Ejemplo de Configuración de Autenticación de Usuario VPN ASA contra Servidor NPS de Windows 2008 (Active Directory) con RADIUS

Contenido

Introducción

Este documento explica cómo configurar un dispositivo de seguridad adaptable (ASA) para comunicarse con un servidor de políticas de red (NPS) de Microsoft Windows 2008 con el protocolo RADIUS de modo que los usuarios WebVPN heredados de Cisco VPN Client/AnyConnect/Clientless WebVPN se autentiquen con Active Directory. NPS es una de las funciones de servidor que ofrece Windows 2008 Server. Es equivalente a Windows 2003 Server, IAS (Internet Authentication Service), que es la implementación de un servidor RADIUS para proporcionar autenticación de usuario de marcado remoto. De manera similar, en Windows 2008 Server, NPS es la implementación de un servidor RADIUS. Básicamente, ASA es un cliente RADIUS a un servidor RADIUS NPS. ASA envía solicitudes de autenticación RADIUS en nombre de los usuarios de VPN y NPS las autentica con Active Directory.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

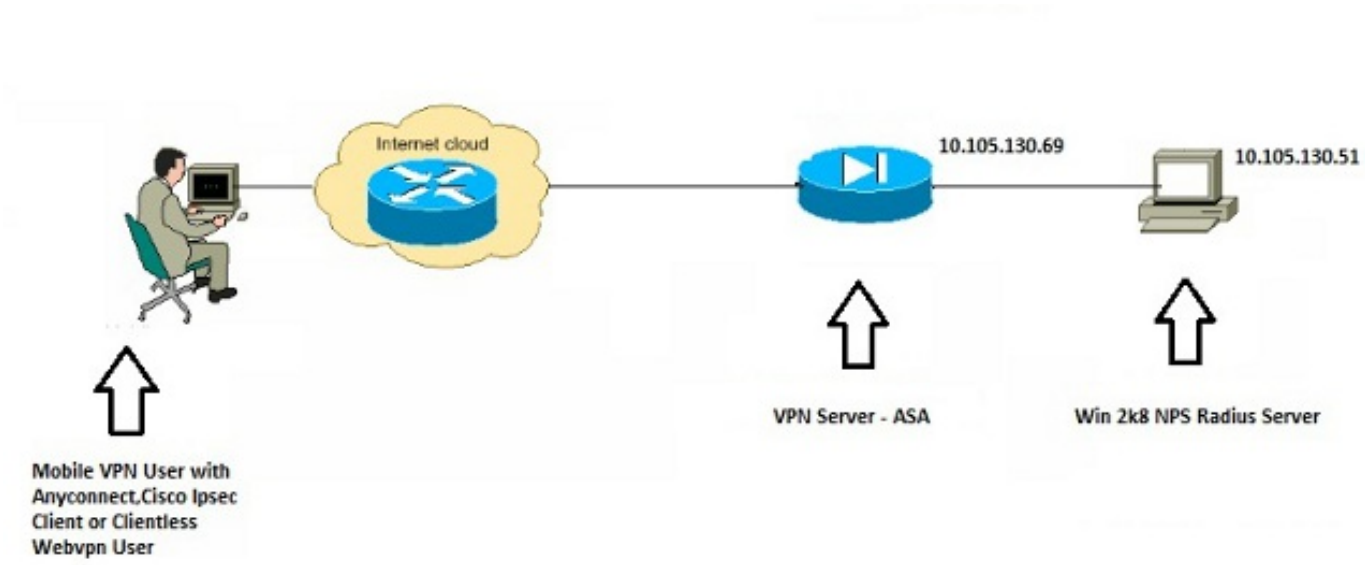
- ASA que ejecuta la versión 9.1(4)
- Servidor Windows 2008 R2 con servicios de Active Directory y función NPS instalada

