針對使用RADIUS的Windows 2008 NPS伺服器(Active Directory)的ASA VPN使用者身份驗證配置示例

目錄

簡介

本文檔介紹如何配置自適應安全裝置(ASA)以使用RADIUS協定與Microsoft Windows 2008網路策略伺服器(NPS)通訊，以便按照Active Directory對舊版Cisco VPN客戶端/AnyConnect/無客戶端WebVPN使用者進行身份驗證。NPS是Windows 2008 Server提供的伺服器角色之一。它等效於Windows 2003 Server，即IAS（Internet身份驗證服務），IAS是RADIUS伺服器的實現，用於提供遠端撥入使用者身份驗證。同樣，在Windows 2008 Server中，NPS是RADIUS伺服器的實現。一般來說，ASA是NPS RADIUS伺服器的RADIUS客戶端。ASA代表VPN使用者傳送RADIUS身份驗證請求，NPS根據Active Directory對使用者進行身份驗證。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

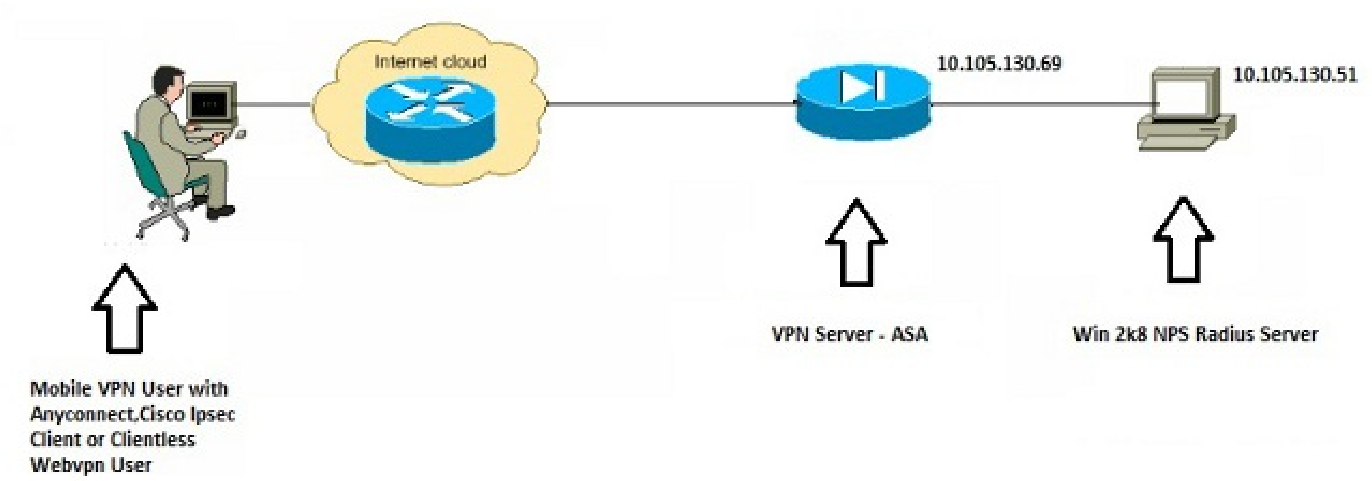
- 運行9.1(4)版的ASA
- 安裝了Active Directory服務和NPS角色的Windows 2008 R2伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

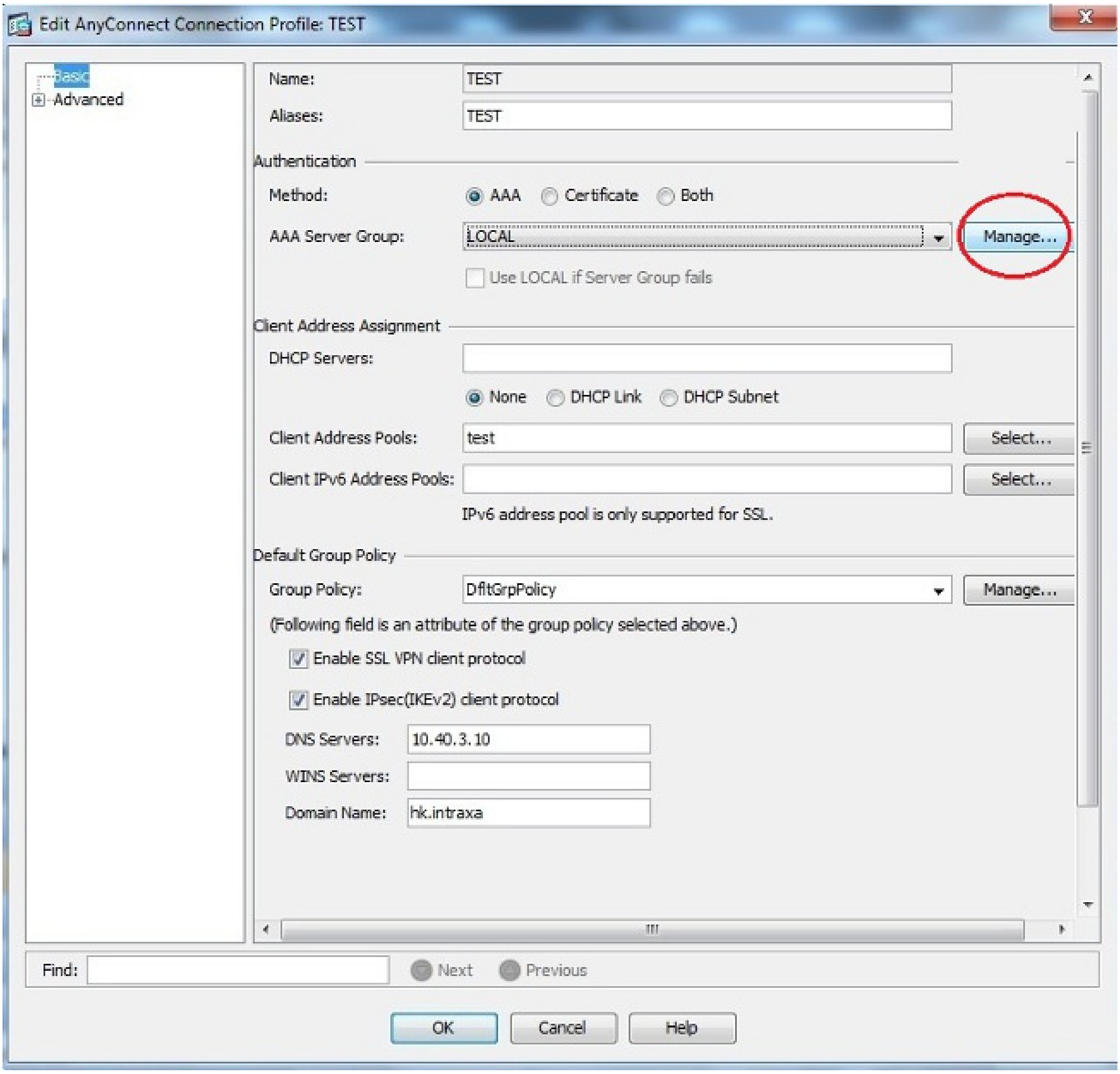
網路圖表


Internet cloud
10.105.130.69
10.105.130.51
Mobile VPN User with Anyconnect,Cisco Ipsec Client or Clientless Webvpn User
VPN Server - ASA
Win 2k8 NPS Radius Server

組態

ASDM配置

1. 選擇需要NPS身份驗證的隧道組。
2. 按一下「**Edit**」，然後選擇「**Basic**」。
3. 在Authentication部分中，按一下**Manage**。



Edit AnyConnect Connection Profile: TEST

Name: TEST

Aliases: TEST

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: LOCAL

□ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: test

Client IPv6 Address Pools:

IPv6 address pool is only supported for SSL.

Default Group Policy

Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

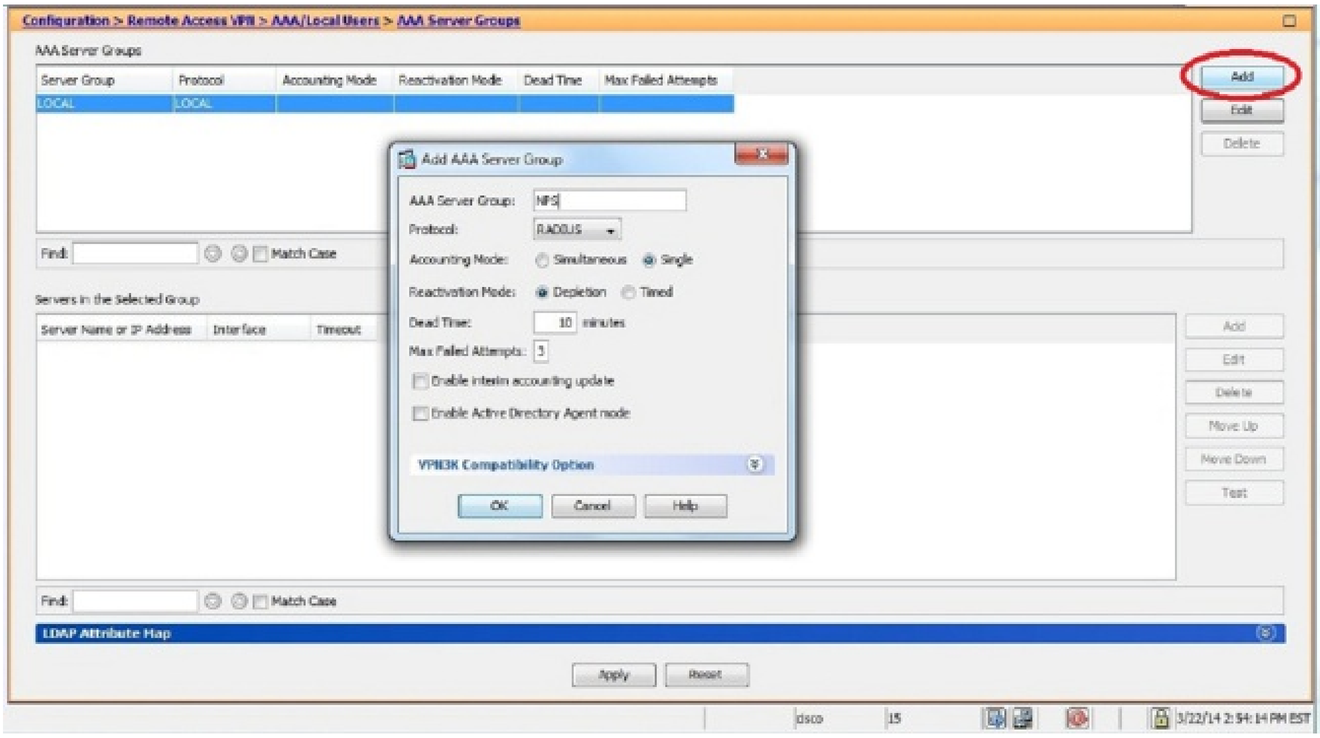
☑ Enable IPsec(IKEv2) client protocol

DNS Servers: 10.40.3.10

WINS Servers:

