RADIUS 컨피그레이션을 사용하는 Windows 2008 NPS 서버(Active Directory)에 대한 ASA VPN 사용자 인증 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램](#)
[구성](#)
[ASDM 컨피그레이션](#)
[CLI 컨피그레이션](#)
[NPS 구성이 포함된 Windows 2008 Server](#)
[다음을 확인합니다.](#)
[ASA 디버그](#)
[문제 해결](#)

소개

이 문서에서는 레거시 Cisco VPN Client/AnyConnect/Clientless WebVPN 사용자가 Active Directory에 대해 인증되도록 RADIUS 프로토콜과 Microsoft Windows 2008 NPS(Network Policy Server)와 통신하도록 ASA(Adaptive Security Appliance)를 구성하는 방법에 대해 설명합니다 .NPS는 Windows 2008 Server에서 제공하는 서버 역할 중 하나입니다.원격 전화 접속 사용자 인증을 제공하기 위해 RADIUS 서버를 구현하는 Windows 2003 Server, IAS(Internet Authentication Service)와 같습니다.마찬가지로 Windows 2008 Server에서 NPS는 RADIUS 서버의 구현입니다.기본적으로 ASA는 NPS RADIUS 서버에 대한 RADIUS 클라이언트입니다.ASA는 VPN 사용자를 대신하여 RADIUS 인증 요청을 전송하고 NPS는 Active Directory에 대해 이를 인증합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

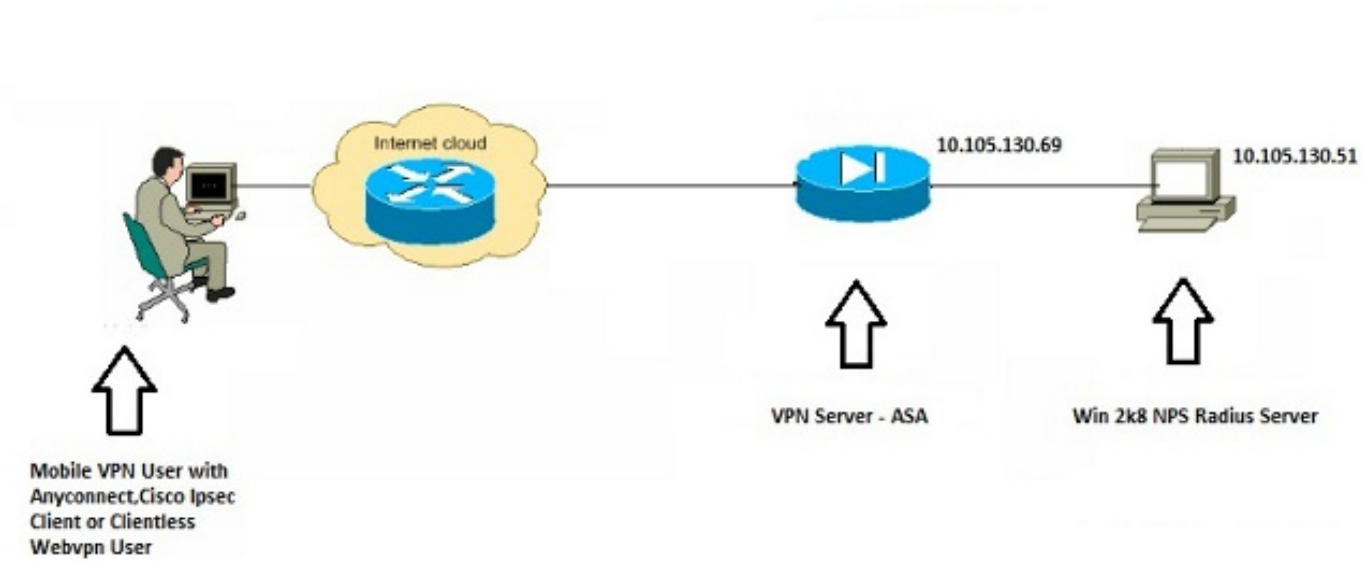
- 버전 9.1(4)을 실행하는 ASA
- Active Directory 서비스 및 NPS 역할이 설치된 Windows 2008 R2 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

