RADIUS を使用した Windows 2008 NPS サーバ（Active Directory）に対する ASA VPN ユーザ認証の設定例

内容

概要

このドキュメントでは、RADIUS プロトコルを使用して Microsoft Windows 2008 Network Policy Server（NPS）と通信するように適応型セキュリティ アプライアンス（ASA）を設定する方法を説明します。これにより、レガシー Cisco VPN Client/AnyConnect/Clientless WebVPN のユーザが Active Directory に対して認証されます。NPSは、Windows 2008 Serverが提供するサーバーの役割の1つです。これは、リモートダイヤルインユーザ認証を提供するためのRADIUSサーバの実装であるWindows 2003 Server, IAS(Internet Authentication Service)に相当します。同様に、Windows 2008 Serverでは、NPSはRADIUSサーバの実装です。基本的に、ASAはNPS RADIUSサーバへのRADIUSクライアントです。ASAはVPNユーザに代わってRADIUS認証要求を送信し、NPSはActive Directoryに対してそれらを認証します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

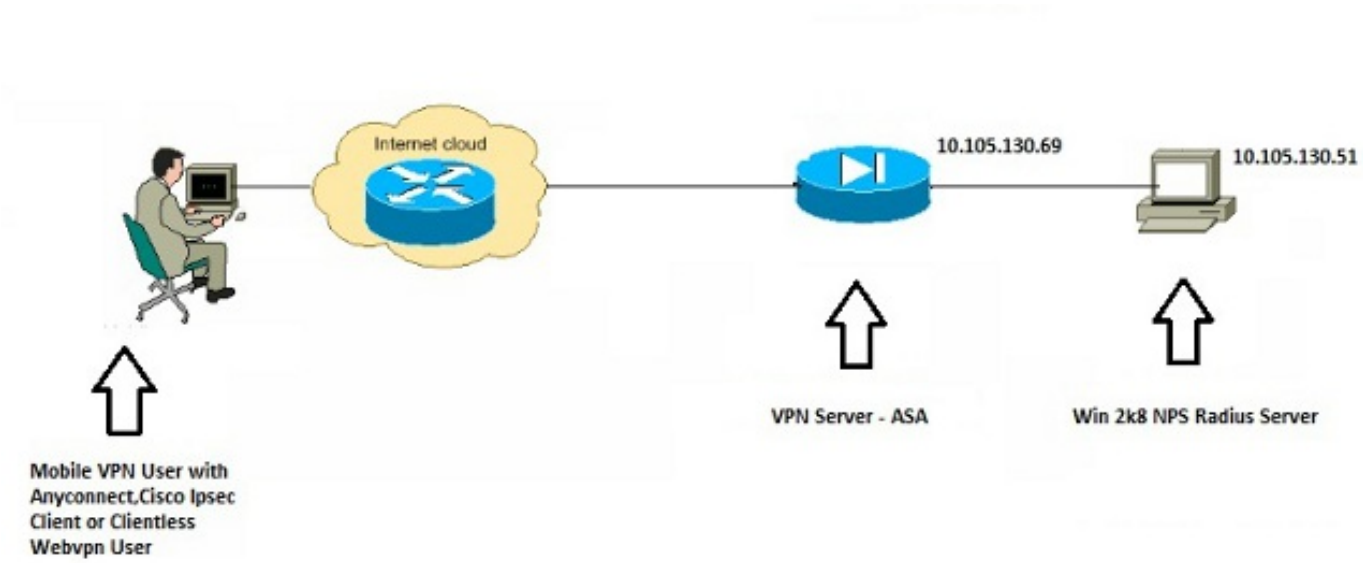
- バージョン9.1(4)が稼働するASA
- Active DirectoryサービスとNPSの役割がインストールされたWindows 2008 R2 Server

