Autenticação de usuário ASA VPN no Windows 2008 NPS Server (Ative Diretory) com exemplo de configuração RADIUS

Contents

Introduction

Este documento explica como configurar um Adaptive Security Appliance (ASA) para se comunicar com um Microsoft Windows 2008 Network Policy Server (NPS) com o protocolo RADIUS para que os usuários legados do Cisco VPN Client/AnyConnect/Clientless WebVPN sejam autenticados no Ative Diretory. O NPS é uma das funções de servidor oferecidas pelo Windows 2008 Server. É equivalente ao Windows 2003 Server, IAS (Internet Authentication Service), que é a implementação de um servidor RADIUS para fornecer autenticação de usuário de discagem remota. Da mesma forma, no Windows 2008 Server, o NPS é a implementação de um servidor RADIUS. Basicamente, o ASA é um cliente RADIUS para um servidor NPS RADIUS. O ASA envia solicitações de autenticação RADIUS em nome de usuários de VPN e o NPS os autentica no Ative Diretory.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

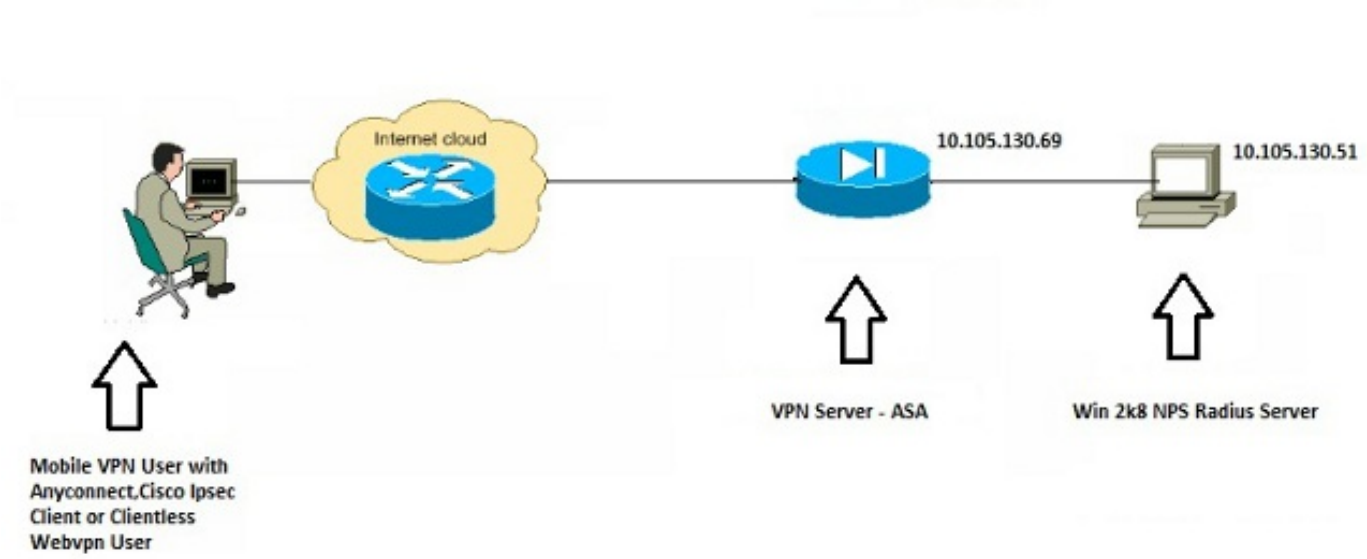
- ASA com versão 9.1(4)
- Windows 2008 R2 Server com serviços Ative Diretory e função NPS instalada

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.

