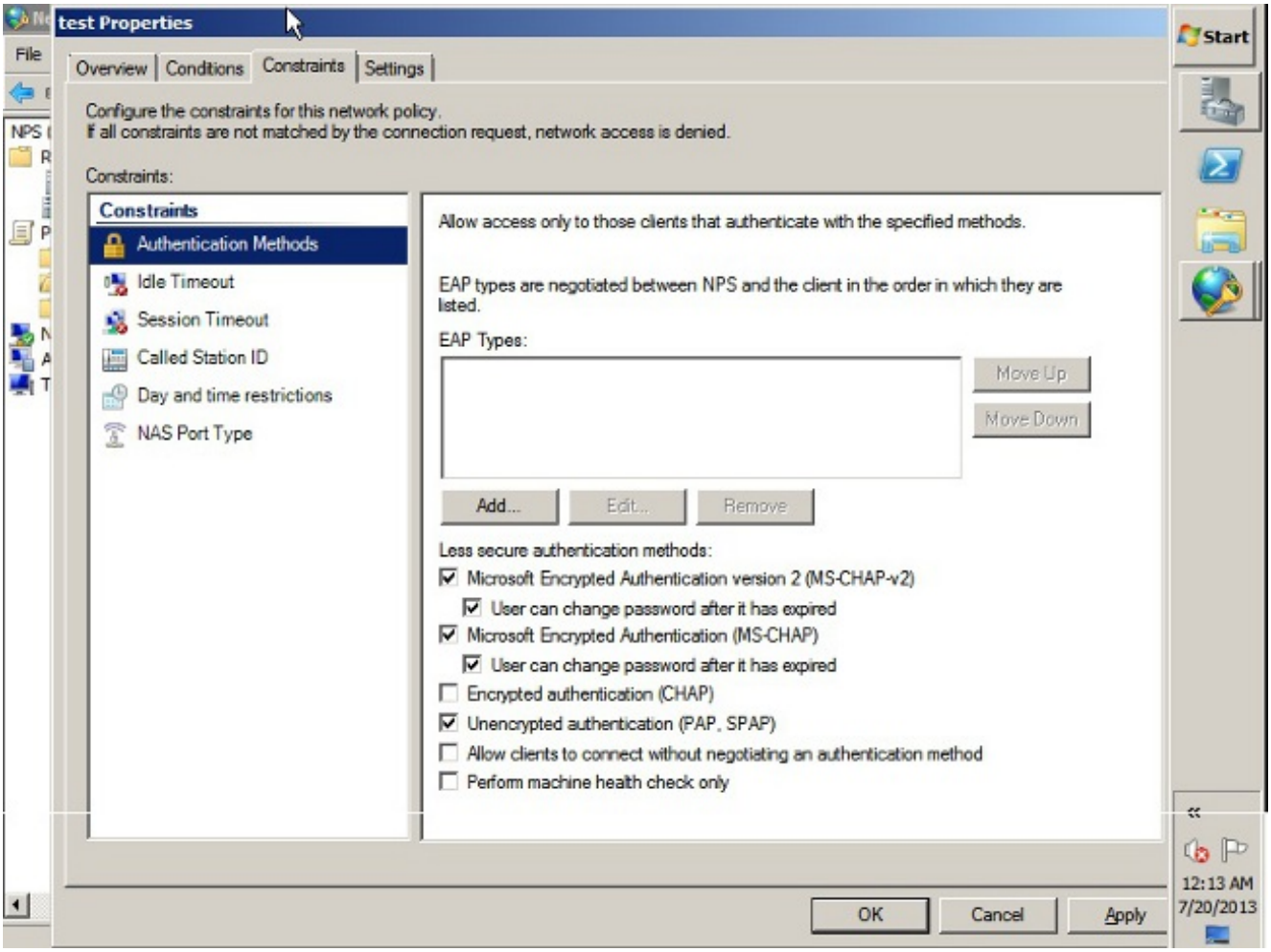
3. 添加网络策略，在该策略中可以指定允许哪些用户进行身份验证。例如，可以添加Active Directory用户组作为条件。只有属于指定Windows组的用户才会在此策略下进行身份验证。在NPS下，选择**Policies**。右键单击**Network Policy**并创建新策略。确保已选择Grant access单选按钮。从Type of network access server下拉列表中，选择**Unspecified**。



单击“条件”选项卡。单击 **Add**。输入ASA的IP地址作为客户端IPv4地址条件。输入包含VPN用户的Active Directory用户组。



单击“约束”(Constraints)选项卡。选择Authentication Methods。确保选中Unencrypted authentication(PAP，SPAP)复选框。Click OK.