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

> **Nota:** Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

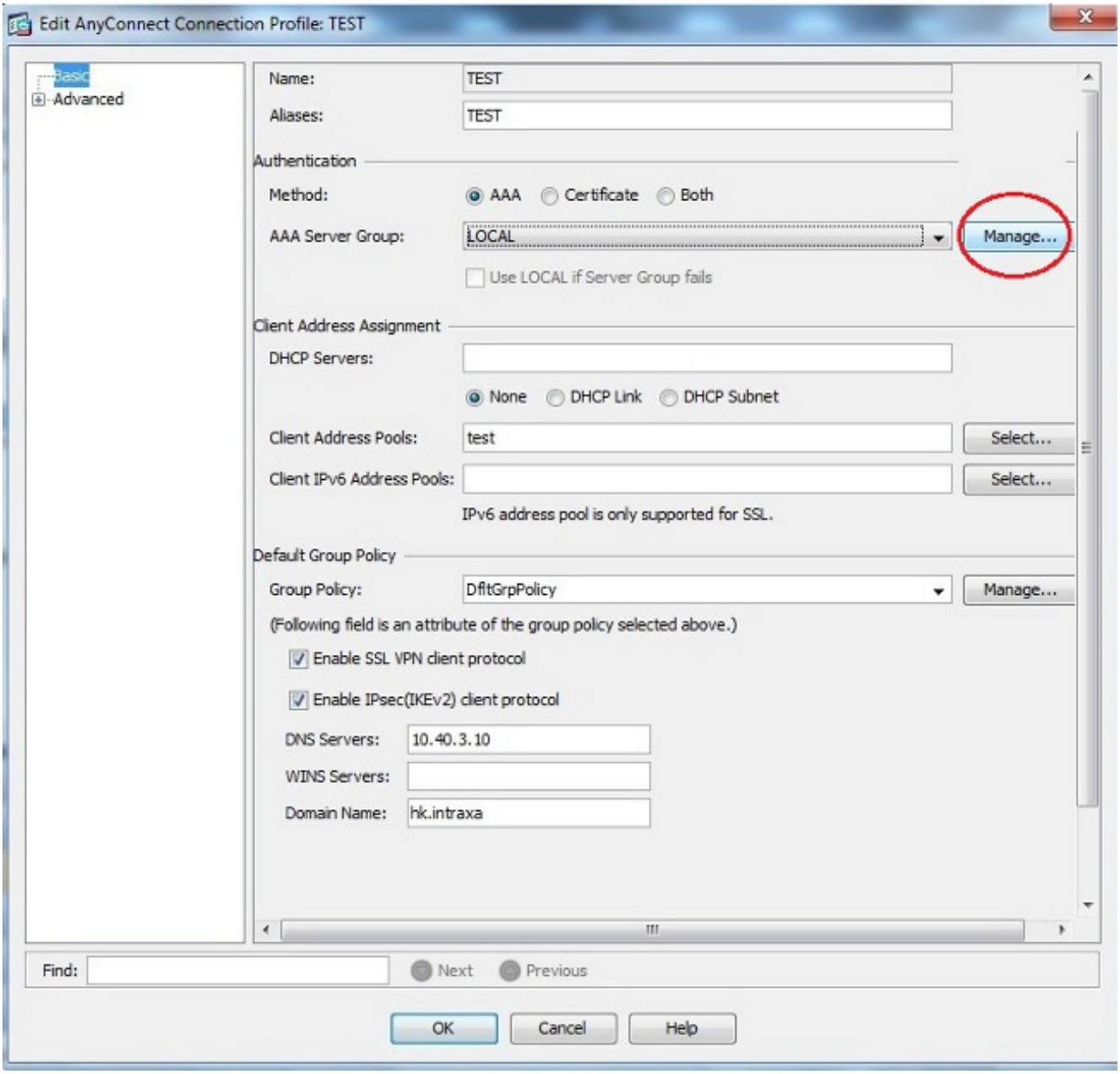
Diagrama de la red



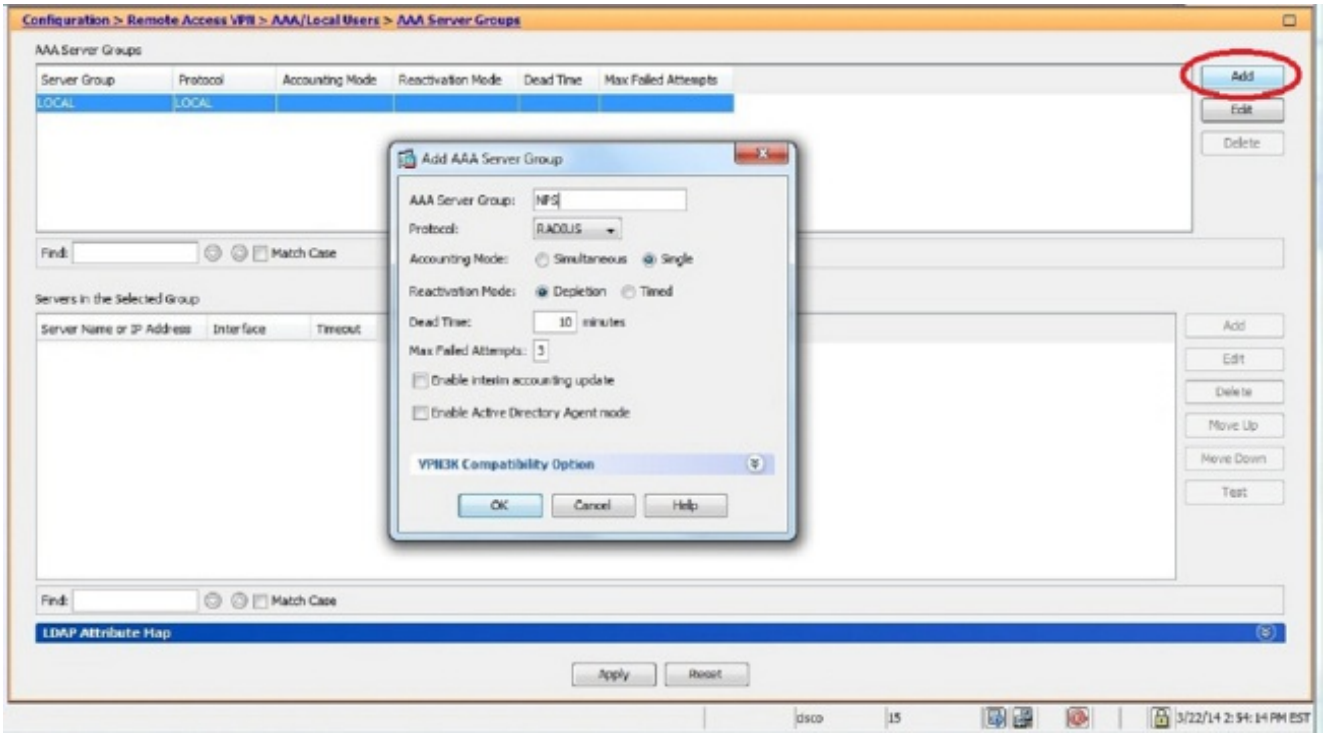
Configuraciones

Configuración de ASDM

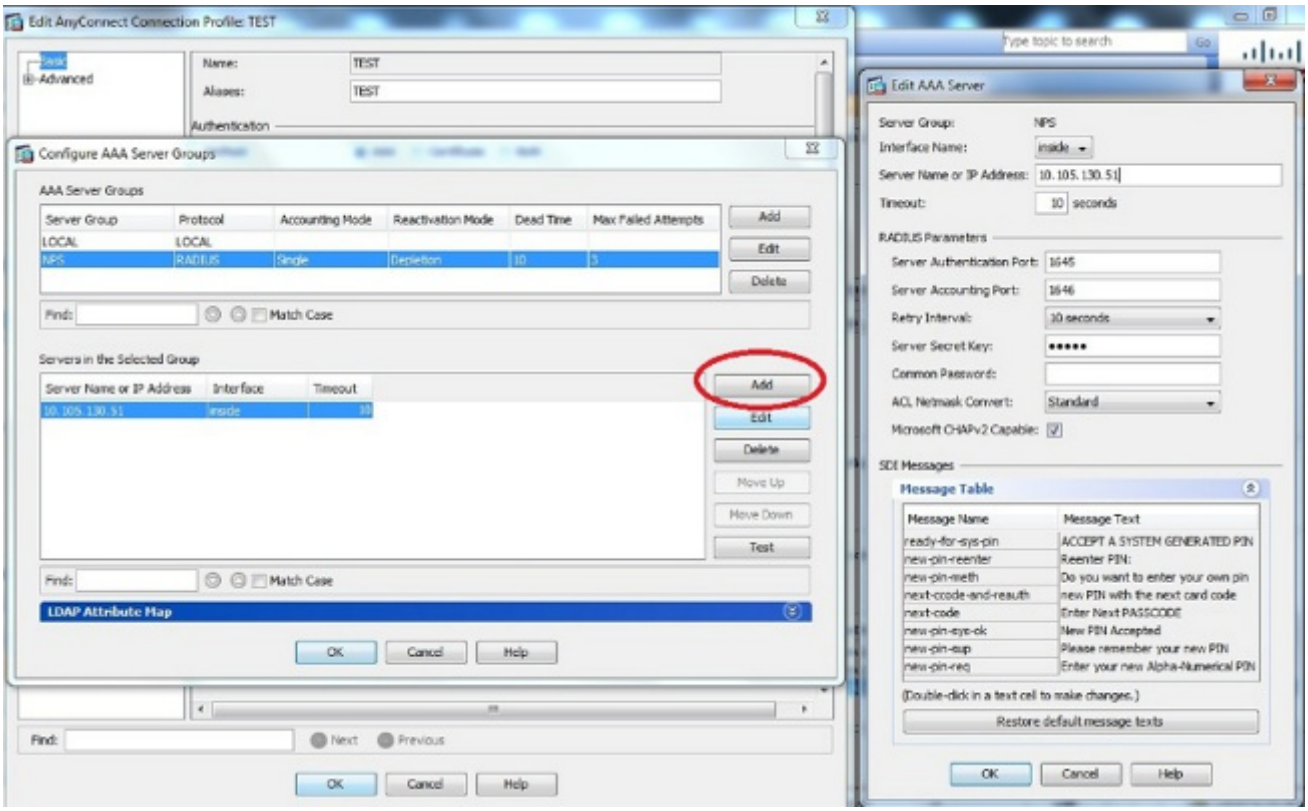
1. Elija el grupo de túnel para el que se requiere autenticación NPS.
2. Haga clic en **Editar** y elija **Básico**.
3. En la sección Autenticación, haga clic en **Administrar**.



4. En la sección AAA Server Groups , haga clic en **Add**.
5. En el campo AAA Server Group (Grupo de servidores AAA), introduzca el nombre del grupo de servidores (por ejemplo, NPS).
6. En la lista desplegable Protocol , elija **RADIUS**.
7. Click
   OK.

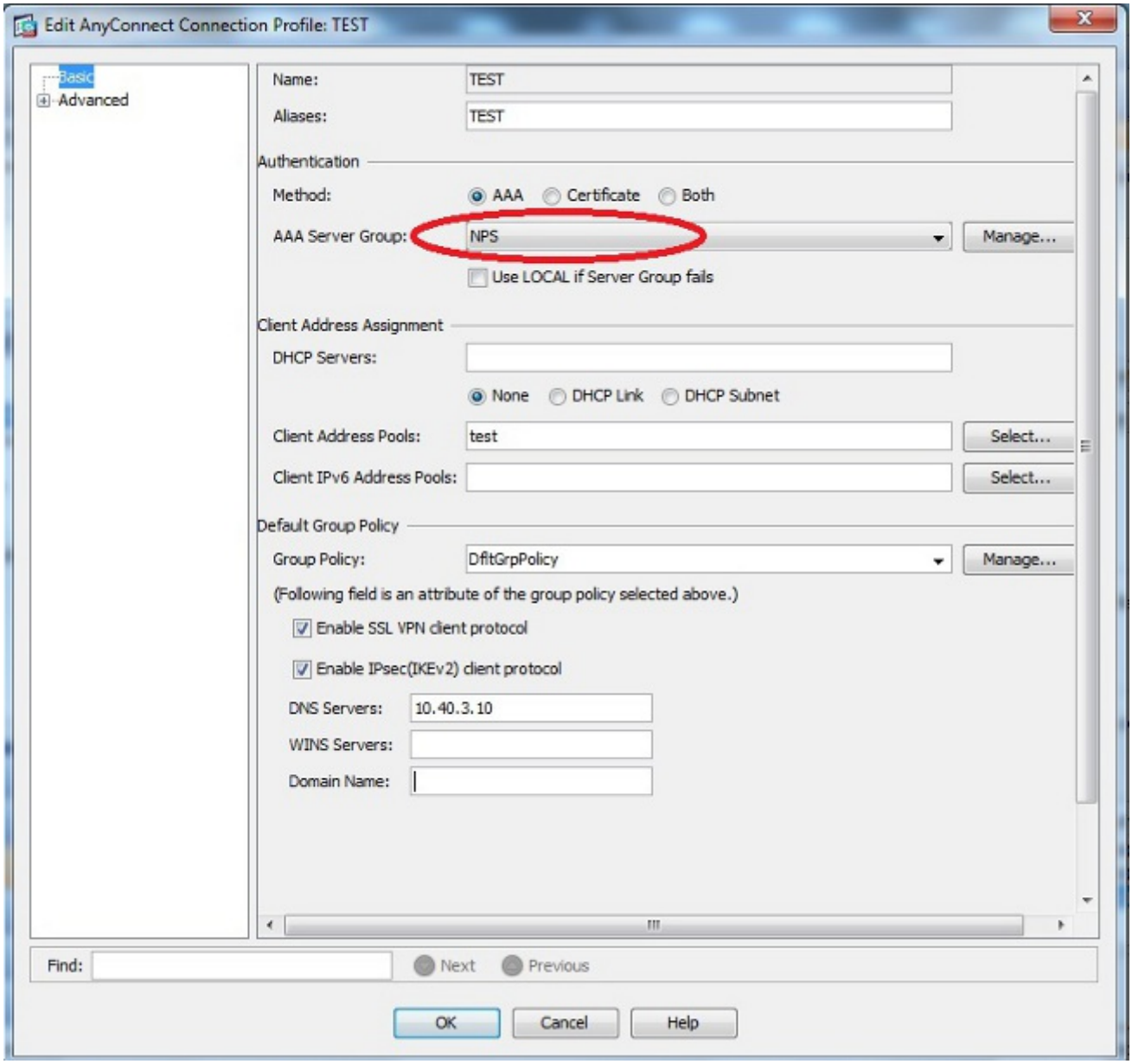


8. En la sección Servidores de la sección Grupo Seleccionado, elija el Grupo de Servidor AAA agregado y haga clic en **Agregar**.
9. En el campo Server Name (Nombre de servidor) o IP Address (Dirección IP), introduzca la dirección IP del servidor.
10. En el campo Server Secret Key (Clave secreta del servidor), introduzca la clave secreta.
11. Deje los campos Server Authentication Port y Server Accounting Port en el valor predeterminado a menos que el servidor escuche en un puerto diferente.
12. Click OK.
13. Click
    OK.



