Exemple de configuration de l'authentification d'utilisateur VPN ASA contre Windows 2008 NPS Server (Active Directory) avec RADIUS

Contenu

Introduction

Ce document explique comment configurer un dispositif de sécurité adaptatif (ASA) pour communiquer avec un serveur NPS (Network Policy Server) Microsoft Windows 2008 avec le protocole RADIUS de sorte que les anciens utilisateurs de Cisco VPN Client/AnyConnect/Clientless WebVPN soient authentifiés contre Active Directory. NPS est l'un des rôles de serveur proposés par Windows 2008 Server. Il est équivalent à Windows 2003 Server, IAS (Internet Authentication Service), qui est l'implémentation d'un serveur RADIUS pour fournir une authentification d'utilisateur à distance par accès commuté. De même, dans Windows 2008 Server, NPS est la mise en oeuvre d'un serveur RADIUS. En gros, l'ASA est un client RADIUS vers un serveur RADIUS NPS. ASA envoie des requêtes d'authentification RADIUS au nom des utilisateurs VPN et NPS les authentifie contre Active Directory.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

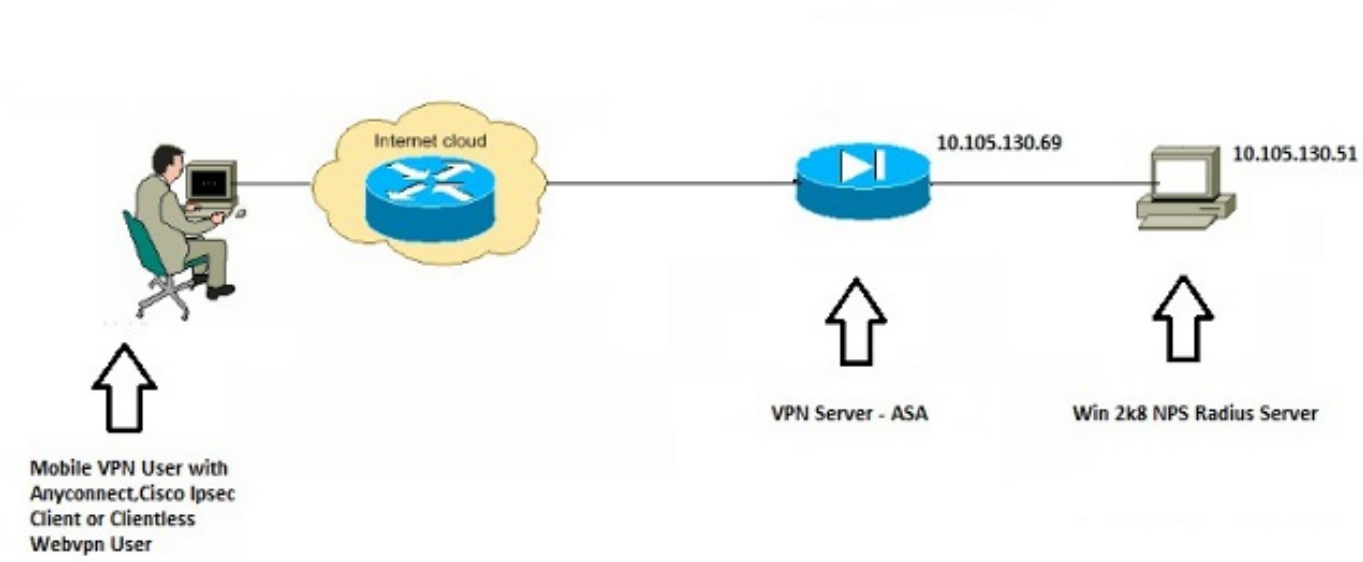
- ASA qui exécute la version 9.1(4)
- Windows 2008 R2 Server avec services Active Directory et rôle NPS installés

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.