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

> **注：**このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

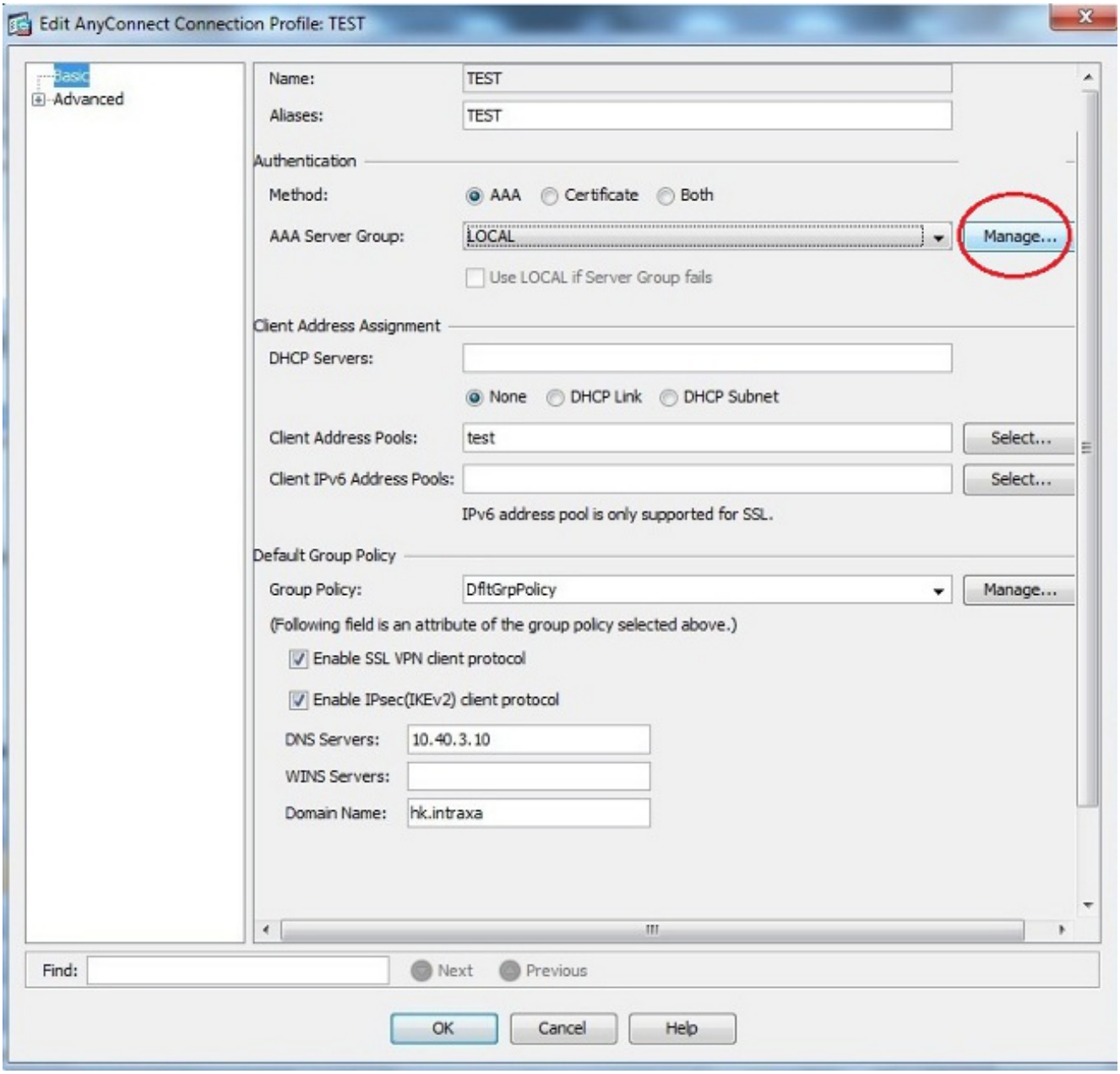
ネットワーク図



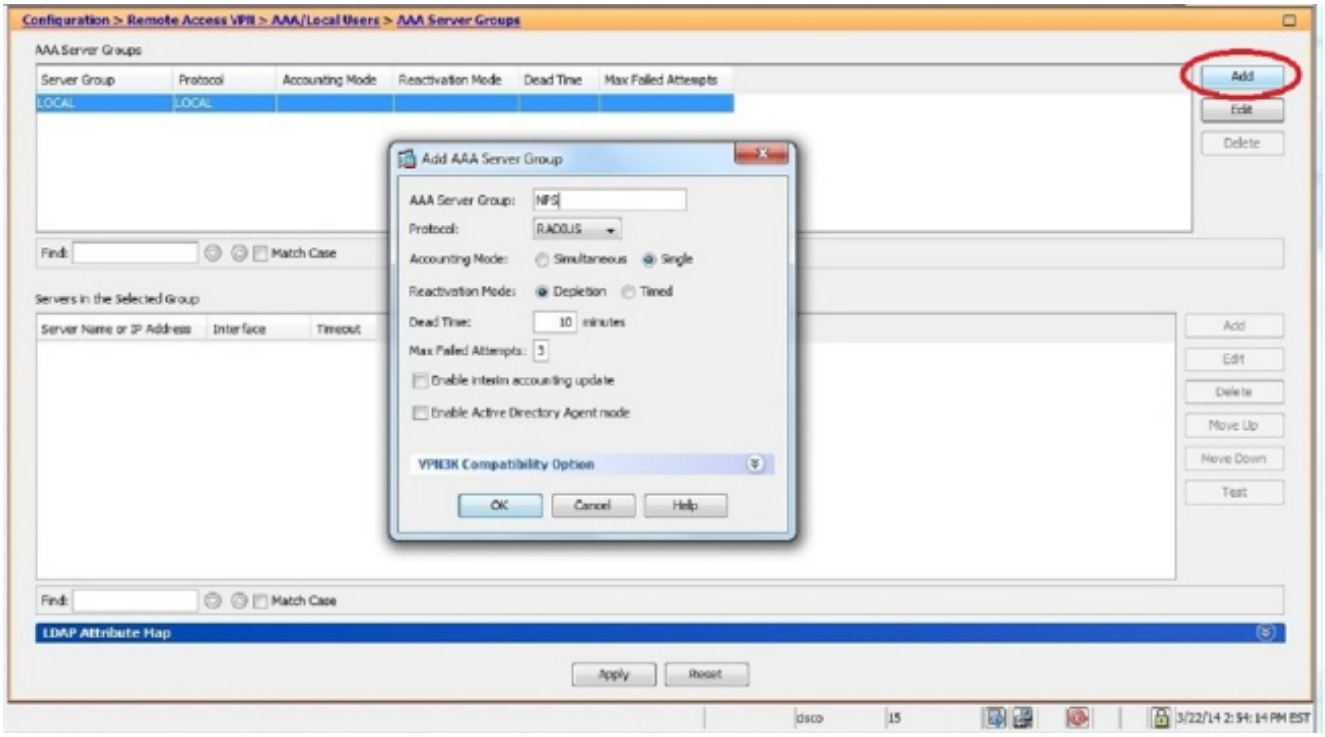
設定

ASDM の設定

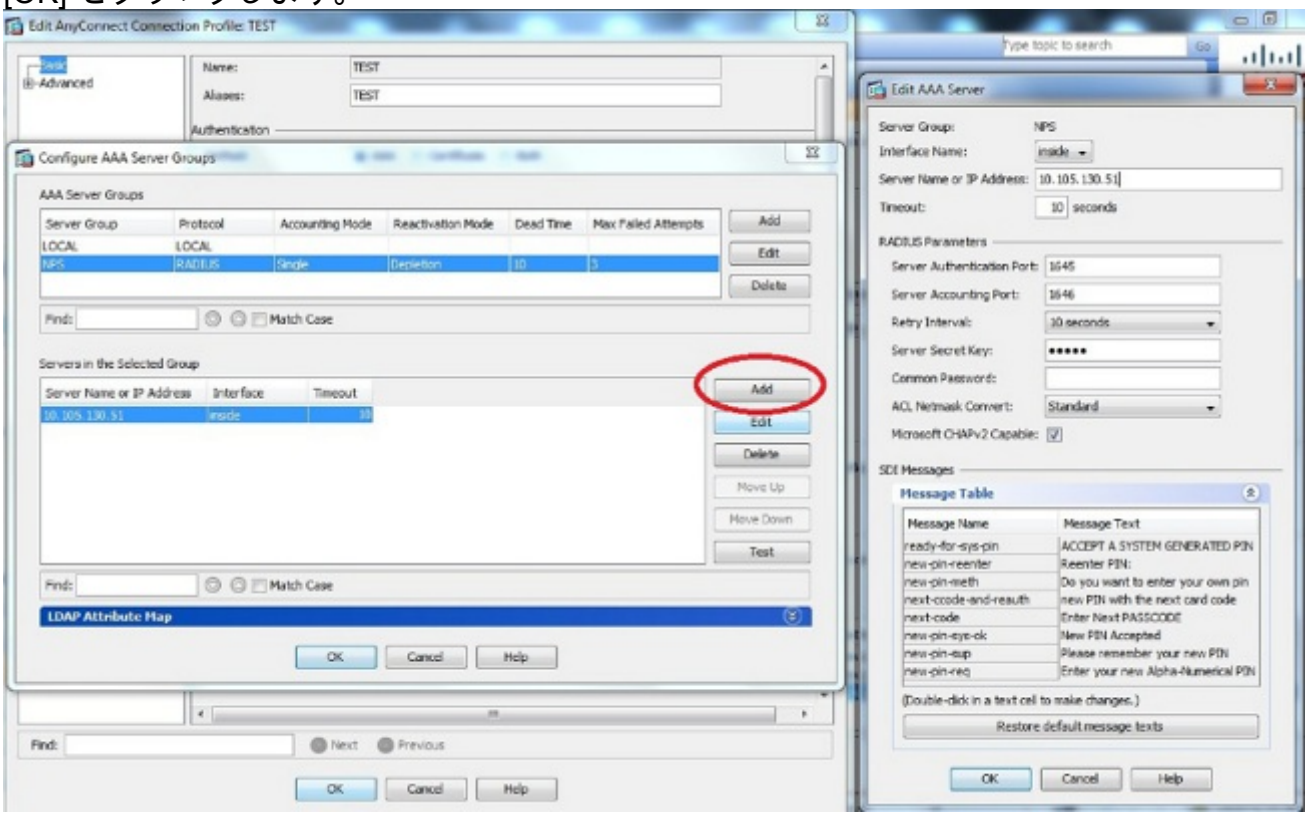
1. NPS認証が必要なトンネルグループを選択します。
2. [Edit]をクリックし、[Basic]を選択します。
3. [Authentication]セクションで、[Manage]をクリックします。



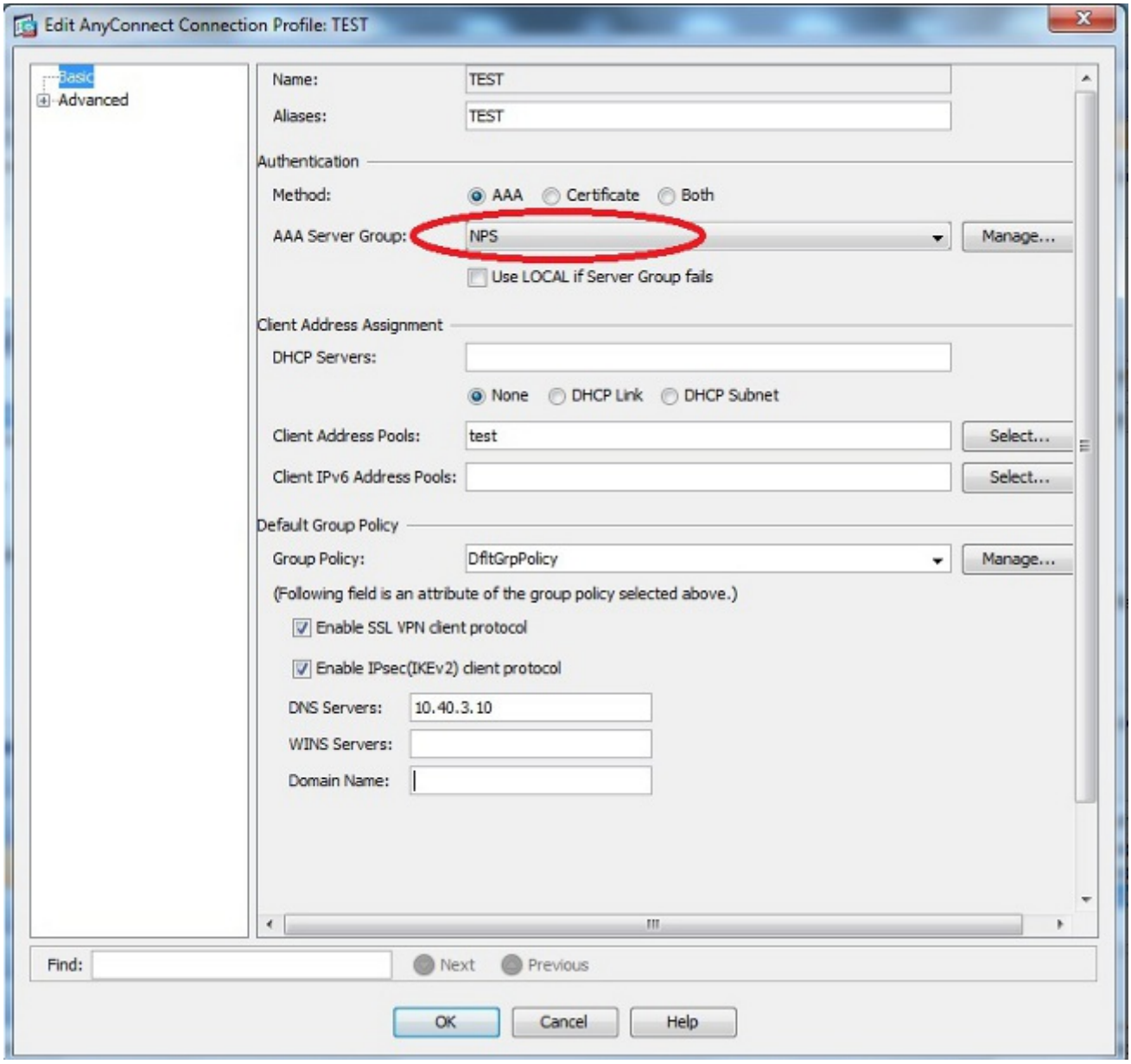
4. [AAA Server Groups]セクションで、[Add]をクリックします。
5. [AAA Server Group]フィールドに、サーバグループの名前（NPSなど）を入力します。
6. [プロトコル]ドロップダウンリストから、[RADIUS]を選択します。
7. [OK] をクリックします。