14. En la lista desplegable Grupo de servidores AAA, elija el grupo (NPS en este ejemplo) agregado en los pasos anteriores.

15. Click OK.



Configuración 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
```

De forma predeterminada, ASA utiliza el tipo de autenticación del protocolo de autenticación de contraseña (PAP) no cifrado. Esto no significa que el ASA envíe la contraseña en texto sin formato cuando envía el paquete RADIUS REQUEST. Más bien, la contraseña de texto sin formato se cifra con el secreto compartido RADIUS.

Si la administración de contraseñas se habilita bajo el grupo de túnel, ASA utiliza el tipo de autenticación MSCHAP-v2 para cifrar la contraseña de texto sin formato. En tal caso, asegúrese de que la casilla de verificación **Microsoft CHAPv2 Capable** esté marcada en la ventana Edit AAA Server configurada en la sección ASDM configuration.

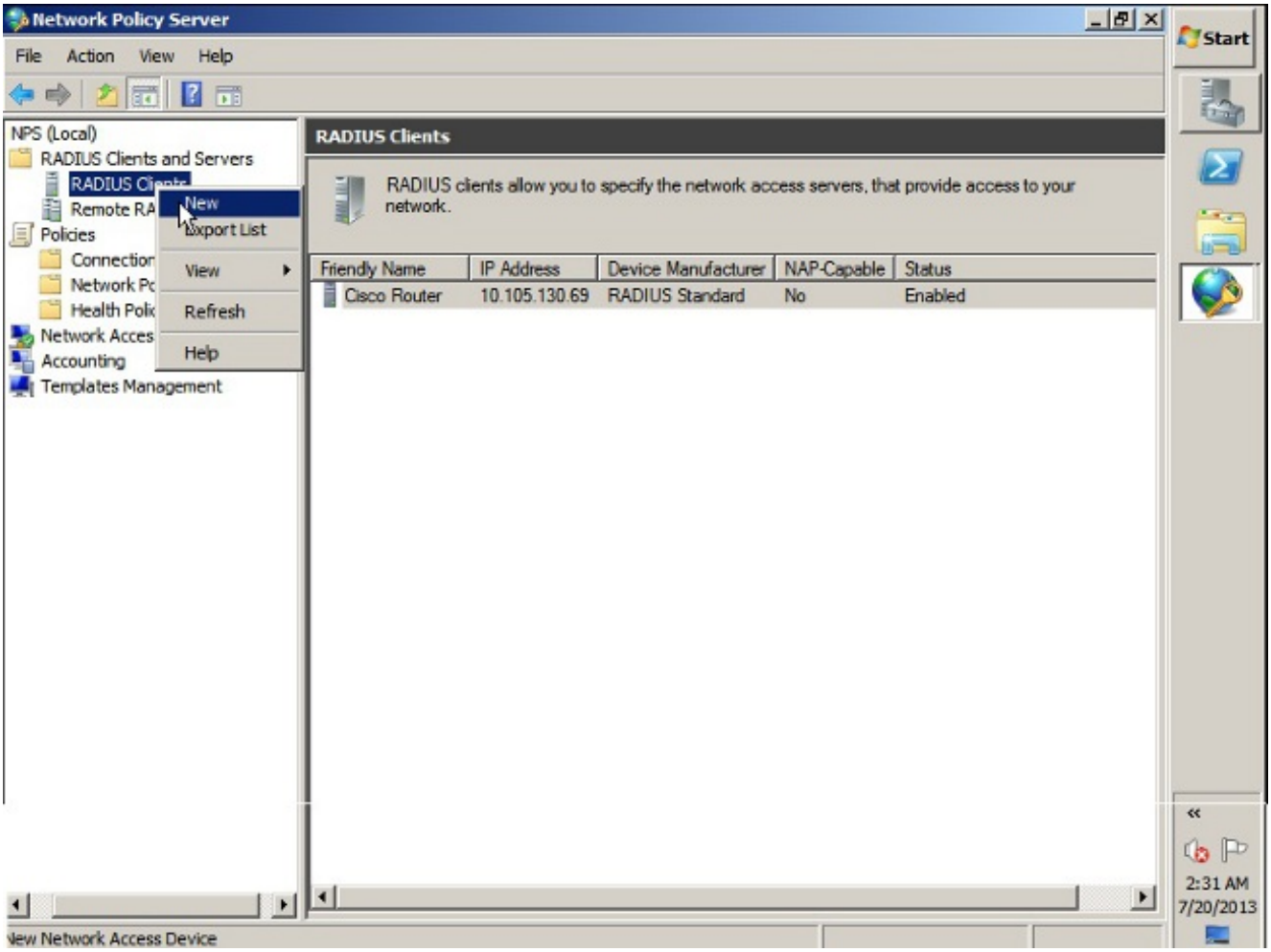
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **Nota:** El comando **test aaa-server authentication** siempre utiliza PAP. Sólo cuando un usuario inicia una conexión con un grupo de túnel con la administración de contraseñas