Domain Name: hk.intraxa

4. 在AAA Server Groups部分，按一下**Add**。
5. 在AAA Server Group欄位中，輸入伺服器組的名稱（例如NPS）。
6. 在「Protocol」下拉式清單中選擇**RADIUS**。
7. 按一下「**OK**」（確定）。



Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				

Add AAA Server Group

AAA Server Group: NPS

Protocol: RADIUS

Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

□ Enable interim accounting update

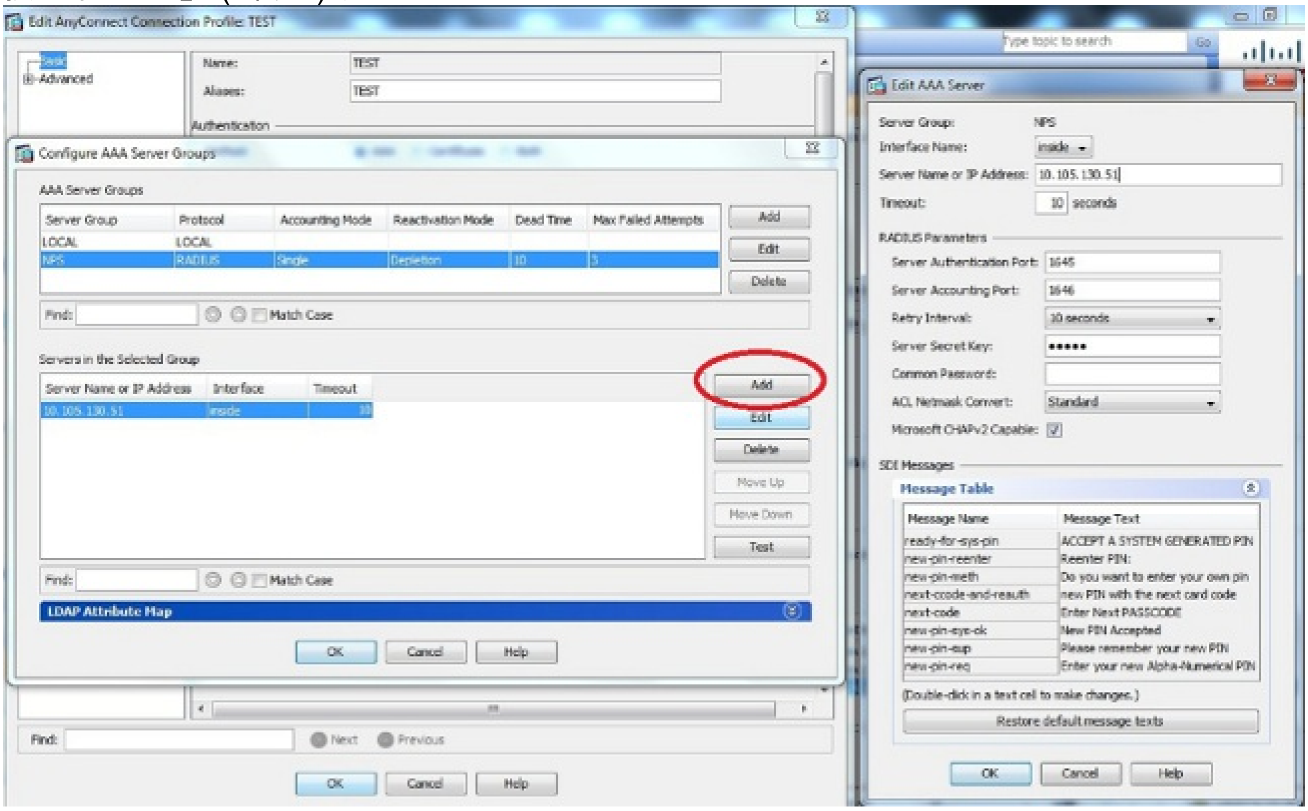
□ Enable Active Directory Agent mode

VPN3K Compatibility Option

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout

8. 在Servers in the Selected Group部分，選擇the AAA Server Group added，然後點選**Add**。
9. 在Server Name or IP Address欄位中，輸入伺服器IP地址。
10. 在「伺服器金鑰」欄位中，輸入金鑰。
11. 將Server Authentication Port和Server Accounting Port欄位保留為預設值，除非伺服器偵聽不同的埠。
12. 按一下「**OK**」（確定）。
13. 按一下「**OK**」（確定）。



Edit AnyConnect Connection Profile: TEST

Name: TEST

Aliases: TEST

Configure AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
LOCAL	LOCAL				
NPS	RADIUS	Single	Depletion	10	3

Servers in the Selected Group

Server Name or IP Address	Interface	Timeout
10.105.130.51	inside	10

Edit AAA Server

Server Group: NPS

Interface Name: inside

Server Name or IP Address: 10.105.130.51

Timeout: 10 seconds

RADIUS Parameters

Server Authentication Port: 1645

Server Accounting Port: 1646

Retry Interval: 10 seconds

Server Secret Key: •••••

Common Password:

ACL Netmask Convert: Standard

Microsoft CHAPv2 Capable: ☑

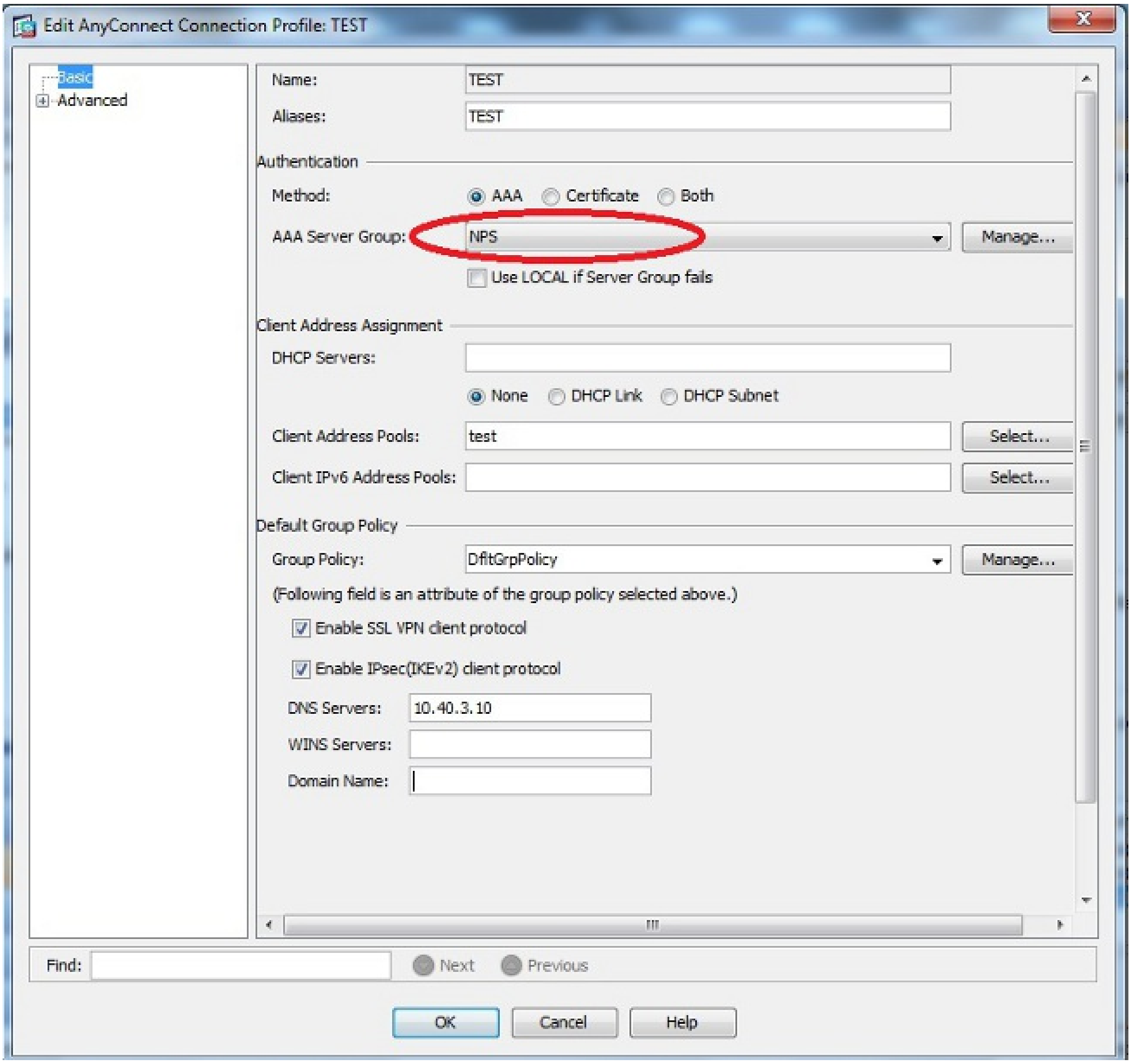
SDI Messages

Message Table

Message Name	Message Text
ready-for-sys-pin	ACCEPT A SYSTEM GENERATED PIN
new-pin-reenter	Reenter PIN:
new-pin-meth	Do you want to enter your own pin
next-code-and-reauth	new PIN with the next card code
next-code	Enter Next PASSCODE
new-pin-sys-ok	New PIN Accepted
new-pin-sup	Please remember your new PIN
new-pin-req	Enter your new Alpha-Numerical PIN

(Double-click in a text cell to make changes.)

