Palo Alto
Admin Access via Microsoft IAS
Step by step guide

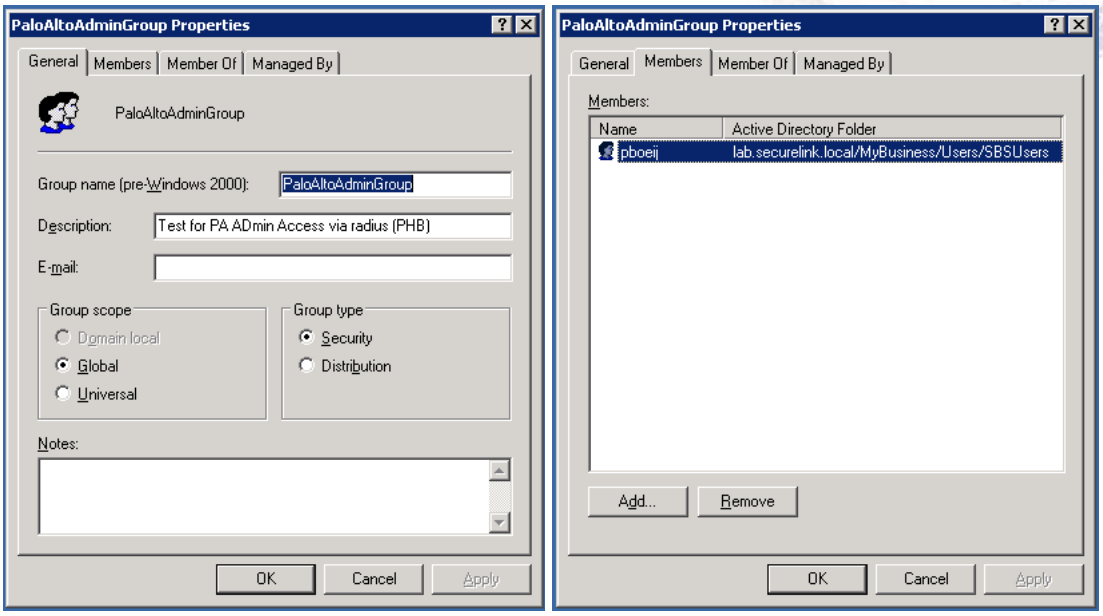
Prepared for:
Securelink
Uilenbaan 80
2160 Wommelgem

Prepared by:
Philippe Boeij
Version 1
Thursday, 23 September 2010

1 Table of Contents

2 Microsoft Active Directory

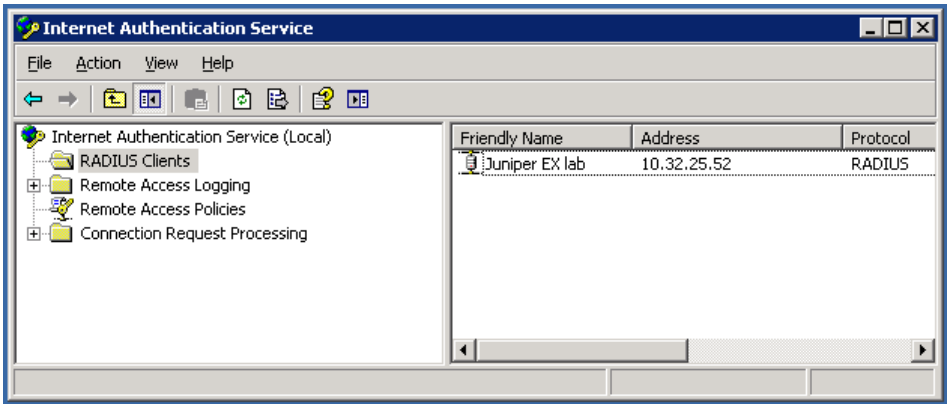
In needed, create a new security group and add some users to this group. Otherwise an existing security group can be used. Only users who are member of this group will be able to access the administration pages of the Palo Alto.



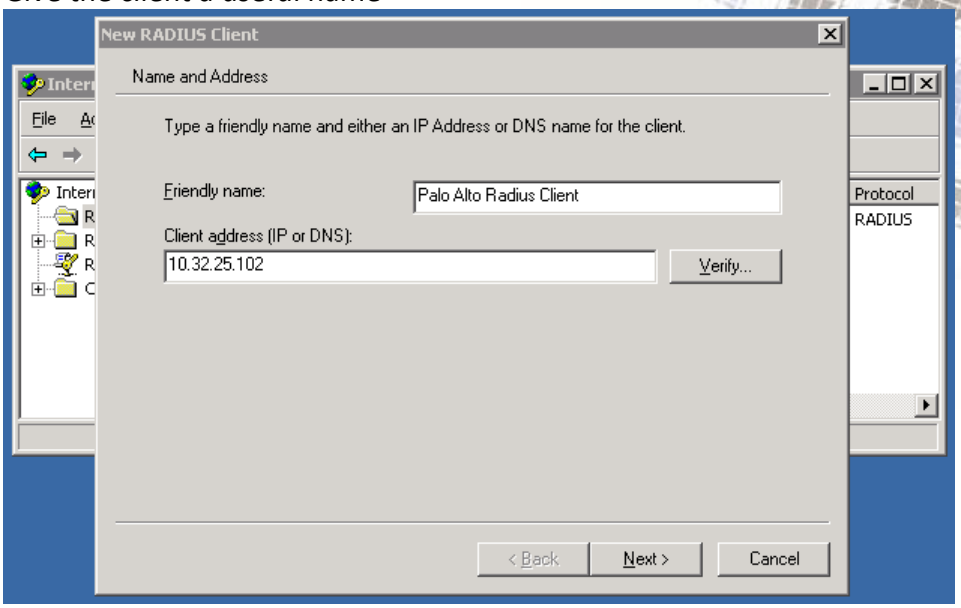
3 Microsoft Internet Authentication Service (IAS)