habilitada, el ASA utiliza MSCHAP-v2. Además, la opción 'password-management [password-caduc-in-days]' solo se admite con LDAP (protocolo ligero de acceso a directorios). RADIUS no proporciona esta función. Verá la opción de caducidad de la contraseña cuando la contraseña ya haya caducado en Active Directory.

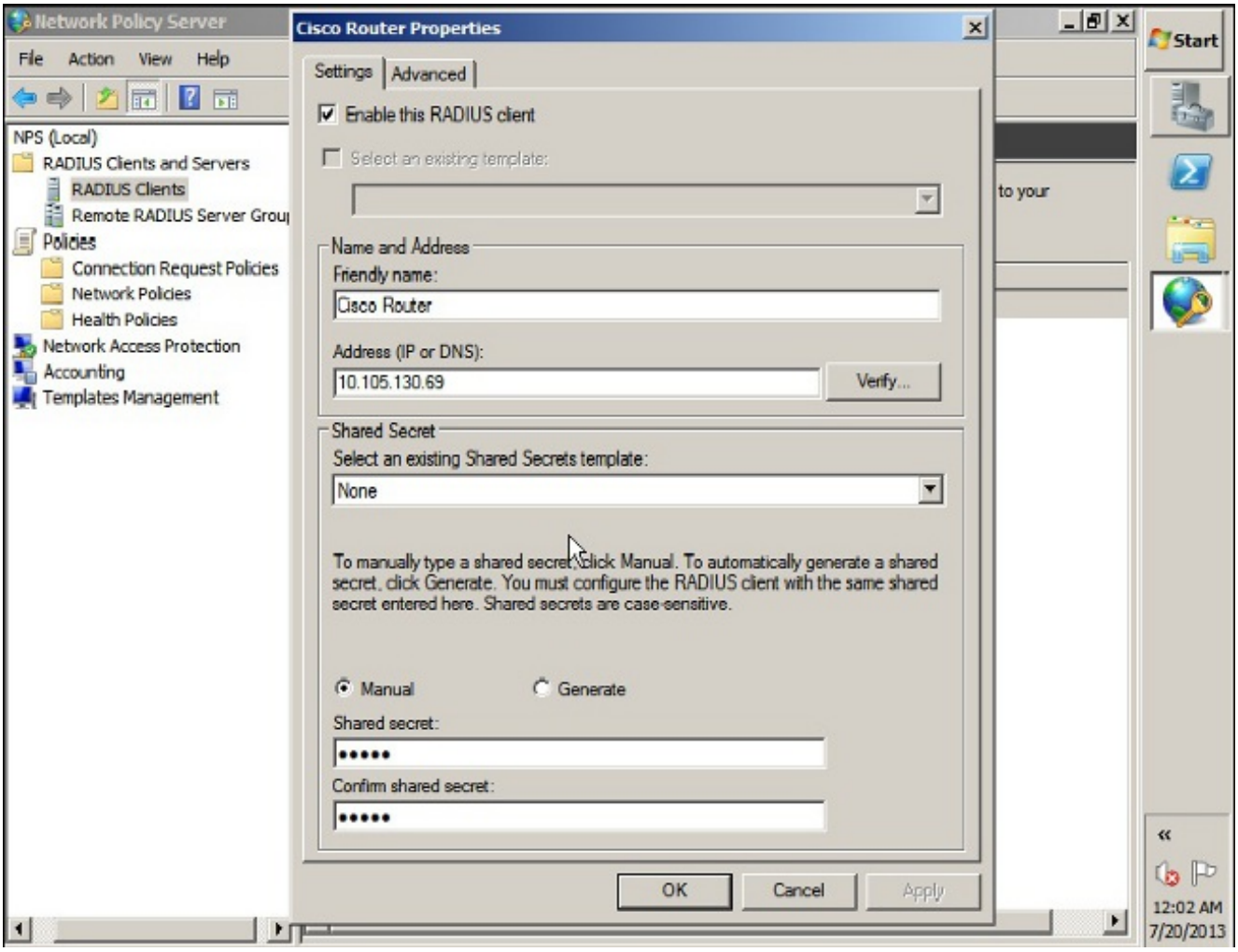
Windows 2008 Server con configuración de NPS

La función de servidor NPS se debe instalar y ejecutar en el servidor de Windows 2008. Si no es así, elija **Inicio > Herramientas administrativas > Roles de servidor > Agregar servicios de rol**. Elija Network Policy Server e instale el software. Una vez instalado el rol de servidor NPS, complete estos pasos para configurar el NPS para aceptar y procesar las solicitudes de autenticación RADIUS del ASA:

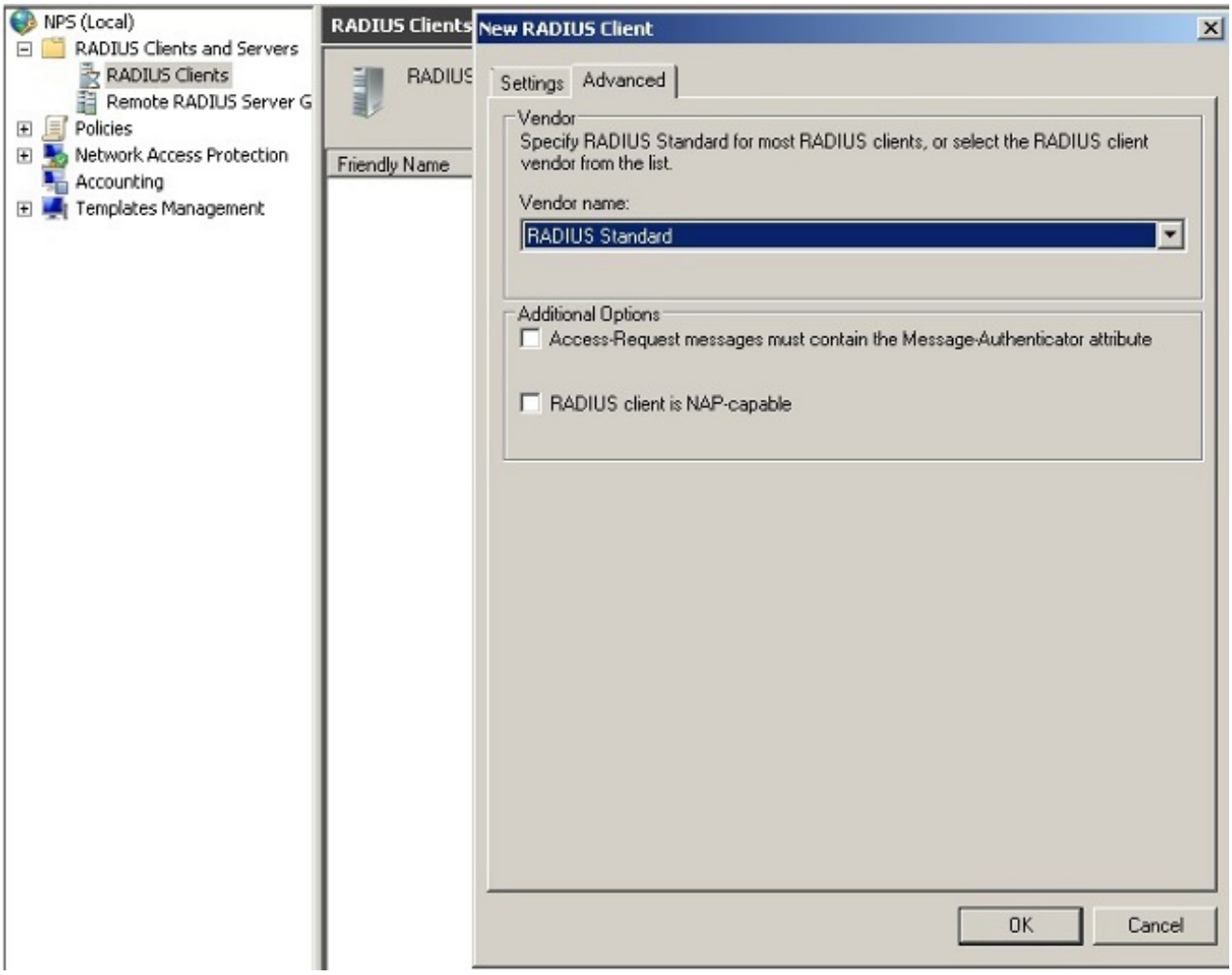
1. Agregue el ASA como cliente RADIUS en el servidor NPS. Elija **Administrative Tools > Network Policy Server .**Haga clic con el botón derecho en **Clientes RADIUS** y elija **Nuevo**.



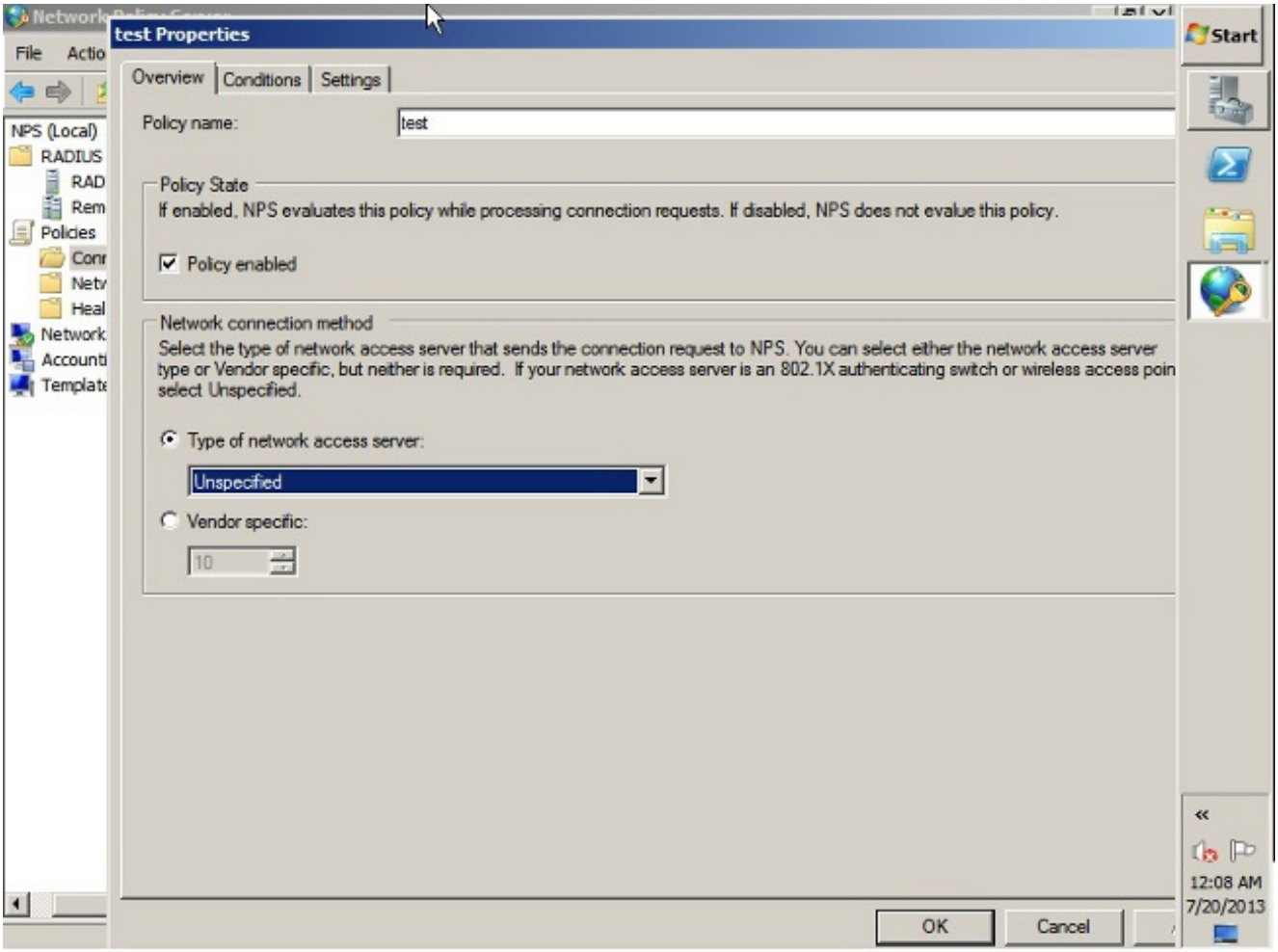
Introduzca un nombre descriptivo, una dirección (IP o DNS) y un secreto compartido configurados en el
