مصادقة المستخدم ASA VPN مقابل خادم Windows 2008 NPS (Active Directory) مع مثال تكوين RADIUS

المحتويات

المقدمة

يشرح هذا المستند كيفية تكوين جهاز أمان متكيف (ASA) للاتصال بخادم نهج الشبكة (NPS) لنظام التشغيل Microsoft Windows 2008 مع بروتوكول RADIUS حتى تتم مصادقة مستخدمي Cisco VPN Client/AnyConnect/ClientVPN المتواردين مقابل Active Directory. NPS هو أحد أدوار الخادم التي يوفرها Windows 2008 Server. وهو مكافئ ل IAS، Windows 2003 Server (خدمة مصادقة الإنترنت)، وهو تنفيذ خادم RADIUS لتوفير مصادقة مستخدم الطلب الهاتفي عن بعد. وعلى نحو مماثل، في Windows 2008 Server، يمثل NPS تنفيذ خادم RADIUS. أساسا، ASA هو عميل RADIUS لخادم NPS RADIUS. يرسل ASA طلبات مصادقة RADIUS نيابة عن مستخدمي VPN و NPS للمصادقة عليهم مقابل Active Directory.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

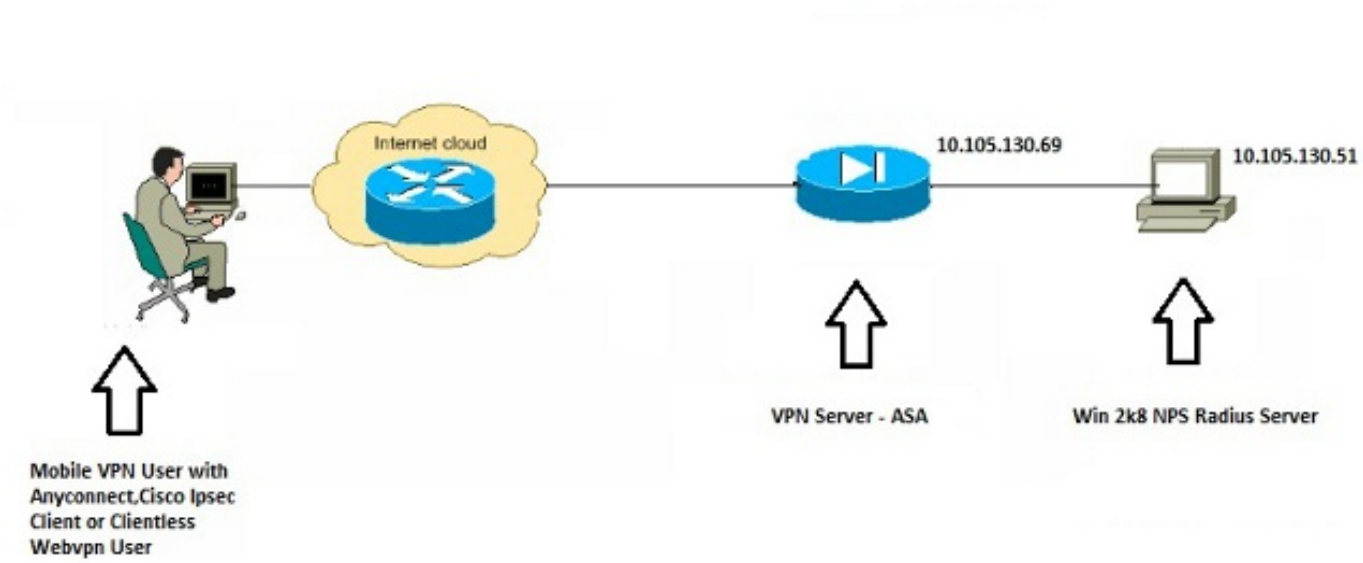
- ASA الذي يشغل الإصدار 9.1(4)
- Windows 2008 R2 Server المثبت عليه خدمات Active Directory ودور NPS

