Esempio di autenticazione utente VPN ASA su server dei criteri di rete Windows 2008 (Active Directory) con configurazione RADIUS

Sommario

Introduzione

In questo documento viene spiegato come configurare un'appliance ASA (Adaptive Security Appliance) per comunicare con un server dei criteri di rete (NPS) di Microsoft Windows 2008 tramite il protocollo RADIUS in modo che gli utenti Cisco VPN Client/AnyConnect/WebVPN senza client legacy vengano autenticati in Active Directory. Server dei criteri di rete è uno dei ruoli server offerti da Windows 2008 Server. Equivale a Windows 2003 Server, IAS (Internet Authentication Service), ovvero all'implementazione di un server RADIUS per l'autenticazione remota degli utenti connessi tramite connessione remota. Analogamente, in Windows 2008 Server dei criteri di rete è l'implementazione di un server RADIUS. In pratica, l'appliance ASA è un client RADIUS collegato a un server RADIUS Server dei criteri di rete. ASA invia richieste di autenticazione RADIUS per conto di utenti VPN e Server dei criteri di rete le autentica in Active Directory.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

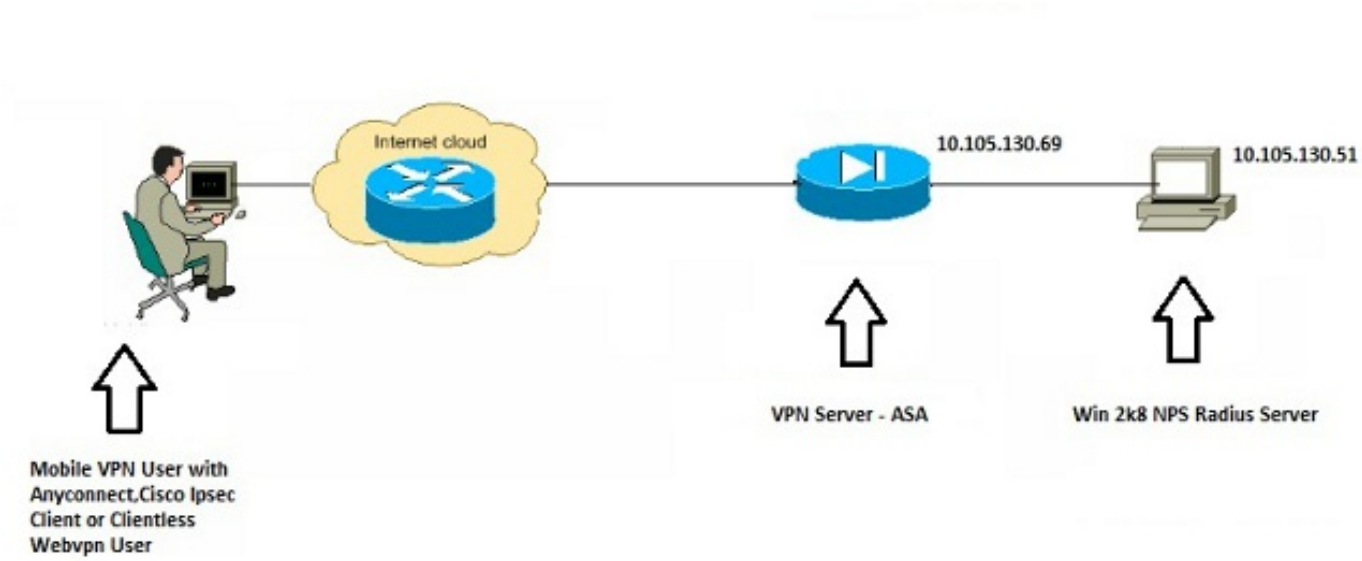
- ASA con versione 9.1(4)
- Server Windows 2008 R2 con i servizi Active Directory e il ruolo Server dei criteri di rete installati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