8. [Servers in the Selected Group]セクションで、追加したAAAサーバグループを選択し、[Add]をクリックします。
9. [Server Name or IP Address]フィールドに、サーバのIPアドレスを入力します。
10. [Server Secret Key]フィールドに秘密キーを入力します。
11. サーバが別のポートでリッスンしない限り、[Server Authentication Port]フィールドと[Server Accounting Port]フィールドはデフォルト値のままにします。
12. [OK] をクリックします。
13. [OK] をクリックします。



14. [AAA Server Group]ドロップダウンリストから、前の手順で追加したグループ（この例ではNPS）を選択します。
15. [OK] をクリックします。



CLI での設定

```
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
```

デフォルトでは、ASAは暗号化されていないパスワード認証プロトコル(PAP)認証タイプを使用します。これは、ASAがRADIUS REQUESTパケットを送信するときにプレーンテキストでパスワードを送信することを意味するものではありません。プレーンテキストのパスワードは、RADIUS共有秘密で暗号化されます。

トンネルグループでパスワード管理が有効になっている場合、ASAはプレーンテキストのパスワードを暗号化するためにMSCHAP-v2認証タイプを使用します。このような場合、ASDM設定セク

ションで設定した[Edit AAA Server]ウィンドウで**[Microsoft CHAPv2 Capable]**チェックボックスがオンになっていることを確認します。

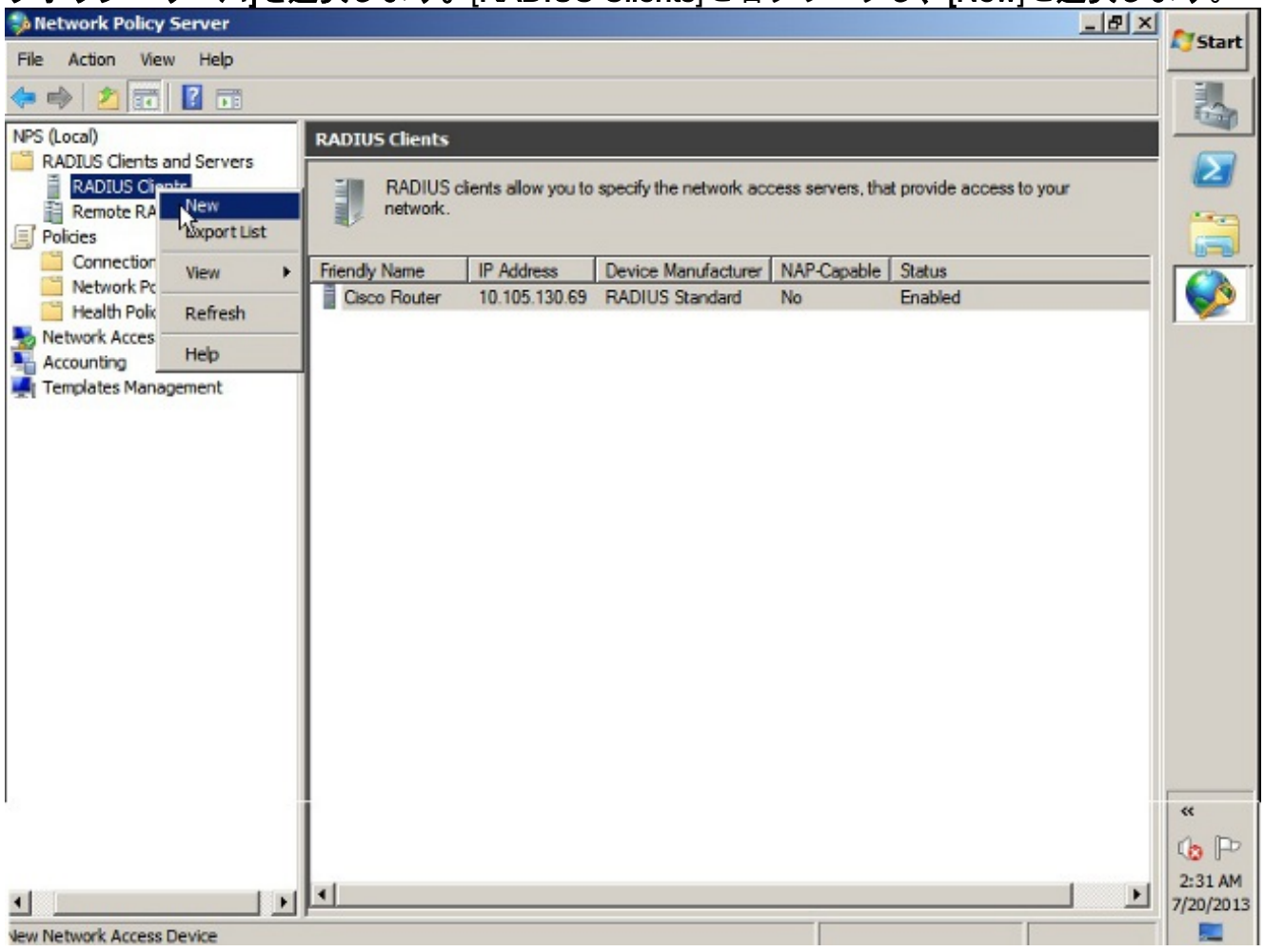
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **注：test aaa-server authenticationコマンドは、常にPAP**を使用します。ユーザがパスワード管理が有効なトンネルグループへの接続を開始した場合にのみ、ASAはMSCHAP-v2を使用します。また、'password-management [password-expire-in-days]'オプションはLightweight Directory Access Protocol(LDAP)でのみサポートされます。RADIUSにはこの機能はありません。Active Directoryでパスワードの有効期限が既に切れている場合は、[password expire]オプションが表示されます。

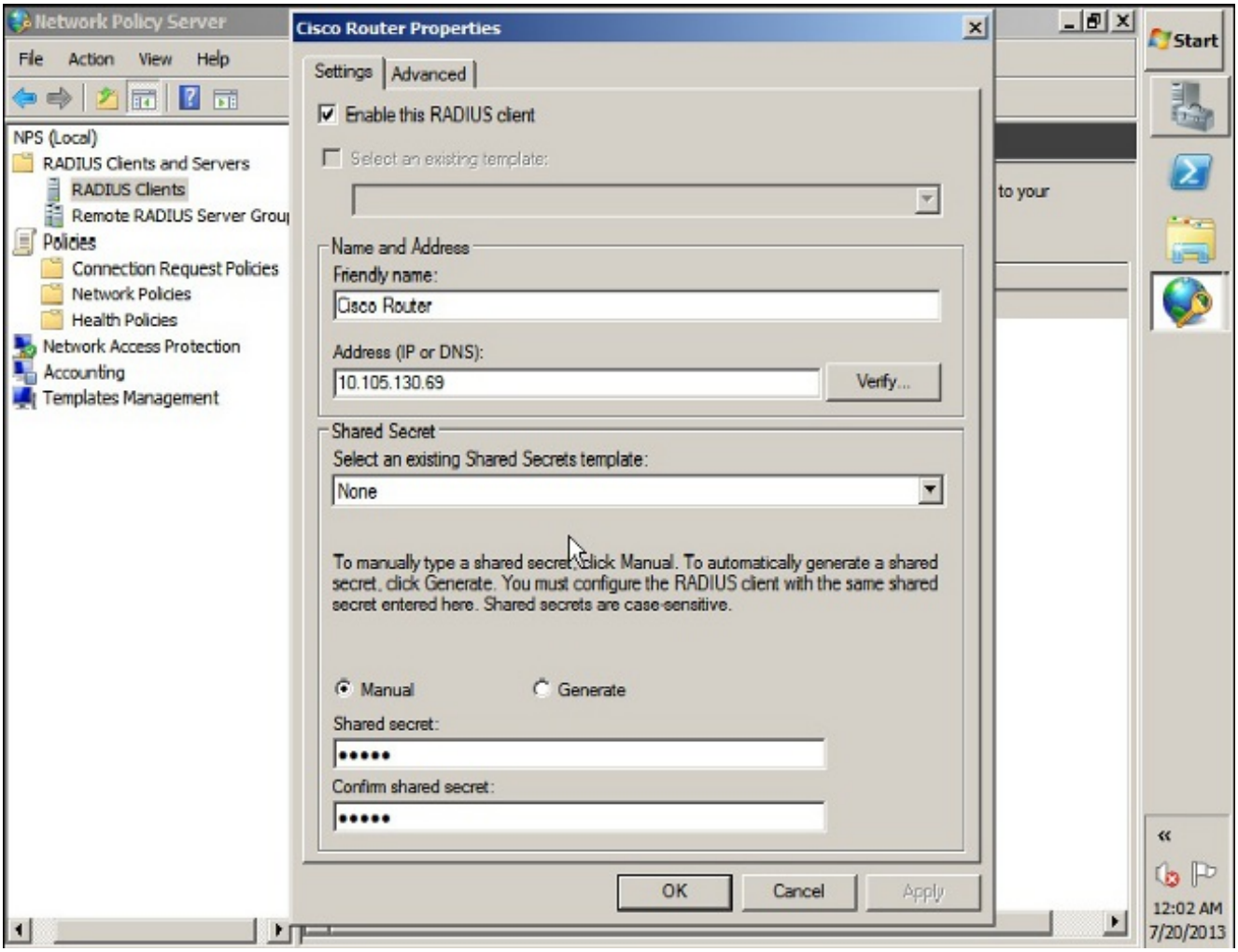
Windows 2008 ServerとNPSの構成

NPSサーバーの役割がインストールされ、Windows 2008サーバーで実行されている必要があります。そうでない場合は、**[Start] > [Administrative Tools] > [Server Roles] > [Add Role Services]を選択します。**ネットワークポリシーサーバを選択し、ソフトウェアをインストールします。NPSサーバーの役割がインストールされたら、次の手順を実行して、ASAからのRADIUS認証要求を受け入れて処理するようにNPSを構成します。