Configurar

> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

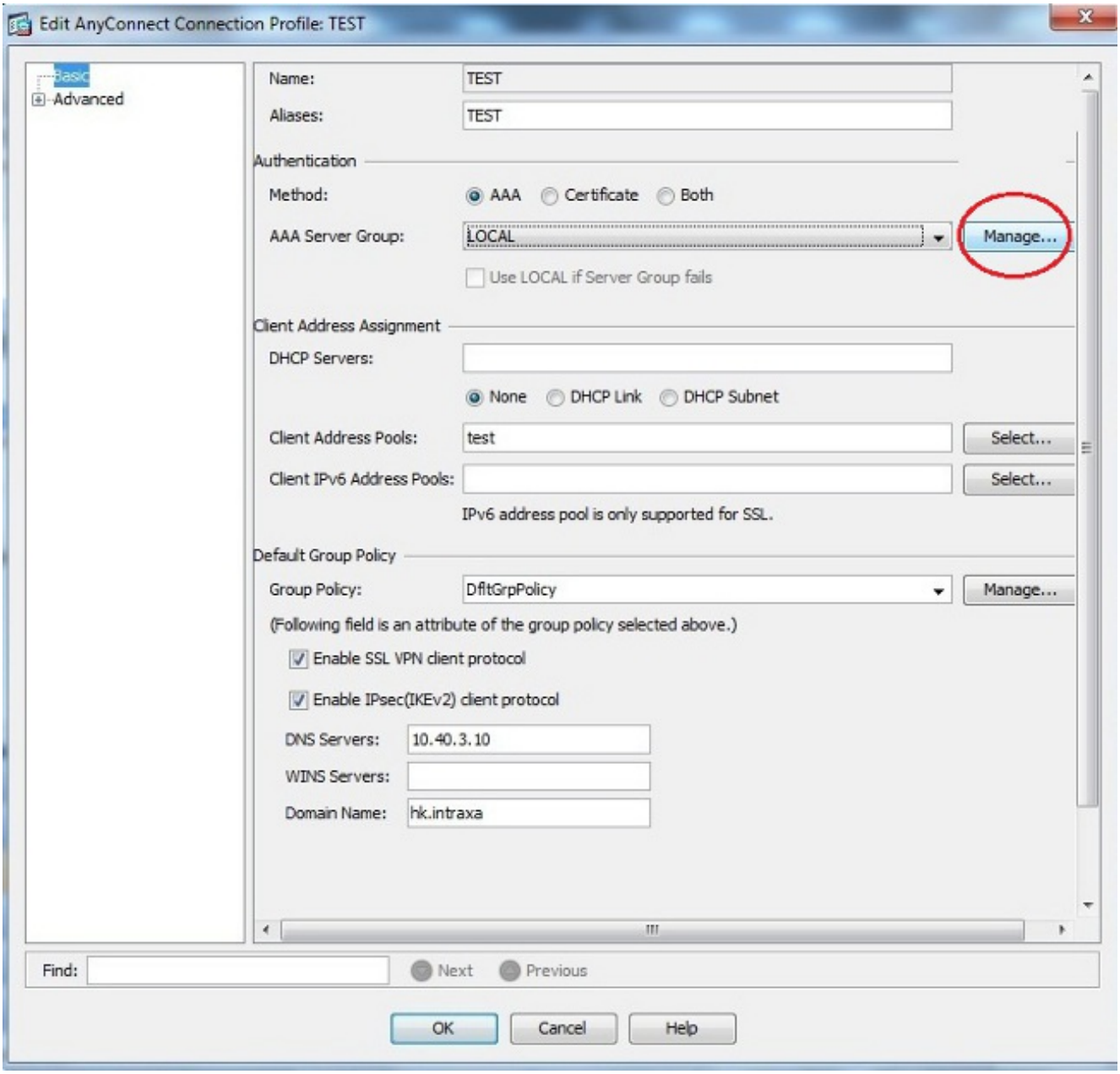
Diagrama de Rede



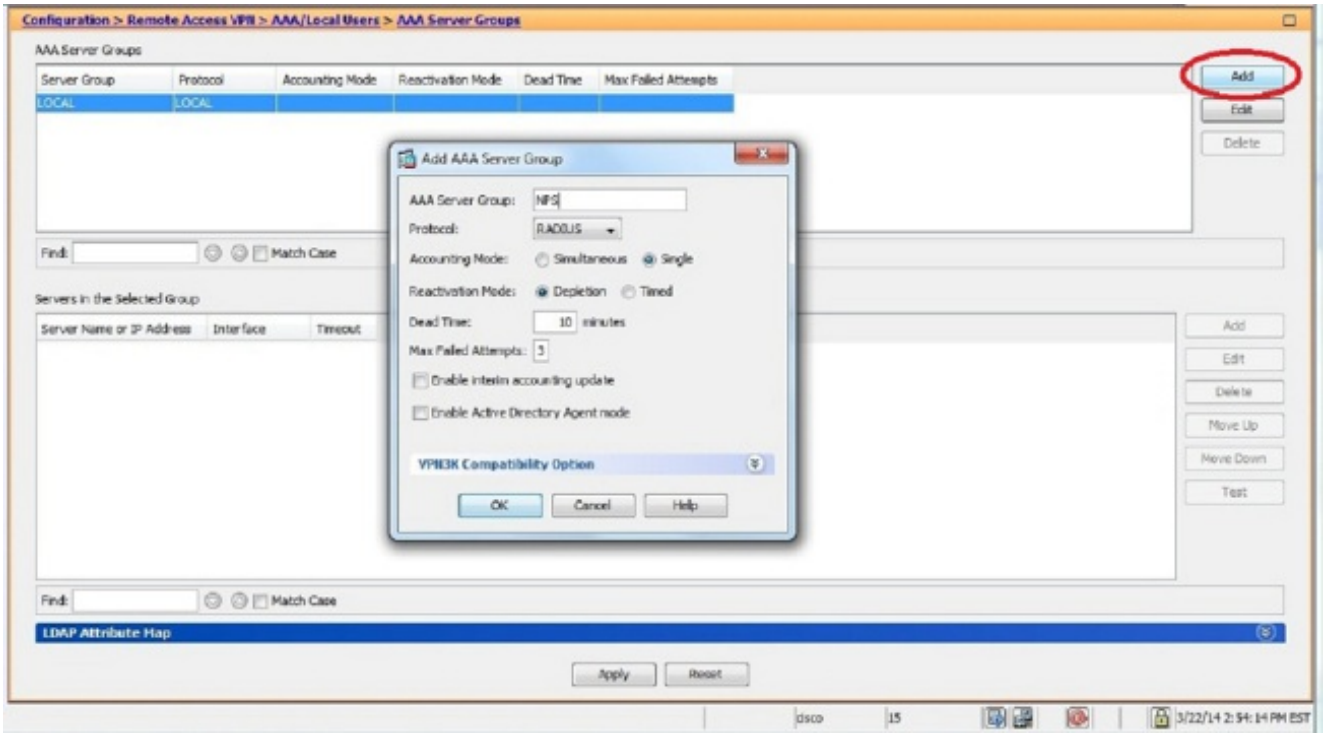
Configurações

Configuração do ASDM

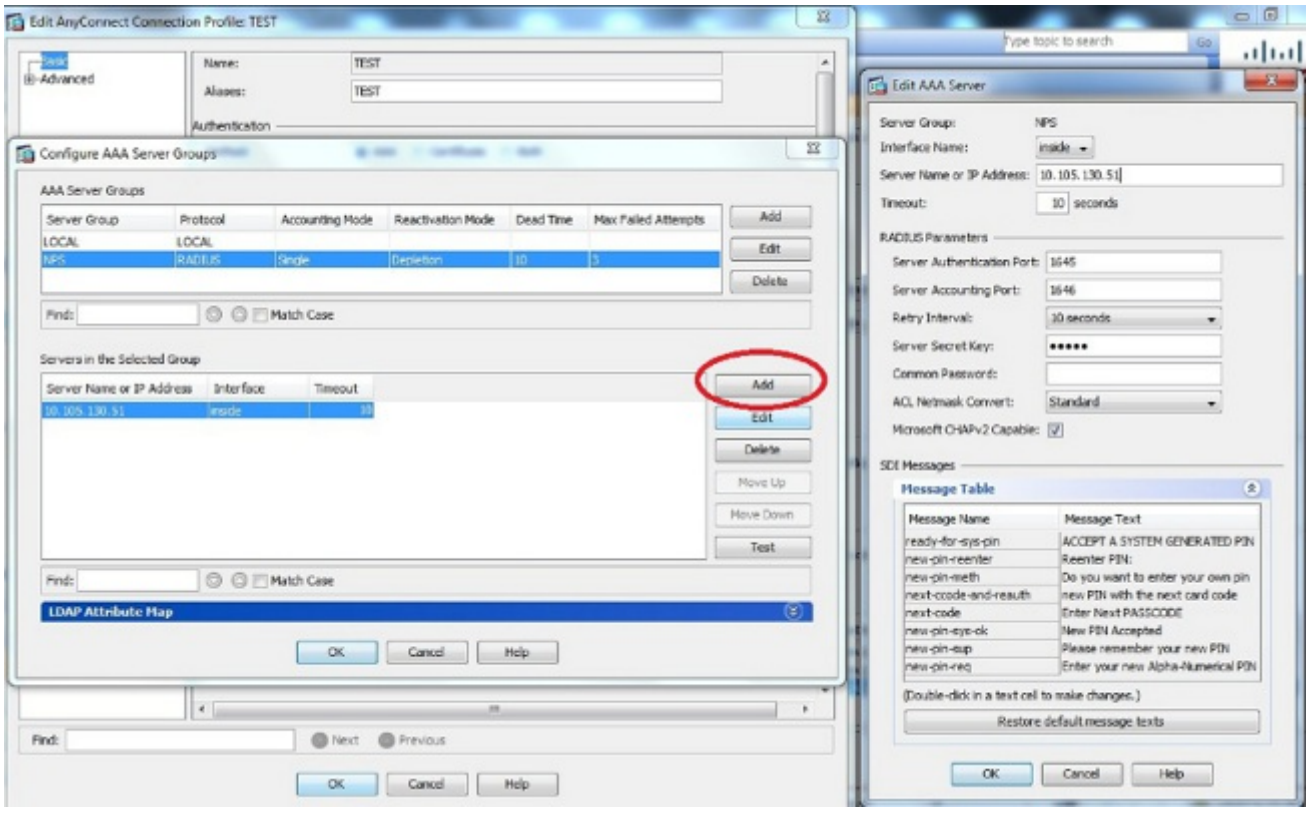
1. Escolha o grupo de túneis para o qual a autenticação NPS é necessária.
2. Clique em **Editar** e escolha **Básico**.
3. Na seção Autenticação, clique em **Gerenciar**.



4. Na seção Grupos de servidores AAA, clique em **Adicionar**.
5. No campo AAA Server Group (Grupo de servidores AAA), digite o nome do grupo de servidores (por exemplo, NPS).
6. Na lista suspensa Protocolo, escolha **RADIUS**.
7. Click
   OK.

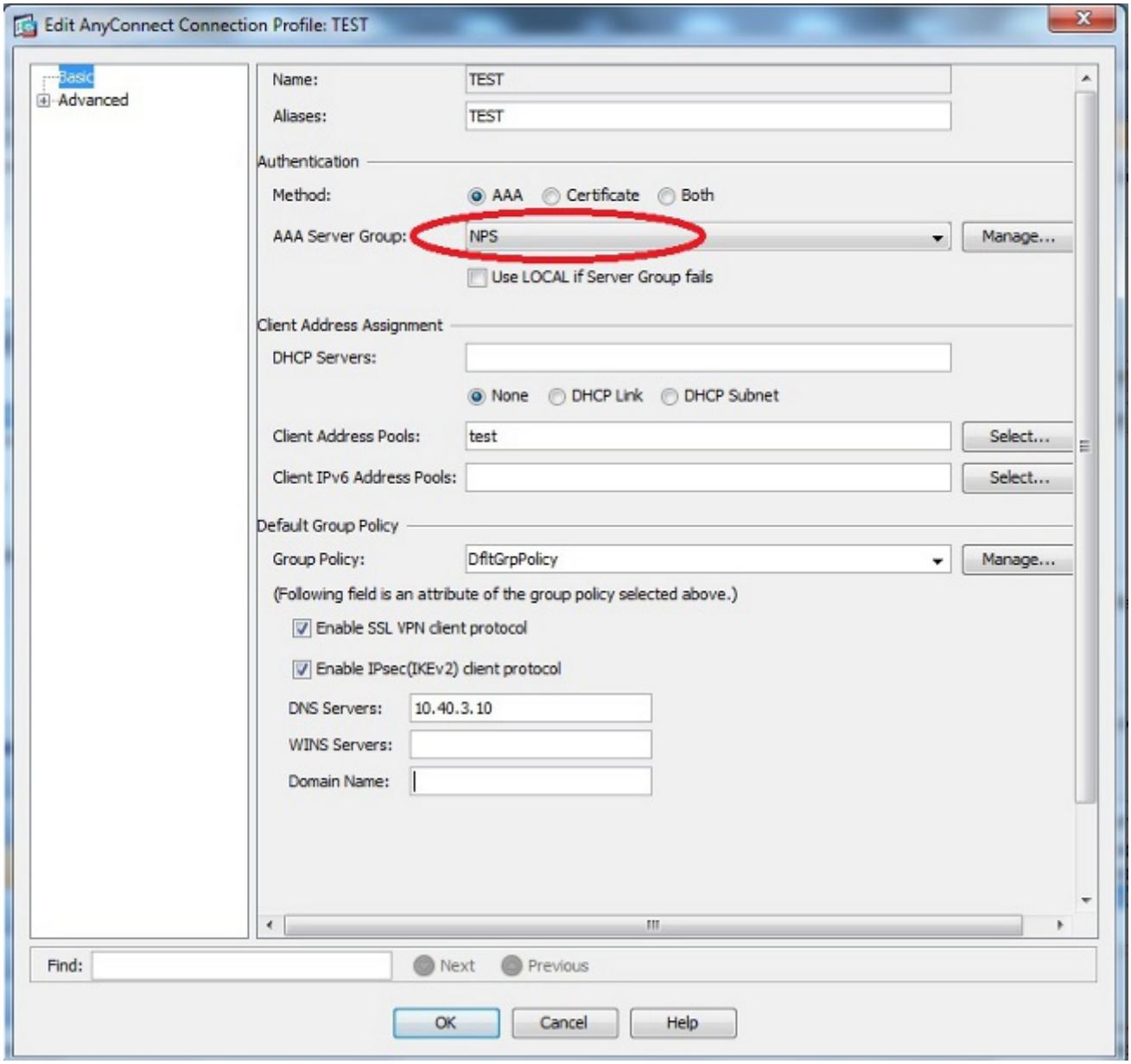


8. Na seção Servidores no Grupo selecionado, escolha o Grupo de servidores AAA adicionado e clique em **Adicionar**.
9. No campo Nome do servidor ou Endereço IP, insira o endereço IP do servidor.
10. No campo Chave secreta do servidor, digite a chave secreta.
11. Deixe os campos Server Authentication Port e Server Accounting Port no valor padrão, a menos que o servidor ouça em uma porta diferente.
12. Click **OK**.
13. Click **OK**.