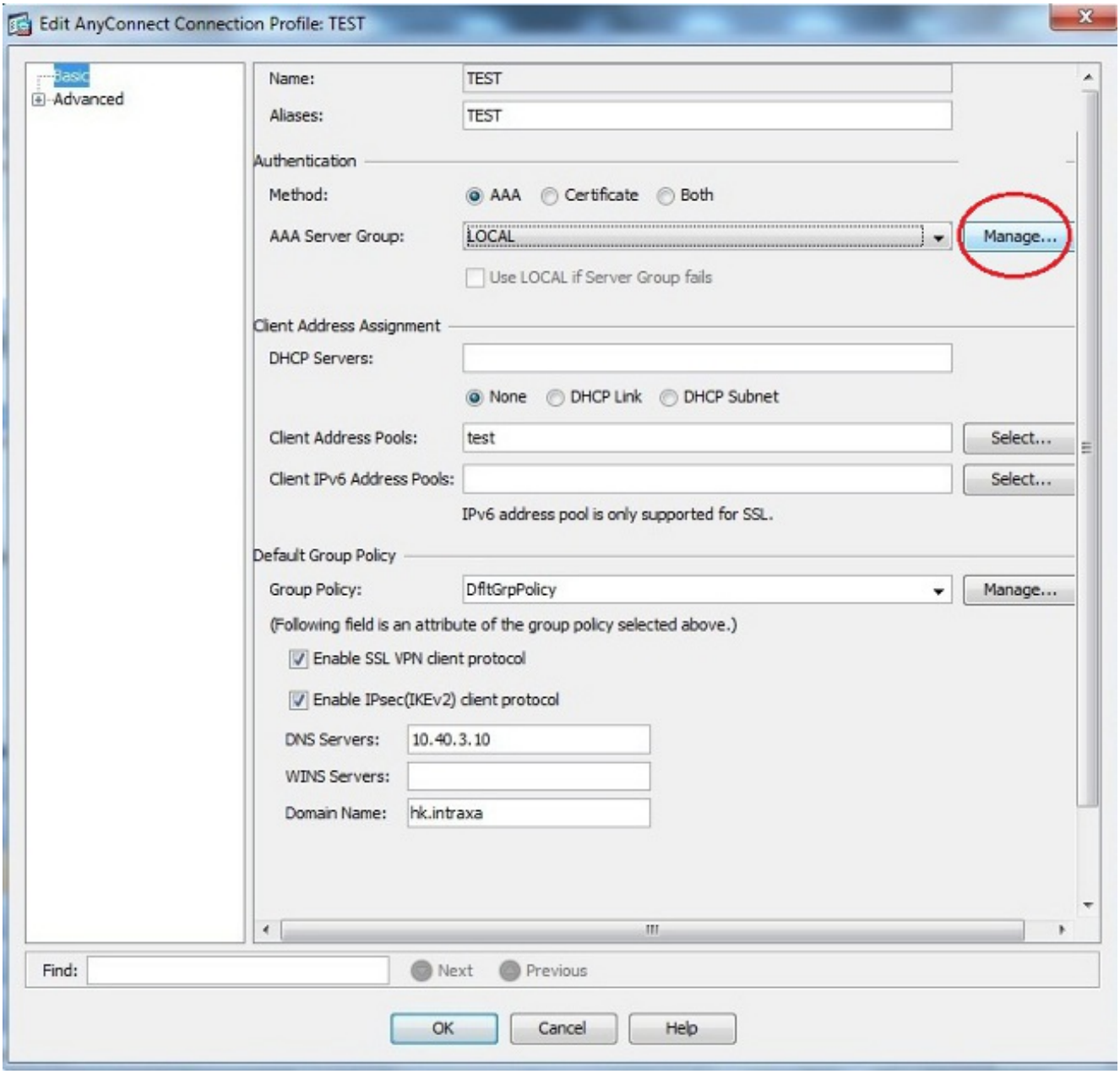
Esempio di rete



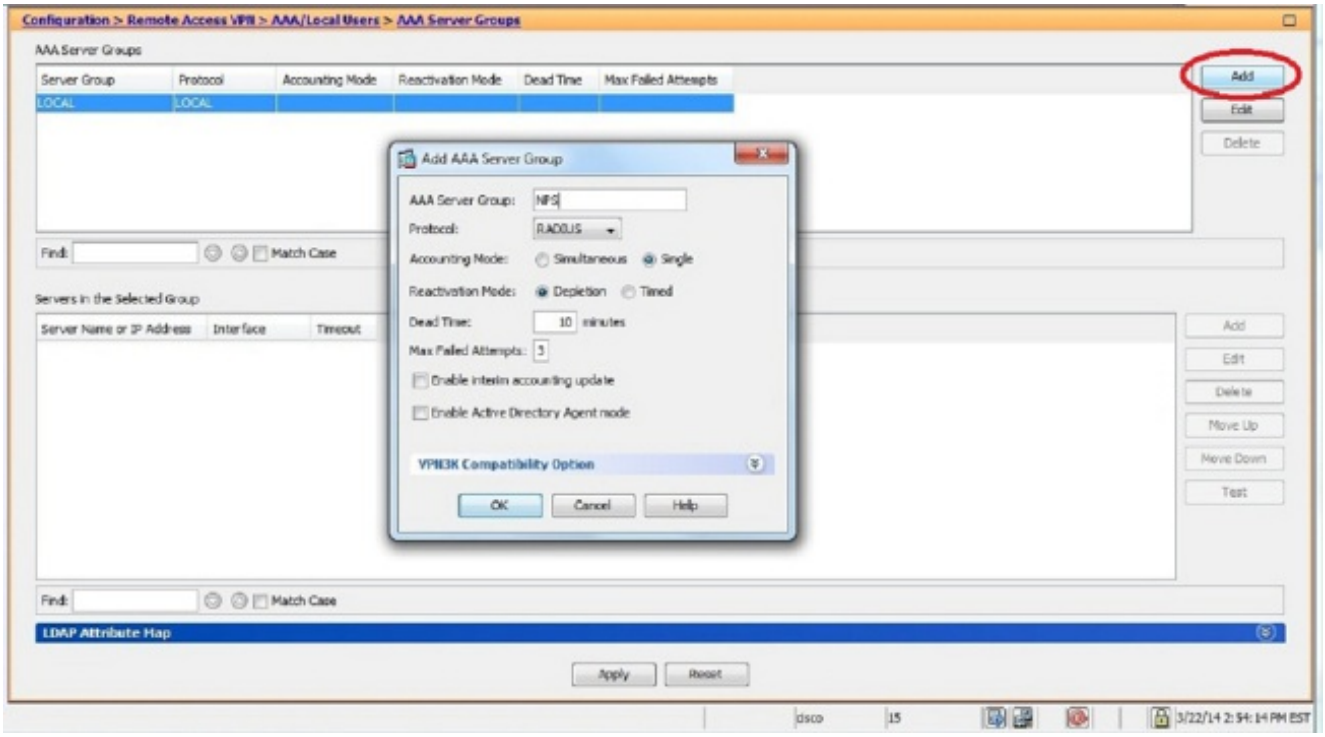
Configurazioni

Configurazione ASDM

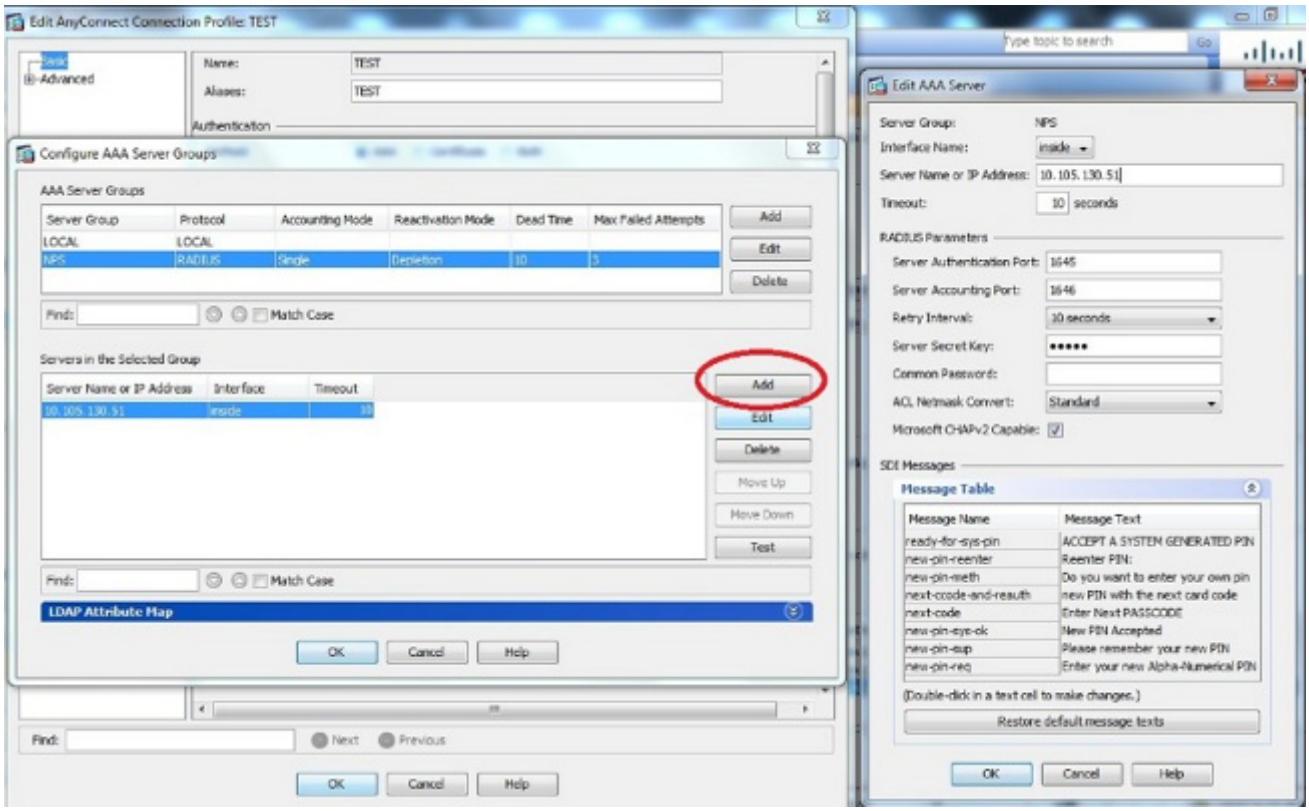
1. Scegliere il gruppo di tunnel per il quale è richiesta l'autenticazione di Server dei criteri di rete.
2. Fare clic su **Modifica** e scegliere **Base**.
3. Nella sezione Autenticazione fare clic su **Gestisci**.



4. Nella sezione Gruppi di server AAA, fare clic su **Aggiungi**.
5. Nel campo Gruppo server AAA immettere il nome del gruppo di server (ad esempio, Server dei criteri di rete).
6. Dall'elenco a discesa Protocollo, scegliere **RADIUS**.
7. Fare clic su
   OK.

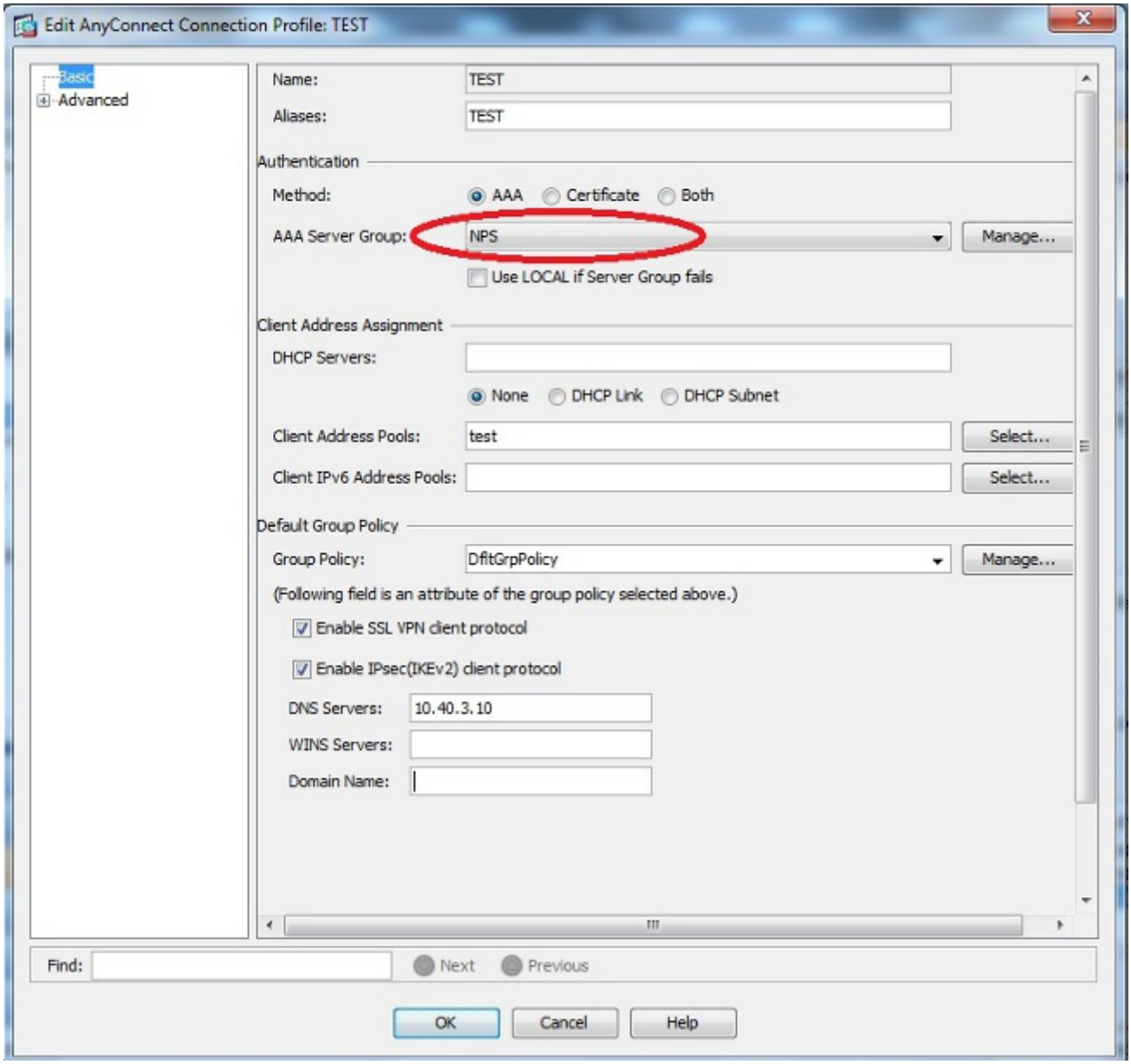


8. Nella sezione Server del gruppo selezionato, scegliere il gruppo di server AAA aggiunto e fare clic su **Aggiungi**.
9. Nel campo Nome server o Indirizzo IP immettere l'indirizzo IP del server.
10. Nel campo Chiave privata server immettere la chiave segreta.
11. Lasciare i campi Porta di autenticazione server e Porta accounting server sul valore predefinito a meno che il server non sia in ascolto su una porta diversa.
12. Fare clic su **OK**.
13. Fare clic su **OK**.