ASA.



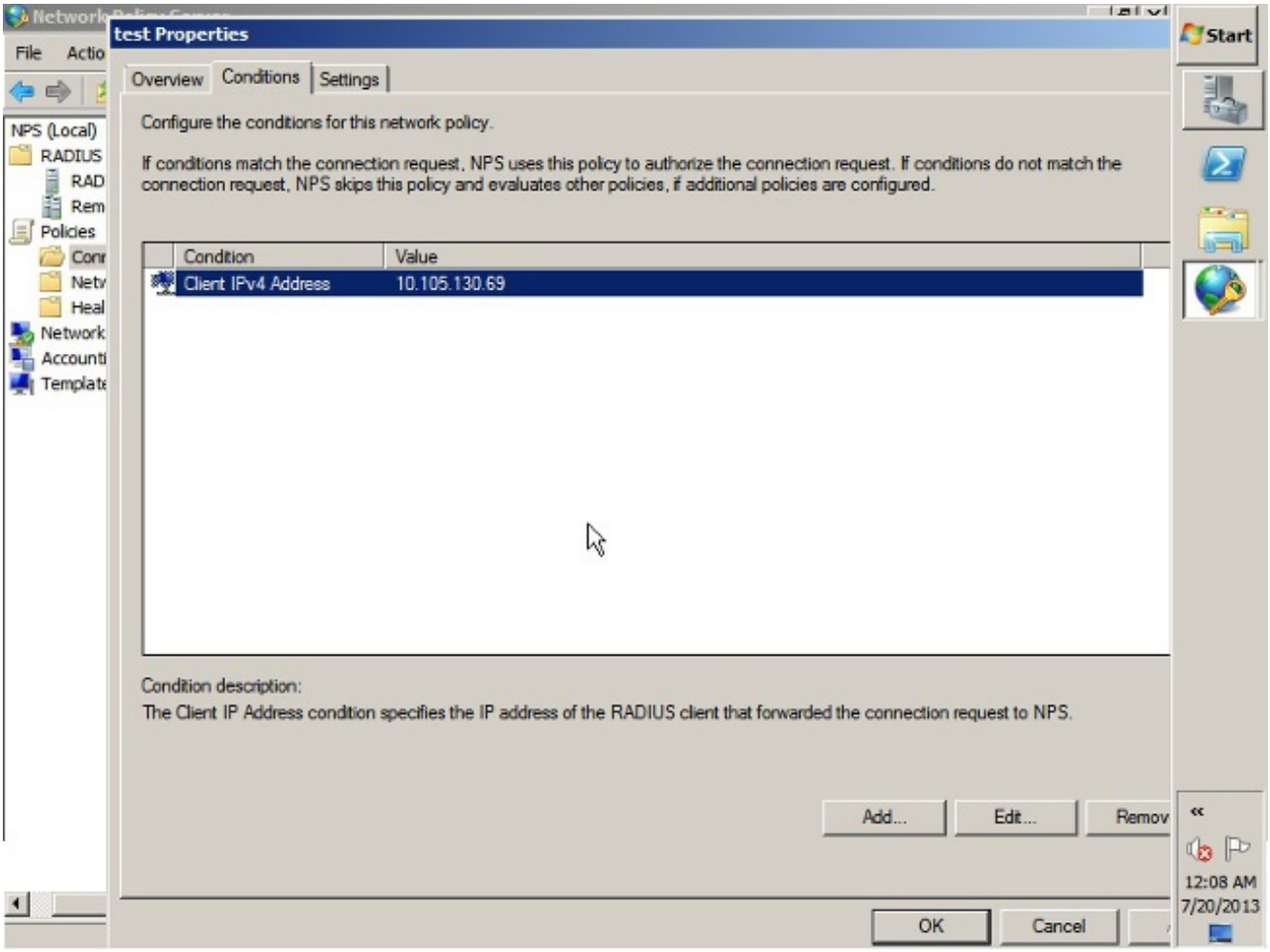
Haga clic en la ficha Advanced (Opciones avanzadas).En la lista desplegable Nombre del proveedor, elija **Estándar RADIUS**.Click
OK.



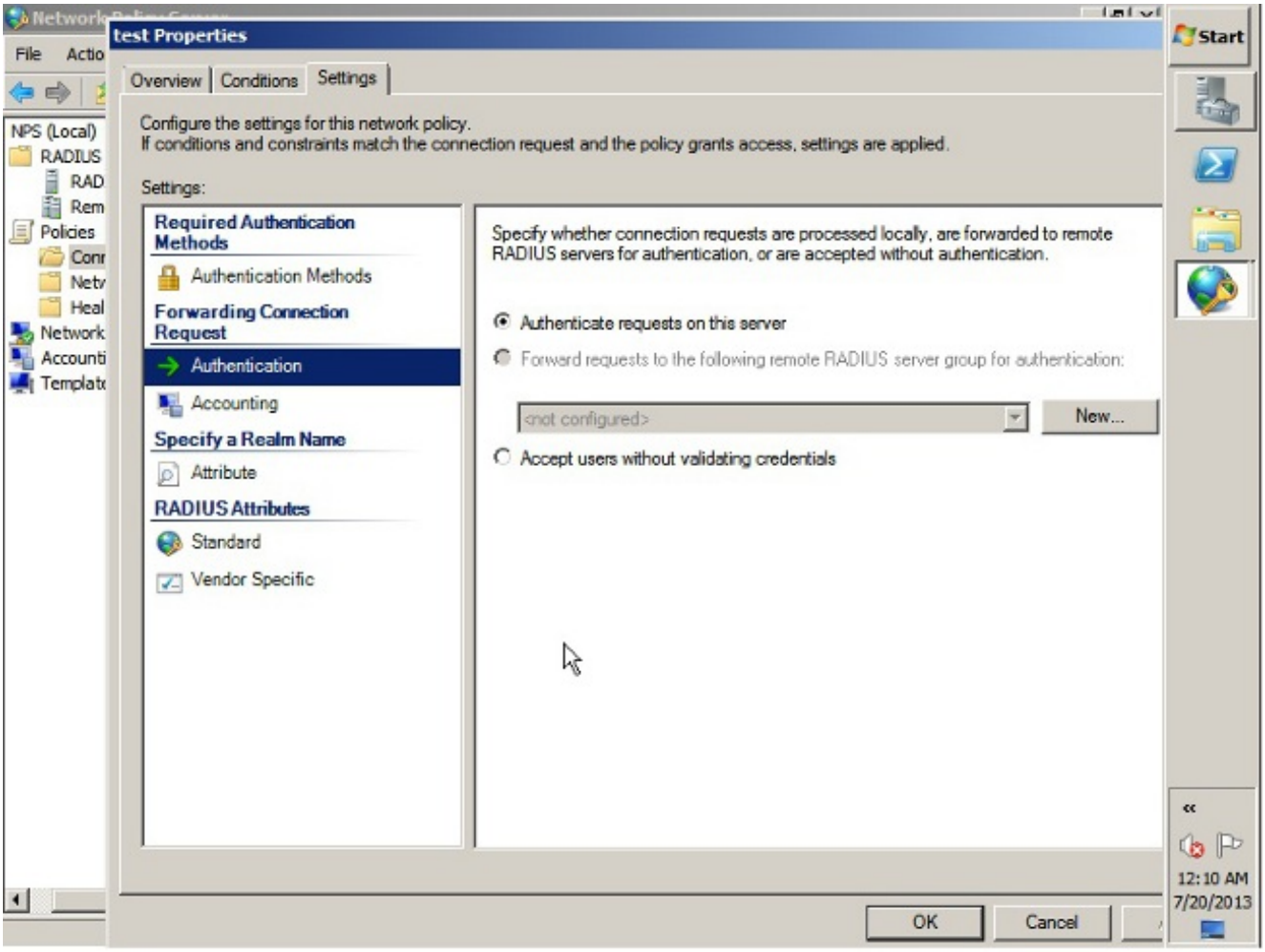
2. Cree una nueva política de solicitud de conexión para los usuarios de VPN. El propósito de la política de solicitud de conexión es especificar si las solicitudes de los clientes RADIUS se procesarán localmente o se reenviarán a los servidores RADIUS remotos. En NPS > Policies, haga clic con el botón derecho del ratón en **Connection Request Policies** y cree una nueva política.En la lista desplegable Tipo de servidor de acceso a la red, elija **Sin especificar**.



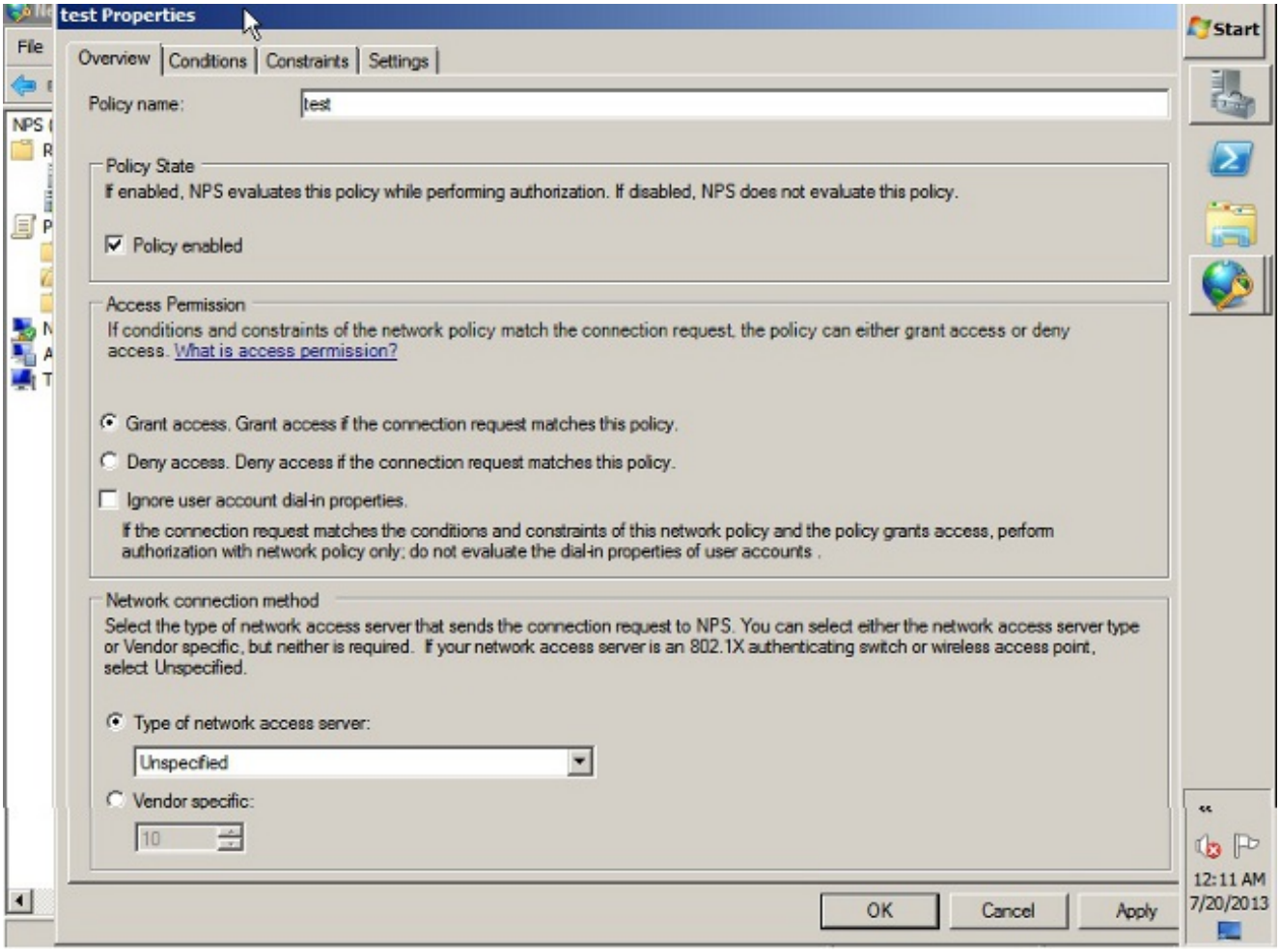
Haga clic en la pestaña **Condiciones**.Haga clic en Add (Agregar).Introduzca la dirección IP del ASA como condición 'Dirección IPv4 del cliente'.



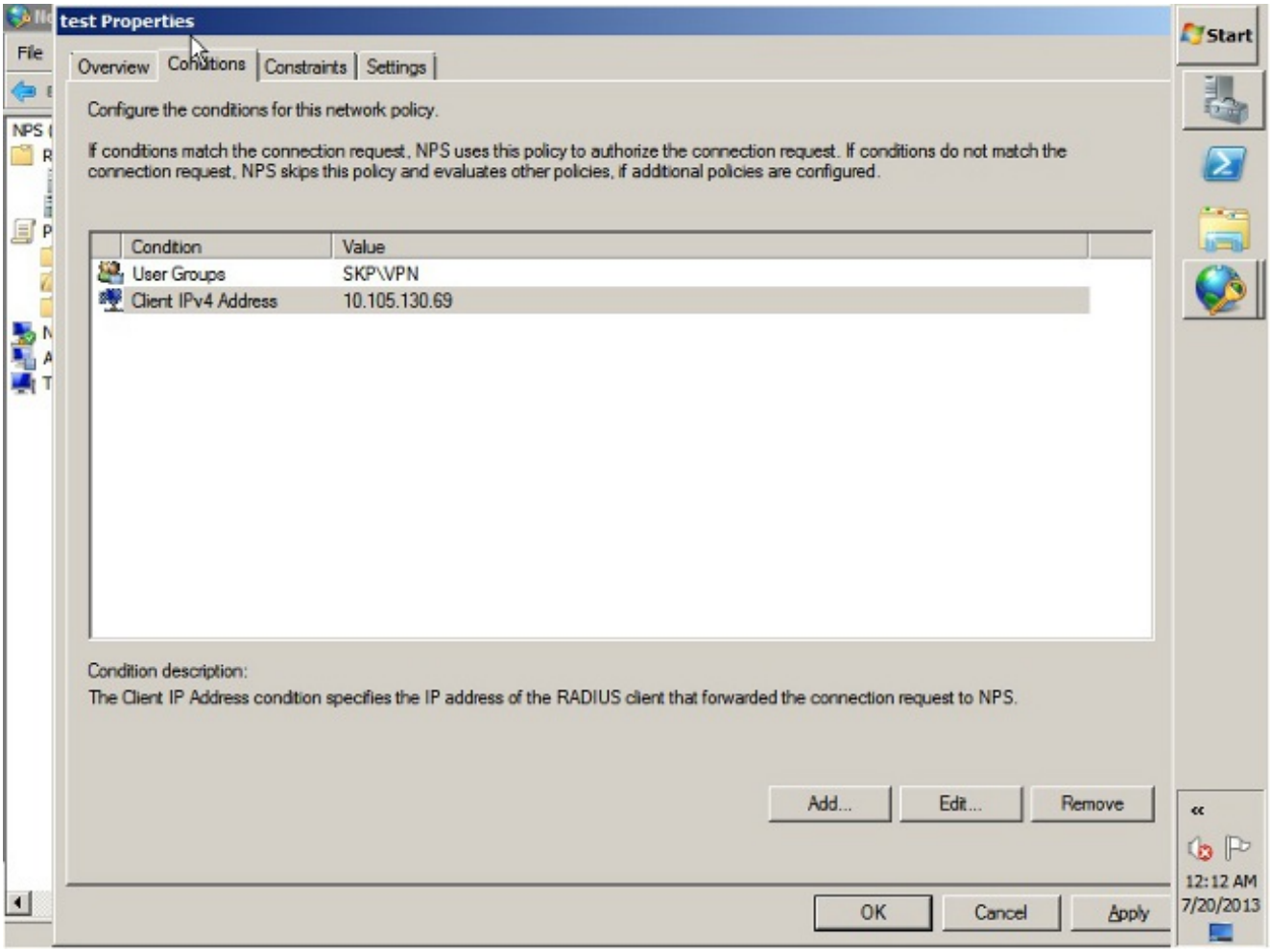
Haga clic en la pestaña **Settings**.En Forwarding Connection Request , elija **Authentication**. Asegúrese de seleccionar el botón de opción Autenticar solicitudes en este servidor.Click OK.