Configuration

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

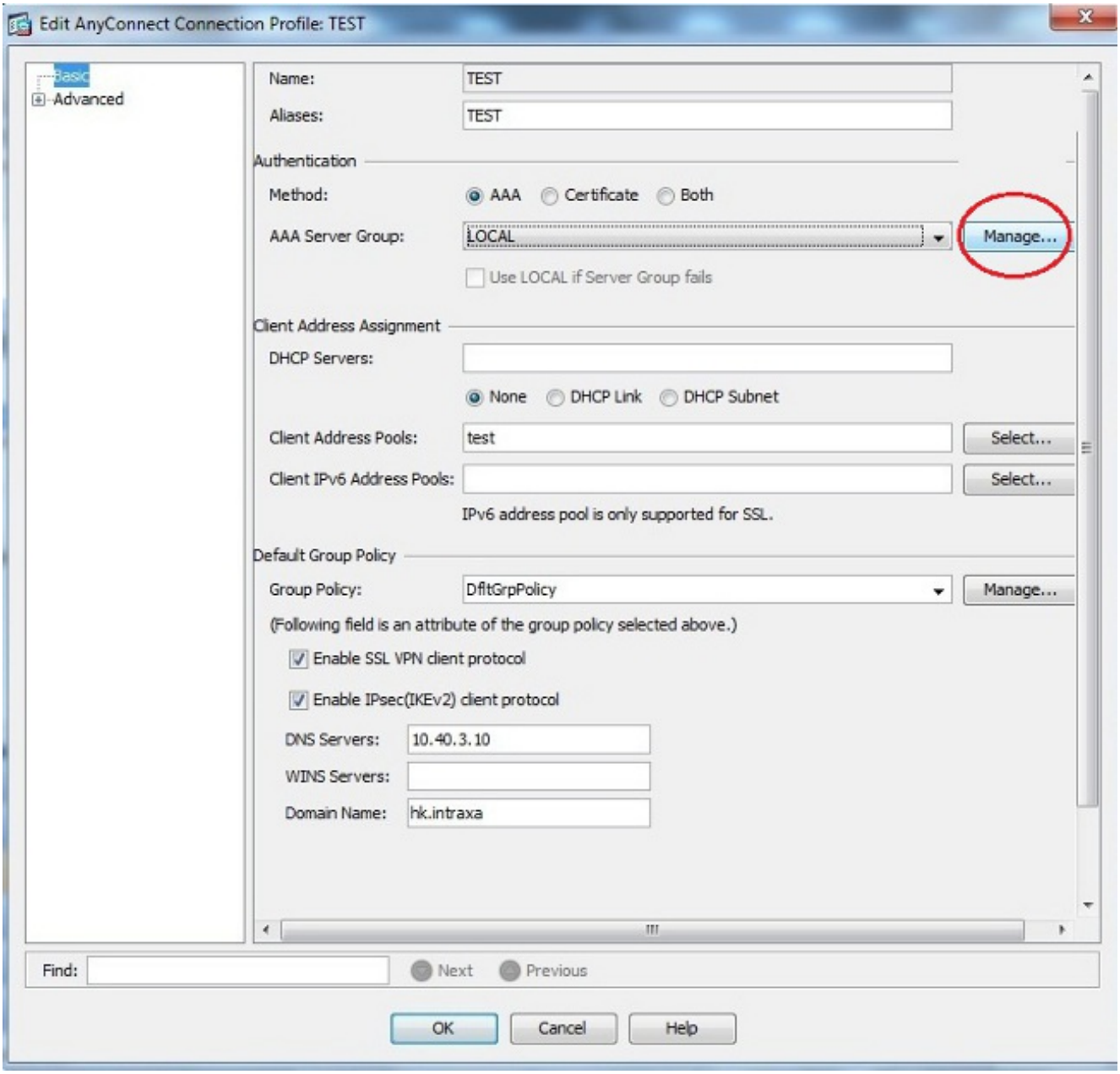
Diagramme du réseau



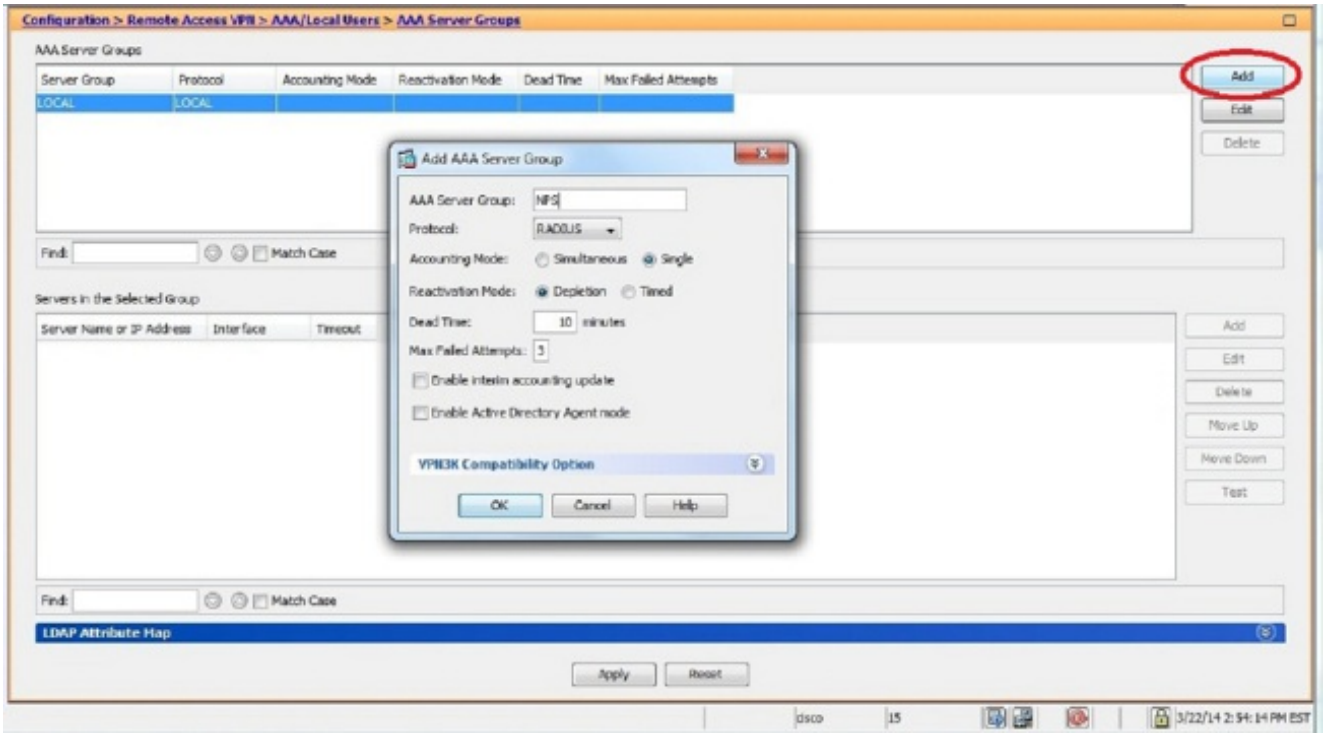
Configurations

Configuration ASDM

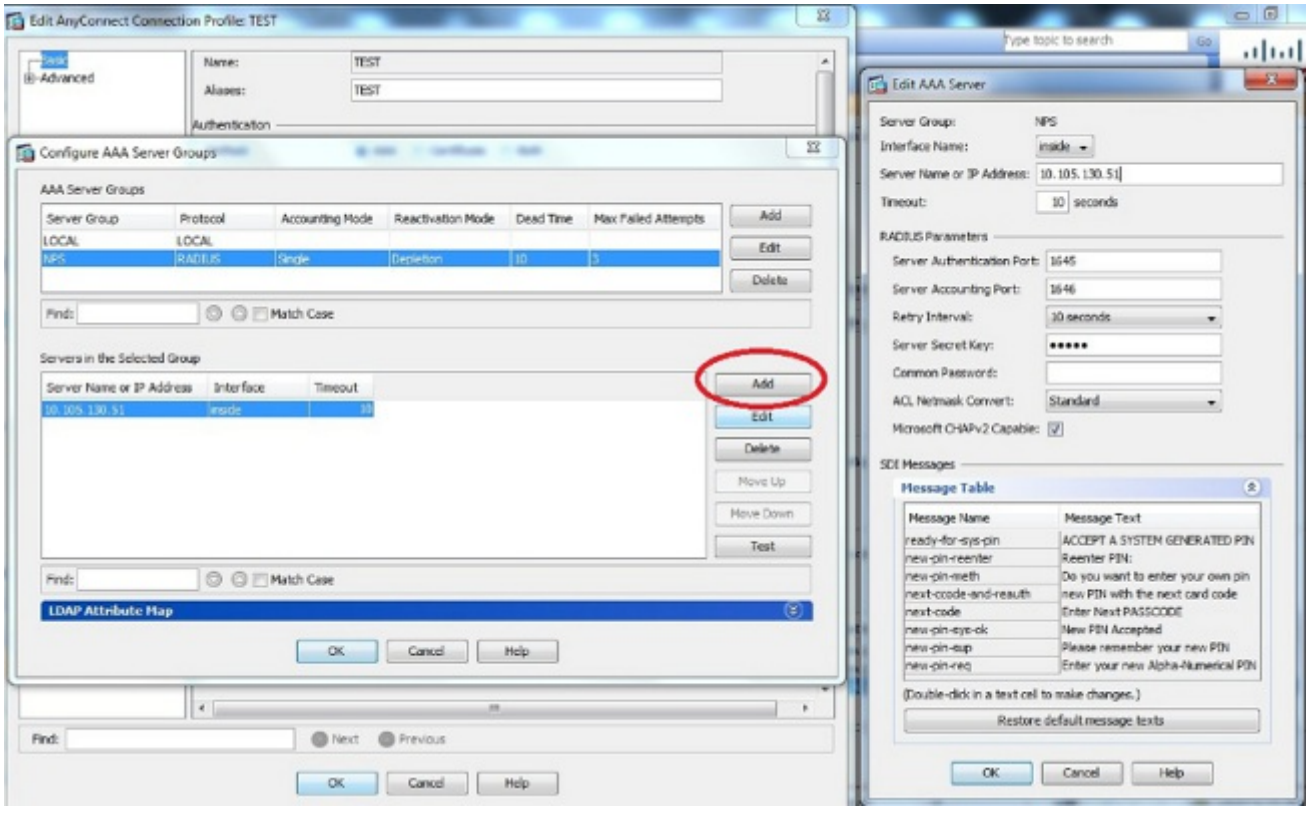
1. Sélectionnez le groupe de tunnels pour lequel l'authentification NPS est requise.
2. Cliquez sur **Modifier** et choisissez **Basic**.
3. Dans la section Authentification, cliquez sur **Gérer**.



4. Dans la section AAA Server Groups, cliquez sur **Add**.
5. Dans le champ AAA Server Group, saisissez le nom du groupe de serveurs (par exemple, NPS).
6. Dans la liste déroulante Protocole, sélectionnez **RADIUS**.
7. Click
   OK.

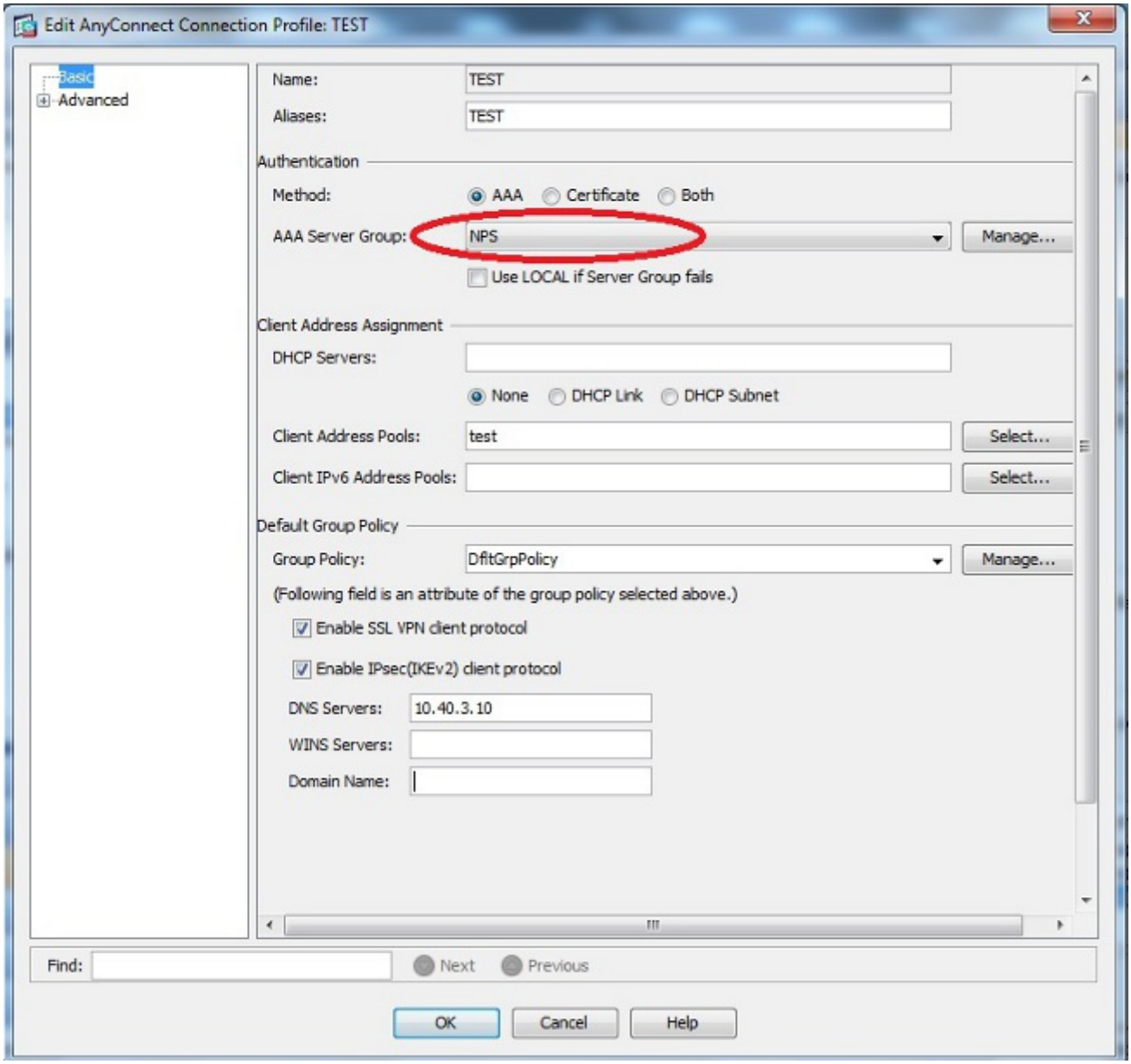


8. Dans la section Serveurs du groupe sélectionné, sélectionnez le groupe de serveurs AAA ajouté et cliquez sur **Ajouter**.
9. Dans le champ Server Name ou IP Address, saisissez l'adresse IP du serveur.
10. Dans le champ Server Secret Key, saisissez la clé secrète.
11. Laissez les champs Port d'authentification du serveur et Port de comptabilité du serveur à la valeur par défaut, sauf si le serveur écoute sur un autre port.
12. Click OK.
13. Click
    OK.