3.1 Create a new radius client.

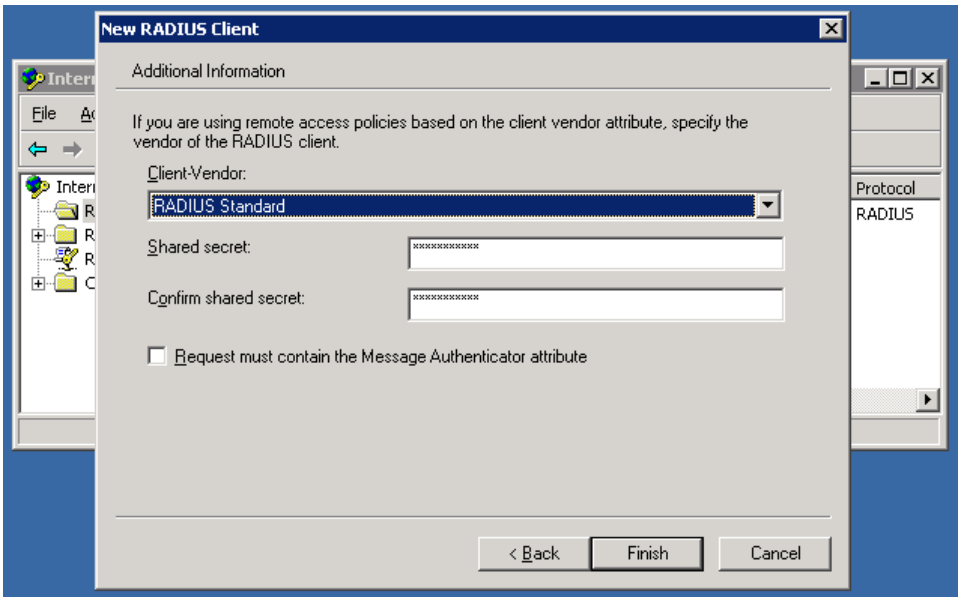
Action -> New Radius Client



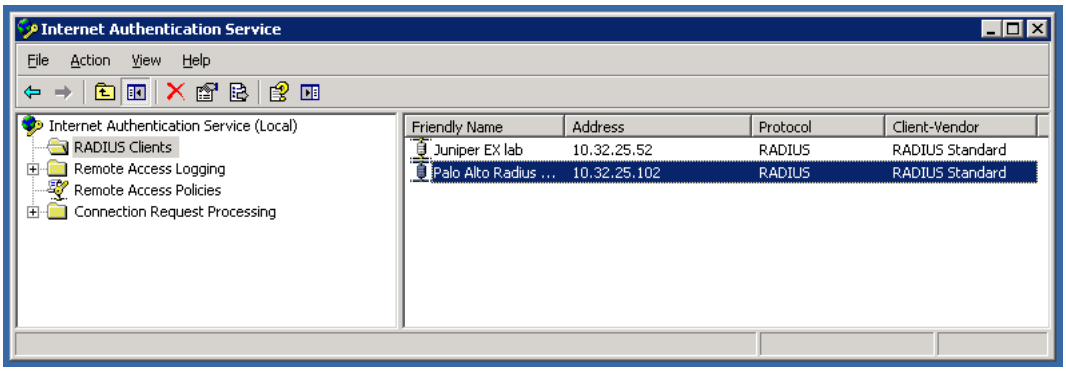
Give the client a useful name



Enter a shared secret for communication between the Palo Alto firewall and the Windows server.