14. Na lista suspensa Grupo de servidores AAA, escolha o grupo (NPS neste exemplo) adicionado nas etapas anteriores.
15. Click

OK.



Configuração de CLI

```
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
```

Por padrão, o ASA usa o tipo de autenticação PAP (Password Authentication Protocol) não criptografado. Isso não significa que o ASA envie a senha em texto simples quando envia o pacote RADIUS REQUEST. Em vez disso, a senha em texto simples é criptografada com o segredo compartilhado RADIUS.

Se o gerenciamento de senha estiver habilitado no grupo de túneis, o ASA usará o tipo de autenticação MSCHAP-v2 para criptografar a senha de texto simples. Nesse caso, verifique se a caixa de seleção **Microsoft CHAPv2 Capable** está marcada na janela Edit AAA Server configurada na seção de configuração do ASDM.

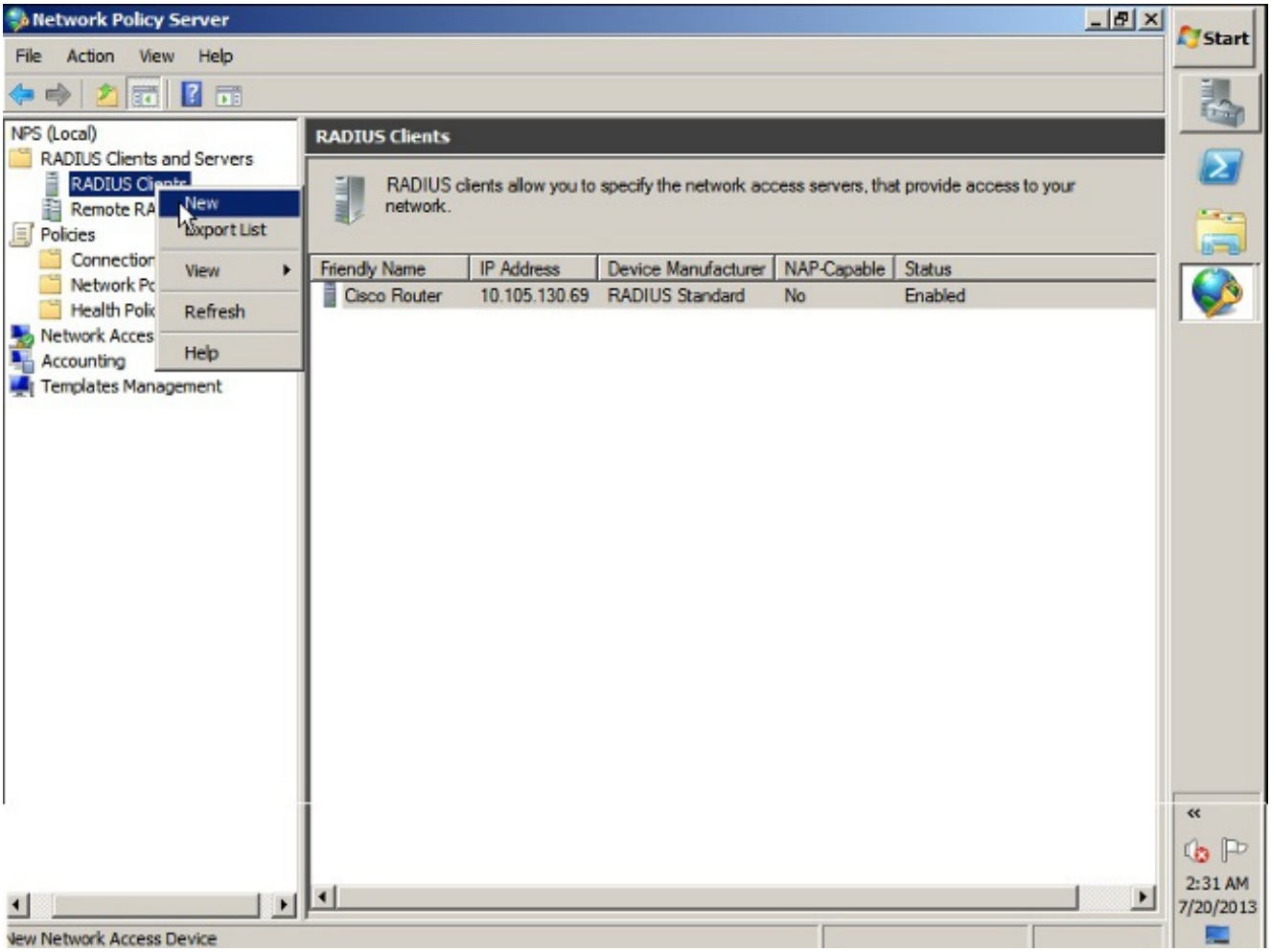
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **Note**: O comando **test aaa-server authentication** sempre usa PAP. Somente quando um usuário inicia uma conexão com um grupo de túneis com o gerenciamento de senha habilitado o ASA usa o MSCHAP-v2. Além disso, a opção 'password-management [password-expire-in-days]' só é suportada com o Lightweight Diretory Access Protocol (LDAP). RADIUS não fornece este recurso. Você verá a opção password expire quando a senha já tiver expirado no Ative Diretory.

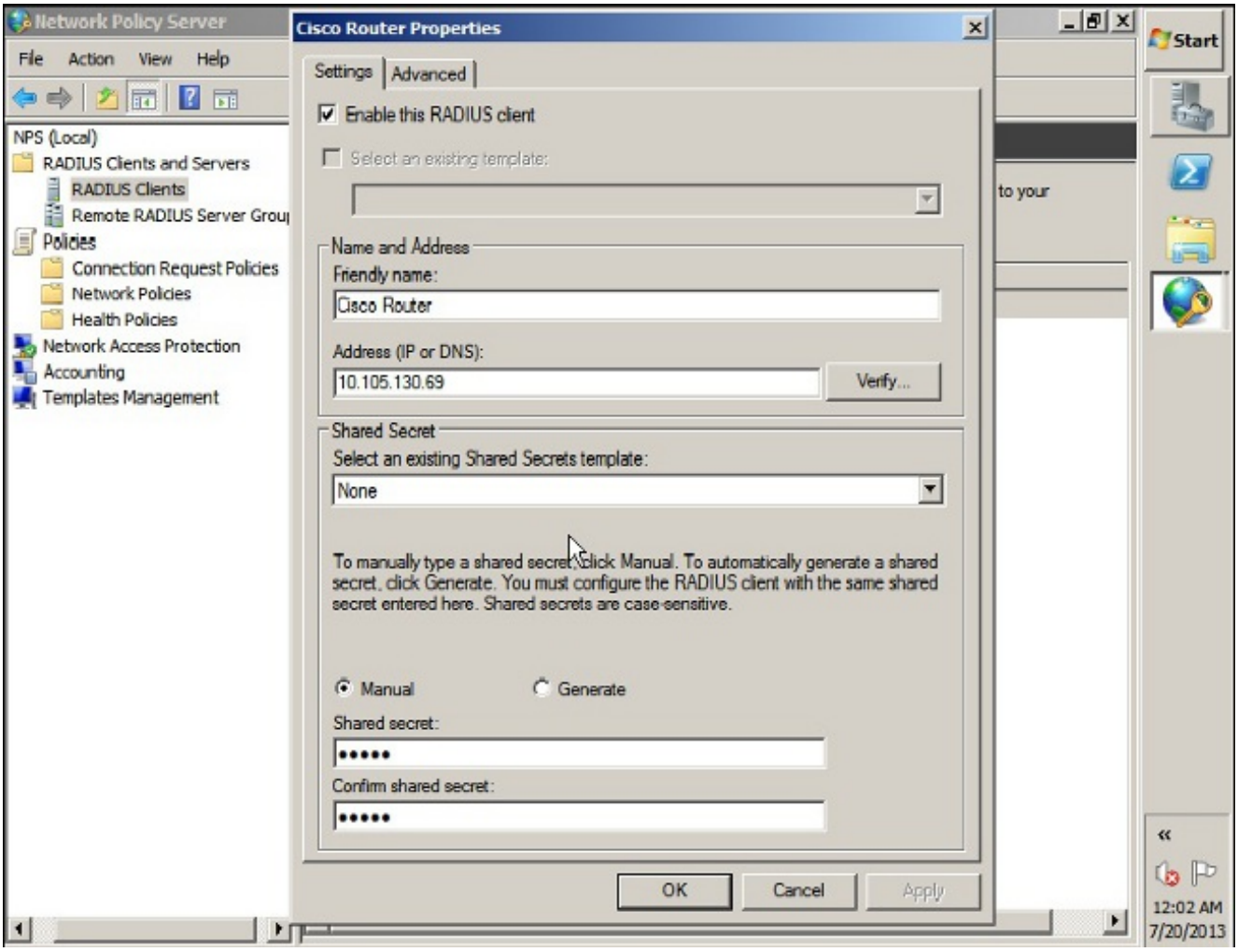
Windows 2008 Server com configuração de NPS