14. Dans la liste déroulante Groupe de serveurs AAA, sélectionnez le groupe (NPS dans cet exemple) ajouté aux étapes précédentes.
15. Click

OK.



Configuration 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
```

Par défaut, l'ASA utilise le type d'authentification PAP (Password Authentication Protocol) non chiffré. Cela ne signifie pas que l'ASA envoie le mot de passe en texte clair lorsqu'il envoie le paquet RADIUS REQUEST. Au contraire, le mot de passe en clair est chiffré avec le secret partagé RADIUS.

Si la gestion des mots de passe est activée sous le groupe de tunnels, ASA utilise le type d'authentification MSCHAP-v2 afin de chiffrer le mot de passe en clair. Dans ce cas, assurez-vous que la case **Microsoft CHAPv2 Capable** est cochée dans la fenêtre Edit AAA Server configurée dans la section de configuration ASDM.

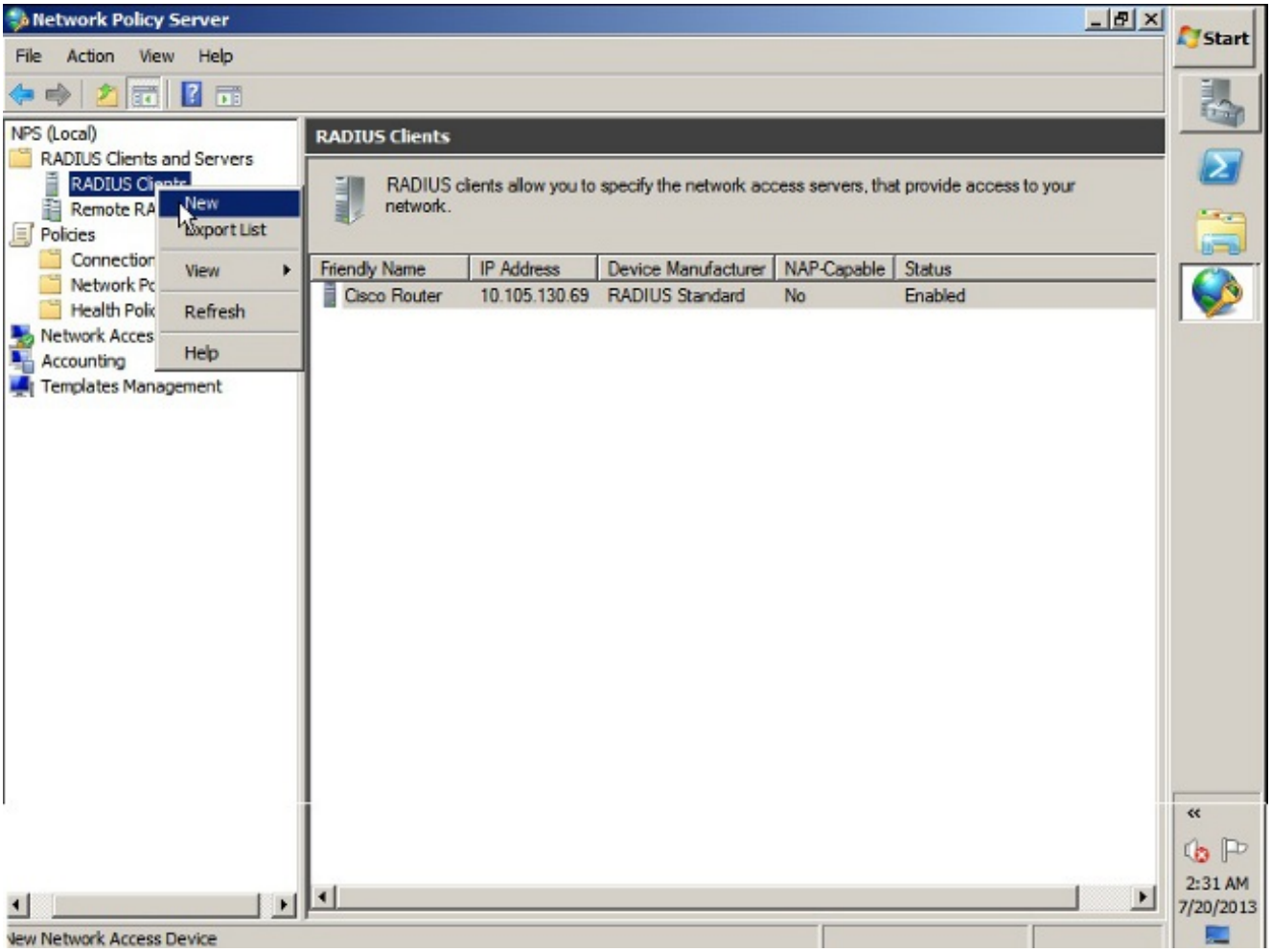
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **Note**: La commande **test aaa-server authentication** utilise toujours PAP. Ce n'est que lorsqu'un utilisateur lance une connexion à tunnel-group avec la gestion des mots de passe activée que l'ASA utilise MSCHAP-v2. En