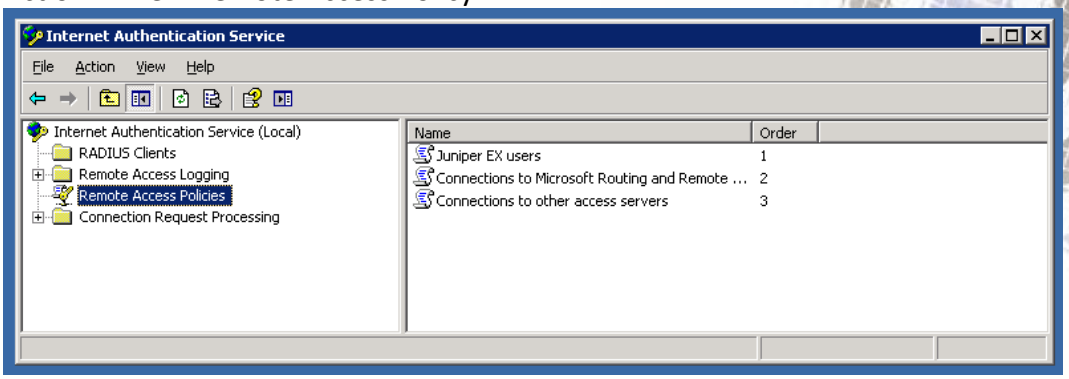


Click finish

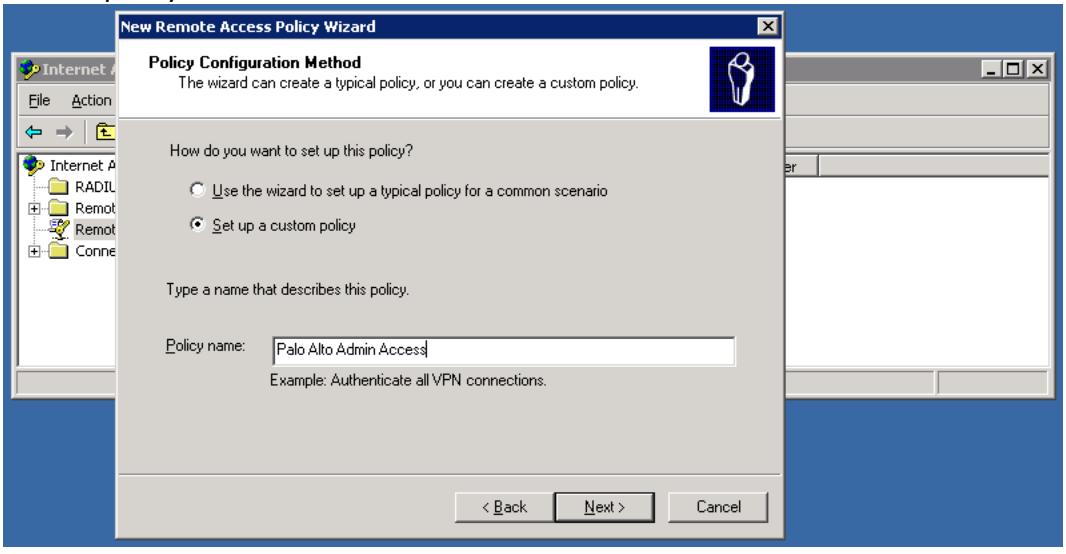


3.2 Create a new remote access policy

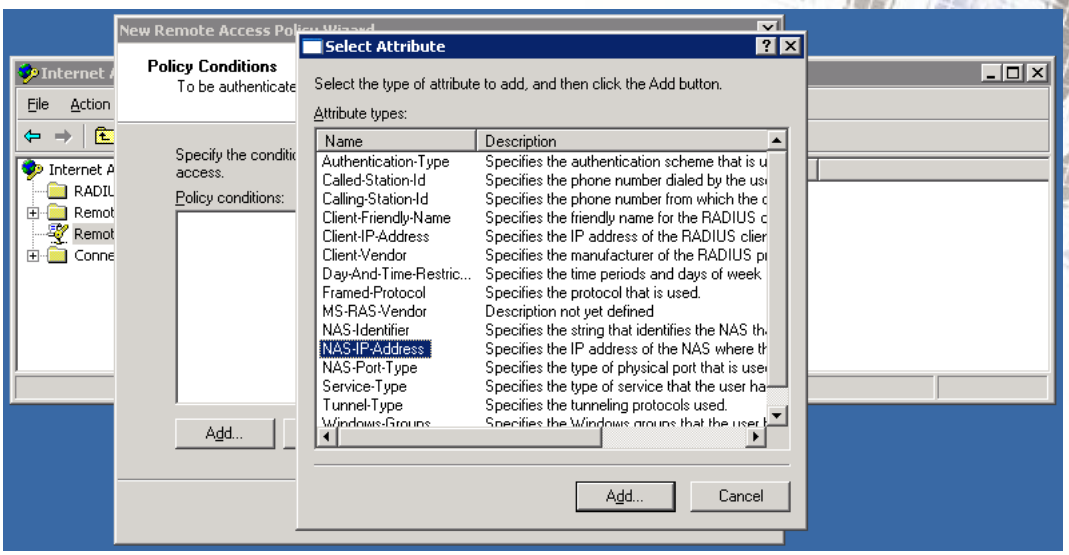
Action -> New Remote Access Policy

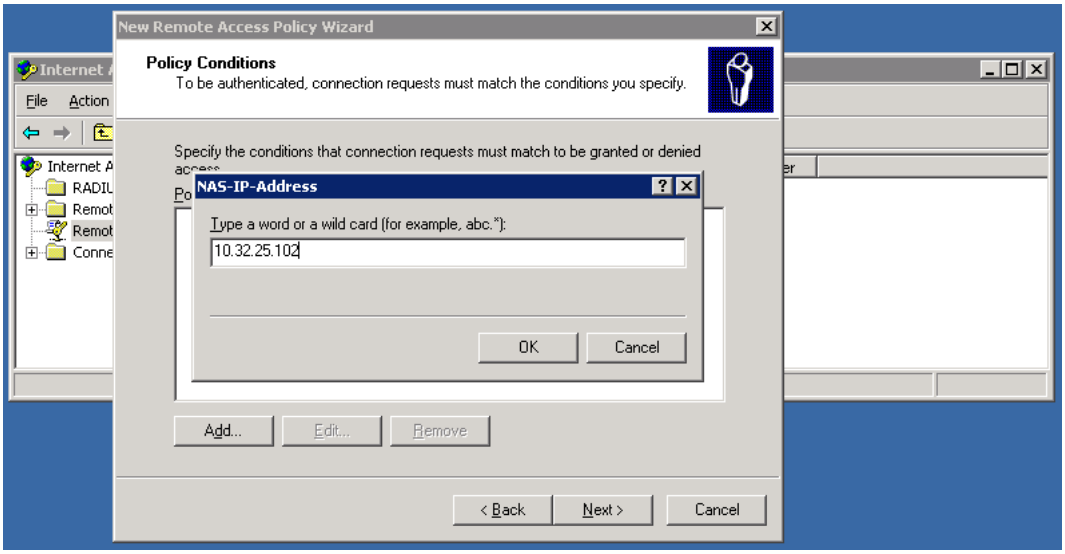


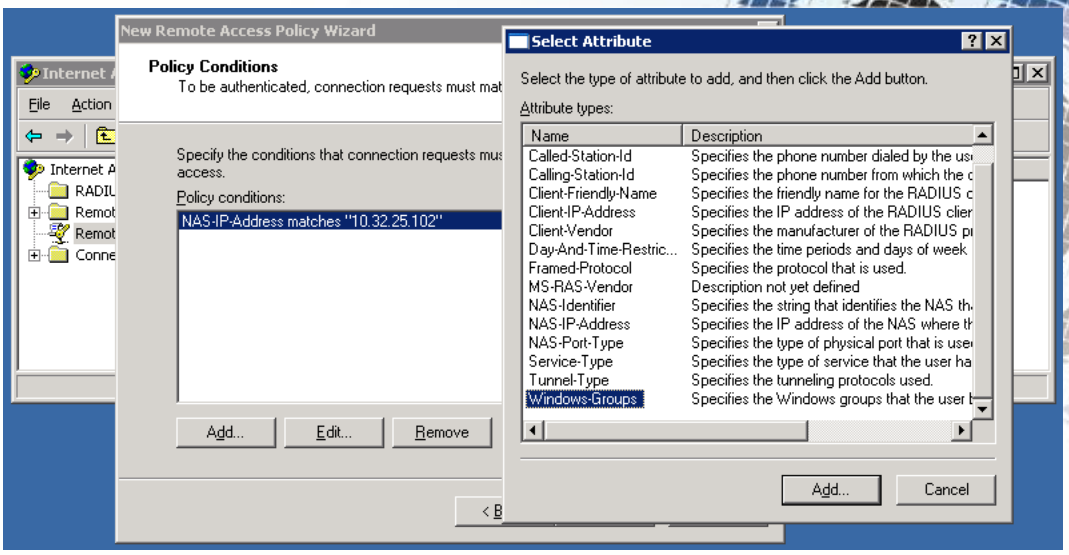
Enter a policy name

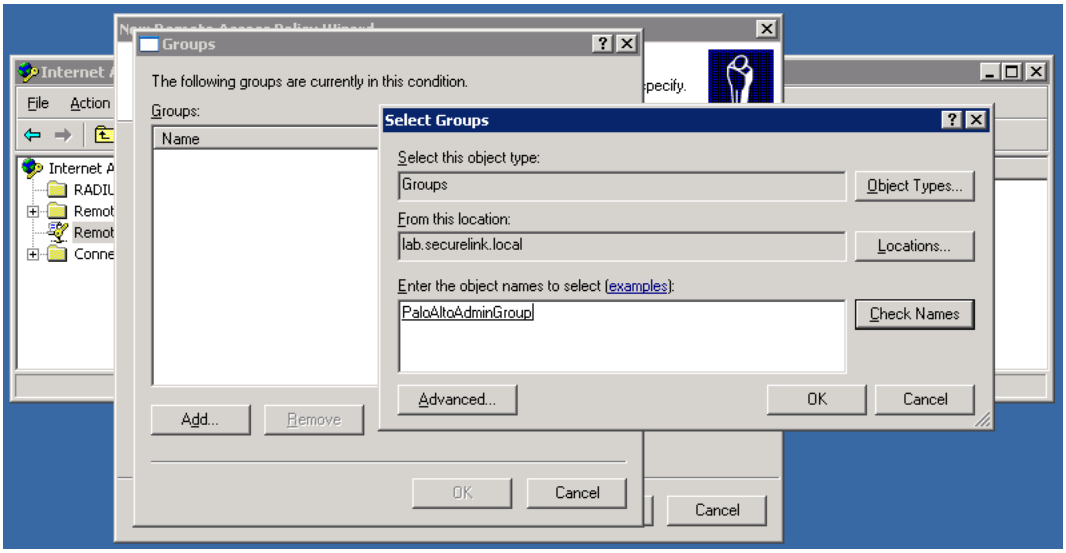


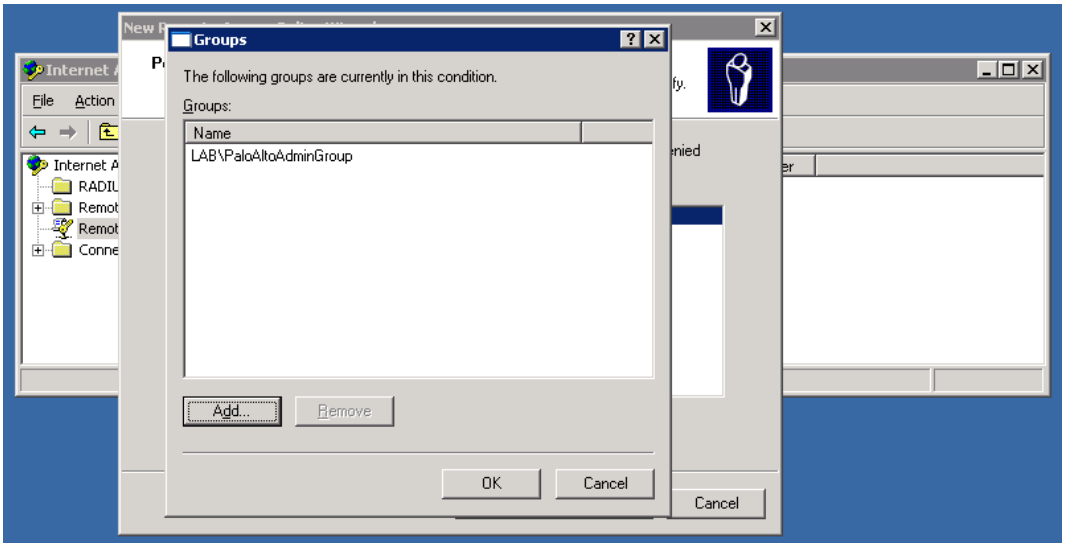
Add some ‘filters’ to limit who can use this Access Policy. We’ll add the IP address of the firewall and we’ll add an AD Security Group.