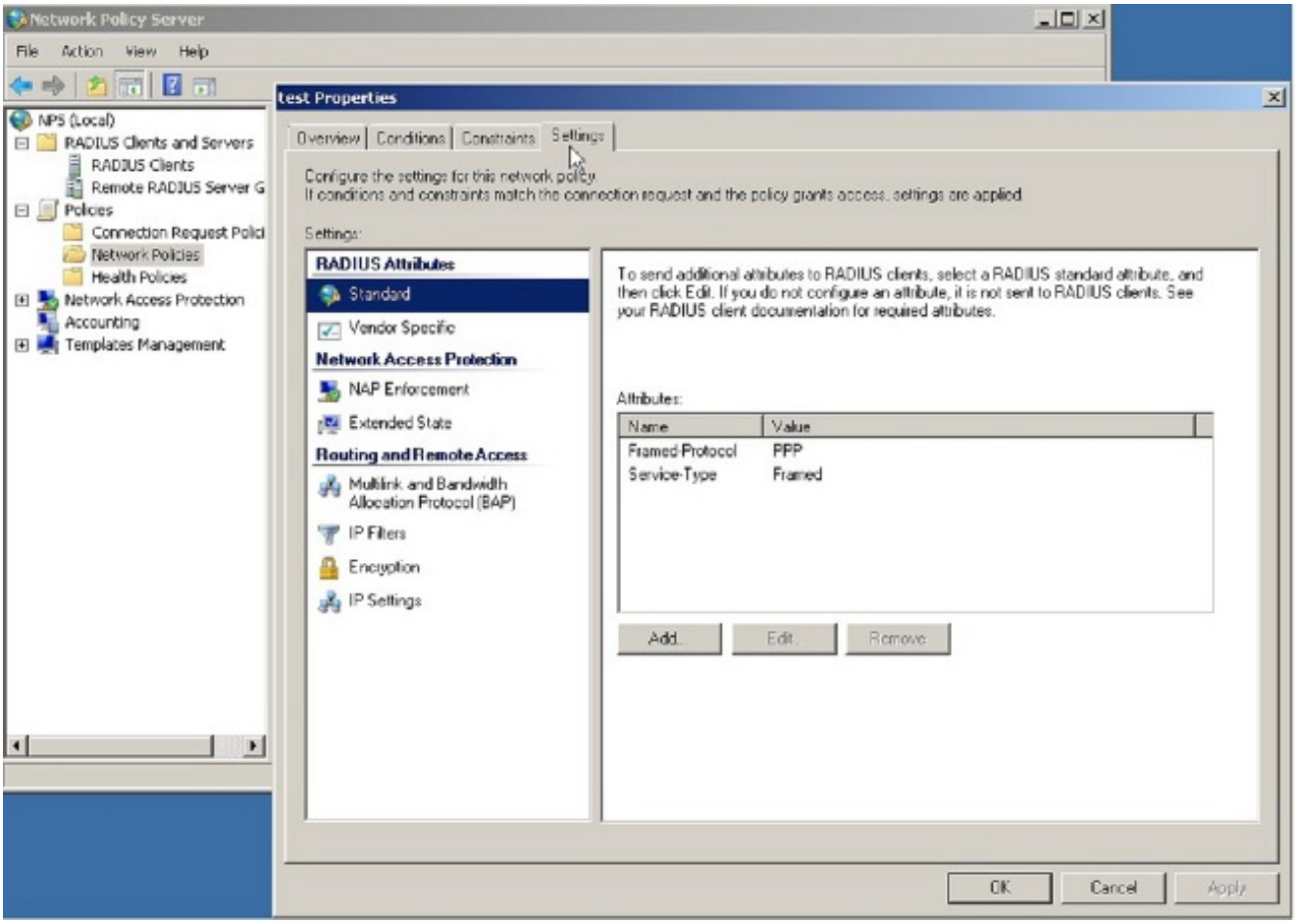


从NPS RADIUS服务器传递组策略属性（属性25）