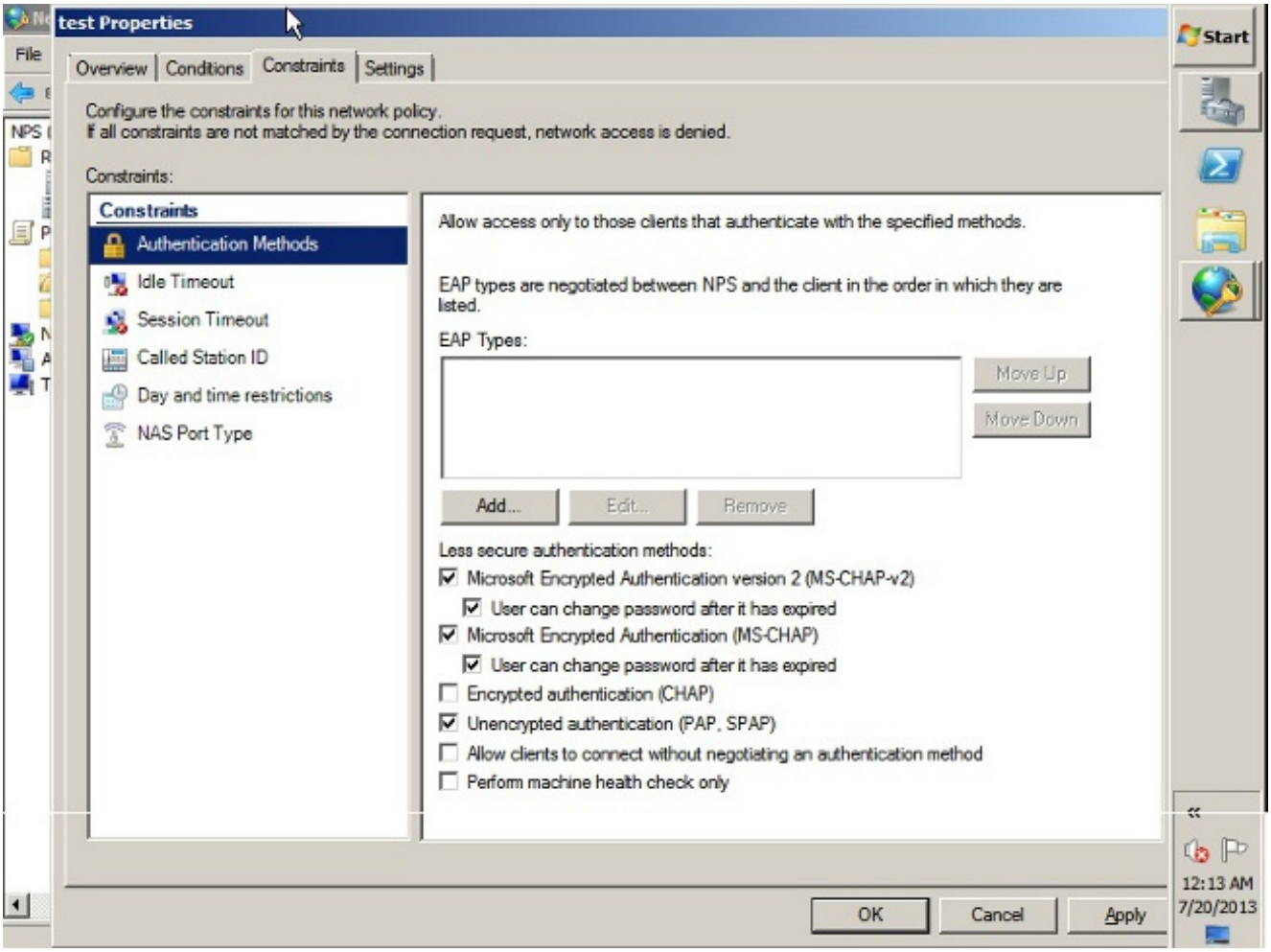
3. Agregue una política de red donde puede especificar qué usuarios pueden autenticarse.Por ejemplo, puede agregar grupos de usuarios de Active Directory como condición. En esta directiva sólo se autentican los usuarios que pertenecen a un grupo de Windows especificado.En NPS, elija **Políticas**.Haga clic con el botón derecho del ratón en **Directiva de red** y cree una nueva política.Asegúrese de seleccionar el botón de opción Conceder acceso.En la lista desplegable Tipo de servidor de acceso a la red, elija **Sin especificar**.



Haga clic en la pestaña **Condiciones**.Haga clic en Add (Agregar).Introduzca la dirección IP del ASA como condición de dirección IPv4 del cliente.Introduzca el grupo de usuarios de Active Directory que contiene usuarios de
VPN.



Haga clic en la pestaña **Restricciones**.Elija **Métodos de Autenticación**.Asegúrese de que la casilla de verificación Autenticación no cifrada (PAP, SPAP) está marcada.Click OK.

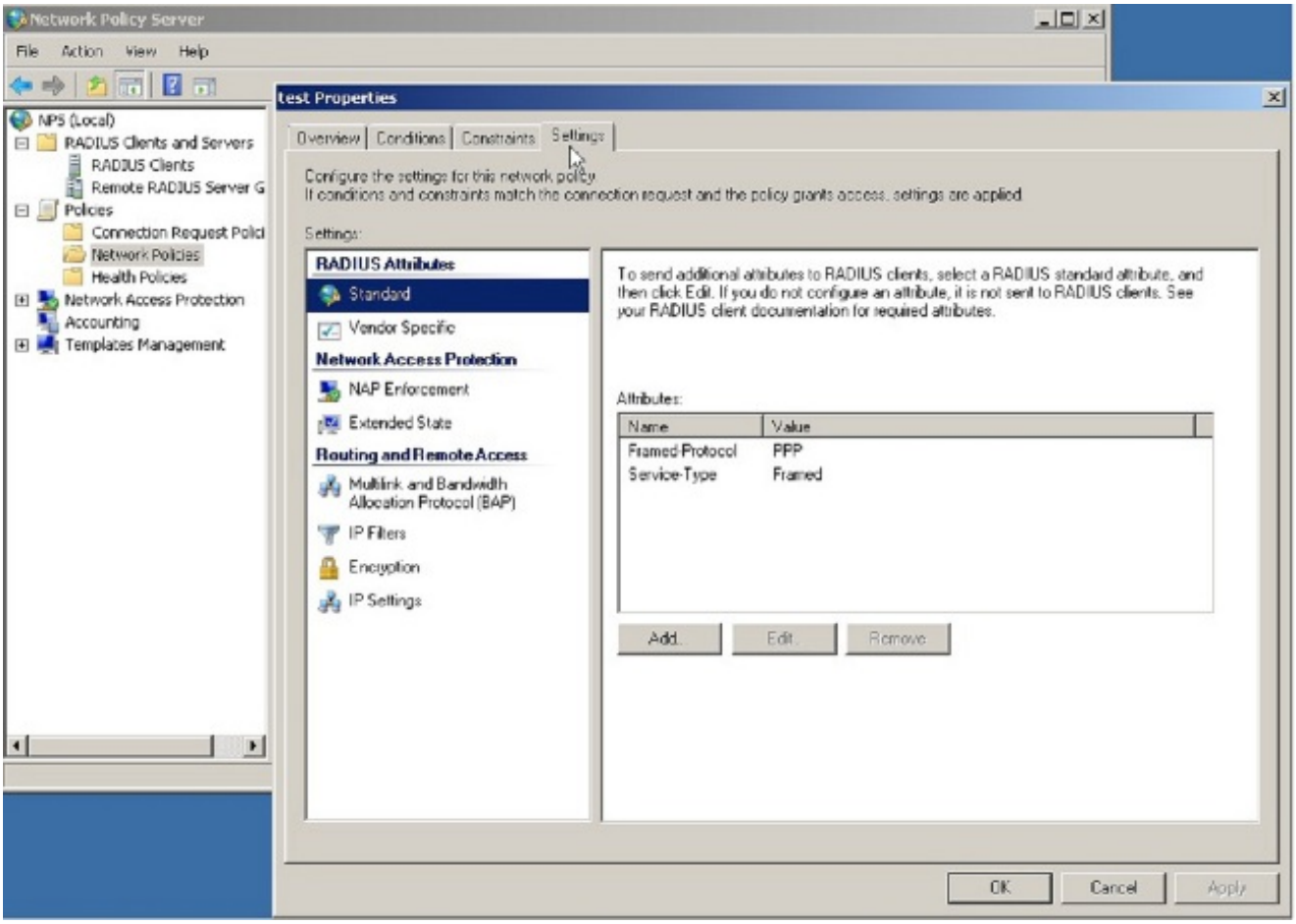


Pasar atributo de política de grupo (atributo 25) desde el servidor RADIUS NPS

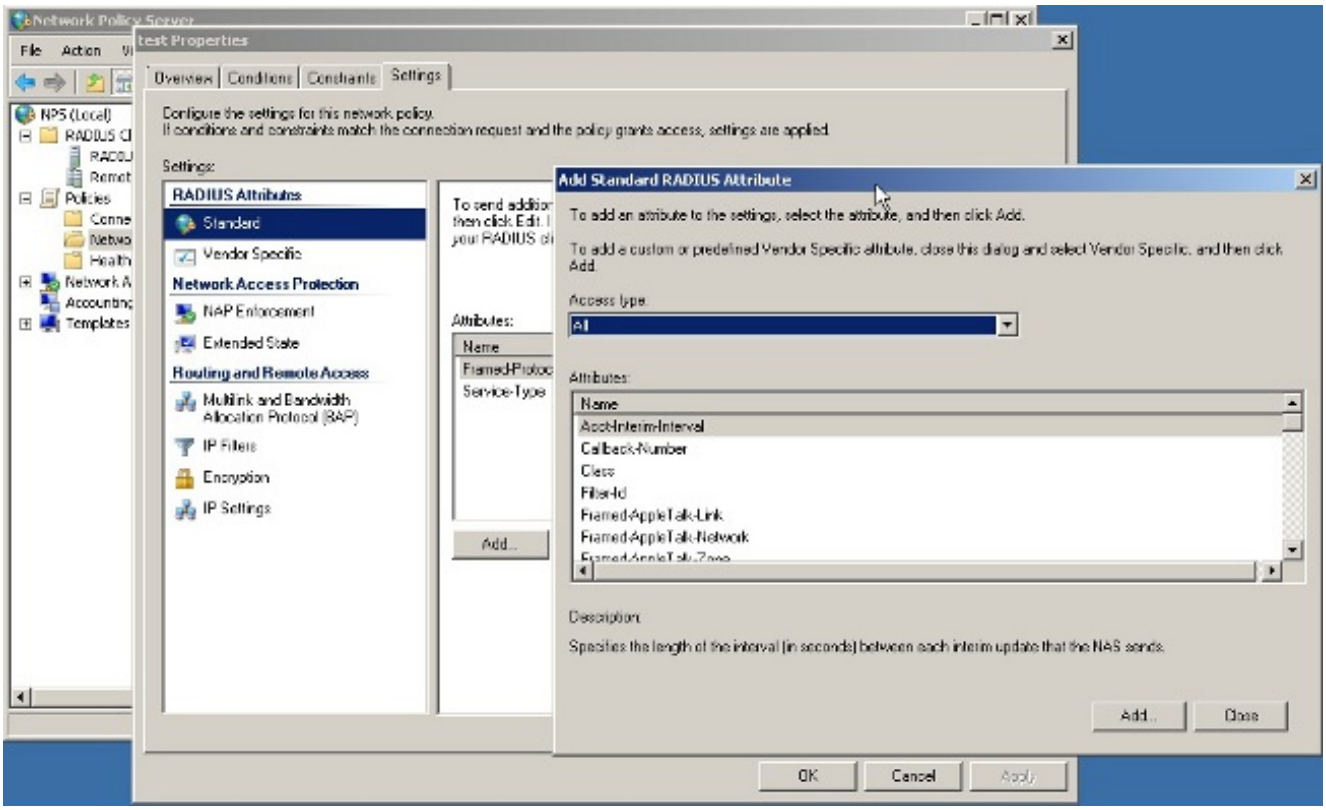