outre, l'option 'password-management [password-expire-in-days]' n'est prise en charge que par le protocole LDAP (Lightweight Directory Access Protocol). RADIUS ne fournit pas cette fonctionnalité. L'option password expire s'affiche lorsque le mot de passe a déjà expiré dans Active Directory.

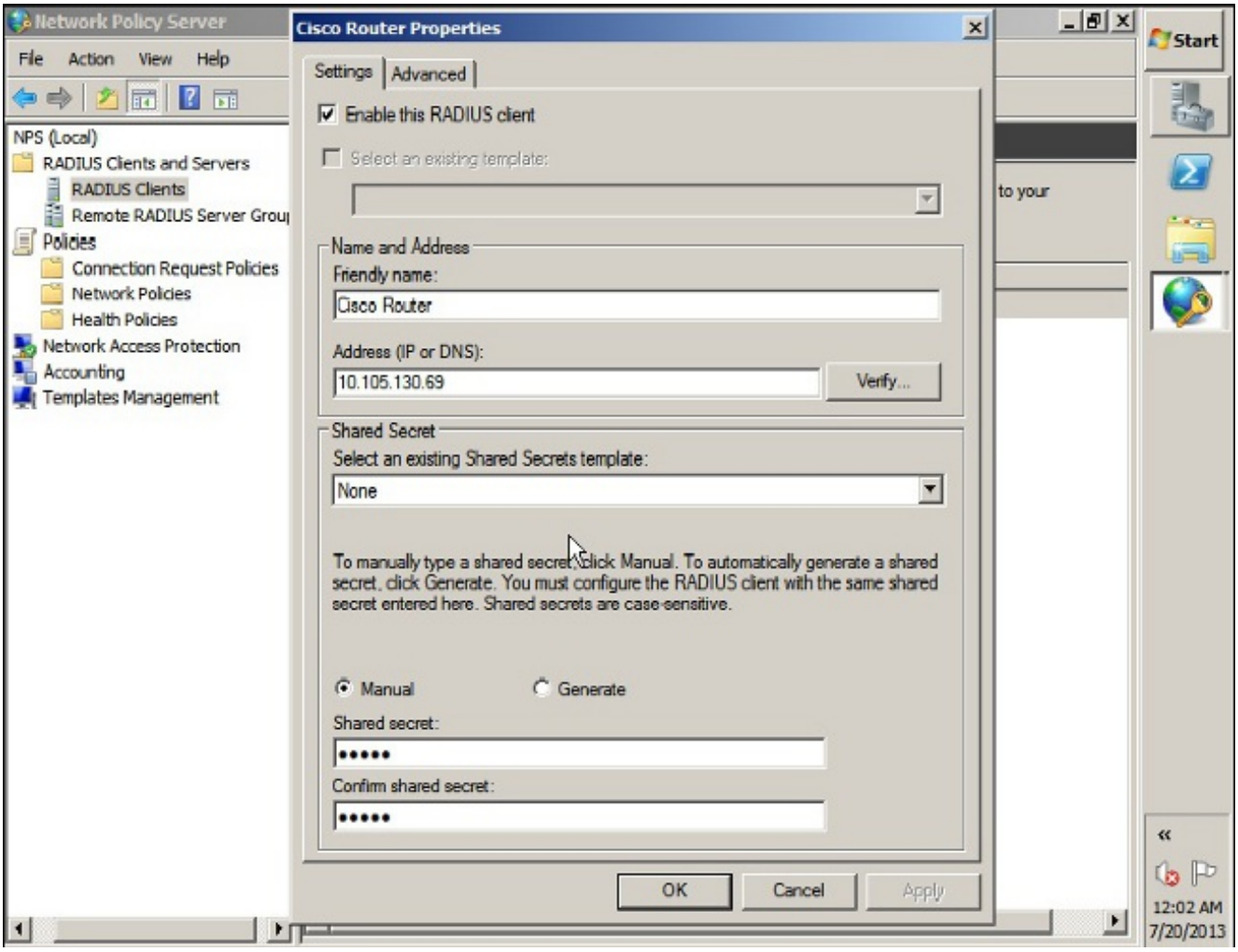
Configuration de Windows 2008 Server avec NPS

Le rôle serveur NPS doit être installé et exécuté sur le serveur Windows 2008. Sinon, sélectionnez **Démarrer > Outils d'administration > Rôles serveur > Ajouter des services de rôle**. Sélectionnez Network Policy Server et installez le logiciel. Une fois le rôle serveur NPS installé, complétez ces étapes afin de configurer le NPS pour accepter et traiter les demandes d'authentification RADIUS de l'ASA :

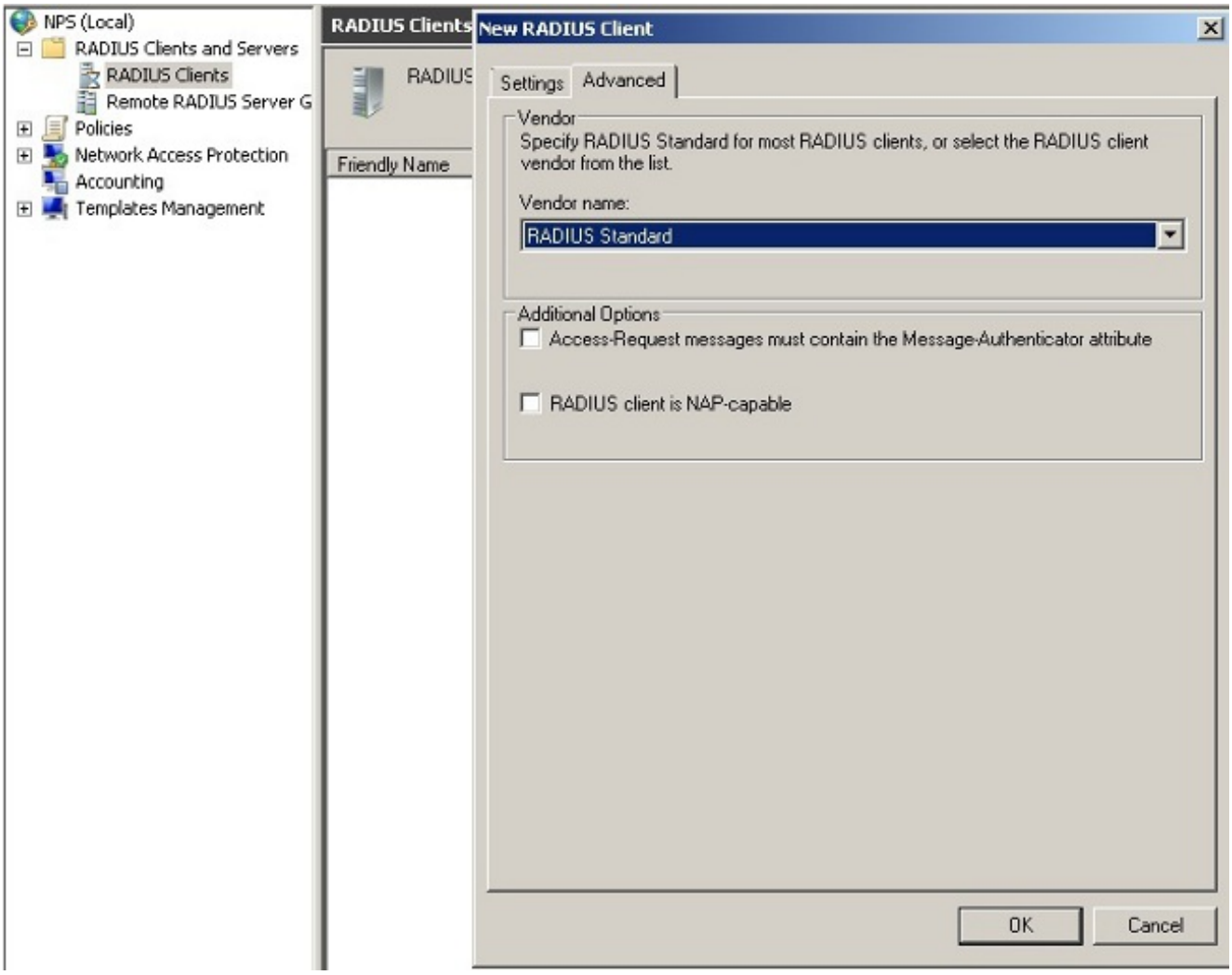
1. Ajoutez l'ASA en tant que client RADIUS dans le serveur NPS. Choisissez **Outils d'administration > Serveur de stratégie réseau.**Cliquez avec le bouton droit sur **Clients RADIUS** et sélectionnez
   Nouveau.



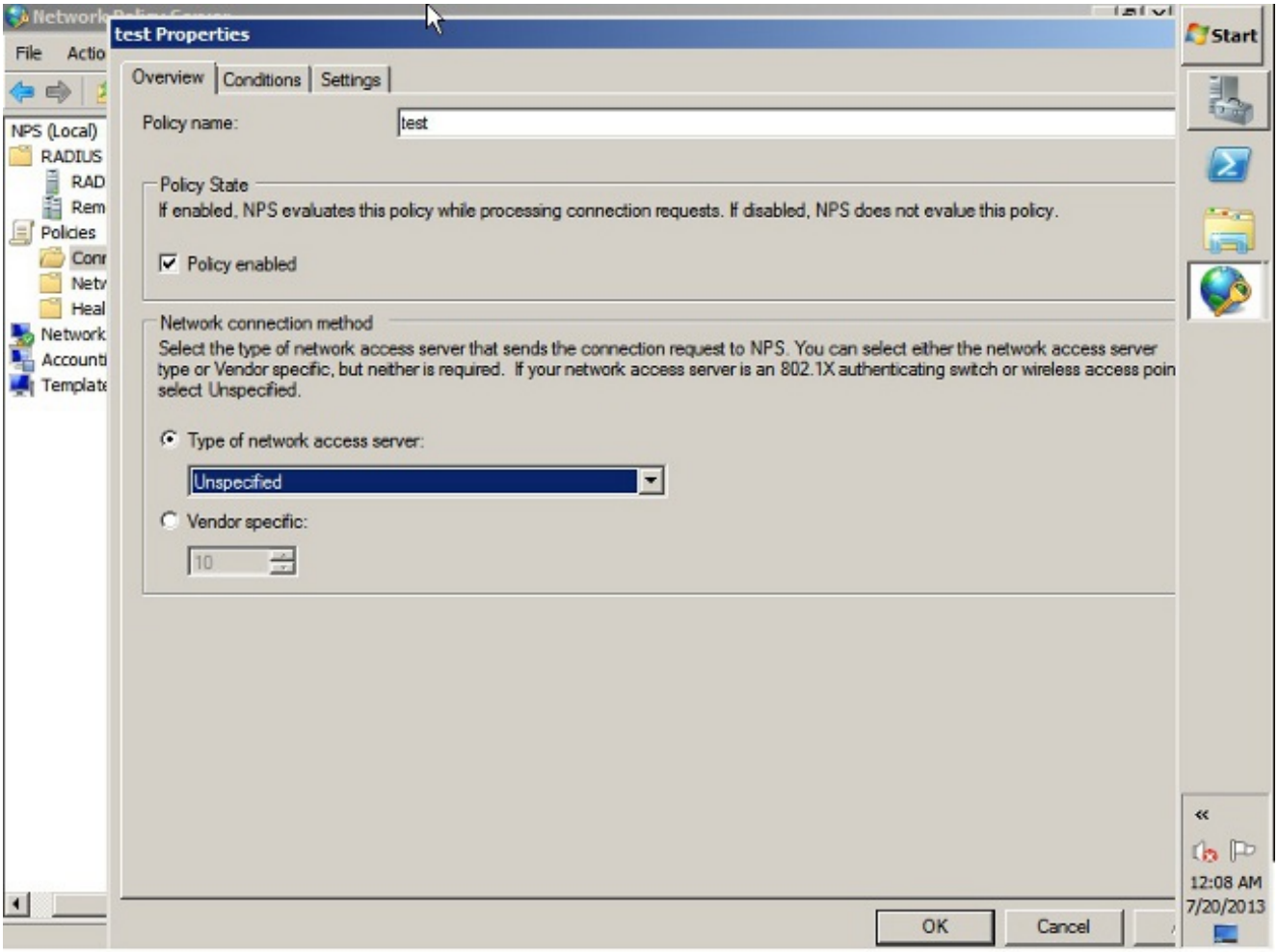
Saisissez un nom convivial, une adresse (IP ou DNS) et un secret partagé configurés sur l'ASA.