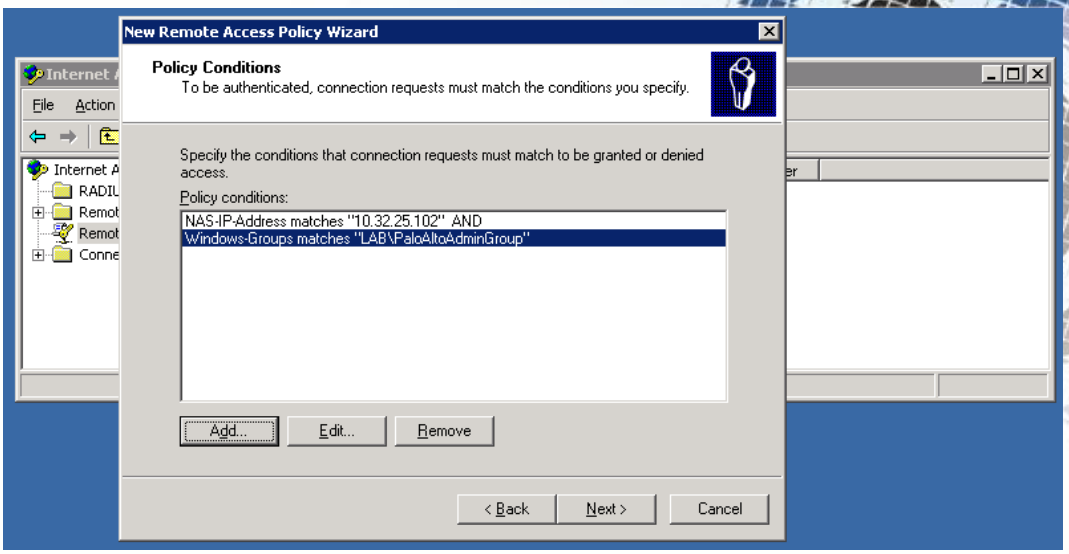






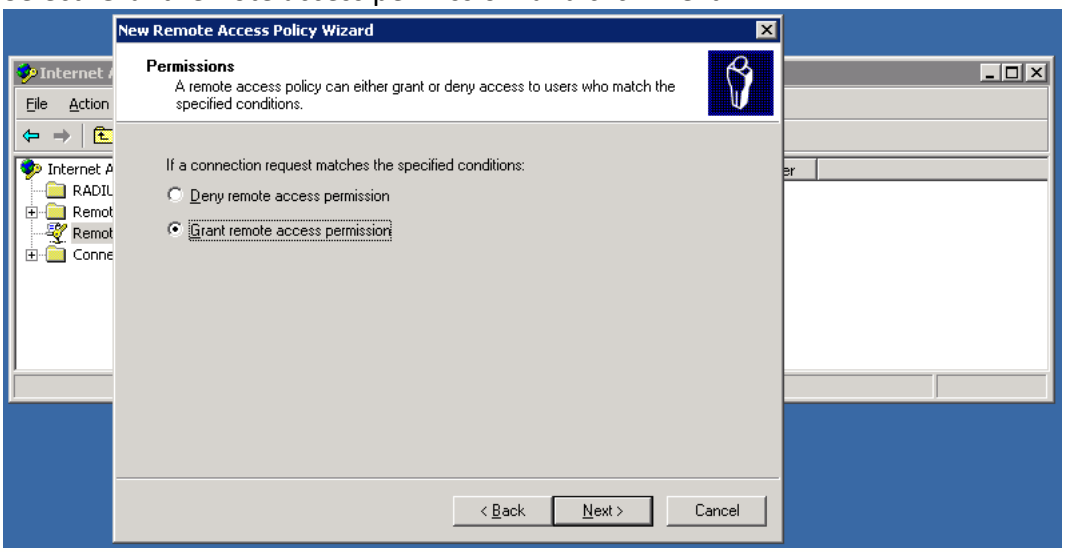


It will look like this:



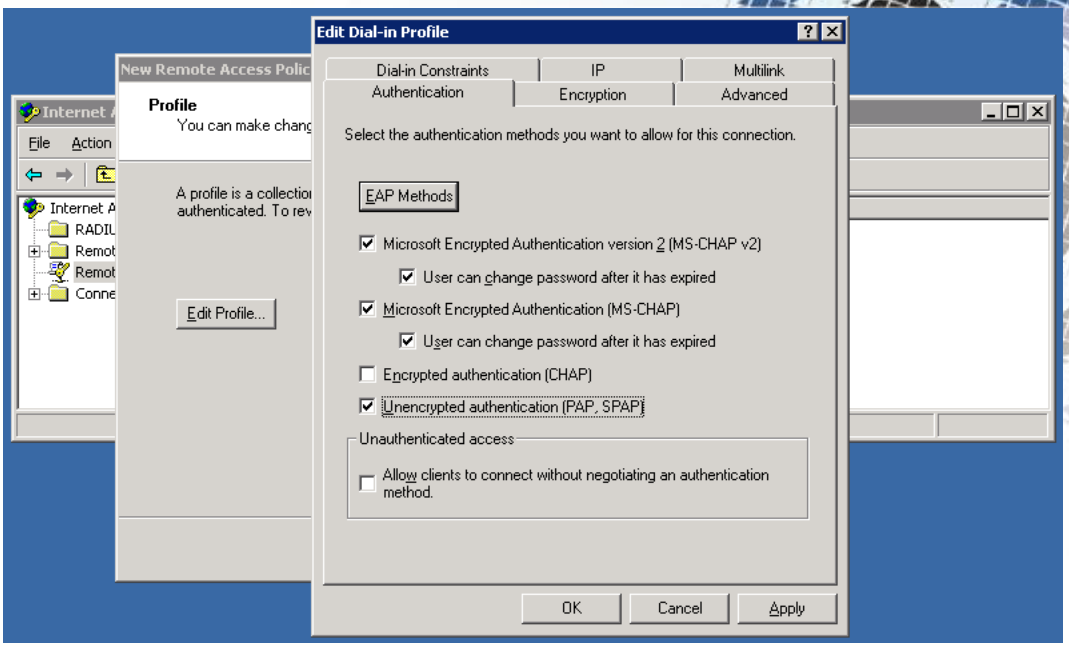
Click 'Next' to continue…

Select 'Grant remote access permission' and click 'Next'.