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

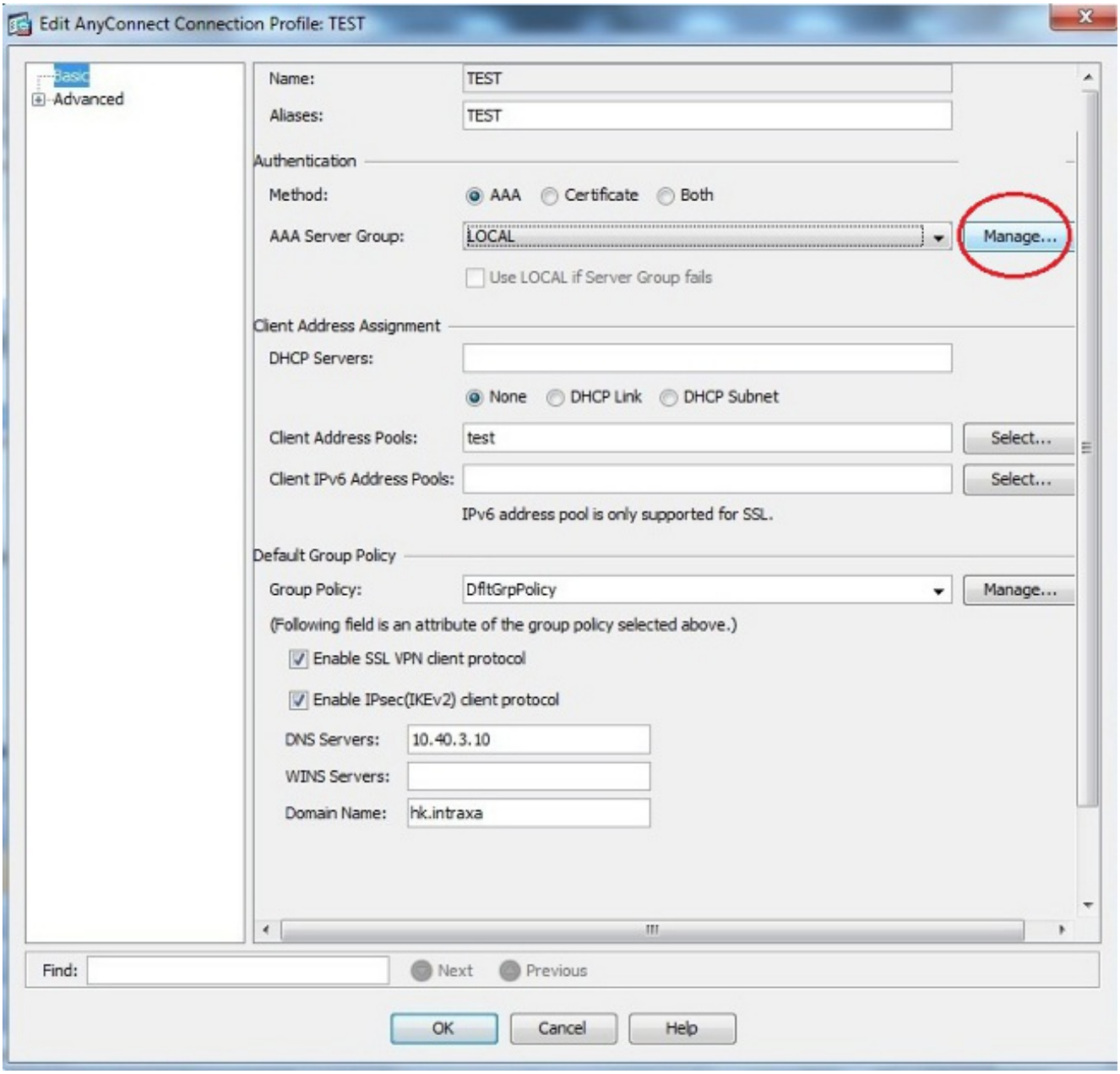
الرسم التخطيطي للشبكة



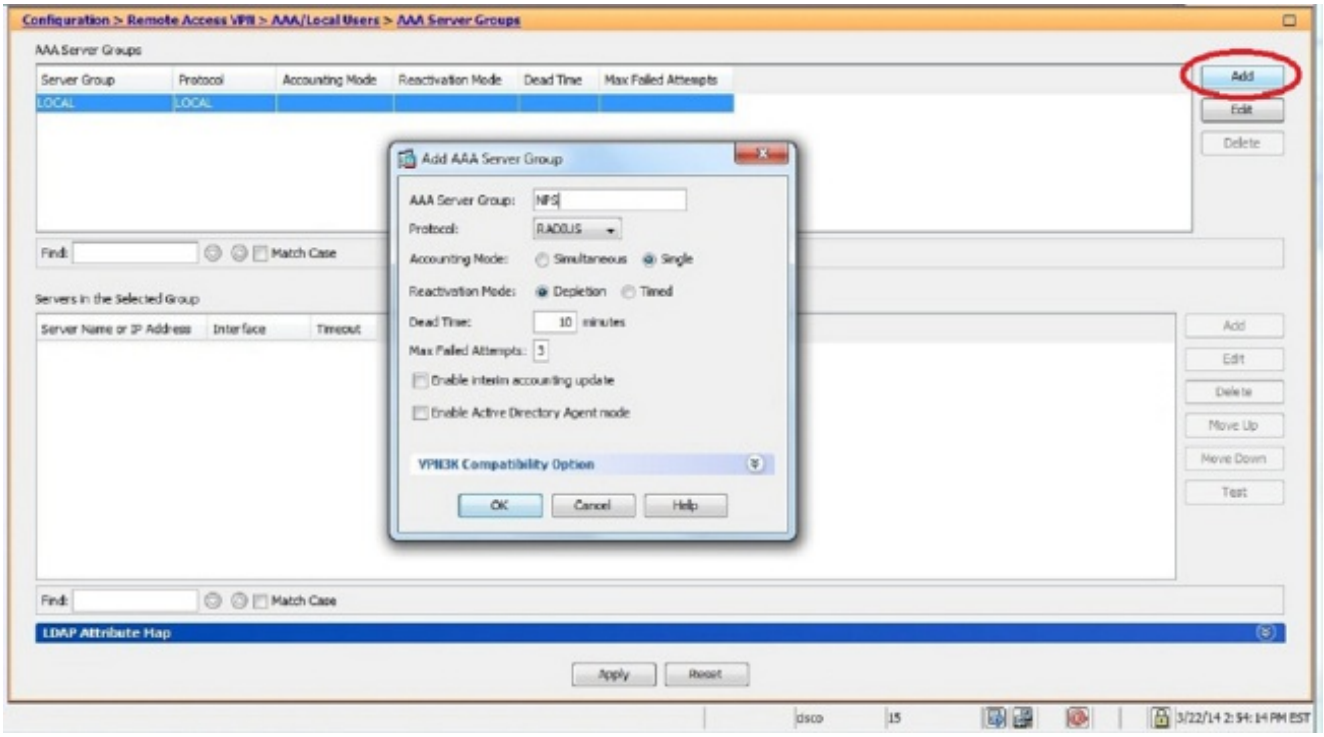
التكوينات

تكوين ASDM

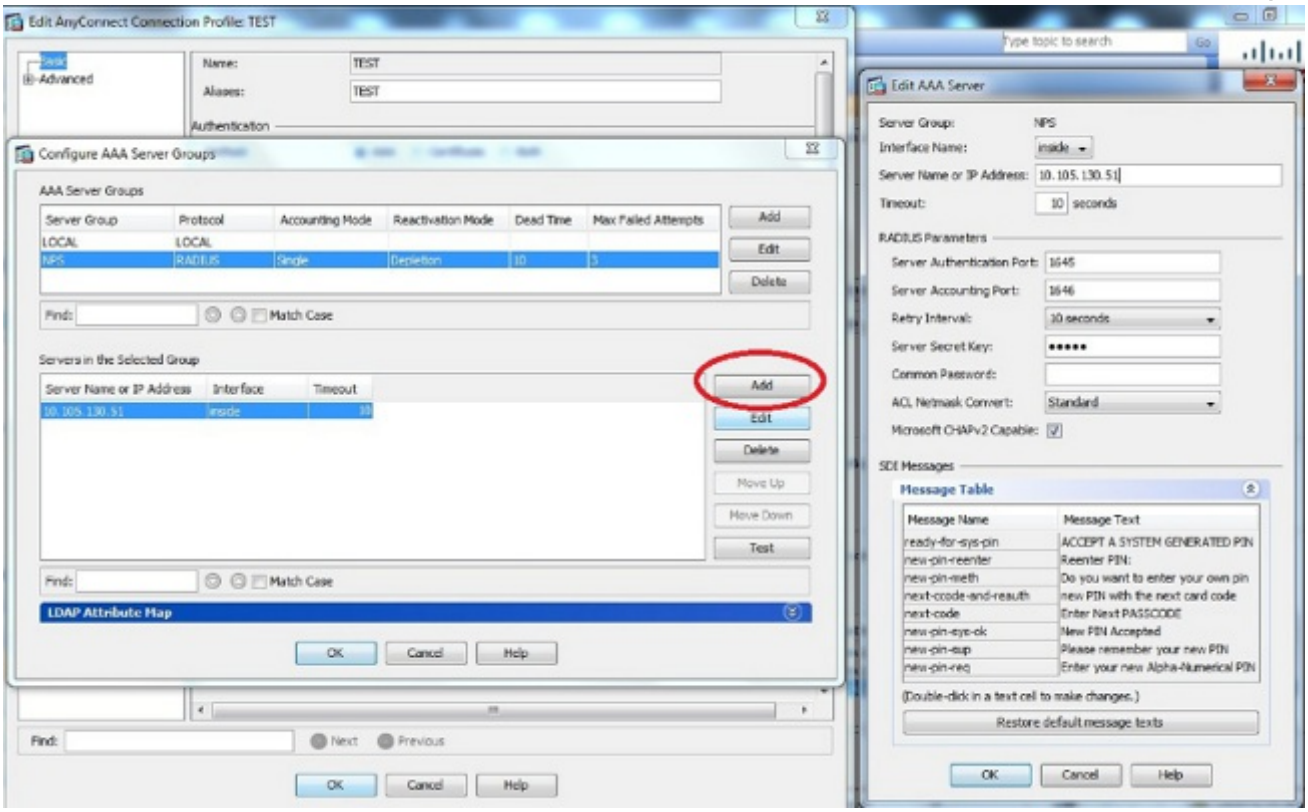
1. أختر مجموعة النفق التي يلزم لها مصادقة NPS.
2. طقطقة **يحرر** واخترت **أساسي**.
3. في قسم المصادقة، انقر على
إدارة.



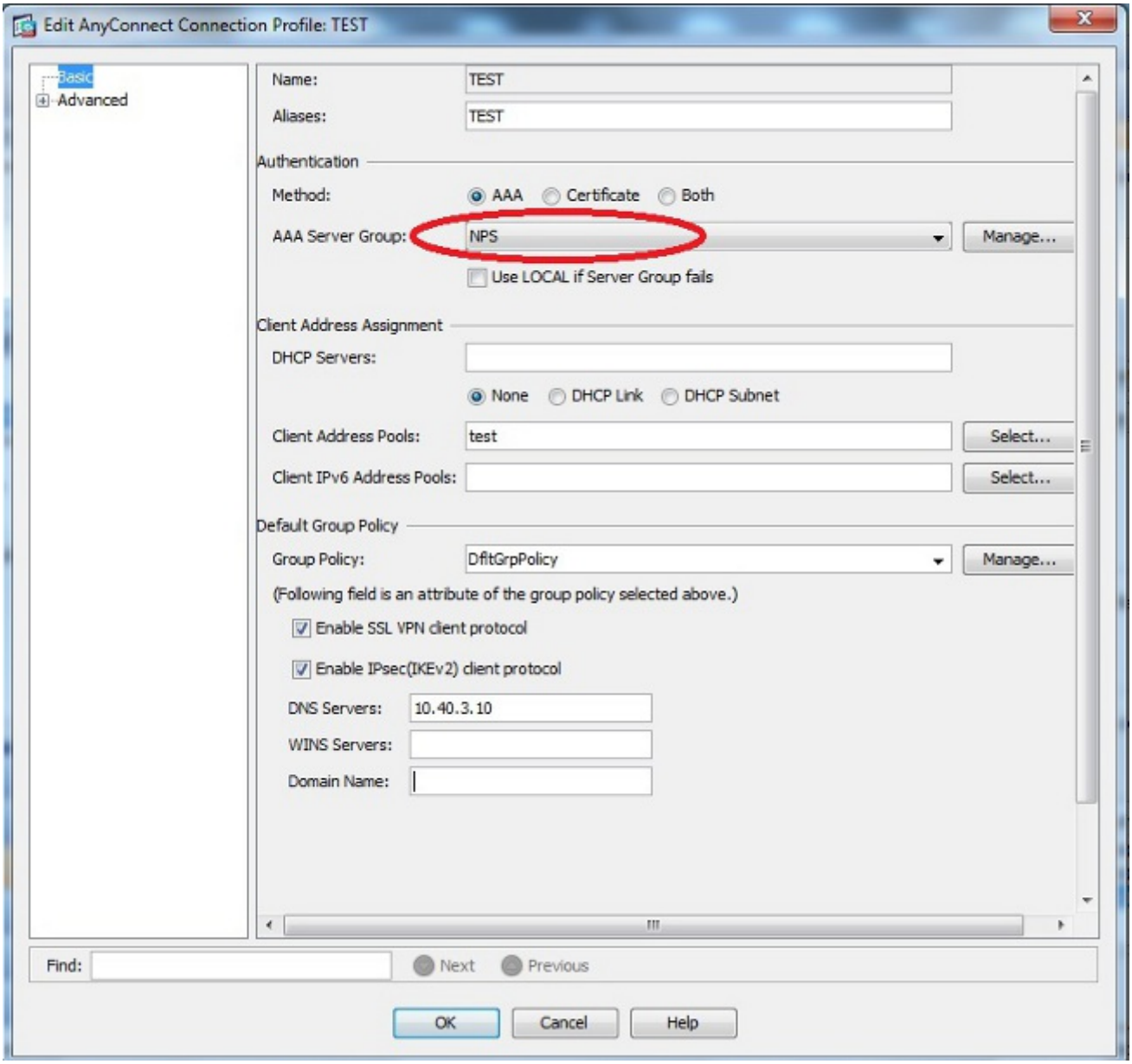
4. في قسم مجموعات خادم AAA، انقر فوق **إضافة**.
5. في حقل مجموعة خوادم AAA، أدخل اسم مجموعة الخوادم (على سبيل المثال، NPS).
6. من القائمة المنسدلة للبروتوكول، أختر **RADIUS**.
7. وانقر فوق
OK.



8. في قسم الخوادم في المجموعة المحددة، أختر مجموعة خوادم AAA التي تمت إضافتها وانقر فوق **إضافة**.
9. في حقل اسم الخادم أو عنوان IP، أدخل عنوان IP الخاص بالخادم.
10. في حقل "مفتاح سر الخادم"، أدخل المفتاح السري.
11. أترك منفذ مصادقة الخادم وحقول منفذ محاسبة الخادم عند القيمة الافتراضية ما لم يستمع الخادم إلى منفذ مختلف.
12. وانقر فوق OK.
13. وانقر فوق
OK.