14. 從AAA Server Group下拉選單中，選擇前幾個步驟中新增的組（在本示例中為NPS）。
15. 按一下「**OK**」（確定）。



Edit AnyConnect Connection Profile: TEST

- Basic
- ⊞ Advanced

Name: TEST

Aliases: TEST

Authentication

Method: ● AAA ○ Certificate ○ Both

AAA Server Group: NPS

☐ Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

● None ○ DHCP Link ○ DHCP Subnet

Client Address Pools: test

Client IPv6 Address Pools:

Default Group Policy

Group Policy: DfltGrpPolicy

(Following field is an attribute of the group policy selected above.)

☑ Enable SSL VPN client protocol

☑ Enable IPsec(IKEv2) client protocol

DNS Servers: 10.40.3.10

WINS Servers:

Domain Name:

CLI組態

```
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
```

預設情況下，ASA使用未加密的密碼身份驗證協定(PAP)身份驗證型別。這並不意味著當ASA傳送RADIUS請求資料包時，會以純文字檔案形式傳送密碼。相反，明文密碼使用RADIUS共用金鑰進行加密。

如果在隧道組下啟用密碼管理，則ASA使用MSCHAP-v2身份驗證型別來加密明文密碼。在這種情況下，請確保在ASDM配置部分中配置的「編輯AAA伺服器」視窗中選中**Microsoft CHAPv2 Capable**覈取方塊。

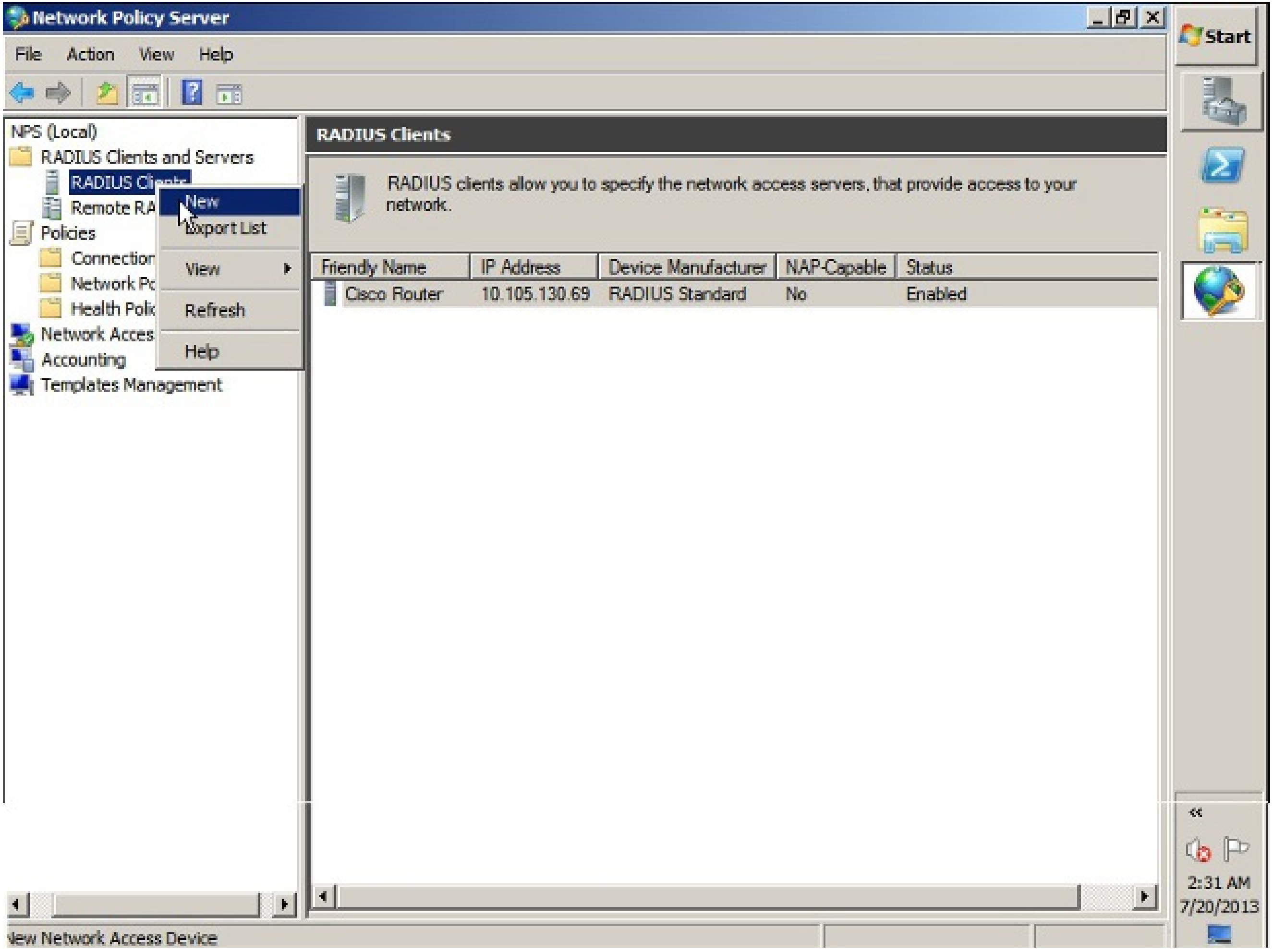
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **附註**：**test aaa-server authentication**命令始終使用PAP。僅當使用者發起到已啟用密碼管理的隧道組的連線時，ASA才會使用MSCHAP-v2。此外，僅輕型目錄訪問協定(LDAP)支援「password-management [password-expire-in-days]」選項。RADIUS不提供此功能。當密碼在Active Directory中已過期時，您將看到密碼到期選項。

採用NPS配置的Windows 2008 Server

NPS伺服器角色應安裝在Windows 2008伺服器上運行。否則，請選擇**開始>管理工具>伺服器角色>新增角色服務**。選擇Network Policy Server並安裝軟體。安裝NPS伺服器角色後，請完成以下步驟，以便將NPS配置為接受並處理來自ASA的RADIUS身份驗證請求：

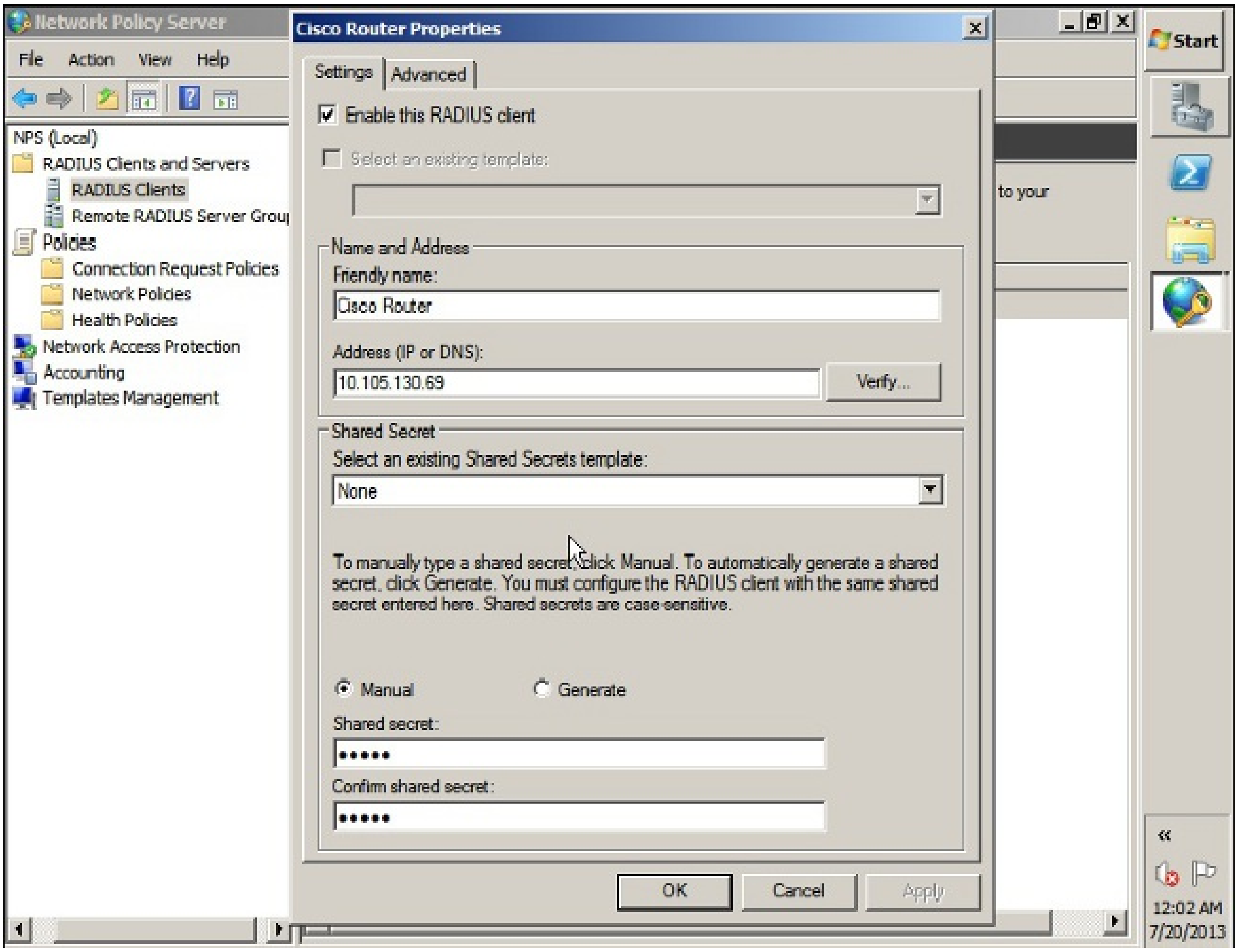
1. 將ASA新增為NPS伺服器中的RADIUS客戶端。 選擇**Administrative Tools > Network Policy Server**。按一下右鍵**RADIUS Clients**，然後選擇**New**。



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
Cisco Router	10.105.130.69	RADIUS Standard	No	Enabled