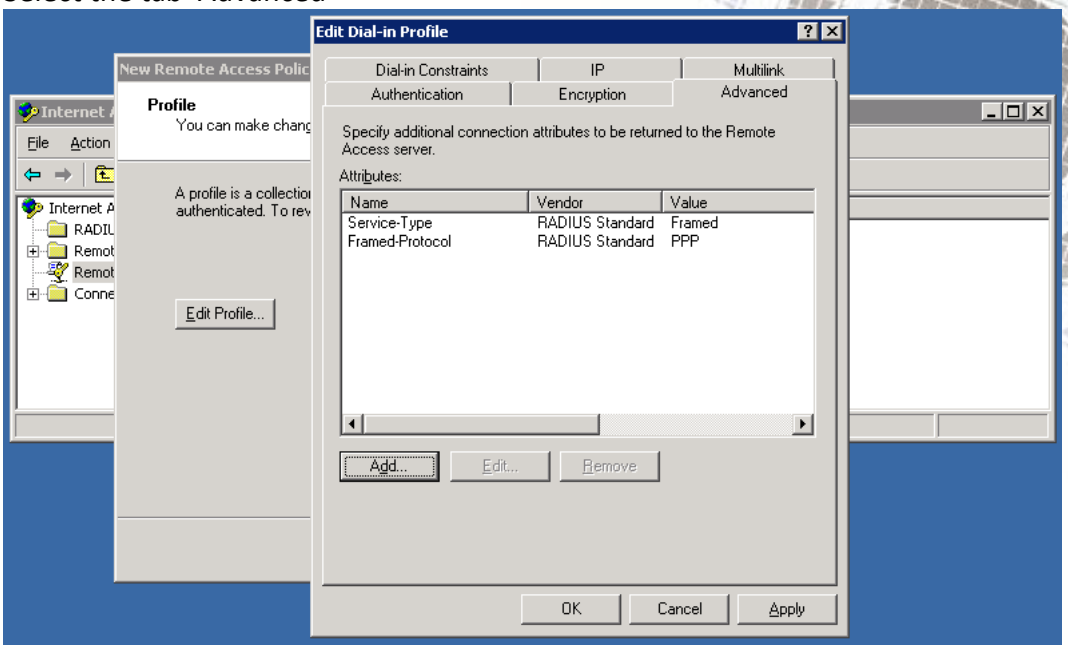


3.3 Modify the 'Dial in Profile'

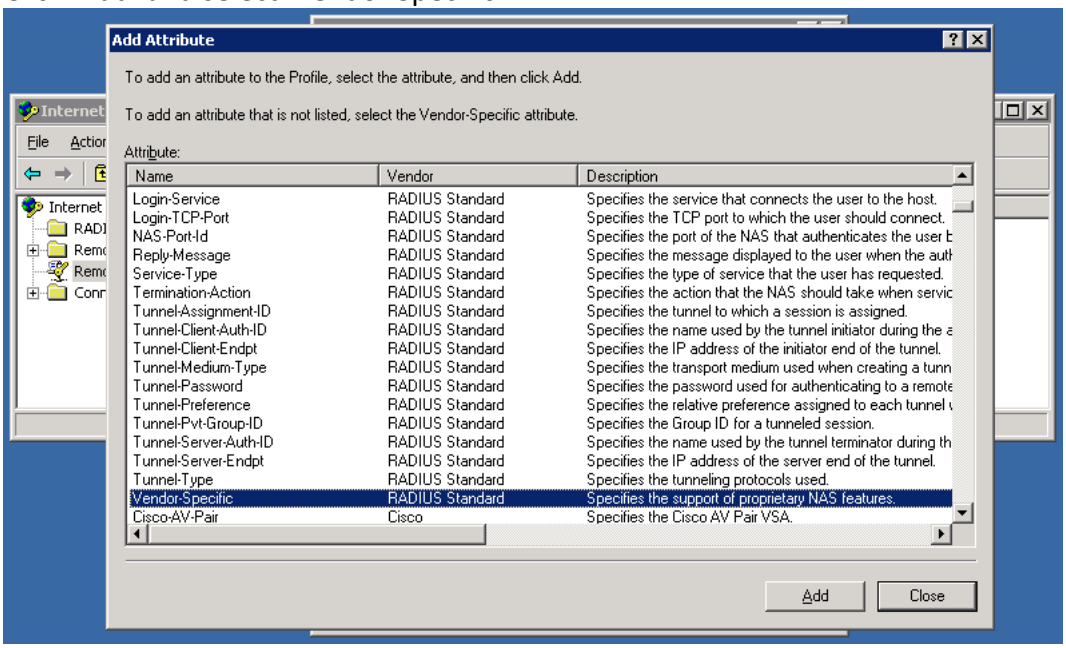
Click 'Edit Profile' and select the tab 'Authentication'. Check 'Unencrypted authentication'


Edit Dial-in Profile
Dial-in Constraints
IP
Multilink
Authentication
Encryption
Advanced
Select the authentication methods you want to allow for this connection.
EAP 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)
Unauthenticated access
Allow clients to connect without negotiating an authentication method.
OK
Cancel
Apply
New Remote Access Polic
Profile
You can make chang
A profile is a collectio
authenticated. To rev
Edit Profile...
Internet A
File
Action
Internet A
RADIU
Remot
Remot
Conne

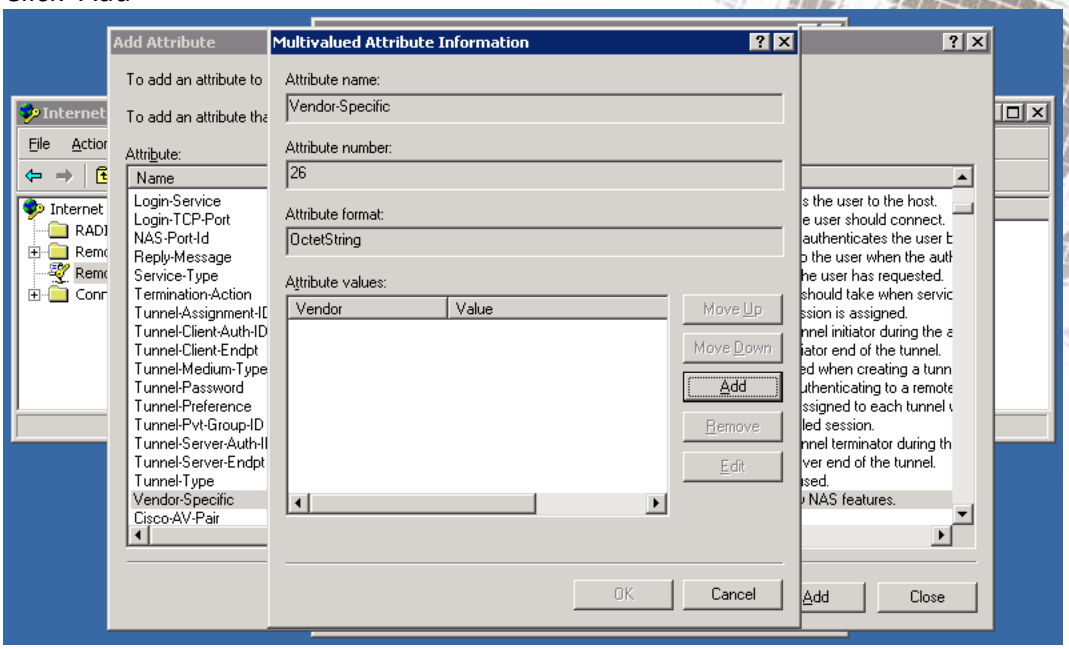
Select the tab ‘Advanced’