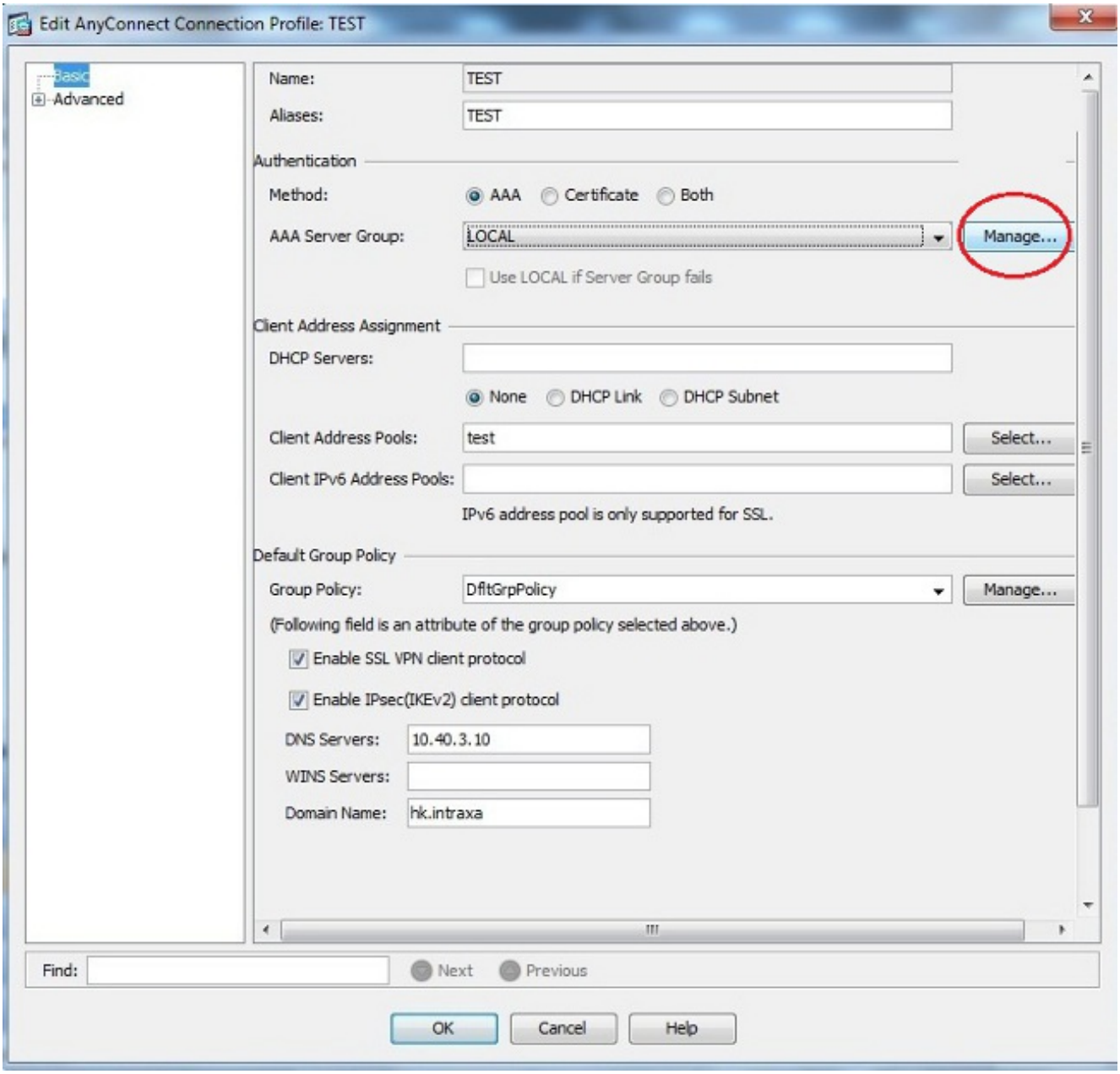
네트워크 다이어그램



구성

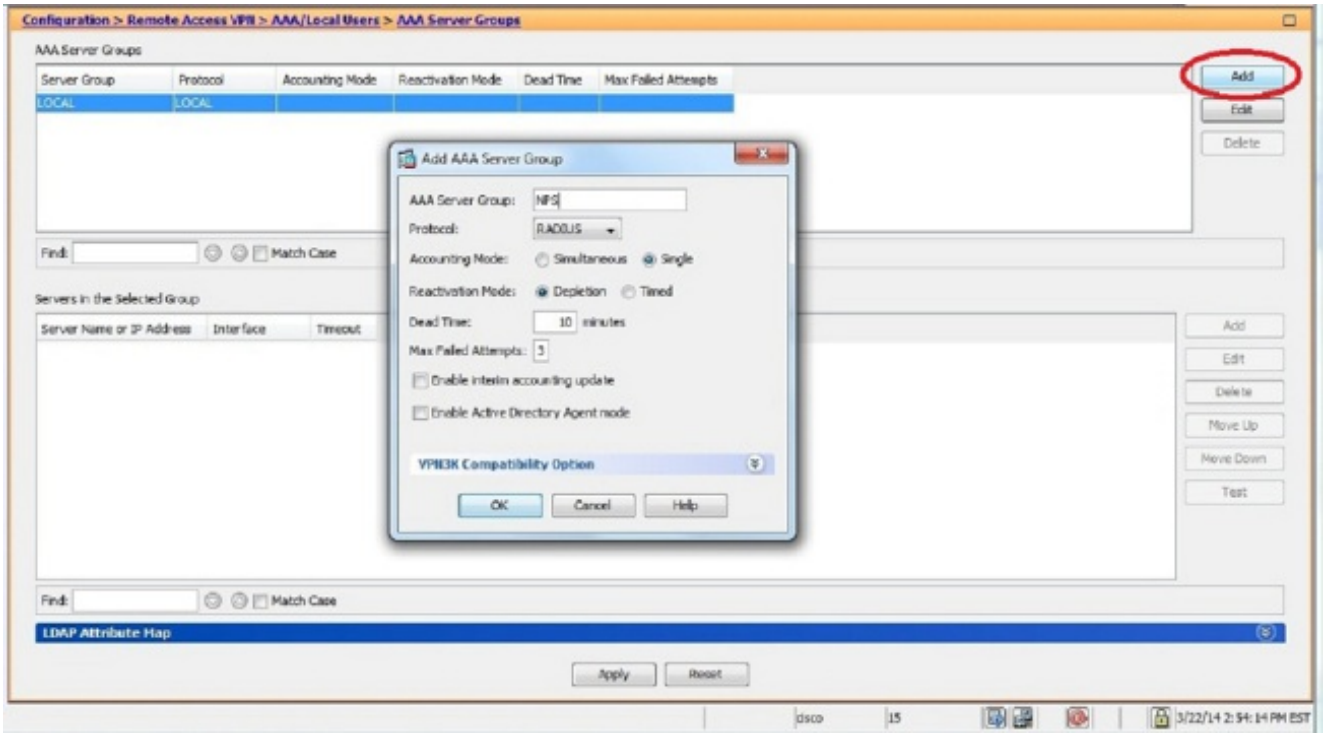
ASDM 컨피그레이션

1. NPS 인증이 필요한 터널 그룹을 선택합니다.
2. Edit(**편집**)를 클릭하고 **Basic(기본)을** 선택합니다.
3. Authentication(인증) 섹션에서 Manage(**관리**)를 클릭합니다
   .



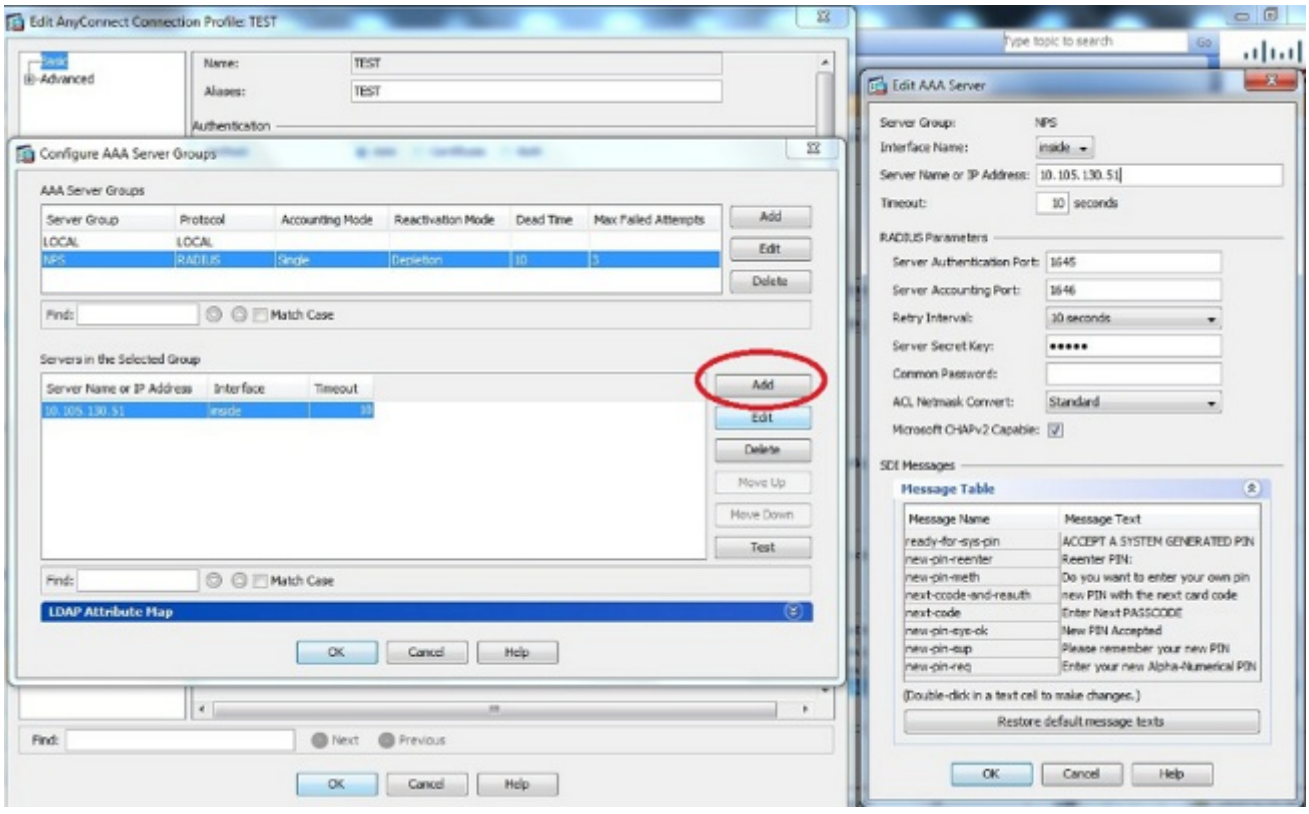
4. AAA Server Groups(AAA 서버 그룹) 섹션에서 Add(**추가)**를 클릭합니다.
5. AAA Server Group(AAA 서버 그룹) 필드에 서버 그룹의 이름(예: NPS)을 입력합니다.
6. Protocol 드롭다운 목록에서 **RADIUS**를 선택합니다.
7. **확인**을 **클릭합니다**

.



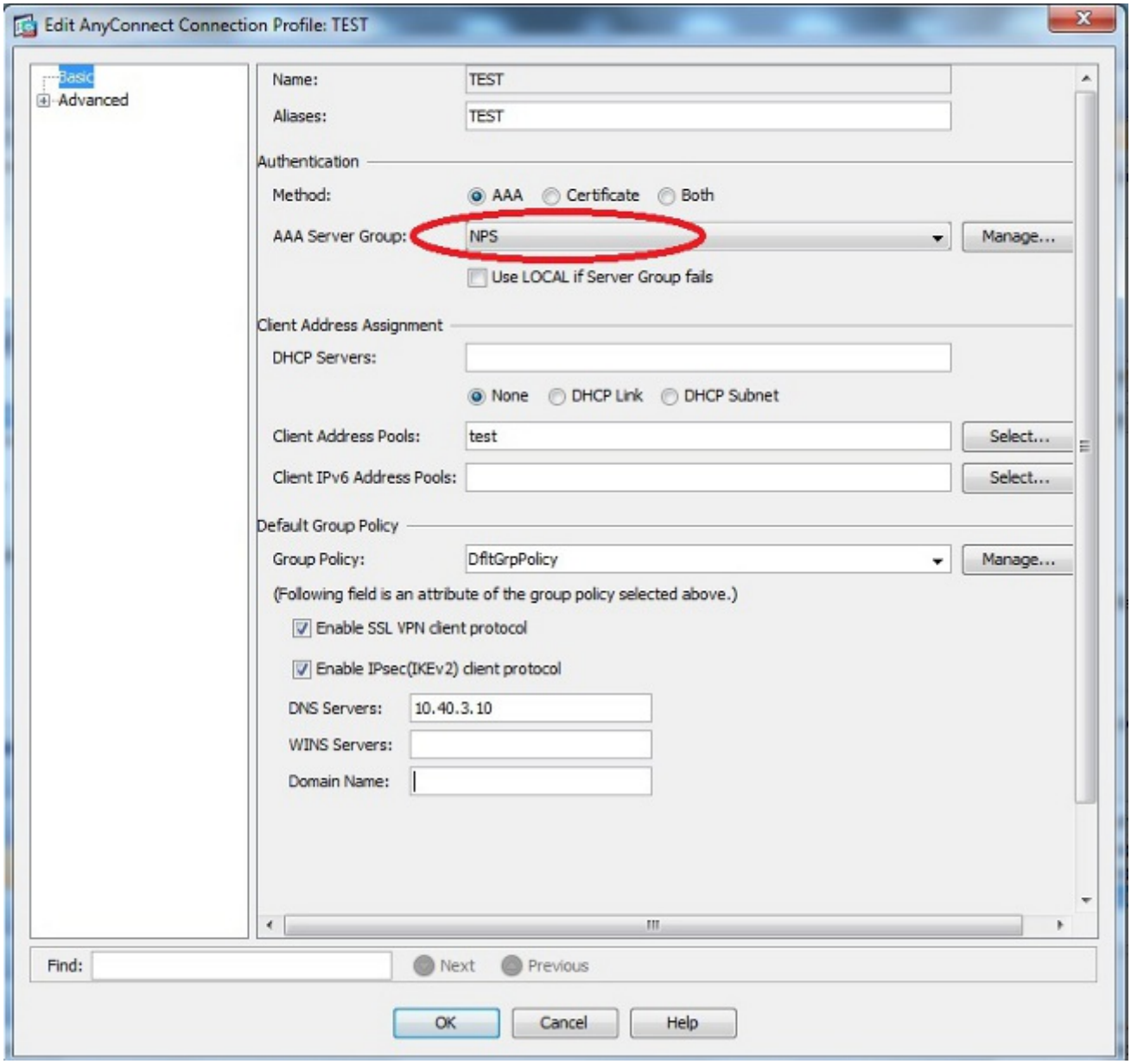
8. Servers in the Selected Group(선택한 그룹의 서버) 섹션에서 추가된 AAA Server Group(AAA 서버 그룹)을 선택하고 Add(**추가)**를 클릭합니다.
9. Server Name or IP Address 필드에 서버 IP 주소를 입력합니다.
10. Server Secret Key 필드에 비밀 키를 입력합니다.
11. 서버가 다른 포트에서 수신 대기하지 않는 한 서버 인증 포트 및 서버 계정 포트 필드를 기본값으로 둡니다.
12. **확인**을 **클릭합니다**.
13. **확인**을 **클릭합니다**

.