14. Dall'elenco a discesa Gruppo server AAA, scegliere il gruppo (Server dei criteri di rete in questo esempio) aggiunto nei passaggi precedenti.
15. Fare clic su

OK.



Configurazione 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
```

Per impostazione predefinita, l'ASA usa il tipo di autenticazione PAP (Password Authentication Protocol) non crittografato. Ciò non significa che l'ASA invii la password in testo normale quando invia il pacchetto RADIUS REQUEST. Al contrario, la password in testo normale viene crittografata con il segreto condiviso RADIUS.

Se la gestione delle password è abilitata nel gruppo di tunnel, l'appliance ASA usa il tipo di autenticazione MSCHAP-v2 per crittografare la password in testo normale. In tal caso, verificare che la casella di controllo **Funzionalità CHAPv2 Microsoft** sia selezionata nella finestra Modifica server AAA configurata nella sezione Configurazione ASDM.

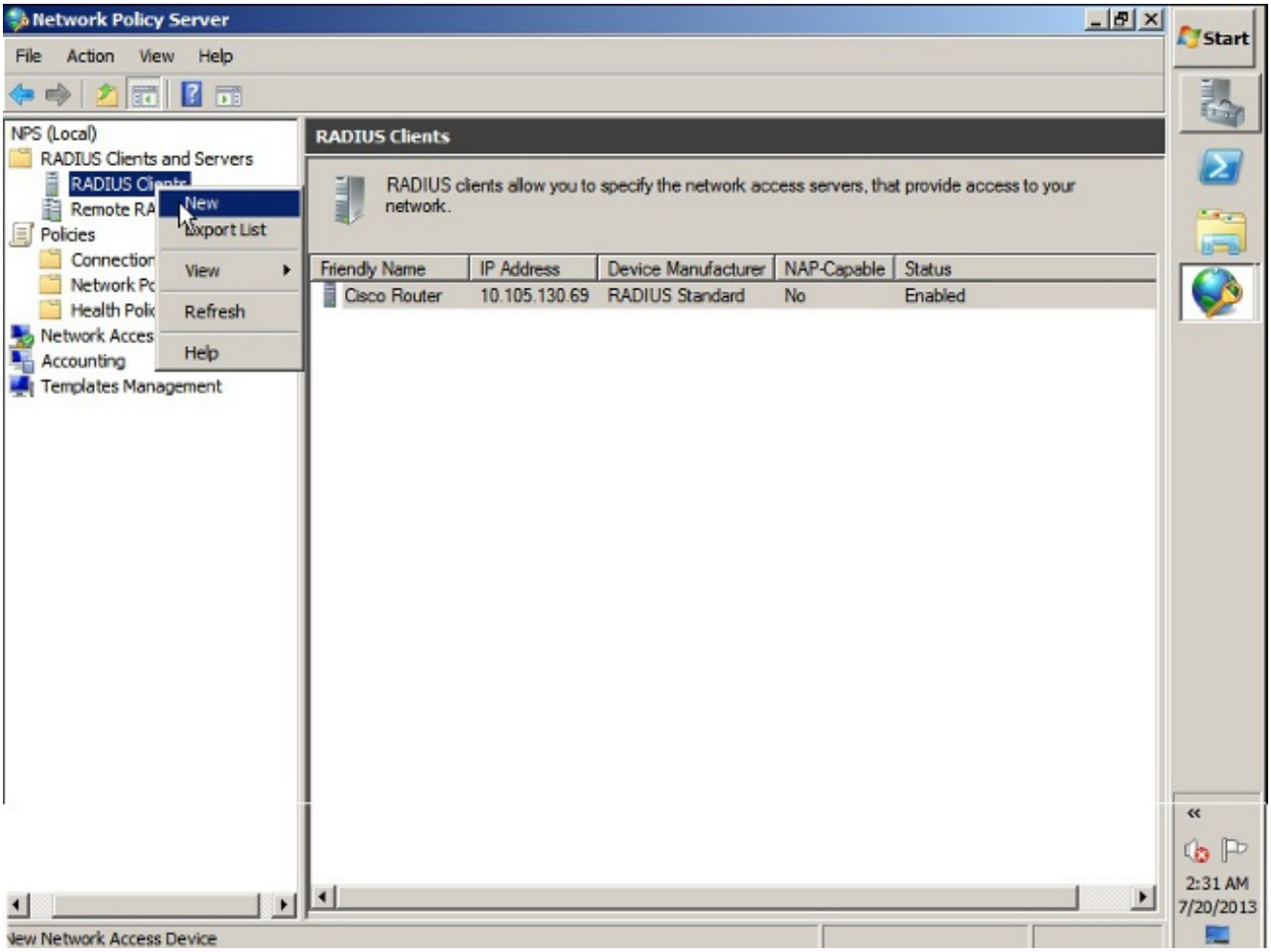
```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> **Nota:** Il comando **test aaa-server authentication** utilizza sempre il protocollo PAP. Solo quando un utente avvia una connessione a un gruppo di tunnel con gestione password abilitata, l'ASA utilizza MSCHAP-v2. Inoltre, l'opzione 'gestione password [giorni di scadenza password]' è supportata solo con il protocollo LDAP (Lightweight Directory Access Protocol). RADIUS non fornisce questa funzione. L'opzione relativa alla scadenza della password verrà visualizzata quando la password è già scaduta in Active Directory.

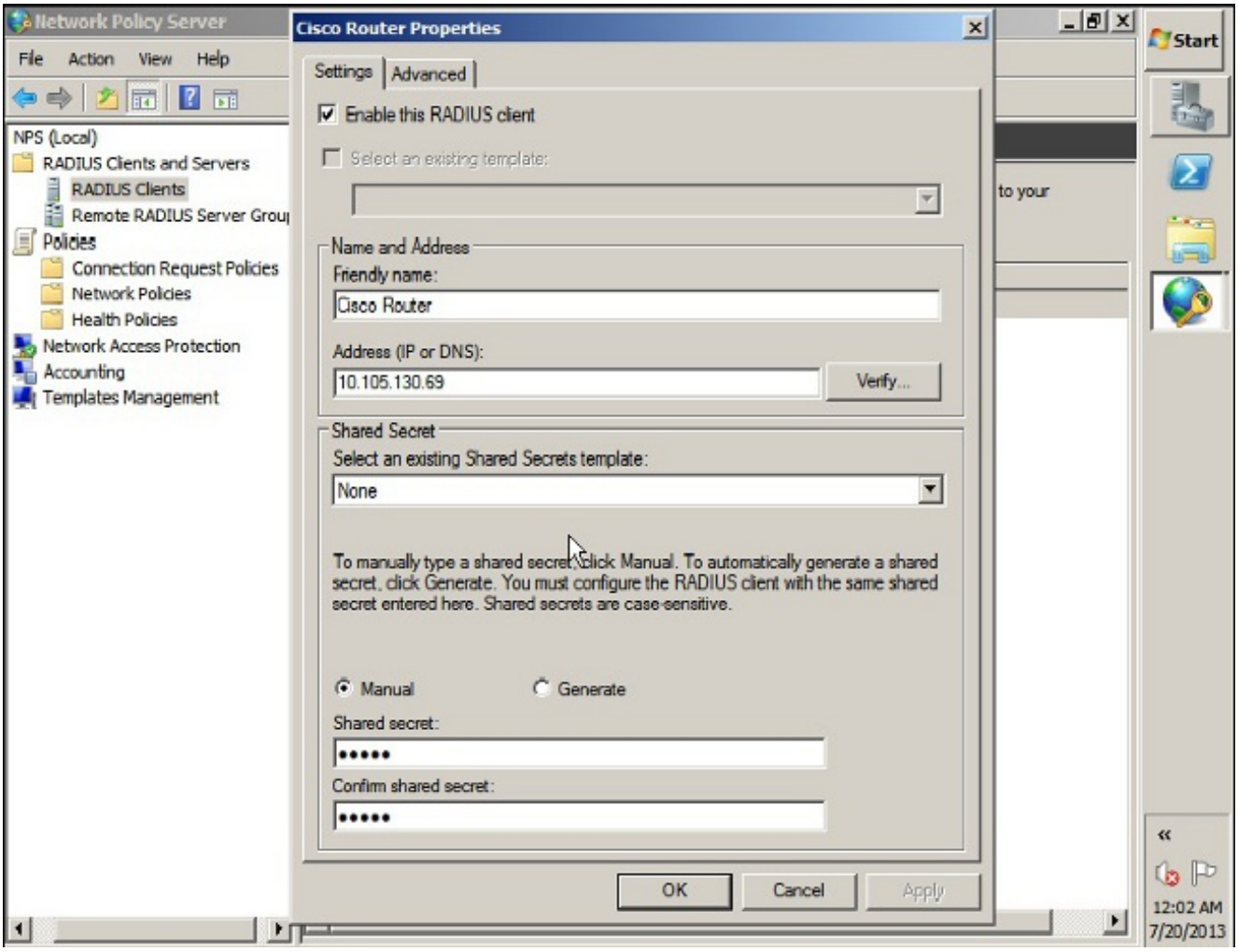
Windows 2008 Server con configurazione Server dei criteri di rete