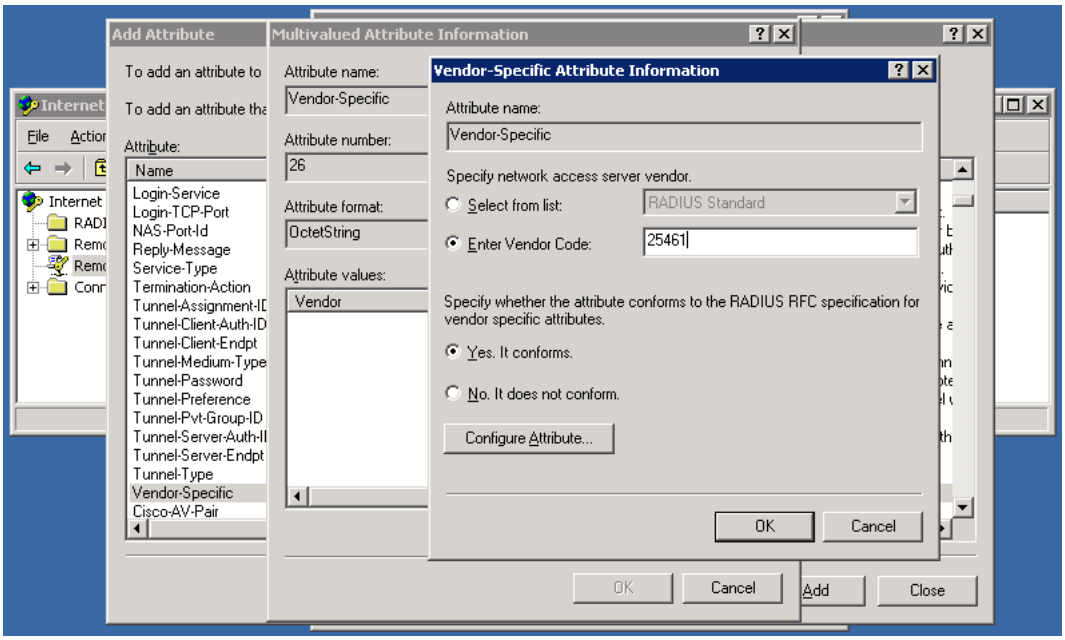
Click ‘Add’ and select ‘Vendor Specific’



Click ‘Add’



Enter vendor code ‘25461’ and select ‘Yes. It conforms’.

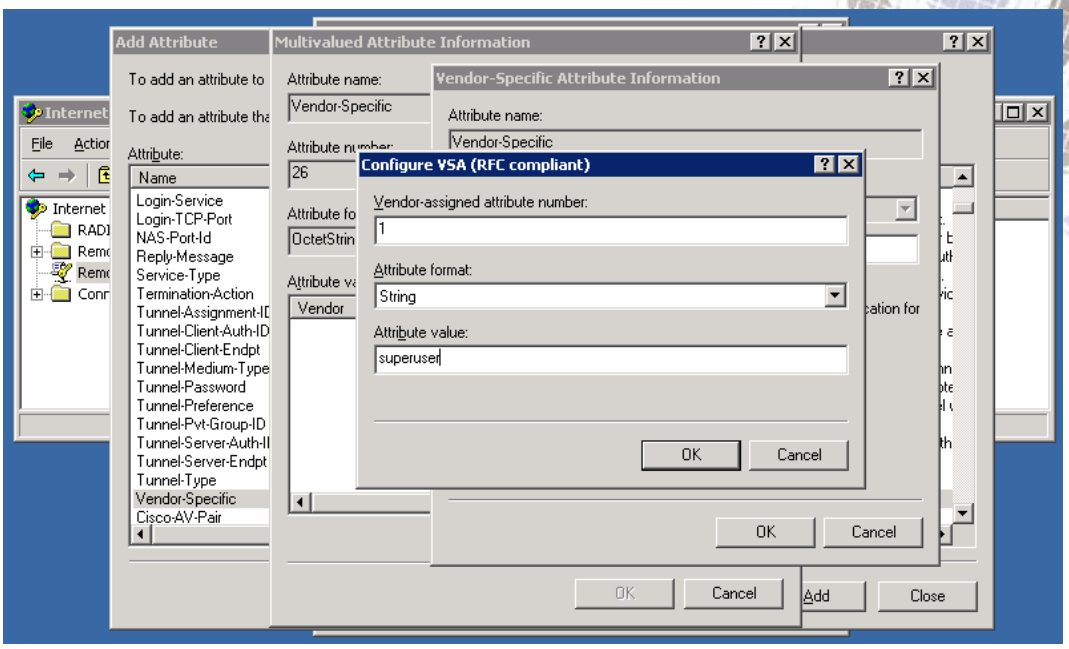


Click ‘Configure Attribute’. Here we add custom attribute number 1 and value ‘superuser’.

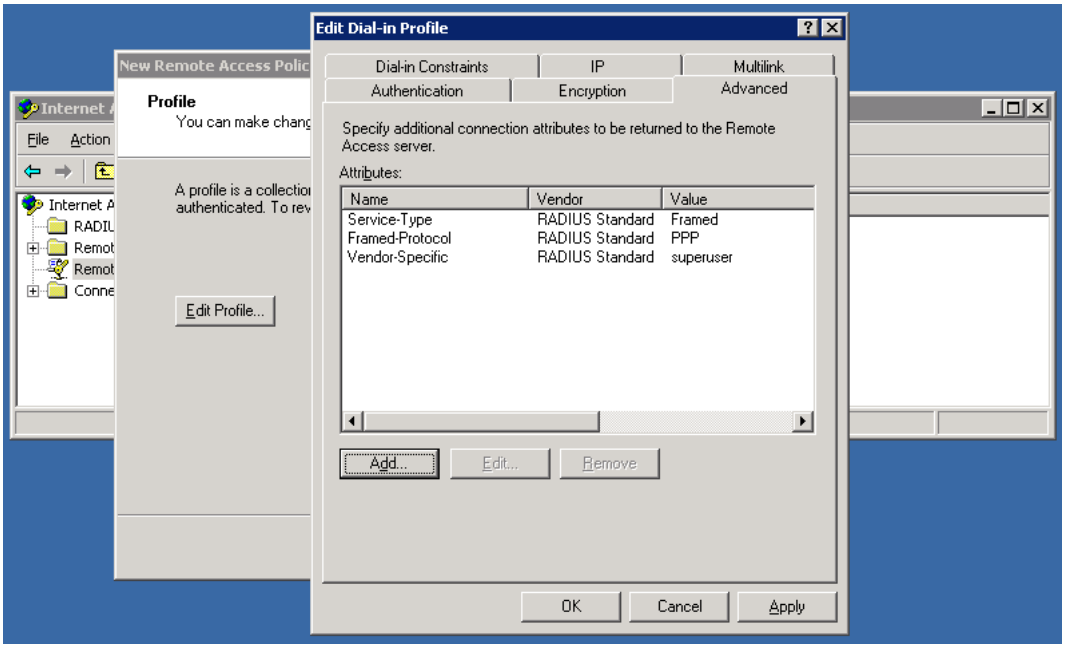
Possible values (from the Palo Alto knowledge base):

```
VENDOR          PaloAlto                        25461
ATTRIBUTE       PaloAlto-Admin-Role                     1
string          PaloAlto
# PaloAlto-Admin-Role is the name of the role for the user
# it can be the name of a custom Admin role profile configured on the
# PAN device or one of the following predefined roles
# superuser : Superuser
```