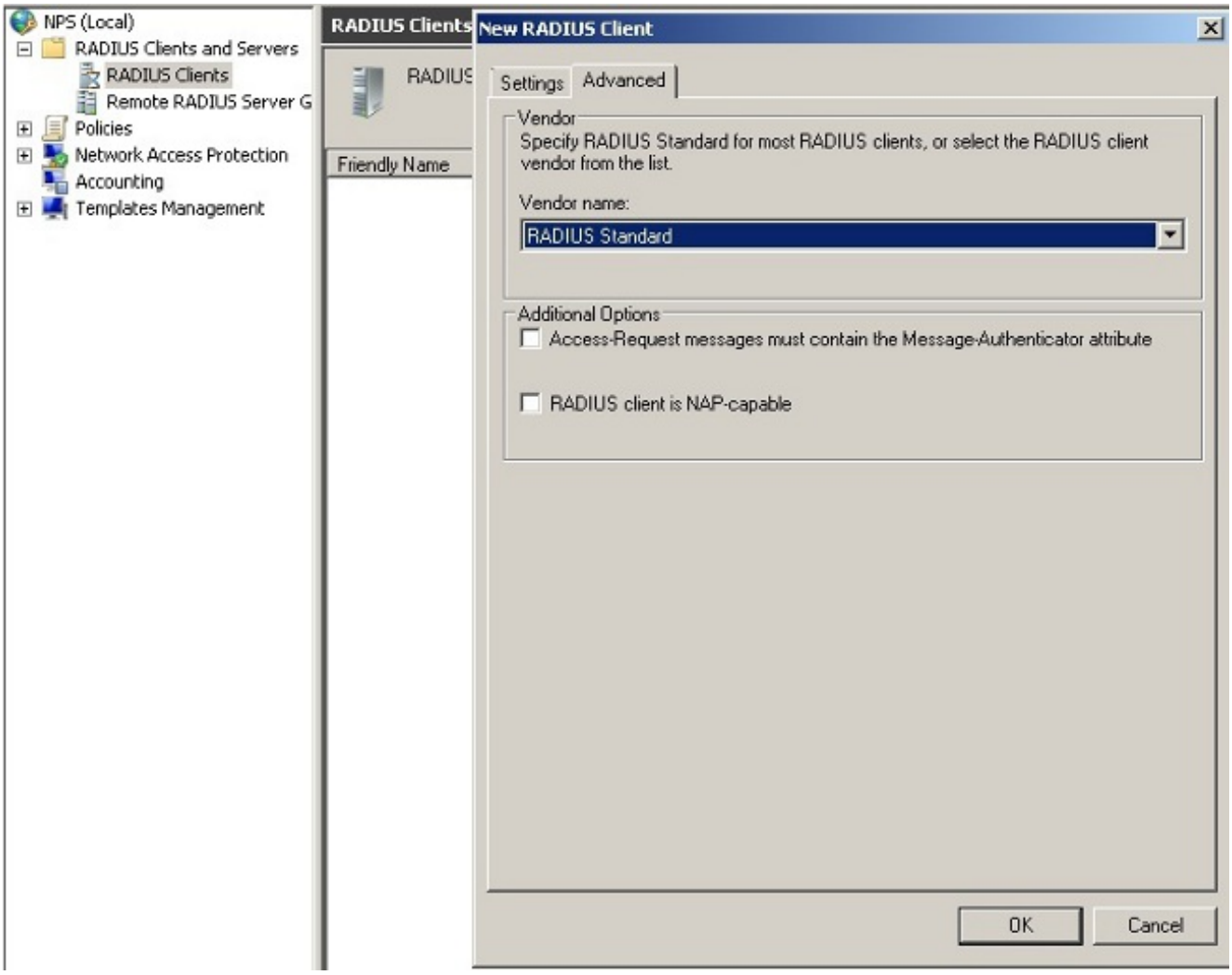
1. ASAをNPSサーバーのRADIUSクライアントとして追加します。 **[管理ツール] > [ネットワークポリシーサーバ]を選択します。**[RADIUS Clients]を右クリックし、**[New]を選択します。**



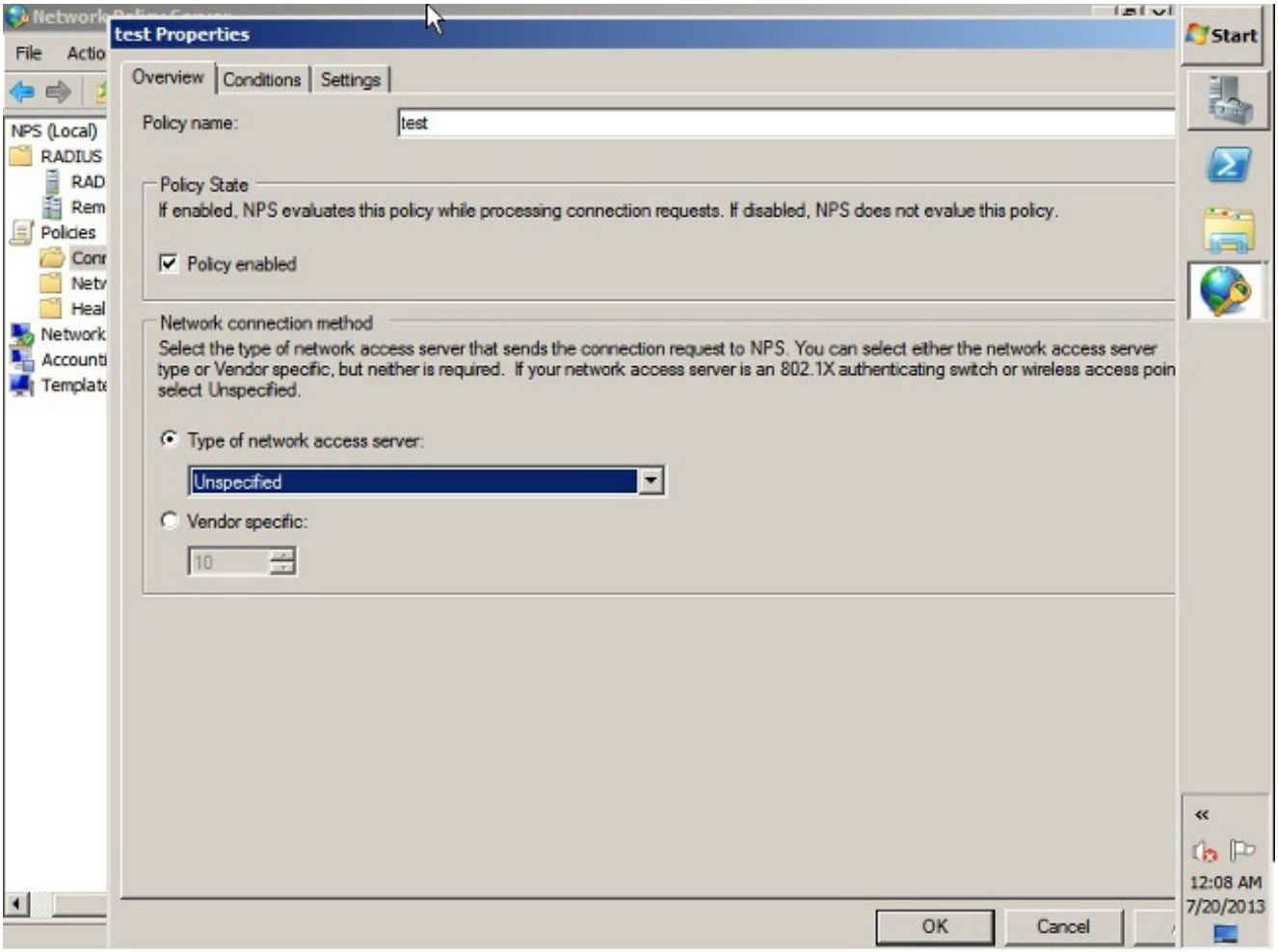
ASAで設定されているフレンドリ名、アドレス（IPまたはDNS）、および共有秘密を入力します。