輸入在ASA上配置的友好名稱、地址（IP或DNS）和共用金鑰。



Cisco Router Properties

Settings | Advanced

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: Cisco Router

Address (IP or DNS): 10.105.130.69

Shared Secret

Select an existing Shared Secrets template: None

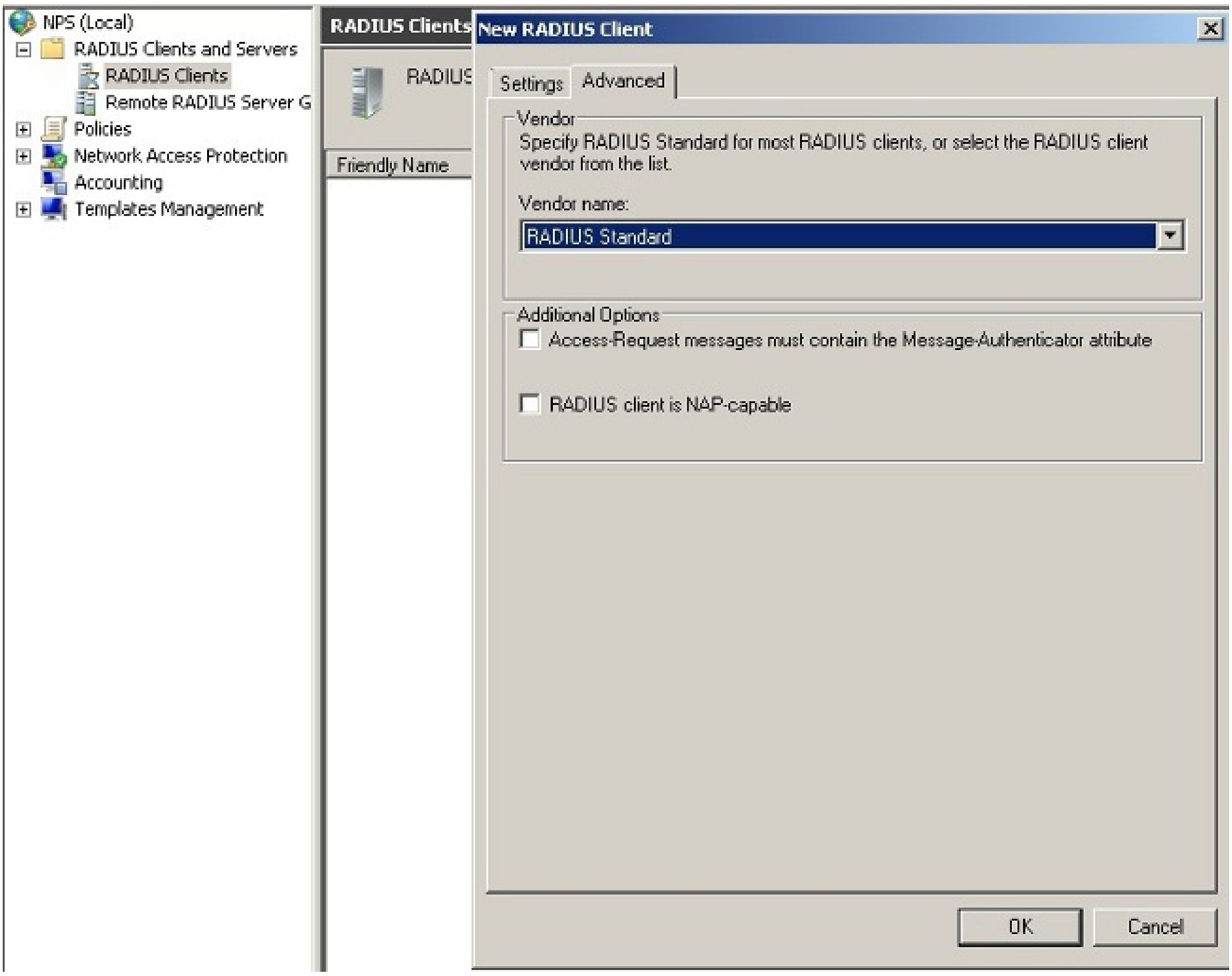
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••

Confirm shared secret: •••••

按一下Advanced頁籤。在「廠商名稱」下拉式清單中選擇RADIUS Standard。按一下「OK」（確定）。



Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:

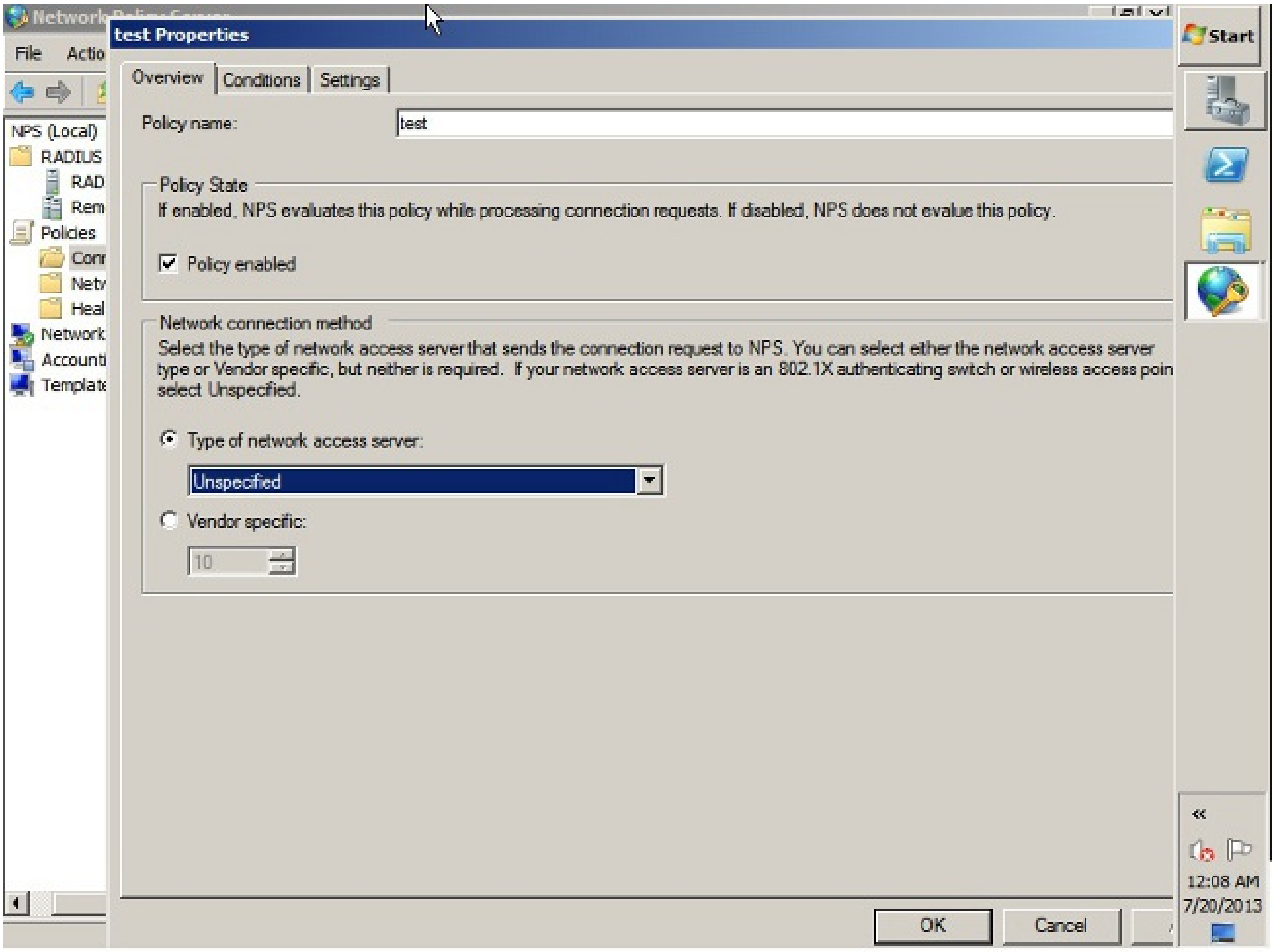
RADIUS Standard

Additional Options

□ Access-Request messages must contain the Message-Authenticator attribute

□ RADIUS client is NAP-capable

2. 為VPN使用者建立新的連線請求策略。連線請求策略的目的是指定來自RADIUS客戶端的請求是本地處理還是轉發到遠端RADIUS伺服器。 在NPS > Policies下，按一下右鍵**Connection Request Policies**，然後建立新策略。從Type of network access server下拉選單中，選擇**Unspecified**。



test Properties

Overview | Conditions | Settings

Policy name: test

Policy State

If enabled, NPS evaluates this policy while processing connection requests. If disabled, NPS does not evalue this policy.

☑ Policy enabled

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access poin select Unspecified.

● Type of network access server:

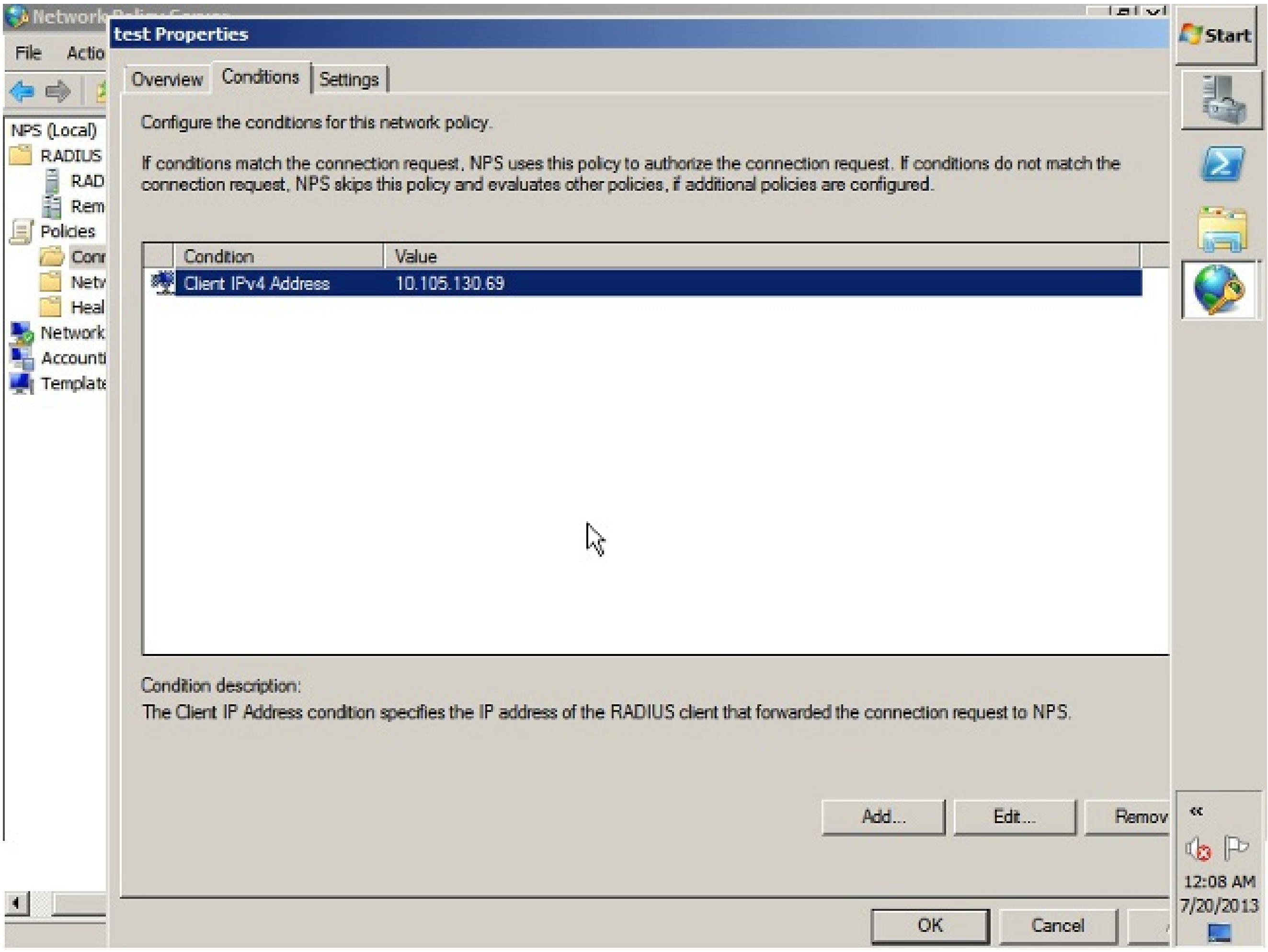
Unspecified

○ Vendor specific:

10

OK　Cancel

按一下Conditions頁籤。按一下「Add」。輸入ASA的IP地址作為「客戶端IPv4地址」條件。



test Properties

Overview | Conditions | Settings

Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
Client IPv4 Address	10.105.130.69

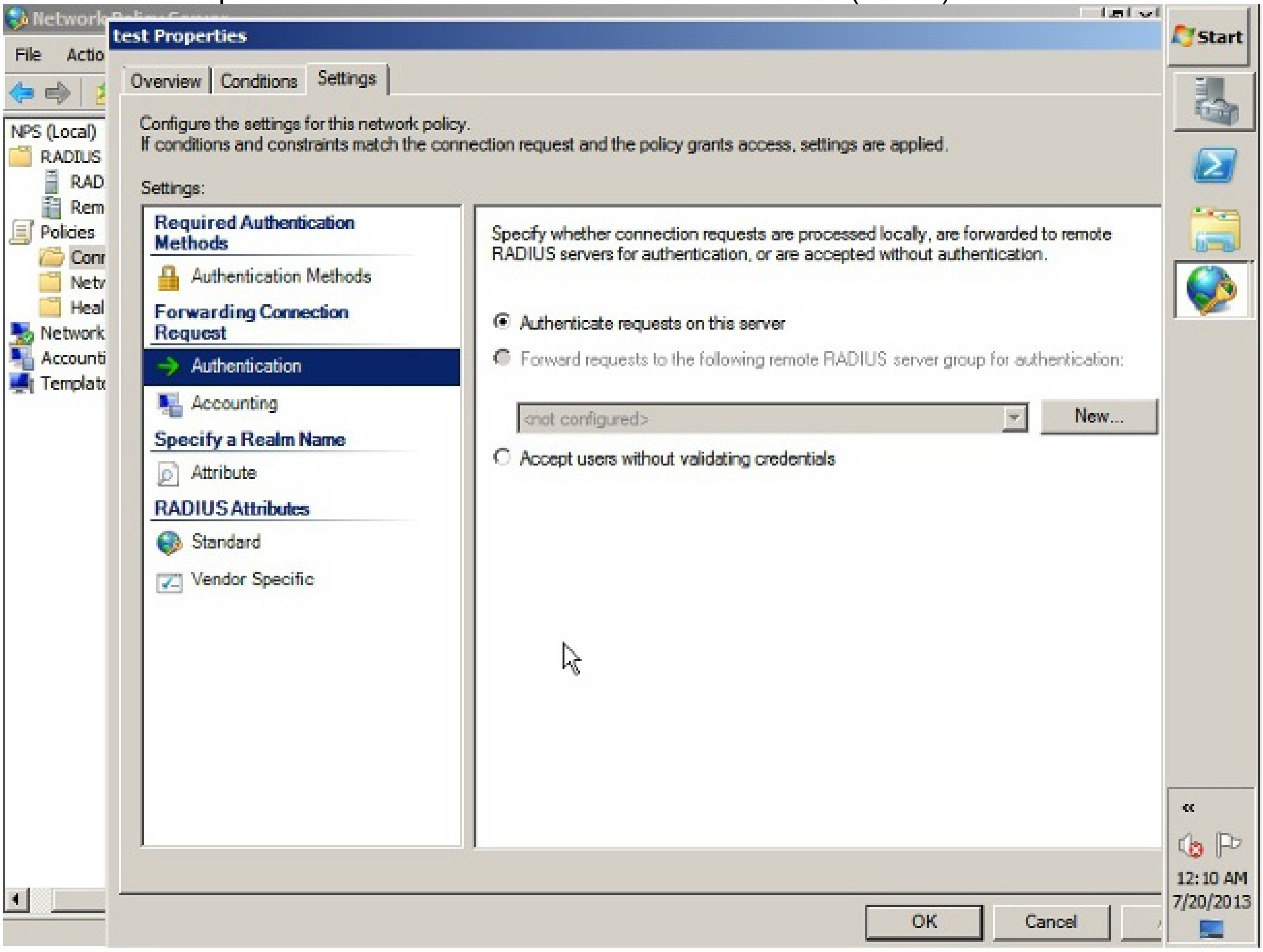
Condition description:

The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

Add...　Edit...　Remov

OK　Cancel

按一下**Settings**頁籤。在Forwarding Connection Request下，選擇**Authentication**。確保選中Authenticate requests on this server單選按鈕。按一下「**OK**」（確定）。



test Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Specify whether connection requests are processed locally, are forwarded to remote RADIUS servers for authentication, or are accepted without authentication.

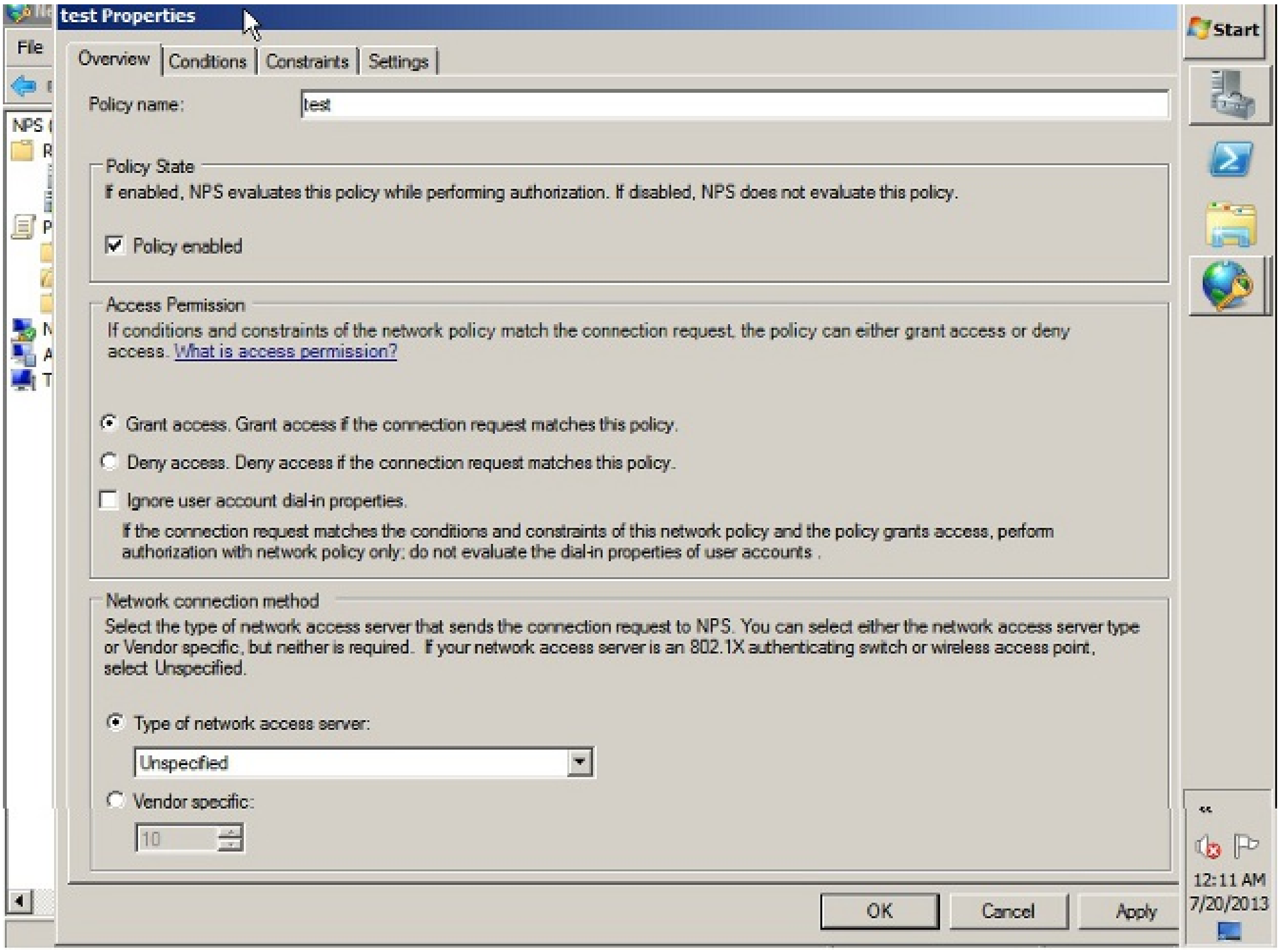
● Authenticate requests on this server

○ Forward requests to the following remote RADIUS server group for authentication:

<not configured>

○ Accept users without validating credentials

3. 新增網路策略，您可以在其中指定允許哪些使用者進行身份驗證。例如，可以將Active Directory使用者組新增為條件。只有屬於指定Windows組的那些使用者才能使用此策略進行身份驗證。在NPS下，選擇**Policies**。按一下右鍵**Network Policy**並建立新策略。確保選中「Grant access（授予訪問許可權）」單選按鈕。從Type of network access server下拉選單中，選擇**Unspecified**。



test Properties

Policy name: test

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

□ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

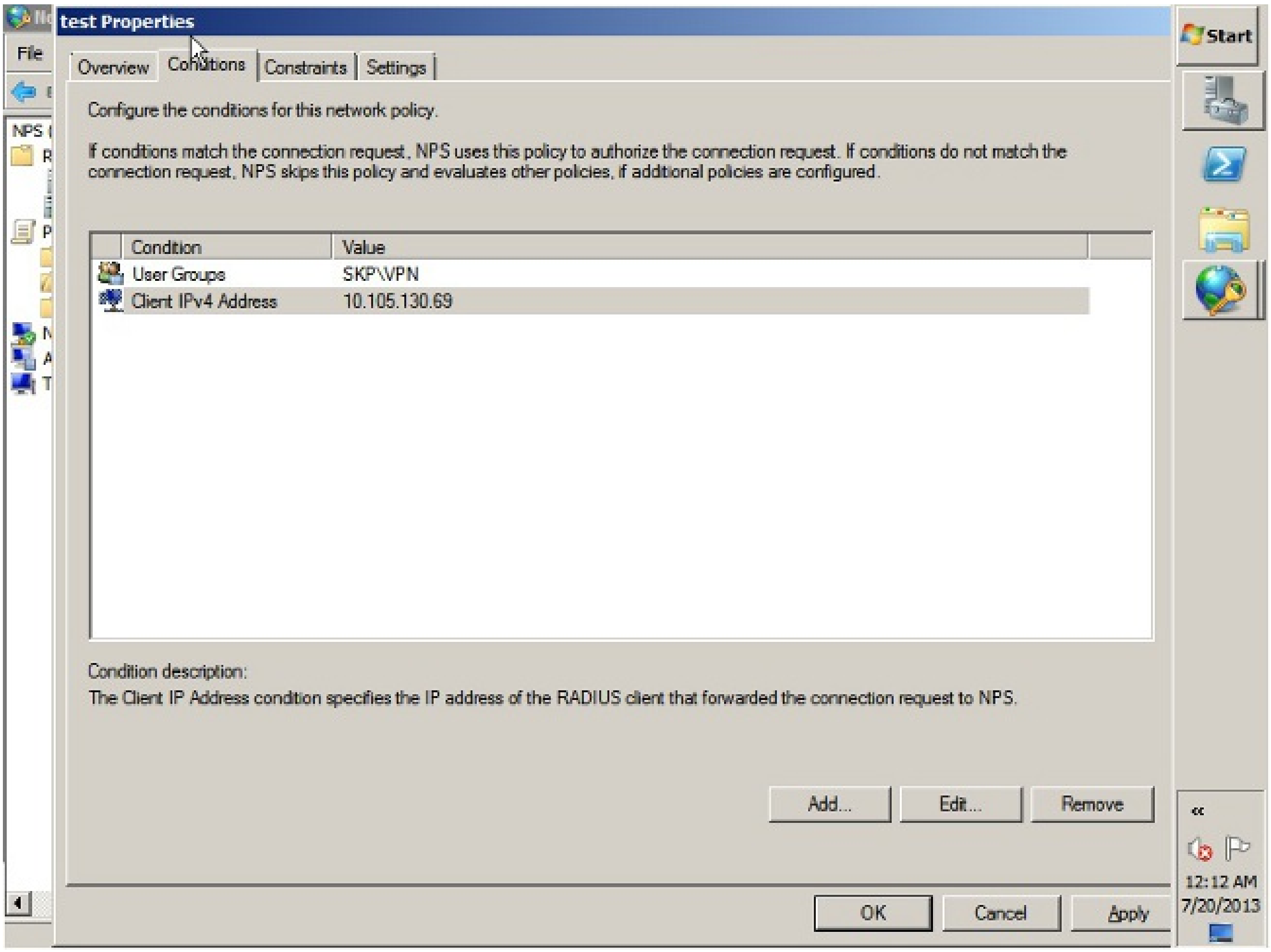
● Type of network access server:

Unspecified

○ Vendor specific:

10

按一下**Conditions**頁籤。按一下「**Add**」。輸入ASA的IP地址作為客戶端IPv4地址條件。輸入包含VPN使用者的Active Directory使用者組。



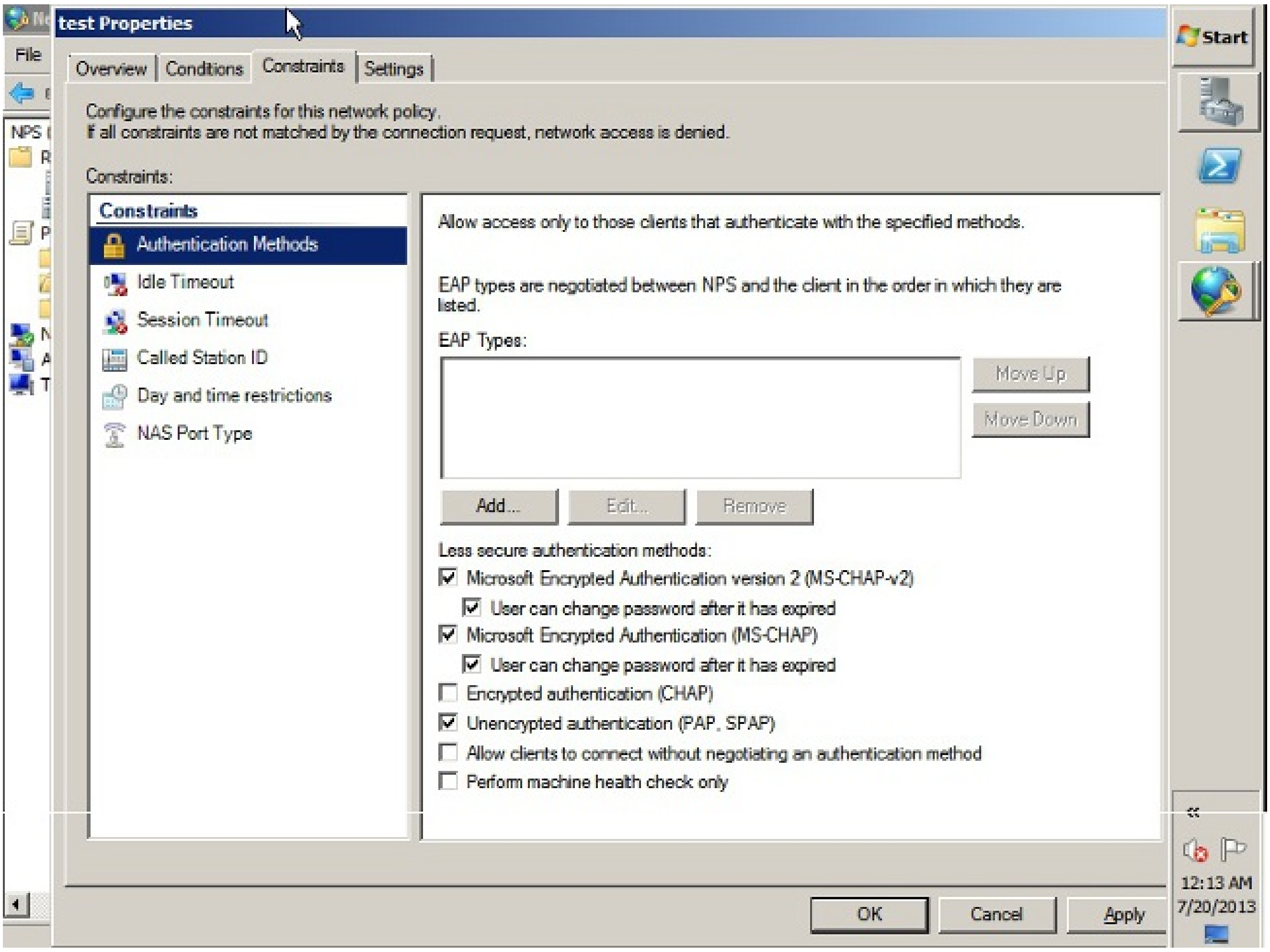
Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
User Groups	SKP\VPN
Client IPv4 Address	10.105.130.69

Condition description:
The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the connection request to NPS.

按一下**Constraints**頁籤。選擇**Authentication Methods**。確保選中Unencrypted authentication(PAP， SPAP)覈取方塊。按一下「**OK**」（確定）。



Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints
- Authentication Methods
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up
Move Down
Add...
Edit...
Remove

Less secure authentication methods:

☑ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
  ☑ User can change password after it has expired
☑ Microsoft Encrypted Authentication (MS-CHAP)
  ☑ User can change password after it has expired
□ Encrypted authentication (CHAP)
☑ Unencrypted authentication (PAP, SPAP)
□ Allow clients to connect without negotiating an authentication method
□ Perform machine health check only