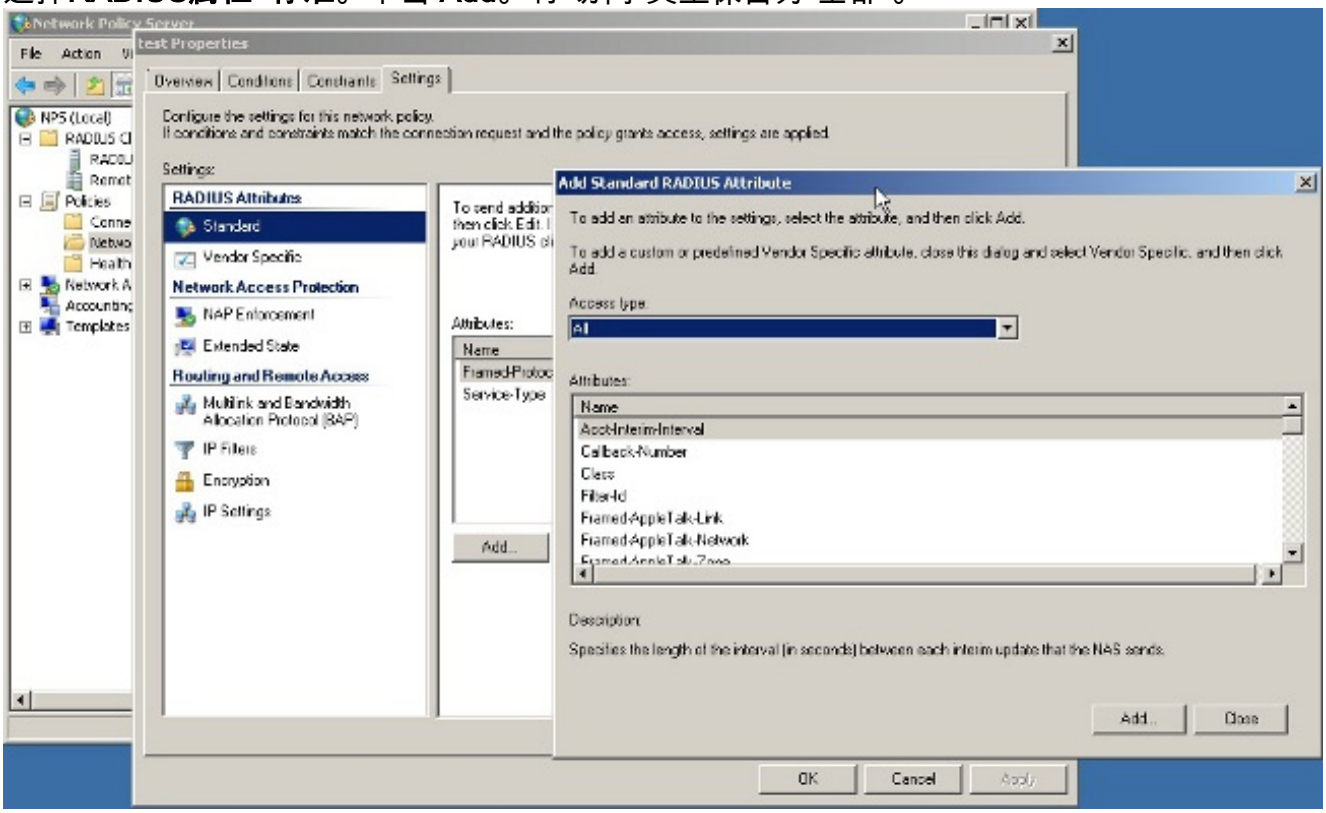
如果需要使用NPS RADIUS服务器将组策略动态分配给用户，则可以使用组策略RADIUS属性（属性25）。