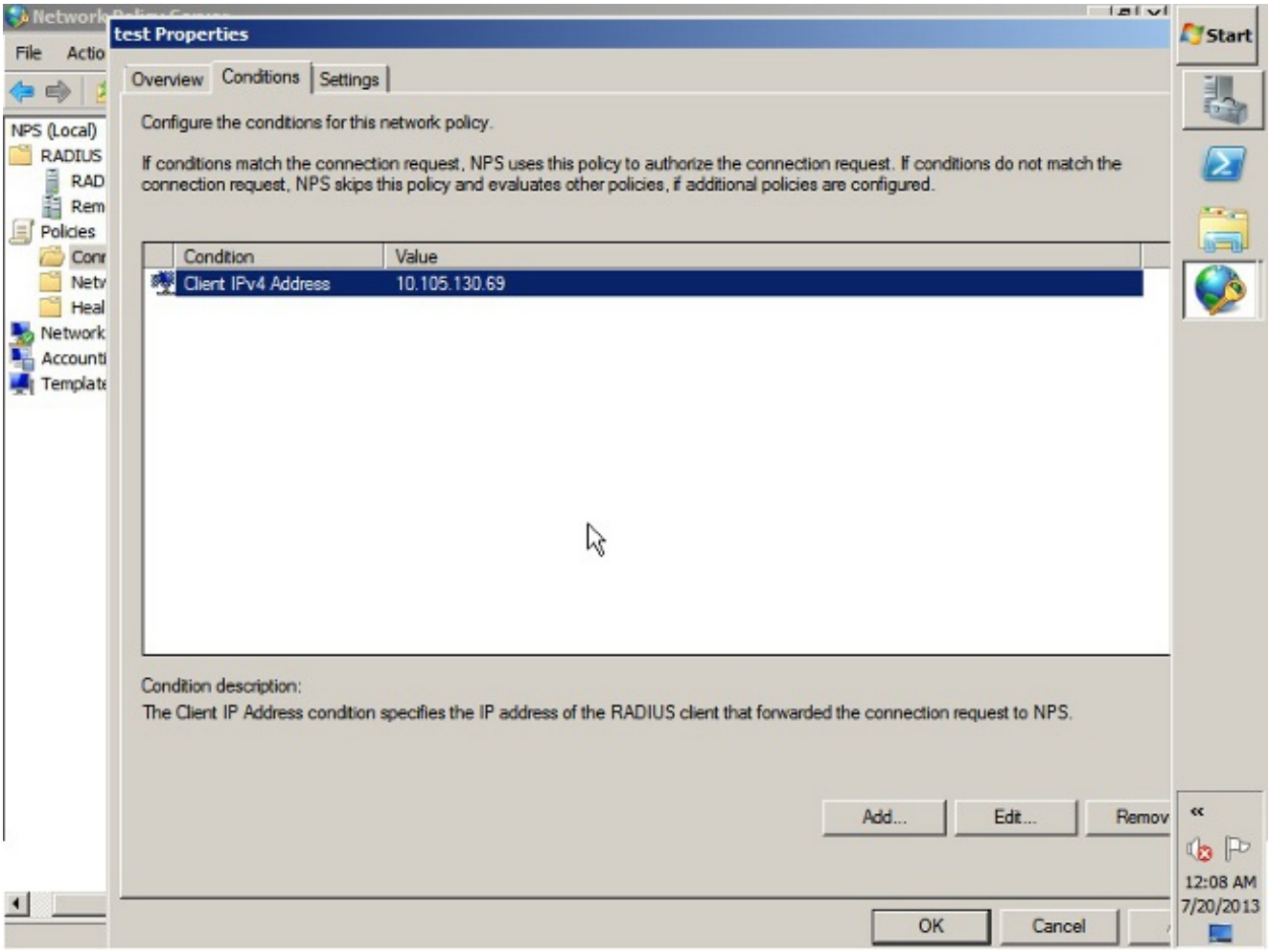
[Advanced] タブをクリックします。[ベンダー名]ドロップダウンリストから、**[RADIUS Standard]を選択します**。[OK] をクリックします。



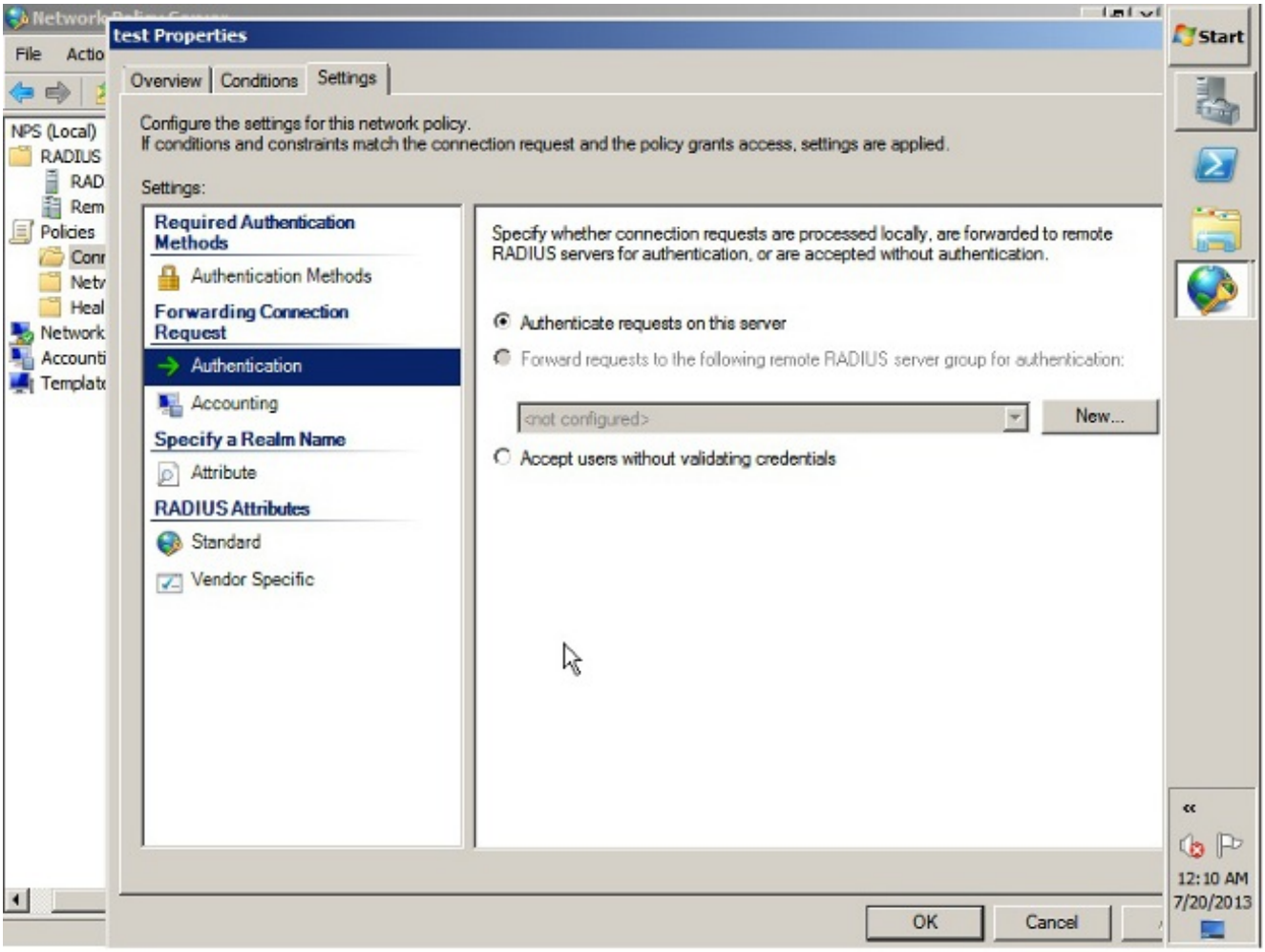
2. VPNユーザの新しい接続要求ポリシーを作成します。接続要求ポリシーの目的は、RADIUSクライアントからの要求を**ローカルで処理するか、リモートRADIUSサーバに転送するかを指定することです。** [NPS] > [ポリシー]で、[接続要求ポリシー]**を右クリック**し、新しいポリシーを作成します。[Type of network access server]ドロップダウンリストから、[**Unspecified**]を選択します。