14. من القائمة المنسدلة لمجموعة خوادم AAA، أختر المجموعة (مصادر الشبكة (NPS) في هذا المثال) التي تمت إضافتها في الخطوات السابقة.
15. وانقر فوق
OK.



تكوين واجهة سطر الأوامر (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
```

وبشكل افتراضي، يستخدم ASA نوع مصادقة بروتوكول مصادقة كلمة المرور (PAP) غير المشفر. لا يعني ذلك أن ال ASA يرسل الكلمة في نص عادي عندما يرسل هو ال radius طلب ربط. وبدلا من ذلك، يتم تشفير كلمة مرور النص العادي باستخدام سر RADIUS المشترك.

إذا تم تمكين إدارة كلمة المرور ضمن مجموعة النفق، فعندئذ يستخدم ASA نوع مصادقة MSCHAP-V2 لتشفير كلمة مرور النص العادي. في مثل هذه الحالة، تأكد من تحديد خانة الاختيار **قدرة Microsoft CHAPv2** في نافذة Edit AAA Server التي تم تكوينها في قسم تكوين ASDM.

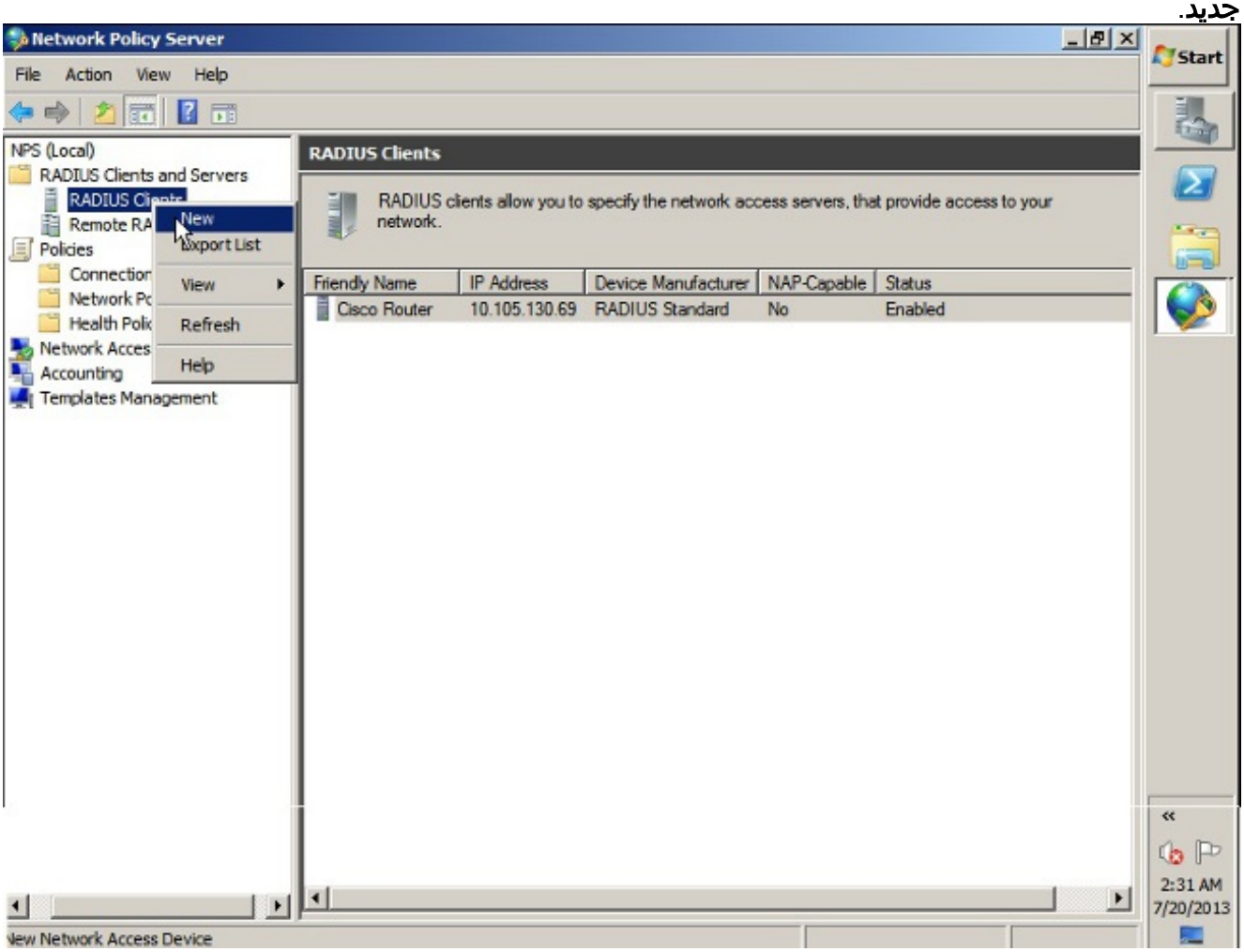
```
tunnel-group TEST general-attributes
                                        address-pool test
                                authentication-server-group (inside) NPS
                                        password-management
```

ملاحظة: يستخدم أمر **مصادقة AAA-Server** دائما PAP. لا يستخدم ASA MSCHAP-V2 إلا عندما يقوم المستخدم بتهيئة اتصال بمجموعة النفق مع تمكين إدارة كلمة المرور. أيضا، ال 'كلمة إدارة [كلمة مرور-تنتهي في يوم]' ساندت خيار فقط مع خفيف وزن دليل منفذ بروتوكول (LDAP). لا يوفر RADIUS هذه الميزة. سترى خيار انتهاء صلاحية كلمة المرور عندما تكون كلمة المرور منتهية الصلاحية بالفعل في Active Directory.