完成以下步骤，以便向用户发送RADIUS属性25，以便动态分配组策略。

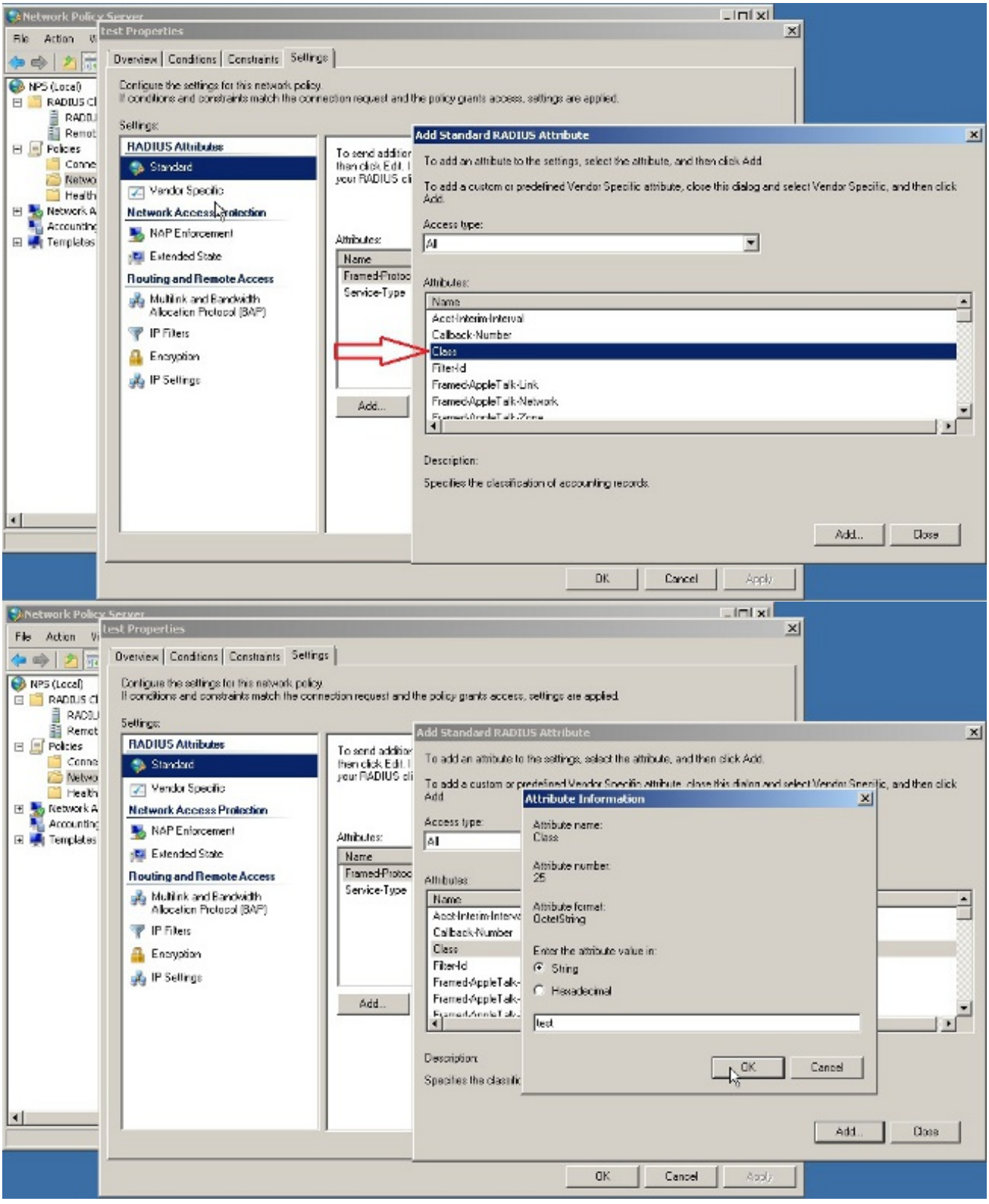
1. 添加网络策略后，右键单击所需的网络策略，然后单击“设置”**选**项卡。



2. 选择**RADIUS属性>标准**。单击 **Add**。将“访问”类型保留为“全部”。



3. 在“属性”框中，选择“**类**”并单击“**添加**”。输入属性值，即作为字符串的组策略名称。请记住，必须在ASA中配置具有此名称的组策略。这样，ASA在RADIUS响应中收到此属性后将其分配给VPN会话。