14. AAA Server Group(AAA 서버 그룹) 드롭다운 목록에서 이전 단계에 추가된 그룹(이 예의 NPS)을 선택합니다.
15. **확인**을 **클릭합니다**

.



CLI 컨피그레이션

```
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
```

기본적으로 ASA는 암호화되지 않은 PAP(Password Authentication Protocol) 인증 유형을 사용합니다.이는 ASA가 RADIUS REQUEST 패킷을 전송할 때 일반 텍스트로 비밀번호를 전송하는 것을 의미하지는 않습니다.대신 일반 텍스트 비밀번호는 RADIUS 공유 암호로 암호화됩니다.

터널 그룹에서 비밀번호 관리가 활성화된 경우 ASA는 일반 텍스트 비밀번호를 암호화하기 위해

MSCHAP-v2 인증 유형을 사용합니다.이 경우 ASDM 컨피그레이션 섹션에서 구성된 Edit AAA Server(AAA 서버 수정) 창에서 **Microsoft CHAPv2 Capable**(**Microsoft CHAPv2 지원**) 확인란이 선택되어 있는지 확인합니다.

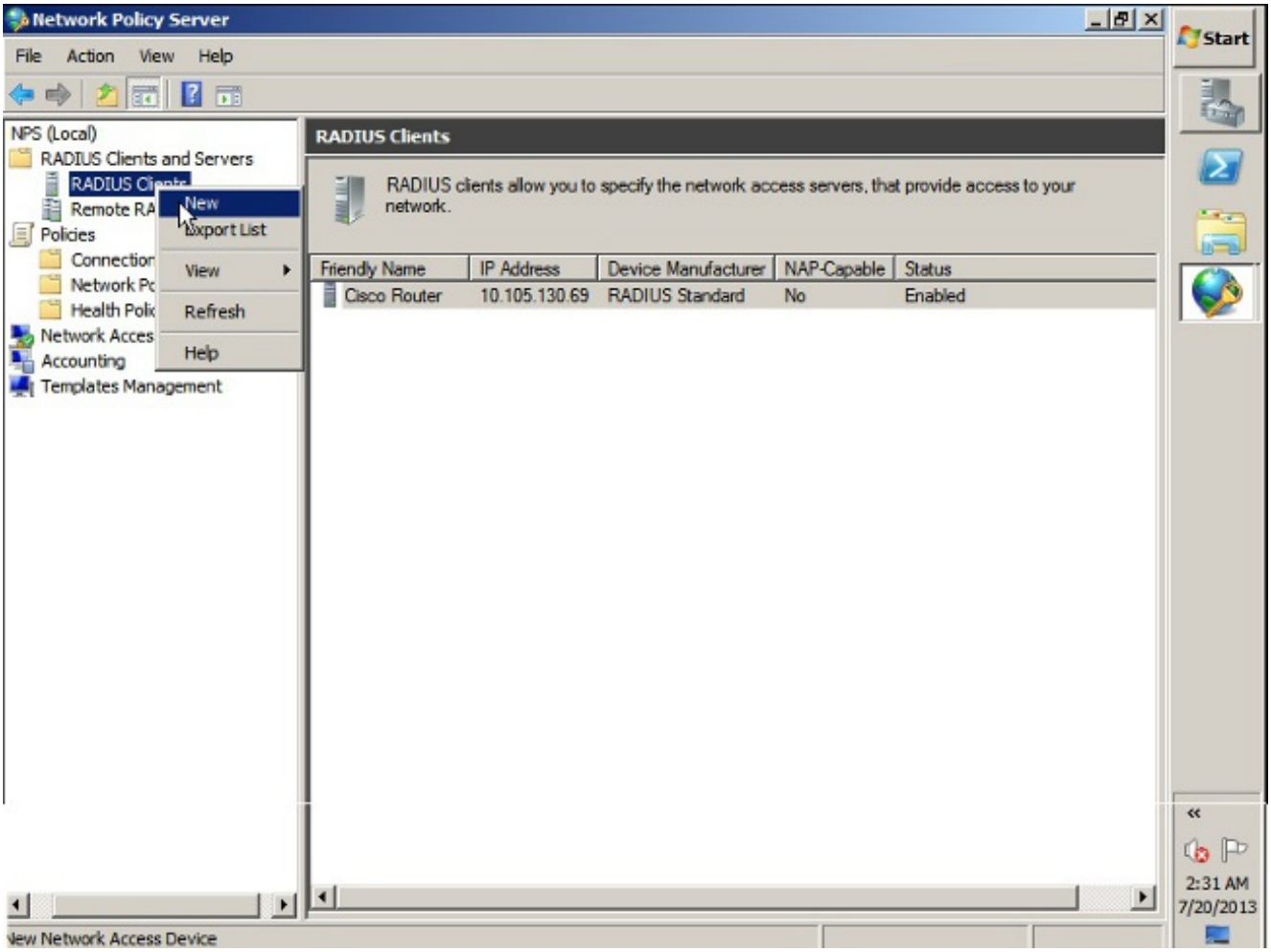
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **참고:**test aaa**-server authentication** 명령은 항상 PAP를 사용합니다.사용자가 비밀번호 관리가 활성화된 터널 그룹에 대한 연결을 시작하는 경우에만 ASA는 MSCHAP-v2를 사용합니다.또한 'password-management [password-expire-in-days]' 옵션은 LDAP(Lightweight Directory Access Protocol)에서만 지원됩니다.RADIUS는 이 기능을 제공하지 않습니다.Active Directory에서 암호가 이미 만료된 경우 비밀번호 만료 옵션이 표시됩니다.

NPS 구성이 포함된 Windows 2008 Server

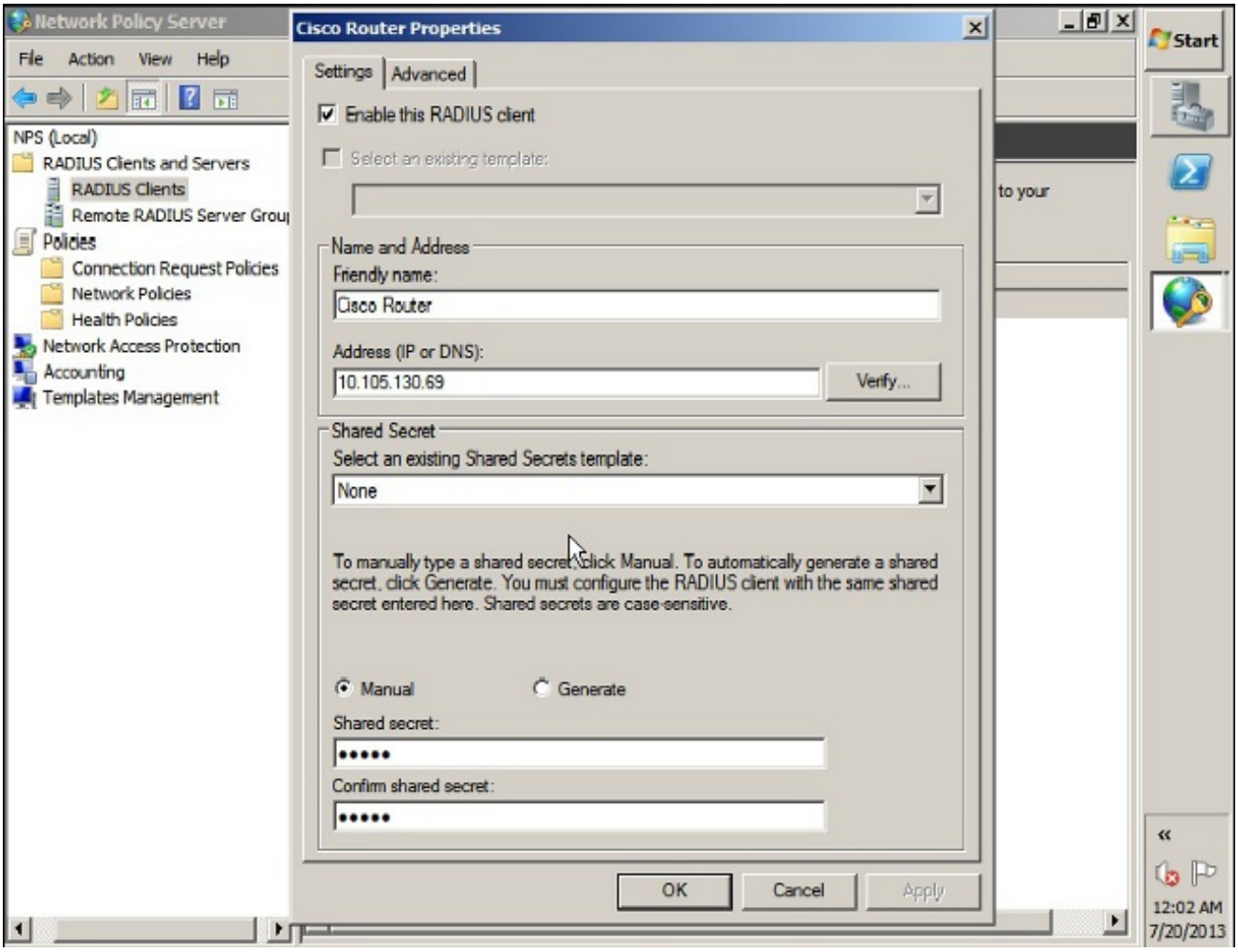
NPS 서버 역할이 Windows 2008 서버에 설치되어 실행되고 있어야 합니다.그렇지 않은 경우 **시작 > 관리 도구 > 서버 역할 > 역할 서비스 추가를** 선택합니다.네트워크 정책 서버를 선택하고 소프트웨어를 설치합니다.NPS 서버 역할이 설치되면 ASA에서 RADIUS 인증 요청을 수락하고 처리하도록 NPS를 구성하려면 다음 단계를 완료하십시오.