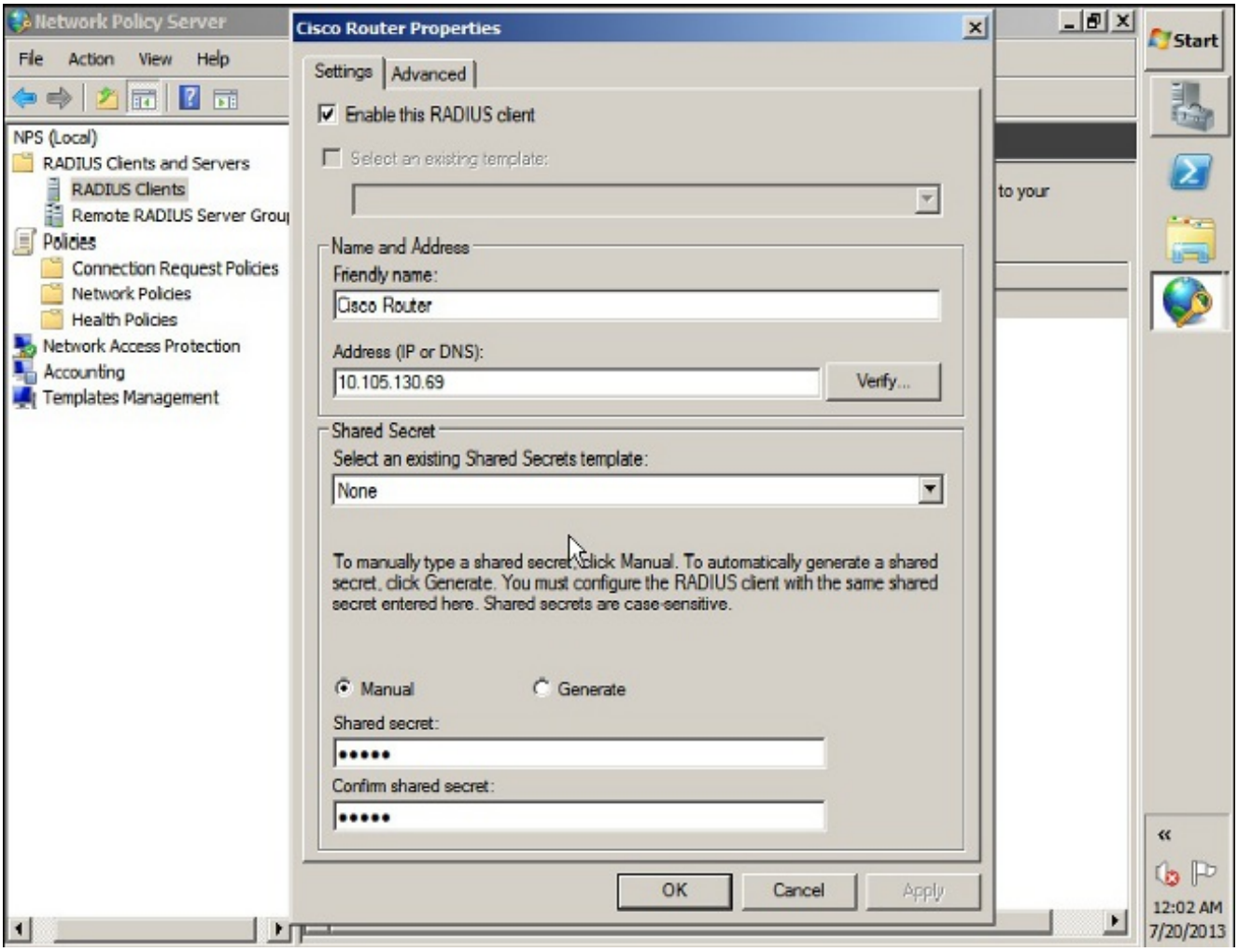
Windows 2008 Server مع تهيئة NPS

يجب تثبيت "دور خادم NPS" وتشغيله على خادم Windows 2008. إذا لم تكن هناك مساحة، أختر **ابدأ > أدوات إدارية > أدوار الخادم > إضافة خدمات الأدوار**. أختر "خادم نهج الشبكة" وقم بتثبيت البرنامج. بمجرد تثبيت دور خادم NPS، أكمل الخطوات التالية لتكوين NPS لقبول طلبات مصادقة RADIUS ومعالجتها من ASA:

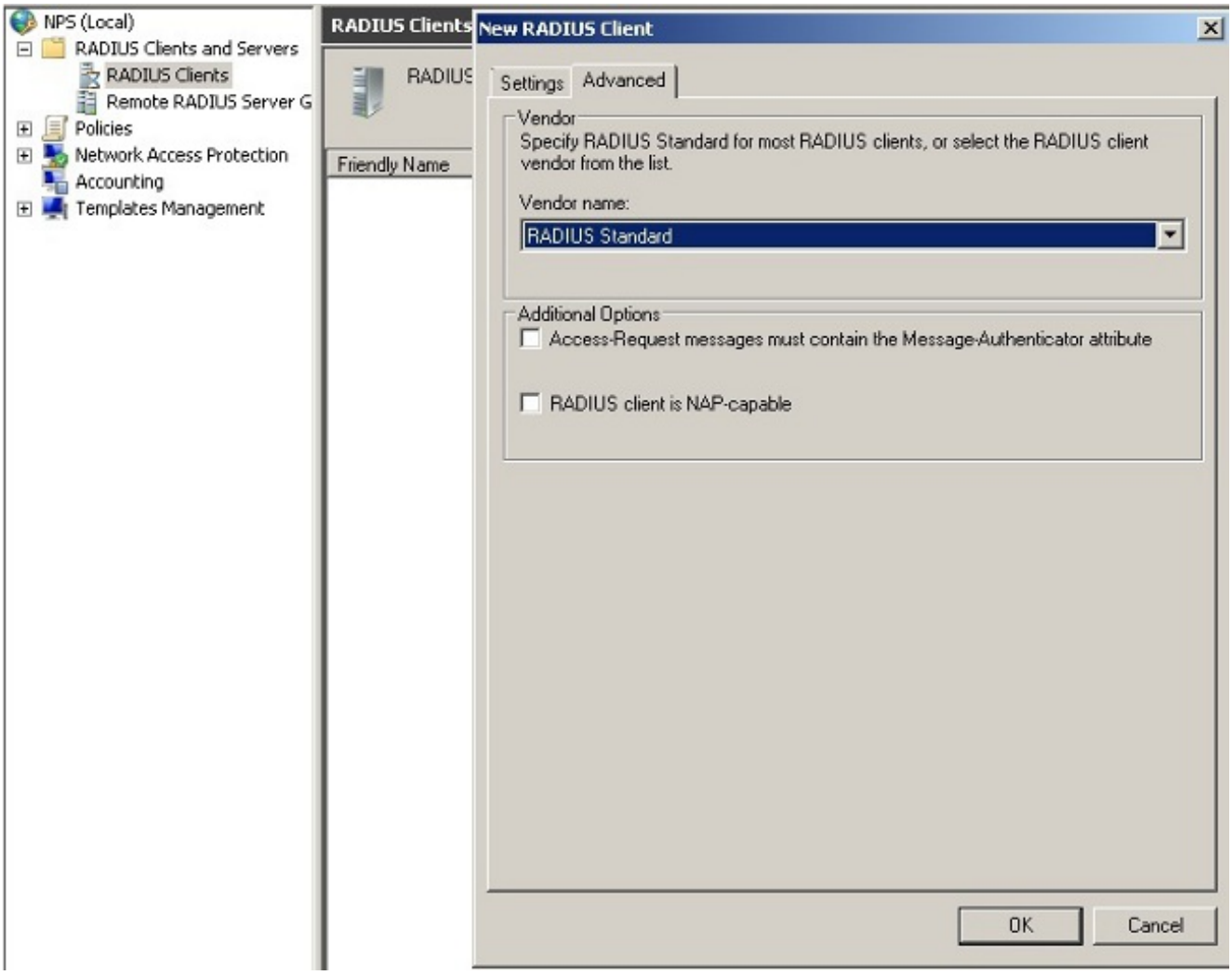
1. إضافة ASA كعميل RADIUS في خادم NPS. أختر **أدوات إدارية > خادم نهج الشبكة**.انقر بزر الماوس الأيمن فوق **عملاء RADIUS** واختر **جديد**.



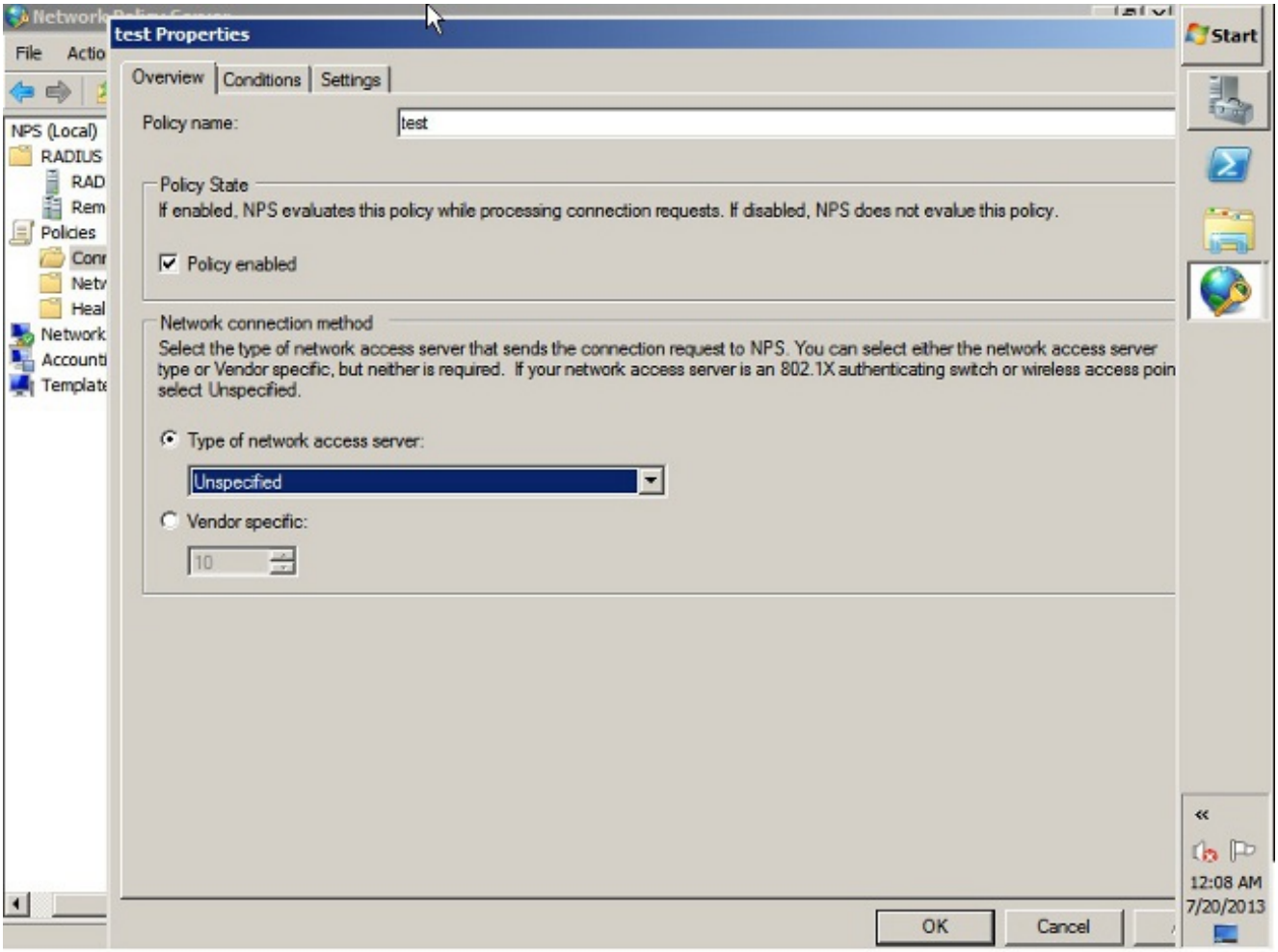
أدخل اسما مألوفا وعنوانا (IP أو DNS) وسرا مشتركا تم تكوينه على ASA.



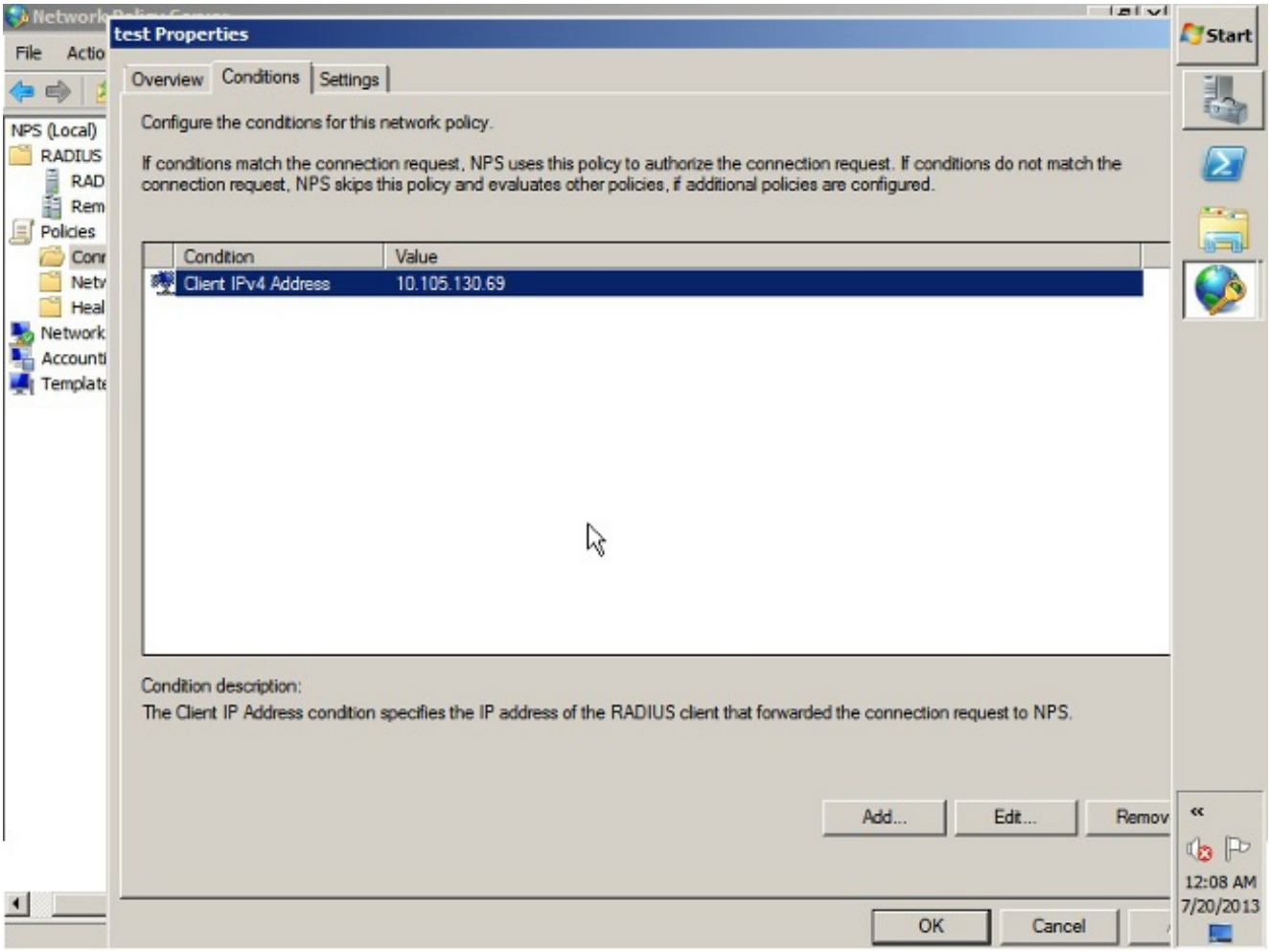
انقر فوق علامة التبويب **خيارات متقدمة**.من القائمة المنسدلة اسم المورد، أختر **معيار RADIUS**.وانقر فوق **OK**.



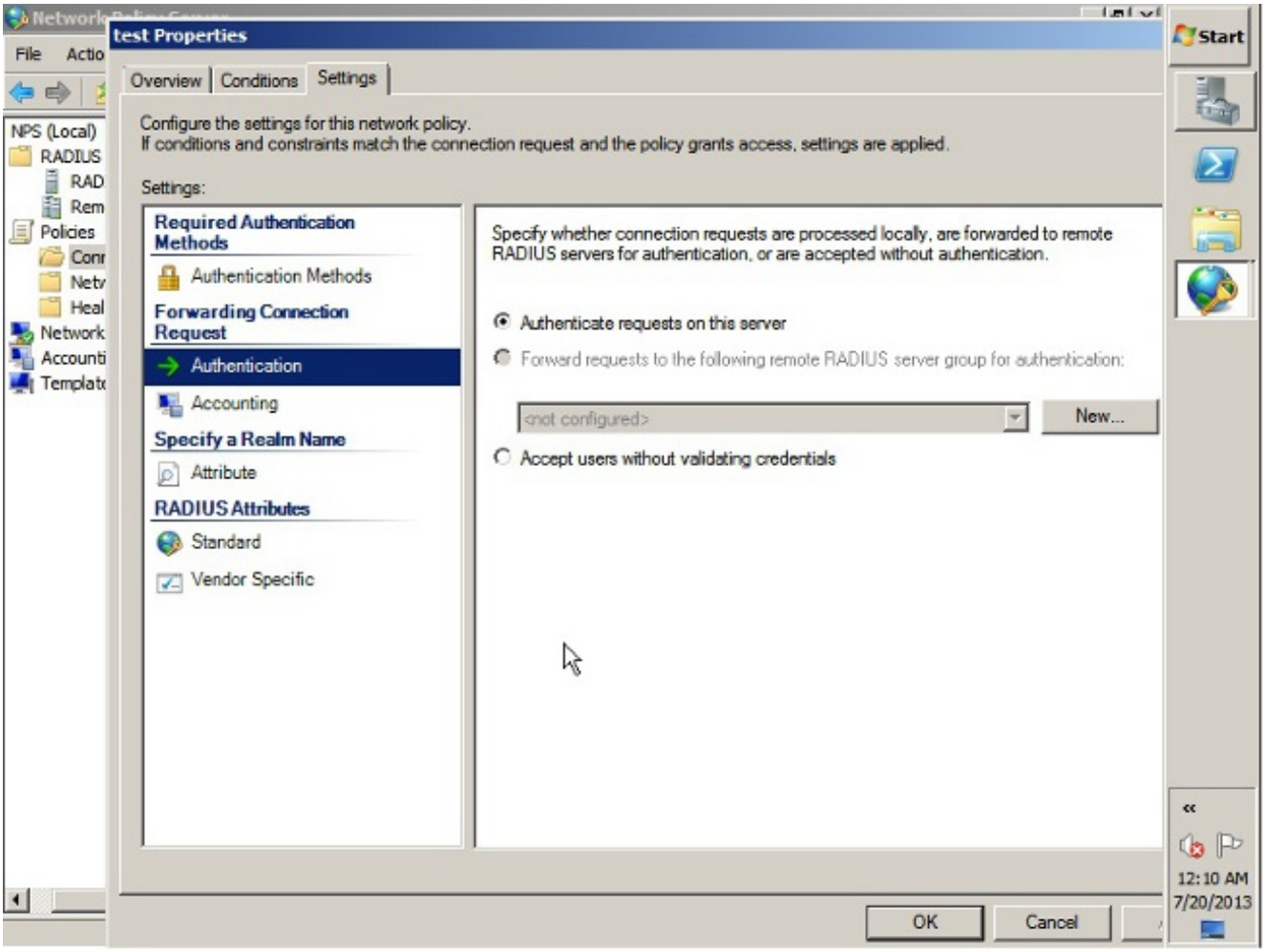
2. إنشاء نهج جديد لطلب الاتصال لمستخدمي VPN. الغرض من نهج "طلب الاتصال" هو تحديد ما إذا كانت الطلبات من عملاء RADIUS ستتم معالجتها محليا أو إعادة توجيهها إلى خوادم RADIUS البعيدة. تحت NPS > السياسات، انقر بزر الماوس الأيمن فوق **نهج طلب الاتصال** وقم بإنشاء سياسة جديدة.من نوع القائمة المنسدلة لخادم الوصول إلى الشبكة، أختر **غير محدد**.