验证

使用本部分可确认配置能否正常运行。

注意：使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

ASA调试

在ASA上启用debug radius all。

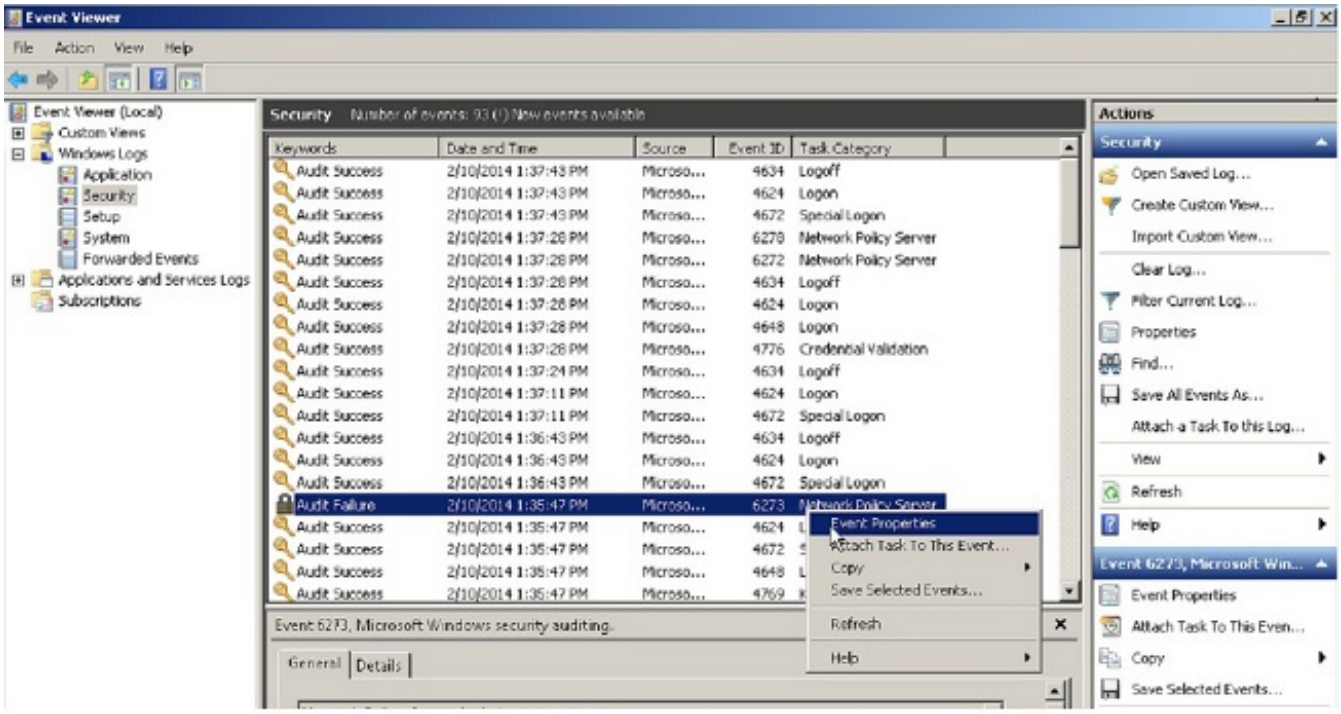
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

故障排除

本部分提供的信息可用于对配置进行故障排除。

- 确保ASA和NPS服务器之间的连接正常。应用数据包捕获，确保身份验证请求离开ASA接口（从可访问服务器的位置）。 确认路径中的设备不会阻止UDP端口1645（默认RADIUS身份验证端口），以确保其到达NPS服务器。有关ASA上数据包捕获的详细信息，请参阅 ASA/PIX/FWSM:使用 CLI 和 ASDM 进行数据包捕获的配置示例.
- 如果身份验证仍然失败，请查看Windows NPS上的事件查看器。在“事件查看器”>“Windows日志”下，选择“安**全”。**查找在身份验证请求期间与NPS关联的事件。



打开事件属性后，您应该能够看到失败的原因，如示例所示。在本示例中，未在网络策略下选择PAP作为身份验证类型。因此，身份验证请求失败。

```
 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.
```