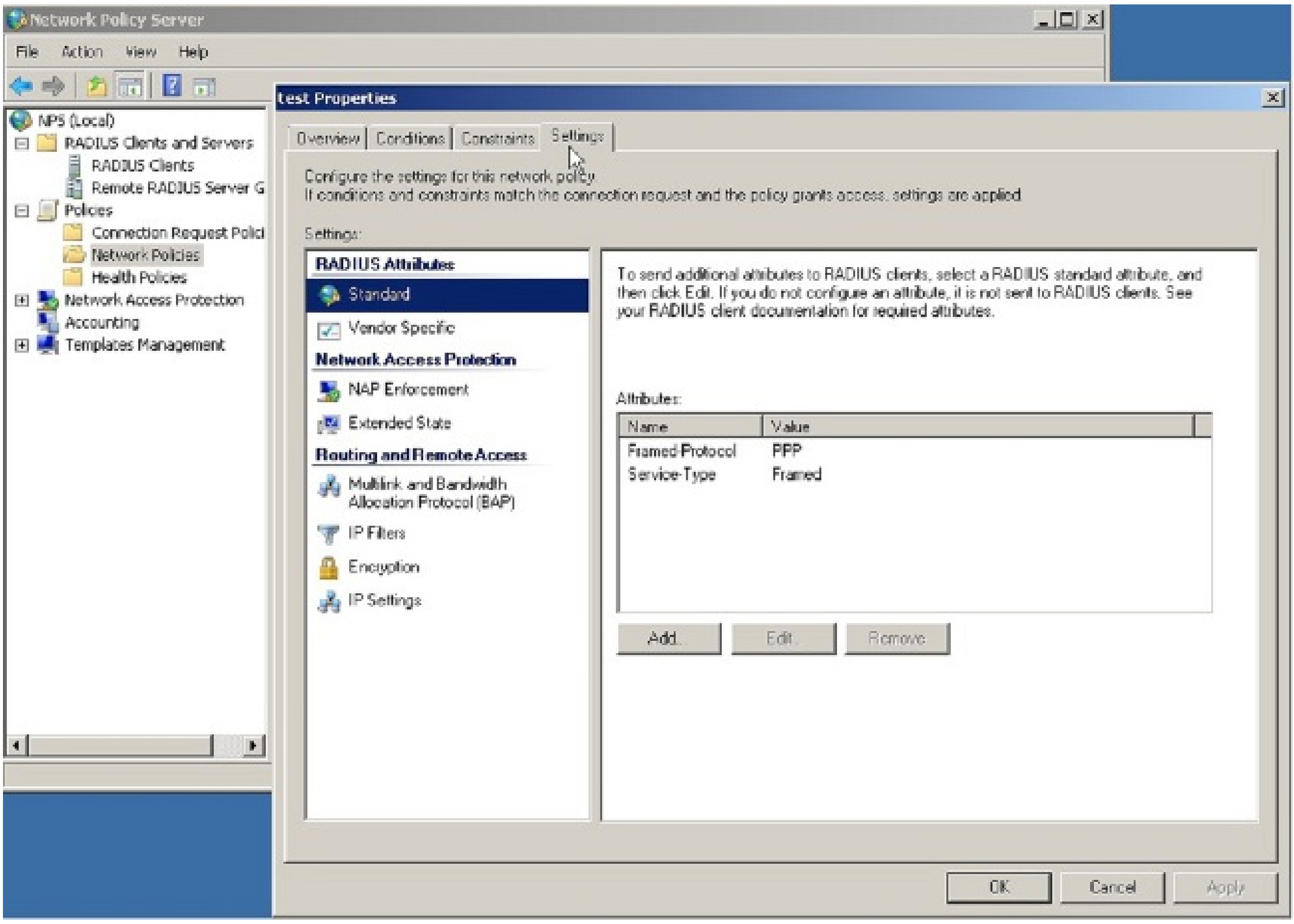
OK
Cancel
Apply

從NPS RADIUS伺服器傳遞組策略屬性（屬性25）

如果需要使用NPS RADIUS伺服器將組策略動態分配給使用者，可以使用組策略RADIUS屬性（屬性25）。

完成這些步驟，以便將RADIUS屬性25傳送給使用者，該屬性用於動態分配組策略。

1. 新增網路策略後，按一下右鍵所需的網路策略，然後按一下**設定**頁籤。



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

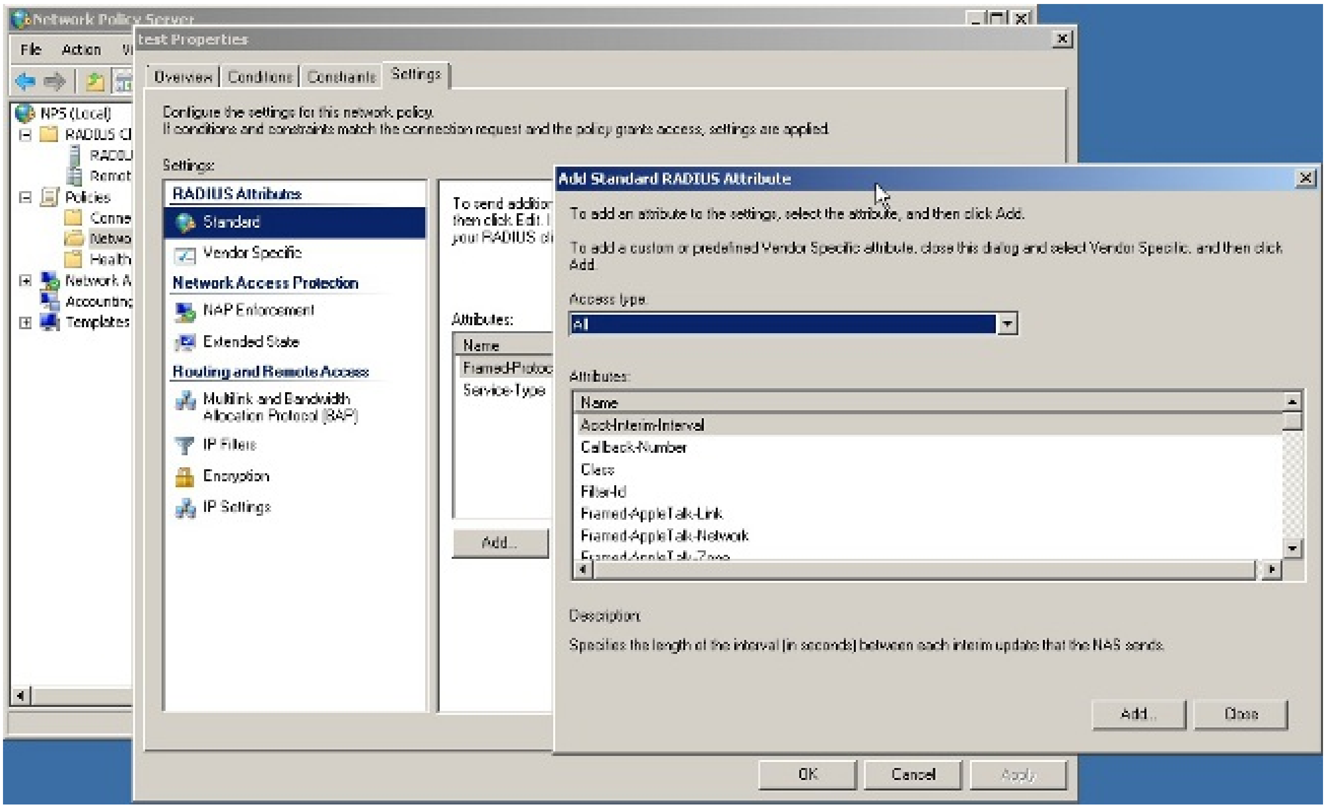
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Value
Framed-Protocol	PPP
Service-Type	Framed

2. 選擇**RADIUS Attributes > Standard**。按一下「**Add**」。將Access型別保留為All。



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

To add an attribute to the settings, select the attribute, and then click Add.

To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type:
All

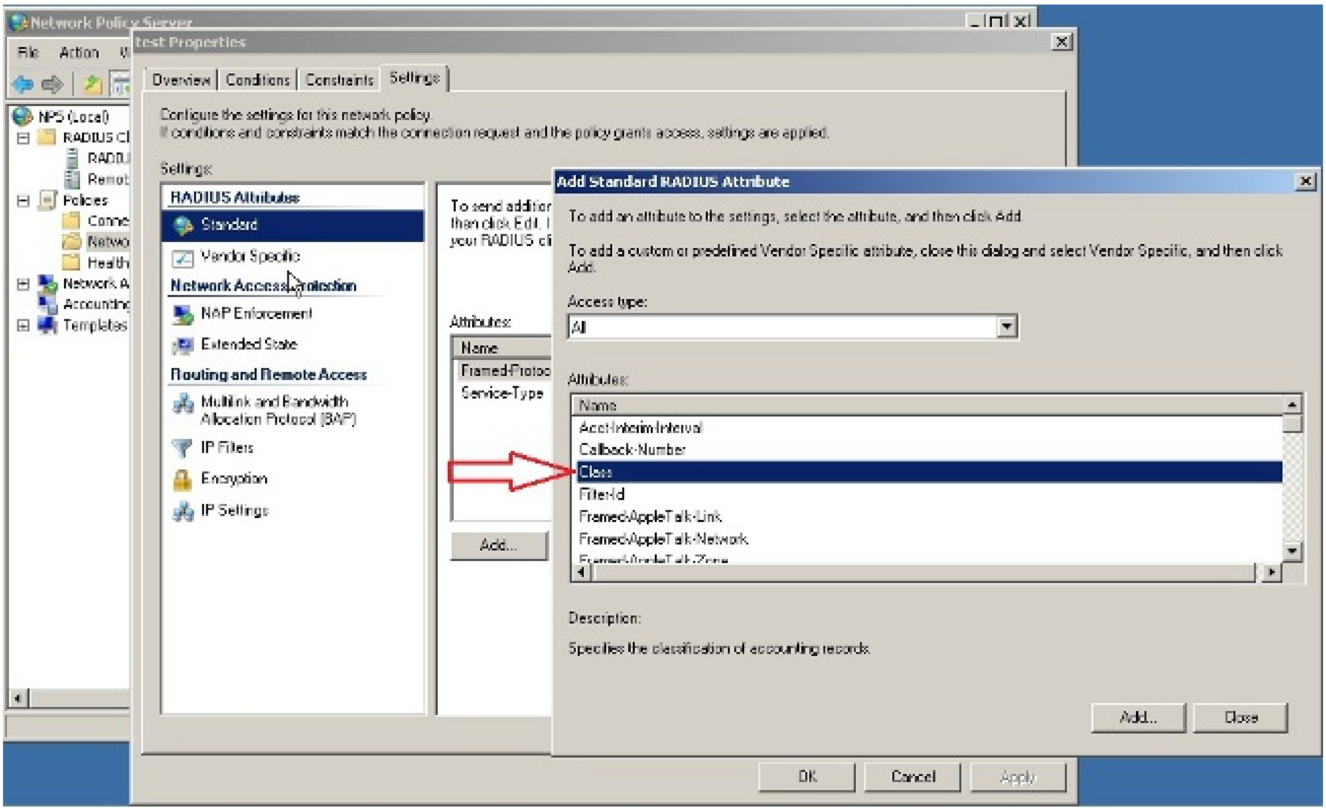
Attributes:

Name
Acct-Interim-Interval
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network
Framed-AppleTalk-Zone

Description:

Specifies the length of the interval (in seconds) between each interim update that the NAS sends.