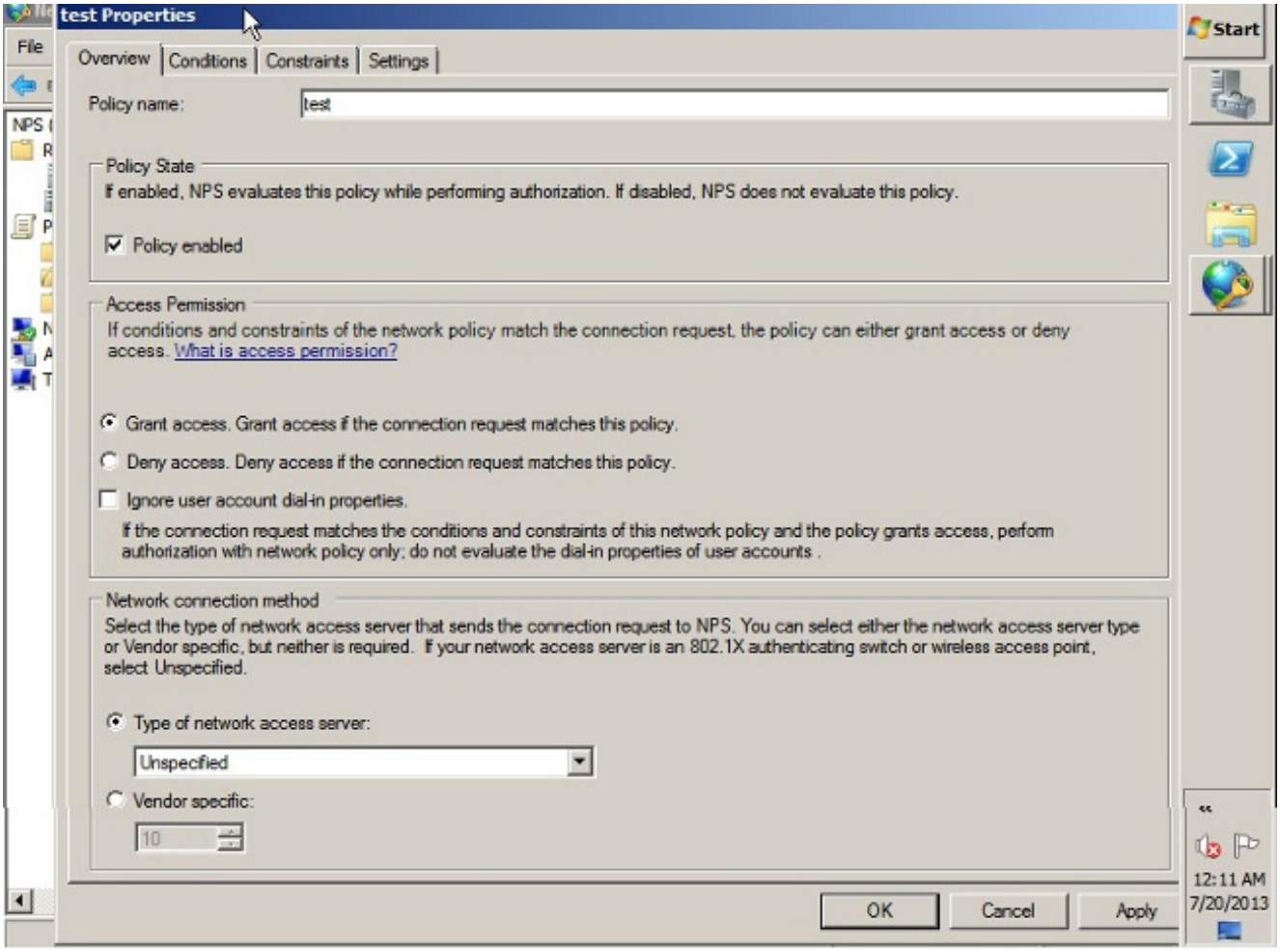
انقر على علامة التبويب **الشروط**.انقر فوق **إضافة (Add)**.أدخل عنوان IP الخاص ب ASA كشرط 'عنوان IPv4 للعميل'.



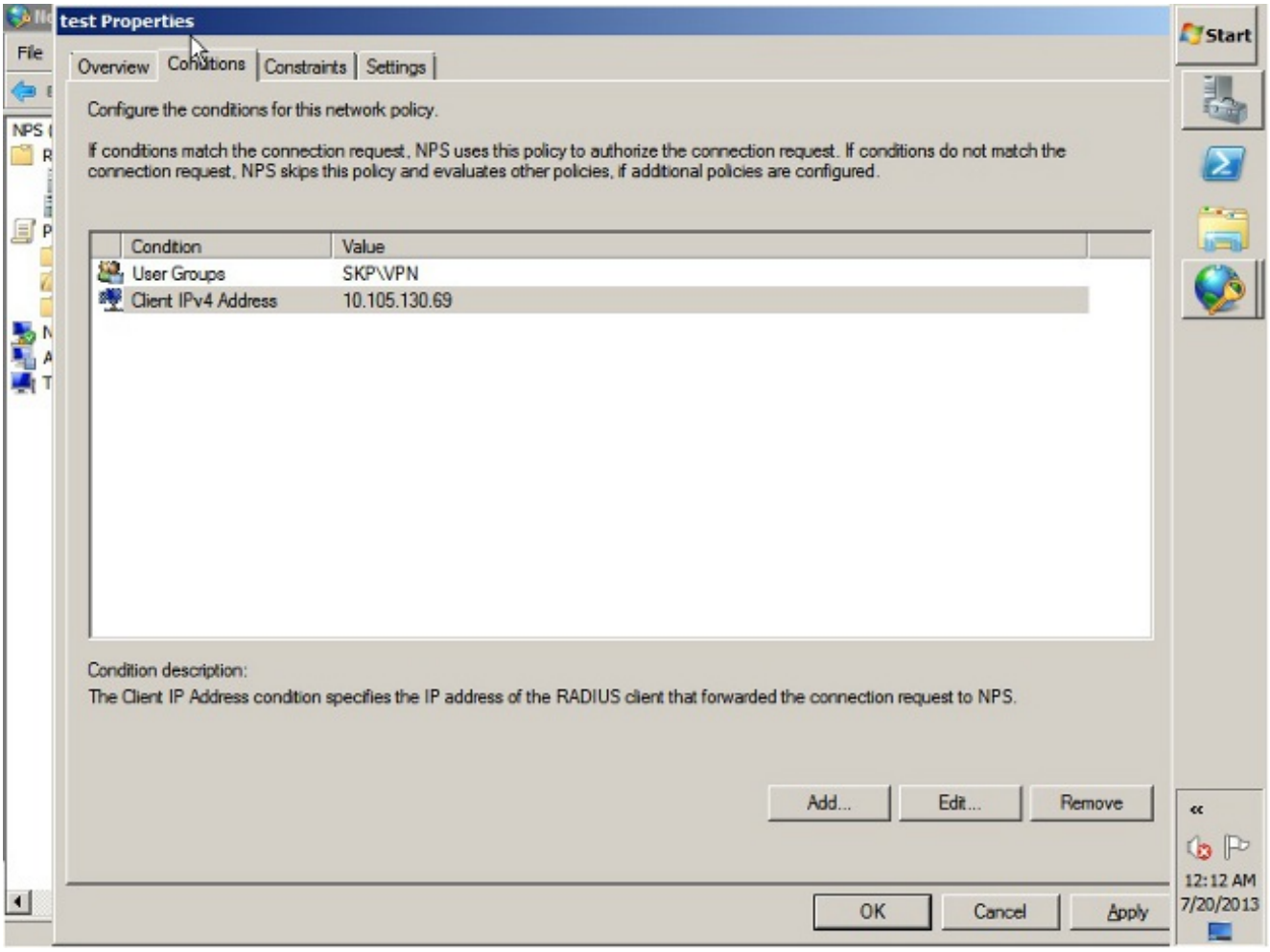
انقر على صفحة **الإعدادات**.أختر **المصادقة** تحت طلب إعادة توجيه الاتصال. تأكد من إختيار طلبات المصادقة على زر الخيار للخادم.وانقر فوق
.**OK**



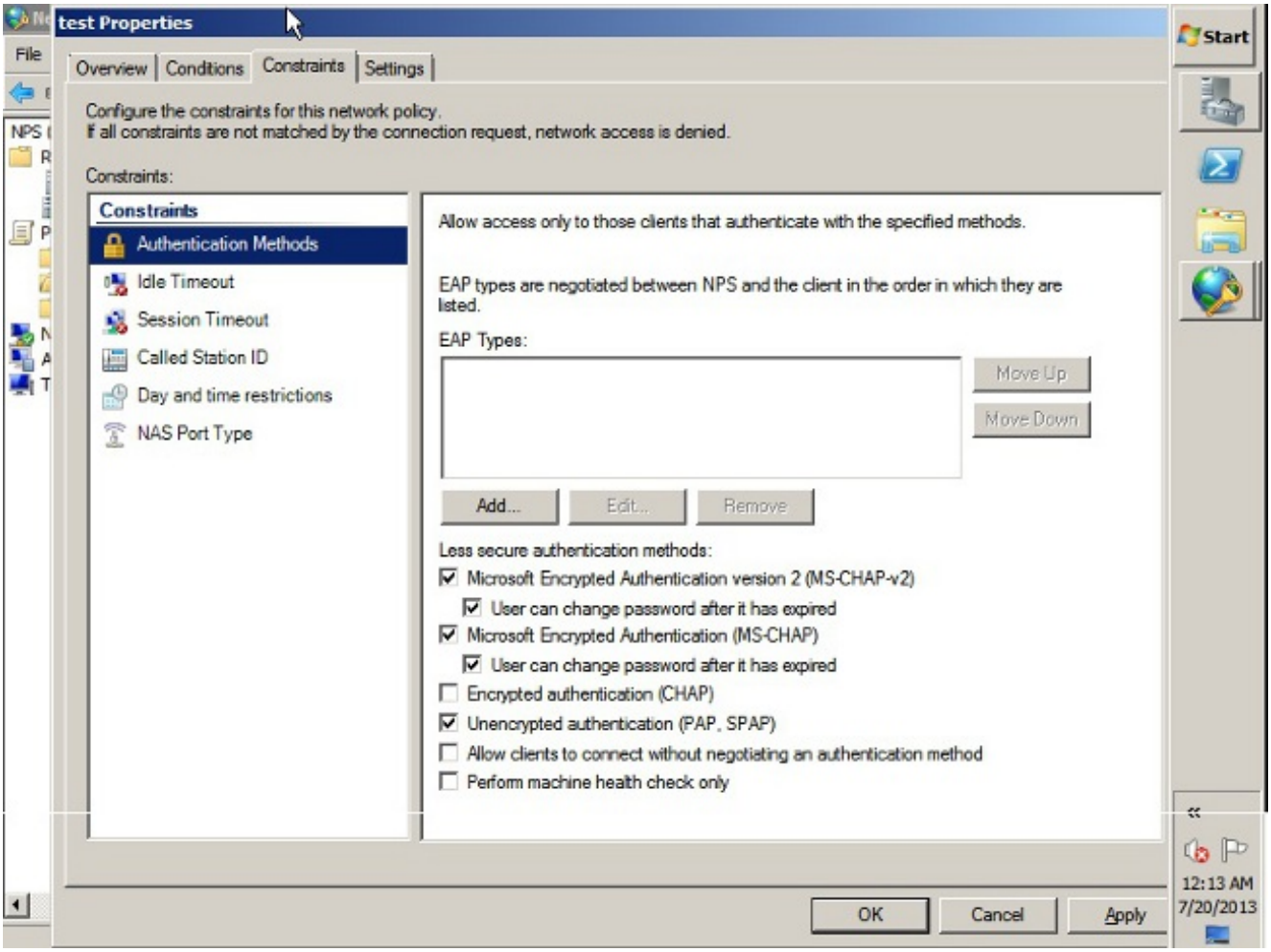
3. إضافة نهج شبكة حيث يمكنك تحديد المستخدمين المسموح لهم بالمصادقة.على سبيل المثال، يمكنك إضافة مجموعات مستخدمي Active Directory كشرط. تتم مصادقة أولئك المستخدمين الذين ينتمون إلى مجموعة Windows محددة فقط بموجب هذا النهج.تحت NPS، أختر **السياسات**.انقر بزر الماوس الأيمن فوق **نهج الشبكة** وقم بإنشاء نهج جديد.تأكد من إختيار الزر "منح حق الوصول".من نوع القائمة المنسدلة لخادم الوصول إلى الشبكة، أختر **غير محدد**.



انقر على علامة التبويب **الشروط**.انقر فوق **إضافة (Add)**.أدخل عنوان IP الخاص ب ASA كحالة عنوان IPv4 للعميل.أدخل مجموعة مستخدمي Active Directory التي تحتوي على مستخدمي VPN.



انقر فوق علامة التبويب **القيود**.أختر **طرق المصادقة**.تأكد من تحديد خانة الاختيار المصادقة غير المشفرة (PAP، SPAP).وانقر فوق
OK.

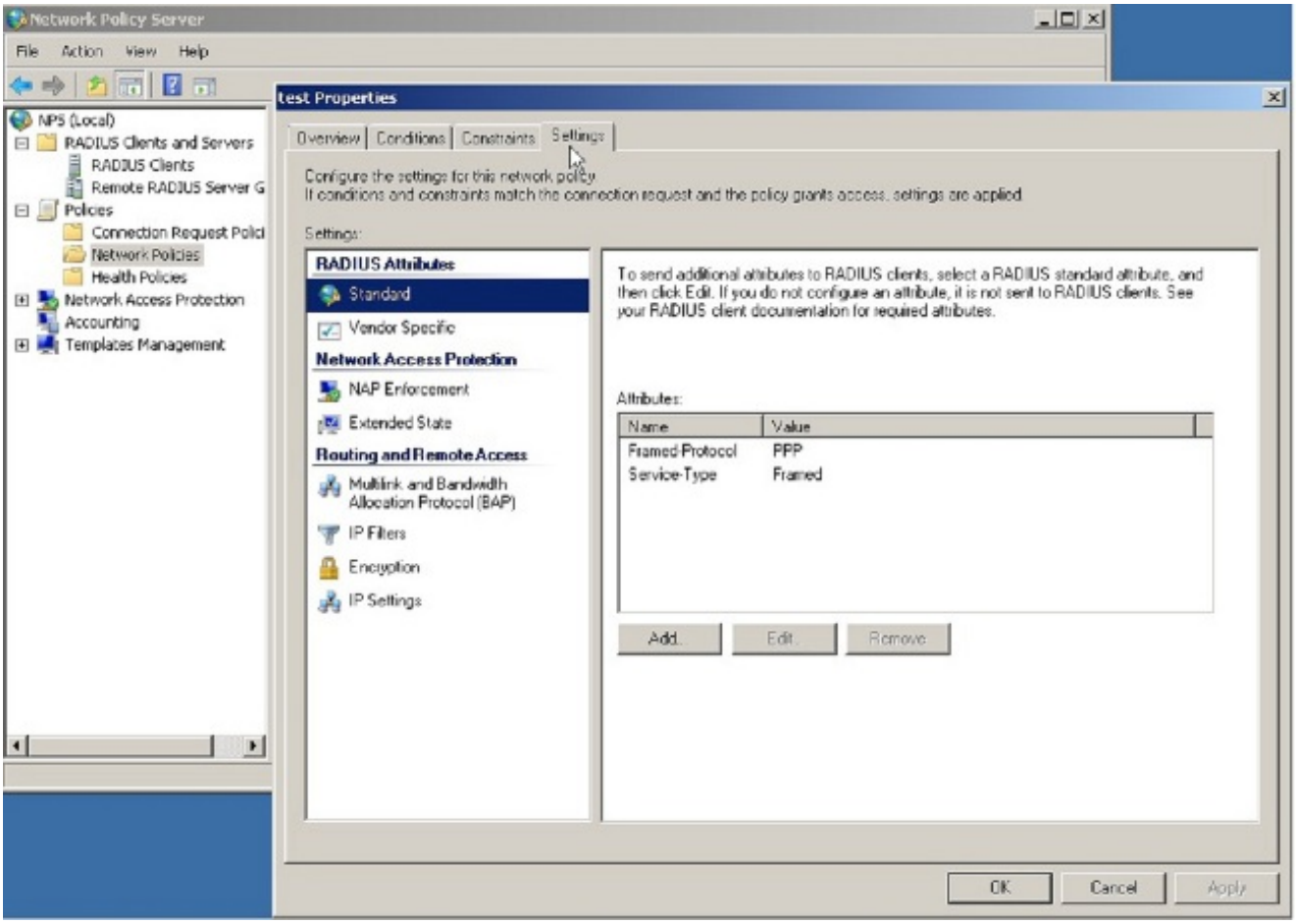


تمرير سمة نهج المجموعة (السمة 25) من خادم NPS RADIUS

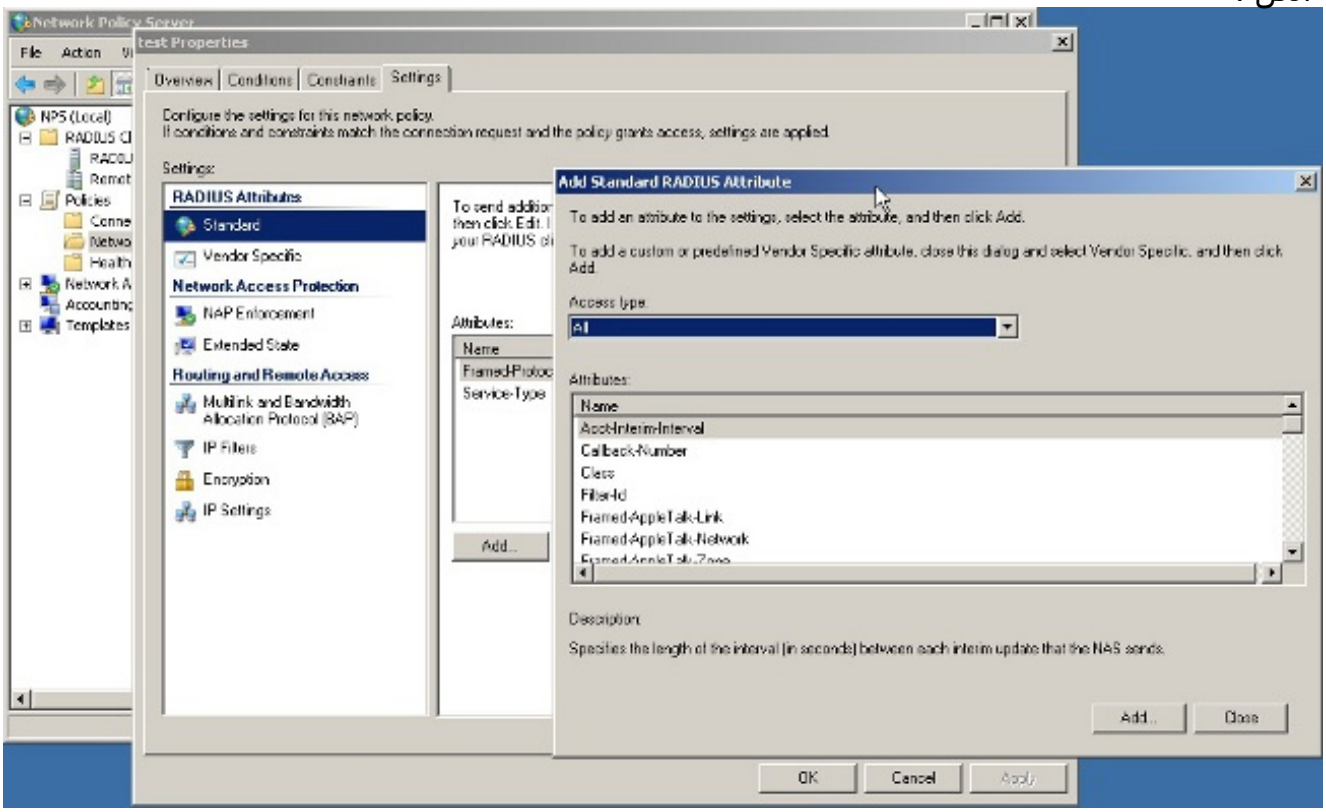