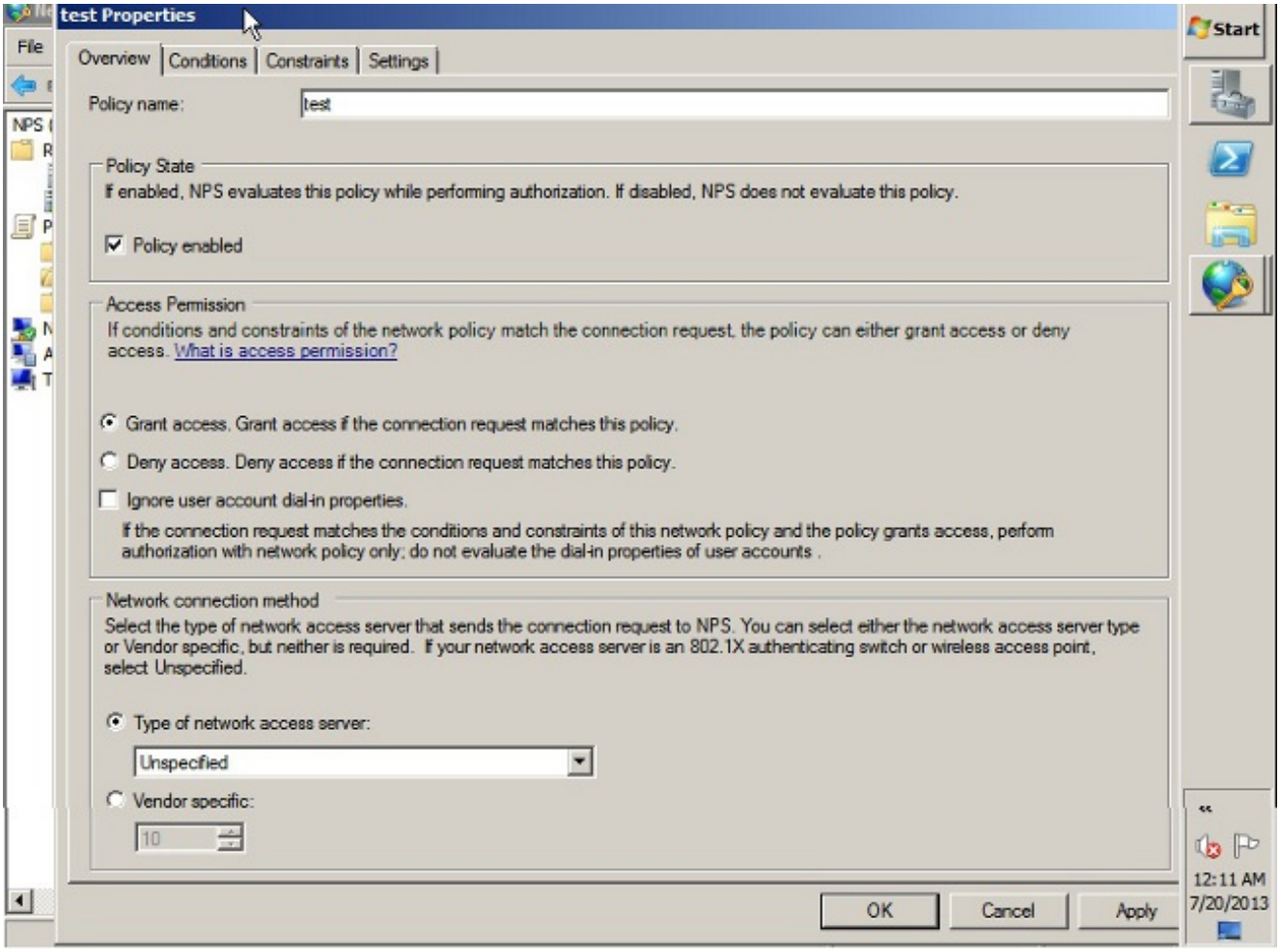
[条件]タブを**クリック**します。[Add] をクリックします。ASAのIPアドレスを[Client IPv4 Address]条件として入力します。



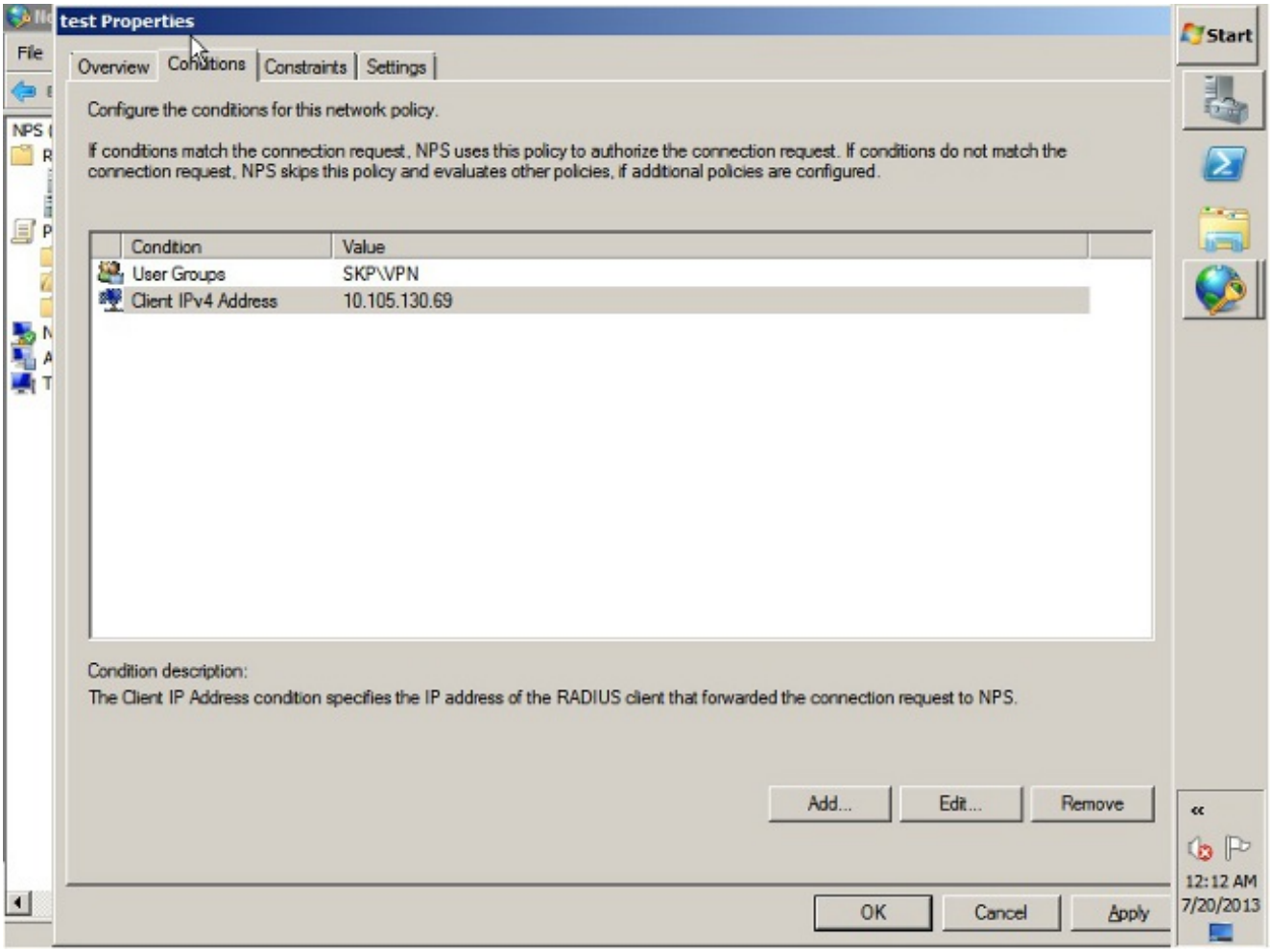
[設定]タブを**クリック**します。[Forwarding Connection Request]で、[**Authentication**]を選択**します**。[Authenticate requests on this server]オプションボタンが選択されていることを確認します。[OK] をクリックします。



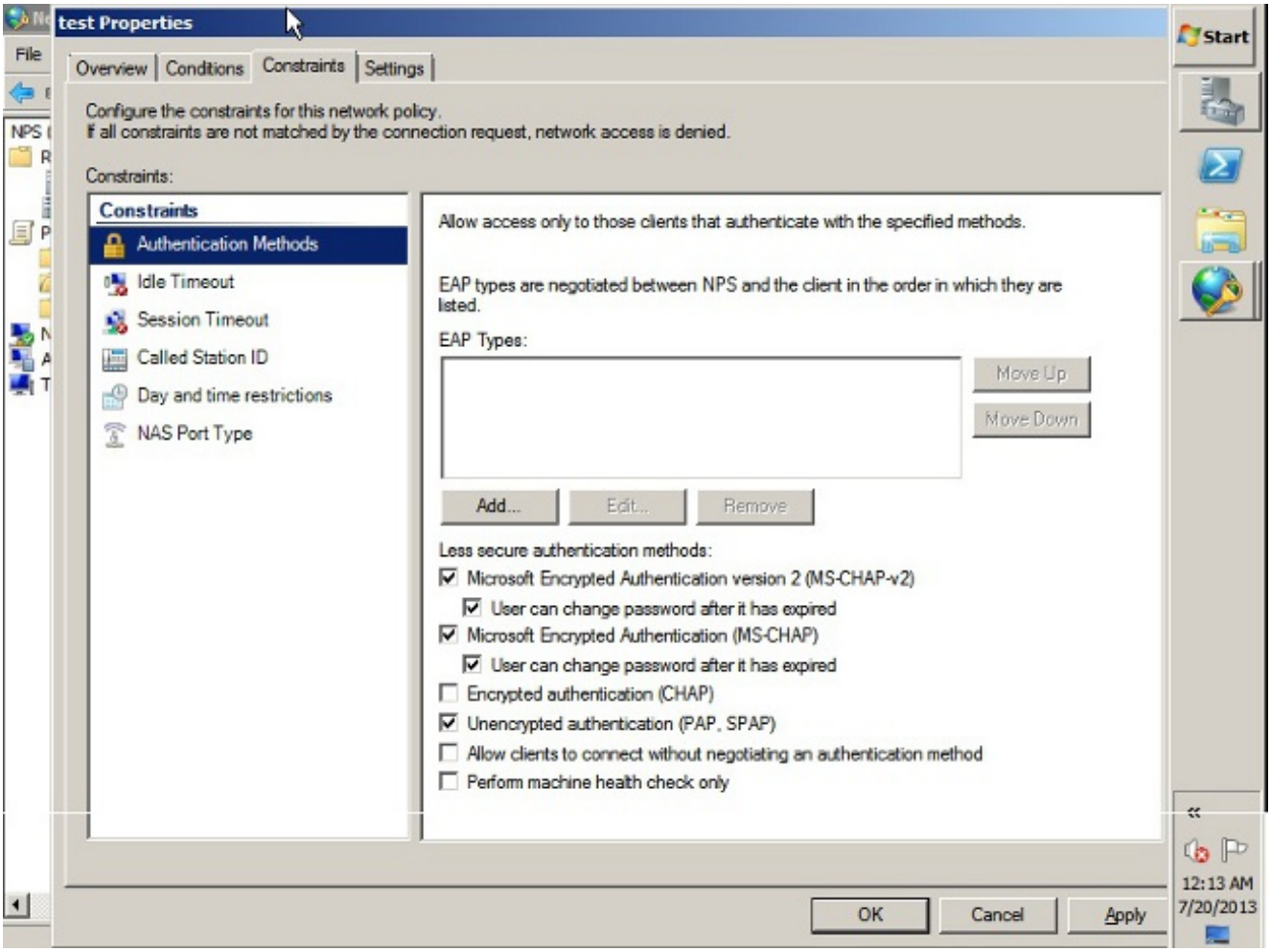
3. 認証を許可するユーザを指定できるネットワークポリシーを追加します。たとえば、Active Directoryユーザグループを条件として追加できます。指定されたWindowsグループに属するユーザーのみが、このポリシーで認証されます。[NPS]で[ポリシー]を**選択します**。[ネットワークポリシー]**を右クリック**し、新しいポリシーを作成します。[Grant access]オプションボタンが選択されていることを確認します。[Type of network access server]ドロップダウンリストから、[**Unspecified**]を選択します。