1. NPS 서버에서 ASA를 RADIUS 클라이언트로 추가합니다. Administrative **Tools > Network Policy Server를 선택합니다.**RADIUS Clients(RADIUS **클라이언트)를 마우스 오른쪽 버튼으로** 클릭하고 New(새로 만들기)를 **선택합니다**
   .



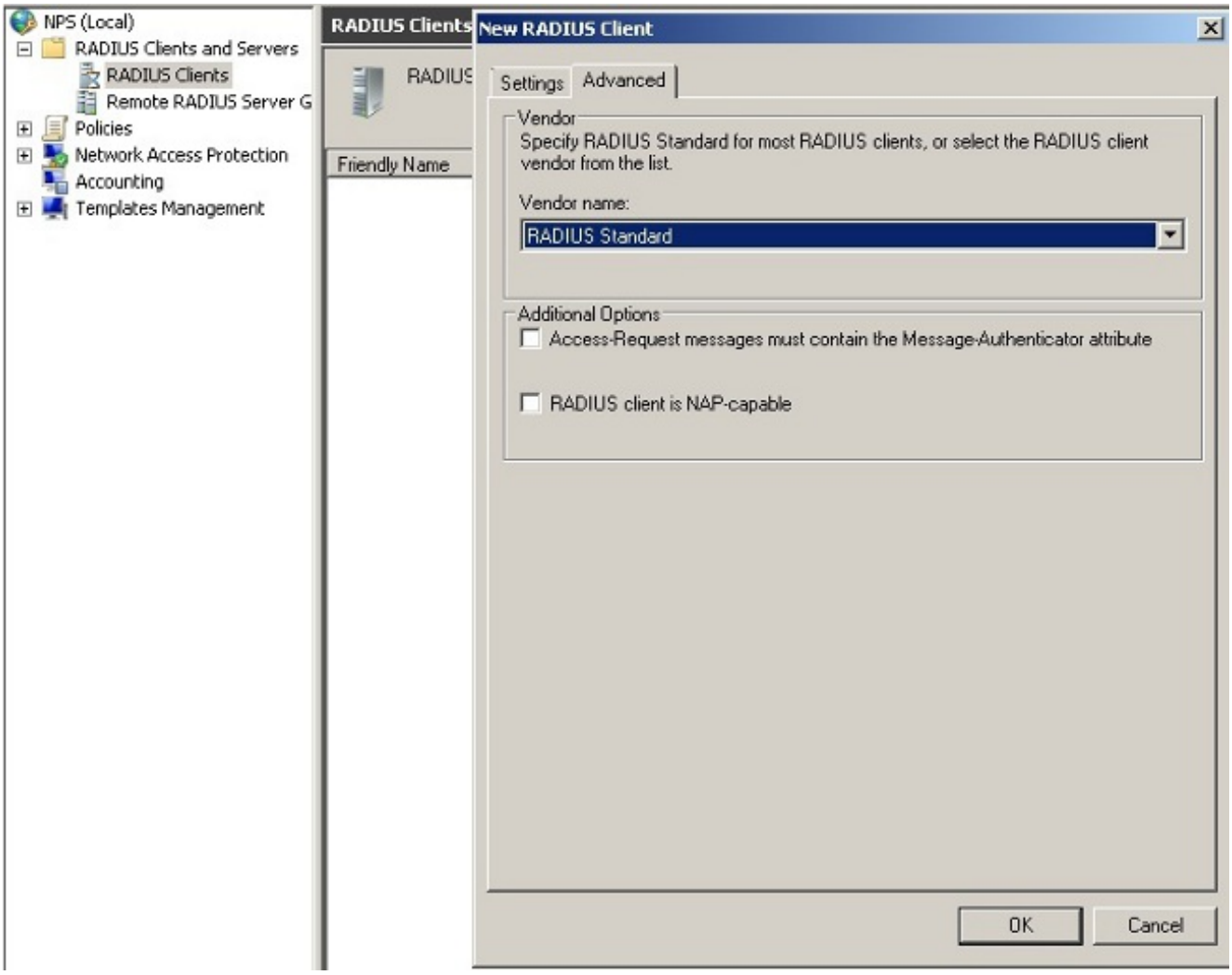
ASA에 구성된 이름, 주소(IP 또는 DNS) 및 공유 암호를 입력합니다

.



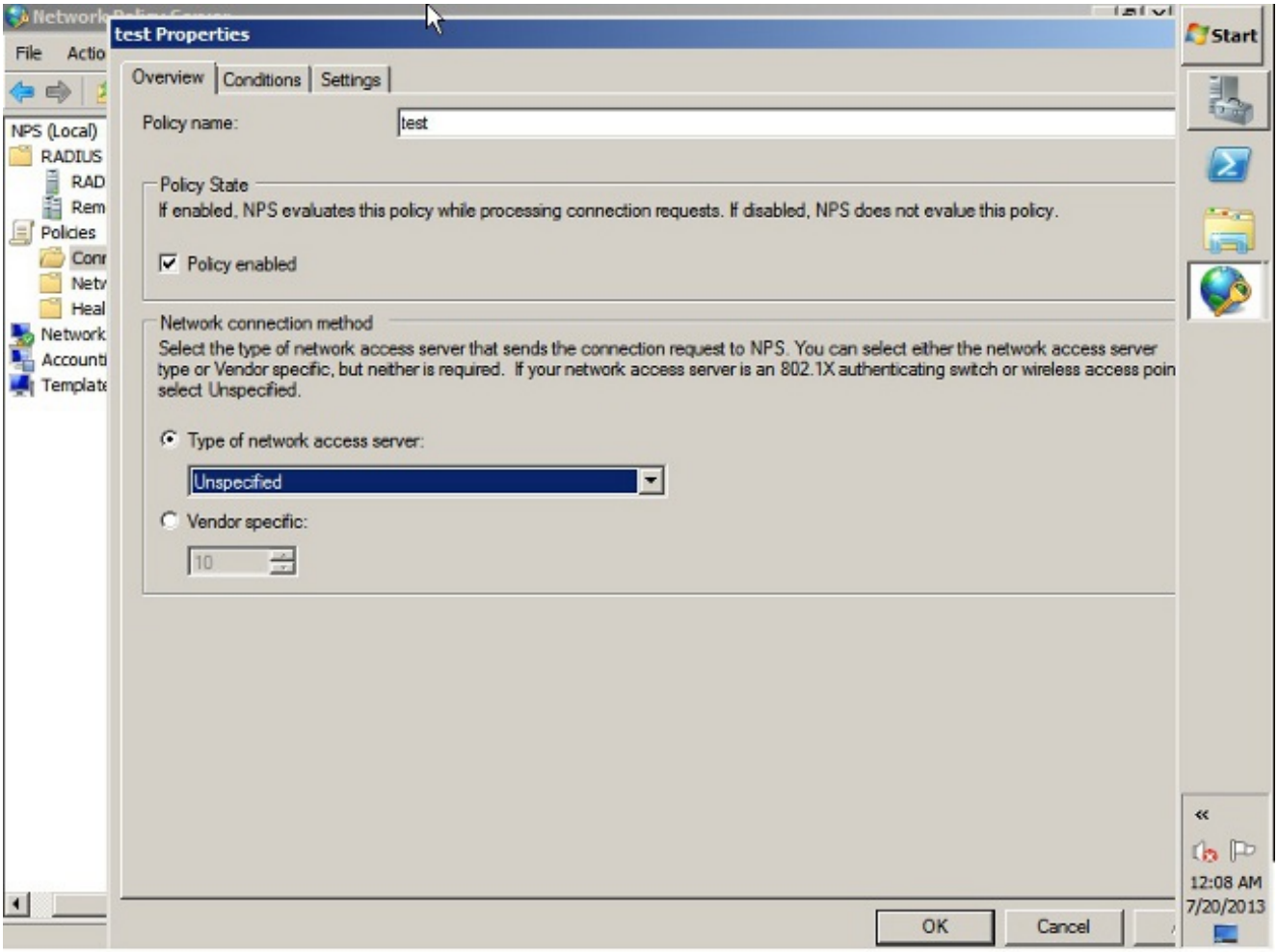
Advanced 탭을 클릭합니다.Vendor name(공급업체 이름) 드롭다운 목록에서 RADIUS **Standard**를 선택합니다.**확인**을 **클릭합니다**

.