إذا كان نهج المجموعة بحاجة إلى تعيينه للمستخدم بشكل ديناميكي باستخدام خادم NPS RADIUS، يمكن إستخدام سمة RADIUS لنهج المجموعة (السمة 25).

أكمل هذه الخطوات لإرسال سمة RADIUS 25 للتعيين الديناميكي لنهج المجموعة للمستخدم.

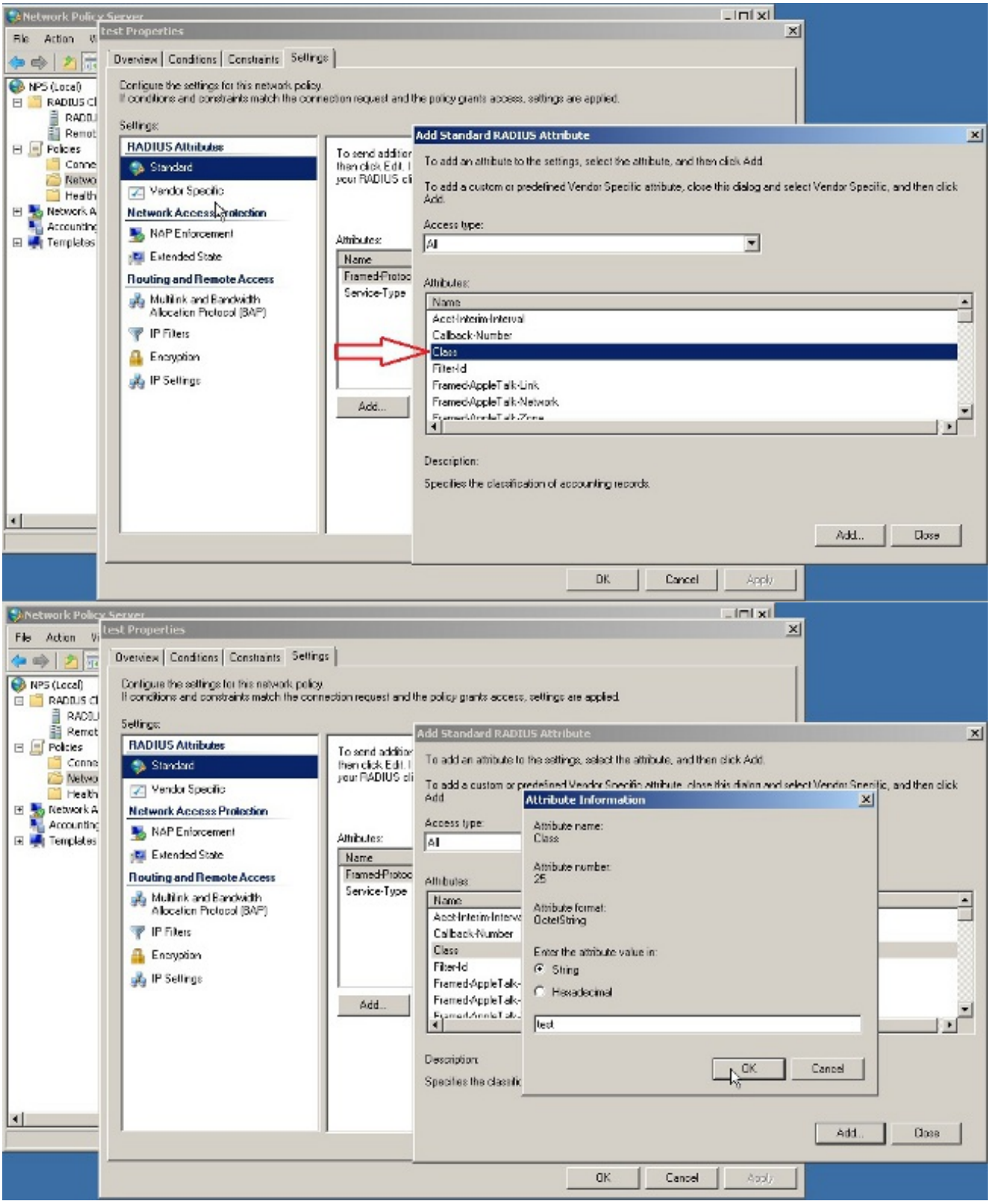
1. بعد إضافة "نهج الشبكة"، انقر بزر الماوس الأيمن فوق "نهج الشبكة" المطلوب وانقر فوق علامة التبويب **إعدادات**.



2. أختر **خصائص RADIUS > قياسية**. انقر فوق **إضافة (Add)**. أترك نوع الوصول "الكل".



3. في مربع الخصائص، أختر **فئة** وانقر **إضافة**. أدخل قيمة السمة، أي اسم نهج المجموعة كسلسلة. تذكر أنه يجب تكوين سياسة مجموعة بهذا الاسم في ASA. هذا حتى أن ASA يقوم بتعيينه إلى جلسة VPN بعد أن يستلم هو هذه السمة في إستجابة RADIUS.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

تصحيح أخطاء ASA

مكنت ASA on the **debug radius all**.

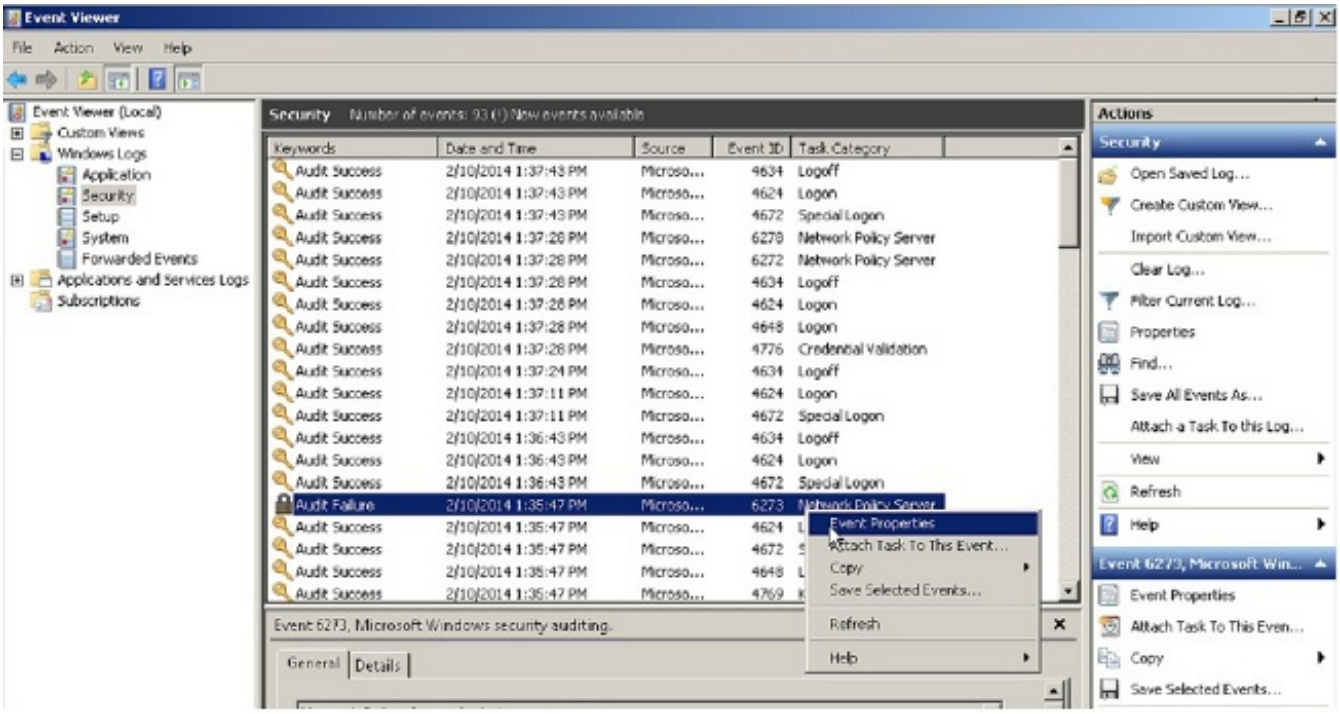
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
 (INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds
                                                    radius mkreq: 0x80000001
                                                       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
  ...c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f    |  ...A.....~m 41 00 08 01