Il ruolo Server dei criteri di rete deve essere installato e in esecuzione nel server Windows 2008. In caso contrario, scegliere **Start > Strumenti di amministrazione > Ruoli server > Aggiungi servizi ruolo**. Scegliere Server dei criteri di rete e installare il software. Una volta installato il ruolo Server dei criteri di rete, completare la procedura seguente per configurare il Server dei criteri di rete per accettare ed elaborare le richieste di autenticazione RADIUS dall'appliance ASA:

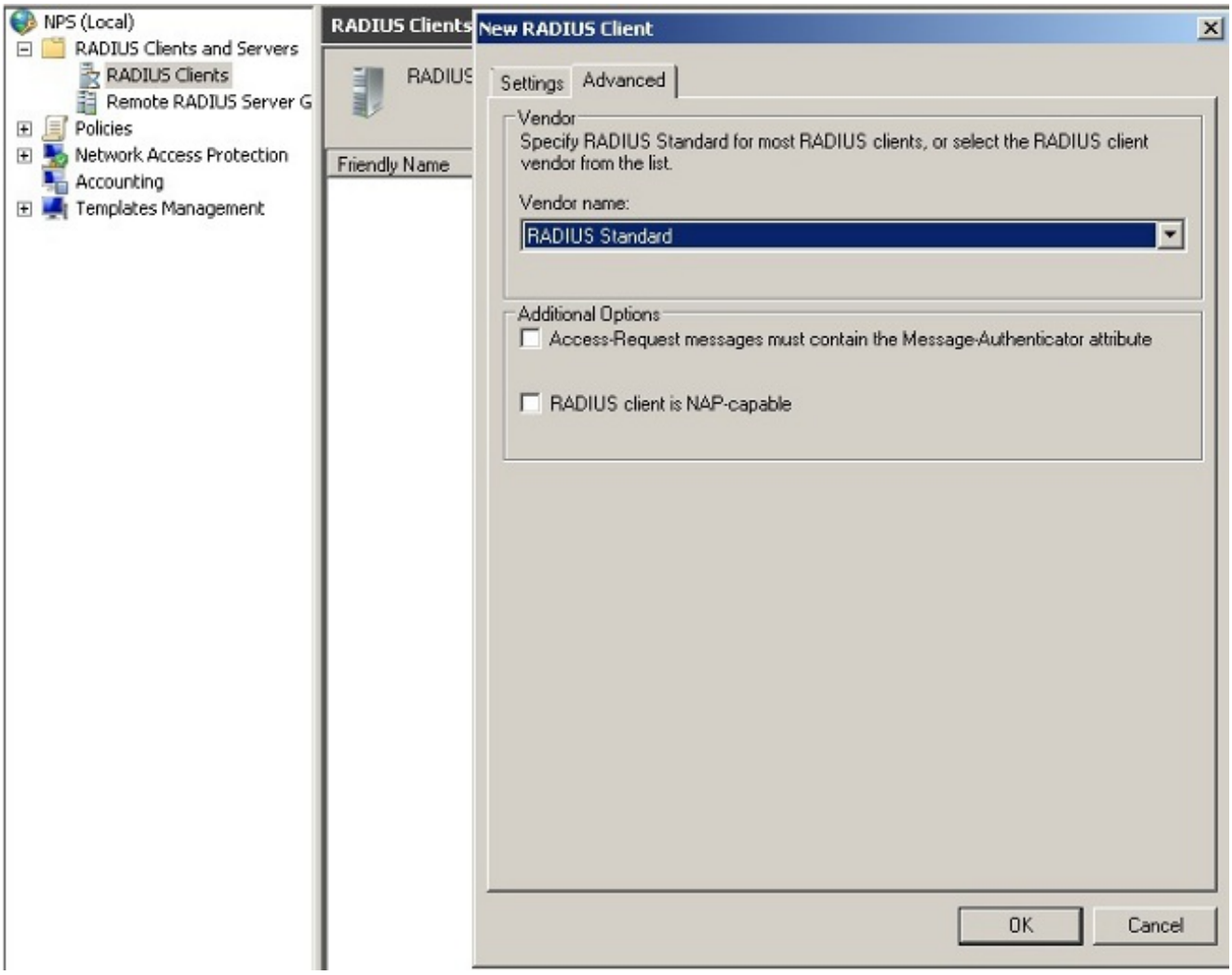
1. Aggiungere l'appliance ASA come client RADIUS nel Server dei criteri di rete. Scegliere **Strumenti di amministrazione > Server dei criteri di rete.**Fare clic con il pulsante destro del mouse su **Client RADIUS** e scegliere
   Nuovo.



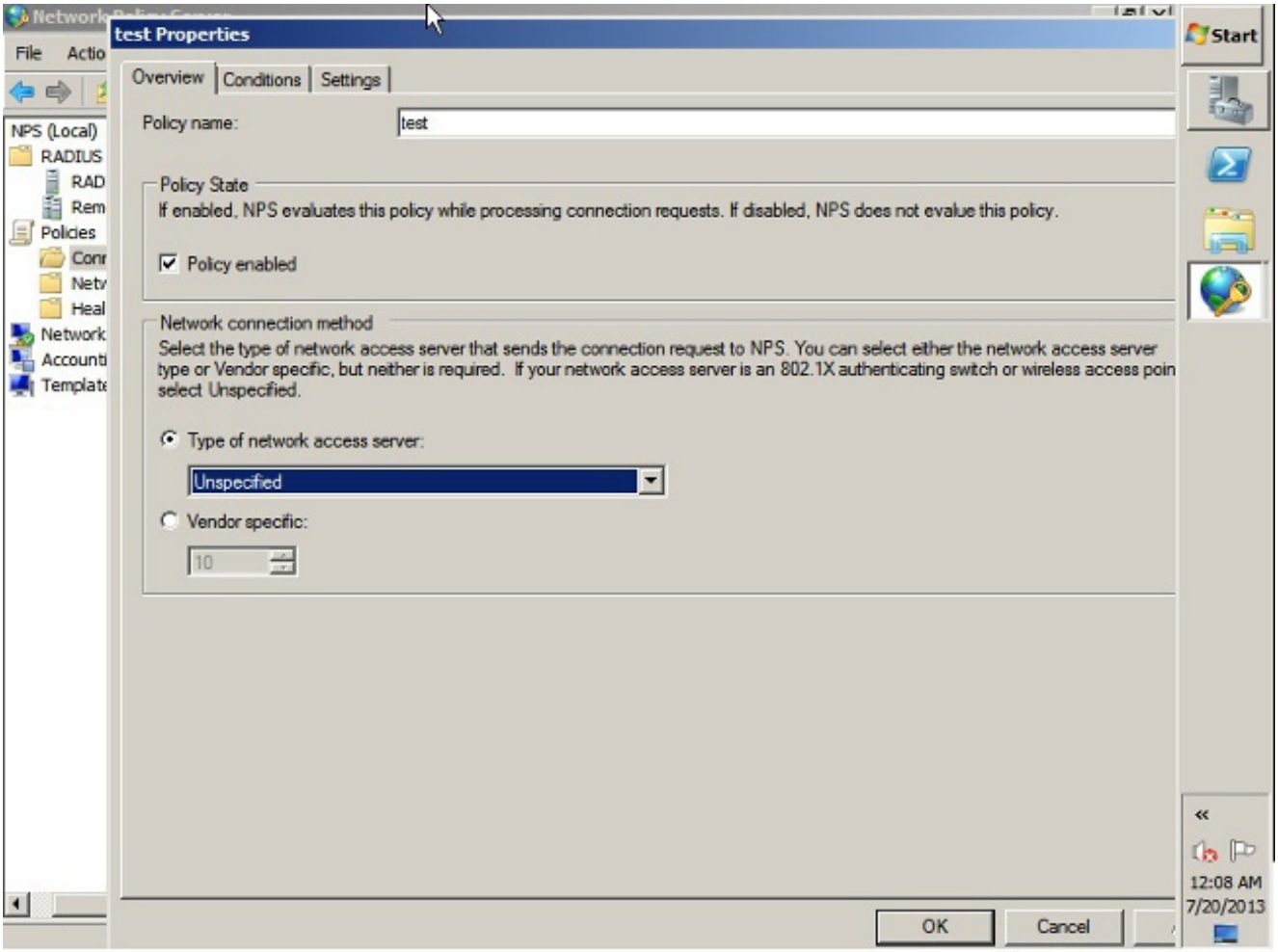
Immettere un nome descrittivo, un indirizzo (IP o DNS) e un segreto condiviso configurati sull'appliance
ASA.