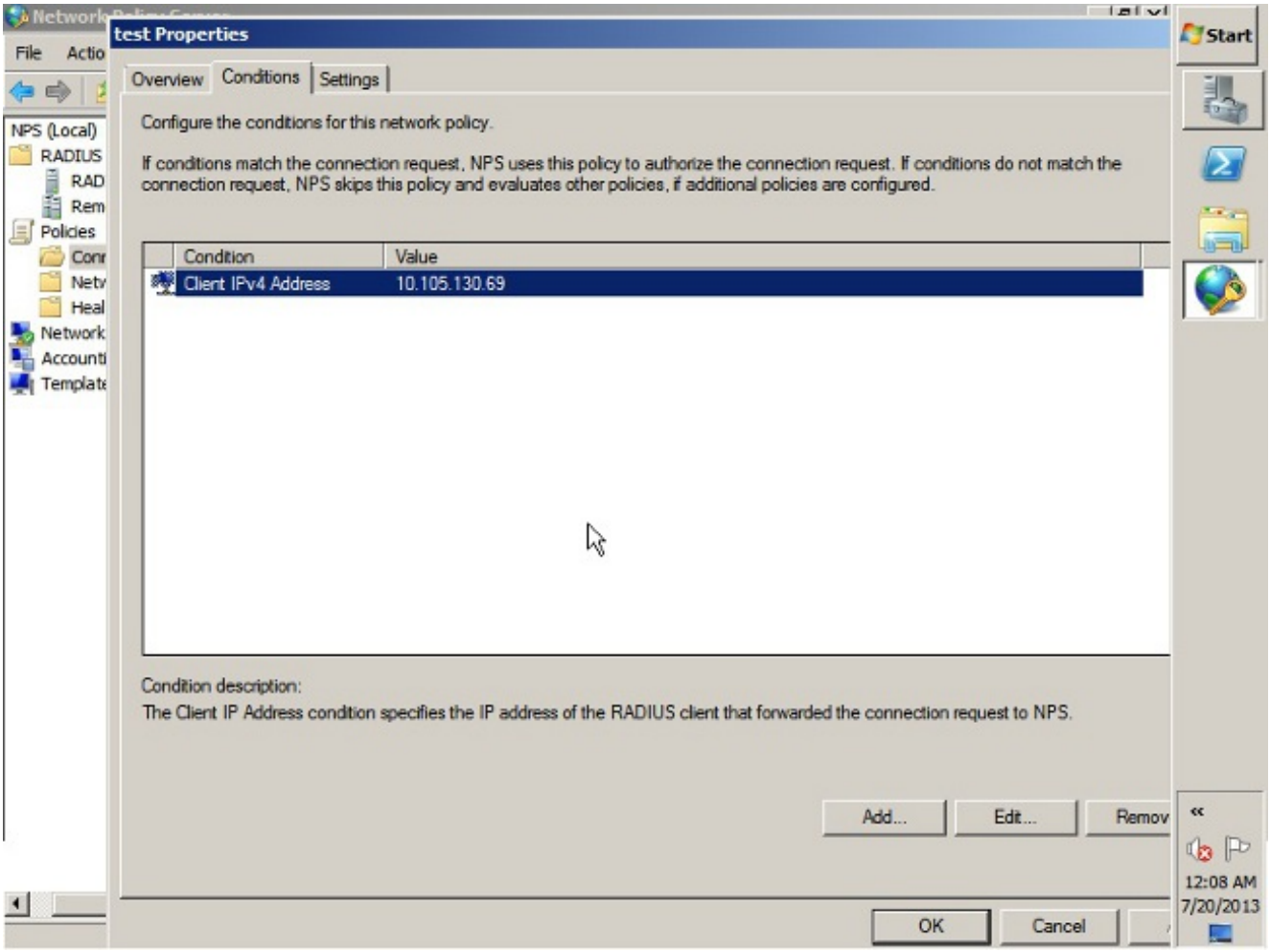
Cliquez sur l'onglet **Advanced.**Dans la liste déroulante Nom du fournisseur, sélectionnez **RADIUS Standard**.Click
OK.



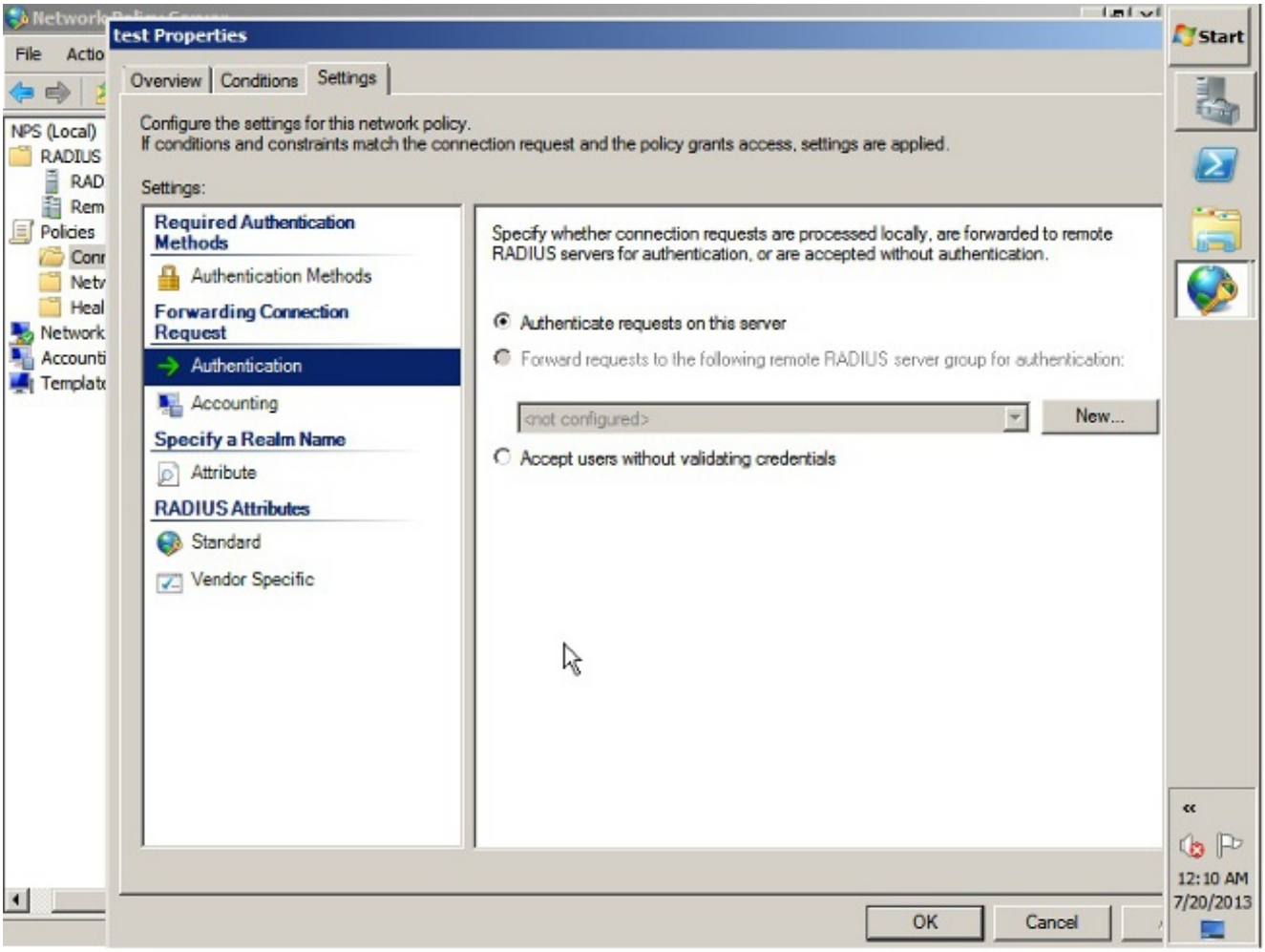
2. Créez une nouvelle stratégie de demande de connexion pour les utilisateurs VPN. L'objectif de la stratégie de demande de connexion est de spécifier si les demandes des clients RADIUS doivent être traitées localement ou transférées vers des serveurs RADIUS distants. Sous NPS > Policies, cliquez avec le bouton droit sur **Connection Request Policies** et créez une nouvelle stratégie.Dans la liste déroulante Type de serveur d'accès au réseau, sélectionnez **Non spécifié**.



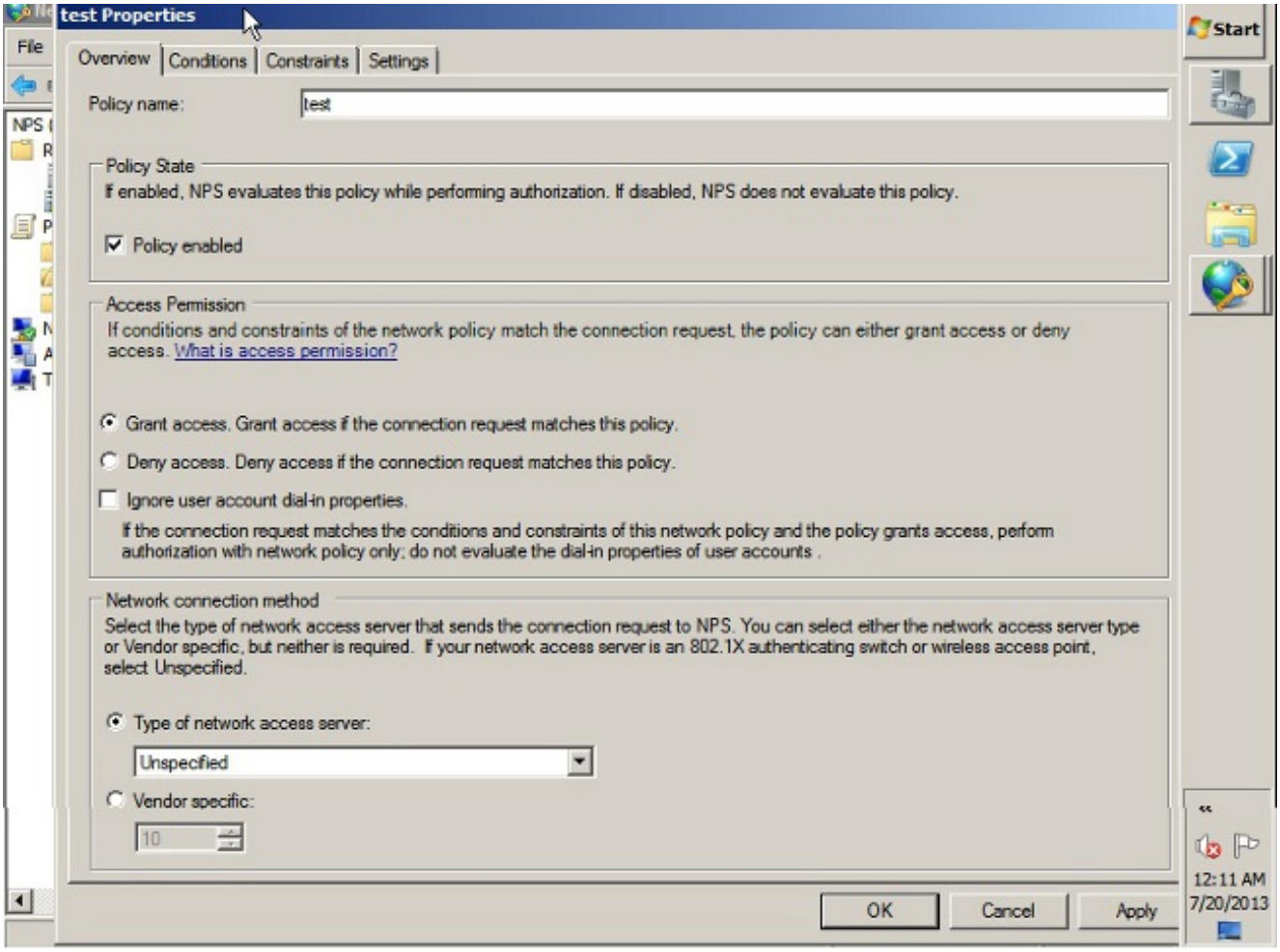
Cliquez sur l'onglet **Conditions**.Cliquez sur **Add**.Saisissez l'adresse IP de l'ASA comme condition 'Adresse IPv4 du
client'.



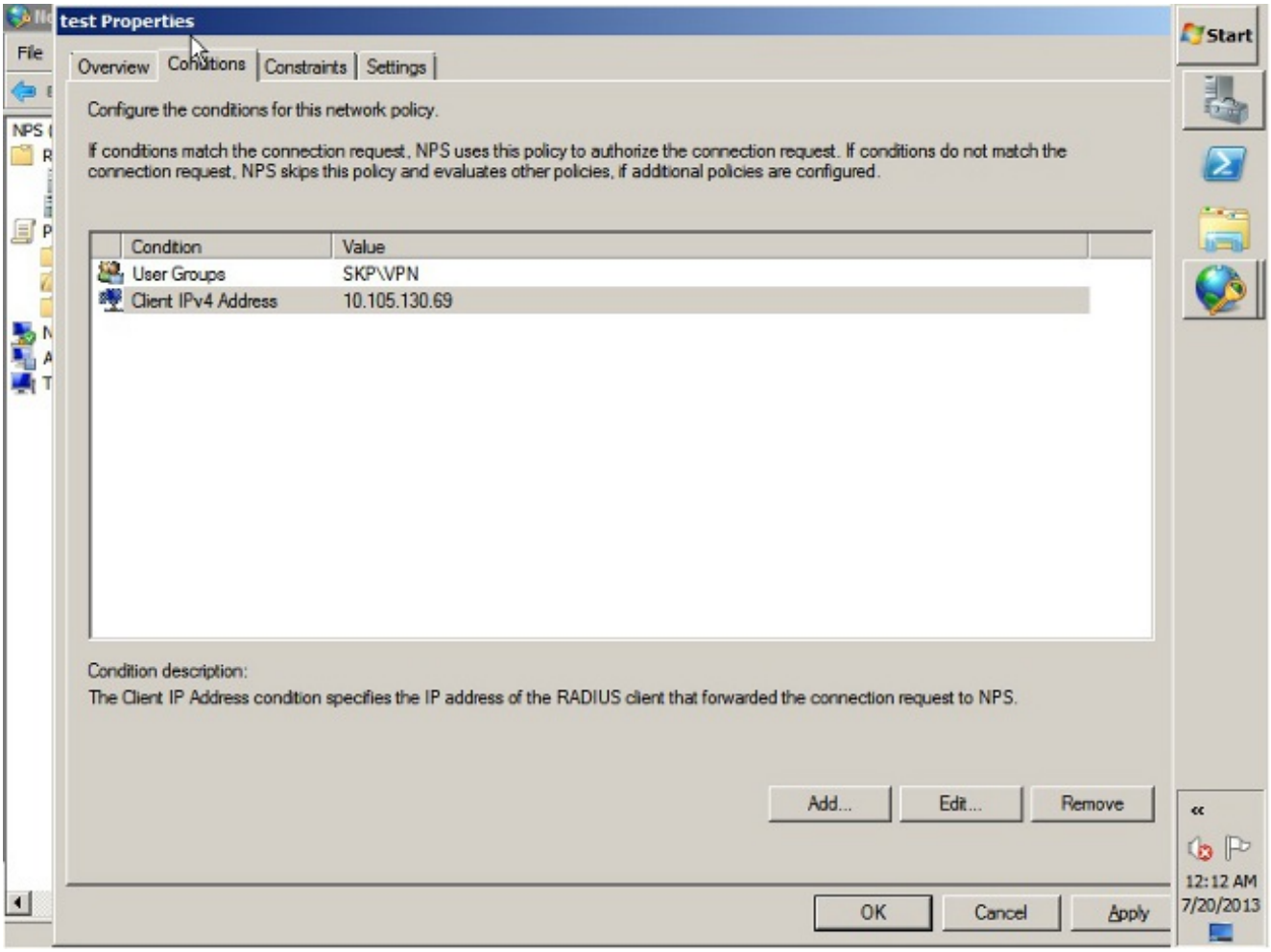
Cliquez sur l'onglet **Paramètres**.Sous Forwarding Connection Request, sélectionnez **Authentication**. Assurez-vous que la case d'option Authentifier les demandes sur ce serveur est sélectionnée.Click
OK.



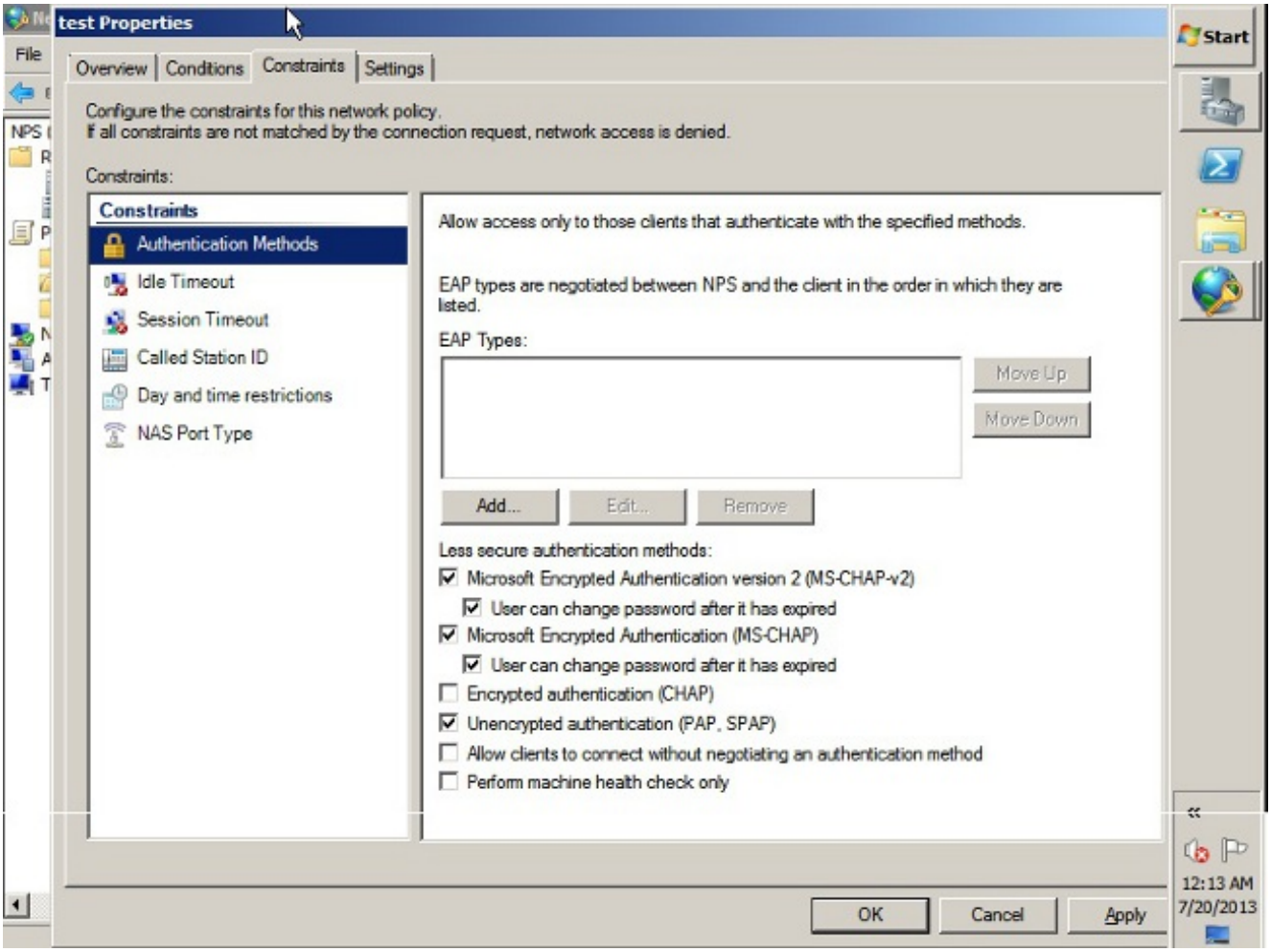