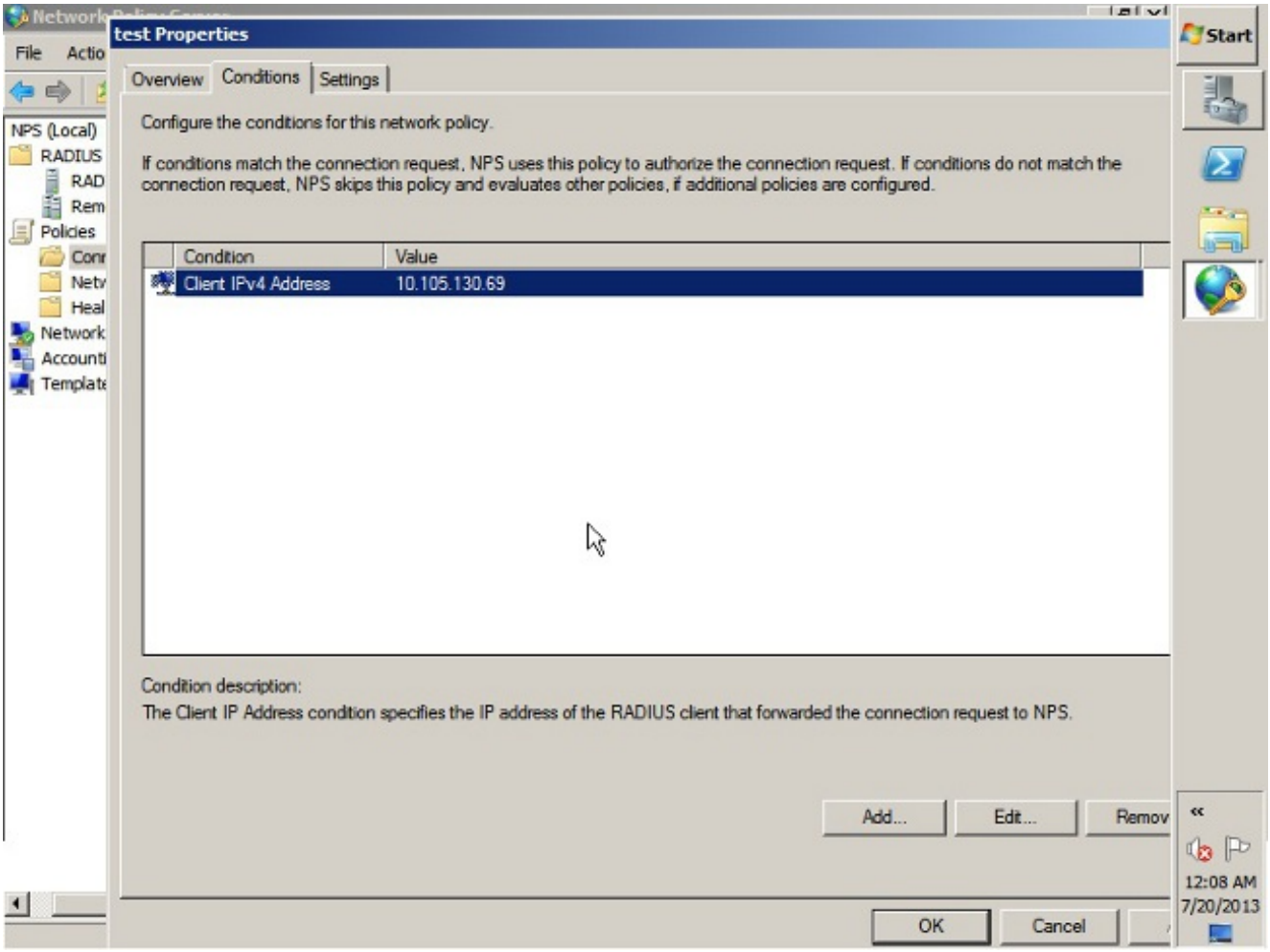
2. VPN 사용자를 위한 새 연결 요청 정책을 만듭니다.연결 요청 정책의 목적은 RADIUS 클라이언트의 요청을 로컬에서 처리할지 또는 원격 RADIUS 서버로 전달할지를 지정하는 것입니다. NPS > Policies 아래에서 Connection **Request Policies(연결 요청 정책)를** 마우스 오른쪽 버튼으로 클릭하고 새 정책을 생성합니다.Type of network access server(네트워크 액세스 서버 유형) 드롭다운 목록에서 Unspecified(미지정)를 **선택합니다**

.



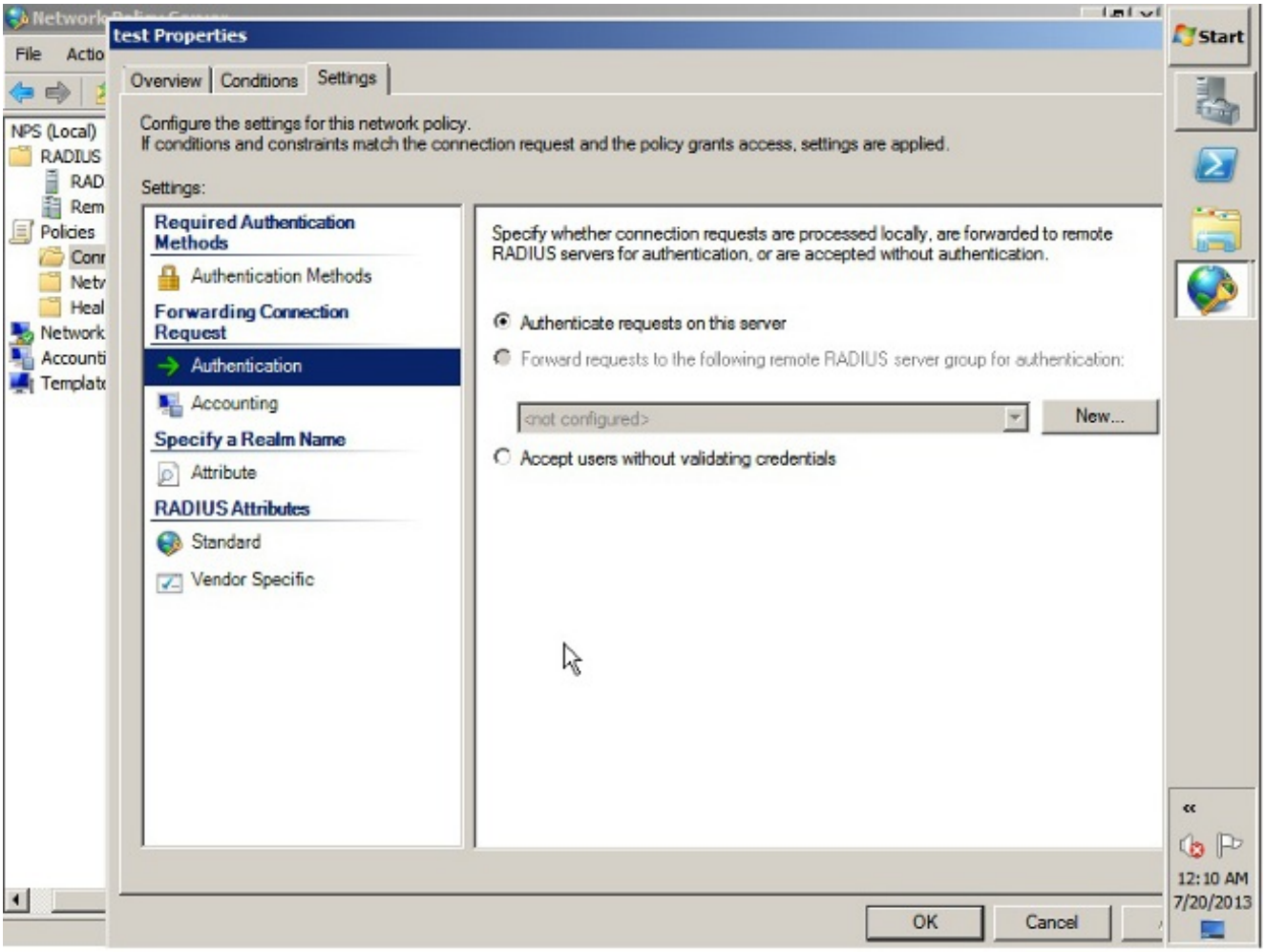
Conditions(조건) 탭을 클릭합니다.Add(**추가)를 클릭합니다**.ASA의 IP 주소를 'Client IPv4 Address' 조건으로 입력합니다

.