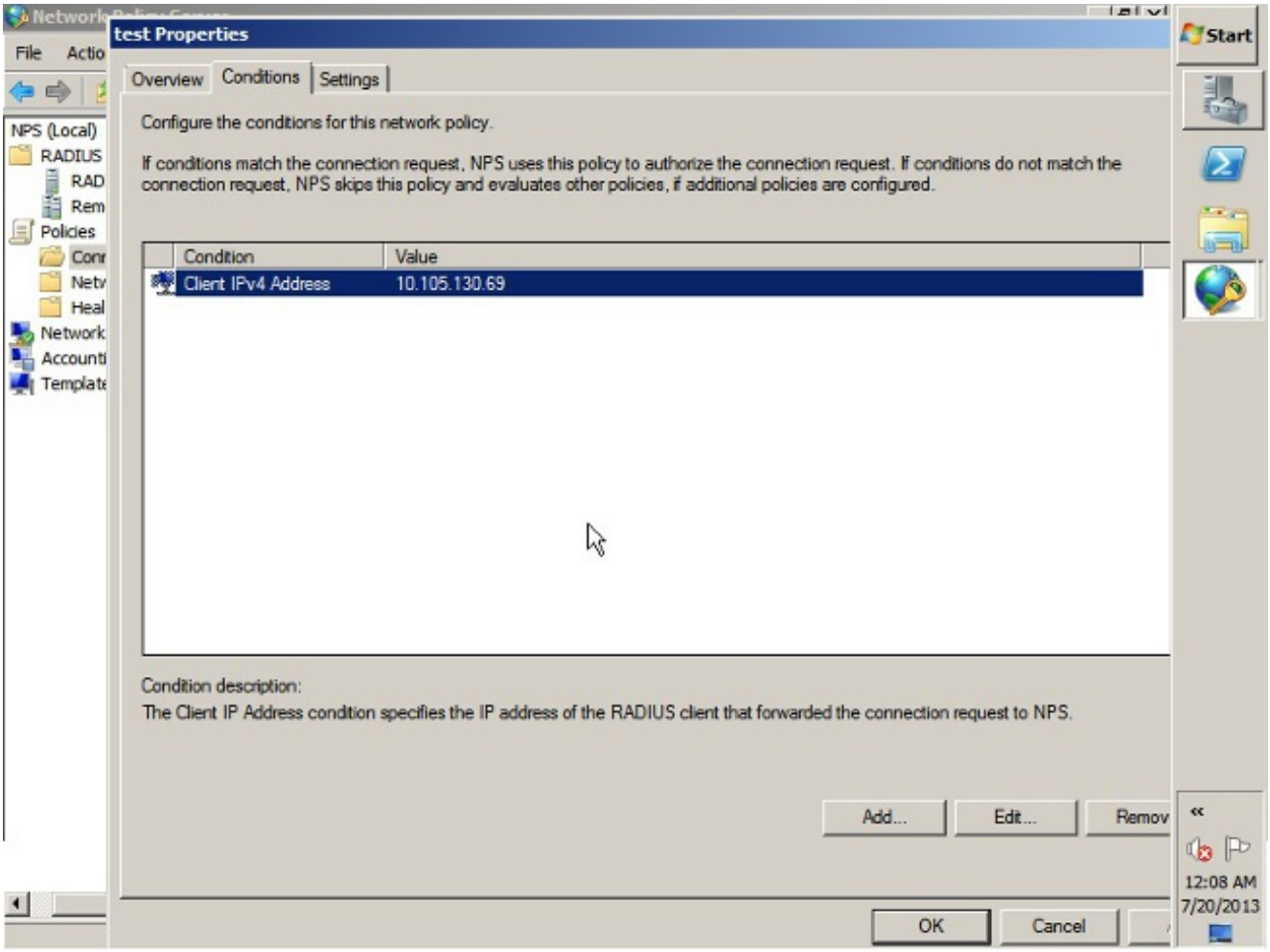
Fare clic sulla scheda **Avanzate**.Dall'elenco a discesa Nome fornitore scegliere **RADIUS Standard**.Fare clic su
OK.



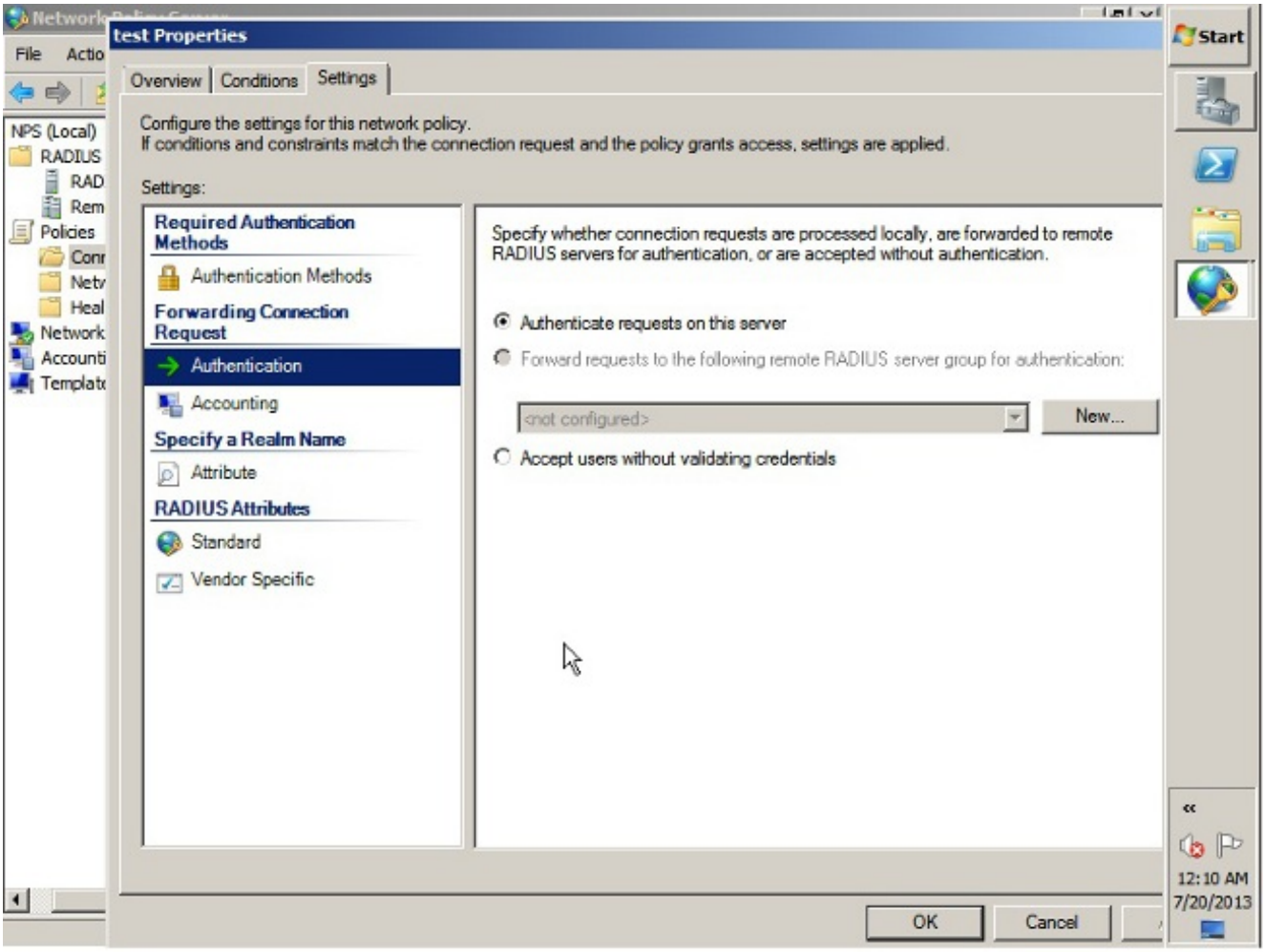
2. Crea un nuovo criterio di richiesta di connessione per gli utenti VPN. Lo scopo del criterio di richiesta di connessione è specificare se le richieste dei client RADIUS devono essere elaborate localmente o inoltrate ai server RADIUS remoti. In Server dei criteri di rete > Criteri fare clic con il pulsante destro del mouse su **Criteri di richiesta di connessione** e creare un nuovo criterio.Dall'elenco a discesa Tipo di server di accesso alla rete scegliere **Non specificato**.