A função de servidor NPS deve ser instalada e executada no servidor Windows 2008. Caso contrário, escolha **Start > Administrative Tools > Server Roles > Add Role Services**. Escolha o Network Policy Server e instale o software. Depois que a função de servidor NPS for instalada, faça o seguinte para configurar o NPS para aceitar e processar solicitações de autenticação RADIUS do ASA:

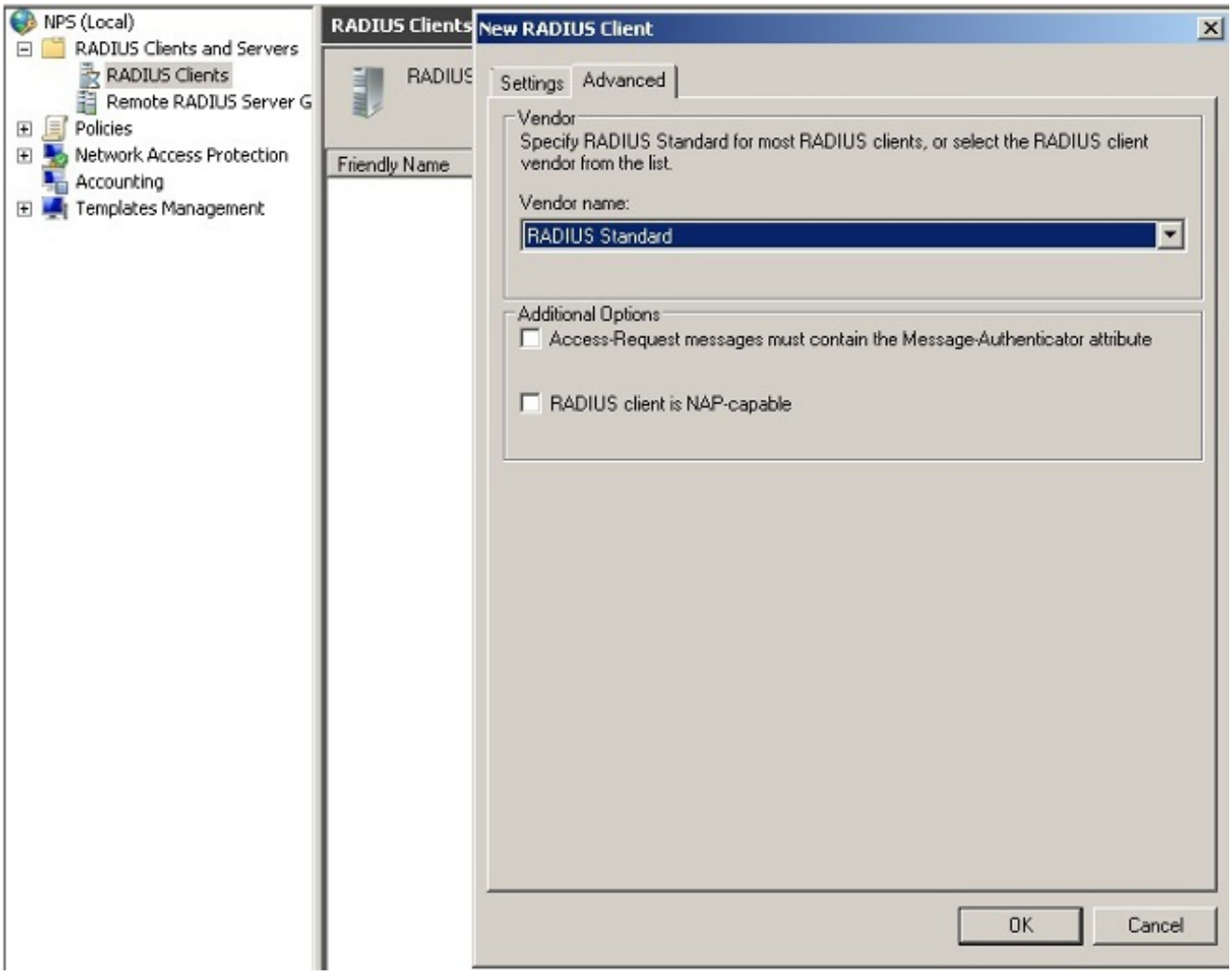
1. Adicione o ASA como um cliente RADIUS no servidor NPS. Escolha **Ferramentas Administrativas > Servidor de Políticas de Rede.**Clique com o botão direito do mouse em **RADIUS Clients** e escolha
   New.



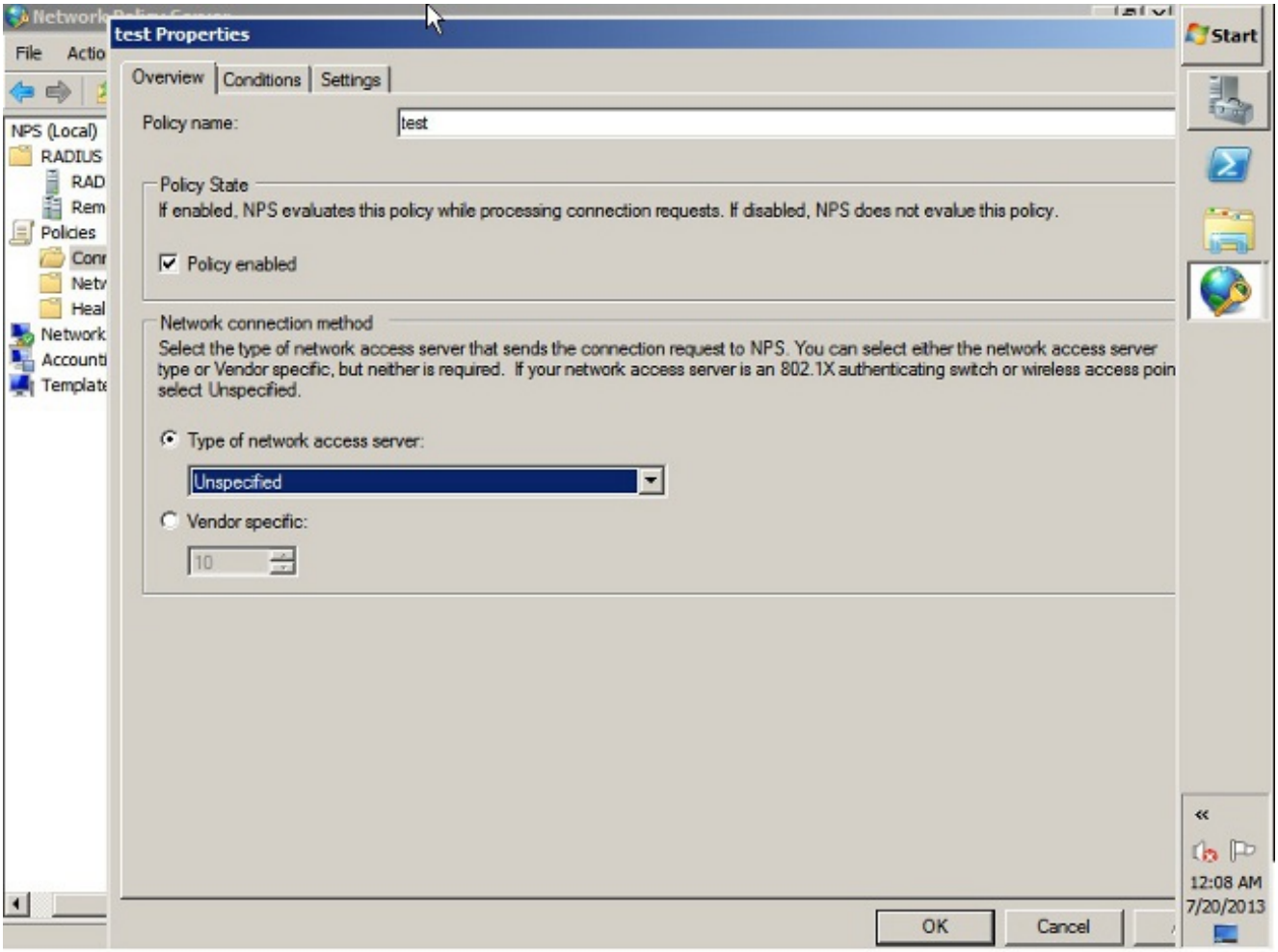
Insira um nome amigável, um endereço (IP ou DNS) e um segredo compartilhado configurados no
ASA.