[条件]タブを**クリック**します。[Add] をクリックします。ASAのIPアドレスを[Client IPv4 Address]条件として入力します。VPNユーザを含むActive Directoryユーザグループを入力します。



[拘束]タブを**クリック**します。[**Authentication Methods]を選択します**。[Unencrypted authentication (PAP, SPAP)]チェックボックスがオンになっていることを確認します。[OK]をクリックします。

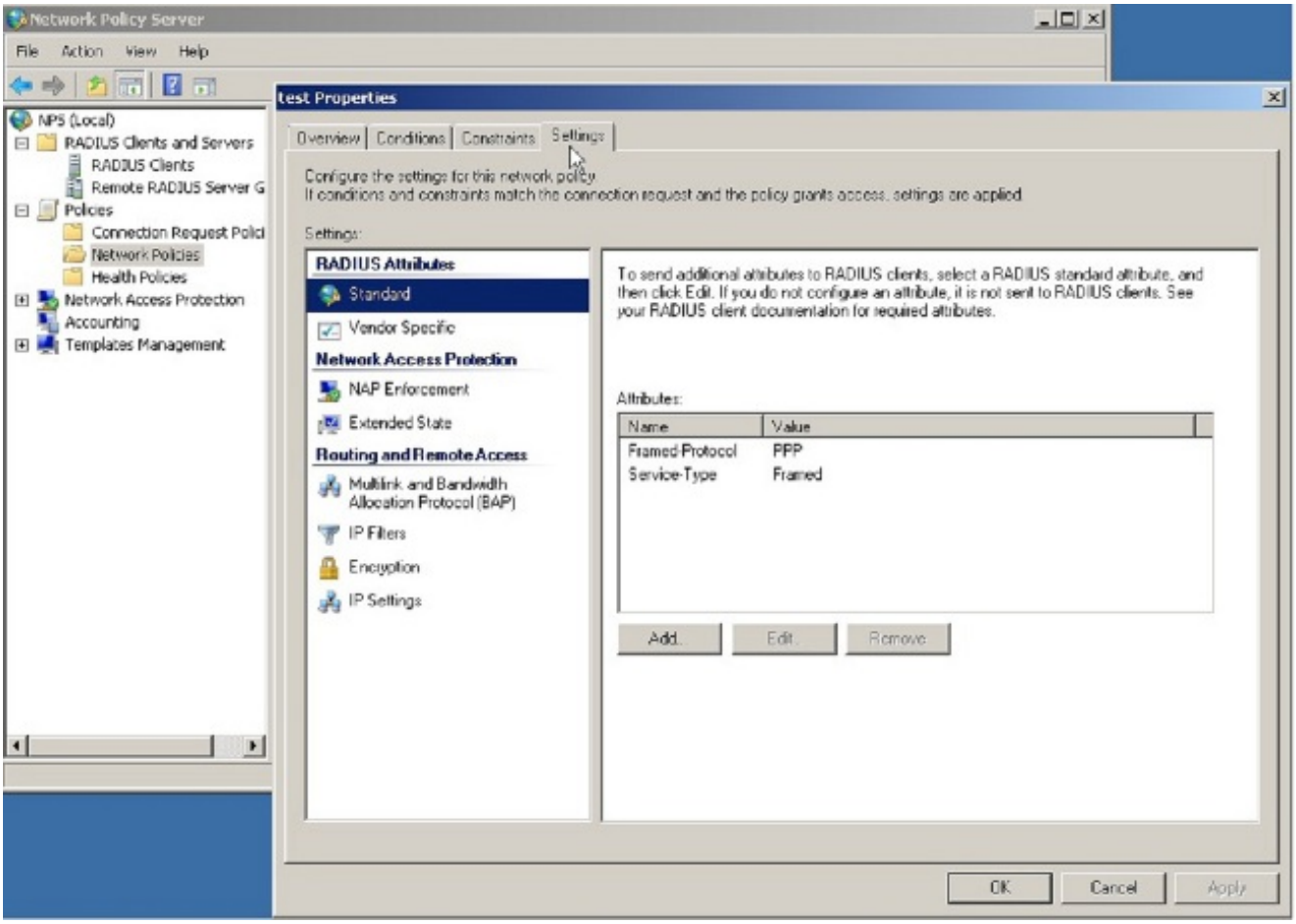


NPS RADIUSサーバーからグループポリシー属性（属性25）を渡す

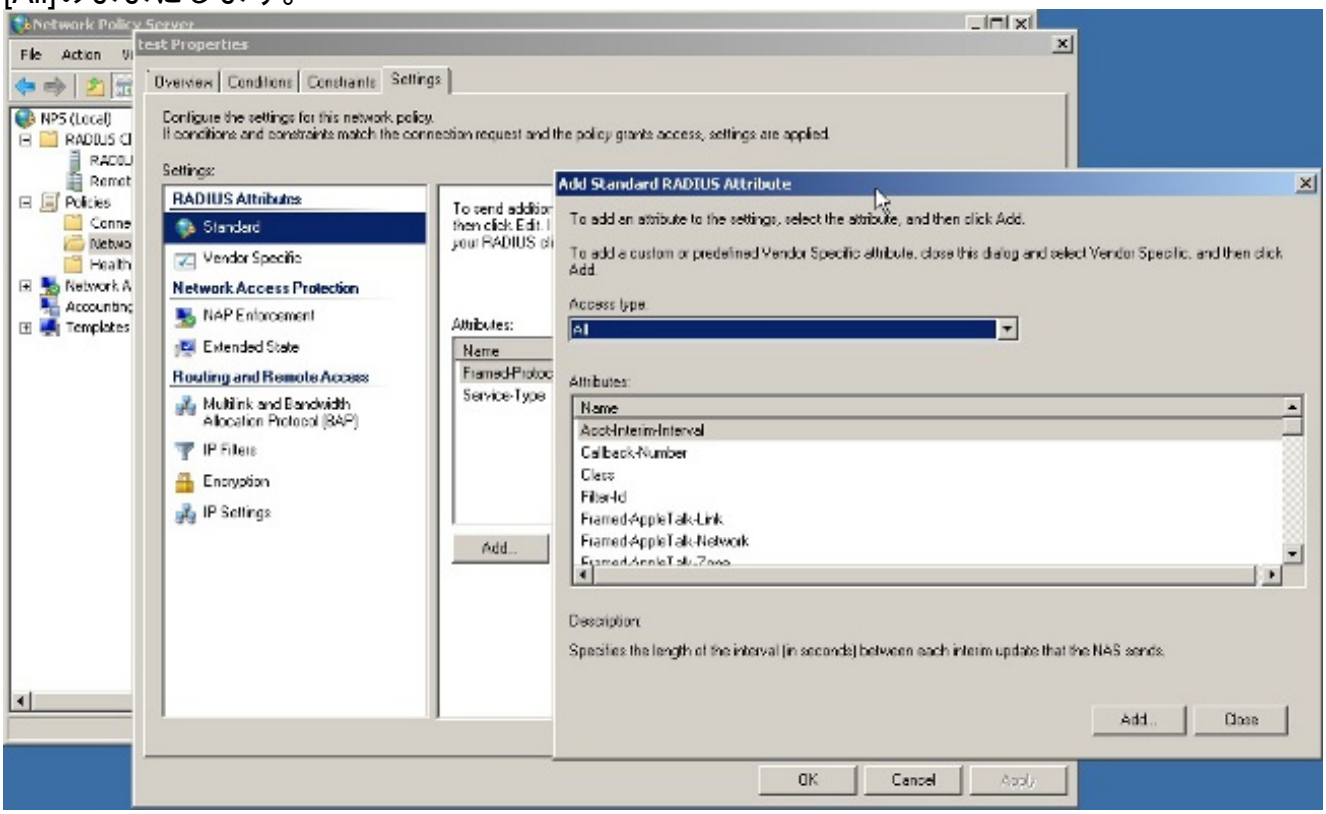
グループポリシーをNPS RADIUSサーバーでユーザーに動的に割り当てる必要がある場合は、グループポリシーのRADIUS属性（属性25）を使用できます。