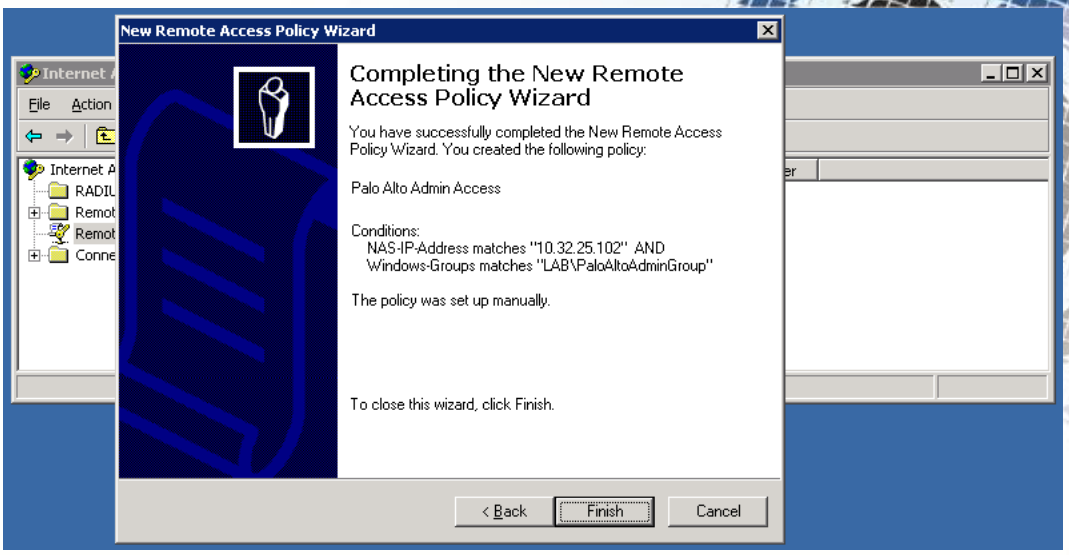
```
# superreader : Superuser (read-only)
# deviceadmin : Device administrator
# devicereader : Device administrator (read-only)
# vsysadmin : Virtual system administrator
# vsysreader : Virtual system administrator (read-only)
```



It will look like:



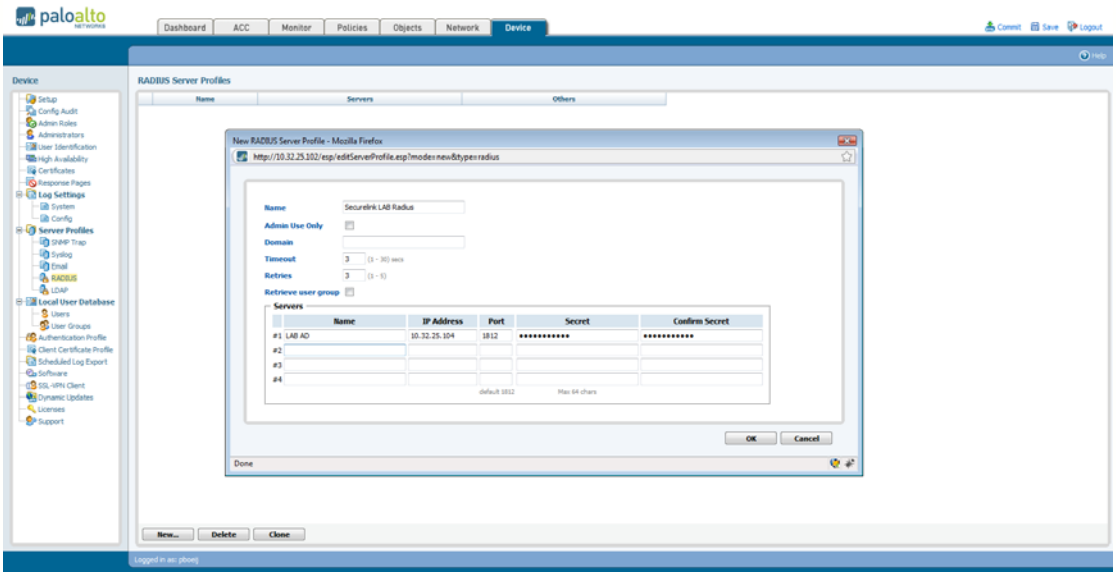
Close all open windows



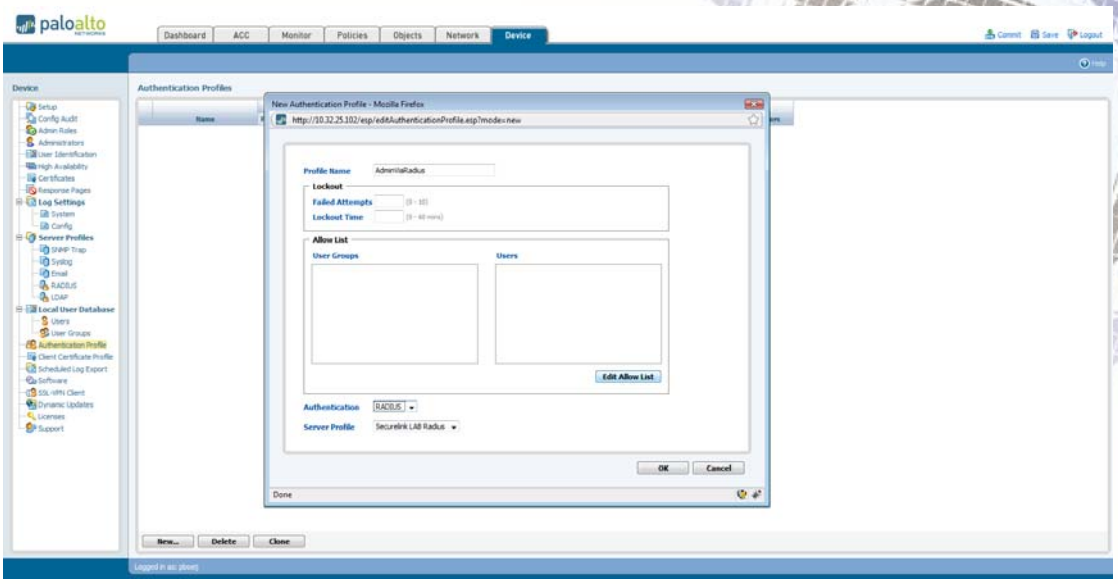
So a successful authentication will be returns only if the request is received from ip address 10.32.25.102 and if the user is member of the windows security group 'PaloAltoAdminGroup'.