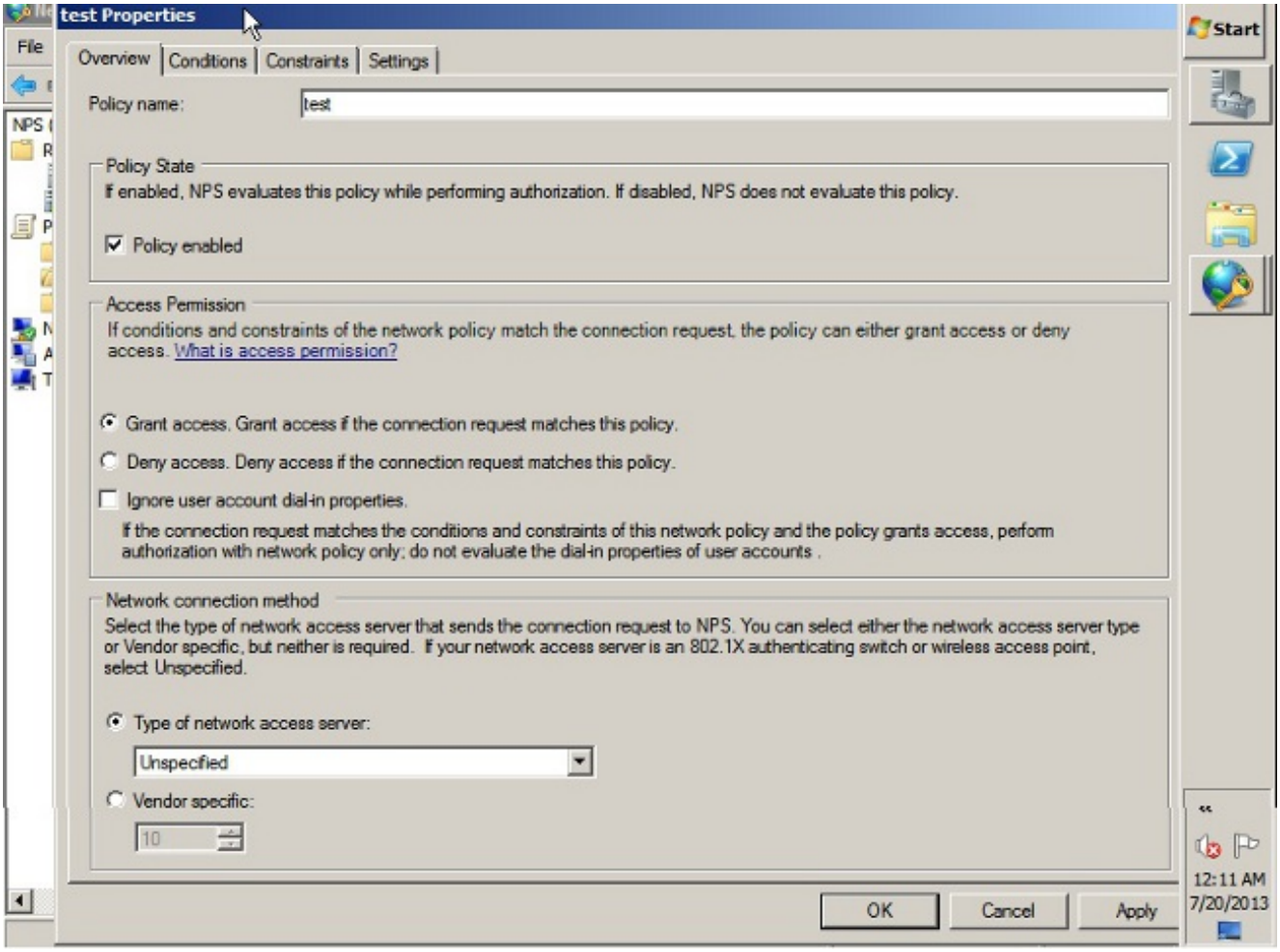
Fare clic sulla scheda **Condizioni**.Fare clic su **Add**.Immettere l'indirizzo IP dell'ASA come condizione 'Indirizzo IPv4
client'.



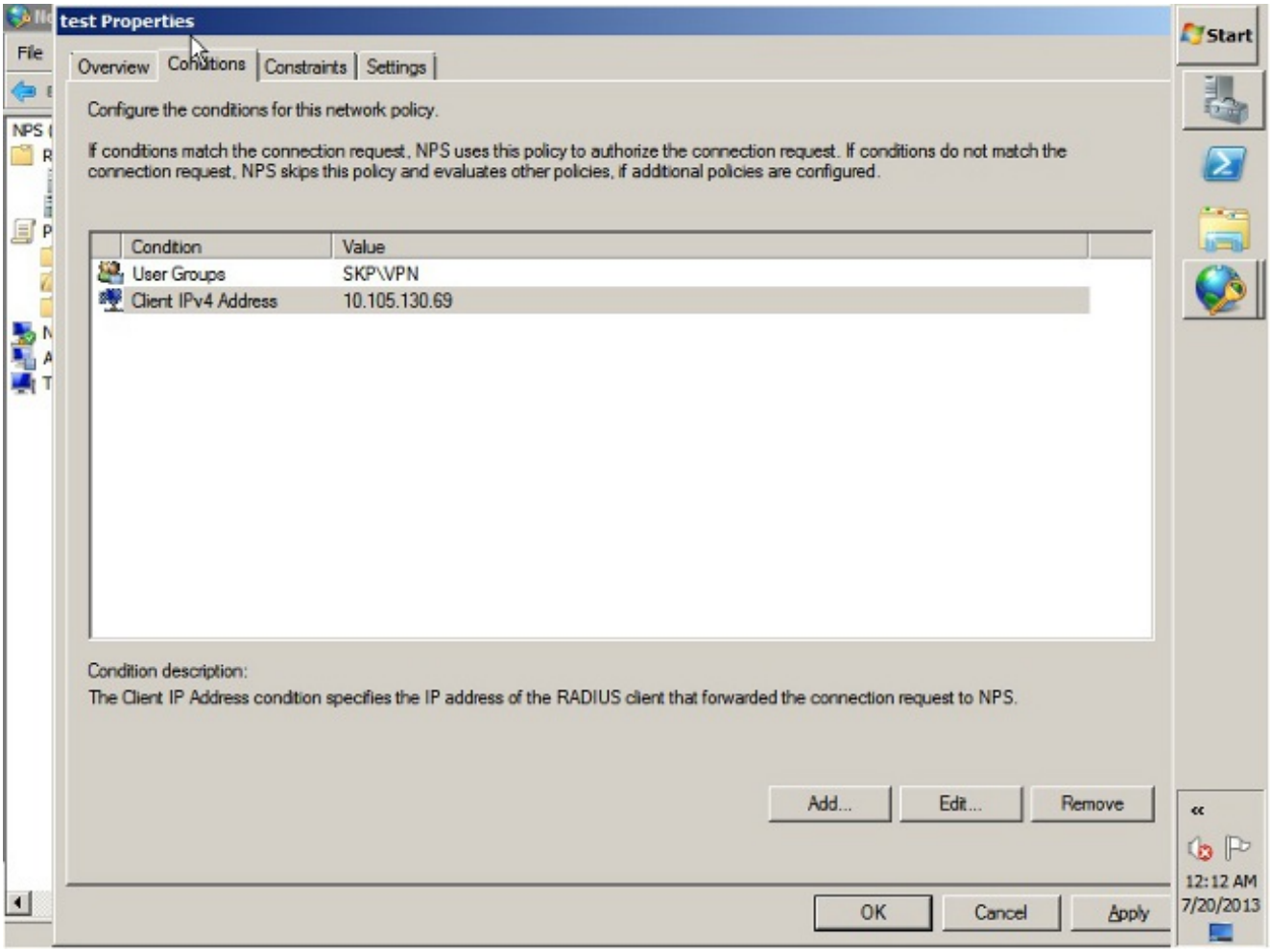
Fare clic sulla scheda **Impostazioni**.In Inoltro richiesta di connessione scegliere **Autenticazione**. Accertarsi che il pulsante di opzione Autentica richieste sul server sia selezionato.Fare clic su
OK.



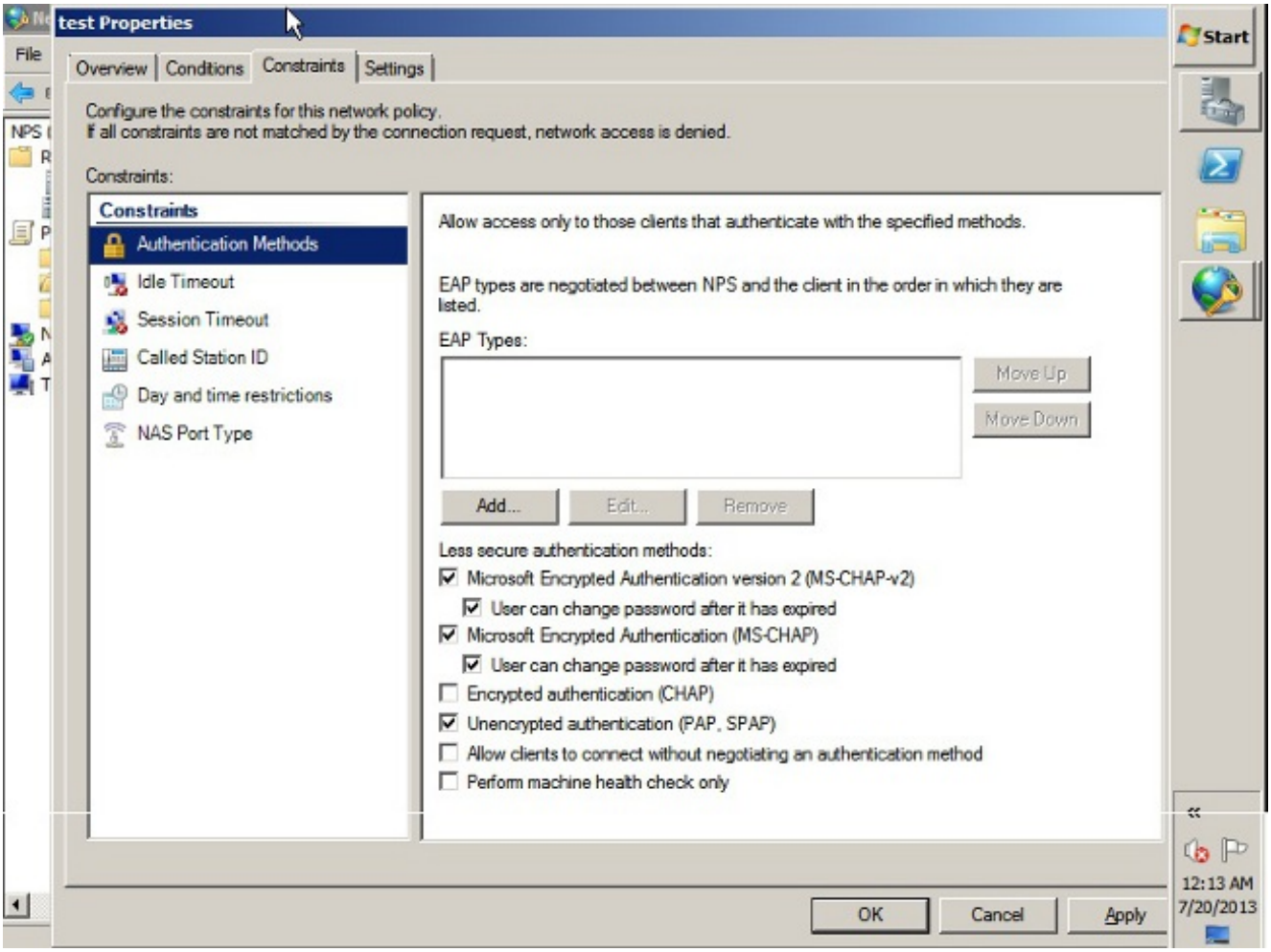
3. Aggiungere un criterio di rete in cui è possibile specificare gli utenti autorizzati all'autenticazione.Èad esempio possibile aggiungere gruppi di utenti di Active Directory come condizione. Solo gli utenti che appartengono a un gruppo di Windows specificato vengono autenticati in base a questo criterio.In Server dei criteri di rete scegliere **Criteri**.Fare clic con il pulsante destro del mouse su **Criteri di rete** e creare un nuovo criterio.Assicurarsi che sia selezionato il pulsante di opzione Concedi accesso.Dall'elenco a discesa Tipo di server di accesso alla rete scegliere **Non specificato**.