ユーザにグループポリシーを動的に割り当てるためにRADIUS属性25を送信するには、次の手順を実行します。

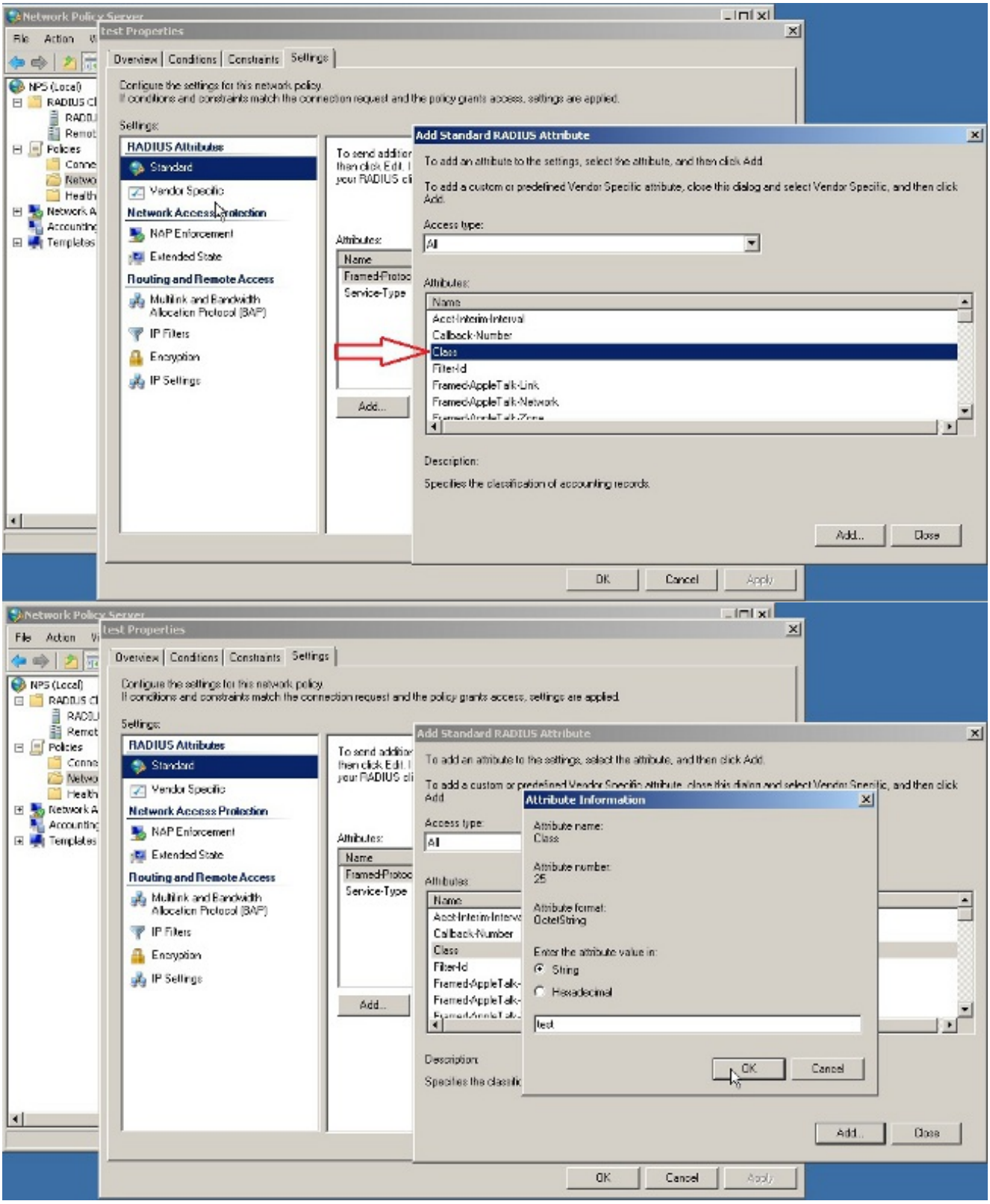
1. ネットワークポリシーを追加したら、必要なネットワークポリシーを右クリックし、[設定]タブを**クリック**します。



2. [**RADIUS Attributes**] > [**Standard**]**を選択します。**[Add] をクリックします。[Access type]は[All]のままにします。



3. [Attributes]ボックスで、[Class]を選択し、[**Add**]をクリックします。属性値、つまりグループポリシーの名前を文字列として入力します。この名前のグループポリシーは、ASAで設定する必要があることに注意してください。これは、ASAがRADIUS応答でこの属性を受信した後、VPNセッションに割り当てるためです。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

注：debug コマンドを使用する前に、「デバッグ コマンドの重要な情報」を参照してください。

ASA のデバッグ

ASAで**debug radius all**を有効にします。

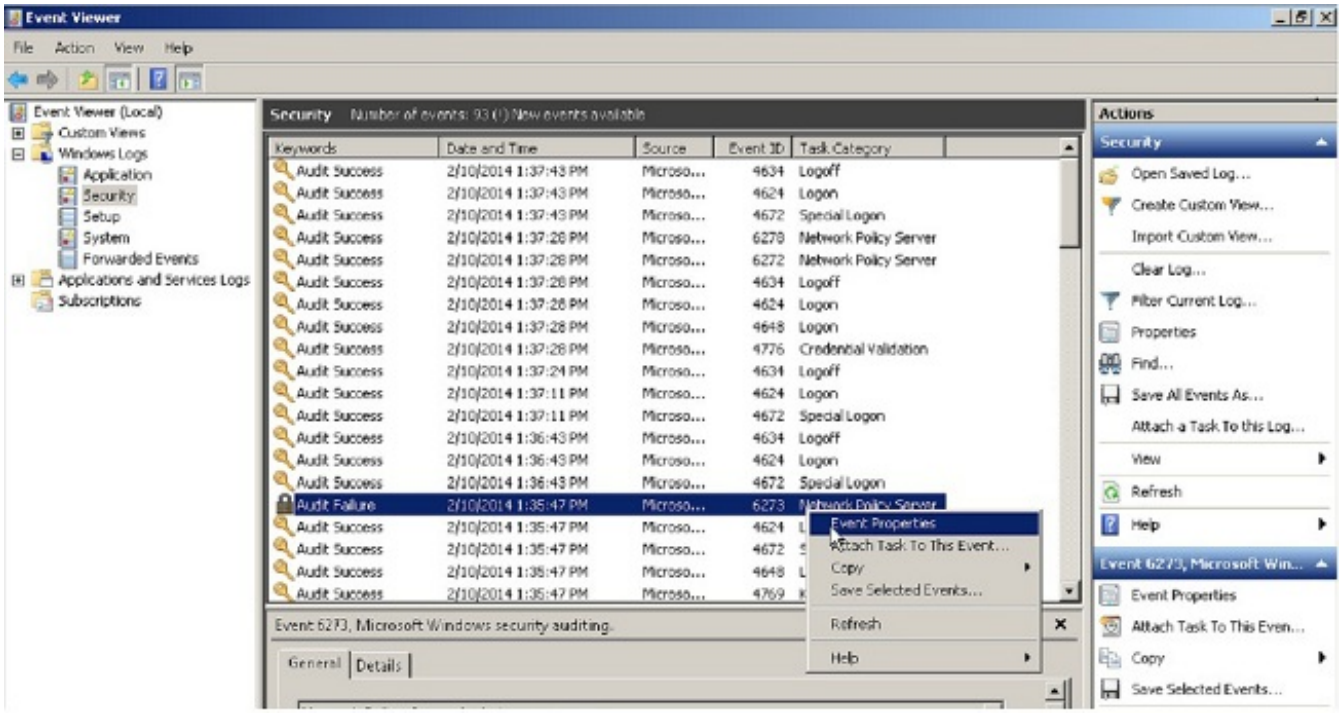
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- ASAとNPSサーバ間の接続が良好であることを確認します。パケットキャプチャを適用して、認証要求が（サーバが到達可能な場所から）ASAインターフェイスを離れるようにします。 UDPポート1645（デフォルトのRADIUS認証ポート）がパス内のデバイスによってブロックされていないことを確認し、NPSサーバに到達するようにします。ASAでのパケットキャプチャの詳細については、『ASA/PIX/FWSM:CLI および ASDM を使用したパケットのキャプチャの設定例.
- それでも認証が失敗する場合は、Windows NPSのイベントビューアで確認します。[イベントビューア] > [Windowsログ]で、[セキュリティ]を選択**します。**認証要求時にNPSに関連するイベントを探します。



[Event Properties]を開くと、次の例に示すように、失敗の理由が表示されます。この例では、ネットワークポリシーの下で認証タイプとしてPAPが選択されていません。したがって、認証要求は失敗します。

```
 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.**