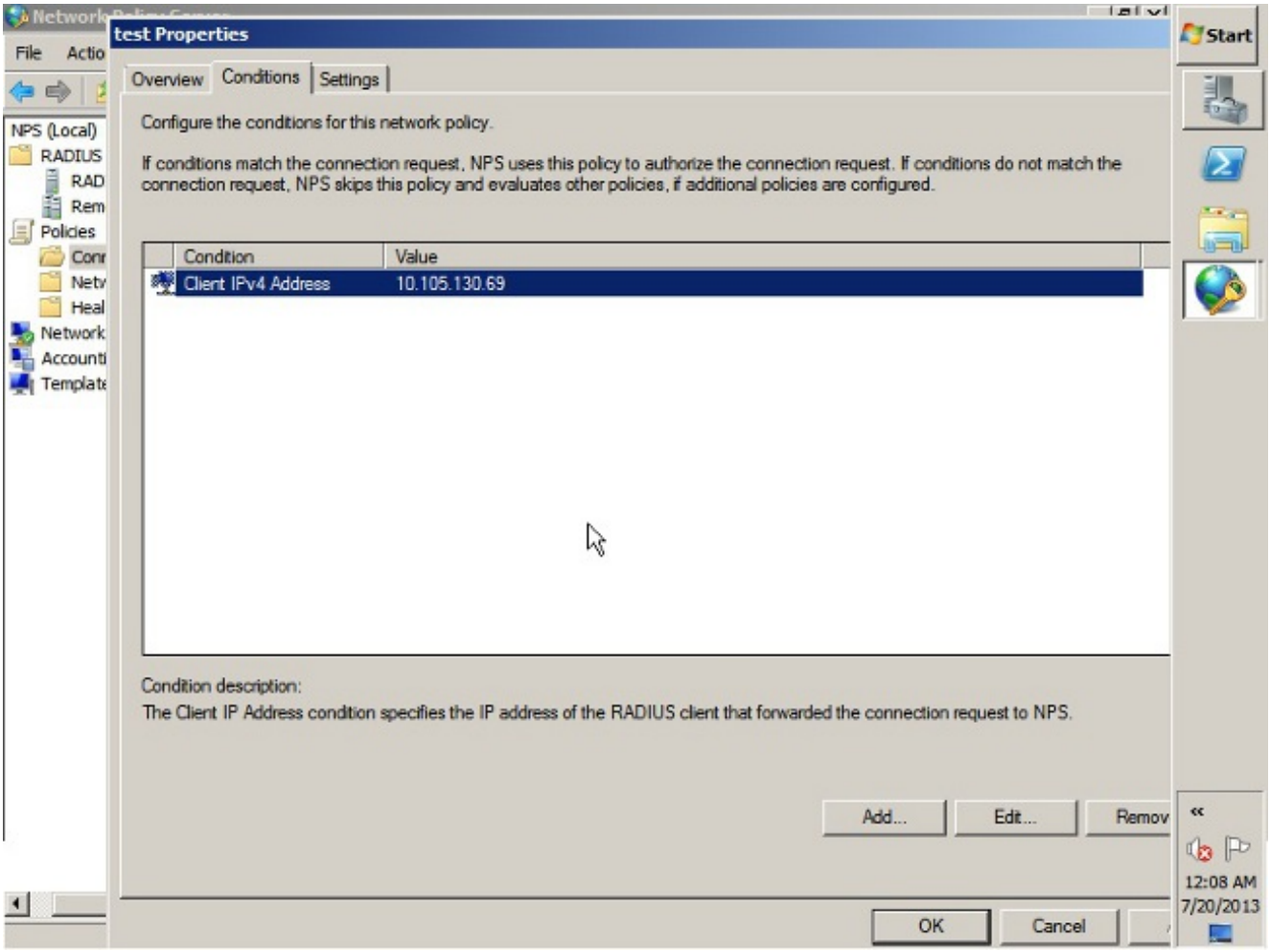
Clique na guia Advanced.Na lista suspensa Nome do fornecedor, escolha **RADIUS Standard**.Click
OK.



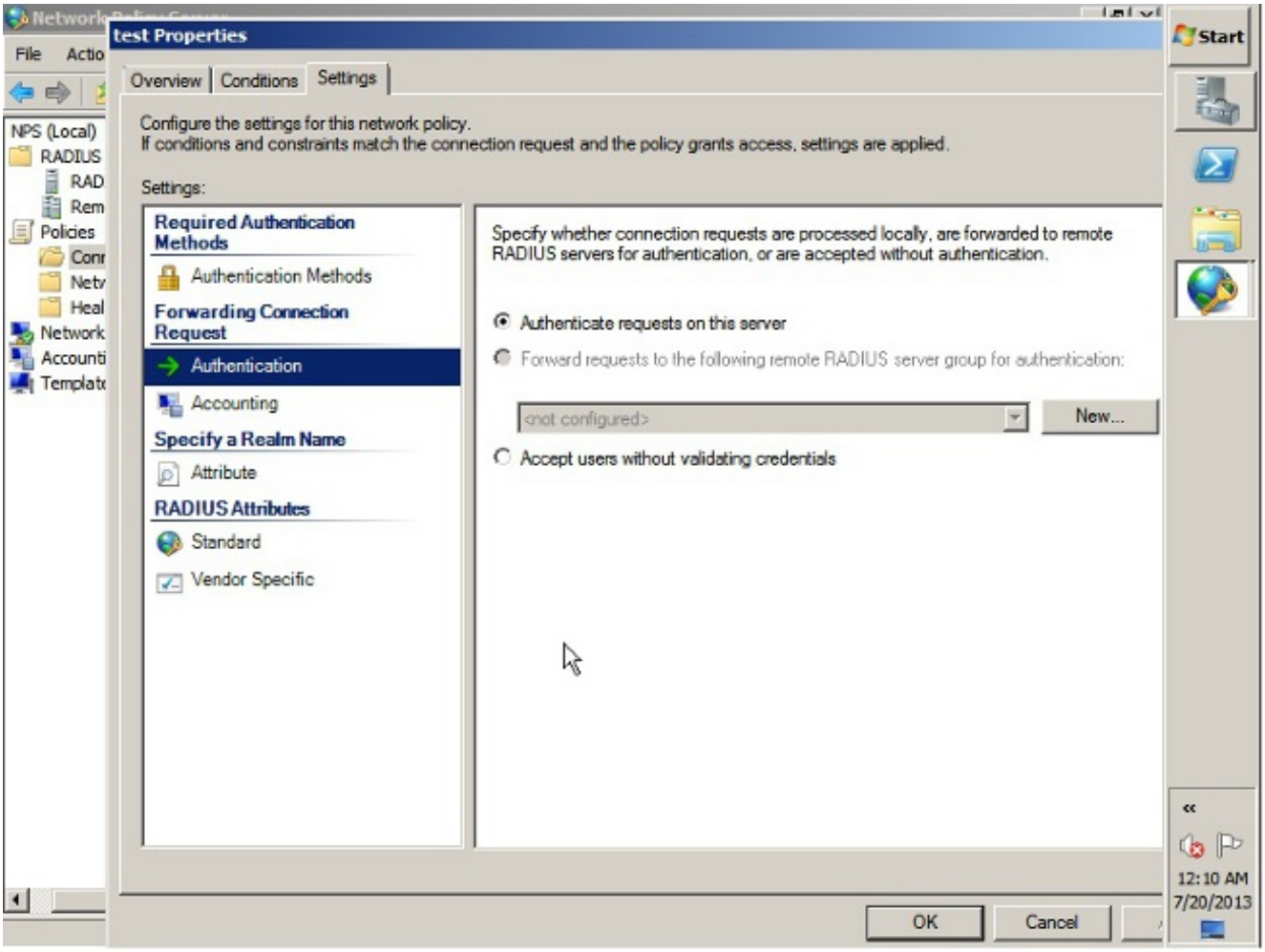
2. Crie uma nova Política de Solicitação de Conexão para usuários de VPN. A finalidade da Política de Solicitação de Conexão é especificar se as solicitações de clientes RADIUS devem ser processadas localmente ou encaminhadas para servidores RADIUS remotos. Em NPS > Policies, clique com o botão direito do mouse em **Connection Request Policies** e crie uma nova política.Na lista suspensa Tipo de servidor de acesso à rede, escolha **Não especificado**.