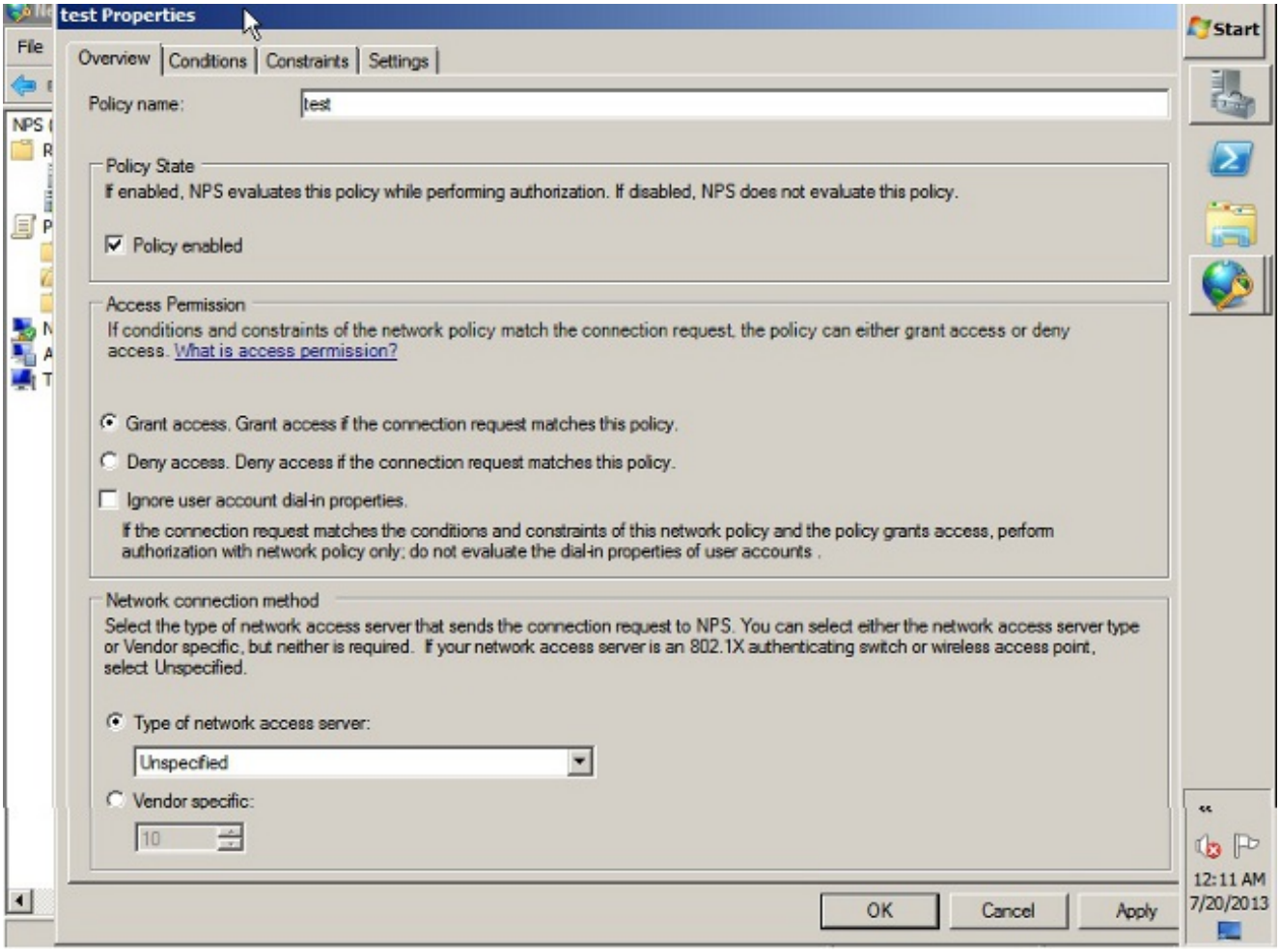
설정 탭을 클릭합니다.Forwarding Connection Request(연결 요청 전달)에서 Authentication(**인증)을** 선택합니다.Authenticate requests on this server(이 서버의 요청 인증) 라디오 버튼이 선택되어 있는지 확인합니다.**확인**을 **클릭합니다**

.



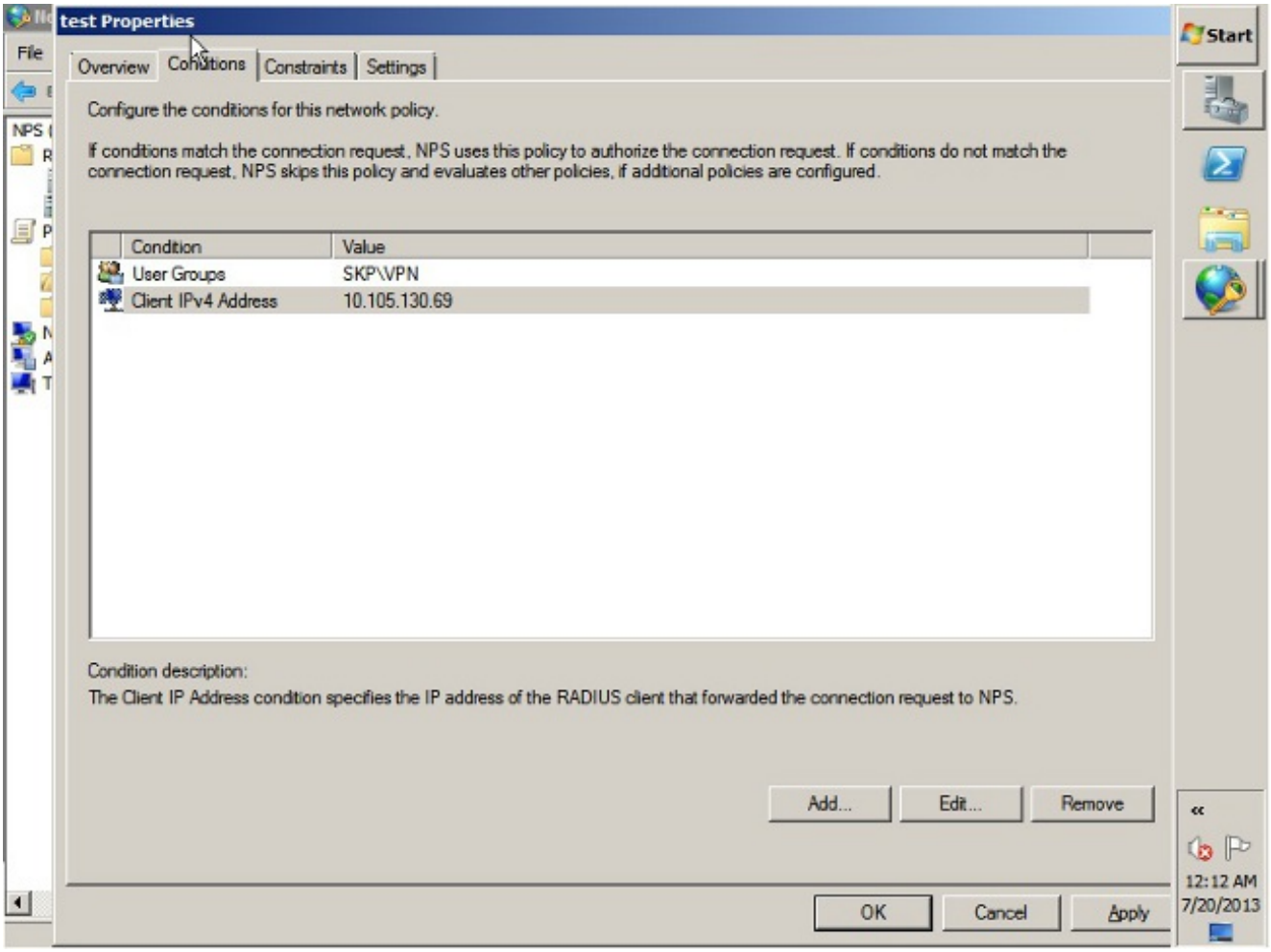
3. 인증할 수 있는 사용자를 지정할 수 있는 네트워크 정책을 추가합니다.예를 들어 Active Directory 사용자 그룹을 조건으로 추가할 수 있습니다.지정된 Windows 그룹에 속한 사용자만 이 정책에서 인증됩니다.NPS에서 Policies(정책)를 **선택합니다.네트워크 정책**을 마우스 오른쪽 버튼으로 클릭하고 새 정책을 생성합니다.액세스 권한 부여 라디오 버튼이 선택되었는지 확인합니다.Type of network access server(네트워크 액세스 서버 유형) 드롭다운 목록에서 Unspecified(미지정)를 **선택합니다**

.