)..a8 36 01 09 76 70 6e 75 73 65 72 02 12 28    |  @P.6..vpnuser 50 40
.c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04    |  .h.........Z.oC
....=........0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00    |  ..i 06
                .  |                                                    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
                        6e 75 73 65 72                              |  vpnuser 70 76
                                             Radius: Type = 2 (0x02) User-Password
                                                     (Radius: Length = 18 (0x12
                                                       = (Radius: Value (String
c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43    |  (.h.........Z.oC 28
                                           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
4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37    |  ...N..Kv ....+.7 00 08 02
............bf 9a 6c 4c 07 06 00 00 00 01 06 06 00 00 00 02    |  ..lL
2e 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a    |  .........7.....j 19
..@...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
:...@...3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a    |  ....<..n 00 00 00 00
    ..........6f 05 81 00 00 00 00 00 00 00 03               |  .o 18
                                                                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
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- تأكد من أن الاتصال بين خادم ASA و NPS جيد.تطبيق التقاط الحزم لضمان أن يترك طلب المصادقة واجهة ASA (من حيث يمكن الوصول إلى الخادم). تأكد من أن الأجهزة الموجودة في المسار لا تمنع منفذ UDP 1645 (منفذ مصادقة RADIUS الافتراضي) لضمان وصوله إلى خادم NPS. يمكن العثور على مزيد من المعلومات حول التقاط الحزم على ASA في ASA/PIX/FWSM: التقاط الحزم باستخدام CLI ومثال تكوين ASDM.
- في حالة إستمرار فشل المصادقة، ابحث في عارض الأحداث على NPS ل Windows. تحت عارض الأحداث > سجلات Windows، أختر **التأمين**. ابحث عن الأحداث المقترنة ب NPS في وقت طلب المصادقة.



بمجرد فتح "خصائص الحدث"، يجب أن تكون قادرا على رؤية سبب الفشل كما هو موضح في المثال. في هذا المثال، لم يتم إختيار PAP كنوع مصادقة ضمن نهج الشبكة. وبالتالي، يفشل طلب المصادقة.

```
                                    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 -

Accounting information was written to the local log file .Logging Results:

Reason Code: 66

Reason: **The user attempted to use an authentication method that is .not enabled on the matching network policy**

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).