Fare clic sulla scheda **Condizioni**.Fare clic su **Add**.Immettere l'indirizzo IP dell'ASA come condizione dell'indirizzo IPv4 del client.Immettere il gruppo di utenti di Active Directory che contiene gli utenti
VPN.



Fare clic sulla scheda **Vincoli**.Scegliere **Metodi di autenticazione**.Assicurarsi che la casella di controllo Autenticazione non crittografata (PAP, SPAP) sia selezionata.Fare clic su **OK**.

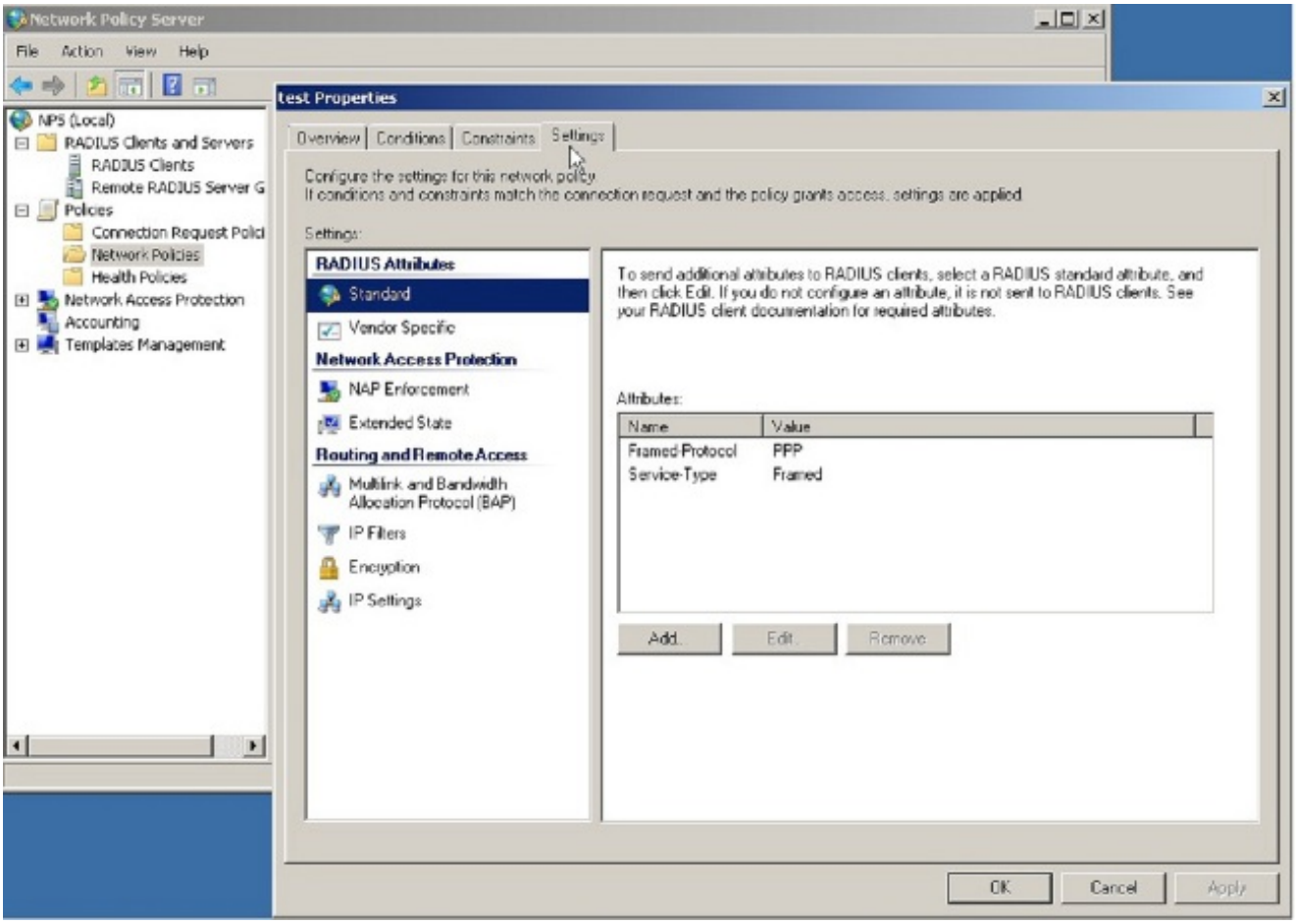


Passa l'attributo Criteri di gruppo (attributo 25) dal server RADIUS Server dei criteri di rete

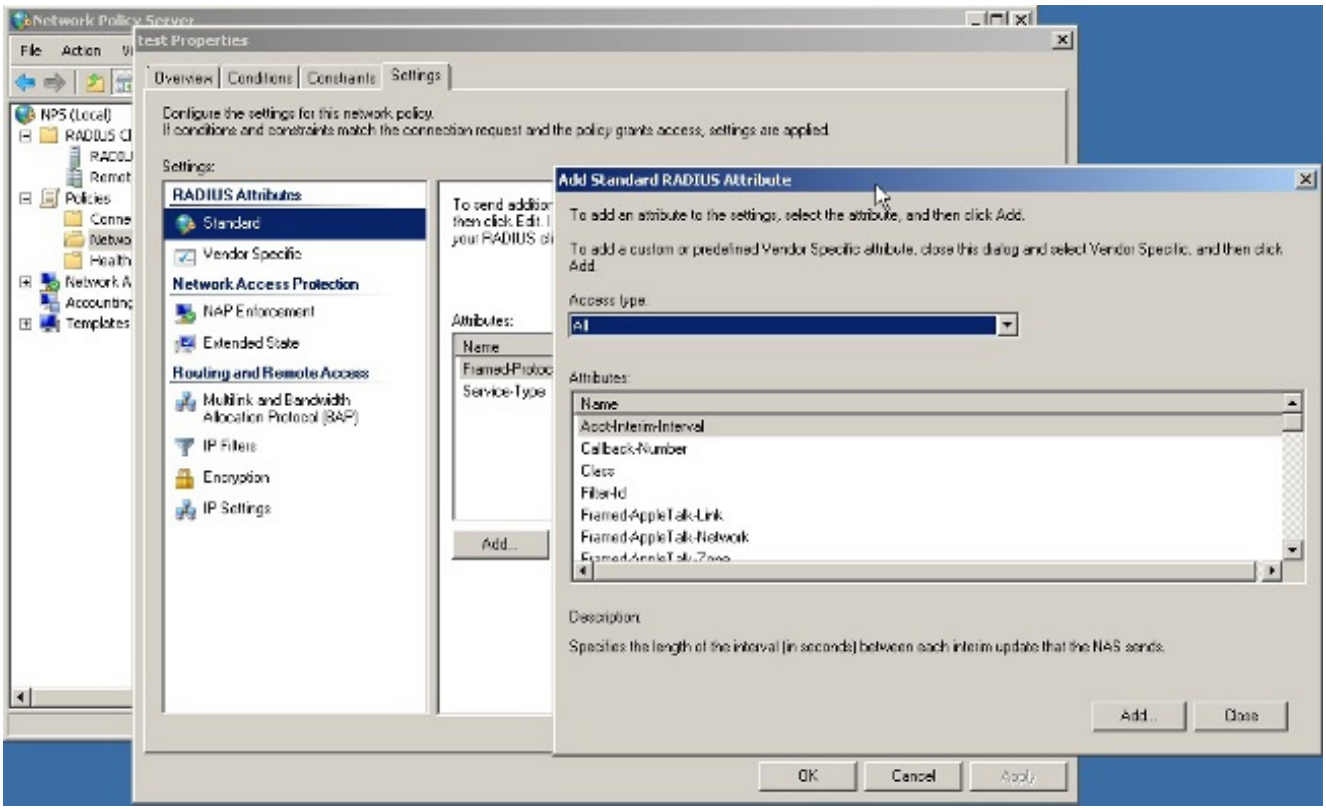
Se il criterio di gruppo deve essere assegnato dinamicamente all'utente con il server RADIUS Server dei criteri di rete, è possibile utilizzare l'attributo RADIUS del criterio di gruppo (attributo 25).