3. Ajoutez une stratégie réseau dans laquelle vous pouvez spécifier les utilisateurs autorisés à s'authentifier.Par exemple, vous pouvez ajouter des groupes d'utilisateurs Active Directory en tant que condition. Seuls les utilisateurs appartenant à un groupe Windows spécifié sont authentifiés en vertu de cette stratégie.Sous NPS, sélectionnez **Stratégies**.Cliquez avec le bouton droit sur **Stratégie réseau** et créez une nouvelle stratégie.Assurez-vous que la case d'option Accorder l'accès est sélectionnée.Dans la liste déroulante Type de serveur d'accès au réseau, sélectionnez **Non spécifié**.



Cliquez sur l'onglet **Conditions**.Cliquez sur **Add**.Saisissez l'adresse IP de l'ASA en tant que condition d'adresse IPv4 du client.Entrez le groupe d'utilisateurs Active Directory qui contient les utilisateurs
VPN.



Cliquez sur l'onglet **Contraintes**.Choisissez **Méthodes d'authentification**.Vérifiez que la case Authentification non chiffrée (PAP, SPAP) est cochée.Click
OK.

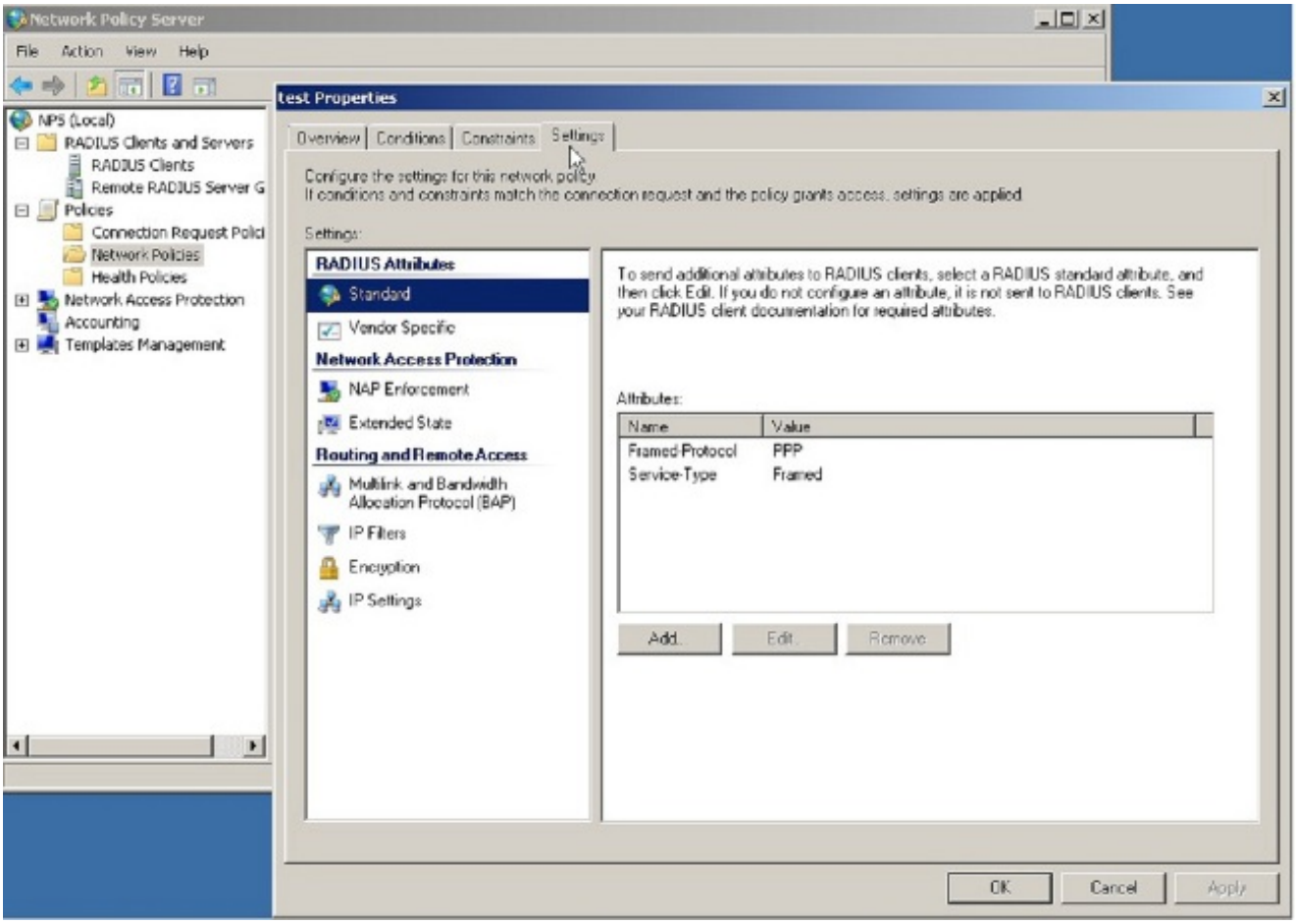


Attribut Pass Group-policy (Attribut 25) du serveur RADIUS NPS

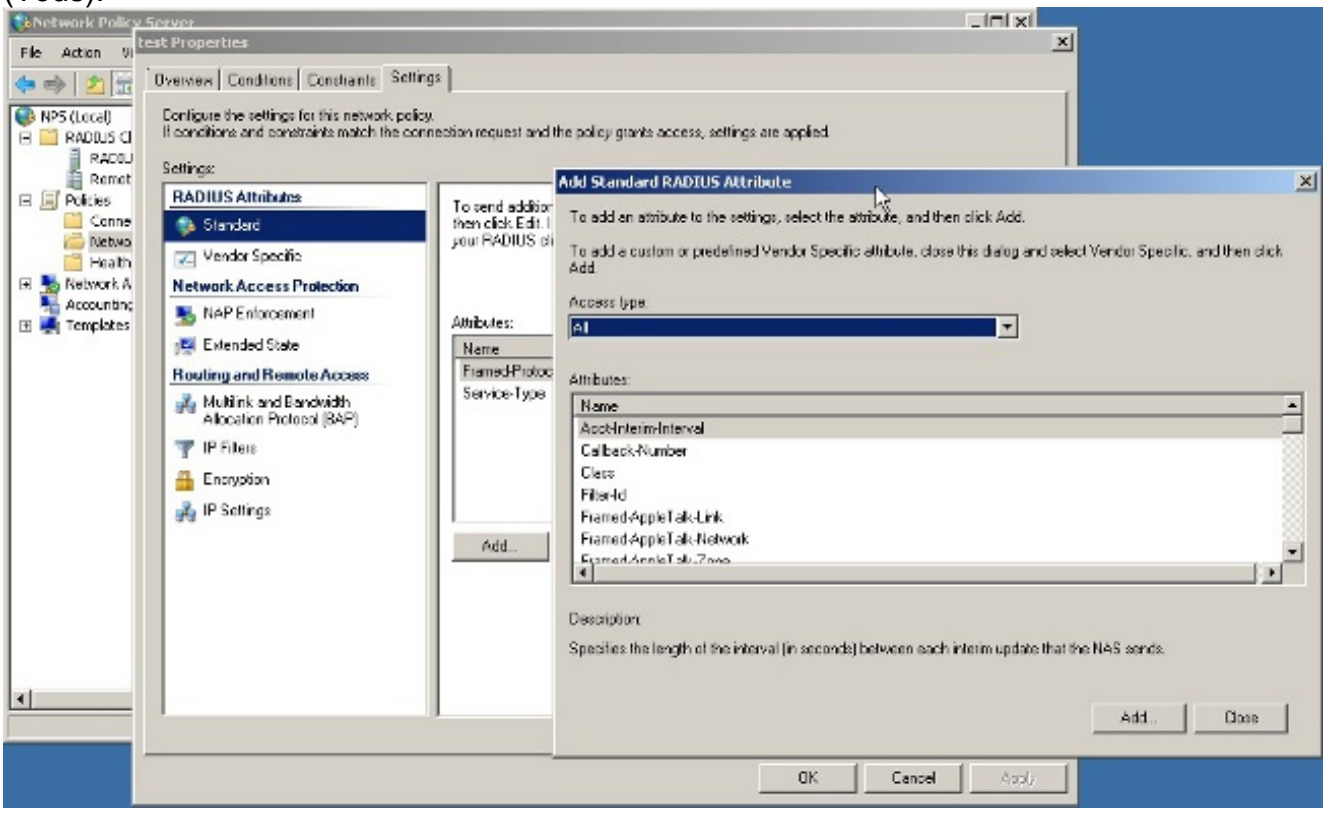