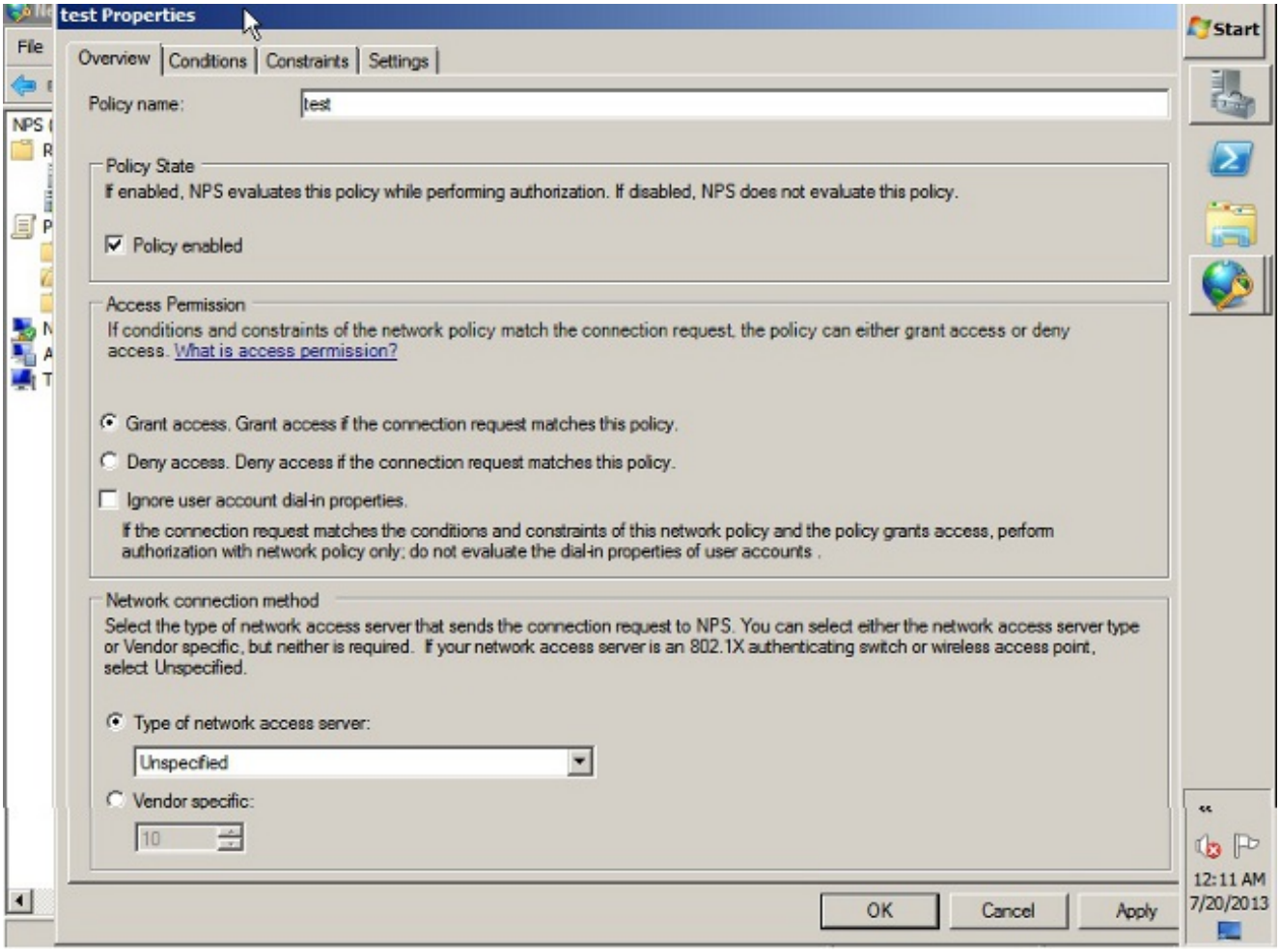
Clique na guia **Condições**.Clique em Add.Digite o endereço IP do ASA como uma condição 'Endereço IPv4 do
cliente'.



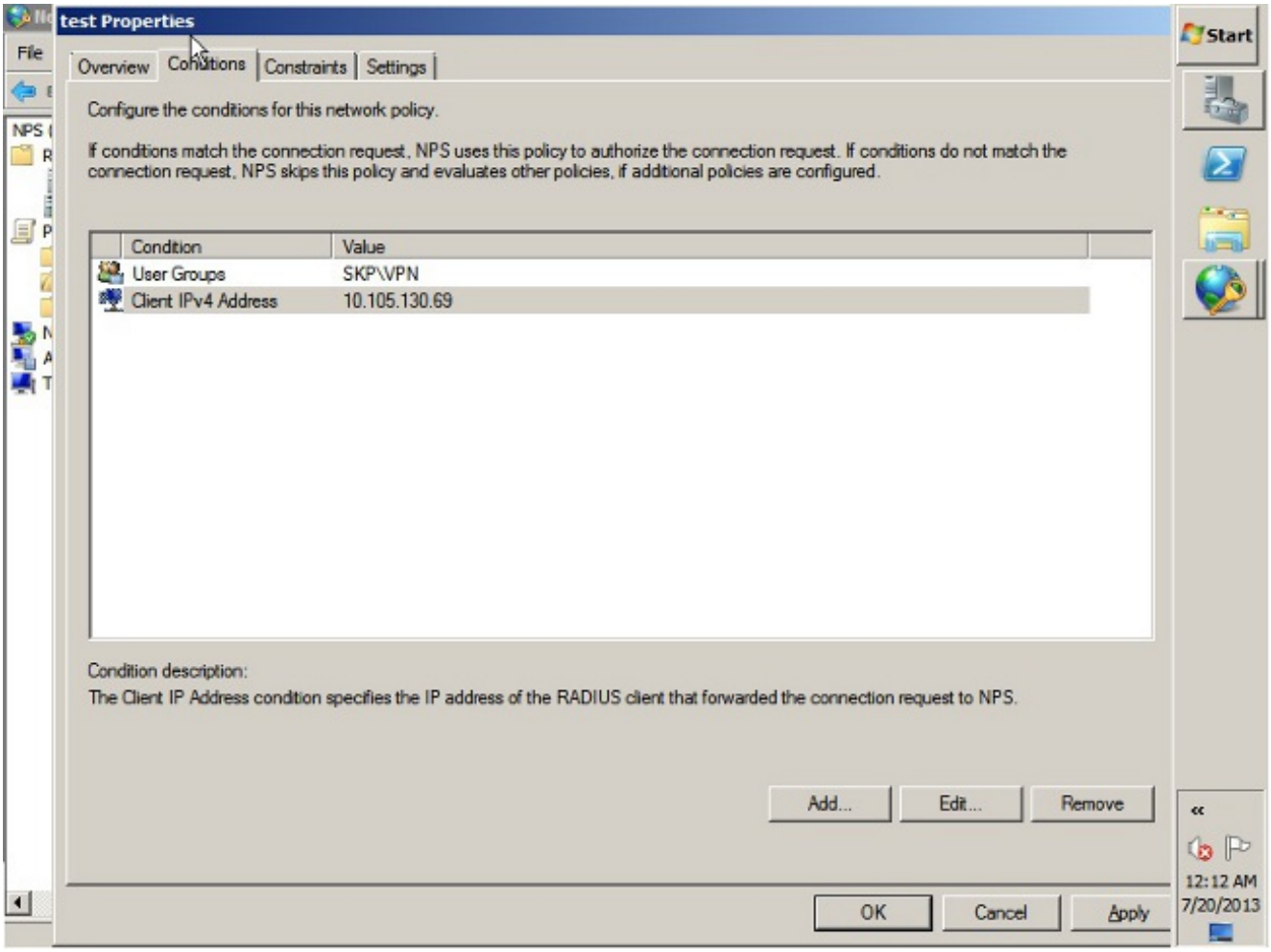
Clique na guia **Configurações**.Em Forwarding Connection Request, escolha **Authentication**. Verifique se o botão de opção Autenticar solicitações neste servidor está selecionado.Click **OK**.



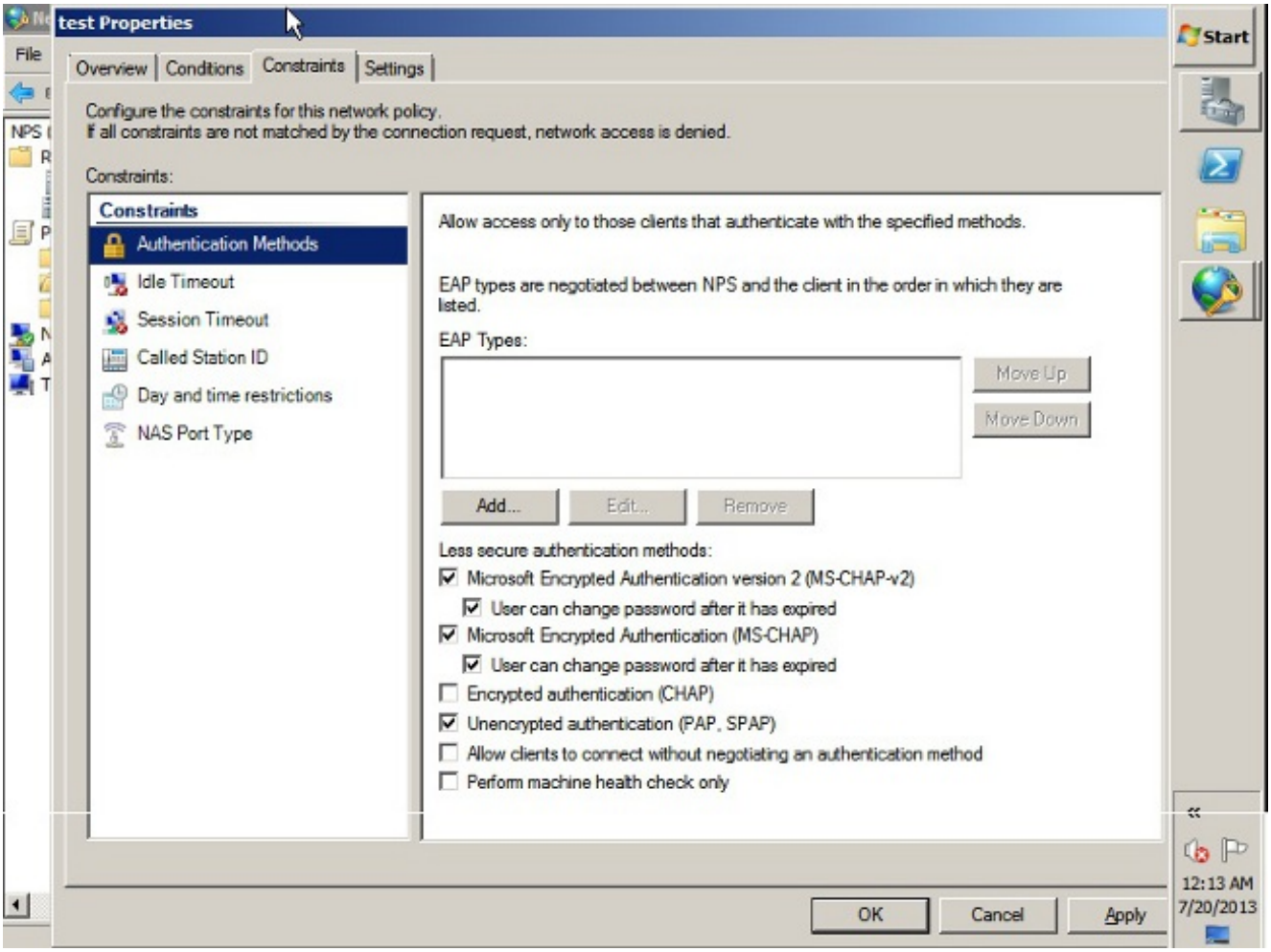
3. Adicione uma política de rede onde você possa especificar quais usuários têm permissão para autenticar.Por exemplo, você pode adicionar grupos de usuários do Ative Diretory como uma condição. Apenas os usuários que pertencem a um grupo especificado do Windows são autenticados sob esta política.Em NPS, escolha **Policies**.Clique com o botão direito do mouse em **Política de rede** e crie uma nova política.Verifique se o botão de opção Conceder acesso está selecionado.Na lista suspensa Tipo de servidor de acesso à rede, escolha **Não especificado**.