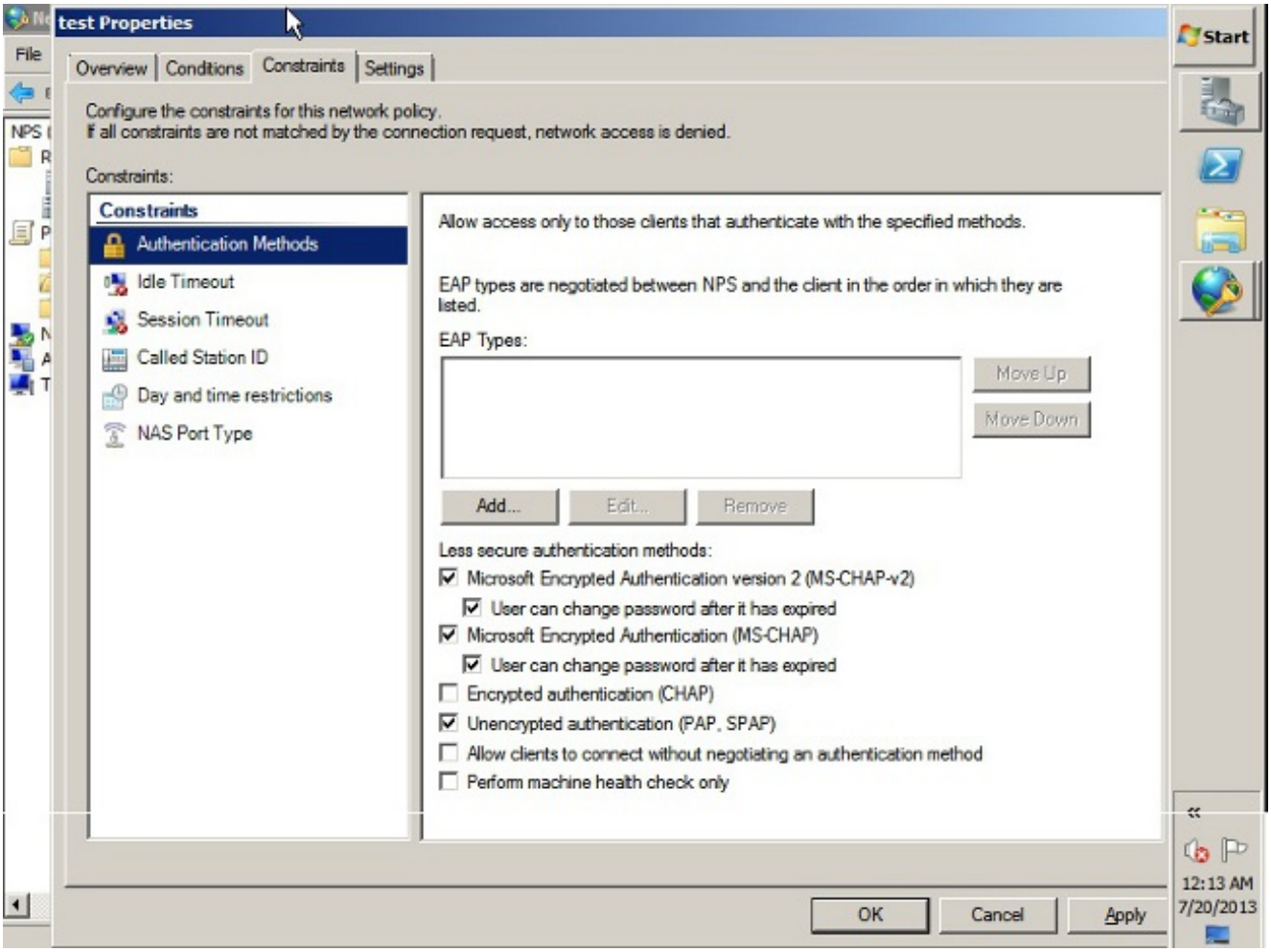
Conditions(조건) 탭을 클릭합니다.Add(**추가)를 클릭합니다**.ASA의 IP 주소를 클라이언트 IPv4 주소 조건으로 입력합니다.VPN 사용자를 포함하는 Active Directory 사용자 그룹을 입력합니다

.



구속 탭을 **클릭합니다**.Authentication **Methods를 선택합니다**.Unencrypted authentication (PAP, SPAP) 확인란을 선택합니다.**확인**을 **클릭합니다**

.

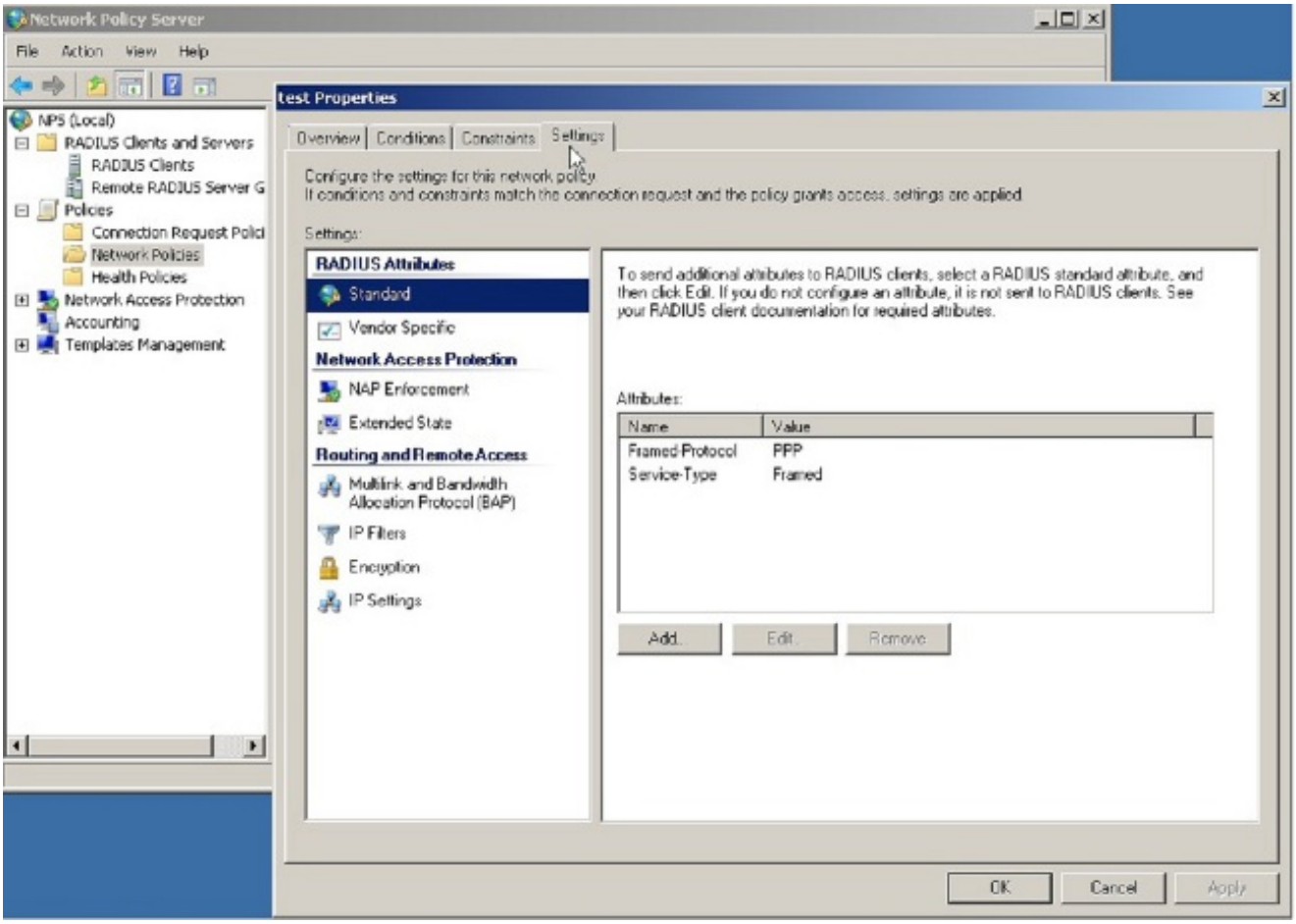


NPS RADIUS 서버에서 그룹 정책 특성(특성 25) 전달

NPS RADIUS 서버를 사용하여 동적으로 사용자에게 그룹 정책을 할당해야 하는 경우 그룹 정책 RADIUS 특성(특성 25)을 사용할 수 있습니다.

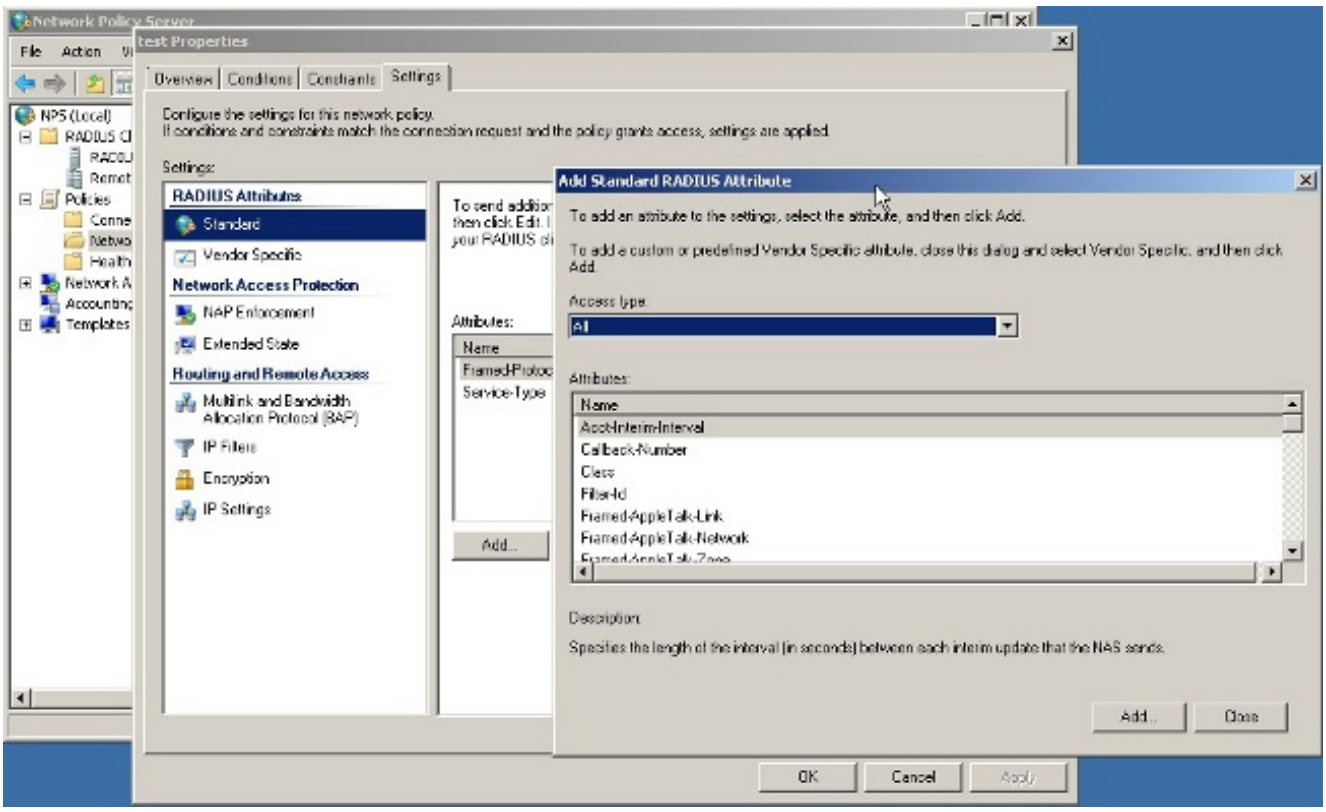
그룹 정책의 동적 할당을 위해 RADIUS 특성 25를 사용자에게 전송하려면 다음 단계를 완료합니다.