Si la política de grupo debe asignarse dinámicamente al usuario con el servidor RADIUS NPS, se puede utilizar el atributo RADIUS de política de grupo (atributo 25).

Complete estos pasos para enviar el atributo RADIUS 25 para la asignación dinámica de una política de grupo al usuario.

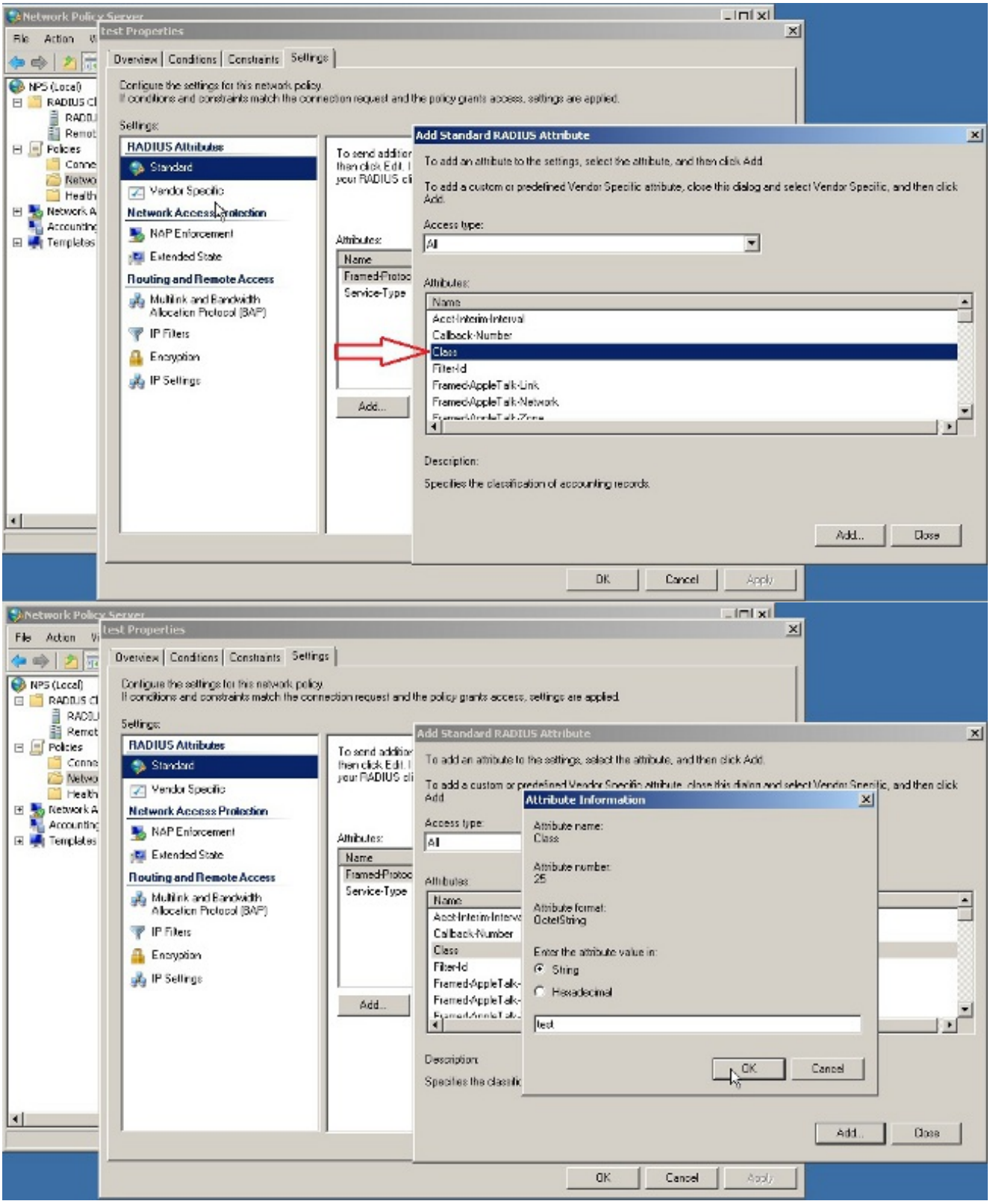
1. Después de agregar la política de red, haga clic con el botón derecho del ratón en la política de red requerida y haga clic en la ficha **Configuración**.



2. Elija **Atributos RADIUS > Estándar**. Haga clic en Add (Agregar). Deje el tipo de acceso como Todos.



3. En el cuadro Atributos, elija **Clase** y haga clic en **Agregar**. Introduzca el valor del atributo, es decir, el nombre de la política de grupo como cadena. Recuerde que una política de grupo con este nombre debe configurarse en el ASA. Esto es para que el ASA lo asigne a la sesión VPN después de recibir este atributo en la respuesta RADIUS.



Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

> **Nota:** Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Depuraciones de ASA

Habilite **debug radius all** en el ASA.

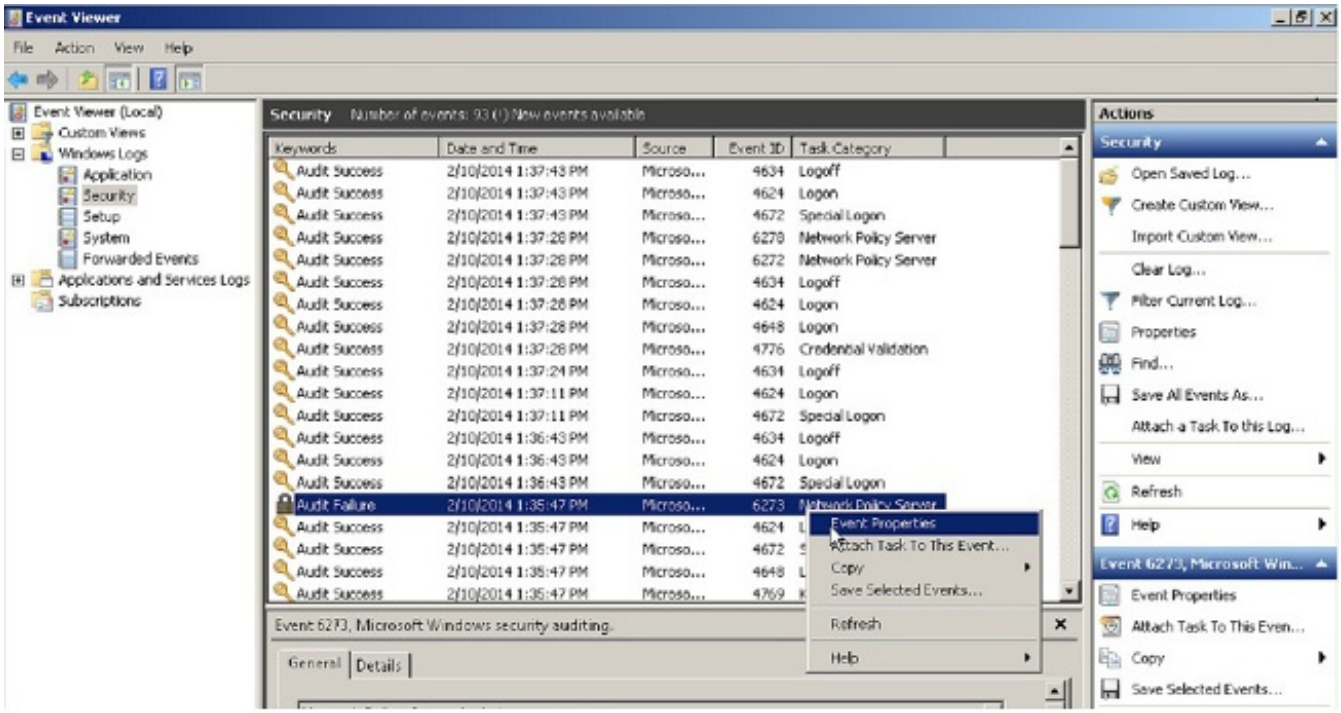
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

- Asegúrese de que la conectividad entre el ASA y el servidor NPS sea buena.Aplique capturas de paquetes para asegurarse de que la solicitud de autenticación abandone la interfaz ASA (desde donde se puede acceder al servidor). Confirme que los dispositivos en la trayectoria no bloqueen el puerto UDP 1645 (puerto de autenticación RADIUS predeterminado) para asegurarse de que llegue al servidor NPS. Se puede encontrar más información sobre las capturas de paquetes en el ASA en ASA/PIX/FWSM: Ejemplo de Captura de Paquetes con CLI y Configuración de ASDM.
- Si la autenticación aún falla, mire en el visor de eventos en el NPS de Windows. En Visor de eventos > Registros de Windows, elija **Seguridad.** Busque eventos asociados con NPS alrededor del momento de la solicitud de autenticación.



Una vez abiertas las propiedades del evento, debe poder ver el motivo del error, como se muestra en el ejemplo. En este ejemplo, PAP no se eligió como el tipo de autenticación en la política de red. Por lo tanto, la solicitud de autenticación falla.

```
 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.**