Clique na guia **Condições**.Clique em Add.Insira o endereço IP do ASA como condição de endereço IPv4 do cliente.Insira o grupo de usuários do Ative Diretory que contém usuários de
VPN.



Clique na guia **Restrições**.Escolha **Métodos de Autenticação**.Verifique se a caixa de seleção Autenticação não criptografada (PAP, SPAP) está marcada.Click **OK**.

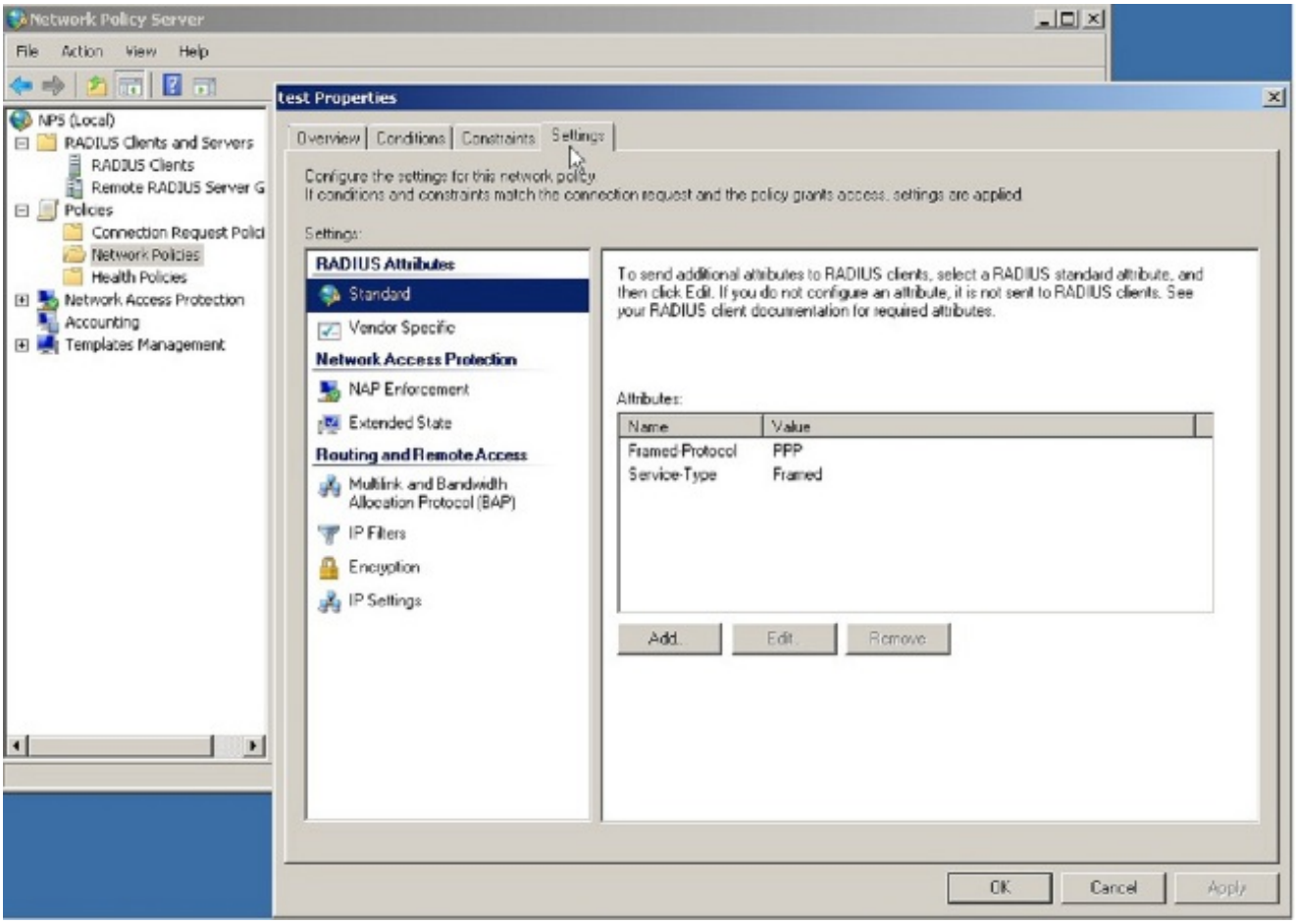


Pass Group-policy Attribute (Atributo 25) do Servidor NPS RADIUS

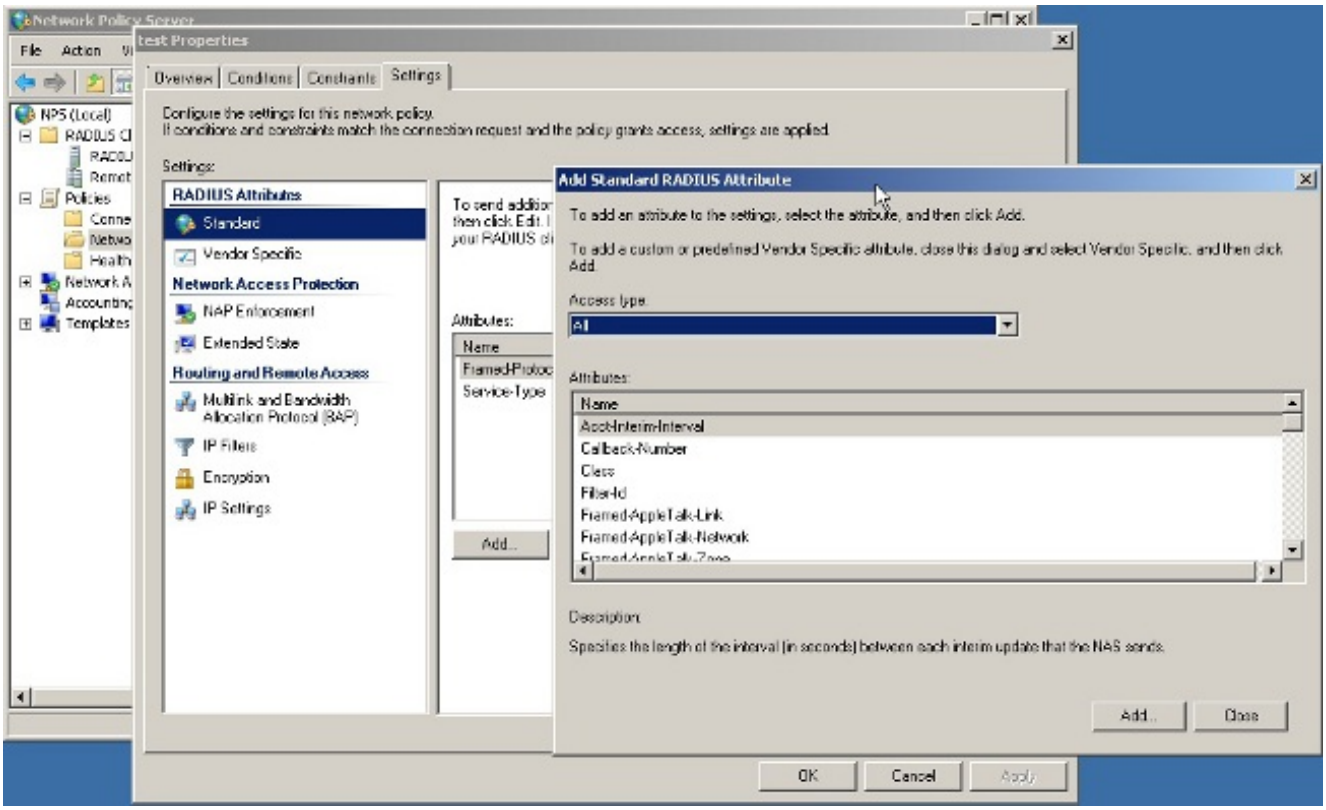
Se a política de grupo precisar ser atribuída ao usuário dinamicamente com o servidor NPS RADIUS, o atributo RADIUS da política de grupo (atributo 25) poderá ser usado.