4 Palo Alto

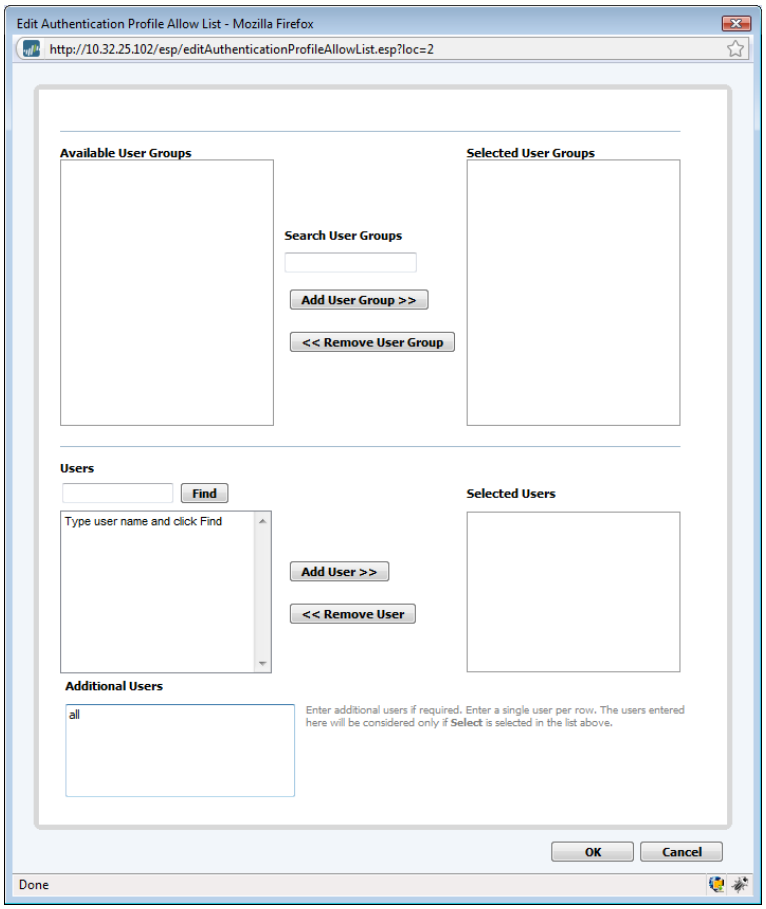
4.1 Create a new Radius Server Profile

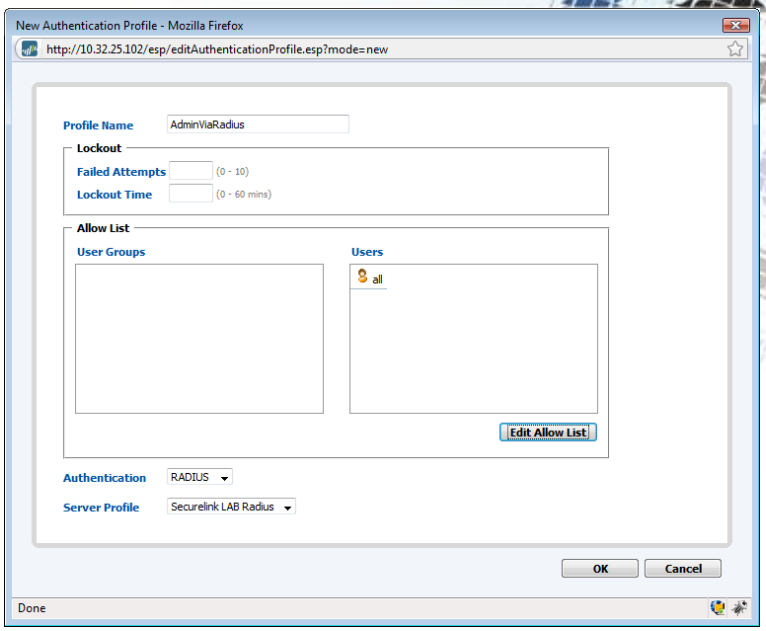


4.2 *Create a new Authentication profile*



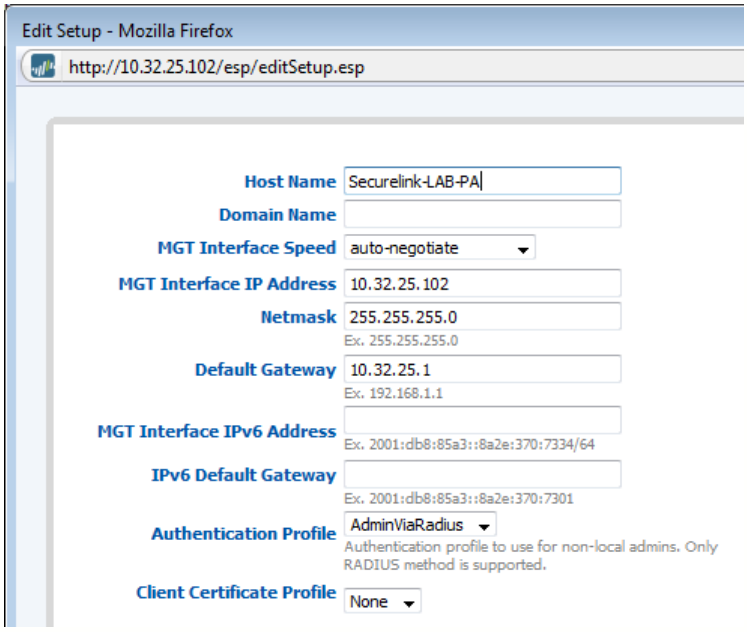
Edit the Allow List and add the user ‘all’. This will allow any user that can authenticate via the defined Radius server (therefore we added the ‘Windows-Group’ restriction in the IAS profile).





4.3 Edit Admin access

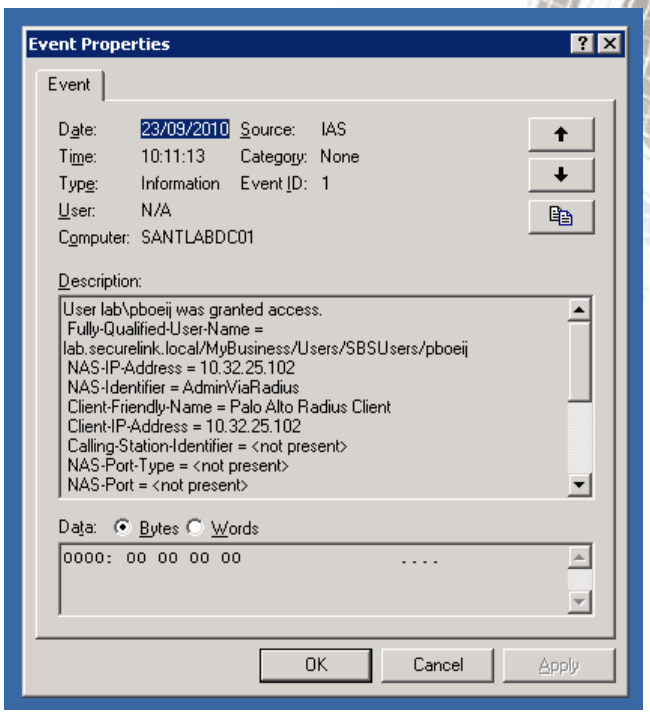
The last step: add the radius authentication profile for admin access. Tab 'Device' -> Setup -> Edit and change the 'Authentication Profile'.



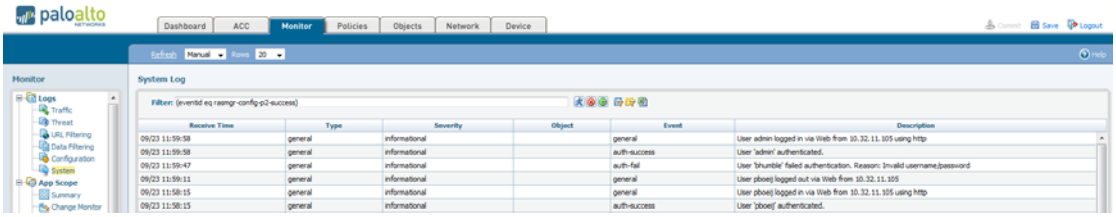
Don't forget to commit all changes.

From now, users in the AD group 'PaloAltoAdminGroup' can logon onto the Palo Alto firewall.

Event log on the Windows server:



System log on the Palo Alto firewall



For Windows 2008 configuration guide, I can refer to a document on the support site of Palo Alto: https://live.paloaltonetworks.com/docs/DOC-1561