Completare questa procedura per inviare l'attributo RADIUS 25 per l'assegnazione dinamica di un criterio di gruppo all'utente.

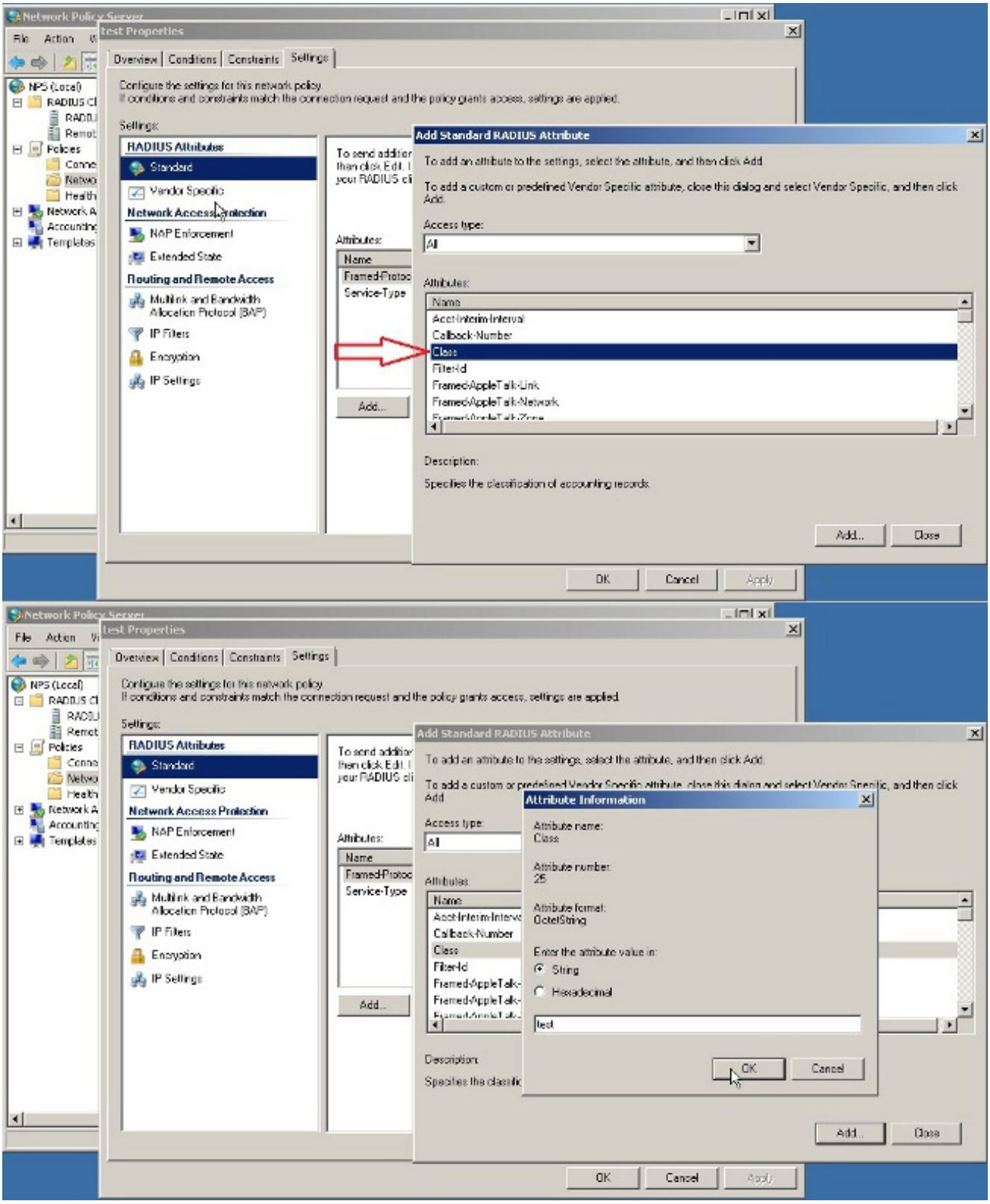
1. Dopo aver aggiunto il criterio di rete, fare clic con il pulsante destro del mouse sul criterio di rete desiderato e scegliere la scheda
   Impostazioni.



2. Scegliete **Attributi RADIUS > Standard**. Fare clic su **Add**. Lasciare il tipo di accesso Tutto.



3. Nella casella Attributi, scegliere **Classe**, quindi fare clic su **Aggiungi**. Immettere il valore dell'attributo, ovvero il nome del criterio di gruppo come stringa. Tenere presente che i criteri di gruppo con questo nome devono essere configurati nell'appliance ASA. In questo modo, l'ASA la assegna alla sessione VPN dopo aver ricevuto l'attributo nella risposta RADIUS.



Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

Debug dell'ASA

Abilitare il **raggio di debug** su **tutte** le appliance ASA.

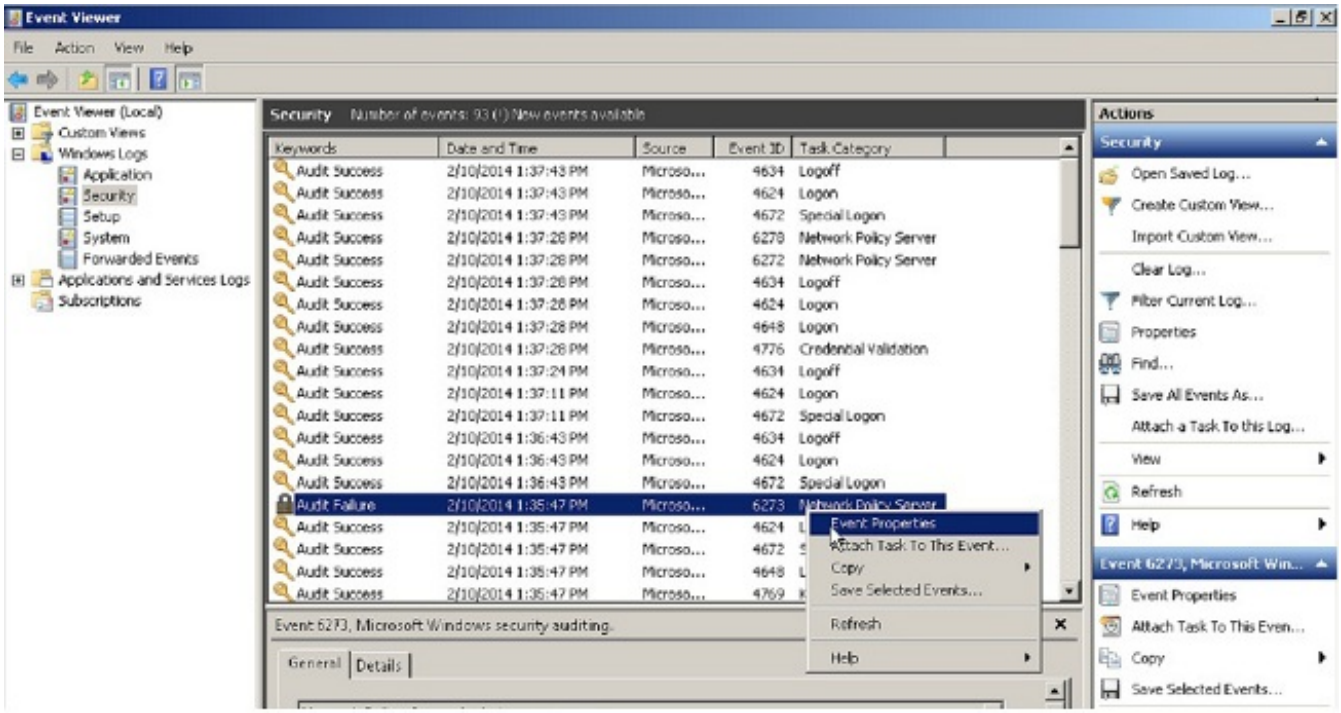
```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

- Verificare che la connettività tra l'appliance ASA e il Server dei criteri di rete sia corretta.Applicare le acquisizioni dei pacchetti per assicurarsi che la richiesta di autenticazione lasci l'interfaccia ASA (da cui è raggiungibile il server). Confermare che i dispositivi nel percorso non blocchino la porta UDP 1645 (porta di autenticazione RADIUS predefinita) per garantire che raggiunga Server dei criteri di rete. Per ulteriori informazioni sull'acquisizione dei pacchetti sull'appliance ASA, consultare il documento ASA/PIX/FWSM: Acquisizione di pacchetti mediante CLI e ASDM.
- Se l'autenticazione ha ancora esito negativo, controllare il Visualizzatore eventi in Server dei criteri di rete di Windows. In Visualizzatore eventi > Registri di Windows scegliere **Protezione.** Cercare gli eventi associati a Server dei criteri di rete nel periodo di tempo della richiesta di autenticazione.



Dopo aver aperto Proprietà evento, dovrebbe essere possibile visualizzare il motivo dell'errore come illustrato nell'esempio. Nell'esempio riportato sotto, il tipo di autenticazione PAP non è stato scelto in Criteri di rete. La richiesta di autenticazione ha pertanto esito negativo.

```
 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.**