1. 네트워크 정책을 추가한 후 필요한 네트워크 정책을 마우스 오른쪽 버튼으로 클릭하고 **설정** 탭을 클릭합니다
   .



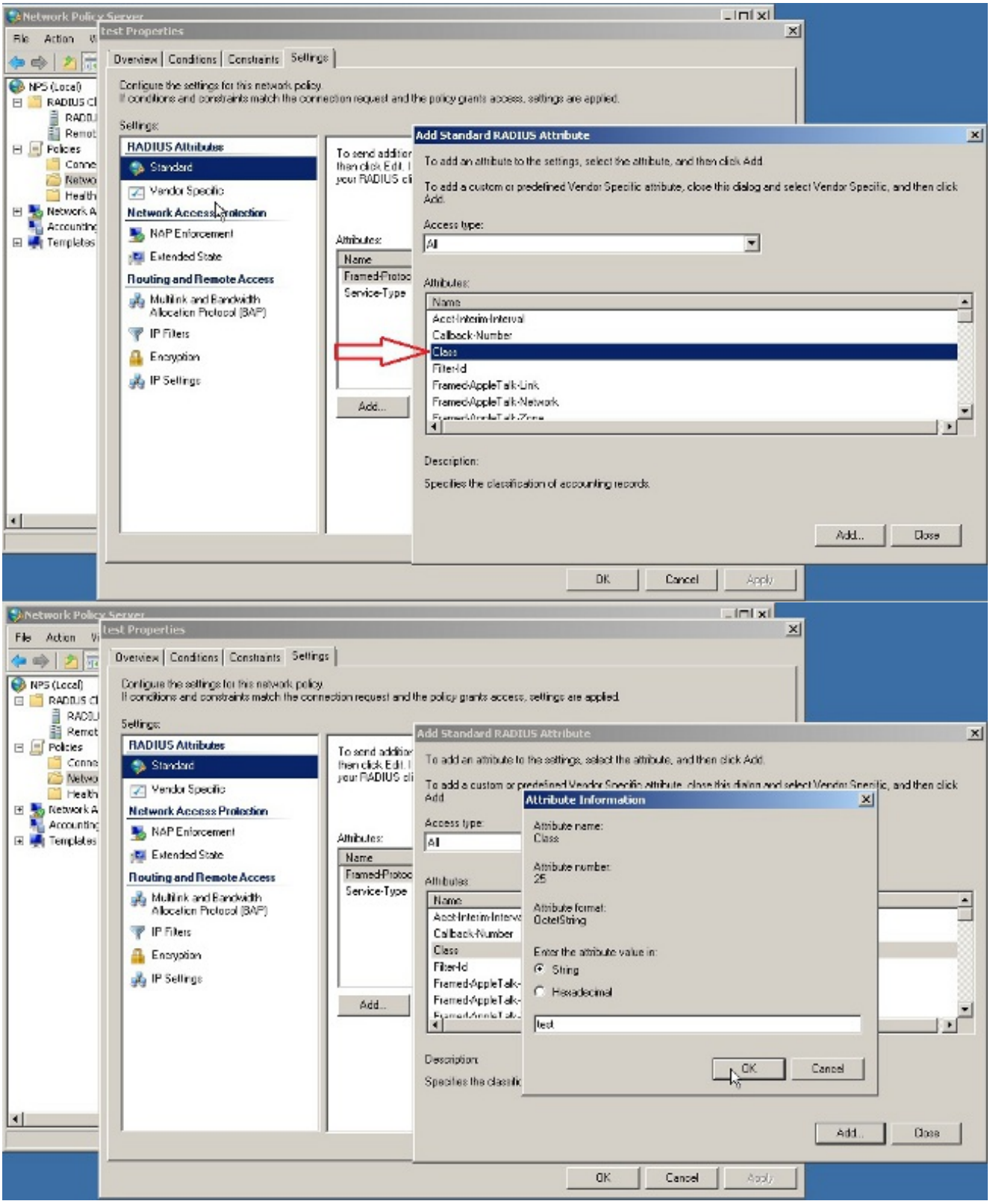
2. RADIUS **Attributes > Standard를 선택합니다**.Add(**추가)를 클릭합니다**.액세스 유형을 All로 둡니다

.



3. 속성 상자에서 **클래스**를 선택하고 **추가**를 클릭합니다.속성 값, 즉 그룹 정책의 이름을 문자열로 입력합니다.이 이름의 그룹 정책은 ASA에서 구성해야 합니다.이는 ASA가 RADIUS 응답에서 이 특성을 수신한 후 VPN 세션에 ASA가 이를 할당하기 때문입니다

.



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

참고:debug 명령을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

ASA 디버그

ASA**에서 디버그 반경**을 활성화합니다.

```
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
```

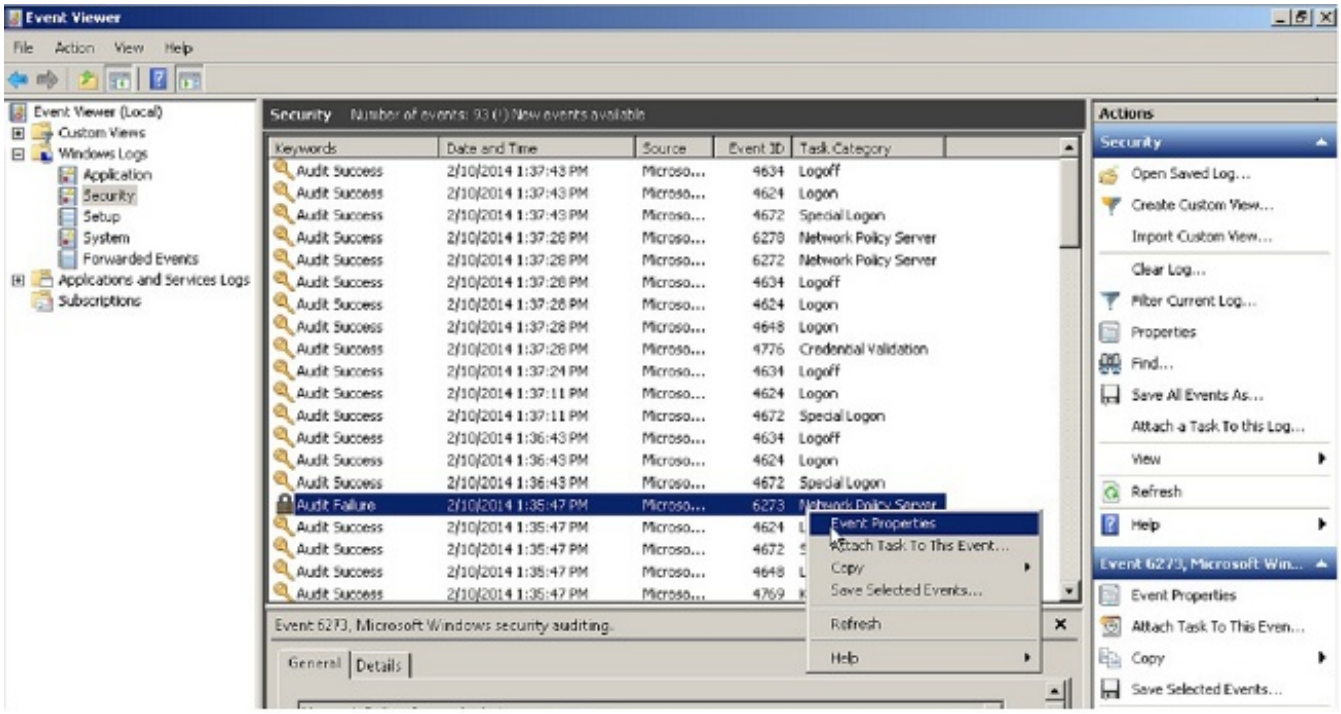
```
    type 1

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
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

- ASA와 NPS 서버 간의 연결이 정상인지 확인합니다.패킷 캡처를 적용하여 인증 요청이 ASA 인터페이스(서버에서 연결할 수 있는 위치)를 벗어나게 합니다. 경로의 디바이스가 NPS 서버에 도달하도록 UDP 포트 1645(기본 RADIUS 인증 포트)를 차단하지 않는지 확인합니다.ASA의 패킷 캡처에 대한 자세한 내용은 ASA/PIX/FWSM에서 확인할 수 있습니다.CLI 및 ASDM 컨피그레이션을 사용하여 패킷 캡처.
- 인증이 계속 실패하면 Windows NPS의 이벤트 뷰어에서 확인하십시오.Event Viewer(이벤트 뷰어) > Windows Logs(Windows 로그)에서 Security(**보안)를** 선택합니다.인증 요청 시간에 NPS와 연결된 이벤트를 찾습니다

  .



Event Properties(이벤트 속성)를 연 후에는 예와 같이 실패 사유를 볼 수 있어야 합니다.이 예에서 PAP는 Network policy(네트워크 정책)에서 인증 유형으로 선택되지 않았습니다.따라서 인증 요청이 실패합니다.

```
 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.**