Si la stratégie de groupe doit être attribuée à l'utilisateur de manière dynamique avec le serveur RADIUS NPS, l'attribut RADIUS de stratégie de groupe (attribut 25) peut être utilisé.

Complétez ces étapes afin d'envoyer l'attribut RADIUS 25 pour l'attribution dynamique d'une stratégie de groupe à l'utilisateur.

1. Une fois la stratégie réseau ajoutée, cliquez avec le bouton droit sur la stratégie réseau requise et cliquez sur l'onglet
   Paramètres.

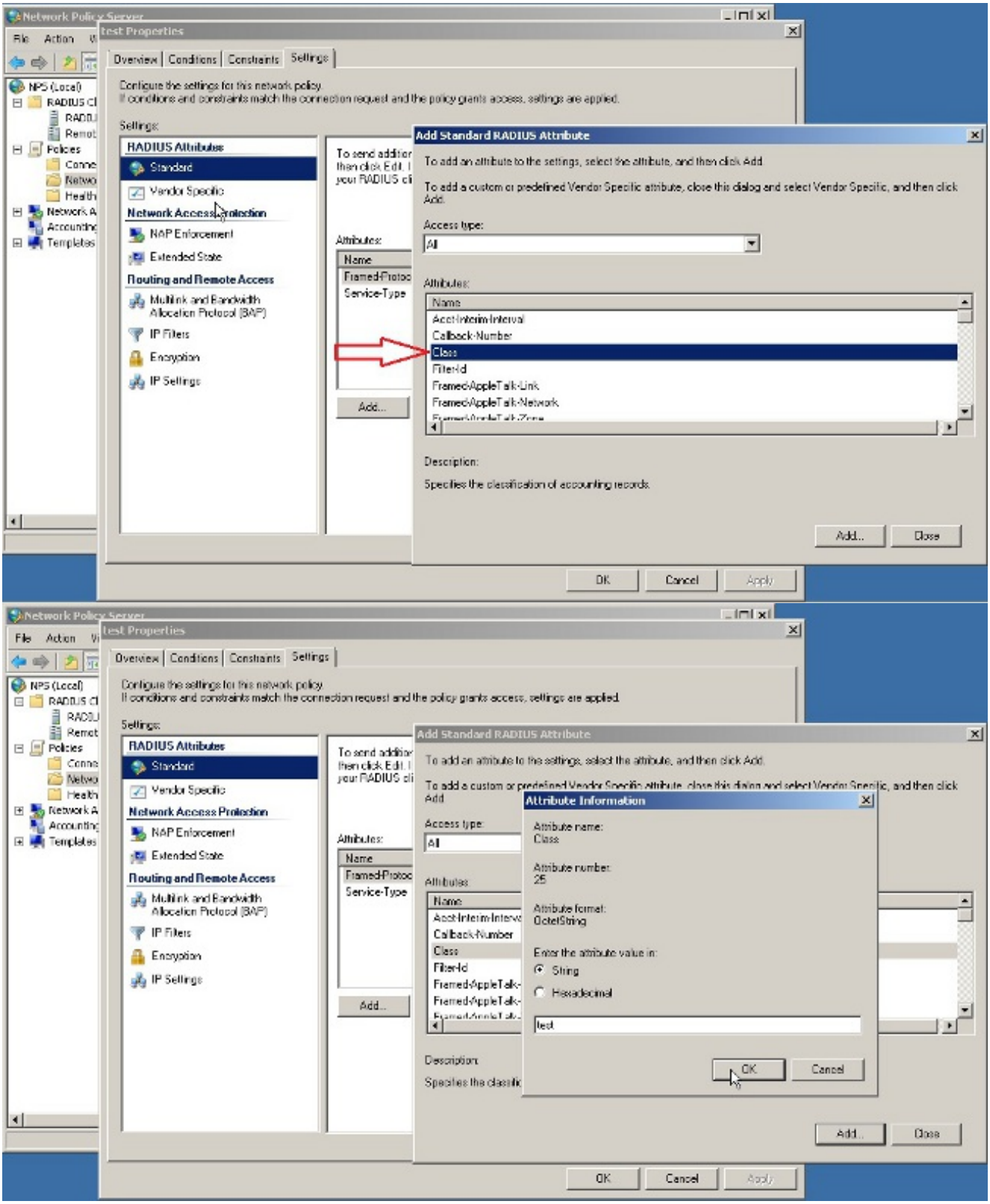


2. Choisissez **Attributs RADIUS > Standard**. Cliquez sur **Add**. Laissez le type Access comme All
(Tous).



3. Dans la zone Attributs, sélectionnez **Classe** et cliquez sur **Ajouter**. Entrez la valeur d'attribut, c'est-à-dire le nom de la stratégie de groupe sous la forme d'une chaîne. N'oubliez pas qu'une stratégie de groupe portant ce nom doit être configurée dans l'ASA. Cela signifie que l'ASA l'attribue à la session VPN après avoir reçu cet attribut dans la réponse

RADIUS.



Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Débogage de l'ASA

Activez **debug radius all** sur l'ASA.

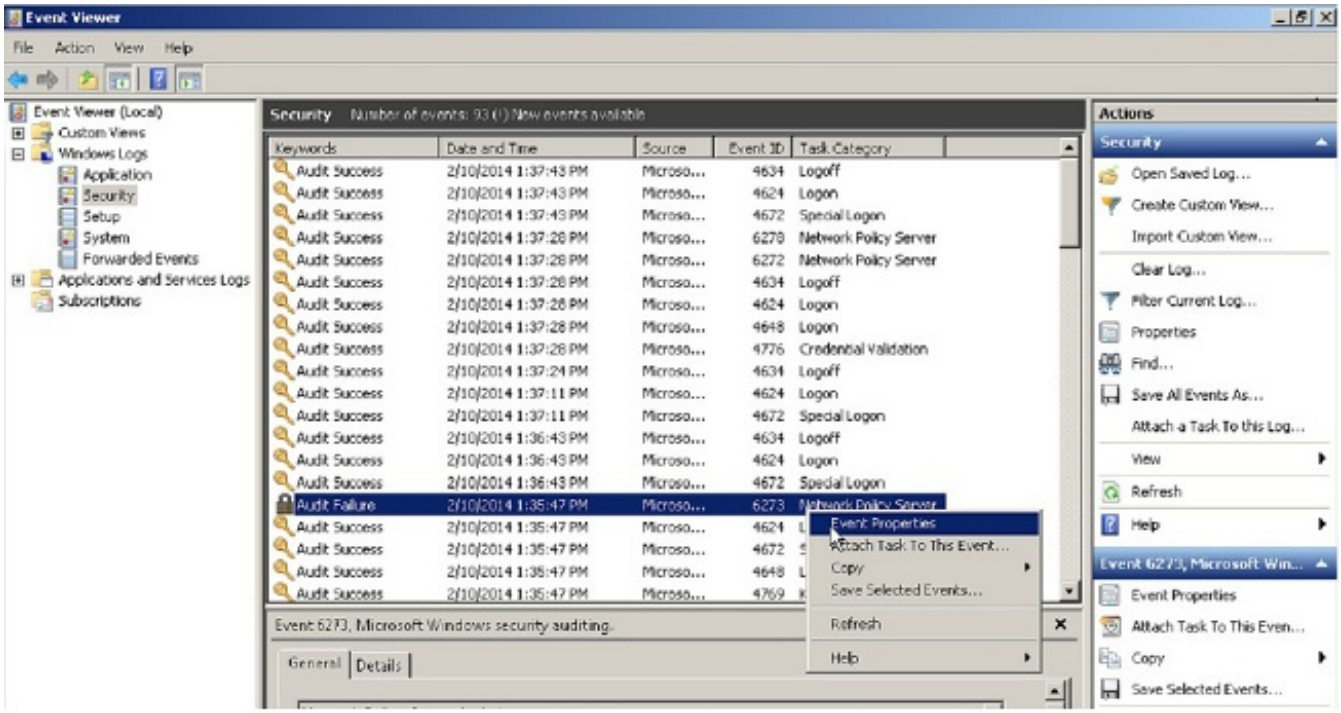
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Assurez-vous que la connectivité entre l'ASA et le serveur NPS est bonne.Appliquer des captures de paquets pour s'assurer que la demande d'authentification quitte l'interface ASA (à partir de laquelle le serveur est accessible). Vérifiez que les périphériques du chemin ne bloquent pas le port UDP 1645 (port d'authentification RADIUS par défaut) afin de s'assurer qu'il atteint le serveur NPS. Plus d'informations sur les captures de paquets sur l'ASA sont disponibles dans ASA/PIX/FWSM : Exemple de configuration de capture de paquets CLI et ASDM.
- Si l'authentification échoue toujours, recherchez l'observateur d'événements dans la fenêtre NPS. Sous Observateur d'événements > Journaux Windows, sélectionnez **Sécurité.** Recherchez les événements associés à NPS au moment de la demande d'authentification.



Une fois que vous avez ouvert Event Properties, vous devriez voir la raison de l'échec comme indiqué dans l'exemple. Dans cet exemple, PAP n'a pas été choisi comme type d'authentification dans la stratégie de réseau. Par conséquent, la demande d'authentification échoue.

```
 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.
```