Conclua estes passos para enviar o atributo RADIUS 25 para atribuição dinâmica de uma política de grupo ao usuário.

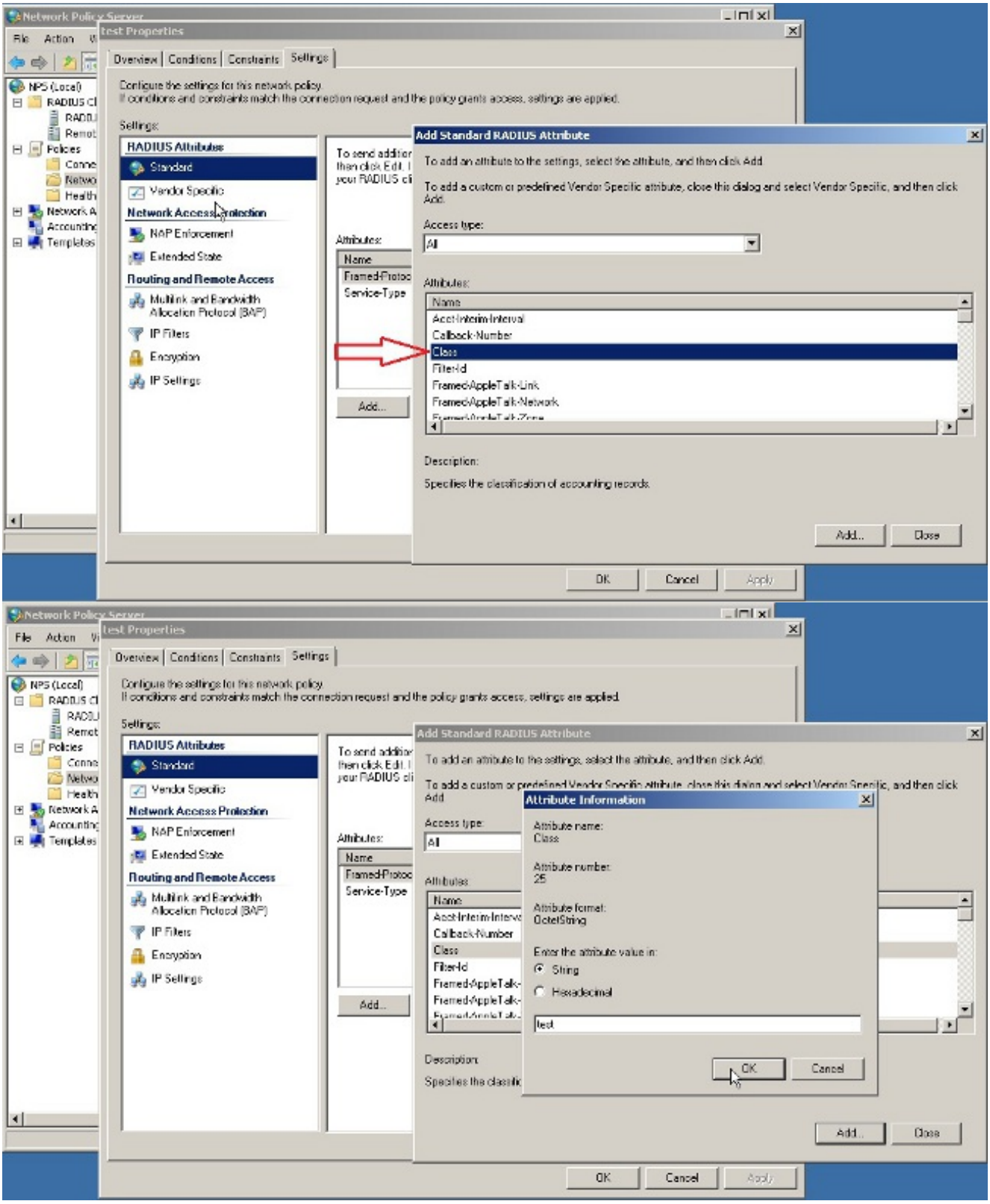
1. Depois que a Diretiva de rede for adicionada, clique com o botão direito do mouse na Diretiva de rede necessária e clique na guia **Configurações**.



2. Escolha **Atributos RADIUS > Padrão**. Clique em Add. Deixe o tipo de acesso como Todos.



3. Na caixa Atributos, escolha **Classe** e clique em **Adicionar**. Digite o valor do atributo, ou seja, o nome da política de grupo como uma string. Lembre-se de que uma política de grupo com esse nome deve ser configurada no ASA. Isso significa que o ASA o atribui à sessão VPN após receber esse atributo na resposta
RADIUS.



Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

> **Note**: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug.**

Depurações do ASA

Ative **debug radius all** no ASA.

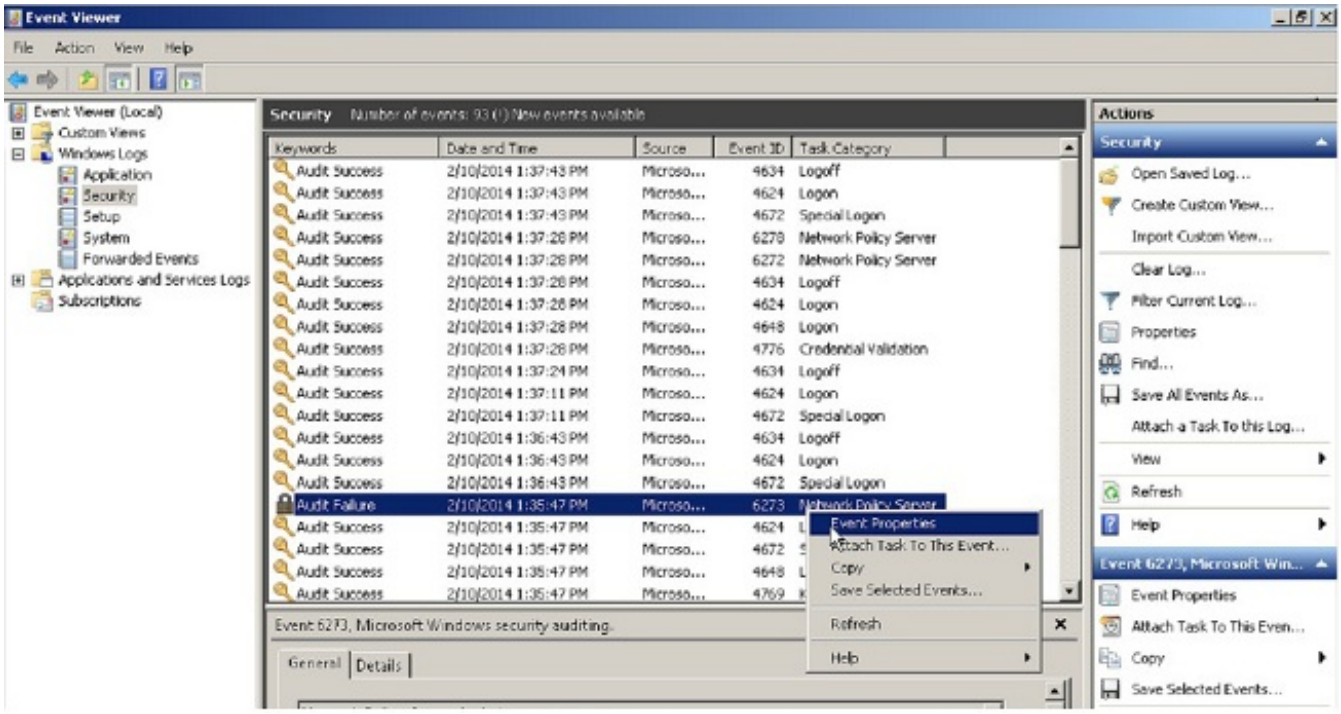
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Verifique se a conectividade entre o ASA e o servidor NPS está boa.Aplique capturas de pacotes para garantir que a solicitação de autenticação saia da interface ASA (de onde o servidor pode ser alcançado). Confirme se os dispositivos no caminho não bloqueiam a porta UDP 1645 (porta de autenticação RADIUS padrão) para garantir que ela chegue ao servidor NPS. Mais informações sobre capturas de pacotes no ASA podem ser encontradas no ASA/PIX/FWSM: Exemplo de Captura de Pacotes usando CLI e ASDM Configuration.
- Se a autenticação ainda falhar, verifique o visualizador de eventos no NPS do Windows. Em Visualizador de Eventos > Logs do Windows, escolha **Segurança.** Procure eventos associados ao NPS por volta da hora da solicitação de autenticação.



Depois de abrir as Propriedades do evento, você poderá ver o motivo da falha, como mostrado no exemplo. Neste exemplo, PAP não foi escolhido como o tipo de autenticação na política de rede. Portanto, a solicitação de autenticação falha.

```
 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.**