3. 在「屬性」框中，選擇**Class**，然後按一下**Add**。輸入屬性值，即字串形式的組策略名稱。請記住，必須在ASA中配置具有此名稱的組策略。這樣，ASA在RADIUS響應中收到此屬性後，會將其分配給VPN會話。



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes
- Standard
- Vendor Specific

Network Access Protection
- NAP Enforcement
- Extended State

Routing and Remote Access
- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

To add an attribute to the settings, select the attribute, and then click Add.

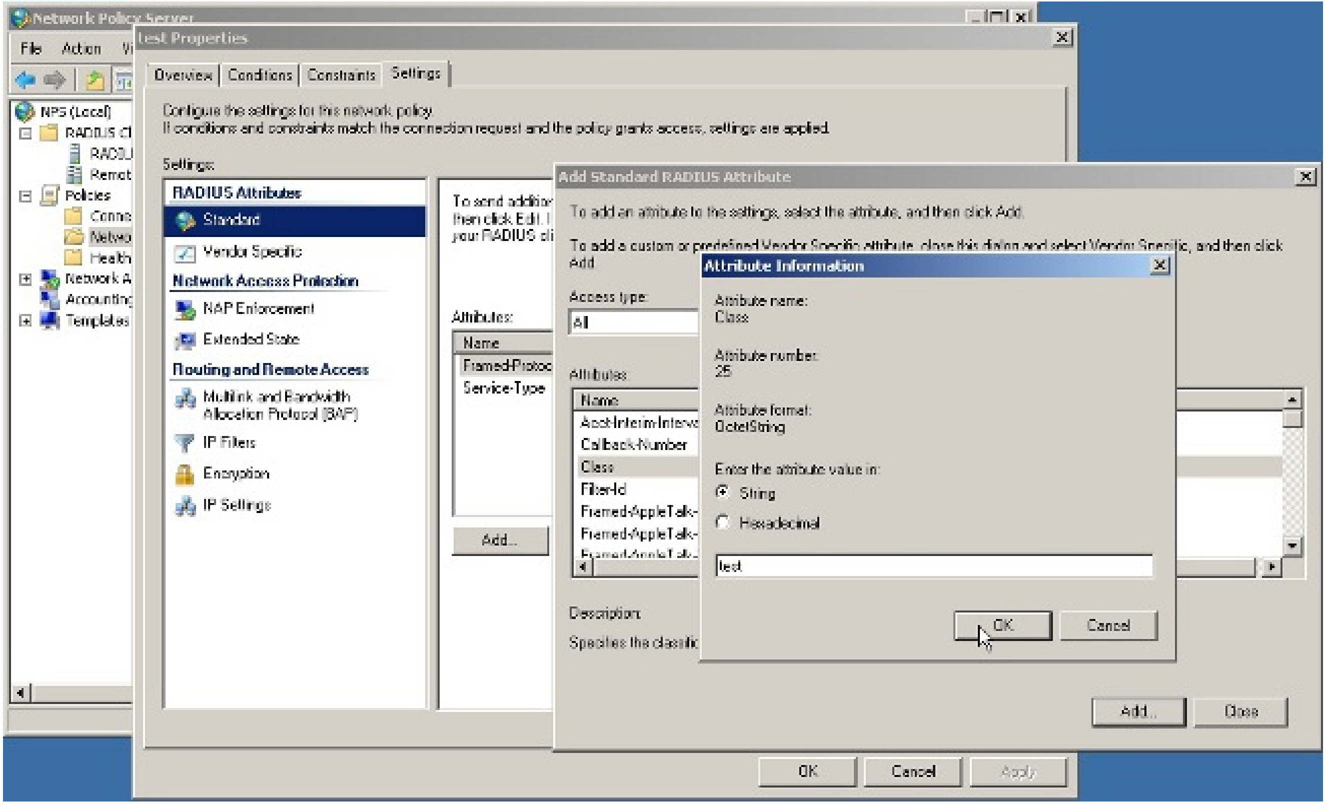
To add a custom or predefined Vendor Specific attribute, close this dialog and select Vendor Specific, and then click Add.

Access type: All

Attributes:

Name
Acct-Interim-Interval
Callback-Number
Class
Filter-Id
Framed-AppleTalk-Link
Framed-AppleTalk-Network
Framed-AppleTalk-Zone

Description:
Specifies the classification of accounting records.



Attribute name:
Class

Attribute number:
25

Attribute format:
OctetString

Enter the attribute value in:
● String
○ Hexadecimal

test

驗證

使用本節內容，確認您的組態是否正常運作。

附註：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

ASA調試

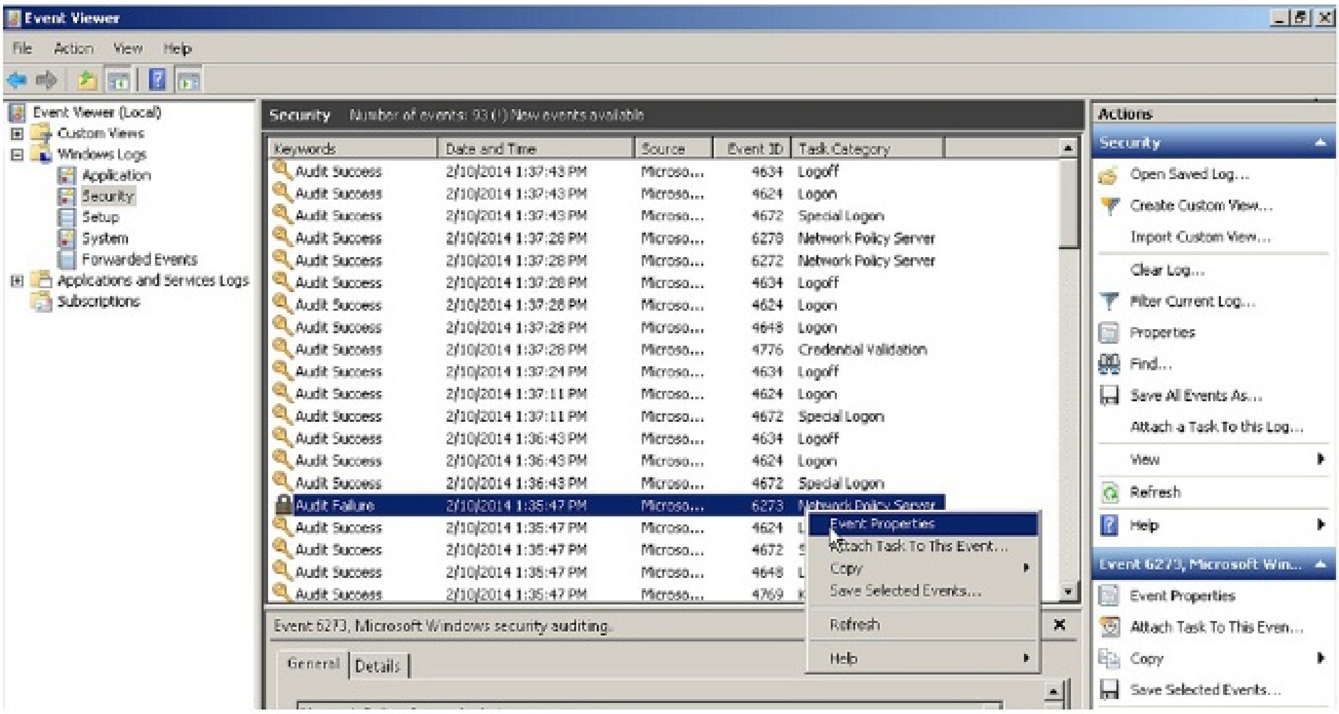
在ASA上啟用**debug radius all**。

```
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).....
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 確保ASA和NPS伺服器之間的連線正常。應用資料包捕獲，確保身份驗證請求離開ASA介面（可從其訪問伺服器）。 確認路徑中的裝置沒有封鎖UDP連線埠1645（預設的RADIUS驗證連線埠），以確保其到達NPS伺服器。有關ASA上資料包捕獲的詳細資訊，請參閱ASA/PIX/FWSM:使用CLI和ASDM捕獲資料包的配置示例。
- 如果身份驗證仍失敗，請在Windows NPS上的事件檢視器中查詢。在Event Viewer > Windows Logs下，選擇**Security。**在身份驗證請求前後查詢與NPS關聯的事件。



Security Number of events: 93 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/10/2014 1:37:43 PM	Microso...	4634	Logoff
Audit Success	2/10/2014 1:37:43 PM	Microso...	4624	Logon
Audit Success	2/10/2014 1:37:43 PM	Microso...	4672	Special Logon
Audit Success	2/10/2014 1:37:28 PM	Microso...	6278	Network Policy Server
Audit Success	2/10/2014 1:37:28 PM	Microso...	6272	Network Policy Server
Audit Success	2/10/2014 1:37:28 PM	Microso...	4634	Logoff
Audit Success	2/10/2014 1:37:28 PM	Microso...	4624	Logon
Audit Success	2/10/2014 1:37:28 PM	Microso...	4648	Logon
Audit Success	2/10/2014 1:37:28 PM	Microso...	4776	Credential Validation
Audit Success	2/10/2014 1:37:24 PM	Microso...	4634	Logoff
Audit Success	2/10/2014 1:37:11 PM	Microso...	4624	Logon
Audit Success	2/10/2014 1:37:11 PM	Microso...	4672	Special Logon
Audit Success	2/10/2014 1:36:43 PM	Microso...	4634	Logoff
Audit Success	2/10/2014 1:36:43 PM	Microso...	4624	Logon
Audit Success	2/10/2014 1:36:43 PM	Microso...	4672	Special Logon
Audit Failure	2/10/2014 1:35:47 PM	Microso...	6273	Network Policy Server
Audit Success	2/10/2014 1:35:47 PM	Microso...	4624	L
Audit Success	2/10/2014 1:35:47 PM	Microso...	4672	S
Audit Success	2/10/2014 1:35:47 PM	Microso...	4648	L
Audit Success	2/10/2014 1:35:47 PM	Microso...	4769	K

Event 6273, Microsoft Windows security auditing.

開啟「事件屬性」後，您應該能夠看到失敗的原因，如示例所示。在本示例中，未選擇PAP作為Network policy下的身份驗證型別。因此，身份驗證請求失敗。

```
 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.
```